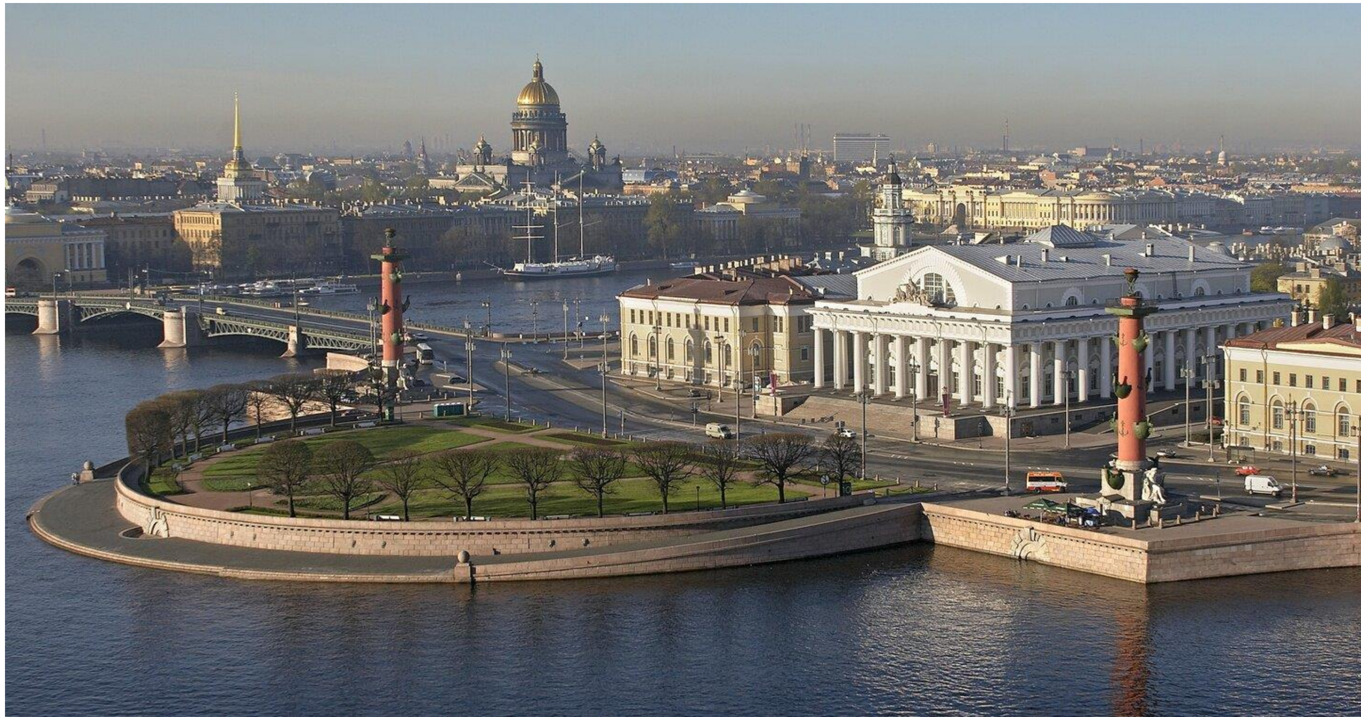
Quantum communication in Russia: status and perspective

Vladimir I. Egorov, PhD

Assistant professor, ITMO University,
Department of Photonics and
Optical Information Technologies

Senior researcher, Quanttelecom LLC

viegorov@itmo.ru



Shanghai, 2019

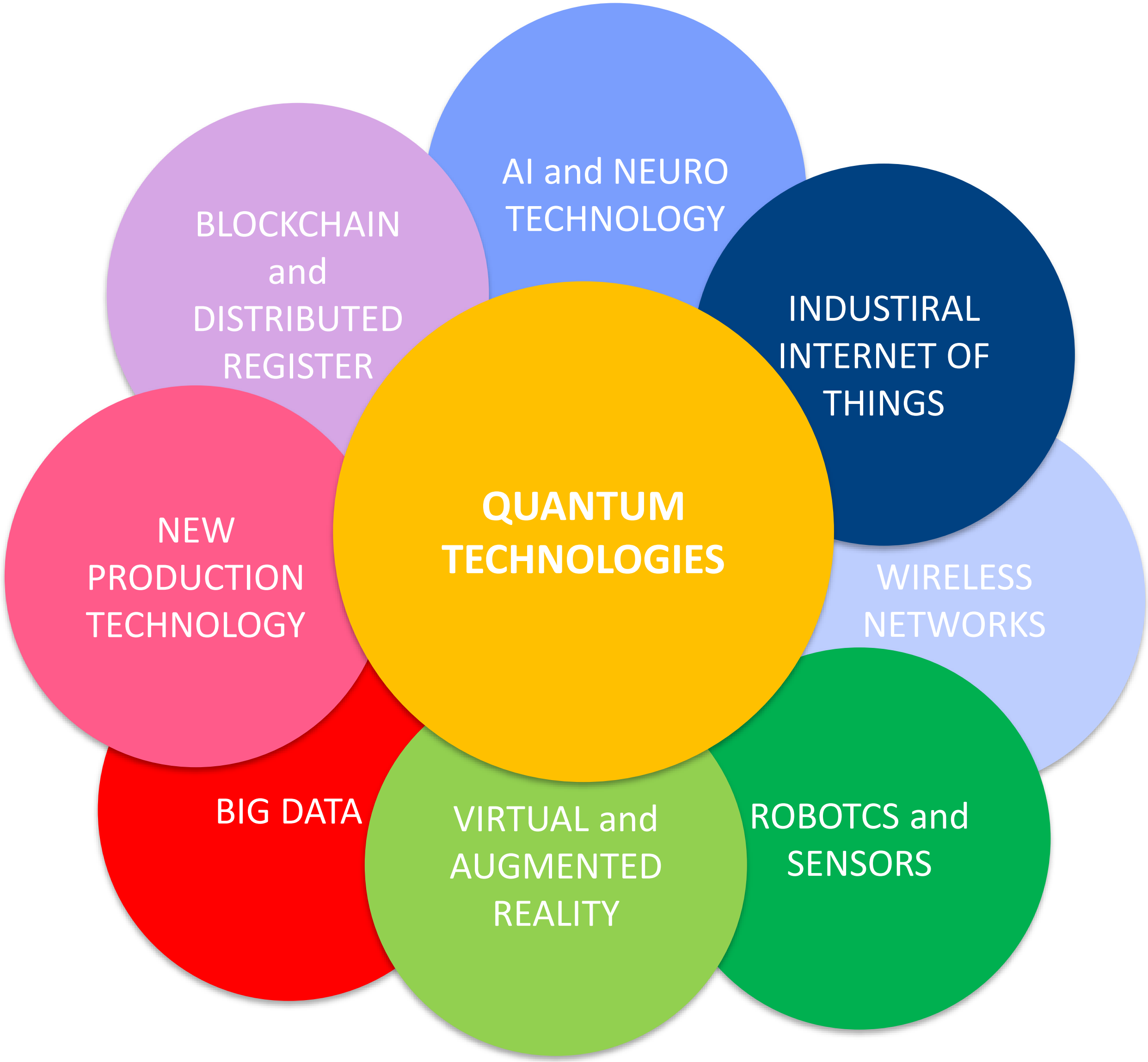
Outline

- Quantum communication as a strategic technological priority
- Government programs and investment
- Major QKD research groups in Russia
- Development directions and status
- QKD standardization policy
- Our view of quantum-secure future

“Point-to-point QKD technology in Russia is characterized by **a high degree of completeness** (with a notable exception of certification procedures) and has been included into National Technology Initiative as well as industrial investment programs”.

