Quantum Information and Quantum Physics in Space: Experimental Evaluation ("QIPS")

Executive Summary

H. Weinfurter, T. Schmitt-Manderbach, H. Weier, M. Fürst, P. Trojek
Max-Planck Institute for Quantum Optics, Garching, Germany

A. Zeilinger, M. Aspelmeyer, R. Ursin, Th. Jennewein, F. Tiefenbacher, Th. Scheidl, A. Fedrizzi
IQOQI, Austrian Academy of Sciences and University of Vienna, Austria

J. Rarity, D. Benton, P. Gorman, D. Taylor, P. Tapster
University of Bristo and QinetiQ, United Kingdom

C. Barbieri, F. Tamburini, P. Villoresi, I. Capraro, T. Occhipinti, G. Bianco
University of Padova, Italy

F. Heine
TESAT Spacecom, Germany

G. Baister
Contraves Space/Oerlikon, Zürich, Switzerland

G. P. Guizzo
Carlo Gavazzi Space, Italy

Prepared for the European Space Agency under ESTEC/Contract No.18805/04/NL/HE
Contractor: Max-Planck-Institute for Quantum Optics, Garching, Germany
October 31st, 2007

Max Planck Institute
for Quantum Optics
(D)

CARLO-GAVAZZI SPACE
(I)

CONTRAVES SPACE
(CH)

IQOQI
Austrian Academy of
Sciences (A)

QinetiQ
University of Bristol
(UK)

TESAT
(D)

University of Padua
(I)

ESA STUDY CONTRACT REPORT

<table>
<tr><td>ESA Contract No:
18805/04/NL/HE</td><td colspan="2">Subject:
QUANTUM INFORMATION AND QUANTUM PHYSICS IN SPACE: EXPERIMENTAL EVALUATION</td><td>Contractor:
Max-Planck-Institute for Quantum Optics
Garching, Germany</td></tr>
<tr><td>*ESA CR() No</td><td>* STAR CODE</td><td>No of Volumes: 1
This is volume No 1</td><td>Contractor's Reference
QIPS</td></tr>
</table>

ABSTRACT:

Space links offer an ideal solution for global Quantum Communication, e.g. for secure key exchange. At the same time, the space environment enables fundamental tests of quantum phenomena, in particular quantum non-locality.

Within the first part of this study, the detailed designs of mid-term and long-term experiments for the demonstration of Quantum Communications applications as well as fundamental principles of Quantum Physics have been further investigated, both from the scientific impact point of view, and in terms of the technical feasibility of the required space infrastructure.

In the second part of the study, a multi-purpose ground-based proof-of-concept experiment was defined and its detailed design was carried out. Its flexible and modular design of the demonstrator ensured compatibility with the testing of several phenomena (single photon channel, testing of atmospheric effects, entanglement distribution). Using this demonstrator, we performed basic ground-to-ground Quantum Communications experiments, that are representative of the needs of space systems in order to identify and evaluate the main limitations of future space-to-ground (or fully space-based) experiments. These experiments established single photon links between the Canary islands of La Palma and Tenerife over a distance of 144 km. Utilising schemes with an entangled photon source and attenuated laser pulses, we demonstrated secure key exchange at optical attenuation values expected for a downlink from a low earth orbit (LEO) satellite. We also demonstrated that the Optical Ground Station (OGS) on Tenerife, developed for standard optical communication to and from satellites, can be adapted for the use in quantum communication protocols.

The results thus clearly demonstrate the feasibility of satellite-based quantum key distribution. On the way towards a quantum communication experiment in space, further developments of components and technologies are required. We identified associated critical areas and proposed future activities for the development of a space-based quantum communication terminal.

The work described in this report was done under ESA contract. Responsibility for the contents resides in the author organisation that prepared it.

Names of authors:

H. Weinfurter, T. Schmitt-Manderbach, H. Weier, M. Fürst, P. Trojek, A. Zeilinger,
M. Aspelmeyer, R. Ursin, Th. Jennewein, F. Tiefenbacher, Th. Scheidl, A. Fedrizzi,
J. Rarity, D. Benton, P. Gorman, D. Taylor, P. Tapster, C. Barbieri, F. Tamburini,
P. Villoresi, I. Capraro, T. Occhipinti, G. Bianco, F. Heine, G. Baister, G. P. Guizzo

** Name of ESA Study Manager: **Josep Maria Perdigués Armengol** Div: **MMO** Directorate: **TEC**	** ESA Budget Handling: G/1/100.060/600.5100/GE+/RD100/04N56

Contents

1. Introduction 4
2. Objectives and Overview 5
3. Preliminary design of a mid-term exeriment.. 5
4. Long-term experiment.. 9
5. Long-distance ground-to-ground demonstration.. 12
6. Conclusions 17
7. References 18

1. Introduction

Quantum mechanics lies at the heart of modern physics. The characteristic and very fundamental effects of quantum physics now found application in the emerging field of quantum information. The superposition principle, Heisenberg's uncertainty relation, the inherent randomness in quantum physics and last but not least the principle of entanglement enable secure and highly efficient classical communication, the transfer of quantum information via quantum teleportation and the formulation of novel, powerful quantum algorithms that completely outperform their classical counterparts. Both, the understanding of quantum physics, as well as the applicability of novel quantum communication methods can significantly benefit if experiments and developments are carried into space.

Quantum Key Distribution

Whenever sensitive information has to be exchanged between two parties, cryptography is employed to ensure that no unauthorized third party can get access to the content. Classical cryptographic methods like the one-time pad have been shown to be provably secure, if and only if the key has been deployed securely. Yet, this task cannot be provably accomplished by classical means. Quantum cryptography, also known as quantum key distribution (QKD), makes use of fundamental principles of quantum mechanics to ensure the security of secret key generation [1]. The most crucial parameters for practical applications are system cost and maximum distance over which a secure key can be established. Distance is mainly limited by the noise of the detectors and the overall link efficiency of the quantum channel and the detection system. For fiber based systems, loss through the channel is low, however, the low detection efficiency and high noise of single photon detectors for telecom wavelengths limit the maximum distance to about 100-200 km [2]. In principle, one can concatenate shorter links, ideally by quantum repeaters [3]. As these devices are still beyond state-of-the-art technology, a network of trusted nodes might serve for the time being [4]. Complementary to such fiber based networks, free space quantum channels can be used for various different purposes. Authentication to money machines is one example, where link distances on the order of 1 m are already of significant benefit [5]. Another application arises with link distances of up to 5 km. Such cost efficient systems could serve as the "last-mile" connection between the provider network and the customer [6]. Ultimately, a free-space link from a low-earth-orbit (LEO) satellite to a ground station could be established [7, 8]. By exchanging quantum keys between the satellite and different ground stations consecutively, one can easily generate a secret key between any two ground stations worldwide. These ground stations could again be integrated in fiber based networks, thereby enabling truly global, secure quantum key distribution.

