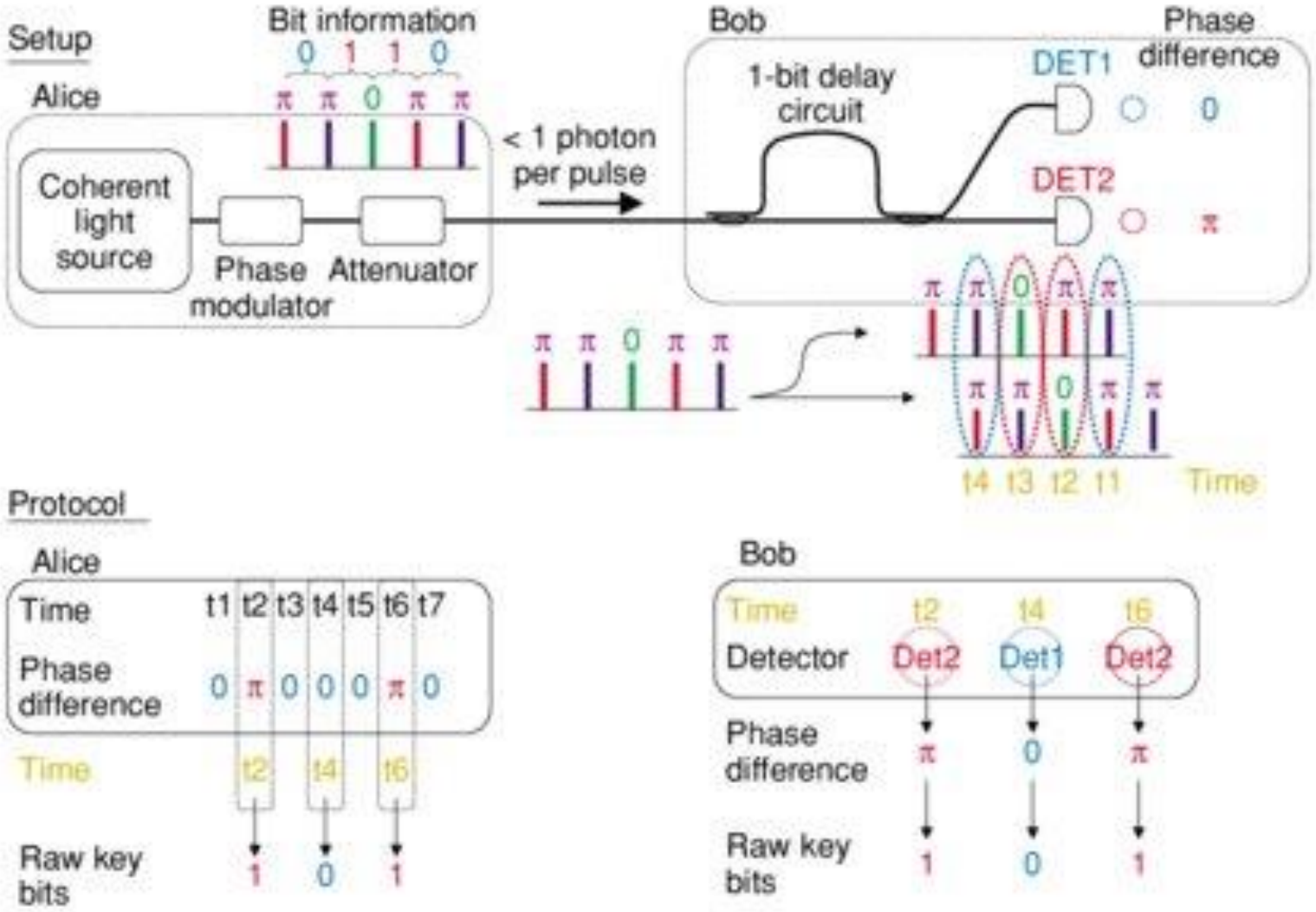
Lecture 5: Implementations of quantum cryptography

Content

- Properties of fiber-optic and open channels.
- Fiber-optic, atmospheric and satellite systems and their main characteristics.
- Key distribution networks.
- Interfacing to classical encryptors.
- Commercialization.

