Memory-assisted measurement-device-independent quantum key distribution

2014 New J. Phys. 16 043005

(http://iopscience.iop.org/1367-2630/16/4/043005)

New Journal of Physics
The open access journal at the forefront of physics
Deutsche Physikalische Gesellschaft DPG | IOP Institute of Physics

Memory-assisted measurement-device-independent quantum key distribution

Christiana Panayi[1,5], Mohsen Razavi[1], Xiongfeng Ma[2] and Norbert Lütkenhaus[3,4]

[1] School of Electronic and Electrical Engineering, University of Leeds, Leeds LS2 9JT, UK
[2] Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, People's Republic of China
[3] Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada
[4] Department of Physics and Astronomy, University of Waterloo, Waterloo, ON N2L 3G1, Canada
E-mail: py10cp@leeds.ac.uk, m.razavi@leeds.ac.uk, xma@tsinghua.edu.cn and nlutkenhaus@uwaterloo.ca

Received 24 September 2013, revised 31 January 2014
Accepted for publication 4 February 2014
Published 7 April 2014

New Journal of Physics **16** (2014) 043005

doi:10.1088/1367-2630/16/4/043005

Abstract

A protocol with the potential of beating the existing distance records for conventional quantum key distribution (QKD) systems is proposed. It borrows ideas from quantum repeaters by using memories in the middle of the link, and that of measurement-device-independent QKD, which only requires optical source equipment at the user's end. For certain memories with short access times, our scheme allows a higher repetition rate than that of quantum repeaters with single-mode memories, thereby requiring lower coherence times. By accounting for various sources of nonideality, such as memory decoherence, dark counts, misalignment errors, and background noise, as well as timing issues with memories, we develop a mathematical framework within which we can compare QKD systems with and without memories. In particular, we show that with the state-of-the-art technology for quantum memories, it is potentially possible to devise memory-assisted QKD systems that, at certain distances of practical interest, outperform current QKD implementations.

[5] Author to whom any correspondence should be addressed.

Keywords: quantum key distribution, quantum memory, measurement device independent, quantum repeaters, quantum networks

1. Introduction

Despite all commercial [1] and experimental achievements in quantum key distribution (QKD) [2–10], reaching arbitrarily long distances is still a remote objective. The fundamental solution to this problem, i.e., quantum repeaters, has been known for over a decade. From early proposals by Briegel *et al* [11] to the latest no-memory versions [12–14], quantum repeaters, typically, rely on highly efficient quantum gates comparable to what we may need for future quantum computers. While the progress on that ground may take some time before such systems become functional, another approach based on *probabilistic* gate operations was proposed by Duan and co-workers [15], which could offer a simpler way of implementing quantum repeaters for moderate distances of up to around 1000 km. The latter systems require quantum memory (QM) modules with high coupling efficiencies to light *and* with coherence times exceeding the transmission delays, which are yet to be achieved together. In this paper, we propose a protocol that, although is not as scalable as quantum repeaters, for certain classes of memories, relaxes, to some extent, the harsh requirements on memories' coherence times, thereby paving the way for the existing technologies to beat the highest distance records achieved for no-memory QKD links [2]. The idea behind our protocol was presented in [16], and independent work has also been reported in [17]. This work proposes additional practical schemes and rigorously analyses them under realistic conditions.

Our protocol relies on concepts from quantum repeaters, on the one hand, and the recently proposed measurement-device-independent QKD (MDI-QKD), on the other. The original MDI-QKD [18] relies on sending encoded photons by the users to a middle site at which a Bell-state measurement (BSM) is performed. One major practical advantage of MDI-QKD is that this BSM can be done by an *untrusted* party, e.g., the service provider, which makes MDI-QKD resilient to detector attacks, e.g., time-shift, remapping, and blinding attacks [19–26]. The security is then guaranteed by the reverse EPR protocol [27]. Another practical advantage is that this BSM does not need to be a perfect measurement, but even a partial imperfect BSM implemented by linear optical elements can do the job. In our scheme, by using two QMs at the middle site, we first store the state of the transmitted photons in the memories, and perform the required BSM, only when both memories are loaded. In that sense, our memory-assisted MDI-QKD is similar to a single-node quantum repeater, except that there is no memories at the user's end. This way, similar to quantum repeaters, we achieve a rate-versus-distance improvement as compared to the MDI-QKD schemes proposed in [18, 28–30], or other conventional QKD systems that do not use QMs.

There is an important distinction between our protocol and a conventional quantum repeater system that relies on single-mode memories. In such a quantum repeater link, which relies on initial entanglement distribution among neighbouring nodes, the repeat period for the protocol is mainly dictated by the transmission delay for the shortest segment of the repeater system [31, 32]. In our scheme, however, the repeat period is constrained by the writing time, including the time needed for the herald/verification process, into memories. This implies that using sufficiently fast memories, i.e., with short writing times, one can run our scheme at a faster rate than that of a quantum repeater, thereby achieving higher key generation rates, as

compared to conventional QKD links, and at lower coherence times, as compared to probabilistic repeater systems. This increase in clock rate is what our proposal shares with the recently proposed third generation of quantum repeaters, which use quantum error correction codes to compensate for loss and errors, thus also being able to speed up the clock rate to local processing times [12]. The need for long coherence times remains one of the key challenges in implementing the first generations of quantum repeaters before the latest no-memory quantum repeater proposals can be implemented.

The above two benefits would offer a midterm solution to the problem of long-distance QKD. While our scheme is not scalable the same way that quantum repeaters are, it possibly allows us to use the existing technology for QMs to improve the performance of QKD systems. In the absence of fully operational quantum repeater systems, our setup can fill the gap between theory and practice and will become one of the first applications of realistic QMs in quantum communications.

It is worth mentioning that the setups we propose here are compatible with different generations of hybrid quantum-classical (HQC) networks [33]. In such systems, home users are not only able to use broadband data services, but they can also use quantum services such as QKD. MDI-QKD offers a user-friendly approach to the access part of such networks as the end users only require source equipment. Whereas, in the first generation of HQC networks, the service provider may only facilitate routing services for quantum applications, in the future generations, probabilistic, deterministic, and eventually no-memory quantum repeaters constitute the quantum core of the network. In each of these cases, our setups are extensible and compatible with forthcoming technologies for HQC networks.

The rest of the paper is structured as follows. In section 2, we describe our proposed schemes and the modelling used for each component therein. Section 3 presents our key rate analysis, followed by some numerical results in section 4. Section 5 concludes the paper.

2. System description

Our scheme relies on 'loading' QMs with certain, unknown, states of light. This loading process needs to be heralding, that is, by the end of it, we should learn about its success. Within our scheme, two types of memories can be employed, which we refer to by *directly* versus *indirectly* heralding QMs. Some QMs can operate in both ways, while some others are more apt to one than the other. By directly heralding memories we refer to the class of memories to which we can directly transfer the state of a photon *and* we can verify—without revealing or demolishing the quantum state—whether this writing process has been successful. An example of such memories is a trapped atom in an optical cavity [34]. In the case of indirectly heralding memories, a direct writing-verification scheme may not exist. Instead, we assume that we can entangle a photonic state with the state of such QMs [15, 35–40], and later, by doing a measurement on the photon, we can effectively achieve a heralded writing into the memory. These two approaches of writing cover most relevant practical examples to our scheme.

The scheme for directly heralding memories works as follows [16, 17]; see figure 1(a). The two communicating parties, Alice and Bob, send BB84 encoded pulses [41], by either single-photon or weak laser sources, towards QM units located in the middle of the link. Each QM stores a photon in a possibly probabilistic, but *heralding*, way. Once both memories are loaded,

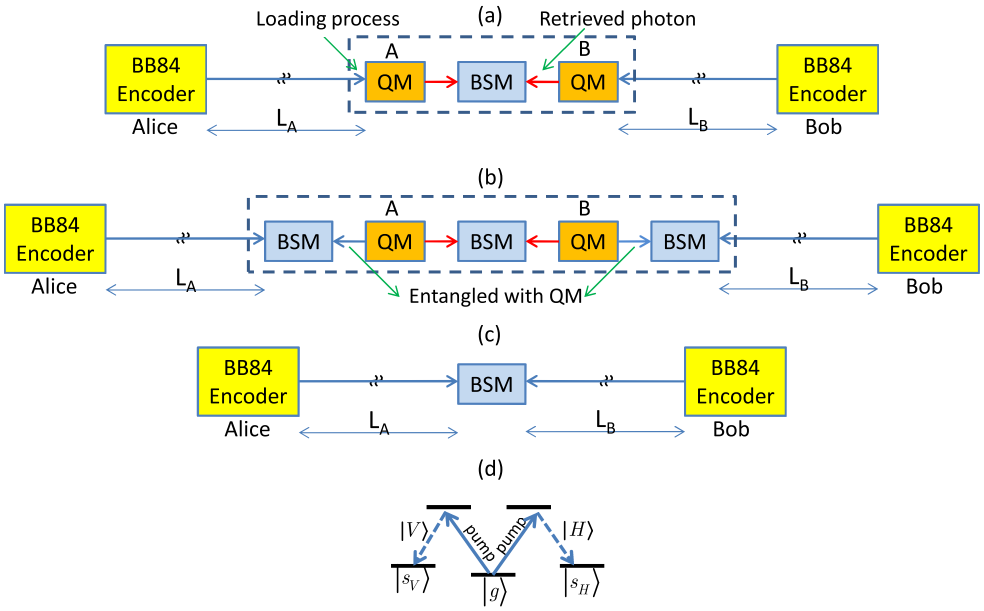

Figure 1. (a) Measurement-device-independent quantum key distribution (MDI-QKD) with directly heralding quantum memories. Alice and Bob use the efficient BB84 protocol to encode and send pulses to their respective quantum memory (QM) in the middle of the link. At each round, each QM attempts to store the incoming pulse. Once they are both loaded, we retrieve the QMs' states and perform a BSM on the resulting photons. (b) MDI-QKD with indirectly heralding quantum memories. At each round, an entangling process is applied to each QM, which would generate a photon entangled, in polarization, with the QM. These photons interfere at the BSM modules next to the QMs with incoming pulses from the encoders. As soon as one of these BSMs succeeds, we stop the entangling process on the corresponding QM, and wait until both QMs are ready for the middle BSM operation. In this case, QMs are not required to be heralding; a trigger event is declared by the success of the BSM located between the QM and the respective encoder. (c) The original MDI-QKD protocol [18]. (d) One possible energy-level configuration for a QM suitable for polarization encoding.

we retrieve their states and perform a BSM on the corresponding photons. A successful BSM indicates some form of correlation between the transmitted bits by Alice and Bob.

