Spatial Mode Side Channels in Free-Space QKD Implementations

Markus Rau, Tobias Vogl, Giacomo Corrielli, Gwenaelle Vest, Lukas Fuchs, Sebastian Nauerth, and Harald Weinfurter

(Invited Paper)

***Abstract*—The quantum key distribution protocol uses one degree of freedom of a single quantum system to encode information. If this information has correlations with the system's other degrees of freedom, or if the measurement efficiencies on the receiver side depend on them, a security loophole called side channel is created. An eavesdropper can exploit it to gain information without disturbing the system, and thus, without revealing the attack. Here, we analyze side channels in a free-space QKD sender and receiver implementation and focus especially on the dependencies and side channels for the spatial degree of freedom.**

***Index Terms*—Cryptographic protocols, quantum key distribution (QKD), optical transmitters, optical receivers.**

I. Introduction

Quantum key distribution (QKD) [1] is a provably secure protocol for growing a shared secret key between two parties by exchanging quantum systems. Any eavesdropping attempt will disturb the quantum states, which then can be detected. By measuring these disturbances, one can calculate the maximum information an eavesdropper might have obtained [2], which consequently can be removed by shrinking the key in a privacy amplification step [3].

However, real QKD devices typically do not have an ideal quantum system, which satisfies the requirements of theoretical QKD protocols available. For example, in the BB84 protocol [4], the phase or polarization of photons is used to encode the qubit. However, photons also have additional degrees of freedom, like wavelength and time–position. This can cause a so-called side channel if the qubit degree of freedom becomes correlated to the others [5]. If, for example, photons with different polarization are emitted at different wavelengths, an eavesdropper could gain full information by measuring only the wavelength while leaving the polarization degree of freedom undisturbed. Since QKD relies on such disturbances to reveal eavesdropping attempts, this could completely break the security of the QKD implementation.

Side channels are also a threat on the receiver side: if the detection efficiencies depend on the timing of the photons [6], [7], an eavesdropper might manipulate light propagation such that only one detector can register the photons. If the detection time is later publicly revealed during the protocol, the measurement result is known to the eavesdropper, without having caused a disturbance in the qubit degree of freedom. Other side channels might arise from disturbances due to daylight operation [8], [9].

The E91 QKD protocol [10], [11] is not affected by such side channels as the integrity of the source and quantum channel is verified during the protocol by a Bell test. However, the protocol is vulnerable to flaws in the receiver setups, where sensitive single-photon detectors are required. An eavesdropper can exploit the behavior of the detectors' electronic circuitry to fake a violation of Bell's inequality [12] in an E91 implementation or hide any disturbances caused by him [13]–[15] in BB84 systems.

Imperfections in the sender or receiver implementation are no security risk in device independent QKD protocols [16], however they require very high detection efficiencies and so far no experimental demonstration has been achieved.

Here, we analyze side channels in setups for sending and receiving QKD signals over a free-space link, where compared to fiber links, an additional degree of freedom is relevant: The photon's spatial mode.

II. QKD Sender Setup and Security

The security of a free-space QKD sender setup used for links over 500 m as well as for the record long inter-island link over 144 km [17] was analyzed previously [18]. This sender, which was designed for the BB84 [4] and decoy state protocols [19], employed eight separate laser diodes to generate four polarization states at two different intensity levels. Compared to using a single laser diode and electro-optical modulators to set polarization and intensity, this might create a side channel if the pulses from the different laser diodes can be distinguished by their spectral or temporal characteristics.

Manuscript received August 14, 2014; revised October 15, 2014; accepted October 31, 2014. This work was supported by the EU projects CHIST-ERA/QUASAR, FP7/QWAD, and FP7/CIPRIS (MC ITN-287252).

M. Rau, T. Vogl, and L. Fuchs are with the Faculty of Physics, Ludwig-Maximilian-Universität, 80799 München, Germany (e-mail: markus.rau@physik.lmu.de; Tobias.Vogl@physik.uni-muenchen.de; Lukas.Fuchs@physik.uni-muenchen.de).

G. Corrielli is with the Istituto di Fotonica e Nanotecnologie, Consiglio Nazionale delle Ricerche (IFN-CNR), 20133 Milano, Italy (e-mail: giacomo.corrielli@polimi.it).

