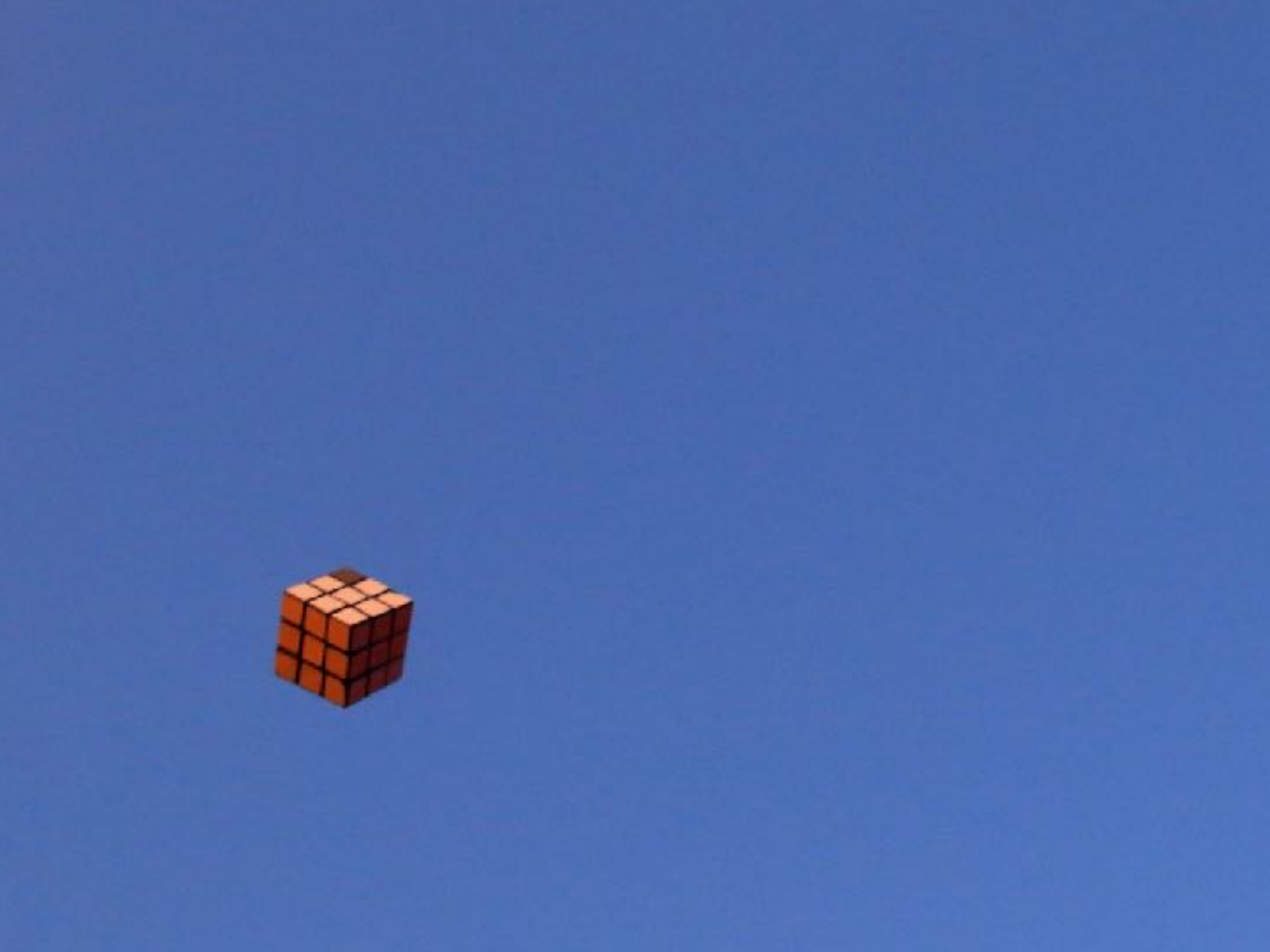
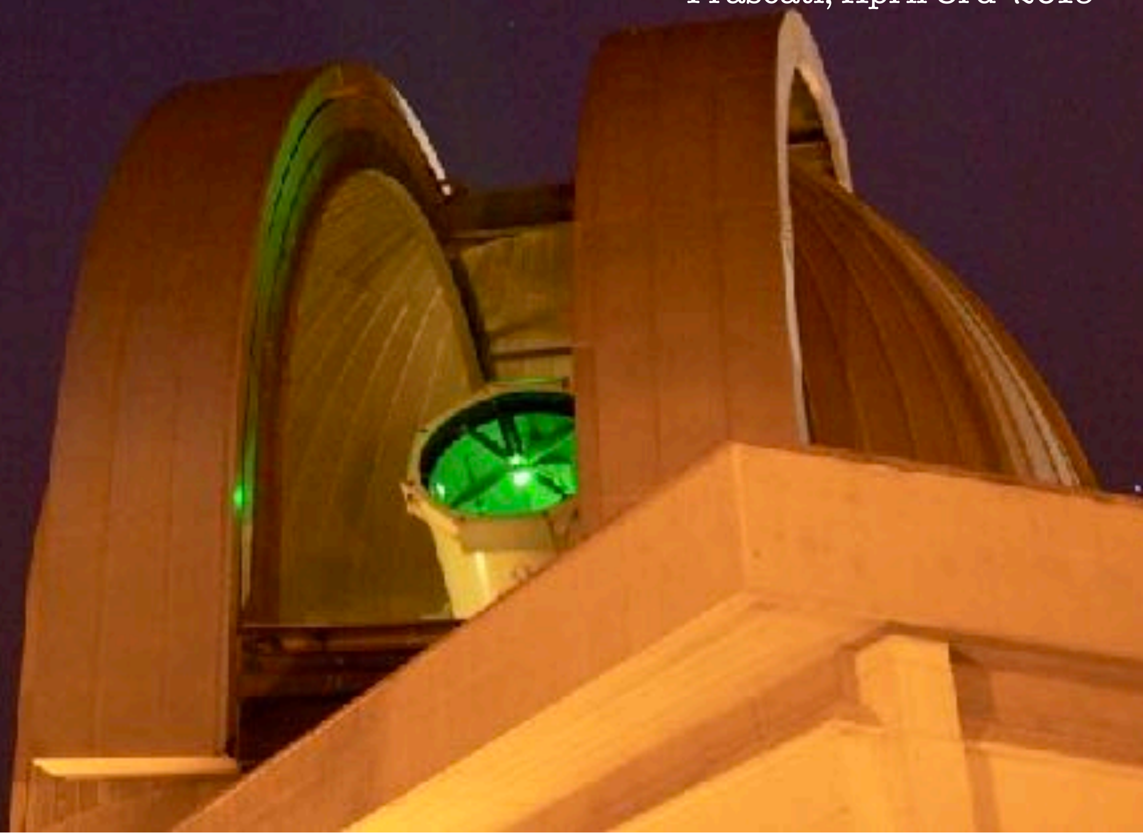


MEET THE QUBIT… AND SEND IT AROUND!

PAOLO VILLORESI
Università di Padova
Dipartimento di Ingegneria dell'Informazione
CNR – Istituto di Fotonica e Nanotecnologie -
- Istututo Nazionale Fisica Nucleare

INSPYRE – INternational School on modern PhYsics and Research,
Challenges in Modern Physics and Quantum Technologies
Frascati, April 3rd 2019

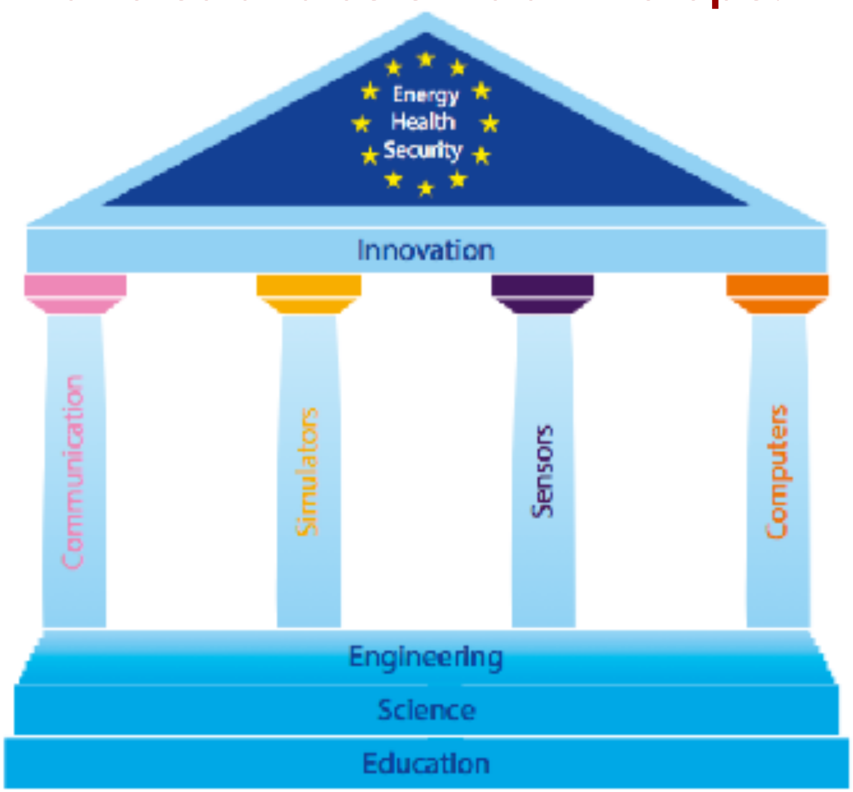



Quantum Manifesto
A New Era of Technology
May 2016
http://qurope.eu/manifesto

Quantum Manifesto

A New Era of Technology May 2016

This Manifesto calls upon Member States and the European Commission **to launch a €1 billion flagship-scale initiative in Quantum Technology, started in 2018** within the European H2020 research and innovation framework programme. **It is endorsed by a broad community of industries, research institutes and scientists in Europe.**



Elements of a European programme in quantum technologies.

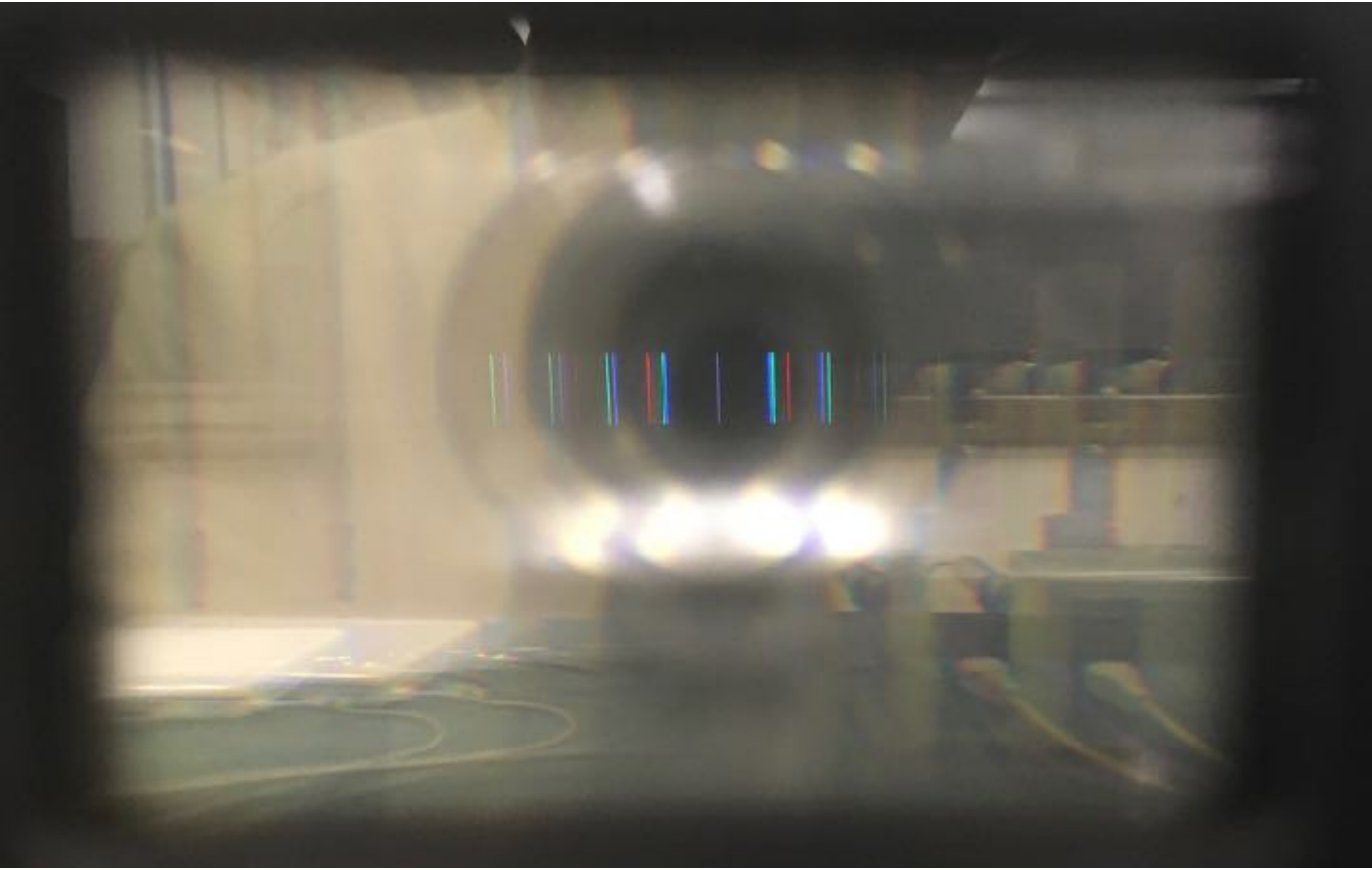
Opening at Vienna on 29OCT18 of the Quantum Technology Flagship 2018-2028

Quantum Manifesto

A New Era of Technology

May 2016

Quantum Technologies Timeline



N. Bohr, Philos. Mag. **26**, 1

1913

On the Constitution of Atoms and Molecules

N. Bohr,
Dr. phil. Copenhagen
(Received July 1913)

Introduction

- **Atoms are not objects that can be described by the laws of Maxwell alone:**
- **energy levels cannot have any value**
- **Electrons are in states with fixed energy**
- **the transition between states occurs with specific energy quanta for each atom**

In order to explain the
matter Prof. Rutherfo
According to this theo
surrounded by a system
the nucleus; the total ne
charge of the nucleus. Further, the nucleus is assumed to be the seat of

Ann. Physik **17**, 132 (1905)

In fact, it seems to me that the observations on "black-body radiation", photoluminescence, the production of cathode rays by ultraviolet light and other phenomena involving the emission or conversion of light can be better understood on the assumption that the energy of light is distributed discontinuously in space. According to the assumption considered here, when a light ray starting from a point is propagated, the energy is not continuously distributed over an ever increasing volume, but it consists of a finite number of energy quanta, localised in space, which move without being divided and which can be absorbed or emitted only as a whole.

6. ***Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt;***
von A. Einstein.

Emission and Transformation of Light from an Empirical point of view

Light: wave AND particles

The photon has characteristics of:

a wave: in the way it diffracts and forms interference

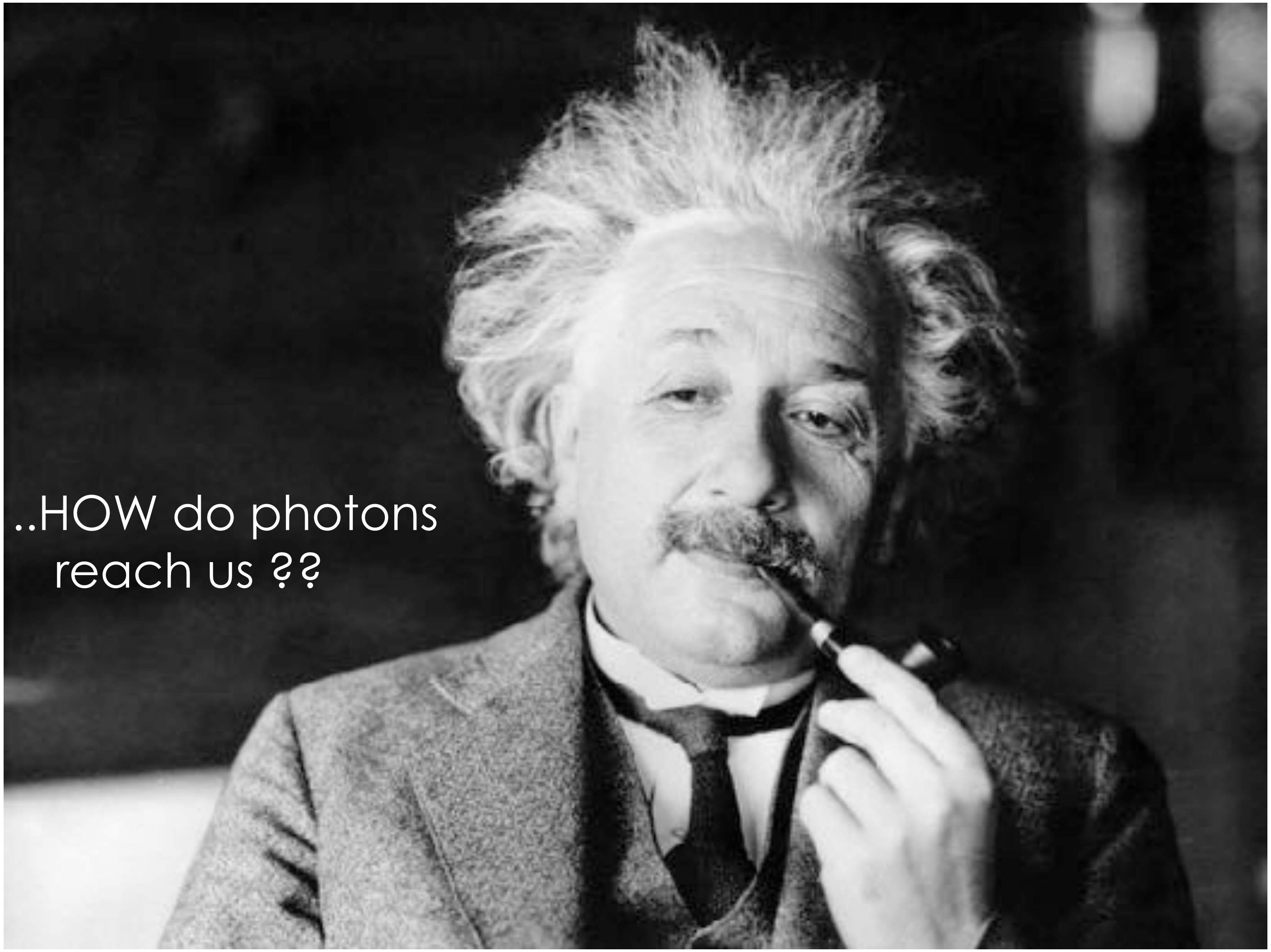
a particle: it is indivisible, it is generated and absorbed in its entirety

they.. *solved the problem of black-body radiation, Planck 1900,*

and that of the photoelectric effect, Einstein 1905

Photons are quantum states of radiation

If light is grainy..



