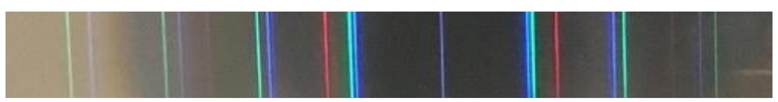
Quantum Communications in Space

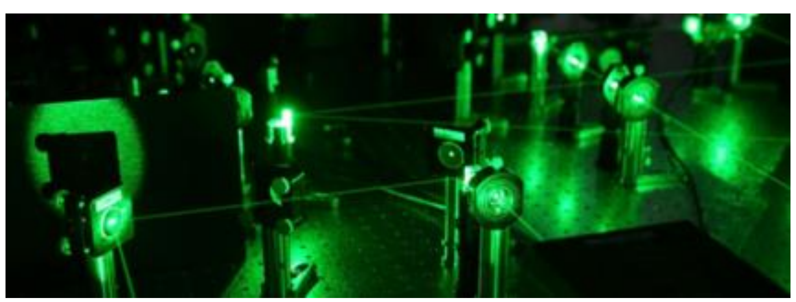
Paolo Villoresi

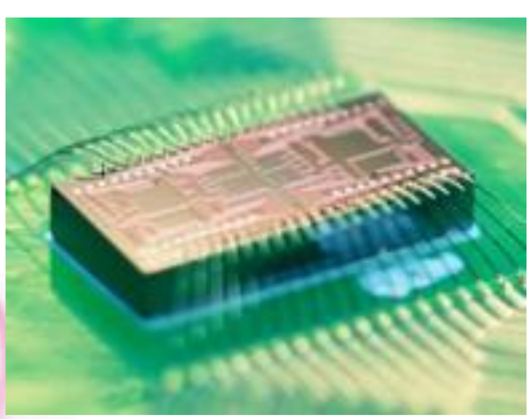
QuantumFuture Research Group
Università degli Studi di Padova, DEI, Padova, Italy

Committee on the Peaceful Uses of Outer Space
Scientific and Technical Subcommittee - Fifty-sixth session
ONU - United Nations - Vienna, 19 February 2019

Quantum Communications are part of Quantum Technologies



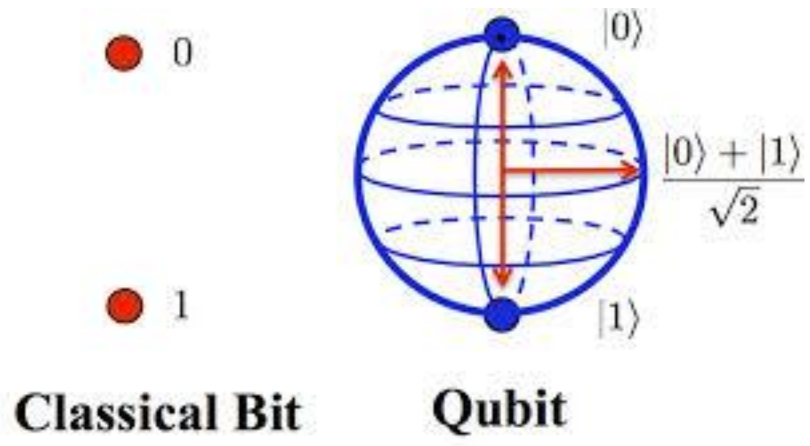


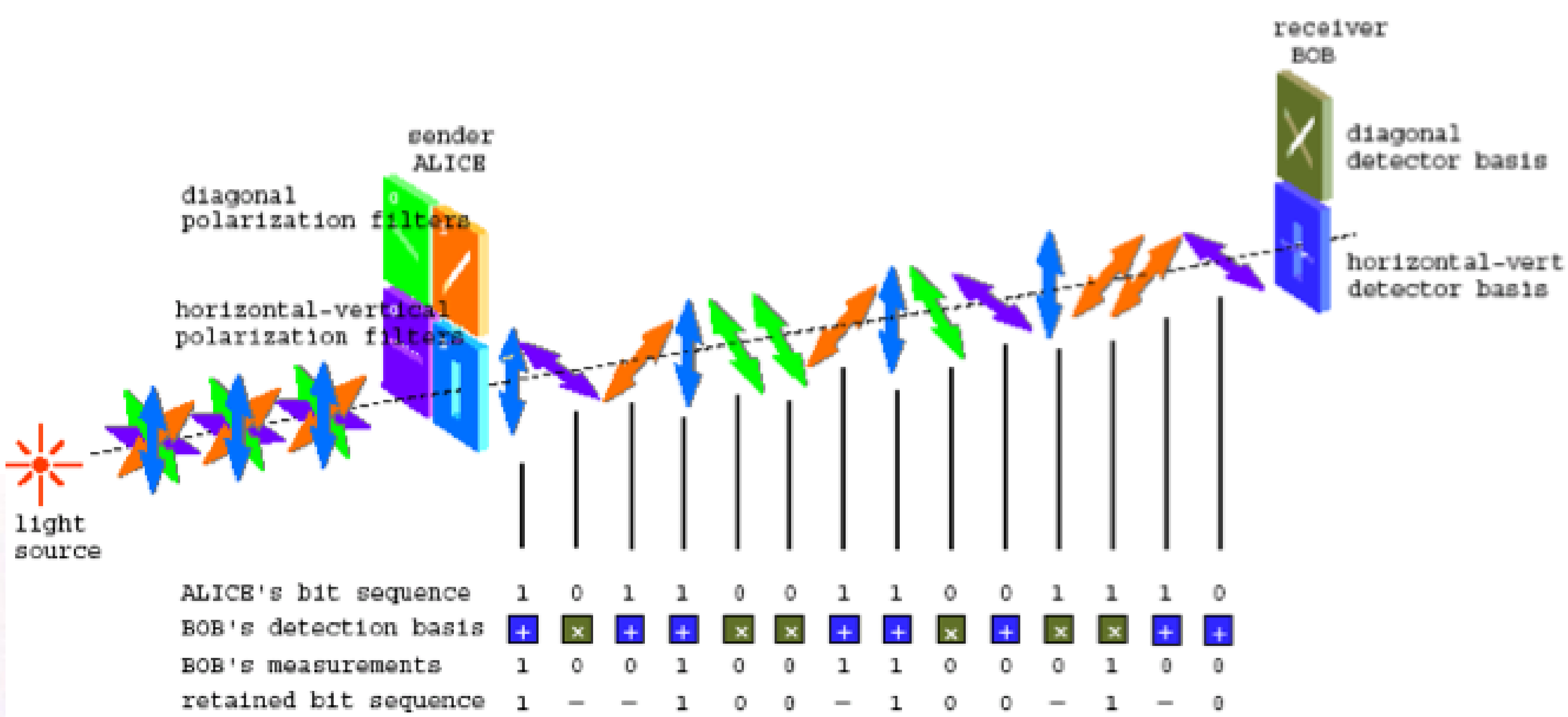


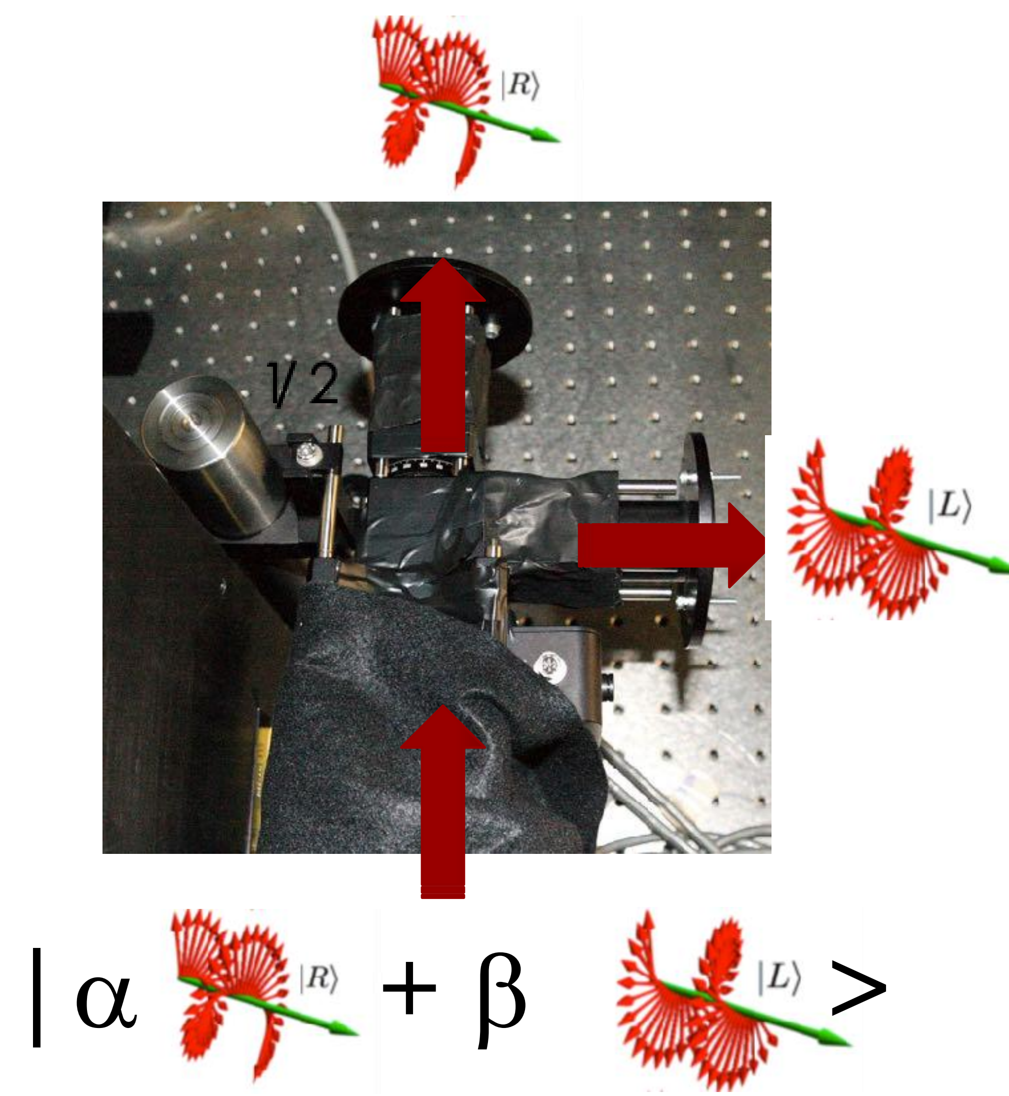
- *Quantum Mechanics*: the **interpretation of physical reality** in the **microcosmos**
  - provided the *understanding of atoms, molecules, fundamental particles, superconductivity*, etc.
  - allowed the *invention of transistors, lasers, integrated devices, etc.*
- **QM is now inspiring a *new age in the Theory of Information***, where **elementary particle are quantum bits, or qubits**, expanding the classical concept of the logical bit.
- **From a theory for understand Nature to a toolset for computing, communicate, measure..**

