Quantum Key Distribution over Atomic-Ensemble Quantum Repeaters

Mohsen Razavi[1,2,3], Jeyran Amirloo[1], and A. Hamed Majedi[1]

[1] *Institute for Quantum Computing and Department of Electrical and Computer Engineering, University of Waterloo, 200 University Ave. W., Waterloo, ON, Canada N2L 3G1*

[2] *School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK LS2 9JT*

[3] *email: m.razavi@leeds.ac.uk*

Abstract: The key generation rate for quantum key distribution systems that rely on quantum repeaters with atomic-ensemble memories is obtained. We find the cross-over distances at which quantum repeaters outperform direct entanglement-distribution links.

OCIS codes: (060.5565) Quantum communications; (270.5568) Quantum cryptography.

1 Introduction

Future secure communications relies on the advancement of quantum key distribution (QKD) systems based on single-photon communication. The original BB84 protocol, [1], as well as its weak-laser, [2], or decoy-state, [3], implementations all fall into this category. The inevitable loss in optical channels, however, not only results in low key generation rates, but also, in conjunction with detector deficiencies, limit the range within which a secure key can be exchanged between two parties. Long-distance secure communication is then a challenging problem especially if there are no trusted intermediate nodes between the two parties through which a secure key can be established. Fortunately, there is an alternative solution to QKD that uses entangled states [4]. Entanglement—although may rely on single-photon communication for initial distribution over short distances—is extensible to arbitrarily long distances by using entanglement swapping techniques within quantum repeater setups [5]. For reliable and effective performance, quantum repeaters require a large number of quantum memories that interact efficiently with light and demonstrate long coherence times. In this paper, we look at the Duan, Lukin, Cirac, and Zoller (termed DLCZ, hereafter) proposal for quantum repeaters, which is a probabilistic scheme that uses ensembles of neutral atoms as quantum memories [6]. Recently, coherence times in excess of 5 ms are demonstrated for such memories [7]. This is, in principle, sufficient to cover distances up to 1000 km, provided that a large number of logical memories can be employed in parallel [8]. Atomic ensembles can potentially be used as multiple logical memories by applying/collecting light at/from different directions. In this paper, we find the optimum driving power that maximizes the key generation rate in the DLCZ QKD protocol with and without a repeater node. We also find the cross-over distance at which the DLCZ repeater outperforms its direct entanglement distribution counterpart.

2 System Description

The DLCZ scheme for entanglement distribution works as follows; see Fig. 1(a). Ensembles A and B, at distance L, consisting of atoms with Λ-level configuration, are coherently pumped in order to drive off-resonant Raman transitions that create anti-Stokes photons. The probability of one such transition, p_c, is commonly kept much below one to avoid multiple excitations. The resulting photons are routed down towards a 50-50 beam splitter located halfway between A and B. The beam splitter erases any which-way information so that if, ideally, only one photon has been created at the ensembles, one of the two detectors D_1 and D_2, and at most only one of them, clicks. In that case, A and B are heralded to be entangled.

The fundamental source of error in the DLCZ scheme is the multiple excitation effect, where more than one anti-Stokes photon is created in the above process. Multiple photons passed through a lossy channel can reproduce an erroneous heralding event. This effect can be alleviated, to some extent, by using photon-number resolving detectors (PNRDs), rather than non-resolving photodetectors (NRPDs). In our work, we consider both detectors and compare the system performance in the two cases.

The 50-50 beam splitter together with the single photon detectors in Fig. 1(a) effectively perform a partial Bell-sate measurement (BSM) on the incoming photons. The DLCZ quantum repeater protocol uses this idea to distribute entanglement over longer distances. Figure 1(b) shows the DLCZ repeater setup in which, we first entangle ensembles $A\&A'$ and $B\&B'$, and then perform a partial BSM on the retrieved photons from the middle ensembles A' and B', which, upon success, leaves A and B entangled.