Fundamental Quantum Physics

In addition to enabling global quantum key distribution, the space infrastructure allows for fundamental tests of quantum theory far beyond the capabilities of earth-bound laboratories. The most genuine quantum physical property is entanglement [9], which is not only the origin of various nonclassical interference phenomena but also the key to most quantum communication schemes such as quantum state teleportation or quantum dense coding [10]. These schemes could change our way of processing and communicating information completely. Depending on their preparation, entangled states imply nonclassical phenomena such as Greenberger-Horne-Zeilinger-correlations or correlations violating Bell's inequality [11, 12]. Testing the violation of Bell's inequality in a Bell experiment is one of the most fundamental experiments for quantum physics. Specifically, in a space scenario, quantum entanglement can be established and studied in a Bell-experiment over distances not possible on Earth. In the long run, the influence of gravitation and relativistic effects on quantum physics, albeit minor, might be accessible in a space-based large-scale experiment using quantum entanglement for further fundamental tests [13,14].

2. Objectives and Overview

Before installing satellites with a dedicated payload, the feasibility of quantum communication over comparably long distance has to be proven. Thus, the aim of the QIPS project was to explore quantum phenomena and to demonstrate quantum communication over long distances in a ground-to-ground experiment.

Based on the current state-of-the-art, and building on the findings from previous studies [13,15], the first part of the QIPS study (TN1, TN2) reviews the objectives of possible mid-term and long-term experiments and gives a preliminary design of the required space and ground infrastructure.

In the second, experimental part (TN3-TN5), we designed and tested a proof-of-concept demonstrator for establishing single photon links over a distance of 144 km between the Canary Islands of La Palma and Tenerife to evaluate main limitations for future space experiments. The goal of the demonstration was to further optimize hardware but also to implement new protocols to reach sufficient key rates even in the presence of low link efficiency.

3. Preliminary design of a mid-term exeriment

The mid-term experiment shall be performed with one spacecraft and various (at least two) ground stations. The quantum communication terminal could be either placed on the Columbus external payload facility of the ISS or as a payload on a LEO-satellite. The low orbit is recommended to maximize the link rate with the ground station. The mid-term experiment design enables:

- demonstration of faint pulse QKD between spacecraft and one ground station at a time
- demonstration of single photon QKD between spacecraft and one ground station
- trusted satellite global key distribution
- demonstration of entanglement based QKD using the spacecraft and two ground stations
- Bell experiment over ~1000 km with 2 observers (2 ground stations)

Since space-to-ground links compared to ground-to-space links suffer less from increased beam spreading due to atmospheric turbulence, it is favorable to place the transmitter on the spacecraft and accommodate the receiver in the ground station.

The transmitter terminal consists of infrastructure for standard optical links (including classical optical pointing, acquisition, and tracking (PAT) systems and telescopes for the establishment of the downlink) and a quantum optical terminal. The latter comprises a source of faint laser pulses, the entangled photon source, and modules for polarisation-sensitive manipulation and measurement of single photons. To distribute entangled photon pairs for the entanglement based QKD and for the Bell experiment, two independent telescope units are required. All of the photons of the quantum sources are coupled into optical fibres which are subject to a polarisation control via piezomechanical bending of the fibres. Coupling to the classical optical head is then achieved via a fibre coupler. In order to be able to perform single photon QKD, the entangled pair photons can either be redirected to the polarisation analyzer or to the optical head units for transmission to earth.

The reference laser of the PAT subsystem is linearly polarized and optionally pulsed to provide both an orientational and a timing refence frame between transmitter and receiver site. Also, the entangled photon source subsystem comprises additional laser diodes for fast alignment of the optical fibres. A functional block diagram for quantum optical and classical optical components is shown in Figure 1, the preliminary design of the Quantum Communication Payload. is presented in Figure 2.

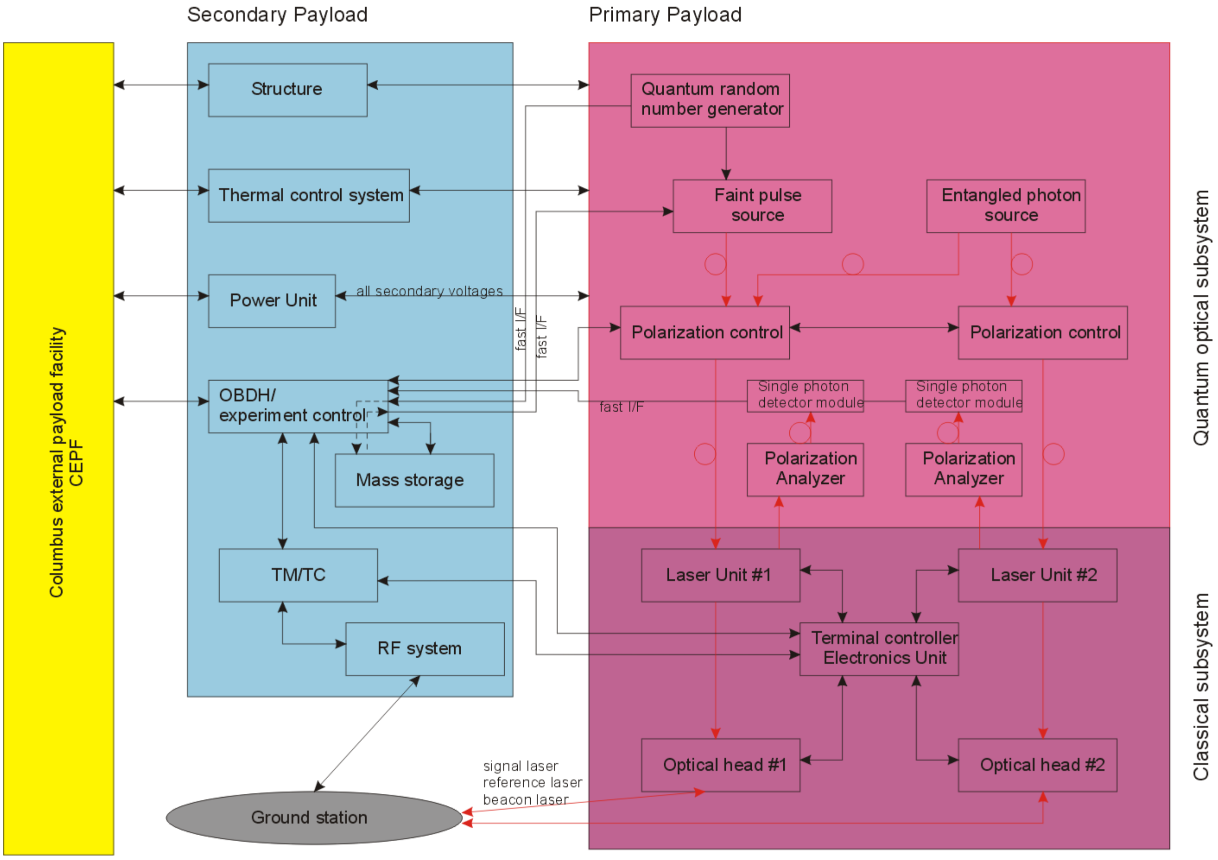

Figure 1 The transmitter module of a possible mid-term mission comprises two different photon sources, which can be alternatively used for quantum key distribution (faint laser-pulse source and entangled photons source) and fundamental quantum physics experiments (entangled photon pair source). The photons can be redirected either to a module for polarisation analysis or to the telescopes pointing nadir to one or two ground stations. Two separate telescopes with independent Pointing-Acquisition-Tracking modules are used, since in the main experiment (test of Bell’s inequality and entanglement-based QKD), entangled photon pairs are created and distributed to separate experimental stations.