Differential phase shift-quantum key distribution



[Takesue, Hiroki & Honjo, Toshimori & Tamaki, Kiyoshi & Tokura, Yasuhiro. (2009). Differential phase shift-quantum key distribution. Communications Magazine, IEEE. 47. 102 - 106. 10.1109/MCOM.2009.4939284.]

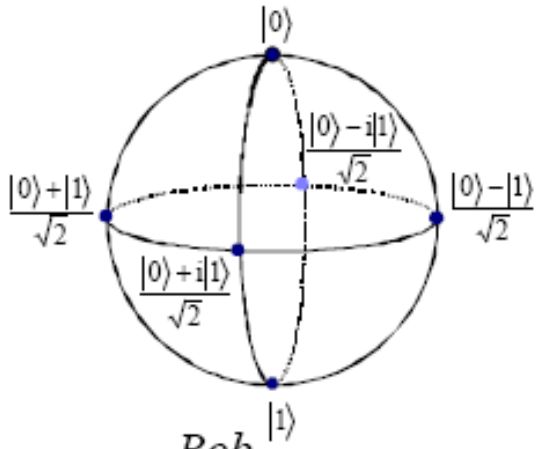
QRATE QUANTUM COMMUNICATIONS

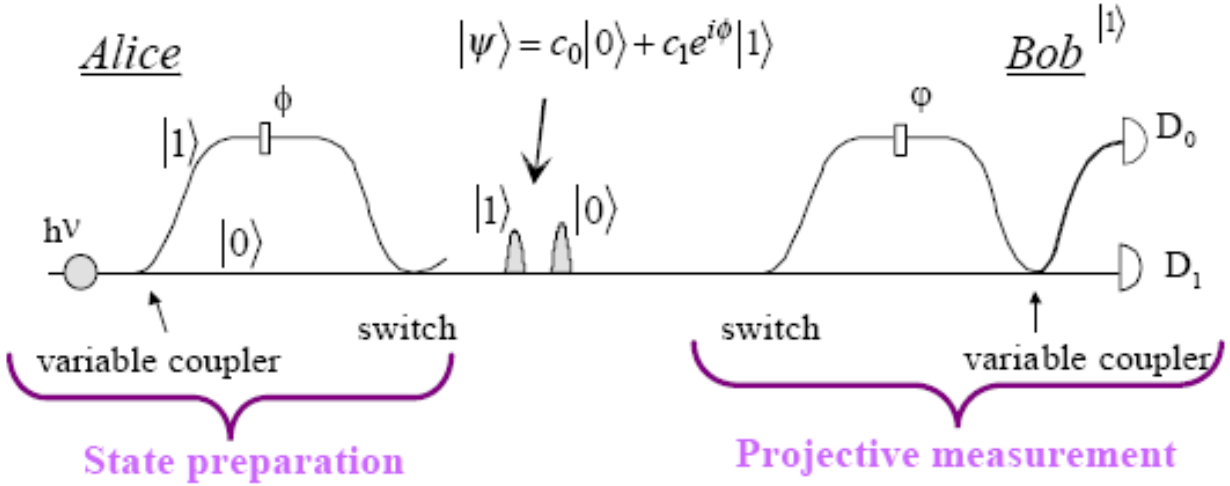
РКЦ Российский Квантовый Центр

How to prepare states: Phase encoding

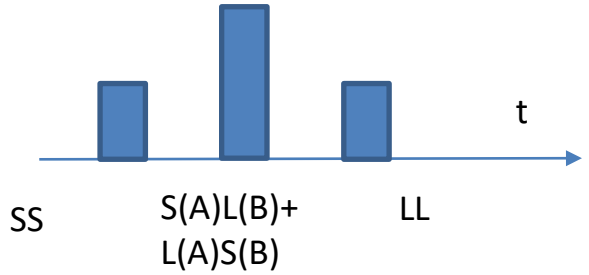
- **qubit :** $|\psi\rangle = c_0|0\rangle + c_1 e^{i\phi}|1\rangle$

