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
(Dated: October 23, 2019)

We propose a scheme that generalizes the loss scaling properties of twin-field or phase-matching QKD related to a channel of transmission \( \eta_{\text{total}} \) from \( \sqrt{\eta_{\text{total}}} \) to \( \sqrt[4]{\eta_{\text{total}}} \) 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 present the obtainable secret-key rates for up to \( n = 4 \) including memory dephasing and for \( n = 2 \) (i.e. \( \sqrt[4]{\eta_{\text{total}}-\text{MA-PM QKD assisted by a single memory station} } \)) 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 \( \eta_{\text{total}} \) can be reached for realistic, high-quality quantum memories (up to 1s 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 5s; beating ideal twin-field QKD requires 1s. 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 an analysis of sequential instead of parallel entanglement swapping of the memory qubits.

I. INTRODUCTION

In 1984 Bennett and Brassard presented a protocol (BB84) [1] that allows to distribute an information-theoretically secure key by utilizing the fundamental laws of quantum mechanics. This was the beginning of the new field of quantum key distribution (QKD) which nowadays already has commercial applications (see [2] for a recent overview of QKD). A key distribution over 421 km of glass fiber was demonstrated recently [3]. However, a complication of realistic QKD schemes is the linear scaling of the secret-key rate with the channel transmittance \( \eta_{\text{total}} \), where \( \eta_{\text{total}} \) 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 the 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 \( \eta_{\text{total}} \ll 1 \). Therefore, one needs to split the total channel into multiple segments of smaller length in order to overcome the linear scaling. This channel splitting is the main concept of all types of quantum repeaters making use of either quantum memories [6, 7] or quantum error-correcting codes [8, 11] or both in order to reduce the transmission cost. Due to the no-cloning theorem it is impossible that a quantum repeater simply reamplifies the signal at every intermediate station along the channel like a classical repeater. To date Ref. [12] is the only experimental demonstration yet of a quantum repeater that employs the above resources or tools to outperform the PLOB bound.

More than a decade ago it was shown that QKD systems are vulnerable to hacking attacks (see [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 only yields 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 treated as a black box. As such, the middle station can be completely untrusted, with Charlie potentially embodied by an eavesdropper, Eve. This approach protects 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 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. Now there already exist first experimental demonstrations of twin-field QKD that claim

† fschmi@students.uni-mainz.de
‡ loock@uni-mainz.de
to have overcome the PLOB bound [27–30].

In this work, we introduce a scheme that is an extension of the twin-field/phase-matching protocol to more than two physical segments exploiting quantum memories, similar to Ref. [31] and further extending a four-segment variant of Ref. [31], but with single-photon-based single-rail qubits replaced by coherent states. Thus, our scheme makes use of quantum memories - a kind of memory-assisted extension of phase-matching QKD [20, 22], ideally with sufficiently good memories and operations, in principle, scalable to arbitrary long distances. It also shares similarities with a hybrid quantum repeater (HQR) [32] 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, half way 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 \( L \rightarrow L/2 \) for \( 2n \) physical segments with only \( n - 1 \) memory stations. While this scheme could be supplemented by additional quantum error correction or detection mechanisms such as entanglement purification [6, 32, 33], here we shall consider the theoretically and especially experimentally simplest intermediate-scale versions without error correction.

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 new type of HQR and discuss its obtainable secret-key rate by employing a BB84 protocol, first for the channel-loss-only case and then for different error models - including channel loss, memory dephasing, detector dark counts, phase mismatch, and depolarization errors. We will also briefly describe a variant of our scheme based on optical homodyne measurements, similar to the original HQR [32]. Then we will explicitly calculate the attainable secret-key rates in Sec. IV for the first-order generalization \((n=2)\) considering mostly realistic parameters. We conclude in Sec. V and give more details about the calculations in the appendices.

II. BACKGROUND

A. Twin-field/Phase-matching QKD

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

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

- 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 \( \alpha \)). 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 (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) \( (\text{anti-})\)-correlated depending on which of the two detectors clicked. In our scheme, the level of security of these \( (\text{anti-})\)-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).

- The usual QKD steps of siftiung, estimating the error rate and leaked information, error correction and privacy amplification need to be performed.

Note that a pre-agreed complex amplitude \( \alpha \) 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 somewhat 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 [32] 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 send 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

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

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 \( \hat{p} := \frac{\hbar}{2} (\hat{a} - \hat{a}^\dagger) \), where \( \hat{a} \) and \( \hat{a}^\dagger \) are bosonic annihilation and creation operators. We can then choose a sufficiently small \( \Delta_p \) 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 \( \alpha \sin(2\theta) \). In the regime of large detuning \( \delta \) (see for example, Ref. [41]), we expect a coupling constant, \( \sigma_\pm \) are atomic transition operators and \( \sigma_z \) 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 \( \theta = \frac{\hbar}{2} \alpha^2 t_{\text{int}} \) where \( t_{\text{int}} \) denotes the interaction time. However, it is demanding to achieve a sufficiently strong nonlinear interaction corresponding to a \( \theta \) of the order of \( \frac{\pi}{4} \). Therefore, here we shall also consider the case where \( \theta \) is small (corresponding to a weak nonlinear interaction), similar to the analysis in Ref. [32].

A different approach was considered in the recent experiment of Ref. [12], 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 or not. 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 \( \pi \)-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 \( \pi \) 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 Fig. 1(a) and (b)).

1) Alice and Bob each have an atom as a quantum memory and generate a hybrid entangled state between their memory and an optical mode starting in a coherent state, resulting in $\frac{1}{\sqrt{2}} (|\uparrow\rangle, \alpha \exp(-i\theta)) + |\downarrow\rangle, \alpha \exp(i\theta))$. 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 already measured them, then this can be done via classical post-processing 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 $\alpha$ of the coherent state. Choosing a small $\theta$ 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 $\eta$ to a middle station operated by Charlie (angled states through a lossy channel of transmittance $\eta_{\text{total}} = \eta^2$).

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 following transformation,

$$\begin{pmatrix} \hat{a}' \\ \hat{b}' \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix}. \tag{4}$$

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 intuition 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 for the case of general $n$. The state before the BS is given by $\frac{1}{2} (|\uparrow\rangle, \alpha \exp(-i\theta)) + |\downarrow\rangle, \alpha \exp(i\theta))^{\otimes 2}$. After the BS (and changing order) the state is given by

$$\begin{align*}
\frac{1}{2} \left( |\uparrow\rangle, \sqrt{2} \alpha \exp(-i\theta), 0 \rangle + |\downarrow\rangle, \sqrt{2} \alpha \exp(i\theta), 0 \rangle \\
+ |\uparrow\rangle, \sqrt{2} \alpha \cos(\theta), -i\sqrt{2} \alpha \sin(\theta) \rangle \\
+ |\downarrow\rangle, \sqrt{2} \alpha \cos(\theta), i\sqrt{2} \alpha \sin(\theta) \rangle \right). \tag{5}
\end{align*}$$

FIG. 1. (Color online) 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 line). Such a $n$-segment quantum repeater scheme consists of $2n$ physical segments. (e) Set-up of the OM. Usually these detectors are on/off-detectors, but we could also use PNRDs. For $\theta \ll 1$ we only need one detector.
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 non-zero 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 non-zero measurement outcome (even or odd number) Charlie’s measurement would project the quantum memories onto $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|\uparrow, \downarrow\rangle \pm |\downarrow, \uparrow\rangle)$. As a consequence, our wish to need only small $\theta$ 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 $\frac{1}{2} \left(1 - e^{-2\alpha^2 \sin^2(\theta)}\right)$. When considering on/off detectors instead of PNRDs one projects onto a mixture of two Bell states. Note that the post-measurement memory state and the success probability only depend on the product $\alpha \sin(\theta)$ and therefore we can use an arbitrarily small $\alpha$ by employing correspondingly large amplitudes $\theta$ in this simplified model.

