Communication system technology for demonstration of BB84 quantum key distribution in optical aircraft downlinks

Florian Moll*[a], Sebastian Nauerth[b], Christian Fuchs[a], Joachim Horwath[a], Markus Rau[b], Harald Weinfurter[b, c]

[a]Institute of Communications and Navigation, German Aerospace Center (DLR), Oberpfaffenhofen, 82234 Weßling, Germany; [b]Fakultät für Physik, Ludwig-Maximilians-Universität, 80799 München, Germany; [c]Max-Planck-Institut für Quantenoptik, 80539 München

ABSTRACT

Quantum Key Distribution (QKD), either fiber based or free-space, allows for provably secure key distribution solely based on the laws of quantum mechanics. Feasibility of QKD systems in aircraft-ground links was demonstrated with a successful key exchange. Experiment flights were undertaken during night time at the site of the German Aerospace Center (DLR) Oberpfaffenhofen, Germany. The aircraft was a Dornier 228 equipped with a laser communication terminal, originally designed for optical data downlinks with intensity modulation and direct detection. The counter terminal on ground was an optical ground station with a 40 cm Cassegrain type receiver telescope. Alice and Bob, as the transmitter and receiver systems usually are called in QKD, were integrated in the flight and ground terminals, respectively. A second laser source with 1550 nm wavelength was used to transmit a 100 MHz signal for synchronization of the two partners. The so called BB84 protocol, here implemented with faint polarization encoded pulses at 850nm wavelength, was applied as key generation scheme. Within two flights, measurements of the QKD and communication channel could be obtained with link distance of 20 km. After link acquisition, the tracking systems in the aircraft and on ground were able to keep lock of the narrow QKD beam. Emphasis of this paper is put on presentation of the link technology, i.e. link design and modifications of the communication terminals. First analysis of link attenuation, performance of the QKD system and scintillation of the sync signal is also addressed.

Keywords: Quantum key distribution, free-space optical communication, aircraft-ground link

1. INTRODUCTION

Free-space optics (FSO) will enable future aeronautical communications to exploit the benefit of optical frequencies to achieve highest data rates together with compact transceivers. Several investigations and demonstrations proofed the feasibility of this technology [1][2][3][4] and commercial systems are already available [5][6]. The advantages of optical communication systems are well known: high modulation bandwidth, small terminal sizes, and high efficiency of transmit power. Although, the divergence of the transmit beam is relatively narrow and therefore the foot-print small, compared to radio frequency systems, the communication system is not free from interception. However, particular applications have to be fully tap-proof. For that requirement, quantum key distribution (QKD) is the most promising technology and conventional free-space systems may serve as basis [7]. QKD systems are already proven to be suitable for secure key transmission in a range of experiments [8][9], and are also available off-the-shelf [10]. Since the overall idea of global secure communication is a key exchange between satellites and ground stations, the precursor step following this goal is a demonstration of QKD between aircraft and a ground station. In this scenario, similar conditions as they exist in LEO-ground links can be created and therefore, feasibility of the technology further evaluated. Thus, the goal of this experiment was to proof and demonstrate feasibility of QKD with the BB84 protocol [11] from a fast moving airborne platform.

Since the signal paths in the FSO system from the signal sources to the transmitter antenna (and vice versa) are all optical, integration of additional optical systems using the same free-space path can be easily realized. The Free space Experimental Laser Terminal 2 (FELT2) [2] and the Optical Ground Station Oberpfaffenhofen (OGS-OP) of the DLR Institute of Communications and Navigation hosted a QKD system of the Ludwig-Maximilians-Universität Munich.

*florian.moll@dlr.de

Laser Communication and Propagation through the Atmosphere and Oceans,
edited by Alexander M. J. van Eijk, Christopher C. Davis, Stephen M. Hammel, Arun K. Majumdar,
Proc. of SPIE Vol. 8517, 851703 · © 2012 SPIE · CCC code: 0277-786X/12/$18 · doi: 10.1117/12.929739

The QKD transmitter, called Alice, was integrated in the airborne terminal, the receiver, called Bob, in the ground station. Care was especially taken not to interfere somehow with the communication link equipment but serve as an add-on which is compact and easy to install. The place of the experiments was the DLR site Oberpfaffenhofen, 30 km in the West of Munich, Germany. The flight carrier was the DLR aircraft Do228-212. The flight height was between 1100 m and 1300 m, the distance between OGS-OP and aircraft about 20 km. A scenario illustration is in Figure 1.

