Quantum Communications for GLOBAL SECURE COMMs

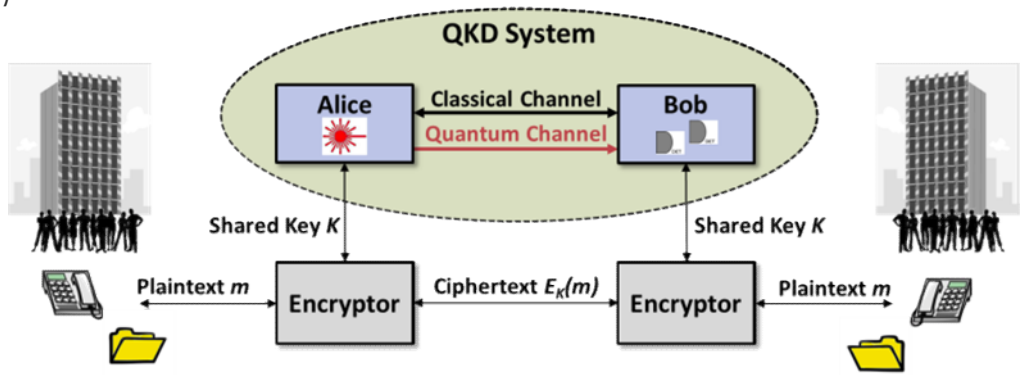
Paolo Villoresi

University of Padua,
Quantum Tech. Res. center and Dept. Information Eng.,
Padova, Italy

Submarine networks:
the infrastructure of a global connection
Webinar Under the aegis of G20 Italian Presidency 4 Aug. 2021

Secure Communications based on Quantum Communications

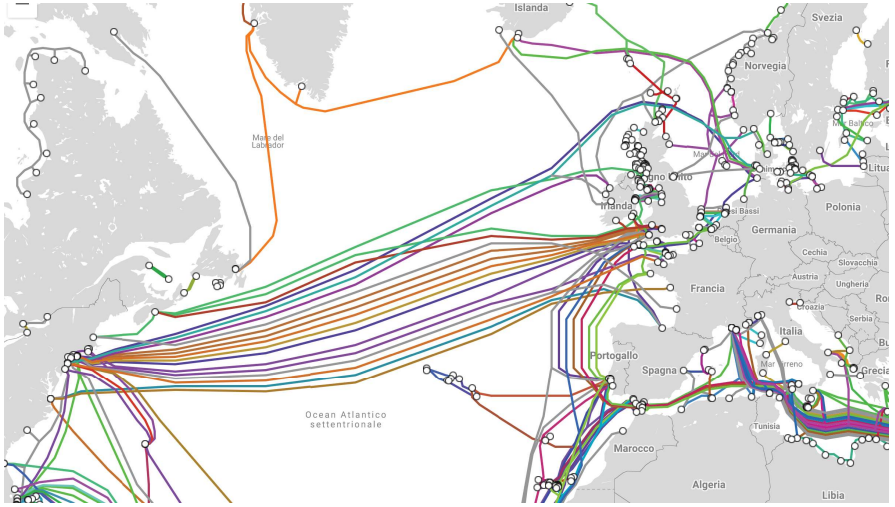
- The need of security is of paramount importance in current communication systems.
- Secure exchange of secret keys along public channels is an essential task in cryptography, and it is crucial to symmetric encryption, at the core of current security protocols as Internet Protocol Security (IPSec) and Transport Layer Security (TLS)
- Several aspects of the communication system are at stake:
  - message authentication
  - integrity of the content
  - data encryption
- Quantum Technologies here contribute with the **Quantum Key Distribution (QKD)**: a key shared by two parties and that is
  - random and equal on both sides
  - clean from shared information with other agents (malicious or not)



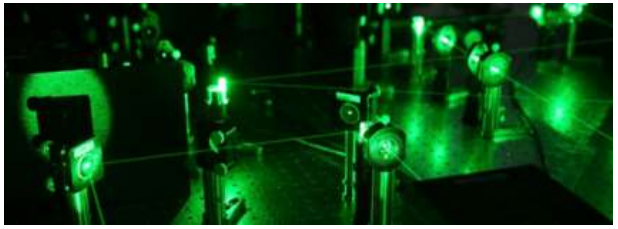
- Bennett, C. H. and Brassard G., Quantum cryptography: Public key distribution and coin tossing, Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing, Bangalore 175 (1984)
- Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. Nat. Photonics 8, 595–604 (2014)
- Pirandola, S. et al. Advances in quantum cryptography. Adv. Opt. Photonics 12, 1012 (2020)

