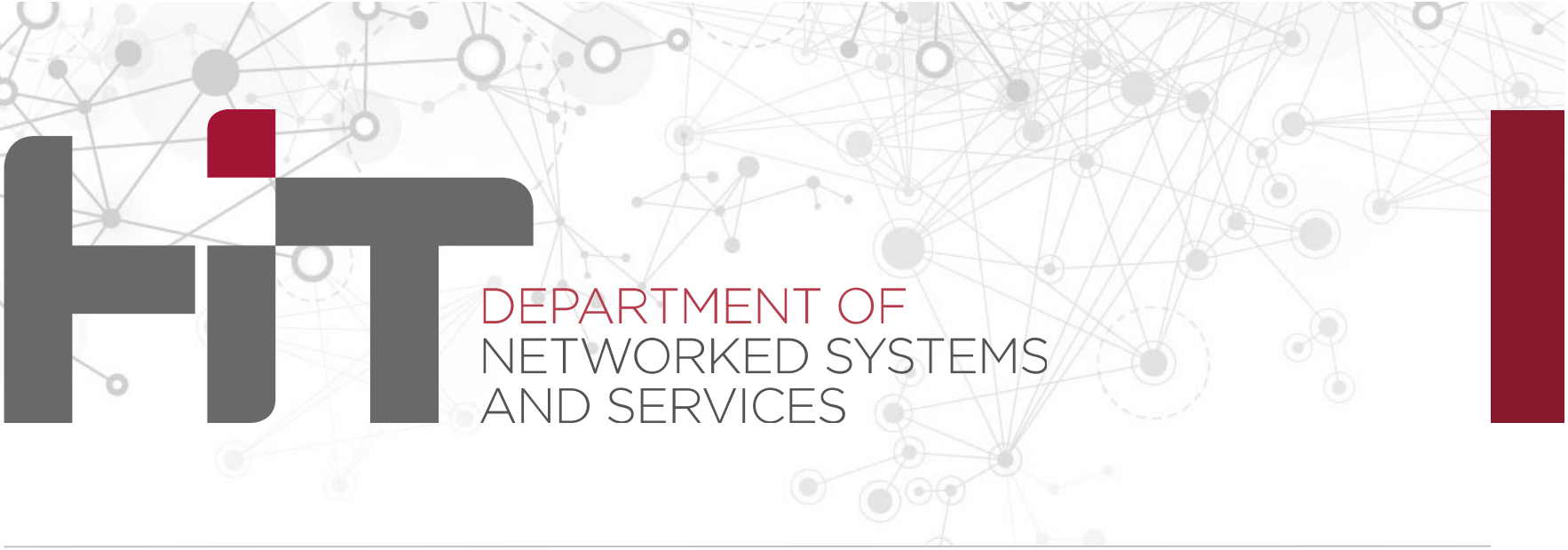


A Short Introduction to Quantum Computing and Communications

László Bacsárdi, PhD

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

Dec 6, 2018


quantum
European
flagship
Commission
billion
industry
communication
initiative
computing
research
Europe
Commissioner
years
sensing
part
Dutch
launch
future
markets
technological
revolution
strategy
sources
development
Technologies
Research
technology
Oettinger
market
Programme
scientific
science
leadership
expected
already
notably
secure
EU
public
second
like
blogpost
work
world-class
available
support
outlined
academia
theory
opportunities
investment
key
put
imaging
FET
Manifesto
effort
simulation
engineering
around
ambitious

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.

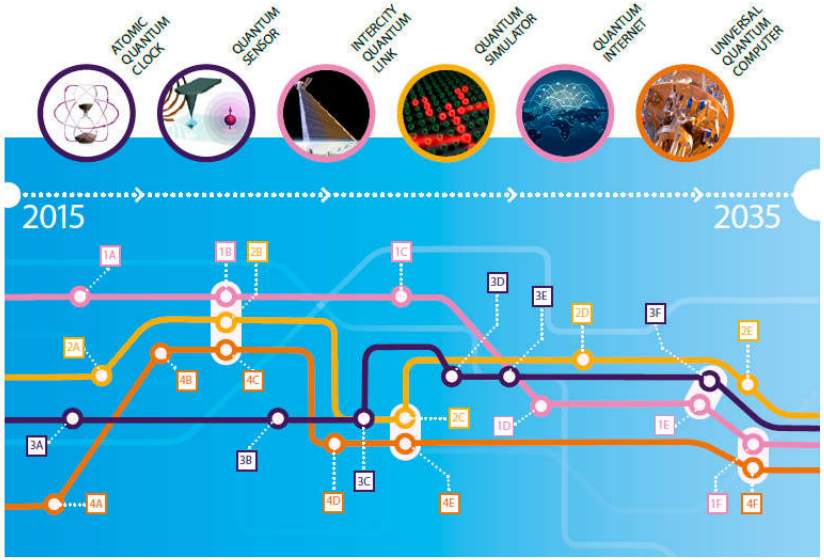
LEARN MORE

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

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

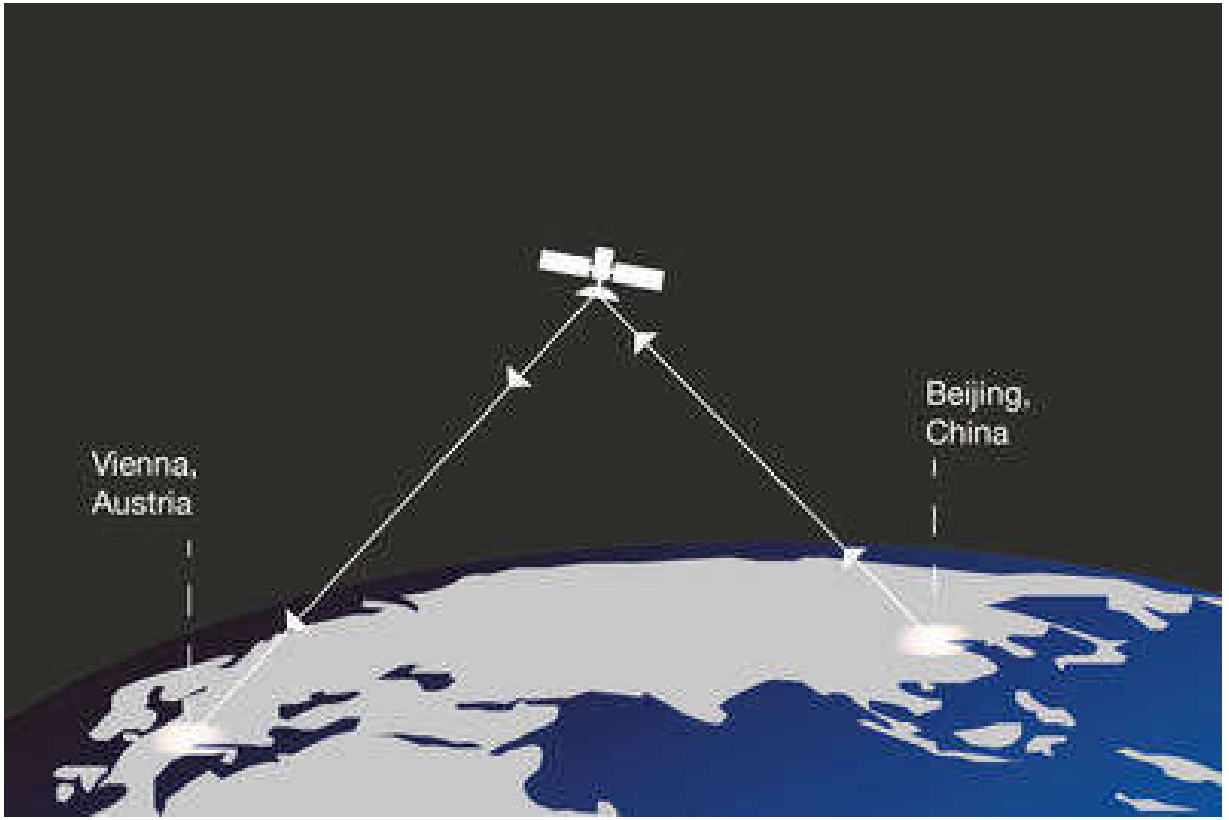
‘Much better than expected’: Chinese ‘hack-proof’ quantum communication satellite put into service

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.

