



UNIVERSITY OF LEEDS

This is a repository copy of *Long-Distance Trust-Free Quantum Key Distribution*.

White Rose Research Online URL for this paper:
<http://eprints.whiterose.ac.uk/85019/>

Version: Accepted Version

Article:

Piparo, NL and Razavi, M (2015) Long-Distance Trust-Free Quantum Key Distribution. IEEE Journal of Selected Topics in Quantum Electronics, 21 (3). 6600508. - . ISSN 1077-260X

<https://doi.org/10.1109/JSTQE.2014.2364129>

Reuse

Unless indicated otherwise, fulltext items are protected by copyright with all rights reserved. The copyright exception in section 29 of the Copyright, Designs and Patents Act 1988 allows the making of a single copy solely for the purpose of non-commercial research or private study within the limits of fair dealing. The publisher or other rights-holder may allow further reproduction and re-use of this version - refer to the White Rose Research Online record for this item. Where records identify the publisher as the copyright holder, users can verify any specific terms of use on the publisher's website.

Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.



eprints@whiterose.ac.uk
<https://eprints.whiterose.ac.uk/>

Long-Distance Trust-Free Quantum Key Distribution

Nicoló Lo Piparo¹ and Mohsen Razavi¹

¹*School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK*

Abstract

The feasibility of *trust-free* long-haul quantum key distribution (QKD) is addressed. We combine measurement-device-independent QKD (MDI-QKD), as an access technology, with a quantum repeater setup, at the core of future quantum communication networks. This will provide a quantum link none of whose intermediary nodes need to be trusted, or, in our terminology, a trust-free QKD link. As the main figure of merit, we calculate the secret key generation rate when a particular probabilistic quantum repeater protocol is in use. We assume the users are equipped with imperfect single photon sources, which can possibly emit two single photons, or laser sources to implement decoy-state techniques. We consider apparatus imperfection, such as quantum efficiency and dark count of photodetectors, path loss of the channel, and writing and reading efficiencies of quantum memories. By optimizing different system parameters, we estimate the maximum distance over which users can share secret keys when a finite number of memories are employed in the repeater setup.

arXiv:1407.8025v3 [quant-ph] 25 Nov 2014

I. INTRODUCTION

Future quantum communications networks will enable secure key exchange among remote users. They ideally rely on user friendly access protocols in conjunction with a reliable network of core nodes [1–3]. For economic reasons, they need to share infrastructure with existing and developing classical optical communication networks, such as passive optical networks (PONs) that enable fiber-to-the-home services [4, 5]. The first generation of quantum key distribution (QKD) networks are anticipated to rely on a *trusted* set of core nodes [6, 7]. This approach, although the only feasible one at the moment, may suffer from security breaches over the long run. In the future generations of quantum networks, this trust requirement can be removed by relying on entanglement in QKD protocols [8, 9]. This can be facilitated via using the recently proposed measurement-device-independent QKD (MDI-QKD) [10–13] at the access nodes of a PON [14] and quantum repeaters at the backbone of the network, as we consider in this paper. The former enables easy access to the network via low-cost optical sources and encoders, whereas the latter may rely on high-end technologies for quantum memories and gates. Both systems, however, rely on entanglement swapping, which makes them naturally merge together. More importantly, in neither systems would we need to trust the intermediary nodes that perform Bell-state measurements (BSMs). In this paper, we study the feasibility of such a *trust-free* hybrid scheme by finding the relationship between the achievable secret key generation rate as a function of various system parameters. We remark that this setup does not provide full device-independence but it removes the trust requirement from the intermediary network nodes that perform measurement operations. Our work provides insights into the feasibility of such systems in the future. The system proposed in [15] combines MDI-QKD with quantum repeaters by using time reversed all photonic quantum repeaters. However, [15] requires single photon sources as well as large cluster states. Instead, our scheme relies on conventional quantum repeaters, where entangled quantum memories are used to store qubits which are teleported to large distances through entanglement swapping. Moreover, users can use imperfect single-photon sources or lasers. MDI-QKD is an attractive candidate for the access part of quantum networks. First, it provides a means to secure key exchange without trusting measurement devices. This is a huge practical advantage considering the range of attacks on the measurement tools of QKD users [16–19]. Moreover, at the users’ ends, it only requires optical encoders

driven by weak laser pulses. That not only makes the required technology for the end users much simpler, but also it implies that the costly parts of the network, including detectors and quantum memories, are now shared between all networks users, and are maintained by service providers. One final advantage of MDI-QKD is its reliance on entanglement swapping, which makes its merging with quantum repeaters, also relying on the same technique, straightforward. This will help us develop quantum networks in several generations, where the compatibility of older, e.g. trusted-node, and newer, e.g., our trust-free, networks can be easily achieved.

Quantum repeaters are the key ingredients to trust-free networks. They traditionally rely on quantum memories (QMs) to store entangled states. In order to avoid the exponential decay of rate with channel length, in quantum repeaters, entanglement is first distributed over shorter distances and stored in QMs. Once we learn about the establishment of this initial entanglement, we can perform BSs to extend entanglement over longer distances [20]. Considering the complexity of joint operations needed for BSs, as well as possible purification thereafter, quantum repeaters are anticipated to be developed in several stages. The first generation of quantum repeaters may rely on probabilistic approaches to BSs, which can be implemented using linear optics devices [21–24]. These systems expect to cover moderately long distances up to around 1000 km without the need for purification. In order to go farther we need to develop efficient tools for purification and deterministic BSs as was initially envisaged in [25]. Such deterministic quantum repeaters will replace the probabilistic setups once their technology is sufficiently mature. Finally, the most advanced class of repeaters are the recently proposed no-memory ones [15, 26, 27], in which, by using extensive error correction, one can literally transfer quantum states from one point to another.

