IAC-07-B2.3.05

QUANTUM COMMUNICATIONS AT ESA: TOWARDS A SPACE EXPERIMENT ON THE ISS

Josep Maria Perdigues Armengol (1), Bernhard Furch (1), Clovis Jacinto de Matos (2), Olivier Minster (1), Luigi Cacciapuoti (1), Martin Pfennigbauer (3), Markus Aspelmeyer (4), Thomas Jennewein (5), Rupert Ursin (4), Tobias Schmitt-Manderbach (6), Guy Baister (7), John Rarity (8), Walter Leeb (9), Cesare Barbieri (10), Harald Weinfurter (6), Anton Zeilinger (4,5)

(1) ESA/ESTEC, the Netherlands, e-mail: Josep.Maria.Perdigues.Armengol@esa.int, Bernhard.Furch@esa.int, Olivier.Minster@esa.int, Luigi.Cacciapuoti@esa.int

(2) ESA/HQ, France, e-mail: Clovis.De.Matos@esa.int

(3) RIEGL Laser Measurement Systems, Austria, e-mail: mpfennigbauer@riegl.co.at

(4) Vienna University, Austria, e-mail: markus.aspelmeyer@ap.univie.ac.at, Rupert.Ursin@univie.ac.at, anton.zeilinger@univie.ac.at

(5) Austrian Academy of Sciences, Austria, e-mail: thomas.jennewein@ap.univie.ac.at, anton.zeilinger@univie.ac.at

(6) Max Planck Institute of Quantum Optics, Germany, e-mail: Tobias.Schmitt-Manderbach@physik.uni-muenchen.de, harald.weinfurter@physik.uni-muenchen.de

(7) Oerlikon Space, Switzerland, e-mail: guy.baister@unaxis.com

(8) Bristol University, United Kingdom, e-mail: John.Rarity@bristol.ac.uk

(9) Vienna University of Technology, Austria, e-mail: walter.leeb@tuwien.ac.at

(10) University of Padova, Italy, e-mail: cesare.barbieri@unipd.it

Abstract

The European Space Agency (ESA) has supported since 2002 – in the frame of its General Studies Programme - several studies in the field of quantum communications for space systems. As a result of these studies, a European research consortium led by Prof. Zeilinger (Vienna University) submitted the mission proposal Space-QUEST (“QUantum Entanglement for Space ExperimenTs”) to the *European Life and Physical Sciences in Space Programme* of ESA, aiming at a quantum communications space-to-ground experiment from the International Space Station. This paper will present the achievements of the ESA studies on quantum communications and discuss the programmatic roadmap and the proposed technology development activities for the implementation of the proposed Space-QUEST experiment on-board the ISS.

1 Introduction

The emergence of applications and technologies based on the foundations of quantum physics has revolutionized our understanding of information theory. Quantum superposition and entanglement constitute a novel type of resource that enables new developments in the fields of communications, computation, metrology, etc., and opens new doors for fundamental physics research [1].

Quantum communications has recently matured from a purely fundamental research area of quantum physics to an applied science with a potentially huge economic impact [2]. The unit of quantum information is the “qubit” (a bit of information “stamped” in a quantum physical property, for instance the polarization of a photon). Moreover, information can be encoded in the correlations between two (or more) particles (e.g. photons or atoms). The properties of “superposition of states” and “entanglement” lead to innovative methods of information processing (e.g. quantum key distribution, quantum teleportation, quantum dense coding) and computation, with some algorithms more powerful than their classical counterparts.

At present, the most mature application is quantum key distribution (QKD). QKD provides means for two (or more) parties to exchange with unconditional security an enciphering key over a quantum channel, since its privacy against an eavesdropper can always be detected. This symmetrical key - after successful distribution - can then be used for encrypting classical information for transmission over a conventional, non-secure communication channel (e.g. telephone line, RF link, optical fibre, optical free-space link).

The utilization of the space segment for distributing quantum keys has been proposed by several groups, [3]-[6]. One clear vision of the science community is to test the theory of quantum physics over long distances and to establish a worldwide network for quantum communication - tasks that can only be realized by tackling the additional challenge of bringing concepts and technologies of quantum physics to space [7]. Only the space environment allows performing very long-range experiments of quantum communications and fundamental quantum physics.

This paper is organized as follows. Section 2 summarizes the main results of the ESA studies on quantum communications. These studies provided the ideas and concepts for the definition of the proposed Space-QUEST experiment (QUantum Entanglement for Space ExperimenTs) as presented in Section 3. The programmatic roadmap towards this experiment and the related technology development activities are described in Section 4. The potential impact of quantum communications on future space communication systems and on the evolution of global navigation space systems is discussed in Section 5. A number of quantum physics experiments that become only feasible using the added value of the space environment are also discussed. Space environment offers a unique environment compared to ground based experimental facilities (no disturbing influence of atmospheric turbulence, no birefringence/absorption effects like in optical fibers, microgravity conditions, etc.). Section 6 summarises the technological challenges and programmatic steps towards the implementation of the proposed Space-QUEST experiment.

2 ESA studies on quantum communications

Since 2002, the following studies have been funded under the General Studies Programme of the European Space Agency:

- Quantum communications in space (“QSpace”; 2002-2003. Contractors: Vienna University of Technology, Vienna University, QinetiQ and Ludwig Maximilian University)
- Accommodation of a quantum communication transceiver in an optical terminal (“ACCOM”, 2004. Contractors: Vienna University of Technology, Vienna University, Contraves Space and Ludwig Maximilian University)
- Experimental evaluation of quantum communications (“QIPS”, 2005-2007. Contractors: Max Planck Institute, Austrian Academy of Sciences, QinetiQ, University of Bristol, University of Padova, Contraves Space, TESAT and Carlo Gavazzi Space)

The main results and achievements of these studies are described in the following sections.

2.1 Quantum communications in space (“QSpace”)

The first objective of this study was to identify and investigate novel concepts for space communication systems based on the principles of quantum physics. Special emphasis was put on the areas related to quantum communications (quantum key distribution, quantum teleportation, quantum dense coding).

As a second objective, the study conceived several scientific experiments for the demonstration of fundamental principles of quantum physics which will benefit from the special environmental conditions in space, like the lack of atmospheric disturbance and absorption allowing very long propagation distances. The technical feasibility of the associated space infrastructure required to carry out those experiments was analyzed in this study.

As far as the communications aspects are concerned, Table 1 summarizes the main outcomes. Quantum communications allows the transfer of quantum information (i.e. the quantum state of a particle). However, it cannot be exploited for superluminal communications (i.e. beyond the speed of light), as it would violate causality as defined in special relativity. Nevertheless, quantum communications guarantees the distribution of random sequences of bits with a level of confidentiality that cannot be achieved by any classical means.

