Space Secure Communications using Single-Photon

Paolo Villoresi

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

First International SPAD Sensor Workshop (ISSW)
Les Diablerets (CH) 27 Feb 2018

QuantumFuture Research Group

Founded in 2003 (PV) at the Dept. of Information Engineering of the UniPD

Interdisciplinary expertise – faculties:

Quantum and Classical Optics, *G. Vallone, G. Naletto, V. Da Deppo, PV*

Quantum communications engineering, *N. Laurenti, R. Corvaja, G. Cariolaro, G. Pierobon*

Quantum Control theory *F. Ticozzi, A. Ferrante, M. Pavon*

Quantum Astronomy *C. Barbieri, S. Ortolani*

Fundend by **University of Padova**, **Italian Space Agency**, **European Space Agency**, industrial research contracts

Strategic Res. Project of UniPD 2009-2013 (35 man-years PhD and Assegnisti)

Currently **5 Faculties, 10 PhD Students + 3 Post-Docs+ undergraduates (incl. 2 EU MSCT PhD 2017-20)**

QF group in 2016

Outline

Quantum Communications principles

Quantum Key Distributions protocols

Need of "Space"

Need of "Secure"

QKD implementation
- space links
- toward the "Quantum Internet"

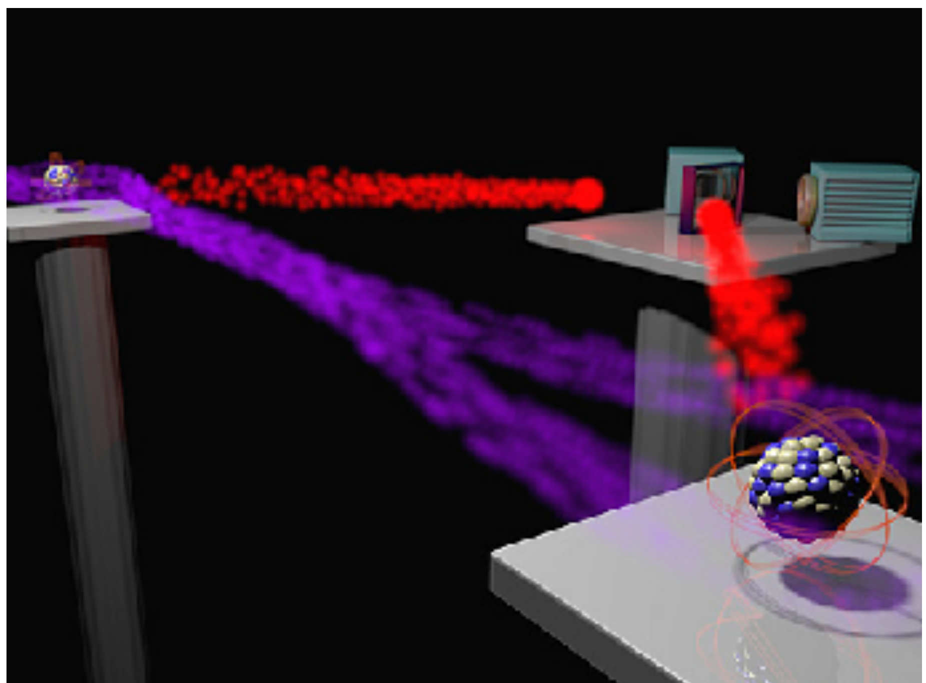
Genuine randomness from quantum processes

Perspectives with the Flagship

Conclusions

Quantum Communications

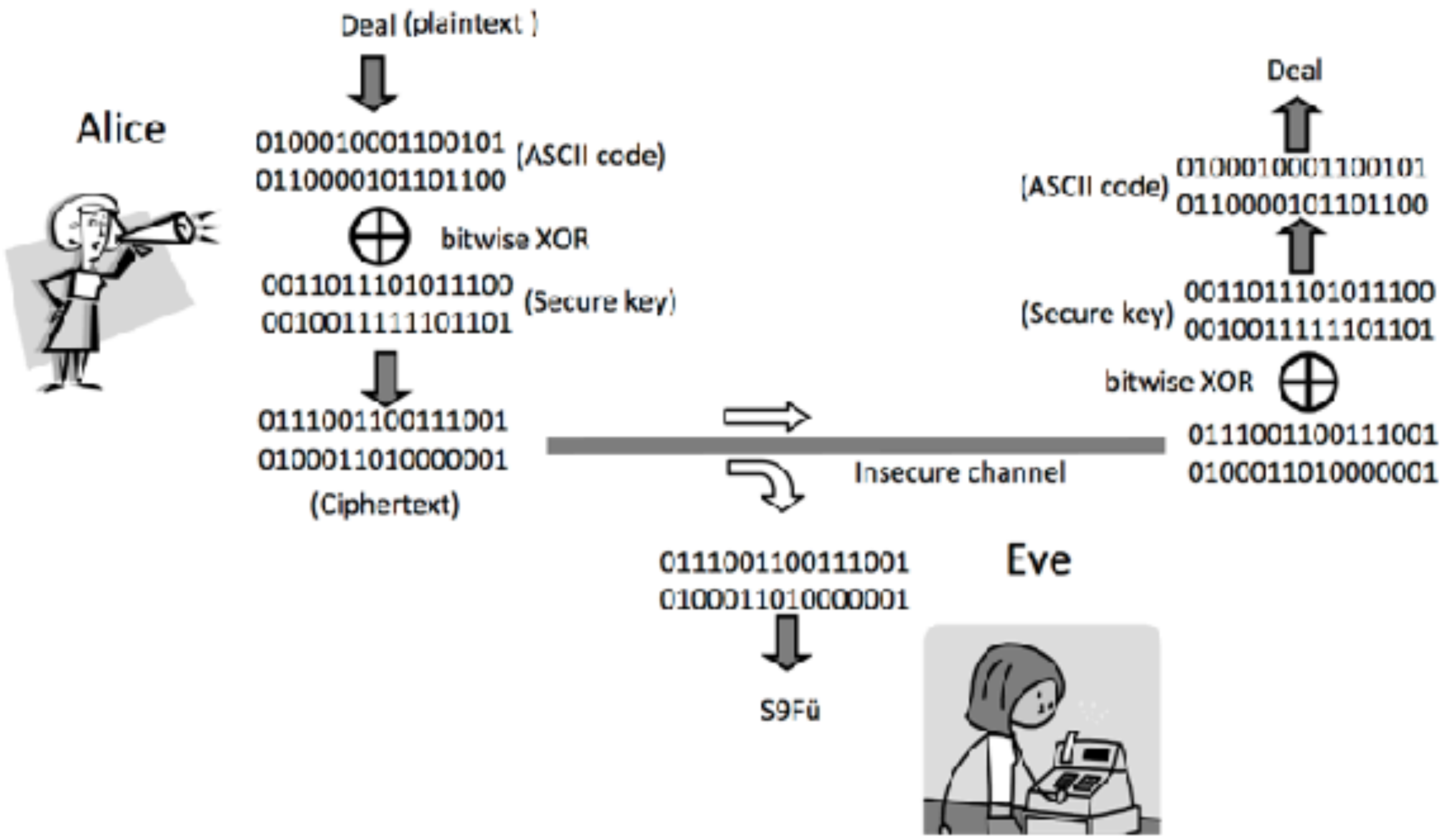
Quantum Communications is the art of **sharing quantum states** between distant partners.



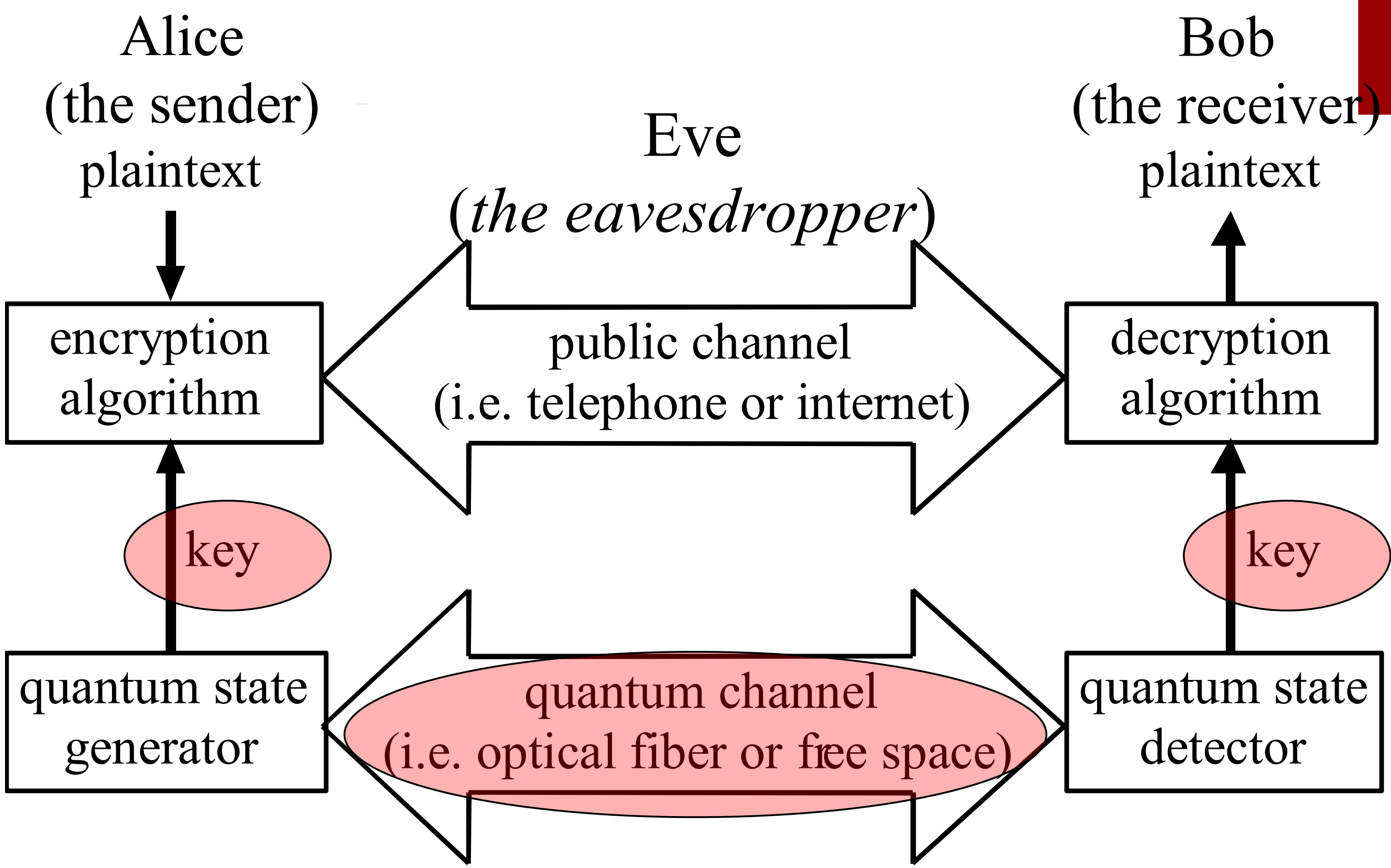
http://qurope.eu/manifesto

Cryptographic use of Quantum Communications

general scheme of secure comms



Quantum Key Distribution Scheme



Essence of Quantum Key Distribution

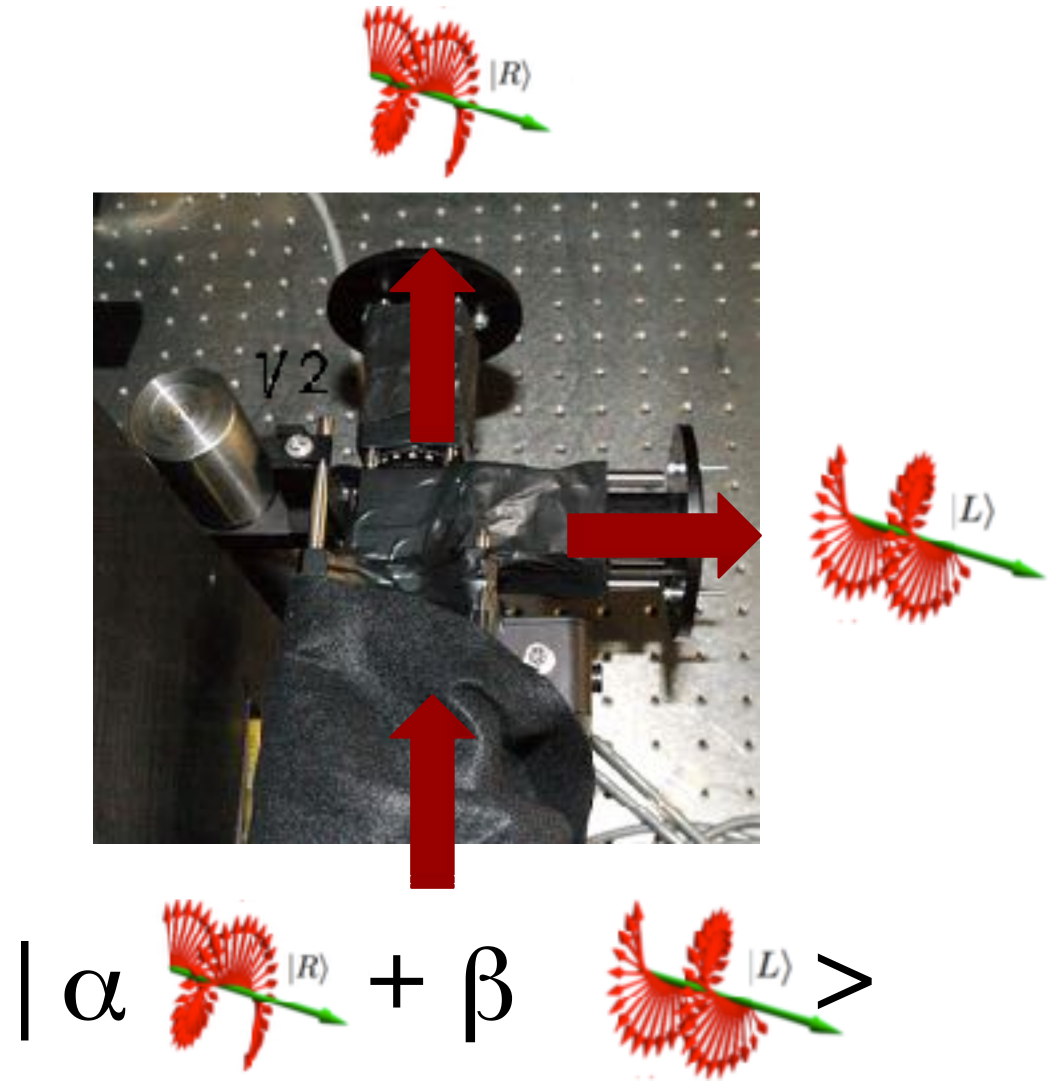
Quantum key distribution (QKD), the best-known application of quantum cryptography, promises to achieve the Holy Grail of cryptography — **unconditional security in communication**.