In this paper, we focus on the probabilistic setups for quantum repeaters, and, among all possible options, we use the protocol proposed in [28], which relies on single-photon sources (SPSs). In an earlier work [29], we compared the performance of this protocol, which we refer to as the SPS protocol, in the context of QKD, with several other alternatives, once imperfections in the SPSs are accounted for. We found that under realistic assumptions, this protocol is capable of providing the best (normalized) key rate versus distance behavior as compared to other protocols considered in [29]. The particular setup that we are going to consider in this paper is then a phase-encoded MDI-QKD setup, whose reach and rate are

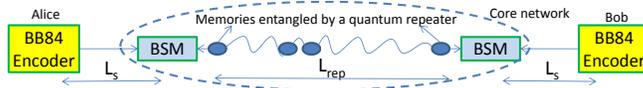


FIG. 1. A general scheme for trust-free QKD links. Entangled states are created between internal nodes of the core network using quantum repeaters. The two BSMs will then enable an end-to-end MDI-QKD protocol.

improved by incorporating a repeater setup, as above, in between the two users. It is worth noting that the easiest way to improve rate-vs-distance behavior is to add two quantum memories in the MDI-QKD setup [30–32]. This approach will almost double the distance one can exchange secret keys without trusting middle nodes, but it is not scalable the same way that quantum repeaters are. It, nevertheless, provides a practical route toward building scalable quantum-repeater-based links.

The paper is structured as follows. In Sec. II, we describe the main ingredients of our setup including the phase encoding MDI-QKD and the SPS-based quantum repeaters. In Sec. III, we present our methodology for calculating the secret key generation rate for our hybrid system, followed by numerical results in Sec. IV. We draw our conclusions in Sec. V.

II. SETUP DESCRIPTION

In this section we first introduce the general idea behind our trust-free architecture and, then, explain particular MDI-QKD and quantum-repeater protocols considered for its implementation. Let us first consider the ideal scenario considered in Fig. 1. In this scheme, by using quantum repeaters, we distribute (polarization) entanglement between two memories apart by a distance L_{rep} . This operation is part of the core network and is facilitated by the service provider. On the users' end, each user is equipped with a BB84 encoder, which sends polarization-encoded single photons to a BSM module at a short distance L_s from its respective source. This resembles the access part of the network, where the BSM module is located at the nearest service point to the user. For each transmitted photon by the users, we need an entangled pair of memories to be read, i.e., their states need to be transferred into single photons. These photons will then interact with the users' photons at the two BSMs in Fig. 1.

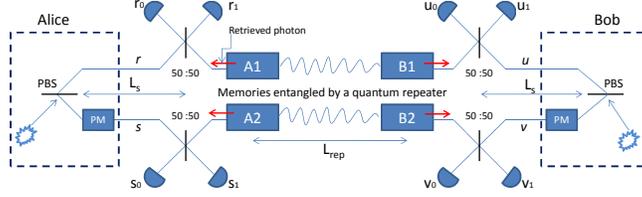


FIG. 2. Schematic diagram for a trust-free QKD link based on phase encoding. Memories are entangled using the SPS repeater protocol. Here, PBS stands for polarizing beam splitter and PM stands for phase modulator.

The setup of Fig. 1 effectively enables an enlarged MDI-QKD scheme. In MDI-QKD, the two photons sent by Alice and Bob are directly interacting at a BSM module [10]. Here, by the use of entangled memories, it is as if the Alice’s photon is being *teleported* to the other side, and will interact with the Bob’s photon at the second BSM. The overall effect is, nevertheless, the same, and once Alice and Bob consider the possible rotations in the memory states corresponding to the obtained BSM results, they can come up with correlated or anti-correlated bits for their sifted keys. Post processing is then performed to convert these sifted keys to secret keys.

The same idea as in Fig. 1 can be implemented via phase-encoding techniques as shown in Fig. 2. Here, for simplicity, we have considered the dual-rail setup. The equivalent, and more practical, single-rail setup can also be achieved by time multiplexing as shown in [11]. In Fig. 2, the quantum repeater ideally leaves memories A_i - B_i , for $i = 1, 2$, in the state $|\psi_{\text{ent}}\rangle_{A_i B_i} = |0\rangle_{A_i}|1\rangle_{B_i} + |1\rangle_{A_i}|0\rangle_{B_i}$, where we have neglected normalization factors, and $|n\rangle_K$ represents n excitations in memory K . The implicit assumption is that the memory is of ensemble type so that it can store multiple excitations [33]. The phase encoding that matches this type of entangled states is as follows. Alice and Bob encode their states either in the z or in the x basis. Alice encodes her bits in the z basis by sending, ideally, a photon in the r or in the s mode. This can be achieved by sending horizontally or vertically polarized pulses to the polarizing beam splitter (PBS) at the encoder. The same holds for Bob and his u and v modes. As for the x basis, we can send a $+45^\circ$ -polarized signal through the PBS to generate a superposition of r (u) and s (v) modes for Alice (Bob) state. Alice (Bob) encodes her (his) bits by choosing the phase value of the phase modulator (PM), ϕ_A (ϕ_B), to be either 0 or π .

Basis	Alice BSM	Bob BSM	Bit assignement
z	type I/II	type I/II	Bob flips his bit
x	type I (II)	type I (II)	Bob keeps his bit
x	type I (II)	type II (I)	Bob flips his bit

TABLE I. Bit assignment protocol depending on the results of the two BSMs.

The BSMs used in the scheme of Fig. 2 are probabilistic ones. They will be successful if exactly two detectors, one from the top branch, and one from the bottom one, click. We recognize two types of detection. For the Alice’s side (and, similarly, for the Bob’s side), type I refers to getting a click on r_0-s_0 or on r_1-s_1 . Type II refers to the case when r_0-s_1 or r_1-s_0 click. In order to get one bit of sifted key, Alice and Bob must use the same basis and both BSMs in Fig. 2 must be successful. Depending on the results of these BSMs and the chosen basis by the two parties, Alice and Bob may end up with correlated or anti-correlated bits, where in the latter case, Bob will flip his bit. Table I summarizes the bit assignment procedure for our scheme. Note that these BSMs can be performed by untrusted parties.