Quantum Communications are based on the sharing of qubits

- From the bit (binary unit) used in classical information systems, with Quantum Technologies it is used the qubit (quantum bit), embodied in a elementary (quantum) object as photons, electrons..
- Qubit peculiar feature: it is a superposition of alternatives, that in classical terms are antithetic It takes a complex number for the preparation of qubits
- The measurements gives a click on a particular output
- This create a correlation, useful in protocols as QKD, distributed quantum computing, metrology, ..

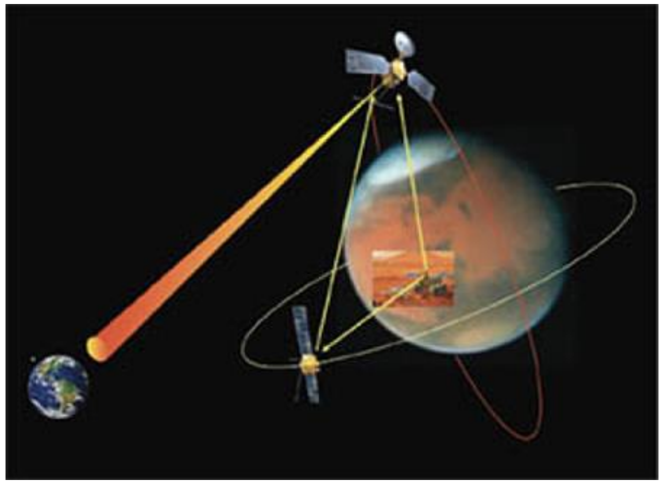


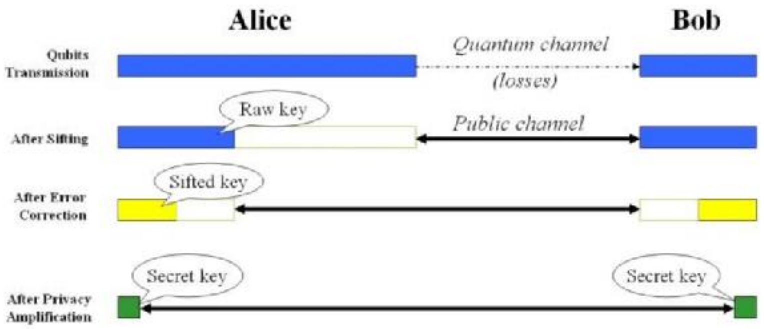


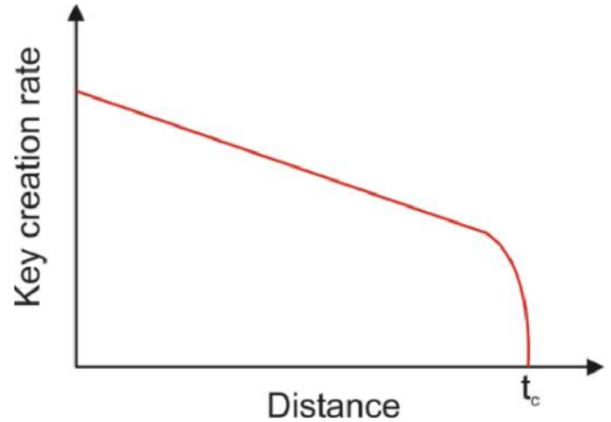


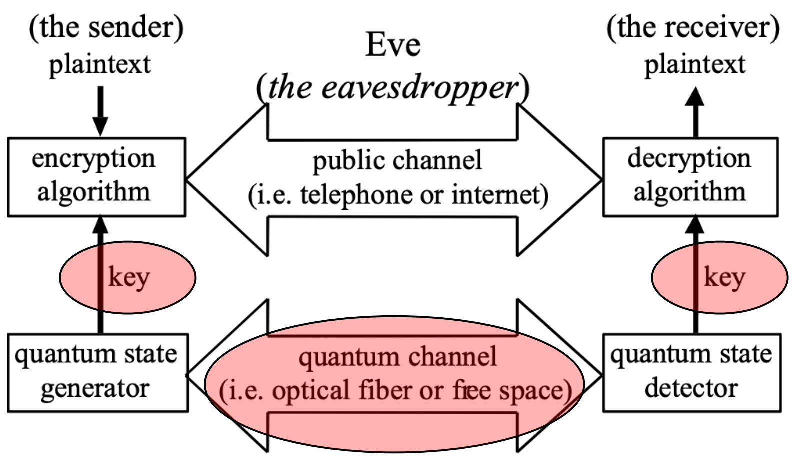
Quantum Key Distribution (QKD) in Space

- The correlations based on the measure of individual photons, that can travel along Space channels, are used to generate a string, the raw-key, that is degraded if an eavesdropper taps in (seen as the mismatch of samples from transmitter and receiver).
- Such tapping is assessed as a noise level. Privacy amplification get rid of the fraction of string of key that is shared with the eventual eavesdropper, producing a private and random key.
- The noise level poses an upper limit to the protocol, above which no key is generated.
- The key is used in standard protocols, as encryption.