H-K Lo et al. Secure quantum key distribution *Nat. Phot.* **8** 595 (2014)

Q Comms: Establishing correlations by measuring photon observables

Single photon in a **superposition of states,** with normalized **amplitude** α **and** β**.**

Probabilities follow from the **choice of the base** and the values of $|\alpha|^2$ and $|\beta|^2$



Essence of Quantum Key Distribution

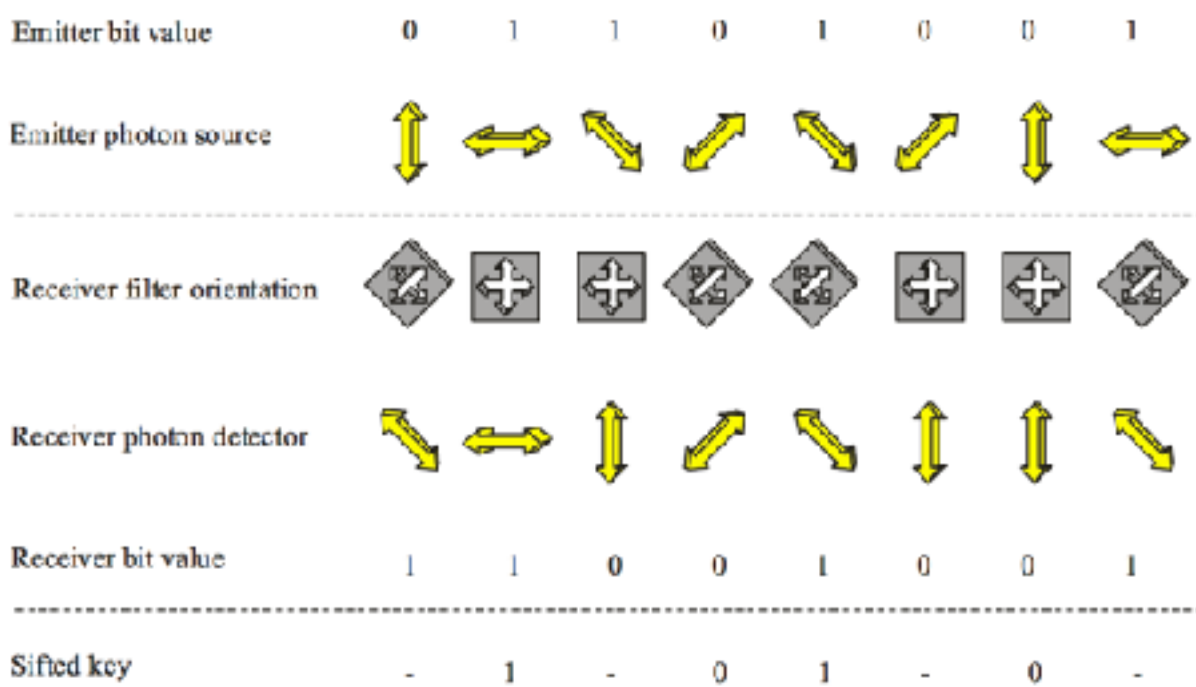
1. the exchange of a key is based on **private correlations between Alice and Bob**
2. such correlation is realized by **quantum communications using random choice of states**
3. the **privacy is based on the Law of Physics**
   1. no cloning theorem
   2. measurement of a superposition states
4. if a third party **tap the channel**, Eve the eavesdropper, eg she measures the photon stream and resend the observed results, **she introduce errors due to base wrong guess**
5. such errors and the non-ideality of the device **are eliminated using the methods of Information Theory**
6. **the resulting key is private and random**

H-K Lo et al. Secure quantum key distribution *Nat. Phot.* **8** 595 (2014)

QKD Protocol using photons

Practical example: Bennett and Brassard 1984

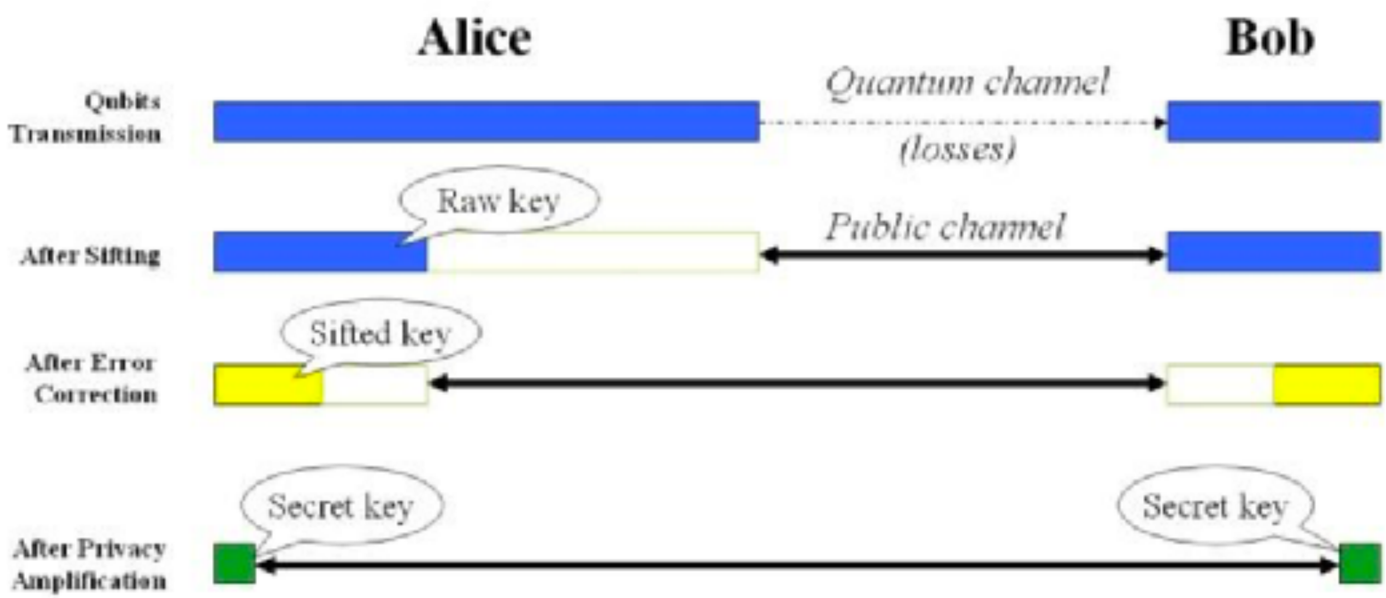
- 4 photon states:
  - Two orthogonal polarization states
  - Two non-orthogonal reference frames



QKD Protocol using photons

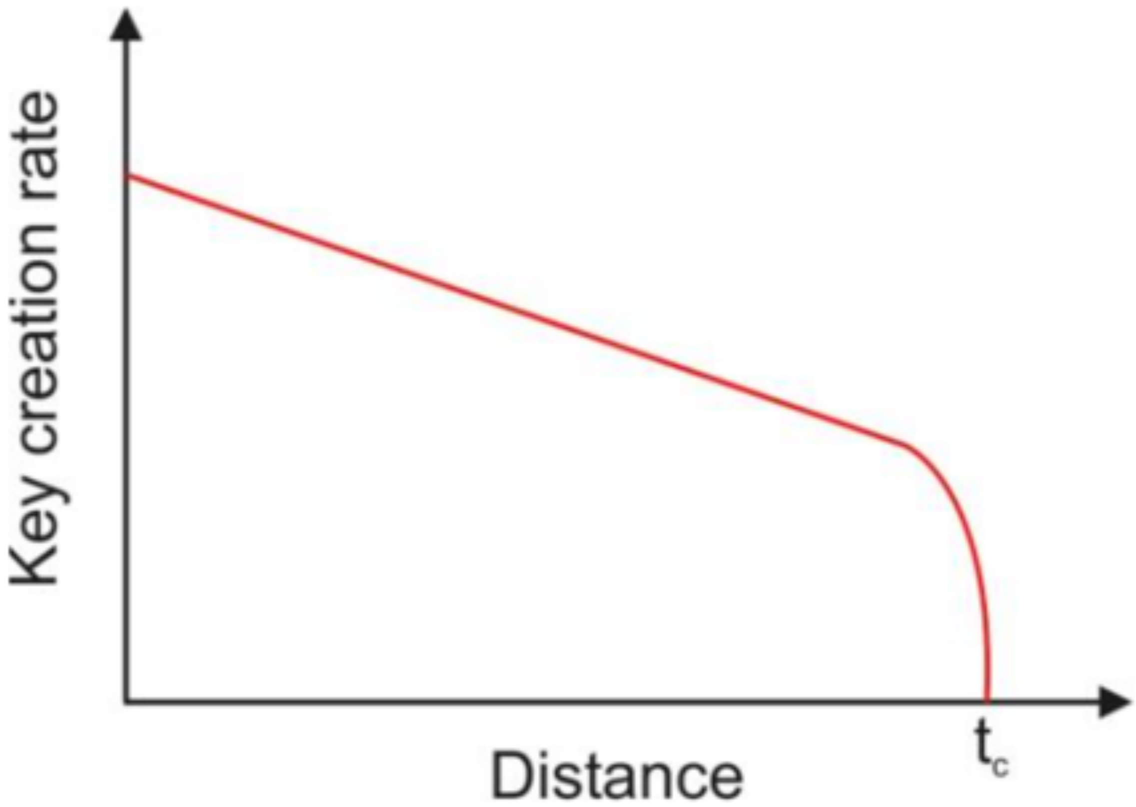
steps of BB84:

1. quantum communications
2. sifting – selection of the true correlation
3. error estimate
4. error correction
5. privacy amplification



QKD Protocol using photons

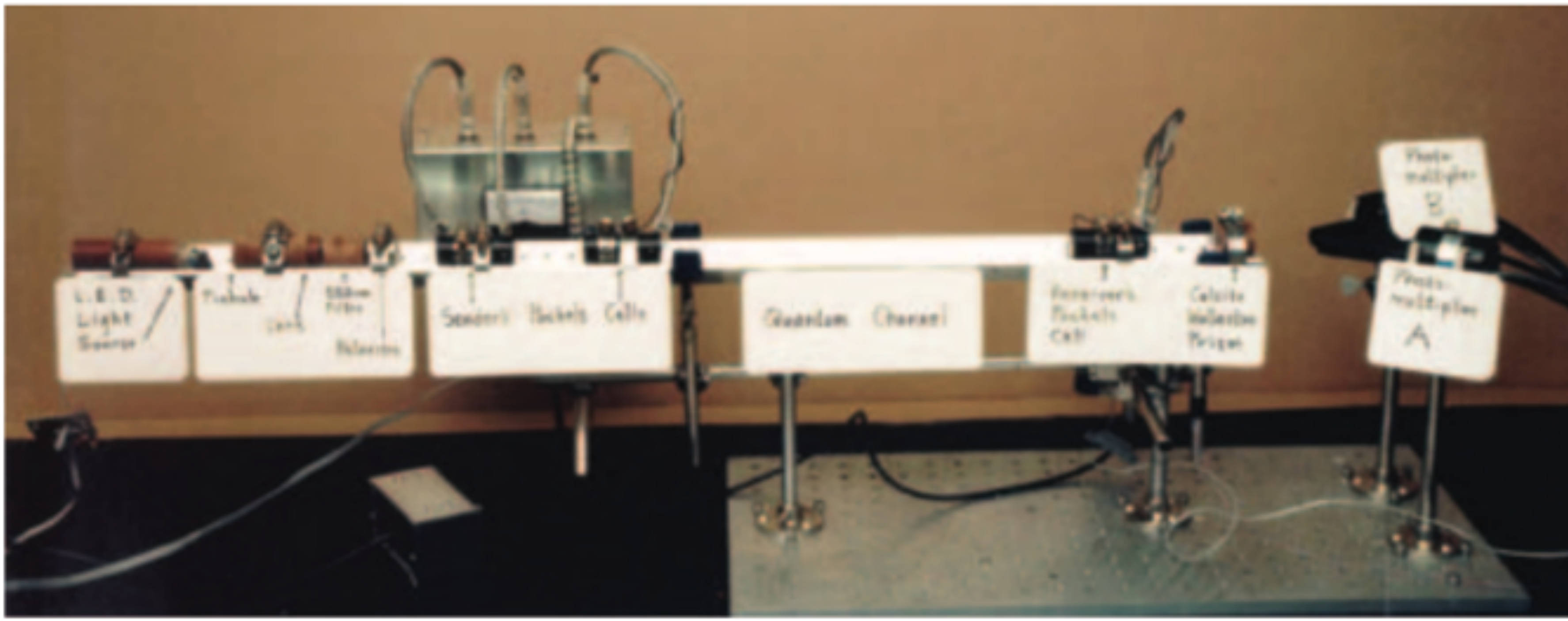
trend of key exchange rate with distance (losses)



QKD Protocol using photons

first realization of BB84 protocol, in 1992

320 mm of QKD link



C. Bennett et al. Experimental quantum cryptography. *J. Cryptol.* **5**, 3–28 (1992)

QKD using discrete components

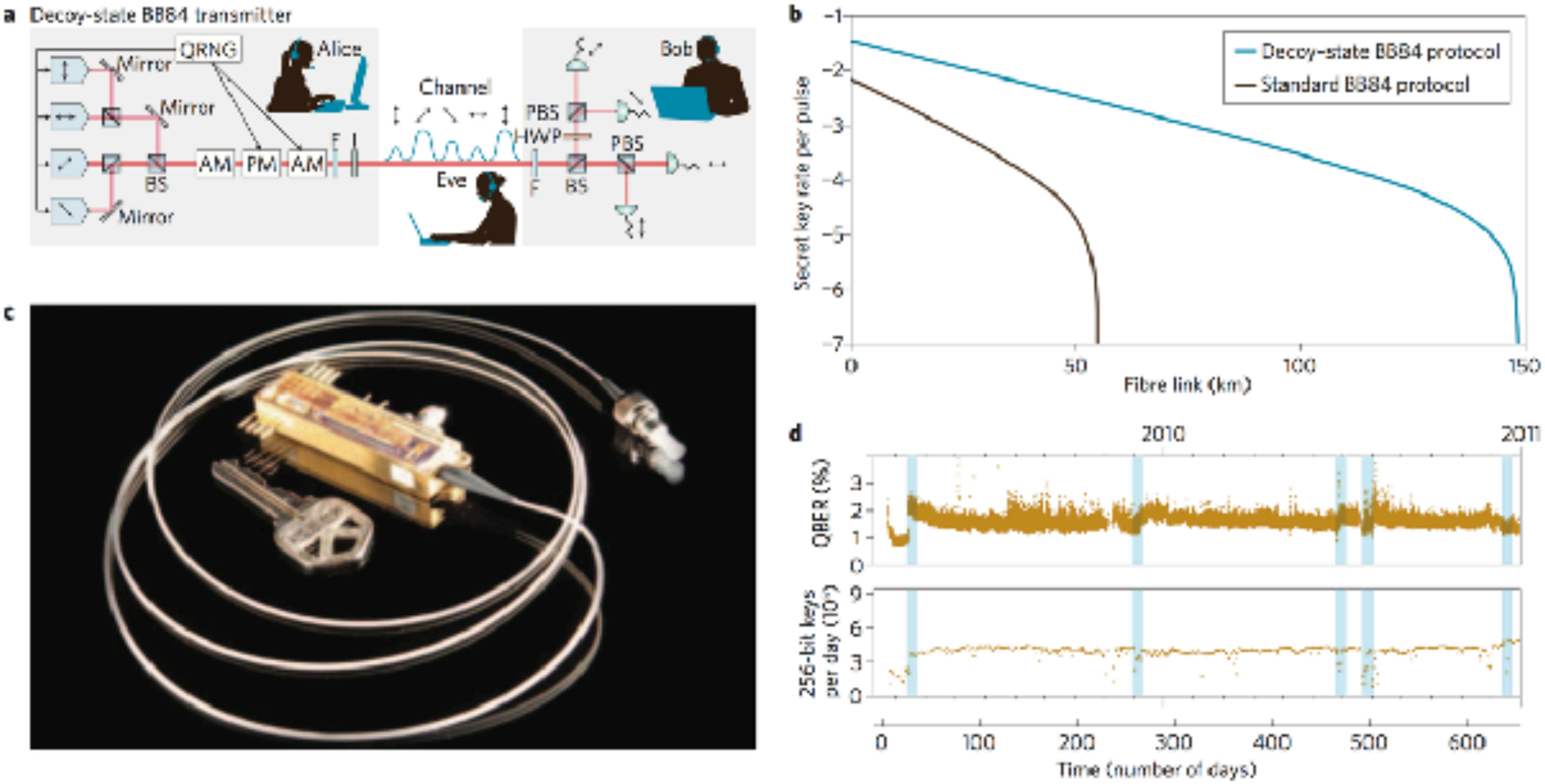
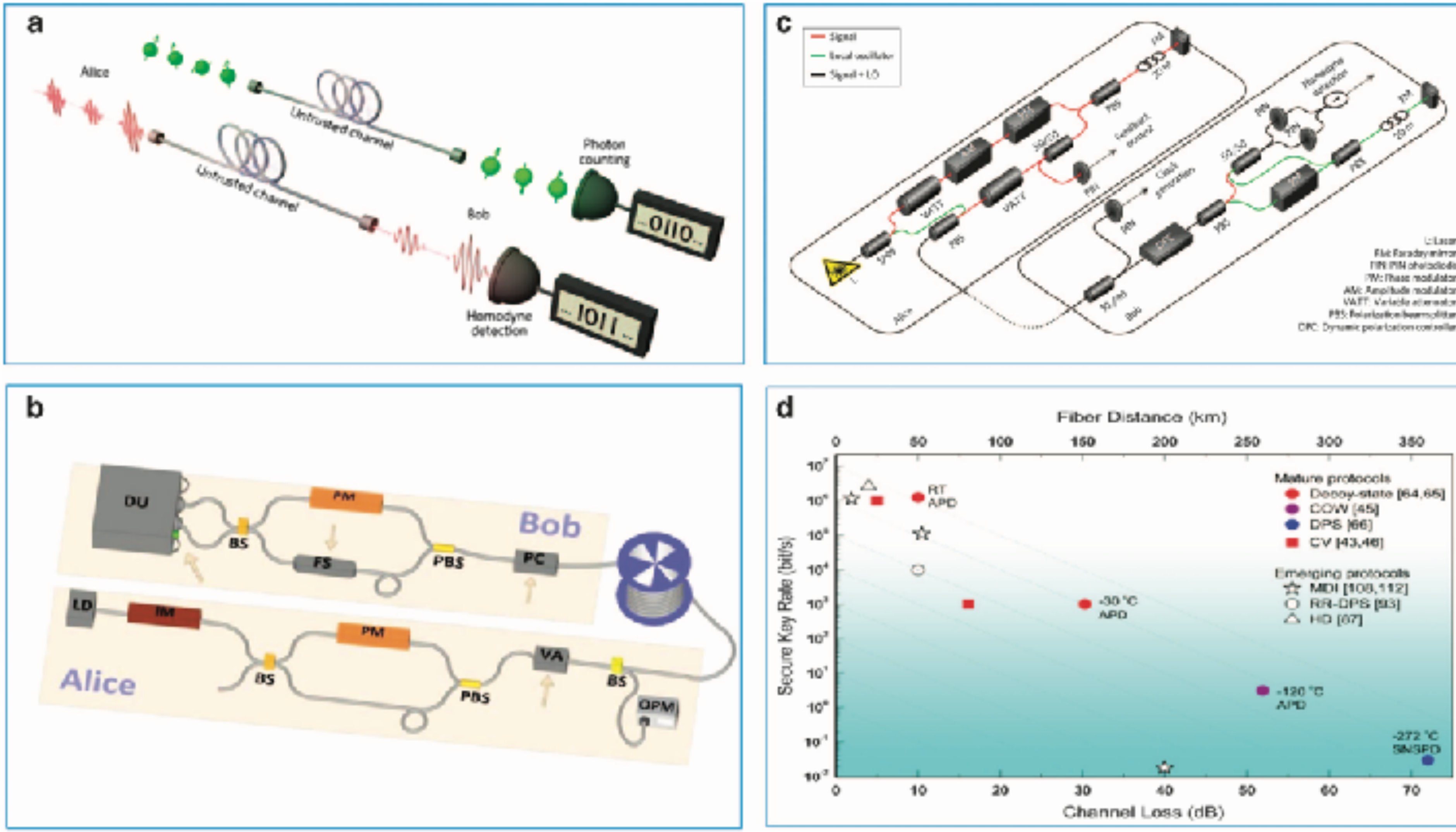


