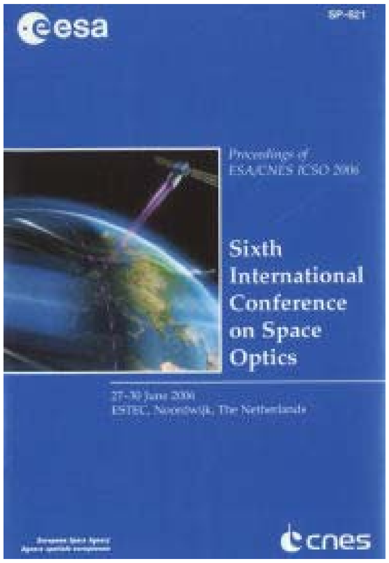
International Conference on Space Optics—ICSO 2006

Noordwijk, Netherlands

27–30 June 2006

Edited by Errico Armandillo, Josiane Costeraste, and Nikos Karafolas



SP-621

Proceedings of
ESA/CNES ICSO 2006

Sixth
International
Conference
on Space
Optics

27–30 June 2006
ESTEC, Noordwijk, The Netherlands

QIPS: quantum information and quantum physics in space

*Tobias Schmitt-Manderbach, Thomas Scheidl, Rupert Ursin,
Felix Tiefenbacher, et al.*

International Conference on Space Optics — ICSO 2006, edited by Errico Armandillo, Josiane Costeraste,
Nikos Karafolas, Proc. of SPIE Vol. 10567, 1056728 · © 2006 ESA and CNES
CCC code: 0277-786X/17/$18 · doi: 10.1117/12.2308067

QIPS – QUANTUM INFORMATION AND QUANTUM PHYSICS IN SPACE

Tobias Schmitt-Manderbach[1]**, Thomas Scheidl**[3,4]**, Rupert Ursin**[3]**, Felix Tiefenbacher**[3,4]**, Henning Weier**[2]**,**
Martin Fürst[2]**, T. Jennewein**[4]**, J. Perdigues**[5]**, Z. Sodnik**[2]**, J. Rarity**[6]**, Anton Zeilinger**[3,4] **,**
and Harald Weinfurter[1,2]

[1] Max-Planck Institut fuer Quantenoptik, Hans-Kopfermannstrasse, D-85748 Garching, Germany
[2] Ludwig-Maximilians-University, Department für Physik, Schellingstr. 4/III, D-80799 München, Germany
[3] Institute for Experimental Physics, University of Vienna, Boltzmanng. 5, A-1090 Vienna, Austria
[4]Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanng. 3, A-1090 Vienna, Austria
[5]European Space Agency, 2200 AG Noordvijk, The Netherlands
[6]Department of Electrical and Electronic Engineering, University of Bristol, Bristol, BS8 1UB, United Kingdom

Author's contact: tobias.schmitt-manderbach@physik.uni-muenchen.de

ABSTRACT

The aim of the QIPS project (financed by ESA) is to explore quantum phenomena and to demonstrate quantum communication over long distances. Based on the current state-of-the-art a first study investigating the feasibility of space based quantum communication has to establish goals for mid-term and long-term missions, but also has to test the feasibility of key issues in a long distance ground-to-ground experiment. We have therefore designed a proof-of-concept demonstration 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. Here we report on the progress of this project and present first measurements of crucial parameters of the optical free space link.

1. INTRODUCTION

With the exponential expansion of electronic commerce the need for global protection of data is paramount. Data is normally protected by encoding it bit-wise using a large random binary number known as a key. An identical key is used to decode the data at the receiver. The secure distribution of these keys thus becomes essential to secure communications and transactions across the globe. At present electronic commerce generally exchanges keys using Public Key methods [1]. These methods rely on computational complexity, in particular the difficulty of factoring very large (publicly declared) numbers, as proof against tampering and eavesdropping. Any confidential information exchanged using such a key thus becomes insecure after a time when the rapid improvements in computational power or algorithmic development render the public key insecure. To guarantee long-term security the cryptographic key must be exchanged in an absolutely secure way. The conventional method used for this for most of the last century has been the 'trusted courier' carrying a long random key from one location to the other. Following the idea of Bennett and Brassard in 1984 [2], absolutely secure key exchange between two sites has been demonstrated over fibre [3-5] and free space [6-9] optical links. This technique, known as quantum cryptography, has security based on the laws of nature and is, in principle, absolutely secure against any computational improvements.