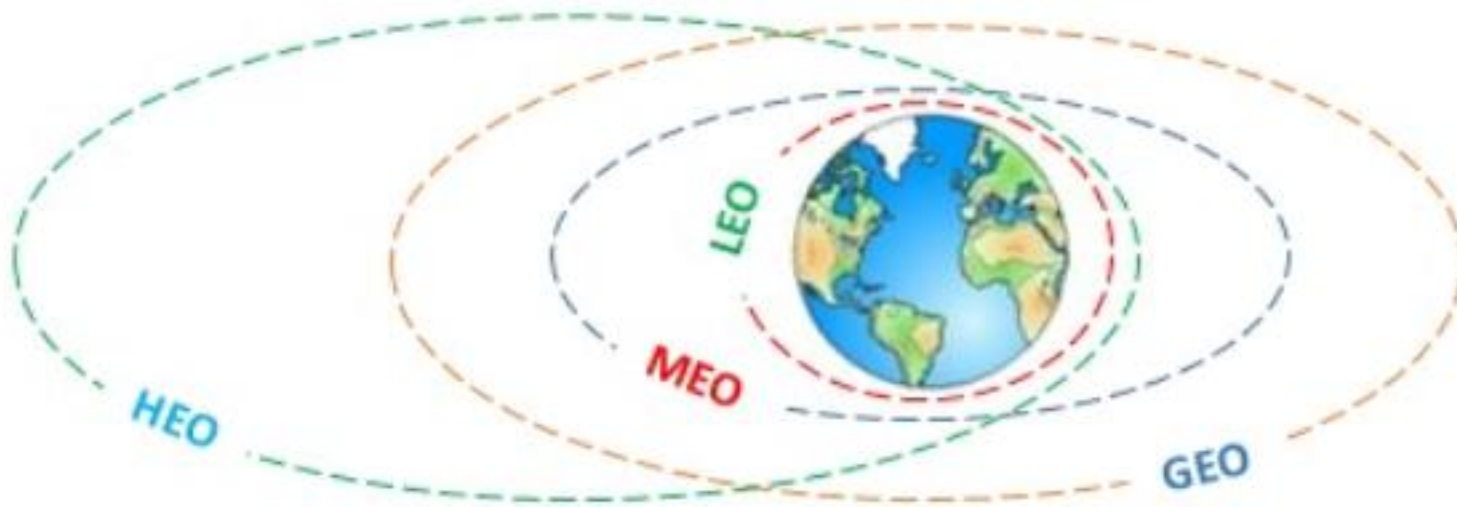








Orbits for QComms

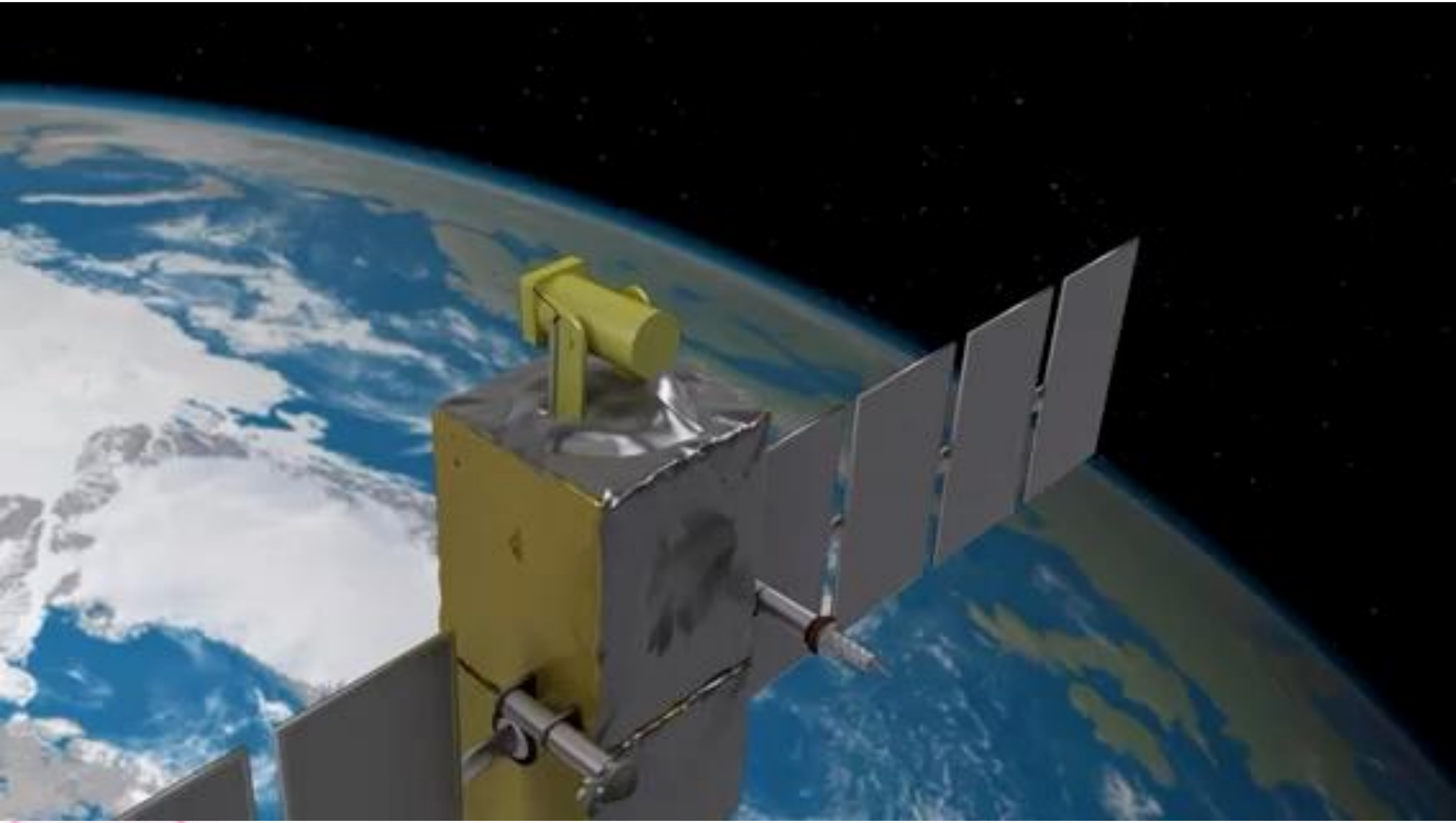


LEO orbits
rapid passages – large coverage – small payloads (potentially numerous)
secure communications (QKD – encryption of data)
fundamental test of Quantum Physics (Bell’s test)
Micius and SOTA are here

MEO and GNSS orbits
dual use of the QKD setup (interesat, Space to ground)
securing positioning and navigation service
securing timing applications

GEO orbits
large optical aperture
securing data relay - EDRS

Inter-Sat Q-Comms for a GNSS constellatons

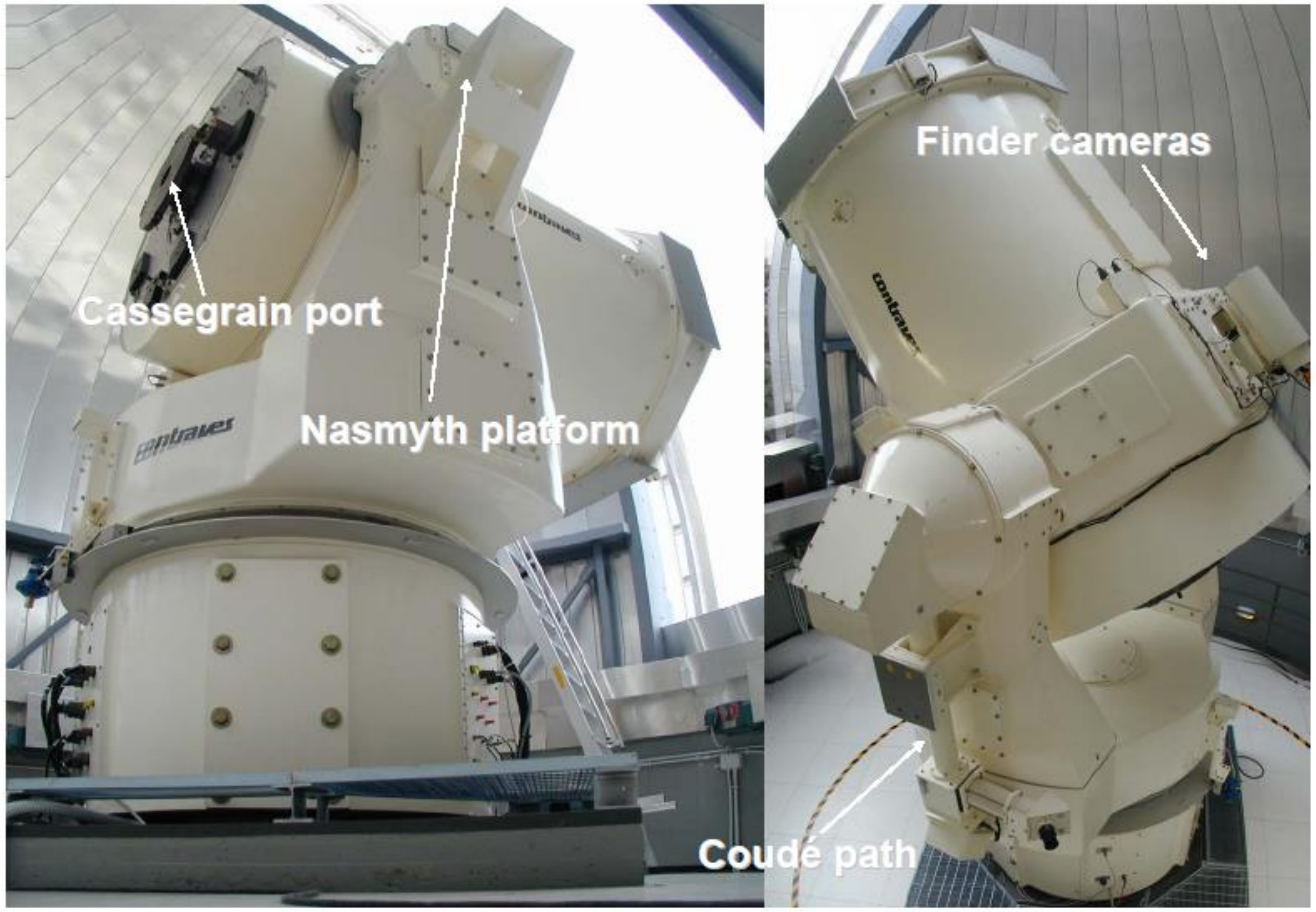


Project ESA Q-GNSS 2011-2015
F. Gerlin et al. Proc. 2013 Int. Conf. Localization and GNSS

