DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES

Satellite-based quantum communication

Space communication

May 15, 2023

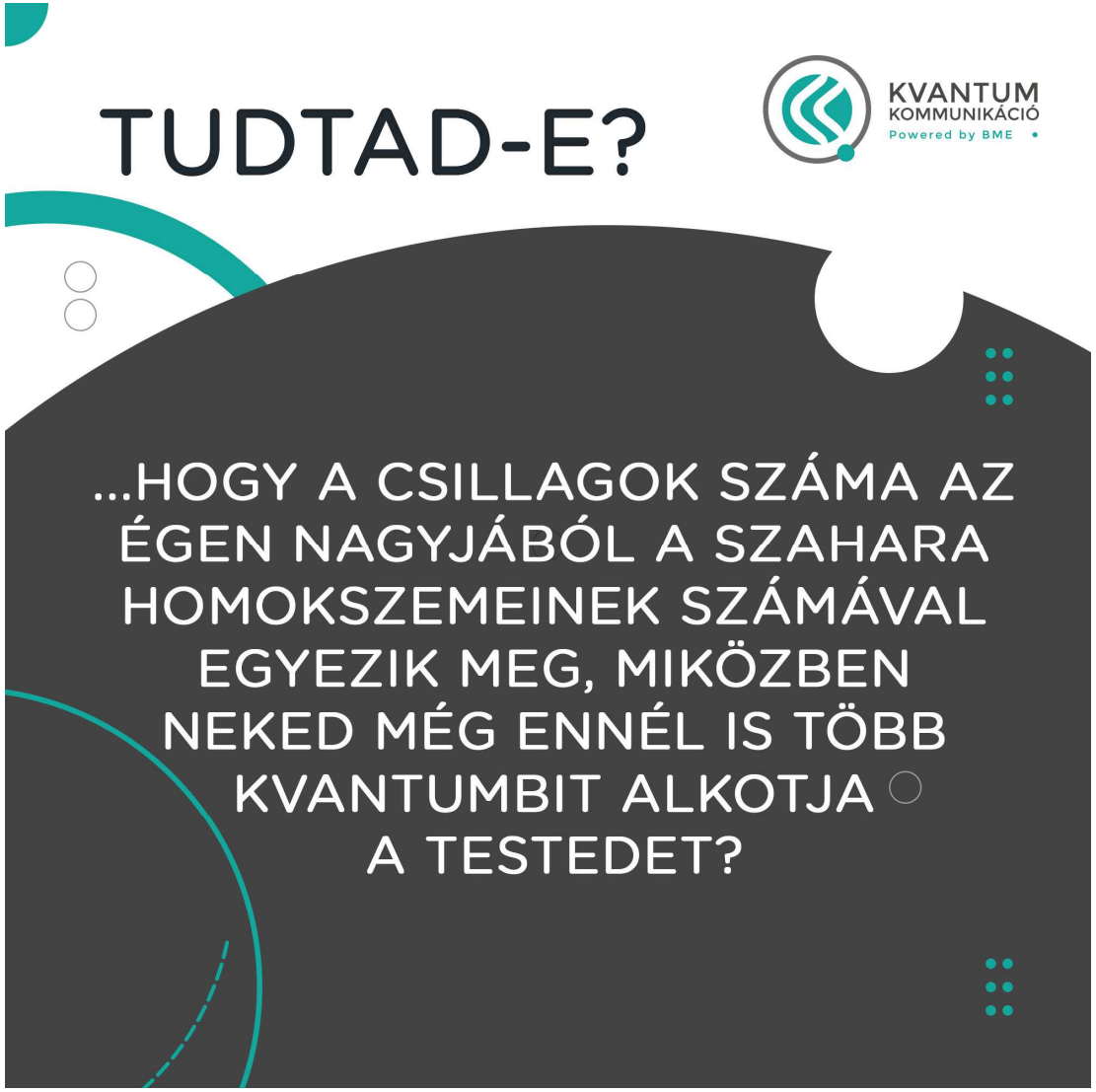
László Bacsárdi, PhD

Department of Networked Systems and Services
Budapest University of Technology and Economics
bacsardi@hit.bme.hu

MŰEGYETEM 1782


HEY, SCHRÖDINGER. WHAT'S IN THE BOX?
MY CAT.
OH. IS IT ALIVE OR DEAD?
YES.
2011© www.ALittleWhiteNoise.com

FACEBOOK.COM/KVANTUMKOMMUNIKACIO
LINKEDIN.COM/COMPANY/KVANTUMKOMMUNIKACIO



QUANTUM FLAGSHIP

Discover About Newsroom

Stay tuned

The future is Quantum.

The Second Quantum Revolution is unfolding now, exploiting the enormous advancements in our ability to detect and manipulate single quantum objects. The Quantum Flagship is driving this revolution in Europe.

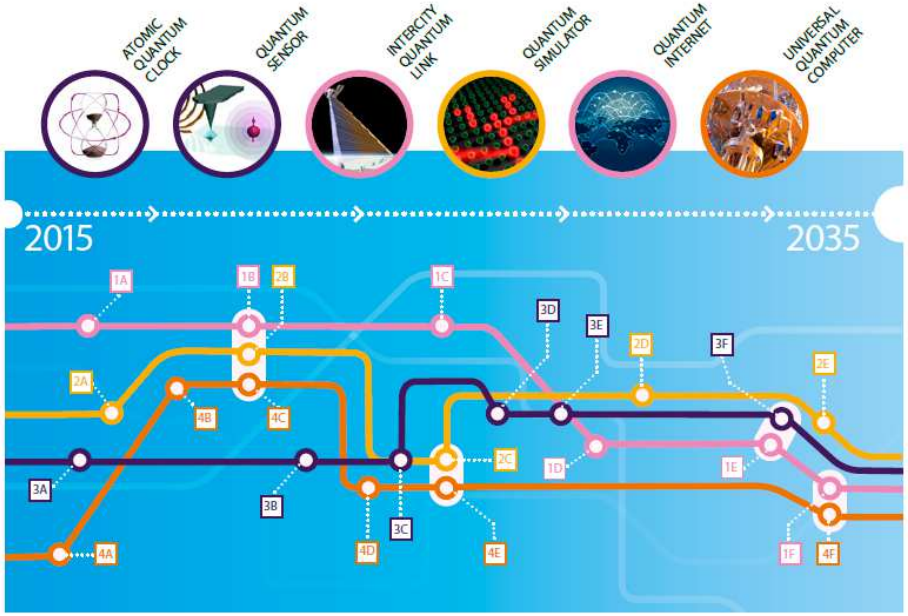
LEARN MORE

Quantum Manifesto

A New Era of Technology

May 2016

Quantum Technologies Timeline



1. Communication	2. Simulators	3. Sensors	4. Computers
0 – 5 years			
A Core technology of quantum repeaters	A Simulator of motion of electrons in materials	A Quantum sensors for niche applications (incl. gravity and magnetic sensors for health care, geosurvey and security)	A Operation of a logical qubit protected by error correction or topologically
B Secure point-to-point quantum links	B New algorithms for quantum simulators and networks	B More precise atomic clocks for synchronisation of future smart networks, incl. energy grids	B New algorithms for quantum computers
			C Small quantum processor executing technologically relevant algorithms
5 – 10 years			
C Quantum networks between distant cities	C Development and design of new complex materials	C Quantum sensors for larger volume applications including automotive, construction	D Solving chemistry and materials science problems with special purpose quantum computer > 100 physical qubit
D Quantum credit cards	D Versatile simulator of quantum magnetism and electricity	D Handheld quantum navigation devices	
> 10 years			
E Quantum repeaters with cryptography and eavesdropping detection	E Simulators of quantum dynamics and chemical reaction mechanisms to support drug design	E Gravity imaging devices based on gravity sensors	E Integration of quantum circuit and cryogenic classical control hardware
F Secure Europe-wide internet merging quantum and classical communication		F Integrate quantum sensors with consumer applications including mobile devices	F General purpose quantum computers exceed computational power of classical computers

Atomic quantum clocks can be synchronised with GPS to provide very high levels of timing stability and traceability, even in hostile environments where GPS is unavailable or denied. These timing solutions can be useful within future smart networks, for instance for the synchronization of energy grids, as well as in telecoms, broadcasting, energy and security.

Quantum sensors that exploit quantum superposition and/or entanglement to achieve a higher sensitivity and resolution will be purchased and used by companies and public institutions for demanding construction projects; for instance, to measure voids under the ground and to detect mineral deposits or legacy infrastructure. They will also be used to provide non-invasive point-of-care diagnosis.

A secure **intercity quantum link** between a number of European capitals will allow transmission of highly sensitive data without any risk of interception. It may contain ground or satellite-based protected nodes derived from the development of trusted nodes and quantum repeaters.

Quantum simulators can be constructed for the special purpose of simulating materials or chemical reactions. Simulation allows new processes or properties to be explored before the material exists, as a tool to design new materials that are needed in multiple sectors, such as energy or transport.

A global **quantum-safe communication network** – a quantum internet combining quantum with classical information and encryption – offers security for internet transactions against the threat of a quantum computer breaking purely classical encryption schemes.

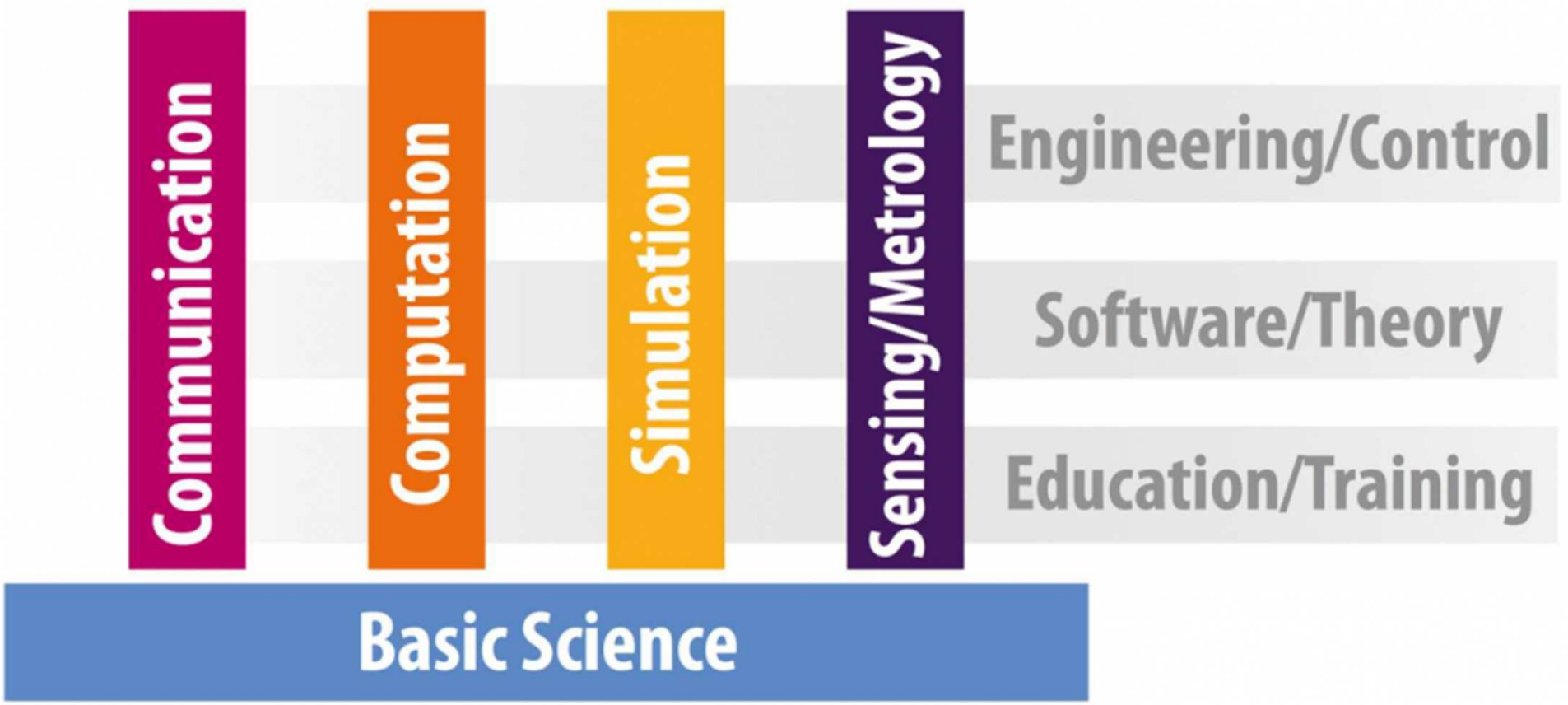
Universal quantum computers will be available with computational power at a level of performance that will exceed even the most powerful classical computers of the future. They will be reprogrammable machines used to solve demanding computational problems, such as optimisation tasks, database searches, machine learning and image recognition. They will contribute to Europe's smart industry, helping to make European manufacturing industries more efficient.