G. Vest is with the qutools GmbH, 81371 München, Germany and also with the Faculty of Physics, Ludwig-Maximilian-Universität 80799, München, Germany (e-mail: gwenaelle.vest@lmu.de).

S. Nauerth is with qutools GmbH, 81371 München, Germany (e-mail: sebastian.nauerth@qutools.com).

H. Weinfurter is with the Max-Planck-Institut für Quantenoptik, 85748 Garching, Germany and also with the Faculty of Physics, Ludwig-Maximilian-Universität, 80799 München, Germany (e-mail: h.w@lmu.de).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSTQE.2014.2372008

The effect of such source imperfections is analyzed in [5] and even a simple example shows how critical they can be in systems with high channel attenuation: If, e.g., the transmission is lower than 1% (20 dB attenuation) and if only 1% of the sent pulses can be projected to distinct modes in other degrees of freedom correlated with the polarization, an eavesdropper could gain full information.

In the system analyzed, here, the spectral overlap of the emitted pulses was controlled by selecting laser diodes with well matched spectra and by using a narrow interference filter at the output [18], [20]. The temporal shape of the pulses and their timing relative to the system's clock was determined by the driving electronics. By using finely adjustable delay elements in the circuit of each laser diode, the temporal pulse shape can be set and brought to near perfect overlap.

While spectral and temporal distinguishability are also a concern in fiber based systems, a free-space system must also consider the spatial mode of the emitted pulses. The output modes of the laser diodes are elliptically shaped and oriented along the polarization axis. Thus, spatial filtering was required to make them overlap well, which was achieved by a short piece of single mode fiber. While it requires quite some effort to efficiently couple eight diodes into one fiber, fortunately not much efficiency was necessary for the setup. Since the bright laser pulses had to be attenuated to the single photon level at the output, most of this attenuation could happen in a relatively simple coupling scheme. One drawback of this filtering solution was the fiber's birefringence. It strongly changed with temperature and rotated the prepared polarization states. Measurements showed that a $20\,^{\circ}\mathrm{C}$ temperature change would cause a $10\,\%$ quantum bit error ratio in one basis [20]. Thus, an active temperature stabilization of the fiber was necessary, resulting in a bulky setup, which was not suitable for integration in smaller devices.

More recently, a new method for overlapping the spatial modes of several laser diodes was designed [21], which utilizes a waveguide circuit in a glass substrate manufactured by femtosecond laser pulses [22], [23]. This circuit consists of three non-polarizing beamsplitters, which overlap the pulses of four laser diodes into a single spatial mode. By mounting a laser diode array closely to the glass chip, the optical part of a QKD sender system can be miniaturized to a degree, where it is suitable for integration even in handheld devices, but also offers now significantly more compact and robust add-ons for long distance QKD systems compared to previous systems [17], [18], [24].

III. QKD Receiver Setup and Security

Similar to the sender side, where emitted photons must not be distinguishable by a degree of freedom other than their polarization, the detection efficiencies on the receiver side must be distinguished only by the polarization of the light signals.

Since any practical free-space QKD system will use a narrow spectral filter on the receiver side to suppress stray light, one can assume that the detection efficiency is practically constant for all wavelengths that pass the filter. A dependence on the temporal domain is mainly an issue for systems that use gated detectors. This was already exploited to demonstrate an attack on a real QKD system [7], but potential counter measures have been found since then [25].

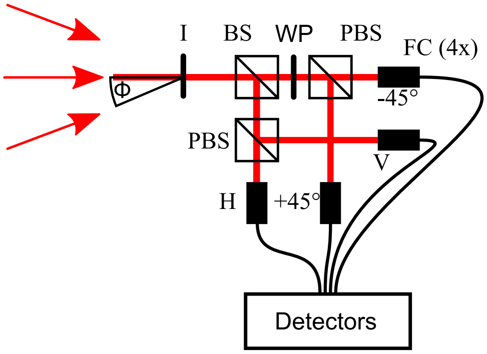

Fig. 1. Schematic of the receiver module. It uses a non polarizing beamsplitter (BS), a half wave plate (WP), two polarizing beamsplitters (PBS), and four fiber couplers (FC). The horizontal angle ϕ and vertical angle θ (not shown) of the input beam at the first iris (I) was varied for analyzing the detection efficiency mismatch.