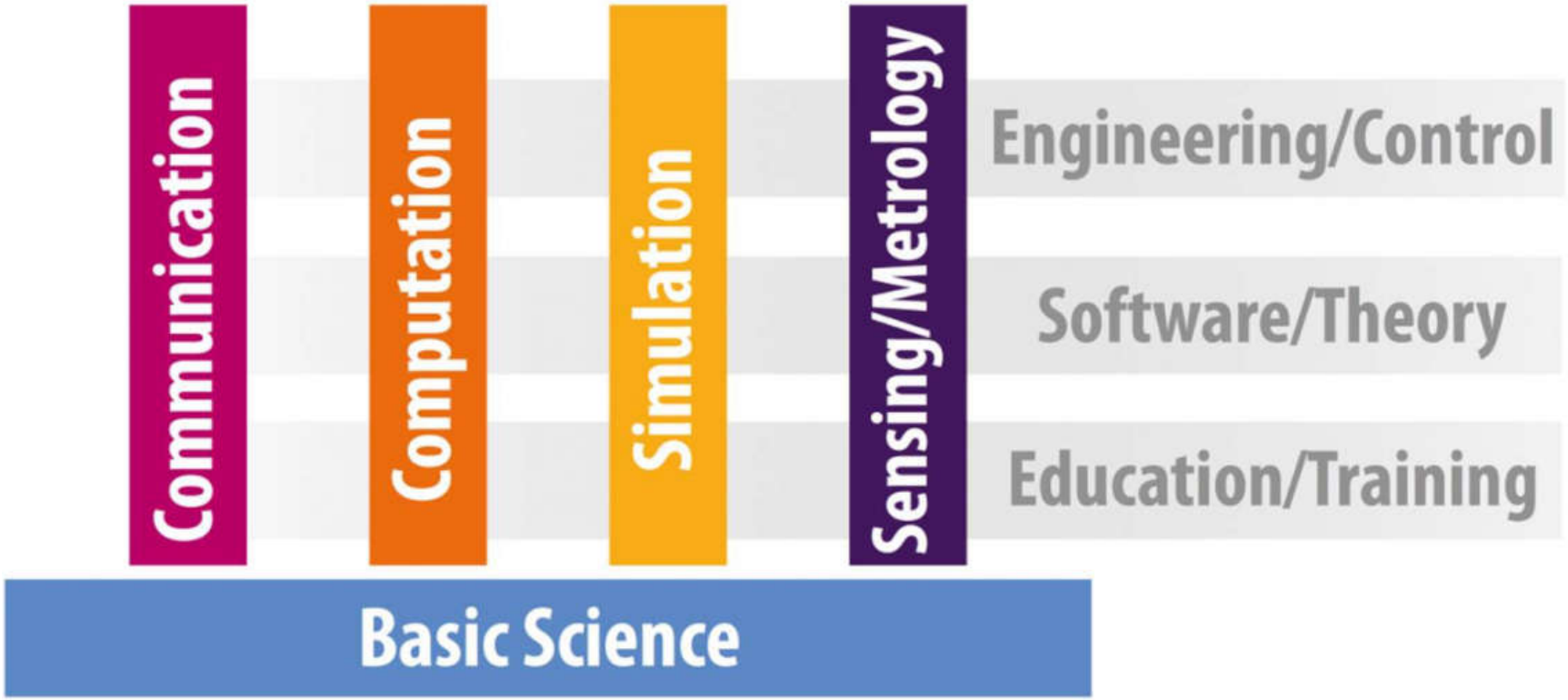
Source of image: https://www.rt.com/news/374167-china-quantum-satellite-operational/


Vienna,
Austria
Beijing,
China

Quantum Manifesto

A New Era of Technology

May 2016



QTSPACE Organization Working Groups Activities Mobility News Dissemination Publications Members

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 landmarl
Quantum theory and space science form buildi
research framework for exploring the **boundari**
through the unique working conditions offered
performed in space.

⟨InfiniQuant⟩

Infos | Projects | Community | Ressources/Media | Contact | News

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...

Quantum Encryption and Science Satellite (QEYSSat)

Principal Investigator Professor Thomas Jennewein

Institute for Quantum Computing (IQC) researcher Thomas Jennewein is pioneering new applications for quantum technologies, in particular quantum communications networks in space.

DOWNLOAD
QUANTUM SCIENCE HEADING TO SPACE »

Recent media

04/27/17 - Press release from Innovation, Science and Economic Development Canada

02/02/17 - Wired article by Sophia Chen

12/22/16 - "We've got photons!"

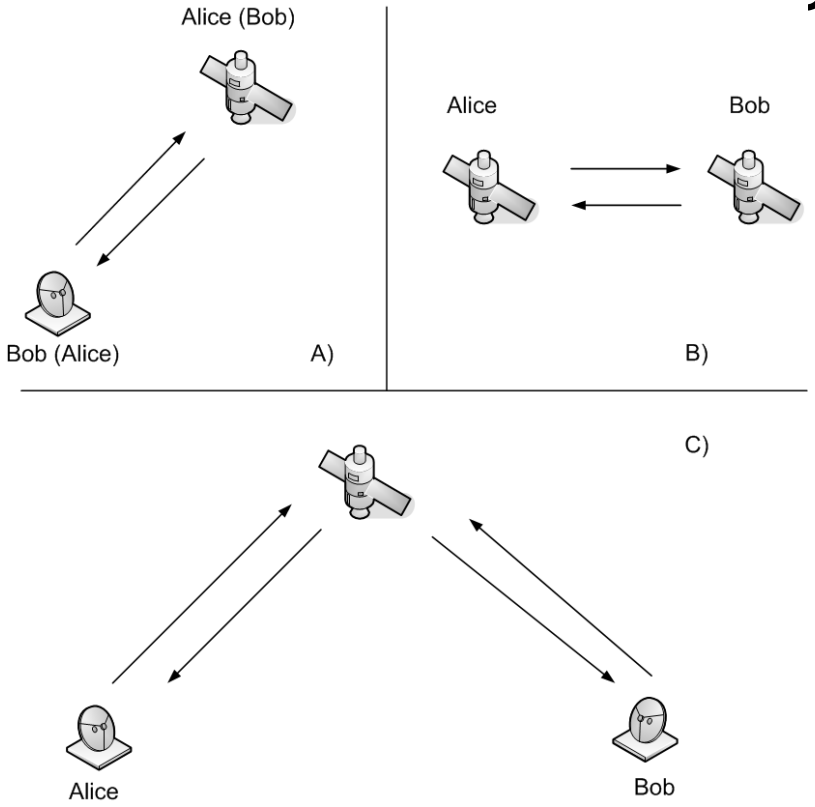
12/21/16 - Researchers successfully demonstrate prototype for space-based quantum-secured communication