http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf

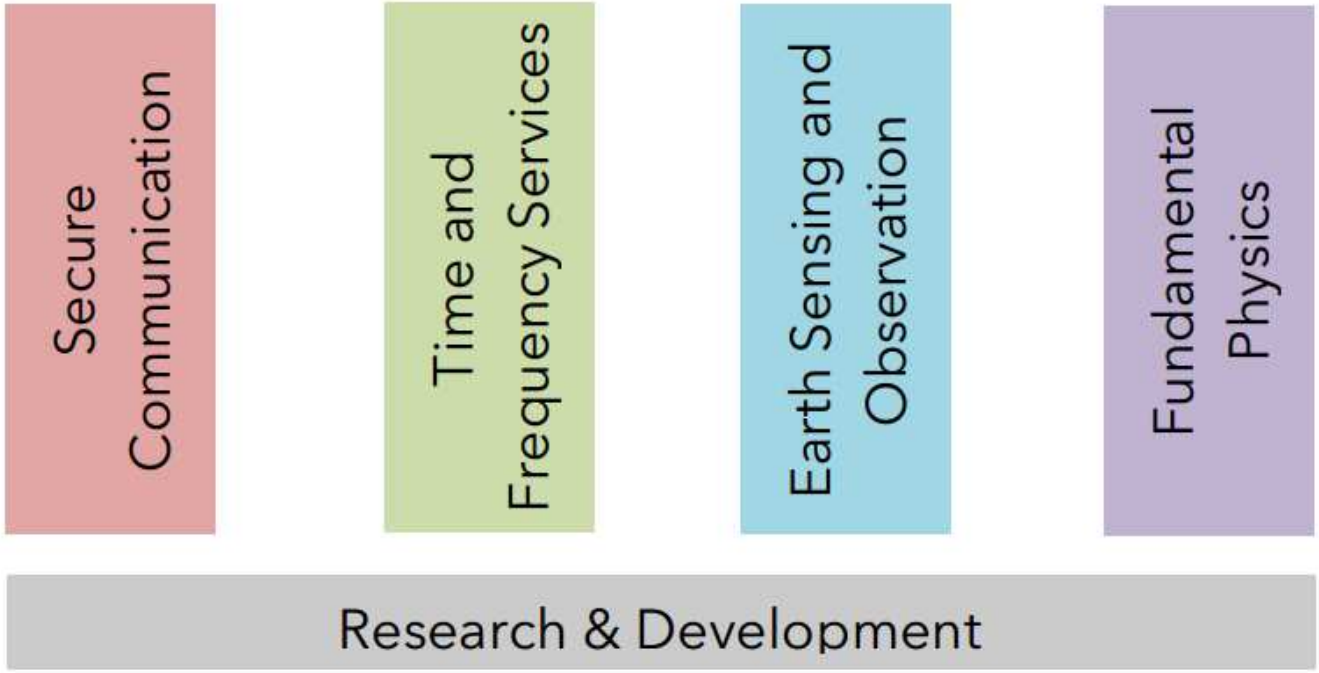
Quantum Manifesto

A New Era of Technology

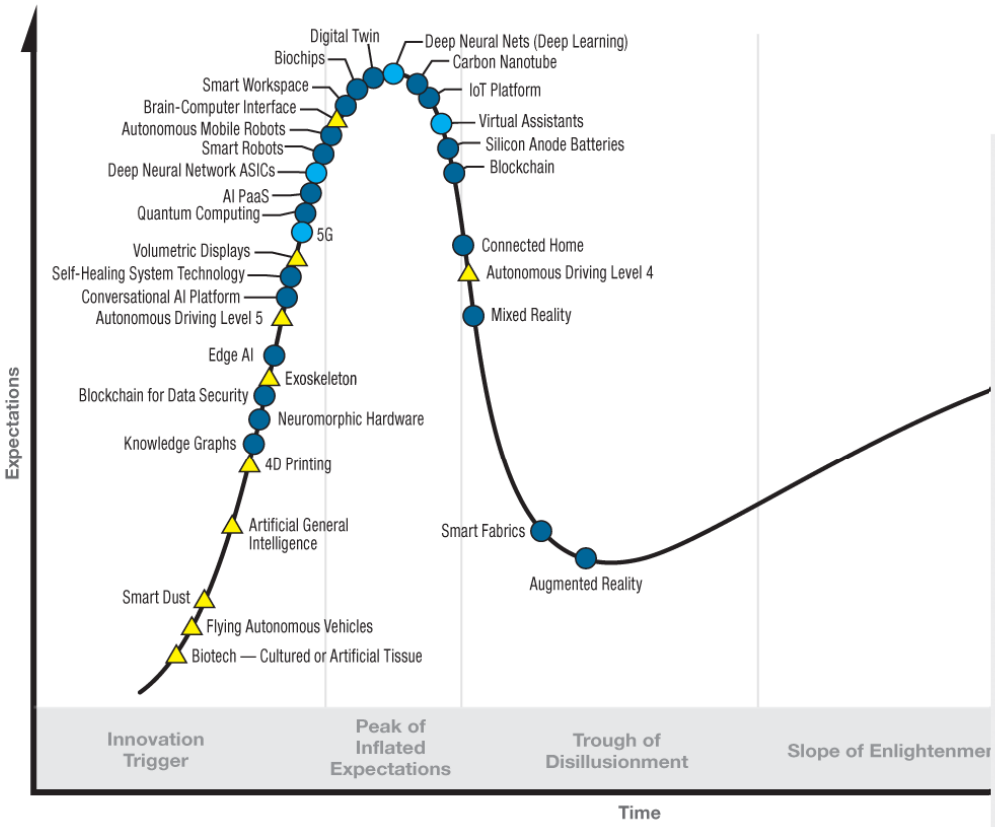
May 2016



The scientific and technological legacy of the 2
milestones such as **quantum mechanics** and **p**
Both endeavours have opened new avenues fo
understanding of Nature, and are true landmar
Quantum theory and space science form buildi
research framework for exploring the **boundari**
through the unique working conditions offered
performed in space.



Hype Cycle for Emerging Technologies, 2018



Plateau will be reached in:
- less than 2 years
- 2 to 5 years
- 5 to 10 years

gartner.com/SmarterWithGartner

Source: Gartner (August 2018)
© 2018 Gartner, Inc. and/or its affiliates. All rights reserved.

Quantum Computing
Key Potential Applications

5 Unknown Problems
100,000+ qubits

1 Chemistry
100 – 200 qubits

4 Material Science
100s – 1,000s qubits

2 Optimization
100s – 1,000s qubits

3 Machine Learning
100s – 1,000s qubits

gartner.com/SmarterWithGartner

Source: "Nature," Wikipedia
© 2019 Gartner, Inc. All rights reserved.

Gartner

Space.com › Tech

China Launches Pioneering 'Hack-Proof' Quantum-Communications Satellite

By Mike Wall, Space.com Senior Writer | August 16, 2016 06:13pm ET

385
54
19
37
1388
MORE

China launched the first-ever quantum-communication satellite, known as QUESS, atop a Long March-2D rocket from the Jiuquan Satellite Launch Center on Aug. 15, 2016 (Aug. 15 local time).

Credit: Xinhua/Jin Liwang

Source of image: http://www.space.com/33760-china-launches-quantum-communications-satellite.html

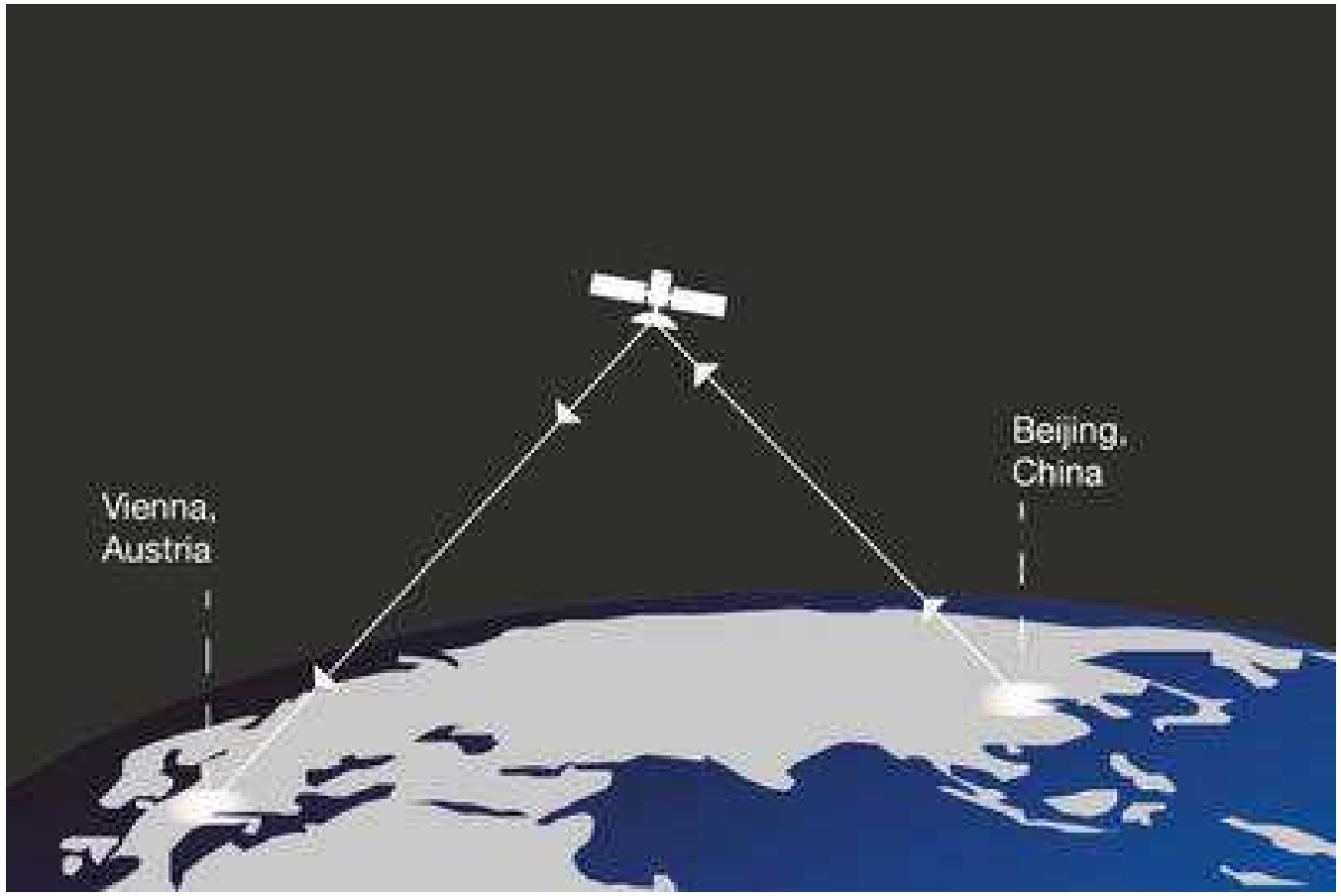
‘Much better than expected’: Chinese ‘hack-proof’ quantum communication satellite put into service

Published time: 19 Jan, 2017 04:43 Get short URL

Beijing Aerospace Control Center. © Ju Zhenhua / Xinhua / Global Look Press via ZUMA Press

The world’s first quantum communication satellite is now officially operational following months of in-orbit testing, the Chinese Academy of Sciences (CAS) announced, saying that performance of the device is “much better” than was initially expected.

Source of image: https://www.rt.com/news/374167-china-quantum-satellite-operational/


Vienna,
Austria
Beijing,
China

⟨InfiniQuant⟩

Metropolitan Quantum Communication

Using coherent quantum communication to enhance the security of intra-city cryptography. Coherent Quantum Key Distribution Our quantum key distribution systems are based on coherent telecommunication technology. Quantum states are distributed with state-of-the-art rates of 10 Gbaud via an optical fiber link,...

Satellite Quantum Communication

We use quantum-enhanced satellites to provide quantum communication on a global scale. Quantum Communication on a global scale Current quantum communication technologies are limited by a fixed amount of tolerable loss for the quantum signals. In fibers, this loss scales...

Quantum Random Number Generation

Harnessing the power of quantum mechanics to generate true and unique, high-speed random numbers. Quantum random numbers from the vacuum While a coin toss or the casting of a die may seem random, short-term behaviour is very predictable when for example...

10.08.2021 10:55

Teilen:

First quantum-secured video conference between German Federal agencies: QuNET demonstrates quantum communication

Desiree Haak *Strategie / Marketing / Koordination*
Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF

Today, two German federal authorities communicated via video for the first time in a quantum-secure manner. The QuNET project, an initiative funded by the German Federal Ministry of Education and Research (BMBF) to develop highly secure communication systems, is thus demonstrating how data sovereignty can be guaranteed in the future. This technology will not only be important for governments and public authorities but also to protect everyday data.

It was a foretaste of the communication of the future - or rather, the "data security" of the future. Because when Federal Research Minister Anja Karliczek invited members of the Federal Office for Information Security (BSI) to a video conference today, everything looked the same, at least for outsiders. Together with Andreas Könen, Head of Department CI "Cyber and IT Security" at the Federal Ministry of the Interior, Building and Community (BMI) and BSI Vice President Dr. Gerhard Schabhüser, the minister talked via video stream.

DECLARATION ON A

QUANTUM COMMUNICATION INFRASTRUCTURE

FOR THE EU

All 27 EU Member States

have signed a declaration agreeing to **work together** to explore how to **build a quantum communication infrastructure** (QCI) across Europe, boosting European capabilities in **quantum technologies, cybersecurity and industrial competitiveness.**

@FutureTechEU #EuroQCI

European Commission organises event on quantum communication infrastructure

Published on: 04/10/2019

On 30 September, the European Commission and the European Space Agency (ESA) organised a joint industry day on "quantum communication infrastructure (QCI) for Europe – space segment". This event was aimed at helping European industry and researchers develop the necessary technology for this emerging sector. The main goal was to share and discuss various options for potential space infrastructure for different use cases with QCI stakeholders.

https://ec.europa.eu/growth/content/european-commission-organises-event-quantum-communication-infrastructure_en

HUNGARIAN QUANTUM ECOSYSTEM

2017-2021:

HUNQUTECH

2020-2025:

Quantum Information National Laboratory HUNGARY

2023-2025:

QCIHungary (EuroQCI)

QUANTUM COMMUNICATION RESEARCH GROUP



















QUANTUM COMMUNICATIONS ACTIVITIES @BME

MCL Mobile Communications & Quantum Technologies Lab.

Competences and actual projects

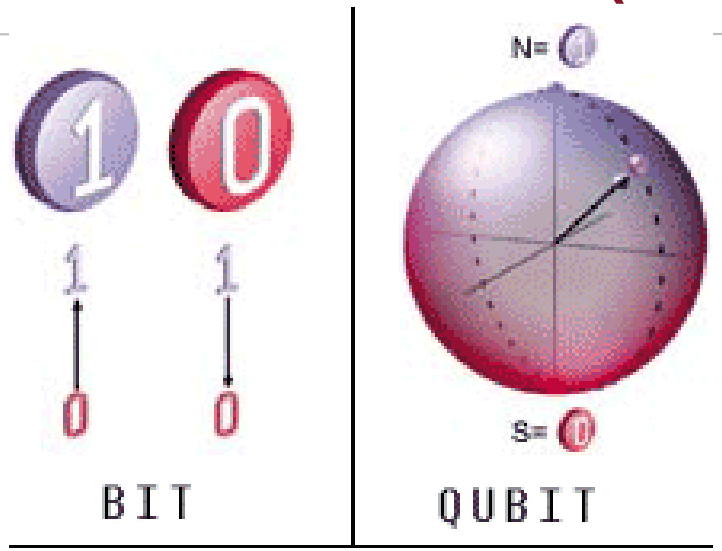
Fiber

- BB84 QKD demonstration with own developed system *(in cooperation with Ericsson Hungary)*
- CV QKD long distance demonstration with own developed system as part of the national QKD network *(in cooperation with Hungarian Telekom and Wigner Research Centre for Physics)*
- Own developed Optical Quantum Random Number Generator
- Beyond QKD: Developing entanglement-based medium access control; focusing on quantum internet
- Entanglement-based QKD system (under-development)
- OpenQKD OpenCall: QuantumGigalink *(in cooperation with Magyar Telekom)*

Free-space and space

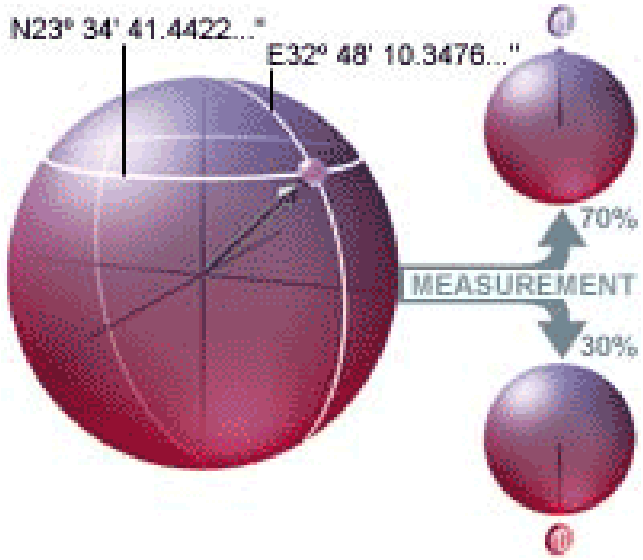
- Entanglement-based free-space QKD over River Danube *(in cooperation with Vodafone Hungary)*
- Participating in two ESA projects (QuStatoin, Certain) (in cooperation with ATL Zrt., Relcom Kft.)
- Investigating the possibilities for cubesat-based QKD
- Investigating the possibilities for quantum capable optical ground stations
- Theoretical work on future's satellite based QKD systems

QUANTUM BIT (QUBIT)



$$|\phi\rangle = a|0\rangle + b|1\rangle$$

$$a, b \in C \text{ and } |a|^2 + |b|^2 = 1$$



QUANTUM REGISTERS

$$|\varphi\rangle = a|0\rangle + b|1\rangle$$

$$|\varphi\rangle^{\otimes 2} = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

$$|\varphi\rangle^{\otimes 4} = a|0000\rangle + b|0001\rangle + \ldots + o|1110\rangle + p|1111\rangle$$