- **any qubit state can be created and measured in any basis**

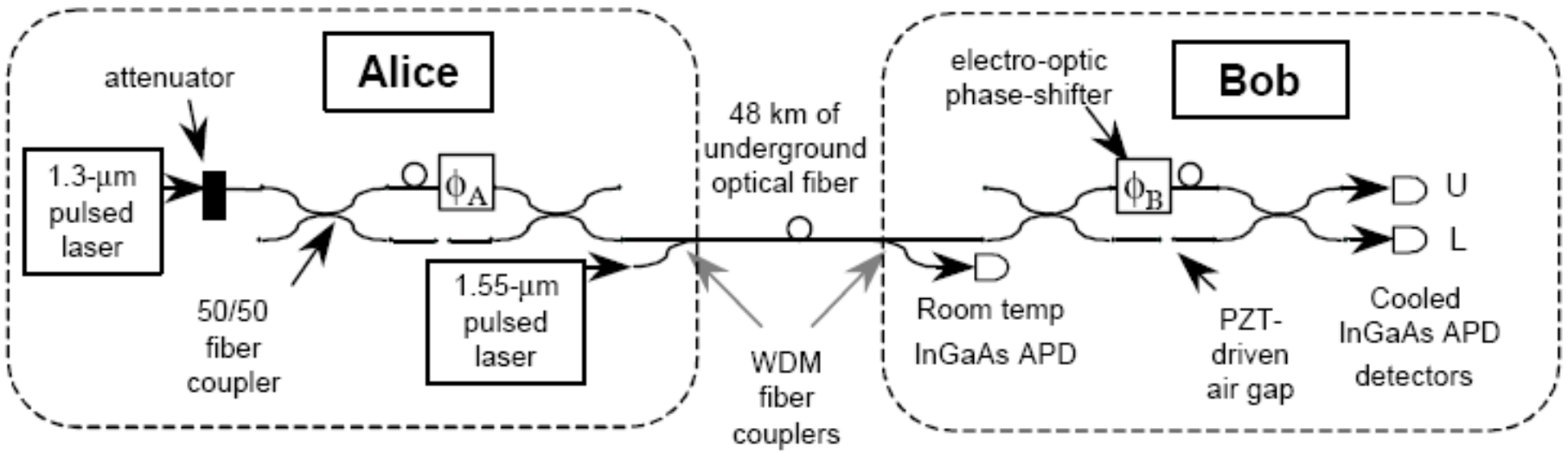




[C. H. Bennett, Phys. Rev. Lett. 68, 3121 (1992)]



Practical realization



As the two coherent contributions are separated by a few nanoseconds but propagating along the same fiber, the are essentially no temperature or stress induced fluctuation.

