
Article:
Lo Piparo, N and Razavi, M (2013) Long-distance quantum key distribution with imperfect devices. Physical Review A: Atomic, Molecular and Optical Physics, 88 (1). 012332. ISSN 1050-2947

https://doi.org/10.1103/PhysRevA.88.012332

Long-distance quantum key distribution with imperfect devices

Nicoló Lo Piparo and Mohsen Razavi*
School of Electronic and Electrical Engineering, University of Leeds, Leeds, United Kingdom
(Received 5 November 2012; published 30 July 2013)

Quantum key distribution over probabilistic quantum repeaters is addressed. We compare, under practical assumptions, two such schemes in terms of their secret key generation rates per quantum memory. The two schemes under investigation are the one proposed by Duan *et al*. [Nature (London) **414**, 413 (2001)] and that of Sangouard *et al*. [Phys. Rev. A **76**, 050301 (2007)]. We consider various sources of imperfection in both protocols, such as nonzero double-photon probabilities at the sources, dark counts in detectors, and inefficiencies in the channel, photodetectors, and memories. We also consider memory decay and dephasing processes in our analysis. For the latter system, we determine the maximum value of the double-photon probability beyond which secret key distillation is not possible. We also find crossover distances for one nesting level to its subsequent one. We finally compare the two protocols in terms of their achievable secret key generation rates at their optimal settings. Our results specify regimes of operation where one system outperforms the other.

DOI: 10.1103/PhysRevA.88.012332 PACS number(s): 03.67.Bg, 03.67.Dd, 03.67.Hk, 42.50.Ex

I. INTRODUCTION

Despite all practical progress with quantum key distribution (QKD) [1–4], its implementation over long distances remains to be a daunting task. In conventional QKD protocols such as BB84 [5], channel loss and detector noises set an upper bound on the achievable security distance [6]. In addition, the path loss results in an exponential decay of the secret key generation rate with distance. Both of these issues can, in principle, be overcome if one implements entanglement-based QKD protocols [7,8] over quantum repeater systems [9–12]. This approach, however, is not without its own challenges. Quantum repeaters require quantum memory (QM) units that can interact with light and can store their states for sufficiently long times. Moreover, highly efficient quantum gates might be needed to perform two-qubit operations on these QMs [9]. The latter issue has been alleviated, to some extent, by introducing a novel technique by Duan, Lukin, Cirac, and Zoller (DLCZ) [10], in which initial entanglement distribution and swapping, thereafter, rely on probabilistic linear-optic operations. Since its introduction, the DLCZ idea has been extended and a number of new proposals have emerged [13–18]. Such probabilistic schemes for quantum repeaters particularly find applications in QKD systems of mid- to long distances, which makes them worthy of analytical scrutiny. This paper compares DLCZ with one of its favorite successors [17], which relies on single-photon sources (termed SPS protocol, hereafter). Using a general system-level approach, which encompasses many relevant physical sources of imperfections in both systems, we provide a realistic account of their performance in terms of their secret key generation rates per logical memory used. This measure not only quantifies performance, but it also accounts for possible costs of implementation.

The SPS protocol attempts to resolve one of the key drawbacks in the original DLCZ protocol: multiphoton emissions. DLCZ uses atomic ensembles as QMs, which lend themselves to multiphoton emissions. This leads to obtaining not fully entangled states, hence resulting in lower key rates when used for QKD. To tackle this issue, in the SPS protocol, entanglement is distributed by ideally generating single photons, which will either be stored in QMs or directed toward a measurement site. Whereas, in principle, the SPS protocol should not deal with the multiphoton problem, in practice, it is challenging to build on-demand single-photon sources that do not produce any multiphoton components. A fair comparison between the two systems is only possible when one considers different sources of nonidealities in both cases, as we pursue in this paper.

The SPS protocol is one of the many proposed schemes for probabilistic quantum repeaters. In [18] authors provide a review of all such schemes and compare them in terms of the average time that it takes to generate entangled states, of a certain *fidelity*, between two remote memories. Their conclusion is that in the limit of highly efficient memories and detectors, the top three protocols are the SPS protocol and two others that rely on entangled and two photon sources [14,16]. In more practical regimes, however, the SPS protocol seems to have the best performance per memory and/or mode used. In this paper, we therefore focus on the SPS protocol and investigate, under practical assumptions, whether the above conclusion remains valid in the context of QKD systems.

Our work is distinct from previous related work in its focusing on the performance of *QKD* systems over quantum repeaters. In [18], authors have adopted the general measure of fidelity to find the average time of entanglement generation. Whereas their approach provides us with a general insight into some aspects of quantum repeater systems, it cannot be directly applied to the case of QKD. In the latter, the performance is not only a function of the entanglement generation rate, but also the quantum bit error rate caused by using nonideal entangled states. To include both of these issues, here we adopt the secret key generation rate per memory as the main figure of merit, by which we can specify the optimal setting of the system and its performance in different regimes of operation.

Another key feature of our work is to use a *normalized* figure of merit to compare the DLCZ and SPS protocols. In practice, to obtain a sufficiently large key rate in such probabilistic systems, one must use multiple memories and/or modes in parallel. In order to account for the cost of the system, in

*m.razavi@leeds.ac.uk

our analysis, we provide a normalized key rate per memory and/or mode. We calculate the dependence of the secret key generation rate on different system parameters when resolving or nonresolving detectors are used. In particular, we find the optimal values for relevant system parameters if loss, double-photon emissions, and dark counts are considered. Moreover, we account for the dephasing and the decay of memories in our analysis. Memory decoherence is one of the key challenges in any practical setup.

The paper is structured as follows. In Sec. II, we review the DLCZ and the SPS protocols, their entanglement distribution and swapping schemes, as well as their QKD measurements. In Sec. III, we present our methodology for calculating the secret key generation rate for the SPS protocol, followed by numerical results in Sec. IV. We draw our conclusions in Sec. V.

II. TWO PROBABILISTIC SCHEMES FOR QUANTUM REPEATERS

In this section we review two probabilistic schemes, namely, DLCZ and SPS, for quantum repeaters. We describe the multiple-memory setup for such systems and model relevant system components.

A. DLCZ entanglement-distribution scheme

The DLCZ scheme works as follows [see Fig. 1(a)]. Ensemble memories A and B, at distance L, are made of atoms with Λ-level configurations. They are all initially in their ground states. By coherently pumping these atoms, some of them may undergo off-resonant Raman transitions that produce Stokes photons. The resulting photons are sent toward a 50:50 beam splitter located at distance $L/2$ between

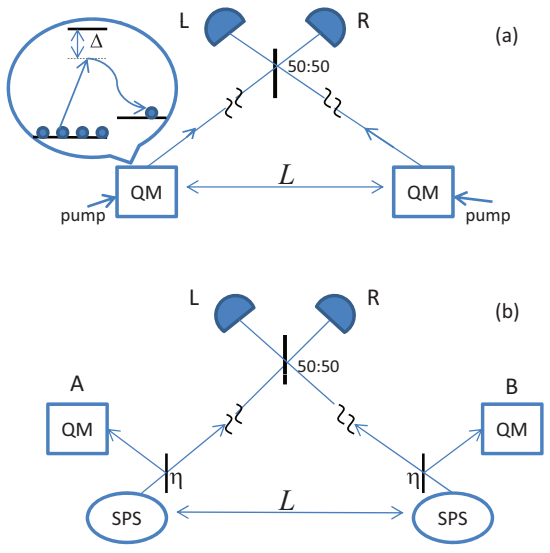

FIG. 1. (Color online) Schematic diagram for entanglement distribution between quantum memories (QMs) A and B for (a) the DLCZ protocol and (b) the SPS protocol. In both cases, we assume QMs can store multiple excitations. Sources, memories, and detectors are represented by circles, squares, and half circles, respectively. Vertical bars denote beam splitters. In both protocols the detection of a single photon ideally projects the two memories onto an entangled state.

A and B. If, ideally, only one photon has been produced in total at the ensembles, one and, at most, only one of the detectors in Fig. 1(a) clicks. In such a case, the DLCZ protocol heralds A and B to be ideally in one of the Bell states $|\psi_\pm\rangle_{AB} = (|10\rangle_{AB} \pm |01\rangle_{AB})/\sqrt{2}$, where $|0\rangle_J$ is the ensemble ground state and $|1\rangle_J = S_J^\dagger|0\rangle_J$ is the symmetric collective excited state of ensemble $J = A, B$, where $S_J^\dagger$ is the corresponding creation operator [10]. An important feature of such collective excitations is that they can be read out by converting their states into photonic states.

