QUANTUM COMMUNICATIONS IN SPACE  
(“QSpace”)

Executive Summary Report

Markus Aspelmeyer, Hannes R. Böhm, Caslav Brukner, Rainer Kaltenbaek, Michael Lindenthal, Julia Petschinka, Thomas Jennewein, Rupert Ursin, Philip Walther, Anton Zeilinger

Martin Pfennigbauer, Walter R. Leeb

Prepared for the European Space Agency under ESTEC/Contract No. 16358/02/NL/SFe

ESTEC Technical Management: J.M.Perdigues (TOS-MMO)

EUROPEAN SPACE AGENCY CONTRACT REPORT

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

May 19, 2003
Abstract

Quantum information science is an intriguing example where purely fundamental and even philosophical research can lead to a new technology. The developments in this young field experience a worldwide boom. Quantum communication provides qualitatively new concepts, which are much more powerful than their classical counterparts. This report is a detailed study of the feasibility for adopting the concepts of fundamental quantum physics and quantum communications to a space infrastructure. It also develops physical and technological concepts specifically designed for a space environment.

After reviewing the basics of physics of quantum information we characterize and compare quantum communications and classical optical communications. We discuss how to produce, manipulate, and measure qubits to be employed in quantum communication systems. Emphasis is put on photonic qubits, but we also review the present status of non-photonic realizations of qubits. We show that the various protocols discussed in connection with quantum information (like quantum cryptography or quantum teleportation) are feasible with today’s technology when being based on photonic entanglement. Several space scenarios are analyzed in detail both with respect to quantum communication applications and to novel fundamental quantum physics experiments. With the latter one may address, e.g., open questions on quantum non-locality and on the possible influence of relativity on quantum coherence.

In the last chapter we establish selection criteria for first proof-of-principle quantum communication experiments in space. Specifically, we propose to realize down-links from the International Space Station (ISS) to optical ground stations. For this scenario, we suggest a series of four experiments, one following in a logical way from the other, with increasing complexity and expenditure. We also present a preliminary design of the experiments. This includes block diagrams for space and ground terminals, a rough cost estimate, and a description of the quantum measurements to be performed. For these experiments we propose the use of entangled photon pairs. They do not only allow the implementation of “standard” quantum cryptography schemes but also open up new avenues both for fundamental research and for quantum communication.
1 Introduction

1.1 Study objectives

The study has two main objectives: The first is to identify and investigate novel concepts for space communication systems based on the principles of quantum physics with emphasis on those areas related to quantum communications. The second objective is to conceive and define experiments for the demonstration of fundamental principles of quantum physics, which make advantageous use of the space infrastructure. The aim of the proposed experiments is to make specific use of the added value of space infrastructure for fundamental quantum experiments and practical quantum communication based on the generation and manipulation of entangled photon pairs. The purpose of the proposed experiments is within

- general studies: to establish a free space optical link suitable as quantum channel for single photons (in contrast to existing optical space technology) and perform a systematic study on the influence of link parameters such as atmospheric birefringence, absorption or scattering on the decoherence of quantum states,
- physical sciences: to perform fundamental quantum physics experiments beyond the capabilities of earth-bound laboratories by utilizing the added value of space/ISS environment,
- technology innovation and commercial R&D: to perform quantum key distribution between ISS and a single ground station and also between ISS and two different ground stations to demonstrate the principle feasibility of satellite-based quantum communication.

1.2 Economic potential of quantum communication

Although classical information technology will surly not vanish with the advent of quantum communication, there is no doubt about the huge economic potential of this new technology. Gartner-Group analysts predict the advent of quantum communication technologies, both of quantum computers (within a ten-year time frame) and of quantum cryptography (expected as early as 2008). “Quantum mechanics is now on the speculative edge of computing research. (...) Enterprises that show a realistic understanding of advancing technologies will be more successful in their reassurances” [1]. Also EU politics indicate that quantum communication research has indeed taken the step from the laboratory into the world of industry. The European Commission is planning to move quantum cryptography research from the FET (Future and Emerging Technologies) Framework Programme into the main industrial applications programme within the calls of the 6th Framework Programme.

2 Principles of physics of quantum information

The most fundamental physical concepts of quantum information science are:

- superposition: The superposition principle allows the description of a physical system as a superposition of alternatives. This so-called “superposition of states” does not only
provide all predictions for the outcome of a physical measurement but has also drastic consequences for the nature of the physical state which we ascribe to a system.

