Free-Space Optical Quantum Key Distribution Using Intersatellite Links

Martin Pfennigbauer, Walter R. Leeb
Institut für Nachrichtentechnik und Hochfrequenztechnik, Technische Universität Wien,
Gusshausstrasse 25/389, A-1040 Wien, Austria
Tel.: +43-1-58801-38901, Fax.: +43-1-58801-38999, martin.pfennigbauer@ieee.org

Markus Aspelmeyer, Thomas Jennewein, Anton Zeilinger
Institut für Experimentalphysik, Universität Wien,
Boltzmanngasse 5, A-1090 Wien, Austria
Tel.: +43-1-4277-51201, Fax.: +43-1-4277-9512

Abstract

Communication schemes employing quantum entanglement open a wide field of possible applications with properties outperforming their classical counterparts. Promising examples are quantum key distribution, quantum dense coding, and quantum state teleportation. We investigate the potential of quantum cryptography, i.e. quantum key distribution (QKD), with special emphasis on the demands and opportunities provided by intersatellite links.

I. Introduction

QUANTUM communication describes a novel branch of communication protocols such as quantum dense coding [1], quantum teleportation [2] or quantum cryptography [3], [4]. These schemes utilize the principles of quantum physics to achieve communication tasks much more powerful than their classical counterparts. Within the last years the technology needed for quantum communication has been rapidly maturing, both for applications in fiber-based and in free-space systems. Specifically, quantum key distribution (QKD) is about to become a readily available technology for cryptography [5]–[13]. With QKD, ultimately secure keys can be distributed, where the privacy does not depend on, e.g., computational power, but is given by the laws of nature.

Following the results of a recently finished ESA study [14], we analyze an important scenario for sharing secure keys between a communication satellite and a ground station, namely the employment of a second satellite carrying a source for entangled photons. Using both an optical intersatellite link and an optical downlink to distribute the entangled photon pairs between the communicating parties a cryptographic link between the communications satellite and the ground station can then be established via classical optical or RF channels. It is an important feature of this concept that the quantum source cannot obtain any information of the generated key. While recent proposals mainly focussed on the space-to-ground link [15], [16], we now investigate the intersatellite aspect of the scenario.

The paper is organized as follows: In Sect. II, we present a brief introduction to the principles of quantum cryptography. The state of the art in quantum communication is outlined in Sect. III. In Sect. IV, the properties of classical and quantum optical communication are compared. Next, we summarize possible free-space scenarios and the experiments that could be performed. An assessment of the technological requirements for the feasibility of intersatellite links will be presented in Sect. VI. Employing today's technology, the maximum affordable link attenuation to successfully establish these protocols is some 60 dB. Calculations on the expected link attenuation for different space scenarios show that quantum communication links even including GEO satellites are within reach. In Sect. VII we investigate specifically the possibility of distributing a secure key between a satellite and a ground station by using an intersatellite link and a space-to-ground link.

II. Principles of entanglement based quantum cryptography

Cryptography relies on the sharing of secret keys between communicating parties, typically named Alice and Bob. One of the major loopholes in classical cryptography is that, in principle, it is always possible to intercept

the distribution of the cryptographic key unnoticedly. Quantum key distribution (QKD) [3], [4], [17], also generally called quantum cryptography, can cover this defect, since it allows Alice and Bob to share completely secure keys by transmitting single quanta (qubits) along a quantum channel. The underlying principle of QKD is that nature prohibits to gain information on the state of a quantum system without disturbing it due to the no-cloning theorem [18]. Therefore, in appropriately designed protocols, no tapping of the qubits is possible without deceiving itself to Alice and Bob.

The working principle of entanglement based quantum cryptography is as follows: both Alice and Bob receive one particle out of an entangled pair, say a pair of polarization-entangled photons [6]. They perform polarization measurements along at least three different directions on each side, where measurements along parallel axes are used for key generation and oblique angles are used for testing a Bell inequality [19]. Since eavesdropping inevitably affects the entanglement between the two constituents of a pair it detectably reduces the degree of violation of Bell's inequality. In contrast to single qubit schemes, e.g. based on faint-laser pulses, entanglement based quantum cryptography does not require security of the source location, which is an intrinsic benefit from a practical point of view.

