

Repeater-based quantum communication with advanced optical encoding

Dissertation zur Erlangung des Grades
„Doktor der Naturwissenschaften“

am Fachbereich Physik, Mathematik und Informatik
der Johannes Gutenberg-Universität in Mainz



eingereicht von
Frank Schmidt
geboren in Wiesbaden

Mainz, Mai 2023

Datum der mündlichen Prüfung: 7. November 2023

Zusammenfassung

Quantenkommunikation ermöglicht es Nachrichten informationstheoretisch beweisbar sicher zu verschlüsseln, wobei die Datenübertragungsraten über große Distanzen durch Verluste und Fehler stark reduziert sind. Diese niedrigen Übertragungsraten können durch den Einsatz von Quantenrepeatern, die die Gesamtdistanz in mehrere kleine Teildistanzen aufteilen, verbessert werden. In dieser Arbeit werden zwei unterschiedliche Ansätze von Quantenrepeatern untersucht. Bezüglich speicherbasierter Quantenrepeater schlagen wir ein neues Schema vor, das auf der Interferenz einzelner Photonen basiert und durch das kürzlich vorgestellte Twin-field Quantenschlüsselaustauschprotokoll inspiriert wurde. Außerdem werden erreichbare Datenübertragungsraten geheimer Schlüssel, die bereits mit kleinen Quantenrepeatern auf unterschiedlichen physikalischen Plattformen erzielt werden können, auf Grundlage von experimentell vorgegebenen Parametern berechnet. Des Weiteren werden auch größere Quantenrepeater untersucht, wobei wir das Dephasieren der Quantenspeicher exakt berechnen. Damit werden dann auch Übertragungsraten geheimer Schlüssel für verschiedene speicherbasierte Quantenrepeater berechnet und miteinander verglichen. Bezüglich des alternativen Ansatzes eines Quantenrepeaters basierend auf Quantenfehlerkorrektur stellen wir zunächst eine experimentell einfachere Möglichkeit, die auf linearer Optik beruht, vor, um das Fehlersyndrom eines GKP Codes zu bestimmen. Diese Methode führt zusätzlich zu geringeren Fehlerraten und wir diskutieren auch Grenzen der linearen Optik. Schlussendlich wenden wir diese Methoden im Kontext eines auf GKP Qudits basierenden Quantenrepeaters an. Dabei zeigt sich, dass es für in der näheren Zukunft experimentell sinnvolle Parameter besser ist GKP Qubits anstatt höherdimensionaler GKP Qudits zu nutzen.

Abstract

Quantum communication makes it possible to encrypt messages providing information-theoretic security, but suffers from a large decrease of the transmission rate for larger distances due to loss and errors. These low rates can be increased by employing quantum repeaters which divide the total distance into multiple smaller segments and this thesis deals with two different approaches for such quantum repeaters. Regarding quantum repeaters employing memories we propose a new scheme based on single-photon interference inspired by the recently discovered twin-field quantum key distribution protocol. Furthermore, we calculate secret-key rates obtainable in small-scale repeaters with different physical platforms using realistic parameters obtained from experimentalists and we also perform an analysis for larger repeaters where we calculate the memory dephasing exactly and compare secret-key rates for different memory-based repeater proposals. Concerning the repeater approach employing solely quantum error correction we propose experimentally simpler methods of obtaining the error syndrome for GKP codes based on linear optics also leading to an improved performance and we also discuss limitations of linear optics. We then apply these methods of GKP error correction to a repeater employing GKP qudits. There we find that for experimentally reasonable parameters in the near future it is better to use GKP qubits instead of high-dimensional GKP qudits.

List of publications

The main part of this dissertation consists of the following five papers:

- Paper I** Frank Schmidt and Peter van Loock,
“Memory-assisted long-distance phase-matching quantum key distribution”,
Phys. Rev. A **102**, 042614 (2020).
- Paper II** Peter van Loock, Wolfgang Alt, Christoph Becher, Oliver Benson, Holger Boche, Christian Deppe, Jürgen Eschner, Sven Höfling, Dieter Meschede, Peter Michler, Frank Schmidt, and Harald Weinfurter,
“Extending Quantum Links: Modules for Fiber- and Memory-Based Quantum Repeaters”,
Advanced Quantum Technologies **3** (11), 1900141 (2020).
- Paper III** Frank Schmidt and Peter van Loock,
“Quantum error correction with higher Gottesman-Kitaev-Preskill codes: minimal measurements and linear optics”,
Phys. Rev. A **105**, 042427 (2022).
Editors’ Suggestion
- Paper IV** Lars Kamin, Evgeny Shchukin, Frank Schmidt, and Peter van Loock,
“Exact rate analysis for quantum repeaters with imperfect memories and entanglement swapping as soon as possible”,
Phys. Rev. Research **5**, 023086 (2023)
- Paper V** Frank Schmidt, Daniel Miller, and Peter van Loock,
“Error-corrected quantum repeaters with GKP qudits”,
arXiv:2303.16034, submitted to Quantum (2023).

Although not part of this dissertation, I was also involved in the following publications during my work as a PhD student. However, this was mostly in the process of writing the papers and making only minor contributions to their actual content. My major contributions to their content originate from my bachelor and master theses.

- Paper VI** Evgeny Shchukin, Frank Schmidt, and Peter van Loock,
“Waiting time in quantum repeaters with probabilistic entanglement swapping”,
Phys. Rev. A **100**, 032322 (2019).
- Paper VII** Frank Schmidt and Peter van Loock,
“Efficiencies of logical Bell measurements on Calderbank-Shor-Steane codes with static linear optics”,
Phys. Rev. A **99**, 062308 (2019).

During my PhD I contributed the discussion of the asymptotic waiting time with deterministic entanglement swapping (Sec. III) to the content of **Paper VI** and the idea of randomized Bell measurements (App. F) to the content of **Paper VII**.

Contents

1	Introduction	1
2	Background	3
2.1	Basic quantum information theory	3
2.2	Quantum optics	9
2.2.1	Quantization of the electromagnetic field	9
2.2.2	Passive linear optics	10
2.2.3	Squeezing operations	10
2.2.4	Coherent states	11
2.2.5	Noise channels	12
2.2.6	Detectors	12
2.3	Quantum error correction	14
2.3.1	Prominent error channels	14
2.3.2	General theory	15
2.3.3	Gottesman-Kitaev-Preskill (GKP) codes	18
2.4	Quantum communication	25
2.5	Quantum repeaters	30
3	Results	35
3.1	Memory-based quantum repeaters	35
3.1.1	Twin-field-inspired quantum repeater	35
3.1.2	Theoretical analysis of experiments in the Q.Link.X project	39
3.1.3	Analysis of a multi-segment twin-field-inspired quantum repeater	42
3.2	Error-correction-based all optical quantum repeaters	45
3.2.1	GKP syndrome measurements and linear optics	45
3.2.2	GKP qudit repeater	48
4	Conclusion and outlook	51
5	Bibliography	53
6	Publications	65

1 Introduction

In the last few years noisy small-scale quantum computers became reality [1, 2, 3] already resulting in an enormous public interest. Quantum computers can efficiently solve some specific problems which are believed to be intractable on classical computers. For example, the behavior of large molecules, described by quantum mechanics, can be simulated much more efficiently on a quantum computer which will probably allow chemists and pharmacists to design better materials and medicines. In Shor's groundbreaking work [4] he showed that quantum computers are also able to perform prime factorization efficiently. However, the fact that multiplying numbers is easy, but finding the prime factors of a large random number is very difficult, is the basis of many cryptographic protocols as e.g. RSA encryption. Thus, upcoming large-scale fault-tolerant quantum computers will break many of today's encryptions and we need to come up with encryption schemes unaffected by quantum computers.

One approach to solve this problem is the field of post-quantum cryptography [5] where one tries to find problems which are computationally hard even for a quantum computer. This solution is rather inexpensive as we only need to change software, but computational hardness assumptions against quantum computers may be problematic as the field of quantum algorithms is relatively new and therefore long-term secrecy may be even less provided than currently against classical computers.

A different approach consists of using the one-time pad (OTP) in combination with quantum key distribution (QKD) for obtaining the required secret shared key. Correctly implemented this scheme allows for information-theoretic security based on the fundamental laws of quantum mechanics instead of computational hardness assumptions. Quantum mechanics does not allow copying an arbitrary unknown quantum state and a measurement might change the state such that it is disturbed with high probability. Communicating parties may then use this disturbance in order to bound the information an eavesdropper might have gained about their key and distill a secret key, provided not too much information has been leaked. Due to its high speed the typical information carrier is light in fibers. However, absorption causes the signal to decay exponentially with the fiber length, resulting in an exponential decay of the secret-key rate for any point-to-point QKD protocol [6].

On the one hand, the inability to copy unknown quantum states allows for secrecy, but on the other hand, it also forbids simple information amplification stations similar to classical repeaters. Nowadays, several quantum repeater protocols have been proposed and they all have in common that the total distance is split into much shorter segments finally allowing low-noise transmission of quantum states at a fairly high rate. Although QKD is a very prominent application of quantum repeaters, there are many more like for example connecting distant quantum computers, blind quantum computing¹ [7, 8], synchronizing clocks [9, 10], improving telescopes [11] and there is ongoing research in finding further applications.

The first quantum repeater proposed by Briegel et al. [12] makes use of quantum memories and entanglement swapping in order to distribute entanglement over the total distance which can then be used for quantum transmission via the quantum teleportation protocol.

¹In blind quantum computing a client may only be able to perform some basic quantum tasks, wishes to perform universal quantum computing at some company, and wants to be sure that the company does not learn anything about the input data of the computation.

A different approach [13, 14, 15, 16, 17, 18], avoiding two-way classical communication, considers quantum error correcting codes where a recovery operation is applied at every station after at most a few km. Thus, only few errors accumulate and the recovery operation succeeds almost every time further reducing the error rates.

In this thesis we discuss both of these approaches for distributing entanglement over large distances. A new memory-based quantum repeater scheme based on single-photon interference is proposed in **paper I**. In comparison to schemes relying on two-photon interference this scheme has a square root scaling advantage as only one photon needs to arrive. In **paper II** we then calculate secret-key rates for potential repeaters with quantum memories based on two-photon interference with parameters reported by experimentalists in the project of “Q.Link.X” and for the different experimental platforms. The last paper dealing with memory-based quantum repeaters is **paper IV** which is an analysis for general memory-based repeaters where the focus lies on an exact calculation of the memory dephasing for different protocols filling also some gaps in the work of **paper I**. These results are then used for comparing three different general repeater schemes.

Relevant works in the context of quantum repeaters based on error correction are **paper III** and **paper V**. **Paper III** discusses possibilities to obtain the error syndrome of Gottesman-Kitaev-Preskill (GKP) codes with simple linear optics in addition to the GKP ancilla instead of using general Gaussian operations also involving in-line squeezing operations, which is experimentally considerably more demanding. Furthermore, we also discuss limitations of linear optics. These results are not only relevant in the context of a potential quantum repeater, but also for quantum computation with GKP codes. In **paper V** we consider a quantum repeater based on GKP qudits employing techniques from **paper III**.

The outline of this thesis is as follows. In chapter 2 we present the background of this work starting with basic quantum information theory, followed by a brief introduction to quantum optics since we will consider photons as the information carriers. Then we come to the topic of quantum error correction, where we first introduce the general theory, followed by a detailed introduction to GKP codes, which encode qubits/qudits within a harmonic oscillator. Subsequently, we come to the more applied topics of quantum communication and quantum repeaters where we explain how quantum mechanics can lead to information-theoretic secure encryption and how one can achieve high secret-key rates over large distances. In the next chapter 3 the results from my papers are summarized. Afterwards we conclude and finally we present the papers with a short section explaining my contributions to each paper.

2 Background

2.1 Basic quantum information theory

The basis unit of classical information used in all of our computers is the so-called bit taking the values 0 or 1, which can be easily realized by all kinds of physical processes involving two states as e.g. a voltage which is either above or below a specific threshold. In the context of quantum information (nice and comprehensive introductions are Refs. [19, 20]) we have to replace the bit by its quantum generalization called qubit. A (noiseless) qubit is a quantum two-level system and can be represented by a vector $|\psi\rangle$ in a two-dimensional complex Hilbert space spanned by $|0\rangle$ and $|1\rangle$ in the computational basis,¹

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1. \quad (2.1)$$

By allowing for these complex amplitudes instead of an element of \mathbb{Z}_2 much more information is required to represent a qubit in comparison to a bit. This effect becomes much more pronounced when considering multiple qubits. While n bits can represent 2^n different states, n qubits require 2^n complex numbers for their representation or 2^{n+1} real numbers, although there are only $2^{n+1} - 2$ independent ones, because of the normalization and irrelevance of a global phase. This exponentially increasing number of parameters makes it infeasible to simulate a quantum many-body system exactly on a classical computer and let Richard Feynman propose the idea of using quantum systems instead of a classical computer.

'Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.' (Feynman, 1981)

However, we cannot use multiple qubits as a dense information storage, because when performing measurements on the n qubits we can obtain at most n bits of information (Holevo bound) [21, 19] as only the absolute square of the amplitudes is relevant for the probability distribution of measurement outcomes which we also sample only once.

In order to perform computations we do not want to build hardware for a specific calculation, but instead we want to decompose every possible calculation into a small set of operations, which we should then be able to implement on our computer. For classical computers every function of bits can be represented by some combination of NAND gates. Such a universal set of gates also exists for arbitrary quantum computations. First, one shows that CNOT-gates (controlled NOT, whenever two indices are referenced the first one denotes the controlling input) together with arbitrary single-qubit gates are universal. As the set of single-qubit operations is uncountably large, there exists no finite set of quantum gates which can generate every element of $SU(2)$ exactly. However, we can get around this issue by allowing for sequences of universal gates which do not generate the desired unitary exactly, but only approximate it up to some error ϵ in the operator norm. An ϵ -approximation can be obtained by applying $O(\log^c(\frac{1}{\epsilon}))$ gates using the Solovay-Kitaev algorithm [22, 23], where c depends on the actual set of universal single-qubit gates. The

¹The generalization to a D -dimensional Hilbert space is called qudit of dimension D .

canonical set consists of the Hadamard gate H , the phase gate S , the $\pi/8$ gate T and the CNOT-gate. Their matrix representation in the computational basis is given by

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, \quad (2.2)$$

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \quad (2.3)$$

Other very important gates are the Pauli operators

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (2.4)$$

In the paragraph above we only discussed gate-based quantum computing, which is the standard approach for universal quantum computing. However, there are also other approaches for universal quantum computing like for example measurement-based quantum computing (MBQC), where one starts with some large entangled state and performs measurements in order to perform computational steps, or adiabatic quantum computing. The latter approach relies on the adiabatic theorem and typically problems are framed as finding the ground-state energy of some specific Hamiltonian. First one starts in the ground state of a very simple Hamiltonian and then this Hamiltonian is slowly changed to the desired one. For a slow enough transition the final state is close to the ground state of the desired Hamiltonian allowing for a good ground state energy estimation. For optical quantum computing MBQC is of particular interest as photons are easily lost. When generating a large entangled cluster state not all parts thereof have to exist at the same time, but the state can be build step by step and after a short time the photons are already measured. As a consequence a photon only needs to survive the short time between state generation and measurement while in an gate based approach it must survive the time it takes to apply all gates in the quantum computation.

A fundamental restriction of any quantum information processing is the no-cloning theorem [24, 25], stating that it is impossible to make a perfect copy of an arbitrary unknown state. While this seems quite remarkable from a classical point of view, it immediately follows from the linearity of quantum mechanics. The cloning of arbitrary unknown states corresponds to an operation

$$(\alpha |0\rangle + \beta |1\rangle) |0\rangle \rightarrow (\alpha |0\rangle + \beta |1\rangle) (\alpha |0\rangle + \beta |1\rangle), \quad (2.5)$$

where the left side of the equation is linear in α and β , while the right side is quadratic, violating the linearity of quantum mechanics. This does not contradict classical copying as there we are copying known orthogonal basis states, i.e. we are considering the special case where the coefficients α and β only take the values 0 or 1.

When considering noisy quantum systems or a system involving classical ignorance as for example in the case of an imperfect state preparation this additional (classical) uncertainty can be described nicely with density operators which are bounded linear operators acting on the Hilbert space instead of being an element of the Hilbert space in the noiseless case. Such a density operator $\hat{\rho}$ also needs to fulfill the properties

$$\hat{\rho} = \hat{\rho}^\dagger, \quad (2.6)$$

$$\hat{\rho} \geq 0, \quad (2.7)$$

$$\text{Tr}(\hat{\rho}) = 1. \quad (2.8)$$

Self-adjointness is needed in order to guarantee orthogonal eigenvectors with real eigenvalues while the other two conditions constrain the eigenvalues to be non-negative and summing to 1 which is necessary in order to interpret them as probabilities. If we have an ensemble of states $|\psi_i\rangle$ each occurring with probability p_i this corresponds to the density operator $\hat{\rho} = \sum_i p_i |\psi_i\rangle \langle \psi_i|$.²

Any time evolution (channel) should linearly map a valid density operator to a valid density operator leading to the notion of completely-positive trace-preserving (CPTP) maps. In order to obtain a valid density operator it is obvious that the map should be positive, i.e. mapping positive operators to positive operators, and preserve the trace. However, a channel even needs to be completely-positive meaning that the channel tensored by arbitrarily many identity operations is still positive. This restriction is needed in order to ensure that an operation is still physically meaningful when it only acts on parts of a larger system which involves entanglement.

As shown by Stinespring's dilation theorem [26] every CPTP map can be represented as

$$\mathcal{E}(\hat{\rho}) = \text{Tr}_{\text{env}} \left(\hat{U} (\hat{\rho} \otimes |e\rangle \langle e|) \hat{U}^\dagger \right), \quad (2.9)$$

where $|e\rangle$ is some state of the environment. We can then interpret the CPTP map as some unitary operation, generated by a Hamiltonian, acting on our system of interest and the environment. As we have no access to the environment's degrees of freedom, we have to ignore them, formally represented by tracing them out. When explicitly performing the trace with some orthonormal basis $\{|e_i\rangle\}$ of the environmental system, we obtain the Kraus representation of the CPTP map

$$\mathcal{E}(\hat{\rho}) = \sum_i \hat{K}_i \hat{\rho} \hat{K}_i^\dagger \quad (2.10)$$

with $\hat{K}_i = \langle e_i | \hat{U} | e \rangle$, fulfilling the completeness relation $\sum_i \hat{K}_i^\dagger \hat{K}_i = \mathbb{1}$. As one can choose different bases, the Kraus representation is not unique.

In many applications we only care about the probability distribution of a measurement and not the actual post-measurement state itself. In some cases, as for example the destructive measurement of a photon's properties by absorbing it at some detector, it does not even make sense to talk about its post-measurement state. For these cases it is quite convenient to use the POVM (positive-operator-valued-measure) formalism where one assigns positive operators $\{\hat{E}_m\}$, fulfilling $\sum_m \hat{E}_m = \mathbb{1}$, to measurement outcomes m . The probability of a measurement outcome m for a state $\hat{\rho}$ is then given by $p(m) = \text{Tr}(\hat{E}_m \hat{\rho})$. In contrast to projective measurements in standard quantum mechanics POVM elements $\hat{E}_m, \hat{E}_{m'}$ do not need to be orthogonal. However, this generalization is equivalent to projective measurements and unitary time evolution with additional auxiliary states.

When considering noisy states it is useful to have measures describing the closeness between two states. One relevant quantity is the trace norm

$$\|\hat{\rho}\|_1 = \text{Tr}(|\hat{\rho}|), \quad (2.11)$$

which does not have an operational interpretation by itself, but it can be used to define many measures with important operational interpretations. For example, it can be used to define the trace distance $\frac{1}{2} \|\hat{\rho}_1 - \hat{\rho}_2\|_1$ which is related to the distinguishability of the states $\hat{\rho}_1$ and $\hat{\rho}_2$. Suppose someone generates states $\hat{\rho}_1$ and $\hat{\rho}_2$ with equal probability and we are asked to distinguish them. The optimal probability to succeed in this task is then given by $\frac{1}{2} (1 + \frac{1}{2} \|\hat{\rho}_1 - \hat{\rho}_2\|_1)$ [20, pp. 235]. These scenarios are important when doing security

²When there is only one term in the sum, the state is called pure. Otherwise it is called mixed state.

2 Background

proofs for QKD schemes with finite key length, where one needs to calculate the probability of distinguishing the ideal QKD output state from the realized one. However, in this thesis we will always consider the asymptotic regime of infinitely long keys. Quite similar, it is also possible to define the diamond norm [27] which measures the distinguishability of two channels.

A different measure of similarity of two states is the fidelity³

$$F(\hat{\rho}_1, \hat{\rho}_2) = \text{Tr} \left(\sqrt{\hat{\rho}_1 \hat{\rho}_2 \sqrt{\hat{\rho}_1}} \right)^2, \quad (2.12)$$

which is symmetric and bounded by $0 \leq F(\hat{\rho}_1, \hat{\rho}_2) \leq 1$, where the fidelity is 1 for equal states and 0 for orthogonal density operators. Typically we are comparing a noisy state $\hat{\rho}_1$ to an ideal pure one $\hat{\rho}_2 = |\psi\rangle\langle\psi|$, simplifying the equation to

$$F(\hat{\rho}_1, |\psi\rangle\langle\psi|) = \langle\psi|\hat{\rho}_1|\psi\rangle. \quad (2.13)$$

In this scenario the fidelity has a nice intuitive meaning. Let us assume that $\hat{\rho}_1$ is a noisy version of $|\psi\rangle\langle\psi|$. We consider the task of state discrimination with POVMs $\{|\psi\rangle\langle\psi|, \mathbb{1} - |\psi\rangle\langle\psi|\}$ and the fidelity simply gives the probability of $\hat{\rho}_1$ passing the test. Thus, the fidelity can be directly measured in an experiment while the other distance measures have the disadvantage that one first needs to perform quantum state tomography in order to reconstruct the density operator and then calculate the distance. In the remaining thesis we will only consider the fidelity and no distance measures of quantum states.

As soon as one considers multiple quantum systems they might be entangled with each other which is a stronger notion than classical correlation known from probability theory. Let us briefly discuss the subtle differences between entanglement and classical correlation. For example, two perfectly correlated bits may look completely random when viewed individually, but both bits have the same value. When preparing such a state with two qubits we obtain

$$\begin{aligned} \hat{\rho}_1 &= \frac{1}{2} (|00\rangle\langle 00| + |11\rangle\langle 11|) \\ &= \frac{1}{8} \left[(|+\rangle + |-\rangle)^{\otimes 2} (\langle +| + \langle -|)^{\otimes 2} + (|+\rangle - |-\rangle)^{\otimes 2} (\langle +| - \langle -|)^{\otimes 2} \right], \end{aligned} \quad (2.14)$$

with $|\pm\rangle = 2^{-1/2} (|0\rangle \pm |1\rangle)$. Here we have completely correlated measurement outcomes when measuring the qubits in the Z -basis, but we obtain uncorrelated measurement outcomes in the X -basis. When instead preparing a maximally entangled state

$$\begin{aligned} \hat{\rho}_2 &= \frac{1}{2} (|00\rangle + |11\rangle) (\langle 00| + \langle 11|) \\ &= \frac{1}{2} (|++\rangle + |--\rangle) (\langle ++| + \langle --|), \end{aligned} \quad (2.15)$$

we obtain perfectly correlated measurement outcomes in both complementary bases which is impossible for only classically correlated states. Also notice that $\hat{\rho}_1$ is a mixed state with one bit of entropy meaning that the randomness of the measurement outcome in the Z -basis originates from our ignorance of the actual state. In contrast $\hat{\rho}_2$ is a pure state, i.e. we have no uncertainty about the prepared state and the randomness in the measurement outcome originates from the quantum mechanically probabilistic measurement process. For the special case of pure states an entangled state cannot be written as the tensor product

³The fidelity is not a distance measure in the mathematical sense. There are also two different conventions of the definition differing up to a square, but we will use the version that is more common in the literature.

of two one-qubit states $|\psi\rangle_{12} \neq |\phi_1\rangle_1 \otimes |\phi_2\rangle_2$. That means there is no way of describing one of the two qubits individually without neglecting some kind of information. For mixed states one says that they are separable iff (if and only if) there exists a decomposition of the form

$$\hat{\rho}_{12} = \sum_j p_j \hat{\rho}_{1,j} \otimes \hat{\rho}_{2,j}. \quad (2.16)$$

Detecting entanglement is straightforward for pure states as we can simply trace out one subsystem and calculate the entropy of the remaining reduced density operator. Whenever the entropy is non-zero the initial state was entangled. However, the detection becomes much more complicated for mixed states, especially when the subsystems have dimensions larger than 2.

Building upon the idea that entangled states may have correlations in complementary bases Einstein, Podolsky and Rosen came up with their famous discussion about the incompleteness of quantum mechanics [28]. There, they argued that either the quantum mechanical description of reality is incomplete or physical quantities of complementary observables do not have a simultaneous reality. By making use of the correlations in entangled states they showed that physical quantities of complementary observables can have a simultaneous reality in a weak sense⁴, letting them conclude that quantum mechanics is incomplete, which then led to the idea of local hidden-variable theories. In order to make the existence of local hidden-variable theories testable, Bell proposed an experiment where two qubits are separated by a large distance and for each qubit one locally decides which measurement should be performed [29]. The separation needs to be large enough such that no information can be exchanged between the measurement devices until the outcomes are announced. Bell proved an inequality of expectation values of the measurements which should hold provided that measurement outcomes can be described by a local hidden-variable theory. Furthermore, he showed that a specific entangled state violates this inequality when calculating the expectation value with the standard quantum mechanics formalism. As a simplification for an experimental demonstration Clauser, Horne, Shimony and Holt generalized Bell's inequality to the CHSH inequality [30]. In this proposed experiment Alice measures one of the two observables \mathbf{a}, \mathbf{a}' and Bob measures one of \mathbf{b}, \mathbf{b}' where each of the observables takes values in $\{1, -1\}$. We then define the observable

$$C = (\mathbf{a} + \mathbf{a}') \mathbf{b} + (\mathbf{a} - \mathbf{a}') \mathbf{b}'. \quad (2.17)$$

Clauser, Horne, Shimony and Holt showed that $\mathbb{E}(|C|) \leq 2$ holds under the assumption of local realism. In order to understand this result let us naively assign a probability distribution $\mathbb{P}(a, a', b, b')$. One immediately sees that $C = \pm 2$ as either $\mathbf{a} + \mathbf{a}'$ or $\mathbf{a} - \mathbf{a}'$ must give ± 2 and the other one gives 0. Thus, we obtain $-2 \leq \mathbb{E}(C) \leq 2$. However, by assigning a simultaneous probability distribution for \mathbf{a} and \mathbf{a}' we already made use of the locality assumption. As the expectation value is a linear function, we can simply decompose C in its four parts and take the expectation value of each term. Since all terms only involve a single observable for Alice and Bob, we can also obtain these expectation values in an experiment.

Let us now assume that Alice measures the observables X and Z , while Bob measures $\frac{X+Z}{\sqrt{2}}$ and $\frac{X-Z}{\sqrt{2}}$. Then it is a simple calculation that the expectation value of C is given by $\langle \Phi^+ | C | \Phi^+ \rangle = 2\sqrt{2}$, where $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is one of the four Bell states. This CHSH inequality was violated by multiple experiments, where early experiments had some loopholes regarding low detector efficiencies or the locality condition [31, 32, 33, 34],

⁴They were aware that their definition of reality might not be restrictive enough.

but these have been closed now simultaneously ruling out local hidden-variable theories [35, 36, 37]⁵. For the proposal and demonstrated experimental violation of this inequality Clauser, Aspect and Zeilinger were awarded with the Nobel price in 2022.

While being of particular interest in the foundations of quantum mechanics, entanglement also plays an important role in many quantum information applications. There we will be mostly interested in the four maximally entangled Bell states

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}} (|00\rangle \pm |11\rangle), \quad |\Psi^\pm\rangle = \frac{1}{\sqrt{2}} (|01\rangle \pm |10\rangle), \quad (2.18)$$

which form an orthonormal basis of the two-qubit Hilbert space. One application is quantum teleportation which can replace a qubit channel with local operations, a shared Bell state and two bits of classical communication. Suppose Alice has a qubit encoding some quantum information which she does not know and wants to transmit the information to Bob. Furthermore, she does not want to send the qubit directly to him as the connecting quantum channel might be very noisy, but we assume that they already share a noiseless Bell state $|\Phi^+\rangle$ (it works similarly for all other Bell states),

$$|\psi\rangle_A |\Phi^+\rangle_{A'B} = \frac{1}{2} \left(|\Phi^+\rangle_{AA'} |\psi\rangle_B + |\Psi^+\rangle_{AA'} X |\psi\rangle_B + |\Psi^-\rangle_{AA'} (-iY) |\psi\rangle_B + |\Phi^-\rangle_{AA'} Z |\psi\rangle_B \right). \quad (2.19)$$

The quantum teleportation protocol consists of the following three steps already suggested by Eq. 2.19:

- Alice measures qubits A and A' in the Bell basis.
- Alice tells Bob her measurement result.
- Bob applies a recovery operation from the set $\{\mathbb{1}, X, iY, Z\}$ depending on the measurement outcome.

After Alice performed her Bell measurement, only one term remains where Bob has the information up to some Pauli operator, which depends on the measurement outcome. When Bob learns the measurement outcome he can easily apply the inverse Pauli operator. Without this information all Pauli operators are equally likely such that Bob's qubit is in a maximally mixed state from his point of view. Therefore, faster-than-light communication is impossible with quantum teleportation as the transmission of the measurement outcome using classical communication is limited by the speed of light. The first experimental demonstration of this protocol was already shown in 1998 [38] and since then new experiments demonstrated the protocol [39, 40, 41, 42] even overcoming distances of up to 1400km between a satellite and a ground station [43].

A very similar protocol is entanglement swapping, effectively implementing the operation $|\Phi^+\rangle_{12} |\Phi^+\rangle_{34} \rightarrow |\Phi^+\rangle_{14}$ by performing a Bell measurement on qubits 2 and 3 and applying a Pauli correction conditional on the measurement outcome. Some people call this protocol also quantum teleportation as it can be understood as teleportation protocol, where the input state $|\psi\rangle$ is now an entangled state and one half of this entangled state is teleported to Bob. This protocol was also demonstrated experimentally a long time ago [44].

⁵However, local hidden-variable theories are not ruled out if one considers superdeterminism, where Alice's and Bob's measurement choices are assumed to be not independent from the hidden variables.

2.2 Quantum optics

2.2.1 Quantization of the electromagnetic field

As there is a vast amount of literature (e.g. [45, 46]) discussing the quantization of the electromagnetic field, we will only discuss it briefly for the sake of completeness. Let us consider the electromagnetic field in the vacuum without charges or currents given by

$$\vec{E} = -\nabla\phi - \frac{\partial}{\partial t}\vec{A}, \quad (2.20)$$

$$\vec{B} = \nabla \times \vec{A}, \quad (2.21)$$

where ϕ is the scalar potential and \vec{A} is the vector potential. Using the Coulomb gauge $\nabla \cdot \vec{A} = 0$ and Maxwell's equation $\nabla \cdot \vec{E} = 0$, one finds that both fields are completely characterized by the vector potential \vec{A} . By inserting the fields definition into $\nabla \times \vec{B} = \frac{1}{c^2} \frac{\partial \vec{E}}{\partial t}$, where c is the speed of light, and using a vector calculus identity, it follows that the vector potential \vec{A} fulfills the homogeneous wave equation

$$\Delta \vec{A} - \frac{1}{c^2} \frac{\partial^2}{\partial t^2} \vec{A} = 0. \quad (2.22)$$

By applying separation of variables and constructing the potential to be real-valued, one then obtains

$$\vec{A}(t, \vec{r}) = \sum_k c_k \vec{u}_k(\vec{r}) a_k(t) + c_k^* \vec{u}_k^*(\vec{r}) a_k^*(t), \quad (2.23)$$

where c_k are constants chosen in such a way that the set $\{\vec{u}_k\}$ forms an orthonormal basis and a_k are dimensionless. The summation involves all possible wavevectors \vec{k} and the polarization degrees of freedom.

In the quantization process we replace the complex-valued amplitudes a_k with the mode operators \hat{a}_k with commutation relations

$$[\hat{a}_k, \hat{a}_{k'}] = [\hat{a}_k^\dagger, \hat{a}_{k'}^\dagger] = 0, \quad [\hat{a}_k, \hat{a}_{k'}^\dagger] = \hat{1} \delta_{k,k'}. \quad (2.24)$$

Inserting the quantized vector potential into the definition of the \vec{E} - and \vec{B} -fields, using the free field energy density $\epsilon_0 |\vec{E}|^2 + \frac{1}{\mu_0} |\vec{B}|^2$ and integrating over the whole space leads after some calculations to the Hamiltonian

$$\hat{H} = \sum_k \omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2} \right), \quad (2.25)$$

where ω_k is the frequency of the corresponding light mode and we set $\hbar = 1$ ⁶. Thus every light mode of the free field corresponds to a simple harmonic oscillator. The operators \hat{a}_k and \hat{a}_k^\dagger , respectively, annihilate and create excitations of the field referred to as photons as one can see from the commutation relation in Eq. 2.24. The field's dimensionless position and momentum operators⁷ are given by

$$\hat{x} = \frac{1}{\sqrt{2}} \left(\hat{a} + \hat{a}^\dagger \right), \quad \hat{p} = \frac{1}{\sqrt{2}i} \left(\hat{a} - \hat{a}^\dagger \right), \quad (2.26)$$

fulfilling the canonical commutation relation $[\hat{x}, \hat{p}] = i\hat{1}$.

⁶In **paper I** the convention $\hbar = \frac{1}{2}$ was used instead.

⁷These operators do not represent a position or momentum in real space, but correspond to the in-phase and out-of-phase amplitude with respect to some phase reference.

2.2.2 Passive linear optics

Passive linear optical operations are the easiest experimentally implementable class of transformations on the mode operators \hat{a} . These operations transform the mode operators linearly, i.e. when considering N optical modes they are transformed as

$$\hat{a}_j \rightarrow \hat{a}'_j = \sum_{k=0}^N U_{jk} \hat{a}_k, \quad (2.27)$$

where U_{jk} are the elements of a unitary matrix. Due to the unitarity it is easy to check that the total number of photons is a conserved quantity (hence "passive"). This can also be observed by calculating the commutator between the total photon number operator and the generating Hamiltonian

$$\hat{H} = \sum_{j,k} A_{jk} \hat{a}_j^\dagger \hat{a}_k, \quad (2.28)$$

where A_{jk} are elements of a hermitian matrix. As shown by Reck et al. [47] it is possible to decompose any such passive linear optical operation into at most $\frac{N(N-1)}{2}$ beam splitters and N phase shifters.

Often it is also quite useful to describe the electromagnetic field by its quadrature operators where the linear optical transformation corresponds to an orthogonal, symplectic linear transformation O of the quadrature operators

$$(\hat{x}'_1, \dots, \hat{x}'_N, \hat{p}'_1, \dots, \hat{p}'_N)^T = O (\hat{x}_1, \dots, \hat{x}_N, \hat{p}_1, \dots, \hat{p}_N)^T, \quad (2.29)$$

$$O^T \begin{pmatrix} 0 & \mathbb{1}_N \\ \mathbb{1}_N & 0 \end{pmatrix} O = \begin{pmatrix} 0 & \mathbb{1}_N \\ \mathbb{1}_N & 0 \end{pmatrix}, \quad (2.30)$$

$$O^T = O^{-1}. \quad (2.31)$$

2.2.3 Squeezing operations

Another important class of operations are single-mode squeezing operations. They can be used to squeeze one quadrature while anti-squeezing the conjugated one. Their generating Hamiltonian has the form

$$H = i\kappa \left(\hat{a}^2 e^{-2i\phi} - (\hat{a}^\dagger)^2 e^{2i\phi} \right). \quad (2.32)$$

The angle ϕ characterizes which quadrature gets squeezed, for example, $\phi = 0$ squeezes the x -quadrature and anti-squeezes the p -quadrature

$$\hat{x} \rightarrow \hat{x} e^{-r} \quad \hat{p} \rightarrow \hat{p} e^r, \quad (2.33)$$

where $r = 2\kappa t$ is the effective squeezing parameter. In contrast to linear optical transformations squeezers do not conserve the photon number as the terms in the Hamiltonian either annihilate or generate two photons. In an experiment such a transformation can be obtained by spontaneous parametric-down conversion where a pump photon in a crystal with an optical nonlinearity (the polarization of the crystal is nonlinear in the electric field) is converted into two photons and the crystal is pumped by a strong classical field, such that its mode operator can be approximated by its classical amplitude. While it is easy to implement all linear optical operations in an experiment, implementing squeezers with high r is difficult and today the record lies at 15 dB of squeezing [48] (squeezing in dB $\hat{=} 10r$). When implementing a squeezing operation by pumping a non-linear crystal higher squeezing values are obtained by placing the crystal within a cavity. In the case

of a squeezing operation within a quantum circuit this has the disadvantage that one first needs to couple the unknown quantum state into the cavity and after the interaction out of the cavity resulting in additional losses. An experimentally more suitable approach was proposed in Ref. [49] where they generate a squeezed state and couple it with the unknown quantum state by linear optics followed by a homodyne measurement. In the limit of an infinitely squeezed state this protocol implements the desired squeezing operation, but as every physical squeezed state is only finitely squeezed this results in some intrinsic noise. Thus it is beneficial to avoid in-line squeezing operations whenever possible.

Furthermore, for any system consisting of N modes an arbitrary operation generated by a Hamiltonian quadratic in the mode operators can be decomposed into a linear optical operation acting on all N modes, followed by N single-mode squeezing operations followed by a final linear optical transformation acting on all N modes and possibly some displacement operators [50]. In this case the transformation matrix of the quadrature operators is simply given by a symplectic one in order to preserve the commutation relation of the transformed quadrature operators. These transformations are also known as Gaussian unitaries in the literature as they map Gaussian states onto Gaussian states⁸.

2.2.4 Coherent states

The most classical states in quantum optics are coherent states. Their defining relation is the eigenvalue problem of the mode operator \hat{a} ,

$$\hat{a} |\alpha\rangle = \alpha |\alpha\rangle \quad \alpha \in \mathbb{C}. \quad (2.34)$$

In the quantization we replaced the classical fields' amplitude α with the mode operator \hat{a} and now we defined a coherent state to be an eigenstate of this operator. By using the defining relation, we can already see the close relation between coherent states $|\alpha\rangle$ and classical light fields as the expectation value of any normal-ordered operator of the form $\sum_{n,m} c_{nm} (\hat{a}^\dagger)^n \hat{a}^m$ is the same as the result obtained by a purely classical calculation with a classical field with amplitude α . As a consequence the expectation value of the position and momentum operators behave exactly the same as expected from a classical harmonical oscillator.

Despite being very classical pure coherent states also show purely quantum mechanical features such as a non-zero position variance, because not all observables of interest are already in this normal-ordered form and bringing them into this form introduces some extra terms involving the commutator $[\hat{a}, \hat{a}^\dagger] = \hat{1}$. These states are also minimum uncertainty states satisfying $\text{Var}(\hat{x})\text{Var}(\hat{p}) = \frac{1}{4}$, achieving equality in the Heisenberg uncertainty relation.

In the Fock space representation coherent states are given by

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{k=0}^{\infty} \frac{\alpha^k}{\sqrt{k!}} |k\rangle, \quad (2.35)$$

and it is easy to see that they are always non-orthogonal as

$$\langle \alpha | \beta \rangle = \exp\left(-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2} + \alpha^* \beta\right), \quad |\langle \alpha | \beta \rangle|^2 = \exp(-|\alpha - \beta|^2). \quad (2.36)$$

⁸States are called Gaussian iff their representation in terms of the Wigner function [51] is a Gaussian function. As applying Gaussian operations on Gaussian states with a following homodyne measurement can be simulated efficiently on classical hardware [52] and they still show some genuine quantum effects like entanglement, the field of Gaussian operations has been well studied in the literature.

Formally all coherent states are related to the vacuum state by the displacement operator

$$\hat{D}(\alpha) = \exp\left(\alpha\hat{a}^\dagger - \alpha^*\hat{a}\right) = \exp\left(i\sqrt{2}\left(\hat{x}\operatorname{Im}\{\alpha\} - \hat{p}\operatorname{Re}\{\alpha\}\right)\right), \quad (2.37)$$

$$|\alpha\rangle = \hat{D}(\alpha)|0\rangle. \quad (2.38)$$

Eq. 2.38 can be obtained by using the relation $\hat{D}(\alpha)^\dagger\hat{a}\hat{D}(\alpha) = \hat{a} + \alpha$ and the property that coherent states are eigenstates of the annihilation operator.

2.2.5 Noise channels

One of the most important sources of noise in quantum optics and especially in the context of quantum communication is the loss of photons due to absorption and scattering. This process is formally described by the bosonic loss channel. The mode of interest \hat{a} is coupled to an environmental mode \hat{b} with a beam splitter of transmission η where in general the environment is assumed to be in the vacuum state and we then trace out the environmental mode \hat{b}' ,

$$\begin{pmatrix} \hat{a}' \\ \hat{b}' \end{pmatrix} = \begin{pmatrix} \sqrt{\eta} & \sqrt{1-\eta} \\ \sqrt{1-\eta} & -\sqrt{\eta} \end{pmatrix} \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix}. \quad (2.39)$$

To be more precise one should consider a thermal state

$$\hat{\rho}_{thermal} = \frac{1}{1 - \exp\left(-\frac{\hbar\omega}{k_B T}\right)} \sum_{j=0}^{\infty} \exp\left(-\frac{\hbar\omega}{k_B T}\right)^j |j\rangle\langle j| \quad (2.40)$$

instead of the vacuum state, but we are mostly interested in the regime of optical frequencies where $\hbar\omega \gg k_B T$ even holds for room temperature such that we can neglect the higher excitations. Finally we obtain the bosonic loss channel

$$\hat{\rho} \rightarrow \sum_{k=0}^{\infty} \hat{E}_k \hat{\rho} \hat{E}_k^\dagger \quad (2.41)$$

with $\hat{E}_k = \sum_{n=k}^{\infty} \sqrt{\binom{n}{k} \eta^{n-k} (1-\eta)^k} |n-k\rangle\langle n|$.

Another very important noise channel is the Gaussian displacement channel. In this channel displacements occur in the position and momentum quadrature according to a Gaussian probability distribution. We will assume that these shifts are independent and identically distributed (i.i.d.) with zero mean and a variance of σ^2 ,

$$\hat{\rho} \rightarrow \frac{1}{2\pi\sigma^2} \int_{\mathbb{R}^2} dx dp \exp\left(-\frac{(x^2 + p^2)}{2\sigma^2}\right) \hat{D}\left(\frac{x+ip}{\sqrt{2}}\right) \hat{\rho} \hat{D}^\dagger\left(\frac{x+ip}{\sqrt{2}}\right). \quad (2.42)$$

2.2.6 Detectors

In this thesis we make use of three different detectors of the electromagnetic field which we will discuss briefly without going into their inner workings as this is outside of the scope of this thesis.

On the one hand, there are on-off detectors which are able to discriminate the vacuum state from excited ones and their POVM is given by $\{|0\rangle\langle 0|, \hat{1} - |0\rangle\langle 0|\}$. On the other hand, there are photon-number-resolving detectors (PNRDs) which can resolve multiple photons corresponding to a POVM $\{|0\rangle\langle 0|, |1\rangle\langle 1|, |2\rangle\langle 2|, \dots\}$. PNRDs are experimentally much more demanding than on-off detectors and up to now only PNRDs which can resolve a

few photons have been demonstrated in an experiment [53, 54]. Some detectors work at higher temperatures, but have a lower efficiency. However, both kinds of detectors have the disadvantage that they can mostly only be operated at cryogenic temperatures.

A different detector which can be used at room temperature is a (balanced) homodyne measurement. In such a measurement the mode of interest is coupled with a strong classical light field with amplitude α by a 50:50 beam splitter (see Eq. 2.42 with $\eta = \frac{1}{2}$). Then the intensity of each output mode is measured by a common photo diode and one considers the difference of the two signals. The resulting observed quantity is then proportional to a quadrature operator of the input field, when considering a semi-classical approach where we replace the auxiliary strong coherent state by a classical light field. In a fully quantum-mechanical picture proportionality holds between the expectation values of the quadrature operator and the output signal, while for higher orders of the quadrature operator there are some correction terms which are neglectable for $|\alpha| \gg 1$. Different quadratures can be measured by adjusting the phase of α (see Fig. 2.1),

$$\begin{aligned} \hat{a}'^\dagger \hat{a}' - \hat{b}'^\dagger \hat{b}' &= \frac{1}{2} \left((\hat{a}^\dagger + \alpha^*) (\hat{a} + \alpha) - (\hat{a}^\dagger - \alpha^*) (\hat{a} - \alpha) \right) \\ &= \hat{a}^\dagger \alpha + \hat{a} \alpha^* . \end{aligned} \quad (2.43)$$

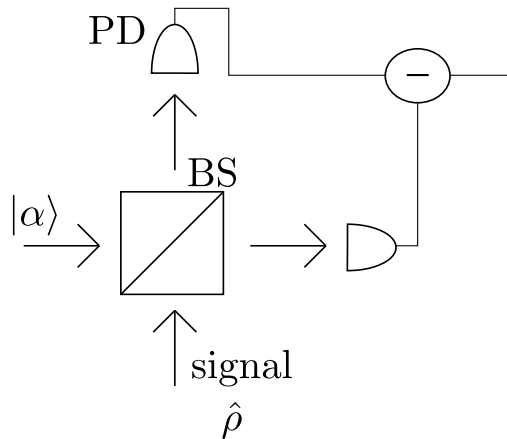


Figure 2.1: Schematic of a homodyne measurement: A coherent state is coupled by a 50:50 beam splitter (BS) with a light field whose quadrature is to be measured. The output modes are then measured by common photo diodes and their output current is subtracted. The resulting current is proportional to the expectation value of the quadrature measurement.

2.3 Quantum error correction

2.3.1 Prominent error channels

Before starting with error correction we shall briefly discuss two qubit error channels of particular interest.

On the one hand, we have the depolarizing channel

$$\hat{\rho} \rightarrow \mu \hat{\rho} + (1 - \mu) \frac{\mathbb{1}}{2} \quad (2.44)$$

$$= \frac{1 + 3\mu}{4} \hat{\rho} + \frac{1 - \mu}{4} (X \hat{\rho} X + Y \hat{\rho} Y + Z \hat{\rho} Z), \quad (2.45)$$

where the last equation was obtained by using the identity

$$\frac{\mathbb{1}}{2} = \frac{1}{4} (\hat{\rho} + X \hat{\rho} X + Y \hat{\rho} Y + Z \hat{\rho} Z). \quad (2.46)$$

When no error and X, Y, Z -error occur with equal probability, then the complete information of a single qubit is erased. Therefore, the depolarizing channel can be understood as a worst-case scenario where no error occurs with probability μ and otherwise the complete information is lost. There exist multiple conventions what is meant by an error probability in the depolarizing channel. Some call the probability to replace $\hat{\rho}$ by the maximally mixed state $\frac{\mathbb{1}}{2}$ error probability and others call the probability that a X, Y or Z -error happens error probability.

The other really important error channel is the dephasing (sometimes also called phase-flip) channel

$$\hat{\rho} \rightarrow (1 - p) \hat{\rho} + p Z \hat{\rho} Z. \quad (2.47)$$

Quite often the probability p of a phase-flip is parameterized as $p = \frac{1}{2} \left(1 - \exp\left(-\frac{t}{T_{\text{coh}}}\right) \right)$ due to physical reasons. Let us assume that $\hat{\rho}$ starts in the state $\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \left(\frac{\langle 0| + \langle 1|}{\sqrt{2}}\right)$ and we apply the dephasing channel. As a consequence the off-diagonal terms will be suppressed by a factor of $1 - 2p$ corresponding to an exponential decay with coherence time T_{coh} in the other parametrization, which can be observed in many experiments. After some time we obtain a classical mixture of $|0\rangle$ and $|1\rangle$ instead of the initial superposition.

Let us now derive this channel more rigorously from fundamental principles. We assume that our qubit interacts with the environment due to e.g. scattering with probability p' , where the probabilities of $|0\rangle_A$ and $|1\rangle_A$ are left invariant and the environmental state depends on the qubit state. One example for such a scenario would be that $|0\rangle_A$ and $|1\rangle_A$ denote the energy eigenstates of a system which scatters without energy exchange,

$$|0\rangle_A |0\rangle_E \rightarrow \sqrt{1 - p'} |0\rangle_A |0\rangle_E + \sqrt{p'} |0\rangle_A |1\rangle_E, \quad (2.48)$$

$$|1\rangle_A |0\rangle_E \rightarrow \sqrt{1 - p'} |1\rangle_A |0\rangle_E + \sqrt{p'} |1\rangle_A |2\rangle_E. \quad (2.49)$$

Since we have no access to the degrees of freedom of the environment, we have to calculate the partial trace. By using the canonical basis for the partial trace, we obtain the three Kraus operators which can be represented as matrices in the canonical basis

$$\hat{K}_0 = \sqrt{1 - p'} \mathbb{1}, \quad \hat{K}_1 = \sqrt{p'} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \hat{K}_2 = \sqrt{p'} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \quad (2.50)$$

Kraus operators are not unique as one can choose different bases for the partial trace and it is possible to find a more compact set of Kraus operators,

$$\hat{K}_0 = \sqrt{1 - \frac{p'}{2}} \mathbf{1}, \quad \hat{K}_1 = \sqrt{\frac{p'}{2}} Z. \quad (2.51)$$

We can also obtain the exponential form in the decaying off-diagonal terms by considering a continuous dephasing process with a dephasing rate Γ . For a small time segment Δt we have $p' = \Gamma \Delta t \ll 1$ and for each application of the dephasing channel the off-diagonal elements are damped by $1 - p'$. Thus we can split the overall time evolution of length t into n segments of length $\Delta t = \frac{t}{n}$ and we consider the limit of $n \rightarrow \infty$. The off-diagonal terms are then damped by

$$(1 - \Gamma \Delta t)^n = \left(1 - \frac{\Gamma t}{n}\right)^n \xrightarrow{n \rightarrow \infty} \exp(-\Gamma t). \quad (2.52)$$

There also exists a different approach for deriving the dephasing channel with another nice operational interpretation. Let us assume that we prepared an imperfect version of $\hat{\rho}$, where phase kicks occurred following a Gaussian distribution with variance σ^2

$$\frac{1}{\sqrt{2\pi\sigma^2}} \int_{-\infty}^{\infty} \exp\left(-\frac{\theta^2}{2\sigma^2}\right) \exp\left(\frac{i\theta}{2} Z\right) \hat{\rho} \exp\left(-\frac{i\theta}{2} Z\right) d\theta. \quad (2.53)$$

The diagonal terms are unharmed, but the off-diagonal ones are damped by a factor $\exp\left(-\frac{\sigma^2}{2}\right)$. Such an interpretation is very useful for experiments. For example, we may have an atom that shall store its quantum information for a long time. We assume constant electric and magnetic fields, but this is an idealization and not what is happening in the lab. There, the magnetic field is fluctuating, shifting the energy difference between both energy levels resulting to some unforeseen phases due to the time evolution, which we have to average over.

2.3.2 General theory

Although quantum systems are very fragile and susceptible to noise a very similar problem arose in the last century when trying to sent classical information through a noisy environment. There, the solution was to use encodings of the information with some amount of redundancy. The simplest encoding with redundancy is the 3-bit repetition code

$$0_L = 000, \quad 1_L = 111, \quad (2.54)$$

where one simply copies the information multiple times and from time to time one applies a recovery operation, where one applies majority voting, i.e. if there is a single 1 one flips it to 0 and vice versa. This scheme succeeds whenever at most one error happened. Provided that bit-flip errors occur independently and with a low enough probability p , this code reduces the error rate to $3p^2(1 - p) + p^3$, but it also introduces an hardware overhead.

Several issues arise when trying to generalize such an error correction scheme to the quantum realm:

- The quantum information cannot be simply duplicated due to the no-cloning theorem.
- Measuring all qubits in order to learn the error destroys the quantum information.
- We have to correct uncountably many different errors.

2 Background

Due to the no-cloning theorem it is impossible to copy the input qubit, but it is possible to consider a similar scheme. Here, we consider the code

$$|0_L\rangle = |000\rangle, \quad |1_L\rangle = |111\rangle, \quad (2.55)$$

thus encoding a superposition results in an entangled state and not multiple copies of the superposition. In order to correct bit flip errors we cannot measure all qubits in the Z -basis as this would also reveal encoded information. For example, already a single measurement of Z_1 corresponds to a measurement of the logical Pauli operator \bar{Z} in the error correcting code and thus superpositions in the logical qubit are already destroyed. Thus, we have to gain less information while still getting enough information in order to learn the occurring error. This can be done by measuring Z_1Z_2 and Z_2Z_3 with the projectors

$$P_1 = |000\rangle\langle 000| + |111\rangle\langle 111| \quad \text{apply } \mathbb{1} \text{ as recovery,} \quad (2.56)$$

$$P_2 = |100\rangle\langle 100| + |011\rangle\langle 011| \quad \text{apply } X_1 \text{ as recovery,} \quad (2.57)$$

$$P_3 = |010\rangle\langle 010| + |101\rangle\langle 101| \quad \text{apply } X_2 \text{ as recovery,} \quad (2.58)$$

$$P_4 = |001\rangle\langle 001| + |110\rangle\langle 110| \quad \text{apply } X_3 \text{ as recovery.} \quad (2.59)$$

Here, we only obtain 2 bits of information, which is enough to learn the error without leaking the encoded information, such that we can apply an appropriate recovery operation. In classical error correction we measure Z_1 , Z_2 and Z_3 , which are then multiplied to Z_1Z_2 and Z_2Z_3 . In quantum error correction we skip the first step and only measure the information that is really necessary for the recovery.

As an example, let us consider the case where on each qubit a bit-flip occurs independently with probability p and no error with probability $1 - p$. Furthermore, we consider the general encoded state $\alpha|000\rangle + \beta|111\rangle$. With probability $p(1 - p)^2$ we have the pre-measurement state $\alpha|100\rangle + \beta|011\rangle$. The measurement projects onto P_2 leaving the actual state invariant. Then we know that we have to apply X_1 as a recovery in order to go back to the code space.

Up to now we have not discussed the important issue of continuous errors. Especially in the context of performing single-qubit rotations it is easy to imagine that in an experiment the interaction times will never be perfect, resulting in small under- or overrotations. Let us assume we want to perform some rotation on the first qubit and in addition to the desired rotation we also got the error $a\mathbb{1} + bX_1$ due to an overrotation. When measuring Z_1Z_2 and Z_2Z_3 on the state $(a\mathbb{1} + bX_1)(\alpha|000\rangle + \beta|111\rangle)$ we project onto P_1 with probability $|a|^2$ resulting in the state $\alpha|000\rangle + \beta|111\rangle$ and with probability $|b|^2$ we project onto P_2 resulting in the state $\alpha|100\rangle + \beta|011\rangle$. After the recovery operation we obtain the state $\alpha|000\rangle + \beta|111\rangle$ in both cases. Here we can see that the projection in the measurement process of Z_1Z_2 and Z_2Z_3 reduced the continuous error to a discrete one that we have to correct.

In general, a quantum error-correcting code is a subspace of a Hilbert space where the canonical correction process consists of two steps. First, we perform a syndrome measurement, i.e. a measurement which allows us to gain information about the occurring error without leaking any encoded information. Conditional on this measurement outcome we then apply an operation in order to recover a state lying in the code space. In general, arbitrary qubit rotations can occur as an error leading to an uncountable set of errors that we have to correct. However, measuring the syndrome discretizes the errors such that we only have to correct a finite set. A general theory of quantum error correcting codes is described in Ref. [19] and the Knill-Laflamme conditions [55] specify whether a code can correct a given set of errors.

Theorem 1 (Knill-Laflamme conditions). *A code C can correct errors from a set \mathcal{A} iff for all basis states $|i_L\rangle, |j_L\rangle$ ($i \neq j$) and $A_a, A_b \in \mathcal{A}$ the conditions*

$$\langle i_L | A_a^\dagger A_b | i_L \rangle = \langle j_L | A_a^\dagger A_b | j_L \rangle \quad (2.60)$$

and

$$\langle i_L | A_a^\dagger A_b | j_L \rangle = 0 \quad (2.61)$$

are satisfied.

Both conditions have an intuitive interpretation. The first condition means that correctable errors must not introduce deformations depending on the encoded information, which would change the coefficients in a superposition otherwise, and the second condition means that logical basis states can still be discriminated for correctable errors.

Suppose, we consider a finite set of correctable errors $\{A_j\}_{j=1}^n$, then it is easy to show that every linear combination thereof $A'_a = \sum_{k=1}^n a_k A_k$, where a_k is a scalar, can also be corrected,

$$\langle i_L | A_a'^\dagger A_b' | j_L \rangle = \langle i_L | \sum_{k,l=1}^n a_k^* A_k^\dagger b_l A_l | j_L \rangle = \sum_{k,l=1}^n a_k^* b_l \langle i_L | A_k^\dagger A_l | j_L \rangle = 0. \quad (2.62)$$

The other condition can be proven similarly and thus every linear combination of correctable errors is also correctable, such that we only have to consider a basis of correctable errors. Every possible single-qubit Kraus operator can be described by a 2×2 matrix. A really convenient basis for these single-qubit errors is given by $\{\mathbb{1}, X, Y, Z\}$ which even forms an orthogonal basis with respect to the Frobenius inner product $\langle A, B \rangle = \text{Tr}(A^\dagger B)$. The elements of this basis are part of the n -qubit Pauli group

$$\begin{aligned} P_n &= \{i^\alpha B_1 \otimes B_2 \otimes \cdots \otimes B_n | \alpha \in \{0, 1, 2, 3\}, \\ & B_j \in \{\mathbb{1}, X, Y, Z\}, j \in \{1, \dots, n\}\}, \end{aligned} \quad (2.63)$$

which also has the additional property that two group elements either commute or anti-commute with each other. We can then consider multi-qubit errors by choosing the elements⁹ of P_n as the basis for expanding the error Kraus operators.

Almost all qubit quantum error correcting codes belong to the class of stabilizer codes, which can be described quite nicely in the stabilizer formalism making heavy use of the Pauli group. An n -qubit stabilizer code is represented by a stabilizer group which is an abelian subgroup (not including $-\mathbb{1}$)¹⁰ of the n -qubit Pauli group P_n . The code space is then given by the common $+1$ eigenspace of all elements in the stabilizer group. This group can be generated by $n - k$ independent stabilizer generators¹¹ and corresponds to a code which encodes k logical qubits within n physical ones. Stabilizer codes have two really nice features. First, we can describe a code compactly with $n - k$ stabilizers although the underlying Hilbert space dimension increases exponentially with n . Tracking the stabilizers even allows for an efficient simulation¹² of Clifford-circuits [56] consisting of gates from the Clifford group $C_n = \{V \in U(2^n) | V P_n V^\dagger = P_n\}$, i.e. it is the normalizer of the Pauli group and can be generated by the gates H, S and CNOT. Similarly, one can define the normalizer $\mathcal{N}(S) := \{P \in P_n | P S P^\dagger = S\}$ of a stabilizer group S in P_n . It is possible

⁹with trivial phase

¹⁰Otherwise, the codespace is empty.

¹¹Often only called stabilizers for brevity. Rigorously, all elements in the stabilizer group are stabilizers.

¹²As a consequence, quite often one considers Pauli noise consisting of probabilistic Pauli-operator errors, because such an error correction process can be simulated efficiently.

to choose a basis for the logical qubits in such a way that logical Pauli-operators then correspond to the cosets $\mathcal{N}(S)/S$ and the lowest weight of an element in $\mathcal{N}(S)$ not belonging to S is the code distance d , where the weight of an operator is the number of qubits with non-trivial action. Such a code can then correct $d - 1$ errors with known positions and only $\lfloor \frac{d-1}{2} \rfloor$ errors when their positions are unknown. Quite often the most important properties of a code are written down as the triple $\llbracket n, k, d \rrbracket$, where n is the number of used physical qubits for encoding k logical ones with a code distance of d . Another benefit of the stabilizer formalism is that the stabilizer generators already explicitly define syndrome measurements. In our example with the 3-qubit bit flip code two stabilizer generators are given by $Z_1 Z_2$ and $Z_2 Z_3$ which are exactly the syndrome measurements discussed above.

When ignoring global phases every n -qubit Pauli operator can be represented by an \mathbb{Z}_2^{2n} string via the symplectic representation

$$X_1^{e_1} Z_1^{f_1} \otimes \cdots \otimes X_n^{e_n} Z_n^{f_n} \leftrightarrow (e_1, \dots, e_n, f_1, \dots, f_n) = (e|f). \quad (2.64)$$

Two Pauli operators commute when the symplectic form $\omega((e|f), (e'|f')) = ef' - f'e'$ is a multiple of 2.¹³

A very important subclass of stabilizer codes are Calderbank-Shor-Steane (CSS) codes where it is possible to find a set of stabilizer generators such that each generator only consists of $\mathbb{1}$ and X or $\mathbb{1}$ and Z . Therefore, one can correct X - and Z -errors independently and the overall code can be decomposed into two classical codes each correcting either the X - or Z -errors. Furthermore, the logical CNOT gate can be implemented transversally between two CSS codes, i.e. by applying physical CNOT gates in a bitwise fashion.

2.3.3 Gottesman-Kitaev-Preskill (GKP) codes

So far we considered quantum error-correcting codes for qubits which can be applied in principle to all kinds of quantum systems since only two states are used. However, this might be very hardware-inefficient as only a two dimensional subspace of the overall Hilbert space is used for the physical qubit and no other degrees of freedom are utilized for encoding the logical information and an error syndrome. The smallest qubit code being able to correct arbitrary single-qubit errors is the 5-qubit code. Thus, one would naively employ five physical systems in order to obtain one logical qubit. Especially in the case of a harmonic oscillator the Hilbert space is infinite-dimensional such that it would be wasteful to only use a two-dimensional subspace instead of considering additional parts of the space for redundancy.

Thus, it makes sense to consider quantum error-correcting codes which are already defined within the Hilbert space of a harmonic oscillator, which are known as bosonic codes. As these codes are not built out of abstract qubits, they can also be designed in such a way that they are able to correct more physically realistic error models as e.g. photon loss or small diffusive displacements.

The most important bosonic codes are cat [57] and binomial codes [58] which are designed to correct photon loss and GKP codes [59] which are designed to correct displacement errors. These GKP codes were already proposed in 2001 and are therefore also one of the oldest bosonic codes. However, back then an implementation thereof was considered experimentally impractical or even “beyond impossible” [60] and only in the last years first experiments could be demonstrated [61, 62, 63, 64, 65]. Quite impressively an experiment with active GKP error correction was demonstrated in superconducting circuits very

¹³In the case of general qudits of dimension D the generalized Pauli operators commute when the symplectic form is a multiple of D . There is no unique way to generalize the Pauli operators from qubits to higher dimensional system and we consider the choice of $X = \sum_{j=0}^{D-1} |j+1 \bmod D\rangle \langle j|$ and $Z = \sum_{j=0}^{D-1} \exp(-i\frac{2\pi}{D}j) |j\rangle \langle j|$.

recently overcoming break-even [65], i.e. the coherence time of the information encoded within the GKP code was higher than the best passive encoding employing the same hardware. Especially in the last few years when these codes came in reach they also gained enormous interest from the theoretical side and it was shown that GKP codes can even beat cat and binomial codes in their own game of photon loss [66].

The most famous ideal GKP codes consist of a Dirac comb as the position-wavefunction, i.e. the wave function consists of delta peaks with some period,

$$|0\rangle = \sum_{n \in \mathbb{Z}} |\hat{x} = 2n\beta\rangle, \quad |1\rangle = \sum_{n \in \mathbb{Z}} |\hat{x} = (2n+1)\beta\rangle, \quad (2.65)$$

$$|+\rangle = \sum_{n \in \mathbb{Z}} \left| \hat{p} = 2n\frac{\pi}{\beta} \right\rangle, \quad |-\rangle = \sum_{n \in \mathbb{Z}} \left| \hat{p} = (2n+1)\frac{\pi}{\beta} \right\rangle. \quad (2.66)$$

The corresponding X and Z -operations can be represented by

$$X = \exp(-i\beta\hat{p}), \quad Z = \exp\left(i\frac{\pi}{\beta}\hat{x}\right). \quad (2.67)$$

Therefore, all position displacements with a magnitude smaller than $\frac{\beta}{2}$ and all momentum displacements with a magnitude smaller than $\frac{\pi}{2\beta}$ can be corrected by measuring the error syndrome and shifting the state back to the nearest codeword. Usually noise in the position and momentum quadratures is equally strong and therefore one chooses $\beta = \sqrt{\pi}$ making the code symmetric.

To make the error correction scheme more illustrative we will briefly discuss a standard approach for error correction for the symmetric scheme also shown in Fig. 2.2. For simplicity we assume that a position displacement of strength u occurs at a $|0\rangle$ state and we want to correct it. Analogously we could also do the same for superpositions in the codespace and for superpositions of errors, but the calculation would be less clear. Hence we stick with this simple model.

In order to obtain the syndrome information we consider an ancilla state $\sum_{j \in \mathbb{Z}} |\hat{x} = \sqrt{\pi}j\rangle_2$ and couple it with the other state by employing a CSUM gate $e^{-\hat{x}_1\hat{p}_2}$. The idea of this coupling is that the position shift is copied from mode 1 onto mode 2 which is then measured, so that we can learn the shift. In the end we measure the position in mode 2 and thus we learn $u \bmod \sqrt{\pi}$. We assume that it is more likely for u to be small and therefore we estimate u to be in the interval $[-\frac{\sqrt{\pi}}{2}, \frac{\sqrt{\pi}}{2})$ and apply a corresponding correction shift $-u_{\text{estimated}}$ to the position of mode 1. For $|u| < \frac{\sqrt{\pi}}{2}$ the correction always succeeds, but for larger shifts it leads to logical errors¹⁴.

$$\sum_{j,k \in \mathbb{Z}} |\hat{x} = 2j\sqrt{\pi} + u\rangle_1 |\hat{x} = k\sqrt{\pi}\rangle_2 \quad (2.68)$$

$$\xrightarrow{CSUM} \sum_{j,k \in \mathbb{Z}} |\hat{x} = 2j\sqrt{\pi} + u\rangle_1 |\hat{x} = (2j+k)\sqrt{\pi} + u\rangle_2 \quad (2.69)$$

$$= \sum_{j,k' \in \mathbb{Z}} |\hat{x} = 2j\sqrt{\pi} + u\rangle_1 |\hat{x} = k'\sqrt{\pi} + u\rangle_2 \quad (2.70)$$

GKP codes can also be described as a kind of stabilizer code where the underlying group

¹⁴We are neglecting the cases where error and correction add to a large shift of for example $2\sqrt{\pi}$, because these events only occur with a very low probability.

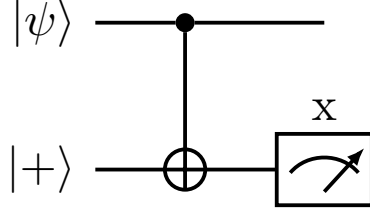


Figure 2.2: The CNOT_{12} realized by $\exp(-i\hat{x}_1\hat{p}_2)$ acts as the identity when both qubits are in the GKP code space. However, it also propagates position shifts from mode 1 to mode 2 and vice versa for momentum shifts. Thus, the position measurement of mode 2 gives us the required syndrome information in the form of $x \bmod \sqrt{\pi}$.

is the Weyl-Heisenberg group instead of the Pauli group. Elements of the Weyl-Heisenberg group acting on N modes take the form of

$$D(\theta, \vec{\alpha}, \vec{\beta}) = e^{i\theta} \exp \left(i\sqrt{2\pi} \sum_{j=1}^N (\alpha_j \hat{x}_j + \beta_j \hat{p}_j) \right), \quad (2.71)$$

$$D(\theta_1, \vec{\alpha}_1, \vec{\beta}_1) D(\theta_2, \vec{\alpha}_2, \vec{\beta}_2) = e^{-i2\pi\omega((\vec{\alpha}_1|\vec{\beta}_1), (\vec{\alpha}_2|\vec{\beta}_2))} D(\theta_2, \vec{\alpha}_2, \vec{\beta}_2) D(\theta_1, \vec{\alpha}_1, \vec{\beta}_1),$$

where ω is again the symplectic form introduced in the symplectic representation of the Pauli group. In fact, when ignoring global phases we already have a symplectic representation in \mathbb{R}^{2N} with the vector $(\vec{\alpha}|\vec{\beta})$. The similarity of the Weyl-Heisenberg and Pauli groups is no coincidence as they can also be understood as unitary representations of the continuous or respectively finite Heisenberg group [67]. The stabilizer generators of the described GKP code are then given by

$$e^{i2\sqrt{\pi}\hat{p}} \text{ and } e^{i2\sqrt{\pi}\hat{x}}. \quad (2.72)$$

Notice that products of stabilizers are also stabilizers and the set of possible stabilizers forms a lattice in the symplectic representation. For this reason we will refer to this code as square GKP as it forms a square lattice \mathcal{L} in the symplectic representation.

Additionally we can consider the dual (in the symplectic form) lattice

$$\mathcal{L}^\perp = \{v \in \mathbb{R}^{2N} | \omega(v, l) \in \mathbb{Z} \quad \forall l \in \mathcal{L}\}$$

corresponding to displacements commuting with all stabilizers. Logical Pauli operators are then represented by the coset $\mathcal{L}^\perp/\mathcal{L}$. Different GKP codes then correspond to different lattices where the symplectic form between any two basis elements of the lattice has to be an integer such that the stabilizers commute with each other.

Unfortunately, the exact codewords are unphysical as they are not normalizable due to the translation-invariance and additionally they are superpositions of infinitely squeezed states which would require an infinite amount of energy. A very intuitive approach [59] consists of replacing the delta peaks with sharp Gaussian peaks and introducing an overall Gaussian envelope resulting in the approximate states

$$|\tilde{0}\rangle \propto \sum_{s \in \mathbb{Z}} \int_{\mathbb{R}} e^{-\frac{1}{2}\kappa^2(2s\sqrt{\pi})^2} e^{-\frac{1}{2\Delta^2}(q-2s\sqrt{\pi})^2} |\hat{x} = q\rangle dq, \quad (2.73)$$

$$|\tilde{1}\rangle \propto \sum_{s \in \mathbb{Z}} \int_{\mathbb{R}} e^{-\frac{1}{2}\kappa^2((2s+1)\sqrt{\pi})^2} e^{-\frac{1}{2\Delta^2}(q-(2s+1)\sqrt{\pi})^2} |\hat{x} = q\rangle dq. \quad (2.74)$$

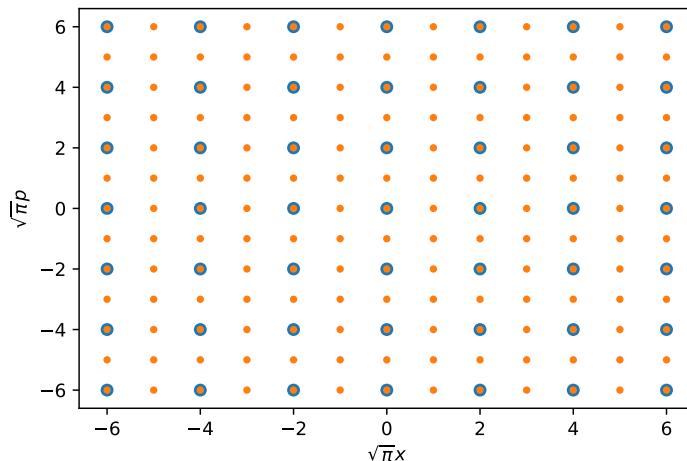


Figure 2.3: Snippet of square GKP's stabilizers in the symplectic representation forming a square lattice. The blue dots show the lattice points \mathcal{L} and the orange ones show the symplectically dual lattice \mathcal{L}^\perp .

Alternatively, one can consider

$$|\tilde{\psi}\rangle \propto \int_{\mathbb{R}^2} \frac{1}{2\pi\gamma\delta} e^{-\frac{1}{2}\left(\frac{u^2}{\gamma^2} + \frac{v^2}{\delta^2}\right)} e^{i\left(-\frac{u\hat{p}+v\hat{x}}{\sqrt{2}}\right)} |\psi\rangle dudv, \quad (2.75)$$

where $|\tilde{\psi}\rangle$ is the approximate version of the ideal square GKP state $|\psi\rangle$ (see Fig. 2.4). Multiple different approximate codewords have been proposed [59, 68] and they have been shown to be (almost) equivalent¹⁵ when assuming equal error rates in both quadratures, i.e. $\gamma = \delta$ [69]. The last equivalent approximation consists of applying the operator $\exp(-\xi(\hat{n} + \frac{1}{2}))$ on the ideal codewords, where \hat{n} is the number operator [68]. This also allows for a simple calculation of stabilizers for finitely-squeezed GKP states [70], which we will demonstrate for the stabilizer $e^{i2\sqrt{\pi}\hat{p}}$,

$$|\tilde{\psi}\rangle = e^{-\xi(\hat{n} + \frac{1}{2})} |\psi\rangle = e^{-\xi(\hat{n} + \frac{1}{2})} e^{i2\sqrt{\pi}\hat{p}} |\psi\rangle \quad (2.76)$$

$$= e^{-\xi(\hat{n} + \frac{1}{2})} e^{i2\sqrt{\pi}\hat{p}} e^{+\xi(\hat{n} + \frac{1}{2})} e^{-\xi(\hat{n} + \frac{1}{2})} |\psi\rangle \quad (2.77)$$

$$= e^{i2\sqrt{\pi}(\cosh^2(\xi)\hat{p} - i \sinh^2(\xi)\hat{q})} |\tilde{\psi}\rangle. \quad (2.78)$$

Quite often in the literature the coherent Gaussian displacements are replaced by incoherent ones as a simplification, resulting in a Gaussian displacement channel. This approximation has the advantage that one can combine the Gaussian noise originating from the environment with the Gaussian noise from the approximate states to a single Gaussian channel, which is simply described by its covariance matrix, followed by ideal GKP error correction simplifying calculations enormously. The approach of considering incoherent instead of coherent noise is also well-established in the context of qubit quantum error correction. There, in principle it is possible to actually perform this conversion by a process called twirling [71, 72], where one applies a random operation from a set before the error channel followed by the inverse operation. Similar schemes have been proposed

¹⁵The state given in Eq. 2.74 is not symmetric in position and momentum and therefore the wave function has to be squeezed by a factor of $\sqrt{1 + \kappa^2\sigma^2}$ in order to make it equivalent with the parameterization given in Eq. 2.75. Thus, in the limit of good approximation this squeezing is neglectable.

2 Background

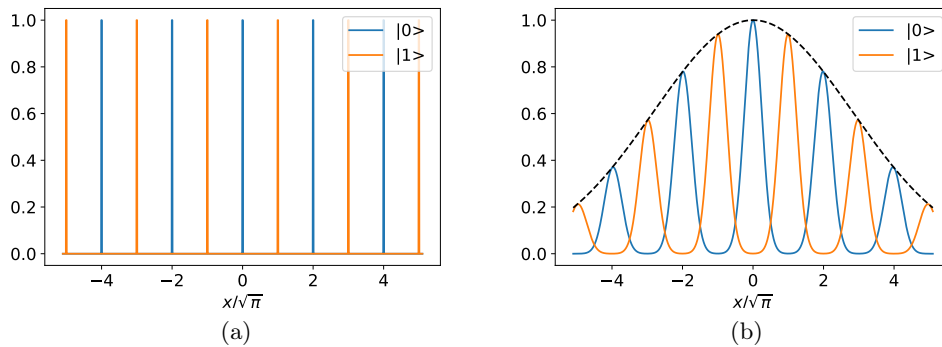


Figure 2.4: GKP wavefunction in the position representation with (a) ideal GKP qubits, (b) finitely squeezed approximate (unnormalized) GKP states with $\Delta = \kappa = 0.25$.

in the GKP context [73, 74], but in this infinite-dimensional Hilbert space the off-diagonal terms cannot be brought to zero exactly but only in a limit.

In order to perform error correction we also need to perform measurements in order to obtain the syndrome information. For example, measuring the syndrome of the stabilizer $e^{i\frac{2\pi}{\sqrt{\pi}}\hat{x}}$ is equivalent to measuring $\hat{x} \bmod \sqrt{\pi}$. Such a measurement can be performed by a circuit shown in Fig. 2.2. An experimentally simpler variation thereof is discussed in **paper III**.

Often GKP codes are considered in combination with a concatenated high-level qubit stabilizer code and the error correction of both codes is done independently [75, 76, 77]. However, the logical error rate can be boosted by using the analog GKP syndrome information also in the decoding process of the high-level code. Suppose that a shift error of $\frac{\sqrt{\pi}}{2} - \epsilon$ with $0 < \epsilon \ll 1$ occurs and this has the same syndrome as a shift of $-\left(\frac{\sqrt{\pi}}{2} + \epsilon\right)$. A confusion of these two shifts would result in a logical Pauli error after the error correction and both shift errors have almost the same probability according to the Gaussian distribution. Hence, we have low confidence in the correctness of the recovery operation for this specific error syndrome. However, in the case of a shift of ϵ it is rather easy to decide correctly as alternative shifts with the same syndrome are $\epsilon \pm \sqrt{\pi}$ and according to the Gaussian probability distribution these shifts are very rare such that we have high confidence in our recovery operation. This measure of confidence can then be used by the recovery of the high-level code [78, 73]. The performance of several codes with additional analog information have been studied and large improvements have been found [76, 75, 79, 80].

Another advantage of GKP codes is that Clifford operations can be realized on the logical level of the GKP code by physical Gaussian operations (mapping Gaussian states onto Gaussian states) as they transform quadrature operators linearly while preserving the canonical commutation relations. For example, in the square GKP code Pauli operations are realized by displacements, the Hadamard gate is realized by the rotation $e^{i\frac{\pi}{2}\hat{n}}$ and a CNOT_{12} is given by the conditional displacement $e^{-i\hat{q}_1\hat{p}_2}$.

The five experimental demonstrations of the GKP code make use of different physical platforms, as on the one hand, Refs. [61, 63] use the harmonic motion of a trapped $^{40}\text{Ca}^+$ as the oscillator mode which is controlled by a qubit in the internal state of the ion ($|S_{1/2}, m_j = 1/2\rangle$ and $|D_{5/2}, m_j = 3/2\rangle$) due to state-dependent optical forces. On the other hand, Refs. [62, 64, 65] use a microwave cavity controlled by a transmon, but the schemes [61, 62, 65] have in common that they apply controlled displacement operations

or more generally an entangling operation, consisting of multiple controlled displacements and single-qubit rotations, between the oscillator and the transmon qubit before measuring the qubit. Conditional on the measurement outcome an operation may be applied on the mode. In the trapped-ion experiment [61] they first generate a squeezed state and prepare the qubit in a $|+\rangle$ state, apply a controlled displacement operation and measure the qubit on the X -basis. This generates a superposition of squeezed states and by repeating these steps additional peaks of the GKP state can be added step by step. In the other experiment [62] they make use of the fact that the controlled displacement can equivalently also be seen as a qubit rotation conditional on the oscillators state. By performing suitable measurements on the qubit after each controlled displacement operation they are able to reconstruct the expectation value of the stabilizer generator. By measuring these stabilizers again and again they project the oscillator state onto the GKP codespace. However, every qubit measurement can only give a single bit of information such that many measurements are needed in order to obtain an accurate estimation of a stabilizer syndrome consisting of a phase. Although the experiments [61, 63] use the same encoding, their state preparation is completely different since there are no measurements involved in experiment [63], but instead they designed a dissipative process where they apply some spin-dependent displacement operations followed by resetting the spin via optical pumping. This process is designed in such a way that its steady state contains the GKP codespace and thus codewords are prepared by applying multiple iterations of this process. By using this re-pumping instead of the spin-state readout one has the advantage that less photons scatter with the ion (~ 2 vs ~ 1000 photons) and therefore less noise originates from the recoil. Ref. [64] also generates GKP states without performing measurements. They consider an interaction between a microwave cavity and a transmon qubit in the dispersive regime with an interaction Hamiltonian $H = \chi \hat{a}^\dagger \hat{a} Z / 2$, where χ is the rate of non-linear interaction. Typically, universal control of the harmonic oscillator is impossible in the regime where the dispersive non-linearity is not much larger than the decoherence rates. However, by applying large displacements and suitable chosen echo sequences, one can obtain a large effective non-linearity. This approach was then used for the generation of GKP states.

Unfortunately there has been no demonstration of GKP states in the optical domain yet. The main problem consists in the unavailability of naturally occurring and strong non-linearity in quantum optics. However, it has been well-known for a long time that measurements can be used in order to effectively induce nonlinearities [81]. Hence, quite recently it was proposed to use adaptations of Gaussian Boson Sampling (GBS) experiments for the generation of arbitrary bosonic states with some cut-off in the Fock representation. In a GBS experiment we first generate single-mode squeezed states in all modes which is easily possible with state-of-the-art experiments (only the amount of squeezing is restricted by experimental constraints). Then we send these states through a network of beamsplitters and phase shifters implementing some general linear-optical operation. Up to this point the state can be described efficiently in the formalism of Gaussian states, but as the last step we measure the photon number distribution. The calculation of the probability distribution is related to the computation of the hafnian of some matrix which is conjectured to be really hard [82] and GBS is a non-universal type of quantum computing. When measuring the photon distribution of all except one mode, the state of the remaining mode is non-Gaussian and depends on the measurement outcomes. By varying the parameters of the squeezed states and the linear-optical network one can adjust which states should be generated, but because of the measurement process the generation will only work probabilistically with rather low probabilities [83, 84, 85]. With the right choice of parameters and for the right measurement outcomes a approximate GKP state is generated. There is also some trade-off between a high probability of success and the quality of the state, i.e. the amount of squeezing in the peaks.

2 Background

However, there are also some proposals relying on nonlinearities [86, 87]. In Ref. [86] more efficient decompositions of gates into small nonlinearities were considered, while in Ref. [87] nonlinear effects due to Rabi interactions between a two-level system and a bosonic mode (e.g. a trapped ion and a microwave field in a cavity) are considered and approximate GKP states can already be obtained with cavities that are already proposed.

2.4 Quantum communication

The no-cloning theorem and the inability of discriminating non-orthogonal states without distortion lies at the heart of any quantum protocol promising some kind of security. The former follows directly from the linearity of quantum mechanics [24, 25]. The latter can also be proven easily as follows. Let $|\phi\rangle, |\psi\rangle$ be two distinct non-orthogonal states and let $|u\rangle$ be some ancillary state which is used for discrimination. The unitary discrimination operation results in

$$|\psi\rangle |u\rangle \rightarrow |\psi\rangle |v\rangle , \quad (2.79)$$

$$|\phi\rangle |u\rangle \rightarrow |\phi\rangle |v'\rangle . \quad (2.80)$$

By assuming $\langle\psi|\phi\rangle \neq 0$ and making use of the unitarity $1 = \langle u|u\rangle = \langle v|v'\rangle$ needs to hold and thus $|v\rangle = |v'\rangle$ making any discrimination impossible.

The first application of these properties goes back to Wiesner with his idea of unforgeable quantum money [88]. In this proposal a banknote does not only have a printed serial number, but each digit is also encoded within a qubit using either the X - or the Z -basis. The random basis choice is set by the bank at the note generation and it stores the basis choice. When someone wants to deposit the note at the bank, the bank measures the qubits according to the stored bases and only accepts the money when the measurement results match the serial number. Under the assumption of noiseless qubits a note printed by the bank will always be accepted by the bank. However, a forger does not know the base choices belonging to a serial number and therefore he has to guess each basis. With a probability of 50% he guesses right and in the other case the bank obtains the correct measurement result with 50% probability, thus for each individual digit he has a probability of 75% such that the bank does not notice the forgery. A typical serial number consists of multiple digits resulting in an exponentially decreasing acceptance rate of the bank. Hence, for a sufficiently long serial number the banknote is practically unforgeable.

Building upon this idea Bennett and Brassard proposed the first quantum key distribution (QKD) protocol in 1984 encoding the information within two mutually unbiased bases (eigenbases of X and Z), nowadays simply known as BB84 [89]. As it (and variants thereof) is the most prominent QKD protocol and has a structure similar to most other QKD protocols, we will now discuss a pedagogical version thereof in detail following Ref. [19].

Let Alice and Bob be two parties who wish to communicate privately and the eavesdropper is referred to as Eve. We assume that Alice and Bob use a public, authenticated channel for communication, i.e. Eve can listen to messages, but she cannot manipulate them. This is an important assumption as otherwise Eve can easily break the encryption which we will later discuss in detail.

The protocol consists of the following steps:

- Alice uses a random number generator generating two bit-strings a, b of length $(4 + \delta)n$ where all strings are equally likely ($\delta > 0$).
- Alice encodes the random strings in her $(4 + \delta)n$ qubits according to $|\psi_{a_k, b_k}\rangle$ with

$$\begin{aligned} |\psi_{0,0}\rangle &= |0\rangle , & |\psi_{1,0}\rangle &= |+\rangle , \\ |\psi_{0,1}\rangle &= |1\rangle , & |\psi_{1,1}\rangle &= |-\rangle . \end{aligned}$$

- Alice sends her qubits to Bob, who randomly measures them in the X - or Z -basis and confirms the qubits' arrival over a public channel.

2 Background

- Alice and Bob publicly reveal their chosen bases.
- Alice and Bob discard all events where their bases do not match (sifting phase). With high probability a key of length $2n$ remains (δ can be chosen in such a way).
- Alice and Bob announce n bits of their key in order to estimate the error rate.
- Alice and Bob apply error correction such that they obtain a smaller, but equal key.
- Alice and Bob apply privacy amplification in order to obtain a smaller key uncorrelated with Eve.

Intuitively, security originates from Alice using the X - and Z -eigenbasis for encoding the information. As these four states are not mutually orthogonal Eve cannot gain any information without distorting the state. She might as well also perform measurements in the X - or Z -basis on Alice qubits. When she correctly guesses the basis with a probability of 50% she obtains the encoded information and does not change Alice's state. However, whenever she uses the wrong basis she does not obtain any information about Alice's encoded information and the qubit's state is changed which would result in an error rate of 50%. Thus, Eve would introduce a total error rate of 25%. Here, we can already see that the security critically depends on Eve not finding out the preparation bases before Bob performs his measurements as otherwise she could perfectly align her measurements with the preparation basis such that she obtains all the information and does not disturb the qubits. Hence, Bob needs to confirm the arrival over an authenticated channel such that Alice can be sure she talks with Bob and is not tricked into telling Eve the bases too early. Similarly, when Alice and Bob compare their bits an authenticated communication channel is needed as otherwise Eve could tamper with the messages hiding errors. In the end Alice and Bob probably come up with a non-zero error rate due to either eavesdropping attempts or simply noise in the implementation. Typically all information that leaked out due to noise is assumed to be accessible for Eve and the error rates are then used to bound the information that she might have gained about the key. Alice and Bob then make use of classical error-correction (information reconciliation) in order to obtain an equal key with high probability which is then used for privacy amplification such that Eve only has negligible information on the resulting key. The last two steps might either use one-way or two-way classical communication between Alice and Bob allowing for different tolerable error rates [90].

Furthermore, an authenticated communication channel is also needed in order to prevent so-called "man-in-the-middle attacks". In such an attack Eve would impersonate Bob towards Alice and impersonate Alice towards Bob. Then she would simply perform the actual QKD protocol with Alice and Bob giving her a shared secret key with Alice and Bob as well. When Alice uses her secret-key for encryption Eve can simply decrypt the message and later she uses her key shared with Bob to send him the original message. However, Eve is not required to only read the message, but she may even send him a different one.

Secure authentication is a hard problem to achieve without meeting in person to establish a shared secret. Many of today's authentication schemes rely on computational hardness assumptions which we want to get rid of. In order to be information-theoretically secure¹⁶ we need to consume a common secret in order to authenticate each message. Hence, Alice and Bob already need a short secret key in order to start the protocol and parts of the distilled secret-key must be used for authentication in the following rounds.

In principle, one could also use authentication schemes based on computational hardness assumptions in order to distribute the first secret key for practical purposes. Any attack

¹⁶This means the protocol is secure against an adversary with unbounded computing resources and time.

exploiting the hardness assumption must be done during the first round of the QKD protocol. If one is confident that the authentication scheme cannot be broken in this short time, one can still generate secret keys, because the security is not invalidated when the initial authentication scheme is broken at some later point of time after Alice's and Bob's communication. See Ref. [91] for a detailed discussion.

The pedagogical variant of BB84 discussed here has the disadvantage of a large fraction of qubits being discarded or used for testing. This issue was resolved in Ref. [92], where it was shown that it is possible to choose a basis with a probability different from 50% even approaching zero in the asymptotic limit while performing a more sophisticated error analysis, where one does not consider a single error rate Q , but two error rates e_z and e_x for both bases. Thus, the probability of discarding events due to differently chosen bases is highly reduced. Furthermore, it suffices to use only a small subset of qubits for estimating the error rates even approaching a vanishing fraction in the asymptotic regime. A very similar scheme is the six-state protocol [93] where not only two mutually unbiased qubit bases (X, Z) but all three (X, Y, Z) are used. As there is an additional basis, it is more likely that Eve guesses a wrong basis resulting in a higher amount of tolerable noise. Both the BB84 and six-state protocol cannot only be defined for qubits but also for more general qudits [94].

Here we presented BB84 as a prepare-and-measure scheme meaning that Alice prepares some states being measured by Bob, but one can also interpret it as an entanglement-based scheme where entanglement is distributed between Alice and Bob who then both perform X or Z measurements. Imagine Alice generates a perfect Bell state, sends one half thereof to Bob and then they perform the measurements corresponding to the entanglement-based scheme. However, when she measures her half before sending the other half to Bob instead, she simply generated BB84 states and we would call it a prepare-and-measure scheme. From an experimentalist's point of view a prepare-and-measure scheme is simpler to implement, but viewing it as an (virtual) entanglement-based scheme allows for simpler security proofs. From this point of view one would argue that the origin of security lies in the monogamy of entanglement [95], i.e. when two qubits (Alice and Bob) are maximally entangled they cannot be entangled with another qubit (Eve).

The amount of secret key which can be generated is described by the so-called secret-key rate. This decomposes into a raw-rate and a secret-key fraction. The raw-rate is given by the amount of bits which can be generated per time unit and the secret-key fraction gives the amount of secret key which can be distilled per raw bit. For BB84 using one-way classical communication for post-processing the asymptotic secret-key fraction is given by

$$r_{BB84} = \max(1 - h(e_x) - h(e_z), 0) , \quad (2.81)$$

where $h(\cdot)$ is the binary entropy.

Today, countless physical implementations of QKD have been demonstrated using single photons [96, 97] or approximate single photons such as weak coherent states [98, 99, 100, 101], which then need a more detailed security analysis because of multi-photon events [102, 103]. There already exist commercially available QKD cryptosystems (e.g. ID Quantique, MagiQ) and for short metropolitan distances secret-key rates on the order of 10-100 Mbps have been reported [104, 105]. Despite the promise of information-theoretic security multiple QKD systems have been hacked exploiting deviations between the idealized protocol and the actual physical implementation thereof (see Refs. [106, 107] for a review). As most of these attacks targeted Bob's detector, measurement-device independent (MDI) QKD was proposed. In such a scheme Alice and Bob send signals to an untrusted party

2 Background

Charlie who performs measurements potentially correlating Alice and Bobs raw keys (see Fig. 2.5). One can even consider device-independent QKD based on the violation of a Bell inequality such that Alice and Bob only have to assume that their measurement devices do not communicate with an adversary. However, this additional level of security comes at the cost of low secret-key rates.

For large distances the achievable secret-key rates drop significantly because the transmission η decays exponentially within an optical fiber due to absorption. It was shown that for point-to-point QKD a secret-key rate per channel use of at most $-\log_2(1 - \eta) \approx 1.44\eta$ can be achieved (PLOB bound) [6]. Thus, in order to obtain high rates for large distances one has to introduce some intermediate stations in order to reduce the effective length of the transmission channel. One approach is to use so-called quantum repeaters which we will discuss in detail in the next section. Alternatively one can consider trusted-node networks which are already in use connecting, for example, Beijing with Shanghai [108]. In this case many stations are introduced between the endpoints and usual QKD protocols are executed between neighboring stations. As every station is able to decode the messages they need to be trusted.

However, in 2018 the twin-field (TF) QKD protocol was proposed which allows for a secret key rate of $O(\sqrt{\eta})$ without being an experimentally difficult quantum repeater [109]. Several further adaptations have been proposed [110, 111, 112, 113, 114] and an enormous number of experiments overcame the PLOB bound [115, 116, 117, 118, 119, 120, 121, 122, 123, 124]. All adaptations of the twin-field QKD have in common that they do not perform point-to-point QKD (otherwise the PLOB bound would apply), but instead Alice and Bob send coherent states to Charlie in the middle who then should apply a 50:50 beam splitter and measure the photons in both outputs. Similar to BB84 Alice and Bob use some rounds for key generation and some for parameter estimation in order to guarantee security. In the process of key generation, Alice and Bob encode their information within the local phase of the coherent states. Therefore, both require a common phase reference over a possibly large separation which is the main experimental difficulty of this scheme. For example, Alice and Bob could encode a key bit k_A and k_B in a coherent state $|(-1)^{k_{A/B}}\alpha\rangle$ and send them through a lossy channel of transmission $\sqrt{\eta}$ to Charlie who then applies the beam splitter

$$|(-1)_A^{k_A}\alpha, (-1)_B^{k_B}\alpha\rangle \rightarrow \left| \left((-1)^{k_A} + (-1)^{k_B} \right) \sqrt[4]{\eta}\alpha, \left((-1)^{k_A} - (-1)^{k_B} \right) \sqrt[4]{\eta}\alpha \right\rangle. \quad (2.82)$$

Assuming Charlie is honest and detects a photon in the first detector, Alice and Bob learn that they used the same value for k , when Charlie detects a photon in the other mode either Alice or Bob has to flip their bit. In the case where no photon is detected Alice and Bob have to discard their round. However, it is unknown whether Charlie is honest or might even conspire with Eve and therefore we only assume that he performs some POVM with 4 elements corresponding to his announcement “no photon detected”, “photon in the first (second) mode detected” and “photon in both modes detected”. In order to obtain information about the noise channel and the POVM, Alice and Bob send coherent states according to some probability distribution reconstructing the action on the 4-dimensional subspace relevant for key generation. Another major benefit of this scheme is that this scheme does not rely on classical communication except for the classical post-processing in the end such that one can achieve repetition rates on the order of 1 GHz. To summarize, the twin-field protocol consists of the following steps:

- Alice and Bob choose randomly and independent from each other with a probability p_{mode} whether the current round is used for generating a key or for estimating parameters needed for bounding the information leakage to Eve (test mode).

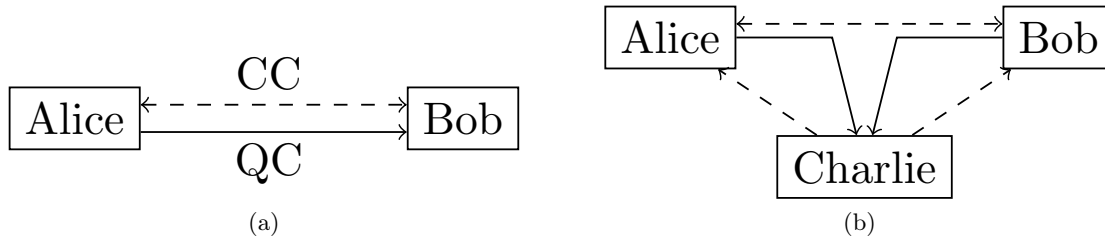


Figure 2.5: Schematic of different types of QKD protocols. Solid lines denote quantum communication and dashed ones denote (authenticated) classical communication. (a) point-to-point QKD, (b) measurement-device-independent QKD as e.g. twin-field QKD.

- If the key-generation mode is chosen, Alice (Bob) generate uniformly distributed random bits k_A (k_B) and send coherent states with amplitude $(-1)^{k_{A/B}}\alpha$ to an untrusted middle station called Charlie (Alice and Bob pre-agreed upon an α requiring a common phase reference). If the test mode is chosen, they generate coherent states of an amplitude according to some fixed probability distribution and send the optical states to the middle station.
- If Charlie is honest, he applies a balanced beam splitter to Alice's and Bob's optical modes and employs on/off detectors for the beam splitters output modes, announcing the measurement results. If Alice and Bob use the key-generation mode and exactly one of the two detectors clicks, k_a and k_b are perfectly (assuming no dark counts) (anti-)correlated depending on which of the two detectors clicked.
- All previous steps are repeated until a long data set is obtained.
- The usual QKD steps of sifting rounds where Alice and Bob used different modes, estimating the error rate and leaked information, error correction and privacy amplification need to be performed.

The summary involving the bullet points is based on Sec. II.A. in **paper I**.

2.5 Quantum repeaters

Due to photonic loss it is very hard to transmit quantum information faithfully over large distances since the transmission probability of a single photon within a fiber $\eta = \exp\left(-\frac{L}{L_{att}}\right)$ decays exponentially with the total distance L and the attenuation length L_{att} depends on the photons' wavelength. For a typical optical fiber minimal loss occurs at telecom wavelength (≈ 1550 nm) corresponding to $L_{att} = 22$ km. In principle, a similar problem arises in the transmission of classical information. However, this problem is solved by repeaters which simply amplify (and reshape if necessary) the signal. Due to the no-cloning theorem this is impossible for general quantum information as it does not allow copying the unknown quantum information without adding some additional noise.

In principle, for long distances the problem of exponentially decreasing transmission can be avoided to large parts by considering satellite uplinks instead of fiber transmission [125]. When using satellite links we only have to consider absorption and scattering in the atmosphere with significant losses in the first and last 10-20 km, for the remaining distance there are almost no losses and the beam width broadens. Of course this approach also has the disadvantage of beam wandering due to turbulences in the atmosphere resulting in a reduced overlap between the beam and the detector. Another drawback is the weather dependence: haze, fog or heavy rain scatter the beam leading to high error rates. Most likely a combination of quantum repeaters and satellites will be considered in the future for very long distance transmission of quantum information where the ground and satellite states are used in order to overcome the really large distance and quantum repeaters will then be used in order to distribute the information from the ground station to the receiver.

In their seminal work Briegel et al. [12] proposed the first quantum repeater in 1998 which is still the underlying basis of today's memory-based quantum repeaters. They considered the problem of the exponential photon decay in fibers and furthermore the exponentially decreasing output state fidelity. In order to tackle this problem they divide the large total distance L into n segments each of length $L_0 = \frac{L}{n}$. Every segment consists of two stations with memories and one tries to generate heralded entanglement between the memories. Heralded entanglement means that one obtains some signal, as for example the measurement of two photons, confirming the successful generation of entanglement. Having this information is absolutely crucial for the quantum memories. Without this information the memories would not know whether the state generation was successful and the memory state should be stored or whether the memory state should be discarded in order to allow for a new entanglement generation attempt. Both memory stations in a segment must have this information and therefore it takes $\frac{L_0}{c}$ to $2\frac{L_0}{c}$ time for an entanglement generation attempt depending on the actual protocol for the transmission of the quantum state and the classical heralding signal. On top there comes the time required for performing the local operations on the memory which can typically be neglected in comparison to the communication times.

Let us now describe how such an entanglement generation could look like in detail. Alice and Charlie are separated by a distance L_0 and both have an atom as their memory system. First, both generate entanglement between the atom and a photon. This might be done by exciting the atom into some state which can then decay into two different ground states and depending on the resulting ground state the emitted photon has a different polarization. Both parties then send their photon to a middle station with a beam splitter followed by polarization beam splitters in order to separate the different polarizations into different spatial modes for the detection. Each mode is measured with on-off detectors and measuring a photon in two modes corresponds to a successful Bell state measurement entangling both atoms via entanglement swapping. Sending the photons to the middle

station takes $\frac{L_0}{2c}$ and sending the heralding information back to the atoms takes the same time, therefore a single entanglement generation attempt takes roughly $\frac{L_0}{c}$. This process is highly probabilistic as both photons must be successfully coupled into the fiber, must not be lost in the fiber and the optical Bell measurement also works only in half of the time [126].

All entanglement generation attempts succeed independently in terms of the different segments and also in time. Therefore, we can assign independent, geometrically distributed random variables for waiting times with probability of success p in each entanglement generation attempt for every segment. For the sake of simplicity, let us now assume that n is a power of two. As soon as two neighboring segments generated entanglement successfully, one can then perform entanglement swapping. In this step two memories in a station are measured collectively in order to perform a Bell state measurement. This operation converts two Bell states each of length L_0 to a single Bell state of length $2L_0$. As the initial Bell states are of imperfect quality, the swapped Bell states quality is further reduced even for an idealized swapping procedure because the noise originating from both Bell states is mapped onto a single state¹⁷. In principle, entanglement distribution in the elementary segments and entanglement swapping is performed until entanglement is distributed over the total distance and the approximate expected distribution time for parallel entanglement distribution is given by $\frac{H(n)}{p}$, where $H(n)$ is the n 'th harmonic number $\sum_{j=1}^n \frac{1}{j}$. Without the quantum memories we would expect a much longer waiting time of p^{-n} as all segments would need to succeed simultaneously. Despite the exponential gain in the waiting time we still have the problem that the final state is of low quality. The idea is to use entanglement purification [128, 129] which transforms many entangled states of low quality into a smaller set of higher quality entangled states by employing local operations and classical communication (LOCC). However, as the input states still have to be entangled, they may not degrade too much and therefore we perform purification after every entanglement swapping which doubles the distance. Hence, we need at least two memories per station in order to perform the purification although it may be reasonable to consider more memories for faster, parallel entanglement generation as the states in the memories also degrade while waiting.

Repeaters following a similar approach [130, 131] are considered as quantum repeaters of the first generation [132]. They have the disadvantage that in the process of entanglement purification they have to communicate over the total distance L resulting in a fairly low achievable distribution rate as the classical communication of the last entanglement purification step already gives an upper bound of $\frac{c}{L}$. Furthermore, due to the long communication times quantum memories with a high coherence time are needed. Thus, when considering an intercontinental communication over a distance of 1000 km the maximal rate achievable by such a repeater without multiplexing would be lower than 200 bits per second. An exemplary repeater protocol involving entanglement purification is shown from a high-level perspective in detail in Fig. 2.6.

Repeaters of the second generation [133, 134] work quite similar, but they do not make use of techniques for improving the state quality that need to communicate over a distance larger than L_0 . Such an approach employs quantum error correction locally on the quantum memories and possibly combines it with entanglement purification on the elementary segment level.

For these memory-based quantum repeaters many other proposals have been made, as for example, the DLCZ protocol [130] based on atomic ensembles and linear optics or the hybrid repeater [131] based on a phase space rotation of a coherent state controlled by a memory qubit.

¹⁷For Pauli-noise this statement also holds in a rigorous sense. (see [127, App. D])

Since the hybrid repeater has some similarities with our repeater proposed in **paper I**, we will discuss it in more detail. In each segment there are two quantum memories and first a non-linear interaction is introduced between the first memory and a cavity mode entangling the coherent state's phase ($\alpha \in \mathbb{R}$) with the memory state

$$\frac{1}{\sqrt{2}} (|\uparrow\rangle + |\downarrow\rangle) |\alpha\rangle \rightarrow \frac{1}{\sqrt{2}} \left(|\uparrow, \alpha\rangle + |\downarrow, \alpha e^{-i\theta}\rangle \right). \quad (2.83)$$

Then the coherent state is sent through an optical fiber to the other memory where the same non-linear interaction is applied followed by a phase shift of θ . For the special case of no loss in the fiber one obtains the state

$$\frac{1}{2} \left(|\uparrow, \uparrow, \alpha e^{i\theta}\rangle + \sqrt{2} |\Psi^+, \alpha\rangle + |\downarrow, \downarrow, \alpha e^{-i\theta}\rangle \right). \quad (2.84)$$

The quantum memories can then be projected onto an entangled state by discriminating the 0 from the $\pm\theta$ phase. One possibility easily applicable in an experiment consists of performing a momentum-quadrature measurement as the 0 phase corresponds to a Gaussian peak at 0 in the momentum space while the $\pm\theta$ phases correspond to Gaussian peaks at $\pm\alpha \sin(\theta)$. However, these peaks have some overlap such that it is impossible to perfectly discriminate the states resulting in some contributions of $|\uparrow, \uparrow\rangle$ and $|\downarrow, \downarrow\rangle$ in the memory state. We have to set a threshold for the momentum deviation from 0 we are willing to accept. On the one hand, by reducing this threshold we improve the state quality, but on the other hand the probability of success also decreases. The contribution from $|\uparrow, \uparrow\rangle$ and $|\downarrow, \downarrow\rangle$ can be avoided by using generalized measurements for unambiguous state discrimination (USD) based on on/off detectors [135] instead of homodyne measurements.

Additional noise arises from the photon loss in the optical fiber and due to dephasing noise occurring in the quantum memory. The memory dephasing can be modeled as

$$\rho \rightarrow \frac{1}{2} \left(1 + e^{-\frac{t}{T_{\text{coh}}}} \right) \rho + \frac{1}{2} \left(1 - e^{-\frac{t}{T_{\text{coh}}}} \right) Z \rho Z, \quad (2.85)$$

where t is the elapsed time, T_{coh} is the memory coherence time (in the remaining thesis the coherence time may also be called T or τ_{coh} in order to be consistent with my other papers) as already discussed in section 2.3.1.

Although, all individual parts of a quantum repeater have been demonstrated already some time ago, the first demonstration of a memory-based quantum repeater overcoming the PLOB bound has only been shown in 2019 [136]. However, in this repeater the authors considered two segments and Alice and Bob sent their signal to the memory station. As both memories are next to each other there is no communication time needed between them such that Alice and Bob can send states at a high repetition rate. This allows them to use a relative short coherence time of ≈ 0.2 ms, but as soon as one considers a repeater scheme that needs classical communication such a low coherence time will not suffice as it would only suffice for communicating over 40km. For repeaters with more than two segments there is no way of getting rid of the communication times entirely and therefore higher memory coherence times will be needed.¹⁸ In 2021 an additional experiment demonstrated a quantum repeater with a much higher coherence time of more than 20 ms even allowing for a protocol involving memory waiting times depending on classical communication times and still producing a non-zero secret-key rate. Although in this experiment they did not beat the PLOB-bound, they were still able to improve the η -scaling of the secret-key rate [137]. Furthermore, in a real-life application the secret-key rate per channel use will not

¹⁸For three segments it is possible to find a scheme with almost constant dephasing time L_0/c .

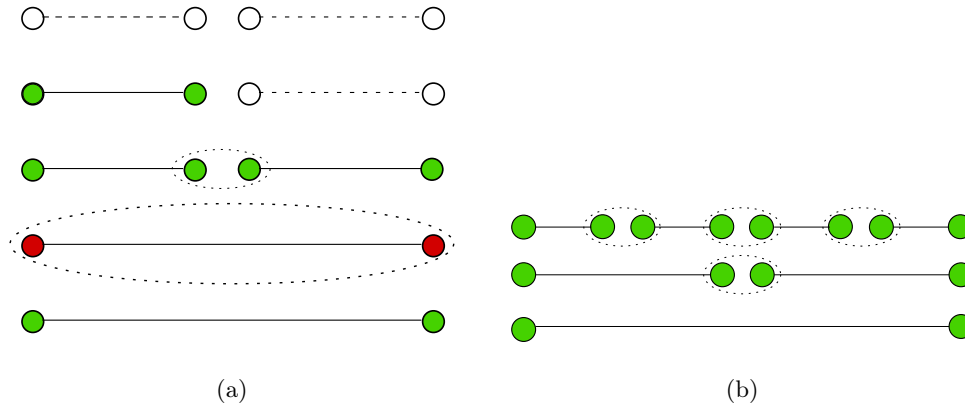


Figure 2.6: (a) Initially, no entanglement is distributed (dashed line) until it succeeds in the left segment denoted by the solid line and green filling to represent that the memories state’s fidelity is above a threshold. Then entanglement is also distributed in the other segment such that one can perform entanglement swapping (dotted ellipse of the inner memories). Due to the imperfect input states the fidelity of the resulting Bell state is lower falling below the threshold (denoted by the red filling) such that purification must be applied (dashed ellipse of the outer two memories). The resulting Bell state is now of high quality. This process is applied recursively to span larger distances. Purification can be used at different times (e.g. even before the first swapping) and it is a branch of research finding protocols with a low cost for a fixed fidelity goal. (b) Doubling the entanglement distance by applying entanglement swapping recursively.

be of much relevance, but rather the secret-key rate per second. State-of-the-art prepare-and-measure QKD schemes can operate at repetition rates on the order of GHz. However, when using memories the interaction between light and memory limits the rate to the order of MHz and when considering communication over 100km the repetition rate even goes down to the order of kHz. Therefore, for a quantum repeater it is not enough to simply overcome the PLOB bound, but one has to overcome it by several orders of magnitude to even compensate the low repetition rate of a memory-based quantum repeater.

A totally different approach tackling the long-distance loss problem without the disadvantage of slow communication times is considered by repeaters of the third generation. These repeaters [13, 14, 15, 16, 17, 18, 138, 139] make no use of quantum memories, but use quantum error correcting codes instead in order to correct the photon loss and the operational errors as well. Typically, Alice encodes the quantum information within an error-correcting code consisting of one or more optical modes and sends the photonic state to the first repeater station. There, one round of error correction is applied and the corrected state is then sent to the next station repeatedly until it arrives at Bob.

On the one hand, these repeaters have the advantage of high repetition rates which are only limited by the local processing times of the error-correction operations and state preparation, but on the other hand, one has the disadvantage of smaller possible distances between repeater stations, because error correcting codes work best in the regime of low error rates. For high loss of $\eta < \frac{1}{2}$ the code cannot improve the transmission, because the environment has more information than the receiving station and as soon as the environment is able to perform a logical measurement on their half the encoded information received at the station is distorted. Thus, the repeater spacing must be smaller than $22 \ln(2) \text{km} \approx 15.2 \text{ km}$ and typical spacings lie in the range of 0.5-5 km in contrast to

2 Background

spacings of tens to hundreds of km in the case of memory-based quantum repeaters.

Most of third-generation repeaters [13, 14, 15, 16, 17, 18] employ a multimode encoding where they encode a physical qubit or possibly a high-dimensional qudit in the presence of a single photon within multiple modes. For example, a qubit might be defined by a photon within two modes, where the two modes are the polarization degrees of freedom. However, of course one can also consider different spatial modes or a time-bin encoding where a photon pulse is either sent early or late. These encodings consist of a total photon number of exactly one such that the channel loss simplifies under the assumption of equal loss rates for all modes. Either the photon is not lost leaving the qubit undisturbed or it is lost leading to a detectable error. Thus, in principle we can measure the total photon number non-destructively giving us the information whether an (erasure) error occurred or not. This information is extremely valuable when considering a concatenation with a qubit-stabilizer code with code distance d . In the case of unknown error position at least $\lfloor \frac{d-1}{2} \rfloor$ errors can be corrected, but when their positions are known the number of correctable errors increases to $d - 1$.

However, performing the measurement of the total photon in a non-demolishing way, which is needed as the syndrome measurements have to be performed later, is experimentally really demanding [140].

A possible workaround is given by an optical implementation of Knill's error correction by teleportation [141]. For this protocol we need an ancillary encoded Bell state. In this protocol we perform quantum teleportation on the high level of the qubit stabilizer code. The measurement of the logical Bell state is then replaced by transversal Bell measurements on the physical qubits. All Bell measurements commute with the logical Bell measurement and their measurement results can be used to obtain the logical Bell measurement outcome and the syndrome. Thus, even in the presence of operational errors one can find the most likely Pauli correction which needs to be applied at the other half of the ancillary logical Bell state. As this half consists of n photons the photon loss has been corrected after a successful teleportation, but it is possible that too many photons of the transmitted code have been lost such that it is impossible to gain enough information for the logical Bell measurement, then the teleportation failed and the photon loss could not be corrected. Unfortunately, a deterministic physical Bell measurement is impossible when using only linear optics and photon counting [142]. Without usage of ancillary photons the maximally obtainable efficiency is given by 50% [126] which can simply be achieved with a balanced beam splitter followed by two polarization beam splitters such that the detectors can discriminate the different polarizations. However, this issue can partly be compensated by the redundancy of the quantum code [15]. By making use of different physical Bell measurements or even using feed-forward, such that the choice depends on previous measurement outcomes, can boost the success probability even further [143, 144]. All these repeater proposals are based on the multi-mode encoding concatenated with a stabilizer code assuming idealized perfectly indistinguishable photons.

The main difficulty of these schemes lies in the state preparation which requires single-photon sources and non-linear interactions [145, App. C/D].

Quite recently also GKP qubits have been considered for repeaters [138, 139] and they have the advantage of simpler Bell measurements, but their state generation is even harder. Bell measurements on GKP codes are discussed in large detail in **paper III** in the main text. An application of GKP qudits in combination with quantum polynomial codes for quantum repeaters is also discussed in **paper V**.

3 Results

The papers in this thesis can be classified into two topics. On the one hand, we consider quantum repeaters based on quantum memories (**paper I, II and IV**), which are well suited for a near-term implementation, but have the disadvantage of low repetition rates. On the other hand, we also take a look at quantum repeaters solely based on quantum error correction (**paper III and V**) which ultimately can achieve much higher rates, but require much more sophisticated hardware, such that they will probably only be implemented in the far future. In this section I will briefly summarize the results of the papers.

3.1 Memory-based quantum repeaters

3.1.1 Twin-field-inspired quantum repeater

When discussing twin-field QKD we already saw that it is possible to improve the loss scaling of the secret-key rate in comparison to point-to-point QKD from $\mathcal{O}(\eta_{total})$ to $\mathcal{O}(\sqrt{\eta_{total}})$ by considering a beam splitter in the middle between Alice and Bob. A conventional memory-based quantum repeater reduces the loss scaling by breaking up the total distance into n segments each equipped with quantum memories reducing the loss scaling from $\mathcal{O}(\eta_{total})$ to $\mathcal{O}(\sqrt[n]{\eta_{total}})$. The main idea of this paper (**paper I**) is to combine the advantages of both approaches resulting in a loss scaling of $\mathcal{O}(\sqrt[2n]{\eta_{total}})$. Our considered QKD protocol is an adaptation of the BB84 protocol applied to a repeater very similar to the hybrid quantum repeater. In our proposed repeater in every segment and in each of both memories we generate the state

$$\frac{1}{\sqrt{2}} \left(\left| \uparrow, \alpha e^{-i\theta} \right\rangle + \left| \downarrow, \alpha e^{i\theta} \right\rangle \right), \quad (3.1)$$

where the coherent state's phase is entangled with the memory state due to a non-linear interaction, and we send the two photonic modes to a beam splitter in the middle between both memories. After applying the beam splitter we consider either on/off detectors, PNRDs or homodyne measurements. The transition from twin-field QKD to a twin-field inspired quantum repeater is shown in Fig. 3.1. For the sake of simplicity, let us first consider the case where loss is the only type of noise occurring.

The resulting states when employing on/off detectors or PNRDs are very similar as both project the memories onto a mixture of two Bell states. For the most relevant case of on/off detectors we obtain

$$\frac{1}{2} \left(1 + e^{-2(2-\sqrt{\eta})\alpha^2 \sin^2(\theta)} \right) \left| \Psi^+ \right\rangle \left\langle \Psi^+ \right| + \frac{1}{2} \left(1 - e^{-2(2-\sqrt{\eta})\alpha^2 \sin^2(\theta)} \right) \left| \Psi^- \right\rangle \left\langle \Psi^- \right|, \quad (3.2)$$

where η denotes the transmission from one memory to the other.

When considering PNRDs instead of on/off detectors the distributed state takes a similar form, but the exponential is replaced by $e^{-4(1-\sqrt{\eta})\alpha^2 \sin^2(\theta)}$ ¹, hence significant discrepancies between both detectors only occur at small distances between the memories. The loss does not only reduce the probability of generating entangled memory states, but it also affects

¹This is stated incorrectly in the main text of the published version, where $e^{-2(1-\sqrt{\eta})\alpha^2 \sin^2(\theta)}$ is written. However, in appendix E of the paper it is given correctly. Employing PNRDs instead of on/off detectors does not lead to any advantage in the regime of $\sqrt{\eta} \ll 1$.

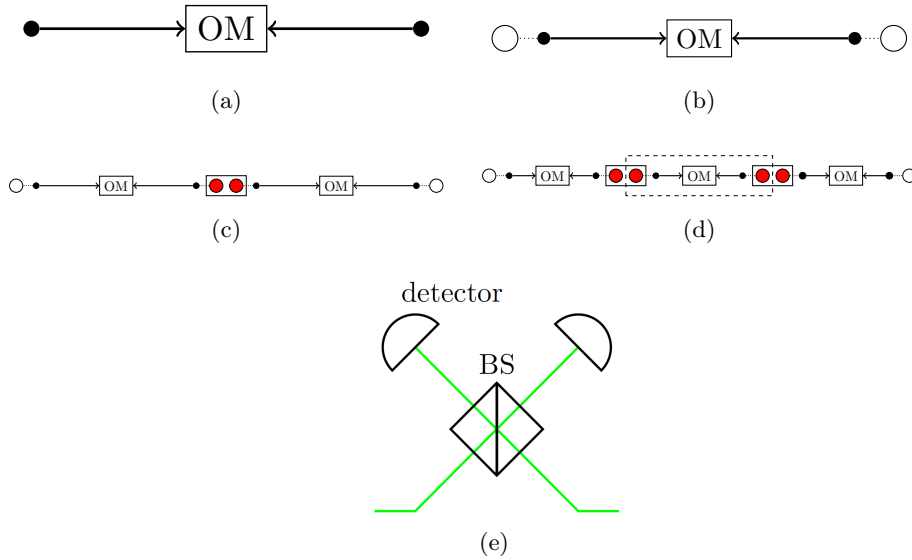


Figure 3.1: Illustration of the protocol. (a) Phase-matching QKD. Alice and Bob send optical coherent states (black filled points) to Charlie who performs an optical measurement (OM). (b) Entanglement-based variation of phase-matching QKD ($n = 1$). Alice and Bob each have an optical mode (black filled point) entangled with a short-lived memory (white filled circle). The optical fields are sent to Charlie's OM. The memories can be short-lived since it does not matter when Alice and Bob perform the measurements on their memories (as long as they wait with communicating their choice of measurement basis). (c) Two-segment repeater variant ($n = 2$). Two copies of (b) are used where the memories in the central node need to be long-lived (red filled circles), since either of them has to wait until the other segment succeeds. When both segments succeeded, a Bell measurement is performed on the two long-lived memories for entanglement swapping. (d) Three-segment repeater variant ($n = 3$). In order to obtain the n -segment repeater one simply needs to use $n - 2$ inner segments (marked by the dashed box). Such a n -segment quantum repeater scheme consists of $2n$ physical segments. (e) Set-up of the OM. Usually the detectors are on/off-detectors, but we could also use PNRDs. For $\theta \ll 1$ we only need one detector. 'BS' stands for beam splitter. Reprinted from **paper I**.

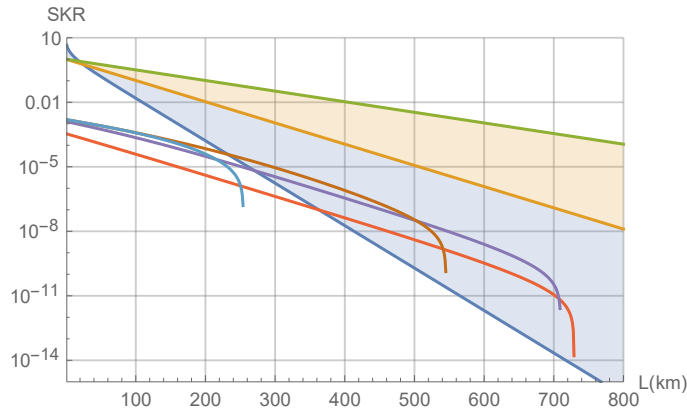


Figure 3.2: Secret-key rates per channel use for a two-segment repeater ($n = 2$, parallel scheme) without phase mismatch assuming the parameters as listed in the main text of **paper I** (including $p_{\text{det}} = 0.15$) and a memory coherence time T of 1 second. The straight lines (from bottom to top) denote the PLOB bound, $\sqrt{\eta_{\text{total}}}$, and $\sqrt[4]{\eta_{\text{total}}}$. The rates are for different values of the memory cut-off (10,100,1000,10000) (from right to left). The areas between PLOB and $\sqrt{\eta_{\text{total}}}$ and between $\sqrt{\eta_{\text{total}}}$ and $\sqrt[4]{\eta_{\text{total}}}$ are highlighted in color. Adapted from **paper I**.

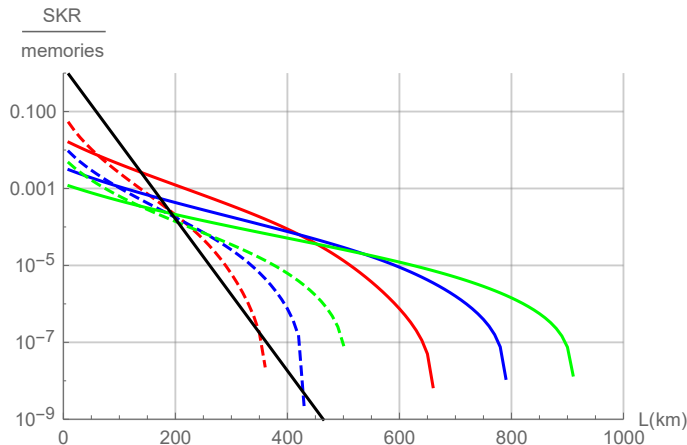


Figure 3.3: Comparison of the secret-key rate per channel use per employed memory (station) for our scheme (solid lines) and the USD hybrid scheme (dashed lines) for $n = 2, 3, 4$ (from left to right in the regime of rates dropping towards zero) assuming a coherence time of $T = 10$ s, a depolarizing channel with $p_{\text{depol}} = 10^{-3}$ and a sequential scheme (parallel for $n = 2$). The black solid line corresponds to the PLOB bound. Reprinted from **paper I**.

the state quality as it introduces dephasing which comes on top to the dephasing due to imperfect memories. The probability to measure at least one photon at one specific beam splitter output is given by $p = \frac{1}{2} \left(1 - e^{-2\sqrt{\eta}\alpha^2 \sin^2(\theta)} \right)$ in the case of a small non-linearity θ , which is often easier to achieve experimentally. However, for $\theta = \frac{\pi}{2}$ this probability can be doubled as photons at both output modes result in entangled memory states. After performing the entanglement swapping on all n segments, we obtain a memory state which is again a mixture of two Bell states and the exponential simply needs to be taken to the n 'th power. In this proposal α is a real parameter tuning the tradeoff between a high probability of success and a high state quality. Here, we consider the application of BB84 and choose α in such a way that the secret-key rate is maximized resulting in a rate per channel use of approximately $2\sqrt{\eta_{total}} \frac{3.57 \times 10^{-2}}{nH(n)}$, where $H(n)$ is the n 'th harmonic number $\sum_{j=1}^n \frac{1}{j}$. For this approximation we assume that all segments generate entanglement in parallel, photon loss is the only occurring error channel and $\sqrt{\eta} \ll 1$.

Additionally, we also calculate secret-key rates for a more sophisticated error model consisting of memory dephasing, detector dark counts, random phase differences between Alice's and Bob's oscillators and imperfect swapping operations. As one can see in Fig. 3.2 it becomes apparent that even under a detailed error model the PLOB bound can be overcome by our proposal even with $n = 2$. For $n = 2$ we consider parallel entanglement distribution as we are able to calculate the expected memory dephasing. However, for $n > 2$ we only consider a sequential distribution as this allows for a simple and exact calculation of the expected memory dephasing, while for the parallel distribution we are only able to bound the dephasing with Jensen's inequality leading to worse rates.

Regarding the finite memory coherence time we show that it is very beneficial for the secret-key rate to consider memory cut-offs, i.e. after some time one discards memory states in order to guarantee a high state quality. Additionally, Alice and Bob should perform their QKD measurement on their memories as soon as possible and do not wait until they share an entangled state. As a consequence their memories do not accumulate unnecessary dephasing noise. Especially, in a sequential entanglement distribution scheme this becomes apparent as there is always only a single memory pair waiting and when Alice/Bob measure their memory at the beginning only a single memory dephases, effectively doubling the memory coherence time.

Finally, we also compare our proposed repeater with the hybrid quantum repeater using unambiguous state discrimination as both scheme employ almost the same resources. In Fig. 3.3 one can see that our proposal based on the beam splitter in the middle gives rise to much higher secret-key rates.

3.1.2 Theoretical analysis of experiments in the Q.Link.X project

In **paper II** we compare different experimental platforms such as color centers (NV, SiV), quantum dots, ions (calcium, ytterbium) and atoms (rubidium) from the Q.Link.X project as possible quantum memories for quantum repeaters. In order to compare them we consider a simple set of three parameters, namely P_{link} which incorporates imperfections going into the probability of generating entanglement within a repeater segment on top of the photon loss. This may involve for example probabilistic state generation, coupling inefficiencies, detector inefficiencies, memory write-in inefficiencies and the frequency conversion to the telecom wavelength. Another very important parameter is the memory coherence time τ_{coh} , the last and least important parameter is the time τ_{clock} required for one entanglement generation attempt without communication times, e.g. it is limited by the memory write-in time or the detectors dead time.