Applications	Benefits	Space application
Quantum key distribution (QKD) using single and entangled photons	Unconditional security = detection of eavesdropper	• Secure access to a satellite • Secure communications between gateways / ground stations • Secure satellite-to-satellite communication
Quantum state teleportation (QT)	Transfer of quantum information without disturbing the quantum information, but speed of light limit for classical information	• Quantum telecomputation for deep space missions • Global distribution of quantum entanglement and global quantum networks
Quantum dense coding (QDC)	Higher channel capacity	• Satellite telecommunications • Deep space missions
Quantum communication complexity (QCC)	Higher efficiency	• Deep space missions

Table 1. Summary of quantum communication protocols for space communications and space applications

2.2 Accommodation of a quantum communication transceiver in an optical terminal ("ACCOM")

The investigation of potential scenarios for a demonstration of quantum communications in space concluded that a space-to-ground (or a ground-to-space) experiment should be the first step towards a fully space-based experiment. Due to technical complexity, state-of-the-art technology, development costs and risks, it was recommended to first execute a space-to-ground experiment, which would already allow major scientific achievements. The selected scenario envisaged establishing free-space optical communication links between a space-based transceiver and several ground-based transceivers located at spatially separated ground stations.

Such a scenario will to a large extent take advantage of optical technologies already developed and used in classical free-space optical communications links between satellites. With the successful SILEX experiment (optical data transmission between SPOT-4 and ARTEMIS satellites) in 2001 [8] ESA has demonstrated to be at the forefront of such technology developments.

Considering duly the status of already developed optical communications hardware this study investigated first which subsystems of a classical optical terminal could be re-utilized or removed, and which subsystems needed to be optimised or modified to best accommodate a quantum communication transceiver (i.e. the hardware needed for carrying out quantum communications experiments).

A functional block diagram of the quantum communications terminal identifying the subsystems of an optical terminal for classical free-space optical communications and those subsystems specific for the quantum communication transceiver is depicted in Figure 1.

A complete space-based quantum communications terminal was designed (including classical and quantum subsystems) which can perform downlink as well as uplink quantum experiments. The design of existing space-qualified and/or space-designed hardware (e.g., telescope, pointing / acquisition / tracking mechanisms, acquisition sensor, etc.) was adapted for this purpose. This communications terminal is equipped with two telescopes, each with an independent pointing/acquisition/tracking subsystem capable of distributing entangled photon pairs from space towards two widely separated optical ground stations [9]. The quantum communications transceiver includes an entangled photon source, weak pulse laser sources, single photon detection modules and the associated optics for manipulating and analysing single photons.

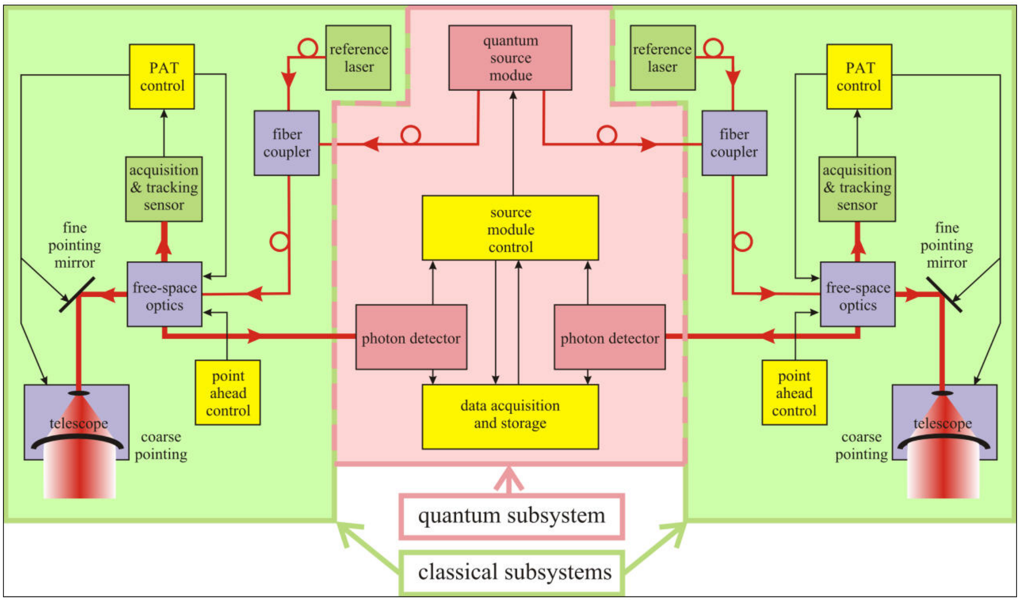


Figure 1. Generic block diagram of the quantum communications terminal outlined for space-ground experiments

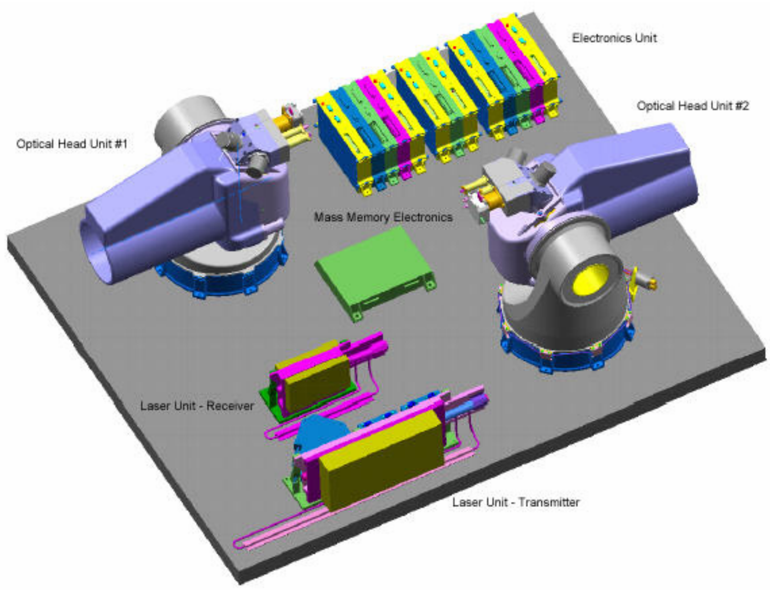


Figure 2. Design of a complete space-based quantum communication payload including the quantum communication transceiver and two classical optical terminals independently controlled for the demonstration of quantum communications from space to two ground stations

2.3 Experimental evaluation of quantum communications ("QIPS")

Within 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 addition, a multipurpose short-term proof-of-concept experiment was defined and its detailed design carried out. The flexible and modular design of this ground-based proof-of-concept demonstrator ensured compatibility with the testing of several phenomena (single photon channel, testing of atmospheric effects, entanglement distribution).

