Quantum cryptography in RQC

The quantum cryptography provide solution which is impossible in classical world

RQC Russian Quantum Center

	Advantages	Disadvantages
One-time key	• The strongest protection	A way to distribute a secret key needs be found • Expensive and inconvenient
Public-key cryptography	• Based on the computational complexity of some problems (factorization, for example) • Security is not proved mathematically, but tested on practice • Could be used in the major number of cases, excluding the most important ones • Allows a protected key distribution over a public channel	May be easily hacked by the quantum computer
Quantum cryptography	• Security guaranteed by the fundamental laws of nature	• **Distance and bit rate limitation**

Particles’ quantum properties protect the information from the growing computing power

The information is coded in the state (polarization) of the single photon

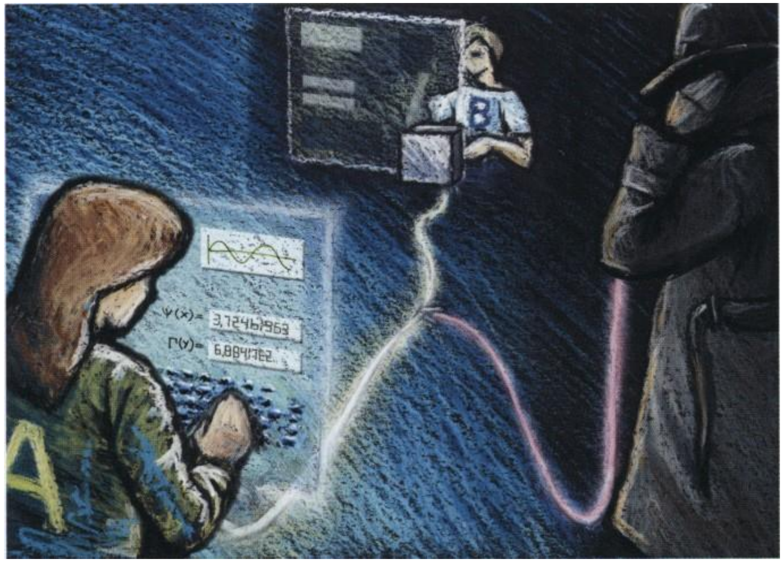
Quantum mechanics basics

- One cannot divide photon into parts
- One cannot duplicate a quantum state
- One cannot take measurements without changing the system state

Eavesdropping leads to the key errors, so it will be detected

What happens if one tries to hack the channel?

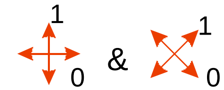
- Eavesdropper may intercept the photons, measure them and resend in the measured state or carry out any other actions, allowed by the laws of physics.
- Using of non-orthogonal states makes it impossible to find out everything about the state, within a single photon
- Any measurement attempt causes noise, which would be detected



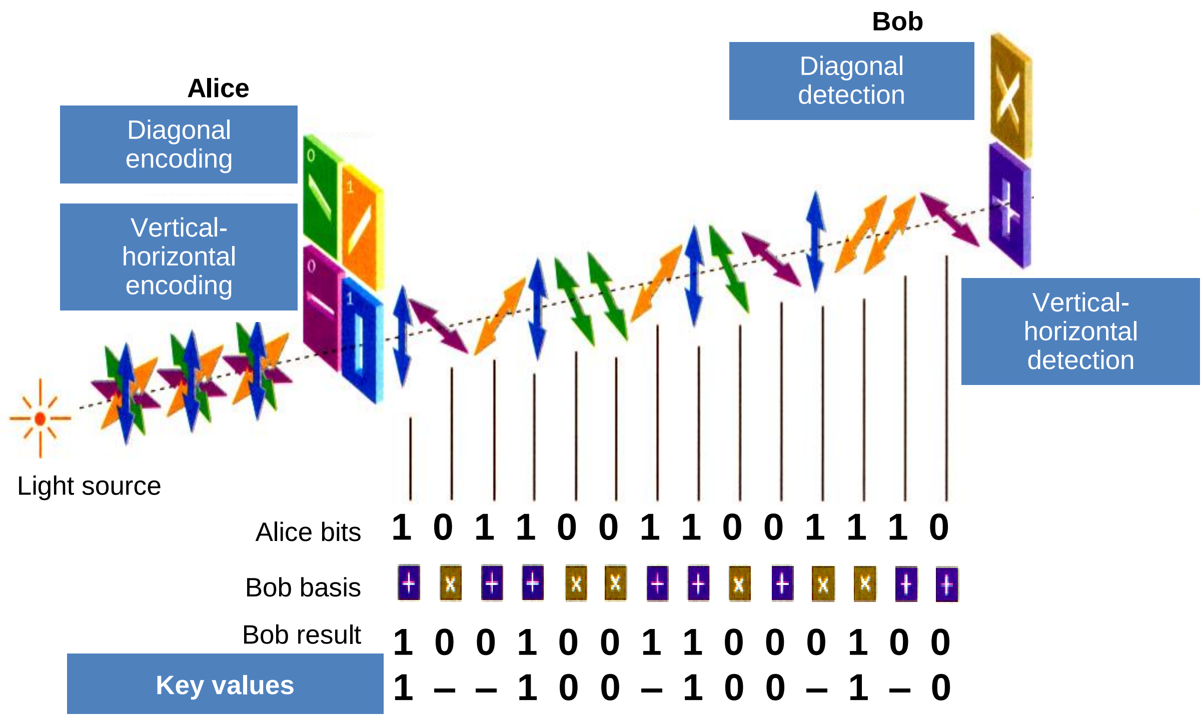
The first quantum cryptography protocol BB84