12/20/16 - Globe and Mail article by Ivan Semeniuk

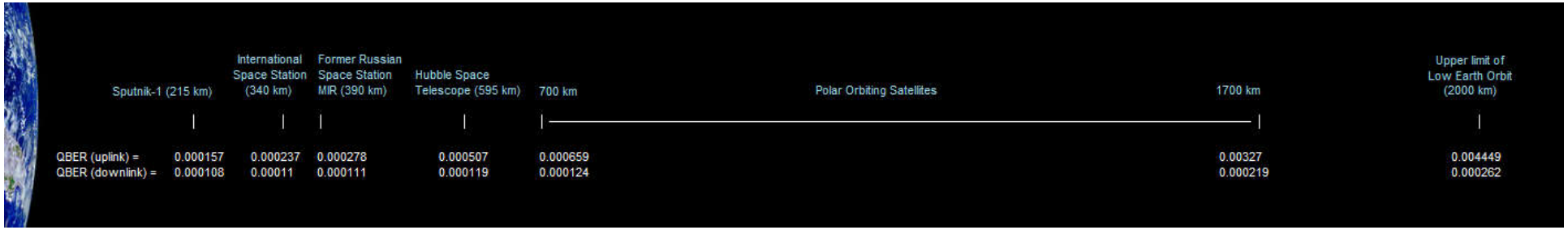
09/12/16 - IQC researchers successfully conduct airborne demonstration of quantum key distribution

05/05/16 - IQC researcher awarded CSA grant to demonstrate quantum communications technologies aboard student space mission

QKD



The latest version of the Quantum Satellite Communication Simulator is available:
http://mcl.hu/quantum/simulator/



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

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

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

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

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

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

$$|\varphi\rangle = |0\rangle \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

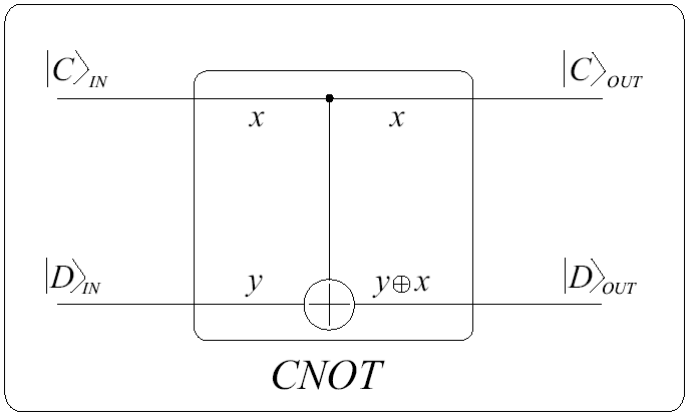
IMPORTANT CONSEQUENCES

- 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!

ENTANGLEMENT

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

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



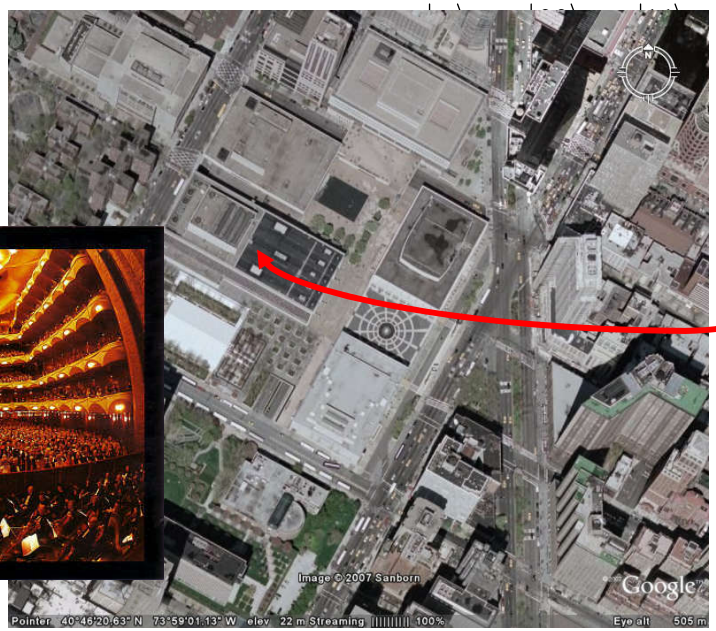
- Upper wire: control
- Lower wire: data

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

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

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

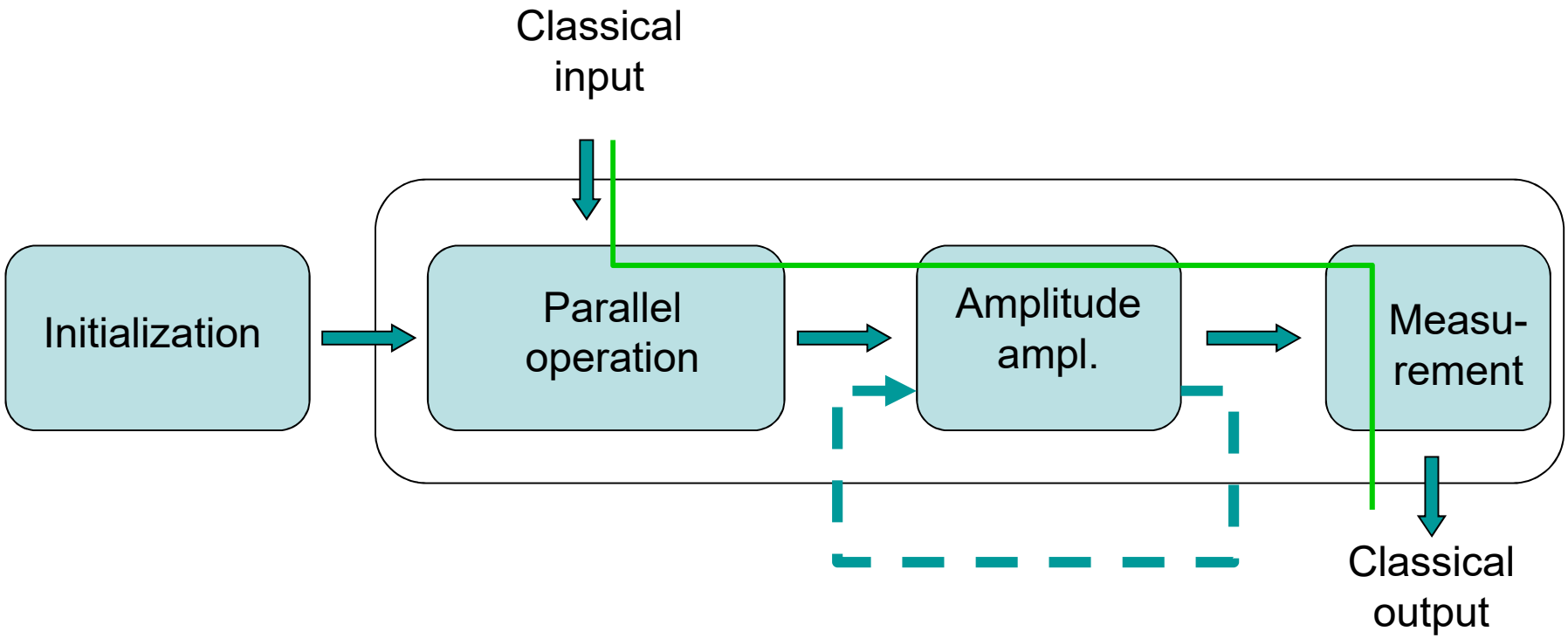
$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$



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

Application: Quantum Computing

GENERAL MODEL OF QUANTUM ALGORITHMS



HISTORY OF DATA BASE SEARCHING V1

What was the basic problem of the hunting/gathering prehistoric men?