The fundamental source of error in the DLCZ scheme is the multiple-excitation effect, where more than one Stokes photon are produced [11]. If the probability of generating one Stokes photon is denoted by p_c, there is a probability p_c^2 that each ensemble emits one photon. If this happens, a click on one of the two detectors heralds entanglement generation, whereas the memories are in the separable state $|11\rangle_{AB}$.

In practice, one has to find the right balance between the heralding probability, which increases with p_c, and the quantum bit error rate (QBER), which also increases with p_c. In [11], authors find the optimal value of p_c that maximizes the secret key generation rate in various scenarios when photon-number resolving detectors (PNRDs) or nonresolving photon detectors (NRPDs) are used. In this paper, we use their results in our comparative study.

B. SPS entanglement-distribution scheme

The SPS protocol, proposed in [17] aims at reducing multiphoton errors and, in particular, terms of the form $|11\rangle_{AB}$ by using single-photon sources. The architecture of this scheme is presented in Fig. 1(b). The two remote parties each have one single-photon source and one memory. In the ideal scenario, each source produces exactly one photon on demand, and these photons are sent through identical beam splitters with transmission coefficients η. It can be shown that the state shared by the QMs after a single click on one of the detectors in Fig. 1(b) is given by [17]

$$\eta|00\rangle_{AB}\langle 00| + (1-\eta)|\psi_\pm\rangle_{AB}\langle\psi_\pm|, \tag{1}$$

which has our desired entangled state plus a vacuum component. The latter, at the price of reducing the rate, can be selected out once the above state is measured at later stages [10,11].

In a practical setup, several sources of imperfection must be considered in Fig. 1(b). First, most known techniques for generating single photons suffer from multiple-photon emissions. That includes single-photon sources that rely on parametric down-conversion [19,20], quasiatomic structures such as quantum dots [21], or the partial memory-readout technique described in [18]. In all cases, there is a nonzero probability to generate more than one photon, which manifests itself in producing nonzero values for second-order coherence functions [19,20]. For practical purposes, however, it is often sufficient to consider the effect of two-photon states, as we do in this paper. It turns out that this approximation is particularly valid for the systems of interest in this paper. One should also consider nonidealities in QMs. In our analysis, we account for reading and writing efficiencies of QMs, as well as their decay and dephasing processes. We assume that QMs can store multiple excitations.

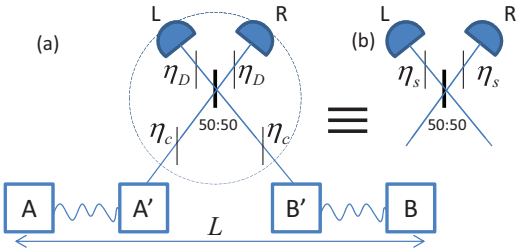

FIG. 2. (Color online) (a) Entanglement connection between two entangled links A-A' and B'-B. The memories A' and B' are read out and the resulting photons are combined on a 50:50 beam splitter. A click on one of the detectors projects A and B into an entangled state. The retrieval efficiencies and quantum efficiencies are represented by fictitious beam splitters with transmission coefficient η_c and η_D, respectively. (b) The equivalent butterfly transformation to the measurement module, where $\eta_s = \eta_c\eta_D$.

Throughout the paper, we assume that both setups in Fig. 1 are symmetric and phase stabilized. Furthermore, all conditions required for a proper quantum interference at 50:50 beam splitters are assumed to be met. Recent experimental progress in QKD shows that it is indeed possible to achieve these conditions [22,23].

C. Entanglement swapping and QKD measurements

Figure 2(a) shows the entanglement swapping setup for the DLCZ and the SPS protocols. Entanglement is established between QM pairs AA' and $B'B$ using either protocol. A partial Bell-state measurement (BSM) on photons retrieved from the middle QMs A' and B' is then followed, which, upon success, leaves A and B entangled. The BSM is effectively performed by a 50:50 beam splitter and single-photon detectors. To include the effects of the atomic-to-photonic conversion efficiency and the photodetectors' quantum efficiency, we introduce two fictitious beam splitters with transmission coefficients η_c and η_D, respectively. All photodetctors in Fig. 2 will then have unity quantum efficiencies. Note that the parameter η_c also includes the memory decay during the storage time.

Figure 2(b) provides a simplified model for the measurement module in Fig. 2(a). The 50:50 beam splitter and the two fictitious beam splitters in Fig. 2(b) constitute what we call a *butterfly* operation, which is further studied in Sec. III and Appendix A.

Alice and Bob use two butterfly operations to generate a raw key bit, as shown in Fig. 3. After generating entangled pairs over a distance L, Alice and Bob retrieve the states of memories and perform a QKD measurement on the resulting photons. They apply a random relative phase shift, φ, of either 0 or $\pi/2$ between their two fields. They later, at the sifting stage, keep only data points where the same phase value is used by both parties. They then turn their sifted keys into a secret key by using privacy amplification and error reconciliation techniques. Eavesdroppers can be detected by following the BBM92 or the Ekert protocol [7,24].

As mentioned in Sec. I, previous analyses only provide the fidelity or the time required for a successful creation of an entangled state [17]. Instead, in Sec. III, we calculate the

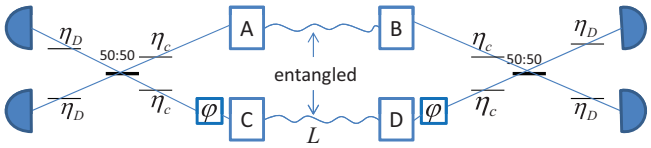

FIG. 3. (Color online) QKD measurements on two entangled pairs. Two pairs of memories, A-B and C-D, each share an entangled state. Memories are read out and the resulting photons are combined at a beam splitter and then detected. Different QKD measurements can be performed by choosing different phase shift values, φ, of 0 and $\pi/2$.

secret key generation rate for the SPS scheme and compare it with that of the DLCZ protocol reported in [11].

It is worth noting that because of the reliance of our QKD protocols on entanglement, all entanglement swapping operations at the middle nodes can be done by untrusted parties, e.g., service providers. This is, in essence, similar to the recently proposed measurement-device-independent QKD (MDI-QKD) protocols [25–27], which also rely on entanglement swapping. MDI-QKD schemes, in their original form, are not suitable for long-distance quantum cryptography. By combining them with quantum repeaters in a hybrid setup that relies on MDI-QKD for the access network and on quantum repeaters for the core network, one can achieve the best of the two worlds. Preliminary analysis on such hybrid networks has been done [28] and the extended work is in preparation.

D. Multiple-memory configuration

In order to compare different quantum repeater setups, we consider the multiple-memory configuration shown in Fig. 4(a) along with the cyclic protocol described in [29,30]. In this protocol, in every cycle of duration L_0/c, where L_0 is the length of the shortest segment in a quantum repeater and c

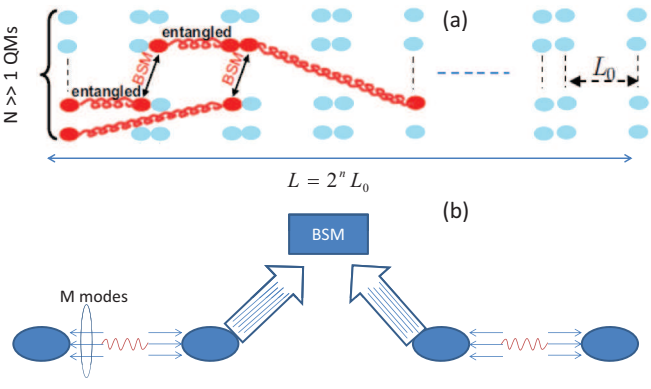

FIG. 4. (Color online) (a) A quantum repeater with multiple quantum memories per node. At each round, we employ entanglement distribution protocol to entangle any unentangled memory pairs over shortest links. At any such cycle, we also match up entangled pairs at different stations to perform Bell-state measurements (BSMs). (b) A quantum repeater with multimode memories. In each round, we apply our entanglement distribution scheme on all M modes, until one of them becomes entangled. BSM will be followed as soon as entanglement is established on both sides.

is the speed of light in the channel, we try to entangle any unentangled pairs of memories at distance L_0. We assume our entanglement-distribution protocol succeeds with probability $P_S(L_0)$. 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 l (*informed* BSMs). We use the results of [29] to calculate the generation rate of entangled states *per memory* in the limit of infinitely many memories. It is given by $R_{\text{ent}}(L) = P_S(L/2^n)P_M^{(1)}P_M^{(2)}\cdots P_M^{(n)}/(2L/c)$, where $P_M^{(i)}$, $i = 1,\ldots,n$, is the BSM success probability at nesting level i for a quantum repeater with n nesting levels.