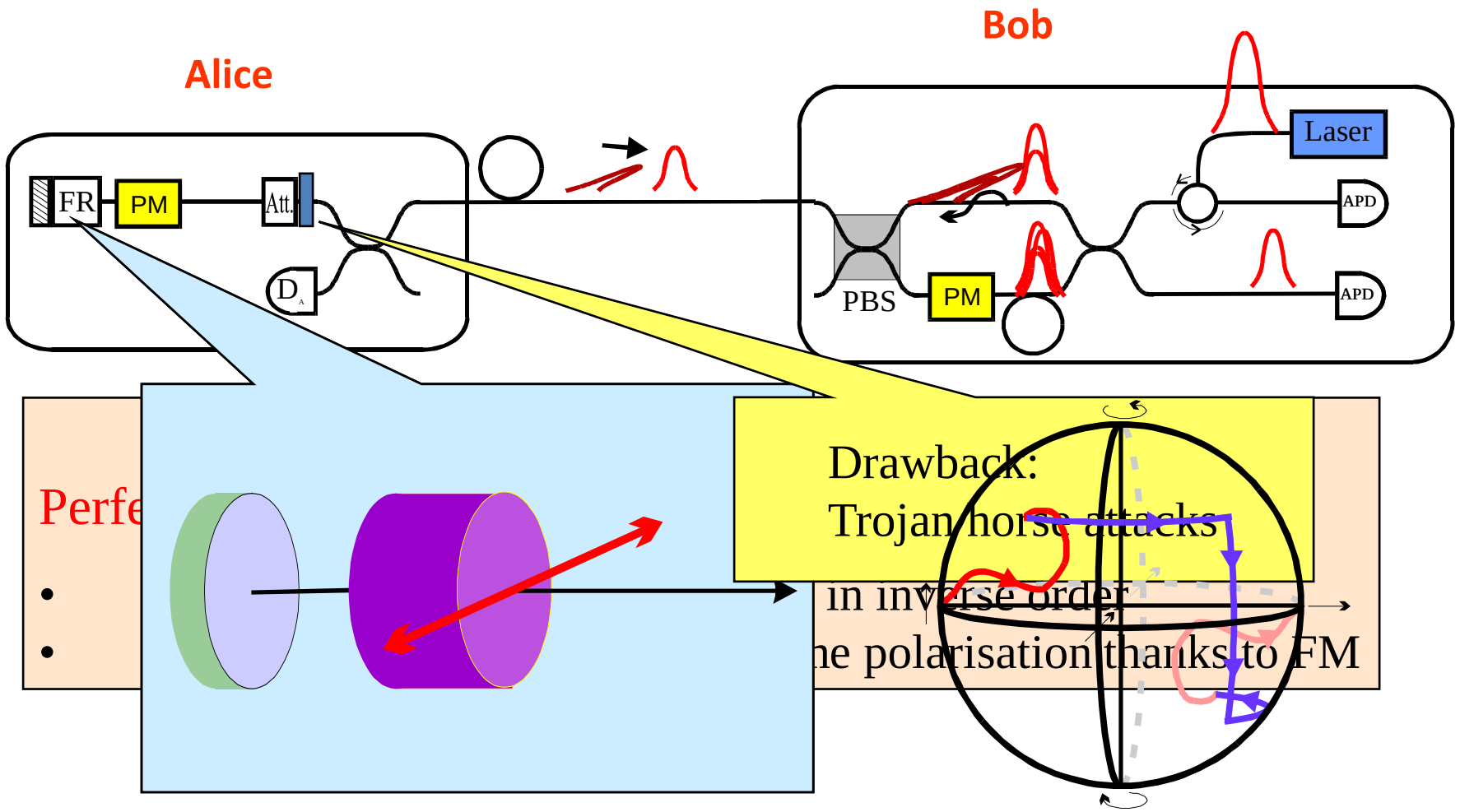
[R. J. Hughes et al., Advances in Cryptology – Proceeding of Crypto'96, Springer, (1996)]

QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

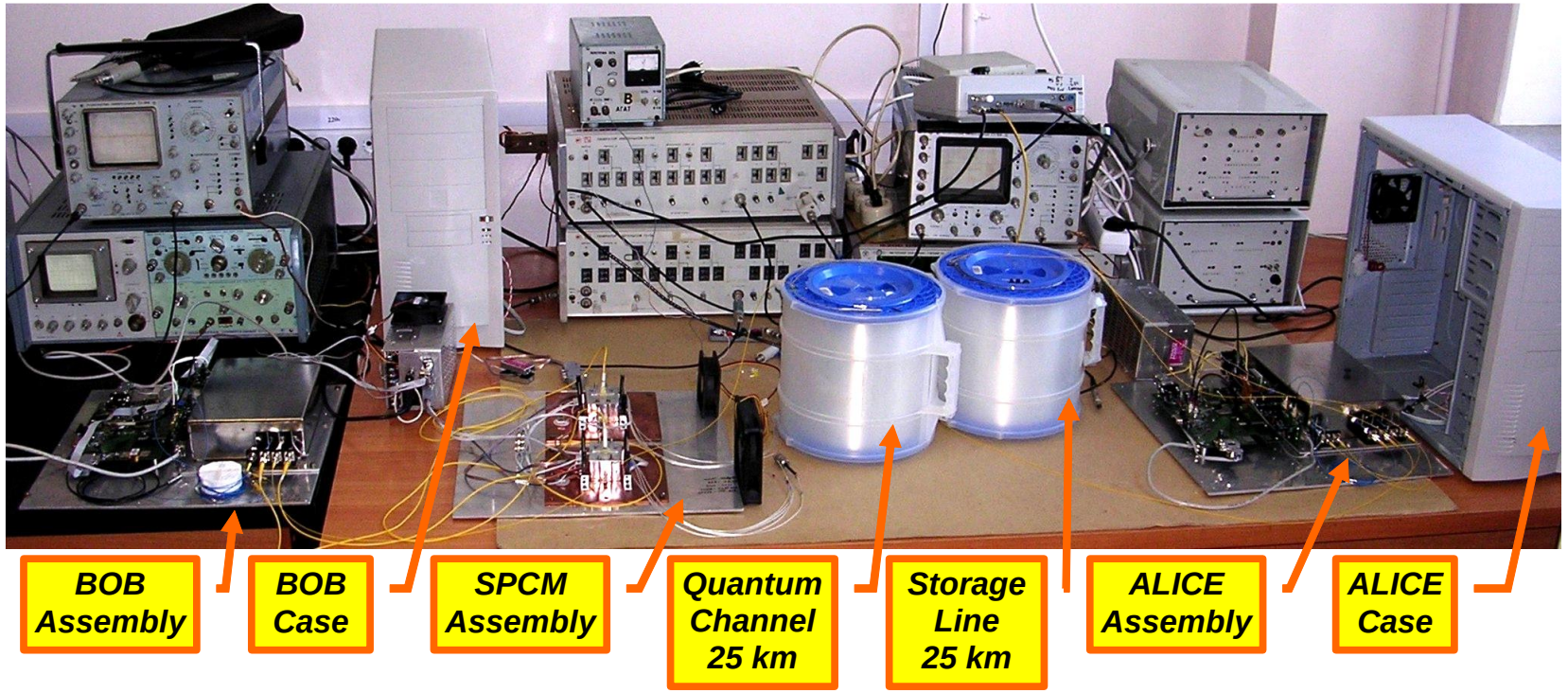
Plug & Play

Phase; Fiber; 67KM
[D. Stucki et al., New J. Phys. 4, 41(2002)]



First commercial product by ID Quantique used this scheme

First in Russia fiber based quantum cryptography setup developed in ISP



25 km quantum channel of single mode fiber for 1550nm
10% quantum efficiency at 5*10-5 dark count probability per 3 ns gate.
Operates at 0,1-0,2 photon/pulse (BB84 protocol)
30 bit/s sifted key rate demonstrated

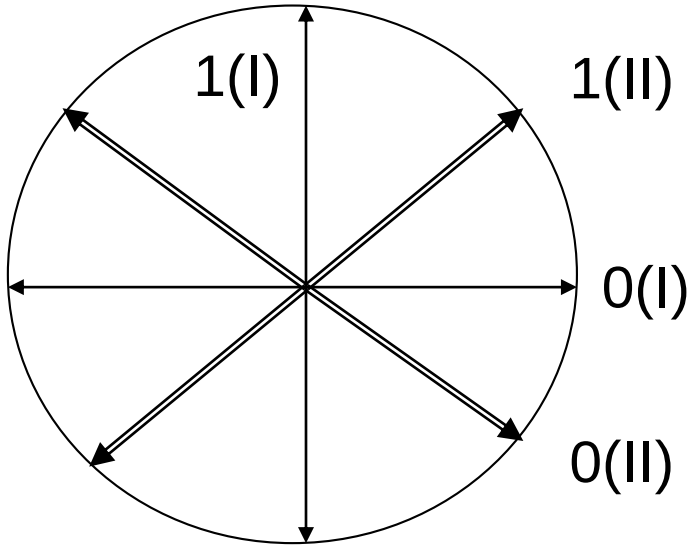
QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

