Space-QUEST: quantum physics and quantum communication in space

Rupert Ursin[a], Thomas Jennewein[b], and Anton Zeilinger[a,b]

[a]Faculty of Physics, University of Vienna, Austria;
[b]Institute for Quantum Optics and Quantum Information (IQOQI),
Austrian Academy of Sciences, Austria

ABSTRACT

Fundamental quantum optics test as well as quantum cryptography and quantum teleportation are based on the distribution of single quantum states and quantum entanglement respectively. We will discuss recent experimental achievements in the field of long-distance quantum communication via optical fiber as well as in free-space over a record breaking distance of 144 km. The European Space Agency (ESA) has supported a range of studies in the field of quantum physics and quantuminformation science in space for several years, and consequently a mission proposal Space-QUEST Quantum Entanglement for Space Experiments was submitted to the European Life and Physical Sciences in Space Program. This proposal envisions to perform space-to-ground quantum communication tests from the International Space Station (ISS) and will presented in this article.

Keywords: Quantum communication, quantum cryptography, quantum teleportation

1. INTRODUCTION

Quantum mechanics predicts that entangled systems have stronger than classical correlations that are independent of the distance between the particles and are not explicable with classical physics.[1,2] It is an open issue whether quantum laws, originally established to describe nature at the microscopic level of atoms, are also valid in the macroscopic domain accessible in space. Testing the quantum correlations over distances achievable with systems placed in the Earth orbit or even beyond[3] would allow to verify both the validity of quantum physics and the preservation of entanglement over distances impossible to achieve on ground.

Quantum mechanics is also the basis for emerging technologies of quantum information science, presently a very active research field in physics. Today's most prominent application is quantum key distribution (QKD),[4] i.e. the generation of a provably unconditionally secure key at distance, which is not possible with classical cryptography. Another area of applications is in metrology, where quantum clock synchronization and quantum positioning[5] are studied.

Classical physics inherently includes assumptions of locality and realism. Reality supposes that results of measurements are associated to properties that the particles carry prior to and independent of measurements. Locality supposes that the measurement results are independent of any action performed at space-like separated locations. Consequently local realism imposes constraints on statistical correlations of measurements on multi-particle systems (in so called Bell-type experiments[1]). Quantum mechanics, however, predicts much stronger correlations and is therefore in contradiction with at least one of the underlying principles. Up to now, many experiments performed on ground have been performed confirming the quantum mechanical predictions on these scales. To perform such kind of experiments over long (even astronomic) distances would verify the validity of quantum physics and the preservation of entanglement on the new scales accessible and will eventually allow us to realize quantum communication demonstrations on a global scale.

Here we will first discuss experiments we performed as a proof-of-principle demonstration of the various quantum communication protocols. In the last section we will give more details on our proposal to the European Space Agency ESA to perform theses experiments in space.

Send correspondence to E-mail: Rupert.Ursin@univie.ac.at

Quantum Communications Realized II, edited by Yasuhiko Arakawa, Masahide Sasaki, Hideyuki Sotobayashi,
Proc. of SPIE Vol. 7236, 723609 · © 2009 SPIE · CCC code: 0277-786X/09/$18 · doi: 10.1117/12.814711