Message sending

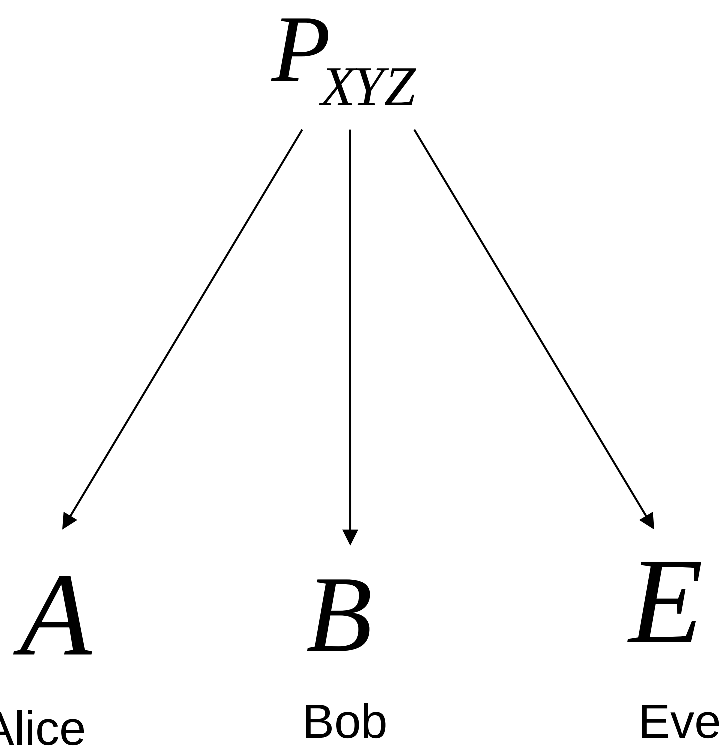
- The sender chooses random value among: 0 and 1
- The sender randomly chooses one of the polarization coding bases:



- The sender encrypts the value in one of the bases and sends to the receiver
- The receiver measures the photon using a polarization beam splitter, which is randomly tuned on the vertical-horizontal or the diagonal base.
- The receiver would get the right answer only if the bases he used equaled the sender's.
- After sending a big amount of values the sender and the receiver exchange information about the bases they used, over a public channel. Due to the fact that single photons were used, potential eavesdropper won't be able to get all information.
- The sender and the receiver remove the values which have been measured in the different bases.
- After that the receiver and the sender have an identical secret value sequences, which means that they have a one-time key.



When can we generate a secret key?



Error correction

+

Privacy amplification

Secret Key generation is possible if Alice knows 'more' about what Bob received than Eve does, and
Bob knows 'more' about what Alice received than Eve does.

$$I(A;B) > I(E;B)$$

$$I(B;A) > I(E;A)$$

To prohibit Eve to obtain the part of the transmitted key
the key needs postprocessing

QBER = $N_{wrong}/(N_{correct} + N_{wrong})$

QBER < 11%

Quantum cryptography: the absolute security, guaranteed by the fundamental laws of physics

The idea

- Information is coded in the quantum states of individual photons
- Quantum mechanics postulates:
  - One cannot divide photon into parts
  - One cannot duplicate a quantum state
  - One cannot take measurements without changing the system state

- **If eavesdropping took place it would be detected**

- **Security is guaranteed by the fundamental laws of physics**

Commercial technology

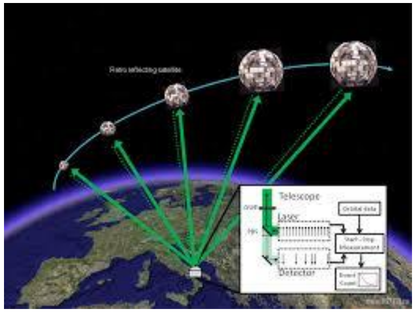
- Experimentally demonstrated key distribution over the 100 km

Ways of implementation

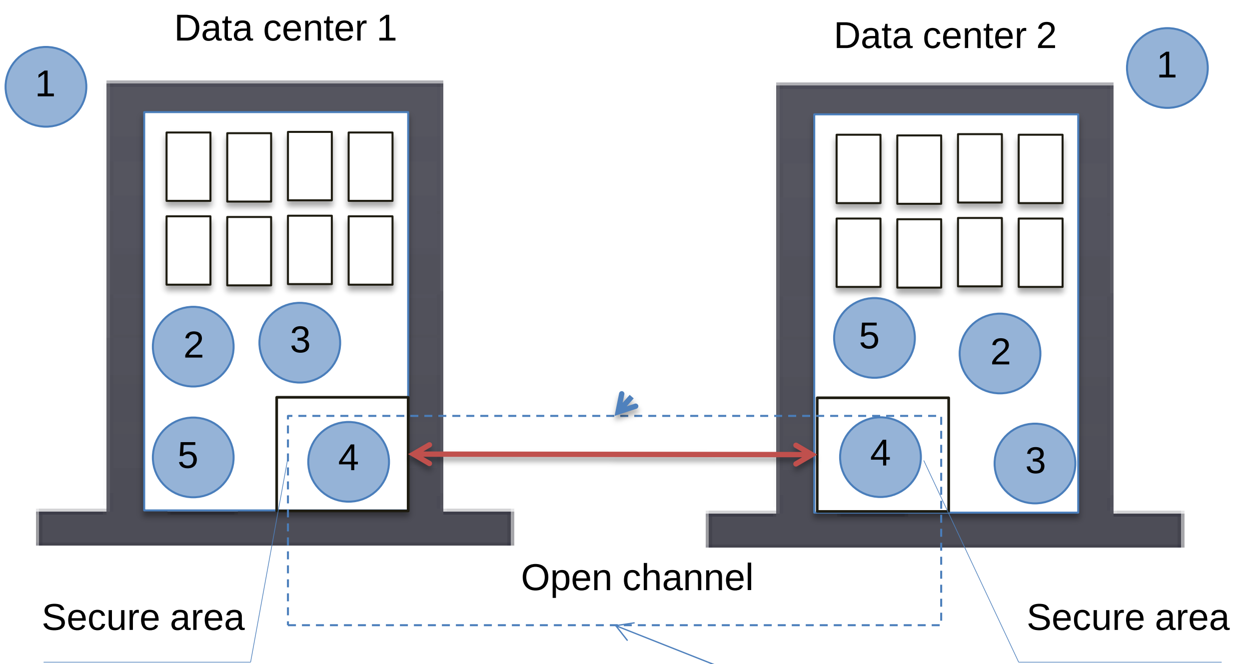
Optical fiber
- Server may be connected to the existing communication channels
- The information transfer distance is limited by the losses in the fiber (practically up to 100km)
- Optical fiber can be easily damaged

Free space
- Mobile platforms installation is possible
- Sensitive to visibility changes

Satellite
- Quantum key distribution between a ground station and a satellite on the near orbit
- The satellite motion allows key exchange between any two Earth points
- Expensiveness of the technology. First launch is planned for the 2016 (China).