In this paper we describe the next step towards global secure key exchange: the demonstration over a test range with a distance of 144 km. Starting from previous experiments [10,11] 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. There, the distance of 144 km is bridged with a coupling efficiency of 30dB which will be sufficient for the demonstration of secure communication. Such a system combined with sophisticated automatic pointing and tracking hardware of the ground station could 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.

2. THE METHOD

Following the first experimental realisation [6], in the QC technique the transmitter (Alice) encodes a random binary number in weak pulses of light using one linear polarisation to encode '1's and orthogonally polarised pulses to encode zero's. To prevent eavesdropping the

Proc. '6th Internat. Conf. on Space Optics', ESTEC, Noordwijk, The Netherlands, 27-30 June 2006 (ESA SP-621, June 2006)

number of photons per pulse is limited to much less than unity (the actual attenuation is linked to the overall transmission and is usually chosen as 0.1 photons per pulse). Furthermore, the encoding basis is randomly changed by introducing a 45° polarisation rotation on half the sent pulses. In the receiver (Bob) single photon counting detectors detect the pulses, converting the light to macroscopic electronic pulses. The two polarisations are separated in a polarising beam-splitter and a zero or one is recorded depending on the detected polarisation. A random switch selects whether to measure in a 0° or 45° polarisation basis.

Due to the initial attenuation and the attenuation along the transmission line only very few of the sent pulses result in detected events at the receiver. A record of when the pulses are detected is kept and at the end of the transmission the receiver uses a classical channel (e.g. an ethernet connection) to tell the sender which pulses arrived and what basis they were measured in. All lost pulses and all detected pulses measured in a different basis to the encoding basis are erased from the sender's record. Thus identical random keys are retained by sender and receiver. Any remaining differences (errors) signal the interception of an eavesdropper! If an eavesdropper measures the polarisation of one pulse, that pulse, being a single photon, is destroyed and does not reach Bob and thus is not incorporated in the key. The eavesdropper could choose a basis, measure the pulses then re-inject copies. However, this strategy has to fail because half the time the eavesdropper will have chosen the wrong measurement basis and the re-injected pulses will induce an error rate of 25%. Of course a certain level of error could be caused by imperfections in the equipment used, but in order to guarantee absolute security any error should be attributed to (partial) interception. Below a certain threshold the error can be corrected and potential knowledge of the key by any eavesdropper can be erased by privacy amplification protocols [12,13].

An alternate scheme 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 selcted 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 continaing 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.

3. THE TOOLS

A typical free space set up consists of the transmitter module emitting either attenuated, randomly polarized light pulses or a source of polarization entangled photon pairs. These components are descibed in greater detail in previous publications [10,11]. The generated photons are sent through single mode optical fibre into a transmitter telescope (shown in Fig. 1). 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. Both the sender and the receiver station are situated at an altitude of more than 2400 m above sea level, meaning that the optical beam path usually ran above the cloud level.

