QUANTUM COMMUNICATIONS challenges and perspectives

Paolo Villoresi
QuantumFuture Research Group

University of Padua, Italy
Padua Quantum Technologies Research Center
Department of Information Engineering

GARR Online Workshop 2021, 8 nov 2021

800 1222 · 2022 ANNI

UNIVERSITÀ DEGLI STUDI DI PADOVA

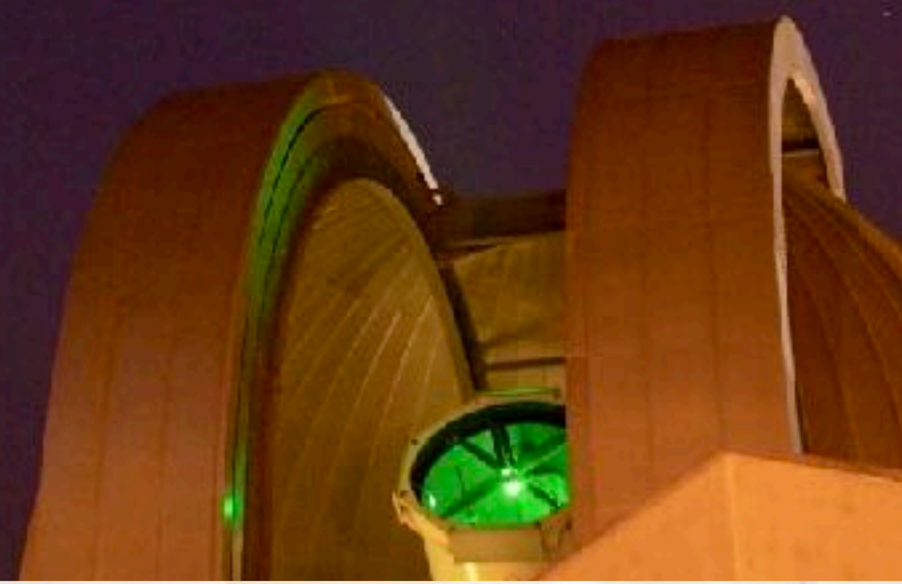
PADUA QTECH

QUANTUM COMMUNICATIONS challenges and perspectives

Paolo Villoresi
QuantumFuture Research Group

University of Padua, Italy
Padua Quantum Technologies Research Center
Department of Information Engineering

GARR Online Workshop 2021, 8 nov 2021



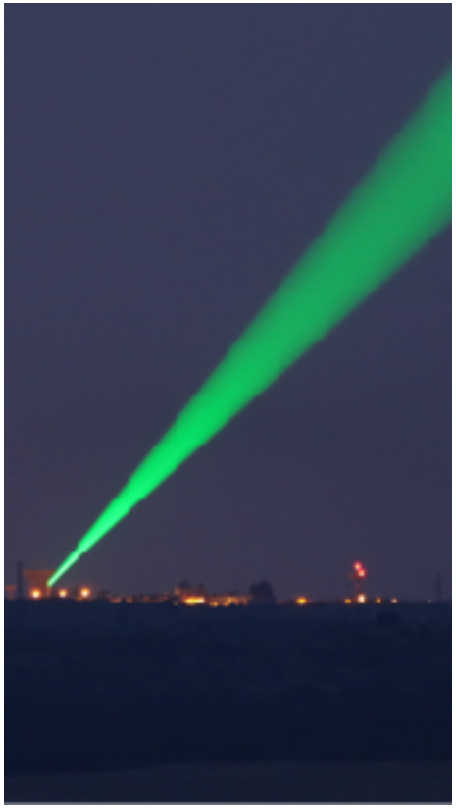
1222 · 2022 800 ANNI

UNIVERSITÀ DEGLI STUDI DI PADOVA

PADUA Q TECH

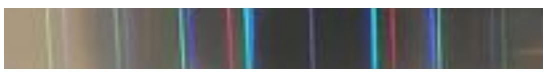
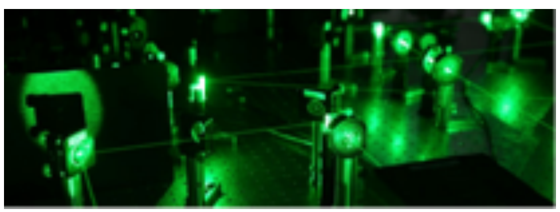
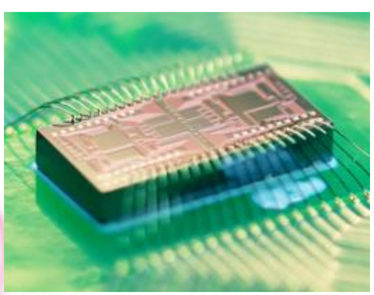
overview

- introduction to Quantum Information
- introduction to Quantum Communications
- essence for QKD
- how to realize it
- how we may cover the entire planet, and beyond..
- next moves



Quantum Communications are part of Quantum Technologies

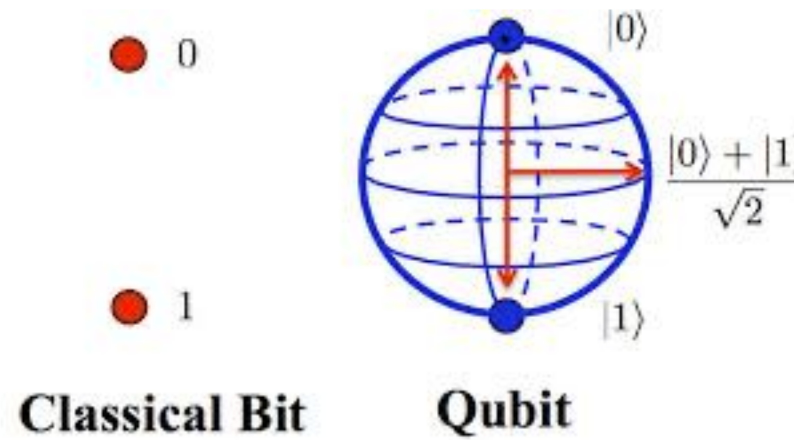


- *Quantum Mechanics*: the **interpretation of physical reality** in the **microcosmos**
  - provided the *understanding of atoms, molecules, fundamental particles, superconductivity*, etc.
  - allowed the *invention of transistors, lasers, integrated devices, etc.*
- **QM is now inspiring a *new age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

What the good of quantum states?

- Take a degree of freedom of a single photon
- EG polarization: 2D (Hilbert) space
- Superposition of base states: simultaneously H and V
- Enrich the concept of bit: welcome the qubit

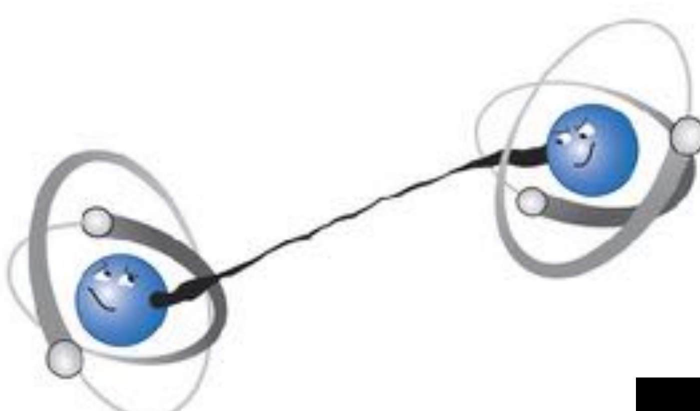


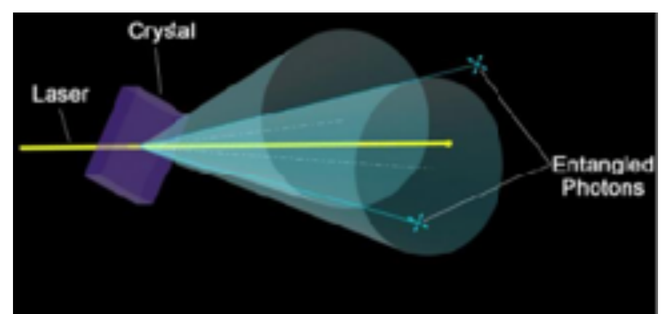
What the good of quantum states?

Entanglement

Erwin Schrödinger

Maximal knowledge of a total system does not necessarily include total knowledge of all its parts





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

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

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.

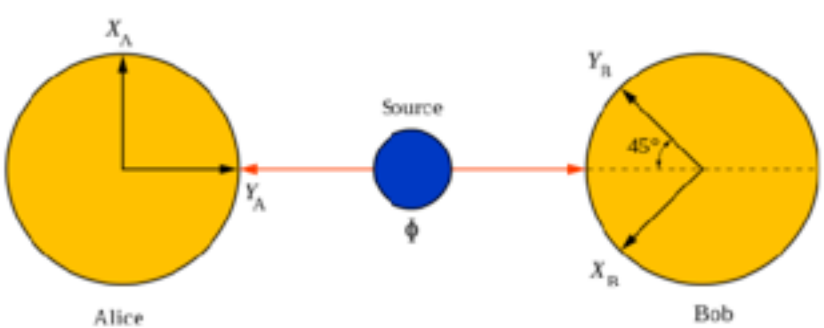
Locality

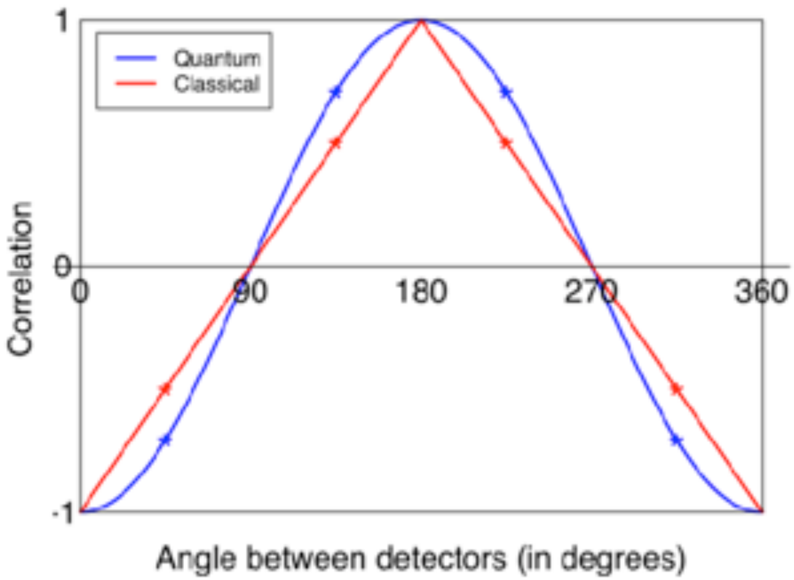
Realism

Bell's Theorem 1964

No physical theory based on locality and hidden variables can reproduce all Quantum Mechanics predictions

John S. Bell





VOLUME 47, NUMBER 7 PHYSICAL REVIEW LETTERS 17 AUGUST 1981

Experimental Tests of Realistic Local Theories via Bell's Theorem

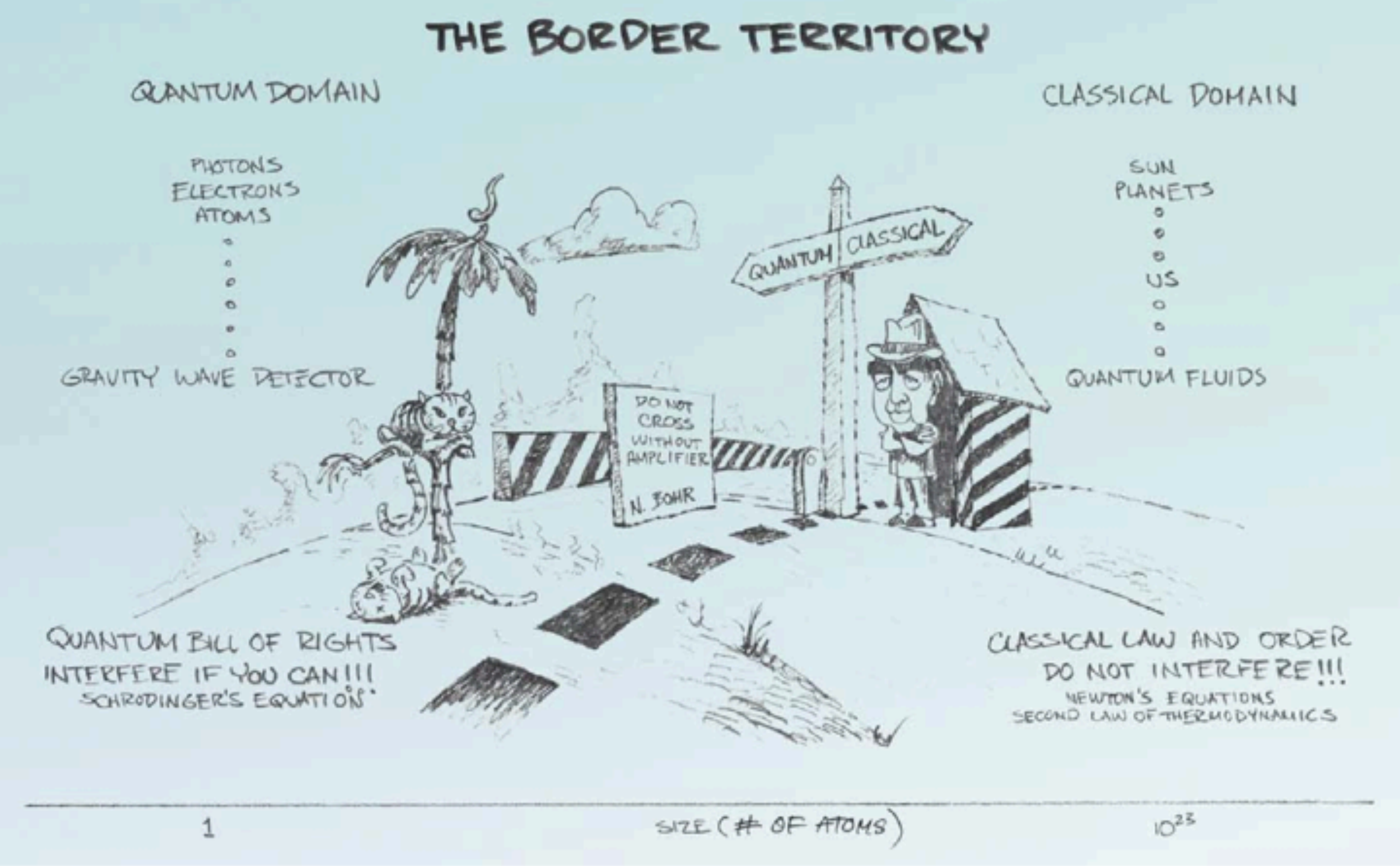
Alain Aspect, Philippe Grangier, and Gérard Roger
Institut d'Optique Théorique et Appliquée, Université Paris-Sud, F-91406 Orsay, France
(Received 30 March 1981)

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-Classical frontier



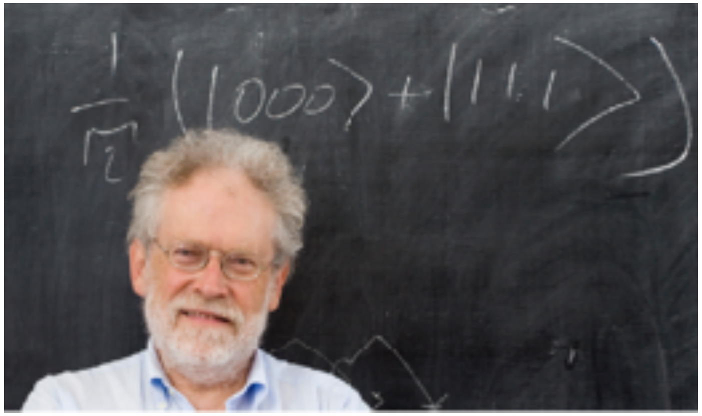
Wojciech H. Zurek, Decoherence and the Transition from Quantum to Classical *Physics Today (1991)*

http://www.physics.arizona.edu/~cronin/Research/Lab/some%20decoherence%20refs/zurek%20phys%20today.pdf

See also http://vykuz.ru/books/zurek.pdf

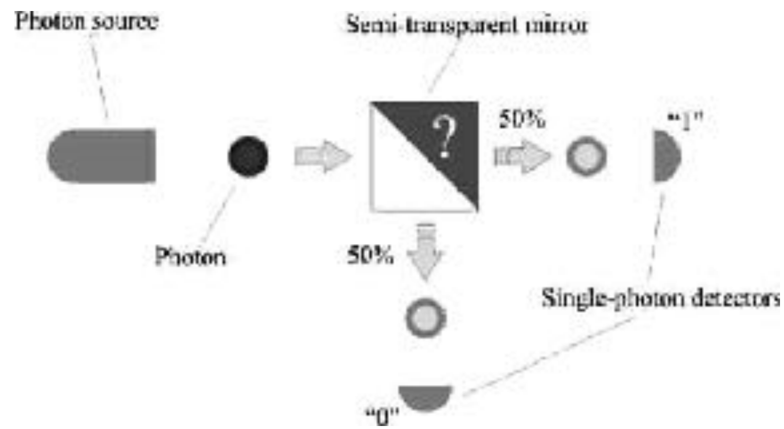
Quantum Information was born

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



A family of protocols: Quantum Random Number Generators

- A photon stream is sent on a semi-transparent mirror
- As each photon cannot be divided and they have equal probability to 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

Randomness is an invaluable resource for cryptography….