We can easily extend the above idea to the case of indirectly heralding memories. An additional BSM, on each side, along with an entangling process between photons and QMs, can replace the verification process needed for directly heralding memories. In this case, see figure 1(b), a successful BSM between the transmitted photon by the users and the one entangled with the QM, would effectively herald a successful loading process, that is, the state of the QM is correlated with the quantum state sent by the users.

In order to entangle a QM with a photon, one can think of two standard ways. One approach would be to generate a pair of entangled photons, e.g., by using spontaneous parametric down-converters [42, 43], and then store one of the photons in the memory and use the other one for interference with the incoming photon sent by the user. While this approach is not fully heralding (because we cannot be sure of the absorption of the locally generated photon by the memory), it is still a viable option for highly efficient writing procedures. Another approach to entangle a photon with a memory, which this paper is mainly concerned with, is to start from the memory and generate a photon entangled with the memory by driving certain

transitions in the memory [15, 40]. With entangling times as short as 300 ps reported in the literature [44], high repetition rates are potentially achievable for indirectly heralding memories.

In either approach, it is possible to have multiple-excitation effects, which can cause errors in our setup. In this paper, for readability reasons, we make the simplifying assumption of having only single excitations in the memories, and address the multiple excitation effect in a separate publication [45]. Furthermore, here we only consider the polarization entanglement. The extension to other types of entanglement is straightforward and will be dealt with in forthcoming publications.

Under all above assumptions, suppose once we entangle the memory A with a single photon P, the joint state of the two is given by

$$\frac{1}{\sqrt{2}}\left[\left|s_H\right\rangle_A|H\rangle_P + \left|s_V\right\rangle_A|V\rangle_P\right], \tag{2.1}$$

where $|H\rangle_P$ and $|V\rangle_P$, respectively, represent horizontally and vertically polarized single photons, and $|s_H\rangle_A$ and $|s_V\rangle_A$ are the corresponding memory states; see figure 1(d). In equation (2.1), the conditional state of the photon, knowing the memory state, has the same form as in BB84. Each leg of figure 1(b), from the user end to the respective QM, is then similar to an asymmetric setup of the original MDI-QKD scheme as depicted in figure 1(c). The working of the system in figure 1(b) will then follow that of the original MDI-QKD. We will use this similarity in our analysis of the system in figure 1(b).

The main advantage of our scheme as compared to the original MDI-QKD, in figure 1(c), is its higher resilience to channel loss and dark count. In the no-memory MDI-QKD, both pulses, sent by Alice and Bob, should survive the path loss before a BSM can be performed. The key generation rate then scales with the loss in the entire channel. In our scheme, each pulse still needs to survive the path loss over half of the link, but this can happen in different rounds for the signal sent by Alice as compared to that of Bob. We therefore achieve the quantum repeater benefit in that the key generation rate, in the symmetric case, scales with the loss over half of the total distance. Moreover, in the case of directly heralding memories, our scheme is almost immune against dark counts [17]. This is because the measurement efficiency in the BSM module is typically a few orders of magnitude higher than that of dark count rates. Dark counts will then only sightly add to the error rate. In our scheme, memory decoherence errors play a major role as we will explain in this and the following sections.

In the following, we describe the protocol and its components in more detail.

2.1. Protocol

In our protocol, Alice and Bob, at a rate R_S, send BB84 encoded pulses to the middle station (dashed boxes in figure 1). At the QMs, for each incoming pulse, we either apply a loading process by which we can store the state of the photons into memories and verify it, or use the indirectly heralding scheme of figure 1(b). Once successful for a particular QM, we stop the loading procedure on that QM, and wait until both memories are loaded, at which point, a BSM is performed on the QMs. The BSM results are sent back to Alice and Bob, and the above procedure is being repeated until a sufficient number of raw key bits is obtained. The rest of the protocol is the same as that of MDI-QKD. Sifting and postprocessing will be performed on the raw key to obtain a secret key. In this paper, we neglect the finite-size-key effects in our analysis [29].

2.2. Component modeling

In this section, we model each component of figure 1 including sources and encoders, the channel, QMs, and the BSM module.

2.2.1. Sources and encoders. We consider two types of sources: ideal single-photon sources and phase-randomized weak laser pulses. The latter will be used in the decoy-state [46] version of the protocol. Each source, at both Alice's and Bob's sides, generates pulses at a rate R_S. Each pulse is polarization encoded in either the rectilinear (Z) or diagonal (X) basis. In the case of ideal single photons, we, correspondingly, send states $|H\rangle$ and $|V\rangle$ in the Z basis, and $(|H\rangle + |V\rangle)/\sqrt{2}$ and $(|H\rangle - |V\rangle)/\sqrt{2}$ in the X basis. In each basis, the two employed states, respectively, represent bits 1 and 0. In the case of the decoy-state protocol, the single-photon states are replaced with weak phase-randomized coherent states of the same polarization. Here, we use the efficient version of BB84 encoding, where the Z basis is used much more frequently than the X basis [47]. The pulse duration is denoted by τ_p and it is chosen in accordance with the requirements of the memory system in use.

There are several sources of nonideality one may be concerned with at the encoder box. For instance, in [48], one major source of error is in not generating fully orthogonal states in each basis. Note that secure exchange of keys may still be possible, although at a possibly reduced rate, by using even uncharacterized sources [49]. Another possible issue would be in having multiple-photon components if one uses parametric down-converters to generate single photons [50, 51]. Although all these issues, among others, are important in the overall performance of the system, here we would rather focus on the memory side of the system, which is newly introduced, and deal with the details of source imperfections, and their effects on the secret key generation rate in a separate publication [45].

2.2.2. Channels. The distance between Alice (Bob) and the respective QM is denoted by L_A (L_B). The total distance between Alice and Bob is denoted by $L = L_A + L_B$. The transmission coefficient for a channel with length l is given by

$$\eta_{\mathrm{ch}}(l) \equiv \exp(-l/L_{\mathrm{att}}), \tag{2.2}$$

where L_{att} is the attenuation length of the channel (roughly, 22 km for 0.2 dB per km of loss).

The channel is considered to have a background rate of γ_{BG} per polarization mode, which results in an average $p_{\mathrm{BG}} = 2\gamma_{\mathrm{BG}}\tau_p$ background photons per pulse. This can stem from stray light or crosstalk from other channels, especially if classical signals are multiplexed with quantum ones in a network setup [5, 6, 52–54].

We also consider setup misalignment in our analysis. We assume certain polarization maintenance schemes are in place for the Alice's and Bob's channels, so that the reference frames at the sources and memories are, on average, the same. We, nevertheless, consider a setup misalignment error probability e_{dK}, for $K = A, B$, to represent misalignment errors in each channel.

2.2.3. Quantum memories. We use the following assumptions and terminologies for the employed QMs. This list covers most relevant parameters in an experimental setup relying on polarization encoding, whether the QM is operated in the directly or indirectly heralding mode.

- In the case of a successful loading, each QM in figure 1 ideally stores a polarization *qubit* corresponding to the polarization of the incoming pulse. We assume that such a squashing operation occurs [55, 56] even if at the input of the QM there is a nonqubit state, e.g., a phase-randomized coherent state. That is, if, for instance, two photons with horizontal polarizations are at the input of the memory, the QM would only store the polarization information, and ignores the photon-number information. In practice, the loading efficiency would be a function of input photon numbers, but, for simplicity, here we neglect this dependence. This is in line with our single-excitation assumption we have adopted in this paper. One suitable energy level structure for such a memory is the double-Λ configuration in figure 1(d), with a common ground state and two other metastable states corresponding to two orthogonal polarizations. The excited states can then facilitate Raman transitions from the ground state to each of the metastable states, using known optical transition techniques [57, 58], in response to the input polarization state.
  We assume that each QM only stores one spatio-temporal mode of light. Our protocol can be extended to incorporate multimode QMs [59–62] or multiple QMs [31], in which case a linear improvement in the rate is expected. In this work, we focus on the case of a single logical memory per user and leave extensions to future work.
- For directly heralding memories, we denote the QM's writing efficiency by η_w. The writing efficiency is the probability to store a qubit and herald success conditioned on having a single-photon at the QM's input. Note that η_w also includes the chance of failure for our verification process. For indirectly heralding memories, we introduce an entangling efficiency, η_{ent}, which is the probability of success for entangling a photon with our QM.
- We denote the QM's reading efficiency by η_r. That is the probability to retrieve a single photon out of the QM conditioned on a successful loading in the past. The reading efficiency is expected to decay over a time period t as $\eta_r(t) = \eta_{r0} \exp[-t/T_1]$, where T_1 is the memory amplitude decay time and η_{r0} is the reading efficiency right after loading. In our example of a double-Λ-level memory of figure 1(d), such a decay corresponds to the transition form one of the metastable states $|s_H\rangle$ or $|s_V\rangle$ to the ground state $|g\rangle$, in which case, no photon will be retrieved from the memory.
- We denote the QM's writing time by τ_w. For directly heralding memories, it is the time difference between the time that a pulse arrives (beginning of the pulse) at the QM and the time that a successful/unsuccessful loading is declared. This is practically the fastest repeat period one can run our protocol. In the case of indirectly heralding memories, τ_w includes the time for the entangling process as well as that of the side BSM operation. Accounting for such timing parameters is essential in enabling us to have a fair comparison between memory-assisted and no-memory QKD systems.
  One must note that in a practical setup there will be time periods, e.g., for synchronization purposes or memory refreshing, over which no raw key is exchanged. The total number of key bits exchanged over a period of time must therefore exclude such periods once the total key generation rate is calculated. In our work, we neglect all these overhead times, with the understanding that one can easily modify our final result by considering the percentage of the time spent on such processes within a specific practical setup.