QUREGISTER

© Department of Networked Systems and Services

POSTULATES OF QUANTUM MECHANICS FROM ENGINEERING POINT OF VIEW

- 1th postulate: quantum bit
  - Vector in Hilbert space
- 2th postulate : logic gates
  - Unitary transform
  - Elementary logic gates
- 3rd postulate : Q/C conversion
  - Measurement statistics
  - Post measurement state
- 4th postulate : registers
  - Tensor product

$$|\varphi\rangle = \sum_{i=0}^{2^n-1} \varphi_i |i\rangle$$

$$U^\dagger \equiv U^{-1}$$

$$P(m \mid |\varphi\rangle) = \langle\varphi|M_m^\dagger M_m|\varphi\rangle$$

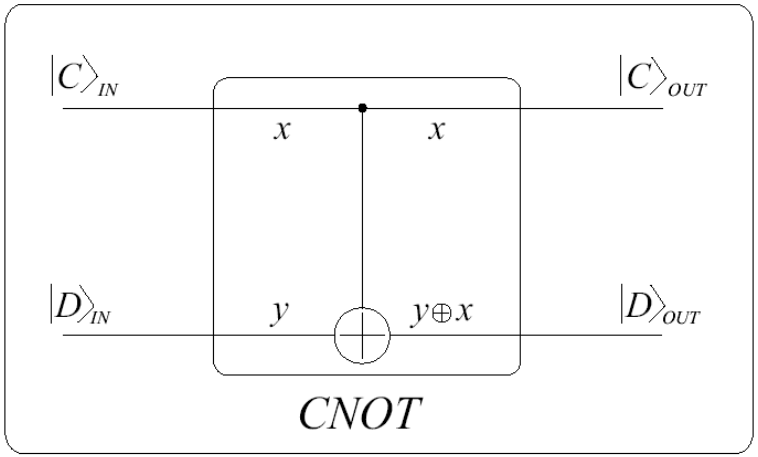
$$|\varphi'\rangle = \frac{M_m|\varphi\rangle}{\sqrt{\langle\varphi|M_m^\dagger M_m|\varphi\rangle}}$$

$$|\varphi\rangle = |0\rangle \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|00\rangle + |01\rangle}{\sqrt{2}}$$

ENTANGLEMENT

$$|\varphi\rangle = \varphi_0|00\rangle + \varphi_1|01\rangle + \varphi_2|10\rangle + \varphi_3|11\rangle$$

$$|\varphi\rangle = \varphi_0|00\rangle + \varphi_3|11\rangle$$



- Upper wire: control
- Lower wire: data

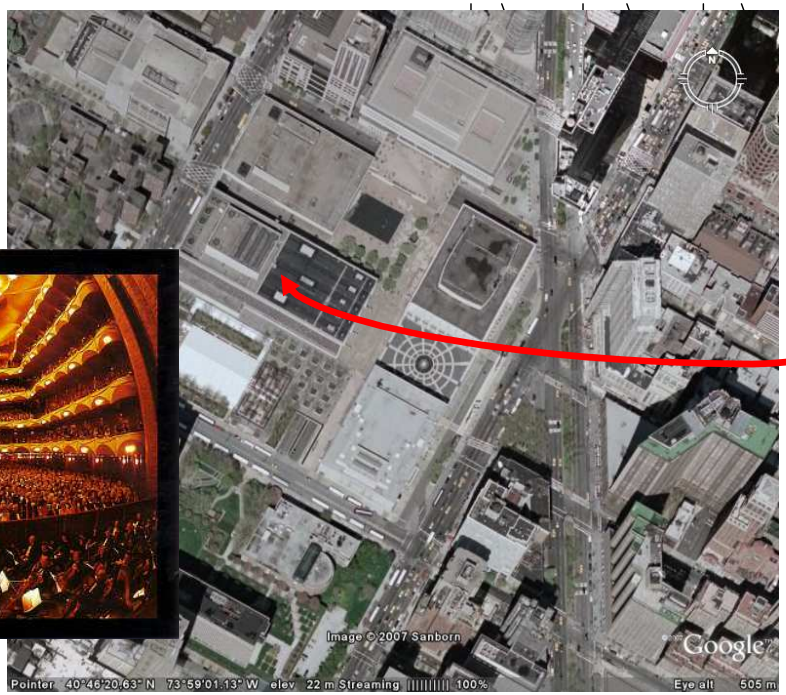
$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}},$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}},$$

$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

© Department of Networked Systems and Services

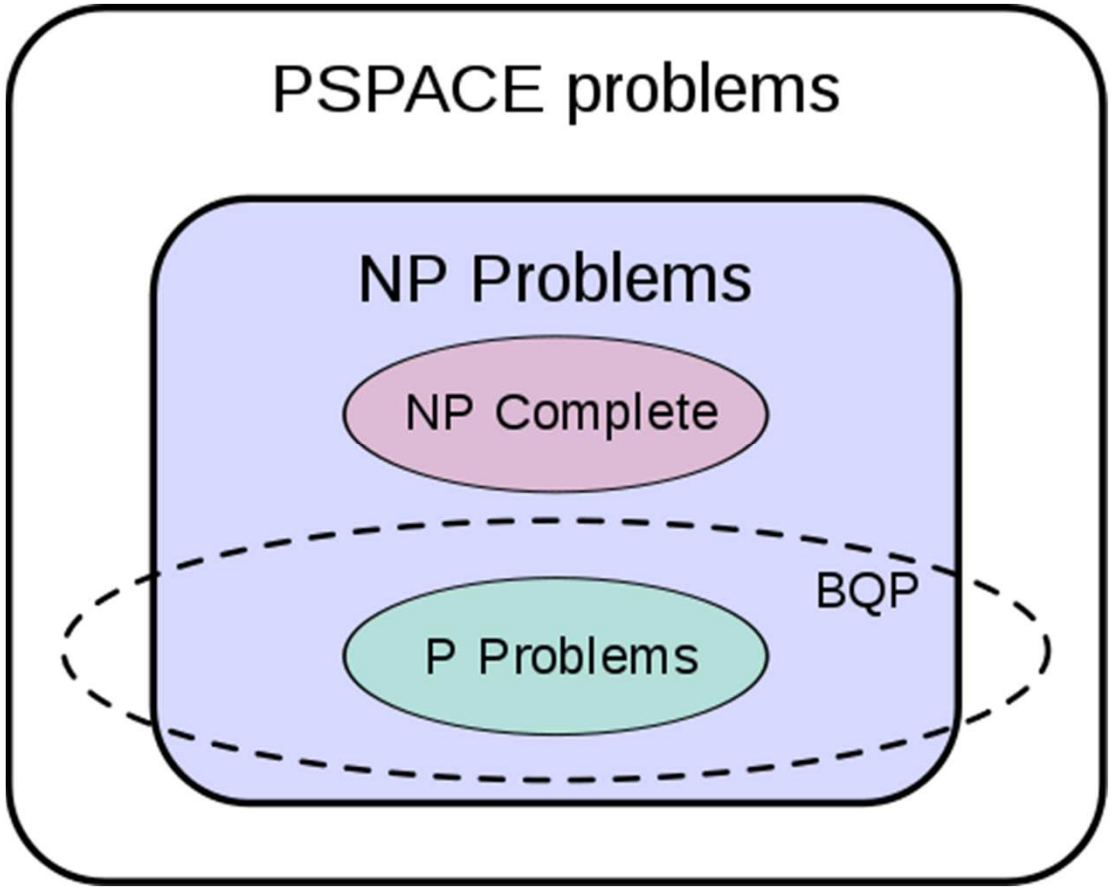


$$|\varphi\rangle = \varphi_0|00\rangle + \varphi_3|11\rangle$$

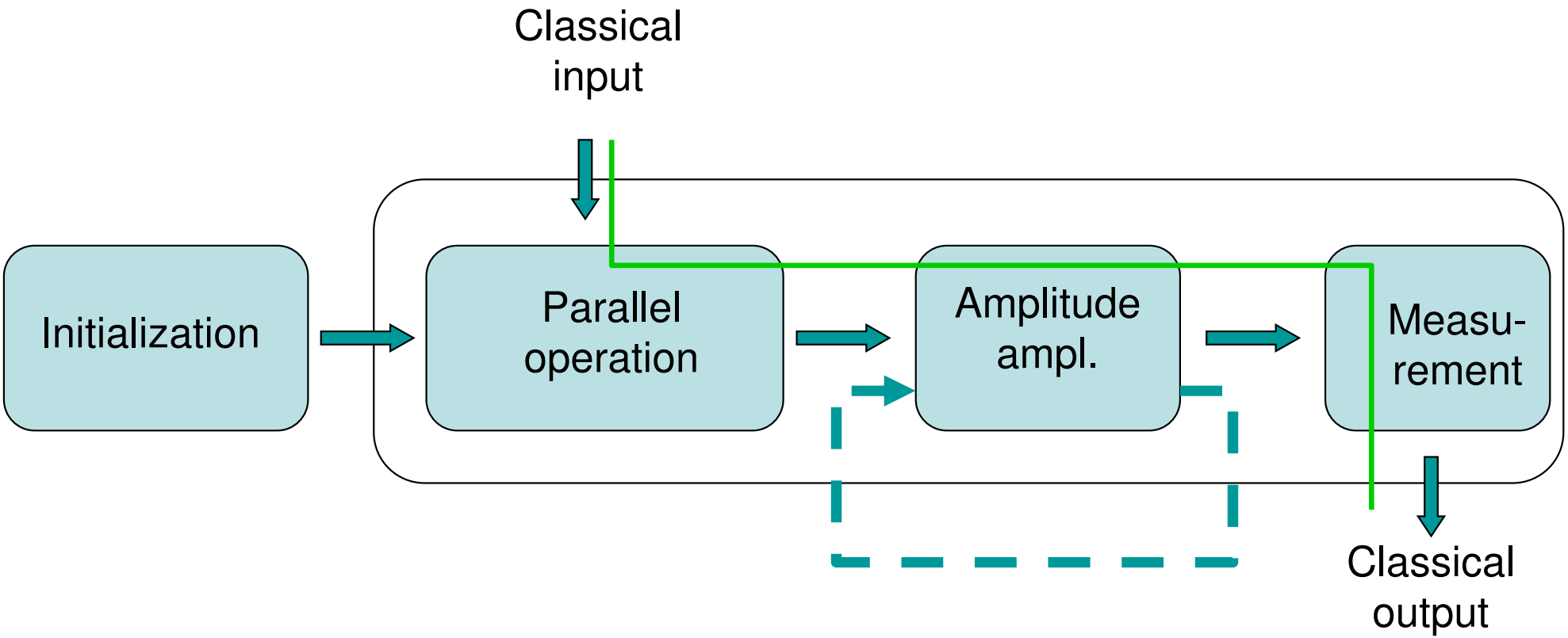
IMPORTANT CONSEQUENCES

- NO-cloning: only orthogonal and/or known states can be copied!
  - Differentiation (measurability) and making perfect copies are twin brothers.
  - Amplification=copying!
  - NO universal COPY command!!!
- Entanglement – special resource
  - Non tensor product states.
  - Measuring one half of the pair will influence the measurement result of the other half.
  - Information can not be delivered in this way between distant points!

