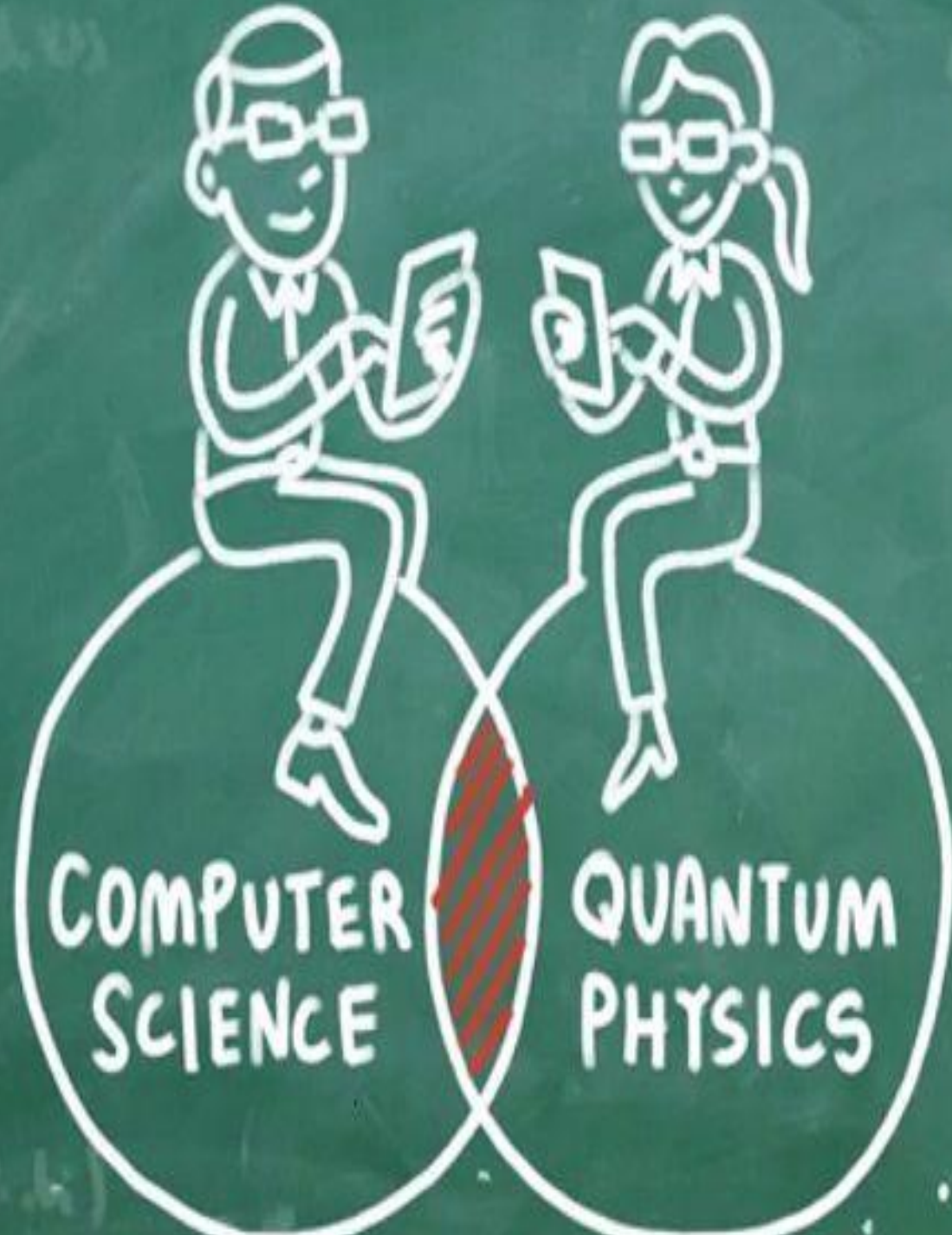




**Quantum
Computation**

Assoc. prof. Maria Nenova, PhD
Technical University of Sofia
e-mail: mariamnenova@gmail.com



COMPUTER
SCIENCE

QUANTUM
PHYSICS

PKC: the modern cryptography

- ▶ In 1970, public key cryptography enters;
- ▶ Each user has two keys – changeable;
- ▶ The encryption key is public;
- ▶ The decryption key is secret;
- ▶ Anyone can send a message, but only you can read it.

RSA алгоритъм

- ▶ The most widely used algorithm for PKC is **RSA**, based on the difficulty of finding the product divisor from two large prime numbers.

