

Air to Ground Quantum Communication

Sebastian Nauerth^{1*}, Florian Moll², Markus Rau¹, Christian Fuchs², Joachim Horwath², Stefan Frick¹ and Harald Weinfurter^{1,3}

¹Fakultät für Physik, Ludwig-Maximilians-Universität, 80799 München, Germany

²Institut für Kommunikation und Navigation, Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR), 82234 Weßling, Germany

³Max-Planck-Institut für Quantenoptik, 80539 Garching, Germany

*email: sebastian.nauerth@lmu.de

Quantum key distribution^{1,2} (QKD) is the first commercial application in the new field of quantum information with first routine applications in governmental and financial sectors³ and with successful demonstrations of trusted node networks^{4,5}. Today, the grand goal is efficient long range key distribution either via quantum repeaters⁶ or via satellites⁷⁻⁹ in order to enable global secure communication. On the way to QKD via satellites a free-space demonstration of secure key distribution was performed over 144 km between two ground stations¹⁰. This scenario is comparable to links between satellites in low earth orbits (LEO) and ground stations with respect to both attenuation and fluctuations. However, we still miss key exchange with rapidly moving platforms. Here we prove for the first time the feasibility of BB84 quantum key distribution between an airplane and a ground station. Establishing a stable and low noise quantum communication channel with the plane moving with 290 km/h at a distance of 20 km, i.e., 4 mrad/s, our results are representative for typical communication links to satellites¹¹ or to high altitude platforms.

Quantum key distribution provides a whole new level of information security. Any information gained by eavesdropping on the quantum channel can be quantified by the observed transmission noise, the quantum bit error ratio (QBER)¹². Security proofs, solely based on the laws of quantum mechanics, show how to determine the necessary amount of privacy amplification (i.e., key shrinkage according to the QBER) to eliminate the knowledge of a possible adversary¹³. Starting with a first quantum channel of 30 cm length in 1989¹⁴ quantum key distribution quickly was enabled on successively longer distances. Two main branches for communicating qubits encoded with quantum states of light were established: either via telecom fiber channels or via free-space transmission. In both cases increasing attenuation and noise limit the maximum distance for a successful key distribution to typically 150 – 200 km^{10,15,16}. So far, long range free-space quantum communication experiments used a direct line of sight either between two Canary Islands (144 km) or across a lake in China (95 km) to demonstrate free-space QKD, entanglement distribution^{10,17-19}, or quantum teleportation^{20,21}. In spite of this remarkable progress, all quantum communication so far was performed with stationary systems only. Contrary, for classical optical free-space communication high bandwidth links to aircrafts and satellites have been shown to be feasible in recent years^{11,22,23}.

Here we report on an experiment combining recent advances in classical and in quantum optical technologies to demonstrate the feasibility of quantum key distribution from an airplane to ground (fig. 1). Major challenges in this experiment are the higher pointing requirements compared to classical free-space communication, the development of a precise compensation technique to account for the relative rotations of airborne and ground station qubit encoding bases, and the integration of the QKD hardware into an existing communi-

cation system.

The host system for integration of the QKD quantum channel is the "free-space experimental laser terminal 2" (FELT2) in a Donier 228 turboprop aircraft and the optical ground station (OGS) operated by the German Aerospace Center Oberpfaffenhofen^{22,24} (fig. 1). Inside the airplane all lasers and sensors together with electronics for tracking, telemetry and data transmission are built on a 500 mm \times 800 mm optical bench shock mounted to the seat rails. Light is guided via a short tunnel to the coarse pointing assembly (exit aperture 35 mm) in a quartz half dome outside the aircraft fuselage (fig. 1a). The ground station, also capable of optical communication with satellites¹¹, consists of a 40 cm Cassegrain telescope, with the respective laser and receiver systems mounted on an optical breadboard moving with the telescope²² (fig. 1c, for further details see methods).