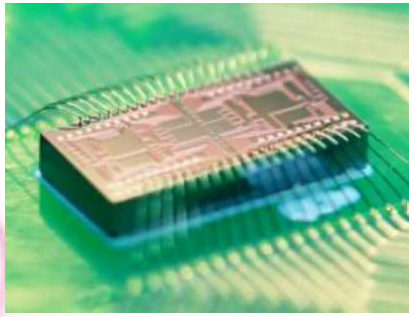
Long distance secure connections

- Submarine connections are intrinsically point-to-point
- Their security would be enhanced by using quantum technologies and in particular quantum-key-distribution (QKD)
- QKD is point-to-point too, and is developing (mainly) on ground and in space
- The global secure connections would evolve toward the quantum internet



Quantum Communications are part of Quantum Technologies

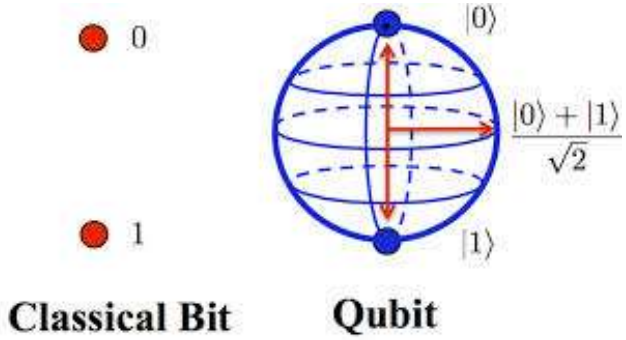


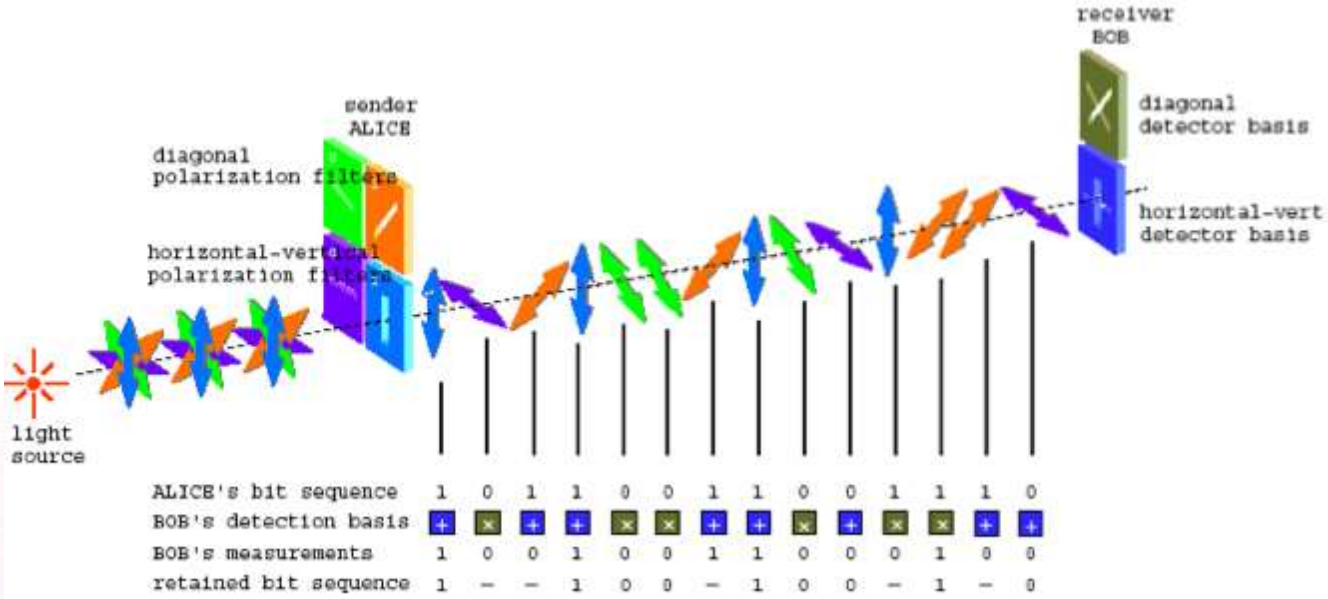


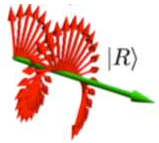
- *Quantum Mechanics*: the **interpretation of physical reality** in the **microcosmos**
  - provided the *understanding of atoms, molecules, fundamental particles, superconductivity*, etc.
  - allowed the *invention of transistors, lasers, integrated devices, etc.*
- **QM is now inspiring a *new age 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..**

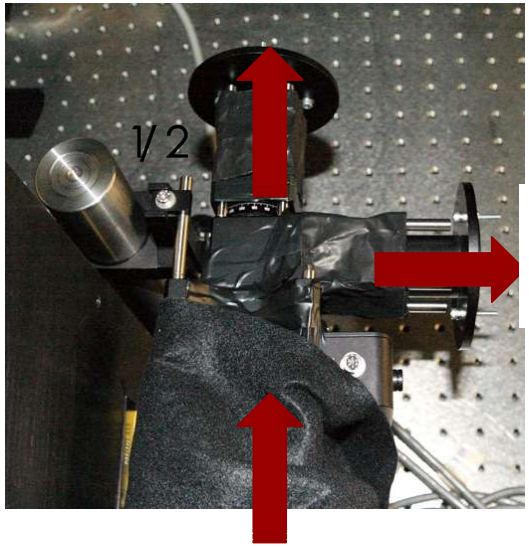
Quantum Communications are based on the sharing of qubits