Any efficiency mismatch can be employed by an eavesdropper, and thus, can be related to an information leakage reducing the key rate. Yet, it was shown that even with a mismatch of the detection efficiencies a secure key can be generated [26]. For the secure key rate R_X (R_Z) in the X-basis (Z-basis) follows[1]

$$\begin{aligned} R_X &\geq -h(E_X) + \eta_X(1 - h(E_Z/\eta_X)) \\ R_Z &\geq -h(E_Z) + \eta_Z(1 - h(E_X/\eta_Z)) \end{aligned} \quad (1)$$

where $h(x)$ is the entropy function [27], E_X (E_Z) is the qubit error ratio in the X-basis (Z-basis), and η_X (η_Z) is the detection efficiency mismatch in the X-basis (Z-basis). It is defined as

$$\begin{aligned} \eta_X &= \min_t \min \left\{ \frac{\eta_{X0}(t)}{\eta_{X1}(t)}, \frac{\eta_{X1}(t)}{\eta_{X0}(t)} \right\} \\ \eta_Z &= \min_t \min \left\{ \frac{\eta_{Z0}(t)}{\eta_{Z1}(t)}, \frac{\eta_{Z1}(t)}{\eta_{Z0}(t)} \right\} \end{aligned} \quad (2)$$

where $\eta_{X0}(t)$, $(\eta_{Z0}(t))$, and $\eta_{X1}(t)$ $(\eta_{Z1}(t))$ are the detection efficiencies of the two detectors in the X-basis (Z-basis) depending on all possible degrees of freedom subsumed in the parameter t.

In the following, we want to focus on detection efficiency mismatch for the spatial degree of freedom, by characterizing a QKD receiver module used in a previous single photon QKD experiment [28].

A. Setup

The receiver module used four detectors to measure in the linear polarizations H/V and ±45° (see Fig. 1). Incoming photons first passed a non-polarizing 50:50 beamsplitter, which was used to randomly choose the measurement basis. Photons reflected at this first beamsplitter were analyzed in the H-V-basis via a polarizing beamsplitter. Photons not reflected were

[1] For simplicity, we assume a single photon source and equal detection rates in both bases. We refer to [26] for the general case.