An initial orientation of the telescopes is accomplished via a GPS based tracking system where the aircraft transmits its position to ground using a low rate UHF telemetry link. With this initial direction, a beacon laser from the ground station illuminates the aircraft, where the FELT2 at the same time performs a scan to acquire the laser signal with its telescope (fig. 1d shows a scheme of the optics and electronics system). The FELT2 now keeps tracking on this signal and so does the optical ground station using the communication laser sent down from the aircraft as beacon source.

While in classical free-space communication the transmitted power can be adjusted within a wide range to compensate coupling loss between transmitter and receiver, for QKD the average intensity per pulse sent over the quantum channel has to be at the single photon level, requiring significantly higher link efficiencies. Thus, we had to narrow down the QKD beam to a divergence of ≈ 180 μ rad (3.4 m diameter at a distance of 20 km, limited by the maximum usable aperture of 15 mm and the beam path in the FELT2 optics), much smaller than the communication beam which was allowed a divergence of 2.6 mrad (diameter 50 m) in this scenario. To guarantee a stable link with this smaller divergence, fine pointing assemblies were implemented and optimized on both sides. Each of them consisted of a fast actuated mirror in a control loop with a position sensitive sensor detecting the beacon light (voice-coil mounted mirror / quadrant photodiode in FELT2 and piezo driven mirror / camera in the OGS). From independent analysis using the coarse pointing camera, we can specify an upper bound of 150 μ rad for the FPA precision even in the presence of engine vibrations aboard the aircraft.

Another important prerequisite for this experiment arises from the polarization encoding used. The relative motion between sender and receiver results in a relative rotation between their coordinate systems. In addition, the numerous mirrors and coatings introduce further birefringent phases. For that reason a motorized polarization controller was developed, which uses three waveplates to compensate for arbitrary polarization rotations. All birefringence was measured beforehand and modeled as a function of the FELT2 telescope angular positions, which were also broadcast via the UHF link.

After enabling an efficient and stable quantum channel the QKD sender and receiver had to be integrated directly into the existing communication system. With the FELT2 covered by a safety hood and the OGS moving continuously there was no possibility for readjustments during flight. Thus, the QKD modules had to be highly robust against vibrations or temperature changes in the plane and at the OGS. A transmitter module (Alice, 80 \times 100 \times 150 mm³) for polarization encoded, attenuated pulse QKD^{25,26} (fig. 2a) was

designed to fit into the FELT2 terminal (fig. 2b). For this proof of principle experiment, the classical optical link was able of unidirectional communication only. To still enable an immediate analysis of the performance even without classical communication between Alice and Bob, we sent a continuous repetition of the four states instead of a random bit string. To switch between alignment and QKD mode intensities, an attenuator is mounted on a servo arm. Additionally, the servo can place a photo diode in the beam path enabling calibration of the pulse intensity by individually tuning the exact brightness of the four diodes electronically. At the ground station (Bob) a dichroic mirror was used to separate the classical and quantum communication wavelengths. The polarization controller was mounted in the quantum channel followed by a four channel QKD receiver²⁵ analyzing the incoming pulses (fig. 2c+d).

The co-alignment of the classical and quantum channels is utterly important as the direction of the QKD beam is not sensed by the tracking control loop. Therefore, the overlap was readjusted before every flight over a test distance of 330 m. In flight, first a fine tuning of the pointing was done with the higher pulse intensity from the QKD-system: A small offset added in the FELT2 fine pointing allowed to optimize the efficiency of the QKD transmission, while the classical link, in this demonstration used for synchronization, was unaffected due to the much higher divergence of the FELT2 laser. Preparations were finished by a recalibration of Alice's pulse intensities to 0.5 photons/pulse.