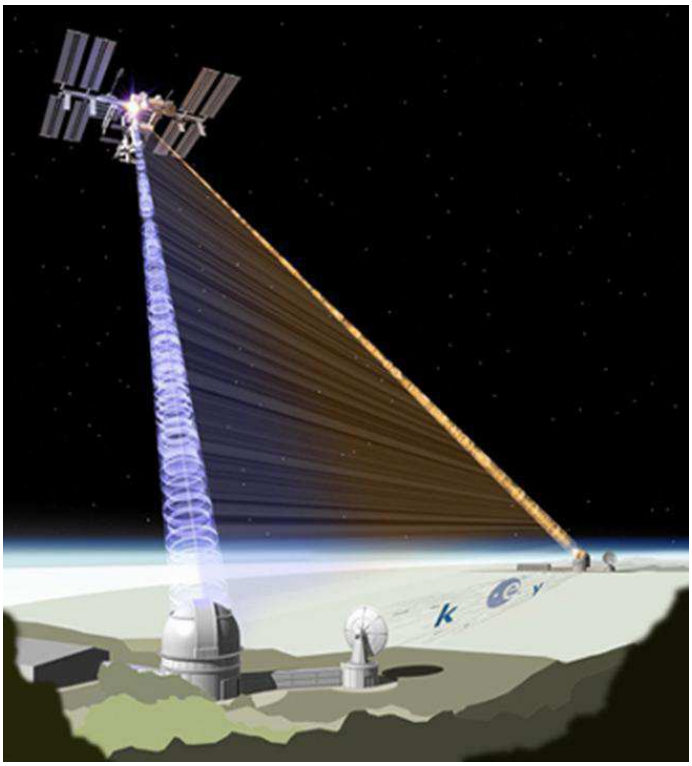

Figure 1. The Vision: Distribution of pairs of entangled photons using the International Space Station (ISS). Entangled photon pairs are simultaneously distributed to two separated locations on Earth thus enabling both fundamental quantum physics experiments and novel applications such as quantum key distribution (QKD).

1.1 QUANTUM KEY DISTRIBUTION

Quantum key distribution provides informationtheoretically provable secure communication methods for individuals based on qualitatively new concepts in quantum mechanics, which are much more powerful than their classical counterparts. Unlike traditional cryptography, which depends on the computational complexity of mathematical techniques to reduce the possibility that eavesdroppers might learn the contents of encrypted messages, quantum cryptography depends on the fact that naive attempts to read quantum information will destroy the information (ie. there is no way to copy unknown quantum states[6] nor to measure it with an arbitrarily high precision due to the Heisenberg uncertainty principle). For the communicating partners, a combination of quantum and classical techniques are used to produce keys which can be proven to be information theoretically unconditional secure - that is, a produced hidden key cannot have been read by any other than the intended participants. This is because measurements on the quantum carrier of information disturbs it and therefore leaves traces, for an overview see Ref.[4] Two well known schemes of QKD are used in practical systems used today. The first is to send random single quantum states (generated usually from a faint pulsed laser) to a receiver.[7] The second scheme is based on entangled pairs and uses Bell's inequality to establish security.[8] Both Alice and Bob receive one particle out of an entangled pair.[9] Using receiver units identical to the one used in the faint pulse cryptography scheme, they establish identical random keys at both receiver units.

The potential eavesdropper would introduce errors with her measurement, so that the quantum bit error ratio (QBER) of the sifted key gives an upper bound on the information an eavesdropper might have gained. The QBER is calculated during the classical error correction procedure and is used to infer the shrinking ratio that is needed to make sure that the information of a potential eavesdropper on the key is negligible. The key is then hashed to this secure length during privacy amplification. Such a quantum source on a space-based terminal could distribute quantum states to one- or even simultaneously to two optical ground stations where the quantum key will be generated.