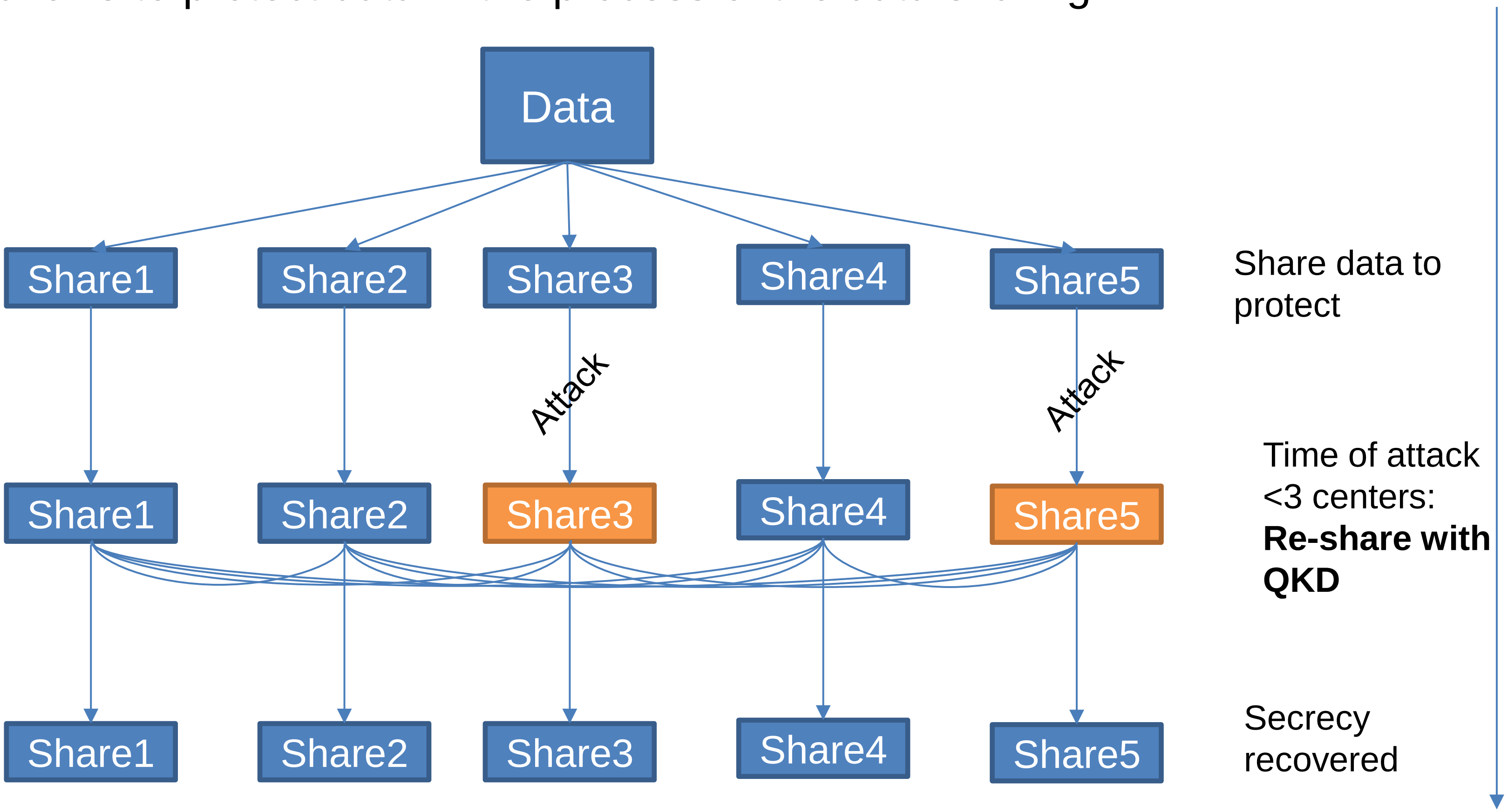
Quantum cryptography provides channel protection



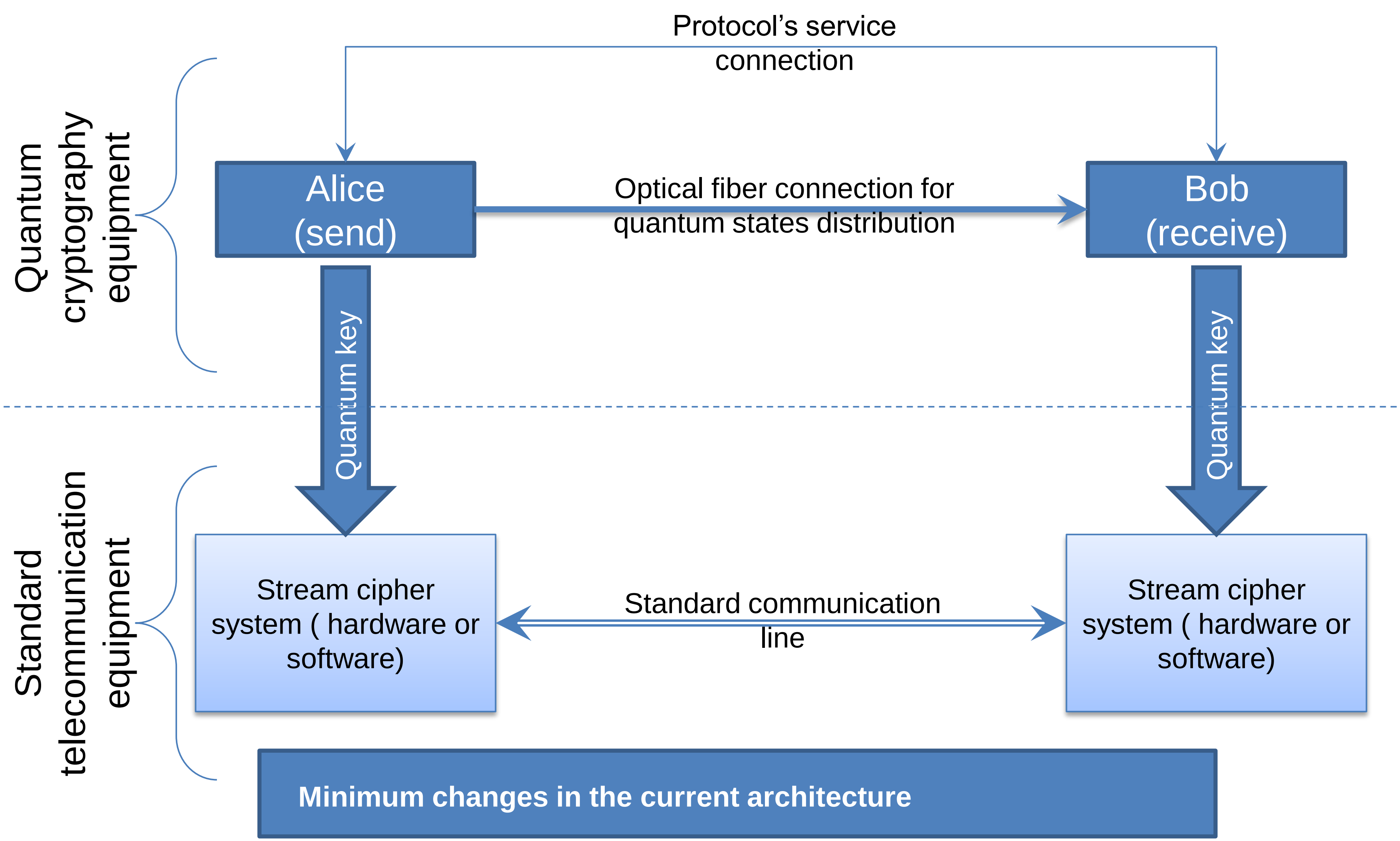
- Технические средства.
  1. Системы охраны и физической защиты.
  2. Защита от несанкционированного доступа.
  3. Защита от утечки по техническим каналам.
  4. **Защита передаваемой информации.**
  5. Компьютерная безопасность.
- Организационно-правовые меры.