Experimental demonstration
@ Space Q-Comms hub Matera ASI-MLRO

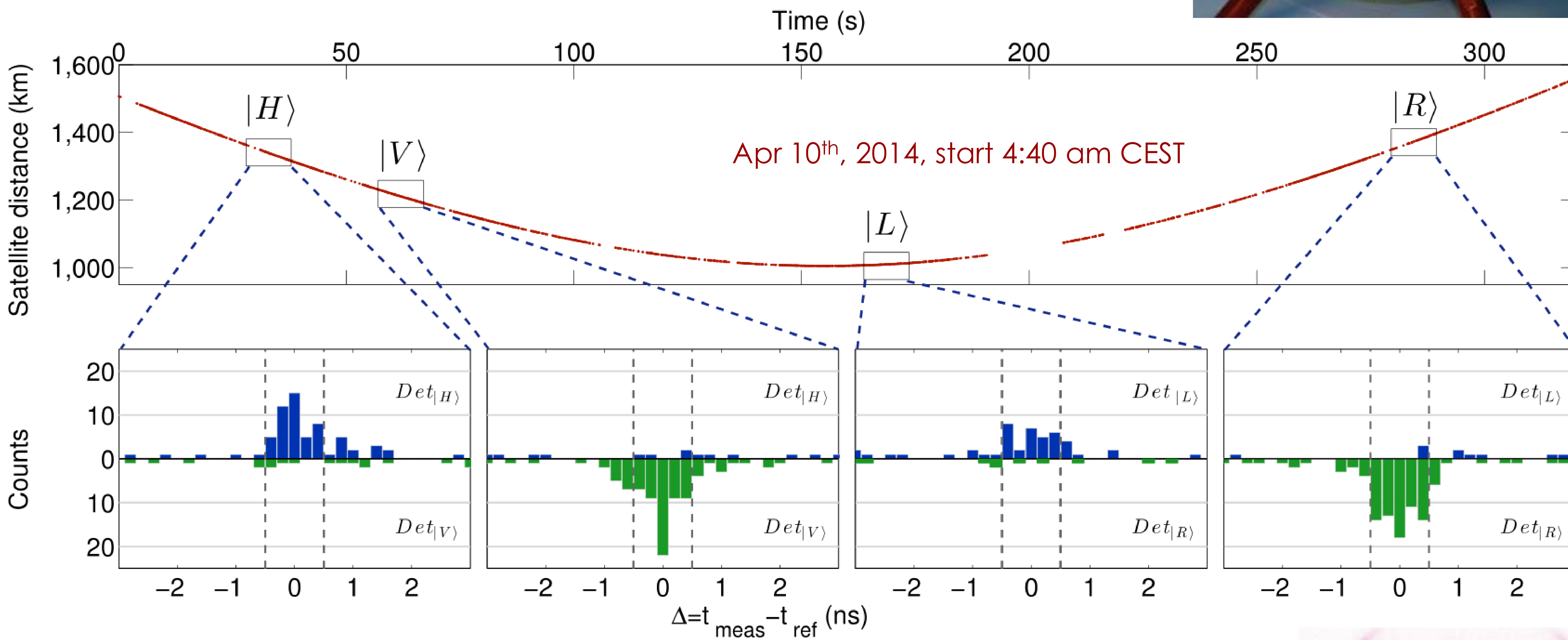
agenzia spaziale italiana

- *Giuseppe Colombo* Space Geodesy Centre of Italian Space Agency - Matera Laser Ranging Observatory (MLRO)
- Director Dr. Giuseppe Bianco President of ILRS
- World highest accuracy in SLR: mm-level for about 10^7 m range
- Accurate lunar ranging



First QComms in Space, using LARETS satellite

60 cube corner retroreflectors (CCR) were used as a synthetic quantum source in orbit, at 690 km. The metallic coating on CCR preserve the polarization.
A train of qubits were directed toward MLRO



- **10 s windows**
- **Timebin width ≤ 1 ns**

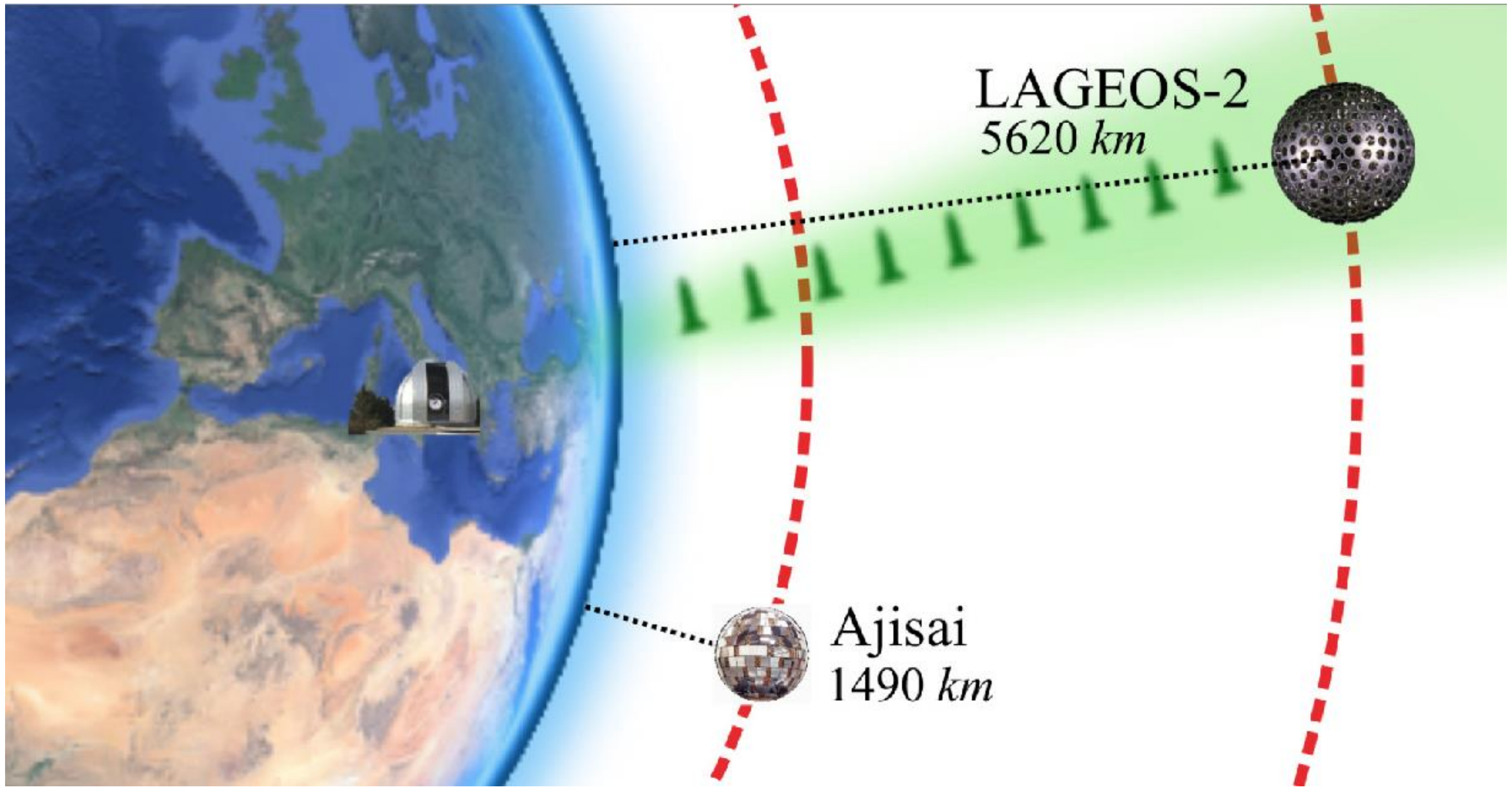
- **QBER ≃ (6.6±1.7) %**
- **Return rate 147 cps**

up to 10^4 bits for each satellite passage

G. Vallone et al, *Experimental Satellite Quantum Communications*, Physical Review Letters, **115** 040502, 2015

Single Photon exchange: from LEO to MEO

Demonstration of the detection of photon from the satellite which, according to the radar equation, is emitting a single photon per pulse from a Medium-Earth-Orbit MEO satellite.



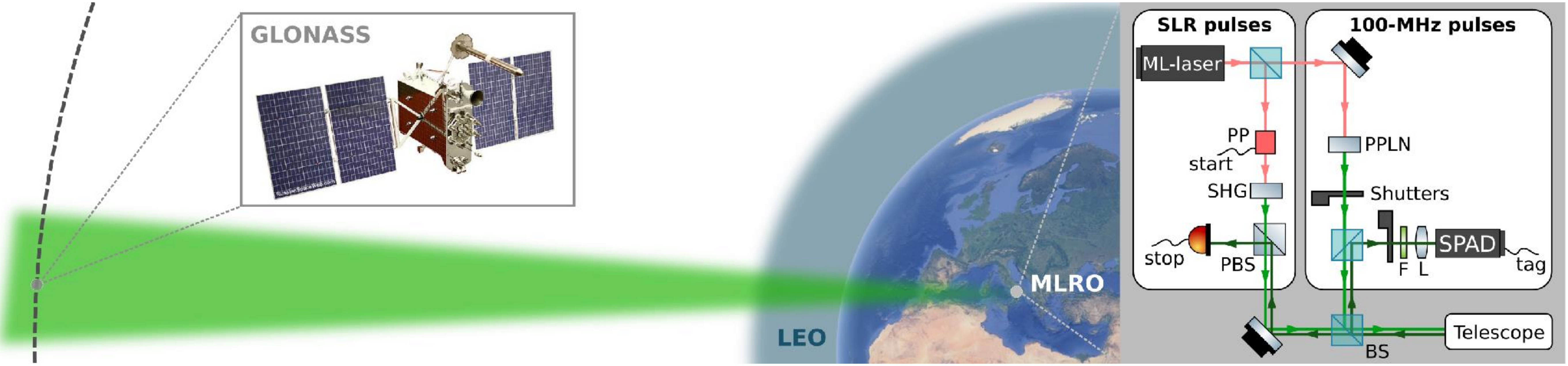
P. Villoresi et al., *Experimental verification of the feasibility of a quantum channel between space and Earth*," New J. Phys. **10** 033038, 2008.
D. Dequal et al. *Experimental single photon exchange along a space link of 7000 km*, PRA Rapid Comm **93** 010301, 2016.

