Invited Paper

Air to Ground Quantum Key Distribution

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

[a]Fakulät für Physik, Ludwig-Maximilians-Universität, 80799 München
[b]Institut für Kommunikation und Navigation,
Deutsches Zentrum für Luft- und Raumfahrt (DLR), 82234 Weßling
[c]Max-Planck-Institut für Quantenoptik, 80539 München

ABSTRACT

To enable global scale quantum key distribution[1–3] (QKD), satellite based systems[4,5] are the most promising approach. So far, free-space QKD has already been demonstrated on communication channels with attenuation comparable to satellite downlinks,[6] and classical laser communications with satellites and aircrafts is heavily explored.[7–10] Here, combining both these challenges, we demonstrate an aircraft to ground QKD transmission obtaining a sifted key rate of 145 bit/s and a QBER, largely dominated by background events and stray light, of 4.8 %.

Keywords: airborne, free-space, quantum key distribution, QKD

1. INTRODUCTION

While in classical communication the bit values "0" and "1" are used to encode the message, in quantum information qubits are used. They can be formed by in principle every two-level quantum system and additionally allow for a coherent superposition of the quantum states $|\,0\rangle$ and $|\,1\rangle$. For communication applications, photons are most often used to implement the qubits as they can be easily transmitted through the air or via fibers. For free-space transmissions the polarization degree of freedom is the best choice for encoding quantum information.

Exploiting the extra properties of qubits compared to classical bits, Quantum key distribution (QKD)[3] can offer a level of security[11] which can not be reached with any classical methods: The underlying QKD protocols (here we use BB84[1]) base exclusively on quantum mechanical principles. Moreover, the security proofs[12] show that the QKD transmission noise, i.e. the quantum bit error rate (QBER), is a measure for the amount of information an eavesdropper may have gained. This allows for the distillation of a shorter, yet secure key from the transmitted raw data using classical hash functions. This approach is in contrast to classical key distribution schemes where eavesdropping can not be detected or quantified and where the security is only given by the computational complexity of the algorithm used and thus may vanish with future technology.

The distance over which QKD was demonstrated could be increased over the last years successively both in fiber and free-space[6,13,14] and also the combination of several links to trusted node quantum networks was shown.[15,16] Noisy quantum channels and detectors, however, impose upper limits on the operating distance of a QKD system in the range of $150 - 200$ km.[6,13,14] Quantum repeaters[17] could extend these distances, however, they seem to be available rather on a long time scale. For secure key exchange on a global scale QKD transmitters on (trusted) satellites are promising candidates.

Experiments on the channel characteristics of aircraft and satellite downlinks[7,9,10] have already demonstrated successful telescope tracking and classical communication with moving airborne/space systems. In addition, long range free-space QKD and entanglement distribution was shown on a horizontal distance of 144 km between two of the canary islands[6,18–20] coping with attenuation and fluctuations comparable to optical links between satellites and telescopes on the ground. So far, however, all these experiments are restricted to stationary systems. Our

Further author information:
S.N.: E-mail: sebastian.nauerth@lmu.de

Quantum Communications and Quantum Imaging X, edited by Ronald E. Meyers, Yanhua Shih, Keith S. Deacon, Proc. of SPIE Vol. 8518, 85180D · © 2012 SPIE
CCC code: 0277-786/12/$18 · doi: 10.1117/12.929790