How cay I sort among **different types of grains**? (*any type??*)

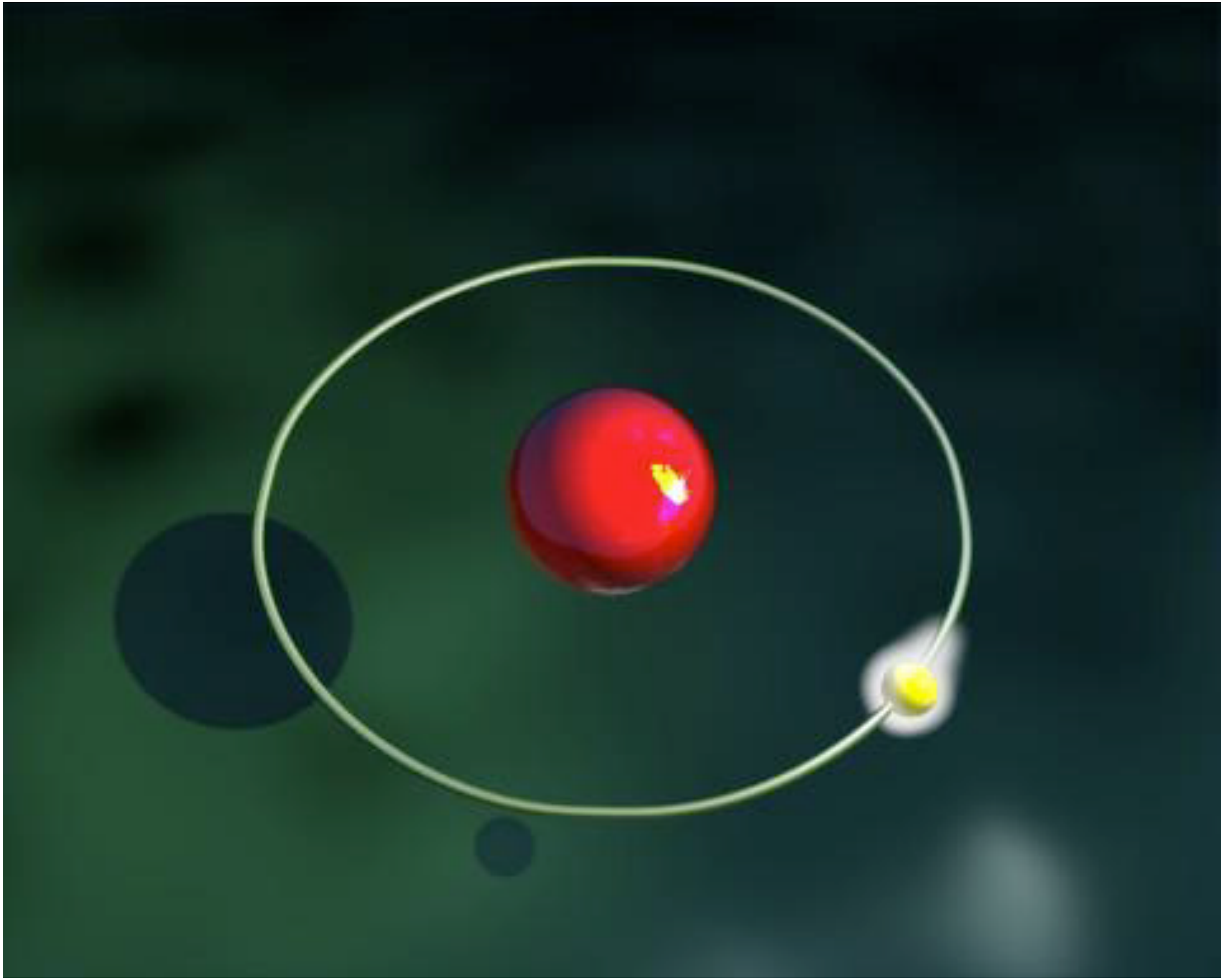
..well, I know that I may try to listens at their sound!

Let's try..

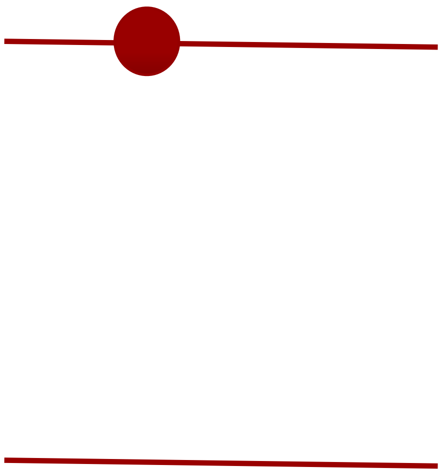


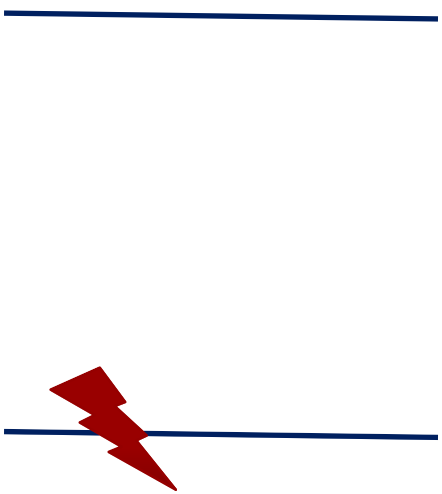

1 2 3 4

Likewise, as the light is grainy..
..we can feel it!



Let’s visualize the two processes separately:

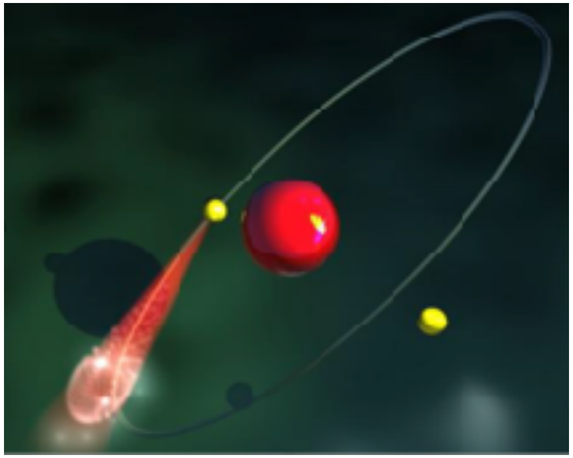


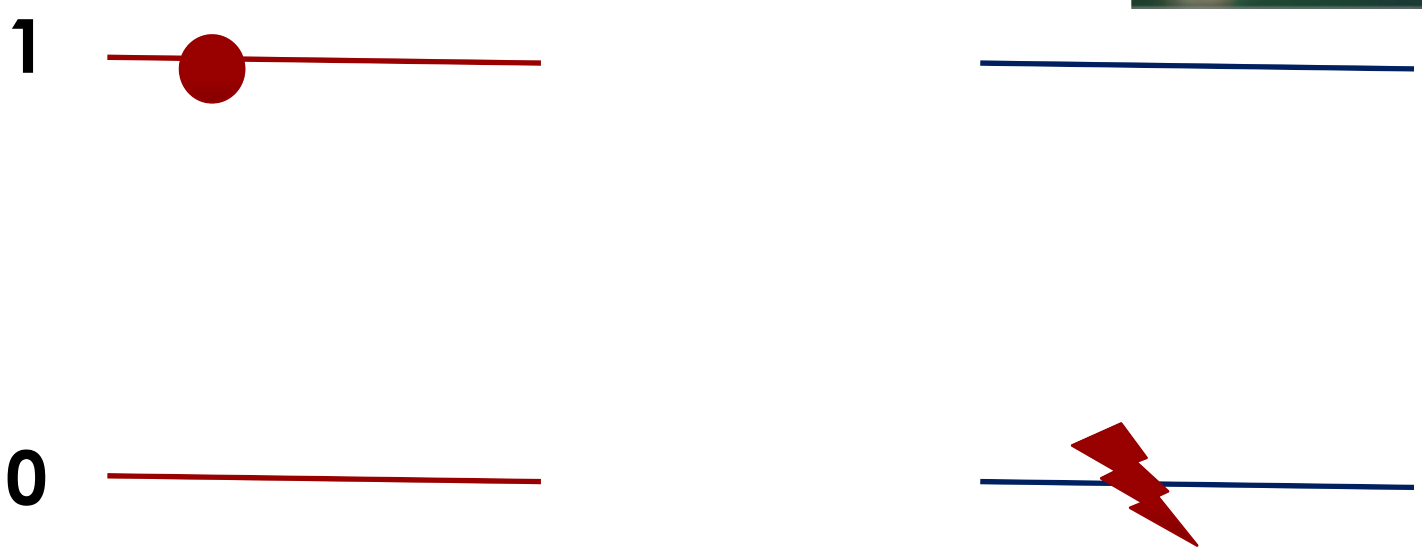


in the Atom, the electron does a transition

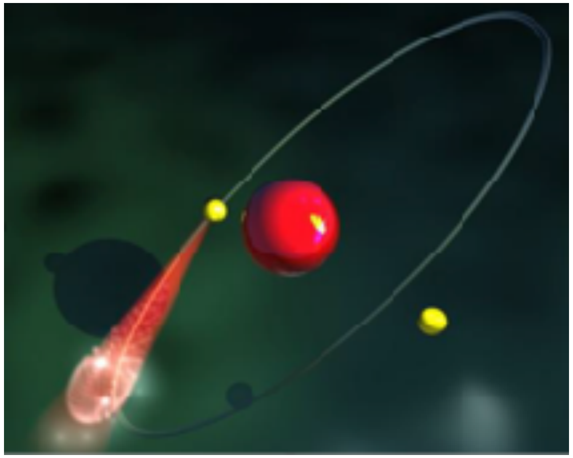
the photon is generated by this transition

during the process of emission, the atom is in a superposition of the upper and lower state

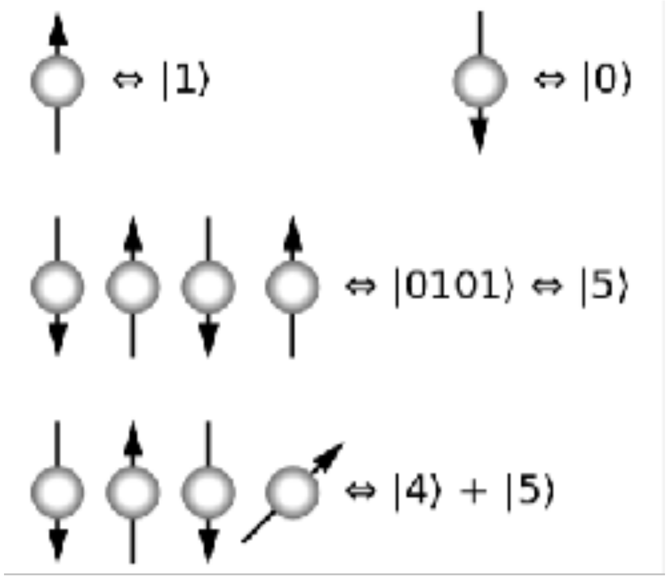




A two-level quantum system is a **qubit**

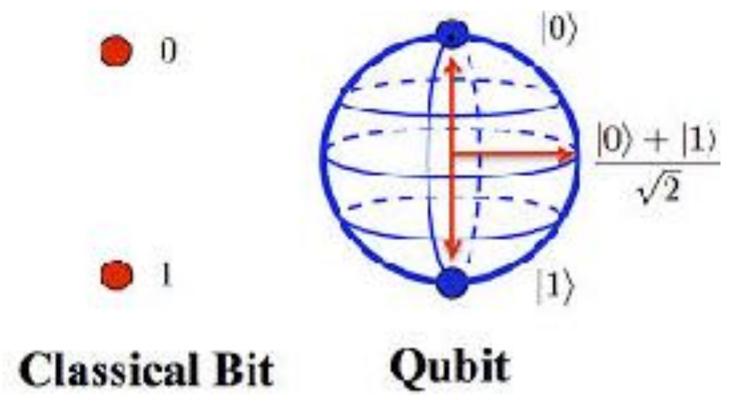


Other particle characteristics
of the microcosmos they can stay in superposition,
providing different qubit realizations



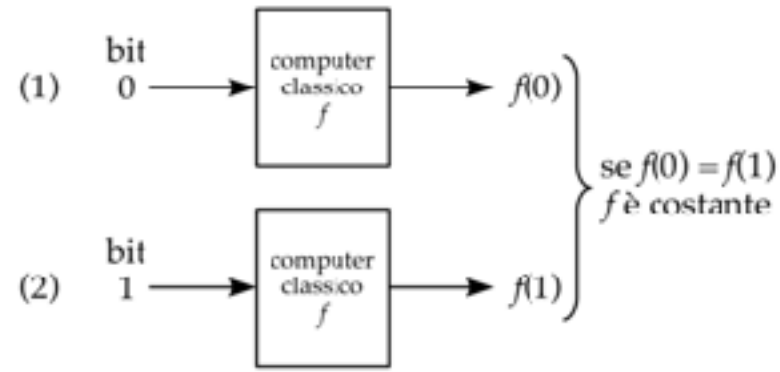
What's good about quantum states?

- Unlike the classic bit, which is 1 or 0, a quantum particle can form a state with the superposition of base vectors: simultaneously high and low.
- **The concept of information is enriched: welcome qubit!**

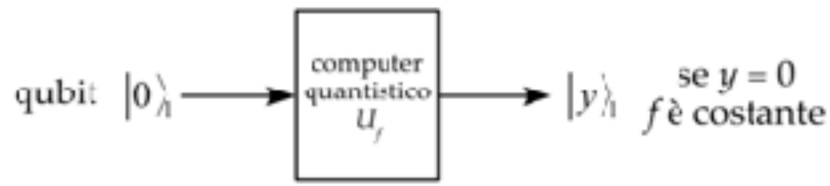


You can use the qubits.. to compute!

David Deutsch



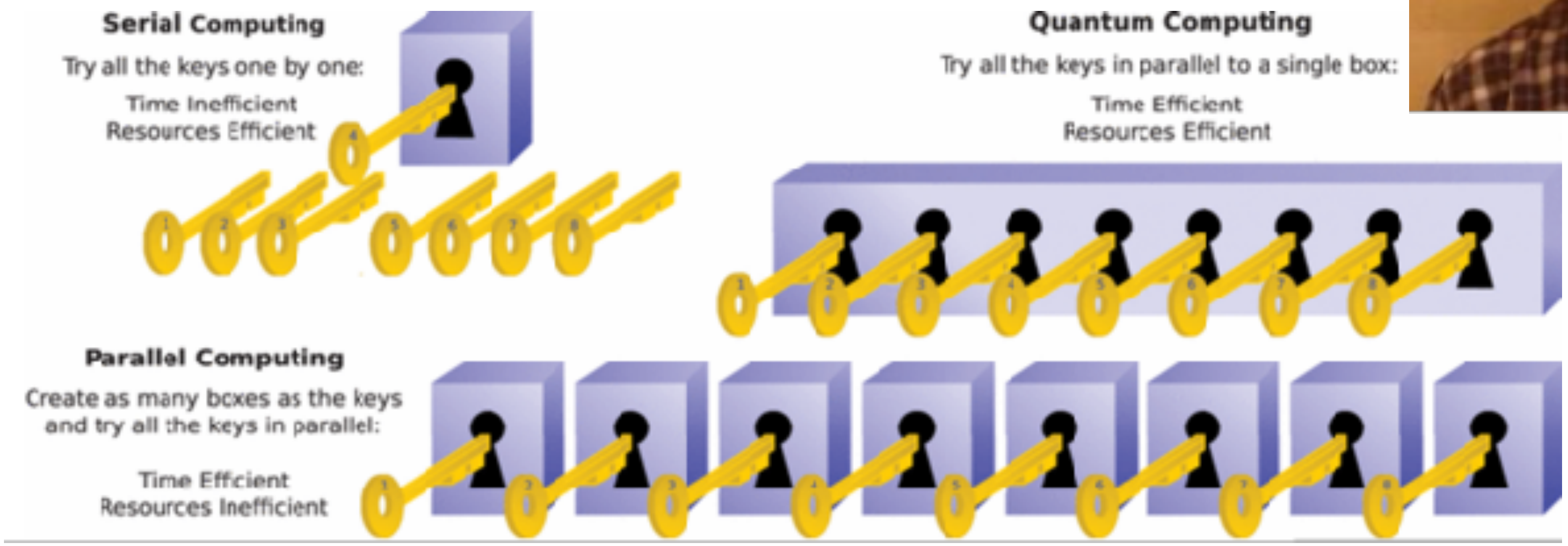
	f_{01}	f_{10}	f_{00}	f_{11}
0	**0**	**1**	**0**	**1**
1	**1**	**0**	**0**	**1**

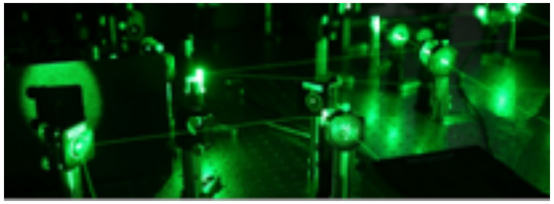


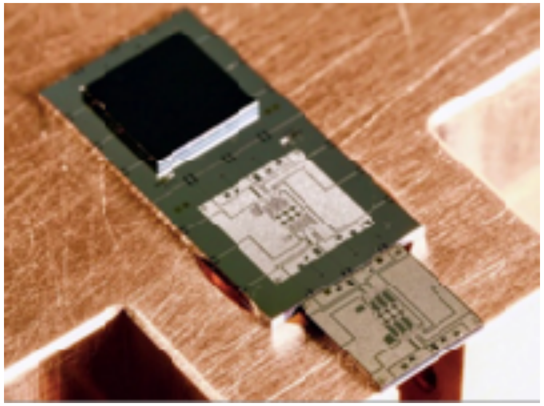
the Deutsch-Josza algorithm proved in 1992 the first example of **quantum parallelism**

Quantum Computers

Seth Lloyd





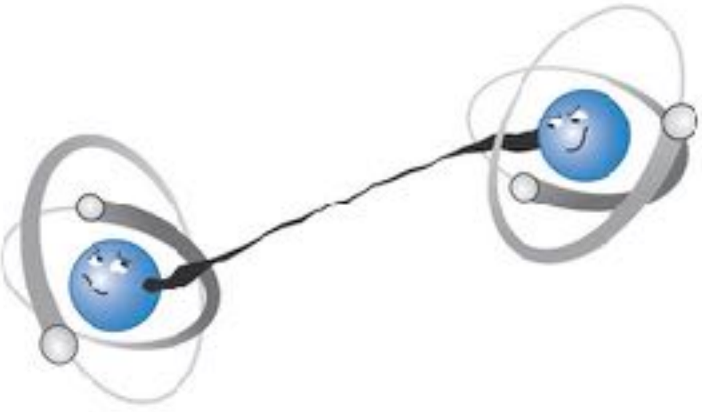


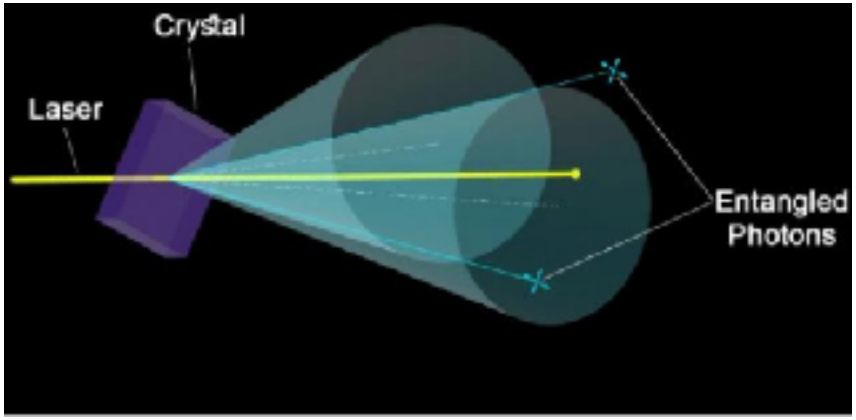
What's good about quantum states?

Entanglement: sharing the quantum state has effect even at a distance - and instantly!