GNSS orbit reached at 20000km: single photons returns from GLONASS

two GLONASS terminals equipped with an array of corner-cube retroreflectos (CCRs), namely Glonass-134 and Glonass-131 (Space Vehicle Number: 802 and 747, respectively)

The targeted GNSS satellites are part of different generations, GLONASS-K1 for Glonass-134 and GLONASS-M for Glonass-131, both equipped with a planar array of CCRs, with circular and rectangular shape respectively

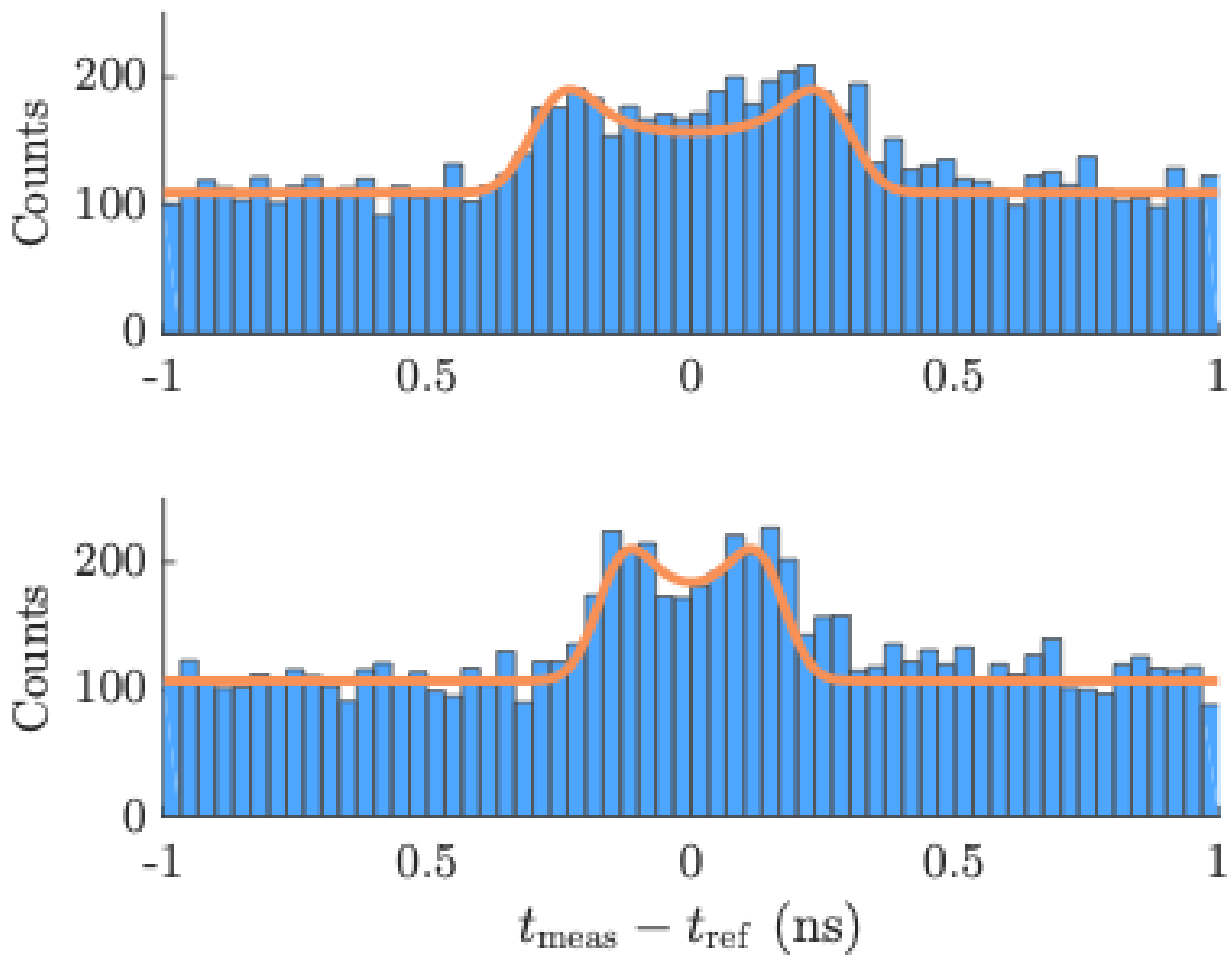
Their CCRs are characterized by the absence of coating on the reflecting faces, such that the light is back reflected by total internal reflection (TIR). This implies a far field diffraction pattern (FFDP) which is quite different from the simple Airy disk given by a circular aperture



L. Calderaro et al. *Towards Quantum Communication from Global Navigation Satellite System*, **Quantum Sci. Technol. 4 015012** (2019).

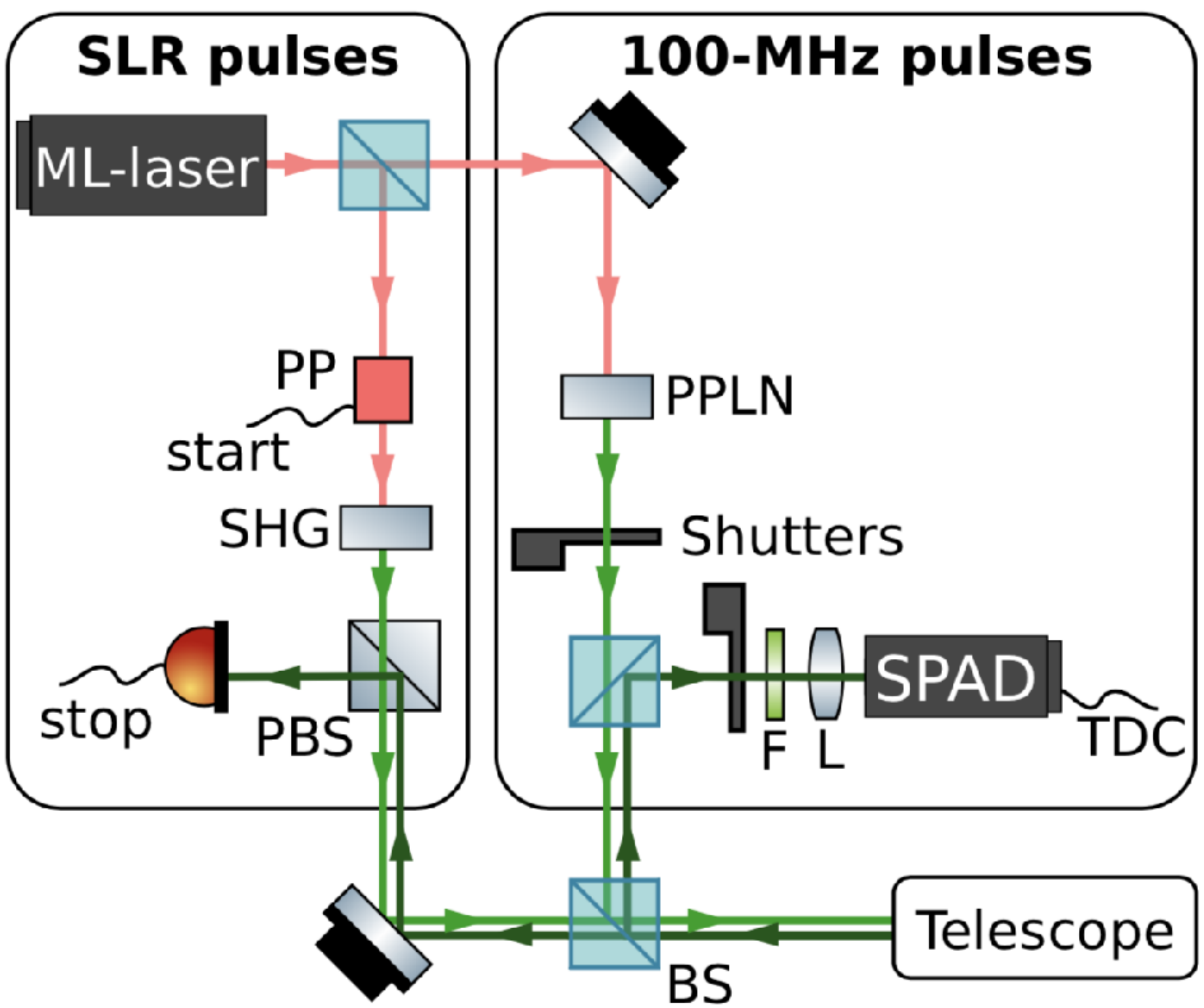
GLONASS temporal footprint in the single photon arrival time