A major part of this study focused on the execution of basic ground-to-ground quantum communications experiments using the abovementioned demonstrator, which 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 were carried out on the Canary islands, between the Observatorio Roque de los Muchachos on the island of La Palma (transmitter's location) and the Observatorio del Teide on the neighbouring island of Tenerife (receiver's location), 144 km apart. On La Palma the transmitter generated entangled photon pairs, and sent one photon towards a 1-meter-diameter receiver telescope located on Tenerife, whilst keeping the other for correlation analysis. Figure 3 depicts a schematic layout of the inter-island experiment. A picture of the receiver telescope is shown in Figure 4.

When comparing the correlations between the coincident detections in Tenerife and La Palma, it became evident that the photons remained entangled even after having travelled 144 km through the atmosphere [10]. Decoherence effects caused by atmospheric turbulence (e.g. random rotation of single photon's polarization, time-of-arrival jitter due to fluctuations of the optical path) were negligible as predicted by theory. In addition to the pure diffraction loss the atmosphere introduces a certain amount of attenuation (absorption, scattering, beam wander, beam spreading and scintillation effects), which obviously needs specially engineered countermeasures, but entanglement is preserved. The established 144 km quantum channel through the atmosphere can be considered a worst case scenario for a space-to-ground link from the atmospheric turbulence point of view. As a matter of fact the overall end-to-end loss of this horizontal atmospheric link and a link between a LEO satellite and a ground receiver is very similar, 25 to 30 dB.

In addition, the implementation of a decoy-state protocol with a weak pulse laser source and with loss values representative of a space-to-ground link (up to 30dB) was experimentally proven [11]. Weak pulse laser sources emulate single photon sources by attenuating the optical power of a standard laser down to the single photon regime (in average). Attenuated lasers are technologically much simpler than entangled photon sources or true single photon sources, but, due to the non-zero probability of having more than one photon per pulse, may give the opportunity for information leakage. The implementation of the decoy-state protocol guarantees the security of QKD with weak coherent laser pulses against an eavesdropper's attack even over such large link distances. With state-of-the-art technology, the key rate achieved with the weak pulse laser source was an order of magnitude higher than with the entangled photon source.

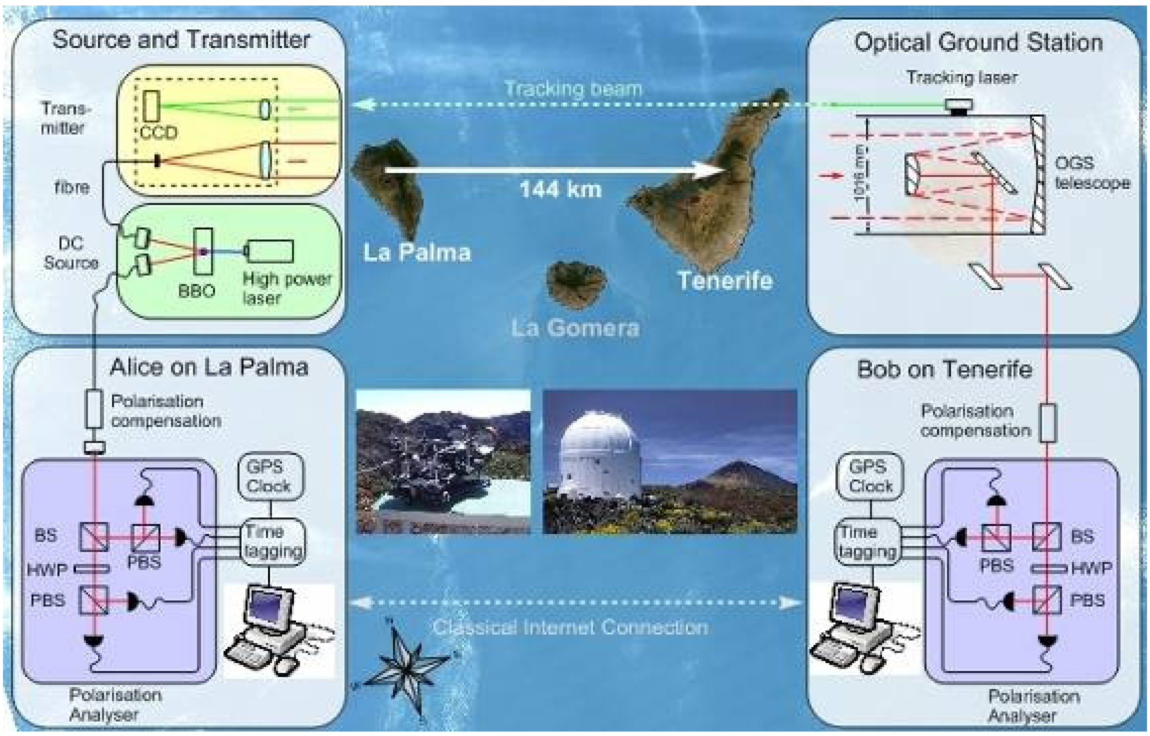


Figure 3. Inter-island quantum communication experiment between La Palma and Tenerife [10]

Figure 4. The telescope of ESA's optical ground station (OGS) on Tenerife used for the experiments is a Zeiss 1 meter Ritchey-Chrétien/Coudé telescope supported by an English mount [12]

3 Space-QUEST

Based on the results obtained in the previous studies, a European research consortium led by Vienna University submitted in 2004 the Space-QUEST proposal (QUantum Entanglement for Space ExperimenTs) in the frame of the "Announcement of Opportunity for Life and Physical Sciences and Applied Research Projects 2004" for the ELIPS-2 programme of the European Space Agency [13]. The consortium partners of Vienna University are Vienna University of Technology, Austrian Academy of Sciences, Max Planck Institute, University of Padova, Matera Laser Ranging Observatory and Observatoire de la Côte d'Azur.

The ELIPS-2 programme is promoting life and physical sciences and applications using the European Columbus module on the International Space Station (ISS). The evaluation committee of the ELIPS-2 programme rated the scientific and technological case of Space-QUEST as "outstanding" and strongly recommended the implementation of this proposal.

3.1 Mission concept

The objectives of the Space-QUEST experiment are to demonstrate, for the first time:

- Unconditional secure global distribution of cryptographic keys from space, based on novel quantum communication techniques (QKD)
- Fundamental quantum physics principles beyond the capabilities of earth-bound laboratories by utilizing the added value of space environment.

The experiments will establish free-space optical communication links between a quantum communications terminal on the ISS and optical receiver(s) in one or more ground stations.

Two options have been assessed for the payload on-board of ISS with one (or two) telescopes of 10-15 cm diameter aperture. The mass estimate for the quantum communications terminal shown in Figure 2 (i.e. in dual-telescope configuration) is <100 kg, with a peak power consumption of <250 W [14]. The proposed payload is compliant with the mass/power/volume figures and accommodation requirements given for the external ISS pallet of the European Columbus module.