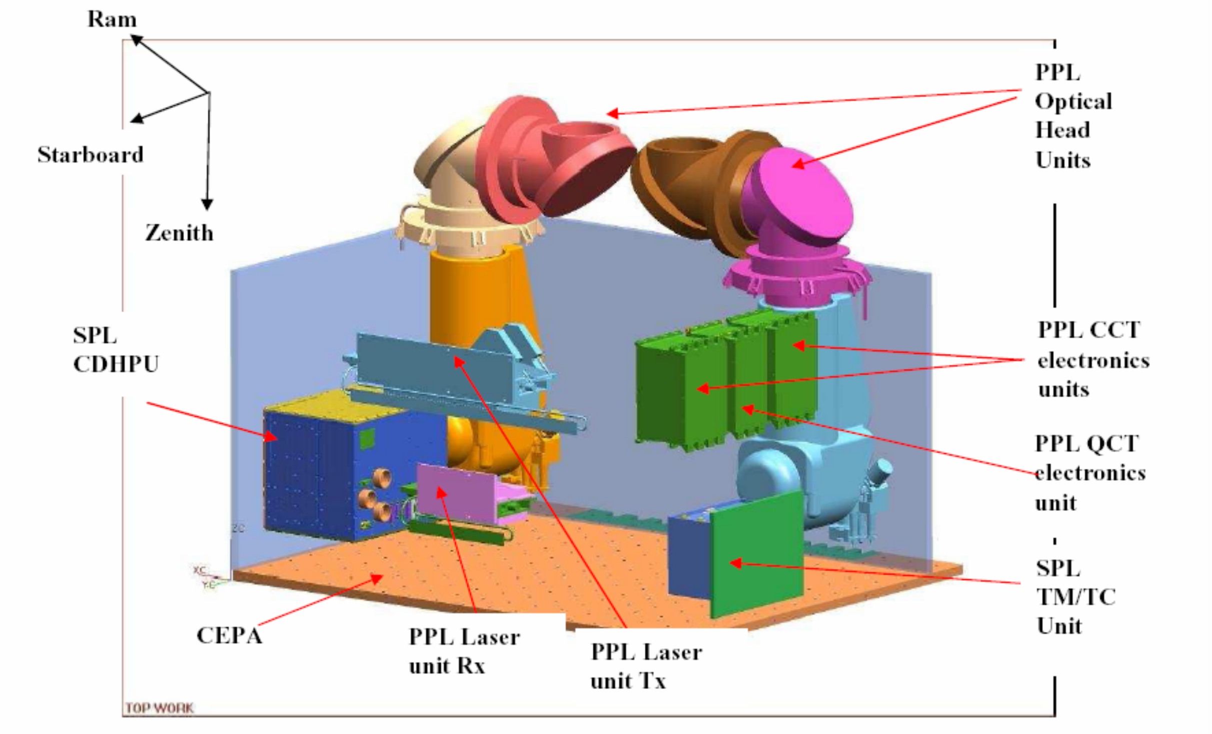

Figure 2 Preliminary architecture and accomodation of Quantum Communication Terminal on the Columbus External Payload Assembly (3D view without structure).

Table 1 and Table 2 summarize the estimated mass and power consumption budgets of the preliminary design, taking into account a safety margin of 20%.

	No. operating	**Power consumption**
Optical Head Unit	2	80.4 W
Laser Unit – Tx	1	42.2 W
Laser Unit - Rx	1	12.0 W
CCT Electronics	2	37.4 W
QCT Electronics	1	10.0 W
Inter-Unit Harnesses		-
Secondary payload		114 W
TOTAL		**296 W**

Table 1: Power consumption budget (with 20% margin)**.**

	No. required	**Total mass**
Optical Head Unit	2	54.1 kg
Laser Unit – Tx	1	4.8 kg
Laser Unit – Rx	1	2.1 kg
CCT Electronics	2	8.4 kg
QCT Electronics	1	3.0 kg
Inter-Unit Harnesses		7.9 kg
Secondary Payload		57.9 kg
TOTAL		**138.2 kg**

Table 2: Mass budget (with 20% margin)

The quantum communication terminal could either be placed on the Columbus external payload facility of the ISS or as a payload on a LEO-satellite. Initially, this study was confined to the design for an ISS external payload, but due to the changes in the schedules of the space-shuttle project and its implications for the the planned installation of the Columbus-module it can be hardly foreseen when such an experiment could be performed. Therefore, options to perform the experiments (or a subset thereof) at other free-flying platforms were studied. The platforms considered are based on what is commercially available today to avoid a dedicated platform development for the QIPS payload which would add significant development costs to the QIPS/SpaceQuest programme.

Table summarizes the payload capabilities of the free-flying platforms that have been identified as an alternative to be considered to the ISS flight opportunity.

Platform	Payload Mass Capability	Payload Power Capability	Platform Dimensions	Memory Available (Typical)
SSTL-300	70	200 W	70 cm x 70 cm x 70 cm	16 Gbytes
SSTL-900	250	700 W	130 cm x 130 cm x 130 cm	Not Known
PROBA	60	200 W	80 cm x 60 cm x 60 cm	1 Gbyte
MITA	100	200 W	TBD	2 Gbytes
Resurs-DK1	470	360 W	TBD	20 Gbytes
Myriade	80	100 W	80 cm x 80 cm x 80 cm	2 Gbytes
Proteus	275	300 W	80 cm x 160 cm x 80 cm	0.5 Gbyte

Table 3: Summary of the Micro-/ Small Satellite Platforms Considered as an Alternative to the ISS

The envisaged experiments use optical ground station telescopes for efficiently collecting the light emitted by the quantum communication module onboard ISS or a LEO satellite. In order to achieve a high link rate and maximum link time, the ground stations should be equipped with a high aperture telescope (typically 1m diameter) and tracking capabilities. A number of geodetic and astronomical telescopes were examined with respect to their suitability (link availability, tracking capability, telescope aperture >1 m, access to RF communications) for a mid-term experiment, and necessary modifications (such as upgrade of tracking subsystems and mirror coatings) of the most adequate were discussed.