The airborne QKD transmission was performed shortly after sunset on a roughly circular path around the OGS with a radius of 20 km (fig. 1b, see methods). The new bidirectional fine pointing enabled continuous precise tracking for the whole aircraft passage time of 10 min (fig. 3). We achieved an overall link efficiency of about -38 dB from outside Alice's terminal to Bob's detections. This value includes the detector efficiency of about -4 dB and the losses on the main and secondary telescope mirror, which, using protected aluminum coatings, contribute with at least -2 dB at the QKD wavelength. In addition, signals which were sampled during the flashes from the anti collision lights had to be discarded. Yet, as these flashes are only about 1.5 ms long this reduction does not contribute noteworthy to the overall attenuation. Bob's detectors showed a background rate of about 1000 s⁻¹ each (with dark counts and stray light contributing about equally), while the overall signal count rate was around 800 s⁻¹. With time filtering of $\Delta t = 500$ ps we achieved a mean sifted key rate of 145 bit/s with a QBER of 4.8 %, largely determined by the detector background counts. The technical error²⁷ of signal events contributed only 1.8 % to the QBER. This proves very precise dynamic polarization compensation of the changing aircraft and mirror orientations. During one passage, we were able to gather 80 kbit of sifted key in total. A decoy protocol^{27,28}, necessary to detect eavesdropping on attenuated light pulses, was not implemented here. However, thorough analysis of the data showed that with additional decoy and vacuum pulses one can obtain an asymptotically secure key at a rate of 7.9 bit/s (see methods).

In summary, we demonstrate the possibility of a BB84 key exchange to a fast moving airborne platform. This was possible using an advanced pointing and tracking system, which guaranteed stable transmission of QKD signals at the single photon level and which will significantly improve the performance of future applications of the classical communication link, too. We were able to successfully compensate for mutual rotations of sender and receiver inherent to an airborne scenario and thus achieved a small QBER. Furthermore,

by integrating QKD hardware into an existing communication system, we demonstrate the suitability of QKD as an add-on for a variety of optical and point-to-point radio links. Larger apertures, particularly for the airborne terminal, and quieter single photon detectors will allow to increase the key rate. Given the high angular speed our demonstration achieved a key milestone towards QKD to satellites, high altitude platforms or intercontinental planes which together will form the basis for an efficient trusted node network enabling secure communication on a global scale.

Methods

transmitter and receiver telescopes: The light pulses encoding the QKD states generated in the Alice module are coupled using a dichroic mirror to the terminal’s 1:2 telescope with an exit aperture of 35 mm²⁹. As the QKD beam is fed adjacent to the FELT2 beacon into the telescope, only a diameter of 15 mm of the whole aperture is available. In between its two lenses, a coude type coarse pointing assembly is installed.

The 40 cm Cassegrain telescope (40 : 1) of the OGS is followed by an additional beam compression of 2 : 1 before the light is focused onto the receiver diodes (diameter of 500 μm) with a focal length of 75 mm. The resulting effective focal length of 6 m defines a field of view of 83 μrad for the Bob module.

flight campaign: The experimental flight campaign was scheduled around new moon. While the first day was dedicated to the assembly of the system in the aircraft and its certification, in the following seven days the aircraft was available for flight tests. On two days, flights had to be aborted due to insufficient weather conditions for aircraft operation under visual flight rules and technical problems inhibited two further starts. Yet, three out of four planned flights could be carried out shortly after sunset ($\approx 18:00$) until the night flight ban (21:00). On the first flight, the pointing system was optimized and on the second flight a link with bright pulses (50 photons/pulse) could be achieved between the QKD modules. The quantum key distribution reported here was performed on the last day of the campaign. During this trial it was slightly hazy under a high closed cloud cover which limited the aircraft altitude to 1100 m above ground.

next steps In summary, not yet implemented in this proof-of-principle demonstration are a bidirectional classical communication channel with online sifting and a quantum source of randomness in order to produce shared, secret random numbers. Additionally, enabling varying intensities at the laser diodes allows for an analysis using a decoy state protocol. Future improvements, to enable a secure key exchange even for short transmission durations will comprise better telescope coupling and higher repetition rates.

key analysis: In the analysis of the secure key rate we assume the implementation of a decoy protocol with one weak decoy intensity ν and vacuum pulses in addition to the signal pulses with intensity μ . Information leakage due to side channels (e.g. Laser diode emission times, frequency mismatch, mode overlap) is not taken into account here. Due to variations in the detection efficiencies, the sifted key exhibits a bias of 58 % ones. Balancing the detectors would reduce the sifted key by 16 %.