From the scientific point of view the dual-telescope configuration with two independently controlled telescopes is preferred, as it allows to execute for the first time a test of non-local quantum correlations (i.e. Bell type experiments) between two ground stations physically separated by more than 1000 km. Such distances are far beyond the possibilities of any ground-based experiment with current fibre and detector technologies.

An artistic view of entanglement distribution from the ISS is given in Figure 5. Each photon of the entangled pair is transmitted to a different ground station. Quantum correlations are established between two ground stations, which are then used to generate an enciphering key for encrypting classical information to be transmitted over a classical, non-secure communication channel (e.g. RF link, optical fibre).

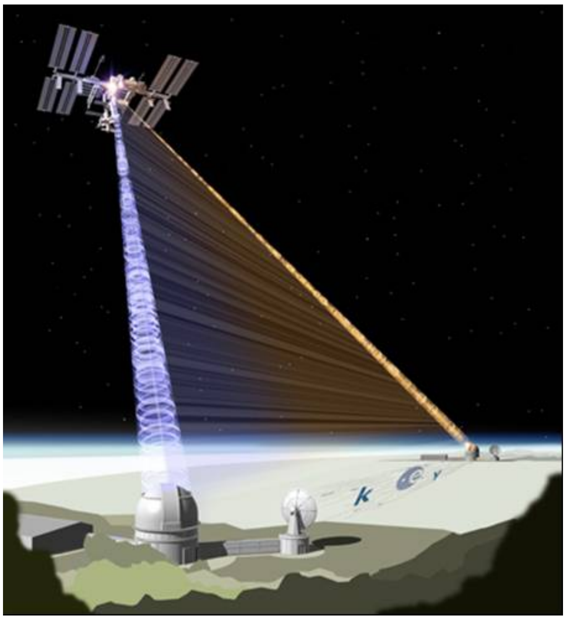


Figure 5. Distribution of pairs of entangled photons using the International Space Station (ISS). Entangled photon pairs are simultaneously distributed to two separated locations on Earth thus enabling both fundamental quantum physics experiments and novel applications such as quantum key distribution

3.2 Orbit trade-off

Several orbits were investigated for the Space-QUEST experiment. For the trade-off, a figure of merit was defined as the average key length per day normalized to the average key length per day in LEO orbit. This figure of merit depends on the orbit type, the minimum elevation angle imposed by optical ground station's constraints and the link acquisition time (i.e. time needed for establishing an optical link between the space terminal and the ground counterpart). In turn, the type of orbit restricts the number of available links per day, the duration of these links and the link distance. The figure of merit does not depend on the timing of the experiment (i.e. whether the experiments are carried out during day and night or only during night).

The calculated figure of merits are compared in Figure 6 for the case of a single downlink and in Figure 7 for the case of simultaneous double downlinks from the ISS to two ground receivers. For the single downlink scenario with the transmitter placed in LEO orbit (on the ISS), the average key length per day is 3.7 and 5.7 times longer than for a transmitter in GEO and MEO orbit, respectively. For the simultaneous double downlink scenario the comparison is even more in favour of the LEO orbit.

The achievable average key length per day depends on the link acquisition time, especially for the case of the LEO orbit. Figure 8 illustrates this dependency. As the parameter represented is normalized with respect to the average key length per day in LEO orbit, the figure of merit for the LEO orbit remains constant, whereas for the MEO and GEO orbits it improves when increasing the link acquisition time. For typical link acquisition times <60 sec the LEO orbit is clearly the optimum choice. Above 90 sec, the figure of merit in MEO and GEO orbits improves sharply.

The experiments based on the distribution of entangled photon pairs over very long distances requires simultaneous double downlinks from the ISS to two separate ground stations. Thus, placing the quantum communications terminal in LEO orbit performs best for the Space-QUEST experiment.

3.3 Platform alternatives to ISS

The ISS is presently the baseline for the implementation of the Space-QUEST experiment. However, the proposed Space-QUEST experiment is, by no means, restricted to the ISS. In fact, a survey of alternative platforms indicates that there are several European and non-European space platforms in LEO orbit available (e.g. Resurs-DK1), which could accommodate the complete quantum communications terminal as proposed in Space-QUEST (Figure 2).

Furthermore, additional smaller platforms become feasible (e.g. of the Proba type), if a descoping of the experiment objectives is acceptable allowing a reduction of mass, size and power consumption of the quantum communication payload. Several reduced quantum communication payloads have been outlined in accordance with descoped mission objectives.

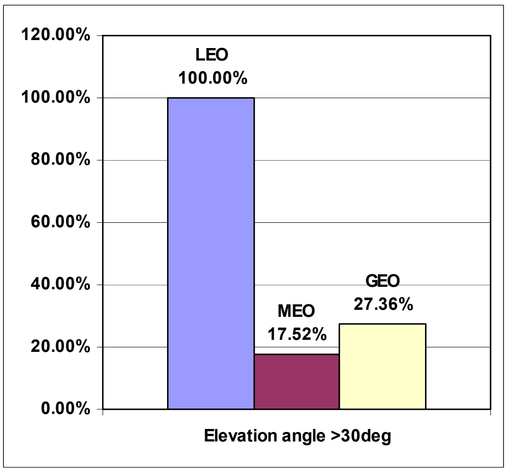


Figure 6. Figure of merit of QKD (average key length normalized to LEO case) versus type of orbit for the scenario of single downlink from the ISS to one optical ground station

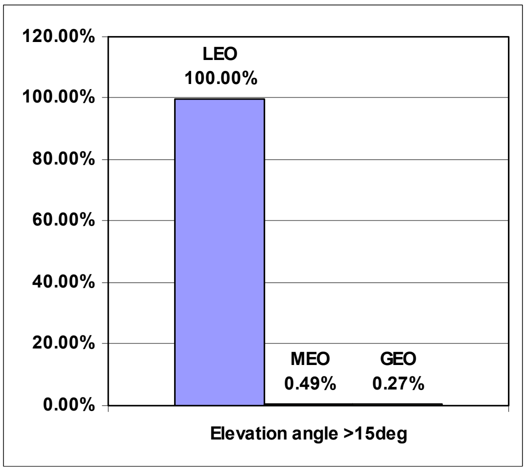


Figure 7. Figure of merit of QKD (average key length normalized to LEO case) versus type of orbit for the scenario of simultaneous double downlinks from the ISS to two separated optical ground stations