The repetition rate for our scheme is a function of several factors. In order to do a proper BSM, for each photon sent by the users, there must be *two* entangled pairs of memories ready to be read. In principle, the fastest that we can repeat our scheme is the minimum of the maximum source repetition rate, R_S , and half the entanglement generation rate of the quantum repeater, $R_{\text{rep}}/2$. The latter is a function of the number of memories in use [34]. We therefore consider two regimes of operation. If $R_S > R_{\text{rep}}/2$, we then run our encoders at a rate equivalent to $R_{\text{rep}}/2$ and will look at the achievable key rate per QM used. If $R_S < R_{\text{rep}}/2$, i.e., when for every photon sent, there will be more than two entangled pairs ready, then we run our scheme at the rate R_S and will look at the key rate per transmitted pulse as a figure of merit.

In the following, we describe the quantum repeater protocol used in our scheme as well as different types of (imperfect) sources that users may use. Later, we look at the above achievable key rates once certain imperfections are considered in our setup.

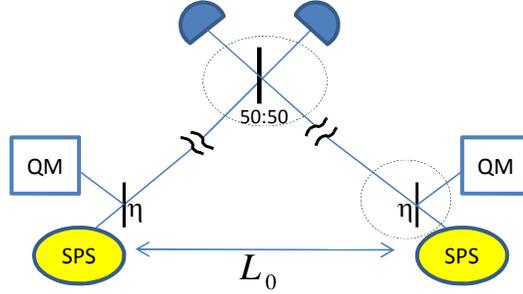


FIG. 3. The SPS protocol for entanglement distribution.

A. Source Imperfections

In our work, we consider two types of sources for the end users. The first type, which we will use as a point of reference for comparison purposes, is an imperfect SPS, with the following output state

$$\rho_j^{(\text{SPS})} = (1 - p) |1\rangle_{jj}\langle 1| + p |2\rangle_{jj}\langle 2|, \quad j = A, B \quad (1)$$

where p is the probability to emit two, rather than one, photons. In practical regimes of operation, $p \ll 1$, hence, in our analysis, we neglect the simultaneous emission of two photons by both sources. The second type of source considered is a phase-randomized coherent source, which will be used in the decoy-state version of the protocol. In this case, Alice (Bob) will send $\mu = |\alpha|^2$ ($\nu = |\beta|^2$) photons on average for her (his) main signal states. Other values will be used for decoy pulses. Our analysis here only considers the case when there are infinitely many decoy states in use, although in practice we expect to achieve the same performance by using just a small number of decoy states [12].

B. SPS Repeater Protocol

The SPS protocol, proposed in [28], attempts to reduce the contribution of multi-photon errors by using single-photon sources. The SPS setup for its initial entanglement distribution is shown in Fig. 3. In order to entangle two QMs at a distance L_0 , corresponding to the shortest segment of the repeater setup, we send single photons through identical beam splitters with transmission coefficients η . The photons can be reflected and stored in the QM or go through the quantum channel and be coupled at a 50:50 beam splitter. If exactly one of the two photodetectors in Fig. 3 clicks, the memories are left in a mixture of an

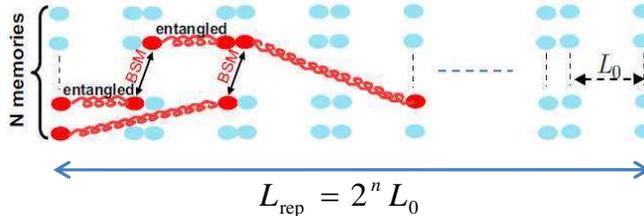


FIG. 4. Multi-memory configuration for quantum repeaters.

entangled state and a spurious vacuum term, where the latter can be selected out in later stages. For the entanglement swapping stage, we again use the 50:50 beam splitter followed by two single-photon detectors to perform a partial BSM. In [29], we calculate the secret key generation rate for the SPS protocol assuming that, instead of perfect SPSs, we are equipped with imperfect sources as in Eq. (1). This is particularly a fundamental source of error, if one uses ensemble-based memories and the partial readout technique for generating single photons [28]. Without loss of generality, we assume ensemble-based QMs with Λ -level configuration and infinite decoherence time. The effect due to a finite decoherence time has been already considered in a previous paper [32]. By considering writing and reading efficiencies for the QMs in use, respectively, denoted by η_w and η_r , here we use the results of [29] to find the relevant density matrices, $\rho_{A_i B_i}$ for $i = 1, 2$, for memories entangled by the SPS protocol for different values of p and for different nesting levels n . Other sources of imperfections considered throughout the paper are the path loss given by $\eta_{\text{ch}}(l) = \exp(-l/L_{\text{att}})$ with L_{att} being the attenuation length of the channel, photodetectors' quantum efficiency, η_d , and photodetectors' dark count per pulse given by d_c .

In order to improve the entanglement generation rates in probabilistic quantum repeaters, it is essential to make use of multiple memories and/or multi-mode memories. Here, we assume a multi-memory structure as shown in Fig. 4 with N memories per node, and employ the cyclic protocol proposed in [20]. In this protocol, at each cycle of duration L_0/c where c the speed of light in the channel, we try to entangle, here using the SPS protocol, all the unentangled pairs of QMs at distance L_0 . At each cycle, we also perform as many BSMs as possible at the intermediate nodes. The main requirement for such a protocol is that, at the stations that we perform BSMs, we must be aware of establishment of entanglement over links of length $l/2$ before extending it to distance l (informed BSMs). We use the results of

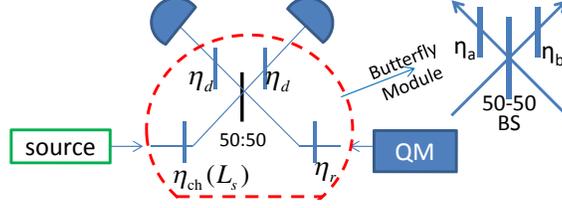


FIG. 5. BSM module with generic transmission coefficient represented by fictitious beam splitters. In our setup, η_a is the path loss; η_b is the reading efficiency and η_d is the detection efficiency.