We use the following procedure, in forthcoming sections, to find the secret key generation rate of the setup in Fig. 4(a). For each entanglement distribution scheme, we find $P_S(L_0)$ and relevant P_M probabilities to derive $R_{\text{ent}}(L)$. We then find the sifted key generation rate by multiplying $R_{\text{ent}}(L)$ by the probability, P_{click}, that an acceptable click pattern occurs upon QKD measurements. Finally, the ratio between the number of secure bits and the sifted key bits is calculated using the Shor-Preskill lower bound [31]. In the limit of an infinitely long key, the secret key generation rate per logical memory is lower bounded by

$$R_{\text{QKD}}(L) = \max\{R_{\text{ent}}(L)P_{\text{click}}[1 - 2\,H(\epsilon_Q)],0\}, \qquad (2)$$

where ϵ_Q denotes the QBER, and $H(p) = -p\log_2 p - (1-p)\log_2(1-p)$, for $0 \leqslant p \leqslant 1$.

E. Multimode-memory configuration

Another way to speed up the entanglement generation rate is via using multimode memories [15,32]. As can be seen in Fig. 4(b), in this setup, we use only one physical memory per node but each memory is capable of storing multiple modes. In each round, we attempt to entangle memories at distance L_0 by entangling, at least, one of the existing M modes. Once this occurs, we stop entanglement generation on that leg and wait until a BSM can be performed. For readout, all modes must be retrieved in order to perform BSMs or QKD measurements on particular modes of interest. In effect, this scheme is similar to that of Fig. 4(a), except that entanglement distribution is not sequentially applied to unentangled modes. The success probability for entanglement distribution between the two memories is, however, M times that of Fig. 4(a). One can show that, the generation rate of entangled states per mode is approximately given by $(\frac{2}{3})^n R_{\text{ent}}(L)$ [18,30].

In our forthcoming analysis, we consider only the case of Fig. 4(a), but our results are extensible to the case of Fig. 4(b) by accounting for the relevant prefactor.

F. Memory decay and dephasing

Quantum memories are expected to decay and dephase while storing quantum states. In this paper, we model these two decoherence processes independently. The decay process, with a time constant T_1, can be absorbed in the retrieval efficiency of memories. If the retrieval efficiency immediately after writing into the memory is given by η_0, after a storage time T, the retrieval efficiency is given by $\eta_c = \eta_0\exp(-T/T_1)$. Different memories in the multiple-memory setup of Fig. 4(a) undergo different decay times. In our analysis, we consider the worst-case scenario, where all memories have decayed for $T = L/c$, which is applicable only to the far-end memories. Under this assumption, η_c can be treated as a constant at all stages of entanglement swapping.

We model the memory dephasing via a dephasing channel, by which the probability of dephasing after a period T is given by $e_d = [1 - \exp(-T/T_2)]/2$. In the context of the QKD protocol in Fig. 3, this phase error is equivalent to the misalignment error in a conventional polarization-based BB84 protocol and has mostly the same effect. In our analysis, we neglect the effect of dephasing at the middle stages and consider only its effect on the far-end memories used for the QKD protocol. Again, for the multiple-memory setup of Fig. 4(a), the relevant storage time is given by $T = L/c$ [29].

III. SPS SECRET KEY GENERATION RATE

In this section, the secret key generation rate for the SPS scheme proposed in [17] is calculated. As shown in Sec. II, this scheme relies on simultaneous generation of single photons in two remote sites. Most practical schemes for the generation of single photons, however, suffer from the possibility of multiple-photon emissions. To address this issue, in this section we consider nonideal photon sources with nonzero probabilities for two-photon emissions and find the secret key generation rate in the repeater and no-repeater cases.

Suppose our photon sources emit one photon with probability $1 - p$ and two photons with probability p. We therefore have the following input density matrix for the initial state of l and r sources in Fig. 5(a):

$$\rho_{lr}^{(\text{in})} = \rho_l^{(\text{in})} \otimes \rho_r^{(\text{in})}, \qquad (3)$$

where

$$\rho_j^{(\text{in})} \equiv (1-p)|1\rangle_{jj}\langle 1| + p|2\rangle_{jj}\langle 2|, \quad j = l, r. \qquad (4)$$

As we show later, in a practical regime of operation, $p \ll 1$; hence, in our following analysis, we neglect $O(p^2)$ terms corresponding to the simultaneous emission of two photons by both sources.

A. No-repeater case

In this section, we describe how we obtain parameters P_S, P_{click}, and R_{QKD} for the setup in Fig. 5(a) and QKD measurements as in Fig. 3.

Figure 5(a) depicts the entanglement-distribution setup for the SPS scheme. In our model the memories' writing efficiencies, the path loss, and the detectors' efficiencies are represented by fictitious beam splitters with transmission coefficients η_m, η_t, and η_D, respectively, where $\eta_t = \exp[-L/(2L_{\text{att}})]$, with $L_{\text{att}} = 25$ km for an optical fiber channel. Photodetectors, in Fig. 5, are then assumed to have unity quantum efficiencies.

In our analysis, we use an equivalent setup, as shown in Fig. 5(b), where beam splitters have been rearranged such that $\eta_t\eta_D = \eta_m\eta_d$. We can then recognize similar building blocks, which we referred to as butterfly modules, in Fig. 5(b). A butterfly module, as shown in Fig. 6, is a two-input, two-output

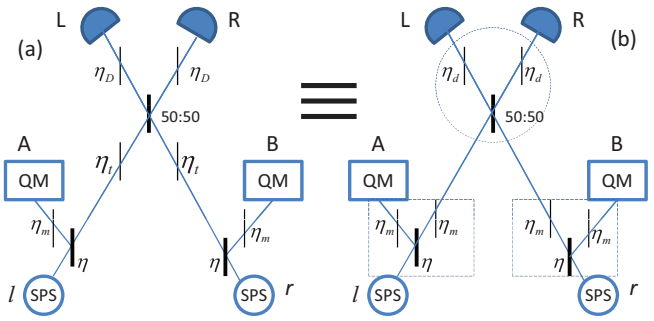

FIG. 5. (Color online) A schematic model for the SPS scheme. In (a) the memories' writing efficiencies, the path loss, and the detectors' efficiencies are represented by fictitious beam splitters with transmission coefficients η_m, η_t and η_D, respectively. In (b), an equivalent model is represented, where we have grouped beam splitters in the form of butterfly modules; see Fig. 6. Here, $\eta_t\eta_D = \eta_m\eta_d$ and the model is valid so long as $\eta_t\eta_d \leqslant \eta_m$.

building block consisting of three beam splitters. For an input state $\rho_{L'R'}$ in Fig. 6, we denote the output state on ports L and R as $B_{\eta_B,\eta_x}(\rho_{L'R'})$.