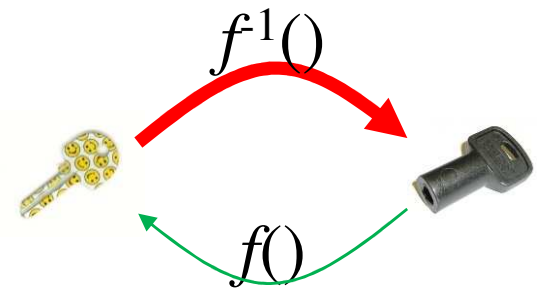
Application: Quantum Computing

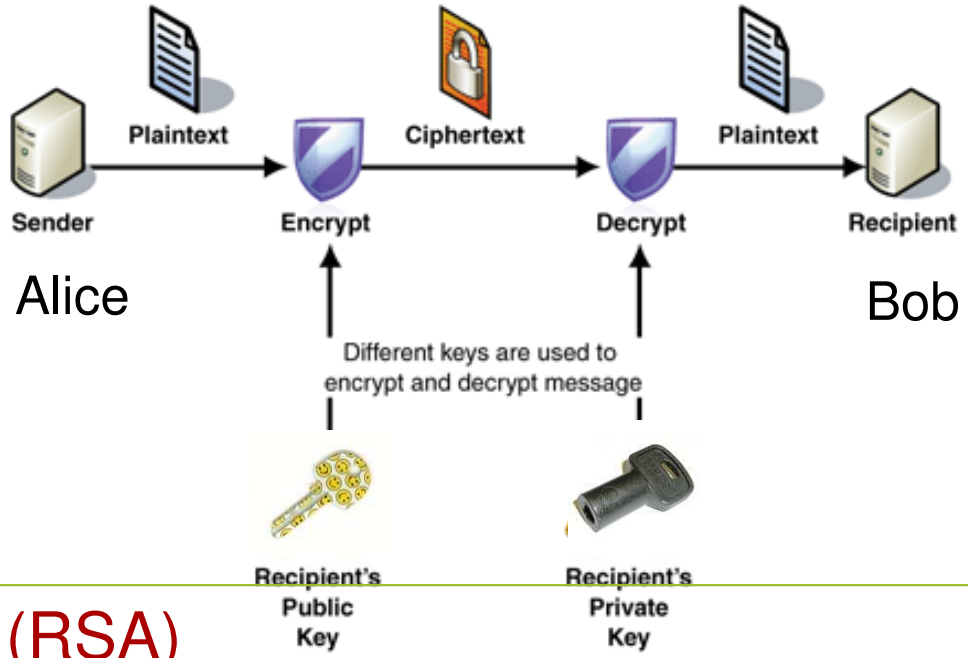

PSPACE problems
NP Problems
NP Complete
BQP
P Problems

GENERAL MODEL OF QUANTUM ALGORITHMS



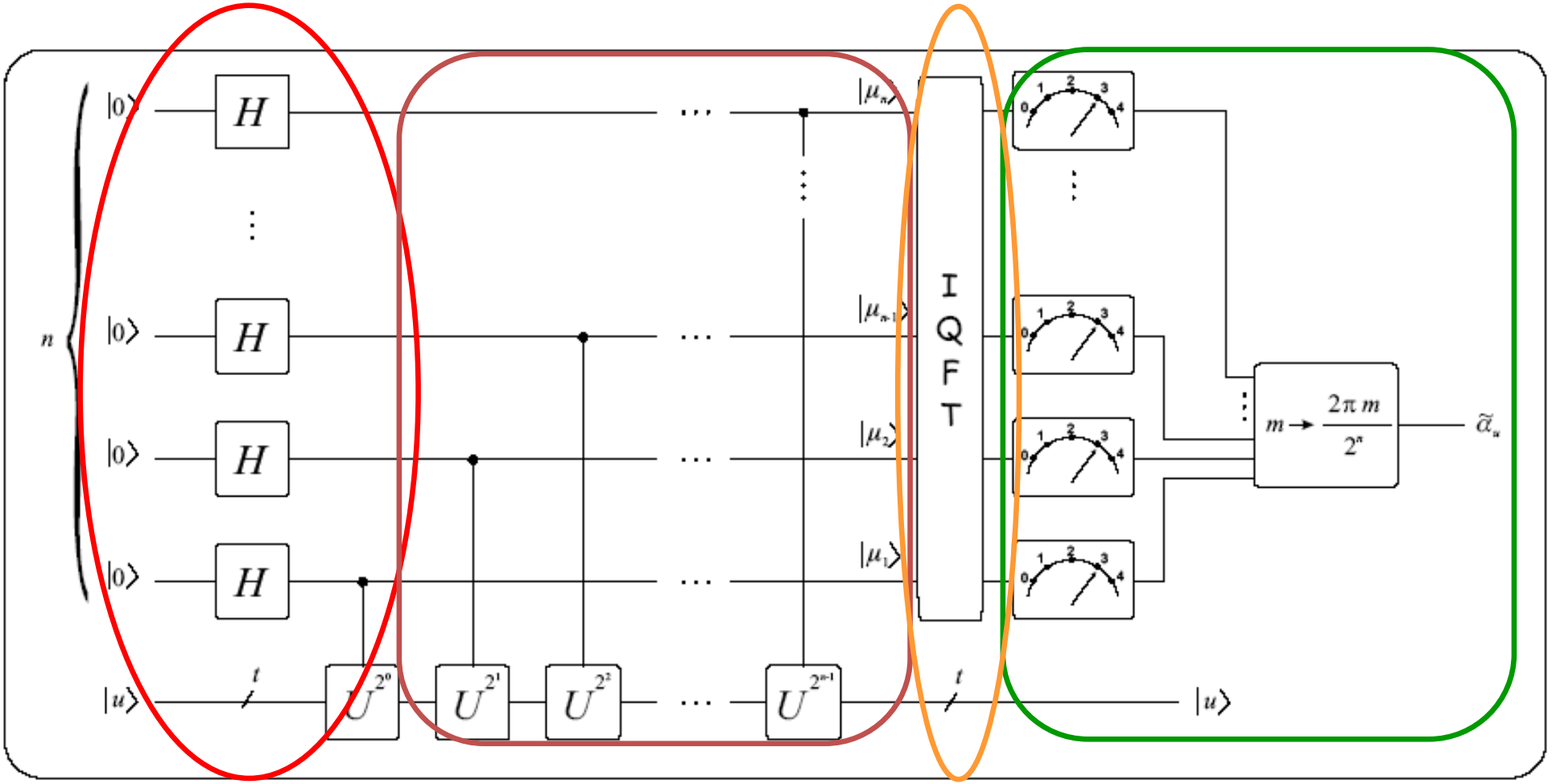
PUBLIC (ASYMMETRIC) KEY CRYPTOGRAPHY



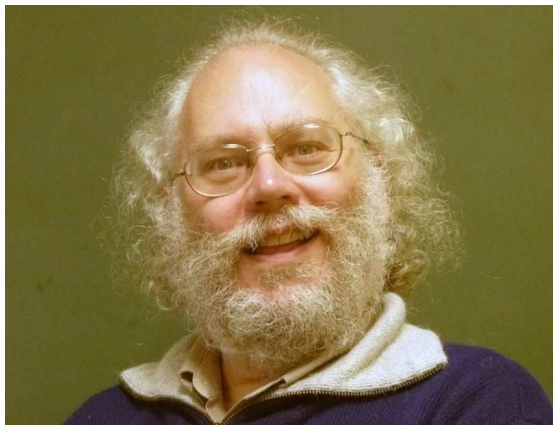


- Public key cryptography (RSA)
  - Public key for encryption, secret key for decryption
  - Key generation: using the product of two huge prime numbers
  - Hacking: computing the prime factors
- There exists no efficient method for prime factorization
- At least classically
- **However Shor's quantum order finding algorithm…**

RSA BREAKING DEVICE



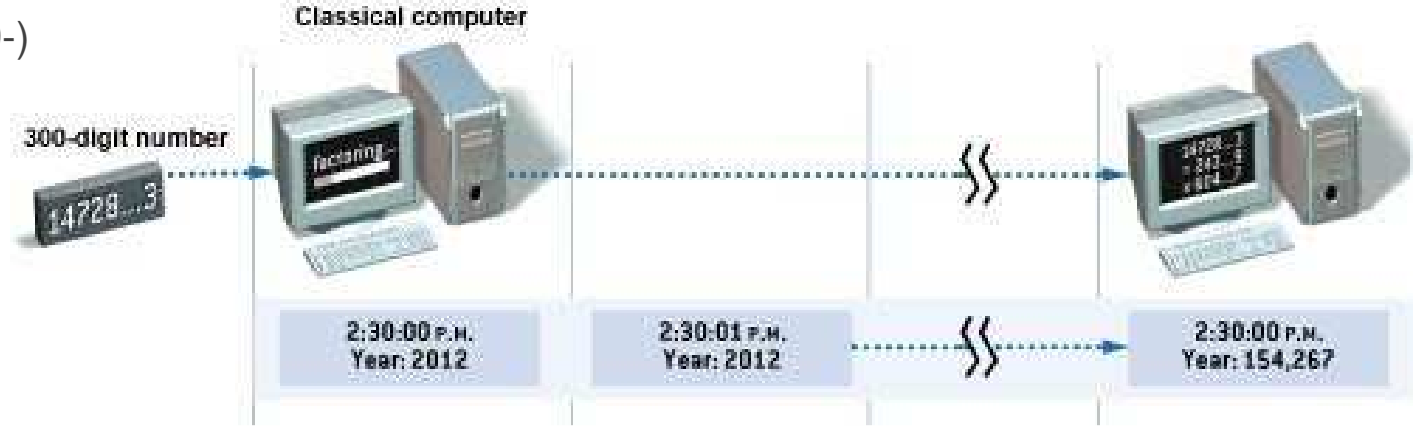
POWER OF SHOR'S ALGORITHM



Peter Shor (1959-)

$$O\left(\log^3(N)\right)$$

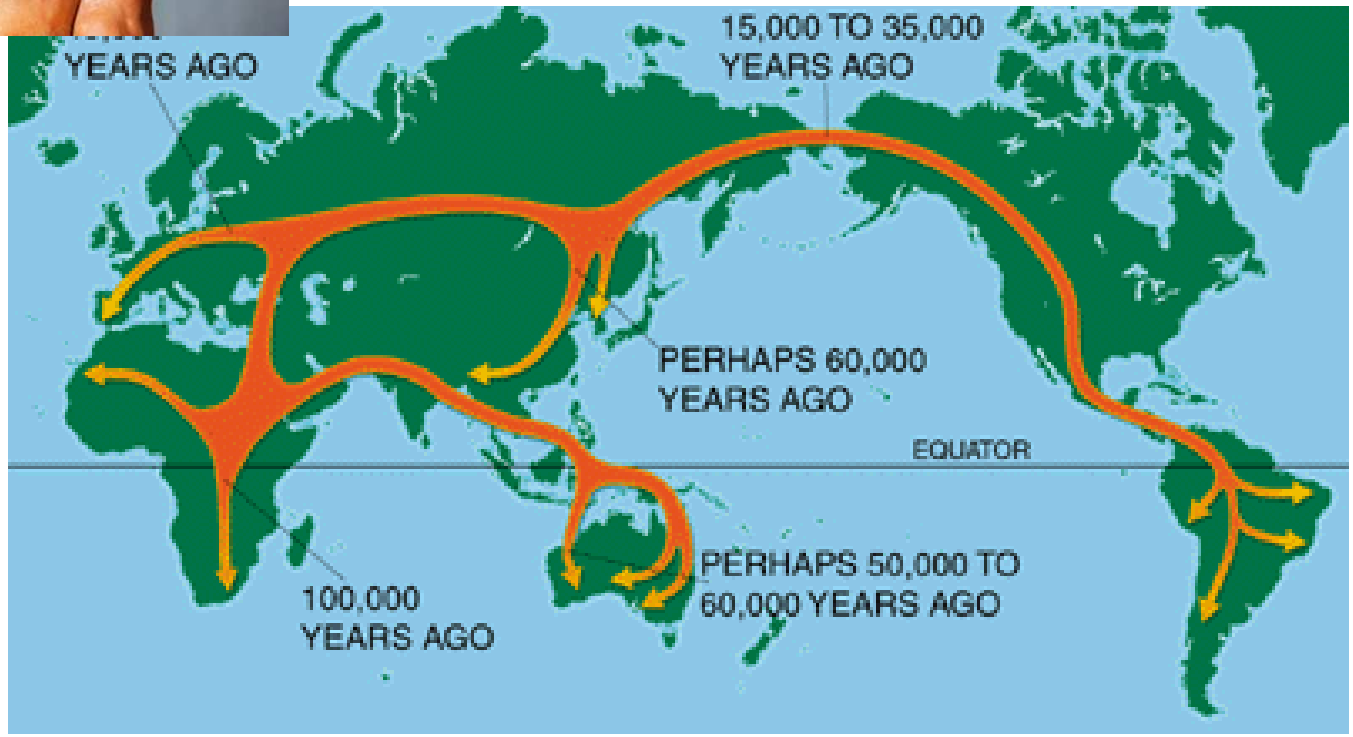
152 000 years



Adam (~ 150 000 BC)

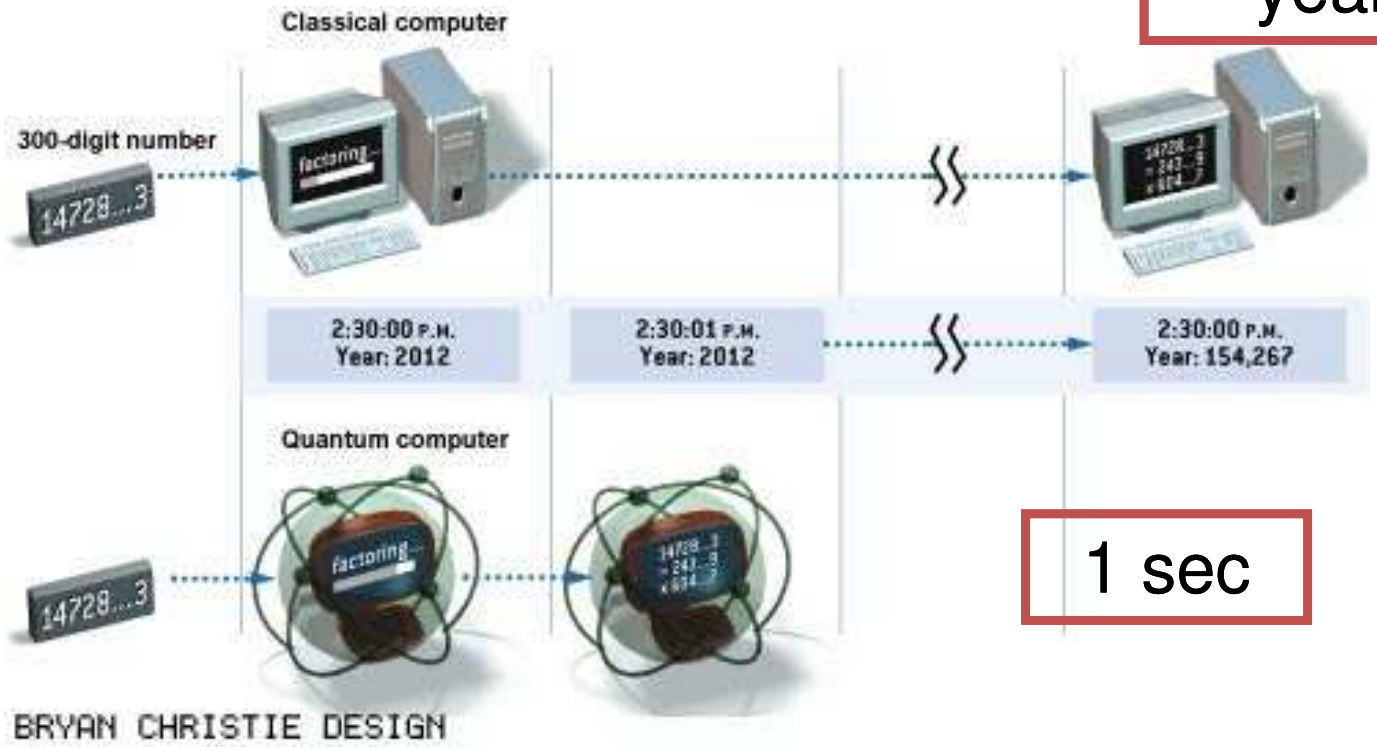
152 000
years

Starman (2018-2002018)



$$O\left(\log^3(N)\right)$$

152 000 years



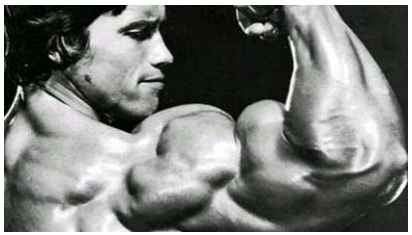
1 sec

EFFICIENCY OF HACKING

Table 9.1 Code-breaking methods and related complexity

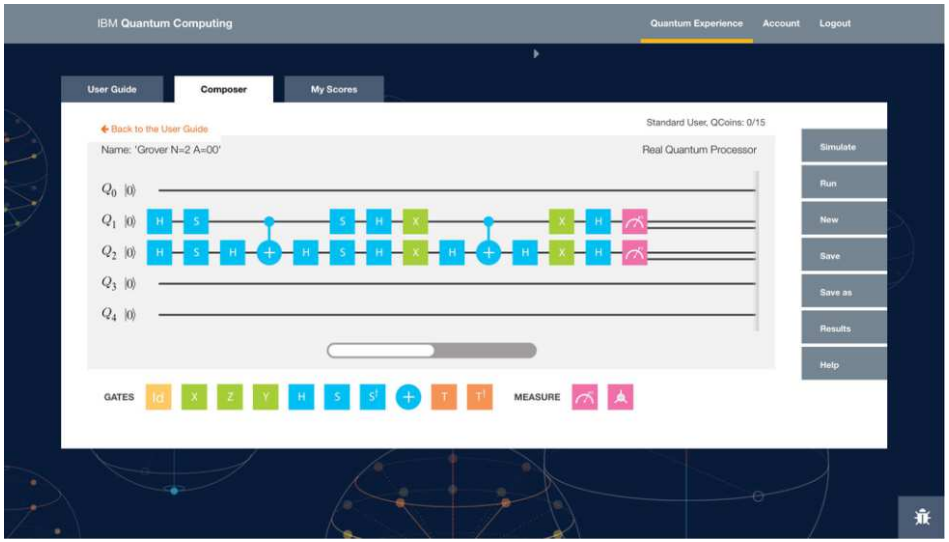
Method	$n = 128$	$n = 128$	$n = 1024$	$n = 1024$	1s barrier
BF	$1.8 \cdot 10^{7}$ s	0.58 year	$1.3 \cdot 10^{142}$ s	$4 \cdot 10^{134}$ year	80 bit
BC	$6 \cdot 10^{-4}$ s	$1.9 \cdot 10^{-11}$ year	$3.5 \cdot 10^{8}$ s	11.29 year	273 bit
G	$4 \cdot 10^{-3}$ s	$1.3 \cdot 10^{-10}$ year	$1.1 \cdot 10^{65}$ s	$3.7 \cdot 10^{57}$ year	159 bit
S	$2 \cdot 10^{-5}$ s	$6.6 \cdot 10^{-14}$ year	**0.01** s	$3.4 \cdot 10^{-11}$ year	**10000** bit

- BF: *brute force* classical method which scans the integer numbers from 2 to $\lceil \sqrt{N} \rceil$ with complexity $O(\sqrt{N})$,
- BC: *best classical* method requiring $O(\exp[c \cdot \mathrm{ld}^{\frac{1}{3}}(N)\mathrm{ld}^{\frac{2}{3}}(\mathrm{ld}(N))])$ steps,
- G: *Grover* search based scheme with $O(N^{\frac{1}{4}})$,
- S: *Shor* factorization with $O(\mathrm{ld}(N)^3)$. ← Brutal!



Arnold Schwarzenegger (1947-)

IBM QUANTUM COMPUTER ACCESS!