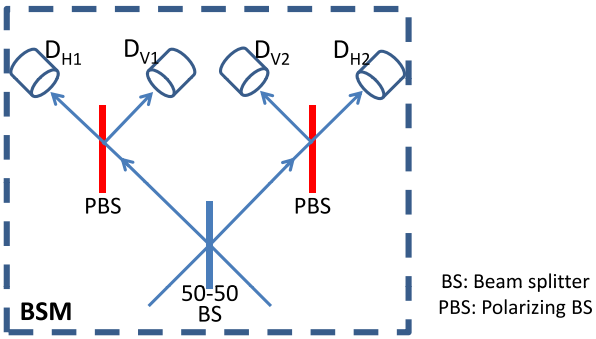

Figure 2. Bell-state measurement module for polarization states.

- We denote the QM's reading time by τ_r. It is the time difference between the time that the retrieval process is applied until a pulse (end of the pulse) is out.
- We denote the QM's coherence (dephasing) time by T_2. For an initial state $\rho(0)$ of the QM at time zero, its state at a later time t is given by [31]

$$\rho(t) = p(t)\rho(0) + [1 - p(t)]Z\rho(0)Z, \tag{2.3}$$

where $p(t) = [1 + \exp(-t/T_2)]/2$. Note that dephasing would only occur if we are in a superposition of Z eigenstates, e.g., the eigenstates of X. The above model of decoherence is expected to have more relevance in some practical cases of interest [31, 34, 40] than the model used in [17], in which the memory state switches suddenly from an intact one to a fully randomized version after a certain time. We discuss the implications of each model in our numerical result section. It is, however, beyond the scope of this paper to fully model every possible decoherence mechanisms in QMs. Specific adjustments are needed if one uses a memory that is not properly modelled by our T_1 and T_2 time constants.

2.2.4. BSM module. Figure 2 shows the schematic of the BSM module used in our analysis. This module enables an incomplete BSM over photonic states. In order to use this module, in our scheme, we first need to read out the QMs and convert their qubit states into polarization-encoded photons. The BSM will then be successful if exactly two detectors click, one H-labelled and one V-labelled. Depending on which detectors have clicked and what basis is in use, Alice and Bob can identify what bits they ideally share [28].

We assume the BSM module is symmetric. We lump detector quantum efficiencies with other possible sources of loss in the BSM module and denote it by η_d for each detector. We also assume that each detector has a dark count rate of γ_{dc}, which results in a probability $p_{\mathrm{dc}} = \gamma_{\mathrm{dc}}\tau_p$ of having a dark count per pulse. The implicit assumption here is that the retrieved and the writing photons have the same pulse width. Finally, we assume that there is no additional misalignment error in the BSM module.

3. Key rate analysis

In this section, we find the secret key generation rate for our proposed schemes in figures 1(a) and (b). The common assumption in our predicting the relevant observed parameters in a QKD experiment is that we work under the normal mode of operation, where there is no eavesdropper present, and we are only affected by the imperfections of the system, behind which an

eavesdropper can in principle hide. We later compare our results with two conventional QKD schemes, namely, BB84, summarized in appendix A, and the original MDI-QKD in figure 1(c), summarized in appendix B, that use no memories. In all cases, we consider both single-photon and decoy-state sources. In all forthcoming sections, f denotes the inefficiency of the error correction scheme, i.e., the ratio between the actual cost of error correction and its minimum value obtained by the Shannon's theorem, assumed to be constant, and we denote the binary entropy function as $h(p) = -p\ \log_2(p) - (1-p)\log_2(1-p)$, for $0 \leqslant p \leqslant 1$.

3.1. Key rate for single-photon sources

With ideal single-photon sources, the secret key generation rate in the setups of figures 1(a) and (b) is lower bounded by [63]

$$R_{\mathrm{QM}} = R_S Y_{11}^{\mathrm{QM}} \left[1 - h\left(e_{11;X}^{\mathrm{QM}}\right) - fh\left(e_{11;Z}^{\mathrm{QM}}\right)\right], \tag{3.1}$$

where efficient BB84 encoding is employed [47]. In the above equation, $e_{11;X}^{\mathrm{QM}}$ and $e_{11;Z}^{\mathrm{QM}}$, respectively, represent the quantum bit error rate (QBER) between Alice and Bob in the X and Z basis, when single photons are used, and Y_{11}^{QM} represents the probability that both memories are loaded with single photons of the same basis *and* the middle BSM is successful.

To obtain the individual terms in equation (3.1), we can decompose the protocol into two parts: the memory loading step and the measurement step, once both memories are loaded. The first step is a probabilistic problem with two geometric random variables, N_A and N_B, corresponding, respectively, to the number of attempts until we load Alice and Bob's memories with single photons. The number of rounds that it takes to load both memories is then $\max\{N_A, N_B\}$. Once both memories are loaded, the rest of the protocol is similar to that of original MDI-QKD in terms of rate analysis: the QMs replace the sources in figure 1(c) and the total transmission-detection efficiency is replaced by the reading-measurement efficiency in the BSM module. We can therefore use many of the relationships obtained for the original MDI-QKD, summarized in appendix B, for the memory-assisted versions of figure 1.

For finite values of T_1, the reading efficiency for the Alice's QM could be different from that of Bob. In fact, we can assume that, once both memories are loaded, one of the memories (late) will be read immediately, while the other (early) $|N_A - N_B|$ rounds after its successful loading. The effective measurement efficiency for the leg K, $K = A, B$, corresponding to the path originating from memory K in the BSM module will then be given by

$$\eta_{mK} = \begin{cases} \eta_m \equiv \eta_{r0}\eta_d, & \text{if memory } K \text{ is late} \\ \eta_d\, \eta_r(t = \left|N_A - N_B\right| T), & \text{if memory } K \text{ is early.} \end{cases} \tag{3.2}$$

With the above setting, and considering the required time for reading from the QMs, we obtain

$$\begin{aligned} Y_{11}^{\mathrm{QM}} &= \frac{1}{N_L(\eta_{1A}, \eta_{1B}) + N_r} \mathrm{E}\{Y_{11}(\eta_{mA}, \eta_{mB})\} \\ &= \frac{1}{N_L(\eta_{1A}, \eta_{1B}) + N_r} Y_{11}(\eta_m, \eta_m'), \end{aligned} \tag{3.3}$$

where Y_{11} is the corresponding yield term, given by equation (B.4), for the MDI-QKD protocol and $N_L = \mathrm{E}\{\max(N_A, N_B)\}$ is given by equation (C.3). Here, $\mathrm{E}\{\cdot\}$ represents the expectation value operator with respect to N_A and N_B, and $\eta_m' = \eta_d \overline{\eta}_r$, where $\overline{\eta}_r = \eta_{r0}\mathrm{E}\{\exp(-|N_A - N_B|T/T_1)\}$ can be obtained from equation (C.4). In equation (3.3), N_r, represents the extra rounds lost due to the nonzero reading times of QMs, once they are both loaded, and is given by

$$N_r = \left\lceil \frac{\tau_r + \tau_w}{T} \right\rceil - 1, \quad \tau_r, \tau_w > 0, \quad \tau_w \leqslant T, \tag{3.4}$$

where $T = 1/R_S$ is the repetition period. The condition $\tau_w \leqslant T$ is a matter of practicality as sending photons faster than they can be stored is of no benefit. The fastest possible rate is then obtained at $T = \tau_w$.

In the case of directly heralding memories of figure 1(a), we have

$$\eta_{1K} = 1 - \left(1 - \eta_w \eta_{\mathrm{ch}}(L_K)\right) e^{-\eta_w p_{\mathrm{BG}}}, \quad K = A, B, \tag{3.5}$$

as the probabilities of successful loading of Alice and Bob's QMs with single-photon sources (or background noise). In the case of indirectly heralding memories of figure 1(b), following our discussion in (2) about the equivalence of each leg of figure 1(b) to an asymmetric MDI-QKD system, we have

$$\eta_{1K} = Y_{11}\left(\eta_d \eta_{\mathrm{ch}}(L_K), \eta_d \eta_{\mathrm{ent}}\right), \quad K = A, B, \tag{3.6}$$

where the above terms must be calculated at an effective dark count rate of $\gamma_{\mathrm{dc}} + \gamma_{\mathrm{BG}}\eta_d/2$.

We remark that, although obtained from different methods, the analysis in [17] also finds similar expressions for the yield term. In [17], the analysis is only concerned with the symmetric setup, and some of the parameters considered in our work take their ideal values. It can be verified, however, that in the special case of $\tau_w = T$, $\tau_r = 0$, $\gamma_{\mathrm{BG}} = 0$, $L_A = L_B$, $\eta_w = 1$, and $T_1 \to \infty$, for directly heralding memories, equation (3.3) reduces to the same result obtained in [17]. By accounting for additional relevant parameters, our analysis offers a better match to realistic experimental scenarios.