In this work we always consider small-scale repeaters of two segments, but we also consider two different repeater protocols. For both protocols we calculate the distributed quantum state in the process of quantum memory dephasing. We assume parallel state distribution in both segments and the relevant quantity for the memory dephasing depends on the used memory time $|N_1 - N_2|T_0$, where N_1 and N_2 are random variables counting the entanglement distribution attempts and T_0 denotes the total time required for a entanglement generation attempt. Since each individual distributed quantum state depends on the quantity $\exp\left(-\frac{T_0}{\tau_{\text{coh}}}|N_1 - N_2|\right)$, we calculate the expectation value $\mathbb{E}\left(\exp\left(-\frac{T_0}{\tau_{\text{coh}}}|N_1 - N_2|\right)\right)$ for cases with and without cut-off while for the calculation of waiting times we use results known from the literature [146, 147]. On the one hand, we have the node-sends-photon protocol (see Fig. 3.4 (a)), where in each segment the memory nodes send a photon to a station in the middle of the segment performing a photonic Bell state measurement requiring a communication time of $\frac{L_0}{c}$ per entanglement generation attempt. On the other hand, we consider the node-receives-photon protocol (see Fig. 3.4 (b)), where the photons are sent to the memory node and written in locally, thus the memory does not need to wait for some classical communication in order to decide whether it should keep the state or not. Therefore, the repetition rate is only limited by the local operation time τ_{clock} making this protocol very attractive for platforms with a small τ_{clock} as typically communication times are much longer. However, the complete omission of communication time does not work for larger repeaters with $n > 2$.

We then use parameter values obtained in discussions with experimentalists in order to calculate secret-key rates and obtainable raw rates with a minimal fidelity of 0.95 for both repeater protocols. We consider a memory cutoff in order to guarantee the minimal fidelity or to optimize the secret-key rate.

Employing the node-sends-photon protocol we find that rubidium atoms are the only platform that is able to overcome the PLOB bound with current experimental parameters and it also barely does it (see Fig. 3.5). Probably it would not overcome it in a real experiment or when considering a less idealized error model. However, when considering potential future parameter values all platforms except quantum dots are able to beat the PLOB bound in our idealized model. The reason for the bad performance of quantum dots is that they have the advantage of a really high clock rate of 1 GHz, but they also have the disadvantage of an extremely small memory coherence times of $0.3 \mu\text{s}$. Unfortunately, the high clock rate cannot be made use of and the low memory coherence time makes this platform unsuitable for this protocol.

Employing the node-receives-photon protocol we find that already with today's experimental parameters all platforms are able to overcome the PLOB bound, but this protocol will not be scalable to more than two segments without losing its advantage of the high clock rate. In the calculation for the node-receives-photon protocol we assume a deterministic write-in process of the photonic qubit into the memory. However, such a direct

3 Results

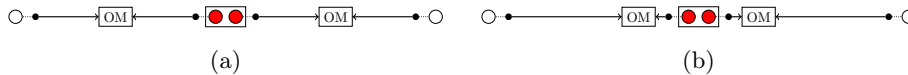


Figure 3.4: (a) Node-sends-photon: In each segment the nodes with quantum memories (in the context of QKD the memories represented by the white balls can be replaced by sources of BB84 states) send the photons to a middle station for a Bell measurement. Sending the photons to the middle station takes a time of $\frac{L_0}{2c}$ and communicating the measurement outcome to the quantum memory (red ball) additionally takes the same time. The quantum memory needs to obtain this information in order to know whether (virtual) entanglement between the two memories has been created such that the state should be stored or if a new distribution attempt should be started. (b) Node-receives-photons: In essence it is a similar protocol as discussed in (a), but the optical measurement is performed at the quantum memories (red balls) such that the communication times are close to 0 for the used quantum memories. The outside memories are replaced by sources of BB84 states with an high repetition rate which give the clock rate of the protocol. Events where the optical measurement fails can simply be discarded in the classical post-processing.

write-in often has the problem that one does not know whether the photon arrived at the memory station. Thus, we also consider an additional variation of the memory write-in where the quantum memory generates an entangled state with a photon and a photonic Bell measurement is performed between this auxiliary photon and the photon sent through the fiber. If the photon is not lost in the fiber, the Bell measurement can succeed teleporting the sent quantum state directly into the memory where the measurement of both photons heralds the successful memory-write in. Unfortunately, the generation of the entangled state between the memory and the auxiliary photon slows down the obtainable clock rate. This variation also leads to lower secret-key rates per channel use than the approach assuming direct memory-write in, but by assuming future experimental parameters the PLOB bound can also be beaten easily.

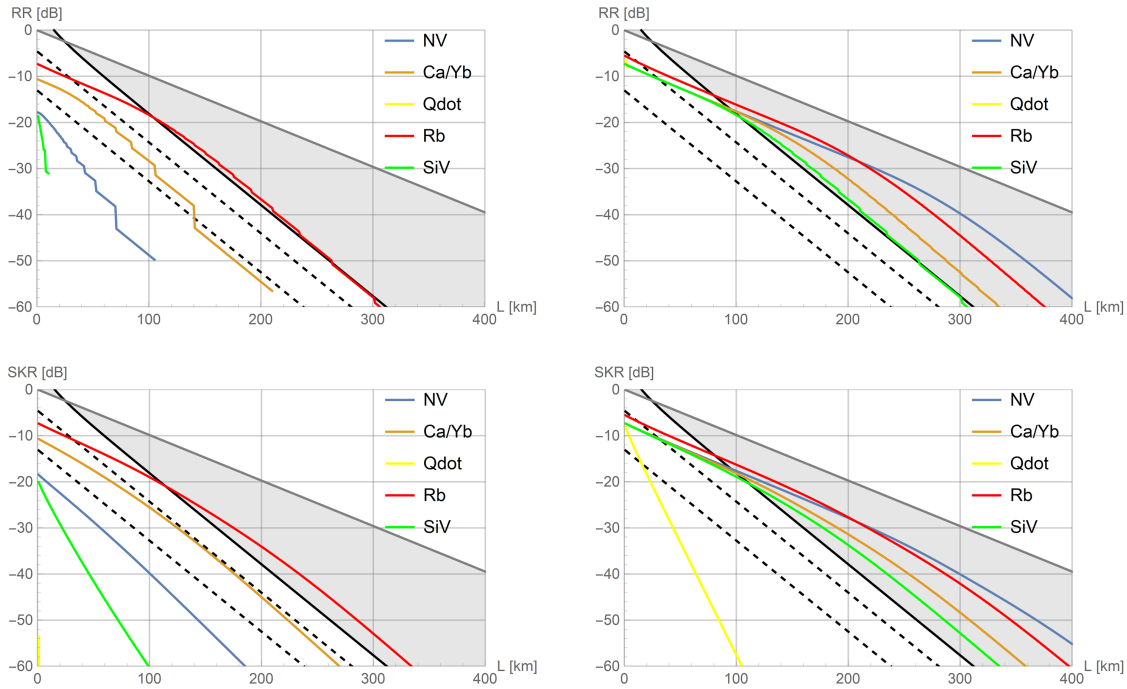


Figure 3.5: Secret key rates (SKR) and high-fidelity raw rates (RR) for a small NSP-based QR scheme (QR cell). The bottom plots show SKR in dB as a function of the total distance L in km for experimental parameters as currently available (left) and as potentially available in the future (right). The top plots show RR in schemes where the entangled states effectively created over the total distance L have a fidelity of at least 0.95 (left: current parameters, right: future parameters). Curves that are disappearing beyond certain distances (or completely missing for quantum dots) no longer (never) exceed $F = 0.95$. The different platforms correspond to NV (violet) and SiV (green) centers, ions (brown), rubidium atoms (red), and quantum dots (yellow). The light gray area illustrates the (secret key) rate regime between $\sim \eta$ (curve in bold black: “repeaterless” bound) and $\sqrt{\eta}$ (line in dark gray: optimal rate for QR cells or two-segment QR schemes). The bold black dashed lines represent the realistic “repeaterless” bound $P_{\text{link}}\eta/2$ (direct transmission via PPL) with finite link efficiencies $P_{\text{link}}=0.1, 0.7$.

Reprinted from **paper II**.

3.1.3 Analysis of a multi-segment twin-field-inspired quantum repeater

This work (**paper IV**) deals with larger quantum repeaters of up to 8 segments without considering entanglement purification under the assumption of deterministic entanglement swapping. The paper can be separated into two parts. In the first part we discuss the general error model consisting of constant Pauli channels and memory dephasing dependent on a random variable counting the totally accumulated used storage time of all memories similar as in **paper I** or **paper II**. This random variable depends on multiple factors like the overall number of segments n , the strategy of how entanglement should be distributed (sequentially vs. in parallel), and on when entanglement swapping should be performed. The main results of this first part are systematically calculated probability generating functions (PGFs) $f_D(t) := \sum_{j=0}^{\infty} \mathbb{P}(D = j)t^j$ of these random variables D counting the accumulated used memory time for various protocols, containing all of their information and allowing for an easy calculation of $\mathbb{E}(e^{-\alpha D}) = f_D(e^{-\alpha})$ which is the expected dephasing with α being a real number including the memory coherence time and time per entanglement generation attempt. Especially practical strategies beyond sequential entanglement distribution and swapping are considered filling a gap of **paper I** where such protocols could only be considered in calculations by making use of Jensen's inequality leading to rather loose bounds in the regime of realistic memory coherence times. Furthermore, we also consider strategies involving memory cut-offs and multiplexing, where multiple entanglement generation attempts are done in parallel in each segment. In addition, for the case of $n = 3$ segments we consider all possible entanglement distribution and swapping strategies without a cut-off with a fixed entanglement distribution time in each segment, but including protocol variations adapted towards QKD where Alice and Bob perform their measurements on the end nodes as soon as possible and they do not wait until entanglement has been distributed over the total distance. This variation has the advantage that some quantum memories are used a shorter time and therefore accumulate less dephasing noise.

Using these calculations we analyze minimal parameters needed in our general error model such that it is possible to obtain a non-zero secret-key rate or even beat the PLOB bound for different distances. Our calculations show that the best secret-key rates can be obtained by strategies with parallel entanglement distribution, swapping as soon as possible and minimizing the amount of parallel quantum storage time. Swapping as soon as possible is beneficial, since it reduces the number of quantum memories which need to store quantum information in parallel during the time of entanglement distribution over the overall distance. These conditions can be expected intuitively, but there is also some tension between the parallel entanglement distribution and the minimal amount of parallel storage. In a sequential entanglement distribution strategy Alice can perform her BB84 measurement in the beginning and thus in each time step there is only a single quantum memory dephasing in a segment. Furthermore, after entanglement has been distributed in the second segment, one can perform entanglement swapping between the first two segments and again there is only one memory waiting until entanglement is distributed in next segment. However, when considering parallel entanglement distribution, it is possible that first entanglement is distributed in a middle segment where both quantum memories need to store quantum information because neither Alice nor Bob can perform a measurement. It is also possible that first entanglement is distributed in the segments next to Alice and Bob, but the segments in the middle did not succeed also leading to two quantum memories dephasing simultaneously. Therefore, parallel distribution has advantages regarding the waiting time until entanglement is distributed over the total distances, but other schemes can be better concerning dephasing due to multiple memories dephasing simultaneously in the parallel scheme. This effect becomes most prominent for low memory coherence times. In most reasonable cases one obtains optimal or at least rather good

secret-key rates by considering a parallel entanglement distribution scheme where entanglement swapping is performed as soon as possible.

In the second part of the paper we apply our previous results to different quantum information encodings and compare three kinds of repeater architectures:

In all three architectures we consider the same qubit memories and the same optical measurements in the middle station. The only difference of the three architectures lies within different optical states which are entangled with the memories. The first architecture consists of a multimode encoding (dual-rail), which means the photonic information carrier is a single photon in two modes, e.g. horizontally or vertically polarized. As the second architecture we consider a twin-field-inspired repeater as introduced in **paper I**, thus the photonic information is encoded in the phase of a coherent state. As the third and last architecture we consider the Cabrillo scheme, where the photonic information is encoded in a superposition of either zero or one photon.

Schemes 2 and 3 rely on single-photon interference at the beam splitter in the middle of a segment and have therefore a scaling advantage in comparison to the first scheme which relies on two-photon interference. However, in the multimode encoding the distributed states are of higher quality as the measurement of both photons heralds that no photon was lost, which would leak information to the environment. As a consequence schemes 2 and 3 outperform scheme 1 when there are almost no depolarizing errors ($\mu \approx 1$), because then the increased error rates are not problematic as they lie well below the critical error rates for QKD, but the improved scaling has a huge impact. When considering more and more depolarizing noise, the increased error rates become very important as the secret-key fraction drops to 0. Therefore, the multi-mode encoding is highly competitive or even the better option when considering rather realistic noise parameters. Although schemes 2 and 3 both rely on single-photon interference, their idealized distributed entangled states are not the same. Scheme 2 prepares the memories in a mixture of two Bell states, such that there is only one basis with a non-zero error rate. For scheme 3 the probability of an error is smaller, but they affect both error rates reducing the secret-key fraction enormously. Hence, scheme 2 is significantly better than scheme 3 for small depolarizing error rates ($\mu \approx 1$) as then there are almost no errors in one error basis. For larger probabilities of depolarizing errors scheme 3 becomes better as it has less intrinsic errors and because of the depolarizing errors both schemes have a significant error rate in both bases (see Fig. 3.6).

3 Results

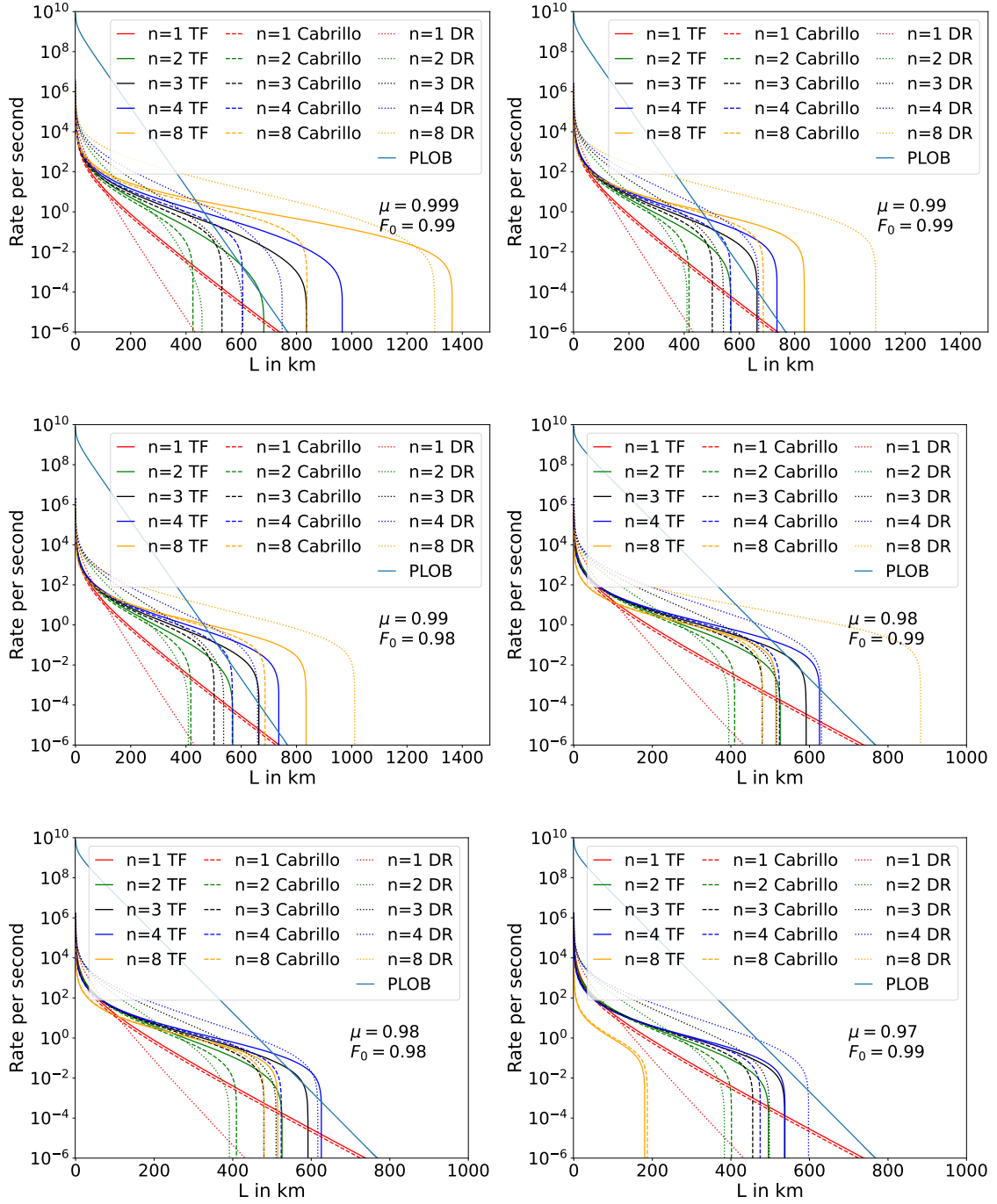


Figure 3.6: Secret key rates per second for the three repeater architectures for different error parameters (μ denotes depolarization errors in individual segments and the swapping operation). As the schemes based on single-photon interference (TF and Cabrillo) already generate imperfect entangled memory states we also consider some dephasing with parameter F_0 for the dual rail (DR) scheme in order to avoid comparing ideal states with imperfect ones. We always assume a coherence time $\tau_{coh}=10\text{s}$, $p_{link,TF} = 0.9$, and no multiplexing. Adapted from **paper IV**.

3.2 Error-correction-based all optical quantum repeaters

3.2.1 GKP syndrome measurements and linear optics

Paper III is about efficient ways to obtain the error syndrome of general GKP codes. By using GKP ancillae, Gaussian operations and homodyne measurements it is straightforward to obtain the GKP error syndrome as already discussed in section 2.3.3 (also see Fig. 3.7 (a)). However, these required Gaussian operations typically also involve squeezing operations. Although, it is usually easier to implement them than other non-linear interactions, their online implementation is experimentally not that simple especially for high amounts of squeezing. Therefore, we investigate whether these Gaussian operations can be replaced by linear optical ones and we find that it is possible.

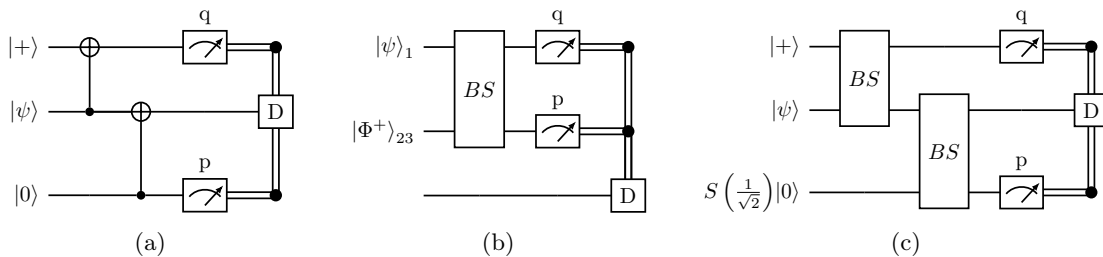


Figure 3.7: Different syndrome measurement schemes for GKP codes. Depending on the measurement outcomes a displacement D is applied as the recovery operation. (a) Scheme proposed in the original GKP paper. CSUM gates are used to copy the displacement errors from the data qubit to the ancilla states where homodyne measurements can detect them. (b) Teleportation based syndrome measurement using only linear optics. (c) Scheme similar to the one in (a) but the CSUM gates are replaced by simple balanced beam splitters, requiring one offline squeezed ancilla state. Adapted from **paper III**.

The first proposed method is based on quantum teleportation (see Fig. 3.7 (b)). Interestingly, the teleportation can be understood from two perspectives. On the one hand, it can be seen as a continuous-variable (CV) teleportation as the measurement works exactly the same as in the CV teleportation and the calculation can be done in a very analogous way where the (infinitely squeezed) two-mode squeezed state is simply replaced by a GKP Bell state. On the other hand, it can also be understood as the discrete-variable teleportation explained in Eq. 2.19, where all qubit operations are replaced by their realization of the GKP qubit. In the special case of square GKP qubits the Bell measurement is simply implemented with a balanced beam splitter followed by homodyne measurements in the q and p quadrature. However, these quadrature measurements return a real number instead of an integer one required for choosing the suitable Pauli correction and therefore it also includes the GKP error syndrome that we wanted to measure. Similar approaches also work for more general GKP codes where n qubits are encoded within n modes. The required GKP Bell states can be systematically obtained by simply applying $\text{CNOT}_{12} |+\rangle_1 |0\rangle_2$ and replacing everything with the GKP representative. However, this has multiple drawbacks as the CNOT requires squeezing operations. First of all it is harder to implement Gaussian instead of linear optical operations and furthermore, being even more important, Gaussian operations can propagate displacement shifts resulting in correlated errors on multiple modes. When these correlations are neglected (which is sometimes inevitable as e.g. in repeater chains with local decoders) the effective error rate is increased. This is a very significant issue as ideal GKP states are unphysical and thus every physical GKP realization necessarily does involve displacement errors in comparison to the ideal state. In stark con-

trast to Gaussian operations, isotropic noise is left invariant by linear optical operations. A method for obtaining square GKP qubit Bell states from GKP-like state in combination with a simple balanced beam splitter has been proposed in Ref. [148]. In **paper III** we generalize this result from the square GKP code to arbitrary GKP codes encoding n qubits within n modes. In addition, we also show that there is no direct generalization to GKP codes encoding k qubits within $n > k$ modes. Furthermore, we also generalize the scheme from the qubit case to arbitrary qudits of even dimension.

Additionally, we also propose another scheme for obtaining the syndrome information using linear optics (see Fig. 3.7 (c)) which is very similar to the scheme involving general Gaussian operations proposed in the original GKP paper. In our proposed scheme we replace the CSUM gates with simple balanced beam splitters and we have to squeeze one of the ancilla state by a factor of $\frac{1}{\sqrt{2}}$ which can simply be absorbed into the state generation without making it experimentally any harder.

When considering the concatenation of a GKP code with a high level qubit stabilizer code, people in the literature typically first performed $2n$ measurements of the GKP qubits for correcting the small shifts on the GKP qubits followed by $n - k$ measurements in order to obtain the syndrome information of the higher level code, where every measurement requires a GKP ancilla. For example, let us consider the concatenation of square GKP qubits with a two qubit repetition code stabilized by $Z_1 Z_2$. Thus, following this naive approach we would first measure the four stabilizers of the GKP qubits

$$\exp(i2\sqrt{\pi}\hat{q}_1), \quad \exp(-i2\sqrt{\pi}\hat{p}_1), \quad \exp(i2\sqrt{\pi}\hat{q}_2), \quad \exp(-i2\sqrt{\pi}\hat{p}_2) \quad (3.3)$$

followed by a measurement of

$$\exp(i\sqrt{\pi}(\hat{q}_1 + \hat{q}_2)) \quad (3.4)$$

as the stabilizer measurement of the high-level repetition code. However, it is easy to see that there is some redundancy in the syndrome measurements since

$$\exp(i2\sqrt{\pi}\hat{q}_2) = \exp(i\sqrt{\pi}(\hat{q}_1 + \hat{q}_2))^2 \exp(i2\sqrt{\pi}\hat{q}_1)^{-1} \quad (3.5)$$

and therefore we see that there are only 4 independent stabilizer generators to be measured for the concatenation of the GKP code with the repetition code instead of 5 stabilizer measurements. As a consequence we can avoid the preparation of one GKP ancilla for obtaining the syndrome information. We show that the concatenation of any $[[n, k, d]]$ qubit stabilizer code with GKP codes corresponds to some general GKP code defined on a lattice in the $2n$ -dimensional phase space. Since stabilizer generators correspond to basis elements of this lattice, it is clear that there are only $2n$ stabilizers needed to be measured. Using the naive approach one would first perform $2n$ measurements for correcting the individual GKP codes followed by additional $n - k$ measurement for obtaining the syndrome information of the high level code leading to a significant waste of GKP ancilla states.

It is even possible to combine the idea of performing only $2n$ measurements with linear optics. This can be seen easily by obtaining the syndrome information of the high level code by Knill's error correction by teleportation, where the Bell measurements are realized by a balanced beam splitter followed by two quadrature measurements. As already discussed in this section these individual Bell measurement also give the syndrome information of the GKP code.

Unfortunately, the required logical Bell state cannot be generated by independent single-mode GKP states with a rectangular lattice followed by a linear-optical operation when the high-level code is able to correct arbitrary single-qubit errors. This problem does not only exist in the context of logical Bell state generation, but it also applies in many other cases. We assume that for the input state there exists an orthogonal basis of the lattice

and linear optics preserves this property. However, following Ref. [149] one can see that codewords of most relevant codes correspond to a lattice where no orthogonal basis exists.

Similar to the teleportation it is also possible to generalize our proposed sequential syndrome measurement scheme for concatenations of GKP codes with high-level codes. One simply has to replace the ancilla states to the corresponding equivalents of the high level code and all beams splitters and measurements have to be applied in a transversal way.

Finally, we observe that it is also really useful to view GKP codes concatenated with a high level code as a code defined by a lattice as this allows one to use tools from lattice theory like Voronoi cells of a lattice. Voronoi cells can be defined for every space and a set of points being element of this space. For every point of this set one can consider the region of the space where no other point of this set is nearer according to some metric. These regions then define the Voronoi cells.

Instead of considering the analog information in the GKP syndrome as proposed by Fukui [78] and feeding it in the decoder of the high-level code and performing a Monte-Carlo simulation for calculating the resulting error probabilities, one can also calculate the Voronoi-cells with respect to the euclidean distance of the symplectically-dual lattice and integrate the Gaussian probability distribution of the displacement shifts over the Voronoi-cells belonging to lattice points corresponding to the logical identity operation as a more systematic approach. For the example of the three-qubit bit-flip code most of the integration can be done analytically and one is only left with a one dimensional integral, which can then be calculated numerically.

Although all of these results are obtained while having a quantum repeater as an application in mind, they are much more general and can e.g. also be applied in the context of quantum computation with GKP codes.

3.2.2 GKP qudit repeater

In section 2.5 we discussed the different generations of quantum repeaters with their advantages and disadvantages. Here, in **paper V** we consider a third-generation quantum repeater based on GKP codes. For quantum communication we only require Clifford operations, which can be implemented on GKP codes by using Gaussian operations. In some of our protocols we even got rid of the Gaussian operations and replaced them with linear optical ones. We do not only consider square GKP qubits, but also higher dimensional qudits, such that the qudit dimension D is a free parameter which shall be optimized. As GKP codes are designed to correct displacement errors, we consider two methods which convert the loss to a Gaussian displacement channel. The first method consists of applying a quantum amplifier with gain η^{-1} before the loss channel with transmission η is applied. The concatenation of these two channels is equivalent to a Gaussian displacement channel with variance $1 - \eta$. The second method only works with teleportation-based protocols where both halves of a Bell state are sent into opposite directions and where the amplification is applied on the classical measurement data by a simple multiplication leading to an experimental simplification.

For obtaining the syndrome information we follow two different approaches. The first one is a teleportation based syndrome measurement introduced in **paper III** correcting errors in both quadratures at every repeater station and the other approach is an adaptation of Ref. [18] where in each repeater station errors of only one quadrature are corrected in an alternating manner.

First, we consider a teleportation-based repeater employing bare square GKP qudits with a fixed repeater spacing with optimal qudit dimension D for different total distances and different amounts of squeezing in the GKP state preparation. As shown in Fig. 3.8 one can see that qudits beyond qubits can be beneficial for the achievable secret-key rate when high quality GKP states are available.

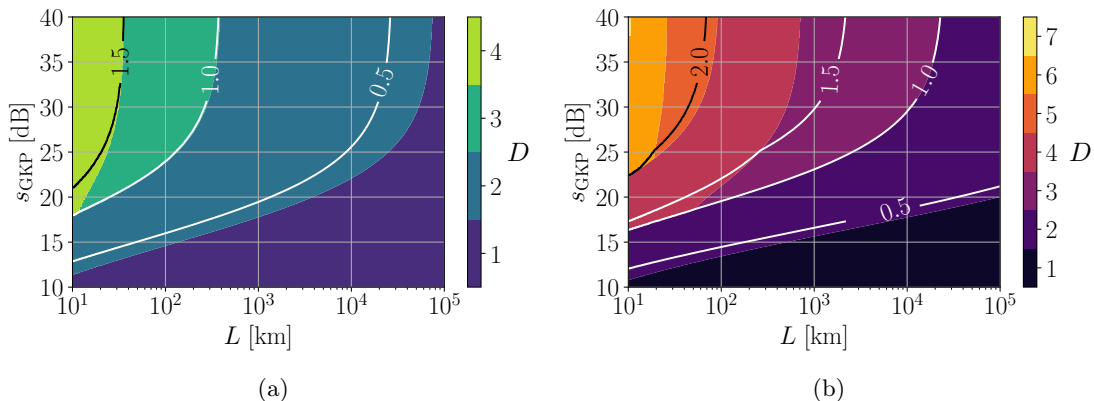


Figure 3.8: Optimal qudit dimension D of a GKP-based quantum repeater with repeater spacing $L_0 = 500\text{m}$ and coupling efficiency $\eta_c = 99\%$ using the pre-amplification scheme (a) and the two-way scheme (b). For each choice of total repeater length L and squeezing parameter s_{GKP} , the qudit dimension D (color coded) is adjusted to the value that maximizes the secret key rate. The latter is depicted by insets of the white lines. In the region of $D = 1$ it is not possible to generate secret keys. Reprinted from **paper V**.

In addition, we also consider the concatenation of GKP qudits with quantum polynomial codes [150, 151, 152]. When using quantum error correcting codes with a fixed number of physical qudits there is a trade-off between the number of logical qudits and the code distance, formally expressed in the quantum Singleton bound [153]. While for qubits there

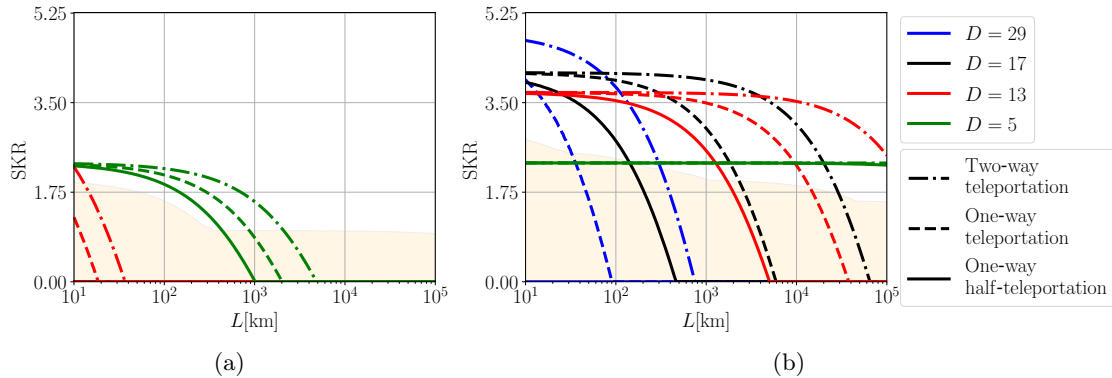


Figure 3.9: Comparison of the BB84 secret-key rate in dependence of the total transmission length with a repeater spacing $L_0 = 100\text{m}$ obtained by different quantum polynomial codes in combination with different error correction methods assuming GKP qudits with (a) 20 dB and (b) 30 dB of squeezing. The highlighted area shows secret-key rates obtainable with single GKP qudits with optimized dimension D and using the two-way scheme. Reprinted from **paper V**.

only exist one non-trivial code satisfying this bound with a code distance of at least 3, allowing for the correction of an arbitrary single-qubit error [154, 155], arbitrary large code distances satisfying the bound are possible when employing high dimensional qudits. Therefore, we employ quantum polynomial codes requiring a prime qudit dimension, because they achieve equality in the Singleton bound. We analyze the achievable secret-key rate for concatenated codes and find that they can achieve a better state quality resulting in a higher secret-key rate than optimized bare GKP codes. However, when taking the overhead of the high level code into account and choosing the secret-key rate per mode as the relevant metric, then the bare GKP codes result in better rates. In some other applications with a high required state fidelity it might be useful to employ these polynomial codes. The rather poor performance of the concatenation of GKP qudits with polynomial codes can be explained by the fact that increasing the qudit dimension of the GKP code decreases the spacing of the code words and the polynomial codes require rather high qudit dimensions. As a consequence one also obtains very demanding constraints on the squeezing parameter of the GKP states. Furthermore, we also calculate optimal repeater spacings and analyze when imperfect coupling efficiencies or finite squeezing of the GKP states dominate the overall noise.

Overall, we find that employing GKP qudits can be useful in principle, but then we need to employ experimentally unrealistic high amounts of squeezing in order to see an improvement in comparison to GKP qubits. Therefore, we can conclude that one should use GKP qubits instead of qudits in the foreseeable future.

4 Conclusion and outlook

In this thesis we followed two different approaches towards a quantum repeater either based on heralded entanglement distribution and quantum memories or solely based on quantum error correction.

Concerning the first approach we proposed a repeater protocol based on single-photon interference (**paper I**). In comparison to repeater schemes based on two-photon interference our scheme has the advantage of a much better loss scaling for the case when only photon loss is considered as the probability of not losing a single photon is much higher than not losing any of the two photons. However, this advantage comes at the cost of additional dephasing of the qubits. Thus, by varying an excitation parameter one trades between a high probability of success for distributing entanglement and a high state quality. Considering the loss-only case we found the optimal excitation value for QKD. Additionally, we also calculated secret-key rates for more realistic error models also involving memory dephasing, detector dark counts and phase mismatch in the state generation. Furthermore, it might be an interesting fundamental question whether it is possible to obtain a better loss-scaling with a memory-based quantum repeater for a fixed number of quantum memories than with our proposal by making use of multiple middle stations between two memories.

In another project (**paper II**) we calculated secret-key rates for different repeater protocols consisting of two segments using various experimental platforms (color centers, quantum dots, ions and atoms) whose parameters were reported in the Q.Link.X project. We found that with currently experimentally available parameters and employing a protocol where the memories are dephasing while waiting for classical communication signals, only the platform of rubidium atoms is barely able to overcome the PLOB bound. However, in order to cope with the low coherence times we also considered a second protocol which can make use of the higher source repetition as the memories do not have to wait for classical communication signals. Employing this protocol allows all platforms to overcome the PLOB bound, but such a protocol, that avoids all classical communication times, is not scalable to more than two segments. In future research schemes involving entanglement purification and small-scale quantum error correction should be investigated for these experimental platforms and it should be checked which platforms might be best suited for a possible proof-of-principle demonstration of such an advanced repeater scheme. Another open question is to which extent it is possible to make use of high clock rates for more than two segments in the context of QKD.

In addition we also performed an analysis of large-scale quantum repeaters without purification, but involving multiplexing (**paper IV**). We calculated the exact memory dephasing for different general repeater schemes. There, we found that optimal schemes should distribute entanglement in parallel, perform entanglement swapping as soon as possible and use parallel quantum storage as little as possible. We also calculated secret-key rates for repeaters of different number of segments and with different underlying processes for generating entanglement in each segment. We found that our proposal from **paper I** can lead to really high rates for low noise parameters, but because of the additional dephasing it may even become worse than schemes based on two-photon interference for more realistic noise parameters. Again it might be an interesting idea to also consider repeaters of the second generation. This might fit quite nicely in the framework of this work as the depolarizing and dephasing channels can be approximated as different depolarizing

4 Conclusion and outlook

and dephasing channels after error correction such that one simply has to replace α and μ by improved α_{eff} and μ_{eff} in the formulas. To some extent it might also be tractable to consider entanglement purification for small systems. However, for larger systems the schemes involving entanglement purification become rather complex such that it should be more feasible to consider Monte-Carlo simulations.

For the quantum repeater approach based on quantum error correction we considered GKP codes. First, we developed simpler methods for obtaining the GKP error syndrome information using linear optics, homodyne measurements and GKP ancillae (**paper III**). This is a simplification in comparison to canonical circuits which employ general Gaussian operations also involving squeezing operations instead of making only use of linear optics. We need slightly different GKP ancilla states modified by a Gaussian transformation. However, we have the advantage that this operation may be applied offline or even better simply incorporated in the GKP generation process. This process involves already non-linear optics and the modified GKP ancilla can be simply obtained by tuning a parameter in the state generation making the state generation not any harder. Thus, single-mode GKP states are only coupled via beam splitters which has the advantage of a simpler and better noise propagation. We generalized two linear-optical syndrome measurement schemes to the concatenation of GKP codes with high level codes and discuss when the required ancilla states can be obtained with linear optics and single-mode rectangular GKP states. This syndrome measurement scheme for the concatenation of GKP and an $[[n, k, d]]$ stabilizer code has the advantage of performing only $2n$ instead of $3n - k$ measurements, where each measurement typically consumes a single GKP state. Finally, we also used tools from lattice theory in order to calculate error rates exactly for the concatenation of square GKP codes with the three-qubit repetition code making use of the analog syndrome information. In this project we found multiple open questions for future research. First, it is a really relevant question whether the usage of the minimal set of measurements allows to reduce the noise threshold for quantum error correction because less noisy ancilla states are introduced in the syndrome measurement. A follow-up question arises in the context of generating the necessary multi-mode ancilla state. We already showed that it is impossible to generate such ancilla states with single-mode rectangular GKP states and linear optics. Is it any harder to produce the multi-mode ancilla state with GBS than it is to produce all of the individual GKP states with GBS? Another open question is for which codes it is possible to find rather simple expressions for the error rates when considering the analog syndrome information in the decoding process.

Finally, we apply these results to a repeater based on GKP qudits (**paper V**). We find that in principle it can be beneficial to employ GKP qudits with a dimension $D > 2$. However, this requires GKP states of really high quality such that in the near future it will be better to use GKP qubits only. It might also be an interesting question for which high-level qubit codes one can obtain the best rates in combination with GKP codes in a third-generation repeater. Another interesting question is whether it might be useful to consider GKP or other bosonic codes in the memories of a second-generation quantum repeater.

5 Bibliography

- [1] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, “Quantum supremacy using a programmable superconducting processor,” *Nature*, **574**, pp. 505–510, Oct 2019.
- [2] P. Jurcevic, A. Javadi-Abhari, L. S. Bishop, I. Lauer, D. F. Bogorin, M. Brink, L. Capelluto, O. Günlük, T. Itoko, N. Kanazawa, A. Kandala, G. A. Keefe, K. Kr-sulich, W. Landers, E. P. Lewandowski, D. T. McClure, G. Nannicini, A. Narasgond, H. M. Nayfeh, E. Pritchett, M. B. Rothwell, S. Srinivasan, N. Sundaresan, C. Wang, K. X. Wei, C. J. Wood, J.-B. Yau, E. J. Zhang, O. E. Dial, J. M. Chow, and J. M. Gambetta, “Demonstration of quantum volume 64 on a superconducting quantum computing system,” *Quantum Science and Technology*, **6**, p. 025020, mar 2021.
- [3] J. M. Arrazola, V. Bergholm, K. Brádler, T. R. Bromley, M. J. Collins, I. Dhand, A. Fumagalli, T. Gerrits, A. Goussev, L. G. Helt, J. Hundal, T. Isacsson, R. B. Israel, J. Izaac, S. Jahangiri, R. Janik, N. Killoran, S. P. Kumar, J. Lavoie, A. E. Lita, D. H. Mahler, M. Menotti, B. Morrison, S. W. Nam, L. Neuhaus, H. Y. Qi, N. Quesada, A. Repeatingon, K. K. Sabapathy, M. Schuld, D. Su, J. Swinarton, A. Száva, K. Tan, P. Tan, V. D. Vaidya, Z. Vernon, Z. Zabaneh, and Y. Zhang, “Quantum circuits with many photons on a programmable nanophotonic chip,” *Nature*, **591**, pp. 54–60, Mar 2021.
- [4] P. W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” *SIAM Journal on Computing*, **26**, no. 5, pp. 1484–1509, 1997.
- [5] D. J. Bernstein and T. Lange, “Post-quantum cryptography,” *Nature*, **549**, pp. 188–194, Sep 2017.
- [6] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, “Fundamental limits of repeaterless quantum communications,” *Nature Communications*, **8**, p. 15043, Apr 2017.
- [7] A. M. Childs, “Secure assisted quantum computation,” *Quantum Info. Comput.*, **5**, p. 456–466, sep 2005.
- [8] J. F. Fitzsimons, “Private quantum computation: an introduction to blind quantum computing and related protocols,” *npj Quantum Information*, **3**, p. 23, Jun 2017.

- [9] R. Jozsa, D. S. Abrams, J. P. Dowling, and C. P. Williams, “Quantum Clock Synchronization Based on Shared Prior Entanglement,” *Phys. Rev. Lett.*, **85**, pp. 2010–2013, Aug 2000.
- [10] P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin, “A quantum network of clocks,” *Nature Physics*, **10**, pp. 582–587, Aug 2014.
- [11] D. Gottesman, T. Jennewein, and S. Croke, “Longer-Baseline Telescopes Using Quantum Repeaters,” *Phys. Rev. Lett.*, **109**, p. 070503, Aug 2012.
- [12] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, “Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication,” *Phys. Rev. Lett.*, **81**, pp. 5932–5935, Dec 1998.
- [13] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, “Quantum communication without the necessity of quantum memories,” *Nature Photonics*, **6**, pp. 777–781, Nov 2012.
- [14] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, “Ultrafast and Fault-Tolerant Quantum Communication across Long Distances,” *Phys. Rev. Lett.*, **112**, p. 250501, Jun 2014.
- [15] F. Ewert, M. Bergmann, and P. van Loock, “Ultrafast Long-Distance Quantum Communication with Static Linear Optics,” *Phys. Rev. Lett.*, **117**, p. 210501, Nov 2016.
- [16] S. Muralidharan, C.-L. Zou, L. Li, J. Wen, and L. Jiang, “Overcoming erasure errors with multilevel systems,” *New Journal of Physics*, **19**, p. 013026, jan 2017.
- [17] S. Muralidharan, C.-L. Zou, L. Li, and L. Jiang, “One-way quantum repeaters with quantum Reed-Solomon codes,” *Phys. Rev. A*, **97**, p. 052316, May 2018.
- [18] D. Miller, T. Holz, H. Kampermann, and D. Bruß, “Parameter regimes for surpassing the PLOB bound with error-corrected qudit repeaters,” *Quantum*, **3**, p. 216, Dec. 2019.
- [19] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.
- [20] M. M. Wilde, *Quantum Information Theory*. Cambridge University Press, 2 ed., 2017.
- [21] A. S. Holevo, “Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel,” *Probl. Peredachi Inf.*, **9**, 1973.
- [22] A. Y. Kitaev, “Quantum computations: algorithms and error correction,” *Russian Mathematical Surveys*, **52**, pp. 1191–1249, dec 1997.
- [23] C. M. Dawson and M. A. Nielsen, “The Solovay-Kitaev Algorithm,” *Quantum Info. Comput.*, **6**, p. 81–95, jan 2006.
- [24] J. L. Park, “The concept of transition in quantum mechanics,” *Foundations of Physics*, **1**, pp. 23–33, Mar 1970.
- [25] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” *Nature*, **299**, pp. 802–803, Oct 1982.

- [26] W. F. Stinespring, “Positive Functions on C^* -Algebras,” *Proceedings of the American Mathematical Society*, **6**, pp. 211–216, 2022/03/29/ 1955. Full publication date: Apr., 1955.
- [27] D. Aharonov, A. Kitaev, and N. Nisan, “Quantum circuits with mixed states,” in *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC ’98, (New York, NY, USA), p. 20–30, Association for Computing Machinery, 1998.
- [28] A. Einstein, B. Podolsky, and N. Rosen, “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?,” *Phys. Rev.*, **47**, pp. 777–780, May 1935.
- [29] J. S. Bell, “On the Einstein Podolsky Rosen paradox,” *Physics Physique Fizika*, **1**, pp. 195–200, Nov 1964.
- [30] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, “Proposed Experiment to Test Local Hidden-Variable Theories,” *Phys. Rev. Lett.*, **23**, pp. 880–884, Oct 1969.
- [31] S. J. Freedman and J. F. Clauser, “Experimental Test of Local Hidden-Variable Theories,” *Phys. Rev. Lett.*, **28**, pp. 938–941, Apr 1972.
- [32] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, “Violation of Bell’s Inequality under Strict Einstein Locality Conditions,” *Phys. Rev. Lett.*, **81**, pp. 5039–5043, Dec 1998.
- [33] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, “Experimental violation of a Bell’s inequality with efficient detection,” *Nature*, **409**, pp. 791–794, Feb 2001.
- [34] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger, “Bell violation using entangled photons without the fair-sampling assumption,” *Nature*, **497**, pp. 227–230, May 2013.
- [35] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiiau, and R. Hanson, “Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres,” *Nature*, **526**, pp. 682–686, Oct 2015.
- [36] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, “Significant-Loophole-Free Test of Bell’s Theorem with Entangled Photons,” *Phys. Rev. Lett.*, **115**, p. 250401, Dec 2015.
- [37] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, “Strong Loophole-Free Test of Local Realism,” *Phys. Rev. Lett.*, **115**, p. 250402, Dec 2015.
- [38] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, “Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels,” *Phys. Rev. Lett.*, **80**, pp. 1121–1125, Feb 1998.

- [39] R. Ursin, T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther, and A. Zeilinger, “Quantum teleportation across the danube,” *Nature*, **430**, pp. 849–849, Aug 2004.
- [40] X.-M. Jin, J.-G. Ren, B. Yang, Z.-H. Yi, F. Zhou, X.-F. Xu, S.-K. Wang, D. Yang, Y.-F. Hu, S. Jiang, T. Yang, H. Yin, K. Chen, C.-Z. Peng, and J.-W. Pan, “Experimental free-space quantum teleportation,” *Nature Photonics*, **4**, pp. 376–381, Jun 2010.
- [41] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, “Quantum teleportation over 143 kilometres using active feed-forward,” *Nature*, **489**, pp. 269–273, Sep 2012.
- [42] H. Takesue, S. D. Dyer, M. J. Stevens, V. Verma, R. P. Mirin, and S. W. Nam, “Quantum teleportation over 100 km of fiber using highly efficient superconducting nanowire single-photon detectors,” *Optica*, **2**, pp. 832–835, Oct 2015.
- [43] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li, K.-X. Yang, X. Han, Y.-Q. Yao, J. Li, H.-Y. Wu, S. Wan, L. Liu, D.-Q. Liu, Y.-W. Kuang, Z.-P. He, P. Shang, C. Guo, R.-H. Zheng, K. Tian, Z.-C. Zhu, N.-L. Liu, C.-Y. Lu, R. Shu, Y.-A. Chen, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, “Ground-to-satellite quantum teleportation,” *Nature*, **549**, pp. 70–73, Sep 2017.
- [44] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, “Experimental Entanglement Swapping: Entangling Photons That Never Interacted,” *Phys. Rev. Lett.*, **80**, pp. 3891–3894, May 1998.
- [45] C. Gerry and P. Knight, *Introductory Quantum Optics*. Cambridge University Press, 2004.
- [46] P. Kok and B. W. Lovett, *Introduction to Optical Quantum Information Processing*. Cambridge University Press, 2010.
- [47] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, “Experimental realization of any discrete unitary operator,” *Phys. Rev. Lett.*, **73**, pp. 58–61, Jul 1994.
- [48] H. Vahlbruch, M. Mehmet, K. Danzmann, and R. Schnabel, “Detection of 15 dB Squeezed States of Light and their Application for the Absolute Calibration of Photoelectric Quantum Efficiency,” *Phys. Rev. Lett.*, **117**, p. 110801, Sep 2016.
- [49] R. Filip, P. Marek, and U. L. Andersen, “Measurement-induced continuous-variable quantum interactions,” *Phys. Rev. A*, **71**, p. 042308, Apr 2005.
- [50] S. L. Braunstein, “Squeezing as an irreducible resource,” *Physical Review A*, **71**, May 2005.
- [51] E. Wigner, “On the quantum correction for thermodynamic equilibrium,” *Phys. Rev.*, **40**, pp. 749–759, Jun 1932.
- [52] S. D. Bartlett, B. C. Sanders, S. L. Braunstein, and K. Nemoto, “Efficient classical simulation of continuous variable quantum information processes,” *Phys. Rev. Lett.*, **88**, p. 097904, Feb 2002.
- [53] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, “Invited review article: Single-photon sources and detectors,” *Review of scientific instruments*, **82**, no. 7, p. 071101, 2011.

- [54] L. You, “Superconducting nanowire single-photon detectors for quantum information,” *Nanophotonics*, **9**, no. 9, pp. 2673–2692, 2020.
- [55] E. Knill and R. Laflamme, “A Theory of Quantum Error-Correcting Codes,” 1996.
- [56] D. Gottesman, “The heisenberg representation of quantum computers,”
- [57] P. T. Cochrane, G. J. Milburn, and W. J. Munro, “Macroscopically distinct quantum-superposition states as a bosonic code for amplitude damping,” *Phys. Rev. A*, **59**, pp. 2631–2634, Apr 1999.
- [58] M. H. Michael, M. Silveri, R. T. Brierley, V. V. Albert, J. Salmilehto, L. Jiang, and S. M. Girvin, “New Class of Quantum Error-Correcting Codes for a Bosonic Mode,” *Phys. Rev. X*, **6**, p. 031006, Jul 2016.
- [59] D. Gottesman, A. Kitaev, and J. Preskill, “Encoding a qubit in an oscillator,” *Phys. Rev. A*, **64**, p. 012310, Jun 2001.
- [60] D. Gottesman, M. Devoret, D. DiVincenzo, and S. Girvin, “Frontiers in Bosonic Codes.” <https://www.youtube.com/watch?v=-BTKUe-5Boo>, 2020. Byron Bay Quantum Workshop 2020.
- [61] C. Flühmann, T. L. Nguyen, M. Marinelli, V. Negnevitsky, K. Mehta, and J. P. Home, “Encoding a qubit in a trapped-ion mechanical oscillator,” *Nature*, **566**, p. 513–517, Feb 2019.
- [62] P. Campagne-Ibarcq, A. Eickbusch, S. Touzard, E. Zalys-Geller, N. E. Frattini, V. V. Sivak, P. Reinhold, S. Puri, S. Shankar, R. J. Schoelkopf, L. Frunzio, M. Mirrahimi, and M. H. Devoret, “Quantum error correction of a qubit encoded in grid states of an oscillator,” *Nature*, **584**, pp. 368–372, Aug 2020.
- [63] B. de Neeve, T.-L. Nguyen, T. Behrle, and J. P. Home, “Error correction of a logical grid state qubit by dissipative pumping,” *Nature Physics*, Feb 2022.
- [64] A. Eickbusch, V. Sivak, A. Z. Ding, S. S. Elder, S. R. Jha, J. Venkatraman, B. Royer, S. M. Girvin, R. J. Schoelkopf, and M. H. Devoret, “Fast universal control of an oscillator with weak dispersive coupling to a qubit,” *Nature Physics*, **18**, pp. 1464–1469, Dec 2022.
- [65] V. V. Sivak, A. Eickbusch, B. Royer, S. Singh, I. Tsioutsios, S. Ganjam, A. Milano, B. L. Brock, A. Z. Ding, L. Frunzio, S. M. Girvin, R. J. Schoelkopf, and M. H. Devoret, “Real-time quantum error correction beyond break-even,” *Nature*, **616**, pp. 50–55, Apr 2023.
- [66] V. V. Albert, K. Noh, K. Duivenvoorden, D. J. Young, R. T. Brierley, P. Reinhold, C. Vuillot, L. Li, C. Shen, S. M. Girvin, B. M. Terhal, and L. Jiang, “Performance and structure of single-mode bosonic codes,” *Phys. Rev. A*, **97**, p. 032346, Mar 2018.
- [67] M. R. Kibler, “Variations on a theme of Heisenberg, Pauli and Weyl,” *Journal of Physics A: Mathematical and Theoretical*, **41**, p. 375302, aug 2008.
- [68] N. C. Menicucci, “Fault-Tolerant Measurement-Based Quantum Computing with Continuous-Variable Cluster States,” *Phys. Rev. Lett.*, **112**, p. 120504, Mar 2014.
- [69] T. Matsuura, H. Yamasaki, and M. Koashi, “Equivalence of approximate Gottesman-Kitaev-Preskill codes,” *Physical Review A*, **102**, Sep 2020.

- [70] B. Royer, S. Singh, and S. Girvin, “Stabilization of Finite-Energy Gottesman-Kitaev-Preskill States,” *Physical Review Letters*, **125**, Dec 2020.
- [71] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, “Mixed-state entanglement and quantum error correction,” *Phys. Rev. A*, **54**, pp. 3824–3851, Nov 1996.
- [72] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, “Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels,” *Phys. Rev. Lett.*, **76**, pp. 722–725, Jan 1996.
- [73] Y. Wang, “Quantum Error Correction with the GKP Code and Concatenation with Stabilizer Codes,” 2019.
- [74] J. Conrad, “Twirling and Hamiltonian engineering via dynamical decoupling for Gottesman-Kitaev-Preskill quantum computing,” *Phys. Rev. A*, **103**, p. 022404, Feb 2021.
- [75] K. Noh and C. Chamberland, “Fault-tolerant bosonic quantum error correction with the surface-Gottesman-Kitaev-Preskill code,” *Physical Review A*, **101**, Jan 2020.
- [76] C. Vuillot, H. Asasi, Y. Wang, L. P. Pryadko, and B. M. Terhal, “Quantum error correction with the toric Gottesman-Kitaev-Preskill code,” *Physical Review A*, **99**, Mar 2019.
- [77] L. Hänggeli, M. Heinze, and R. König, “Enhanced noise resilience of the surface-Gottesman-Kitaev-Preskill code via designed bias,” *Phys. Rev. A*, **102**, p. 052408, Nov 2020.
- [78] K. Fukui, A. Tomita, and A. Okamoto, “Analog Quantum Error Correction with Encoding a Qubit into an Oscillator,” *Phys. Rev. Lett.*, **119**, p. 180507, Nov 2017.
- [79] K. Noh, C. Chamberland, and F. G. Brandão, “Low-Overhead Fault-Tolerant Quantum Error Correction with the Surface-GKP Code,” *PRX Quantum*, **3**, Jan 2022.
- [80] N. Raveendran, N. Rengaswamy, F. Rozpędek, A. Raina, L. Jiang, and B. Vasić, “Finite Rate QLDPC-GKP Coding Scheme that Surpasses the CSS Hamming Bound,” *Quantum*, **6**, p. 767, July 2022.
- [81] E. Knill, R. Laflamme, and G. J. Milburn, “A scheme for efficient quantum computation with linear optics,” *Nature*, **409**, pp. 46–52, Jan 2001.
- [82] C. S. Hamilton, R. Kruse, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex, “Gaussian boson sampling,” *Phys. Rev. Lett.*, **119**, p. 170501, Oct 2017.
- [83] D. Su, C. R. Myers, and K. K. Sabapathy, “Conversion of Gaussian states to non-Gaussian states using photon-number-resolving detectors,” *Physical Review A*, **100**, Nov 2019.
- [84] I. Tzitrin, J. E. Bourassa, N. C. Menicucci, and K. K. Sabapathy, “Progress towards practical qubit computation using approximate Gottesman-Kitaev-Preskill codes,” *Physical Review A*, **101**, Mar 2020.
- [85] K. Fukui, S. Takeda, M. Endo, W. Asavanant, J.-i. Yoshikawa, P. van Loock, and A. Furusawa, “Efficient backcasting search for optical quantum state synthesis,” *Phys. Rev. Lett.*, **128**, p. 240503, Jun 2022.

- [86] N. Budinger, A. Furusawa, and P. van Loock, “All-optical quantum computing using cubic phase gates,” 2022.
- [87] J. Hastrup, K. Park, J. B. Brask, R. Filip, and U. L. Andersen, “Measurement-free preparation of grid states,” *npj Quantum Information*, **7**, p. 17, Jan 2021.
- [88] S. Wiesner, “Conjugate Coding,” *SIGACT News*, **15**, p. 78–88, Jan 1983.
- [89] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Theoretical Computer Science*, **560**, p. 7–11, Dec 2014.
- [90] D. Gottesman and H.-K. Lo, “Proof of security of quantum key distribution with two-way classical communications,” *IEEE Transactions on Information Theory*, **49**, no. 2, pp. 457–475, 2003.
- [91] G. Van Assche, “Quantum cryptography and secret-key distillation,” 2006.
- [92] H.-K. Lo, H. F. Chau, and M. Ardehali, “Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security,” *Journal of Cryptology*, **18**, pp. 133–165, Apr 2005.
- [93] D. Bruß, “Optimal Eavesdropping in Quantum Cryptography with Six States,” *Phys. Rev. Lett.*, **81**, pp. 3018–3021, Oct 1998.
- [94] L. Sheridan and V. Scarani, “Security proof for quantum key distribution using qudit systems,” *Phys. Rev. A*, **82**, p. 030301, Sep 2010.
- [95] M. Pawłowski, “Security proof for cryptographic protocols based only on the monogamy of bell’s inequality violations,” *Phys. Rev. A*, **82**, p. 032313, Sep 2010.
- [96] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, “Entanglement-based quantum communication over 144 km,” *Nature Physics*, **3**, pp. 481–486, Jul 2007.
- [97] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, “Satellite-based entanglement distribution over 1200 kilometers,” *Science*, **356**, no. 6343, pp. 1140–1144, 2017.
- [98] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, “Experimental Quantum Key Distribution with Decoy States,” *Phys. Rev. Lett.*, **96**, p. 070502, Feb 2006.
- [99] Y. Zhao, B. Qi, X. Ma, H.-k. Lo, and L. Qian, “Simulation and Implementation of Decoy State Quantum Key Distribution over 60km Telecom Fiber,” in *2006 IEEE International Symposium on Information Theory*, pp. 2094–2098, 2006.
- [100] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, “Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber,” *Phys. Rev. Lett.*, **98**, p. 010503, Jan 2007.

- [101] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, “Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km,” *Phys. Rev. Lett.*, **98**, p. 010504, Jan 2007.
- [102] W.-Y. Hwang, “Quantum Key Distribution with High Loss: Toward Global Secure Communication,” *Phys. Rev. Lett.*, **91**, p. 057901, Aug 2003.
- [103] X.-B. Wang, “Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography,” *Phys. Rev. Lett.*, **94**, p. 230503, Jun 2005.
- [104] H. Wang, Y. Li, Y. Pi, Y. Pan, Y. Shao, L. Ma, Y. Zhang, J. Yang, T. Zhang, W. Huang, and B. Xu, “Sub-gbps key rate four-state continuous-variable quantum key distribution within metropolitan area,” *Communications Physics*, **5**, p. 162, Jun 2022.
- [105] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, J. F. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields, “10-Mb/s Quantum Key Distribution,” *Journal of Lightwave Technology*, **36**, no. 16, pp. 3427–3433, 2018.
- [106] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, “Attacks on practical quantum key distribution systems (and how to prevent them),” *Contemporary Physics*, **57**, no. 3, pp. 366–387, 2016.
- [107] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, “Secure quantum key distribution with realistic devices,” *Rev. Mod. Phys.*, **92**, p. 025002, May 2020.
- [108] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, and J.-W. Pan, “An integrated space-to-ground quantum communication network over 4,600 kilometres,” *Nature*, **589**, pp. 214–219, Jan 2021.
- [109] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters,” *Nature*, **557**, pp. 400–403, May 2018.
- [110] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, “Twin-field quantum key distribution with large misalignment error,” *Phys. Rev. A*, **98**, p. 062323, Dec 2018.
- [111] X. Ma, P. Zeng, and H. Zhou, “Phase-Matching Quantum Key Distribution,” *Phys. Rev. X*, **8**, p. 031043, Aug 2018.
- [112] M. Curty, K. Azuma, and H.-K. Lo, “Simple security proof of twin-field type quantum key distribution protocol,” *npj Quantum Information*, **5**, p. 64, Jul 2019.
- [113] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, “Twin-Field Quantum Key Distribution without Phase Postselection,” *Phys. Rev. Applied*, **11**, p. 034053, Mar 2019.
- [114] J. Lin and N. Lütkenhaus, “Simple security analysis of phase-matching measurement-device-independent quantum key distribution,” *Phys. Rev. A*, **98**, p. 042332, Oct 2018.

- [115] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, “Experimental quantum key distribution beyond the repeaterless secret key capacity,” *Nature Photonics*, **13**, pp. 334–338, May 2019.
- [116] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, “Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System,” *Phys. Rev. X*, **9**, p. 021046, Jun 2019.
- [117] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, “Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution,” *Phys. Rev. Lett.*, **123**, p. 100506, Sep 2019.
- [118] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, “Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending,” *Phys. Rev. Lett.*, **123**, p. 100505, Sep 2019.
- [119] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, “Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km,” *Phys. Rev. Lett.*, **124**, p. 070501, Feb 2020.
- [120] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, Z. Wang, L. You, M.-J. Li, H. Chen, Y.-A. Chen, Q. Zhang, C.-Z. Peng, X. Ma, T.-Y. Chen, and J.-W. Pan, “Implementation of quantum key distribution surpassing the linear rate-transmittance bound,” *Nature Photonics*, **14**, pp. 422–425, Jul 2020.
- [121] H. Liu, C. Jiang, H.-T. Zhu, M. Zou, Z.-W. Yu, X.-L. Hu, H. Xu, S. Ma, Z. Han, J.-P. Chen, Y. Dai, S.-B. Tang, W. Zhang, H. Li, L. You, Z. Wang, Y. Hua, H. Hu, H. Zhang, F. Zhou, Q. Zhang, X.-B. Wang, T.-Y. Chen, and J.-W. Pan, “Field Test of Twin-Field Quantum Key Distribution through Sending-or-Not-Sending over 428 km,” *Phys. Rev. Lett.*, **126**, p. 250502, Jun 2021.
- [122] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, “Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas,” *Nature Photonics*, **15**, pp. 570–575, Aug 2021.
- [123] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, “600-km repeater-like quantum communications with dual-band stabilization,” *Nature Photonics*, **15**, pp. 530–535, Jul 2021.
- [124] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, “Twin-field quantum key distribution over 830-km fibre,” *Nature Photonics*, **16**, pp. 154–161, Feb 2022.
- [125] K. Boone, J.-P. Bourgoin, E. Meyer-Scott, K. Heshami, T. Jennewein, and C. Simon, “Entanglement over global distances via quantum repeaters with satellite links,” *Phys. Rev. A*, **91**, p. 052325, May 2015.

- [126] J. Calsamiglia and N. Lütkenhaus, “Maximum efficiency of a linear-optical bell-state analyzer,” *Applied Physics B*, **72**, pp. 67–71, Jan 2001.
- [127] F. Schmidt and P. van Loock, “Memory-assisted long-distance phase-matching quantum key distribution,” *Phys. Rev. A*, **102**, p. 042614, Oct 2020.
- [128] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, “Concentrating partial entanglement by local operations,” *Phys. Rev. A*, **53**, pp. 2046–2052, Apr 1996.
- [129] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, “Quantum repeaters based on entanglement purification,” *Phys. Rev. A*, **59**, pp. 169–181, Jan 1999.
- [130] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, “Long-distance quantum communication with atomic ensembles and linear optics,” *Nature*, **414**, pp. 413–418, Nov 2001.
- [131] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, “Hybrid Quantum Repeater Using Bright Coherent Light,” *Phys. Rev. Lett.*, **96**, p. 240501, Jun 2006.
- [132] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, “Optimal architectures for long distance quantum communication,” *Scientific Reports*, **6**, p. 20463, Feb 2016.
- [133] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, “Quantum repeater with encoding,” *Phys. Rev. A*, **79**, p. 032325, Mar 2009.
- [134] N. K. Bernardes and P. van Loock, “Hybrid quantum repeater with encoding,” *Physical Review A*, **86**, Nov 2012.
- [135] P. van Loock, N. Lütkenhaus, W. J. Munro, and K. Nemoto, “Quantum repeaters using coherent-state communication,” *Phys. Rev. A*, **78**, p. 062319, Dec 2008.
- [136] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin, “Experimental demonstration of memory-enhanced quantum communication,” *Nature*, **580**, pp. 60–64, Apr 2020.
- [137] S. Langenfeld, P. Thomas, O. Morin, and G. Rempe, “Quantum repeater node demonstrating unconditionally secure key distribution,” *Phys. Rev. Lett.*, **126**, p. 230506, Jun 2021.
- [138] F. Rozpędek, K. Noh, Q. Xu, S. Guha, and L. Jiang, “Quantum repeaters based on concatenated bosonic and discrete-variable quantum codes,” *npj Quantum Information*, **7**, p. 102, Jun 2021.
- [139] K. Fukui, R. N. Alexander, and P. van Loock, “All-optical long-distance quantum communication with Gottesman-Kitaev-Preskill qubits,” *Physical Review Research*, **3**, Aug 2021.
- [140] K. Xia, “Quantum Non-Demolition Measurement of Photons,” in *Photon Counting* (N. Britun and A. Nikiforov, eds.), ch. 3, Rijeka: IntechOpen, 2018.
- [141] E. Knill, “Quantum computing with realistically noisy devices,” *Nature*, **434**, pp. 39–44, Mar 2005.

- [142] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, “Bell measurements for teleportation,” *Phys. Rev. A*, **59**, pp. 3295–3300, May 1999.
- [143] F. Schmidt and P. van Loock, “Efficiencies of logical Bell measurements on Calderbank-Shor-Steane codes with static linear optics,” *Physical Review A*, **99**, Jun 2019.
- [144] S.-W. Lee, T. C. Ralph, and H. Jeong, “Fundamental building block for all-optical scalable quantum networks,” *Phys. Rev. A*, **100**, p. 052303, Nov 2019.
- [145] F. Ewert and P. van Loock, “Ultrafast fault-tolerant long-distance quantum communication with static linear optics,” *Phys. Rev. A*, **95**, p. 012327, Jan 2017.
- [146] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, “Quantum repeaters based on atomic ensembles and linear optics,” *Rev. Mod. Phys.*, **83**, pp. 33–80, Mar 2011.
- [147] E. Shchukin, F. Schmidt, and P. van Loock, “Waiting time in quantum repeaters with probabilistic entanglement swapping,” *Phys. Rev. A*, **100**, p. 032322, Sep 2019.
- [148] B. W. Walshe, B. Q. Baragiola, R. N. Alexander, and N. C. Menicucci, “Continuous-variable gate teleportation and bosonic-code error correction,” *Physical Review A*, **102**, Dec 2020.
- [149] K. Chandrasekaran, V. Gandikota, and E. Grigorescu, “Deciding orthogonality in construction-a lattices,” *SIAM Journal on Discrete Mathematics*, **31**, no. 2, pp. 1244–1262, 2017.
- [150] R. Cleve, D. Gottesman, and H.-K. Lo, “How to Share a Quantum Secret,” *Phys. Rev. Lett.*, **83**, pp. 648–651, Jul 1999.
- [151] D. Aharonov and M. Ben-Or, “Fault-Tolerant Quantum Computation with Constant Error Rate,” *SIAM Journal on Computing*, **38**, no. 4, pp. 1207–1282, 2008.
- [152] A. Ketkar, A. Klappenecker, S. Kumar, and P. Sarvepalli, “Nonbinary Stabilizer Codes Over Finite Fields,” *IEEE Transactions on Information Theory*, **52**, no. 11, pp. 4892–4914, 2006.
- [153] E. Rains, “Nonbinary quantum codes,” *IEEE Transactions on Information Theory*, **45**, no. 6, pp. 1827–1832, 1999.
- [154] M. Grassl and M. Rötteler, “Quantum MDS codes over small fields,” in *2015 IEEE International Symposium on Information Theory (ISIT)*, pp. 1104–1108, 2015.
- [155] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, “Perfect Quantum Error Correcting Code,” *Phys. Rev. Lett.*, **77**, p. 198, Jul 1996.
- [156] S. Glancy and E. Knill, “Error analysis for encoding a qubit in an oscillator,” *Physical Review A*, **73**, Jan 2006.
- [157] K. H. Wan, A. Neville, and S. Kolthammer, “Memory-assisted decoder for approximate Gottesman-Kitaev-Preskill codes,” *Phys. Rev. Research*, **2**, p. 043280, Nov 2020.

6 Publications

Contribution to publications

The initial idea of **paper I** arose when Peter van Loock asked me to investigate whether it would be possible to somehow combine the improved distance scaling of the secret-key rate of TF QKD with the improved scaling from a memory-based quantum repeater. While first approaching the problem with the general framework of QKD using the Holevo information in order to bound Eve’s obtained information, I soon realized that the obtained secret-key fraction looked very similar to the secret-key fraction in a BB84 protocol and found that one can interpret the scheme as a simple application of the BB84 protocol to some quantum repeater. All calculations and choices of error models required for the analysis of the quantum repeater secret-key rate were done completely by myself. However, the idea to improve the secret-key rate per second by choosing asymmetric positions of the beams splitter was proposed by Peter van Loock. When writing the paper he helped me improving the style and also wrote the paragraph about the experiment performed in the group of Gerhard Rempe which could be used to generate the required states.

Paper II gives an overview about the progress achieved in the experiments of the project “Q.Link.X” and shows where they stand on their path to a functioning quantum repeater. Originally, it was planned to only calculate the raw rate of a protocol with some worst-case fidelity given by a memory cut-off. I suggested to additionally calculate the expected state instead of the worst-case scenario by making use of the results obtained in **paper I**. Thus, I performed all of the calculations and generated the plots. Furthermore, during discussions between Peter van Loock and me we had the idea to consider different memory write-in proposals as e.g. a local Bell measurement in order to herald the memory write-in. In addition, Appendix S2 was also written completely by myself.

When learning about GKP codes I read Ref. [156] and noticed that although they simplified the circuit to obtain the error syndrome, it was still possible to get rid of the in-line squeezing operation when considering syndrome measurements in both quadratures.¹ This inspired me to investigate for which other GKP codes it is also possible to employ only off-line squeezing operations in order to gain the syndrome information which is the main content of **paper III**. Especially with regard to **paper V** I got interested in Bell measurements for general GKP qudits and found that by using Knill’s error correction by teleportation it is possible to obtain the whole error syndrome of an n -qudit code concatenated with a GKP code with only $2n$ measurements. In a discussion then Peter van Loock had the idea that any GKP qubit state can be represented by only $2n$ stabilizers because otherwise there is some redundancy. Later I generalized this result to qudits using a lattice-based approach. All other results in this paper were obtained without Peter van Loock’s help, but he again helped me with stylistic improvements of the paper.

My main contributions to **paper IV** are the following:

The application of the memory dephasing expectation values to the different physical implementations where we consider dual-rail encoded qubits, the scheme introduced in **paper**

¹This was also noticed in Ref. [157] a long time before **paper III** was published, but after my observation.

I and a similar scheme also based on single-photon interference (section H/App. I). When we numerically found out that there are minimal values of μ which need to be achieved by the repeater in order to allow for a non-zero secret-key rate, I showed that this is not an effect arising from an interplay between different occurring errors, but it is a simple fundamental property of the chosen QKD protocol (Sec. 5.D). In addition, I also had the idea for the rule of thumb in Sec. 5.F. For sequential entanglement distribution I proposed to improve the coherence time by a factor 2 by performing the QKD measurements immediately and I showed that when using a cut-off protocol it is better to use individual cut-off values for each segment instead of a single global one, which only aborts the protocol when the accumulated dephasing overcomes the global cut-off. Of course, I also was involved in other parts of the paper, but there the work was done jointly with the other authors such that an exact attribution of contribution is not really possible. This applies especially to writing the paper and performing calculations and double checking in App. E.

The rough idea of **paper V** was developed at the 1. DPG fall meeting (2019) where I met Daniel Miller, who gave a talk about third-generation repeaters employing multi-mode/Fock encoded qudits in combination with quantum polynomial codes. We thought that it would be a nice idea to generalize his analysis also towards GKP qudits as they would allow for rather simple measurements which were a rather unfeasible in his previous proposals. In this project he had the background in the quantum polynomial codes and I brought the expertise in GKP codes. For this paper we discussed the general outline together. Regarding the code we wrote, he converted some code from his previous repeater from C++ to python and I was in charge of writing the remaining functions and performing the calculations and finding simple adaptations of the general protocols for GKP codes. Furthermore, I generated all figures, while he helped a lot improving the style of the text.

Paper I


Memory-assisted long-distance phase-matching quantum key distribution

Frank Schmidt and Peter van Loock

Phys. Rev. A **102**, 042614 (2020)

Memory-assisted long-distance phase-matching quantum key distribution

Frank Schmidt* and Peter van Loock†

Institute of Physics, Johannes Gutenberg-Universität Mainz, Staudingerweg 7, 55128 Mainz, Germany (Received 28 October 2019; revised 30 August 2020; accepted 16 September 2020; published 26 October 2020)

We propose a scheme that generalizes the loss scaling properties of twin-field or phase-matching quantum key distribution (QKD) related to a channel of transmission η_{total} from $\sqrt{\eta_{\text{total}}}$ to $\sqrt[n]{\eta_{\text{total}}}$ by employing $n - 1$ memory stations with spin qubits and n beam-splitter stations including optical detectors. Our scheme's resource states are similar to the coherent-state-based light-matter entangled states of a previous hybrid quantum repeater, but unlike the latter our scheme avoids the necessity of employing $2n - 1$ memory stations and writing the transmitted optical states into the matter memory qubits. The full scaling advantage of this memory-assisted phase-matching QKD (MA-PM QKD) is obtainable with threshold detectors in a scenario with only channel loss. We mainly focus on the obtainable secret-key rates per channel use for up to $n = 4$ including memory dephasing and for $n = 2$ (i.e., $\sqrt[n]{\eta_{\text{total}}}$ -MA-PM QKD assisted by a single memory station) for error models including dark counts, memory dephasing and depolarization, and phase mismatch. By combining the twin-field concept of interfering phase-sensitive optical states with that of storing quantum states up to a cutoff memory time, distances well beyond 700 km with rates well above η_{total} can be reached for realistic, high-quality quantum memories (up to 1-s coherence time) and modest detector efficiencies. Similarly, the standard single-node quantum repeater, scaling as $\sqrt{\eta_{\text{total}}}$, can be beaten when approaching perfect detectors and exceeding spin coherence times of 5 s; beating ideal twin-field QKD requires 1 s. As for further experimental simplifications, our treatment includes the notion of weak nonlinearities for the light-matter states, a discussion on the possibility of replacing the threshold by homodyne detectors, and a comparison between sequential and parallel entanglement distributions.

DOI: [10.1103/PhysRevA.102.042614](https://doi.org/10.1103/PhysRevA.102.042614)**I. INTRODUCTION**

In 1984, Bennett and Brassard presented a protocol (BB84) [1] that allows two parties (typically referred to as Alice and Bob) to distribute an information-theoretically secure key exploiting the fundamental laws of quantum mechanics. This was the beginning of the new field of quantum key distribution (QKD), leading now to the first commercial applications of quantum technology (see Ref. [2] for a recent overview of QKD). Based on this concept, a key distribution scheme over 421 km of glass fiber was demonstrated recently [3]. Nonetheless, a complication of realistic QKD schemes is the linear scaling of the secret-key rate with the channel transmittance η_{total} [4], where η_{total} decreases exponentially with the distance, $\eta_{\text{total}} = \exp(-L/L_{\text{att}})$, where $L_{\text{att}} = 22$ km is the typical attenuation distance of an optical fiber. In fact, it was shown that this linear scaling for large distances is a fundamental property of point-to-point QKD, expressed by the so-called repeaterless (or PLOB) bound [5], $-\log_2(1 - \eta_{\text{total}})$, in terms of secret bits per channel use, where $-\log_2(1 - \eta_{\text{total}}) \approx 1.44\eta_{\text{total}}$ for $\eta_{\text{total}} \ll 1$.

As a consequence, one needs to split the total channel into multiple segments of smaller lengths in order to overcome the linear scaling. Splitting the total distance into multiple segments of smaller length is the underlying idea of all types of quantum repeaters making use of either quantum memories [6,7], quantum error-correcting codes [8–11], or both

in order to improve the transmission rate. Because of the quantum mechanical no-cloning theorem, it is impossible that a quantum repeater simply reamplifies an incoming optical quantum state at every intermediate station along the channel like for a classical repeater with classical light pulses. The only experimental demonstration of a quantum repeater so far overcoming the PLOB bound in terms of a secret key rate per channel use was reported recently in Ref. [12] based on a solid-state light-matter interface and memory system using SiV color centers in diamond.

Besides its scalability, an essential element of a QKD scheme is its security in a realistic setting. More than a decade ago, it was shown that QKD systems are vulnerable to hacking attacks (see Refs. [13,14] for a review) and it was realized that the typical assumptions of the security proofs are not met in a practical implementation. Device-independent QKD [15,16] was proposed as a possible solution. Its security proof no longer depends on the actual implementation, since it relies on the violation of a Bell inequality. However, this type of protocol yields only very small secret-key rates. A more promising approach in this respect is measurement-device-independent (MDI) QKD [17,18], where Alice and Bob send states to a middle station, Charlie, who performs a measurement that can be treated as a black box. As such, the middle station may be completely untrusted, with Charlie potentially embodied by an eavesdropper, Eve. This approach becomes secure against the most problematic class of detector attacks and yields reasonable secret-key rates.

Quite recently it was shown that MDI QKD, exploiting interference of phase-sensitive phase-encoded optical states sent from Alice and Bob to Charlie, gives a scaling of the

*fschmi@students.uni-mainz.de

†loock@uni-mainz.de

asymptotic secret-key rate of $O(\sqrt{\eta_{\text{total}}})$ [19], originally named as twin-field QKD. Many works have now appeared improving or simplifying the security proof and suggesting variations of this protocol [20–26]. For the present work, especially relevant is the version referred to as phase-matching QKD [20,22]. Therefore, it is possible, in principle, to overcome the PLOB bound [5] without making use of quantum memories or quantum error-correcting codes. There are already first experimental demonstrations of twin-field QKD that claim to have overcome the PLOB bound [27–31].

In this work, we introduce a scheme that is an extension of the twin-field/phase-matching protocol to more than two physical segments (i.e., beyond a single middle station), exploiting quantum memories similar to Ref. [32] and further extending a four-segment variant of Ref. [32], but with single-photon-based single-rail (single-mode) qubits replaced by coherent states. Our scheme makes use of quantum memories, a kind of memory-assisted extension of phase-matching QKD [20,22], and thus is ideally, with sufficiently good memories and operations, in principle scalable to long distances. The scheme shares similarities with a hybrid quantum repeater (HQR) [33] where an optical coherent state subsequently interacts with two spin-based matter quantum memories and entangles these two spin qubits after a suitable measurement of the optical mode. However, in the original HQR, the optical mode travels all the way from one memory station to another before its detection at that station. In our scheme, crucially, there will be a middle station, halfway between the memories, equipped with a beam splitter and detectors. This way we will be able to generalize the loss scaling behavior of twin-field/phase-matching QKD from an effective channel length of $\frac{L}{2}$ to $\frac{L}{2n}$ for $2n$ physical segments and a total physical channel of length L with only $n - 1$ memory stations. We find that compared with the original HQR based on unambiguous state discrimination [34], the new MA-PM QKD scheme leads to a scaling advantage where in all relevant quantities η (transmittance per repeater segment) becomes $\sqrt{\eta}$. While our scheme could be supplemented by additional quantum error correction or detection mechanisms such as entanglement purification [6,33,35], here we shall consider the theoretically and especially experimentally simplest intermediate-scale versions without error correction.

The outline of our paper is as follows. In Sec. II, we will briefly introduce the main ideas of twin-field/phase-matching QKD, the HQR, and possibilities for generating the entangled states needed for our scheme. In Sec. III, we will then describe our version of a type of HQR and discuss its obtainable secret-key rate by employing a BB84 protocol and focusing on the channel-loss-only case. For the more general and realistic situation, we will briefly mention different error models including channel loss, memory dephasing, detector dark counts, phase mismatch, and depolarization, referring to the Appendixes for details. We will also briefly describe a variant of our scheme based on optical homodyne measurements, similar to the original HQR [33]. Then we will explicitly calculate the attainable secret-key rates in Sec. IV for the first-order generalization (i.e., four physical segments, $n = 2$) considering a fairly large and representative set of realistic parameters. Although our main focus is on secret-key rates per channel use, we will also include a discussion on the usefulness of our scheme in terms

of the ultimate figure of merit, the secret-key rate per second. We conclude in Sec. V and give more details about the basic concepts, assumptions, and calculations in the Appendixes.

II. BACKGROUND

A. Twin-field/phase-matching QKD

There are many different variations of twin-field QKD [19–26] and we will stick to the version in Ref. [20], since that protocol is conceptually easy to understand and very similar to the generalized scheme that we will introduce:

(1) Alice and Bob choose randomly and independent from each other with a probability p_{mode} if the current round is used for key generation or for estimating information leakage (test mode).

(2) If the key-generation mode is chosen, Alice (Bob) generate uniformly distributed random bits k_A (k_B) and send coherent states with amplitude $\alpha e^{i\pi k_{A/B}}$ to an untrusted middle station called Charlie (Alice and Bob pre-agreed upon an α). If the test mode is chosen, they generate coherent states of an amplitude according to some fixed probability distribution and send the optical states to the middle station.

(3) If Charlie is honest, he applies a balanced beam splitter (BS) to Alice's and Bob's optical modes and employs threshold (on-off) detectors for the BS output modes, announcing the measurement results. These steps are repeated until a long data set is obtained. If Alice and Bob use the key-generation mode and exactly one of the two detectors clicks, k_a and k_b are perfectly (assuming no dark counts) (anti)correlated depending on which of the two detectors clicked. In our scheme, the level of security of these (anti)correlations that manifests itself in the quality of the randomly phase-flipped entangled (effective) density operator shared by Alice and Bob will depend on the channel transmission, the overlap of the coherent states, and the type of detectors (we shall also consider photon-number resolving detectors, PNRDs).

(4) The usual QKD steps of sifting, estimating the error rate and leaked information, error correction, and privacy amplification need to be performed.

Note that a pre-agreed complex amplitude α implies that Alice's and Bob's lasers should not differ in their phase. However, it is also unreasonable to assume that the optical path length between Alice and Charlie perfectly coincides with that of Bob and Charlie. Therefore, it is necessary to stabilize Alice's and Bob's laser frequencies and also apply phase-stabilization techniques because of the phase drift in the fiber of the communication channel. This extra experimental complication in a twin-field/phase-matching QKD scheme is the price to pay for the scaling gain, $\eta_{\text{total}} \rightarrow \sqrt{\eta_{\text{total}}}$.

Since the untrusted Charlie (who could always be Eve) performs the measurements, the protocol is a MDI protocol [17,18], meaning that we are immune to attacks upon the detectors, which seems to be the most vulnerable part in a QKD system.

B. Hybrid quantum repeater

Each segment of a so-called HQR consists of two quantum memories placed at its ends [33] and connected by an optical channel. Each quantum memory is represented by a two-level

spin system which is initially in the state $\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$. We will consider a light-matter interaction between each memory and a single-mode coherent state of light such that

$$\hat{U}_{\text{int}}(\theta)(|\uparrow\rangle + |\downarrow\rangle)|\alpha\rangle = |\uparrow\rangle|\alpha e^{-i\theta}\rangle + |\downarrow\rangle|\alpha e^{i\theta}\rangle. \quad (1)$$

Thus, the coherent-state light amplitude is phase-rotated conditioned upon the state of the spin. We call the result of this interaction a hybrid entangled state and there exist different physical phenomena for obtaining this transformation. An attractive feature here is that we may even consider a fairly weak interaction, $\theta \ll 1$. A few more details about these interactions will be given in the next subsection.

First, we let one memory interact with the optical mode, which is then sent to the other memory at the next repeater station where we again apply the light-matter interaction. This results, in the absence of channel loss, in the (normalized) state

$$\frac{(|\uparrow, \downarrow\rangle + |\downarrow, \uparrow\rangle)|\alpha\rangle + |\uparrow, \uparrow\rangle|\alpha e^{-2i\theta}\rangle + |\downarrow, \downarrow\rangle|\alpha e^{2i\theta}\rangle}{2}. \quad (2)$$

By discriminating the $\pm 2\theta$ phase shifts from the zero phase shift, we can project the two memories onto an entangled Bell state $|\uparrow, \downarrow\rangle + |\downarrow, \uparrow\rangle$. Such a discrimination can be performed, for example, by using quadrature homodyne measurements. In the following, let us assume that $\alpha \in \mathbb{R}^+$. Then we could discriminate the phase shifts by performing a measurement of the momentum quadrature $\hat{p} := \frac{1}{2i}(\hat{a} - \hat{a}^\dagger)$, where \hat{a} and \hat{a}^\dagger are bosonic annihilation and creation operators. We can then choose a sufficiently small Δ_p and if the measurement outcome $p \in [-\Delta_p, \Delta_p]$, we say that we successfully identified a zero phase shift. However, this is not an exact projection onto a Bell state and the fidelity of the state is a function of the measured value p and $\alpha \sin(2\theta)$, i.e., $2\alpha\theta$ for small θ . We could improve the fidelity at the expense of the success probability by choosing a smaller Δ_p , which means that we are discarding many low-quality states. Alternatively, we could also set Δ_p to a fixed value and increase $\alpha \sin(2\theta)$; however, we cannot increase this value arbitrarily much as soon as the photon loss of the fiber channel is included, since a larger value leads to more decoherence due to the loss. Therefore, one has to find a compromise between average fidelity and raw rate. For small θ , the probability of success and the fidelity are only dependent on the transmittance η in the repeater segment and on $\alpha\theta$. One may also consider different measurements on the optical mode such as unambiguous state discrimination based on PNRDs or on-off detectors [34]. While in our work we discuss both types of measurements, discrete photon and continuous homodyne (Appendixes F and H) detections, the former allow us to entirely suppress discrimination errors even for small $\alpha\theta$, and thus longer repeater segments are possible. Later, we will compare our scheme with a HQR based on unambiguous state discrimination using on-off detectors.

C. Generation of hybrid entangled states

States of the form $|\uparrow\rangle|\alpha e^{-i\theta}\rangle + |\downarrow\rangle|\alpha e^{i\theta}\rangle$ are also known as Schrödinger cat states, because for large amplitudes of the coherent state they serve as an example of entanglement between a microscopic object like an atom and a macroscopic object like a strong optical field, exactly like in Schrödinger's famous

thought experiment [36]. In order to realize this in the laboratory, large efforts have been made to generate these states. Mostly the entanglement was generated between the internal state of an atom or ion and its motional degree of freedom, or with microwave radiation [37–39]. A few other experiments with atom-induced phase shifts were realized for electromagnetic radiation in the optical frequency domain [40,41].

We will briefly discuss two different approaches for generating these states. A general advantage of the corresponding physical platform, namely cavity QED with atoms and light, is that it allows for room-temperature operations at optical frequencies, as opposed to solid-state-based approaches such as that of Ref. [12] where sufficient cooling is a necessity. One possible approach considers the interaction of light (for a coherent state with amplitude α) with a two-level atom (Jaynes-Cummings model [42] of cavity QED) where the light frequency is largely detuned from the atomic resonance frequency. The effective interaction Hamiltonian is then given by

$$\hat{H}_{\text{eff}} = \hbar \frac{g^2}{\delta} (\hat{\sigma}_+ \hat{\sigma}_- + \hat{a}^\dagger \hat{a} \hat{\sigma}_z), \quad (3)$$

in the regime of large detuning δ (see, for example, Ref. [42]). Here, g denotes the coupling constant, $\hat{\sigma}_\pm$ are atomic transition operators, and $\hat{\sigma}_z$ is the Pauli-Z operator. This interaction Hamiltonian results (up to some phase, which can be compensated easily) in the desired state, equivalent to applying the operator $\hat{U}_{\text{int}}(\theta)$ with $\theta = \hbar \frac{g^2}{\delta} \alpha^2 t_{\text{int}}$, where t_{int} denotes the interaction time. However, it is demanding to achieve a sufficiently strong nonlinear interaction corresponding to a θ of the order of $\frac{\pi}{2}$. Therefore, here we shall also consider the case where θ is small (corresponding to a weak nonlinear interaction), similar to the analysis in Ref. [33].

A different approach was considered in the recent experiment of Ref. [43], where a resonant light-atom interaction was employed in a cavity. More precisely, in this case the internal state of an atom determines whether a light mode initially in a coherent state couples with the cavity. In one atomic state (uncoupled with the cavity), the cavity mode and the incoming light pulse are on resonance such that the light will enter the cavity and experience a π -phase shift after leaving it again. In the other atomic state coupled with the cavity, the effective cavity mode is no longer on resonance with the incoming pulse. In this case, the light will not enter the cavity and immediately be reflected back directly by the cavity mirror with no resulting phase shift. As a consequence, an atomic superposition state leads to a state for the reflected pulse that is entangled with the atom, similar to Eq. (1), with a phase difference of π for the two coherent states. Therefore, in this case it is also possible to obtain $\theta = \frac{\pi}{2}$.

III. MEMORY-ASSISTED PHASE-MATCHING QKD PROTOCOL

A. Description of the protocol

Let us start by describing the smallest example of our version of a HQR, which is very similar to an entanglement-based description of phase-matching QKD [see Figs. 1(a) and 1(b)].

(1) Alice and Bob each have an atom as a quantum memory and generate a hybrid entangled state between their memory

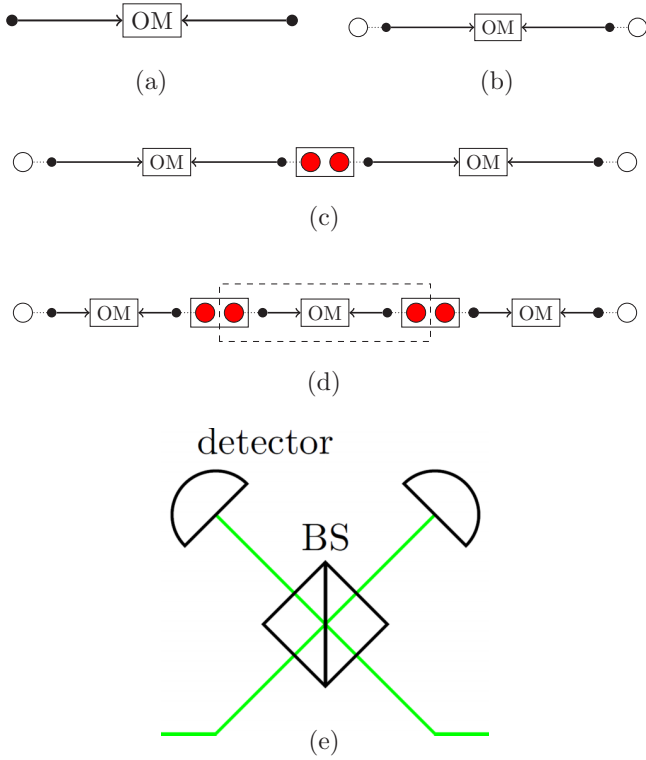


FIG. 1. Illustration of the protocol. (a) Phase-matching QKD. Alice and Bob send optical coherent states (black filled points) to Charlie who performs an optical measurement (OM). (b) Entanglement-based variation of phase-matching QKD ($n = 1$). Alice and Bob each have an optical mode (black filled point) entangled with a short-lived memory (white filled circle). The optical fields are sent to Charlie's OM. The memories can be short-lived since it does not matter when Alice and Bob perform the measurements on their memories (as long as they wait with communicating their choice of measurement basis). (c) Two-segment HQR variant ($n = 2$). Two copies of (b) are used where the memories in the central node need to be long-lived (red filled circles), since either of them has to wait until the other segment succeeds. When both segments succeeded, a Bell measurement is performed on the two long-lived memories for entanglement swapping. (d) Three-segment HQR variant ($n = 3$). In order to obtain the n -segment repeater, one simply needs to use $n - 2$ inner segments (marked by the dashed box). Such an n -segment quantum repeater scheme consists of $2n$ physical segments. (e) Setup of the OM. Usually the detectors are on-off detectors, but we could also use PNRDs. For $\theta \ll 1$, we only need one detector. BS stands for beam splitter.

and an optical mode starting in a coherent state, resulting in $\frac{1}{\sqrt{2}}(|\uparrow, \alpha \exp(-i\theta)\rangle + |\downarrow, \alpha \exp(i\theta)\rangle)$. Notice that Alice and Bob can also prepare BB84 states (thus distributing effective entanglement) instead of real entanglement. This is equivalent to the case where they generate real entanglement and perform measurements on the memories before sending the optical modes, because the measurements commute with Eve's operations provided that Alice and Bob only send information about the chosen measurement basis after establishing the raw key. Whenever Alice or Bob should apply Pauli operations to their memories but they have already measured them, this can be done via classical postprocessing of the measurement data.

The generation of these entangled states was described in the previous section. We will show that for our repeater protocol we can use, in principle, any $\theta > 0$ at the expense of a larger amplitude α of the coherent state. Choosing a small θ is also accompanied by the need of a better phase stabilization.

(2) Alice and Bob send the optical part of their hybrid entangled states through a lossy channel of transmittance $\sqrt{\eta}$ to a middle station operated by Charlie ($\eta_{\text{total}} = \eta$).

(3) If Charlie is honest, he applies a 50:50 BS to the two incoming optical modes with annihilation operators \hat{a} and \hat{b} described by the transformation, $\hat{a}' = (\hat{a} + \hat{b})/\sqrt{2}$, $\hat{b}' = (\hat{a} - \hat{b})/\sqrt{2}$. Then he measures mode b' with an on-off detector or, alternatively, with a PNRD, while he does not need to measure anything for mode a' [see Fig. 1(e)]. If he measures at least one photon, his measurement correlates Alice's and Bob's quantum memories.

In order to distribute entanglement over very large distances, we divide the overall channel that connects Alice and Bob into n smaller segments where in each we run the above protocol. The smallest example above then was for $n = 1$ [Fig. 1(b)] and the $n = 2$ case with two repeater segments, each with a detection station in the middle (so, effectively four physical segments), can be seen in Fig. 1(c). As the next step, we perform entanglement swapping between neighboring quantum memories as soon as they are ready, as usual in quantum repeaters. In the end, we have an (effective) two-qubit state shared by Alice and Bob that can be used for generating a secret key by employing, e.g., the (entanglement-based) BB84 protocol.

Let us now get some insight into why we may use any $\theta > 0$, especially $\theta \neq \frac{\pi}{2}$, and only need to measure one mode. For this, we will still omit channel losses. We again consider the smallest $n = 1$ case, corresponding to one repeater segment in the notation of general n . The state before the BS is given by $\frac{1}{2}[|\uparrow, \alpha \exp(-i\theta)\rangle + |\downarrow, \alpha \exp(i\theta)\rangle]^{\otimes 2}$. After the BS (and changing order), the state is given by

$$\begin{aligned} & \frac{1}{2}(|\uparrow, \uparrow, \sqrt{2}\alpha e^{-i\theta}, 0\rangle + |\downarrow, \downarrow, \sqrt{2}\alpha e^{i\theta}, 0\rangle \\ & + |\uparrow, \downarrow, \sqrt{2}\alpha \cos \theta, -i\sqrt{2}\alpha \sin \theta\rangle \\ & + |\downarrow, \uparrow, \sqrt{2}\alpha \cos \theta, i\sqrt{2}\alpha \sin \theta\rangle), \end{aligned} \quad (4)$$

where the last two entries in each ket vector refer to the two modes a' and b' , respectively. In this simplified scenario, also assuming that Charlie uses a PNRD, by detecting mode b' he projects the memories onto $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|\uparrow, \downarrow\rangle \pm |\downarrow, \uparrow\rangle)$, where the sign depends on whether he measured an even or odd nonzero number of photons. If we set $\theta = \frac{\pi}{2}$, we could in addition also use a PNRD for mode a' and depending on the nonzero measurement outcome (even or odd number) Charlie's measurement would project the quantum memories onto $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|\uparrow, \uparrow\rangle \pm |\downarrow, \downarrow\rangle)$. As a consequence, our wish to need only small θ comes at the price that the success probability is only half of the ideal probability of success for $\theta = \frac{\pi}{2}$. The protocol succeeds when there is at least one photon measured in mode b' and therefore the success probability is given by $\frac{1}{2}(1 - e^{-2\alpha^2 \sin^2 \theta})$. When considering on-off detectors instead of PNRDs, one projects onto a mixture of two Bell states. Note that the postmeasurement memory state and the success probability only depend on the product $\alpha \sin \theta$

and therefore we can use an arbitrarily small θ by employing correspondingly large amplitudes α in this simplified model.

B. Channel loss only

As the next step, we will include the lossy channel with transmittance $\sqrt{\eta}$ (between Alice/Bob and the middle station, again considering the $n = 1$ case) and obtain the density operator of Alice and Bob's qubits after Charlie's successful measurement. In order to keep this straightforward calculation clear, we will introduce auxiliary modes such that the lossy channel acts as a unitary operation on a larger Hilbert space. After Charlie's measurement, we trace out all subsystems except Alice's and Bob's memory qubits. More details on this calculation can be found in Appendix E. When Charlie uses a PNRD, the resulting density operator is given by

$$\frac{1}{2}(1 + e^{-2(1-\sqrt{\eta})\alpha^2 \sin^2 \theta})|\Psi^\pm\rangle\langle\Psi^\pm| + \frac{1}{2}(1 - e^{-2(1-\sqrt{\eta})\alpha^2 \sin^2 \theta})|\Psi^\mp\rangle\langle\Psi^\mp|, \quad (5)$$

where the upper sign holds in the even and the lower sign holds in the odd photon number case. Because of the successful measurement, the qubits can only be in the $\{|\uparrow, \downarrow\rangle, |\downarrow, \uparrow\rangle\}$ subspace. If Charlie uses an on-off detector, the density operator is given by

$$\frac{1}{2}(1 + e^{-2(2-\sqrt{\eta})\alpha^2 \sin^2 \theta})|\Psi^-\rangle\langle\Psi^-| + \frac{1}{2}(1 - e^{-2(2-\sqrt{\eta})\alpha^2 \sin^2 \theta})|\Psi^+\rangle\langle\Psi^+|. \quad (6)$$

Here, the state $|\Psi^-\rangle$ has a larger probability because of the larger fraction of an odd nonzero photon number than that for an even nonzero photon number. Therefore, Alice and Bob could exploit this to distill $1 - h(\frac{1}{2}[1 + e^{-2(1-\sqrt{\eta})\alpha^2 \sin^2 \theta}])$ or $1 - h(\frac{1}{2}[1 + e^{-2(2-\sqrt{\eta})\alpha^2 \sin^2 \theta}])$ ebits in the cases of PNRDs or on-off detectors, respectively, using one-way classical communication in the asymptotic limit, where $h(\cdot)$ denotes the binary entropy function. When using on-off detectors, one obtains an ebit rate of

$$\frac{1}{2}(1 - e^{-2\sqrt{\eta}\alpha^2 \sin^2 \theta})\{1 - h[\frac{1}{2}(1 + e^{-2(2-\sqrt{\eta})\alpha^2 \sin^2 \theta})]\} \approx_{\sqrt{\eta} \ll 1} \sqrt{\eta}\alpha^2 \sin^2 \theta \{1 - h[\frac{1}{2}(1 + e^{-4\alpha^2 \sin^2 \theta})]\}. \quad (7)$$

Note that this is the same as the secret-key rate of BB84 in the asymptotic limit. The tradeoff of the original HQR (assuming small θ) between high fidelities for small $\alpha\theta$ and high success probabilities for large $\alpha\theta$ in the version with unambiguous state discrimination [34] now becomes manifest in a high secret-key fraction (second factor) for small $\alpha\theta$ and a high raw rate (first factor) for large $\alpha\theta$. However, the crucial difference is that the entanglement distribution probability in a single repeater segment ($n = 1$) now scales with $\sqrt{\eta}$ instead of η due to the middle station between Alice and Bob. Since a similar expression appears in the PNRD case, it is useful to optimize the function $f(x) = x(1 - h(\frac{1}{2}(1 + e^{-2x})))$ and choose $\alpha^2 \sin^2 \theta$ accordingly. The maximum of f is approximately 7.141×10^{-2} with $x \approx 0.229$. With this function, it can be seen easily that the use of PNRDs instead of on-off detectors only gives improvement of a factor of 2 for the rate in the high-loss regime. Therefore, we will only consider on-off detectors since these are readily available in comparison to

PNRDs. The resulting overall ebit rate (allowing for small θ) is given by $0.5 \times 7.141 \times 10^{-2} \sqrt{\eta_{\text{total}}}$ (similar to Ref. [20]¹).

Next, we consider the case of n segments [see Fig. 1(d)]. It is then straightforward to calculate Alice's and Bob's density operator after the quantum teleportation steps, because the input states are Bell diagonal (see Appendix D for details). For the case of on-off detections, up to suitable Pauli operations (which can also be applied via classical postprocessing if Alice and Bob already measured their qubits in the beginning) after the Bell measurements on the memory qubits for entanglement swapping [see Fig. 1(c) for the $n = 2$ case], Alice and Bob share the (effective) state

$$\frac{1}{2}(1 + e^{-2n(2-\sqrt{\eta})\alpha^2 \sin^2 \theta})|\Phi^+\rangle\langle\Phi^+| + \frac{1}{2}(1 - e^{-2n(2-\sqrt{\eta})\alpha^2 \sin^2 \theta})|\Phi^-\rangle\langle\Phi^-|. \quad (8)$$

When using PNRDs, one obtains a similar state with a different coefficient of $|\Phi^\pm\rangle$ ($1 - \sqrt{\eta}$ instead of $2 - \sqrt{\eta}$). Let us consider a scheme where we try to distribute the entanglement in all segments in parallel and only at the end do we perform the entanglement swapping everywhere. Using the results for the exact raw rate with deterministic entanglement swapping [44], one can calculate the obtainable ebit and secret-key rate for this simple case exactly. However, to obtain a rough overview it is useful to apply an approximation for the raw rate (assuming $\sqrt{\eta} \ll 1$; see details in Appendix B) and use the optimal value for $n\alpha^2 \sin^2 \theta$, resulting in an overall secret-key rate of

$$\frac{2\sqrt{\eta_{\text{total}}}}{2n} H(n)^{-1} \frac{0.07}{2n} \sim 3.57 \times 10^{-2} \frac{2\sqrt{\eta_{\text{total}}}}{n(\gamma + \ln(n))}, \quad (9)$$

where $H(n)$ are the harmonic numbers and $\gamma = 0.57721 \dots$ is the Euler-Mascheroni constant. Notice that we always have to reduce the mean photon number α^2 of each optical pulse with increasing n ($\alpha_{\text{optimum}} \approx \frac{1}{\sin(\theta)} \sqrt{\frac{0.229}{2n}}$). All these considerations are for secret-key rates per channel use (and per mode, but in our schemes, the optical states are single-mode). We define one channel use as a single attempt to generate entanglement in all repeater segments.

One benefit of this scheme is that in order to obtain a secret-key rate scaling of $\frac{2\sqrt{\eta_{\text{total}}}}{2n}$ one only needs $n - 1$ stations equipped with quantum memories. In comparison, a

¹The difference in the protocol between Ref. [20] and our work with $n = 1$ is that the authors of Ref. [20] use $\theta = \frac{\pi}{2}$ and two on-off detectors, such that their raw rate is larger by a factor of 2. However, there are also differences in the approach of calculating the secret-key rate. We employ a BB84-like protocol since it easily allows us to go to a larger number of repeater segments, whereas the authors of Ref. [20] consider the Devetak-Winter formula for obtaining the secret-key fraction by calculating the mutual information between Alice's and Bob's bits and estimating the mutual information between Eve and the key via the Holevo information. This approach allows the authors of Ref. [20] to employ only coherent states for estimating Eve's information, while in our approach we need to generate hybrid entangled or cat states, even for the simplest $n = 1$ case, without memory assistance.

standard quantum repeater [6]² would need $2n - 1$ stations with memories when directly employed for QKD with Alice and Bob immediately measuring their qubits (otherwise the standard repeater uses $2n + 1$ memories, while our scheme would use $n + 1$ memories). Note that the scaling of $\sqrt[2n]{\eta_{\text{total}}}$ is consistent with the ultimate end-to-end capacity in repeater-assisted quantum communication where the channel is divided into $2n$ physical channel segments (assuming large segment lengths) [46]. When considering first experimental realizations of small-scale memory-based quantum repeaters, using a scheme like ours (or related schemes like those of Ref. [32]) could be beneficial, because in order to obtain a secret-key rate scaling of $\sqrt[2n]{\eta_{\text{total}}}$ only a single memory station is needed instead of three.

For the case of this section where channel loss is the only error considered, the distillable entanglement (when allowing one-way, forward classical communication) coincides with the asymptotic secret-key rate obtainable with BB84. In order to obtain a reasonably realistic description of such a repeater, we also have to include dark counts and the efficiency of the on-off detectors, memory dephasing, phase mismatch, and errors in the deterministic entanglement swapping which will be described by a depolarizing channel. Before turning to such a model including all of these errors, however, one may first only include the most important errors which still enables one to see their influence onto the secret-key rate in simple, analytical expressions. For our treatment here, all conceptual and technical details regarding the more realistic cases beyond just channel loss are presented in the Appendixes. There, we first consider detector inefficiencies and memory dephasing where we can still describe the resulting states as mixtures of two Bell states. Including detector efficiencies (η_{det}) is trivial, because we only have to substitute $\sqrt{\eta} \rightarrow \sqrt{\eta} \times \eta_{\text{det}}$. However, things become trickier when considering the dephasing in the memories. Nonetheless, since the dephasing channel is a Pauli channel, it commutes with the entanglement swapping and therefore we can assume that we first distribute perfect entanglement via multiple quantum teleportations and then apply the errors to the qubits (according to the loss channel and the memory dephasing; see Appendixes A and D). Later, we also consider imperfections of the Bell

measurements which still result in Bell-diagonal states. Finally, we will also take into account dark counts, eventually leading to Bell-nondiagonal states. A detailed discussion of the influence of these error sources to the secret-key rate is given in Appendix F. We also present a detailed discussion on the use of homodyne detectors for our scheme in Appendixes F and H. The secret-key rates as obtainable with our model (based on on-off detectors) will be presented and compared among different scenarios in the following section. The extra experimental parameters as required for the discussion there are all introduced in Appendixes A and F.

IV. COMPARISON OF SECRET-KEY RATES

A. Secret-key rate per channel use

Let us now consider the performance in terms of BB84 secret-key rates per channel use of our proposed scheme for some physically reasonable parameters. We start with the example of a two-segment repeater [i.e., $n = 2$, corresponding to two segments connected at a memory station and each segment equipped with an optical middle station; see Fig. 1(c)]. We assume the following parameters (similar to Ref. [20]):

- (1) $\sqrt{\eta} = 0.15 \exp(-\frac{L}{2nL_{\text{att}}})$,
- (2) $L_{\text{att}} = 22\text{km}$,
- (3) $\alpha = 23.9$,
- (4) $\theta = 0.01$,
- (5) dark count probability $p_{\text{dark}} = 8 \times 10^{-8}$,
- (6) $p_{\text{depol}} = 10^{-2}$,
- (7) $\tau = \frac{L}{nc}$,
- (8) $c = 2 \times 10^8 \frac{\text{m}}{\text{s}}$, and
- (9) error correction inefficiency $f_{\text{EC}} = 1.15$.

The transmission parameter $\sqrt{\eta}$, when we set $n = 2$, corresponds to a quarter of the total distance L between Alice and Bob, because every mode travels only for this distance to the corresponding detector station. This parameter also includes a finite detector efficiency (factor $p_{\text{det}} = 0.15$). We shall also consider perfect detectors, $p_{\text{det}} = 1$. Since we do not know the optimal value of α (for given θ) when considering all possible errors in our model, we simply use the optimal α from the loss-only case assuming $n = 2$. This already gives a good starting point for α , which we use everywhere unless stated otherwise. Further parameters are explained in Appendixes A and F.

The BB84 secret-key fraction [2] is given by

$$1 - h(e_X) - f_{\text{EC}} h(e_Z), \quad (10)$$

where $e_{X/Z}$ are the error probabilities in the X and Z bases which can also be expressed in terms of the four Bell-state coefficients of the density matrix. Note that we consider the biased BB84 scheme where one of the two bases is employed more often, allowing us to increase the sifting factor to unity in the asymptotic limit of infinite repetitions [47]. The overall secret-key rate is then given by the product of the raw rate and the secret-key fraction.

The memory coherence time T and the phase mismatch will be varied in order to assess their influence on the secret-key rate (see Appendix F). Let us first study the effect of the memory dephasing, since insufficient coherence times are

²Note that there are well-known proposals for quantum repeaters that are based on single-photon interference and thus intrinsically contain the twin-field-type scaling advantage. One such protocol makes use of a single atom or spin entangled with a light mode that either contains a photon or not [45]; see also Ref. [32]. Another protocol, proposed by Duan, Lukin, Cirac, and Zoller (DLCZ) [7], initially employs entanglement between a light mode and the collective spin mode of an atomic ensemble. The finally resulting two-mode single-excitation spin entanglement in DLCZ, however, cannot be straightforwardly used for applications like QKD and therefore DLCZ suggests a postselection strategy by considering two copies of a repeater chain and accepting only those cases where each end point of the double-chain state carries exactly one spin excitation. As a consequence, the DLCZ scheme loses its additional scaling advantage. The schemes of Refs. [32,45] do not share this complication, because their resulting spin-spin entanglement is of immediate use.

an important issue for quantum repeaters. As can be seen in Figs. 7 and 8 (in Appendix F), one really needs demanding memory coherence times such as 1000 s or more in order to be able to expect nearly the total benefit of the memory-based repeater capabilities. When considering more realistic, currently available memories with a coherence time of around 1 s,³ it can be seen that it is not even possible to overcome the PLOB bound (Fig. 7 with inefficient detectors). This means in this case the additional memory element even worsens the secret-key rate in comparison to simple twin-field QKD. However, we also found that the detection efficiency p_{det} is a highly influential parameter determining whether PLOB can be exceeded or even the ultimate $\sqrt[4]{\eta_{\text{total}}}$ scaling can be approached, with realistic (~ 1 s) or potential future ($\gtrsim 10$ s) coherence times, respectively (see Fig. 8).⁴

Based on the above observations, one may infer that the MA-PM QKD scheme cannot help increasing long-distance secret-key rates using currently available memories and finite, modest detector efficiencies. However, up to now we assumed that the participants will always wait until the entanglement is distributed in both segments no matter how long this distribution lasts for. It is possible, though, to introduce a maximal memory waiting time [32,50–54] until which the entanglement must be distributed in both segments; otherwise, the entanglement already distributed in one segment is discarded in order to prevent large error rates at the expense of a lower raw rate. References [52,53] derive the raw qubit rate for a two-segment repeater with such a memory cutoff, while Ref. [54] presents a rate formula for the more general case of arbitrarily many segments under the constraint of deterministic entanglement swappings. References [32,50] analyze the dephased qubit states for schemes with at most two segments.

³Currently available memory coherence times are ranging from several μs (quantum dots) to tens of ms (color centers, atoms, and ions) [48]. Although there are very recent reports on approaching coherence times of up to a few or even above 60 min [49], we assume that future coherence times that are also compatible with the requirement of telecom-frequency conversion are within the range of almost 1 ms (quantum dots) and 0.1–1 s (atoms and ions) up to 10 s (color centers). In our quantitative rate analysis including memory dephasing, we will thus have a particular focus on coherence time values of 0.1, 1, and 10 s (see especially Figs. 2–6). For a more detailed discussion on the interplay between experimental clock times (with or without the need of additional spin sequences on the memory qubits), memory coherence times, and the need for frequency conversion, for various experimental hardware platforms, see Ref. [48]. In that reference as well as in the present work, the focus is on single-spin quantum memories subject to dephasing rather than spin ensembles (as employed in atomic-ensemble-based quantum repeaters [7]), which instead must be modeled including memory loss acting on collective, bosonic spin modes.

⁴Throughout all plots, as benchmarks, we show the PLOB bound $-\log_2(1 - \eta_{\text{total}})$ for point-to-point communication between Alice and Bob [5] and, instead of the ultimate repeater bounds for a quantum repeater with $2n$ physical segments $-\log_2(1 - \sqrt[2n]{\eta_{\text{total}}})$ [46], several benchmarks of the form $\sqrt[2n]{\eta_{\text{total}}}$ (which up to a factor of 1.44 coincide with the former for small $\sqrt[2n]{\eta_{\text{total}}}$), since our particular qubit-based scheme can never exceed $\sqrt[2n]{\eta_{\text{total}}}$ similar to the ideal standard twin-field scheme that never goes above $\sqrt{\eta_{\text{total}}}$.

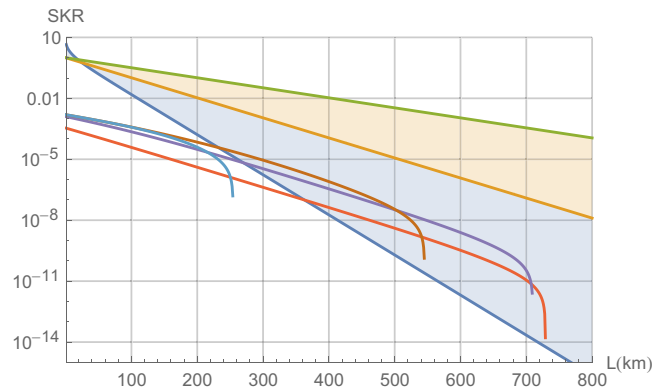


FIG. 2. Secret-key rates for a two-segment repeater ($n = 2$, parallel scheme) without phase mismatch assuming the parameters as listed in the main text (including $p_{\text{det}} = 0.15$) and a memory coherence time T of 1 s. The straight lines (from bottom to top) denote the PLOB bound, $\sqrt{\eta_{\text{total}}}$, and $\sqrt[4]{\eta_{\text{total}}}$. The rates are for different values of the memory cutoff (10, 100, 1000, 10 000) (from right to left). The areas between PLOB and $\sqrt{\eta_{\text{total}}}$ and between $\sqrt{\eta_{\text{total}}}$ and $\sqrt[4]{\eta_{\text{total}}}$ are highlighted in color.

As can be seen in Fig. 2, it is possible to overcome the PLOB bound by introducing a cutoff, and furthermore, it is even possible to distribute secret keys over a distance of 700 km and more with modestly performing memories and detectors (compare this with Fig. 7, even with $T = \infty$). In this work, we only consider rates including cutoff for $n = 2$.

We expect that a cutoff will also enhance the final rates for more than two segments. Thus, our rate analysis leads us to the following conclusion. Even though the PLOB bound can in principle be exceeded for our $n = 2$ scheme by introducing a memory cutoff, a higher experimental cost would be needed, i.e., sufficiently efficient memories and detectors, in order to benefit from the improved scaling of our $n = 2$ scheme compared with twin-field QKD. However, in Sec. IV B, we will see that when rates per second are considered, it is generally hard for a small-scale repeater like our $n = 2$ scheme to compete against twin-field QKD at high clock rates. Therefore, we will also consider more than two repeater segments (as for an alternative, we also explore the possibility of an asymmetric two-segment repeater operating at a higher clock rate in Appendix G).

In Fig. 3, one can see the scaling behavior of repeaters based on our protocol with $n = 2, 3$, or even 4 repeater segments considering a finite memory coherence time of 10 s and no additional errors in comparison to the PLOB bound and ideal quantum repeaters. For all n , we choose $\alpha = 23.9$ even though it is generally not the optimal value in the loss-only case, but it yields better rates when considering other errors. However, note that we did not try to find an optimal α in the general case. When we optimize α this will be explicitly stated. We found that for these three different segment numbers PLOB is overcome at an overall distance of approximately 140 km. However, since the PLOB bound can be overcome by twin-field QKD without memory stations, the more relevant benchmark for our protocol may be $\sqrt{\eta_{\text{total}}}$ which can be exceeded at approximately 350 km. Due to the

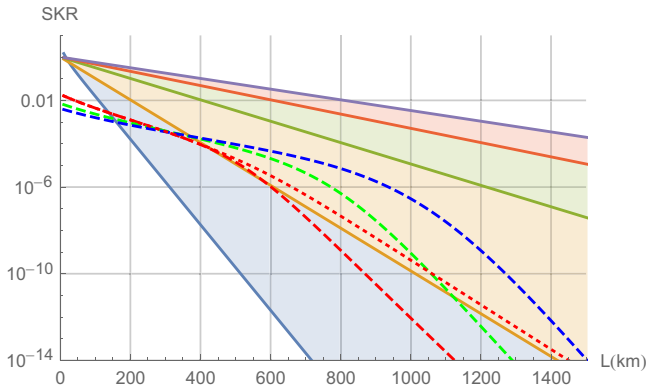


FIG. 3. Secret-key rates for a repeater with $n = 2$ (red), 3 (green), and 4 (blue) (dashed, from left to right) segments using a sequential protocol (parallel for $n = 2$) without cutoff (dashed lines, $\alpha = 23.9$ in all cases). For all curves, we consider a finite memory coherence time of 10 s (no other errors are assumed). The red dotted line denotes a $n = 2$ scheme where we do use a cutoff. The benchmarks (from bottom to top) PLOB, $\sqrt{\eta_{\text{total}}}$, $\sqrt[4]{\eta_{\text{total}}}$, $\sqrt[6]{\eta_{\text{total}}}$, and $\sqrt[8]{\eta_{\text{total}}}$ can also be seen. The regions between two of those benchmarks are highlighted in color accordingly.

coherence time of only 10 s we can barely surpass $\sqrt{\eta_{\text{total}}}$, but with an appropriately chosen cutoff parameter (in the $n = 2$ case) we can overcome this benchmark even for distances between 450 and 1500 km (see Fig. 3). Furthermore, we find that by making use of a memory cutoff and perfect-efficiency detectors, but also including dark counts and an imperfect Bell measurement, it suffices to require a coherence time of 5 s for overcoming $\sqrt{\eta_{\text{total}}}$ (not shown in plots). In order to obtain better rates than in the ideal twin-field scheme, a coherence time of 1 s suffices, even without making use of a memory cutoff (see Fig. 8).

B. Secret-key rate per second

For practical applications, the secret-key rate per second is the more important figure of merit for comparing quantum repeaters with other types of QKD schemes. A large disadvantage of scalable memory-based quantum repeaters is that they rely on classical communication for confirming success, setting an upper bound on the repetition rate due to classical communication times. For example, when assuming a spacing of 100 km between two repeater stations, this limits the repetition rate to the order of kHz. However, theoretically, this also makes it easy to convert the secret-key rate per channel use to a secret-key rate per second, because the (classical and quantum) communication times are typically much larger than the local operation times and thus the latter can be neglected in the regimes that we mainly consider here.⁵ Therefore, in order to perform better than twin-field QKD in terms of secret-key rate

per second by using a memory-assisted repeater, one needs to employ sufficiently many repeater stations for a given total distance (with $\eta_{\text{total}} \ll 1$), such that the communication times become smaller (and also the scaling advantage increases). However, even for repeater spacings as small as 100 m, the repetition rate only grows to the order of MHz. Hence, one can see that a scalable memory-based quantum repeater with a reasonable repeater spacing has to outperform twin-field QKD by many orders of magnitude in terms of secret-key rate per channel use, only to obtain rates similar to twin-field QKD per second. Nonetheless, there are at least three reasons for why it is still beneficial to employ our memory-assisted schemes.

First, like general memory-based quantum repeaters, in principle, long-distance regimes become accessible for rates per second that are otherwise (including for twin-field QKD) unreachable at the same rates. This happens because of the scaling advantage which eventually dominates over the clock-rate disadvantage for sufficiently long distances. At such distances, the final rates per second are generally low, but this applies to both twin-field QKD and MA-PM QKD while rates end up strongly biased toward MA-PM QKD with growing distance. In this case, the small final rates of MA-PM QKD may be enhanced up to practical values by employing many repeater chains in parallel (multiplexing). Second, also for distances where dark counts greatly reduce the secret-key rate, a repeater can overcome the twin-field QKD secret-key rate per second. However, it is also possible to obtain the same effect by using entangled light sources with a high repetition rate as a relay in order to keep the dark count effect small. With our system, such a relay could be realized when all spins of the hybrid spin-light entangled states are measured immediately. In this case, we only lose a factor of $\frac{1}{2}$ when employing small θ ; however, with a simple relay ($n = 2$), as we no longer make use of memories, the effect is squared. Third, unlike direct-transmission or twin-field QKD at high repetition rates, our memory-based schemes can also be used in applications different from QKD such as distributed quantum computing.

As can be seen in Fig. 4, our proposed schemes (for $n \geq 8$) can outperform (in terms of secret-key rate per second) idealized twin-field QKD even when we consider dark counts, memory dephasing ($T = 10$ s), and depolarizing errors $p_{\text{depol}} = 10^{-3}$ in our repeater scheme for distances above 1000 km.⁶ However, even a maximally idealized four-segment quantum repeater (in a standard approach employing as many memories as our $n = 4$ scheme) that attains the corresponding repeater capacity [46] outperforms idealized twin-field QKD just at distances of 1000 km. Thus, it is a rather fundamental problem to overcome idealized twin-field QKD with further scalable memory-based quantum repeaters for a small number of memories in a regime where the single-chain secret-key rate per second is not too low for practical purposes. Also, notice that here we did not consider a memory cutoff (for $n > 2$ there are many different strategies to implement such a cutoff protocol) and therefore we expect that it is possible

⁵The problem of these low repetition rates can be circumvented when using so-called third-generation quantum repeaters which make use of quantum error correction [55]. However, an optical implementation of suitable quantum error correcting codes is currently still hard to achieve.

⁶In Fig. 4, we need to optimize α for the different schemes. Otherwise, if we use $\alpha = 23.9$ in all schemes the rates for $n = 16$ become the worst in the plots. We used the following values for α : 30, 23.9, 23.9, 18, 17, 9 (ordered by increasing n).

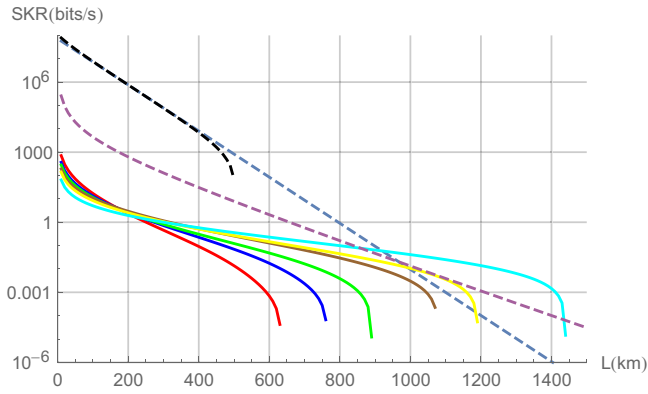


FIG. 4. Comparison of the secret-key rate in bits/s between twin-field QKD (ideal, blue dashed; with dark counts, black dashed) assuming a repetition rate of 1 GHz and our proposed scheme for $n = 2, 3, 4, 6, 8, 16$ (left to right in terms of vanishing rates, parallel scheme for $n = 2$), where we assumed detectors with unit efficiency ($p_{\text{det}} = 1$), a dark count rate of 7×10^{-8} , a memory coherence time of 10 s and $p_{\text{depol}} = 10^{-3}$. The dashed purple line (for $L \approx 0$ beginning at a rate of $\approx 10^5$ bits/s) represents an ideal standard repeater with four physical segments attaining the repeater-assisted capacity [46], whose repetition rate is limited by the communication time. Notice that for $n = 8$ and distances as large as 1000 km we outperform ideal twin-field QKD with a noisy repeater in terms of secret-key rate per second while still attaining rates as high as 10^{-2} Hz without making use of memory cutoffs.

to improve the secret-key rates of our schemes significantly (recall the improvement in the comparison between Figs. 2 and 7). When comparing our schemes with a noisy twin-field QKD protocol, it is easy to see that our schemes allow for a longer communication range until the secret-key rates drop to zero.

In Fig. 5, it can be seen that our scheme with $n = 2$ including memory cutoff is able to outperform twin-field QKD in a scenario where dark counts are taken into account. Even a scheme with memories of rather low coherence time such as 0.1 s is able to outperform realistic twin-field QKD at a distance of approximately 440 km, though resulting in a rather low secret-key rate of 10 bits/h. Memories with such coherence times are already available [48]. However, it can also be seen that a similar enhancement is achieved with a relay (which actually scales better than the memory-based scheme for a coherence time of 0.1 s). In order to see an improved scaling for the repeater, one needs a coherence time as large as 10 s. Since the huge gap between twin-field QKD and our proposal in terms of secret-key rate per second in some regimes originates from the different repetition rates of both schemes, it is reasonable to consider the possibility for $n = 2$ not to place the beam splitter in the middle for one segment, but in an asymmetric way [thus modifying Fig. 1(c)]. Improvement is possible then, because Alice and Bob can send light states at an in principle arbitrarily high repetition rate, since they only need the information regarding success from the beam splitter in order to decide whether they should count or discard that round in the final classical postprocessing. However, the memory station requires this information immediately in order to decide if the state in the memory should

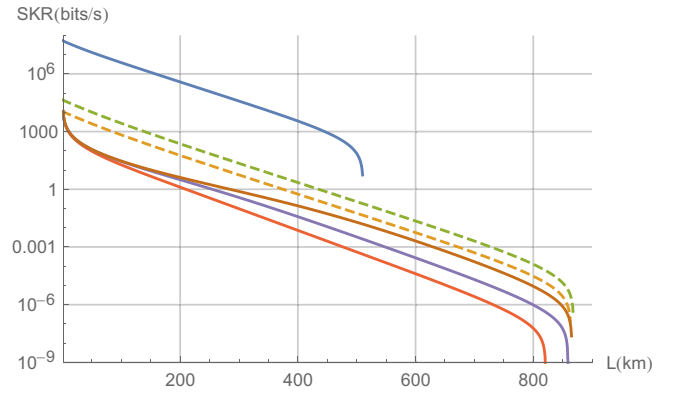


FIG. 5. Comparison of the secret-key rate in bits/s between twin-field QKD (blue, top) assuming a repetition rate of 1 GHz and our proposed scheme for $n = 2$ including a memory cutoff and assuming different memory coherence times of (0.1, 1, 10) s (solid lines, bottom to top) ($p_{\text{det}} = 1$, parallel scheme, other parameters are as described in the main text). The dashed lines (yellow, small θ hence smaller rate) refer to a relay configuration assuming a repetition rate of 1 MHz taking into account the finite spin-light interaction times for the optical entangled-state generations in our relay.

be held or discarded. When placing the beam splitter nearer to the memory, one decreases the secret-key rate per channel use, but at the same time enhances the possible repetition rate. We discuss this scheme in Appendix G. We find that for a not fully asymmetric scheme one can increase the secret-key rate per second by up to a few percent.

