A scalable quantum key distribution network based on time-bin entanglement - reloaded

Maximilian Tippmann, Jakob Kaltwasser, Maximilian Mengler, and Thomas Walther

TU Darmstadt, Institute for Applied Physics, Schlossgartenstr. 7, Darmstadt, Germany

With the upcoming rise of quantum computers, most commonly used cryptography schemes in day-to-day communications will in time turn insecure. One way to preserve security is the development of quantum key distribution (QKD) and deployment of QKD-systems in large networks. For that, robust and scalable systems are needed.

We contribute to that goal with the construction and extension of a star-shaped QKD network utilizing the entanglement based BBM92 protocol. Adapting to the needs of a metropolitan network, we followed a fiber-based approach and chose time and phase as the bases of entanglement as opposed to polarization, which would be subject to varying birefringence in the fibers, e.g. due to vibrations or thermal instabilities [1].

Here, we report on the progress in various aspects of our QKD network. Specifically, in this contribution we address the scalability and cost of the system by simplifying the source setup, reducing the number of necessary detectors per party by implementing detector time multiplexing (DTM) [2] and physically separating two parties completing a key exchange including error correction.

This research has been funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation), under Grant No. SFB 1119–236615297.

[1] E. Fitzke, L. Bialowons, T. Dolejsky, M. Tippmann, O. Nikiforov, T. Walther, F. Wissel, and M. Gunkel, PRX Quantum 3 (2022) 020341.

[2] J. Kaltwasser, J. Seip, E. Fitzke, M. Tippmann, and T. Walther, PRA 109 012618.