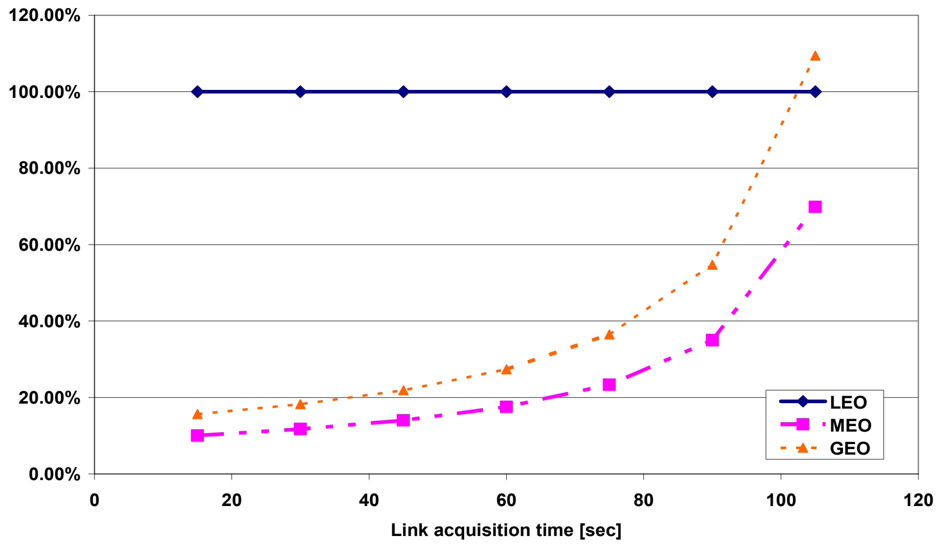


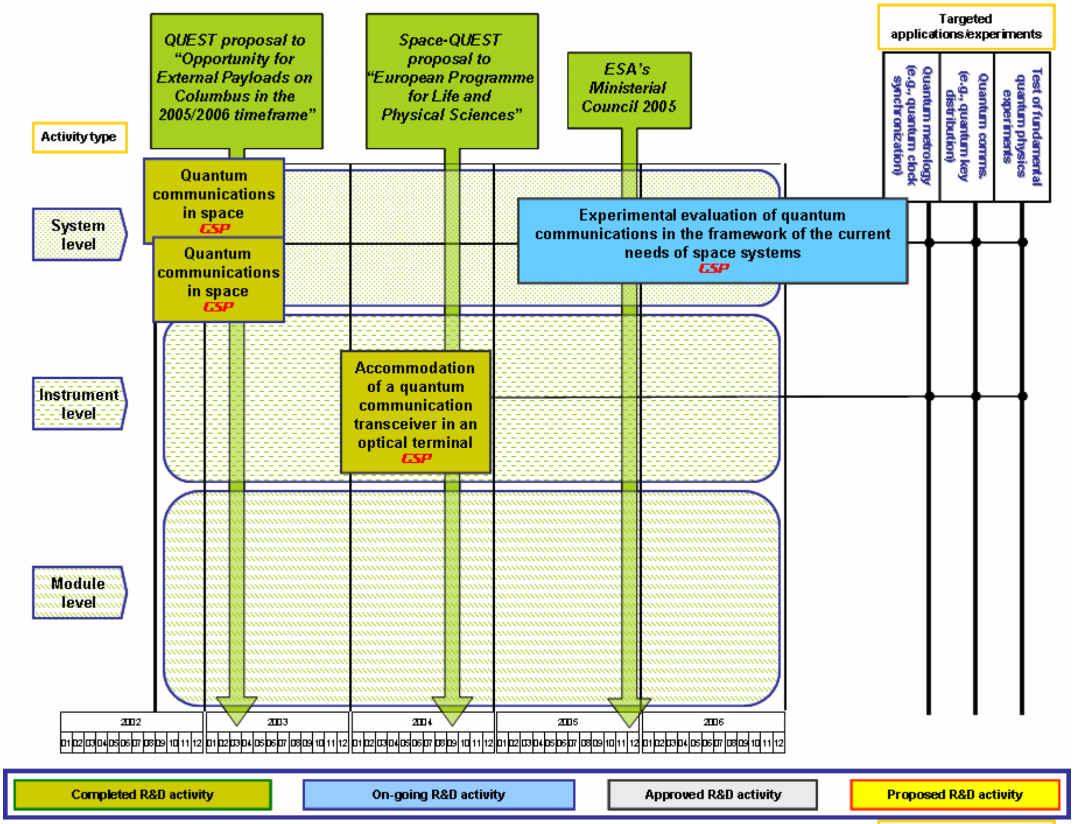
Figure 8. Figure of merit of QKD (average key length normalized to LEO case) versus link acquisition time for different types of orbits (case of single downlink from the ISS to one optical ground station)

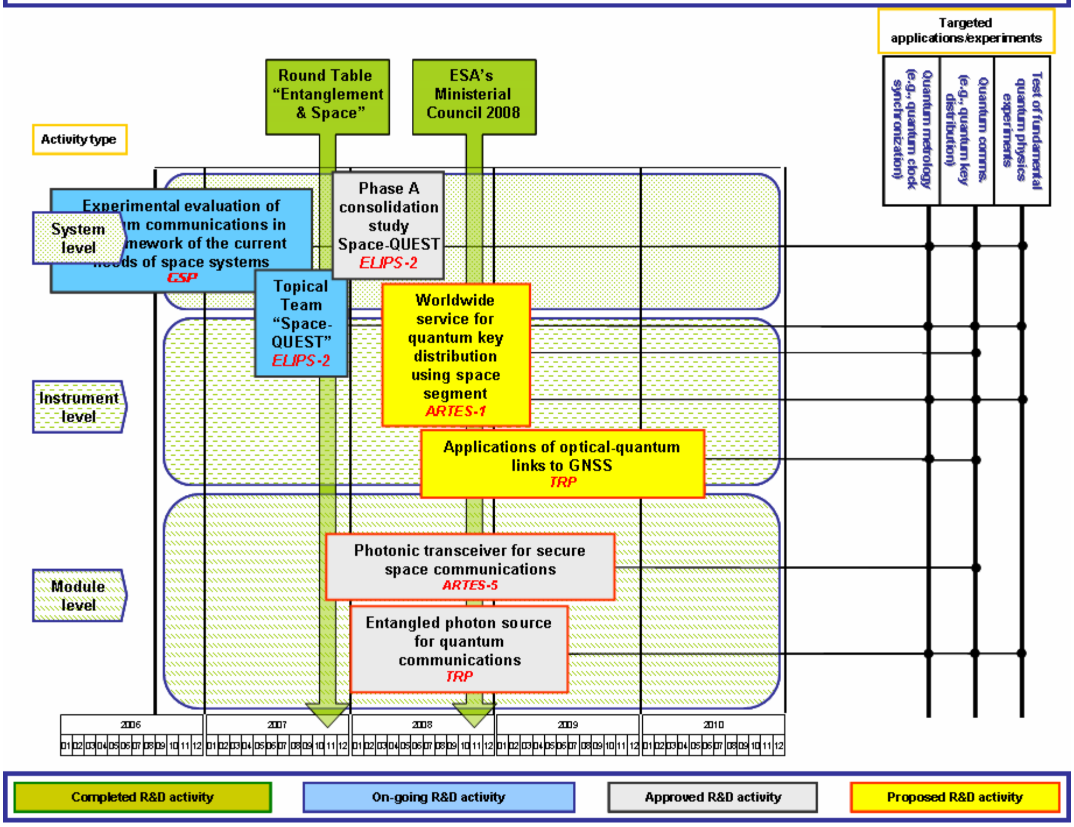
4 Programmatic aspects towards a flight demonstration