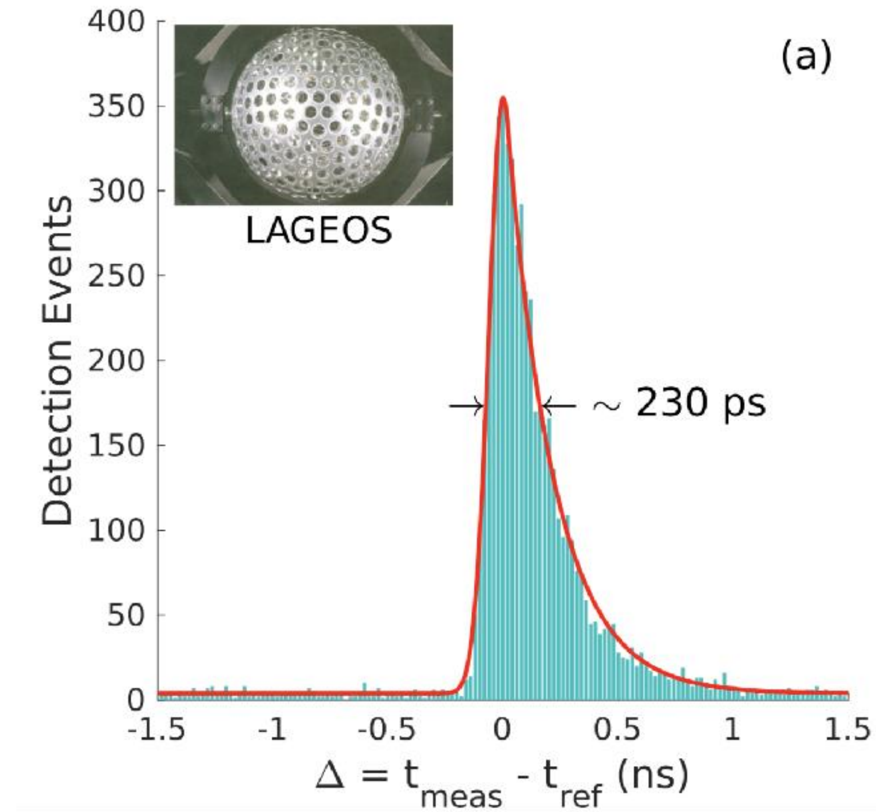
Examples of incident angle of the beam on the array: 9 deg and 5 deg



L. Calderaro et al. *Towards Quantum Communication from Global Navigation Satellite System*, **Quantum Sci. Technol. 4 015012** (2019).

Temporal resolution *in the single photon* ***time tagging reduced to 230 ps over 7000km***





The 100-MHz pulse train is detected after a 50:50 BS to separate the outgoing and incoming beams and 3 nm spectral filter a **silicon single photon avalanche detector (SPAD), provided by Micro-Photon-Devices Srl, with ≈ 50% quantum efficiency, ≈ 400 Hz dark count rate and 40 ps of jitter**.

The time of arrival is tagged with **1 ps** resolution (quTAG TDC from qutools GmbH)

C. Agnesi et al., *Sub-ns timing accuracy for satellite quantum communications*,
J. Opt. Soc. Am. B, **36**, B59, 2019

Envisioned **Space Q-Comms in Europe**

- Quantum Communications **in/from/to Space** are crucial building blocks of the **large-scale network of European Secure Communications**, that are needed for:
  - **point-to-point communications on ground**, at *every scale*,
  - to **secure the uplink of commands to satellites** or
  - the **download of data originated in Space**, as well as
  - to provide a significant step in the **security of the European Global- Navigation-Satellite-System Galileo**.

Within the **Quantum Technology Flagship** perspective, it was presented to European Commission:

Goal 1: payloads demonstrating SC from LEO, at high rate (low-loss links),

Goal 2: the creation of a secure network with ground,

Goal 3: the implementation of GEO platforms,

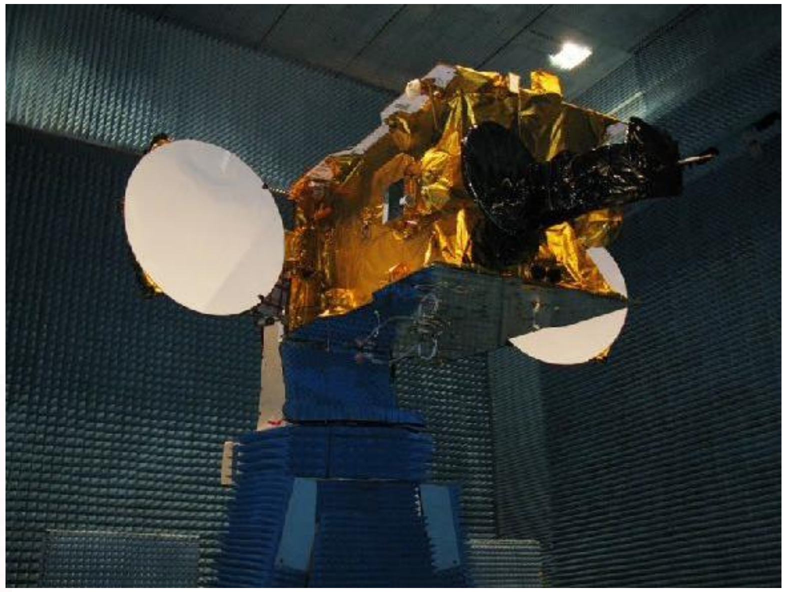
Goal 4: and then to GNSS.

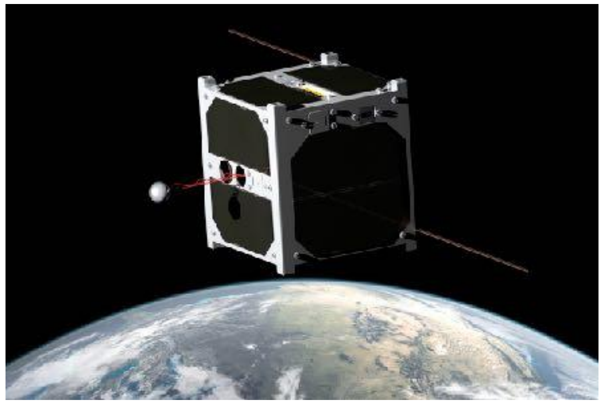
ESA SciLight (ARTES) program on **Optical Communications and QKD demonstration**

European Space QComms Scientific Committee: Paolo Villoresi, coordinator, Padova (I), Eleni Diamanti, Sorbonne-Paris (F), John Rarity, Bristol (UK), Rupert Ursin, Acad. Sci. Vienna (A), Bruno Hüttner, idQuantique SA, Geneve (CH).

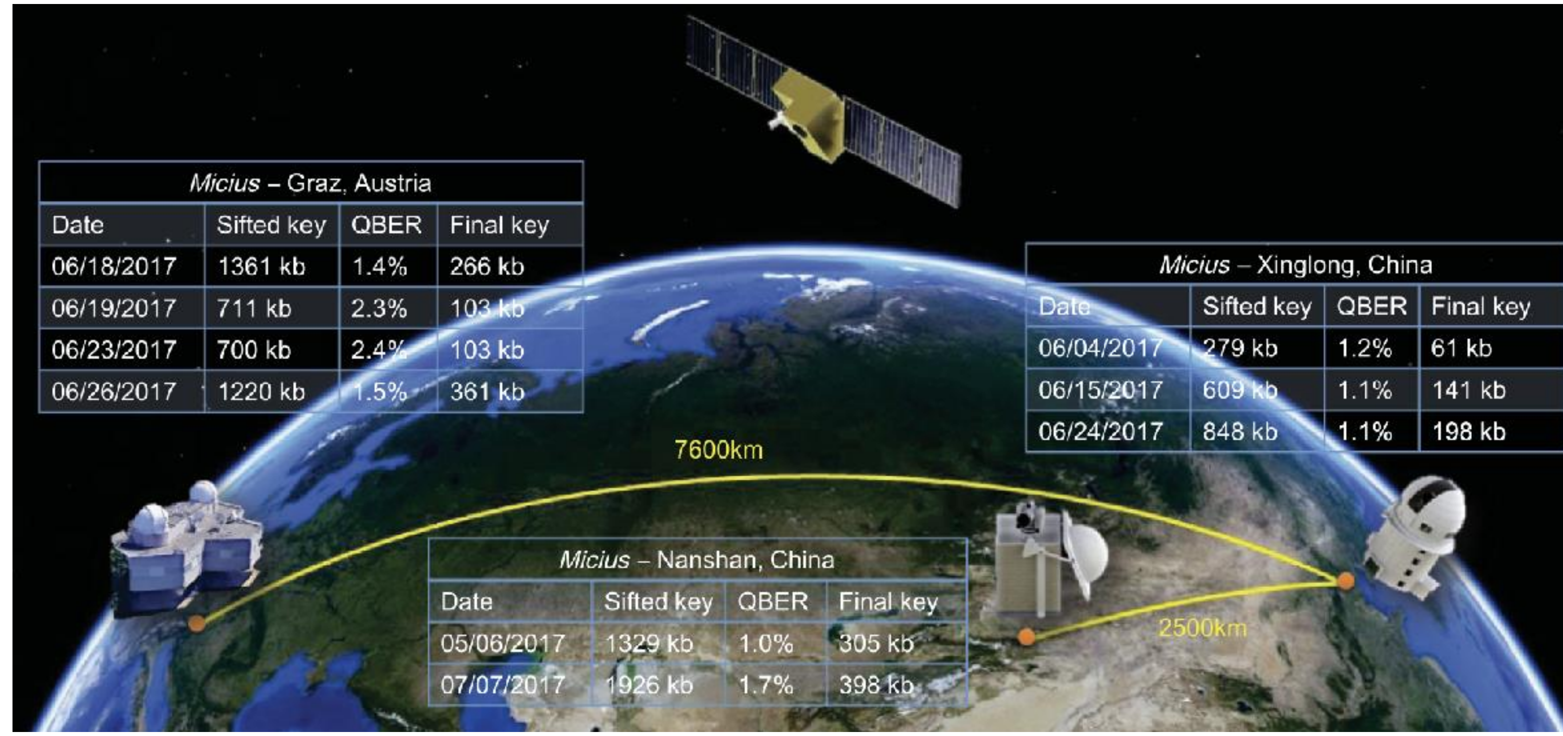
Global situation for Space QComms

- very ambitius projects in China, addressing all orbit types
- Japan will develop LEO sats
- Singapore will test entangled sources in cubesats
- USA expressed interest for experiments on the ISS