Figure 2 | Experimental QKD. a, Schematic of the decoy-state BB84 protocol[28–35] based on polarization coding. Four lasers are used to prepare the polarizations needed in BB84. Decoy states are generated with an amplitude modulator (AM). On Bob's side, a 50:50 beamsplitter (BS) is used to passively ensure a random measurement basis choice. Active receivers are also common. PM, phase modulator; F, optical filter; I, optical isolator; HWP, half-wave plate; PBS, polarizing beamsplitter; QRNG, quantum random number generator. **b**, Lower bound on the secret key rate (per pulse) in logarithmic scale for a BB84 set-up with two decoys (blue line)[25]. In the short-distance regime, the key rate scales linearly with the transmittance, η. Standard BB84 protocol without decoy states (dark brown line)[23,25]; its key rate scales as η^2. **c**, Photograph of a fibre-coupled modularly integrated decoy-state BB84 transmitter based on polarization coding[27]; it produces decoy-state BB84 signals at a repetition rate of 10 MHz. **d**, Performance of the SwissQuantum network[9]. This network was operated for more than 18 months in Geneva, Switzerland. The data shown in the figure correspond to a QKD link of 14.4 km; they highlight the stability of current QKD set-ups. QBER, quantum bit error rate. Figure adapted with permission from: **c**, ref. 37, © 2013 LANL; **d**, ref. 9, © 2011 IOP.

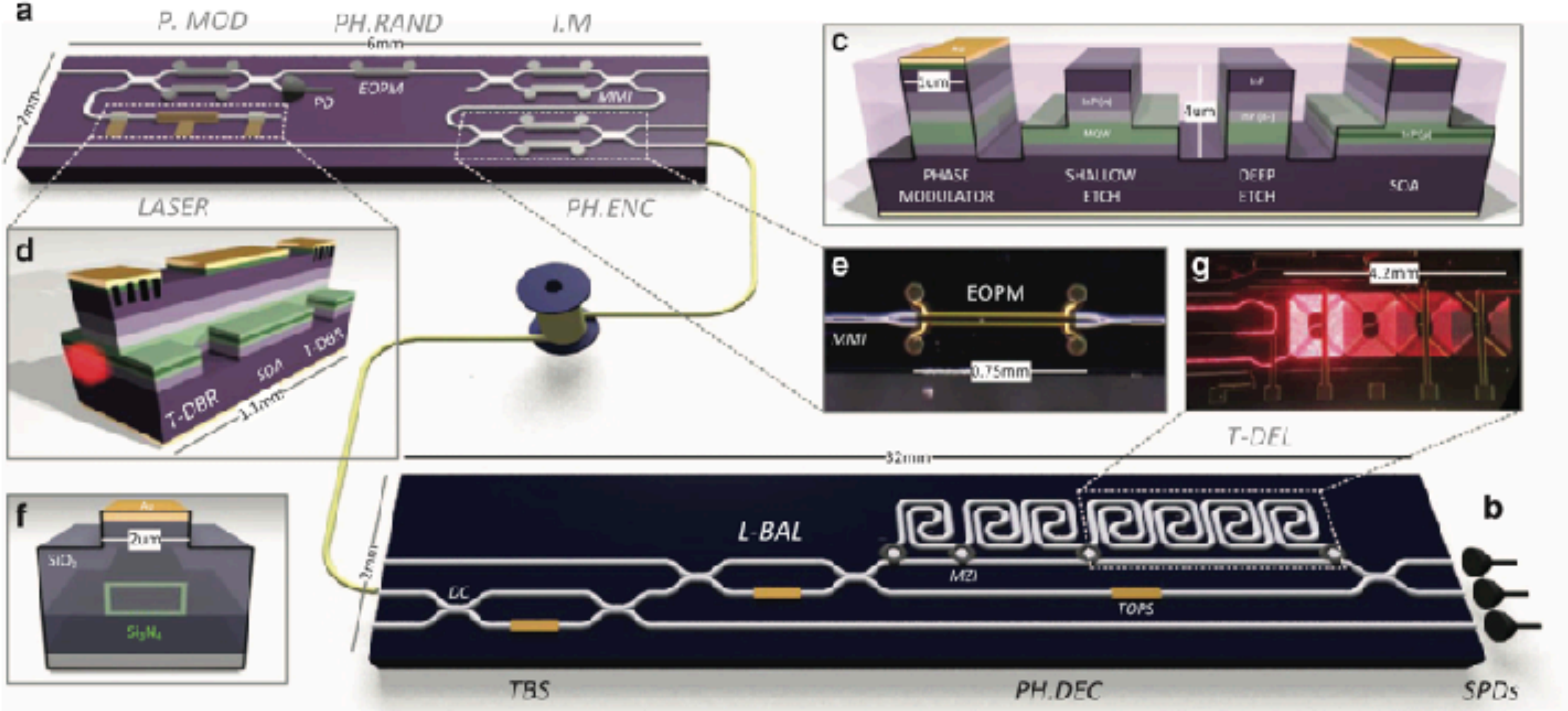
H-K Lo et al. Secure quantum key distribution *Nat. Phot.* **8** 595 (2014)

QKD Protocol using photons



E. Diamanti et al. Practical challenges in quantum key distribution
npj Quantum Infor. **2** *16025 (2016)*

QKD integrated photonics



E. Diamanti et al. Practical challenges in quantum key distribution
npj Quantum Infor. **2** *16025 (2016)*

QKD fiber commercial devices

China devices for key distribution

Quantum Safe Service Mobile Engine

QSS–ME

QSS–ME enables the quantum key resources to be integrated into mobile equipments through quantum secure media products and manages mobile requirements dynamically. It provides various services to users including but not limited to key agreements between multi-points, access authentication, access control, security storage.

Based on wide distribution network of quantum keys, QSS–ME provides local and roaming access–service for users to access quantum network easily and keep its highly security protection especially, even at home, in an office or in travel.

QSS–ME breaks though the limitation of point–to–point mobile encrypted communication, provides security to users as a service. It shows infinite possibilities of application extensions which are not restricted by OS, application protocols and application platforms.

QKChr

Quantum Keys Charger (QKChr) is a storage station of the resources of quantum keys. It is safe and trusted for QUKey, QTCard and other secure media to access the quantum networks through QKChr and updates the resources of quantum keys which will escort the quantum mobile security.

QKChr acquires quantum keys from KM in real-time through a dedicated communication interface, performs charging by using local USB, Micro SD, etc. at the same time. With rich interfaces, QKChr can be smoothly connected to diverse systems and platforms, meeting the requirements of quantum key charging in various application scenarios.

QTCard

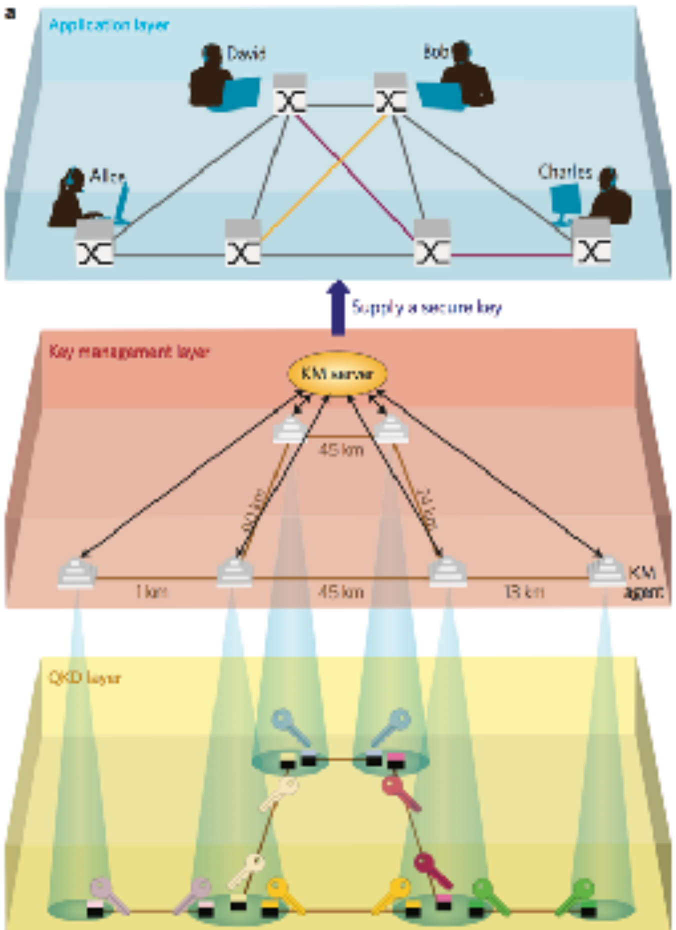
QTCard has same appearance and interface with standard TF card which accepts a low power and high speed dedicated security chip. With new online QSS–ME, QTCard can combine the quantum keys with mobile phones, PADs and other mobile terminal applications. It helps to provide mobile security services which is based on quantum keys to satisfy storage expanding of mobile devices.

Quantum Security Encryption Mobile Phone ZTE AXON 7S

The world's first commercial Quantum security encryption mobile phone–The Quantum Security Version of ZTE AXON 7S, is jointly developed by QuantumCTek and ZTE. QuantumCTek and ZTE had maintained close cooperation and achieved many successes. Based on each other's core strengths and communications security demand, Technology R & D team innovatively incorporate quantum secure communications technology into ZTE's Flagship Model–AXON 7S to create the Quantum Security of AXON 7S. The mobile phone is based on the QSS–ME platform and NTOS autonomous secure operating system. Compared with the traditional mobile phone, its unique quantum security encryption and operating system security features more application value in the age of information security that emphasizes privacy protection.

http://www.quantum-comm.com/English/product/

QKD networking



QKD networks have been deployed in the USA, Austria, Switzerland, China and Japan

Italy has the national QKD backbone initiative

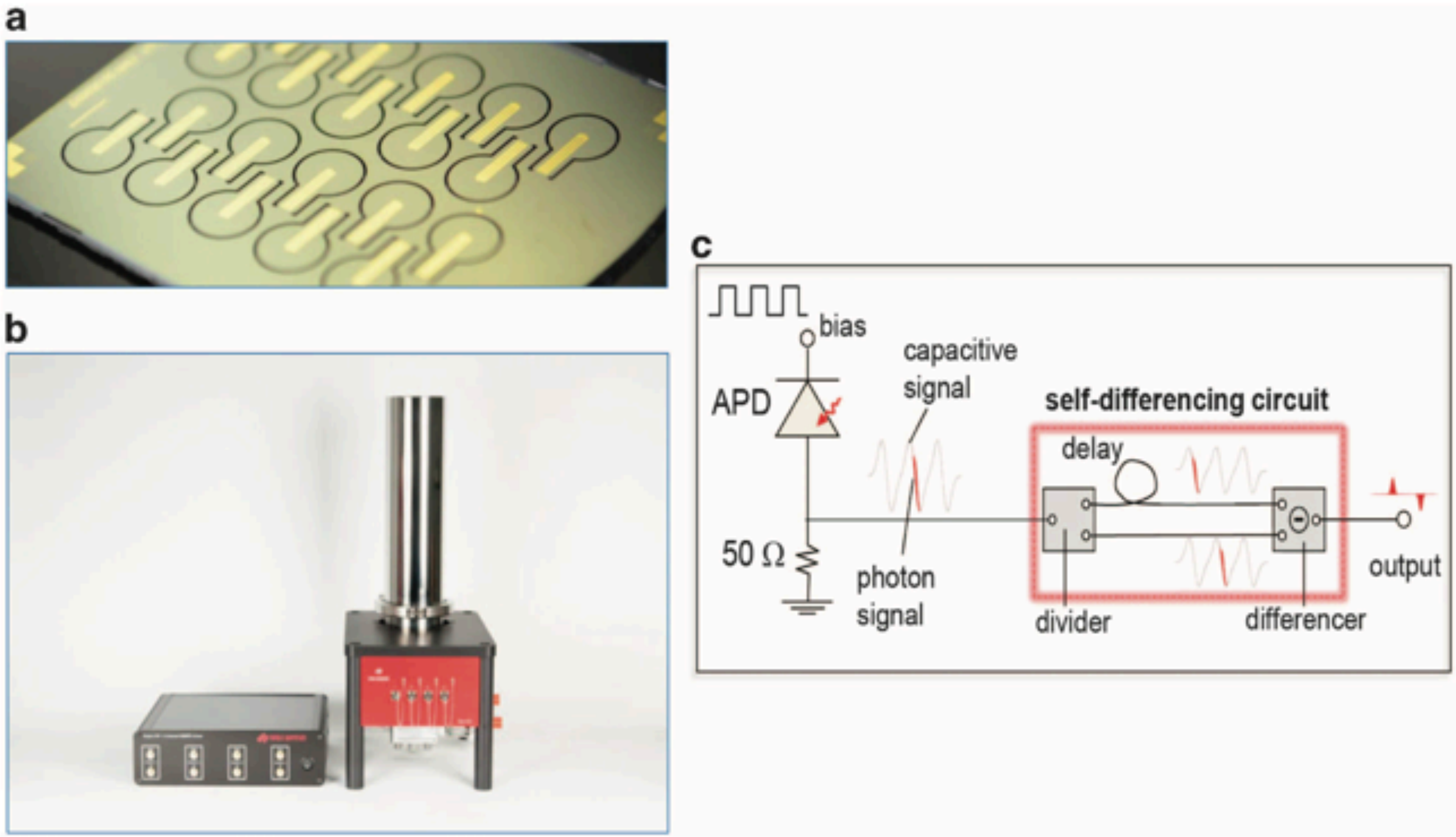
the scope is to join locations using trusted nodes

