This is a repository copy of *Long-distance quantum key distribution with imperfect devices*.

White Rose Research Online URL for this paper: http://eprints.whiterose.ac.uk/78176/

Version: Published Version

**Article:**

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

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

**Takedown**
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.
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 nonideals 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,
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 $A$-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 $A$ 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 $|\psi_{AB}\rangle = (|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B) / \sqrt{2}$, where $|0\rangle_J$ is the ensemble ground state and $|1\rangle_J = S^+_J |0\rangle_J$ is the symmetric collective excited state of ensemble $J = A, B$, where $S^+_J$ 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 $p^2_c$ 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 $\eta$. 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]

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

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 nonidealties 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. 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.
Figure 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 coefficients $\eta_c$ and $\eta_D$, respectively. (b) The equivalent butterfly transformation to the measurement module, where $\eta_c = \eta_c \eta_D$.

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 $A$-$A'$ 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 $\eta_c$ and $\eta_D$, respectively. All photodetectors in Fig. 2 will then have unity quantum efficiencies. Note that the parameter $\eta_c$ 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, $\varphi$, 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 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 $c$...
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 BSMSs). 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 $R_{\text{ent}}(L) = P_S(L/L_0)^2 P_M^{(1)} P_M^{(2)} \cdots P_M^{(n)} / (2L/c)$, 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, $P_{\text{click}}$, 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

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

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

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 $(\gamma^2)^M R_{\text{ent}}(L)$ [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 $\eta_0$, 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, $\eta_c$ 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-repeate 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):

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

$$\rho_j^{(\text{in})} = (1 - p) |1\rangle_j |1\rangle + p |2\rangle_j |2\rangle , \quad j = l, r . \quad (4)$$

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-repeate case

In this section, we describe how we obtain parameters $P_S$, $P_{\text{click}}$, and $R_{\text{QKD}}$ 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 $\eta_m$, $\eta_l$, and $\eta_D$, respectively, where $\eta_l = \exp[-L/(2L_{\text{att}})]$, 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 $\eta_l \eta_D = \eta_m \eta_d$. 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
would herald the success to perform QKD measurements. For simplicity, we model clicks. This can be modeled by applying measurement to modes entering detectors \( L \) and \( R \) as \( B_{L,R}(\rho_{L,R}) \).

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 \( \rho_{ALBR} \), 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:

\[
\rho_{ALBR} = B_{0.5,\eta_d}(B_{0,\eta_m}(\rho^{(in)}_L) \otimes B_{0,\eta_m}(\rho^{(in)}_R)).
\]

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 PNDRs or NRPDs are used. For example, for a click on detector \( L \), the explicit form of the measurement operator is given by

\[
M = \begin{cases} \frac{1}{2} - d_c |1 \rangle \langle 1|_{LL} (1 \otimes |0\rangle_{RR} |0\rangle_{RR}), & \text{PNRD} \\ + \frac{d_c}{2} |1 \rangle \langle 1|_{LL} (0 \otimes |0\rangle_{RR} |0\rangle_{RR}), & \text{PNRD} \\ |1 - d_c \rangle (|1 - |0\rangle_{LL} |0\rangle_{RR} |0\rangle_{RR}) + \frac{d_c}{2} |1 - |0\rangle_{LL} |0\rangle_{RR} |0\rangle_{RR}), & \text{NRPD} \\ \end{cases}
\]

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, \( \rho_{AB} \), of quantum memories is given by

\[
\rho_{AB} = \frac{\text{tr}_{L,R}(\rho_{ALBR} M)}{P},
\]

where

\[
P = \text{tr}(\rho_{ALBR} M) = \frac{P_S(L)}{2} \frac{P_{\text{click}}}{2}
\]

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 \( \eta_L \) and \( \eta_D \). 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 \( \eta_s = \eta_L, \eta_D \). 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 \( P_{\text{click}} \) and \( \epsilon_Q \) as outlined in Appendix B.

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

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

where \( P_S(L) \), given by Eq. (8), is the generation rate of creating sifted pairs per logical memory, \( P_{\text{click}} \) 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 \( P_{\text{click}} \) is given by Eq. (B3). The QBER,

\[
\epsilon_Q = \frac{P_{\text{error}}}{P_{\text{click}}}
\]