We use well-known models for beam splitters [33] to find output density matrices for input states to a generic butterfly module. In Appendix A, we find the relevant input-output relationships for the states of interest. We use MAPLE 15 to simplify some of our analytical results. We can then find ρ_{ALBR}, the joint state of the memories and the optical modes entering detectors L and R in Fig. 5(b) by applying the butterfly operation three times, as follows:

$$\rho_{ALBR} = B_{0.5,\eta_d}\left(B_{\eta,\eta_m}\left(\rho_l^{(in)}\right) \otimes B_{\eta,\eta_m}\left(\rho_r^{(in)}\right)\right). \tag{5}$$

According to the SPS protocol, a click on exactly one of the detectors L or R in Fig. 5(b) would herald the success of entanglement distribution. This process can be modeled by applying proper measurement operators considering whether PNRDs or NRPDs are used. For example, for a click on detector L, the explicit form of the measurement operator is given by

$$M = \begin{cases} (1-d_c)[|1\rangle_{LL}\langle 1| \otimes |0\rangle_{RR}\langle 0| \\ \quad + d_c|0\rangle_{LL}\langle 0| \otimes |0\rangle_{RR}\langle 0|], & \text{PNRD} \\ (1-d_c)[(I_L - |0\rangle_{LL}\langle 0|) \otimes |0\rangle_{RR}\langle 0| \\ \quad + d_c|0\rangle_{LL}\langle 0| \otimes |0\rangle_{RR}\langle 0|], & \text{NRPD} \end{cases} \tag{6}$$

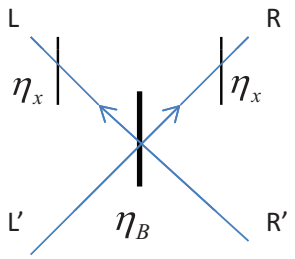

FIG. 6. (Color online) A generic butterfly module, represented by B_{η_B,η_x}, where η_B and η_x are transmissivities for beam splitters shown in the figure.

where I_L denotes the identity operator for the mode entering the left detector [34], and d_c is the dark count rate per gate width per detector.

After the measurement, the resulting joint state, ρ_{AB}, of quantum memories is given by

$$\rho_{AB} = \frac{\mathrm{tr}_{L,R}(\rho_{ALBR}M)}{P}, \tag{7}$$

where

$$P = \mathrm{tr}(\rho_{ALBR}M) = \frac{P_S(L)}{2} \tag{8}$$

is the probability that the conditioning event M occurs. The last equality is due to the symmetry assumption.

For QKD measurements, we assume that two pairs of memories, A-B and C-D, are given in an initial state similar to that of Eq. (7). We use the scheme described in Fig. 3 to perform QKD measurements. For simplicity, we assume both users use zero phase shifts; other cases can be similarly worked out in our symmetric setup. In Fig. 3, the retrieval efficiency and the quantum detectors efficiency are represented by fictitious beam splitters with, respectively, transmission coefficient η_c and η_D. It is again possible to remodel the setup in Fig. 3 as shown in Fig. 2(b) and use the butterfly operation $B_{0.5,\eta_s}$, where $\eta_s = \eta_c\eta_D$. The density matrix right before photodetection in Fig. 3 is then given by $B_{0.5,\eta_s}(B_{0.5,\eta_s}(\rho_{AB} \otimes \rho_{CD}))$, where one of the B operators is applied to modes A and C, and the other one to modes B and D. Using this state, we find P_{click} and ϵ_Q as outlined in Appendix B.

Using Eq. (2), the secret key generation rate per memory, R_{QKD}, in the no-repeater setup, is then lower bounded by [11]

$$R_1 = \max\left[[1 - 2\,H(\epsilon_Q)]\,\frac{P_S(L)}{2L/c}\,P_{\text{click}}/2, 0\right], \tag{9}$$

where $\frac{P_S(L)}{2L/c}$, given by Eq. (8), is the generation rate of entangled pairs per logical memory, P_{click} is the probability of creating a sifted key bit by using two entangled pairs, and $[1 - 2\,H(\epsilon_Q)]$ is the probability of creating a secret key bit out of each sifted key bit. Here, we assume a biased basis choice to avoid an extra factor of two reduction in the rate [35]. The full definition for P_{click} is given by Eq. (B3). The QBER,

$$\epsilon_Q = \frac{P_{\text{error}}}{P_{\text{click}}}, \tag{10}$$

where P_{error} is the probability that Alice and Bob assign different bits to their sifted keys, is given by Eq. (B4).

B. Repeater case

First, consider the repeater setup of nesting level one in Fig. 2(a). We use the structure of Fig. 5(a) to distribute entanglement between A-A' and B'-B memories. The initial joint state of the system, $\rho_{AA'BB'} = \rho_{AA'} \otimes \rho_{BB'}$, can then be found, using Eq. (7), as described in the previous section. We then apply a BSM by reading memories A' and B' and interfering the resulting optical modes at a 50:50 beam splitter. Success is declared if exactly one of the detectors in Fig. 2(a) clicks. This can be modeled by applying measurement

operators in Eq. (6), which results in

$$\rho_{AB} = \frac{\mathrm{tr}_{LR}(M\rho'_{ALBR})}{P_L}, \tag{11}$$

where $\rho'_{ALBR} = B_{0.5,\eta_s}(\rho_{AA'BB'})$, where L and R represent the input modes to the photodetectors. Note that in Fig. 2 the detectors have ideal unity quantum efficiencies. Moreover,

$$P_L = \mathrm{tr}(M\rho'_{ALBR}) = P_M/2 \tag{12}$$

is the probability that only the left detector clicks in the BSM module of Fig. 2. A click on the right detector has the same probability by symmetry.

In order to find the secret key generation rate, we follow similar steps to the no-repeater case. That is, we apply the butterfly operation to find relevant density matrices, from which P_{click} and ϵ_Q can be obtained. From Eq. (2), in the one-node repeater case, R_{QKD} is lower bounded by

$$R_2 = \max\left[[1 - 2\,H(\epsilon_Q)]\,\frac{P_S\,(L/2)}{2L/c}\,P_M\,P_{\mathrm{click}}/2, 0\right]. \tag{13}$$

Using the same approach, and by using Eq. (2), we find the secret key generation rate for higher nesting levels. The details of which have, however, been omitted for the sake of brevity.

IV. NUMERICAL RESULTS

In this section, we present numerical results for the secret key generation rate of the SPS protocol, versus different system parameters, in the no-repeater and repeater cases, and we compare them with that of the DLCZ protocol. As mentioned earlier, we have used MAPLE 15 to analytically derive expressions for Eqs. (2), (9), and (13) when PNRDs or NRPDs are used. Unless otherwise noted, we use the nominal values summarized in Table I for all the results presented in this section.

A. SPS key rate versus system parameters

1. *Source transmission coefficient*

Figure 7 shows the secret key generation rate per memory, R_{QKD}, versus the source transmission coefficient η in Fig. 1(b),

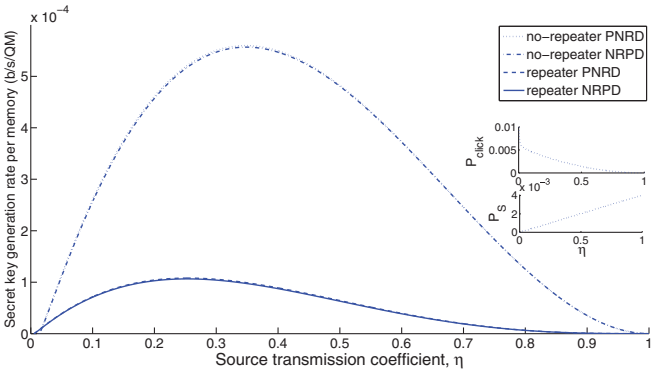

FIG. 7. (Color online) R_{QKD} versus the source transmission coefficient η for the PNRDs and NRPDs in the no-repeater and one-node repeater cases. Here, $p = 0.001$, $L = 250$ km, and $n = 1$ for the repeater system; other parameters are listed in Table I

at $p = 0.001$ and $L = 250$ km. It can be seen that there exist optimal values of η for both repeater and no-repeater systems. Table II summarizes these optimum values for different nesting levels. The optimal value of η for the no-repeater system is higher than the repeater ones, and that is because of the additional entanglement swapping steps in the latter systems. Another remarkable feature in Fig. 7 is that the penalty of using NRPDs, versus PNRDs, seems to be minor at $p = 10^{-3}$. PNRDs better show their advantage at higher values of p when double-photon terms become more evident.

The existence of an optimal value for η arises from a competition between the probability of entanglement distribution P_S, which grows with η, and P_{click}, which decreases with η. This has been demonstrated in the inset of Fig. 7. The latter issue is mainly because of the vacuum component in Eq. (1). In the case of the repeater system, P_M also decreases with η for the same reason, and that is why the optimal value of η is lower for repeater systems.