- ▶ **Easy task**

Two big prime numbers are given p and q

The product has to be calculated:

- ▶ **Hard task**

n is given,

What are p и q ?

$$n = p \times q$$

To find multipliers, the value of the multiplication of two prime numbers

- ▶ The best known algorithm takes time to reach the solution:

$$T(n) = \exp\left[c(\ln n)^{1/3} (\ln \ln n)^{2/3}\right]$$

- ▶ For p & q with a length of 65 digits $T(n)$ is approximately **one month** work of a cluster of working stations.
- ▶ For p & q with 200 digits $T(n)$ is astronomically big.

Quantum Computing Algorithm за разлагане

- ▶ 1994 Peter Shore from AT&T Bell Laboratory proves that quantum computers could, in seconds, carry out the division of multipliers even of very large numbers.
- ▶ The computing time for the Shore algorithm is

$$T(n) = O[(\ln n)^3]$$

After creation of quantum computers RSA method will no longer be secure!

Elements of Quantum Theory

- ▶ Light waves spread like discrete **quanta**, called **photons**.
- ▶ They have **no mass**, they have **energy**, momentum and angle are called **spin**.
- ▶ **Spin** shows polarization.
- ▶ If a polarizing filter is placed on its way, the photon will pass through it or it will be stopped.
- ▶ A detector can be used to check if the photon has passed through the filter.

Development of computing equipment

- ▶ First generation (1940–1956)
 - lamps
- ▶ Second generation (1956–1963)
 - Transistors
- ▶ Third generation (1964–1971)
 - Integrated circuits
- ▶ Forth generation (1971– now)
 - Microprocessors
- ▶ Fifth generation (now and in the future)
 - Artificial inteligence

