Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km

Tobias Schmitt-Manderbach,[1,2,*] Henning Weier,[2] Martin Fürst,[2] Rupert Ursin,[3] Felix Tiefenbacher,[4,3] Thomas Scheidl,[4,3] Josep Perdigues,[5] Zoran Sodnik,[5] Christian Kurtsiefer,[6] John G. Rarity,[7] Anton Zeilinger,[4,3] and Harald Weinfurter[1,2]

[1]*Max-Planck-Institute for Quantum Optics, D-85748 Garching, Germany*
[2]*Department of Physics, Ludwig-Maximilians-University, D-80799 Munich, Germany*
[3]*Institute for Experimental Physics, University of Vienna, A-1090 Vienna, Austria*
[4]*Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, A-1090 Vienna, Austria*
[5]*European Space Agency, NL-2200 AG Noordwijk, The Netherlands*
[6]*Department of Physics, National University of Singapore, Singapore 117542, Singapore*
[7]*Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1UB, United Kingdom*

(Received 23 August 2006; published 5 January 2007)

We report on the experimental implementation of a Bennett-Brassard 1984 (BB84) protocol type quantum key distribution over a 144 km free-space link using weak coherent laser pulses. Optimization of the link transmission was achieved with bidirectional active telescope tracking, and the security was ensured by employing decoy-state analysis. This enabled us to distribute a secure key at a rate of 12.8 bit/s at an attenuation of about 35 dB. Utilizing a simple transmitter setup and an optical ground station capable of tracking a spacecraft in low earth orbit, this outdoor experiment demonstrates the feasibility of global key distribution via satellites.

DOI: 10.1103/PhysRevLett.98.010504 PACS numbers: 03.67.Dd, 03.67.Hk, 42.50.−p

Quantum cryptography [or quantum key distribution (QKD)] [1] was the first application of the evolving field of quantum information technology to become commercially available. The maximum distance for QKD in practical applications, however, is currently limited by the noise of available single photon detectors and the absorption along the quantum channel, for example, in fiber to about 100 km [2]. In principle, this problem can be overcome by subdividing a larger distance into smaller segments and employing a quantum repeater scheme. Yet, this is still far beyond state-of-the-art technology. In the meantime, a network of trusted nodes connected by fiber or short free-space links is one option for bridging longer distances [3]. Alternatively, a free-space link from a low-earth-orbit (LEO) satellite to a ground station could be used [4,5]. By exchanging quantum keys between the satellite and different ground stations consecutively, one can easily establish a secret key between any two ground stations worldwide, thereby enabling truly global quantum key distribution.

QKD traces its security back to the fact that it is impossible to determine the general quantum state of a single photon [6]. Yet, compared to using sources of single [7] or entangled photons [5,8] it is technologically much simpler for the transmitter to generate attenuated laser pulses. Even for a low average photon number well below one (typically $\mu_S \approx 0.1$), the Poissonian nature of the laser photon statistics opens back doors for attacks by a potential eavesdropper. In the most powerful one, the photon number splitting (PNS) attack, the eavesdropper removes a photon from all pulses containing two or more photons and measures its state after bases are announced. In high loss situations, he obtains the full key. To avoid such leakage one has to strongly attenuate the laser pulses [9], approximately proportional to the link efficiency. The significantly lower key rate makes attenuated pulse QKD very unattractive or even impossible (Fig. 1). The recently proposed decoy-state analysis enables one to detect such attacks [10]. There, the mean photon number for secure commu-