Maximum knowledge on the global properties of a system does not necessarily imply the total knowledge of all its parts

Erwin Schrödinger

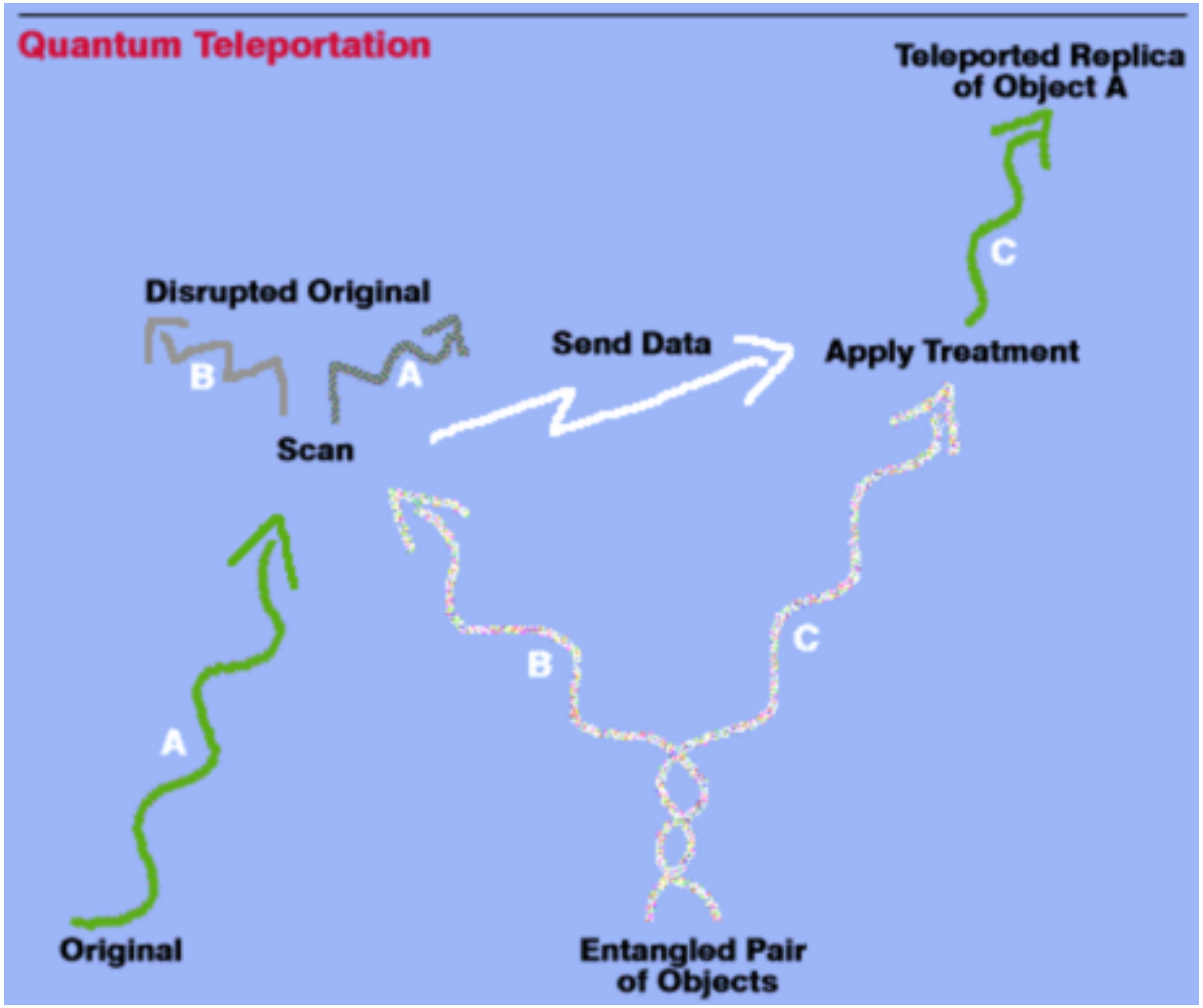




http://www.improbable.com/airchives/paperair/volume7/v7i6/doubleslit.html

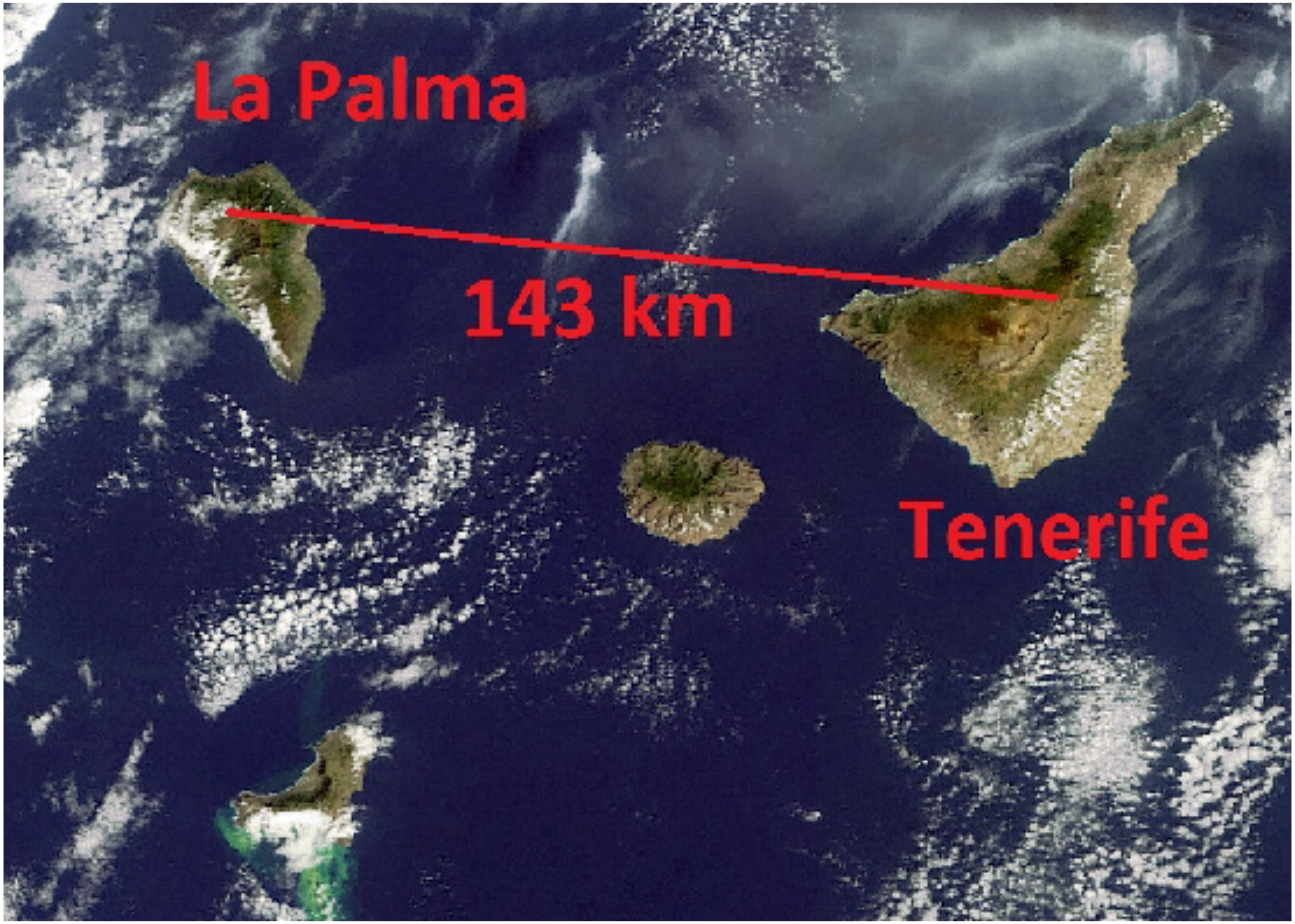
Quantum teleportation

(top, left) Richard Jozsa, William K. Wootters, Charles H. Bennett. (bottom, left) Gilles Brassard, Claude Crépeau, Asher Peres. Photo: André Berthiaume.



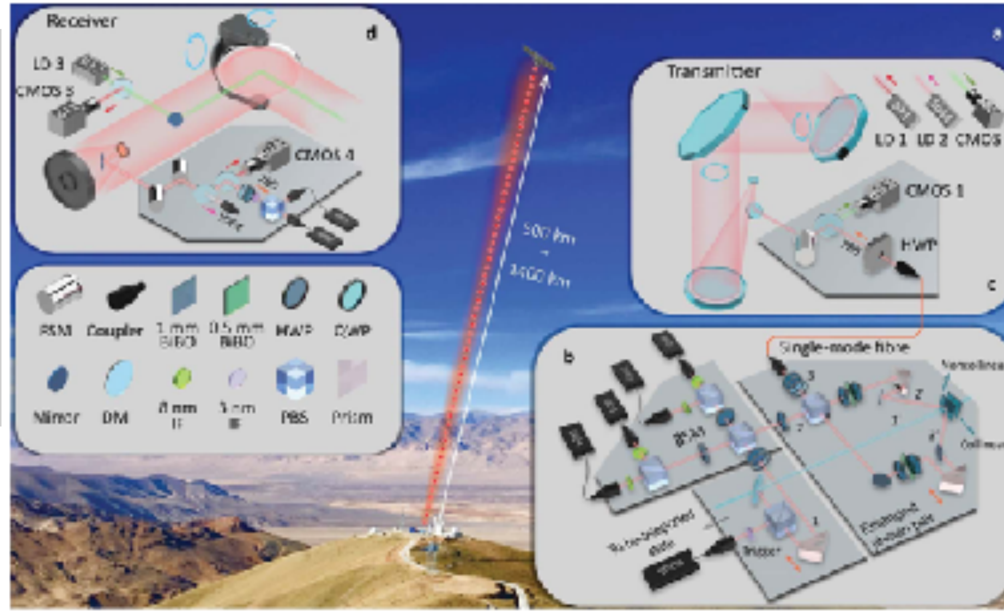

(C) C.H.Bennett

Quantum teleportation on the ground

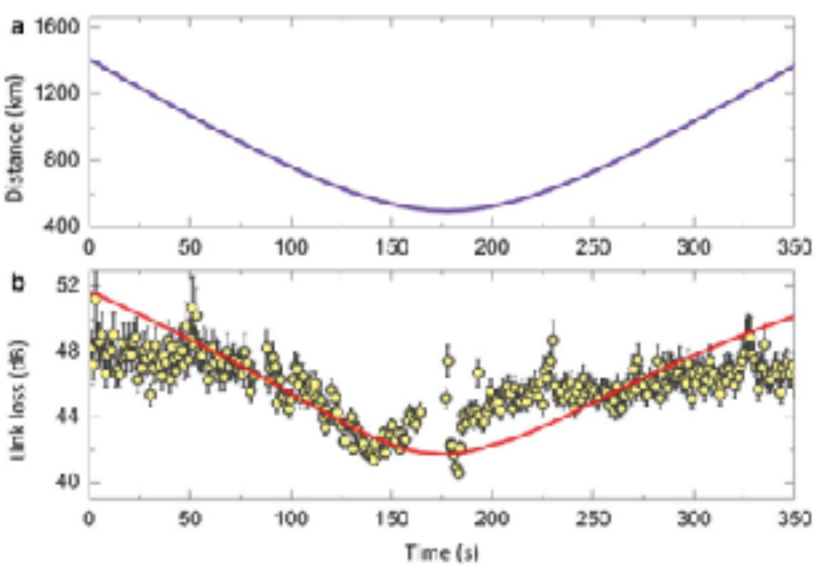


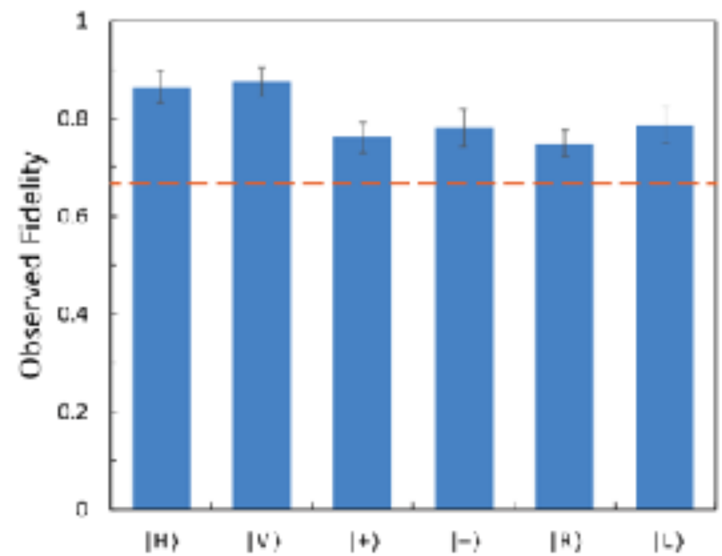
Ground-to-satellite quantum teleportation

Ji-Gang Ren[1,2], Ping Xu[1,2], Hai-Lin Yong[1,2], Liang Zhang[2,3], Sheng-Kai Liao[1,2], Juan Yin[1,2], Wei-Yue Liu[1,2], Wen-Qi Cai[1,2], Meng Yang[1,2], Li Li[1,2], Kui-Xing Yang[1,2], Xuan Han[1,2], Yong-Qiang Yao[4], Ji Li[5], Hai-Yan Wu[5], Song Wan[6], Lei Liu[6], Ding-Quan Liu[3], Yao-Wu Kuang[3], Zhi-Ping He[3], Peng Shang[1,2], Cheng Guo[1,2], Ru-Hua Zheng[7], Kai Tian[8], Zhen-Cai Zhu[6], Nai-Le Liu[1,2], Chao-Yang Lu[1,2], Rong Shu[2,3], Yu-Ao Chen[1,2], Cheng-Zhi Peng[1,2], Jian-Yu Wang[2,3], Jian-Wei Pan[1,2].

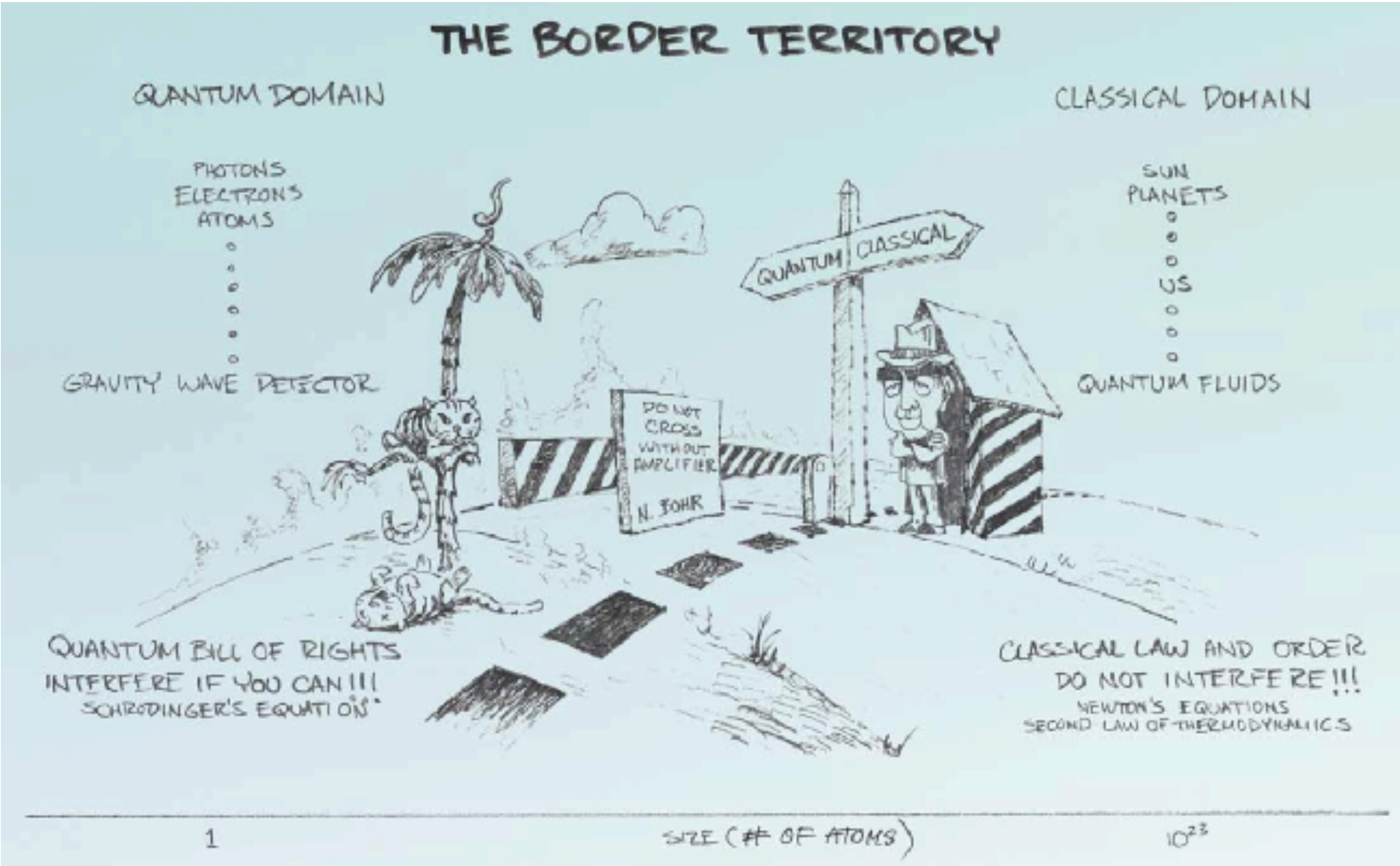


arxiv:1707.00934
appeared **5 July 2017**





Classical-Quantum border



Wojciech H. Zurek, Decoherence and the Transition from Quantum to Classical *Physics Today (1991)*

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

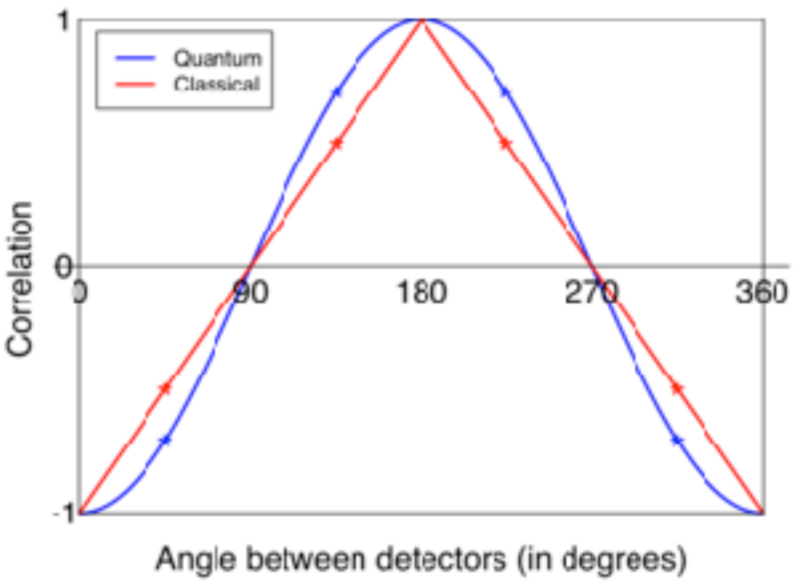
In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

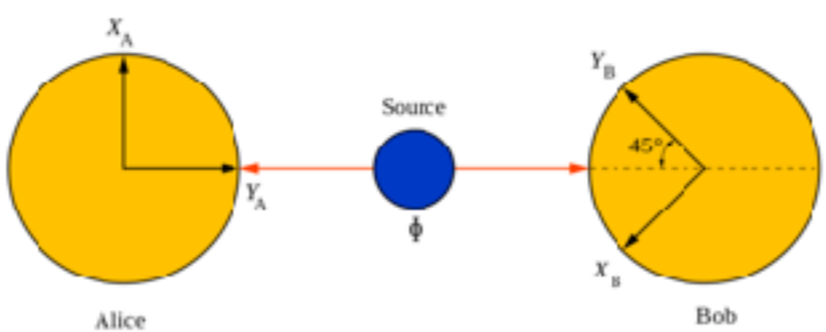
Locality

Realism

Bell's Theorem 1964
55° anniversary

No physical theory based on location and hidden variables can reproduce all the predictions of Quantum Mechanics John S. Bell





VOLUME 47, NUMBER 7 PHYSICAL REVIEW LETTERS 17 AUGUST 1981

Experimental Tests of Realistic Local Theories via Bell's Theorem

Alain Aspect, Philippe Grangier, and Gérard Roger
Institut d'Optique Théorique et Appliquée, Université Paris-Sud, F-91406 Orsay, France
(Received 30 March 1981)

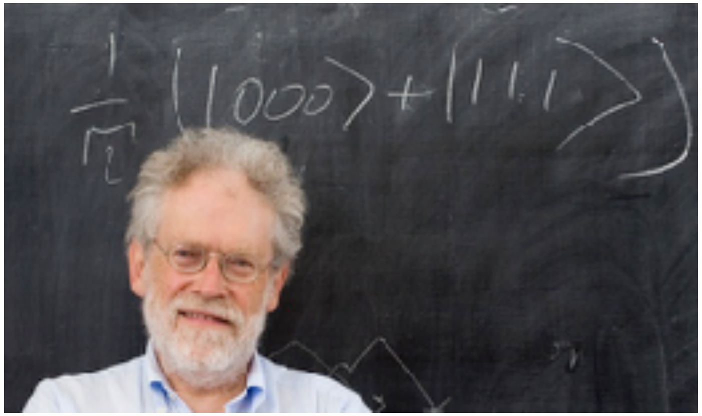
We have measured the linear polarization correlation of the photons emitted in a radiative atomic cascade of calcium. A high-efficiency source provided an improved statistical accuracy and an ability to perform new tests. Our results, in excellent agreement with the quantum mechanical predictions, strongly violate the generalized Bell's inequalities, and rule out the whole class of realistic local theories. No significant change in results was observed with source-polarizer separations of up to 6.5 m.