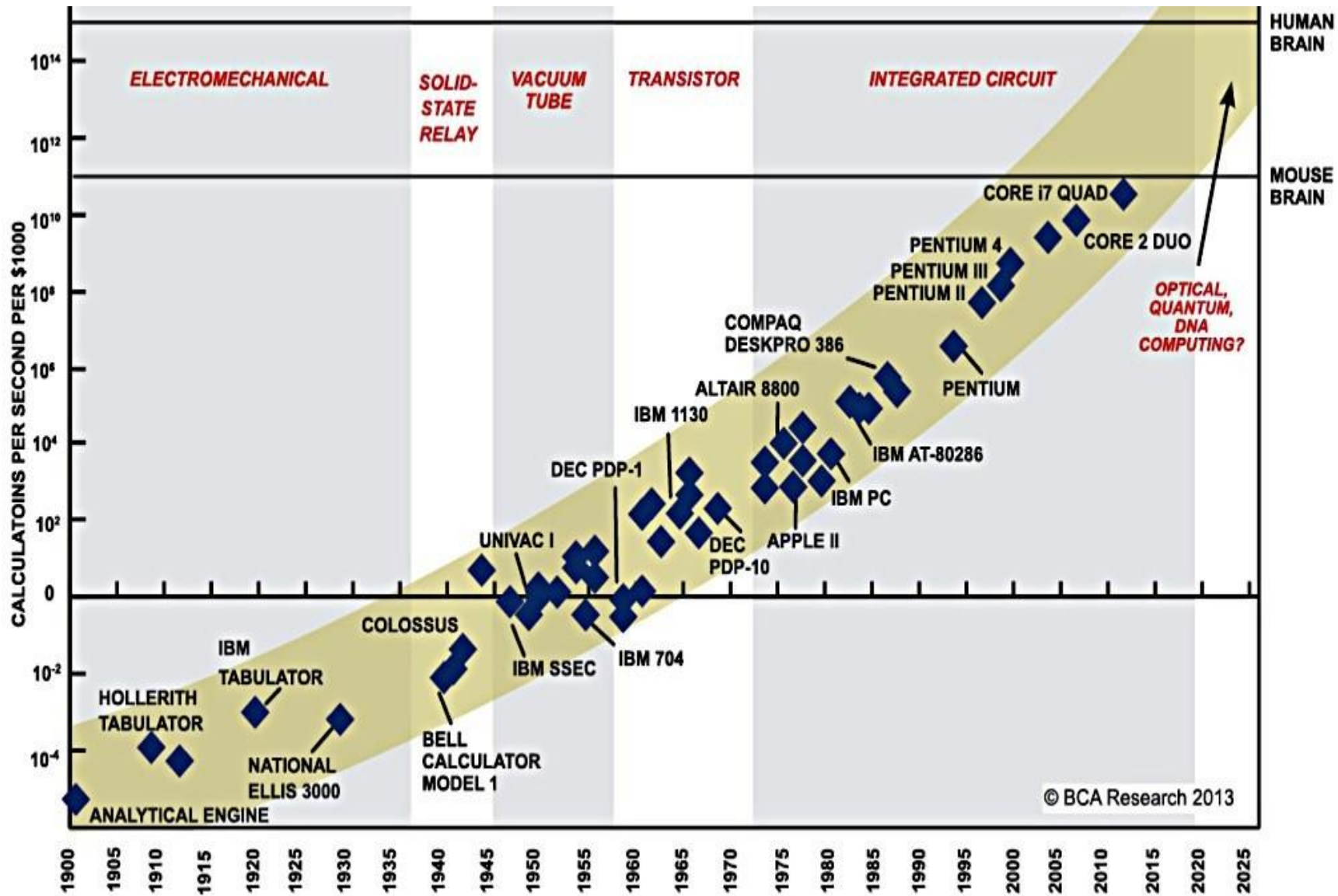


Why quantum computers?

"The number of transistors incorporated in a chip will approximately double every 24 months."

Gordon Moore, Intel Co-Founder



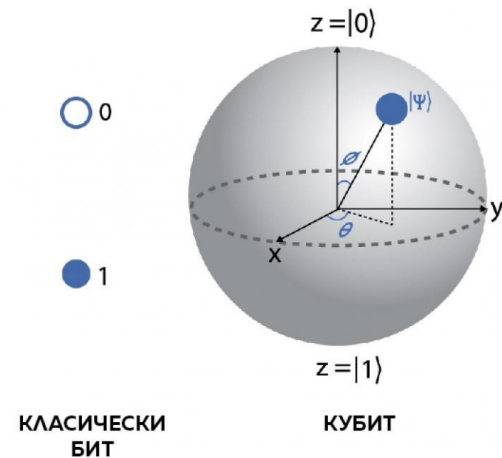


Quantum logic and representation

- ▶ Quantum computers use quantum mechanics characteristics
 - Entanglement
 - Superposition
- ▶ Quantum computing operations are performed with a very small number of Qubits (quantum bits)

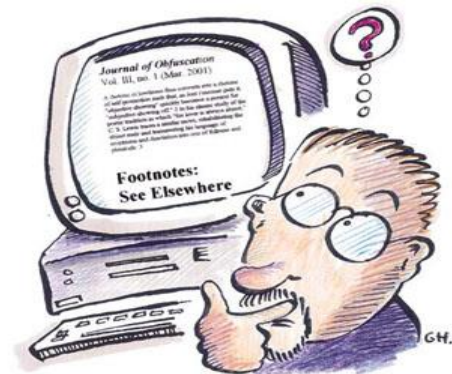
Quantum logic and representation

- ▶ The traditional computer uses 1 and 0 as bits for serial execution of commands.
- ▶ In the quantum computer, **Qbits** – quantum bits, which can be in the so-called “superposition” – to be simultaneously in both states.
- ▶ When using **Qbits**, the machine does not work serial, and can calculate all possible variants at the same time.



How quantum computers work?

- ▶ Quantum computers are **not limited** to two states like today's computers.
- ▶ Superposition quantum computers are both 0 and 1 as well as everything between them at **the same time**.
- ▶ The quantum computer performs **one million calculations** at a time, while the laptop or desktop computer has only one.



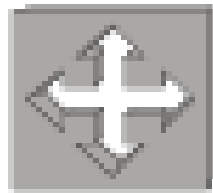
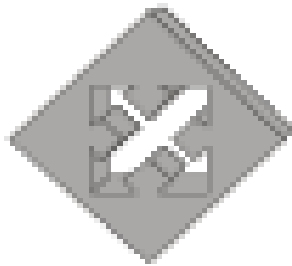
Filter polarization

- ▶ A pair of **orthogonal filters**, for example, horizontal and vertical, is called a **basis**.
- ▶ A pair of basis's is **conjugated** if the first baseline measurement completely randomizes measurement of the second baseline.

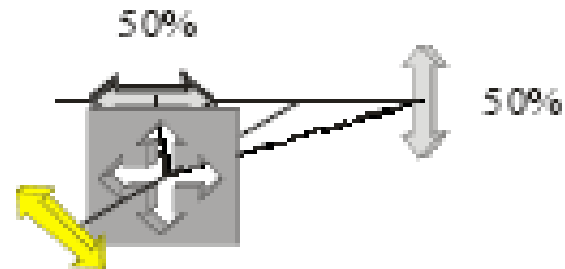
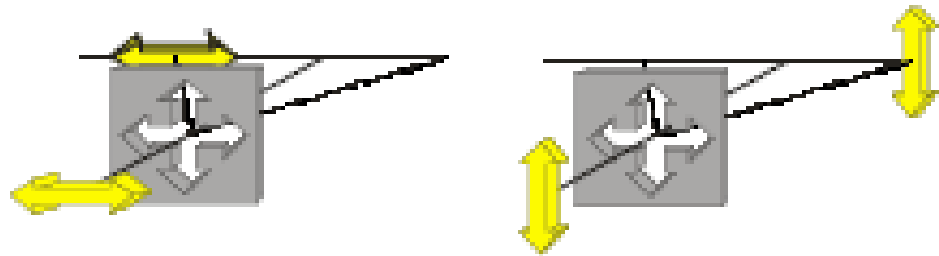
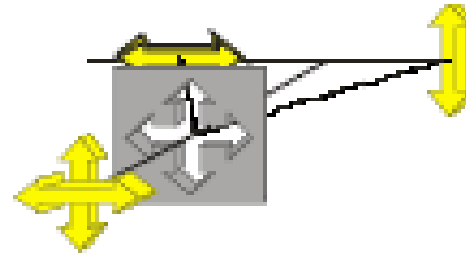
Polarized photons and filters