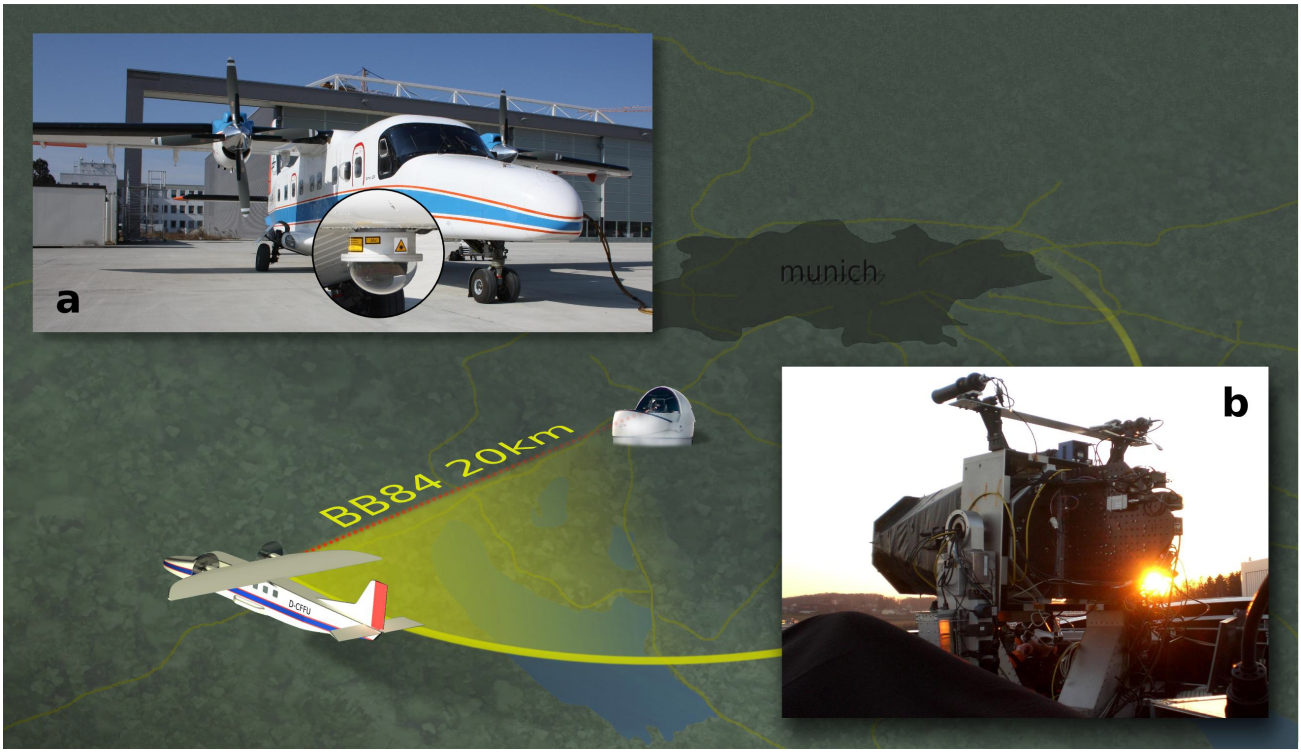

Figure 1. Experiment scenario: **a** The Do228 aircraft equipped with the flight terminal. The inset shows the optical dome underneath the fuselage housing the coarse pointing assembly (CPA). **b**, the optical ground station (OGS) of the German Aerospace Center's institute of communications and navigation. The normally open framework of the telescope was covered here to shield against stray light. All optics is mounted to the breadboard attached to the back of the main mirror.

experiment now for the first time integrates a BB84 system with an airborne platform (fig. 1). Major challenges arise from the integration into an existing communication terminal, from the need for polarization compensation of the optical channel and from the high pointing requirements compared to classical optical communication.

2. EXPERIMENTAL SETUP

In the presented experimental flight campaign the QKD equipment was integrated into the Free-space Experimental Laser Terminal 2 (FELT2) and the optical ground station (OGS) of the German Aerospace Center's (DLR) Institute for Communications and Navigation.[7,8] This system was originally built to provide fast data links for large area imaging and to measure channel behaviour of the aircraft-ground and LEO-ground link.[7] It can provide a stable optical channel with the help of bidirectional beacon lasers (1550 nm/1590 nm) in aircraft to ground scenarios. Additionally, the OGS is also capable of communicating optically with satellites in low earth orbit and thus can operate with sufficiently high angular velocities.

As a qubit has to be a single quantum entity, in contrast to classical optical communications, it is not possible to increase the transmitter power in order to adapt to a particular channel attenuation. Rather, efficient coupling between sender and receiver by small beam divergence and precise pointing has to be ensured. Therefore, both the FELT2 and the OGS were equipped with additional fine pointing assemblies (FPA) each consisting of a fast actuated mirror and a position sensitive sensor in a control loop to enable this experiment.