Name	**Longitude (deg)**	**Latitude (deg)**	**Elevation (m)**	**Diameter (m)**	**Coudeè focus**	**Nasmyth focus**
LRT	-17.87919	+28.76254	2344	2.0	N	Y
Mercator	- 17.87833	+ 28.762222	2333	1.2	N	Y
JKT	-17.87811	+28.770806	2362	1.2	N	N
OGS	-16.51172	+28.30086	2410	1.0	Y	N
Calar Alto	- 2.54625	+37.22360	2168	3.5, 2.2, 1.5, 1.2	Y,Y,(Y),N	Y,Y,Y,Y
Asiago - Ekar	+11.56889	+45.84862	1340	1.8	(Y)	Y
Etna	+14.97333	+37.69167	1735	0.9, 0.8	N,N	N,N
Toppo	+15.46278	+ 40.80000	1250	1.5	N	Y
Matera	+16.70500	+40.68433	530	1.5	Y	Y
Lubljana				0.7	N	N
TAM	+20.61	+ 38.17	1040	0.6	N	N
Chelmos	+ 22.2167	+ 37.9833	2340	2.3	N	N
Kryonery	+ 22.61667	+37.96667	930	1.2	N	N
Skinakas	+24.89917	+35.21194	1750	1.3	N	N

Table 4: Table of Astronomical Telescopes in Southern Europe (in order of increasing longitudes)

4. Long-term experiment

Technical Note 2 ("Preliminary design of long-term experiments") identifies and investigates experiments for the demonstration of fundamental principles of quantum physics, which make advantageous use of the space infrastructure on a long-term scale. Special consideration is given to conceive and define the technologies needed to perform these long-term experiments.

From the experimental parameters and conditions found for the range of proposed long-term visions, three scenarios are selected as the most interesting candidates:

- Bell-experiment over one light second distance, involving human observers (**"Free-will Bell experiment"**). The source for entangled photons must be located symmetrically between the two observers. One possible experiment could involve two observers located at the distance Moon to Earth (Figure 3). An even more advanced experiment could make use of a future Mars mission, where a manned Space-craft will travel a very distance away from earth.
- **Satellite flotilla experiments**. In order to perform true world wide quantum communication, entanglement swapping and teleportation protocols via relay satellites are mandatory. One possible way would be to place two entangled photon sources onboard of two satellites (source terminal), see Figure 4. One photon of each entangled pair has to be sent to the swapping terminal preferably in a GEO orbit in order to be visible to the source terminals all the time. After the two photons are overlapped in the swapping terminal, the respective partners are entangled at the end and can be used in any quantum communication protocol and interconnection of

quantum computers. This allows performing quantum communication between two locations with very large distances (> 10000 km).

- Bell experiment exploiting the **timing paradox** which arises from the two observers travelling at high speed towards (or away) from the source of entangled photon pairs. With the relative velocities possible with satellites, Bell-type experiments are possible where each observer can claim to measure his system before the observation could have performed on it's respective partner particle. The relative velocity of the two receiver terminal should be on the order of 7,5 km/s. A proposed arrangement of the various source and receiver terminals is shown in Figure 5.

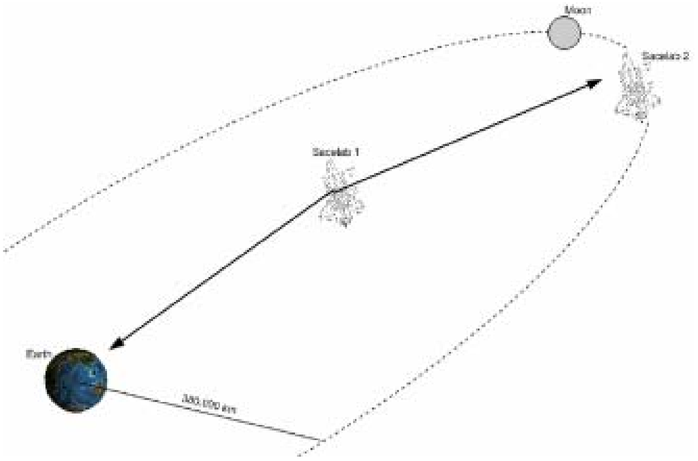

Figure 3 A possible scenario for the "ultimate Bell-Experiment". Two human observers, one located on Earth, the other observer on a Space-ship at a distance corresponding to about 1 light second, e.g. on the Moon. The source of entangled photons is located symmetrically between the two observers, and sends the photons in opposite directions towards the receivers. Both observers randomly choose the settings of their analysers of the photons.

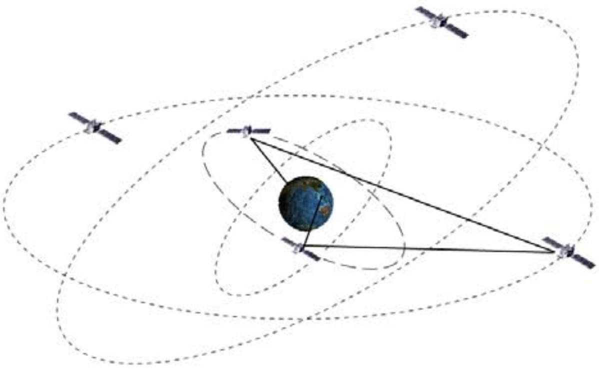

Figure 4 A swapping terminal placed on a platform in GEO receiving two entangled photons from two sources placed in LEO. This allows two photons be distributed to two distant receivers on the Earth. Also, it is possible that one of the photons is sent to a further satellite, e.g., in a LEO orbit.

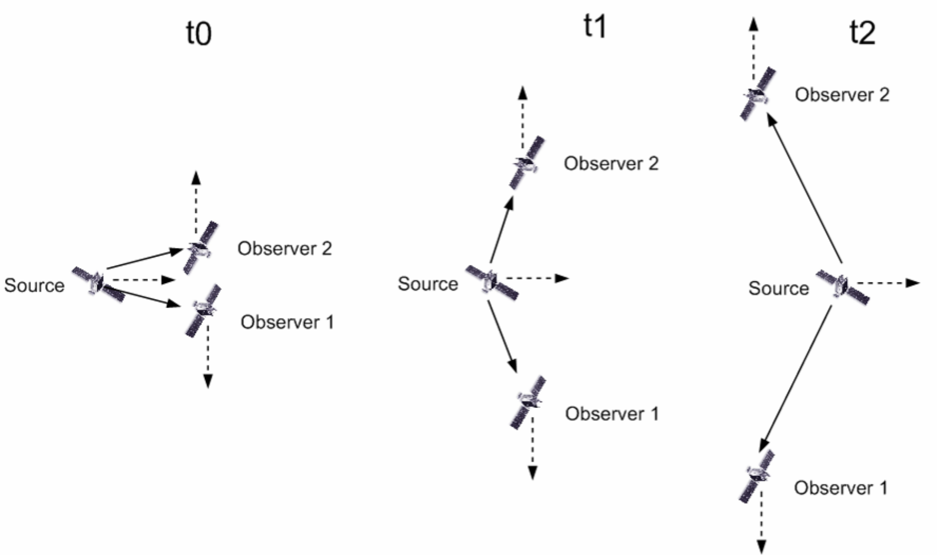

Figure 5 Arrangement of the three satellites to demonstrates the relative timing paradox. The Source is emitting two entangled particles to the two observers (1 and 2) while passing between them. t0, t1 and t2 denote three arbitrary times during the performance of the experiment.