B. Channel-loss only

As the next step we will include the lossy channel with transmittance $\eta$ (between Alice/Bob and the middle station, again considering the $n = 1$ case) and obtain the density operator of Alice’s 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 App. 8. When Charlie uses a PNRD the resulting density operator is given by

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

where the upper sign holds in the even and the lower sign holds in the odd photon number case. Due to 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

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

Here, the state $|\Psi^-\rangle$ has a larger probability because of the larger fraction of an odd non-zero photon number than that for an even non-zero photon number. Therefore, Alice and Bob could exploit this to distill $1 - h(\frac{1}{2}(1 + e^{-2(1-\eta)\alpha^2 \sin^2(\theta)})$ or $1 - h(\frac{1}{2}(1 + e^{-2(2-\eta)\alpha^2 \sin^2(\theta)})$ ebits in the cases of PNRD 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

$$\frac{1}{2} \left(1 - e^{-2\eta\alpha^2 \sin^2(\theta)}\right) \left(1 - h \left(\frac{1}{2} \left(1 + e^{-2(2-\eta)\alpha^2 \sin^2(\theta)}\right)\right)\right).$$

Note that this is the same as the secret-key rate of BB84 in the asymptotic limit. The trade-off of the original HQR (assuming small $\theta$) between high fidelities for small $\alpha \theta$ and high success probabilities for large $\alpha \theta$ in the version with unambiguous state discrimination now becomes manifest in a high secret-key fraction (2nd factor) for small $\alpha \theta$ and a high raw rate (1st factor) for large $\alpha \theta$. However, the crucial difference now is that $\eta$ only refers to half of the distance between Alice and Bob thanks to the middle station even for a single repeater segment ($n = 1$). 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 $7.141 \cdot 10^{-2}$ 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 a factor of two improvement 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 $\theta$) is given by $0.5 \cdot 7.141 \cdot 10^{-2} \sqrt{\eta_{\text{total}}}$ (similar to [20], [43]).

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 App. 1 for details). For the case of on/off-detections, up to suitable Pauli operations (which can also be applied via classical post-processing if Alice and Bob already measured their qubits) 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

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

When using PNRDs one obtains a similar state with a different coefficient of $|\Phi^\pm\rangle (1 - \eta$ instead of $2 - \eta$). Using the results of the exact raw rate for determinisitic entanglement swapping [44], one can calculate the obtainable ebit/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 $\eta \ll 1$, see details in App. 8) and use the optimal value for $n\alpha^2 \sin^2(\theta)$, resulting in an overall secret-key rate of
z_{\text{scaling}} H(n)^{-1.07/2n} \sim 3.57 \cdot 10^{-2} {2^{z_{\text{scaling}}}} n(n+1) \gamma = 0.57721 \ldots \text{ is the Euler-Mascheroni constant. Also note that we always have to reduce the mean photon number } \alpha^2 \text{ of each optical pulse with increasing } n \left( \eta_{\text{optimum}} \approx \frac{1}{\sin(\theta)} \sqrt{\frac{0.22}{2n}} \right).

One benefit of this scheme is that in order to obtain a secret-key rate scaling of $\sqrt{z_{\text{scaling}}}$ one only needs $n-1$ stations equipped with quantum memories. In comparison, a standard quantum repeater 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 $\sqrt{z_{\text{scaling}}}$ 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) \[6\].

When considering first experimental realizations of small-scale memory-based quantum repeaters, using a scheme like ours (or related schemes like those of Ref. \[31\]) could be beneficial, because in order to obtain a secret-key rate scaling of $\sqrt{z_{\text{scaling}}}$ only a single memory station is needed instead of three.

For the case of this section where 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, we will first only include the most important errors which still allows us to see their influence onto the secret-key rate in simple, analytical expressions. We first consider detector inefficiencies and memory dephasing where we can still describe the resulting states as mixtures of two Bell states. Later we also consider imperfections of the Bell measurement which will still give us Bell-diagonal states. Finally, we will also take into account dark counts which will lead to Bell-non-diagonal states.

Including detector efficiencies ($\eta_{\text{det}}$) is trivial, because we only have to substitute $\eta \rightarrow \eta \cdot \eta_{\text{det}}$. 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 App. \[AD\]).

C. Including memory dephasing

Consider $n$ repeater segments ($n > 1$, otherwise no memory is needed), then we can assign independent random variables $X_j$ ($j \in \{1, \ldots, n\}$) to every segment counting for each the number of attempts until the entanglement is distributed due to a successful measurement outcome of the detector for that segment. These random variables follow a geometric distribution $P(X = k) = p \cdot q^{k-1}$ with $q = 1 - p$ where $p$ is the probability of success of the measurement. We can then introduce a new random variable $M$ describing the totally used memory time for which the quantum states dephased. If Alice and Bob exploit the quantum repeater immediately for QKD and do not store their qubits during the whole protocol, we define

$$M := \max(X_1, \ldots, X_n) - X_1$$

$$+ 2 \sum_{j=2}^{n-1} (\max(X_1, \ldots, X_n) - X_j)$$

$$+ \max(X_1, \ldots, X_n) - X_n, \quad (9)$$

and otherwise we define

$$M := 2 \sum_{j=1}^{n} (\max(X_1, \ldots, X_n) - X_j). \quad (10)$$

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

$$\frac{1}{2} \left( 1 + e^{-2n(2-\eta)\alpha^2 \sin^2(\theta)} \cdot \exp \left( -M_T \frac{\tau}{T} \right) \right) |\Phi^+ \rangle \langle \Phi^+ | \quad (11)$$

$$+ \frac{1}{2} \left( 1 - e^{-2n(2-\eta)\alpha^2 \sin^2(\theta)} \cdot \exp \left( -M_T \frac{\tau}{T} \right) \right) |\Phi^- \rangle \langle \Phi^- |,$$

where $\tau$ 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 definitions of Eqs. (9,10) rely on the observation that the memory dephasing that occurs in all segments for different durations will just accumulate as a sum in the final state (see App. \[D\]).