For the quantum key exchange, a transmitter for polarization encoded, attenuated pulse QKD[21,22] according to the BB84 protocol (Alice module, fig. 2) was designed and integrated into the FELT2. With the help of a photodiode on a servo arm, the Alice module can autonomously calibrate the average QKD pulse intensity to 0.5 photons/pulse to compensate temperature drifts underneath the safety hood covering the terminal during flight. On the ground, the OGS was supplemented with a QKD receiver (Bob module, fig 3) analyzing the

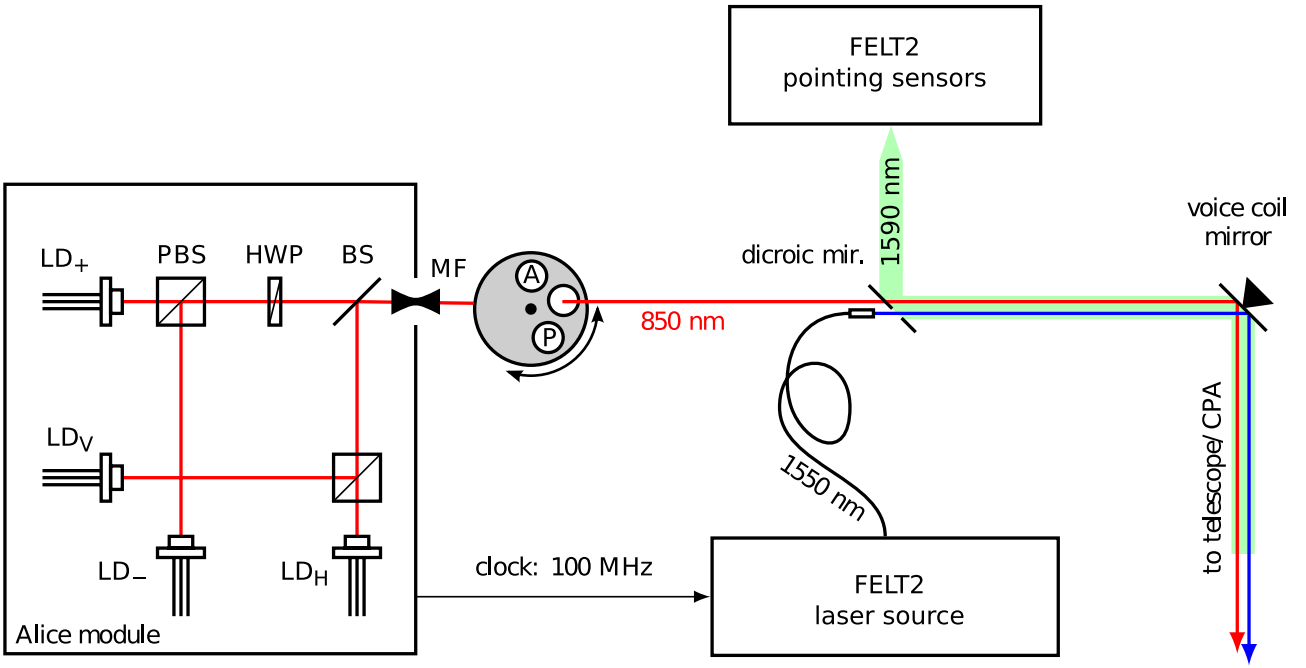

Figure 2. Optical path on the transmitter side: In the Alice module[22] 4 Laserdiodes (LD) generate the BB84 polarization states (H,V,+,-) according to the BB84 protocol. The light is combined with (polarizing) beam splitters (PBS/BS) and a half wave plate (HWP) introduces the rotation between the $\{H, V\}$ and the $\{+, -\}$ basis. A mode filter (MF) selects a common mode of all four diodes. The servo arm can place a photo diode (P) for calibration or an attenuator (A) in the beam. The latter is used for pulse intensities in the single photon regime, here 0.5 photons/pulse. On a dichroic mirror the outgoing Alice beam (850 nm) is overlapped with the incoming beacon from the OGS (1590 nm). The FELT2 beacon (1550 nm), also modulated to transmit the data, is sent through a 4 mm hole in the dichroic mirror to minimize stray light. Note that as Alice is not part of the pointing control loop a precise parallel alignment of the Alice beam and the tracking axis is crucial. A fast voice coil mirror as part of the FPA ensures fine pointing and directs the beams to the coarse pointing assembly (CPA) in the dome underneath the aircraft (see fig: 1a).

incoming qubits in accordance with the BB84 protocol. Upstream to this module, a polarization controller was mounted consisting of three motorized wave plates which allowed to compensate for polarization rotations due to the constantly changing orientation of the aircraft relative to the OGS and thus the FELT2 pointing mirrors. Compensation parameters were obtained from prior measurements of the birefringence for all pointing directions and online pointing information transmitted live from the FELT2 (via uhf-link).

