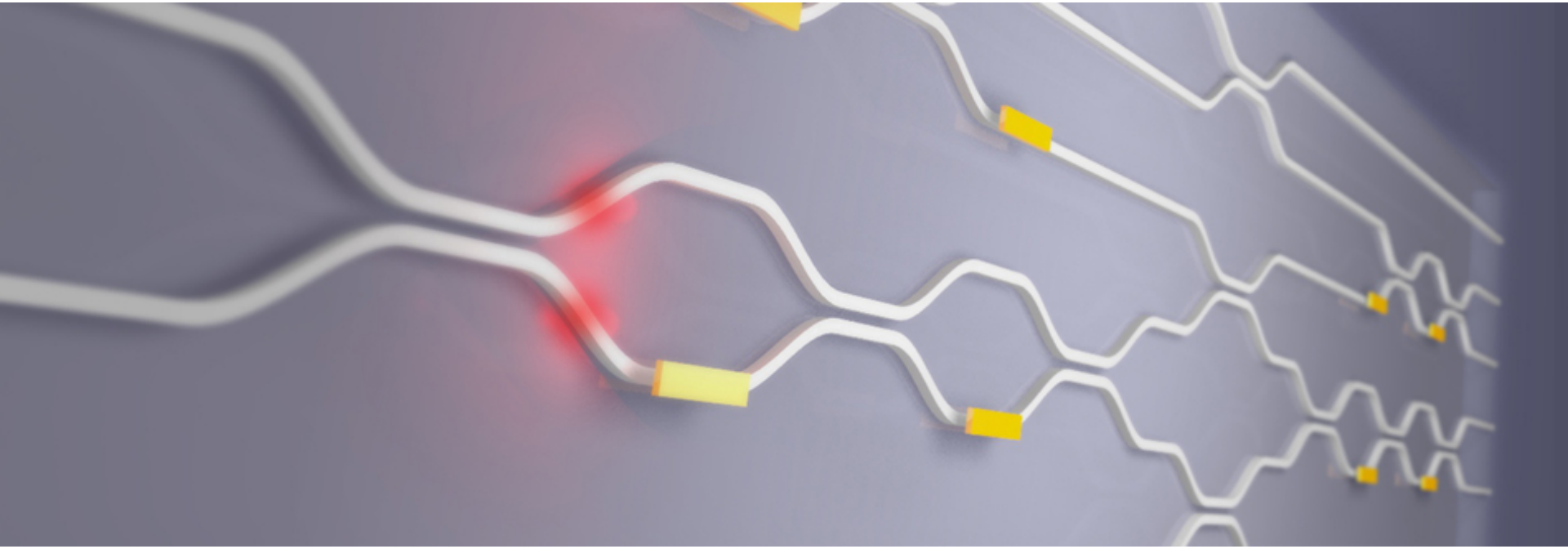
QUANTUM COMMUNICATIONS



QuantTelecom

Information protection at physical level

About company

«QuantTelecom» - developer of quantum data coding systems, providing protection of information transmission at the physical level

- Start of the project – 2011;
- Own unique technology, protected by patents;
- A laboratory prototype of the device was developed and tested;
- Achieved parameters of the system exceed all existing commercial competitors;
- Pilot shipments of the first sets of devices amounted to 30 million rubles in 2016;
- In 2016 preliminary tests were successfully completed at the Academy of the Federal Security Service of Russia
- In 2017 specialists of the Kazan Quantum Center using the devices of LLC "QuantTelecom" launched the first multi-node quantum network in Russia. Together with SMARTS data center with quantum protection is creating

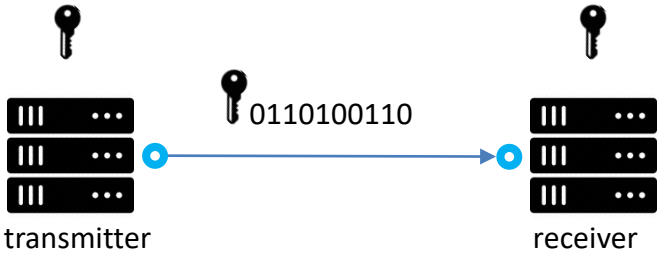
Data protection today(1/3)

QUANTUM COMMUNICATIONS

Encryption is a key element of information security.