III. Current status

The first experimental demonstration of QKD was achieved in 1989 by Bennett and Bessette [20], a QKD scheme based on entangled photons was realized for the first time by Jennewein *et al.* [6]. Up to date, many different protocols have been implemented with an ongoing trend towards larger distances and smaller hardware [5], [7], [21]. However, photon absorption limits the bridgeable distance for single photons to the order of 100 km both in present silica fibers [21], [22] and in earth-based free-space links [11]. Recent quantum cryptography experiments already achieve such distances [23], [24]. Still, in order to establish quantum cryptography networks over large distances or even on a global scale, it is essential to distribute single photons or entangled photons over these distances. Optical free-space links could provide a unique solution to this problem since they allow in principle for much larger propagation distances of photons due to the low absorption of the atmosphere in certain wavelength ranges. Free-space optical links have been studied and successfully implemented already for several years for their application in quantum cryptography based on faint classical laser pulses [10], [25], [26]. To fully exploit the benefits of entanglement-based QKD it is necessary to share not only single photons but entangled photons over such distances. Recently some of us succeeded in demonstrating a crucial step, namely the distribution of quantum entanglement via a free-space link, which was verified by violating a Bell inequality between two distant receivers without a direct line of sight between them [27]. In this experiment, the setup for the source generating the entangled photon pairs has been miniaturized to fit on a small optical breadboard and it could easily be operated completely independent from an ideal laboratory environment.

In the long run, to fully exploit the advantages of free-space links, it will be necessary to use space and satellite technology. By transmitting and/or receiving either photons or entangled photon pairs to and/or from a satellite, entanglement can be distributed over truly large distances and thus would allow quantum cryptography on a global scale.

We have already discussed in detail the scenario, where a space based source is used to distribute entanglement between two communicating ground stations [16]. We will now continue this analysis by using the same source to provide shared entanglement between a ground station and a satellite that is capable of manipulating and detecting single photons. In that way, *one* satellite-based entangled photon source can be utilized to allow quantum communication not only between arbitrary ground stations but also between a ground station and an arbitrary satellite or even between two satellites.

IV. Comparison between quantum communications and classical optical communications

Table I summarizes the main conceptual differences and communalities of quantum and classical optical communications. The performance may be characterized by speed, capacity, security, technology, and complexity. As a sidenote, we want to point out a common source of misconception, namely that quantum physics does permit communication at superluminal speeds. Although the non-local features of quantum entanglement would suggest this, the principal limit for communication is still the speed of light!

TABLE I

COMPARISON BETWEEN QUANTUM COMMUNICATIONS AND CLASSICAL OPTICAL COMMUNICATIONS

	classical theory	**quantum theory**	**common properties**	**differences**
speed			speed of light, delays in electronics	
capacity				increased capacity via quantum dense coding
security	low beam divergence makes eavesdropping more difficult than for radio frequency	perfect single photon sources allow perfect security		security is based on the laws of nature (quantum cryptography)
complexity	reasonable, there are already classical systems in orbit	fast progress keeps complexity at a reasonably low level		
technology	transceivers are state-of-the-art	rapidly evolving standard technologies	pointing, acquisition and tracking is close to state-of-the-art	there exist no optical amplifiers for quantum information (no-cloning-theorem)

V. SCENARIOS OF SPACE EXPERIMENTS

Before we study the specific case which uses a space-based source for entangled photons, let us briefly review the alternative scenarios of entanglement-assisted quantum communication experiments in space. We may distinguish the cases in which the transmitter of entangled photons is located on ground or aboard a satellite. These scenarios will all lead to different performance and will thus permit different applications.

A. Earth-based transmitter terminal

The scenarios involving an Earth-based transmitter terminal allow to share quantum entanglement between ground and satellite or between two satellites and thus to communicate between such terminals employing quantum communication protocols. In the most simple case, a straight uplink to one satellite-based receiver (see Fig. 1 a) can be used to perform secure quantum key distribution between the transmitter and the receiver. Here, one of the photons of the entangled pair is being detected right at the transmitter site and thus the entangled photon source is used as a triggered source for single photons. Shared entanglement between two parties can be achieved by directing each of the photons of an entangled pair either towards another Earth-based station and a satellite or towards two separate satellites (see Figs. 1 b). Possible applications for shared entanglement between two parties are quantum key distribution or entanglement-enhanced communication protocols [26].

B. Space-based transmitter terminal

A transmitter with an entangled photon source placed on a space-based platform not only allows longer link distances because of reduced influence of atmospheric turbulence (see Sect. VI) but also leads to more flexible scenarios. Again, already a simple downlink allows to establish a single-photon link, e.g. for quantum cryptography (see Fig. 1 c). In this configuration, a key exchange between two ground stations is also possible. To this end each of the two ground stations has to establish a separate quantum key with the satellite. Since the space terminal has access to both keys, it can transmit a logical combination of the keys which can then be used by either ground station or both ground stations such that they arrive at the same key. This logical combination can easily be chosen such that it does not reveal any information about the key. Note that the key is not generated simultaneously at both receiver stations. In principle, a quantum key exchange can be performed between arbitrarily located ground stations at different times. However, as already mentioned above, this scheme imposes the same high security constraints onto the source as is required for the laboratories of the two parties. The use of entangled states sent simultaneously to two separate ground stations (Fig. 1 d) or satellites (Fig. 1 e) or a ground station and a satellite (Fig. 1 f) allows instantaneous key exchange between these two communicating parties and guarantees that the transmitter has no information about the shared key. Therefore, no security requirement has to be imposed onto the source; in principle, the source could even be in the hands of a potential eavesdropper.