Alain Aspect

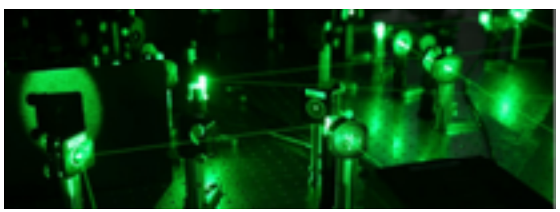
As a conclusion, **our results, in excellent agreement with quantum mechanics predictions**, are to a high statistical accuracy a **strong evidence against the whole class of realistic local theories**; furthermore, *no effect of the distance between measurements on the correlations was observed.*

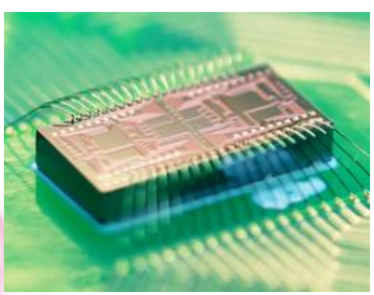
Quantum Information is born!

- Quantum Computation
- Quantum Dense Coding
- Quantum Cryptography
- Quantum Teleportation
- Quantum Metrology
- Quantum Random-Number Generation
- World Wide Quantum Communications



and so.. 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..**

First application: on Randomness
This is an invaluable resource for cryptography….


BBC | Sign in | News | Sport | Weather | Shop | Earth | Travel

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment &

Technology

NSA 'altered random-number generator'

11 September 2013 Technology Share

US intelligence agency the NSA subverted a standards process to be able to break encryption more easily, according to leaked documents.

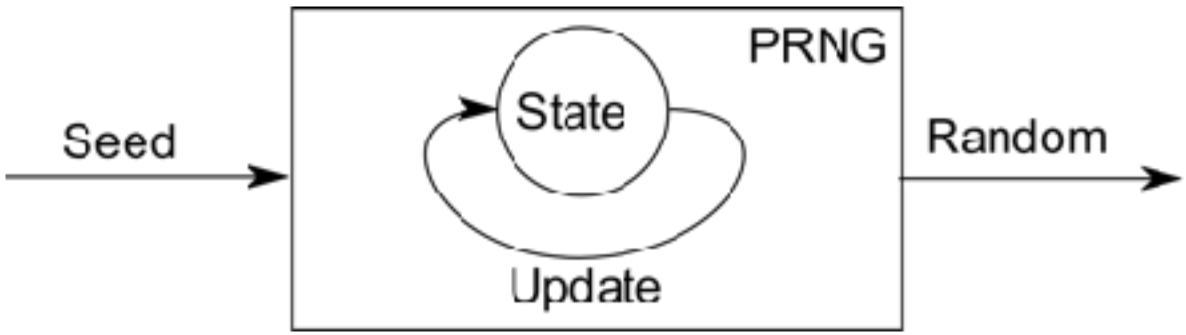
It had written a flaw into a random-number generator that would allow the agency to predict the outcome of the algorithm, the New York Times reported.

but it can completely compromise security.

QRNG Slides prepared by Marco Avesani @ UniPD

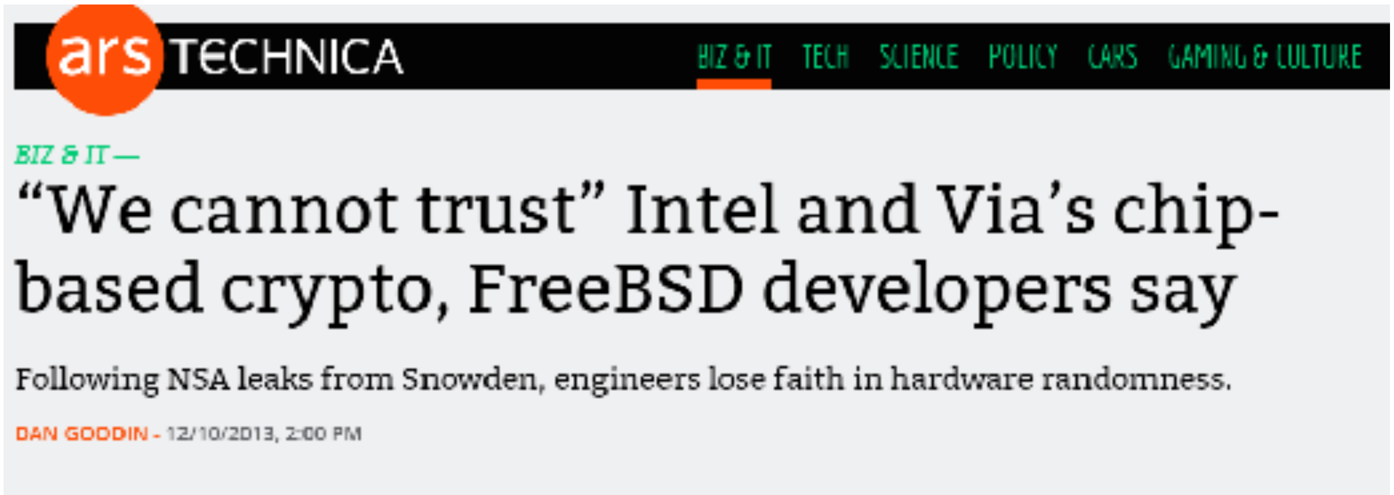
Most widely used source of random numbers are cryptographically secure pseudo random number generator (CSPRNG)

They are based on an algorithm that deterministically produces numbers that seems random.



Why quantum? We still have (Classical) Hardware RNG

Vulnerability in HRNG:


ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

BIZ & IT —

“We cannot trust” Intel and Via’s chip-based crypto, FreeBSD developers say

Following NSA leaks from Snowden, engineers lose faith in hardware randomness.

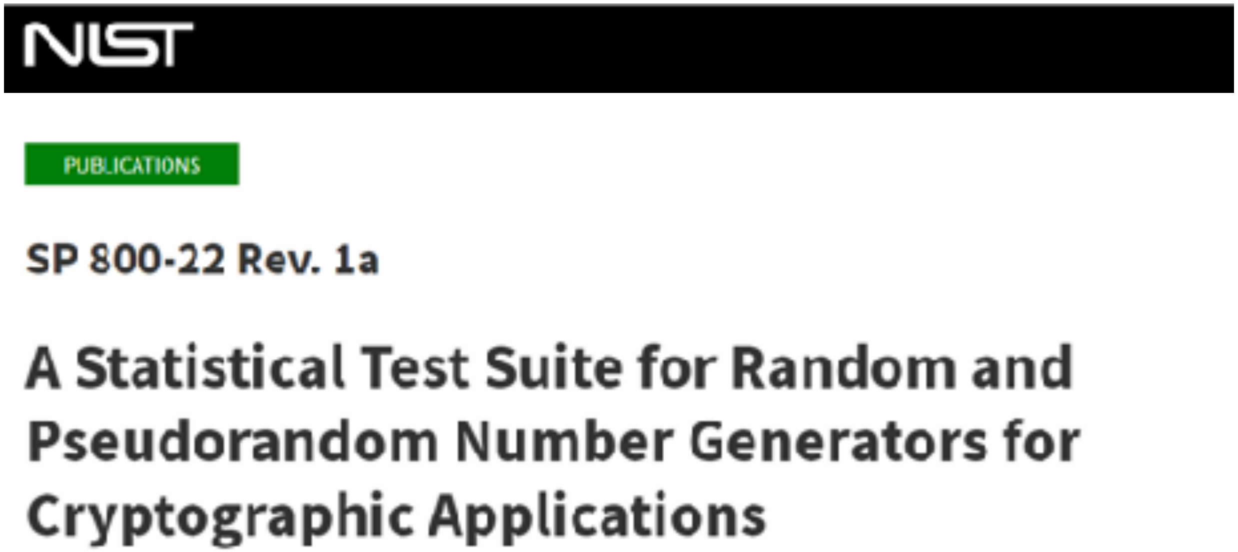
DAN GOODIN - 12/10/2013, 2:00 PM

Full trust on the device and manufacturer

We are still relying in processes that only appear random! We just don’t know

Laws of **CLASSICAL** physics are completely deterministic.

All the vulnerable RNG pass the standard suites of statistical tests


NIST

PUBLICATIONS

SP 800-22 Rev. 1a

A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications

If the generators systematically fail the test we can say that patterns are present in the data

But if the tests are passed, it only means that **THOSE SPECIFIC** patterns are not present

Why are Quantum RNG different?

Quantum mechanics is the only domain in physics where random phenomena can happen.

For example, radioactive decays are random process!

Quantum Mechanics can predict **exactly** the **average time** that takes for an atom to decay but at the same time states that is impossible to know **when** it will decay: that is **random!**

$$^{137}\mathrm{Cs} \xrightarrow{30.17\mathrm{y}} {}^{137m}\mathrm{Ba} + \beta^- + \overline{\nu}_e \xrightarrow{156\mathrm{s}} {}^{137}\mathrm{Ba} + \gamma$$

They have been used as generators, but they are quite unpractical…

But Quantum Mechanics can also tell you how much randomness you can extract

Not only is possible to have true random processes, but it's possible to say how much randomness we can get **at least** from the process

For example Heisenberg famous uncertainty principle says:

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2}$$

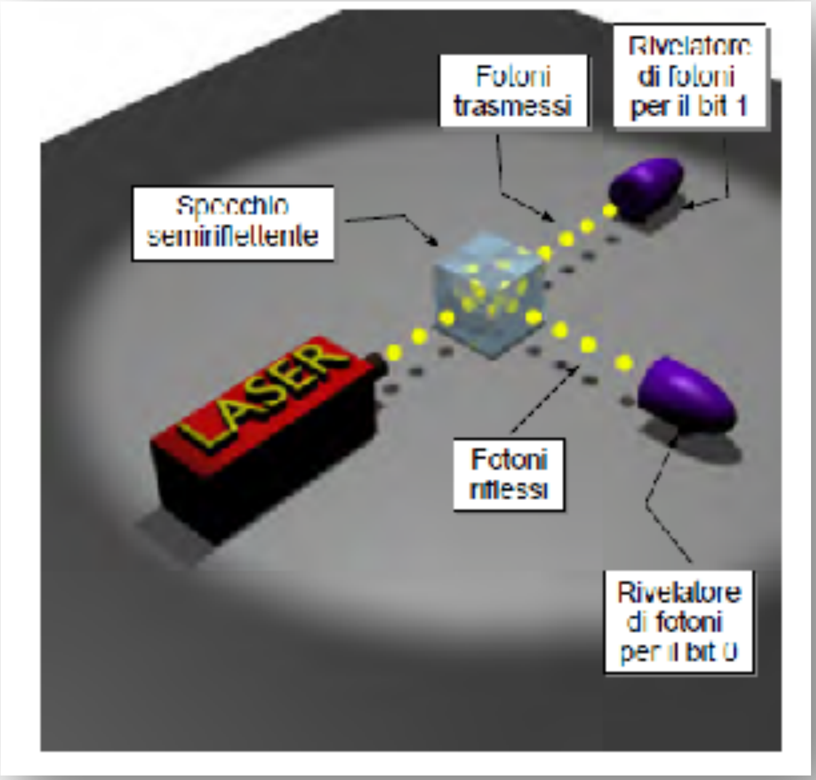
It is impossible to know the position and the momentum of a particle with arbitrary precision

If we know with high precision the position of a particle, we already know the minimal uncertainty, or randomness, of a measure on the momentum.

The laws of Nature guarantee the randomness!
This is impossible with any other type of generator

An example of QRNG

- Indivisible particle of light, photons, are sent over a semi-transparent mirror
- They cannot be divided and they end in a state of superposition with equal probability output from one of the two exits
- No way to predict from which port a particular photon will come out.



Randomness is not due to ignorance of enough variables (like the coin), but on physical laws

Commercial QRNG

- Speed is in the range of **Mbps**… Still slow for practical applications

- You still need to **fully trust** the **manufacturer** and the **devices** What if they don't work as expected?

- They can only certify that the generated number are truly random, they cannot say anything about **privacy.**

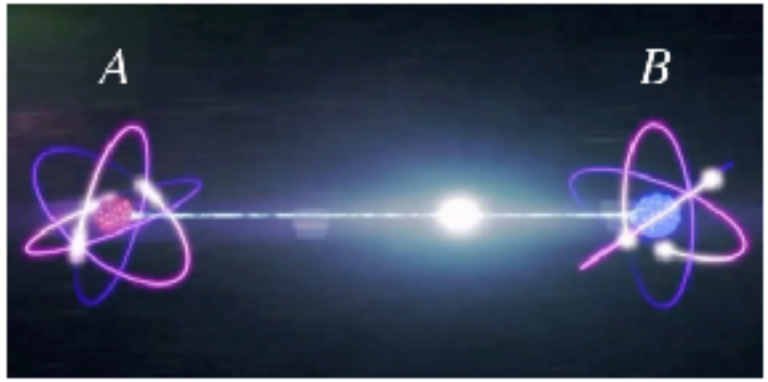
What if an **attacker** has **access** to classical or quantum **side-information** about the internal state of the device?

This would be similar to the case if the attacker has **full, or partial, access** to the **seed** of the PRNG. In this case the security is compromised.

Can Quantum Mechanics guarantee security also in this paranoid scenario?

Device-Independent QRNG

Quantum mechanics describes an effect called **Entanglement**



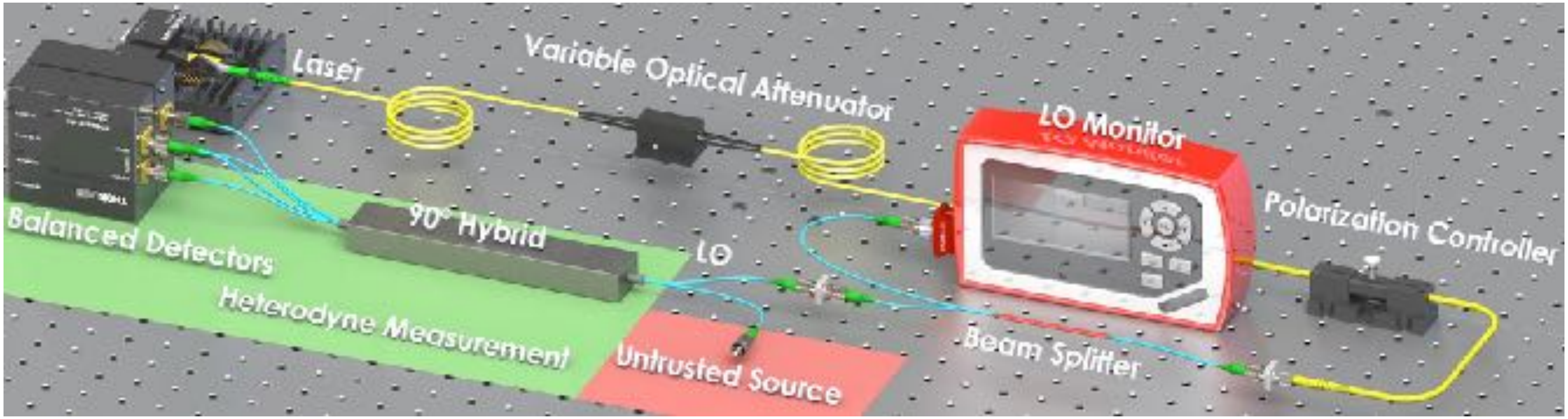
Correlations that cannot be obtained by classical systems!

It can be used to generate random numbers **without any knowledge or trust on the device** used, that are considered black boxes.

However, it is very unpractical:

- Speed: < bps
- Requires initial randomness. Expansion not generation
- Extremely expensive and complex
- Needs km of separation between the two systems
- Not scalable

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

Advances of UniPD scheme with respect to commercial (and non) QRNG

- The **FIRST secure protocol** that **generates** randomness and **does not expand** it. No need of initial randomness

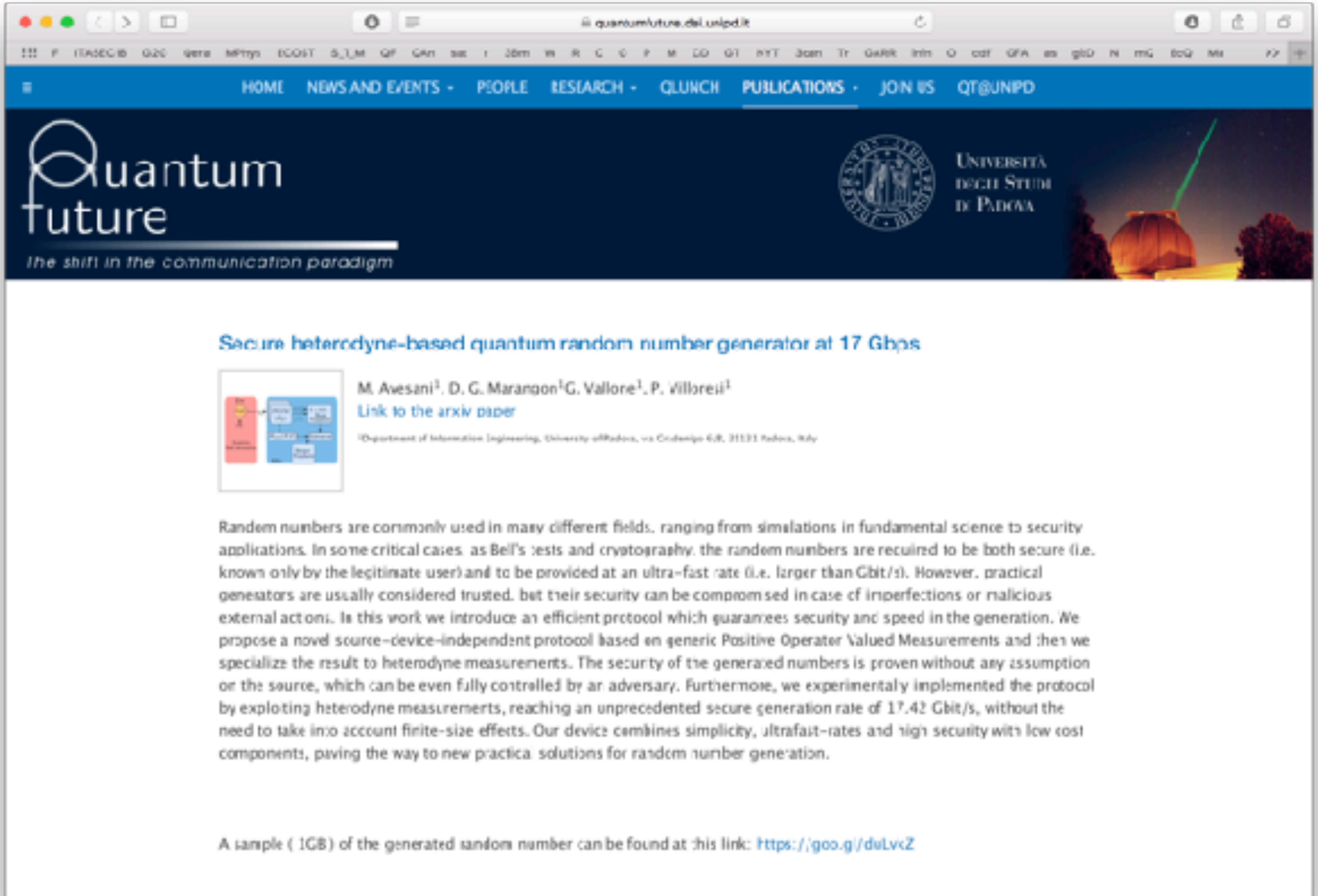
- Our protocol is able to guarantee both **true randomness and privacy** of the generated numbers. The security is evaluated in the most paranoid scenario where the attacker has **classical or quantum side information**