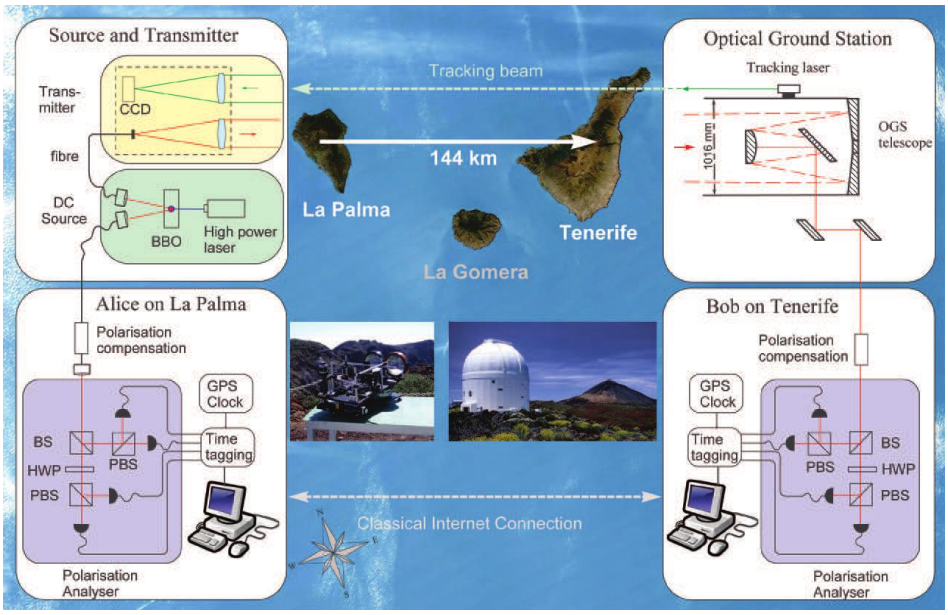

Figure 2. The setup for free-space entanglement distribution between La Palma and Tenerife. An entangled photon pair is created in La Palma, one photon is measured locally and it's partner is sent over the 144 km free-space path to Tenerife, where it's measured using a 1 m telescope of the European Space Agency.

QKD is intrinsically a point-to-point key establishment protocol between the two locations where the QKD devices are located. It is also possible to extend single QKD links, as described above, to a quantum network by key relaying along a chain of trusted nodes[10,11] using satellites as well as fiber-based systems. Furthermore, the efficiency of quantum networks can be improved employing quantum percolation protocols.[12] Furthermore such a quantum transceiver in space is capable of performing two consecutive single downlinks using the entangled or the weak pulse laser onboard the satellite establishing two different secure keys between the satellite and each of the ground stations (say, Vienna and Tokyo). Then a logical combination of the two keys (e.g. bitwise XOR) is sent publicly to one of the two ground stations. Out of that one unconditionally secure key between the two ground stations can be computed. Using such a scheme would allow for the first demonstration of global quantum key distribution. Networked QKD have much greater impact, and indeed will ultimately become additionally to optical fiber in communication networks on local area network key distribution schemes.

2. FREE-SPACE QUANTUM COMMUNICATION

As an important step towards quantum communication protocols using satellites, various proof-of-principle demonstrations of quantum communication protocols have already been performed over terrestrial free-space links.[13–16] An experiment was carried out on the Canary islands using a 144 km free-space link, between the neighboring Canary islands La Palma and Tenerife (Spain), where ESA's 1-meter-diameter receiver telescope, originally designed for classical laser communication with satellites, was used to receive single photons. Entangled photons were distributed between this two islands[17] as well as an faint laser pulsed quantum key distribution was demonstrated over this 144 km link.[18]

A satellite-to-Earth quantum-channel down-link was simulated in an experiment by reflecting attenuated laser pulses off the optical retroreflector on board of the satellite Ajisai, whose orbit has a perigee height of 1485 km.[19] We choosed the relevant experimental parameters in order to make the number of photons per laser pulse in the downward link much less than unity. Our investigation differs with respect to the satellite laser ranging techniques,[20] since we were counting the returns in a series of pre-determined time bins and not measuring the range time. Our observable was not the range itself but the number of detected photons per second, as an initial step toward the measurement of the individual photons in quantum communication. Our

