Memory-Assisted Measurement-Device-Independent Quantum Key Distribution

Christiana Panayi1, Mohsen Razavi1, Xiongfeng Ma2, and Norbert Lütkenhaus3
1School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK
2Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, China
3Institute for Quantum Computing, University of Waterloo, Waterloo, Canada

Quantum key distribution (QKD) is a developing field that enables secure communications between two remote parties, namely, Alice and Bob [1]. The security of QKD follows from the laws of quantum physics. QKD relies on single photons to generate secret keys. That would impose numerous problems when long-distance communications is concerned. Moreover, detection loopholes often open up the system to security threats [2]. Recently, a measurement-device independent QKD (MDI-QKD) scheme has been proposed [3], which, by relying on entanglement swapping techniques, remedies, to some extent, both issues. In this paper, we take one step further and use quantum memory modules before entanglement swapping to further improve the rate-versus-distance behavior. We study the required characteristics of the employed quantum memories, and find out at which point a system equipped with memories outperforms a fully optical setup.

The main advantage of our protocol, as compared to a full quantum repeater setup, is the possibility of running our protocol at a faster rate than that of quantum repeaters. In our scheme, the repetition rate is limited by the writing time into memories, whereas in quantum repeaters, the repetition rate of the protocol is determined by the distance of the shortest segment in the system. That is if fast quantum memories are available, our protocol can be run at a faster rate, hence allowing memories with possibly lower coherence times to be used. Figure 2 shows the required coherence time for the memories in our protocol (figure 1), as compared to that of a probabilistic quantum repeater system [4]. The latter requires a coherence time on the order of the transmission delay L/c between the two end parties, whereas, in the former, that would also depend on the repetition period of single-photon sources. It can be seen that for writing times, τw, shorter than 10 ns, the required coherence time, for our protocol, is lower than that of such quantum repeaters for roughly up to 500 km. This would imply that our protocol can possibly be implemented even with current imperfect memories, whose coherence times are not sufficiently long for quantum repeater purposes.

Our proposed scheme is not scalable with distance the same way that quantum repeaters are. Its less demanding memory requirements can, however, be used to demonstrate the first generation of long-distance QKD systems that outperform no-memory QKD systems. This can be considered as a midterm objective for experimentalists in the field before the first, and higher, generations of quantum repeaters become available.

The latter could rely on quantum error correction techniques and deterministic entanglement swapping operations, both of which require further advances in our quantum computing and memory capabilities. This research has received funding from the European Seventh Framework Programme under Grant Agreement 277110 and the UK Engineering and Physical Science Research Council Grant No. EP/J005762/1.

REFERENCES