3. FLIGHT CAMPAIGN

The flight campaign took place at the special aircraft Oberpfaffenhofen Germany. The experiment was performed on half circles with a radius of $\approx$ 20 km around the OGS located on a rooftop close to the runway. As the important co-alignment of the QKD beam and the pointing axis could not be stabilized actively, this was readjusted before every flight on a distance of 300 m.

A fine tuning of this alignment in flight was possible by introducing small offsets in the FELT2 control loop. Thereby we were able to increase the coupling for the QKD beam (divergence $\approx$ 180 µrad) without negative impact on the performance of the pointing system as the terminal beacon had a much wider divergence of 3 mrad.

The new FPA provided a stable optical channel for the whole passage with a mean pointing error of the FELT2 of less then 150 µrad. This enabled a continuous quantum transmission for 10 min during which we experienced an overall attenuation of 42.7 dB including also software time filtering of the events with acceptance windows of 500 ps width. At a repetition frequency of 10 MHz we achieved a sifted key rate of 145 bit/s at a QBER of 4.8 %. As over 60 % of the errors occurred due to stray light and dark count events ($\approx$ 4000 s^{-1}), this QBER proves for a precise compensation of the dynamic polarization disturbance inherent to any airborne

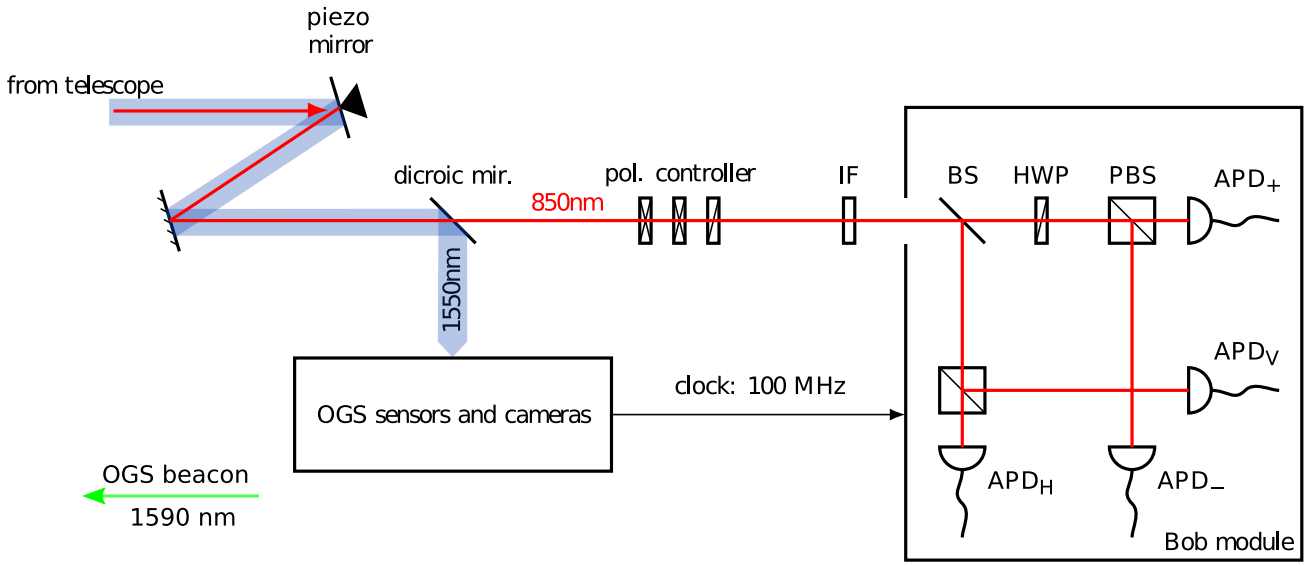

Figure 3. Optical path on the receiver side: The beam coming from the telescope is reflected by a voice coil mirror that is part of the FPA. A dichroic mirror then separates the QKD signal and the FELT2-beacon. The 1550 nm light is analysed to do fine tracking of the airplane and to extract the payload data – in this case a 100 Mhz clock signal – from the FELT-beacon. The 850 nm part of the signal is fed into the polarization controller ($\lambda/4$, $\lambda/4$, $\lambda/2$ waveplates). After an interference filter (FWHM 10 nm) the signal enters the bob module,[21] where a beamsplitter directs the photons to a polarization analysis in either the $\{H, V\}$ or the $\{+, -\}$ bases. HWP: half wave plate, PBS/BS: (polarizing) beam splitter. All detection events are timestamped and -filtered electronically with respect to the clock signal

scenario. While decoy states have yet to be implemented to make the system robust against attacks on the poissonian nature of the Alice pulses, thorough analysis predict a secure key rate of 4.8 bit/s once a so-called vacuum+weak[23] decoy protocol is implemented.