where \( P_{\text{error}} \) 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
\[ \rho_{AB} = \frac{\text{tr}_{LR}(M\rho_{\text{ALBR}}^i)}{P_L}, \]
(11)
where \( \rho_{\text{ALBR}}^i = B_{0.5,0}(\rho_{A/AB}) \), where \( L \) and \( R \) represent the input modes to the photodetectors. Note that in Fig. 2 the detectors have ideal unity quantum efficiencies. Moreover,
\[ P_L = \text{tr}(M\rho_{\text{ALBR}}) = P_M/2 \]
(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 \( P_{\text{click}} \) and \( \epsilon_Q \) can be obtained. From Eq. (2), in the one-node repeater case, \( R_{\text{QKD}} \) is lower bounded by
\[ R_2 = \max \left[ (1 - 2H(\epsilon_Q)) \frac{P_S(L/2)}{2L/c} \frac{P_M P_{\text{click}}/2}{0}, 0 \right]. \]
(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, \( R_{\text{QKD}} \), versus the source transmission coefficient \( \eta \) in Fig. 1(b), at \( p = 0.001 \) and \( L = 250 \) km. It can be seen that there exist optimal values of \( \eta \) for both repeater and no-repeater systems. Table II summarizes these optimum values for different nesting levels. The optimal value of \( \eta \) 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 \( p = 10^{-3} \). NRPDs better show their advantage at higher values of \( p \) when double-photon terms become more evident.

The existence of an optimal value for \( \eta \) arises from a competition between the probability of entanglement distribution \( P_S \), which grows with \( \eta \), and \( P_{\text{click}} \), which decreases with \( \eta \). 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 \( \eta \) for the same reason, and that is why the optimal value of \( \eta \) is lower for repeater systems.

The optimum values of \( \eta \) in Fig. 7 are interestingly almost identical to the value of \( \eta \) 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 \( \eta \). More generally, the optimum values of \( \eta \) remain constant as in Table II so long as the error terms are well below the cutoff threshold in QKD.

<table>
<thead>
<tr>
<th>Nesting level</th>
<th>PNRD</th>
<th>NRPD</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.35</td>
<td>0.34</td>
</tr>
<tr>
<td>1</td>
<td>0.28</td>
<td>0.27</td>
</tr>
<tr>
<td>2</td>
<td>0.21</td>
<td>0.20*</td>
</tr>
<tr>
<td>3</td>
<td>0.12</td>
<td>0.11*</td>
</tr>
</tbody>
</table>

TABLE I. Nominal values used in our numerical results.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory writing efficiency, ( \eta_m )</td>
<td>0.5</td>
</tr>
<tr>
<td>Quantum efficiency, ( \eta_D )</td>
<td>0.3</td>
</tr>
<tr>
<td>Memory retrieval efficiency, ( \eta_C )</td>
<td>0.7</td>
</tr>
<tr>
<td>Dark count per pulse, ( d_n )</td>
<td>10^-6</td>
</tr>
<tr>
<td>Attenuation length, ( L_{\text{at}} )</td>
<td>25 km</td>
</tr>
<tr>
<td>Speed of light, ( c )</td>
<td>2 \times 10^5 km/s</td>
</tr>
<tr>
<td>Decay (dephasing) time constants, ( T_1, T_2 )</td>
<td>( \infty )</td>
</tr>
</tbody>
</table>
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 $P_{\text{S}}(L/2^n)$, 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 the value the lower the crossover distance. Larger values of $\eta_m$ 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 suboptimal distancing. The latter would further reduce the secret key generation rate. Our result is somehow different from what 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 $\eta$ 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 $R_{\text{QKD}}$ 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 $d_c/\eta_d$ 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 $d_c$. 

![Graph showing secret key generation rate versus distance for different nesting levels](image1)

![Graph showing 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 $\eta_m$, at $p = 10^{-4}$](image2)

![Graph showing secret key generation rate, 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.](image3)
TABLE III. Cutoff double-photon probabilities when PNRDs are used for different nesting levels. The parameter values used are listed in Tables I and II.

<table>
<thead>
<tr>
<th>Nesting level</th>
<th>Cutoff double-photon probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$2.5 \times 10^{-2}$</td>
</tr>
<tr>
<td>1</td>
<td>$5.0 \times 10^{-3}$</td>
</tr>
<tr>
<td>2</td>
<td>$1.8 \times 10^{-3}$</td>
</tr>
<tr>
<td>3</td>
<td>$2.1 \times 10^{-4}$</td>
</tr>
</tbody>
</table>

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 $\eta$ 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 500$p$ 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 $\epsilon_Q \approx \epsilon_d = [1 - \exp(-L/(cT_2))] / 2 \approx 0.11$, 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.

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 $\eta$ in Table II. In the DLCZ protocol, the adjustable parameter is the excitation probability $p_e$. Note that, whereas in the SPS protocol, the rate decreases monotonically with $p_e$ in the DLCZ protocol, it peaks at a certain value of $p_e$. That is because in the SPS protocol, as obtained in [32], for the no-repeater system, the optimum value of $\epsilon$ is used; for the DLCZ protocol, the optimum value of $p_e$ 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.
LONG-DISTANCE QUANTUM KEY DISTRIBUTION WITH . . .