- **qubit**: A qubit is the quantum analogue of the classical bit, i.e. information that is encoded on an individual quantum system with separate states $|0\rangle$ and $|1\rangle$. In contrast to its classical counterpart, the qubit also entails the possibility of coherent superposition, i.e. it can be either “0”, “1”, or a superposition of “0” and “1”. It is principally impossible to obtain a perfect copy of a qubit in an arbitrary state without destroying the information content of the original. This so-called “no-cloning theorem” is the basis for the security of all quantum cryptographic schemes.

- **entanglement**: Quantum entanglement [2] describes correlations between physical systems that cannot be modeled by classical means. It is the basis both for fundamental physical studies and for the design of quantum communication schemes such as quantum cryptography, quantum dense-coding or quantum teleportation [3]. The quantum nature of entanglement is revealed by testing correlations between independent observers against so-called Bell inequalities, which impose a classical limit to such correlations. Interactions of an entangled system with its environment can result in a loss of entanglement, and in an increase of its noise content, i.e. in a decrease of its purity. This so-called “decoherence” is equivalent with a loss of information.

**Communication schemes** based on those fundamental quantum physical principles can be much more efficient (or without any analogue) than their classical counterpart. We have investigated the following well-known quantum communication protocols:

- **Quantum key distribution (QKD)** using single and entangled qubits: The quantum cryptographic protocol relies on the transmission and detection of single photons. Its security is based on the impossibility to copy the quantum state of a single photon and is thus guaranteed by the laws of quantum physics [4, 5, 6].

- **Quantum dense coding (QDC)**: This communication protocol utilizes quantum entanglement as a resource for communication with higher-than-classical channel capacity [7].

- **Quantum state teleportation**: This means the transfer of a quantum state from one site to another without the use of a physical carrier but by utilizing shared entanglement between transmitter and receiver. The implementation of quantum state teleportation is also a necessary requirement to establish a quantum repeater, which allows to share entanglement over arbitrary distances [8].

- **Entanglement-enhanced classical communication**: This scheme is based on the transmission of entangled states and is more noise-resistant than any classical communication [9].

- **Quantum communication complexity (QCC)**: This protocol utilizes entanglement to decrease the amount of information exchange that is necessary to accomplish computational tasks between distant parties [10, 11].
3 Concepts based on entangled particles

3.1 Photons versus particles

In most state-of-the-art quantum information experiments, photons are used for several reasons. They are “easy” to entangle and do not need sophisticated equipment for keeping the system stable. For photonic qubits, the two bit levels “0” and “1” can for example be realized by means of polarization, by angular momentum or by energy and time. Treating non-photonic systems leads to completely new conditions for creating and reading out qubits. Also decoherence effects are more noticeable when working with particles including a mass or potential. For non-photonic qubits the most common degrees of freedom which are experimentally accessible to store information are:

- **spin**: Every particle containing a spin, like electrons, protons, neutrons or atoms can be entangled.

- **internal levels**: This possibility to realize a qubit exists for atoms, as well as for ions and molecules, e.g. in their modes of vibration

- **energy levels**: For many schemes this seems to be the easiest way to entangle particles. The only condition is to own a stable ground- and excited state ($|g\rangle, |e\rangle$).

3.2 Experimental realization and recent results

To build hardware for a quantum information network or computer, technology will be needed that enables to manipulate and store qubits. The main requirements are:

- **storage**: Qubits have to be stored for a long time, long enough to complete the operation.

- **isolation**: The quantum system or the collection of qubits must be initialized in a well-defined state and therefore well-isolated from the environment to minimize decoherence errors.

- **readout**: Techniques will be needed to measure the qubits efficiently and reliably.

- **gate**: For manipulating a quantum state, arbitrary unitary operators must be available and controlled to launch the initial state to an arbitrary entangled state.

- **precision**: The quantum gates should be implemented with high fidelity if the device is to perform reliably.

These stringent hardware requirements unfortunately rule out most known physical systems. Conventional solid-state architectures such as silicon are ideal for classical information, for the same reason they are unsuitable for quantum information; their stability is given by the latching of logic levels, or continuous monitoring by the environment. The most attractive candidates for quantum information processors currently come from the area of atomic physics and quantum optics. Here, individual atoms and photons are manipulated in a controlled environment with well understood couplings, offering environmental isolation much better than in other physical systems. An elegant proposal to marry atomic and photonic quantum bits in
optical cavity quantum electrodynamics (QED) was developed in 1997 [12]. In this scheme, a small number of cold atoms are confined to the anti-nodes of a single-photon standing-wave field in a high-finesse Fabry-Pérot optical cavity. Qubit states stored in the internal states of the atoms can be mapped to the qubit spanned by the number of photons (0 or 1) in the cavity by applying an appropriate laser pulse from the side. The photon can be made to leak out of the cavity within a predefined time window, resulting in an ideal single-photon source for use in quantum communication. Moreover, after the photon leaks out of the cavity, it can be deterministically “caught” in a second cavity by the application of another laser pulse, whose envelope is time reversed with respect to the first pulse.