For a decoy protocol one obtains for the lower bound R of the secure key rate^{13,27,28}:

$$R \geq \frac{1}{2} \left(-Q_{\mu} f(E_{\mu}) H_2(E_{\mu}) + Q_1^L (1 - H_2(e_1^U)) \right) \quad (1)$$

Where Q_μ is the gain²⁷ of signal states, and Q_1^L the gain of single photon pulses. E_μ is the overall QBER observed and e_1^U is the error rate of single photon states. $H_2(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ is the binary entropy function and f models the efficiency of the error correction protocol relative to the Shannon limit³⁰. The factor 1/2 is intrinsic to the BB84 protocol only providing useful results in case of matching bases. Note, however, that this factor can be overcome for long keys³¹. The superscripted values can not be measured directly. The decoy theory, however, provides upper (“U”) and lower (“L”) bounds. For the so called vacuum+weak decoy scheme²⁷ Q_1^L evaluates to

$$Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2} \left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Q_{vac} \right) \leq Q_1 \quad (2)$$

with the gain of decoy (Q_ν) and vacuum (Q_{vac}) states. e_1^U can be written as

$$e_1^U = \frac{E_\mu Q_\mu - 1/2 Q_{vac} e^{-\mu}}{Q_1^L} \geq e_1. \quad (3)$$

In the experiment we observed values of $Q_\mu = 2.86 \times 10^{-5}$, $Q_{vac} = 1.75 \times 10^{-6}$, and a QBER of $E_\mu = 4.77$ % for a mean signal pulse intensity of $\mu = 0.5$ photons/pulse. Within 575 s usable transmission time 164,617 pulses could be registered by Bob resulting in a channel attenuation of $\eta = 42.7$ dB. Note that this value indicates the attenuation for true single photons, the observed attenuation for pulses with poissonian distributed photon numbers is slightly different due to the threshold behavior of the detectors²⁷. With an assumed weak decoy intensity of $\nu = 0.076$ this leads to an asymptotically secure bit rate of 7.9 bit/s Here the fraction of decoy and vacuum pulses of all sent pulses is 12.8 % and 9.5 % respectively.

Given the limited length of the key, with worst case estimations³² of one standard deviation for the statistical error of the QBER and all gain values a key is produced at a rate of 4.8 bit/s, for two standard deviations the secure key rate almost vanishes. Recent more rigorous approaches to incorporate finite key effects with decoy state QKD^{33–35} suggest that more than 10^6 detected signals are necessary to obtain a secret key. Especially with respect to satellite based applications, limited transmission times and thus finite data sets are a challenge in achieving security. Increased repetition rates in the GHz regime and better optics, however, still offer much room for improvements of the raw data rates.

References

- [1] Bennett, C. H. & Brassard, G. Quantum cryptography: Public-key distribution and coin tossing. in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175–179 (1984).
- [2] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
- [3] <http://www.idquantique.com/>.
- [4] Peev, M. *et al.* The secoqc quantum key distribution network in vienna. *New J. Phys.* **11**, 075001 (2009).
- [5] Sasaki, M. *et al.* Field test of quantum key distribution in the tokyo qkd network. *Opt. Express* **19**, 10387–10409 (2011).