C. Comparison with USD hybrid repeater

Let us now compare our new HQR with a HQR that uses on-off detectors for unambiguous state discrimination (USD) [34]. In our scheme, in each segment we have two qubit memories each interacting nonlinearly with a coherent state and these optical states are then sent to a middle station with a 50:50 beam splitter followed by an on-off detector. In the USD scheme, we have two memories but only one optical state. First, this state interacts with the first memory, is then sent to the other, and interacts with this second memory. In the end, a USD measurement using linear optics, phase-space displacements, and three on-off detectors is performed. Thus, one can see that both schemes employ very similar resources. We can evaluate and compare the two schemes in a simple error model where we consider channel loss, depolarization, and memory dephasing.

In our scheme, the probability to generate entanglement in one segment in a single try is given by $\frac{1}{2}(1 - e^{-2\sqrt{\eta}\alpha^2 \sin^2 \theta})$, while for the USD hybrid repeater it is given by $\frac{1}{2}(1 - e^{-2\eta\alpha^2 \sin^2 \theta})$. Here we can already see the improvement of our scheme in the raw rate since η is simply replaced by $\sqrt{\eta}$. The loss channel and the measurement also induce a dephasing channel with parameter $e^{-2(2-\sqrt{\eta})\alpha^2 \sin^2 \theta}$ in our scheme. In the USD scheme, this is given by $e^{-2(1-\eta)\alpha^2 \sin^2 \theta}$. The memory dephasing works similar in both cases, but in our scheme the duration of a single entanglement generation

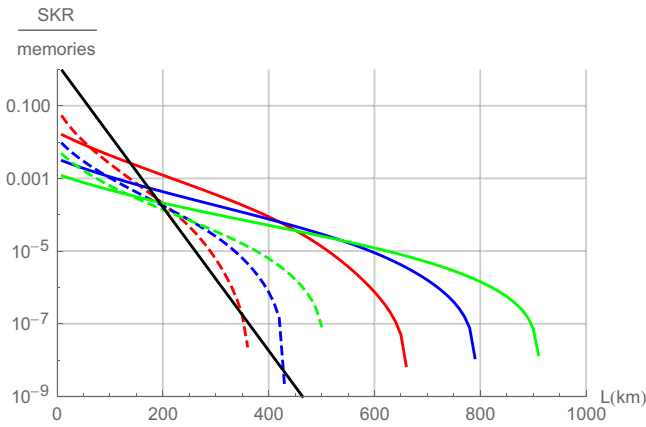


FIG. 6. Comparison of the secret-key rate per channel use per employed memory (station) for our scheme (solid lines) and the USD hybrid scheme (dashed lines) for $n = 2, 3, 4$ (from left to right in the regime of rates dropping toward zero), assuming a coherence time of $T = 10$ s, a depolarizing channel with $p_{\text{depol}} = 10^{-3}$, and a sequential scheme (parallel for $n = 2$). The black solid line corresponds to the PLOB bound.

attempt is given by $\frac{L}{nc}$ whereas in the USD scheme it is $2\frac{L}{nc}$.⁷ As can be seen in Fig. 6, already our $n = 2$ scheme gives better secret-key rates per employed memory than the USD hybrid repeater for $n = 2, 3, 4$ for relevant distances. In the regime of small distances, the USD scheme achieves rates slightly better than our scheme, because for $\eta = 1$ there is no dephasing due to loss and the measurement in the USD scheme. However, our scheme always has dephasing originating from the usage of the on-off detectors. Nonetheless, our scheme has a better distance scaling and therefore our schemes achieve better rates than the USD scheme for the relevant large-distance regime. For these distances, our schemes often achieve rates which are orders of magnitude better than those of the USD scheme. Thus, we obtain a better secret-key rate while employing a smaller supply of quantum memories.

V. CONCLUSION

We introduced a measurement-device-independent QKD scheme based on the twin-field QKD concept but making use of memories in order to extend the overall distance for which a secret key can be distributed. The secret-key rates per channel use of our scheme scale as $[nH(n)]^{-1} \frac{2^n}{\sqrt{\eta_{\text{total}}}}$ [harmonic number $H(n) = \gamma + \ln(n) + O(n^{-1})$] in the loss-only case (assuming $\frac{2^n}{\sqrt{\eta_{\text{total}}}} \ll 1$ and using a parallel entanglement distribution scheme), where $\gamma = 0.57721\dots$ is the Euler-Mascheroni constant and n is the number of repeater

segments, each equipped with memory stations at their ends and a beam splitter and optical-detector station in their middles. The transmission parameter $\eta_{\text{total}} = \exp(-\frac{L}{L_{\text{att}}})$ represents the total channel connecting Alice and Bob separated by a distance L .

Our scheme shares some similarities with the so-called hybrid quantum repeater such as the usage of hybrid entangled states and the dependencies and tradeoff related to the entanglement generation rate and state quality with regard to $\alpha \sin \theta$, where α is the optical coherent-state amplitude and θ is the angle of a spin-controlled phase rotation of the optical mode due to a dispersive light-matter interaction. However, due to the photonic middle stations in each repeater segment, our version inherits the twin-field-like scaling advantage. In some distance regimes, this difference results in rates for our scheme that are larger by orders of magnitude compared with the original HQR version based on unambiguous state discrimination. For this version, we explicitly showed that the relevant quantities do not exhibit the twin-field-type square-root enhancement of the transmission parameter per repeater segment like in our scheme. We further showed that it is possible, in principle, to employ small dispersive phase rotations θ corresponding to weak optical nonlinearities at the expense of using larger coherent state amplitudes α and more demanding phase stabilization. Another advantage of our scheme compared to the original hybrid quantum repeater is that it is no longer necessary to couple nonclassical light states with a spin system (like an atom in a cavity) “inline”. It is now sufficient to prepare hybrid light-spin entangled states “offline” and couple the optical parts with beam splitters when executing the repeater protocol.

For the $n = 2$ case with only one memory station based on a parallel distribution scheme, we considered the most important imperfections like photon loss, detector inefficiencies, memory dephasing, dark counts, phase mismatch, and faulty Bell measurements on the memories modeled by depolarization. This error analysis can also be extended to n repeater segments when using a sequential distribution and swapping strategy. This approach enabled us to calculate exact BB84 secret-key rates (in the asymptotic limit) for the general case of n repeater segments. For $n = 2$, the parallel scheme outperforms the sequential one and for $n > 2$ we have evidence that the sequential scheme is better. As we did not include quantum error correction, we focused on repeaters up to $n = 16$. We calculated secret-key rates per channel use for realistic parameter regimes and showed that introducing a cutoff (maximal duration) for the memory waiting time can increase the secret-key rate enormously.

Our main quantitative results in terms of secret-key rates per channel use are that by introducing quantum memories into a twin-field-based relay, for distances beyond 700 km, the PLOB bound can be beaten with memory coherence times of 1 s and modest detector efficiencies. The ideal single-repeater scaling of $\sqrt{\eta_{\text{total}}}$ can be exceeded when coherence times of 5 s and perfect detector efficiencies are approached. In order to overcome the ideal twin-field rate, only a coherence time of 1 s is needed. Since our scheme is mainly for threshold detectors but also involves light-matter interactions, the light wavelengths must be suitably chosen (possibly including additional frequency conversions which have not been considered here)

⁷For the USD scheme, it is also possible to shorten the duration of one time step to $\frac{L}{nc}$ by switching the roles of sender and receiver. If the entanglement generation fails, Bob usually communicates this failure to Alice, who then tries again. However, briefly after sending the classical communication he can also start to send an optical pulse to Alice, who needs this short break for switching from sender to receiver mode, which might be experimentally complicated.

and the basic processing times, as usually in memory-based quantum repeaters determined by classical communication times and the speed of the light-matter operations, are longer than those in twin-field QKD without memory assistance. Nonetheless, for sufficiently many and short elementary segments, the scaling advantage of the memory-assisted scheme can potentially overcome the disadvantage of the slower clock rates (for phase-matching QKD without memories, the source clock rate is just given by that of a laser generating coherent states; creating cat states like in our BB84-type scheme is unnecessary and so are light-matter couplings and classical waiting times). We explicitly showed this by also considering secret-key rates per second.

We also investigated a variant of our scheme based on homodyne detectors. According to our analysis, the regimes where a homodyne-based scheme works is incompatible with the regimes where the scaling advantage of a MA-PM QKD scheme becomes relevant. Thus, secret-key rates for segments of 10 km and more are obtained to be zero for the homodyne-based scheme. This is conceptually similar to the original hybrid quantum repeater based on homodyne measurements where the segment lengths also needed to remain sufficiently short (at around 10 km). A difference there, however, was that additional quantum error detection (entanglement purification) was included such that high-fidelity entangled states were still obtainable. In our scheme, active methods for quantum error correction or detection were not considered.

Like in all twin-field-type QKD approaches based on single-photon interference or, more generally, interference of phase-sensitive single-mode states, as opposed to those schemes relying on two-photon interference, a means for robust phase stabilization must be included. In our scheme, this could be achieved by sending a coherent-state reference pulse along the fiber channels together with the signal pulses.

ACKNOWLEDGMENTS

We thank the BMBF in Germany for support via Q.Link.X and the BMBF/EU for support via QuantERA/ShoQC. We also thank Stefano Pirandola and Mark Wilde for useful comments.

APPENDIX A: ERROR MODELS

Here we briefly describe all error models employed for our analysis. A lossy channel with transmittance η can be described as a beam splitter acting on the optical mode of interest a and an environmental mode b corresponding to the mode operator transformation

$$\begin{pmatrix} \hat{a}' \\ \hat{b}' \end{pmatrix} = \begin{pmatrix} \sqrt{\eta} & \sqrt{1-\eta} \\ \sqrt{1-\eta} & -\sqrt{\eta} \end{pmatrix} \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix}, \quad (\text{A1})$$

where \hat{a}' is the relevant output mode operator of interest and we trace out the environmental mode expressed by mode operator \hat{b}' . For fiber transmission, η is given by $\exp(-\frac{L}{L_{\text{att}}})$, where L is the fiber's length and L_{att} is the attenuation length of 22 km in a typical optical fiber.

The dephasing of the memories is described by the following dephasing channel,

$$\begin{aligned} \mathcal{E}_{\text{dephasing}}(t, T, \rho) \\ = \frac{1}{2} \left[1 + \exp\left(-\frac{t}{T}\right) \right] \rho + \frac{1}{2} \left[1 - \exp\left(-\frac{t}{T}\right) \right] Z \rho Z, \end{aligned} \quad (\text{A2})$$

where ρ is a single-qubit density matrix, Z is the Pauli qubit phase-flip operator, t is the time for which the memory dephases, and T is the memory coherence time. The imperfections of the Bell measurement on the quantum memories are modeled by the following depolarizing channel,

$$\mathcal{E}_{\text{depol}}(p_{\text{depol}}, \rho) = (1 - p_{\text{depol}})\rho + p_{\text{depol}} \frac{\mathbb{1}}{2}. \quad (\text{A3})$$

The POVM element corresponding to a click of the on-off detector is given by

$$\hat{E} = \mathbb{1} - D(0)|0\rangle\langle 0|, \quad (\text{A4})$$

where $D(0)$ denotes the probability that the detector does not click on a vacuum state. This means the dark count probability is given by $1 - D(0)$. Fortunately, we will not require an explicit expression for the conditional density operator that incorporates dark counts, because we trace out the measured mode (see Appendix E).

APPENDIX B: APPROXIMATION OF $\mathbb{E}[\max(X_1, \dots, X_n)]$

In order to distribute entanglement over the whole distance of the repeater, entanglement needs to be generated in all n segments. When generating entanglement in the n segments independently, the total waiting time is given by $\max(X_1, \dots, X_n)$, where the geometrically distributed random variables X_j describe the number of entanglement generation attempts until success in segment j and where p is the probability of success in a single attempt. Therefore, the raw rate scales inversely with $\mathbb{E}[\max(X_1, \dots, X_n)]$. This expectation value will also appear when we will discuss the dephasing in a parallel scheme using Jensen's inequality. For the case $p \ll 1$ and deterministic entanglement swapping, it is possible to obtain a simple approximation of $\mathbb{E}[\max(X_1, \dots, X_n)]$ where X is geometrically distributed:

$$\mathbb{E}[\max(X_1, \dots, X_n)] = \sum_{j=1}^n \binom{n}{j} \frac{(-1)^{j+1}}{1 - (1-p)^j} \quad (\text{B1})$$

$$\approx \sum_{j=1}^n \binom{n}{j} \frac{(-1)^{j+1}}{jp}. \quad (\text{B2})$$

This approximation is based on the exact expression of Ref. [44] for arbitrary p . We then expanded $(1-p)^j$ with the binomial theorem and neglected quadratic and higher orders of p . We can furthermore prove by induction

$$\sum_{j=1}^n \binom{n}{j} \frac{(-1)^{j+1}}{j} = \sum_{j=1}^n \frac{1}{j} =: H(n), \quad (\text{B3})$$

where $H(n)$ are also known as harmonic numbers. We approximate the harmonic numbers by using only the first terms of

their asymptotic expansion,

$$H(n) \approx \gamma + \ln(n) + \frac{1}{2n}, \quad (\text{B4})$$

where $\gamma = 0.57721 \dots$ is the Euler-Mascheroni constant. In the end, we obtain the simple approximation

$$\mathbb{E}[\max(X_1, \dots, X_n)] \approx \frac{1}{p} \left(\gamma + \ln(n) + \frac{1}{2n} \right). \quad (\text{B5})$$

Note that this approximation scales with $\ln(n)$, while the widely used approximation $\left(\frac{3}{2}\right)^{\frac{\log_2(n)}{p}}$ scales with $n^{\log_2(1.5)}$. However, note that the latter depends on the assumption of both small p and small swapping probabilities, so it is inapplicable here for deterministic swapping [53].

APPENDIX C: EFFECT OF MEMORY DEPHASING FOR $n = 2$

For the case of two quantum repeater segments, the definition of $M_{\text{par}} \equiv M$ in Eq. (F3) simplifies to $|X_1 - X_2|$, where X_1 and X_2 are independent geometrically distributed random variables. Therefore, we have for the corresponding distribution

$$\mathbb{P}(M = 0) = \sum_{k=1}^{\infty} \mathbb{P}(X_1 = X_2 = k) = \sum_{k=1}^{\infty} p^2 q^{2(k-1)} = \frac{p}{2-p},$$

and for $j > 0$,

$$\mathbb{P}(M = j) = \sum_{k=1}^{\infty} 2p^2 q^{2(k-1)+j} = 2 \frac{pq^j}{2-p},$$

where the factor 2 comes from the fact that the two cases $X_1 > X_2$ and $X_2 > X_1$ are possible.

This allows us to calculate for $M := |X_1 - X_2|$

$$\mathbb{E} \left[\exp \left(-M \frac{\tau}{T} \right) \right] = \frac{p}{2-p} \left[\frac{2}{1 - q \exp \left(-\frac{\tau}{T} \right)} - 1 \right], \quad (\text{C1})$$

and by summing only up to a constant instead of infinity and considering a renormalization, one can easily obtain the expectation value for protocols which abort after the memory has dephased for a given time (cutoff). The additional complexity of this protocol lies solely in the raw rate, which is already known in the literature [52–54]. Note that we also have to consider an additional nonrandom dephasing time, because each memory already dephased during the time between sending the optical mode and obtaining the information on whether the optical measurement was successful. Therefore, each memory dephases for a time unit of $\frac{L}{nc}$. If we perform the measurements on the two outer memories immediately, we only accumulate a constant dephasing time of $2(n-1)\frac{L}{nc} = \frac{2L}{c} \left(1 - \frac{1}{n}\right)$. If we perform the measurements of the outer memories at the end of the entanglement distribution [like in Eq. (F2)], we accumulate a constant dephasing time of $\frac{2L}{c}$.

APPENDIX D: PAULI CHANNELS AND ENTANGLEMENT SWAPPING

We call a single-qubit channel $\mathcal{N}(\cdot)$ a Pauli channel if and only if $\mathcal{N}(\rho) = \sum_i p_i P_i \rho P_i^\dagger$, where p_i are probabilities and

P_i are Pauli operators ($\mathbb{1}, X, Y, Z$). Since all of these Pauli operators either commute or anticommute, Pauli channels commute. The composition of two Pauli channels is again a Pauli channel, because the product of two Pauli operators is again a Pauli operator up to a phase which becomes irrelevant for the case of a Pauli channel since P_i and P_i^\dagger are both applied such that these phases cancel. Since one can switch between all four two-qubit Bell states by applying one of the four single-qubit Pauli operators, it can be seen that every Bell-diagonal state is equivalent to a Pauli channel acting on a perfect Bell state. Let us now show that Pauli channels commute with the entanglement swapping operation on perfect Bell states.

Without loss of generality, we assume that the Bell measurement on two memory qubits for entanglement swapping yields $|\Phi^+\rangle$ as the measurement outcome, while the other three cases work analogously. It is also sufficient to consider only two two-qubit pairs initially prepared in the Bell states $|\Phi^+\rangle_{12}$ and $|\Phi^+\rangle_{34}$ and each being partially subject to an arbitrary Bell-diagonal channel, \mathcal{N}'_2 and \mathcal{N}'_3 for qubits 2 and 3:

$$\begin{aligned} & \langle \Phi^+ |_{23} \mathcal{N}'_2(|\Phi^+\rangle_{12} \langle \Phi^+|) \otimes \mathcal{N}'_3(|\Phi^+\rangle_{34} \langle \Phi^+|) | \Phi^+ \rangle_{23} \\ &= \langle \Phi^+ |_{23} \sum_{i,j=1}^4 p_i p'_j P_{i,2} |\Phi^+\rangle_{12} \langle \Phi^+ | P_{i,2}^\dagger \\ & \quad \otimes P_{j,3} |\Phi^+\rangle_{34} \langle \Phi^+ | P_{j,3}^\dagger | \Phi^+ \rangle_{23} \\ &= \sum_{i,j=1}^4 p_i p'_j P_{i,1} P_{j,4} \langle \Phi^+ |_{23} | \Phi^+ \rangle_{12} \langle \Phi^+ | \\ & \quad \otimes | \Phi^+ \rangle_{34} \langle \Phi^+ | \Phi^+ \rangle_{23} P_{i,1}^\dagger P_{j,4}^\dagger \\ &= \frac{1}{4} \sum_{i,j=1}^4 p_i p'_j P_{i,1} P_{j,4} | \Phi^+ \rangle_{14} \langle \Phi^+ | P_{j,4}^\dagger P_{i,1}^\dagger \\ &= \frac{1}{4} \sum_{i,j=1}^4 p_i p'_j P_{i,1} P_{j,1} | \Phi^+ \rangle_{14} \langle \Phi^+ | P_{j,1}^\dagger P_{i,1}^\dagger \\ &= \frac{1}{4} \mathcal{N}'_1(\mathcal{N}'_1(|\Phi^+\rangle_{14} \langle \Phi^+|)). \end{aligned} \quad (\text{D1})$$

Here we used the fact that $P_{i,1} P_{i,2} |\Phi^+\rangle_{12} = |\Phi^+\rangle_{12}$ holds for all Pauli operators P_i and we also employed that (qubit) Pauli operators are Hermitian and unitary and therefore self-inverse.

We can then apply this result for all entanglement swapping operations successively. Note that this argument relies on the assumption of Pauli channels and Bell-diagonal states, but initially when including detector dark counts the memory states are no longer Bell diagonal and already dephasing before we apply a operation which erases the Bell nondiagonal elements [56, Sec. 3.2.1]. However, this erasing is done by applying random correlated two-qubit Pauli operations and hence commutes with the decoherence channel. As a consequence, we can first apply the erasing channel and therefore we have Bell-diagonal states (which are equivalent to a Pauli channel on a perfect Bell state), allowing us to use the result above. There is no additional temporal overhead due to the communication time needed for generating the correlations.

For example, a memory could generate two correlated random variables and send one of them to the other memory belonging to this segment. The necessary communication time is given by $\frac{L}{nc}$, which is the same time as between sending the optical mode and obtaining the information whether the optical measurement succeeded or failed. Alternatively, the middle station could also generate the correlated random variables and send them to the memories if the optical measurement was successful. Therefore, only the amount of sent information by the middle station increases and thus there are no temporal issues. In the end, we have to consider a concatenation of n dephasing channels, each with a random decoherence time which is equivalent to a single dephasing channel where the dephasing time is given by the sum of all the individual dephasing times, e.g., $t + t'$ (assuming the same coherence time for both memories) for \mathcal{N}_1 and \mathcal{N}'_1 in Eq. (D1) for t as defined in Eq. (A2). Similarly, we can simplify the concatenation of the $n - 1$ depolarizing channels with parameter p_{depol} , describing the probability of no depolarization, into a depolarizing channel with $1 - p'_{\text{depol}} = (1 - p_{\text{depol}})^{n-1}$. The concatenation of the Pauli channel corresponding to dark counts and measurements cannot be simplified as much as for the depolarizing or dephasing channel. For the concatenation of a general single-qubit Pauli channel,

$$\mathcal{N}(\rho) = p_1\rho + p_2Z\rho Z + p_3X\rho X + p_4Y\rho Y, \quad (\text{D2})$$

we obtain the following recursive set of equations,

$$\begin{pmatrix} p_1^{(n+1)} \\ p_2^{(n+1)} \\ p_3^{(n+1)} \\ p_4^{(n+1)} \end{pmatrix} = \begin{pmatrix} p_1 & p_2 & p_3 & p_4 \\ p_2 & p_1 & p_4 & p_3 \\ p_3 & p_4 & p_1 & p_2 \\ p_4 & p_3 & p_2 & p_1 \end{pmatrix} \begin{pmatrix} p_1^{(n)} \\ p_2^{(n)} \\ p_3^{(n)} \\ p_4^{(n)} \end{pmatrix}, \quad (\text{D3})$$

where $p_1^{(0)} = 1$ and $p_2^{(0)} = p_3^{(0)} = p_4^{(0)} = 0$. Therefore, we have

$$\begin{pmatrix} p_1^{(n)} \\ p_2^{(n)} \\ p_3^{(n)} \\ p_4^{(n)} \end{pmatrix} = \begin{pmatrix} p_1 & p_2 & p_3 & p_4 \\ p_2 & p_1 & p_4 & p_3 \\ p_3 & p_4 & p_1 & p_2 \\ p_4 & p_3 & p_2 & p_1 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \quad (\text{D4})$$

The transition matrix is real and symmetric and can thus be diagonalized, such that it is easy to calculate the power of the matrix.

APPENDIX E: CALCULATION OF THE QUANTUM REPEATER STATES WITH ON-OFF DETECTORS

Our simplest protocol ($n = 1$) starts by creating hybrid entanglement at the two cavities [see Fig. 1(b)]; i.e., we first have the state

$$\begin{aligned} & \frac{1}{2}(|\uparrow, \uparrow, \alpha e^{-i\theta}, \alpha e^{-i\theta}\rangle + |\downarrow, \downarrow, \alpha e^{i\theta}, \alpha e^{i\theta}\rangle) \\ & + |\downarrow, \uparrow, \alpha e^{i\theta}, \alpha e^{-i\theta}\rangle + |\uparrow, \downarrow, \alpha e^{-i\theta}, \alpha e^{i\theta}\rangle). \end{aligned} \quad (\text{E1})$$

After applying the lossy channels of transmittance $\sqrt{\eta}$ (corresponding to the distance between Alice/Bob and the middle station) and the 50:50 beam splitter at the middle station, we

obtain the following state:

$$\begin{aligned} & \frac{1}{2}(|\uparrow, \uparrow, \sqrt{2\sqrt{\eta}\alpha}e^{-i\theta}, 0, \sqrt{1-\sqrt{\eta}\alpha}e^{-i\theta}, \sqrt{1-\sqrt{\eta}\alpha}e^{-i\theta}\rangle \\ & + |\downarrow, \downarrow, \sqrt{2\sqrt{\eta}\alpha}e^{i\theta}, 0, \sqrt{1-\sqrt{\eta}\alpha}e^{i\theta}, \sqrt{1-\sqrt{\eta}\alpha}e^{i\theta}\rangle \\ & + |\uparrow, \downarrow, \sqrt{2\sqrt{\eta}\alpha}\cos\theta, -i\sqrt{2\sqrt{\eta}\alpha}\sin\theta, \\ & \sqrt{1-\sqrt{\eta}\alpha}e^{-i\theta}, \sqrt{1-\sqrt{\eta}\alpha}e^{i\theta}\rangle \\ & + |\downarrow, \uparrow, \sqrt{2\sqrt{\eta}\alpha}\cos\theta, i\sqrt{2\sqrt{\eta}\alpha}\sin\theta, \\ & \sqrt{1-\sqrt{\eta}\alpha}e^{i\theta}, \sqrt{1-\sqrt{\eta}\alpha}e^{-i\theta}\rangle). \end{aligned} \quad (\text{E2})$$

Here, the last two entries in each ket vector represent the loss modes that initially start in a vacuum state. In order to calculate the partial trace we will use the following calculation trick. Suppose we are given a state of the form $\sum_k c_k |k\rangle_1 \otimes |\Psi_k\rangle_2$ ($|k\rangle_1$ form an orthonormal basis, while $|\Psi_k\rangle_2$ may be arbitrary pure states) and we want to calculate the reduced density matrix of system 1:

$$\begin{aligned} & \text{Tr}_2 \left(\sum_{k,j} c_k c_j^* |k\rangle_1 \langle j| \otimes |\Psi_k\rangle_2 \langle \Psi_j| \right) \\ & = \sum_{k,j} c_k c_j^* \text{Tr}_2 (|k\rangle_1 \langle j| \otimes |\Psi_k\rangle_2 \langle \Psi_j|) \\ & = \sum_{k,j} c_k c_j^* |k\rangle_1 \langle j| \sum_l \langle l|_2 |\Psi_k\rangle_2 \langle \Psi_j|_2 \langle l|_2 \\ & = \sum_{k,j} c_k c_j^* |k\rangle_1 \langle j| \sum_l \langle \Psi_j|_2 \langle l|_2 |\Psi_k\rangle_2 \\ & = \sum_{k,j} c_k c_j^* |k\rangle_1 \langle j| \langle \Psi_j|_2 \langle \Psi_k\rangle_2. \end{aligned} \quad (\text{E3})$$

Similarly, one can show for the conditional state of subsystem 1 with measurement operators A acting on subsystem 2:

$$\begin{aligned} & \text{Tr}_2 \left(\sum_{k,j} c_k c_j^* |k\rangle_1 \langle j| \otimes A_2 |\Psi_k\rangle_2 \langle \Psi_j| A_2^\dagger \right) \\ & = \sum_{k,j} c_k c_j^* |k\rangle_1 \langle j| \langle \Psi_j| A_2^\dagger A_2 |\Psi_k\rangle_2. \end{aligned} \quad (\text{E4})$$

Note that $A^\dagger A$ is a POVM element and the POVM of an on-off detector including dark counts [see \hat{E} of Eq. (A4)] is known in the literature [57] and therefore we do not need to explicitly calculate a corresponding measurement operator A . Moreover, there is no need to explicitly compute the effect of dark counts on the conditional states. This allows us to express all coefficients of the two memories' final density operator in terms of scalar products between coherent states.

If we measure the photon number (without dark counts) on the second optical mode after the beam splitter at the middle station and trace out all other modes, we obtain the following density operator for Alice's and Bob's

qubits:

$$\frac{1}{2}(|\uparrow, \downarrow\rangle\langle\uparrow, \downarrow| + |\downarrow, \uparrow\rangle\langle\downarrow, \uparrow| \pm |\langle\sqrt{1 - \sqrt{\eta}\alpha}e^{i\theta}| \times \sqrt{1 - \sqrt{\eta}\alpha}e^{-i\theta}\rangle|^2(|\uparrow, \downarrow\rangle\langle\downarrow, \uparrow| + |\downarrow, \uparrow\rangle\langle\uparrow, \downarrow|)), \quad (\text{E5})$$

where $|\langle\sqrt{1 - \sqrt{\eta}\alpha}e^{i\theta}|\sqrt{1 - \sqrt{\eta}\alpha}e^{-i\theta}\rangle|^2$ evaluates to $\exp[-4(1 - \sqrt{\eta})\alpha^2 \sin^2 \theta]$. When considering only on-off detectors, the off-diagonal terms change and one additionally needs to take into account a factor of $\frac{\langle -i\sqrt{2\sqrt{\eta}\alpha} \sin \theta | (\mathbb{1} - |0\rangle\langle 0|) | i\sqrt{2\sqrt{\eta}\alpha} \sin \theta \rangle}{e^{2\sqrt{\eta}\alpha^2 \sin^2 \theta} - 1}$, which simplifies to $-e^{-2\sqrt{\eta}\alpha^2 \sin^2 \theta}$. Therefore, we obtain in total $e^{-2(2 - \sqrt{\eta})\alpha^2 \sin^2 \theta}$ as the factor of the off-diagonal terms. This state is a mixture of two Bell states and, for the cases $n > 1$, if we perform (ideal) Bell measurements on all n segments, it is easy to see (due to the Pauli channel argument) that the exponent of the off-diagonal terms in the remaining state (after applying Pauli operations depending on the Bell measurement outcomes) is simply multiplied by n . For Bell-diagonal states with only two nonzero coefficients, it is trivial to check that the distillable entanglement with only one-way classical communication coincides with the asymptotic secret-key fraction of BB84.

When considering also dark counts for the on-off detectors, we obtain the following (unnormalized) state:

	$\langle\uparrow, \uparrow $	$\langle\downarrow, \downarrow $	$\langle\uparrow, \downarrow $	$\langle\downarrow, \uparrow $
$ \uparrow, \uparrow\rangle$	a	c^*	d_1^*	d_2^*
$ \downarrow, \downarrow\rangle$	c	a	d_2	d_1
$ \uparrow, \downarrow\rangle$	d_1	d_2^*	b	f^*
$ \downarrow, \uparrow\rangle$	d_2	d_1^*	f	b

with $a = \langle 0|\hat{E}|0\rangle = 1 - D(0)$, where \hat{E} is the click operator considering dark counts [57] and $D(0)$ is the probability that the detector does not click when a vacuum state is used as the input. Further, we have

$$b = \langle \pm i\sqrt{2\sqrt{\eta}\alpha} \sin \theta | \hat{E} | \pm i\sqrt{2\sqrt{\eta}\alpha} \sin \theta \rangle = 1 - e^{-2\sqrt{\eta}\alpha^2 \sin^2 \theta} D(0), \quad (\text{E6})$$

$$c = \langle \sqrt{1 - \sqrt{\eta}\alpha}e^{-i\theta} | \sqrt{1 - \sqrt{\eta}\alpha}e^{i\theta} \rangle^2 \times \langle \sqrt{2\sqrt{\eta}\alpha}e^{-i\theta} | \sqrt{2\sqrt{\eta}\alpha}e^{i\theta} \rangle a = e^{2\alpha^2[\exp(2i\theta) - 1]} a = ae^{-4\alpha^2 \sin^2 \theta + i2\alpha^2 \sin 2\theta}, \quad (\text{E7})$$

$$d = d_1 = d_2 = \langle \sqrt{1 - \sqrt{\eta}\alpha}e^{-i\theta} | \sqrt{1 - \sqrt{\eta}\alpha}e^{i\theta} \rangle \times \langle \sqrt{2\sqrt{\eta}\alpha} \cos \theta | \sqrt{2\sqrt{\eta}\alpha}e^{i\theta} \rangle \langle 0|\hat{E}|i\sqrt{2\sqrt{\eta}\alpha} \sin \theta \rangle = ae^{-2\alpha^2 \sin^2 \theta + i\alpha^2 \sin 2\theta}, \quad (\text{E8})$$

$$f = |\langle \sqrt{1 - \sqrt{\eta}\alpha}e^{-i\theta} | \sqrt{1 - \sqrt{\eta}\alpha}e^{-i\theta} \rangle|^2 \times \langle i\sqrt{2\sqrt{\eta}\alpha} \sin \theta | \hat{E} | -i\sqrt{2\sqrt{\eta}\alpha} \sin \theta \rangle = e^{-2\alpha^2 \sin^2 \theta (2 - \sqrt{\eta})} [e^{-2\sqrt{\eta}\alpha^2 \sin^2 \theta} - D(0)]. \quad (\text{E9})$$

Note that without dark counts, $a = c = d = 0$, and $D(0) = 1$, we recover the effective 2×2 matrix of the loss-only case. A distinction between d_1 and d_2 has to be made when we consider entanglement swapping strategies which do not double the distance.

Note that the phases of these parameters now also have a $\alpha^2 \sin 2\theta$ dependency, while there was no such dependency in the ideal case without dark counts. If we transform the state into a Bell-diagonal state, we have the parameter c which gives use information about the relative distribution of $|\phi^\pm\rangle$ and this parameter varies periodically with θ . Therefore, it can be useful to apply local transformations for permuting the four Bell-state coefficients [58] in order to obtain a higher secret-key fraction using BB84. When considering a swapping scheme where entanglement swapping is performed between two segments of equal size, one obtains the following set of recursive equations describing the unnormalized two-qubit state (assuming 2^j elementary segments and $|\Phi^+\rangle$ as measurement outcome, while above we considered the case of $j = 0$ and omitted the subscript):

$$\begin{aligned} a_{j+1} &= a_j^2 + b_j^2 + 2\text{Re}(d_j^2), \\ b_{j+1} &= 2[a_j b_j + \text{Re}(d_j^2)], \\ c_{j+1} &= 2d_j^2 + f_j^2 + c_j^{*2}, \\ d_{j+1} &= d_j(a_j + b_j + c_j^*) + d_j^* f_j, \\ f_{j+1} &= 2[|d_j|^2 + f_j \text{Re}(c_j)]. \end{aligned} \quad (\text{E10})$$

Note that for $n = 1$ the BB84 secret-key fraction is not reduced due to discarding the off-diagonal terms in the Bell basis. For $n = 2$, the effect of discarding them is negligibly small. Also note that the approach here that leads to these recursive equations does not yield the same rates as using the protocol version based on the results of Ref. [59] without correlated Pauli operations (see Appendix F 2), because we do not average over all possible Bell measurement outcomes. The calculation of the reduced state considering phase mismatch is completely analogous.

APPENDIX F: ERRORS BEYOND LOSS, HOMODYNE DETECTION

1. Memory dephasing

Let us consider n repeater segments ($n > 1$; otherwise, no memory is needed). We can then assign independent random variables X_j ($j \in \{1, \dots, n\}$) to every segment counting for each the number of attempts until the entanglement is distributed due to a successful measurement outcome of the detector(s) for that segment. These random variables follow a geometric distribution $\mathbb{P}(X = k) = pq^{k-1}$ with $q = 1 - p$, where p is the probability for a successful measurement outcome. We can then introduce a new random variable M , which is a function of the random variables X_j , describing the totally accumulated memory time for which the quantum states dephase. Note that the specific form of the random variable

M differs for different entanglement generation and swapping protocols. In Sec. III B, we only considered a scheme where entanglement distributions in the n segments are done in parallel. In terms of the raw rate, it is clear that such a scheme achieves better rates than any sequential approach. However, when we also consider finite memory times it is no longer obvious whether the parallel scheme still performs better in terms of secret-key rate, because it is possible during the parallel distributions that multiple segments dephase simultaneously, resulting in a longer accumulated memory dephasing time. In contrast, in an appropriate sequential scheme where always only one pair is distributed and swapping is immediately performed as soon as two pairs are present next to each other, at most a single memory pair is subject to a longer dephasing at any time.

In the special case of $n = 2$, it is impossible that multiple memory pairs dephase simultaneously and therefore in terms of secret-key rate the parallel scheme ($M = 2|X_1 - X_2|$) outperforms the sequential one ($M = 2X_2$). The factor two here takes into account the situation when there are two memories dephasing in each segment. It is intuitive that for $n = 2$ the parallel scheme outperforms the sequential one for two reasons. First, in the parallel scheme we only need to wait $\max(X_1, X_2)$ time steps instead of $X_1 + X_2$ in order to distribute entanglement in both segments. Second, the memories also dephase to a lesser extent in the parallel scheme, because in both schemes at most one memory pair has to wait, but in the parallel scheme it is also possible that both segments succeed simultaneously. In general, for n segments, the raw rate in a sequential scheme is given by $\frac{p}{n}$, while in a parallel scheme it is given by $\frac{p}{H(n)}$, where $H(n)$ is the n th harmonic number (assuming $p \ll 1$; see Appendix B). Let us emphasize that this raw rate approximation holds for any memory-based quantum repeater that distributes entanglement in parallel and operates without nested quantum error detection or correction. However, for $n > 2$, it is easy to calculate the average dephasing for the sequential scheme exactly while it is more complicated for the parallel one. In order to calculate it for a parallel scheme, we assume that entanglement swapping is performed when entanglement was distributed in all segments in order to simplify the analysis (see Appendix I). We found that the sequential scheme always gives better secret-key rates than our simple parallel scheme (except for $n = 2$). This comparison is based on both exact and lower bounded dephasing factors for the sequential scheme together with lower bounds on the secret-key fraction for the parallel scheme. Supported by this, whenever memory dephasing is included, we shall consider the parallel scheme for the $n = 2$ case and the sequential scheme otherwise ($n > 2$). Thus, our focus on the sequential scheme for $n > 2$ has two benefits: The secret-key rates can be calculated exactly and they turn out to be better thanks to the reduced total average dephasing. The inferior raw rates, $\frac{p}{n}$ versus $\frac{p}{H(n)}$ for the parallel scheme, appear to have a smaller impact on the secret-key rates (for up to $n = 16$, the difference is a factor smaller than 5).

The resulting random state of a single protocol run with on-off detectors is then given by the density

matrix:

$$\frac{1}{2} \left[1 + e^{-2n(2-\sqrt{\eta})\alpha^2 \sin^2 \theta} \exp\left(-M \frac{\tau}{T}\right) \right] |\Phi^+\rangle\langle\Phi^+| + \frac{1}{2} \left[1 - e^{-2n(2-\sqrt{\eta})\alpha^2 \sin^2 \theta} \exp\left(-M \frac{\tau}{T}\right) \right] |\Phi^-\rangle\langle\Phi^-|, \quad (\text{F1})$$

where τ is the duration of a single entanglement generation attempt in one segment and T is the coherence time of the memory. Note that this state corresponds to the final state shared between Alice and Bob over the total channel distance (while for the case of Alice and Bob immediately measuring their qubits it is an effective rather than a physically occurring state).

The density operator in Eq. (F1) describes the state after a single run, but we are interested in the averaged state. This means we have to calculate the expectation value $\mathbb{E}[\exp(-M \frac{\tau}{T})]$. We calculate this expectation value for the case $n = 2$ for the parallel scheme in Appendix C. In a sequential scheme, the expectation value $\mathbb{E}[\exp(-M \frac{\tau}{T})]$ can be calculated easily for arbitrary n , because M is simply a sum of (independent and identically distributed) geometric random variables, whereas for a parallel scheme it is generally not known how to calculate the expectation value for arbitrary n . In Appendix I, we will discuss a lower bound on the secret-key rate based on Jensen's inequality when using a parallel scheme with arbitrary n .

Since we are here only interested in the secret-key rate, we do not need to consider distributing physical entanglement over the whole distance. This means we can perform the measurement on Alice's and Bob's memories in the beginning with no need to wait until the entanglement is distributed over the whole repeater. For the parallel scheme, this has only a little effect by improving

$$M_{\text{par}} = 2 \sum_{j=1}^n [\max(X_1, \dots, X_n) - X_j] \quad (\text{F2})$$

to

$$M_{\text{par}} = 2 \sum_{j=2}^{n-1} [\max(X_1, \dots, X_n) - X_j] + 2 \max(X_1, \dots, X_n) - X_1 - X_n. \quad (\text{F3})$$

For Eq. (F3), in the segments next to Alice and Bob there is only one memory dephasing instead of two like for Eq. (F2).

In the case of the sequential scheme, we can improve

$$M_{\text{seq}} = 2 \sum_{j=2}^n X_j \quad (\text{F4})$$

to

$$M_{\text{seq}} = \sum_{j=2}^n X_j, \quad (\text{F5})$$

since in the sequential scheme there is always a single segment dephasing where for Eq. (F5) we removed the dephasing in one of the two memories. Therefore, we effectively double the

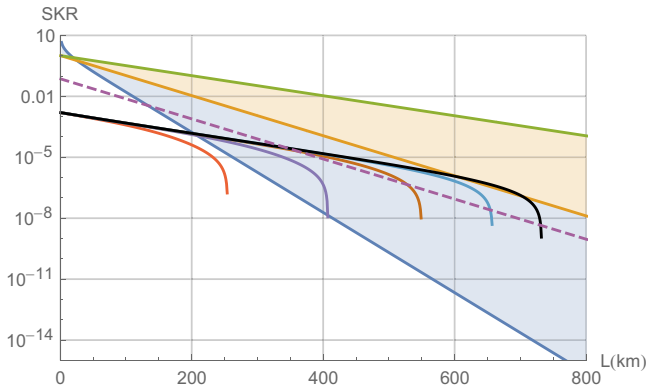


FIG. 7. Secret-key rates for a two-segment repeater ($n = 2$, parallel scheme) without phase mismatch and assuming the parameters as listed in the main text. The straight lines (from bottom to top) denote the PLOB bound, $\sqrt{\eta_{\text{total}}}$, and $\sqrt[4]{\eta_{\text{total}}}$. The rates are for different coherence times T of (1, 10, 100, 1000, ∞) seconds (from left to right). The areas between PLOB and $\sqrt{\eta_{\text{total}}}$ and between $\sqrt{\eta_{\text{total}}}$ and $\sqrt[4]{\eta_{\text{total}}}$ are highlighted in color. The purple dashed line denotes the loss-only case of standard twin-field QKD with perfect detector efficiencies and assuming a coherent-state amplitude optimized for the regime of large loss [20].

memory coherence time for arbitrary n , whereas in the parallel scheme the improvement reduces with increasing segment number n .

Due to the finite memory time, it is useful to consider a cutoff parameter which defines a maximal decoherence time before a state is discarded. For the case of only two segments, we have calculated the expectation value of the dephasing fractions with cutoff. In this paper, the main focus is on repeaters with $n = 2, 3, 4$ repeater segments whose ultimate secret-key rates per channel use scale as $\sqrt[4]{\eta_{\text{total}}}$, $\sqrt[6]{\eta_{\text{total}}}$, and $\sqrt[8]{\eta_{\text{total}}}$, respectively.

2. Dark counts and phase mismatch

With the inclusion of detector dark counts, we need to use the full 4×4 density matrix (in the computational basis) instead of an (effective) 2×2 matrix (in the case without dark counts all matrix elements except a 2×2 submatrix were zero) in order to describe the two-qubit state. Calculating the state before the entanglement swapping is straightforward but lengthy (see Appendix E) and the state after multiple entanglement swappings can be described by a set of recursive relations (see also Appendix E). In order to simplify the analysis, we apply classically correlated Pauli operations to both parts of the imperfect Bell states, such that we erase the off-diagonal terms in the Bell basis [56, Sec. 3.2.1]. We do not need to let the memories dephase additionally for obtaining the classical correlations as required for the correlated Pauli operations, because an entanglement generation attempt takes $\tau = 2 \frac{L_0}{2c}$ in order to send the optical mode to the detector in the middle of the segment (length L_0) and to learn the measurement outcome. If one party sends the bits for establishing classical correlations at the same time as it sends the mode to the detector, then we do not get an additional temporal overhead. As a consequence, this allows us to describe all

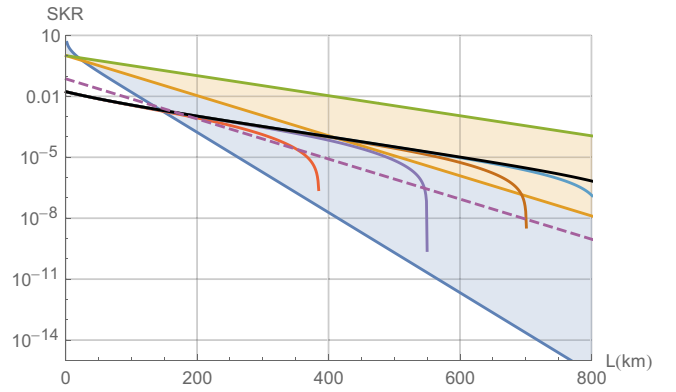


FIG. 8. Secret-key rates assuming the same parameters as in Fig. 7 except for $p_{\text{det}} = 1$ instead of $p_{\text{det}} = 0.15$.

errors as Pauli channels which act onto perfect Bell states. Therefore, we can conduct our analysis as if we perform the entanglement swapping on perfect Bell states and apply all the errors afterward (see Appendix D). Also notice that it is possible to obtain the advantage of a simplified analysis without the need for correlated Pauli operations [59]. In this case, one performs entanglement swapping as usual; i.e., one applies Pauli corrections depending on the measured Bell state, but after the Pauli correction one discards the information about the measurement outcome. Because of this averaging, the teleportation reduces to a Pauli channel. Therefore, we can also interpret our protocol as applying $n - 1$ teleportation steps (each represented by a Pauli channel) onto a non-Bell-diagonal state. Since a channel is linear, we can split the non-Bell-diagonal state into a Bell-diagonal part and a part containing the off-diagonal elements. When applying the Pauli channel to these two parts, we see that the first part is exactly the state we considered in the previous protocol. In the second part, the Bell states are simply permuted by Pauli operations, such that the state after applying the Pauli channels again only contains off-diagonal elements. However, these off-diagonal elements do not matter for the BB84 secret-key rate. Note that these simplifications (applying correlated Pauli operations or discarding the measurement outcome) are at the expense of a worse secret-key rate in comparison to the case without correlated Pauli operations, where we still keep track of the measurement outcome and do not average.

We compared the secret-key fraction of the simplification and the exact case (for $n = 2$) using the parameters as mostly chosen in Sec. IV. For this comparison, we considered loss and dark counts with parameters as in Sec. IV. We found that the relative error increases exponentially with the distance of the total repeater. However, only for distances that are just a bit shorter than the distance where the secret-key fraction drops to zero the relative error becomes relevant, up to the point when the relative error diverges near the point where the secret-key fraction drops to zero. Therefore, we conclude that it is safe to use this simplification when not considering the neighborhood of the point where the secret-key fraction drops to zero.

In order to allow for phase-mismatch errors, which occur, e.g., due to small differences in the laser frequencies and

length fluctuations of the optical path, we model this error by assuming that one party employs a coherent state with amplitude α for generating the hybrid entangled states while the other party uses a coherent state with amplitude $\alpha e^{i\phi}$, where ϕ is a random variable with, for simplicity, a uniform distribution on the interval $(-\frac{\Delta}{2}, \frac{\Delta}{2})$. We also have to bear in mind that this random-phase difference has an influence on the raw rate [depending on $\alpha \sin \theta$] and especially for a small dispersive phase rotation θ the rate can vary up to a few percent. However, the relevant distribution for the secret-key fraction is the probability distribution of ϕ after conditioning onto a detector click. Therefore, the relevant distribution is not uniform anymore but larger values of $|\phi|$ have a larger probability (up to the point where the probability drops to zero). Nevertheless, the difference between the actual and uniform distributions is small. We calculated the Bell-diagonal coefficients and their expectation values with respect to ϕ . However, even for the uniform distribution, it is only possible to calculate the expectation value by numerical integration and therefore one could easily consider a more realistic model for the distribution of the phase difference ϕ .

According to Fig. 9, the phase mismatch can be almost neglected when $\Delta < 0.1\theta$ (this even holds for $\theta = \frac{\pi}{2}$). However, for larger Δ , the secret-key rate drops to zero very fast. For $\Delta = \theta = 0.01$, it is even impossible to obtain a secret key using the above parameters. Therefore, we cannot choose θ arbitrarily small since this increases too much the required precision of the phase matching.

3. Homodyne measurement

In the main part of the paper, we only consider a scenario where Charlie (besides the less practical case of PNRDs) employs an on-off detector. This is similar to previous twin-field QKD schemes. However, it is straightforward to treat homodyne measurements for the two modes instead. Homodyne measurements have the benefit of near-unit efficiencies. When reconsidering Eq. (4), one can see that the state shares some similarities to that of the HQR in Eq. (2). If we can discriminate the peak at 0 from those at $\pm\sqrt{2}\alpha \sin \theta$ in the first mode with a p measurement (imaginary part of $\sqrt{2}\alpha \cos \theta$ versus that of $\sqrt{2}\alpha \exp(\pm i\theta)$ for, recall, $\alpha \in \mathbb{R}^+$), then we learn only that Alice and Bob have different bits but not their values. However, in order to not learn their values by measuring the second mode (to disentangle it from the remaining system), we need to measure the x quadrature in the second mode (real part of $\pm i\sqrt{2}\alpha \sin \theta$). It is also possible to exchange the two modes by which one obtains the same secret-key fraction after a suitable postselection of states. The actual calculation is similar to that with on-off detectors and can be found in Appendix H. Using homodyne measurements, it is not obvious how to define a successful detector event. We will consider an event to be successful if the measurement result of the quadrature p_1 lies within the interval $(-\Delta_p, \Delta_p)$, and the measurement result of x_2 must also occur within the interval $(-\Delta_x, \Delta_x)$. Choosing Δ_x and Δ_p is a compromise between a high raw rate and a high state quality. For a given α and θ , we can reduce the Z -error rate by decreasing Δ_p . One might think that the parameter Δ_x is not relevant and can therefore be set to ∞ . However, this is not true since it also has an influence on

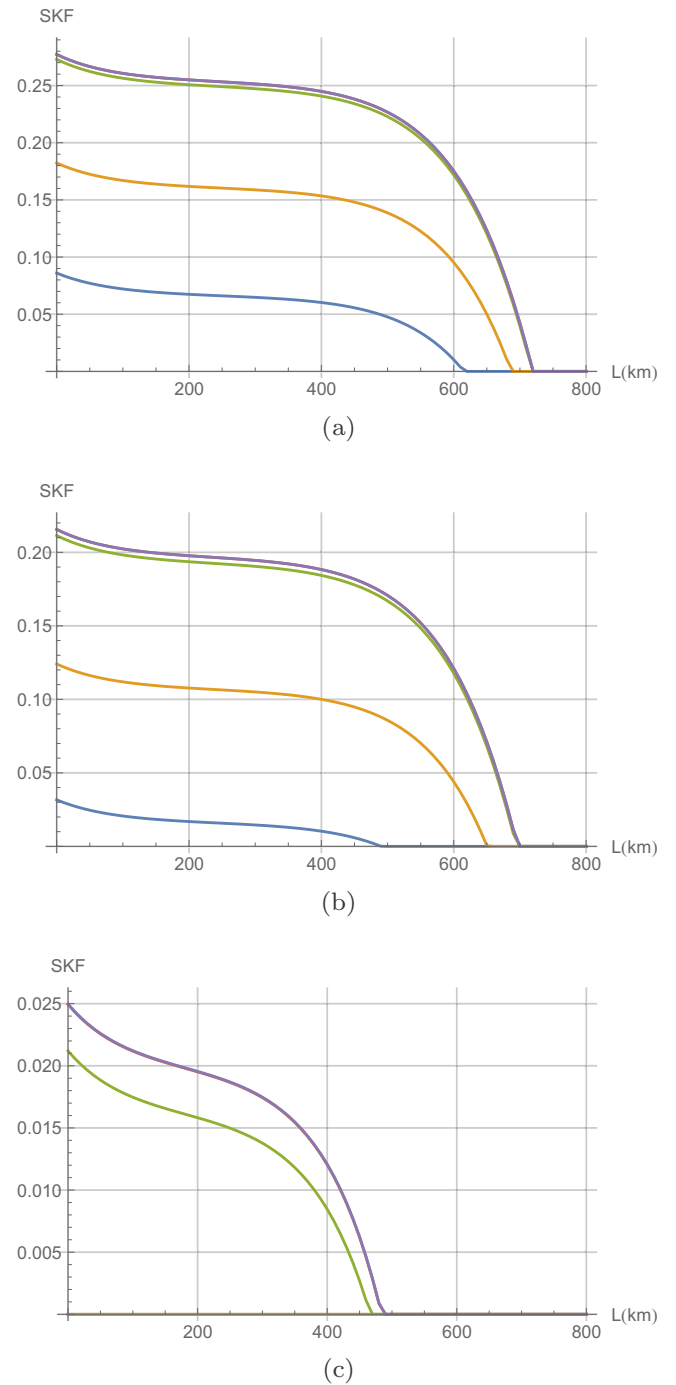


FIG. 9. Secret-key fraction for the two-segment quantum repeater ($n = 2$, parallel scheme) using the parameters discussed in Sec. IV. We choose different memory coherence times for the three different plots and in each plot we consider a phase mismatch Δ of $(0, 10^{-4}, 10^{-3}, 5 \times 10^{-3}, 7.5 \times 10^{-3})$ (from top to bottom). (a) Ideal memories, (b) $T = 10E(M)\tau$, and (c) $T = E(M)\tau$.

the X -error rate, making it even impossible to share a secret key in the no-loss case of $\sqrt{\eta} = 1$ for too large Δ_x . This problem can be solved by simply choosing a sufficiently small Δ_x , but even then a nonzero secret-key rate cannot be obtained for even moderate losses like $\sqrt{\eta} = 0.7$ (about 8 km for the physical segment length assuming perfect detectors).

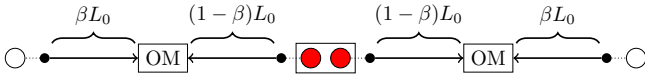


FIG. 10. Asymmetric variation of our proposed scheme for $n = 2$. The beam splitter is placed nearer to the memory station ($\beta > \frac{1}{2}$) such that the overall repetition rate can be increased. Note that for $n > 2$ there is no gain with this variation. Because of this asymmetry, Alice (as well as Bob) and the central memory station have to choose different amplitudes of the coherent states, and we denote the amplitude arriving at the beam splitter by α_{BS} .

APPENDIX G: CALCULATION OF THE QUANTUM REPEATER STATES WITH ASYMMETRIC LINK LENGTHS

In this Appendix, we discuss the obtainable secret-key rates per second in an asymmetric setting (for $n = 2$) where the beam splitters are placed closer to the central memory station and farther away from Alice and Bob. This way, compared with the fully symmetric scheme, repetition rates can be increased (thanks to shorter classical communication times) at the expense of a worse scaling with distance. Similar to the case with symmetric link lengths as discussed in Appendix E, we can calculate the resulting two-qubit state in the asymmetric setting as illustrated in Fig. 10. When we consider the loss-only case, we obtain

$$\begin{aligned}
 a &= c = d = 0, \\
 b &= 1 - \exp(-2\alpha_{BS}^2 \sin^2 \theta), \\
 f &= [\exp(-2\alpha_{BS}^2 \sin^2 \theta) - 1] \exp(-2\alpha_{BS}^2 \sin^2 \theta) \\
 &\quad \times \exp\left(-\alpha_{BS}^2 \exp\left(\frac{L_0}{L_{att}}\right)\right) \left\{ \exp\left(-\frac{L_0\beta}{L_{att}}\right) (1 - e^{-2i\theta}) \right. \\
 &\quad \left. + \exp\left[-\frac{L_0(1-\beta)}{L_{att}}\right] (1 - e^{2i\theta}) - 2[1 - \cos(2\theta)] \right\}. \quad (G1)
 \end{aligned}$$

Here, β describes the asymmetry of the scheme as follows. The distance from Alice and Bob to the beam splitter is given by βL_0 and the distance between the memory and the beam splitter is therefore given by $(1 - \beta)L_0$. Since Alice and Bob have different distances to the beam splitter compared with the memory, both parties need to use different amplitudes in the light-spin entangled states. We choose their amplitudes in such a way that the amplitude at the beam splitter is given in both cases by α_{BS} .

Notice that in this general case f is no longer a real number and it is even possible that $\text{Re}(f) = 0$. Therefore, the secret-key fraction may become zero in this simple error model. As can be seen in Fig. 11, for a fixed total distance, the secret-key rate oscillates with respect to β including an envelope. The oscillations originate from the fact that $\text{Im}(f) \neq 0$ is possible. The envelope takes the following form: For $\beta < \beta_{\max}$ it increases with $\beta_{\max} > \frac{1}{2}$, while it drops when $\beta > \beta_{\max}$. This comes from the gain in repetition rate while not losing too much from the worse scaling per channel use. By further increasing β , the envelope now decreases due to the worse scaling. In the region of $\beta \approx 1$, the secret-key rate per second rapidly increases again, because the repetition rate grows

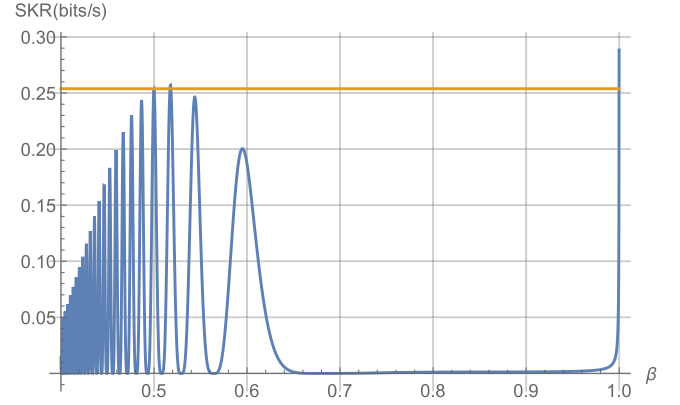


FIG. 11. Secret-key rate per second in the loss-only case of our asymmetric parallel scheme ($n = 2$) for a total distance of 400 km in dependence of the asymmetry parameter β . The constant line is given by the secret-key rate of the symmetric scheme ($\beta = \frac{1}{2}$). We assume that the repetition rate is limited to 10 MHz because of local operation times. In this case, we can comfortably beat the symmetric scheme for strong asymmetry ($\beta \rightarrow 1$); however, this almost resembles the twin-field QKD configuration where GHz repetition rates can be used in principle. Also note that for a maximal repetition rate of 1 MHz the completely asymmetric scheme no longer outperforms the symmetric one.

quickly up to the point where it is limited by the possible repetition rate of the light source. Because of the oscillations, it is necessary to optimize β for any given total distance. When considering increasing distances, β_{\max} moves nearer to $\frac{1}{2}$ and the advantage compared to the symmetric case of $\beta = \frac{1}{2}$ becomes less pronounced. For total distances of 200 km, we can increase the secret-key rate by 4.6%, while for a total distance of 400 km we only gain 1.1%.

APPENDIX H: CALCULATION OF THE QUANTUM REPEATER STATES WITH HOMODYNE MEASUREMENTS

Let us first start with the no-loss case and again consider the state

$$\begin{aligned}
 &\frac{1}{2}(|\uparrow, \uparrow, \alpha e^{-i\theta}, \alpha e^{-i\theta}\rangle + |\downarrow, \downarrow, \alpha e^{i\theta}, \alpha e^{i\theta}\rangle \\
 &\quad + |\downarrow, \uparrow, \alpha e^{i\theta}, \alpha e^{-i\theta}\rangle + |\uparrow, \downarrow, \alpha e^{-i\theta}, \alpha e^{i\theta}\rangle). \quad (H1)
 \end{aligned}$$

After applying the beam splitter and the measurements of $\hat{p}_1 = p$ and $\hat{x}_2 = x$, we have the conditional two-qubit state (after tracing out the optical modes)

$$\begin{aligned}
 &\frac{1}{2}(|\uparrow, \uparrow\rangle \langle \hat{p} = p | \sqrt{2}\alpha e^{-i\theta}\rangle \langle \hat{x} = x | 0\rangle \\
 &\quad + |\downarrow, \downarrow\rangle \langle \hat{p} = p | \sqrt{2}\alpha e^{i\theta}\rangle \langle \hat{x} = x | 0\rangle \\
 &\quad + |\downarrow, \uparrow\rangle \langle \hat{p} = p | \sqrt{2}\alpha \cos \theta\rangle \langle \hat{x} = x | i\sqrt{2}\alpha \sin \theta\rangle \\
 &\quad + |\uparrow, \downarrow\rangle \langle \hat{p} = p | \sqrt{2}\alpha \cos \theta\rangle \langle \hat{x} = x | -i\sqrt{2}\alpha \sin \theta\rangle). \quad (H2)
 \end{aligned}$$

As the next step, we calculate position- and momentum-space wave functions of a coherent state with amplitude $x_0 + ip_0$. In order to express these wave functions in terms of vacuum-state wave functions of the harmonic oscillator, we will make use of the displacement operator ($\hbar = \frac{1}{2}$ in our notation) and the

Baker-Campbell-Hausdorff formula:

$$\begin{aligned}
\langle \hat{x} = x | x_0 + ip_0 \rangle &= \langle \hat{x} = x | \exp[(x_0 + ip_0)(\hat{x} - i\hat{p}) - (x_0 - ip_0)(\hat{x} + i\hat{p})] | 0 \rangle \\
&= \langle \hat{x} = x | \exp[2i(p_0\hat{x} - x_0\hat{p})] | 0 \rangle \\
&= \langle \hat{x} = x | \exp(2ip_0\hat{x}) \exp(-2ix_0\hat{p}) \exp(-ip_0x_0) | 0 \rangle \\
&= \langle \hat{x} = x - x_0 | 0 \rangle \exp\left[2ip_0\left(x - \frac{x_0}{2}\right)\right] \\
&= \sqrt{\frac{2}{\pi}} \exp\left[-(x - x_0)^2\right] \exp\left[2ip_0\left(x - \frac{x_0}{2}\right)\right]. \quad (\text{H3})
\end{aligned}$$

Similarly, one can show

$$\begin{aligned}
\langle \hat{p} = p | x_0 + ip_0 \rangle &= \sqrt{\frac{2}{\pi}} \exp[-(p - p_0)^2] \\
&\quad \times \exp\left[-2ix_0\left(p - \frac{p_0}{2}\right)\right]. \quad (\text{H4})
\end{aligned}$$

We postselect onto states where $p \in (-\Delta_p, \Delta_p)$ and $x \in (-\Delta_x, \Delta_x)$. Further, we label the density matrix elements in the same way as in the case with on-off detectors (see Appendix E) and we obtain the following results (all elements must be divided by the matrix trace, $2(a + b)$, for normalization; for brevity we also omitted some extra factors which cancel anyway then through normalization),

$$a = \frac{1}{2} [\text{erf}(\sqrt{2}\Delta_p - 2\alpha \sin \theta) + \text{erf}(\sqrt{2}\Delta_p + 2\alpha \sin \theta)], \quad (\text{H5})$$

$$b = \text{erf}(\sqrt{2}\Delta_p), \quad (\text{H6})$$

$$c = \exp(2\alpha^2[-1 + \exp(2i\theta)]) \text{erf}(\sqrt{2}\Delta_p), \quad (\text{H7})$$

$$f = \exp(-4\alpha^2 \sin^2 \theta) \text{erf}(\sqrt{2}\Delta_p) \frac{\text{Re}[\text{erf}(\sqrt{2}\Delta_x + 2i\alpha \sin \theta)]}{\text{erf}(\sqrt{2}\Delta_x)}. \quad (\text{H8})$$

When including loss, we can make use of Eq. (E3), and after simplifications one can see that the expressions for a, b, c, f almost stay the same. We only have to replace $\alpha \rightarrow \alpha \sqrt{\sqrt{\eta}}$ within the erf functions and otherwise nothing changes where $\sqrt{\eta}$ is the transmission parameter corresponding to one physical segment (half a repeater segment). For example, for $n = 1$, we have $\alpha \rightarrow \sqrt[4]{\eta_{\text{total}}}\alpha$. Using the expressions a, b, c, f we can then calculate the BB84 secret-key fraction as before (we did not explicitly calculate d_1 and d_2 , because we only need their values when considering $n > 1$ and also not discarding the off-diagonal terms in the Bell basis).

APPENDIX I: DIFFERENT DISTRIBUTION AND SWAPPING STRATEGIES

Let us discuss the effects of memory dephasing for the sequential and a parallel entanglement distribution schemes. First of all, we have to point out that the choice of M_{par} is not optimal for more than two segments, because it assumes that the entanglement swapping operations are performed at the end, only after the entanglement distributions in all segments have succeeded. To illustrate this point, let us consider the example that first two adjacent segments succeeded and we

have to wait one more time step until all the other segments succeeded so that we can perform all swapping operations. This means the value of M would be 4, because two segments (with two memories each) waited for one time step. Instead, we could also consider the case that we first perform the swapping operation on the two segments immediately after their successful creations and after the extra single time step we perform the remaining swapping operations. As a consequence, the value of M is only 2, because only two memories waited for one time step. This means it is beneficial to swap as soon as possible in order to keep the number of dephasing memories low.⁸

Unfortunately, it is currently not even known how to calculate the probability distribution of $M = M_{\text{par}}$ for $n > 2$ in the simple case where we wait for the success of all segments before performing the swapping operations. If we want to consider more than two segments in a parallel distribution scheme, however, we can use the bound $\mathbb{E}[\exp(-M\frac{\tau}{T})] \geq \exp[-\mathbb{E}(M)\frac{\tau}{T}]$ which can be obtained by applying Jensen's inequality. As the expectation value operation is linear, we can easily calculate $\mathbb{E}(M)$ since the exact $\mathbb{E}[\max(X_1, \dots, X_n)]$ is already known in the literature [44], and we obtain [for the case when Alice and Bob do not store their halves, so for M from Eq. (F3)]:

$$\mathbb{E}(M_{\text{par}}) = 2(n-1) \left[\sum_{j=1}^n \binom{n}{j} \frac{(-1)^{j+1}}{1 - q^j} - \frac{1}{p} \right], \quad (\text{I1})$$

also using the well-known result for a geometrically distributed variable, $\mathbb{E}(X_j) = \frac{1}{p}$, $\forall j = 1 \dots n$. We can use the inequality in order to obtain a lower bound on the secret-key fraction. However, one needs to bear in mind that this is only a lower bound that becomes very loose in the regime of bad memories. For the simple case of $n = 2$, we calculated $\exp[-\mathbb{E}(M)\frac{\tau}{T}]$ and $\mathbb{E}[\exp(-M\frac{\tau}{T})]$ (see Appendix C) and compared their corresponding secret-key fractions (assuming $p = 10^{-4}$, $\sqrt{\eta} \ll 1$). For the case of $T = 10\mathbb{E}(M)\tau$, we found that the exact calculation yields a 1% higher secret-key rate. When considering $T = \mathbb{E}(M)\tau$, the error increased to 86% and when looking at memories with $T = 0.1\mathbb{E}(M)\tau$ the approximation underestimated the secret-key fraction by six orders of magnitude, although the exact secret-key fraction of 2×10^{-3} was not ridiculously low. Numerical simulations show that the bound becomes tighter for an increasing number of repeater segments. Unfortunately, realistic coherence times are often too small for obtaining a good bound by applying Jensen's inequality.

Let us now discuss the difference between a sequential and a parallel scheme with respect to the secret-key fraction. In order to be sure that improvements in the state quality arise from the changed strategy and not only from using the exact

⁸However, note that if we assumed probabilistic entanglement swapping instead of a deterministic one, swapping as soon as possible would yield a nonoptimal raw rate, because one does not want to perform many entanglement swapping operations between entangled pairs of long and short distances since if the operation fails all involved segments have to start from scratch.

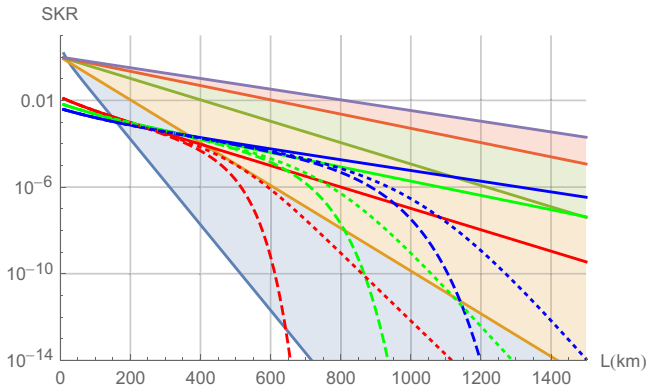


FIG. 12. Secret-key rate for a repeater with $n = 2$ (red), 3 (green), and 4 (blue) (from left to right in terms of dropping secret-key rate) segments using a sequential protocol ($\alpha = 23.9$ in all cases). The solid lines show the ideal loss-only case ($p_{\text{det}} = 1$), while the dashed lines correspond to the case where we additionally consider a finite memory coherence time of 10 s. The dotted lines use the exact expression for the expectation value of the dephasing. The benchmarks (from bottom to top) PLOB, $\sqrt{\eta_{\text{tot}}}$, $\sqrt[4]{\eta_{\text{tot}}}$, $\sqrt[3]{\eta_{\text{tot}}}$, and $\sqrt[5]{\eta_{\text{tot}}}$ can also be seen. The regions between two of those benchmarks are highlighted in color.

expression instead of a lower bound, we will now also compare the two strategies using for both the lower bound based on Jensen's inequality (for the sequential scheme, in addition, we use the exact rates). For simplicity, let us consider the case where Alice and Bob perform the measurements on their qubits at the end after the entanglement was distributed over the whole distance and define the random variable $M_{\text{seq}} := 2 \sum_{j=2}^n X_j$ (in the other case, the sequential scheme also has a larger improvement than the parallel one). We then have

$$\mathbb{E}[M_{\text{seq}}] = 2 \frac{n-1}{p}, \quad (12)$$

$$\mathbb{E}[M_{\text{par}}] \approx 2n \frac{H(n) - 1}{p}, \quad (13)$$

where M_{par} is taken from Eq. (F2) and we used the approximation for the parallel scheme derived in Appendix B, assuming $p \ll 1$. For $n = 2$, the protocols are the same and it can easily be checked that the sequential protocol is better for $n \geq 3$. Better here means that less memory time is needed leading to a better secret-key fraction. Which protocol is the best in terms of the secret-key rate also depends on the memory coherence time T . If we have perfect memories ($T = \infty$), we do not gain any advantage due to the sequential protocol, but we have the

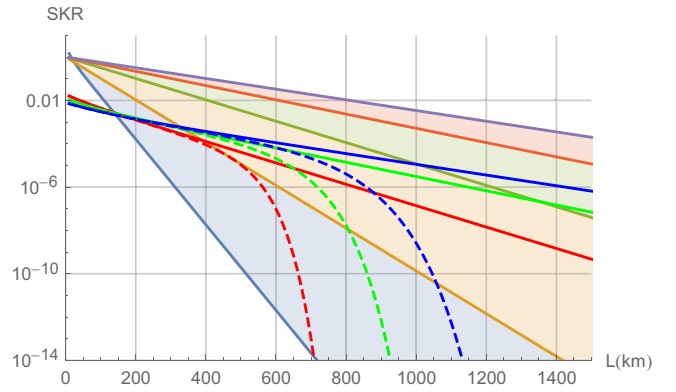


FIG. 13. Secret-key rate for a repeater with $n = 2$ (red), 3 (green), and 4 (blue) (from left to right in terms of dropping secret-key rate) segments using a parallel protocol ($\alpha = 23.9$ in all cases). The solid lines show the ideal loss-only case ($p_{\text{det}} = 1$), while the dashed lines correspond to the case where we additionally consider a finite memory coherence time of 10 s using Jensen's inequality. The benchmarks (from bottom to top) PLOB, $\sqrt{\eta_{\text{tot}}}$, $\sqrt[4]{\eta_{\text{tot}}}$, $\sqrt[3]{\eta_{\text{tot}}}$, and $\sqrt[5]{\eta_{\text{tot}}}$ can also be seen. The regions between two of those benchmarks are highlighted in color.

disadvantage of a lower raw rate ($\frac{p}{n}$ versus $\frac{p}{H(n)}$), resulting in a lower overall secret-key rate. Note that for $n = 2$ when we use the exact dephasing expressions for both the parallel and the sequential schemes, the parallel one even has a smaller dephasing than the sequential one, as already pointed out in Appendix F.

The obtainable secret-key rate using Jensen's inequality for the sequential and parallel protocols with a memory coherence time of 10 s can be seen in Figs. 12 and 13. It can be seen that for $n = 2$ the parallel scheme is superior, because both schemes have the same amount of dephasing but the parallel scheme has a better raw rate. However, for $n = 3$ the rates of both schemes are quite similar and for $n = 4$ the sequential scheme outperforms the parallel one as one might anticipate due to the better dephasing. Clearly, when using the exact expression for the dephasing in the sequential scheme, we obtain significantly better rates than for the parallel scheme with rates calculated from the lower bound. However, for $n > 2$, the rates of the sequential scheme based on the lower bound are still at least as good or even better ($n > 3$) than those for the parallel scheme. This is our motivation for employing the sequential scheme throughout whenever we consider $n > 2$ (besides the benefit that this allows us to compute the exact rates also for larger schemes, $n > 2$).

- [1] C. H. Bennett and G. Brassard, *Theor. Comput. Sci.* **560**, 7 (2014).
 [2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, [arXiv:1906.01645](https://arxiv.org/abs/1906.01645).

- [3] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussi eres, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, *Phys. Rev. Lett.* **121**, 190502 (2018).
 [4] M. Takeoka, S. Guha, and M. M. Wilde, *Nat. Commun.* **5**, 5235 (2014).

- [5] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Nat. Commun.* **8**, 15043 (2017).
- [6] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **81**, 5932 (1998).
- [7] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, *Nature (London)* **414**, 413 (2001).
- [8] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, *Phys. Rev. Lett.* **112**, 250501 (2014).
- [9] F. Ewert, M. Bergmann, and P. van Loock, *Phys. Rev. Lett.* **117**, 210501 (2016).
- [10] K. Azuma, K. Tamaki, and H.-K. Lo, *Nat. Commun.* **6**, 6787 EP (2015).
- [11] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, *Nat. Photon.* **6**, 777 (2012).
- [12] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin, *Nature (London)* **580**, 60 (2020).
- [13] H.-K. Lo, M. Curty, and K. Tamaki, *Nat. Photon.* **8**, 595 (2014).
- [14] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, *Rev. Mod. Phys.* **92**, 025002 (2020).
- [15] D. Mayers and A. Yao, *Quantum Inf. Comput.* **4**, 273 (2004).
- [16] U. Vazirani and T. Vidick, *Phys. Rev. Lett.* **113**, 140501 (2014).
- [17] S. L. Braunstein and S. Pirandola, *Phys. Rev. Lett.* **108**, 130502 (2012).
- [18] H.-K. Lo, M. Curty, and B. Qi, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [19] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, *Nature (London)* **557**, 400 (2018).
- [20] J. Lin and N. Lütkenhaus, *Phys. Rev. A* **98**, 042332 (2018).
- [21] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, [arXiv:1805.05511](https://arxiv.org/abs/1805.05511).
- [22] X. Ma, P. Zeng, and H. Zhou, *Phys. Rev. X* **8**, 031043 (2018).
- [23] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, *Phys. Rev. A* **98**, 062323 (2018).
- [24] M. Curty, K. Azuma, and H.-K. Lo, *npj Quantum Inf.* **5**, 64 (2019).
- [25] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, *Phys. Rev. Appl.* **11**, 034053 (2019).
- [26] F. Grasselli and M. Curty, *New J. Phys.* **21**, 073001 (2019).
- [27] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, *Phys. Rev. X* **9**, 021046 (2019).
- [28] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, *Phys. Rev. Lett.* **123**, 100505 (2019).
- [29] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, *Phys. Rev. Lett.* **123**, 100506 (2019).
- [30] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, *Nat. Photon.* **13**, 334 (2019).
- [31] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, Z. Wang, L. You, M.-J. Li, H. Chen, Y.-A. Chen, Q. Zhang, C.-Z. Peng, X. Ma, T.-Y. Chen, and J.-W. Pan, [arXiv:1908.01271](https://arxiv.org/abs/1908.01271).
- [32] F. Rozpędek, R. Yehia, K. Goodenough, M. Ruf, P. C. Humphreys, R. Hanson, S. Wehner, and D. Elkouss, *Phys. Rev. A* **99**, 052330 (2019).
- [33] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, *Phys. Rev. Lett.* **96**, 240501 (2006).
- [34] P. van Loock, N. Lütkenhaus, W. J. Munro, and K. Nemoto, *Phys. Rev. A* **78**, 062319 (2008).
- [35] N. K. Bernardes and P. van Loock, *Phys. Rev. A* **86**, 052301 (2012).
- [36] E. Schrödinger, *Naturwissenschaften* **23**, 807 (1935).
- [37] S. Haroche, *Rev. Mod. Phys.* **85**, 1083 (2013).
- [38] P. C. Haljan, K.-A. Brickman, L. Deslauriers, P. J. Lee, and C. Monroe, *Phys. Rev. Lett.* **94**, 153602 (2005).
- [39] J.-Q. Liao, Y. Guo, H.-S. Zeng, and L.-M. Kuang, *J. Phys. B: At. Mol. Opt. Phys.* **39**, 4709 (2006).
- [40] S. A. Aljunid, M. K. Tey, B. Chng, T. Liew, G. Maslennikov, V. Scarani, and C. Kurtsiefer, *Phys. Rev. Lett.* **103**, 153601 (2009).
- [41] M. Fischer, B. Srivathsan, L. Alber, M. Weber, M. Sondermann, and G. Leuchs, *Appl. Phys. B* **123**, 48 (2017).
- [42] C. Gerry and P. Knight, in *Introductory Quantum Optics* (Cambridge University Press, Cambridge, UK, 2004), pp. 308–311.
- [43] B. Hacker, S. Welte, S. Daiss, A. Shaikat, S. Ritter, L. Li, and G. Rempe, *Nat. Photon.* **13**, 110 (2019).
- [44] N. K. Bernardes, L. Praxmeyer, and P. van Loock, *Phys. Rev. A* **83**, 012323 (2011).
- [45] C. Cabillo, J. I. Cirac, P. García-Fernández, and P. Zoller, *Phys. Rev. A* **59**, 1025 (1999).
- [46] S. Pirandola, *Commun. Phys.* **2**, 51 (2019).
- [47] H.-K. Lo, H. Chau, and M. Ardehali, *J. Cryptol.* **18**, 133 (2005).
- [48] P. van Loock, W. Alt, C. Becher, O. Benson, H. Boche, C. Deppe, J. Eschner, S. Höfling, D. Meschede, P. Michler, F. Schmidt, and H. Weinfurter, *Adv. Quantum Technol.* (to be published).
- [49] P. Wang, C.-Y. Luan, M. Qiao, M. Um, J. Zhang, Y. Wang, X. Yuan, M. Gu, J. Zhang, and K. Kim, [arXiv:2008.00251](https://arxiv.org/abs/2008.00251).
- [50] F. Rozpędek, K. Goodenough, J. Ribeiro, N. Kalb, V. C. Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D. Elkouss, *Quantum Sci. Technol.* **3**, 034002 (2018).
- [51] S. Santra, L. Jiang, and V. S. Malinovsky, *Quantum Sci. Technol.* **4**, 025010 (2019).
- [52] O. A. Collins, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy, *Phys. Rev. Lett.* **98**, 060502 (2007).
- [53] E. Shchukin, F. Schmidt, and P. van Loock, *Phys. Rev. A* **100**, 032322 (2019).
- [54] L. Praxmeyer, [arXiv:1309.3407](https://arxiv.org/abs/1309.3407).
- [55] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, *Sci. Rep.* **6**, 20463 (2016).
- [56] W. Dür and H. J. Briegel, *Rep. Prog. Phys.* **70**, 1381 (2007).
- [57] P. Kok and B. W. Lovett, *Introduction to Optical Quantum Information Processing* (Cambridge University Press, Cambridge, UK, 2010).
- [58] J. Dehaene, M. Van den Nest, B. De Moor, and F. Verstraete, *Phys. Rev. A* **67**, 022310 (2003).
- [59] G. Bowen and S. Bose, *Phys. Rev. Lett.* **87**, 267901 (2001).

Paper II

Extending Quantum Links: Modules for Fiber- and Memory-Based Quantum Repeaters

Peter van Loock, Wolfgang Alt, Christoph Becher, Oliver Benson, Holger Boche,
Christian Deppe, Jürgen Eschner, Sven Höfling, Dieter Meschede, Peter Michler,
Frank Schmidt, and Harald Weinfurter

Advanced Quantum Technologies **3** (11), 1900141 (2020)

Extending Quantum Links: Modules for Fiber- and Memory-Based Quantum Repeaters

Peter van Loock,* Wolfgang Alt, Christoph Becher, Oliver Benson, Holger Boche, Christian Deppe, Jürgen Eschner, Sven Höfling, Dieter Meschede,* Peter Michler, Frank Schmidt, and Harald Weinfurter

Elementary building blocks for quantum repeaters based on fiber channels and memory stations are analyzed. Implementations are considered for three different physical platforms, for which suitable components are available: quantum dots, trapped atoms and ions, and color centers in diamond. The performances of basic quantum repeater links for these platforms are evaluated and compared, both for present-day, state-of-the-art experimental parameters as well as for parameters that can in principle be reached in the future. The ultimate goal is to experimentally explore regimes at intermediate distances—up to a few 100 km—in which the repeater-assisted secret key transmission rates exceed the maximal rate achievable via direct transmission. Two different protocols are considered, one of which is better adapted to the higher source clock rate and lower memory coherence time of the quantum dot platform, while the other circumvents the need of writing photonic quantum states into the memories in a heralded, nondestructive fashion. The elementary building blocks and protocols can be connected in a modular form to construct a quantum repeater system that is potentially scalable to large distances.

1. Introduction

Quantum key distribution (QKD) and related schemes are offering a paradigm change in establishing secure communication: algorithmic security is replaced by physically secure generation of encryption keys.^[1] The symmetric keys created by QKD can be used to securely transmit messages between two stations (Alice and Bob) via public channels. Security is warranted by physically detecting any eavesdropping attack. To generate a key, the iconic BB84 protocol^[2] employs nonorthogonal quantum states of photons carrying qubit information, while other schemes make use of measuring entangled photon pairs, such as the Ekert protocol.^[3] More generally, establishing entanglement of distant quantum objects provides a critical resource for efficient distribution of quantum information, both at short and long distances;

Prof. P. van Loock, F. Schmidt
Institute of Physics
Johannes Gutenberg University Mainz
Staudingerweg 7, Mainz 55128, Germany
E-mail: loock@uni-mainz.de

Dr. W. Alt, Prof. D. Meschede
Institute of Applied Physics
University of Bonn
Wegelerstraße 8, Bonn 53115, Germany
E-mail: meschede@uni-bonn.de

Prof. C. Becher, Prof. J. Eschner
Fachrichtung Physik
Universität des Saarlandes
Campus E2.6, Saarbrücken 66123, Germany


Prof. O. Benson
Institut für Physik
Humboldt-Universität zu Berlin
Newtonstr. 15, Berlin 12489, Germany

Prof. O. Benson
IRIS Adlershof
Humboldt-Universität zu Berlin
Zum Großen Windkanal 6, Berlin 12489, Germany

Prof. H. Boche
Lehrstuhl für Theoretische Informationstechnik
Technische Universität München
München 80290, Germany

Prof. H. Boche
Munich Center for Quantum Science and Technology (MCQST)
München 80799, Germany

Dr. C. Deppe
Lehrstuhl für Nachrichtentechnik
Technische Universität München
München 80290, Germany
(Affil Cont)

 The ORCID identification number(s) for the author(s) of this article can be found under <https://doi.org/10.1002/qute.201900141>

© 2020 The Authors. Published by Wiley-VCH GmbH. This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

DOI: 10.1002/qute.201900141

(affiliation continued on next page)

applications beyond quantum cryptography, such as distributed quantum information processing and future quantum networks,^[4] will also depend on this resource.

Networks based on individual point-to-point links (PPLs) over 50–80 km length have been realized at the metropolitan area level, and even a long distance connecting Beijing and Shanghai (≈ 2.000 km) has been bridged via 32 intermediate stations.^[5] So far, however, such networks rely on independent quantum PPLs chained together by “trusted nodes,” connecting the links by classical operations (“receive and resend”) and thus providing full access to the transmitted bits at each node. Truly long-range quantum links have been realized via satellite channels,^[6] yet up to now also the satellites serve as trusted nodes in such schemes. Moreover, since these links require large-scale send-and-receive facilities, it is likely that they need to be combined with “local-area” ground-based quantum networks (of a smaller, intermediate range) as obtainable from the elementary fiber-based schemes presented and discussed here.

At present the main obstacle in establishing large-scale quantum networks are inherent losses of the transmission channels. The current record for terrestrial, fiber-based point-to-point QKD lies in the range of about 400 km.^[7,8] As a consequence,^[9] secret key rates (SKRs) obtained via direct transmission (without intermediate stations) through an optical quantum channel of length L are effectively limited by the channel transmission efficiency $\eta = \exp(-L/L_{\text{att}})$ for large L where L_{att} is the attenuation length of the channel.^[10] More precisely, this limit corresponds to a secret key capacity of 1.44η (per channel use and per mode, in units of secret bits^[11]),^[12] In particular, optical fiber systems feature a loss rate of about 0.2 dB km^{-1} (corresponding to $L_{\text{att}} = 22 \text{ km}$), limiting useful distances to a few hundred km (Figure 1).

There are interesting methods to overcome this limitation without the use of quantum memories by sending fairly simple quantum states (in the form of single photons or optical coherent states) to a detector station placed in the middle of

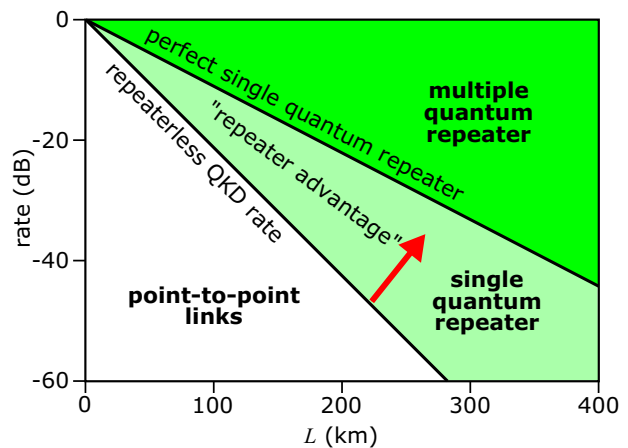


Figure 1. QKD rate in dB (normalized to the protocol’s clock rate) as a function of distance in km. Point-to-point protocols scale as $\sim \eta = \exp(-L/L_{\text{att}})$, limited by the “repeaterless” bound.^[12] For telecom fibers: $L_{\text{att}} = 22 \text{ km}$. An ideal “single” quantum repeater with only one middle station^[13] scales as $\sim \sqrt{\eta} = \exp(-L/2L_{\text{att}})$. “Multiple” repeaters may further reduce the effective loss and extend the transmission distance. The exact “repeaterless” bound (secret key capacity) is $-\log_2(1-\eta) \approx 1.44\eta$ in units of secret bits,^[12] where the approximation only holds for sufficiently small η (large distances).

the channel.^[14,15] Especially the “twin-field QKD” concept^[15] is appealing, as it needs^[16] neither multiple parallel channel transmissions nor nondestructive measurements with feedforward and multiplexing,^[14] but instead only transmission of phase-sensitive single-mode quantum states and their interference at the middle station. Experimental proof-of-principle demonstrations of the twin-field concept were reported very recently.^[17–19] Both approaches^[14,15] reduce the effective channel length by a factor of two, corresponding to an enhanced transmission efficiency of $\sqrt{\eta} = \exp[-(L/2)/L_{\text{att}}]$. However, neither of them has been shown to be scalable to larger distances by further improving the effective transmission. In principle, there are other, all-optical approaches for long-distance, even scalable quantum communication with no need for storing qubits in matter-based memories, but such schemes depend on the engineering of complex multiphoton (entangled) quantum states and a sufficiently close spacing of stations along the channel (every 1–5 km) in order to exploit the sophisticated concept of quantum error correction codes.^[20]

Therefore, it is currently assumed that the most feasible and promising route toward long-distance quantum communication, while entirely avoiding trusted node configurations, is based upon the use of quantum repeaters (QRs)^[21] that include intermediate stations (typically every 10–100 km) equipped with quantum memories realized by atomic or solid-state qubits. Here, we consider elementary fiber- and memory-based schemes, which we refer to as quantum repeater cells (QR cells). By storing quantum states for sufficiently long, these schemes allow to enter the rate regime^[13] between η and $\sqrt{\eta}$ and may serve as modular building blocks for bridging larger distances. Thus, ultimately, true quantum networks based on quantum repeaters should not only eliminate the need to trust the stations along the channels of the network but also achieve a QKD rate scaling with distance at least as efficient as a trusted relay or

Prof. S. Höfling
Technische Physik
Physikalisches Institut und Wilhelm Conrad Röntgen Center for Complex Material Systems
Universität Würzburg
Am Hubland, Würzburg 97074, Germany

Prof. P. Michler
Institut für Halbleitertechnik und Funktionelle Grenzflächen (IHFG)
Center for Integrated Quantum Science and Technology (IQST) and SCoPE
University of Stuttgart
Allmandring 3, Stuttgart 70569, Germany

Prof. H. Weinfurter
Fakultät für Physik
Ludwig-Maximilians-Universität München
Schellingstr. 4, München 80799, Germany

Prof. H. Weinfurter
Munich Center for Quantum Science and Technology (MCQST)
München 80799, Germany

Prof. H. Weinfurter
Max-Planck Institut für Quantenoptik
Hans-Kopfermann-Str. 1, Garching 85748, Germany

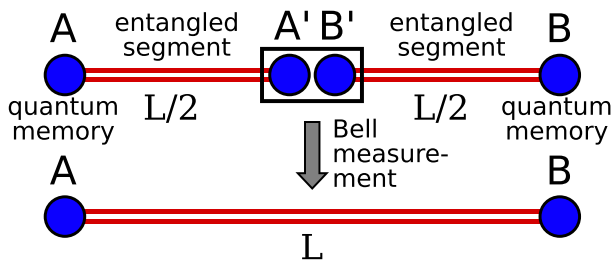


Figure 2. Generic QR link for increasing the communication distance. Initially, for each segment AA' and B'B, quantum memories (full circles) are entangled with each other (double red line) over a distance $L/2$. Via a Bell-state measurement (black box) on the two memories in the central repeater node, the entanglement is swapped to the outer memories A and B separated by distance L . Thus, a new, longer segment is created that is usable for further extensions of the quantum link by repeated concatenation of this procedure including some form of quantum error detection or correction.

an entanglement distribution rate scaling more efficient than a quantum relay where each node only measures optical quantum states without storing them. Compared with quantum PPLs chained together by trusted nodes and other forms of quantum relays, genuine repeater-based quantum networks would thus represent a leap both conceptually and quantitatively.

The first QR concepts were proposed already 20 years ago^[21] to overcome the distance limitation by distributing, enhancing, and connecting short-range entanglement through local quantum operations and classical communication. In the simplest case, quantum correlations from two entangled point-to-point segments AA' and B'B are connected via a collective Bell-state measurement (BM) at the central "repeater" node A'B', resulting in so-called entanglement swapping to nodes A and B (Figure 2). These larger segments can then be concatenated further in the same way, while a simple multiplication of the channel transmission efficiencies per segment and a propagation and accumulation of errors can be prevented by storing quantum information in quantum memories and applying entanglement purification on many entangled pairs in each segment^[21] or incorporating quantum error correction codes into the memory qubits.^[20] Overcoming the distance and rate limitations in a scalable fashion, QRs offer highly attractive functionality for future long-range quantum networks.^[22]

Experimentally, QRs have remained an enormous challenge up to now.^[20,23] A QR constitutes a system based on several different hardware components. Although all necessary components have been demonstrated to some extent individually, combining these into a fully operational (and hence scalable) repeater system is demanding and first experimental demonstrations in this direction are now only beginning to be reported.^[24]

One of the most critical hardware components are the quantum memories required to effectively synchronize the arrival of quantum information for further processing at the individual nodes. Depending on the range and the application of the repeater system, the required memory coherence times vary. For example, in order to establish entanglement over 1000 km via a standard QR^[21] at least millisecond storage times are needed only to be able to cover the waiting time for a classical signal sent over the total distance. In a fully nested quantum repeater with proba-

bilistic entanglement purification and swapping steps including two-way classical communication, even longer storage times will be required.^[25] Deterministic entanglement swapping and quantum error correction of local gate and memory errors may reduce these requirements,^[20] but most memory systems are still not sufficiently long-lived or fault-tolerant.^[26]

Here we analyze small-scale, functional QR systems that may serve as elementary building blocks for experimental QR realizations on a larger scale. Implementations are considered for three different physical platforms, for which suitable components are available: quantum dots, trapped atoms and ions, and color centers in diamond. The aim of these elementary schemes is to experimentally approach a regime at intermediate distances (up to several 100 km) in which the qubit transmission and secret key rates exceed the limits of direct transmission. Based on a simple model we compare the properties of the different platforms capturing the influence of source and memory efficiencies on the repeater performance for each system.

In order to assess and compare the specific capabilities of each platform, we primarily consider the most dominating and distinct effects in a typical elementary QR, namely, transmission loss in the fiber channel and memory dephasing at the repeater stations. In addition, we do include source and detector efficiencies, but we omit, for example, detector dark counts. These have a significant impact on secret key rates for larger distances.^[27] The overall performance of the source includes an experimentally determined efficiency and a clock (repetition) rate whose influence on the repeater rates depends on the repeater protocol.

The memory quality is given by an experimentally determined coherence time, but the impact of memory dephasing errors on the entanglement fidelity and thus the secret key fraction can be controlled by a freely chosen, so-called memory cutoff time.^[28] This means a quantum state is never kept in the memory for longer than a maximal storage time in order to optimize the secret key rates or almost entirely suppress dephasing errors. In our model, for comparison with the dimensionless "repeaterless" bound (secret key capacity), the finally considered secret key rates per channel use and per mode are also dimensionless and not expressed in Hz. Thus, clock rates given in Hz only have an indirect effect on the QR performance via the accumulated dephasing times and the corresponding variations of the required cutoff. We consider two different protocols, one of which is better adapted to the higher source clock rate and lower memory coherence time of the quantum dot platform. The other protocol, however, circumvents the need of writing the transmitted optical quantum states into the memories in a heralded, nondestructive fashion. It will become apparent that for both protocols, in principle, the elementary building blocks can be connected in a modular fashion to construct a QR system that is potentially scalable to larger distances. Let us now first introduce a minimal set of experimental parameters that can be used to quantitatively assess the performance of a memory-based QR system.

2. Minimal Set of Experimental Parameters Characterizing QR Performance

We assess the performance of a single QR cell (as it will be defined in Section 3) or, similarly, a two-segment QR in a simplified

model applicable to all three physical platforms. For this purpose, we choose three experimental parameters that are primarily related to the sources', the detectors', and the memories' efficiencies: the zero-length channel or link coupling efficiency, P_{link} , the source/memory clock time τ_{clock} (time span between two trigger/excitation events or memory write-in and reset time),^[29] and the memory coherence time τ_{coh} . The link coupling efficiency P_{link} incorporates the photon creation efficiency, fiber channel in- and outcoupling efficiencies, and, depending on the protocol, a detector efficiency or a memory write-in efficiency; the fiber channel transmission efficiency η will be treated separately from P_{link} . We consider sources generating true single-photon states as obtainable from initial entangled spin-photon resources. A single photonic qubit that is launched into the fiber channel is encoded into two field modes (typically corresponding to polarization or time-bin encoding). Such single-photon-based two-mode qubits can be easily "rotated" into any qubit state and measured in any qubit basis; for two qubits simple partial Bell-state measurements are available. These single-photon qubit states are also most robust against path length fluctuations along the optical channels and compatible with the stationary matter qubits (as opposed to weak coherent states or other phase-sensitive single-mode states, although also for this case repeater protocols exist^[23]). The memory coherence time τ_{coh} is defined via the time-dependent probability for a random phase flip to occur on a memory qubit, $\frac{1}{2}(1 - \exp(-\frac{t}{\tau_{\text{coh}}}))$, see Section S2 (Supporting Information). In addition, we include a memory cutoff time, i.e., a maximally allowed storage time until any quantum memory is reset and reinitialized. For a summary of the relevant experimental parameters and our notation used throughout the paper, see Section S1 (Supporting Information).

Let us briefly discuss the influence of the finite link coupling and channel transmission efficiencies in an idealized general QR, without errors and for an arbitrary number of stations/segments, on the QR performance, corresponding to a raw rate in the QKD context. We can then compare this with a quantum PPL, i.e., a scheme without the use of quantum memories solely based on direct transmission of quantum states. A single QR segment can be thought of as a quantum PPL over distance L/n when the total channel of length L is divided into n segments. The raw rate in Hz, i.e., the number of (quantum) bits (secret bits in QKD without errors) per time and per mode, for one segment is then given by

$$\mathcal{R}_{\text{link}}(L/n) = \frac{R_{\text{link}}(L/n)}{NT_0} \quad (1)$$

where R_{link} is the overall (dimensionless) link efficiency,^[30] T_0 is the time duration between two channel uses (i.e., time consumed per use), and N is the number of modes in case that several modes are sent in parallel through the optical channel. In general, $R_{\text{link}}(L/n)$ may exceed unity, but it must necessarily remain smaller than one either for not too short segment lengths (i.e., channel segments with more than 3 dB transmission loss for each^[12]) in a single-mode link or for an optical encoding based on discrete qubit states, as it applies to our two-mode-qubit-based schemes. This is why we refer to $R_{\text{link}}(L/n)$ as an efficiency and we may decompose it into the two contributions

coming from the link coupling and channel transmission efficiencies

$$R_{\text{link}}(L/n) = P_{\text{link}}\eta^{1/n} \quad (2)$$

where, more specifically, the second factor describes the channel transmission in a single repeater segment $\eta^{1/n} = \exp[-(L/n)/L_{\text{att}}]$ (i.e., η is the probability that a single-photon two-mode qubit remains intact after its parallel transmission over two independent amplitude damping channels of length L , while $\sqrt{\eta}$ represents the amplitude damping parameter of a Gaussian single-mode loss channel of length L).

If we connect the segments without the use of quantum memories like in a relay, effectively multiplying the efficiencies of the individual segments, we obtain at best $(R_{\text{link}}(L/n))^n = (P_{\text{link}})^n(\eta^{1/n})^n = (P_{\text{link}})^n\eta$. Since this scales with distance like a PPL over the whole channel, we may just remove the intermediate stations to obtain $R_{\text{link}}(L) = P_{\text{link}}\eta =: R_{\text{PPL}}(L)$. This link efficiency for the total two-mode PPL, up to a factor of 1.44 and for small $P_{\text{link}}\eta$, can also be identified as a "realistic repeaterless" bound for a single-mode channel of length L including a finite link coupling efficiency for the quantum PPL between Alice and Bob with finite source, fiber coupling, and detector efficiencies at Alice's and Bob's stations. For the raw rate in Hz (per mode) obtainable over the whole channel, we can now also write $\mathcal{R}_{\text{PPL}}(L) = R_{\text{PPL}}(L)/NT_0 = (P_{\text{link}}\eta)/NT_0$. In this case, if Alice directly sends a qubit to Bob over the entire distance, she will use $N = 2$ modes for a two-mode-encoded photonic qubit and she may also send many qubits sequentially at a high source clock rate $(\tau_{\text{clock}})^{-1} \sim \text{GHz}$ such that the final rate \mathcal{R}_{PPL} is ultimately limited only by η since $T_0 = \tau_{\text{clock}}$ (also assuming sufficiently fast detectors at Bob's station).

Once quantum memories are employed at the intermediate stations, in principle, a raw rate in Hz (per mode) for the total distance scaling as $\mathcal{R}_{\text{QR}} \sim (P_{\text{link}}\eta^{1/n})/NT_0$ can be approached (at fixed n), which corresponds to an expression similar to that for the rate in a single QR segment. The quantity P_{link} is once again the link coupling efficiency related with a single repeater segment and recall that we do not consider additional success probabilities from entanglement purification and swapping in the present discussion on an idealized QR. However, P_{link} should now also contain any inefficiencies related to the light-matter interface or the memory write-in for one segment. Even more important, compared with a memoryless quantum PPL bridging the total distance, the time unit for one channel use T_0 (as only for a PPL uniquely defined and coinciding with the source/detector clock time) will be significantly larger than a source clock time τ_{clock} . For the memory-based QR, depending on the specific protocol, T_0 must include the local memory write-in and reset times ($\sim \text{MHz}^{-1}$) and the necessary waiting times for classical signals announcing successful quantum state transmissions. Thus, although typically one also has $N = 2$ modes for the optical qubits, beating even the realistic "repeaterless" bound expressed in Hz requires a sufficiently long distance such that the superior scaling of $\eta^{1/n}$ dominates over the inferior "clock rate" of the memory-based repeater. So it is important to recognize that even the ideal memory-based QR, compared to a quantum PPL with fast sources and detectors, starts with a "repeater disadvantage," and only for sufficiently large distances can this be converted into a

“repeater advantage.” If errors are included, no longer all transmitted (quantum) bits (when employed for QKD) can be turned into secret bits. Related with this, for large distances, the QR rates drop further due to the need of probabilistic quantum error detection (such as entanglement purification) on higher repeater levels (alternatively, as said before, quantum error correction may be employed for all local gate and memory errors).

Note that all-optical quantum repeaters (at least those that work entirely without feedforward operations at the intermediate stations) can, in principle, operate at the same clock rate as a direct-transmission PPL. However, not only do we need rather complicated encoded states for this approach but also typically (though not necessarily) many optical modes $N > 2$ are required to transmit a logical qubit. Therefore, also in this case, sufficiently many segments have to be concatenated to benefit from the better effective transmission per segment, $(R_{\text{link}})'(L/n)$, compared to the long-distance PPL that works with $N = 2$. Such a better effective transmission due to quantum error correction at every station requires sufficiently short segment lengths, as opposed to the schemes we consider here. For short segment lengths, as already mentioned above, non-qubit-based schemes would in principle even allow for a “link efficiency” greater than one corresponding to the transmission of more than a single qubit (secret bit) per channel use.^[31] A unique exception is the twin-field QKD concept, for which we also have a high clock rate, only limited by lasers and detectors, and even just a single mode $N = 1$ for the optical transmission. However, this approach is not known to be scalable beyond $\sqrt{\eta}$.^[32]

To conclude, beating the (realistic) dimensionless “repeaterless” bound by means of a multimode memory-based quantum repeater with an effective overall transmission efficiency R_{QR} , i.e., effectively exceeding the overall efficiency of a multimode direct-transmission PPL

$$R_{\text{QR}}(L) > 1.44 N P_{\text{link}} \eta = 1.44 N R_{\text{PPL}}(L) \gtrsim (N/2) R_{\text{PPL}}(L) \quad (3)$$

is the minimal requirement even for a small-scale quantum repeater module to eventually be able to obtain better rates \mathcal{R} in Hz for large-distance quantum communication with many modules than what is obtainable via a long-distance PPL. Here, N is the number of modes and $R_{\text{PPL}}(L) = P_{\text{link}} \eta$, as introduced earlier, refers to a two-mode direct-transmission PPL that covers the total channel and employs no quantum memories at all. Thus, here the link coupling efficiency contains only source (with fiber incoupling) and detector (with fiber outcoupling) efficiencies, $P_{\text{link}} = P_{\text{source}} \eta_{\text{det}}$. The factor $1/2$ in the lowest bound above has been included to stress that $R_{\text{PPL}}(L)$ represents a two-mode link efficiency. The bound in the middle is the (realistic^[33]) multimode “repeaterless” bound for large L . In other words, overcoming the dimensionless bounds with a small, elementary repeater is the first necessary condition to be met for an experimental demonstration of in-principle scalable quantum repeater functionality. In our schemes, the QR stations are connected by optical two-mode channels, hence $N = 2$. In this case, overcoming the direct-transmission efficiency bound expressed by a two-mode PPL corresponds to $R_{\text{QR}}(L) > R_{\text{PPL}}(L) = P_{\text{link}} \eta$. In our quantitative comparison later (Figures 5 and 7), we will consider as a figure of merit the SKR in a memory-based QR scheme per channel use and per mode. Up to the secret key fraction factor that includes

the effect of the dephasing errors for a chosen QKD protocol (see Section S2, Supporting Information), SKR then corresponds to $R_{\text{QR}}(L)/2$. The relevant benchmarks will be the ideal “repeaterless” bound (single-mode secret key capacity), $-\log_2(1 - \eta)$, and SKR for a “realistic” but error-free PPL (per channel use and per mode), $R_{\text{PPL}}(L)/2 = P_{\text{link}} \eta/2$. Yet ultimately, a comparison must rely on rates in Hz, per time and per mode: \mathcal{R}_{QR} versus \mathcal{R}_{PPL} .

To sum up, for a given channel transmission efficiency (with $L_{\text{att}} = 22$ km), we consider three fundamental parameters:

- 1) The link efficiency R_{link} , which is composed of the link coupling efficiency P_{link} (now also including memory efficiencies) and the channel transmission efficiency per segment $\eta^{1/n}$,
- 2) The memory coherence time τ_{coh} , which can influence both the repeater raw rates and the secret key fraction in the QKD context, and
- 3) The clock time τ_{clock} , which, depending on the protocol, can have a significant impact even on the dimensionless repeater rates, namely, indirectly in the presence of memory dephasing.

In the following, we will discuss in detail several variants of small-scale proof-of-principle repeater protocols which can be classified into basically two distinct classes: node sends photons (“NSP”) and node receives photons (“NRP”). For each protocol we will then specify the particular form of the above three fundamental parameters, especially decomposing the link efficiency into further experimental parameters depending on the protocol. Eventually, we will be able to insert particular values for each of the three hardware platforms in order to compare their possible present and future repeater performances.

3. QR Cell: A Generic Experimental System Showing QR Functionality

Before introducing the basic concept of a QR cell in detail, and applying it to two different protocols and three different physical platforms, let us start by summarizing the overall concept for establishing a QR within our framework:

- A quantum channel is realized by an optical fiber.
- Intermediate stations along the channel include sources of single/entangled photons or spin–photon entanglement, beam splitters, detectors, possibly wavelength converters.
- The “repeaterless” bound limits the (secret key) rates in point-to-point communication (direct transmission without intermediate stations).
- The QR segments create entanglement of two spatially separated quantum memories connected by a direct quantum channel.
- The QR cells consist of two half QR segments with a central QR node containing quantum memories.

As described in the Introduction, the focus here is on fiber channels with a fixed channel attenuation. In our model, the quantitative effect of wavelength converters can be absorbed into P_{link} via a wavelength conversion efficiency (see Section S6, Supporting Information). While Figure 2 shows how entangled QR

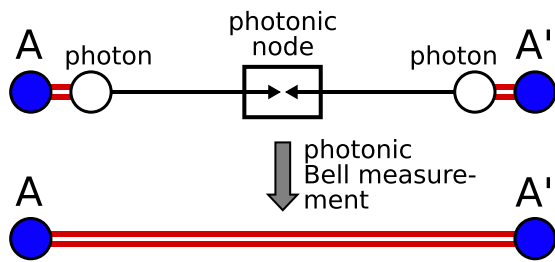


Figure 3. Entanglement creation within a QR segment (with QR nodes sending photons like in the “NSP” protocol below). At the end nodes spin–photon entanglement (full-open pair of circles) is generated. An optical Bell-state measurement on photons arriving at the central photonic node produces entanglement of the end nodes. This configuration does not yet exploit the storage capabilities of the quantum memories, since the photons need to arrive simultaneously at the middle station.

segments, once they are available, can be connected by entanglement swapping to increase the distance of a QR, **Figure 3** illustrates how a single QR segment itself, defined as an entangled pair of quantum memories located at neighboring repeater stations, may be established via an optical BM on two photons (two qubits) emitted by the two quantum memories placed each at the end points.^[34]

3.1. Protocol 1: Node Sends Photons

3.1.1. Model, Parameters, Modularity, and Rate Analysis

One of the simplest, most generic protocols promising to show the functionality of a memory-based QR system was put forward by Luong et al.^[35] This protocol, which we refer to as NSP protocol, is based on an arrangement that we will call a QR cell. Generally, this is an elementary structure that contains the minimal set of components required to show the functionality of a memory-based QR scheme, thus allowing to analyze schemes that can, in principle, overcome the “repeaterless” bound. An additional important property of a QR cell is that concatenation of QR cells renders the system (if, ideally, only affected by channel loss), in principle, scalable (**Figure 4**). This extra feature is needed, as we know that the “repeaterless” bound can be overcome in a restricted (not fully scalable) sense via a middle station not equipped with quantum memories.^[14,15] The NSP protocol relies on only a few generic parameters, whose impact on the QR performance can be clearly identified. It thus allows to compare different hardware platforms, including a qualitative and quantitative assessment of their relative strengths and weaknesses.

For a functioning QR cell (**Figure 4b**), the central node, equipped with a pair of quantum memories, is crucial. It allows to asynchronously establish effective entanglement in the two half segments, although an entangled state will never be physically shared between the end points of a QR cell. Instead, one would measure the optical signals emitted from the central node at the end points of the cell to establish correlations and obtain a secret key. The specific feature of the NSP protocol for the QR cell is that at the central QR node quantum states with spin–photon entanglement are locally created and then the photons are coupled into the communication channels, i.e., the node sends photons

toward the detectors placed on the left and right ends of the cell (**Figure 4b**). The concatenation of several QR cells then involves two-photon interferences to perform optical two-qubit BMs at the photonic nodes (**Figure 4a**).

Note that similar elementary QR schemes with a single QR node emitting and sending photons were considered in refs. [36,37] (considering a range of experimental parameters similar to ref. [35], however, including additional memory cutoffs, being adapted to the specific hardware platform of NV centers, and, in ref. [37] incorporating the twin-field QKD concept^[15] based on single-photon interference).

Let us discuss the underlying model for a QR cell with the NSP protocol in more detail. A single QR cell (**Figure 4b**) of total length L is composed of a central memory station placed in the middle between two receiving stations each equipped with photon detectors. The conceptually simplest scenario is when the two quantum memories each emit a single photon in two polarization modes entangled with the memory internal state. One photon is sent to the left receiver and the other photon to the right receiver (**Figure 4b**). The probability for each photon to arrive at its intended detector after travelling over a channel distance $L/2$ is $\exp[-(L/2)/L_{\text{att}}] \equiv \sqrt{\eta}$. Without the use of quantum memories both detectors must click simultaneously for the transmission to succeed, which happens with a probability $\sqrt{\eta}^2 = \eta = \exp(-L/L_{\text{att}})$ corresponding to the direct-transmission efficiency over a distance L . Thus, a single photon could be equivalently sent directly from left to right without the central station. However, by employing quantum memories, once the middle station is informed about the detection of one photon left or right, the respective memory is kept and for the other light-memory pair further attempts are made to eventually have a second photon arriving at its detector and being detected. A final BM on the two quantum memories, effectively swapping the entanglement of the two spin–photon pairs onto the two successfully distributed photons, establishes correlations between the two detectors such that a secret key can be shared provided that noncommuting observables were measured at the photon detectors (like in a BB84 protocol). Thanks to the memories, in principle, the transmission probability for the total distance L then scales as $\sqrt{\eta}$, corresponding to an effective transmission over only half the distance $L/2$.

The most extreme scenario in a QR cell would be to attempt distributing effective entanglement by sequentially (rather than simultaneously) sending photons entangled with memory qubits to the left and to the right (e.g., first to the left), and start sending those photons entangled with a second spin (e.g., the right one) only when the arrival of a photon belonging to the first spin (e.g., arriving at the left detector) was confirmed and the first spin qubit (e.g., the left quantum memory) was determined to be held for storage. Such an approach can be experimentally useful, because the central node may no longer require two distinct memory systems (with the typical example of a single NV center whose nuclear spin with coherence times of the order of seconds allows for efficient storage and whose electron spin with coherence times of the order of milliseconds can be employed as an interface to the optical communication channel,^[36,37] another example would be an ion-based quantum memory composed of two ion species where one is adapted for storage and the other for light–matter interfacing^[38]).

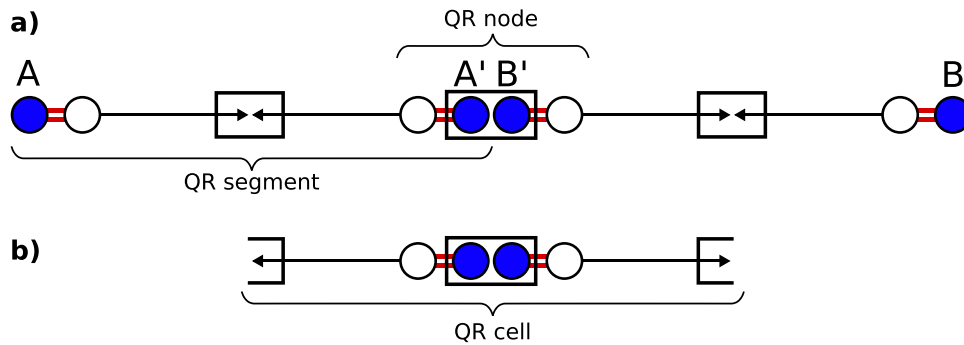


Figure 4. a) Full QR link with two QR segments (NSP) like in Figure 3. b) QR cell (NSP) with two half QR segments and a central node for storage as a minimal element for exploiting memory capability. The pair of quantum memories at the central node enables a valid Bell-state measurement also when the left and right half segments become entangled at different times.

The effective transmission probability R_{QR} is related to the inverse average number of attempts it takes for successfully transmitting the photons to both ends. However, besides this average number, the ultimate secret key (or qubit) rate of a repeater scheme expressed in secret bits (or qubits) per second, \mathcal{R}_{QR} , also depends on the actual duration per attempt (recall the discussion in Section 2). Moreover, the longer a single attempt takes, the smaller the number of attempts becomes that can be executed well within a given quantum memory's coherence time. In the NSP protocol, the duration per attempt is distance-dependent, because any new attempt can only be initiated when the classical signal from the detector has been received. Thus, the total duration of a single attempt is dominated by this waiting time that includes quantum and classical signal transmissions, $T_0 = \frac{L}{c}$ for the QR cell (Figure 4b) and $T_0 = \frac{L}{2c}$ for the two-segment setup in Figure 4a assuming the same total distance L in either case. Hence, the influence of an increased experimental clock rate $(\tau_{\text{clock}})^{-1}$ for preparing spin-photon entanglement and emitting a photon is less significant for the NSP protocol. More precisely, the average dephasing is determined by the factor $\exp(-\frac{T_0}{\tau_{\text{coh}}})$, including the memory- and protocol-dependent quantity τ_{coh}/T_0 that counts how many distribution attempts fit into the given memory coherence time window (see Section S2, Supporting Information). In the NSP protocol, for the QR cell, we have $T_0 = \frac{L}{c} + \tau_{\text{clock}} \approx \frac{L}{c}$ with the relatively large distances that we are interested in.

For the QR cell in the NSP protocol (Figure 4b), we have the link coupling efficiency $P_{\text{link}} = P_{\text{source}} \eta_{\text{det}}$ where P_{source} includes all efficiencies related to a source emitting photons entangled with a spin memory and coupling them in (and eventually out of) the fiber channel, i.e., it is the probability to get a photon into and out of a single-mode fiber channel per trigger/excitation event, and η_{det} is the detector efficiency (regarding the effect of wavelength converters, see Section S6, Supporting Information). Constructing two QR segments like in Figure 4a with the NSP protocol corresponds to $P_{\text{link}} = 1/2(P_{\text{source}})^2 (\eta_{\text{det}})^2$, because one segment is successfully bridged only when both sources at its end points create photons that are both detected at the photonic node in the middle (the factor 1/2 takes into account the efficiency of a standard partial, beam-splitter-based two-photon two-qubit BM). However, the time duration per attempt for one segment of the two-segment scheme (Figure 4a) is half as big as that for the QR cell (Figure 4b) at any given total distance L , as mentioned above.

Table 1. Currently available experimental parameters for the three QR platforms: color centers (NV, SiV), quantum dots, ions (calcium, ytterbium), and atoms (rubidium).

Platform	P_{link} [%]	$(\tau_{\text{clock}})^{-1}$ [MHz]	τ_{coh} [ms]
NV centers ^{a)}	5	50 (0.5)	10
SiV centers ^{b)}	5	30 (5)	1
Quantum dots ^{c)}	10	1000 (32)	0.003
Ions ^{d)} (Ca/Yb)	25	0.47 (0.007)	20
Atoms ^{e)} (rubidium)	50	5 (0.005)	100

^{a)} Refs. [36,37]; ^{b)} Refs. [39,40]; ^{c)} Refs. [41–43]; ^{d)} Refs. [44–46]; ^{e)} Refs. [47,48].

Table 2. Potentially available future experimental parameters for the three QR platforms: color centers (NV, SiV), quantum dots, ions (calcium, ytterbium), and atoms (rubidium).

Platform	P_{link} [%]	$(\tau_{\text{clock}})^{-1}$ [MHz]	τ_{coh} [ms]
NV centers ^{a)}	50	250 (5)	10 000
SiV centers ^{b)}	50	500 (50)	100
Quantum dots ^{c)}	60	1000 (323)	0.3
Ions ^{d)} (Ca/Yb)	50	10 (1)	300
Atoms ^{e)} (rubidium)	70	10 (1)	1000

^{a)} Refs. [36,37]; ^{b)} Refs. [24,39]; ^{c)} Refs. [43,49]; ^{d)} Ref. [50,51]; ^{e)} Refs. [47,48].

In addition to the three experimentally determined parameters P_{link} , τ_{clock} , and τ_{coh} , we include a memory cutoff parameter imposing the rule that quantum states will never be stored for a longer time than given by the cutoff.^[28] In other words, the QR protocol is aborted and started from scratch as soon as a quantum memory's storage time has exceeded the imposed storage limit. The memory cutoff can be freely chosen. Our analysis is based on the experimental parameters for the three platforms as given in the tables next.

Table 1 refers to the state of the art presenting the currently available, realistic values for each platform. **Table 2** shows potential future parameter values, i.e., an idealization compared to the state of the art. Nonetheless, the latter are physically reasonable and not fundamentally unobtainable.

For $(\tau_{\text{clock}})^{-1}$ we list two types of values for all platforms, as will be explained later when we discuss the NRP protocol, because

$(\tau_{\text{clock}})^{-1}$ is not important here for the NSP protocol. Since $(\tau_{\text{clock}})^{-1}$ is of the order of MHz or higher for most platforms, the clock times $\sim 1 \mu\text{s}$ or shorter are negligible compared with $\frac{L}{c} \gtrsim 50 \mu\text{s}$ for distances $L > 10 \text{ km}$. The only exceptions are ions and atoms with the longest clock times around $200 \mu\text{s}$. For distances $L > 100 \text{ km}$ this also goes below $\frac{L}{c} \gtrsim 500 \mu\text{s}$. Moreover, for smaller distances, the elementary time unit T_0 , even including the experimental clock times, is small compared with the values of τ_{coh} assumed for ions and atoms. Overall, $(\tau_{\text{clock}})^{-1}$ plays no significant role in the NSP protocol.

The future parameters of NV centers are obtained by extrapolating the values of refs. [36,37], especially for the link coupling efficiency (and for the clock times as needed later), and assuming a ^{13}C nuclear spin for the memory. Similar assumptions are made for the SiV centers based on refs. [24,39,40]. Compared to NV centers, the SiV platform has the advantage of not only allowing for efficient quantum storage via the nuclear spins but also providing a potentially more efficient photon–spin interface (with higher cooperativities available); though a drawback of SiV is the need for very low temperatures^[52] (below 500 mK).^[53] Further details regarding the experimentally assumed parameters can be found in Section S6 (Supporting Information).

For the quantum dot platform, based on experimentally achieved quantum dot photon-collection efficiencies of 60% ^[42] connected with a near Gaussian beam profile which is preferential for large fiber incoupling efficiencies, we estimate the link coupling efficiency P_{link} to 10% (Table 1). Anticipating improvements in photon-collection efficiencies up to 90% together with improved fiber-coupling efficiencies, we assume that a possible future value of P_{link} is 60% (Table 2). Regarding the clock times, we estimate spin-preparation times in a quantum dot to be in the few 100 ps regime, and together with reported radiative recombination times also in the range of a few 100 ps ,^[43] we expect achievable clock rates of 1000 MHz for a quantum-dot-based nonclassical light source (we refer to Section 3.2 for a further discussion on the impact of experimental clock rates). Additional remarks concerning these experimental parameters can be found in Section S6 (Supporting Information).

We assumed fairly good experimental parameters for the rubidium atom and calcium ion platforms. The presently available values for P_{link} and τ_{coh} refer to current experiments with rubidium atoms in a cavity.^[47,48] More specifically, atomic eigenstates can be chosen for the qubit encoding such that the effect of external magnetic fields is significantly reduced. This way coherence times above 100 ms have been measured.^[47]

The performance of a QR may be quantified in a meaningful way by the secret key rate that can be obtained for a given length L of the quantum channel connecting the two parties Alice and Bob. The advantage of using the secret key rate as a figure of merit is that it incorporates both the efficiency and the quality (or fidelity) of the quantum state transmission at the same time. A high efficiency, i.e., a high (effective) transmission probability or raw rate leads to an increasing secret key rate, whereas a low fidelity, i.e., a high error rate, results in a decreasing secret key rate (typically incorporated via a secret key fraction). In our rate analysis, we shall consider, on the one hand, secret key rates in an entanglement-based BB84-type scheme, for which optimal memory cutoffs exist, since a cutoff chosen too small will reduce the raw rate and a cutoff chosen too large will lead to a stronger ac-

cumulation of dephasing errors reducing the secret key fraction. In other words, the infidelities from the finite coherence times of the memories, eventually becoming manifest as an infidelity of the effective entangled state shared between Alice and Bob after the BM on the memory qubits, are mapped onto a reduced secret key fraction for a BB84 QKD scheme (see Section S2, Supporting Information).

On the other hand, in an alternative picture independent of QKD, we shall only consider the raw rate (without inclusion of dephasing errors) by choosing the cutoff sufficiently small in order to almost entirely suppress dephasing errors and keep the final fidelities of the (effective) entangled state above a certain value such as 0.95 . This means the maximally allowed storage time is chosen well below the memory's coherence time for the loaded memory at the central station waiting for the second transmission to succeed. More details can be found in Section S3 (Supporting Information).

It should be stressed that our simplified model does not entirely capture intrinsic effects arising from specific memory errors (beyond pure dephasing) and other error sources for a given hardware platform, such as an imperfect initial spin–photon state prior to its storage-time-dependent dephasing and imperfections of the final two-spin two-qubit BMs, but also detector dark counts. All these additional error sources lead to effective entangled states that are random mixtures of four instead of just two Bell states (see Section S2, Supporting Information) resulting in secret key rates eventually dropping to zero beyond certain distances. An advantage of our simple model, however, is that we are able to use only very few parameters to compare QR schemes employing different hardware realizations with different error mechanisms for the preparation and storage of quantum states. We can then clearly identify which parameter influences the (still to some extent idealized) QR performance in a certain way, mainly manifesting itself in the rate versus distance plot of Figure 1 as a negative offset, i.e., a downshift of the curve due to link coupling inefficiencies, and an increased slope, i.e., an additional distance-dependent rate reduction due to memory inefficiencies.

3.1.2. Results and Comparison for Different Platforms

The resulting raw and secret key rates calculated for our model in the case of the NSP-QR cell (as illustrated by Figure 4b) with the different hardware platforms can be seen in **Figure 5**. The upper part shows the raw rates RR for distributing effective entangled states with a fidelity of at least 0.95 for current (left) and future (right) experimental parameters. The lower part shows the corresponding SKRs. All rates (in dB) are per channel use and per mode (recall the discussion at the end of Section 2).^[54]

With current parameters, only the rubidium atom platform enters the repeater regimes. For future values, as calculated, all platforms except for quantum dots enter the repeater regimes. However, the different platforms exhibit a slope increase, i.e., a more rapid decline of the rate with distance, to a different extent in accordance with their ranking in terms of memory coherence time (see Table 2). Apparently, the slope of the rates is clearly connected to the memory efficiencies. The plots cover distances up to 400 km and the curves may be extrapolated to larger distances.

