Overcoming lossy channel bounds using a single quantum repeater node

D. Luong[1] · L. Jiang[2] · J. Kim[3] · N. Lütkenhaus[1]

Abstract We propose a scheme for performing quantum key distribution (QKD) which has the potential to beat schemes based on the direct transmission of photons between the communicating parties. In our proposal, the communicating parties exchange photons with two quantum memories placed between them. This is a very simple quantum repeater scheme and can be implemented with currently available technology. Ideally, its secret key rate scales as the square root of the transmittivity of the optical channel, which is superior to QKD schemes based on direct transmission because key rates for the latter scale at best linearly with transmittivity. Taking into account various imperfections in each component of our setup, we present parameter regimes in which our protocol outperforms protocols based on direct transmission.

1 Introduction

One of the outstanding problems of quantum key distribution (QKD) is the question of how to distribute key over

✉ D. Luong
dluong@uwaterloo.ca

1 Department of Physics and Astronomy and Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada

2 Department of Applied Physics, Yale University, New Haven, CT 06511, USA

3 Electrical and Computer Engineering Department, Duke University, Durham, NC 27708, USA

arbitrarily long distances. The transmittivity of an optical channel decreases rapidly as the length of the channel grows (exponentially, in the case of fiber). This imposes a strong limit on the secret key rate achievable when photons are directly transmitted from Alice to Bob over long distances. Takeoka, Guha, and Wilde have shown that, when multi-mode signals are sent through a pure-loss bosonic channel with transmittivity η_{ch}, the secret key rate can be no greater than $\log_2[(1 + \eta_{ch})/(1 - \eta_{ch})]$ bits per mode per channel use [1]. This is proportional to η_{ch} for small η_{ch}, meaning that the key rate, too, decreases rapidly with distance. In order to improve this scaling behavior and achieve even a modest key rate at very long distances, it is necessary to look beyond direct transmission.

One way to surpass the Takeoka–Guha–Wilde (TGW) bound is by using quantum repeaters [2]. First described in [3], these are auxiliary quantum devices placed along the channel between the communicating parties, effectively breaking it up into multiple low-loss channels. A full repeater scheme might involve the use of many stations, each containing multiple qubits [3–11]. These resource requirements are too demanding for such a scheme to be practical at present. Conceptually, then, quantum repeaters represent a path to transcending the limit imposed by the TGW bound, but their implementation remains a subject of intense research. No experiment has been performed that beats the TGW bound over any distance.

In this paper, we propose a simplified scheme which has the potential to beat the TGW bound. Two parties perform QKD by measuring photons sent from a central station containing two quantum memories (Fig. 1). If the station is placed midway between the parties, each photon need only travel half the distance between them. Moreover, the presence of the memories means that the probability of one party successfully measuring a photon is independent
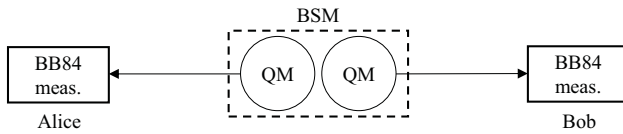
Fig. 1 Schematic of the proposed protocol. One QM sends entangled photons to Alice, the other to Bob. Once both parties successfully measure photons using BB84 measurements, a Bell measurement (BSM) is performed on the QMs

of the success of the other party. Together, these imply that the secret key rate for our protocol is expected to scale as $\sqrt{\eta_{ch}}$. Such scaling would be a fundamental improvement over any scheme relying on direct transmission, and gives it the potential to surpass the TGW bound. Our paper explores whether this scheme can beat the TGW bound in practice, taking into account experimental imperfections such as memory dephasing (whose effect on quantum repeaters was studied in, e.g., [12]).

The protocol is basically a rudimentary quantum repeater scheme, but it can be implemented using currently available technology. Though not directly scalable, it represents a step toward the full implementation of quantum repeaters. It is similar in spirit to the protocol described in [13], except that in their proposal single photons or weak laser pulses are sent *toward* the central station instead of being emitted *from* the QMs. Our protocol thus simplifies the experimental requirements.

The remainder of this paper is organized as follows. Section 2 describes our proposed protocol, and Sect. 3 lists the benchmarks we will compare it to. Section 4 describes how we mathematically model each component in our protocol; these models are assembled in Sect. 5 to produce an expression for the secret key rate of our protocol. In Sect. 6, we discuss the behavior of the key rate of our protocol as a function of the distance between the communicating parties. We also discuss variations of our protocol and describe the parameter regimes required to beat the benchmarks listed in Sect. 3. In particular, we show that beating the TGW bound is within reach. Finally, we present some concluding remarks in Sect. 7.

2 Description of the protocol

The protocol we propose in this paper is illustrated in Fig. 1. It uses two quantum memories (QMs) in a central station placed between Alice and Bob, who wish to establish a secret key via QKD. We do not assume a particular implementation of the QMs, but we do require that each QM can be entangled with a single photon (as in, for example, ion–photon entanglement [14] or the DLCZ scheme [4]). The photonic degree of freedom

used to encode qubits can be freely chosen; examples include polarization or time-bin encoding. We further assume that the two QMs can be jointly measured in the Bell basis, either by applying a CNOT gate and directly measuring them or by mapping the memory states onto photons and performing an optical Bell measurement. Alice and Bob are connected to the central station by lossy optical channels, and each have measurement apparatuses that allow them to measure incoming photons in one of two settings which correspond to mutually unbiased bases of the qubit subspace (as in BB84). We will call the bases X and Z.

The procedure to produce one bit of raw key is as follows:

1. An entangled memory-photon state is prepared in one of the QMs and the photon sent to Alice, who performs a BB84 measurement on the photon. This is repeated until she successfully detects a photon.
2. Same as the previous step, but with Bob and the other QM.
3. A Bell measurement is performed on the two QMs and the result announced to Bob.
4. If Bob measured in the Z basis, he applies a bit flip to his BB84 measurement if the Bell measurement yielded $|\Psi^+\rangle$ or $|\Psi^-\rangle$. Similarly, if he measured in the X basis, he applies a bit flip if the Bell measurement yielded $|\Phi^-\rangle$ or $|\Psi^-\rangle$.