The optimum values of η in Fig. 7 are interestingly almost identical to the value of η that minimizes the total time for a successful creation of an entangled state, as prescribed in [17]. It is because, at a fixed distance, the QBER term in Eqs. (9) and (13) is mainly a function of the double-photon probability and the dark count rate, and it does not vary considerably with η. More generally, the optimum values of η remain constant as in Table II so long as the error terms are well below the cutoff threshold in QKD.

TABLE I. Nominal values used in our numerical results.

Memory writing efficiency, η_m	0.5
Quantum efficiency, η_D	0.3
Memory retrieval efficiency, η_c	0.7
Dark count per pulse, d_c	10^{-6}
Attenuation length, L_{att}	25 km
Speed of light, c	2×10^5 km/s
Decay (dephasing) time constants, T_1 (T_2)	∞

TABLE II. Optimal values of η, at $p = 0.001$ and $L = 250$ km, for repeater and no-repeater systems, when PNRDs or NRPDs are used. The figures with an asterisk are approximate values.

Nesting level	PNRD	NRPD
0	0.35	0.34
1	0.28	0.27
2	0.21	0.20*
3	0.12	0.11*

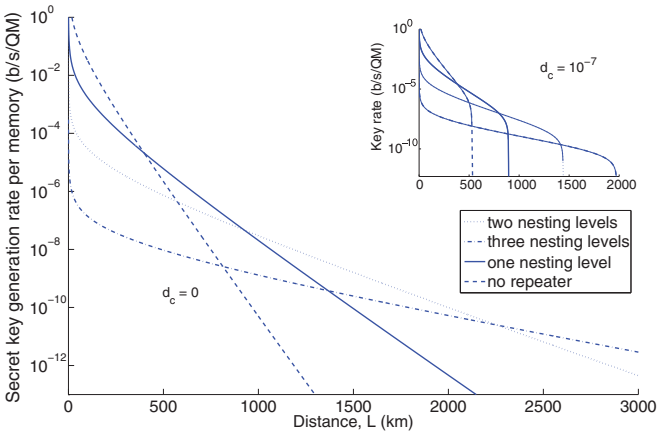

FIG. 8. (Color online) R_{QKD} versus distance for up to three nesting levels at two different dark count rates at $p = 10^{-4}$. All other values are listed in Tables I and II.

2. *Nesting levels and crossover distance*

Figure 8 depicts the normalized secret key generation rate versus distance for different nesting levels. At $d_c = 0$, the slope advantage, proportional to $P_S(L/2^n)$, for higher nesting levels is clear in the figure. Because of additional entanglement swapping stages, the no-path-loss rate at $L = 0$ is, however, lower for higher nesting levels. That would result in crossover distances—at which one system outperforms another—once we move from one nesting level to its subsequent one. The crossover distance has architectural importance and will specify the optimum distance between repeater nodes.

The crossover distance is a function of various system parameters. As shown in the inset of Fig. 8, positive dark count rates can change considerably the crossover distance. By including dark counts in our analysis, there will be a cutoff security distance for each nesting level. By increasing the dark count rate, these cutoff distances will decrease and become closer to each other. That would effectively reduce the crossover distance. At dark count rates as high as $d_c = 10^{-6}$, the superiority of three over two nesting levels at long distances would almost diminish as they both have almost the same cutoff distances.

The crossover distance will decrease if component efficiencies go up. This has been shown in Fig. 9 when the crossover distance is depicted versus measurement efficiency. The latter directly impacts the BSM success probability, P_M, and that is why the larger its value the lower is the crossover distance. Larger values of η_m also reduce the vacuum component, thus enhancing the chance of success at the entanglement swapping stage.

It can be noted in Fig. 9 that, even for highly efficient devices, the optimum distance between repeater nodes would tend to lie at around 150–200 km. For instance, at $L = 1000$ km, and with the nominal values used in this paper, the optimum nesting level is 2, which implies that the distance between two nodes of the repeater is 250 km. This could be a long distance for practical purposes, such as for phase stabilization, and that might require us to work at a suboptimal distancing. The latter would further reduce the secret key generation rate. Our result is somehow different from what

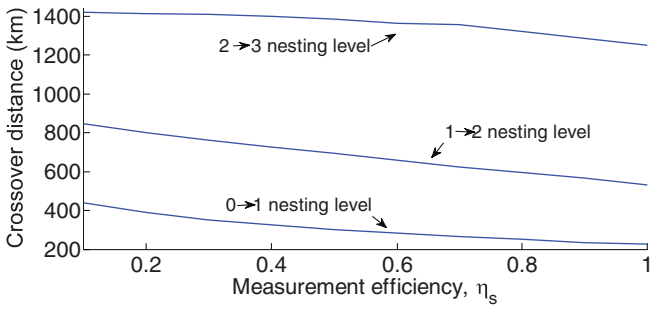

FIG. 9. (Color online) The crossover distance, at which a repeater system with nesting level n outperforms a system with nesting level $n-1$, as a function of measurement efficiency $\eta_s = \eta_c \eta_D$, at $p = 10^{-4}$. All other parameters are taken from Tables I and II, except for the dark count, which is 10^{-7}.

is reported in [18,30], although one should bear in mind the different set of assumptions and measures used therein.

3. *Double-photon probability*

Figures 10 show the secret key generation rate for the SPS protocol, at the optimal values of η listed in Table II, versus the double-photon probability p in the no-repeater and repeater cases. It can be seen that, in both cases, there exists a cutoff probability at which R_{QKD} becomes zero. This point corresponds to the threshold QBER of 11% from the Shor-Preskill security proof. In the case of QMs with sufficiently long coherence times, as is the case in Fig. 10, the QBER in our system stems from two factors: dark count and double-photon probability. The former is proportional to d_c/η_d and it comes into effect only when the path loss is significant. The latter, however, affects the QBER at all distances. To better see this issue, in Fig. 10(b) the cutoff probability is depicted versus the dark count rate. It can be seen that the cutoff probability linearly goes down with d_c,

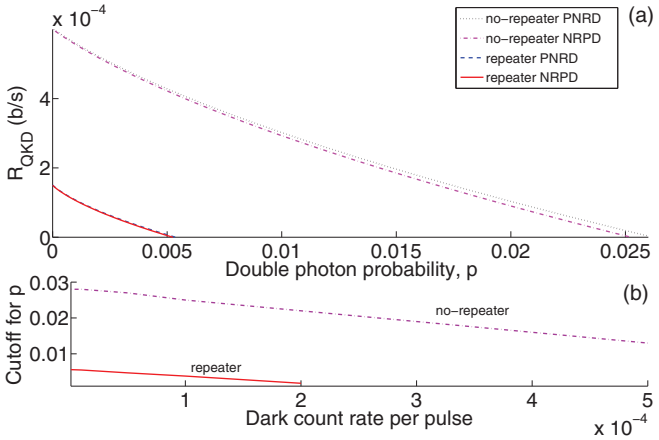

FIG. 10. (Color online) (a) R_{QKD} versus double-photon probability, p, using PNRDs and NRPDs in the no-repeater and one-node repeater cases. (b) Cutoff double-photon probability, at which the key rate becomes zero, versus the dark count rate d_c. The higher the dark count rate, the less room for multiphoton errors. All graphs are at $L = 250$ km.

TABLE III. Cutoff double-photon probabilities when PNRDs are used for different nesting levels. The paramter values used are listed in Tables I and II.

Nesting level	Cutoff double-photon probability
0	2.5×10^{-2}
1	5.0×10^{-3}
2	1.8×10^{-3}
3	2.1×10^{-4}

which confirms the additive contribution of dark counts and two-photon emissions to the QBER.

The cutoff probability at $d_c = 0$ deserves particular attention. As can be seen in Fig. 10(b), for the no-repeater system, the maximum allowed value of p is about 0.028 for PNRDs and 0.026 for NRPDs. This implies that the QBER in this case, at $d_c = 0$, is roughly given by $4p$. This can be verified by finding the contributions from two- and single-photon components in Eq. (4). We can then show that the QBER, at the optimal value of η in Table II, is roughly given by $3(1+\eta)p \approx 4p$. Similarly, in the repeater case, one can show that each BSM almost doubles the contribution of two-photon emissions to the QBER. Considering that four pairs of entangled states is now needed, and that the chance of making an error for an unentangled pair is typically 1/2, the QBER is roughly given by $4 \times 2 \times 3(1+\eta)p/2 \approx 16p$, which implies that, to the first-order approximation, the maximum allowed value for p is about $0.11/16 = 0.0068$. Figure 10(a) confirms this result, where the cutoff probability is about 0.0056 for the PNRDs and 0.0054 for the NRPDs, corresponding to $\epsilon_Q \approx 20p$.

