# Quantum Transceiver for secure Space Communications

Arnaud GARDELEIN[1], Marc JOFRE[1], Gabriel MOLINA-TERRIZA[1,2], Morgan W. MITCHELL[1], Juan PEREZ[1], Valerio PRUNERI[1,2], Eusebio BERNABEU[3], Luis Miguel SANCHEZ-BREA[3], Waldimar AMAYA[4], José CAPMANY[4], Rupert URSIN[5,6], Thomas JENNEWEIN[5,6], Laura PEÑATE[7], Francisco GUTIERREZ[7], Jose L. SAN JUAN[8], Javier MORENO[8]

1. ICFO, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain
2. ICREA-Institució Catalana de Recerca i Estudis Avançats, 08010, Barcelona, Spain
3. Departamento de Optica, Universidad Complutense de Madrid,Facultad de Ciencias Físicas. Ciudad Universitaria. 28040 Madrid, Spain.
4. Institute of Telecommunications and Multimedia Applications (ITEAM), Universidad Politécnica de Valencia, Spain
5. Institute for Quantum Optics and Quantum Information (IQOQI, Austrian Academy of Sciences, Austria
6. Faculty of Physics, University of Vienna, Austria
7. ALTER Technology Group, Spain
8. LIDAX, Av. Cristobal Colón 16, Torrejon de Ardoz, Spain

Contact name: Valerio.Pruneri@icfo.es

## ABSTRACT:

We report on the development of a photonic transceiver for secure space communication, including an entangled photon source and a faint pulse laser source. Through the laws of Quantum Physics, it will allow the development of global communication with unprecedented security.

**Key words:** Photon entanglement, Decoy transmission, Quantum Key Distribution, Parametric down-conversion, Non-linear optics, Space applications

## 1.- Introduction

Quantum communications offers many advantages for secure data transmission, e.g. confidentiality, integrity, eavesdropper's detectability. Information is encoded in quantum bits (qubits), intrinsic physical properties, such as polarization of a photon. Quantum physics allows encoding information using the correlation between two or more particles (photons, atoms). Quantum Key Distribution (QKD) is one of the innovative methods of information processing that emerged from the properties of "superposition of states" and "entanglement".

QKD allows two (or more) parties to know when a communication channel is completely secure to exchange an encrypted key. QKD is used before classical information is transmitted over conventional non-secure communication channels like telephone lines, RF links and optical fibre networks. Since quantum physics laws state that a single particle like a photon cannot be split or cloned, it certifies the absolute security of communication.

Quantum communication channels however are limited on Earth. Optical fibre link losses and current photon-detector technology limit the maximum span length without using regeneration (amplification) to 100 km, while for free space transmission the limit is the visible horizon [1, 2]. Such problems are in principle nearly absent in space, and are less severe in ground to space links. In fact, quantum links in free space combined with fibre counterparts could extend secure communication between points on earth to a global level (Fig. 1). In addition space applications requiring secure link are numerous: remote access, communication between distant ground stations via space segment, positioning systems (GALILEO), etc....

Various proof-of-principle experiments have been already performed. For example, a 144 km free-space link between the two Canary Islands La Palma and Tenerife used the ESA's 1-meter-diameter receiver telescope to receive single photons [3, 4]. A satellite-to-Earth link was also simulated between the Matera-Laser-Ranging-Observatory (Italy) and the low-earth orbit (LEO) satellite Ajisai [5].

In this paper, we present a mandatory subsystem for quantum communication in space, a photonic transceiver capable of generating and detecting entangled photons as well as faint laser pulses, which we call Quantum Transceiver (QTxRx). The QTxRx has to fulfil highly demanding specifications for space applications, i.e. a total size < 200 x 150 x 100 $mm^3$, a mass < 3 kg and a peak total power consumption (including electronics) < 15 W as well as all the severe environmental requirements (vibration, shock temperature, radiation).