Satellite-Relayed Intercontinental Quantum Network



Micius – Graz, Austria			
Date	Sifted key	QBER	Final key
06/18/2017	1361 kb	1.4%	266 kb
06/19/2017	711 kb	2.3%	103 kb
06/23/2017	700 kb	2.4%	103 kb
06/26/2017	1220 kb	1.5%	361 kb

Micius – Xinglong, China			
Date	Sifted key	QBER	Final key
06/04/2017	279 kb	1.2%	61 kb
06/15/2017	609 kb	1.1%	141 kb
06/24/2017	848 kb	1.1%	198 kb

Micius – Nanshan, China			
Date	Sifted key	QBER	Final key
05/06/2017	1329 kb	1.0%	305 kb
07/07/2017	1926 kb	1.7%	398 kb

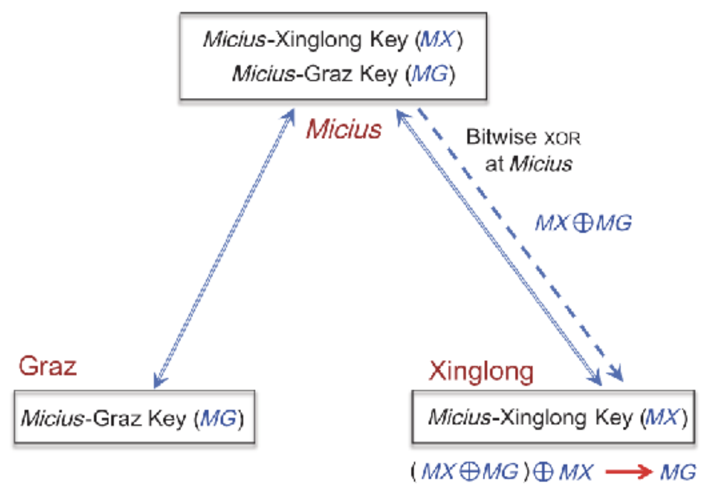
Micius satellite as a trusted relay to distribute secure keys between multiple distant locations in China and Europe

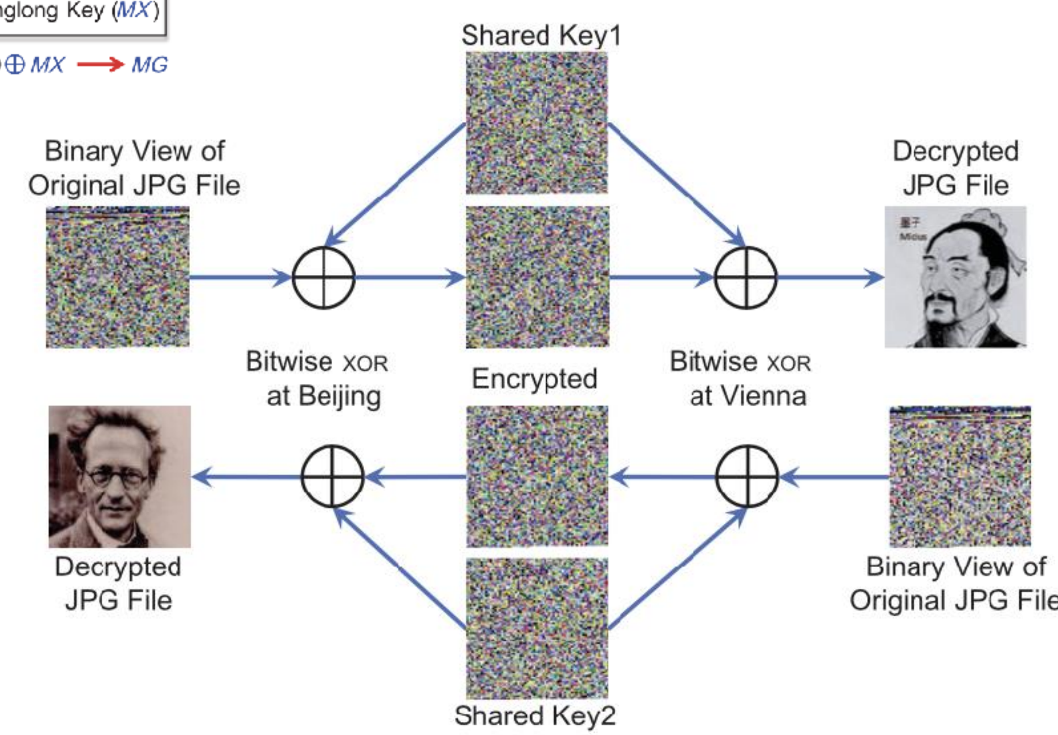
QKD is performed in a downlink scenario—from the satellite to the ground.

sifted key rate of a ~3 kb=s at ~1000 km physical separation distance and ~9 kb=s at ~600 km distance (at the maximal elevation angle),

In this work, it was established a 100 kB secure key between Xinglong and Graz.

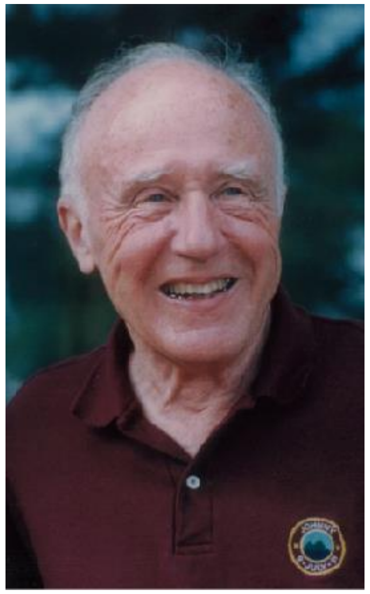
Video conference with AES)-128 protocol that refreshed the 128-bit seed keys every second.



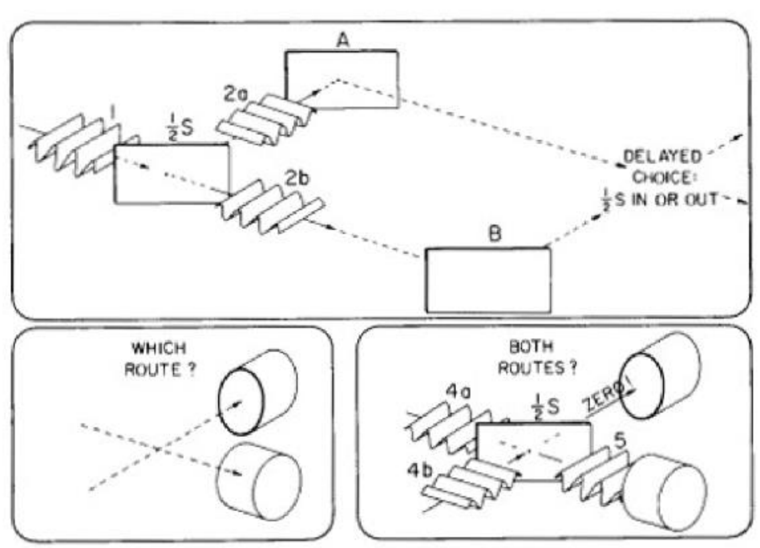


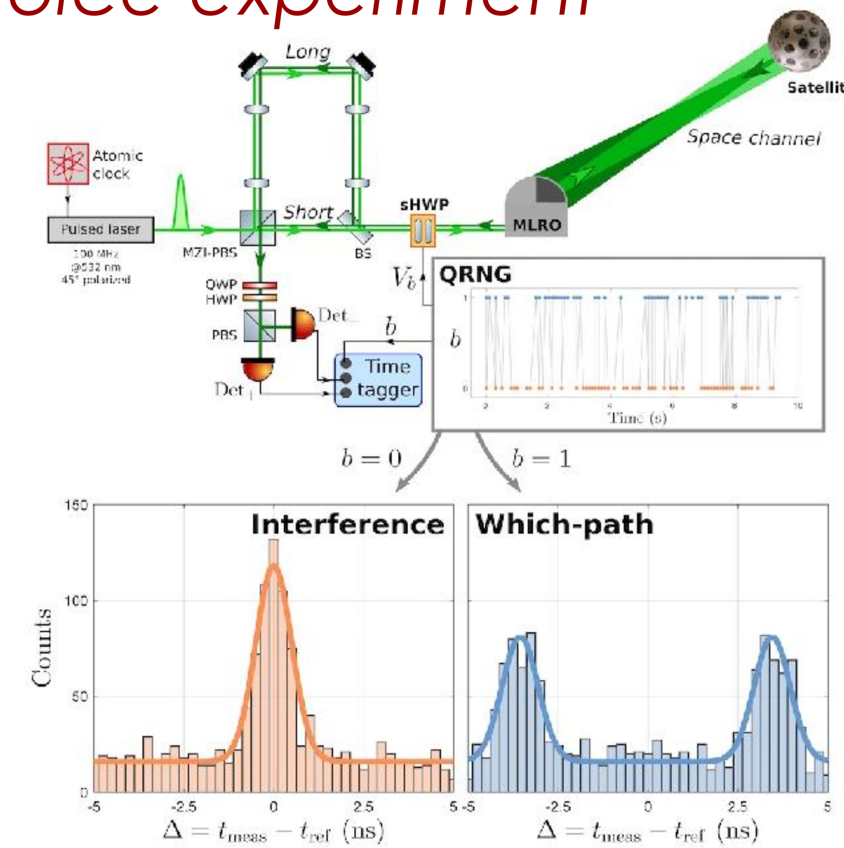
S-K Liao et al, Phys. Rev. Lett. 120, 030501 (2018)