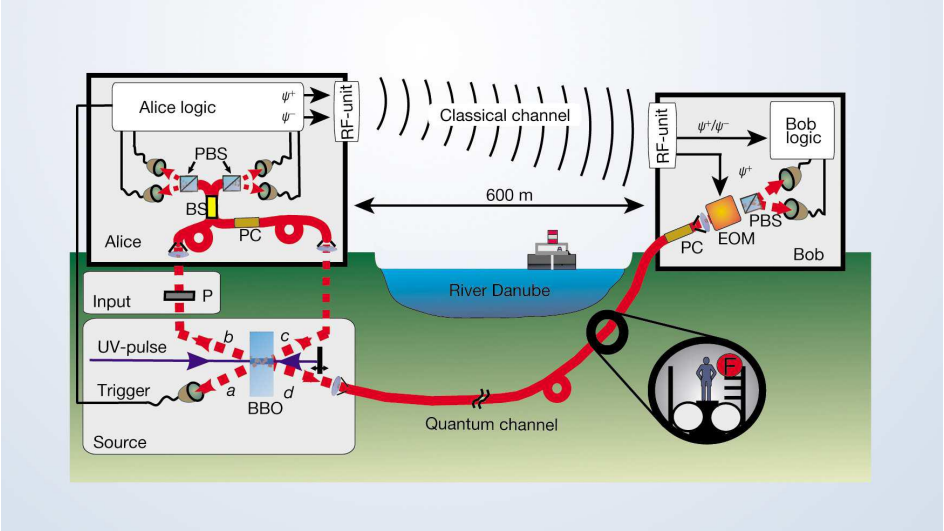

Figure 3. Long-distance quantum teleportation across the River Danube.

aim was to demonstrate that a source corresponding to a single photon emitter on a LEO satellite can indeed be identified and detected by an optical state-of-the-art ground station, even in the presence of a very high background noise. According to the link-budget, only an average of 0.4 photons are directed in the downward channel, thus realizing the condition of the single-photon channel. The return rate observed for satellite Ajisai corresponds to a total attenuation along the light path of −157 dB, including the telescope, the optical bench and the detector.

An important component in space based quantum communication is a source for entangled photons, that is suitable for space applications in terms of efficiency, mass and power consumption. A source fulfilling the payload requirements based on highly efficient down-conversion crystals which deliver the necessary numbers of photon pairs is published in.[21,22]

3. QUANTUM TELEPORTATION

Efficient long-distance quantum teleportation[23] is a crucial ingredient for future quantum computer application,[24] since quantum computers[25,26] internally compute quantum states and will have to communicate among each other. Quantum repeaters[27] will allow to distribute quantum entanglement over distances thus being vital for future global quantum communication networks. At present the only suitable system for efficient long-distance quantum communication is photons. A quantum teleportation over long-distances was performed in fiber over 600m.[28] This fiber was installed in the sewage system underneath the city of Vienna across the river Danube.

Quantum teleportation is based on a quantum channel, here established through a pair of polarization-entangled photons shared between Alice and Bob. This was implemented by using an 800-metre-long optical fibre installed in a public sewer system located in a tunnel underneath the River Danube, where it is exposed to temperature fluctuations and other environmental factors. For Alice to be able to transfer the unknown polarization state of an input photon, she has to perform a joint so-called Bell-state measurement on the input photon and her member of the shared entangled photon pair. Our scheme allows her to identify two out of the four Bell states which is the optimum achievable with only linear optics.[29] As a result of this Bell-state measurement, Bob's receiver photon will always be found in a state already containing full information or a simple bit-flip operation depending on the specific Bell state that Alice observed. Our teleportation scheme therefore also includes active feed-forward of Alice's measurement results, which is achieved by means of a classical microwave channel together with a fast electro-optical modulator (EOM). It enables Bob to perform the bit-flip on his photon to obtain an exact replica of Alice's input photon. For successful operation of this experimental scheme, Bob has to set the EOM correctly before photon arrives. Because of the reduced velocity of light within the

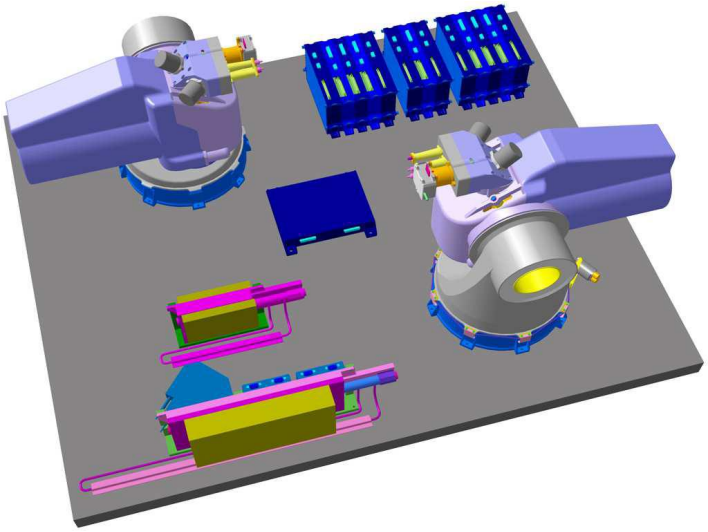

Figure 4. The terminal foreseen to be attached to the European ISS module Columbus consists of an entangled photon pair and a faint laser module. The two telescopes will be used to transmit the single photons to two different ground ground stations.