H-K Lo et al. Secure quantum key distribution *Nat. Phot.* **8** 595 (2014)

Chinese QKD networking

Chinese QKD networking

QKD single photon detectors



E. Diamanti et al. Practical challenges in quantum key distribution
npj Quantum Infor. **2** *16025 (2016)*

QKD device hacking

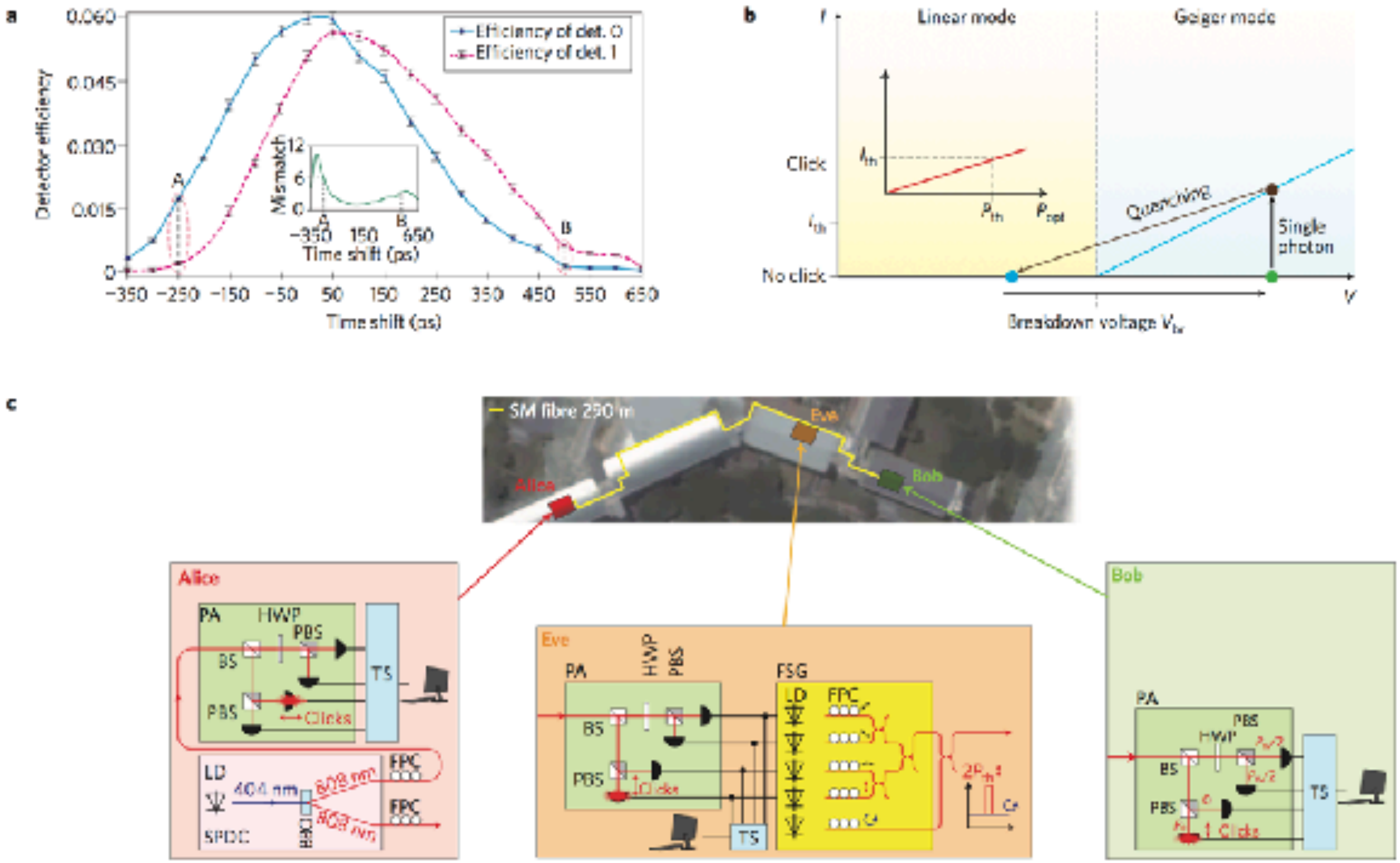


Figure 4 | Examples of quantum hacking. a, Experimentally measured detection efficiency mismatch between two detectors from a commercial QKD system versus time shifts[76]. Eve could exploit this to perform a time-shift attack[75]; that is, she could shift the arrival time of each signal such that one detector has a much higher detection efficiency than the other. **b,** Working principle of the detector blinding attack[80]. By shining intense light onto the detectors, Eve can make them leave Geiger-mode operation (used in QKD) and enter linear-mode operation. In so doing, she can control which detector produces a 'click' each given time and learn the entire secret key without being detected. **c,** Full-field implementation of a detector blinding attack on a running entanglement-based QKD set-up[83]. HWP, half-wave plate; PBS, polarizing beamsplitter; BS, beamsplitter; LD, laser diode; SPDC, spontaneous parametric downconversion; BBO; β-barium-borate crystal; FPC, fibre polarization controller; TS, timestamp unit; PA, polarization analyser; FSG, faked-state

H-K Lo et al. Secure quantum key distribution *Nat. Phot.* **8** 595 (2014)

Quantum Communications in Space

- **Quantum Communications: faithful sharing of qubits between separate correspondents**
  - **Test for the Principles of Quantum Physics in a new context**
  - **Massless Probe from a moving terminal, along a channels where Relativistic effects may be revealed using quantum interferometry, polarization, etc.**
- **Space QC: demonstration of protocols for secure communications such as quantum-key-distribution (QKD) and quantum teleportation along**
  - **satellite-to-ground or**
  - **intersatellite links.**

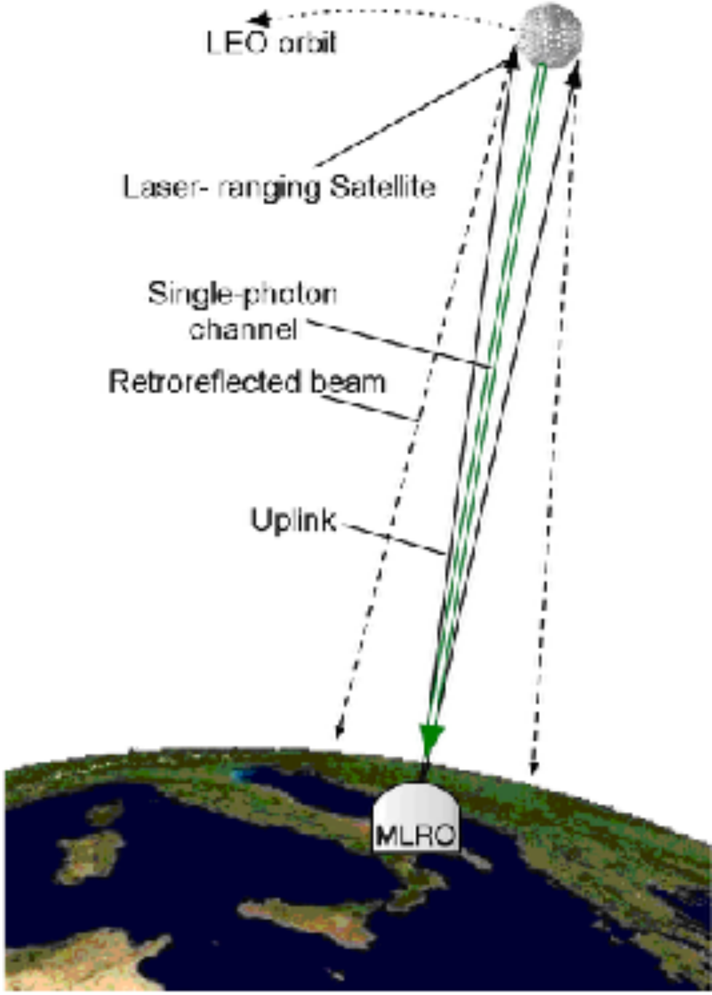
Our knowledge is ultimately restricted by the boundaries of what we have explored by direct observation or experiment.

Scenario opportunities in Space Q-Comms

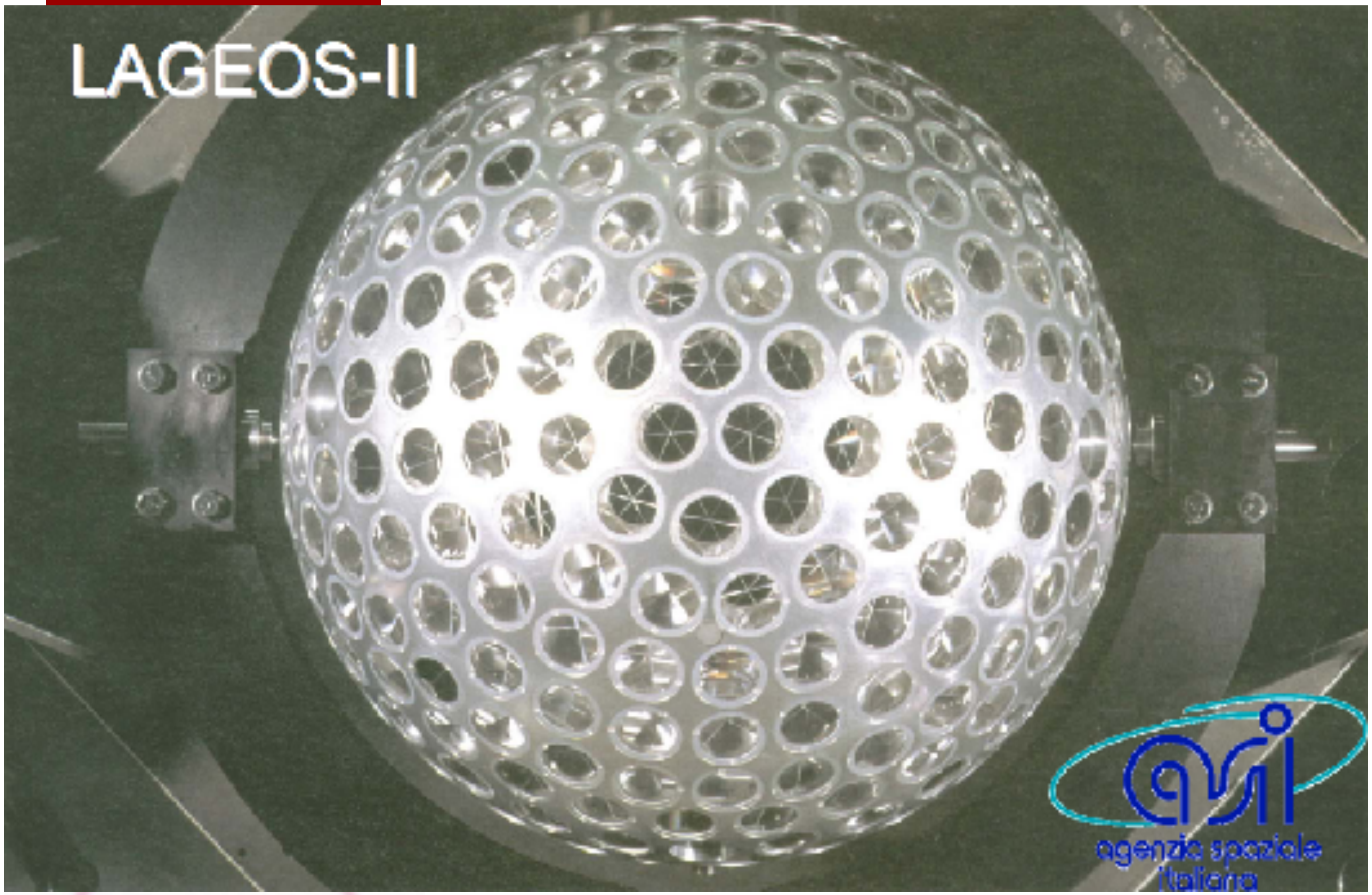
- **LEO orbits**
  - rapid passages – large coverage – small payloads
  - secure communications (QKD – encryption of data)
  - fundamental test of Quantum Physics (Bell's test)
- **GEO orbits**
  - large optical aperture
  - securing data relay
  - precise test of interplay of Gravity and Quantum Physics
- **Intersat links and deep space missions**
  - exploring the limits of quantum correlations
  - interconnession of atomic clocks

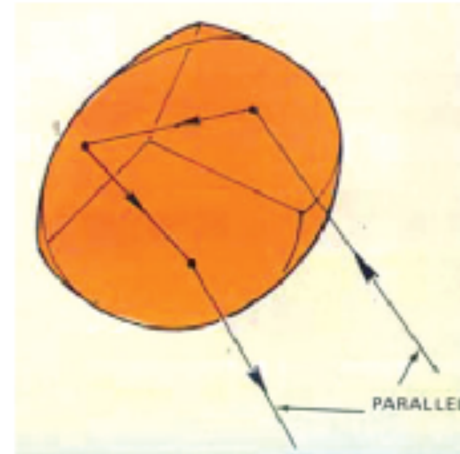
Investigation of QC along space channel without active satellite

- **Orbiting retroreflectors may be used in a two-way link with a single telescope on ground**
- They ***may*** preserve
  - **the polarization state**
  - **the temporal coherence**
- **The channel transfer function** is modeled according to:
  - **diffraction losses,**
  - **atmospheric absorption,**
  - **wavefront degradation due to turbulence**
  - **reflectivity of the retroreflector**
  - **optical characteristic of the ground station**



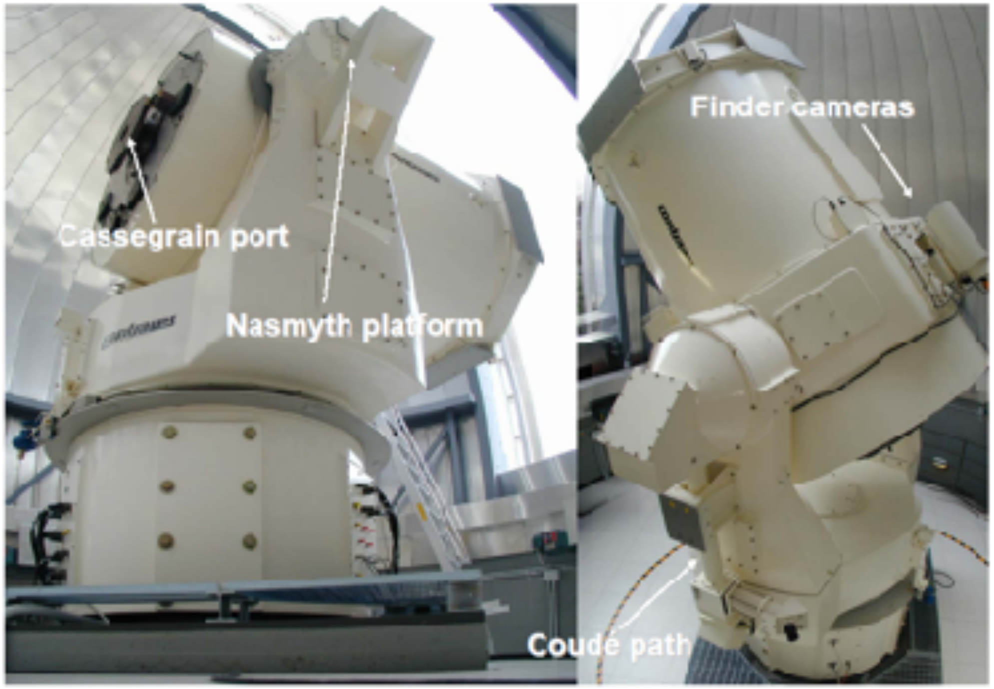
Corner-cube retroreflectos



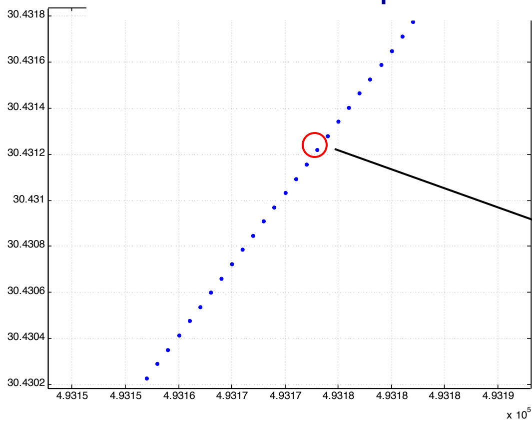


The ground station: Matera ASI-MLRO

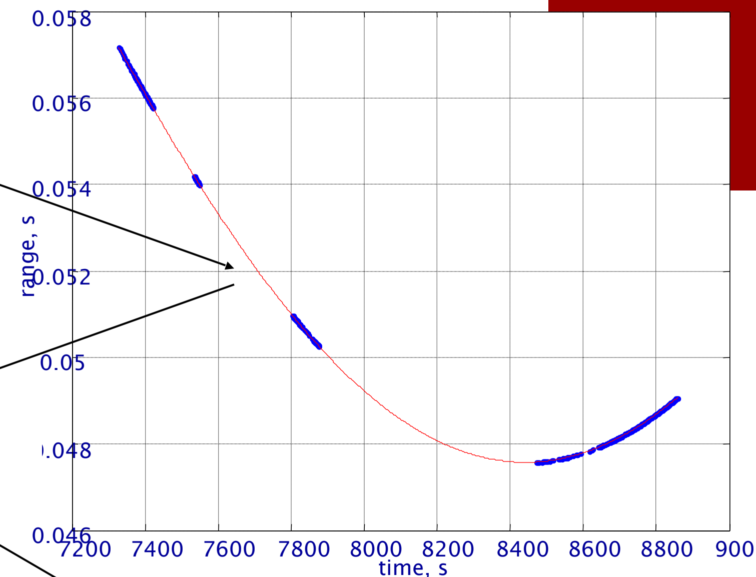
- *Giuseppe Colombo* Space Geodesy Centre of Italian Space Agency - Matera Laser Ranging Observatory (MLRO)
- Director Dr. Giuseppe Bianco President of ILRS
- World highest accuracy in SLR: mm-level for about 10^7 m range
- Accurate lunar ranging



