Space-QUEST: Quantum Communication Using Satellites

Thomas Scheidl and Rupert Ursin
Institute for Quantum Optics and Quantum Information
Austrian Academy of Sciences
Vienna, Austria
thomas.scheidl@univie.ac.at, rupert.ursin@univie.ac.at

Abstract — **The emerging applications and technologies based on the foundations of quantum physics have revolutionized our understanding of information theory. Particularly, the quantum physical principles of superposition and entanglement constitute a novel type of resource that enables new developments in the fields of communications, computation, metrology, etc., and open new doors for fundamental physics research [1]. The European Space Agency (ESA) has supported several studies in the field of quantum communications for space systems. As a result of these studies, the mission proposal Space-QUEST ("QUantum Entanglement for Space ExperimenTs") was submitted to the European Life and Physical Sciences in Space Program of ESA by a European research consortium, led by Prof. Zeilinger (Vienna University), aiming at quantum communication space-to-ground experiments from the International Space Station (ISS). This paper is to present an overview of the proposed experiments and to summarize the experimental proof-of-concept demonstrations that have been performed on a 144km horizontal free-space link between the Canary Islands of La Palma and Tenerife up to the present.**

Keywords – quantum communication; quantum entanglement; Space-QUEST; free-space

I. Introduction

Quantum physics, originally established to describe nature at the microscopic level of atoms, is one of the main areas of modern physics and is well tested at length scales and velocities available in ground based laboratories. It is, however, an open issue whether quantum laws are also valid in the macroscopic domain such as long distances. Entanglement is probably the most important concept of quantum mechanics and at the same time its most counterintuitive feature. The perfect correlations between entangled quantum systems are in conflict with the concepts of classical physics. Various proposals predict that quantum entanglement is limited to certain mass and length scales or is altered under specific gravitational circumstances. On the quest for investigating the validity of quantum mechanics, experimental tests must be extended beyond distances and velocities achievable on the ground and must enter regimes where effects of quantum physics and relativity begin to interplay. Therefore, only the unique space environment offers the potential for performing experiments on quantum interference or quantum entanglement on distances of up to thousands of kilometers and with observers moving at relativistic velocities.

Closely related to the scientific interests of extending the distances between quantum systems are the commercial interests of the fairly young technical field of quantum cryptography. There, quantum entanglement is already used in an application called "quantum key distribution" (QKD) [2], where a provable unconditionally secure key is generated between two communicating parties at a distance, a task not possible with classical cryptography. The use of satellites allows demonstrating quantum communication on a global scale and proofing the feasibility of a future global quantum communication network. With current optical fiber and photon-detector technology quantum communication is limited to the order of 200 km [3]. Hence, the only way to overcome this limitation with state-of-the art technology is to bring quantum communication into space.

Photons are ideal for propagating over long-distances in free-space and are thus best suited for quantum communication experiments between space and ground. The unit of quantum information is the "qubit" (a bit of information "stamped" in a quantum physical property, for instance the polarization of a photon).

II. Proposed Experiments

A. Bell Test

Bell's theorem shows that local realistic theories (e.g. classical physics) place strong restrictions on observable correlations between different systems, giving rise to Bell's inequality [4]. Using entangled quantum states (e.g. the polarization-entangled state of two photons) the Bell inequality can be violated in an experiment. The standard quantum model predicts no limit for the distance-range of such non-local quantum correlations between entangled photon pairs and up to now they could be observed between two observers separated by 144 km. Verifying the quantum mechanical predictions over significantly longer distances remains still to be experimentally proven and necessitates the use of satellite-to-ground or inter-satellite free-space links.

The experimental prerequisites to perform Bell experiments are a source of entangled photons (located in the transmitter terminal) and two analyzing receiver-terminals, which individually can vary their measurement basis and store the arrival time of single-photon detection events with respect to a local time standard. Specifically, in the case of polarization-entangled photons, polarization measurements are performed with varying polarizer settings at each receiver site. To achieve distances on the scale of 1000 km it would be sufficient to have an entangled photons source in a low-earth-orbit (LEO), which sends the two photons to two ground based receivers.

B. Quantum Key Distribution (QKD)

Depending on the type of protocol, QKD relies on the transmission and detection of either single photons or entangled photon pairs. In both case, the security is essentially based on the impossibility to copy an unknown quantum state of a single photon (no-cloning theorem) and thus by the laws of quantum physics. One clear vision of the science community is to establish a worldwide network for quantum communication — a task that can only be realized by tackling the additional challenge of bringing QKD technology into space [5].