Quantum cryptography is a key for storage protection

- One of the solutions to protect data in the data center in s to spread it to different centers.
- To prevent compromise of the centers one propose to use proactive secret sharing [HJKY 95]
- QKD allows to protect data in the process of the data sharing.



Quantum cryptography mechanism



Quantum cryptography prevents attack on the present critical information in the case of future computational power growth (ETSI materials)

NSA data center Utah – $3x10^{18}$ - 10^{24} bytes

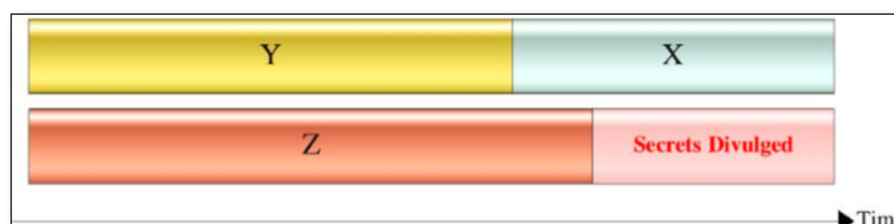
Store ciphertexts now – decrypt later

x: "how many years we need our encryption to be secure“

y: "how many years it will take us to make our IT infrastructure quantum-safe"

z: "how many years before a large-scale quantum computer will be built"

Figure 4 - Lead time required for quantum safety



Players of the quantum cryptography market

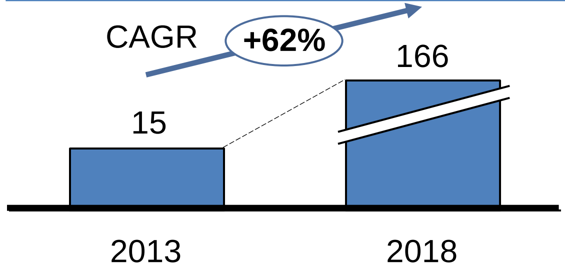
Russian Quantum Center

Products manufacturers

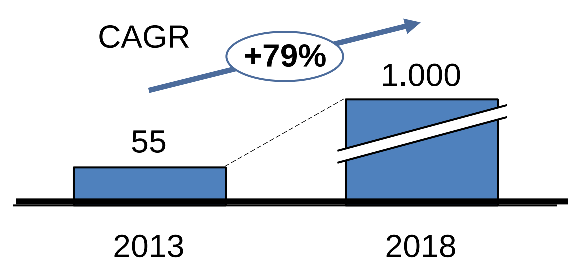
Company	Product	price	Distance, km	Speed, Kbits
Id Quantique	Cerberis	$ 300 000 Including installation	25	1
MagiQ	QPN	$ 100 000	50	3,5
SequreNet	Cyngus	?	20	10

The sizes of the classical and quantum cryptography markets

Hardware encryption market, $BN.



Quantum cryptography market, $MM.