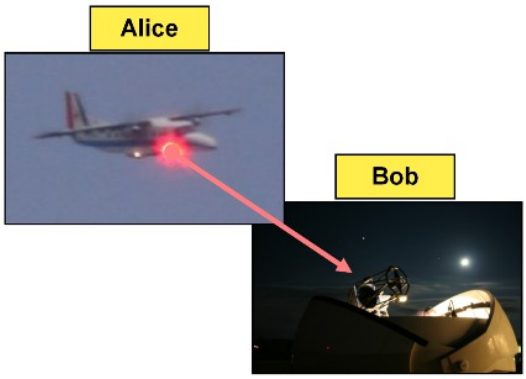

Figure 1. Scenario illustration for the quantum key distribution flight experiments. The ground station is located at the DLR site Oberpfaffenhofen near Munich, Germany. The flight routes were approximately southern half circles with 20 km radius around Oberpfaffenhofen.

This paper describes the undertaken flight campaign and shows first results and analysis of the achieved measurements. In the following, first the basic principle of the QKD algorithm is explained. Then the link design of the QKD system is outlined and the respective terminals and its integrated components explained. Then, overview of the conducted flight experiments is given and results are discussed. In the remainder of this paper, the communication system is designated as Comm system, the designations QKD system and Alice and Bob remain.

2. QUANTUM KEY DISTRIBUTION WITH BB84

Two technologies, both promising secure communication with quantum key distribution [12], are in the focus of industry oriented research these days: QKD with entangled photons and QKD with the BB84 protocol using encoded attenuated pulses. Whereas the first technology exploits the quantum effect of entanglement of particular states [13], the second uses an encoding algorithm developed by Bennet and Brassard in 1984 [11]. For secure key distribution the BB84-protocol combines two quantum mechanical effects. The first is the indistinguishability of two orthogonal states in a corresponding diagonal basis. The second is the no-cloning theorem. Different polarizations of a single photon denote different states. Instead of using the same basis for all transmission, the transmitter continuingly and randomly changes between the two bases. Thus, each bit uses either the (H;V) or (+45;-45) basis. Eventually, photons are transmitted that have either horizontal, vertical, or diagonal (in both directions) polarization. Transmitter and receiver must use a common coding scheme like the example given in Table 1.

Table 1. Coding of classical bits with polarization states in two different bases as suggested in [11].

Basis	Classical bit value	Polarization
(H; V)	0; 1	0°; 90°
(+45; -45)	0; 1	+45°; -45°

Without knowledge of the corresponding basis it is impossible to decode deterministically weather a received photon denotes a “0” or “1”. For instance, if a photon is sent with (H;V) basis and measured in (+45;-45) basis, there is always a fifty-fifty chance to be measured in either +45° or -45° which makes eavesdropping difficult. But since the receiver, that is supposed to receive the key, does not have the information either, it must choose its basis randomly, too. Therefore, it will also have a non-deterministic result in fifty percent of the measurements. With classical information exchange of the used bases – i.e. any means of yet authenticated communication like email, ftp, etc. – it is possible to assort the invalid cases and only use the ones where both shared the same basis. In the ideal case there is an identical key on both sides in the end.

Since in this experiment, polarization encoding is applied, polarization integrity of all applied optical devices, refracting and reflecting, is of big importance. With increasing distortion, QBER becomes higher and therefore, key rate decreases and eventually, no key can be transmitted if QBER exceeds a certain threshold. Thus, special care had to be taken designing the optical systems of Tx and Rx in a way that the polarization integrity could be guaranteed for the experiment.