fibre-based quantum channel (two-thirds of that in vacuum), the classical signal arrives well before the photon which has to be teleported. In this experiment we were able to teleport a qubit with a fidelity of up to $0,86\%$. In a future space experiment a quantum teleportation might also be possible in an uplink scenario similar to what is described in.[30]

4. SPACE-QUEST

Terrestrial free-space links suffer from obstruction of objects in the line of sight, from possible severe attenuation due to weather conditions and aerosols[31] and, ultimately, from the Earths curvature. With current optical fiber and photon-detector technology quantum communication on ground is limited also to the order of 100 of kilometers[32] this was tested in experiments by.[33,34] The use of satellites allows for experimental tests on quantum entanglement on a global (or even an astronomical) scale and it allows for demonstrations of quantum communication on a global scale clearly not possible on ground.

The Space-QUEST (**Qu**antum **E**ntanglement for **S**pace Experimen**t**s) proposal envisions to perform space-to-ground quantum communication tests from the International Space Station (ISS) orbiting at a hight of about 400 km. The single and entangled photons will be produced by a quantum source onboard the ISS and transmitted via free-space optical communication links simultaneously to one or two different optical ground stations.[35] The quantum transceiver is currently foreseen to be placed on the external pallet of the European Columbus module at the ISS. The proposed payload is compliant with the specifications given for pallet payloads as provided by ESA.[36] The requirements are: size 1.391.170.86 m^3, mass < 100 kg, and a peak power consumption of < 250 W, respectively. A preliminary design of a satellite-based quantum transceiver (including an entangled photon source, a weak pulse laser sources, single photon detection modules together with two transceiver telescopes) based on state-of-the-art optical communication terminals and adapted to the needs of quantum communication is described in detail in[37] and is currently developed in a collaboration with partners from academia and industry.

5. CONCLUSION

After having reviewed experiments to demonstrate the feasibility of quantum communication in real world scenario over free-space links we presented our Space-QUEST proposal to the European Space Agency. The space environment will allow quantum physics experiments with photonic entanglement and single photon quantum states to be performed on a large, even global, scale. The Space-QUEST proposal aims to place a quantum

communication transceiver containing the entangled photon source, a weak pulsed (decoy states) laser source and single photon counting modules in space and will accomplish the first-ever demonstration in space of fundamental tests on quantum physics and quantum-based telecom applications. The unique features of space offer extremely long propagation paths to explore the limits of the validity of quantum physic's principles. In particular, this system will allow for a test of quantum entanglement over a distance exceeding $1000km$, which is impossible on ground. The present programmatic roadmap of Space-QUEST is compatible with a launch date by end of 2014.[38]

ACKNOWLEDGEMENTS

This work was supported by the European Space Agency under contract numbers 16358/02/NL/SFe, 17766/03/NL/PM and 18805/04/NL/HE as well as by Austrian Space Agency (FFG). Additional funding was provided by the European Commission (QAP).

REFERENCES

[1] Bell, J. S., "On the Einstein Podolsky Rosen paradox," *Physics* **1**, 195–200 (1964).

[2] Leggett, A. J., "Nonlocal hidden-variable theories and quantum mechanics: An incompatibility theorem," *Found. Phys.* **33**, 14691493 (2003).

[3] Kaltenbaek, R., Aspelmeyer, M., Pfennigbauer, M., Jennewein, T., Brukner, C., Leeb, W. R., and Zeilinger, A., "Proof-of-concept experiments for quantum physics in space," *Proc. of SPIE* **5161**, 252–268 (2003).