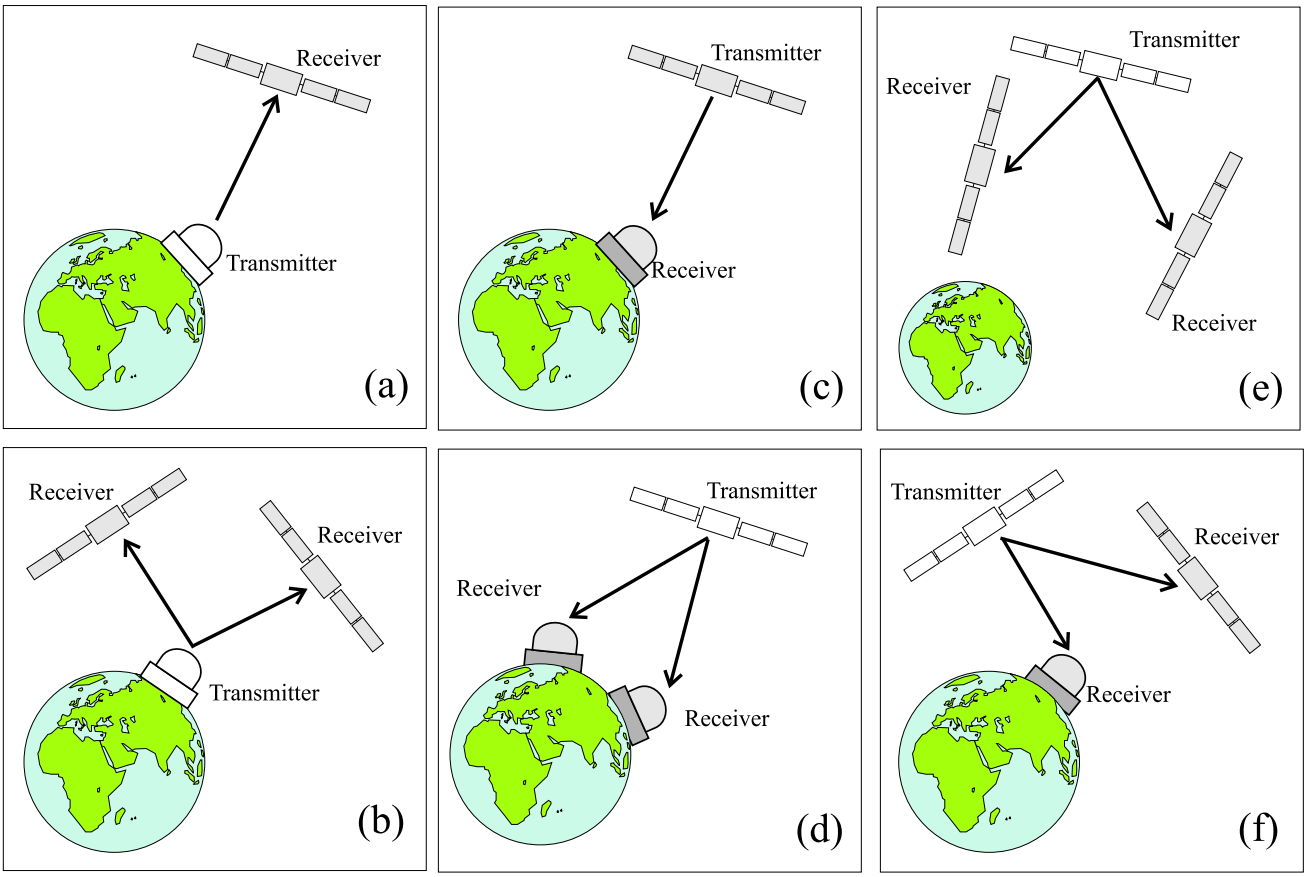

Fig. 1. Scenarios for quantum communication with Earth-based transmitter terminals (a, b) and space-based transmitter terminals (c–f).

VI. Link properties

A. Link budget

In the following, we will assess the affordable link attenuation to establish a QKD protocol based on entangled photons. It is determined by the timing resolution and the dark count rates of the detectors employed, as well as by the net production rate of the source.