Several recent experiments from the universities of Harvard and Berkeley have reported slowing and even “stopping” of light using the techniques of electromagnetically induced transparency in an atomic vapor. These experiments offer the potential for mapping quantum states of photons onto collective quantum states of the atomic vapor. For example, single-photon qubits can be mapped onto a single qubit spanning all N-spins in a vapor.

The basic element for the scheme of “atomic ensembles” to entangle atoms or molecules is a system which has the relevant level structure as shown in Fig. 1. All the atoms are initially prepared in the ground state $|g\rangle$. Then a sample is illuminated by a short, off-resonant laser pulse ($\Delta|e\rangle$) that induces Raman transition into the state $|h\rangle$ by emitting a Stokes photon. An emission of only one single photon in a forward direction results in an entangled state of the two ensembles, where either one atom/molecule of the left or the right box is in the state $|h\rangle$.

Although extensive research is being performed on the utilization of non-photonic systems for quantum communication, up to date the only practical realizations are based on photons.

Figure 1: Set-up for entanglement generation and relevant structure of the ensemble with $|g\rangle$, the ground state, $|h\rangle$ the (long-living) metastable state for storing a qubit and $|e\rangle$, the excited state.

4 Comparison between quantum communications and classical optical communications

Table I summarizes the main conceptual differences and common properties of the performance of quantum and classical optical communications. The performance is defined by speed, capacity, efficiency, security, technology, complexity and influence of the atmosphere.
It is a common source of misconception that quantum physics does permit communication at superluminal speeds, although the non-local features of quantum entanglement would suggest this. The principal limit is still the speed of light!

<table>
<thead>
<tr>
<th></th>
<th>Classical Theory</th>
<th>Quantum Theory</th>
<th>common properties</th>
<th>differences</th>
</tr>
</thead>
<tbody>
<tr>
<td>speed</td>
<td></td>
<td></td>
<td>speed of light, delays in electronics</td>
<td></td>
</tr>
<tr>
<td>capacity</td>
<td></td>
<td></td>
<td>data rate</td>
<td>increased capacity via quantum dense coding</td>
</tr>
<tr>
<td>efficiency</td>
<td></td>
<td></td>
<td>basically same efficiency</td>
<td>possibly higher bit rates by quantum measurements, entanglement-enhanced communication and computation</td>
</tr>
<tr>
<td>security</td>
<td>low beam divergence makes eavesdropping more difficult than for radio frequency</td>
<td>perfect single photon sources needed for perfect security</td>
<td>security is based on the laws of nature (quantum cryptography)</td>
<td></td>
</tr>
<tr>
<td>complexity</td>
<td>reasonable, there are already classical systems in orbit</td>
<td>fast progress keeps complexity at a reasonably low level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>technology</td>
<td>transceivers are state-of-the-art</td>
<td>rapidly evolving standard technologies</td>
<td>pointing, acquisition and tracking is close to state-of-the-art</td>
<td>there exist no perfect optical amplifiers for quantum information (no-cloning-theorem)</td>
</tr>
<tr>
<td>influence of atmosphere</td>
<td></td>
<td></td>
<td>wavelength- and time-dependent attenuation</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Comparison between quantum communications and classical optical communications
5 Technologies for quantum communications in space

5.1 Preparation of single qubits and entangled qubits

At present, all quantum communication schemes are based on single photons and entangled photons, since this is straightforward to realize and least affected by environmental decoherence (as compared to massive particles).

Most of the photonic qubit realizations rely on the preparation of coherent single-photon number states of the electromagnetic field (single-photon Fock-states). This can be approximated by a strongly attenuated laser pulse with an ultralow mean photon number. At present, the best available source for single photons is based on spontaneous parametric down-conversion (SPDC). This method relies on the creation of simultaneously created photon pairs via the (nonlinear) process of parametric down conversion, where one of the two photons is used as a trigger photon. Other devices are currently under investigation but have not yet reached a level of reliable application. Table 2 summarizes the most popular candidates for single-photon generation.