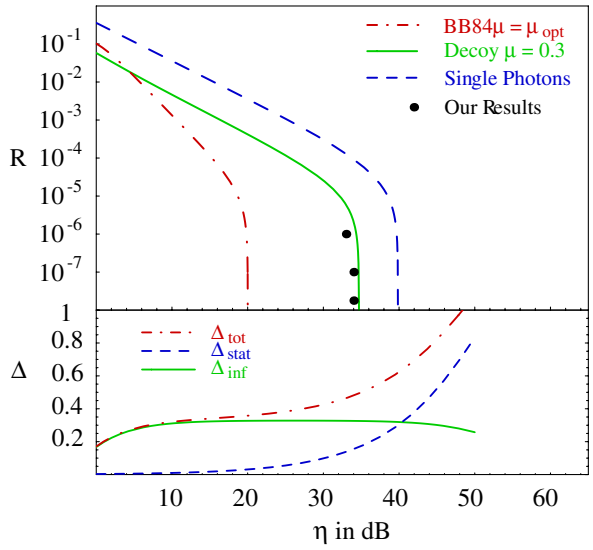

FIG. 1 (color online). The key generation rate for the BB84 protocol, the decoy-state protocol, and ideal single photon sources depending on the transmission of the quantum channel. For the parameters achieved in the experiment secure communication is not possible with the BB84 protocol at attenuations of more than 20 dB. For the comparison with the ideal single photon source, we assumed a photon rate equal to $\mu = 0.3$. The lower graph shows the dependence of the percentage of tagged pulses depending on the attenuation. One clearly sees that for a wide region Δ_{tot} is roughly constant and thus enables a performance similar to the single photon case, before it again increases due to poor statistics in the decoy-state analysis.

nication becomes approximately independent of the link loss and the key rate scales equally to the single photon case.

Here we report on successful quantum key distribution over a real distance of 144 km. This link between the Canary islands of La Palma and Tenerife has a path length through atmosphere much longer than from LEO satellites to a ground station and serves as a realistic test bed for future quantum communication to space [11]. We developed bidirectional tracking of the telescopes [5] for continuous optimization of the link efficiency reaching a transmission as high as -30 dB. Because of stray light and dark counts, secure communication over such a distance would not be possible anymore with the Bennett-Brassard 1984 (BB84) protocol. We demonstrate how decoy-state analysis enables one to ensure the secrecy of the key.

The Poissonian photon statistics of attenuated laser pulses makes eavesdropping possible. Multiphoton pulses emitted by the transmitter will contribute to the key, but potentially could have been attacked by an eavesdropper. If Δ is the fraction of such so-called tagged photons, the lower bound for the secure key rate is [12]

$$R = \frac{p}{2}\{(1-\Delta)(1-\Gamma) - f[\mathrm{QBER}]H(\mathrm{QBER})\}. \quad (1)$$

The factor p is the probability for Bob detecting a signal pulse and QBER (quantum bit error ratio) is the ratio between false bits and all bits of the sifted key. $H(\mathrm{QBER})$ is the binary entropy function, and $f(\mathrm{QBER})$ is the bidirectional error correction rate. The value $\Gamma = \log_2(1 + 4\epsilon - 4\epsilon^2)$, with $\epsilon = \frac{\mathrm{QBER}}{1-\Delta}$, is the fraction of bits, which has to be discarded during privacy amplification to ensure that an eavesdropper has less than 1 bit of information of the final key [13].

The simplest attack for an eavesdropper is the beam-splitting attack, where he can access all photons not detected by the receiver. However, the information gained by such an attack, and thus also the fraction Δ, saturate for higher loss, which makes such an attack not very effective. On the contrary, for the PNS attack Δ can reach 1.

The decoy-state method now enables one to determine an upper bound for Δ directly from the data taken in the key generation process. For that purpose, several different values μ_i for the mean photon number are used at random when sending the attenuated pulses. Coherent states with mean photon numbers less than one are not orthogonal to each other, and thus not distinguishable for the eavesdropper. Thus, without knowing the particular attenuation, the photon number subtraction done in the PNS attack cannot be adopted to the respective value. This leads to detectable changes in the photon statistics, which finally reveal the attack.

In our experiment, in addition to the signal pulses with mean attenuation μ_S, the transmitter also emits decoy pulses with a mean photon number of $\mu_d > \mu_S$, and "pulses" with no light at all, $\mu_0 = 0$ [14]. By finally evaluating the detection probabilities Q_i (at the receiver's detectors) corresponding to pulses with mean photon numbers μ_i ($i \in \{0, S, d\}$), one can calculate an upper bound for the fraction of tagged bits:

$$\Delta \le \Delta_{\mathrm{inf}} = \frac{\mu_S}{\mu_d - \mu_S}\left(\frac{\mu_S e^{-\mu_S} Q_d}{\mu_d e^{-\mu_d} Q_S} - 1\right) + \frac{\mu_S e^{-\mu_S} Q_0}{\mu_d Q_S}. \quad (2)$$

Δ_{inf} will have a minimum value, which already accounts for the beam-splitting attack or other attacks, which do not change the Poissonian photon statistics and thus cannot be discriminated from losses. For all other attacks, Δ_{inf} will increase according to the amount of information that could have been gathered by the adversary.