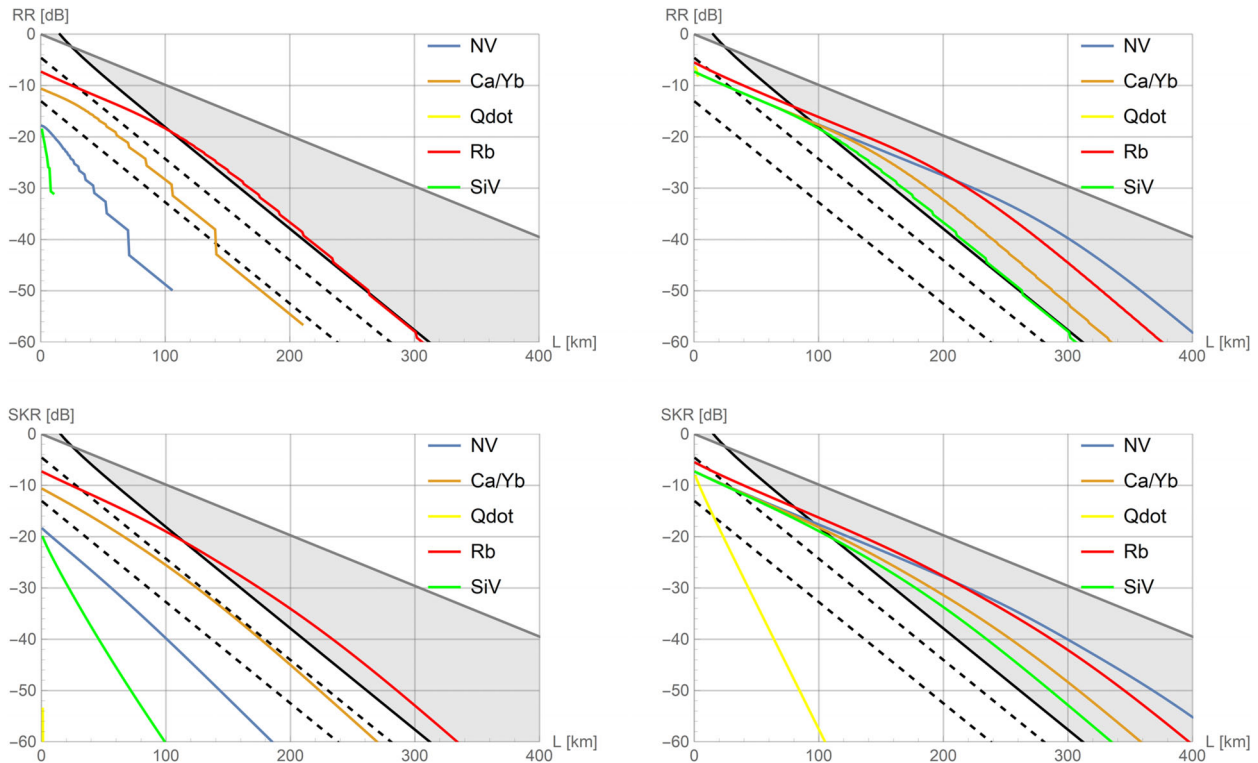


Figure 5. Secret key rates (SKR) and high-fidelity raw rates (RR) for a small NSP-based QR scheme (QR cell). The bottom plots show SKR in dB as a function of the total distance L in km for experimental parameters as currently available (left) and as potentially available in the future (right). The top plots show RR in schemes where the entangled states effectively created over the total distance L have a fidelity of at least 0.95 (left: current parameters, right: future parameters). Curves that are disappearing beyond certain distances (or completely missing for quantum dots) no longer (never) exceed $F = 0.95$. The different platforms correspond to NV (violet) and SiV (green) centers, ions (brown), rubidium atoms (red), and quantum dots (yellow). The light gray area illustrates the (secret key) rate regime between $\sim \eta$ (curve in bold black: “repeaterless” bound) and $\sqrt{\eta}$ (line in dark gray: optimal rate for QR cells or two-segment QR schemes). The bold black dashed lines represent the realistic “repeaterless” bound $P_{\text{link}}\eta/2$ (direct transmission via PPL) with finite link efficiencies $P_{\text{link}} = 0.1, 0.7$.

However, recall that detector dark counts and some other imperfections that could make the rates eventually drop to zero are not included here. The negative offset from the “repeaterless” bounds at zero distance is related to the link coupling efficiency. The quantum dot platform, as calculated here for the NSP protocol, does not enter the repeater regime at all, not even for future parameters (it does though for rather short distances when compared with a “realistic repeaterless” bound as a benchmark that is defined with a smaller link coupling efficiency $P_{\text{link}} = 0.1$). Some curves drop faster than the “repeaterless” bound, which seems contradictory. However, note that even when the very first qubit distribution attempt is successful both memories are already subject to dephasing for one time unit. For platforms with insufficient coherence times, this results in an even steeper decline of the secret key rates compared to the “repeaterless” bound, although the η scaling could be formally attained via the raw rate by not storing the quantum states at all, i.e., setting the cutoff value to zero (see the Supporting Information). All this will become different for another protocol below (NRP) for which, in particular, all platforms are able to access the repeater regimes.

For the NSP protocol, besides a single QR cell (Figure 4b), there is also the variant of a QR with two full segments (Figure 4a). As discussed before, for equal total distance L , the two-segment scheme has a smaller elementary time unit compared

to the QR cell ($T_0 = \frac{L}{2c}$ vs $T_0 = \frac{L}{c}$). However, at the same time, the two-segment scheme has a smaller link coupling efficiency ($P_{\text{link}} = 1/2(P_{\text{source}})^2 (\eta_{\text{det}})^2$ vs $P_{\text{link}} = P_{\text{source}} \eta_{\text{det}}$).

For comparison and completeness, we present the rates of the two-segment scheme in Section S4 (Supporting Information).^[55] One can see that it performs slightly worse compared to the QR cell. In all plots the secret key rates can sometimes be greater than the raw rates, which again seems contradictory. However, note that for the secret key rates, the optimized memory cutoff (which must neither be too small nor too large to prevent a too small raw rate or a too small secret key fraction, respectively) typically leads to a worst-case fidelity much lower than the minimal fidelity of 0.95 allowed for the calculation of the raw rates alone (requiring a very small memory cutoff to almost entirely suppress dephasing errors).

3.2. Protocol 2: Node Receives Photons

3.2.1. Model, Parameters, Modularity, and Rate Analysis

In order to potentially benefit from a higher source repetition rate as available from the quantum dot platform, we shall consider an alternative NRP protocol (Figure 6). In this protocol, photons

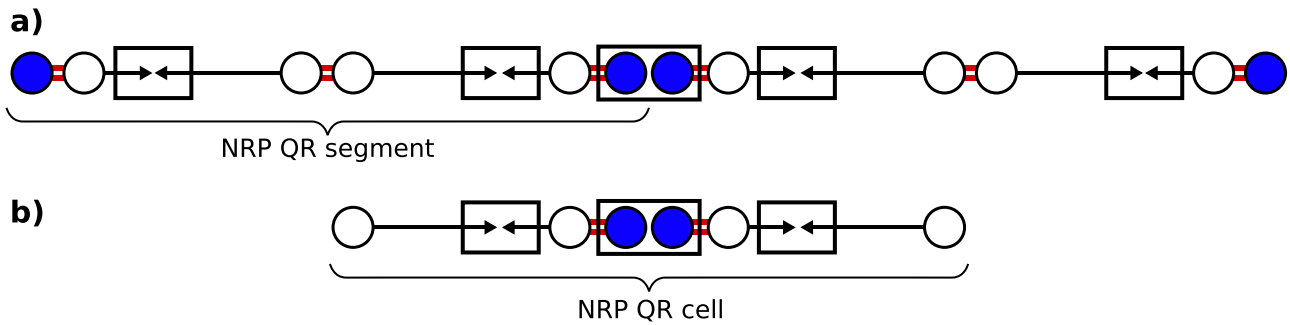


Figure 6. a) Full QR link with two QR segments incorporating the NRP concept. The BMs in Figure 4a are now replaced by Bell-state sources. b) QR cell consisting of two half QR segments and a central node for storage as a minimal element for exploiting memory capability. As opposed to the QR cell in Figure 4b, here the quantum memories “receive” photons from two sending stations; whether a photon has arrived must be confirmed by a nondestructive measurement on the qubit, here realized by a photonic BM on a “local” photon emitted from the memory (open circle) and the photon transmitted through the channel. As before, the final BM on the memories can also be valid when the QR segments become entangled at different times.

are sent from two sending stations to the central memory station where the arrival of a photonic qubit is nondestructively (e.g., by a linear-optics photonic BM teleporting the arriving photonic qubit to the memory qubit) detected before or while it is “written into” the memory. At any failure event, the next photon pulse can be processed with a delay only depending on the repetition rate of the source or depending on the typically longer write-in and reset times of the memory. In this case, the duration per attempt corresponds to the clock time of the source or the write-in time and is independent of the channel distance, $T_0 = \tau_{\text{clock}}$, as opposed to the situation for the NSP protocol where T_0 is mainly determined by the length of the repeater segments.

Thus, the factor that specifies the average memory dephasing (see Section S2, Supporting Information) now becomes $\exp(-\frac{\tau_{\text{clock}}}{\tau_{\text{coh}}})$, while it is now the ratio $\tau_{\text{coh}}/\tau_{\text{clock}}$ that counts the number of distribution attempts fitting into the given memory coherence time. However, note that this feature is specific to a single NRP-QR cell and as soon as several cells are combined into a larger QR system, distance-dependent waiting times for classical signals have to be taken into account again. As a consequence, similar to what holds in general for the case of the NSP protocol, a scalable QR based upon NRP modules (see next) will also be mostly influenced by an experimental improvement of the link coupling efficiency and the memory coherence time, and much less by an enhanced experimental clock time.

A QR cell now still has a central node equipped with quantum memories, but at the end points there are no longer detectors, but sources for optical quantum states such as BB84-encoded single-photon-based qubits (Figure 6b). The memory node now receives the photons. This may be realized by a direct and heralded write-in mechanism (such as those of refs. [56–58]), for which certain write-in inefficiencies and infidelities would apply, or by first preparing spin–photon entangled states at the central node and then coupling the photons near the memories locally with the arriving photons coming from the left and right sources (by an optical BM, see Figure 6b). Similar to the NSP protocol, also QR cells based upon the NRP protocol can be concatenated in order to scale up the QR system to larger distances (Figure 6a). The “photonic nodes” where the half segments meet are now no longer performing BMs like in the NSP case, but

are instead equipped with entangled photon pair sources (Figure 6a). Compared to the NRP-based QR cell here, a similar elementary QR scheme with a single QR node receiving photons, for BB84-encoded photonic qubits equivalent to what is referred to as measurement-device-independent QKD^[59,60] assisted by a quantum-memory-based middle station, was considered in refs. [61–64] (again mainly adapted to the specific hardware platform of NV centers, but also presenting comparisons with other platforms in ref. [63] and incorporating the idea of a deterministic final BM on the electronic and nuclear spins of a single NV center in ref. [64]).

In order to keep memory dephasing errors small and the fidelity of the effective entanglement shared between Alice and Bob above a certain minimum, in the NSP protocol, for an increasing L a decreasing number of attempts can be executed at a given memory coherence time because of the L -dependence of a single attempt’s duration and the growing storage time needed per transmission attempt. In the NRP-protocol-based QR cell (Figure 6b), this L -dependence disappears, since the quantum signals are sent to, and no longer emitted from, the quantum memories. The memory cutoff can be chosen independent of distance and the time duration per transmission attempt can be made arbitrarily small by increasing the repetition rate of the sources up to the local memory write-in and reset times. This means the cutoff (expressed by the number of allowed attempts during one storage cycle) can be chosen much higher resulting in larger raw rates. Moreover, this way the memories have less time to be subject to dephasing during a given number of attempts leading to a larger secret key fraction. Generally, the NSP and NRP protocols have both their benefits and disadvantages. The NSP protocol does not require a nondestructive detection of an arriving photonic qubit or an efficient heralded write-in mechanism, but the memory station has to wait for the classical signals from the receiving detector stations. In contrast, the NRP protocol relies on a nondestructive measurement or any other means to nondestructively write the incoming “flying qubit” into a “stationary qubit” in a heralded fashion; however, there are no extra waiting times for classical signals (as long as we consider the elementary QR cell of Figure 6b). In addition, the NRP scheme inherits all benefits of

measurement-device-independent QKD with an untrusted middle station receiving and measuring the quantum states coming from two outer sending stations.^[59–64] For the rate analysis of the NRP-based schemes, the main experimental parameters taken into account in our simple model are the same as for the NSP-based schemes: the link coupling efficiency P_{link} , the memory coherence time τ_{coh} , and the source/memory clock time τ_{clock} which now for the NRP-QR cell may have an actual impact on the repeater performance.

The two types of values given in Tables 1 and 2 for $(\tau_{\text{clock}})^{-1}$ either exclude (numbers without brackets) or include (numbers in brackets) the additional sequences and operations that are typically needed in order to reinitialize a spin every time when an attempted write-in of an arriving photonic qubit failed. Clearly, these numbers differ significantly, and it depends on the particular protocol whether the spin is affected by a failed write-in and has to be reset or not. The specific teleportation-assisted write-in processes as illustrated in Figure 6 would always, in every round, require a newly prepared spin–photon entangled state. However, there are also schemes where the initial spin state is to a great extent only altered at those events when a photonic qubit is actually arriving, ready to be coupled to the spin qubit, and eventually detected (we refer to such schemes as a direct write-in).^[24,56–58] Therefore, we will consider both above-mentioned types of values for $(\tau_{\text{clock}})^{-1}$ corresponding to the two extreme scenarios where the experimental clock rate in the NRP protocol is either determined by the repetition rate of a nonclassical source (reaching values as high as 1 GHz for a quantum-dot-based source) or where the necessary spin reset times are fully taken into account.^[65] The former scenario is somewhat more general, as it does not rely upon a particular protocol for the spin–photon interface. However, it is idealized assuming an ultrafast write-in mechanism. In our quantitative analysis in Section 3.2.2, we shall combine this idealization with the extra assumption of a deterministic write-in. The complementary scenario of a non-deterministic, slow write-in including memory reset times will be considered in Section S5 (Supporting Information). Further details regarding the experimentally assumed parameters can be found in Section S6 (Supporting Information).

For the QR cell in the NRP protocol (Figure 6b), we now have $P_{\text{link}} = P_{\text{source}} P_{\text{write}}$ where P_{source} again includes all efficiencies related to a source emitting photons (this time prepared in BB84 states) and coupling them into (and eventually out of) the fiber channel. The parameter P_{write} represents the probability for successfully writing a photonic qubit arriving at the central node into the respective memory (regarding the effect of wavelength converters, see Section S6, Supporting Information). If a spin–photon entangled state and a linear-optics BM are exploited for this in order to teleport the arriving photonic qubit to the memory spin qubit (see Figure 6b), we have $P_{\text{write}} = 1/2 P_{\text{source}} (\eta_{\text{det}})^2$ where P_{source} specifically refers to the generation of a spin–photon entangled state. Note that if the BB84-encoded photons were produced in a similar fashion (via initial spin–photon entanglement) with the same source efficiency P_{source} , we would obtain the link coupling efficiency $P_{\text{link}} = P_{\text{source}} P_{\text{write}} = 1/2 (P_{\text{source}})^2 (\eta_{\text{det}})^2$, which actually coincides with that of the NSP-based two-segment QR (Figure 4a), because in terms of the link couplings the two schemes become identical when the photonic nodes in the middle of each segment of the NSP scheme both move to the central

node right next to the memories (except that the “local” photons may no longer require fiber coupling).^[66] For other write-in methods,^[56–58] we may just directly insert numbers for P_{write} . Although the two-segment concatenation of NRP-based QR cells and half segments (Figure 6a) demonstrates that the basic modules can be systematically combined to build an in-principle scalable QR system, we shall not consider this scheme in our rate analysis. As opposed to the QR cell in Figure 6b, the combined scheme in Figure 6a does require classical communication to inform the two central memories about the successful loading of their memory counterparts with photons originating from the same entangled photon pair, and thus it will have smaller rates than the QR cell alone (in this context, however, see also the discussion on quantum repeater design presented in ref. [67]). More theoretical details can be found in Sections S2 and S3 (Supporting Information).

3.2.2. Results and Comparison for Different Platforms

The resulting raw and secret key rates calculated for our model in the case of the NRP-QR cell (as illustrated by Figure 6b) with the different hardware platforms can be seen in Figure 7. The upper part again shows the raw rates for distributing effective entangled states with a fidelity of at least 0.95 for current (left) and future (right) experimental parameters. The lower part again shows the corresponding secret key rates. All rates (in dB) are again per channel use and per mode (recall the discussion at the end of Section 2). The plots in Figure 7 are for a deterministic memory write-in scheme, $P_{\text{write}} = 1$. Moreover, as for the values given in Tables 1 and 2 for $(\tau_{\text{clock}})^{-1}$, the rates in Figure 7 have been calculated excluding additional spin sequences (numbers without brackets).^[68]

This time we observe that already with current parameters all platforms enter the repeater regimes. With future parameters, for the simple model used in the rate calculations (no dark counts and no depolarizing errors), all platforms achieve a rate slope $\sim \sqrt{\eta}$ over the entire distance of 400 km as shown, thus fully exhibiting the repeater advantage. This also holds in particular for the quantum dot platform that, though having the worst memory coherence time, can fully benefit in the NRP protocol from the highest clock rate (see Table 2).

For the NRP-QR cell, we may then also consider an explicit write-in mechanism in the form of a linear optical BM (Figure 6b). In this case, instead of assuming unit write-in efficiency like for the rates calculated in Figure 7, we have $P_{\text{write}} = 1/2 P_{\text{source}} (\eta_{\text{det}})^2$ as mentioned above. Moreover, the additional sequences for spin reinitialization are included in $(\tau_{\text{clock}})^{-1}$ (numbers in brackets in Tables 1 and 2). We present the corresponding rates calculated for this situation in Section S5 (Supporting Information).

4. Conclusion

As the effective clock rate in a memory-based QKD or QR system is always slower than that of a direct point-to-point quantum connection driven from a laser source at \sim GHz rates, the memory-based system will become potentially more efficient only at large

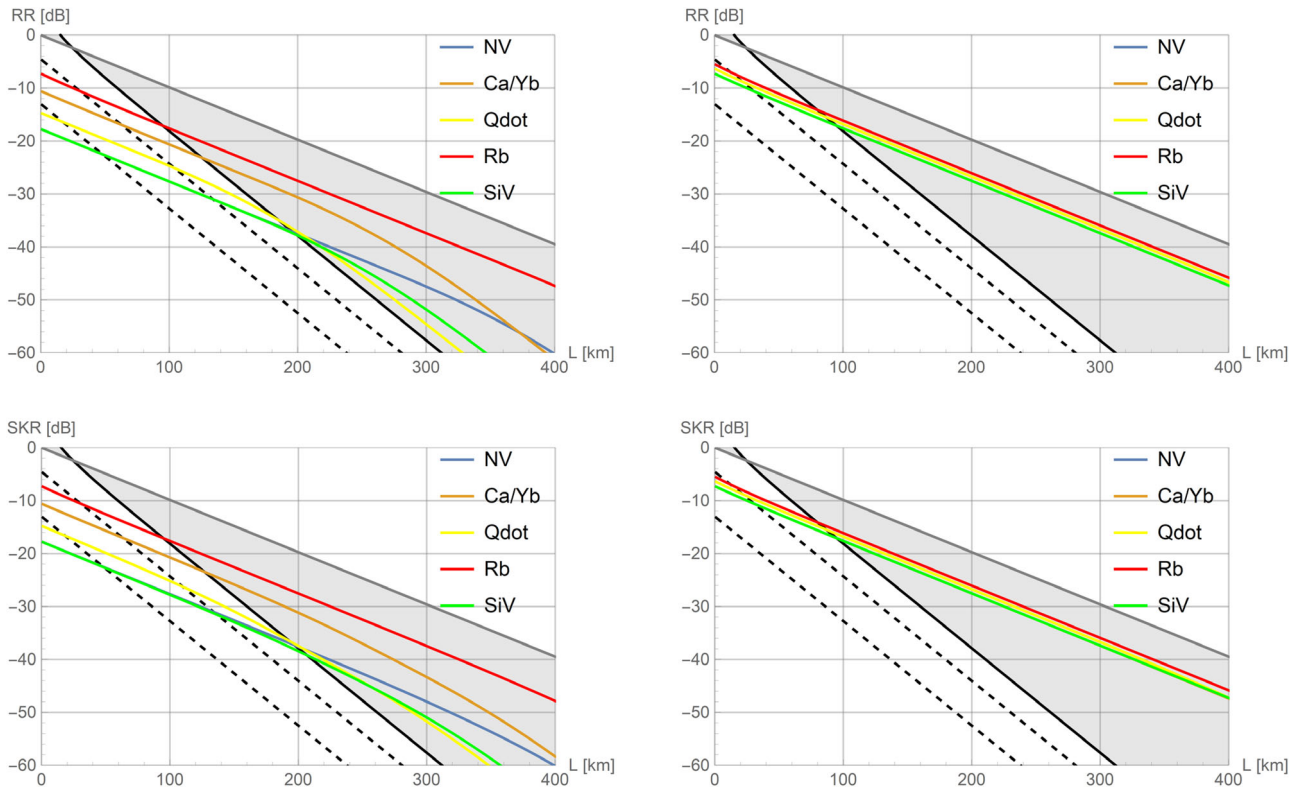


Figure 7. Secret key rates (SKR) and high-fidelity raw rates (RR) for small NRP-based QR schemes (QR cell assuming $P_{\text{write}} = 1$ in $P_{\text{link}} = P_{\text{source}} P_{\text{write}}$). The bottom plots show SKR in dB as a function of the total distance L in km for experimental parameters as currently available (left) and as potentially available in the future (right). The top plots show RR in schemes where the entangled states effectively created over the total distance L have a fidelity of at least 0.95 (left: current parameters, right: future parameters). The different platforms correspond to NV (violet) and SiV (green) centers, ions (brown), rubidium atoms (red), and quantum dots (yellow). The NV/ions curves, invisible for future parameters, coincide with those of the other platforms. The light gray area illustrates the (secret key) rate regime between $\sim \eta$ (curve in bold black: “repeaterless” bound) and $\sqrt{\eta}$ (line in dark gray: optimal rate for QR cells or two-segment QR schemes). The bold black dashed lines represent the realistic “repeaterless” bound $P_{\text{link}}\eta/2$ (direct transmission via PPL) with finite link efficiencies $P_{\text{link}} = 0.1, 0.7$.

communication distances requiring sufficiently many elementary QR segments and additional quantum error detection and correction at higher “nesting levels” of the QR. At such large scales, quantum memories must be sufficiently long-lived or fault-tolerant to survive the necessary waiting times especially for the classical signals sent back and forth between the QR stations. However, a necessary requirement for a large-scale QR to show a performance superior to that of direct transmission is that its fundamental elements already exceed the bounds constraining a “repeaterless” system on a smaller scale: employing an elementary QR cell or a two-segment QR should on average lead to a larger secret key or qubit transmission rate than obtainable in a direct transmission. We have investigated such basic elements for a QR system considering two protocol variants for three different hardware platforms.

Combining the basic building blocks in a modular fashion allows to construct a QR system, that is, considering only channel loss, scalable to larger distances. For the realistic situation including general memory and operation errors (such as depolarizing errors with infidelities from the initial states, the light–matter interfaces, and write-in processes, or the spin–spin Bell measurements as well as detector dark counts) eventually additional methods of quantum error correction/detection will

be required. Nonetheless, for the small-scale QR elements (cells and two-segment schemes) discussed in this work the impact of both finite link and memory efficiencies (the latter described by a simple dephasing model including a “memory cutoff”) on the repeater performance has been analyzed for various hardware platforms. The aim was to keep our model sufficiently simple in order to allow for an analytic treatment and to be able to assess the performances in terms of a small set of experimental parameters. Among the three parameters identified—link coupling efficiency, memory coherence time, and experimental clock rate—most important, especially toward combining the QR modules into a large-scale system, turn out to be the former two parameters. The experimental clock rate specifically influences the performance of our NRP-QR cell.

While, depending on the protocol, some platforms turn out to be superior to others with current and future experimental parameters as assumed in our model, a promising further direction could be a hybridization between the different platforms, for instance, combining the high clock rates of quantum-dot-based sources with the long memory coherence times of rubidium atoms or NV centers. In our NRP protocol, where quantum memories can receive photons at a rate only limited by the source’s clock rate and the memory write-in and reset times, but not by the

classical communication times, the “repeaterless” bounds can be exceeded quite comfortably under the assumptions of our simplified model. Even when NRP-based QR cells are connected to reach larger distances, like in our NRP-based two-segment QR scheme using sources of entangled photon pairs, high source clock rates can still be of great benefit.^[67] Yet, in general, once QR building blocks are connected to construct a larger system composed of many repeater segments or cells, the classical communication times become a limiting factor in any protocol based on quantum memories.

Ultimately, deciding which quantum communication system performs better for a given range must rely upon rates determined in Hz, i.e., per time in seconds. Nonetheless, for a sufficiently large range, the better effective transmission efficiency of a memory-based QR system that becomes manifest in a scaling-with-distance advantage over any point-to-point link will eventually also lead to higher rates in Hz for the QR. In particular, combining many sufficiently short repeater segments improves the scaling and allows to keep the classical communication times small, provided that errors beyond transmission loss can be dealt with via additional quantum error correction. The resulting rates may still be rather small for a single repeater chain, but they can be increased by operating many chains in parallel or via more advanced multiplexing techniques. Such approaches, besides quantum error correction, can also help to keep memory errors small, thus enhancing the overall secret key rates.

Supporting Information

Supporting Information is available from the Wiley Online Library or from the author.

Acknowledgements

The authors acknowledge support from the BMBF in Germany for the project Q.Link.X.

Open access funding enabled and organized by Projekt DEAL.

Conflict of Interest

The authors declare no conflict of interest.

Keywords

color centers, quantum communication, quantum dots, quantum repeaters, trapped atoms/ions

Received: December 22, 2019

Revised: June 29, 2020

Published online: October 20, 2020

- [1] a) V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, *Rev. Mod. Phys.* **2009**, *81*, 1301; b) S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, P. Wallden, *arXiv:1906.01645*, **2019**.

- [2] C. H. Bennett, G. Brassard, in *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing*, Vol. 175, IEEE, New York **1984**, p. 8.
- [3] A. K. Ekert, *Phys. Rev. Lett.* **1991**, *67*, 661.
- [4] S. Wehner, D. Elkouss, R. Hanson, *Science* **2018**, *362*, eaam9288.
- [5] http://www.chinadaily.com.cn/china/2017-09/30/content_32669593.htm (accessed: October 2017).
- [6] a) J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, J.-W. Pan, *Science* **2017**, *356*, 1140; b) G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, P. Villoresi, *Phys. Rev. Lett.* **2015**, *115*, 040502.
- [7] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, H. Zbinden, *Phys. Rev. Lett.* **2018**, *121*, 190502.
- [8] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, J.-W. Pan, *Phys. Rev. Lett.* **2016**, *117*, 190501.
- [9] In combination with transmission losses another limiting factor are dark counts of the detectors. At a distance of 400 km, only ≈ 10 photonic qubits would be transmitted per second when sent at GHz clock rate. Thus, beyond 400 km the optical signals will eventually vanish under dark count noise. In this work, the maximal total distance considered is 400 km, which in the repeater scenario is divided at least into two segments of maximally 200 km length for each.
- [10] M. Takeoka, S. Guha, M. M. Wilde, *Nat. Commun.* **2014**, *5*, 5235.
- [11] The factor 1.44 stems from the change of base of the logarithm in the Taylor expansion of the secret key capacity, $-\log_2(1 - \eta) = -\frac{\ln(1 - \eta)}{\ln 2} = \frac{\eta}{\ln 2} + O(\eta^2)$, where $\frac{1}{\ln 2} = 1.442695 \dots$ and $\eta \ll 1$.
- [12] S. Pirandola, R. Laurenza, C. Ottaviani, L. Banchi, *Nat. Commun.* **2017**, *8*, 15043.
- [13] S. Pirandola, *Commun. Phys.* **2019**, *2*, 51.
- [14] K. Azuma, K. Tamaki, W. J. Munro, *Nat. Commun.* **2015**, *6*, 10171.
- [15] M. Lucamarini, Z. L. Yuan, J. F. Dynes, A. J. Shields, *Nature* **2018**, *557*, 400.
- [16] For a small-scale experiment along the lines of ref. [14], but circumventing such complications, see ref. [69].
- [17] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, J.-W. Pan, *arXiv:1902.06268*, **2019**.
- [18] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, Z.-F. Han, *arXiv:1902.06884*, **2019**.
- [19] X. Zhong, J. Hu, M. Curty, L. Qian, H.-K. Lo, *arXiv:1902.10209*, **2019**.
- [20] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, L. Jiang, *Sci. Rep.* **2016**, *6*, 20463.
- [21] H.-J. Briegel, W. Dür, J. I. Cirac, P. Zoller, *Phys. Rev. Lett.* **1998**, *81*, 5932.
- [22] For a summary of our graphical symbols to represent QR elements, see Section S1 (Supporting Information).
- [23] N. Sangouard, C. Simon, H. de Riedmatten, N. Gisin, *Rev. Mod. Phys.* **2011**, *83*, 33.
- [24] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, M. D. Lukin, *arXiv:1909.01323*, **2019**.
- [25] Therefore, rates expressed in Hz are bounded above by $\frac{c}{L}$ for a total distance L between Alice and Bob if the quality of their finally shared entangled state depends on entanglement purification.^[20] For instance, for $L = 1000$ km we obtain a rate clearly below 1 kHz. It is thus useful to first consider small-scale repeaters without purification. For larger scales, one could include purification only at the beginning and otherwise replace it by quantum error correction on the

- memories to avoid two-way classical communication over distances beyond one segment length.
- [26] Y.-W. Cho, G. T. Campbell, J. L. Everett, J. Bernu, D. B. Higginbottom, M. T. Cao, J. Geng, N. P. Robins, P. K. Lam, B. C. Buchler, *Optica* **2016**, *3*, 100.
- [27] However, thanks to recent technological developments typical dark count rates can be reduced dramatically (below 1 dark count s^{-1}).
- [28] O. A. Collins, S. D. Jenkins, A. Kuzmich, T. A. B. Kennedy, *Phys. Rev. Lett.* **2007**, *98*, 060502.
- [29] Thus, note that τ_{clock} is a parameter that is determined by the experimental hardware. Additional waiting times for classical signals that depend on the type and the arrangement of the repeater protocol will be treated separately.
- [30] Generally, R_{link} counts the number of raw (quantum) bits (secret bits) transmitted per channel use in a multimode channel with N modes. It is upper bounded by the multimode secret key capacity $-N \log_2(1 - \eta) \approx 1.44 N \eta$.^[12]
- [31] This is consistent with a general “realistic” quantum PPL-capacity bound^[12] in a single-mode QR segment, $-\log_2(1 - P_{\text{link}} \eta^{1/n})$, that exceeds one for $P_{\text{link}} \eta^{1/n} > \frac{1}{2}$ and grows to infinity for $P_{\text{link}} \eta^{1/n} \rightarrow 1$.
- [32] Note that the upper part of Figure 3 below with an appropriate optical encoding, with the memories A and A' each immediately measured in the BB84 bases, and an optical measurement at the middle station would resemble a twin-field scheme for which a $\sqrt{\eta}$ scaling is ideally attainable.
- [33] Note that in our notation for P_{link} we do not make a distinction between links of different mode numbers.
- [34] For a summary of our graphical symbols to represent QR elements, see Section S1 (Supporting Information).
- [35] D. Luong, L. Jiang, J. Kim, N. Lütkenhaus, *Appl. Phys. B* **2016**, *122*, 96.
- [36] F. Rozpędek, K. Goodenough, J. Ribeiro, N. Kalb, V. C. Vivoli, A. Reiserer, R. Hanson, S. Wehner, D. Elkouss, *Quantum Sci. Technol.* **2018**, *3*, 034002.
- [37] F. Rozpędek, R. Yehia, K. Goodenough, M. Ruf, P. C. Humphreys, R. Hanson, S. Wehner, D. Elkouss, *Phys. Rev. A* **2019**, *99*, 052330.
- [38] S. Santra, S. Muralidharan, M. Lichtman, L. Jiang, C. Monroe, V. S. Malinovsky, *arXiv:1811.10723*, **2018**.
- [39] C. T. Nguyen, D. D. Sukachev, M. K. Bhaskar, B. Machielse, D. S. Levonian, E. N. Knall, P. Stroganov, R. Riedinger, H. Park, M. Lončar, M. D. Lukin, *Phys. Rev. Lett.* **2019**, *123*, 183602.
- [40] C. T. Nguyen, D. D. Sukachev, M. K. Bhaskar, B. Machielse, D. S. Levonian, E. N. Knall, P. Stroganov, C. Chia, M. J. Burek, R. Riedinger, H. Park, M. Lončar, M. D. Lukin, *Phys. Rev. B* **2019**, *100*, 165428.
- [41] D. Press, K. De Greve, P. L. McMahon, T. D. Ladd, B. Friess, C. Schneider, M. Kamp, S. Höfling, A. Forchel, Y. Yamamoto, *Nat. Photonics* **2010**, *4*, 367.
- [42] H. Wang, Y.-M. He, T.-H. Chung, H. Hu, Y. Yu, S. Chen, X. Ding, M.-C. Chen, J. Qin, X. Yang, R.-Z. Liu, Z.-C. Duan, J.-P. Li, S. Gerhardt, K. Winkler, J. Jurkat, L.-J. Wang, N. Gregersen, Y.-H. Huo, Q. Dai, S. Yu, S. Höfling, C.-Y. Lu, J.-W. Pan, *Nat. Photonics* **2019**, *13*, 770.
- [43] *Quantum Dots for Quantum Information Technologies* (Ed: P. Michler), Springer, New York **2017**.
- [44] M. Bock, P. Eich, S. Kucera, M. Kreis, A. Lenhard, C. Becher, J. Eschner, *Nat. Commun.* **2018**, *9*, 1998.
- [45] V. Krutyanskiy, M. Meraner, J. Schupp, V. Krcmarsky, H. Hainzer, B. P. Lanyon, *NPJ Quantum Inf.* **2019**, *5*, 72.
- [46] D. Hucul, I. V. Inlek, G. Vittorini, C. Cracker, S. Debnath, S. M. Clark, C. Monroe, *Nat. Phys.* **2015**, *11*, 37.
- [47] M. Körber, O. Morin, S. Langenfeld, A. Neuzner, S. Ritter, G. Rempe, *Nat. Photonics* **2018**, *12*, 18.
- [48] O. Morin, M. Körber, S. Langenfeld, G. Rempe, *Phys. Rev. Lett.* **2019**, *123*, 133602.
- [49] H. Bluhm, S. Foletti, I. Neder, M. Rudner, D. Mahalu, V. Umansky, A. Yacoby, *Nat. Phys.* **2011**, *7*, 109.
- [50] B. Casabone, K. Friebe, B. Brandstätter, K. Schüppert, R. Blatt, T. E. Northup, *Phys. Rev. Lett.* **2015**, *114*, 023602.
- [51] T. G. Ballance, H. M. Meyer, P. Kobel, K. Ott, J. Reichel, M. Köhl, *Phys. Rev. A* **2017**, *95*, 033812.
- [52] SiV serves as a representative of a new class of defect centers in solid-state systems (e.g., group IV-vacancy centers in diamond, defects in SiC or hBN and other 2D materials) currently being investigated with the goal of combining long spin coherence times and favorable optical properties. Whether dilution refrigeration systems are a roadblock is a question of the price one is willing to pay to realize a fiber- and memory-based quantum repeater. It will be a general requirement for all solid-state systems to protect them from their surrounding phonon baths.
- [53] K.-M. Fu, *Physics* **2019**, *12*, 117.
- [54] The apparent discontinuities in the RR curves occur, because the cutoff parameter must always be readjusted depending on distance in order to ensure that a fidelity of at least 0.95 is attained (in particular, the discontinuities are not the result of a numerical simulation; our rate calculations are entirely analytical). For calculating SKR always a fixed cutoff parameter was chosen, although there are actually different optimal cutoffs for different distances. The fixed cutoff was chosen such that over the entire regime of distances, rates cannot be much further improved through cutoff variations.
- [55] To be more specific, for obtaining the curves in Figure 5 (QR cell) we directly use the values for P_{link} from Tables 1 and 2. For the curves in Figure S1 (Supporting Information) (two-segment QR), we use the table values for P_{link} squared and multiplied with one half, since $P_{\text{link}} = P_{\text{source}} \eta_{\text{det}}$ for the cell and $P_{\text{link}} = 1/2(P_{\text{source}})^2 (\eta_{\text{det}})^2$ for the two-segment scheme.
- [56] N. Kalb, A. Reiserer, S. Ritter, G. Rempe, *Phys. Rev. Lett.* **2015**, *114*, 220501.
- [57] C. Kurz, M. Schug, P. Eich, J. Huwer, P. Müller, J. Eschner, *Nat. Commun.* **2014**, *5*, 5527.
- [58] C. Kurz, P. Eich, M. Schug, P. Müller, J. Eschner, *Phys. Rev. A* **2016**, *93*, 062348.
- [59] H. K. Lo, M. Curty, B. Qi, *Phys. Rev. Lett.* **2012**, *108*, 130503.
- [60] S. L. Braunstein, S. Pirandola, *Phys. Rev. Lett.* **2012**, *108*, 130502.
- [61] C. Panayi, M. Razavi, X. Ma, N. Lütkenhaus, *New J. Phys.* **2014**, *16*, 043005.
- [62] S. Abruzzo, H. Kampermann, D. Bruß, *Phys. Rev. A* **2014**, *89*, 012301.
- [63] N. L. Piparo, M. Razavi, W. J. Munro, *Phys. Rev. A* **2017**, *95*, 022338.
- [64] N. L. Piparo, M. Razavi, W. J. Munro, *Phys. Rev. A* **2017**, *96*, 052313.
- [65] Taking into account the additional spin sequences corresponds to the assumption of τ_{clock} being composed of times for spin initialization (e.g., optical pumping), times for preparing internal degrees of freedom (e.g., generation of a spin superposition state), and the emission times (e.g., on spin-dependent transitions). For further details, see Section S6 (Supporting Information).
- [66] From a practical point of view, it appears sensible to assign the same link coupling efficiency to the “local” photons as for those photons that travel through the fiber communication channel, since all sources of loss considered in P_{link} remain present also for the local states in an all-fiber-based setup. Therefore, in our calculations for the NRP-QR cell with teleportation-assisted write-in, we use the same value for P_{link} throughout.
- [67] C. Jones, D. Kim, M. T. Rakher, P. G. Kwiat, T. D. Ladd, *New J. Phys.* **2016**, *18*, 083015.
- [68] While the assumption of a (near-)deterministic write-in is not so unrealistic, for instance, for the atom platform,^[56] another important experimental parameter in this case would be the write-in fidelity, which we do not explicitly include into our simple model here.
- [69] Y. Hasegawa, R. Ikuta, N. Matsuda, K. Tamaki, H.-K. Lo, T. Yamamoto, K. Azuma, N. Imoto, *Nat. Commun.* **2019**, *10*, 378.
- [70] H.-K. Lo, H. Chau, M. Ardehali, *J. Cryptol.* **2005**, *18*, 133.

- [71] L. J. Stephenson, D. P. Nadlinger, B. C. Nichol, S. An, P. Drmota, T. G. Ballance, K. Thirumalai, J. F. Goodwin, D. M. Lucas, C. J. Ballance, *Phys. Rev. Lett.* **2019**, *124*, 110501.
- [72] T. Ruster, C. T. Schmiegelow, H. Kaufmann, C. Warschburger, F. S. Kaler, U. G. Poschinger, *Appl. Phys. B* **2016**, *122*, 254.
- [73] S. Daiss, S. Welte, B. Hacker, L. Li, G. Rempe, *Phys. Rev. Lett.* **2019**, *122*, 133603.
- [74] Gerhard Rempe, private communication.
- [75] E. Shchukin, F. Schmidt, P. van Loock, *Phys. Rev. A* **2019**, *100*, 032322.
- [76] P. C. Humphreys, N. Kalb, J. P. J. Morits, R. N. Schouten, R. F. L. Vermeulen, D. J. Twitchen, M. Markham, R. Hanson, *Nature* **2018**, *558*, 268.
- [77] H. Bluhm, S. Foletti, I. Neder, M. Rudner, D. Mahalu, V. Umansky, A. Yacoby, *Nat. Phys.* **2011**, *7*, 109.
- [78] M. Gurioli, Z. Wang, A. Rastelli, T. Kuroda, S. Sanguinetti, *Nat. Mater.* **2019**, *18*, 799.
- [79] D. Huber, M. Reindl, Y. Huo, H. Huang, J. S. Wildmann, O. G. Schmidt, A. Rastelli, R. Trotta, *Nat. Commun.* **2017**, *8*, 15506.
- [80] Y. Chen, M. Zopf, R. Keil, F. Ding, O. G. Schmidt, *Nat. Commun.* **2018**, *9*, 2994.
- [81] F. B. Basset, M. B. Rota, C. Schimpf, D. Tedeschi, K. D. Zeuner, S. F. Covre da Silva, M. Reindl, V. Zwiller, K. D. Jöns, A. Rastelli, R. Trotta, *Phys. Rev. Lett.* **2019**, *123*, 160501.
- [82] M. Zopf, R. Keil, Y. Chen, J. Yang, D. Chen, F. Ding, O. G. Schmidt, *Phys. Rev. Lett.* **2019**, *123*, 160502.
- [83] J. Zhang, J. S. Wildmann, F. Ding, R. Trotta, Y. Huo, E. Zallo, D. Huber, A. Rastelli, O. G. Schmidt, *Nat. Commun.* **2015**, *6*, 10067.
- [84] R. de Sousa, S. D. Sarma, *Phys. Rev. B* **2003**, *68*, 115322.
- [85] D. A. Gangloff, G. Éthier-Majcher, C. Lang, E. V. Denning, J. H. Bodey, D. M. Jackson, E. Clarke, M. Hugues, C. L. e Gall, M. Atatüre, *Science* **2019**, *364*, 62.
- [86] K. M. Weiss, J. M. Elzerman, Y. L. Delley, J. Miguel-Sanchez, A. Imamoglu, *Phys. Rev. Lett.* **2012**, *109*, 107401.
- [87] H. Wang, Y.-M. He, T.-H. Chung, H. Hu, Y. Yu, S. Chen, X. Ding, M.-C. Chen, J. Qin, X. Yang, R.-Z. Liu, Z.-C. Duan, J.-P. Li, S. Gerhardt, K. Winkler, J. Jurkat, L.-J. Wang, N. Gregersen, Y.-H. Huo, Q. Dai, S. Yu, S. Höfling, C.-Y. Lu, J.-W. Pan, *Nat. Photonics* **2019**, *13*, 770.
- [88] J. Liu, R. Su, Y. Wei, B. Yao, S. F. C. D. Silva, Y. Yu, J. Iles-Smith, K. Srinivasan, A. Rastelli, J. Li, X. Wang, *Nat. Nanotechnol.* **2019**, *14*, 586.
- [89] H. Wang, H. Hu, T.-H. Chung, J. Qin, X. Yang, J.-P. Li, R.-Z. Liu, H.-S. Zhong, Y.-M. He, X. Ding, Y.-H. Deng, Q. Dai, Y.-H. Huo, S. Höfling, C.-Y. Lu, J.-W. Pan, *Phys. Rev. Lett.* **2019**, *122*, 113602.
- [90] S. Unsleber, Y.-M. He, S. Gerhardt, S. Maier, C.-Y. Lu, J.-W. Pan, N. Gregersen, M. Kamp, C. Schneider, S. Höfling, *Opt. Express* **2016**, *24*, 8539.
- [91] J. Iles-Smith, D. P. S. McCutcheon, A. Nazir, J. Mørk, *Nat. Photonics* **2017**, *11*, 521.
- [92] H. Snijders, J. A. Frey, J. Norman, V. P. Post, A. C. Gossard, J. E. Bowers, M. P. van Exter, W. Löffler, D. Bouwmeester, *Phys. Rev. Appl.* **2018**, *9*, 031002.
- [93] T. Gissibl, S. Thiele, A. Herkommer, H. Giessen, *Nat. Photonics* **2016**, *10*, 554.
- [94] T. van Leent, M. Bock, R. Garthoff, K. Redeker, W. Zhang, T. Bauer, W. Rosenfeld, C. Becher, H. Weinfurter, *Phys. Rev. Lett.* **2020**, *124*, 010510.
- [95] J. H. Weber, B. Kambs, J. Kettler, S. Kern, J. Maisch, H. Vural, M. Jetter, S. L. Portalupi, C. Becher, P. Michler, *Nat. Nanotechnol.* **2019**, *14*, 23.
- [96] A. Dréau, A. Tchebotareva, A. El Mahdaoui, C. Bonato, R. Hanson, *Phys. Rev. Appl.* **2018**, *9*, 064031.

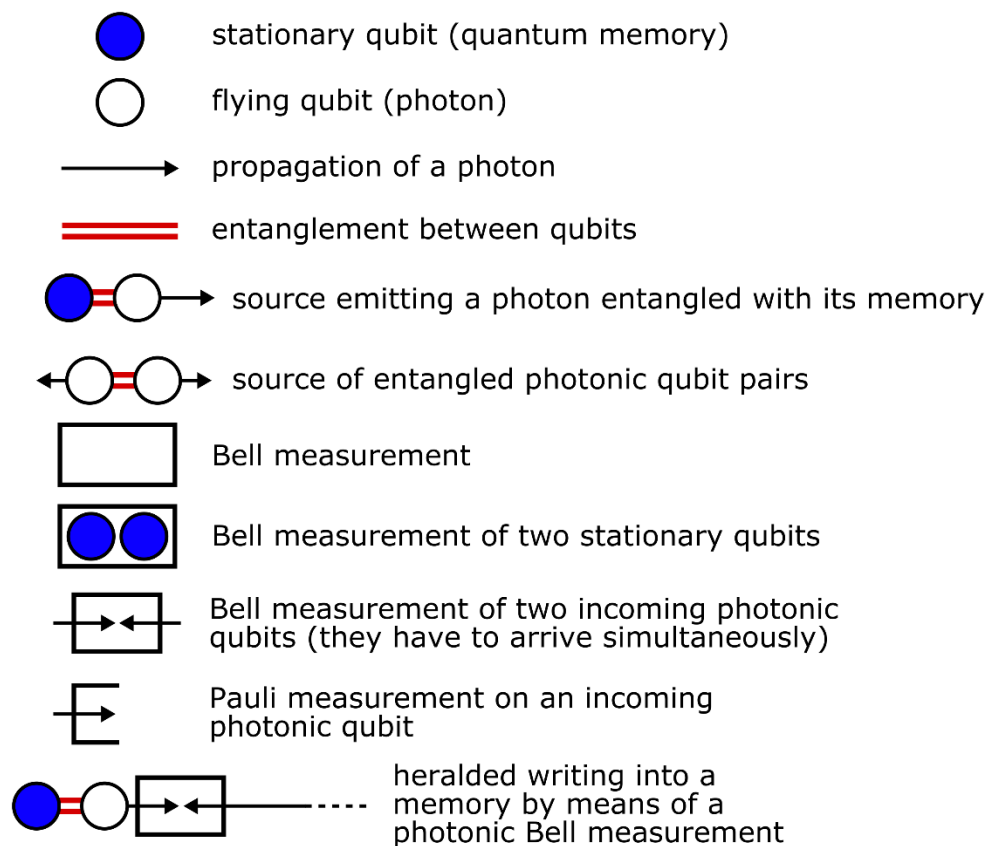
Supporting Information

Extending Quantum Links: Modules for Fiber- and Memory-Based Quantum Repeaters

Peter van Loock, Wolfgang Alt, Christoph Becher, Oliver Benson, Holger Boche, Christian Deppe, Jürgen Eschner, Sven Höfling, Dieter Meschede*, Peter Michler, Frank Schmidt, Harald Weinfurter*

S1. Graphical language, experimental parameters, and figures of merit

Here we summarize the graphical symbols as used in this paper, which we propose for a visual representation of the structure and the protocols of QR links.



We further summarize the most important experimental parameters and the figures of merit to assess the performance of a QR link:

P_{link}	zero-length coupling efficiency, link coupling efficiency
τ_{clock}	source/memory clock time (inverse clock rate)
τ_{coh}	memory coherence time
η	fiber channel transmission efficiency, amplitude damping parameter for a single-mode loss channel
\mathcal{R}	raw rate in Hz (number of qubits transmitted per time and per mode)
R	raw rate (number of qubits transmitted per channel use), inverse average number of qubit transmission attempts needed for one success
R_{link}	multi-mode link efficiency, raw rate (number of qubits transmitted in link per channel use)
T_0	elementary time unit, effective time consumed per channel use, effective time duration for one transmission/distribution attempt
SKR	secret key rate (number of secret bits per channel use and per mode)
RR	raw rate with fidelity bound (number of qubits/ebits per channel use and per mode)
c	speed of light in a fiber channel: $2 \cdot 10^8$ m/s
L_{att}	attenuation length in a fiber channel: 22 km

S2. Memory dephasing model including cutoff and secret key rates for QKD

The memory error model we shall consider is pure memory dephasing as described by

$$\rho \rightarrow \frac{1}{2} \left(1 + \exp\left(-\frac{t}{\tau_{coh}}\right) \right) \rho + \frac{1}{2} \left(1 - \exp\left(-\frac{t}{\tau_{coh}}\right) \right) Z \rho Z,$$

where $\frac{1}{2} \left(1 - \exp\left(-\frac{t}{\tau_{coh}}\right) \right)$ is the probability for a Pauli-Z phase-flip to occur on the state of a single memory qubit.

For the case of two QR segments or, equivalently, a QR cell with two half segments, we define a random variable M as $|X_1 - X_2|$ where X_1 and X_2 are independent geometrically distributed random variables describing the number of attempts until success in a single (half) segment. This means the random variable M counts the number of time steps for which either one of the two memories (i.e. the first memory whose link has been successfully established via detection of a transmitted photon) has to wait for the other one that still attempts to be connected. The waiting quantum memory is subject to dephasing for a duration of MT_0 . Here T_0 is the time duration per attempt whose value is protocol-dependent and, for simplicity, two additional protocol-dependent extra units of dephasing, $2T_0$, are omitted in M (in the quantitative rate analysis and in the plots for the NSP protocol, these two units are included, see below).

Either of the protocols as described in the main text can be effectively treated like an entanglement swapping (quantum teleportation) process in which a final effective entangled state emerges after the BM on the two quantum memories at the central node. Considering a suitable Pauli correction (depending on the BM result) and tracing out the two measured memories, this final state takes the form of

$$\frac{1}{2} \left(1 + \exp \left(-M \frac{T_0}{\tau_{coh}} \right) \right) |\phi^+\rangle\langle\phi^+| + \frac{1}{2} \left(1 - \exp \left(-M \frac{T_0}{\tau_{coh}} \right) \right) |\phi^-\rangle\langle\phi^-|,$$

where $|\phi^\pm\rangle$ are the two two-qubit Bell states $|\phi^\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$.

We remark that depending on the protocol and the application we may not actually prepare such an entangled state (for instance, physically present in two spatially separated quantum memories). Instead, in the QKD context, we convert e.g. the usual BB84 protocol that does not rely on physically distributing entangled states into an equivalent entanglement-based QKD protocol, thus simplifying the theoretical analysis. This equivalence can be understood

in the following way. Suppose Alice prepares the state $|\phi^+\rangle$ and sends one half to Bob. After its arrival, Alice and Bob perform X - and Z -measurements on their halves of the entangled state. Then Alice's measurement acts only on the Hilbert space of her qubit and therefore it commutes with Bob's measurement and possible attacks by Eve. Consequently, she could also perform her measurement before she sends her half to Bob, which is equivalent to preparing and sending BB84 states to Bob. Also notice that the BM on the memories takes place after two successful detections and therefore the Pauli correction can be applied simply on the level of the classical post-processing of the measurement data. We need to save all measurement results and any information about the state preparations and in the end we can discard the information for those cases where the transmission failed.

For the probability distribution of the random variable M we obtain (p is the success, $q=1-p$ the failure probability for one attempt related with the individual geometric random variables)

$$\mathbb{P}(M = 0) = \sum_{k=1}^{\infty} \mathbb{P}(X_1 = X_2 = k) = \sum_{k=1}^{\infty} p^2 q^{2(k-1)} = \frac{p}{2-p},$$

and for $j > 0$,

$$\mathbb{P}(M = j) = \sum_{k=1}^{\infty} 2p^2 q^{2(k-1)+j} = \frac{2pq^j}{2-p},$$

where the factor 2 comes from the fact that both cases $X_1 > X_2$ and $X_2 > X_1$ are possible. This allows us to calculate the following expectation value,

$$\mathbb{E}\left(\exp\left(-M \frac{T_0}{\tau_{coh}}\right)\right) = \frac{p}{2-p} \left(\frac{2}{1 - q \exp\left(-\frac{T_0}{\tau_{coh}}\right)} - 1 \right),$$

and by summing only up to a cutoff constant m instead of infinity, including a renormalization of the probability distribution, one can easily obtain the expectation value for protocols which

abort after the memory has dephased for a predetermined, given number of time steps (attempts). Again note that, depending on the protocol, the overall state may be subject to dephasing for an additional constant amount of $2T_0$. In the case of the NSP protocol, we first generate entanglement between the memory and a photon, and as the next step we send this photon to a detector over a distance $L_0 = L/2$. Then the detector sends a classical signal to the memory announcing whether the photon was detected or not. Therefore, we have to wait for a time unit of $T_0 = 2L_0/c = L/c$ until we can decide which action should be applied to the memory: storage of the qubit or initialization for a new attempt. Hence, the memory would always decohere for at least one such time step, even in the case when the very first attempt is already successful. Since this argument applies to both memories, the total state decoheres (is subject to dephasing) for $M + 2$ time steps, each with duration $T_0 = L/c$.

However, if we consider the NRP protocol, we send photons to the memory and therefore the memories (almost) immediately know when a transmission was successful. As a consequence, there is no additional constant dephasing in this case and T_0 is simply given via the repetition rate of the photon source or the local processing times including the write-in time, whichever is longer.

Using the BB84 protocol,¹ we obtain an ideal asymptotic secret key fraction of $1 - h(e_x) - h(e_z)$, where $h(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$ is the binary entropy and e_x, e_z are the error rates in the X and Z basis, respectively. Since the Z-error rate is equivalently given by the probability to obtain the effective state $|\psi^\pm\rangle$, one can easily see that e_z is zero in our error model. Similarly, the X-error rate is given by the probability to obtain $|\psi^-\rangle$ or $|\phi^-\rangle$ and is therefore given by $\frac{1}{2} \left(1 - \mathbb{E}(\exp(-M \frac{T_0}{\tau_{coh}}))\right)$ up to the protocol-dependent constant dephasing. Hence the asymptotic secret key fraction is given by

$1 - h\left(\frac{1}{2} \left(1 - \mathbb{E}(\exp(-M \frac{T_0}{\tau_{coh}}))\right)\right)$, and the final secret key rate is then the product of the raw rate (the so-called ‘‘yield’’) and this secret key fraction.

Also notice that the binary entropy function takes on its maximum of 1 when the argument of the function is $\frac{1}{2}$. Thus, we always obtain a non-zero secret key fraction, which is a specific

¹ We consider the biased BB84 scheme here where one of the two bases is employed more often than the other which, in the asymptotic limit of infinite repetitions, allows to remove the $\frac{1}{2}$ factor in the rates of standard BB84 and increase the sifting factor to unity.^[50]

feature of our error model. If we also consider additional error sources like, for example, imperfect (though still deterministic) BMs on the memories, we typically have non-zero error rates in both the X and the Z basis (unlike the sole phase-flip error in the effective entangled state above). Therefore, the secret key fraction can become zero and we typically get more demanding requirements for the memory coherence times.

S3. Calculation of raw rates

The performance of a QR may be quantified by the secret key rate that can be obtained for a given length L of the quantum channel connecting the two parties Alice and Bob who aim to securely communicate with each other. Besides the secret key fraction, for calculating the (asymptotic) secret key rate, we need an expression for the raw rate, i.e. in our case, the number of quantum bits that can be transmitted over a lossy channel of length L , employing that channel once and sending one optical mode through that channel (i.e. “per channel use” and “per mode”). As the memory-based QR has at least one intermediate station as opposed to a PPL for direct transmission, it may not be immediately obvious how to count the channel uses. In our case, one channel use corresponds to one attempt to establish a link, and because the two (half) segments can be simultaneously attempted to be bridged, the total number of attempts, on average, to transmit one qubit over the entire distance can be expressed by $\mathbb{E}(\max(X_1, X_2))$. The probability for successfully transmitting one qubit can then be written as $1/\mathbb{E}(\max(X_1, X_2))$. This then corresponds to the number of qubits transmitted per channel use, i.e. a dimensionless raw rate expressed per channel use.

The effect of imperfect quantum memories, i.e., quantum memories with finite coherence times (see the dephasing model of the preceding section), can be taken into account in the raw rate by imposing a maximally allowed storage time of the loaded memory at the central station waiting for a second transmission to succeed. In other words, the QR protocol is

aborted as soon as a quantum memory's storage time limit is exceeded. If this "cutoff" is chosen to be well below the memory's coherence time, one can ensure that the quality of the entangled light-matter state is still so high and hence that of the final (effective) entangled state too, such that errors are negligible. In the QKD context, this corresponds to a secret key fraction near unity. However, such an approach would be at the expense of the raw rate, because aborting and restarting the protocol more frequently for a small cutoff time means that it takes longer to finally distribute a qubit over the total distance, thus reducing the raw rate. Due to this trade-off, there is an optimal cutoff that maximizes the secret key rate. Nonetheless, we shall also consider sufficiently small cutoffs that lead to fidelities of the final (effective) entangled states that are above a certain fidelity value. This may also be relevant for applications different from QKD. Generally, smaller memory coherence times and thus shorter storage time limits require a correspondingly faster abortion and restart of the protocol leading to a smaller transmission probability. For the NSP protocol, this effect depends on the total distance L , because for larger L , the required storage time per transmission attempt grows such that for a given, fixed memory coherence time the effective memory efficiency drops, which becomes visible in the QR performance. As a consequence, in this case, the cutoff becomes distance-dependent in order to keep the fidelity above a certain threshold and the maximal secret key rates have smaller optimal cutoffs for larger distances. In the NRP protocol, this L -dependence disappears, because the quantum signals are sent to, and no longer emitted from, the quantum memories, in which case the duration of every transmission attempt only depends on the source's repetition rate and the local processing / write-in times, and no longer on the distance between memories and detectors.

Calculating the expression $1/E(\max(X_1, X_2))$, the dimensionless raw rate (or qubit transmission probability) for a memory-based scheme with one central memory node including memory cutoff time is given by ^[23,57]

$$R(m) = \frac{p [2 - p - 2q^{m+1}]}{3 - 2p - 2q^{m+1}} P_{\text{BM}} .$$

Here, p and q are again the success and failure probabilities of a single attempt in one (half) segment of length $L/2$. Thus, for deterministic local state preparations (or, more generally, unit link coupling efficiencies), we have $p = \sqrt{\eta}$. The final BM efficiency on the two memories is included via the extra factor P_{BM} , which can be set to one for a deterministic BM ($P_{\text{BM}} = 1$ in the following). The parameter m determines the maximal acceptable number of attempts (the above-mentioned memory cutoff) a loaded memory is allowed to wait for a second successful transmission attempt. Note that for $m = 0$ we obtain the no-memory case, corresponding to $R(0) = p^2 = \eta$, which is just the result one obtains for direct transmission, i.e. the ‘‘repeaterless’’ bound for distance L (for not too small L). Conversely, for $m \rightarrow \infty$ (corresponding to the perfect memory case with no need for aborting the protocol), we have $R \rightarrow \frac{p(2-p)}{3-2p} \equiv R(m \rightarrow \infty)$, which, for small p becomes approximately $R \approx \frac{2}{3} p \sim \sqrt{\eta}$ (and this scaling becomes $\eta^{1/n}$ for n repeater segments). The $\sqrt{\eta}$ -scaling corresponds to the optimal transmission in a memory-based QR with a single node or, equivalently, two segments.

S4. Additional results: two-segment QR in the NSP protocol

In comparison to the rates of the NSP-QR cell (illustrated by Fig. 4b) as shown in Fig. 5, below we also present the rates calculated for the two-segment QR as illustrated by Fig. 4a. The subtle differences between these two small-scale QR variants are discussed in the main text. In addition to the short discussion there, let us emphasize here that for a reasonable comparison, we did not include dephasing errors on the outer memories (those most left and right in Fig. 4a). Practically, in the context of QKD, this means that Alice and Bob would immediately measure their qubits and not store any quantum states at all; thus, storage again

takes place only at the central node. On the other hand, such an approach prevents the two-segment scheme from its possible use beyond QKD, because the two-segment scheme is potentially more versatile compared with the NSP-QR cell when the outer memories of the two segments are also exploited for quantum storage.

One can see that comparing the two QR variants (Fig. S1 with Fig. 5 of the main text) there is a visibly better performance of the QR cell. Some platforms that enter the repeater regimes for the QR cell no longer achieve this for the two-segment scheme.

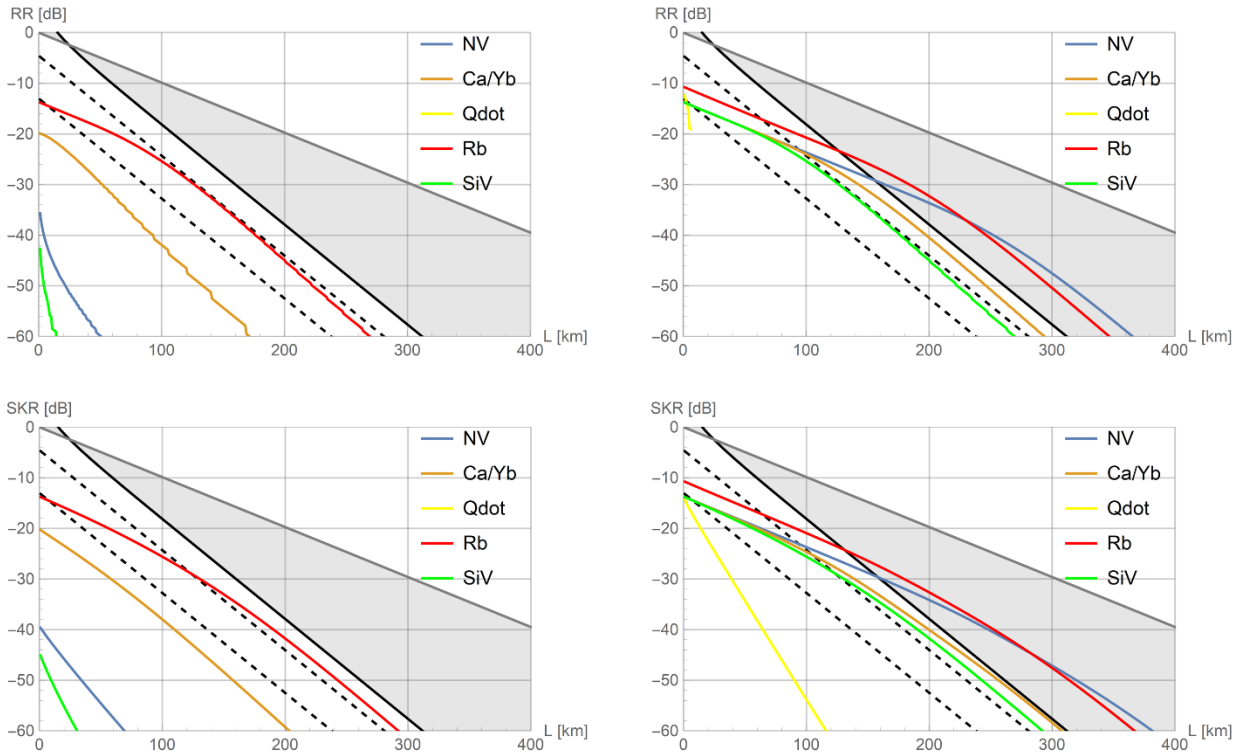


Fig. S1: Secret Key Rates (SKR) and High-Fidelity Raw Rates (RR) for a small NSP-based QR scheme (two-segment QR). The bottom plots show SKR in dB as a function of the total distance L in km for experimental parameters as currently available (left) and as potentially available in the future (right). The top plots show RR in schemes where the entangled states effectively created over the total distance L have a fidelity of at least 0.95 (left: current parameters, right: future parameters). Curves that are disappearing beyond certain distances (or completely missing) no longer (never) exceed $F=0.95$. The different platforms correspond to NV (violet) and SiV (green) centers, ions (brown), Rubidium atoms (red), and quantum dots (yellow). The light grey area illustrates the (secret key) rate regime between $\sim\eta$ (curve in bold black: “repeaterless” bound) and $\sqrt{\eta}$ (line in dark grey: optimal rate for QR cells or two-segment QR schemes). The bold black dashed lines represent the realistic “repeater-less” bound $P_{\text{link}}\eta/2$ (direct transmission via PPL) with finite link efficiencies $P_{\text{link}} = 0.1, 0.7$.

S5. Additional results: Bell-state measurement-assisted memory write-in (NRP)

In comparison to the rates of the NRP-QR cell with ideal unit write-in efficiency as shown in Fig. 7, below we also present the rates calculated for the scheme based on quantum teleportations of the arriving photonic qubits onto the spin qubits with the help of locally prepared spin-photon entangled states and linear optical BMs (see Fig. 6b). In this case, instead of assuming unit write-in efficiency like for the rates calculated in Fig. 7 (where the values for $P_{link} = P_{source}$ are directly taken from Tables 1 and 2), we have $P_{write} = \frac{1}{2} P_{source} (\eta_{det})^2$ and hence $P_{link} = P_{source} P_{write} = \frac{1}{2} (P_{source})^2 (\eta_{det})^2$. For obtaining the curves in Fig. S2, we thus use for P_{link} the Table values squared and multiplied with one half (without explicitly considering the factor $(\eta_{det})^2$). Moreover, the additional sequences for spin reinitialization are included in $(\tau_{clock})^{-1}$ (numbers in brackets in Tables 1 and 2).

For current experimental parameters, where previously with ideal and fast photon-spin interfaces all platforms entered the repeater regimes (Fig. 7), we now observe that under the assumption of non-deterministic and slow interfaces, most platforms stay within the “repeater-less” regimes. Only the secret key rate for Rubidium atoms slightly exceeds the limit. Note that the curves for NV and SiV color centers completely overlap, since the relevant factor that counts the number of possible distribution attempts within the memory coherence time is equal for both, $\tau_{coh}/\tau_{clock} = 5000$ (while the individual times are different). Here, NV and SiV also share the same link coupling efficiency, $P_{link} = 0.05$, which appears to be the stronger limitation for the distances considered when compared with the values for Rubidium, $P_{link} = 0.5$ and $\tau_{coh}/\tau_{clock} = 500$, especially because the Table values for P_{link} now enter quadratic into the rates.

This discussion also serves as a nice illustration that the actual memory efficiency in a QR protocol depends on the ratio of the coherence time and the (effective) repetition time. With future parameters, for all platforms, the repeater regimes can still be entered and the repeater rate slopes can be fairly well maintained over 400 km despite the non-unit write-in efficiency and slower interfaces.

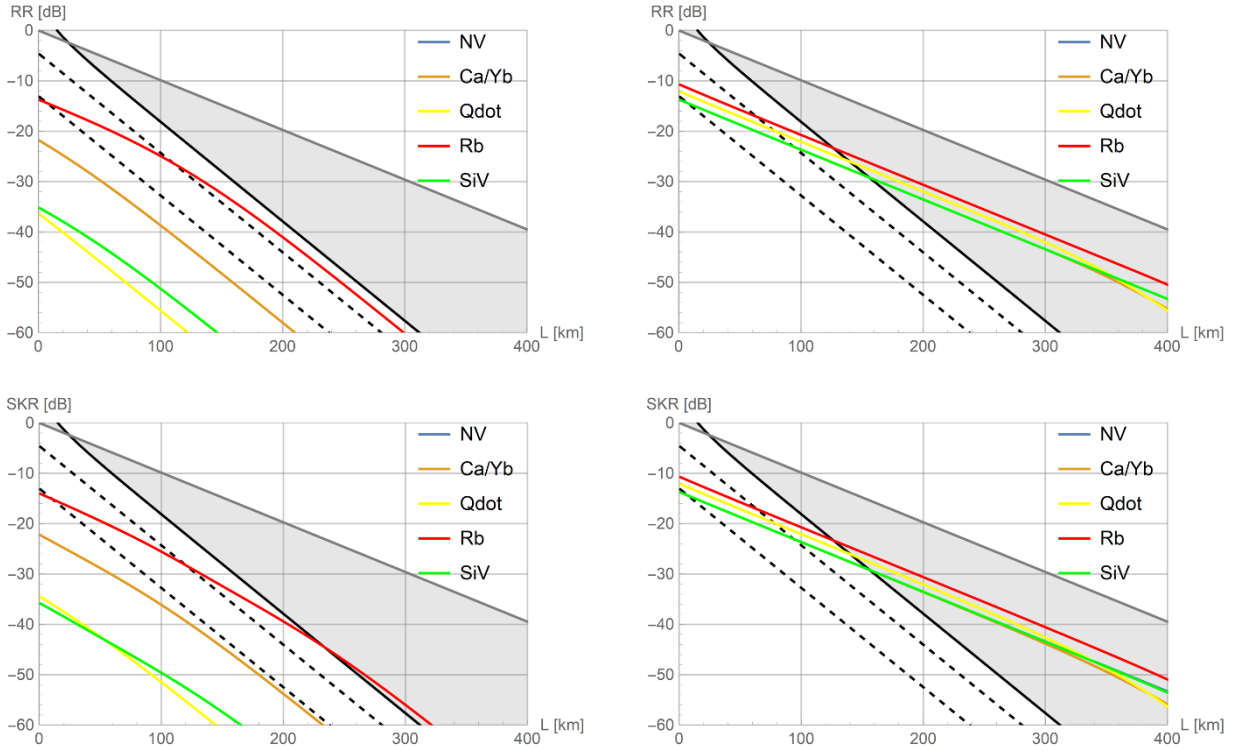


Fig. S2: Secret Key Rates (SKR) and High-Fidelity Raw Rates (RR) for a small NRP-based QR scheme (QR cell with linear optical teleportation-assisted memory write-in). The bottom plots show SKR in dB as a function of the total distance L in km for experimental parameters as currently available (left) and as potentially available in the future (right). The top plots show RR in schemes where the entangled states effectively created over the total distance L have a fidelity of at least 0.95 (left: current parameters, right: future parameters). The different platforms correspond to NV (violet) and SiV (green) centers, ions (brown), Rubidium atoms (red), and quantum dots (yellow). The NV curves are invisible coinciding with those of the SiV platform. The light grey area illustrates the (secret key) rate regime between $\sim\eta$ (curve in bold black: “repeaterless” bound) and $\sqrt{\eta}$ (line in dark grey: optimal rate for QR cells or two-segment QR schemes). The bold black dashed lines represent the realistic “repeater-less” bound $P_{link}\eta/2$ (for direct transmission via PPL) with finite link efficiencies $P_{link} = 0.1, 0.7$.

S6. Remarks on QR parameters, wavelength conversion and fiber-coupling efficiencies

We will give a few additional details especially regarding the future experimental parameters of the three hardware platforms (as given in Table 2). The discussion here will also include some remarks and additional rate calculations concerning the use of wavelength converters.

For NV centers we extrapolate the values of Refs. [25,26] for the link coupling efficiency and the clock rate, excluding additional spin sequences, and for the coherence time assuming a ^{13}C nuclear spin for the memory. Similar assumptions are made for the SiV centers based on Refs. [21,28,29]. As already mentioned in the main text, the SiV platform provides a potentially more efficient photon-spin interface including higher cooperativities. More specifically, in the recent experiment of Ref. [21], the SiV centers are placed inside a cavity with a cooperativity of 105, leading to a Purcell factor ~ 200 and shortening the spontaneous emission time of a SiV center to below 100 ps. This would, in principle, result in even higher clock rates than 500 MHz. However, the experimental data of Ref. [21] were collected including extra spin sequences after a certain fixed and finite number of distribution attempts. Averaging over these extra sequences eventually leads to an overall clock rate \sim MHz. Overall a full system detection efficiency of about 85% was deduced in Ref. [21] exceeding our assumed value of 50% for the link coupling efficiency. Reference [28] extended the SiV electron spin coherence time by swapping to a ^{13}C nuclear spin reaching a number above 100 ms. To sum up, in Table 2 we give numbers for SiV that have been achieved individually already, but we refer to them as future values as they have to be achieved concurrently in a single system.

When including the minimal times required for spin reinitialization etc. (τ_{clock} including initialization, preparation, and emission times), current NV experiments^[58] have already demonstrated clock times τ_{clock} as low as 2 μs corresponding to clock rates of 500 kHz (here

the main limitation appears to be the spin initialization). This number is the NV clock rate (number in brackets) in Table 1. As for the future clock rates (Table 2), we assume that for the spin initialization at least one cycle involving the NV singlet system must be completed while the lifetime of the lowest singlet state is ~ 200 ns. This corresponds to a clock rate of 5 MHz (Table 2, number in brackets). In the case of SiV, we currently assume a (slow) clock rate of 5 MHz (Table 1, number in brackets), which is an order of magnitude larger than that for NV, since the spin initialization mechanism is different (independent of a singlet system). However, as the coherence time of SiV is assumed to be an order of magnitude smaller than that for NV, the relevant dephasing factor is equal for both, $\tau_{coh}/\tau_{clock} = 5000$. The slow, future SiV clock rate value is assumed to be 50 MHz (Table 2, number in brackets). In this case, the spin initialization is limited by the duration for one cyclic optical transition. Based on the number of Table 1 (5 MHz), assuming 100 cycles until a spin flip, and considering an extra gain by a factor of 10 through the possibility of Purcell cant, a future clock rate of 50 MHz seems feasible.

For the quantum dot platform, the numbers given in the Tables correspond to the most commonly studied and highly performant quantum dots, namely InGaAs strained quantum dots. However, already published results (at low temperature in the mK regime using gate defined quantum dots in GaAs as III-V material) have reported coherence times on the order of 300 μ s based on dynamical decoupling.^[59] These existing experimental parameters can be, in principle, linked to the optical regime. Recent material physics developments in the growth of strain-free GaAs quantum dots (i.e., fabricated by droplet epitaxy^[60,61]) have also made significant progress and these systems have now a quality comparable to strained InGaAs quantum dots. In fact, in Ref. [62], highly entangled photons were efficiently extracted from symmetric GaAs quantum dots, based on the earlier work reported in Ref. [61]. In the context of implementing a quantum repeater, it is worth mentioning that with the same GaAs quantum

dot system, photonic entanglement swapping has been demonstrated.^[63,64] Moreover, the emission of entangled photon pairs based on quantum dots at a clock rate of 400 MHz was demonstrated already five years ago.^[65]

The level of control of the nuclear spin system which is the main source of spin dephasing also improved dramatically recently, for instance, via optically pumped nuclear state narrowing techniques.^[66] Coherent addressing of nuclear spin waves promises^[67] further enhanced coherence times. Furthermore, using quantum dot molecules one can employ single/triplet qubit bases which are less sensitive to electric and magnetic field fluctuations^[68] as another approach to improve the coherence times in quantum dot systems.

Important efficiency parameters for a quantum repeater based on the quantum dot platform are the photon collection and fiber-coupling efficiencies. Photon collection efficiencies between 60% - 85% have already been reported for quantum dot micropillar and so-called bullseye cavities.^[69,70,71,72] Theoretical values of up to 96% have been estimated in Ref. [73]. To achieve such values one can optimize the cavity design to improve unidirectional emission, and at the same time optimize the vertical and lateral design of the etching processes. For instance, for the bullseye it is known that the exact thicknesses of the epitaxial membrane structure and the lateral grating are critical to obtain maximal values. Moreover, the quantum dot needs to be well located, which can be realized via deterministic placement techniques.

For the fundamental mode of laser light (Gaussian TE₀₀ mode), fiber-coupling efficiencies of 80% - 90% can be achieved in the labs. To achieve a comparable value for a quantum dot light source, the quantum dot has to be embedded into a cavity structure exhibiting a nearly Gaussian fundamental mode. This is possible for the pillar and bullseye microcavities. Excellent cavity-mode-to-fiber coupling efficiency of 85% have already been achieved.^[74]

Additionally, one can implement a new type of 3D printed micro- and nano-optics with complex lens designs for photon collection.^[75] This allows for high optical performance and corrects for aberrations when imaging at wide angles. We therefore anticipate fiber-coupling efficiencies in optimized cavities on the order of 80% - 90%.

For the ion platform, we refer to existing and potential future experiments with Calcium and Ytterbium. The current parameters for Calcium are extracted from the recent experimental results of Ref. [51] where the clock rate of 7 kHz is fairly small in comparison with the other platforms (Table 1, number in brackets). A higher clock rate with $(\tau_{clock})^{-1} = 0.47$ MHz has been achieved for Ytterbium.^[52] However, the link coupling efficiency in that Ytterbium-based experiment^[52] was smaller ($P_{link} = 1.2\%$) than that obtained in the Calcium-based experiment^[51] ($P_{link} = 25\%$). Nonetheless, for the rate calculations based on Table 1 using the faster clock rate (Fig. 7), we assume as well the higher value for P_{link} , as the two relevant experiments are both from the ion platform. Similarly, for the memory coherence time we choose a value of 20 ms throughout.^[51] As for the future parameters, we refer again to Ref. [51] where ~25% photon-to-fiber link coupling probability per attempt was demonstrated. Based on this result, assuming more efficient detectors and moderately improved ion-cavity coupling, we infer as an extrapolation a future link coupling efficiency of 50%. A clock rate of 1 MHz has already been achieved in Ref. [53] in a system without cavity, and this also appears to be applicable to an ion-cavity system provided that the cavity is sufficiently short, like in Ref. [38]. The memory coherence time is an already demonstrated value from Ref. [54].

Finally, for the Rubidium atom platform, the currently available values for P_{link} and τ_{coh} refer to reported experiments with Rubidium atoms in a cavity.^[34,35] More specifically, atomic eigenstates can be chosen for the qubit encoding such that the effect of external magnetic fields is significantly reduced. This way coherence times above 100 ms have been

measured.^[34] Also from an earlier experiment, demonstrating atom-atom entanglement as highly relevant in the context of quantum repeaters, we can infer a link coupling efficiency of 50% which can be further improved. Typical values for the clock rate in these experiments, including additional operations such as intermediate atom cooling, are about 5 kHz (Table 1, number in brackets). The assumption of potentially higher values then depends on a repeater protocol that circumvents such slow additional sequences. Generally, the state fidelity plays an important role for the atom platform. While currently fidelities of almost 70% are possible,^[55] with realistic fiber-based cavities of higher cooperativity fidelities of up to 96% should be possible.^[56] As a main challenge, like for all platforms, it is crucial to combine high values of the three experimental parameters proposed in our simple model together with sufficiently high state fidelities in a single system.

Let us finally comment on the quantitative effect of wavelength converters for switching from the sources' and memories' wavelengths to the telecom wavelength as most suitably adapted to a fiber communication channel. In our model, the effect of these converters can be absorbed into P_{link} via a wavelength conversion efficiency. For simplicity, we assume a constant factor of $\frac{1}{2}$ for all platforms, while the relevant wavelengths in some platforms are certainly harder to convert than in others. Quantum frequency conversion nonetheless now achieves device efficiencies exceeding 50%. In particular, for Rubidium atoms, atom-telecom-photon entanglement was recently demonstrated with a conversion efficiency of 57%.^[76] For ions and quantum dots, conversion efficiencies of almost 30% and exceeding 30% were reported in Ref. [33] and Ref. [77], respectively. Current experiments with Calcium ions produce (yet unpublished) experimental data compatible with a conversion efficiency above 50% (based on the earlier experiment achieving above 25%,^[33] see also Ref. [51] for a Calcium ion experiment that achieved 25% conversion efficiency). For NV color centers, an existing experiment reports a conversion efficiency of 17%.^[78] Thus, again, in all platforms,

conversion to telecom wavelength has been experimentally demonstrated with efficiencies of similar order of magnitude. We shall then analyze what the general effect of the assumed factor $\frac{1}{2}$ reduction of P_{link} on the repeater rates is.

The figures below show the repeater rates calculated based on our model including throughout an additional factor of $\frac{1}{2}$ for the experimental parameter P_{link} . Figure S3 corresponds to the rates of the NSP-QR cell as shown in Fig.5, but this time including the conversion efficiency. Although the overall effect of the extra inefficiency does not appear dramatic, some platforms that previously enter the repeater regimes now no longer achieve this.

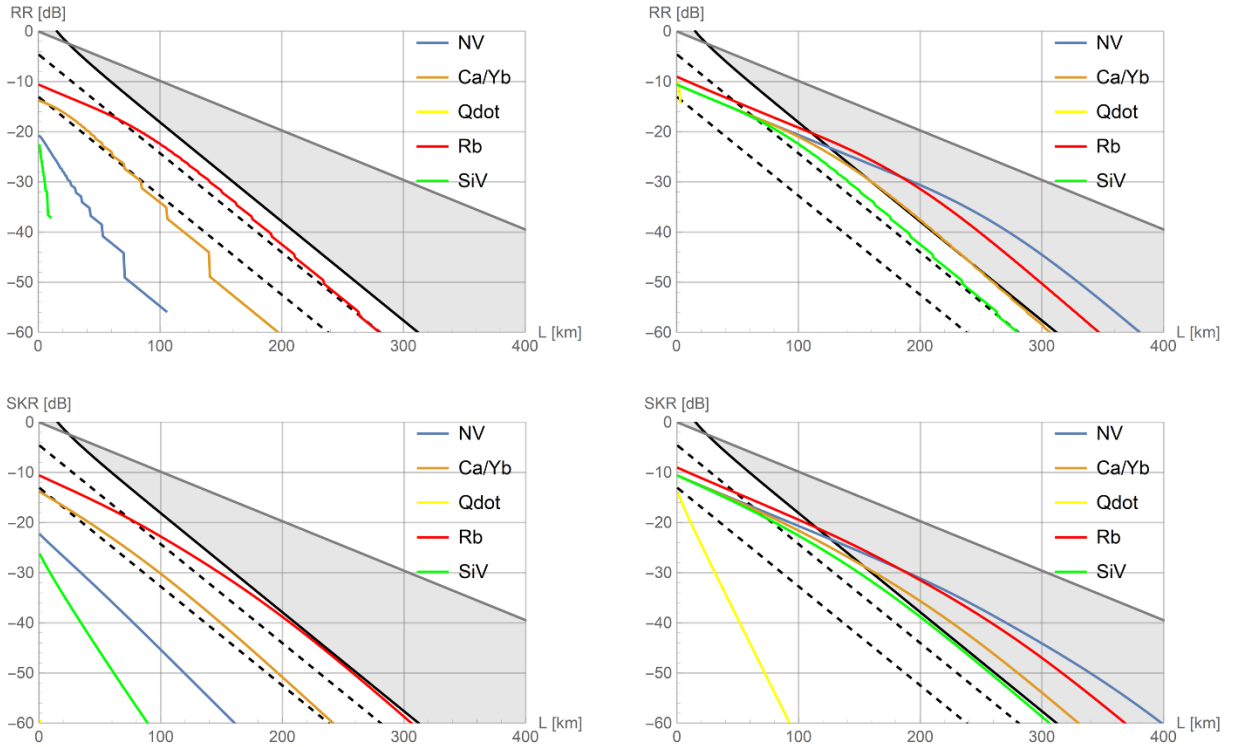


Fig. S3: Secret Key Rates (*SKR*) and High-Fidelity Raw Rates (*RR*) for the NSP-QR cell as shown in Fig.5, but including a factor $\frac{1}{2}$ in the link coupling efficiencies to take into account the effect of wavelength conversions. Bottom plots show *SKR* in dB as a function of the total distance *L* in km for experimental parameters as currently available (left) and as potentially available in the future (right). Top plots show *RR* in schemes where the entangled states effectively created over the total distance *L* have a fidelity of at least 0.95 (left: current right: future).

Similarly, we show the rates for the NRP protocol including the conversion efficiency. Figure S4 corresponds to the rates of the NRP-QR cell as shown in Fig. 7 assuming a deterministic

and fast memory write-in, but now also including the extra factor $\frac{1}{2}$ in P_{link} . The effect of this factor on the rates appears relatively small. Figure S5 is the counterpart of Fig. S2 (NRP-QR cell with a teleportation-based, non-deterministic and slow write-in), with the only difference now being the factor of $\frac{1}{2}$ in P_{link} . In this case, the effect appears stronger. For the future parameters, it can be most easily seen that the rates are basically downshifted, while the repeater regime can still be entered over the distance considered.

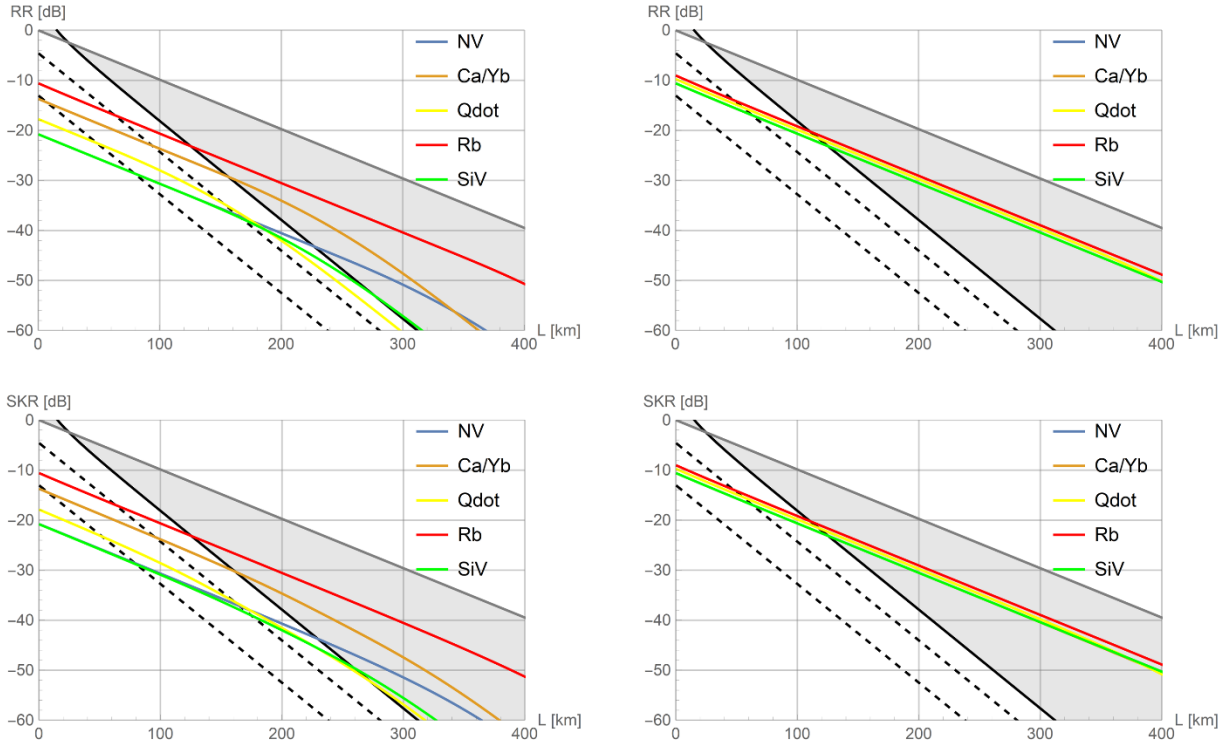


Fig. S4: Secret Key Rates (*SKR*) and High-Fidelity Raw Rates (*RR*) for the NRP-QR cell as shown in Fig.7, but including a factor $\frac{1}{2}$ in the link coupling efficiencies to take into account the effect of wavelength conversions. Bottom plots show *SKR* in dB as a function of the total distance *L* in km for experimental parameters as currently available (left) and as potentially available in the future (right). Top plots show *RR* in schemes where the entangled states effectively created over the total distance *L* have a fidelity of at least 0.95 (left: current right: future).

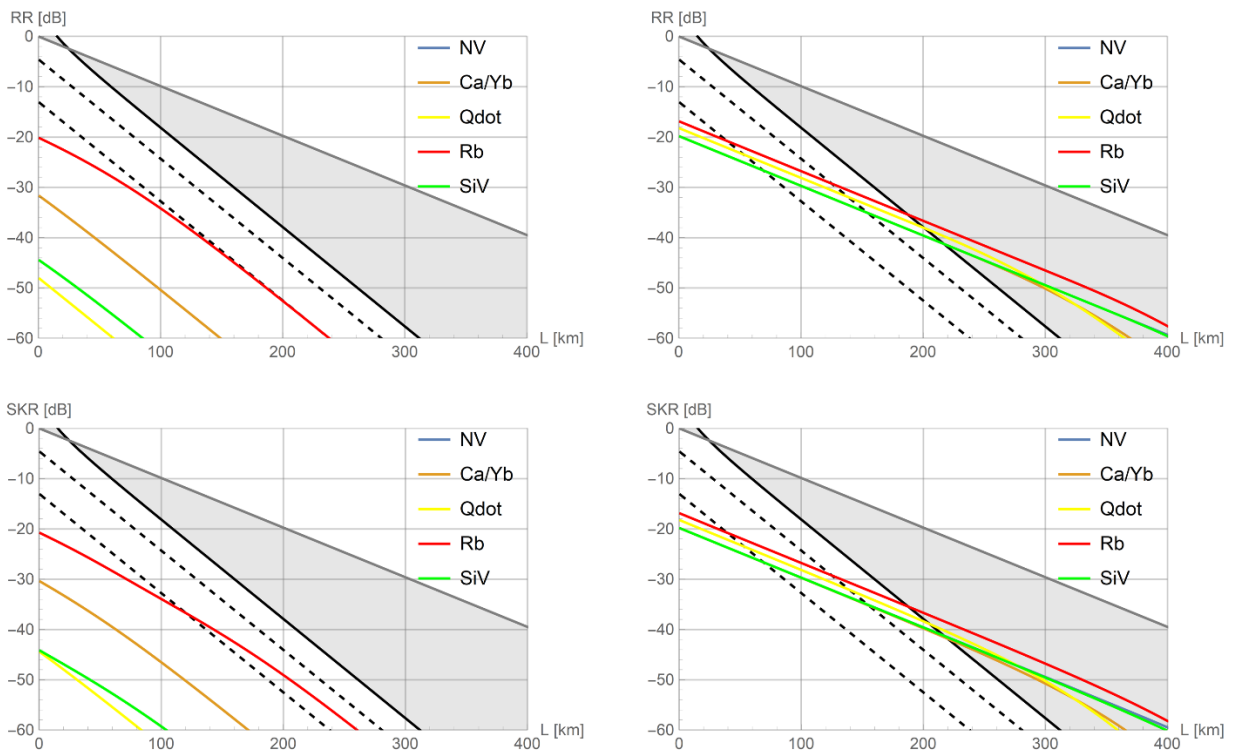


Fig. S5: Secret Key Rates (*SKR*) and High-Fidelity Raw Rates (*RR*) for the NRP-QR cell as shown in Fig.S2, but including a factor $\frac{1}{2}$ in the link coupling efficiencies to take into account the effect of wavelength conversions. Bottom plots show *SKR* in dB as a function of the total distance *L* in km for experimental parameters as currently available (left) and as potentially available in the future (right). Top plots show *RR* in schemes where the entangled states effectively created over the total distance *L* have a fidelity of at least 0.95 (left: current right: future).

Paper III

Quantum error correction with higher Gottesman-Kitaev-Preskill codes: Minimal measurements and linear optics

Frank Schmidt and Peter van Loock

Phys. Rev. A **105**, 042427 (2022)

Editors' Suggestion

Quantum error correction with higher Gottesman-Kitaev-Preskill codes: Minimal measurements and linear optics

Frank Schmidt* and Peter van Loock†

Institute of Physics, Johannes Gutenberg-Universität Mainz, Staudingerweg 7, 55128 Mainz, Germany



(Received 12 November 2021; accepted 24 March 2022; published 20 April 2022)

We propose two schemes to obtain Gottesman-Kitaev-Preskill (GKP) error syndromes by means of linear-optical operations, homodyne measurements, and GKP ancillas. This includes showing that for a concatenation of GKP codes with an $[n, k, d]$ stabilizer code only $2n$ measurements are needed in order to obtain the complete syndrome information, significantly reducing the number of measurements in comparison to the canonical concatenated measurement scheme and at the same time generalizing linear-optics-based syndrome detections to higher GKP codes. Furthermore, we analyze the possibility of building the required ancilla states from single-mode states and linear optics. We find that for simple GKP codes this is possible, whereas for concatenations with qubit Calderbank-Shor-Steane codes of distance $d \geq 3$ it is not. We also consider the canonical concatenated syndrome measurements and propose methods for avoiding crosstalk between ancillas. In addition, we make use of the observation that the concatenation of a GKP code with a stabilizer code forms a lattice in order to see the analog information decoding of such codes from a different perspective allowing for semianalytic calculations of the logical error rates.

DOI: [10.1103/PhysRevA.105.042427](https://doi.org/10.1103/PhysRevA.105.042427)

I. INTRODUCTION

In the last few years large interest arose in bosonic quantum error correcting schemes, which encode a finite-dimensional system within a harmonic oscillator, such as cat and Gottesman-Kitaev-Preskill (GKP) codes [1,2]. This growing interest for such codes came from experiments demonstrating first implementations of these codes [3–5] and partly already outperforming simple encodings, although the codes were proposed already two decades ago. As these codes even allow for error correction with a single oscillator mode they are very hardware efficient. However, the GKP codes are only able to correct small displacement errors and therefore concatenations with stabilizer codes [6–10] are often considered in order to correct larger shifts. The analog syndrome information of individual GKP codes has gained a lot of attention as it helps to further boost the error-correction capability of the code concatenation, because even for a code of distance $d = 3$ it allows for correcting some two-qubit errors.

GKP codes are now also considered for quantum communication, since they can be encoded in an electromagnetic light field, which is the ideal long-distance quantum information carrier, and so have been shown to almost achieve the capacity of the loss channel in the low-loss regime [11]. Furthermore, for quantum communication one only needs Clifford gates and Pauli measurements which can be implemented in the GKP encoding with Gaussian optics and homodyne measurements. Recently concatenations with qubit stabilizer codes have been

considered for communication [12], making also use of the analog information in the GKP error syndrome [13].

In this paper we primarily describe the GKP codes by making use of their stabilizer formulation, because this allows us to simply generalize results from the usual square-lattice GKP code to more general lattices and it is also useful for the concatenation with high-level codes, which we assume to be qubit (qudit) stabilizer codes. We show that it is not necessary to first perform the GKP syndrome measurements and later those of the stabilizer code independently as it is usually done in the literature. Instead it is possible to find a joint minimal set of stabilizer generators for the concatenation of both codes which can then be measured, reducing the overhead of necessary ancilla states. Related to this result, we propose two explicit methods for obtaining this syndrome information without inline squeezing operations and based on passive linear optics. In particular, our linear-optics schemes for the error-correction syndrome detections include those of the higher GKP codes, thus extending existing linear-optics schemes for sole GKP qubit syndrome detection. These linear-optical syndrome measurements might be useful in the context of generalized approaches to fault-tolerant photonic quantum computing with GKP codes [14]. We show that the error-correcting properties of a code remain invariant under (passive) linear-optical transformations for isotropic displacement noise. Additionally, we also discuss the possibility of generating the ancilla states necessary for error correction with linear optics and show that it is impossible to generate codewords of such a high-level GKP qubit code with code distance $d \geq 3$ by employing rectangular single-mode grid states and linear optics. These results are not in contradiction and complementary to the results from Ref. [15], which considers additional GKP states which are then measured, while

*fschmi@students.uni-mainz.de

†loock@uni-mainz.de

we do not assume such additional GKP states. We also discuss some other results concerning the possibility of building GKP-type states with passive linear optics, namely, for GKP Bell states composed of two general (multimode) GKP codes or codewords assuming that two copies of suitable codes or codewords are already experimentally accessible.

Moreover, we also discuss the possibility of performing syndrome measurements of the higher-level code following the canonical measurement approach in such a way that there is no error propagation from one ancilla to another one. Finally, we demonstrate how one can systematically calculate the performance of the concatenation of GKP qudits with a high-level code when making use of the analog syndrome information in a semianalytic way.

The paper is structured as follows. In Sec. II we review qudits and GKP codes, and in Sec. III we give a brief review about different schemes for obtaining the GKP syndrome information. In Sec. IV we discuss the minimal number of measurements for higher GKP codes and propose a linear-optical realization based on error correction by teleportation. In Sec. V we propose another linear-optical realization of the minimal set of measurements and in Sec. VI we discuss methods for avoiding error propagation between ancillas when performing stabilizer measurements. Finally, we compare the different methods of obtaining the syndrome information in Sec. VII and conclude in Sec. VIII.

II. BACKGROUND

A. Qudits

We refer to a quantum system represented by a finite-dimensional Hilbert space of dimension D as a qudit of dimension D . Furthermore, we label states in the Z basis by elements of \mathbb{Z}_D . For these qudits we can generalize the Pauli operators as

$$X_D = \sum_{j=0}^{D-1} |j+1 \pmod D\rangle\langle j|, \quad (1)$$

$$Z_D = \sum_{j=0}^{D-1} \exp\left(i\frac{2\pi}{D}j\right) |j\rangle\langle j|, \quad (2)$$

$$Z_D X_D = \exp\left(i\frac{2\pi}{D}\right) X_D Z_D. \quad (3)$$

For qudits we can then give D^2 basis elements for all operators, taking the form $P^{rs} := X_D^r Z_D^s$ with $r, s \in \mathbb{Z}_D$. For brevity we drop the index D in Pauli operators. When neglecting global phase information, it is possible to map Pauli operators acting on n qudits onto \mathbb{Z}_D^{2n} via

$$\phi(X_1^{r_1} Z_1^{s_1} \cdots X_n^{r_n} Z_n^{s_n}) = (r_1, \dots, r_n | s_1, \dots, s_n). \quad (4)$$

Using Eq. (3) we see that

$$P^{rs} P^{r's'} = \exp\left(-i\frac{2\pi}{D}\omega((r, s), (r', s'))\right) P^{s',r} P^{s,r}, \quad (5)$$

where $\omega(\cdot, \cdot)$ is the canonical symplectic form given by $\omega((r, s), (r', s')) = r \cdot s' - s \cdot r'$. Thus, two Pauli operators commute if and only if the symplectic form of the two

symplectic representations of the Pauli operators vanishes modulo D .

Stabilizer codes (see Refs. [16,17] for more details) are defined by an Abelian subgroup S of the Pauli group which acts as the identity within the code space. Given such a group it is possible to find a small set generating the whole group. For the special case of prime D there is the nice relation that the number of stabilizer generators is equal to $n - k$, where n is the number of physical qudits and k is the number of encoded qudits. However, for nonprime D we can have up to $2n$ stabilizer generators [17]. The code distance of a stabilizer code is given by the lowest-weight element in $\mathcal{N}(S)/S$, where $\mathcal{N}(S)$ denotes the normalizer of S . It is quite convenient to give a stabilizer code by an $l \times 2n$ matrix given by the symplectic representation of the l stabilizer generators. For Calderbank-Shor-Steane (CSS) codes this matrix can be brought to the following form:

$$H = \begin{pmatrix} H_X & 0 \\ 0 & H_Z \end{pmatrix}. \quad (6)$$

Thus, bit and phase flips can be corrected independently.

Employing high-dimensional qudits instead of qubits might be of practical relevance as qudits can tolerate more (hardware-agnostic) depolarizing noise before entanglement is lost or one is unable to perform quantum key distribution [18–21]. Additionally, in the context of quantum error correction there is the quantum singleton bound showing that there is a trade-off between the number of logical qudits and the code distance for a given number of physical qudits. For qubits there only exists a five-qubit code with code distance 3 satisfying the bound while for higher-dimensional qudits there also exist codes for arbitrary large code distance d . An example for such codes is the family of quantum polynomial codes defined for prime qudit dimension D [22].

B. GKP codes

GKP codes [2] encode n qudits within the phase space of a harmonic oscillator with n modes. These codes can be understood as stabilizer codes, where the code space is stabilized by a discrete, Abelian subgroup of the continuous Weyl-Heisenberg group [23].

The elements of the continuous Weyl-Heisenberg group for n modes can be given as $U(\theta, \alpha, \beta) = \exp(i\theta) \exp(i\sqrt{2\pi} \sum_{j=1}^n (\alpha_j \hat{q}_j + \beta_j \hat{p}_j))$ with real numbers $\alpha, \beta \in \mathbb{R}^n$ and where \hat{q} and \hat{p} denote the position and momentum operators fulfilling $[\hat{q}, \hat{p}] = i\hbar$; in this article we set $\hbar = 1$. Thus this group is isomorphic to $U(1) \times \mathbb{R}^{2n}$. The commutation relation of two group elements is given by

$$\begin{aligned} U(\theta_1, \alpha_1, \beta_1) U(\theta_2, \alpha_2, \beta_2) \\ = U(\theta_2, \alpha_2, \beta_2) U(\theta_1, \alpha_1, \beta_1) \\ \times \exp(-i2\pi\omega((\alpha_1, \beta_1), (\alpha_2, \beta_2))), \end{aligned} \quad (7)$$

where $\omega(\cdot, \cdot)$ is the canonical symplectic product already introduced in the previous qudit section extended to real numbers and can be obtained by the Baker-Campbell-Hausdorff formula. In order to obtain commuting operators, we need to find elements in \mathbb{R}^{2n} whose symplectic product gives pairwise an integer. We will refer to the parametrization via \mathbb{R}^{2n} as

phase-space or symplectic representation. In order to encode a finite-dimensional system in the $2n$ -dimensional code space, we need $2n$ independent stabilizer generators which we use as a definition for the stabilizer group. If we have found those elements in \mathbb{R}^{2n} , then we know that also all elements in the lattice \mathcal{L} generated by the $2n$ independent vectors in \mathbb{R}^{2n} also correspond to commuting operators due to the linearity of the symplectic product [24]. The set of operators commuting with all stabilizers corresponds to the dual lattice \mathcal{L}^\perp (with respect to the symplectic form). Thus $\mathcal{L}^\perp/\mathcal{L}$ give logical operators and therefore we can define the code distance (with respect to the Euclidean norm), analogously to qudit stabilizer codes, as the minimum weight of nontrivial elements in $\mathcal{L}^\perp/\mathcal{L}$ giving the smallest error commuting with all stabilizers.

As an example let us consider the well-known square-lattice code. The stabilizer generators are given by

$$\exp(-i\sqrt{2\pi D}\hat{p}), \quad \exp(i\sqrt{2\pi D}\hat{q}), \quad (8)$$

with logical operators

$$\bar{X} = \exp\left(-i\sqrt{\frac{2\pi}{D}}\hat{p}\right), \quad \bar{Z} = \exp\left(i\sqrt{\frac{2\pi}{D}}\hat{q}\right). \quad (9)$$

Thus all displacement errors smaller than $\sqrt{\frac{\pi}{2D}}$ can be corrected [25]. However, notice that the logical states $|j\rangle$ in the Z basis are given as

$$|j\rangle = \sum_{k \in \mathbb{Z}} \left| \hat{q} = \sqrt{2\pi D}\left(k + \frac{j}{D}\right) \right\rangle. \quad (10)$$

The codewords consist of an infinite series of delta peaks in position or momentum representation such that the states are unphysical, because they are not normalizable and have infinite energy. Thus one needs to consider approximate GKP states, where we replace the delta peaks by narrow Gaussian peaks and we also consider an overall Gaussian envelope in order to make the state normalizable. Such a state can be obtained by applying coherent, Gaussian displacements on an ideal codeword. There are multiple approximations known in the literature which have been shown to be equivalent [26]. In this article, we replace the coherent Gaussian displacements by incoherent ones, simplifying the calculations. This can be understood as the result of an unphysical limit of a twirling operation [27,28] acting on a state with coherent displacements similar to the qubit case where it is also possible to reduce arbitrary noise to Pauli channels by applying twirling operations. Thus the resulting state is noisier such that we obtain a conservative estimate of the error-correction properties.

One main advantage of this GKP encoding is that all Clifford operations acting on the GKP code can be implemented by Gaussian operations. Additionally, Pauli measurements can be implemented by using homodyne measurements. Furthermore, GKP syndrome measurements, which can be implemented by GKP states and Gaussian operations, applied to the vacuum state are known to produce states that can be distilled to magic states [29]. Thus, the generation of the GKP states is the only needed non-Gaussian element for a universal set of quantum gates. An all-Gaussian system can be simulated efficiently [30].

Although only codewords of qubit GKP codes have been explicitly demonstrated in experiments with ions [4] and superconducting qubits [5], it is not much more difficult at all to obtain codewords of GKP qudits. For example, in the experiment in Ref. [4] one only has to modify the parameter α in the conditional displacement in order to generate qudits instead of qubits on a square lattice. Furthermore, the X and Z eigenstates of the qubit square-lattice GKP code prepared in the experiment can already be understood as a qudit GKP codeword based on an appropriately chosen rectangular lattice. Thus, for example the codeword $|0\rangle$ is given by the same physical state for both codes and the difference of the two codes only lies in the different definitions of Pauli and recovery operations.

III. REVIEW OF SYNDROME MEASUREMENTS

We consider a concatenation of GKP qudits with qudit stabilizer codes. We refer to the syndrome measurement where we obtain information about the small shifts needed for correcting the GKP qudit as GKP syndrome, while we will refer to the syndrome obtained by measuring the stabilizer generators as stabilizer syndrome.

A. Stabilizer syndrome

The syndrome of a stabilizer code which encodes k logical qudits into n physical qudits is formally obtained by measuring all $n - k$ stabilizer generators (for D prime, otherwise up to $2n$). When coupling ancilla qubits with data qubits for obtaining the code syndrome it is highly desirable that every ancilla qubit only couples with a single data qubit in order to prevent a single error of the ancilla propagating onto multiple data qubits. One such scheme is the Steane error correction [31] where the n data qubits are coupled with $2n$ ancilla qubits by transversal controlled-NOT (CNOT) gates. The CNOTs act as the identity on the logical level for this ancilla such that we learn the error syndrome but gain no information about the encoded quantum information. In the special case of a CSS code the $2n$ qudit ancilla states can be decomposed into the two logical codewords $|\bar{\mp}\rangle$ ($|\bar{0}\rangle$) being target (control) of the transversal CNOTs and measured in the Z (X) basis.

A different approach is the so-called Knill scheme [32], where the ancilla is given by a logical Bell state and Bell measurements are applied to the data qubits and one-half of the logical Bell state. In the original paper the scheme was only proven for qubits, but in Appendix C we show that it also works for $D > 2$ CSS codes.

B. GKP syndrome

Let us begin to review the different known methods for obtaining the GKP syndrome. The schemes can be put into two categories. On the one hand, we have sequential measurements as the one proposed in the original GKP paper [2], which is inspired by the Steane error-correction scheme for CSS qubit codes [31], and further improved schemes reducing the experimental resources [33,34]. On the other hand, we have a teleportation-based scheme [29,35] inspired by Knill's error correction by teleportation [32] which only started to gain more interest recently [36].

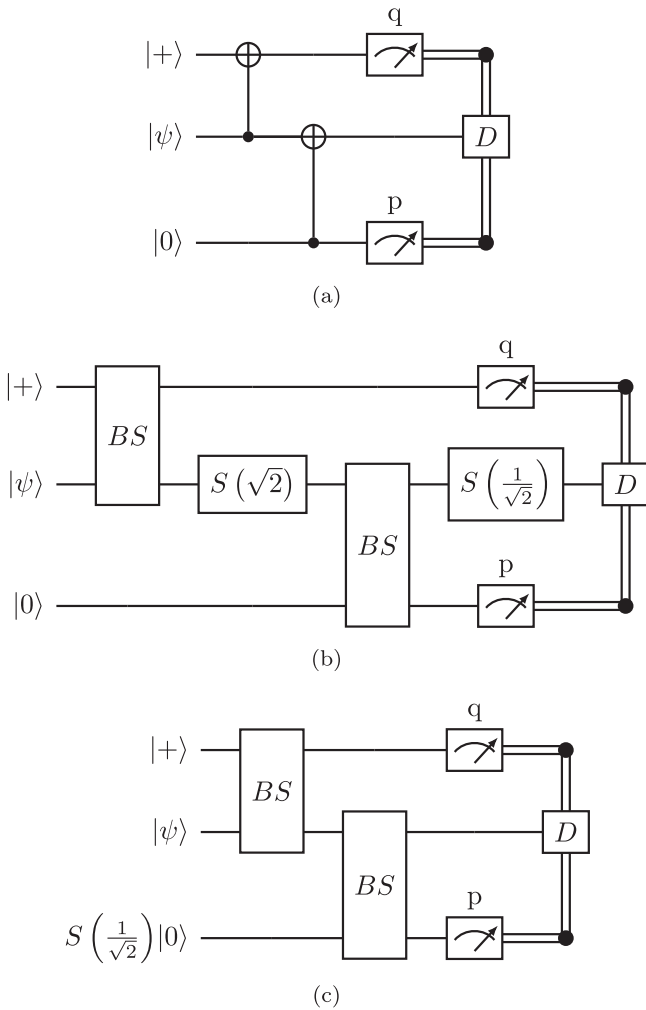


FIG. 1. Different methods to obtain the syndrome information of a square GKP code. (a) Steane-inspired approach introduced in Ref. [2]. The CNOT gates are implemented by CSUM gates where each can be decomposed into two beam splitters and two squeezers. (b) Knill-Glancy scheme [33] where each CSUM gate is replaced by a single beam splitter and squeezer. (c) Improved Knill-Glancy scheme where we only need beam splitters and an offline-squeezed state.

1. Steane scheme

Now let us further discuss the sequential scheme. For square GKP qubits the Steane error-correction scheme [Fig. 1(a)] was proposed for performing the syndrome measurement. First we have one code block containing the data and two ancilla code blocks being in the $|+\rangle$ and $|0\rangle$ state. In order to obtain the syndrome information of the modular position a CNOT is applied to the data code (control) and the first ancilla code (target) and the mode of the first ancilla code is measured in the position quadrature. Similarly, we obtain the modular momentum stabilizers by applying a CNOT to the second ancilla code (control) and data code (target) and the mode of the ancilla code is measured in the momentum quadrature. In the code space this acts as the identity and therefore by obtaining the error syndrome we do not obtain information about the logical state. For the square GKP code CNOT gates are implemented by controlled-SUM (CSUM)

gates $[\exp(-i\hat{q}_1\hat{p}_2)]$ which can be decomposed into two beam splitters and two squeezing operations. From an experimental point of view arbitrary passive linear-optical transformations, decomposable into beam splitters and phase shifters, are easy to implement while squeezing operations are not that simple to implement (highest squeezed vacuum state 15 dB [37]). Furthermore, it is hard to implement an operation which acts as the squeezing operation on arbitrary input states. Thus these squeezing operations are typically implemented via gate teleportation with an, ideally infinitely, squeezed ancilla state [38] and have already been used for implementing a CSUM gate experimentally [39]. However, infinitely squeezed vacuum states are unphysical and can only be approximated by highly squeezed vacuum states resulting in an approximation error. Thus, it is beneficial to avoid inline squeezing and use offline squeezing whenever possible.

2. Knill-Glancy scheme

The Knill-Glancy scheme [33] [Fig. 1(b)] was proposed for a square-lattice (although it is easy to see that it also works for rectangular lattices) GKP code and it can be understood as a variation of Steane error correction where the CSUM gate is replaced by a 50:50 beam splitter followed by a squeezing operation with a squeezing factor $\sqrt{2}$. Independently from our work, it was recently shown in Ref. [34] that the Knill-Glancy scheme is equivalent to a scheme where no inline squeezing is used [Fig. 1(c)], but one of the two ancilla GKP states is squeezed by a factor of $\sqrt{2}$. In Sec. V we will show that these improvements also work for arbitrary GKP codes. Furthermore, this improves the noise introduced by finite squeezing and there also exists a similar scheme which also gives the syndrome information of a high-level CSS code.

IV. IMPROVEMENT OF SYNDROME MEASUREMENTS

In many works [6–10] concatenations of GKP codes with higher-level qubit codes are considered and the syndrome measurements of the GKP code and the high-level code are done independently. This means one first obtains the GKP syndrome information for correcting the small shifts and then one obtains the syndrome information of the higher-level code for correcting the larger shifts. Each of these measurements typically makes use of a GKP-like ancilla state which is costly. Therefore, we discuss alternative measurement schemes which only make use of a minimal number of measurements.

Let us begin with the qubit case where we concatenate an n -mode GKP code with an arbitrary stabilizer code. We show that by using $2n$ measurements we not only obtain the GKP syndrome information of the n -mode GKP code, but also the additional syndrome information for decoding the higher-level code. This can be seen rather easily by describing the whole concatenated code by a set of independent (Weyl-Heisenberg) stabilizer generators. The stabilizer of the GKP code can be obtained by applying logical Pauli operators twice. In a naive approach one would construct a set of stabilizer generators by first considering the stabilizers of the GKP code and then adding the qubit stabilizers. However, these stabilizer generators are not independent, because we can

apply the qubitlike stabilizers twice in order to obtain stabilizer generators of the GKP code. Thus we can remove these, such that we still have $2n$ independent stabilizer generators. When encoding quantum information into a code we have a product state of inputs in Pauli eigenstates. This state can therefore be described by $2n$ independent stabilizer generators. In order to do the encoding we perform a sequence of Clifford (Gaussian) operations, changing the actual stabilizer generators but their number remains invariant. Thus, we only need to measure the $2n$ independent stabilizer generators in order to obtain full syndrome information. Furthermore, we can generalize this result to arbitrary qudit dimensions D by using a different proof technique based on lattice theory instead due to technical difficulties. The proof is given in Appendix A. This result is quite remarkable, because one needs no additional measurements in order to obtain the additional syndrome information of the higher-level code, which consists of up to $2n$ (Pauli) stabilizer generators for the case of nonprime D . While such minimal measurements have been proposed in an *ad hoc* way for some codes [6,40], in the next sections we discuss two schemes which allow us to obtain the full syndrome information in a systematic way for general GKP codes concatenated with stabilizer codes employing only GKP-like states, linear optics, and homodyne measurements.

A. Teleportation-based error correction

1. GKP syndrome

Here we will discuss how to obtain the syndrome information of a general GKP code which will be a building block for the scheme that additionally also gives the syndrome information of the high-level code. Let us first discuss the special case of a GKP qudit code using a square lattice and show that it is possible to obtain the syndrome information without needing inline squeezing operations. Recall that the (Weyl-Heisenberg) stabilizers of such a code encoding a qudit (with dimension D) are given by

$$\exp(-i\hat{p}\sqrt{2\pi D}) \text{ and } \exp(i\hat{q}\sqrt{2\pi D}), \quad (11)$$

where \hat{q} and \hat{p} are quadrature operators of the harmonic oscillator. The logical Pauli operators of the GKP code are given by

$$\bar{X} = \exp\left(-i\hat{p}\sqrt{\frac{2\pi}{D}}\right) \text{ and } \bar{Z} = \exp\left(i\hat{q}\sqrt{\frac{2\pi}{D}}\right). \quad (12)$$

Therefore, the logical information encoded in $|\psi\rangle^{GKP}$ is encoded in modular quadrature operators. Let us consider a qudit Bell state

$$|\Phi_{00}\rangle_{2,3} := \frac{1}{\sqrt{D}} \sum_{k=0}^{D-1} |k, k\rangle_{2,3}, \quad (13)$$

which can also be described by the two (qudit) stabilizers X_2X_3 and $Z_2Z_3^{-1}$ [41]. We can construct all other Bell states via

$$|\Phi_{rs}\rangle_{2,3} := \bar{X}_2^r \bar{Z}_3^s |\Phi_{00}\rangle_{2,3}, \quad (14)$$

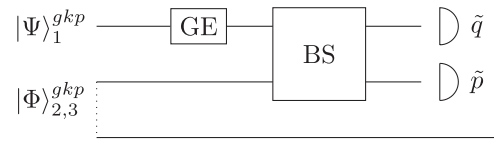


FIG. 2. A logical qudit is encoded in mode 1 and is affected by Gaussian errors (GE). Then it is coupled with one half of a logical Bell state pair via a balanced beam splitter (BS). The position and momentum quadratures of the beam splitter output are measured. We can use these measurement results for error correction of the GKP code and for correcting the higher-level code. The teleportation protocol actually also involves applying conditional displacements. However, when considering multiple rounds of this teleportation protocol we actually do not need to apply the displacement in every step, but we can keep track of the displacements and apply only one displacement in the end, because they only shift the measurement results of the next error-correction cycle. This is similar to the Pauli frame for qubits. The dotted line denotes that modes 2 and 3 share an entangled state.

where $r, s \in \mathbb{Z}_D$. If we have such a qudit Bell state encoded in two GKP qudits, the Bell state stabilizer conditions are equivalent to

$$\left(\hat{p}_2 + \hat{p}_3 - s\sqrt{\frac{2\pi}{D}} \pmod{\sqrt{2\pi D}} \right) |\Phi_{rs}\rangle_{2,3}^{GKP} = 0, \quad (15)$$

$$\left(\hat{q}_2 - \hat{q}_3 - r\sqrt{\frac{2\pi}{D}} \pmod{\sqrt{2\pi D}} \right) |\Phi_{rs}\rangle_{2,3}^{GKP} = 0. \quad (16)$$

Notice that these two stabilizers alone do not define a GKP Bell state uniquely, because for example an infinitely squeezed two-mode squeezed state also satisfies these conditions.

We consider a beam splitter with the transformations

$$\hat{q} = \frac{1}{\sqrt{2}}(\hat{q}_1 - \hat{q}_2), \quad (17)$$

$$\hat{p} = \frac{1}{\sqrt{2}}(\hat{p}_1 + \hat{p}_2). \quad (18)$$

Let us first assume an ideal ancilla state $|\Phi_{rs}\rangle_{2,3}^{GKP}$ and also an arbitrary ideal data state $|\psi\rangle_1^{GKP}$. Now we first show that we can use the circuit illustrated in Fig. 2 for teleporting the information encoded in the GKP qudit:

$$\begin{aligned} & \hat{q}_1 \pmod{\sqrt{2\pi D}} |\psi\rangle_1^{GKP} |\Phi_{rs}\rangle_{2,3}^{GKP} \\ &= \hat{q}_1 - \hat{q}_3 + \hat{q}_3 \pmod{\sqrt{2\pi D}} |\psi\rangle_1^{GKP} |\Phi_{rs}\rangle_{2,3}^{GKP} \\ &= \hat{q}_1 - \hat{q}_2 + r\sqrt{\frac{2\pi}{D}} + \hat{q}_3 \pmod{\sqrt{2\pi D}} |\psi\rangle_1^{GKP} |\Phi_{rs}\rangle_{2,3}^{GKP} \\ &= \hat{q}_3 + \sqrt{2}\hat{q} + r\sqrt{\frac{2\pi}{D}} \pmod{\sqrt{2\pi D}} |\psi\rangle_1^{GKP} |\Phi_{rs}\rangle_{2,3}^{GKP}. \end{aligned} \quad (19)$$

Here we only used the stabilizer property of the GKP Bell state. If we measure \hat{q} and shift \hat{q}_3 by $\sqrt{2}\hat{q} + r\sqrt{\frac{2\pi}{D}}$, we then have successfully teleported the information encoded in the modular position quadrature. Similarly we can teleport the information encoded in the modular momentum quadrature

by measuring \hat{p} and shifting \hat{p}_3 accordingly:

$$\begin{aligned}
& \hat{p}_1 \bmod \sqrt{2\pi D} |\psi\rangle_1^{GKP} |\Phi_{rs}\rangle_{2,3}^{GKP} \\
&= \hat{p}_1 - \hat{p}_3 + \hat{p}_3 \bmod \sqrt{2\pi D} |\psi\rangle_1^{GKP} |\Phi_{rs}\rangle_{2,3}^{GKP} \\
&= \hat{p}_1 + \hat{p}_2 + \hat{p}_3 - s\sqrt{\frac{2\pi}{D}} \bmod \sqrt{2\pi D} |\psi\rangle_1^{GKP} |\Phi_{rs}\rangle_{2,3}^{GKP} \\
&= \hat{p}_3 + \sqrt{2}\hat{p} - s\sqrt{\frac{2\pi}{D}} \bmod \sqrt{2\pi D} |\psi\rangle_1^{GKP} |\Phi_{rs}\rangle_{2,3}^{GKP}. \tag{20}
\end{aligned}$$

The demonstrated teleportation is exactly the well-known qudit teleportation applied to GKP qudits, if we assume that the GKP states are in their code space such that they are well-defined qudits. We already saw that we can use the measurement result from the two homodyne detections for shifting the GKP states back into the code space. Thus we can understand the protocol in the following way: First we use the homodyne measurement for correcting small shifts to the nearest codeword in mode 1 and then we perform a common qudit teleportation protocol, teleporting the encoded information into mode 3. Therefore, the only actually interesting observation lies in the fact that the homodyne measurements give us information about the measured GKP Bell state and the GKP syndrome information at the same time. Also notice that the displacement for correcting the small shift together with the displacement from the teleportation protocol reduces to a single GKP Pauli operation.

2. Incoherent noise

Up to now, we considered only ideal GKP states which are clearly unphysical since they are not normalizable and have infinite energy. Realizable approximate GKP states are for example given by a coherent superposition of Gaussian displacements acting on an ideal GKP state. For simplicity we will consider an error model of finite squeezing where we replace the coherent displacements by stochastic ones.

First we will show that we can correct Gaussian shift errors acting on the data mode, while assuming noiseless ancilla states. Later we show that we can also consider noisy ancilla states (in our error model) and this is equivalent to considering noiseless ancilla states, but with more noise on the data mode.

In order to perform error correction of the GKP code we actually have to measure $\hat{q} \bmod \sqrt{\frac{2\pi}{D}}$ and $\hat{p} \bmod \sqrt{\frac{2\pi}{D}}$ which give the result “0” for square-lattice GKP codewords. For correcting shift errors we simply apply the smallest shift needed to obtain a codeword again:

$$\begin{aligned}
& \sqrt{2}\hat{q} \bmod \sqrt{\frac{2\pi}{D}} |\psi\rangle_1^{GKP} |\Phi_{rs}\rangle_{2,3}^{GKP} \\
&= \hat{q}_1 - \hat{q}_2 \bmod \sqrt{\frac{2\pi}{D}} |\psi\rangle_1^{GKP} |\Phi_{rs}\rangle_{2,3}^{GKP} \\
&= \hat{q}_1 \bmod \sqrt{\frac{2\pi}{D}} |\psi\rangle_1^{GKP} |\Phi_{rs}\rangle_{2,3}^{GKP}. \tag{21}
\end{aligned}$$

For the last step we used our assumption that mode 2 is part of a perfect GKP state and thus $\hat{q}_2 \bmod \sqrt{\frac{2\pi}{D}} = 0$. Hence,

we know the syndrome information and can apply the corresponding correction shift onto mode 3. When we consider the shift from the teleportation and the correction shift together, we obtain simply a Pauli operator. The same reasoning holds for the modular momentum quadrature.

Let us now consider also noisy ancilla states (assuming a random shift model). Let v_i denote the random variable describing the momentum shift acting on mode i and u_i denote the corresponding random variable for the position shifts. As it can be seen in Eq. (18) a shift of \hat{p}_1 by v_1 and a shift of \hat{p}_2 by v_2 have the same outcome of the measurement as a shift of \hat{p}_1 by $v_1 + v_2$. Similarly one can show by using Eq. (17) that the position shifts acting on modes 1 and 2 have the same effect on the measurement outcome as a shift of \hat{q}_1 by $u_1 - u_2$. We interpret the shift errors on mode 2 as additional shifts on mode 1 and the shifts of mode 3 are the finite squeezing shifts of the data GKP qudit in the next error-correction step. Also notice that there is no need (in the random shift model) to perform the displacement operations after each correction step, but one can keep track of them similar to a Pauli frame. We did not assume a particular distribution of the random variables describing the shift errors and their possible correlations. We will do this later when we discuss different approaches of generating GKP Bell states.

3. General GKP codes

Let us now generalize this scheme from a GKP code based on a square lattice to general GKP codes which may even be defined on n modes. The stabilizer generators span a lattice in the $2n$ -dimensional phase space. The corresponding logical Pauli operators are of the form $\bar{X}_j = \exp(-ia_j\hat{P}_j)$ and $\bar{Z}_j = \exp(ib_j\hat{Q}_j)$ where \hat{Q} and \hat{P} are linear combinations of quadrature operators, fulfilling the canonical commutation relation $[\hat{q}_k, \hat{p}_l] = i\delta_{kl}$, and some $a_j, b_j \in \mathbb{R}$. Since we are considering quantum teleportation, our resource states must be Bell states encoded in the same code as the input modes. For measuring the Bell states we only need to measure $\bar{X}_{j,1}\bar{X}_{j,2} = \exp[-ia_j(\hat{P}_{j,1} + \hat{P}_{j,2})]$ and $\bar{Z}_{j,1}\bar{Z}_{j,2}^{-1} = \exp[-ib_j(\hat{Q}_{j,1} - \hat{Q}_{j,2})]$. However, the observables $\hat{P}_{j,1} + \hat{P}_{j,2}$ and $\hat{Q}_{j,1} - \hat{Q}_{j,2}$ commute such that we can measure them simultaneously instead of only measuring the quantities modulo some constant. We have shown that it is possible to interpret mode 2 as noiseless when considering more noise on mode 1. Measuring the relevant syndrome means measuring $\hat{Q}_{j,1} \bmod \frac{2\pi}{Da_j}$ and $\hat{P}_{j,1} \bmod \frac{2\pi}{Db_j}$. However, we know that the state in mode 2 is part of the logical Bell state and therefore the relevant modulus of mode 2's quadrature operators are zero. Thus, we can obtain the modulo of the quadrature operators of mode 1 by applying the mod function on the measurement outcome of the commuting observables $\hat{Q}_{j,1} - \hat{Q}_{j,2}$ and $\hat{P}_{j,1} + \hat{P}_{j,2}$. Recall that \hat{P} and \hat{Q} are linear combinations of quadrature operators and therefore we can measure them with passive, linear optics and homodyne measurements.

