Air to Ground Quantum Key Distribution

Sebastian Nauerth[1*], Florian Moll[2], Markus Rau[1], Christian Fuchs[2], Joachim Horwath[2] and Harald Weinfurter[1,3]

[1]Fakulät für Physik, Ludwig-Maximilians-Universität, 80799 München
[2]Institut für Kommunikation und Navigation, Deutsches Zentrum für Luft- und Raumfahrt, 82234 Weßling
[3]Max-Planck-Institut für Quantenoptik, 80539 München

The range of quantum key distribution (QKD) systems is known to be limited to a few hundreds of km[1–3] due to the attenuation of the channel and the finite signal to noise ratio of available detectors. Satellite based systems, however, could provide efficient links for global scale QKD. While both classical satellite downlinks[4] and long range terrestrial free-space QKD[1, 2] were shown successfully, a quantum key exchange with a rapidly moving platform is still missing. Here we report on the first experimental demonstration of a BB84[5] QKD transmission from an airplane at a speed of 290 km/h to ground. Our system uses attenuated laser pulses with a mean photon number of $\mu = 0.5$ and polarization encoding. Over a distance of 20 km a stable link was achieved for 10 min yielding a sifted key rate of 145 bits/s with a quantum bit error rate (QBER) of 4.8 %.

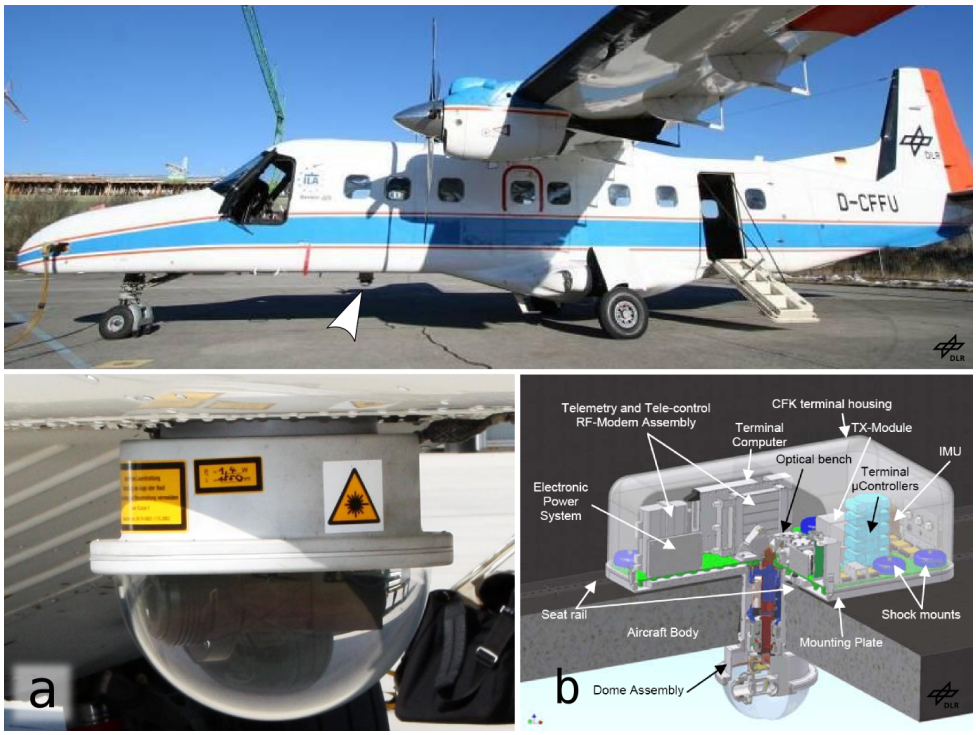

Figure 1: The Do228 aircraft equipped with the flight terminal. One can see the optical dome underneath the fuselage (marker). **a** shows a closeup of this dome housing the coarse pointing assembly. **b** shows a schematic section view of the flight terminal.

The experiment is based on the Free-space Experimental Laser Terminal 2 (FELT2) of the German Aerospace Center (DLR)[6] designed for high data rate classical communications from an airplane to ground using telecom wavelengths around 1550 nm. It consists of a compact integrated flight terminal (fig. 1) and an optical ground station (fig. 2) on top of a DLR institute building. Here we implemented a specifically designed QKD transmitter (Alice) in the flight terminal and equipped the ground station with a receiver[7] suitable to measure the incoming pulses according to the BB84 protocol. Dichroic mirrors were used to couple in and to separate the QKD wavelength of 850 nm.