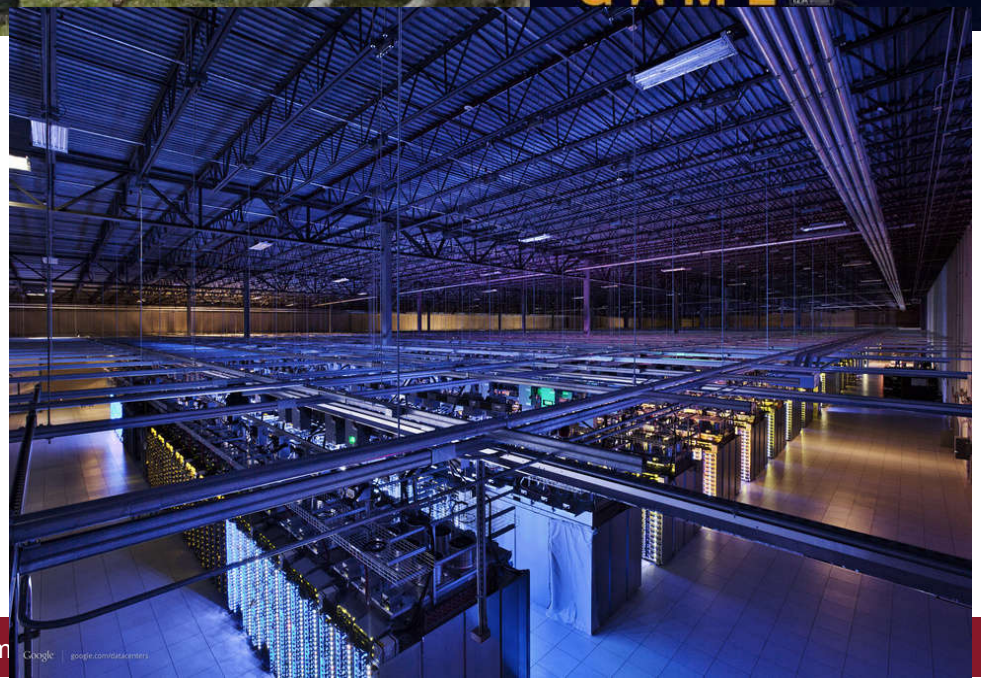
What is the reason?

How to solve it?

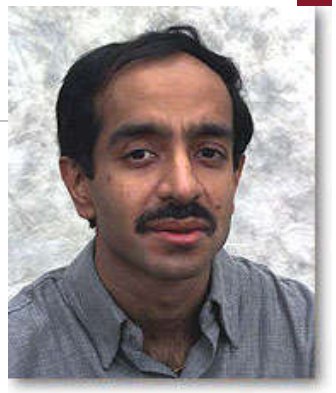
HISTORY OF DATA BASE SEARCHING V2

HISTORY OF DATA BASE SEARCHING V3

DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES
www.hit.bme.hu



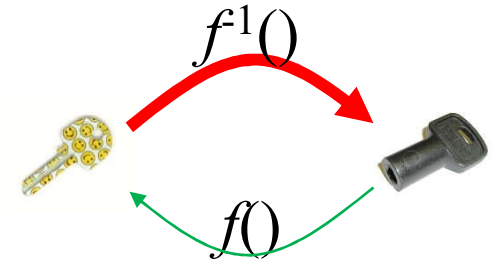
HISTORY OF DATA BASE SEARCHING V4

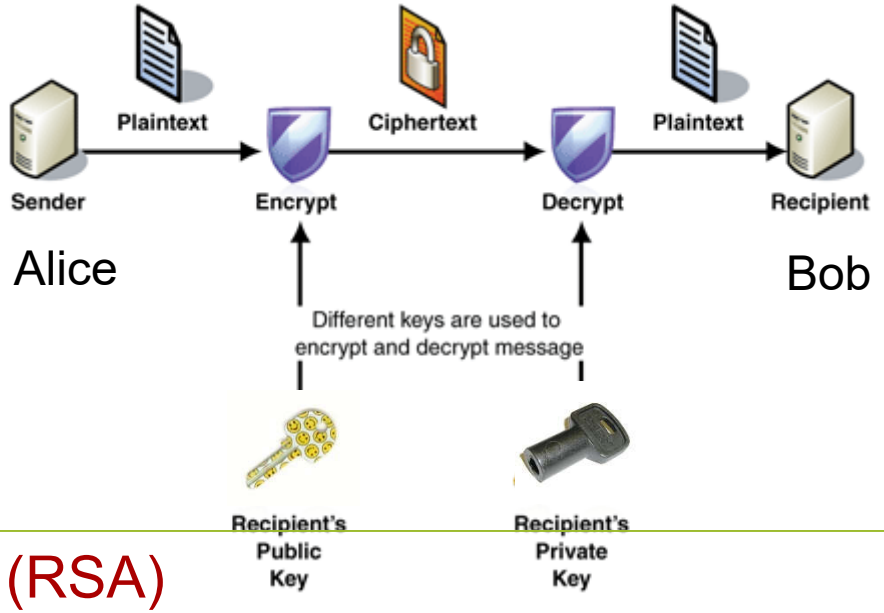


Lov Grover (1961-)

- Grover algorithm
- Unsorted date based with *N* different item. DB[*x*]
- Classical complexity?
- Quantum complexity: $O\left(\sqrt{N}\right)$
- Application areas are not restericted to computing
  - Optimal route selection in a large network
  - Signal detection, stc.