This procedure is repeated until a sufficient amount of raw key is obtained. The rest of the protocol is the same as in efficient BB84 [15].

The protocol described here admits of a few variations: the QMs could either be *concurrently* or *sequentially loaded* by performing steps 1 and 2 either at the same time or in sequence, and the position of the central station can be changed. In Sect. 6, we will explore the difference between con and sequential loading as well as the effect of changing the position of the central station.

3 Benchmarks

In comparing our protocol to schemes based on the direct transmission of photons from Alice to Bob, the TGW bound [1] is the most stringent standard of comparison. We will, however, compare our protocol to other scenarios as well; this will make it easier to see how well it matches up to concrete schemes that can be performed in a lab. The direct transmission benchmarks with which we will compare our protocol are as follows:

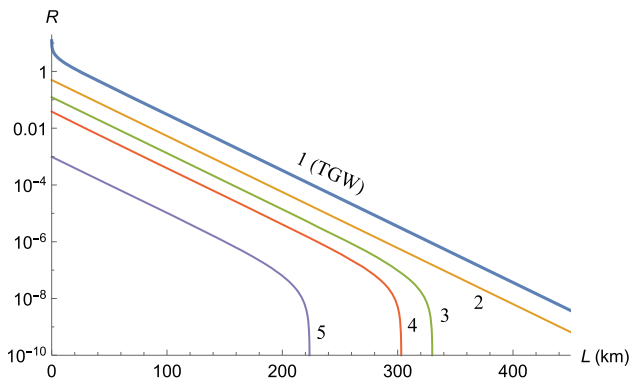1. The TGW bound on the secret key rate per mode,

Fig. 2 Key rate per channel use per mode versus distance for the benchmarks listed in Sect. 3. The thick curve corresponds to the TGW bound (benchmark 1). Parameter values are as given in Sect. 6

$$R_{\mathrm{TGW}} = \log_2\left(\frac{1 + \eta_{\mathrm{ch}}}{1 - \eta_{\mathrm{ch}}}\right), \qquad (1)$$

where η_{ch} is the channel transmittivity. For small η_{ch}, this reduces to $R_{\mathrm{TGW}} \approx (2/\ln 2)\eta_{\mathrm{ch}} \approx 2.89\eta_{\mathrm{ch}}$.

2. BB84 with an ideal single-photon source and an ideal detector setup (no errors and no losses other than channel loss).
3. BB84 with an ideal single-photon source and a realistic detector setup (nonzero misalignment error and dark counts, imperfect detector efficiency).
4. Decoy-state BB84 with a laser and a realistic detector setup.
5. BB84 using a quantum memory as a single-photon source and a realistic detector setup.

Throughout this paper, we will use the efficient variant of BB84 in which the Z basis is measured much more frequently than the X basis [15].

The figure of merit to be considered is the key rate *per mode*. Because BB84 requires two optical modes when implemented with the usual polarization or time-bin encoding, its key rate expression takes on a factor of 1/2. We may compare the key rate per mode of our protocol to those of the benchmarks above either on a per time unit or a per channel use basis. In this paper we will compare key rates per channel use only, though the ultimate goal is of course to compete on a per time unit basis. Any reference to "key rates" in the remainder of this paper, then, should be taken to mean "key rates per mode per channel use." Expressions for the key rates of benchmarks 2–5 are given in Appendix 1.

Figure 2 shows plots of key rate per channel use as a function of the distance between Alice and Bob. Note that all of these benchmarks are proportional to η_{ch} (within certain limits, depending on the benchmark).

4 Component modeling

In this section, we present a simple model of the behavior of each component in the setup described in Sect. 2 in the absence of eavesdropping.

4.1 Quantum memories

In this paper, we consider QMs that are adequately described by the following model. A photon-memory entangled state can be generated in a QM with probability η_p; each attempt to do so requires a preparation time of T_p. When a photon is successfully generated, it is *maximally entangled* with the QM; without loss of generality, we may take the initial memory-photon state to be the Bell state $\left|\Phi^+\right\rangle$.

The memory-channel photon coupling efficiency is η_c. This includes not only the probability of a photon entering the optical channel, but the success probability of any process that occurs between the memory and the channel. For example, it contains the probability of successfully performing a wavelength conversion (if such is necessary).

The QM dephasing time is T_2. We will model dephasing using the following map [8], which takes as input the initial state ρ of the QM and returns the state of the QM after it has dephased for time t:

$$\Gamma_t(\rho) := [1 - \lambda_{\mathrm{dp}}(t)]\rho + \lambda_{\mathrm{dp}}(t)Z\rho Z \qquad (2)$$

where

$$\lambda_{\mathrm{dp}}(t) := \frac{1 - e^{-t/T_2}}{2} \qquad (3)$$

and Z is the Pauli Z operator. In this model, the off-diagonal elements of ρ go to zero as $t \to \infty$.

4.2 Channels

Alice and Bob are connected to the central station by optical channels of lengths L_A and L_B, respectively; the length of the total channel is therefore $L = L_A + L_B$. The speed of light through these channels is c. The transmittivity of a channel of length l is

$$\eta_{\mathrm{ch}}(l) = e^{-l/L_{\mathrm{att}}} \qquad (4)$$

where L_{att} is the attenuation length.

The probability of error due to setup misalignment between Alice and the central station is e_{mA}. Setup misalignment rotates the qubit state of the photon; if we assume the rotation angle to be random and symmetrically distributed about 0, the initial memory-photon state $\left|\Phi^+\right\rangle$ becomes

$$(1 - e_{mA})\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + e_{mA}\left|\Psi^-\right\rangle\left\langle\Psi^-\right| \qquad (5)$$

when the photon reaches a detector. This holds for Bob as well, with misalignment error e_{mB}.

4.3 Detectors

For their BB84 measurements, Alice and Bob each use a detector setup consisting of an optical element that can distinguish photonic qubit states in the X and Z bases (such as a polarizing beam splitter for polarization qubits) and two threshold detectors. We assume that they actively choose the basis in which to measure. Each detector has a dark count probability of p_d; each setup has efficiency η_d.

