Memory-Assisted Quantum Key Distribution Immune to Multiple-Excitation Effects

Nicoló Lo Piparo[1] and Mohsen Razavi[1]

[1]School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK

[1]Woodhouse Lane, Leeds, LS2 9DX, UK. Tel.:+44 0113 3432082 - email: eennl@leeds.ac.uk

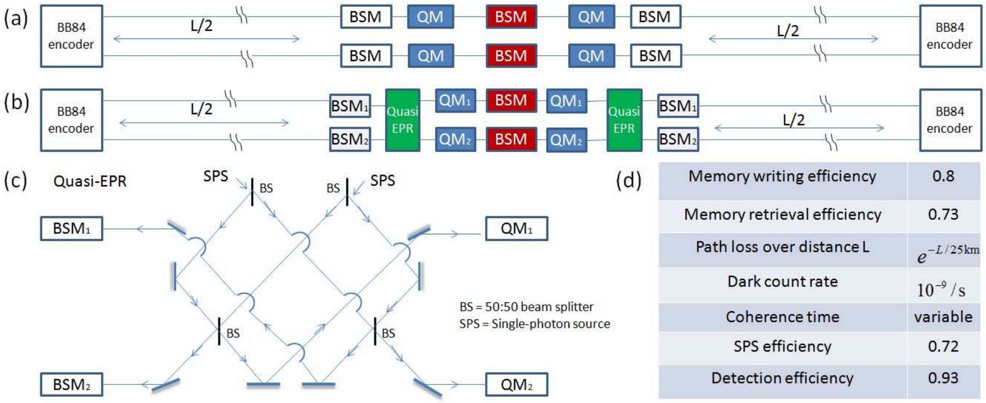
Abstract

Memory-assisted quantum key distribution aims to use existing quantum-device technologies to offer rate-versus-distance enhancements. Here, a variant of such systems, relying on single-photon sources, is proposed that counters the multiple-excitation effects in ensemble-based memories.

Long-distance quantum communications (LDQC) has a fundamental role in sharing secure information in future quantum networks. The key solution to trust-free LDQC relies on quantum repeaters. However, the demanding requirements for the implementation of the repeater systems do not allow an immediate use of such a technology. Here, we present a simple solution based on memory-assisted measurement-device-independent quantum key distribution (MA-MDI-QKD) structure [1] that can improve the rate-versus-distance behavior using state-of-the-art devices. Our proposal also remedies the multiple-excitation errors that could preclude ensemble-based memories from being used in such structures [2].

MA-MDI-QKD resembles a single-node quantum repeater with quantum memories (QMs) only in the middle; see Fig. 1(a) for the dual-rail phase-encoded setup. In this scheme, both users send a single photon, which has been encoded in one of the four BB84 states, to a middle station. The photon interacts with another photon entangled with the QMs in a side Bell-state measurement (BSM) module. If a side-BSM is successful, the state sent by the user is ideally teleported into the QMs. Once all QMs are loaded with the relevant states, they are read and a central-BSM is performed on the retrieved photons, creating, thus, correlated keys among users. The QMs in use must meet certain criteria, such as having a high bandwidth-storage product and fast entangling times [1], where both these conditions are met by ensemble-based QMs [1]. The conventional entangling procedure for such QMs will however lead to multiple excitations, which have been shown to be detrimental for the performance of the system [2].

In this paper, we propose to use single-photon sources (SPSs) in order to generate entangled photons. Figure 1(b) shows the dual-rail phase-encoded version of our proposed MA-MDI-QKD system, where



Memory writing efficiency	0.8
Memory retrieval efficiency	0.73
Path loss over distance L	$e^{-L/25\mathrm{km}}$
Dark count rate	$10^{-9}/\mathrm{s}$
Coherence time	variable
SPS efficiency	0.72
Detection efficiency	0.93

Figure 1: (a) MA-MDI-QKD scheme with indirectly heralding QMs [1]. (b) The proposed scheme with the proposed scheme relying on quasi-EPR module as sketched in (c). (d) The nominal values of the parameters used.