From the roadmap “Data Economy: Quantum technologies”, 2019

Data Economy government program (2019-2024)



Contuniation of National Technology Initiative (NTI) program (launched in 2014), that focused on forming hi-tech markets. *See https://asi.ru/eng/nti/*

Aims:

1. Adapting laws, regualations and standards
2. Research and development
3. Education
4. Information infrastructure
5. Information security (for people and state)

Program amount: $7.5 bil. (government funding), plus comparable amount of industrial investment. $0.7 bil. for Quantum Technologies

Main instruments:

1. Creation of Leading Research Centers
2. Co-funding of R&D supported by industry
3. Technological start-up funding
4. Regional project support
5. Industry digital platforms support

Data Economy: "Quantum technologies". Main directions (2019-2024)

Quantum computing and simulation:

Subtechnologies:

1. Superconducting
2. Neutral atoms
3. Ion traps
4. Photonic circuits
5. Polariton condensers

R&D directions:

1. Quantum computers and simulators
2. Quantum error correction codes
3. Quantum algorithms
4. Cloud platform for quantum computing

Quantum communication:

1. Point-to-point QKD
2. CV QKD
3. Quantum networking
4. Quantum and classical channel multiplexing
5. Trusted repeater network
6. QKD on-chip
7. MDI QKD
8. Quantum memory
9. Quantum repeaters
10. Free-space QKD
11. Satellite QKD
12. QKD for IoT
13. Single photon detectors
14. Quantum IoT

Quantum sensing and metrology:

1. Quantum clock
2. Giroscopes
3. Accelerometers and gravitometers
4. Temperature, electric and magnetic field sensors
5. Spintronic sensors
6. Plasmonic 2D materials
7. Solid state photomultipliers
8. Electroinic nose

Source: roadmap draft "Data Economy: Quantum technologies", 2019

QKD in Russia as an industry-ready technology

QKD research centers

ITMO UNIVERSITY

RQC Russian Quantum Center

KQC Kazan Quantum Center

QKD manufacturers

SMARTS QUANTTELECOM

infotecs

QRATE QUANTUM COMMUNICATIONS

Network device manufacturers

СПБ

s-terra

АМИКОН

Telecom operators and IT

СМАРТС

ТАТТЕЛЕКОМ

open{code} открытый код

RUS®SOFT

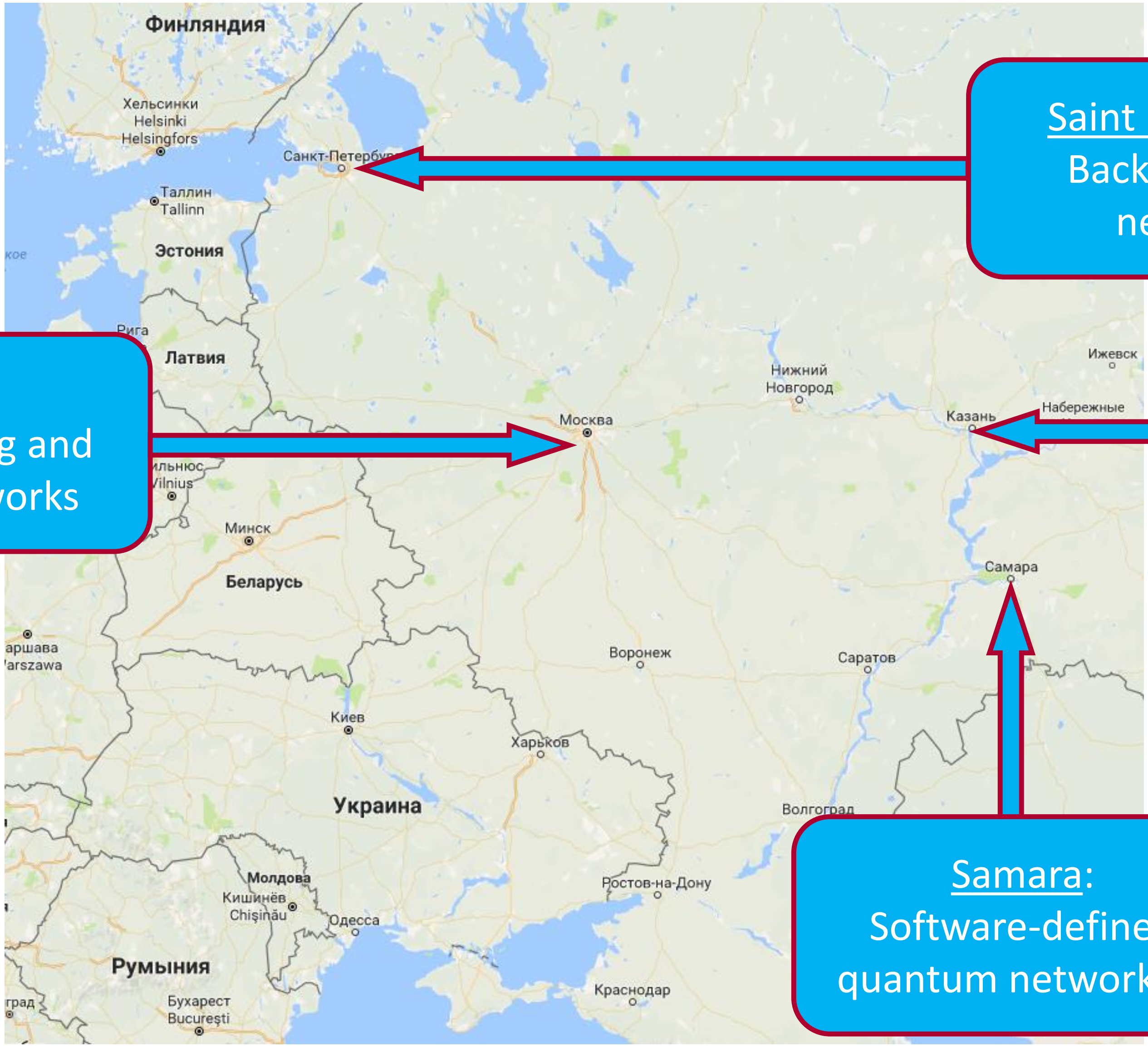
International companies

Rostelecom

SBERBANK

GAZPROMBANK

Quantum network testbeds in Russia



__Saint Petersburg__:
Backbone QKD networks

__Moscow__:
Secure banking and regional networks

__Kazan__:
QKD networks with trusted and quantum repeaters

__Samara__:
Software-defined quantum networking

ITMO UNIVERSITY

QUANTUM COMMUNICATIONS

RQC Russian Quantum Center

QRATE QUANTUM COMMUNICATIONS

infotecs®

KQC 2014 Kazan Quantum Center

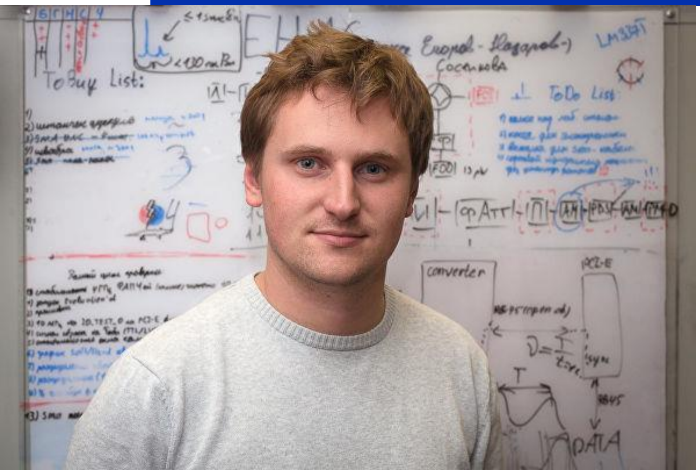
ITMO UNIVERSITY

ТАТТЕЛЕКОМ

СМАРТС

open{code} открытый код

QKD research groups: ITMO University (St. Petersburg)