3. LINK DESIGN

The experiment scenario is basically defined by the capabilities of the Comm and QKD systems applying a wavelength of 1550 nm and 850 nm. For successful key transmission tests, the total ex-aperture path loss had to be minimized to meet the requirements set by Bob's sensitivity. Thus, link distance was rather short to reduce free-space loss and atmospheric extinction in the link budget. On the other hand, a lower bound of slew rate defines the minimal distance to ensure stable tracking. Together, this resulted in a distance of around 20 km. Furthermore, laser safety issues of the airworthiness certification limited the lower flight height to 610 m above ground. Highest operation without oxygen mask is only possible till flight level 100 (~3300 m MSL). Within this height corridor, depending on actual weather conditions, the installed equipment would be operated.

Whereas in classical optical communication systems power losses may be overcome by increased transmit power, typical ex-aperture transmission power of Alice to test secure key exchange is at 0.5 photons per pulse with 10 Mpps. Since impact of scintillation has minimal influence on the system [14], this was not taken into account. Influence of beam wander and broadening was considered, but was found to be negligible in this scenario. However, wave-front distortion, if sufficiently strong, may have an impact and cause diode coupling loss due to spot broadening in the focal plane. Since the flights were conducted after sunset during night time, turbulence was rather weak. The link budget of the Comm system is not outlined here since it is used for sync signal transmission and optical tracking only and it has been proven in earlier experiments to perform well enough even for much longer distances[1]. However, it is important to notice that scintillation can have significant impact on a communication system in this scenario.

To evaluate feasibility of QKD in the air-ground scenario, link budget calculation was performed to estimate the overall mean loss between Alice (ex-aperture of flight terminal) and Bob (entrance aperture of module). The total mean power loss L_{tot} comprises the free-space loss L_{fs}, the atmospheric attenuation L_{atm}, the tracking loss on Tx and Rx side $L_{\mathrm{tr,tx}}$ and $L_{\mathrm{tr,rx}}$, the attenuation due to imperfect optical devices L_{opt}, and the coupling loss of the diode in the focal plane of Bob L_{cp}.

$$L_{\mathrm{tot}} = L_{\mathrm{fs}} \cdot L_{\mathrm{atm}} \cdot L_{\mathrm{tr,tx}} \cdot L_{\mathrm{tr,rx}} \cdot L_{\mathrm{opt}} \cdot L_{\mathrm{cp}} \,. \tag{1}$$

With the specifications from Table 3, the overall loss for the 20 km path is estimated for nominal atmospheric conditions to be 33 dB (Table 2). Assumption of best and worst case conditions predict 30 dB and 63 dB.

Table 2. Mean losses relevant for the QKD system for 20 km distance and 1.4 km flight height above ground. All losses are estimated mean values.

Loss	Free-space L_{fs}	Atm. Att.[2] L_{atm}	Tracking Tx[3] $L_{\mathrm{tr,tx}}$	Tracking Rx[4] $L_{\mathrm{tr,rx}}$	Optics Rx[5] L_{opt}	Coupling Rx[6] L_{cp}	Total L_{tot}
Value [dB]	15	6-9-39	3	1	3	2	30-33-63

[1] Further flight campaigns are ongoing in the framework of the DLR project Vabene. Here, a data transmission with distance of 120 km was demonstrated [15] (press release in German only).
[2] Estimation of atmospheric attenuation was calculated with the tool PFUI (Phyton Fascode User Interface) in DLRs VirtualLab [16]. The atmospheric profile was midlatitude winter, the boundary layer aerosols model set to tropospheric/rural conditions with visibility values of 50, 23 and 5 km for best, nominal and worst case.
[3] Loss due to mean spot broadening.
[4] Maximum loss for the condition that the field of view of Bob is four times larger than tracking std as described in [17].
[5] This comprises all non-ideal surfaces, i.e. non-ideal coating, absorbing and scattering dirt, etc.
[6] Diode coupling loss determined with Hufnagel-Valley profile and a C_n^2 ground value of $1.7\mathrm{x}10^{-14}$ $\mathrm{m}^{-2/3}$.