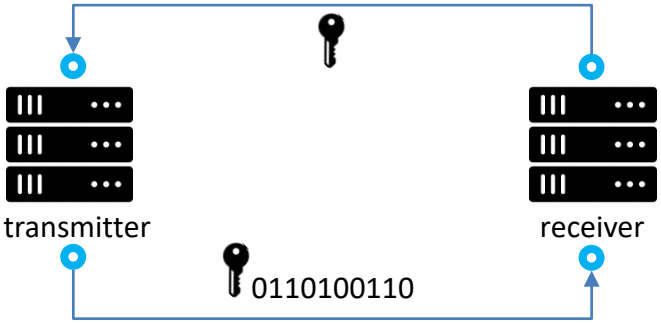
There are two basic types of cryptosystems

Cryptography with symmetric key



- Information is encrypted and decrypted using a single "key";
- It is assumed that transmitter and receiver know the key before information exchange process begins;
- Examples of algorithms: AES, DES, GOST 28147-89

Cryptography with public key



- Receiver generates and sends to transmitter a key for encryption over the open communication channel;
- Receiver stores a private key and a decryption function for decoding the message;
- Examples of algorithms: RSA, DSA, GOST P 34.10-2001

Data protection today (2/3)

QUANTUM COMMUNICATIONS

II Problems with existing encryption methods

Cryptography with symmetric key

- A secure private key transmission channel is required;
- In the most important cases (state secret, bank information), the key is transferred to transmitter and receiver in manual mode on a physical medium;
- To ensure a high level of data transmission security, frequent key changes are necessary, which entails the problem of its transmission.

Cryptography with public key

- Safety of widely used methods is based on the fact that interceptor will not have time to decipher the information while it is relevant;
- Complexity of decrypting messages depends on length of the key. Increasing its length significantly overloads infrastructure and reduces speed of messaging;
- Decoding a key of a limited length is possible. (RSA 768 bit was decoded in 2010. *)

* http://www.emc.com/emc-plus/rsa-labs/historical/rsa-768-factored.htm

Data protection today (3/3)

QUANTUM COMMUNICATIONS

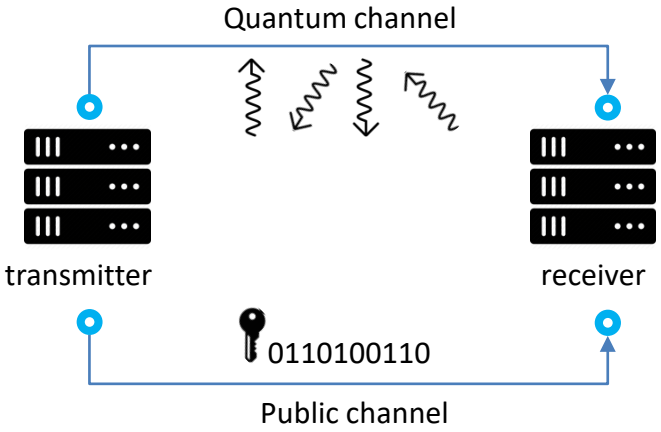
The existing algorithmic encryption methods can be cracked by using a quantum computer.