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.

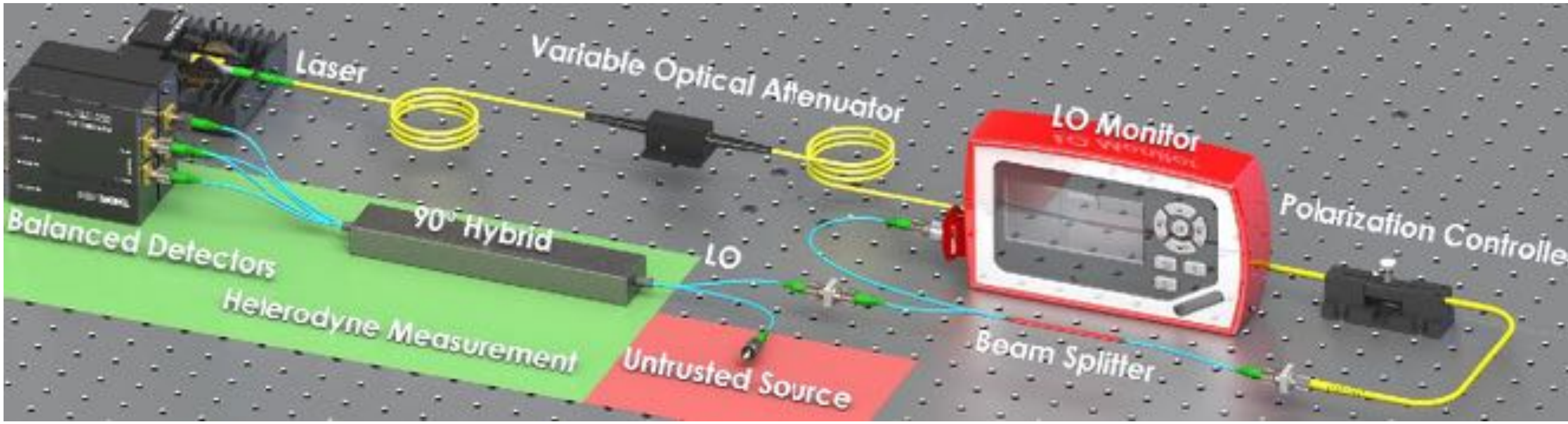
It had written a flaw into a random-number generator that would allow the agency to predict the outcome of the algorithm, the New York Times reported.

Android random number flaw implicated in Bitcoin thefts

Android, Cryptography, Data loss, Google

but it can completely compromise security.

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

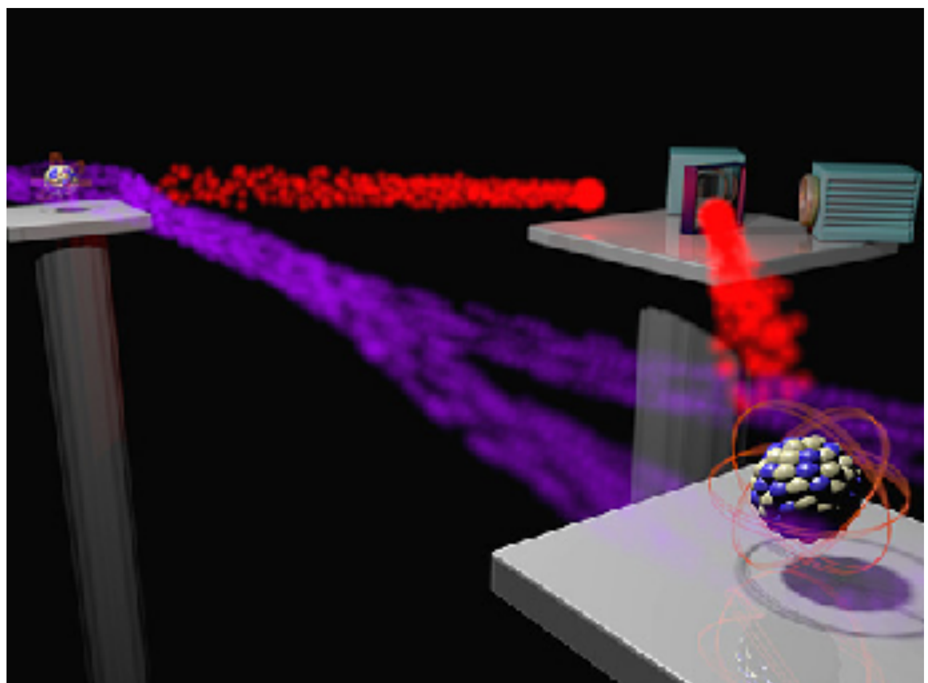


Hybrid approach, we **trust only one part of the device**, the measurement. However it is **monitored in real-time** to check for anomalies.
The **source is untrusted** and can be even **controlled by the attacker**.
Can offer security and speed at the same time: It is able to generate more than 17 Gbps of secure and private random numbers

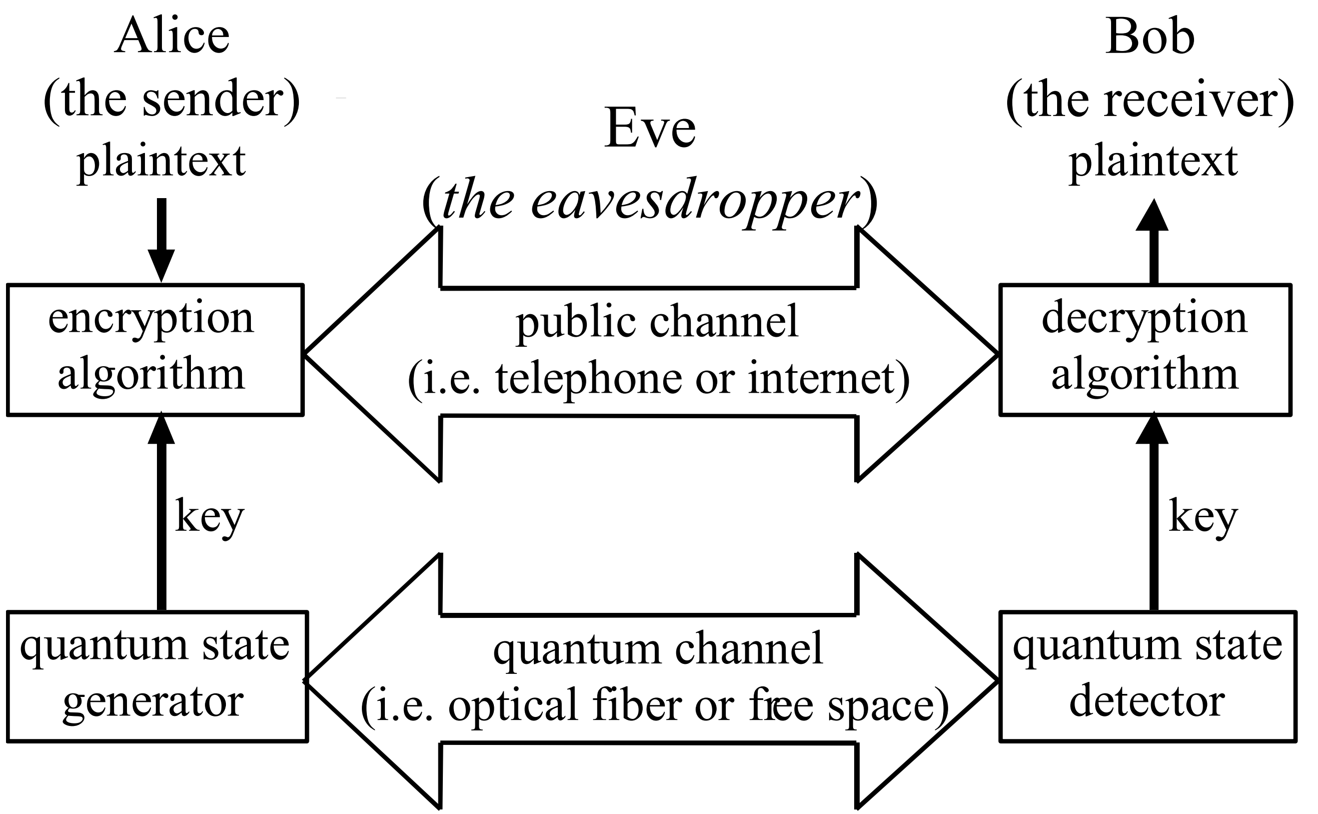
- M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, "***Source-device-independent heterodyne-based quantum random number generator at 17 Gbps***," Nat. Commun., vol. 9, no. 1, p. 5365, Dec. 2018.
- D. G. Marangon, G. Vallone, and P. Villoresi, "***Source-Device-Independent Ultrafast Quantum Random Number Generation***," Phys. Rev. Lett., vol. 118, no. 6, p. 060503, Feb. 2017.
- D. G. Marangon, G. Vallone, U. Zanforlin, and P. Villoresi, "***Enhanced security for multi-detector quantum random number generators***," Quantum Sci. Technol., vol. 1, no. 1, p. 015005, Nov. 2016.

Quantum Communications

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



The Quantum Key Distribution - QKD - application scheme



Is QKD needed?

On 4 December 2011, an American Lockheed Martin RQ-170 Sentinel unmanned aerial vehicle (UAV) **was captured by Iranian forces near the city of Kashmar** in northeastern Iran.

The drone was captured by jamming both satellite and land-originated control signals to the UAV, followed up by a GPS spoofing attack that fed the UAV false GPS **data to make it land in Iran at what the drone thought was its home base in Afghanistan.**

Iran–U.S. RQ-170 incident

PRESS TV

Home | News | Programs | Documentaries | US | فارسی

Thursday Jan 30, 2014 10:12 AM GMT Rob Ford brother-in-law accuses mayor of arranging jailhouse beatin

Home > Iran > Politics

Email Print

Iran military downs US spy drone

Sun Dec 4, 2011 2:17PM

8 0

Share Tweet

LAST UPDATE

An American RQ-170 Sentinel unmanned reconnaissance aircraft (file photo)

A senior Iranian military official says Iran's Army has downed a remote-controlled reconnaissance drone operated by the US military in the eastern part of the country.

The informed source said on Sunday that the Iranian Army's electronic warfare unit successfully targeted the US-built RQ-170 Sentinel stealth aircraft after it crossed into Iranian airspace over the border with neighboring Afghanistan.

He added that the US reconnaissance drone has been seized with minimum damage.

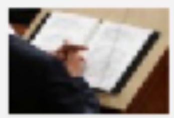
Is QKD needed?

The Washington Post | PostTV | Politics | Opinions | Local | Sports | National | World | Busine

National Security

In the News | State of the Union | School closings | John McCain | Pete Seeger | Super Bowl


Obama calls for year of action


Full text of Obama's speech


To mil

NSA seeks to build quantum computer that could crack most types of encryption

By Steven Rich and Barton Gellman, Published: January 2 E-mail the writers

In room-size metal boxes secure against electromagnetic leaks, the National Security Agency is racing to build a computer that could break nearly every kind of encryption used to protect banking, medical, business and government records around the world.

According to documents provided by former NSA contractor Edward Snowden, the effort to build "a cryptologically useful quantum computer" — a machine exponentially faster than classical computers — is part of a \$79.7 million research program titled "Penetrating Hard Targets." Much of the work is hosted under classified contracts at a laboratory in College Park, Md.

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)

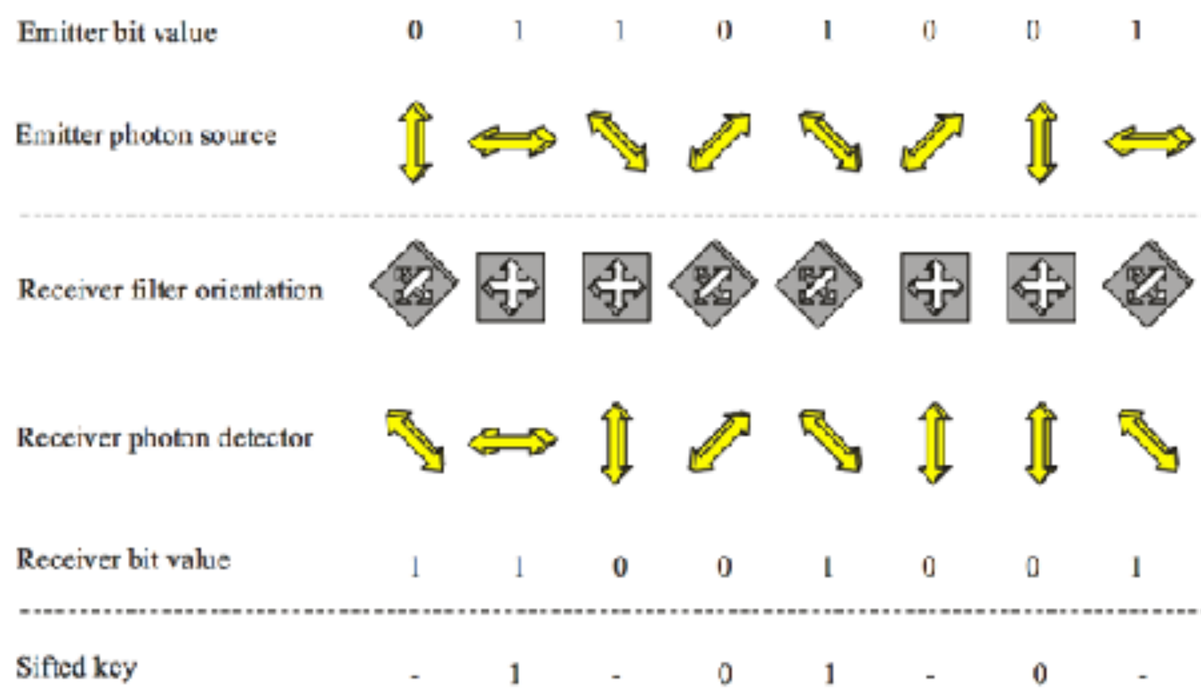
Will there be a QKD in our future ?