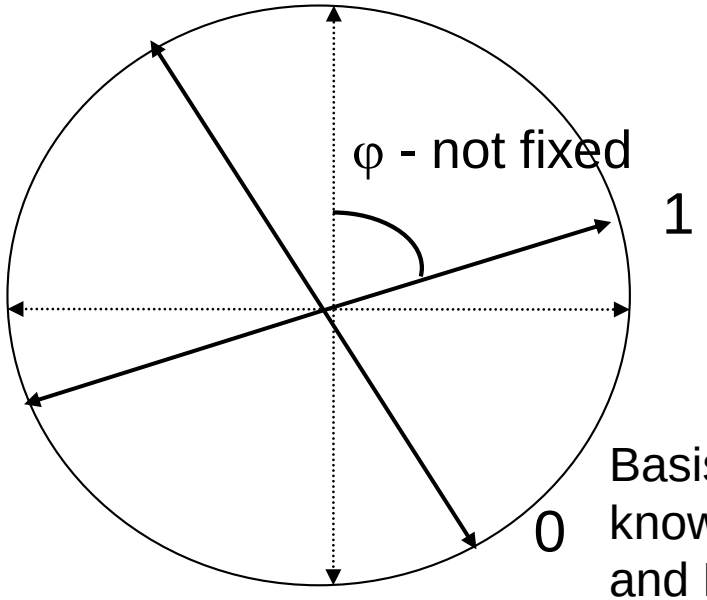
Floating basis protocol

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

Basis shift also protects from the detector manipulation attack

QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

Coherent one way protocol is inspired by classical communication

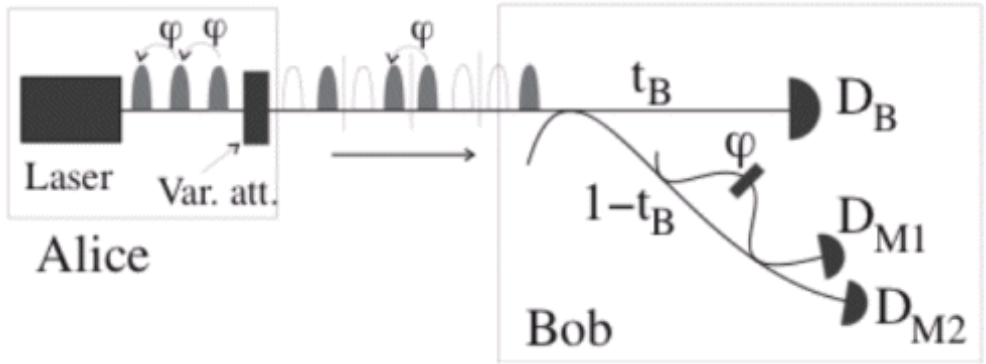
Coherent one way (COW) protocol (currently used by ID Quantique and University of Geneva)

Logical “0” 

Logical “1” 

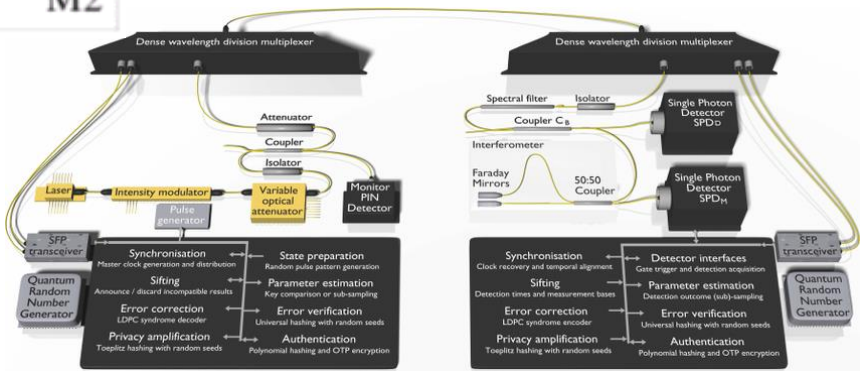
Decoy state  is used to monitor the attempt to unauthorized measurement

Unconditional proofs in process



A fast and versatile QKD system with hardware key distillation and wavelength multiplexing