This selection is based on the respective scientific merit and feasibility, taking into account today's technology and foreseeable technological advancements. With respect to fundamental physics, a test of Bell's inequality over astronomic distances is the most important and scientifically most interesting goal for an entanglement-based quantum experiment in space. The selected experiments are clearly not feasible with today's technology. Many of the required key components still require many years of development, and some technologies do even not exist today. Potential development areas include high flux entangled photon sources in the UV, high speed (>10ps) and high efficient (QE>82%) detectors, and large diffraction limited telescopes (>1 m) for space use.

Additionally, the remarkable scientific merit and the technological feasibility for experiments on the wavefunction collaps at a certain distance, gravitational waves, Wheeler's delayed choice experiment, and entanglement-enhanced interferometry were identified and described.

5. Long-distance ground-to-ground demonstration

Before installing satellites for quantum cryptography, or even embarking on more ambitious quantum communication schemes, the feasibility of secure communication over comparably long distance has to be proven. The goal of the ground-to-ground demonstration performed here was thus to further optimize hardware but also to implement new protocols to reach sufficient key rate even in the presence of low link efficiency.

General Setup

Starting from previous experiments [16,17] we adopted technology for quantum communication with the requirements of long distance free space communication. In particular, the implementation of tracking systems enabled the establishment of an optical link between the Canary Islands of La Palma and Tenerife.

The typical setup consisted either of the transmitter module emitting attenuated, randomly polarized light pulses or of various sources of polarization entangled photon pairs. One of the generated photons were sent through single mode optical fibre into a transmitter telescope (shown in Figure 6). The beam was guided via a 150 mm diameter lens with 400 mm focal length (f/2.7) matching the divergence of the optical fibre over the 144 km long free-space link to the receiver in the Optical Ground Station (OGS) on Tenerife [18]. Both the sender and the receiver station were situated at an altitude of about 2400 m above sea level, i.e., usually above the cloud level.

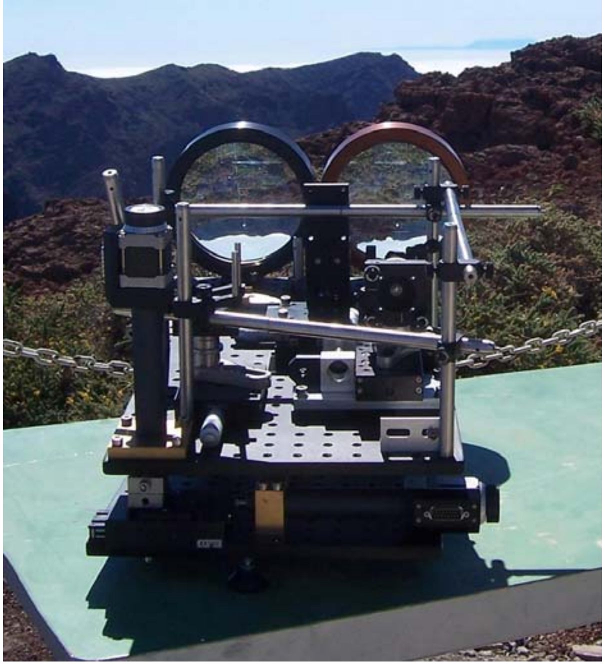

Figure 6. The transmitting telescope on La Palma. The 15 cm front lens on the right is used for sending the single photon beam to the receiver, the identical lens on the left collects the light of the beacon laser, focusing it onto a CCD camera to perform the tracking.

Due to various atmospheric influences such as drifts in the atmospheric layering and the temperature and humidity gradients, the apparent bearing of the receiver station varied on timescales of tens of seconds to minutes (see Figure 7). Most classical optical communication channels prevent the beam from drifting off the receiver aperture by defocusing the beam. This is not an option in single photon experiments, where maintaining the maximum link efficiency is essential. Hence in our experiment the alignment of the transmitter and the receiver telescope was controlled automatically by a closed-loop tracking system employing 532 nm beacon lasers shining from the OGS to the single photon transmitter and in opposite directions. Beam drifts were compensated by permanently readjusting the pointing direction of the telescopes. With tracking enabled we maintained a stable link efficiency of typically 30 dB (measured at 808 nm wavelength), whereas the transmitted power decreased dramatically within minutes when the tracking system was switched off (Figure 7). The observed link attenuation was predominantly due to turbulence induced beam spreading beyond the diffraction limit in vacuum (the effective beam diameters at the OGS varied between 3.6 m and 20 m depending on weather conditions), and atmospheric absorption and scattering effects.

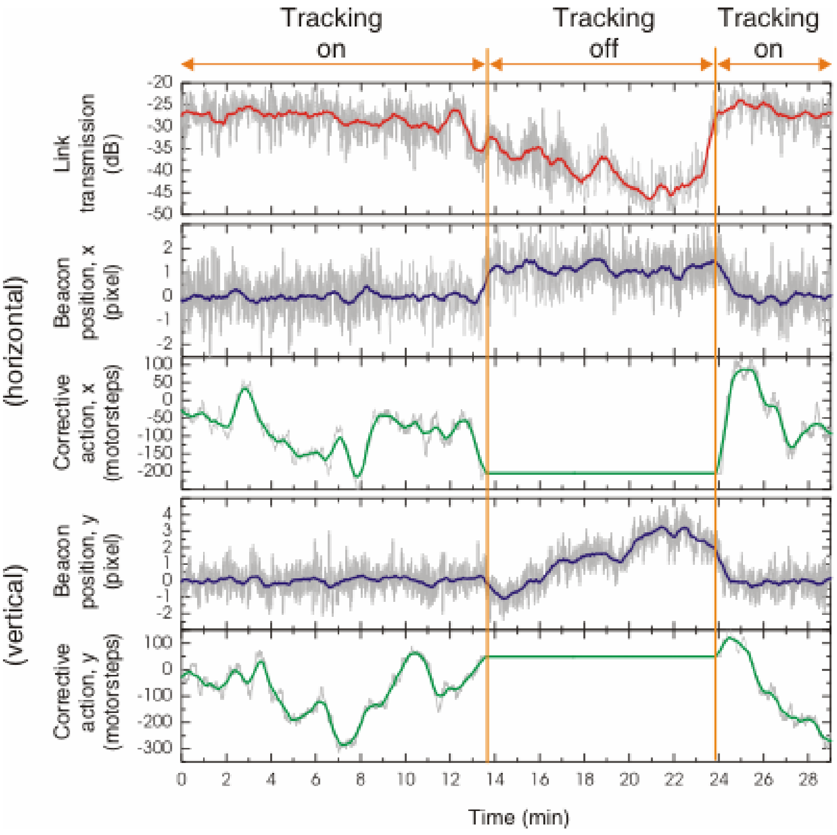

Figure 7. Link attenuation and motor movement (horizontal and vertical direction) of the transmitter telescope's tracking system to compensate for slow beam wander caused by atmospheric effects.