Let us first explain why this is possible in the single-mode case. In order to measure $\hat{Q}_1 - \hat{Q}_2$ and $\hat{P}_1 + \hat{P}_2$ we have to couple modes 1 and 2 at a 50:50 beam splitter and then we need to measure the resulting operators \hat{Q}_2 and \hat{P}_1 which are both linear combinations of position and momentum

operators. Equivalently, it is possible to represent this linear combination in polar coordinates $\alpha\hat{q} + \beta\hat{p} = \gamma[\cos(\theta)\hat{q} + \sin(\theta)\hat{p}]$ with $\alpha, \beta, \gamma, \theta \in \mathbb{R}$. Thus, the measurement of the linear combination can be understood as the measurement of a rotated quadrature which was squeezed in the direction of θ where the squeezing corresponds to the factor γ . However, we can also understand the measurement of the linear combination as a measurement of the rotated quadrature operator where we classically rescale the measurement outcome by a factor γ . In other words we have replaced the squeezing operation by multiplication in a postprocessing step of the measurement data. Let us now discuss the general multi-mode case ($n \geq 1$). We need to measure all \hat{P}_j and \hat{Q}_j ($j \in \{1, \dots, n\}$). Here, we only consider the case of \hat{P}_j , because the other one works analogously. In the symplectic representation \tilde{P}_j of the operators \hat{P}_j , we see that $\text{span}_{\mathbb{R}}(\tilde{P}_1, \dots, \tilde{P}_n)$ generates an n -dimensional linear subspace of the phase space. However, notice that the basis $\{\tilde{P}_1, \dots, \tilde{P}_n\}$ does not necessarily form an orthonormal basis. Let $\{\tilde{\xi}_1, \dots, \tilde{\xi}_n\}$ be an orthonormal basis of the same linear subspace. Then there exists an invertible ($n \times n$) matrix A relating both bases via

$$\tilde{P}_j = \sum_{i=1}^n A_{ji} \tilde{\xi}_i. \quad (22)$$

Thus, we can implement a measurement of $(\hat{p}_1, \dots, \hat{p}_n)$ by measuring $(\tilde{\xi}_1, \dots, \tilde{\xi}_n)$ and applying the matrix A onto the classical measurement data. Since $\{\tilde{\xi}_1, \dots, \tilde{\xi}_n\}$ is an orthonormal basis, we can employ linear-optical transformations, which induce arbitrary orthogonal transformations on this n -dimensional linear subspace (symplectic, orthogonal transformations on the whole $2n$ -dimensional phase space), and quadrature measurements of independent modes in order to measure $\{\tilde{\xi}_1, \dots, \tilde{\xi}_n\}$.

Therefore, for measuring the syndrome of any GKP code we only need offline-squeezing operations and all inline operations are passive, linear optics and homodyne measurements. This result is not obvious, because initially we only knew that it is possible for the square-lattice GKP code. A straightforward way of showing this generalization would be by going from a general lattice to a square one, performing the syndrome measurement, and going back to the general lattice. The transformation between two GKP codes is realized by a Gaussian operation, which in general involves squeezing operations; thus the resulting circuit for performing the syndrome measurement is given by a linear-optical operation conjugated by a Gaussian one. However, after conjugation we do not necessarily obtain a linear-optical operation (for a single-mode counterexample consider, e.g., a $\frac{\pi}{2}$ phase shift conjugated by a squeezing operation).

B. Obtaining the higher-level syndrome

Let us furthermore not only consider GKP qudit codes, but a concatenation with a high-level $[n, k, d]_D$ stabilizer code built with GKP qudits. Here, in order to obtain the syndrome of the high-level code we explicitly perform Knill's error correction by teleportation scheme [32]. The qudit teleportation in the Knill scheme is here given by the GKP teleportation

discussed previously, which is also capable of additionally obtaining the syndrome of the GKP code provided the resource state is a GKP Bell state. A logical Bell state is given by a superposition of GKP Bell states, because the set of Bell states forms an orthonormal basis for two qudits. As it can be seen in Eq. (21), we can obtain the error syndrome of the GKP code for any GKP Bell state and therefore by linearity also when using the logical Bell state. We can then use this syndrome information for mapping mode 1 into the code space (via classical postprocessing) and then we can correct errors of the high-level code simply by applying Knill's error correction by teleportation protocol and treating each of the three modes as a qudit.

As a consequence, this scheme demonstrates that, on the one hand, one does not need to measure the $2n$ stabilizers in order to obtain the syndrome of the individual GKP qudits followed by an additional measurement of the high-level code's stabilizer, but $2n$ measurements suffice and, on the other hand, inline squeezing is neither needed for correcting small shifts on GKP qudits nor for obtaining the high-level error syndrome. In the original paper [32] it was shown that the Knill scheme works for arbitrary qubit codes. In Appendix C we show that it also works for qudit CSS codes with an arbitrary qudit dimension D . Furthermore, for non-CSS codes one can find a similar scheme where we need an ancilla state different from a logical Bell state. This difference comes from the asymmetry in the stabilizers $Z_1 Z_2^{-1}$ and $X_1 X_2$ of a qudit Bell state. X and Z are treated differently in the general qudit case, while in the special case of qubits, X and Z are treated equally, because the Pauli operators are self-inverse.

C. Example: Three-mode code

As an example let us consider the error correction of the concatenation of square GKP qubits with the three-qubit bit-flip code. It was already shown in Ref. [6] that the code's performance can be improved significantly by using the complete (analog) error syndrome of the GKP syndrome measurement in the decoder of the high-level stabilizer code. This means we assign a value of reliability to every single GKP error correction; i.e., the further we are away from a codeword the lower the value of reliability. As it can be seen in Fig. 3 we perform error correction by coupling the (three-mode) input state with one-half of an ancilla state consisting of a Bell state encoded in two three-qubit codes with transversal 50:50 beam splitters. Then we perform homodyne measurements on the first six modes which allow us to calculate the needed correction shifts as the six measurements contain the same information as the measurement of the code's six stabilizer generators (explicit stabilizers are given in Appendix G).

When we consider ideal codes followed by independent and identically distributed (i.i.d.) Gaussian noise, we can calculate the resulting error channel we obtain when using the analog information in an exact approach instead of requiring simulations as in Refs. [6, 13]. The crucial observation allowing this is that the concatenation of square GKP codes with a stabilizer code is a code with a more sophisticated lattice in the phase space. The exact calculation can be performed by calculating the Voronoi cells for $\mathcal{L}^\perp/\mathcal{L}$. More details can be found in Appendix G.

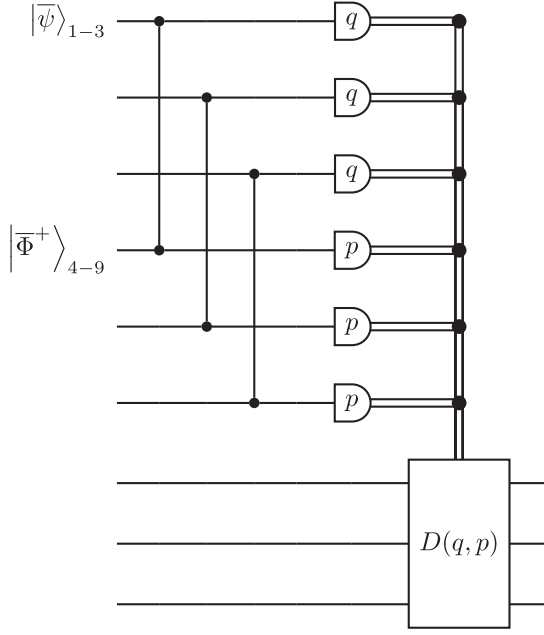


FIG. 3. Error correction by teleportation for the concatenation of a square GKP code with a three-qubit repetition code. In the first three modes we have the noisy input encoded in the code. In modes 4–9 we have an encoded Bell state of the full code where we then couple the first half with the three input modes transversally with beam splitters. We then perform homodyne measurements and apply conditional displacements on the second half of the encoded Bell state.

D. Linear-optics state generation

1. GKP Bell states

Up to now we have not assumed anything about the random variables despite their being Gaussian. However, depending on the actual state generation there might be correlations involved. For example, let us consider the case where we generate a square GKP Bell state by coupling a noisy $|+\rangle_2$ and a noisy $|0\rangle_3$ with a CSUM gate. We further assume that the noise of both GKP qubits consists of i.i.d. Gaussian shifts in position (u_2^*, u_3^*) and momentum (v_2^*, v_3^*) with variance Δ^2 . Due to the CSUM gate we see that the random variables $u_2 = u_2^*$, $v_2 = v_2^* - v_3^*$ and $u_3 = u_2^* + u_3^*$, $v_3 = v_3^*$ contain some correlations. The states of modes 2 and 3 are used in different error-correction steps and in usual decoding schemes (quite recently decoders making use of the syndrome information of multiple rounds have been considered [34]) it is assumed that each correction step only uses local information, neglecting the correlations. Therefore, it seems that the CSUM gate amplifies the noise such that we have momentum shifts with variance $2\Delta^2$ in mode 2 and position shifts of variance $2\Delta^2$ in mode 3. When additionally considering the noise from mode 1 we obtain the same result as in Ref. [33] that the sum of initially three random variables of individual variance Δ^2 should be smaller than $\sqrt{\frac{2\pi}{D}}/2$. Thus, in terms of thresholds we do not gain anything by using a teleportation scheme instead of the Knill-Glancy scheme.

Let us now consider a different scheme for generating Bell states as introduced in Ref. [36] using only a beam splitter to

couple two noisy GKP-like states. Thanks to the simple linear-optical coupling the resulting random variables u_2, u_3, v_2, v_3 are all i.i.d. with variance Δ^2 . This allows us to use simple decoders depending only on the syndrome information from this correction step without losing the capability of correcting errors. Thus, in an error correction by teleportation we only need to consider $2\sigma_{sq}^2$ using this beam splitter approach instead of $3\sigma_{sq}^2$ when using CSUMs for generating the Bell states and neglecting correlations between different teleportation steps.

In Ref. [36], it was shown for a square GKP qubit code that a Bell state can be obtained by mixing two “qunaught” states at a 50:50 beam splitter by using the state picture. Here, we will first reproduce this result in the stabilizer formalism, such that it will be easy to generalize the result to more general GKP codes.

Now we will consider the slightly more general case of a square-lattice GKP code with even qudit dimension D . Consider the two single-mode states described by the stabilizer group generated by the set of stabilizer generators:

$$\left\{ \exp(i\sqrt{\pi D}\hat{q}_1), \exp\left(i\sqrt{\frac{4\pi}{D}}\hat{p}_1\right), \exp\left(i\sqrt{\frac{4\pi}{D}}\hat{q}_2\right), \exp(i\sqrt{\pi D}\hat{p}_2) \right\}. \quad (23)$$

Let us apply a 50:50 beam splitter mixing both modes, resulting in the stabilizer generators

$$\left\{ \exp\left(i\sqrt{\frac{\pi D}{2}}(\hat{q}_1 + \hat{q}_2)\right), \exp\left(i\sqrt{\frac{2\pi}{D}}(\hat{p}_1 + \hat{p}_2)\right), \exp\left(i\sqrt{\frac{2\pi}{D}}(\hat{q}_1 - \hat{q}_2)\right), \exp\left(i\sqrt{\frac{\pi D}{2}}(\hat{p}_1 - \hat{p}_2)\right) \right\}. \quad (24)$$

This set of stabilizer generators already describes the canonical Bell state of the square GKP code. However, we will consider a different set of stabilizer generators by multiplying stabilizers such that it is more obvious that this set stabilizes the Bell state:

$$\left\{ \exp(i\sqrt{2\pi D}\hat{q}_1), \exp\left(i\sqrt{\frac{2\pi}{D}}(\hat{p}_1 + \hat{p}_2)\right), \exp\left(i\sqrt{\frac{2\pi}{D}}(\hat{q}_1 - \hat{q}_2)\right), \exp(i\sqrt{2\pi D}\hat{p}_1) \right\}. \quad (25)$$

Here we multiplied the first (fourth) stabilizer generator $D/2$ times with the third (second) stabilizer generator. Since the number of multiplications must be an integer, we have the restriction that D has to be even. For odd D it seems that no scheme using only linear optics and two product states is possible (a simple beam splitter solution does not exist), but we have no rigorous proof for this. We obtained our results ($n = 1$) by going through the above steps in opposite direction in order to obtain the input state. We started with the stabilizers of the desired Bell state [Eq. (25)], applied an arbitrary two-mode passive linear-optical transformation, and tried to multiply stabilizers such that there are only local stabilizer pairs for each mode [Eq. (23)]. Notice that this arbitrary operation can be decomposed into a relative phase

followed by a beam splitter followed by another relative phase and a global phase. The two phases applied after the beam splitter are single-mode operations and are therefore useless for changing entanglement, so we can ignore them.

Furthermore, it is also possible to show similar results (for even D) not only for the square-lattice GKP code, but for more general ones. However, this is meant in the sense that we can obtain a $2n$ -mode Bell state by mixing two n -mode states at n 50:50 beam splitters in a transversal fashion. The proof for this is given in Appendix B.

2. Higher encoded GKP Bell states

The most important ingredient for the error correction by teleportation of the high-level code is the generation of the logical Bell state. Here, we discuss the possibility of generating these high-level states by sending product states of single-mode grid states through a linear optical network. Such a generation would be nice for two reasons. First, the linear-optical operations do not amplify the noise (we assume the initial noise is isotropic), and second, inline squeezing is experimentally demanding and usually implemented via the teleportation of a finitely squeezed state necessarily introducing errors due to the finite squeezing. It is easy to see that this linear-optical network is unable to transform small GKP codes and states into a concatenation of a GKP code with a stabilizer code, because linear-optical operations are represented by symplectic, orthogonal matrices in phase space and due to the orthogonality the code distance remains invariant (details are given in Appendix F). However, while this shows that it is impossible to encode arbitrary quantum information into a code of higher code distance using linear-optical transformations, it might still be possible to generate some codewords which can then be used for performing error correction.

As the next step we discuss this loophole for relevant cases. Remember that linear-optical transformations are represented by orthogonal and symplectic linear maps in the phase-space representation. We will now use the orthogonality in order to obtain necessary conditions. Thus, we need to check whether the desired state admits a lattice representation with an orthogonal basis. Conditions for the existence of an orthogonal basis are discussed in Ref. [42] for so-called construction-A lattices (for every linear code $C \in \mathbb{Z}_p^n$ we can construct a lattice $\{x \in \mathbb{Z}^n | x \bmod p \in C\}$), which appear when we consider the concatenation of a GKP code with a high-level CSS code (the codewords of C correspond to the stabilizers of the high-level code, while the mod corresponds to the stabilizers of the low-level GKP code), where the stabilizers of this concatenation are given by the columns of the matrix

$$A = \frac{1}{\sqrt{D}} \mathbb{1}_{2n \times 2n} \cdot \begin{pmatrix} G^X & 0 \\ 0 & G^Z \end{pmatrix}. \quad (26)$$

Each column of G^X , G^Z corresponds to a basis element of the corresponding construction-A lattice and each column of $\frac{1}{\sqrt{D}} \mathbb{1}_{2n \times 2n}$ gives the phase-space representation of the X and Z operators of the square-lattice GKP code. Because much experimental effort has been made in order to generate rectangular grid states [4,5], it is a relevant question whether these states can be transformed into codewords of the concatenation of the square-lattice GKP code with a CSS code by passive

linear-optical operations. Thus, we want $A = U \cdot A'$ to hold where U is an orthogonal, symplectic matrix describing the passive transformation and A' is a diagonal matrix denoting the stabilizers of independent rectangular grid states. Since A' and U are orthogonal matrices, it is necessary that A and therefore also G^X and G^Z (needs to hold for at least one basis) have to be orthogonal matrices in order for a passive transformation to exist.

Before we consider a large class of CSS codes let us first consider a specific example, namely, the three-qubit GKP-GHZ state. Its qubit stabilizer generators are $X_1 X_2 X_3$, $Z_1 Z_2$, and $Z_2 Z_3$. As a consequence we obtain

$$G^X = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 0 & 2 \end{pmatrix}, \quad G^Z = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}, \quad (27)$$

as a possible basis of the construction-A lattices generated by the code $C = C_1 \oplus C_2 = \text{span}_{\mathbb{Z}_2}(0, 0, 0 | 1, 1, 1) \oplus \text{span}_{\mathbb{Z}_2}((1, 1, 0 | 0, 0, 0), (0, 1, 1 | 0, 0, 0))$. Since C_1 has code distance of 3, it is obvious that code C cannot be factored into (permuted) linear subcodes of maximum length 2. Hence, by Ref. [42] there exists no orthogonal basis and thus we are not able to generate the GHZ state from single-mode grid states and linear optics.

In CSS codes the set of X -type operators (involving stabilizers and logical operators) corresponds to codewords of C_Z and the set of Z -type operators corresponds to codewords of C_X . Therefore, all operators stabilizing a logical Pauli eigenstate correspond to a subcode of $C_Z \oplus C_X$ using the symplectic representation and its code distance $d(C_Z \oplus C_X)$ is given by $\min(d(C_Z), d(C_X))$. We are mostly interested in codes which are able to correct at least arbitrary single-qubit errors demanding that the minimum code distance is at least 3. In Ref. [42] it was shown that a construction-A lattice over a binary field can only have an orthogonal basis if the corresponding code can be decomposed in a specific structure with a code distance of at most 2. Thus it is impossible in the qubit case to find such a passive transformation. In the qutrit case we can make a similar argument where the code distance must not be greater than 3 (it might still be impossible for 3); i.e., we can exclude the possibility of a passive transformation for high-distance codes. Up to now we only considered the concatenation with a square-lattice GKP code, but in our argument we only used the property that the matrix representing the X and Z operators of the GKP code is orthogonal. Therefore, the result also holds for concatenations involving any GKP code fulfilling this relation.

Up to now we assumed idealized infinitely squeezed GKP states in the proof of the above no-go statement, but a similar argument also works for the physically more relevant case of approximate GKP states with coherent Gaussian displacement errors where the Gaussian's covariance matrix needs to be proportional to the identity up to symplectic transformations. We make use of the finite-squeezing stabilizers introduced in Ref. [43], where finite squeezing with coherent Gaussian displacement errors (covariance matrix proportional to the identity) is applied by the operator $e^{-\Delta^2 \hat{n}}$ (Δ^2 as a parameter in order to be consistent with the notation of Ref. [43])

transforming the stabilizer of an ideal GKP state $\exp(i\hat{g})$ to

$$e^{-\Delta^2\hat{n}} \exp(i\hat{g}) e^{\Delta^2\hat{n}} = \exp\{i[\hat{g} \cosh(\Delta^2) + i\hat{g} \sinh(\Delta^2)]\}, \quad (28)$$

where \hat{g} and \hat{g} are (real) linear combinations of quadrature operators and \hat{n} is the total photon number in all modes. Using the (canonical extension of the) symplectic representation one can map the stabilizer conditions of the finitely squeezed states to a lattice embedded in \mathbb{C}^{2n} instead of \mathbb{R}^{2n} . Since Gaussian unitary operations do not couple the real and imaginary parts in the symplectic representation, the real part of the lattice also needs to fulfill the orthogonality constraints as for the ideal GKP states independent from the imaginary part. Up to scaling factors we have the same problem as in the infinite squeezing case and since scaling factors are irrelevant for orthogonality, we again obtain a no-go result. Let us now briefly show that this holds for all Gaussians with a covariance matrix which is related by a symplectic transformation A to a covariance matrix proportional to the identity. We can see this by first applying \hat{A}^{-1} to the ideal desired state, followed by $e^{-\Delta^2\hat{n}}$ in order to introduce the isotropic Gaussian noise followed by \hat{A} bringing the covariance matrix to the desired form. The resulting stabilizer is then given by

$$\begin{aligned} & \exp\{i[\hat{A}\hat{A}^{-1}\hat{g}\hat{A}^{-1} \cosh(\Delta^2) + i\hat{A}\hat{A}^{-1}g\hat{A}^{-1} \sinh(\Delta^2)]\} \\ & = \exp\{i[\hat{g} \cosh(\Delta^2) + i\hat{A}\hat{A}^{-1}g\hat{A}^{-1} \sinh(\Delta^2)]\}, \end{aligned}$$

which has the exact form as in Eq. (28).

As it is impossible to build logical Bell states of a high-level GKP code from single-mode grid states with linear-optical transformations, one might be wondering if one could use linear-optical transformations and two suitable n -mode grid states as a resource instead. However, this also turns out to be impossible for simple transversal beam splitters (see Appendix B), although we have not proven yet the impossibility of this with general linear optics.

An alternative approach to get rid of inline squeezing operations circumventing this no-go case was shown in Ref. [15] where the authors propose to generate an n -mode GKP cluster state by applying a linear-optical transformation on $4n$ rectangular GKP states, performing homodyne measurements on $3n$ modes and applying conditional displacements. Thus one might think that one also obtains the advantage of amplifying no noise. While technically true, one adds additional noise due to the additional finitely squeezed GKP states. Strictly speaking this approach would introduce even more noise than the canonical circuit involving (ideal) controlled-Z (CZ) gates, because by applying circuit identities one can show (see Fig. 2 of Ref. [15]) that the linear-optical scheme is equivalent to the canonical scheme up to some CSUM gates which act as the identity on the code space, but propagate noise from the auxiliary states to the data state. Another disadvantage of this scheme, despite its conceptual beauty and other possible practical advantages, lies in the overhead of the required costly GKP states.

It is an interesting question whether there exist similar schemes with a lower overhead, potentially introducing less noise than the canonical encoding scheme.

V. KNILL-GLANCY ERROR CORRECTION

In the previous section we discussed one scheme allowing us to obtain the full error syndrome without using inline squeezing. In this section we will consider another such scheme. This scheme is an improvement of the Knill-Glancy scheme such that all squeezing operations only act on ancilla states. For the square-lattice qubit GKP code this improved scheme was already (independently from our work) proposed in Ref. [34].

Here we will first discuss the stabilizer formalism and measurements by discussing the error correction of one quadrature in the original Knill-Glancy scheme as an example. Then it is easy to first generalize the improved Knill-Glancy scheme to arbitrary n -mode GKP codes encoding qudits of arbitrary dimension D (see Appendix D) and later we also show that we can obtain an analogous scheme in the case where we concatenate these general GKP codes with arbitrary CSS codes (see Appendix E).

The stabilizers of the square qubit GKP code are $\exp(i2\sqrt{\pi}\hat{q})$ and $\exp(i2\sqrt{\pi}\hat{p})$. Let us first consider the correction of position shifts. Thus we have to consider a general GKP state and a GKP- $|+\rangle$ state. After the Gaussian error channel we have an (unknown) error operator $\exp[i(v_1\hat{q}_1 + v_2\hat{q}_2 - u_1\hat{p}_1 - u_2\hat{p}_2)]$. After this error the two-mode state is stabilized by the following four stabilizers:

$$\begin{aligned} & \exp(-iv_12\sqrt{\pi}) \exp(i2\sqrt{\pi}\hat{p}_1), \\ & \exp(-iu_12\sqrt{\pi}) \exp(i2\sqrt{\pi}\hat{q}_1), \\ & \exp(-iv_2\sqrt{\pi}) \exp(i\sqrt{\pi}\hat{p}_2), \\ & \exp(-iu_22\sqrt{\pi}) \exp(i2\sqrt{\pi}\hat{q}_2). \end{aligned}$$

After applying the beam splitter, we obtain the stabilizer generators:

$$\begin{aligned} & \exp(-iv_12\sqrt{\pi}) \exp(i\sqrt{2\pi}(\hat{p}_1 + \hat{p}_2)), \\ & \exp(-iu_12\sqrt{\pi}) \exp(i\sqrt{2\pi}(\hat{q}_1 + \hat{q}_2)), \\ & \exp(-iv_2\sqrt{\pi}) \exp\left(i\sqrt{\frac{\pi}{2}}(\hat{p}_1 - \hat{p}_2)\right), \\ & \exp(-iu_22\sqrt{\pi}) \exp(i\sqrt{2\pi}(\hat{q}_1 - \hat{q}_2)). \end{aligned}$$

As the next step we perform a position measurement of mode 2. We can then use the stabilizers to find the set of possible measurement outcomes. By multiplication we find that $\exp[-i2\sqrt{\pi}(u_1 - u_2)] \exp(i2\sqrt{2\pi}\hat{q}_2)$ is also a stabilizer and thus possible measurement values of \hat{q}_2 take the form of $\frac{u_1 - u_2}{\sqrt{2}} + \frac{\sqrt{\pi}}{\sqrt{2}}z$ for $z \in \mathbb{Z}$. In order to obtain the stabilizers after the measurement we simply replace \hat{q}_2 by the measurement value of \hat{q}_2 . For the stabilizers involving \hat{p} we simply take the smallest product of stabilizer generators such that there appears no \hat{p}_2 . This is quite similar to the qubit stabilizer formalism, where one takes products of stabilizer generators such that there is only one stabilizer generator which anti-commutes with the observable. Since we are not interested in the eigenstate after obtaining the measurement result we can discard this mode, such that we only need two stabilizer generators to specify our state. Thus the stabilizer generators

are given by

$$\begin{aligned} & \exp[-i2\sqrt{\pi}(v_1 + v_2)] \exp(i2\sqrt{2\pi}\hat{p}_1), \\ & (-1)^z \exp[-i\sqrt{\pi}(u_1 + u_2)] \exp(i\sqrt{2\pi}\hat{q}_1). \end{aligned}$$

It is now easy to check that after applying a squeezing operation (reducing the q variances by a factor of $1/2$) and a position displacement by $\frac{\hat{q}_2}{\sqrt{2}} - \frac{1}{2} \text{mod}_{2\sqrt{\pi}}(2\sqrt{2}\hat{q}_2)$ [44] we completed the error correction and are in a state which is stabilized by

$$\begin{aligned} & \exp[-i2\sqrt{\pi}(v_1 + v_2)] \exp(i2\sqrt{\pi}\hat{p}_1), \\ & \exp\left\{-i2\sqrt{\pi}\left[u_1 + \frac{1}{2} \text{mod}_{2\sqrt{\pi}}(2u_2 - 2u_1)\right]\right\} \exp(i2\sqrt{\pi}\hat{q}_1). \end{aligned}$$

However, this only shows that we are close to the code space of a GKP code, but we do not know if the information within the code space is disturbed. Therefore, we have to check that up to small phases (corresponding to small errors remaining after the error correction) we also have $\exp(i\sqrt{\pi}\hat{q}_1) \rightarrow \exp(i\sqrt{\frac{\pi}{2}}\hat{q}_1)$ which is easy to check (before applying the squeezing operation). However, in order to show $\exp(i\sqrt{\pi}\hat{p}_1) \rightarrow \exp(i\sqrt{2\pi}\hat{p}_1)$ we also need to exploit that the ancilla GKP qubit is in the $|+\rangle$ state, because otherwise we cannot have the product $\exp[i\sqrt{\frac{\pi}{2}}(\hat{p}_1 - \hat{p}_2)] \exp[i\sqrt{\frac{\pi}{2}}(\hat{p}_1 + \hat{p}_2)] = \exp(i\sqrt{2\pi}\hat{p}_1)$. When considering shift errors one simply has to check if the overall phase at the end is approximately “0” (no error) or “ π ” (error). Since we discarded stabilizer generators after the homodyne measurement it could be possible that we discarded too many such that we allow for too many states. However, after the measurement we only have one mode of interest, but still two independent stabilizer generators defining the code. Thus we did not discard too many stabilizers.

In the improved Knill-Glancy scheme the first ancilla is still a $|+\rangle$ state, but the second ancilla is now a $|0\rangle$ state which is squeezed by a factor $\sqrt{2}$ which can already be incorporated in the state generation, while we do not use inline squeezing of the data mode [see Fig. 1(c)]. For the case where we consider a concatenation with a CSS code we simply have to do the same and replace the GKP Pauli eigenstates by Pauli eigenstates of the high-level code and all beam splitters and homodyne measurements are applied in a transversal manner.

VI. ERROR PROPAGATION IN STABILIZER MEASUREMENTS

Let us consider prime qudit dimension D and a high-level CSS code. Such a stabilizer code is also defined by $n - k$ stabilizer generators which generate the whole stabilizer group. Usually the syndrome of a stabilizer code is obtained by directly measuring the $n - k$ stabilizer generators. In order to measure the stabilizers, we couple an ancilla with the code’s GKP qudits. The ancillas are finitely squeezed and therefore we need to carefully design our stabilizer measurements in such a way that a shift on one ancilla does not introduce errors in other stabilizer measurements. This has been done for the surface code in Ref. [7]. Here, we discuss whether this is possible for every CSS code and how these measurements need to be modified.

In this section we restrict ourselves to square-lattice GKP codes concatenated with CSS codes. In order to perform stabilizer measurements of CSS codes one couples an ancilla state with the data qubits with controlled- X ($CX_{i,j}$) operations. For example, measuring the stabilizer $\prod_{i \in \text{support}} X_i$ can be realized by measuring the ancilla a of $\prod_i CX_{a,i}|+\rangle_a$ in the X basis, while the stabilizer $\prod_{i \in \text{support}} Z_i$ can be measured by measuring $\prod_i CX_{i,a}|0\rangle_a$ in the Z basis. We implement the CX gate by using a CSUM gate since we consider a square-lattice GKP code. Notice that operators acting equally within the code space do not necessarily act the same way outside of the code space. Furthermore, because ideal GKP states are unphysical, we are almost surely outside of the code space and should therefore take these differences into account.

When performing the Z -stabilizer measurements in a standard way the CSUM gates transfer momentum shifts from the ancilla state originating from the finite squeezing to the data GKP states resulting in correlated momentum shifts on multiple data GKP qudits. When performing the X -stabilizer measurements later these shifts may introduce errors in the syndrome. Especially due to the correlations these shifts can easily add up and overcome the threshold of correctable shifts as the variance of the sum of n independent random variables increases linearly while the variance of n times the same random variable increases quadratically. Furthermore, due to the correlated shifts the faults of the stabilizer measurements would no longer be independent.

In Ref. [7] the authors introduced a way of using CSUM and inverse CSUM gates to exploit the correlations of the shift errors such that they cancel in the next stabilizer measurement, and so there is no error propagation from one ancilla to another ancilla for the planar-square surface code.

Let us now discuss this error propagation in a systematic way in an attempt to generalize the scheme from Ref. [7] to more general quantum error-correcting codes with parameters $[n, k, d]_D$. Let us define the vector

$$\vec{\Delta}_{\text{data}}^T = (\vec{u}_d, \vec{v}_d) = (u_{d,1}, \dots, u_{d,n}, v_{d,1}, \dots, v_{d,n}) \quad (29)$$

of random variables describing the shift errors (u for position shifts and v for momentum shifts) acting on data GKP qudits. Similarly we can define such a vector for the ancilla GKP qudits which are used to measure the X/Z stabilizer generators:

$$\vec{\Delta}_{X/Z}^T = (\vec{u}_{X/Z}, \vec{v}_{X/Z}) = (u_{X/Z,1}, \dots, u_{X/Z,l_{X/Z}}, \quad (30)$$

$$v_{X/Z,1}, \dots, v_{X/Z,l_{X/Z}}), \quad (31)$$

where $l_{X/Z}$ gives the number of X - or Z -type stabilizer generators. Suppose we assume that all data GKP qudits performed their syndrome measurement before measuring the stabilizers of the higher code. This means that all u and v are i.i.d. Gaussian random variables with mean zero and variance σ_{sq}^2 .

We now first perform the X -stabilizer measurements and due to the coupling we obtain the following error vectors:

$$\vec{u}'_d = \vec{u}_d + H_X^T \vec{u}_X, \quad (32)$$

$$\vec{v}'_d = \vec{v}_d, \quad (33)$$

$$\vec{u}'_X = \vec{u}_X, \quad (34)$$

$$\vec{v}'_X = \vec{v}_X - H_X \vec{v}_d. \quad (35)$$

In order to measure the X stabilizer we measure the momentum quadrature of the ancillas and therefore we always obtain a faulty syndrome whenever a random variable in \vec{v}'_X lies in the set of uncorrectable errors.

When we now perform the Z -stabilizer measurements we obtain due to the coupling the error vectors

$$\vec{u}''_d = \vec{u}'_d = \vec{u}_d + H_X^T \vec{u}_X, \quad (36)$$

$$\vec{v}''_d = \vec{v}'_d - H_Z^T \vec{v}_Z = \vec{v}_d - H_Z^T \vec{v}_Z, \quad (37)$$

$$\vec{u}'_Z = \vec{u}_Z + H_Z \vec{u}'_d = \vec{u}_Z + H_Z \vec{u}_d + H_Z H_X^T \vec{v}_X, \quad (38)$$

$$\vec{v}'_Z = \vec{v}_Z. \quad (39)$$

In order to have a successful Z -stabilizer measurement we demand that \vec{u}'_Z needs to lie in the set of correctable errors. The variance of $(\vec{u}'_Z)_j$ is given by $(1 + \|(H_Z)_{j,*}\|_2 + \|(H_Z H_X^T)_{j,*}\|_2) \sigma_{sq}^2$. Also note that $H_Z H_X^T = 0$ needs to hold in order to avoid error propagation between the GKP ancillas. However, up to now we only required that we are given a valid CSS code, which means that all stabilizer generators need to commute demanding $H_Z H_X^T \bmod D = 0$. These two conditions are equivalent to requiring that the symplectic form of any two rows of H vanishes (without or with $\bmod D$). Therefore, it is useful to generalize the check matrix $H \in \mathbb{Z}_D^{(n-k) \times 2n}$ to $\tilde{H} \in \mathbb{Z}^{(n-k) \times 2n}$, where $H \sim \tilde{H} \bmod D$, \sim denotes row equivalence with respect to the finite field \mathbb{Z}_D , and, furthermore, we need that the symplectic form vanishes for any two distinct rows of \tilde{H} .

In a recent work (see Theorem 12 of Ref. [45]) in the context of generalizing qubit to qudit codes, it was shown that it is always possible to find such an \tilde{H} . Thus, there is no error propagation anymore. However, this construction does not guarantee that the stabilizer weights remain small such that the noise actually coming from the data qudits may be amplified in the syndrome measurement.

As one possible approach to reduce the stabilizer weights we can simply add rows of the matrix \tilde{H} and try to minimize the stabilizer weights, which means we simply look for a different set of stabilizer generators. However, note that this approach is not feasible, because the problem is equivalent to being given a basis of a lattice and trying to find a different basis with minimal length and this is also known as the shortest basis problem on a lattice which was shown to be NP hard [46].

A different approach relies on fixing the stabilizer weight and trying to fulfill the symplectic condition. Here we will look at the cases $D = 2$ and $D > 2$ separately, because in the $D = 2$ case X and Z are self-inverse, giving us much more freedom while having the same stabilizer weight.

For $D > 2$ it is not possible to sustain the minimal stabilizer weight from the canonical scheme and avoid error propagation for arbitrary CSS codes, as it can be seen for the example of the $[D, D - 2, 2]_D$ error-detecting code with stabilizers $\prod_{j=1}^D X_j$ and $\prod_{j=1}^D Z_j$. In order to sustain the minimal stabilizer weight, we cannot modify the stabilizer generators, but their corresponding symplectic form does not vanish (without $\bmod D$). However, for $D = 2$ we can consider the stabilizers $X_1 X_2$ and $Z_1 Z_2^{-1}$ which still have minimal stabilizer

weight, but their corresponding symplectic form vanishes (without $\bmod D$).

For $D = 2$ we can ideally fulfill the two conditions $\tilde{H}_Z \tilde{H}_X^T = 0$ and $\|(\tilde{H}_{X/Z})_{j,*}\|_2 = \|(H_{X/Z})_{j,*}\|_2$ simultaneously. Let us now show some examples where we are able to fulfill both conditions.

As the first example let us consider the quantum parity code [47]; this is a CSS code and the Z stabilizers consist of weight 2 checks. Thus we choose $\tilde{H}_X = H_X$ and for \tilde{H}_Z we use H_Z , but in each row we replace one of the two 1s by -1 ; thus the symplectic form is given by $1 \times 1 + 1 \times (-1) = 0$ (when it does not vanish trivially). Also note that it is possible to define the quantum parity code for qudits.

Let us now consider two-dimensional surface codes on lattices without boundary. If all face stabilizers have an even number of qubits in their support or if all vertex stabilizers have an even number of qubits in their support it is possible to achieve the optimal minimum. In order to do so we will modify $\tilde{H}_{X/Z}$ for the type of stabilizers with even support (if it works for both faces and vertices we can choose) and we do not change the other. Notice that face and vertex operators have either zero or two common qubits in their support. As an example let us consider that our faces have even support. Instead of assigning each edge (corresponding qubit) the value 1 we assign ± 1 in an alternating way (“neighboring edges have different values”). Thus similar to the quantum parity code the symplectic form vanishes. Notice that this already includes many surface codes such as those with square, triangular, and hexagonal tilings or even [4,5] tilings in hyperbolic geometry [48].

However, also note that many surface and color codes have already been generalized from qubits to qudits by considering inverse Pauli operations [49–52], implying that we can use their orientations to avoid error propagation and also obtain the optimal minimum.

VII. COMPARISON OF DIFFERENT SYNDROME MEASUREMENTS

We have discussed two different approaches for obtaining the GKP syndrome information, namely, an improvement of the Knill-Glancy scheme and an adaption of the error correction by teleportation scheme. Both schemes have the advantage of using no inline squeezing in contrast to schemes which make use of CSUM gates, which are only implemented approximately. In general, the GKP Bell states needed for the teleportation scheme can be considered more expensive than the ancilla states for the Glancy-Knill scheme, because the former consist of a $2n$ -mode entangled GKP state instead of two n -mode entangled states. However, for the case of even qudit dimension D we have shown that it is possible to generate such a state by sending two n -mode entangled GKP states transversally through n beam splitters. Because there are only beam splitters and there is also no offline squeezing we even get less noise than in the Knill-Glancy scheme.

For obtaining the high-level syndrome information we have considered three different schemes. Two of them (variations of the teleportation and the Knill-Glancy scheme) need no inline squeezing, but complicated ancilla states consisting of high-level encoded Bell states or (presqueezed) high-level

Pauli eigenstates. These two schemes also have the advantage that we also obtain the GKP syndrome such that we only need to perform $2n$ measurements in order to obtain the full syndrome information. One might say that generating a high-level Bell state of a CSS code is not much more problematic than producing high-level Pauli eigenstates because one could implement the logical CNOT via transversal CSUM gates, but there we also have the issue that we correlate or rather amplify the noise of different modes if we ignore the correlations. However, in the third scheme (only for square GKP codes) we first use $2n$ measurements in order to correct displacements on the GKP qudits and then we perform the high-level stabilizer measurements by coupling ancilla states with the data qudits via CSUM gates. This scheme has the advantage that the needed ancilla states are rather easy to generate, but one has various disadvantages: one needs inline squeezing operations, one has to use already $2n$ measurements in order to correct the small displacements, and then additionally one has to measure the high-level stabilizers which also increases the noise of the already corrected data qudits due to backpropagation of errors originating from the finitely squeezed ancillas.

VIII. CONCLUSION

In this article we have considered syndrome measurements of general GKP codes encoding qudits of dimension D and their concatenation with stabilizer codes. We showed that we can obtain the full syndrome information of such an arbitrary n -mode code by making use of only $2n$ measurements. Furthermore, we discussed two schemes which allow us to obtain the GKP syndrome information by using either two suitable n -mode ancilla states or a single $2n$ -mode GKP Bell state ancilla, transversal beam splitters, and homodyne measurements. For the case of even qudit dimension D we were able to show how GKP Bell states can be generated with transversal beam splitters and n -mode grid states.

Concerning the high-level syndrome information, we also proposed two similar schemes without inline squeezing which give us the whole syndrome information with $2n$ homodyne measurements employing an ancilla state. We believe that not only for the Knill and Steane schemes as explicitly presented in this work, but for all fault-tolerant error-correction schemes where the data modes are coupled by transversal CNOTs with an ancilla state (e.g., Shor states; see Sec. 4 of Ref. [53]) in order to perform the syndrome measurements of the higher code, one can additionally obtain the GKP syndrome information of all involved GKP codes. Moreover, we discussed error propagation in usual stabilizer measurements and also showed that linear-optical transformations leave the code distance of GKP codes and more generally error-correcting properties of codes against isotropic displacement noise invariant. We further analyzed the possibility of generating high-level codewords by rectangular single-mode grid states and linear optics. Besides this, we proposed an approach to calculate the logical error rates of a concatenation of a GKP code with a stabilizer code making use of the analog syndrome information where we calculate integrals instead of performing Monte Carlo simulations. Our main results can be summarized as follows:

(1) For GKP higher code syndrome detection, we proposed a minimal stabilizer set to be measured to obtain the full syndrome information.

(2) For logical qubits as well as qudits with nonprime dimensions the minimal measurement set is directly obtainable through Knill's error correction by teleportation on the higher level using higher GKP Bell states; this directly provides an operational interpretation leading to a possible implementation with transversal GKP qubit teleportations using beam splitters.

(3) For general logical qudits the minimal set can be derived via lattice theory.

(4) In a second scheme, different from Knill's, we achieved the same for higher code syndrome detections, generalizing known results for only the lower GKP level, still avoiding inline squeezing.

(5) For GKP higher code state generation, given higher n -mode GKP codes ($k < n$ qudits), we showed that the corresponding higher GKP Bell states cannot be obtained via transversal beam splitters; for arbitrary passive linear optics, it remains open.

(6) For GKP higher code state generation, given copies of arbitrary rectangular single-mode grid states, we have shown that the codewords of the higher GKP codes can generally not be obtained via passive linear optics.

(7) For GKP qudit Bell state generation, generalizing a known result for GKP qubits, we showed that for even qudit dimension the Bell states can be created from a number of suitable input grid states via transversal beam splitters (this result includes states with $k = n$ qudits encoded into n modes); whether this is also possible for odd qudit dimensions remains open.

Note added. At the final preparation stage of this work, Ref. [54] was posted. Similar to our treatment, that work also addresses the issue of a minimal stabilizer basis in higher GKP codes. While there is also some overlap in terms of the methods used, overall the two works are complementary, where our work has a particular focus on linear-optical realizations of the error-correction schemes.

ACKNOWLEDGMENTS

We thank Daniel Miller for useful discussions about the generation of the GKP Bell states. We thank the BMBF in Germany for support via Q.Link.X/QR.X and the BMBF/EU for support via QuantERA/ShoQC.

APPENDIX A: MINIMAL SET OF STABILIZER GENERATORS

Theorem 1. For any GKP code (n modes, arbitrary qudit dimension D) concatenated with an arbitrary stabilizer code it is possible to obtain the full syndrome information with $2n$ measurements.

Proof. It is well known that the phase-space representation of the stabilizers of a GKP code forms a lattice $\mathcal{L} \subset \mathbb{R}^{2n}$. Similarly, the phase-space representation of the set of operators commuting with the stabilizers $\mathcal{L}^\perp \subset \mathbb{R}^{2n}$ also forms a lattice (see Sec. VI of Ref. [2]). We can show that the phase-space representation Λ of the stabilizers of a GKP code concate-

nated with a higher-level stabilizer code also forms a lattice. For this we have to show that Λ is a discrete, linear subgroup of \mathbb{R}^{2n} and we will use the relation $\mathcal{L} \subseteq \Lambda \subset \mathcal{L}^\perp$ (the last relation holds because all stabilizers have to commute). Since we can obtain Λ by adding additional points to \mathcal{L} in a linear way, it is easy to see that Λ forms a linear subset of \mathbb{R}^{2n} . Since Λ is a subset of \mathcal{L}^\perp which is discrete (since it is a lattice), meaning that there exists an $\epsilon > 0$ such that there is always at most one lattice point in an ϵ neighborhood, it is clear that Λ is also discrete and therefore also forms a lattice. Every lattice has a basis (see Theorem 8 of Ref. [55]) and therefore we only have to measure the $2n$ operators corresponding to the lattice basis elements. ■

APPENDIX B: LINEAR-OPTICAL DECOMPOSITION OF BELL STATES

Here we show that it is possible for arbitrary GKP codes with even qudit dimension D to generate Bell states by mixing two GKP-like states at n beam splitters transversally. Let us choose a fixed arbitrary GKP code (encoding $k = n$ qudits in n modes) and let us write the logical Pauli operators as $\bar{X}_j = \exp(i\hat{x}_j)$ ($j \in \{1, \dots, n\}$) implicitly defining \hat{x}_j and we do the same for \hat{z}_j with $\bar{Z}_j = \exp(i\hat{z}_j)$.

In the next step the first index will number the logical operators of a GKP code and the second one will number the two codes. We start with the product state stabilized by the $4n$ stabilizers (j takes every value in $\{1, \dots, n\}$)

$$\left\{ \exp\left(i\frac{D}{\sqrt{2}}\hat{z}_{j,1}\right), \exp(i\sqrt{2}\hat{x}_{j,1}), \exp(i\sqrt{2}\hat{z}_{j,2}), \exp\left(i\frac{D}{\sqrt{2}}\hat{x}_{j,2}\right) \right\}.$$

For the special case of $n = 1$ and $D = 2$ we have the four stabilizers of the product state of two GKP ‘‘qunaught’’ states (each representing a one-dimensional GKP space and hence a state with equal lattice spacing along x and p , $\sqrt{2}\pi$).

After applying a 50:50 beam splitter transversally upon every pair of code states 1 and 2 for every j , we obtain

$$\left\{ \exp\left[i\frac{D}{2}(\hat{z}_{j,1} + \hat{z}_{j,2})\right], \exp[i(\hat{x}_{j,1} + \hat{x}_{j,2})], \exp[i(\hat{z}_{j,1} - \hat{z}_{j,2})], \exp\left[i\frac{D}{2}(\hat{x}_{j,1} - \hat{x}_{j,2})\right] \right\}.$$

After a suitable multiplication (strictly assuming even D to make sure an integer number of multiplications) of the stabilizers as discussed in the main text, we get

$$\left\{ \exp(iD\hat{z}_{j,1}), \exp[i(\hat{x}_{j,1} + \hat{x}_{j,2})], \exp[i(\hat{z}_{j,1} - \hat{z}_{j,2})], \exp(iD\hat{x}_{j,1}) \right\},$$

where it is obvious that this set stabilizes GKP Bell states as this set contains $\bar{X}_1\bar{X}_2$ and $\bar{Z}_1\bar{Z}_1^{-1}$ which are the stabilizers of a Bell state and furthermore we have two independent stabilizer generators from the original GKP code. For the cases with odd D we do not know whether GKP Bell states can be built from two n -mode code states with linear optics.

When we consider a code encoding $k < n$ qudits in n modes, unfortunately it is impossible to generate logical Bell states by coupling two product states by simple transversal beam splitters. In this case, the code space is defined by $4n$ independent stabilizer generators and $4k$ of them are proportional to logical Pauli operators. For these stabilizer generators we already know what the input stabilizers should look like. Thus, we only need to know what the remaining input stabilizers should look like. In order to obtain these we first consider the desired stabilizer generators and transform them by the inverse beam splitters (our beam splitters are self-inverse). Also notice that these stabilizer generators are independent (linearly independent in the symplectic representation) and thus we only need to consider a pair of equivalent stabilizers of both codes:

$$\begin{aligned} & \{\exp(i\hat{g}_1), \exp[i(\hat{g}_1 + \hat{g}_2)]\} \\ & \rightarrow \left\{ \exp\left[\frac{i}{\sqrt{2}}(\hat{g}_1 + \hat{g}_2)\right], \exp(i\sqrt{2}\hat{g}_1) \right\}. \end{aligned}$$

It is obvious then that it is impossible to multiply the first stabilizer with the second one in such a way that the first stabilizer only acts on the modes belonging to code 2.

APPENDIX C: KNILL ERROR CORRECTION FOR QUDITS

Here we generalize the error correction by teleportation scheme proposed by Knill [32] from qubits to qudits. Although this scheme works for arbitrary qubit stabilizer codes, we have to restrict ourselves to CSS codes for the generalization to qudits, because the Pauli operators are not self-inverse anymore.

The projection operator onto the code space with syndrome s is given by (Q is a matrix where each row corresponds to the symplectic representation of a stabilizer generator, see Ref. [32])

$$\Pi(Q, e) = \prod_l \left(\sum_{j=0}^{D-1} \exp(i\omega e_l \hat{g}_l)^j \right), \quad (C1)$$

where \hat{g}_l is the l th stabilizer generator of the code represented by the matrix Q , and

$$\Pi_2(Q, 0)|\Phi^+\rangle_{12}^{\otimes n} \quad (C2)$$

$$= \Pi_2(Q, 0)\Pi_2(Q, 0)|\Phi^+\rangle_{12}^{\otimes n} \quad (C3)$$

$$= \Pi_2(Q, 0)\Pi_1(\bar{Q}, 0)|\Phi^+\rangle_{12}^{\otimes n}. \quad (C4)$$

In the first step, we wrote down the state which is needed to follow Knill’s proof. We then try to simplify this expression. In the second line we used the idempotence of projection operators. In the next step we used that qudit Bell states are stabilized by the X_1X_2 and $Z_1Z_2^{-1}$. Therefore, the projection onto the code represented by the matrix Q with syndrome 0 on the second n qudits is equivalent to a projection onto the code represented by \bar{Q} with syndrome 0 on the first n qudits. Here \bar{Q} is given via Q where all entries corresponding to X operators are multiplied by -1 . If Q is a CSS code then this means that some rows have to be multiplied by -1 and their syndrome should yield 0. One can multiply these rows again by -1 to obtain Q , but the syndrome does not change. This can also be understood in the following way: all X -type operators in

the stabilizer generators have been inverted. Thus for CSS codes the stabilizer group remains invariant. However, if Q does not represent a CSS code it may describe a different code from \hat{Q} . We checked it for the five-qudit (with stabilizer generators $X \otimes Z \otimes Z^{-1} \otimes X^{-1} \otimes \mathbb{1}$ and cyclic permutations thereof) code that the stabilizer group generated by Q does not equal the group generated by \hat{Q} for $D > 2$ in general.

The remaining proof is completely analogous to Knill's proof where he changes the order of the conditional Pauli operations and the projection operator, resulting in a changed syndrome and using the fact that the quantum teleportation protocol implements the identity.

APPENDIX D: LINEAR-OPTICAL KNILL-GLANCY SCHEME FOR GENERAL GKP CODES

Let us consider an n -mode GKP code which encodes qudits of dimension D , but now without concatenation with a stabilizer code. Let us consider normalized quadrature operators \hat{u}_j ($j \in \{1, \dots, n\}$) generating X_j and normalized quadrature operators \hat{v}_j generating Z_j . Thus we know that only $[\hat{u}_k, \hat{v}_k] \neq 0$ and all other commutators vanish. Furthermore, for a quadrature operator \hat{s} there exists a symplectic representation as a $2n$ -dimensional vector. We will refer to this symplectic representation as well as a measurement result of \hat{s} as s , but it should always be clear from the context what the meaning is in each case. The quantity $\omega(\cdot, \cdot)$ denotes the canonical symplectic form.

The stabilizers are then given by X_j^D and Z_j^D ($j \in \{1, \dots, n\}$) with

$$X_j = \exp\left(i\hat{u}_j \frac{1}{\sqrt{D\omega(u_j, v_j)}}\right), \quad (D1)$$

$$Z_j = \exp\left(i\hat{v}_j \frac{1}{\sqrt{D\omega(u_j, v_j)}}\right). \quad (D2)$$

Without loss of generality we have assumed that $\omega(u_j, v_j) > 0$ (the square GKP code is obtained with $\hat{u}_j = -\hat{p}_j$ and $\hat{v}_j = \hat{q}_j$). In order to consider shift errors in the stabilizer formalism we use the identity

$$e^{i\hat{a}} e^{i\hat{b}} e^{-i\hat{a}} = e^{i\hat{b}} e^{-i2\pi\omega(a,b)}. \quad (D3)$$

Let us now briefly discuss how the stabilizers of a GKP code transform under shift errors $e^{i\hat{a}}$:

$$|\psi\rangle = e^{i\hat{b}} |\psi\rangle, \quad (D4)$$

$$|\tilde{\psi}\rangle := e^{i\hat{a}} |\psi\rangle = e^{i\hat{a}} e^{i\hat{b}} |\psi\rangle = e^{i\hat{a}} e^{i\hat{b}} e^{-i\hat{a}} e^{i\hat{a}} |\psi\rangle \quad (D5)$$

$$= e^{i(\hat{b}-2\pi\omega(a,b))} |\tilde{\psi}\rangle. \quad (D6)$$

We will now show that we can apply the linear-optical Knill-Glancy scheme to general GKP codes. In the first stage the n data modes and the first n ancilla modes are given by the following stabilizers assuming displacement errors with symplectic representation e_1 and e_2 , and subscripts 1 and 2 refer to the data and half of the ancilla modes, respectively:

$$\exp\left(i(\hat{u}_{j,1} - 2\pi\omega(e_1, u_j)) \sqrt{\frac{D}{\omega(u_j, v_j)}}\right),$$

$$\exp\left(i(\hat{v}_{j,1} - 2\pi\omega(e_1, v_j)) \sqrt{\frac{D}{\omega(u_j, v_j)}}\right),$$

$$\exp\left(i(\hat{u}_{j,2} - 2\pi\omega(e_2, u_j)) \sqrt{\frac{1}{D\omega(u_j, v_j)}}\right),$$

$$\exp\left(i(\hat{v}_{j,2} - 2\pi\omega(e_2, v_j)) \sqrt{\frac{D}{\omega(u_j, v_j)}}\right).$$

After applying the 50:50 beam splitters we obtain the following stabilizers:

$$\exp\left(i\left(\frac{\hat{u}_{j,1} + \hat{u}_{j,2}}{\sqrt{2}} - 2\pi\omega(e_1, u_j)\right) \sqrt{\frac{D}{\omega(u_j, v_j)}}\right),$$

$$\exp\left(i\left(\frac{\hat{v}_{j,1} + \hat{v}_{j,2}}{\sqrt{2}} - 2\pi\omega(e_1, v_j)\right) \sqrt{\frac{D}{\omega(u_j, v_j)}}\right),$$

$$\exp\left(i\left(\frac{\hat{u}_{j,1} - \hat{u}_{j,2}}{\sqrt{2}} - 2\pi\omega(e_2, u_j)\right) \sqrt{\frac{1}{D\omega(u_j, v_j)}}\right),$$

$$\exp\left(i\left(\frac{\hat{v}_{j,1} - \hat{v}_{j,2}}{\sqrt{2}} - 2\pi\omega(e_2, v_j)\right) \sqrt{\frac{D}{\omega(u_j, v_j)}}\right).$$

In the next step we perform measurements of $\hat{v}_{j,2}$ and the measurement outcomes $\tilde{v}_{j,2}$ give us partial information about $\omega(e_1 - e_2, v_j)$ as it can be seen by the stabilizers (before the measurement):

$$\exp\left(i(\sqrt{2}\hat{v}_{j,2} - 2\pi\omega(e_1 - e_2, v_j)) \sqrt{\frac{D}{\omega(u_j, v_j)}}\right).$$

After the measurement the stabilizers of the data qudits are given by

$$\exp\left(i(\sqrt{2}\hat{u}_{j,1} - 2\pi\omega(e_1 + e_2, u_j)) \sqrt{\frac{D}{\omega(u_j, v_j)}}\right),$$

$$\exp\left(i\left(\frac{\hat{v}_{j,1} + \tilde{v}_{j,2}}{\sqrt{2}} - 2\pi\omega(e_1, v_j)\right) \sqrt{\frac{D}{\omega(u_j, v_j)}}\right).$$

We then apply a shift $\exp(i\hat{u}_{j,1} \frac{\tilde{v}_{j,2}}{2\pi\omega(u_j, v_j)})$. The stabilizers in the second phase of the scheme are

$$\exp\left(i(\sqrt{2}\hat{u}_{j,1} - 2\pi\omega(e_1 + e_2, u_j)) \sqrt{\frac{D}{\omega(u_j, v_j)}}\right),$$

$$\exp\left(i\left(\frac{\hat{v}_{j,1}}{\sqrt{2}} - 2\pi\omega(e_1, v_j)\right) \sqrt{\frac{D}{\omega(u_j, v_j)}}\right),$$

$$\exp\left(i(\sqrt{2}\hat{u}_{j,3} - \sqrt{2}2\pi\omega(e_3, u_j)) \sqrt{\frac{D}{\omega(u_j, v_j)}}\right),$$

$$\exp\left(i\left(\frac{\hat{v}_{j,3}}{\sqrt{2}} - \frac{2\pi\omega(e_3, v_j)}{\sqrt{2}}\right) \sqrt{\frac{1}{D\omega(u_j, v_j)}}\right).$$

After applying the beam splitter we obtain

$$\begin{aligned} & \exp\left(i(\hat{u}_{j,1} + \hat{u}_{j,3} - 2\pi\omega(e_1 + e_2, u_j))\sqrt{\frac{D}{\omega(u_j, v_j)}}\right), \\ & \exp\left(i\left(\frac{\hat{v}_{j,1} + \hat{v}_{j,3}}{2} - 2\pi\omega(e_1, v_j)\right)\sqrt{\frac{D}{\omega(u_j, v_j)}}\right), \\ & \exp\left(i(\hat{u}_{j,1} - \hat{u}_{j,3} - \sqrt{2}2\pi\omega(e_3, u_j))\sqrt{\frac{D}{\omega(u_j, v_j)}}\right), \\ & \exp\left(i\left(\frac{\hat{v}_{j,1} - \hat{v}_{j,3}}{2} - \frac{2\pi\omega(e_3, v_j)}{\sqrt{2}}\right)\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right). \end{aligned}$$

We then measure the operators $\hat{u}_{j,3}$ which are again constrained by a stabilizer and this gives us partial information about $\omega(e_1 + e_2 - \sqrt{2}e_3, u_j)$. Thus, after the measurement the GKP code is stabilized by

$$\begin{aligned} & \exp\left(i\left(\hat{v}_{j,1} - 2\pi\omega\left(e_1 + \frac{e_3}{\sqrt{2}}, v_j\right)\right)\sqrt{\frac{D}{\omega(u_j, v_j)}}\right), \\ & \exp\left(i(\hat{u}_{j,1} + \hat{u}_{j,3} - 2\pi\omega(e_1 + e_2, u_j))\sqrt{\frac{D}{\omega(u_j, v_j)}}\right). \end{aligned}$$

Similarly as before we apply a shift $\exp(-i\hat{v}_{j,1}\frac{\hat{u}_{j,3}}{2\pi\omega(u_j, v_j)})$ in order to obtain the stabilizer

$$\exp\left(i(\hat{u}_{j,1} - 2\pi\omega(e_1 + e_2, u_j))\sqrt{\frac{D}{\omega(u_j, v_j)}}\right).$$

A similar calculation can be done for the logical operators \bar{X} and \bar{Z} . When doing this for \bar{X} one can see that the logical operator transforms as

$$\begin{aligned} & \exp\left(i(\hat{u}_{j,1} - 2\pi\omega(e_1, u_j))\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right) \\ & \rightarrow \exp\left(i(\hat{u}_{j,1} - 2\pi\omega(e_1 + e_2, u_j))\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right), \end{aligned} \quad (D7)$$

which means we need to know $\omega(e_1 + e_2, u_j)$ in order to perform the error correction, but we only know $\omega(e_1 + e_2 - \sqrt{2}e_3, u_j) \bmod 2\pi\sqrt{\frac{\omega(u_j, v_j)}{D}}$ from our measurement results.

Up to small displacements originating from the noise on the ancilla states, we now have the same state as before the error correction, but we can use our measurement results for a maximum-likelihood estimation (which might also consider correlations between the measurement results) of $\omega(e_1, v_j)$ and $\omega(e_1 + e_2, u_j)$ and apply correction shifts accordingly. Since we never use the periodicity of the exponential it is straightforward to see that a similar calculation also holds if one assumes that the data qudits are stabilized by either X_j or Z_j . Thus logical errors can only occur if the maximum-likelihood estimation fails.

APPENDIX E: LINEAR-OPTICAL KNILL-GLANCY SCHEME FOR CONCATENATED CSS CODES

Here we show that it is possible to obtain the full syndrome information in a scheme similar to the one described in the previous section. We only have to consider (squeezed) logical Pauli eigenstates of the high-level code instead of the GKP code. Since we consider a concatenation of a GKP code and a high-level code, we also have the GKP code stabilizers and additional ones from the high-level code. Thus, we obtain the syndrome information of the GKP code completely analogously as in the proof in the previous section and we only need to prove that we are able to obtain the syndrome information of the high-level code. However, notice that our new stabilizer set does not contain GKP Pauli operators, which were needed in order to ensure that the information encoded in the GKP code is not corrupted. This looks like a big problem, but actually we do not care whether the information in single GKP codes is corrupted. We only want that the information encoded in the concatenation of the GKP and the high-level code remains unchanged. This is achieved by having (squeezed) logical Pauli operators of the high-level code instead of those for the low-level GKP codes in the stabilizer group.

Let us now prove that we are able to obtain the syndrome information of the high-level code. The stabilizers corresponding to the high-level code are given by (subscript l numbers independent stabilizer generators of the high-level qudit code)

$$\begin{aligned} & \exp\left(i\sum_{j=1}^n (\hat{u}_{j,1} - 2\pi\omega(e_1, u_j))H_{jl}^{\hat{u}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right), \\ & \exp\left(i\sum_{j=1}^n (\hat{v}_{j,1} - 2\pi\omega(e_1, v_j))H_{jl}^{\hat{v}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right), \\ & \exp\left(i\sum_{j=1}^n (\hat{u}_{j,2} - 2\pi\omega(e_2, u_j))H_{jl}^{\hat{u}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right), \\ & \exp\left(i\sum_{j=1}^n (\hat{v}_{j,2} - 2\pi\omega(e_2, v_j))H_{jl}^{\hat{v}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right). \end{aligned}$$

After applying the 50:50 beam splitter we obtain

$$\begin{aligned} & \exp\left(i\sum_{j=1}^n \left(\frac{\hat{u}_{j,1} + \hat{u}_{j,2}}{\sqrt{2}} - 2\pi\omega(e_1, u_j)\right)H_{jl}^{\hat{u}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right), \\ & \exp\left(i\sum_{j=1}^n \left(\frac{\hat{v}_{j,1} + \hat{v}_{j,2}}{\sqrt{2}} - 2\pi\omega(e_1, v_j)\right)H_{jl}^{\hat{v}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right), \\ & \exp\left(i\sum_{j=1}^n \left(\frac{\hat{u}_{j,1} - \hat{u}_{j,2}}{\sqrt{2}} - 2\pi\omega(e_2, u_j)\right)H_{jl}^{\hat{u}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right), \\ & \exp\left(i\sum_{j=1}^n \left(\frac{\hat{v}_{j,1} - \hat{v}_{j,2}}{\sqrt{2}} - 2\pi\omega(e_2, v_j)\right)H_{jl}^{\hat{v}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right). \end{aligned}$$

We then measure $\hat{v}_{j,2}$ which is constrained by stabilizer conditions

$$\exp\left(i\sum_{j=1}^n(\sqrt{2}\hat{v}_{j,2} - 2\pi\omega(e_1 - e_2, v_j))H_{jl}^{\hat{v}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right),$$

giving us partial information about the displacement errors. If we perform an ideal formal stabilizer measurement we would learn the stabilizer

$$\exp\left(i\sum_{j=1}^n(\hat{v}_{j,2} - 2\pi\omega(e_1, v_j))H_{jl}^{\hat{v}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right).$$

Thus, up to a bit of noise originating from the noisy ancilla and a rescaling by a factor of $\sqrt{2}$, both approaches give the same information about the displacement errors. The state after the measurement, considering the new ancilla, is then given by

$$\begin{aligned} & \exp\left(i\sum_{j=1}^n(\sqrt{2}\hat{u}_{j,1} - 2\pi\omega(e_1 + e_2, u_j))H_{jl}^{\hat{u}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right), \\ & \exp\left(i\sum_{j=1}^n\left(\frac{\hat{v}_{j,1} + \hat{v}_{j,2}}{\sqrt{2}} - 2\pi\omega(e_1, v_j)\right)H_{jl}^{\hat{v}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right), \\ & \exp\left(i\sum_{j=1}^n(\sqrt{2}\hat{u}_{j,3} - \sqrt{2}2\pi\omega(e_3, u_j))H_{jl}^{\hat{u}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right), \\ & \exp\left(i\sum_{j=1}^n\left(\frac{\hat{v}_{j,3}}{\sqrt{2}} - \frac{1}{\sqrt{2}}2\pi\omega(e_3, v_j)\right)H_{jl}^{\hat{v}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right). \end{aligned}$$

By applying a corresponding displacement shift as in the previous section, we can remove the phase depending on $\hat{v}_{j,2}$. After applying the second beam splitter we obtain

$$\begin{aligned} & \exp\left(i\sum_{j=1}^n(\hat{u}_{j,1} + \hat{u}_{j,3} - 2\pi\omega(e_1 + e_2, u_j))H_{jl}^{\hat{u}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right), \\ & \exp\left(i\sum_{j=1}^n\left(\frac{\hat{v}_{j,1} + \hat{v}_{j,3}}{2} - 2\pi\omega(e_1, v_j)\right)H_{jl}^{\hat{v}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right), \\ & \exp\left(i\sum_{j=1}^n(\hat{u}_{j,1} - \hat{u}_{j,3} - \sqrt{2}2\pi\omega(e_3, u_j))H_{jl}^{\hat{u}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right), \\ & \exp\left(i\sum_{j=1}^n\left(\frac{\hat{v}_{j,1} - \hat{v}_{j,3}}{2} - \frac{1}{\sqrt{2}}2\pi\omega(e_3, v_j)\right) \right. \\ & \left. \times H_{jl}^{\hat{v}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right). \end{aligned}$$

We then measure $\hat{u}_{j,3}$ where we obtain partial information about the displacement errors due to the stabilizer constraint:

$$\begin{aligned} & \exp\left(i\sum_{j=1}^n(2\hat{u}_{j,2} - 2\pi\omega(e_1 + e_2 - \sqrt{2}e_3, u_j)) \right. \\ & \left. \times H_{j,l}^{\hat{u}}\sqrt{\frac{1}{D\omega(u_j, v_j)}}\right). \end{aligned}$$

After the measurement the states are approximately (because of the small displacements on the ancillas) back to the code space and we have obtained the full syndrome information. The steps involving the logical Pauli operators showing that the logical information is not corrupted work completely analogously as in main text where we discuss the original Knill-Glancy scheme.

APPENDIX F: LINEAR OPTICS PRESERVES CODE DISTANCE

(Passive) Linear-optical operations acting on n modes are described by elements of the unitary group $U(n)$ acting on the mode operators. Using the two-out-of-three property (see p. 44 of Ref. [56]) of unitaries we see that $U(n) \cong O(2n) \cap Sp(2n)$. Therefore, the linear-optical operation is represented by an orthogonal and symplectic matrix in the $2n$ -dimensional phase space.

Let us consider a lattice $S \subset \mathbb{R}^{2n}$ where the symplectic form between any two lattice points yields an integer representing the commutation condition of stabilizer groups in the symplectic representation. This includes the case of general GKP codes and concatenations with higher-level stabilizer codes. Furthermore, we define the dual (with respect to the symplectic form) lattice $\mathcal{L}^\perp(S)$ as the set of points whose symplectic form yields an integer with every point of the lattice S . The code distance of the corresponding code is then defined as $\min_{\substack{u, v \in \mathcal{L}(S)/S \\ u \neq v}} \|u - v\|_2$ [57].

When we now apply a linear-optical transformation to the corresponding state, we have to transform our lattice by multiplying it by an orthogonal and symplectic matrix M . Therefore, the new lattice is given by MS , where the product is defined elementwise for every element of the group S . Since symplectic matrices do not change symplectic forms, it can be seen from the definition of the dual lattice that $M\mathcal{L}^\perp(S) \subseteq \mathcal{L}^\perp(MS)$. However, since M is invertible, we even have equality between both sets (for a proof first apply M and then M^{-1} and obtain a sequence of subsets where the left and right sides are the same). We now calculate the code distance after applying M and see that it is left invariant since unitaries do not change the norm:

$$\begin{aligned} \min_{\substack{u', v' \in \mathcal{L}(MS)/(MS) \\ u' \neq v'}} \|u' - v'\|_2 &= \min_{\substack{u, v \in \mathcal{L}(S)/S \\ u \neq v}} \|M(u - v)\|_2 \\ &= \min_{\substack{u, v \in \mathcal{L}(S)/S \\ u \neq v}} \|u - v\|_2. \end{aligned}$$

Thus, linear-optical transformations preserve the code distance of general GKP codes and we cannot hope to find a linear-optical circuit transforming independent GKP codes into a high-level concatenated GKP code. However, it might still be possible that some codewords of the high-level code can be generated easily by individual GKP-like states and linear optics. One application of this possible loophole is the generation of the ancilla states that we need for our error-correction schemes.

Furthermore, it is also easy to see that two general quantum error-correcting codes (not necessarily GKP codes) which are equivalent up to some linear-optical transformation have

the same error-correcting properties against isotropic displacement error channels (e.g., i.i.d. Gaussian displacements). Instead of transforming the codes we can transform the noise channel accordingly. However, the isotropic displacement error channel is left invariant by the linear-optical transformation, because the probability distribution of the isotropic displacement noise channel only depends on the 2-norm of the displacement vector. This norm is preserved by the transformation as it acts as an orthogonal matrix in the phase-space representation. As a consequence, the error-correcting properties of these two codes are the same against isotropic displacement error channels.

APPENDIX G: EXACT CALCULATION OF ANALOG INFORMATION IN THE THREE-QUBIT REPETITION CODE

When using a minimum-weight decoding scheme, we are applying a correction shift of minimum weight such that we recover the code space; i.e., the combination of the error and correction shift is an element of the dual lattice \mathcal{L}^\perp . Since the three-qubit repetition code is a CSS code, we can correct position and momentum shifts independently, reducing the dimensionality of the computational problem by a factor of 2. Here we will also only discuss the position shifts as the momentum stabilizers are those of independent square-lattice GKP qubits. The stabilizer generators and representatives of logical operators of the code are given by

$$\begin{aligned} & \exp[i\sqrt{\pi}(\hat{q}_1 - \hat{q}_2)], & \exp[i\sqrt{\pi}(\hat{q}_2 - \hat{q}_3)], \\ & \exp(i2\sqrt{\pi}\hat{q}_3), & \exp(i2\sqrt{\pi}\hat{p}_1), \\ & \exp(i2\sqrt{\pi}\hat{p}_2), & \exp(i2\sqrt{\pi}\hat{p}_3), \\ & \bar{X} = \exp[i\sqrt{\pi}(\hat{p}_1 + \hat{p}_2 + \hat{p}_3)], \\ & \bar{Z} = \exp(i\sqrt{\pi}\hat{q}_1). \end{aligned}$$

We can then decompose $\mathcal{L}^\perp = \mathcal{L}_\perp^\perp \cup \mathcal{L}_\times^\perp$, corresponding to the represented operator \bar{X} . In order to obtain the set of correctable errors we have to calculate the Voronoi cells, where each cell consists of all points being closest to a given lattice point, of \mathcal{L}^\perp and consider the union of all Voronoi cells including a point in \mathcal{L}_\perp^\perp . This can easily be done by generating a finite-size lattice and using the SCIPY function `scipy.spatial.Voronoi` for calculating the Voronoi cells. Using the translation invariance of the actual lattice we can then obtain all Voronoi cells by applying it to cells which are not distorted due to finite-size effects.

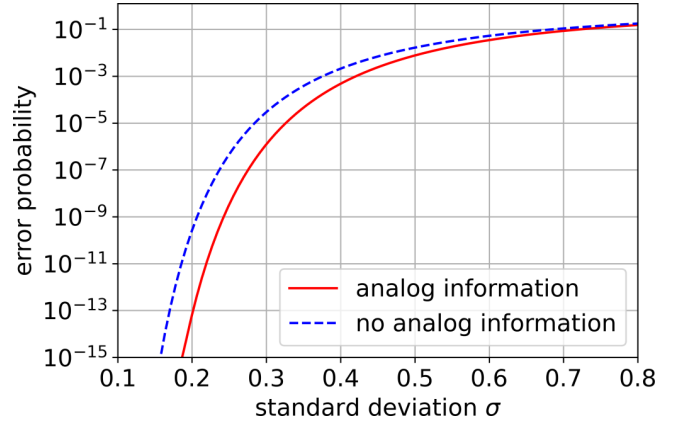


FIG. 4. Logical bit-flip error rate of square GKP code concatenated with the three-qubit bit-flip code using our exact calculation. Our results are in good agreement with Fig. 2 of Ref. [6], where the results were obtained by a Monte Carlo simulation. However, due to the simple numerical integration we are able to calculate small error rates where a Monte Carlo approach would be infeasible.

Since we consider a three-dimensional (3D) lattice this can be visualized nicely and one sees that the correctable set of errors is given by a union of octagons where the elementary octagon is given by the convex span of the points $(\pm\frac{3\sqrt{\pi}}{2}, 0, 0)$, $(0, \pm\frac{3\sqrt{\pi}}{2}, 0)$, $(0, 0, \pm\frac{3\sqrt{\pi}}{2})$ and the other ones can be obtained by translations of $2\sqrt{\pi}(\mathbb{Z}, \mathbb{Z}, \mathbb{Z})$.

In order to obtain the probability of no bit-flip error we have to integrate the probability distribution of displacement errors over the set of correctable errors. The overall set of correctable errors is too complicated for integration and therefore we integrate over a subset of octagons and obtain lower bounds on the probability of success (when considering the union we must not count some areas twice).

Let us now consider the most common case of i.i.d. Gaussian noise with a variance of σ^2 . For the elementary octagon (and all others which are only displaced along one axis) we can split the octagon into two pyramids and consider new rotated integration variables, such that the base of the pyramid is aligned with the integration axes. This way we can do these integrations analytically and we are only left with the integral $\frac{2}{\sqrt{2\pi\sigma^2}} \int_0^{\frac{3\sqrt{\pi}}{2}} \exp(-\frac{z^2}{2\sigma^2}) \text{erf}((\frac{3\sqrt{\pi}}{2} - z)\frac{1}{2\sigma})^2 dz$ for the probability of no bit-flip error which then can be calculated numerically. The results of this calculation are shown in Fig. 4 and compared with the case where we do not make use of the analog GKP syndrome information.

-
- [1] P. T. Cochrane, G. J. Milburn, and W. J. Munro, Macroscopically distinct quantum-superposition states as a bosonic code for amplitude damping, *Phys. Rev. A* **59**, 2631 (1999).
 [2] D. Gottesman, A. Kitaev, and J. Preskill, Encoding a qubit in an oscillator, *Phys. Rev. A* **64**, 012310 (2001).
 [3] N. Ofek, A. Petrenko, R. Heeres, P. Reinhold, Z. Leghtas, B. Vlastakis, Y. Liu, L. Frunzio, S. M. Girvin, L. Jiang, M. Mirrahimi, M. H. Devoret, and R. J. Schoelkopf, Extending the

- lifetime of a quantum bit with error correction in superconducting circuits, *Nature (London)* **536**, 441 (2016).
 [4] C. Flühmann, T. L. Nguyen, M. Marinelli, V. Negnevitsky, K. Mehta, and J. P. Home, Encoding a qubit in a trapped-ion mechanical oscillator, *Nature (London)* **566**, 513 (2019).
 [5] P. Campagne-Ibarcq, A. Eickbusch, S. Touzard, E. Zalys-Geller, N. E. Frattini, V. V. Sivak, P. Reinhold, S. Puri, S. Shankar, R. J. Schoelkopf, L. Frunzio, M. Mirrahimi, and

- M. H. Devoret, Quantum error correction of a qubit encoded in grid states of an oscillator, *Nature (London)* **584**, 368 (2020).
- [6] K. Fukui, A. Tomita, and A. Okamoto, Analog Quantum Error Correction with Encoding a Qubit into an Oscillator, *Phys. Rev. Lett.* **119**, 180507 (2017).
- [7] K. Noh and C. Chamberland, Fault-tolerant bosonic quantum error correction with the surface–Gottesman–Kitaev–Preskill code, *Phys. Rev. A* **101**, 012316 (2020).
- [8] C. Vuillot, H. Asasi, Y. Wang, L. P. Pryadko, and B. M. Terhal, Quantum error correction with the toric Gottesman–Kitaev–Preskill code, *Phys. Rev. A* **99**, 032344 (2019).
- [9] K. Fukui, A. Tomita, A. Okamoto, and K. Fujii, High-Threshold Fault-Tolerant Quantum Computation with Analog Quantum Error Correction, *Phys. Rev. X* **8**, 021054 (2018).
- [10] L. Hänggeli, M. Heinze, and R. König, Enhanced noise resilience of the surface–Gottesman–Kitaev–Preskill code via designed bias, *Phys. Rev. A* **102**, 052408 (2020).
- [11] K. Noh, V. V. Albert, and L. Jiang, Quantum capacity bounds of Gaussian thermal loss channels and achievable rates with Gottesman–Kitaev–Preskill codes, *IEEE Trans. Inf. Theory* **65**, 2563 (2019).
- [12] K. Fukui, R. N. Alexander, and P. van Loock, All-optical long-distance quantum communication with Gottesman–Kitaev–Preskill qubits, *Phys. Rev. Research* **3**, 033118 (2021).
- [13] F. Rozpędek, K. Noh, Q. Xu, S. Guha, and L. Jiang, Quantum repeaters based on concatenated bosonic and discrete-variable quantum codes, *npj Quantum Inf.* **7**, 102 (2021).
- [14] N. C. Menicucci, Fault-Tolerant Measurement-Based Quantum Computing with Continuous-Variable Cluster States, *Phys. Rev. Lett.* **112**, 120504 (2014).
- [15] I. Tzitrin, T. Matsuura, R. N. Alexander, G. Dauphinais, J. E. Bourassa, K. K. Sabapathy, N. C. Menicucci, and I. Dhand, Fault-tolerant quantum computation with static linear optics, *PRX Quantum* **2**, 040353 (2021).
- [16] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, Cambridge, UK, 2010).
- [17] V. Gheorghiu, Standard form of qudit stabilizer groups, *Phys. Lett. A* **378**, 505 (2014).
- [18] M. Horodecki and P. Horodecki, Reduction criterion of separability and limits for a class of distillation protocols, *Phys. Rev. A* **59**, 4206 (1999).
- [19] D. Kaszlikowski, P. Gnaniński, M. Żukowski, W. Miklaszewski, and A. Zeilinger, Violations of Local Realism by Two Entangled N -Dimensional Systems are Stronger than for Two Qubits, *Phys. Rev. Lett.* **85**, 4418 (2000).
- [20] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Bell Inequalities for Arbitrarily High-Dimensional Systems, *Phys. Rev. Lett.* **88**, 040404 (2002).
- [21] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of Quantum Key Distribution Using d -Level Systems, *Phys. Rev. Lett.* **88**, 127902 (2002).
- [22] D. Aharonov and M. Ben-Or, Fault-tolerant quantum computation with constant error rate, *SIAM J. Comput.* **38**, 1207 (2008).
- [23] We denote this continuous Weyl–Heisenberg group simply as a Weyl–Heisenberg group, while we refer to the discrete Weyl–Heisenberg group as a Pauli group.
- [24] Every point in the lattice corresponds to a member of the stabilizer group. However, we defined the stabilizer group by products of stabilizer generators and when converting the product into a single Weyl–Heisenberg operator by using the Baker–Campbell–Hausdorff formula a phase of ± 1 can appear. This sign ambiguity, however, does not affect our results.
- [25] For a given noise channel increasing the code dimension D of the GKP code also increases the error rate and it is a nontrivial task to evaluate whether the increased noise robustness and higher code dimension can compensate the higher error rates on the physical qudit level. The present work only addresses improved techniques for obtaining the syndrome information, and an evaluation of the concatenation of GKP codes with actual qudit codes is left for future research.
- [26] T. Matsuura, H. Yamasaki, and M. Koashi, Equivalence of approximate Gottesman–Kitaev–Preskill codes, *Phys. Rev. A* **102**, 032408 (2020).
- [27] Y. Wang, Quantum error correction with the GKP code and concatenation with stabilizer codes, [arXiv:1908.00147](https://arxiv.org/abs/1908.00147).
- [28] J. Conrad, Twirling and Hamiltonian engineering via dynamical decoupling for Gottesman–Kitaev–Preskill quantum computing, *Phys. Rev. A* **103**, 022404 (2021).
- [29] B. Q. Baragiola, G. Pantaleoni, R. N. Alexander, A. Karanjai, and N. C. Menicucci, All-Gaussian Universality and Fault Tolerance with the Gottesman–Kitaev–Preskill Code, *Phys. Rev. Lett.* **123**, 200502 (2019).
- [30] S. D. Bartlett, B. C. Sanders, S. L. Braunstein, and K. Nemoto, Efficient Classical Simulation of Continuous Variable Quantum Information Processes, *Phys. Rev. Lett.* **88**, 097904 (2002).
- [31] A. M. Steane, Active Stabilization, Quantum Computation, and Quantum State Synthesis, *Phys. Rev. Lett.* **78**, 2252 (1997).
- [32] E. Knill, Scalable quantum computing in the presence of large detected-error rates, *Phys. Rev. A* **71**, 042322 (2005).
- [33] S. Glancy and E. Knill, Error analysis for encoding a qubit in an oscillator, *Phys. Rev. A* **73**, 012325 (2006).
- [34] K. H. Wan, A. Neville, and S. Kolthammer, Memory-assisted decoder for approximate Gottesman–Kitaev–Preskill codes, *Phys. Rev. Research* **2**, 043280 (2020).
- [35] I. Tzitrin, J. E. Bourassa, N. C. Menicucci, and K. K. Sabapathy, Progress towards practical qubit computation using approximate Gottesman–Kitaev–Preskill codes, *Phys. Rev. A* **101**, 032315 (2020).
- [36] B. W. Walshe, B. Q. Baragiola, R. N. Alexander, and N. C. Menicucci, Continuous-variable gate teleportation and bosonic-code error correction, *Phys. Rev. A* **102**, 062411 (2020).
- [37] H. Vahlbruch, M. Mehmet, K. Danzmann, and R. Schnabel, Detection of 15 dB Squeezed States of Light and their Application for the Absolute Calibration of Photoelectric Quantum Efficiency, *Phys. Rev. Lett.* **117**, 110801 (2016).
- [38] R. Filip, P. Marek, and U. L. Andersen, Measurement-induced continuous-variable quantum interactions, *Phys. Rev. A* **71**, 042308 (2005).
- [39] J.-i. Yoshikawa, Y. Miwa, A. Huck, U. L. Andersen, P. van Loock, and A. Furusawa, Demonstration of a Quantum Nondemolition Sum Gate, *Phys. Rev. Lett.* **101**, 250501 (2008).
- [40] In Ref. [6] the authors proposed to measure the stabilizers $\exp(i\sqrt{\pi}(\hat{q}_1 + \hat{q}_2))$, $\exp(i\sqrt{\pi}(\hat{q}_2 + \hat{q}_3))$, $\exp(i2\sqrt{\pi}\hat{q}_3)$.
- [41] Even for nonprime D there are no additional stabilizers needed.
- [42] K. Chandrasekaran, V. Gandikota, and E. Grigorescu, Deciding orthogonality in construction-A lattices, *SIAM J. Discrete Math.* **31**, 1244 (2017).

- [43] B. Royer, S. Singh, and S. M. Girvin, Stabilization of Finite-Energy Gottesman-Kitaev-Preskill States, *Phys. Rev. Lett.* **125**, 260509 (2020).
- [44] This expression differs by a factor of -1 from Eq. (14) in Ref. [33] as we use a beam splitter with different phases.
- [45] L. G. Gunderman, Local-dimension-invariant qudit stabilizer codes, *Phys. Rev. A* **101**, 052343 (2020).
- [46] J. Blömer and J.-P. Seifert, On the complexity of computing short linearly independent vectors and short bases in a lattice, in *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing, STOC '99* (Association for Computing Machinery, New York, 1999), pp. 711–720.
- [47] T. C. Ralph, A. J. F. Hayes, and A. Gilchrist, Loss-Tolerant Optical Qubits, *Phys. Rev. Lett.* **95**, 100501 (2005).
- [48] N. P. Breuckmann, C. Vuillot, E. Campbell, A. Krishna, and B. M. Terhal, Hyperbolic and semi-hyperbolic surface codes for quantum storage, *Quantum Sci. Technol.* **2**, 035007 (2017).
- [49] S. S. Bullock and G. K. Brennen, Qudit surface codes and gauge theory with finite cyclic groups, *J. Phys. A: Math. Theor.* **40**, 3481 (2007).
- [50] H. Bombin and M. A. Martin-Delgado, Homological error correction: Classical and quantum codes, *J. Math. Phys.* **48**, 052105 (2007).
- [51] P. Sarvepalli, Topological color codes over higher alphabet, in *2010 IEEE Information Theory Workshop* (IEEE, Piscataway, NJ, 2010), pp. 1–5.
- [52] F. H. E. Watson, E. T. Campbell, H. Anwar, and D. E. Browne, Qudit color codes and gauge color codes in all spatial dimensions, *Phys. Rev. A* **92**, 022312 (2015).
- [53] P. Shor, Fault-tolerant quantum computation, in *Proceedings of 37th Conference on Foundations of Computer Science* (IEEE, Piscataway, NJ, 1996), pp. 56–65.
- [54] J. Conrad, J. Eisert, and F. Arzani, Gottesman-Kitaev-Preskill codes: A lattice perspective, *Quantum* **6**, 648 (2022).
- [55] A. Basu, Lectures on modern approaches to cutting planes, https://www.ams.jhu.edu/~abasu9/RFG/lecture_notes.pdf.
- [56] D. McDuff and D. Salamon, *Introduction to Symplectic Topology*, Oxford Mathematical Monographs (Oxford University Press, Oxford, UK, 2017).
- [57] We consider the 2-norm because for Gaussian noise the probability density only depends on the 2-norm of the symplectic error representation.

Paper IV

Exact rate analysis for quantum repeaters with imperfect memories and entanglement swapping as soon as possible

Lars Kamin, Evgeny Shchukin, Frank Schmidt, and Peter van Loock,

Phys. Rev. Research **5**, 023086 (2023)

Exact rate analysis for quantum repeaters with imperfect memories and entanglement swapping as soon as possible

Lars Kamin^{⊗,*}, Evgeny Shchukin^{⊗,†}, Frank Schmidt^{⊗,‡} and Peter van Loock[§]

Johannes-Gutenberg University of Mainz, Institute of Physics, Staudingerweg 7, 55128 Mainz, Germany



(Received 30 May 2022; revised 31 January 2023; accepted 3 February 2023; published 10 May 2023)

We present an exact rate analysis for a secret key that can be shared among two parties employing a linear quantum repeater chain. One of our main motivations is to address the question whether simply placing quantum memories along a quantum communication channel can be beneficial in a realistic setting. The underlying model assumes deterministic entanglement swapping of single-spin quantum memories and it excludes probabilistic entanglement distillation, and thus two-way classical communication, on higher nesting levels. Within this framework, we identify the essential properties of any optimal repeater scheme: entanglement distribution in parallel, entanglement swapping as soon and parallel quantum storage as little as possible. While these features are obvious or trivial for the simplest repeater with one middle station, for more stations they cannot always be combined. We propose an optimal scheme including channel loss and memory dephasing, proving its optimality for the case of two stations and conjecturing it for the general case. In an even more realistic setting, we consider additional tools and parameters such as memory cutoffs, multiplexing, initial state and swapping gate fidelities, and finite link coupling efficiencies in order to identify potential regimes in memory-assisted quantum key distribution beyond one middle station that exceed the rates of the smallest quantum repeaters as well as those obtainable in all-optical schemes unassisted by stationary memory qubits and two-way classical communication. Our analytical treatment enables us to determine simultaneous trade-offs between various parameters, their scaling, and their influence on the performance ordering among different types of protocols, comparing two-photon interference after dual-rail qubit transmission with one-photon interference of single-rail qubits or, similarly, optical interference of coherent states. We find that for experimental parameter values that are highly demanding but not impossible (up to 10 s coherence time, about 80% link coupling, and state or gate infidelities in the regime of 1%–2%), one secret bit can be shared per second at a total channel loss budget of 157.6 dB, i.e. a total distance of 800 km for a fiber attenuation length of 22 km with repeater stations placed at every 100 km—a clear improvement over realistic twin-field or, much more pronouncedly, ideal point-to-point quantum key distribution at GHz clock rates.

DOI: [10.1103/PhysRevResearch.5.023086](https://doi.org/10.1103/PhysRevResearch.5.023086)

I. INTRODUCTION

Recent progress on quantum computers with tens of qubits led to experimental demonstrations of quantum devices able to solve specifically adapted problems not efficiently soluble with the help of classical computers alone. Typically, these devices are based on solid-state (superconducting) systems [1,2], however, there are also photonics approaches [3]. While these schemes still have to be enhanced in terms of size, i.e., the number of qubits (scalability), their error robustness and corresponding logical encoding (fault tolerance), as well as their range of applicability (eventually reaching universality), this progress represents a threat to common classical

communication systems. Eventually, this may compromise current key distribution protocols. Although there are recent developments in classical cryptography to address the threat imposed by such quantum devices (“postquantum cryptography”), quantum mechanics also gives a possible solution to this by means of quantum key distribution (QKD) [4,5]. Many QKD protocols have been proposed such as the most prominent, so-called BB84 scheme [6]. Among the various quantum technologies that promise to enable their users to fulfill tasks impossible without quantum resources, quantum communication is special. Unlike quantum computers there are already commercially available quantum communication systems intended for costumers who wish to communicate in the classical, real world in a basically unconditionally secure fashion—independent of mathematically unproven assumptions exploiting the concept of QKD. QKD systems are naturally realized for photonic systems using nonclassical optical quantum states such as single-photon, weak [7,8], or even bright coherent states [5].

Current point-to-point QKD systems, directly connecting the sender (Alice) and the receiver (Bob) via an optical-fiber channel, are limited in distance due to the exponentially growing transmission loss along the channel. Typical maximal

*lars.kamin@outlook.com

†evgeny.shchukin@gmail.com

‡scfrank@uni-mainz.de

§loock@uni-mainz.de

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article’s title, journal citation, and DOI.

distances are 100–200 km. A very recent QKD variant, so-called twin-field (TF) QKD [9], allows to push these limits farther (basically doubling the effective distance) by placing an (untrusted) middle station between Alice and Bob. Remarkably, TF QKD achieves this loss scaling advantage in an all-optical fashion with no need for quantum storage at the middle station and at an, in principle, unlimited clock rate with no need for two-way classical communication. It further inherits the improved security features of measurement-device-independent (MDI) QKD schemes [10,11]. However, the original TF QKD concept is not known to be further scalable beyond the effective distance doubling.

A. Quantum repeaters: Previous works

In classical communication, the distance problem is straightforwardly overcome by introducing repeater stations along the fiber channel (about every 50–100 km) in order to reamplify (and typically reshape) the optical pulses. On a fundamental level, the famous No-Cloning-theorem [12,13], prohibits such solutions for quantum communication. As a possible remedy, the concept of quantum repeaters has been developed [14–16]. With the help of sufficiently short-range entanglement distributions, quantum memories, entanglement distillation and swapping, in principle, scalable long-distance, fiber-based quantum communication becomes possible, including long-range QKD. While this original quantum repeater concept would still impose high experimental requirements on the various implementation platforms [17–21], these first proposals made a possible realization of a large-scale quantum repeater more likely. Nonetheless, even when completely implemented, such schemes would still be fundamentally limited in their achievable (secret) key rates per second. The reason for this is the need for two-way classical communication on all, including the highest “nesting” levels in order to conduct entanglement distillation and confirm successful entanglement swappings when these are probabilistic. Today this type of quantum repeater schemes are referred to as first-generation quantum repeaters. Alternative schemes circumventing the fundamental limitations are the so-called second- and third-generation quantum repeaters that exploit quantum error correction codes to suppress the effect of memory (and gate) errors or channel loss (and gate errors), respectively [22].

It is important to stress that all these quantum repeaters are designed to allow for a genuine long-distance quantum state transfer. In the QKD context, this means that the intermediate stations along the repeater channel may be untrusted. If instead sufficiently many trusted stations can be placed along the channel between Alice and Bob, and the quantum signals can be converted into classical information at each station (as a whole, effectively corresponding to classically connected, independent, sufficiently short-range QKD links), large-scale QKD is already possible and being demonstrated [23]. Conceptually, this also applies to long-range links enabled by satellites [24,25]. It is only the genuine quantum repeater that incorporates two main features at the same time: *long-distance scalability and long-distance privacy*.

From a practical point of view, it is expected that global quantum communication systems will be a combination of

both elements: genuine fiber-based quantum repeaters over intermediate distances (thousands of kilometers) and satellite-based quantum links bridging even longer distances (tens of thousands of kilometers; the earth’s circumference is about 40 000 km). While such truly global quantum communication may eventually lead to some form of a “quantum internet” [26], only the coherent long-distance quantum state transfer as enabled by a genuine quantum repeater allows to consider applications that go beyond long-range QKD. In fact, the original quantum repeater proposals were not specifically intended for or adapted to long-range QKD. They can be used for any application that relies upon the distribution of entangled states over large distances including large-scale quantum networks. Obvious applications are distributed quantum tasks such as distributed quantum computing, coherently connecting quantum computers which are spatially far apart. These ultimate long-distance quantum communication applications will then impose much higher demands on the fault tolerance of the experimental quantum states and gates. In particular, QKD-specific classical postprocessing will no longer be applicable. In this work, we shall consider small to intermediate-scale quantum repeaters that allow to do QKD or coherently connect quantum nodes at a corresponding size and at a reasonably practical clock rate.

B. Quantum repeaters: Present work

In this work, we will focus on small-scale or medium-size quantum repeater systems beyond a single middle station and without probabilistic entanglement distillation on higher “nesting levels.” This class of quantum repeaters is of great interest for at least two reasons.

(i) There are now first experiments of memory-enhanced quantum communication basically demonstrating memory-assisted MDI QKD [27,28]. Therefore the natural next step for the experimentalists will be to connect such elementary modules to obtain larger repeater systems with *two or more intermediate stations*, thus bridging larger distances and, unlike memory-assisted MDI QKD, ultimately relying upon classical communication between the repeater stations [29].

These next near-term experiments will aim at a distance extension still independent of additional and more complicated schemes such as entanglement distillation on “higher nesting levels.” Restricting the entanglement manipulations to the level of the elementary repeater segments will also help to avoid the use of long-distance two-way classical signalling like in a fully scalable first-generation quantum repeater, and hence allow for still limited but reasonable repeater clock rates. In this regime, comparing (secret key) rates per second of the quantum repeaters with those of an (ideal) point-to-point link or TF QKD scheme is in some way most fair and meaningful.

While the current experimental repeater demonstrations with a single repeater station [27,28] would still suffer from too low clock rates and link coupling efficiencies before giving a practical repeater advantage, an urgent theoretical question is whether, under practical realistic circumstances, it really helps to place memory stations along a quantum communication channel and execute memory-assisted QKD without extra active quantum error correction. In principle,

placing a middle station between Alice and Bob allows to gain a repeater advantage per channel use [29–31].

Omitting the nonscalable all-optical TF approach, is there a practical benefit also in terms of secret bits per second when using a two-segment quantum repeater? Moreover, and this is the focus of the present work, is there even a further advantage when adding more stations beyond a single middle station under realistic assumptions and with no extra quantum error correction? We will see that for up to eight repeater segments, covering distances up to around 800 km, the quantum repeaters treated in this work, assuming experimental parameter values that are demanding but not impossible to achieve in practice, can exceed the performance limits of the other schemes. For larger distances, the attainable absolute rates of point-to-point quantum communication become extremely small. However, for quantum repeaters, additional elements of quantum error correction will be needed, as otherwise the final rates would vanish and no gain can be expected over point-to-point communication.

(ii) The second point refers to the theoretical treatment. Typically, the repeater rates can be calculated either numerically including many protocol variations and (experimental) degrees of freedom [32] or approximately in certain regimes [18] (there are also semi-analytical approaches, see Refs. [33,34]).

If errors are neglected an exact and even optimized raw rate calculation is possible even for nonunit (but constant) entanglement swapping probabilities using the formalism of Markov chains and decision processes [35,36] (see also Refs. [37,38]). This approach works well for repeaters up to about ten segments; for too many repeater segments the resulting linear equation systems become intractable. Nonetheless, for the smallest repeaters with only a single middle station, it was shown how to calculate secret key rates even including various experimental parameters, though partially also employing approximations for the raw rates [30,31]. In this work we will go beyond the case of a single middle station and present exact calculations of *secret key rates obtainable with realistic small and intermediate-scale quantum repeaters*. The theoretical difficulty here is, even already when only channel loss and memory dephasing is considered, that for repeaters beyond a single middle station there are various distribution and swapping strategies and so it becomes nontrivial to determine the optimal ones. The usual treatment in this case is based upon the so-called doubling strategy where for a repeater with a power-of-two number of segments only certain pairs of segments will be connected in order to double the distances at each repeater level. As a consequence, sometimes entanglement connections will be postponed even though neighboring pairs may be ready already, thus unnecessarily accumulating more memory dephasing errors. With regards to memory dephasing, the best strategy appears to be *to swap as soon as possible* and here we will show how this type of repeater strategy can be exactly and analytically treated. This element is the crucial step that enables us to propose optimal quantum repeater schemes.

On the hardware side, memory-based quantum repeaters require sufficiently long-lived quantum memories and efficient, typically light-matter-based interfaces converting flying into stationary qubits. In the context of our theoretical treat-

ment, the stationary qubits are assumed to be represented by single spins in a suitable solid-state quantum node such as color (NV or SiV) centers in diamond, usually separately treated as short-lived electronic and long-lived nuclear spins [39,40]. As for efficient quantum emitters and short-lived quantum memories semiconductor quantum dots may be considered too [29]. Alternatively, various types of atom or ion qubits could be taken into account [29].

While all these different hardware platforms have their own assets and disadvantages (e.g., the required temperatures which range from room or modestly low temperatures for atoms/ions/NV to cryogenic temperatures for NV/SiV/quantum dots), and every one eventually requires a specifically adapted physical model, to a certain extent the quantum repeater performance based on these elements and assuming only a single repeater station can be assessed (or at least qualitatively bounded from above) using a fairly simple physical model that includes *three experimental parameters*: the link coupling efficiency, the memory coherence time, and the experimental clock rate [29].

In order to incorporate an appropriate experimental memory coherence time into the model, qubit dephasing errors can be considered where the stationary qubit is never lost but subject to random phase flips with a probability exponentially growing with the storage time. Already this rather simple model is theoretically nontrivial, because it leads to two distinct impacts on the final secret key rates. On the one hand, a finite link coupling efficiency (including all constant inefficiencies per segment from the sources, detectors, and interfaces) and a segment-length-dependent transmission efficiency affect the raw rate of the qubit transmission (which, if expressed as rate per second, also directly depends on the repeater clock rate). Thereby, in logarithmic rate-versus-distance plots (like those frequently shown later in this paper), a finite link coupling leads to an offset towards smaller rates at zero distance, while a finite channel transmission results in a certain (negative) slope. On the other hand, a finite memory coherence time influences the final Alice-Bob state fidelity or QKD error rate (which also indirectly depends on the repeater clock rate, i.e., the time duration per entanglement distribution attempt per segment, determining the possible number of distribution attempts within a given memory coherence time). This becomes manifest as an increase of the (negative) slope for growing distances, moving from an initially repeaterlike slope towards one corresponding to a point-to-point transmission.

There are interesting concepts to suppress this latter effect by introducing more sophisticated memory models such as (spatial or temporal) memory buffers or cutoffs. Especially a memory cutoff [41] has turned out to be useful without the need for additional experimental resources. It means that a maximal storage time is imposed at every memory node and any loaded stationary qubits waiting for a longer duration will be reinitialized. As a result, state fidelities can be kept high at the expense of a decreasing raw rate due to the frequently occurring reinitializations (which implies that a memory cutoff must neither be set too low nor too high). Theoretically, including memory cutoffs into the rate analysis significantly increases the complexity (becoming manifest in, e.g., quickly growing Markov-chain matrices) [35].

For small quantum repeaters, especially those with only one middle station, a secret key rate analysis remains possible [29,31]. For larger quantum repeaters, the effective rates may be calculated via recursively obtained expressions [42], via different kinds of approximations and assumptions [43] or with the help of numerical simulations [32]. Nonetheless, in our treatment, we shall explicitly include a memory cutoff in some protocols allowing us to extrapolate its positive impact on other schemes.

We choose to incorporate random dephasing as the dominating source of memory errors. While memory dephasing is generally an error to be taken into account, it is particularly important for those stationary qubits encoded into single solid-state spins, e.g., for color centers or quantum dots [29]. We omit (time-dependent) memory decay (loss) which additionally becomes relevant for atomic memories, either as collective spin modes of atomic ensembles or in the form of an individual atom in a cavity (generally, atoms and trapped ions may be subject to both dephasing and decay) [17,21,28,44]. It turns out that the effect of memory dephasing can be accurately included into the statistical repeater model, since the total, accumulated dephasing in the final Alice-Bob density operator follows a simple sum rule [45]. Thus, the statistical averaging can be applied to the final state, for which we derive a recursive formula that also includes depolarizing errors from the initially distributed states and from the imperfect Bell measurement gates in every entanglement swapping operation. The main complication will be to determine the correct dephasing variables for the different swapping strategies and identify the optimal schemes. As a result, we extend the simple model of Ref. [29] not only with regards to the repeater's size, but also to include additional experimental parameters: *besides the above three parameters we then have one or two extra parameters for the initially distributed states* (taking into account initial dephasing or depolarization errors depending on the protocol) *and one extra depolarization parameter for the local gates and Bell measurements*.

Our analytical treatment enables us to identify the scaling of the various parameters, their specific impact onto the repeater performance (for QKD, affecting either the raw rate or the error-dependent secret key fraction), and the resulting trade-offs. Most apparent is the trade-off for quantum repeaters with n segments and $n - 1$ intermediate memory stations leading to an improved loss scaling with an n -times bigger effective attenuation distance compared with a point-to-point link ($n = 1$), but a final state fidelity parameter decreasing as the power of $2n - 1$ (assuming equal gate and initial state error rates). We will then be able to consider repeater protocol variations with an improved scaling of the basic loss and fidelity parameters. Based upon the above-mentioned TF concept with coherent states or basically replacing two-photon by one-photon interferences at the beam splitter stations, these repeaters exhibit a $2n$ -times bigger effective attenuation distance while keeping the $2n - 1$ power scaling of the final state fidelity parameter for $n - 1$ memory stations [45]. However, they are subject to some extra intrinsic (dephasing) errors even when only channel loss is considered, which will turn out to be an essential complication that prevents to fully exploit the improved scaling of the basic parameters in comparison with the

standard repeater protocols that do not suffer from intrinsic dephasing.

Comparing different repeater protocols and incorporating the optimized memory dephasing from our statistical model into them, we find that for experimental parameter values that are highly demanding but not impossible (up to 10 s coherence time, 80% link coupling, and state or gate infidelities in the regime of 1%–2%), one secret bit can be shared per second over a total distance of 800 km. This represents a significant improvement over ideal point-to-point or realistic TF QKD at GHz clock rates. In particular, the repeaterless, point-to-point bound [46], for, e.g., 800 km is 3×10^{-16} bits per channel use or 0.3 μ bits per second (at GHz clock rate).¹ We will see that, in order to clearly beat this with those reasonable experimental parameters from above, the number of repeater stations must neither be too high nor too low, and so placing a station at every 100 km will work well.

As mentioned before, our schemes are generally independent of the typically used doubling strategies in quantum repeaters (which are most suitable to incorporate entanglement distillation in a systematic way and which are included as a special case in our sets of swapping strategies). Instead we will consider general memory-assisted entanglement distribution with possible QKD applications. Compatible with our analysis are also schemes that aim at an enhanced initial state distribution efficiency or fidelity as, for example, in multiplexing-assisted or the above-mentioned second-generation quantum repeaters. In any case, the subsequent steps after the initial distributions in each repeater segment are simple entanglement swapping steps combined with quantum storage in single spins. For the entanglement swapping we assume unit success probability. This assumption is experimentally justified for systems where Bell measurements or, more generally, (entangling) gates can be performed in a

¹The most recent TF QKD experiments achieve remarkably large distances in the range between 509 and 833 km [64–67]. Especially the most recent demonstration of Ref. [67] over 833 km is a strong statement in favour of the TF QKD approach. However, it is important to notice that low-loss fibers were employed in that demonstration corresponding to $L_{\text{att}} = 25.747$ km, 0.168 dB/km, or a tolerated total loss budget of 140 dB/833.8 km. This loss budget, if ultra-low-loss fibers were used corresponding to $L_{\text{att}} = 30.606$ km or 0.1419 dB/km, would even allow to reach distances near 1000 km. Nonetheless, in our theoretical rate analysis, we assume standard fiber transmission throughout, corresponding to $L_{\text{att}} = 22$ km or 0.197 dB/km. For these values, ideal TF QKD achieves about 1 secret bit per second over 800 km (this is a bound which is also related to the one-way distillable entanglement) [22,68]. Any realistic TF QKD experiment over such distances will certainly perform worse than this ideal bound or, in other words, for a ultra-low-loss fiber transmission also the ideal TF QKD rate would move up, e.g., for $L_{\text{att}} = 30$ km, to a value as high as about 100 secret bits per second for 800 km. The results of the experiment of Ref. [67], of course, are also clearly below the ideal TF QKD bound when compared with identical fiber transmission parameters. Our optimized quantum repeater that achieves 1 secret bit per second over 800 km would correspond to a scheme that tolerates a total channel loss budget of 157.6 dB. With improved, low-loss fiber channels, this loss budget would also allow us to go to much larger distances beyond 1000 km.

deterministic fashion, for instance, with atoms or ions or solid-state-based spin qubits [29]. For a linear quantum repeater chain, this system is still remarkably complex.

The assumption of deterministic entanglement swapping will allow us to calculate the exact (secret key) rates in a quantum repeater up to eight segments. We will distinguish schemes with sequential and parallel entanglement distributions and also consider different swapping strategies. Based on *two characteristic random variables*, the total repeater waiting time and the accumulated dephasing time of the final state, and their probability generating functions, we will be able to determine exact, optimized secret key rates. In principle, this gives us access to the *full statistics of this class of quantum repeaters*. Optimality here refers to the minimal dephasing among all parallel-distribution (and hence maximal raw-rate) schemes. For three segments and two intermediate stations, we show that the resulting secret key rates are optimal among all schemes (with distribution attempts in every segment limited by equal signaling time units). For more segments, we conjecture this to hold too, however, there is the loophole that sequential-distribution schemes (generally exhibiting smaller raw rates) may accumulate less dephasing and as a result, in combination, lead to a higher secret key rate. We conclude that our treatment gives evidence for any optimal scheme to distribute entangled pairs in parallel, to swap as soon as possible, and to simultaneously store qubits as little as possible. However, here the first and the third property are not compatible, which leads to another trade-off between high efficiencies (raw rates) and small state fidelities (high error rates) as commonly encountered for entanglement distribution and quantum repeaters. The (partially or fully) sequential schemes have the advantage that parallel storage of qubits can be avoided to a certain (or even a full) extent. However, since the sequential schemes are overall slower, their total dephasing may still exceed that of the fastest repeater schemes with parallel storage. For up to eight repeater segments, our optimal scheme, exhibiting the smallest total dephasing among all fast repeater schemes, also exhibits a smaller total dephasing than the fully sequential scheme.

The outline of the paper is as follows. In Sec. II, we first review the known results and existing approaches to analyze secret key rates for the smallest possible quantum repeater based upon a single middle station, including calculations of the repeater raw rate and physical error models to describe the evolution of the relevant density operators. The methods for the statistical analysis—probability generating functions, and the figure of merit to quantitatively assess the repeater performance—a QKD secret key rate, will be introduced in Sec. III. In Sec. IV, we start introducing our new, generalized treatment for quantum repeaters beyond a single middle station. We present two sections on the two characteristic random variables—the waiting time and the dephasing time, which contain the entire statistical information of the class of quantum repeaters considered in our work. In order to be able to take into account optimal strategies for the initial entanglement distribution and the subsequent entanglement swapping in more complex quantum repeaters with two or more intermediate repeater stations, we discuss in detail in various sections sequential and parallel distribution as well as optimal swapping schemes. Still in Sec. IV, we show how

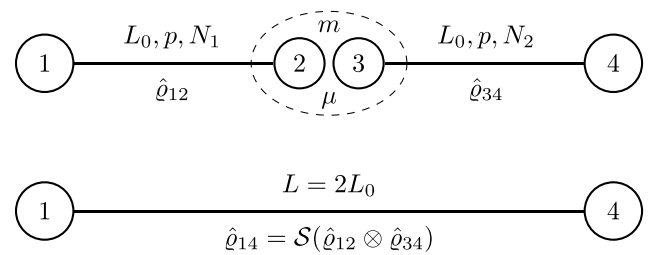


FIG. 1. A two-segment quantum repeater. Each segment has length L_0 and is characterized by a distribution success probability p , a (geometrically distributed) random number of distribution attempts N (with expectation value $\bar{N} = 1/p$), and a “final” two-qubit state $\hat{\rho}$ (subscripts denote segments or qubits at the nodes). “Final” here means that the, in general, imperfectly distributed states may be further subject to memory dephasing for a maximal number of m time steps (distribution attempts). After an imperfect swapping operation \mathcal{S} (error parameter μ), the repeater end nodes share an entangled state over distance $2L_0$.

these optimizations can be applied to the statistics of various quantum repeaters, explicitly calculating the probability generating functions of the two basic random variables for two-, three-, four-, and eight-segment quantum repeaters. In particular, for the four- and eight-segment cases we will show how and to what extent our optimized and exact treatment of the memory dephasing will improve the relevant quantities of the final state density operators as compared with the usually employed, canonical schemes such as “doubling.” The interesting case of a three-segment repeater and its optimization will be discussed in more detail in an Appendix. Finally, in Sec. V we will analyze the secret key rates of all proposed schemes and compare them for various repeater sizes with the “PLOB” bound [46].² For this, we will explicitly consider the extended set of experimental parameters and insert experimentally meaningful values (representing current and future experimental capabilities) for them. A particular focus will be on the initial state and gate parameters and their impact on the repeater performance. We shall compare the performances of different schemes, discuss the possibility of including multiplexing, and examine what influence a memory cutoff and what (scaling) advantages the different types of encoding for the flying qubits can have. For the latter, we discuss in more detail schemes based on the TF concept and, for the comparison between different schemes and encodings, the final secret key rates per second. Section VI concludes the paper with a final summary of the results and their implications. Various additional technical details can be found in the appendices.

II. QUANTUM REPEATERS WITH ONE MIDDLE STATION

A small quantum repeater composed of two segments and one middle station, as schematically shown in Fig. 1,

²See also Ref. [61] for a related work on the general secret key loss scaling in a point-to-point link, and also the more recent Refs. [69,70] on bounds on the key and entanglement rates that can be achieved by means of repeaters (assisted by local operations and classical communication).

is pretty well understood and it is known how to obtain the secret key rates in a QKD scheme assisted by a single memory station, even including experimental imperfections [29–31,45], including memory cutoffs [29,31,35,41], and for general, probabilistic entanglement swapping [35]. First experimental demonstrations of memory-enhanced quantum communication are also based on this simplest repeater setting [27]. In such a small quantum repeater, there is only a single Bell measurement on the spin memories at the central station, and so the entanglement swapping “strategy” is clear. Later we will briefly discuss the two-segment case as a special case of our more general rate analysis treatment, easily deriving the statistical properties of the two basic random repeater variables, the total waiting and dephasing times, and obtaining the optimal scheme [29,45].

The smallest, two-segment quantum repeater also serves as a basic building block for general, larger quantum repeaters. In the scheme of Fig. 1, each segment distributes an entangled pair of (mostly) stationary qubits by connecting its end nodes through flying qubits. The goal is to share entanglement between the two qubits at the end nodes of the whole repeater. The specific entanglement distribution scheme in each segment depends on the repeater protocol and it may involve memory nodes sending or receiving photons [29].

In the notation of Fig. 1, from an entangled state $\hat{\rho}_{12}$ of qubits 1 and 2 and an entangled state $\hat{\rho}_{34}$ of qubits 3 and 4, we create an entangled state $\hat{\rho}_{14}$ of qubits 1 and 4. The states $\hat{\rho}_{12}$ and $\hat{\rho}_{34}$ subject to the Bell measurement for the entanglement swapping operation are those quantum states present in the segments at the moment when the swapping is performed. If, for example, segment 1 generates an entangled state earlier than segment 2, then $\hat{\rho}_{12}$ enters the swapping step in the form of the initially, distributed state (which is not necessarily a pure maximally entangled state) after it was subject to memory dephasing while waiting for segment 2. Thus our physical model includes state imperfections that originate from the initial distribution as well as from the storage time, as we shall discuss in detail below. In addition, we will include an error parameter for the swapping gate itself.

A. Raw rate

The entanglement distribution in an elementary segment is typically not a deterministic process and several attempts are necessary to successfully share an entangled pair of qubits among two neighboring stations. If the probability of successful generation in each attempt is p , then the number of time steps until success is a geometrically distributed random variable N with success parameter p . We denote the failure probability as $q = 1 - p$. The parameter p is primarily given by the probability that a photonic qubit is successfully transmitted via a fiber channel of length L_0 connecting two stations, $\exp(-L_0/22 \text{ km})$. It also includes local state preparation/detection, fiber coupling, frequency conversion, and memory “write-in” efficiencies. The random variables for different segments (in Fig. 1 denoted as N_1 and N_2 for the first and the second segment, respectively) are independent and identically distributed geometric random variables. Only when both segments have generated an entangled state, we perform a swapping operation on the adjacent ends (nodes 2

and 3) of the segments and, when successful, we will be left with an entangled state of qubits 1 and 4.

In general, the swapping operation is also nondeterministic, but here we consider only the case of deterministic swapping. Under this simple assumption, we can still cover a large class of physically relevant and realistic repeater schemes and obtain exact and optimized rates for them. Moreover, especially for larger repeaters (still with no entanglement distillations), this assumption allows to circumvent the need for classical communication times longer than the elementary time τ (as defined below) in order to confirm successful entanglement swapping operations on “higher” repeater levels beyond the initial distributions in each segment. Physically, this assumption requires that in our schemes the Bell measurements for entanglement swapping (including the memory “read-out” operations) can be performed deterministically. Nonetheless, the swapping operations can still be imperfect, introducing errors in the states, as will be described below.

Due to the nondeterministic nature of the initial entanglement generation, the whole process of entanglement distribution is also nondeterministic and fully described by the number of attempts up to and including the successful distribution (so, this number is always larger than zero). The real, wall-clock time needed for entanglement generation or distribution can be obtained from the number of attempts by multiplying it with an elementary time unit, typically $\tau = L_0/c_f$, where again L_0 is the length of the segment and $c_f = c/n_r$ is the speed of light in the optical fiber (c is the speed of light in vacuum and n_r is the index of refraction of the fiber, and depending on the specific distribution protocol there may be an extra factor 2). The elementary time unit is actually composed of the classical (and quantum) signaling time per segment τ and the local processing time. However, for typical L_0 values as considered here, the former largely dominates over the latter, and so we may neglect the local times, as they would hardly change the final secret key rates [29].

If one of the two segments generates entanglement earlier than the other, then the created state must be kept in memory. The exact technique employed to implement this quantum memory is irrelevant for our analysis. The simplest model assumes that the state can be kept in memory for arbitrarily long. A useful assumption in the realistic setting with imperfect quantum memories is to set a certain limit of m time units on the memory storage time, thus restarting the creation process whenever this threshold is reached.

B. Errors

When the quantum repeater is employed for long-range QKD, errors will become manifest in terms of a reduced secret key fraction, as introduced in the subsequent section. In order to compute this secret key fraction, we need to know the finally distributed state (density operator) of the complete repeater system, and for this we require a more detailed physical model. We shall establish a relation between the finally distributed state as a function of the initial states in each segment and various errors that appear in the process of entanglement distribution. The physical model is rather common and has been used before in several works, both analytical and

numerical. Especially, a two-segment quantum repeater can be treated analytically based on simple Pauli errors representing memory dephasing and gate (Bell measurement) errors.

We address the effect of imperfect quantum storage at a memory node via a dephasing model where the stored quantum state is waiting for an adjacent segment to successfully generate or distribute entanglement. This kind of memory error can be modelled by a one-qubit dephasing channel,

$$\Gamma_\lambda(\hat{\rho}) = (1 - \lambda)\hat{\rho} + \lambda Z\hat{\rho}Z, \quad (1)$$

where Z is a qubit Pauli phase flip operator. We assume that $0 \leq \lambda < 1/2$, and any such number can be represented as $\lambda = (1 - e^{-\alpha})/2$ for some $\alpha > 0$. We denote the map in Eq. (1) also as Γ_α . To avoid confusion, throughout this work we use the following definition:

$$\Gamma_\alpha(\hat{\rho}) = \frac{1 + e^{-\alpha}}{2}\hat{\rho} + \frac{1 - e^{-\alpha}}{2}Z\hat{\rho}Z. \quad (2)$$

The definition for a dephasing two-qubit channel is obtained from Eqs. (1) and (2) by the replacement $Z \rightarrow Z \otimes I$ if the dephasing acts on the first qubit and by $Z \rightarrow I \otimes Z$ if the dephasing acts on the second qubit.

Errors may also occur when a Bell state measurement is performed. This kind of errors is modelled by a two-qubit depolarizing channel,

$$\tilde{\Gamma}_\mu(\hat{\rho}) = \mu\hat{\rho} + (1 - \mu)\frac{\hat{1}}{4}. \quad (3)$$

We do not consider dark counts of the detectors, since the optical propagation distances L_0 after which a detection attempt takes place remain sufficiently small in any quantum relay or repeater. Thanks to recent technological developments typical dark count rates can be reduced far below 1 dark count per second. In Ref. [47], they were shown to be in the range of mHz. Dark counts of such a low frequency have no significant impact on the secret key rate in our schemes.

Let us now apply this to the case of a two-segment quantum repeater. The Bell measurement of qubits 2 and 3 produces from a pair of states $\hat{\rho}_{12}$ and $\hat{\rho}_{34}$ a state $\hat{\rho}_{14}$, see Fig. 1. The initial state $\hat{\rho}_{1234} = \hat{\rho}_{12} \otimes \hat{\rho}_{34}$ of all four qubits 1, 2, 3, and 4 is the product of the states of qubits 1, 2 and qubits 3, 4. After the measurement the state $\hat{\rho}_{14}$ of qubits 1 and 4 becomes

$$\hat{\rho}_{14} \equiv \mathcal{S}(\hat{\rho}_{1234}) = \frac{\text{Tr}_{23}(\hat{P}_{23}\tilde{\Gamma}_{\mu,23}(\hat{\rho}_{1234})\hat{P}_{23})}{\text{Tr}(\hat{P}_{23}\tilde{\Gamma}_{\mu,23}(\hat{\rho}_{1234})\hat{P}_{23})}, \quad (4)$$

where μ describes the imperfection of the measurement and $\hat{P}_{23} = |\Psi^+\rangle_{23}\langle\Psi^+|$ is one of the four measurement operators in the two-qubit Bell state basis of the central subsystem (qubits 2 and 3), $\{|\Phi^\pm\rangle_{23}\langle\Phi^\pm|, |\Psi^\pm\rangle_{23}\langle\Psi^\pm|\}$, where $|\Phi^\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$, $|\Psi^\pm\rangle = (|10\rangle \pm |01\rangle)/\sqrt{2}$, for qubits defined via the two Z eigenstates $|0\rangle, |1\rangle$ (for any one of the other three Bell measurement outcomes, the analysis below is similarly applicable). In this case, Eq. (4) reduces to

$$\hat{\rho}_{14} \equiv \mathcal{S}(\hat{\rho}_{1234}) = \frac{23\langle\Psi^+|\tilde{\Gamma}_{\mu,23}(\hat{\rho}_{1234})|\Psi^+\rangle_{23}}{\text{Tr}_{23}(\langle\Psi^+|\tilde{\Gamma}_{\mu,23}(\hat{\rho}_{1234})|\Psi^+\rangle_{23})}. \quad (5)$$

A simple way to compute the right-hand side of this relation for an arbitrary density operator $\hat{\rho}_{1234}$ is given in Appendix B.

In general, states of the form

$$\hat{\rho}_0 = \tilde{\Gamma}_{\mu_0}(F_0|\Psi^+\rangle\langle\Psi^+| + (1 - F_0)|\Psi^-\rangle\langle\Psi^-|) \quad (6)$$

play an important role in the full theory presented below. It is easy to verify that

$$(I \otimes Z)\hat{\rho}_0(I \otimes Z) = (Z \otimes I)\hat{\rho}_0(Z \otimes I), \quad (7)$$

so it does not matter whether Γ_α acts on the first or second qubit of $\hat{\rho}_0$ and either application we simply denote as $\Gamma_\alpha(\hat{\rho}_0)$. An easily checkable relation is

$$\Gamma_\alpha(\hat{\rho}_0) = \tilde{\Gamma}_{\mu_0}(F|\Psi^+\rangle\langle\Psi^+| + (1 - F)|\Psi^-\rangle\langle\Psi^-|), \quad (8)$$

where the new parameter F is expressed in terms of the original one, F_0 , as

$$F = \frac{1}{2}(2F_0 - 1)e^{-\alpha} + \frac{1}{2}. \quad (9)$$

The initial fidelity parameter F_0 (describing an initial dephasing of the distributed states) combined with the μ_0 -dependent initial depolarization are both included in the initial $\hat{\rho}_0$ in Eq. (6), because later this will allow for an elegant recursive state relation for larger repeaters. It will also allow to switch between different initial physical errors depending on the specific repeater realization. In general, the maps in Eq. (2) satisfy the relation $\Gamma_\alpha \circ \Gamma_\beta = \Gamma_{\alpha+\beta}$. In particular, we have $\Gamma_\alpha \circ \dots \circ \Gamma_\alpha = \Gamma_{k\alpha}$, where Γ_α is used k times on the left-hand side. So, applying Γ_α to the state $\hat{\rho}_0$ given by Eq. (6) several times, we have to multiply α in Eq. (9) by this number of times.

In a two-segment quantum repeater, if we start with the distributed states $\hat{\rho}_{12}$ and $\hat{\rho}_{34}$ of the special form [similar to Eq. (6)]

$$\begin{aligned} \hat{\rho}_{12} &= \tilde{\Gamma}_{\mu_1}(F_1|\Psi^+\rangle_{12}\langle\Psi^+| + (1 - F_1)|\Psi^-\rangle_{12}\langle\Psi^-|), \\ \hat{\rho}_{34} &= \tilde{\Gamma}_{\mu_2}(F_2|\Psi^+\rangle_{34}\langle\Psi^+| + (1 - F_2)|\Psi^-\rangle_{34}\langle\Psi^-|), \end{aligned} \quad (10)$$

then the ‘‘swapped,’’ finally distributed state $\hat{\rho}_{14}$, given by Eq. (5), is also of the same form

$$\hat{\rho}_{14} = \tilde{\Gamma}_{\mu_d}(F_d|\Psi^+\rangle_{14}\langle\Psi^+| + (1 - F_d)|\Psi^-\rangle_{14}\langle\Psi^-|), \quad (11)$$

where $\mu_d = \mu\mu_1\mu_2$ and F_d reads as

$$F_d = \frac{1}{2}(2F_1 - 1)(2F_2 - 1) + \frac{1}{2}. \quad (12)$$

We see that the form of the state is preserved by the total distribution procedure of a two-segment repeater. The same conclusion will be applicable to larger repeaters as well—if all segments start in a state of the form given by Eq. (6), then the finally distributed state will also be of the same form.

For the two-segment repeater, let us now assume that both segments generate the same state as in Eq. (6), but not necessarily simultaneously, and so generally only after some waiting time we perform the entanglement swapping and distribute entanglement over the two segments. If the first segment generates entanglement after N_1 time units, and the second segment after N_2 time units, and we perform the entanglement swapping after N time units, with $N \geq N_1, N_2$, then the states $\hat{\rho}_{12}$ and $\hat{\rho}_{34}$ prior to swapping will be of the form in Eq. (10) with $\mu_1 = \mu_2 = \mu_0$ and

$$\begin{aligned} F_1 &= \frac{1}{2}(2F_0 - 1)e^{-(N-N_1)\alpha} + \frac{1}{2}, \\ F_2 &= \frac{1}{2}(2F_0 - 1)e^{-(N-N_2)\alpha} + \frac{1}{2}. \end{aligned} \quad (13)$$

The final, distributed state is then given by Eq. (11) where, according to Eq. (12), the parameters are $\mu_d = \mu\mu_0^2$ and

$$F_d = \frac{1}{2}(2F_0 - 1)^2 e^{-(2N - N_1 - N_2)\alpha} + \frac{1}{2}. \quad (14)$$

This distributed state is subject to less dephasing when we swap as early as possible, thus $N = \max(N_1, N_2)$, so the integer term in front of α is equal to $2 \max(N_1, N_2) - N_1 - N_2 = |N_1 - N_2|$. The precise physical meaning of α will be discussed later when we calculate the memory-assisted secret key rates in a quantum repeater. Here we omitted explicit factors depending on the number of memory qubits that are subject to dephasing in a single repeater segment (in our model this will be one or, typically, two corresponding to one distributed spin pair). These factors can be absorbed into α .

III. METHODS AND FIGURE OF MERIT

Before we move to the more general case of more than two segments and more than just one middle station, we need some general methods and tools from statistics. This will enable us to derive an analytic, statistical model for larger quantum repeaters beyond one middle station (the physical model remains basically the same as for the elementary two-segment quantum repeater) and to calculate average values or moments of two random variables: the total repeater waiting time K_n and the total (i.e., the totally accumulated) memory dephasing time D_n . As a quantitative figure of merit, it is useful to consider the secret key rate of QKD, as it combines in a single quantity the two typically competing effects in a quantum repeater system: the speed at which quantum states can be distributed over the entire communication distance and the quality of the totally distributed quantum states. These two effects are naturally related to the above-mentioned two random variables. For our purposes here, throughout we shall rely on asymptotic expressions for the secret key rate omitting effects of finite key lengths. Of course, alternatively, one could also treat the total state distribution efficiencies and qualities (fidelities) separately and individually, and then also consider quantum repeater applications beyond long-range QKD.