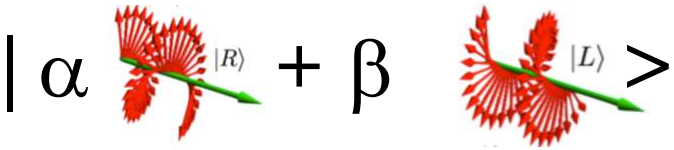
- From the bit (binary unit) used in classical information systems, with Quantum Technologies it is used the qubit (quantum bit), embodied in a elementary (quantum) object as photons, electrons..
- Qubit peculiar feature: it is a superposition of alternatives, that in classical terms are antithetic. It takes a complex number for the preparation of qubits
- Quantum Entanglement of a photon pair: unique wavefunction for two separate photons, that keep their correlations afar
- No-cloning theorem prevent perfect copies of generic qubits
- The measurements clicks create a correlation, useful in protocols as QKD, distributed quantum computing, metrology and more
- Qubits based on single photons cannot be amplified.





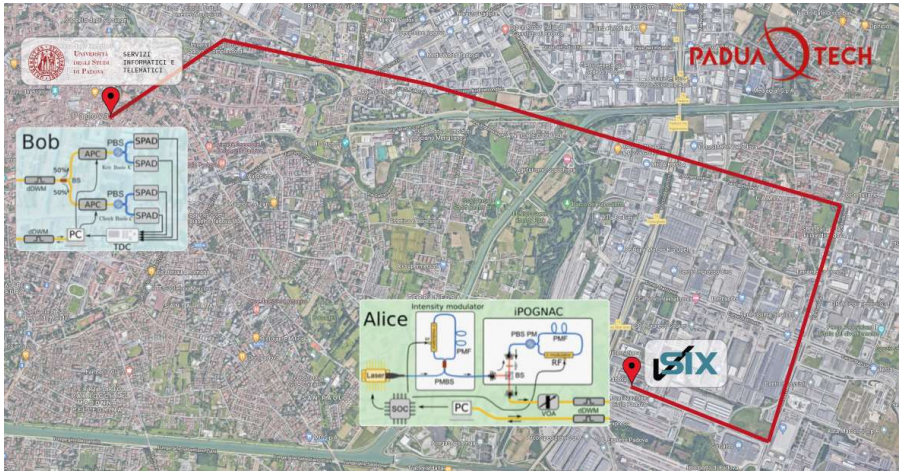






QKD in a fiber network

- Fibre links for QKD are spreading over existing network
- Dark fibers or accept some commercial data traffic - exploiting WDM
- no amplifiers and limited by background noise
- repeaterless single-haul limit at few hundreds km