In the experiment (Fig. 2) the optics of the QKD transmitter (Alice) consisted of four laser diodes, whose orientation was rotated by 45° relative to the neighboring ones. At a clock rate of $R_0 = 10$ MHz one of them emitted a 2 ns optical pulse centered at 850 nm with a full width at half maximum (FWHM) of 1.5 nm, according to random bit values, that were generated beforehand by a physical random number generator and stored on Alice's hard disk. The output beams of all diodes were overlapped by a concave-convex pair of conical mirrors and coupled into a single mode optical fiber running to the transmitter telescope. Decoy pulses at higher μ_d were randomly interspersed in the signal sequence by firing two randomly chosen diodes simultaneously [15]. For the empty decoy pulses, the electrical pulse driving the laser diode was suppressed. The mean photon number for all decoy states was monitored with a calibrated single photon detector at one of the output ports of a 50:50 fiber beam splitter before coupling to the telescope. Single photon polarization analysis was performed inside the transmitter telescope to correct changes along the fiber.

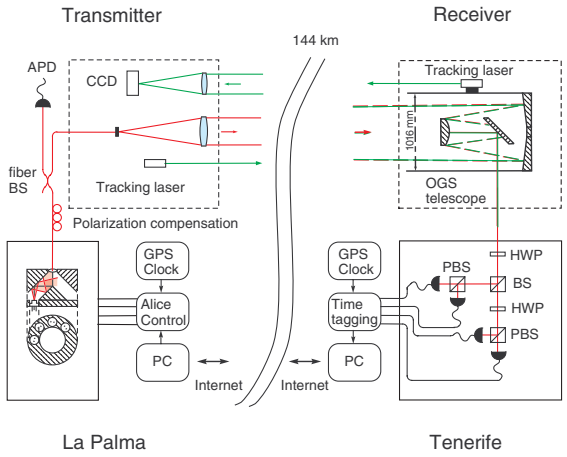

FIG. 2 (color online). Schematics of the experimental setup on the two canary islands. BS, beam splitter; PBS, polarizing beam splitter; HWP, half-wave plate; APD, avalanche photo diode.

The Alice unit was located at a platform next to the Nordic Optical Telescope at the Observatorio Roque de los Muchachos on the island of La Palma. The transmitter telescope was mounted on a heavy workbench outside a portakabin where Alice's optics and control electronics were placed. In the telescope the light emitted from the bare fiber was collimated by a 150 mm diameter $f/2.7$ achromat and sent over 144 km optical path at a mean altitude of ~2400 m to the Optical Ground Station (OGS) of the European Space Agency (ESA) on Tenerife [16].

The OGS is a 1 m Ritchey-Chrétien telescope with the Coudé focus and an effective focal length of 39 m and a field of view of 8 arcmin. We employed active tracking techniques for both the transmitter and the receiver telescope, in order to assure optimal coupling in the presence of slowly varying atmospheric influences [5]. Fast beam wander and beam spreading due to diffraction and scattering of the atmosphere resulted in an effective beam diameter between 4 and 20 m at the OGS, depending on weather conditions. In the diffraction limited case in vacuum, the transmitter telescope would have produced a beam of 1.5 m in diameter.

The light collected by the primary mirror of the OGS was directed to an optical bench inside the telescope building. With an adjustable iris in the Coudé focus, the effective field of view could be reduced to minimize stray light detection. After polarization adjustment via a half wave plate to undo rotations along the optical path of the receiver station, the beam was detected by a single photon polarization analyzer setup, enabling analysis either along H/V or $\pm 45°$ depending on whether the photon was detected in the reflected or transmitted output behind the beam splitter, respectively. Each analysis path contained a 40 mm focusing lens and an interference filter (center wavelength 850 nm, 10 nm FWHM) attached to a passively quenched silicon avalanche photodiode module. The detectors' electrical output pulses were fed into a timestamp unit [clocked by signals derived from the global positioning system (GPS)], determining the detection time and which of the detectors had clicked for each photoevent. These data were then transferred via a digital input/output card to a personal computer (PC) for further processing.