However, this definition of $M$ is not optimal for more than two segments, because it assumes that the entanglement swapping operations are performed after all segments 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.\(^\text{[17]}\)

The density operator in Eq. (11) describes the state after a single run, but we are interested in the averaged state. This means we have to calculate the expectation value \( E[\exp(-M\tau)] \). We calculate this expectation value for the case \( n = 2 \) in App. C\(^\text{[44]}\). Unfortunately, it is not even known how to calculate the probability distribution of \( M \) 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, however, we can use the bound \( E[\exp(-M\tau)] \geq \exp(-E(M)\tau) \) which can be obtained by applying Jensen’s inequality. As the expectation value operation is linear, we can easily calculate \( E(M) \) since the exact \( E(\max(X_1, \ldots, X_n)) \) is already known in the literature\(^\text{[14]}\), and we obtain (for the case when Alice and Bob do not store their halves, so for \( M \) from Eq. (9)):

\[
E(M) = 2(n-1) \left( \sum_{j=1}^{n} \binom{n}{j} \frac{(-1)^j}{q^j} \frac{1}{3} - \frac{1}{p} \right),
\]

also using the well-known result for a geometric distributed variable, \( E(X_j) = \frac{1}{p}, \forall j = 1 \ldots n \). 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 for very large numbers of dephasing memories. For the simple case of \( E(\tau) = 2 \) (previously all submatrix were zero) 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 \( \exp(-E(M)\tau) \) and \( \exp(-E(M)\tau) \) (see App. C\(^\text{[44]}\)) and compared their corresponding secret-key fractions (assuming \( p = 10^{-4}, \eta \ll 1 \)). For the case of \( T = 10E(M)\tau \), we found that the exact calculation yields a 1% higher secret-key rate. When considering \( T = E(M)\tau \) the error increased to 86% and when looking at memories with \( T = 0.1E(M)\tau \) the approximation underestimated the secret-key fraction by six orders of magnitude, although the exact secret-key fraction of \( 2 \cdot 10^{-3} \) was not ridiculously low. Note that even after including memory dephasing the distillable entanglement and the asymptotic secret-key fraction of BB84 coincide. Numerical simulations show that the bound becomes tighter for an increasing number of repeater segments.\(^\text{[19]}\)

Unfortunately, realistic coherence times are often too small for obtaining a good bound by applying Jensen’s inequality. Besides the quality of a theoretical bound, in practice, the negative impact of short memory times can also be seen in Sec. IV where we calculate secret-key rates for a two-segment repeater. There it will help to consider a cut-off parameter which defines a maximal decoherence time before a state is discarded. In the case of only two segments we can also calculate the expectation value of the dephasing fractions with cut-off. For more than two segments we could use the results of Ref.\(^\text{[45]}\), where the authors consider a repeater protocol that involves an additional waiting time where the memories dephase. They considered multiple nesting levels of a repeater always doubling the number of segments with each new nesting level. Due to the additional waiting time, it is a self-similar scheme, such that the authors are also able to calculate the dephasing errors for many segments. Methods to calculate the effects of dephasing and cut-offs apply to general quantum repeaters and not only to our proposed scheme. According to our knowledge, Ref.\(^\text{[45]}\) is the only reference that considers effects of dephasing errors and cut-offs for large quantum repeaters. Since it is possible to increase secret-key fractions enormously by introducing cut-offs, it is important to further investigate the effects of dephasing and cut-offs for large-scale quantum repeaters in future work. Here our focus will be mainly on repeaters with \( n = 2, 3, 4 \) segments whose ultimate secret-key rates scale as \( \sqrt{\eta_{\text{total}}}, \sqrt{\eta_{\text{total}}} \), and \( \sqrt{\eta_{\text{total}}} \) respectively.

### D. Including dark counts and phase mismatch

With the inclusion of detector dark counts we need to use the full \( 4 \times 4 \) density matrix (in the computational basis) instead of an (effective) \( 2 \times 2 \) matrix (previously all matrix elements except a \( 2 \times 2 \) submatrix were zero) in order to describe the two-qubit state. Calculating the state before the entanglement swapping is straightforward but lengthy (see App.\(^\text{[3]}\)) and the state after multiple entanglement swappings can be described by a set of recursive relations (see also App.\(^\text{[3]}\)). 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\(^\text{[19]}\). 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 \( \tau = 2 \cdot \frac{\log_2 3}{2\epsilon} \) 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 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 afterwards (see App.\(^\text{[3]}\)). Also notice that it is possible to obtain the advantage of a simplified analysis without the need for correlated Pauli operations.\(^\text{[50]}\) 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. Due to 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 only a bit shorter than the distance where the secret-key fraction drops to zero the relative error becomes relevant, up to the point that 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 \( \alpha \) for generating the hybrid entangled states while the other party uses a coherent state with amplitude \( \alpha e^{i\phi} \), where \( \phi \) 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 \( \theta \) the rate can vary up to a few percent. However, the relevant distribution for the secret-key fraction is the probability distribution of \( \phi \) 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, and so the secret-key rate is nearly unaffected. We calculated the Bell-diagonal coefficients and their expectation values with respect to \( \phi \). 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 \( \phi \).

### E. Homodyne measurement

Up to now we only considered a scenario where Charlie (besides the less practical case of PNREs) 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. (5) 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, \( \alpha \in \mathbb{R}^+ \), we only learn that Alice and Bob have different bits but we do not learn 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 \( \pm \sqrt{2\alpha \sin(\theta)} \)). 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 App. [E]. 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 \( \Delta_x \) and \( \Delta_p \) is a compromise between a high raw rate and a high state quality. For a given \( \alpha \) and \( \theta \) we can reduce the \( Z \)-error rate by decreasing \( \Delta_p \). One might think that the parameter \( \Delta_x \) is not relevant and can therefore be set to \( \infty \). However, this is not true since it also has an influence on the \( X \)-error rate making it even impossible to share a secret key in the no-loss case of \( \eta = 1 \) for too large \( \Delta_x \). This problem can be solved by simply choosing a sufficiently small \( \Delta_x \), but even then a non-zero secret-key rate cannot be obtained for even moderate losses like \( \eta = 0.7 \) (about 8 km for the physical segment length assuming perfect detectors).

### IV. COMPARISON OF SECRET-KEY RATES

Let us now consider the performance in terms of BB84 secret-key rates 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]):

- \( \eta = 0.15 \exp\left(-\frac{L}{4L_{\text{att}}}\right) \)
- \( L_{\text{att}} = 22\text{km} \)
- \( \alpha = 23.9 \)
• \( \theta = 0.01 \)
• dark count probability \( 8 \cdot 10^{-8} \)
• \( p_{\text{depol}} = 0.99 \)
• \( \tau = \frac{L}{2c} \)
• \( c = 2 \cdot 10^8 \frac{\text{m}}{\text{s}} \)
• error correction inefficiency \( f_{\text{EC}} = 1.15 \)

The transmission parameter \( \eta \) is here for a quarter of the total distance \( L \) between Alice and Bob, because every mode travels only for this distance to the corresponding detector station, and it contains a finite detector efficiency (factor \( \eta_{\text{det}} = 0.15 \)). We shall also consider perfect detectors, \( \eta_{\text{det}} = 1 \). Since we do not know the optimal value of \( \alpha \) (for given \( \theta \)) when considering all these errors, we simply use the optimal \( \alpha \) from the loss-only case. Further parameters are explained in the appendix.