4. RESULTS

In this experiment we successfully integrated QKD technology with an existing system for classical free-space laser communication. Thereby we prove QKD to be a suitable add-on for a variety of communication systems working on a direct line of sight. The fine pointing assemblies developed in this work enabled a stable link for the complete passage of the airplane. Moreover, the constantly changing birefringence introduced by the various moving mirrors and the optical coatings could be compensated precisely. By successfully addressing these challenges, we were able to demonstrate the first BB84 key exchange with an airborne transmitter at high angular velocity. This experiment can thus be regarded as a huge step towards QKD with and between airplanes and satellites enabling world wide, secure key exchange in a trusted node topology.

REFERENCES

[1] Bennett, C. H. and Brassard, G., "Quantum cryptography: Public-key distribution and coin tossing," in [*Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*], 175 (1984).

[2] Bennett, C. H. and Brassard, G., "Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working," *SIGACT News* **20**, 78 (1989).

[3] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H., "Quantum cryptography," *Rev. Mod. Phys.* **74**, 145 (2002).

[4] Buttler, W. T., Hughes, R. J., Kwiat, P. G., Lamoreaux, S. K., Luther, G. G., Morgan, G. L., Nordholt, J. E., Peterson, C. G., and Simmons, C. M., "Practical free-space quantum key distribution over 1 km," *Phys. Rev. Lett.* **81**, 3283 (1998).

[5] Armengol, J. P., Furch, B., Matos, C., Minster, O., Cacciapuoti, L., Pfennigbauer, M., Aspelmeyer, M., Jennewein, T., Schmitt-Manderbach, T., Baister, G., Rarity, J., Leeb, W., Barbieri, C., Weinfurter, H., and et al., A. Z., "Quantum communications at ESA: Towards a space experiment on the ISS," *Acta Astronautica* **63**, 165 (2008).

[6] Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, J. G., Zeilinger, A., and Weinfurter, H., "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.* **98**, 010504 (2007).

[7] Horwath, J. and Fuchs, C., "Aircraft to ground unidirectional laser-communication terminal for high resolution sensors," in [*Free-Space Laser Communication Technologies XXI*], **7199**, SPIE (2009).

[8] Giggenbach, D., Horwath, J., and Markus, K., "Optical data downlinks from earth observation platforms," in [*Free-Space Laser Communication Technologies XXI*], **7199**, SPIE (2009).

[9] Takayama, Y., Toyoshima, M., Shoji, Y., Koyama, Y., Kunimori, H., Sakaue, M., Yamakawa, S., Tashima, Y., and Kura, N., "Expanded laser communications demonstrations with oicets and ground stations," in [*Free-Space Laser Communication Technologies XXII*], **7587**, SPIE (2010).

[10] Perlot, N., Knapek, M., Giggenbach, D., Horwath, J., Brechtelsbauer, M., Takayama, Y., and Jono, T., "Results of the optical downlink experiment kiodo from oicets satellite to optical ground station oberpfaffenhofen (ogs-op)," in [*Free-Space Laser Communication Technologies XIX*], **6457**, SPIE (2007).

[11] Gottesman, D., Lo, H.-K., Lütkenhaus, N., and Preskill, J., "Security of quantum key distribution with imperfect devices," *Quant. Inf. Comput.* **5**, 325 (2004).

[12] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M., "The security of practical quantum key distribution," *Rev. Mod. Phys.* **81**, 1301 (2009).

[13] Hiskett, P. A., Rosenberg, D., Peterson, C. G., Hughes, R. J., Nam, S., Lita, A. E., Miller, A. J., and Nordholt, J. E., "Long-distance quantum key distribution in optical fibre," *New Journal of Physics* **8**, 193 (2006).