- Trust on the device is highly reduced (and constantly monitored), thus also **trust on the manufacturer is reduced**

- **The fastest secure QRNG** with more than **17 Gbps** of secure rate

- **Low cost and compact**: it only employs standard telecom devices

For details see the paper:
M. Avesani, D.G Marangon, G. Vallone, P. Villoresi
Nature Comm. 2019



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]

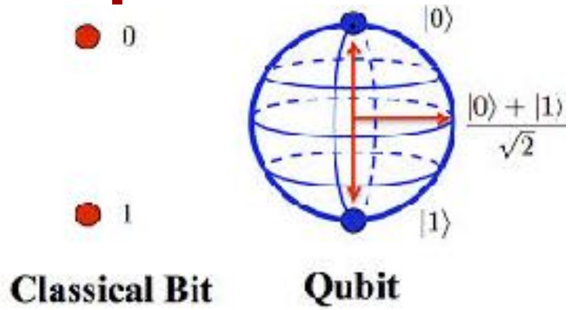
Link to the arxiv paper

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

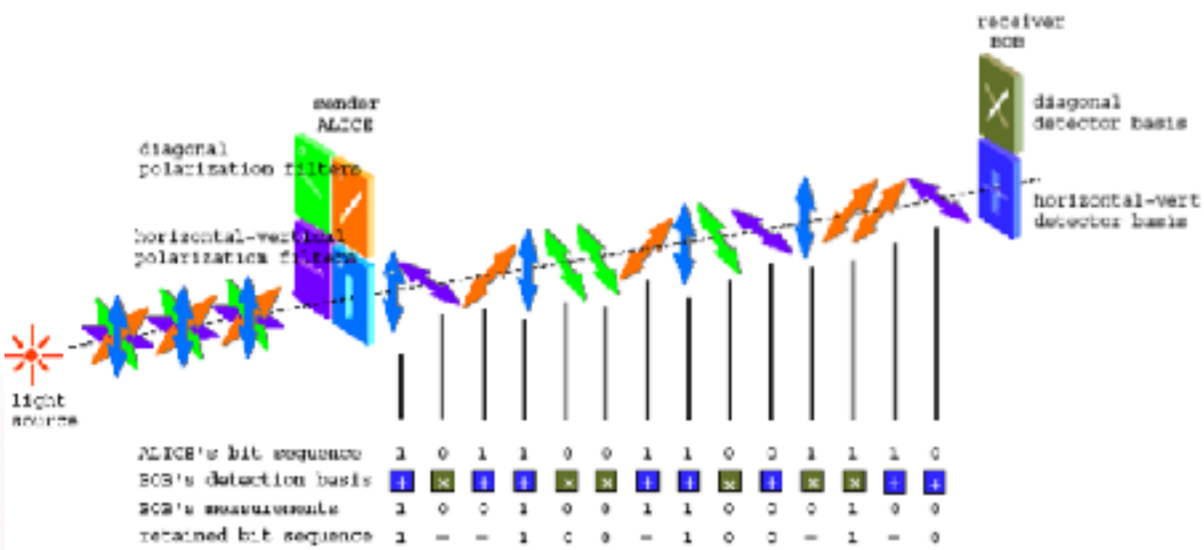
Random numbers are commonly used in many different fields, ranging from simulations in fundamental science to security applications. In some critical cases, as Bell's tests and cryptography, the random numbers are required to be both secure (i.e. known only by the legitimate user) and to be provided 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.

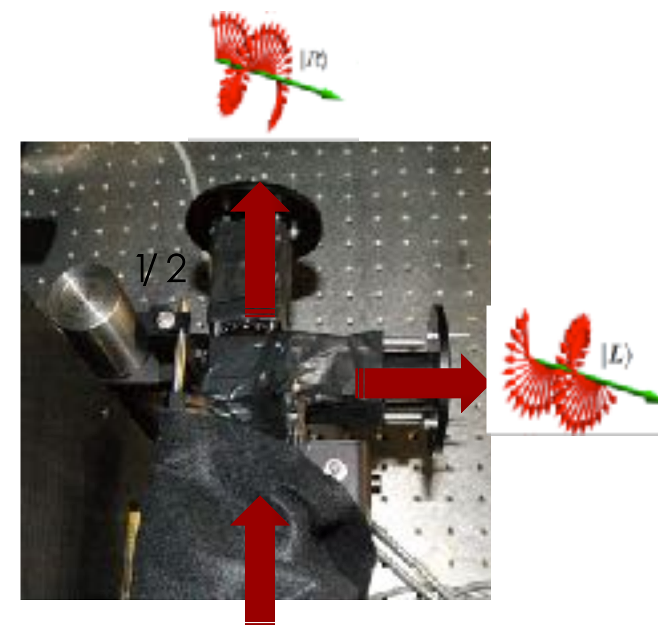
A sample (1GB) of the generated random number can be found at this link: https://goo.gl/duLvcZ

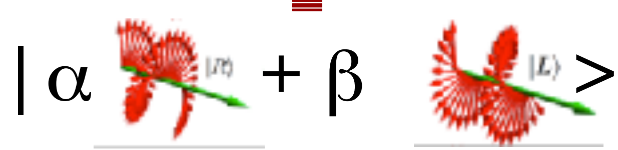
Other application: Quantum Communications
They are based on the sharing of qubits



- 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, ..

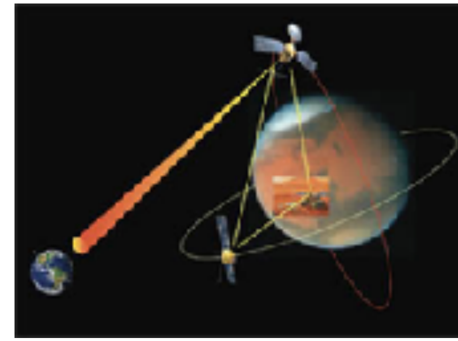


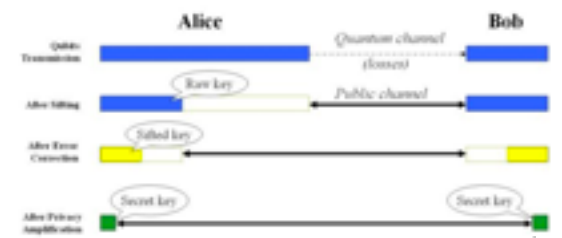


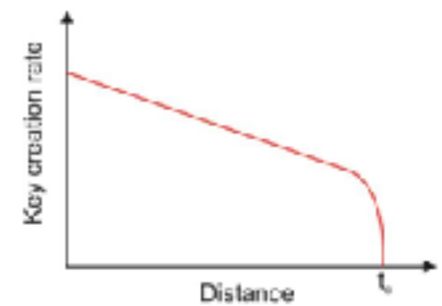


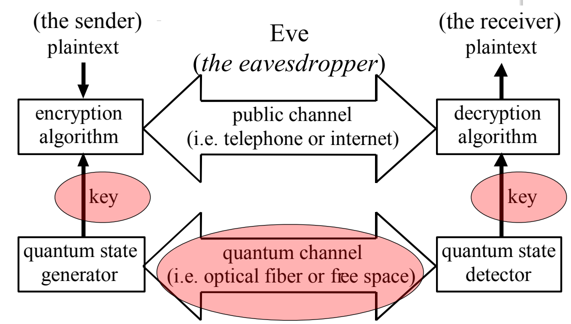
Quantum Key Distribution (QKD) in Space

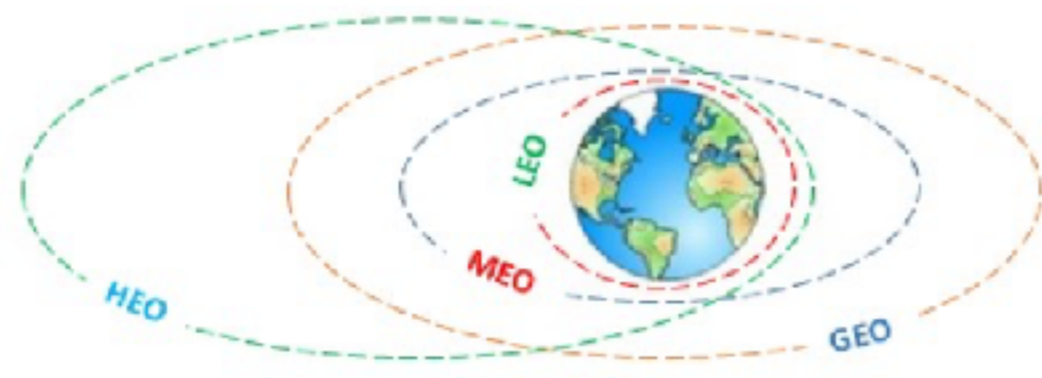
- The correlations based on the measure of individual photons, that can travel along Space channels, are used to generate a string, the raw-key, that is degraded if an eavesdropper taps in (seen as the mismatch of samples from transmitter and receiver).
- Such tapping is assessed as a noise level. Privacy 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.









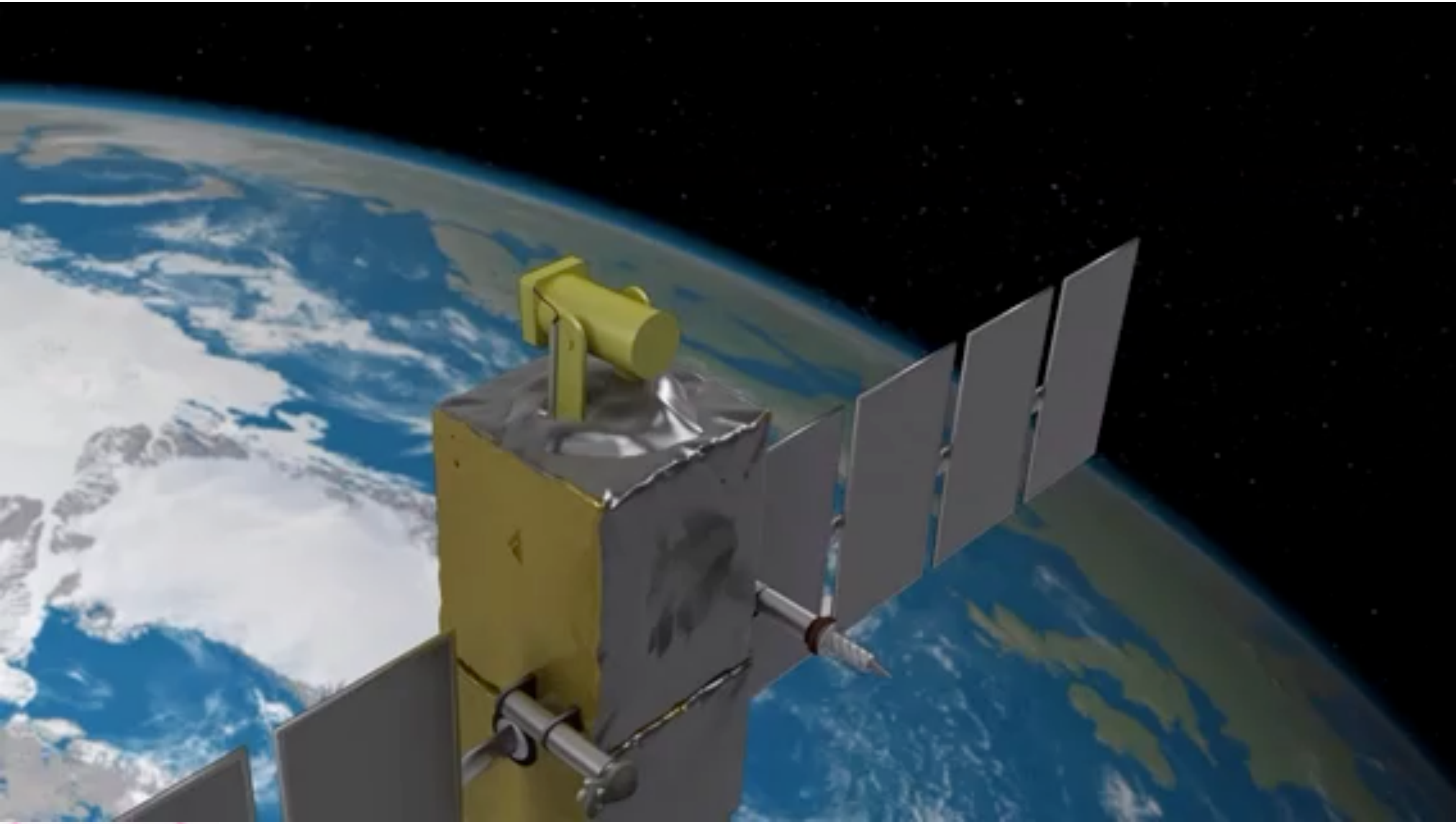


LEO orbits
rapid passages – large coverage – small payloads (potentially numerous)
secure communications (QKD – encryption of data)
fundamental test of Quantum Physics (Bell's test)
Micius and SOTA are here

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

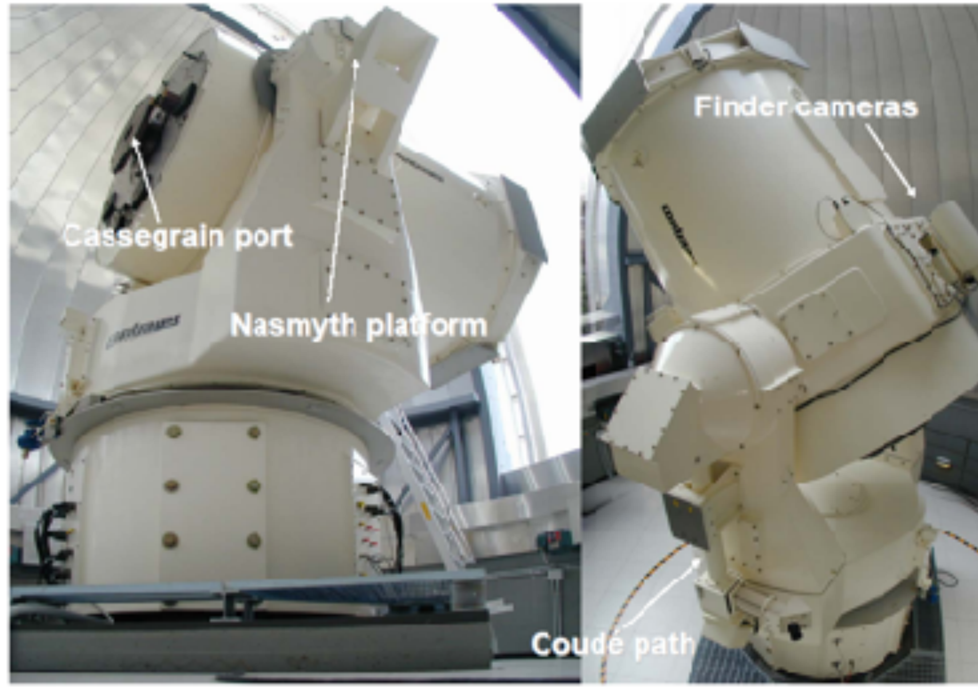
Inter-Sat Q-Comms for a GNSS constellatons



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

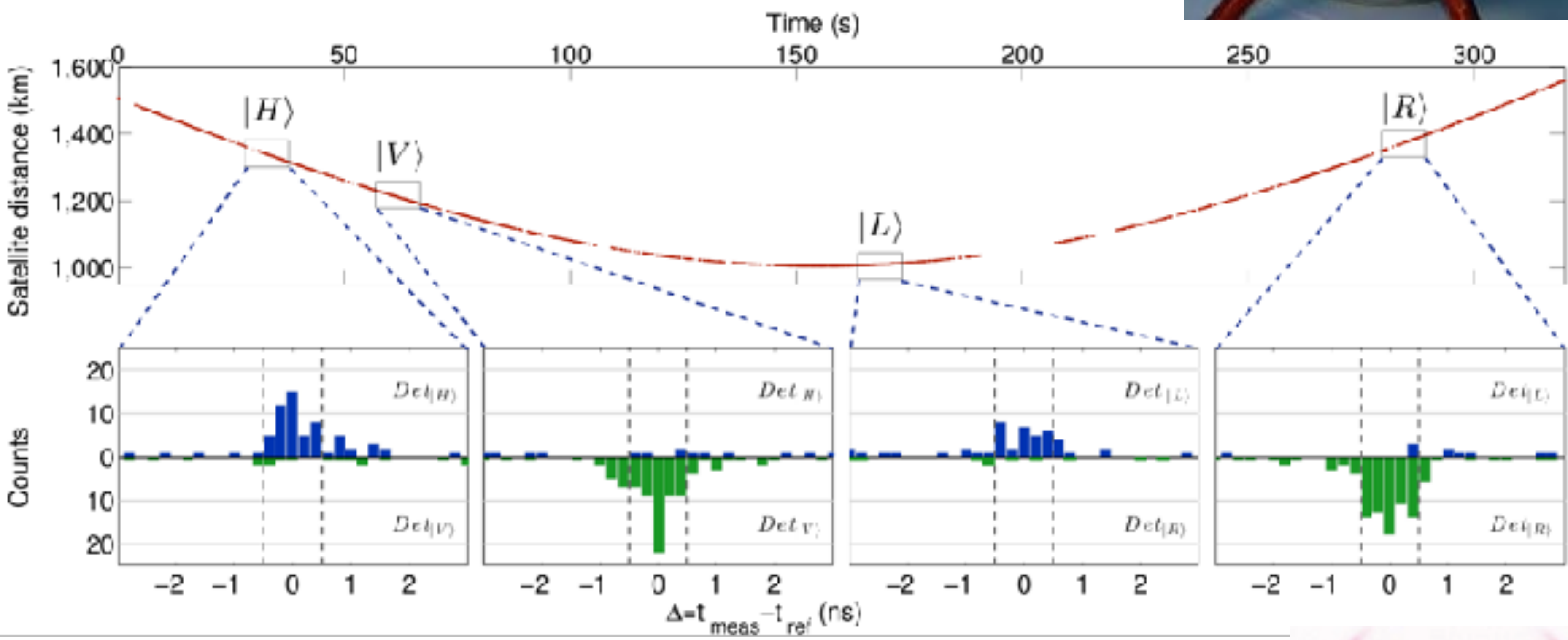
- *Giuseppe Colombo* Space Geodesy Centre of Italian Space Agency - Matera Laser Ranging Observatory (MLRO)
- Director Dr. Giuseppe Bianco President of ILRS
- World highest accuracy in SLR: mm-level for about 10^7 m range
- Accurate lunar ranging