PHYSICAL REVIEW A 88, 012332 (2013)

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
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 advan-
tage 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 \( \eta \) 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,
der 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
\( B_{n,n_0} \) 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 \( B_{n_0,n} (\rho_{in}^{\text{in}}) \otimes
B_{n,n_0} (\rho_{in}^{\text{in}}) \), to be used in Eq. (5).

The last operation required in Eq. (5) is the symmetric
butterfly operation \( B_{0,5,n} \). Table V lists the input-output
relationships for all relevant input terms in our system for the
more general operation \( B_{0,5,n} \). Note that by choosing \( n_s = n_t \),
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 \( P_{\text{dark}} \) AND \( P_{\text{error}} \)

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

012332-9
is then given by $\rho_{ABCD} = B_{0.5,\eta}(B_{0.5,\eta}(\rho_{AB} \otimes \rho_{CD}))$, 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 $\rho_{ABCD}$, 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

$$M_{abcd} = |a\rangle_A|a\rangle_A \otimes |b\rangle_B|b\rangle_B \otimes |c\rangle_C|c\rangle_C \otimes |d\rangle_D|d\rangle_D$$

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 take $|1\rangle_K$ with $(I_K - |0\rangle_K\langle 0|)K$, where $I_K$ is the identity operator for mode $K$.

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

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

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

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

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

<table>
<thead>
<tr>
<th>$\rho_{in}$</th>
<th>$B_{0.5,\eta}(\rho_{in})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>10\rangle\langle 10</td>
</tr>
<tr>
<td>$</td>
<td>01\rangle\langle 01</td>
</tr>
<tr>
<td>$</td>
<td>11\rangle\langle 11</td>
</tr>
<tr>
<td>$</td>
<td>20\rangle\langle 20</td>
</tr>
<tr>
<td>$</td>
<td>02\rangle\langle 02</td>
</tr>
<tr>
<td>$</td>
<td>21\rangle\langle 21</td>
</tr>
<tr>
<td>$</td>
<td>21\rangle\langle 21</td>
</tr>
<tr>
<td>$</td>
<td>10\rangle\langle 01</td>
</tr>
<tr>
<td>$</td>
<td>20\rangle\langle 10</td>
</tr>
<tr>
<td>$</td>
<td>11\rangle\langle 20</td>
</tr>
<tr>
<td>$</td>
<td>02\rangle\langle 11</td>
</tr>
<tr>
<td>$</td>
<td>21\rangle\langle 21</td>
</tr>
<tr>
<td>$</td>
<td>12\rangle\langle 12</td>
</tr>
<tr>
<td>$</td>
<td>22\rangle\langle 22</td>
</tr>
</tbody>
</table>
LONG-DISTANCE QUANTUM KEY DISTRIBUTION WITH . . .  

PHYSICAL REVIEW A 88, 012332 (2013)

and

\[ P_{\text{error}} = e_d P_C + (1 - e_d) P_E. \]  

(B4)

where \( e_d \) is the dephasing (misalignment) error,

\[ P_C = \left\{ \begin{array}{l}
\frac{1}{2} (1 - d_c)^2 \left[ P_{1000} + P_{0010} + d_c (P_{1001} + P_{0010} + P_{0001} + P_{0100}) + 2 d_c^2 P_{0001}\right], \quad \text{PNRD} \\
\frac{1}{2} (1 - d_c)^2 \left[ P_{1001} + P_{0011} + d_c (P_{1010} + P_{0010} + P_{0100}) + d_c^2 (P_{0001} + P_{1001}) \right] + \frac{1}{2} (2 - d_c) (P_{0010} + P_{0100}) + \frac{1}{2} P_{1111}, \quad \text{NRPD}
\end{array} \right. \]  

(B5)

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

\[ P_E = \left\{ \begin{array}{l}
\frac{1}{2} (1 - d_c)^2 \left[ P_{1000} + P_{0100} + d_c (P_{1001} + P_{0100} + P_{0001} + P_{0010}) + 2 d_c^2 P_{0001}\right], \quad \text{PNRD} \\
\frac{1}{2} (1 - d_c)^2 \left[ P_{1001} + P_{0101} + d_c (P_{1010} + P_{0100} + P_{0010}) + \frac{1}{2} (2 - d_c) (P_{0010} + P_{1001}) + \frac{1}{2} P_{1111}, \quad \text{NRPD}
\end{array} \right. \]  

(B6)

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


012332-11