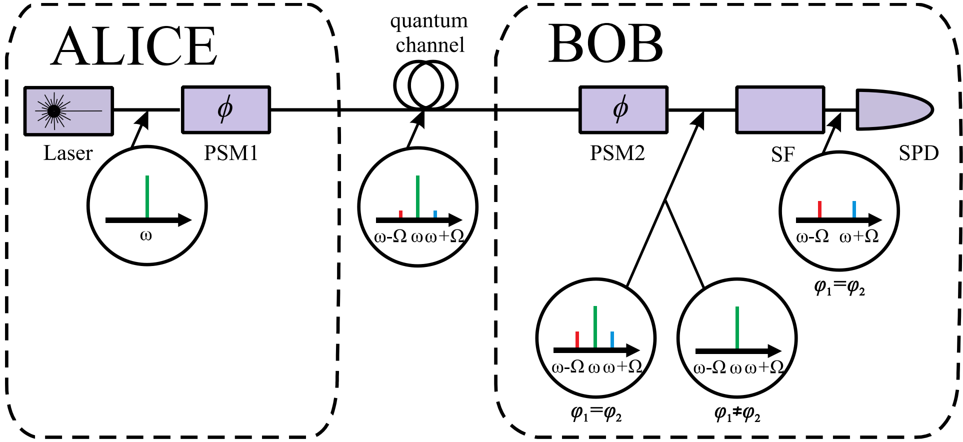
Dr. Artur Gleim, head of quantum information lab, ITMO University.
Director general, Quanttelecom LLC.

ITMO UNIVERSITY

SMARTS QUANTTELECOM

Main development directions:

- Subcarrier wave QKD
- CV QKD
- Quantum hacking
- QKD protocols
- Single photon detectors
- Quantum RNGs
- SDN QKD networking
- Quantum networking

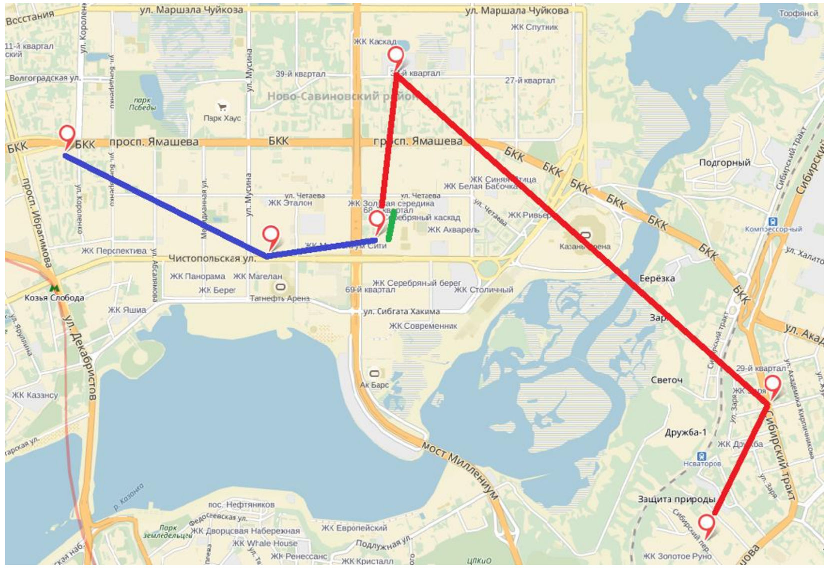


Subcarrier wave QKD scheme

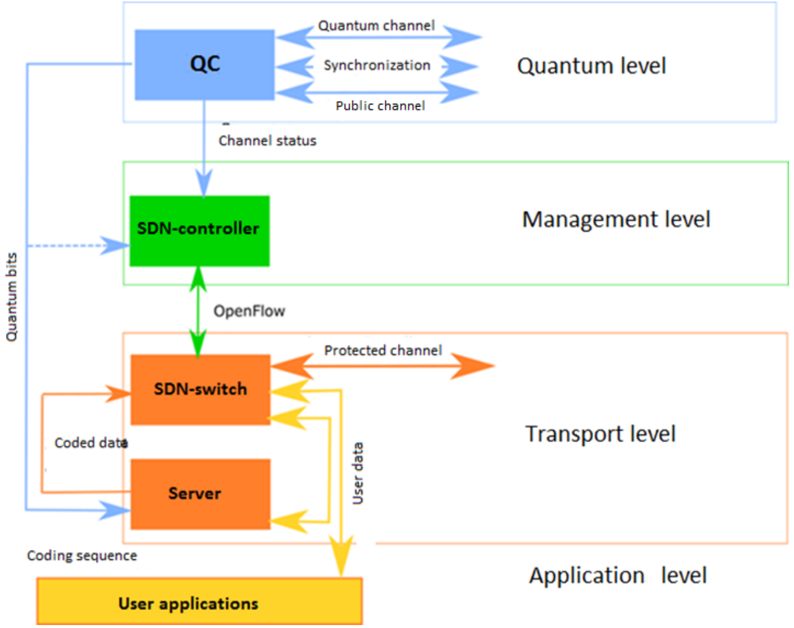
QKD research groups: ITMO University (St. Petersburg)