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

Apr 10th, 2014, start 4:40 am CEST



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

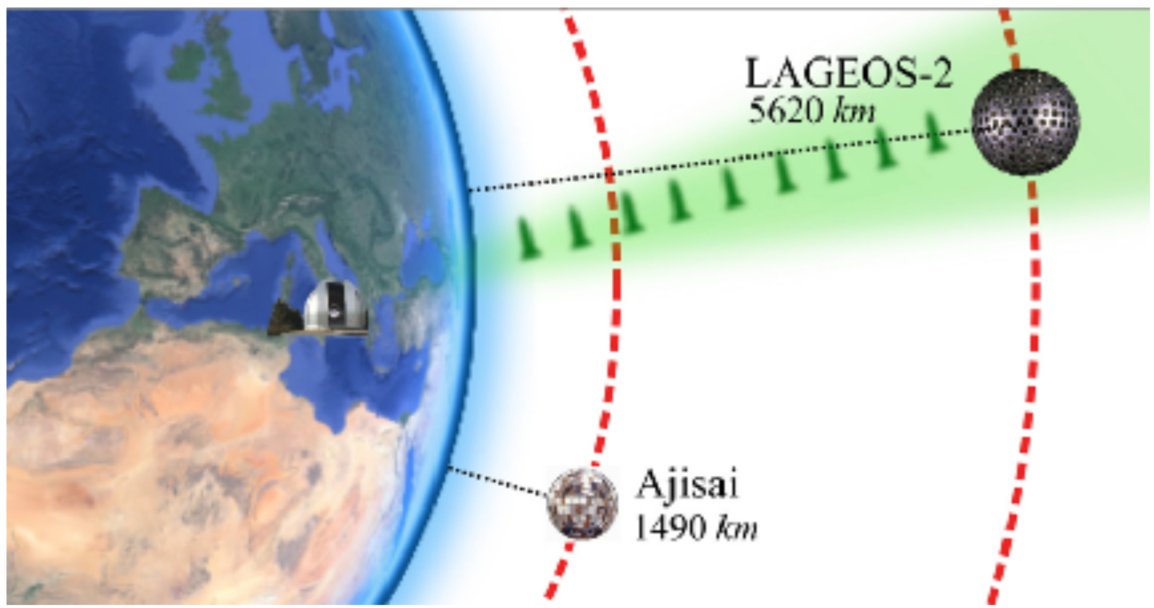
- **QBER ≃ (6.6±1.7) %**
- **Return rate 147 cps**

up to 10^4 bits for each satellite passage

G. Vallone et al, *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.



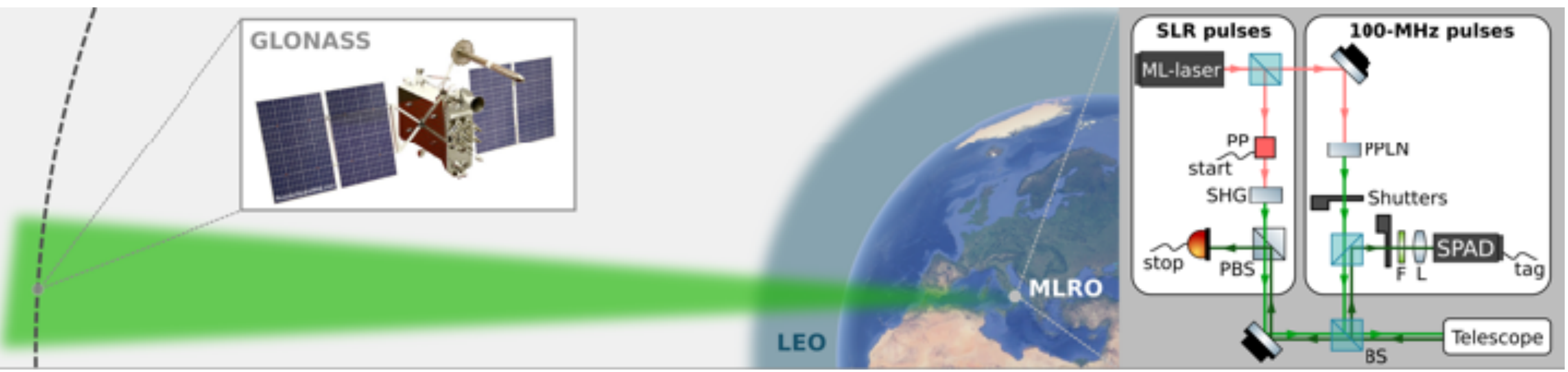
P. Villoresi et al., *Experimental verification of the feasibility of a quantum channel between space and Earth,*" New J. Phys. **10** 033038, 2008.
D. Dequal et al. *Experimental single photon exchange along a space link of 7000 km*, PRA Rapid Comm **93** 010301, 2016.

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).

Single passage of LARETS

Orbit height 690 km , spherical brass body

Text to be encrypted:

Universa Universis Patavina Libertas

Crypto key obtained on Apr. 11 2014 at 4:40 CEST

111011000011101101111100110101101101011111100011000101111011110011111000
111101011010011111110001110101000010101111101011111100100010011000101111
100110111111000101110111110111110100111101000101101101011100111111101101110
111110110110110110100110010111000111110110011111111001110111111011110110

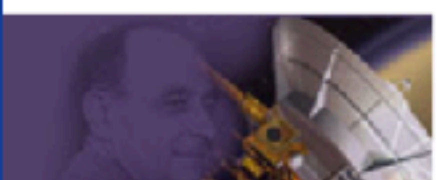
Encrypted text:
1011100101010101000101011010000010110010100100010110010011011101011011000
101000001100100110011000101000100100111010011001100000010100111101011100
1011101110110010100011101100101011111111111110100000010111100010001111
110110110010000111001110011111000011000111011011001001100011111110000101

Decripted text:

Universa Universis Patavina Libertas

NEWS
- Archivio News
- RSS Feed

- 01. ESPLORARE LO SPAZIO
- 02. OSSERVARE LA TERRA
- 03. ABITARE LO SPAZIO
- 04. ACCESSO ALLO SPAZIO
- 05. TELECOMUNICAZIONI E NAVIGAZIONE



Mezzo secolo di missioni spaziali italiane.

La storia dello spazio

E' italiana la prima trasmissione quantistica via satellite

Inviato un segnale a 1700 km di distanza tramite fotoni. L'esperimento dell'Università di Padova e dell'Agenzia spaziale italiana apre la strada ai futuri sistemi di telecomunicazione a prova di hacker

24 Giugno 2015

Inviare **informazioni protette**, praticamente **inviolabili**, fino alla **distanza record di 1700 km** utilizzando un fascio di **fotoni** 'sparato' nello spazio e rispedito a terra in un nanosecondo, è possibile. Lo hanno **dimostrato l'Università di Padova** e il **Centro di geodesia spaziale** dell'**Asi** di Matera che in sinergia hanno effettuato la **prima trasmissione satellitare quantistica** della storia.

L'esperimento, che è valso al team di studio la pubblicazione sulla rivista *Physical Review Letters*, è stato presentato **dal presidente dell'Asi Roberto Battiston** presso la sede dell'Agenzia insieme a **Paolo Villoresi**, coordinatore del gruppo dell'ateneo padovano che ha lavorato alla ricerca, **Giuseppe Vallone**, prima firma dell'articolo *Experimental satellite quantum communications* e **Giuseppe Bianco**, direttore del Centro geodesia spaziale dell'Asi. "C'è

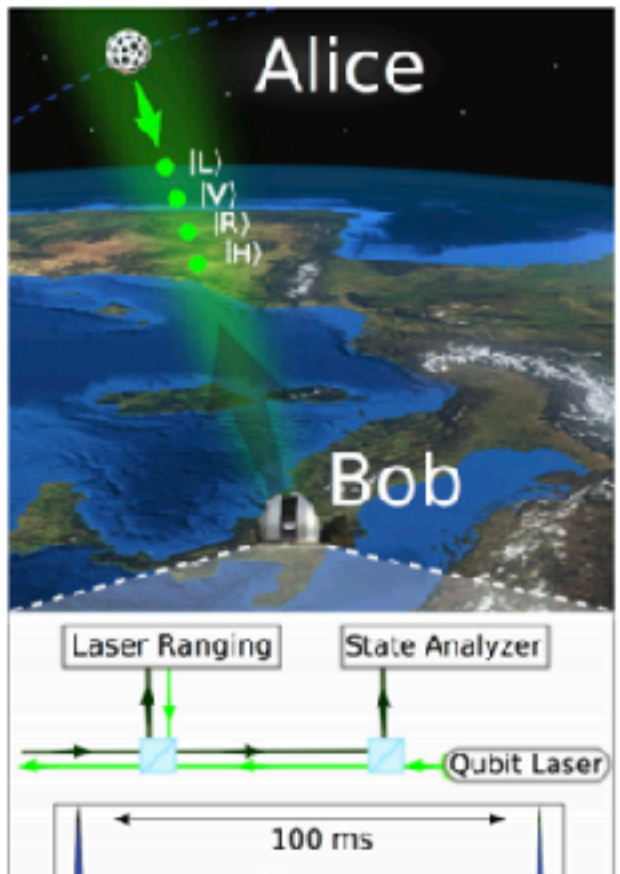
MIT Technology Review

NEWS & ANALYSIS ▾ FEA

Emerging Technology From the arXiv
June 27, 2014

The Space-Based Quantum Cryptography Race

Europe and China are gaining the upper hand in the race to bounce perfectly secure messages off satellites in low Earth orbit.



One of the great benefits of quantum communication is the ability to send messages from one point in space to another with perfect security. Not so great is the fact that so-called quantum cryptography is limited to distances of around 100 kilometers.

That's because over longer distances, photons tend to be absorbed by the glass in fiber-optic cables and by the atmosphere when beamed from one location to another. That causes errors that are too great for perfect privacy.

But there is a potential way around this–to send photons to an orbiting spacecraft, which then retransmits the message securely when it is over another part of the planet. That's possible because the photons traveling straight up only have to negotiate a few tens of kilometers of the atmosphere before reaching space.

First quantum transmission sent through space

- 17:53 26 June 2014 by Jacob Aron
- For similar stories, visit the Computer crime and Quantum World Topic Guides

Worried about keeping secrets? Here's a quantum of solace. The first quantum transmission to go via space paves the way for ultra-secure communications satellites.

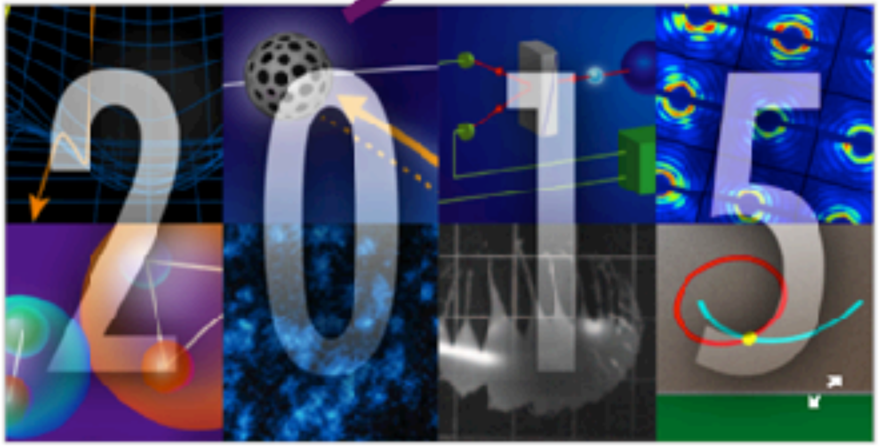
Secret encryption keys transmitted via quantum links provide the ultimate way to communicate securely. That's because any attempt to intercept the key will be revealed thanks to the laws of quantum mechanics, which say that interception will introduce changes that give away eavesdroppers.

The technology is already available for fibre-optic cables, but a truly global network would need satellites to beam quantum data between distant locations. To test how these might work, Paolo Villoresi at the University of Padua in Italy and his colleagues turned to satellites covered in ultra-reflective mirrors. These are normally used to bounce laser beams back to Earth. The time they take to return shows up any shifts in gravity.

Highlights of the Year

December 18, 2015 • *Physics* 8, 126

Physics picks its favorite stories from 2015.



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.

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

SCIENZA Grande scoperta pubblicata sulla «Physical Review Letters»

Parleremo coi marziani E lo faremo in italiano

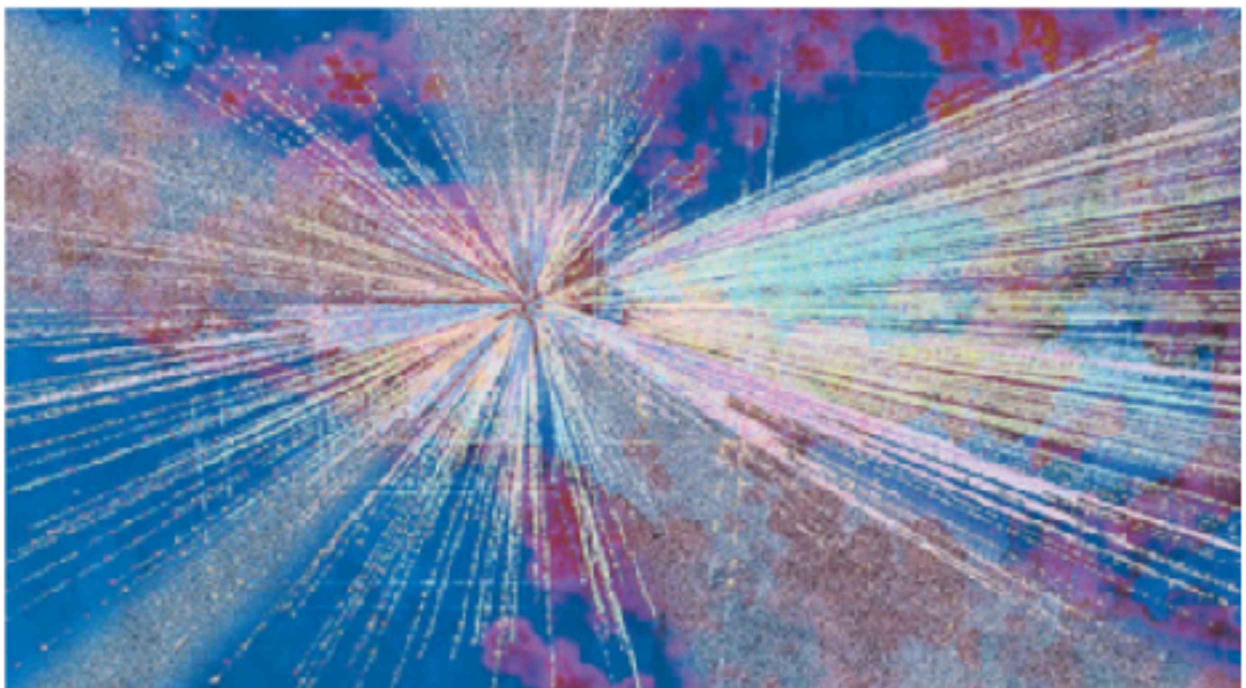
Si apre una nuova frontiera nella comunicazione quantistica grazie ai nostri scienziati: i dati viaggiano per 1700 km su particelle di luce

Gianluca Grossi

Comunicare nello spazio e sulla terra in modo da non essere mai intercettati e poter quindi consegnare senza problemi un messaggio segreto: è il sogno di ogni governo, di tutti i servizi di intelligence, e, in fondo, di ognuno di noi, abituati a scambiarci informazioni via mail o tramite Facebook con il timore di essere «scoperti». O volendo dare voce all'immaginazione, potremmo azzardare

COLLABORAZIONE

Tra Asi, ateneo di Padova e Centro Geodesia di Matera



TRA SCIENZA E FANTASCIENZA Primo messaggio quantistico al mondo via satellite

Observers of LARETS passages

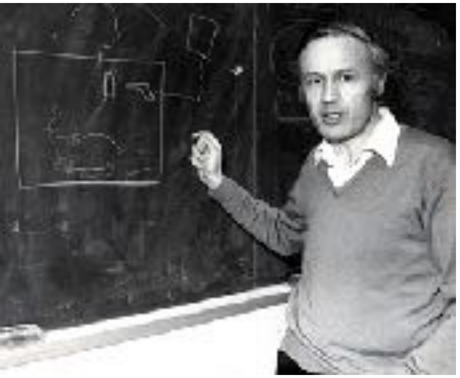
IOP PUBLISHING CLASSICAL AND QUANTUM GRAVITY
Class. Quantum Grav. 29 (2012) 224011 (44pp) doi:10.1088/0264-9381/29/22/224011

Fundamental quantum optics experiments conceivable with satellites—reaching relativistic distances and velocities

David Rideout[1,2,3], Thomas Jennewein[2,4], Giovanni Amelino-Camelia[6], Tommaso F Demarie[7], Brendon L Higgins[2,4], Achim Kempf[2,3,4,5], Adrian Kent[3,8], Raymond Laflamme[2,3,4], Xian Ma[2,4], Robert B Mann[2,4], Eduardo Martín-Martínez[2,4,5], Nicolas C Menicucci[3,9], John Moffat[3], Christoph Simon[10], Rafael Sorkin[3], Lee Smolin[3] and Daniel R Terno[7]

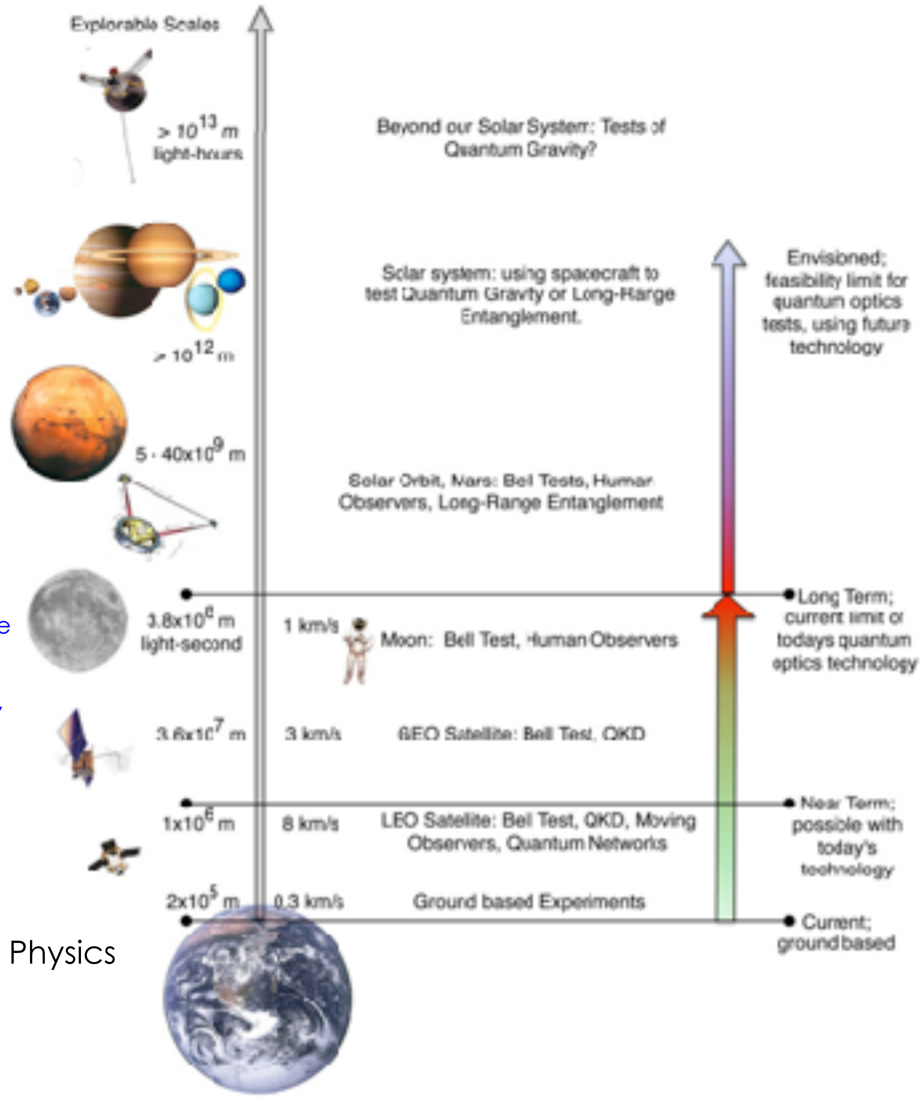
The tests have the potential **to determine the applicability of quantum theory at larger length scales**, eliminate various alternative physical theories, and **place bounds on phenomenological model**s motivated by ideas about **spacetime microstructure from quantum gravity**.