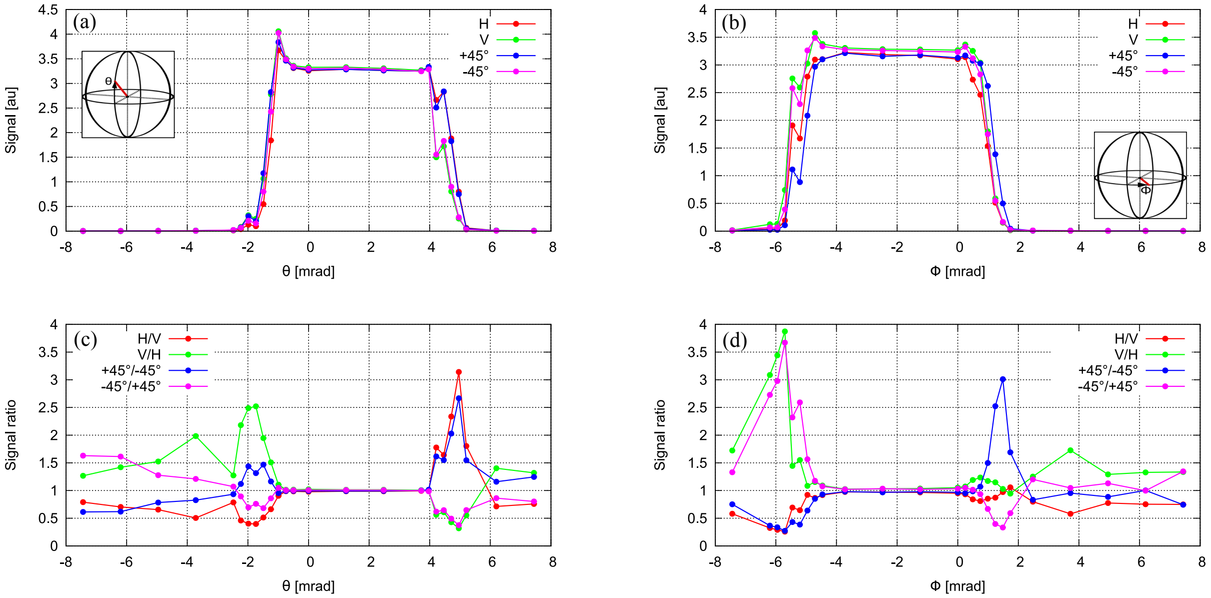

Fig. 2. (a), (b) Detector signals for different angles θ and ϕ in the vertical respectively horizontal axis of the incident beam. (c), (d) Ratio of the signals in each basis. (Measurement errors are less than dot size.)

measured in the $\pm 45^\circ$-basis by a combination of a half wave plate oriented at 22.5° and a polarizing beamsplitter. In this way, the light was split into four separate beams (one for each polarization), which were then coupled into multi-mode fibers (core diameter $= 65\,\mu$m, NA $= 0.275$).

To guarantee stability the receiver module was built on a milled aluminum block with fixed holders for the three beamsplitters. The four fiber couplers were mounted in adjustable mirror holders which offered two angular degrees of freedom for alignment. Due to the construction, the optical path length to two fiber couplers (V, $+45^\circ$ output) was 32 mm longer than to the other two. As discussed previously [29], this path difference can cause an efficiency mismatch: an incoming beam with a large angle might completely miss the detector, which is further away, but still partially hit the closer detector.

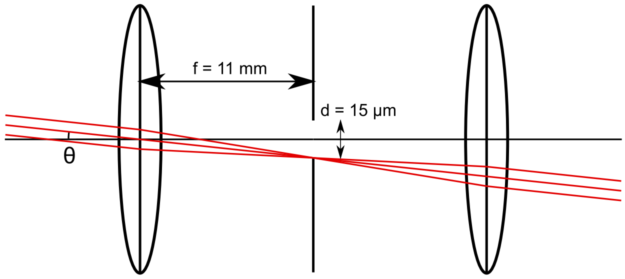

Fig. 3. Schematic of the spatial filter used to restrict the incoming beam's angle.

B. Initial Measurement

To analyze the dependence of the detection efficiency on the direction of the incoming mode, a collimated laser beam ($\phi = 1\,$mm, $\lambda = 850\,$nm) with circular polarization was used. Ideally, all four detectors should register the same intensity, independent of the angle of the input beam. Fig. 2 shows the detected intensities for varying vertical and horizontal angles (θ and ϕ, respectively) of the input beam. While all four channels showed the same detection efficiency over a range of $\approx 2\,$mrad [see Fig. 2(a) and (b)], there were large differences in the detection efficiencies at the border of this range, which is clearly seen in the ratios of the efficiencies in both bases [see Fig. 2(c) and (d)].

The smallest ratio of $\approx 1/4$ was found at an angle of $\phi = -6\,$mrad on the horizontal axis. According to (2), it determines the system's detection efficiency mismatch $\eta_Z \simeq \eta_X \simeq 1/4$. Using this value in (1), a secure key could only be generated for a qubit error ratio of $E \leq 2\,\%$.[2] This was clearly not sufficient and spatial filtering was required.

C. Spatial Filtering

Implementing a spatial filter as shown in Fig. 3 restricted the angle of the input beam to 2 mrad. Analysis of the coupling to the four detectors then showed a much better match of the detection efficiencies (see Fig. 4). However, some differences remained resulting in a detection efficiency mismatch of $\eta_X = 0.84$ and $\eta_Z = 0.73$. From (1), it follows that a secure key can be obtained for a qubit error ratio of up to 8.7%, which is now much easier achievable. However, already at a moderate error ratio of 3%, the secure key rate is reduced by 26% compared to the case with no detection efficiency mismatch ($\eta_X = \eta_Z = 1$).

It is expected that the remaining detection efficiency mismatch can be further reduced by matching the optical path lengths in the receiver module and with a better alignment of the four fiber couplers onto the optical axis. In the current design,

[2] A graph of the maximum error ratio for a given η is shown in [26].