For the sifting process, each photoevent had to be assigned an absolute pulse number in order to allow Alice and Bob to discuss their respective choice of basis. This was accomplished without any reference channel but solely by means of the dim pulses. After basic synchronization of the PCs' system clocks with a standard network time protocol we applied a fast-Fourier-transform algorithm to the raw event timings to obtain an initial value for the basic pulse repetition rate of the transmitter with respect to the receiver clock. Since both clock signals were derived from GPS signals, local drifts were smaller than 10^{-11} over 100 s. A software phase-locked-loop compensated for any slow residual drifts. Each photoevent was accepted if it was detected within a time window Δt around the expected arrival time or rejected as background, otherwise. Finally, pseudorandom bit sequences in the photon stream (1.2% of the attenuated pulses) enabled Bob to find the absolute offset of the pulse number.

All events falling into the detection time window Δt were buffered in the PC memory until full synchronization was achieved. From that point on, basis reconciliation was performed for all data on-the-fly over the classical channel (10 Mbit/s Ethernet). After that, both Alice and Bob held a binary key of the same length, possibly with errors due to experimental imperfections or the presence of an eavesdropper. Because of strong fluctuations of the link efficiency and frequent fades of the quantum signal, the errors were not evenly distributed within the sifted key but accumulated in certain blocks. We discarded all blocks where the header was already corrupted by more than a factor of 1.1 during the synchronization process. We applied the classical two-way error correction algorithm CASCADE [17] to remove any errors, and privacy amplification to limit the maximum information of the perfect eavesdropper.

Under good atmospheric conditions we observed an optical link efficiency of -28 dB, measured between the transmitter and the OGS Coudé focus. From this we assume approximately -10 dB to be due to atmospheric losses, and roughly -14 dB due to beam spreading to spot sizes greater than the aperture of the telescope. Optical components in the OGS together with the output lens in the transmitter telescope accounted for -4 dB attenuation. Finally, our detector system (including the polarization optics and interference filters) had an efficiency ~25% equivalent to a further -6 dB of loss. Background resulted from dark counts (~1000/s) and stray light from nearly full moon (for a field of view reduced to $\sim 15''$ between 400 and 1000/s). After numerical optimization for these data we set the mean photon numbers of the transmitter for signal and decoy states to $\mu_S = 0.27$ and $\mu_d = 0.39$, respectively. The probabilities of signal, decoy, and vacuum pulses were chosen to be 87%, 9%, and 4%, respectively. Under these conditions, about ~1000 photoevents per second were due to the attenuated pulses sent by the transmitter.

The cumulative effects of timing jitter of the Alice electronics, reference clock noise, timing jitter of the photodetectors, and noise in the timestamp unit led to a temporal distribution of signal events with a FWHM of 4 ns. For raw key generation, we accepted photoevents within a time window $\Delta t = 5.9$ ns, leading to a QBER = 6.48% for the entire measurement run. We attribute ~3% to spurious events within Δt, ~3% to alignment errors of the Alice module including compensation in the single mode fiber, and finally, another 0.5% to imperfections in the polarization analyzer.

For a typical measurement of 17 min we obtained 799 000 detection events, and thereof $n_{\mathrm{sif}} = 218$ kbit of

sifted key. During error correction a total number of 63 kbit were disclosed. The limited statistics caused uncertainty for the relevant security parameters QBER and Δ_{inf}, which in turn resulted in a higher uncertainty for the security of the final key. To reduce this uncertainty, we substitute these parameters in (1) and (2) by QBER $\rightarrow$ QBER $+ \delta_{\text{QBER}}$ and $\Delta_{\text{inf}} \rightarrow \Delta_{\text{inf}} + \Delta_{\text{stat}}$ with δ_{QBER} depending on n_{sif} and the probability for the eavesdropper to have 1 bit of Shannon information of the final key. If we limit this probability to as low as 10^{-5}, we obtain, using the Hoeffding inequality as in [13] and Gaussian error propagation, respectively, $\delta_{\text{QBER}} = 0.5\%$ and $\Delta_{\text{stat}} = 0.16$. We then obtained a secure key of 12.5 kbit, corresponding to an average secure key rate of 12.8 bit/s, in good agreement with theory (Fig. 1).

Under the same conditions, the original BB84 protocol would not yield any secure key. If we assume that the eavesdropper does not exploit multiphoton pulses, we can use the unmodified BB84 protocol. In a second experiment employing this scheme, we obtained 94.6 kbit of secure key within 20 min of measurement time corresponding to a 28 bit/s final key rate. The QBER was in this case 6.77%. This value also gives the limit of what is achievable with an ideal single photon source emitting on average the same number of photons as our source.