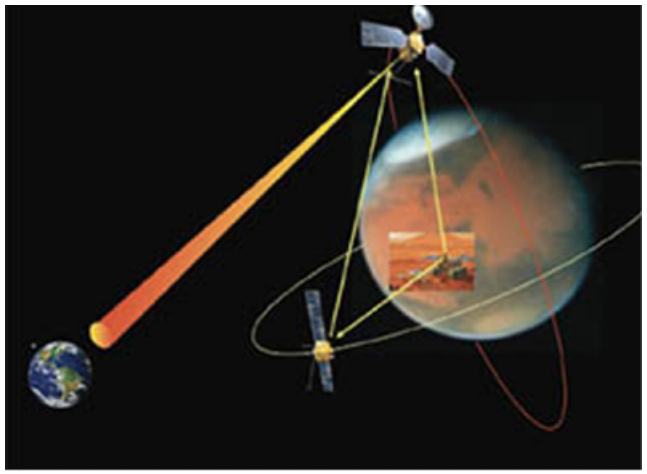


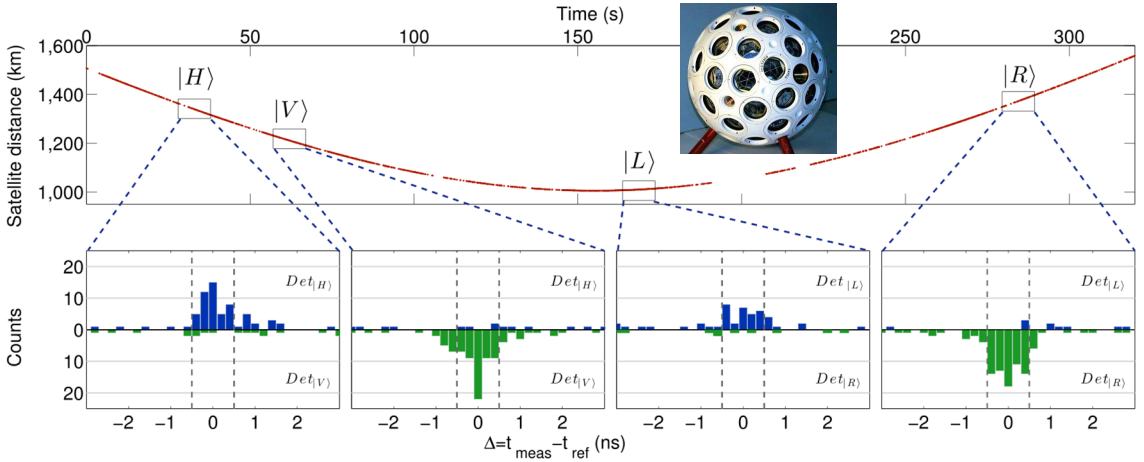
Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. npj Quantum Inf. 2, 16025 (2016).
Avesani, M. et al. Resource-effective quantum key distribution: a field trial in Padua city center. Opt. Lett. 46, 2848 (2021).
undersea: S. Wengerowsky et al. Entanglement distribution over a 96-km-long submarine optical fiber. Proc. Natl. Acad. Sci. 116, 6684–6688 (2019).

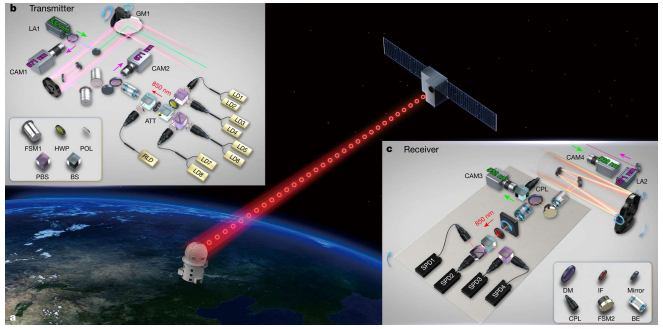
qtech.unipd.it
quantumfuture.dei.unipd.it
www.thinkquantum.com

Quantum Key Distribution in Space

- QKD protocols are suitable for space links, enjoying the channel losses that scale with diffraction (quadratically) and not with fiber attenuation (exponentially)
- Feasibility studies and demonstrations have spurred the development of in-orbit terminals and the design of satellite constellations for providing secure comms
- ESA SAGA, China, Canada, Japan, Italy, Germany, UK