Launched laser pulses

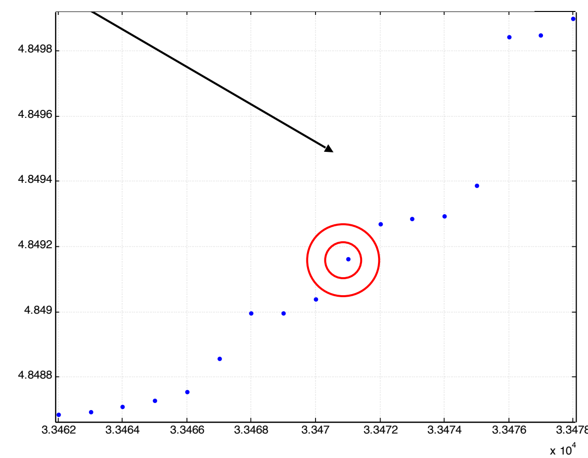


Satellite range



Instrumental offset

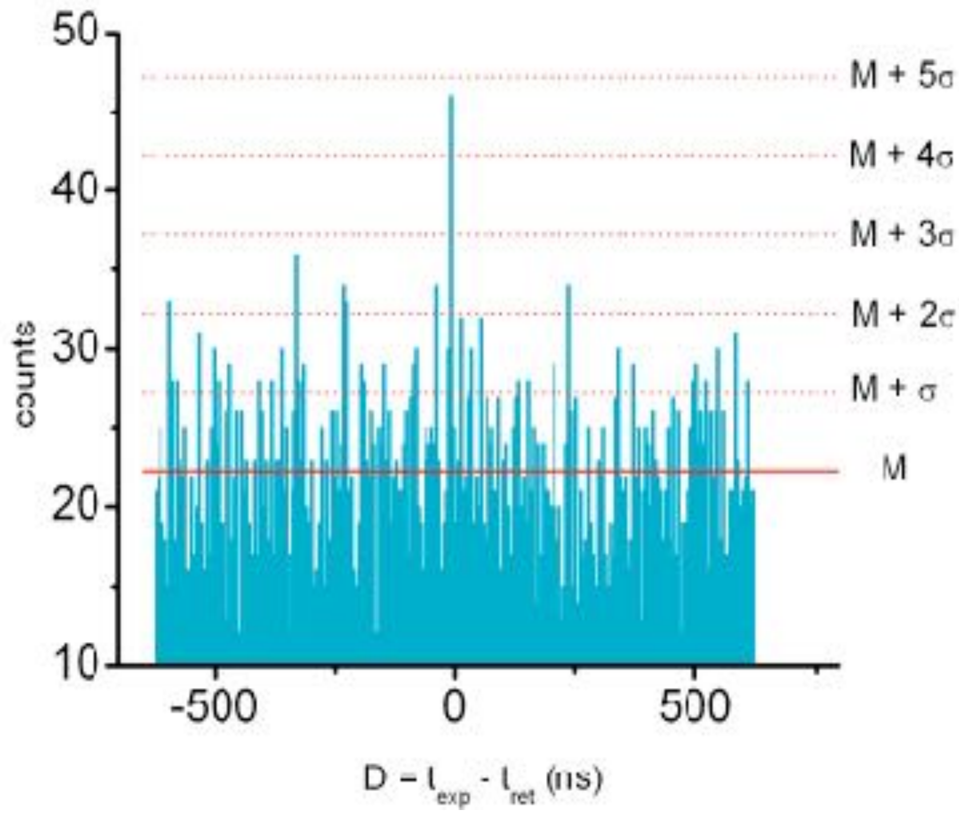
Detector clics vs. time



Scheme for the search of the returns

Single-photon link with Ajisai

- A peak of 5 cps was observed at D=0 above the background.
- The peak height exceeds 4 times the rms of the background.
- Total losses are of -157 dB.
- In the downlink channel, $\mu = 0.4$, and so clearly in the single-photon regime.
- DCR = 17 kHz X p(click) 3 10^{-4} per pulse.
  - Integration 5 s
  - Bin-size 5 ns
  - FOV 30”
  - Filter 10 nm BW

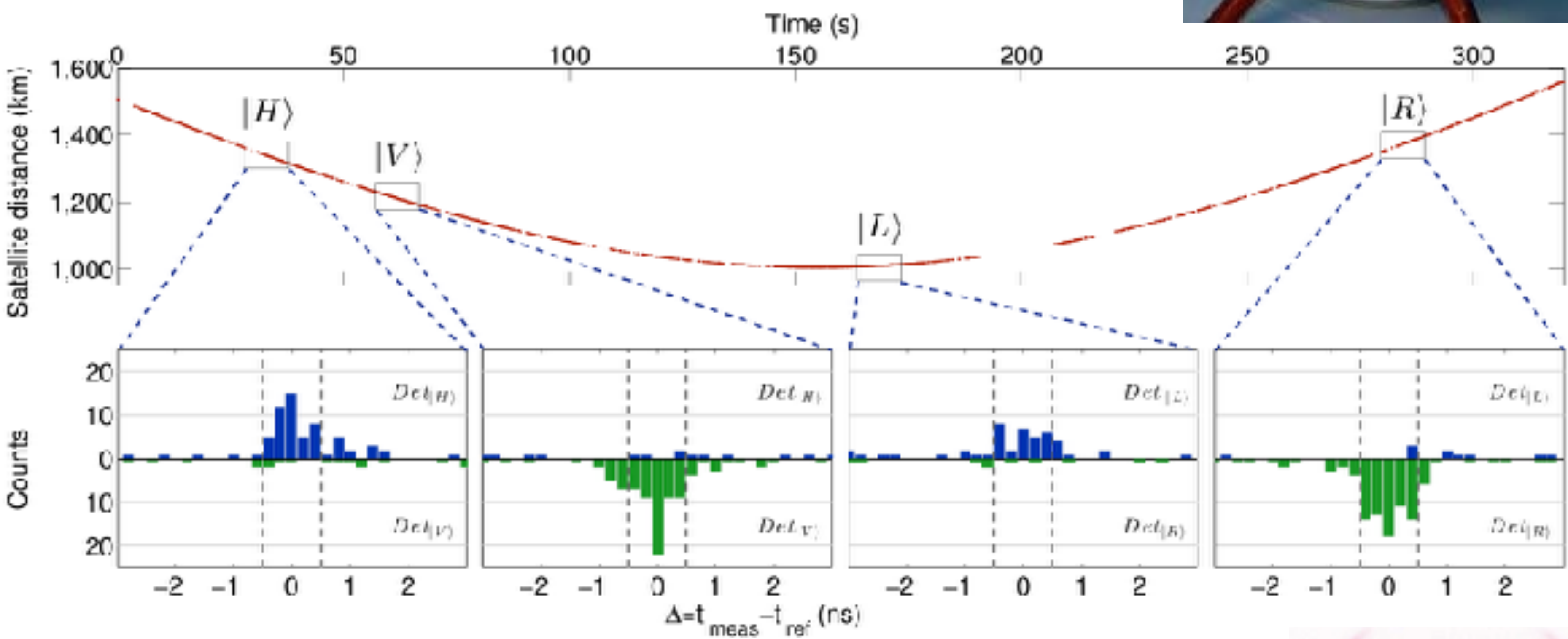


P. Villoresi et al. New J. Phys. 10 033038 (2008)

Single passage of LARETS

Orbit height 690 km - spherical brass body
24 cm in diameter, 23 kg mass,
60 cube corner retroreflectors (CCR)
Metallic coating on CCR

Apr 10^{th}, 2014, start 4:40 am CEST



- **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, Physical Review Letters, **115** 040502, 2015

QBER

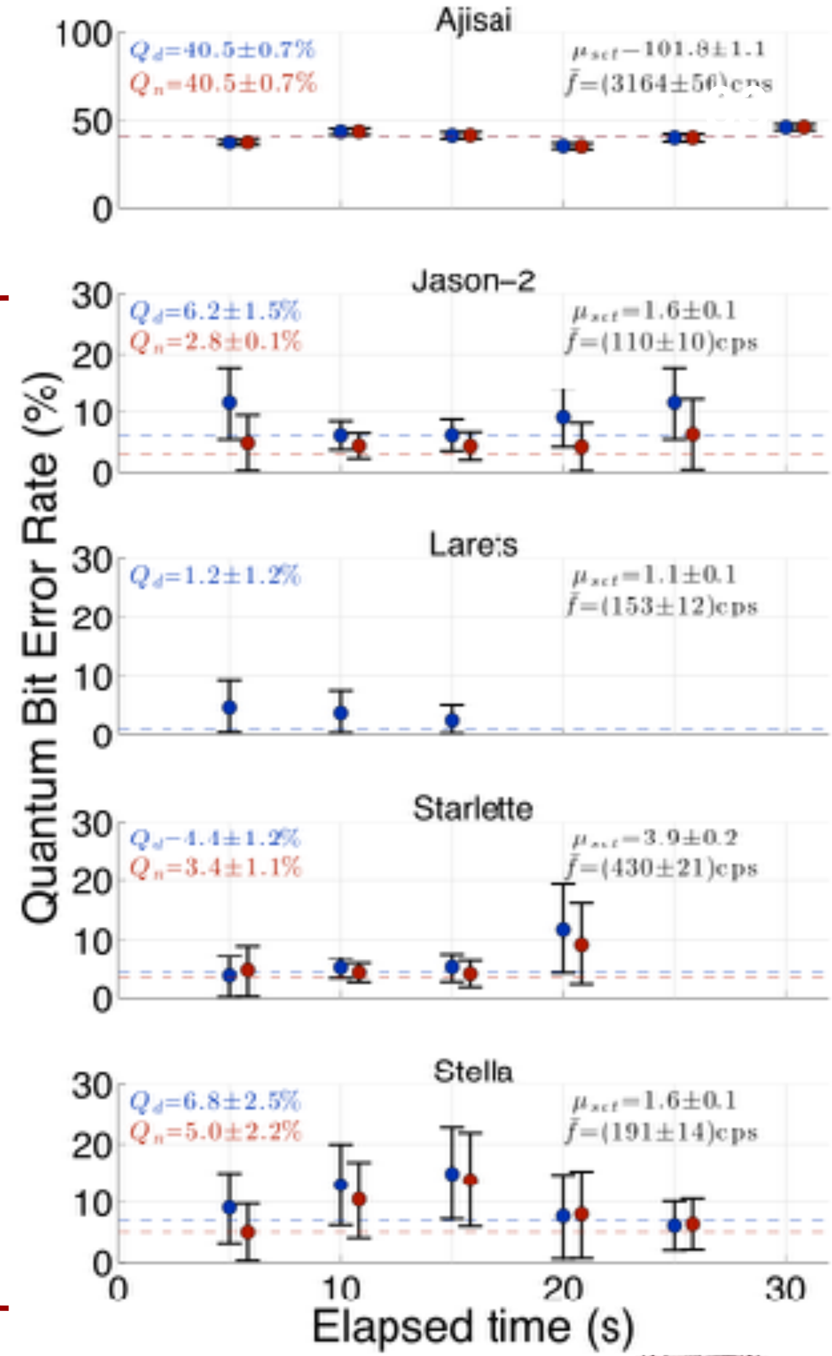
Non polarization maintaining CCR
Polarization QComm not possible

Polarization maintaining CCR

Polarization QComm with QBER compatible with applications

Demonstration of stable QBER over extended link duration

With LARETS μ=1.1 and QBER 1.2%

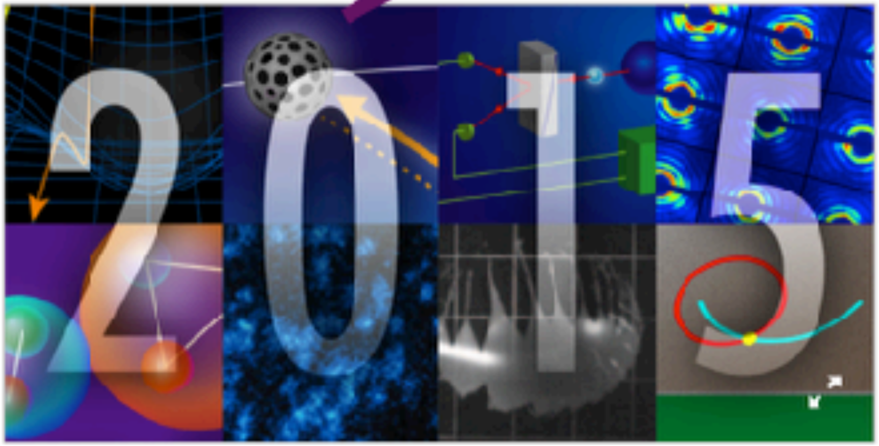


G. Vallone et al, Physical Review Letters, **115** 040502, 2015

Highlights of the Year

December 18, 2015 • *Physics* 8, 126

***Physics* picks its favorite stories from 2015.**



As 2015 draws to a close, we look back on the research covered in *Physics* that really made waves in and beyond the physics community

Wishing everyone an excellent 2016.