Similarly, the error terms are given by

$$\begin{aligned} e_{11;Z}^{\mathrm{QM}} &= \mathrm{E}\left\{e_{11;Z}\left(\eta_{mA}, \eta_{mB}, e_{dZ}^{\mathrm{QM}}(\eta_{1A}, \eta_{1B})\right)\right\} \\ &= e_{11;Z}\left(\eta_m, \eta_m', e_{dZ}^{\mathrm{QM}}(\eta_{1A}, \eta_{1B})\right), \\ e_{11;X}^{\mathrm{QM}} &= \mathrm{E}\left\{e_{11;X}\left(\eta_{mA}, \eta_{mB}, e_{dX}^{\mathrm{QM}}(\eta_{1A}, \eta_{1B})\right)\right\} \\ &\approx e_{11;X}\left(\eta_m, \eta_m', \mathrm{E}\left\{e_{dX}^{\mathrm{QM}}(\eta_{1A}, \eta_{1B})\right\}\right), \end{aligned} \tag{3.7}$$

where, $e_{11;Z}$ and $e_{11;X}$, given by equation (B.4), are the corresponding error terms for the original MDI-QKD. In addition to the typical sources of error, such as loss and dark count, the above expressions are functions of misalignment parameters. This misalignment could be a statistical error in the polarization stability of our setup, modelled by e_{dA} and e_{dB}, or an effective misalignment because of memory dephasing [64] and/or background photons. Putting all these effects together, as we have done in appendix D, we obtain

$$e_{dS}^{\mathrm{QM}}(\eta_A, \eta_B) = e_{dS}^{(A)}(\eta_A, \eta_B)\left(1 - e_{dS}^{(B)}(\eta_A, \eta_B)\right) + e_{dS}^{(B)}(\eta_A, \eta_B)\left(1 - e_{dS}^{(A)}(\eta_A, \eta_B)\right), \quad S = X, Z, \tag{3.8}$$

where $e_{dS}^{(A)}$ and $e_{dS}^{(B)}$, respectively, represent the misalignment probabilities for Alice's and Bob's memories, for basis $S = X, Z$, at loading probabilities η_A and η_B and are given by equations (D.2) and (D.5). The above equation accounts for the fact that if the state of both memories are flipped, Alice and Bob will still share identical key bits. We assume that the BSM module is balanced and does not have any setup misalignment.

Note that in equation (3.8), because of no dephasing errors for the Z eigenstates, e_{dZ}^{QM} is independent of N_A and N_B, whereas e_{dX}^{QM} is a function of them. The approximation in equation (3.7) assumes $\mathrm{E}\{e_{dX}^{\mathrm{QM}}\eta_{mA}\eta_{mB}\} \approx \mathrm{E}\{e_{dX}^{\mathrm{QM}}\}\mathrm{E}\{\eta_{mA}\eta_{mB}\}$, which is valid when $T_1 \gg T_2$, to give a more readable final result.

Equation (3.8) can also be used in the case of indirectly heralding QMs as explained in appendix D. The main idea is to use the analogy of each leg in figure 1(b) with the original MDI-QKD in figure 1(c).

3.2. Key rate for decoy states

Suppose Alice and Bob use a decoy-state scheme with average photon numbers μ and ν, respectively, for the two main signal intensities, and infinitely many auxiliary decoy states. The secret key generation rate, in the limit of infinitely long key, is then given by

$$R_{\mathrm{QM}} = R_S\left[Q_{11}^{\mathrm{QM}}\left(1 - h\left(e_{11;X}^{\mathrm{QM}}\right)\right) - fQ_{\mu\nu;Z}^{\mathrm{QM}}h\left(E_{\mu\nu;Z}^{\mathrm{QM}}\right)\right], \tag{3.9}$$

where

$$Q_{\mu\nu;Z}^{\mathrm{QM}} = \frac{1}{N_L\left(\eta_{\mu A}, \eta_{\nu B}\right) + N_r}Y_{11}\left(\eta_m, \eta_m'\right) \tag{3.10}$$

is the rate at which both memories are loaded, by Alice (Bob) sending a coherent state in the Z basis with μ (ν) average number of photons, and a successful BSM is achieved. In the case of directly heralding memories,

$$\eta_{\mu A} = 1 - e^{-\eta_{\mathrm{ch}}(L_A)\eta_w\mu - \eta_w p_{\mathrm{BG}}} \text{ and } \eta_{\mu B} = 1 - e^{-\eta_{\mathrm{ch}}(L_B)\eta_w\nu - \eta_w p_{\mathrm{BG}}} \tag{3.11}$$

are the probabilities for successful loading of Alice and Bob's QMs with coherent-state sources. Similarly,

$$E_{\mu\nu;Z}^{\mathrm{QM}} = e_{11;Z}\left(\eta_m, \eta_m', e_{dZ}^{\mathrm{QM}}\left(\eta_{\mu A}, \eta_{\nu B}\right)\right) \tag{3.12}$$

is the QBER in the Z basis, and

$$Q_{11}^{\mathrm{QM}} = Q_{\mu\nu;Z}^{\mathrm{QM}}\frac{\eta_{1A}\eta_{1B}}{\eta_{\mu A}\eta_{\nu B}}\mu\nu e^{-\mu-\nu} \tag{3.13}$$

is the contribution of single-photon states in the gain term of equation (3.10).

Similar to the treatment in the previous subsection, one can find or approximate the above terms in the case of indirectly heralding memories as well. For the sake of brevity, we leave this extension to the reader.

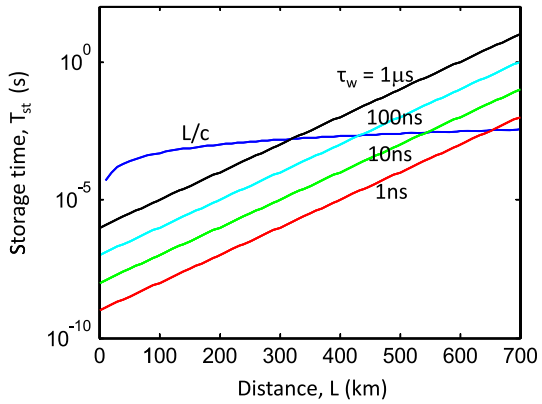

Figure 3. Average required storage time, T_{st}, versus distance, in our scheme, for different repetition rates $1/\tau_w$. As compared to that of a probabilistic quantum repeater, labelled by L/c, where $c = 2 \times 10^8$ m s^{-1} is the speed of light in optical fibre, our scheme requires lower coherence times up to a certain distance. The crossover distance at $\tau_w = 1\,\mu$s is over 300 km and at $\tau_w = 1$ ns is nearly 700 km. In all curves, $\eta_w = \eta_d = \eta_{\text{ent}} = 1$ and $p_{\text{BG}} = 0$.

Apart from all additional parameters considered in our model as compared to [17], our treatment of the decoy-state QKD is different from that of [17] in the way that QMs are modelled. In our work, we assume QMs store qubits, which while is not necessarily an exact model, it often serves a good first-order approximation to the reality. In [17], however, QMs are assumed to be able to store number states. This assumption cannot be applied to certain QMs, such as single trapped atoms or ions, that can only store one photon.

3.3. Storage time

To get some insight into the working of our system, in this section, we simulate the achievable rates assuming $L_A = L_B = L/2$. The average number of trials to load both memories from equation (C.3) is then given by [65]

$$N_L(\eta, \eta) = \frac{3 - 2\eta}{\eta(2 - \eta)} \approx \frac{3}{2} \cdot \frac{1}{\eta}, \text{ for } \eta \ll 1, \tag{3.14}$$

where η is the probability of successfully loading a QM at distance $L/2$, approximately, given by $\eta_{\text{QM}} \exp(-(L/2)/L_{\text{att}})$, where $\eta_{\text{QM}} = \eta_w$ for directly heralding memories, and $\eta_{\text{QM}} = \eta_{\text{ent}}\eta_d^2$ for indirectly heralding QMs. Similarly, the average required storage time, from equation (C.5), is given by

$$T_{st} = \text{E}\left\{ \left| N_A - N_B \right| \right\} T = \frac{2(1 - \eta)T}{\eta(2 - \eta)} \approx \frac{T}{\eta}, \text{ for } \eta \ll 1, \tag{3.15}$$

which is similar to the result reported in [17].

The secret key generation rate in equations (3.1) and (3.9) is proportional to the pulse generation rate $R_S = 1/T$ at the encoder. To maximize R_S, we choose $T = \tau_w$, throughout this section and next, resulting in $T_{st} \approx \tau_w/\eta$. Figure 3 compares T_{st} with the required storage time in multi-memory probabilistic quantum repeaters [31], L/c, where c is the speed of light in the channel. It can be seen that our scheme offers lower required coherence times until a certain

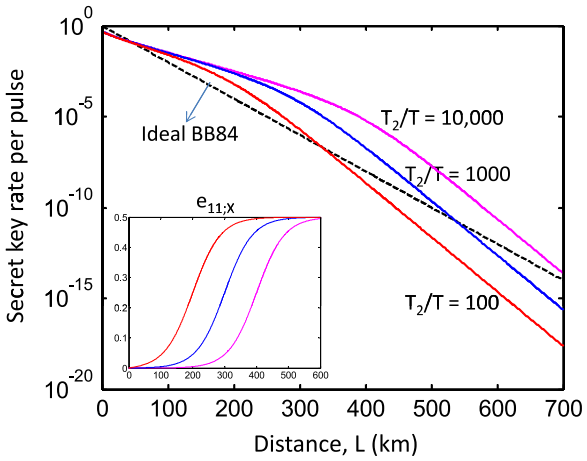

Figure 4. Secret key generation rate per pulse for the heralded scheme of figure 1(a) for different values of T_2/T using single-photon sources. The dashed line represents the ideal efficient BB84 case. Unless explicitly mentioned, all other parameters assume their ideal values: $T_1 \to \infty$, $\eta_w = \eta_{r0} = \eta_d = 1$, $\gamma_{\rm BG} = \gamma_{\rm dc} = 0$, $e_{dA} = e_{dB} = 0$, and $\tau_r = 0$.

distance. With fast memories of shorter than 10 ns of access time, this crossover distance could be longer than 500 km. With such memories, the required coherence time at 300 km is roughly 1 μs, or lower, as compared to over 1 ms for probabilistic quantum repeaters.

It is worth mentioning that the possible advantage of requiring low coherence times is only achievable for systems with nesting level one, i.e., with one stage of entanglement swapping. Unlike quantum repeaters, our protocol, in terms of its timing, is not scalable to higher nesting levels. Nevertheless, even with only one entanglement swapping stage, our protocol can outperform conventional QKD schemes in terms of rate-versus-distance behaviour, and, more importantly, this can possibly be achieved with existing technology for QMs. We explore this and other aspects of our scheme in the next section.