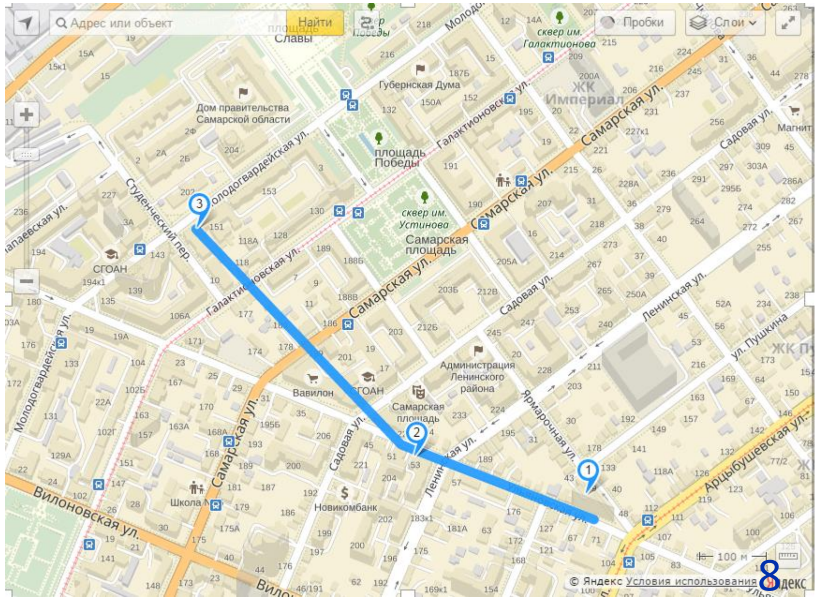
ITMO UNIVERSITY

SMARTS QUANTTELECOM

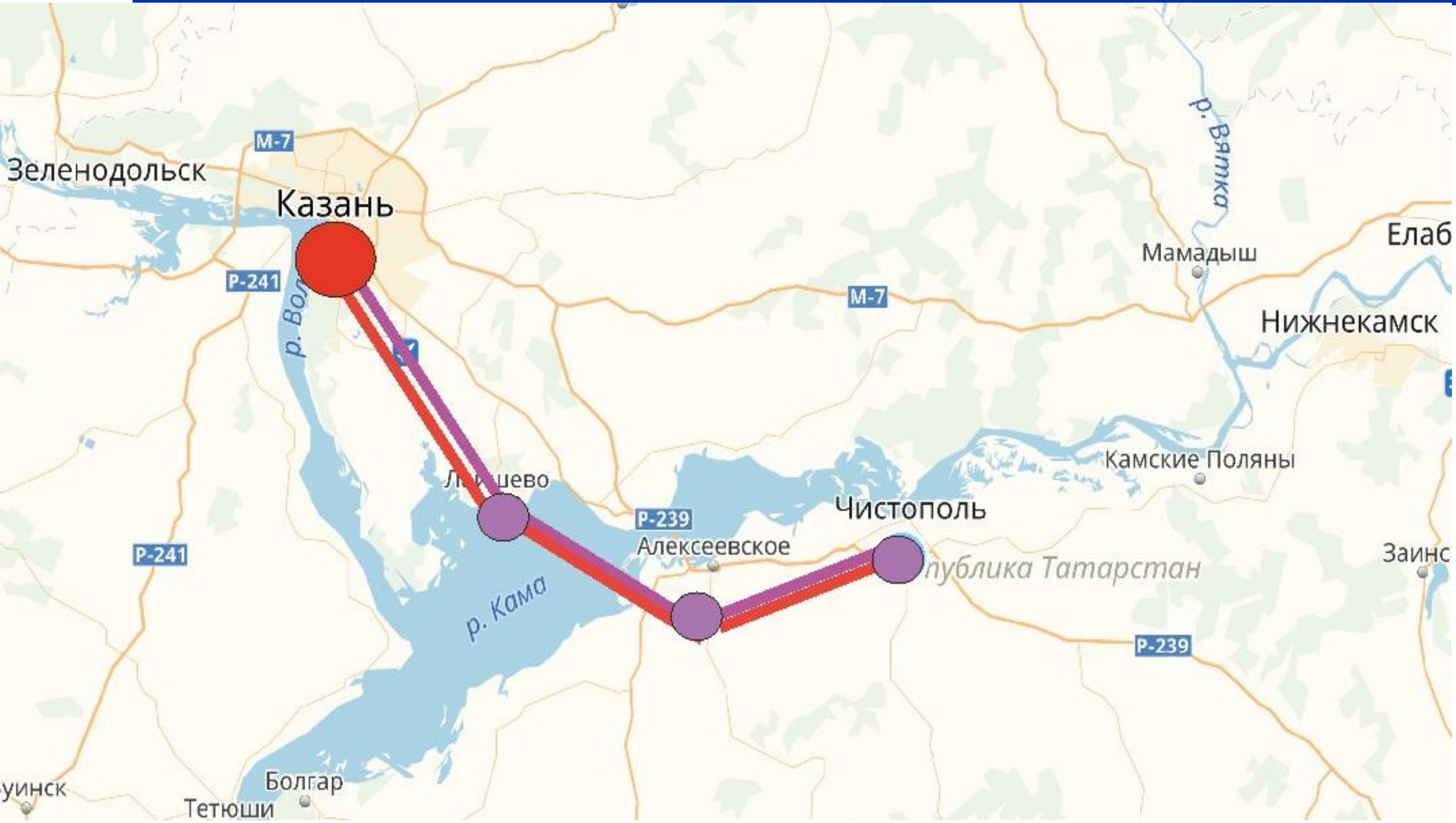


- 2011 – R&D, experimental demonstration of quantum channel formation and communication using the subcarrier wave QKD method;
- 2012-2013 – Working prototype created, successful laboratory tests of technical parameters
- 2014 – **Metropolitan area quantum link launched at ITMO**
- 2014-2015 – Finalization of separate system modules for optimizing their characteristics
- 2015-2016 – Quantum Communications LLC launches sales with a 340 000 EUR contract
- 2016 – ITMO & KRNTU-KAI launch **the first Russian multimode quantum network** in Kazan
- 2017 – ITMO and OpenCode launched **the first software defined quantum network**
- 2018 – ITMO and SMARTS are developing **quantum-secure distributed data center**
- 2019 – ITMO and KRNTU-KAI launched **160 km intercity quantum channel** over a deployed fiber





Field-test of intercity QKD link (160 km), 2019



Node 1: Kazan Quantum Center, KRNTU-KAI, Kazan
Node 2: Tattelecom PJSC building, Chistopol town

Quantum channel length: 160 km (45 dB)

Year: 2019 (to be published)
QKD protocol: phase subcarrier wave [1,2]
Wavelength: 1550.12 nm
Mean photon mumber: 0.2
Clock frequency: 100 MHz
Bob loss: 6,4 dB
Quantum channel loss: 45 dB

Detector: SNSPD (Scontel, Russia)
Quantum efficency: 50%
Dark counts: 0.5 Hz

ITMO UNIVERSITY
SMARTS QUANTTELECOM
ТАТТЕЛЕКОМ
KQC 2014 Kazan Quantum Center

1. Gleim, A. V., et al. Optics express 24.3 (2016): 2619-2633.
2. Kozubov, Anton, Andrei Gaidash, and George Miroshnichenko. arXiv preprint arXiv:1903.04371 (2019).

QKD research groups: Russian quantum center (Moscow)

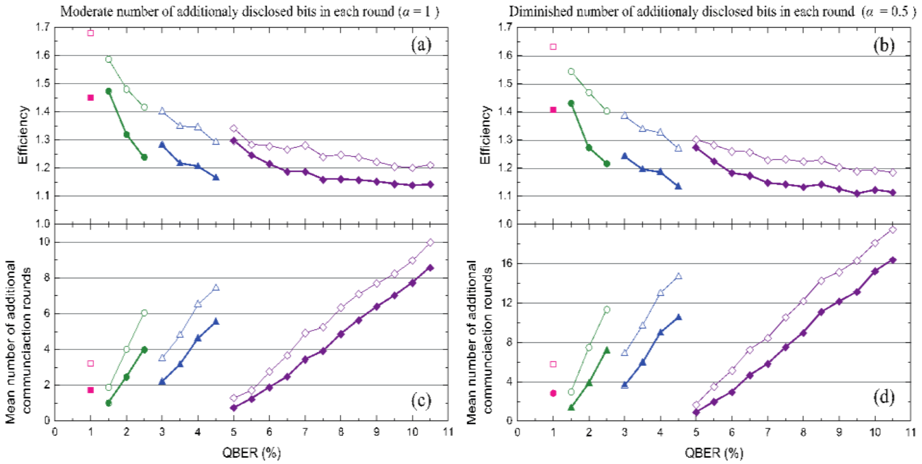
Dr. Yury Kurochkin, leader of quantum comunication group, RQC. Technical director, Qrate LLC.