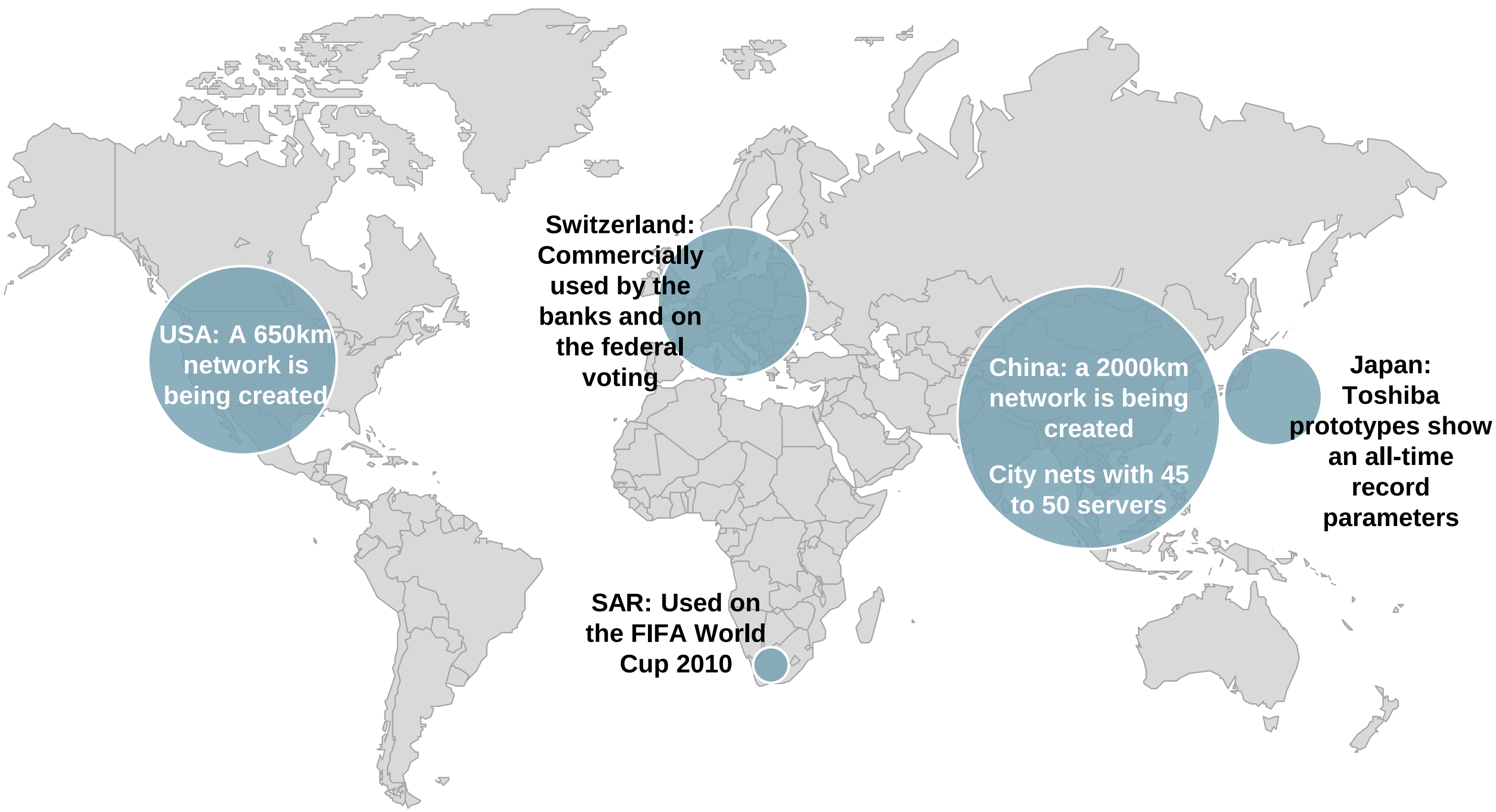
!

Furthermore, R&D in the sphere of quantum communications is actively carried out by the major IT and telecommunication companies.

To become certificated in Russia, the device should be produced in Russia.

IBM TOSHIBA CISCO Microsoft hp Alcatel·Lucent

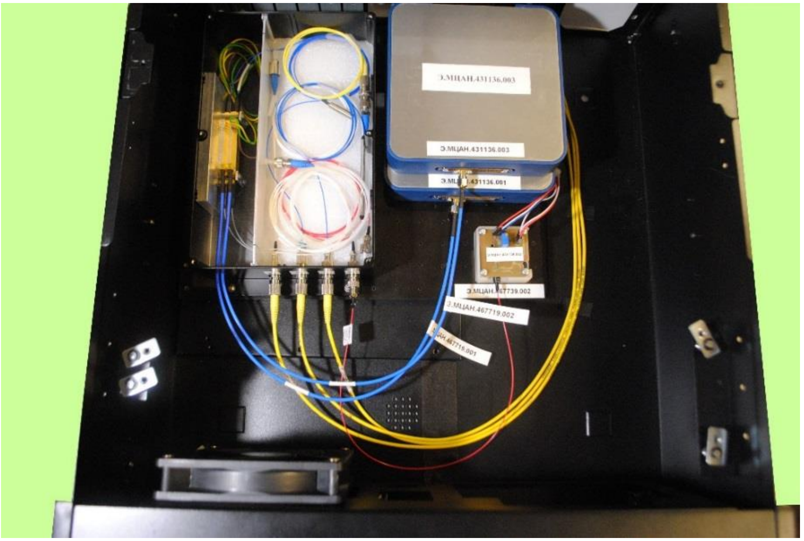
Both government and industry quantum cryptography projects are in progress around the world



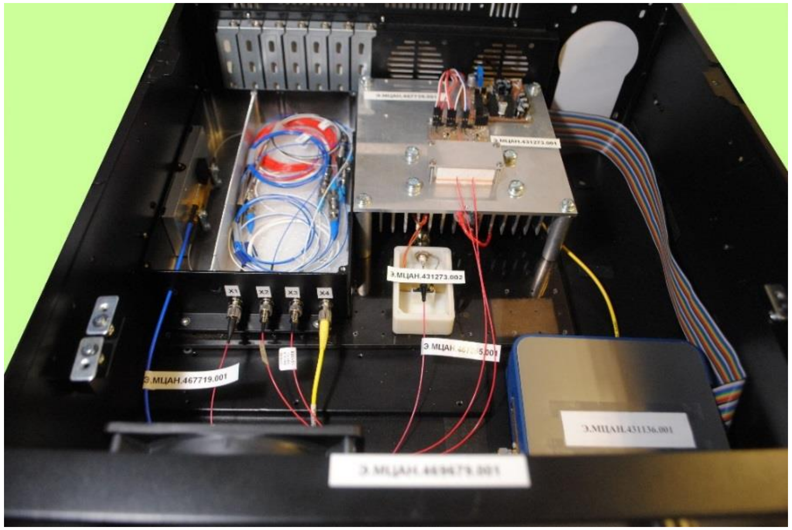
Quantum cryptography ends up being a PR project and becomes an applied system.