- [6] Briegel, H.-J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81**, 5932–5935 (1998).
- [7] Nordholt, J., Hughes, R., Morgan, G., Peterson, C. & Wipf, C. Present and future free-space quantum key distribution. in *Proc. SPIE 4635*, 116–126 (2002).
- [8] Hughes, R. J., Nordholt, J. E., McCabe, K. P., Newell, R. T. & Peterson, C. G. Satellite-based quantum communications. in *Proceedings of Updating Quantum Cryptography and Communications 2010*, 71–72 (Tokyo, 2010).
- [9] Perdignes Armengol, J. *et al.* Quantum communications at ESA: Towards a space experiment on the ISS. *Acta Astronaut.* **63**, 165–178 (2008).
- [10] Schmitt-Manderbach, T. *et al.* Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.* **98**, 010504 (2007).
- [11] Perlot, N. *et al.* Results of the optical downlink experiment KIDO from OICETS satellite to optical ground station Oberpfaffenhofen (OGS-OP). in *Proc. SPIE 6457*, 645704–1 (2007).
- [12] Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
- [13] Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comp.* **5**, 325–360 (2004).
- [14] Bennett, C. H. & Brassard, G. Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working. *Sigact News* **20**, 78–80 (1989).
- [15] Hiskett, P. A. *et al.* Long-distance quantum key distribution in optical fibre. *New J. Phys.* **8**, 193 (2006).
- [16] Rosenberg, D. *et al.* Practical long-distance quantum key distribution system using decoy levels. *New J. Phys.* **11**, 045009 (2009).
- [17] Ursin, R. *et al.* Entanglement-based quantum communication over 144 km. *Nature Phys.* **3**, 481–486 (2007).
- [18] Scheidl, T. *et al.* Feasibility of 300 km quantum key distribution with entangled states. *New J. Phys.* **11**, 085002 (2009).
- [19] Fedrizzi, A. *et al.* High-fidelity transmission of entanglement over a high-loss free-space channel. *Nature Phys.* **5**, 389–392 (2009).
- [20] Yin, J. *et al.* Teleporting independent qubits through a 97 km free-space channel. *Preprint at <http://arxiv.org/abs/1205.2024>* (2012).
- [21] Ma, X. *et al.* Quantum teleportation over 143 kilometres using active feed-forward. *Nature* **489**, 269–273 (2012).
- [22] Horwath, J. & Fuchs, C. Aircraft to ground unidirectional laser-communication terminal for high resolution sensors. in *Proc. SPIE 7199*, 719909 (2009).

- [23] Takayama, Y. *et al.* Expanded laser communications demonstrations with aircraft and ground stations. in *Proc. SPIE 7587*, 75870D (2010).
- [24] Giggenbach, D., Horwath, J. & Markus, K. Optical data downlinks from earth observation platforms. in *Proc. SPIE 7199*, 719903 (2009).
- [25] Weier, H., Schmitt-Manderbach, T., Regner, N., Kurtsiefer, C. & Weinfurter, H. Free space quantum key distribution: Towards a real life application. *Fortschr. Phys.* **54**, 840–845 (2006).
- [26] Nauerth, S., Fürst, M., Schmitt-Manderbach, T., Weier, H. & Weinfurter, H. Information leakage via side channels in freespace BB84 quantum cryptography. *New J. Phys.* **11**, 065001 (2009).
- [27] Ma, X., Qi, B., Zhao, Y. & Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).
- [28] Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
- [29] Moll, F. *et al.* Communication system technology for demonstration of BB84 quantum key distribution in optical aircraft downlinks. in *Proc. SPIE 8517*, 851703 (2012).
- [30] Shannon, C. E. A mathematical theory of communication. *Bell Syst. Tech. J.* **27**, 379–423, 623–656 (1948).
- [31] Lo, H., Chau, H. & Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.* **18**, 133–165 (2005).
- [32] Zhao, Y., Qi, B., Ma, X., Lo, H. & Qian, L. Experimental quantum key distribution with decoy states. *Phys. Rev. Lett.* **96**, 070502 (2006).
- [33] Cai, R. & Scarani, V. Finite-key analysis for practical implementations of quantum key distribution. *New J. Phys.* **11**, 045024 (2009).
- [34] Song, T., Zhang, J., Qin, S. & Wen, Q. Finite-key analysis for quantum key distribution with decoy states. *Quant. Inf. Comp.* **11**, 374–389 (2011).
- [35] Hasegawa, J., Hayashi, M., Hiroshima, T. & Tomita, A. Security analysis of decoy state quantum key distribution incorporating finite statistics. *Preprint at <http://arxiv.org/abs/0707.3541>* (2007).