https://www.youtube.com/watch?v=zmVEyXRJ3hI&feature=youtu.be

QKD Protocol using photons

Practical example: Bennett and Brassard 1984

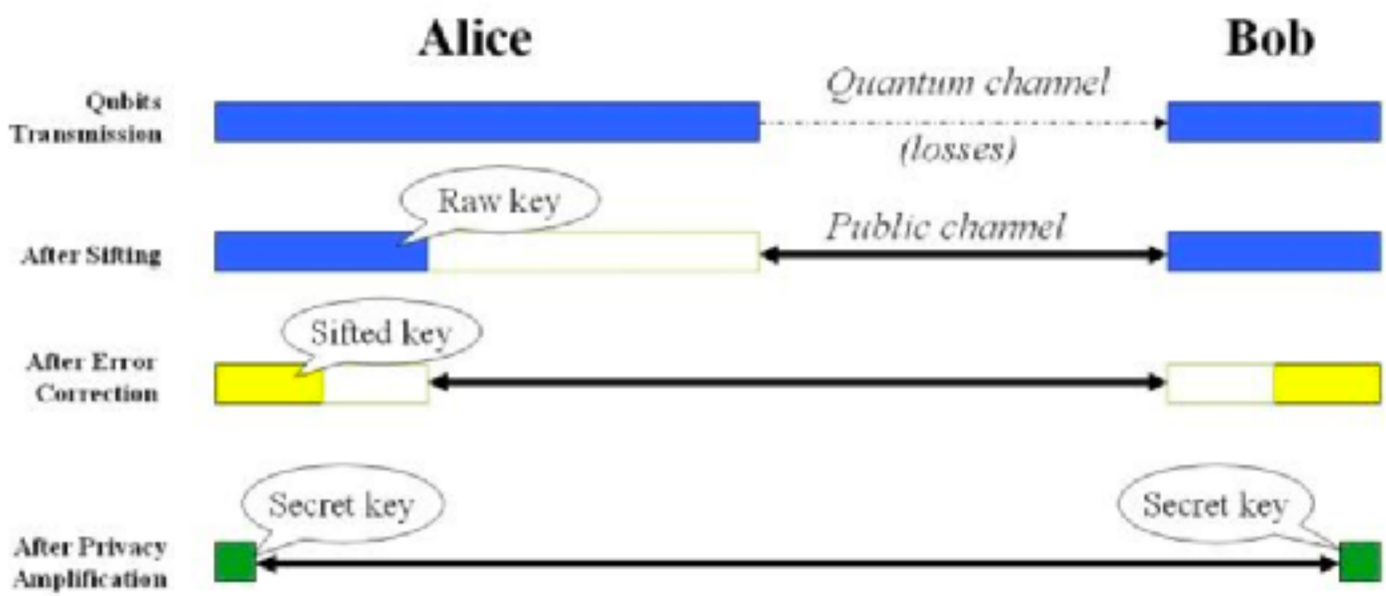
- 4 photon states:
  - Two orthogonal polarization states
  - Two non-orthogonal reference frames



QKD Protocol using photons

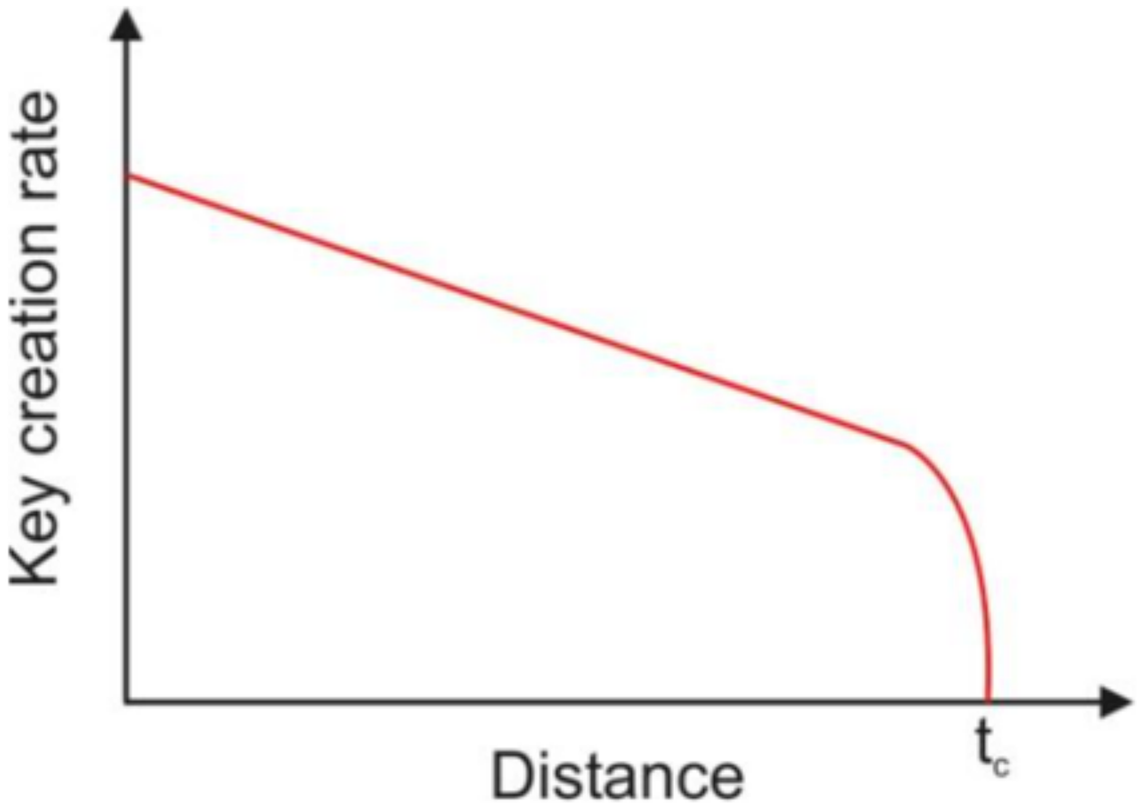
steps of BB84:

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



QKD Protocol using photons

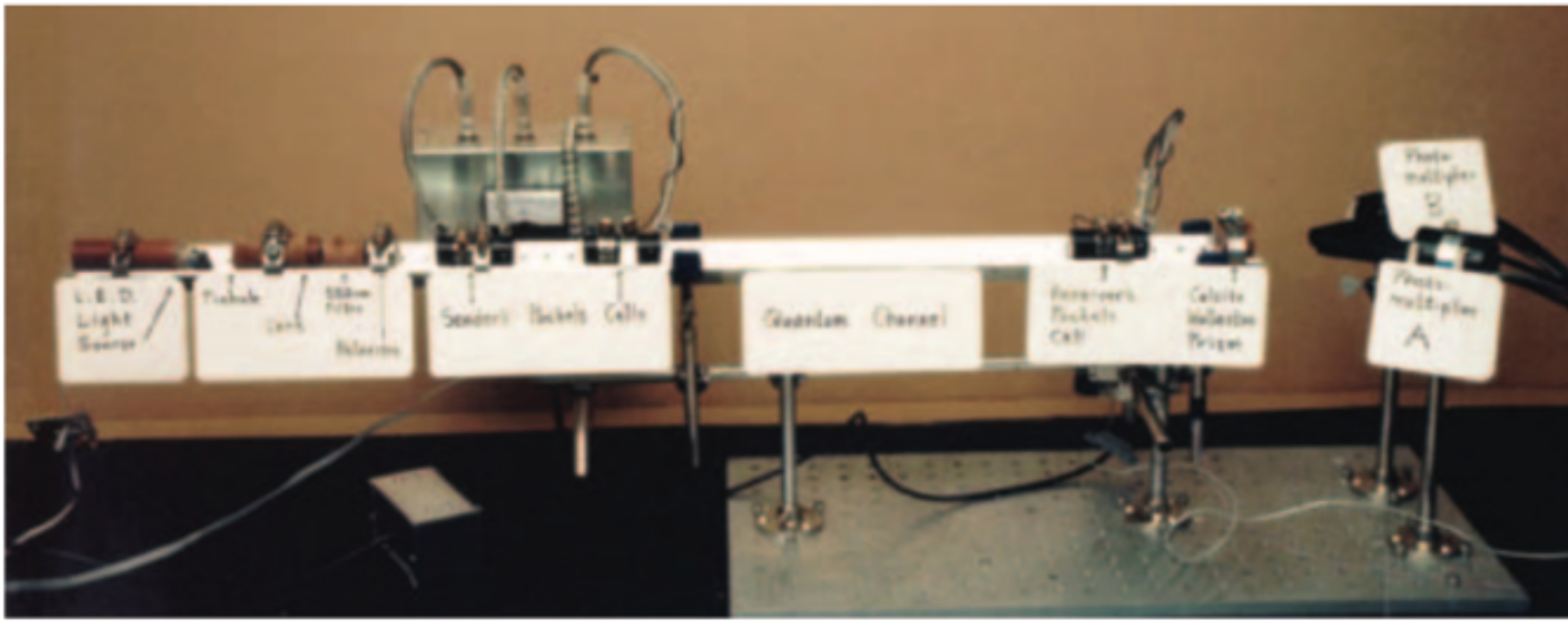
trend of key exchange rate with distance (losses)



QKD Protocol using photons

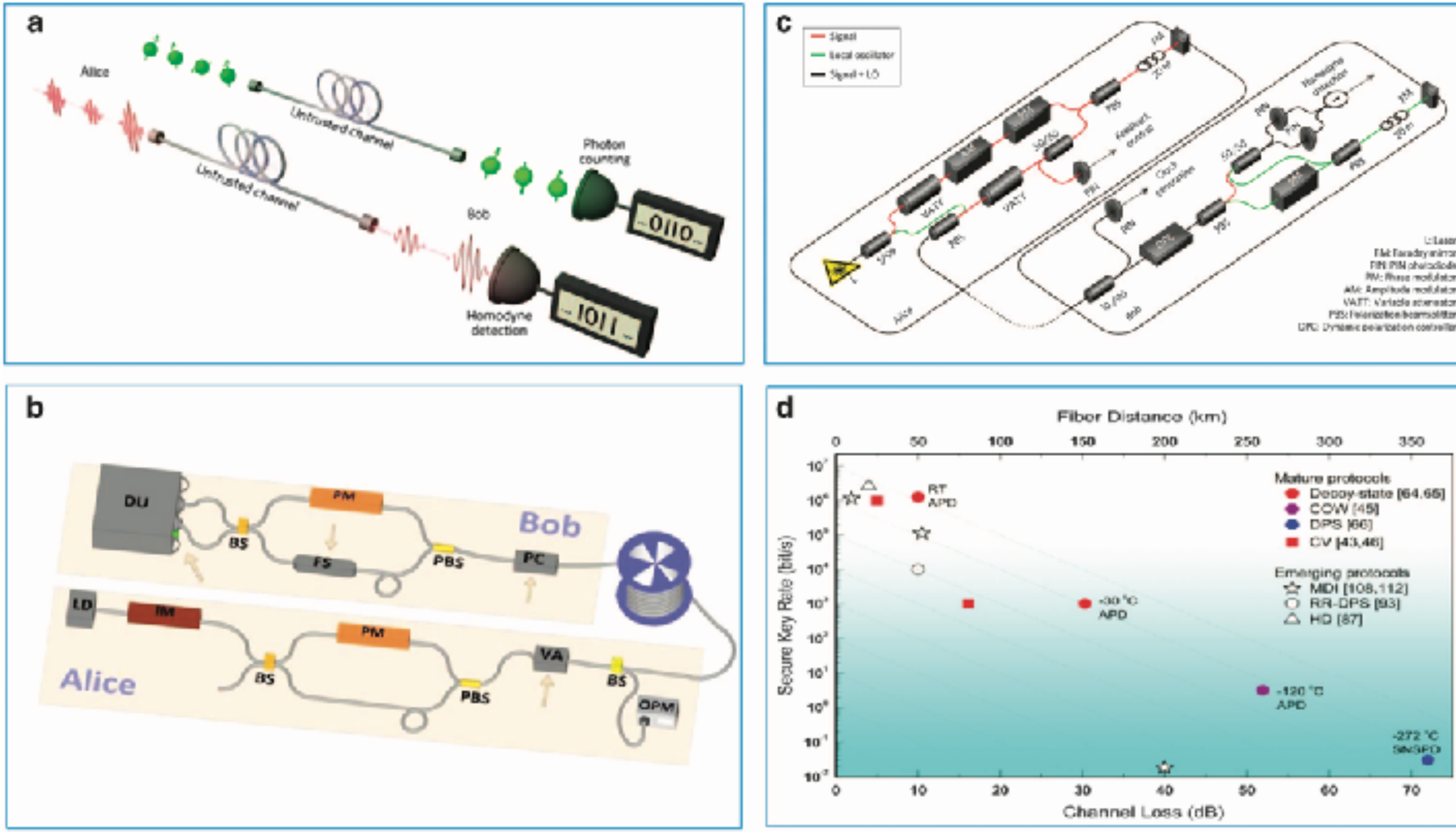
first realization of BB84 protocol, in 1992

320 mm of QKD link



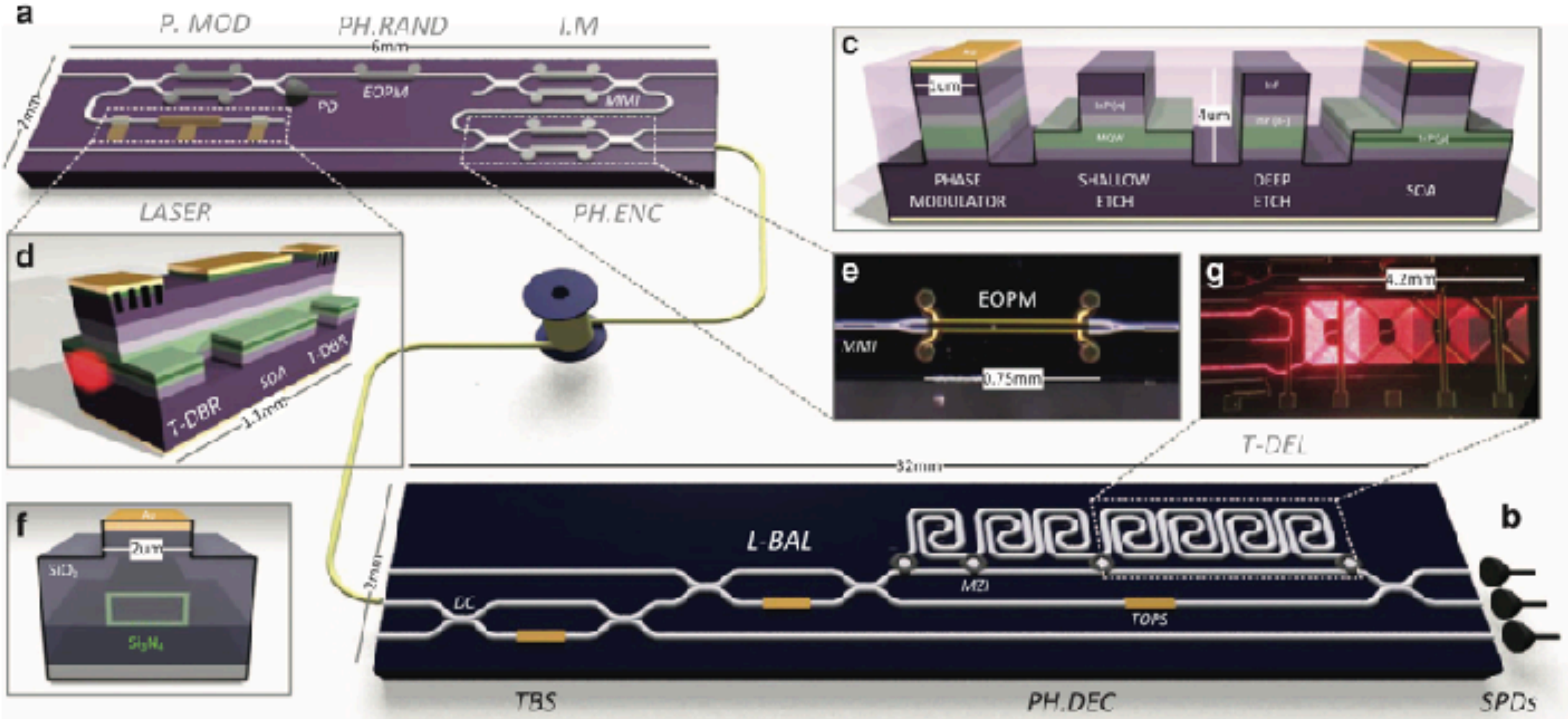
C. Bennett et al. Experimental quantum cryptography. *J. Cryptol.* **5**, 3–28 (1992)

QKD 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

Chinese advanced devices for QKD

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 capacity, 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.

