Long-Distance Measurement-Device-Independent QKD

Nicoló Lo Piparo and Mohsen Razavi
School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK

Quantum key distribution (QKD) promises unconditional security for sharing secret keys by relying on the laws of quantum physics. Its practical implementation, however, faces some challenges. For instance, that we need to trust some of the equipment used by our legitimate users poses a threat that has partly been remedied by recently proposed measurement-device-independent QKD (MDI-QKD) schemes [1]. In such schemes, the end users encode (decoy) BB84 signals and transmit them to a middle station at which entanglement swapping operation is performed; see Fig. 1(a)-(b). Channel loss will also impose an exponential decay of the key rate with distance. This can in principle be avoided by using (probabilistic) quantum repeater (QR) setups, which also rely on entanglement swapping. The combination of the two systems, MDI-QKD and QRs, will then provide us with a system that while offers easy affordable access to the end users, will enable them to exchange secret keys over long distances. Here, we present such a hybrid system as in Fig. 1(c), and find the secret key generation rate, R_{QKD}, for such a system.

While MDI-QKD systems can be run using weak laser pulses, quantum repeaters often rely on quantum memories, e.g., (quasi-) atomic systems. Once two quantum memories are entangled, one need to read them out, i.e., convert their internal states to photonic states, and interfere the resulting photons with those sent by QKD users. The photons obtained from quantum memories is typically an imperfect single photon. In our analysis, we then first consider the scheme proposed in [2], see Fig. 1(a), where one (or both) of the sources could be an imperfect single-photon source, representing the memory, and the other is a coherent state. The scheme works as follows. Two parties randomly choose between x and z basis by using diagonal or rectangular polarized beams, respectively, at the source. A partial Bell state measurement (BSM) is performed by an untrusted party in the middle station. A successful partial BSM occurs when one, and only one, of r_0 and r_1, and one, and only one, of s_0 and s_1, click. All other detection events are discarded.

In this work we find R_{QKD} considering various sources of imperfection such as quantum efficiency η_D, path loss η_t, dark count d_c, and the retrieval efficiency of the memories η_b. Figure 2(a) compares R_{QKD} versus the distance for the setup of Fig. 1(a) when both parties use an imperfect single photon source (solid line) with a probability p to emit two photons, and $1-p$ to send exactly one photon, with the case when one of the two parties has a coherent state source (dashed line). By using a coherent state the performance is lower compared to the case when single photons are used. In the latter case, it is possible to reach a longer distance of $\sim$ 450 km.

To establish a secret key to further distances, the setup in Fig. 1(c) is used. Two pairs of quantum memories (QMs) are prepared with an entangled state each. Then, both parties send a photon each, which are coupled with the photons retrieved from the QMs, and sent to a measurement station, where a partial BSM is performed. A successful partial BSM occurs if one, and only one, of the two detectors clicks in each of the four stations. The setup used to distribute entanglement between the QMs is the single photon source protocol proposed in [3]. Our results follow from the analysis in [4] with the aforementioned inefficiencies.

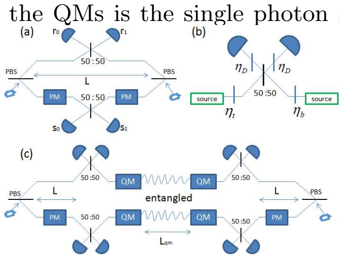

FIG. 1. (a) MDI-QKD setup. (b) Measurement setup. (c) Quantum repeaters + MDI-QKD setup.

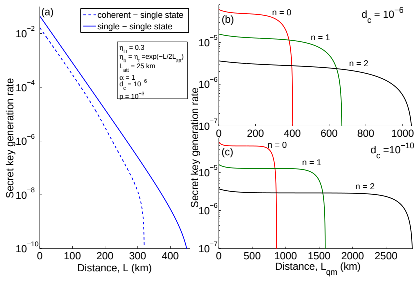

FIG. 2. (a) R_{QKD} versus distance for MDI-QKD with single photon state (solid) and coherent state (dashed) as the source. In (b) and (c) R_{QKD} for MDI-QKD with repeaters up to 2 nesting levels, n, for two different values of dark count.

Figures 2(b) and (c) show R_{QKD} versus distance for the setup of Fig. 1(c) when a quantum repeater protocol is used for two different values of dark count and up to two nesting levels. We can reach a longer distance by using two nesting levels. We also can determine how the dark count affects the cutoff distance. In fact, for $d_c = 10^{-6}$ and for two nesting levels the cutoff distance is $\gtrsim$ 1000 km. It reaches $\sim$ 3000 km for $d_c = 10^{-10}$. Hence, by reducing the dark count, it is possible to reach very long distances, even though the rate of the secret key is not high ($\sim 5 \cdot 10^{-6}$).

[1] H.-K. Lo, M. Curty and B. Qi, Phys. Rev. Lett. 108, 130503 (2012).
[2] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).
[3] N. Sangouard *et al.*, Phys. Rev. A 76,050301 (2007).
[4] N. Lo Piparo and M. Razavi, arXiv:1210.8042v2 (2013).