4. COMMUNICATION TERMINALS

4.1 System overview

The counter terminals hosting Alice and Bob are the flight terminal FELT2 and the ground station OGS-OP. A block diagram of the whole system with indicated QKD integration is shown in Figure 2, on the left the flight terminal, on the right the ground station. The system specs are listed in Table 3. An initial GPS based pointing system enables the ground station's two beacon systems to illuminate the aircraft. The aircraft scans for this signal and aligns its optical path accordingly by application of a two-fold optical closed-loop tracking system. For the coarse tracking, an InGaAs camera (focal plane array) supplies input to the controller driving the torque motors. The fine tracking is realized with a four-quadrant diode and a voice-coil mirror system. For optimization of coupling efficiency, a pointing target shift is implemented in the fine tracking system. Thus, it is possible to fine adjust beam orientation during experiment runtime. On the ground side, the OGS-OP also uses a two-step system, however combining two InGaAs cameras with wide and narrow field of view. These feed the control of the telescope mount and a piezo mirror on the optical bench. What is not shown in this diagram is the UHF system that is run in parallel for transmission of instantaneous aircraft GPS data. Furthermore, this low-rate link is used to transmit azimuth and elevation values of the coarse pointing assembly necessary for the polarization controller ahead of Bob. On transmitter and receiver side, dichroic mirrors are applied for wavelength combination and separation.

Table 3. System specifications of the scenario, the flight terminal and ground station.

Parameter	Value	Remarks
Wavelength downlink Comm	1550 nm	Sync signal 100 MHz (1 W[7])
Wavelength uplink beacon	1590 nm	Beacon signal 2 kHz (2 x 2.5 W[8])
Wavelength downlink QKD	850 nm	Weak pulses 10 MHz (0.5 ph/pulse[9])
Receiver aperture	40 cm	Aperture for Comm and QKD path
Link distance	20 km	Half circle around ground station
Flight height above ground	1100…1300 m	Depending on cloud occurrence
Full beam divergence/diameter Comm (1/e2)	3.0 mrad / 1.7 mm	Setup for QKD experiment
Full beam divergence/diameter QKD (1/e2)	170 µrad / 7.5 mm	
Field of view coarse/ fine tracking sensor FELT2[10]	48 mrad / 3.3 mrad	InGaAs FPA sensor/ 4QD
Tracking accuracy std	< 150 µrad[11]	
Field of view RFE	250 µrad	InGaAs APD; used for sync signal reception
Field of view QKD receiver	83 µrad	Si APD Geiger mode
Field of view coarse/ fine tracking sensor OGS-OP	12.8 mrad / 960 µrad	2 x InGaAs FPA camera
Tracking accuracy OGS-OP std.	~20 µrad	

[7] Maximum mean output power of the EDFA. During experiment runtime, the power was set according to the link distance and atmospheric conditions.
[8] Maximum mean output power of the two fiber lasers. During experiment runtime, the power was set according to the link distance.
[9] Mean photon number per pulse. The pulses were attenuated with calibrated absorption filters.
[10] Smaller size of rectangular sensor is used here. In this paper, all field of views are defined by ray-trace of the chief ray.
[11] The overall tracking accuracy is estimated with data from the coarse tracking system and can therefore only be meant as upper bound.

In the aircraft, Alice comprises a four-path laser diode source polarized according to the BB84 rules with pulse repetition rate of 10 MHz. On ground side, Bob is set up with a polarization controller to compensate for polarization shifts and a four-diode single photon receiver that measures the counts in the respective polarization.

