Testing of the Time-Frequency QKD-Protocol over different Transmission Channels

F. Beutel[1,2], J. Rödiger[1,2], N. Perlot[1], O. Benson[2], R. Freund[1]
[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) provides means to securely transfer keying material between two parties, backed by the fundamental laws of quantum physics.

While the traditional BB84 protocol uses different polarization orientations as bases for the signal encoding, the use of modulation in time or frequency has previously been proposed as a promising alternative. In this so called time-frequency (TF-) QKD protocol, pulses are either encoded using pulse-position modulation (PPM) or frequency-shift keying (FSK). Due to the time-frequency uncertainty and similar to traditional BB84 protocols, measuring in the wrong basis increases the uncertainty in the other basis, hence information encoded therein is deleted (Fig. 1). One advantage of the TF-protocol is the ability to encode more than one symbol per basis. Since no polarization encoding is used, it remains a candidate for the implementation of multiplexing like bidirectional communication.

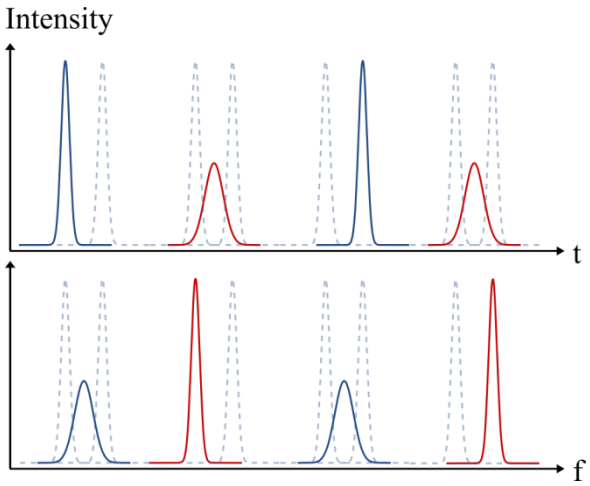

Figure 1: Pulse forms of PPM pulses (blue) and FSK pulses (red) in both, time and frequency domains. Measuring in the wrong basis leads to a loss of information.

Recently we have implemented the TF-QKD protocol in the laboratory using mostly standard telecom-components and avalanche photo-diodes (APDs) as single photon detectors at the 1550 nm wavelength. With strongly attenuated laser pulses on average less than one photon per pulse is being sent. However, with the current setup the decoy-state method can easily be integrated.

We measured the quantum bit error rate (QBER) as well as the achieved raw key rates depending on the transmission line and pulse widths used. Considering a simple intercept-resend eavesdropping attack we were able to numerically calculate bounds for secret-key rates.

With the back-to-back setup we achieved secret-key rates of about 300 kbit/s. Over a dispersion compensating single-mode fiber of 25 km length, secret key rates of about 80 kbit/s could be achieved. First experiments with transmissions over free-space links have also been realized in the lab and will soon be extended to longer outdoor testbeds of a few hundred meters. Moreover, an implementation with more than two symbols per basis has previously been established.

Because PPM and FSK are well-established coding techniques in classical communication and because of the demonstrated ability to implement secure quantum communication with mostly off-the-shelf telecom components, the TF-QKD protocol is a promising candidate for both, free space and fiber-based QKD implementations.