4.1 Programmatic roadmap

The proposed programmatic roadmap for the implementation of the Space-QUEST experiment on the ISS is presented in Figure 9. Activities are split into system, instrument and module levels. The status of each activity (e.g. completed, on-going, approved and proposed) is distinguished by colour. This roadmap encompasses all development activities from the first studies initiated in 2002 until the envisaged launch by end of 2014. The duration of the Space-QUEST experiment is estimated to be 1 year.

The results of the Phase-A consolidation study will be available by mid 2008. Hardware pre-developments will be executed between 2008 and 2010 to bring the maturity of the technology up to TRL 3 (Technology Readiness Level). Critical modules (entangled photon source and overall photonic transceiver) will be completed by end of 2009. Additional breadboard developments, mainly for the adaptations of the classical subsystems of the optical terminal, will be finalized by end of 2010.


Targeted applications/experiments
Quantum metrology (e.g., quantum clock synchronization)
Quantum comms. (e.g., quantum key distribution)
Test of fundamental quantum physics experiments
QUEST proposal to "Opportunity for External Payloads on Columbus in the 2005/2006 timeframe"
Space-QUEST proposal to "European Programme for Life and Physical Sciences"
ESA's Ministerial Council 2005
Activity type
System level
Instrument level
Module level
Quantum communications in space GSP
Quantum communications in space GSP
Experimental evaluation of quantum communications in the framework of the current needs of space systems GSP
Accommodation of a quantum communication transceiver in an optical terminal GSP
2002
2003
2004
2005
2006
Completed R&D activity
On-going R&D activity
Approved R&D activity
Proposed R&D activity


Targeted applications/experiments
Quantum metrology (e.g., quantum clock synchronization)
Quantum comms. (e.g., quantum key distribution)
Test of fundamental quantum physics experiments
Round Table "Entanglement & Space"
ESA's Ministerial Council 2008
Activity type
System level
Instrument level
Module level
Experimental evaluation of quantum communications in the framework of the current needs of space systems GSP
Phase A consolidation study Space-QUEST ELIPS-2
Topical Team "Space-QUEST" ELIPS-2
Worldwide service for quantum key distribution using space segment ARTES-1
Applications of optical-quantum links to GNSS TRP
Photonic transceiver for secure space communications ARTES-5
Entangled photon source for quantum communications TRP
2006
2007
2008
2009
2010
Completed R&D activity
On-going R&D activity
Approved R&D activity
Proposed R&D activity

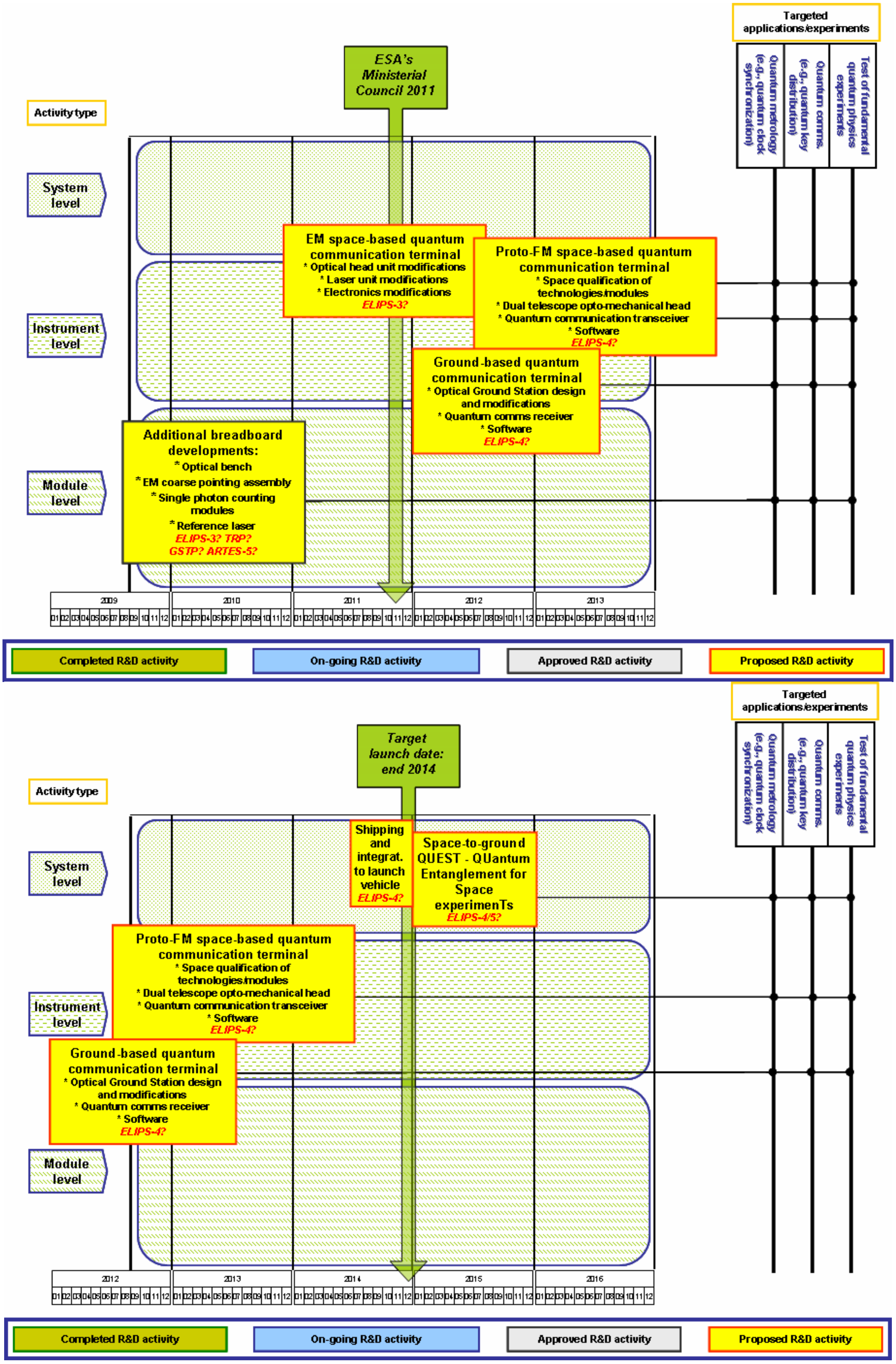


Figure 9. Programmatic roadmap of Space-QUEST towards a flight experiment on the International Space Station

Developments at EM level (engineering model) will be initiated early 2011. By mid 2012 the space-based quantum communications terminal will have attained TRL 4. The development of the proto-flight model (PFM) of the complete quantum communications terminal (including both hardware and software) will start mid 2012 with a delivery date ready for shipping and integration by mid 2014 (TRL 6 successfully achieved). The development of the ground-based quantum communication receivers (hardware and software parts) and the modifications in the optical ground stations needed to accommodate the ground-based receivers will be carried out between 2012 and mid 2013.