Polarized states



Filters



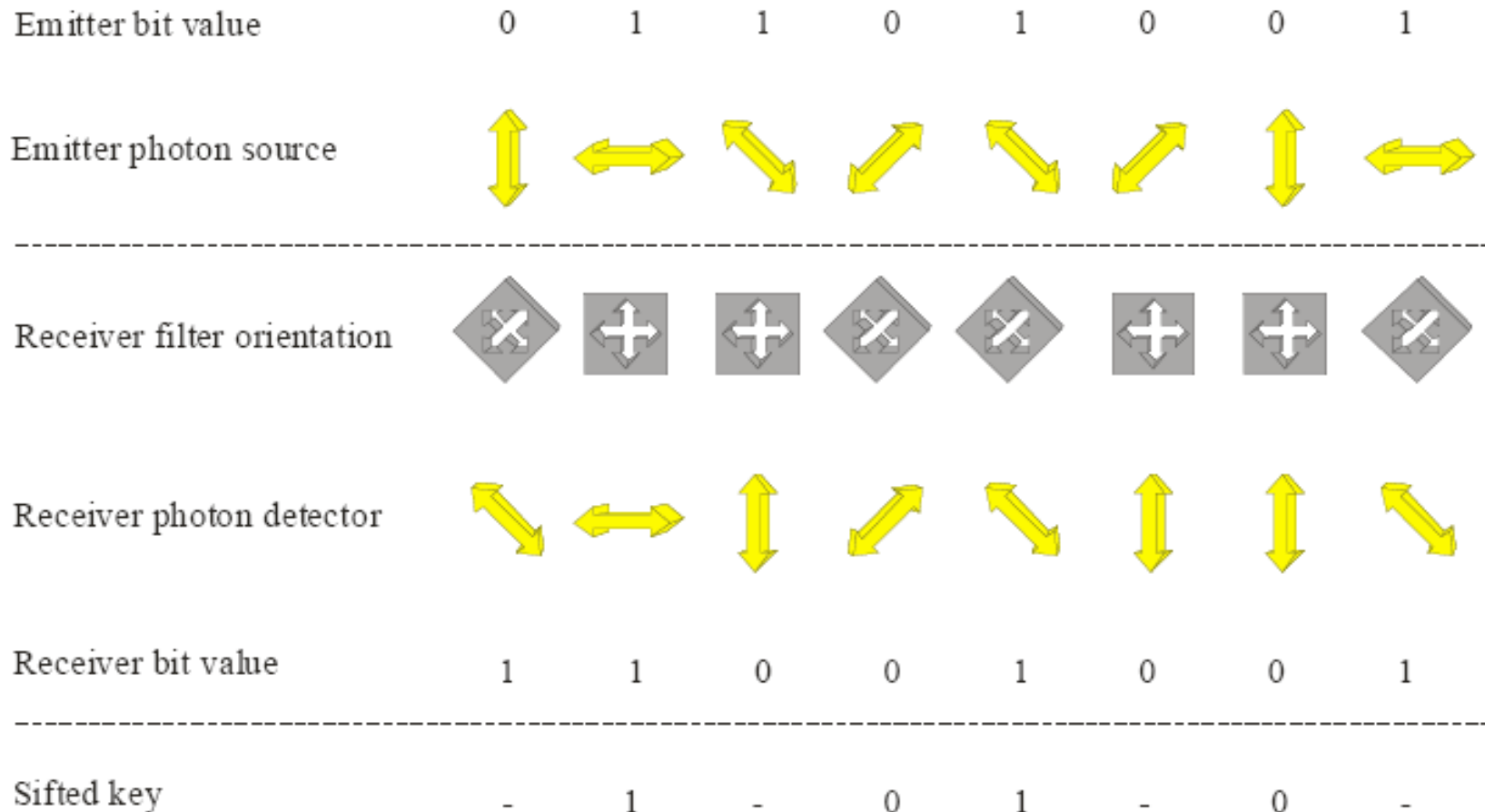
Can be used (+) basis or (X), but not both of them in one and the same time.