Acknowledgements

We acknowledge funding by the EU (Q-ESSENCE) and the German BMBF (CHIST-ERA project QUASAR). S.N. acknowledges support by the Elite Network of Bavaria through the excellence program QCCC.

Author Contributions

All authors contributed equally to the realization of the experiment, discussed the results and commented on the manuscript at all stages. S.N., M.R. and S.F. designed, built and operated the QKD hardware new to this project. F.M., C.F. and J.H. initially developed the optical communications (classical) system, took care of modifications and operations and organized the flight campaign including airworthiness certification. S.N. evaluated the data and H.W. supervised the work.

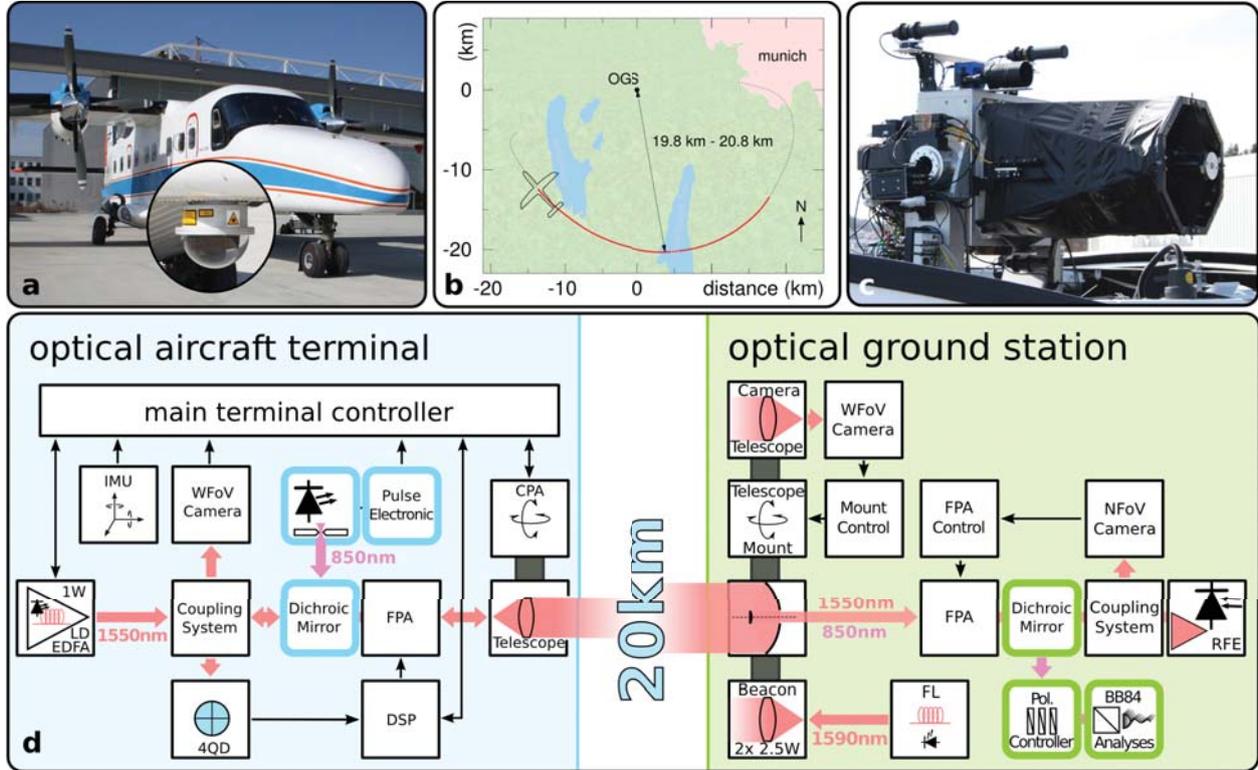


Figure 1: Overview of the classical communication system of the German Aerospace Center's Institute of Communications and Navigation. Initially developed to provide efficient communication for large area monitoring²² it is able to provide a stable link using optical tracking with beacon lasers on ground station and aircraft side. **a**, Dornier 228 used in this experiment with the inset showing the optical dome housing the coarse pointing assembly. **b**, Airplane track with the red section indicating the positions during QKD-transmission. **c**, Optical Ground Station telescope. **d**, Sketch of airborne and ground terminal with integrated QKD system (colored boxes). Laser diode and Erbium doped fiber amplifier (LD EDFA), inertial measurement unit (IMU), digital signal processor (DSP), wide field of view (WFoV) camera, narrow field of view (NFOV) camera, four quadrant diode (4QD), coarse pointing assembly (CPA), fine pointing assembly (FPA), fiber laser (FL), and receiver front-end (RFE).