At present, the most immediate steps are:

- Organization of the Round Table "Entanglement & Space" in November 2007, in combination with the final presentation of the on-going QIPS study
- Initiation of critical technology pre-developments (the quantum communication transceiver)
- Preparation of a consolidated Space-QUEST proposal for the next ESA's Ministerial Council in 2008

4.2 Description of technology development activities

The main objectives of each of the technology development activities outlined in the programmatic roadmap above are summarized in Table 2.

Activity title	Status	Starting date	Duration (months)	Activity description
Topical Team "Space-QUEST"	On-going	2Q 2007	6	To support the teaming-up of European R&D groups in the field of quantum communications and the interaction with industrial partners to improve the scientific return of the proposed Space-QUEST experiment on the ISS.
Phase-A consolidation study Space-QUEST	Approved in ELIPS-2	4Q 2007	8	To carry out the Phase-A consolidation study of Space-QUEST, including the detailed design of the experiment and its associated infrastructure. This study shall assess in detail the technical feasibility of the experiment and shall carry out the definition and the design of the required interfaces for the integration of a quantum communications terminal (QCT) on the external pallet of the Columbus module on the ISS, resulting in a "consolidated" QCT design.
Photonic transceiver for secure space communications	Approved in ARTES-5	4Q 2007	24	To design, develop and test an elegant breadboard of a photonic quantum communications transceiver to provide unconditional security to space communications. This elegant breadboard shall validate the feasibility/reliability/robustness of the key building blocks of a quantum communication transceiver (e.g. entangled photon source module, faint laser source module, optical components for photon manipulation)
Entangled photon source for quantum communications	Approved in TRP	1Q 2008	18	To design, develop and test (in laboratory environment) a breadboard for the validation of novel concepts for a highly efficient entangled photon source module that potentially could be used in space.
Worldwide service for quantum key distribution using space segment	Proposed in ARTES-1	2Q 2008	12	To assess and design a service for distributing secure quantum keys using the space segment in order to achieve true worldwide coverage. The resulting "hybrid" network combining secure short-range ground connections and secure long-range satellite connections shall be optimized in terms of efficiency and costs (i.e. minimum required resources) without jeopardizing

				security aspects.
Applications of optical-quantum links to GNSS	Proposed in TRP	3Q 2008	24	To investigate the potential of optical-quantum links for next generation navigation systems and to design an optical-quantum terminal (i.e. optical terminal with an integrated quantum transceiver, as part of a complete optical-quantum intersatellite link and/or space-ground link). The proposed design of an optical-quantum terminal shall be validated by means of a "representative" proof-of-concept demonstrator.
Additional breadboard developments of a quantum communications terminal	Proposed	3Q 2009	18	To design, develop and test (in laboratory environment) a breadboard for the validation of a complete quantum communications terminal (QCT), including the development of highly isolated optical bench, dual PAT subsystem, single photon detection module, etc.
EM space-based quantum communications terminal	Proposed	1Q 2011	18	To design, develop and test (in laboratory environment) an engineering model of a quantum communications terminal (EM QCT). This EM QCT shall include an upgraded EM photonic quantum communication transceiver. Initial environmental testing shall be carried out.
Ground-based quantum communications terminal	Proposed	1Q 2012	18	Firstly, to design and implement the needed modifications in the selected optical ground stations for Space-QUEST. Secondly, to design, manufacture and test the ground-based quantum communication breadboards, compatible with the interface and the operational requirements of the optical ground station(s), where the breadboards shall be placed (e.g. ESA's OGS on Canary islands).
Proto-FM space-based quantum communications terminal	Proposed	3Q 2012	24	To design, develop and test a Proto-FM of the quantum communications terminal (Proto-FM QCT) capable of simultaneously distributing entangled photon pairs to 2 separated receiver terminals (i.e. 2 Optical Ground Stations) . In addition, the QCT shall be capable of receiving and detecting single photons (only 1 receiver).
Space-to-ground QUEST experiment	Proposed	1Q 2015	12	First ever space-to-ground demonstration of innovative quantum communication schemes (e.g. quantum cryptography for space applications) and fundamental tests of quantum physics. The experiment could consist in a space-based quantum communications terminal placed on the ISS distributing single photons and entangled photons to one or several Optical Ground Stations.

Table 2. Description of the technology development activities for Space-QUEST

5 Future space applications after Space-QUEST

5.1 Telecommunications & Navigation

After the successful SILEX flight demonstration, ESA and several European National Agencies (DLR, SSO, French MOD) have maintained the effort in developing the next generation of optical communications terminals with reduced mass, size and power consumption, and increased data transmission rate, aiming at potential optical data relay applications between future LEO satellites / aircrafts and GEO satellites. The integration of a quantum communication transceiver in next generation optical terminals will broaden the range of applications beyond optical data relay. In particular, the capability of QKD is perceived as highly attractive for those space applications, where a very high level of security in key management is compulsory:

- Secure distribution of keys for satellite remote access (e.g. for secure TT&C links between satellite and control ground stations)
- Satellite systems (e.g. Galileo, GMES)
- Secure distribution of cryptographic keys at a global (i.e. worldwide) scale via the space segment (e.g. for secure communications between separated end users) to implement a truly global quantum network
- Secure intersatellite links

Besides, entanglement distribution might be of use for synchronizing isolated clocks for navigation purposes (i.e. quantum clock synchronization) [15]-[16], or it could be exploited to efficiently communicate with deep space probes (e.g. quantum communication complexity, quantum telecomputation). These applications are presently under consideration.