A. Probability generating function

The method of probability generating functions (PGFs) plays an important role in our treatment of statistical properties of quantum repeaters. For any random variable X , taking integer non-negative values its PGF $G_X(t)$ is defined via

$$G_X(t) = \mathbf{E}[t^X] = \sum_{k=0}^{+\infty} \mathbf{P}(X = k)t^k. \quad (15)$$

The series on the right-hand side converges at least for all complex values of t such that $|t| \leq 1$. The PGF contains all statistical information about X , which can be easily extracted if an explicit expression for $G_X(t)$ is known. For example, the average value of X , $\mathbf{E}[X] \equiv \bar{X}$, and its variance $\mathbf{V}[X] \equiv \sigma_X^2 = \mathbf{E}[(X - \bar{X})^2]$, are expressed as follows:

$$\begin{aligned} \mathbf{E}(X) &= G'_X(1), \\ \mathbf{V}(X) &= G''_X(1) + G'_X(1) - G_X'^2(1). \end{aligned} \quad (16)$$

For any $\alpha \geq 0$ the random variable $e^{-\alpha X}$ has a finite average value, which can be computed as

$$\mathbf{E}[e^{-\alpha X}] = G_X(e^{-\alpha}). \quad (17)$$

Note that for this random variable, besides the mean or average value, any statistical moment can be easily obtained and the k th-moment simply becomes $\mathbf{E}[e^{-\alpha k X}] = G_X(e^{-k\alpha})$. Two kinds of random variables appear in our model of quantum repeaters where one is related to the raw rate and the other to the secret key fraction of QKD as introduced below. It is not always possible to get a compact expression for the PGF of these random variables explicitly, but when it is, we use the equations above to obtain statistical properties of the corresponding random variables.

B. Secret key rate

The main figure of merit in our study is the quantum repeater secret key rate, which can be defined as the product of two quantities,

$$S = Rr, \quad (18)$$

where R is the raw rate and r is the secret key fraction. The raw rate is simply the inverse average waiting time,

$$R = \frac{1}{T}, \quad (19)$$

where $T = \mathbf{E}[K]$ is the average number of steps K needed to successfully distribute one entangled qubit pair over the entire communication distance between Alice and Bob (giving an average time duration in seconds when multiplied with an appropriate time unit τ). The secret key fraction of the BB84 QKD protocol [5,6], assuming one-way postprocessing, is given by

$$r = 1 - h(\bar{e}_x) - h(\bar{e}_z), \quad (20)$$

where e_x and e_z are the quantum bit error rates (QBERs),

$$\begin{aligned} e_z &= \langle 00 | \hat{\rho}_n | 00 \rangle + \langle 11 | \hat{\rho}_n | 11 \rangle, \\ e_x &= \langle +- | \hat{\rho}_n | +- \rangle + \langle -+ | \hat{\rho}_n | -+ \rangle, \end{aligned} \quad (21)$$

and $h(p)$ is the binary entropy function,

$$h(p) = -p \log_2(p) - (1-p) \log_2(1-p). \quad (22)$$

The QBERs e_x and e_z in Eq. (21) are obtainable from the final, distributed state $\hat{\rho}_n$ of an n -segment quantum repeater, which in our case will depend on the dephasing random variable, and so we have to insert average values in Eq. (20) as indicated by the bars. We thus need a complete model of quantum repeaters to compute the statistical properties of the relevant random variables associated with the number of steps to distribute entanglement or the density operator of the distributed state. Given such a model, the aim of our work is to compute and analyze secret key rates of quantum repeaters with an increasing size, up to eight segments, considering and optimizing different distribution and swapping schemes. Besides the most common BB84 QKD protocol, alternatively, we may also consider the six-state protocol [48] which would slightly improve the secret key rate. Assuming again one-way postprocessing, the secret key fraction r of the six-state protocol is given by $1 - H(\lambda)$ [[4], App. A] where

$H(\cdot)$ is the Shannon entropy and the vector λ must contain the corresponding weights of the four Bell states in the final density operator $\hat{\rho}_n$. Throughout this work all secret key rates are calculated from their asymptotic expressions and hence effects of finite key lengths are not included here. This simplifies the analytical treatment of a quantum repeater chain, which, as we will see, quickly becomes rather complex for a growing number of stations, involving many distinct choices and strategies for the entanglement manipulations. Moreover, our rate analysis shall also be useful to assess and compare the performances of different quantum repeaters in applications beyond QKD.

IV. QUANTUM REPEATERS BEYOND ONE MIDDLE STATION

Larger repeaters with more than two segments and one middle station can now be modeled in a way similar to the two-segment case discussed above. However, the extended, more general case is also more complex and there are both different ways to perform the initial entanglement distributions in all elementary segments and different ways to connect the successfully distributed segments via entanglement swapping. For the initial distributions, we make a distinction between sequential and parallel schemes, where the former refers to a scheme in which, according to a predetermined order, the distributions are attempted step by step starting from e.g., the first segment. In a parallel scheme, the distributions are attempted simultaneously in all segments, which obviously leads to a smaller total repeater waiting time than for the sequential distribution schemes. Nonetheless, since the sequential schemes do make use of the quantum memories, they do already offer the repeaterlike scaling advantage over point-to-point quantum communication links. Even for a two-segment quantum repeater, we may choose a sequential scheme, where we first only distribute e.g., the left segment and only once we succeeded there we attempt to distribute the right segment. Experimentally, this can be of relevance for those realizations where only a single short-term quantum memory is available at every station for the light-matter interface and another quantum memory for the longer-term storage (e.g., respectively, an electronic and a nuclear spin in color-center-based repeater nodes) [40,49]. Theoretically and conceptually, there are at least two advantages of a (fully) sequential distribution approach [45].

First, the two basic random variables of a quantum repeater are very simple and so the secret key rates are fairly easy to calculate. Second, always only at most one entangled qubit pair (or even only a single spin if, e.g., Alice measures her qubit immediately) may be subject to memory dephasing during all distribution steps. For the entanglement connections via entanglement swapping, the two-segment case is special, as there is only one swapping to be performed at the end when pairs in both segments are available. However, already with three segments and two repeater stations there is no unique swapping order anymore, and we may either fix the order or “dynamically” choose where we swap as soon as swapping is possible for two neighboring, successfully distributed segments. In a fixed scheme, two neighboring segments, though ready, may have to wait before being connected. Thus the

choice of the entanglement swapping scheme has a significant impact on the totally accumulated dephasing time. In a worst-case scenario, we could wait until all segments have been distributed and then do all the entanglement connections at the very end; for deterministic entanglement swapping, like in our model, this would not affect the raw waiting times, but it would lead to a maximal total dephasing. In this case, a sequential distribution where entanglement swapping takes place immediately when a new, successfully bridged segment is available can lead to a higher secret key rate than a combination of parallel distribution and swapping at the end (where the rates of the latter scheme may still only be obtainable approximately) [45]. The crucial innovation in our analytical treatment here is that we will be able to obtain the exact secret key rates for schemes that combine fast, parallel distributions with fast, immediate swappings (and hence a suppressed level of parallel storage). In other words, among all parallel-distribution schemes we will calculate the exact rates that are optimized with regards to the total repeater dephasing.

A. Waiting times

The average total waiting times in a quantum repeater or even the full statistics of the waiting-time random variable can be, in principle, obtained via the Markov chain formalism, even when the swapping is probabilistic [35,36]. More generally, the PGFs as introduced earlier contain the full statistical information, and for deterministic swapping, we can obtain the PGF of K_n through combinatorics. In order to minimize the total waiting time, the distributions should occur in parallel. However, there is no unique way to perform the entanglement swapping, and so let us briefly consider this aspect in the context of the waiting times. For example, for a four-segment repeater, two possible swapping strategies are shown in Figs. 2 and 3. Both schemes are for a fixed swapping order, while we may distribute the individual segments in parallel. In the first scheme, typically referred to as “doubling”, we swap the two halves of the repeater independently and only when both are ready, we swap them too. In the second scheme, we swap the segments one after the other starting in one of the repeater’s ends (here the left end); we may refer to this scheme as “iterative” swapping. Other schemes are possible, and the more segments the repeater has, the more possibilities for performing swappings there are. The raw rate of a repeater is characterized by the number of steps, K_n , needed to successfully distribute an entangled pair, and this random variable can be expressed in terms of the geometric random variables N_i associated with each segment. For example, for the swapping schemes shown in Figs. 2 and 3, when combined with parallel distributions, we have $K_4 = \max(N_1, N_2, N_3, N_4)$, so the two schemes have the same raw rate. In general, the waiting times of all such schemes that distribute in parallel are of a similar form. Those schemes that we later classify as “optimal” in terms of the whole secret key rate are assumed to be parallel distribution schemes. Conversely, combining iterative swapping with sequential distribution can lead to a reduced accumulated dephasing time at the expense of an increased total repeater waiting time. We shall discuss the accumulated dephasing times next.

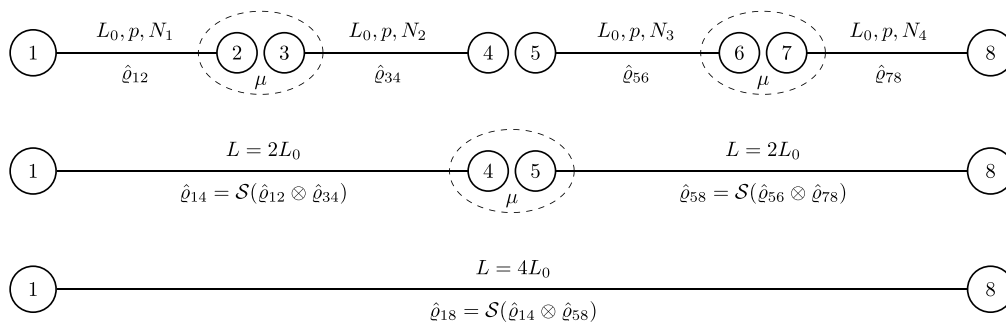


FIG. 2. “Doubling” swapping scheme for a four-segment quantum repeater. This is the most common swapping strategy which allows to systematically include entanglement distillation at each repeater “nesting level.” Without extra distillation, however, “doubling” is never optimal: combined with fast, parallel distributions it exhibits increased parallel storage times and hence memory dephasing (while combined with sequential distributions the repeater waiting times become suboptimal). Memory cutoff parameters are omitted in the illustration.

B. Dephasing times

In order to treat the total dephasing time in a quantum repeater with more than two segments, we have to generalize the methods and the model that led to the result for the distributed state for two segments, Eqs. (11) and (12), and the discussion below, to larger repeaters with, in principle, an arbitrary number of segments n . In fact, we did the two-segment derivations in such a way that an n -segment extension is now straightforward. We obtain the following expression for the final, distributed state in the general case:

$$\hat{\rho}_n = \tilde{\Gamma}_{\mu_n} \left[\frac{1 + (2F_0 - 1)^n e^{-\alpha D_n}}{2} |\Psi^+\rangle\langle\Psi^+| + \frac{1 - (2F_0 - 1)^n e^{-\alpha D_n}}{2} |\Psi^-\rangle\langle\Psi^-| \right], \quad (23)$$

where $\mu_n = \mu^{n-1} \mu_0^n$ and $D_n = D_n(N_1, \dots, N_n)$ is a random variable describing the total number of time units that contribute to the total dephasing in the final output state. For $n = 2$, the expression for $D_2(N_1, N_2) = |N_1 - N_2|$ has been obtained before, for larger n the value of D_n now depends on the swapping scheme. As before, we omitted explicit factors

depending on the number of memory qubits that are subject to dephasing in a single repeater segment (one or two spins in our model) which also depends on the application and the specific execution of the protocol. Such factors can always be absorbed into α . The precise physical meaning of α will be discussed later when we calculate the memory-assisted secret key rates in a quantum repeater. The QBERs for the state in Eq. (23) are easy to compute,

$$e_z = \frac{1}{2} (1 - \mu^{n-1} \mu_0^n),$$

$$e_x = \frac{1}{2} (1 - \mu^{n-1} \mu_0^n (2F_0 - 1)^n e^{-\alpha D_n}). \quad (24)$$

For one of the averages, we have $\bar{e}_z = e_z$, and in order to obtain the other average \bar{e}_x we need to calculate the expectation value $\mathbf{E}[e^{-\alpha D_n}]$. This average can be obtained with the help of Eq. (17) if we know the PGF of D_n . Again, in principle, we can get the full statistics of D_n (and functions of it) from this PGF. More specifically, according to Eq. (17), for the random variable $e^{-\alpha D_n}$ we can easily obtain all statistical moments of order k , $\mathbf{E}[e^{-\alpha D_n k}]$. This may be useful for a rate analysis that includes keys of a finite length, though here in this work we shall focus on asymptotic keys. The PGF of D_n , however, is generally harder to obtain than that of K_n . For example,

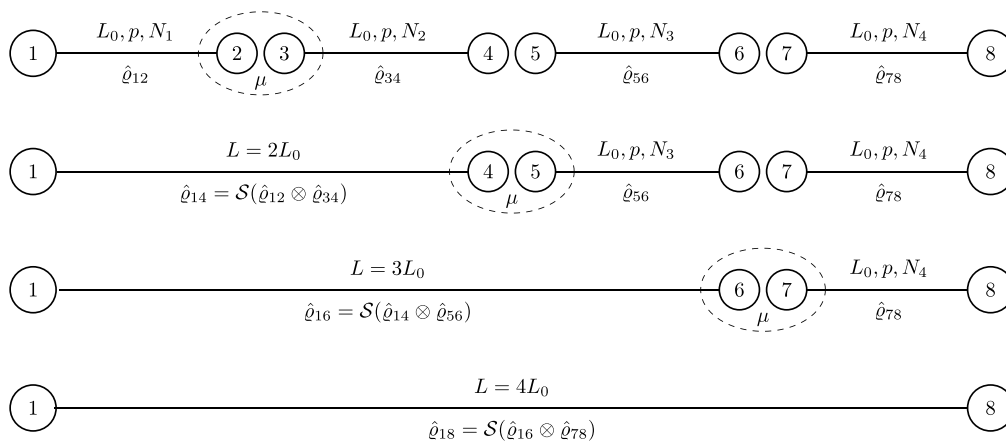


FIG. 3. “Iterative” swapping scheme for a four-segment quantum repeater. The swapping operations are performed step by step (here from left to right). Also this scheme, when executed with parallel distributions in each segment, leads to an increase of the total dephasing. However, if combined with sequential distributions, the accumulated dephasing times can be reduced (with always at most one spin or spin pair being subject to a long dephasing) at the expense of a growing repeater waiting time. Memory cutoff parameters are omitted in the illustration.

the PGF of D_n is not obtainable via the absorption time of a Markov chain (unlike that of K_n , which is obtainable even when the entanglement swapping is probabilistic) [35,36]. Nonetheless, at least without considering the more complicated case including a memory cutoff, we can calculate the relevant PGF of D_n by analyzing all permutations of the basic variables (there are also other, more elegant, but still not so efficient and well scalable methods to treat the statistics of D_n , e.g., based on algebraic geometry).

We see that in order to compute the secret key rate of a quantum repeater we need to study the two integer-valued random variables K_n and D_n . The former describes the number of steps to successfully distribute entanglement and is responsible for the repeater’s raw rate. The latter describes the quality of the final state and strongly depends on the swapping scheme. For example, for a four-segment repeater with a predetermined swapping order like the iterative scheme in Fig. 3, we could actually also choose to adapt the initial entanglement distributions to the swapping strategy and hence wait with every subsequent distribution step until the corresponding connection from the left has been performed. Since this is no longer the parallel distribution (it is the “sequential” distribution), we would obtain an increased total waiting time. However, the accumulated dephasing time may be reduced this way, as we discuss in the next section.

In general, we may also consider schemes with a memory cutoff, where we put a certain restriction of m time units on the maximum time a qubit can be kept in memory. So, in this case, we study four variables—the total number of distribution steps and the total dephasing, both with and without cutoff. In order to maximize the secret key rate we need a scheme with small $\mathbf{E}[K_n]$ and large $\mathbf{E}[e^{-\alpha D_n}]$. In the following sections, we will introduce different schemes for performing the entanglement swapping and, where possible, compute the PGFs of the corresponding random variables. The PGF of K_n is denoted as $G_n(t)$ and that of D_n as $\tilde{G}_n(t)$. For the corresponding quantities with cutoff m , we use the superscript $[m]$, e.g., $K_n^{[m]}$. We will see and argue that there are three basic properties that a quantum repeater protocol (unassisted by additional quantum error detection or correction) should exhibit: distribute the entangled states in each segment in parallel, swap the initially distributed states as soon as possible, and avoid parallel storage of already distributed pairs as much as possible. Obviously, all these three “rules” cannot be fully obeyed at the same time. In particular, parallel distribution will ultimately lead to some degree of parallel storage.

C. Sequential distribution schemes

In what we refer to as a sequential entanglement distribution scheme, the initial, individual pairs are no longer distributed in parallel but strictly sequentially according to a predetermined order. If this order is chosen in a suitable way, it is possible that at any time during the repeater protocol at most one entangled pair is subject to dephasing (apart from small constant dephasing units for single attempts), because once a new pair is available an entanglement connection can be immediately performed and only then another new segment starts distributing. This may lead to a reduced accumulated dephasing time. Moreover, from a secret key rate analysis

point of view, an appropriate sequential scheme can allow for a straightforward calculation of the statistics of both random variables, the total waiting and the accumulated dephasing times, even when a memory cutoff is included.

Let us consider a simple, sequential distribution and swapping scheme where the above discussion applies and the secret key rate can be computed exactly by means of elementary combinatorics. In this scheme, we start by distributing entanglement in segment 1 (most left segment), and only after a success we start to attempt distributions in segment 2. As soon as we succeed there too, we immediately swap segments 1 and 2 and start to distribute entanglement in segment 3. As soon as we succeed with the distribution in segment 3, we swap segment 3 with the first two, already connected segments, start distributing in segment 4, and so on, repeating this process until entanglement has also been distributed in the most right segment followed by a final entanglement swapping step. This scheme, for $n = 4$, is also illustrated by Fig. 3. The variables K_n and D_n for this scheme and general n are thus defined as

$$K_n^{\text{seq}} = N_1 + \dots + N_n, \quad D_n^{\text{seq}} = N_2 + \dots + N_n. \quad (25)$$

The PGFs of these random variables are just powers of the PGF of the geometric distribution:

$$G_n^{\text{seq}}(t) = \left(\frac{pt}{1-qt} \right)^n, \quad \tilde{G}_n^{\text{seq}}(t) = \left(\frac{pt}{1-qt} \right)^{n-1}. \quad (26)$$

In Appendix C, we derive the following expressions for the PGFs of the random variables with memory cutoff. We assume an accumulated, global cutoff where the total storage (dephasing) time across all segments must not exceed the value m . The PGF of $K_n^{[m]}$ is given by

$$G_n^{[m]}(t) = \frac{p^n t^n \sum_{j=0}^{m-n+1} \binom{j+n-2}{n-2} q^j t^j}{1-qt - p \sum_{i=0}^{n-2} \binom{m}{i} p^i q^{m-i} t^{m+1}}, \quad (27)$$

and the PGF of $D_n^{[m]}$ becomes

$$\tilde{G}_n^{[m]}(t) = \frac{t^{n-1} \sum_{j=0}^{m-n+1} \binom{j+n-2}{n-2} q^j t^j}{\sum_{i=0}^{m-n+1} \binom{m}{i+n-1} p^i q^{m-n+1-i}}. \quad (28)$$

Because it takes at least one time step for each segment to succeed, we have the inequalities $n \leq K_n^{[m]}$ and $n-1 \leq D_n^{[m]} \leq m$, which agree with the PGFs of these quantities presented above. Moreover, for $m \rightarrow +\infty$, we have

$$G_n^{[+\infty]}(t) = G_n^{\text{seq}}(t), \quad \tilde{G}_n^{[+\infty]}(t) = \tilde{G}_n^{\text{seq}}(t). \quad (29)$$

These relations are easy to prove, just note that

$$\sum_{i=0}^{m-n+1} \binom{m}{i+n-1} p^i q^{m-n+1-i} = \frac{1}{p^{n-1}} \left[1 - \sum_{i=0}^{n-2} \binom{m}{i} p^i q^{m-i} \right]. \quad (30)$$

The binomial coefficient $\binom{m}{i}$ is polynomial in m of i th degree, and thus $\binom{m}{i} q^m \rightarrow 0$ when $m \rightarrow +\infty$ for all $i = 0, \dots, n-2$, which proves the relations of Eq. (29).

There are also variations of the above sequential cutoff scheme. In the previous scheme we only abort a round when we already waited m time units. Now consider the case where we already waited $m/2$ time units, but only a small number of

segments succeeded. Hence, it is highly unlikely that we will succeed in all segments within the m time steps. Therefore it is better not to waste time and already abort the current round to start from scratch. A very simple strategy following this idea makes use of an individual (local) cutoff in each segment. However, it is beneficial to use a different cutoff in every segment; one should choose a smaller cutoff in the first segments and then increase the cutoff for later segments. The rationale behind this is that in the first segments we have not invested much effort and can discard rather aggressively, whereas later we should discard less aggressively since we already consumed lots of resources.

The advanced protocol is uniquely defined by a vector of cutoffs $\mathbf{m} = (m_1, \dots, m_{n-1})$ and the random variables K_n and D_n for this protocol and general n are given by

$$K_n^{\text{seq}, \mathbf{m}} = \tilde{N}^{(m_{n-1})} + (T_{n-1} - 1)m_{n-1} + \sum_{j=1}^{T_{n-1}} K_{n-1, j}^{\text{seq}, \mathbf{m}}, \quad (31)$$

where $K_1^{\text{seq}, \mathbf{m}}$ is geometrically distributed with parameter p , $\tilde{N}^{(m_{n-1})}$ follows a truncated geometric distribution with cutoff m_{n-1} , and T_{n-1} is a geometric random variable with parameter $(1 - q^{m_{n-1}})$ describing the number of starts of the protocol. For the dephasing we have

$$D_n^{\text{seq}, \mathbf{m}} = \tilde{N}^{m_1} + \dots + \tilde{N}^{m_{n-1}}. \quad (32)$$

The PGF of $K_n^{\text{seq}, \mathbf{m}}$ is given recursively by (see Appendix C)

$$G_n^{[\mathbf{m}]}(t) = G_2^{[m_{n-1}]}(t) t^{-m_{n-1}} P^{(m_{n-1})}(G_{n-1}^{[\mathbf{m}]}(t) t^{m_{n-1}}), \quad (33)$$

where $P^{(m)}(t) = \frac{(1-q^m)t}{1-q^m t}$ and $G_1^{[\mathbf{m}]} = G_1^{\text{seq}}$. The PGF of $D_n^{\text{seq}, \mathbf{m}}$ is simply given by

$$\tilde{G}_n^{[\mathbf{m}]}(t) = \prod_{j=1}^{n-1} \tilde{G}_2^{[m_j]}(t), \quad (34)$$

since the sum of independent random variables translates to a product for PGFs. As the state quality only depends on the total dephasing time, the best sequential protocol would count the total number of storage steps and discard based on a cutoff as a function of the number of already succeeded segments, and one may also employ an early aggressive discarding.

D. Parallel distribution schemes

A more efficient class of schemes is constructed when we do not wait for some segments to finish before we start others. In these schemes, we start all segments independently and distribute in parallel. It follows that for these schemes without a cutoff, we have

$$K_n^{\text{par}} = \max(N_1, \dots, N_n), \quad (35)$$

i.e., all such schemes give the same raw rate. In Appendix A, we derive the following expressions for the PGF of K_n :

$$\begin{aligned} G_n^{\text{par}}(t) &= t \sum_{i=1}^n (-1)^{i+1} \binom{n}{i} \frac{1 - q^i}{1 - q^i t} \\ &= 1 + (1 - t) \sum_{i=1}^n (-1)^i \binom{n}{i} \frac{1}{1 - q^i t}. \end{aligned} \quad (36)$$

The two expressions are identical, since their difference reduces to $(1 - 1)^n = 0$. From the first expression, it is clear that the values of K_n start at 1, as it must be, because it takes at least one time unit to distribute entanglement. In the other expression, the necessary property of all PGFs becomes manifest, $G_n(1) = 1$. From the first relation of Eqs. (16), we get the well-known expression for the average waiting time of a quantum repeater with parallel distribution and deterministic entanglement swapping (at any time possible, e.g., at the very end)

$$\overline{K_n^{\text{par}}} = \frac{d}{dt} G_n^{\text{par}}(t) \Big|_{t=1} = \sum_{i=1}^n (-1)^{i+1} \binom{n}{i} \frac{1}{1 - q^i}, \quad (37)$$

previously obtained in Ref. [50] (not including the full probability distribution). All other relevant expressions, the total number of distribution steps including memory cutoff as well as the finally distributed quantum state including memory imperfections, both for the model with and without memory cutoff, depend on the particular swapping strategy chosen (e.g., unnecessarily postponing some or even all entanglement swapping steps until the very end maximizes the amount of parallel storage and hence the total dephasing in the final state). For this, there is a growing number of choices for larger repeaters, and in the following we shall derive an optimal swapping scheme that results in a minimal total dephasing time (while sharing the high raw rates, i.e., the minimal total waiting times, with all parallel distribution schemes).

1. Optimal swapping scheme

Because all schemes (without a cutoff) considered in this section have equal raw rates, the best secret key rate is determined by the optimal scheme with regards to the secret key fraction. In this section, we shall present this scheme. In contrast to the schemes presented in Figs. 2 and 3, which are fixed, the optimal swapping scheme is dynamic. In a fixed scheme the order of swappings is fixed at the beginning and does not depend on the order in which the segments become ready. For example, for the “doubling” scheme as shown in Fig. 2 for $n = 4$, we never swap segments 2 and 3, even if they are ready and segments 1 and 4 are not. We always wait for segments 1 and 2 or segments 3 and 4 to become ready, swap these pairs, and then swap the larger segments to finish the entanglement distribution over the whole repeater. In a dynamical scheme, we do not follow a prescribed order and can swap the segments based on their state. Of course, we can freely mix and match fixed and dynamic behaviors. For example, for $n = 8$, we can first swap four pairs of segments in a fixed way and then swap the four new, larger segments dynamically. We now show that the fully dynamic scheme, where we always swap the segments that are ready, is the optimal one.

To prove this we give two characterizations of this fully dynamic scheme. One is the straightforward translation of the description to the definition, but this definition is not explicitly optimal. The other one is optimal by construction, but is not fully dynamic explicitly. We then show that the two constructions coincide demonstrating the validity of our statement. Swapping an earliest pair of segments means that we choose

an index i for which $\max(N_i, N_{i+1})$ is minimal (there can be several such indices), swap the pair of segments i and $i + 1$, and recursively apply this procedure to the other segments (if

there are several such pairs, choose one of them arbitrarily). If we denote the dephasing random variable of this scheme as \tilde{D}_n , its formal definition reads as

$$\tilde{D}_n(N_1, \dots, N_n) = |N_{i_0} - N_{i_0+1}| + \tilde{D}_{n-1}(N_1, \dots, N_{i_0-1}, \max(N_{i_0}, N_{i_0+1}), N_{i_0+2}, \dots, N_n), \tag{38}$$

where $i_0 = \operatorname{argmin}_i \max(N_i, N_{i+1})$. This definition is a greedy, locally optimal scheme, which optimizes only one step. As it is known from algorithm theory, greedy algorithms do not always produce globally optimal results. By doing only locally optimal steps, we may miss an opportunity for a much better reward in the future if we make a nonoptimal step now. Fortunately, in this case the greedy, locally optimal scheme expressed by Eq. (38) does give the globally optimal result, as we show below.

In any scheme, the first step will be to swap a pair of neighboring segments, let us say segments i and $i + 1$. We do this at the time moment $\max(N_i, N_{i+1})$, and the contribution of these segments to the total dephasing is $|N_i - N_{i+1}|$. After this swapping, we are left with $n - 1$ new segments, one of which is the combination of two original ones. Any initial segment j , where $j \neq i, i + 1$, generates an entangled state after N_j time units, and the combined segment “generates” entanglement after $\max(N_i, N_{i+1})$ time units. If we swap these $n - 1$ segments in any way in D_{n-1} time units, then the total swapping takes $D_n = |N_i - N_{i+1}| + D_{n-1}$ time units. To find the minimal dephasing we simply take the minimum over $i = 1, \dots, n - 1$ of this expression, and recursively apply it for the new segments. If we denote the dephasing random variable corresponding to this scheme as D_n^* , this description translates into the following definition:

$$D_n^*(N_1, \dots, N_n) = \min_{i=1, \dots, n-1} [|N_i - N_{i+1}| + D_{n-1}^*(N_1, \dots, N_{i-1}, \max(N_i, N_{i+1}), N_{i+2}, \dots, N_n)]. \tag{39}$$

The base case of this recursive definition is $D_2^*(N_1, N_2) \equiv D_2(N_1, N_2) = |N_1 - N_2|$. This definition by construction gives the globally minimal number of dephasing time units required to distribute long-distance entanglement if it takes N_i time units for segment i to generate entanglement.

We now have two quantities, the locally optimal one, given by Eq. (38), and the globally optimal one, given by Eq. (39). The former has semantics of swapping the earliest, but may not be globally optimal. The latter is optimal by construction, but does not necessarily correspond to the swapping earliest strategy. It turns out that the two quantities coincide, at least for all $n = 2, \dots, 8$. A straightforward way to check this is to consider all possible inequality relations between N_i . There are $n!$ such relations, which correspond to the permutations of N_i in the following inequality:

$$N_1 \leq \dots \leq N_n. \tag{40}$$

For any given inequality relation between N_i , we can compute both quantities explicitly in terms of N_i . For example, for the relation in Eq. (40), both quantities reduce to the same expression, $\tilde{D}_n = D_n^* = N_n - N_1$. For all other possible relations, we have

$$\tilde{D}_n(N_1, \dots, N_n) = D_n^*(N_1, \dots, N_n), \tag{41}$$

for all $n = 2, \dots, 8$. This can be easily verified with the help of a computer algebra system. Our conjecture is that the statement is valid for all $n \geq 2$, but in this work, we consider repeaters with up to eight segments only, and for such n we have verified this statement directly.

In contrast to the sequential scheme introduced earlier, there is no compact expression for the PGF of the optimal scheme here. Each case will be considered separately in the next sections. Where possible, we present explicit expressions of the PGFs of the quantities in question. The main difficulty is encountered for those schemes with memory cutoff, and hence when including a cutoff, even for smaller repeaters (but $n > 2$), we only consider the fully sequential scheme,

for which we have got the exact expressions. In the following sections, we discuss quantum repeaters for $n = 2, 3, 4$, and 8 segments. Although the case $n = 2$ is rather well known and there is no set of different swapping strategies to choose from in this case, it will be briefly reproduced based on the formalism introduced in this work. The case $n = 3$ is interesting, as it represents the simplest, nontrivial case beyond one middle station, already requiring a choice regarding distribution and swapping strategies (here, in the main text, the focus remains on schemes with an optimal dephasing for parallel distribution; in Appendix E, we discuss the full secret key rate for $n = 3$ including all possible distribution schemes). Finally, the cases $n = 4$ and $n = 8$ are chosen, as they allow for a comparison with “doubling” (see Fig. 2). Larger quantum repeaters with $n > 8$ become increasingly difficult to treat (in terms of the optimized total dephasing). We will later also see that for $n = 8$, without additional methods of quantum error detection or correction, the necessary experimental parameter values in our model become already highly demanding.

2. Two-segment repeater

This is the simplest kind of a quantum repeater. The PGF $G_2(t)$ of $K_2 = \max(N_1, N_2)$ is given by Eq. (36) with $n = 2$ and in this case reads as

$$G_2(t) = \frac{p^2 t (1 + qt)}{(1 - qt)(1 - q^2 t)}. \tag{42}$$

As we noted before, there is only one choice for the dephasing variable, $D_2 = |N_1 - N_2|$ (parallel distribution). In Appendix D, we derive the following expression for the PGF of this variable:

$$\tilde{G}_2(t) = \frac{p^2}{1 - q^2} \frac{1 + qt}{1 - qt}. \tag{43}$$

There we also show that the PGFs of the variables with cutoffs are

$$G_2^{[m]}(t) = \frac{p^2 t (1 + qt - 2(qt)^{m+1})}{(1 - qt)(1 - q^2 t - 2p(qt)^{m+1})},$$

$$\tilde{G}_2^{[m]}(t) = \frac{p}{1 + q - 2q^{m+1}} \frac{1 + qt - 2(qt)^{m+1}}{1 - qt}. \quad (44)$$

It is obvious that we have the same consistency relations as for the sequential distribution scheme:

$$G_2^{[+\infty]}(t) = G_2(t), \quad \tilde{G}_2^{[+\infty]}(t) = \tilde{G}_2(t). \quad (45)$$

3. Three-segment repeater

For three segments, there are various ways how to distribute entanglement. One could use a fully sequential scheme, start at one end and distribute entanglement in concurrent segments. Alternatively, one could consider schemes where pairs of segments generate entanglement in parallel and the remaining segment goes last or, the other way around, it goes first. There are also combined distribution schemes with “overlapping” parallel and sequential distributions. Finally, there are those schemes which attempt to generate entanglement in all segments at once and thereby use different swapping schemes. Among the latter here only the potentially optimal scheme is of interest, as it minimizes the accumulated dephasing, while having the same total waiting time as any other parallel distribution scheme.

However, it could still be the case that a scheme from the other, slower class of schemes performs better in terms of the full secret key rate. This is possible, because there is typically a trade-off between the raw rate and the dephasing or, more generally, the QBER. In particular, the fully sequential distribution scheme is interesting, since its total dephasing becomes minimal, as there is basically always only one segment waiting at every time step. On the other hand, for the fully parallel schemes the raw rate is optimal.

In Appendix E, we present all possible schemes for $n = 3$ and calculate the PGFs of their total waiting and dephasing times. Then we use these results to obtain the secret key rate for each scheme and to compare the different schemes. We also show in the Appendix that the PGF of the optimal dephasing random variable, equivalently defined by Eqs. (38) and (39), reads as

$$\tilde{G}_3^*(t) = \frac{p^3}{1 - q^3} \frac{1 + (q + 2q^2)t - (2q^2 + q^3)t^3 - q^4 t^4}{(1 - qt)(1 - q^2 t)(1 - qt^2)}. \quad (46)$$

It turns out that with regards to the full secret key rate the parallel-distribution optimal-dephasing scheme is indeed optimal in all relevant regimes and especially in the limit of improving hardware parameters, which can be seen in Figs. 22 and 23 for two different memory coherence times. In the same section one can also find a more detailed discussion of the figures. In addition, aiming at the most general treatment of the $n = 3$ case, we also consider the scenario where Alice and Bob measure their qubits immediately, thus suppressing their memory dephasing, and we apply this to all possible schemes. The comparison of these “immediate-measurement” schemes is shown in Figs. 20 and 21, again for two different coherence times. The conclusion remains the same: overall “optimal” is

optimal. However, note that the option with immediate measurements for Alice and Bob only exists when they operate the quantum repeater for the purpose of long-range QKD.³ More advanced quantum repeater applications may require quantum storage for the qubits at each end (user) node. In any case, the memory qubits at each intermediate repeater node are (jointly) measured as soon as possible when the two adjacent segments are filled with an entangled pair (or even later, depending on the particular swapping strategy, but in Appendix E, we only consider swap-as-soon-as-possible schemes that minimize the dephasing).

The above discussion leads us to the conclusion that there are three basic properties that a quantum repeater protocol (unassisted by additional quantum error detection or correction) should exhibit: distribute the entangled states in each segment in parallel, swap the initially distributed states as soon as possible, and avoid parallel storage of already distributed pairs as much as possible. It is obvious that all these three “rules” cannot be fully obeyed at the same time. However, our optimal scheme has the optimal balance with regards to these rules for three segments. We conjecture that this also holds true for larger $n > 3$ -segment repeaters.

4. Four-segment repeater

Of particular interest to us is the case of a four-segment repeater which is commonly operated via “doubling.” Here we are now able to discuss more general schemes, especially those that would always swap as soon as possible, unlike doubling where the second and third segments may not be immediately connected even when they are both ready. Overall there are many more schemes than in the previous $n = 3$ case, and here for $n = 4$ we focus on the parallel-distribution schemes. All these schemes (without cutoff) have identical $K_4 = \max(N_1, N_2, N_3, N_4)$, whose PGF is given by Eq. (36) for $n = 4$. The dephasing variable D_4 and its PGF become different for different schemes. One such scheme, the common “doubling,” is illustrated in Fig. 2, where we first swap the pairs of segments 1, 2 and 3, 4 independently and then swap the two larger segments. Note that the swappings will typically take place at different moments in time - one pair of segments will usually swap earlier than the other. The state of the faster pair that goes into the final swapping operation is the state of these segments after their connection and at the moment when the final swapping is done, and so the state has been subject to a corresponding memory dephasing. For example, if the swapping of segments 1 and 2 is done first, the state of the distributed state over segments 1 and 2 just after the swapping is $\hat{\rho}_{12} = \mathcal{S}(\hat{\rho}_{12} \otimes \hat{\rho}_{34})$. If k time units later segments 3 and 4 swap, producing the state $\hat{\rho}_{58} = \mathcal{S}(\hat{\rho}_{56} \otimes \hat{\rho}_{78})$, the former state becomes $\Gamma_{k\alpha}(\hat{\rho}_{12})$, and the state distributed over the whole repeater is

$$\hat{\rho}_{18} = \mathcal{S}(\Gamma_{k\alpha}(\mathcal{S}(\hat{\rho}_{12} \otimes \hat{\rho}_{34})) \otimes \mathcal{S}(\hat{\rho}_{56} \otimes \hat{\rho}_{78})), \quad (47)$$

³For QKD applications, there is another variation that would indeed allow to achieve higher secret key rates, namely, when Alice and Bob send their signals at a high clock rate and the memory stations can locally decide how to process the arriving qubits [29].

instead of just $\hat{\rho}_{18} = \mathcal{S}(\mathcal{S}(\hat{\rho}_{12} \otimes \hat{\rho}_{34}) \otimes \mathcal{S}(\hat{\rho}_{56} \otimes \hat{\rho}_{78}))$. Again, as before, we omitted any extra factors that depend on the number of spins subject to dephasing in a single repeater segment. So, Fig. 2 shows just a workflow of swapping operations, while the exact expressions should be adjusted according to the respective time differences. The dephasing variable D_4 in this doubling scheme is defined as follows:

$$D_4^{\text{dbl}} = |N_1 - N_2| + |N_3 - N_4| + |\max(N_1, N_2) - \max(N_3, N_4)|. \quad (48)$$

The first two terms are due to the possible time difference for generating entangled states within each pair of segments. The last term is due to the time difference between the pairs [e.g., the difference of the two maxima is k time steps in Eq. (47)]. Note that this particular form of D_4^{dbl} is consistent with the commonly used ‘‘doubling’’ where the initial distributions happen in parallel, but the swapping strategy is fixed and sometimes disallows to swap as soon as possible. In Appendix D, we derive the PGF of this random dephasing variable,

$$\tilde{G}_4^{\text{dbl}}(t) = \frac{p^4 P_4^{\text{dbl}}(q, t)}{1 - q^4 Q_4^{\text{dbl}}(q, t)}, \quad (49)$$

where the numerator and denominator are given by

$$\begin{aligned} P_4^{\text{dbl}}(q, t) &= 1 + (q^2 + 3q^3)t + (3q + 3q^2 - q^5)t^2 \\ &\quad - (q^3 - q^5)t^3 + (q^3 - 3q^6 - 3q^7)t^4 \\ &\quad - (3q^5 + q^6)t^5 - q^8t^6, \\ Q_4^{\text{dbl}}(q, t) &= (1 - q^2t)(1 - q^3t)(1 - qt^2)(1 - q^2t^2). \end{aligned}$$

The dephasing variable corresponding to the iterated scheme as shown in Fig. 3 differs from that of the doubling scheme. In the iterative scheme, we first distribute entanglement over segments 1 and 2, then extend it over segment 3, and finally over segment 4. Note that the figure can be understood to illustrate both sequential distribution and iterated swapping. In the sequential distribution scheme, we would start to generate entanglement in each segment only when all previous segments (e.g., from left to right) have successfully generated entanglement. In the iterated swapping scheme, all segments may start simultaneously (parallel distribution), thus increasing the chances to swap sooner, but also the number of qubits potentially stored in parallel. The variable D_4^{itr} for this scheme is

$$D_4^{\text{itr}}(N_1, N_2, N_3, N_4) = |N_1 - N_2| + |\max(N_1, N_2) - N_3| + |\max(N_1, N_2, N_3) - N_4|.$$

The PGF of this random variable is rather large and reads as

$$\tilde{G}_4^{\text{itr}}(t) = \frac{p^4 P_4^{\text{itr}}(q, t)}{1 - q^4 Q_4^{\text{itr}}(q, t)}, \quad (50)$$

where the numerator and denominator are given by

$$\begin{aligned} P_4^{\text{itr}}(q, t) &= 1 + 3q^3t + (4q^2 - q^4 - 2q^5)t^2 \\ &\quad + (q - q^2 - 3q^3 - 6q^4 + 2q^5 + q^6)t^3 \\ &\quad + (-2q^2 - 5q^3 + q^4 + 2q^5 - q^6 - 3q^7)t^4 \\ &\quad + (-2q^2 + 4q^4 - 4q^6 + 2q^8)t^5 \\ &\quad + (3q^3 + q^4 - 2q^5 - q^6 + 5q^7 + 2q^8)t^6 \\ &\quad + (-q^4 - 2q^5 + 6q^6 + 3q^7 + q^8 - q^9)t^7 \\ &\quad + (2q^5 + q^6 - 4q^8)t^8 - 3q^7t^9 - q^{10}t^{10}, \\ Q_4^{\text{itr}}(q, t) &= (1 - qt)(1 - q^2t)(1 - q^3t)(1 - qt^2) \\ &\quad \times (1 - q^2t^2)(1 - qt^3). \end{aligned}$$

We present an example for another, mixed swapping strategy in Appendix G.

For the dephasing random variable D_4^* , corresponding to the optimal swapping scheme given by Eq. (39) for $n = 4$, we derive the following PGF:

$$\tilde{G}_4^*(t) = \frac{p^4 P_4^*(q, t)}{1 - q^4 Q_4^*(q, t)}, \quad (51)$$

where the numerator and denominator read as

$$\begin{aligned} P_4^*(q, t) &= 1 + (q + 2q^2 + 3q^3)t + (q + 2q^2 + q^4)t^2 \\ &\quad - (3q^2 + 4q^3 + 4q^4)t^3 - (4q^5 + 4q^6 + 3q^7)t^4 \\ &\quad + (q^5 + 2q^7 + q^8)t^5 + (3q^6 + 2q^7 + q^8)t^6 + q^9t^7, \\ Q_4^*(q, t) &= (1 - qt)(1 - q^2t)(1 - q^3t)(1 - qt^2)(1 - q^2t^2). \end{aligned}$$

5. Eight-segment repeater

As before, again all parallel-distribution schemes (without cutoff) have identical total waiting times, $K_8 = \max(N_1, \dots, N_8)$, whose PGF is given by Eq. (36) for $n = 8$. For the dephasing variable, there are many more possibilities now. We shall consider and compare five different schemes—the doubling and the optimal schemes, and three less important schemes, which nevertheless exhibit an interesting behavior. The somewhat less important ones are described and discussed in Appendix G.

The optimal dephasing D_8^* is defined equivalently by Eqs. (38) and (39) for $n = 8$ and the doubling dephasing D_8^{dbl} is defined recursively as

$$\begin{aligned} D_8^{\text{dbl}}(N_1, \dots, N_8) &= D_4^{\text{dbl}}(N_1, \dots, N_4) + D_4^{\text{dbl}}(N_5, \dots, N_8) \\ &\quad + |\max(N_1, \dots, N_4) \\ &\quad - \max(N_5, \dots, N_8)|, \end{aligned} \quad (52)$$

with D_4^{dbl} defined as in Eq. (48). The comparison of the five different schemes can be found in Appendix G. In this Appendix, Appendix G, we present some figures showing the ratios between the average dephasing of the four sub-optimal schemes and the optimal scheme, with and without exponentiation. We can then compare the relative positions of the curves

in Fig. 26 with those of the curves of the ratios

$$\frac{\mathbf{E}[D_8^{\text{sch}}]}{\mathbf{E}[D_8^{\text{opt}}]} = \frac{\tilde{G}_8^{\text{sch}}(1)}{\tilde{G}_8^{\text{opt}}(1)}, \quad (53)$$

which are shown in Fig. 27. Looking at the two figures, we see that

$$\mathbf{E}[D_8^{\text{dbl}}] > \mathbf{E}[D_8^{44}], \quad \mathbf{E}[e^{-\alpha D_8^{\text{dbl}}}] < \mathbf{E}[e^{-\alpha D_8^{44}}]. \quad (54)$$

This behavior is in full agreement with the properties of the exponential function: if $x > y \geq 0$ and $\alpha > 0$, then $e^{-\alpha x} < e^{-\alpha y}$. However, for the other pair of schemes, we have

$$\mathbf{E}[D_8^{242}] > \mathbf{E}[D_8^{2222}], \quad \mathbf{E}[e^{-\alpha D_8^{242}}] > \mathbf{E}[e^{-\alpha D_8^{2222}}]. \quad (55)$$

Nonetheless there is no contradiction here. This is a known property of nonlinear functions of random variables. This property can be observed even in the simplest case of random variables X and Y each taking two values only. One can easily construct an example such that $\mathbf{E}[X] > \mathbf{E}[Y]$ and $\mathbf{E}[e^{-\alpha X}] > \mathbf{E}[e^{-\alpha Y}]$. However, the inequalities (55) show that it is not necessary to consider artificial constructions. This property can be observed for simple and natural schemes.

The important conclusion is that the optimal scheme by construction minimizes $\mathbf{E}[D]$, but to have the highest fidelity of the distributed state we need to maximize $\mathbf{E}[e^{-\alpha D}]$. For an ordinary nonnegative function $f(x)$ and a positive parameter $\alpha > 0$ the minimum of $f(x)$ is the maximum of $e^{-\alpha f(x)}$ and vice versa, but for random variables, this is not necessarily true. Strictly speaking, in general, we know only the scheme that minimizes $\mathbf{E}[D]$, but not the scheme that maximizes $\mathbf{E}[e^{-\alpha D}]$. The two schemes seem to be identical, but there is no strict proof of this statement. We have to rely on evidence based on computing the properties of some schemes explicitly and comparing them. For the examples for $n = 8$ given in this section and in the Appendix, we see that dividing the exponentiated dephasing of all other schemes by that of the optimal scheme gives a number smaller than one, whereas the same ratios without exponentiation give a number greater than one. Thus minimal dephasing corresponds to minimal dephasing errors, and the optimal dephasing scheme exhibits the smallest fraction of dephasing errors.

To summarize, our optimization of the secret key rates obtainable with different distribution and swapping strategies is based on three steps. First, we can rely upon the proof of the minimal dephasing variable for up to $n = 8$ segments given in Sec. IV D 1 assuming parallel initial distributions (it is already nontrivial to extend this proof to larger $n > 8$). Second, in order to compare the average dephasing errors in the final density operators, we need to consider the average dephasing exponentials for the different schemes. Finally, in order to assess the optimality of the secret key rate over all possible schemes, we have to take into account also those schemes where the initial distributions no longer occur in parallel which generally leads to smaller raw rates, but at the same time can result in a smaller dephasing by (partially) avoiding parallel storage. For the first nontrivial case beyond a single middle station, we have explicitly gone through all these three steps, namely, for the case of a three-segment repeater with two intermediate stations (Appendix E), and found that “optimal” is optimal. For larger repeaters beyond eight

segments, $n > 8$, we conjecture that our “optimal” scheme also gives the best secret key rate. This includes conjecturing that our minimized dephasing is minimal also for $n > 8$, that it minimizes the dephasing errors in the final density operator, and that overall the dephasing-optimized parallel-distribution approach is superior to any partially or fully sequential distribution scheme. Especially the last point cannot be taken for granted. In Appendix F, we present some rate calculations for $n = 8$ where, beyond a certain distance, “optimal” can be beaten by a sequential scheme. However, there we allow for immediate measurements at an end node only for the sequential scheme (for which this is easy to include), but not for “optimal”; a comparison which is slightly unfair and also only relevant for QKD applications. In the case of nonimmediate-measurement schemes including potential beyond-QKD applications, “optimal” remains optimal.

V. SECRET KEY RATE ANALYSIS

A useful and practically relevant figure of merit for quantifying a quantum repeater’s performance is its secret key rate in long-range QKD, which determines the amount of secret key generated in bits per channel use or second. As briefly reviewed in Sec. III B, the secret key rate consists of two parts: the raw rate or yield and the secret key fraction. The former quantifies how long it takes to send a raw quantum bit or to (effectively) generate entanglement, independent of the quality of the final state; the latter then determines the average amount of secret key that can be extracted from a single raw bit, depending on the particular QKD protocol chosen and including the corresponding procedures for the classical postprocessing.

Here we will focus on the asymptotic BB84 secret key rate $S = Rr = r/T$ with one-way postprocessing. In the most general scenario of long-range memory-assisted QKD, i.e., including a finite swapping probability a and a memory cutoff parameter m , it is given by

$$S(p, a, m) = \frac{1 - h(\bar{e}_x(p, a, m)) - h(\bar{e}_z(p, a, m))}{T(p, a, m)}, \quad (56)$$

where h is the binary entropy function, T the average number of steps needed to successfully distribute long-distance entanglement, and e_x, e_z are the QBERs of Eq. (24). The probability of successful entanglement generation in a single attempt in a single elementary segment is p , as introduced in Sec. II A. The denominator of S , $T = \mathbf{E}[K]$, is basically the total raw waiting time of the repeater which generally depends on p and a where a is a finite success probability of the entanglement swapping using the same notation as in Refs. [35,36] (where it was shown how to compute [35] and optimize [36] $T = \mathbf{E}[K]$ for arbitrary a). The dependency on the cutoff parameter m means: the smaller m becomes, the longer it takes to distribute an entangled state. The numerator of S , r , generally also depends on p , a , and m through the QBERs. Recall that we have to take the averages here, $\bar{e}_z = e_z$ and \bar{e}_x obtainable via $\mathbf{E}[e^{-\alpha D_n}]$. A smaller m can lead to a higher state quality with a smaller total dephasing and thus to a larger secret key fraction r . It is generally hard to optimize S over general p , a , and m . Our approach here is based on the simplifying (and experimentally still relevant) assumption $a = 1$ (deterministic

entanglement swapping) and the idea that the highest secret key rates will be obtainable with the fastest schemes (parallel distributions minimizing the total waiting time) and, among these, with those that swap entanglement as soon as possible (minimizing the total dephasing time, see Sec. IV D 1). While for a two-segment repeater the cases of deterministic and non-deterministic swapping can be treated similarly, for repeater chains beyond a single middle station ($n > 2$) our results for optimizing distribution and swapping strategies only hold for the deterministic swapping case. Using the results of all previous sections, the secret key rate can then be calculated. Thus, in what follows, we always have $a = 1$.

The above secret key rate S is expressed in terms of bits per channel use. For a rate per second, the average total number of distribution attempts T must be multiplied with the duration of a single attempt in seconds, i.e., the elementary time unit $\tau = L_0/c_f$. Note that a single attempt or channel use is uniquely defined only for direct channel transmission in a point-to-point link, whereas the channel in a quantum repeater is used directly only between neighboring memory stations. Since our model always assumes that the interfaces at each station connect a single channel (to the left or to the right) with a single memory qubit (unit memory “buffer”), those channel segments that belong to already successfully distributed pairs remain unused until new attempts in these segments will be started (e.g., when the memory cutoff has been exceeded or when a long-distance pair has been finally created). Nonetheless, at every attempt, we shall always count a full channel use over the entire distance despite the growing number of unused channel segments during memory-assisted long-distance entanglement distribution. Thus, strictly speaking, we underestimate the secret key rate per channel use and one could continue distributing pairs in all channel segments provided sufficient memory qubits are available.

The parameter values as given in Table I have been used to obtain the quantitative results discussed in this section. Most parameters there have been introduced in the previous sections in the context of our physical model. The resulting probability to distribute entanglement over one link in terms of the parameters of Table I now includes a zero-distance link-coupling efficiency

$$p(L_0) = p_{\text{link}} e^{-\frac{L_0}{L_{\text{att}}}}, \quad (57)$$

with $p(0) = p_{\text{link}}$ and where $p_{\text{link}} = \eta_c \eta_d \eta_p$ incorporates various efficiencies of the experimental hardware independent of the channel transmission itself, especially wavelength conversion, fiber coupling, preparation, and detector efficiencies.

In the context of our statistical and physical model, the memory coherence time τ_{coh} in Table I, an experimentally determined parameter that describes the average speed of the memory dephasing, can be converted into a (dimensionless) effective coherence time in units of the repeater’s elementary time unit, τ_{coh}/τ . Equivalently, we can say that the (number of) dephasing time (steps) D_n is to be multiplied with an elementary time τ before it can be divided by τ_{coh} in $\mathbf{E}[e^{-D_n \tau/\tau_{\text{coh}}}]$. In any case, we absorb both τ and τ_{coh} in our dimensionless α dephasing parameter,

$$\alpha(L_0) = \frac{\tau}{\tau_{\text{coh}}} = \frac{L_0}{c_f \tau_{\text{coh}}}. \quad (58)$$

TABLE I. Experimental parameter values used to calculate secret key rates. The star symbols * allow for various choices. The exact choices vary for each experimental platform. Some of the “improved values” are the ideal values which allow to consider idealized, fundamental scenarios such as “channel-loss-only” or “channel-loss-and-memory-dephasing-only” (for which we may also set $p_{\text{link}} = 1$).

Constant	Meaning	Current value	Improved value
a	Swapping probability	1	1
τ_{coh}	Coherence time	0.1 s	10 s
μ	Gate depolarization (Bell measurement)	0.97	1
μ_0	Initial state depolarization	0.97	1
F_0	Initial state fidelity (dephasing)	1	1
L_{att}	Attenuation length	22 km	22 km
n_r	Index of refraction	1.44	1.44
η_p	Preparation efficiency	*	*
η_c	photon-fibre coupling efficiency \times wavelength conversion	*	*
η_d	Detector efficiency	*	*
$p_{\text{link}} := \eta_c \cdot \eta_d \cdot \eta_p$	Total efficiency	0.05	0.7

Thus α can be referred to as an inverse effective coherence time. Note that in order to count the dephasing times appropriately in a specific protocol, we may have to add an extra factor of 2 (depending on the number of spins dephasing at each time step in a certain elementary or extended segment) and a constant dephasing term $\sim 2n$ that takes into account memory dephasing that occurs even when the first distribution attempt in a segment succeeds. Any missing factors in the dephasing can be reinterpreted in terms of α or τ_{coh} , e.g., a missing factor of 2 corresponds to a coherence time twice as big.

In Table I, two sets of current and improved parameter values are listed, which specifically refer to τ_{coh} and p_{link} for which we choose 0.1 s or 10 s and 0.05 or 0.7, respectively. The other state and gate fidelity parameters will be either set to unity or close to but below one (in some of the following plots we will also treat them as a free parameter). We will see that in memory-assisted QKD without additional quantum error detection or correction, the fidelity parameters must always be above a certain threshold value which (obviously) grows with the number of stations (and which generally depends on the particular QKD protocol and the classical postprocessing method).

To compare the performance of each repeater protocol with a direct point-to-point link over the total distance L , we will use the PLOB bound [46], which is given by

$$S^{\text{PLOB}}(L) = -\log_2(1 - e^{-\frac{L}{L_{\text{att}}}}). \quad (59)$$

It represents an upper bound on the number of secret bits that can be shared per channel use. For example, for $e^{-\frac{L}{L_{\text{att}}}} = 1/2$ corresponding to $L = 15$ km, we have $S^{\text{PLOB}} = 1$, and so at most one secret bit can be distributed per channel use (per mode) independent of the optical encoding. It will also be useful to consider an upper bound on the number of secret

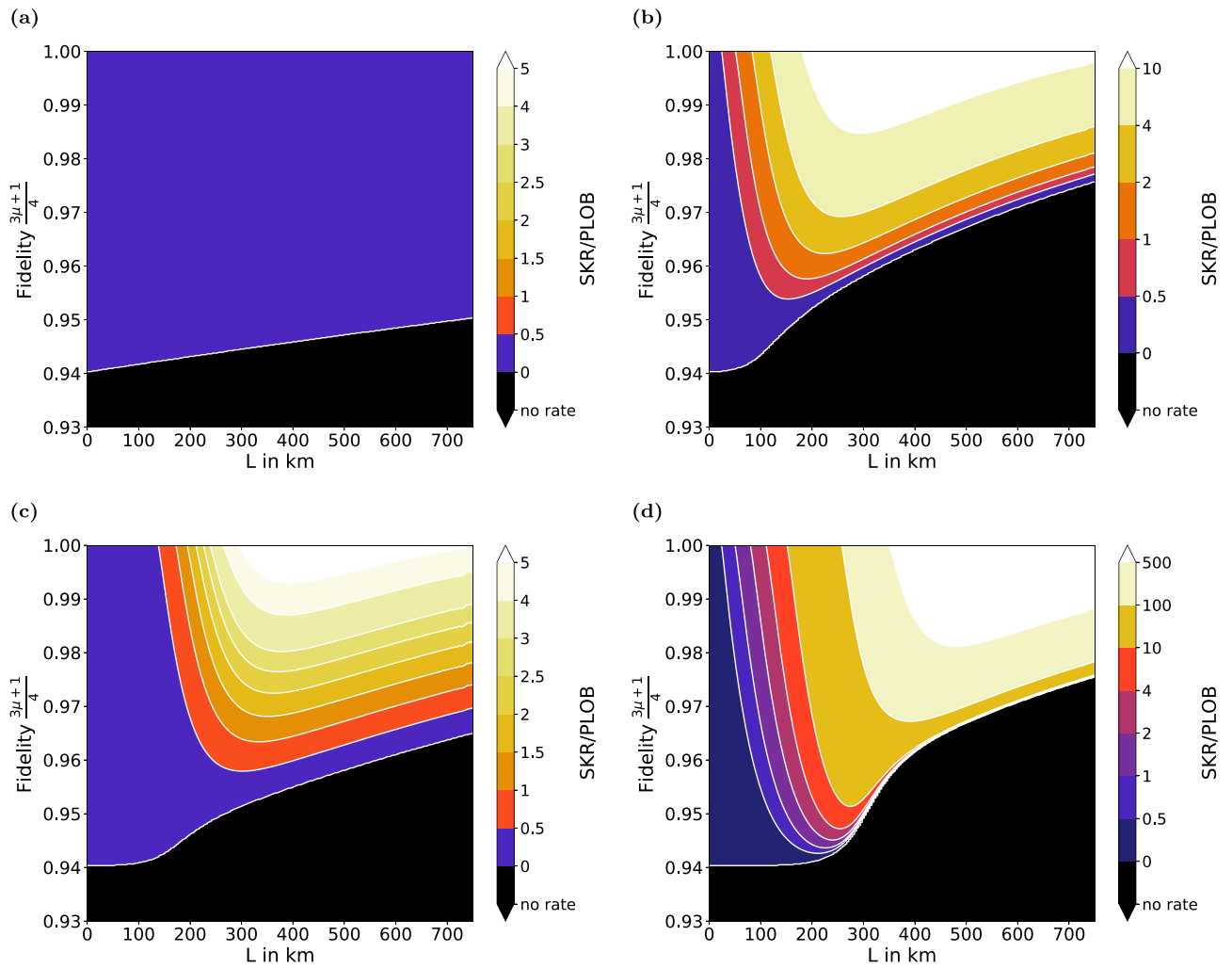


FIG. 4. Contour plots illustrating the minimal fidelity requirements to overcome the PLOB bound by a two-segment repeater with different parameters: (a) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.05$, $m = 10$; (b) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.7$, $m = 50$; (c) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.05$, $m = 3000$; and (d) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.7$, $m = 5000$. In all contour plots, $\mu = \mu_0$ and $F_0 = 1$ has been used.

bits that can be shared with the help of a quantum repeater [51],

$$S^{\text{PLOB,QR}}(L_0) = -\log_2(1 - e^{-\frac{L_0}{L_{\text{att}}}}), \quad (60)$$

corresponding to the PLOB bound for one segment (in the case of equal segment lengths L_0). For a point-to-point link, $n = 1$ with $L = L_0$, we thus use the notation $S^{\text{PLOB}} = S^{\text{PLOB,QR}}$. The rates we will focus on first in the following are to be understood as secret key rates per channel use. Later we shall also discuss secret key rates per second.

A. Two-segment repeater

Let us start with the rates for the simplest case: a two-segment quantum repeater with one middle station. We shall only consider one scheme, the “optimal” scheme, with and without a memory cutoff. First, we address the question whether and when it is possible to overcome the PLOB bound with a two-segment repeater given the (current and improved) parameter values from Table I. We stick to $F_0 = 1$ and, for illustrative clarity, we set $\mu = \mu_0$ (while, first, μ is not fixed).

Physically, this means that the repeater states when initially distributed in each segment and then manipulated at the middle station for the Bell measurement are subject to the same depolarizing error channels (and there is no extra initial dephasing). The cutoff parameter m is chosen most appropriately such that the final secret key rate is close to optimal over the entire range.

In Fig. 4, one can see various contour plots of the secret key rate. For convenience, we translated the error parameter μ into a fidelity, $F = (3\mu + 1)/4$. The plots clearly indicate the minimal fidelity values below which the rates drop below the PLOB bound or even to zero rates, for different total repeater distances L . The resulting contours are color-coded such that a particular color represents the secret key rate to be, e.g., twice the rate of the PLOB bound. Thus one can see that in certain parameter regimes it becomes impossible to beat the PLOB bound with a two-segment repeater. However, if both the memory coherence time τ_{coh} and the link efficiency p_{link} take on their improved values, it is possible to reach secret key rates as high as 500 times the rate of the PLOB bound, and beyond, in a certain distance regime.

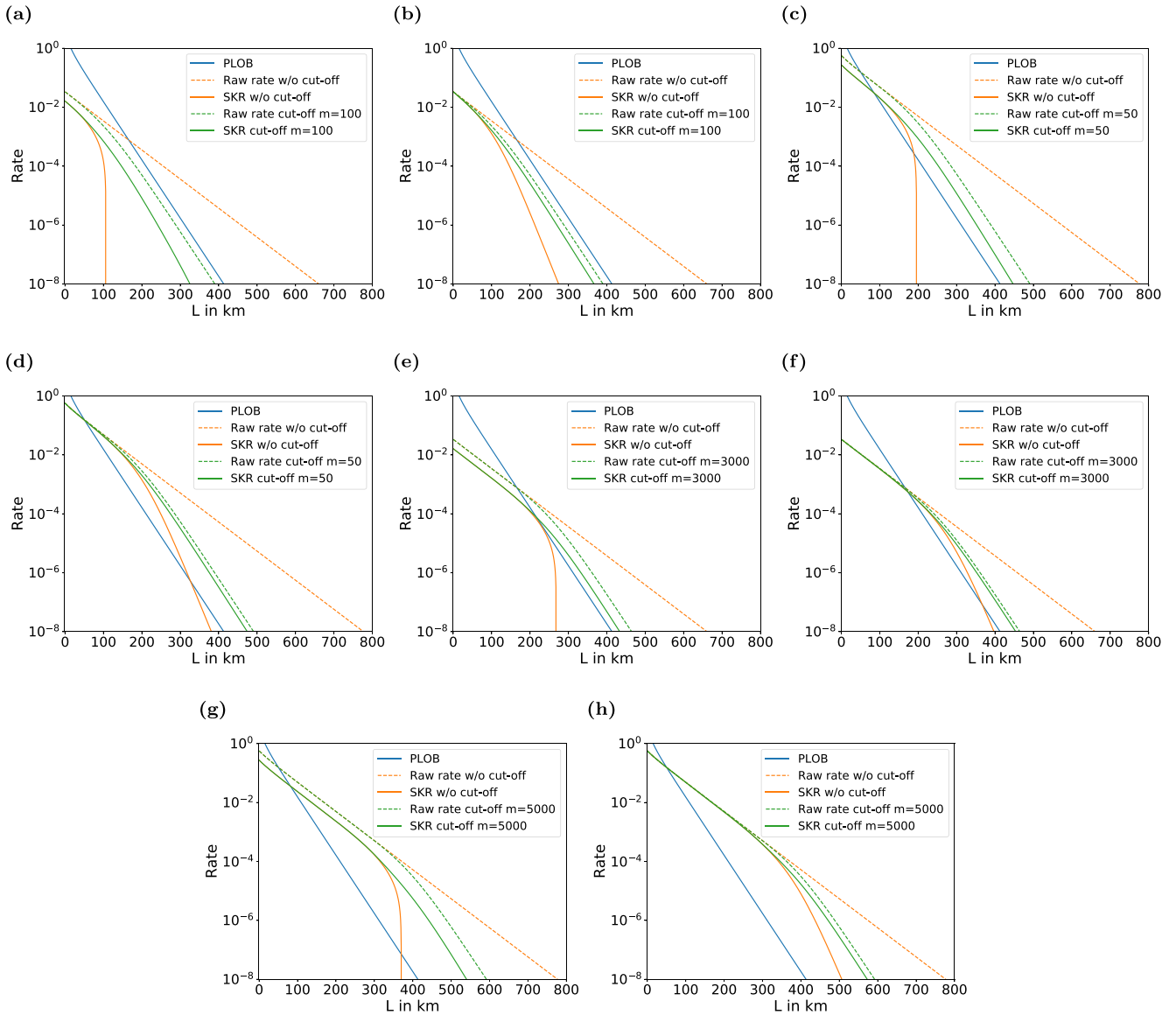


FIG. 5. Rates (secret key or raw) for a two-segment repeater over distance L for different experimental parameters: (a) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 0.97$; (b) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 1$; (c) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 0.97$; (d) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 1$; (e) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 0.97$; (f) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 1$; (g) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 0.97$; and (h) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 1$.

In Fig. 5, we show the resulting secret key rates for the experimental parameters from Table I, for both the scheme with and without a memory cutoff. This time the error parameter $\mu = \mu_0$ is fixed, and it either takes on its “current” or its “improved” (ideal) value. For comparison, as a reference, we also included the raw rates in each case. The loss scaling of the rates in all schemes is, as expected, proportional to $p_{\text{link}} e^{-\frac{L}{2L_{\text{att}}}} = p_{\text{link}} \sqrt{e^{-\frac{L}{L_{\text{att}}}}}$ (corresponding to a linear decrease with distance due to the log scale representation). The effect of the different experimental parameter values is clearly visible. The choice of $p_{\text{link}} = 0.05$ or $p_{\text{link}} = 0.7$ determines the offset along the y axis (rate axis) at zero distance. A higher p_{link} allows to cross the PLOB bound at a smaller distance. Note that the PLOB bound itself can arbitrarily exceed the value of one secret bit towards zero distance; in our schemes we

always distribute qubits and so one secret bit per channel use is the maximum (and depending on the number of modes to encode the photonic qubits there could be extra factors, “per mode”). The choice of $\tau_{\text{coh}} = 0.1$ s or $\tau_{\text{coh}} = 10$ s determines when (at which distance) the (negative) slope of the secret key rate increases such that the repeater switches from a $\sqrt{e^{-\frac{L}{L_{\text{att}}}}}$ to a $e^{-\frac{L}{L_{\text{att}}}}$ (PLOB-like) scaling, or even worse. This effect is an effect of the memory dephasing that occurs even when $\mu = \mu_0 = 1$. If, in addition, $\mu = \mu_0 = 0.97 < 1$, the secret key rates can drop abruptly down to zero, since then the QBERs have nonzero contributions both in e_z and e_x , see Eq. (24). Note that this effect happens also when either of the two parameters, μ or μ_0 , drop below one, i.e., when either the gates or the initial states become imperfect. Also note that nonunit μ or μ_0 in addition lead to an increased y -axis offset

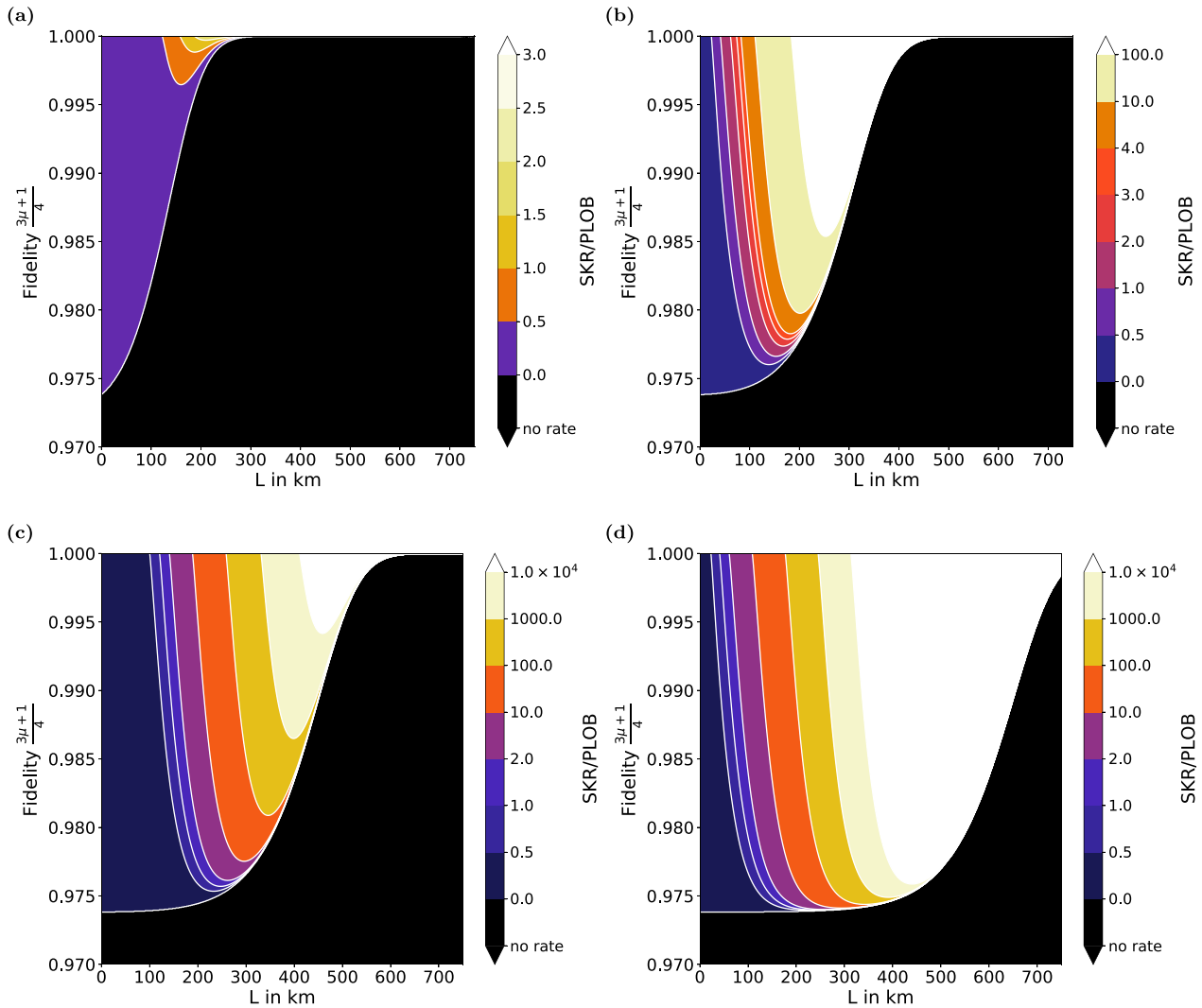


FIG. 6. Contour plots illustrating the minimal fidelity requirements to overcome the PLOB bound by a four-segment repeater for different parameters: (a) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.05$; (b) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.7$; (c) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.05$; and (d) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.7$. In all contour plots, $\mu = \mu_0$ and $F_0 = 1$ has been used.

which will become more apparent for larger repeaters with larger n .

However, a memory cutoff can significantly change the picture, and it can increase the achievable distance compared to the scheme without a cutoff (compare the solid yellow with the solid green curves in Fig. 5). More specifically, beyond distances when the rates of the no cutoff scheme drop dramatically, the cutoff scheme still scales proportional to the PLOB bound. Note that for the scheme with a cutoff, even the raw rates (dashed green curves) can switch from an $L/2$ to an L scaling (like PLOB), because a finite cutoff value “simulates” an imperfect memory in the raw rate (whose loss scaling resembles the scaling without a quantum memory, i.e., that of the PLOB bound, in the limit of $m = 1$) [41]. Again, one can also see that with “current” parameter values, see Fig. 5(a), it is impossible to beat the PLOB bound [here even when $\mu = \mu_0 = 1$, see Fig. 5(b)], but with improving values for the coherence time and the link efficiency, it becomes possible. This holds even when only one of the two parameters, p_{link} or τ_{coh} , is improved, as long as we can cross PLOB at a

sufficiently small distance or maintain the repeater’s slope for sufficiently long, respectively. In the next section we will turn to a four-segment repeater (a three-segment repeater is discussed in great detail in Appendix E).

B. Four-segment repeater

As we have seen in Sec. IV D 4, there are various swapping strategies possible for a four-segment repeater in contrast to a simple two-segment repeater. Our conjecture is (see also Appendix E for the case $n = 3$) that the “optimal” scheme is optimal in the regimes of increasingly good hardware parameters. Thus let us first again focus on the minimal fidelities to overcome the PLOB bound for this scheme, similar to our analysis for two segments, but now without cutoff only. The results are shown in Fig. 6. It becomes apparent that now a much higher fidelity or equivalently μ is needed, but in turn also much higher secret key rates, 10^4 -times the PLOB rate and beyond, are possible. Since we have $n = 4$ now, nonunit μ values have a stronger impact on the QBERs, see Eq. (24). At

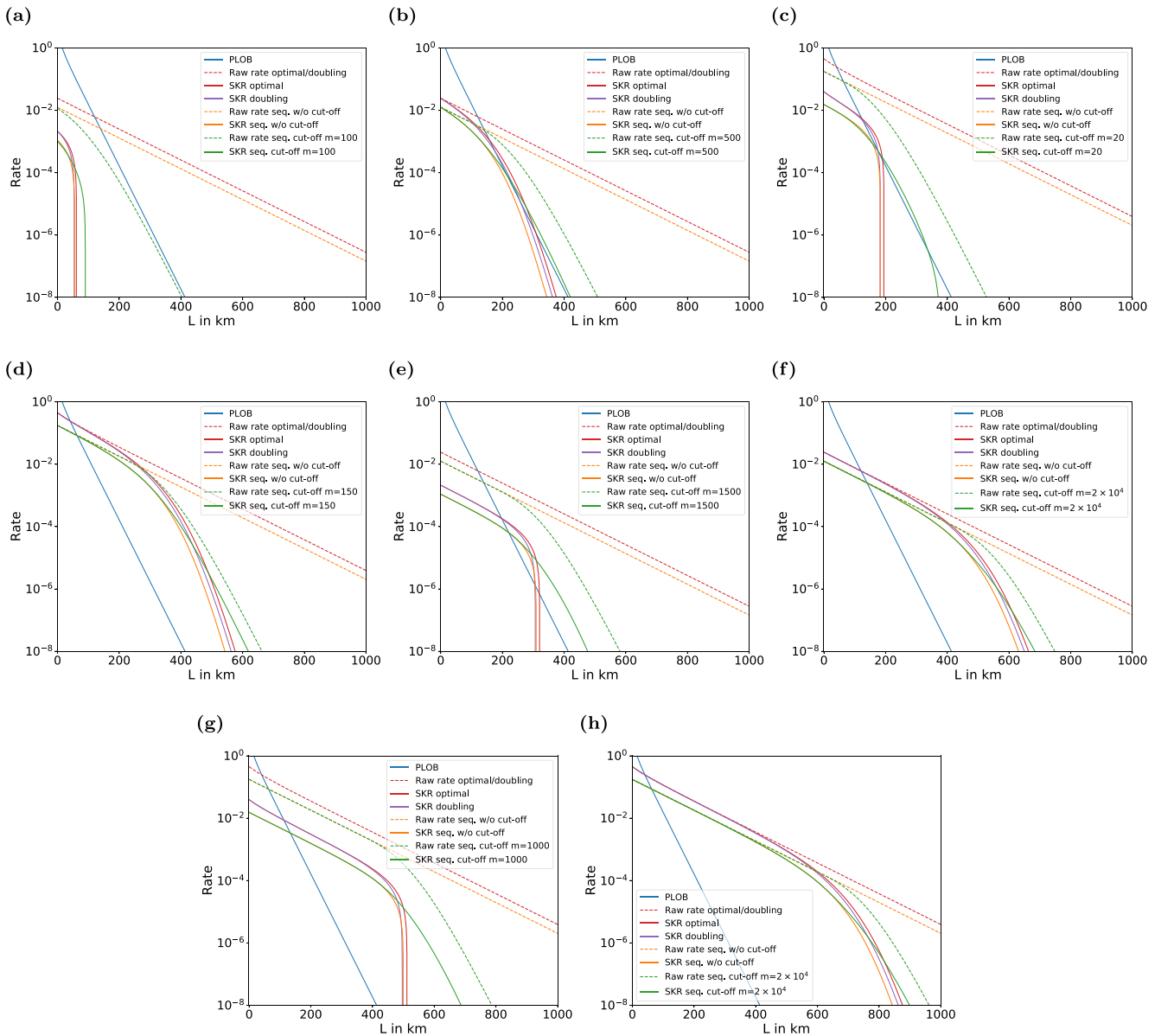


FIG. 7. Rates (secret key or raw) for a four-segment repeater over distance L for different experimental parameters: (a) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 0.97$; (b) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 1$; (c) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 0.97$; (d) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 1$; (e) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 0.97$; (f) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 1$; (g) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 0.97$; and (h) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 1$.

the same time, however, the loss scaling becomes proportional to $p_{\text{link}} e^{-\frac{L}{4l_{\text{att}}}} = p_{\text{link}} \sqrt[4]{e^{-\frac{L}{l_{\text{att}}}}}$. Furthermore, note that a different scaling of the contours is observable, due to the lack of a memory cutoff.

Next, we consider the secret key rates for a particular choice of the experimental parameters including $\mu = \mu_0$ according to Table I. Besides the “optimal” scheme, now we also include the sequential and the doubling schemes in the rate analysis (sequential/iterative swapping together with sequential distributions and doubling with parallel distributions). In Fig. 7, one can see the PLOB bound and the secret key rates for the sequential scheme with and without a cutoff, for the doubling scheme and for the optimal scheme (both without a

cutoff). In addition, again the raw rates are shown as a reference, and the corresponding three dashed curves are the raw rates for (equivalently) doubling and “optimal,” and for the sequential scheme with and without cutoff. Compared to the previous two-segment repeater, it is now easier to overcome the PLOB bound, but the crossing happens at longer distances, since the four-segment repeater starts with a lower rate at $L = 0$ km.

C. Eight-segment repeater

In comparison with the usual treatment of quantum repeaters via doubling the links at each repeater level, the next

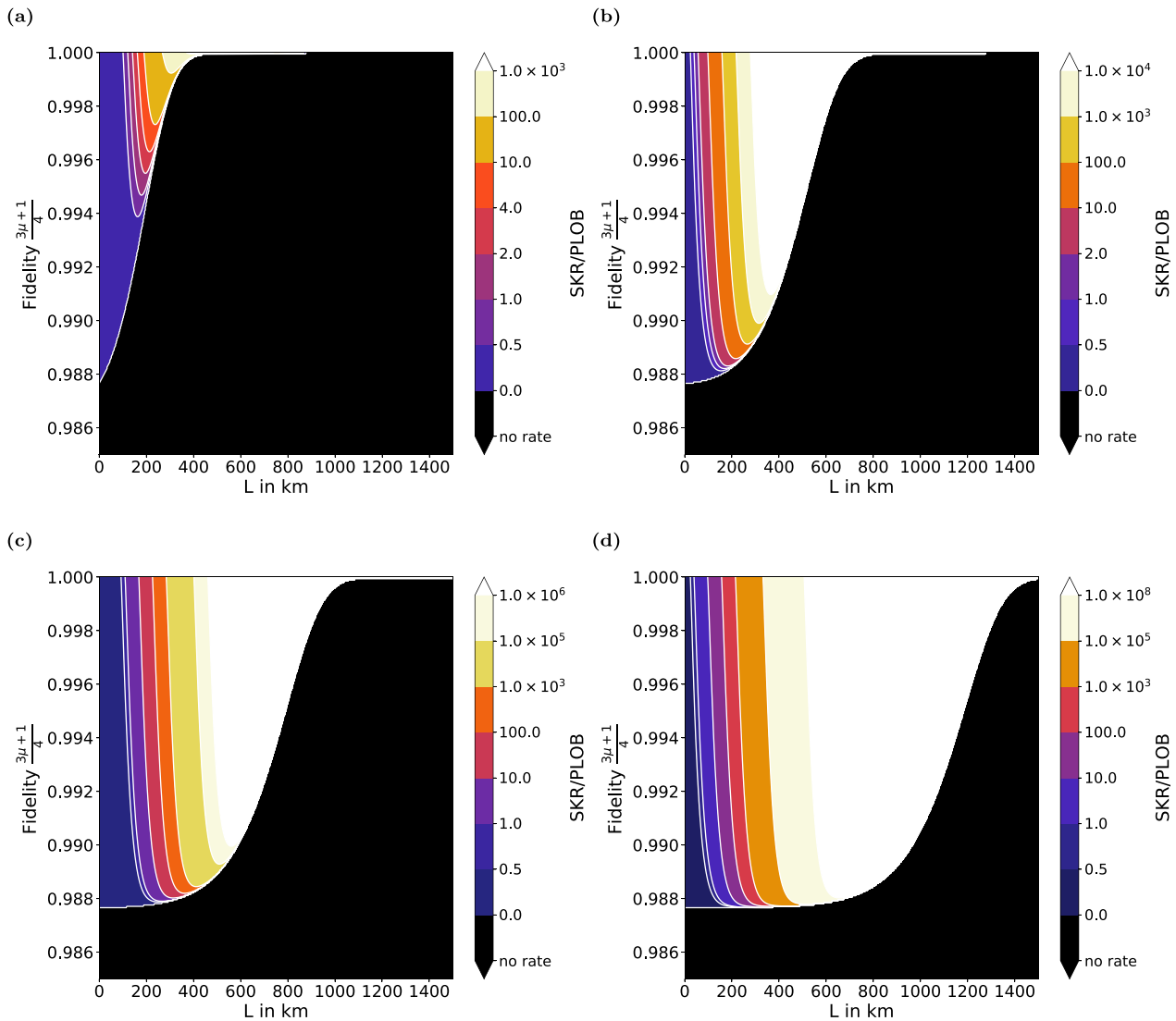


FIG. 8. Contour plots illustrating the minimal fidelity requirements to overcome the PLOB bound by an eight-segment repeater for different parameters: (a) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.05$; (b) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.7$; (c) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.05$; and (d) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.7$. In all contour plots, $\mu = \mu_0$ and $F_0 = 1$ has been used.

logical step is to consider an eight-segment repeater. For eight segments, there is an increasing number of possible distribution and swapping strategies, and for the swapping we have discussed this in more detail in Sec. IV D 5. Here we will only consider the sequential, the doubling, and the optimal schemes (the former one with sequential distributions, the latter two with parallel distributions). Again, in Fig. 8, we present limitations on the error parameter μ to overcome the PLOB rate at different distances. The regions are color-coded as before. Compared to the limits observed for a two-segment repeater they exhibit a different behavior now, but this is again due to the fact that we do not consider a cutoff scheme here. The requirements for the fidelity or μ are higher, but this was expected, since the secret key fraction includes terms $\propto \mu^{2n-1}$, again setting $\mu_0 = \mu$. Nevertheless, for sufficiently high fidelities, the attainable secret key rates are much higher

than for any of the previously considered repeater schemes, becoming as high as 10^8 times the rate of the PLOB bound, and beyond.

Finally, we have also evaluated the performance of an eight-segment repeater for our experimental parameter set. Now caution is required when these plots are compared directly with the previous ones, as we had to improve the “current,” nonunit value of μ to $\mu = 0.99$. Without this fidelity adjustment, it would be impossible to achieve a nonzero secret key rate for an eight-segment repeater (see next section). The μ scaling with n in the QBERs prohibits to scale up a realistic quantum repeater to arbitrarily large distances and n values, as long as no extra elements for quantum error detection or correction are included. For example, in a second-generation quantum repeater, the effective μ_0 and μ values could be kept close to one, at the expense of extra resources

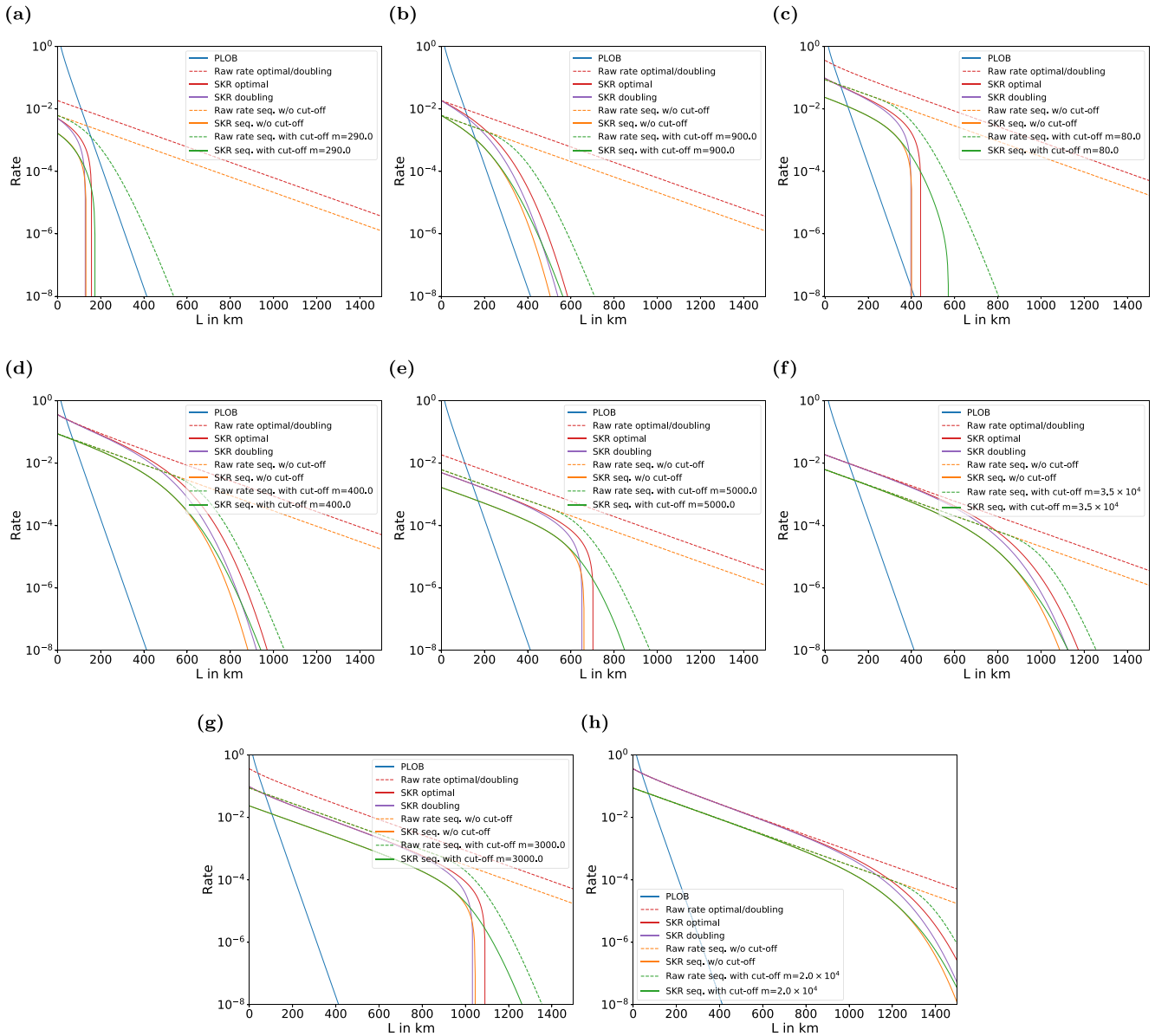


FIG. 9. Rates (secret key/raw) for an eight-segment repeater over distance L for different experimental parameters: (a) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 0.99$; (b) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 1$; (c) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 0.99$; (d) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 1$; (e) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 0.99$; (f) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 1$; (g) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 0.99$; and (h) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 1$.

for quantum error correction and a typically decreasing initial distribution efficiency p (e.g., due to an extra step of entanglement distillation for the distributed, encoded memory qubits). Our formalism could be also applied to such a more sophisticated scenario by considering the effective changes of μ , μ_0 , and p (and possibly α too). Nevertheless, our plots in Fig. 9 show that an eight-segment quantum repeater in a memory-assisted QKD scheme is, in principle, already able to cover large distances by reaching usable rates up to 1000 km or even 1200 km, provided that $\mu = 0.99$ or $\mu \rightarrow 1$, respectively. Besides this, the behavior of an eight-segment repeater is very similar to that of the previous four-segment repeater.

D. Minimal μ values

We have already seen that the secret key rate of memory-assisted QKD is highly sensitive to the depolarizing errors that we use to model the imperfect gates and the imperfect initial states in the quantum repeater. Here let us explicitly give some minimal values for the error parameter μ which at least have to be achieved in order to obtain a nonzero secret key fraction for QKD protocols restricted to one-way postprocessing (see Table II). More generally, in principle, much higher error rates can be tolerated by allowing for two-way postprocessing in the QKD protocols [52]. However, in this work, we primarily utilize the secret key rate as a practical and useful quantitative figure of merit to assess a

TABLE II. Minimal values of μ required for a nonzero secret key rate in one-way postprocessing protocols.

n	$\mu_0 = 1,$	$\mu_0 = \mu,$	$\mu_0 = 1,$	$\mu_0 = \mu,$
	BB84	BB84	6-state	6-state
2	0.780	0.920	0.748	0.908
4	0.920	0.965	0.908	0.959
8	0.965	0.984	0.959	0.981

quantum repeater's performance. Nonetheless, the quantum repeater schemes that we consider may also be employed for other, more general quantum information and communication tasks. Thus we decided not to include schemes with two-way postprocessing, as this would certainly lead to a narrower specialization towards QKD applications. Clearly, in the context of long-range QKD, we believe that considering schemes with two-way postprocessing will be very valuable, since potential, future large-scale quantum repeaters will be rather noisy and therefore protocols which still work for large error rates are very useful. Such a further optimization of our schemes with a special focus on long-range QKD is possible and we leave this option for future work.

It is easy to check that the concatenation of two depolarizing channels with parameters μ_1 and μ_2 is equivalent to a single depolarizing channel with parameter $\mu_1\mu_2$. Thus, for an n -segment repeater, we would expect a total depolarizing channel with parameter $\mu_n = \mu_0^n \mu^{n-1}$. We have carefully and systematically checked and confirmed this in the first part of the paper including other parameters too, such as constant initial and time-dependent memory dephasing. For the BB84 and the six-state protocols, the amount of tolerable noise, such that a secret key can still be obtained with one-way postprocessing, has been extensively studied. For BB84 the error threshold lies at $Q = 11.0\%$ and for the six-state protocol it is $Q = 12.6\%$ [[4], Appendix A]. Since a maximally mixed state results in an error rate of 50%, this gives us a constraint on the minimal values of $\mu_n \geq 1 - 2Q$.

More specifically, the BB84 secret key fraction of Eq. (20) on which we focus here vanishes when the two QBERs both exceed $Q = 11\%$. This holds true for $\mu_n < 1 - 2Q$ even when all other elements are perfect, i.e., even when there is no memory dephasing at all ($\alpha \rightarrow 0$). In this case, the two QBERs as described by Eq. (24) coincide (assuming zero initial dephasing $F_0 = 1$) and neither includes a random variable. These two constant QBERs then express the sole faultiness of the repeater elements without any time-dependent quantum storage (i.e., only the initial states and the gates) which can suffice to prevent Alice and Bob from finally sharing a nonzero secret key.

E. Comparisons

1. Sequential versus doubling versus optimal schemes

In the previous sections (together with the Appendix), we have presented our results for the obtainable secret key rates of two-, three-, four-, and eight-segment quantum repeaters based on various entanglement distribution and swapping strategies. While it is generally straightforward to include a

memory cutoff for the case of two segments, for more than two segments, we have achieved this only for the fully sequential scheme. This was depicted in green in the (noncontour) plots for four and eight segments. The memory cutoff allows to maintain a scaling proportional to the PLOB bound even beyond the distance where the scheme without cutoff drops more quickly. As a consequence, the cutoff can significantly increase the achievable distance. However, it is hard to obtain an exact result for the secret key rate for the more complicated swapping strategies. Nonetheless, for larger distances, one could extrapolate the behavior of the doubling and optimal schemes including a cutoff by simply continuing the curves with lines parallel to the PLOB bound after the drops. Alternatively, inferring from our plots, at larger distances one can rely on a continuation of the curves that behaves exactly like the sequential scheme with a memory cutoff. Both approaches give us a fairly good picture of the behavior of the doubling and optimal schemes including the cutoff.

Nevertheless, the optimal scheme outperforms all other schemes without a cutoff before each one drops completely. The doubling scheme achieves almost similar rates, although it starts earlier to decline. The secret key rates are similar thanks to the equivalent, high raw rates of the doubling and optimal schemes (both being based upon parallel entanglement distributions), and due to our general assumption of deterministic entanglement swapping with $a = 1$ [36].⁴ Thus, for the doubling scheme, one could additionally incorporate nested entanglement distillations in the usual, well-known way, which would allow to reduce the QBERs at the expense of the effective raw rates and with the need of extra physical resources. The differences between the doubling and optimal schemes may not be so large for the repeater sizes mainly considered here ($n \leq 8$). However, note that for doubling we kept a constant signaling time $\tau = L_0/c_f$ independent of the nesting level. As a consequence, we certainly overestimate doubling, since signaling beyond the elementary segments can become necessary for a fixed doubling scheme (which could be compensated via “blind swapping” at higher nesting levels [16,53]). Our exact statistical treatment enabled us to determine the optimal swapping scheme (optimizing the dephasing) and thus allows for a quantitative comparison with the nonoptimal doubling and possible other (including “mixed”) schemes. The fully sequential scheme, based on sequential entanglement distributions, leads to the lowest raw rate. The longer total waiting times of this scheme also contribute to an increased accumulated dephasing. On the other hand, the dephasing of the fully sequential scheme remains limited, as only one segment is waiting at any time step. Overall, although the sequential scheme is the easiest to analyze theoretically, it would typically result in the lowest secret key rate. Nonetheless, the fully sequential scheme is conceptually special and serves as a useful reference for comparison with the other schemes.

⁴For $a < 1$, regimes exist where for the raw rates “doubling” performs strictly worse than “swap as soon as possible” [36], similar to regimes here for the full secret key rates with $a = 1$ when the dephasing becomes dominant.

2. Two- versus four- versus eight-segment repeaters

In this section, let us finally address one of the main questions that motivates the exact secret key rate analysis that we have presented: is there an actual benefit of additional (memory) stations and repeater segments compared with schemes that work entirely without quantum memories (such as point-to-point links or twin-field QKD) or compared to schemes with a smaller number of memory stations? More specifically, is it useful to replace a simple two-segment repeater by a four- or eight-segment repeater in a realistic setting, i.e., even when the extra quantum memories are subject to additional preparation and operational errors and contribute to an increased accumulated memory dephasing? In the preceding section with Table II, we saw that the sole faultiness of the memory qubit initial states and gates, even with no time- and distance-dependent memory dephasing, can make the secret key rate completely vanish, and this effect grows with the segment number n . In the last section of the paper, we shall also look at schemes that minimize the actual number of memory stations by combining the twin-field QKD and repeater memory concepts, for instance, in a four-segment scheme with only one of the three intermediate stations being equipped with memory qubits.

Now here we only consider the “optimal” scheme (generally and rigorously only without memory cutoff, as discussed before), since this ensures we always consider the highest possible secret key rates. By adding extra repeater stations the requirements on the initial state preparations and the Bell measurements become much higher, where the corresponding terms scale as $\propto \mu^{n-1} \mu_0^n$ in the QBERs. We stress again that in order to achieve a nonzero secret key rate for the eight-segment repeater, we had to alter the nonideal value of μ of Table I to a sufficiently large value, $\mu = 0.99$, see also Table II. For a fair comparison, this value is then also used here to obtain the curves of the two- and four-segment repeaters.

The resulting secret key rates can be seen in Fig. 10. As one would expect, for example, the scaling changes from $\sqrt{e^{-L/L_{\text{att}}}}$ to $\sqrt[8]{e^{-L/L_{\text{att}}}}$ when the transition from a two-segment to an eight-segment repeater is considered. However, the rate at $L = 0$ km decreases when increasing the number of segments. This effect occurs for the raw rates (and the secret key rates assuming $\mu = 1$), but it becomes more apparent for $\mu = 0.99$. Still, at long distances, eight segments are superior to a smaller number of segments. Therefore acknowledging that the necessary μ requirements are extremely demanding but not entirely impossible to achieve in practice, we conclude that it is indeed beneficial to add repeater stations. In particular, the effect of the memory dephasing alone (besides channel loss), for possible coherence times like those in Table I and used throughout the plots, will not prevent the benefit of adding more stations. Even when both p_{link} and τ_{coh} take on their lowest of the two considered values as shown in Fig. 10(b), by placing seven memory stations along the channel it is in principle still possible to exceed the PLOB bound significantly. However, realistically, when $\mu < 1$ like in Fig. 10(a), all secret key rates stay below the PLOB bound. In this case, it becomes crucial that either p_{link} [Fig. 10(c)] or τ_{coh} [Fig. 10(e)] is sufficiently large such that the curves can cross PLOB at a sufficiently

small distance (thanks to the small y-axis offset) or they can maintain their repeater loss scaling for sufficiently long distances, respectively. Recall that all rates shown and discussed here are per channel use. Further it should be stressed here that we did not explicitly include time-dependent memory loss (assuming that the memory imperfections are dominated by the time-dependent memory dephasing), which can additionally jeopardize the benefits of adding more, in this case lossy memory stations [54]. (If this loss is detectable it may lead to a nondeterministic entanglement swapping like in the “DLCZ” quantum repeater, which is harder to accurately analyze and optimize even for a constant swapping probability [36]; if the loss remains partially undetected at each station, it can lead to a reduced final state fidelity and thus an increased QBER.)

Let us discuss the comparison of repeaters with different segment numbers in a little more detail. It is indeed quite subtle and for this we shall also take into account larger repeater systems, far beyond the $n = 8$ case. For the general discussion, it is helpful to first consider the fully sequential scheme, as in this case we have access to all relevant (physical and statistical) quantities even for large repeaters, see Table III. If we only consider channel loss or, equivalently, if we only look at the raw rates, there is an optimal number of segments for a given total distance. In Table III, among the possibilities considered there, this is $n = 80$ for $L = 800$ km, and so we should put stations every $L_0 = 10$ km. If we include the memory dephasing (“channel-loss-and-memory-dephasing-only case”), we observe that not only the average (number of) waiting time (steps) $\mathbf{E}[K_n]$, but also the average (number of) dephasing time (steps) $\mathbf{E}[D_n]$ is minimized for $n = 80$ when $L = 800$ km. In fact, these two averages, n/p and $(n-1)/p$, respectively, become identical for larger n , and both grow in the two limits of many and very few segments, $L_0 \rightarrow 0$ ($n \rightarrow \infty$) and $L_0 \rightarrow L/2$ ($n \rightarrow 2$), respectively. However, when changing the segment length L_0 , also the inverse effective coherence time $\alpha = L_0/(c_f \tau_{\text{coh}})$ will change, where now α is simply maximal at $L_0 = L/2$ and it steadily becomes smaller when $L_0 \rightarrow 0$ at fixed τ_{coh} . Note that below a certain L_0 value the repeater’s elementary time unit is no longer dominated by the classical communication times and instead the maximal local processing times must go into α which we refer to as α^{loc} . This effect implies that in order to maximize the effective coherence time τ_{coh}/τ , one should simply use as many stations as possible, eventually approaching the limitation given by the local processing times at each station. For these, we may typically assume $\alpha_1^{\text{loc}} = \tau/\tau_{\text{coh}} = \text{MHz}^{-1}/0.1 \text{ s} = 0.00001$ and $\alpha_2^{\text{loc}} = \tau/\tau_{\text{coh}} = \text{MHz}^{-1}/10 \text{ s} = 0.0000001$.

However, the first really relevant quantity to assess the effect of the memory dephasing is the effective average dephasing time $\alpha \mathbf{E}[D_n]$ that is related to the memory dephasing channel evolution. Interestingly, for the fully sequential scheme, this quantity, $\alpha \mathbf{E}[D_n] = (L/n)(n-1)/(c_f \tau_{\text{coh}} p)$, converges for growing n (small L_0) to $L/(c_f \tau_{\text{coh}} p)$ with $p \rightarrow 1$. For example, in Table III, for $L = 800$ km, we have $L/(c_f \tau_{\text{coh}} p) = 0.0374$ for $\tau_{\text{coh}} = 0.1 \text{ s}$ and $L/(c_f \tau_{\text{coh}} p) = 0.0004$ for $\tau_{\text{coh}} = 10 \text{ s}$. These limits are attainable for about $n = 8000$ and for $n = 800$, respectively. With $\tau_{\text{coh}} = 10 \text{ s}$ the limit is also almost attainable for $n = 80$, so again $L_0 = 10$ km, and there is no further benefit by further increasing n . However, we also have $\alpha_1^{\text{loc}} \mathbf{E}[D_n] = 0.00001 \times$

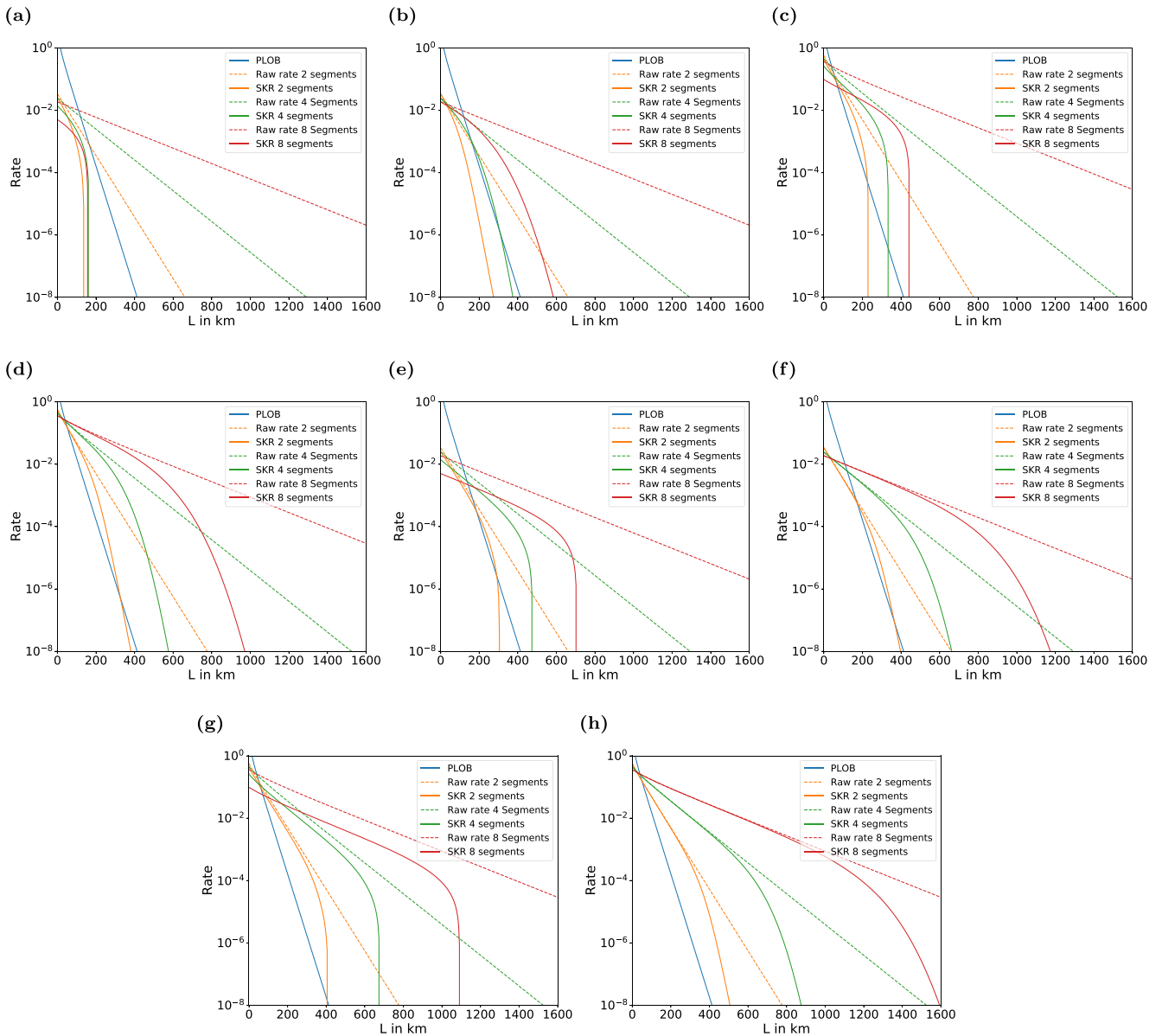


FIG. 10. Comparison of secret key rates of two-, four-, and eight-segment repeaters at total distances L for different experimental parameters: (a) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 0.99$; (b) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 1$; (c) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 0.99$; (d) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 1$; (e) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 0.99$; (f) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 1$; (g) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 0.99$; and (h) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 1$.

$(n - 1)/p = 0.0804$ for $n = 8000$ and $\alpha_2^{\text{loc}} \mathbf{E}[D_n] = 0.0000001 \times (n - 1)/p = 0.0001$ for $n = 800$.

Next let us consider the relevant quantities for the optimal scheme as presented in Table IV. In this case, we no longer have access to all exact values for larger repeaters $n > 8$. However, there is a distinction between the waiting times K_n and the dephasing times D_n . For the total waiting times or the raw rates R we can calculate the numbers for small and also for larger n according to the exact analytical expression in Eq. (37). There are also good approximations for both small n (small p) and larger n (p closer to one) which may be easier to calculate [35,43,55]. Importantly, unlike the case of the fully sequential scheme, the raw rate R now grows with all n (though slowly for larger n) thanks to the fast,

parallel distributions in all segments together with the loss scaling that improves with n . This behavior even matches that of the repeater-assisted capacity bounds for increasing n , as given in the last row of Table IV. However, recall that for our qubit-based quantum repeaters the raw rate can never exceed one secret bit per channel use, whereas $S^{\text{PLOB,QR}}(L_0)$ can, for decreasing L_0 .

For the average total dephasing we can calculate the exact values up to $n = 8$. Comparing these values in Tables III and IV, we see that the optimal scheme accumulates less dephasing than the fully sequential scheme when $n = 4$ and 8 . The two competing effects in the fully sequential scheme, long total waiting time versus minimal number of simultaneously stored memory qubits per elementary time unit, overall result

TABLE III. Overview of the relevant quantities for the *fully sequential scheme*: segment number n , segment length L_0 (km), average (number of) waiting time (steps) $\mathbf{E}[K_n]$, raw rate R , average (number of) dephasing time (steps) $\mathbf{E}[D_n]$, inverse effective coherence time $\alpha_1 = L_0/(c_f 0.1\text{s})$, effective average dephasing time $\alpha_1 \mathbf{E}[D_n]$, inverse effective coherence time $\alpha_2 = L_0/(c_f 10\text{s})$, effective average dephasing time $\alpha_2 \mathbf{E}[D_n]$, average dephasing fractions $\mathbf{E}[e^{-\alpha_1 D_n}]$ and $\mathbf{E}[e^{-\alpha_2 D_n}]$, secret key fractions and rates, r and S , for different $\mu = \mu_0$ (subscript corresponds to the choice of α_1 or α_2 , $\mu = 1$ is the channel-loss-and-memory-dephasing-only case), and the (repeater-assisted) capacity bound $S^{\text{PLOB,QR}}(L_0)$. We further assumed $p_{\text{link}} = F_0 = 1$ for the link coupling efficiency and the initial state dephasing.

n	1	2	4	8	80	800	8000
L_0 (km)	800	400	200	100	10	1	0.1
$\mathbf{E}[K_n]$	$\sim 10^{16}$	$\sim 10^8$	35497	754	126	837	8036
R	$\sim 10^{-16}$	$\sim 10^{-8}$	$\sim 10^{-5}$	0.0013	0.0079	0.0012	0.0001
$\mathbf{E}[D_n]$	—	$\sim 10^8$	26623	659	124	836	8035
α_1	—	0.0192	0.0096	0.0048	0.0005	$\sim 10^{-5}$	$\sim 10^{-6}$
$\alpha_1 \mathbf{E}[D_n]$	—	$\sim 10^6$	256	3.1674	0.0598	0.0402	0.0386
α_2	—	0.0002	0.0001	$\sim 10^{-5}$	$\sim 10^{-6}$	$\sim 10^{-7}$	$\sim 10^{-8}$
$\alpha_2 \mathbf{E}[D_n]$	—	15131	2.5576	0.0317	0.0006	0.0004	0.0004
$\mathbf{E}[e^{-\alpha_1 D_n}]$	—	$\sim 10^{-6}$	$\sim 10^{-6}$	0.0729	0.9420	0.9606	0.9621
$\mathbf{E}[e^{-\alpha_2 D_n}]$	—	0.0001	0.1573	0.9689	0.9994	0.9996	0.9996
$r_1(\mu = 1)$	—	$\sim 10^{-13}$	$\sim 10^{-12}$	0.0038	0.8106	0.8603	0.8646
$r_2(\mu = 1)$	—	$\sim 10^{-9}$	0.0179	0.8843	0.9961	0.9972	0.9973
$r_1(\mu = 0.99)$	—	0	0	0	0	0	0
$r_2(\mu = 0.99)$	—	0	0	0.2203	0	0	0
$S_1(\mu = 1)$	—	$\sim 10^{-21}$	$\sim 10^{-17}$	$\sim 10^{-5}$	0.0064	0.0010	0.0001
$S_2(\mu = 1)$	—	$\sim 10^{-17}$	$\sim 10^{-6}$	0.0012	0.0079	0.0012	0.0001
$S_1(\mu = 0.99)$	—	0	0	0	0	0	0
$S_2(\mu = 0.99)$	—	0	0	0.0003	0	0	0
$S^{\text{PLOB,QR}}(L_0)$	$\sim 10^{-16}$	$\sim 10^{-8}$	0.0002	0.0154	1.4530	4.4921	7.7846

TABLE IV. Overview of the relevant quantities for the *optimal scheme*: segment number n , segment length L_0 (km), average (number of) waiting time (steps) $\mathbf{E}[K_n]$, raw rate R , average (number of) dephasing time (steps) $\mathbf{E}[D_n]$, inverse effective coherence time $\alpha_1 = L_0/(c_f 0.1\text{s})$, effective average dephasing time $\alpha_1 \mathbf{E}[D_n]$, inverse effective coherence time $\alpha_2 = L_0/(c_f 10\text{s})$, effective average dephasing time $\alpha_2 \mathbf{E}[D_n]$, average dephasing fractions $\mathbf{E}[e^{-\alpha_1 D_n}]$ and $\mathbf{E}[e^{-\alpha_2 D_n}]$, secret key fractions and rates, r and S , for different $\mu = \mu_0$ (subscript corresponds to the choice of α_1 or α_2 , $\mu = 1$ is the channel-loss-and-memory-dephasing-only case), and the (repeater-assisted) capacity bound $S^{\text{PLOB,QR}}(L_0)$. For the cases $n > 8$, not all exact values are available and hence we inserted approximate values or (lower or upper) bounds. We assumed $p_{\text{link}} = F_0 = 1$ for the link coupling efficiency and the initial state dephasing.

n	1	2	4	8	80	800	8000
L_0 (km)	800	400	200	100	10	1	0.1
$\mathbf{E}[K_n]$	$\sim 10^{16}$	$\sim 10^8$	18487	255	5.4	2.9	2.2
R	$\sim 10^{-16}$	$\sim 10^{-8}$	0.0001	0.0039	0.1841	0.3490	0.4646
$\mathbf{E}[D_n]$	—	$\sim 10^8$	22923	488	< 124	< 836	< 8035
α_1	—	0.0192	0.0096	0.0048	0.0005	$\sim 10^{-5}$	$\sim 10^{-6}$
$\alpha_1 \mathbf{E}[D_n]$	—	$\sim 10^6$	220	2.3484	< 0.0598	< 0.0402	< 0.0386
α_2	—	0.0002	0.0001	$\sim 10^{-5}$	$\sim 10^{-6}$	$\sim 10^{-7}$	$\sim 10^{-8}$
$\alpha_2 \mathbf{E}[D_n]$	—	15131	2.2022	0.0235	< 0.0006	< 0.0004	< 0.0004
$\mathbf{E}[e^{-\alpha_1 D_n}]$	—	$\sim 10^{-6}$	$\sim 10^{-5}$	0.1552	> 0.9420	> 0.9606	> 0.9621
$\mathbf{E}[e^{-\alpha_2 D_n}]$	—	0.0001	0.2215	0.9769	> 0.9994	> 0.9996	> 0.9996
$r_1(\mu = 1)$	—	$\sim 10^{-13}$	$\sim 10^{-11}$	0.0174	> 0.8106	> 0.8603	> 0.8646
$r_2(\mu = 1)$	—	$\sim 10^{-9}$	0.0357	0.9090	> 0.9961	> 0.9972	> 0.9973
$r_1(\mu = 0.99)$	—	0	0	0	0	0	0
$r_2(\mu = 0.99)$	—	0	0	0.2323	0	0	0
$S_1(\mu = 1)$	—	$\sim 10^{-21}$	$\sim 10^{-15}$	0.0001	> 0.1492	> 0.3002	> 0.3997
$S_2(\mu = 1)$	—	$\sim 10^{-17}$	$\sim 10^{-6}$	0.0036	> 0.1834	> 0.3480	> 0.4633
$S_1(\mu = 0.99)$	—	0	0	0	0	0	0
$S_2(\mu = 0.99)$	—	0	0	0.0009	0	0	0
$S^{\text{PLOB,QR}}(L_0)$	$\sim 10^{-16}$	$\sim 10^{-8}$	0.0002	0.0154	1.4530	4.4921	7.7846

in a larger dephasing rate in comparison with our optimal scheme for $n \leq 8$. We extrapolate this relative behavior to larger n and therefore assume that the dephasing values of the fully sequential scheme may serve as upper bounds on those for the optimal scheme when $n > 8$ in Table IV. We make the same assumption for the other dephasing-dependent quantities, in particular, the secret key fractions, for which the fully sequential values then serve as lower bounds. Looking at the entries of Table IV for the optimal scheme, as a final result, we conclude that while for $\mu = 1$ (“channel-loss-and-memory-dephasing-only” case) it may be best to choose as many segments as $n = 80$ (i.e., stations are placed at every 10 km), similar to what is best for the fully sequential scheme (Table III), for $\mu = 0.99 < 1$, we must not go to segment numbers higher than $n = 8$. In fact, for $\mu = 0.99$, both for the sequential and the optimal schemes, effectively the only nonzero secret key rate is obtainable for $n = 8$ and the larger of the two coherence times considered, with a factor-three enhancement for the optimal scheme over the sequential one. If $n > 8$, the faulty states and gates make S vanish, if $n < 8$ the small raw rates and the high effective average dephasing times do not permit practically usable secret key rates. Note that the entire discussion here in the context of Tables III and IV is for a total distance of $L = 800$ km. We may infer that an elementary segment length of $L_0 \sim 100$ km is not only highly compatible with existing classical repeater and fiber network architectures, but also seems to offer a good balance between an improved memory-assisted loss scaling and an only limited addition of extra faulty elements. This conclusion here holds for our repeater setting based upon heralded loss-tolerant entanglement distribution, deterministic entanglement swapping, and a memory dephasing model. Similar elementary lengths have been used before for schemes with probabilistic entanglement swapping and memory loss [17,18]. For schemes with deterministic entanglement swapping, but a less loss-tolerant entanglement distribution mechanism, [21] smaller segment lengths may be preferable. We will include such schemes, exhibiting an intrinsic channel-loss-dependent dephasing, into the discussion in a later section. Let us now consider a simple form of multiplexing in order to improve the repeater performance, provided sufficient extra resources are available.

F. Multiplexing

Operating M repeater chains in parallel automatically leads to an enhancement of the overall rates by a factor of M . However, since in this case the corresponding number of channels grows as well by a factor of M , the rates per channel use remain unchanged. The situation becomes different though when the chains can “interact” with each other. In particular, the loss scaling of heralded entanglement distributions can be improved, at least for small systems in an MDI QKD setting (even without the use of quantum memories but with the need for a nondestructive heralding) [56]. For memory-based quantum repeaters, memory imperfections may be compensated via multiplexing techniques [41,53,57,58]. Experimentally, multiplexing can be realized through various degrees of freedom. Apart from spatial multiplexing with additional memory qubits at each station that can be coupled to additional fiber

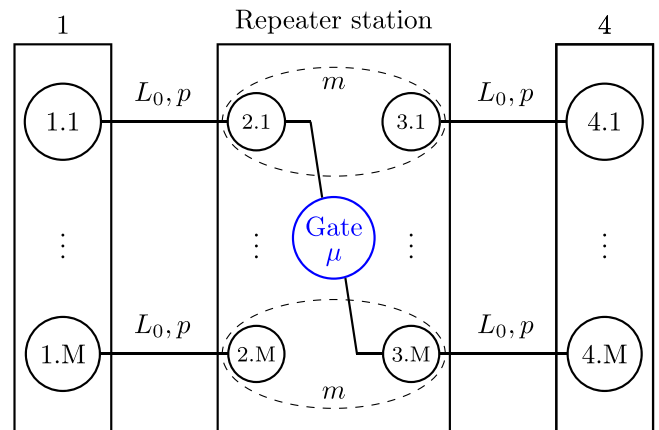


FIG. 11. Multiplexing in a two-segment repeater.

channels, this can be forms of temporal or spectral multiplexing where a single fiber may be employed sequentially at a high clock rate [59] or at the same time with multiple wavelengths, respectively. In this section, we shall incorporate a simple form of multiplexing into our formalism and our repeater models and systems. We have seen that either high total efficiencies or sufficiently long coherence times are needed to achieve usable secret key rates at long distances. We will now see that multiplexing can be understood as a means to effectively enhance the memory coherence time. In the following, we will describe in more detail which kind of multiplexing we consider and why it indeed effectively increases the coherence time.

The simplest way to include multiplexing in our repeater models is by using M memories simultaneously to generate entanglement. These memories can either be connected to the same fiber by a switch or they may each be coupled to their own fiber channel. For simplicity, we consider the switch to be perfect such that both approaches become equivalent (and where the additional channel uses take place either in time or in space). A lossy switch could be easily incorporated into our model by using an additional parameter which is included in p_{link} (note that the loss from the switch is time-independent and so always the same). A possible setup for a two-segment repeater with multiplexing is shown in Fig. 11. Here all entanglement distribution attempts happen simultaneously. Since we have M replica of all memories and channels, this setup acts as if $p \mapsto 1 - (1 - p)^M$, provided that memory qubits from different chains can talk to each other in the middle station so that we may again swap as soon as possible.

For an M multiplexing, let us thus define the effective distribution probability $p_{\text{eff}} = 1 - (1 - p)^M$. For small p , only keeping linear terms, we have $p_{\text{eff}} \approx Mp$. As the expected waiting time in a single segment is then given by $\frac{1}{Mp}$, we can already gain insight on the possibility that multiplexing increases the effective coherence time by a factor of M . More specifically, for example, for the fully sequential scheme the expectation value of D_n is $(n - 1)/p$, thus the transition $p \mapsto p_{\text{eff}} \approx Mp$ reduces the number of dephasing steps, on average, by a factor of $1/M$. This is equivalent to an increase of the coherence time by a factor M . In the following, let us be more precise and show what “small” p really means in terms of

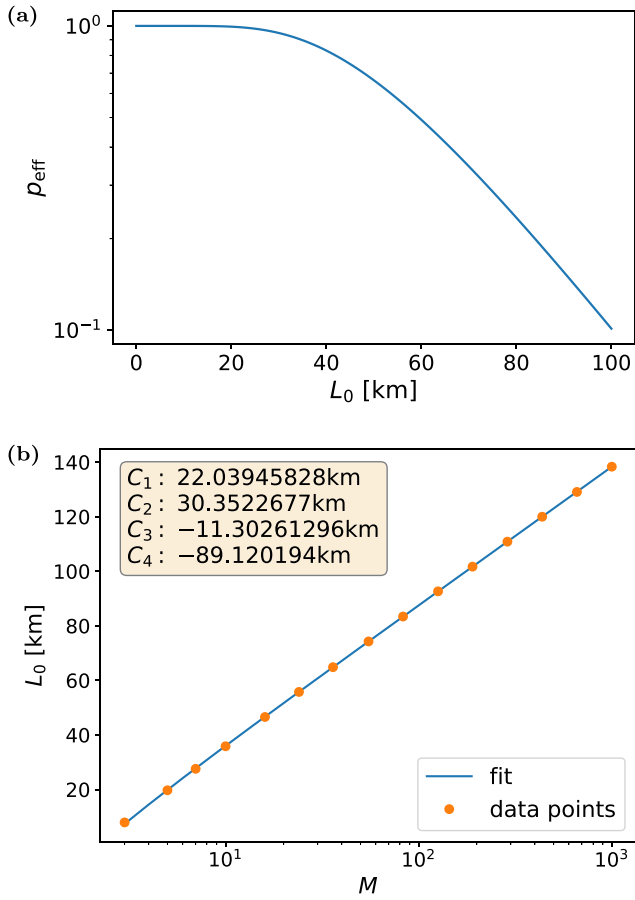


FIG. 12. (a) p_{eff} for $M = 10$ (b) rule of thumb: the orange points show the numerical minimization for different M and the blue line shows the fitted function. It was obtained by fitting the numerical function for all values in the interval (3,1000) (for $M = 2$ our algorithm has convergence problems.) However, it also works well for larger M like, e.g., 10^4 up to some small deviations at high M probably due to the numerical precision. For the meaning of the fitting parameters, see main text. As always, we assumed $L_{\text{att}} = 22$ km.

the corresponding segment length L_0 . In fact, including multiplexing, the secret key rates in dependence of the repeater distance behave in a more complicated way and one can see that for small distances the rate is nearly constant and only for larger distances the rates behave as we would expect from the nonmultiplexed schemes.

In the general, exact model using $p_{\text{eff}} = 1 - (1 - p)^M$, it becomes clear that the above-mentioned behavior originates from this general expression for p_{eff} . In Fig. 12(a), one can see that p_{eff} can be divided in three regimes. In the first regime of small L_0 , p_{eff} is a constant. In the second regime of large L_0 , p_{eff} is a simple exponential decay, while in between it has a more complicated form interpolating both regimes. In the first regime, the effective probability is nearly constant, because in our simple multiplexing protocol we only make use of a single “entanglement excitation” in each segment of the parallelized repeater chains, but for small L_0 we would typically have multiple excitations in each segment. Thus increasing L_0 decreases the number of excitations, but as we anyway only make use of a single one, this barely matters (making use

of more excitations and keeping the “residual entanglement” could potentially further enhance the rates [60]; however, here our focus is on a simple and clear interpretation of the impact of the multiplexing on the coherence time and the memory dephasing in our statistical model). In the second regime of rather large L_0 , the contributions of multiple excitations can be neglected and therefore the rates behave exactly like in the $M = 1$ case. Hence, this regime two is exactly that where we can increase the effective coherence time by a factor of M with the help of multiplexing. We can give a rough rule of thumb for the minimal length of L_0 when one may use the simple approximation of increasing the coherence time by a factor of M . For this we assume $p = \exp(-\frac{L_0}{L_{\text{att}}})^5$ and take the minimizing argument of $\frac{\partial^2 \ln(p_{\text{eff}})}{\partial L_0^2}$ for a given M in order to estimate the midpoint of the interpolating regime. For general M , this expression can be nicely fitted to an expression of the form $c_1 \ln(c_2 M + c_3) + c_4$, as one can see in Fig. 12(b). One should then consider L_0 to be slightly larger for the approximation to hold.

Let us give another, more rigorous derivation of the effective coherence time in the presence of multiplexing. The coherence time primarily characterizes the increasing decline of the secret key rate with distance. However, a massive drop actually happens when the secret key fraction r reaches zero, which is possible when $e_z > 0$, i.e., when $\mu < 1$ or $\mu_0 < 1$. Thus let us determine the probability at which $r = 0$ holds with multiplexing and from that deduce an equivalent coherence time without multiplexing. Since the QBER e_z is constant ($e_z = \bar{e}_z$), we have to solve for the expectation value of \bar{e}_x such that

$$1 - h(e_z) \stackrel{!}{=} h(\bar{e}_x). \quad (61)$$

In order to find the probability p or equivalently the distance at which the drop happens, let us use the Taylor series of the binary entropy function at $x = \frac{1}{2}$,

$$h(x) = 1 - \frac{1}{2 \ln(2)} \sum_{n=1}^{\infty} \frac{(1 - 2x)^{2n}}{n(2n - 1)}, \quad \forall 0 < x < 1. \quad (62)$$

Then one finds for \bar{e}_x up to first order:

$$\bar{e}_x = \frac{1}{2} - \sqrt{\frac{\ln(2)h(e_z)}{2}}, \quad (63)$$

where only the negative root is possible, as $0 \leq e_x \leq \frac{1}{2}$. Inserting \bar{e}_x and solving for $\mathbf{E}[e^{-\alpha D_n}]$ gives

$$\mathbf{E}[e^{-\alpha D_n}] = \frac{\sqrt{2 \ln(2)h(e_z)}}{\mu^{n-1} \mu_0^n (2F_0 - 1)^n}. \quad (64)$$

If $\mu = \mu_0 = 1$, including especially the channel-loss-and-memory-dephasing-only case (for which also $F_0 = 1$), we have $h(e_z) = 0$ and so the requirement becomes $\mathbf{E}[e^{-\alpha D_n}] = 0$, which is impossible. However, as soon as $e_z > 0$, i.e., $\mu < 1$ or $\mu_0 < 1$, a sufficiently small nonzero (average) dephasing fraction $\mathbf{E}[e^{-\alpha D_n}]$ leads to a zero secret key fraction. As we can always calculate this expectation value by our previously

⁵When considering $p_{\text{link}} < 1$ one can incorporate this as an additional length of $-\ln(p_{\text{link}})L_{\text{att}}$ regarding L_0 .