Quantum Safe Service-Mobile Engine

QKChr

Quantum keys Charger (QKChr) is a filling 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 driver 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

QuantumCTek Security Mobile PhoneA2021H

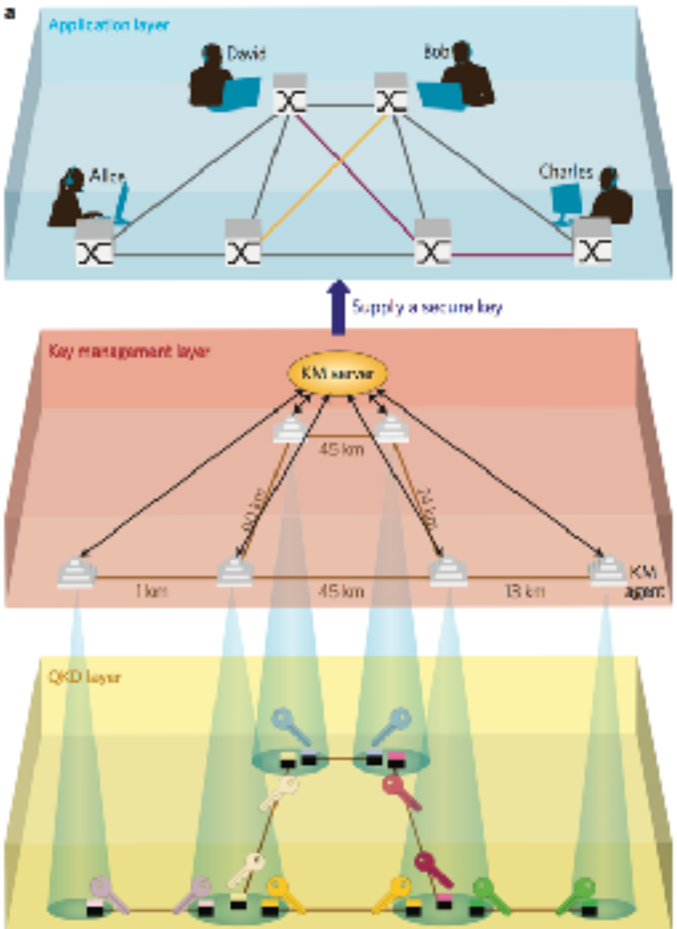
The commercial Quantum security encryption mobile phone-The Quantum Security Version of ZTE AXON 7S,is jointly developed by QuantumCTek and ZTE. The mobile phone is based on the QSS-ME platform and Autonomous secure operating system. Compared with the traditional mobile phone, its unique characteristics and function of quantum secure encryption security operating system has higher application value in the era of information security privacy protection.

Quantum SSL VPN

Quantum SSL VPN product is a high- security quantum security product, combining quantum security communication technology and SSL VPN technology. The product is the world's first quantum SSL VPN launched by QuantumCTek and SANGFOR, with quantum key protection, comprehensive security, fast access and other features.

http://www.quantum-info.com/English/product/ptwo/yidongjiamiyingyongchanpin/

QKD networking



QKD networks have been deployed in the several Countries

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)

Security model of QKD

1. **the security of QKD is measured with respect to a perfect key distribution scheme** in which Alice and Bob share **a true random secret key**.
2. **QKD system is ε-secure** if and only if the probability distribution of an outcome of any measurement performed on the QKD scheme and **the resulting key deviates by at most ε** from that of the perfect key distribution protocol and the perfect key. A typical value for ε is 10^{-10}.
3. **QKD is composably secure**: if we have a set of cryptographic protocols with security parameter ε_i, then the security of the whole system is given by $\sum_i \varepsilon_i$.

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

QKD device hacking

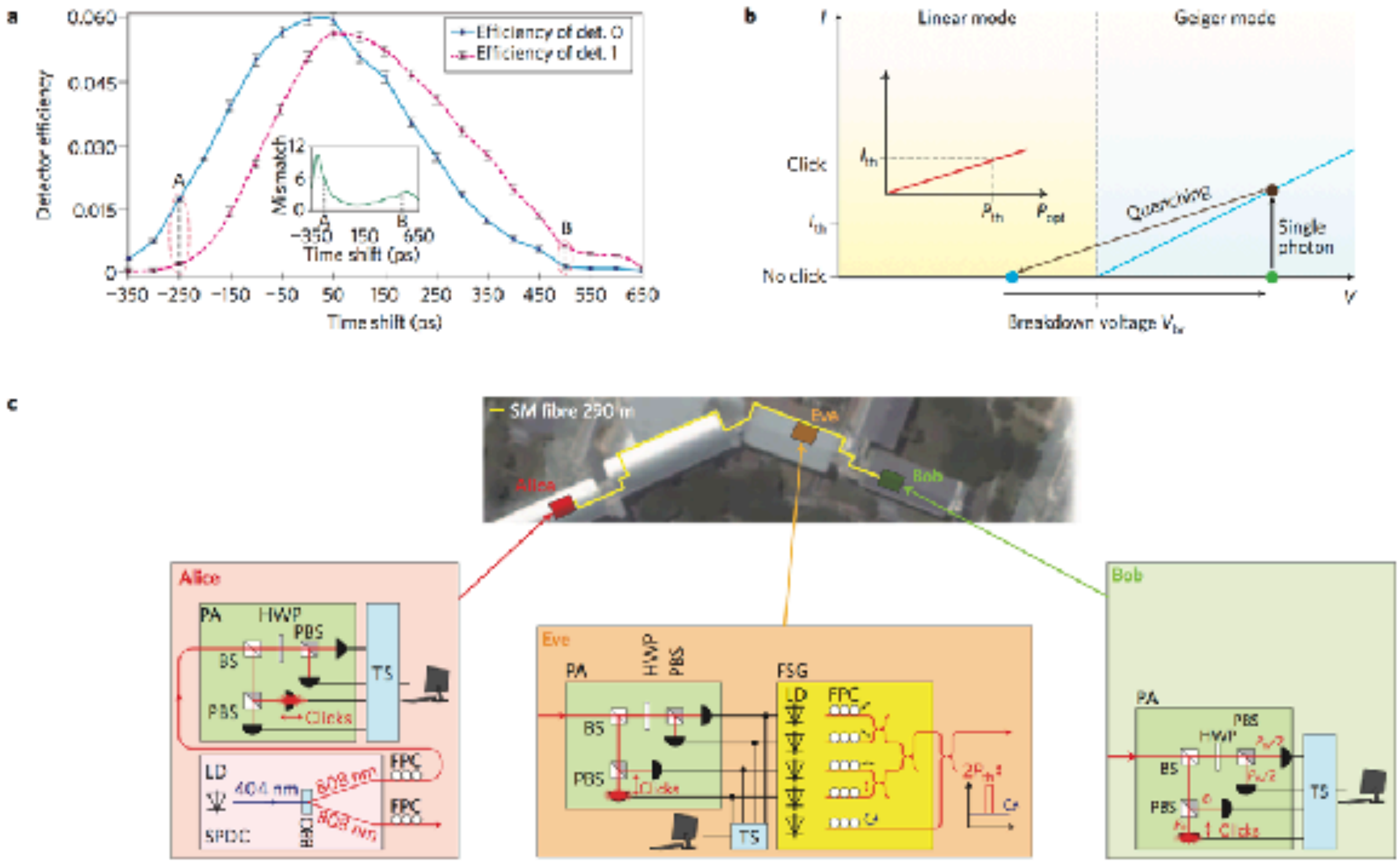
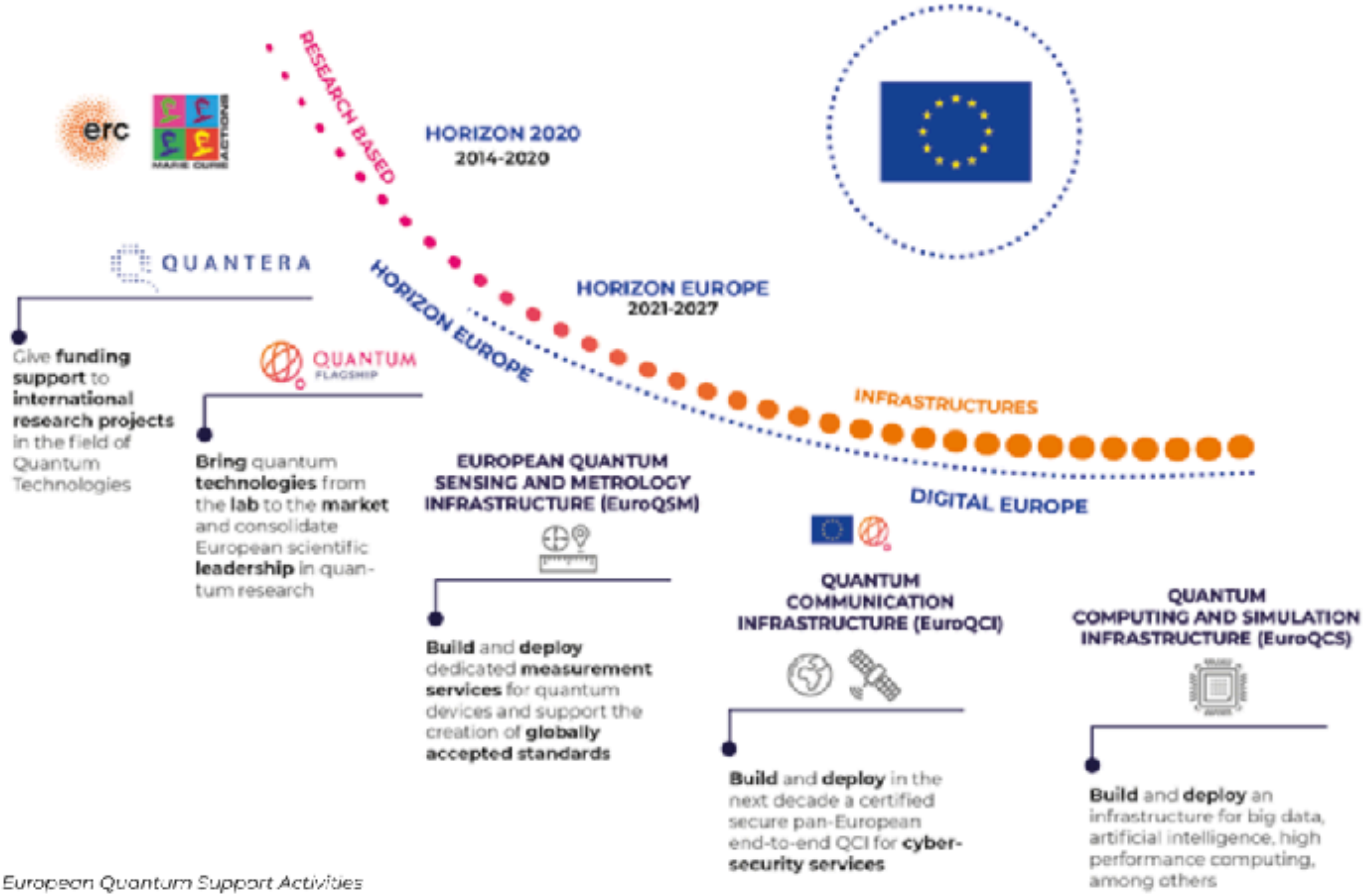


Figure 4 | Examples of quantum hacking. a, Experimentally measured detection efficiency mismatch between two detectors from a commercial QKD system versus time shifts[25]. Eve could exploit this to perform a time-shift attack[75]; that is, she could shift the arrival time of each signal such that one 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)



European Quantum Support Activities

https://qt.eu/app/uploads/2020/04/Strategic_Research-_Agenda_d_FINAL.pdf

strong growth forecasted

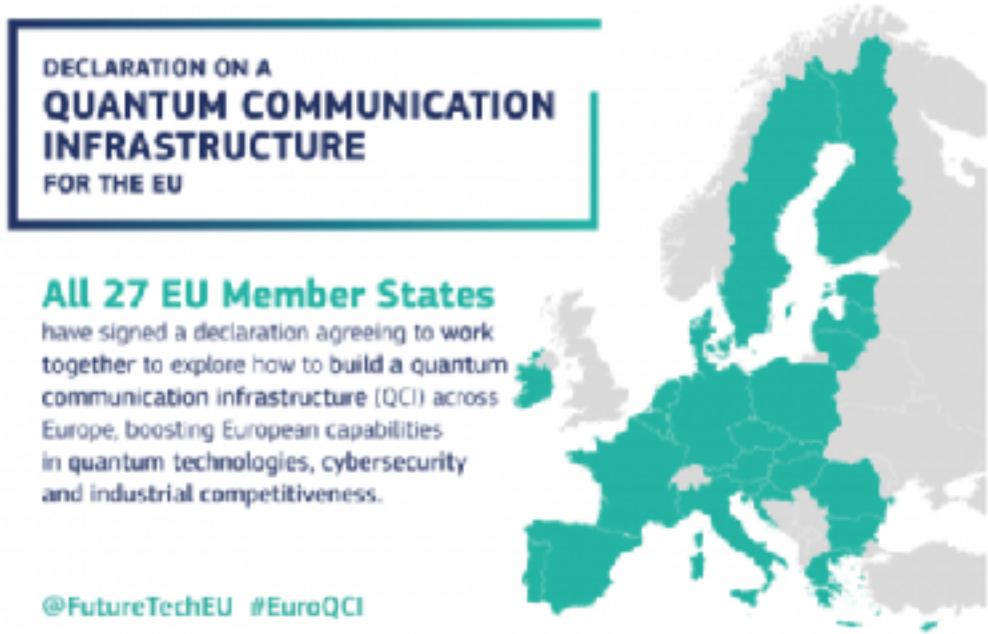
- **QKD market: the target clients are the government, financial companies, medical data protection, datacenter secure communications, corporations, medium-sized business and universities.**

- At the moment, sales of QKD systems appear to be restricted to certain high-end financial systems and classified government communications. In the previous year, Financial segment dominated the market with the share of 37.61%, followed by Government segment and Military & Defense segment, which accounted for the market of 30.90% and 27.16% respectively. Further development requires diversifying into new applications.