August 2015 - developed the first 1000-qubit quantum computer

Encryption that can not be hacked

QUANTUM COMMUNICATIONS

Quantum cryptography systems



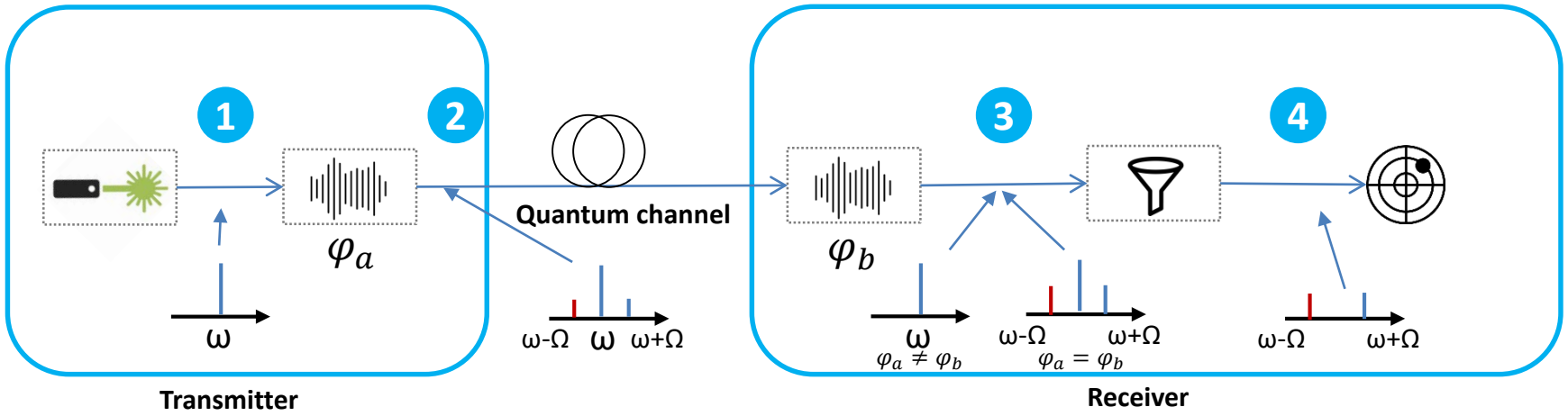
- Photons are used to create the encryption key;
- Due to the physical properties of photons transmission (destroyed during measurement, it is impossible to split and copy the state) - sender and receiver will always know if there is an "intruder" in the system who is trying to steal data;
- A private encryption key of the required length (equal to the message length) is generated by measuring the photon states by receiver and comparing them with the sender's data.

Systems of quantum cryptography can not be "eavesdropped " or hacked because of physical laws

Our solution

QUANTUM COMMUNICATIONS

Sub-carrier wave quantum cryptography (SCW QC)



1. The laser generates a continuous signal, characterized by a carrier frequency (wavelength).

2. As a result of phase modulation, two sub-carrier frequencies (ω-Ω; ω + Ω) appear in the spectrum of generated signal, they characterized by the phase of sender's modulating signal - φ_a, which is randomly selected from predefined states in two non-orthogonal bases. The signal power of sub-carrier frequencies corresponds to energy of a single photon.

3. The phase of the receiver's modulating signal φ_b is chosen randomly from the same set of states as φ_a. If $\varphi_a = \varphi_b$, then constructive interference is observed, and the signal power ≠ 0. For various choices of the bases φ_a and φ_b, the measurement result is fixed, but does not participate in the formation of the key.

4. The spectral filter separates the center frequency from the sub-carriers. The signal at sub-carrier frequencies is sent to a single photon detector. Analyzing the results of measurements, including number of errors in the previous step, a conclusion is drawn about eavesdropping and an encryption key is generated

Current status. Product

QUANTUM COMMUNICATIONS

- 2011 - research, the possibility of organizing a quantum channel at sub-carrier frequencies is demonstrated.
- 2012-2013 - laboratory prototype of the device was created, tests for compliance with the declared parameters were carried out.
- 2014-2015 - modifying of individual blocks and nodes in order to optimize parameters.
- 2016-2017 – NEOTECH LLC provided investments for starting commercialization of the project. Quanttelecom LLC launched.
- 2018 – Skolkovo Fund and SMARTS JSC approved investments for completion of development work for industrial production.

At present, a tested laboratory prototype of the device with record parameters for quantum systems has been developed:

- Data transfer rate: **up to 10 Gbit / s**
- Generation speed of a quantum key: **up to 1 Mbit / s**
- Limit transmission distance: 250 km *
- Full polarization independence, which guarantees resistance to external influences and signal distortion in the communication line.
- The equipment of the company is fully compatible with the standard fiber-optic infrastructure.

* The maximum signal loss in the line can reach 42 dB

Commercialisation Projects

QUANTUM COMMUNICATIONS

2016 :: Supply of three sets of equipment to the Republic of Tatarstan to create a pilot section of the quantum network in commercial communication lines.
The customer - KNRTU-KAI. Telecommunication partner is TatTelecom.
The amount of the project was 24.5 million rubles.

2016 :: Successfully passed tests in the Academy of Federal Security Service of Russia to confirm properties of the quantum channel and the characteristics of the devices.

2016 :: Supply of a set of equipment for pilot operation in a dynamic information infrastructure

2016 :: The process of coordinating the conditions of the pilot project in Samara region with SMARTS (telecom operator) was started.

2017 :: The coordination of technical task for the pilot operation of the systems of "QuantTelecom" by SAP.

2017 :: The polygon of a multinode quantum network for working off network technologies in urban conditions and docking with a telecommunications operator Tattelecom in Kazan is launched.