<table>
<thead>
<tr>
<th>single photon source</th>
<th>max photon rate</th>
<th>bandwidth-limited</th>
<th>operating conditions</th>
<th>comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPDC(^a)</td>
<td>limited by pump-intensity and repetition rate (presently approx. (10^6) Hz)</td>
<td>yes</td>
<td>room temperature, ambient pressure</td>
<td></td>
</tr>
<tr>
<td>faint laser pulses</td>
<td>limited by repetition rate</td>
<td>yes</td>
<td>room temperature, ambient pressure</td>
<td></td>
</tr>
<tr>
<td>color centers in diamond</td>
<td>limited by state decay time (presently approx. (10^6) Hz)</td>
<td>no</td>
<td>room temperature, ambient pressure, low collecting efficiencies</td>
<td></td>
</tr>
<tr>
<td>quantum dots</td>
<td>limited by repetition rate</td>
<td>no</td>
<td>5 K</td>
<td>bandwidth-limit is approached with additional microcavities</td>
</tr>
<tr>
<td>cavity QED with atoms</td>
<td>limited by state decay time (presently approx. (10^3) Hz)</td>
<td></td>
<td>mK, UHV</td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Summary of present-day technology of single photon sources.

\(^a\)The bandwidth limit is a measure of coherence, given by the ratio between the decay lifetime of a photon state and its coherence time. Only bandwidth-limited states (ratio = 1) can be used for high-fidelity quantum communication and quantum computation protocols.

\(^b\)Spontaneous Parametric Down-Conversion

At present, the most efficient source of entangled photons is spontaneous parametric down conversion (SPDC), which allows to generate different kinds of entanglement:

- **Polarization-entangled qubits**: Polarization entanglement can be achieved by di-
Figure 2: Source of entangled photons based on spontaneous parametric down-conversion. The phase matching condition governs the “decay” of the photons such that they emerge from the crystal along cones. In the degenerate case, i.e. when the two photons have the same wavelength, the intersection lines of the cones yield entangled photons. This is when the photons carry no information about whether they emerged with horizontal or vertical polarization, yet they will always opposite polarization.

- **Momentum-entangled qubits**: Momentum-entanglement is achieved between different signal and idler modes such that each single photon carries no information about the spatial mode it was prepared in [15].

- **Time-bin-entangled qubits**: In the case of time-bin entanglement, photon pair creation via SPDC is stimulated by temporally distinguishable pump pulses resulting in a state in which the single photons in the signal and idler modes do not carry any information about their preparation time (time-bin one or two). Since the pump pulses are created within an interferometer, a fixed phase relation between subsequent pulses can be established which intrinsically excludes the possibility of gaining any timing information and therefore corresponds to maximal entanglement [16].

### 5.2 Single photons vs. entangled photons

The mere use of single photons (qubits) as the information carrier of classical bits does not increase the classical communication capacities. However, this situation changes either if entangled single particles are utilized as carriers of classical information and sent between distant users (entanglement enhanced classical communication), or if entangled particles are being shared by distant users even before the communication is established (quantum dense coding). This means that, in order to achieve more efficient communication based on the principles of quantum communication, the reduction of the signal level to the single-particle regime is not sufficient and the use of entanglement is absolutely necessary. We therefore suggest in the following to also consider a source of entangled photons as a potential source of single photons, where one of the photons is used as a trigger photon.
In quantum communication schemes with photons, the single photons used must be detected with a high efficiency, and with a high timing accuracy. Table 3 gives an overview on existing single photon detection technologies. 

In principle, an identification of an entangled Bell state of two qubits would require a direct interaction of the two photons. Since a direct coupling is too weak to exploit, other methods with higher efficiencies have to be used. The best method up to now is based on linear optics exclusively and can distinguish two out of four Bell states. One of the main issues for the utilization of polarization entangled photon pairs is the ability to discriminate subsequent pairs, since perfect correlations due to entanglement are only established between single pairs. This necessitates the possibility of detecting photon pairs at different observer positions accurately with respect to a joint time basis. In practical terms, a timing accuracy of the order of some ns is necessary.

### 6 Experimental scenarios

The scenarios involving an earth-based transmitter terminal allow to share quantum entanglement between ground and satellite, between two ground stations or between two satellites and thus to communicate between such terminals employing quantum communication protocols (see Fig. 3). In the most simple case, a straight up-link to one satellite-based receiver can be used to perform secure quantum key distribution between the transmitter station and the receiver. Here, one of the photons of the entangled pair is being detected right at the transmitter site and thus the entangled photon source is used as a triggered source for single photons. If the satellite acts as a relay station, the same protocol can be established between two distant earth-based communication parties. Shared entanglement between two parties can be achieved by pointing each of the photons of an entangled pair either towards an earth-based station and a satellite or towards two separate satellites. Another set of satellite-based relays can be used to further distribute the entangled photons to two ground stations. Possible applications for shared entanglement between two parties are quantum key distribution or entanglement-enhanced communication protocols.