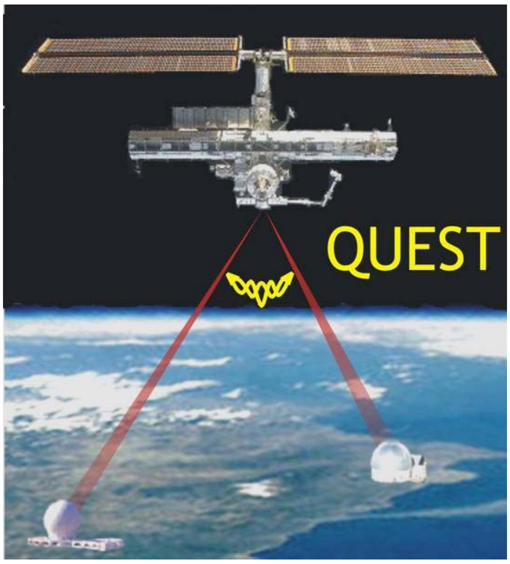


*Fig. 1. Distribution of pairs of entangled photons using the International Space Station (ISS). Entangled photon pairs are distributed to two separated places on Earth.*

## 2.- Quantum Transceiver (QTxRx) for space

The QTxRx is to be embedded aboard a LEO satellite, for example the International Space Station. As said in the introduction it is composed of two experiences of quantum cryptography based on single photon emission: 1) an entangled photon source (EPS) and 2) a faint pulse source (FPS) (Fig. 2). The EPS generates entangled photon pairs while the two FPS generate weak photon pulses. Both EPS and FPS can be used for transmitting from a LEO satellite to two separate ground stations either one common secure key simultaneously or two *different* secure keys consecutively.

The outputs of the sources are coupled together using an optical combiner. The photons are sent through space from the satellite to each Optical Ground Support Equipment (OGSE), where they are analyzed. In the case of simultaneous key transmission, one station reveals publicly to the other some random elements of the received key. If the elements match its proper key, then the key is secure. In the case of consecutive key transmission, one station sends a logical combination (XOR) of both keys to the other station. From this, one unconditionally secure key is computed.

Space environment add constraints like temperatures range, vibrations, radiations. Thus components have to be selected and tested for space qualification, especially for sensitive components like laser diodes and nonlinear crystals. For example, the only manufacturer of laser diode chips at 405 nm is Nichia, and such a component has never been used in space.

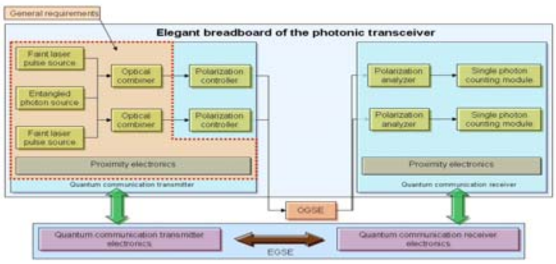


*Fig. 2. The QTxRx layout, incorporating the EPS, FPS, OGSE, EGSE and proximity electronics.*

## 3.- Entangled photon source (EPS)

Entanglement is widely described in quantum physics. Entangled particles are correlated, which means that modifying one property of one particle will affect also the pair-mate. The entangled states are generated by means of spontaneous parametric down-conversion (SPDC). The output photons are called by convention signal and idler. This means that an eavesdropper detecting one photon of a pair will modify the pair mate state thus revealing its presence when transmission results will be compared.

Some configurations have already been proposed by several teams [6-10]. The purpose of this project is to develop one of the existing sources for lab experiments into an integrated product compliant with space requirements, including physical dimensions, weight and power consumption. Selection criteria include optical performances, pump requirements, opto-mechanics. As a first iteration, non-collinear sources have been excluded because of the very low separation between the output cones which would require either a long structure or the use of mirrors into the optical path [6, 7]. Sources using periodically poled potassium titanyl phosphate (PPKTP) crystal are preferred to those using β-barium borate (BBO) because of efficiency.

Optomechanical tolerance analysis has to be conducted to determine the elements of each configuration which are sensitive to position or angle misalignments and would induce efficiency loss. To this end, pump beam should be numerically propagated to the non-linear crystal, as well as the signal and idler beams should be numerically back-propagated from the output coupling to the crystal centre. The efficiency is then calculated from the overlap between the pump and signal and idler beams.

## 4.- Faint pulse source for decoy

One protocol which provides full security of transmission of single photons using weak pulses is the so called Decoy State protocol [11-13]. Signal and decoy states are pulses containing a fixed average number of photons (e.g. 0.1, 1 and 10 photons). The decoy state should be identical in time, spectrum and amplitude to the signal state, so that an eavesdropper cannot distinguish between decoy and signal states. After transmission, the receiving station reveals detection events, and then emitting station broadcasts which states were signal or decoy. A careful analysis of received states will then detect with high probability an eavesdropper using a strategy based on photon number splitting.