[4] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H., "Quantum cryptography," *Rev. Mod. Phys.* **74**, 145–195 (Mar 2002).

[5] Valencia, A., Chekhova, M. V., Trifonov, A., and Shih, Y., "Entangled two-photon wave packet in a dispersive medium," *Phys. Rev. Lett.* **88**, 183601 (Apr 2002).

[6] Wooters, W. K. and Zurek, W. H., "A single quantum cannot be cloned," *Nature* **299**, 802 (1982).

[7] Bennett, C. H. and Brassard, G., "Quantum cryptography," in [*Proceedings of IEEE International Conference on Computers, Systems, andSignal Processing, Bangalore, India*], 175, IEEE, New York (1984).

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

[9] Jennewein, T., Simon, C., Weihs, G., Weinfurter, H., and Zeilinger, A., "Quantum cryptography with entangled photons," *Phys. Rev. Lett.* **84**, 4729 (2000).

[10] Poppe, A., Peev, M., and Maurhart, O., "Outline of the secoqc quantum-key-distribution network in vienna," *to appear in Int. J. Quant. Inf.* (2008).

[11] Dianati, M. and und M. Gagnaire und X. Shen, R. A., "Architecture and protocols of the future european quantum key distribution network," *Security and Communication Networks* **1**, 57–74 (2008).

[12] Acin, A., Cirac, J. I., and Lewenstein, M., "Entanglement percolation in quantum networks," *Nature Physics* **3**, 256–259 (2007).

[13] Hughes, R. J., Nordholt, J. E., Derkacs, D., and G.Peterson, "Practical free-space quantum key distribution over 10 km in daylight andat night," *New Journal of Physics* **4**, 43 (2002).

[14] Kurtsiefer, C., Zarda, P., Halder, M., Weinfurter, H., Gorman, P. M., Tapster, P. R., and Rarity, J. G., "A step towards global key distribution," *Nature* **419**, 450 (2002).

[15] Aspelmeyer, M., Böhm, H., Gyatso, T., Jennewein, T., Kaltenbaek, R., Lindenthal, M., Molina-Terriza, G., Poppe, A., Resch, K., Taraba, M., Ursin, R., Walther, P., and Zeilinger, A., "Long-distance free-space distribution of entangled photons," *Science* **301**, 621–623 (2003).

[16] Peng, C. Z., Yang, T., Bao, X. H., Z, J., andF. Y. Feng, X. M. J., Yang, J., Yin, J., Zhang, Q., Li, N., Tian, B. L., and Pan, J. W., "Experimental free-space distribution of entangled photon pairs over a noisy ground atmosphere of 13km," *Phys. Rev. Lett.* **94**, 150501 (2005).

[17] Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H., Scheidl, T., Lindenthal, M., Blauensteiner, B., Jennewein, T., Perdigues, J., Trojek, P., Oemer, B., Fuerst, M., Meyenburg, M., Rarity, J., Sodnik, Z., Barbieri, C., Weinfurter, H., and Zeilinger, A., "Entanglement-based quantrum communication over 144 km," *Nature Physics* **3**, 481 – 486 (2007).

[18] Schmitt-Manderbach, T., Weier, H., Fuerst, 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).

[19] Villoresi, P., Jennewein, T., Tamburini, F., Aspelmeyer, M., Bonato, C., Ursin, R., Pernechele, C., Luceri, V., Bianco, G., Zeilinger, A., and Barbieri, C., "Experimental verification of the feasibility of a quantum channel between space and earth," *New Journal of Physics* **10**(3), 033038 (12pp) (2008).

[20] P, B. and C, G., [*Probable LAGEOS contribution to a worldwide geodynamics control network The Use of Artificial Satellites for Geodesy and Geodynamics vol II ed G Veis and E Livieratos*], Athens: National Technical University (1979).

[21] Fedrizzi, A., Herbst, T., Poppe, A., Jennewein, T., and Zeilinger, A., "A wavelength-tunable fiber-coupled source of narrowband entangled photons," *Opt. Express* **15**(23), 15377–15386 (2007).