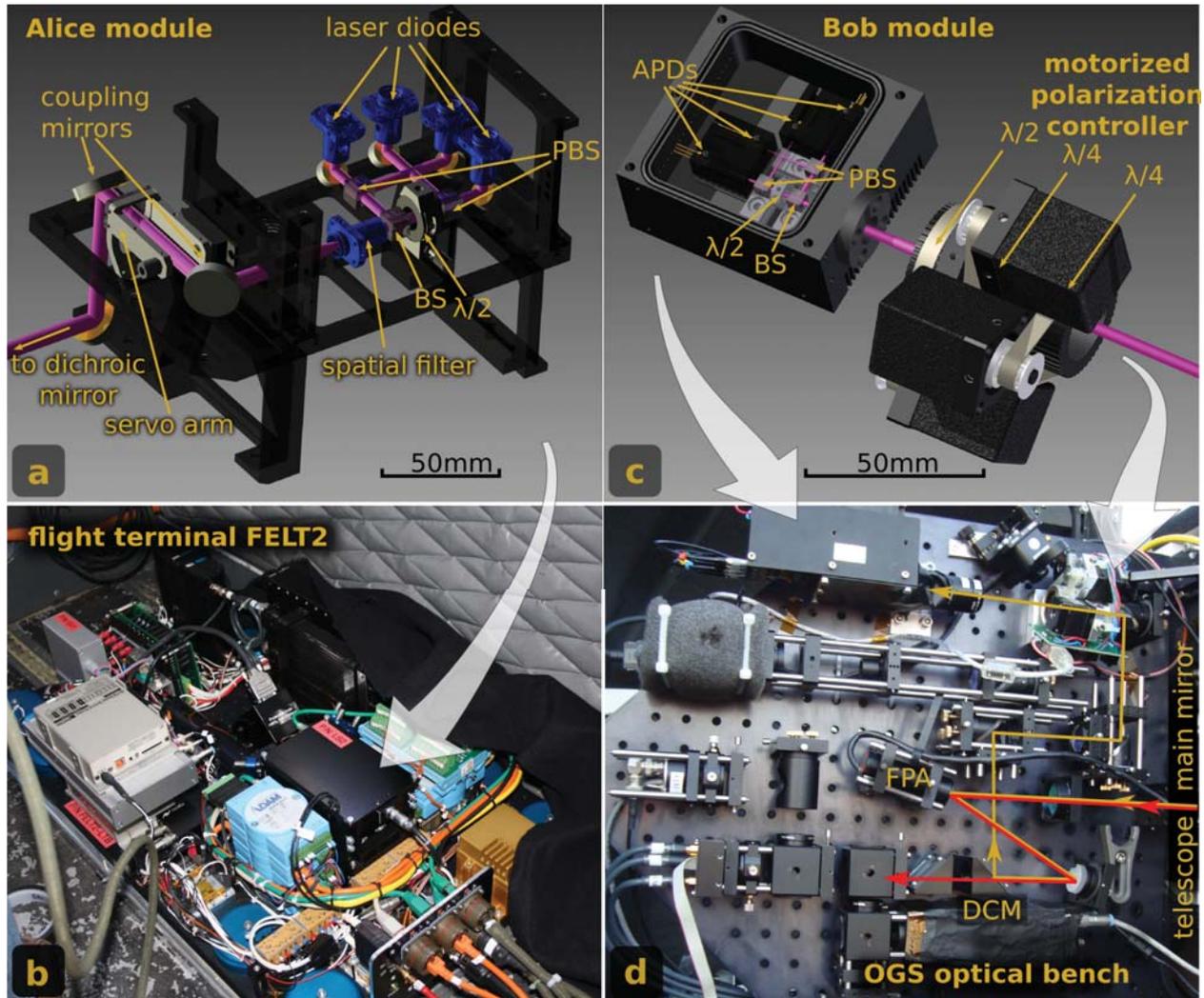


Figure 2: QKD and classical communication hardware. **a**, Illustration of the Alice module. Four laser diodes emit short pulses (1 ns, 10 MHz, 850 nm). Their light is overlapped using (polarizing) beam splitters (BS, PBS) in a spatial filter. A half wave plate ($\lambda/2$) is used to set the angle between the two BB84 bases. Two precision mounted mirrors and a dichroic mirror are used to overlap the 850 nm output with the classical link (1550 nm). **b**, Photo of the module mounted in the FELT2 terminal. For safety reasons the FELT2 has to be covered during flight by a fiberglass hood and is then controlled via Ethernet and USB using laptops only. **c**, Design of the Bob module and the free-space polarization controller (waveplates $\lambda/4$, $\lambda/2$). Four avalanche photo diodes (APD) analyze the state of the QKD-signals randomly in the H/V and $\pm 45^\circ$ basis. **d**, the optical bench attached to the back of the OGS main mirror with the Bob module and polarization controller