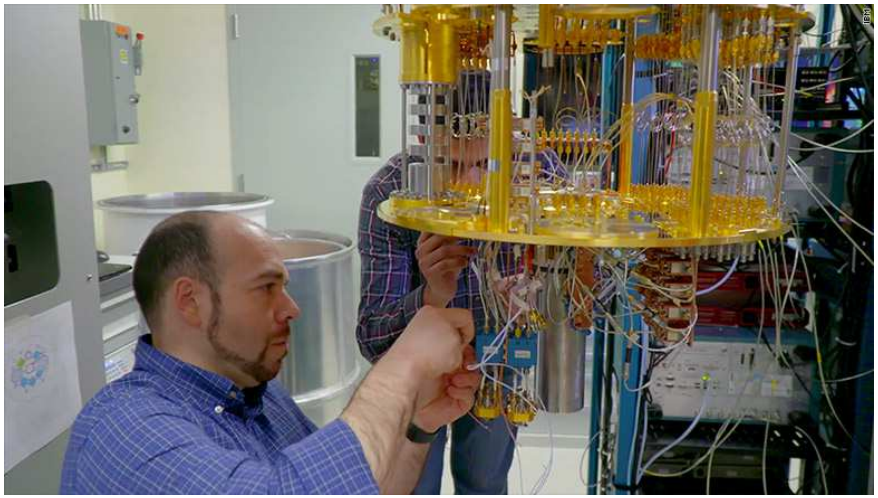


2016: 5 qubit

https://quantum-computing.ibm.com/

2017: 16 qubit

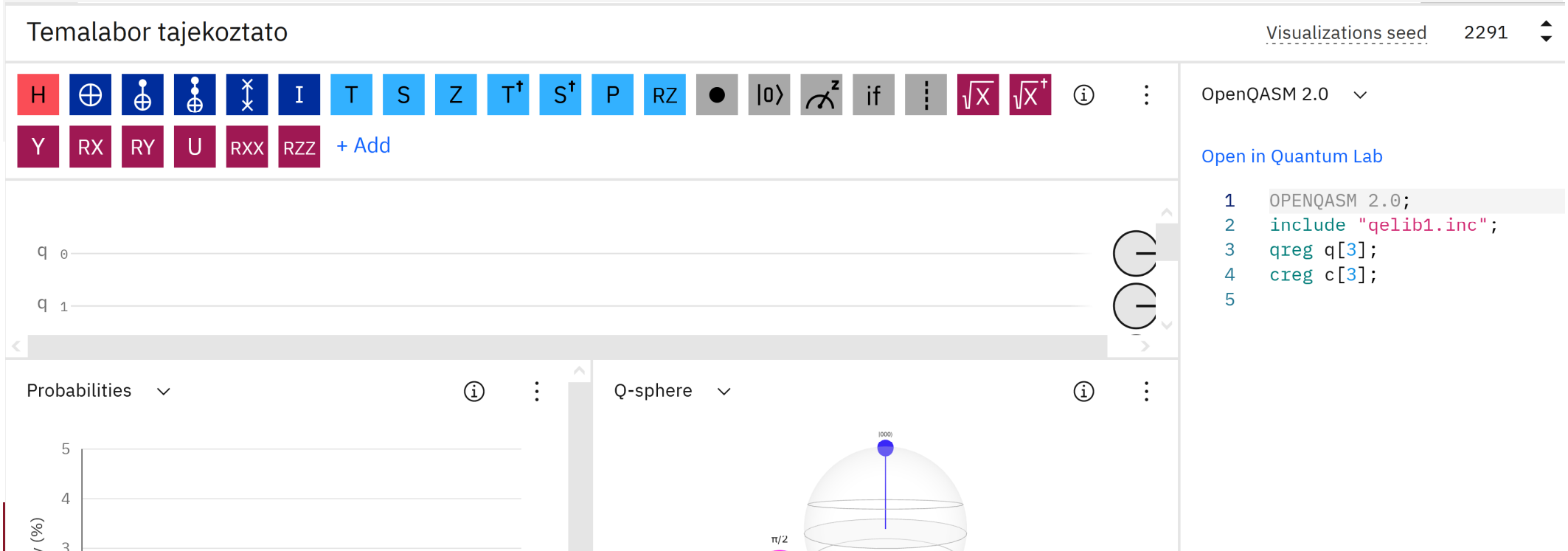
IBM Q Awards:
https://qx-awards.mybluemix.net/



IBM Quantum

Real quantum computers. Right at your fingertips.

IBM offers cloud access to the most advanced quantum computers available. Learn, develop, and run programs with our quantum applications and systems.

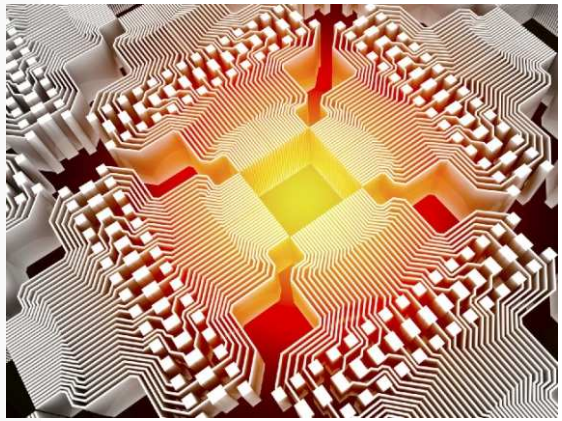


Quantum Programing language: Q#

```
operation BellTest (count : Int, initial: Result) : (Int,Int)
{
    body
    {
        mutable numOnes = 0;
        using (qubits = Qubit[1])
        {
            for (test in 1..count)
            {
                Set (initial, qubits[0]);

                let res = M (qubits[0]);

                // Count the number of ones we saw:
                if (res == One)
                {
                    set numOnes = numOnes + 1;
                }
            }
            Set(Zero, qubits[0]);
        }
        // Return number of times we saw a |0> and number of times we saw a |1>
        return (count-numOnes, numOnes);
    }
}
```



https://docs.microsoft.com/en-us/quantum/index?view=qsharp-preview

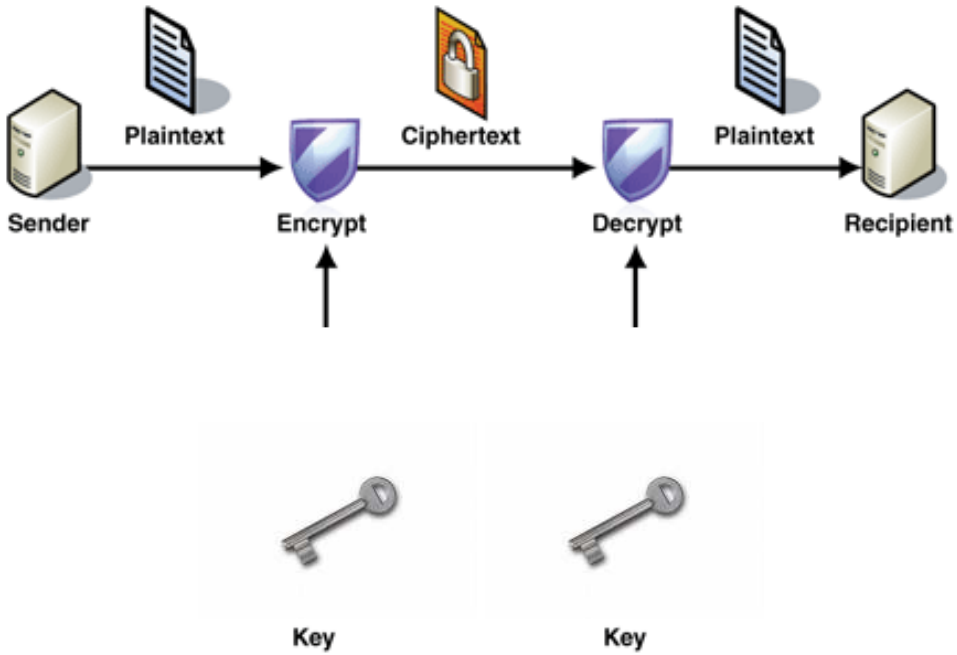
GOOGLE, SEPTEMBER 2019

https://index.hu/techtud/2019/09/24/a_google_elerte_a_kvantumfolenyt/

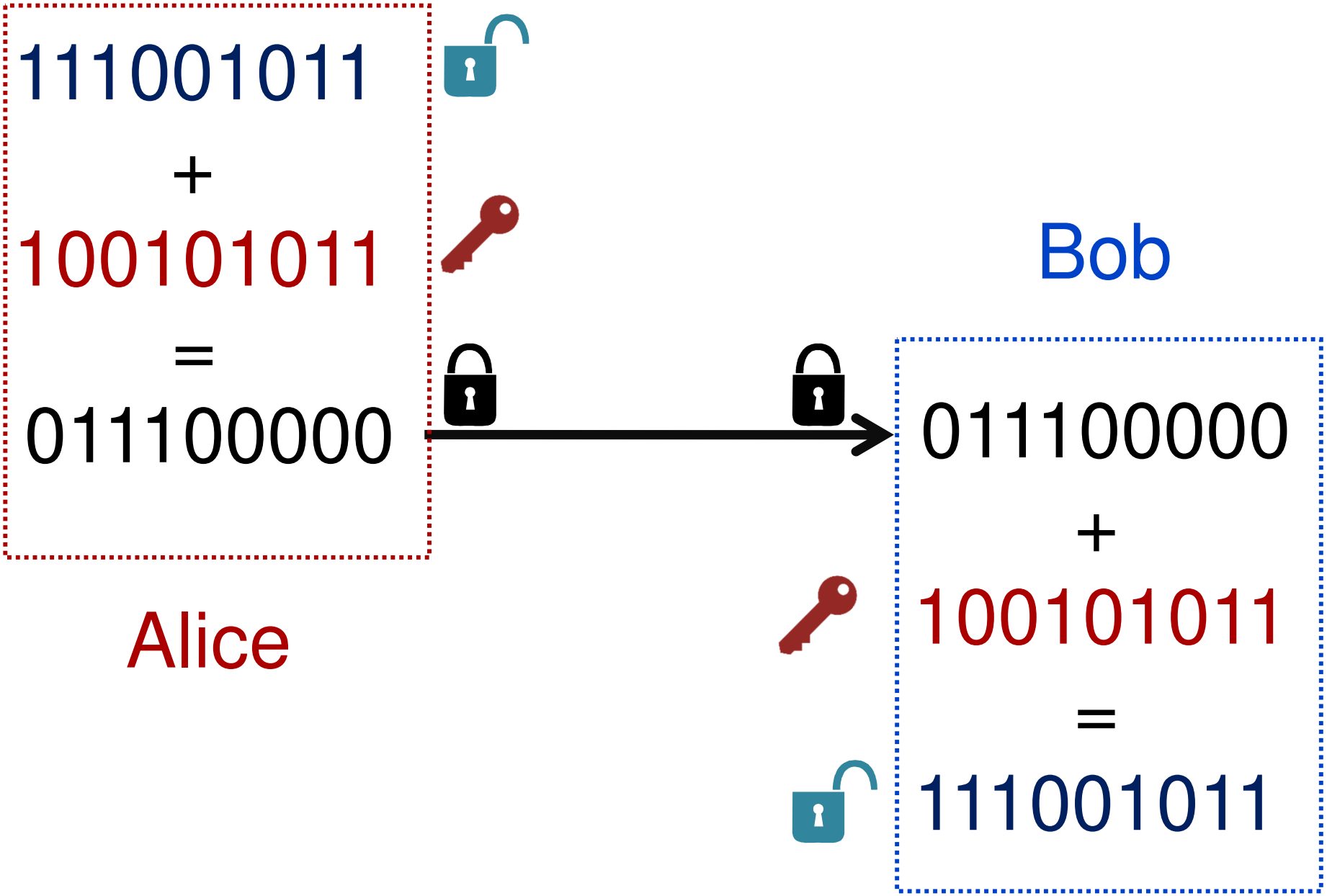
© Department of Networked Systems and Services

Application: Quantum Key Distribution

SYMMETRICAL CRYPTOGRAPHY



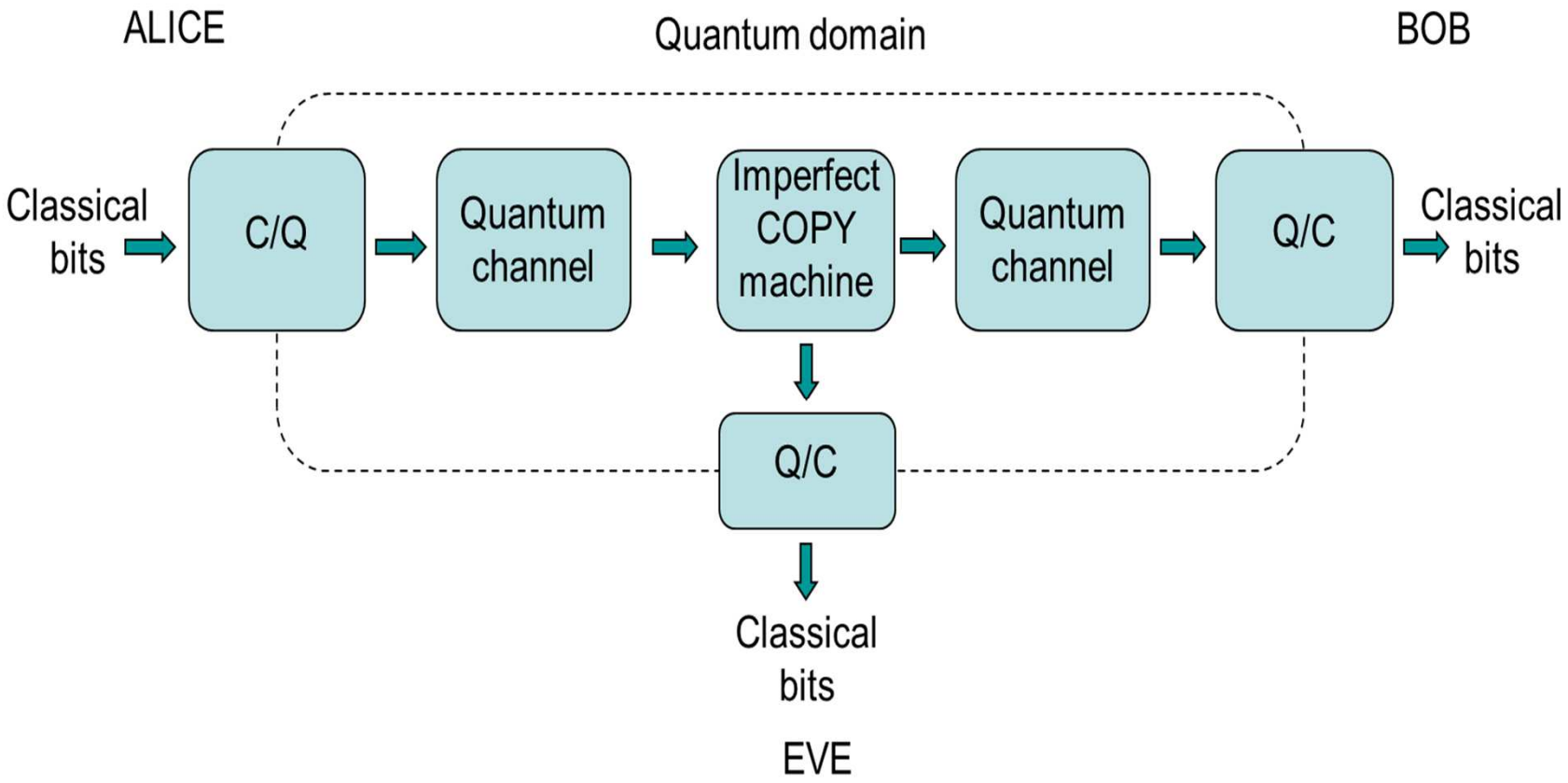
ONE TIME PAD VERNAM CYPHER



WHY QKD?