The experiment presented here exceeds the previous distance record for free-space QKD by almost 1 order of magnitude. This was possible only by applying the recently developed decoy-state protocols in order to exclude the disastrous photon number splitting attack possible for attenuated light pulses. This technologically much simpler method thus again is competitive with single photon QKD. When comparing it with a related experiment over the same link [5], we see that the reduction of the key at this time is stronger by a factor of 3 to 7, depending on link efficiency. Close to the edge of secure QKD this results in significantly reduced key rates; however, there is room for improvements. First, new electronics for the pulse generation should allow one to produce decoy pulses with single diodes as well. Second, in tests such electronics already enabled gate times of about 2 ns, thus reducing background influence. Alignment errors should be reduced when employing bright instead of attenuated pulses. By reducing the QBER this way, a clear increase in the key rate should be feasible. And, finally, an upgrade to faster electronics will increase the key rate accordingly.

The current outdoor experiment definitely shows the feasibility of secure key exchange with low-earth-orbit satellites. It achieved a distance comparable with fiber-on-a-coil laboratory demonstrations, and most importantly, the design of our experiment laid the foundation for the next steps. The receiver optics is already integrated into an existing ground station for optical communication with satellites and the compactness and simplicity of our faint pulse transmitter unit provides a good starting point for future integration into optical terminals as developed for satellite communications. Pointing, acquisition, and tracking techniques required to establish and maintain a LEO-to-ground optical link are well established. Thus satellite-based QKD is feasible—with almost state-of-the-art technology—at reasonable secret key rates.

This work was supported by ESA under the General Studies Programme (QIPS study, ESA Contract No. 18805/04/NL/HE), the Austrian Science Foundation (SFB1520), the Bavarian High-Tech Initiative, the EU projects SECOQC and QAP, and the ASAP programme of the Austrian Space Agency (FFG). The authors wish to thank the staffs of the Instituto de Astrofísica de Canarias, the Nordic Optical Telescope, and the OGS for their support at the trial sites, and QinetiQ for providing the random number generator.

Note added.—A new Alice module now enabled, for 10 MHz pulse rate, a secure key rate of 42 bit/s.

*Electronic address: tschmitt@lmu.de

[1] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002).
[2] D. Stucki *et al.*, New J. Phys. **4**, 41 (2002); E. Waks, A. Zeevi, and Y. Yamamoto, Phys. Rev. A **65**, 052310 (2002).
[3] EU project SECOQC: http://www.secoqc.net.
[4] C. Kurtsiefer *et al.*, Nature (London) **419**, 450 (2002); R. J. Hughes *et al.*, New J. Phys. **4**, 43 (2002); H. Weier *et al.*, Fortschr. Phys. **54**, 840 (2006).
[5] R. Ursin *et al.*, quant-ph/0607182.
[6] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
[7] E. Waks *et al.*, Nature (London) **420**, 762 (2002); A. Beveratos *et al.*, Phys. Rev. Lett. **89**, 187901 (2002).
[8] A. Poppe *et al.*, Opt. Express **12**, 3865 (2004); K. J. Resch *et al.*, Opt. Express **13**, 202 (2005); I. Marcikic *et al.*, Appl. Phys. Lett. **89**, 101122 (2006).
[9] N. Luetkenhaus, Phys. Rev. A **61**, 052304 (2000).
[10] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005); Y. Zhao *et al.*, Phys. Rev. Lett. **96**, 070502 (2006); C.-Z. Peng *et al.*, Phys. Rev. Lett. **98**, 010505 (2007); D. Rosenberg *et al.*, Phys. Rev. Lett. **98**, 010503 (2007).
[11] M. Pfennigbauer *et al.*, J. Opt. Networking **4**, 549 (2005).
[12] D. Gottesman, H.-K. Lo, N. Luetkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[13] N. Luetkenhaus, Phys. Rev. A **59**, 3301 (1999).
[14] These instances serve to determine the background from dark counts and stray light from the original data.
[15] J. Harrington, J. Ettinger, R. Hughes, and J. Nordholt, quant-ph/0503002.
[16] R. Czichy, Z. Sodnik, and B. Furch, Proc. SPIE Int. Soc. Opt. Eng. **2381**, 26 (1995).
[17] G. Brassard and L. Salvail, Lect. Notes Comput. Sci. **765**, 410 (1994).