Main advantage of quantum cryptography

- ▶ It solves the problem of the **distribution and forwarding** of the keys.
- ▶ A secure key distribution method is suggested by : **Charles Bennett** и **Gilles Brassard** in 1984.
The method is called BB84.
- ▶ Once the key is received without compromising, it can be used to encrypt the message transmitted over a **common communication channel**.

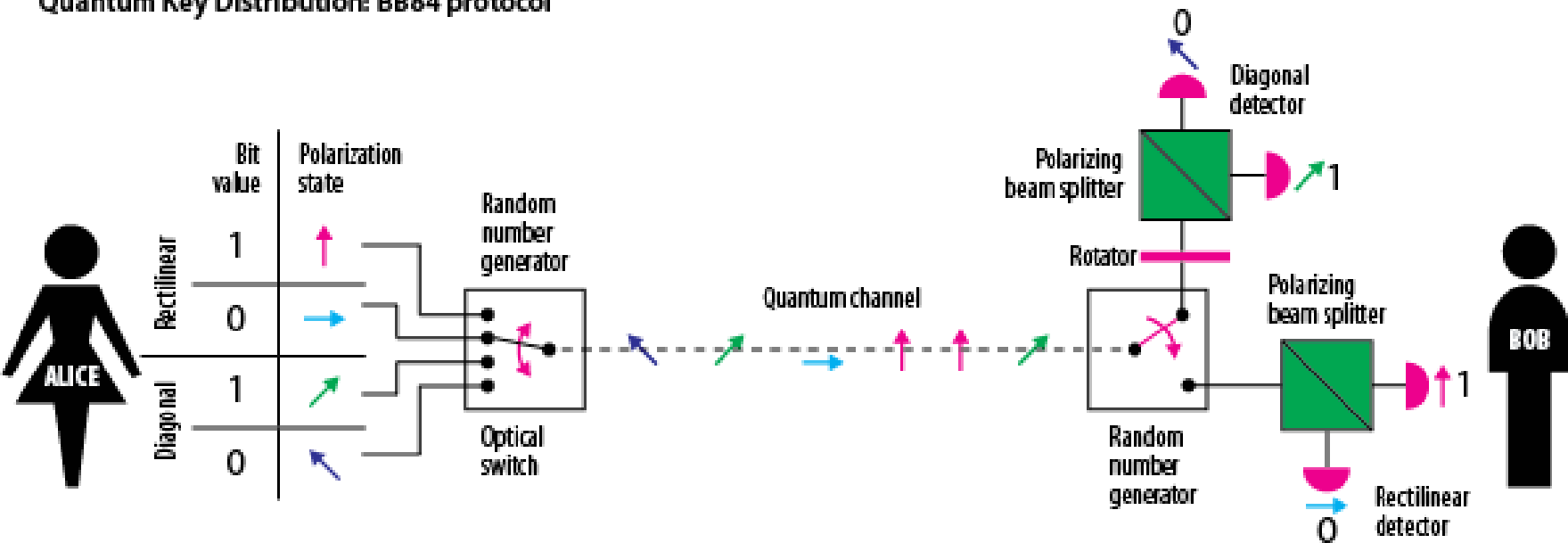
BB84 Protocol

Charles H. Bennett and Gilles Brassard



Source: id Quantix – Vectis...

