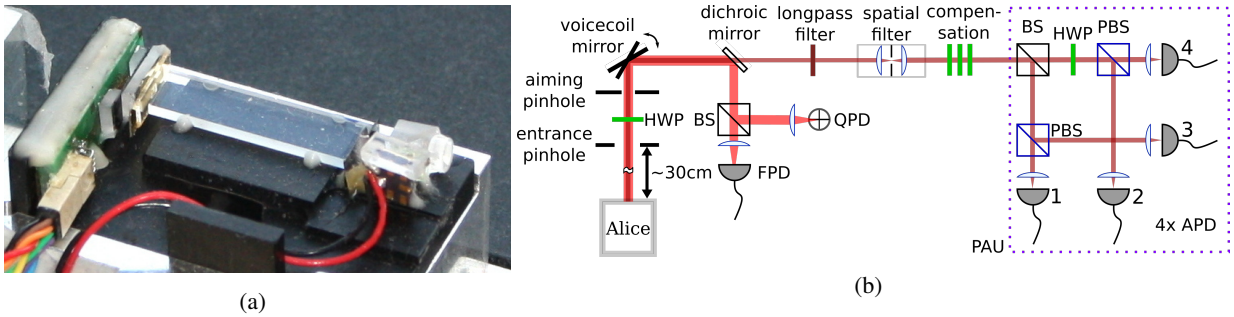
Handheld Quantum Key Distribution

Peter Freiwang[1], Gwenaelle Mélen[2], Jannik Luhn[1], Tobias Vogl[3], Markus Rau[4], Clemens Sonnleitner[1], Wenjamin Rosenfeld[1] and Harald Weinfurter[1,2]

1. Ludwig-Maximilian-University, Munich, Germany
2. Max Planck Institute of Quantum Optics, Garching, Germany
3. Australian National University, Canberra, Australia
4. qutools GmbH, Munich, Germany

Abstract:
We present quantum key distribution between a handheld integrated sender unit and a stationary tracking receiver. This system achieves, at a QBER of 2%, a secure bit rate of several 10 kBit/s.

Quantum Key Distribution (QKD) is an unconditionally secure method, only based on quantum mechanical laws, to generate a shared secret key between two trusted parties. While a large effort is made to extend the range of QKD systems, also short range applications exist, e.g., the secure communication with an ATM or a point of sale. At this point the integration into conventional communication platforms plays a major role. The small size of our sender optics of only $35 \times 20 \times 8\,\mathrm{mm}^3$ [1] (Fig. 1 (a)) realistically allows for the integration into mobile devices. In combination with a tracking receiver (Fig. 1 (b)), it enables a free-space key exchange (operating distance $\sim$ 30cm) in handheld operation [2].



(a) (b)

Fig. 1. (a) Sender module assembled onto a micro-optical bench. The micro-optics consists of a VCSEL array, microlenses, wire grid polarizers, an optical waveguide and a beacon laser. (b) Optical setup of the receiver. Between the entrance pinhole and the polarization analysis unit (PAU), a voicecoil mirror together with a quadrant photo diode (QPD) and a fast photo diode (FPD) enable beam tracking and synchronization. The half wave plate (HWP) behind the entrance pinhole allows for the alignment of the reference frames. The spatial filter restricts the acceptance angle disabling spatial side channel attacks. Three wave plates in front of the PAU serve for the phase compensation of the polarisation states. Silicon avalanche photo diodes (APDs) enable low noise single photon detection.

Our system implements the BB84 protocol using weak coherent laser pulses from four vertical-cavity surface-emitting lasers (VCSELs) at 850 nm, driven by a FPGA controlled printed circuit board operating with a repetition rate of 100 MHz. Light from the VCSELs is polarized using an array of four wire-grid polarizers [3] (H, V, +45, 45) and focused by a microlens array into a waveguide chip to ensure the spatial indistinguishability of the four states. A beacon laser enables beam tracking and is additionally modulated (100 MHz) for synchronization.