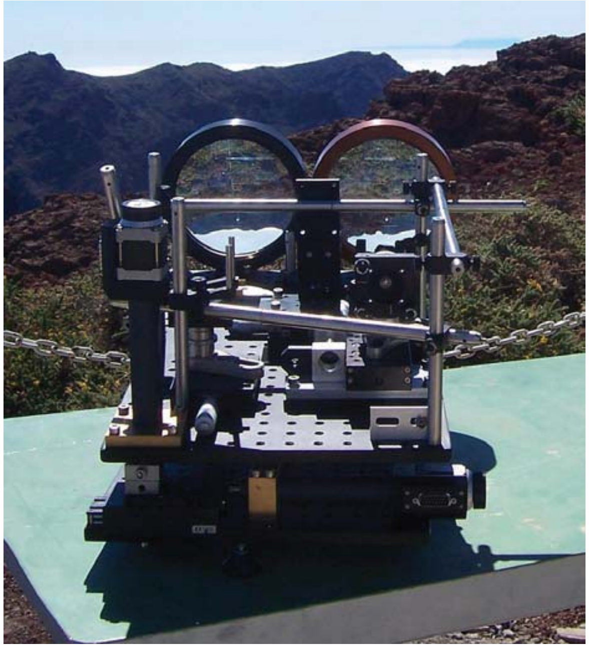


Fig. 1. The transmitting telescope on La Palma. The 15 cm front lens on the right is used for sending the single photon beam to the receiver, the identical lens on the left collects the light of the beacon laser, focusing it onto a CCD camera to perform the tracking.

Due to various atmospheric influences such as changes 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

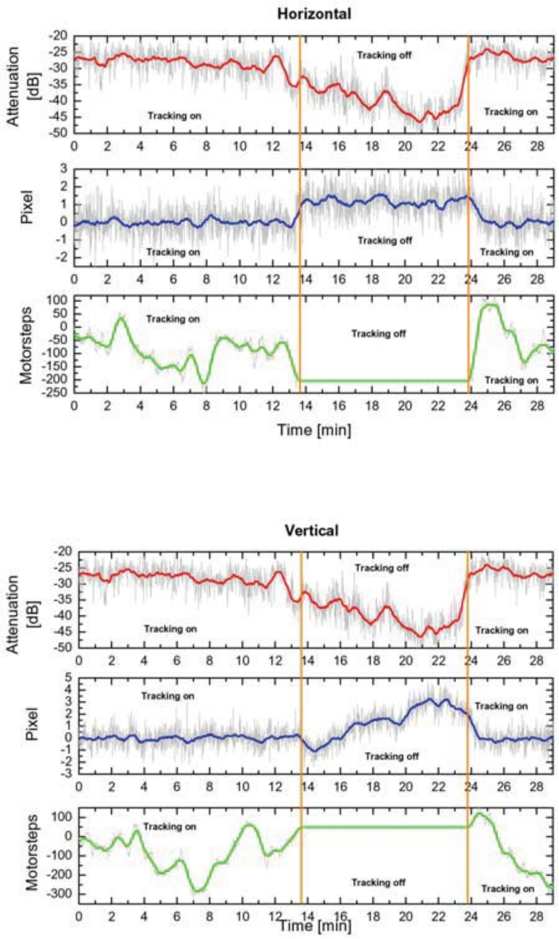


Fig. 2. Link attenuation and motor movement (horizontal and vertical direction) of the transmitter telescope's tracking system to compensate for slow beam wander caused by atmospheric effects.

minutes. Accordingly, vertical movements appeared more pronounced than horizontal ones (see Fig. 2). 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 telescope was controlled automatically by a closed-loop tracking system employing a 532 nm beacon laser shining from the OGS to the single photon transmitter. Its light was focused onto a CCD camera which was attached to the optical platform of the transmitter. Beam drifts were compensated by permanently readjusting the pointing direction of the transmitter platform with stepper motors, thus keeping the spot of the tracking laser on a fixed reference position on the CCD chip. 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 (Fig. 2).

Besides these beam drifts further processes lead to an attenuation of the optical link: beam spreading loss due to diffraction, absorption of the atmosphere and losses due to imperfections of the optical components in the setup. Atmospheric losses are expected to be around 0.07 dB/km at this altitude [15]. In addition, effects due to atmospheric turbulence, such as beam wander, rapidly evolving speckle patterns and turbulence induced beam spreading, cause losses. Thus, the effective beam diameters at the OGS varied between 3.6 and 20 m depending on weather conditions. In the diffraction limited case in vacuum, the transmitter telescope would have produced a beam of 1.5 m in diameter. All these losses reduce the link efficiency but do not affect the polarization. Within the accuracy of our experiment we did not detect any birefringence of the atmosphere.