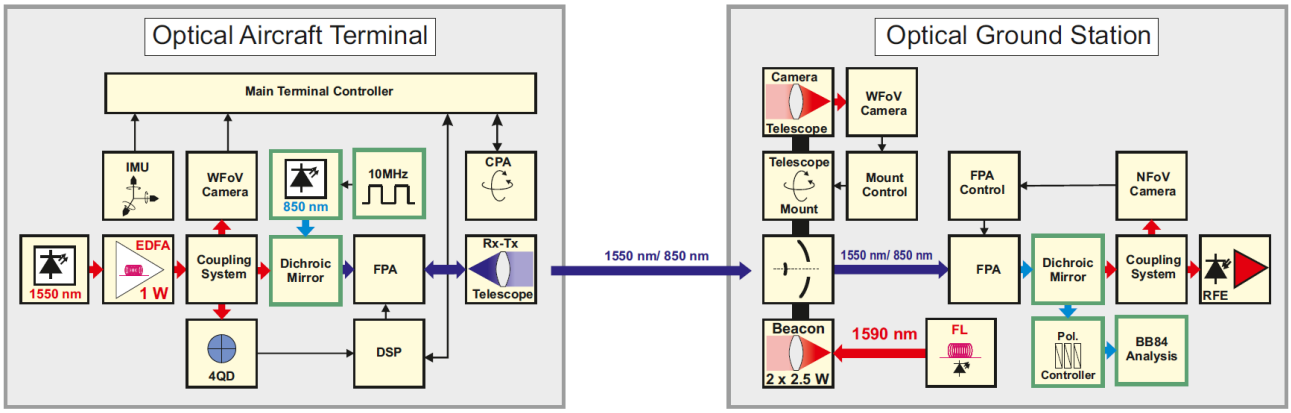

Figure 2. Block diagram of experiment system. At transmitter side, the Comm path and QKD path are co-aligned. The terminal comprises the laser diode with erbium doped fiber amplifier (EDFA), the wide field of view camera (WFoV), the four-quadrant detector (4QD), the main terminal computer and a digital signal processor (DSP), the 850 nm QKD system and the coarse pointing assembly steering the telescope. At receiver side, Comm and QKD beam are separated and guided to the respective receiver systems. It contains two fiber lasers for beacons, a wide field of view camera (WFoV), the mount steering the telescope, the fine-pointing assembly (FPA), its control and narrow field of view camera (NFoV), the receiver front-end (RFE) and the QKD receiver system.

4.2 Flight terminal

The flight platform is the twin engine turboprop aircraft Do228-212 from the DLR aircraft fleet with a service ceiling of 28000 ft (8534 m). The optical bench, hosting all optical, opto-electrical and opto-mechanical parts is mounted to the seat rails inside the cabin (Figure 3, top right).

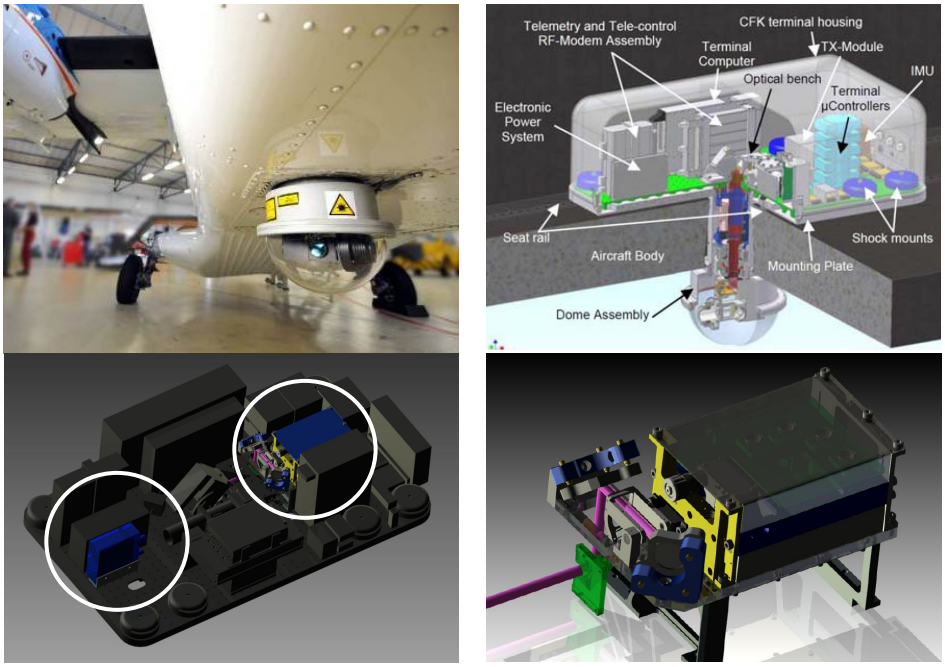

Figure 3. Illustration of flight terminal. The outer part is the coarse pointing assembly protected by a coated glass dome (top left).