Current stage is prototyping

Fast prototyping electronics is based on National Instruments boards and ID230 detectors

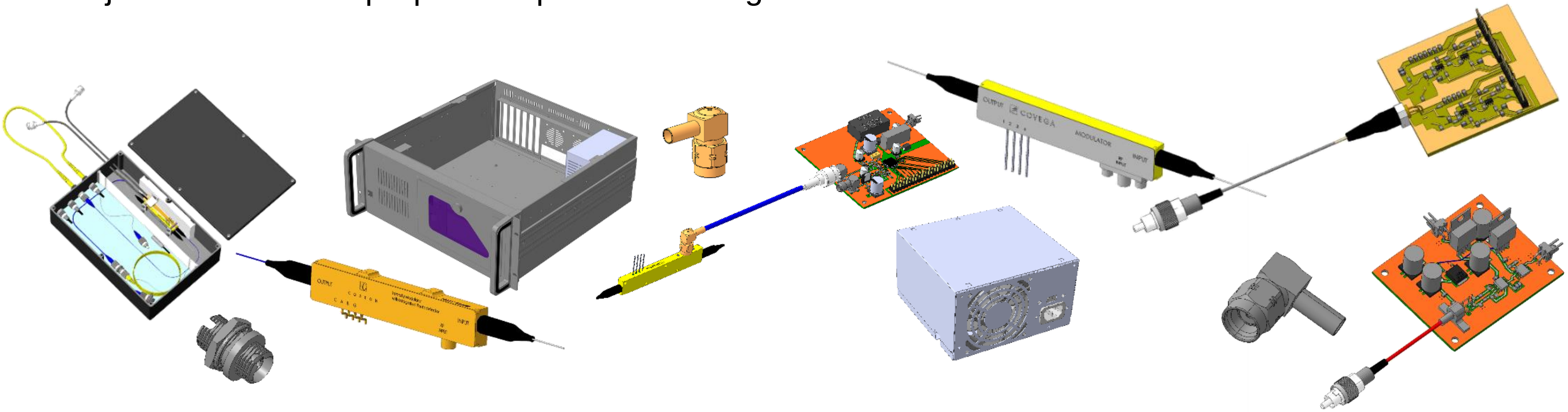


Alice prototype



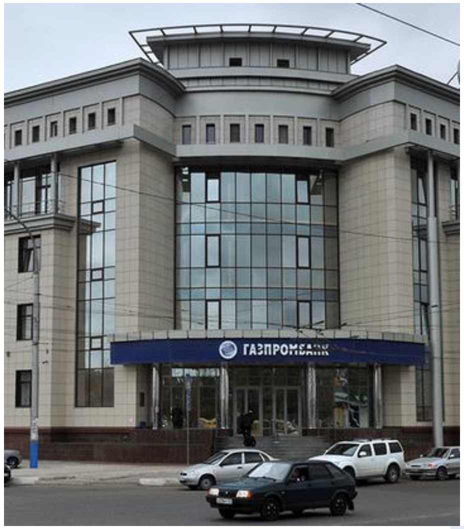
Bob prototype

3D objects database to prepare for production stage



Prototype has demonstrated operation at the city installed fiber line

- Autocompensated optical scheme Plug&Play.
- Robustness against polarization and phase disturbances.
- Phase coding of single photons 0.2 photon/pulse.
- 30,6 km quantum channel.
- 11 dB optical loss from Alise's output to Bob's detectors.
- 25 km storage line at Alice.
- 10 MHz pulse repetition rate.
- 10 ns detection gate.
- 10% quantum efficiency.
- 1,8 kbit/s sifted key rate
- 5% quantum bit error rate demonstrated.
- 0,5 kbit/s final key rate demonstrated.



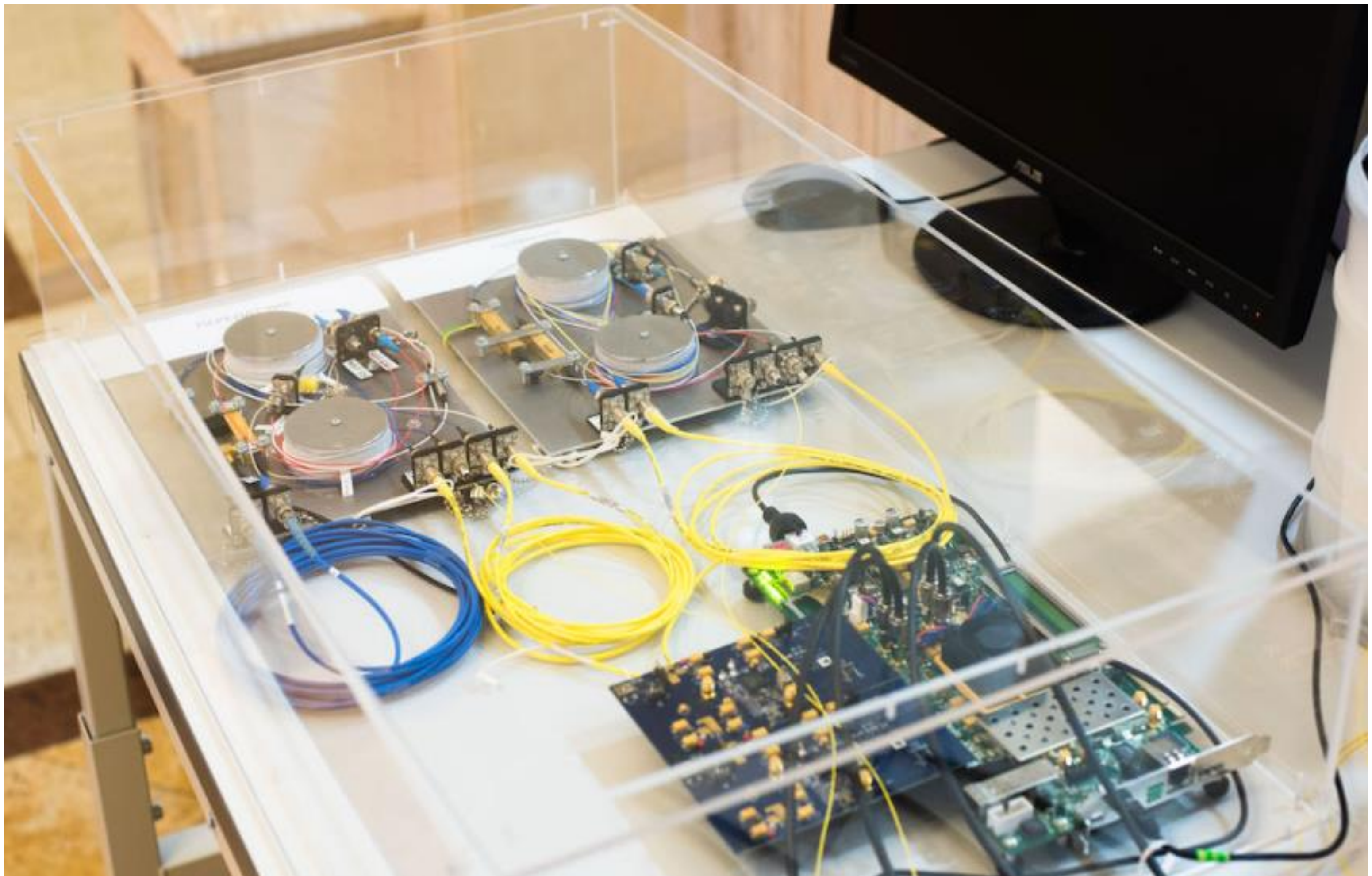
Ofis
«Коровий вал, 7»