If a photon heading toward one of the setups is in the state ρ, the effect of dark counts can be mimicked by photons which are effectively in the modified state

$$\alpha(\eta)\rho + [1 - \alpha(\eta)]\frac{\mathbb{1}}{2}, \tag{6}$$

where

$$\alpha(\eta) := \frac{\eta(1 - p_d)}{1 - (1 - \eta)(1 - p_d)^2} \tag{7}$$

and η is the probability that the photon reaches the detector setup. This assumes the use of a squashing map [16] which randomly assigns a measurement outcome to events in which both detectors click, reflected by ρ being mapped into the maximally mixed state.

4.4 Bell state measurement

The probability of successfully performing a Bell state measurement (BSM) on the two QMs is p_{BSM}.

We model errors in the BSM by applying the depolarizing channel

$$\Delta_{\lambda_{BSM}}(\rho) = \lambda_{BSM}\rho + (1 - \lambda_{BSM})\frac{\mathbb{1}}{4} \tag{8}$$

to the QMs before a perfect BSM. The parameter λ_{BSM} indicates how close the actual BSM is to an ideal BSM. When ρ is pure, λ_{BSM} is related to the fidelity by

$$F_{BSM} = \sqrt{\frac{3\lambda_{BSM} + 1}{4}}. \tag{9}$$

Because the fidelity is jointly concave, this is the minimum fidelity with which a BSM can be achieved.

5 Key rate analysis

The secret key rate is lower bounded by [15, 17]

$$R = \frac{Y}{2}[1 - h(e_X) - fh(e_Z)]. \tag{10}$$

Here, the yield Y is the probability per channel use that Alice and Bob's measurements, as well as the BSM, were successful. $h(e)$ is the binary entropy function, e_X and e_Z are the quantum bit error rates (QBERs) between Alice and Bob in the X and Z bases, and f is the error correction inefficiency. The factor of $1/2$ comes from the fact that our protocol requires the use of two optical modes.

Because the total channel between Alice and Bob is divided in two by the central station and because the number of signals sent over each segment of the channel may in general be different, it is not immediately clear how to count channel uses. To be conservative, we define the number of channel uses required to produce one bit of raw key to be the *greater* of the number of times Alice or Bob used their segments of the channel during the production of that bit. (Note that this is not the *sum* of the number of times Alice and Bob used their segments of the channel, even in the case of sequential loading.)

5.1 Yield

The probability that a photon emitted from the central station is detected by Alice is

$$\eta_A := \eta_{tot}e^{-L_A/L_{att}}. \tag{11}$$

where we have defined

$$\eta_{tot} := \eta_p\eta_c\eta_d. \tag{12}$$

Due to the effect of dark counts, the probability that her detector clicks is

$$\eta_A' := 1 - (1 - \eta_A)(1 - p_d)^2. \tag{13}$$

Let N_A denote the number of photons that need to be sent to Alice so that her detector clicks once; it is a geometrically distributed random variable with success probability η_A'. Expressions similar to the above apply for Bob.

The average number of channel uses required for both Alice and Bob's detectors to click is $\mathbb{E}[\max(N_A, N_B)]$ where $\mathbb{E}$ is the expected value operator. The yield is therefore

$$Y = \frac{p_{BSM}}{\mathbb{E}[\max(N_A, N_B)]}$$
$$= p_{BSM}\left(\frac{1}{\eta_A'} + \frac{1}{\eta_B'} - \frac{1}{\eta_A' + \eta_B' - \eta_A'\eta_B'}\right)^{-1}. \tag{14}$$

The expectation value was evaluated in [13].

5.2 Quantum bit error rates

Taking into account all the parameters listed in Sect. 4, we find (in the absence of eavesdropping) that

$$e_X = \lambda_{\text{BSM}} \alpha(\eta_A) \alpha(\eta_B) [\varepsilon_m (1 - \varepsilon_{\text{dp}}) + (1 - \varepsilon_m) \varepsilon_{\text{dp}}]$$
$$+ \frac{1}{2} [1 - \lambda_{\text{BSM}} \alpha(\eta_A) \alpha(\eta_B)] \tag{15}$$

$$e_Z = \lambda_{\text{BSM}} \alpha(\eta_A) \alpha(\eta_B) \varepsilon_m + \frac{1}{2} [1 - \lambda_{\text{BSM}} \alpha(\eta_A) \alpha(\eta_B)] \tag{16}$$

where

$$\varepsilon_m = e_{mA} (1 - e_{mB}) + (1 - e_{mA}) e_{mB} \tag{17}$$

$$\varepsilon_{\text{dp}} = \mathbb{E}\big[\lambda_{\text{dp}}(t_A)[1 - \lambda_{\text{dp}}(t_B)] + [1 - \lambda_{\text{dp}}(t_A)]\lambda_{\text{dp}}(t_B)\big]. \tag{18}$$

We may interpret ε_m and ε_{dp} as the total misalignment and dephasing errors, respectively, between Alice and Bob. Here t_A and t_B are the times that Alice and Bob's QMs are left to dephase for.

At this point, we have fully determined e_Z in terms of the parameters set out in Sect. 4. In order to evaluate e_X, we need only two more quantities: the dephasing time intervals t_A and t_B. These are the subject of the following subsection.

5.2.1 Dephasing

Each time a QM emits a photon toward Alice, she must signal whether or not she successfully measured her photon before the QM prepares another one. This constrains the amount of time that elapses between photons to be at least

$$\tau_A = T_p + \frac{2L_A}{c}. \tag{19}$$

Similar remarks apply to Bob.

If it happens that $L_A \neq L_B$, then (19) allows the QMs to run at different rates. Throughout this paper, we will assume that each QM runs at the maximum rate allowed by (19). It is possible to choose the rates to be the same, but we will not do so in this paper.