- **QKD market size is estimated to grow to $5858.01 million by 2025 from $1712.41 million in 2018, growing at an estimated compound annual growth rate CAGR of 19.21% between 2018 and 2025.** Ambitious plans for QKD networks exist in US (Battelle), Japan (NICT) and China (QuantumCTek).

https://market.biz/report/global-quantum-key-distribution-qkd-market-gm/568521/

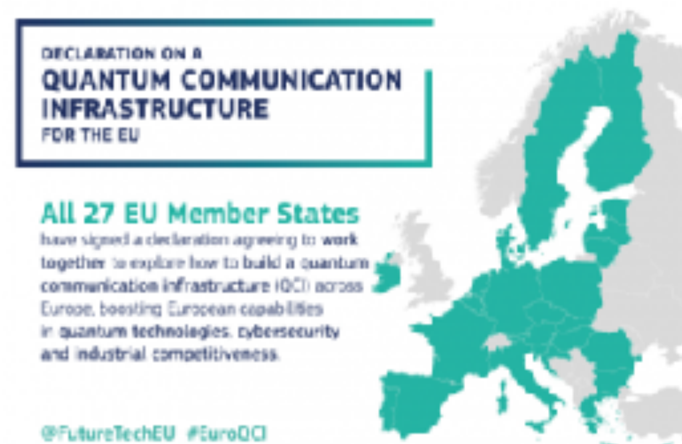
Q-Comms in Europe: fibers and satellites



OpenQKD: all EU QKD testbed

- 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

38 Partners from 13 EU countries



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

standards and space QKD

- standardisation of QKD is ongoing
- the space part is in the development phase
- this will lead to standards to help a global operation

https://www.etsi.org/technologies/quantum-safe-cryptography

QKD with networks - fibers and free-space

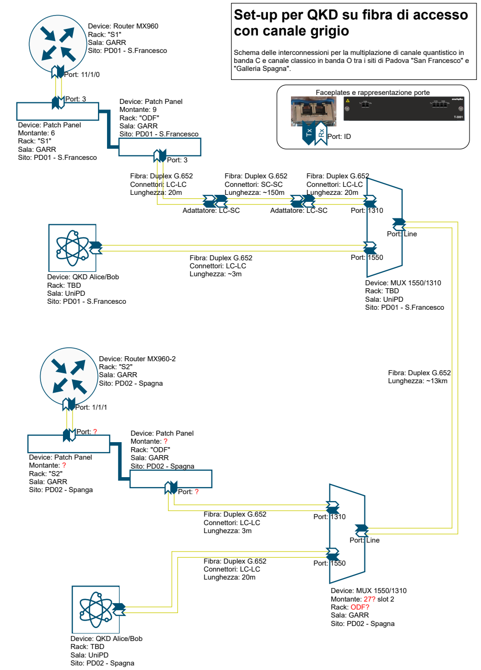
QuantumFuture
The shift in the communication paradigm

PADUA TECH ThinkQUANTUM

Avesani, M. et al. Resource-effective quantum key distribution: a field trial in Padua city center. Opt. Lett. 46, 2848 (2021).

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

Collaboration between QTech-UniPD and GARR QKD on a operative fiber link



Key distribution over existing and live fiber - grey -links

operative since Nov. 5 2021

1 Gbps data traffic and >2 kbs of secure key

pave the way to secure key distribution for Italy

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

QKD for the largest scale

- the QKD in the Space is developing from a scientific research subject in experimental Quantum Communications, in a phase for demonstrators of different realisations to a technology for supporting cybersecurity at the planetary scale and beyond

- at present, space-QKD is point-to-point, eg. one terminal in orbit an one on the ground, or inter-satellite-links ISL, or two terminals on the ground fed by one orbiter simultaneously

image from: www.esa.int/ESA_Multimedia/Directorates/Observing_the_Earth

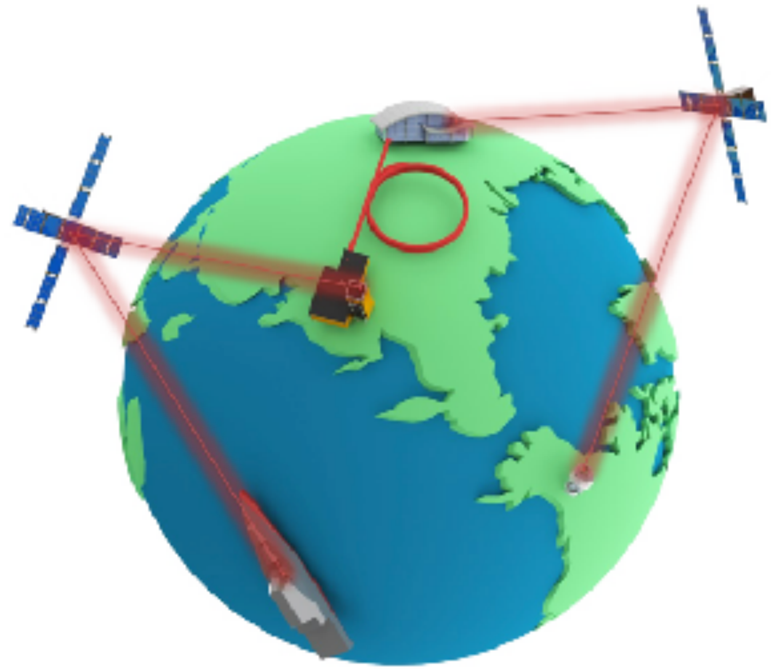
QKD for the largest scale

- one satellite in orbit may connect terminals all over the planet and a constellation of satellites may speed up the mutual connection of two random spots on the ground in the need of a shared secret key
- the satellite design shall envisage a networking use, with versatility of the interlocutors

image from: www.esa.int/ESA_Multimedia/Directorates/Observing_the_Earth

why going in the Space, with QKD?

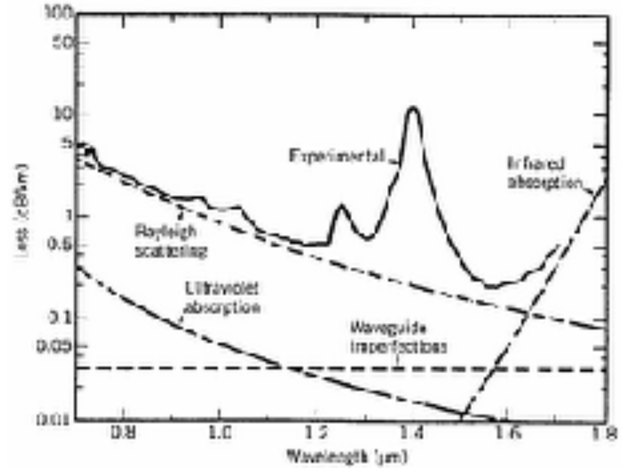
- cybersecurity is a global issue
- even a single Country needs to communicate globally, for reaching embassies or commercial branches
- QKD for inter-governmental communications, eg within EU27 Countries, require the connection of capitals in a range >4000 km and including islands
- mobile terminals require free-space links and ships are not typically at sight from land

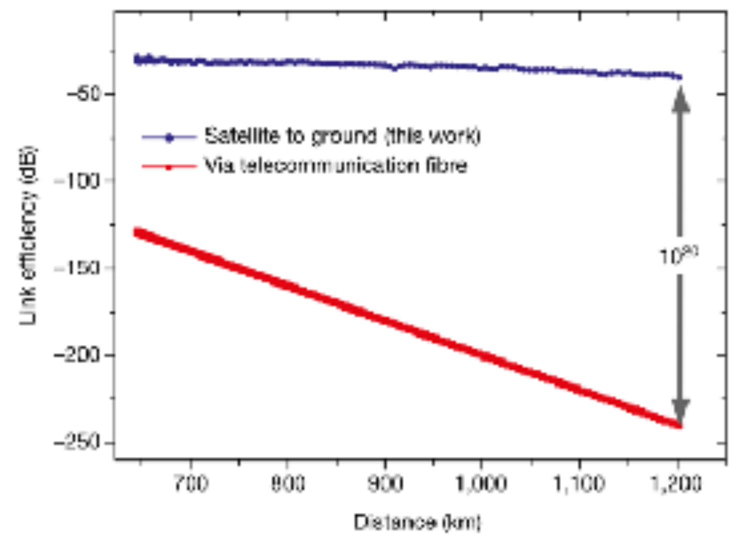


J.S. Sidhu et al. Advances in space quantum communications. IET Quantum Commun. qtc2.12015 (2021)

beyond fiber-based QKD

- propagation along fiber is affected by an exponential attenuation, strongly depended on photon wavelength
- lowest values about 0.15 dB/km are obtained around 1550 nm
- free-space propagation losses, in the far field, scales with the inverse square of the distance
- there is a **crucial advantage in the loss law** when considering planetary scale and when amplifier are not used
- from *Liao et al*. “over a distance of 1,200 km, even with a perfect 10-GHz single-photon source and ideal single-photon detectors with no dark count, transmission through optical fibres would result in only a 1-bit sifted key over six million years”

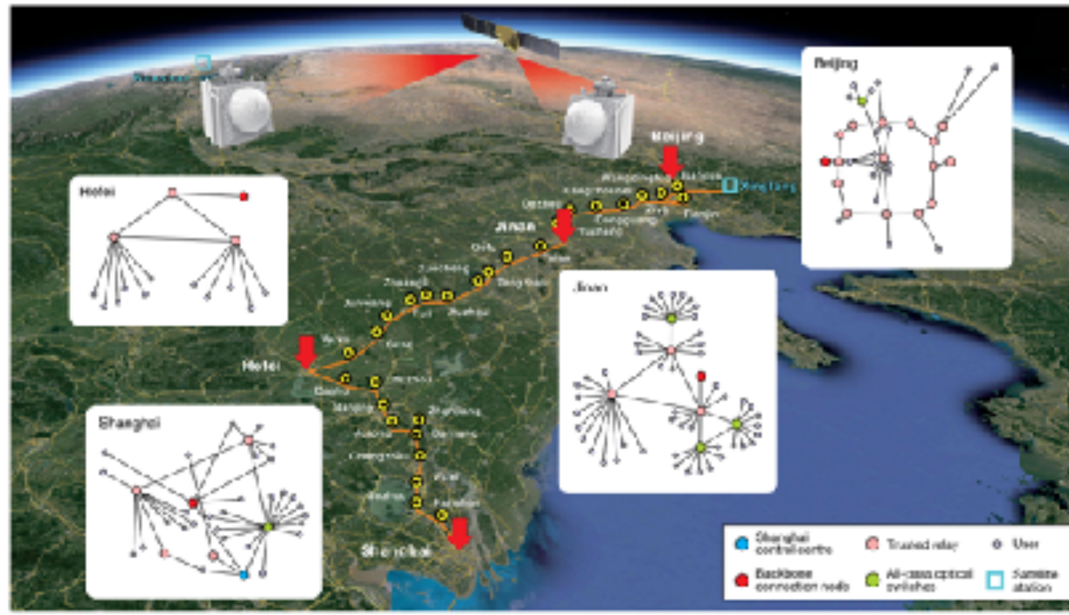




Liao, S.-K. et al. Satellite-to-ground quantum key distribution. Nature 549, 43–47 (2017)

ground and space links for QKD

- fiber links on ground are very pervasive (up to the fiber-to-the-home service)
- they are naturally organized in hierarchy, as dorsal, national, regional, metropolitan and local networks
- satellite terminals are to be integrated on network nodes as well as connecting isolated users



Y.-A. Chen et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature 589, 214–219 (2021).

QKD networking with satellites

The Sat may be a flying

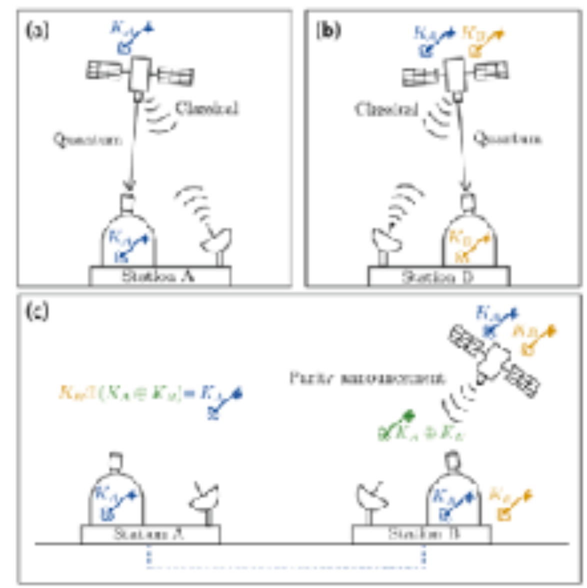
trusted-node or an untrusted one

QKD operations with distinct ground stations to establish independent secret keys with each of them: **sat holds all keys, while the stations only have access to their own keys**.

To enable any pair of stations to share a common key, the satellite combines their respective keys KA and KB and broadcasts their bit-wise parity KA $\oplus$ KB.

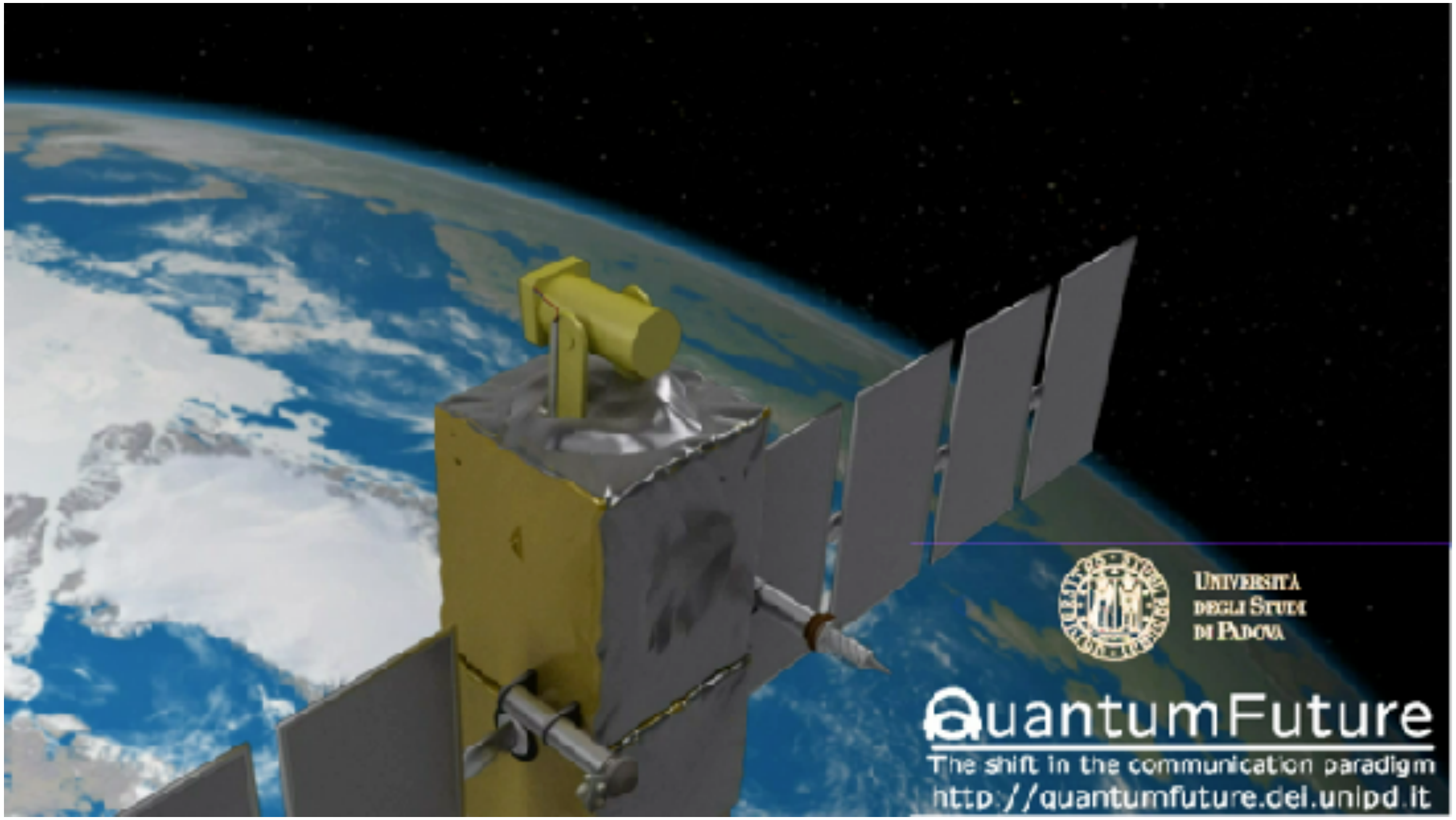
stations can retrieve each other's keys because KA $\oplus$ (KA $\oplus$ KB)= KB and KB $\oplus$ (KA $\oplus$ KB)= KA.