The accidental coincidence rate is given by

$$C_{acc} = B_1 B_2 \Delta\tau, \tag{1}$$

where B_1, B_2 are the dark count rates of the two detectors and $\Delta\tau$ is the timing resolution for the electronic registration of a two-fold coincidence event. As the minimum signal-to-noise ratio we assume that necessary for the violation of a Bell inequality [28]. For the case of polarization entangled photons this necessitates a two-fold coincidence visibility of at least 71%, corresponding to a signal-to-noise ratio (SNR) of $6:1$. Below that ratio a local realistic modeling of the observed correlations is possible thus allowing unobserved eavesdropping[1]. Therefore, to discriminate the signal from the background coincidences, the minimal observed coincidence rate $C_{s,min}$ must be at least six times larger than C_{acc}.

The coincidence detection rate C_s is determined by the total coincidence efficiency η_{link}, which is the product of the individual efficiencies for the two qubit links,

$$\eta_{link} = \eta_{link1}\eta_{link2} \quad . \tag{2}$$

[1]Note, that phase-coded entanglement results in slightly higher requirements to show that Bell's inequality can be violated without any loophole [29].

The rate of detected signal coincidences, C_s, is given by the product

$$C_s = R\eta_{link}\eta_{det1}\eta_{det2} \quad , \tag{3}$$

where R is the pair production rate of the source and η_{det1}, η_{det2} are the detection probabilities. In order to achieve a violation of Bell's inequality, the signal coincidences must exceed the limit $C_{s,min} = SNR \cdot C_{acc}$, which leads to the following limit for the total link efficiency

$$\eta_{link} \geq SNR\frac{C_{acc}}{R\eta_{det1}\eta_{det2}} = SNR\frac{B_1 B_2 \Delta\tau}{R\eta_{det1}\eta_{det2}} \quad . \tag{4}$$

With a typical detection efficiency $\eta_{det} = 0.3$, a photon production rate of $R = 5 \cdot 10^5\,\mathrm{s}^{-1}$, an estimated total background count rate of $B = 10^3\,\mathrm{s}^{-1}$ and a coincidence timing window of $\Delta\tau = 5 \cdot 10^{-9}\,\mathrm{s}$, the link efficiency should obey

$$\eta_{link} \geq 6.67 \cdot 10^{-7} \quad . \tag{5}$$

Hence a total link efficiency of $\eta_{link} \approx 10^{-6}$ (corresponding to $-60\,\mathrm{dB}$) is necessary.

B. Link Attenuation

We define the link attenuation factor A as the ratio of the mean transmit and receive power, P_T and P_R [30], measured at the entrance and the exit of the transmit and the receive telescope, respectively. Thus losses due to single photon detection efficiency and optical elements such as filters, polarizers or retarders are not included in this number. For ground-to-space links the influence of atmosphere is taken into account by an additional attenuation due to absorption and by increased beam divergence due to atmospheric turbulence. When the receiver is in the transmitter's far field, i.e. when $L \geq D_T^2/\lambda$ and for diffraction-limited transmit telescopes, the attenuation factor A of a one-way link is thus given by

$$A = \frac{L^2(\theta_T^2 + \theta_{\text{atm}}^2)}{D_R^2}\frac{1}{T_T(1-L_P)T_R}10^{A_{\text{atm}}/10} \quad , \tag{6}$$

where L is the link distance, λ is the wavelength, and D_T and D_R are the diameters of the transmit and receive telescope, respectively. With T_T and T_R we denote the transmission factors (≤ 1) of the telescopes, L_P is the pointing loss due misalignment of transmitter and receiver and A_{atm} is the attenuation of the atmosphere, given in dB. The divergence angle resulting from the transmit telescope can be approximated by

$$\theta_T = \frac{\lambda}{D_T} \tag{7}$$

and the atmospheric turbulence causes the additional divergence

$$\theta_{\text{atm}} = \frac{\lambda}{r_0} \quad . \tag{8}$$

Here r_0 is the *Fried parameter* which can be interpreted as an "effective aperture" [31]. We assumed that the divergence due to turbulence adds quadratically to the divergence caused by the telescope.

The effect of turbulence is in general quite different for a space-to-ground link and a ground-to-space link. In a space-to-ground link the light propagates through vacuum for the most of the distance before being disturbed by the atmosphere, whereas for a ground-to-space link the beam spreading effect of turbulence occurs in the first part of the path, causing a strongly enhanced spot diameter at the receiver. Therefore, for space-to-ground links as well as for intersatellite links, we set r_0 to infinity. For ground-to-space links, we assumed $r_0 = 9\,\mathrm{cm}$ at $\lambda = 800\,\mathrm{nm}$, corresponding to weak turbulence [32].