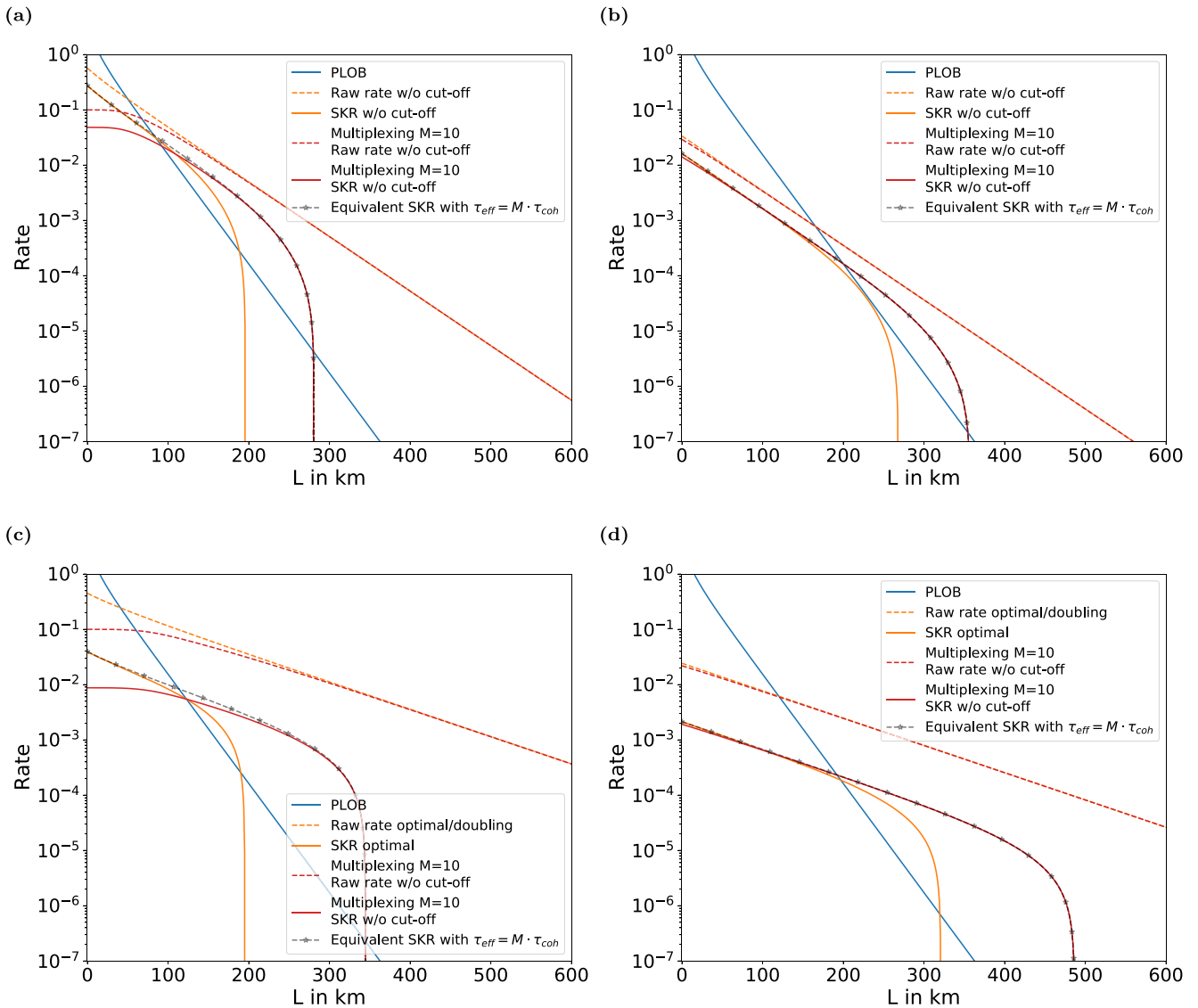


FIG. 13. Rates (secret key/raw) of [(a) and (b)] two- and [(c) and (d)] four-segment repeaters using multiplexing $M = 10$ at distances L for different experimental parameters: [(a) and (c)] $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 0.97$ and [(b) and (d)] $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 0.97$. The rate of a repeater without multiplexing, but with the same coherence time is shown in orange, whereas the rate of a repeater using multiplexing is shown in red. Additionally, a repeater without multiplexing, but with an equivalent effective coherence time is presented in dashed black. All rates are expressed per channel use and hence include a division by M .

derived PGFs, we now have an accurate and systematic way to derive the probability p (or the total distance $L = nL_0$) at which the drop takes place for given values of n , τ_{coh} , μ , μ_0 , and F_0 . Recall that the inverse effective coherence time $\alpha = L_0/(c_f \tau_{\text{coh}})$ typically also depends on L_0 . On the other hand, we may use the above relation to determine an (inverse) effective coherence time by calculating the drop for a repeater with multiplexing and then the equivalent α , which would be needed to achieve the same distance without any multiplexing. From this α , one can recover the coherence time τ_{coh} and finds the approximate relation

$$\tau_{\text{coh}} \mapsto M \cdot \tau_{\text{coh}}, \tag{65}$$

when a multiplexing of M is used and the remaining setup is kept the same. Thus one can achieve an M -times longer effective coherence time with the help of multiplexing.

In Fig. 13, we show the rates of two- and four-segment repeaters using a multiplexing of $M = 10$ in red. Note that because we use the SKR per channel use, the rates are obtained including a division by M . The rates of the same repeaters without multiplexing are presented in orange. Furthermore, a repeater without multiplexing, but with the equivalent ‘effective’ coherence time of $\tau_{\text{eff}} = M \tau_{\text{coh}}$ is shown in dashed black. One can see that for small distances, i.e. large probabilities, the multiplexed repeater does not quite behave like its non-multiplexed counterpart with an effectively increased coherence time. A clear splitting between the red and black curves is visible. However, for larger distances, especially after crossing the PLOB bound, the multiplexed repeater behaves exactly the same as if simply memories with an effectively longer coherence time were used. For smaller link efficiencies, the splitting becomes much less pronounced, as can be seen in

the plots on the right of Fig. 13. All this holds for both two and four segments, according to Fig. 13. In particular, for small link efficiencies, the secret key rate of an equivalent repeater with $\tau_{\text{eff}} = M\tau_{\text{coh}}$ is almost indistinguishable from a repeater with multiplexing. This is in agreement with the above discussion on the occurrence of single versus multiple ‘entanglement excitations’ in each segment where the latter are then highly suppressed even at short distances due to the small value of p_{link} . Thus, for practical purposes, in all our discussions, we may treat several cases equivalently, for instance, a repeater with $\tau_{\text{coh}} = 10$ s and $M = 1$ would be equivalent to a repeater with $\tau_{\text{coh}} = 1$ s and $M = 10$.

G. Secret key rate per second

In a real-world application, the important figure of merit is not the rate per channel use, it will be the rate per second. In particular, a memory-assisted QKD system or generally a memory-based quantum repeater, as typically based upon light-matter interactions and classical communication at least between neighboring stations, has a limited ‘‘clock rate.’’ Classical communication is needed to declare successful transmission of photons for the entanglement distribution. In general, also extra communication would be needed to signal any successful entanglement swapping, but as we assumed deterministic swapping no such communication is needed in our repeater models.

As we already discussed frequently throughout the paper, a repeater’s performance generally depends on an elementary time unit τ , which is contained in the inverse effective coherence time $\alpha = \tau/\tau_{\text{coh}}$, where generally $\tau = \tau_{\text{clock}} + L_0/c_f$ including the experimental local processing time τ_{clock} . We have mostly argued that in the relevant distance regimes, this quantity is dominated by the (quantum and classical) communication times between neighboring stations, thus $\tau = L_0/c_f$ and $\alpha = L_0/(c_f\tau_{\text{coh}})$. Already with segment lengths above 10 km, one can neglect the local clock rates, since these are much higher than the rates given by the transmission times. An extra factor of two could be included in τ for some protocols due to the L_0 transmission of a photon entangled with a memory qubit and the classical answer (sent back over L_0) heralding its successful transmission. However, this would depend on the specific protocol and so we have chosen the simplest, minimal form $\tau = L_0/c_f$. Only for very short segment lengths do we have $\alpha \approx \alpha^{\text{loc}} = \tau_{\text{clock}}/\tau_{\text{coh}} = \text{MHz}^{-1}/\tau_{\text{coh}}$ with experimental clock rates τ_{clock}^{-1} typically of the order of MHz.

However, there are repeater schemes that are independent of additional classical communication and the decision to keep or reinitialize a memory state can be made at the memory station. These schemes may be referred to as ‘‘node receives photons’’ (NRP) unlike the class of schemes ‘‘node sends photons’’ (NSP) [29]. An NRP protocol and application that circumvents the need of extra signal waiting times can be realized with two ‘‘segments’’ and a middle station in memory-assisted MDI QKD [29].

Such a scheme, when treating it as an elementary quantum repeater unit or module many of which a large-scale repeater can be made of, may be referred to as a ‘‘quantum repeater cell,’’ actually composed of two half-segments [[29],

Fig. 6(b)]. In this case, even for large (half-)segment length L_0 , we have $\alpha = \alpha^{\text{loc}} = \tau_{\text{clock}}/\tau_{\text{coh}}$. For completeness, we show the rates of such an NRP-based two-segment scheme in the form of contour plots in Appendix H. By circumventing the need for extra classical communication and thus significantly reducing the effective memory dephasing, the minimal state and gate fidelity values can even be kept constant over large distance regimes. However, as soon as the NRP concept is applied to larger repeaters effectively connecting several complete repeater segments [[29], Fig. 6(a)], the need for extra classical communication to initiate an entanglement swapping operation can no longer be entirely avoided (though there are ideas to still partially benefit from the NRP concept [59]). A quantum repeater cell can also be considered employing the NSP protocol [30] and one such cell (two half-segments) or the corresponding complete segment can then be used as an elementary quantum repeater unit [[29], Fig. 4]. For the NSP concept, the extra signal waiting time is generally required at every distribution attempt. In any case or protocol, the repeater’s elementary time unit τ determines the effective coherence time τ_{coh}/τ and as such, even when the rates per channel use are considered, it determines how many distribution attempts are possible within a given τ_{coh} and hence how big the effective dephasing time αD_n becomes.

Compared with memory-assisted quantum communication schemes, a big asset of an all-optical point-to-point quantum communication link is that it can operate at a high clock rate, typically of the order of GHz, only limited by the speed of Alice’s laser (quantum state) source and Bob’s (quantum state) detector. For such a direct state transmission, no extra classical communication is required as for heralding the successful transfer of entangled photons between repeater links. Thus the rate per second is simply given by the two local clock rates, especially the time it takes to generate the photonic qubit states or any other quantum states in QKD based on different types of encoding (however, due to the known linear bounds on the key distribution via a long and lossy point-to-point quantum communication channel [46,61], it is clear that the rate scaling of qubit-based QKD cannot be beaten by any form of nonqubit encoding).

Other all-optical schemes such as MDI QKD or twin-field QKD, which are no longer point-to-point and do include a middle station between Alice and Bob, also benefit from such high clock rates. The remarkable feature of twin-field QKD is that it shares both advantages: the high clock rate with point-to-point quantum communication and the $L \rightarrow L/2$ loss scaling gain with memory-based two-segment quantum repeaters. In order to assess whether there is a real benefit of employing a two-segment quantum repeater or even adding extra repeater stations, we must eventually consider the rates per second and take into account the corresponding clock rates in all schemes. As a consequence, comparing clock rates of MHz with those of GHz (of memory-based versus all-optical quantum communication), there is a penalty of a factor of about 1000 from the start for the memory-based approach. In the regime where $\alpha \approx L_0/(c_f\tau_{\text{coh}})$, this penalty even gets worse. In this case, when $\tau \approx L_0/c_f$, there are at least two disadvantages of τ growing with L_0 : a reduced effective coherence time τ_{coh}/τ and a reduced raw rate per second R/τ . Beating the PLOB bound for the rates per channel use is only

TABLE V. Overview of the relevant quantities for the *fully sequential scheme* of Table III calculated per second (shown are only those entries that change, but again with segment number n , segment length L_0 (km)): raw rate R/τ , secret key rate S/τ for different $\mu = \mu_0$ (again subscript corresponds to the choice of α_1 or α_2 , $\mu = 1$ is the channel-loss-and-memory-dephasing-only case), and the (repeater-assisted) capacity bound per elementary time unit $S^{\text{PLOB,QR}}(L_0)/\tau$ where we choose $\tau = \text{GHz}^{-1}$ for the cases $n = 1, 2$, i.e., the bounds, expressed per second, on all-optical point-to-point and twin-field QKD. Note that for realistic but still GHz-clock-rate twin-field QKD, we rather have $S/\tau \sim 1$ Hz. In any of the other, memory-based scenarios, we choose $\tau = \tau_{\text{clock}} + L_0/c_f$ with $\tau_{\text{clock}} = \text{MHz}^{-1}$. We again assumed $p_{\text{link}} = F_0 = 1$ for the link coupling efficiency and the initial state dephasing.

n	1	2	4	8	80	800	8000
L_0 (km)	800	400	200	100	10	1	0.1
R/τ	$\sim 10^{-14}$ Hz	$\sim 10^{-6}$ Hz	0.0293 Hz	2.8 Hz	165.2 Hz	248.7 Hz	259.1 Hz
$S_1(\mu = 1)/\tau$	—	$\sim 10^{-18}$ Hz	$\sim 10^{-14}$ Hz	0.0106 Hz	133.9 Hz	213.9 Hz	224.0 Hz
$S_2(\mu = 1)/\tau$	—	$\sim 10^{-14}$ Hz	0.0005 Hz	2.4 Hz	164.5 Hz	248.0 Hz	258.4 Hz
$S_1(\mu = 0.99)/\tau$	—	0 Hz	0 Hz	0 Hz	0 Hz	0 Hz	0 Hz
$S_2(\mu = 0.99)/\tau$	—	0 Hz	0 Hz	0.6086 Hz	0 Hz	0 Hz	0 Hz
$S^{\text{PLOB,QR}}(L_0)/\tau$	$\sim 10^{-7}$ Hz	18.3 Hz	0.2 MHz	15.5 MHz	1.5 GHz	4.5 GHz	7.8 GHz

a necessary criterion that a quantum repeater can be beneficial. In order to confirm a real benefit, we have to consider the secret key rates per second $S/\tau = rR/\tau$. Thus even with perfect memories $\tau_{\text{coh}} \rightarrow \infty$, the different τ values matter. The situation is similar to throwing two or more dices at once at a fast rate. To get all dices showing six eyes, this may still be faster than throwing them very slowly while being allowed to only continue with the unsuccessful dices in each round. The final raw and secret key rates per second obtainable with our two most prominent and mostly discussed repeater schemes, the fully sequential and the optimal schemes, are given in Tables V and VI, respectively.

H. Application and comparison of protocols

Let us now consider various quantum repeater protocols based on different types of the optical encoding and calculate their corresponding secret key rates per second using the methods developed in the preceding sections. We shall look at (i) a kind of standard scheme employing two-mode (dual-rail, DR) photonic qubits distributed through the optical-fiber channels (either emitted from a central source of entangled photon pairs and written into the spin memory qubits or emitted from the repeater nodes employing spin-photon en-

tangled states and utilizing two-photon interference in the middle of each segment) [29], (ii) a scheme based upon spin-photon (spin-light-mode) entanglement and one-photon interference with an encoding similar to that introduced by Cabrillo *et al.* [62] effectively using one-mode (single-rail, SR) photonic qubits, and (iii) a scheme that extends the concepts of twin-field QKD with coherent states to a specific variant of memory-assisted QKD, i.e., a kind of twin-field quantum repeater [45]. We refer to scheme (ii) as the Cabrillo scheme and discuss it in more detail in Appendix I. For all three schemes we consider a quantum repeater with $n = 1, 2, 3, 4, 8$ segments matching the size of the repeater systems that we have formally/theoretically treated in great detail in the first parts of this paper. We always use the previously derived “optimal” quantum repeater protocol that belongs to the fastest schemes and gives the smallest dephasing among all fast schemes.

The two schemes (ii) and (iii) share the potential benefit that for quantum repeaters with n segments and $n - 1$ intermediate memory stations (not counting the memories at Alice and Bob or assuming immediate measurements there) they lead to an improved loss scaling with a $2n$ times bigger effective attenuation distance compared with a point-to-point link (unlike the standard scheme (i) that only achieves an

TABLE VI. Overview of the relevant quantities for the *optimal scheme* of Table IV calculated per second [shown are only those entries that change, but again with segment number n , segment length L_0 (km)]: raw rate R/τ , secret key rate S/τ for different $\mu = \mu_0$ (again subscript corresponds to the choice of α_1 or α_2 , $\mu = 1$ is the channel-loss-and-memory-dephasing-only case), and the (repeater-assisted) capacity bound per elementary time unit $S^{\text{PLOB,QR}}(L_0)/\tau$ where we choose $\tau = \text{GHz}^{-1}$ for the cases $n = 1, 2$, i.e., the bounds, expressed per second, on all-optical point-to-point and twin-field QKD. Note that for realistic but still GHz-clock-rate twin-field QKD we rather have $S/\tau \sim 1$ Hz. In any of the other, memory-based scenarios, we choose $\tau = \tau_{\text{clock}} + L_0/c_f$ with $\tau_{\text{clock}} = \text{MHz}^{-1}$. We again assumed $p_{\text{link}} = F_0 = 1$ for the link coupling efficiency and the initial state dephasing.

n	1	2	4	8	80	800	8000
L_0 (km)	800	400	200	100	10	1	0.1
R/τ	$\sim 10^{-14}$ Hz	$\sim 10^{-6}$ Hz	0.0563 Hz	8.2 Hz	3.8 kHz	72.7 kHz	967.2 kHz
$S_1(\mu = 1)/\tau$	—	$\sim 10^{-18}$ Hz	$\sim 10^{-12}$ Hz	0.1423 Hz	>3.1 kHz	>62.5 kHz	>832.1 kHz
$S_2(\mu = 1)/\tau$	—	$\sim 10^{-14}$ Hz	0.0020 Hz	7.4 Hz	>3.8 kHz	>72.4 kHz	>964.5 kHz
$S_1(\mu = 0.99)/\tau$	—	0 Hz	0 Hz	0 Hz	0 Hz	0 Hz	0 Hz
$S_2(\mu = 0.99)/\tau$	—	0 Hz	0 Hz	1.9 Hz	0 Hz	0 Hz	0 Hz
$S^{\text{PLOB,QR}}(L_0)/\tau$	$\sim 10^{-7}$ Hz	18.3 Hz	0.2 MHz	15.5 MHz	1.5 GHz	4.5 GHz	7.8 GHz

n -times bigger effective attenuation distance), but a final state fidelity parameter still decreasing as the power of $2n - 1$ (assuming equal gate and initial state error rates) like the standard scheme (i). However, scheme (ii) has an intrinsic error during the distribution step due to the initial two-photon terms in combination with channel loss. Similarly, scheme (iii) is more sensitive to channel loss exhibiting an intrinsic loss-dependent dephasing error, because the optical state is a phase-sensitive continuous-variable state [21]. The two models of channel-loss-induced errors for schemes (ii) and (iii) thus slightly differ, while the transmission loss scaling is identical. As a consequence, for both (ii) and (iii), we have the constraint that the excitation amplitudes (the weights of the nonvacuum terms) must not become too large. Despite the above-mentioned benefits compared with scheme (i) it will turn out that the intrinsic errors of schemes (ii) and (iii) represent an essential complication that prevents to fully exploit the improved scaling of the basic parameters in comparison with the standard repeater protocols.

For a fair comparison, assuming similar types of initial state imperfections in all three schemes, we set $\mu_0 = 1$ with $F_0 = 0.99, 0.98$ and so replace the initial depolarizing error for scheme (i) by an initial dephasing error. Thus, in the expressions of the QBERs as given by Eq. (24), the contribution of μ_0^n to the initial error scaling from the analysis of the preceding sections (where $F_0 = 1$) is now replaced by a corresponding scaling with $F_0 < 1$. The gate error scaling with μ^{n-1} remains unchanged in all schemes. Of course, our formalism also allows to focus on specific schemes including initial state errors with $\mu_0 < 1$. In this case, the specific contributions of the different elements in each elementary repeater unit (segments, half-segments, “cells”) [29] to the link coupling efficiency p_{link} and the initial state error parameters μ_0 or F_0 depend on the protocol [29].

For example, zooming in on an NSP segment [29], we have a squared contribution from the two spin-photon entangled states on the left and on the right, $\mu_{\text{sp,ph}}^2$, and another possible gate error factor, μ_{OBM} , coming from the optical Bell measurement in the middle of the segment. In this scenario, already in a single segment, we effectively have one imperfect entanglement swapping operation (acting on the two photons in the middle of the segment) connecting two initially distributed, depolarized entangled states (the two spin-photon states), to which our physical model directly applies replacing our initial μ_0 for one segment according to $\mu_0 \rightarrow \mu_{\text{sp,ph}}^2 \mu_{\text{OBM}}$. This overall initial distribution error will most likely be dominated by the imperfect spin-photon states, assuming near-error-free (though probabilistic) photonic Bell measurements, thus $\mu_0 \sim \mu_{\text{sp,ph}}^2$.

In a full NRP segment, the memory write-in may be realized via quantum teleportation using a locally prepared spin-photon state and an optical Bell measurement on the photon that arrives from the fiber channel and the local photon. In this scenario, already in a single complete segment, we may effectively have three initial entangled states (two local spin-photon states on the left and on the right together with one distributed entangled photon pair emitted from a source in the middle of the segment) and two optical Bell measurements, [[29], Fig. 6(a)] with our model resulting in

a $\mu_0 \sim \mu_{\text{ph,ph}} \mu_{\text{sp,ph}}^2 \mu_{\text{OBM}}^2$ scaling of the initial error parameter for one segment (i.e., similar to the effective final scaling of a three-segment repeater in our more abstract model, with $\mu_0 \rightarrow \mu_{\text{sp,ph}}$ and $\mu \rightarrow \mu_{\text{OBM}}$, and setting for this simplifying analogy, quite unrealistically, $\mu_{\text{sp,ph}} = \mu_{\text{ph,ph}}$). Assuming near-error-free Bell measurements, and near-perfect (though possibly only probabilistically created) photon pairs, we would again arrive at an overall scaling of $\mu_0 \sim \mu_{\text{sp,ph}}^2$ for the initial error parameter. In case of an entangled photon pair source that deterministically produces imperfect photon-photon states (such as a quantum dot source), we would have $\mu_0 \sim \mu_{\text{ph,ph}} \mu_{\text{sp,ph}}^2$ instead. There is also the option of a heralded memory write-in that no longer relies on the generation of local spin-photon states and optical Bell measurements [28]. In this case, our physical model has to be slightly adapted to such a scenario and a decomposition of the different error channels, including an imperfect memory write-in operation, into one effective initial error channel should be considered.

Thus zooming in on our general initial-state error parameters μ_0 or F_0 for a specific implementation is straightforwardly possible, but it will eventually lead to even stronger fidelity requirements for the individual experimental components that contribute to μ_0 or F_0 . The different contributions to the link coupling efficiencies p_{link} can be similarly decomposed into the different experimental elements, also including some differences for the different types of quantum repeater units and protocols [29]. However, note that for our comparison in this section, especially assuming that two photonic states are combined in the middle of each segment (i.e., in a kind of NSP scenario), the two-photon interference of scheme (i) results in a quadratic disadvantage not only for the channel transmission but also in terms of the link coupling efficiency p_{link} in comparison with the protocols based on one-photon interference [schemes (ii) and (iii)], $p_{\text{link,(i)}} = p_{\text{link,(ii)}}^2 = p_{\text{link,(iii)}}^2$. For this, let us write in short $p_{\text{link,DR}} = p_{\text{link,TF}}^2$, given the similarity of schemes (ii) and (iii).

In Fig. 14, we compare the secret key rates for the dual-rail scheme (i) (DR), the Cabrillo scheme (ii), and the twin-field repeater (iii) (TF). The two twin-field-type schemes include a free parameter describing the number of excitations. More excitations lead to a higher transmission rate at the expense of a lower state quality. In the plots, we optimize this parameter for each data point to obtain the maximal secret key rate. Recall, for the DR scheme, we introduce a small dephasing via the parameter $F_0 < 1$ in order to avoid comparing perfect initial entangled states with noisy ones. When comparing schemes (ii) and (iii) one can see that for $\mu \approx 1$ (iii) performs better while for lower μ (ii) is the better performing scheme. This is because the probability of an error is smaller for the Cabrillo scheme, but the error would affect both QBERs of the BB84 protocol, significantly reducing the secret key rate. For the TF scheme (iii), we have an effect on only one of the two error rates. When μ gets smaller, all schemes have a nonvanishing error rate in both bases and therefore the lower error rate of the Cabrillo scheme is helpful.

Figure 14 shows that, although the DR scheme has a scaling disadvantage in comparison to both other schemes, it is often highly competitive, since both twin-field-type schemes suffer from their low initial probabilities of success when

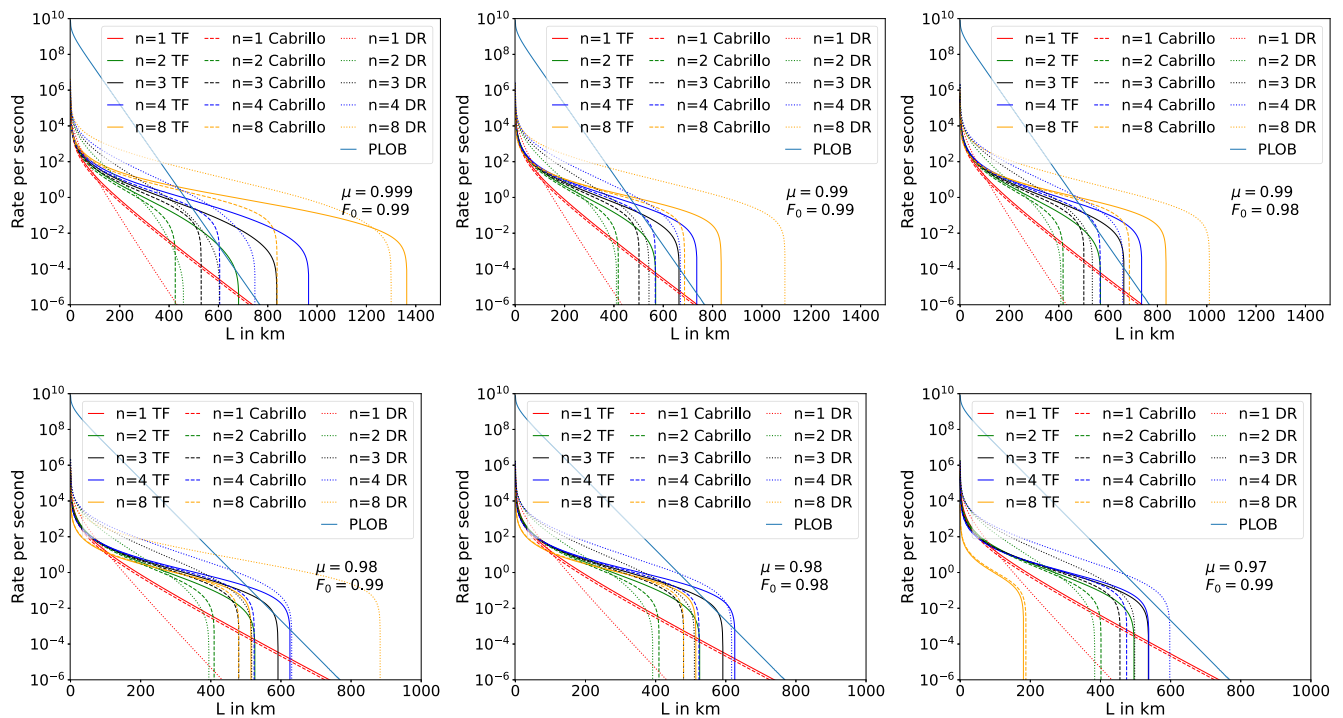


FIG. 14. Secret key rates per second. We always assume a coherence time $\tau_{\text{coh}} = 10$ s, $p_{\text{link,TF}} = 0.9$, and $M = 1$.

only weak excitations can be used to avoid introducing too much noise from the loss channel. Considering a memory coherence time of 10 seconds, a gate error parameter $\mu \geq 0.97$, and coupling efficiencies as $p_{\text{link,TF}} = 0.9$, one can already overcome the PLOB bound with only three memory stations using either the DR scheme (i) or the TF protocol (iii). For this comparison, in terms of secret bits per second, we assume a source repetition rate of 1 GHz for an ideal point-to-point link as associated with the PLOB bound per channel use. Note that we do not include an extra factor of $1/2$ for the final rates which would strictly be needed in the DR-based scheme in comparison with the PLOB bound for a single-mode loss channel. Here the parallel transmission of the two modes for a DR qubit does not change the rates per second and this optical encoding does not cause an extra experimental resource overhead (in fact, it even simplifies the optical transmission circumventing the need for long-distance phase stabilization as for the TF-type schemes). Moreover, an optical point-to-point direct transmission would most likely be based on DR qubit transmission as well. The other, previously mentioned factor 2 that occurs in front of the effective inverse coherence time α when the two spins of a two-qubit spin pair simultaneously dephase while waiting in one segment has now been included here for each segment (i.e., a small improvement would be possible when Alice and Bob measure their spins immediately).

In Fig. 14, we always assume a coherence time $\tau_{\text{coh}} = 10$ s, $p_{\text{link,TF}} = 0.9$, and $M = 1$. Recall from our discussions of the possibility of multiplexing that we may equivalently consider schemes for which, for instance, $\tau_{\text{coh}} = 1$ s and $M = 10$ according to Eq. (65). The plots lead to the following observations. The two TF-type schemes (ii) and (iii) more heavily rely upon sufficiently good error parameters than the DR scheme

(i). In Figs. 14(a) and 14(b), for two different initial dephasing fidelities (which is only relevant for DR), we see that only the TF scheme (iii) performs as good as DR with a gate error as low as $\mu = 0.999$. In this case, for the given parameters, TF even allows to reach slightly larger distances compared with DR, both going well above $L = 1200$ km giving more than a hundredth of a secret bit per second at such distances. Note that in order to achieve this, the TF scheme requires a loss scaling with a 16 times bigger effective attenuation distance compared with a point-to-point link, whereas the DR scheme only has to exhibit an 8 times bigger effective attenuation distance (“ $n = 8$ TF” versus “ $n = 8$ DR”). The number of memory stations is the same for both, namely, seven (not counting those at Alice and Bob).

With increasing gate errors $\mu \leq 0.99$, as shown in Figs. 14(c)–14(g), only the DR scheme allows to reach distances above or near $L = 1000$ km. If both error parameters, that for the gates, μ , and that for the initial states, F_0 , are no longer sufficiently good (both or in combination), also the DR scheme ceases to reach large distances and barely beats the PLOB bound [see Figs. 14(f) and 14(g)]. For the two TF-type schemes (ii) and (iii), we generally checked both types of detectors, on-off as well as photon-number-resolving (Fig. 14 shows the results for on-off detections), and we did not see a significant difference in the logarithmic plots of the secret key rates for both schemes. The reason is that for larger distances the two-photon events at either of the two detectors (detectable via PNRDs) get increasingly unlikely compared with one-photon detection events coming from the two-photon terms in combination with the loss of one photon during transmission (causing errors which remain undetectable via PNRDs).

The practically most relevant situation is shown in Figs. 14(c)–14(e). In particular, for the numbers chosen there,

i.e., state and gate errors of the order of 1%–2%, the DR scheme reaches a distance of $L = 800$ km with about one secret bit per second, and even beyond with a lower rate. The link coupling efficiency for this scenario, like in all others, is $p_{\text{link,DR}} = p_{\text{link,TF}}^2 = 0.81$; the coherence time is $\tau_{\text{coh}} = 10$ s. The number of segments is $n = 8$ (“ $n = 8$ DR”, dotted yellow curve) corresponding to a memory station placed at every $L_0 = 100$ km. The result for this scheme is consistent with the results obtained for $S_2(\mu = 0.99)$ and especially $S_2(\mu = 0.99)/\tau$ in Tables IV and VI, respectively, for $n = 8$. However, note that for the values in Tables IV and VI we chose $p_{\text{link}} = F_0 = 1$ and $\mu = \mu_0$, slightly different from the parameter choice for Fig. 14(c) where $\mu_0 = 1$ and $F_0 = 0.99$ playing the role of an imperfect state parameter instead of μ_0 (in addition, we have $p_{\text{link}} = 0.81$ for DR, and also two spins dephasing at any time step included). Reiterating the previous discussions in Secs. V E 2, the choice of $L_0 \sim 100$ km seems not only highly compatible with existing classical repeater and fiber network architectures, but also offers a good balance between an improved memory-assisted loss scaling and an only limited addition of extra faulty elements. Here now we found, in particular, that the standard DR scheme (i) provides another good choice in order to really benefit from these well balanced parameters. Finally, we also considered the six-state QKD protocol [48] instead of BB84, but this only improved the final rates marginally. In the case of $\mu = 0.98$ and $\mu_0 = 1$, the rate could be, in principle, improved significantly for $n = 8$, but for these parameters, in practice, it is easier to use BB84 and $n = 4$ instead. When considering sufficiently good error parameter values like $\mu = 0.99$, such that $n = 8$ outperforms $n = 4$, then again there is only a minimal improvement by employing the six-state QKD protocol.

VI. CONCLUSION

We presented a statistical model based on two random variables and their probability-generating functions (PGFs) in order to describe, in principle, the full statistics of the rates obtainable in a memory-based quantum repeater chain. The physical repeater model assumes a heralded initial entanglement distribution with a certain elementary probability for each repeater segment (including fiber channel transmission and all link coupling efficiencies), deterministic entanglement swapping to connect the segments, and single-spin quantum memories at each repeater station that are subject to time-dependent memory dephasing. No active quantum error correction is performed on any of the repeater “levels,” while our model does not even rely upon the basic assumption of any nested repeater level structure. The two basic statistical variables associated with this physical repeater model are the total repeater waiting time and the total, accumulated dephasing time.

In the context of an application in long-range quantum cryptography, our model corresponds to a form of memory-assisted quantum key distribution, for which we calculated the (asymptotic, primarily BB84-type) secret key rates as a figure of merit to assess the repeater performance against known benchmarks and all-optical quantum communication schemes. Apart from the theoretical complexity that grows with the size of the repeater (i.e., the number of repeater

segments), it was clear from the start that experimentally the memory-assisted schemes of our model cannot go arbitrarily far while still producing a nonzero secret key rate. One motivation and goal of our work was to quantify this intuition and to provide an answer to the question whether it is actually beneficial, in a real setting, to add faulty memory stations to a quantum communication line. Existing works had their focus on the smallest repeaters with only two segments and one middle station. So, the aim was to further explore these smallest repeaters and then extend them to repeaters of a larger scale, answering the above question.

Within this framework, we determined an optimal repeater scheme that belongs to the class of the fastest schemes (minimizing the average total waiting time and hence maximizing the long-distance entanglement distribution “raw rate”) and, in addition, minimizes the average accumulated memory dephasing within the class of the fastest schemes. We have achieved this optimization for medium-size quantum repeaters with up to eight segments. In particular, for the minimal dephasing, this led us to a scheme to “swap as soon as possible.” The technically most challenging element of our treatment is to determine an explicit analytical expression for the random dephasing variable of the fast schemes and its PGF. In order to confirm the correspondence of the minimum of the dephasing variable with the minimal QKD quantum bit error rate (for the variable related to memory dephasing), we calculated the relevant expectation values and compared the optimal scheme with schemes based on other, different swapping strategies. More generally, our formalism enables one to also consider mixed strategies in which different types of entanglement distribution and swapping can be combined, including the traditionally used doubling strategy that allows to systematically incorporate methods for quantum error detection (entanglement distillation).

Our new results especially apply to quantum repeaters beyond one middle station for which an optimization of the distribution and swapping strategies is no longer obvious. For the special case of three repeater segments, assuming only channel loss and memory dephasing, and with equal distribution time units in every segment given by the signaling time, we showed that our optimal scheme gives the highest secret key rate among not only all the fastest schemes but among all schemes including overall slower schemes that may still potentially lead to a smaller accumulated dephasing. We conjecture that our optimal scheme also gives the highest secret key rate for more than three segments under the same physical assumptions. A rigorous proof of this is nontrivial, because the number of distinct swapping and distribution strategies grows fast with the number of repeater segments. Moreover, in a long-range QKD application, some of the spin qubits may be measured immediately which is generally hard to include in the statistical analysis and the optimization for all possible schemes; for three segments though we did include this additional complexity of the protocols. Towards applications beyond QKD, this extra variation may no longer be relevant.

We identified three criteria that should be satisfied by an optimal repeater scheme: distribute entanglement in parallel as fast as possible, store entanglement in parallel as little as possible, and swap entanglement as soon as possible. It is not always possible to satisfy these conditions at the same

time, and we discussed specific schemes that are particularly good or bad with regards to some of the criteria. For example, a fully sequential repeater scheme is particularly slow, but avoids parallel storage of many spin qubits. Nonetheless, since it is overall slow, the fully sequential scheme can still accumulate more dephasing. We presented a detailed analysis comparing such different repeater protocols and approaches.

With regards to a more realistic quantum repeater modeling, we considered additional tools and parameters such as memory cutoffs, multiplexing, initial state and swapping gate fidelities in order to identify potential regimes in memory-assisted quantum key distribution beyond one middle station where, exploiting our optimized swapping strategy, it becomes useful to add further memory stations along the communication line and connect them via two-qubit swapping operations. Importantly, we found that the initial state and gate fidelities must exceed certain minimal values (generally depending on the specific QKD protocol including postprocessing), as otherwise the sole faultiness of the spin-qubit preparations and operations prevents to obtain a nonzero secret key rate even when no imperfect quantum storage (no memory dephasing) at all takes place and independent of the finite channel transmission. This effect becomes stronger with an increasing number of repeater nodes, scaling with the power of $2n - 1$ for the error parameters in the QKD secret key rate. Once this minimal state and gate fidelity criterion is fulfilled and when the other experimental imperfections are included too, especially the time-dependent memory dephasing, it is essential to consider the exact secret key rates obtainable in optimized repeater protocols in order to conclude whether a genuine quantum repeater advantage over direct transmission schemes is possible or not. This is what our work aimed at and achieved based on the standard notion of asymptotic QKD figures of merit.

By quantifying the influence of (within our physical model) basically all relevant experimental parameters on the final long-range QKD rate, we were able to determine the scaling and trade-offs of these parameters and analytically calculate exact, optimal rates. A quantum repeater of $n = L/L_0$ segments is thereby characterized by the parameter set (p, a, α) where p is the entanglement distribution probability per segment (including the n -dependent channel transmission and zero-distance link coupling efficiency per segment), a is the entanglement swapping success probability, and α is the inverse effective memory coherence time which, in most protocols, depends on n via the quantum and classical communication times per distribution attempt (we also considered small-scale two-segment protocols without this dependence and ideas exist to minimize the impact of the inevitable signal waiting times for the elementary units of larger repeaters in combination with high experimental source and processing clock rates [59]). In addition, we have introduced a set of initial state and gate parameters $(\mu_0/F_0, \mu)$ where μ_0 and F_0 can be adapted to the specific protocols. Additional memory parameters can be collected as (m, M, B) where m is the memory cutoff (maximal time at which any spin qubit is stored), M is the number of simultaneously employed memory qubits in a simple multiplexing scenario with M repeater chains used in parallel, and B is the (spatial) “memory buffer” (the number of

memory qubits per half station in a single repeater chain). In our work, we focused on schemes with $a = 1$ and $B = 1$. The use of $B > 1$ memories at each station would allow to continue the optical quantum state transfer even in segments that already possess successfully distributed states and to potentially replace the earlier distributed lower-quality pairs (subject to memory dephasing) by the later distributed pairs. We also did not put the main emphasis on the use and optimization of m , though we did include this option in some schemes. We found that $M > 1$ leads to an effective improvement of the memory coherence time by a factor of M .

In this setting, the three essential experimental parameters that have to be sufficiently good are the link coupling efficiency (via p), the memory coherence time (via α), and the state/gate error parameter μ_0/μ . While the latter must not go below the above-mentioned limits, generally two of these three parameters should be sufficiently good as a rule of thumb in order to exceed the repeaterless bound and obtain practically meaningful rates. If this is the case, or even better, if all three are of high quality, memory-assisted quantum key distribution based on heralded entanglement distribution and swapping without additional quantum error correction or detection is possible to allow Alice and Bob to share a secret key at a rate orders of magnitude faster than in all-optical quantum state transmission schemes. For instance, for a total distance of 800 km and experimental parameter values that are highly demanding but not impossible (up to 10 s coherence time, about 80% link coupling, and state or gate infidelities in the regime of 1%–2%), one secret bit can be shared per second with repeater stations placed at every 100 km, providing the best balance between a minimal number of extra faulty repeater elements and a sufficient number of repeater stations for an improved loss scaling.

ACKNOWLEDGMENTS

We thank the BMBF (German ministry of education and research) in Germany for support via Q.Link.X/QR.X and the BMBF/EU for support via QuantERA/ShoQC. We also would like to thank Marco Lucamarini for very helpful comments in order to compare our theoretical results with recent experiments of TF QKD.

APPENDIX A: DERIVATION OF EQ. (36)

In this section, we derive the PGF $G_n(t)$ of the random variable K_n defined via

$$K_n = \max(N_1, \dots, N_n), \quad (\text{A1})$$

where N_i are the geometrically distributed random variables with parameter p . We have

$$\begin{aligned} G_n(t) &= \sum_{k_1, \dots, k_n=1}^{+\infty} p q^{k_1-1} \dots p q^{k_n-1} t^{\max(k_1, \dots, k_n)} \\ &= p^n t F_n(q, t), \end{aligned} \quad (\text{A2})$$

where the function $F_n(x, t)$ is defined as

$$F_n(x, t) = \sum_{k_1, \dots, k_n=0}^{+\infty} x^{k_1+\dots+k_n} t^{\max(k_1, \dots, k_n)}. \quad (\text{A3})$$

The series on the right-hand side of this definition converges for all $|x| < 1$ and $|t| \leq 1$, since we have

$$|F_n(x, t)| \leq \sum_{k_1, \dots, k_n=0}^{+\infty} |x|^{k_1+\dots+k_n} = \frac{1}{(1-|x|)^n}. \quad (\text{A4})$$

The function $F_n(x, t)$ can be written in a compact form, having only a finite number of terms. We have

$$\begin{aligned} \frac{F_n(x, t)}{1-t} &= \sum_{k_1, \dots, k_n=0}^{+\infty} \sum_{k=\max(k_1, \dots, k_n)}^{+\infty} x^{k_1+\dots+k_n} t^k \\ &= \sum_{k=0}^{+\infty} t^k \sum_{k_1, \dots, k_n=0}^k x^{k_1+\dots+k_n} \\ &= \sum_{k=0}^{+\infty} t^k \left(\frac{1-x^{k+1}}{1-x} \right)^n. \end{aligned} \quad (\text{A5})$$

Expanding the n th power on the right-hand side and applying simple algebraic transformations, we obtain the following compact expression:

$$F_n(x, t) = \frac{1-t}{(1-x)^n t} \sum_{i=0}^n (-1)^i \binom{n}{i} \frac{1}{1-x^i t}. \quad (\text{A6})$$

From Eq. (A2), we derive the following expression for the PGF of K_n :

$$\begin{aligned} G_n(t) &= (1-t) \sum_{i=0}^n (-1)^i \binom{n}{i} \frac{1}{1-q^i t} \\ &= 1 + (1-t) \sum_{i=1}^n (-1)^i \binom{n}{i} \frac{1}{1-q^i t}, \end{aligned} \quad (\text{A7})$$

which is exactly the expression of the main text.

APPENDIX B: TRACE IDENTITIES

We have

$$\begin{aligned} {}_{23}\langle \Psi^+ | \tilde{\Gamma}_{\mu, 23}(\hat{\rho}_{1234}) | \Psi^+ \rangle_{23} \\ = \mu \cdot {}_{23}\langle \Psi^+ | \hat{\rho}_{1234} | \Psi^+ \rangle_{23} + \frac{1-\mu}{4} \text{Tr}_{23}(\hat{\rho}_{1234}). \end{aligned} \quad (\text{B1})$$

Here we show how to compute the quantities on the right-hand side of this equality. A simple way is to work with density matrices. We use the order of basis elements induced by the tensor product. From the one-qubit basis $(|0\rangle, |1\rangle)^T$ we obtain the two-qubit basis

$$\begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} \otimes \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} = \begin{pmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{pmatrix}. \quad (\text{B2})$$

Taking the tensor product once again, we obtain the ordering of four-qubit basis vectors $|0000\rangle, |0001\rangle, |0010\rangle, |0011\rangle, |0100\rangle, |0101\rangle, |0110\rangle, |0111\rangle, |1000\rangle, |1001\rangle, |1010\rangle, |1011\rangle, |1100\rangle, |1101\rangle, |1110\rangle, |1111\rangle$. If a four-qubit state is described by a density operator $\hat{\rho}_{1234}$ which has a 16×16 density matrix ϱ in the standard basis ordered as described

above, then two-qubit partial diagonal states have the following matrices in the basis (B2):

$$\begin{aligned} {}_{23}\langle 00 | \hat{\rho}_{1234} | 00 \rangle_{23} &= \rho[1, 2, 9, 10], \\ {}_{23}\langle 01 | \hat{\rho}_{1234} | 01 \rangle_{23} &= \rho[3, 4, 11, 12], \\ {}_{23}\langle 10 | \hat{\rho}_{1234} | 10 \rangle_{23} &= \rho[5, 6, 13, 14], \\ {}_{23}\langle 11 | \hat{\rho}_{1234} | 11 \rangle_{23} &= \rho[7, 8, 15, 16], \end{aligned} \quad (\text{B3})$$

where $\varrho[I]$, I being a set of 1-based indices, is the submatrix of ϱ with row and column indices in I . For the off-diagonal states, we have

$$\begin{aligned} {}_{23}\langle 01 | \hat{\rho}_{1234} | 10 \rangle_{23} &= \rho[3, 4, 11, 12 | 5, 6, 13, 14], \\ {}_{23}\langle 10 | \hat{\rho}_{1234} | 01 \rangle_{23} &= \rho[5, 6, 13, 14 | 3, 4, 11, 12], \end{aligned} \quad (\text{B4})$$

where $\varrho[I|J]$ is the submatrix of ϱ with row indices in I and column indices in J .

The state of the form given by Eq. (10)

$$\hat{\rho} = \tilde{\Gamma}_{\mu}(F|\Psi^+\rangle\langle\Psi^+| + (1-F)|\Psi^-\rangle\langle\Psi^-|) \quad (\text{B5})$$

has the following density matrix in the basis (B2):

$$\varrho = \frac{1}{4} \begin{pmatrix} 1-\mu & 0 & 0 & 0 \\ 0 & 1+\mu & 2\mu(2F-1) & 0 \\ 0 & 2\mu(2F-1) & 1+\mu & 0 \\ 0 & 0 & 0 & 1-\mu \end{pmatrix}. \quad (\text{B6})$$

Taking the Kronecker product of two states of this form, Eq. (B1) together with the relations Eqs. (B3) and (B4) lead to the final form of the distributed state in Eq. (11).

APPENDIX C: COMPUTING PGFs OF THE SEQUENTIAL SCHEME

In the sequential scheme, the number of steps K_n and the dephasing D_n are given by

$$K_n = N_1 + \dots + N_n, \quad D_n = N_2 + \dots + N_n. \quad (\text{C1})$$

Their PGFs are thus the n th and $(n-1)$ th power of the single-segment PGF:

$$G_n(t) = \left(\frac{pt}{1-qt} \right)^n, \quad \tilde{G}_n(t) = \left(\frac{pt}{1-qt} \right)^{n-1}. \quad (\text{C2})$$

In the case of a cutoff, the process of entanglement distribution is visualized in Fig. 15. There are zero or more failure parts, with number of steps generating function $B_n^{[m]}(t)$, and one and only one success part, with generating function $A_n^{[m]}(t)$. The total PGF $G_n^{[m]}(t)$ of the number of steps $K_n^{[m]}$ is thus given by

$$G_n^{[m]}(t) = \frac{A_n^{[m]}(t)}{1-B_n^{[m]}(t)}. \quad (\text{C3})$$

We start with the derivation of the failure part's PGF. The PGF of the top line is clearly

$$G_0(t) = \frac{pt}{1-qt}. \quad (\text{C4})$$

Among the rest $n-1$ lines there are i lines that succeed, where $0 \leq i \leq n-2$, so we have to put i p 's into m places

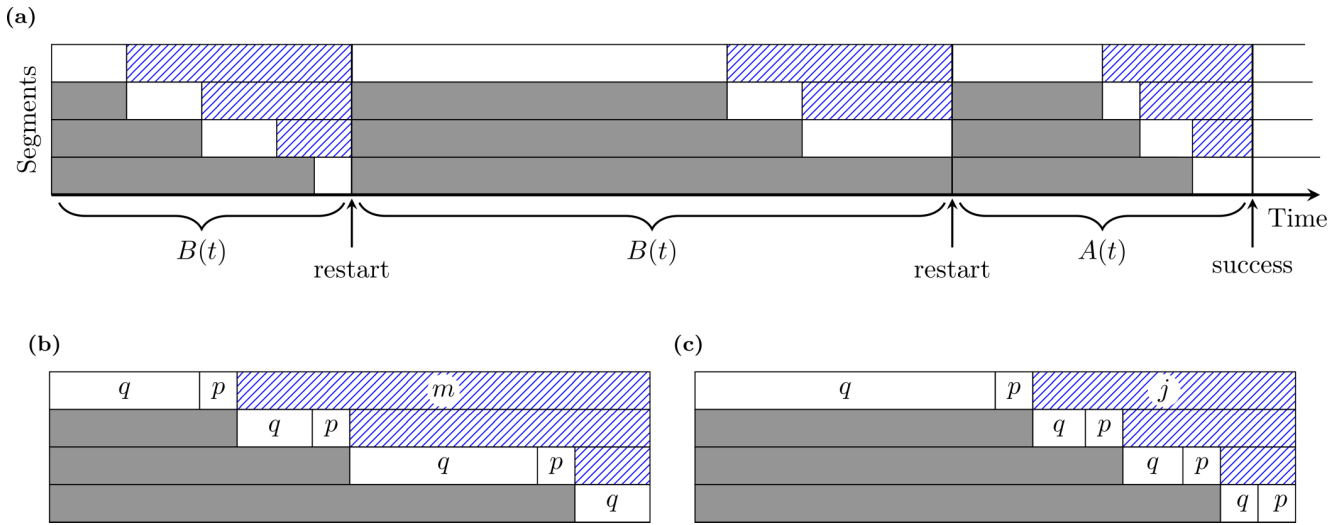


FIG. 15. A visualization of the entanglement distribution process with the sequential scheme for $n = 4$. (a) The general structure of failure periods (if any) and the success period. (b) A detailed view of the failure part generating function $B(t)$. (c) A detailed view of the success part generating function $A(t)$.

and the rest $m - i$ places will be taken by q 's. We thus have

$$B_n^{[m]}(t) = G_0(t) \sum_{i=0}^{n-2} \binom{m}{i} p^i q^{m-i} t^m. \quad (C5)$$

For the success part's PGF, we have

$$A_n^{[m]}(t) = G_0(t) \sum_{j=n-1}^m \binom{j-1}{n-2} p^{n-1} q^{j-n+1} t^j, \quad (C6)$$

since the length of the success part can vary from $n - 1$ to m (we need to put at least $n - 1$ p 's there). The position of the last p is fixed, so we need to place $n - 2$ p 's into $j - 1$ places and the rest $j - n + 1$ will be taken by q 's. Making substitution $j \rightarrow j - n + 1$, we arrive to the expression (27) of the main text.

The random variable for the waiting time of the scheme involving multiple cutoffs is given by

$$K_n^{\text{seq}, \mathbf{m}} = \tilde{N}^{(m_{n-1})} - m_{n-1} + \sum_{j=1}^{T_{n-1}} (K_{n-1, j} + m_{n-1}). \quad (C7)$$

Exploiting that sums of independent random variables correspond to products of their PGFs and using [[63], Satz 3.8] for the sum one immediately obtains the result in the main text.

APPENDIX D: COMPUTING DEPHASING PGFs FOR PARALLEL SCHEMES

In this section, we derive explicit expressions for the PGFs of the dephasing random variables D_n for different schemes considered in the main text. All these schemes have the same property—if the order of N_i 's is known then one can obtain an analytical expression for the corresponding random variable D_n explicitly. Having an explicit expression for D_n , we can compute a part of its PGF corresponding to a given order of arguments. Combining these parts for all possible ordering of arguments, we get the expression for PGF of D_n .

More formally, the space $\Omega = \mathbb{N}^n$ of elementary events consists of all n vectors $\mathbf{N} = (N_1, \dots, N_n)$ of positive integers. The components N_i are independent identically distributed (i.i.d.) random variables with geometric distribution with success probability p , so N_i is the number of attempts (including the last successful one) of the i th segment to distribute entanglement. The failure probability we denote $q = 1 - p$. To every point $\mathbf{N} = (N_1, \dots, N_n) \in \Omega$, we assign the probability

$$\mathbf{P}(\mathbf{N}) = pq^{N_1-1} \dots pq^{N_n-1} = p^n q^{N_1 + \dots + N_n - n}. \quad (D1)$$

The sum of these probabilities is obviously 1, so we have a valid probability space (Ω, \mathbf{P}) .

The PGF of every component N_i is given by the following simple expression:

$$g_{N_i}(t) = \frac{pt}{1 - qt}. \quad (D2)$$

To find PGFs of more complicated random variables involving several components, we appropriately partition Ω , compute the partial PGF on each part and then combine these partial results into the full expression. For every permutation $\pi \in S_n$, we define a subset of Ω which is determined by the corresponding relations between n arguments. For $n = 2$, we have two permutations (12) and (21) with corresponding relations $N_1 \leq N_2$ and $N_2 < N_1$. For $n = 3$, we have six permutations and six corresponding relations

$$\begin{aligned} N_1 \leq N_2 \leq N_3, & \quad N_1 \leq N_3 < N_2, & \quad N_2 < N_1 \leq N_3, \\ N_2 \leq N_3 < N_1, & \quad N_3 < N_1 \leq N_2, & \quad N_3 < N_2 < N_1. \end{aligned} \quad (D3)$$

To make all these subsets nonoverlapping, we use strict inequality between an inversion and nonstrict inequality in other positions between numbers in permutations. We thus have the following decomposition:

$$\Omega = \bigsqcup_{\pi \in S_n} \Omega_\pi, \quad (D4)$$

TABLE VII. Explicit expressions for the optimal and doubling dephasing for all possible relations between arguments in the case of $n = 4$.

Permutation	$D_4^*(\mathbf{N})$	$D_4^{\text{dbl}}(\mathbf{N})$
$N_1 \leq N_2 \leq N_3 \leq N_4$	$N_4 - N_1$	$2N_4 - N_1 - N_3$
$N_1 \leq N_2 \leq N_4 < N_3$	$2N_3 - N_1 - N_4$	$2N_3 - N_1 - N_4$
$N_1 \leq N_3 < N_2 \leq N_4$	$N_2 + N_4 - N_1 - N_3$	$2N_4 - N_1 - N_3$
$N_1 \leq N_3 \leq N_4 < N_2$	$2N_2 - N_1 - N_3$	$2N_2 - N_1 - N_3$
$N_1 \leq N_4 < N_2 \leq N_3$	$2N_3 - N_1 - N_4$	$2N_3 - N_1 - N_4$
$N_1 \leq N_4 < N_3 < N_2$	$2N_2 - N_1 - N_4$	$2N_2 - N_1 - N_4$
$N_2 < N_1 \leq N_3 \leq N_4$	$N_4 - N_2$	$2N_4 - N_2 - N_3$
$N_2 < N_1 \leq N_4 < N_3$	$2N_3 - N_2 - N_4$	$2N_3 - N_2 - N_4$
$N_2 \leq N_3 < N_1 \leq N_4$	$N_4 - N_2$	$2N_4 - N_2 - N_3$
$N_2 \leq N_3 \leq N_4 < N_1$	$N_1 - N_2$	$2N_1 - N_2 - N_3$
$N_2 \leq N_4 < N_1 \leq N_3$	$2N_3 - N_2 - N_4$	$2N_3 - N_2 - N_4$
$N_2 \leq N_4 < N_3 < N_1$	$N_1 + N_3 - N_2 - N_4$	$2N_1 - N_2 - N_4$
$N_3 < N_1 \leq N_2 \leq N_4$	$N_2 + N_4 - N_1 - N_3$	$2N_4 - N_1 - N_3$
$N_3 < N_1 \leq N_4 < N_2$	$2N_2 - N_1 - N_3$	$2N_2 - N_1 - N_3$
$N_3 < N_2 < N_1 \leq N_4$	$N_4 - N_3$	$2N_4 - N_2 - N_3$
$N_3 < N_2 \leq N_4 < N_1$	$N_1 - N_3$	$2N_1 - N_2 - N_3$
$N_3 \leq N_4 < N_1 \leq N_2$	$2N_2 - N_1 - N_3$	$2N_2 - N_1 - N_3$
$N_3 \leq N_4 < N_2 < N_1$	$N_1 - N_3$	$2N_1 - N_2 - N_3$
$N_4 < N_1 \leq N_2 \leq N_3$	$2N_3 - N_1 - N_4$	$2N_3 - N_1 - N_4$
$N_4 < N_1 \leq N_3 < N_2$	$2N_2 - N_1 - N_4$	$2N_2 - N_1 - N_4$
$N_4 < N_2 < N_1 \leq N_3$	$2N_3 - N_2 - N_4$	$2N_3 - N_2 - N_4$
$N_4 < N_2 \leq N_3 < N_1$	$N_1 + N_3 - N_2 - N_4$	$2N_1 - N_2 - N_4$
$N_4 < N_3 < N_1 \leq N_2$	$2N_2 - N_1 - N_4$	$2N_2 - N_1 - N_4$
$N_4 < N_3 < N_2 < N_1$	$N_1 - N_4$	$2N_1 - N_2 - N_4$

where Ω_π is the subset determined by the relations corresponding to π . For any point $\mathbf{N} \in \Omega_\pi$, we can obtain an explicit expression for D_n for any scheme. In Table VII, we show all possible relations between four arguments and the expression corresponding to the optimal and doubling schemes in the case of $n = 4$. Expressions corresponding to different π might be the same, as can be seen for the doubling scheme.

The PGF of D_n is defined as

$$\tilde{G}_n(t) = \sum_{d=0}^{+\infty} \mathbf{P}(D_n = d)t^d = \sum_{\mathbf{N} \in \Omega} \mathbf{P}(\mathbf{N})t^{D_n(\mathbf{N})}. \quad (\text{D5})$$

Using the decomposition in Eq. (D4), we introduce the partial PGFs via

$$\tilde{G}_n(\pi|t) = \sum_{\mathbf{N} \in \Omega_\pi} p^n q^{N_1 + \dots + N_n - n} t^{D_n(N_1, \dots, N_n)}, \quad (\text{D6})$$

where $D_n(N_1, \dots, N_n)$ is given explicitly as an appropriate linear combination of N_i 's. The total PGF $\tilde{G}_n(t)$ is then just the sum of all of these partial PGFs:

$$\tilde{G}_n(t) = \sum_{\pi \in S_n} \tilde{G}_n(\pi|t). \quad (\text{D7})$$

We demonstrate computing these sums by an example for $n = 4$. We have the correspondence

$$\pi = (2134) \rightarrow N_2 < N_1 \leq N_3 \leq N_4 \quad (\text{D8})$$

and the explicit expressions

$$D_4^*(N_1, N_2, N_3, N_4) = N_4 - N_2,$$

$$D_4^{\text{dbl}}(N_1, N_2, N_3, N_4) = 2N_4 - N_2 - N_3. \quad (\text{D9})$$

For the partial PGFs, we have

$$\begin{aligned} \tilde{G}_4^*(\pi|t) &= \sum_{N_2=1}^{+\infty} \sum_{N_1=N_2+1}^{+\infty} \sum_{N_3=N_1}^{+\infty} \sum_{N_4=N_3}^{+\infty} p^4 q^{N_1+N_2+N_3+N_4-4} t^{N_4-N_2} \\ &= \frac{p^4}{1-q^4} \frac{q^3 t}{(1-qt)(1-q^2 t)(1-q^3 t)}, \\ \tilde{G}_4^{\text{dbl}}(\pi|t) &= \sum_{N_2=1}^{+\infty} \sum_{N_1=N_2+1}^{+\infty} \sum_{N_3=N_1}^{+\infty} \\ &\quad \times \sum_{N_4=N_3}^{+\infty} p^4 q^{N_1+N_2+N_3+N_4-4} t^{2N_4-N_2-N_3} \\ &= \frac{p^4}{1-q^4} \frac{q^3 t}{(1-q^2 t)(1-q^3 t)(1-qt^2)}. \end{aligned} \quad (\text{D10})$$

Summing up the expression for all $\pi \in S_4$, we obtain the expressions for $\tilde{G}_4^*(t)$ and $\tilde{G}_4^{\text{dbl}}(t)$ presented in the main text. For completeness, we also give the optimal PGFs for $n = 2$ and $n = 3$:

$$\tilde{G}_2^*(t) = \frac{p^2}{1-q^2} \frac{1+qt}{1-qt},$$

$$\tilde{G}_3^*(t) = \frac{p^3}{1-q^3} \frac{1+(q+2q^2)t - (2q^2+q^3)t^3 - q^4 t^4}{(1-qt)(1-q^2 t)(1-qt^2)}.$$

The size of the expressions grows rather quickly with n , so we do not present them explicitly for $n > 4$. We see that obtaining $\tilde{G}_n(t)$ reduces to computing sums of many geometrical series, which is a rather trivial task. The only nontrivial part of this algorithm is its superexponential $n!$ -complexity. So, this algorithm is applicable only for small n ; we used it up to a practically relevant $n = 8$.

APPENDIX E: OPTIMALITY FOR THREE SEGMENTS

Here we will compare the secret key rates of all possible schemes for a three-segment repeater, when swapping is applied as soon as possible. We will not consider any scheme that delays swapping and swaps at the end, further increasing the dephasing. For each scheme we calculate the random variables for the waiting time and the dephasing. In case of the dephasing the probability generating function is most useful, whereas for the waiting time we only have to consider the expectation value. Moreover, we will examine two different types of schemes. The first type, indicated by ‘‘imm,’’ describes schemes where Alice and Bob measure their qubits immediately. This scenario is useful for QKD applications. The second type of schemes is indicated by a subscript ‘‘non.’’ Here, Alice and Bob no longer measure immediately and this type of schemes is important in applications beyond QKD. A possible application is transferring quantum information between quantum computers by exchanging entangled photons. In this case, Alice and Bob will not measure their qubits until they share an entangled state.

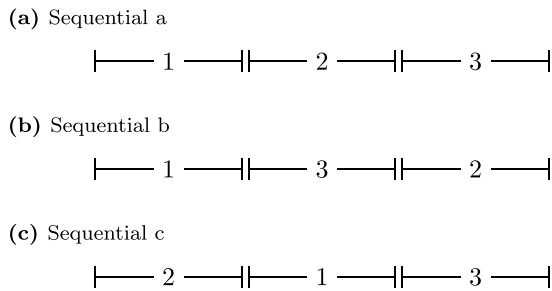


FIG. 16. Sequential arrangements of entanglement generation in a three-segment repeater. The number in each segment corresponds to the order when it starts.

Note that for schemes adapted to QKD, there is another variation that would indeed allow to achieve higher secret key rates than our optimal scheme, namely when Alice and Bob send their signals at a high clock rate and the memory stations can locally decide how to process the arriving qubits, i.e., in a “node receives photon” (NRP) setting [29]. In our model and optimization here, we assume throughout that the distribution attempts in every segment are treated equally and hence are limited by the same elementary time unit $\tau = L_0/c_f$ incorporating all necessary signaling times. This also means that we may overestimate the fixed swapping schemes, since these can require signaling beyond neighboring stations.

1. Sequential schemes

Let us start with sequential schemes, where entanglement generation only takes places in one segment after another. There are three possibilities. First, one starts generating entanglement in Alice’s or Bob’s segment and always connects adjacent segments after the previous one has finished successfully. Note that here entanglement swapping is performed as soon as possible. We will call this scheme “sequential a,” see Fig. 16(a). The second possibility is given by starting with the left or right segment, followed by the segment on the opposite side. Thus no entanglement swapping is possible. Finally, the middle segment is connected. Let us call this scheme “sequential b,” see Fig. 16(b). The third possible arrangement is given by starting in the middle, continuing with the left or right segment and finishing with the remaining segment on the opposite side, see Fig. 16(c). All other sequential arrangements for three segments are equivalent to those three schemes.

These three sequential schemes share the same waiting time, which is

$$K_3^{\text{seq}} = N_1 + N_2 + N_3, \quad (\text{E1})$$

and has the expectation value

$$\mathbf{E}[K_3^{\text{seq}}] = \frac{3}{p}. \quad (\text{E2})$$

Obviously, the dephasing of the schemes differs, and we also have to distinguish between schemes measuring immediately and nonimmediately. At first, let us consider immediate schemes, as it will turn out the random variables of the nonimmediate schemes are just scaled by a factor of two, although it might not be the random variable of the same scheme. We

find

$$\begin{aligned} D_{3,\text{imm}}^{\text{seq,a}} &= N_2 + N_3, & D_{3,\text{imm}}^{\text{seq,b}} &= 2N_2 + N_3, \\ D_{3,\text{imm}}^{\text{seq,c}} &= 2N_1 + N_3. \end{aligned} \quad (\text{E3})$$

Since N_2 and N_3 are i.i.d., the probability generating function (PGF) of $D_{3,\text{imm}}^{\text{seq,a}}$ is given by

$$\tilde{G}_{3,\text{imm}}^{\text{seq,a}}(t) = g_{N_2}(t) \cdot g_{N_3}(t) = \left(\frac{pt}{1-qt} \right)^2. \quad (\text{E4})$$

Due to the general relation

$$g_{2X}(t) = \mathbf{E}[t^{2X}] = \mathbf{E}[(t^2)^X] = g_X(t^2) \quad (\text{E5})$$

valid for any discrete random variable X , we have

$$\tilde{G}_{3,\text{imm}}^{\text{seq,b}}(t) = g_{N_2}(t^2) \cdot g_{N_3}(t) = \frac{p^2 t^3}{(1-qt)(1-qt^2)}. \quad (\text{E6})$$

The same holds true for the PGF of the immediate measurement scheme “sequential c,” because N_1 and N_2 are i.i.d.. Thus its PGF is also given by

$$\tilde{G}_{3,\text{imm}}^{\text{seq,c}}(t) = \frac{p^2 t^3}{(1-qt)(1-qt^2)}, \quad (\text{E7})$$

which shows, that this scheme is actually equivalent to “sequential b” and will not be considered separately in the later comparison.

On the other hand, for nonimmediate measurements, we find the random variables to be

$$\begin{aligned} D_{3,\text{non}}^{\text{seq,a}} &= 2D_{3,\text{imm}}^{\text{seq,a}} = 2(N_2 + N_3), \\ D_{3,\text{non}}^{\text{seq,b}} &= 2D_{3,\text{imm}}^{\text{seq,b}} = 2(2N_2 + N_3), \\ D_{3,\text{non}}^{\text{seq,c}} &= 2D_{3,\text{imm}}^{\text{seq,a}} = 2(N_1 + N_3). \end{aligned} \quad (\text{E8})$$

By using the same argument as before, we find the corresponding PGFs

$$\begin{aligned} \tilde{G}_{3,\text{non}}^{\text{seq,a}}(t) &= \tilde{G}_{3,\text{imm}}^{\text{seq,a}}(t^2), & \tilde{G}_{3,\text{non}}^{\text{seq,b}}(t) &= \tilde{G}_{3,\text{imm}}^{\text{seq,b}}(t^2), \\ \tilde{G}_{3,\text{non}}^{\text{seq,c}}(t) &= \tilde{G}_{3,\text{imm}}^{\text{seq,a}}(t^2). \end{aligned} \quad (\text{E9})$$

Again, the scheme “sequential c” is equivalent to another scheme, but now it is “sequential a.” Therefore the nonimmediate version of “sequential c” will not be treated separately from “sequential a.”

2. Two segments simultaneously at the start

When we generate entanglement in two segments simultaneously, we can do that by starting with these two segments or by finishing with these two. Here we will consider the case where one starts with them and we only have two different arrangements. However, we still have to distinguish between measuring immediately or not.

For the first scheme in consideration, the middle and the left (or equivalently right) segment start generating entanglement at once. They swap as soon as both are done and then the last segment starts generating entanglement, see Fig. 17(a). Let us call this scheme “start a.” The dephasing random vari-

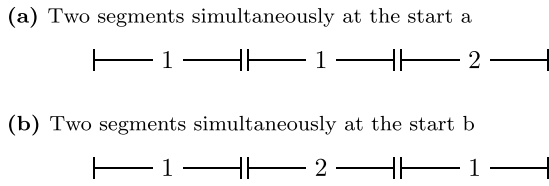


FIG. 17. Possible arrangements of entanglement generation in a three-segment repeater, when two segments start simultaneously. The number in each segment corresponds to the order when it starts.

ables in this case are

$$D_{3,imm}^{start,a} = \begin{cases} N_2 - N_1 + N_3 & N_1 \leq N_2 \\ 2(N_1 - N_2) + N_3 & N_2 < N_1 \end{cases},$$

$$D_{3,non}^{start,a} = 2|N_1 - N_2| + 2N_3. \quad (E10)$$

The PGF of $D_{3,non}^{start,a}$ obviously reads as

$$\tilde{G}_{3,non}^{start,a}(t) = \tilde{G}_2(t^2) \cdot g_{N_3}(t^2) = \frac{p^3 t^2 (1 + qt^2)}{(1 - q^2)(1 - qt^2)^2}. \quad (E11)$$

For immediate measurements, we use the methods presented in the previous section and derive the PGF of $D_{3,imm}^{start,a}$,

$$\tilde{G}_{3,imm}^{start,a}(t) = \frac{p^3 t (1 - q^2 t^3)}{(1 - q^2)(1 - qt)^2 (1 - qt^2)}. \quad (E12)$$

The second scheme is realized when we start with both the left and the right segment at once. As in the second sequential scheme there is no swapping possible, when both segments finished and one has to wait for the middle segment. We will call this scheme “start b.” Schematically, it can be seen in Fig. 17(b). Here we have for the dephasing random variables

$$D_{3,imm}^{start,b} = |N_1 - N_3| + 2N_2,$$

$$D_{3,non}^{start,b} = 2|N_1 - N_3| + 4N_2 = 2D_{3,imm}^{start,b}. \quad (E13)$$

We can simplify the calculation, by considering the immediate scheme first and using $g_{2X}(t) = g_X(t^2)$. The PGF is given by

$$\tilde{G}_{3,imm}^{start,b}(t) = \tilde{G}_2(t) \cdot g_{2N_3}(t) = \frac{p^3 t^2 (1 + qt)}{(1 - q^2)(1 - qt)(1 - qt^2)}.$$

Hence, the PGF of the nonimmediate version is simply

$$\tilde{G}_{3,non}^{start,b}(t) = \tilde{G}_{3,imm}^{start,b}(t^2). \quad (E14)$$

The waiting time is the same for both schemes in this section and amounts to

$$K_3^{simult.} = \max(N_1, N_2) + N_3, \quad (E15)$$

with an expectation value of

$$\mathbf{E}[K_3^{simult.}] = \frac{5 - 3p}{(2 - p)p}. \quad (E16)$$

3. Two segments simultaneously at the end

Finally, the last possible arrangement of two simultaneous segments is to start them in the last step. The waiting time stays the same as in the previous case, but again, there are two possibilities for the dephasing and two to perform measurements, i.e., immediate or nonimmediate. The first scheme

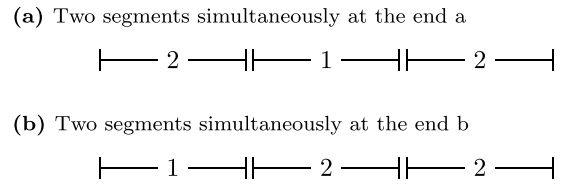


FIG. 18. Possible arrangements of entanglement generation in a three-segment repeater, when only one segment starts and the rest finishes simultaneously. The number in each segment corresponds to the order when it starts.

is realized, when we start with the segment in the middle and when it finishes, the left and right segment start generating entanglement simultaneously. We will call this scheme “end a” and it is shown schematically in Fig. 18(a). In this case, the dephasing random variables are given by

$$D_{3,imm}^{end,a} = N_1 + N_3, \quad D_{3,non}^{end,a} = 2 \max(N_1, N_3), \quad (E17)$$

with the PGFs

$$\tilde{G}_{3,imm}^{end,a}(t) = \tilde{G}_{3,imm}^{seq,a}(t) = \left(\frac{pt}{1 - qt} \right)^2,$$

$$\tilde{G}_{3,non}^{end,a}(t) = \tilde{G}_n^{par}(t^2) = \frac{p^2 t^2 (1 + qt^2)}{(1 - qt^2)(1 - q^2 t^2)}. \quad (E18)$$

The second possibility is to start with the left or right segment and after it finished generate entanglement simultaneously in the remaining segments. The schemes and random variables are equivalent independent whether one starts with the left or right segment. We will call this scheme “end b” and its schematic representation, when starting with the left segment, is shown in Fig. 18(b). Similarly to the scheme “start a,” the dephasing random variables depended on the order of successful entanglement generation.

Let us consider the scheme where we do not measure immediately as an example. First, assume that we started with the left segment and it finished successfully after N_1 attempts. Then both the middle and the right segment start generating entanglement simultaneously. If the middle segments succeeds first after N_2 attempts, we can swap immediately and again have only one segment waiting. Eventually, the right segment will succeed after N_3 attempts, and we can also swap it. In total the dephasing will equal $D_{3,non}^{end,b} = 2N_3$, because $2N_2$ cancels out. This is the optimal case of this scheme.

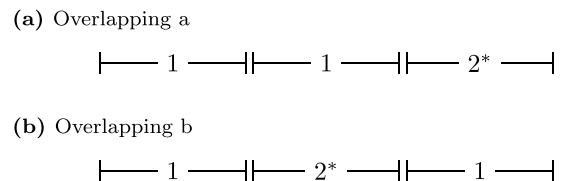


FIG. 19. Possible arrangements of entanglement generation in a three-segment repeater, when two segments start simultaneously and the remaining segment starts as soon as one is successful. The number in each segment corresponds to the order when it starts and the star indicates that this segment starts as soon as one of the others finished.

TABLE VIII. The values of $D_{3,\text{non}}^*$ and $D_{3,\text{imm}}^*$ on the domains of the partition.

Domain	$D_{3,\text{non}}^*$	$D_{3,\text{imm}}^*$
$N_1 \leq N_2 \leq N_3$	$2(N_3 - N_1)$	$N_3 - N_1$
$N_1 \leq N_3 < N_2$	$2(2N_2 - N_1 - N_3)$	$2N_2 - N_3 - N_1$
$N_2 < N_1 \leq N_3$	$2(N_3 - N_2)$	$N_1 + N_3 - 2N_2$
$N_2 \leq N_3 < N_1$	$2(N_1 - N_2)$	$N_1 + N_3 - 2N_2$
$N_3 < N_1 \leq N_2$	$2(2N_2 - N_1 - N_3)$	$2N_2 - N_3 - N_1$
$N_3 < N_2 < N_1$	$2(N_1 - N_3)$	$N_1 - N_3$

Alternatively, it could also happen that the right segment finishes first, and we have two segments waiting for the middle to succeed. In this case, we have $D_{3,\text{non}}^{\text{end,b}} = 4N_2 - 2N_3$. Hence, in total the dephasing is

$$D_{3,\text{non}}^{\text{end,b}} = \begin{cases} 2N_3 & N_3 \geq N_2 \\ 4N_2 - 2N_3 & N_3 < N_2 \end{cases} \quad (\text{E19})$$

A similar consideration yields the dephasing random variable of the immediate measurement scheme to be

$$D_{3,\text{imm}}^{\text{end,b}} = \begin{cases} N_3 & N_3 \geq N_2 \\ 2N_2 - N_3 & N_3 < N_2 \end{cases} \quad (\text{E20})$$

As mentioned a few times so far, we can exploit that $g_{2X}(t) = g_X(t^2)$, and thus we calculate the PGF of the immediate

scheme first, which reads as

$$\tilde{G}_{3,\text{imm}}^{\text{end,b}}(t) = \frac{p^2 t(1 - q^2 t^3)}{(1 - qt)(1 - q^2 t)(1 - qt^2)}. \quad (\text{E21})$$

Therefore the PGF of $D_{3,\text{non}}^{\text{end,b}}$ is given by

$$\tilde{G}_{3,\text{non}}^{\text{end,b}}(t) = \tilde{G}_{3,\text{imm}}^{\text{end,b}}(t^2), \quad (\text{E22})$$

and we covered all possible schemes of this section.

4. Overlapping schemes

Let us now turn our attention to mixed schemes, not only combining sequential and parallel distributions as before, but even “overlapping” them. Therefore, we will call the schemes of this section overlapping schemes. The procedure is as follows. We start generating entanglement in two segments simultaneously and as soon as one of the two segments finishes, we start with the remaining one as well. Thus, the two processes of entanglement generation are overlapping, explaining the naming. In Fig. 19, a schematic version of the overlapping schemes can be seen.

There are two different possible arrangements presented in Figs. 19(a) and 19(b). In the former, the left (or equivalently the right) and the middle segments start from the beginning. This scheme will be called “overlapping, a.” The latter scheme starts with both outer segments and will be called “overlapping, b.”

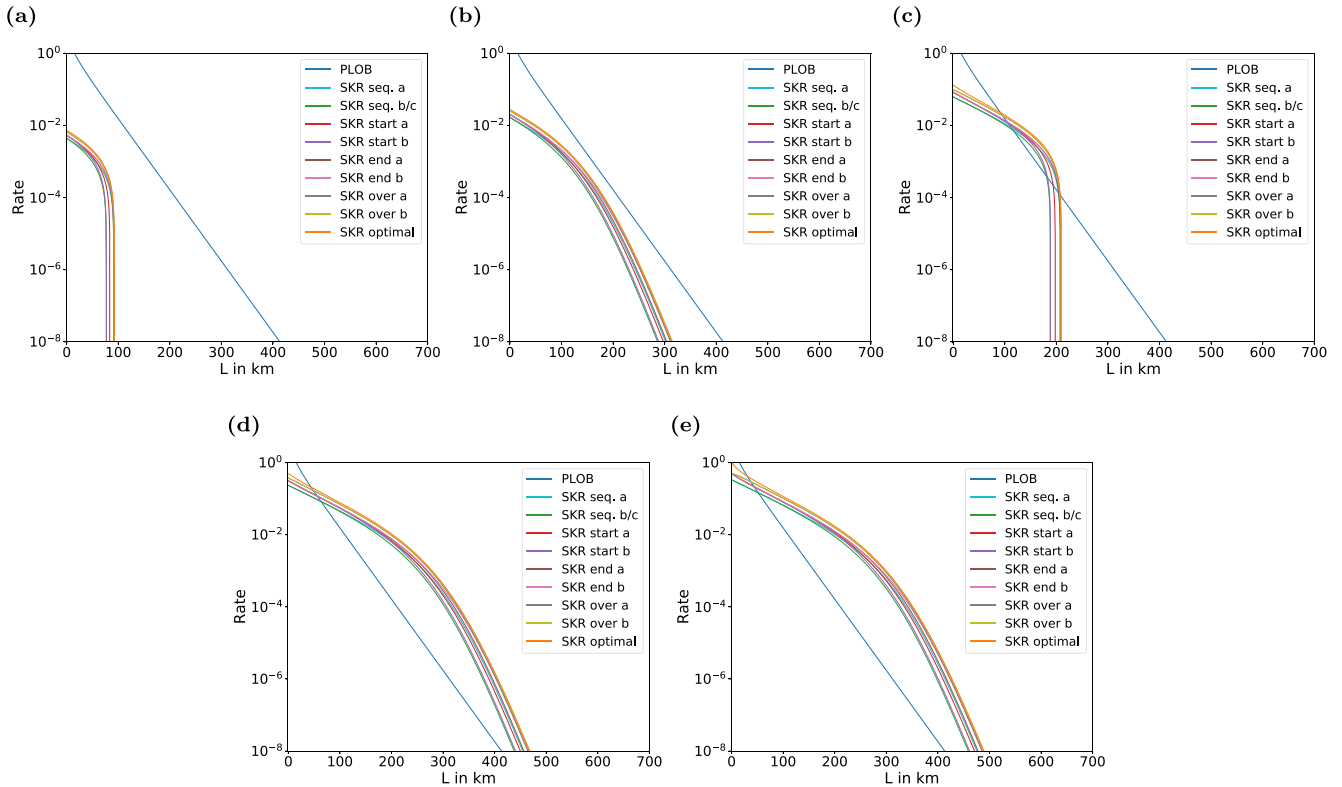


FIG. 20. Comparison of secret key rates of three-segment repeaters performing *immediate* measurements for a total distance L and different experimental parameters: (a) $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 0.97$; (b) $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 1$; (c) $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 0.97$; (d) $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 1$; and (e) $p_{\text{link}} = \mu = \mu_0 = 1$. For all figures, a coherence time of $\tau_{\text{coh}} = 0.1$ s has been used.

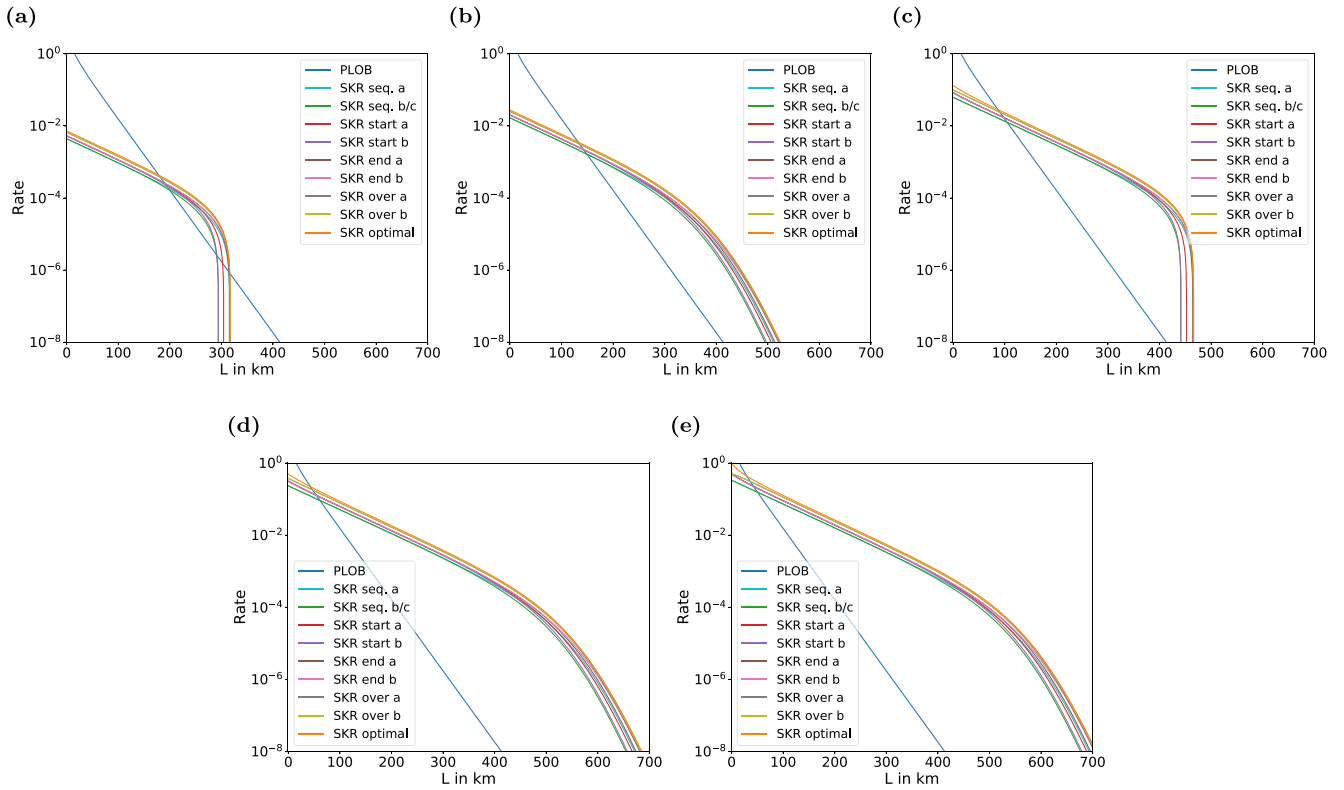


FIG. 21. Comparison of secret key rates of three-segment repeaters performing *immediate* measurements for a total distance L and different experimental parameters: (a) $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 0.97$; (b) $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 1$; (c) $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 0.97$; (d) $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 1$; and (e) $p_{\text{link}} = \mu = \mu_0 = 1$. For all figures, a coherence time of $\tau_{\text{coh}} = 10$ s has been used.

For the scheme “overlapping, a” we find with immediate measurements the dephasing random variable to be

$$D_{3,\text{imm}}^{\text{over,a}} = \begin{cases} N_3 & \Omega_1 \\ 2(N_2 - N_1) - N_3 & \Omega_2, \\ N_1 - N_2 + N_3 & \Omega_3 \end{cases} \quad (\text{E23})$$

where we have chosen the partition $\Omega = \mathbb{N}^3 = \Omega_1 \sqcup \Omega_2 \sqcup \Omega_3$ given by the following inequalities:

$$\begin{aligned} \Omega_1 &= N_1 \leq N_2, N_2 - N_1 \leq N_3, \\ \Omega_2 &= N_1 < N_2, N_2 - N_1 > N_3, \\ \Omega_3 &= N_2 < N_1. \end{aligned} \quad (\text{E24})$$

The dephasing varies depending on the order in which the segments finish, since one cannot swap or measure depending on which segment is done first. Thus we have three different cases. One can calculate the full PGF of the dephasing in a similar way to the previous schemes and finds

$$\tilde{G}_{3,\text{imm}}^{\text{over,a}}(t) = \frac{p^3 t (1 + q - 2q^2 t - qt^2 + q^4 t^4)}{(1 - q^2)(1 - qt)^2(1 - q^2 t)(1 - qt^2)}. \quad (\text{E25})$$

For the nonimmediate version of the scheme “overlapping, a,” we do not have to take the measurements into account, but this still does not result in more symmetries simplifying the expression. Hence, one has to consider all possible orders

separately and we find the dephasing

$$D_{3,\text{non}}^{\text{over,a}} = \begin{cases} 2N_3 & \Omega_1 \\ 2(2(N_2 - N_1) - N_3) & \Omega_2, \\ 2N_3 & \Omega_3, \\ 2(N_1 - N_2) & \Omega_4 \end{cases} \quad (\text{E26})$$

where the partition in this case is given by

$$\begin{aligned} \Omega_1 &= N_1 \leq N_2, N_2 - N_1 \leq N_3, \\ \Omega_2 &= N_1 < N_2, N_2 - N_1 > N_3, \\ \Omega_3 &= N_2 < N_1, N_1 - N_2 \leq N_3, \\ \Omega_4 &= N_2 < N_1, N_1 - N_2 > N_3. \end{aligned} \quad (\text{E27})$$

The resulting PGF reads as

$$\tilde{G}_{3,\text{non}}^{\text{over,a}}(t) = \frac{p^3 t^2 (1 + 2q - q(1 + q)t^4 - q^3 t^6)}{(1 - q^2)(1 - qt^2)(1 - q^2 t^2)(1 - qt^4)}.$$

The other overlapping scheme possesses more symmetry, thus we find more compact expressions for the random variables. It mainly depends on the relative difference of steps between the outer segments. We find for the immediate and nonimmediate schemes:

$$\begin{aligned} D_{3,\text{imm}}^{\text{over,b}} &= \begin{cases} 2N_2 - |N_1 - N_3| & |N_1 - N_3| < N_2 \\ |N_1 - N_3| & |N_1 - N_3| \geq N_2 \end{cases}, \\ D_{3,\text{non}}^{\text{over,b}} &= \begin{cases} 4N_2 - 2|N_1 - N_3| & |N_1 - N_3| < N_2 \\ 2|N_1 - N_3| & |N_1 - N_3| \geq N_2 \end{cases}. \end{aligned} \quad (\text{E28})$$

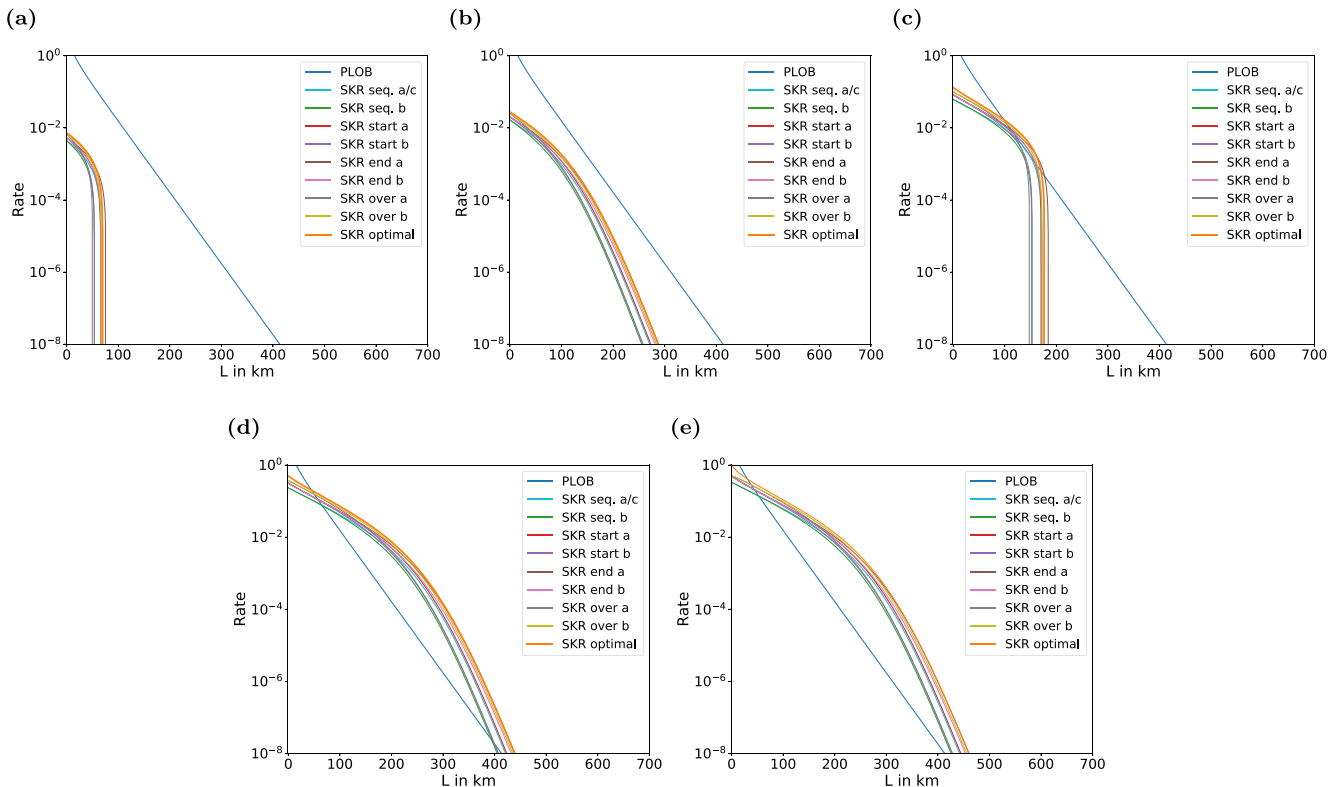


FIG. 22. Comparison of secret key rates of three-segment repeaters performing *nonimmediate* measurements for a total distance L and different experimental parameters: (a) $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 0.97$; (b) $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 1$; (c) $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 0.97$; (d) $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 1$; and (e) $p_{\text{link}} = \mu = \mu_0 = 1$. A coherence time of $\tau_{\text{coh}} = 0.1$ s has been used throughout.

By case analyses, we derive the PGFs

$$\begin{aligned} \tilde{G}_{3,\text{imm}}^{\text{over},b}(t) &= \frac{p^3 t(t + q(2 - t^2(1 + q + q^2 t)))}{(1 - q^2)(1 - qt)(1 - q^2 t)(1 - qt^2)}, \\ \tilde{G}_{3,\text{non}}^{\text{over},b}(t) &= \tilde{G}_{3,\text{imm}}^{\text{over},b}(t^2). \end{aligned} \quad (\text{E29})$$

Finally, the only missing piece is the waiting time of the overlapping schemes and its expectation value. The random variable of the waiting time is

$$K_3^{\text{over}} = \min(N_1, N_2) + \max(|N_1 - N_2|, N_3). \quad (\text{E30})$$

Its expectation value is found to be

$$\mathbf{E}[K_3^{\text{over}}] = \frac{8 - 3p(3 - p)}{p(2 - p)^2}. \quad (\text{E31})$$

5. Parallel schemes

Here we only consider the potentially optimal scheme, since all parallel schemes possess the same raw rate, but differ in dephasing. In the optimal scheme, the dephasing is minimized, such that it has the best secret key rate of all schemes of this class.

The waiting time is $K_3^{\text{par}} = \max(N_1, N_2, N_3)$ and following (37) or Appendix A its expectation value is

$$\mathbf{E}[K_3^{\text{par}}] = \frac{1 + q(4 + 3q(1 + q))}{1 + q - q^3 - q^4}. \quad (\text{E32})$$

The dephasing PGF can be computed with our partitioning approach. The six domains and the values of the dephasing

variables in these domains are given in Table VIII. The final result reads as

$$\begin{aligned} \tilde{G}_{3,\text{non}}^*(t) &= \frac{p^3}{1 - q^3} \frac{1 + q(1 + 2q)t^2 - q^2(2 + q)t^6 - q^4 t^8}{(1 - qt^2)(1 - q^2 t^2)(1 - qt^4)}, \\ \tilde{G}_{3,\text{imm}}^*(t) &= \frac{p^3}{1 - q^3} \frac{1 + q^2 t - 2q^3 t^2 - 2q^2 t^3 + q^3 t^4 + q^5 t^5}{(1 - qt)^2(1 - q^2 t)(1 - qt^2)}. \end{aligned}$$

6. Comparisons

Finally, as we have calculated all necessary statistical quantities we are able to compare the previously discussed schemes. Again as a remark, we only considered schemes here, which swap as soon as possible, as delaying the entanglement swapping increases the dephasing, which in turn decreases the SKR.

First, we consider the immediate measurement schemes. In Fig. 20 ($\tau_{\text{coh}} = 0.1$ s) and Fig. 21 ($\tau_{\text{coh}} = 10$ s), one can see a comparison of all immediate measurement schemes for a three-segment repeater using the previously discussed schemes. In both figures, the SKR of the “optimal” scheme is represented in orange. As mentioned earlier, the scheme “seq. c” is equivalent to “seq. b” in this setting and thus not considered separately. For both coherence times, the optimal schemes outperform all other schemes. Especially for shorter distances, the optimal scheme performs clearly better than others. Only for longer distances, where the rate of any three-segment repeater drops, the schemes “over, b,” “over, a,” and

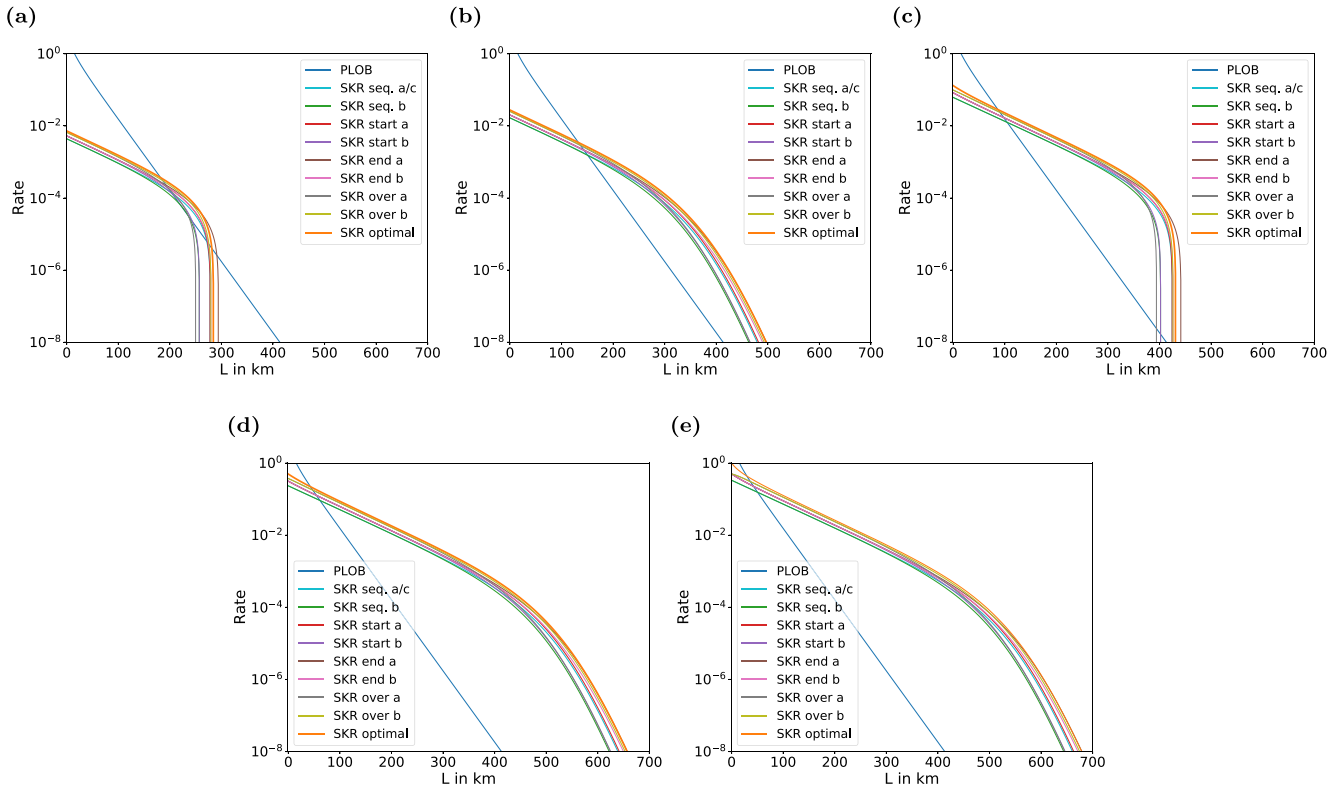


FIG. 23. Comparison of secret key rates of three-segment repeaters performing *nonimmediate* measurements for a total distance L and different experimental parameters: (a) $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 0.97$; (b) $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 1$; (c) $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 0.97$; (d) $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 1$; and (e) $p_{\text{link}} = \mu = \mu_0 = 1$. A coherence time of $\tau_{\text{coh}} = 10$ s has been used throughout.

“end, b” catch up, but do not surpass it. Typically, one would not use this regime of a repeater, as the rates are too low. Additionally, in the limit of increasing hardware parameters, i.e., $p_{\text{link}} \rightarrow 1$, $\mu \rightarrow 1$, $\mu_0 \rightarrow 1$, the optimal scheme keeps performing the best. Thus we conclude that the immediate measurement version of the optimal scheme is truly optimal for $n \leq 3$.

Next, in Fig. 22 ($\tau_{\text{coh}} = 0.1$ s) and Fig. 23 ($\tau_{\text{coh}} = 10$ s), one can see the same comparison of different swapping schemes using nonimmediate measurements. Again, the “optimal” scheme is presented in orange. This time the sequential schemes “seq, a” and “seq, c” are equivalent and thus are not considered separately. As one can see, the optimal scheme outperforms all other schemes in the ideal case when $\mu = \mu_0 = 1$ for all choices of τ_{coh} and p_{link} . Furthermore, it also provides the highest secret key rate in the nonideal case until close to the drop-off. The scheme “end a” surpasses it only at those distances either close to where or after both start declining dramatically, thus increasing the achievable distance. As discussed before, one would typically not operate the repeater in this regime. However, if the main goal is to obtain the longest achievable distance possible, then the scheme “end a” performs the best. Overall, again our optimal scheme provides the best secret key rate for the most realistic use scenarios. Moreover, it is truly optimal in the limit of increasing hardware parameters, i.e., $p_{\text{link}} \rightarrow 1$, $\mu \rightarrow 1$, and $\mu_0 \rightarrow 1$. Thus it will be beneficial to use the “optimal” scheme as technology progresses and hardware improves. Hence, our conclusion for nonimmediate schemes is again that the “optimal” scheme

is optimal with increasing hardware parameters for $n \leq 3$. On the whole, we conjecture that the same is true for both immediate and nonimmediate measurement schemes for all $n \geq 3$ -segment repeaters. This should be further investigated in future research.

APPENDIX F: COMPARISON OF “OPTIMAL” WITH FULLY SEQUENTIAL AND ALICE IMMEDIATELY MEASURING ($n = 8$)

The fully sequential scheme, in which repeater segments are sequentially filled with entangled pairs from, for example, left to right is the overall slowest scheme leading to the smallest raw rates. However, a potential benefit is that parallel qubit storage can be almost entirely avoided. More specifically, when the first segment on the left is filled and waiting for the second segment to be filled too, the first segment waits for a random number of N_2 steps, whereas the second segment always only waits for one constant dephasing unit (for each distribution attempt in the second segment). Thus omitting the constant dephasing in each segment, the accumulated time-dependent random dephasing of the fully sequential scheme has only contributions from a single memory pair subject to memory dephasing at any elementary time step. On average, this gives a total dephasing of $(n - 1)/p$, which is the sum of the average waiting time in one segment for segments 2 through n , as discussed in detail in the main text.

In a QKD application, Alice’s qubit can be measured immediately (and so can Bob’s qubit at the very end when the

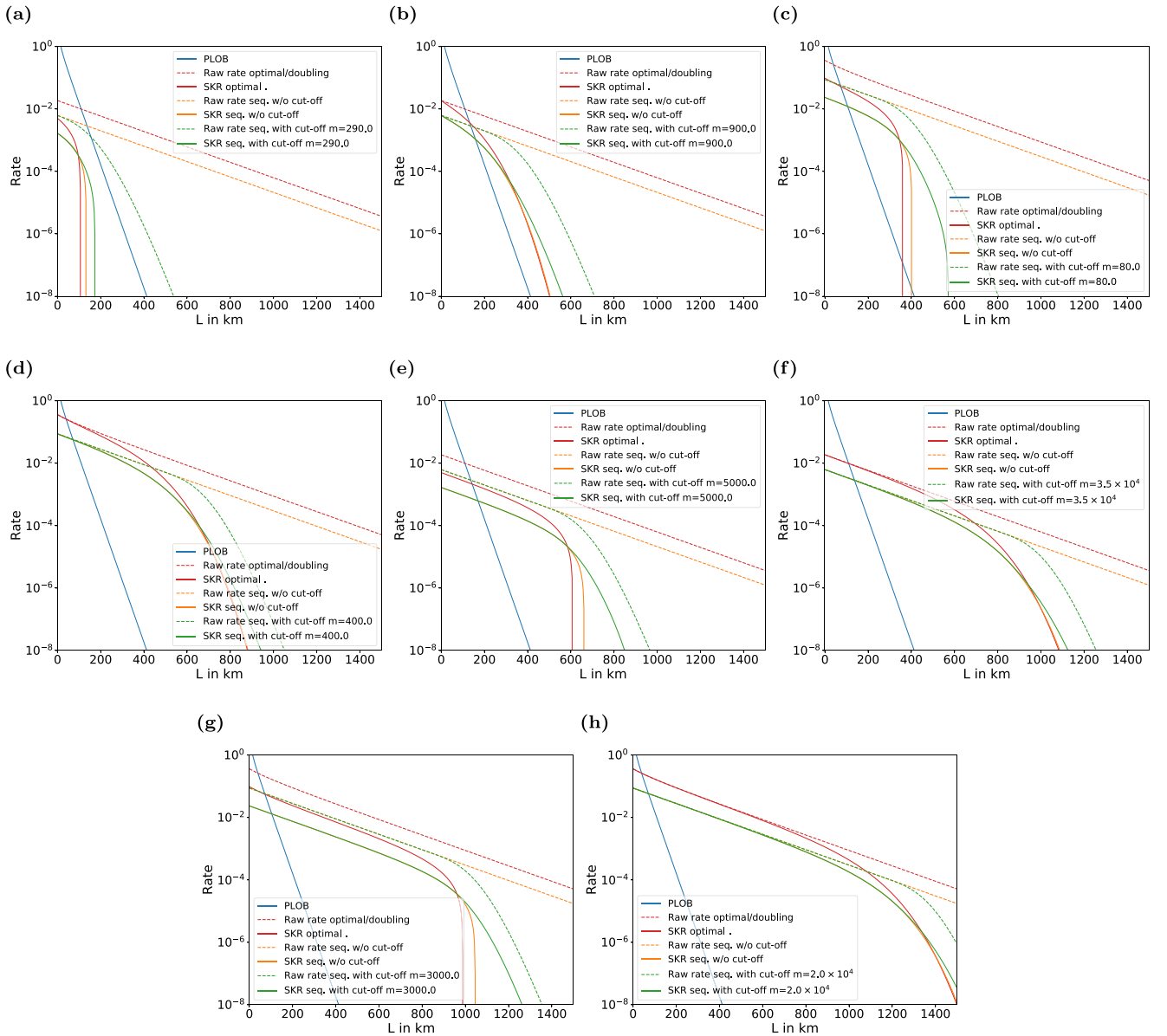


FIG. 24. Comparison of eight-segment repeaters for a total distance L and different experimental parameters: (a) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 0.99$; (b) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 1$; (c) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 0.99$; (d) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 1$; (e) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 0.99$; (f) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.05$, $\mu = \mu_0 = 1$; (g) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 0.99$; and (h) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.7$, $\mu = \mu_0 = 1$. The “optimal” scheme (red) performing BB84 measurements at the end is compared with the fully sequential scheme (orange without the memory cutoff, green with the cutoff) performing immediate measurements on Alice’s/Bob’s sides.

entangled pair of the most right segment is being distributed). This way there is another factor of $1/2$ improvement possible for the effective dephasing, since at any elementary time step there is always only a single memory qubit dephasing instead of a qubit pair. In Fig. 24, for eight repeater segments, we compare this fully sequential scheme and immediate measurements by Alice and Bob with the “optimal” scheme (parallel distribution and swap as soon as possible) where Alice and Bob store their qubits during the whole long-distance distribution procedure to do the BB84 measurements only at the very end. We see that a QKD protocol in which Alice and Bob measure their qubits immediately can be useful in order

to go a bit farther. However, note that in the “optimal” scheme Alice and Bob may also measure their qubits immediately, resulting in higher rates but also requiring a more complicated rate analysis.

APPENDIX G: MIXED STRATEGIES FOR DISTRIBUTION AND SWAPPING

In this Appendix, we shall illustrate that our formalism based on the calculation of PGFs for the two basic random variables is so versatile that we can also obtain the rates for all kinds of mixed strategies. This applies to both the initial

entanglement distributions and the entanglement swappings. In fact, for the case of three repeater segments ($n = 3$), we have already explicitly calculated the secret key rates for all possible schemes with swapping as soon as possible, but with variations in the initial distribution strategies, see Appendix E. This enabled us to consider schemes that are overall slower (exhibiting smaller raw rates), but can have a smaller accumulated dephasing. While swapping as soon as possible is optimal with regards to a minimal dephasing time, it may sometimes also be useful to consider a different swapping strategy. The most commonly considered swapping strategy is doubling which implies that it can sometimes happen that neighboring, ready segments will not be connected, as this would be inconsistent with a doubling of the covered repeater distances at each step. A conceptual argument for doubling could be that for a scalable (nested) repeater system one can incorporate entanglement distillation steps in a systematic way. A theoretical motivation to focus on doubling has been that rates are more easy to calculate—a motivation that is rendered obsolete through the present work, at least for repeaters of size up to $n = 8$. Nonetheless we shall give a few examples for mixed strategies for $n = 4$ and $n = 8$ segments.

For $n = 4$ segments, in addition to those schemes discussed in the main text, let us consider another possibility where we distribute entanglement over the first three segments in the optimal way and then extend it over the last segment. Note that this scheme is a variation of the swapping strategy, while the initial distributions still occur in parallel. As a consequence, it can happen that either segment 4 waits for the first three segments to accomplish their distributions and connections or the first three segments have to wait for segment 4. The scheme serves as an illustration of the rich choice of possibilities for the swapping strategies even when only $n = 4$. We have $D_4^{31}(N_1, N_2, N_3, N_4) = D_3^*(N_1, N_2, N_3) + |\max(N_1, N_2, N_3) - N_4|$ and the PGF of this random variable reads as $\tilde{G}_4^{31}(t) = \frac{p^4}{1-q^4} \frac{P_4^{31}(q,t)}{Q_4^{31}(q,t)}$, with the following numerator and denominator,

$$\begin{aligned}
 P_4^{31}(q, t) &= 1 + (q^2 + 3q^3)t + (q + 3q^2 - q^4 - q^5)t^2 \\
 &\quad + (-2q^2 - 4q^3 - 4q^4 + q^5 + q^6)t^3 \\
 &\quad + (-q^2 - 3q^3 - q^4 - 3q^6 - 3q^7)t^4 \\
 &\quad + (-2q^2 - q^3 + 2q^4 - 2q^6 + q^7 + 2q^8)t^5 \\
 &\quad + (3q^3 + 3q^4 + q^6 + 3q^7 + q^8)t^6 \\
 &\quad + (-q^4 - q^5 + 4q^6 + 4q^7 + 2q^8)t^7 \\
 &\quad + (q^5 + q^6 - 3q^8 - q^9)t^8 - (3q^7 + q^8)t^9 - q^{10}t^{10}, \\
 Q_4^{31}(q, t) &= (1 - qt)(1 - q^2t)(1 - q^3t)(1 - qt^2) \\
 &\quad \times (1 - q^2t^2)(1 - qt^3).
 \end{aligned}$$

If we take the derivatives [see Eq. (16)], we can obtain the following relation:

$$\mathbf{E}[D_4^{\text{dbl}}] = \mathbf{E}[D_4^{31}]. \tag{G1}$$

This means that the two random variables have the same expectation values, even though their distributions are differ-

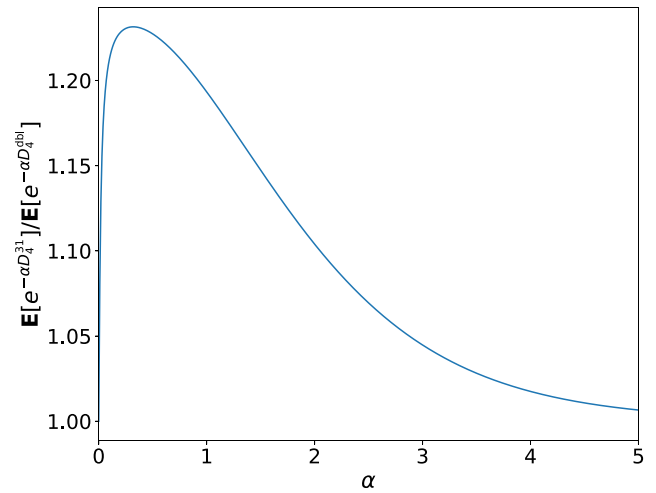


FIG. 25. The ratio given by Eq. (G2) as a function of α for $p = 0.01$ (corresponding to a segment length of 100 km for ideal link coupling).

ent. For the secret key fraction, we need the averages of the exponential of these variables, which essentially leads to the values of the corresponding PGFs [see Eq. (17)]. These do differ, as Fig. 25 illustrates. It shows the ratio

$$\frac{\mathbf{E}[e^{-\alpha D_4^{31}}]}{\mathbf{E}[e^{-\alpha D_4^{\text{dbl}}}] = \frac{\tilde{G}_4^{31}(e^{-\alpha})}{\tilde{G}_4^{\text{dbl}}(e^{-\alpha})}, \tag{G2}$$

as a function of α . The two random variables have the same average, but the average $\mathbf{E}[e^{-\alpha D_4^{31}}]$ is larger than the other, so in the scheme corresponding to the random variable $D_4^{31}(N_1, N_2, N_3, N_4)$ the distributed state has a higher fidelity than the final state in the doubling scheme.

For the case $n = 8$, among a large number of other possibilities to swap the segments, we consider the following three (in addition, the doubling and optimal schemes are discussed in the main text). The first scheme is to swap the two halves of the repeater in the optimal way (for four segments) and then swap the two larger segments. We loosely denote the dephasing variable of these scheme as D_8^{44} , whose definition reads as

$$\begin{aligned}
 D_8^{44}(N_1, \dots, N_8) &= D_4^*(N_1, \dots, N_4) + D_4^*(N_5, \dots, N_8) \\
 &\quad + |\max(N_1, \dots, N_4) \\
 &\quad - \max(N_5, \dots, N_8)|.
 \end{aligned} \tag{G3}$$

Another possibility is to divide the repeater in four pairs, swap them and then swap the four larger segments optimally. The expression for this dephasing variable D_8^{2222} is a straightforward translation of this description:

$$\begin{aligned}
 D_8^{2222}(N_1, \dots, N_8) &= |N_1 - N_2| + \dots + |N_7 - N_8| \\
 &\quad + D_4^*(\max(N_1, N_2), \dots, \max(N_7, N_8)).
 \end{aligned} \tag{G4}$$

Finally, we can divide the segments into three groups, consisting of two, four, and two segments. The middle group we swap optimally (for four segments), and then we swap the three larger segments in the optimal way (for three segments). The

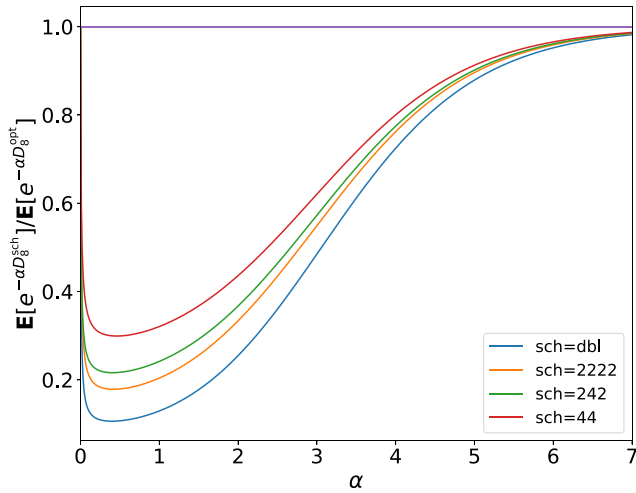


FIG. 26. The ratio in Eq. (G7) for sch = dbl (blue), 2222 (orange), 242 (green), and 44 (red), as a function of α and for $p = 0.01$ (100 km segment length).

definition of the corresponding random variable D_8^{242} reads as

$$D_8^{242}(N_1, \dots, N_8) = |N_1 - N_2| + |N_7 - N_8| + D_4^*(N_3, \dots, N_6) + D_3^*(\max(N_1, N_2), \times \max(N_3, \dots, N_6), \max(N_7, N_8)). \quad (\text{G5})$$

The PGFs of all these variables have all the same form,

$$\frac{p^8 P(q, t)}{1 - q^8 Q(q, t)}, \quad (\text{G6})$$

with appropriate polynomials $P(q, t)$ and $Q(q, t)$. The numerator polynomials $P(q, t)$ are quite large and contain

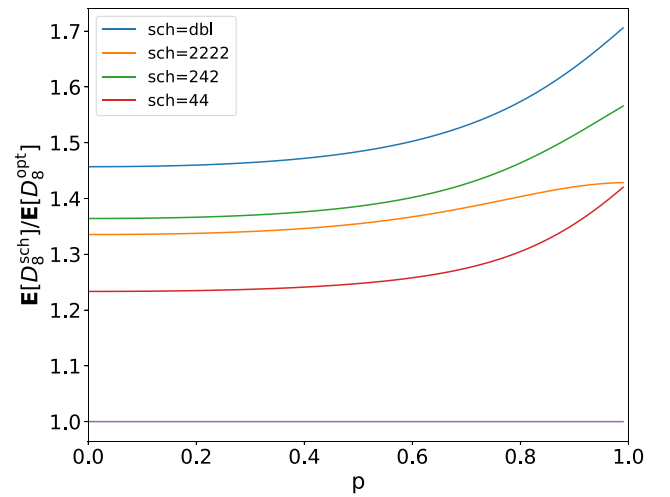


FIG. 27. The ratio in Eq. (53) for sch = dbl (blue), 2222 (orange), 242 (green), and 44 (red), as a function of p .

around one thousand terms, so we do not present them here.

We can compare the performances of different schemes by plotting the ratios

$$\frac{\mathbb{E}[e^{-\alpha D_8^{\text{sch}}}]}{\mathbb{E}[e^{-\alpha D_8^{\text{opt}}}] = \frac{\tilde{G}_8^{\text{sch}}(e^{-\alpha})}{\tilde{G}_8^{\text{opt}}(e^{-\alpha})}, \quad (\text{G7})$$

similar to Eq. (G2), for sch = dbl, 2222, 242, 44. We see that among the five schemes the doubling scheme is the worst with regards to dephasing, and the scheme 44 is the closest to the optimal scheme, see Figs. 26 and 27. This means that the commonly used parallel-distribution doubling scheme, though fast in terms of K_8 , is inefficient in terms of dephasing D_8 by disallowing to swap when neighboring segments are ready on all “nesting” levels [36].

APPENDIX H: TWO-SEGMENT “NODE-RECEIVES-PHOTON” REPEATERS

Figure 28 shows the BB84 rates in a two-segment quantum repeater based on the NRP concept with one middle station receiving optical quantum signals sent from two outer stations at Alice and Bob. By circumventing the need for extra classical communication and thus significantly reducing the effective memory dephasing, the minimal state and gate fidelity values can even be kept constant over large distance regimes. For the experimental clock rate, we have chosen $\tau_{\text{clock}} = 10$ MHz, limited by the local interaction and processing times of the light-matter interface at the middle station.

APPENDIX I: CALCULATION FOR CABRILLO’S SCHEME

First, we consider two entangled states of a single-rail qubit with a quantum memory ($\gamma \in \mathbb{R}$)

$$\frac{1}{1 + \gamma^2} [|\uparrow, \uparrow, 0, 0\rangle + \gamma |\uparrow, \downarrow, 0, 1\rangle + \gamma |\downarrow, \uparrow, 1, 0\rangle + \gamma^2 |\downarrow, \downarrow, 1, 1\rangle]. \quad (\text{I1})$$

After applying a lossy channel with transmission parameter $\eta = p_{\text{link}} \exp(-\frac{L_0}{2L_{\text{att}}})$ to both optical modes, we obtain the following state after introducing two additional environmental modes

$$\frac{1}{1 + \gamma^2} [\gamma^2 |\downarrow, \downarrow\rangle \otimes (\eta |1, 1, 0, 0\rangle + \sqrt{\eta(1-\eta)} (|1, 0, 0, 1\rangle + |0, 1, 1, 0\rangle) + (1-\eta) |0, 0, 1, 1\rangle) + \gamma |\uparrow, \downarrow\rangle \otimes (\sqrt{\eta} |0, 1, 0, 0\rangle + \sqrt{1-\eta} |0, 0, 0, 1\rangle) + \gamma |\downarrow, \uparrow\rangle \otimes (\sqrt{\eta} |1, 0, 0, 0\rangle + \sqrt{1-\eta} |0, 0, 1, 0\rangle) + |\uparrow, \uparrow, 0, 0, 0, 0\rangle]. \quad (\text{I2})$$

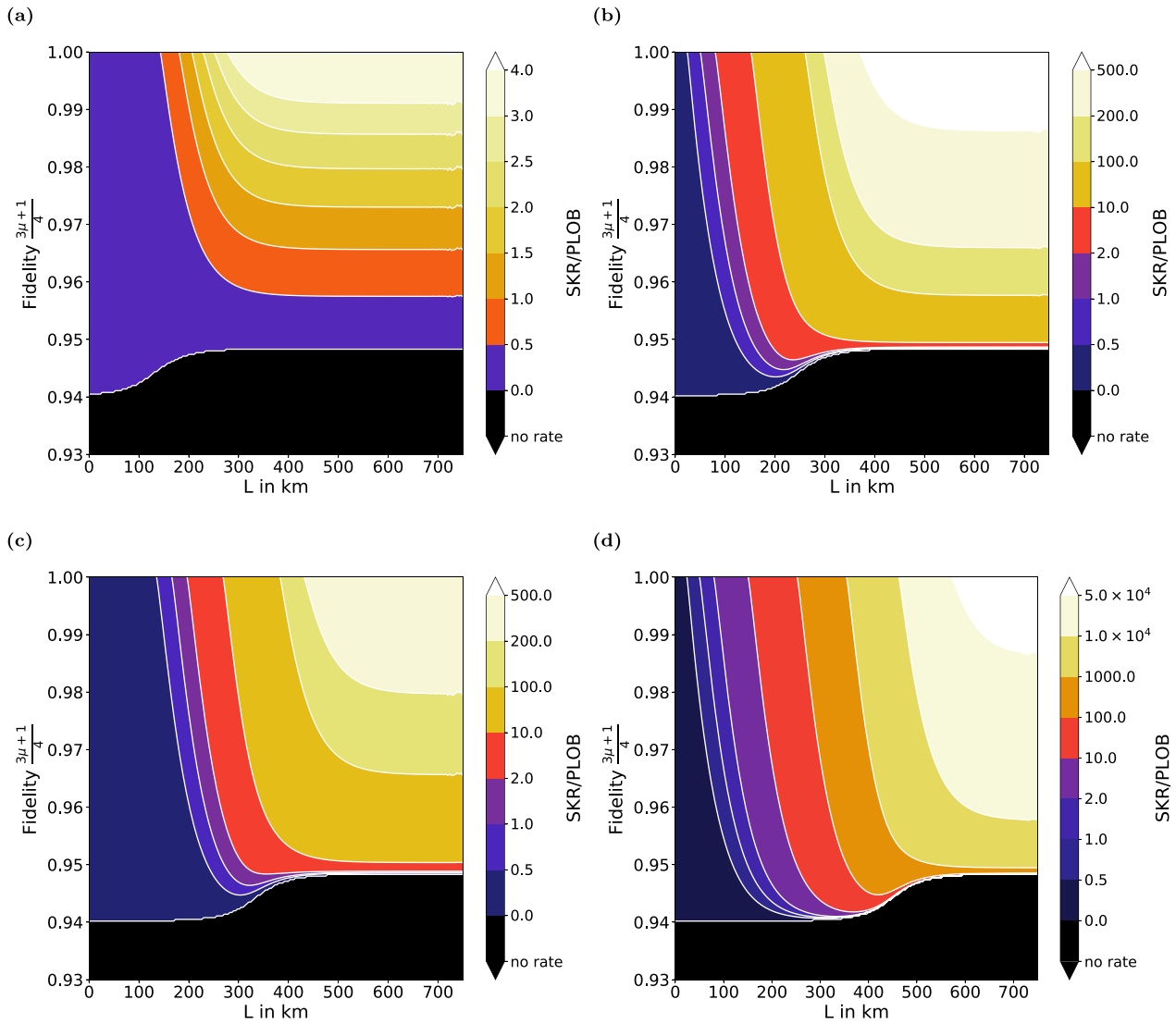


FIG. 28. Contour plots illustrating the minimal fidelity requirements to overcome the PLOB bound by a two-segment NRP repeater for different experimental parameters: (a) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.05$, $m = 1500$; (b) $\tau_{\text{coh}} = 0.1$ s, $p_{\text{link}} = 0.7$, $m = 1500$; (c) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.05$, $m = 1.5 \times 10^5$; and (d) $\tau_{\text{coh}} = 10$ s, $p_{\text{link}} = 0.7$, $m = 1.5 \times 10^5$. In all contour plots, $\mu = \mu_0$, $\tau_{\text{clock}} = 10$ MHz, and $F_0 = 1$ has been used.