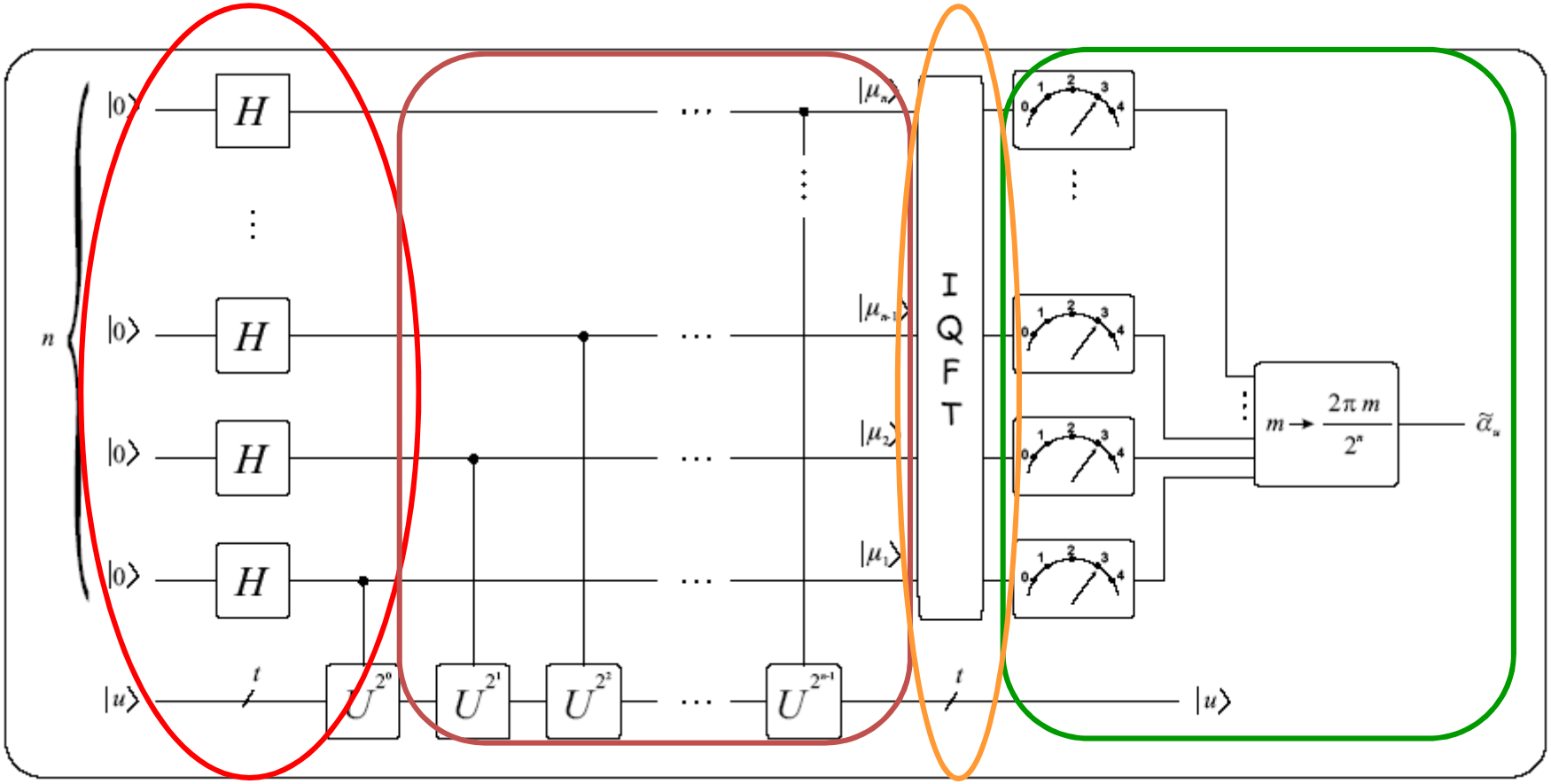
PUBLIC (ASYMMETRIC) KEY CRYPTOGRAPHY





- 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

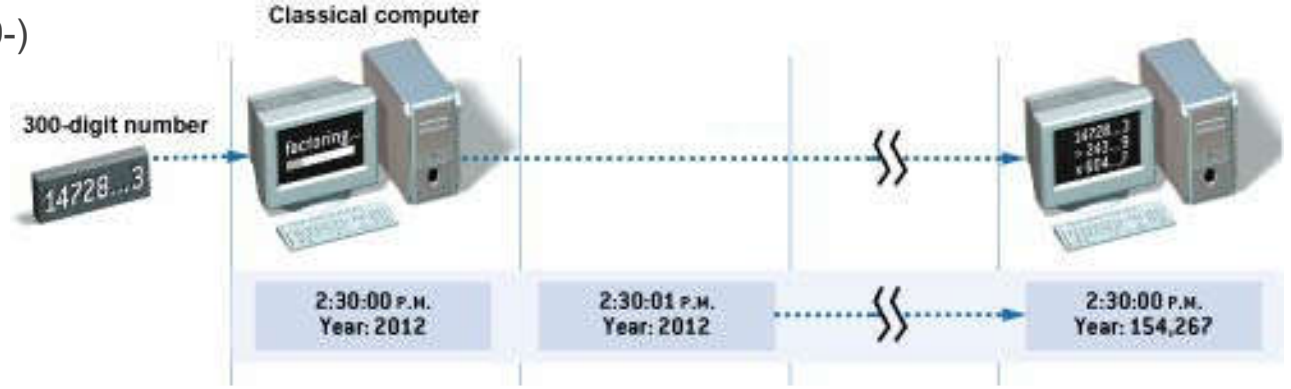


POWER OF SHOR'S ALGORITHM

Peter Shor (1959-)

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

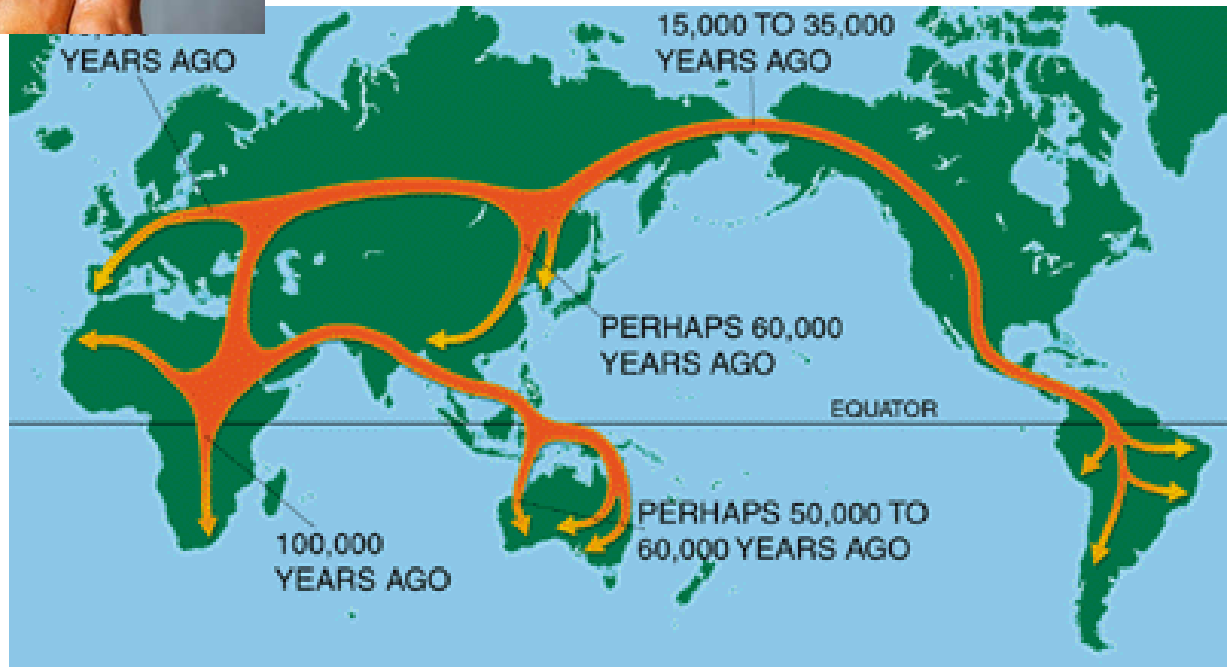
152 000 years



Adam (~ 150 000 BC)

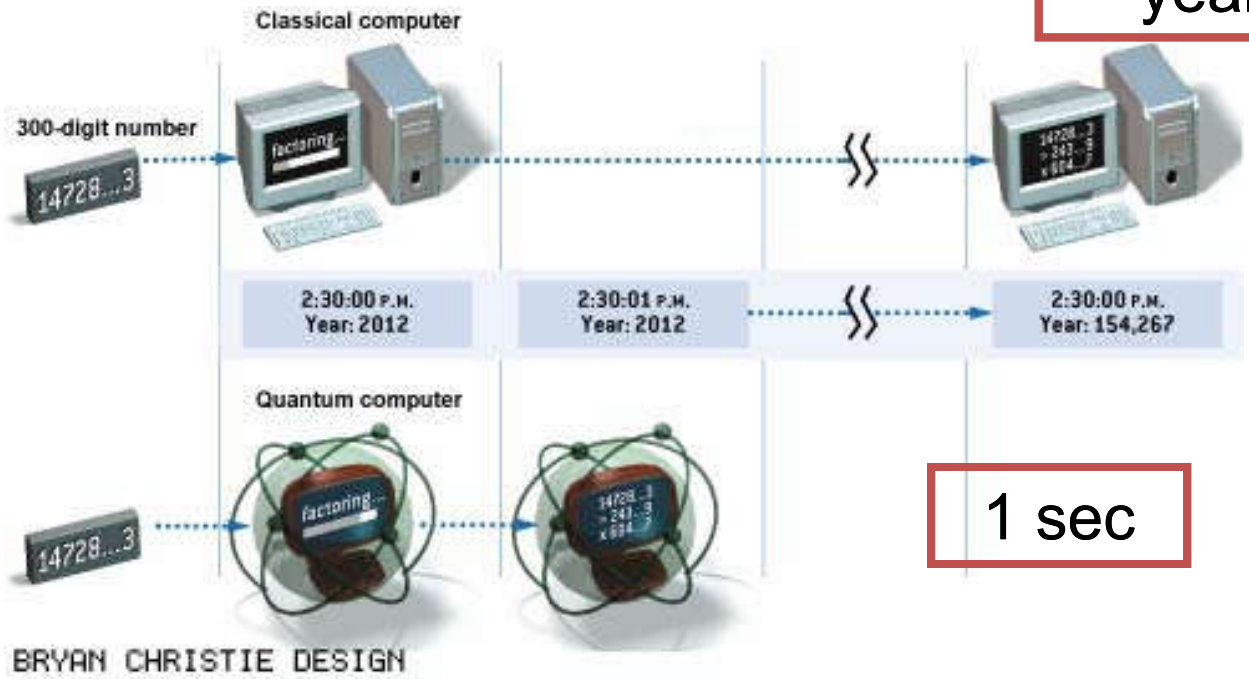
152 000
years

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!