4. Numerical results

In this section, we study the impact of various parameters on the secret key generation rate of our scheme. All results have been obtained assuming the symmetric setup described in (3.3), $\tau_w = T, f = 1.16$, $c = 2 \times 10^8$ m s^{-1}, and 0.2 dB per km of loss in the channel. We also compare our scheme with the efficient BB84 and MDI-QKD protocols, whose secret key generation rates are, respectively, summarized in appendices A and B.

4.1. Coherence time

In this section, we discuss the effects of memory dephasing on the secret key generation rate. As mentioned before, while our scheme in figure 1(a) is particularly resilient to dark count errors, it still suffers from memory errors. Figure 4 demonstrates the secret key generation rate per pulse at different coherence times for the scheme of figure 1(a). A finite coherence time is the only source of nonideality considered in this figure. Since, in our model, the dephasing process only affects the diagonal basis, $e_{11;Z}^{\rm QM} = 0$ at all distances; hence $R_{\rm QM} \propto 1 - h(e_{11;X}^{\rm QM})$ remains always

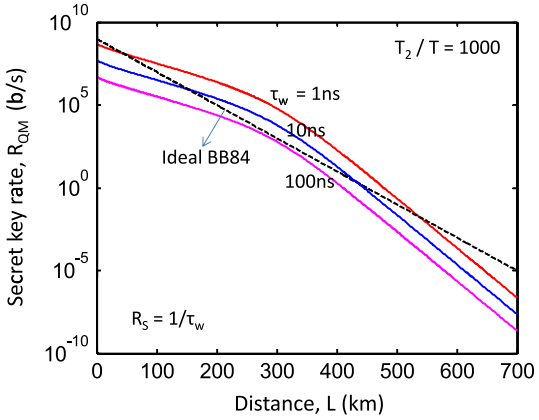

Figure 5. Secret key generation rate for different values of τ_w at $T_2/T = 1000$ using single-photon sources. The dashed line represents the ideal efficient BB84 case at $R_S = 1$ G pulse s^{-1}. Unless explicitly mentioned, all other parameters assume their ideal values: $T_1 \to \infty$, $\eta_w = \eta_{r0} = \eta_d = 1$, $\gamma_{BG} = \gamma_{dc} = 0$, $e_{dA} = e_{dB} = 0$, and $\tau_r = 0$.

positive. The rate is initially proportional to $\exp(-(L/2)/L_{att})$, and with low values of $e_{11;X}^{QM}$ for short distances, our scheme beats the BB84 case depicted by the dashed line. Note that, because of the partial BSM in figure 2, the initial key rate at $L = 0$ for our scheme is lower than that of BB84. At large distances, however, the dephasing process becomes significant and results in $e_{11;X}^{QM}$ approaching 1/2; see the inset. Subsequently, R_{QM} decays with a faster slope and at some point becomes lower than what one can achieve with an ideal BB84 system. The window between the two crossing points on each curve is the range where our scheme, can, in principle, beat a noise-free BB84 system. This window is larger for QMs with longer coherence times.

In [17], authors look at the minimum required coherence time to achieve nonzero key rates, assuming $e_{11;X}^{QM} = e_{11;Z}^{QM}$ within their model of decoherence. Although the models used for decoherence in our work and [17] are different, $e_{11;X}^{QM}$ has a similar behaviour in both cases. In our case, however, the transition from 0 to 1/2 is smoother than that of [17]. This is expected as the model in [17] is an abrupt good–bad model for the memory. A consequence of this difference is that the minimum required coherence time is then higher in our case, which highlights the importance of the more accurate model we have used for decoherence. The comparison in figure 4 assumes that the source rate R_S is the same for both the BB84 protocol and our scheme. In our scheme, however, R_S depends on the writing time of the memories. Figure 5 shows the secret key generation rate for the scheme of figure 1(a) at a fixed value of $T_2/T = 1000$, but for several values of $T = \tau_w = 1/R_S$. The BB84 system is run at a fixed rate of 1 GHz. Again, we assume that the only source of nonideality is memory dephasing. It can be seen that slow memories with writing times of 100 ns, or higher, can hardly compete with an ideal BB84 system. The two orders of magnitude lost because of the lower repetition rate cannot be compensated within the first 300 km. It is still possible to beat the BB84 case, at long distances, if memories have higher coherence times.

4.2. Realistic examples

It is interesting to see if any of the existing technologies for quantum devices can be employed in our scheme to beat conventional QKD systems. Figure 6 makes such a comparison between

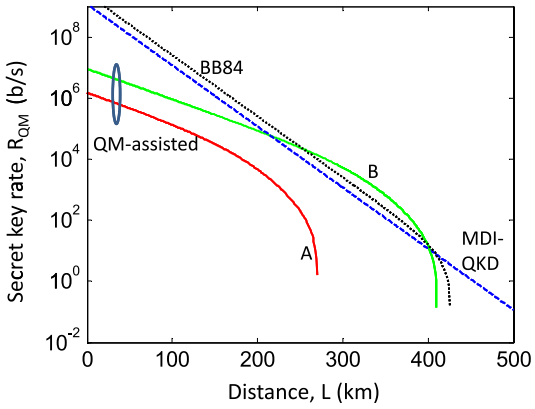

Figure 6. Secret key generation rate for single-photon BB84 (dotted), MDI-QKD (dashed), and our indirectly heralding scheme of figure 1(b) (solid) at practical parameter values. In all curves, $\eta_d = 0.93$, $\gamma_{\rm dc} = 1/{\rm s}$, $\gamma_{\rm BG} = 0$, and $e_{dA} = e_{dB} = 0.005$. For BB84 and MDI-QKD, $R_S = 3.3$ G pulse s^{-1}, similar to $R_S = 1/\tau_w$, in our scheme. For our scheme, we have used some of the experimental parameters reported in [44]. For the curve labelled A, $\eta_{\rm ent} = 0.05$, $\eta_{r0} = 0.3$, $T_1 = T_2 = 4\ \mu$s, and $\tau_w = \tau_r = \tau_p = 300$ ps. It is assumed that there is no multiple excitations in the QMs. For the curve labelled B, everything is the same except that $\eta_{r0} = 0.73$ and $T_1 = T_2 = 100\ \mu$s.

BB84, MDI-QKD, and memory-assisted MDI-QKD for particular experimental parameters. We have chosen our QM parameters based on the two lessons learned from figures 4 and 5: the QM needs to have a high bandwidth-storage product (T_2/τ_w) on the order of 1000 or higher, and, it also needs to be fast, with writing times on the order of nanoseconds. Both these criteria are met for the QM used in [44], which particularly offers fast reading and writing with 300 ps long pulses at a storage time of around 4 μs. The employed memory in this experiment is an atomic ensemble, which fits our indirectly heralding scheme of figure 1(b). We should, however, be careful with multiple excitations in this case, which are not considered in our model. We therefore assume that, by driving this memory with short pulses, one can ideally generate the jointly entangled state in equation (2.1) between the memory and a photon [39], where, in this case, $|s_H\rangle$ and $|s_V\rangle$ are, respectively, the corresponding symmetric collective excited states to horizontal and vertical polarizations [15, 37]. By keeping the entangling efficiency low at $\eta_{\rm ent} = 0.05$, here, we try to keep the effect of multiple excitations in such memories low [35, 66, 64]; further analysis is, however, required to fully account for such effects [45]. We also assume that $T_2 = T_1$ and use the state-of-the-art single-photon detectors with $\eta_d = 0.93$ at $\gamma_{\rm dc} = 1$ count per second and 150 ps of time resolution [67] for all systems.

We consider two sets of parameter values for our employed QM in figure 6. In the first set, corresponding to the curve labelled A on the figure, we use the same numerical values as reported in [44], that is, $\eta_{r0} = 0.3$, $T_1 = 4\ \mu$s, and $\tau_w = \tau_r = \tau_p = 300$ ps. We, however, assume that $R_S = 1/\tau_w$, which is much faster than the repetition rate used in [44]. In the curve labeled B, we improve the performance by assuming $\eta_{r0} = 0.73$, which is what another group has obtained for a similar type of memory [39], and $T_1 = T_2 = 100\ \mu$s, which is attainable by improving magnetic shielding [68]. It can be seen that, whereas the current QM employed in [44] is short of beating either of no-memory systems, our slightly boosted system, in curve B, outperforms

both systems at over roughly 200 km. The cut-off distance in curve B is about 400 km, which is mainly because of memory decoherence, and it can be improved by using memories with longer coherence times. This implies that with slightly improving some experimental parameters, we would be able to employ realistic QMs to improve the performance of practical quantum communication setups. We remark that the example QM chosen in figure 6 is not necessarily the only option, and improved versions of other types of memories can potentially offer the same performance [40, 61, 69–73].

What we have proposed here is an initial step toward improving the performance of QKD systems by using QMs. In particular, we have shown how technologically close we are to beating a direct, no-memory, QKD link in terms of the achievable rate at certain long distances. Our scheme is not, however, scalable to arbitrarily long distances. For that matter, full quantum repeaters would eventually be needed. A possible roadmap for the development of such systems would pass through probabilistic, and then deterministic, and eventually no-memory versions of quantum repeaters [12–14]. It is hard to make a fair comparison between all these and our scheme, as the required resources in each case are different. Some studies have nevertheless compared different repeater schemes under certain assumptions [64, 74]. It is only the future, in the end, that proves which system, and at what price, can be implemented over the course of time.

5. Conclusions

By combining ideas from quantum repeaters and MDI-QKD, we proposed a QKD scheme that relied on QMs. While offering the same rate-versus-distance improvement that quantum repeaters promise, the coherence-time requirements for the QMs employed in our scheme could be less stringent than that of a general single-mode probabilistic quantum repeater system. That would provide a window of opportunity for building realistic QKD systems that beat conventional no-memory QKD schemes by only relying on existing technologies for QMs. In our work, we showed that how close some experimental setups would be in achieving this objective. Our protocol acts as a middle step on the roadmap to long-distance quantum communication systems.