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

\[
1 - h(e_X) - f_{\text{EC}} \cdot h(e_Z),
\]

where \( e_X/Z \) are the error probabilities in the \( X \)- and \( Z \)-basis which can also be expressed in terms of the four Bell coefficients of the density matrix. Note that we consider the biased BB84 scheme where one of the two bases is employed more often allowing to increase the sifting factor to 1 in the asymptotic limit of infinite repetitions [51].

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. Let us first study the effect of the memory dephasing, since insufficient coherence times are an important issue for quantum repeaters. As it can be seen in Figs. 2, 3, one really needs demanding memory coherence times such as 1000 seconds 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 at most 1s, it can be seen easily that it is not even possible to overcome the PLOB bound. 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 \( p_{\text{det}} \) is a highly influential parameter determining whether PLOB can be exceeded or even the ultimate \( \sqrt{n_{\text{total}}} \)-scaling can be approached, with realistic (\( \sim 1s \)) or potential future (\( \gtrsim 10s \)) coherence times, respectively (see Fig. 2 [52]).

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 \( \Delta \) 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 [51, 55] derive the raw qubit rate for a two-segment repeater with such a memory cut-off, while Ref. [60] presents a rate formula for the more general case of arbitrarily many segments under the constraint of deterministic entanglement swappings. References [51, 55] analyze the dephased qubit states for schemes with at most two segments. As it can be seen in Fig. 2 it is possible to overcome the PLOB bound by introducing a cut-off and, furthermore, it is even possible to distribute secret keys over a distance of 700 km and more with realistic memories and detectors (compare this with Fig. 2 even with \( T = \infty \)). In this work we only consider cut-off rates for \( n = 2 \).

In Fig. 5 one can see the scaling behavior of repeaters based on our protocol with \( n = 2, 3 \) or even 4 repeater segments considering infinite and finite memory times (the latter for 1000s) 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 no-loss case, but it yields better rates when considering other errors. However, note that we did not try to find an optimal \( \alpha \) in the general case. 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 TF-QKD without memory stations, the more relevant benchmark for our protocol may be \( \sqrt{n_{\text{total}}} \) which can be exceeded at approximately 350 km. If we consider a coherence time of only 10s we can barely surpass \( \sqrt{n_{\text{total}}} \), but with an appropriately chosen cut-off parameter (\( n = 2 \)) we can overcome this benchmark even for distances between 450 and 1500 km. Furthermore, by making use of a memory cut-off and perfect efficiency detectors, but still considering dark counts and an imperfect Bell measurement, it is also possible to reduce the needed coherence time for overcoming \( \sqrt{n_{\text{total}}} \) from 10s to 5s. In order to obtain better rates than in the ideal twin-field scheme a coherence time of 1s suffices, even without making use of a memory cut-off (see Fig. 3). Up to now we only considered repeater schemes, where we try to generate entanglement in the repeater segments in parallel. In App. C we also discuss the case where we generate entanglement in the repeater segments in a sequential manner. In general, one can say that, on the one hand, the sequential method has the disadvantage of a lower raw rate, but, on the other hand, it has the advantage of a lower total used memory time. Therefore, the sequential scheme yields a worse secret-key rate than a parallel scheme for small distances, but for large distances it yields better secret-key rates. Besides this, the secret-key rates can be calculated exactly for the sequential scheme.

According to Fig. 6 the phase mismatch can be almost neglected when \( \Delta < 0.1 \theta \) (this even holds for \( \theta = \frac{\pi}{2} \)). However, for larger \( \Delta \) the secret-key rate drops to zero
FIG. 2. (Color online) Secret-key rates for a two-segment repeater \((n = 2)\) without phase mismatch and assuming the parameters as listed in the main text. The straight lines denote the PLOB bound, \(\eta_{\text{total}}\), and \(\sqrt{\eta_{\text{total}}}\). The rates are for different coherence times \(T\) of \((1, 10, 100, 1000, \infty)\) seconds (from left to right). The areas between PLOB and \(\eta_{\text{total}}\) and between \(\sqrt{\eta_{\text{total}}}\) and \(\sqrt{\eta_{\text{total}}}\) are highlighted in color.

FIG. 3. (Color online) Secret-key rates assuming the same parameters as in Fig. 2 except for \(p_{\text{det}} = 1\) instead of \(p_{\text{det}} = 0.15\).

FIG. 4. (Color online) Secret-key rates for a two-segment repeater \((n = 2)\) 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 second. The straight lines denote the PLOB bound, \(\sqrt{\eta_{\text{total}}}\), and \(\sqrt{\eta_{\text{total}}}\). The rates are for different values of the memory cut-off times of \((10, 100, 1000, 10000)\). The areas between PLOB and \(\sqrt{\eta_{\text{total}}}\) and between \(\sqrt{\eta_{\text{total}}}\) and \(\sqrt{\eta_{\text{total}}}\) are highlighted in color.

FIG. 5. (Color online) Secret-key rates for a repeater with \(n = 2\) (red), 3 (green), 4 (blue) segments using a parallel protocol without cut-off (\(\alpha = 23.9\) in all cases). The undashed 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 1000 seconds. The benchmarks PLOB, \(\sqrt{\eta_{\text{total}}}\), \(\sqrt{\eta_{\text{total}}}\), \(\sqrt{\eta_{\text{total}}}\), and \(\sqrt{\eta_{\text{total}}}\) can also be seen. The regions between two of those benchmarks are highlighted in color accordingly.

very fast. For \(\Delta = \theta = 0.01\) it is even impossible to obtain a secret key using the above parameters. Therefore, we cannot choose \(\theta\) arbitrarily small since this increases too much the required precision of the phase matching.

V. CONCLUSION

We introduced a measurement-device independent QKD scheme based on the twin-field scheme but making use of memories in order to extend the overall distance where a secret key can be distributed. The secret-key rate of our scheme scales as \((nH(n))^{-1}z\sqrt{\eta_{\text{total}}}\) (harmonic number \(H(n) = \gamma + \ln(n) + O(n^{-1})\)) in the loss-only case (assuming \(z\sqrt{\eta_{\text{total}}} \ll 1\)), where \(\gamma = 0.57721\ldots\) 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 \(\eta_{\text{total}} = \exp\left(-\frac{L}{L_{\text{att}}}\right)\) 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 trade-off related to the entanglement generation rate and state quality with regard to \(\alpha \sin(\theta)\) where \(\alpha\) is the optical coherent-state amplitude and \(\theta\) 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. We showed in particular that it is possible, in principle, to employ small dispersive phase rotations \(\theta\) corresponding to weak optical non-linearities. Another advantage of our scheme compared to the original hybrid quantum repeater is that
FIG. 6. (Color online) Secret-key fraction for the two-segment quantum repeater using the above-mentioned parameters. We choose different coherence times for the three different plots and in each plot we consider a phase mismatch $\Delta$ of $(0, 10^{-4}, 10^{-3}, 5 \cdot 10^{-3}, 7.5 \cdot 10^{-3})$ (from top to bottom). (a) ideal memories, (b) $T = 10E(M)\tau$, (c) $T = E(M)\tau$.

The results show 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 1s and modest detector efficiencies. The ideal single-repeater scaling of $\sqrt{\eta_{\text{total}}}$ can be exceeded when coherence times of 5s and perfect detector efficiencies are approached. In order to overcome the ideal twin-field rate only a coherence time of 1s 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) 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 large 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 also considered 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, methods for quantum error correction or detections were not considered.