Ofis
«Новочеремушкинская, д. 63»

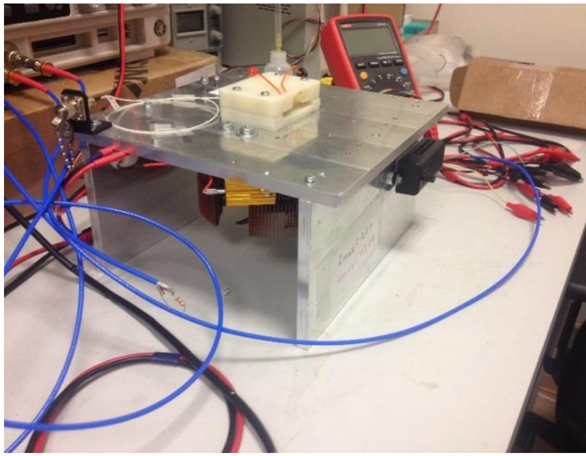
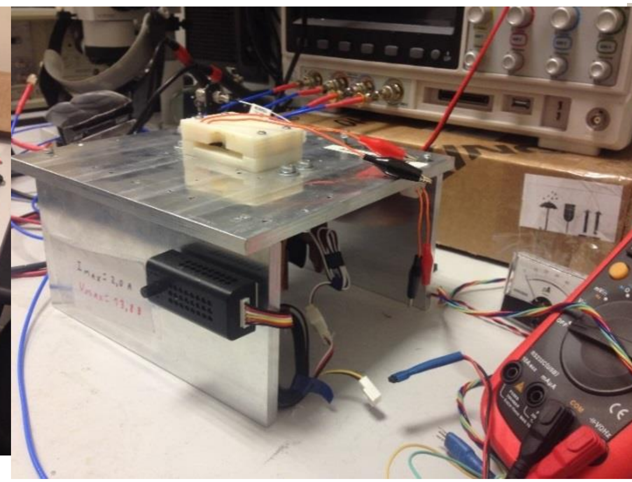
First in Russia demonstration of quantum key distribution on the real city fiber line – 30 km.
Demonstration in Gazprombank offices connected by Rostelecom lines

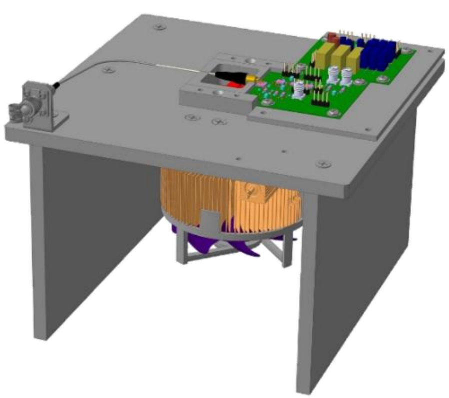
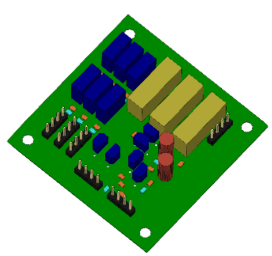
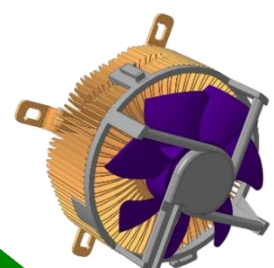
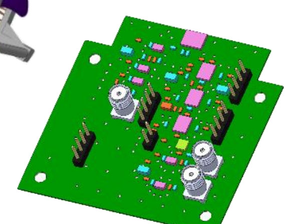
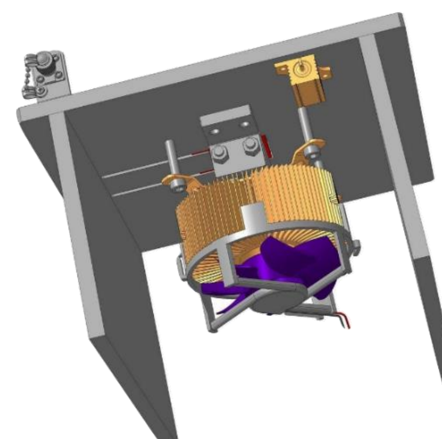
RQC quantum key distribution project's aim is to build industrial product in 2017

Virtex-7 processor allows quantum states to be created with over 1 GHz frequency. It also ensures the stable and automatic system functioning.



Prototype of the single photon detector will allow to reduce cost of the QKD setup