Quantum Key Distribution: BB84 protocol



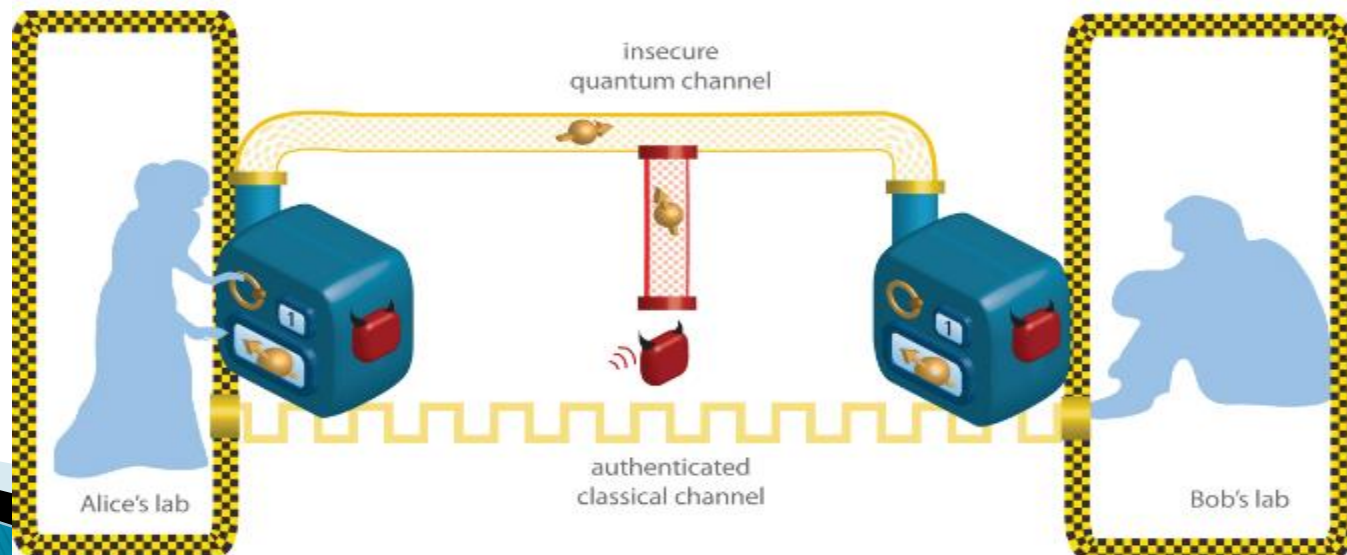
Quantum transmission & detection	ALICE sends photons								
	ALICE's random bits	0	1	0	1	1	1	0	1
	BOB's detection events								
	BOB's detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	BOB tells ALICE the basis choices he made								
	ALICE tells BOB which bits to keep		✓		✓		✓	✓	
	ALICE and BOB's shared sifted key	-	1	-	1	-	1	0	-

Heisenberg principle

- ▶ Some pairs of physical properties are linked in such a way that **measuring one does not allow the observer to know the value of the other.**
- ▶ When measuring photon polarization, choosing which direction to measure affects all subsequent measurements.
- ▶ If a photon **passes through a vertical filter**, it will have a **vertical orientation** regardless of its **original direction of polarization.**

Application

- ▶ A pair of photons is created
- ▶ They are sent turn to Alice and Bob
- ▶ Alice and Bob receive a complementary pair of photons
- ▶ It is difficult to maintain the condition of photons over long distances
- ▶ Still no business applications



Specifics

- ▶ Measurements in quantum systems lead to interference
 - Alice sends a one qubit
 - If Eve will “catch” the photon, Bob is not able to understand that this happened
 - Eve can not represent the original one
 - Neither Eve or Bob can not to recover and accept correctly everything.
- ▶ Physical devices are produced by idQuantique и MagiQ

Main principles

- ▶ Characteristics of quants
 - Photons can not be divided or doubled
 - One measurement is not sufficient to describe the overall state

Security of quantum key distribution

- ▶ Quantum cryptography owes its fundamental certainty to the fact that *each qbit is transferred from one photon*, each photon is changed immediately after it is received / read.
- ▶ This makes **impossible** to intercept the message without being detected.
- ▶ The presence of **noise** can have an impact on the **detection of attacks**.

State of the art of quantum cryptography

- ▶ Experimental application – after 1990.
- ▶ In (2004) QC is performed on distances of 30–40 kilometers via optic fibers.
- ▶ Now

The necessary techniques – two main characteristics.

- (1) One photon generator.
- (2) Can measure single photons.

State of the technology for quantum cryptography

- ▶ Efforts are being made to create and use it *Pulsed Laser Beam* with low intensity for emitting single photons.
- ▶ Detection and measurement of photons is a complex problem.
- ▶ The most commonly used method is through **Avalanche photodiodes** where a photon causes an electronic avalanche.

State of the technology for quantum cryptography

- ▶ Transmissions can take about 80 km. (Geneva, 2001).
- ▶ Repeaters can be used for longer distances. But practically repeaters are still far in the future.
- ▶ Another possibility is the use of satellites. Richard Hughes in LOS ALAMOS NAT LAB (USA).
- ▶ The distance of the satellites to the ground is hundreds of kilometers.

NIST System

- ▶ Infrared lasers are used to generate photons and telescopes with 8-inch mirrors to send and receive photons through the air.
- ▶ Using quantum key transmission, messages are encrypted at **speed *1 million* bits per second**.

The speed is incredible, but the distance between the two buildings of NIST is only 730 meters.