- It is compatible with the nowadays used symmetric cryptography algorithms
- Security based on the laws of the quantum physics
- The quantum channel is used to share the symmetric key for a one time pad communication
- Rest of the communication is over normal channel (optical fiber, RF, Ethernet, etc.)
- The quantum bits based on photons can travel through two types of channels: optical fiber, free-space link

BEHIND THE QKD



SEVERAL PROTOCOLS

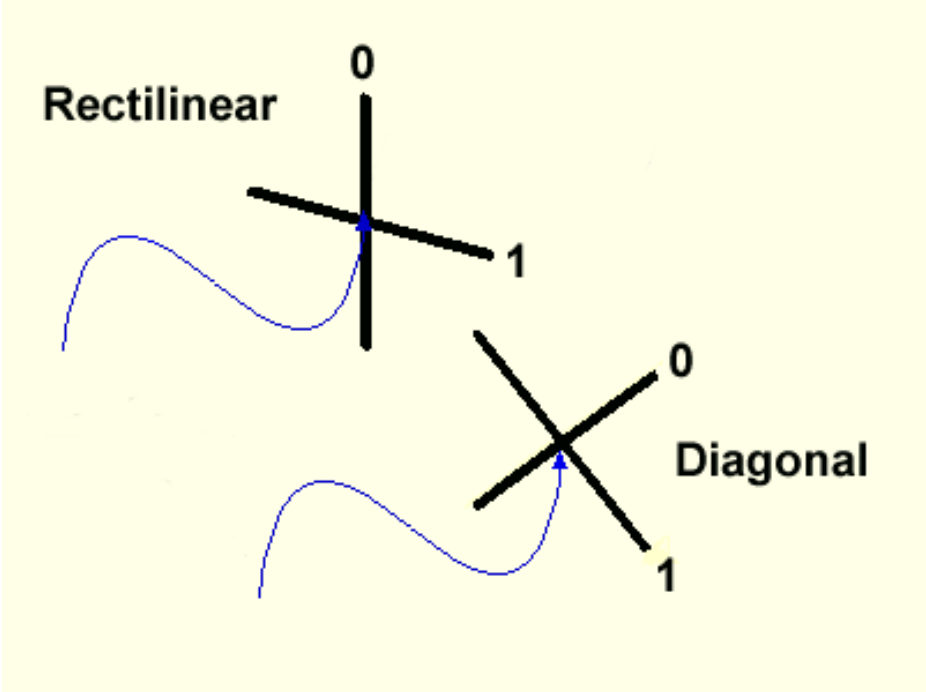
E91

BB84

B92

S09

THE BB84 QKD PROTOCOL (1)



THE BB84 QKD PROTOCOL (2)

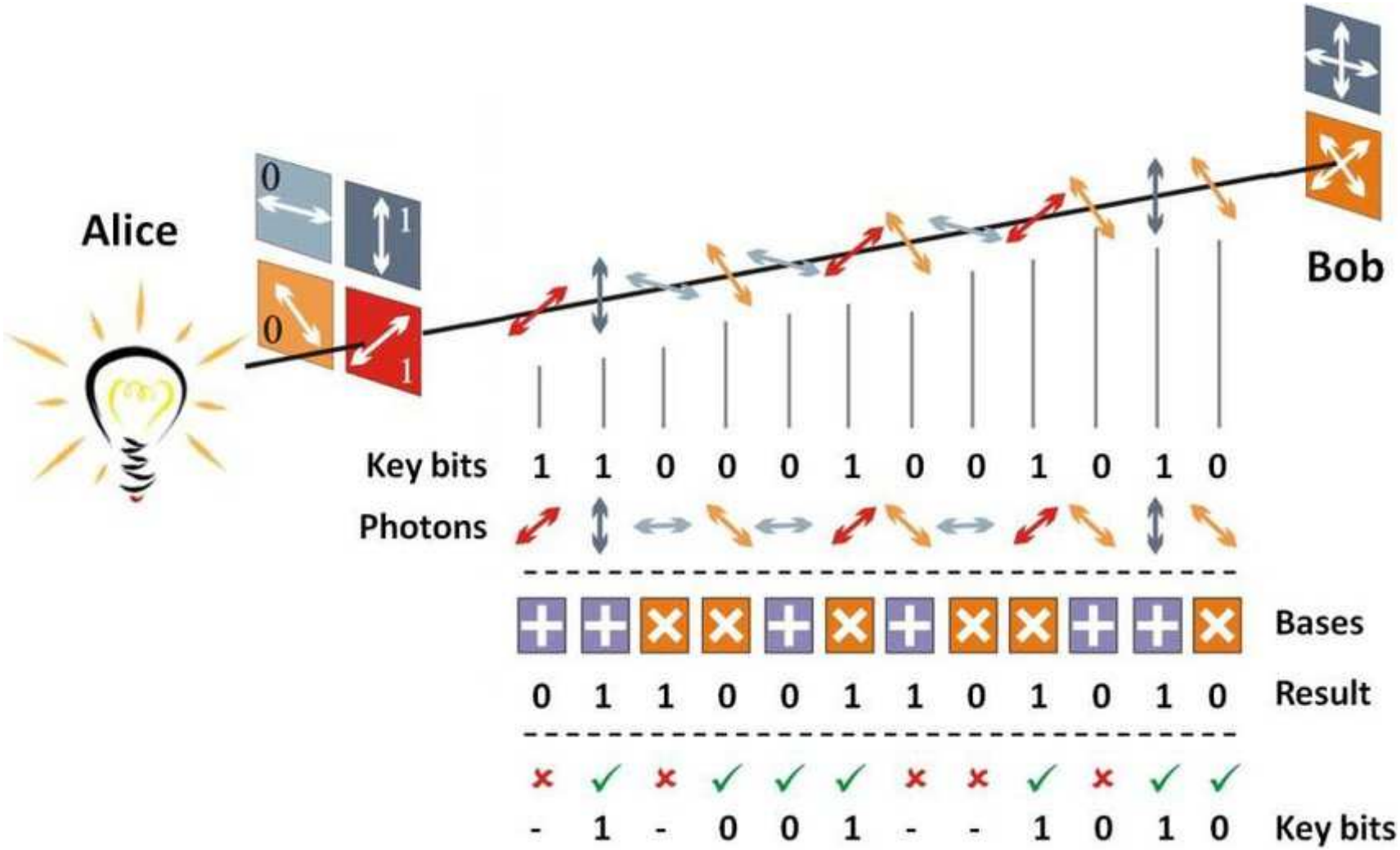
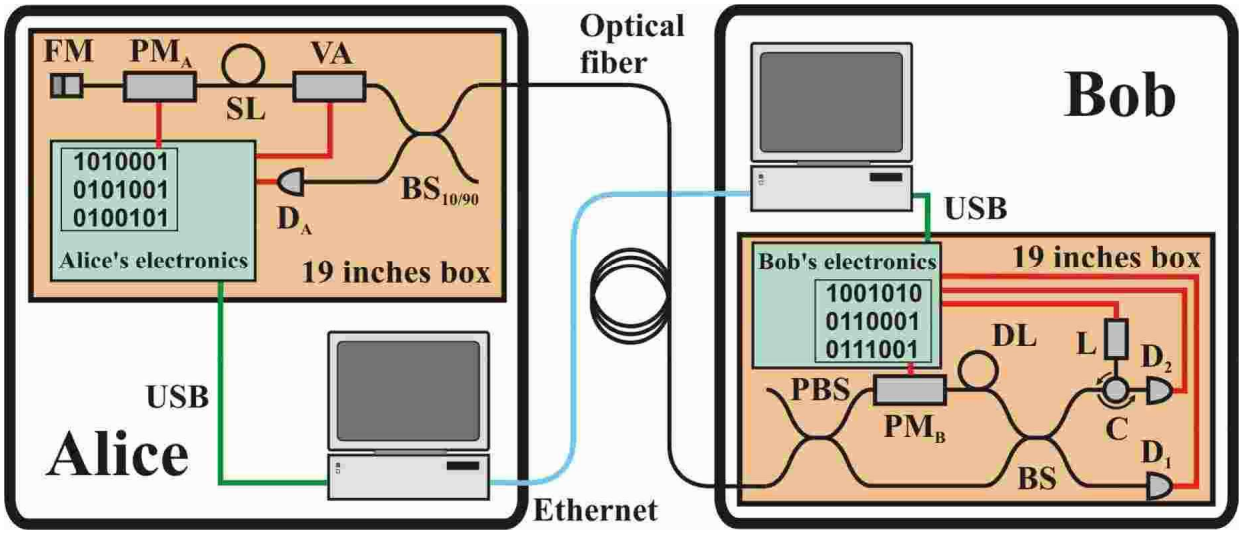
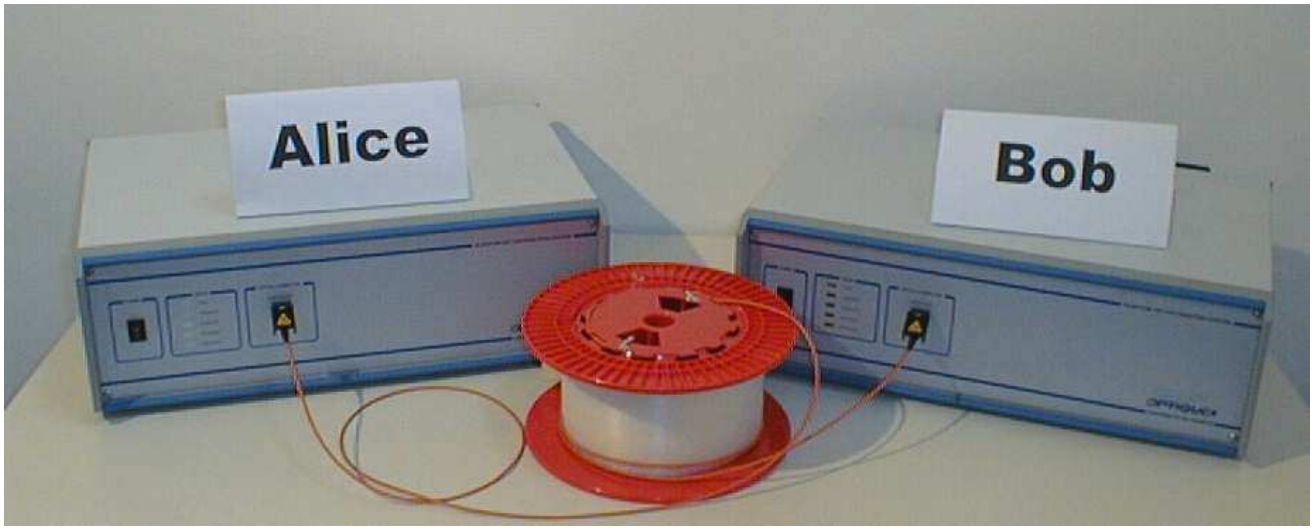


Figure from: [10.1007/978-3-319-30201-0_27](10.1007/978-3-319-30201-0_27)

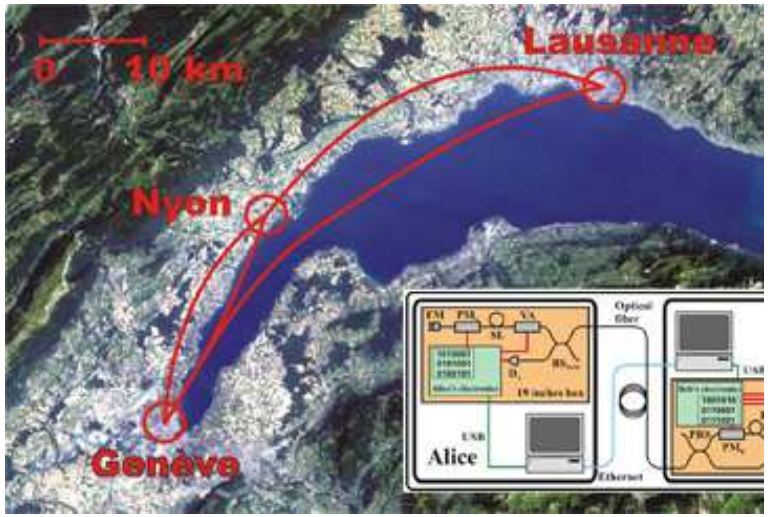
QKD IN PRACTICE



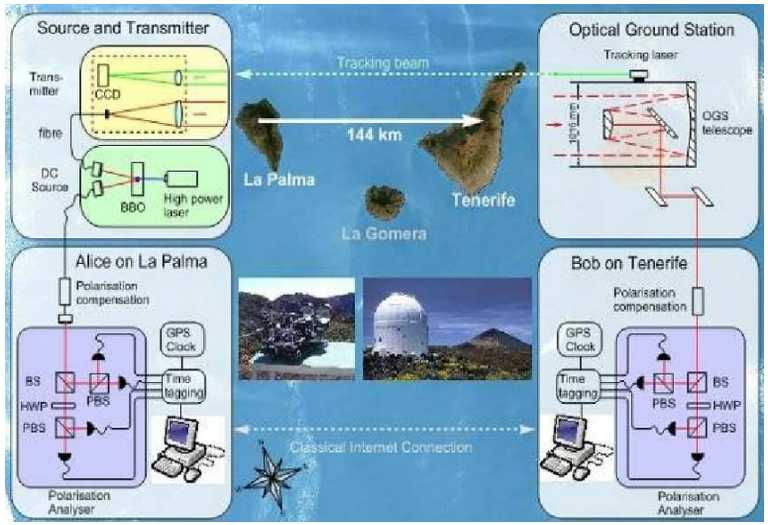


DISTANCES

1989/91	0.3 m
1993	1100 m
1995	23 km
2007	67 km
2016	404 km



1991	0.3m
1996	75 m
1998	1 km
2002	10 km
2006/2007	144 km
2016	space



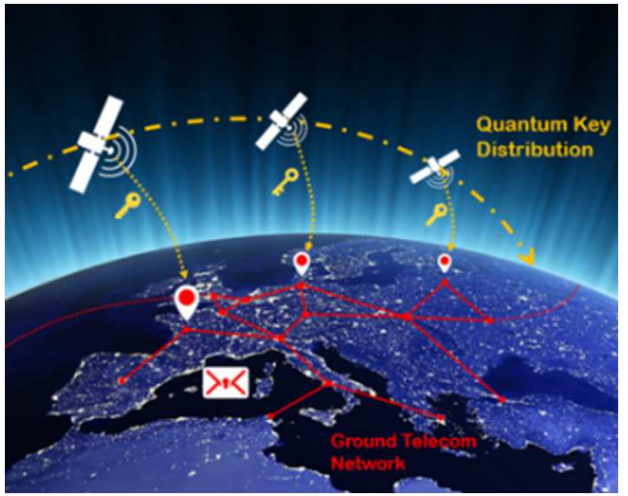
Vision: Quantum Internet in Europe

Distributed quantum computers, and quantum sensors interconnected via quantum communication networks

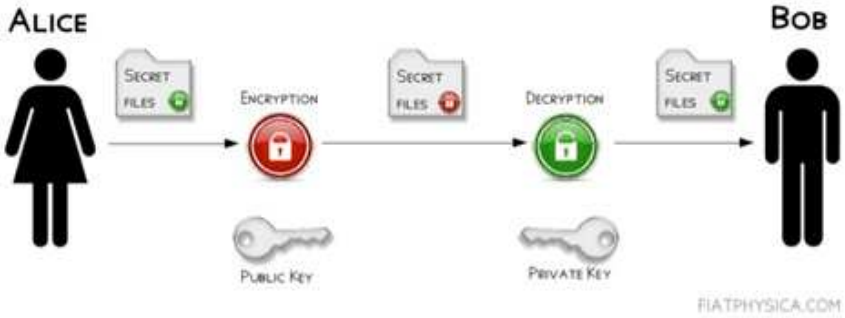
1) The Quantum Technologies Flagship
2) Develop and deploy in the EU an end-to-end quantum-secure communication infrastructure (QCI)