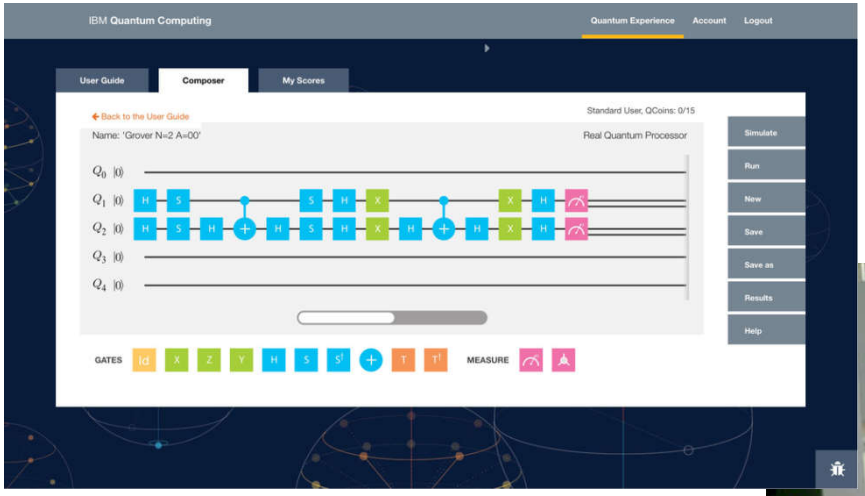
Arnold Schwarzenegger (1947-)

D-WAVE

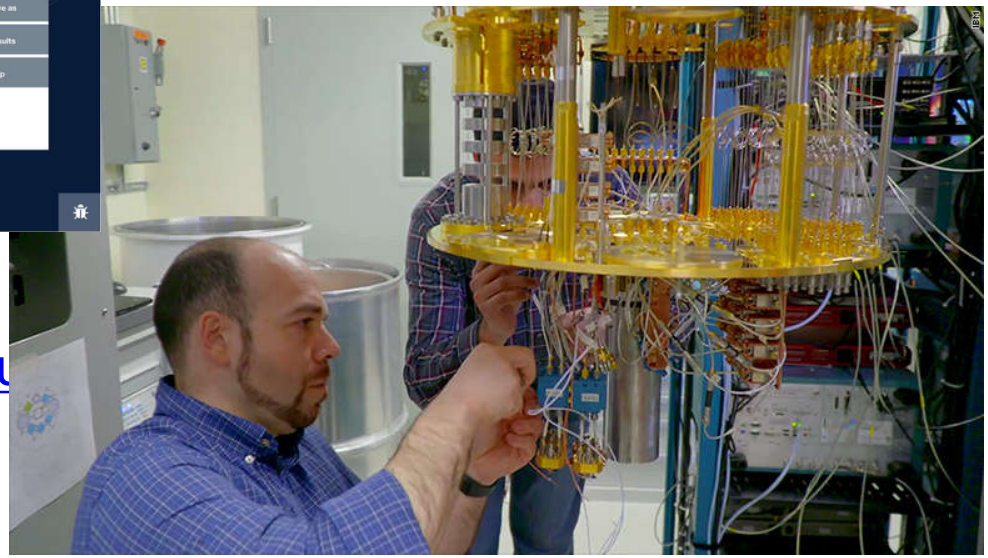
Jan 2017: D-Wave2000Q

D:wave
The Quantum Computing Company™

IBM QUANTUM COMPUTER ACCESS!



2016: 5 qubit



https://quantumexperience.ng.blu

2017: 16 qubit

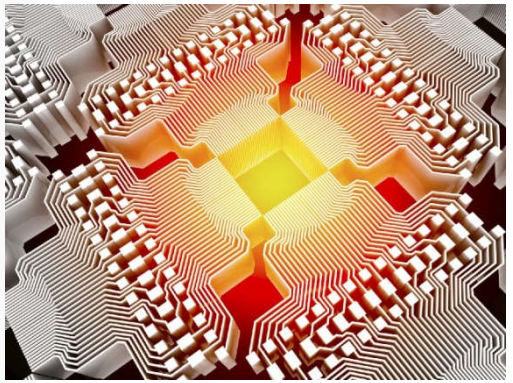
IBM Q Awards:

https://qx-awards.mybluemix.net/

MICROSOFT QUANTUM DEVELOPEMENT KIT

Quantum Programing language: Q#

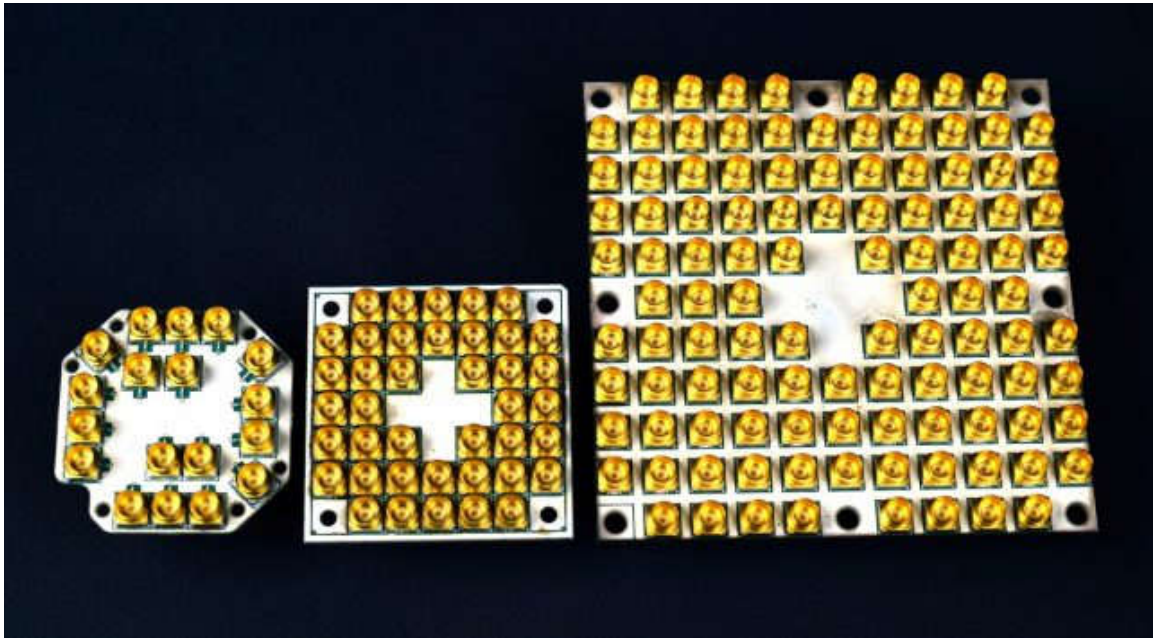
```
operation BellTest (count : Int, initial: Result) : (Int,Int)
{
    body
    {
        mutable numOnes = 0;
        using (qubits = Qubit[1])
        {
            for (test in 1..count)
            {
                Set (initial, qubits[0]);

                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);
    }
}
```



News 2018 !!!