Original keys are independent secret strings, their bit-wise parity is just a uniformly random string, (no useful information to potential eavesdroppers revealed)



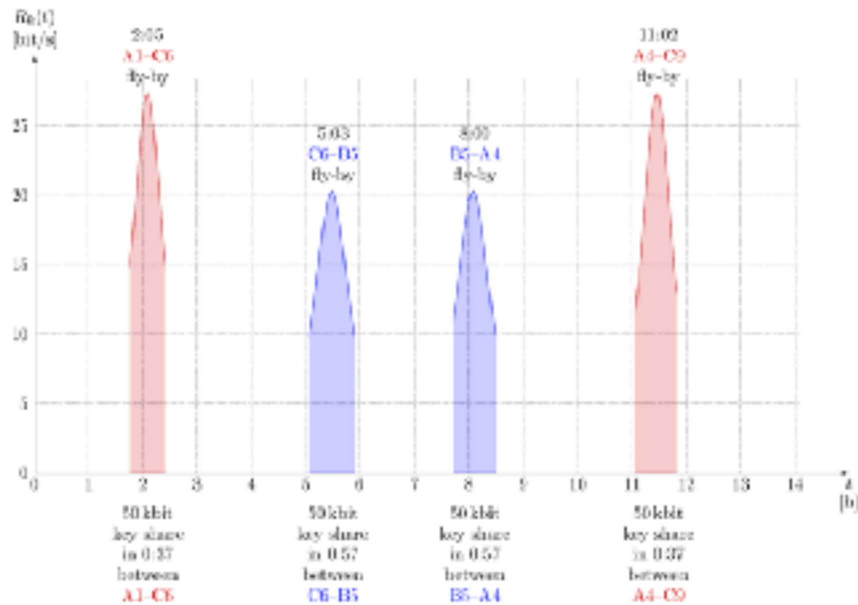
H-K Lo et al. Secure quantum key distribution Nat. Phot. 8 595 (2014)

the intersat QKD concept

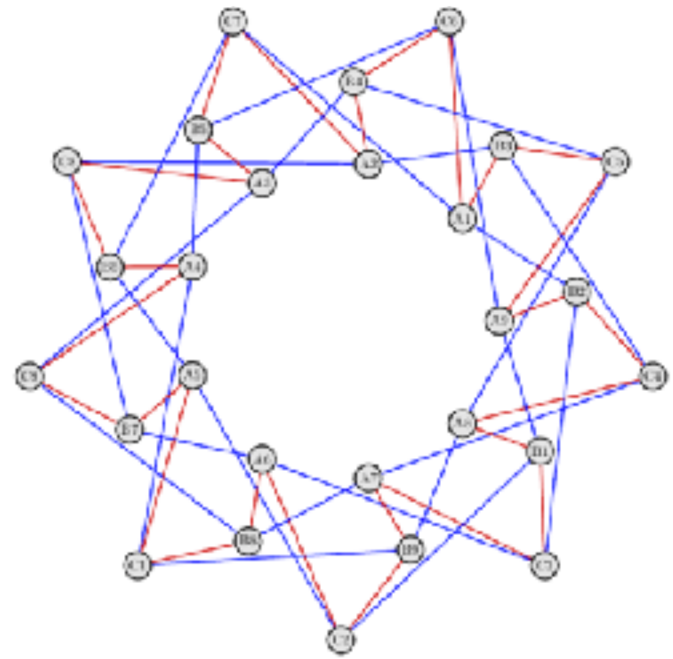


Project ESA Q-GNSS 2011-2015
F. Gerlin et al. Proc. 2013 Int. Conf. Localization and GNSS

the intersat QKD concept

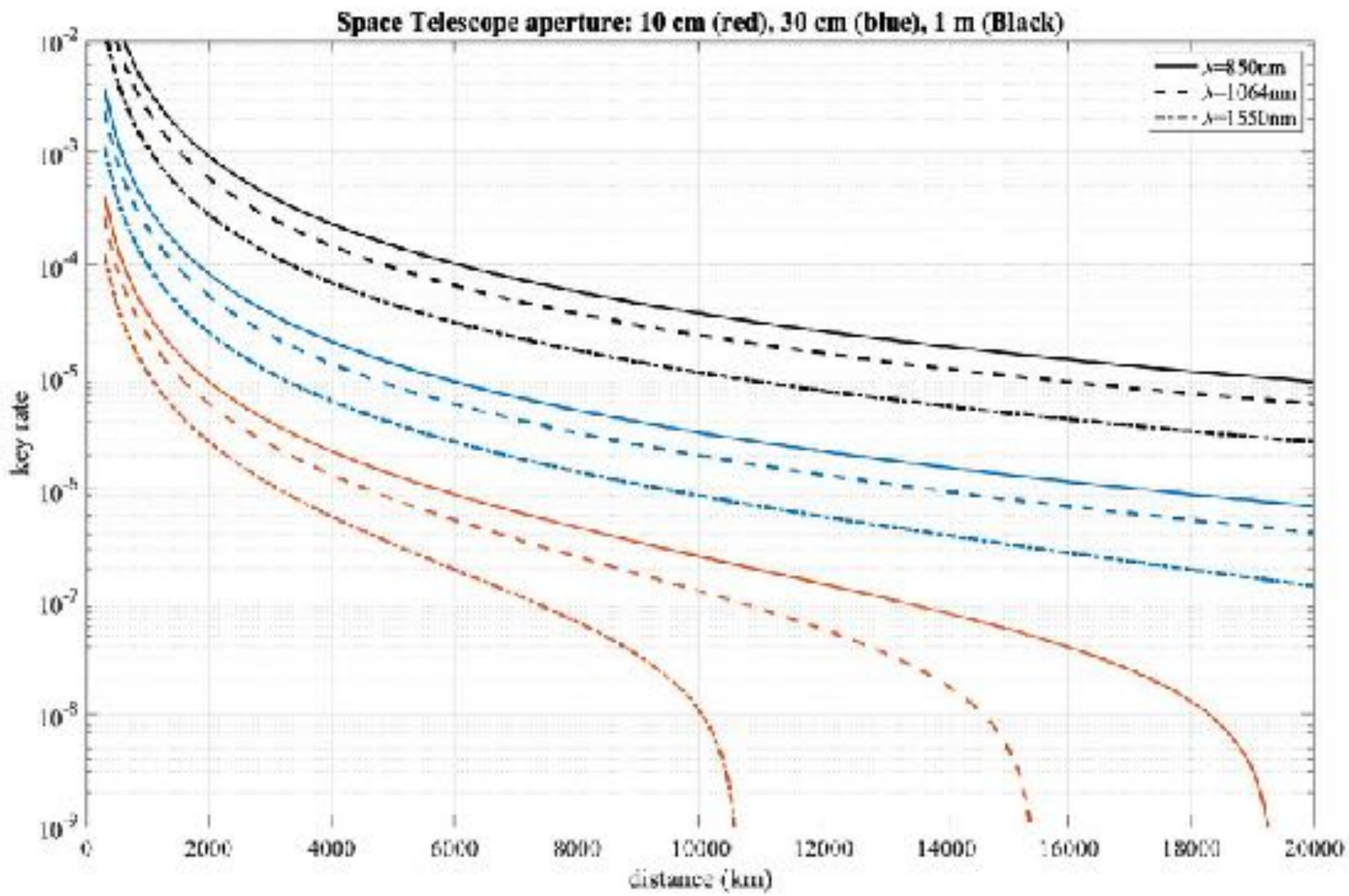


Sequence of four hops to share secret key material between satellite A1 and C9, through C6, B5, A4.



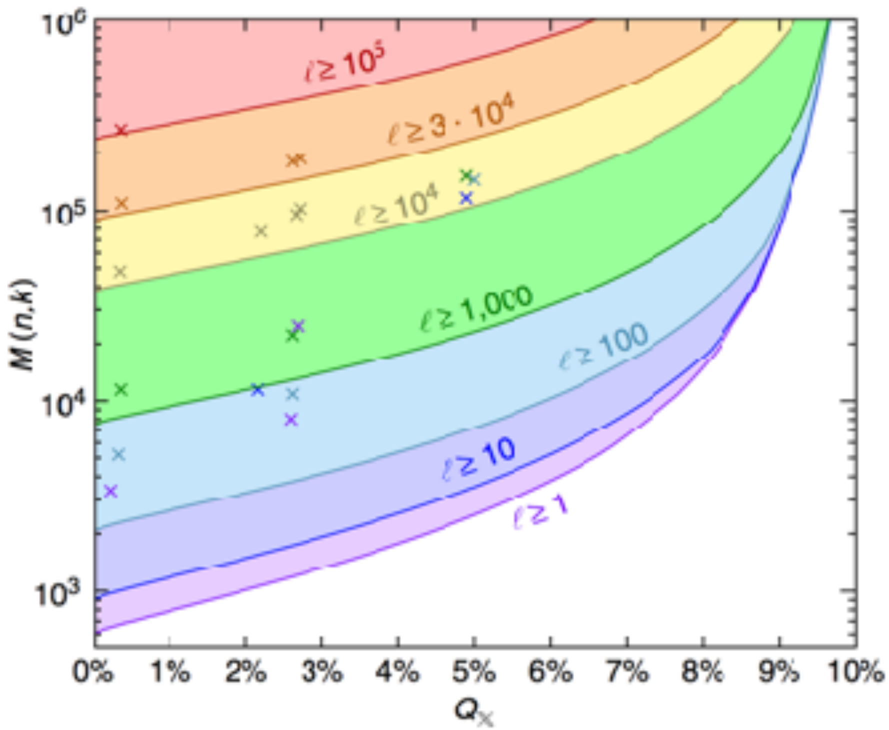
Project ESA Q-GNSS 2011-2015
F. Gerlin et al. Proc. 2013 Int. Conf. Localization and GNSS

QKD rate
50 cm ground telescope as receiver



Map to assess the qubit needed for a given key at a QBER value

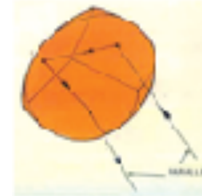
For ***finite length with noise***, the key rate shall be designed according to satellite type of orbit and losses.

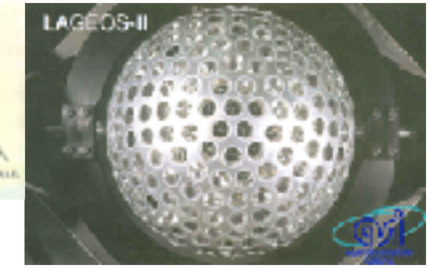


The **minimum number of received bits M(n,k) needed to obtain a key of a given length ℓ** (as labelled on each curve) versus the QBER - Q_X.

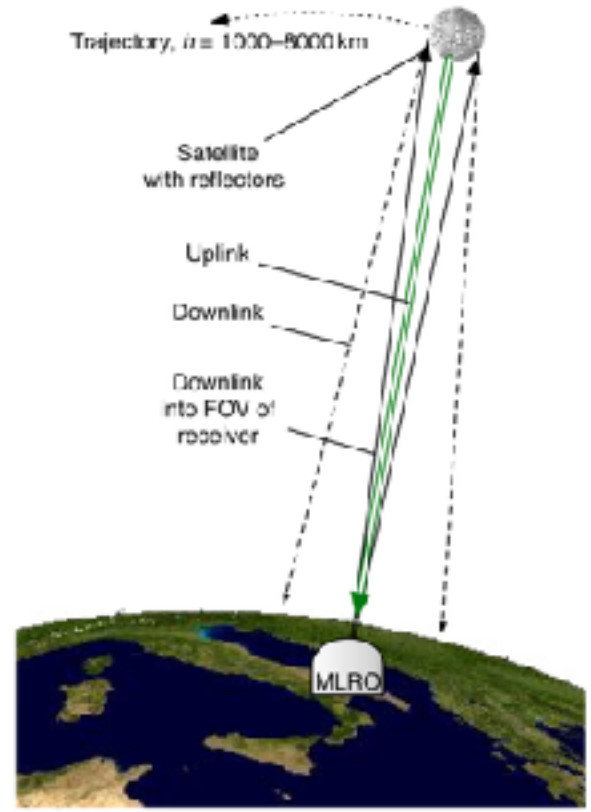
Bacco et al. ***Experimental quantum key distribution with finite-key security analysis for noisy channels*** Nature Communications **4** 2363(2013).

demonstrating the downlink





- exploiting retroreflectors on satellite (often available)
- Return peak of 5 cps was observed at D=0 above the background.
- In the downlink channel, μ = 0.4, attesting the single-photon regime
- Total losses are of -157 dB.



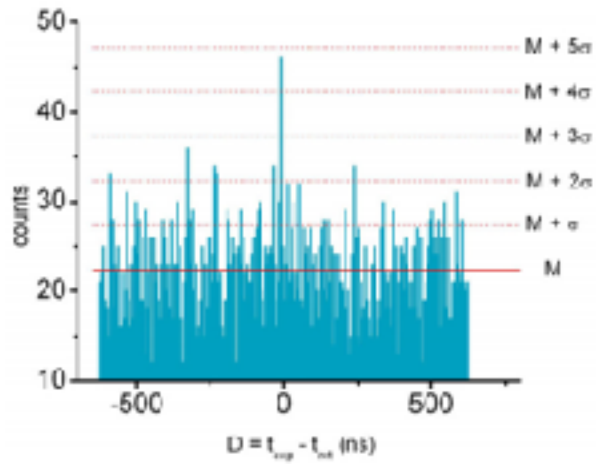


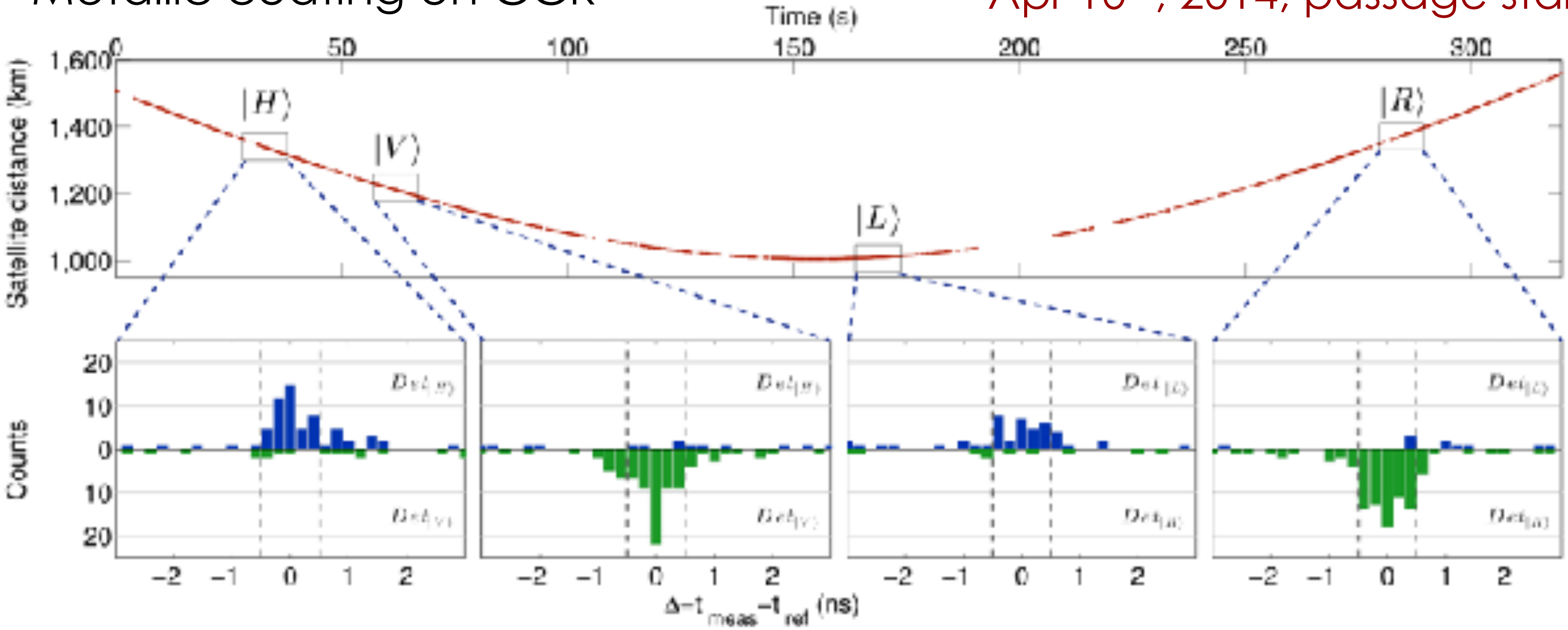
Figure 3. Histogram of the differences D between expected and observed detections for Ajisai satellite. The peak of the histogram is centered at $D = t_{exp} - t_{ret} = 0$ ns, as expected, and is larger than the mean value of the background counts by 4.5 standard deviations. The bin size is $\Delta t = 5$ ns.