Towards a quantum communication infrastructure

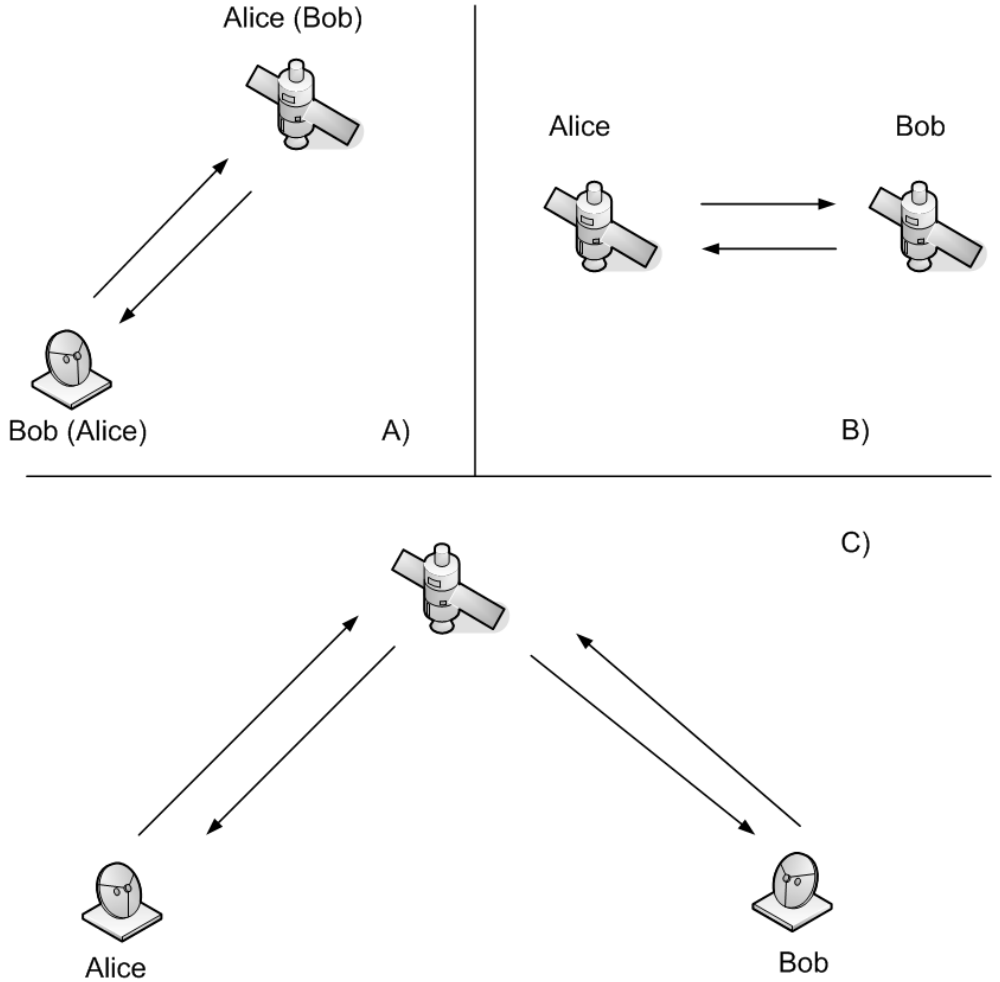
- A pan-European infrastructure integrating quantum cryptography into conventional communication networks
- A terrestrial and space segment



Applications: Quantum Key Distribution (QKD), Time & Frequency distribution, etc.