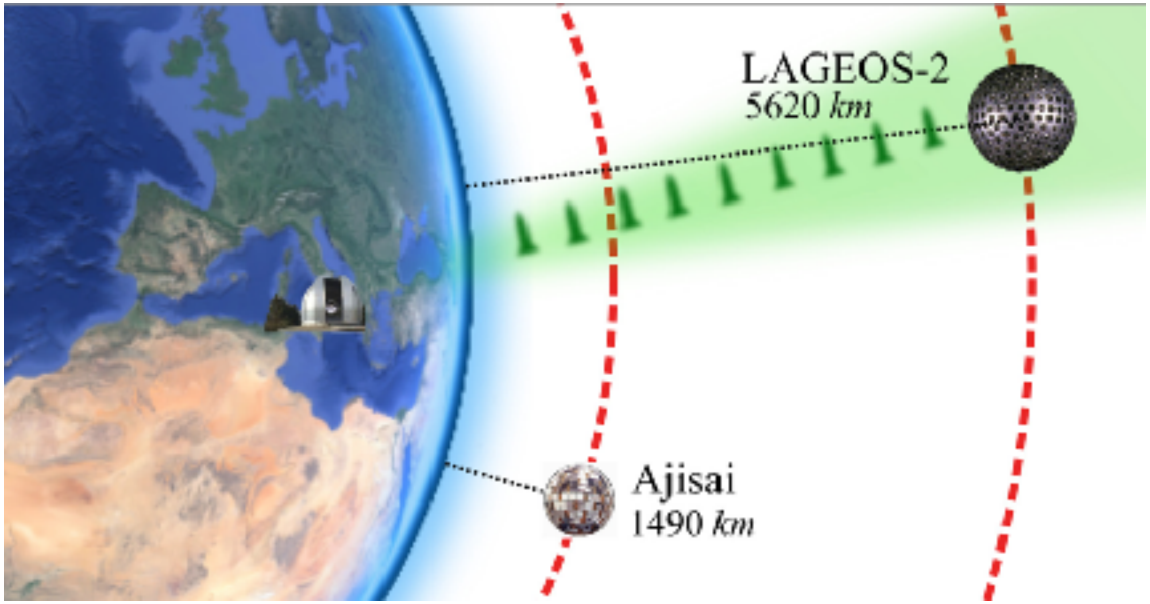
–The Editors

Qubits in Space

Photons have been used to securely transmit quantum encryption keys over more than 300 kilometers of optical fiber. Ultimately, light attenuation limits how far a fiber can transmit a signal without degrading its quantum properties. But satellite-to-Earth links might soon open new frontiers for quantum communication. Researchers from the University of Padua and the Matera Laser Ranging Observatory, both in Italy, demonstrated that qubits encoded in photons can preserve their fragile quantum properties even after a round trip to satellites located more than one thousand kilometers away from Earth (see Viewpoint: Sending Quantum Messages Through Space). The authors encoded qubits in the photons' polarization and sent them to five satellites that bounced the light back to Earth. After the long journey, different qubit states could be distinguished reliably enough for viable quantum protocols.

Single Photon exchange: from LEO to MEO

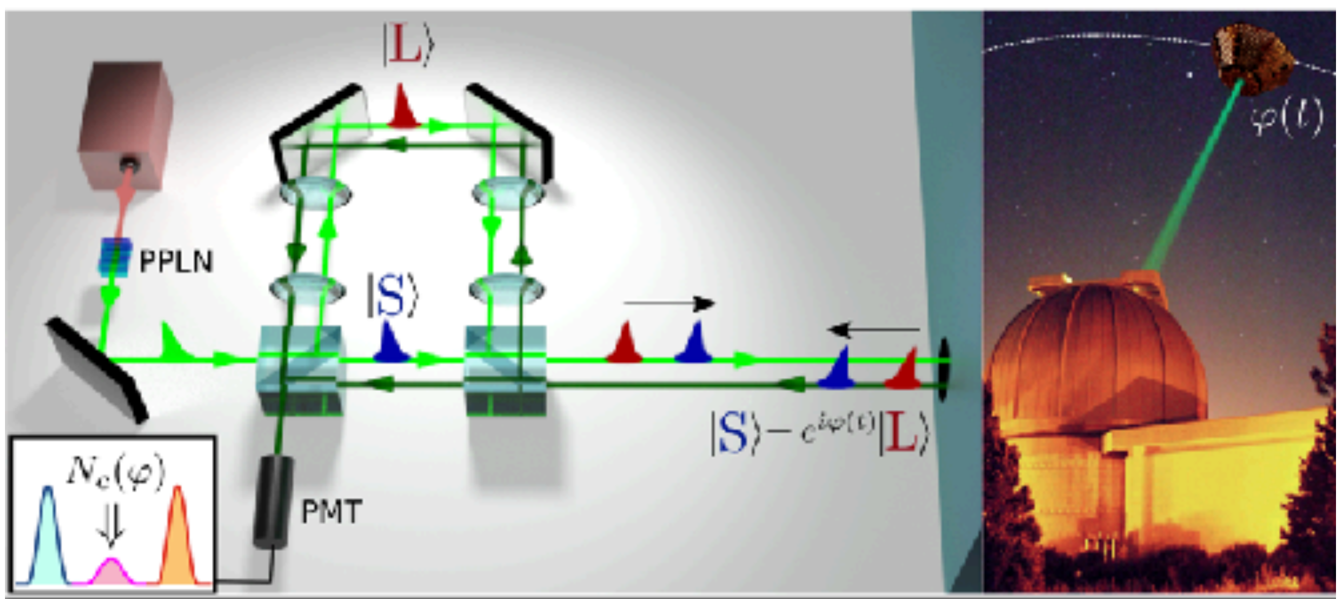
Demonstration of the detection of photon from the satellite which, according to the radar equation, is emitting a single photon per pulse from a **Medium-Earth-Orbit MEO** satellite.



D. Dequal et al. *Experimental single photon exchange along a space link of 7000 km*, PRA Rapid Comm **93** 010301, 2016.

QComms exploiting temporal modes of light

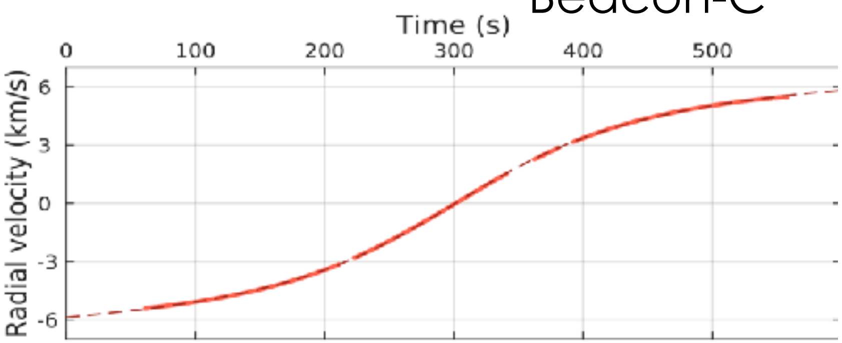
- Quantum interference arising from superposition of states is a striking evidence of the validity of Quantum Mechanics, confirmed in many experiments and also exploited in applications.
- We aim to the single-photon interference at a ground station due to the coherent superposition of two temporal modes reflected by a rapidly moving satellite thousand kilometers away.

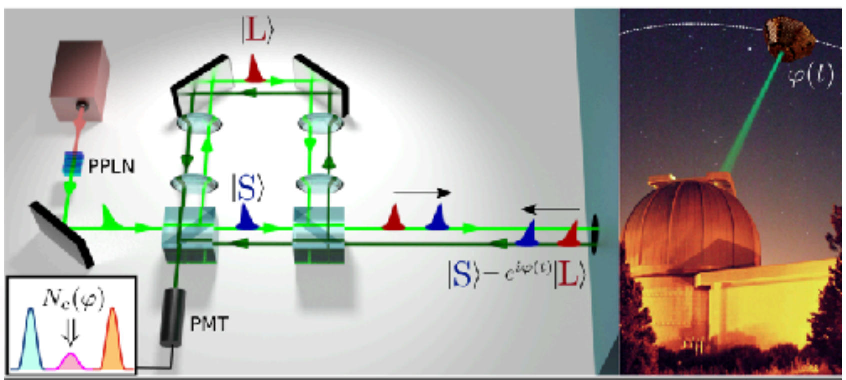


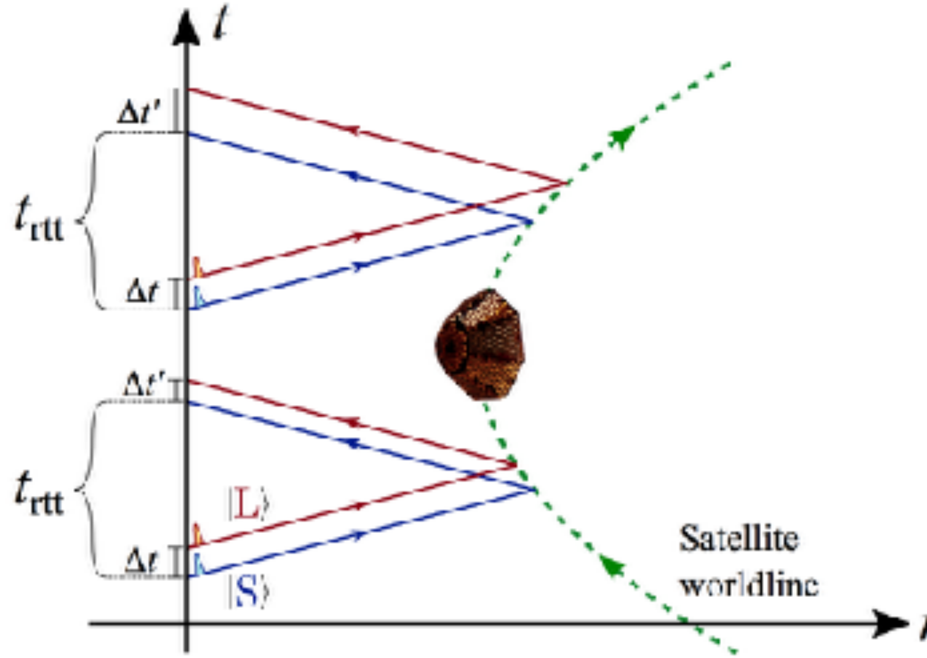
Kinematic Phase modulation

Relativistic effects on the photon interference

Beacon-C







Probability of click in the central peak

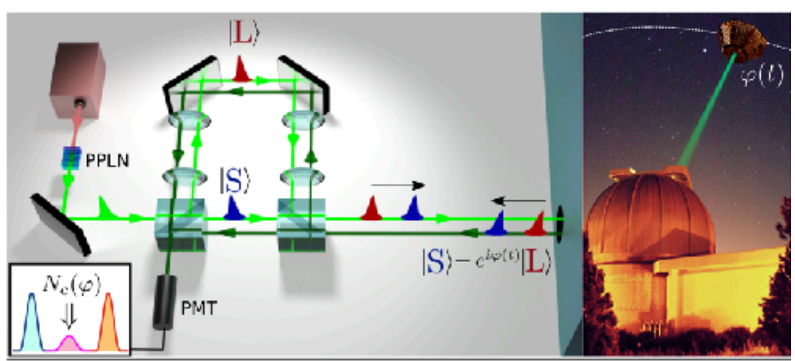
$$P_c(t) = \frac{\gamma^2(1-\beta(t))^2}{4}\int dt' \left|\psi_0(-f_\beta(t'+\Delta t)) - \psi_0(-\Delta t - f_\beta t')\right|^2$$

$$= \frac{1}{2}\left\{1-\sqrt{\frac{2}{\tau_c^2}}\int dt' \Re e\left[e^{-\pi\frac{(t'+f_\beta\Delta t)^2}{\tau_c^2}} e^{-\pi\frac{(t'+\Delta t)^2}{\tau_c^2}} e^{i\omega_0(1-f_\beta)\Delta t}\right]\right\}$$

$$= \frac{1}{2}\left[1-\mathcal{V}(t)\cos\varphi(t)\right],$$

Kinematic phase $\varphi(t) = \omega_0[1-f_\beta)]\Delta t = \frac{2\beta(t)}{1+\beta(t)}\omega_0\Delta t$

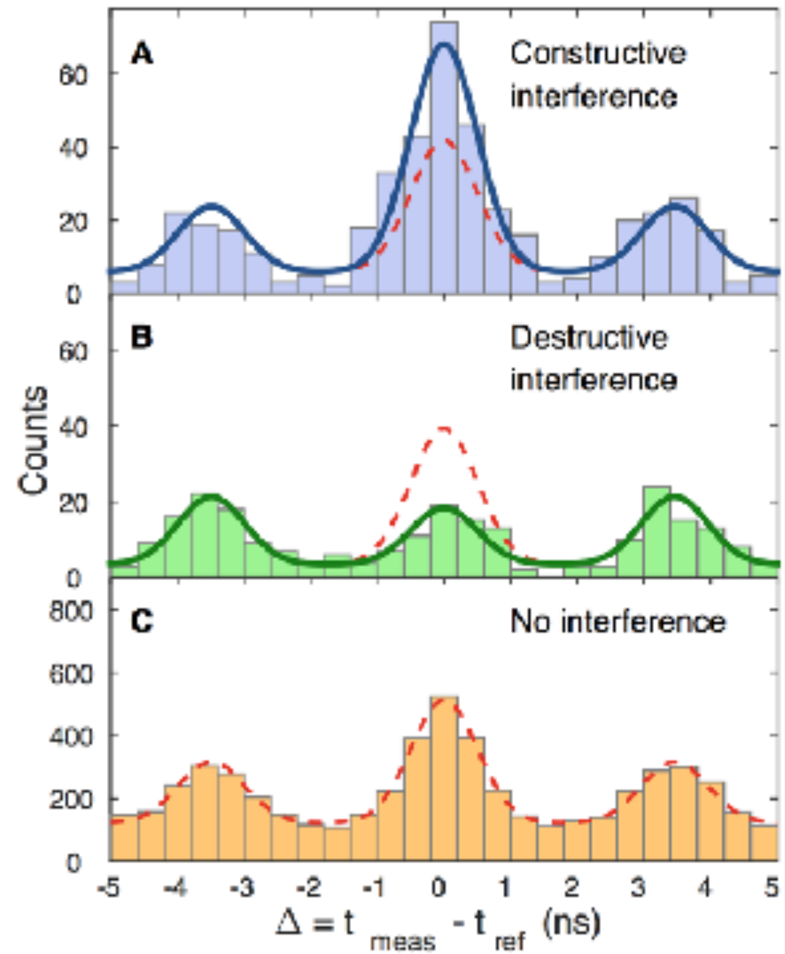
Visibility $\mathcal{V}(t) = \sqrt{\frac{2}{\tau_c^2}}\int dt' \, e^{-\pi\frac{(t'+f_\beta\Delta t))^2}{\tau_c^2}} e^{-\pi\frac{(t'+\Delta t)^2}{\tau_c^2}} = \exp\{-2\pi\left[\frac{\Delta t}{\tau_c}\frac{\beta(t)}{1+\beta(t)}\right]^2\}$