For both sequential and con loading, we may assume without loss of generality that Bob signals a successful measurement later than Alice does. The BSM is performed as soon as he does, so the QM that sends him photons dephases for a time

$$t_B = \frac{2L_B}{c}. \tag{20}$$

The QM that sends photons to Alice dephases for a longer period of time because it must wait for Bob to make a successful measurement. If the QMs are sequentially loaded, Alice's QM dephases for

$$t_A^{\text{seq}} = N_B \tau_B + \frac{2L_A}{c}. \tag{21}$$

If they are loaded concurrently, then it dephases for

$$t_A^{\text{con}} = |N_B - N_A| \tau_B + \frac{2L_A}{c}. \tag{22}$$

In (18), because of the linearity of the operator $\mathbb{E}$, we need only evaluate $\mathbb{E}[e^{-t_A/T_2}]$. For sequential loading,

$$\mathbb{E}\left[e^{-t_A^{\text{seq}}/T_2}\right] = \frac{\eta_B' \exp\left(-\frac{2L_A}{cT_2}\right)}{e^{\tau_B/T_2} + \eta_B' - 1}. \tag{23}$$

For con loading, a result from [13] gives

$$\mathbb{E}\left[e^{-t_A^{\text{con}}/T_2}\right] = \frac{\eta_A' \eta_B' \exp\left(-\frac{2L_A}{cT_2}\right)}{\eta_A' + \eta_B' - \eta_A' \eta_B'} \left[\frac{1}{1 - e^{-\tau_B/T_2}(1 - \eta_A')} + \frac{1}{1 - e^{-\tau_B/T_2}(1 - \eta_B')} - 1 \right]. \tag{24}$$

6 Results

Unless otherwise noted, the following parameter values were used for the results in this section. They are plausible values for an implementation of our protocol using trapped-ion quantum memories connected to Alice and Bob via optical fiber. A single ion fluorescence collection efficiency of 4.2 % has been demonstrated in [18], a trapped-ion qubit was measured to have a dephasing time of 2.5 s in [19], and a two-qubit gate was used to entangle two ions with a fidelity of 99.3 % (corresponding to $\lambda_{\text{BSM}} = 0.99$) in [20].

- η_p (preparation efficiency) $= 0.66$
- T_p (preparation time) $= 2\ \mu$s
- η_c (photon-fiber coupling efficiency $\times$ wavelength conversion) $= 0.04 \times 0.3$
- T_2 (dephasing time) $= 1$ s
- c (speed of light in optical fiber) $= 2 \times 10^8$ m/s
- L_{att} (attenuation length) $= 22$ km
- e_{mA} (misalignment error) $= e_{mB} = 0.01$
- p_d (dark count probability per detector) $= 10^{-8}$
- η_d (detector efficiency) $= 0.3$
- p_{BSM} (BSM success probability) $= 1$
- λ_{BSM} (BSM ideality parameter) $= 0.97$
- f (error correction inefficiency) $= 1.16$
- For decoy-state BB84 (benchmark 4), we will set the mean photon number of the signal states equal to 1. For the above numbers, we find that $\eta_{\text{tot}} = \eta_p \eta_c \eta_d = 0.0024$.

6.1 Protocol variations

6.1.1 Simultaneous versus sequential loading

For this comparison, the central station is located halfway between Alice and Bob.
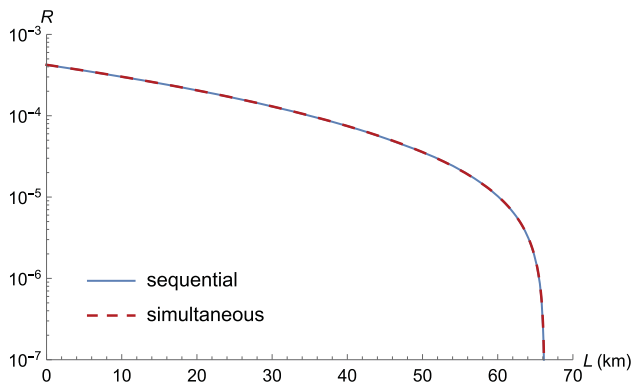
Fig. 3 Key rate per channel use versus distance for con and sequential loading. The two curves are virtually indistinguishable

We have found, for the parameter values given above, that con and sequential loading of QMs in our protocol yield almost indistinguishable key rates per channel use over all values of L for which the rates are nonzero (Fig. 3). A rough comparison of the dephasing time intervals t_A^{seq} and t_A^{con} suggests that this holds whenever $\tau_B/(T_2\eta_{tot})$ is small over all values of L for which the key rates are nonzero. The parameters we have used are within this regime: $\tau_B/(T_2\eta_{tot}) = 0.140$ at $L = 66$ km. Outside of it, however, the difference can be dramatic: there are cases where the key rate is nonzero for con loading but not for sequential loading.

Because we will always be well within the parameter regime where con and sequential loading give nearly the same key rate, we will consider only sequential loading in the remainder of this paper.

6.1.2 Optimization of central station position

When the QMs are sequentially loaded, it need not be true that placing the central station halfway between Alice and Bob will yield the maximum key rate. This is because there is an inherent asymmetry in our protocol in this case: Bob only begins making measurements after Alice has finished hers.

Figure 4 shows the behavior of the key rate (per channel use) as a function of L when the central station is placed at $L / 2$ and when it is placed at the position that maximizes the key rate. For small L, both key rates are approximately the same, and both scale proportionally to $\sqrt{\eta_{ch}} = e^{-L/(2L_{att})}$. When L becomes so large that the dephasing time interval t_A^{seq} is a significant fraction of T_2, the unoptimized key rate drops to zero. (The value of L for which dephasing becomes significant can be quantified using (35) of Appendix 2, which gives a value of 96 km in the case of Fig. 4.) Around that same point, the optimized key rate transitions from $e^{-L/(2L_{att})}$ scaling to $\eta_{ch} = e^{-L/L_{att}}$
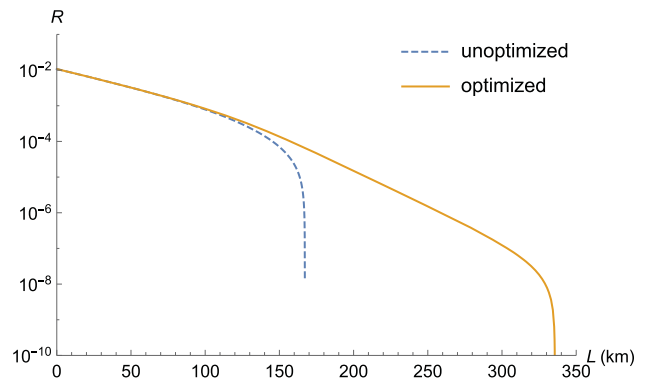