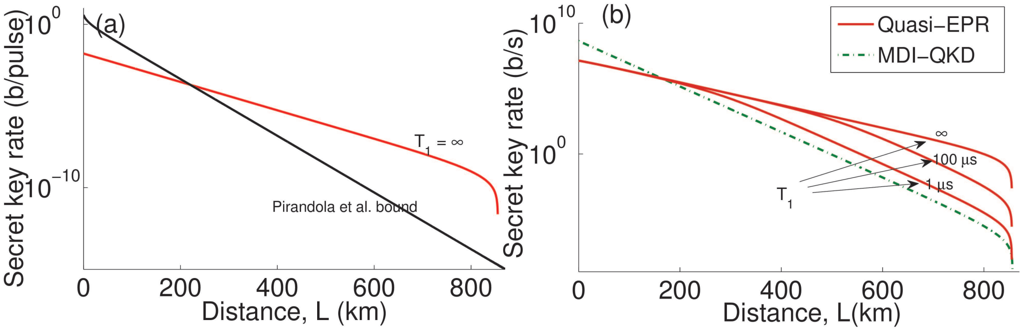


Figure 2: Key rates of the system in Fig. 1(b). In (a), key rate per pulse is compared with the upper bound in [3]. In (b) we consider the key rate in b/s with a the repetition rate of 1 GHz for different values of the coherence time T_1 compared with the no-memory MDI-QKD system. The same value of 200 ps has been used for the writing time, reading time, and duration of the pulse as reported in [4].

the entangling operation is done in the boxes labeled quasi-EPR. The architecture of this module is depicted in Fig. 1(c). Here, two SPSs each generate ideally one photon that interfere at four 50:50 beam splitters. The interaction pattern illustrated in Fig. 1(c) will create an entangled photon pair plus some spurious terms. These spurious terms include four two-photon Fock states, each at every output of Fig. 1(c). In the case of the entangled states, one half will be directed towards the BSM modules and the other half to the QMs, where the latter will be stored into the QMs. Here, we assume that our employed SPS has generated at most one photon, because of which we normally avoid generating multiple excitations in the QMs.

In order to evaluate the performance of our proposed system, we calculate the secret key rate for the setup of Fig. 1(b) by considering the main setup's inefficiencies as listed in Fig. 1(d). Figure 2(a) compares the secret key rate per pulse of the setup of Fig. 1(b) with the upper bound for a no-repeater QKD system reported in [3]. We can see that the key rate of our setup outperforms this bound around above 200 km. We can deduce that the effect of the spurious terms in the output state created by quasi-EPR modules is not detrimental for the overall performance of the system. That is due to the fact that when the two-photon Fock states generated by the quasi-EPR modules are directed towards the QMs, no photons will interact with the state sent by the users. Therefore, the side-BSM can be successful only through a dark count event. Similarly, when the two-photon Fock states are directed towards the side-BSM, a vacuum state will be loaded into the QMs, which would not result in a successful central-BSM, unless again because of the dark count. With a dark count rate as low as 10^{-9}/s, the corresponding errors will be low at short-to-moderate distances. We also consider the total key rate in b/s by assuming a repetition rate of 1 GHz, and for different values of the amplitude decay time constant, T_1. Figure 2(b) shows that our setup outperforms the no-memory system [5] at a distance $L \sim 190$ km for a coherence time as low as to $T_1 = 1\ \mu$s.

The required specifications of our proposed system is within reach of existing technologies. Ensemble-based memories have shown to have fast writing times, needed for high repetition rate, on the order of 200 ps, and coherence times on the order of 1 μs. SPSs based on quantum dots in photonic nanowires, also reach an efficiency of 0.72 [6] and are known to have very low two-photon components. With such state-of-the-art devices our scheme leads to two order of magnitude improvement at distances over 300 km, over existing no-memory QKD systems. This sets an achievable intermediate milestone for LDQC. This work was partly funded by UK's EPSRC Grant EP/M013472/1.

References

[1] C Panayi, M. Razavi, X. Ma, and N. Lütkenhaus. *New. J. Phys.*, 16:043005, 2013.

[2] N. Lo Piparo, M. Razavi, and C. Panayi. *IEEE J. of selected topics in quantum electron.*, 21:6601010, May/June 2015.

[3] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. *arXiv:1510.08863*, 2015.

[4] X.-H. Bao and et al. *Nat. Phys.*, 8:517–521, 2012.

[5] H.-K. Lo, M. Curty, and B. Qi. *Phys. Rev. Lett.*, 108:130503, Mar 2012.

[6] J. Caudon and et al. *Nat. Photon.*, 4:174–177, 2010.