[20] to calculate the generation rate of entangled states *per memory* used, which is given by

$$\begin{aligned} R_{\text{ent}}(L) &= NP_S(L_0)P_M^{(1)}P_M^{(2)}\dots P_M^{(n)}/T_0N2^{n+1} \\ &= P_S(L_0)P_M^{(1)}P_M^{(2)}\dots P_M^{(n)}/(2L/c) \end{aligned} \quad (2)$$

where T_0 is the duration of each cycle and $P_S(L/2^n)$ is the probability that the entanglement distribution protocol succeeds over a distance L_0 , $P_M^{(i)}$, $i = 1\dots n$, is the BSM success probability at nesting level i for a quantum repeater with n nesting levels. In our analysis, we use the expressions for P_S and $P_M^{(i)}$ up to two nesting levels as found in [29]. Finally, the total generation rate of entangled states in the limit of $NR_{\text{ent}}(L)L/c \gg 1$ is given by

$$R_{\text{rep}}(L) = N_{\text{QM}}R_{\text{ent}}(L), \quad (3)$$

where $N_{\text{QM}} = 2^{n+1}N$ is the total number of logical memories in Fig. 4.

III. SECRET KEY GENERATION RATE

In this section, we find the secret key generation rate, R_{QKD} , per logical memory used, for the scheme of Fig. 2 under the normal mode of operation when no eavesdropper is present. We consider two types of sources as discussed in Sec. II A.

A. Imperfect SPSs

Here, Alice and Bob each use an SPS with the output state as given by Eq. (1) in their encoder. In the limit of an infinitely long key and a sufficiently large number of QMs, their normalized secret key generation rate per employed memory is lower bounded by

$$\begin{aligned} R_{\text{QKD}} &= \frac{\min(R_S, R_{\text{rep}}/2)}{N_{\text{QM}}} \\ &\times \max \left\{ Q_{11}^z (1 - h(e_{11}^x)) - Q_{pp}^z f h(E_{pp}^z), 0 \right\} \end{aligned} \quad (4)$$

where $Q_{11}^z = (1-p)^2 Y_{11}^z$, with Y_{11}^z being the probability of a successful click pattern in the z basis when Alice and Bob send exactly one photon each; e_{11}^x is the quantum bit error rate (QBER) in the x basis, provided that Alice and Bob are each sending exactly a single photon; Q_{pp}^z is the probability of a successful click pattern in the z basis when Alice and Bob use sources with outputs as in Eq. (1), with the corresponding QBER given by E_{pp}^z ; f is the error correction inefficiency, and $h(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ is the Shannon binary entropy function.

Appendix A provides us with the full derivation of the relevant terms in Eq. (4). Our general approach to find these terms is as follows. For any basis $\Phi = x, z$ and any possible encoded state $\rho_{\text{enc}}^\Phi = \rho_{rs} \otimes \rho_{uv}$ by Alice and Bob, the initial state of the system for memories A_1 - B_1 and A_2 - B_2 is given by

$$\rho_{\text{in}}^\Phi = \rho_{\text{enc}}^\Phi \otimes \rho_{A_1 B_1} \otimes \rho_{A_2 B_2} \quad (5)$$

where $\rho_{A_i B_i}$ has been obtained in [29]. Once memories are read, their states will be transferred to photonic states, which we denote by the same label as their original memories. In that case, optical fields corresponding to modes r and A_1 , as well as the other three pairs of modes in Fig. 2, would undergo through the setup shown in Fig. 5, where $\eta_a = \eta_r \eta_d$ and $\eta_b = \eta_{\text{ch}}(L_s) \eta_d$. The equivalent sub-module in Fig. 5 is what we refer to as an asymmetric butterfly module, whose operation is denoted by $B_{\eta_a \eta_b}^{ab}$ when it acts on two incoming modes a and b . In [32], we have derived the output states of a butterfly module for relevant number states at its input. Using those results, we can then find the pre-measurement state right before the photodetection at the BSM modules by

$$\rho_{\text{out}}^\Phi = B_{\eta_a \eta_b}^{r A_1} \otimes B_{\eta_a \eta_b}^{s A_2} \otimes B_{\eta_a \eta_b}^{u B_1} \otimes B_{\eta_a \eta_b}^{v B_2} (\rho_{\text{in}}^\Phi). \quad (6)$$

Note that we have already accounted for the quantum efficiency of photodetectors in our butterfly modules. The probability for a particular pattern of clicks on detectors r_i, s_j, u_k , and v_l , for $i, j, k, l = 0, 1$, is given by

$$P_{r_i s_j u_k v_l}(\rho_{\text{enc}}^\Phi) = \text{tr}(\rho_{\text{out}}^\Phi M_{r_i} M_{s_j} M_{u_k} M_{v_l}), \quad (7)$$

where for $x = r, s, u, v$

$$\begin{aligned} M_{x_0} = (1 - d_c) [(I_{x_0} - |0\rangle_{x_0 x_0} \langle 0|) \otimes |0\rangle_{x_1 x_1} \langle 0| \\ + d_c |0\rangle_{x_0 x_0} \langle 0| \otimes |0\rangle_{x_1 x_1} \langle 0|] \end{aligned} \quad (8)$$

is the measurement operator to get a click on detector x_0 but not on x_1 . Here, I_{x_0} denotes the identity operator for the mode entering detector x_0 . One can define a similar operator M_{x_1} by swapping subscripts 0 and 1 in the above equation. Hence, for example, looking at Fig. 2 the measurement operator corresponding to a click on detector r_0 and no click on r_1 is given by

$$M_{r_0} = (1 - d_c) [(I_{r_0} - |0\rangle_{r_0 r_0} \langle 0|) \otimes |0\rangle_{r_1 r_1} \langle 0| + d_c |0\rangle_{r_0 r_0} \langle 0| \otimes |0\rangle_{r_1 r_1} \langle 0|] \quad (9)$$

The relevant terms in Eq. (4) can now be calculated by using Eq. (7) as shown in Appendix A.