Acknowledgments

This research was supported in part by the European Community's Seventh Framework Programme Grant Agreement 277110, the UK Engineering and Physical Sciences Research Council Grant No. EP/J005762/1, the National Basic Research Program of China Grants No. 2011CBA00300 and No. 2011CBA00301, the 1000 Youth Fellowship program in China, the NSERC Discovery Program, and the DARPA Quiness Program.

Appendix A. BB84 key rate analysis

In this appendix we summarize the secret key generation rate for the efficient BB84 protocol [47] shown in figure A1. In figure A1, Alice is the transmitter sending pulses in either the rectilinear or diagonal basis and Bob is the receiver, which decodes the message. They communicate through an optical channel of distance L.

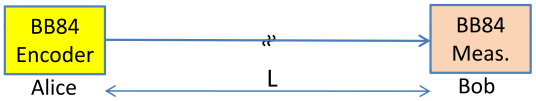

Figure A1. The setup for the BB84 protocol.

With a clock rate of R_S, the secret key generation rate is lower bounded by

$$R_{\mathrm{BB84}} = R_S Y_1[1 - h(e_1) - fh(e_1)], \tag{A.1}$$

in the single-photon case, and

$$R_{\mathrm{BB84}} = R_S\left[Q_1\left(1 - h\left(e_1\right)\right) - fQ_\mu h\left(E_\mu\right)\right], \tag{A.2}$$

in the (infinitely many) decoy-state case, where μ is the average number of photons for signal states, which is dominantly used. In equation (A.1), Y_1 is the yield of single photons, or the probability that Bob gets a click on his measurement devices assuming that Alice has sent exactly one photon, and is given by

$$Y_1 = Y_C + Y_E = 1 - (1 - \eta)(1 - p_{\mathrm{dc}})^2, \tag{A.3}$$

where $\eta = \eta_{\mathrm{ch}}(L)\eta_d$, and

$$Y_C = (1 - p_{\mathrm{dc}}/2)(\eta + (1 - \eta)p_{\mathrm{dc}}) \text{ and } Y_E = p_{\mathrm{dc}}[(1 - \eta)(1 - p_{\mathrm{dc}}/2) + \eta/2] \tag{A.4}$$

correspond, respectively, to the terms that, in the absence of misalignment, result in identical (Correct) versus nonidentical (Error) bits shared by Alice and Bob. The QBER, e_1, which is the same for both bases, is given by

$$\begin{aligned} e_1 Y_1 &= e_d Y_C + (1 - e_d) Y_E = e_0 Y_1 - (e_0 - e_d)(Y_C - Y_E) \\ &= e_0 Y_1 - (e_0 - e_d)\eta(1 - p_{\mathrm{dc}}), \end{aligned} \tag{A.5}$$

where $e_0 = 1/2$ and $e_d = e_{dA} + e_{dB}$ is the total misalignment probability for the channel.

Similarly, in equation (A.2),

$$\begin{aligned} Q_1 &= Y_1 \mu e^{-\mu}, \\ Q_\mu &= Q_C + Q_E = 1 - e^{-\eta\mu}(1 - p_{\mathrm{dc}})^2, \\ Q_C &= (1 - p_{\mathrm{dc}}/2)(1 - e^{-\eta\mu} + e^{-\eta\mu} p_{\mathrm{dc}}), \\ Q_E &= p_{\mathrm{dc}}[e^{-\eta\mu}(1 - p_{\mathrm{dc}}/2) + (1 - e^{-\eta\mu})/2], \end{aligned} \tag{A.6}$$

are the corresponding gain terms [46], and

$$E_\mu Q_\mu = e_0 Q_\mu - (e_0 - e_d)(1 - e^{-\eta\mu})(1 - p_{\mathrm{dc}}),\ e_0 = 1/2, \tag{A.7}$$

gives the QBER.

Appendix B. MDI-QKD key rate analysis

The secret key generation rate for the MDI-QKD scheme of figure 1(c) is lower bounded by [28]

$$R_{\mathrm{MDI-QKD}} = R_S Y_{11}\left[1 - h\left(e_{11;X}\right) - fh\left(e_{11;Z}\right)\right], \tag{B.1}$$

in the single-photon case, and

$$R_{\mathrm{MDI-QKD}} = R_S\left[Q_{11}\left(1 - h\left(e_{11;X}\right)\right) - fQ_{\mu\nu;Z}\,h\left(E_{\mu\nu;Z}\right)\right], \tag{B.2}$$

in the decoy-state case, where μ (ν) is the average number of photons for signal states sent by Alice (Bob). Here, Q_{11} is the probability of generating one photon by the sources and obtaining a successful BSM and is given by

$$Q_{11}(\eta_a, \eta_b) = \mu\nu e^{-\mu-\nu} Y_{11}(\eta_a, \eta_b) \tag{B.3}$$

where $\eta_a = \eta_{\mathrm{ch}}(L_A)\eta_d$ and $\eta_b = \eta_{\mathrm{ch}}(L_B)\eta_d$ are transmission coefficients of each leg in figure 1(c), and [28]

$$\begin{aligned}
Y_{11}(\eta_a, \eta_b) &= (1 - p_{\mathrm{dc}})^2\left[\frac{\eta_a\eta_b}{2} + (2\eta_a + 2\eta_b - 3\eta_a\eta_b)p_{\mathrm{dc}} + 4(1 - \eta_a)(1 - \eta_b)p_{\mathrm{dc}}^2\right],\\
e_{11;X}(\eta_a, \eta_b, e_d)Y_{11}(\eta_a, \eta_b) &= e_0 Y_{11}(\eta_a, \eta_b) - (e_0 - e_d)(1 - p_{\mathrm{dc}})^2\eta_a\eta_b/2,\\
e_{11;Z}(\eta_a, \eta_b, e_d)Y_{11}(\eta_a, \eta_b) &= e_0 Y_{11}(\eta_a, \eta_b) - (e_0 - e_d)(1 - p_{\mathrm{dc}})^2(1 - 2p_{\mathrm{dc}})\eta_a\eta_b/2
\end{aligned} \tag{B.4}$$

with e_d being the total misalignment probability. In the scheme of figure 1(c), $e_d = e_{dA}(1 - e_{dB}) + e_{dB}(1 - e_{dA})$. Similarly, using the results obtained in [28], we have

$$\begin{aligned}
Q_{\mu\nu;Z} &= Q'_C + Q'_E\\
E_{\mu\nu;Z}Q_{\mu\nu;Z} &= e_d Q'_C + (1 - e_d)Q'_E,
\end{aligned} \tag{B.5}$$

where

$$\begin{aligned}
Q'_C &= 2(1 - p_{\mathrm{dc}})^2 e^{-\mu'/2}\left[1 - (1 - p_{\mathrm{dc}})e^{-\eta_a\mu_a/2}\right]\left[1 - (1 - p_{\mathrm{dc}})e^{-\eta_b\mu_b/2}\right]\\
Q'_E &= 2p_{\mathrm{dc}}(1 - p_{\mathrm{dc}})^2 e^{-\mu'/2}[I_0(2x) - (1 - p_{\mathrm{dc}})e^{-\mu'/2}].
\end{aligned} \tag{B.6}$$

In above equations, $I_0(x)$ is the modified Bessel function of the first kind and

$$x = \sqrt{\eta_a\mu\eta_b\nu}/2, \tag{B.7}$$

$$y = (1 - p_{\mathrm{dc}})e^{-\frac{1}{4}(\eta_a\mu + \eta_b\nu)}, \tag{B.8}$$

$$\mu' = \eta_a\mu + \eta_b\nu. \tag{B.9}$$

Appendix C. Loading process

The loading process in the setups of figures 1(a) and (b) are probabilistic ones, with two geometric random variables N_A and N_B playing the major role. Suppose the success probability for each loading attempt corresponding to these random variables is, respectively, given by η_A and η_B. Then, we obtain the following probability distribution for $|N_A - N_B|$:

$$\Pr\left(\left|N_A - N_B\right| = k\right) = \left[\left(1 - \eta_A\right)^k + \left(1 - \eta_B\right)^k\right]P_0,\ k > 0, \tag{C.1}$$

where

$$P_0 = \Pr(N_A = N_B) = \frac{\eta_A \eta_B}{\eta_A + \eta_B - \eta_A \eta_B}. \tag{C.2}$$

Using the above expressions, we then obtain

$$\begin{aligned} N_L(\eta_A, \eta_B) &= \mathrm{E}\{\max(N_A, N_B)\} \\ &= \frac{1}{2}\mathrm{E}\left\{|N_A - N_B| + N_A + N_B\right\} \\ &= \frac{1}{2}\left[\frac{\eta_A(1-\eta_B)}{\eta_B(\eta_A + \eta_B - \eta_A\eta_B)} + \frac{\eta_B(1-\eta_A)}{\eta_A(\eta_A + \eta_B - \eta_A\eta_B)} + \frac{1}{\eta_A} + \frac{1}{\eta_B}\right]. \end{aligned} \tag{C.3}$$

Moreover,

$$\mathrm{E}\left\{\exp\left(-|N_A - N_B|\delta\right)\right\} = P_0\left[\frac{1}{1 - e^{-\delta}(1-\eta_A)} + \frac{1}{1 - e^{-\delta}(1-\eta_B)} - 1\right] \tag{C.4}$$

and the average storage time, T_{st}, is given by

$$T_{st} = \mathrm{E}\left\{|N_A - N_B|\right\} T = \frac{\eta_A(1-\eta_B)T}{\eta_B(\eta_A + \eta_B - \eta_A\eta_B)} + \frac{\eta_B(1-\eta_A)T}{\eta_A(\eta_A + \eta_B - \eta_A\eta_B)}. \tag{C.5}$$

Finally, we can show that

$$\Pr\{N_A \geqslant N_B\} = \frac{\eta_B}{1 - (1-\eta_A)(1-\eta_B)} = 1 - \Pr\{N_A < N_B\} \tag{C.6}$$

and

$$\begin{aligned} S_{A<B}(\delta) &\equiv \sum\nolimits_{1=n_a<n_b}^{\infty} \Pr\{N_A = n_a, N_B = n_b\} \exp\left[(n_a - n_b)\delta\right] \\ &= \frac{\eta_A \eta_B (1-\eta_B) e^{-\delta}}{[1 - (1-\eta_B)e^{-\delta}][1 - (1-\eta_A)(1-\eta_B)]}. \end{aligned} \tag{C.7}$$