P. Villoresi et al. Experimental verification of the feasibility of a quantum channel between space and Earth. New J. Phys. 10, 033038 (2008)

first results: 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 10th, 2014, passage start 4:40 am



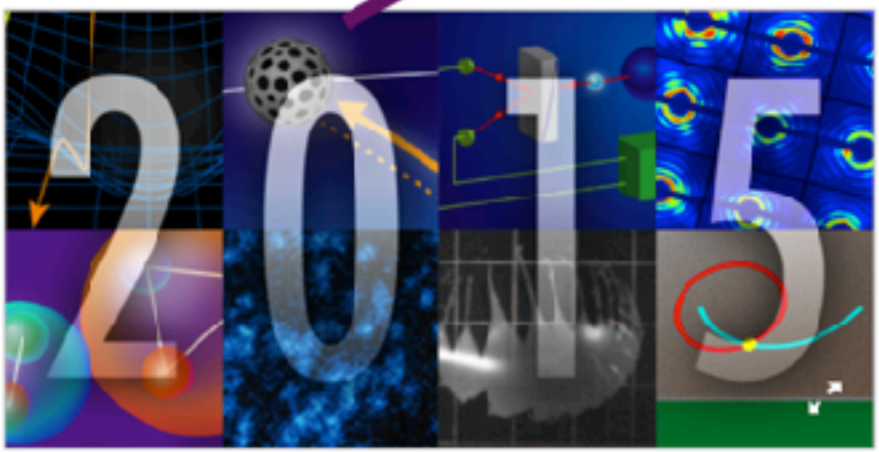
Return rate 147 cps
10^4 bits/passage

G. Vallone et al, ***Experimental Satellite Quantum Communications***, Phys. Rev. Lett. **115** 040502, 2015

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

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.

SCIENZA Grande scoperta pubblicata sulla «Physical Review Letters»

Parleremo coi marziani E lo faremo in italiano

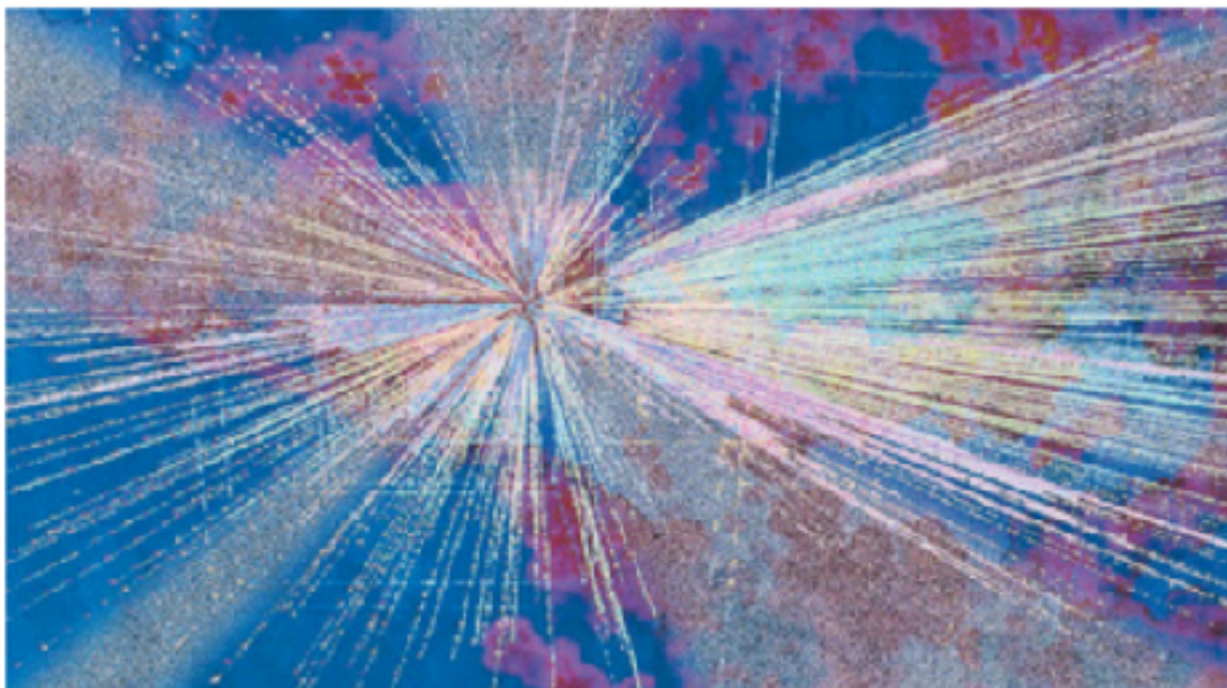
Si apre una nuova frontiera nella comunicazione quantistica grazie ai nostri scienziati: i dati viaggiano per 1700 km su particelle di luce

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

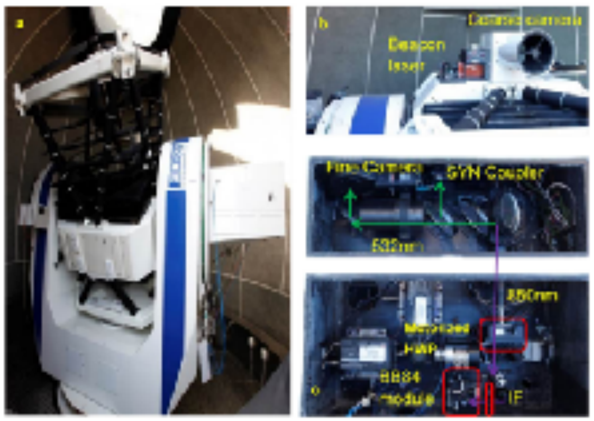
Tra Asi, ateneo di Padova e Centro Geodesia di Matera

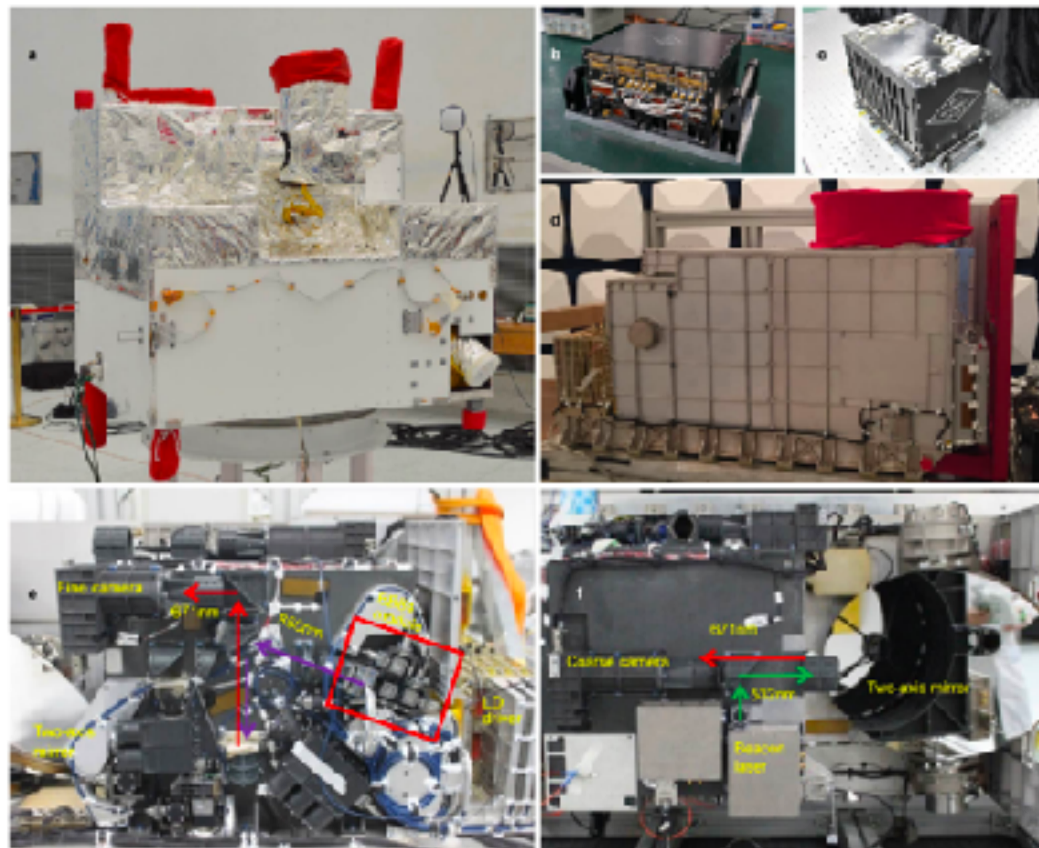


TRA SCIENZA E FANTASCIENZA Primo messaggio quantistico al mondo via satellite

the multipurpose CAS-Micius mission

- launched on 16 August 2016 by a Long March 2D rocket from the Jiuquan Satellite Launch Centre, China





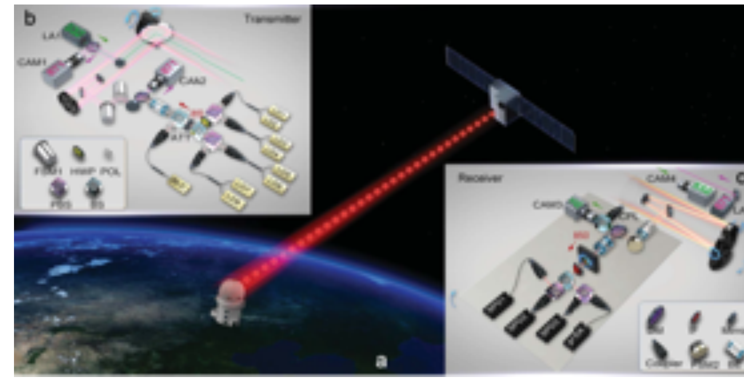
Extended Data Figure 2 | The Micius satellite and the payloads. a, A full view of the Micius satellite before being assembled into the rocket. b, The experimental control box. c, The APT control box. d, The optical transmitter. e, Left side view of the optical transmitter optics head. f, Top side view of the optical transmitter optics head.

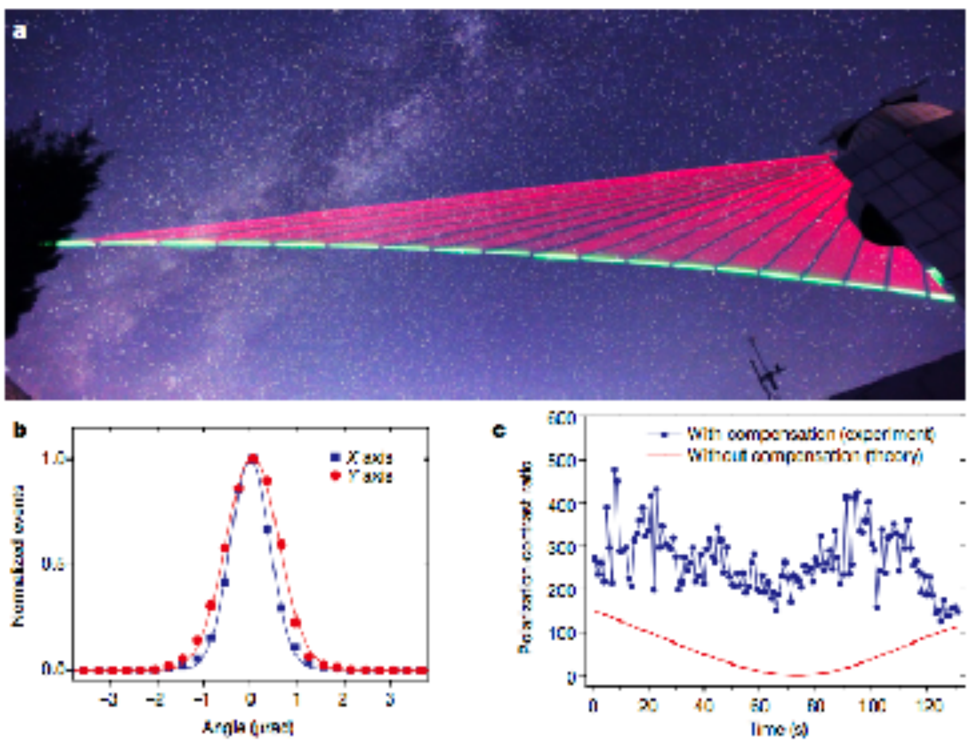
Satellite-to-ground quantum key distribution

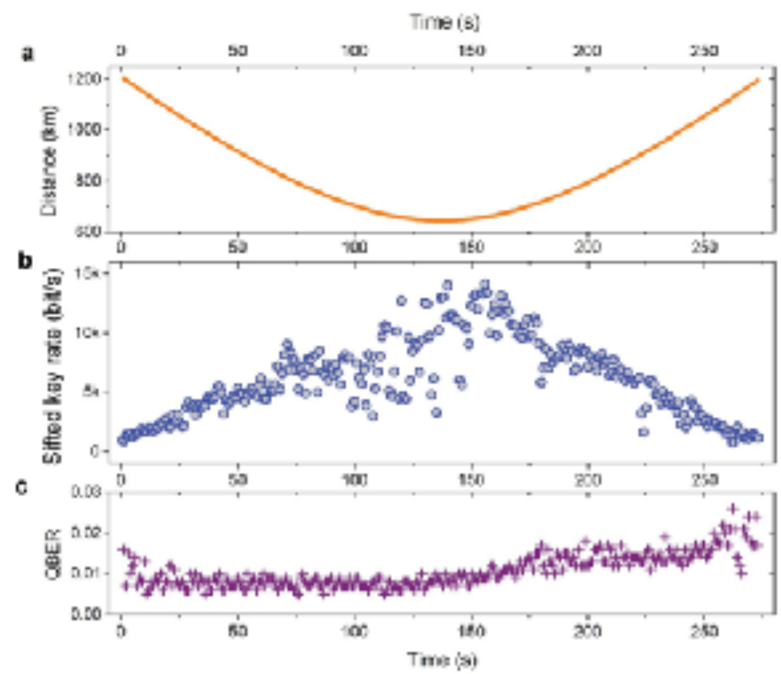
Sheng-Kai Liao[1,2], Wen-Qi Cai[1,2], Wei-Yue Liu[1,2], Liang Zhang[2,3], Yang Li[1,2], Ji-Gang Ren[1,2], Juan Yin[1,2], Qi Shen[1,2], Yuan Cao[1,2], Zheng-Ping Li[1,2], Feng-Zhi Li[1,2], Xia-Wei Chen[1,2], Li-Hua Sun[1,2], Jian-Jun Jia[3], Jin-Cai Wu[3], Xiao-Jun Jiang[4], Jian-Feng Wang[4], Yong-Mei Huang[5], Qiang Wang[5], Yi-Lin Zhou[6], Lei Deng[6], Tao Xi[7], Lu Ma[8], Tai Hu[9], Qiang Zhang[1,2], Yu-Ao Chen[1,2], Nai-Le Liu[1,2], Xiang-Bin Wang[2], Zhen-Cai Zhu[6], Chao-Yang Lu[1,2], Rong Shu[2,3], Cheng-Zhi Peng[1,2], Jian-Yu Wang[2,3] & Jian-Wei Pan[1,2]

decoy–state QKD with a kilo-hertz key rate over a distance of 1200 km.