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

INTEL



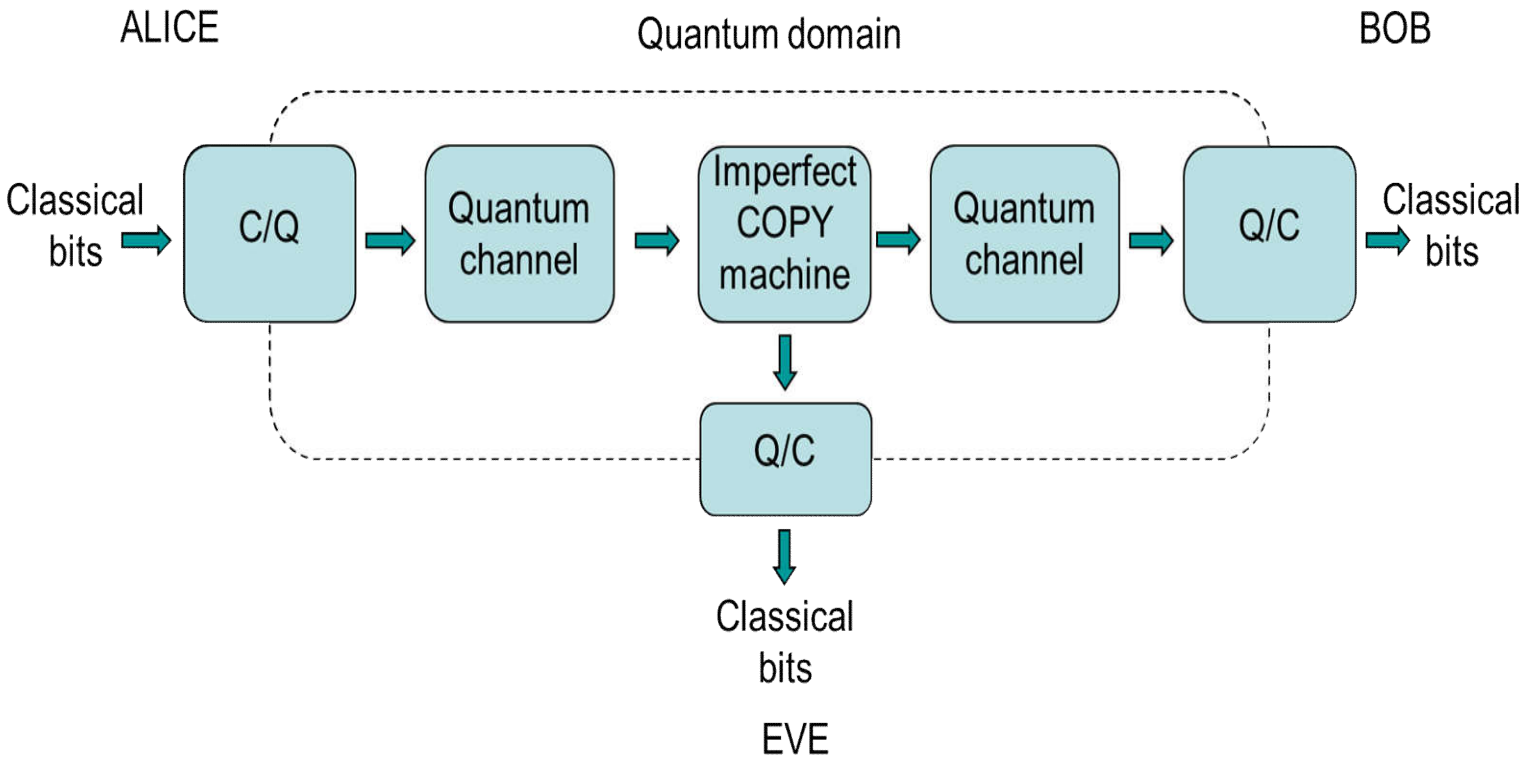
News 2018 !!!

Intel Corporation's 49-qubit quantum computing test chip, code-named "Tangle Lake," is unveiled at 2018 CES in Las Vegas.

https://www.extremetech.com/computing/261734-intel-unveils-new-quantum-computer-declares-quantum-breakthrough