The overall link efficiency of 10^{-6}, corresponding to a maximum attenuation of $60\,\mathrm{dB}$, imposes quite a strong restriction to the various space scenarios. In the following, we present calculation results of the link attenuation for optical free-space links as a function of transmit and receive telescope diameter and link distance.

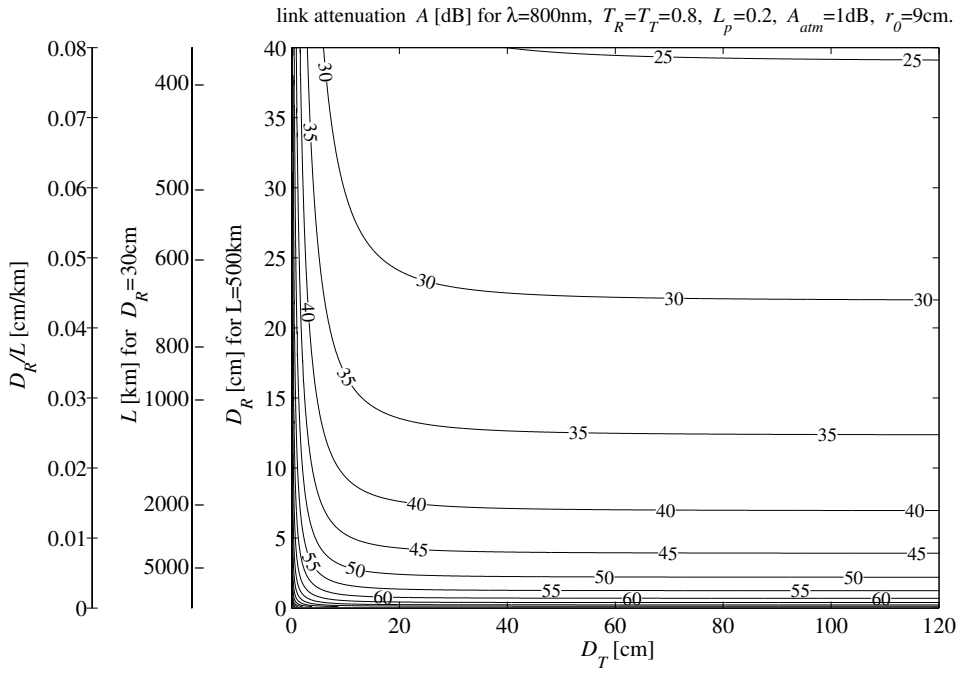

Fig. 2. Contour plot of link attenuation A (in dB) as a function of transmitter and receiver aperture diameter (D_T, D_R) and link distance L for ground-to-LEO uplinks at $\lambda = 800\,\text{nm}$.

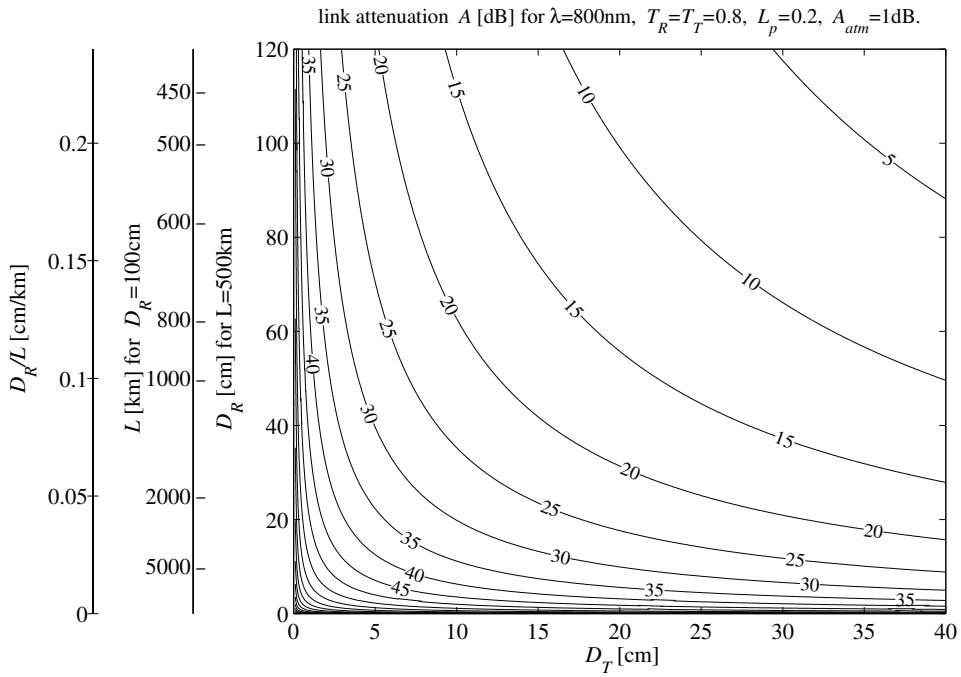

Fig. 3. As Fig. 2 but for LEO-to-ground downlinks.