Appendix D. Misalignment parameters

In this appendix, we obtain the misalignment probability for each of the setups in figures 1(a) and (b). Let us first consider the directly heralding memory case in the Z basis and assume loading probabilities η_A and η_B for Alice's and Bob's memories. Suppose the legitimate state is $|s_H\rangle\langle s_H|$. Assuming setup misalignment probabilities e_{dK}, $K = A, B$, for leg K of figure 1(a), in the absence of background counts, the stored state in memory K will become $\rho_{d0} = (1 - e_{dK})|s_H\rangle\langle s_H| + e_{dK}|s_V\rangle\langle s_V|$. Now, including the background counts, the memory state will become

$$\rho_{dZ} = \left[1 - e_{\mathrm{BG}}^{(K)}\right]\rho_{d0} + e_{\mathrm{BG}}^{(K)} \frac{|s_H\rangle\langle s_H| + |s_V\rangle\langle s_V|}{2}, \tag{D.1}$$

where $e_{\mathrm{BG}}^{(K)} = \frac{1-e^{-\eta_K p_{\mathrm{BG}}}}{\eta_K}$, $K = A, B$, is the probability that our memory has been loaded by a background (unpolarized) photon conditioned on a successful loading. The total misalignment probability in the Z basis for the Alice's and Bob's memory is then given by

$$e_{dZ}^{(K)} = e_{dK}\left(1 - e_{\mathrm{BG}}^{(K)}\right) + e_{\mathrm{BG}}^{(K)}/2,\ K = A, B, \text{ for directly heralding QMs.} \tag{D.2}$$

Now, let's assume the legitimate state, in the X basis, is $|s_+\rangle\langle s_+|$, where $|s_\pm\rangle = (|s_H\rangle \pm |s_V\rangle)/\sqrt{2}$. Right after a successful loading, the state of the memory is then given by

$$\rho_{dX}(0) = \left[1 - e_{\mathrm{BG}}^{(K)}\right]\rho'_{d0} + e_{\mathrm{BG}}^{(K)}\frac{|s_H\rangle\langle s_H| + |s_V\rangle\langle s_V|}{2} \tag{D.3}$$

where $\rho'_{d0} = (1 - e_{dK})|s_+\rangle\langle s_+| + e_{dK}|s_-\rangle\langle s_-|$. If memory A is the late memory, i.e., if $N_A \geqslant N_B$, then there will be no dephasing errors, in which case, $e_{dX}^{(A)} = e_{dZ}^{(A)}$. If it is the early memory, however, the dephasing operation in equation (2.3) will act on $\rho_{dX}(0)$ to give us

$$\rho_{dX}(t) = \left[1 - e_{\mathrm{BG}}^{(K)}\right]\rho'_{d0}(t) + e_{\mathrm{BG}}^{(K)}\frac{|s_H\rangle\langle s_H| + |s_V\rangle\langle s_V|}{2}, \tag{D.4}$$

where
$\rho'_{d0}(t) = [(1 - e_{dK})p(t) + e_{dK}(1 - p(t))]|s_+\rangle\langle s_+| + [e_{dK}p(t) + (1 - e_{dK})(1 - p(t))]|s_-\rangle\langle s_-|$.
The misalignment probability is then given by

$$e_{dX}^{(K)} = e_{dZ}^{(K)} + \beta_A e_{\mathrm{deph}}^{(K)}, \tag{D.5}$$

where $\beta_K = (1 - 2e_{dK})(1 - e_{\mathrm{BG}}^{(K)})$, $K = A, B$, and

$$e_{\mathrm{deph}}^{(A)} = \begin{cases} 0 & N_A \geqslant N_B \\ (1/2)\left[1 - \exp\left(-|N_A - N_B|T/T_2\right)\right] & N_A < N_B \end{cases}, \tag{D.6}$$

where N_A and N_B are geometric random variables with success probabilities η_A and η_B. By averaging over these variables, we obtain

$$\mathrm{E}\left\{e_{dX}^{(A)}\right\} = e_{dZ}^{(A)} + \beta_A \mathrm{E}\left\{e_{\mathrm{deph}}^{(A)}\right\}, \tag{D.7}$$

where

$$\mathrm{E}\left\{e_{\mathrm{deph}}^{(A)}\right\} = [\Pr\{N_A < N_B\} - S_{A<B}(T/T_2)]/2, \tag{D.8}$$

which can be obtained from equations (C.6) and (C.7). One can obtain similar expressions for $e_{dX}^{(B)}$ by swapping A and B in equations (D.6)–(D.8).

To calculate $\mathrm{E}\{e_{dX}^{\mathrm{QM}}\}$ from equation (3.8), the final remaining term is given by

$$\mathrm{E}\left\{e_{dX}^{(A)}e_{dX}^{(B)}\right\} = e_{dZ}^{(A)}e_{dZ}^{(B)} + \beta_A \mathrm{E}\left\{e_{\mathrm{deph}}^{(A)}\right\}e_{dZ}^{(B)} + \beta_B \mathrm{E}\left\{e_{\mathrm{deph}}^{(B)}\right\}e_{dZ}^{(A)}, \tag{D.9}$$

where we used the fact that $e_{\mathrm{deph}}^{(A)}e_{\mathrm{deph}}^{(B)} = 0$, as one of the two terms is always zero regardless of the values of N_A and N_B.

In the case of indirectly heralding QMs, we assume that each erroneous click on the side BSMs will effectively result in a flip to the corresponding QM state, and can also be modeled as misalignment. This assumption is valid at low distances where majority of errors are caused by the setup misalignment. We then obtain

$$e_{dZ}^{(K)} = e_{11;Z}(\eta_d\eta_{\rm ch}(L_K), \eta_d\eta_{\rm ent}, e_{dK}),\ \mathrm{K} = \mathrm{A}, \mathrm{B}, \tag{D.10}$$

for indirectly heralding QMs, where $e_{11;Z}$ can be calculated from equation (B.4) at an equivalent dark count rate of $\gamma_{\rm dc} + \eta_d\gamma_{\rm BG}/2$. At long distances, most errors originate from dark counts or background photons, whose effective misalignment effect will approach half of $e_{11;Z}$ in the above equation. As a conservative assumption, we use the expression in equation (D.10) for all distances.

All other terms in equations (3.7) and (3.8) can be obtained following the same expressions in eqations (D.5)–(D.9) at $\beta_K = 1 - 2e_{dZ}^{(K)}$, for $K = A, B$, and using equation (D.10) for $e_{dZ}^{(K)}$.

References

[1] www.idquantique.com

[2] Wang S, Wei C, Guo J-F, Yin Z-Q, Li H-W, Zhou Z, Guo G-C and Han Z-F 2012 2 GHz clock quantum key distribution over 260 km of standard telecom fiber *Opt. Lett.* **37** 1008–10

[3] Sasaki M *et al* 2011 Field test of quantum key distribution in the Tokyo QKD Network *Opt. Express* **19** 10387–409

[4] Peev M *et al* 2009 The SECOQC quantum key distribution network in Vienna *New J. Phys.* **11** 075001

[5] Choi I, Young R J and Townsend P D 2011 Quantum information to the home *New J. Phys.* **13** 063039

[6] Patel K A, Dynes J F, Choi I, Sharpe A W, Dixon A R, Yuan Z L, Penty R V and Shields A J 2012 Coexistence of high-bit-rate quantum key distribution and data on optical fiber *Phys. Rev.* X **2** 041010

[7] Rubenok A, Slater J A, Chan P, Lucio-Martinez I and Tittel W 2013 Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks *Phys. Rev. Lett.* **111** 130501

[8] da Silva F T, Vitoreti D, Xavier G B, do Amaral G C, Temporão G P and von der Weid J P 2013 Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits *Phys. Rev.* A **88** 052303

[9] Liu Y *et al* 2013 Experimental measurement-device-independent quantum key distribution *Phys. Rev. Lett.* **111** 130502

[10] Tang Z, Liao Z, Xu F, Qi B, Qian L and Lo H-K 2013 Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution arXiv:1306.6134 [quant-ph]

[11] Briegel H-J, Dür W, Cirac J I and Zoller P 1998 Quantum repeaters: the role of imperfect local operations in quantum communication *Phys. Rev. Lett.* **81** 5932–5

[12] Munro W J, Stephens A M, Devitt S J, Harrison K A and Nemoto K 2012 Quantum communication without the necessity of quantum memories *Nat. Photon.* **6** 771–81

[13] Azuma K, Tamaki K and Lo H-K 2013 All photonic quantum repeaters arXiv:1309.7207 [quant-ph]

[14] Muralidharan S, Kim J, Lütkenhaus N, Lukin M D and Jiang L 2013 Ultrafast and fault-tolerant quantum communication across long distances arXiv:1310.5291 [quant-ph]

[15] Duan L-M, Lukin M D, Cirac J I and Zoller P 2001 Long-distance quantum communication with atomic ensembles and linear optics *Nature* **414** 413–8

[16] Panayi C and Razavi M 2012 Measurement device independent quantum key distribution with imperfect quantum memories *Tech. Digest, 6th Int. Conf. on Quantum, Nano and Micro Technologies (Rome, Italy)*

[17] Abruzzo S, Kampermann H and Bruß D 2014 Measurement-device-independent quantum key distribution with quantum memories *Phys. Rev.* A **89** 012301

[18] Lo H-K, Curty M and Qi B 2012 Measurement-device-independent quantum key distribution *Phys. Rev. Lett.* **108** 130503