With a similar argument as above, one may roughly expect a factor of 4 to 5 increase in the QBER for each additional nesting level. This implies that for a repeater system with nesting level 3, we should expect a QBER around $500p$ just because of the double-photon emission. Table III confirms our approximation by providing the actual cutoff figures for different nesting levels. We discuss the practical implications of this finding later in this section.

4. Memory dephasing

Figure 11(a) shows the secret key generation rate per memory for the SPS protocol with NRPDs versus distance for two different values of the dephasing time, T_2, at $p = 10^{-3}$. It is clear that, by reducing the coherence time, the security distance drops to shorter distances. Whereas at $T_2 = 100$ ms the key rate remains the same as that of Fig. 8(b), at $T_2 = 10$ ms both repeater and nonrepeater systems would fall short of supporting distances over 360 km.

Figure 11(b) shows the secret key generation rate per memory versus T_2 at $L = 250$ km. There is a minimum required coherence time of around 5 ms below which we cannot exchange a secret key. This point corresponds to the 11% QBER mainly caused by the dephasing process. In fact, at this point, we have $\epsilon_Q \approx e_d = \{1 - \exp[-L/(cT_2)]\}/2 = 0.11$, which implies that the maximum distance supported by our protocol is about $cT_2/4$. To be operating on the flat region in the curves shown in Fig. 11(b), one even requires a higher coherence time. In other words, the minimum required coherence time to support a link of length L is on the order of $10L/c$. This is in line with findings in [29]. Although not explicitly shown here, the same requirements are expected to be as applicable to other QKD systems that rely on quantum repeaters.

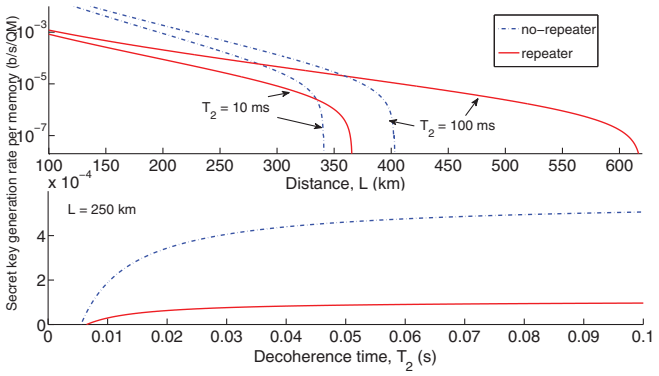

FIG. 11. (Color online) (a) The secret key generation rate versus distance for two values of decoherence time, $T_2 = 10$ and 100 ms. In (b) the secret key rate is plotted as a function of T_2 at $L = 250$ km. In both graphs, $p = 10^{-3}$.

B. SPS versus DLCZ

Figure 12 compares the secret key generation rate for the SPS protocol found in this paper with that of the DLCZ protocol as obtained in [11]. In both systems, we have assumed $d_c = 0$. All other parameters are as in Table I. In both systems, we use the optimal setting in the PNRD case. The conclusion would be similar if one uses NRPDs, as seen in all numerical results presented in this paper. For the SPS protocol, the optimal setting corresponds to the values of η in Table II. In the DLCZ protocol, the adjustable parameter is the excitation probability p_c. Note that, whereas in the SPS protocol, the rate decreases monotonically with p, in the DLCZ protocol, it peaks at a certain value of p_c. That is because in the SPS

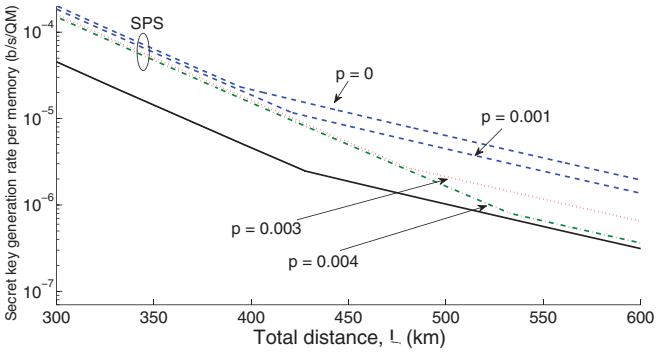

FIG. 12. (Color online) Comparison between the DLCZ and SPS protocols using PNRDs. For both systems, the better of repeater or non-repeater system is used. Both systems operate at their optimal setting: For the SPS protocol, the optimum value of η is used; for the DLCZ protocol, the optimum value of p_c is used. By varying the double-photon probability, p, in the SPS protocol, we find that the maximum p at which SPS outperforms DLCZ is around $p = 0.004$. In all curves, $d_c = 0$. All other parameters are taken from Tables I and II.

protocol we use an on-demand source of photons, whereas in the DLCZ protocol the heralding probability as well as the relative double-photon probability are both proportional to p_c. The optimum value for the excitation probability is given by $p_c = 0.0243$ in the no-repeater case and $p_c = 0.0060$ in the one-node repeater case [11]. Note that the analysis in [11] accounts for all multiexcitation components in the initial state of the system. In all curves in Fig. 12, we have used the better of the repeater and no-repeater systems at each distance. Our results show that the SPS protocol offers a higher key rate per memory than the DLCZ for on-demand single-photon sources with double-photon probabilities of 0.004 or lower. The advantage is, however, below one order of magnitude in most cases.

A key assumption in the results obtained above is the use of on-demand sources in the SPS protocol. The less-than-one-order-of-magnitude difference between the two protocols can then be easily washed away if one uses single-photon sources with less than roughly 50% efficiencies. This means that the conventional methods for generating single photons, such as parametric down-conversion or quantum dots, may not yet be useful in the SPS protocol. The partial memory-readout technique could still be a viable solution. In this scheme, we drive a Raman transition, as in the DLCZ protocol, in an atomic ensemble, such that with some probability p a Stokes photon is released. If we detect such a photon, then we are left with an ensemble, which can be partially read out with probability η to resemble the first part of the SPS protocol. One should, however, note that with limitations on the cutoff probability to be on the order of 10^{-4}–10^{-5}, it may take quite a long time to prepare such a source-memory pair. For instance, if the required p is 10^{-4}, and the efficiency of the collection and detection setup is 0.1, even if we run the driving pulse at a 1-GHz rate, it takes on average 0.1 ms to prepare the initial state. This time is comparable to the time that it takes for light to travel 100 km, which is on the same order of magnitude that we run our cyclic protocol in Fig. 4(a). Considering a particular setup parameters, it is not then an obvious call to which of the DLCZ or SPS protocols performs better, and that underlines the importance of our theoretical analysis.

V. CONCLUSIONS

In this paper, we analyzed the SPS protocol proposed in [17] in terms of the secret key generation rate that it could offer in a QKD-over-repeater setup. This protocol belongs to a family of probabilistic quantum repeaters, perhaps one of their best, inspired by the DLCZ proposal [10]. Our aim was to compare the SPS protocol for QKD applications with the original DLCZ protocol, as reported in [11], in a realistic scenario. To this end, we considered various sources of imperfections in our analysis and obtained the optimal regime of operation as a function of system parameters. We accounted for double-photon probabilities at the source and realized that, under Shor-Preskill's security-proof assumptions, its value should not exceed $0.11/4$ in a direct-link scenario and $0.11/20$ in a one-node repeater case. We would expect the same scaling, if not worse, at higher nesting levels, which implied that for a repeater setup of nesting level 3, the double-photon probability must be on the order of 10^{-4} or lower. That would be a challenging requirement for on-demand single-photon sources needed in the SPS protocol. Under above circumstances, the advantage of the SPS protocol over the DLCZ would be marginal and would not exceed one order of magnitude of key rate in bit/s per memory. In our analysis, we also accounted for memory dephasing and dark counts. The former would quantify one of the key characteristics of quantum memories in order to be useful in long-distance quantum communications. Our results showed that the minimum required coherence time for a link of length L is roughly given by $4L/c$, where c is the speed of light in the channel. The crossover distance at which we have to move up the nesting-level ladder varies for different system parameters. The optimum distancing between repeater nodes can nevertheless be typically as high as 150 to 200 km depending on the measurement efficiency among other parameters. We noticed that, within practical regimes of operation, there would only be a minor advantage in using resolving photodetectors over more conventional threshold detectors. We emphasized that, because of using a normalized figure of merit in our analysis, our results would be applicable to multimemory and/or multimode scenarios.