1) Satellite–ground links: For the case of a LEO-based transmitter or receiver, link attenuation poses no problems. Figure 2 is a contour plot of the link attenuation as a function of transmitter and receiver aperture diameter (D_T,D_R) for ground-to-LEO uplinks operated at a wavelength of $\lambda = 800\,\text{nm}$. Two additional vertical scales give the link distance L for 30 cm receive telescope aperture as well as for the receive telescope aperture for a link distance of $L = 500\,\text{km}$. The corresponding plot for LEO-to-ground downlinks is shown in Fig. 3. One notes that the attenuation is much larger for the uplink than for the downlink. This is caused by the pronounced influence of

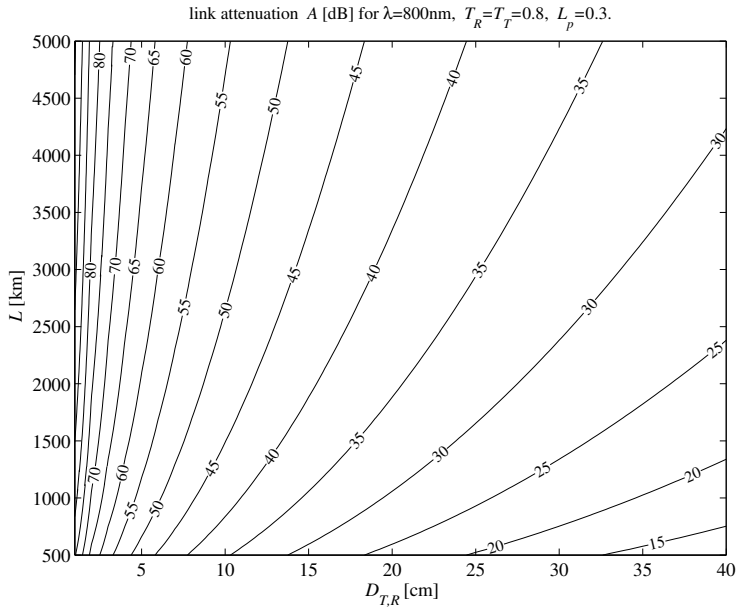

Fig. 4. Contour plot of link attenuation A (in dB) as a function of transmitter and receiver aperture diameter (D_T, D_R) for LEO-to-LEO links at $\lambda = 800\,\text{nm}$.

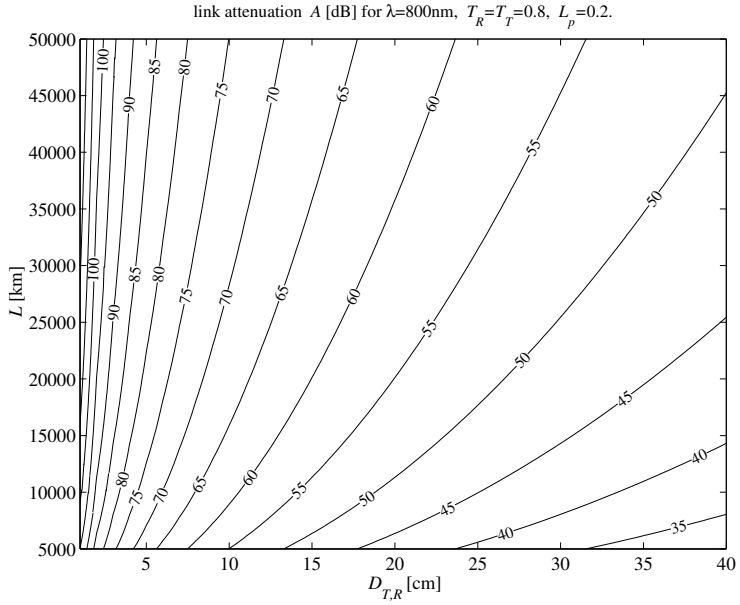

Fig. 5. As Fig. 4 but for GEO-to-GEO links.

atmospheric turbulence for the uplink. Another consequence of turbulence is that increasing the transmitter aperture for the uplink beyond $60\,\text{cm}$ hardly decreases the link attenuation. Even for quite small telescopes on board the LEO satellite, the attenuation factor is well below $60\,\text{dB}$ for all typical cases.

The long distance of links between GEO and ground results in a relatively high attenuation. With a ground station aperture of $D = 100\,\text{cm}$ and a GEO terminal aperture of $D = 30\,\text{cm}$ one will meet the $60\,\text{dB}$-requirement in a downlink, but not in an uplink.