The single photon QKD protocol [6] is usually implemented using weak coherent laser pulses (WCP), prepared by the transmitter randomly in one out of four polarization states. The receiver analyzes the incoming photons again randomly in one of two measurement bases and stores the arrival time of single-photon detection events with respect to a local time standard. After basis reconciliation, classical error correction [7] and privacy amplification [8], the transmitter and receiver end up with an unconditional secure quantum cryptographic key. Such a WCP quantum transmitter in space is capable of performing two consecutive single downlinks, 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, an unconditionally secure key between the two ground stations can be computed.

In case of the entanglement based QKD protocol [9], the two photons of an entangled pair are transmitted via separate downlinks to two different ground stations. There the polarization of each individual photon is measured randomly in one of two different measurement bases. Due to entanglement, both receivers will obtain the same result whenever they have chosen the same measurement basis. Thus, after basis reconciliation and classical error correction an unconditional secure key can be generated between the two ground stations. The experimental prerequisites are the same as for the Bell experiments described above. These are a source of entangled photons on board the satellite and two analyzing receiver-terminals on earth, which individually can vary their measurement basis and store the arrival time of the single-photon detection events.

C. Implementation at the ISS

The above described experiments can be performed by placing a quantum transceiver on the external pallet of the European Columbus module at the ISS (see Figure 1). The entire terminal must not exceed the specifications given for pallet payloads as provided by ESA. The requirements are: size $1.39\times1.17\times0.86\ m^3$, 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 WCP source, single photon detection modules together with two transceiver telescopes, based on state-of-the-

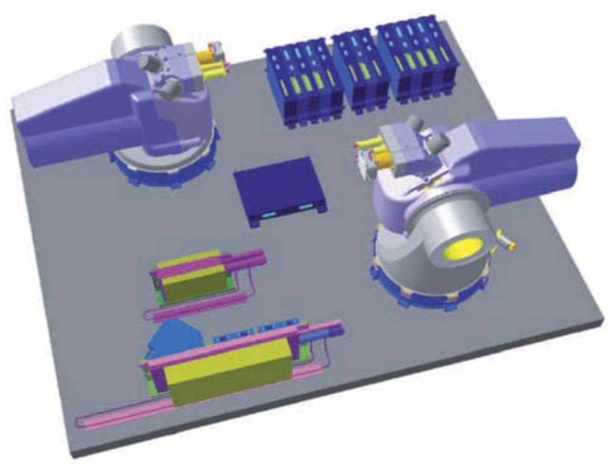

Figure 1. Image of the preliminary design of a transceiver suitable for the external pallet of the European Columbus module at the ISS. The terminal contains a source for entangled photons as well as for weak coherent laser pulses, the onboard electronics and two transmitter telescopes. (Image courtesy RUAG.)

art optical communication terminals and adapted to the needs of quantum communication has already been published in [10].

III. Proof-of-Concept Demonstrations

In this chapter we would like to summarize several experimental on-ground investigations proofing the concept of quantum communication experiments in space.

A. Demonstration of a Single-Photon Satellite Downlink

In a first experimental demonstration of a quantum communication channel between a low-Earth orbit (LEO) satellite and a receiver station on Earth (the ASI-Matera-Laser-Ranging-Observatory, Italy), a single-photon quantum communication channel was effectively simulated by reflecting faint laser pulses off the optical retro-reflecting satellite Ajisai, whose orbit has a perigee height of 1485 km, realizing a satellite-to-Earth quantum-channel [11]. The identification of the exchanged photons was ascertained by observing a significant amount of detector counts at the expected arrival instant with respect to the background value.

B. *Long-Distance Bell Tests*

Several long-distance Bell experiments have been performed between the Canary Islands of La Palma and Tenerife via a 144 km free-space link, and employing ESA's 1-meter-diameter Optical Ground Stations (OGS), originally designed for classical laser communication with satellites, as a receiver for the single photons. In a first experiment, entangled photon-pairs were generated in La Palma via spontaneous parametric down-conversion (SPDC) in a non-linear crystal. The polarization of one photon of a pair was analyzed next to the source, while the other photon was measured in Tenerife after it travelled through the 144 km free-space channel. The observed quantum correlations resulted in a clear violation of the Bell inequality, clearly proofing the conservation of entanglement between particles separated by 144 km [12].

In a consecutive experiment, the development of a new type of SPDC source allowed to transmit both photons of the entangled pair through the free-space quantum channel to the OGS in Tenerife. There they were split up and analyzed in their polarization. Again, quantum entanglement could be observed by violating a Bell inequality, thereby proofing the ability to deal with attenuations in the quantum channels as are expected for a double-downlink scenario from a LEO satellite to two separate ground stations, i.e. ≈ 70 dB [13].