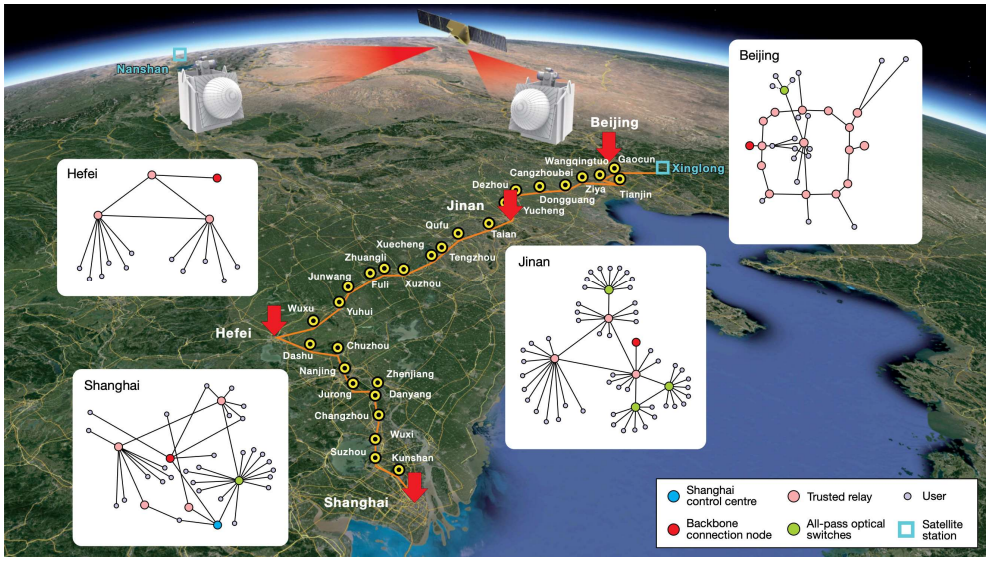


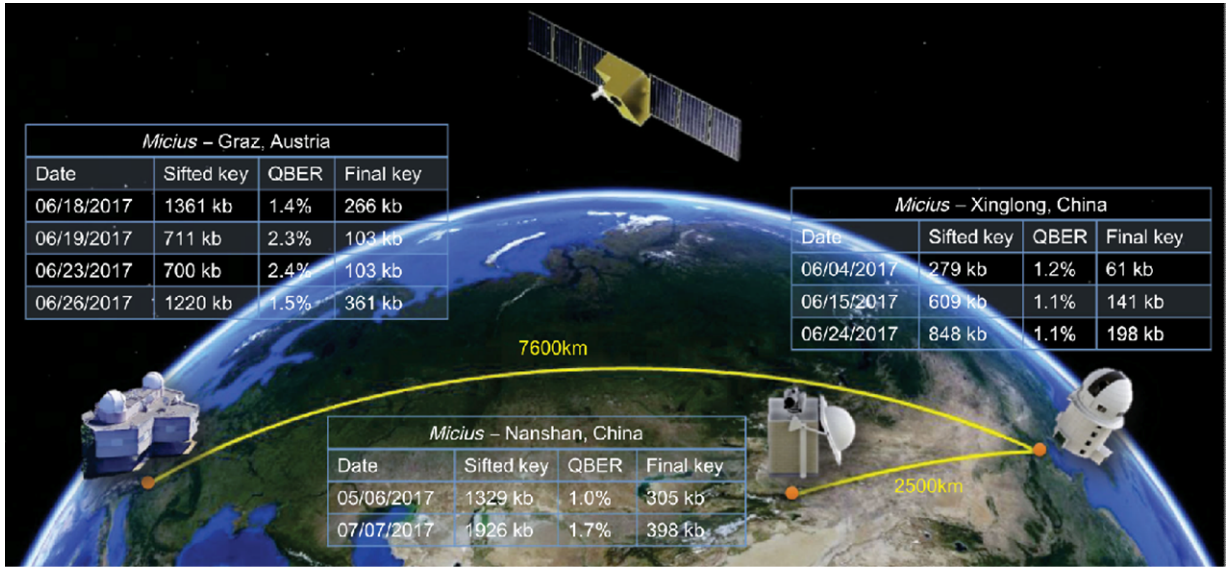


P. Villoresi et al., Experimental verification of the feasibility of a quantum channel between space and Earth," New J. Phys. 10 033038, 2008.
G. Vallone et al, *Experimental Satellite Quantum Communications*, Physical Review Letters, 115 040502, 2015
S.-K. Liao et al. *Satellite-to-ground quantum key distribution* Nature 549, 43–47 (2017).
J. S. Sidhu et al. Advances in space quantum communications. IET Quantum Commun. qtc2.12015 (2021)