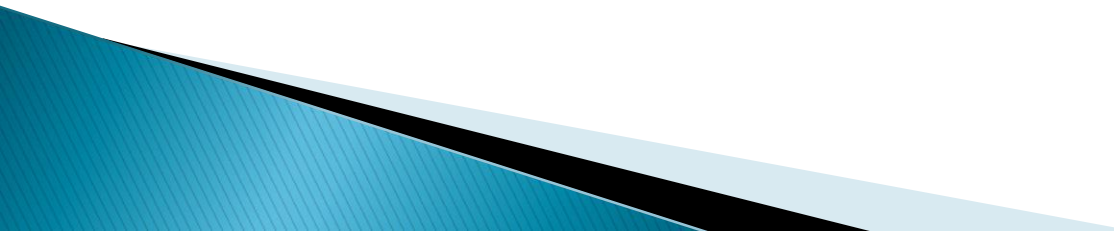
Trading organizations in QC

- ▶ **id Quantique**, Geneva Switzerland
Optical fiber based system
Tens of kilometers distances
- ▶ **MagiQ Technologies**, NY City
Optical fiber-glass
Up to 100 kilometers distances
- ▶ **NEC Tokyo** 150 kilometers
- ▶ **QinetiQ** Farnborough, England
Through the air 10 kilometers.
Supplied system to BBN in Cambridge Mass.

IEEE has taken on quantum computing standards

- ▶ The *development* of quantum computing, though at an *early stage*, away from their practical implementation, has prompted industry organizations IEEE and IEEE Standards Association (IEEE-SA) to standardize the new promising technology.
- ▶ Within the project [IEEE P7130 – Standard for Quantum Computing Definitions](#) a unified terminology for quantum computing will be created to facilitate interaction between professionals working in this field.

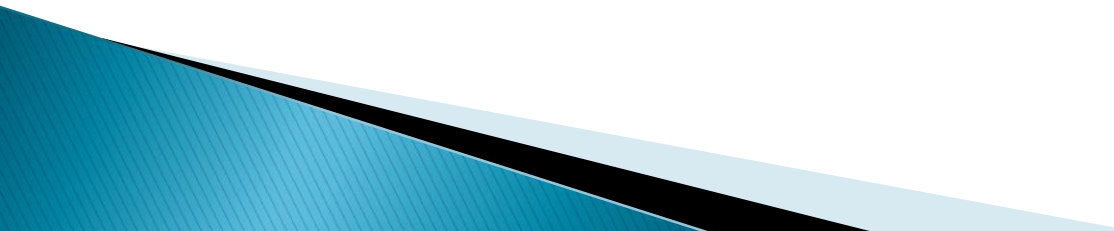
Proves

- ▶ British Columbia's D-Wave Company **promises to demonstrate a machine** that performs 64,000 operations simultaneously in parallel "universes".
 - ▶ But if the new machine goes into action, it will make the current **security schemes useless**.
 - ▶ The **quantum computer will be able to break up** today's encryption schemes as it has unlimited resources for parallel computing.
 - ▶ Analysts expect a **commercial quantum computer in about 20 years**.
- 

Reality

- ▶ A quantum computer has been created in the lab that operates **512 cubes**.
- ▶ For the first time in 2018, Google raises the curtain in front of this short film at a New York Film Festival.
- ▶ The computer operates at a temperature practically equal to **absolute zero**.

Reality

- ▶ In the 2018s, Google created Quantum Artificial Intelligence Lab based on D-Wave equipment.
 - ▶ The project is geared to exploring the capabilities of quantum computer architecture and the secrets of the space.
- 

A real practical task

- ▶ Google Glass Eye Sensor Sensor Optimization Responsible for Human Blink Detection
- ▶ shooting without a voice command, but with a simple blink
- ▶ false work of the sensors that arise from the usual blinking of the human