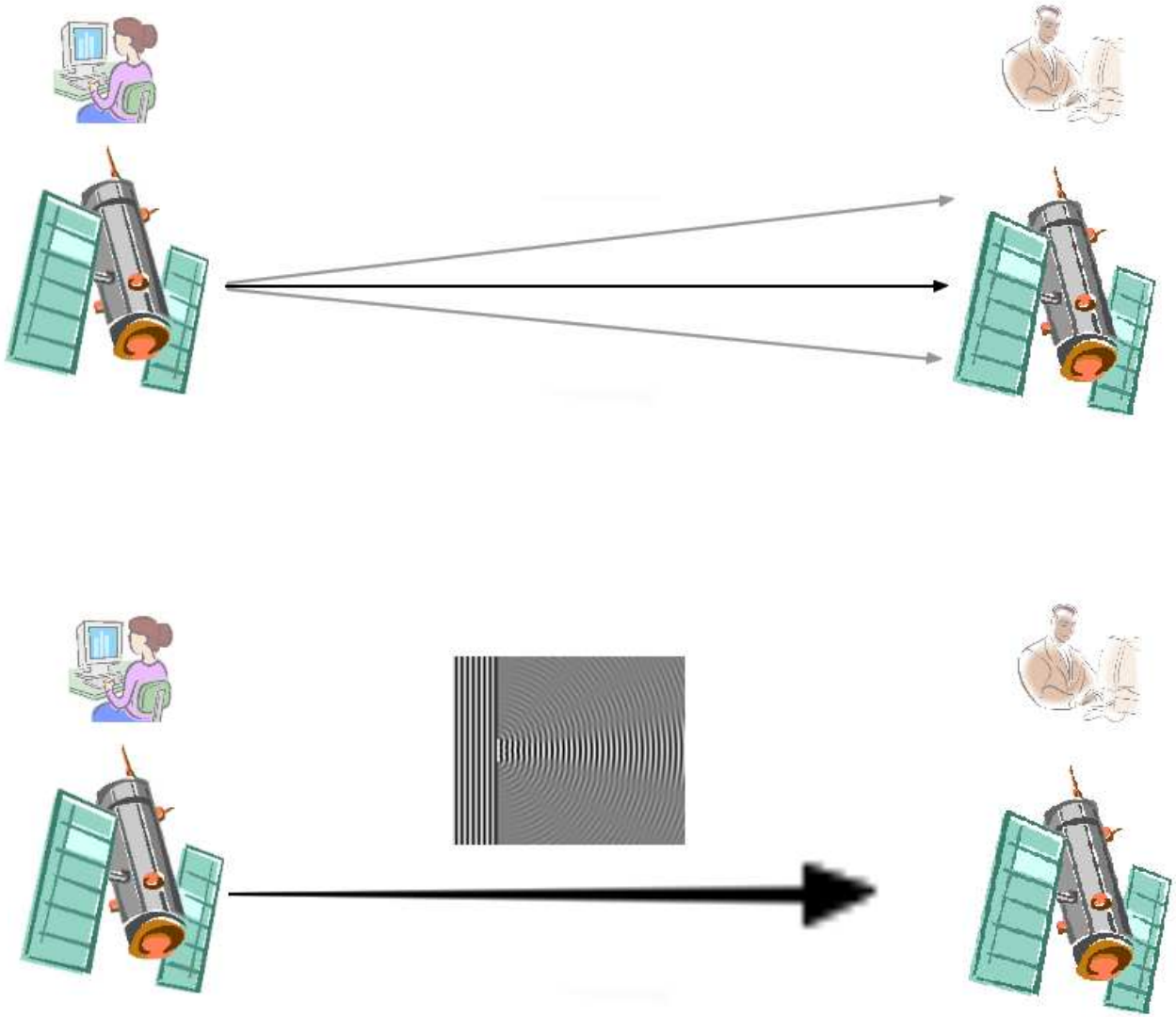


SATELLITE SYSTEMS

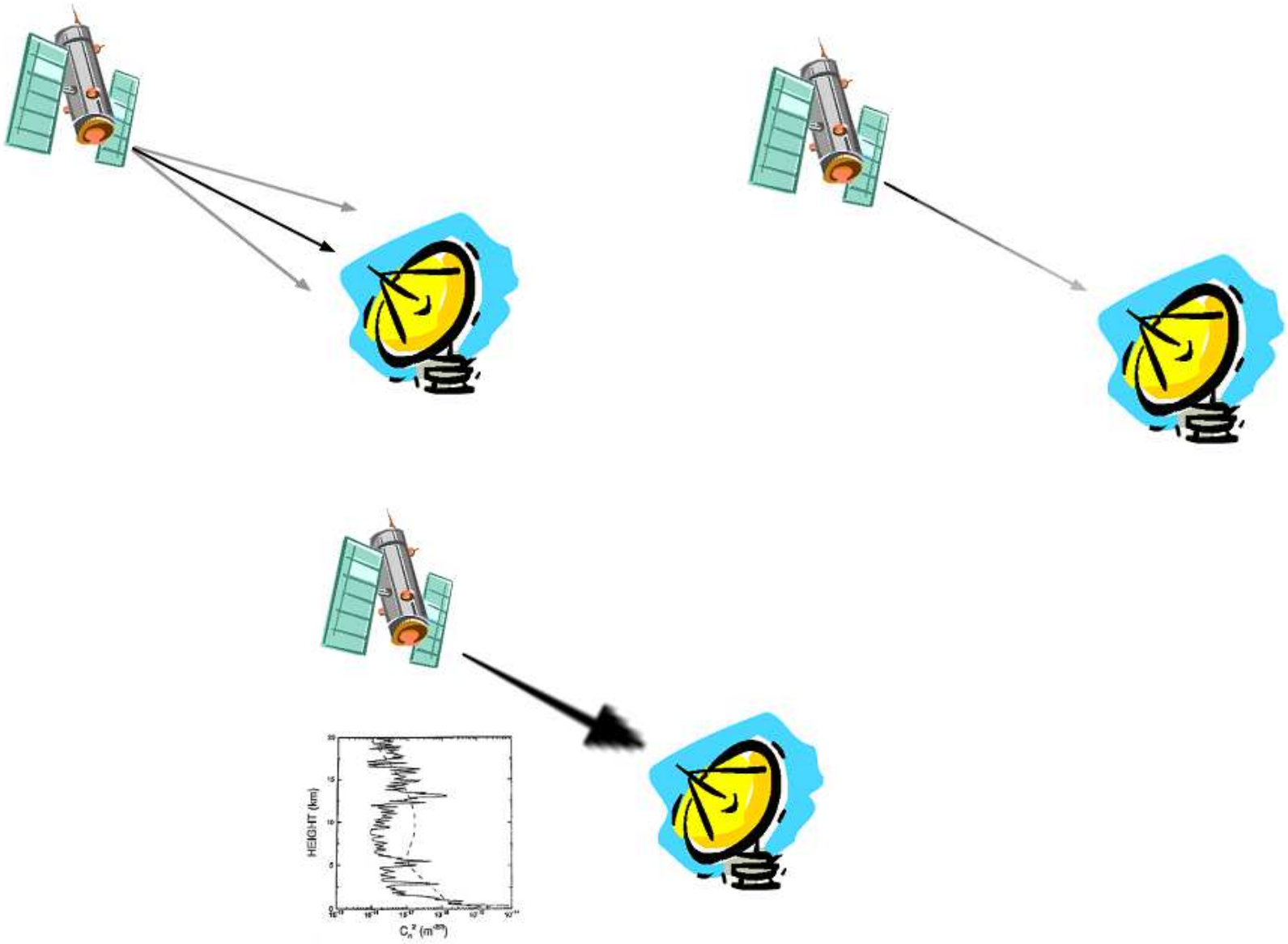


L. Bacsardi, „On the way to Quantum Based Satellite Communication”, IEEE Communications Magazine, 51:(08) pp. 50-55.

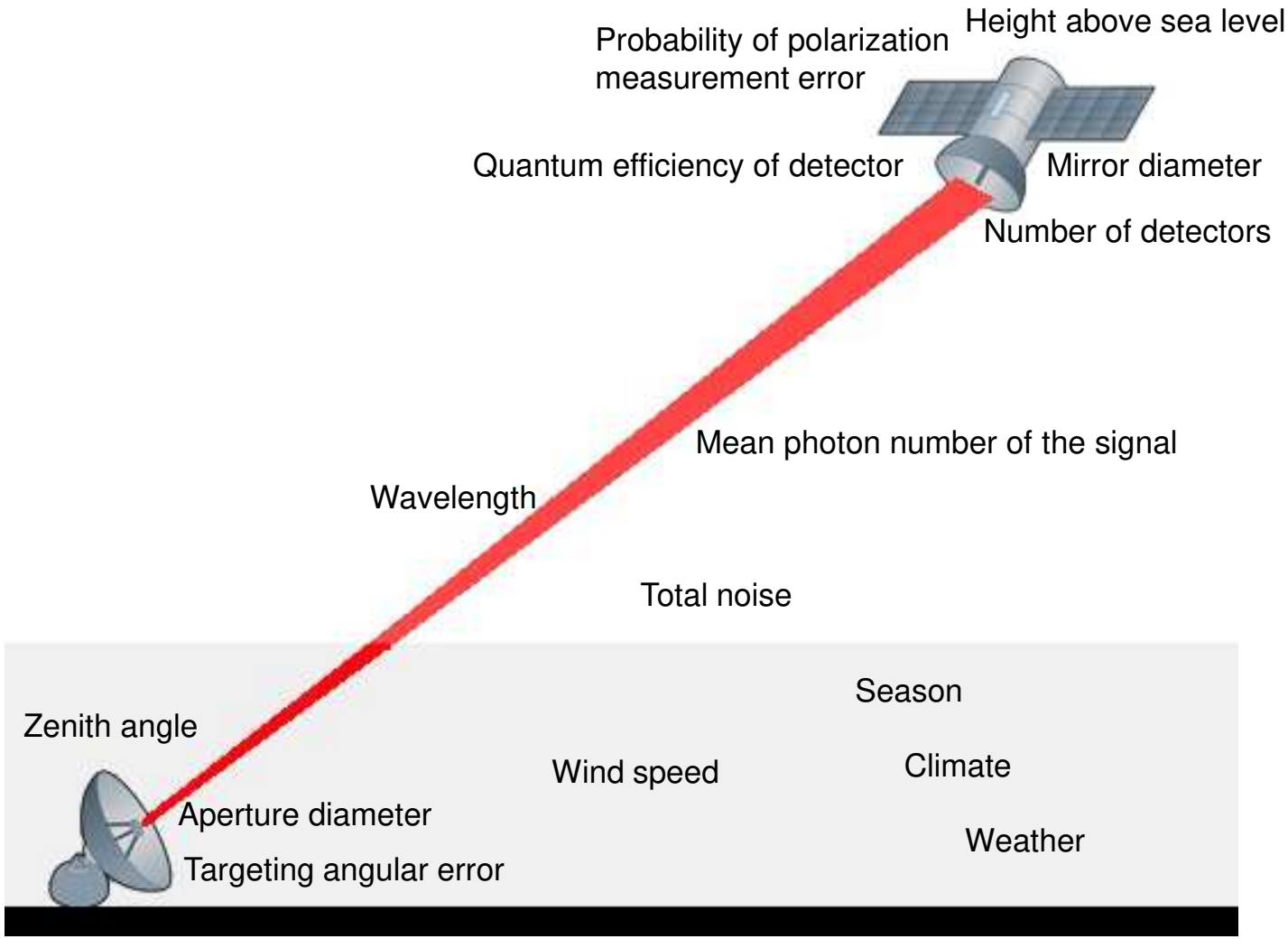
SPACE-SPACE COMMUNICATION



SPACE-GROUND COMMUNICATION

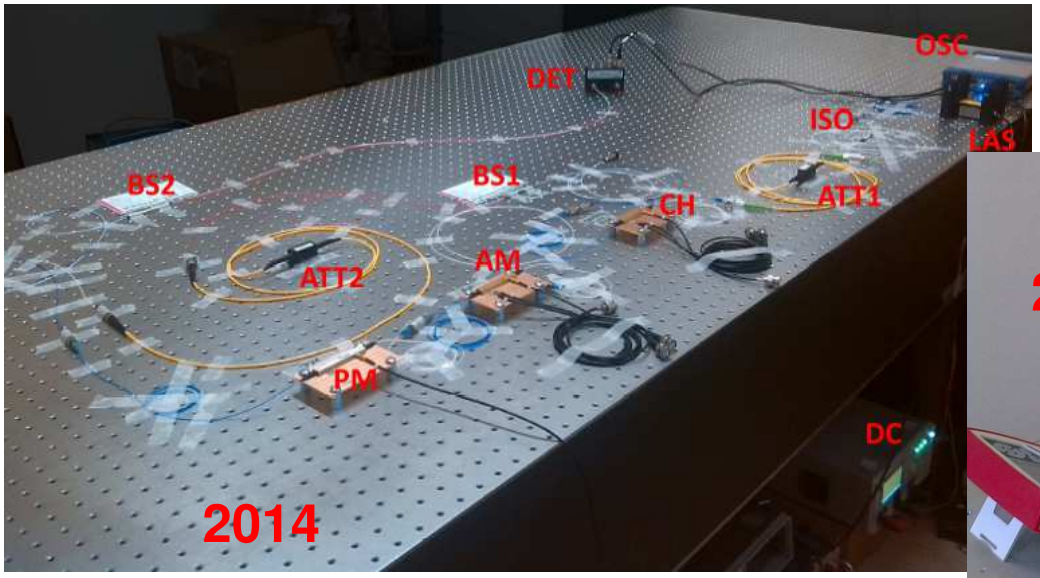


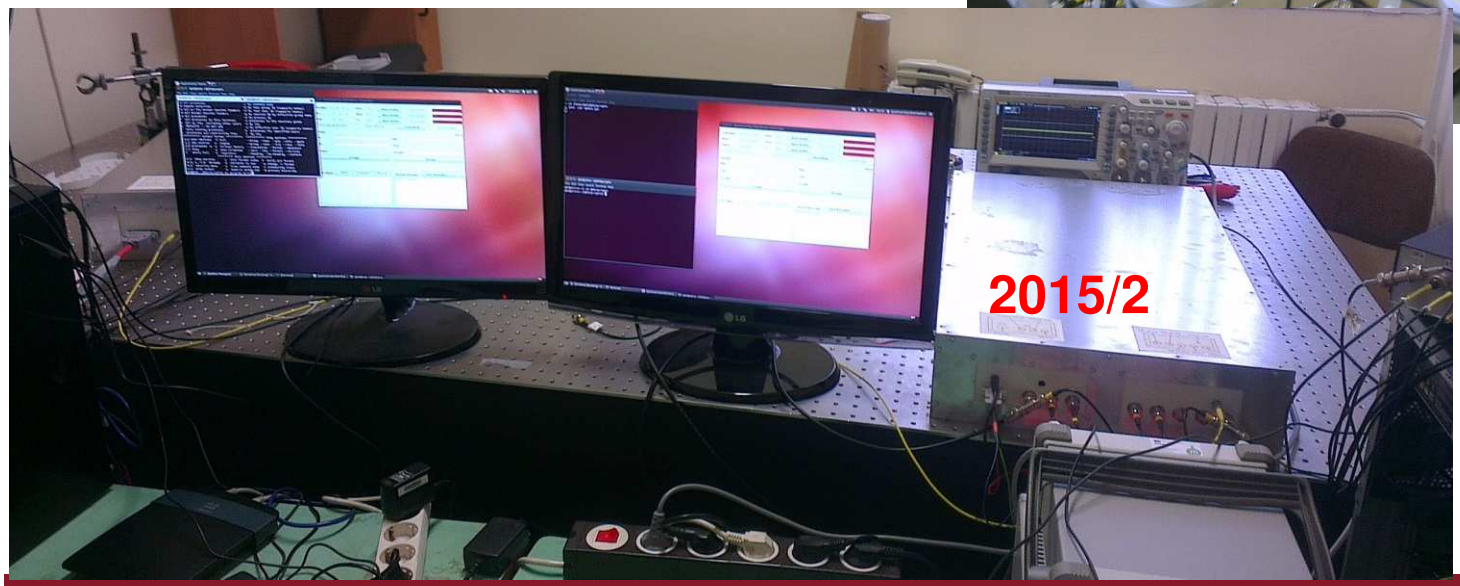
PARAMETERS NEEDED

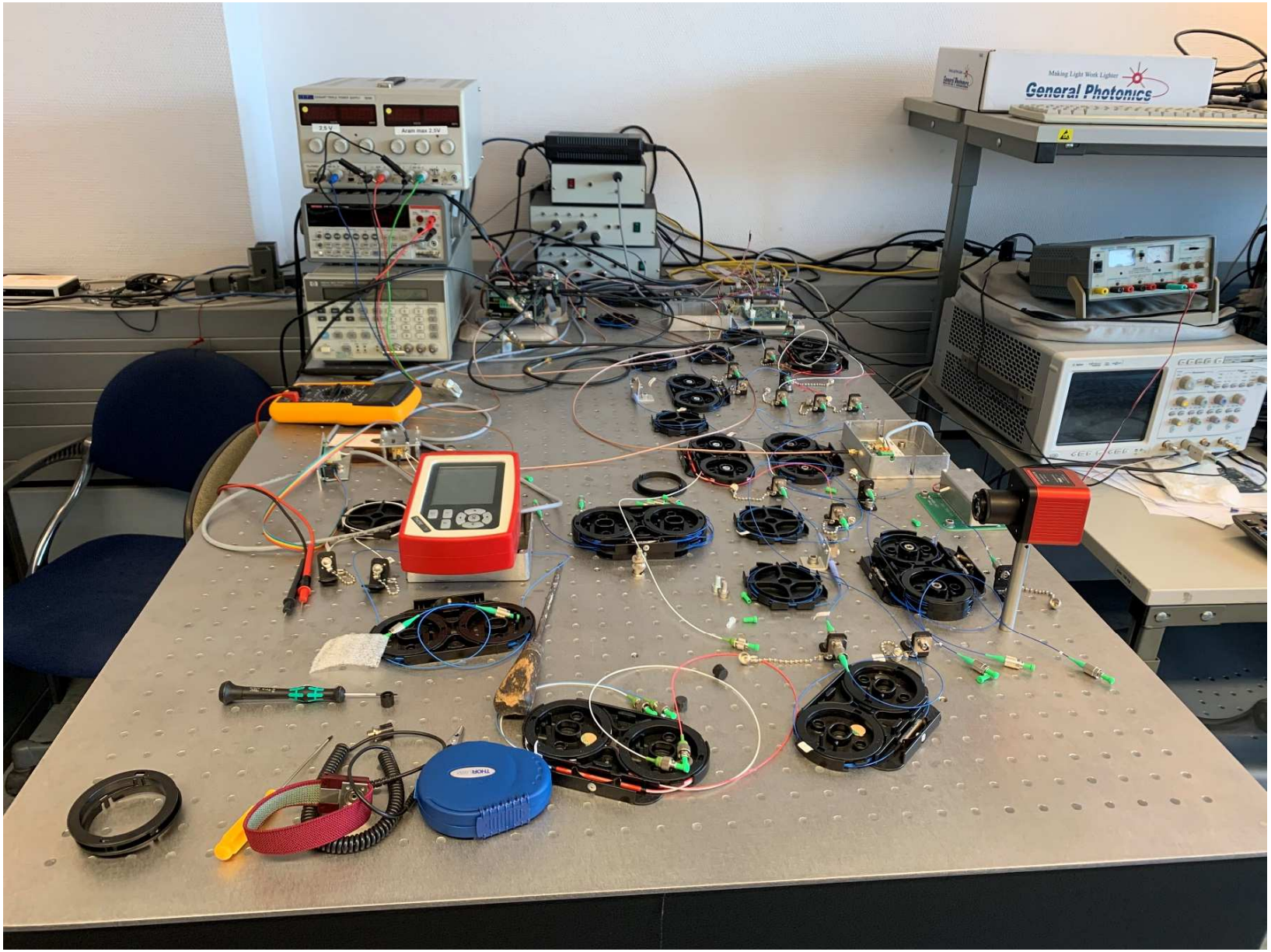


L. Bacsardi and S. Imre, “Supporting Space Communications with Quantum Communications Links”, Global Space Exploration Conference. Washington D.C., USA, 2012, Paper 12300.

AS WE DO IT...






General Photonics


LASER in
Signal out
Status 1
Status 2
Status 3
Status 4
CPU Power
Reset
Power
CVQKD–ALICE
Signal in
Status 1
Status 2
Status 3
Status 4
Power
CVQKD–BOB

FIBER-BASED NATIONAL RECORD

MŰEGYETEM 1782

Sajtóközlemény

Távolsági rekordot döntöttek a Kvantuminformatikai Nemzeti Laboratórium kutatói

Budapest, 2022. május 26. – A Budapesti Műszaki és Gazdaságtudományi Egyetem (BME) Villamosmérnöki és Informatikai Kara és a Wigner Fizikai Kutatóközpont között új hazai távolsági rekordot állítottak fel a kvantum alapú kulcsszétosztás területén saját fejlesztésű eszközükkel a Műegyetem kutatói.

A világban jelenleg is zajló kvantumtechnológiai forradalo
a nemzetközi színvonalú kutatócsoportokat és laborat
feldolgozott témákat tömörítő Kvantuminformatika Nemz
célokra épülő szinergiát teremt a tudományos munkában r
között.

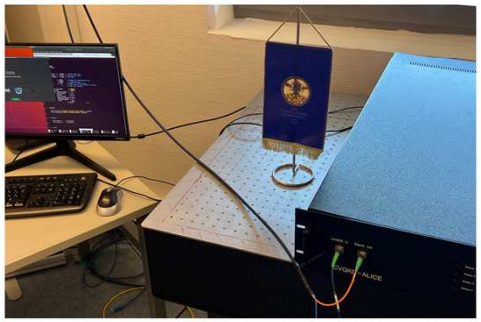
A BME KUTATÓI HAJTOTTÁK VÉGRE A JÖVŐ KVANTUMHÁLÓZATÁNAK ELSŐ SIKERES MAGYARORSZÁGI TESZTJÉT

05.02. / TUDOMÁNY /

telex

Magyar kvantumkommunikációs rekordot döntöttek a BME kutatói

TUDOMÁNY TECH 2022. május 26. – 16:49



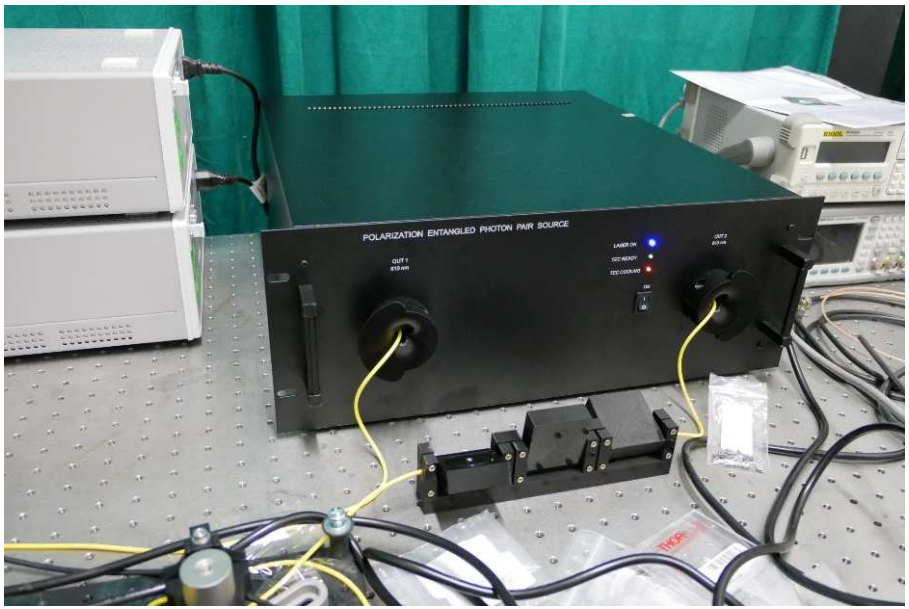
A kísérletben használt berendezés – Forrás: BME

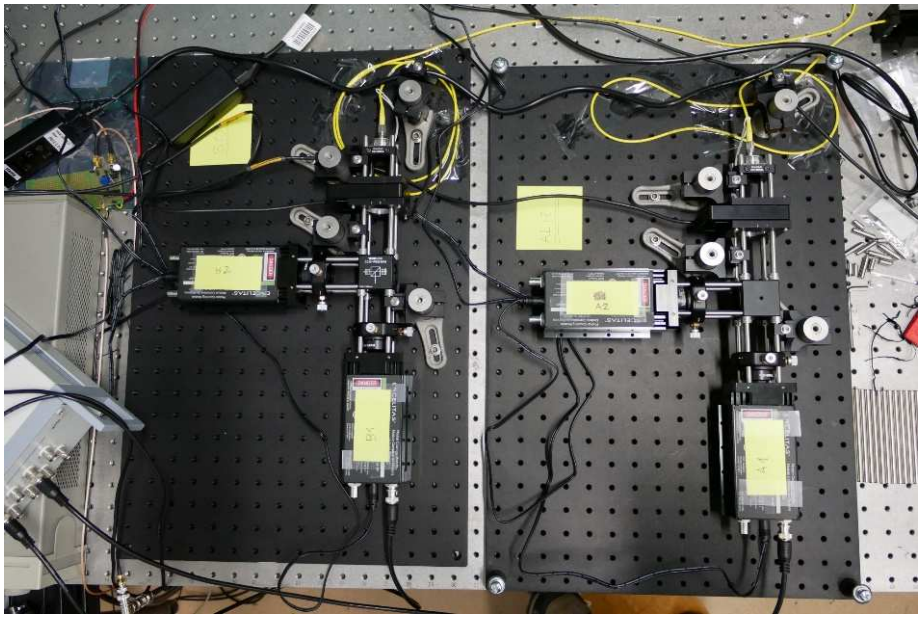
Bolcsó Dániel

Másolás

A Budapesti Műszaki és Gazdaságtudományi Egyetem (BME) Villamosmérnöki és Informatikai Kara és a Wigner Fizikai Kutatóközpont között új hazai távolsági rekordot állítottak fel a kvantumalapú kulcsszétosztás területén saját fejlesztésű eszközükkel a BME kutatói. A kísérlet sikeressége nemcsak azt mutatta meg, hogy nagy távolságokon is megfelelően működik a magyar fejlesztésű kvantumkulcsszétosztó rendszer, hanem jelentős mérföldkő egy budapesti nagyvárosi kvantumkommunikációs hálózat kialakításához vezető úton – írja közleményében az egyetem.

FREE-SPACE QKD EXPERIMENT





DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES

www.hit.bme.hu

FREE-SPACE QKD EXPERIMENT
MAY 19, 2022

© Department of Networked Systems and Servi

SUMMARY

- Quantum mechanics offers unique possibilities for engineering problems.
- Efficient quantum algorithms are available.
- Quantum computers in their childhood, but something is happening.
- There are many available quantum communications products on the market (QRNG, QKD)

QUANTUMCOMMUNICATIONS IN SOCIAL MEDIA

https://www.facebook.com/kvantumkommunikacio

https://linkedin.com/company/kvantumkommunikacio

USEFUL LINKS

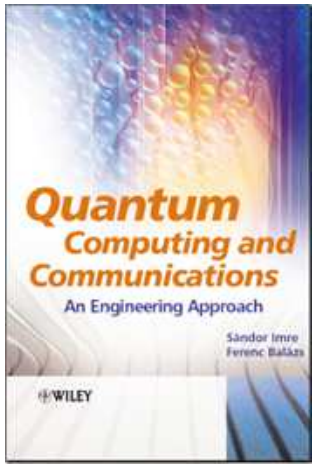
Quantum Information National Laboratory
https://qi.nemzetilabor.hu/

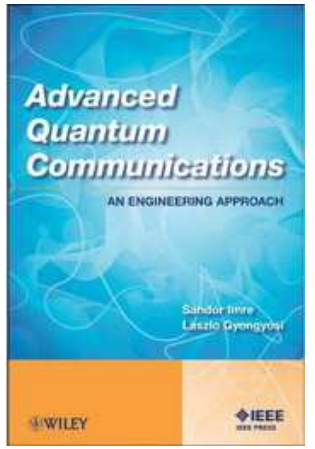
Quantum Information National Laboratory HUNGARY

Quantum Technology Flagship: http://qt.eu
Quantum Technology in Space: http://qtspace.eu

Hungarian Quantum Technology Flagship:
https://wigner.mta.hu/quantumtechnology/en

Our website: http://mcl.hu/quantum





SUPPORT

This research was supported by the Ministry of Culture and Innovation and the National Research, Development and Innovation Office within the Quantum Information National Laboratory of Hungary (Grant No. 2022-2.1.1-NL-2022-00004).

László Bacsárdi's research is supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

L. Bacsárdi's work is supported by the ÚNKP-22-5 New National Excellence Program of the Ministry for Innovation and Technology from the source of the National Research Development and Innovation Fund.

bacsardi@hit.bme.hu