In a second scenario, a transmitter with an entangled photon source is placed

<table>
<thead>
<tr>
<th>Detector</th>
<th>Typical detection efficiency</th>
<th>Typical dark counts</th>
<th>Wavelengths</th>
<th>Operating temperatures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Si-APD</td>
<td>40%</td>
<td>200 to 500 Hz</td>
<td>700 to 800 nm</td>
<td>-25 °C</td>
</tr>
<tr>
<td>SLIK APD</td>
<td>70%</td>
<td>540 Hz</td>
<td>1000 to 1300 nm</td>
<td>-25 °C</td>
</tr>
<tr>
<td>Ge-APD</td>
<td>15%</td>
<td>25000 Hz</td>
<td>1000 to 1300 nm</td>
<td>-200 °C</td>
</tr>
<tr>
<td>InGaAs</td>
<td>10% to 30%</td>
<td>$10^{-5}$ gating frequency</td>
<td>1000 to 1500 nm</td>
<td>-200 to -100 °C</td>
</tr>
<tr>
<td>VLPC</td>
<td>99%</td>
<td>$\approx 10^4$ to $10^5$ Hz</td>
<td>500 to 800 nm</td>
<td>-269 °C</td>
</tr>
</tbody>
</table>

Table 3: Present-day technology for single photon detection.

---

"APD: Avalanche-Photodiode
SLIK: Super Low Ionization k factor
VLPC: Visible Light Photon Counter"
Figure 3: Scenarios for satellite-aided quantum communication with an Earth-based transmitter terminal. The transmitter terminal distributes entangled photon pairs to the receivers which can perform an entanglement-based quantum communication protocol. As indicated, a relay module redirects and/or manipulates qubit states without actually detecting them.
on a space-based platform. This allows not only longer link distances because of reduced influence of atmospheric turbulence; it will also be the preferred configuration for global quantum communication, since only one down-link per photon of the entangled pair is necessary to share entanglement between two earth-based receivers. Again, already a simple downlink allows to establish a single-photon link, e.g., for quantum cryptography. In this configuration, a key exchange between two ground stations is also possible. To this end each of the two ground stations has to establish a quantum key with the satellite. Since the space terminal has access to both keys, it can transmit a logical combination of the keys, which can then be used by either ground station or both ground stations such that they arrive at the same key. This logical combination can easily be chosen such that it cannot reveal any information about the key. Note that the key does not have to be generated simultaneously at both receiver stations. In principle, a quantum key exchange can be performed between arbitrarily located ground stations. However, in all such scenarios based on single photons the security requirement for the transmitter terminal is as high as it is for the ground station. Only the use of entangled states sent to two separate ground stations allows instantaneous key exchange between these two communicating earth-bound parties and also relaxes the security requirement for the transmitter module. Furthermore, more advanced quantum communication schemes will be feasible. The required shared entanglement can be established either by two direct downlinks or by using additional satellite relay stations. Quantum entanglement can also be distributed between a ground station and a satellite or between two satellites. In an even more elaborate scheme a third party might be involved, which is capable of performing a Bell-state analysis on two independent photons. This allows quantum state teleportation and even entanglement swapping and could thus resemble a large-scale quantum repeater for a truly global quantum communication network. Applied to quantum cryptography, this third party might be used to control the communication between the two other parties in a “Third-Man” cryptography protocol. For example, in a polarization-based experiment, depending on whether he performs a simple polarization analysis of the independent photons or a Bell-state measurement, the “Third-Man” can communicate secretly with either of the two parties (or with both) or he can control whether the two can communicate secretly or not without knowing the content of the communication. The presented application scenarios for quantum communication applications are summarized in Fig. 4.

7 Quantum communications applications in space

We identify the following fields of potential space applications for quantum communication schemes:

- **Secure communication with quantum cryptography**: Two main applications have to be considered: Secure communication to and from satellites and secure communication between arbitrary distant earth-based parties. As an example, remote-controlling satellite-based systems necessitates truly secure communication links between a ground-station and a satellite. Another example in which security is mandatory in a space environment would be the Galileo system, where protection against intentional manipulation is of highest importance. Clearly, the technique of quantum key distribution can also be used for secure inter-satellite communication.

- **Efficient communication and computation using quantum dense coding, quan-
tum teleportation and quantum communication complexity: A large economic potential of quantum communication lies in its superior information processing capabilities, which exceed those of classical methods by far.

- Deep space communication using quantum telecomputation and communication complexity: Deep space communication is a specific example where resources for data transmission are limited. Quantum communication complexity could provide a unique means of information transport with very little consumption of communication resources.

7.1 Modules for quantum communication applications

A transmitter module consists of a photon source for single photons or entangled photon pairs (including passive or active manipulation of single qubit-states), a module for timing synchronization with the receiver station, a classical channel to the receiver station and a connection to an up-link or down-link (see Fig. 5).