2018 :: The polygon of a multinode quantum network for working off network technologies in urban conditions and docking with a Sberbank in Moscow is launched.

2018 :: The polygon of a multinode quantum network for working off network technologies in urban conditions and docking with a telecommunications operator Rostelecom in Moscow is launched.

The pipeline was formed from more than 10 potential orders / pilot implementations. Total sales of the product in Russia for 2016-2018 around $1,5 mln.

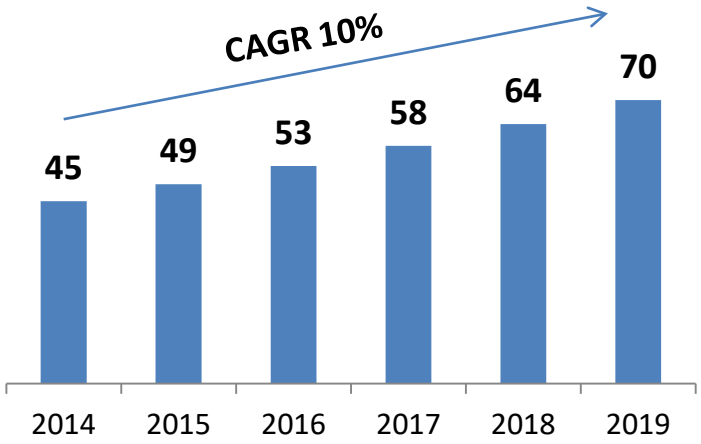
Market

- The market of quantum cryptography systems is at the stage of formation.
- The first commercial system was implemented in 2008.
- The cost of implementation remains quite high at a low data transmission rate.

The system developed by the company “QuantTelecom", can compete at the price and speed of data transfer with existing VPN systems, providing **100% data protection** at the physical level.

The market for VPN systems is growing steadily *

$ bln.



Analysts predict explosive growth of quantum cryptography market already in 2020.

$ 900 mln. - 2020r.
Global Industry Analysts, Inc.

$ 1 bln. - 2020r.
Institute for Quantum Computing.

$ 1,2 bln. - 2020r.
Icon Group International.

Quantum cryptography is a completely new type of information security technology, which has yet to occupy its niche in the information security market

* Source: Statista.com “Size of VPN market worldwide in 2014 and 2019”

Competition

QUANTUM COMMUNICATIONS

Characteristics of QuantTelekom's solutions are significantly superior to competitors performing commercial sales of quantum cryptography systems :

Company	Country	Speed of key generation per 100 km	Limit range	Spectral signal efficiency	Compatibility with existing infrastructure
ID Quantique (Clavis 3)	Switzerland	3 kb/s	100 km	2%-4%	Yes
MAGIQ (Q-Box)	USA	0,1 kb/s	140 km	~ 4%	No
SeQureNet (Cygnus)	France	1 kb/s	80 km	~ 4%	No
QuantTelecom	Russia	125 kb/s	250 km	Up to 40%	Yes

- The key advantage of KvantTelecom's technologies is the maximum data transfer limit on one set of devices, which makes the deployment of networks much cheaper than analogues.
- The technologies of competitors impose significant limitations for the development and improvement of the parameters of their own data transmission systems.

Project team

Artur Gleim, CEO

Artur has been developing systems of quantum informatics and communications for more than 5 years. Head of the Laboratory of Quantum Informatics, ITMO University.
He has experience in conducting research and development and research works, managing a team of engineers and researchers, and implementing major contracts in the field of development and research.
Author of 2 patents and more than 33 scientific publications.

Sergey Kozlov, Director for Science

Dean of the faculty of Photonics and Optical Information, ITMO University.
More than 30 years of scientific and project activities in the field of photonics. Chairman of the educational and methodological council on photonics and optical information of the Ministry of Education and Science of the Russian Federation. Member of the International Society of the SPIE (International Society of Photo-Optical Instrumentation Engineers)
DSc. Author of 2 patents and more than 200 scientific publications.

Sergey Khmelevsky, Development Director

Around 20 years working in the field of innovative marketing and management, has extensive experience in advising on innovation and infrastructure topics, experience in the creation and support of start-up companies and R & D projects.

Mentor and co-investor of the project, managing partner of New Technology Group LLC. Realised investments in innovation industry during last 10 years > $500 mln.