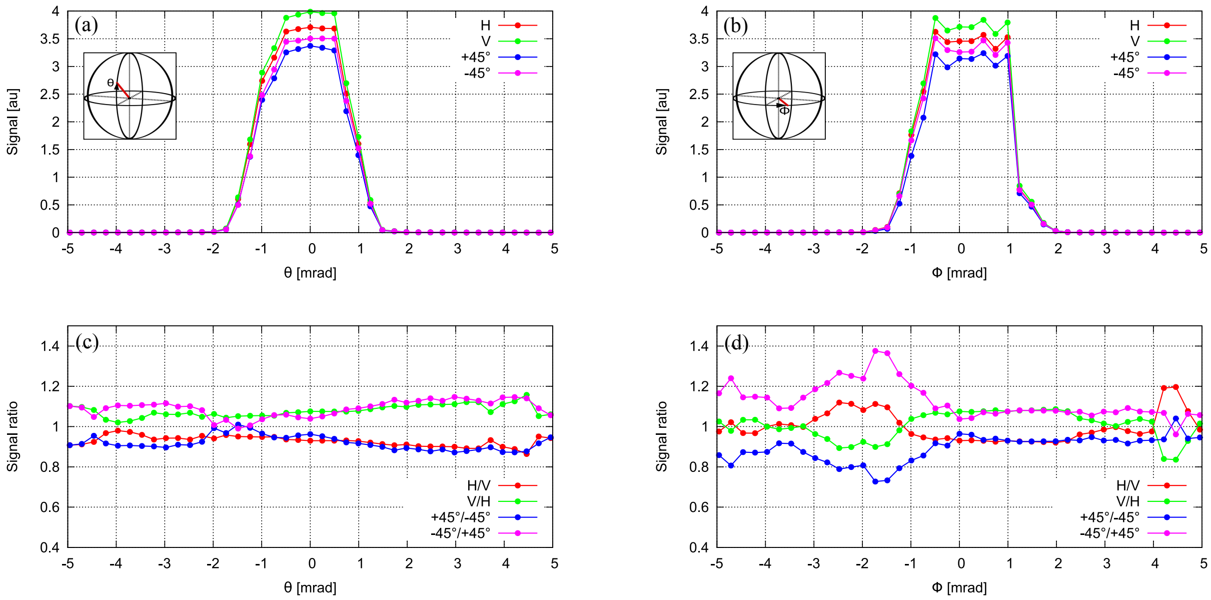

Fig. 4. (a), (b) Detector signals for different angles θ and ϕ in the vertical respectively horizontal axis of the incident beam after implementing a spatial filter. (c), (d) Ratio of the signals in each basis.

this was not perfectly possible since the beamsplitters were mounted in a fixed position, and the fiber couplers were mounted in mirror holders which only offered two degrees of freedom.

IV. Outlook

These measurements showed a dependency of the detection efficiency on the angle of the incoming beam in two axes. Yet, an eavesdropper is not restricted to simply changing this angle, but could shape the beam into an arbitrary spatial phase and intensity distribution.

Then, there might be, e.g., two separate spatial modes, which experience a different phase shift in the receiver. Depending on the mode coupled to the detectors, destructive interference in the fiber couplers can reduce the corresponding channels measurement efficiency to zero. This would allow an eavesdropper to perform an undetectable intercept and resend attack similar to [14].

A possible solution would be a true single mode filter at the input. Due to atmospheric disturbances during a free-space transmission, it is of course very challenging to couple the received light into a single mode, but this can be overcome using adaptive optics [30]. Alternatively, but equally challenging, the detection efficiencies have to be matched for all spatial modes coupled to the detectors.

The advantage an eavesdropper gains from an detection efficiency mismatch can also be removed by randomly assigning each detector to a bit value for every received light pulse [26]. However, this requires an active phase modulator in the receiver setup, making it vulnerable to trojan-horse attacks [31] that read out the modulator setting.

Another way to avoid security problems due to receiver side channels and detector vulnerabilities is the recently developed measurement device independent QKD protocol [32], where both parties only have setups for sending photons, and the receiver setup can be under the full control of an untrusted third party. While this protocol was already demonstrated in fiber based systems [33], a free-space implementation would be challenging, since the photons from both senders have to be overlapped on a beamsplitter in all degrees of freedom. Matching two spatial modes after a free-space transmission is as challenging as single mode filtering.

