AIP Conference Proceedings

Long-distance quantum key distribution with imperfect devices

Nicoló Lo Piparo and Mohsen Razavi

Citation: AIP Conference Proceedings **1633**, 122 (2014); doi: 10.1063/1.4903112

View online: http://dx.doi.org/10.1063/1.4903112

View Table of Contents: http://scitation.aip.org/content/aip/proceeding/aipcp/1633?ver=pdfcov

Published by the AIP Publishing

Long-distance Quantum Key Distribution With Imperfect Devices

Nicoló Lo Piparo[a] and Mohsen Razavi[a]

[a]*School of Electronic and Electrical Engineering, University of Leeds*

.

Abstract. Quantum key distribution over probabilistic quantum repeaters is addressed. We compare, under practical assumptions, two such schemes in terms of their secure key generation rate per memory, R_{QKD}. The two schemes under investigation are the one proposed by Duan *et al.* in [Nat. **414**, 413 (2001)] and that of Sangouard *et al*. proposed in [Phys. Rev. A **76**, 050301 (2007)]. We consider various sources of imperfections in the latter protocol, such as a nonzero double-photon probability for the source, dark count per pulse, channel loss and inefficiencies in photodetectors and memories, to find the rate for different nesting levels. We determine the maximum value of the double-photon probability beyond which it is not possible to share a secret key anymore. We find the crossover distance for up to three nesting levels. We finally compare the two protocols.

Keywords: Quantum key distribution, Quantum repeaters, Secret key generation rate.
PACS: 03.67.Dd, 03.65.Ud, 42.50.-p

INTRODUCTION

Quantum key distribution (QKD), over long distances relies on quantum repeaters to share entangled states between two remote parties, usually called Alice and Bob. A practical way to implementing quantum repeaters is to use probabilistic schemes, which can possibly operate using imperfect devices [1-5]. Here, we compare two such schemes in terms of their secure key generation rates per memory, R_{QKD}, under practical assumptions.

The schemes we consider are the one proposed by Duan, Lukin, Cirac and Zoller [1], denoted by DLCZ hereafter, and the single-photon-source protocol, denoted by SPS, proposed in [2]. The DLCZ protocol uses atomic ensembles as quantum memories (QMs); see Fig, 1(a). By coherently pumping these QMs, they may undergo Raman transitions emitting photons and leaving atoms in symmetric collective states. A single detection at the middle site heralds entanglement generation between QMs. Within the DLCZ scheme, it is possible that both QMs store excited states—a non-entangled state—leading to lower values for R_{QKD}. The SPS protocol, instead, is not ideally affected by this limitation. As shown in Fig. 1(b), entanglement is distributed by ideally generating single photons and directing them toward the middle measurement site via beam splitters with transmission coefficients η. The other ports are directed to and stored in QMs. Again, a single click in the middle heralds entanglement.

Eleventh International Conference on Quantum Communication, Measurement and Computation (QCMC)
AIP Conf. Proc. 1633, 122-124 (2014); doi: 10.1063/1.4903112

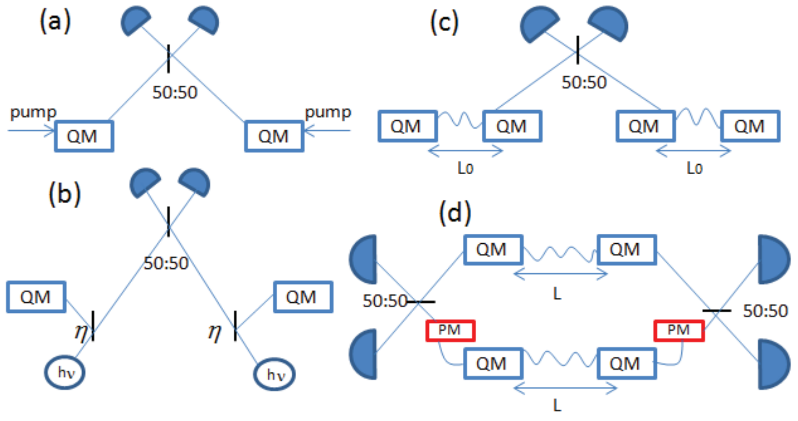

FIGURE 1. (a) Entanglement distribution scheme for the DLCZ protocol; (b) entanglement distribution for theSPS protocol; (c) quantum repeater scheme; and (d) QKD scheme.

In this paper, we consider various sources of imperfection in the SPS protocol, such as a nonzero double-photon probability, *p*, for the source, channel loss and inefficiencies in photodetectors and memories, to find R_{QKD} under two scenarios. In the first scenario, entangled pairs are generated over a distance *L* using the scheme in Fig. 1(b). In the second one, we use entanglement swapping, as shown in Fig. 1(c), by which we extend the distance. The elementary distance L_0 is *L/2*, *L/4* and *L/8* for one, two and three nesting levels, respectively. In both cases, photons are retrieved from QMs and Alice and Bob repeatedly apply a random phase module (PM) of either 0 or π/2, as shown in Fig. 1(d). They will later, at the sifting stage, only keep data points where the same phase values is used by both parties [5]. We assume a multimemory configuration, in which the above procedure can be repeated in parallel in a cyclic way [4]. R_{QKD} is then a normalized figure of merit that accounts for the number of memories used and it is given by:

$$R_{QKD} = \max\{0,(1-2H(\varepsilon_Q)P_S(L/2^n)\cdot P_M^{(1)}P_M^{(2)}...P_M^{(n)}\cdot P_{QKD}/(4L/c)\}, \qquad (1)$$

where $P_S(L/2^n)$ is the success probability for entanglement distribution over an elementary distance $L/2^n$; $P_M^{(i)}$, $i=1..n$, is the success probability of entanglement swapping at nesting level *i* for a quantum repeater with *n* nesting levels and P_{QKD} is the probability that an acceptable click pattern occurs upon QKD measurements. Finally, $1\text{-}2H(\varepsilon_Q)$ is the ratio between the number of secure and the sifted key bits, calculated using the Shor-Preskill lower bound [6], where ε_Q is the quantum bit error-rate and *H* is the binary entropy function.

