Measurement-device-independent quantum key distribution with Nitrogen Vacancies in Diamond

Nicolo' Lo Piparo[1], **Mohsen Razavi**[1], **and William J. Munro**[2]

[1]*School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK*
[2]*NTT Basic Research Laboratories, NTT Corporation, Atsugi, Japan*

Long-distance quantum key distribution (QKD) enables the exchange of secret data without the need to trust intermediate nodes. Quantum repeaters are often considered to be the main means to achieve this goal, but they are facing numerous technical challenges, e.g., the development of reliable quantum memory (QM) units, along their way of implementation. An interim technique to increase the quantum communication range has been proposed in [1], where the authors introduce a *memory-assisted* measurement-device-independent QKD (MDI-QKD) [2] scheme. Such systems will resemble a single-node quantum repeater link with QMs in the middle node. There is, however, no QMs at the users' ends and they are only equipped with encoder/source modules. Instead of distributing entanglement over elementary links, users send BB84-encoded states toward the memories, and once both memories are loaded with the relevant states, an entanglement swapping operation is performed on the memories. This scheme offers the same advantages as in MDI-QKD, i.e., it is resilient to side-channel attacks on the measurement devices. In addition, it improves the rate versus distance behavior without requiring the same demanding specifications on the QMs. More specifically, it relaxes some of the requirements on the coherence time of the QMs if their access time is comparatively short. While the schemes proposed in [1] are not scalable with distance the same way that quantum repeaters are, they eases the way for future generations of quantum networks, on the one hand, and, on the other, they offer QKD services over a range of distances not currently available by conventional direct QKD links.

The performance of the memory-assisted schemes of [1] much relies on their employed QMs. Initially, ensemble-based memories were considered as suitable candidates for this task because of their short sub-nanosecond writing times. It turned out, however, that, within the proposed schemes in [1], the multiple-excitation effect in such QMs would prevent the memory assisted MDI-QKD protocol to beat the no-memory QKD schemes, as shown in [3]. Here, we present a memory-assisted MDI-QKD protocol that outperforms the original MDI-QKD scheme by using nitrogen vacancy (NV) centers in diamond as QMs. We particularly focus on the cavity enhanced NV centers and show that, in terms of the secret key rate per transmitted pulse, we can beat the no-QM QKD systems by up to three orders of magnitude as shown in Fig. 1. Using system parameters achievable by the today's state of the art, we then anticipate some total key rate advantage in the distance range between 300 km and 500 km. We also use NV centers as single-photon sources (SPSs) and propose an SPS-based [4] memory-assisted MDI-QKD protocol embedded with ensemble-based memories. We show that, with ideal SPSs, our method can outperform the no-QM systems, but cannot beat the proposed system here that uses NV centers as QMs (see Fig. 1). In our analysis, we account for major sources of error including the dark count, the channel loss, and the decoherence of the QMs. In conclusion, we note that NV centers in diamond can offer practical solutions for the memory-assisted QKD, in the meantime, and for long-distance QKD in the future.

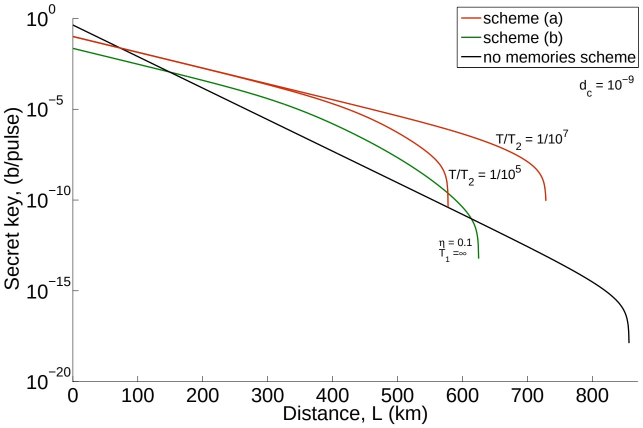

Figure 1: Secret key rates per transmitted pulse for the memory-assisted MDI-QKD protocol with NV centres (red curves), with ensemble-based memories (green curve) plus SPS, and no-memory scheme (black curve). Here, the dark count rate is $10^{-9}/s$, the detector efficiency is 0.93 and the channel loss over distance L is given by $e^{-L/L_{\mathrm{att}}}$, where L_{att} = 25 km. In the figure, T, T_1, and T_2, respectively, represent the repetition period, the decoherence time constant for a depolarizing channel, and the amplitude decay time constant.

References

[1] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, "Memory-assisted measurement-device-independent quantum key distribution," *New. J. Phys.*, vol. 16, p. 043005, 2013.

[2] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130503, Mar 2012.

[3] N. Lo Piparo, M. Razavi, and C. Panayi, "Measurement-device-independent quantum key distribution with ensemble-based memories," *IEEE Journal of selected topics in quantum electronics*, vol. 21, May/June 2015.

[4] N. Sangouard, C. Simon, J. c. v. Minář, H. Zbinden, H. de Riedmatten, and N. Gisin, "Long-distance entanglement distribution with single-photon sources," *Phys. Rev. A*, vol. 76, p. 050301, Nov 2007.