ESA's OGS on Tenerife, a 1 m Richey-Chrétien/Coudé telescope with an effective focal length of 39 m (f/39), was used to collect the transmitted photons with a field-of-view of 8 arcsec. The atmospheric turbulence caused significant beam wander in the focal plane of the telescope of up to 3 mm in the worst case. Analyzing this beam wander by taking time averaged images on a CCD camera we obtained a Fried parameter [19] of r_0 ~ 1…6 cm, depending on the respective weather conditions. r_0 is the aperture which has the "same resolution" as a diffraction-limited aperture in the absence of turbulence. Apart from slow beam wander the turbulences caused an angular beam spread between 13 µR and 73 µR (1/e2 radii) and thus an effective beam diameter at the OGS of 3.6 – 20 m. In the diffraction limited case, the transmitter telescope would produce a beam of 1.5 m in diameter. The employed bidirectional beam tracking reduced the effect of slow beam wander and other drifts on time scales longer than 1 s and thus guaranteed a stable link over hours with a typical link efficiency of 26...30 dB. To prevent the beam from wandering off the detectors we recollimated with an additional f = 400 mm lens to pass through the polarisation analyser and a 10 nm (FWHM) filter.

Decoy-state QKD with attenuated laser pulses

The first QKD scheme demonstrated here employs the so-called BB84 protocol [1], and encodes qubits in the polarization of faint laser pulses. Ideally, one party (Alice) prepares a sequence of single photons, their polarizations being chosen randomly from four possible non-orthogonal states (e.g. horizontal, vertical and ±45◦). She sends the photons to the second party (Bob), who analyses the polarization of each detected photon in a randomly and independently chosen basis (e.g. either H/V or ±45◦). Afterwards both parties publicly compare their basis choices and discard those events where they had used different bases. This process is called key sifting. Due to fundamental laws of quantum mechanics, an eavesdropper (Eve) cannot determine the polarization of a single photon if the polarization states emitted are non-orthogonal. Even worse, she will introduce errors for the receiver's polarization 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. Since single photons are available only with significant technical effort and currently only with low rates, strongly attenuated pulses are used here. Yet, the Poissonian photon statistics enables attacks, which are not revealed by the error analysis described above. For this purpose, we employed the novel decoy state method, where pulses with different attenuation are used [20]. Typical values of $\mu1=0.3$ and $\mu2=0.4$ for the pulse attenuation ensure the necessary non-orthogonality of the states to protect against attacks on the photon number degree of freedom. This renders the attenuated pulse encoding similarly efficient as single photon schemes and enables secure key distribution also over very long links.

A schematic layout of the experimental setup on the Canary Islands is shown in Figure 8. Attenuated light pulses prepared in one out of four polarization directions were generated on La Palma in the sender head fitted with eight laser diodes for the respective polarization and beam brightness (λ=850 nm).

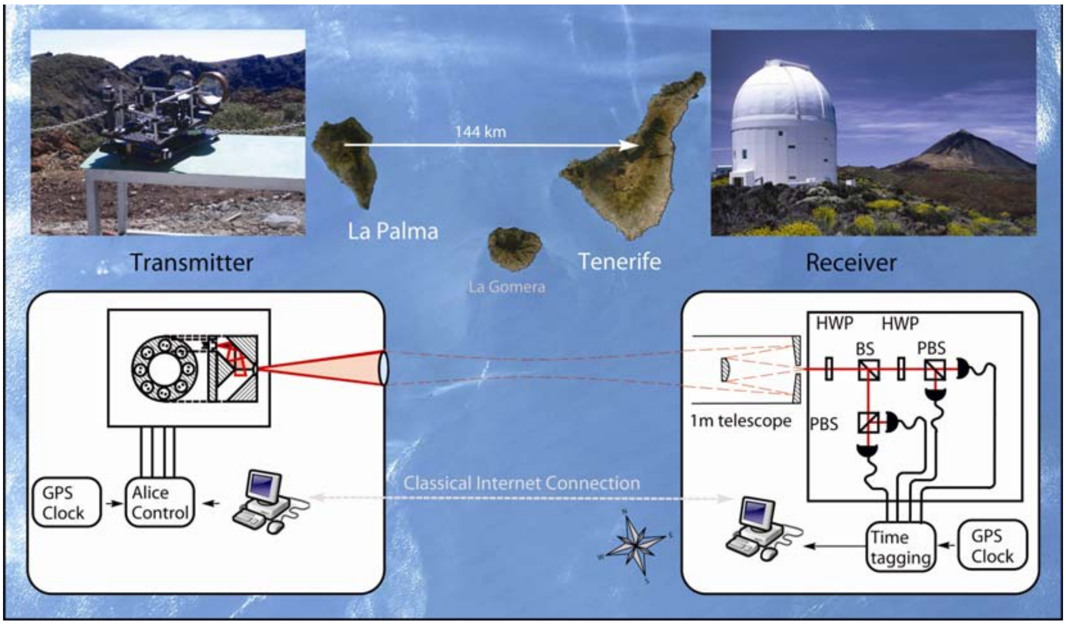

Figure 8: Layout of the decoy state quantum cryptography demonstration.

Under excellent atmospheric conditions we observed an optical link efficiency of -28 dB, measured between the transmitter and the OGS Coude focus, and an additional reduction of about 6dB due to loss in the analyzer optics and the limited single photon detection efficiency. The detectors' electric output pulses were fed into a GPS-disciplined time-stamp unit, determining the detection time and which of the detectors had clicked for each photo-event. These data were then transferred via a digital I/O card to a PC for further processing. For the sifting process, each photo-event 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 between Alice' and Bob's computer, which where connected by standard ethernet, to better than 2 ns. The recent version of decoy-state encoding with four laser diodes [21] was upgraded to eight diodes enabling independent creation of the required attenuations (Figure 9). For a typical measurement run of 17 min we obtained 1530000 events selected after synchronization and thereof n_{sif} = 745 kbit of sifted key. During the error correction we deduced a QBER=2.57% and had to disclose a total of 19.5 %. After decoy state analysis and privacy amplification this results in a key rate of 231 bit/s. This reduction of the key takes into account final statistics of the analysis and also the knowledge of an eavesdropper acquired by a beam-splitting attack, which is not revealed by the decoy analysis. This knowledge is the maximum which still can be gained due to the Poissonian statistics, but, since it only weakly depends on the link efficiency, the final key rate is only little below the one obtainable with single photons.