The detection and analysis of the QKD signals is made by a four channel polarization analysis unit (PAU, Fig. 1 (b)). The overall transmission of the short free-space distance and the receiver is 41.3%. A fast beam tracking system, realized by a voicecoil mirror with a capture angle of 3° and a quadrant photo diode (QPD), allows a high coupling efficiency in handheld operation (averaged over a measurement time of 10 s up to one third relative to the stationary operation) despite the narrow acceptance angle of 0.15° of the spatial filter for avoiding spatial mode side channels [4]. We employ the tilt sensor of a standard mobile phone, which is placed on top of the sender, for reference frame alignment with a refresh rate of 10 Hz by rotating the HWP behind the entrance pinhole.

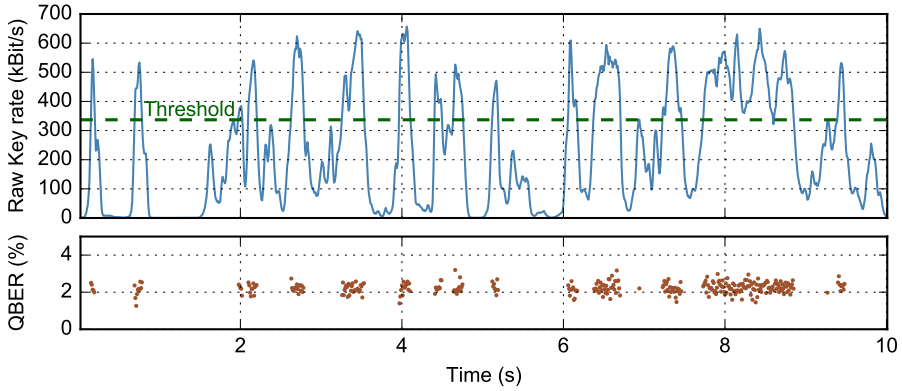


Fig. 2. The raw key rate and the QBER for a typical key exchange over 10 s. Only detections above the detection threshold are used for the generation of a secure key.

Fig. 2 shows an exemplary handheld key exchange with a handheld efficiency of 32.2% achieving an average raw key rate of 150.8 kBit/s at a quantum bit error rate (QBER) of 2.3%. Due to the high total link efficiency, GLLP evaluation [5] still gives satisfying rates and enable a simpler sender module compared to a device for decoy protocols. With a mean photon number of $\mu = 0.045$ and a detection threshold of 337 kBit/s, we achieve a secure key rate of 27.6 kBit/s.

The novel sender module can be integrated in a huge variety of communication schemes, e.g., mobile phones or optical wireless systems connected to a stationary receiver but also in free-space optical systems in urban areas or even micro-satellites. Here, we report the successful key exchange in a handheld scenario, proving the potential of our system to provide future standard components for compact and secure QKD devices for real-life applications.

References

1. G. Vest, M. Rau, L. Fuchs, G. Corrielli, H. Weier, S. Nauerth, A. Crespi, R. Osellame and H. Weinfurter, “Design and Evaluation of a Handheld Quantum Key Distribution Sender module.”, IEEE JSTQE **21**, (2014).
2. G. Mélen, P. Freiwang, J. Luhn, T. Vogl, M. Rau, C. Sonnleitner, W. Rosenfeld and H. Weinfurter, in preparation.
3. G. Mélen, W. Rosenfeld and H. Weinfurter, “Impact of the slit geometry on the performance of wire-grid polarisers.”, Opt. Express **23**, (2015).
4. M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth und H. Weinfurter, “Spatial mode side channels in free-space QKD implementations.”, IEEE Journal of Selected Topics in Quantum Electronics **21**, (2015).
5. D. Gottesman, H. K. Lo, N. Lütkenhaus und J. Preskill, “Security of quantum key distribution with imperfect devices.”, International Symposium on Information Theory, ISIT2004, (2004).