2) Satellite-satellite links: While from a technological point of view a satellite-to-satellite link is the most demanding configuration, it offers highly attractive scientific possibilities. It allows to cover very large distances and might thus also provide a possibility for fundamental tests on quantum entanglement. We calculated the attenuation factor as a function of transmitter and receiver aperture diameter for a LEO-LEO link. Figure 4 displays the attenuation as a function of the satellite distance L and telescope diameters D_T and D_R, assumed to be equal

for both terminals. We conclude that the $60\,$dB-limit poses no problem for LEO-LEO links with reasonable link distance.

For GEO-GEO links, the attenuation can be read off Fig. 5, where again equal telescope apertures have been assumed. For a distance of $L = 45000\,$km, an attenuation of $A = 55\,$dB would result for $D_T = D_R = 30\,$cm.

VII. Proposed experiment

Following the findings of Sect. V, there are three possibilities to establish a secure communication link between a satellite and a ground station, namely scenarios (a), (c) and (f) of Fig. 1. While we have discussed the first two scenarios in detail before [16], [33], the third one can be seen as an extension of the previous two and requires an additional intersatellite link. This configuration has several advantages: As already mentioned in Sect. V-B, the transmitter can by no chance obtain any information about the key the receivers exchange. In addition, the scenario provides more flexibility compared to the previous ones, because none of the two partners sharing the secret key has to posses an entangled-photon source. One and the same transmitter may distribute keys to several pairs of communication partners. If the transmitter terminal is additionally equipped with a reception module, QKD between the transmitter and a ground station (scenario (a) from Fig. 1) can be realized as well as QKD between two satellites.

To set up a QKD protocol as described in Sect. II it is mandatory to establish conventional communication links between all three partners in addition to the two quantum channels discussed above: Data synchronization and comparison of the received key may be established via classical optical or RF links. For this purpose one could use the beacon laser implemented for pointing and acquisition and thus save on hardware [14].

As outlined in Sect. VI-A, the overall link attenuation, i.e. the entire loss for *both* links, must not exceed $60\,$dB. This restricts the scenario to one based on LEO satellites if we stick with telescopes of realistic diameters. Unfortunately, a simultaneous link between two LEO satellites and a ground station is not easy to establish and will typically not last for more than a few minutes. However, the problem would be solved by setting up a network of satellites and ground stations, yielding at the same time a global quantum communication system. In any case, it is still an open matter wether the entanglement of photons is destroyed by decoherence effects taking place in the atmosphere [34].

VIII. Conclusion and outlook

We proposed a scenario for sharing an ultimately secure key between a satellite and a ground station by employing a QKD protocol. In contrast to previous proposals, the quantum source providing the communication partners with pairs of entangled photons is located on a separate satellite. This results in a less stringent security demand on the source and provides more flexibility with regard to future quantum communication networks.

The size and mass of up-to-date entangled photon sources have come down to values where space experiments are feasible. Yet, space qualification is still an issue. It is shown that the overall link attenuation has to be smaller than about $60\,$dB to prohibit a local realistic model of the observed correlations and thus to make impossible eavesdropping by a third party. An assessment of the actual link attenuation for several scenarios has been presented, with the conclusion that the proposed configuration is possible for LEO satellites, unless the telescopes would be excessively large.

The results obtainable with an experiment as suggested would not only give novel insight in our understanding of the validity of quantum physics but also provide a better understanding of the interaction of entangled systems with a “natural” environment. At the same time, the proposed scenario could serve as basis for a new generation of quantum physics experiments.

Acknowledgment

This paper evolved from a project supported by the European Space Agency under ESTEC Contract No. 16358/02/NL/SFe, “Quantum Communications in Space”. We wish to thank Josep Maria Perdigues Armengol for monitoring and supporting this work.

REFERENCES

[1] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Phys. Rev. Lett.*, vol. 69, p. 2881, 1992.

[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, no. 13, pp. 1895–1899, 1993.

[3] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*. New York: IEEE, 1984, p. 175.

[4] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, 1991.

[5] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New Journal of Physics*, vol. 4, pp. 43.1–43.14, 2002.

[6] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum cryptography with entangled photons," *Phys. Rev. Lett.*, 2000.

[7] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," *New Journal of Physics*, vol. 4, pp. 41.1–41.8, 2002.

[8] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Violation of bell inequalities by photons more than 10 km apart," *Phys. Rev. Lett.*, vol. 81, pp. 3563–3566, 1998.

[9] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, "Single photon quantum cryptography," *Phys. Rev. Lett.*, vol. 89, p. 187901, 2002.

[10] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, "A step torwards global key distribution," *Nature*, vol. 419, p. 450, 2002.