A third experiment employing the 144 km free-space link between La Palma and Tenerife investigated a test of Bell's inequality with the two observing stations being space-like separated. This required carefully arranging the experimental equipment in order to ensure that the measured quantum correlations cannot result from some, possibly unknown, communication between the observing stations, which is only limited by the speed of light [14].

C. *Entanglement based QKD*

A modification of the single-photon detection modules used for the long-distance Bell experiments described in the previous chapter additionally allowed performing entanglement based QKD. The distinct experimental settings within these experiments resulted in different total two photon loss. Summing up, unconditional secure quantum cryptographic keys could be generated at two-photon attenuations of 30 dB, 58 dB and 71 dB at a rate of 2.4 bits/s, 0.6 bits/s and 0.02 bits/s, respectively.

D. *Weak-coherent pulse QKD*

An experimental implementation of the QKD protocol with weak coherent laser pulses between the Canary islands La Palma and Tenerife was performed in 2007 also via the free-space link between La Palma and Tenerife over 144 km. The optics of the QKD transmitter (Alice) consisted of four laser diodes, whose linear polarization orientation was rotated by 45° relative to the neighboring ones. According to random bit values, one of them emitted a weak optical pulse (see [15]), thereby implementing the four different polarization states.

In this experiment a Bennett-Brassard 1984 [6] QKD protocol type was implemented whereby the security was ensured by employing decoy-state analysis [16]. Finally, an unconditional secure key rate of 12.8 bits/s could be achieved at an attenuation of approximately 35 dB.

IV. Conclusion

The space environment will allow performing quantum physics experiment with entangled photon pairs and single photons over ultra-long distances. The Space-QUEST proposal aims at performing fundamental physics experiments, investigating the limits of the validity of quantum mechanics, as well as demonstrating telecom applications based on quantum physics on a global scale, by placing a quantum communication transceiver onto the ISS. Hence, this system will allow in particular for a test of quantum entanglement over a distance exceeding 1000 km, which is impossible on ground.

We provided an overview over the proposed experiments and we have summarized their experimental proof-of-concept demonstrations, which have been performed on a terrestrial 144 km free-space path between the Canary Islands of La Palma and Tenerife. The described experiments represent a crucial step towards future quantum networks in space since the atmospheric distance to be overcome between space and ground is certainly shorter than the distance between La Palma and Tenerife. In particular, the results proof the ability of state-of-the-art quantum communication technology to deal with experimental conditions as are expected for space-to-ground links from a LEO satellite, since therefore the total two-photon attenuation is predicted with 30 dB for a single downlink and with 60 dB for a double downlink scenario.

References

[1] D. Bouwmeester, A. Ekert, A. Zeilinger, The Physics of Quantum Information, Springer, Berlin, 2000.

[2] N. Gisin *et al.*, Quantum cryptography, Rev.Mod. Phys. 74(1), 145 (2002).

[3] Z. L. Yuan *et al.*, Practical gigahertz quantum key distribution based on avalanche photodiodes, New J. Phys. 11, 045019 (2009).

[4] J. S. Bell, Speakable and Unspeakable in Quantum Mechanics, Cambridge Univ Press, Cambridge, UK, Rev Ed, pp 243–244, 2004.

[5] M. Aspelmeyer, et al., Quantum communications in space: final report, ESA Contract 16358/02/NL/SFe, 2003.

[6] C. H.Bennett and G. Brassard, Quantum cryptography, Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing. Bangalore, India, New York: IEEE: 175, 1984.

[7] R. G. Gallager, Low-density parity-check codes, IRE Transactions on Information Theory, IT-8, pp 21–28, 1962.

[8] C. H. Bennett, G. Brassard and J. M. Robert, Privacy amplification by public discussion, SIAM J. Comput 17, pp 210–229, 1988.

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

[10] M. Pfennigbauer *et al.*, Satellite-based quantum communication terminal employing state-of-the-art technology, J. Opt. Netw. 4(9), 549 (2005).

[11] P. Villoresi *et al.*, Experimental verification of the feasibility of a quantum channel between space and Earth, New J. Phys. 10, 033038 (2008).

[12] R. Ursin *et al.*, Entanglement based quantum communication over 144 km, Nature Physics 3, 481 (2007).

[13] A. Fedrizzi *et al.*, High-fidelity transmission of entanglement over a high-loss freespace channel, Nature Physics 5, 389 - 392 (2009).

[14] T. Scheidl *et al.*, Violation of local realism with freedom of choice, Proc Natl Acad Sci USA, 19709 – 19713 (2010).

[15] T. Schmitt-Manderbach *et al.*, Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km, Phys. Rev. Lett. 98, 010504 (2007).

[16] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. 91, 057901 (2003);