[22] Trojek, P. and Weinfurter, H., "Collinear source of polarization-entangled photon pairs at nondegenerate wavelengths," *Applied Physics Letters* **92**(21), 211103 (2008).

[23] Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., and andW. K. Wootters, A. P., "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosenchannels," *Phys. Rev. Lett.* **70**, 1895 (1993).

[24] Deutsch, D. and Ekert, E., "Quantum computation," *Phys. World* **11**, 47–52 (1998).

[25] Gottesmann, D. and Chuang, I. L., "Demonstrating the viability of universal quantum computation usinf teleportationanf single-qubit operations," *Nature* **402**, 390 (1999).

[26] Knill, E., Laflamme, R., and Milburn, G. J., "A scheme for efficient quantum computation with linear optics," *Nature* **409**, 46–52 (2001).

[27] Briegel, H.-J., Dr, W., Cirac, J., and Zoller, P., "Quantum repeaters: the role of imperfect local operations in quantum communication," *Phys. Rev. Lett.* **81**, 5932–5935 (1998).

[28] Ursin, R., Jennewein, T., Aspelmeyer, M., Kaltenbaek, R., Lindenthal, M., Walther, P., and Zeilinger, A., "Quantum teleportation across the danube," *Nature* **430**, 849 (2004).

[29] Lütkenhaus, N., Calsamiglia, J., and Suominen, K. A. *Phys. Rev. Lett.* **59**, 3295 (1999).

[30] Rarity, J. G., Tapster, P. R., Gorman, P. M., and Knight, P., "Ground to satellite secure key exchange using quantum cryptography," *New Journal of Physics* **4**, 82 (2002).

[31] Horvath, H., Arboledas, L. A., Olmo, F. J., andM. Gangl, O. J., Kaller, W., Sánchez, C., Sauerzopf, H., and Seidl, S., "Optical characteristics of the aerosol in spain and austria and its effecton radiative forcing," *J. Geophys. Res.* **107(D19)**, 4386 (2002).

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

[33] Takesue, H., Diamanti, E., Honjo, T., Langrock, C., Fejer, M. M., Inoue, K., and Yamamoto, Y., "Differential phase shift quantum key distribution experiment over 105 km fibre," *New Journal of Physics* **7**, 232 (2005).

[34] Tanaka, A., Fujiwara, M., Nam, S. W., Nambu, Y., Takahashi, S., Maeda, W., ichiro Yoshino, K., Miki, S., Baek, B., Wang, Z., Tajima, A., Sasaki, M., and Tomita, A., "Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization," *Opt. Express* **16**(15), 11354–11360 (2008).

[35] Aspelmeyer, M., Jennewein, T., Pfennigbauer, M., Leeb, W. R., and Zeilinger, A., "Long-distance quantum communication with entangled photons using satellites," in [*IEEE Journal of Selected Topics in Quantum Electronics 1541-1551*], (2003).

[36] Carey, W., Isakeit, D., Heppener, M., Knott, K., and Feustel-Bechl, J., "The international space station european users guide," tech. rep., Tech. Rep., European Space Agency, ISS User Information Centre (MSM-GAU), ESTEC (2001).

[37] Pfennigbauer, M., Aspelmeyer, M., Leeb, W., Baister, G., Dreischer, T., Jennewein, T., Neckamm, G., Perdigues, J., Weinfurter, H., and Zeilinger, A., "Satellite-based quantum communication terminal employing state-of-the-art technology," *J. Opt. Netw.* **4**(9), 549–560 (2005).

[38] Perdigues, J., Furch, B., de Matos, C., Minster, O., Cacciapuoti, L., Pfennigbauer, M., Aspelmeier, M., Jennewein, T., Ursin, R., Schmitt-Manderbach, T., Baister, G., Rarity, J., Leeb, W., Barbieri, C., Weinfurter, H., and Zeilinger, A., "Quantum communications at esa: Towards a space experiment on the iss," *Acta Astronautica* **63**, 165–178.