Like in all twin-field-type 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. We also thank Stefano Pirandola and Mark Wilde for useful comments on the manuscript.

Appendix A: Error models

Here we briefly describe all error models employed for our analysis. A lossy channel with transmittance $\eta$ 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

$$\begin{pmatrix} \hat{a}' \\ \hat{b}' \end{pmatrix} = \begin{pmatrix} \sqrt{\eta} & \sqrt{1-\eta} \\ \sqrt{1-\eta} & -\sqrt{\eta} \end{pmatrix} \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix},$$

(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, $\eta$ is given by $\exp(-\frac{L}{L_{\text{att}}})$, where $L$ is the fiber’s length and $L_{\text{att}}$ is the attenuation length of 22km in a typical optical fiber.

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

$$\mathcal{E}_{\text{dephasing}}(x, \rho) = \frac{1}{2}(1 + \exp(-x))\rho + \frac{1}{2}(1 - \exp(-x))Z\rho Z,$$

(A2)

where $\rho$ is a single-qubit density matrix, $Z$ the Pauli qubit phase-flip operator and $x$ counts the dephasing time in units of the memory coherence time. The imperfections of the Bell measurement on the quantum memories is modeled by the following depolarizing channel,

$$\mathcal{E}_{\text{depol}}(\rho_{\text{depol}}) = \rho_{\text{depol}}\rho + (1 - \rho_{\text{depol}})\frac{1}{2}.$$

(A3)

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

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

(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 App. [F]).

Appendix B: Approximation of the raw rate

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 $\max(X_1, \cdots, X_n)$, 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 $\mathbb{E}[\max(X_1, \cdots, X_n)]$. For the case $p \ll 1$ and deterministic entanglement swapping it is possible to obtain a simple approximation of $\mathbb{E}[\max(X_1, \cdots, X_n)]$ where $X$ is geometrically distributed:

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

(B1)

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

(B2)

This approximation is based on the exact expression of Ref. [5] 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

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

(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,

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

(B4)

where $\gamma = 0.57721 \cdots$ is the Euler-Mascheroni constant.

In the end we obtain the simple approximation

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

(B5)

Note that this approximation scales with $\ln(n)$, while the widely used approximation $\frac{1}{p} \log_2(n) \frac{1}{p}$ 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 [5].

Appendix C: Effect of memory dephasing for $n=2$

For the case of two quantum repeater segments, the definition of $M$ in Eq. (5) 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

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

where $p$ and $q = 1-p$. For $p \ll 1$, this expression simplifies to the Poisson distribution for $M = 0$.
and for $j > 0$,

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

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 $M := |X_1 - X_2|$

$$
E \left[ \exp \left( -M^2 \tau \right) \right] = \frac{p}{2 - p} \left( 1 + \frac{2}{1 - q \exp(-\tau)} \right),
$$

(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 (cut-off). The additional complexity of this protocol lies solely in the raw rate, which is already known in the literature [54–56].

Note that we also have to consider an additional non-random dephasing time because each memory already dephased during the time between sending the optical mode and obtaining the information whether the optical measurement was successful or not. Therefore, each memory dephases for a time unit of $\frac{T}{nc}$. If we perform the measurements on the outer memories immediately (like in Eq. (2)), we only accumulate a constant dephasing time of $2(n - 1) \frac{T}{nc} = \frac{2T}{n} (1 - \frac{1}{n})$. If we perform the measurement of the outer memories at the end of the entanglement distribution, we accumulate a constant dephasing time of $\frac{2T}{e}$.

Appendix D: Pauli channels and entanglement swapping

We call a single-qubit channel $\mathcal{N}(\cdot)$ a Pauli channel iff $\mathcal{N}(\rho) = \sum_i p_i \rho \rho_i^\dagger$ where $p_i$ are probabilities and $\rho_i$ are Pauli operators (I, X, Y, Z). Since all of these Pauli operators either commute or anti-commute, 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 $P_1$ and $P_1^\dagger$ 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 $\mathcal{N}_4$ for qubits 2 and 3

$$
\begin{align*}
\langle \Phi^+ \rangle_{23} \mathcal{N}_2 (|\Phi^+\rangle_{12} \langle \Phi^+|) \otimes \mathcal{N}_4 (|\Phi^+\rangle_{34} \langle \Phi^+|) |\Phi^+\rangle_{23} \\
= \langle \Phi^+ \rangle_{23} \sum_{i,j=1}^{4} p_i p_j P_{i,2} \langle \Phi^+ |_{12} \langle \Phi^+| P_{i,2}^\dagger \otimes P_{j,3} |\Phi^+\rangle_{34} \langle \Phi^+| P_{j,3}^\dagger |\Phi^+\rangle_{23} \\
= \sum_{i,j=1}^{4} p_i p_j P_{i,1} P_{j,4} \langle \Phi^+ |_{12} \langle \Phi^+| P_{i,2}^\dagger \otimes P_{j,3} |\Phi^+\rangle_{34} \langle \Phi^+| P_{j,3}^\dagger |\Phi^+\rangle_{23} P_{i,1}^\dagger P_{j,4}^\dagger \\
= \frac{1}{4} \sum_{i,j=1}^{4} p_i p_j P_{i,1} P_{j,4} \langle \Phi^+ |_{14} \langle \Phi^+| P_{j,4}^\dagger P_{i,1}^\dagger \\
= \frac{1}{4} \sum_{i,j=1}^{4} p_i p_j P_{i,1} P_{j,1} \langle \Phi^+ |_{14} \langle \Phi^+| P_{j,1}^\dagger P_{i,1}^\dagger \\
= \frac{1}{4} \mathcal{N}_1 (\mathcal{N}_4^\dagger (|\Phi^+\rangle_{14} \langle \Phi^+|)) .
\end{align*}
$$

(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/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 non-diagonal elements [49, 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 $\frac{d}{c}$, 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. $x + x'$ for $N_1$ and $N_2'$ in Eq. (D1) for $x$ as defined in Eq. (A2). Similarly, we can simplify the concatenation of the $n-1$ depolarizing channels with parameter $p_{\text{depol}}$, describing the probability of no depolarization, into a depolarizing channel with $p'_{\text{depol}} = p_{\text{depol}}^{n-1}$. The concatenation of the Pauli channel corresponding to dark counts/measurements cannot be simplified as much as for the depolarizing or dephasing channel. For the concatenation of a general single-qubit Pauli channel,

$$
\mathcal{N}(\rho) = p_1 \rho + p_2 \mathcal{Z}\rho \mathcal{Z} + p_3 \mathcal{X}\rho \mathcal{X} + p_4 \mathcal{Y}\rho \mathcal{Y},
$$