V. Conclusion

Compared to fiber based systems, a security analysis of a free-space QKD system has to take the light beam's spatial degree of freedom into account. If it correlates with the sent polarization or influences the detection efficiencies, a side channel is created, which compromises a systems security. On the sender side, spatial indistinguishability can be ensured for multi-laser diode sources by single mode filtering at the output [18]. For a multi-detector receiver, spatial filtering helps to reduce the detection efficiency mismatch for varying input beam directions as shown here.

Yet, for security against even more powerful attacks, an advanced receiver design has to reduce any detection efficiency mismatch in order to avoid any additional filtering and the associated losses. This will enable future free-space applications with high link attenuation like global links via QKD to satellites [34], [35] or flying platforms [24].

References

[1] V. Scarani *et al.*, "The security of practical quantum key distribution," *Rev. Modern Phys.*, vol. 81, no. 3, pp. 1301–1350, 2009.

[2] M. Tomamichel and R. Renner, "Uncertainty relation for smooth entropies," *Phys. Rev. Lett.*, vol. 106, no. 11, pp. 110506-1–110506-4, 2011.

[3] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover hashing against quantum side information," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5524–5535, Aug. 2011.

[4] C. H. Bennett *et al.*, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.* New York, NY, USA, 1984, vol. 175.

[5] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Inform. Comput.*, vol. 4, no. 5, pp. 325–360, 2004.

[6] A. Lamas-Linares and C. Kurtsiefer, "Breaking a quantum key distribution system through a timing side channel," *Opt. Exp.*, vol. 15, no. 15, pp. 9388–9393, 2007.

[7] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A*, vol. 78, no. 4, pp. 042333-1–042333-5, 2008.

[8] M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer, "Daylight operation of a free space, entanglement-based quantum key distribution system," *New J. Phys.*, vol. 11, no. 4, pp. 045007-1–045007-13, 2009.

[9] M. P. Peloso and I. Gerhardt, "Statistical tests of randomness on quantum keys distributed through a free-space channel coupled to daylight noise," *J. Lightw. Technol.*, vol. 31, no. 23, pp. 3794–3805, Dec. 2013.

[10] A. K. Ekert, "Quantum cryptography based on Bells theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, 1991.

[11] A. Ling *et al.*, "Experimental quantum key distribution based on a bell test," *Phys. Rev. A*, vol. 78, no. 2, pp. 020301-1–020301-4, 2008.

[12] I. Gerhardt *et al.*, "Experimentally faking the violation of bells inequalities," *Phys. Rev. Lett.*, vol. 107, no. 17, pp. 170404-1–170404-25, 2011.

[13] L. Lydersen *et al.*, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature photon.*, vol. 4, no. 10, pp. 686–689, 2010.

[14] I. Gerhardt *et al.*, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," *Nature Commun.*, vol. 2, pp. 349-1–349-6, 2011.

[15] H. Weier *et al.*, "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," *New J. Phys.*, vol. 13, no. 7, pp. 073024-1–073024-10, 2011.

[16] A. Acín *et al.*, "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 98, no. 23, pp. 230501-1–230501-4, 2007.

[17] T. Schmitt-Manderbach *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, no. 1, pp. 010504-1–010504-2, 2007.

[18] S. Nauerth *et al.*, "Information leakage via side channels in freespace BB84 quantum cryptography," *New J. Phys.*, vol. 11, no. 6, pp. 065001-1–065001-8, 2009.

[19] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, no. 1, pp. 012326-1–012326-15, 2005.

[20] S. Nauerth, "Freiraumoptische quantenkryptographie," Diploma thesis, Ludwig-Maximilians-Universität Munich, Munich, Germany, 2007.

[21] G. Vest *et al.*, "Design and evaluation of a handheld quantum key distribution sender module," *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 3, pp. 1–7, May 2015.

[22] K. M. Davis, K. Miura, N. Sugimoto, and K. Hirao, "Writing waveguides in glass with a femtosecond laser," *Opt. Lett.*, vol. 21, no. 21, pp. 1729–1731, 1996.

[23] G. Della Valle, R. Osellame, and P. Laporta, "Micromachining of photonic devices by femtosecond laser pulses," *J. Opt. A, Pure Appl. Opt.*, vol. 11, no. 1, pp. 013001-1–013001-18, 2009.