This key rate is around 20 orders of magnitudes greater than that expected using an optical fibre of the same length







S-K Liao et al, Satellite-to-ground quantum key distribution Nature 549, 43 (2017)

Satellite-Relayed Intercontinental Quantum Network

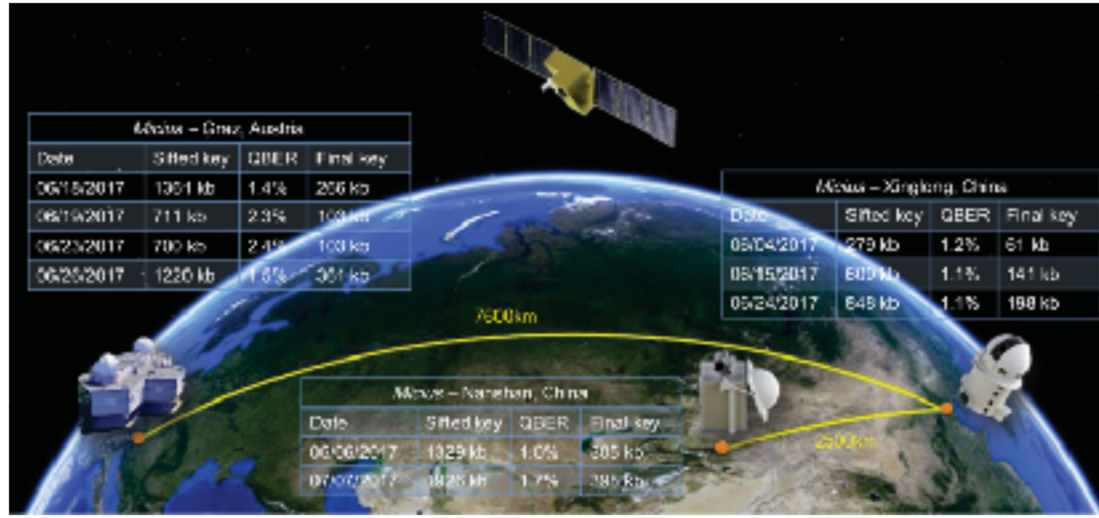
Micius satellite as a trusted relay to distribute secure keys between multiple distant locations in China and Europe

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, we establish a 100 kB secure key between Xinglong and Graz.

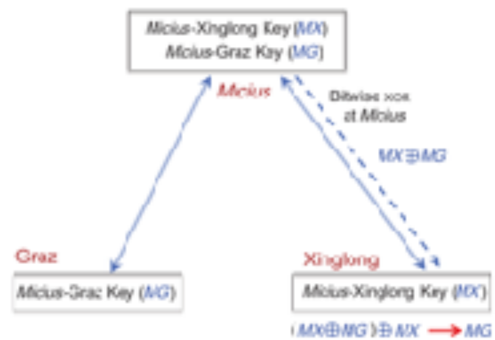
Video conference with AES-128 protocol that refreshed the 128-bit seed keys every second.

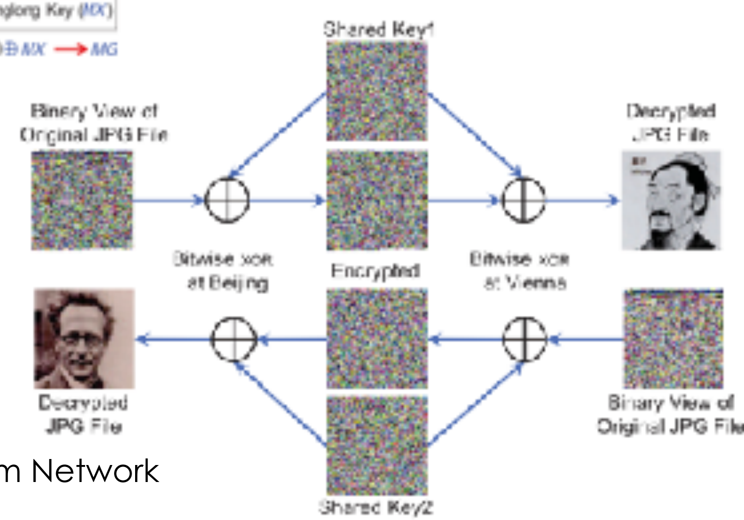


Micius – Graz, Austria			
Date	Sifted key	QBER	Final key
06/15/2017	1361 kb	1.4%	206 kb
06/19/2017	711 kb	2.3%	[illegible]
06/23/2017	700 kb	2.4%	103 kb
06/25/2017	1220 kb	1.8%	361 kb

Micius – Xinglong, China			
Date	Sifted key	QBER	Final key
05/04/2017	279 kb	1.2%	61 kb
05/15/2017	609 kb	1.1%	141 kb
05/24/2017	645 kb	1.1%	188 kb

Micius – Nanshan, China			
Date	Sifted key	QBER	Final key
06/06/2017	1329 kb	1.0%	305 kb
07/07/2017	1828 kb	1.7%	285 kb



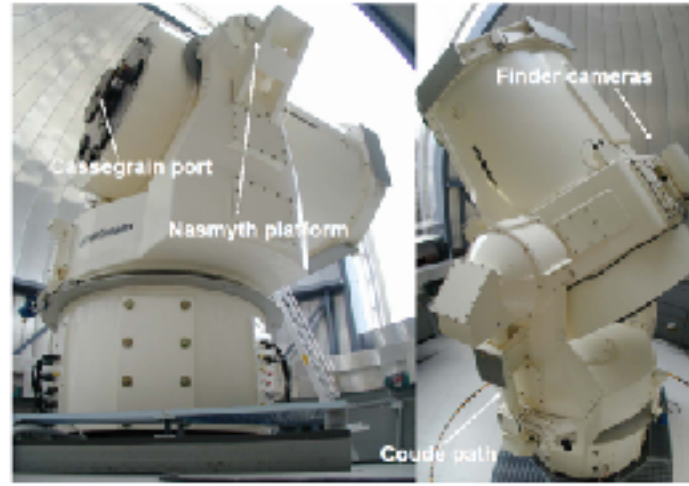


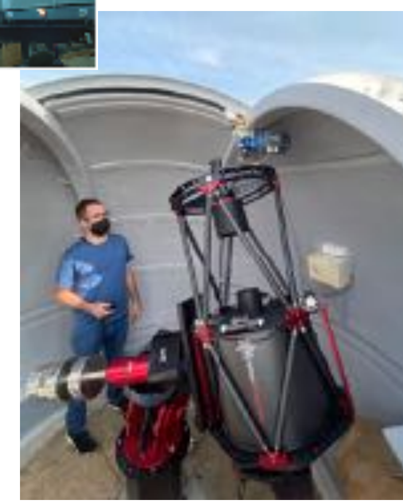
S-K Liao et al, Satellite-Relayed Intercontinental Quantum Network Phys. Rev. Lett. 120, 030501 (2018)

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

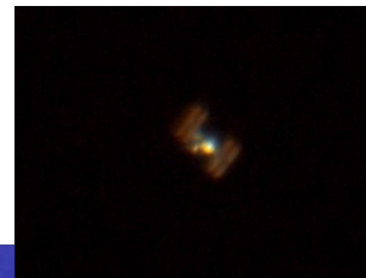


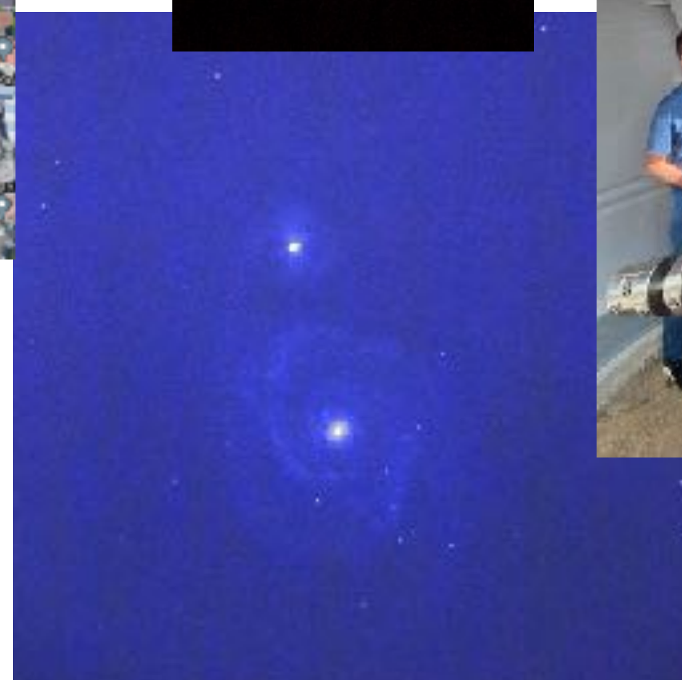


J. S. Sidhu et al. Advances in space quantum communications. IET Quantum Commun. qtc2.12015 (2021)

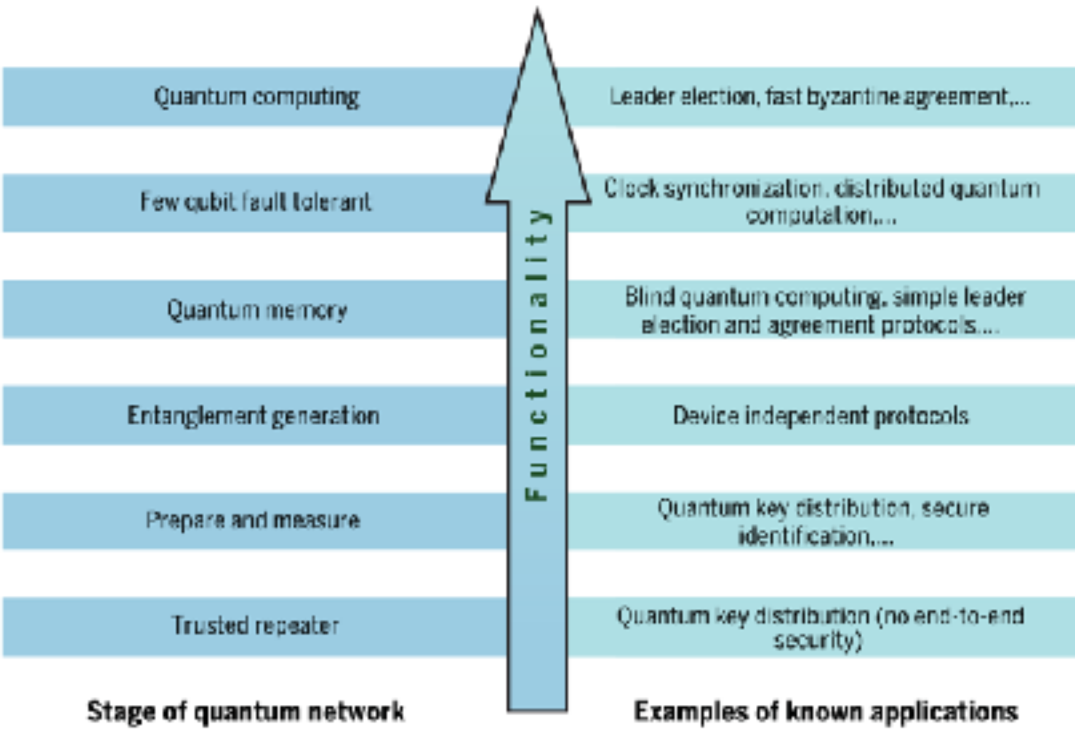
QuantumFuture GaliQeye
urban receiver for Space QKD @ UniPD

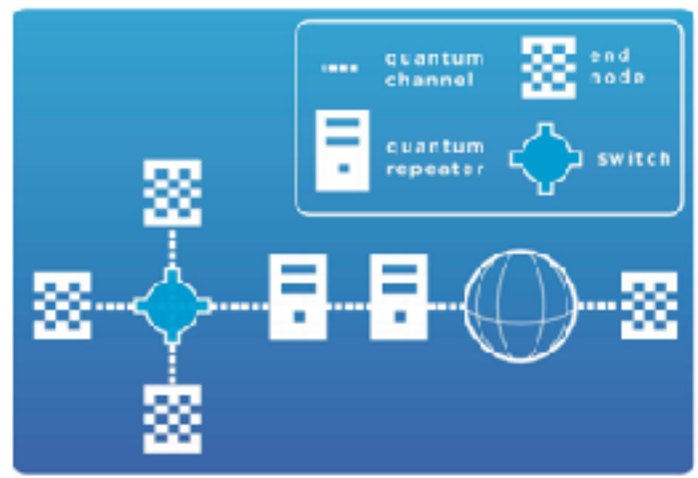
- 40 cm - class telescope
- wide wavelength range and protocols





roadmap to the quantum internet





Wehner et al., *Quantum internet: A vision for the road ahead* Science 362, 9288 (2018)

Conclusioni su Quantum Communications

- il livello di maturità è tale da poter spingere sul trasferimento tecnologico con applicazioni di cybersecurity
- le reti di comunicazione svolgono un ruolo essenziale
- le sperimentazioni del GARR sono già in atto con successo
- l'estensione a protocolli più avanzati richiede un intenso sforzo di ricerca di base che nelle Università italiane ha conoscenze, laboratori e nuove menti da formare
- ci sono importanti opportunità di cooperazione a tutti i livelli per far progredire la conoscenza e trasferirla alle applicazioni
- il PNRR può fare la differenza!

pathway to new science

D. Rideout et al. Fundamental quantum optics experiments conceivable with satellites—reaching relativistic distances and velocities. Class. Quantum Gravity 29, 224011 (2012).
NASA L. Mazzarella et al. Deep Space Quantum Link (DSQL) mission concept Proc. SPIE 11835, 118350J (2021)
J. S. Sidhu et al. Advances in space quantum communications. IET Quantum Commun. qtc2.12015 (2021)

QuantumFuture on Space QComms and QRNG

FACULTY

P. Villoresi

G. Vallone

RtdA

F. Vedovato

POST-DOC

C. Agnesi

M. Avesani

L. Calderaro

A. Stanco

PhD

A. Scriminich

G. Foletto

F. Picciariello

F. Santagiustina

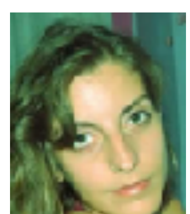
F. Berra

T. Bertapelle

D. Scalcon

E. Bazzani

M. Padovan



E. Karakosta

paolo.villoresi@unipd.it
quantumfuture.dei.unipd.it
qtech.unipd.it
www.thinkquantum.com