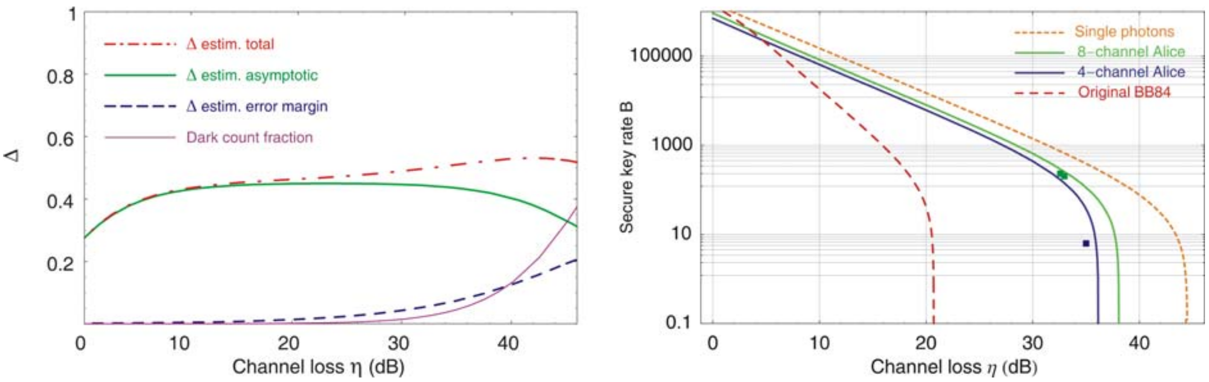

Figure 9: (left) Decoy state analysis indicating flat dependence of the maximum knowledge of the eavesdropper on the link efficiency. (right) Comparison between QKD with different protocols for the typical distance, attenuation, etc., of this experiment. Regular QKD would not produce any key for the link. The rate from the decoy protocol is lower compared to ideal single photon protocol by a constant factor only, and can thus be used for secure QKD over lossy channels.

Distribtution of entanglement and Bell experiment

An alternate scheme for QKD employs entangled photon pairs to achieve provable secure communication. There the nonclassical correlations between the mearuement results of such a pair enable the generation of the distributed key in a similar manner as with the regular BB84 scheme. The security of the key exchange is tested either by evaluating a Bell-inequality or by comparing randomly selected test bits. The very advantage of this method is that no assumptions are necessary anymore about, first, the randomness of the basis choice and, second, about the possibility of the eavesdropper sneaking in on attenuated pulses containing more than one photon. Provided one photon is detected by one of the observers, time gating ensures that the radiation reaching the second observer is a good approximation to a single photon. Moreover, the system is fully passive, no random numbers have to be created for the protocol, since it is only quantum physics where the randomness comes from.

A schematic layout of the experimental setup is shown in Figure 10. Polarization entangled photon pairs were generated on La Palma using a picosecond-pulsed Nd:Vanadate laser emitting light at 355 nm wavelength with an average power of 150 mW. It pumped a β-barium borate crystal in a type-II scheme of spontaneous parametric down conversion (SPDC) [22]. The source produced polarisation entangled photon pairs close to the singlet state. In the singlet state the polarisation measurement results are anti-correlated in any basis. The photons were coupled into single mode optical fibres selecting energy degenerate pairs of entangled photons with a wavelength of 710 nm with a bandwidth of 3 nm. When detecting both photons locally, we were able to observe single count rates of 1 million counts per seconds (Mcps) each, and 145000 coincident events per second. The probability of an emission of a second photon pair per pump pulse was 0.026.

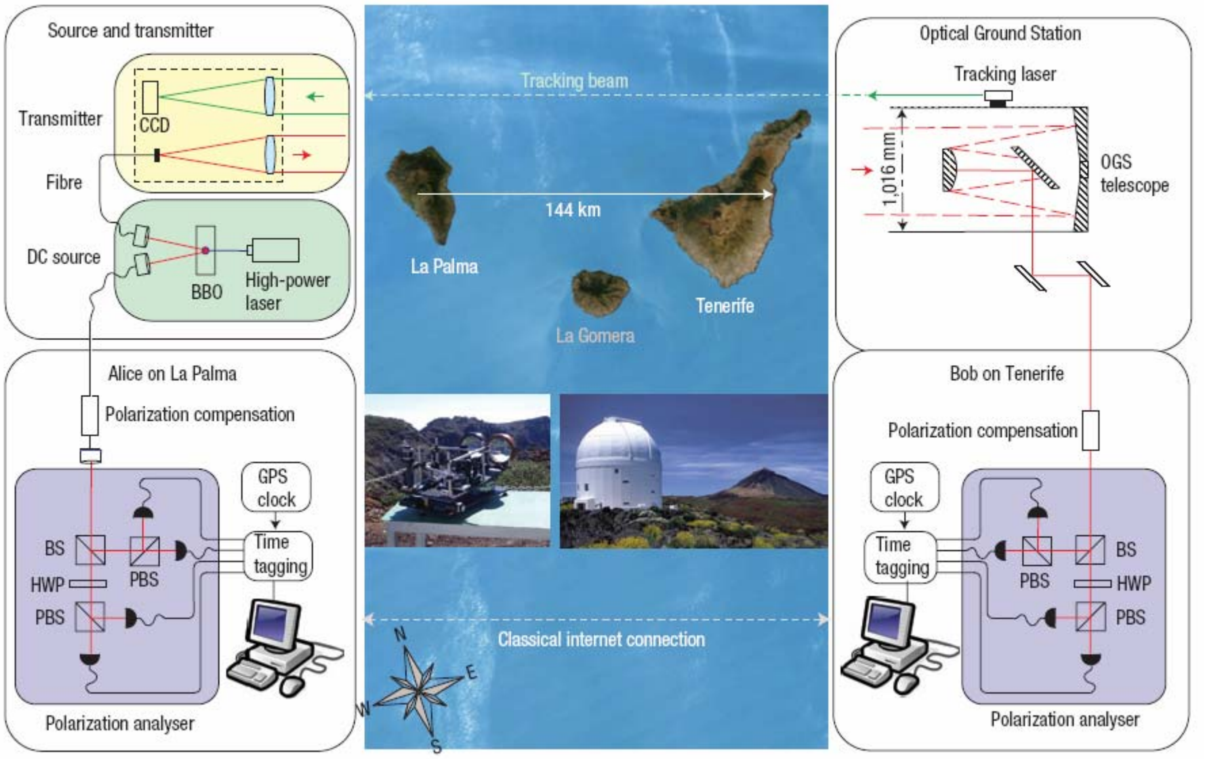

Figure 10: The setup for free-space entanglement distribution between La Palma and Tenerife. Polarisation entangled photon pairs were produced in a type-II parametric down conversion (DC) source by pumping a β-barium-borate crystal (BBO) with a high power UV laser. One photon was measured locally on La Palma, the other one was sent through a 15 cm transmitter lens over the 144 km free-space optical link to the 1 m mirror telescope of the Optical Ground Station (OGS) on the island of Tenerife. Both parties were using four-channel polarisation analysers, consisting of a 50/50 beam-splitter (BS), a half-wave plate (HWP), and two polarising beam-splitters (PBS), which analyzed the polarisation of an incident photon either in the H/V or in the +/-45° basis, randomly split by the BS.

One photon from the entangled pair was measured locally (Alice). The second photon was sent via a single mode fibre to the transmitter telescope, and from there over the optical free-space link to the receiver on Tenerife. From the single photons transmitted at night-time from the source to the OGS we observed 120 cps in each of our four detectors and some 50 cps collected from background photons per detector. Together with the detector dark counts 200 cps per detector, a total count rate of 1500 cps was recorded. Each event in one of Alice's or Bob's detectors was locally labelled with a 64-bit tag, containing the detector channel and a time tag with a timing resolution of 156 ps. The local clocks of the time tagging system were 10 MHz oscillators directly disciplined by the Global Positioning System (GPS) with a relative drift of less than 10^{-11} over 100 s. Furthermore, the 1 Hz GPS synchronization provided a time-reference for Alice's and Bob's time tags and the Network Timing Protocol (NTP) was used to initiate the time-tagging within 500 ms for both parties. Bob sent his time tag data to Alice via the public internet. Alice identified the coincident events by cross-correlating both sets of time tags using software, which determined the offset (~487 µs) and drift of the two timescales. Within a coincidence window of about 1ns the average coincidence count rate was up to 20-40 cps depending on the actual atmospheric conditions.