For LEO satellites it may be **approximate as 1**

Evidence of the interference

Beacon C



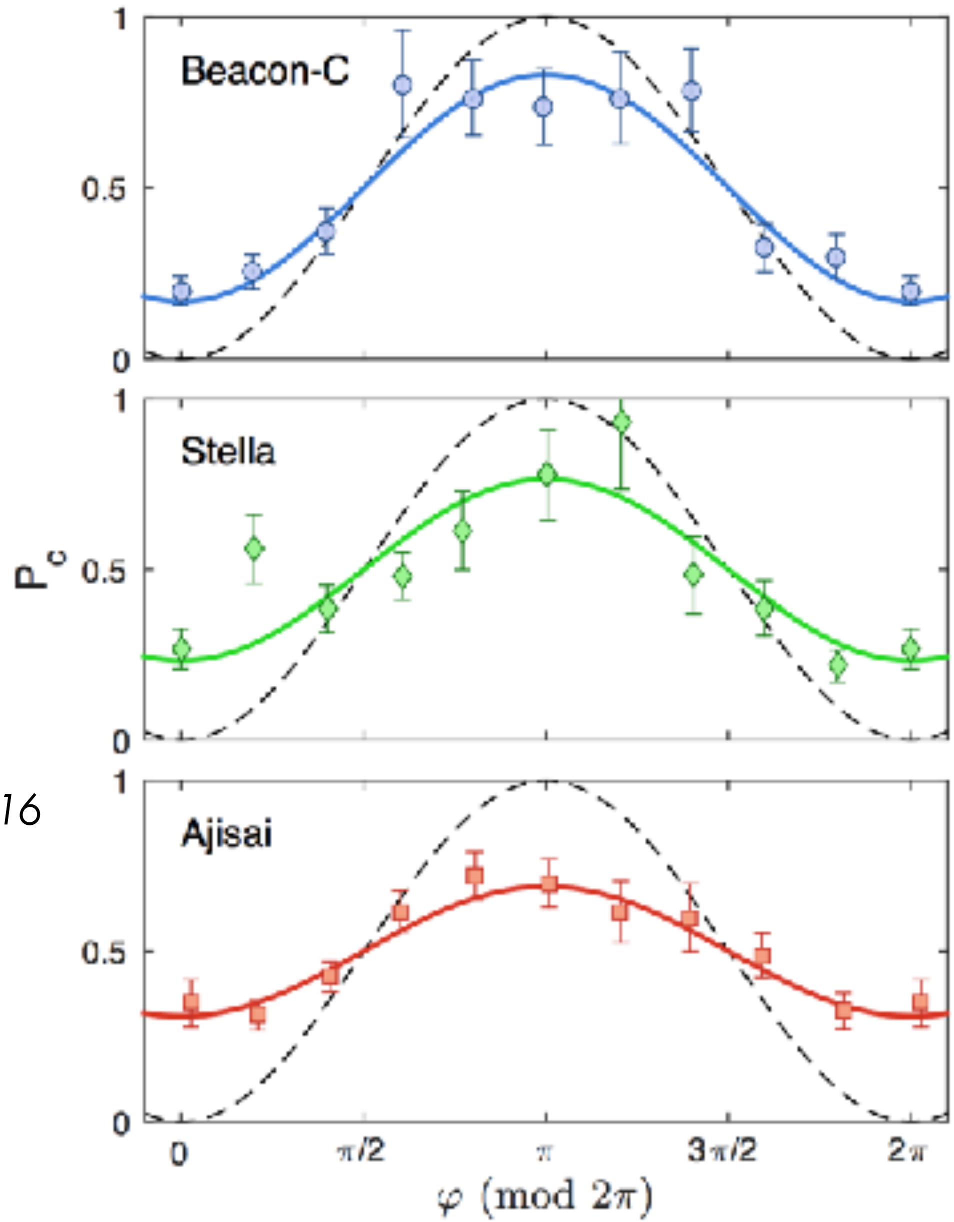
$$P_c(t) = \frac{1}{2}\left[1 - \mathcal{V}(t)\cos\varphi(t)\right]$$

$$\varphi(t) = \frac{2\beta(t)}{1+\beta(t)}\frac{2\pi c}{\lambda}\Delta t$$

$$\mathcal{V}(t) = e^{-2\pi\left(\frac{\Delta t}{\tau_c}\frac{\beta(t)}{1+\beta(t)}\right)^2} \simeq 1\,.$$

G. Vallone et al. *Interference at the Single Photon Level Along Satellite-Ground Channels*
Physical Review Letters ***116*** *253601 2016*
arXiv:1509.07855 (2015)

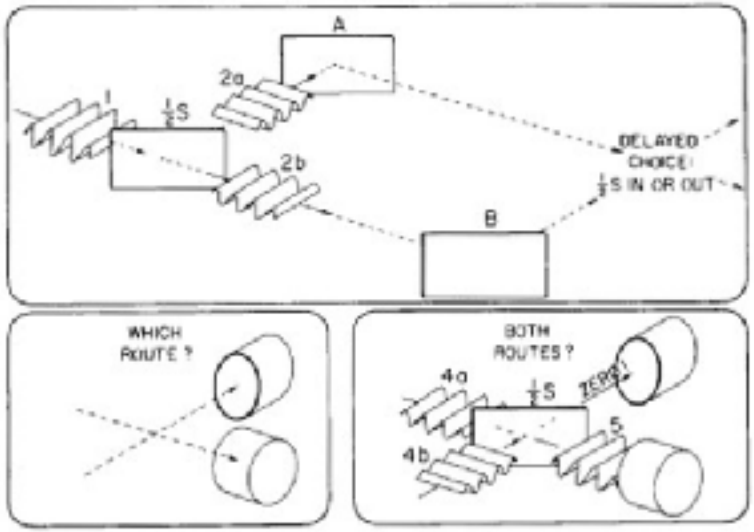
Visibility vs. φ(t)

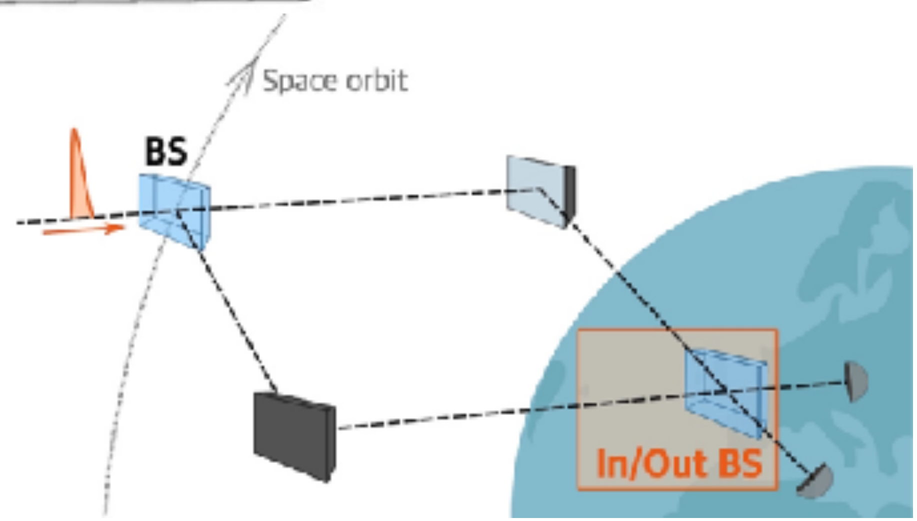


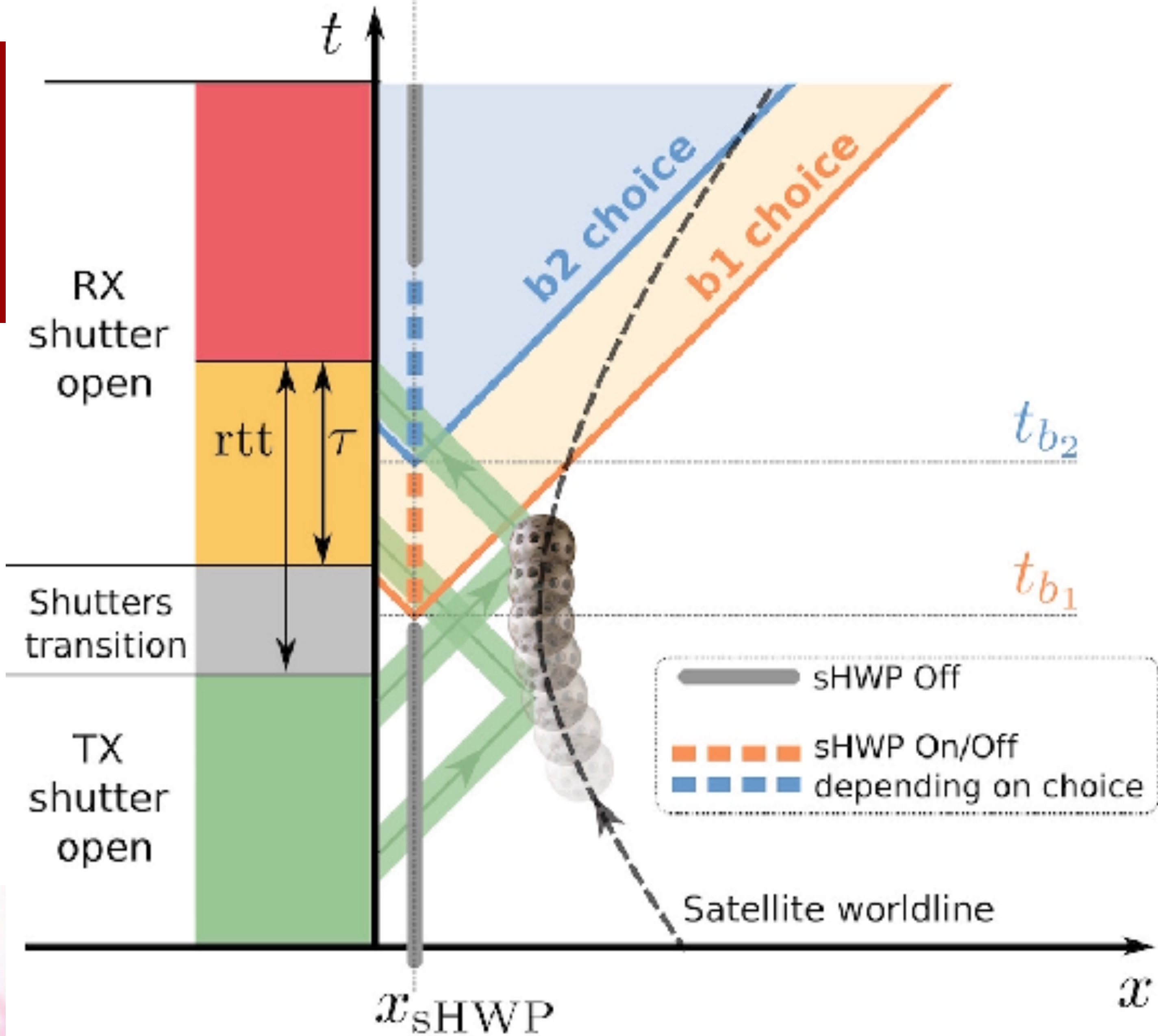
V_{exp}=67±11% for Beacon-C

G. Vallone et al. *Interference at the Single Photon Level Along Satellite-Ground Channels*
Physical Review Letters ***116*** *253601 2016*

Step forward in Space QComms: inquiring the wave-particle duality along a Space channel







F. Vedovato et al. - Science Adv. **3** e1701180 (2017)

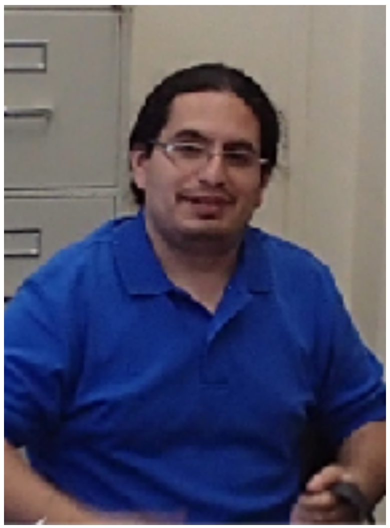
QMemories are crucial tools for QComms!

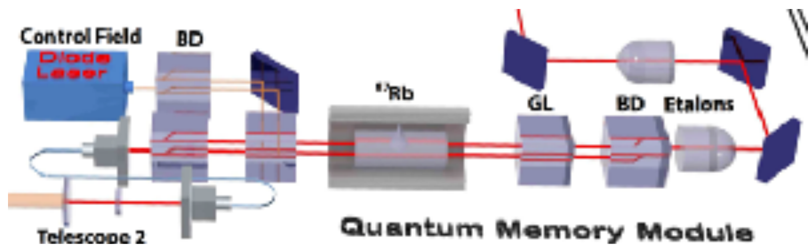
Prof. Eden Figueroa Group @ Stony Brook University

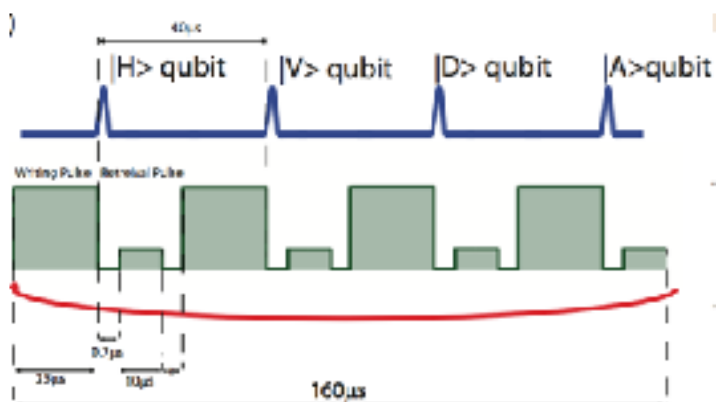
^{87}Rb vapor at room temperature – 795 nm

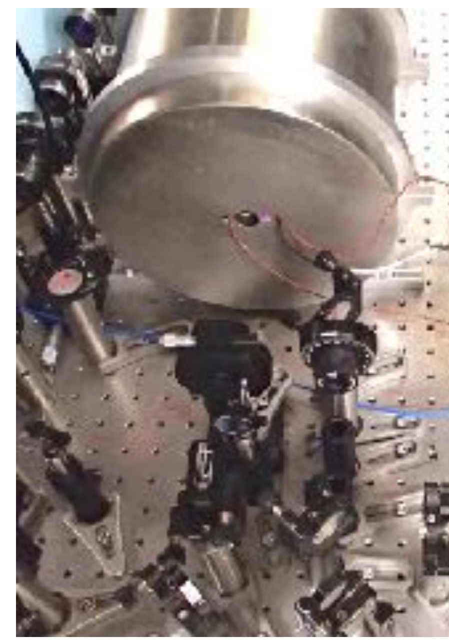
Based on electromagnetically induced transparency (EIT)

Control and writing beams separated by 6.835 GHz





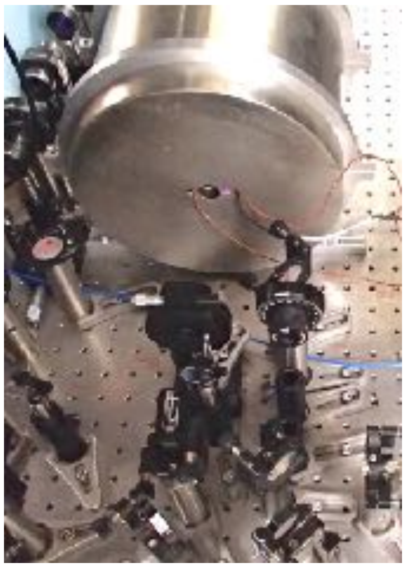


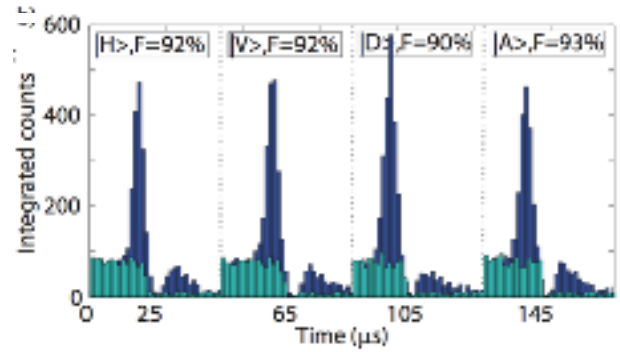


Rb memory for a free-space generic qbit

Use of the memory with an input with μ=1.6 photon
Trasmissivity for probe beam 4.5%
Rejection of control beam 130 dB

QBER analysis: <1% for μ~100 ph
<13% for μ~ 1.6 ph
→need to upgrade the noise rejection
→very good performance in the state storage & reading





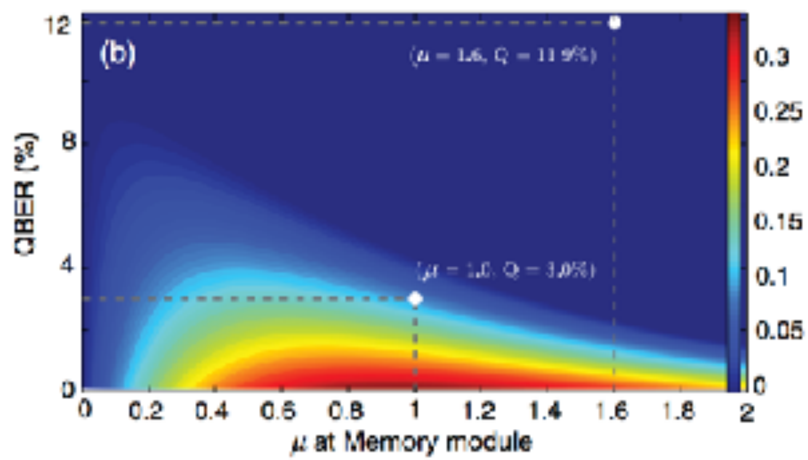
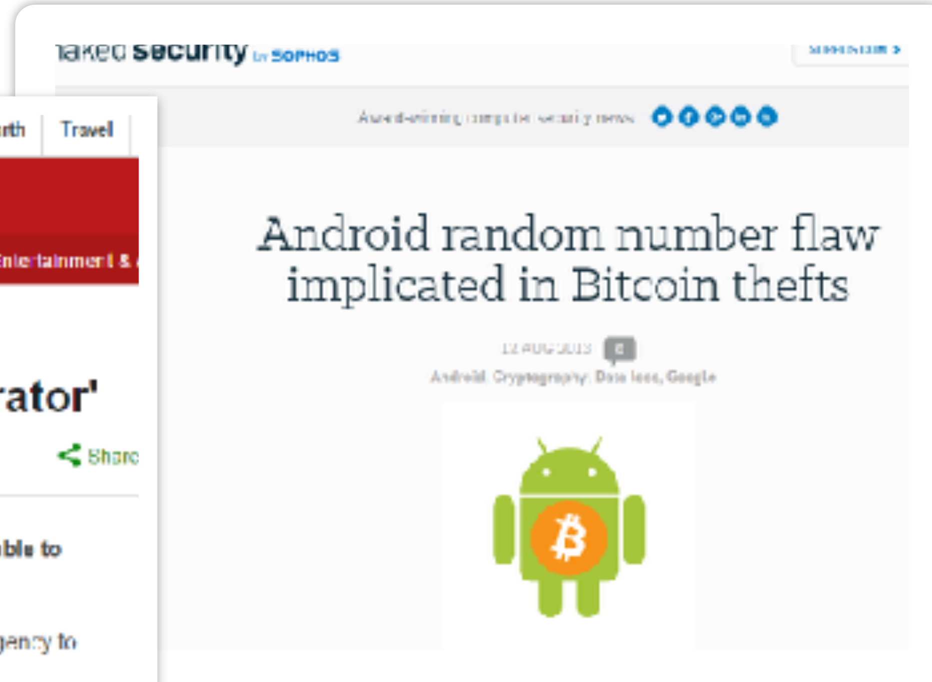


FIG. 5. Ultralow-noise quantum-memory operation. (a) Noise reduction by introducing an auxiliary field; the interaction between dark-state polaritons creates a background-free region.

