Toward feasible long-distance quantum communications systems

National Inst. of Informatics , Leeds Univ. ○Nicolo Lo Piparo

E-mail: nicopale@gmail.com

In the past few years, quantum cryptography has received a big attention due to its goal of guaranteeing secure communication. In particular, quantum key distribution (QKD) is one of the most promising techniques for the secure exchange of cryptographic keys between two users. Its unique property of relying on the laws of physics makes it an appealing tool for secure communications. Here, we present some of the QKD systems theoretically proposed at the University of Leeds within the quantum communication hub (QCH) program.

The QCH program's goal is to implement technological devices based on QKD in the near future. The QCH program gathers several British universities, each of them working on different aspects of QKD, such as the chip-scale integration of QKD and the design and delivery of practical hand-held devices (Bristol University, York University), the creation of a national UK network (Cambridge University and Toshiba), the exploration of new theoretical approaches, applications and protocols for implementation of next generation quantum communication systems (Leeds University, Sheffield University).

At the University of Leeds, we focus on obtaining long-distance secure communications by using trust-free intermediate nodes between two users. While QKD has been implemented over distances on the order of a few hundreds of kilometers, the transmission rate of the key severely drops, when we go to further distances. An easy solution to this could rely on a network of trusted nodes. This solution, however, is far from ideal. Quantum repeaters are at the core of our work and we analytically study different systems under realistic scenarios. We cover a range of repeater setups incorporating quantum memories (QMs), in terms of their short-term and long-term feasibility. We then analytically compare the performance of two probabilistic quantum repeater protocols by calculating their secure key rates. Then, we combine a quantum repeater scheme with the measurement-device-independent (MDI) QKD protocol and we derive the largest distance that is possible to reach under practical assumptions. Finally, we study the performance of a memory-assisted MDI-QKD (MA-MDI-QKD) scheme by using Nitrogen Vacancy (NV) centers in diamond as QMs. The MA-MDI-QKD scheme aims at improving the rate-versus-distance behavior of a QKD system, while relaxing some harsh constraint on QMs needed for quantum repeaters. Therefore, MA-MDI-QKD can be considered as a middle step towards the implementation of quantum repeater systems.

Overall we obtain a realistic account of what can be done with existing technologies in order to improve the reach and the rate of QKD systems within a larger quantum network.