To demonstrate quantum entanglement between measurement results on La Palma and Tenerife, we experimentally determined the polarization correlation coefficients to test the violation of a Clauser–Horne–Shimony–Holt- (CHSH-) type Bell inequality [23]. Combining our experimental data, we obtained the value of S_{Exp} =2.508±0.037, thereby conclusively proving the presence of entanglement between the photons detected at the Canary Islands La Palma and Tenerife. The counting statistics accumulated within the measurement time of 221s leads to a violation of *S* by 13 standard deviations.

To demonstrate the applicability of our setup for quantum communication, we used the quantum entanglement between our pairs to generate a quantum cryptographic key [1,24]. In the experiment, we aligned the polarisation compensators for maximum singlet anti-correlations in the H/V and +/- bases. These settings yielded 789 coincidences within 75 s. The data set was used for quantum key distribution [25,26] implemented on Alice's and Bob's computers starting from 417 bits of raw key with 20 erroneous bits which corresponds to a QBER 4.8 % ± 1 % explicable by the various imperfections of our experimental setup, e.g., the contribution due to the double pair emission of our entangled photon source. Even so, for the error correction and privacy amplification all errors are attributed to an eavesdropper. We finally distilled a secure key with a length of 178 bits in total.

6. Conclusions

Within our ground-based experiment, we have overcome the attenuation expected for a downlink from a low Earth orbit (LEO) satellite. For example the minimum distance from ISS to OGS is about 400 km, whereas the atmospheric thickness is about one order of magnitude less than in our experiment, thus yielding less attenuation compared to the horizontal link here. We also demonstrated that the OGS, developed for standard optical communication to and from satellites, can be adapted for the use in quantum communication protocols. Such optical ground stations could - when combined with sophisticated automatic pointing and tracking hardware - exchange keys with low earth orbit satellites. If we engineer a satellite to be a secure 'relay' station this has the potential for secure key exchange between any two arbitrary locations on the globe. Our results thus clearly demonstrate the feasibility of satellite-based quantum key distribution, which is the first step to establish a worldwide network for quantum communication.

We have developed a prelimary quantum communication terminal design for a mid-term space experiment, capable of demonstrating several quantum key distribution and quantum communication schemes. On the way towards a quantum communication experiment, further developments of components and technologies are required (e.g., space-qualified pump sources at ~400 nm and single photon detectors, as well as refined tracking). We have identified the associated critical areas and proposed future activities for the development of a space-based quantum communication terminal.

7. References

[1] Bennett, C. H. & Brassard, G. Quantum cryptography: Public Key Distribution and coin-tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 175-179 (1984).

[2] D. Stucki et al., “Quantum key distribution over 67 km with a plug&play system”, New J. Phys. **4**, 41 (2002); E. Waks, A. Zeevi, and Y. Yamamoto, “Security of quantum key distribution with entangled photons against individual attacks”, Phys. Rev. A **65**, 52310 (2002).

[3] H.J. Briegel, et al., „Quantum repeaters: the role of imperfect local operations in quantum communication“, Phys. Rev. Lett. **81**, 5932, (1998).

[4] EU project SECOQC: http://www.secoqc.net

[5] J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro, J. G. Rarity, “Low cost and compact quantum key distribution”, New J. Phys. **8**, 249 (2006).

[6] H.Weier et al., „Free space quantum key distribution: towards a real life application“, Fortschr. Phys. **54**, 840 (2006).

[7] W.T. Buttler et al., “Practical free space quantum key distribution over 1 km”, Phys. Rev. Lett. **81**, 3283 (1998); C. Kurtsiefer et al., “Quantum cryptography: a step towards global quantum key distribution”, Nature **419**, 450 (2002); R. J. Hughes et al., “Practical free-space quantum key distribution over 10 km in daylight and at night”, New J. Phys. **4**, 43 (2002).

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

[9] E. Schrödinger, “Die gegenwärtige Situation in der Quantenmechanik,” *Naturwissenschaften*, **23**, 807–812; 823–828; 844–849 (1935).

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

[11] D. M. Greenberger, M. A. Horne, and A. Zeilinger, *Bell’s Theorem, Quantum Theory, and Conceptions of the Universe*, M. Kafatos, Dordrecht: Kluwer, (1989).

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

[13] M. Aspelmeyer, T. Jennewein, R. Kaltenbaek, M. Lindenthal, H. R. Böhm, J. Petschinka, R. Ursin, C. Brukner, A. Zeilinger, M. Pfennigbauer, and W. Leeb, “Quantum communications in space,” European Space Agency (ESA), contract 16358/02 16358/02, 2003.

[14] R. Kaltenbaek, M. Aspelmeyer, T. Jennewein, C. Brukner, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger, “Proof-of-concept experiments for quantum physics in space,” in *Quantum Communications and Quantum Imaging*, R. Meyers and Y. Shih, Eds., **5161**, 252–268 (2003).

[15] M. Pfennigbauer, W. Leeb, G. Neckamm, M. Aspelmayer, Th. Jennewein, F. Tiefenbacher, A. Zeilinger, G. Baister, K. Kdielka, Th. Dreischer, and H. Weinfurter “Accomodation of a quantum communication transceiver in an optical terminal” European Space Agency (ESA), contract 17766/NL/PM, (2005).

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

[17] K. Resch et al., ‘Distributing entanglement and single photons through an intra-city, free-space quantum channel’, Optics Express **13**, 202-209 (2005)

[18] Czichy, R. et al. SPIE **2381**, 26-37 (1995).

[19] D. L. Fried, „Statistics of a geometric representation of wavefront distortion“, J. Opt. Soc. Am. **55**, 1427 (1965).

[20] 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).

[21] T. Schmitt-Manderbach et al., „Experimental demonstration of free-space decoy-state quantum key distribution“ Phys. Rev. Lett. **98**, 010504 (2007).

[22] Kwiat, P. G. et al. « New High-Intensity Source of Polarization-Entangled Photon Pairs.” Phys. Rev. Lett. **75**, 4337 (1995).

[23] Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. “Proposed Experiment to Test Local Hidden-Variable Theories.” Phys. Rev. Lett. **23**, 880-884 (1969).

[24] Ekert, A. K. Quantum Cryptography Based on Bell's Theorem. Phys. Rev. Lett. **67**, 661-663 (1991).

[25] Jennewein, T. et al. “Quantum Cryptography with Entangled Photons.” Phys. Rev. Lett. **84**, 4729 (2000).

[26] Bennett, C. H., Brassard, G. & Mermin N. D. “Quantum cryptography without Bell's theorem.”, Phys. Rev. Lett. **68**, 557-559 (1992).