M. Namazi et al, arXiv:1609.08676, Phis. Rev. Applied 8, 064013 (2017)

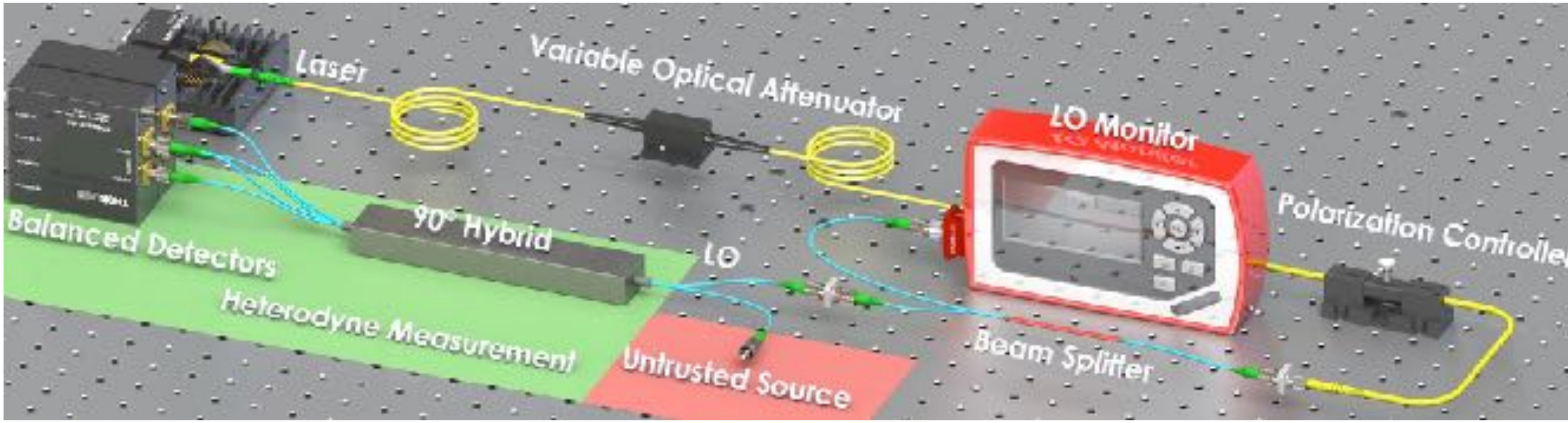
Randomness is an invaluable resource for cryptography….



but it can completely compromise security.

QRNG Slides prepared by Marco Avesani @ UniPD

Semi-Device-Independent QRNG @ UniPD
Speed and security combined



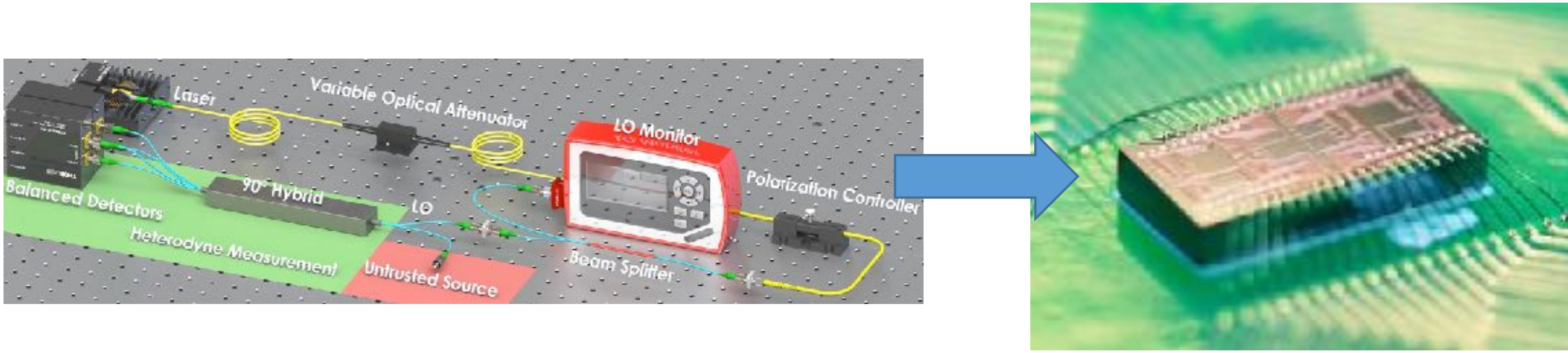
Hybrid approach, we **trust only one part of the device**, the measurement. However it is **monitored in real-time** to check for anomalies.

The **source is untrusted** and can be even **controlled by the attacker**.

Can offer security and speed at the same time:

It is able to generate more than **17 Gbps** of **secure and private** random numbers

Our approach: future perspective



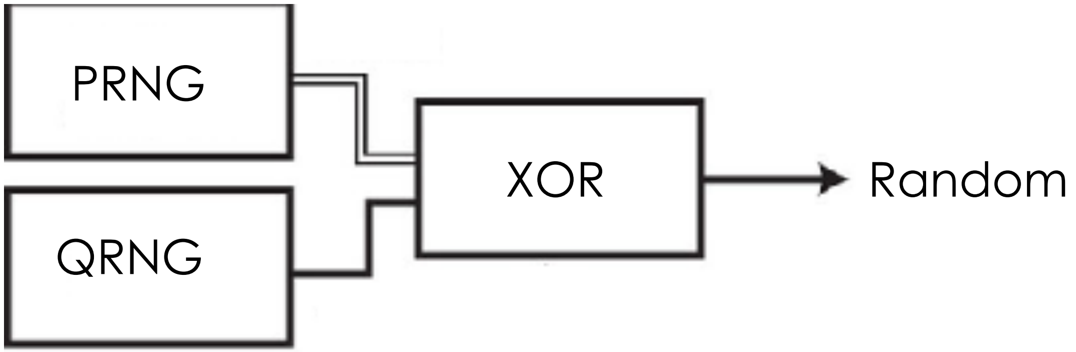
Our setup has been designed to be **scalable**, and modern **integrated optics** technologies offer a way for an **all-chip** solution.

That would make it suitable for an entire new class of **portable devices**

QRNG as a new resource for the current crypto infrastructure

Quantum technologies are completely **compatible** with the current infrastructure that **do not** necessary **compete** with today's solution

They can be thought as a new and powerful resource, that can be **added on top** of current implementations, adding another layer of security.



In the specific example of random numbers, a QRNG can be directly inserted in a standard system that uses a PRNG.

Xoring the two will never decrease the randomness

HOME NEWS AND EVENTS PEOPLE RESEARCH QLUNCH PUBLICATIONS JOIN US QT@UNIPD

Quantum future

The shift in the communication paradigm

Università degli Studi di Padova

Secure heterodyne-based quantum random number generator at 17 Gbps

M. Avesani[1], D. G. Marangon[1] G. Vallone[1], P. Villoresi[1]

Link to the arxiv paper

[1]Department of Information Engineering, University of Padova, via Gradenigo 6/B, 35131 Padova, Italy

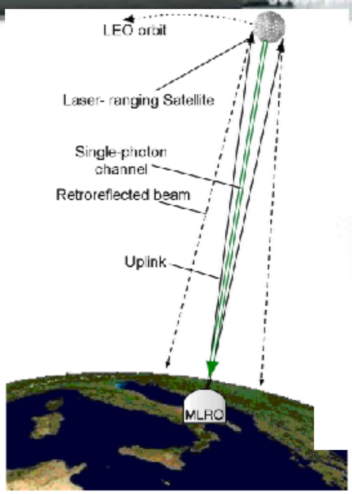
Random numbers are commonly used in many different fields, ranging from simulations in fundamental science to security applications. In some critical cases, as Bell's tests and cryptography, the random numbers are required to be both secure (i.e. known only by the legitimate user) and to be provided at an ultra-fast rate (i.e. larger than Gbit/s). However, practical generators are usually considered trusted, but their security can be compromised in case of imperfections or malicious external actions. In this work we introduce an efficient protocol which guarantees security and speed in the generation. We propose a novel source-device-independent protocol based on generic Positive Operator Valued Measurements and then we specialize the result to heterodyne measurements. The security of the generated numbers is proven without any assumption on the source, which can be even fully controlled by an adversary. Furthermore, we experimentally implemented the protocol by exploiting heterodyne measurements, reaching an unprecedented secure generation rate of 17.42 Gbit/s, without the need to take into account finite-size effects. Our device combines simplicity, ultrafast-rates and high security with low cost components, paving the way to new practical solutions for random number generation.

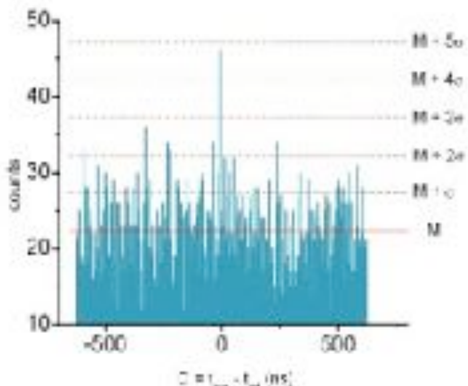
A sample (1GB) of the generated random number can be found at this link: https://goo.gl/duLvcZ

Italian Space Quantum Communications

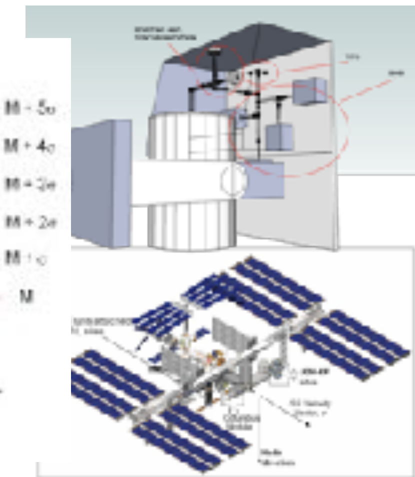
Collaboration of QuantumFuture Research Group of University of Padova with ASI Matera Laser Ranging Observatory, since **2003.**

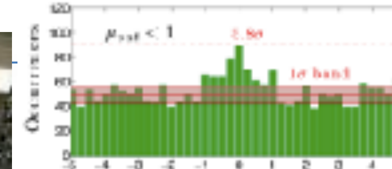
1.5 m telescope with millimeter resolution in Satellite Laser Ranging.

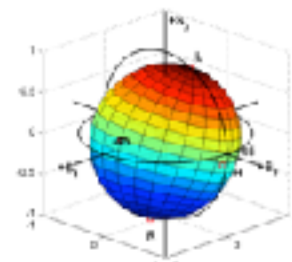




P. Villoresi et al.
New J. Phys.
10 033038 (2008)







G. Vallone et al. Phys. Rev. Lett. vol 115 040502 (2015)

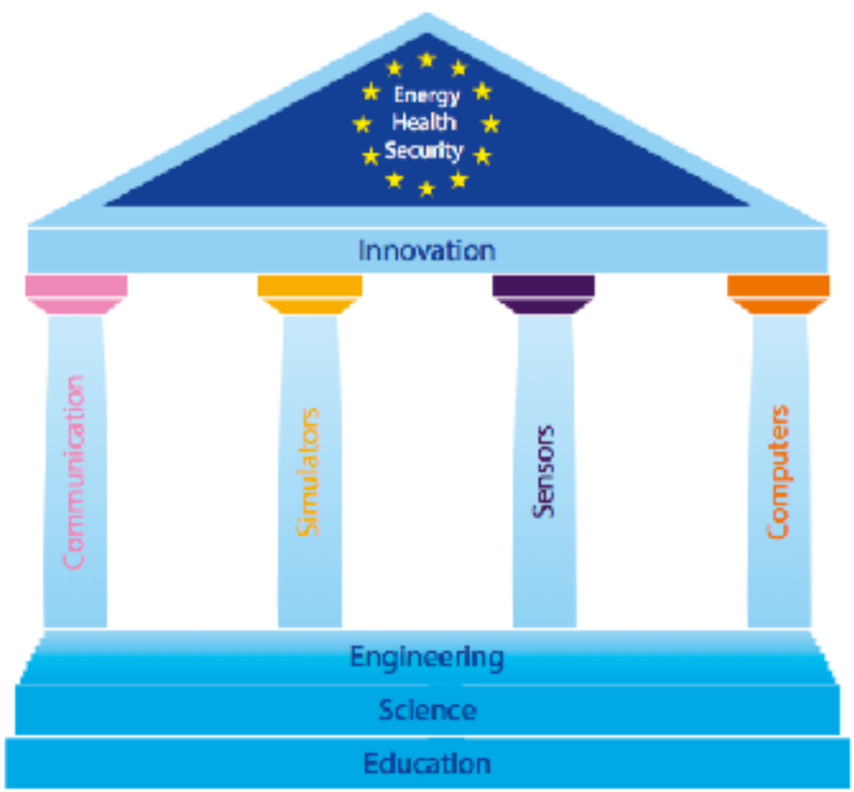
- 2003 – UniPD SpaceQ project
- Optical front-end for single photon transceiver @ MLRO
- 2008 – first single-photon return from Ajisai announced
- 2009 ASI Feasibility study for a quantum payload for the ISS
- 2009-2011 Characterization of MLRO Mueller Matrix
- 2012 - Analysis of response for different satellites CCR
- 2013 – state preparation, state analysis – satellite synchronization
- 2014 – Q-Comm on satellites downlink demonstrated
- 2015 Temporal modes demonstrated in satellite qubit
- 2016 – New limit in single photon exchange from MEO sat
- 2017-Testing wave-particle duality along Space links

D. Dequal et al.
Phys Rev. A Rapid Comm
93 010301 (2016)

Quantum Manifesto

A New Era of Technology May 2016

On this Manifesto, the European Commission **announced the launch a €1 billion flagship-scale initiative in Quantum Technology QUTE-F, starting in early 2018.**
It is endorsed by a broad community of industries, research institutes and scientists in Europe.



Elements of a European programme in quantum technologies.

Quantum Technology Flagship is a Mission, as fostered in the Lamy Report

> *Missions, or "moon shots", should have a breakthrough or transformative potential for science, technology, industry or society.*
> **Lamy Report 2017**

Quantum Technologies in Italy

Conclusions.. so far

QKD is now a commodity, on ground

The frontier of Space Quantum Communications has been opened.

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**

Very successful demonstrations have paved the way to applications on the global scale

Italian backbone and Space network is forming..

there is a lot to be done

get involved!!