Fig. 4 Key rate versus distance when the central station is at $L / 2$ and when its position is optimized. (We have increased η_c to 0.3 to better show the features of the *curves*.) Near 96 km, the unoptimized key rate begins to drop to 0 and the optimized key rate transitions from $e^{-L/(2L_{att})}$ scaling to $e^{-L/L_{att}}$ scaling
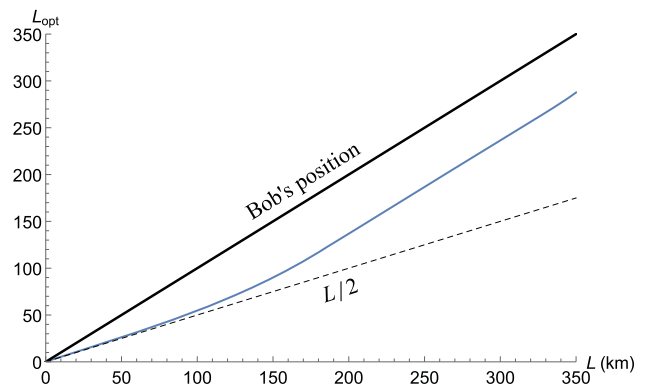

Fig. 5 Optimal central station position as a function of the total distance L. (Alice's position is taken to be at $L = 0$. Again, we have increased η_c to 0.3 to better show the features of the *curves*.) Near where the scaling changes from $e^{-L/(2L_{att})}$ to $e^{-L/L_{att}}$, around $L = 96$ km, the optimal position moves away from $L / 2$ and remains a fixed distance away from Bob

scaling—which is the same as for direct transmission—and continues thus until L is so large that detector dark counts become significant, at which it too drops to zero.

For greater insight into this behavior, consider Fig. 5, which shows the optimal central station position as a fraction of L as L is varied. For lower values of L, the station remains near the middle. Once dephasing becomes significant, the optimal position moves closer to Bob. This keeps dephasing errors low because Bob's link runs quicker, giving Alice's QM less time to dephase. At longer distances, the optimal position is a fixed distance away from Bob, just far enough away that the dephasing in Alice's QM does not overwhelm the system with errors. The price of suppressing dephasing errors in this way is that the key rate scales with the transmittivity of the longer link in the setup, so the key rate scaling is degraded.
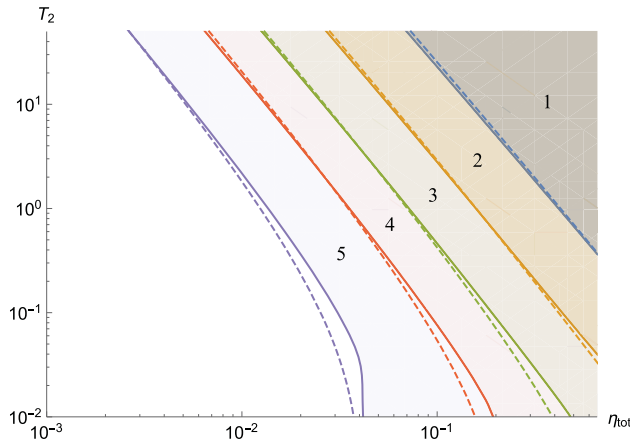
Fig. 6 *Shaded regions* indicate values of η_{tot} and T_2 for which our protocol beats each of the benchmarks listed in Sect. 3. *Dashed lines* indicate approximations to the boundaries of these regions obtained using (25). For benchmark 5 (quantum memory as single-photon source), we have fixed $\eta_c = 0.3 \times 0.3$
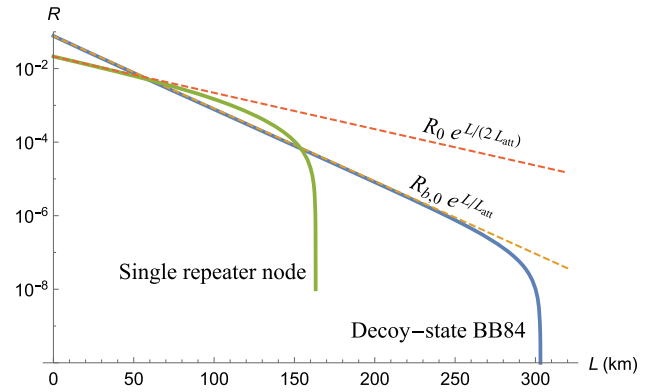

Fig. 7 Approximating the crossover point using the scaling behavior of the key rates. Note that the intersection point of the approximating curves coincides with the crossover point of the key rate curves, and that the intersection occurs before dephasing becomes significant and the key rate of our protocol goes to 0. (We have set $\eta_c = 0.3$.)

6.2 Beating direct transmission

We are now in a position to determine the conditions under which our protocol can beat the direct transmission benchmarks listed in Sect. 3. First, note that at $L = 0$ the performance of our protocol may be worse than that of the benchmarks because the central station introduces additional sources of loss. However, because the key rate for our protocol scales better with distance than the benchmark key rates when L is not too large, *crossover* with one or more of them is possible at some $L > 0$.

When the central station position is optimized, crossover can only occur in the $e^{-L/(2L_{\text{att}})}$ regime (excluding marginal cases)—that is, when the optimal position is near the midpoint between Alice and Bob. Equivalently, crossover can only occur when the unoptimized key rate is nonzero. For this reason, we will fix the central station at $L/2$ for the remainder of this section instead of optimizing its position. It is worth mentioning that crossover with a certain benchmark does not mean that our protocol beats it for *all* L beyond the crossover point; the interval over which our protocol is superior may be quite small. But optimizing the central station position can potentially increase the range of distances over which our protocol beats the benchmark compared to the leaving the station at $L/2$.

We identify two parameters, the combined efficiency η_{tot} and the dephasing time T_2, which are crucial in determining whether crossover occurs with any of the benchmarks and which can be improved from the values given at the beginning of this section. For example, the photon-fiber coupling efficiency in η_c could be pushed from 0.04 to as high as 0.3 [21] (leading to $\eta_{\text{tot}} = 0.0178$), while a T_2 of 50 s has already been demonstrated [22]. Figure 6 shows the regions

in η_{tot}-T_2 space in which we can beat each of the benchmarks. It is clear from the figure that we cannot beat any of the benchmarks with the parameters given at the beginning of the section, and that from our perspective, improving η_{tot} is more likely to result in crossover than improving T_2.