Intercontinental space and ground network

- Ground and space links have been envisaged to operate together for connecting large networks
- Chinese Academy of Science pioneered the interconnection within and across continents





S-K Liao et al, Satellite-Relayed Intercontinental Quantum Network
Phys. Rev. Lett. 120, 030501 (2018)
Chen, Y.-A. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature 589, 214–219 (2021)

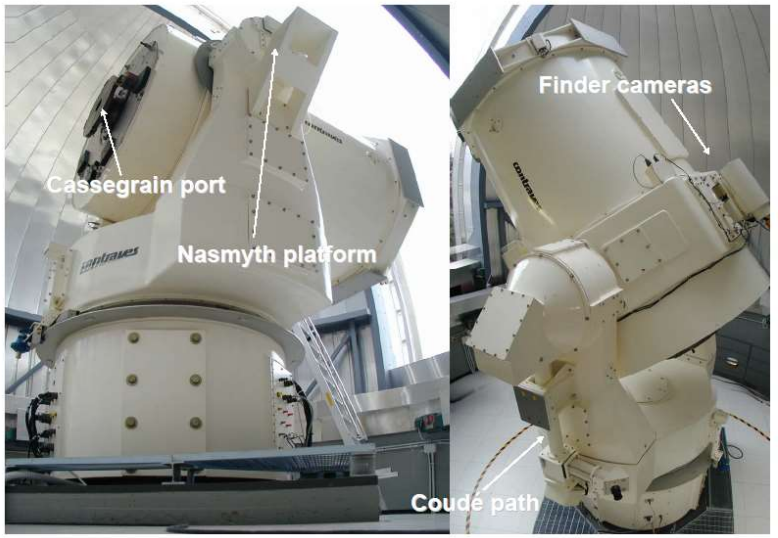
Inter-Sat Q-Comms for a GNSS constellatons

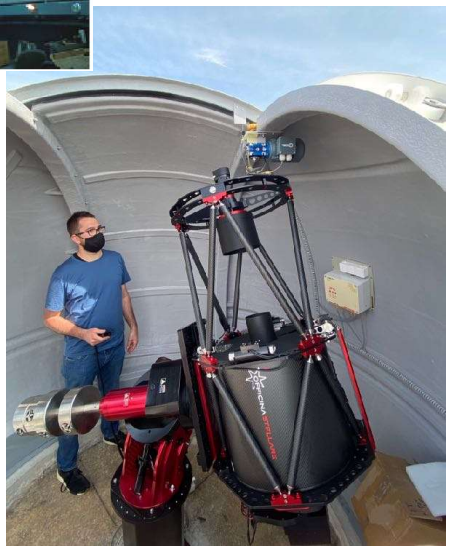
Project ESA Q-GNSS 2011-2015
F. Gerlin et al. Proc. 2013 Int. Conf. Localization and GNSS

QKD ground receivers

Telescope sizes for diverse uses:

- satellite-to-ground link on nodal points - meter class telescope (1.5m ASI- MLRO at Matera Italy and the 1 m OGS of ESA in Tenerife)
- operative user receiver, 40 cm class (GaliQEye - Padova)
- ground-to-ground free-space links night- and day-time with centimeter-class telescopes