A receiver module comprises one or more input channels, in each of which manipulation of qubits can be performed independently. Depending on whether active (remote) control of optical elements for qubit manipulation (such as polarizer or a polarization retarder) is possible or not, we distinguish active and passive receiver modules. Additionally, each receiver is equipped with single photon detectors at each input port, a receiver module for time-synchronization and a classical channel for communication with the transmitter (see Fig. 6). In most cases, both receiving and transmitting classical information is required.
Figure 5: Transmitter module for quantum communication. (The data acquisition module allows the storage of data. It might well be that, e.g. in case of quantum key distribution systems, the key is not generated immediately.)

Figure 6: Receiver module for quantum communication.
7.2 Link attenuation

The maximal acceptable **link attenuation** for a quantum communication system based on entangled photons is determined by the timing resolution and the dark count rates of the detectors used, as well as by the net production rate of the source. As the minimum signal-to-noise ratio we assume that necessary for the violation of a Bell inequality. Roughly speaking, a total link efficiency of $\eta_{\text{link}} = \eta_{\text{link1}}\eta_{\text{link2}} \approx 10^{-6}$ (−60 dB) is necessary. The link attenuation is also important for determining the number of photon pairs that can be received in a certain time window. This could be crucial in scenarios where the links are only available for short times as is for example the case in up-links to low orbiting satellites. We investigated the link attenuation for optical free-space links involving space infrastructure. The attenuation factor calculated includes the effect of beam diffraction, attenuation and turbulence-induced beam spreading caused by the atmosphere, receive aperture diameter, losses within the telescopes acting as antennas, as well as antenna pointing loss. The calculations have been performed for wavelengths of 800 nm and 1 550 nm. The first wavelength is reasonable because the best photon source exists for 800 nm, while the second wavelength is mainly used in telecom systems. Figure 7 summarizes the scenarios considered based on satellites in geostationary orbit (GEO) and in low-earth orbit (LEO). Such satellites may serve as a platform for transmitters or receivers. We presently do not envision the use of passive relays, e.g. retro-reflectors or mirrors, because of the high link loss they would introduce and because of the difficulty to implement a point-ahead angle.

For the case of a **LEO-based transmitter or receiver** (link 1 in Fig. 7), link attenuation poses no problems. Even for quite small telescopes onboard the LEO satellite, the attenuation factor is well below 60 dB for all cases. Figure 8 is a contour plot of the link attenuation as a function of transmitter and receiver aperture diameter ($D_T, D_R$) for the ground-to-LEO uplinks operated at a wavelength of $\lambda = 800$ nm. Two additional vertical scales give the link distance $L$ for 30 cm receive telescope aperture as well as for the receive telescope aperture for a link distance of $L = 500$ km. The corresponding plot for LEO-to-ground downlinks is shown in Fig. 9. The attenuation is much larger for the uplink than for the downlink due to the pronounced influence of atmospheric turbulence for the uplink, where the turbulent layers are close to the transmitter. Another consequence of turbulence is that increasing the transmitter aperture for the uplink beyond 60 cm hardly decreases the link attenuation.
Figure 7: Summary of links involving Earth-based ground stations and LEO satellites or GEO satellites
Figure 8: Contour plot of link attenuation $A$ (in dB) as a function of transmitter and receiver aperture diameter ($D_T, D_R$) and link distance $L$ for ground-to-LEO uplinks at $\lambda = 800$ nm.

Figure 9: As Fig. 8 but for LEO-to-ground downlinks.
The long distance in links between GEO and ground (link 2 in Fig. 7) results in a relatively high attenuation. With a ground station aperture of \( D = 100 \) cm and a GEO terminal aperture of \( D = 30 \) cm one will meet the 60 dB requirement in a downlink, but not in an uplink (compare Tab. 4).

While from a technological point of view a satellite-to-satellite link is the most demanding configuration it offers highly attractive scientific possibilities. It allows to cover, in principle, arbitrarily large distances and might thus also be a possibility for further novel fundamental tests on quantum entanglement. We calculated the attenuation factor as a function of transmitter and receiver aperture diameter for a LEO-LEO link (link 3 in Fig. 7). The 60 dB-limit poses no problem for LEO-LEO links with reasonable link distance. For GEO-GEO links (link 4 in Fig. 7) with a distance of \( L = 45000 \) km, an attenuation of \( A = 55 \) dB would result for \( D_T = D_R = 30 \) cm.