RQC | Russian Quantum Center

QRATE QUANTUM COMMUNICATIONS

Main development directions:

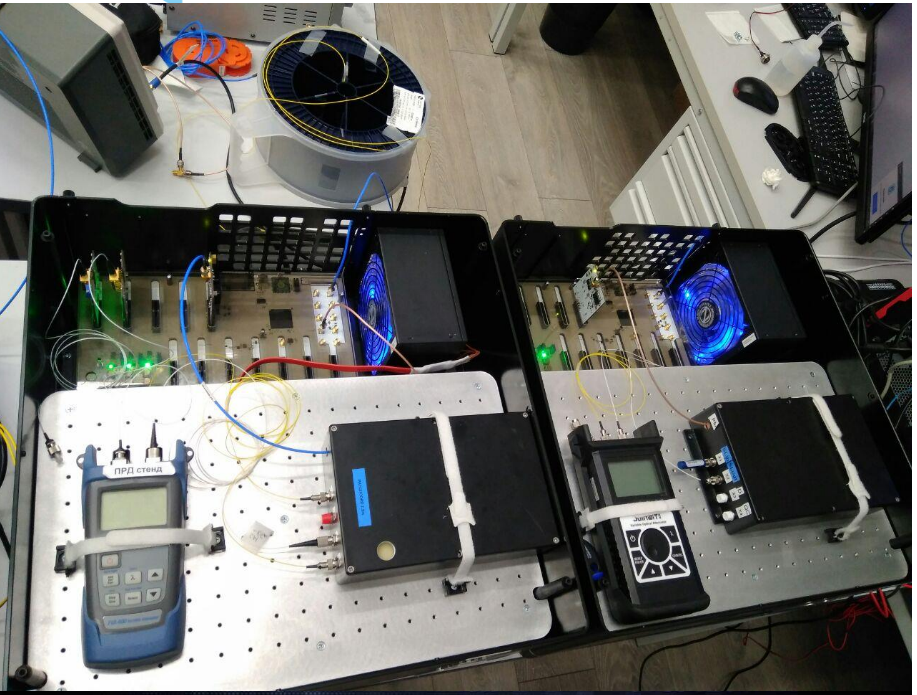
- Fiber and free-space QKD
- Error correction algorithms
- Quantum hacking
- QKD protocols
- Single photon detectors
- Quantum RNGs
- Quantum-secured blockchain
- Quantum networking



QKD research groups: Russian quantum center (Moscow)

RQC | Russian Quantum Center

QRATE QUANTUM COMMUNICATIONS



- 2015 – R&D, experimental demonstration of quantum channel electronic subsystem
- 2015 – QKD project funded by Ministry of Education and science
- 2016 – Developed software platform for quantum key processing
- 2017 – Launched a metropolitan area QKD network in Moscow connecting Gazprombank offices
- 2017 – Developed high-speed (300 MHz) QKD operation electronics
- 2017 – Launched a quantum link between Sberbank offices
- 2017 – Gazprombank infrastructure was used to test quantum key distribution on a blockchain in real-life conditions
- 2018 – Started serial production of QKD systems

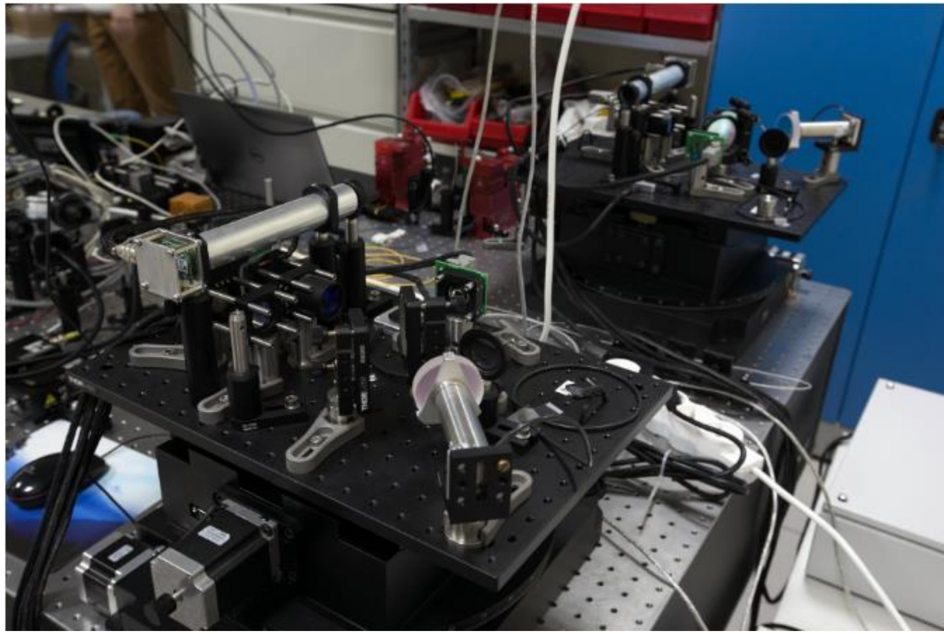
Sources: goqrate.com, https://www.ethnews.com

QKD research groups: Moscow State University

Prof. Sergei Kulik, head of quantum optics lab, NTI center for quantum technology, Moscow State University

Main development directions:

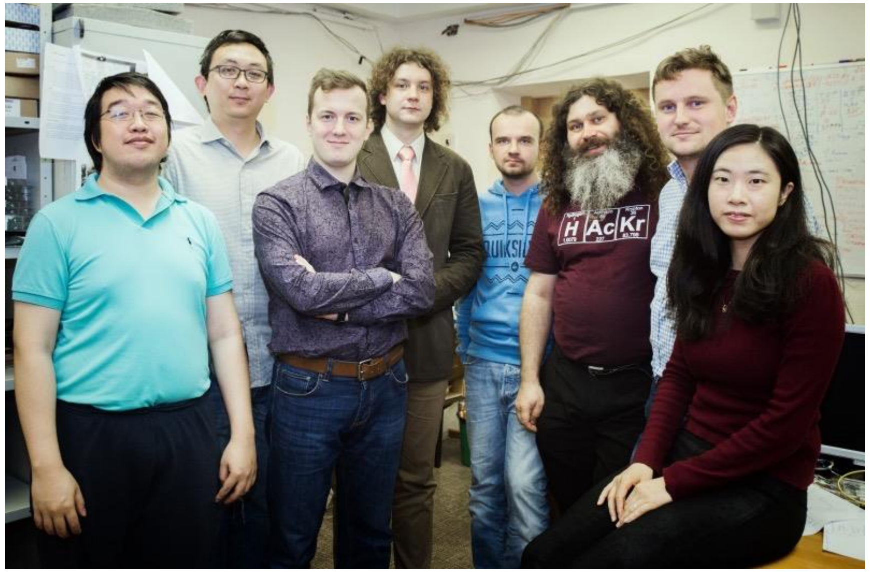
- Fiber and free-space QKD
- Key processing algorithms
- Single photon sources
- QKD protocols
- Single photon detectors
- Quantum RNGs
- Quantum tomography
- Quantum networking