we obtain the following recursive set of equations,

$$
\begin{align*}
\left( \begin{array}{c}
\rho_{1}^{(n+1)} \\
\rho_{2}^{(n+1)} \\
\rho_{3}^{(n+1)} \\
\rho_{4}^{(n+1)}
\end{array} \right) &= \left( \begin{array}{cccc}
p_{1} & p_{2} & p_{3} & p_{4} \\
p_{2} & p_{1} & p_{3} & p_{4} \\
p_{3} & p_{4} & p_{1} & p_{2} \\
p_{4} & p_{3} & p_{2} & p_{1}
\end{array} \right) \left( \begin{array}{c}
\rho_{1}^{(n)} \\
\rho_{2}^{(n)} \\
\rho_{3}^{(n)} \\
\rho_{4}^{(n)}
\end{array} \right),
\end{align*}
$$

where $\rho_{1}^{(0)} = 1$ and $\rho_{2}^{(0)} = \rho_{3}^{(0)} = \rho_{4}^{(0)} = 0$. Therefore, we have

$$
\begin{align*}
\left( \begin{array}{c}
\rho_{1}^{(n)} \\
\rho_{2}^{(n)} \\
\rho_{3}^{(n)} \\
\rho_{4}^{(n)}
\end{array} \right) &= \left( \begin{array}{cccc}
p_{1} & p_{2} & p_{3} & p_{4} \\
p_{2} & p_{1} & p_{3} & p_{4} \\
p_{3} & p_{4} & p_{1} & p_{2} \\
p_{4} & p_{3} & p_{2} & p_{1}
\end{array} \right) \left( \begin{array}{c}
1 \\
0 \\
0 \\
0
\end{array} \right).
\end{align*}
$$

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. 4(b)), i.e. we first have the state

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

After applying the lossy channels of transmittance $\eta$ (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:

$$
\frac{1}{2} \left( |\uparrow, \uparrow, \sqrt{2}\eta \alpha e^{-i\theta}, 0, \sqrt{1-\eta} \alpha e^{-i\theta}, \sqrt{1-\eta} \alpha e^{-i\theta} \rangle + \downarrow, \downarrow, \sqrt{2}\eta \alpha e^{i\theta}, 0, \sqrt{1-\eta} \alpha e^{i\theta}, \sqrt{1-\eta} \alpha e^{i\theta} \rangle 
\right.
\left. + |\uparrow, \downarrow, \sqrt{2}\eta \alpha \cos(\theta), -i \sqrt{2}\eta \alpha \sin(\theta), \sqrt{1-\eta} \alpha e^{-i\theta}, \sqrt{1-\eta} \alpha e^{i\theta} \rangle 
\right.
\left. + \downarrow, \uparrow, \sqrt{2}\eta \alpha \cos(\theta), i \sqrt{2}\eta \alpha \sin(\theta), \sqrt{1-\eta} \alpha e^{i\theta}, \sqrt{1-\eta} \alpha e^{-i\theta} \rangle \right).
$$

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

$$
\text{Tr}_2 \left( \sum_{k,j} c_k c^*_j |k\rangle_1 \langle j | \otimes |\Psi_k\rangle_2 \langle \Psi_j|_2 \right)
$$

to calculate the reduced density matrix of system 1:
Similarly, one can show for the conditional state of sub-system 1 with measurement operators $A$ acting on sub-system 2:

$$\text{Tr}_2 \left( \sum_{k,j} c_k c_j^* |k\rangle_1 \langle j| \otimes |\Psi_k\rangle_2 \langle \Psi_j| \right)$$

$$= \sum_{k,j} c_k c_j^* |k\rangle_1 \langle j| \cdot \sum_l |\Psi_j| l\rangle_2 \langle l|_2 |\Psi_k\rangle_2$$

$$= \sum_{k,j} c_k c_j^* |k\rangle_1 \langle j| \cdot \langle \Psi_j| \Psi_k\rangle_2 . \quad (E3)$$

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:

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

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

| $|\uparrow, \uparrow\rangle$ | $|\downarrow, \downarrow\rangle$ | $|\uparrow, \downarrow\rangle$ | $|\downarrow, \uparrow\rangle$ |
|---|---|---|---|
| $\pm a$ | $\pm e^{i\theta} a^*$ | $d_1^*$ | $d_2^*$ |
| $a$ | $c e^{i\theta}$ | $d_1$ | $d_2$ |
| $|\uparrow, \downarrow\rangle$ | $|\downarrow, \uparrow\rangle$ | $d_2^*$ | $f^*$ |
| $d_2$ | $d_1^*$ | $f$ | $b$ |

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

$$b = \langle \pm i \sqrt{2 \eta \alpha \sin(\theta)} \hat{E} \pm i \sqrt{2 \eta \alpha \sin(\theta)} \rangle$$

$$= 1 - e^{-2 \eta \alpha^2 \sin^2(\theta)} D(0) , \quad (E6)$$

Note that $A^\dagger A$ is a POVM element and the POVM of an on/off detector including dark counts, see $E$ 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.

$$c = \langle \sqrt{1 - \eta \alpha e^{-i\theta}} \rangle \langle \sqrt{1 + \eta \alpha e^{i\theta}} \rangle^2 \cdot \langle \sqrt{2 \eta \alpha e^{-i\theta}} \rangle \cdot \langle \sqrt{2 \eta \alpha e^{i\theta}} \rangle \cdot a$$

$$= e^{2 \alpha^2 (2 \eta - 1)}, \quad a = a \cdot e^{-2 \alpha^2 \sin^2(\theta) + 2 \alpha^2 \sin(2\theta)} , \quad (E7)$$

$$d = d_1 = d_2 = \langle \sqrt{1 - \eta \alpha e^{-i\theta}} \rangle \langle \sqrt{1 - \eta \alpha e^{i\theta}} \rangle \cdot \langle \sqrt{2 \eta \alpha \cos(\theta)} \rangle \langle \sqrt{2 \eta \alpha \sin(\theta)} \rangle \cdot \langle 0 | \hat{E} | \sqrt{2 \eta \alpha \sin(\theta)} \rangle$$

$$= a \cdot e^{-2 \alpha^2 \sin^2(\theta)} , \quad \langle \sqrt{2 \eta \alpha \sin(\theta)} \rangle$$

$$f = | \langle \sqrt{1 - \eta \alpha e^{-i\theta}} \rangle \langle \sqrt{1 - \eta \alpha e^{i\theta}} \rangle^2 \cdot \langle i \sqrt{2 \eta \alpha \sin(\theta)} \hat{E} - i \sqrt{2 \eta \alpha \sin(\theta)} \rangle$$

$$= e^{-2 \alpha^2 \sin^2(\theta)(2 \eta - 2) (e^{-2 \alpha^2 \sin^2(\theta)} - D(0))} . \quad (E9)$$
Note that without dark counts, \( a = c = d = 0 \) and \( D(0) = 1 \), we recover the effective \( 2 \times 2 \) 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 us information about the relative distribution of \( |\phi^\pm\rangle \) and this parameter varies periodically with \( \theta \). Therefore, it can be useful to apply local transformations for permuting the four Bell coefficients \(^{50}\) 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! elementary segments and \( |\Phi^+\rangle \) as measurement outcome, while above we considered the case of \( j = 0 \) and omitted the subscript):

\[
\begin{align*}
a_{j+1} &= a_j^2 + b_j^2 + 2\text{Re}(d_j^2), \\
b_{j+1} &= 2(a_j \cdot b_j + \text{Re}(d_j^2)), \\
c_{j+1} &= 2d_j^2 + f_j^2 + c_j^2, \\
d_{j+1} &= d_j(a_j + b_j + c_j^2) + d_j^2 f_j, \\
f_{j+1} &= 2(d_j^2 + f_j \text{Re}(c_j)).
\end{align*}
\] (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. \(^{50}\) without correlated Pauli operations (see main text), 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: Calculation of the quantum repeater states with homodyne measurements