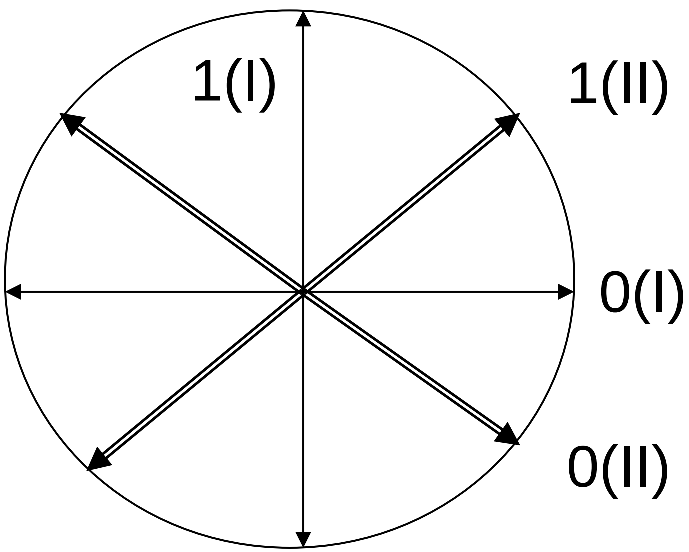



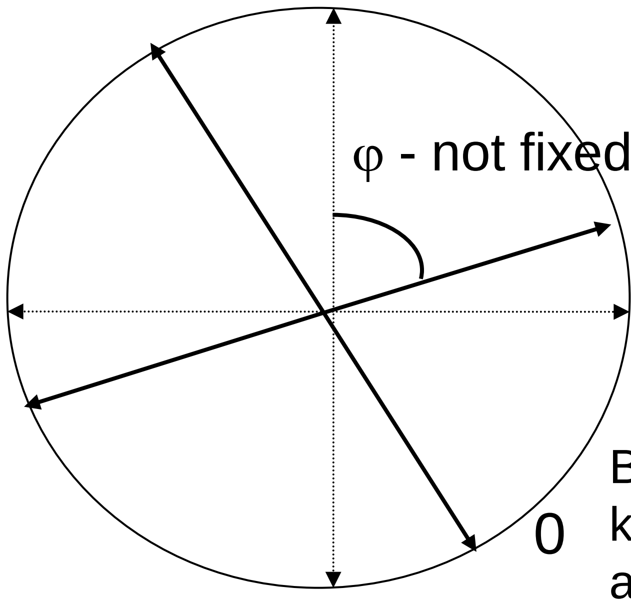
To achieve best practice result we implement our own QKD protocol

New quantum key distribution protocol which refuses from fixed basis. Absence of the fixed basis allows to make setup tolerant to detector blinding attack and increase key generation rate

BB84



Floating basis



Basis position is known only to Alice and Bob

See details on Anton Trushechkin report on 8th of June

The aim is to create a commercial quantum key distribution system

ГАЗПРОМБАНК

RQC Russian Quantum Center

Products

Products being developed

- Quantum cryptography systems for commercial use
- Stream cipher systems (partners)
- High-efficiency detectors
- Low-efficiency detectors

Customers

Detectors

Biomedical equipment:

- Flow cytometers
- DNA-readers
- Tomographs
- SPECT

Quantum cryptography systems

- The government
- Financial companies
- Corporations
- Medium-sized business
- Universities

Краткий план выхода на рынок

2015	2018	2020	2025
Active development	Sales beginning, exploitation experience	Sales increase, city networks building	Break-even point passed, inter-city networks building

Satellite-based system would break the distance limit

Russian Quantum Center

- Atmosphere's absorption between the Earth and the satellite is equivalent to the 10km air absorption at the sea level

- Satellite can be used as a quantum carrier for the two orbit points
    - Related technology– low power consumption laser system for Earth-satellite data transfer

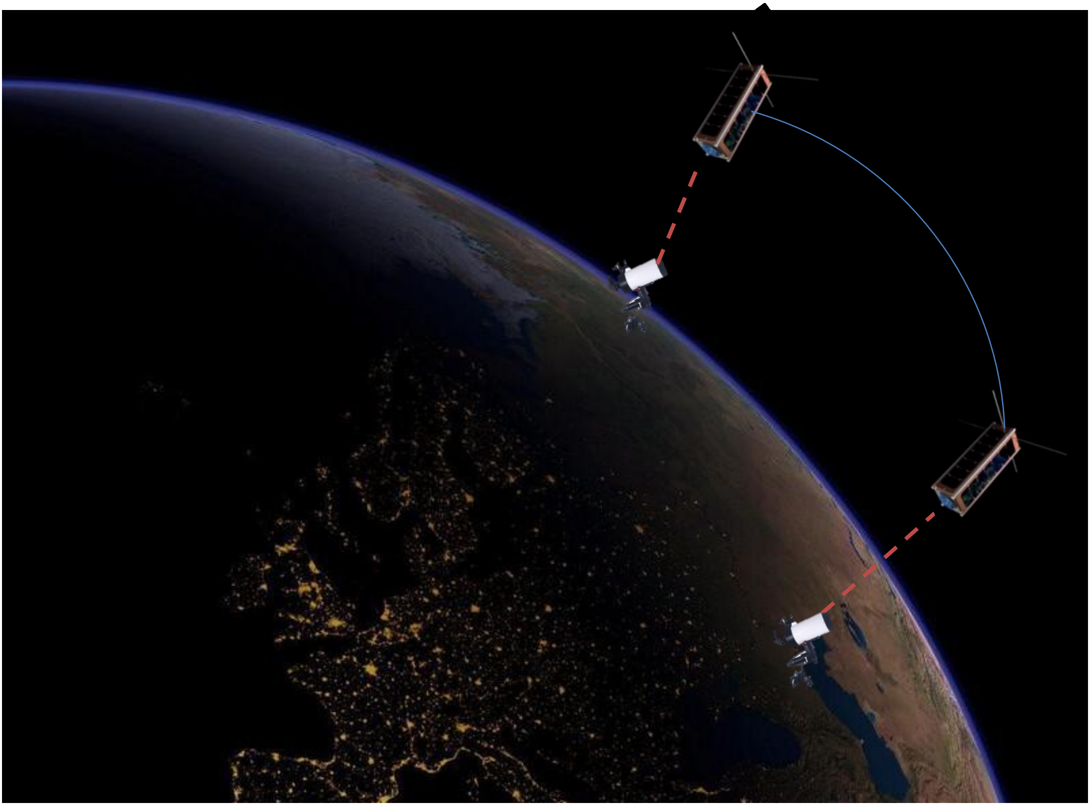
- Free space quantum cryptography is a point on the way to the satellite technology. It can be used for military needs with mobile platforms.
    - Related technology– superweak signals data transfer, which makes it hard to reveal that information exchange has taken place

- This field's leaders are: China(first quantum cryptography satellite launch in 2017), USA (private talks among the specialists), Canada and Singapore

Russian Quantum Center's international connections allow to use other groups' experience in order to overtake the leaders

We propose to use CubeSat platform to demonstrated satellite QKD (project on early stage)

RQC
Russian Quantum Center



Space QKD challenges

- Telescopes collimation
- Atmosphere disturbance
- Backlight

While slowing this problems we will demonstrate energy-efficient LEO-Earth optical data transmoission

Scientific results
• Investigate single photon transmission from the orbit to Earth • Investigate quantum state disturbance in the atmosphere

Applied results
• Develop low energy optical data transmission for satellite • Develop global quantum cryptography solution

Thank you for your attention