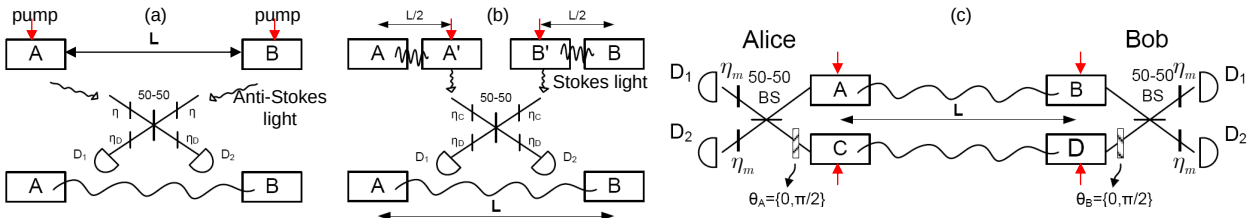

Fig. 1. (a) The DLCZ scheme for entanglement distribution between atomic ensembles A and B. The Λ-level atomic ensembles are coherently pumped to create anti-Stokes photons. Such photons are then routed down toward a 50-50 beam splitter and two single-photon detectors. A single click on one, and only one, of photodetectors heralds entanglement between A and B. (b) The DLCZ scheme for quantum repeaters. In order to entangle ensembles A and B, at distance L, we first entangle $A\&A'$ and $B\&B'$, at distance $L/2$, using the scheme described in (a). We then use a 50-50 beam splitter and single-photon detectors to perform a partial BSM on the photonic states retrieved from middle ensembles A' and B'. A click on one, and only one, of detectors heralds the success of entanglement swapping. (c) The DLCZ setup for QKD. Alice and Bob first create two entangled pairs of ensembles, $A\&B$ and $C\&D$, using the DLCZ schemes described in (a) or (b). They perform a random Pauli measurement by applying random phase shifts to retrieved optical modes, which interfere at a 50-50 beam splitter. After the sifting procedure, a click on detector $D_{1/2}$ is associated with bit 1/0, and in the case of a double click a random bit will be assigned to the raw key.

Based on the above protocols, the DLCZ QKD protocol works as follows. First, our two remote parties, Alice and Bob, generate identical entangled pairs, namely AB and CD, over distance L; see Fig. 1(c). They then retrieve the photons in the four ensembles and perform a QKD measurement on these photons according to the BB84 protocol [1]. The measurement modules used for this purpose is similar to the BSM module used in the repeater setup with additional phase shift units whose phase values are randomly chosen to be either 0 or $\pi/2$. After the sifting procedure, by which Alice and Bob specify the measurement events where they have both used the same phase shifts and have obtained at least one click on their respective detectors, they obtain a raw key by assigning bit one to the key whenever only D_1 has clicked on their side, and bit zero whenever only D_2 has clicked. In the case of a double click, they assign bit zero or one, with equal probability, to their raw keys. By using privacy amplification and reconciliation techniques, Alice and Bob turn their raw keys to a common secure key, which can be used for encryption purposes.

3 Performance Analysis, Numerical Results, and Discussion

Here, we find the key generation rate for the DLCZ QKD protocol when the initial entangled states are obtained via the direct method shown in Fig. 1(a), or via the repeater system of Fig. 1(b). We assume all setups are symmetric and phase stabilized, and dark count is negligible. Memories are assumed to have sufficiently long coherence times. The fundamental source of error that we consider is the possibility of having multiple excitations in our ensembles in conjunction with the path loss and BSM inefficiencies. The methodology that we use is similar to that of [9] in which we first find the relevant characteristic functions and density operators in terms of Gaussian integrals. The parameters of interest will then be reduced to statistical moments of a Gaussian random variable, which can be analytically found.

We use the cyclic protocol proposed in [8] for quantum repeaters in which a large number of logical memories are employed at each node. By using all memories successively, in the steady state, the number of entangled pairs generated per second per logical memory is given by $R_n^{\rm entg} = P_S(L/2^n)P_M^n c/(2L)$, where c is the speed of light in the channel, $P_S(L)$ is the probability that the entanglement distribution scheme of Fig. 1(a) heralds success over distance L, P_M is the probability that the BSM module in Fig. 1(b) heralds success, and n is the nesting level of the system ($n = 0$ in Fig. 1(a), and $n = 1$ in Fig. 1(b)). In the DLCZ QKD protocol, the number of raw key bits generated per second per employed memory is then given by $R_n^{\rm rawkey} = R_n^{\rm entg} P_{\rm click}/2$, where $P_{\rm click}$ is the probability that both Alice and Bob get at least one click on their measurement modules of Fig. 1(c) when they use similar phase shifts.

To include the error in our analysis, we combine the Shor and Preskill's result for the key generation rate of the BB84 protocol [10], i.e., the ratio between the number of secure key bits and the number of raw key bits, in the limit of an infinitely long key, and the squashing technique proposed in [11] to finally obtain

$$R_n = [1 - 2H(\text{QBER})]R_n^{\rm rawkey}, \quad n = 0, 1, \tag{1}$$

where $\text{QBER} = P_{\rm error}/P_{\rm click}$, with $P_{\rm error}$ being the probability that Alice and Bob, conditional on using