[19] Qi B, Fred Fung C-H, Lo H-K and Ma X 2007 Time-shift attack in practical quantum cryptosystems *Quantum Inf. Comput.* **7** 073
[20] Zhao Y, Fung C-H F, Qi B, Chen C and Lo H-K 2008 Experimental demonstration of time-shift attack against practical quantum key distribution systems *Phys. Rev.* A **78** 042333
[21] Fred Fung C-H, Qi B, Tamaki K and Lo H-K 2007 Phase-remapping attack in practical quantum-key-distribution systems *Phys. Rev.* A **75** 032314
[22] Xu F, Qi B and Lo H-K 2010 Experimental demonstration of phase-remapping attack in a practical quantum key distribution system *New J. Phys.* **12** 113026
[23] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 Hacking commercial quantum cryptography systems by tailored bright illumination *Nat. Photon.* **4** 686–9
[24] Wiechers C, Lydersen L, Wittmann C, Elser D, Skaar J, Marquardt C, Makarov V and Leuchs G 2011 After-gate attack on a quantum cryptosystem *New J. Phys.* **13** 013043
[25] Weier H, Krauss H, Rau M, Fürst M, Nauerth S and Weinfurter H 2011 Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors *New J. Phys.* **13** 073024
[26] Jain N, Wittmann C, Lydersen L, Wiechers C, Elser D, Marquardt C, Makarov V and Leuchs G 2011 Device calibration impacts security of quantum key distribution *Phys. Rev. Lett.* **107** 110501
[27] Biham E, Huttner B and Mor T 1996 Quantum cryptographic network based on quantum memories *Phys. Rev.* A **54** 2651
[28] Ma X and Razavi M 2012 Alternative schemes for measurement-device-independent quantum key distribution *Phys. Rev.* A **86** 062319
[29] Ma X, Fred Fung C-H and Razavi M 2012 Statistical fluctuation analysis for measurement-device-independent quantum key distribution *Phys. Rev.* A **86** 052305
[30] Braunstein S L and Pirandola S 2012 Side-channel-free quantum key distribution *Phys. Rev. Lett.* **108** 130502
[31] Razavi M, Piani M and Lütkenhaus N 2009 Quantum repeaters with imperfect memories: cost and scalability *Phys. Rev.* A **80** 032301
[32] Razavi M, Thompson K, Farmanbar H, Piani Ma and Lütkenhaus N 2009 Physical and architectural considerations in quantum repeaters *Proc. SPIE* **7236** 723603
[33] Razavi M, Lo Piparo N, Panayi C and Bruschi D E 2013 Architectural considerations in hybrid quantum-classical networks (invited paper) *Iran Workshop on Communication and Information Theory (IWCIT) (Tehran, Iran)* pp 1–7
[34] Lloyd S, Shahriar M S, Shapiro J H and Hemmer P R 2001 Long distance, unconditional teleportation of atomic states via complete bell state measurements *Phys. Rev. Lett.* **87** 167903
[35] Razavi M and Shapiro J H 2006 Long-distance quantum communication with neutral atoms *Phys. Rev.* A **73** 042303
[36] Kuzmich A, Bowen W P, Boozer A D, Boca A, Chou C W, Duan L-M and Kimble H J 2003 Generation of nonclassical photon pairs for scalable quantum communication with atomic ensembles *Nature* **423** 731
[37] Chanelière T, Matsukevich D N, Jenkins S D, Lan S-Y, Kennedy T A B and Kuzmich A 2005 Storage and retrieval of single photons transmitted between remote quantum memories *Nature* **438** 833–6
[38] Zhao B, Chen Z-B, Chen Y-A, Schmiedmayer J and Pan J-W 2007 Robust creation of entanglement between remote memory qubits *Phys. Rev. Lett.* **98** 240502
[39] Bao X-H, Reingruber A, Dietrich P, Rui J, Dück A, Strassel T, Li L, Liu N-L, Zhao B and Pan J-W 2012 Efficient and long-lived quantum memory with cold atoms inside a ring cavity *Nat. Phys.* **8** 517–21
[40] Ritter S, Nölleke C, Hahn C, Reiserer A, Neuzner A, Uphoff M, Mücke M, Figueroa E, Bochmann J and Rempe G 2012 An elementary quantum network of single atoms in optical cavities *Nature* **484** 195–200
[41] Bennett C H and Brassard G 1984 Quantum cryptography public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing (Bangalore, India)* (New York: IEEE) pp 175–9

[42] Kuklewicz C E, Fiorentino M, Messin G, Wong F N C and Shapiro J H 2004 High-flux source of polarization-entangled photons from a periodically poled $KTiOPO_4$ parametric down-converter *Phys. Rev.* A **69** 013807
[43] Fiorentino M, Messin G, Kuklewicz C E, Wong F N C and Shapiro J H 2004 Generation of ultrabright tunable polarization entanglement without spatial, spectral, or temporal constraints *Phys. Rev.* A **69** 041801
[44] Reim K F, Michelberger P, Lee K C, Nunn J, Langford N K and Walmsley I A 2011 Single-photon-level quantum memory at room temperature *Phys. Rev. Lett.* **107** 053603
[45] Lo Piparo N and Razavi M Measurement-device-independent quantum key distribution with imperfect sources and memories in preparation
[46] Lo H-K, Ma X and Chen K 2005 Decoy state quantum key distribution *Phys. Rev. Lett.* **94** 230504
[47] Lo H-K, Chau H F and Ardehali M 2005 Efficient quantum key distribution scheme and a proof of its unconditional security *J. Cryptol.* **18** 133–65
[48] Chan P, Slater J A, Lucio-Martinez I, Rubenok A and Tittel W 2013 Modeling a measurement-device-independent quantum key distribution system arXiv:1204.0738 [quant-ph]
[49] Yin Z-Q, Fred Fung C-H, Ma X, Zhang C-M, Li H-W, Chen W, Wang S, Guo G-C and Han Z-F 2013 Measurement-device-independent quantum key distribution with uncharacterized qubit sources *Phys. Rev.* A **88** 062322
[50] Bocquillon E, Couteau C, Razavi M, Laflamme R and Weihs G 2009 Coherence measures for heralded single-photon sources *Phys. Rev.* A **79** 035801
[51] Razavi M, Söllner I, Bocquillon E, Couteau C, Laflamme R and Weihs G 2009 Characterizing heralded single-photon sources with imperfect measurement devices *J. Phys. B: At. Mol. Opt. Phys.* **42** 114013
[52] Peters N A *et al* 2009 Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments *New J. Phys.* **11** 045012
[53] Chapuran T E *et al* 2009 Optical networking for quantum key distribution and quantum communications *New J. Phys.* **11** 105001
[54] Razavi M 2012 Multiple-access quantum key distribution networks *IEEE Trans. Commun.* **60** 3071–9
[55] Beaudry N J, Moroder T and Lütkenhaus N 2008 Squashing models for optical measurements in quantum communication *Phys. Rev. Lett.* **101** 093601
[56] Fred Fung C-H, Chau H F and Lo H-K 2011 Universal squash model for optical communications using linear optics and threshold detectors *Phys. Rev.* A **84** 020303
[57] Kuklinski J R, Gaubatz U, Hioe F T and Bergmann K 1989 Adiabatic population transfer in a three-level system driven by delayed laser pulses *Phys. Rev.* A **40** 6741–4
[58] Razavi M and Shapiro J H 2007 Nonadiabatic approach to entanglement distribution over long distances *Phys. Rev.* A **75** 032318
[59] Simon C, de Riedmatten H, Afzelius M, Sangouard N, Zbinden H and Gisin N 2007 Quantum repeaters with photon pair sources and multimode memories *Phys. Rev. Lett.* **98** 190503
[60] Clausen C, Usmani I, Bussières F, Sangouard N, Afzelius M, de Riedmatten H and Gisin N 2011 Quantum storage of photonic entanglement in a crystal *Nature* **469** 508–11
[61] Saglamyurek E, Sinclair N, Jin J, Slater J A, Oblak D, Bussières F, George M, Ricken R, Sohler W and Tittel W 2011 Broadband waveguide quantum memory for entangled photons *Nature* **469** 512–5
[62] Sinclair N *et al* 2013 A solid-state memory for multiplexed quantum states of light with read-out on demand arXiv:1309.3202 [quant-ph]
[63] Shor P W and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol *Phys. Rev. Lett.* **85** 441
[64] Lo Piparo N and Razavi M 2013 Long-distance quantum key distribution with imperfect devices *Phys. Rev.* A **88** 012332
[65] Collins O A, Jenkins S D, Kuzmich A and Kennedy T A B 2007 Multiplexed memory-insensitive quantum repeaters *Phys. Rev. Lett.* **98** 060502

[66] Amirloo J, Razavi M and Majedi A H 2010 Quantum key distribution over probabilistic quantum repeaters *Phys. Rev.* A **82** 032304
[67] Marsili F *et al* 2013 Detecting single infrared photons with 93% system efficiency *Nat. Photon.* **7** 210–4
[68] Camacho R M, Vudyasetu P K and Howell J C 2009 Four-wave-mixing stopped light in hot atomic rubidium vapour *Nat. Photon.* **3** 103–6
[69] Stute A, Casabone B, Schindler P, Monz T, Schmidt P O, Brandstätter B, Northup T E and Blatt R 2012 Tunable ionphoton entanglement in an optical cavity *Nature* **485** 482
[70] Amari A *et al* 2010 Towards an efficient atomic frequency comb quantum memory *J. Lumin.* **130** 1579–85
[71] Clausen C, Bussières F, Afzelius M and Gisin N 2012 Quantum storage of heralded polarization qubits in birefringent and anisotropically absorbing materials *Phys. Rev. Lett.* **108** 190503
[72] Gündoğan M, Ledingham P M, Almasi A, Cristiani M and de Riedmatten H 2012 Quantum storage of a photonic polarization qubit in a solid *Phys. Rev. Lett.* **108** 190504
[73] Zhou Z-Q, Lin W-B, Yang M, Li C-F and Guo G-C 2012 Realization of reliable solid-state quantum memory for photonic polarization qubit *Phys. Rev. Lett.* **108** 190505
[74] Bratzik S, Abruzzo S, Kampermann H and Bruß D 2013 Quantum repeaters and quantum key distribution: the impact of entanglement distillation on the secret key rate *Phys. Rev.* A **87** 062335