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

\[
\frac{1}{2}(|\uparrow, \uparrow, \alpha e^{-i\theta}, \alpha e^{-i\theta}\rangle + |\downarrow, \downarrow, \alpha e^{i\theta}, \alpha e^{i\theta}\rangle)
\] (F1)

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

\[
\frac{1}{2}(|\uparrow, \uparrow, \alpha e^{-i\theta}\rangle \langle \hat{x} = x | \alpha e^{-i\theta}\rangle + |\downarrow, \downarrow, \alpha e^{i\theta}\rangle \langle \hat{x} = x | \alpha e^{i\theta}\rangle + |\downarrow, \uparrow, \alpha e^{-i\theta}\rangle \langle \hat{x} = x | \alpha e^{-i\theta}\rangle + |\uparrow, \downarrow, \alpha e^{i\theta}\rangle \langle \hat{x} = x | \alpha e^{i\theta}\rangle).
\] (F2)

As the next step we calculate position- and momentum-space wave functions of a coherent state with amplitude \( x_0 + i \cdot p_0 \). 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 \((\hat{h} = \frac{1}{2} \text{ in our notation})\) and the Baker-Campbell-Hausdorff formula:

\[
\langle \hat{x} = x| x_0 + ip_0 \rangle = \langle x = x| x_0 + ip_0 \rangle \exp((-2ix_0 \hat{p}) \exp(-ip_0x_0)|0\rangle
\] (F3)

\[
= \langle x = x| 2ip_0(x - x_0)|0\rangle \exp((-2ix_0 \hat{p}) \exp(-ip_0x_0)|0\rangle
\] = \[\langle x = x| \exp(2ip_0\hat{x})|0\rangle \exp((-2ix_0 \hat{p}) \exp(-ip_0x_0)|0\rangle
\] = \[\langle x = x| \exp(\frac{2ip_0x}{x_0}) \exp(-2i\frac{x_0\hat{p}}{x_0})|0\rangle
\] = \[\frac{1}{\sqrt{2} \pi} \exp\left[\frac{-2\pi^2}{2}\right] \] (F4)

Similarly, one can show

\[
\langle \hat{p} = p| x_0 + ip_0 \rangle = \sqrt{\frac{\pi}{2}} \exp\left[\frac{-(p - p_0)^2}{2}\right] \exp\left[\frac{-2i\pi\hat{x}}{2}\right].
\] (F5)

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 the preceding section) and we obtain the following results (all elements must be divided by the matrix trace, \( 2(a + b) \), for normalization),

\[
a = \frac{1}{2} \left( \text{erf}(\sqrt{2}\Delta_p - 2a \sin(\theta)) + \text{erf}(\sqrt{2}\Delta_p + 2a \sin(\theta)) \right),
\] (F5)

\[
b = \text{erf}(\sqrt{2}\Delta_p),
\] (F6)
c = \exp \left( 2 \alpha^2 (-1 + \exp(2\theta)) \right) \text{erf}(\sqrt{2\Delta_p}),
\quad (F7)
\text{f} = \exp \left( -4\alpha^2 \sin^2(\theta) \right) \text{erf}(\sqrt{2\Delta_p}) \frac{\text{Re} \left[ \text{erf}(\sqrt{2\Delta_p} + 2\alpha \sin(\theta)) \right]}{\text{erf}(\sqrt{2\Delta_p})},
\quad (F8)

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 \( \alpha \to \alpha \sqrt{\eta} \) within the erf-functions and otherwise nothing changes where \( \eta \) is the transmission parameter corresponding to one physical segment (half a repeater segment). For example, for \( n = 1 \), we have \( \alpha \to \sqrt{\eta} \alpha \).

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 G: Sequential swapping strategy**

Up to now we considered the entanglement swapping strategy based on trying to distribute entanglement in each segment in parallel and waiting until the entanglement distribution succeeded in all segments. Then all entanglement swapping operations are performed. However, we already noted in the main text that in the case of deterministic swapping, it is better to perform the swapping operations as soon as possible, in order to keep the number of simultaneously dephasing memories low. As a consequence, it seems beneficial to consider the strategy where we distribute entanglement sequentially and immediately perform entanglement swapping. Hence the relevant random variables for the raw rate and the memory dephasing are given by sums of independent random variables, such that the calculations can be easily solved exactly. This means we do not need to use the lower bound on the secret-key fraction based on Jensen’s inequality. However, the raw rate then decreases (recall App. B) from \( \frac{H(n)}{n} \equiv M \) to \( \frac{\mathbb{E}[M_{\text{seq}}]}{n} \) (this holds for general memory-based quantum repeaters). In order to be sure that improvements in the state quality arise from the changed strategy and not only from using the exact expression instead of a lower bound, we will also compare both strategies using the lower bound based on Jensen’s inequality. 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 \( M_{\text{seq}} := 2 \sum_{j=2}^{n} X_j \). We then have
\[
\mathbb{E}[M_{\text{seq}}] = 2 \frac{n-1}{p} < 2 \frac{n}{p},
\quad (G1)
\]

\[
\mathbb{E}[M_{\text{seq}}] \approx 2n \frac{H(n)-1}{p},
\quad (G2)
\]

where \( M_{\text{par}} \equiv M \) from Eq. (10) and we used the approximation for the parallel scheme derived in App. B assuming \( p \ll 1 \). Even when using the strict inequality for the sequential protocol, we see that it uses less memory time than the parallel protocol when \( H(n) > 2 \), which is the case for \( n \geq 4 \). For \( n = 2 \) the protocols are the same and it can easily be checked that the sequential protocol is also better for \( n = 3 \). 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 disadvantage of a lower raw rate, resulting in a lower overall secret-key rate. The obtainable secret-key rate using this sequential protocol with a memory coherence time of 1000s can be seen in Fig. 7 (the exact expression for the memory dephasing has been used here). Note that for large distances the secret-key rate drops much more slowly to zero for the sequential protocol (see Fig. 7) than for the parallel one (see Fig. 5).

**FIG. 7.** (Color online) Secret-key rate for a repeater with \( n=2 \) (red), 3 (green), 4 (blue) segments using a sequential protocol \((\alpha = 23.9\) in all cases). The undashed lines show the ideal loss-only case \((p_{\text{det}} = 1)\), while the dashed lines correspond to the case where we additionally considered a finite memory coherence time of 1000 seconds. The benchmarks PLOB, \( \sqrt{\eta_{\text{tot}}} \), \( \sqrt{\eta_{\text{rot}}} \), \( \sqrt{\eta_{\text{rot}}} \) and \( \sqrt{\eta_{\text{rot}}} \) can also be seen. The regions between two of those benchmarks are highlighted in color.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (India, 1984) pp. 175–179.
[18] H.-K. Lo, M. Curty, and K. Tamaki, Nature Photonics 13, 334 (2019).