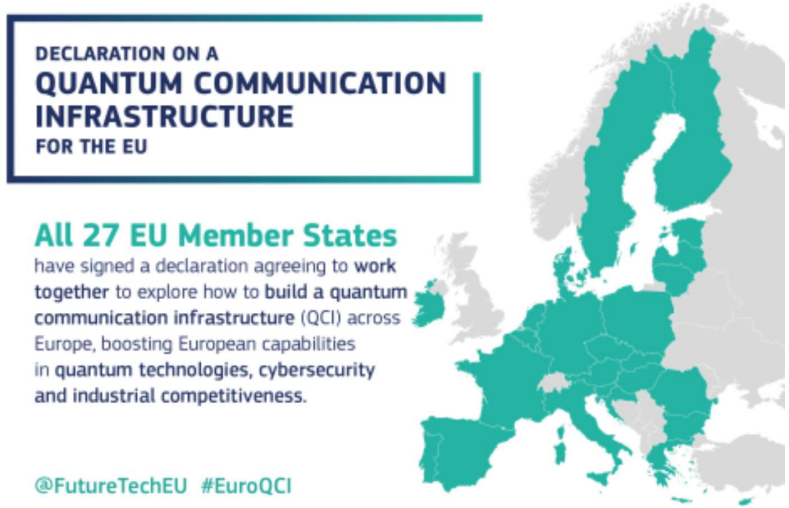




J. S. Sidhu et al. Advances in space quantum communications. IET Quantum Commun. qtc2.12015 (2021)
M. Avesani et al. Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. npj Quantum Inf. 7, 93 (2021)

QKD testbed in EU

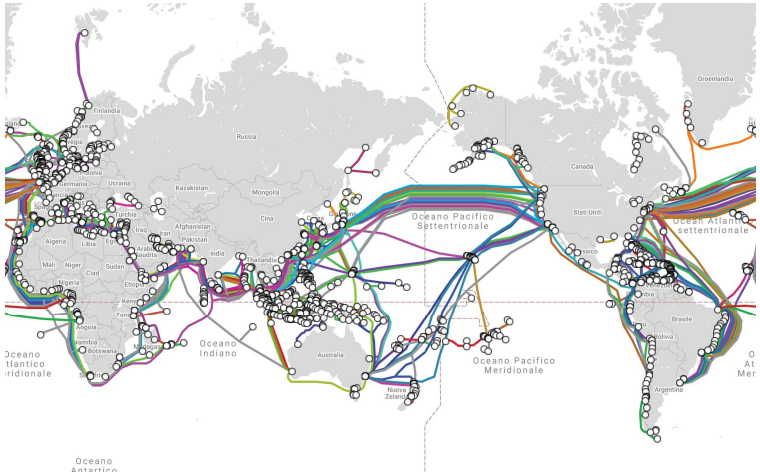
- OpenQKD EU demonstration project
- Demonstrate vertical supply chain from QKD (physical layer) to end-user (application layer)
- Many test sites across Europe to maximise impact
- Demonstration of more than 30 use-cases for QKD featuring:
  - realistic operating environments
  - end-user applications and support
- Secure and digital societies: Inter/Intra datacenter comm., e-Government, High-Performance computing, financial services, authentication and space applications, integration with post-quantum cryptography, securing time-transfer
- Healthcare: Secure cloud storage services and securing patient data in transit

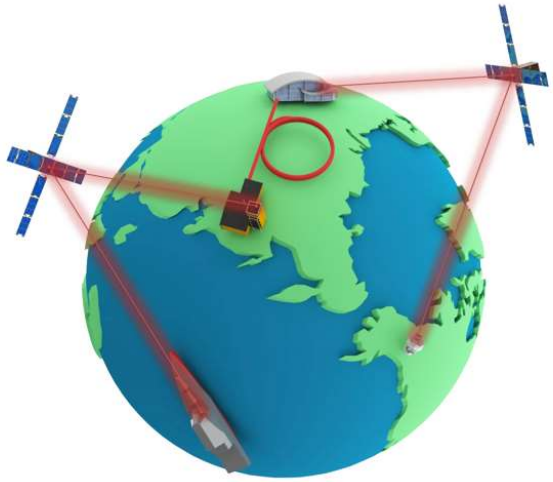


https://openqkd.eu/objectives/
https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

QKD global applications

- Secure communications with a quantum leap
- QKD direct links with fibers are limited to regional scale and shorter undersea cables but are extended with QKD from satellites
- Secure connections on ground planned to be pervasive with QKD *dorsals* (China, Italy, EU)
- Infrastructure for the entanglement sharing, achieving the quantum internet.
- connection to the most elementary level, quantum states, enabling metrology, Q-computer connections, teleportation and more.





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