ACKNOWLEDGMENTS

The authors would like to thank X. Ma for fruitful discussions. This work was in part supported by the European Community's Seventh Framework Programme under Grant Agreement No. 277110 and UK Engineering and Physical Science Research Council Grant No. EP/J005762/1.

APPENDIX A: BUTTERFLY TRANSFORMATION

In this Appendix, we find input-output relationships for the butterfly module in Fig. 6. We do this in the number-state representation only for the relevant input states in Eq. (5).

Table IV provides the output state for the butterfly operation B_{η,η_m} when there is exactly one or two photons at one of the input ports. These are the only relevant terms in the input states in Eqs. (3) and (4). Using Table IV, we find $B_{\eta,\eta_m}(\rho_l^{(\mathrm{in})}) \otimes B_{\eta,\eta_m}(\rho_r^{(\mathrm{in})})$, to be used in Eq. (5).

The last operation required in Eq. (5) is the symmetric butterfly operation $B_{0.5,\eta_d}$. Table V lists the input-output relationships for all relevant input terms in our system for the more general operation $B_{0.5,\eta_x}$. Note that by choosing $\eta_x = \eta_s$, we can use the same relationships for the measurement modules used in entanglement swapping and QKD of Figs. 2 and 3, respectively. For the sake of brevity, in Table V, we have only included the terms that provide us with nonzero values after applying the measurement operation. More specifically, we have removed all *asymmetric* density matrix terms, such as $|10\rangle\langle 01|$ or $|01\rangle\langle 10|$, for which the bra state is different from the ket state, from the output state.

APPENDIX B: DERIVATION OF P_{click} AND P_{error}

In this Appendix, we find the gain and the QBER for the QKD scheme of Fig. 3. Let us assume that the memory pairs AB and CD are already entangled via the no-repeater or the one-node repeater scheme described in Sec. III. In the case of SPS protocol, their state is, respectively, given by Eqs. (7) and (11). The density matrix right before photodetection in Fig. 3

TABLE IV. The input-output relationship for the B_{η,η_m} operator. $|jk\rangle\langle jk| = |j\rangle_{JJ}\langle j| \otimes |k\rangle_{KK}\langle k|$, where $J = L'$ and $K = R'$ for input number states and $J = L$ and $K = R$ for output number states in Fig. 6.

ρ_{in}	$B_{\eta,\eta_m}(\rho_{\text{in}})$
$\|10\rangle\langle 10\|$	$\eta\eta_m\|01\rangle\langle 01\| + \eta_m\sqrt{\eta(1-\eta)}(\|10\rangle\langle 01\| + \|01\rangle\langle 10\|) + \eta_m(1-\eta)\|10\rangle\langle 10\| + (1-\eta_m)\|00\rangle\langle 00\|$
$\|20\rangle\langle 20\|$	$(1-\eta_m)^2\|00\rangle\langle 00\| + 2\eta\eta_m(1-\eta_m)\|01\rangle\langle 01\| + \eta\eta_m^2(1-\eta)(\|20\rangle\langle 02\| + \|02\rangle\langle 20\|)$ $+ 2\eta_m(1-\eta_m)\sqrt{\eta(1-\eta)}(\|10\rangle\langle 01\| + \|01\rangle\langle 10\|) + \eta^2\eta_m^2\|02\rangle\langle 02\| + 2\eta\eta_m^2(1-\eta)\|11\rangle\langle 11\|$ $+ \eta_m^2(1-\eta)\sqrt{2\eta(1-\eta)}(\|20\rangle\langle 11\| + \|11\rangle\langle 20\|) + \eta\eta_m^2\sqrt{2\eta(1-\eta)}(\|02\rangle\langle 11\| + \|11\rangle\langle 02\|)$ $+ 2\eta_m(1-\eta)(1-\eta_m)\|10\rangle\langle 01\| + \eta_m^2(1-\eta)^2\|20\rangle\langle 20\|$

is then given by $\rho_{ABCD} = B_{0.5,\eta_s}(B_{0.5,\eta_s}(\rho_{AB} \otimes \rho_{CD}))$, where one of the B operators is applied to modes A and C and the other one to modes B and D. Using Table V, we can calculate the exact form of ρ_{ABCD}, as we have done in this paper.

The most general measurement on the modes entering the photodetectors of Fig. 3, namely, A, B, C, and D, can be written in terms of the measurement operators

$$M_{abcd} = |a\rangle_{AA}\langle a| \otimes |b\rangle_{BB}\langle b| \otimes |c\rangle_{CC}\langle c| \otimes |d\rangle_{DD}\langle d| \tag{B1}$$

for PNRDs, where $a, b, c, d = 0, 1$ and $|k\rangle_K$ represents a Fock state for the optical mode $K = A, B, C, D$. In the case of NRPDs, we only need to replace $|1\rangle_{KK}\langle 1|$ with $(I_K - |0\rangle_{KK}\langle 0|)$, where I_K is the identity operator for mode K.

Similarly, we can define the corresponding probabilities to the above measurement operators as follows:

$$P_{abcd} = Tr\,(\rho_{ABCD}M_{abcd})\,. \tag{B2}$$

The explicit forms for P_{click} and P_{error} are then given by

$$P_{\text{click}} = P_C + P_E \tag{B3}$$

TABLE V. The input-output relationship for a symmetric butterfly module. The notation used is similar to that of Table IV.