mounted in the upper part. The incoming beam from the telescope first hits the mirror of the fine pointing assembly (FPA) and is then divided spectrally at the dichroic mirror (DCM). While the 1550 nm light from the aircraft beacon is analyzed to maintain the pointing and recover classical data, the 850 nm signal is directed to the QKD analysis behind an interference filter (FWHM 10 nm).

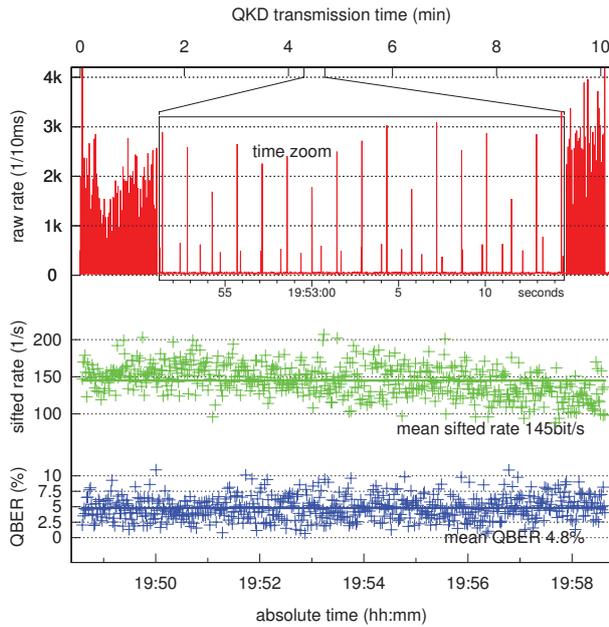


Figure 3: Count rates registered during one aircraft passage (duration 10 minutes and 4 seconds). The raw detector event rate (red) is dominated by the background from the anti collision flashes of ≈ 1.5 ms length. One can clearly distinguish between the flash light close to the terminal dome and the other one at the back of the aircraft. For the analysis the detection events were filtered to remove this background by a simple rate threshold. The sifted key rate (green) and the QBER (blue) are given as averages over intervals of 1 s respectively. The solid lines show the mean value of the whole data.