[24] S. Nauerth *et al.*, "Air-to-ground quantum communication," *Nature Photon.*, vol. 7, no. 5, pp. 382–386, 2013.

[25] L. Lydersen, V. Makarov, and J. Skaar, "Secure gated detection scheme for quantum cryptography," *Phys. Rev. A*, vol. 83, no. 3, pp. 032306-1–032306-7, 2011.

[26] L. Lydersen and J. Skaar, "Security of quantum key distribution with bit and basis dependent detector flaws," *Quantum Inf. Comput.*, vol. 10, no. 1/2, pp. 0060–0076, 2010.

[27] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Modern Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

[28] T. Heindel *et al.*, "Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range," *New J. Phys.*, vol. 14, no. 8, pp. 083001-1–083001-12, 2012.

[29] C.-h. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, "Security proof of quantum key distribution with detection efficiency mismatch," *Quantum Inf. Comput.*, vol. 9, no. 1, pp. 131–165, 2009.

[30] H. Takenaka, M. Toyoshima, and Y. Takayama, "Experimental verification of fiber-coupling efficiency for satellite-to-ground atmospheric laser downlinks," *Opt. Exp.*, vol. 20, no. 14, pp. 15-301–15-308, 2012.

[31] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Phys. Rev. A*, vol. 73, no. 2, pp. 022320-1–022320-6, 2006.

[32] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, pp. 130503-1–130503-5, 2012.

[33] Y. Liu *et al.*, "Experimental measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 111, no. 13, pp. 130502-1–130502-5, 2013.

[34] R. Hughes *et al.*, "Secure communications with low-orbit spacecraft using quantum cryptography," US Patent 5 966 224, 1999.

[35] J.-Y. Wang *et al.*, "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," *Nature Photon.*, vol. 7, no. 5, pp. 387–393, 2013.

Markus Rau received the Graduate degree in physics from the Ludwig-Maximilians-Universität, Munich, Germany, in 2008. He is currently working toward the Ph.D. degree in the group of H. Weinfurter. His research interests include QKD with single photon sources and the security of QKD systems.

Tobias Vogl received the B.Sc. degree in physics from the Ludwig-Maximilians-Universität, Munich, Germany, in 2014, where he is currently working toward the M.Sc. degree and his research interests include quantum information.

Giacomo Corrielli was born in 1986. He received the Graduate degree in physics engineering from Politecnico of Milano, Milano, Italy, in 2011 with a thesis concerning the frequency conversion of single photons for quantum repeater applications developed at ICFO, Barcelona, Spain. He is currently working toward the Ph.D. degree at Politecnico of Milano and his research interests include the fabrication of integrated optical circuits for quantum optics and quantum information application.

Gwenaelle Vest received the Graduate degree in materials engineering from the National Institute of Applied Sciences of Lyon (INSA Lyon), France, in 2011 and in nanotechnologies from the Université de Lyon, France the same year.

She is currently with qutools GmbH, Munich, Germany. Concurrently, she is working toward the Ph.D. degree in physics at the Ludwig-Maximilians-Universität, Munich, on high-speed, handheld quantum key distribution modules.

Lukas Fuchs received the B.Sc. degree in physics at the Ludwig-Maximilians-Universität, Munich, Germany, in 2012. He is currently working toward the M.Sc. degree at the same university and his thesis focuses on integrated quantum key distribution modules.

Sebastian Nauerth received the Ph.D. degree in physics at the Ludwig-Maximilians-Universität, Munich, Germany in 2013 for his work on air-to-ground quantum key distribution. He is now with qutools GmbH, Munich.

Harald Weinfurter studied at the Technical University of Vienna, Wien, Austria, and was a Postdoctoral Fellow at the Hahn-Meitner Institut, Berlin, Germany, and the RISØ-Laboratory, Roskilde, Denmark. After working on foundations of quantum physics and quantum information at the University of Innsbruck, Austria, he became a member of the Faculty of Physics, University of Munich, Munich, Germany. He is currently also a Fellow at the Max-Planck-Institute of Quantum Optics, Garching, Germany. His current research interests include experiments on studying and applying entanglement, e.g., in various demonstrations of quantum communication protocols, in free-space quantum cryptography over record distances of 144 km, or in atom–atom entanglement.