Time-Frequency QKD over Free-Space and Fiber Channels

J. Rödiger[1,2], N. Perlot[1], R. Freund[1], O. Benson[2]
[1]Fraunhofer Heinrich Hertz Institute, Einsteinufer 37, 10587 Berlin, Germany
[2]Humboldt-Universität zu Berlin, AG Nanooptik, Newtonstraße 15, 12489 Berlin, Germany

Quantum key distribution (QKD) is used to distribute a secret key to two parties, which can be used for absolutely secure communication. We investigate a QKD scheme based on the time-frequency uncertainty relation, referred to as time-frequency (TF-) QKD. It is a BB84-like QKD protocol with the two bases being realized by modulations in time and frequency (see Fig. 1), namely pulse position modulation (PPM) and frequency shift keying (FSK) containing one photon per symbol. Measuring in one of the bases increases the uncertainty in the other basis and thus deletes most information encoded therein.

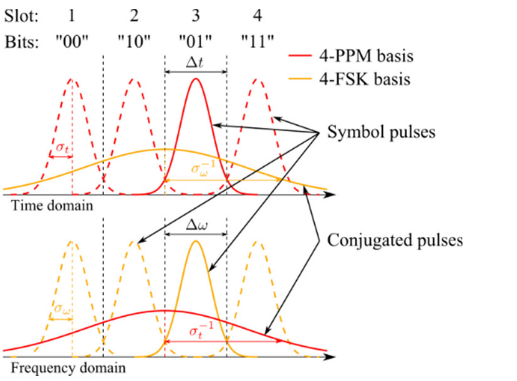

Fig. 1: PPM and FSK modulations. Symbol pulses carry the information, while conjugated pulses are measured, when the basis choice of sender and receiver differ.

TF-QKD is highly compatible with classical communication systems as it can be implemented mostly with standard telecom components in the 1550 nm band. PPM is also well suited for free-space communication. Furthermore, in TF-QKD, polarization is not used (contrary to polarization-based BB84) and thus can be used for duplexing.

With PPM and FSK, it is possible to use an arbitrarily large alphabet and thus to transmit multiple bits per photon. Modulations for four symbols per basis are shown in Fig. 1. Transmitting multiple bits per photon is especially beneficial when many photons reach the detector, thus saturating it, or when there are other limits on the photon rate, e.g. an upper limit on the gating frequency for detectors (e.g. InGaAs avalanche photon-diodes) which need to be operated in gating mode.

We have reported a back-to-back implementation of the TF-QKD protocol [1], the performance of which has been improved since then. In addition, we performed numerical simulations showing which pulse forms are preferable and implying that a higher number of symbols per basis increase the secret key rate (see Fig. 2) [2]. An experiment using four symbols in each basis (4-PPM and 4-FSK) was also successfully demonstrated as a first step toward large alphabets. Experiments over both free-space and fiber channels have been performed.

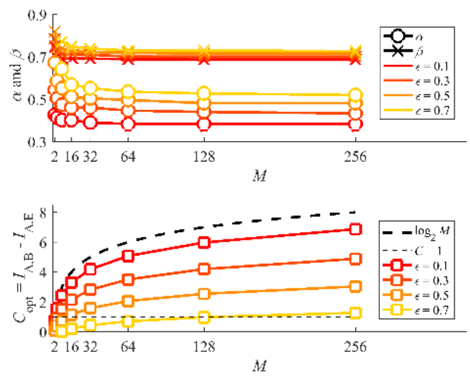

Fig. 2: Optimal relative width of symbol pulses α and conjugated pulses β (top), and estimated channel capacity in bit/photon (bottom), depending on the number of symbols M.

In various scenarios the TF-QKD protocol offers significant advantages: Photons can carry multiple bits, it can be implemented with mostly classical communication components and it is compatible to classical communication systems. Summarizing, TF-QKD is beneficial for fiber as well as for terrestrial or satellite based free-space communication.

[1] M. Leifgen, R. Elschner, N. Perlot, C. Weinert, C. Schubert, and O. Benson, *Phys. Rev. A*, vol. 92, no. 4, p. 042311, 2015.

[2] J. Rödiger, N. Perlot, R. Mottola, R. Elschner, C.-M. Weinert, O. Benson, and R. Freund, *Phys. Rev. A*, vol. 95, p. 052312, May 2017.