B. Coherent sources

In this section we replace the SPSs with lasers sources and use the decoy-state technique to exchange secret keys. This is a more user friendly approach as the complexity of the required equipment for the end users would be minimized. In the limit of infinitely many decoy states, infinitely long key, and sufficiently large number of memories, the secret key generation rate per logical memory used is lower bounded by

$$R_{\text{QKD}} = \frac{\min(R_S, R_{\text{rep}}/2)}{N_{\text{QM}}} \times \max \{ Q_{11}^z (1 - H(e_{11}^x)) - Q_{\mu\nu}^z f H(E_{\mu\nu}^z), 0 \}, \quad (10)$$

where $Q_{\mu\nu}^z$ is the probability of a successful click pattern in the z basis when Alice and Bob send phase-randomized coherent pulses, respectively, with mean photon number $\mu = |\alpha|^2$ and $\nu = |\beta|^2$ and $E_{\mu\nu}^z$ is the QBER in the z basis in the same scenario.

The procedure to find $Q_{\mu\nu}^z$ and $E_{\mu\nu}^z$ is the same as what we outlined in Eqs. (5)-(8). The only difference here is that in our butterfly modules, we now need to know the output of the module to coherent states in one input port, for the signal coming from the users, and number states in the other, representing the state of QMs. Table III in Appendix A provides us with the input-output relations for a range of relevant input states. We can then find the relevant terms of the key rate, as shown in Appendix A.

Memory writing efficiency, η_w	0.78
Quantum efficiency, η_d	0.93
Memory reading efficiency, η_r	0.87
Dark count per pulse, d_c	10^{-9}
Attenuation length, L_{att}	25 km
Speed of light in optical fiber, c	2×10^5 km/s
Double-photon probability, p	10^{-4}
Access network length, L_s	5 km
Error correction inefficiency, f	1.16

TABLE II. Nominal values used in our numerical results.

IV. NUMERICAL RESULTS

In this section, we present numerical results for the secret key generation rate of our long-haul trust-free QKD link versus different system parameters. We look at two regimes of operation; the *source-limited* regime when memories are abundant and we are slowed down by source rates, i.e., $2R_S < R_{rep}$, versus the *repeater-limited* regime when the rate limitations come from the quantum repeater side, i.e., $2R_S > R_{rep}$. In the latter case, we should still satisfy the condition $NR_{ent}(L)L/c \gg 1$ in order that Eqs. (2)-(3) remain valid. We have used Maple 15 to analytically derive expressions for Eqs. 4 and 10. Unless otherwise noted, we use the nominal values summarized in Table II.

The first thing to obtain is the optimum intensity for our decoy-state scheme. Let us assume that in the symmetric scenario, as considered in this paper, Alice and Bob both use the same intensity value $\mu = |\alpha|^2 = \nu$ for their coherent signal states. Figure 6 shows the secret key generation rate per pulse versus $|\alpha|$ for (a) different values of d_c and (b) different values of p of the quantum repeater at $L_{rep} = 100$ km. We assume that $2R_S < R_{rep}$ and the plotted curves represent $R_{QKD}N_{QM}/R_S$ in Eq. (10). It can be seen in both figures that $|\alpha| = 1$ almost gives us the maximum rate in most scenarios. The optimal value is to some extent a function of d_c as can be seen in Fig. 6(a). By increasing d_c , the optimal intensity slightly decreases. Dark count represents the main source of error in the z basis, therefore, when d_c increases, the tolerance for the multiple-photon terms in a coherent state decreases,

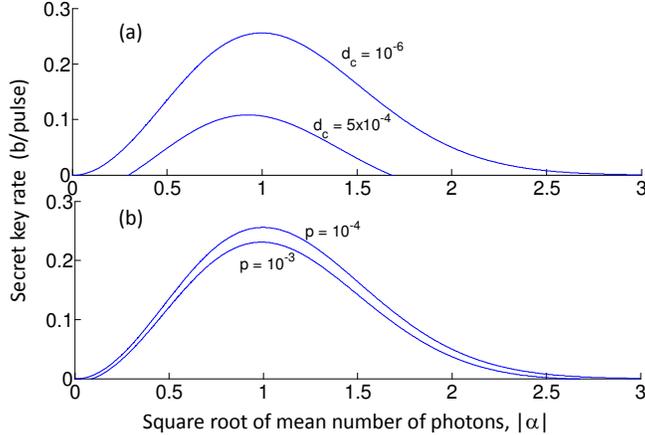


FIG. 6. Secret key generation rate per pulse versus $|\alpha| = |\beta|$ for different values of (a) the dark count and (b) the repeater’s double photon probability. Here, $L_{\text{rep}} = 100$ km and the other values are as in Tab. II.

hence the maximum allowed value of $|\alpha|$ will go down as well. This leads to a slightly shifted curve and therefore lower values for the optimal values of $|\alpha|$. On the contrary, $E_{\mu\nu}^z$ is not affected much by the double-photon probability p and there is not much difference in the optimal intensity when p increases as shown in Fig. 6(b). We also obtain the same optimal values of $|\alpha|$ for nesting levels one and two in the repeater-limited regime. Throughout this section, we then use $|\mu| = |\nu| = 1$ in our calculations.