Numerical results for the attenuation \( A \) are summarized in Tab. 4. The cited values apply for the following default parameters: ground based telescope diameter = 100 cm, space based telescope diameter = 30 cm; link distances: 500 km for ground-LEO, 36000 km for ground-GEO, 2000 km for LEO-LEO, 40000 km for GEO-GEO, 35500 km for LEO-GEO.

<table>
<thead>
<tr>
<th>800 nm</th>
<th>ground based receiver</th>
<th>LEO receiver</th>
<th>GEO receiver</th>
<th>LEO retro-reflector</th>
<th>GEO retro-reflector</th>
</tr>
</thead>
<tbody>
<tr>
<td>1550 nm</td>
<td>ground based transmitter</td>
<td>27 dB</td>
<td>64 dB</td>
<td>31 dB</td>
<td>105 dB</td>
</tr>
<tr>
<td></td>
<td>LEO transmitter</td>
<td>6 dB</td>
<td>28 dB</td>
<td>53 dB</td>
<td>110 dB</td>
</tr>
<tr>
<td></td>
<td>GEO transmitter</td>
<td>44 dB</td>
<td>53 dB</td>
<td>54 dB</td>
<td>60 dB</td>
</tr>
</tbody>
</table>

Table 4: Comparison of the attenuation factors resulting for default parameters. The values within the boxes correspond to a wavelength of 1550 nm, while the others stand for 800 nm.

8 Fundamental quantum physics experiments

For a demonstration of fundamental quantum physics experiments, we focus on the use of entangled two-particle states to test for non-classical correlations violating a Bell-type inequality. Testing for the violation of a Bell inequality, a so-called Bell experiment, is probably the most straightforward fundamental experiment in quantum physics [17]. Making use of the space environment and the present technological infrastructure in space, a class of novel experiments devoted to tests of a Bell inequality can be designed:

- Bell experiments over long distances beyond the capabilities of earth-bound laboratories, addressing the question of persistence of quantum correlations over distances from several hundred kilometers (in the case of LEO satellites) up to solar distances.
• An ultimate Bell experiment, concerned with ultimately closing the final interpretation loophole in such experiments.

• Experiments testing different models for the physical collapse of the wave-function.

With a long-term vision in mind, we are also proposing a set of possible future fundamental experiments making use of quantum entanglement in space:

• Experiments concerning special and general relativistic effects on quantum entanglement.

• Wheeler’s delayed choice experiment [18].

• A novel test of the Lens-Thirring effect, making use of entanglement-enhanced interferometry.

• An experimental test of Gödel’s cosmological model of a rotating universe.

9 Selection and design of an experiment

For a trade-off between possible experiments and their various manifestations we used the following evaluation criteria:

• state-of-the-art of present-day technology,

• technical complexity (link attenuation, PAT requirements, status of space qualification, ...),

• detrimental influence of atmosphere,

• compatibility with available ground and space systems,

• novelty and scientific impact of experiment,

• added value with respect to space.

Concerning the last point one has to consider that in free-space transmission systems, the lack of atmosphere is a major advantage for bridging large distances beyond those presently bridgeable between earth-bound terminals. Further, space links do not encounter the problem of obscured line-of-sight by unwanted objects or due to the curvature of the Earth. The long distances that are manageable in principle when going into space are essential with respect to both fundamental and application aspects. Using space is presently the only method which allows to establish quantum key distribution between arbitrary users on Earth. Earth-based photonic propagation in quantum experiments using glass fibres is limited to some 100 km with present-day technology. In the long run, the influence of gravitation on quantum physics, albeit minor, might be accessible in a space-based large-scale experiment using quantum entanglement for further fundamental tests.
9.1 Selected experimental scenarios

Our final aim is to have available one transmitter module and two receiver modules. In order to cover large distances it would be best to have all modules in space. However, we presently discard this scheme due to the huge technological (and financial) effort. We propose the transmitter to be placed in space, preferably on the ISS, as the terminal can be modified and upgraded more easily than on a satellite. We suggest to place the receiver modules on Earth, as this allows maximum flexibility for the manipulation and detection of the photons. Specifically, we propose to follow a stepwise approach. The upgrade from experiment 1 to 2 (see below) requires the involvement of a second ground station (with a receiver terminal), that from experiment 2 to 3 the modification of the transmitter at the ISS in the form of replacing the – internal – receiver by a second telescope to be pointed to the second ground station. This modification can be performed more easily if two telescopes are present from the beginning. Before going into space, transmitter and receiver terminals are to be tested along a horizontal terrestrial link.

**Experiment 1:** Space-based transmitter of entangled photons and one ground-based receiver. One photon is sent to the ground station, and the other is detected directly at the transmitter. Experimental achievements: (a) the first demonstration of quantum key distribution using single photons (via BB84) between space and ground and (b) investigation of the influence of long-distance propagation on single photons beyond distances achievable on Earth.

