# Large-Alphabet Time-Frequency Quantum Key Distribution

J. Rödiger[1,2], N. Perlot[1], M. Leifgen[2], R. Elschner[1], R. Mottola[2], 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

We investigate a quantum key distribution (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, namely the pulse position modulation (PPM) and frequency shift keying (FSK) which are well-known in optical telecommunications. Assuming having one photon per pulse, measuring in one of the bases increases the uncertainty in the other basis and thus destroys the information possibly encoded there.

With PPM and FSK it is possible to use an arbitrarily large alphabet, thus to send a higher number of bits per photon. The modulations for four symbols are shown in Fig 1.

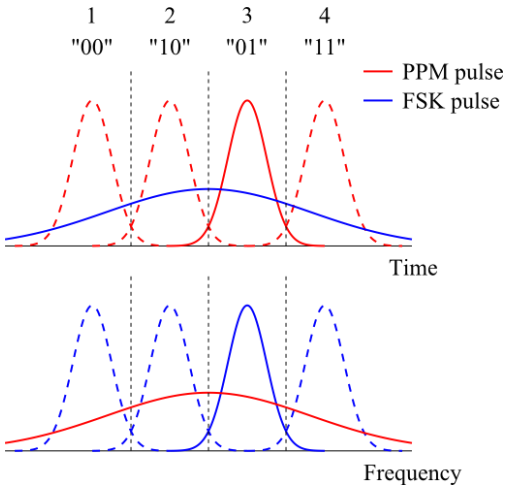


*Fig. 1: PPM- and FSK-modulation in the time and frequency domain. It is possible to have an arbitrary large alphabet in both bases. Here modulations with four symbols, corresponding two bits, are shown.*

With a first proof of principle experiment, using only two symbols per basis, it was possible to distribute a sifted key with a key rate of 12 kbit/s, with the potential of being enhanced by using a larger alphabet.

Our simulations have shown that a larger alphabet not only increases the key rate but also the robustness against the standard intercept/resend eavesdropping attacks, see Fig. 2. The simulations also show an optimal ratio for the pulse separation relative to the pulse distance.

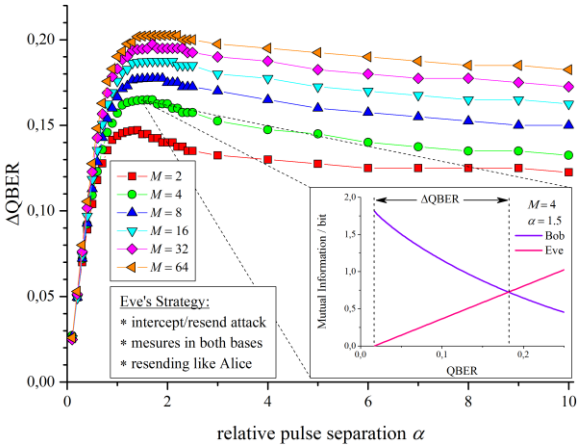


*Fig. 2: Range of quantum bit error rate (ΔQBER), where secure communication is possible, shown over the relative pulse separation α. A larger α represents pulses, which are narrower with respect to the pulse distance. With a larger alphabet M the ΔQBER increases, in other words the protocol becomes more robust.*

TF-QKD can be implemented mostly with standard telecom components, using the 1550 nm telecom band, and thus is compatible to classical communication technology. In addition PPM is a well-established coding technique in free-space communication and therefore TF-QKD is very well suited for combining it with classical free-space communication systems. Furthermore, in TF-QKD polarization is not used (contrary to polarization based BB84) and thus can be used for the duplexing of bidirectional communication, which is an often used technique in free space communication.

Conclusively, for specific applications the TF-QKD protocol has significant advantages over the polarization based BB84 QKD protocol. It is especially promising for implementations such as hybrid systems for classical and quantum free-space communication (e.g. for satellite communication).