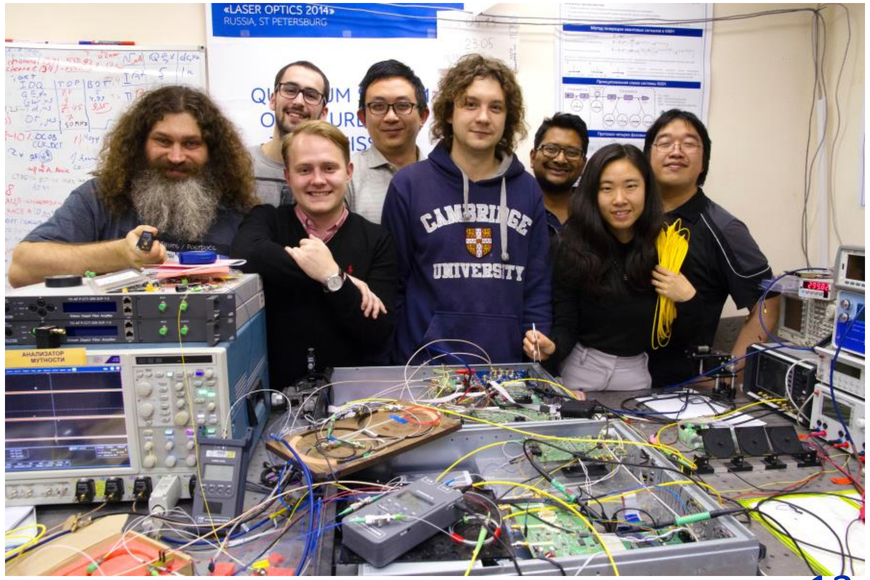


Source: quantum.msu.ru

Quantum hacking research

- **ITMO University QKD system** was analyzed for possible loopholes by Quantum Hacking group (then at University of Waterloo, Canada). Report publication pending.
- Latest results:
  - Laser damage attack against optical attenuators in quantum key distribution // arXiv:1905.10795 [quant-ph]
  - Controlling single-photon detector ID210 with bright light // arXiv:1905.09380 [quant-ph]
- Russian Quantum Center is also actively involved in quantum hacking research.

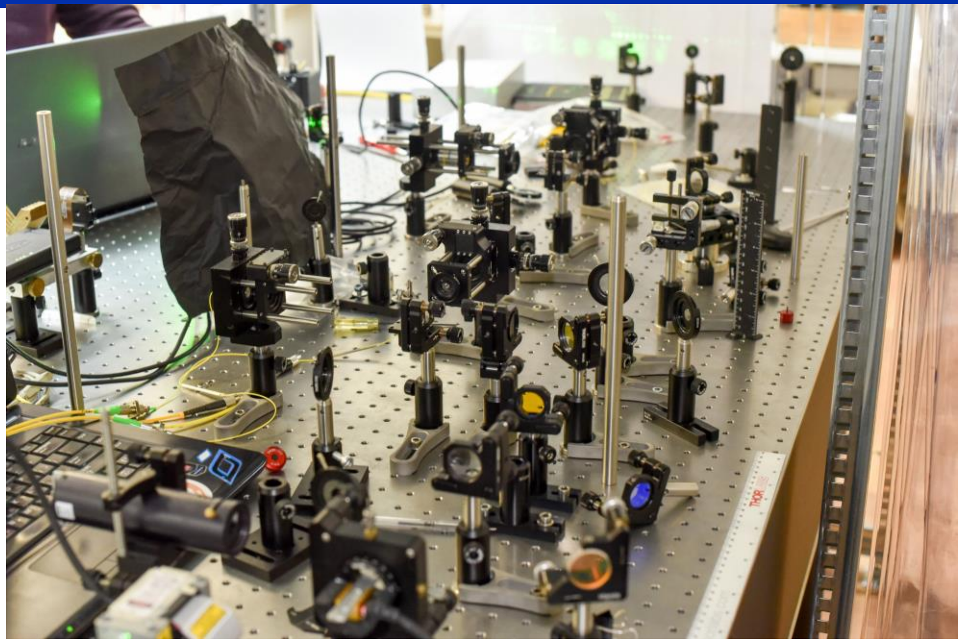




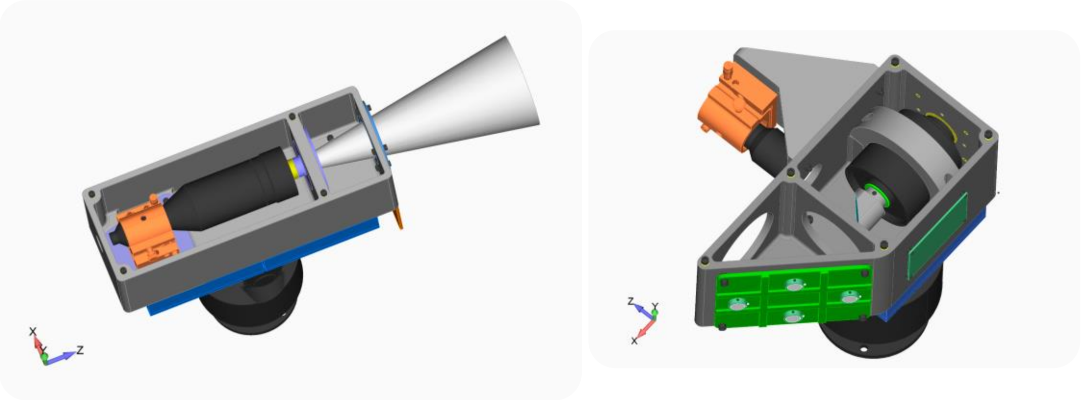
Quantum communication technology groups: Zavoisky Physical-Technical Institute (Kazan)

Main development directions:

- Free-space QKD
- Single photon sources
- High-dimensional quantum states
- Angular momentum photon encoding



Prof. A.A. Kalachev, director of Kazan Zavoisky Physical-Technical Institute of RAS



Automatized precise telescopic systems for free-space QKD

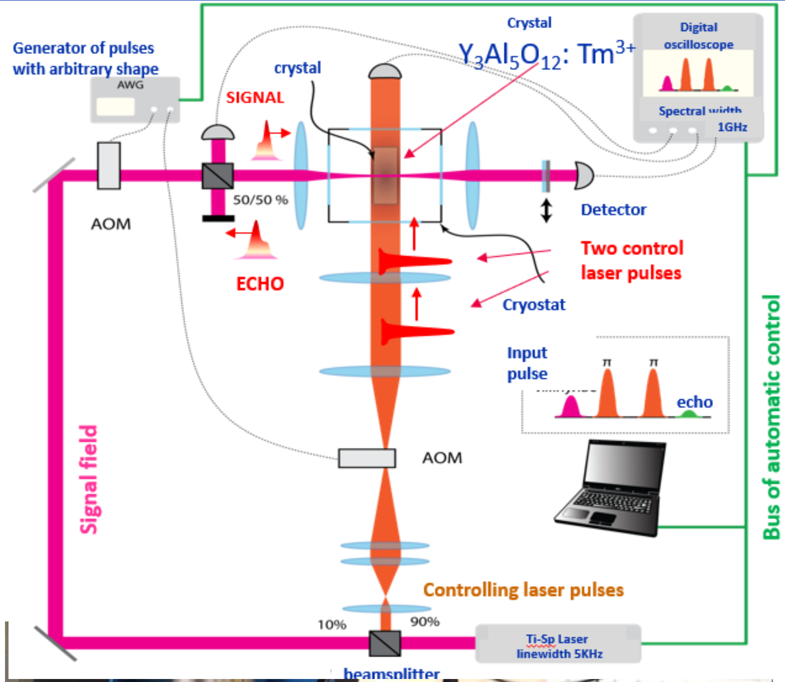
Quantum communication technology groups: Kazan Quantum Center (Kazan)