We apply a 50:50 beam splitter to the (nonenvironmental) optical mode and obtain the state

$$\begin{aligned}
 & \frac{1}{1 + \gamma^2} \left[\gamma^2 |\downarrow, \downarrow\rangle \otimes \sqrt{\frac{\eta(1-\eta)}{2}} (|1, 0, 0, 1\rangle + |0, 1, 0, 1\rangle + |1, 0, 1, 0\rangle - |0, 1, 1, 0\rangle) \right. \\
 & + \gamma^2 |\downarrow, \downarrow\rangle \otimes \frac{\eta}{2} (|2, 0, 0, 0\rangle - |0, 2, 0, 0\rangle) + \gamma^2 |\downarrow, \downarrow\rangle \otimes (1 - \eta) |0, 0, 1, 1\rangle \\
 & + \gamma |\uparrow, \downarrow\rangle \otimes \left(\sqrt{\frac{\eta}{2}} (|1, 0, 0, 0\rangle - |0, 1, 0, 0\rangle) + \sqrt{1 - \eta} |0, 0, 0, 1\rangle \right) \\
 & \left. + \gamma |\downarrow, \uparrow\rangle \otimes \left(\sqrt{\frac{\eta}{2}} (|1, 0, 0, 0\rangle + |0, 1, 0, 0\rangle) + \sqrt{1 - \eta} |0, 0, 1, 0\rangle \right) + |\uparrow, \uparrow, 0, 0, 0, 0\rangle \right]. \tag{I3}
 \end{aligned}$$

We can obtain entangled memory states by postselecting single photon events at the detectors. If we detect a single photon

at the first detector and no photon at the other, we obtain the following (unnormalized) two-memory reduced density

operator (see Ref. [[45], Appendix E])

$$\frac{\gamma^2 \eta}{(1 + \gamma)^2} [|\Psi^+\rangle\langle\Psi^+| + \gamma^2(1 - \eta)|\downarrow, \downarrow\rangle\langle\downarrow, \downarrow|]. \quad (14)$$

When using simple on/off detectors instead of photon number resolving detectors (PNRD) two-photon events will also lead to a detection event. The two-memory state after a two-photon event is given by

$$\frac{\gamma^4 \eta^2}{4(1 + \gamma^2)^2} |\downarrow, \downarrow\rangle\langle\downarrow, \downarrow|. \quad (15)$$

Thus the probability of a successful entanglement generation is given by $p_{\text{PNRD}} = \frac{2\gamma^2 \eta}{(1 + \gamma^2)^2} (1 + \gamma^2(1 - \eta))$, when using PNRD, and $p_{\text{on/off}} = \frac{2\gamma^2 \eta}{(1 + \gamma^2)^2} (1 + \gamma^2(1 - \frac{3}{4}\eta))$, when using on/off detectors. The factor 2 comes from the possibility to detect the photon at the other detector instead, although in this case the memory state differs by a single-qubit Z -operation. After a suitable twirling, we can find a one-qubit Pauli channel which maps the state $|\Psi^+\rangle\langle\Psi^+|$ to the actual memory state, i.e., we can claim that the loss channel acting on the optical modes induces a Pauli channel on the memories. We can

parametrize this Pauli channel by the tuple of error probabilities (p_I, p_X, p_Y, p_Z) and for the case with PNRDs this tuple is given by

$$\frac{1}{1 + \gamma^2(1 - \eta)} \left(1, \frac{\gamma^2}{2}(1 - \eta), \frac{\gamma^2}{2}(1 - \eta), 0 \right), \quad (16)$$

and for on/off detectors it is given by

$$\frac{1}{1 + \gamma^2(1 - \frac{3}{4}\eta)} \left(1, \frac{\gamma^2}{2} \left(1 - \frac{3}{4}\eta \right), \frac{\gamma^2}{2} \left(1 - \frac{3}{4}\eta \right), 0 \right). \quad (17)$$

When we consider an n -segment repeater, we have to consider a concatenation of n such Pauli channels and we finally obtain the error rates

$$e_x = \frac{1}{2} \left(1 - \mu^{n-1} \mu_0^n \frac{(2F_0 - 1)^n \mathbf{E}[e^{-\alpha D_n}]}{(1 + \gamma^2(1 - \eta))^n} \right), \quad (18)$$

$$e_z = \frac{1}{2} \left(1 - \mu^{n-1} \mu_0^n \left(\frac{1 - \gamma^2(1 - \eta)}{1 + \gamma^2(1 - \eta)} \right)^n \right), \quad (19)$$

in the case of PNRDs. When we consider on/off detectors, we can simply replace η by $\frac{3}{4}\eta$ in the error rates.

-
- [1] F. Arute, K. Arya, R. B. *et al.*, Quantum supremacy using a programmable superconducting processor, *Nature* **574**, 505 (2019).
- [2] M. S. ANIS, H. Abraham, A. *et al.*, Qiskit: An open-source framework for quantum computing, 2023, doi: 10.5281/zenodo.2573505.
- [3] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, P. Hu, X.-Y. Yang, W.-J. Zhang, H. Li, Y. Li, X. Jiang, L. Gan, G. Yang, L. You, Z. Wang *et al.*, Quantum computational advantage using photons, *Science* **370**, 1460 (2020).
- [4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, *Rev. Mod. Phys.* **81**, 1301 (2009).
- [5] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, *Adv. Opt. Photon.* **12**, 1012 (2020).
- [6] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 7 (2014), theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.
- [7] W. Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, *Phys. Rev. Lett.* **91**, 057901 (2003).
- [8] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [9] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, *Nature* **557**, 400 (2018).
- [10] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [11] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum Key Distribution, *Phys. Rev. Lett.* **108**, 130502 (2012).
- [12] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature* **299**, 802 (1982).
- [13] D. Dieks, Communication by epr devices, *Phys. Lett. A* **92**, 271 (1982).
- [14] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication, *Phys. Rev. Lett.* **81**, 5932 (1998).
- [15] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Quantum repeaters based on entanglement purification, *Phys. Rev. A* **59**, 169 (1999).
- [16] L. Hartmann, B. Kraus, H.-J. Briegel, and W. Dur, Role of memory errors in quantum repeaters, *Phys. Rev. A* **75**, 032310 (2007).
- [17] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Long-distance quantum communication with atomic ensembles and linear optics, *Nature* **414**, 413 (2001).
- [18] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Quantum repeaters based on atomic ensembles and linear optics, *Rev. Mod. Phys.* **83**, 33 (2011).
- [19] L. Childress, J. M. Taylor, A. S. Sorensen, and M. D. Lukin, Fault-Tolerant Quantum Communication Based on Solid-State Photon Emitters, *Phys. Rev. Lett.* **96**, 070504 (2006).
- [20] P. C. Humphreys, N. Kalb, J. P. J. Morits, R. N. Schouten, R. F. L. Vermeulen, D. J. Twitchen, M. Markham, and R. Hanson, Deterministic delivery of remote entanglement on a quantum network, *Nature* **558**, 268 (2018).
- [21] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, Hybrid Quantum Repeater Using Bright Coherent Light, *Phys. Rev. Lett.* **96**, 240501 (2006).
- [22] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, Optimal architectures for long distance quantum communication, *Sci. Rep.* **6**, 1 (2016).

- [23] Z. Zhihao, Beijing-shanghai quantum link a ‘new era’, https://usa.chinadaily.com.cn/china/2017-09/30/content_32669867.htm.
- [24] J. Yin, Y. Cao, Y.-H. L. *et al.*, Satellite-based entanglement distribution over 1200 kilometers, *Science* **356**, 1140 (2017).
- [25] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, Experimental Satellite Quantum Communications, *Phys. Rev. Lett.* **115**, 040502 (2015).
- [26] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, *Science* **362**, eaam9288 (2018).
- [27] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin, Experimental demonstration of memory-enhanced quantum communication, *Nature* **580**, 60 (2020).
- [28] S. Langenfeld, P. Thomas, O. Morin, and G. Rempe, Quantum Repeater Node Demonstrating Unconditionally Secure Key Distribution, *Phys. Rev. Lett.* **126**, 230506 (2021).
- [29] P. van Loock, W. Alt, C. Becher, O. Benson, H. Boche, C. Deppe, J. Eschner, S. Höfling, D. Meschede, P. Michler, F. Schmidt, and H. Weinfurter, Extending quantum links: Modules for fiber- and memory-based quantum repeaters, *Adv. Quantum Technol.* **3**, 1900141 (2020).
- [30] D. Luong, L. Jiang, J. Kim, and N. Lütkenhaus, Overcoming lossy channel bounds using a single quantum repeater node, *Appl. Phys. B* **122**, 96 (2016).
- [31] F. Rozpedek, K. Goodenough, J. Ribeiro, N. Kalb, V. Caprara Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D. Elkouss, Realistic parameter regimes for a single sequential quantum repeater, *Quantum Sci. Technol.* **3**, 034002 (2017).
- [32] T. Coopmans, R. Knegjens, A. Dahlberg, D. Maier, L. Nijsten, J. de Oliveira Filho, M. Papendrecht, J. Rabbie, F. Rozpedek, M. Skrzypczyk, L. Wubben, W. de Jong, D. Podareanu, A. Torres-Knoop, D. Elkouss, and S. Wehner, Netsquid, a network simulator for quantum information using discrete events, *Commun. Phys.* **4**, 164 (2021).
- [33] V. V. Kuzmin and D. V. Vasilyev, Diagrammatic technique for simulation of large-scale quantum repeater networks with dissipating quantum memories, *Phys. Rev. A* **103**, 032618 (2021).
- [34] V. V. Kuzmin, D. V. Vasilyev, N. Sangouard, W. Dör, and C. A. Muschik, Scalable repeater architectures for multi-party states, *npj Quantum Inf.* **5**, 115 (2019).
- [35] E. Shchukin, F. Schmidt, and P. van Loock, Waiting time in quantum repeaters with probabilistic entanglement swapping, *Phys. Rev. A* **100**, 032322 (2019).
- [36] E. Shchukin and P. van Loock, Optimal Entanglement Swapping in Quantum Repeaters, *Phys. Rev. Lett.* **128**, 150502 (2022).
- [37] S. E. Vinay and P. Kok, Statistical analysis of quantum-entangled-network generation, *Phys. Rev. A* **99**, 042313 (2019).
- [38] S. Khatri, C. T. Matyas, A. U. Siddiqui, and J. P. Dowling, Practical figures of merit and thresholds for entanglement distribution in quantum networks, *Phys. Rev. Res.* **1**, 023032 (2019).
- [39] A. Sipahigil, R. E. Evans, D. D. Sukachev, M. J. Burek, J. Borregaard, M. K. Bhaskar, C. T. Nguyen, J. L. Pacheco, H. A. Atikian, C. Meuwly, R. M. Camacho, F. Jelezko, E. Bielejec, H. Park, M. Lončar, and M. D. Lukin, An integrated diamond nanophotonics platform for quantum-optical networks, *Science* **354**, 847 (2016).
- [40] L. Childress and R. Hanson, Diamond nv centers for quantum computing and quantum networks, *MRS Bull.* **38**, 134 (2013).
- [41] O. A. Collins, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy, Multiplexed Memory-Insensitive Quantum Repeaters, *Phys. Rev. Lett.* **98**, 060502 (2007).
- [42] S. Santra, L. Jiang, and V. S. Malinovsky, Quantum repeater architecture with hierarchically optimized memory buffer times, *Quantum Sci. Technol.* **4**, 025010 (2019).
- [43] T. Coopmans, S. Brand, and D. Elkouss, Improved analytical bounds on delivery times of long-distance entanglement, *Phys. Rev. A* **105**, 012608 (2022).
- [44] T. D. Ladd, P. van Loock, K. Nemoto, W. J. Munro, and Y. Yamamoto, Hybrid quantum repeater based on dispersive cqed interactions between matter qubits and bright coherent light, *New J. Phys.* **8**, 184 (2006).
- [45] F. Schmidt and P. van Loock, Memory-assisted long-distance phase-matching quantum key distribution, *Phys. Rev. A* **102**, 042614 (2020).
- [46] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, *Nat. Commun.* **8**, 15043 (2017).
- [47] C. Schuck, W. H. P. Pernice, and H. X. Tang, Waveguide integrated low noise nbtin nanowire single-photon detectors with milli-hz dark count rate, *Sci. Rep.* **3**, 1893 (2013).
- [48] D. Bruß, Optimal Eavesdropping in Quantum Cryptography with Six States, *Phys. Rev. Lett.* **81**, 3018 (1998).
- [49] F. Rozpedek, R. Yehia, K. Goodenough, M. Ruf, P. C. Humphreys, R. Hanson, S. Wehner, and D. Elkouss, Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission, *Phys. Rev. A* **99**, 052330 (2019).
- [50] N. K. Bernardes, L. Praxmeyer, and P. van Loock, Rate analysis for a hybrid quantum repeater, *Phys. Rev. A* **83**, 012323 (2011).
- [51] S. Pirandola, End-to-end capacities of a quantum communication network, *Commun. Phys.* **2**, 51 (2019).
- [52] D. Gottesman and H.-K. Lo, Proof of security of quantum key distribution with two-way classical communications, *IEEE Trans. Inf. Theory* **49**, 457 (2003).
- [53] M. Razavi, M. Piani, and N. Lütkenhaus, Quantum repeaters with imperfect memories: Cost and scalability, *Phys. Rev. A* **80**, 032301 (2009).
- [54] R. Laurenza, N. Walk, J. Eisert, and S. Pirandola, Rate limits in quantum networks with lossy repeaters, *Phys. Rev. Res.* **4**, 023158 (2022).
- [55] B. Eisenberg, On the expectation of the maximum of iid geometric random variables, *Stat. Probab. Lett.* **78**, 135 (2008).
- [56] K. Azuma, K. Tamaki, and W. J. Munro, All-photonic intercity quantum key distribution, *Nat. Commun.* **6**, 10171 (2015).
- [57] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto, From quantum multiplexing to high-performance quantum networking, *Nat. Photonics* **4**, 792 (2010).
- [58] R. Trényi and N. Lütkenhaus, Beating direct transmission bounds for quantum key distribution with a multiple quantum memory station, *Phys. Rev. A* **101**, 012325 (2020).
- [59] C. Jones, D. Kim, M. T. Rakher, P. G. Kwiat, and T. D. Ladd, Design and analysis of communication protocols for quantum repeater networks, *New J. Phys.* **18**, 083015 (2016).

- [60] M. Razavi, K. Thompson, H. Farmanbar, M. Piani, and N. Lütkenhaus, *Physical and Architectural Considerations in Quantum Repeaters* (SPIE, 2009), p. 723603.
- [61] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, *Nat. Commun.* **5**, 1 (2015).
- [62] C. Cabrillo, J. I. Cirac, P. García-Fernández, and P. Zoller, Creation of entangled states of distant atoms by interference, *Phys. Rev. A* **59**, 1025 (1999).
- [63] A. Klenke, Erzeugendenfunktion, in *Wahrscheinlichkeitstheorie* (Springer, Berlin, Heidelberg, 2020), pp. 85–93.
- [64] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, 600-km repeater-like quantum communications with dual-band stabilization, *Nat. Photonics* **15**, 530 (2021).
- [65] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km, *Phys. Rev. Lett.* **124**, 070501 (2020).
- [66] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, D.-F. Zhao, W.-J. Zhang, F.-X. Chen, H. Li, L.-X. You, Z. Wang, Y. Chen, X.-B. Wang, Q. Zhang, and J.-W. Pan, Quantum Key Distribution over 658 km Fiber with Distributed Vibration Sensing, *Phys. Rev. Lett.* **128**, 180502 (2022).
- [67] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution over 830-km fibre, *Nat. Photonics* **16**, 154 (2022).
- [68] J. Lin and N. Lütkenhaus, Simple security analysis of phase-matching measurement-device-independent quantum key distribution, *Phys. Rev. A* **98**, 042332 (2018).
- [69] S. Das, S. Bauml, M. Winczewski, and K. Horodecki, Universal Limitations on Quantum Key Distribution over a Network, *Phys. Rev. X* **11**, 041016 (2021).
- [70] S. Das, S. Khatri, and J. P. Dowling, Robust quantum network architectures and topologies for entanglement distribution, *Phys. Rev. A* **97**, 012335 (2018).

Paper V

Error-corrected quantum repeaters with GKP qudits

Frank Schmidt, Daniel Miller, and Peter van Loock

arXiv:2303.16034, submitted to Quantum (2023)

Error-corrected quantum repeaters with GKP qudits

Frank Schmidt¹, Daniel Miller², and Peter van Loock¹

¹Institute of Physics, Johannes Gutenberg-Universität Mainz, Staudingerweg 7, 55128 Mainz, Germany.

²Dahlem Center for Complex Quantum Systems and Institut für Theoretische Physik, Freie Universität Berlin, Arnimallee 14, 14195 Berlin, Germany.

March 29, 2023

The Gottesman-Kitaev-Preskill (GKP) code offers the possibility to encode higher-dimensional qudits into individual bosonic modes with, for instance, photonic excitations. Since photons enable the reliable transmission of quantum information over long distances and since GKP states subject to photon loss can be recovered to some extent, the GKP code has found recent applications in theoretical investigations of quantum communication protocols. While previous studies have primarily focused on GKP qubits, the possible practical benefits of higher-dimensional GKP qudits are hitherto widely unexplored. In this paper, we carry out performance analyses for three quantum repeater protocols based on GKP qudits including concatenations with a multi-qudit quantum polynomial code. We find that the potential data transmission gains for qudits are often hampered by their decreased GKP error-correcting capabilities. However, we also identify parameter regimes in which having access to an increased number of quantum levels per mode can enhance the theoretically achievable secret-key rate of the quantum repeater. Some of our protocols share the attractive feature that local processing and complete error syndrome identification are realizable without online squeezing. Provided a supply of suitable multi-mode GKP states is available, this can be realized with a minimal set of passive linear optical operations, even when the logical qudits are composed of many physical qudits.

Frank Schmidt: scfrank@uni-mainz.de

Peter van Loock: loock@uni-mainz.de

Contents

1	Introduction	3
2	Setting	5
2.1	Repeater protocols	5
2.1.1	Two-way teleportation protocol with classical post-amplification . . .	6
2.1.2	One-way teleportation protocol with optical pre-amplification	6
2.1.3	One-way half-teleportation protocol with optical pre-amplification . .	8
2.2	Some comments on potential realizations of qudit repeaters	8
2.3	Noise model	9
2.3.1	Transmission loss and coupling inefficiencies	9
2.3.2	Approximate GKP state generation	9
2.3.3	Converting Gaussian noise into Pauli errors	10
3	Secret-key rates of quantum repeaters	11
3.1	Repeater performance with GKP error correction only	11
3.2	Repeater performance with both GKP and higher-level error correction . . .	13
3.2.1	Optimal choice of the repeater spacing	14
3.2.2	Identifying and overcoming noise bottlenecks	15
3.2.3	Leveraging lower-level syndrome information to improve higher-level error correction	17
4	Conclusion and outlook	18
A	Error analysis of bare GKP repeaters	20
B	Error analysis of GKP repeaters with higher-level codes	21
B.1	Logical performance of GKP qudits concatenated with quantum polynomial codes	21
B.2	Error analysis of the half-teleportation protocol for various placements of GKP syndrome measurements	22
C	Author contributions	24

1 Introduction

Quantum technologies rely on the availability of precisely controllable quantum systems, e.g., qubits, which can be realized with various physical implementations. In 2000, Gottesman, Kitaev, and Preskill (GKP) proposed a method to encode finite-dimensional quantum systems (qudits) into quantum-mechanical harmonic oscillators [1]. More recent theoretical developments include further proposals and assessments of GKP state preparation with superconducting devices [2, 3]. After years of experimental progress, GKP qubits finally have been demonstrated in superconducting microwave cavities [4-6] and in the harmonic motion of ions [7, 8].

In the optical domain, on the other hand, preparing GKP states is notoriously difficult. The main problem is that reliable and strong nonlinearities are required but not readily available. In one approach, Gaussian Boson Sampling [9, 10], one exploits that measurements can induce nonlinear effects. Here, Gaussian resource states are combined via passive linear optics and partially read out via photon-number resolving measurements. In this way, high-quality optical GKP states can be obtained, albeit only probabilistically. Gaussian Boson Sampling requires detectors with a sufficiently high level of photon-number resolution as well as increasingly complex linear circuits [9, 10]. To shift the experimental burden associated with this, alternative approaches have been proposed [11, 12]. If non-Gaussian resource states or non-Gaussian optical elements are available, a recursive application of short linear circuits and homodyne measurements is sufficient for the preparation of GKP states [13-15]. There also exist alternatives which do not rely on measurements at all [15, 16]. A final option is to combine photon-subtraction- and homodyne-based elements to convert many-mode Gaussian cluster states into non-Gaussian few-mode states, which can be further processed into GKP states [17]. Such an approach is compatible with measurement-based, continuous-variable quantum computation [15, 18].

While the best method for creating optical GKP states has not yet been identified, it is safe to assume that their physical realization will require extremely sophisticated experimental procedures. Once such technology is available, however, it will be comparatively straightforward to extend it to higher-dimensional GKP qudits and to concatenated multi-qubit or -qudit GKP codes. For example, multiple GKP qubits can be entangled via Gaussian operations [1]. Furthermore, ordinary beam splitters enable the generation of certain collective GKP ancilla states such as Bell states with GKP qubits [19] or qudits [20], as well as the collective detection of their error syndromes [20]. To guide such future experiments, we find it meaningful to investigate the performance of advanced multi-qudit GKP protocols in the realm of quantum communication.

The GKP encoding enables the correction of small displacement errors of the oscillator's quadratures, in particular, those that originate from typical Gaussian error channels such as amplitude damping or photon loss. However, large displacement errors cannot be avoided completely, especially for realistic, finitely-squeezed GKP states. This can cause misidentification of error syndromes, which leads to discrete logical errors on the affected GKP qudits.

In order to correct such errors, a higher-level quantum error-correcting code (QECC) can be employed to encode a few logical qudits into a larger number of physical GKP qudits [3, 21-26]. Hereby, the error correction capability of the higher-level QECC can benefit from analog information in the single-qudit GKP syndrome measurements [21-24]. In order to satisfy the quantum singleton bound $n - k \geq 2(d - 1)$, every QECC with code parameters $[[n, k, d]]$ must trade off the number of correctable (arbitrary) single-qudit errors against the number of physical qudits per logical qudit, which are given by $\lfloor (d - 1)/2 \rfloor$

and n/k , respectively [27-29]. An optimal trade-off is obtained by those QECCs that meet the quantum singleton bound with equality and are called maximum distance separable (MDS) codes. While, for qubits, the only [30] nontrivial (i.e., $d \geq 3$ and $k \geq 1$) MDS code encodes one logical qubit into five physical qubits [31], there is a plethora of MDS codes for higher-dimensional qudits. Such QECCs are explicitly available in the form of quantum polynomial codes, which exist for every qudit dimension being a prime power [32-35].

Currently, experimental realizations of long-distance quantum communication protocols are limited by the rapid decay of photonic signals that are sent through optical fibers. This process is formally described by a pure-loss bosonic channel $\mathcal{L}(\eta)$, which arises from mixing the bosonic signal mode with an environmental mode in the vacuum state using a beam splitter with transmittance η . In the long-distance limit of $\eta \rightarrow 0$, the secret-key capacity of the single-mode pure-loss channel scales linearly with η [36], more precisely, it is given by $-\log_2(1 - \eta) \approx 1.44 \eta$ [37]. In consequence, the secret-key rate of point-to-point quantum key distribution (QKD) is exponentially suppressed in the length L of an optical fiber, which typically has a transmittance of $\eta = \exp(-L/22 \text{ km})$.

To overcome this problem, quantum repeaters have been proposed [38]. By introducing repeater stations, a long channel is split into multiple shorter ones. To cope with the loss, different strategies have been conceptualized and, subsequently, been classified into three so-called generations of quantum repeaters [39]. These generations fundamentally differ in their speed of operation and in the level of technological maturity required for their realization.

First-generation quantum repeaters are based on heralded, probabilistic entanglement distribution [38]. Once a Bell pair is successfully distributed between two neighboring repeater stations, it is stored in local quantum memories, where it resides until a second Bell pair, which connects the two repeater stations to a third one, is created. Whenever two parts of different Bell pairs are present in a single repeater station, entanglement swapping can be executed, which results in a single Bell pair ranging over a larger distance. This process is repeated until a long-distance Bell pair is shared between Alice and Bob. In addition to channel loss, unavoidable operational gate and storage errors pose a challenge for quantum repeaters. To cope with such errors, first-generation quantum repeaters employ nested entanglement purification [40], a probabilistic protocol for the distillation of multiple low-fidelity Bell pairs into a smaller number of states with higher fidelities, involving two-way classical communication. In the worst case, entanglement purification has to be performed across the total distance L of the entire quantum repeater chain, which slows down the achievable repetition rate to c/L or less, where $c = 2.14 \times 10^8 \frac{\text{m}}{\text{s}}$ is the speed of photons in fiber (for both classical and quantum signaling).

To avoid this slow-down, *second-generation quantum repeaters* [41] replace entanglement purification by QECCs for the local memories. With this modification in place, the rate bottleneck is now posed by classical communication between neighboring repeater stations, which are separated by a distance of L_0 . Only after a failed entanglement distribution attempt has been heralded, the quantum memories can be freed up for the next attempt. Therefore, the improved upper bound on the repetition rate is now given by c/L_0 , which is typically on the order of 1 kHz for $L_0 \sim 100 \text{ km}$ to 1 MHz for $L_0 \sim 100 \text{ m}$. The only possibility to speed up the classical two-way communication is to reduce L_0 , i.e., to invest in a larger number of, realistically imperfect, faulty repeater stations whose quantum information must be consistently protected by the QECC.

Finally, *third-generation quantum repeaters* enable ultrafast quantum communication as they dispense with the temporary storage of quantum information and classical two-way communication altogether [42-44]. Instead, these repeaters employ QECCs to correct both

channel losses and operational errors. The repetition rates in this case are only limited by the speed of state preparations, local gate operations, and measurements in the individual repeater stations. Whereas the preparation of QECC-encoded multi-photon states typically relies on some form of light-matter interaction, all other components of a third-generation quantum repeater can, in principle, be realized in an all-optical fashion [45-49].

In this paper, we theoretically analyze the performance of third-generation quantum repeaters based on optical GKP qudits. Our investigation also includes cases where the GKP code is concatenated with a higher-level QECC. Here, we focus on quantum polynomial codes that previously have been considered in combination with multi-mode and Fock-encoded qudits [50-53]. For GKP-encoded states, similar performance studies have only been carried out in the special case of qubits [54-56]. Our work thus closes the gap between these two approaches to a certain extent as it offers a treatment of the remaining case of GKP qudits. The consideration of qudits, which can transmit more quantum information per channel use than qubits, in the context of GKP and third-generation quantum repeaters is particularly attractive due to the existence of hardware-efficient GKP-qudit operations and syndrome extraction routines based on linear-optical elements alone. In this way, the only fundamental experimental challenge that remains is to provide a supply of suitable multi-mode GKP ancilla states, a problem that can be tackled independently.

This paper is structured as follows. In Sec. 2, we describe the details of our study: we begin with introducing the repeater protocols under investigation in Secs. 2.1 and 2.2 and proceed with our noise model in Sec. 2.3. In Sec. 3, we present the secret-key rates obtainable with the different GKP qudit repeater protocols and discuss the influence of various experimental parameters. Finally, in Sec. 4, we summarize our results and conclude with a recommendation of the most promising quantum repeater protocol based on GKP qudits as identified in this work.

2 Setting

GKP codes encode a D -dimensional qudit within the Fock space \mathcal{F} of a quantum mechanical harmonic oscillator [1]. We denote the annihilation operator of the oscillator by \hat{a} and its quadrature operators by $\hat{p} = \frac{i}{\sqrt{2}}(\hat{a}^\dagger - \hat{a})$ and $\hat{q} = \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{a})$. For simplicity, we focus in this paper on the square GKP code, which is defined as the D -dimensional subspace of \mathcal{F} that is invariant under the action of $S_X = \exp(-i\sqrt{2\pi D}\hat{p})$ and $S_Z = \exp(i\sqrt{2\pi D}\hat{q})$. By repeated non-destructive measurements of the stabilizer operators S_X and S_Z , followed by appropriate displacement operations (or, at least, through tracking of the corresponding generalized Pauli frame), one can enforce the state of the oscillator to (effectively) remain in the GKP code space. Since the logical Pauli operators of the square GKP code are given by $X = \exp(-i\sqrt{\frac{2\pi}{D}}\hat{p})$ and $Z = \exp(i\sqrt{\frac{2\pi}{D}}\hat{q})$, it is thereby possible (in the idealizing limit of perfect GKP states) to correct arbitrary displacement errors that are smaller than $\sqrt{\pi/2D}$ in magnitude. To implement two-qudit gates between GKP qudits, one can utilize common two-mode Gaussian gates. For example, on the level of GKP qudits, the bosonic CSUM-gate, $\exp(-i\hat{q}_1\hat{p}_2)$, acts as a two-qudit controlled- X gate, $CX = \sum_{k=0}^{D-1} |k\rangle\langle k|_1 \otimes X_2^k$. A similarly defined CZ -gate is implemented by means of a CPHASE-gate, $\exp(i\hat{q}_1\hat{q}_2)$.

2.1 Repeater protocols

Since GKP qudits can be encoded into photons, which are the ideal carriers of "flying" quantum information propagating at maximal speed, they have been envisioned in the context of quantum communication [55-57]. In this paper, we investigate certain quantum

communication protocols that only require qudit Clifford operations and generalized Pauli measurements [58], which can be simply realized with GKP qudits by means of Gaussian optics and homodyne detection, respectively. More precisely, we analyze and compare the performance of three third-generation quantum repeater protocols introduced in the following subsections. For each protocol, the term “qudit” may either refer to a bare (physical) GKP qudit or to an ensemble of multiple GKP qudits encoding a single (logical) qudit using a higher-level QECC, in particular, in combination with Knill’s error-correction-by-teleportation procedure [20, 59]. Even in the absence of a higher-level QECC, our protocols represent instances of error-corrected (third-generation) quantum repeaters, as the availability of GKP syndrome information facilitates the correction of displacement errors to a certain extent.

2.1.1 Two-way teleportation protocol with classical post-amplification

The first of the three quantum repeater chains under investigation is portrayed in Fig. 1 (a). For this protocol, every repeater station prepares a pair of qudits in a (logical) Bell state. One of the qudits is sent in the direction of the next repeater station, while the other one is sent backward. In the middle between two neighboring repeater stations, the forward- and backward-propagating qudits are joined in a (logical) Bell measurement, which is implementable on the physical level with (transversal) beam splitters and two homodyne detectors per physical Bell measurement [20]. During the transmission from the repeater stations to the central Bell measurement apparatus, the states of the qudits are altered due to the finite transmittance of the optical fiber channel. For the general case of many physical qudits representing one logical qudit, the optical loss channels act individually and independently (i.i.d.) upon the different modes of the physical multi-mode state that propagates through each fiber segment. To facilitate a direct comparison with the other protocols, we denote the channel transmittance by $\sqrt{\eta} = \exp(-L_0/2L_{\text{att}})$, as the relevant length of the fiber is given by $L_0/2$ here. Throughout this paper, L_0 denotes the distance between two adjacent repeater stations, and $L_{\text{att}} = 22$ km is the attenuation length of a typical fiber at the telecommunication wavelength of 1550 nm. In order to compensate for the loss-induced state change (with damped quadrature amplitudes), the classical measurement signal of the Bell measurements needs to be correspondingly amplified by a factor of $\sqrt{\eta}^{-1}$ before decoding the GKP syndrome. Overall, this protocol produces an imperfect Bell pair ranging from one end of the repeater chain to the other. Note that classical communication is only needed for post-processing and, therefore, it does not slow down the repetition rates of this protocol. Further note that for the case of a logical qudit composed of many physical qudits, classical post-amplification is performed individually for each physical Bell measurement to obtain the syndrome of the higher-level QECC [20].

2.1.2 One-way teleportation protocol with optical pre-amplification

As a modification of the protocol from Sec. 2.1.1, we also consider a quantum repeater chain where the Bell measurements are executed within the repeater stations, see Fig. 1 (b). Here, only one qudit per Bell pair is transmitted through the fiber channel. This time, the transmittance is given by $\eta = \exp(-L_0/L_{\text{att}})$ because the traveling distance of the photons now covers a full repeater segment, i.e., twice the distance as in the previous scenario. To cope with the fiber losses, an optical pre-amplification channel $\mathcal{A}(\eta^{-1})$ is i.i.d. applied to each (physical) GKP mode before it is sent through the fiber; this step replaces the classical post-amplification of the measurement signal from Sec. 2.1.1.

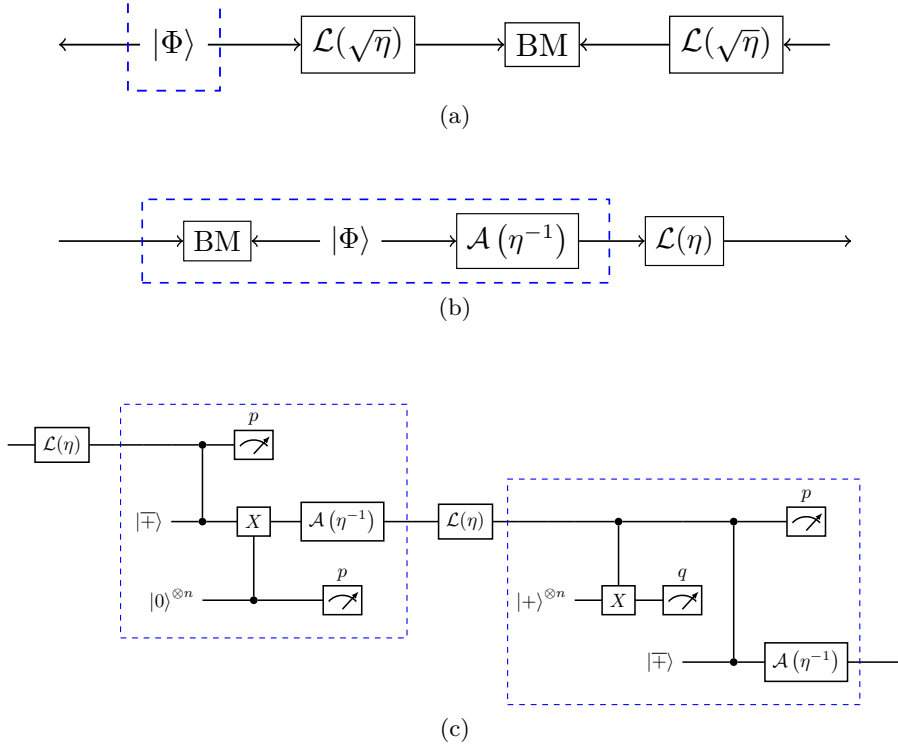


Figure 1: Unit cells of the quantum repeater protocols considered in this work. The transmittance $\eta = \exp(-L_0/L_{\text{att}})$ of the bosonic pure-loss channel $\mathcal{L}(\eta)$ is exponentially suppressed in the distance L_0 between adjacent repeater stations (dashed blue boxes). Here, the qudits can be either individual GKP qudits or logical qudits that are comprised of multiple GKP qudits by means of a higher-level $\llbracket n, 1, d \rrbracket_D$ QECC. **(a)** In the **two-way teleportation protocol**, every repeater station prepares two qudits in the maximally entangled state $|\Phi\rangle = \frac{1}{\sqrt{D}} \sum_{k=0}^{D-1} |k, k\rangle$. One of the two qudits is sent forward and the other one backward. After propagating a distance of $L_0/2$, at which each physical mode has been subject to a loss channel $\mathcal{L}(\sqrt{\eta})$, a Bell measurement (BM) is performed. **(b)** Also in the **one-way teleportation protocol**, two qudits are prepared in state $|\Phi\rangle$. In contrast to (a), only one of the qudits is sent to an adjacent repeater station. To compensate for loss, a quantum-limited amplification channel $\mathcal{A}(\eta^{-1})$ with gain η^{-1} is applied to each of the physical GKP modes. After propagating a distance of L_0 , a BM combines the forward-moving qudit with the stationary qudit of the subsequent repeater station. **(c)** The **one-way half-teleportation protocol** is a GKP-adaptation of a previously-studied discrete-variable protocol [53]. Here, we add measurements to convert displacement errors into Pauli errors. Overlined ancilla states represent codewords of the higher-level $\llbracket n, 1, d \rrbracket_D$ QECC, while ancilla states without overscore stand for GKP codewords. The \overline{CX} -gates correspond to transversal CSUM-gates and the \overline{CZ} -gates corresponds to semi-transversal CPHASE-gates. Measurements of q and p denote the measurement of the position and momentum quadrature, respectively. Loss and amplifier channels are again to be understood to act individually and independently on the physical GKP modes.

2.1.3 One-way half-teleportation protocol with optical pre-amplification

The utilization of a Bell measurement (protocols described in Sec. 2.1.1 and Sec. 2.1.2) provides GKP syndrome information for both quadratures. This facilitates the correction of displacement errors on the level of the (physical and logical) GKP qudits. For the final repeater chain under consideration, on the other hand, every repeater station is responsible for preparing and measuring only a single logical GKP qudit, see Fig. 1 (c). This protocol has two core components. First, a lower-level GKP error correction converts naturally occurring Gaussian displacement errors into Pauli errors on the physical qudits, see Sec. 2.3.3. Second, a higher-level QECC is utilized to cope with the resulting Pauli errors. At the start of the repeater chain, Alice prepares two higher-level logical qudits in the state $|\overline{\mp}\rangle = \sum_k |\bar{k}\rangle/\sqrt{D}$ and entangles them with a logical \overline{CZ} -gate. Since we restrict ourselves to quantum polynomial codes, the \overline{CZ} -gate admits a semi-transversal implementation with favorable error-spreading properties [33]. Alice stores one of the logical qudits and to the second one, she applies a quantum-limited amplifier with gain η^{-1} to each of the physical GKP modes before she sends them jointly through a lossy fiber of transmittance η to the first repeater station, where the incoming logical qudit is entangled with a new logical qudit in state $|\overline{\mp}\rangle$. A subsequent destructive, (physical) quditwise p -measurement effectively transfers the encoded quantum information onto the next qudit and simultaneously delivers syndrome information involving X -stabilizers. These steps are then repeated at every repeater station. Besides yielding higher-level X -syndromes, the p -measurements are also responsible for providing lower-level GKP syndrome information $p \bmod \sqrt{2\pi/D}$. The physical CZ -gates propagate Gaussian p -errors on one mode into q -errors on the next one. To prevent these q -errors from merging with q -errors that occur at the subsequent transmission, we introduce an additional ancilla-based GKP syndrome measurement in every repeater station. This can be done in multiple ways, as discussed in App. B.2. To complete the protocol, all measurement results are communicated to Bob, who applies a suitable correction operator depending on the measurement outcomes [52]. Assuming N is even and in the absence of errors, this protocol is equivalent to $N/2$ teleportation sub-routines spread over $N + 1$ different laboratories. For this reason, we refer to this protocol as *half-teleportation*.

2.2 Some comments on potential realizations of qudit repeaters

To compensate for fiber loss, it is crucial to amplify the signal. For the two protocols in Secs. 2.1.1 and 2.1.2, one may opt between optical pre-amplification and classical post-amplification. For the half-teleportation protocol in Sec. 2.1.3, on the other hand, optical pre-amplification is the only option. This is because the GKP qudits need to be correctly scaled, i.e., they need to be in the GKP code space up to a displacement, before the CZ -gate is applied. Since classical post-amplification can be carried out conveniently in software, lacking this option may be considered as a disadvantage of the half-teleportation protocol.

While we analyze their performance for GKP qudits, these protocols can be straightforwardly adapted to other qudit encodings, such as multi-mode (MM) qudits, which have been experimentally demonstrated in the context of (repeaterless) higher-dimensional quantum key distribution in the form of orbital angular momentum [60] and time-bin qudits [61]. Two of the three repeater protocols under consideration rely on Bell measurements. For GKP qudits, a deterministic Bell measurement can easily be implemented with static linear optics by employing a balanced beam splitter and continuous-variable homodyne measurements. Experimental implementations of Bell measurements for MM-encoded

qudits, on the other hand, are disproportionately more involved. Moreover, deterministic CX -gates for MM qudits require strong nonlinearities that are typically mediated through auxiliary matter qudits, which reduces the achievable repetition rates to the order of MHz. This is in stark contrast to all-optical implementations that can reach GHz repetition rates. An attempt to circumvent this shortcoming of MM qudits is based on probabilistic linear optical Bell measurements, enabling an all-optical error correction step at every repeater station [45-49]. Such probabilistic Bell measurements cannot exceed 50% for MM qubits in the simplest setting without additional resources such as photonic ancilla states [62-64]. For a deterministic Bell measurement, nonlinear optics is required. Furthermore, probabilistic unambiguous state discrimination measurement of the corresponding two-qudit Bell states, making only use of linear optics and photon counting without ancilla photons, is impossible for MM qudits with $D > 2$ [65, 66]. Therefore, overall, the GKP concept and the GKP-based QR protocols presented in this work represent a unique way to combine an increased communication capacity based on photonic qudit encoding with an enhanced loss (and error) robustness based on photonic qudit quantum error correction.

2.3 Noise model

GKP codes are designed to correct displacement errors. As we review next, this allows us to model photon loss and imperfect GKP state preparation with incoherent Gaussian displacement channels. For our error analyses, it will suffice to keep track of their variances.

2.3.1 Transmission loss and coupling inefficiencies

The bosonic pure-loss channel $\mathcal{L}(\eta)$ is commonly used to model fiber loss and coupling inefficiencies in quantum communication protocols [67, 68]. When $\mathcal{L}(\eta)$ is applied to a GKP state, its quadratures are damped, which shrinks the GKP lattice. To rescale the lattice, one has to amplify the signal. Depending on whether this amplification is carried out optically before $\mathcal{L}(\eta)$, optically after $\mathcal{L}(\eta)$, or classically after the measurement of a quadrature operator, the effective error channel on the GKP subspace is altered.

For the one-way protocols in Secs. 2.1.2 and 2.1.3, we consider the usage of an optical amplification channel $\mathcal{A}(\eta^{-1})$. If $\mathcal{A}(\eta^{-1})$ is applied *after* $\mathcal{L}(\eta)$, the result is a Gaussian displacement channel with variance $\sigma^2 = (1 - \eta)/\eta$ [54]. If $\mathcal{A}(\eta^{-1})$ is applied *before* $\mathcal{L}(\eta)$, however, the variance is improved to $\sigma^2 = 1 - \eta$, as this avoids amplifying noise that occurs during transmission [57]. In our analyses of the one-way protocols, we will therefore consider the latter strategy. Furthermore, we will assume a total transmittance of $\eta_{\text{tot}} = \eta_c \exp(-L_0/L_{\text{att}})$, where η_c denotes the efficiency for coupling into the fiber ($\eta_c = 0.99$ unless stated otherwise) and $L_{\text{att}} = 22$ km is the attenuation length.

For the two-way teleportation-based protocol in Sec. 2.1.1, it is possible and beneficial to replace $\mathcal{A}(\sqrt{\eta}^{-1})$ with a classical amplification of the measured signal. Effectively, this turns the loss into a Gaussian error channel with variance $\sigma^2 = 1/\sqrt{\eta_{\text{tot}}} - 1$ [56], where $\eta_{\text{tot}} = \eta_c^2 \exp(-L_0/L_{\text{att}})$ takes into account that, in a two-way protocol, two signals are coupled into the fiber.

2.3.2 Approximate GKP state generation

The second, important noise contribution arises during the preparation of GKP states. In position basis, the state vector of an ideal square GKP qudit takes the form

$$|j\rangle = \sum_{k \in \mathbb{Z}} \left| \hat{q} = \sqrt{\frac{2\pi}{D}} (j + Dk) \right\rangle, \quad (1)$$

where $j \in \{0, \dots, D-1\}$ labels a computational basis state. These ideal states are unphysical as they are neither normalizable nor superpositions of finite-width peaks. To describe normalizable, physical instances of GKP states and eventually also predict real-world experimental performances, we instead consider approximate GKP states for which multiple realizations have been proposed that are essentially¹ equivalent [1, 69, 70]. Normalizability can be restored using an overall slowly decaying Gaussian envelope and the delta peaks can be approximated with (a still infinite number of) highly squeezed Gaussian peaks. This results in approximate GKP states of the form

$$|\tilde{j}\rangle \propto \sum_{k \in \mathbb{Z}} \exp\left(-\frac{\pi\kappa^2}{D}(j + Dk)^2\right) \int_{-\infty}^{\infty} dq \exp\left(-\frac{(q - \sqrt{\frac{2\pi}{D}}(j + Dk))^2}{2\Delta^2}\right) |\hat{q} = q\rangle, \quad (2)$$

where Δ and κ are squeezing parameters corresponding to the peaks' width in position and momentum representation, respectively. Alternatively, $|\tilde{j}\rangle$ can be interpreted as an ideal GKP state $|j\rangle$ to which coherent Gaussian displacements have been applied, i.e.,

$$|\tilde{j}\rangle \propto \int_{\mathbb{R}^2} du dv \exp\left(-\frac{1}{2}\left(\frac{u^2}{\gamma^2} + \frac{v^2}{\delta^2}\right) + i\left(\frac{-u\hat{p} + v\hat{q}}{\sqrt{2}}\right)\right) |j\rangle, \quad (3)$$

where the squeezing parameters γ and δ are in one-to-one correspondence to Δ and κ , see Thm. 1 in Ref. [70]. In this work, we only consider the symmetric case of $\gamma = \delta$. As a further simplification, we assume incoherent Gaussian displacements with variance σ_{sq}^2 , which can be understood as a twirling-approximation [22, App. A]. Numerical simulations confirm that such an approximation does not overestimate the approximate GKP state's fidelity [71]. Following Refs. [22, 69, 72], we define the *squeezing parameter* (given in dB),

$$s_{\text{GKP}} = -10 \log_{10} \left(\frac{\sigma_{\text{sq}}^2}{\sigma_{\text{vac}}^2} \right), \quad (4)$$

where $\sigma_{\text{vac}}^2 = 1/2$ denotes the quadrature variance of the vacuum state.

By means of a higher-level QECC, it is possible to concatenate multiple approximate GKP qudits, each of which is modeled by an ideal GKP state followed by Gaussian squeezing errors, into a single logical qudit. The corresponding unitary encoding circuit may redistribute the error probabilities between the modes, which in principle leads to correlated errors [52]. The resulting error probabilities have a complicated dependence on the selected encoding circuit, thus, they cannot be easily captured in full generality in our analytical model. Therefore, we leave such details for future work. For the purpose of the present investigation, we are satisfied with a noise model, where unphysical, ideal GKP states are first encoded using a higher-level QECC and, afterward, physicality is restored by applying Gaussian squeezing channels i.i.d. to each qudit, as motivated above.

2.3.3 Converting Gaussian noise into Pauli errors

The purpose of the GKP error-correction step shown in Fig. 1 is to discretize the continuous displacement errors that build up on the GKP qudits. In general, a single-qudit Pauli error channel is completely described by its joint error probability distribution of X - and

¹The state given in Eq. (2) is not symmetric under exchange of position and momentum. However, this state can be squeezed by a factor of $\sqrt{1 + \kappa^2 \Delta^2}$ to obtain the parameterization given in Eq. (3).

Z -errors [52]. We denote such a distribution by

$$\mathcal{P}(X, Z) = \begin{pmatrix} P(X^0, Z^0) & \dots & P(X^0, Z^{D-1}) \\ \vdots & \ddots & \vdots \\ P(X^{D-1}, Z^0) & \dots & P(X^{D-1}, Z^{D-1}) \end{pmatrix}. \quad (5)$$

Let us calculate, for a square-lattice GKP qudit, the Pauli error channel that results from a Gaussian noise channel with zero mean and a covariance matrix $\Sigma_{\text{sq}} = \sigma^2 \mathbb{I}$ (with respect to q and p). We find that X - and Z -errors are independent because the same is true for the two Gaussian random variables describing q - and p -shifts. In other words, the matrix $\mathcal{P}_{\text{sq}}(X, Z) = \mathcal{P}_{\text{sq}}(X) \otimes \mathcal{P}_{\text{sq}}(Z)$ factors into the outer product of the error probability vectors that store the marginal distributions of X - and Z -errors. By symmetry of the square lattice, we have $\mathcal{P}_{\text{sq}}(X) = \mathcal{P}_{\text{sq}}(Z)$. The probability to suffer $k \in \{0, \dots, D-1\}$ shifts can be expressed as

$$\begin{aligned} P_{\text{sq}}(X^k, \sigma^2) &= \sum_{j \in \mathbb{Z}} \int_{\sqrt{\frac{2\pi}{D}}(jD+k-\frac{1}{2})}^{\sqrt{\frac{2\pi}{D}}(jD+k+\frac{1}{2})} \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{q^2}{2\sigma^2}\right) dq \\ &= \sum_{j \in \mathbb{Z}} \frac{1}{2} \left(\text{erf}\left(\sqrt{\frac{2\pi}{D}} \frac{jD+k+\frac{1}{2}}{\sigma}\right) - \text{erf}\left(\sqrt{\frac{2\pi}{D}} \frac{jD+k-\frac{1}{2}}{\sigma}\right) \right), \end{aligned} \quad (6)$$

where $\text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x \exp(-q^2) dq$ is the error function. For our purposes, it is sufficient to keep only the three terms with $|j| \leq 1$.

3 Secret-key rates of quantum repeaters

The central figure of merit that we employ to compare the performance of different repeater protocols is the secret-key rate (SKR) per channel use. More precisely, we use $\log_2(D) - H(\mathcal{P})$, which is a lower bound on the two-way capacity [37], where $H(\mathcal{P})$ denotes the Shannon entropy of a Pauli error probability distribution \mathcal{P} as in Eq. (5). Note that this bound can be achieved by a qudit generalization (using $D+1$ bases, assuming D to be prime) of the six-state protocol [73] in the asymptotic limit, where almost every round the same basis is used [74]. Moreover, if X - and Z -errors are independent, the same rate is obtainable with a generalization of the BB84 protocol [75] (2 bases, arbitrary D).²

3.1 Repeater performance with GKP error correction only

For near-term applications, it is certainly more convenient to operate a quantum repeater with bare GKP qudits and not with multiple GKP qudits in a QECC. To guide such initial experiments, we begin our discussion with this important special case. For the two protocols considered with bare GKP qudits, which are described in Secs. 2.1.1 and 2.1.2, lower-level error correction is performed via a teleportation step on the logical level of the GKP code, which leads to independent X - and Z -errors. As mentioned above, the SKR per channel use is thus given by $\log_2(D) - H(\mathcal{P})$ not only for the generalized six-state protocol (D prime) but also for the generalized BB84 protocol (D arbitrary). The precise value of $H(\mathcal{P})$ has a complicated dependence on the repeater spacing L_0 , on the total repeater length L , on the squeezing parameter s_{GKP} that characterizes approximate

²The secret-key fraction is given by $I(A, B) - I(A, E) = \log_2(D) - H(g_{01}) - I(A, E)$, where expressions of the mutual information $I(A, E)$ between Alice and Eve are provided in Eqs. (5) and (7) of Ref. [74].

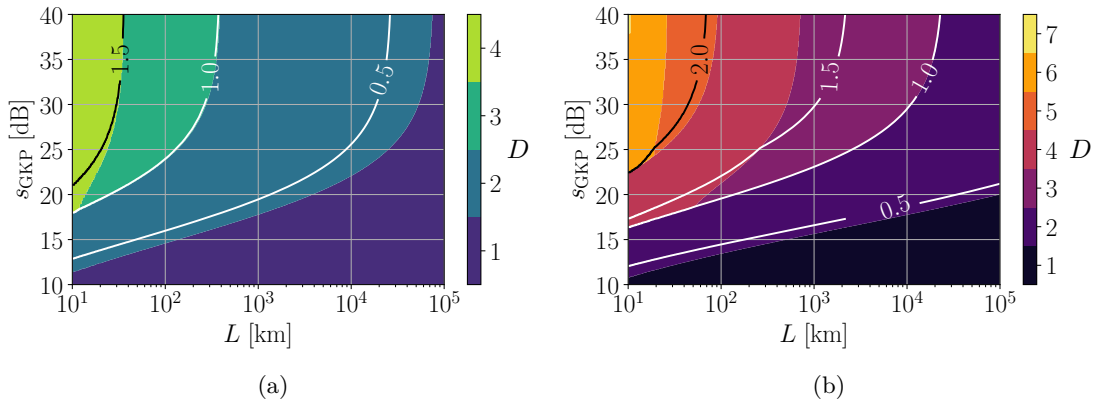


Figure 2: Optimal dimension D of bare GKP qudits utilized in a quantum repeater line with coupling efficiencies $\eta_c = 99\%$ and an intermediate repeater spacing of $L_0 = 500$ m, where the (a) one-way or (b) two-way teleportation protocol is used. For each choice of total repeater length L and squeezing parameter s_{GKP} , the qudit dimension is adjusted such that the SKR per channel use, $\log_2(D) - H(\mathcal{P})$, is optimized (inset lines). In the parameter regions of $D = 1$, it is not possible to generate secret keys.

GKP states, and on the qudit dimension D . However, we can numerically assess $H(\mathcal{P})$, see App. A. In Fig. 2, we show the optimal choice (color-coded) of qudit dimension D for different values of L and s_{GKP} , where $L_0 = 500$ m is fixed. Using inset lines, we also display the corresponding (maximal) value of the SKR per channel use. As expected, the key rate vanishes if the GKP approximation is too bad (small s_{GKP}) or too much loss accumulates (large L). Since increasing the squeezing poses a core experimental challenge, the smallest value of s_{GKP} at which a nonzero SKR can be achieved is of particular interest. Below $s_{\text{GKP}} = 10$ dB, neither protocol is suitable for generating secret keys. For both protocols and for every fixed value of L , we observe that GKP qubits ($D = 2$) represent the leading contender for near-term quantum repeaters based on the GKP code. To some degree, this result is surprising because in the ideal case, the SKR per channel use is given by $\log_2(D) - H(\mathcal{P})$, and increasing the qudit dimension would be beneficial. In the presence of noise, however, higher-dimensional GKP qudits have the severe disadvantage of decreased error correction capabilities: a D -dimensional GKP qudit can only correct displacement errors that are smaller than $\sqrt{\pi/2D}$ in magnitude. Only in the regime of very small errors, i.e., where the qubit GKP protocol has almost reached its maximum performance of $\log_2(D) - H(\mathcal{P}) = \log_2(2) - 0 = 1.0$, it is beneficial to employ qutrits ($D = 3$) instead of qubits. To see such benefits at all, we need at least $s_{\text{GKP}} \gtrsim 18$ dB. For repeater lines of modest lengths of a few ten kilometers, however, larger squeezing levels of 20 dB-25 dB are required to compensate for additional loss. At some value of L , loss errors become so severe that only an unrealistically disproportional improvement of s_{GKP} could compensate them. For the one-way protocol in Fig. 2 (a), qutrits cease to be the optimal option for repeaters longer than a few hundred kilometers, whereas the two-way protocol in Fig. 2 (b) can still benefit from qutrits even for repeaters exceeding $L = 10,000$ km. For the latter, however, a squeezing level above 30 dB is required, which will only be available in the long term (if at all). The reason for the better performance of the two-way protocol is the lower required amplification factor $\sqrt{\eta}^{-1}$ in the usage of the classical post-amplification, as discussed in Sec. 2.3.1.

Finally note that, in our error analysis, we distinguish the cases of even and odd qudit dimensions. Only if D is even, we can leverage a beneficial linear-optics protocol for the generation of GKP Bell pairs, see App. A. For very short repeater chains, we indeed

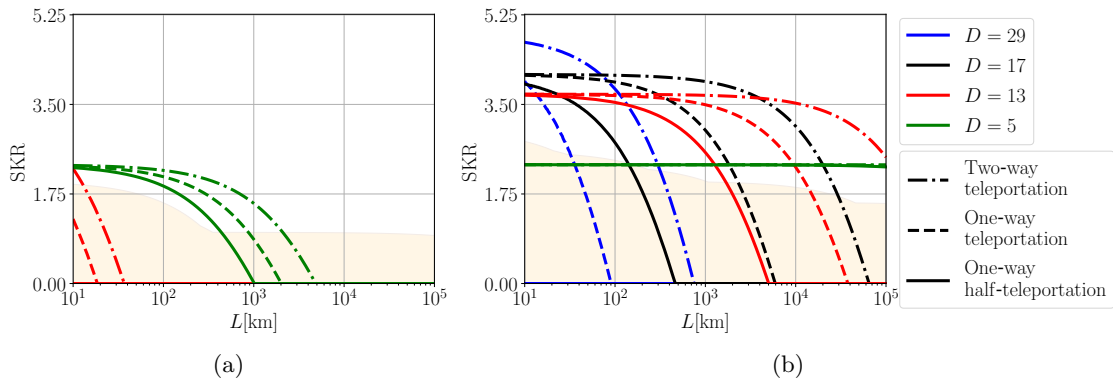


Figure 3: Lower bound on the SKR per logical channel use, $\log_2(D) - H(\mathcal{P})$, as a function of the total length L for a quantum repeater line with coupling efficiencies $\eta_c = 99\%$, an intermediate repeater spacing of $L_0 = 100$ m, and squeezing levels of (a) $s_{\text{GKP}} = 20$ dB or (b) $s_{\text{GKP}} = 30$ dB. The highlighted area shows the achievable SKR per physical channel use of a bare GKP repeater as in Fig. 2 (b).

observe that GKP qudits with D even outperform those with D odd. For larger values of L , however, loss errors begin to dominate and parameter regions emerge where the optimal SKR is obtained by odd-dimensional GKP qudits.

3.2 Repeater performance with both GKP and higher-level error correction

In comparison to the experimental challenge of creating high-quality GKP qudits in the first place, concatenating multiple of them into a single logical qudit by means of a higher-level QECC is relatively straightforward. In the following, we study the performance of third-generation quantum repeaters that make use of $[[D, 1, \frac{D+1}{2}]]_D$ quantum polynomial codes ($D \geq 3$ prime), as reviewed in a related context in App. A of Ref. [52]. The Pauli weight of the stabilizer generators is immense for quantum polynomial codes, which renders them unsuitable for applications in quantum computing. For quantum repeaters, on the other hand, this is not an issue, as non-destructive measurements of stabilizer operators are not required. Instead, destructively measuring all qudits individually is sufficient here. This facilitates syndrome extraction and decoding in a purely classical manner. Since the distance of a quantum polynomial code is given by $d = \frac{D+1}{2}$, any collection of errors that affect no more than $\lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{D-1}{4} \rfloor$ qudits can be corrected. For error patterns that affect more qudits than this, we assume (as a worst-case approximation) that a uniformly random logical error occurs. This maximizes the Shannon entropy $H(\mathcal{P})$ and lower bounds the SKR, $\log_2(D) - H(\mathcal{P})$, that would be achieved if a more sophisticated decoder for correcting specific high-weight errors was used. Thus, it makes sense for us to limit the discussion to prime qudit dimensions where $D - 1$ is a multiple of four. We defer our derivation of $H(\mathcal{P})$ for this suboptimal decoder to App. B.

In Fig. 3, we plot the (lower bound on the) SKR per logical channel use as a function of L , where $L_0 = 100$ m is fixed. For each of the three repeater protocols introduced in Sec. 2.1, we show the SKR for $D = 5$ (green), $D = 13$ (red), $D = 17$ (black), and $D = 29$ (blue). For any fixed value of D , we again (as in Fig. 2) observe that the two-way teleportation protocol (dash-dotted curve) from Sec. 2.1.1 performs best. It is followed by the one-way teleportation protocol (dashed curve) from Sec. 2.1.2. The least-efficient protocol is the one-way half-teleportation protocol (solid curve) from Sec. 2.1.3. We attribute the poor performance of the latter protocol to the fact that it employs only half as many (compared to the other protocols) logical measurements, which facilitate the correction of errors.

Recall from Sec. 3.1 that for bare GKP repeaters, the decreased error-correcting capabilities render higher-dimensional qudits unfeasible for near-term applications. Since the code distance $d = \frac{D+1}{2}$ grows with D , one could expect that concatenating bare GKP qudits with quantum polynomial codes would turn the tide. We see that this is not the case: for an optimistic but conceivable value of $s_{\text{GKP}} = 20$ dB, we see in Fig. 3 (a) that only the smallest code with $D = 5$ achieves a nonzero SKR for repeater lengths $L > 70$ km. To assess the performance of larger codes, we need to assume exorbitant squeezing levels, e.g., $s_{\text{GKP}} = 30$ dB as in Fig. 3 (b). In this scenario, the $[[5, 1, 3]]_5$ -code operates near its maximum performance of $\log_2(5) \approx 2.3$ for all considered values of L . Depending on the distance L , the largest value of $\log_2(D) - H(\mathcal{P})$ is obtained by a different code: until $L \approx 100$ km, the $[[29, 1, 15]]_{29}$ -code achieves a value beyond the optimal performance of $\log_2(17) \approx 4.1$ of the $[[17, 1, 9]]_{17}$ -code. The latter starts to lose performance after a few thousand kilometers, where it falls behind the $[[13, 1, 7]]_{13}$ -code. For comparison, we also show in Fig. 3 the performance of the two-way repeater protocol with bare GKP qudits (shaded region), where we select the value of D that optimizes the SKR, as in Fig. 2 (b). For $s_{\text{GKP}} = 20$ dB in Fig. 3 (a), bare GKP ququarts ($D = 4$) are optimal until $L \approx 200$ km. For longer repeaters, too much loss accumulates, and lower-dimensional GKP codes with higher error-correcting capabilities become beneficial: in a small range of L , bare qutrits are the optimal choice, but already for $L \gtrsim 300$ km, qubits perform best. As before, this advantage of even dimensions over odd ones is due to improved Bell state availability [20]. For $s_{\text{GKP}} = 30$ dB in Fig. 3 (b), losses are less of an issue and eight-dimensional GKP qudits are optimal until $L \approx 20$ km. For $30 \text{ km} \lesssim L \lesssim 200 \text{ km}$, $D = 6$ is optimal. For $1000 \text{ km} \lesssim L \lesssim 50,000 \text{ km}$, a bare GKP repeater should operate with $D = 4$.

It is important to stress that, from a practical perspective and for the considered parameters, it is not useful to employ higher-level QECCs if the application is quantum key distribution (QKD). For example, if $s_{\text{GKP}} = 30$ dB and $L = 1000$ km, the two-way teleportation protocol with a logical $[[17, 1, 9]]_{17}$ -code achieves the largest rate of about four secret bits per logical channel use. To accomplish this, however, seventeen GKP qudits (entangled in a QECC), i.e., seventeen GKP-encoded and entangled optical modes, need to be transmitted. With an even lower experimental effort, one could simply transmit in parallel seventeen bare GKP ququarts, i.e., seventeen GKP-encoded but unentangled optical modes, each of which establishes almost two secret bits. In other words, here the best bare protocol is more efficient than the best higher-level encoded one by a factor of about 8.5.

3.2.1 Optimal choice of the repeater spacing

In our discussion of Fig. 3, we have pointed out that no practical benefit is to be expected when switching from bare GKP qudits to a higher-level QECC if the repeater spacing is fixed to $L_0 = 100$ m. This raises the question of how the choice of L_0 influences this conclusion. Since implementation cost scales with the total number $N = L/L_0$ of repeater stations, here we focus on SKR/N as a figure of merit. In a commercial setting, SKR/N is roughly proportional to the return on investment. In Fig. 4, we plot SKR/N as a function of L_0 for a quantum repeater line of fixed length $L = 2000$ km. The colors and line styles have the same meaning as in Fig. 3. This time, we assume a more optimistic value of $\eta_c = 99.9\%$, which benefits higher-level QECCs. Despite this optimistic assumption, we still find that (for QKD) bare GKP qudits outperform those encoded into quantum polynomial codes. For example, for $s_{\text{GKP}} = 20$ dB in Fig. 4 (a), the $[[5, 1, 3]]_5$ -code performs best among the quantum polynomial codes and reaches the optimal value of SKR/N at a repeater spacing of $L_0 \approx 0.55$ km. For this optimal repeater configuration, the $[[5, 1, 3]]_5$ -code can generate

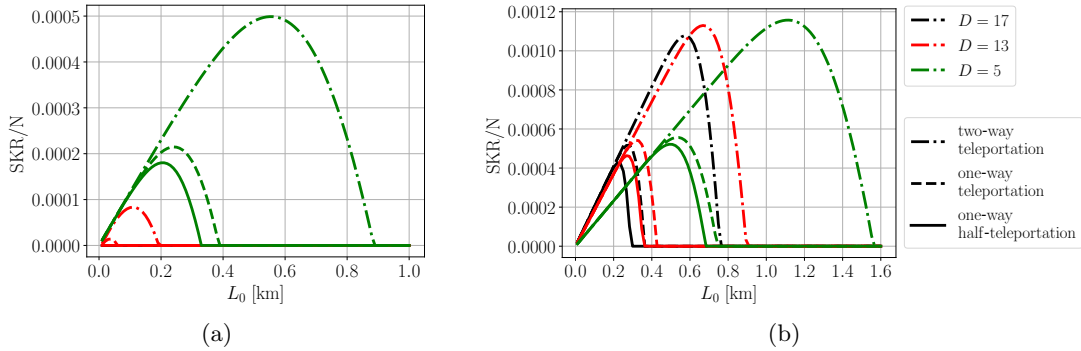


Figure 4: Lower bound on the SKR per logical channel use, $\log_2(D) - H(\mathcal{P})$, normalized by the number N of repeater segments ($N - 1$ repeater stations) as a function of the repeater spacing L_0 for a repeater line of total length $L = NL_0 = 2000$ km, coupling efficiencies $\eta_c = 99.9\%$, and squeezing levels of (a) $s_{\text{GKP}} = 20$ dB or (b) $s_{\text{GKP}} = 30$ dB.

approximately 1.8 secret bits by transmitting five GKP ququints ($D = 5$). In the same setting, one can generate almost 5.0 secret bits by transmitting five bare GKP qubits (not shown). The same behavior is observed for $s_{\text{GKP}} = 30$ dB in Fig. 4 (b), where the $[[5, 1, 3]]_5$ -code now achieves approximately 2.0 secret bits per logical channel use at the optimal operating point of $L_0 \approx 1.1$ km. In the same setting, transmitting five bare GKP qutrits would generate more than 5.6 secret bits.

From Fig. 4, we can also infer the maximal repeater spacing at which the secret-key rate drops to zero. For the considered parameters, the best higher-level encoded protocol, i.e., the two-way protocol from Sec. 2.1.1 with the $[[5, 1, 3]]_5$ -code and $s_{\text{GKP}} = 30$ dB, is operational for all values of $L_0 < 1.5$ km, however, $L_0 \approx 1.1$ km is most effective. For the one-way protocols from Secs. 2.1.2 and 2.1.3, the $[[5, 1, 3]]_5$ -code already fails for $L_0 \approx 0.7$ km. As expected, we find that better repeaters (larger s_{GKP} , smaller D) allow for a larger repeater spacing.

3.2.2 Identifying and overcoming noise bottlenecks

Before one takes a great effort of building a quantum repeater based on GKP qudits, it is important to ensure that the experimental building blocks work sufficiently well. There are multiple components for which improvements might be beneficial or even necessary. Thus, it is important to identify and remove the noise bottleneck, which would otherwise diminish the performance. We distinguish three error mechanisms: input noise, fiber channel losses, and imperfect homodyne measurements. Since measurements work comparatively well and we have already discussed the impact of fiber loss, here we focus on input noise that arises from approximate GKP state preparation and coupling losses. As explained in Sec. 2.3, both processes can be modeled by Gaussian noise. Errors propagate through the circuit and eventually accumulate on individual measurement results in the repeater stations, which for the two-way post-amplification protocol from Sec. 2.1.1 can be described by a Gaussian channel with variance

$$\sigma_{\text{in}}^2 = 3\sigma_{\text{sq}}^2 + \frac{1 - \eta_c}{\eta_c} \exp\left(\frac{L_0}{2L_{\text{att}}}\right). \quad (7)$$

Indeed, there are three sources from which GKP state preparation errors can propagate to the measurements, which leads to the first term in Eq. (7). The second term in Eq. (7) accounts for coupling losses: since the variance (incorporating both coupling and fiber channel

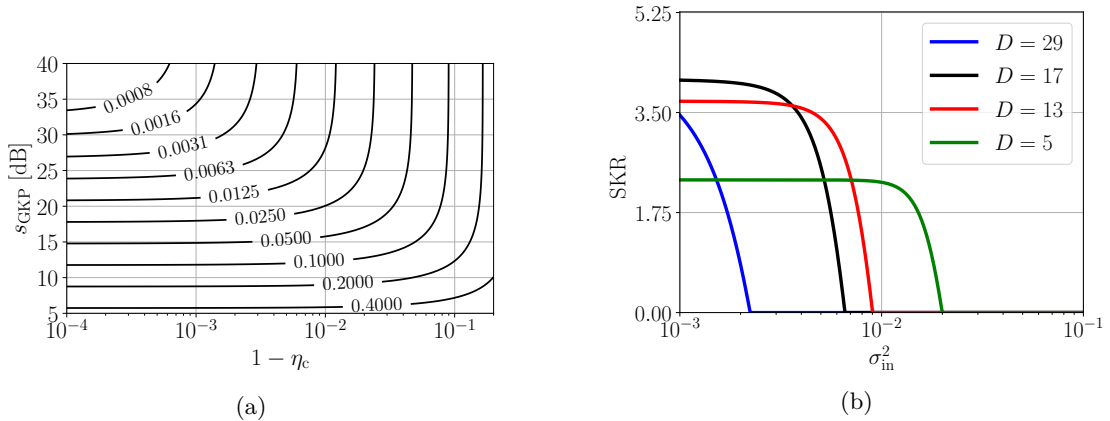


Figure 5: (a) Variance σ_{in}^2 of Gaussian noise effectively affecting a physical GKP qudit after it has been coupled into fiber as a function of the squeezing level s_{GKP} and coupling efficiency η_c . (b) Lower bound on the SKR per logical channel use, $\log_2(D) - H(\mathcal{P})$, as a function of σ_{in}^2 for a quantum repeater line with a total transmission distance of $L = 5000$ km and a repeater spacing of $L_0 = 500$ m, where the two-way protocol in combination with a $[[D, 1, \frac{D+1}{2}]]_D$ quantum polynomial code is utilized.

losses) of a length- L_0 link in the two-way protocol is given by $(\eta_c \exp(-L_0/2L_{\text{att}}))^{-1} - 1$, the noise difference between a link with coupling errors and without is given by

$$((\eta_c \exp(-\frac{L_0}{2L_{\text{att}}}))^{-1} - 1) - ((\exp(-\frac{L_0}{2L_{\text{att}}}))^{-1} - 1) = \frac{1 - \eta_c}{\eta_c} \exp\left(\frac{L_0}{2L_{\text{att}}}\right). \quad (8)$$

In Fig. 5 (a), we plot σ_{in}^2 as a function of both s_{GKP} and η_c . Recall that σ_{sq}^2 and s_{GKP} can be converted into each other via Eq. (4). Here, we assume a repeater spacing of $L_0 = 500$ m, however, the situation remains almost unchanged if L_0 takes any other value between 1 m and 1 km. The contour lines in Fig. 5 can be used to infer whether one should work on improving s_{GKP} or η_c : since moving along a contour line does not improve performance, a series of improvements should instead correspond to a path orthogonal to the contour lines. For example, for $s_{\text{GKP}} = 6$ dB and $\eta_c = 0.99$, we have $\sigma_{\text{in}}^2 \approx 0.4$, which can be reduced to $\sigma_{\text{in}}^2 \approx 0.2$ if the GKP approximation is improved to $s_{\text{GKP}} = 9$ dB; increasing η_c , on the other hand, would not help at all. Conversely, if coupling losses dominate, e.g., $s_{\text{GKP}} = 30$ dB and $\eta_c = 0.92$, the variance $\sigma_{\text{in}}^2 \approx 0.1$ can be reduced by a factor of two if coupling efficiencies are improved to $\eta_c = 0.97$; increasing s_{GKP} , however, would show no significant effect here.

In Fig. 5 (b), we depict the influence of σ_{in}^2 on the SKR obtained with the two-way protocol from Sec. 2.1.1 for an error-corrected quantum repeater line with $L = 5000$ km, $L_0 = 500$ m, and a $[[D, 1, \frac{D+1}{2}]]_D$ -code. Here, each physical GKP qudit in every repeater station is affected by a Gaussian channel with variance σ_{in}^2 . Note that also the effect of imperfect homodyne measurements can be inferred from Fig. 5 (b) if a corresponding variance term σ_{meas}^2 is added to σ_{in}^2 . As before, we find that a larger value of D both allows for a larger SKR per logical channel use in the low-noise regime and for a smaller noise level to be tolerated before the SKR drops to zero. We also observe that the parameter range of σ_{in}^2 where the SKR drops from its optimal value to zero is alarmingly small. This effect is most pronounced for the $[[5, 1, 3]]_5$ -code, which has almost optimal performance until $\sigma_{\text{in}}^2 \approx 0.01$ but already for $\sigma_{\text{in}}^2 \approx 0.02$ its SKR is equal to zero. This showcases that moderate improvements can have a huge impact if they address a noise bottleneck.

3.2.3 Leveraging lower-level syndrome information to improve higher-level error correction

So far, we have independently treated the error correction procedures of lower-level GKP qudits and the higher-level QECC. More precisely, we assumed that, in the first step, displacement errors on the physical GKP qudits are removed. This may or may not result in a logical GKP qudit error. Then, in a second step, the higher-level $[[n, 1, d]]_D$ -code deals with potential errors on the GKP qudits: the correction succeeds if the number of errors with unknown locations is not larger than $\frac{d-1}{2}$. In this final subsection, we investigate the more general case, where the location of some of the errors are known. The modified error correction routine succeeds whenever $t_k + 2t_u < d$, where t_k and t_u denote the number of errors with known and unknown locations, respectively. To obtain some information about error location, one can exploit the continuous, “analog” results of the homodyne measurements in the repeater stations [21, 23]. If a displacement error of the form $\exp(i\epsilon\hat{p})$ occurs, the homodyne measurement of \hat{q} reveals the value of ϵ modulo $\sqrt{2\pi/D}$, which we call analog GKP syndrome. In particular, every displacement error with $|\epsilon| < \sqrt{\pi/2D}$ can be corrected. The probability of successful error correction is large if ϵ is small. When an error of magnitude $\epsilon \approx \sqrt{\pi/2D}$ occurs, however, the situation is less clear. Borrowing ideas from Ref. [76], we introduce a discarding parameter $\gamma \in [0, 1]$, and treat any instances of ϵ which are closer than $\sqrt{\pi/2D}(1 - \gamma)$ from the boundary of two bins as an erasure error with a known location. In the case $\gamma = 1$, we do not discard any qudits, which corresponds to the strategy considered so far. The other extreme, $\gamma = 0$, corresponds to the absurd approach where all qudits are always discarded.

The advantage of this modification is that, for every qudit that is not discarded, the probabilities for errors (with unknown locations) are improved from Eq. (6) to

$$P_{\text{sq}}^{(\gamma)}(X^k, \sigma^2) \propto \sum_{j \in \mathbb{Z}} \int_{\sqrt{\frac{2\pi}{D}(jD+k-\frac{\gamma}{2})}}^{\sqrt{\frac{2\pi}{D}(jD+k+\frac{\gamma}{2})}} \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{q^2}{2\sigma^2}\right) dq, \quad (9)$$

where the proportionality constant follows from $\sum_{k=0}^{D-1} P_{\text{sq}}^{(\gamma)}(X^k, \sigma^2) = 1$. This improvement comes at the expense that we have to introduce an erasure error with probability

$$p_{\text{discard}} = 1 - \sum_{k=0}^{D-1} \sum_{j \in \mathbb{Z}} \int_{\sqrt{\frac{2\pi}{D}(jD+k-\frac{\gamma}{2})}}^{\sqrt{\frac{2\pi}{D}(jD+k+\frac{\gamma}{2})}} \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{q^2}{2\sigma^2}\right) dq, \quad (10)$$

however, we can still exploit our knowledge about the location of this error.

Denote the probability that a single GKP qudit is free of errors by $p_0 = P_{\text{sq}}^{(\gamma)}(X^0, \sigma^2)$. Then, the condition $t_k + 2t_u < d$ and basic combinatorics leads to the probability of a failed error correction attempt

$$p_{\text{fail}}(\gamma) = 1 - \sum_{t_k=0}^{d-1} \binom{n}{t_k} p_{\text{discard}}^{t_k} (1 - p_{\text{discard}})^{n-t_k} \sum_{t_u=0}^{t_{u,\text{max}}} \binom{n-t_k}{t_u} p_0^{n-t_k-t_u} (1 - p_0)^{t_u}, \quad (11)$$

where $t_{u,\text{max}} = \lfloor (d - t_k - 1)/2 \rfloor$ is the maximal number of correctable errors with unknown locations, assuming that t_k erasures occurred, and n is the number of physical GKP qudits.

In Fig. 6, we show how the logical failure rate (red) depends on the discarding parameter γ for a $[[13, 1, 7]]$ -code. For each physical GKP qudit, we assume that all noise combined (stemming, e.g., from GKP approximation, coupling, or transmission) corresponds to a fairly small but finite variance $\sigma^2 = 0.01$ of the overall Gaussian noise channel. For $\gamma = 1$, i.e., without discarding (black), the failure rate has a remarkably low value of $p_{\text{fail}} \approx 5 \times 10^{-11}$, which is due to the low level of noise and the high error-correcting

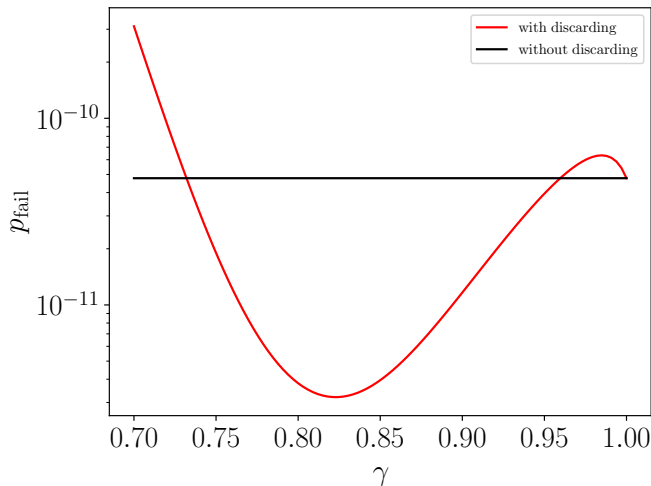


Figure 6: Failure probability p_{fail} for decoding the result of a logical measurement for a $[[13, 1, 7]]_{13}$ -code as a function of the discarding parameter γ . Each physical GKP qudit is subject to Gaussian noise with variance $\sigma^2 = 0.01$.

distance of $d = 7$. We observe a local minimum at $\gamma_{\text{opt}} \approx 0.82$, where the failure rate is improved by more than an order of magnitude to $p_{\text{fail}}(\gamma_{\text{opt}}) \approx 3 \times 10^{-12}$. If γ is decreased below γ_{opt} , we begin to introduce more erasures than the QECC can deal with, and the failure rate increases. On the other hand, if γ is increased above γ_{opt} , then the error rates $P_{\text{sq}}^{(\gamma)}(X^k, \sigma^2)$ start to deteriorate. This causes an increasing amount of errors with unknown locations and leads to the rise in p_{fail} . A curious effect in Fig. 6 is that the performance in the seldom-discarding regime ($\gamma > 0.96$) is worse than in the never-discarding case ($\gamma = 1$). We attribute this to the fact, that for $0.96 < \gamma < 1.0$, those cases dominate where only a single erasure error is introduced, i.e., $t_k = 1$ and the number of correctable errors with unknown locations is decreased to $t_{\text{u,max}} = 2$. At the same time, the error probabilities $P_{\text{sq}}^{(\gamma)}(X^k, \sigma^2)$ are only slightly improved because they continuously depend on γ . Thus, the performance is worse than for the naive approach with $\gamma = 1$, i.e., $t_k = 0$ and $t_{\text{u,max}} = 3$.

4 Conclusion and outlook

In this paper, we have analyzed the performance of third-generation quantum repeaters that operate with higher-dimensional GKP qudits. We have focused on the GKP square lattice and also considered concatenations with quantum polynomial codes.

The missing component that is currently holding back an experimental realization of such repeaters is efficient sources of high-quality GKP states. Once such sources are available, however, there will be no need for quantum memories or classical two-way communication. Therefore, the achievable repetition rates will only be limited by fast optical elements for the local processing of GKP qudits.

Our initial motivation for the present investigation was that, at a first glance, GKP qudits and quantum polynomial codes seem like a perfect match in the context of quantum repeaters: GKP states can be encoded into photons, which is crucial for repeaters; polynomial codes achieve the singleton bound at the expense of high-weight stabilizers, which is a problem for quantum computation but not for quantum repeaters; polynomial codes require higher-dimensional qudits, which the GKP encoding has to offer. However, our study revealed that the decreased lower-level error-correcting capabilities of higher-

dimensional GKP qudits severely limit their potential benefits. While this finding might disappoint to a certain extent, it is somewhat good news for experimentalists. Indeed, the most promising GKP repeater protocol identified in this work is also the one, which is the easiest to implement.

Our recommendation for a first experimental target is a repeater protocol (Sec. 2.1.1) that makes use of two-dimensional GKP qubits. Admittedly, these qubits will require challenging squeezing levels beyond 10 dB. However, the identified protocol has the advantage of readily available syndrome measurements based on balanced beam splitters and homodyne measurements alone. Furthermore, this protocol is compatible with rescaling the GKP lattice in classical software, whereas other protocols would require optical amplifiers to compensate for the loss.

We also found that, in the medium-to-long term, when squeezing levels above 20 dB will be available, the error-correcting capabilities of bare GKP qutrits will suffice to outperform GKP qubits for meaningful repeater lengths. Only in the very long term, if squeezing levels around 30 dB can possibly be reached, we expect some benefit from concatenating multiple GKP qudits using quantum polynomial codes, however, only for tasks like entanglement distribution where utmost fidelities are important. For the application of quantum key distribution, on the other hand, our analysis showed that it is typically more cost-effective to operate bare GKP qudit repeaters instead. With regards to potential experimental realizations, a useful feature of the case with bare GKP qudits is that the necessary GKP two-qudit Bell pair for teleportation-based syndrome detection and error correction can often be directly created by applying a balanced beam splitter upon two suitable, individual single-mode GKP/grid states [19, 20]. In case that the concatenation with the higher-level code is employed, for potential, future high-fidelity quantum network applications, the complete syndrome information of the QECC can still be obtained in one linear-optics step with no need for any online squeezing operations and also with no need for separating the physical GKP qudit from the higher-level code's syndrome measurements and adding extra GKP ancilla states for the higher-code detections. This only works, however, provided a suitable logical, higher-level Bell pair is available [20].

In this paper, we have focused on the cases of single GKP qudits and multiple GKP qudits that are concatenated by means of a higher-level qudit stabilizer code. This is, however, not the only possibility that can be envisioned. An interesting open research direction is to study the performance of multi-mode GKP codes that do *not* arise as a concatenation of physical GKP states and a higher-level stabilizer code [20, 77-80]. For such an analysis, theoretical insights about multi-mode Gaussian channels might become important [81]. Moreover, one could analyze how bosonic encodings other than GKP perform in a quantum repeater setting, e.g., cat codes [82, 83], spherical codes [84], etc. [85, 86].

Acknowledgments

FS and PvL acknowledge financial support from the BMBF in Germany via the projects QR.X, QuKuK, and PhotonQ and the BMBF/EU for support via the project QuantERA/ShoQC. DM acknowledges financial support from the BMBF in Germany via the projects RealistiQ, QR.X, and QSolid.

A Error analysis of bare GKP repeaters

We begin our error analysis by reviewing how Gaussian displacement errors of the form $\exp(\epsilon\hat{q}_i)$ and $\exp(\epsilon\hat{p}_i)$, where $\epsilon \in \mathbb{R}$ is the error magnitude, propagate across CSUM- and CPHASE-gates. The CSUM-gate, $\exp(-i\hat{q}_1\hat{p}_2)$ acts as $CX_{1,2} = \sum_{k=0}^{D-1} |k\rangle\langle k|_1 \otimes X_2^k$ on GKP qudits, while the CPHASE-gate, $\exp(i\hat{q}_1\hat{q}_2)$, implements $CZ_{1,2} = \sum_{k=0}^{D-1} |k\rangle\langle k|_1 \otimes Z_2^k$ [1]. Hereby, $X = \sum_{k=0}^{D-1} |k+1 \bmod D\rangle\langle k|$ and $Z = \sum_{k=0}^{D-1} (e^{2\pi i/D})^k |k\rangle\langle k|$ denote the unitary generalizations of the qubit Pauli X - and Z -gates to the case of D -dimensional qudits. It is well known that single-qudit Pauli errors are propagated across CX - and CZ -gates via

$$\begin{aligned} CZ_{1,2}X_1 &= X_1Z_2CZ_{1,2}, \\ CX_{1,2}X_1 &= X_1X_2CX_{1,2}, \\ \text{and } CX_{1,2}Z_2 &= Z_1^\dagger Z_2CX_{1,2}, \end{aligned} \tag{12}$$

see, e.g., Refs. [1, 52]. The error propagation rules of Eq. (12) have their bosonic analogs: applying the Baker-Campbell-Hausdorff formula yields

$$\begin{aligned} \exp(i\hat{q}_1\hat{q}_2)\exp(i\hat{p}_1) &= \exp(i(\hat{p}_1 - \hat{q}_2))\exp(i\hat{q}_1\hat{q}_2), \\ \exp(-i\hat{q}_1\hat{p}_2)\exp(i\hat{p}_1) &= \exp(i(\hat{p}_1 + \hat{p}_2))\exp(-i\hat{q}_1\hat{p}_2), \\ \text{and } \exp(-i\hat{q}_1\hat{p}_2)\exp(i\hat{q}_2) &= \exp(i(\hat{q}_2 - \hat{q}_1))\exp(-i\hat{q}_1\hat{p}_2). \end{aligned} \tag{13}$$

In the two repeater protocols from Sec. 2.1.1 and 2.1.2, every repeater station is responsible for performing a Bell measurement. This is achieved by a beam splitter, followed by two homodyne measurements. For both of these homodyne measurements, the results are post-processed (binned) into a measurement outcome of the GKP qudit. Errors on the GKP qudit lead to errors on the measurement outcomes. The latter can be described by a Pauli error channel $\mathcal{P}_{\text{sq}}(X, \sigma^2)$, as in Eq. (6), where the variance σ^2 comprises all Gaussian noise contributions that have propagated to the measurement device. As discussed in Sec. 2.3, we take the following error sources into account:

- Loss that arises when GKP qudits are coupled into an optical fiber. The resulting coupling efficiency is denoted by η_c .
- Loss that arises during transmission. If the traveling distance is L_0 , the associated transmittance is given by $\eta = \exp(-L_0/L_{\text{att}})$, where L_{att} is the attenuation distance.
- Unavoidable approximation errors of square GKP qudits. These are modeled by a Gaussian channel of variance σ_{sq}^2 .

Since beam splitters and homodyne measurements only require passive linear optical elements, we assume they work perfectly. Similarly, we ignore errors stemming from Gaussian elements, i.e., from CSUM- and CPHASE-gates.

For the two-way teleportation protocol from Sec. 2.1.1, transmission and coupling losses lead to a Gaussian error channel with variance $\frac{1}{\eta_c\sqrt{\eta}} - 1$, see Sec. 2.3.1. Furthermore, there are three GKP state preparations in the causal light cone of any given measurement. All in all, this amounts to a final variance of $\sigma_{2\text{-way}}^2 = 3\sigma_{\text{sq}}^2 + \frac{1}{\eta_c\sqrt{\eta}} - 1$.

For the one-way teleportation protocol from Sec. 2.1.2, the only difference is that the Gaussian error channel arising from losses now has a variance of $1 - \eta_c\eta$, see Sec. 2.3.1. Therefore, the final variance is given by $\sigma_{1\text{-way}}^2 = 3\sigma_{\text{sq}}^2 + 1 - \eta_c\eta$.

If D is even, it is possible to directly generate a two-qudit GKP Bell pair by applying a balanced beam splitter to two grid states [19, 20]. Unlike general Gaussian transformations,

this linear optical transformation does not amplify the noise. In consequence, the above variances are improved to $\sigma_{2\text{-way}}^2 = 2\sigma_{\text{sq}}^2 + \frac{1}{\eta_c\sqrt{\eta}} - 1$ and $\sigma_{1\text{-way}}^2 = 2\sigma_{\text{sq}}^2 + 1 - \eta_c\eta$.

On the physical level, every Bell measurement is comprised of two homodyne measurements. Errors on the measurement of one quadrature effectively propagate into X -errors on Bob's qudits, while those of the other quadrature lead to Z -errors. By symmetry, the final probability distributions for X - and Z -errors coincide, and it suffices to compute it in one case. Ignoring finite size effects³ and potential correlations between the error probabilities of different repeater stations, we estimate the final X -error distribution $\mathcal{P}_{\text{fin}}(X) = \mathcal{P}_{\text{sq}}^{*N}(X, \sigma^2)$ on Bob's qudit as the N -fold discrete convolution of $\mathcal{P}_{\text{sq}}(X, \sigma^2)$, where N denotes the number of repeater stations. We expect that this estimate captures the general behavior of the performance of GKP qudit repeaters. In principle, computing this convolution can be sped up by diagonalizing the corresponding error-probability matrix [52]. For our purposes, however, a direct implementation is sufficient. Then, we compute the outer product $\mathcal{P}_{\text{fin}}(X, Z) = \mathcal{P}_{\text{fin}}(X) \otimes \mathcal{P}_{\text{fin}}(Z)$. The secret-key rate of the repeater line, finally, is given by $\log_2(D) - H(\mathcal{P}_{\text{fin}}(X, Z)) = \log_2(D) - 2H(\mathcal{P}_{\text{fin}}(X))$.

B Error analysis of GKP repeaters with higher-level codes

In this appendix, we lift our error analysis from App. A to the logical level. First, we discuss in App. B.1 the two repeater protocols from Sec. 2.1.1 and 2.1.2. In App. B.2, we discuss the optimal placement of the lower-level GKP measurements for the third protocol from Sec. 2.1.3 and analyze its performance.

B.1 Logical performance of GKP qudits concatenated with quantum polynomial codes

In App. A, we showed that the error probability distribution for measurements in repeater stations is given by $\mathcal{P}_{\text{sq}}(X, \sigma^2)$, where $\sigma_{2\text{-way}}^2 = 3\sigma_{\text{sq}}^2 + \frac{1}{\eta_c\sqrt{\eta}} - 1$ and $\sigma_{1\text{-way}}^2 = 3\sigma_{\text{sq}}^2 + 1 - \eta_c\eta$ for the two-way and one-way teleportation protocol, respectively. When the protocol is lifted to its logical version, we still find the same error distribution for each of the measurements of the physical GKP qudits (of which there are D). This is because $\overline{CZ} = (CZ^\dagger)^{\otimes D}$ is semitransversal for the quantum polynomial code with parameters $[[D, 1, \frac{D+1}{2}]]_D$ [33].

Here, we consider a simple decoder that only corrects errors occurring on a number of qudits not more than half the distance $d = \frac{D+1}{2}$. Thus, the probability that a correctable error pattern occurs at a repeater station is given by

$$p_{\text{cor}} = \sum_{k=0}^{\frac{d-1}{2}} \binom{D}{k} p_0^{D-k} (1-p_0)^k, \quad (14)$$

where $p_0 = P_{\text{sq}}(X^0, \sigma^2)$, as in Eq. (6). If the decoding attempt fails, we replace the measured state with the maximally mixed state (as a worst-case approximation). In other words: with probability $1 - p_{\text{cor}}$, we insert a logical error, uniformly at random from the set $\{1, \dots, D-1\}$. Therefore, the error probability distribution on measurement outcomes in any repeater station is given by

$$P_{\text{rep}}(X^k) = \begin{cases} p_{\text{cor}} & \text{if } k = 0 \\ \frac{1}{D-1}(1 - p_{\text{cor}}) & \text{otherwise.} \end{cases} \quad (15)$$

³In principle, the measurements near the ends of the repeater line have smaller error probabilities. Ignoring this slightly underestimates performance, however, the difference is vanishingly small for a large number of repeater stations.

If the probability of errors is so large that $p_{\text{cor}} < \frac{1}{D-1}(1 - p_{\text{cor}})$, we replace Eq. (15) by the uniform distribution. Again, ignoring correlations between error distributions on different repeater stations, we estimate the final error distribution of the encoded repeater line as $\mathcal{P}_{\text{fin}}(X, Z) = \mathcal{P}_{\text{rep}}^{*N}(X) \otimes \mathcal{P}_{\text{rep}}^{*N}(Z)$.

B.2 Error analysis of the half-teleportation protocol for various placements of GKP syndrome measurements

In this appendix, we discuss how introducing additional ancilla-based measurements of lower-level GKP stabilizers can improve the performance of the one-way half-teleportation protocol with optical pre-amplification from Sec. 2.1.3. Such measurements are pictured in Fig. 1 (c) of the main text. As discussed in Sec. 2.3.1, every transmission from one repeater station to the next is associated with a Gaussian error channel with variance $\sigma_{\text{loss}}^2 = 1 - \eta_c \eta$, where $\eta = \exp(-L_0/L_{\text{att}})$. In every repeater station, all incoming GKP qudits are measured in the p -quadrature. Before this, however, each GKP qudit is coupled via a physical CPHASE[†]-gate to a qudit in the next logical block. Since the CPHASE[†]-gate spreads p -errors into q -errors, but q -errors are not propagated to the next mode, every error source only has a limited range. A p -error that arises during one transmission, does not directly affect p -measurements on the qudit it occurred to, however, it propagates into a q -error on the subsequent GKP qudit, which alters the p -measurement outcome of that qudit. Furthermore, a p -error during GKP state preparation backpropagates through the CPHASE[†]-gate and causes a q -error on the readout of the preceding GKP qudit.

In the plain version (without lower-level GKP stabilizer measurements), errors on physical readouts (in the repeater stations) follow an error distribution $\mathcal{P}_{\text{sq}}(Z, 2\sigma_{\text{loss}}^2 + 3\sigma_{\text{sq}}^2)$, where the variance takes noise from two transmissions and three GKP state preparations into account. By introducing a lower-level GKP stabilizer measurement in every repeater station, we can correct displacement errors after a single transmission. In this way, we effectively avoid combining the two transmission loss channels. Instead, all Gaussian errors in one quadrature are replaced by the discrete Pauli error channel from Eq. (6). Such discrete qudit Pauli errors will propagate to the measurements in the usual way [52]. Depending on where in the repeater station we place the ancilla-based GKP stabilizer measurement, the final error distribution will vary. We discuss four options:

- (i) No additional GKP stabilizer measurements are performed, see Fig. 7 for the error analysis.
- (ii) *After* every CZ-gate, the (physical) target qudit is subjected to a GKP stabilizer measurement of $S_X = \exp(-i\sqrt{2\pi D}\hat{p})$. This is achieved by preparing an ancillary GKP qudit in state $|0\rangle$, applying a CSUM-gate from the ancilla to the repeater qudit, and a p -measurement of the ancilla GKP qudit, see Fig. 8 for the error analysis.
- (iii) *Before* every CZ-gate, the control qudit is subjected to a GKP stabilizer measurement of $S_Z = \exp(i\sqrt{2\pi D}\hat{q})$. This is achieved by preparing a GKP ancilla in state $|+\rangle$, applying a CSUM-gate from the repeater qudit to the ancilla, followed by a q -measurement of the ancilla, see Fig. 9 for the error analysis.
- (iv) We *alternate* between options (ii) and (iii), see Fig. 10 for the error analysis.

In option (i), the error analysis from App. B.1 with $\sigma^2 = 2\sigma_{\text{loss}}^2 + 3\sigma_{\text{sq}}^2$ applies, see Fig. 7. Both in option (ii) and (iii), which we refer to as *symmetric* placements of the GKP stabilizer measurements, it turns out that every p -measurement is subject to two discrete

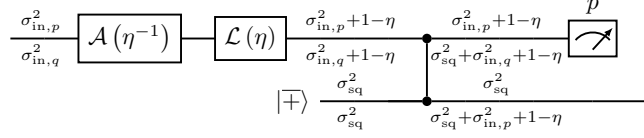


Figure 7: Propagation of Gaussian errors for the half-teleportation protocol *without* additional GKP stabilizer measurements. Because of periodic boundary conditions, we have $\sigma_{\text{in},p}^2 = \sigma_{\text{out},p}^2 = \sigma_{\text{sq}}^2$ and $\sigma_{\text{in},q}^2 = \sigma_{\text{out},q}^2 = 2\sigma_{\text{sq}}^2 + 1 - \eta$. Therefore, the variance of q -errors reaching the p -measurements is given by $\sigma_{\text{sq}}^2 + \sigma_{\text{in},q}^2 + 1 - \eta = 3\sigma_{\text{sq}}^2 + 2(1 - \eta)$.

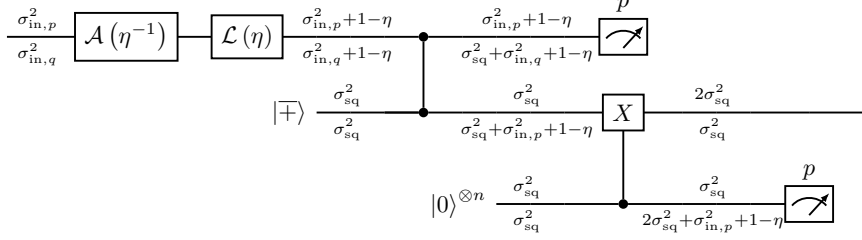


Figure 8: Propagation of Gaussian errors for the half-teleportation protocol with additional GKP stabilizer measurements *after* every CZ -gate. Because of periodic boundary conditions, we have $\sigma_{\text{in},p}^2 = \sigma_{\text{out},p}^2 = 2\sigma_{\text{sq}}^2$ and $\sigma_{\text{in},q}^2 = \sigma_{\text{out},q}^2 = \sigma_{\text{sq}}^2$. Therefore, the variance of q -errors reaching the p -measurements is given by $\sigma_{\text{sq}}^2 + \sigma_{\text{in},q}^2 + 1 - \eta = 2\sigma_{\text{sq}}^2 + 1 - \eta$. In addition to these continuous displacement errors, a discrete Pauli error channel $\mathcal{P}_{\text{sq}}(Z, \sigma_{\text{GKP}}^2)$ leads to lower-level logical errors on every X -measurement, where $\sigma_{\text{GKP}}^2 = 2\sigma_{\text{sq}}^2 + \sigma_{\text{in},p}^2 + 1 - \eta = 4\sigma_{\text{sq}}^2 + 1 - \eta$ is the variance of q -errors reaching the lower-level GKP stabilizer measurement.

Pauli error channels as in Eq. (6), one having variance $2\sigma_{\text{sq}}^2 + \sigma_{\text{loss}}^2$ and the other one $4\sigma_{\text{sq}}^2 + \sigma_{\text{loss}}^2$. Thus, the error analysis from App. B.1 applies after we insert

$$p_0^{\text{sym}} = \sum_{k=0}^{D-1} P_{\text{sq}}(X^k, 2\sigma_{\text{sq}}^2 + \sigma_{\text{loss}}^2) P_{\text{sq}}(X^{D-k}, 2\sigma_{\text{sq}}^2 + \sigma_{\text{loss}}^2) \quad (16)$$

into Eq. (14). Finally, in option (iv) both GKP stabilizer and logical measurements are subject to Gaussian errors with variance $3\sigma_{\text{sq}}^2 + \sigma_{\text{loss}}^2$. This time, we thus have to insert

$$p_0^{\text{alt}} = \sum_{k=0}^{D-1} P_{\text{sq}}(X^k, 3\sigma_{\text{sq}}^2 + \sigma_{\text{loss}}^2) P_{\text{sq}}(X^{D-k}, 3\sigma_{\text{sq}}^2 + \sigma_{\text{loss}}^2) \quad (17)$$

into Eq. (14).

In Fig. 11, we show how the placement of GKP stabilizer measurements influences the performance of the half-teleportation protocol, using the exact same setting as in Fig. 4 of the main text. Overall, the situation is very similar to that in Fig. 4: for $s_{\text{GKP}} = 20$ dB in Fig. 11 (a), only the $[[5, 1, 3]]_D$ -code (green) offers a nonzero SKR, whereas for $s_{\text{GKP}} = 20$ dB in Fig. 11 (b) also the $[[13, 1, 7]]_D$ -code (red) and the $[[17, 1, 9]]_D$ -code (black) have the potential to distribute secret keys. We see in Fig. 11 that an alternating placement of GKP stabilizer measurements (solid curves) leads to the highest values of SKR/ N . For both option (ii) and (iii), the symmetric placements (dotted curves) are governed by Eq. (16), and therefore lead to the same performance. We see that not performing any additional GKP stabilizer measurements (dash-dotted curve) leads to the lowest performance, which is easily explained by the large variance $2\sigma_{\text{loss}}^2 + 3\sigma_{\text{sq}}^2$. The other options break the term $2\sigma_{\text{loss}}^2$ and, therefore, perform better. For the symmetric placement, the bottleneck is

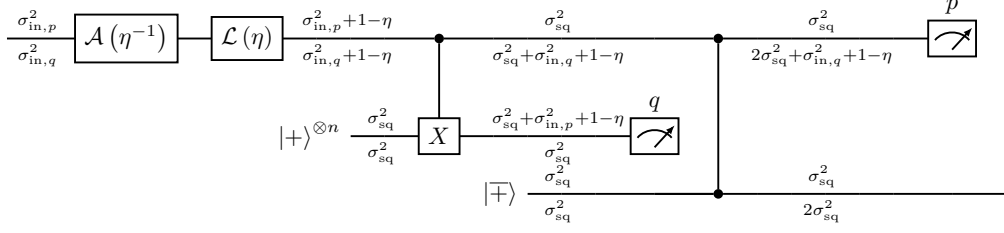


Figure 9: Propagation of Gaussian errors for the half-teleportation protocol with additional GKP stabilizer measurements *before* every CZ -gate. Because of periodic boundary conditions, we have $\sigma_{in,p}^2 = \sigma_{out,p}^2 = \sigma_{sq}^2$ and $\sigma_{in,q}^2 = \sigma_{out,q}^2 = 2\sigma_{sq}^2$. Therefore, the variance of q -errors reaching the p -measurements is given by $2\sigma_{sq}^2 + \sigma_{in,q}^2 + 1 - \eta = 4\sigma_{sq}^2 + 1 - \eta$. In addition to these continuous displacement errors, a discrete Pauli error channel $\mathcal{P}_{sq}(Z, \sigma_{GKP}^2)$ leads to lower-level logical errors on every X -measurement, where $\sigma_{GKP}^2 = \sigma_{sq}^2 + \sigma_{in,p}^2 + 1 - \eta = 2\sigma_{sq}^2 + 1 - \eta$ is the variance of p -errors reaching the lower-level GKP stabilizer measurement. Originally, the lower-level GKP stabilizer measurement results in a discrete Pauli error channel $\mathcal{P}_{sq}(X, \sigma_{GKP}^2)$, which is then propagated to a Pauli error channel $\mathcal{P}_{sq}(Z, \sigma_{GKP}^2)$ in the next segment due to the CZ -gate.

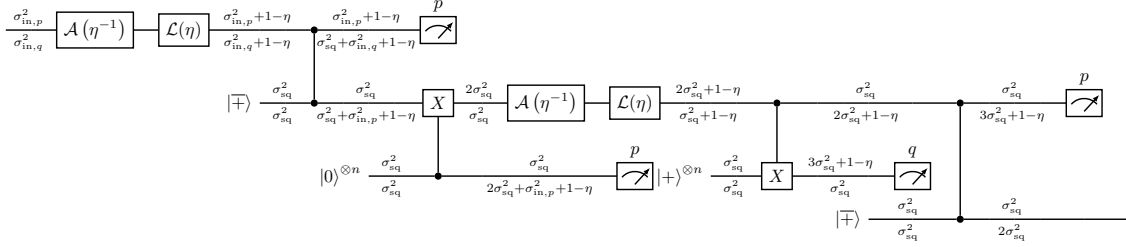


Figure 10: Propagation of Gaussian errors for the half-teleportation protocol with additional GKP stabilizer measurements at *alternating* placements. Because of periodic boundary conditions, we have $\sigma_{in,p}^2 = \sigma_{out,p}^2 = \sigma_{sq}^2$ and $\sigma_{in,q}^2 = \sigma_{out,q}^2 = 2\sigma_{sq}^2$. Therefore, it turns out that the variance of q -errors reaching all p -measurements is given by $\sigma_{sq}^2 + \sigma_{in,q}^2 + 1 - \eta = 3\sigma_{sq}^2 + 1 - \eta$. In addition to these continuous displacement errors, a discrete Pauli error channel $\mathcal{P}_{sq}(Z, \sigma_{GKP}^2)$ leads to lower-level logical errors on every X -measurement, where $\sigma_{GKP}^2 = 2\sigma_{sq}^2 + \sigma_{in,p}^2 + 1 - \eta = 3\sigma_{sq}^2 + 1 - \eta$ is the variance of errors reaching and altering lower-level GKP stabilizer measurements.

posed by the term $4\sigma_{sq}^2$ in Eq. (16), which is worse than $3\sigma_{sq}^2$ in Eq. (17) for the alternating placement. This explains why the latter performs best. For a large squeezing value of $s_{GKP} = 30$ dB, the difference between $3\sigma_{sq}^2$ and $4\sigma_{sq}^2$ is negligible, which causes a nearly perfect overlapping of the dotted and solid curves in Fig. 11 (b).

Since the alternating placement of GKP stabilizer measurements has the best performance, we have assumed this option for the one-way half-teleportation protocol throughout the main text of this paper.

C Author contributions

DM initiated the project as a whole and exploring the idea of concatenating GKP qudits with polynomial codes. FS designed the repeater protocols, derived the analytical model, performed the numerics, and created the figures. FS and DM designed the study, interpreted the results, and wrote the manuscript. PvL supported research and development and helped preparing the manuscript.

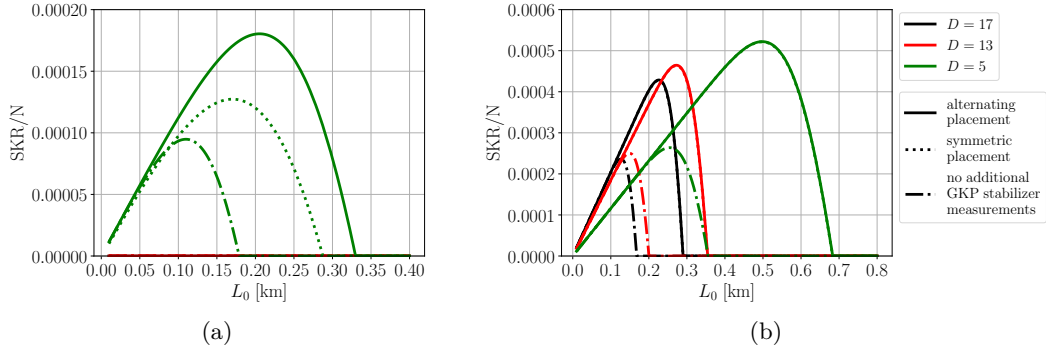


Figure 11: Lower bound on the SKR per logical channel use, $\log_2(D) - H(\mathcal{P})$, normalized by the number N of repeater stations for the one-way half-teleportation protocol and various placements of lower-level GKP stabilizer measurements. We plot SKR/N as a function of the repeater spacing L_0 for a repeater line of total length $L = NL_0 = 2000$ km, coupling efficiencies $\eta_c = 99.9\%$, and squeezing levels of (a) $s_{\text{GKP}} = 20$ dB or (b) $s_{\text{GKP}} = 30$ dB.

References

- [1] Daniel Gottesman, Alexei Kitaev, and John Preskill. “Encoding a qubit in an oscillator”. *Phys. Rev. A* **64**, 012310 (2001).
- [2] Martin Rymar, Stefano Bosco, Alessandro Ciani, and David P. DiVincenzo. “Hardware-Encoding Grid States in a Nonreciprocal Superconducting Circuit”. *Phys. Rev. X* **11**, 011032 (2021).
- [3] Arne L. Grimsmo and Shruti Puri. “Quantum Error Correction with the Gottesman-Kitaev-Preskill Code”. *PRX Quantum* **2**, 020101 (2021).
- [4] Philippe Campagne-Ibarcq, Alec Eickbusch, Steven Touzard, Evan Zaly-Geller, Nicholas E. Frattini, Volodymyr V. Sivak, Philip Reinhold, Shruti Puri, Shyam Shankar, Robert J. Schoelkopf, Luigi Frunzio, Mazyar Mirrahimi, and Michel H. Devoret. “Quantum error correction of a qubit encoded in grid states of an oscillator”. *Nature* **584**, 368 (2020).
- [5] Alec Eickbusch, Volodymyr Sivak, Andy Z. Ding, Salvatore S. Elder, Shantanu R. Jha, Jayameenakshi Venkatraman, Baptiste Royer, Steven M. Girvin, Robert J. Schoelkopf, and Michel H. Devoret. “Fast universal control of an oscillator with weak dispersive coupling to a qubit”. *Nat. Phys.* **18**, 1464 (2022).
- [6] Volodymyr V. Sivak, Alec Eickbusch, Baptiste Royer, Shraddha Singh, Ioannis Tsioutsios, Suhas Ganjam, Alessandro Miano, Benjamin L. Brock, Andy Z. Ding, Luigi Frunzio, Steven M. Girvin, Robert J. Schoelkopf, and Michel H. Devoret. “Real-time quantum error correction beyond break-even” (2022). [arXiv:2211.09116](https://arxiv.org/abs/2211.09116).
- [7] Christa Flühmann, Thanh Long Nguyen, Matteo Marinelli, Vlad Negnevitsky, Karan Mehta, and Jonathan P. Home. “Encoding a qubit in a trapped-ion mechanical oscillator”. *Nature* **566**, 513 (2019).
- [8] Brennan de Neeve, Thanh-Long Nguyen, Tanja Behrle, and Jonathan P. Home. “Error correction of a logical grid state qubit by dissipative pumping”. *Nat. Phys.* **18**, 296 (2022).

- [9] Daiqin Su, Casey R. Myers, and Krishna Kumar Sabapathy. “Conversion of Gaussian states to non-Gaussian states using photon-number-resolving detectors”. *Phys. Rev. A* **100**, 052301 (2019).
- [10] Ilan Tzitrin, J. Eli Bourassa, Nicolas C. Menicucci, and Krishna Kumar Sabapathy. “Progress towards practical qubit computation using approximate Gottesman-Kitaev-Preskill codes”. *Phys. Rev. A* **101**, 032315 (2020).
- [11] Kosuke Fukui, Shuntaro Takeda, Mamoru Endo, Warit Asavanant, Jun-ichi Yoshikawa, Peter van Loock, and Akira Furusawa. “Efficient Backcasting Search for Optical Quantum State Synthesis”. *Phys. Rev. Lett.* **128**, 240503 (2022).
- [12] Kan Takase, Kosuke Fukui, Akito Kawasaki, Warit Asavanant, Mamoru Endo, Jun-ichi Yoshikawa, Peter van Loock, and Akira Furusawa. “Gaussian breeding for encoding a qubit in propagating light” (2022). [arXiv:2212.05436](https://arxiv.org/abs/2212.05436).
- [13] Hilma M. Vasconcelos, Liliana Sanz, and Scott Glancy. “All-optical generation of states for ‘Encoding a qubit in an oscillator’”. *Opt. Lett.* **35**, 3261–3263 (2010).
- [14] Daniel J. Weigand and Barbara M. Terhal. “Generating grid states from Schrödinger-cat states without postselection”. *Phys. Rev. A* **97**, 022341 (2018).
- [15] Niklas Budinger, Akira Furusawa, and Peter van Loock. “All-optical quantum computing using cubic phase gates” (2022). [arXiv:2211.09060](https://arxiv.org/abs/2211.09060).
- [16] Jacob Hastrup, Kimin Park, Jonatan Bohr Brask, Radim Filip, and Ulrik Lund Andersen. “Measurement-free preparation of grid states”. *npj Quantum Inf.* **7**, 17 (2021).
- [17] Miller Eaton, Carlos González-Arciniegas, Rafael N. Alexander, Nicolas C. Menicucci, and Olivier Pfister. “Measurement-based generation and preservation of cat and grid states within a continuous-variable cluster state”. *Quantum* **6**, 769 (2022).
- [18] Nicolas C. Menicucci, Peter van Loock, Mile Gu, Christian Weedbrook, Timothy C. Ralph, and Michael A. Nielsen. “Universal quantum computation with continuous-variable cluster states”. *Phys. Rev. Lett.* **97**, 110501 (2006).
- [19] Blayne W. Walshe, Ben Q. Baragiola, Rafael N. Alexander, and Nicolas C. Menicucci. “Continuous-variable gate teleportation and bosonic-code error correction”. *Phys. Rev. A* **102**, 062411 (2020).
- [20] Frank Schmidt and Peter van Loock. “Quantum error correction with higher Gottesman-Kitaev-Preskill codes: Minimal measurements and linear optics”. *Phys. Rev. A* **105**, 042427 (2022).
- [21] Kosuke Fukui, Akihisa Tomita, and Atsushi Okamoto. “Analog Quantum Error Correction with Encoding a Qubit into an Oscillator”. *Phys. Rev. Lett.* **119**, 180507 (2017).
- [22] Kyungjoo Noh and Christopher Chamberland. “Fault-tolerant bosonic quantum error correction with the surface-Gottesman-Kitaev-Preskill code”. *Phys. Rev. A* **101**, 012316 (2020).
- [23] Christophe Vuillot, Hamed Asasi, Yang Wang, Leonid P. Pryadko, and Barbara M. Terhal. “Quantum error correction with the toric Gottesman-Kitaev-Preskill code”. *Phys. Rev. A* **99**, 032344 (2019).
- [24] Kosuke Fukui, Akihisa Tomita, Atsushi Okamoto, and Keisuke Fujii. “High-Threshold Fault-Tolerant Quantum Computation with Analog Quantum Error Correction”. *Phys. Rev. X* **8**, 021054 (2018).

- [25] Lisa Hägggeli, Margret Heinze, and Robert König. “Enhanced noise resilience of the surface–Gottesman–Kitaev–Preskill code via designed bias”. *Phys. Rev. A* **102**, 052408 (2020).
- [26] Nithin Raveendran, Narayanan Rengaswamy, Filip Rozpędek, Ankur Raina, Liang Jiang, and Bane Vasić. “Finite Rate QLDPC-GKP Coding Scheme that Surpasses the CSS Hamming Bound”. *Quantum* **6**, 767 (2022).
- [27] Eric M. Rains. “Nonbinary quantum codes”. *IEEE Trans. Inf. Theory* **45**, 1827–1832 (1999).
- [28] Emanuel Knill and Raymond Laflamme. “Theory of quantum error-correcting codes”. *Phys. Rev. A* **55**, 900 (1997).
- [29] Arthur R. Calderbank, Eric M. Rains, Peter W. Shor, and Neil J. A. Sloane. “Quantum error correction via codes over $GF(4)$ ”. *IEEE Trans. Inf. Theory* **44**, 1369 (1998).
- [30] Markus Grassl and Martin Rötteler. “Quantum MDS codes over small fields”. In *IEEE Int. Symp. Inf. Theory - Proc.* Pages 1104–1108. (2015).
- [31] Raymond Laflamme, Cesar Miquel, Juan P. Paz, and Wojciech H. Zurek. “Perfect Quantum Error Correcting Code”. *Phys. Rev. Lett.* **77**, 198 (1996).
- [32] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo. “How to Share a Quantum Secret”. *Phys. Rev. Lett.* **83**, 648 (1999).
- [33] Dorit Aharonov and Michael Ben-Or. “Fault-Tolerant Quantum Computation with Constant Error Rate”. *SIAM J. Comput.* **38**, 1207 (2008).
- [34] Avanti Ketkar, Andreas Klappenecker, Santosh Kumar, and Pradeep K. Sarvepalli. “Nonbinary Stabilizer Codes Over Finite Fields”. *IEEE Trans. Inf. Theory* **52**, 4892 (2006).
- [35] Andrew W. Cross. “Fault-tolerant quantum computer architectures using hierarchies of quantum error-correcting codes”. url: dspace.mit.edu/handle/1721.1/44407.
- [36] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. “Fundamental rate-loss tradeoff for optical quantum key distribution”. *Nat. Commun.* **5**, 5235 (2014).
- [37] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. “Fundamental limits of repeaterless quantum communications”. *Nat. Commun.* **8**, 15043 (2017).
- [38] Hans J. Briegel, Wolfgang Dür, J. Ignacio Cirac, and Peter Zoller. “Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication”. *Phys. Rev. Lett.* **81**, 5932 (1998).
- [39] Sreraman Muralidharan, Linshu Li, Jungsang Kim, Norbert Lütkenhaus, Mikhail D. Lukin, and Liang Jiang. “Optimal architectures for long distance quantum communication”. *Sci. Rep.* **6**, 20463 (2016).
- [40] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher. “Concentrating partial entanglement by local operations”. *Phys. Rev. A* **53**, 2046–2052 (1996).
- [41] Liang Jiang, J. M. Taylor, Kae Nemoto, W. J. Munro, Rodney Van Meter, and M. D. Lukin. “Quantum repeater with encoding”. *Phys. Rev. A* **79**, 032325 (2009).
- [42] Austin G. Fowler, David S. Wang, Charles D. Hill, Thaddeus D. Ladd, Rodney Van Meter, and Lloyd C. L. Hollenberg. “Surface Code Quantum Communication”. *Phys. Rev. Lett.* **104**, 180503 (2010).

- [43] Sreraman Muralidharan, Jungsang Kim, Norbert Lütkenhaus, Mikhail D. Lukin, and Liang Jiang. “Ultrafast and Fault-Tolerant Quantum Communication across Long Distances”. *Phys. Rev. Lett.* **112**, 250501 (2014).
- [44] Sylvia Bratzik, Hermann Kampermann, and Dagmar Bruß. “Secret key rates for an encoded quantum repeater”. *Phys. Rev. A* **89**, 032335 (2014).
- [45] Fabian Ewert, Marcel Bergmann, and Peter van Loock. “Ultrafast Long-Distance Quantum Communication with Static Linear Optics”. *Phys. Rev. Lett.* **117**, 210501 (2016).
- [46] Fabian Ewert and Peter van Loock. “Ultrafast fault-tolerant long-distance quantum communication with static linear optics”. *Phys. Rev. A* **95**, 012327 (2017).
- [47] Frank Schmidt and Peter van Loock. “Efficiencies of logical Bell measurements on Calderbank-Shor-Steane codes with static linear optics”. *Phys. Rev. A* **99**, 062308 (2019).
- [48] Koji Azuma, Kiyoshi Tamaki, and Hoi-Kwong Lo. “All-photonic quantum repeaters”. *Nat. Commun.* **6**, 6787 (2015).
- [49] Seung-Woo Lee, Timothy C. Ralph, and Hyunseok Jeong. “Fundamental building block for all-optical scalable quantum networks”. *Phys. Rev. A* **100**, 052303 (2019).
- [50] Sreraman Muralidharan, Chang-Ling Zou, Linshu Li, Jianming Wen, and Liang Jiang. “Overcoming erasure errors with multilevel systems”. *New J. Phys.* **19**, 013026 (2017).
- [51] Sreraman Muralidharan, Chang-Ling Zou, Linshu Li, and Liang Jiang. “One-way quantum repeaters with quantum Reed-Solomon codes”. *Phys. Rev. A* **97**, 052316 (2018).
- [52] Daniel Miller, Timo Holz, Hermann Kampermann, and Dagmar Bruß. “Propagation of generalized Pauli errors in qudit Clifford circuits”. *Phys. Rev. A* **98**, 052316 (2018).
- [53] Daniel Miller, Timo Holz, Hermann Kampermann, and Dagmar Bruß. “Parameter regimes for surpassing the PLOB bound with error-corrected qudit repeaters”. *Quantum* **3**, 216 (2019).
- [54] Daniel Gottesman and John Preskill. “Secure quantum key distribution using squeezed states”. *Phys. Rev. A* **63**, 022309 (2001).
- [55] Filip Rozpędek, Kyungjoo Noh, Qian Xu, Saikat Guha, and Liang Jiang. “Quantum repeaters based on concatenated bosonic and discrete-variable quantum codes”. *npj Quantum Inf.* **7**, 102 (2021).
- [56] Kosuke Fukui, Rafael N. Alexander, and Peter van Loock. “All-Optical Long-Distance Quantum Communication with Gottesman-Kitaev-Preskill qubits”. *Phys. Rev. Research* **3**, 033118 (2021).
- [57] Kyungjoo Noh, Victor V. Albert, and Liang Jiang. “Quantum Capacity Bounds of Gaussian Thermal Loss Channels and Achievable Rates With Gottesman-Kitaev-Preskill Codes”. *IEEE Trans. Inf. Theory* **65**, 2563 (2019).
- [58] Erik Hostens, Jeroen Dehaene, and Bart De Moor. “Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic”. *Phys. Rev. A* **71**, 042315 (2005).
- [59] Emanuel Knill. “Scalable quantum computing in the presence of large detected-error rates”. *Phys. Rev. A* **71**, 042322 (2005).

- [60] Mikka Stasiuk, Felix Hufnagel, Xiaoqin Gao, Frédéric Bouchard, Ebrahim Karimi, and Khabat Heshami. “High-dimensional Encoding in the Round-Robin Differential-Phase-Shift Protocol” (2023). [arXiv:2302.07888](#).
- [61] Tian Zhong, Hongchao Zhou, Robert D Horansky, Catherine Lee, Varun B Verma, Adriana E Lita, Alessandro Restelli, Joshua C Bienfang, Richard P Mirin, Thomas Gerrits, Sae Woo Nam, Francesco Marsili, Matthew D Shaw, Zheshen Zhang, Ligong Wang, Dirk Englund, Gregory W Wornell, Jeffrey H Shapiro, and Franco N C Wong. “Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding”. *New J. Phys.* **17**, 022002 (2015).
- [62] John Calsamiglia and Norbert Lütkenhaus. “Maximum efficiency of a linear-optical Bell-state analyzer”. *Appl. Phys. B* **72**, 67 (2001).
- [63] W. P. Grice. “Arbitrarily complete bell-state measurement using only linear optical elements”. *Phys. Rev. A* **84**, 042331 (2011).
- [64] Fabian Ewert and Peter van Loock. “3/4-efficient bell measurement with passive linear optics and unentangled ancillae”. *Phys. Rev. Lett.* **113**, 140403 (2014).
- [65] John Calsamiglia. “Generalized measurements by linear elements”. *Phys. Rev. A* **65**, 030301 (2002).
- [66] Miloslav Dušek. “Discrimination of the Bell states of qudits by means of linear optics”. *Opt. Commun.* **199**, 161 (2001).
- [67] Samuel L. Braunstein and Peter van Loock. “Quantum information with continuous variables”. *Rev. Mod. Phys.* **77**, 513–577 (2005).
- [68] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. “Gaussian quantum information”. *Rev. Mod. Phys.* **84**, 621–669 (2012).
- [69] Nicolas C. Menicucci. “Fault-Tolerant Measurement-Based Quantum Computing with Continuous-Variable Cluster States”. *Phys. Rev. Lett.* **112**, 120504 (2014).
- [70] Takaya Matsuura, Hayata Yamasaki, and Masato Koashi. “Equivalence of approximate Gottesman-Kitaev-Preskill codes”. *Phys. Rev. A* **102**, 032408 (2020).
- [71] Timo Hillmann, Fernando Quijandría, Arne L. Grimsmo, and Giulia Ferrini. “Performance of Teleportation-Based Error-Correction Circuits for Bosonic Codes with Noisy Measurements”. *PRX Quantum* **3**, 020334 (2022).
- [72] Kosuke Fukui. “High-threshold fault-tolerant quantum computation with the GKP qubit and realistically noisy devices” (2019). [arXiv:1906.09767](#).
- [73] Dagmar Bruß. “Optimal Eavesdropping in Quantum Cryptography with Six States”. *Phys. Rev. Lett.* **81**, 3018–3021 (1998).
- [74] Lana Sheridan and Valerio Scarani. “Security proof for quantum key distribution using qudit systems”. *Phys. Rev. A* **82**, 030301 (2010).
- [75] Charles H. Bennett and Gilles Brassard. “Public Key Distribution and Coin Tossing”. *IEEE Proc. Int. Conf. Computers, Systems and Signal Processing* Page 175 (1984). url: www.isical.ac.in/~rbose/internship/lectures2016/rt08bb84.pdf.
- [76] Kosuke Fukui and Nicolas C. Menicucci. “An efficient, concatenated, bosonic code for additive Gaussian noise” (2021). [arXiv:2102.01374](#).
- [77] Jonathan Conrad, Jens Eisert, and Francesco Arzani. “Gottesman-Kitaev-Preskill codes: A lattice perspective”. *Quantum* **6**, 648 (2022).

- [78] Jonathan Conrad, Jens Eisert, and Jean-Pierre Seifert. “Good Gottesman-Kitaev-Preskill codes from the NTRU cryptosystem” (2023). [arXiv:2303.02432](#).
- [79] Baptiste Royer, Shraddha Singh, and S.M. Girvin. “Encoding qubits in multimode grid states”. *PRX Quantum* **3**, 010335 (2022).
- [80] Mao Lin, Christopher Chamberland, and Kyungjoo Noh. “Closest lattice point decoding for multimode gottesman-kitaev-preskill codes” (2023). [arXiv:2303.04702](#).
- [81] Filippo Caruso, Jens Eisert, Vittorio Giovannetti, and Alexander S. Holevo. “Multimode bosonic Gaussian channels”. *New J. Phys.* **10**, 083030 (2008).
- [82] Zaki Leghtas, Gerhard Kirchmair, Brian Vlastakis, Robert J. Schoelkopf, Michel H. Devoret, and Mazyar Mirrahimi. “Hardware-Efficient Autonomous Quantum Memory Protection”. *Phys. Rev. Lett.* **111**, 120501 (2013).
- [83] Pei-Zhe Li and Peter van Loock. “Memoryless quantum repeaters based on cavity-qed and coherent states” (2022). [arXiv:2207.02443](#).
- [84] Shubham P. Jain, Joseph T. Iosue, Alexander Barg, and Victor V. Albert. “Quantum spherical codes” (2023). [arXiv:2302.11593](#).
- [85] Victor V. Albert. “Bosonic coding: introduction and use cases” (2022). [arXiv:2211.05714](#).
- [86] Arne L. Grimsmo, Joshua Combes, and Ben Q. Baragiola. “Quantum computing with rotation-symmetric bosonic codes”. *Phys. Rev. X* **10**, 011058 (2020).