From a more pragmatic perspective, **as quantum communication technologies such as quantum key distribution advance into space towards large distances..**



'A truly definitive blocking of this loophole would presumably require that the detection be directly a by **two human observers with a spatial separation such that the signal transit time exceeds human reaction times, a few hundred milliseconds** (i.e. a separation of several tens of thousand kilometres). Given the extraordinary progress made in quantum communication in recent years, **this goal may not be indefinitely far in the future.**'

Tony Leggett



Leggett A 2009 Aspect experiment Compendium of Quantum Physics

The need for satellite security
Scenario **ground – ground**

- satellite as trusted relay sharing keys between two ground terminals
  - XOR of the two individual keys –
  - Generating a unique key for direct **ground** secure transmission

The need for satellite security
Scenario **satellite – ground**

1. QKD for symmetric crypto applications of data originating in the satellite
2. secure renewal of satellite keys, GPS P(Y) or Galileo PRS (Authentication and integrity of satellite positioning signal)

Satellite-based entanglement distribution over 1200 kilometers

Juan Yin,[1,2] Yuan Cao,[1,2] Yu-Huai Li,[1,2] Sheng-Kai Liao,[1,2] Liang Zhang,[2,3] Ji-Gang Ren,[1,2] Wen-Qi Cai,[1,2] Wei-Yue Liu,[1,2] Bo Li,[1,2] Hui Dai,[1,2] Guang-Bing Li,[1,2] Qi-Ming Lu,[1,2] Yun-Hong Gong,[1,2] Yu Xu,[1,2] Shuang-Lin Li,[1,2] Feng-Zhi Li,[1,2] Ya-Yun Yin,[1,2] Zi-Qing Jiang,[3] Ming Li,[3] Jian-Jun Jia,[3] Ge Ren,[4] Dong He,[4] Yi-Lin Zhou,[5] Xiao-Xiang Zhang,[6] Na Wang,[7] Xiang Chang,[8] Zhen-Cai Zhu,[5] Nai-Le Liu,[1,2] Yu-Ao Chen,[1,2] Chao-Yang Lu,[1,2] Rong Shu,[2,3] Cheng-Zhi Peng,[1,2*] Jian-Yu Wang,[2,3*] Jian-Wei Pan[1,2*]

Long-distance entanglement distribution is essential for both foundational tests of quantum physics and scalable quantum networks. Owing to channel loss, however, the previously achieved distance was limited to ~100 kilometers. Here we demonstrate satellite-based distribution of entangled photon pairs to two locations separated by 1203 kilometers on Earth, through two satellite-to-ground downlinks with a summed length varying from 1600 to 2400 kilometers. We observed a survival of two-photon entanglement and a violation of Bell inequality by 2.37 ± 0.09 under strict Einstein locality conditions. The obtained effective link efficiency is orders of magnitude higher than that of the direct bidirectional transmission of the two photons through telecommunication fibers.

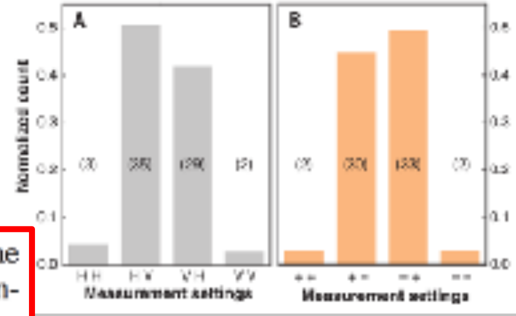


Fig. 4. Measurement of the received entangled photons after transmission by the two downlink channel. (A) Normalized two-photon coincidence counts in the measurement setting of the |H⟩/|V⟩ basis. (B) Normalized counts in the diagonal |±⟩ basis. Numbers in parentheses

we found $S = 2.37 \pm 0.09$, with a violation of the CHSH-type Bell inequality $S \leq 2$ by four standard deviations. The result again confirms the nonlocal feature of entanglement and excludes the models of reality that rest on the notions of locality and realism—on a previously unattained scale of thousands of kilometers.

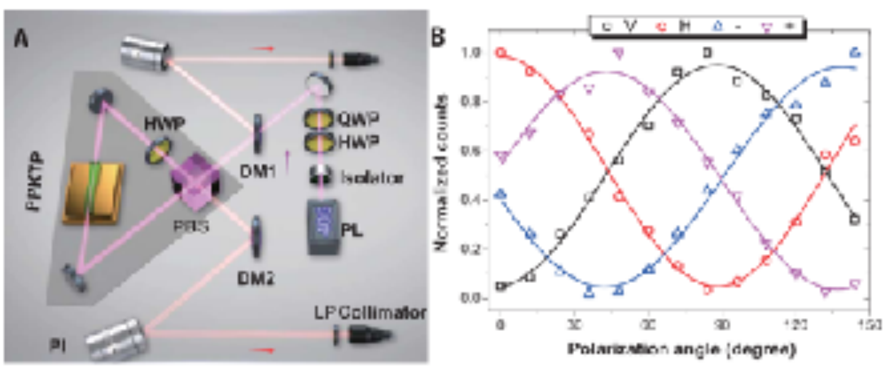


Fig. 1. Schematic of the spaceborne entangled-photon source and its in-orbit performance. (A) The thickness of the $KTiOPO_4$ (PPKTP) crystal is 15 mm. A pair of off-axis concave mirrors focus the pump laser (PL) in the center of the PPKTP crystal. At the output of the Sagnac interferometer, two dichromatic mirrors (DMs) and long-pass filters are used to separate the signal photons from the pump laser. Two additional electrically driven piezo steering mirrors (PIs), remotely controllable on the ground, are used for fine adjustment of the beam-pointing for an optimal collection efficiency into the single-mode fibers. QWP, quarter-wave plate; HWP, half-wave plate; PBS, polarizing beam splitter. (B) The two-photon correlation curves measured on-satellite by sampling 1% of each path of the entangled photons. The count rate measured from the overall 0.01% sampling is about 590 Hz, from which we can estimate the source brightness of 5.9 MHz.

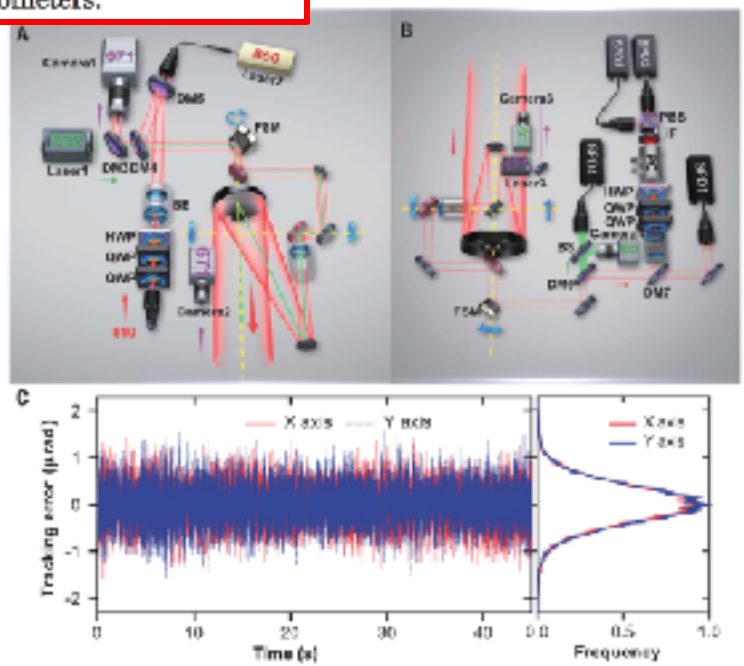
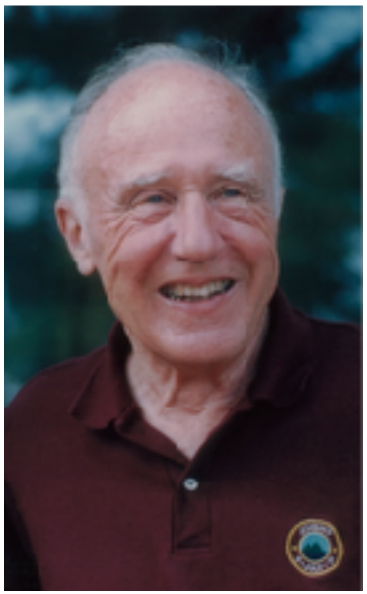


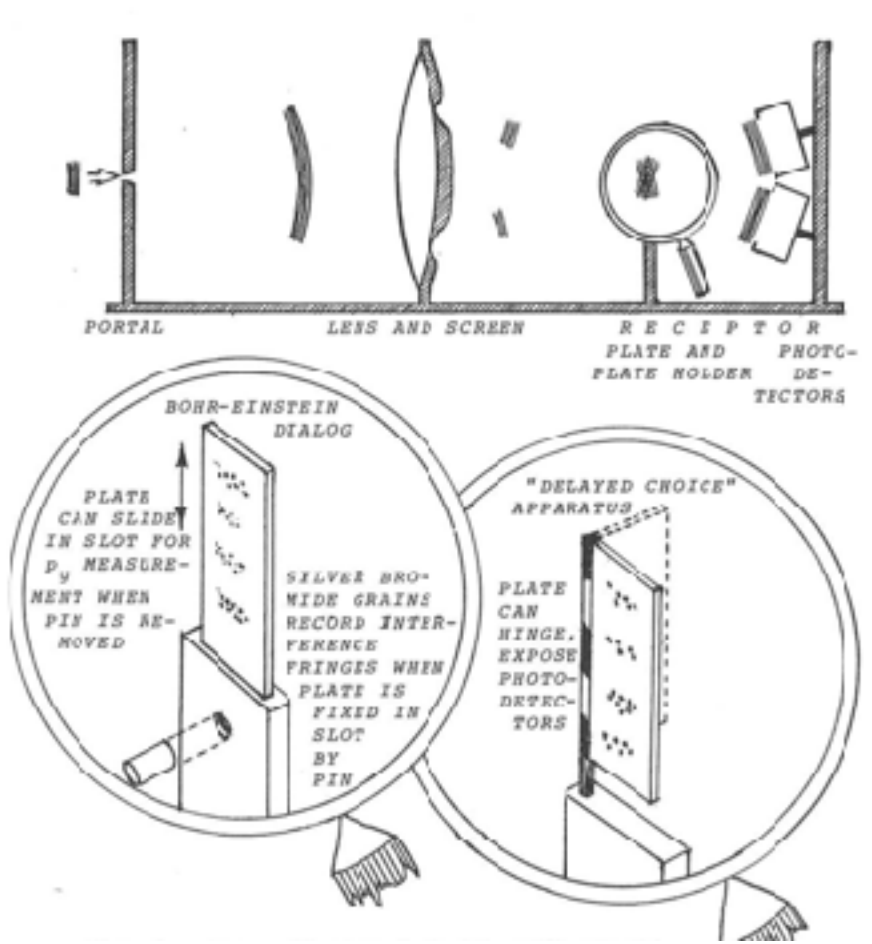
Fig. 2. The transmitters, receivers, and APT performance. (A) The entangled photon beam (810 nm) is combined and co-aligned with a pulsed infrared laser (850 nm) for synchronization and a green laser (532 nm) for tracking by three DMs and sent out from an 8× telescope. For polarization compensation, two motorized QWPs and a HWP are remotely controlled. A fast steering mirror (FSM) and a two-axis turntable are used for closed-loop fine and coarse tracking, based on the 671-nm beacon laser images captured by cameras 1 and 2. BE, beam expander. (B) Schematic of the receiver at Delingha. The cooperating APT and polarization compensation systems are the same as those on the satellite. The tracking and synchronization lasers are separate from the signal photon and detected by single-photon detectors (SPDs). For polarization analysis along bases that are randomly switching quickly, two QWPs, a HWP, a Pockels cell (PC), and a PBS are used. BS, beam splitter; IF, interference filter. (C) The APT system starts tracking after the satellite reaches a 5° elevation angle. The left panel is a 50-s trace of the real-time image readout from the camera. Fine-tracking accuracy of ~0.41 μrad is achieved for both the x and y axes.

Further step: inquiring the wave-particle duality in Space

- **Quantum theory provides the natural context for interpreting the measurement on a quantum state of complementary observables.**
- **In the context of fundamental QM tests, the wave-particle duality has been debated by the Giants**

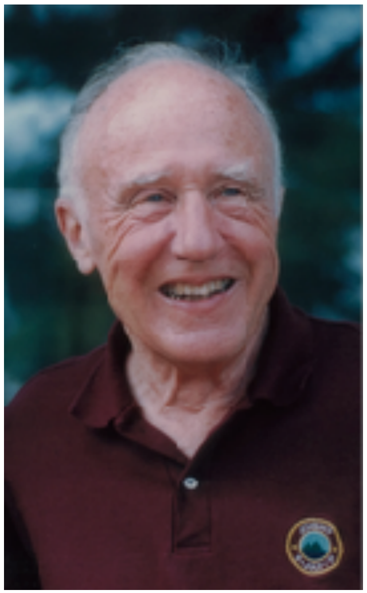
Wheeler Delayed-choice gedanken experiment

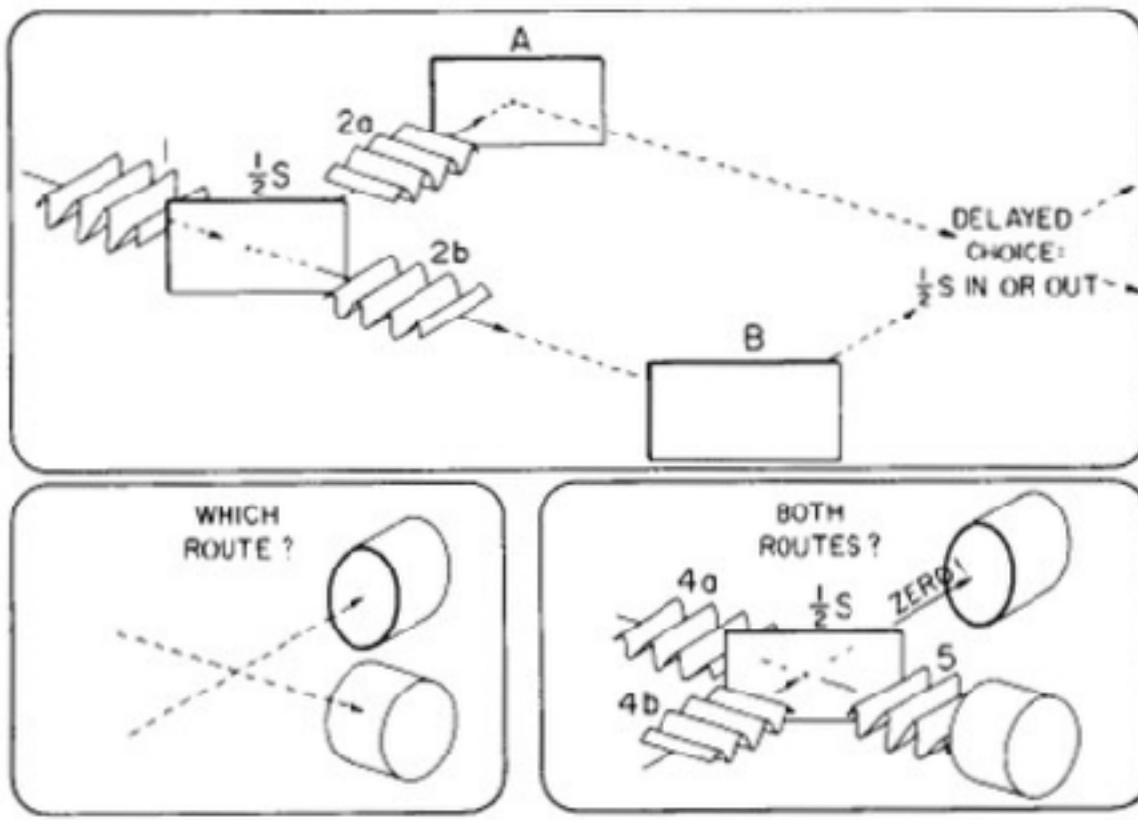




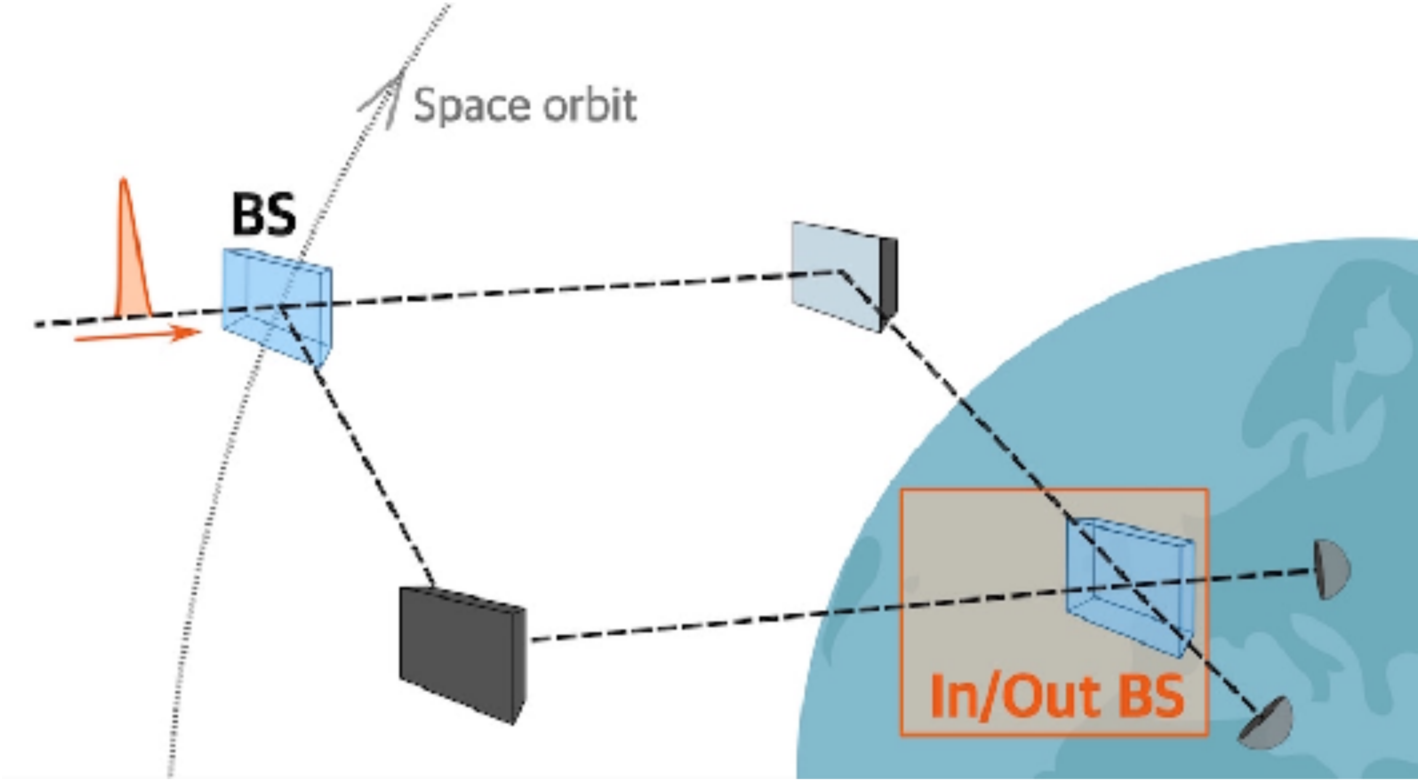
Wheeler JA (1978) The "past" and the "delayed-choice" double-slit experiment. Mathematical Foundations of Quantum Theory (Academic, New York), pp 9–48.