A. Rate versus distance

Figures 7 and 8 show the secret key generation rate, at the optimal value of intensity, versus the total distance, $L = 2L_s + L_{\text{rep}}$, between Alice and Bob. In both figures, we assume L_s is a fixed short distance resembling the length of the access network. We vary L_{rep} then to effectively increase the link distance. Figure 7 shows the secret key generation rate per transmitted pulse in the source-limited regime, whereas Fig. 8 represents the key rate per logical memory used in the repeater-limited regime. In both cases we consider SPSs at $p = 10^{-4}$ as well as coherent decoy states. The difference in the performance of the systems relying on these sources, as expected, is low, and that again confirms the possibility, and practicality, of using the decoy-state technique for end-user devices. The cut-off security distance, i.e., the distance beyond which secure key exchange is not possible,

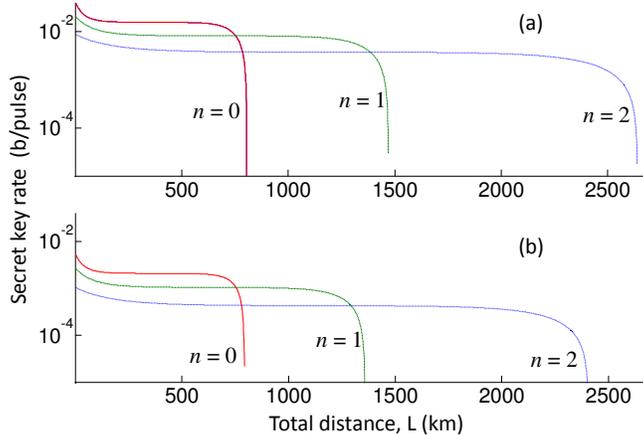


FIG. 7. Secret key generation rate per transmitted pulse, in the source-limited regime, versus distance when (a) imperfect SPSs and (b) decoy coherent states are used.

almost doubles every time we increase the nesting level so long as memories decoherence rates are correspondingly low. This distance at $n = 0$ is about 800 km, similar to the no-memory case for the parameter values used and at $n = 1$ and $n = 2$, respectively, reaches around 1500 km and 2500 km. Security distances are slightly higher for the SPSs than coherent-state sources.

The slope of the curves in Fig. 7 is different than that of Fig. 8. In Fig. 7 curves are almost flat until they reach their cut-off distances. That has two reasons. First, in the source-limited regime, R_{QKD} is proportional to the constant R_S , whereas, it scales with R_{ent} , which exponentially decays with L_0 [29], in the repeater-limited regime. Second, and this is common in both figures, in the absence of the decoherence, the fidelity of the entangled states generated by our probabilistic repeater effectively reaches a constant value once we increase the distance [22]. That means that the double-photon-driven error terms in the key rate are almost fixed until dark count becomes significant and the rate goes down.

The implications on the achievable key rate is also different in the two figures. In Fig. 7, at a nominal distance of $L = 1000$ km and a source rate of $R_S = 1$ GHz, the key rate is in the region of Mb/s. The assumption $2R_S < R_{\text{rep}}$, however, implies that we need something on the order of 10^{15} QMs in our core network to work in the source-limited regime, which seems, at the moment, quite impractical. In the repeater-limited regime, we still need many memories to obtain a decent rate. For instance, at $L = 1000$ km, we would need around 1 billion QMs to get a key rate on the order of kb/s. This is still a huge number of resources

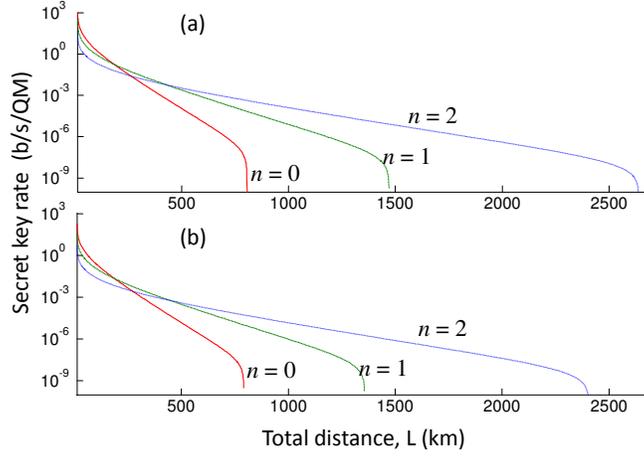


FIG. 8. R_{QKD} , in the repeater-limited regime, versus distance when (a) imperfect SPSs and (b) decoy coherent states are used.

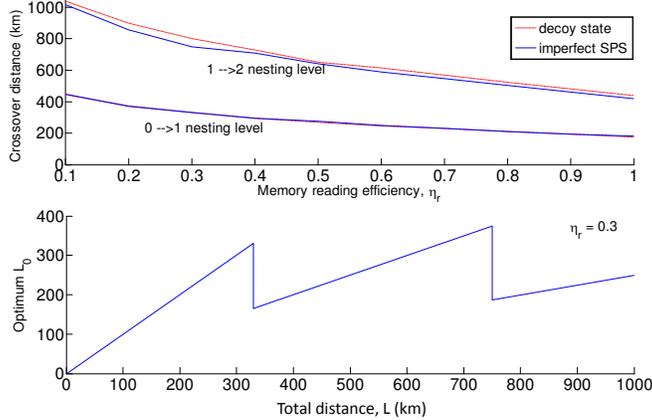


FIG. 9. (a) Crossover distance versus QM's recall efficiency in the repeater-limited regime. (b) Optimum spacing L_0 between adjacent nodes of a quantum repeater at $\eta_r = 0.3$.

for the current technology of QMs. This is in fact the same number of memories in use in our classical computers, which was perhaps inconceivable a few decades ago. Progress in solid-state QMs is much needed to meet the above requirements.

B. Crossover distance

The different slopes in Figs. 7 and 8 result in appreciably different values for crossover distances, i.e., the distances where one nesting level outperforms its previous one. In the source-limited regime, in Fig. 7, the curve for $n = 1$ outperforms that of $n = 0$ for L greater

than around 750 km. The crossover distance to nesting level 2 is then around 1400 km. These are quite large distances, which imply that L_0 , the spacing between adjacent nodes in our quantum repeater, could be as large as 700 km. This sparse location of memories in the system has some advantages in the sense that resources are more or less centralized, rather than distributed, but at the same time it imposes harder conditions on maintaining phase and polarization stability over such long distances. In the repeater-limited regime of Fig. 8, the nodes are much closer as now the crossover distance is around/below 500 km. This implies that the optimum architecture of our core network relies on, among other things, how many QMs are available at the time of development.