The transmitter laser beam is guided via a coudé path through a hole in the fuselage to the coarse pointing assembly which is protected by an optical glass dome (top left). For operations and control, a flight rack with the needed

monitoring and control instrumentation is installed next to the optical bench (not visible). Alice, together with its power supply, is integrated in the remaining free spaces on the optical bench (bottom left). Its output beam (bottom right) is co-aligned to the Rx and Tx path of the terminal.

For the QKD experiment, rather high divergence is chosen for the Comm beam since its link budget for the 20 km link bears high margin. However, for longer distances the divergence would be chosen smaller. In the cockpit, a mission radiation switch was installed to enable the pilots to instantly switch off all laser systems on falling below the defined safety distances which were defined by the airworthiness certification.

4.3 Optical ground station

The ground segment is DLRs Optical Ground Station Oberpfaffenhofen. Figure 4 shows the dome construction, the telescope and the optical bench. A 4 m glass fiber composite dome hosts an azimuth-elevation mount which controls the 40 cm Cassegrain telescope (top left, bottom left). An optical bench is flanged behind the telescope (top right, bottom right). Here, also all optical, opto-mechanical and opto-electrical devices are installed that are necessary for optical tracking, sync signal reception and QKD.

Figure 4. Illustration of ground segment.

Since the Tx and Rx main optical paths of the ground station are not identical, the tracking target as seen from the aircraft differs from the Bob target, which may cause additional coupling loss due to systematic miss-pointing. Thus, the two Tx beacon telescopes are installed symmetrically and in the horizontal plane enclosing the telescopes optical axes to accordingly set the center of gravity of the two beams intensity. The two sources are not resolved by the aircraft tracking sensors and therefore have no influence on tracking performance. Since the QKD receiver is very sensitive to background radiation, the telescope mirror mounts were tubed to suppress this noise source (Figure 4, bottom left).

5. RESULTS OF FLIGHT CAMPAIGN

The flight trials started shortly after daily sunset to minimize noise due to background light of the sun. Furthermore, new moon condition was necessary. Flights later in the night would have been preferable but with one flight lasting between two and three hours, flight times were limited by operation hours of the special airport Oberpfaffenhofen. The procedure after take-off was as follows: a cw transmission of a 850 nm high power beam (1 mW) enabled to conveniently test and optimize coupling efficiency during experiment runtime. Then, crypto mode is used with single photon pulses at 10 MHz. Two successful experiments could be conducted. The first was a test run with mean photon rate of 50 ph/pulse.

The second was the actual experiment testing crypto mode with 0.5 ph/pulse. Here, the sifted key rate was 145 bit/s, the key rate simulating decoy analysis [18] was 4.8 bit/s with QBER of 4.5 % showing the capability of Alice and Bob to exchange a secure key.

An overview of the two flight experiments is given in Table 4. Coupling efficiencies down to 31 dB and 35 dB, were measured at 20 km distance at flight heights of 1100 m to 1300 m above ground. Measurement accuracy is estimated to be at ± 3 dB. Weather conditions were acceptable during both flights since visibility was far better than 5 km during both experiments. Therefore, weather condition on both days can be compared to best and nominal case in Table 2 where total loss is estimated to be between 30 dB and 33 dB. The result is close to the prediction of the link budget but exceeds the calculated values slightly. Causes for this deviation are typical uncertainties in determination of mean Tx/Rx tracking and atmospheric losses. Amongst the two measurements, the 3 dB difference is likely to be caused by lower visibility on the second flight.

Table 4. Overview of the two measurements. System performance on both days was equally good indicating atmospheric extinction being in charge of the higher loss on the second day.

Experiment	Link distance	Flight height	Weather conditions	Total loss	Remarks
Flight 1	20 km	1300 m	Clear sky in southern half circle	31 dB	
Flight 2	20 km	1100 m	High clouds	35 dB	Flight below clouds

Besides the key exchange experiment, scintillation measurements with the sync signal link were run in parallel. First shot analysis of the power vector records resulted in intensity scintillation indices ranging from 0.7 … 1.8 and power scintillation indices from 0.2 … 0.5. However, thorough analysis is still outstanding and will be performed and published later. Although the QKD system is not significantly influenced by scintillation effects, the encrypted payload data stream is affected and therefore, its characterization in this scenario is important.