ρ_{in}	$B_{0.5,\eta_x}(\rho_{\text{in}})$
$\|10\rangle\langle 10\|$	$\frac{\eta_x}{2}(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|) + (1-\eta_x)\|00\rangle\langle 00\|$
$\|01\rangle\langle 01\|$	$\frac{\eta_x}{2}(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|) + (1-\eta_x)\|00\rangle\langle 00\|$
$\|11\rangle\langle 11\|$	$\eta_x(1-\eta_x)(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|) + (1-\eta_x)^2\|00\rangle\langle 00\| + \frac{\eta_x^2}{2}(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|)$
$\|20\rangle\langle 20\|$	$\eta_x(1-\eta_x)(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|) + (1-\eta_x)^2\|00\rangle\langle 00\| + \frac{\eta_x^2}{2}\|11\rangle\langle 11\| + \frac{\eta_x^2}{4}(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|)$
$\|02\rangle\langle 02\|$	$\eta_x(1-\eta_x)(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|) + (1-\eta_x)^2\|00\rangle\langle 00\| + \frac{\eta_x^2}{2}\|11\rangle\langle 11\| + \frac{\eta_x^2}{4}(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|)$
$\|21\rangle\langle 21\|$	$\frac{3}{2}\eta_x(1-\eta_x)^2(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|) + (1-\eta_x)^3\|00\rangle\langle 00\| + \frac{\eta_x^2}{2}(1-\eta_x)\|11\rangle\langle 11\|$ $+ \frac{5}{4}\eta_x^2(1-\eta_x)(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|) + \frac{3}{8}\eta_x^3(\|30\rangle\langle 30\| + \|03\rangle\langle 03\|) + \frac{1}{8}\eta_x^3(\|21\rangle\langle 21\| + \|12\rangle\langle 12\|)$
$\|21\rangle\langle 21\|$	$\frac{3}{2}\eta_x(1-\eta_x)^2(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|) + (1-\eta_x)^3\|00\rangle\langle 00\| + \frac{\eta_x^2}{2}(1-\eta_x)\|11\rangle\langle 11\|$ $+ \frac{5}{4}\eta_x^2(1-\eta_x)(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|) + \frac{3}{8}\eta_x^3(\|30\rangle\langle 30\| + \|03\rangle\langle 03\|) + \frac{1}{8}\eta_x^3(\|21\rangle\langle 21\| + \|12\rangle\langle 12\|)$
$\|10\rangle\langle 01\|$	$\frac{1}{2}\eta_x(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|)$
$\|01\rangle\langle 10\|$	$\frac{1}{2}\eta_x(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|)$
$\|11\rangle\langle 20\|$	$\frac{\sqrt{2}}{2}\eta_x(1-\eta_x)(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|) + \frac{1}{2\sqrt{2}}\eta_x^2(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|)$
$\|11\rangle\langle 02\|$	$\frac{\sqrt{2}}{2}\eta_x(1-\eta_x)(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|) + \frac{1}{2\sqrt{2}}\eta_x^2(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|)$
$\|20\rangle\langle 11\|$	$\frac{\sqrt{2}}{2}\eta_x(1-\eta_x)(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|) + \frac{1}{2\sqrt{2}}\eta_x^2(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|)$
$\|02\rangle\langle 11\|$	$\frac{\sqrt{2}}{2}\eta_x(1-\eta_x)(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|) + \frac{1}{2\sqrt{2}}\eta_x^2(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|)$
$\|21\rangle\langle 21\|$	$\eta_x(1-\eta_x)^2(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|) + \eta_x^2(1-\eta_x)(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|)$ $+ \frac{3}{8}\eta_x^3(\|30\rangle\langle 30\| - \|03\rangle\langle 03\|) + \frac{1}{8}\eta_x^3(\|12\rangle\langle 12\| - \|21\rangle\langle 21\|)$
$\|12\rangle\langle 12\|$	$\eta_x(1-\eta_x)^2(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|) + \eta_x^2(1-\eta_x)(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|)$ $+ \frac{3}{8}\eta_x^3(\|30\rangle\langle 30\| - \|03\rangle\langle 03\|) + \frac{1}{8}\eta_x^3(\|12\rangle\langle 12\| - \|21\rangle\langle 21\|)$
$\|22\rangle\langle 22\|$	$(1-\eta_x)^4\|00\rangle\langle 00\| + 2\eta_x(1-\eta_x)^3(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|) + \eta_x^2(1-\eta_x)^2\|11\rangle\langle 11\|$ $+ \frac{3}{2}\eta_x^3(1-\eta_x)(\|30\rangle\langle 30\| + \|03\rangle\langle 03\|) + \frac{1}{2}\eta_x^3(1-\eta_x)(\|21\rangle\langle 21\| + \|12\rangle\langle 12\|)$ $\frac{5}{2}\eta_x^2(1-\eta_x)^2(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|) + \frac{3}{8}\eta_x^4(\|40\rangle\langle 40\| + \|04\rangle\langle 04\|) + \frac{1}{4}\eta_x^4\|22\rangle\langle 22\|$

and

$$P_{\text{error}} = e_d P_C + (1 - e_d) P_E, \tag{B4}$$

where e_d is the dephasing (misalignment) error,

$$P_C = \begin{cases} (1-d_c)^2\big[P_{1100} + P_{0011} + d_c(P_{1000} + P_{0100} + P_{0010} + P_{0001}) + 2d_c^2 P_{0000}\big], \text{PNRD} \\ \left(\frac{d_c^2}{2} - d_c + 1\right)(P_{1100} + P_{0011}) + d_c(1 - \frac{d_c}{2})(P_{1001} + P_{0110}) \\ + \frac{d_c}{2}(2 - d_c)(P_{1000} + P_{0100} + P_{0010} + P_{0001}) + \frac{d_c^2}{2}(2 - d_c)^2 P_{0000} \\ + \frac{1}{2}(P_{1110} + P_{1101} + P_{0111} + P_{1011}) + \frac{d_c}{2}(2 - d_c)(P_{1010} + P_{0101}) + \frac{1}{2}P_{1111}, \text{NRPD} \end{cases} \tag{B5}$$

is the probability that Alice and Bob assign identical bits to their raw keys if there is no misalignment, and

$$P_E = \begin{cases} (1-d_c)^2\big[P_{1001} + P_{0110} + d_c(P_{1000} + P_{0100} + P_{0010} + P_{0001}) + 2d_c^2 P_{0000}\big], \text{PNRD} \\ \left(\frac{d_c^2}{2} - d_c + 1\right)(P_{1001} + P_{0110}) + \frac{d_c}{2}(2 - d_c)(P_{1000} + P_{0100} + P_{0010} + P_{0001}) \\ + \frac{d_c^2}{2}(2 - d_c)^2 P_{0000} + \frac{1}{2}(P_{1110} + P_{1101} + P_{0111} + P_{1011}) \\ + \frac{d_c}{2}(2 - d_c)(P_{1100} + P_{1010} + P_{0011} + P_{0101}) + \frac{1}{2}P_{1111}, \text{NRPD} \end{cases} \tag{B6}$$

is the probability that they make an erroneous bit assignment in the absence of misalignment.

[1] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, Opt. Lett. **37**, 1008 (2012).

[2] M. Sasaki *et al.*, Opt. Exp. **19**, 10387 (2011).

[3] I. Choi, R. J. Young, and P. D. Townsend, New J. Phys. **13**, 063039 (2011).

[4] M. Razavi, IEEE Trans. Commun. **60**, 3071 (2012).

[5] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore* (IEEE, New York, 1984), pp. 175–179.

[6] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[7] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[8] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[9] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[10] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature (London) **414**, 413 (2001).

[11] J. Amirloo, A. H. Majedi, and M. Razavi, Phys. Rev. A **82**, 032304 (2010).

[12] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruß, Phys. Rev. A **87**, 052315 (2013).

[13] L. Jiang, J. M. Taylor, and M. D. Lukin, Phys. Rev. A **76**, 012301 (2007).

[14] Z.-B. Chen, B. Zhao, Y.-A. Chen, J. Schmiedmayer, and J.-W. Pan, Phys. Rev. A **76**, 022329 (2007).

[15] C. Simon, H. de Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **98**, 190503 (2007).

[16] N. Sangouard, C. Simon, B. Zhao, Y.-A. Chen, H. de Riedmatten, J.-W. Pan, and N. Gisin, Phys. Rev. A **77**, 062301 (2008).

[17] N. Sangouard, C. Simon, J. Minář, H. Zbinden, H. de Riedmatten, and N. Gisin, Phys. Rev. A **76**, 050301 (2007).

[18] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Rev. Mod. Phys. **83**, 33 (2011).

[19] E. Bocquillon, C. Couteau, M. Razavi, R. Laflamme, and G. Weihs, Phys. Rev. A **79**, 035801 (2009).

[20] M. Razavi, I. Söllner, E. Bocquillon, C. Couteau, R. Laflamme, and G. Weihs, J. Phys. B **42**, 114013 (2009).

[21] J. Claudon, J. Bleuse, N. S. Malik, M. Bazin, P. Jaffrennou, N. Gregersen, C. Sauvan, P. Lalanne, and J.-M. Gerárd, Nat. Photon. **4**, 174 (2010).

[22] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[23] A. Rubenok, J. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, arXiv:1304.2463.

[24] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[25] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[26] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).

[27] X. Ma, Chi-Hang Fred Fung, and M. Razavi, Phys. Rev. A **86**, 052305 (2012).

[28] M. Razavi, N. Lo Piparo, C. Panayi, and D. E. Bruschi, *Iran Workshop on Communication and Information Theory (IWCIT), Tehran, Iran, 2013* (IEEE, Piscataway, NJ, 2013), invited paper.

[29] M. Razavi, M. Piani, and N. Lütkenhaus, Phys. Rev. A **80**, 032301 (2009).

[30] M. Razavi, K. Thompson, H. Farmanbar, M. Piani, and N. Lütkenhaus, in *Quantum Communications Realized II*, edited by Y. Arakawa, M. Sasaki, and H. Sotobayashi (SPIE, Bellingham, WA, 2009), Vol. 7236, p. 723603.

[31] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[32] M. Afzelius, C. Simon, H. de Riedmatten, and N. Gisin, Phys. Rev. A **79**, 052329 (2009).

[33] P. L. Knight and A. Miller, in *Measuring the Quantum State of Light*, 1st ed. (Cambridge University Press, Cambridge, 1997), Vol. 1.

[34] M. Razavi and J. H. Shapiro, Phys. Rev. A **73**, 042303 (2006).

[35] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptol. **18**, 133 (2005).