Each region may be explained in the following way. When L is small enough for errors to be negligible, the key rate of our protocol is $R \approx R_0 e^{-L/(2L_{\text{att}})}$ while that of the benchmark of interest is $R_b \approx R_{b,0} e^{-L/L_{\text{att}}}$, where R_0 and $R_{b,0}$ are the key rates at $L = 0$ of our protocol and of the benchmark respectively.[1] These curves intersect at a distance L_{int}. If L_{int} is smaller than some characteristic distance L_{dp} beyond which dephasing becomes significant, then there is a crossover. The boundary of the crossover region corresponds to $L_{\text{int}} = L_{\text{dp}}$. These ideas are illustrated in Fig. 7.

Based on this explanation, we can derive an approximate formula for the boundary of the region in which crossover occurs with a given benchmark with key rate R_b:

$$T_2 = K \left[\frac{Q T_p}{\eta_{\text{tot}}^2} + \frac{2 L_{\text{att}} \ln(Q/\eta_{\text{tot}})}{c} \left(1 + \frac{Q}{\eta_{\text{tot}}^2} \right) \right]. \quad (25)$$

Here

$$Q = \frac{3 R_{b,0}}{2 R_0^{\eta_{\text{tot}}=1}}, \quad (26)$$

$R_0^{\eta_{\text{tot}}=1}$ denotes the key rate of our protocol when $L = 0$ and $\eta_{\text{tot}} = 1$, and K is a fitting parameter characterizing how

---

[1] This does not quite apply to the TGW bound, which goes to infinity as $L \to 0$. In this case, one must continue the $e^{-L/L_{\text{att}}}$ behavior all the way to $L = 0$, so that $R_{b,0} = 2/\ln 2$.

long the QMs must dephase for, as a fraction of T_2, before dephasing becomes significant. It needs to be chosen to fit the exact crossover region boundary; empirically, $K = 14$ gives a good fit. This approximation is valid when $T_p \ll T_2$ and $p_d \ll \eta_{\text{tot}}^2/Q$. A derivation is given in Appendix 2.

The dashed lines in Fig. 6 are the boundary approximations given by (25).

6.2.1 Attenuation length; the high-loss limit

Let us now consider the *high-loss limit*, where the attenuation length L_{att} is very small. This limit is interesting in the context of hybrid quantum-classical networks. In passive optical networks, where multiple users are connected to a source, each user is effectively connected to the source via a high-loss channel. The limit is also applicable when the wavelength of the photons emitted by the QMs happens to be greatly attenuated by the optical channel.

The effect of reducing the attenuation length is to make it easier to beat the benchmarks, as shown in Fig. 8 and predicted in (25). This is because the photons cannot travel as far, so there is less dephasing. However, because of the nonzero preparation time T_p, beating the benchmarks is still nontrivial in the $L_{\text{att}} \to 0$ limit. The high-loss limit thus represents a regime in which experimental requirements are relaxed, yet the benchmarks can still meaningfully be beaten.

Figure 9 shows the effect of changing the preparation time T_p and the dark count probability p_d on the η_{tot}-T_2 regions in which our protocol can beat the TGW bound. As expected from (25), the benchmarks become easier to beat as T_p goes down. (This is true whatever the value of L_{att}.) We also see that when $T_p = 0$ and $L_{\text{att}} \to 0$, they can be beat for any value of T_2. Because there is no dephasing at all in this case, T_2 plays no role in determining whether there is a crossover.

Equation (25) suggests that when $T_p = 0$ and $L_{\text{att}} \to 0$, crossover can happen for any value of η_{tot}. However, Fig. 9 shows that crossover can happen only when η_{tot} is sufficiently large. There is no contradiction: when η_{tot} is too low, the condition $p_d \ll \eta_{\text{tot}}^2/Q$ is violated and (25) no longer holds. It turns out that there is no crossover when η_{tot} is small because dark counts become significant. Using reasoning similar to that employed in deriving (25) (with the characteristic dephasing length L_{dp} replaced with a characteristic dark count length L_d), we can obtain the following approximation to the minimum η_{tot} necessary for our protocol to beat a given benchmark:

$$\eta_{\text{tot}}^{\min} = \sqrt{\frac{Q p_d (2 - p_d)(1 - \xi)}{(1 - p_d)(p_d + \xi - p_d \xi)}}. \tag{27}$$
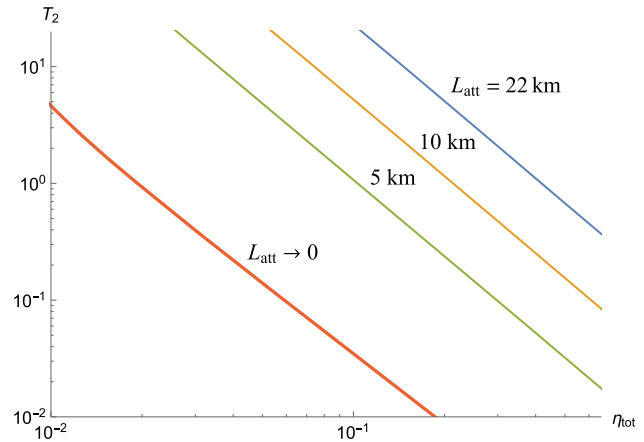
Fig. 8 Boundaries of regions in η_{tot}-T_2 space where our protocol beats the TGW bound for various attenuation lengths
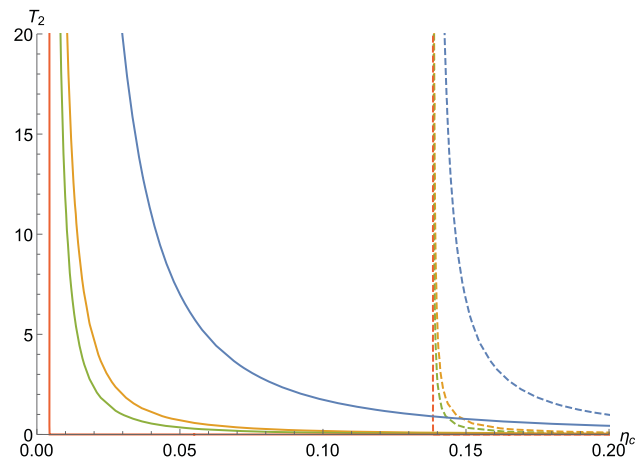