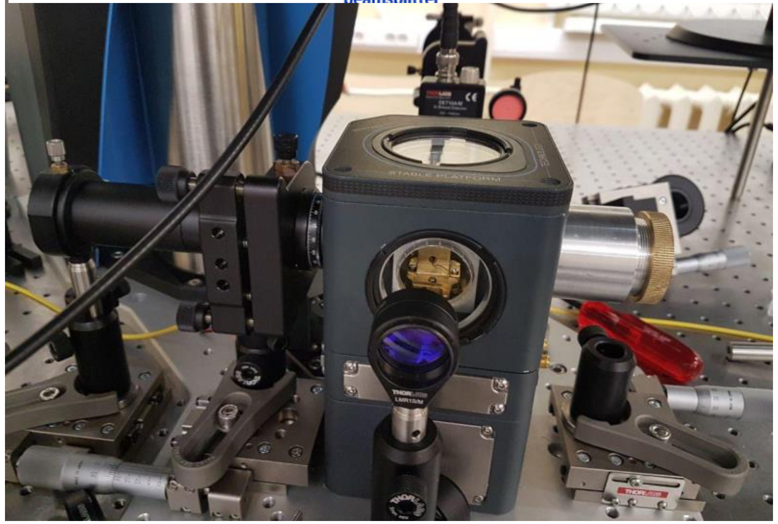
Prof. S.A. Moiseev, director of Kazan Quantum Center, KRNTU-KAI

Kazan Quantum Center

Main development directions:

- Optical quantum memory
- Quantum repeaters
- Fiber optical QKD
- Quantum networking
- QKD protocols
- Quantum sources





Experimental setup of ROSE quantum memory

QKD standartization in Russia

Technical Committee for standartization "Cryptography and security mechanisms"

- Encryption methods
- Blockchain technology
- Message authentication
- Digital signatures

infotecs · Московский государственный университет имени М.В.Ломоносова · RQC Russian Quantum Center · СМАРТС · SMARTS QUANTTELECOM

and others...

https://tc26.ru/en/

TC 194 Cyber-physical systems

Key Technologies

- «Internet of Things»
- «Smart Cities»
- «Big Data»
- «Smart production»
- «Artificial Intelligence»
- «Smart Energy»

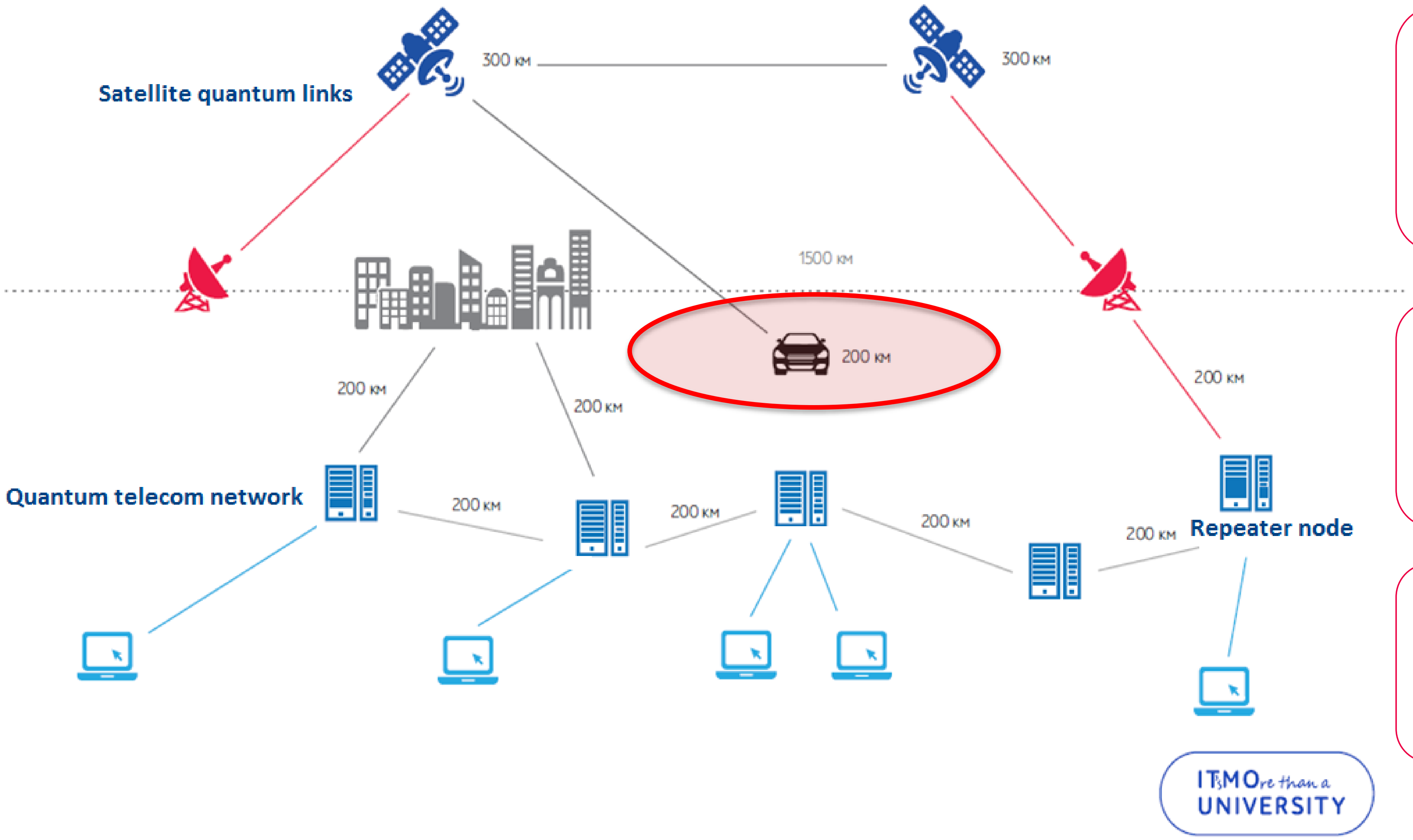
Ростелеком · Московский государственный университет имени М.В.Ломоносова · KASPERSKY lab · Национальный исследовательский университет «Высшая школа экономики» · РВК · МГТУ 1830 · Газпром нефть · РБО · Университет ИТМО · РУС СОФТ · Ангстрем

and others...

- QKD applictions
- Network infrastructures
- Internet of things
- Big data

https://tc194.ru/en/

Our view of secure quantum future



User classes

Groud network nodes
Satellites
Unmanned vehicles
Drones and robots
Industrial internet

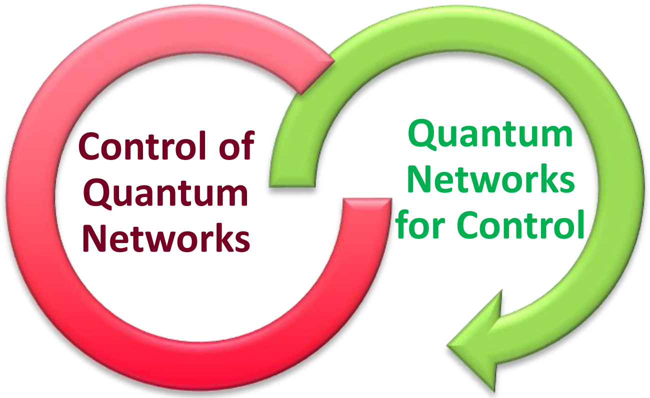
Application areas

Robotics
Smart transport
Secure satellite communication
Distributed quantum calculations

New markets

Quantum communication devices
Quantum network operators
Quantum computing
Security services