[19] 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, “Surpassing the rate-transmittance linear bound of quantum key distribution,” (2019), arXiv:1908.01271.

[20] F. Rozpeďek, R. Yehia, K. Goodenough, M. Ruf, P. C. Humphreys, R. Hanson, S. Wehner, and D. Elkouss, Phys. Rev. A 99, 052330 (2019).

[21] F. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, Phys. Rev. Lett. 96, 240501 (2006).

[22] N. K. Bernardes and F. van Loock, Phys. Rev. A 86, 052301 (2012).

[23] P. van Loock, N. Lütkenhaus, W. J. Munro, and K. Nemoto, Phys. Rev. A 78, 062319 (2008).

[24] E. Schrödinger, Naturwissenschaften 23, 807 (1935).

[25] S. Haroche, Rev. Mod. Phys. 85, 1083 (2013).

[26] P. C. Haljan, K.-A. Brickman, L. Deslauriers, P. J. Lee, and C. Monroe, Phys. Rev. Lett. 94, 153602 (2005).

[27] J.-Q. Liao, Y. Guo, H.-S. Zeng, and L.-M. Kuang, Journal of Physics B: Atomic, Molecular and Optical Physics 39, 4709 (2006).

[28] S. A. Aljunid, M. K. Tey, B. Chng, T. Liew, G. Maslenikov, V. Scarani, and C. Kurtsiefer, Phys. Rev. Lett. 103, 153601 (2009).

[29] M. Fischer, B. Srivathsan, L. Alber, M. Weber, M. Sondermann, and G. Leuchs, Applied Physics B 123, 48 (2017).

[30] C. Gerry and P. Knight, Introductory Quantum Optics (Cambridge University Press, 2004) pp. 308-311.

[31] B. Hacker, S. Welte, S. Daiss, A. Shaukat, S. Ritter, L. Li, and G. Rempe, Nature Photonics 13, 110 (2019).

[32] The difference in the protocol between [20] and our work is that the authors of [20] use two on/off detectors, such that their raw rate is larger by a factor of two. 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 [20] considers the ‘Devetak-Winter formula’ for obtaining the secret-key fraction by calculating the mutual information between Alice’s and Bob’s keys and estimating the mutual information between Eve and the key via the Holevo information. This approach allows the authors of [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.

[33] 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,” (2019), arXiv:1909.01323.

[34] M.-J. Li, H. Chen, Y.-A. Chen, Q. Zhang, C.-Z. Peng, X. Ma, T.-Y. Chen, and J.-W. Pan, “Quantum cryptography with realistic devices,” (2019), arXiv:1903.09051.

[35] 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, “Surpassing the rate-transmittance linear bound of quantum key distribution,” (2019), arXiv:1908.01271.

[36] F. Rozpeďek, R. Yehia, K. Goodenough, M. Ruf, P. C. Humphreys, R. Hanson, S. Wehner, and D. Elkouss, Phys. Rev. A 99, 052330 (2019).

[37] F. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, Phys. Rev. Lett. 96, 240501 (2006).

[38] N. K. Bernardes and F. van Loock, Phys. Rev. A 86, 052301 (2012).

[39] P. van Loock, N. Lütkenhaus, W. J. Munro, and K. Nemoto, Phys. Rev. A 78, 062319 (2008).

[40] E. Schrödinger, Naturwissenschaften 23, 807 (1935).

[41] S. Haroche, Rev. Mod. Phys. 85, 1083 (2013).

[42] P. C. Haljan, K.-A. Brickman, L. Deslauriers, P. J. Lee, and C. Monroe, Phys. Rev. Lett. 94, 153602 (2005).

[43] J.-Q. Liao, Y. Guo, H.-S. Zeng, and L.-M. Kuang, Journal of Physics B: Atomic, Molecular and Optical Physics 39, 4709 (2006).

[44] S. A. Aljunid, M. K. Tey, B. Chng, T. Liew, G. Maslenikov, V. Scarani, and C. Kurtsiefer, Phys. Rev. Lett. 103, 153601 (2009).

[45] M. Fischer, B. Srivathsan, L. Alber, M. Weber, M. Sondermann, and G. Leuchs, Applied Physics B 123, 48 (2017).

[46] C. Gerry and P. Knight, Introductory Quantum Optics (Cambridge University Press, 2004) pp. 308-311.

[47] B. Hacker, S. Welte, S. Daiss, A. Shaukat, S. Ritter, L. Li, and G. Rempe, Nature Photonics 13, 110 (2019).

[48] The difference in the protocol between [20] and our work with $n = 1$ is that the authors of [20] use $\theta = \frac{\pi}{2}$ and two on/off detectors, such that their raw rate is larger by a factor of two. 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 [20] considers the ‘Devetak-Winter formula’ for obtaining the secret-key fraction by calculating the mutual information between Alice’s and Bob’s keys and estimating the mutual information between Eve and the key via the Holevo information. This approach allows the authors of [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.

[49] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Nature Photonics 13, 334 (2019).
photon or not [59], see also [31]. Another protocol, 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 suggest 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 scaling advantage. The schemes of Refs. [31, 59] do not share this complication, because their resulting spin-spin entanglement is of immediate use.

[46] S. Pirandola, Communications Physics 2, 51 (2019)
[47] However, note that if we assumed probabilistic entanglement swapping instead of a deterministic one, swapping as soon as possible would yield a non-optimal raw rate, because one does not want to perform many entanglement swapping operations between entangled pairs of long and short distance since if the operation fails all involved segments have to start from scratch.

[48] S. Santra, L. Jiang, and V. S. Malinovsky, Quantum Science and Technology 4, 025010 (2019)
[49] W. Dürr and H. J. Briegel, Reports on Progress in Physics 70, 1381 (2007)
[50] G. Bowen and S. Bose, Phys. Rev. Lett. 87, 267901 (2001)

[51] H.-K. Lo, H. Chau, and M. Ardehali, Journal of Cryptology 18, 133 (2005)
[52] Throughout 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 $\sqrt[n]{\eta_{\text{total}}}$ (which up to a factor of 1.4 coincide with the former for small $\sqrt[n]{\eta_{\text{total}}}$), 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 $\sqrt[2n]{\eta_{\text{total}}}$.

[53] F. Rozpędek, K. Goodenough, J. Ribeiro, N. Kalb, V. C. Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D. Elkouss, Quantum Science and Technology 3, 034002 (2018)
[54] O. A. Collins, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy, Phys. Rev. Lett. 98, 060502 (2007)
[55] E. Shchukin, F. Schmidt, and P. van Loock, Phys. Rev. A 100, 032322 (2019)
[56] L. Praxmeyer, “Reposition time in probabilistic imperfect memories,” (2013), arXiv:1309.3407
[57] P. Kok and B. W. Lovett, Introduction to Optical Quantum Information Processing (Cambridge University Press, 2010).
[58] J. Dehaene, M. Van den Nest, B. De Moor, and F. Verstraete, Phys. Rev. A 67, 022310 (2003)
[59] C. Cabrillo, J. I. Cirac, P. García-Fernández, and P. Zoller, Phys. Rev. A 59, 1025 (1999)