The OGS, a 1 m Richey-Chrétien/Coudé telescope with an effective focal length of 39 m (f/39), is used to collect the single photons with a field-of-view of 8 arcsec. The atmospheric turbulence also 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 averaged images on a CCD camera one obtains a Fried parameter of r_0 ~1 cm. To prevent the beam wandering off the detectors we recollimate with an additional lens to pass through the polarisation analyser, and finally the single photons are focused with f=40 mm lenses onto Si avalanche photo diodes. The resulting beam size is then smaller than the detector's active area of 500 µm in diameter. Long term beam wander, however, caused the beam focus to leave the detectors, decreasing the end-to-end coupling efficiency. This problem will be adressed in the future by incorporating a similar tracking system for the receiver telescope as well.

4. CONCLUSION

Within our experiment, the 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. Our results demonstrate the feasibility of satellite-based quantum key distribution which is the first step to establish a worldwide network for quantum communication.

5. REFERENCES

1. See for instance 'The Code Book: the science of secrecy from ancient Egypt to Quantum Cryptography', Simon Singh, Anchor 1999.
2. C.H. Bennet, G. Brassard, Proc. Conf. Comp. Syst. And Signal Processing, Bangalore, pp 175 (1984).
3. P.D. Townsend, J.G. Rarity and P R Tapster, 'Single photon interference in a 10km long optical fibre interferometer', Electronics Letters 29, 1993, 634-5; ibid. 'Enhanced single photon fringe visibility in a 10km long prototype quantum cryptography channel', Electronics Letters 29, 1993, 1291-3.
4. Muller A., Breguet J. and Gisin N., 'Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km, Europhys. Lett. **23**, 383-388, (1993).
5. G. Ribordy, J-D. Gautier, N. Gisin, O. Guinnard, H. Zbinden, 'Fast and User-friendly Quantum Key Distribution', J. of Mod. Optics **47** (2/3), 517-531 (2000).
6. C H Bennett et al, 'Experimental Quantum Cryptography', J. Cryptology **5** (1992) 3-28
7. W.T.Buttler R.J. Hughes, S.K. Lamoureaux, G.L. Morgan, J.E.Nordholt and C.G. Peterson, 'Practical Free-Space Quantum Key Distribution over 1km', Phys.Rev.Letts, **81** (1998) 3283.
8. W.T. Buttler, R.J. Hughes, S.K. Lamoureaux, G.L. Morgan, J.E.Nordholtand C.G. Peterson, 'Daylight Quantum Key Distribution Over 1.6km', Phys.Rev.Letts, **84** (2000) 5652-5655.
9. J.G.Rarity, P.M.Gorman, and P.R.Tapster, 'Secure Key Exchange Over A 1.9km Free-space Range Using Quantum Cryptography', Electronics letters 37, 512-514, 2001; ibid Journal of Modern Optics 48, 1887 (2001)
10. 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)
11. K. Resch et al., 'Distributing entanglement and single photons through an intra-city, free-space quantum channel', Optics Express 13, 202-209 (2005)
12. Bennett C.H., Brassard G. and Robert J-M, Privacy Amplification by Public Discussion, SIAM Journal on Computing, (1988) **17**, pp210-229
13. G.Brassard and L.Salvail, Secret Key Reconciliation by public discussion, Adventures in Cryptology, EUROCRYPT93, Lecture Notes in Computer Science, Springer-Verlag. N.Y. (1994) **765,** pp410-423
14. T. Jennewein, C. Simon, G. Weihs, H. Weinfurter and A. Zeilinger, Quantum Cryptography with Entangled Photons, Phys. Rev. Lett. 84, 4729 (2000)
15. L. Eltermann, 'UV, Visible and IR Attenuation for Altitudes to 50 km', AFCRL-68-0153, AFCRL Environmental Research Paper 285 (1968)