The crossover distance is also a function of the efficiency of various system parameters. In Fig. 9(a), we have looked at the crossover distance as a function of the recall efficiency, η_r , in the repeater-limited regime. This is particularly important, because η_r implicitly accounts for the amplitude decay in memories. As expected, the crossover distance decreases with the recall efficiency as there would be less of rate reduction because of the BSM operation. Figure 9(b) shows this effect on the optimal value of L_0 . It can be seen that at $\eta_r = 0.3$ the optimal spacing is much wider than what can be obtained from Fig. 8 at $\eta_r = 0.87$. It can be seen that the curve for optimal L_0 is non-continuous as we have limited our study to the case when the number of segments in a repeater setup is a power of 2. By developing new repeater protocols for arbitrarily number of segments, one can get a smoother curve for optimal L_0 . At $\eta_r = 0.3$, L_0 is on average around 250 km for the set of parameters as in Table II.

V. CONCLUSIONS

In this paper we combined MDI-QKD with a quantum repeater setup in order to obtain a long-distance key exchange scheme without the need to trust any of the intermediate nodes or measurement tools. This trust-free network could be used in future generations of quantum networks, where the easy cost-efficient access to the network would be facilitated by laser-based encoders and the repeater technology, at the backbone, would be maintained by the service provider. We considered a particular entanglement distribution scheme for our quantum repeater, which relied on imperfect single-photon sources. We merged memories entangled by this probabilistic repeater setup with photons sent and phase encoded by the

two users via two BSM modules. We showed that it would be possible to exchange secret keys up to over 2500 km using repeaters with two nesting levels. It turned out that in order to get a key rate on the order of 1 kb/s, one may need to employ and control billions of memories at the core network. We also showed that the network architecture depends on the number of memories at stake. In the limit of infinitely many memories, the repeater nodes would be sparsely located, although each node may contain a large number of memories. Our results showed how challenging it would be to build trust-free quantum communication networks.

Appendix A: Derivation of key rate terms

In this Appendix, we derive the key rate terms in Eqs. (4) and (10) under the normal mode of operation when no eavesdropper is present. We use the formulation developed in Eqs. (5)-(8) to obtain $\Gamma_{11}^z = Y_{11}^z$, $\epsilon_{11}^x = e_{11}^x$, $\Gamma_{pp}^z = Q_{pp}^z$, $\epsilon_{pp}^z = E_{pp}^z$, $\Gamma_{\mu\nu}^z = Q_{\mu\nu}^z$, and $\epsilon_{\mu\nu}^z = E_{\mu\nu}^z$, where new unifying notations Γ and ϵ are used in this section.

Let $\rho_{\text{enc}}^\Phi(mn)$ denote the output state of Alice and Bob's encoders for, respectively, sending bits m and n , for $m, n = 0, 1$, in basis Φ . With the above notation, the probability that an acceptable click pattern occurs in basis Φ , $\Gamma_{\gamma\delta}^\Phi$, is given by

$$\Gamma_{\gamma\delta}^\Phi = \sum_{i,j,k,l,m,n=0,1} P_{r_i s_j u_k v_l}(\rho_{\text{enc}}^\Phi(mn))/4, \quad (\text{A1})$$

where $\gamma = \delta = 1$ refers to the case when Alice and Bob are sending exactly one photon each; when $\gamma = \delta = p$, imperfect SPSs are used and when $\gamma = \mu$ and $\delta = \nu$ coherent states with mean photon number μ and ν , are, respectively, in use. In above, some of the successful click patterns would result in errors in the end, while the other in correct sifted key bits. By separating these two components, we obtain

$$\Gamma_{\gamma\delta}^\Phi = \Gamma_{\gamma\delta;C}^\Phi + \Gamma_{\gamma\delta;E}^\Phi, \quad (\text{A2})$$

where $\Gamma_{\gamma\delta;C(E)}^\Phi$ represents the click terms that result in correct (erroneous) inference of bits by Alice and Bob. In the z basis,

$$\Gamma_{\gamma\delta;C}^z = \sum_{i,j,k,l,m,n=0,1;m+n=1} P_{r_i s_j u_k v_l}(\rho_{\text{enc}}^z(mn))/4 \quad (\text{A3})$$

ρ_{AB}	$\text{tr} (M_{x_0} B_{\eta_a \eta_b}^{AB} (\rho_{AB}))$
$ \alpha 0\rangle\langle\alpha 0 $	$(1 - d_c) \left[e^{-\frac{\eta_a}{2}\mu} \left(1 - e^{-\frac{\eta_a}{2}\mu} \right) + d_c e^{-\eta_a \mu} \right]$
$ \alpha 1\rangle\langle\alpha 1 $	$(1 - d_c) \left[\frac{\eta_b}{2} e^{-\frac{\eta_a}{2}\mu} \left(1 + \frac{\eta_a}{2}\mu \right) + e^{-\frac{\eta_a}{2}\mu} (1 - \eta_b) \left(1 - e^{-\frac{\eta_a}{2}\mu} \right) + d_c (1 - \eta_b) (1 - e^{-\eta_a \mu}) \right]$
$ \alpha 2\rangle\langle\alpha 2 $	$(1 - d_c) \left\{ \frac{\eta_b^2}{4} e^{-\frac{\eta_a}{2}\mu} \left[1 + \frac{\eta_a^2}{4} \mu^2 \left(\frac{1}{2} - 8 e^{-\frac{\eta_a}{2}\mu} \right) + \eta_a \mu \right] + \eta_b e^{-\frac{\eta_a}{2}\mu} (1 - \eta_b) \left(1 + \frac{\eta_a}{2}\mu \right) + e^{-\frac{\eta_a}{2}\mu} (1 - \eta_b)^2 \left(1 - e^{-\frac{\eta_a}{2}\mu} \right) + d_c \left[\frac{\eta_a^2 \eta_b^2}{2} e^{-\eta_a \mu} \mu^2 + e^{-\eta_a \mu} (1 - \eta_b)^2 \right] \right\}$
$ \alpha 1\rangle\langle\alpha 0 $	$(1 - d_c) \left(\frac{1}{2} \sqrt{\eta_a \eta_b} \alpha e^{-\frac{\eta_a}{2}\mu} \right)$
$ \alpha 0\rangle\langle\alpha 1 $	$(1 - d_c) \left(\frac{1}{2} \sqrt{\eta_a \eta_b} \alpha e^{-\frac{\eta_a}{2}\mu} \right)$
$ \alpha 1\rangle\langle\alpha 2 $	$(1 - d_c) \left(\sqrt{\frac{\eta_a \eta_b}{2}} \alpha \left(\frac{\eta_b}{2} - \frac{\eta_a \eta_b}{8} - 1 \right) \right)$
$ \alpha 2\rangle\langle\alpha 1 $	$(1 - d_c) \left(\sqrt{\frac{\eta_a \eta_b}{2}} \alpha \left(\frac{\eta_b}{2} - \frac{\eta_a \eta_b}{8} - 1 \right) \right)$