It has been shown that three pulse levels and four different polarization states are enough to ensure transmission security. The FPS of QTxRx will send random levels at random polarization to both distant ground stations with a repetition rate at least of 10 MHz and a timing resolution of less than 1 ns.

## 5.- Conclusion (expected output ts)

As part of the SPACE-QUEST proposal, this project will be focused on the development of an integrated QTxRx. At the conference we will report on how the demanding technical specifications and environmental requirements drive the design, material procurement and fabrication of this subsystem, essential to achieve global secure communication.

*Acknowledgements*: This work is part of the ESA Artes-5 programme under the contract ESTEC 21460/08/NL/IA and is sponsored by the Spanish Ministry of Industry (CDTI) and Austrian FFG.

## *References*

[1] E. WAKS, A. ZEEVI, and Y. YAMAMOTO. *"Security of quantum key distribution with entangled photons against individual attacks"*. Physical Review A, 65, 52310, 2002

[2] H. TAKESUE, E. DIAMANTI, T. HONJO, C. LANGROCK, M. M. FEJER, K. INOUE, and Y. YAMAMOTO. *"Differential phase shift quantum key distribution experiment over 105 km fibre"*. New Journal of Physics, 7, 232, 2005.

[3] T. SCHMITT-MANDERBACH, H. WEIER, M. FÜRST, R. URSIN, F. TIEFENBACHER, T. SCHEIDL, J. PERDIGUES, Z. SODNIK, C. KURTSIEFER, J. G. RARITY, A. ZEILINGER, and H. WEINFURTER. *"Experimental demonstration of free-space decoy-state quantum key distribution over 144 km"*. Physics Review Letters, 98, 010504, 2007.

[4] R. URSIN, F. TIEFENBACHER, T. SCHMITT-MANDERBACH, H. WEIER, T. SCHEIDL, M. LINDENTHAL, B. BLAUENSTEINER, T. JENNEWEIN, J. PERDIGUES, P. TROJEK, B. OEMER, M. FUERST, M. MEYENBURG, J. RARITY, Z. SODNIK, C. BARBIERI, H. WEINFURTER, and A. ZEILINGER. *"Entanglement-based quantum communication over 144 km"*. Nature Physics, 3, 481 – 486, 2007.

[5] C. BONATO, R. URSIN, C. PERNECHELE, V. LUCERI, G. BIANCO, P. VILLORESI, T. JENNEWEIN, F. TAMBURINI, M. ASPELMEYER, A. ZEILINGER, and C. BARBIERI. *"Experimental verification of the feasibility of a quantum channel between space and earth"*, New Journal of Physics, 10:033038, 2008.

[6] P. G. KWIAT, E. WAKS, A. G. WHITE, I. APPELBAUM, and P. H. EBERHARD, *"Ultrabright source of polarization-entangled photons"*, Physical Review A 60, R773, 1999.

[7] MARCO FIORENTINO, CHRISTOPHER E. KUKLEWICZ, and FRANCO N. C. WONG, *"Source of polarization entanglement in a single periodically poled $KTiOPO_4$ crystal with overlapping emission cones"*, Optics Express, 13, 1, 127, 2005

[8] O. KUZUCU and F. N. C. WONG, *"Pulsed Sagnac source of narrow-band polarization-entangled photons"*, Physical Review A 77, 032314, 2008

[9] A. FEDRIZZI, T. HERBST, A. POPPE, T. JENNEWEIN and A. ZEILINGER, *"A wavelength-tunable fiber-coupled source of narrowband entangled photons"*, Optics Express, 15, 23, 2007

[10] P. TROJEK and H. WEINFURTER, *"Collinear source of polarization-entangled photon pairs at non-degenerate wavelengths"*, arXiv:0804.3799v1 [quant-ph], 2008.

[11] W.-Y. HWANG, *"Quantum key distribution with high loss: toward global secure communication"*, Physical Review Letters, 91, 057901 (2003).

[12] X. B. WANG, *"Beating the photon-number-splitting attack in practical quantum cryptography"*, Physical Review Letters 94, 23, 230503 (2005).

[13] H.-K. LO, X. MA, and K. CHEN, *"Decoy state quantum key distribution"*. Physical Review Letters 94, 230504, 2005.