A first challenge for this demonstration was to achieve a sufficient coupling of the transmitter and receiver telescopes. While in classical free-space communications attenuation can – to some extent – be compensated for by an increased transmitting power, this is not the case for QKD. Therefore the FELT2 pointing system had to be enhanced by a fast fine pointing system, which in the end allowed stable QKD operation for the complete aircraft passage time. In face of a constantly changing relative orientation of the aircraft and the ground station, a second main task was to restore the polarization basis of the qubits arriving at Bob. Especially the mirrors of the coudé-type optics in the FELT2 pointing system introduce varying polarization rotations depending on their angular positions. This would result in excessive QBER, if not compensated.

We therefore measured and modeled theses effects beforehand. This allowed us to deterministically rotate the qubits back with a set of motorized wave plates at Bob. The observed QBER, thus, could be reduced to 4.8 % mainly reflecting the errors due to background events (3 %).

The flights were performed shortly after sunset at the special airport Oberpfaffenhofen near Munich. Before each flight, the coalignment of the QKD beam and the tracking system was checked and readjusted on a distance of 300 m. In flight the QKD pointing could be optimized by introducing small offsets in the FELT2 control loop without affecting the classical link, due to its much wider divergence compared to the QKD beam (1.5 mrad vs. 170 µrad). With the plane going on a roughly semicircular path we were able to transmit qubits for the whole passage time of 10 min producing a total of 80 kBit of sifted key with a QBER of 4.8 %. While decoy states have not been implemented yet, calculations[8–10] prove our system to generate secure key with a rate of 5 Bits/s once additional pulse intensities are used to make the system immune to eavesdropping on attenuated light pulses.

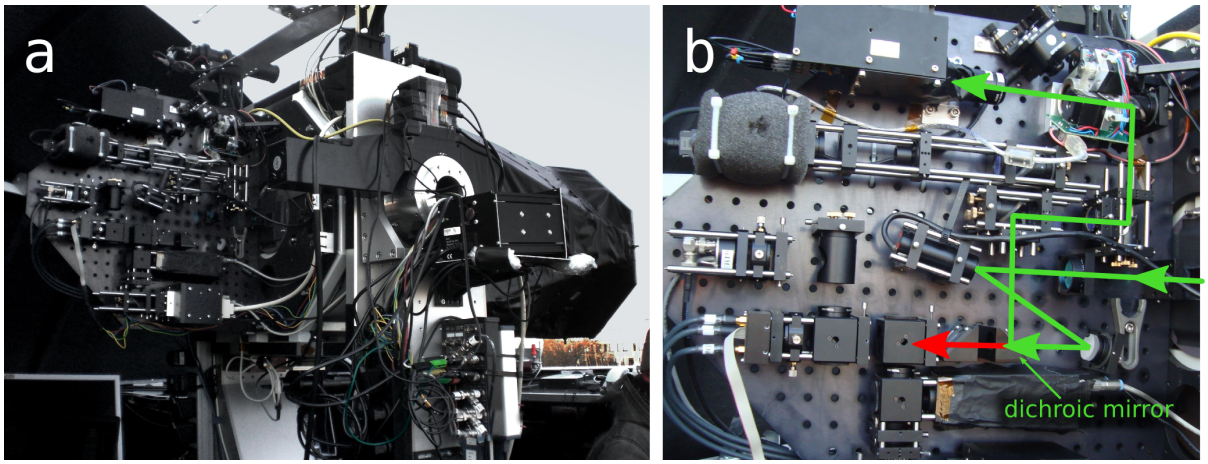

Figure 2: Optical ground station. **a** Telescope of the optical ground station located on the roof of the DLR institute building next to the airport Oberpfaffenhofen. **b** Closeup of the optical breadboard attached to the back of the main telescope mirror indicating the signal path for the qubits (green) and the beacon light (red).

In this work we were able to successfully address both the pointing challenges as well as the requirements for polarization encoded qubits in an airborne scenario and for the first time exchange a quantum key with a rapidly moving platform. Our results are comparable with links to satellites in low earth orbits (LEO) concerning the channel attenuation as well as the angular speed. This demonstration thus clearly proofs the feasibility of QKD to satellites, high altitude platforms or intercontinental planes which together will form the basis for an efficient network enabling secure communication on a global scale.

References

[1] T. Schmitt-Manderbach et al., Phys. Rev. Lett. **98**, 010504 (2007).

[2] R. Ursin et al., Nat Phys **3**, 481 (2007).

[3] P. A. Hiskett et al., New Journal of Physics **8**, 193 (2006).

[4] Y. Takayama et al., in *Free-Space Laser Communication Technologies XXII*, volume 7587, SPIE, 2010.

[5] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 1984.

[6] J. Horwath and C. Fuchs, in *Free-Space Laser Communication Technologies XXI*, volume 7199, SPIE, 2009.

[7] H. Weier, T. Schmitt-Manderbach, N. Regner, C. Kurtsiefer, and H. Weinfurter, Fortschritte der Physik **54**, 840 (2006).

[8] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Physical Review A **72**, 012326 (2005).

[9] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[10] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comput. **5**, 325 (2004).