[14] Rosenberg, D., Peterson, C. G., Harrington, J. W., Rice, P. R., Dallmann, N., Tyagi, K. T., McCabe, K. P., Nam, S., Baek, B., Hadfield, R. H., Hughes, R. J., and Nordholt, J. E., "Practical long-distance quantum key distribution system using decoy levels," *New Journal of Physics* **11**, 045009 (2009).

[15] Peev, M., Pacher, C., Allaume, R., Barreiro, C., Bouda, J., Boxleitner, W., Debuisschert, T., Diamanti, E., Dianati, M., Dynes, J. F., Fasel, S., Fossier, S., Fürst, M., Gautier, J.-D., Gay, O., Gisin, N., Grangier, P., Happe, A., Hasani, Y., Hentschel, M., Hübel, H., Humer, G., Länger, T., Legr, M., Lieger, R., Lodewyck, J., Lorünser, T., Lütkenhaus, N., Marhold, A., Matyus, T., Maurhart, O., Monat, L., Nauerth, S., Page, J.-B., Poppe, A., Querasser, E., Ribordy, G., Robyr, S., Salvail, L., Sharpe, A. W., Shields, A. J., Stucki, D., Suda, M., Tamas, C., Themel, T., Thew, R. T., Thoma, Y., Treiber, A., Trinkler, P., Tualle-Brouri, R., Vannel, F., Walenta, N., Weier, H., Weinfurter, H., Wimberger, I., Yuan, Z. L., Zbinden, H., and Zeilinger, A., "The secoqc quantum key distribution network in vienna," *New Journal of Physics* **11**, 075001 (2009).

[16] Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., Miki, S., Yamashita, T., Wang, Z., Tanaka, A., Yoshino, K., Nambu, Y., Takahashi, S., Tajima, A., Tomita, A., Domeki, T., Hasegawa, T., Sakai, Y., Kobayashi, H., Asai, T., Shimizu, K., Tokura, T., Tsurumaru, T., Matsui, M., Honjo, T., Tamaki, K., Takesue, H., Tokura, Y., Dynes, J. F., Dixon, A. R., Sharpe, A. W., Yuan, Z. L., Shields, A. J., Uchikoga, S., Legré, M., Robyr, S., Trinkler, P., Monat, L., Page, J.-B., Ribordy, G., Poppe, A., Allacher, A., Maurhart, O., Länger, T., Peev, M., and Zeilinger, A., "Field test of quantum key distribution in the tokyo qkd network," *Opt. Express* **19**, 10387 (2011).

[17] Briegel, H.-J., Dür, W., Cirac, J. I., and Zoller, P., "Quantum repeaters: The role of imperfect local operations in quantum communication," *Phys. Rev. Lett.* **81**, 5932 (1998).

[18] Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H., Scheidl, T., Lindenthal, M., Blauensteiner, B., Jennewein, T., Perdigues, J., Trojek, P., Omer, B., Furst, M., Meyenburg, M., Rarity, J., Sodnik, Z., Barbieri, C., Weinfurter, H., and Zeilinger, A., "Entanglement-based quantum communication over 144[thinsp]km," *Nat Phys* **3**, 481 (2007).

[19] Scheidl, T., Ursin, R., Fedrizzi, A., Ramelow, S., Ma, X.-S., Herbst, T., Prevedel, R., Ratschbacher, L., Kofler, J., Jennewein, T., and Zeilinger, A., "Feasibility of 300 km quantum key distribution with entangled states," *New Journal of Physics* **11**, 085002 (2009).

[20] Fedrizzi, A., Ursin, R., Herbst, T., Nespoli, M., Prevedel, R., Scheidl, T., Tiefenbacher, F., Jennewein, T., and Zeilinger, A., "High-fidelity transmission of entanglement over a high-loss free-space channel," *Nat Phys* **5**, 389 (2009).

[21] Weier, H., Schmitt-Manderbach, T., Regner, N., Kurtsiefer, C., and Weinfurter, H., "Free space quantum key distribution: Towards a real life application," *Fortschritte der Physik* **54**, 840 (2006).

[22] Nauerth, S., Fürst, M., Schmitt-Manderbach, T., Weier, H., and Weinfurter, H., "Information leakage via side channels in freespace bb84 quantum cryptography," *New Journal of Physics* **11**, 065001 (2009).

[23] Ma, X., Qi, B., Zhao, Y., and Lo, H.-K., "Practical decoy state for quantum key distribution," *Physical Review A* **72**, 012326 (2005).