Application: Quantum Key Distribution

BEHIND THE QKD



SEVERAL PROTOCOLS

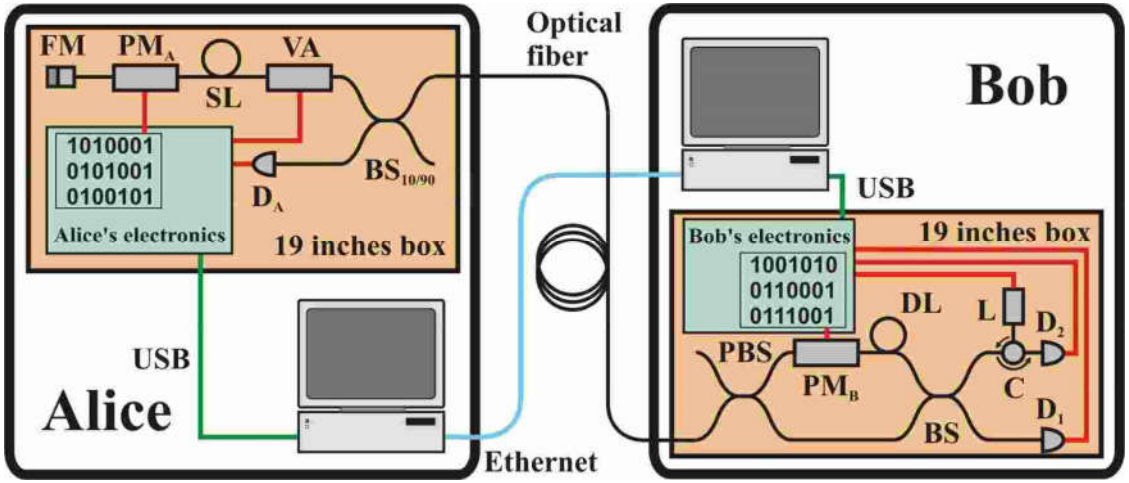
E91

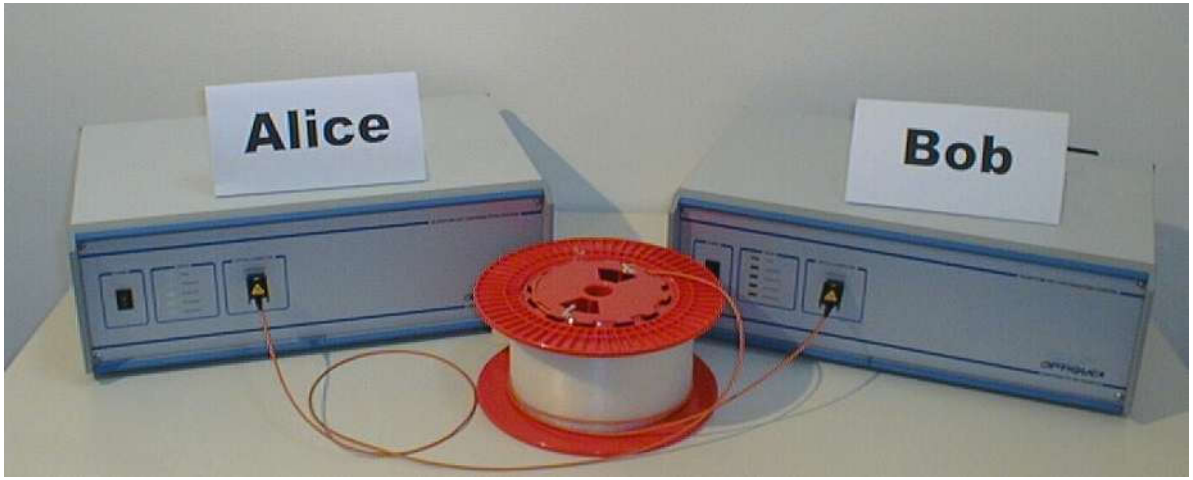
BB84

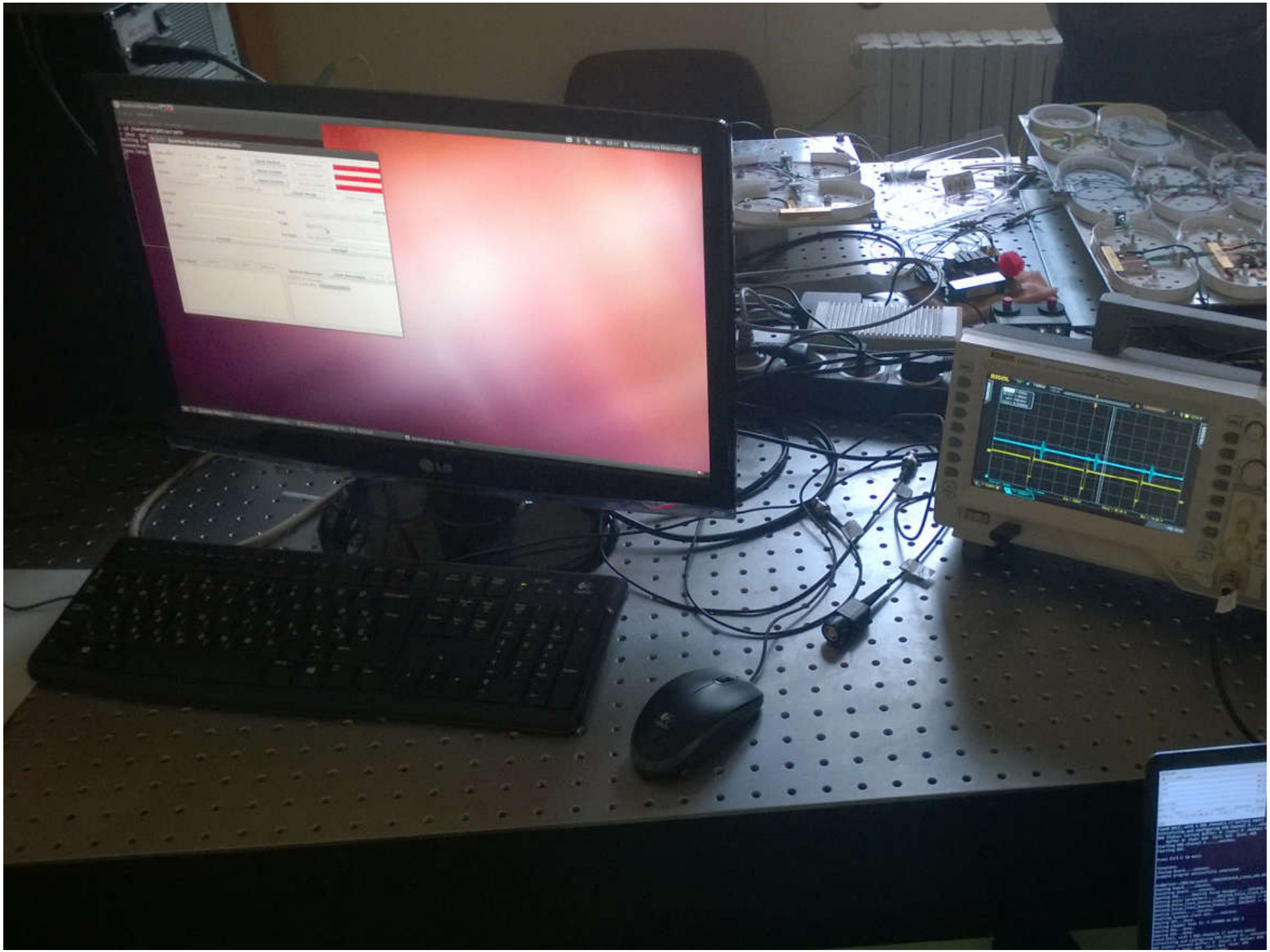
B92

S09

QKD IN PRACTICE

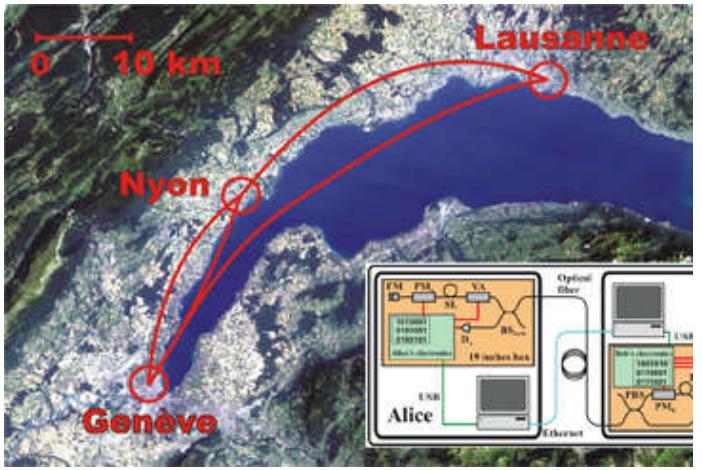




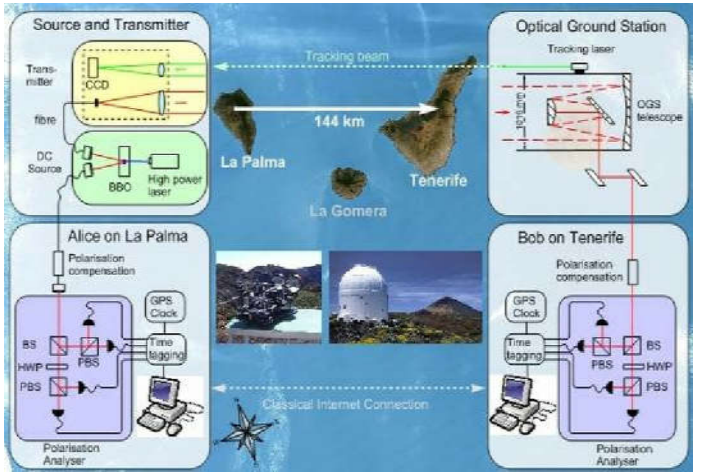


DISTANCES

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



SUMMARY

- Quantum mechanics offers unique possibilities for engineering problems.
- Efficient quantum algorithms are available.
- Quantum computers in their childhood, but something is happening.
- Quantum communications is ready for technology

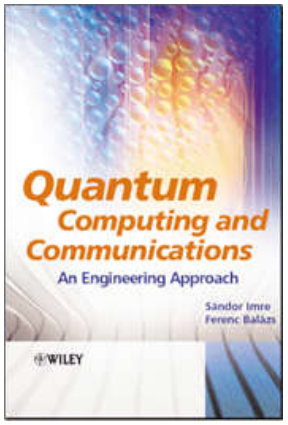
USEFUL LINKS

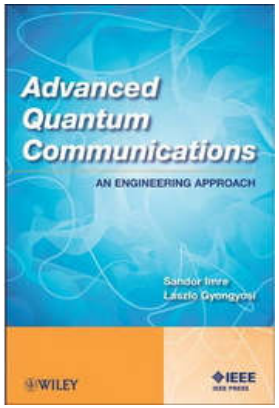
Quantum Technology Flagship: http://qt.eu

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

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

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





bacsardi@hit.bme.hu