OWC2.pdf

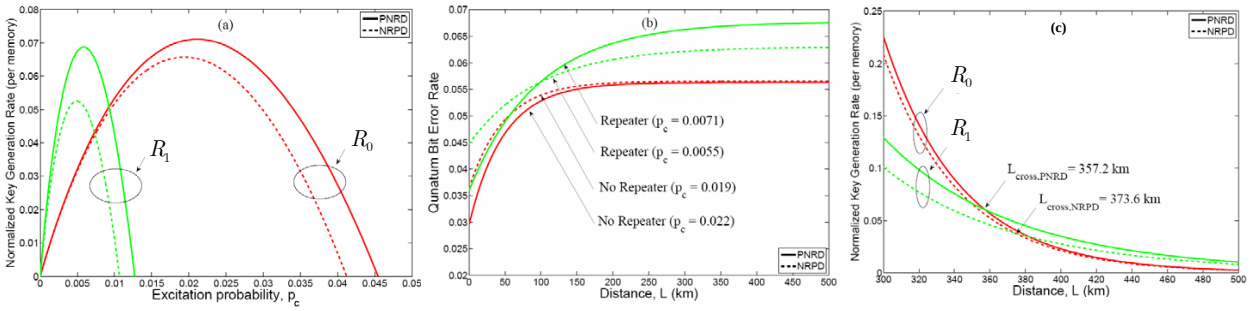

Fig. 2. (a) The number of secure key bits generated per second per memory for the DLCZ QKD protocol with (R_1) and without (R_0) repeater versus p_c at $L = 350$ km. There exists an optimum value of p_c at which the QKD rate peaks. (b) Quantum bit error rate in the DLCZ QKD protocol versus distance at the long-distance-limit optimum values of p_c. (c) Normalized QKD rates at the long-distance-limit optimum values of p_c. In all graphs, solid lines correspond to resolving detectors and dashed lines represent the non-resolving cases. The underlying channel is assumed to be optical fiber with 0.17 dB/km loss and $c = 2 \times 10^8$ m/s. The measurement efficiency, $\eta_m = \eta_C \eta_D$, is 0.35.

similar phase shifts, assign different bits to their raw keys, and $H(p) = -p \log_2 p - (1-p) \log_2 (1-p)$.

Figure 2(a) shows R_0 and R_1 as functions of the excitation probability p_c. We assume that the underlying channel is optical fiber with 0.17 dB/km loss. The efficiency of the measurement module, η_m, the product of the atomic-to-photonic conversion efficiency, η_C, and photodetectors' quantum efficiencies, η_D, is 0.35. It can be seen that there exists an optimum value of p_c at which the QKD rates peak. This optimum value is lower for the repeater setup than for the no-repeater case. It is also lower for non-resolving detectors than the resolving ones. Whereas a higher value of p_c increases the heralding rate of success, it creates more error as well, hence in some cases we are better off to start with a lower value of p_c to allow for a higher margin of error by the end of the QKD procedure. The optimum values of p_c are functions of distance as well. For our parameter setting, however, the optimum values are roughly constant for $L > 100$ km.

Figure 2(b) shows QBER versus distance at the optimum values of p_c (long-distance limit). Repeater systems should tolerate a higher error rate because they undergo an extra step of entanglement swapping. Interestingly, the repeater with resolving detector tolerates a higher QBER than the NRPD case. That is because, with resolving detectors, we can use a higher value of p_c, and get a higher generation rate for the raw key in Eq. (1). In all cases, QBER approaches a constant value at long distances. That is because the optimum value of p_c is fixed for long distances, hence, the possibility of multiple excitations is also limited.

Finally, Fig. 2(c) highlights the trade-off between loss in the channel for the no-repeater case versus higher error rates for the repeater case, by comparing R_0 and R_1. Because the QBER is limited, the repeater setup is the eventual winner of this competition. For the parameters used in our calculations, the cross-over distance is around 350 km. For highly efficient BSM modules, this distance will drop to about 150 km; that is about 75 km between each repeater station. To create 1 kbps of secure key we need about 10,000 memories for the DLCZ system. This work was supported by QuantumWorks, OCE, and NSERC Discovery Grant.

References

[1] C. H. Bennet and G. Brassard,"Quantum Cryptography: Public key distribution and coin tossing," in Proc. of IEEE International Conf. on Computers, Systems, and Signal Processing, Bangalore, 175 (1984).
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74,** 145 (2002).
[3] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," Phys. Rev. Lett. **94,** 230504 (2005).
[4] A. K. Ekert, "Quantum cryptography based on Bell's theorem", Physical Review Letters **67,** 661 (1991).
[5] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81,** 5932 (1998).
[6] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," Nature **414,** 413 (2001).
[7] B. Zhao et al., Nat. Phys. **5,** 95 (2009); R. Zhao et al., ibid. **5,** 100 (2009).
[8] M. Razavi, M. Piani, and N. Lütkenhaus, "Quantum repeaters with imperfect memories: Cost and scalability," Phys. Rev. A **80,** 032301 (2009).
[9] M. Razavi and J. H. Shapiro, "Long-distance quantum communication with neutral atoms," Phys. Rev. A **73,** 042303 (2006).
[10] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85,** 441 (2000).
[11] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, "Squashing Models for Optical Measurements in Quantum Communication," Phys. Rev. Lett. **101,** 093601 (2008).