TABLE III. The input-output relationship for a butterfly module with coherent states in one input and number states in the other. The column on the right represents the probability that the output state causes a click on detector x_0 , but not x_1 , assuming that detector x_0 measures the left output port and x_1 the right one. The expression $\text{tr} (M_{x_1} B_{\eta_a, \eta_b}^{AB} (\rho_{AB}))$ will give the same results as above for symmetrical input states; a minus sign correction is needed for asymmetrical input states. Here, $\mu = |\alpha|^2$.

and $\Gamma_{\gamma\delta;E}^\Phi = \Gamma_{\gamma\delta}^\Phi - \Gamma_{\gamma\delta;C}^\Phi$. In the x basis,

$$\begin{aligned}
\Gamma_{\gamma\delta;C}^x = & \sum_{i,k,m,n=0,1;m\oplus n=0} (P_{r_i s_i u_k v_k} (\rho_{\text{enc}}^x(mn))/4 \\
& + P_{r_i s_i \oplus 1 u_k v_k \oplus 1} (\rho_{\text{enc}}^x(mn))/4) \\
+ & \sum_{i,k,m,n=0,1;m\oplus n=1} (P_{r_i s_i u_k v_k \oplus 1} (\rho_{\text{enc}}^x(mn))/4 \\
& + P_{r_i s_i \oplus 1 u_k v_k} (\rho_{\text{enc}}^x(mn))/4),
\end{aligned} \tag{A4}$$

where \oplus denotes addition modulo two. Finally, all QBER terms can be obtained from the following.

$$\epsilon_{\gamma\delta}^\Phi = \frac{\Gamma_{\gamma\delta;E}^\Phi}{\Gamma_{\gamma\delta}^\Phi}. \tag{A5}$$

-
- [1] H. J. Kimble, *Nature* **453**, 1023 (2008).
- [2] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, *Nature* **501**, 69 (2013).
- [3] M. Razavi, *IEEE Trans. Commun.* **60**, 3071 (2012).
- [4] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, *Phys. Rev. X* **2**, 041010 (2012).
- [5] I. Choi, R. J. Young, and P. D. Townsend, *New J. Phys.* **13**, 063039 (2011).
- [6] M. Peev *et al.*, *New J. Phys.* **11**, 075001 (2009).
- [7] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legre, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Langer, M. Peev, and A. Zeilinger, *Opt. Exp.* **19**, 10387 (2011).
- [8] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
- [9] E. Biham, B. Huttner, and T. Mor, *Phys. Rev. A* **54**, 2651 (1996).
- [10] H.-K. Lo, M. Curty, and B. Qi, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [11] X. Ma and M. Razavi, *Phys. Rev. A* **86**, 062319.
- [12] X. Ma, C.-H. F. Fung, and M. Razavi, *Phys. Rev. A* **86**, 052305 (2012).
- [13] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, *Phys. Rev. Lett.* **111**, 130502 (2013).
- [14] M. Razavi, N. Lo Piparo, C. Panayi, and D. E. Bruschi, in *Iran Workshop on Communication and Information Theory (IWCIT)* (Tehran, Iran, 2013) pp. 1–7.
- [15] K. Azuma, K. Tamaki, and H.-K. Lo, arXiv:1309.7207 [quant-ph] (2013).
- [16] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, *Quant. Inf. Comput.* **7**, 073 (2007).
- [17] V. Makarov, *New Journal of Physics* **11**, 065003 (18pp) (2009).

- [18] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, *New Journal of Physics* **13**, 013043 (2011).
- [19] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, *New Journal of Physics* **13**, 073024 (2011).
- [20] M. Razavi, M. Piani, and N. Lütkenhaus, *Phys. Rev. A* **80**, 032301 (2009).
- [21] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, *Nature* **414**, 413 (2001).
- [22] J. Amirloo, M. Razavi, and A. H. Majedi, *Phys. Rev. A* **82**, 032304 (2010).
- [23] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, *Rev. Mod. Phys.* **83**, 33 (2011).
- [24] D. E. Bruschi, T. M. Barlow, M. Razavi, and A. Beige, arXiv:1407.3362 (2014).
- [25] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **81**, 5932 (1998).
- [26] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, *Nature Photon.* **6**, 771 (2012).
- [27] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, *Phys. Rev. Lett.* **112**, 250501 (2014).
- [28] N. Sangouard, C. Simon, J. c. v. Minář, H. Zbinden, H. de Riedmatten, and N. Gisin, *Phys. Rev. A* **76**, 050301 (2007).
- [29] N. Lo Piparo and M. Razavi, *Phys. Rev. A* **88**, 012332 (2013).
- [30] S. Abruzzo, H. Kampermann, and D. Bruß, *Phys. Rev. A* **89**, 012301 (2014).
- [31] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, *New Journal of Physics* **16**, 043005 (2014).
- [32] N. Lo Piparo, M. Razavi, and C. Panayi, arXiv:1407.8016 (2014).
- [33] M. Razavi and J. H. Shapiro, *Phys. Rev. A* **73**, 042303 (2006).
- [34] M. Razavi, K. Thompson, H. Farmanbar, M. Piani, and N. Lütkenhaus, in *Proc. SPIE*, Vol. 7236 (San Jose, CA, 2009) p. 723603.