RESULTS

Figure 2(a) shows R_{QKD} versus η for the SPS protocol, in Fig. 1(b), when there is no repeater. We find that there exists an optimum value of η, which maximizes R_{QKD}. It is given by the trade off between P_S, which increases with η, and P_{QKD}, which, instead, decreases with η. We obtain slightly different maxima for the repeater cases.

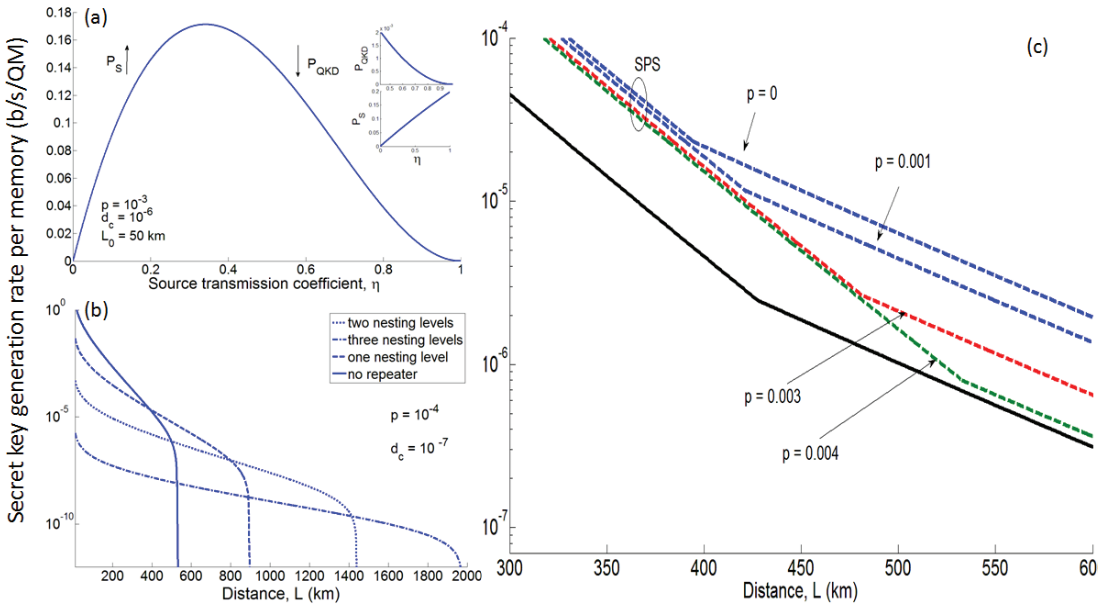

FIGURE 2. (a) R_{QKD} versus η when no repeater is used; (b) R_{QKD} versus distance for the no-repeater case and for repeater cases up to three nesting levels; and (c) R_{QKD} for DLCZ and SPS protocol versus distance for different values of *p*. In all graphs, the channel loss is 0.17 dB/km, the writing efficiency to QMs is 0.5 and the reading efficiency is 0.7; quantum efficiency is 0.3. d_c denotes the dark-count rate per pulse.

Using optimum values for *η*, in Fig. 2(b), we have plotted R_{QKD} versus distance for different nesting levels. From this graph we can determine the crossover distances when the one nesting level outperforms the previous one. Moreover, we can see the effect of the dark count, which determines a cut-off distance after which it is not possible to share a secret key.

Finally, in Fig. 2(c), we show that the SPS protocol outperforms the DLCZ protocol for certain value of *p*. A key assumption in the results obtained above is the use of on-demand sources in the SPS protocol. The SPS advantage over DLCZ can be easily washed away if one uses single-photon sources with less than 50% efficiencies.

ACKNOWLEDGMENTS

This work was in part supported by the European Community's Seventh Framework Programme under Grant Agreement 277110 and the UK Engineering and Physical Science Research Council grant number EP/J005762/1.

REFERENCES

1. L. M. Duan, M.D. Lukin, J. I. Cirac and P. Zoller, *Nature*, (London) **414**, 413 (2001).
2. N. Sangouard, C. Simon, J. C. V. Minar, H. Zbinden, H. de Riedmatten and N. Gisin, *Phys. Rev. A* **76**, 050301 (2007).
3. N. Sangouard, C. Simon, H. de Riedmatten and N. Gisin, *Rev. Mod. Phys* **83**, 33-80 (2011).
4. M. Razavi, M. Piani and N. Lütkenhaus, *Phys. Rev. A* **80**, 032301 (2009).
5. J. Amirloo, M. Razavi and A. H. Majedi, *Phys. Rev. A* **82**, 032304 (2010).
6. P. W. Shor and J. Preskill, *Phys. Rev. Lett.* **85**, 441 (2000).