Although the orbit trade-off presented in Section 3.2 concludes that the LEO orbit is the optimum choice for Space-QUEST, this may not necessarily remain valid, when considering the implementation of an operational service for the distribution of cryptographic keys. Table 3 summarizes additional aspects to be taken into account for the orbit selection. As a result of this system analysis, the GEO orbit constitutes a good alternative to the LEO orbit for an operational service, as it is almost independent of the link acquisition time while it greatly reduces pointing requirements both of the space-based quantum communications terminal and of the ground stations. The possibility of an eavesdropper's attack taking advantage of the large link loss variation in the LEO orbit disappears for MEO and GEO orbits.

5.2 Science

Space-QUEST will carry out Bell type experiments at distances unfeasible using solely ground-based laboratories. The standard quantum model predicts no limit for the range of non-local quantum correlations, but this remains still to be experimentally proven. Space offers the possibility of "unlimited" long paths in vacuum (only diffraction loss, no absorption loss in atmosphere or optical fiber, unobscured line-of-sight), and therefore constitutes an ideal channel to experimentally challenge the limits of entanglement (if there are any).

Additionally, by exploiting the possibilities of distributing quantum entanglement with photons among several spacecrafts, a wide variety of long-term experiments can be envisioned [17], [18], including:

- Bell type experiments to demonstrate quantum correlations over astronomical distances

	LEO	MEO	GEO
Average key length per day (normalized to LEO)	100%	~15%	~30%
Link distance variation	~300%	~5%	~0%
Average gap duration between consecutive links (night operation only)	~1 day	~1 day	~0.5 day
Maximum gap duration between consecutive links (night operation only)	<15 days	< 22 days	~0.5 day
Pointing complexity of space-based quantum communications terminal	High	Medium	Low
Pointing complexity of optical ground station	High	Medium	Low
Sensitivity to link acquisition time	Critical	Uncritical	Independent
Instantaneous ground coverage	<1%	~30%	~33%
Total ground coverage	~100%	~100%	~33%

Table 3. Orbit trade-off for an operational key distribution service via satellite

- Tests of different models considering the collapse of the wave function as a physical process
- Influence of space-time fluctuations on decoherence
- Tests concerning special relativistic and general relativistic effects on quantum entanglement
- Tests of Lense-Thirring effect and Goedel's cosmological model using entanglement-enhanced interferometry
- Wheeler's delayed choice experiment
- Quantum teleportation in space

6 Conclusions

The Space-QUEST experiment will be the first step towards a worldwide network for quantum communications. Moving into space enables photonic entanglement to become a physical resource available for quantum experiments (for QKD and beyond) at a global scale. Space-QUEST will validate the key technologies of a quantum communication transceiver (e.g. entangled photon source, weak pulse laser source, single photon counting modules) and will accomplish the first-ever demonstration in space of quantum-based telecom applications (e.g. QKD) and fundamental tests on quantum physics (e.g. Bell-type experiment at distances over 1000 km). Space offers extremely long propagation paths to explore the limits of the validity of quantum physics principles.

The programmatic roadmap of Space-QUEST has been presented in detail and it is compatible with a launch date by end of 2014. ESA's feasibility studies on the potential use of quantum communications in space started in 2002. The recently achieved inter-island demonstration allows ESA to take a step closer to exploiting entanglement as a way of communicating with satellites with total security. The LEO orbit turned out to be the optimum choice for the demonstration of Space-QUEST. Nevertheless, for an operational distribution service of cryptographic keys the GEO orbit represents an attractive option, especially when other system level aspects are taken into account. Technology developments for Space-QUEST will benefit from synergies with on-going European developments in free-space optical communications. On the long term, the integration of a quantum communication transceiver as an embedded system of a complete optical communications terminal can be envisaged.

In view of the high interest of the scientific community in Space-QUEST and its potential role in future space telecommunications, navigation and science missions, ESA is currently organizing several events (e.g. Round Table "Entanglement & Space", 1st Colloquium Scientific and Fundamental Aspects of the Galileo Programme [19]) to prepare a consolidated Space-QUEST proposal for the next ESA's Ministerial Council in 2008.

References

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

[2] N. Gisin et al., "Quantum Communication", Nature Photonics Vol. 1, No. 3, 165 (2007).

[3] R.J. Hughes et al., "Quantum cryptography for secure satellite communications," IEEE Aerospace Conference, 1803 Vol. 1, pp.191–200 (2000).

[4] J. G. Rarity et al., "Ground to satellite secure key exchange using quantum cryptography," New Journal of Physics 4, 82.1–82.21 (2002).

[5] M. Pfennigbauer et al., "Free-Space Optical Quantum Key Distribution using Intersatellite Links", Proceedings of the CNES - Intersatellite Link Workshop (2003).

[6] M. Aspelmeyer et al., "Long-distance quantum communication with entangled photons using satellites," IEEE J. Select. Topics Quantum Electron. 9, pp. 1541–1551 (2003).

[7] M. Aspelmeyer et al., "Quantum Communications in Space: Final Report", ESA Contract 16358/02/NL/SFe (2003).

[8] T. Tolker-Nielsen et al., "In-orbit test result of an operational optical intersatellite link between ARTEMIS and SPOT4 (SILEX)", Proc. SPIE 4635, 1 (2002).

[9] M. Pfennigbauer et al., "Satellite-based quantum communications terminal employing state-of-the-art technology", Journal of Optical Networking 4, 549-560 (2005).

[10] R. Ursin et al., "Entanglement-based quantum communication over 144 km", Nature Physics 3, pp. 481-486 (2007).

[11] T. Schmitt-Manderbach et al., "Free-Space Decoy State Quantum Key Distribution over

144 km", Physical Review Letters, PRL 98, 010504 (2007).

[12] R. Czichy et al., "Design of an optical ground station for in-orbit check-out of free space laser communication payloads", SPIE, Vol. 2381, pp. 26–37 (1995).

[13] European Science Foundation, "Scientific Perspectives for ESA's Future Programme in Life and Physical sciences in Space", http://www.esf.org/publication/209/Obernai2005Finalcorrected.pdf (2005).

[14] M. Pfennigbauer et al., "Accommodation of a quantum communication transceiver in an optical terminal: Final Report", ESA Contract 17766/03/NL/PM (2005).

[15] Josza et al., "Quantum Clock Synchronization Based on Shared Prior Entanglement", Physical Review Letters, PRL 85, 2010 (2000).

[16] C.J. de Matos et al., "Towards Quantum Space Systems", to appear in Proceedings of the 1st Colloquium on Scientific and Fundamental Aspects of the Galileo Programme (1st-4th October 2007).

[17] R. Kaltenbaek et al., "Proof-of-concept experiments for quantum physics in space", Proc. SPIE 5161, 252 (2004).

[18] J.G. Rarity et al., "Quantum communications in space", Proc. SPIE 5161, 240 (2004).

[19] 1st Colloquium on Scientific and Fundamental Aspects of Galileo, http://www.congrex.nl/07a06/ (1st-4th October 2007).