**Experiment 2:** Space-based transmitter of entangled photons and two independent ground-based receivers, with only one down-link at a time, i.e. one photon is sent to a ground station, and the other is detected directly at the transmitter. No modification of the modules is required. Experimental achievement: Quantum key exchange between two independent ground stations over distances not feasible with earth-bound technology.

**Experiment 3:** Space-based transmitter and simultaneous operation to two independent ground-based receivers. Experimental achievements: (a) testing Bell’s inequality over distances only achievable with space technology, (b) quantum key distribution based on entanglement.

**Experiment 4:** Establishment of an uplink: Space-based receiver, ground-based transmitter module and an additional independent ground-based qubit source. Also, a ground-based receiver module capable of a Bell-state measurement is necessary. Experimental achievements: (a) quantum key distribution in uplink-configuration; (b) quantum state teleportation between a ground station and a satellite.

9.2 Technological baseline and preliminary design

The **transmitter terminal** comprises the entangled photon source, modules for polarization sensitive manipulation and detection of single photons, a classical optical PAT system and a telescope for the establishment of the downlink (see Fig. 10). Each of the photons of the entangled pairs is coupled into optical fibers which are subject to polarization control via (piezomechanical) bending of the fibers. Depending on the stage of the experiment, the two photons of the entangled pair are either both sent through separate telescopes or only one is sent while the other one is immediately detected. The reference laser of the PAT subsystem
is linearly polarized and optionally pulsed to provide both an orientational and a timing reference frame between transmitter and receiver site.

The receiver terminal comprises a single-photon analysis and detection subsystem (analogous to the unit used in the transmitter terminal) and a classical optical subsystem consisting of a telescope and PAT equipment (see Fig. 11). Another polarization analysis subsystem monitors the polarization of the transmitter reference laser, which is used to compensate for any orientational misalignment between transmitter and receiver polarization. The signal from this analysis is used to properly orientate the polarization in the single photon beam path. The reference laser of the receiver station(s) are operating at a wavelength differing from the transmitter reference laser in order to clearly separate the two distinct signals for a more accurate polarization analysis of the transmitter reference laser.

For the quantum communication experiments in mind, we take into account the following four European ground stations:

- Observatorio Del Teide, Tenerife (ES), Instituto de Astrofísica de Canarias
- Centro di Geodesia Spaziale, Matera (IT), Italian Space Agency (ASI)
- Estacion de Observacion de Calar Alto (ES), Instituto Geografico Nacional
- Observatorio de Sierra Nevada (ES), Instituto de Astrofísica de Andalucía
9.3 Mass, volume, and power consumption of space terminal

The basis for - necessarily very crudely - estimating mass, volume, power consumption, and cost (MVPC) were various free-space optical terminals designed (and in a few cases flown) for conventional laser communication. Specifically, we used data of the following terminals: OPALE and PASTEL (ESA’s SILEX system), SOTT (Matra Marconi), CDT (Bosch Telecom), OPTEL-25 (Contraves Space), LUCE (Japan), LCDE (JEM/Japan). All this information together with quite some amount of educated guess led to Tab. 5, which presents the results of our MVPC estimates, both for the terminal with a single telescope (as needed for experiment 1 and 2) and one with two telescopes (experiments 3 and 4). In the table we distinguish between four subunits:

- the source of entangled photons (including polarization control, polarization analysis, and reference detection),
- the optical head consisting of the optical bench, the telescope (including the coarse pointing mechanism),
- the devices needed for PAT (including the reference laser, the point ahead mechanism, and the acquisition and tracking sensor),
- electronics for driving and controlling the opto-electronic and opto-mechanic devices, as well as the harness.
<table>
<thead>
<tr>
<th></th>
<th>Quantum source</th>
<th>Optical head</th>
<th>PAT</th>
<th>Electronics</th>
<th>Total for single-telescope terminal</th>
<th>Total for dual-telescope terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mass [kg]</td>
<td>35</td>
<td>40</td>
<td>20</td>
<td>20</td>
<td>115</td>
<td>185</td>
</tr>
<tr>
<td>Volume [cm³]</td>
<td>50x30x30</td>
<td>50x30x30</td>
<td>30x30x30</td>
<td>50x20x20</td>
<td>50x60x60</td>
<td>50x90x60</td>
</tr>
<tr>
<td>Power [W]</td>
<td>80</td>
<td>15</td>
<td>40</td>
<td>50</td>
<td>185</td>
<td>265</td>
</tr>
</tbody>
</table>

Table 5: Estimate for mass, volume, and power of terminals with a single telescope and with a dual telescope.
References