[11] J. G. Rarity, P. R. Tasper, P. M. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New Journal of Physics*, no. 4, pp. 82.1–82.21, 2002.

[12] Z. Yuan, C. Gobby, and A. J. Shields, "Quantum key distribution over 101 km telecom fibre," in *Proc. CLEO/QUELS*, 2003.

[13] H. Kosaka, A. Tomita, Y. Nambu, T. Kimura, and K. Nakamura, "Single-photon interference experiment over 100 km for quantum cryptography system using a balanced gated-mode photon detector," *quant/ph 0306066*, 2003.

[14] M. Aspelmeyer, H. R. Böhm, C. Brukner, R. Kaltenbaek, M. Lindenthal, J. Petschinka, T. Jennewein, R. Ursin, P. Walther, A. Zeilinger, M. Pfennigbauer, and W. R. Leeb, "Quantum Communications in Space (QSpace): Final Report," Institut für Nachrichtentechnik und Hochfrequenztechnik, TU Wien, Institut für Experimentalphysik, Universität Wien," European Space Agency Contract Report, ESTEC, Contract No. 16358/02/NL/SFe, 2003.

[15] R. Kaltenbaek, M. Aspelmeyer, T. Jennewein, C. Brukner, A. Zeilinger, M. Pfennigbauer, and W. R. Leeb, "Proof-of-concept experiments for quantum physics in space," in *Proc. SPIE, Optical Science and Technology, 48th annual meeting, San Diego (CA)*, 2003.

[16] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger, "Long-distance quantum communication with entangled photons using satellites," *Journal of Selected Topics in Quantum Electronics*, 2003.

[17] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Phys. Rev. Lett.*, vol. 68, pp. 557–559, 1992.

[18] W. K. Wooters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, p. 802, 1982.

[19] J. Bell, *Physics*, vol. 1, p. 195, 1964.

[20] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, pp. 3–28, 1992.

[21] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, 2002.

[22] E. Waks, A. Zeevi, and Y. Yamamoto, "Security of quantum key distribution with entangled photons against individual attacks," *Phys. Rev. A*, vol. 65, p. 52310, 2002.

[23] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, ""Event-ready-detectors" Bell experiment via entanglement swapping," vol. 71, no. 26, pp. 4287–4290, 1993.

[24] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, pp. 5932–5935, 1998.

[25] H. Horvath, L. A. Arboledas, F. J. Olmo, O. Jovanović, M. Gangl, W. Kallner, C. Sánchez, H. Sauerzopf, and S. Seidl, "Optical characteristics of the aerosol on Spain and Austria and its effect on radiative forcing," *J. Geo-phys. Res.*, vol. 107, p. 4386, 2002.

[26] C. H. Bennett, C. A. Fuchs, and J. A. Smolin, "Entanglement-enhanced classical communication on a noisy quantum channel," *Quantum Comminication, Computing, and Measurement (O. Hirota, A. S. Holevo, and C. M. Caves ed.) Plenum, New York (1997) ISBN 0-306-45685-0*, pp. 79–88, 1996.

[27] D. Bouwmeester, A. Ekert, and A. Zeilinger, Eds., *The Physics of Quantum Information*. Berlin: Springer-Verlag, 2000.

[28] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, "Optimal eavesdropping in quantum cryptography. I. information bound and optimal strategy," *Phys. Rev. A*, vol. 56, pp. 1163–1172, 1997.

[29] S. Aerts, P. Kwiat, J.-ÅLarsson, and M. Zukowski, "Two-photon Franson-type experiments and local realism," *Phys. Rev. Lett.*, vol. 83, p. 2872, 1999.

[30] M. Reyes, Z. Sodnik, P. Lopez, A. Alonso, T. Viera, and G. Oppenhäuser, "Preliminary results of the in-orbit test of ARTEMIS with the optical ground station," in *Proc. SPIE, Free-Space Laser Communication Technologies XIV*, vol. 4635, January 2002, pp. 38–49.

[31] D. L. Fried, "Optical resolution through a randomly inhomogeneous medium for very long and very short exposures," *Journal of the Optical Society of America*, vol. 56, pp. 1372–1379, 1966.

[32] Z. Sodnik (ESTEC/ESA), March 2003, personal communication.

[33] J. Rarity, M. Aspelmeyer, H. Weinfurter, C. Kurtsiefer, P. M. Gorman, P. R. Tapster, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger, "Quantum communications in space," in *Proc. CLEO Europe, Conference on Lasers and Electro-Optics*, 2003.

[34] G. Gilbert and M. Hamrick, "Practical quantum cryptography: A comprehensive alalysis (part one)," MITRE," Technical Report, 2000.