Fig. 9 Boundaries of regions in η_{tot}-T_2 space where our protocol beats the TGW bound in the limit $L_{\text{att}} \to 0$. Solid lines indicate $p_d = 10^{-8}$, dashed lines $p_d = 10^{-5}$. Blue, orange, green, and red lines indicate $T_p = 100, 10, 5,$ and $0\ \mu s$ respectively

The quotient of key rates at zero distance, Q, is as defined in (26), and depends on the choice of benchmark. The fitting parameter ξ is a measure of how much error due to dark counts our system can tolerate before the key rate drops to zero. For the parameter values given at the beginning of the section, $\xi = 0.012$ fits well. This equation is valid when $T_p \ll T_2$ and $p_d \ll \eta_{\text{tot}}$. The derivation is in Appendix 2.

7 Conclusion

In this paper, we have analyzed a QKD protocol in which Alice and Bob exchange signals with a central station consisting of two quantum memories: a rudimentary quantum repeater node. We have also introduced a number of

benchmarks to which our protocol can be compared, the most important of them being the Takeoka–Guha–Wilde bound on the secret key rate. We showed that our protocol can, in principle, beat the benchmarks because of its improved rate-versus-distance scaling: the key rate of all protocols relying on direct transmission between Alice and Bob scales at best with $e^{-L/L_{att}}$, while our protocol scales ideally as $e^{-L/(2L_{att})}$. In effect, our protocol doubles the attenuation length when imperfections, particularly memory dephasing, are not too prominent. Finally, we explored the conditions under which we can beat the benchmarks in practice.

Because our protocol uses only one intermediate station with only two memories, we do not obtain the full scalability that quantum repeaters can offer us in theory. However, because it is so simple, it is feasible to implement using currently available technology while still exhibiting the rate improvement of a full quantum repeater scheme and the ability to beat the TGW bound. Beating the bound, or even demonstrating an improvement over the standard $e^{-L/L_{att}}$ key rate scaling, would be a fundamental experimental achievement. We have shown that these achievements are within reach, particularly in the high-loss limit. And we have shown what physical parameters need to be reached in order to attain these goals. In sum, our analysis helps point the way toward an experimental implementation of quantum repeaters.

Appendix 1: benchmark key rates

In this appendix, we give expressions for the secret key rates of benchmarks 2–5 in Sect. 3. For this purpose we model the observables in an experimental demonstration operating normally—that is, in the absence of eavesdropping activity.

For benchmarks 2, 3, and 5, Alice transmits single photons to Bob. In this case the efficient BB84 key rate per mode is lower bounded by [15, 17]

$$R = \frac{Y_1}{2}[1 - h(e_1) - fh(e_1)] \tag{28}$$

where

$$\eta := \eta_{tot}e^{-L/L_{att}}$$
$$Y_1 := 1 - (1 - \eta)(1 - p_d)^2 \tag{29}$$
$$e_1 Y_1 := Y_1/2 - (1/2 - e_m)\eta(1 - p_d).$$

Here Y_1 and e_1 are the yield and QBER for single photons, f is the error correction inefficiency, L is the length of the optical channel between Alice and Bob, and e_m is the setup misalignment error probability. The other variables are as defined in Sect. 4. The factor of 1/2 comes from the fact that BB84 uses two optical modes.

For an ideal single-photon source (benchmark 3), $\eta_p = \eta_c = 1$. For an ideal detector setup (benchmark 2), $\eta_d = 1$ and $p_d = e_m = 0$. This amounts to setting $e_1 = 0$ and results in $R = e^{-L/L_{att}}/2 = \eta_{ch}/2$.

The key rate for decoy-state BB84 with a laser (benchmark 4) is [23]

$$R_{decoy} = \frac{1}{2}\left(Q_1[1 - h(e_1)] - fQ_\mu h(E_\mu)\right) \tag{30}$$

where

$$Q_1 := Y_1\mu e^{-\mu}$$
$$Q_\mu := 1 - e^{-\eta\mu}(1 - p_d)^2 \tag{31}$$
$$E_\mu Q_\mu := Q_\mu/2 - (1/2 - e_m)(1 - e^{-\eta\mu})(1 - p_d).$$

Here μ is the average photon number for signal states; Y_1, e_1, f, and e_m are as defined above.

Appendix 2: approximation of crossover regions in η_{tot}-T_2 space

Throughout this appendix, we will assume that the QMs are loaded sequentially and that the central station is at $L / 2$. Let R_b be the key rate for the benchmark whose crossover region we wish to approximate.

We will first derive (25). As outlined in the discussion leading up to that equation, our approach is to equate the intersection of the curves $R_0 e^{-L/(2L_{att})}$ and $R_{b,0}e^{-L/L_{att}}$ with some characteristic dephasing length L_{dp} in order to find the boundary of the crossover region. (R_0 and $R_{b,0}$ are the key rates at $L = 0$ of our protocol and of the benchmark, respectively.)

The first step is to find conditions under which

$$R_0 \propto \eta_{tot}R_0^{\eta_{tot}=1}. \tag{32}$$

If p_d is small and $T_p \ll T_2$, then e_X and e_Z are approximately independent of η_{tot}—see (7) and (23)—and R_0 only depends on η_{tot} through Y. If we further assume that $\eta'_A \approx \eta_A$, then

$$Y = p_{BSM}\frac{\eta_{tot}(2 - \eta_{tot})}{3 - 2\eta_{tot}} \approx \frac{2}{3}p_{BSM}\eta_{tot}. \tag{33}$$

to first order in η_{tot}. These conditions are therefore sufficient for the approximation in (32) to hold, with proportionality constant 2/3.