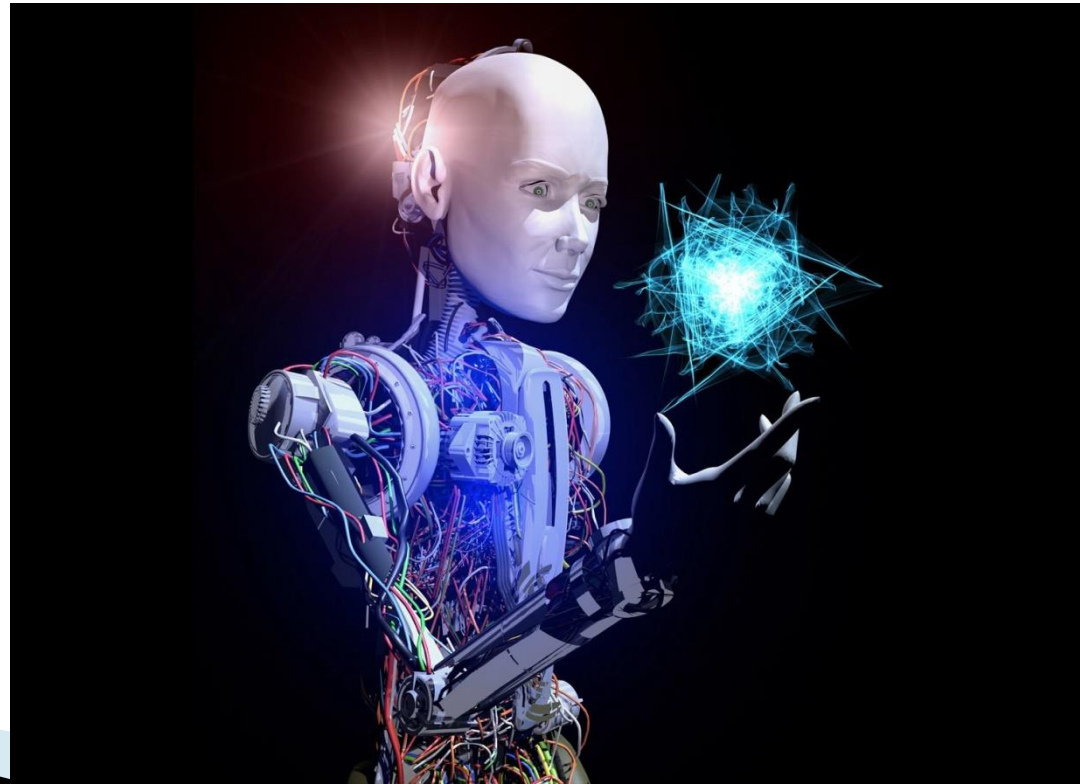
Sales of quantum computers begin

- ▶ D-Wave Systems – developer of quantum computers and software starts selling their innovative machines. With its new model, D-Wave Systems increases productivity from 1000 to 2000 cubes.

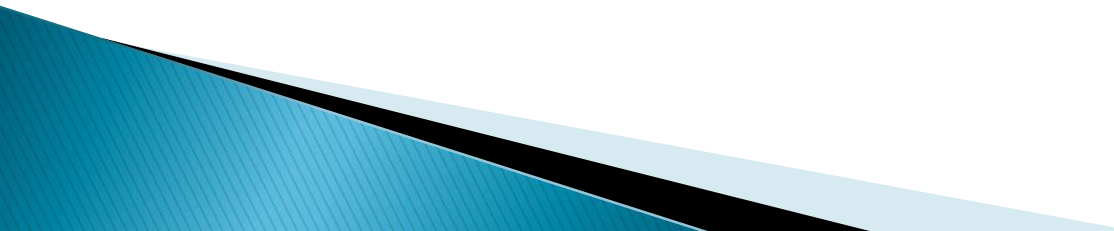


Quantum machines

- ▶ They are used in research areas as:
 - Artificial intelligence
 - Machine learning.



Software

- ▶ the method of operation is completely **different** – the current software is virtually incompatible.
 - ▶ there are software programs for quantum computers – they can do only **some strictly defined activities** in a particular environment.
 - ▶ The **results are impressive**, but due to the many limitations, there are doubts about how quantum computers are actually comparable and faster than traditional computers.
 - ▶ It will be possible after years when there is a **sufficiently efficient quantum computer** with a large number of cubes.
- 

Quantum computing

7.1

2.2

1.8



ABSTRACT BACKGROUND [VECTOR]

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed sagittis lorem ac enim viverra. In fermentum urna pellentesque. Donec gravida luctus sapien, quis fringilla tator porta ac. Morbi tincidunt nunc, sit amet sagittis consequat turpis risus scelerisque lectus, ut consetetur eros nulla tincidunt felis.

1.4

0.6

28

16.1

18.2

6.6

451

ARTIFICIAL INTELLIGENCE

17.1

78.1

23.9

BIG DATA

2.17

12.1

EPS10

9.5

16.7

13.5

13

75

QUANTUM COMPUTING REPORT

WHERE QUBITS ENTANGLE WITH COMMERCE

ABOUT

NEWS

RESOURCES

PLAYERS

SCORECARDS

ANALYSIS

JOB

Private/Startup Companies

The following is a list of startup or private companies working on Quantum Computing. More information on these companies will be added as this website is built out. Any additions or corrections to this list can be sent to info@quantumcomputingreport.com.

1QBit

1QBit is a software and consulting company that solutions to large and difficult problems, using complex algorithms and [software development](#) tools utilizing both classical methods and quantum computers. Much of their work involves utilization of quantum annealing hardware. 1QBit has

Thank you for your attention!
and patience