Fundamental tests using Space QComms



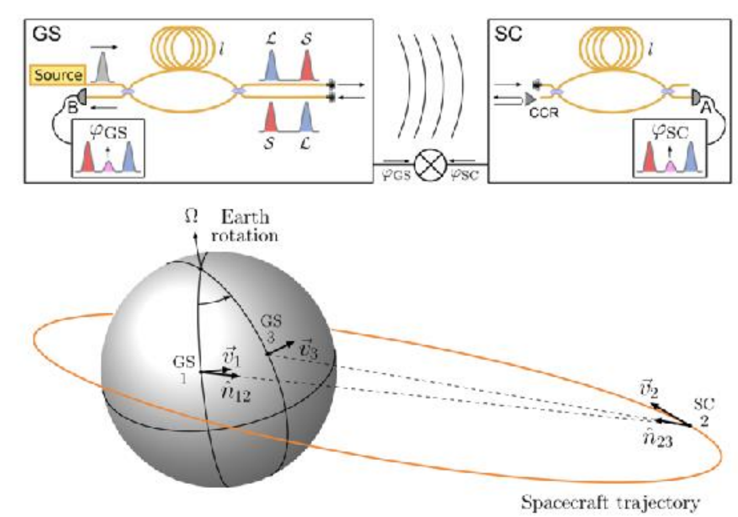
wave-particle duality investigated along a Space channel: John Wheeler delayed choice experiment





F. Vedovato et al. *Extending Wheeler's delayed-choice experiment to Space*, Science Adv. **3** e1701180 (2017)

- Precision measurements of the **gravitational red-shift** tightly bound violations of the **Einstein Equivalence Principle** (EEP): the so-called ***red-shift*** implied by the EEP **affects the locally measured frequencies of a spectral line that is emitted at location 1 with ω_1 and then detected at location 2 with ω_2.**



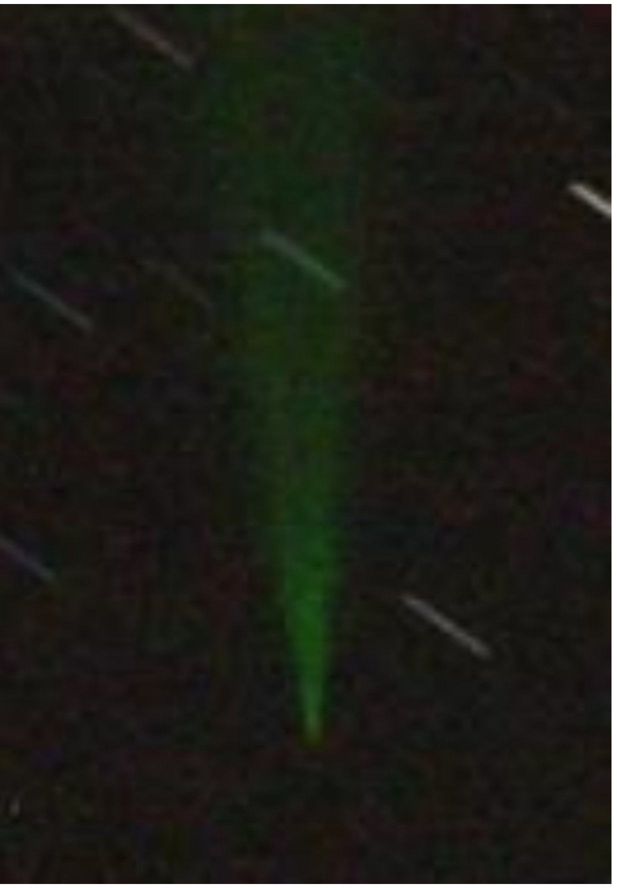
D. R. Terno et al., *Proposal for an Optical Test of the Einstein Equivalence Principle*, arXiv 1811.04835, Nov. 2018.

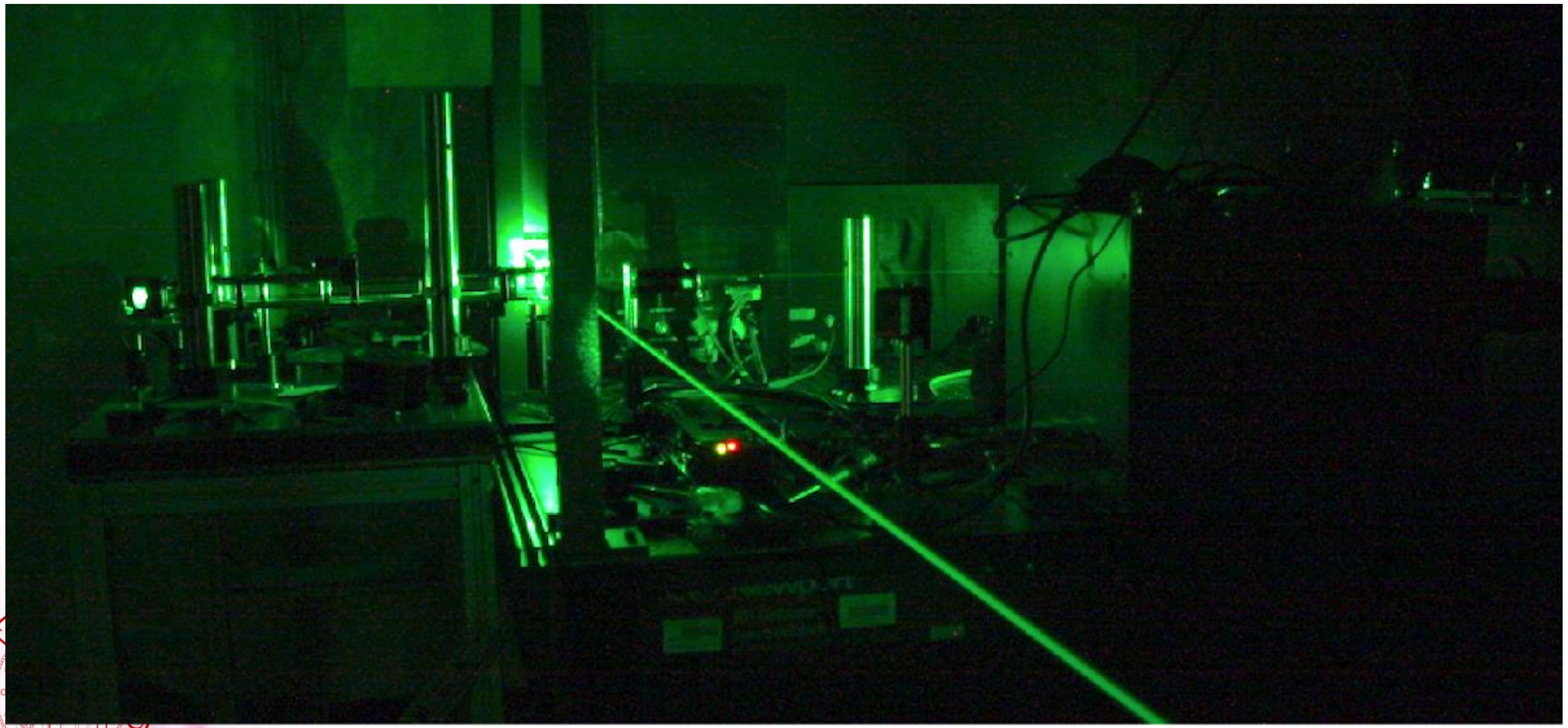
Conclusions and perspective

Advances are sought now for Space Quantum Communications, as QKD is now a commodity on ground

- **QC from a satellite transmitter to the Earth was experimentally demonstrated** as feasible using *polarization coding* – over 2000 km and *time-bins coding* – over 5000 km
- and the *single-ph. exchange for LEO and MEO - feasibility for GNSS*
- Novel fundamental tests in Space
- More properties of the wavefunction and of entanglement to be studied
- International cooperation on technology and applications.

QComms in Space: not limits but horizons





paolo.villoresi@dei.unipd.it
quantumfuture.dei.unipd.it