Given this fact, the intersection of the two curves is at

$$L_{\text{int}} = 2L_{\text{att}} \ln\left(\frac{Q}{\eta_{\text{tot}}}\right) \tag{34}$$

where Q is defined in (26). Note that $T_p \ll T_2$ implies that Q is independent of T_2.

We now derive a characteristic dephasing length by determining the distance at which Alice's QM dephases for a significant fraction of T_2. (Recall that Alice's QM always dephases longer than Bob's.) That is, we put

$$\frac{T_2}{K} = \mathbb{E}(t_A^{\text{seq}}) = \frac{L_{\text{dp}}}{c} + \frac{T_p + L_{\text{dp}}/c}{\eta_{\text{tot}} e^{-L_{\text{dp}}/(2L_{\text{att}})}} \tag{35}$$

where we have again used $\eta_A' \approx \eta_A$. The fitting parameter K determines the amount of time T_2/K that the QMs can dephase for before dephasing errors become significant. It was found in Sect. 6.2 that $K = 14$ fits well.

Equation (35) cannot be solved for the dephasing length L_{dp} using elementary functions, but this is unnecessary: to find the crossover boundary, we need only substitute L_{int} for L_{dp}. After a minor rearrangement of terms, this yields (25).

It may appear that a small p_d implies that $\eta_A' \approx \eta_A$. It is true that $p_d \ll 1$ implies $|\eta_A' - \eta_A| \ll 1$, but since $\eta_A \ll 1$ and $\eta_A' \ll 1$ in general, this is not strong enough to meaningfully say that $\eta_A' \approx \eta_A$. We require instead that $|\eta_A' - \eta_A|/\eta_A \ll 1$. Moreover, because we have used $\eta_A' \approx \eta_A$ in deriving (35), we require this to hold for all L up to L_{dp}—or, equivalently, up to L_{int}. By manipulating (13), we can write

$$\frac{|\eta_A' - \eta_A|}{\eta_A} = \left(\frac{1}{\eta_A} - 1\right)(2p_d - p_d^2) \approx \left(\frac{1}{\eta_A} - 1\right)p_d. \tag{36}$$

If η_A is close to 1, then $(1/\eta_A - 1)p_d$ is already small and the approximation holds. If $\eta_A \ll 1$, then $(1/\eta_A - 1)p_d \approx p_d/\eta_A$, which is small for all L up to L_{int} when $p_d \ll \eta_{\text{tot}}^2/Q$. This condition, then, together with $T_p \ll T_2$, guarantees the validity of (25).

Let us now derive (27). This time, we will compare L_{int} with a length L_d at which errors due to dark counts become significant.

The error due to dark counts is related to $\alpha(\eta_A)$, defined in (13). We will put $1 - \xi = \alpha(\eta_A)$ where ξ is a parameter indicating the amount of error the system can tolerate due to dark counts. Rearranging this equation, we obtain

$$L_d = 2L_{\text{att}} \ln\left(\frac{\eta_{\text{tot}}(1 - p_d)(p_d + \xi - p_d\xi)}{p_d(2 - p_d)(1 - \xi)}\right). \tag{37}$$

By equating L_d and L_{int}, we obtain (27).

In deriving this equation, we have made no assumptions beyond those required for (32). In particular, we do not require $\eta_A' \approx \eta_A$ for all L up to L_{int}, but only at $L = 0$. This means that the condition on p_d is less strict: $p_d \ll \eta_{\text{tot}}$.

Finally, we note that the condition $p_d \ll \eta_{\text{tot}}^2/Q$, required for (25), can be obtained from a linearization of the square of (27).

References

1. M. Takeoka, S. Guha, M.M. Wilde, IEEE Trans. Inf. Theory **60**, 4987 (2014)
2. S. Guha *et al.*, Rate-loss analysis of an efficient quantum repeater architecture (2014). arXiv:1404.7183
3. H.J. Briegel, W. Dür, J.I. Cirac, P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998)
4. L.M. Duan, M.D. Lukin, J.I. Cirac, P. Zoller, Nature **414**, 413 (2001)
5. N. Sangouard, C. Simon, H. de Riedmatten, N. Gisin, Rev. Mod. Phys. **83**, 33 (2011)
6. L. Jiang et al., Phys. Rev. A **79**, 032325 (2009)
7. W. Munro, A. Stephens, S. Devitt, K. Harrison, K. Nemoto, Nat. Photonics **6**, 777 (2012)
8. M. Razavi, M. Piani, N. Lütkenhaus, Phys. Rev. A **80**, 032301 (2009)
9. A.G. Fowler et al., Phys. Rev. Lett. **104**, 180503 (2010)
10. R. Van Meter, T. Satoh, T.D. Ladd, W.J. Munro, K. Nemoto, Netw. Sci. **3**, 82 (2013)
11. S. Muralidharan, J. Kim, N. Lütkenhaus, M.D. Lukin, L. Jiang, Phys. Rev. Lett. **112**, 250501 (2014)
12. L. Hartmann, B. Kraus, H.-J. Briegel, W. Dür, Phys. Rev. A **75**, 032310 (2007)
13. C. Panayi, M. Razavi, X. Ma, N. Lütkenhaus, New J. Phys. **16**, 043005 (2014)
14. B. Blinov, D. Moehring, L.-M. Duan, C. Monroe, Nature **428**, 153 (2004)
15. H.K. Lo, F. Chau, M. Ardehali, J. Cryptol. **18**, 133 (2005)
16. N.J. Beaudry, T. Moroder, N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008)
17. V. Scarani et al., Rev. Mod. Phys. **81**, 1301 (2009)
18. E.W. Streed, B.G. Norton, A. Jechow, T.J. Weinhold, D. Kielpinski, Phys. Rev. Lett. **106**, 010502 (2011)
19. S. Olmschenk et al., Phys. Rev. A **76**, 052314 (2007)
20. J. Benhelm, G. Kirchmair, C.F. Roos, R. Blatt, Nat. Phys. **4**, 463 (2008)
21. T. Kim, P. Maunz, J. Kim, Phys. Rev. A **84**, 063423 (2011)
22. T.P. Harty et al., Phys. Rev. Lett. **113**, 220501 (2014)
23. H.-K. Lo, X. Ma, K. Chen, Phys. Rev. Lett. **94**, 230504 (2005)