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





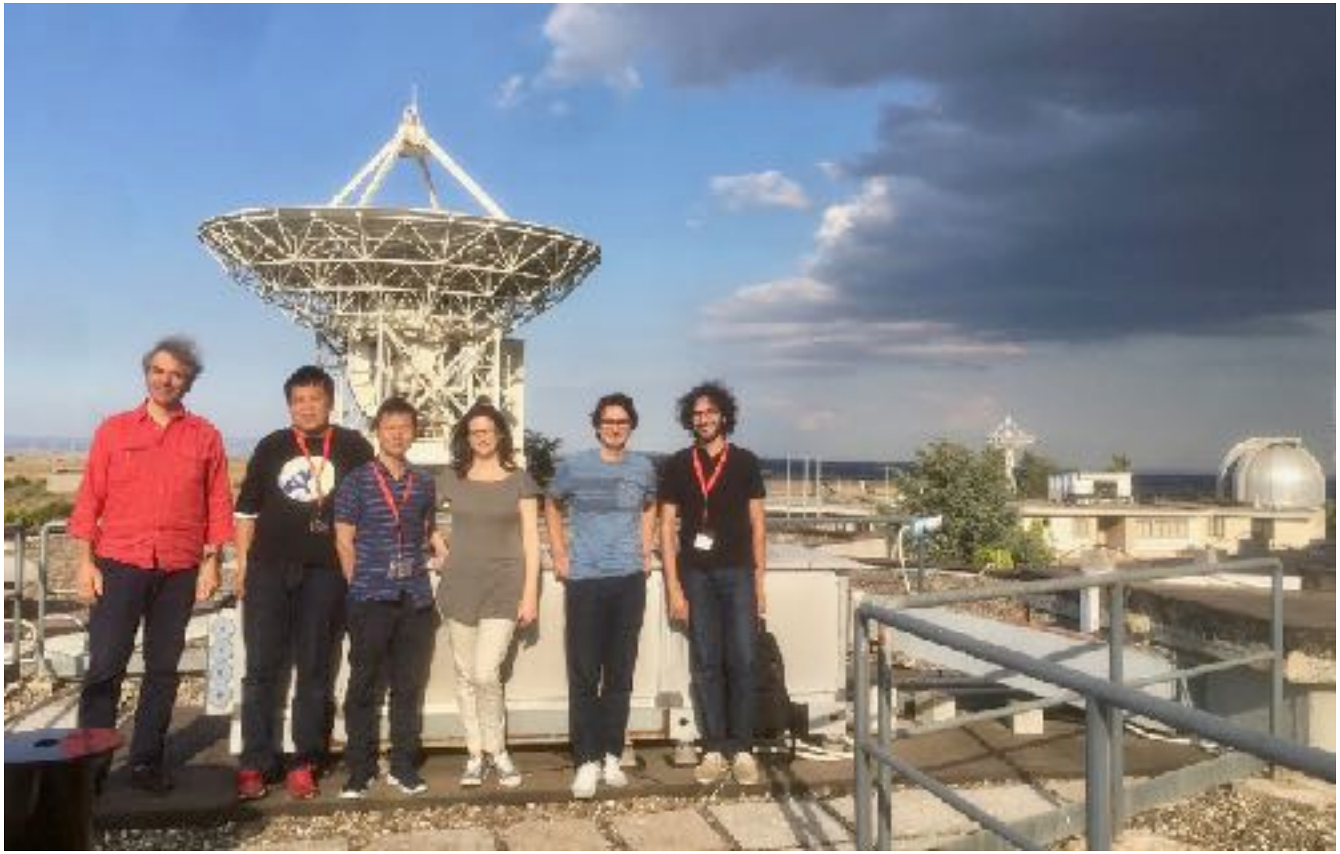
Step forward in Space QComms: inquiring the wave-particle duality along a Space channel



F. Vedovato et al. – arxiv:0417.011911 2017

Micius tracking and synchronization

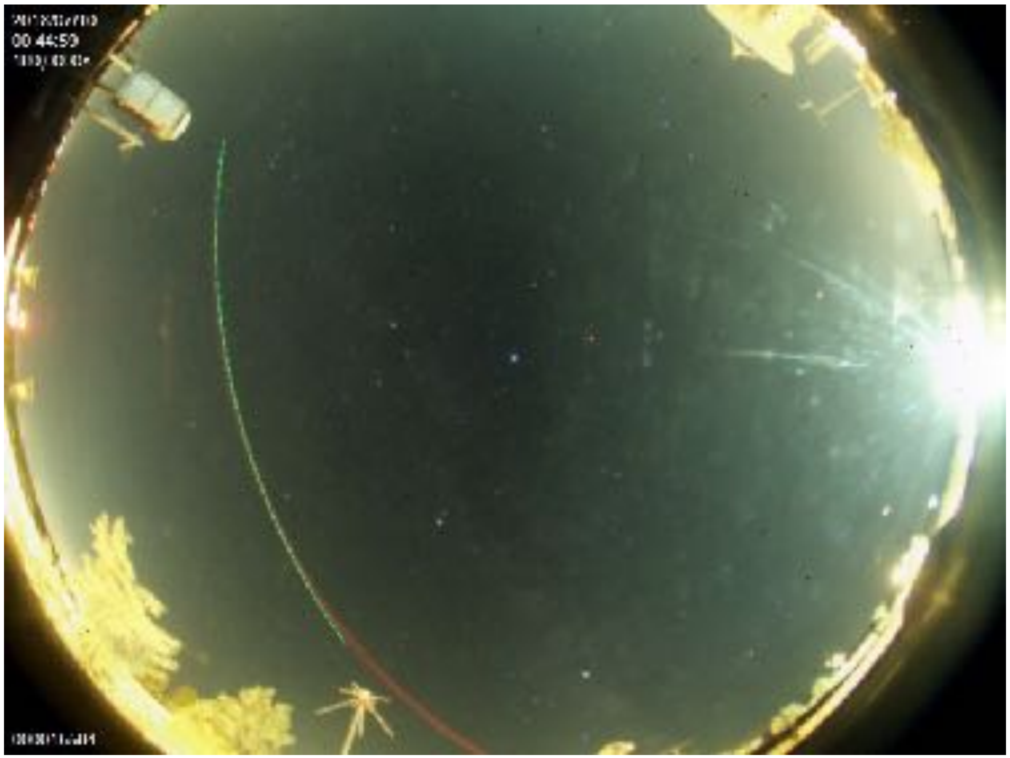
10-13 July 2018 - MLRO Matera



非常美丽的绿色彗星

Micius tracking and synchronization

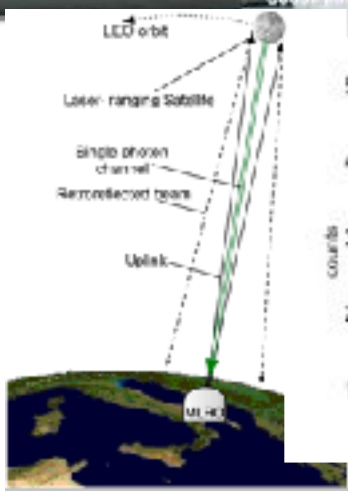
10-13 July 2018 - MLRO Matera

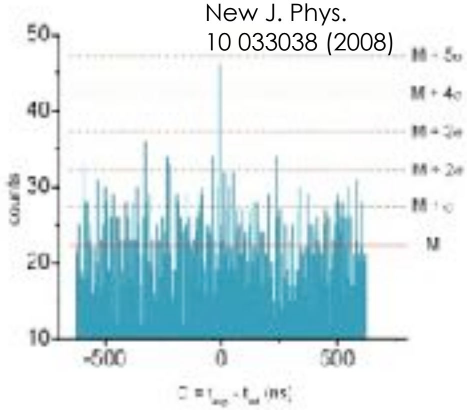


Italian Space Quantum Communications

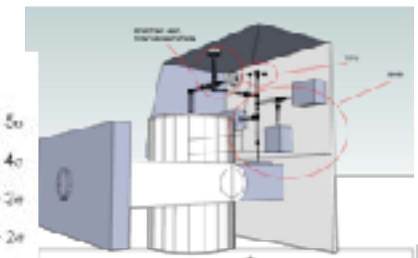
Exchanging quantum states, or quantum communications, allows for the realization of Quantum Information protocols as Quantum Teleportation, Q Key Distributions etc.

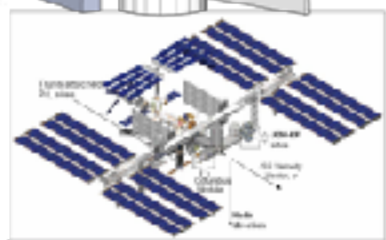
QuantumFuture Research Group of University of Padova, coordinated by **Paolo Villoresi,** operated since **2003** at ASI **Matera Laser Ranging Observatory,** using its **1.5 m telescope with millimeter resolution in Satellite Laser Ranging.**

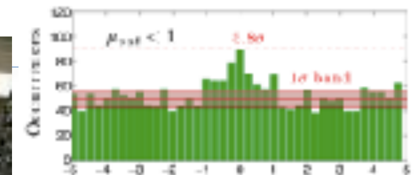


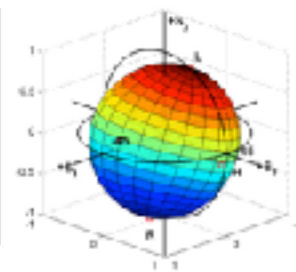


P. Villoresi et al.
New J. Phys.
10 033038 (2008)

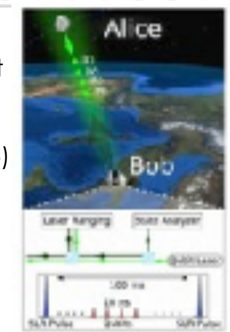








G. Vallone et al. Phys. Rev. Lett. vol 115 040502 (2015)



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

2018 20000km feasibility QComms

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

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,

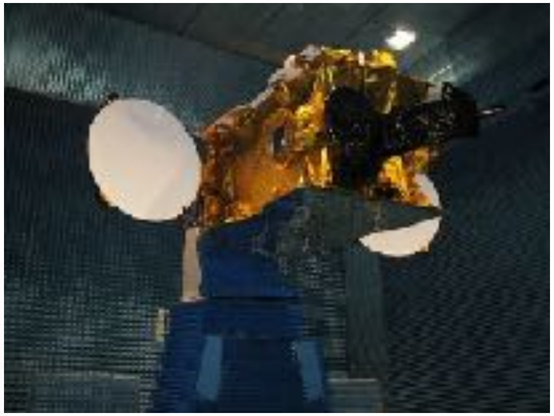
Goal 4: and then to GNSS.

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

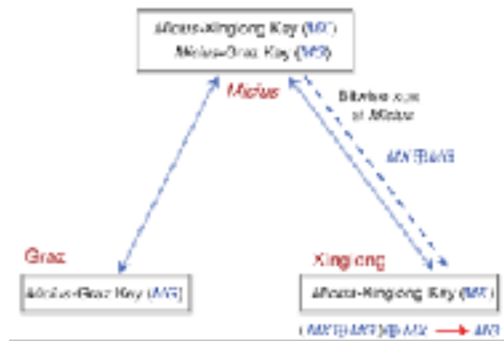


Satellite-Relayed Intercontinental Quantum Network

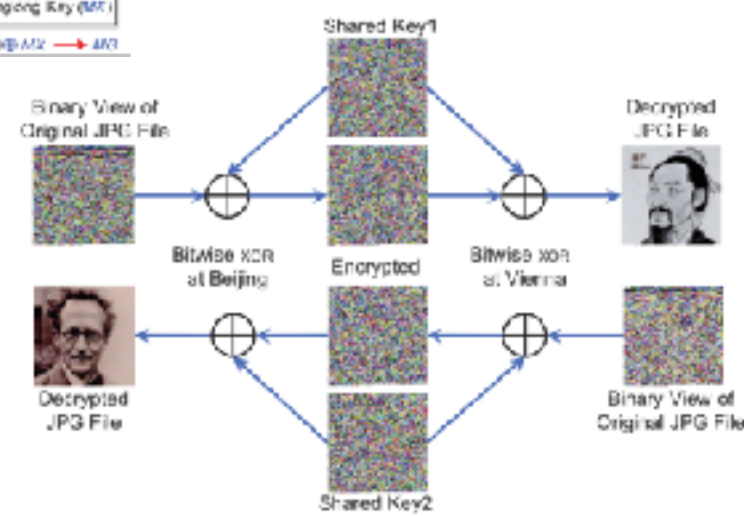
Micius satellite as a trusted relay to distribute secure keys between multiple distant locations in China and Europe

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)

Quantum Mechanics and Gravity Perspectives

The universe is a quantum computer.

Continuously elaborates its future.

Seth Lloyd

Events do not take place in space-time but it is the space-time that emerges from a network of events.

Giacomo Mauro D'Ariano

Lunar ranging
Matera
Laser Ranging
Observatory
Italian Space Agency
11 Jul. 2012

Conclusions and perspective

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

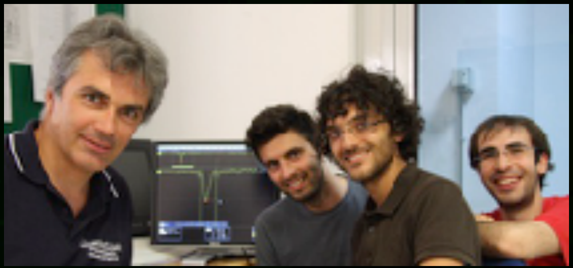
- **QC from a satellite transmitter to the Earth was experimentally demonstrated** as feasible using *polarization coding* – over 2000 km and *time-bins coding* – over 5000 km
- and the *single-ph. exchange for LEO and MEO - feasibility for GNSS*
- Novel fundamental tests in Space
- More properties of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

INTERNATIONAL COOPERATION ON TECHNOLOGY AND APPLICATIONS..

IN OTHER WORDS.. NOW PROJECTS, NEW GRANTS AND POSITIONS FOR STUDENTS

agenzia spaziale italiana

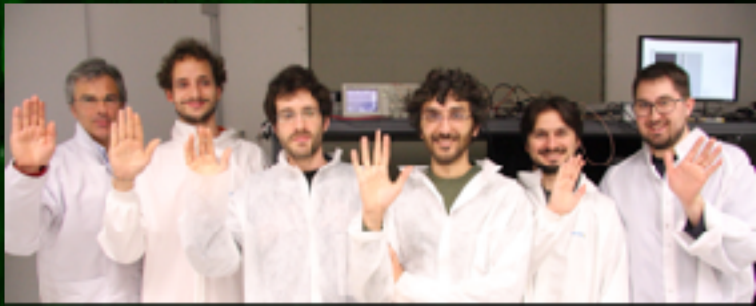
PV Pino Vallone   Simone Gaiarin
Daniele Dequal Davide Bacco



PV Davide Bacco Pino Vallone Nicola Baccichet

Prof. Cesare Barbieri

Fabrizio Tamburini   Cristian Bonato



PV Marco Tomasin   Pino Vallone   Francesco Vedovato
Matteo Schiavon   Daniele Dequal

Andrea Tomaello Alberto Dall'Arche

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, (A. Assalini, G. Pierobon)*

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

Quantum Astronomy *C. Barbieri, S. Ortolani*

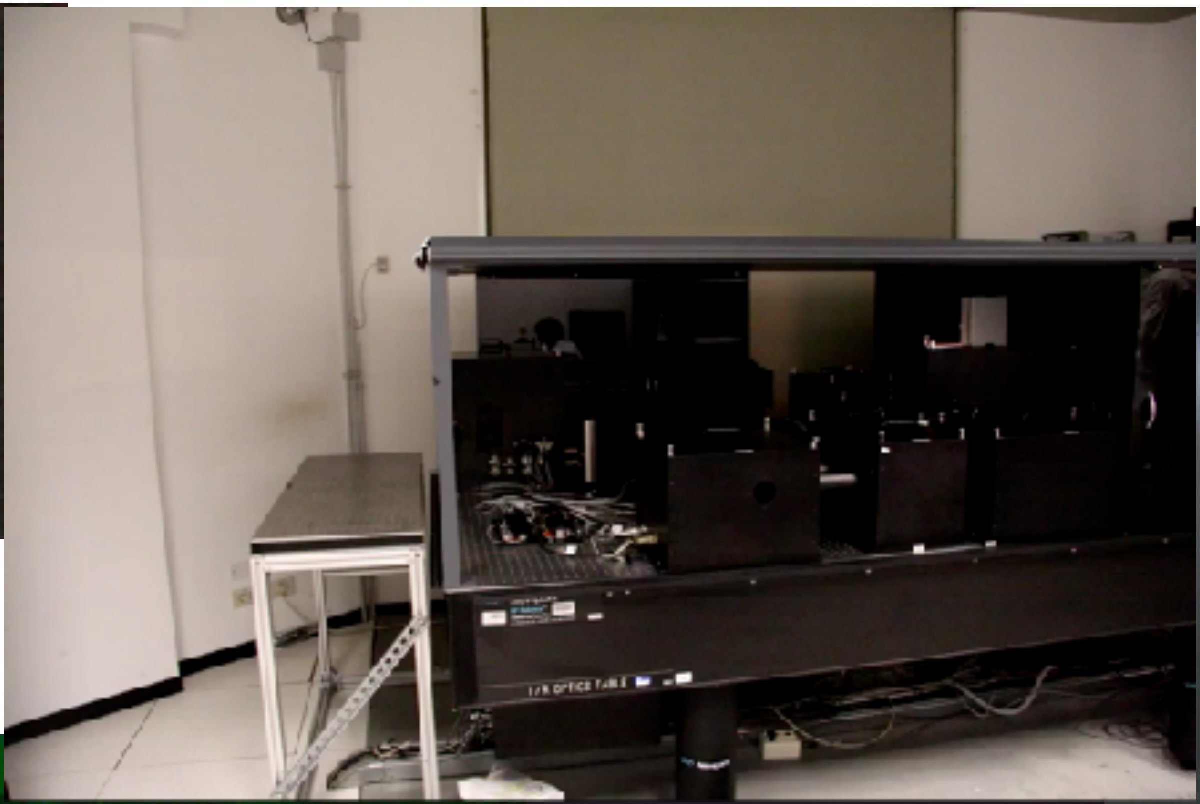
Fundend by **University of Padova**, **Italian Space Agency, European Space Agency,** industrial research contracts

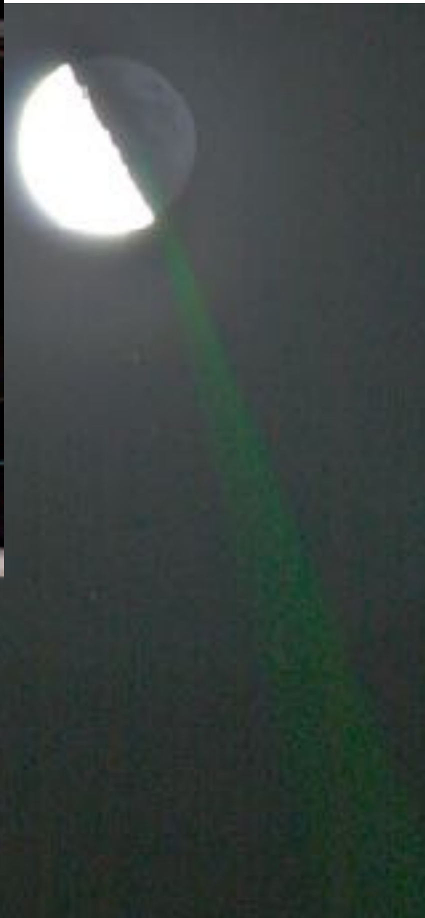
Strategic Res. Project of UniPD 2009-2013 (35 man-years PhD and Assegnisti)

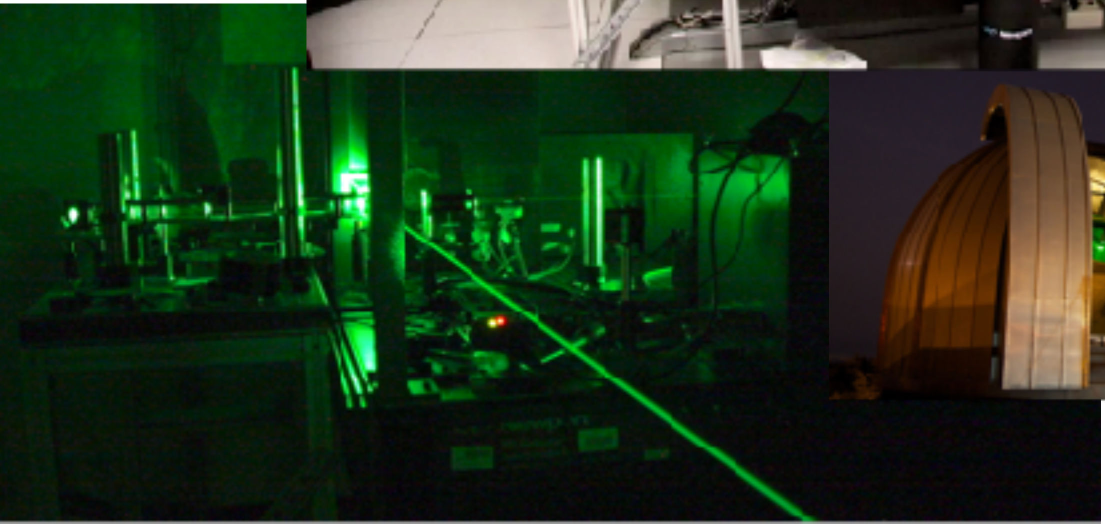
Currently **6 Faculties+6 PhD Students + 3 Post-Docs+ undergraduates + 2 EU MSCT PhD stud (2017)**

QF group in 2016

Comunicazioni Quantistiche: non limiti ma orizzonti







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