6. CONCLUSION

In this experiment, we showed the possibility of quantum key distribution with the BB84 protocol in the air-ground scenario exploiting a classical communication link infrastructure. Secure keys could be transmitted with a rate of 4.8 bit/s and with a QBER of 4.5 %. This can already be sufficient for the transmission of keys to be used for the encryption of data that is sent over the classical communication channel, thus allowing secure data transmission at rates of 1 Gbit/s and more. Having in mind the overall goal of global secure communication, this experiment may be seen as a precursor experiment for future operational space based QKD systems. With improved link technology, i.e. lower Tx beam divergence, according tracking systems and bigger Rx aperture, coupling efficiency can be kept in the same order of magnitude (as in our experiment) where the actual QKD receiver proofed to perform sufficiently well.

REFERENCES

[1] Henniger, H. and Giggenbach, D., "Avionic optical links for high data-rate communications," Proceedings of 25th Congress of ICAS (2006).

[2] Horwath, J. and Fuchs, F., "Aircraft to Ground Unidirectional Laser-Comm. Terminal for High Resolution Sensors," Proceedings of SPIE 7199, 719909-1 - 719909-7 (2009).

[3] Michael, S., Walther F. and Parenti, R. R., "Performance evaluation of an air-to-ground optical communications demonstration," Applications of Lasers for Sensing and Free Space Communications (2010).

[4] Stotts, L. B. et al., "Optical communications in atmospheric turbulence," Proceedings of SPIE 7467, 746403-1 - 746403-17 (2009).

[5] ViaLight Communications GmbH, "Laser communication for aerial applications," 12 July 2012, http://www.vialight.de/.

[6] AOptix Technologies, Inc, "AOptix airborne and ground terminals transmit gigabit speeds over long distances," 12 July 2012, http://www.aoptix.com.

[7] Fuchs, C. and Giggenbach, D., "Optical Free-Space Communication on Earth and in Space regarding Quantum Cryptography Aspects," Proceedings of QuantumComm 2009 (2010).

[8] Peev M., et al., “The SECOQC quantum key distribution network in Vienna, “New Journal of Physics 11, 1-37 (2009).
[9] Schmitt-Manderbach, T. et al., "Experimental demonstration of free-space decoy-state key distribution over 144 km," Physical Review Letters 98, 010504-1 - 010504-4 (2007).
[10] ID Quantique SA, “Network encryption,” 12 July 2012, http://www.idquantique.com/.
[11] Bennett, C. H. and Brassard, G., “Quantum cryptographie: Public key distribution and coin tossing,“ Proceedings of International Conference on Computer, Systems & Signal Processing, 175-179, (1984).
[12] Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H., “Quantum cryptography,” Reviews of Modern Physics 74, 145-195 (2002).
[13] Jennewein, T., Simon, C., Weihs, G., Weinfurter, H. and Zeilinger, A., "Quantum cryptography with entangled photons," Physical Review Letters 84 (20), 4729 – 4732 (2000).
[14] Shapiro, J., “Scintillation has minimal impact on far-field Bennet-Brassard 1984 protocol quantum key distribution,” Physical Review A 84 (3), 032340-1-032340-6 (2011).
[15] DLR Institute of Communications and Navigation, DLR Oberpfaffenhofen, “Mit Laserlicht vom Flugzeug aus den Verkehr erfassen,” 12 July 2012, http://www.dlr.de/dlr/desktopdefault.aspx/tabid-10081/151_read-2325/year-all/151_page-4/.
[16] Ernst, T., Rother, T., Schreier, F., Wauer, J. and Balzer, W., “DLR’s VirtualLab: Scientific software just a mouse click away,” Computing in Science & Engineering 5, 70-79 (2003).
[17] David, F., Giggenbach, D., Henniger, H., Horwath, J., Landrock, R. and Perlot, N., “Design considerations for optical inter-HAP links,“ Proceedings of the 22nd ICSSC (2004).
[18] Lo, H. K., Ma, X. and Chen, K., “Decoy state key distribution,” Physical Review Letters 94 (23), 230504-1 - 230504-4 (2002).