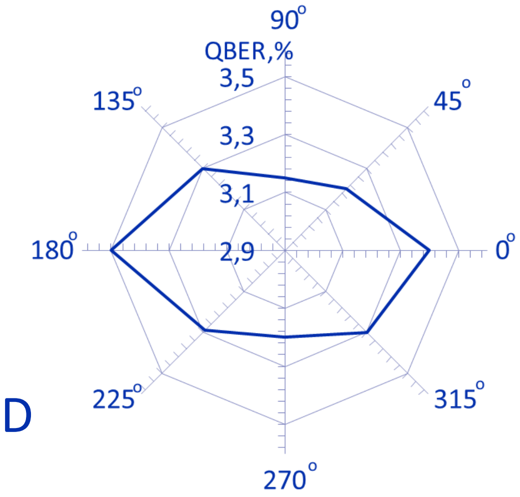
QKD for securing cyber-physical systems





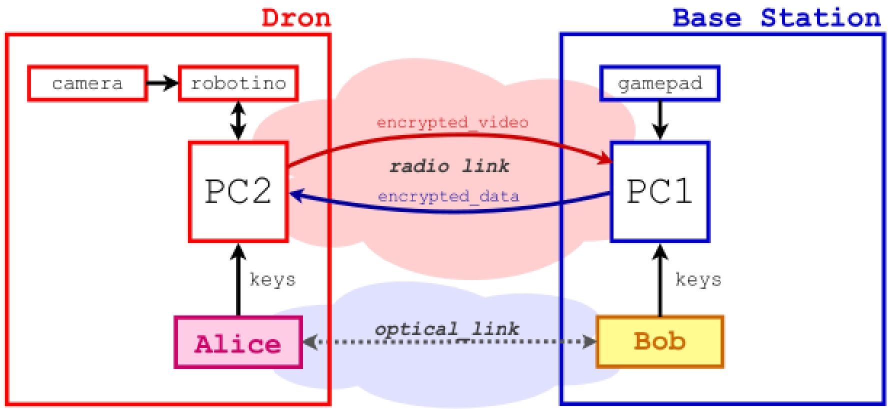
Photos of the implementation: SCW QKD system module, the gamepad issuing movement commands, the mobile robot with a camera operating through a QKD-protected channel.

- Quantum keys **for securing data plane** of cyber-physical systems (e.g. robots, drones)
- Robots as reliable **mobile trusted repeaters** for QKD networks



Project goals

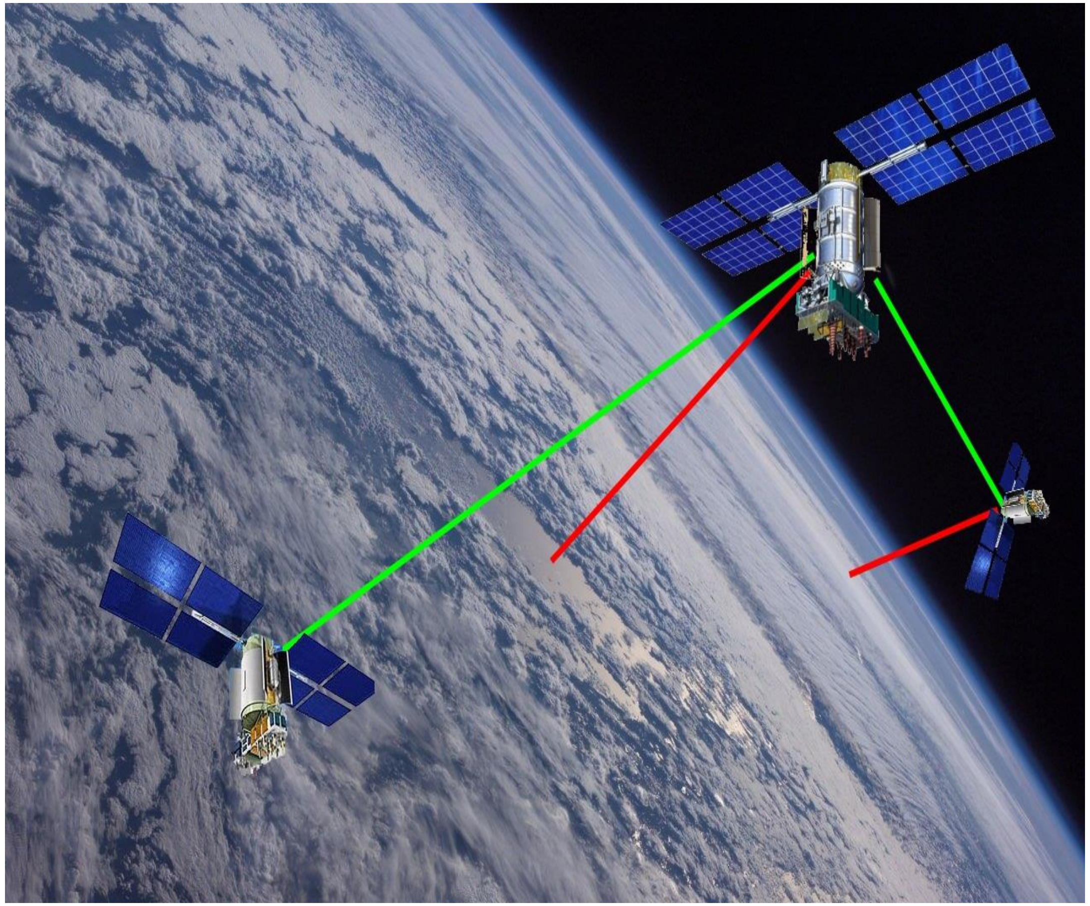
- Short-term: using quantum keys for securing control and data planes of mobile robots
- Mid-term: developing mobile QKD stations (Alice module on robot)
- Long-term: developing metropolitan area QKD networks with cyber-physical and stationary nodes



QKD in space: roadmap

"Satellite QKD system with 1-10 kbit/s quantum and 1-10 Gb/s optical channel"	
Year	Activity
2019	Ground station prepared
2020	Satellite QKD prototype developed
2021	QKD module adapted for satellite
2022	Field test on the ground
2023	First satellite launched
2024+	Development of orbital group

ROSCOSMOS

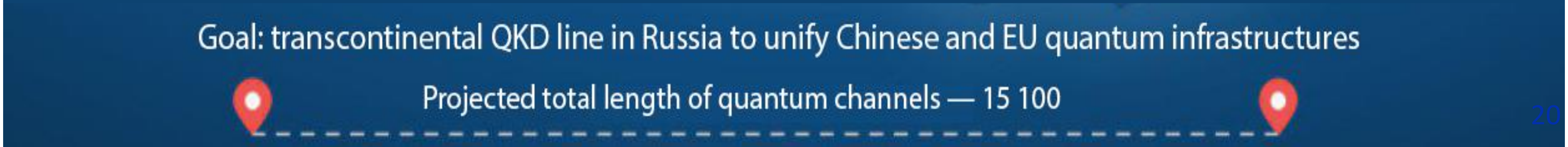


Source: "Digital Economy: Quantum technologies" roadmap, 2019

- All main QKD groups in Russia are involved into free-space QKD research
- These activities are to be included into several Roskosmos development programs and supported by Union state of Russia and Belarus program "Complex-SG" (2019-2023).

QKD: new international security opportunities

We are ready to work with our international partners on creating **regional and global quantum-secure infrastructures** involving backbone and metropolitan fiber QKD networks and satellite QKD channels.



Conclusion

- Quantum technologies have become national research and application priorities for the next five years in Russia.
- Quantum key distribution technology in Russia is ready for industrial integration.
- Proper QKD certification and standardization procedures are in course of development both on national and international level.
- These developments will become a foundation for nation-wide QKD lines in Russia, acting as a unifying link between Chinese and European quantum infrastructures.

ITsMOre than a UNIVERSITY

ITMO UNIVERSITY

Thank you for you attention!

viegorov@itmo.ru