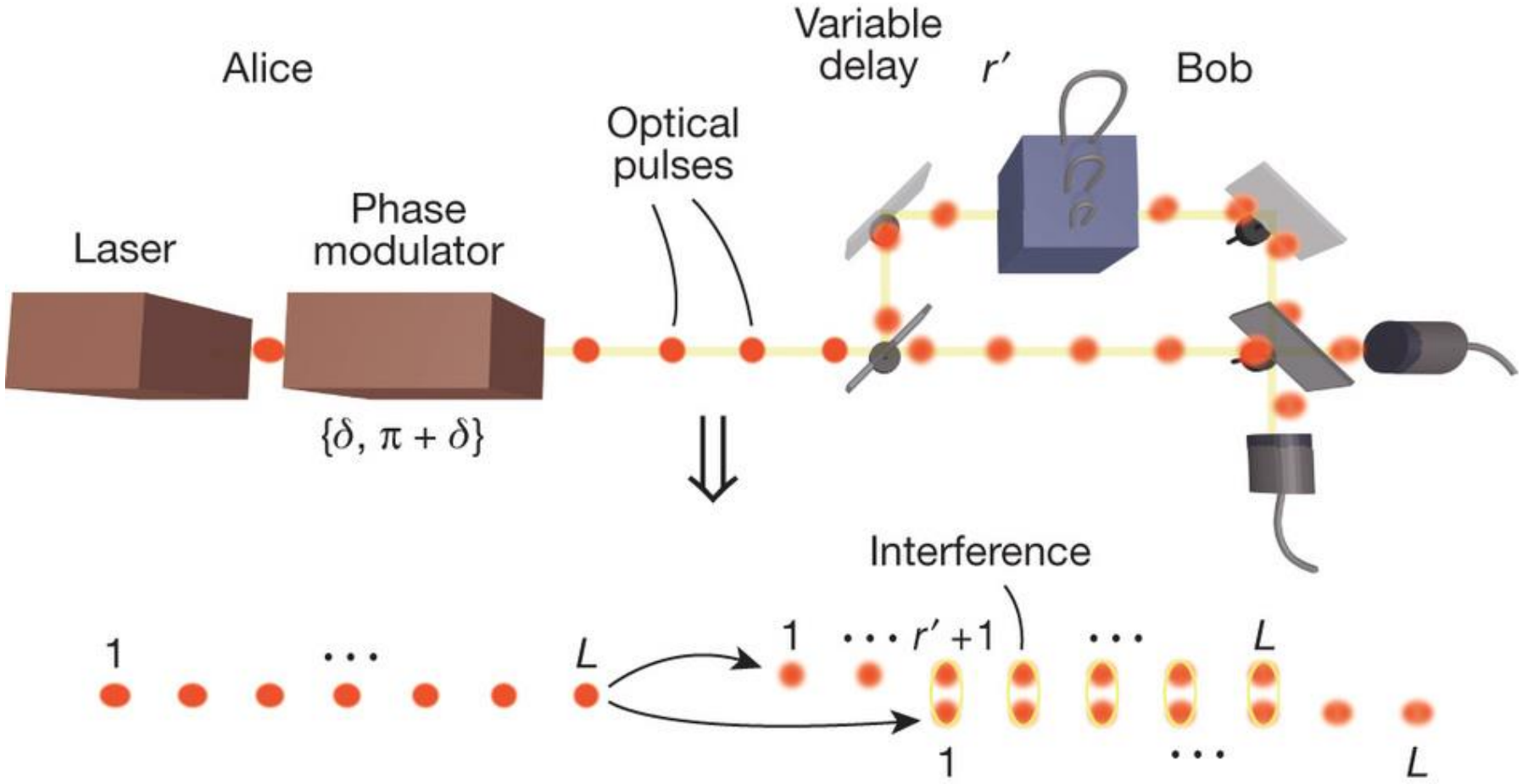
Nino Walenta[1], Andreas Burg[3], Dario Caselunghe[2], Jeremy Constantin[3], Nicolas Gisin[1], Olivier Guinnard[1], Raphael Houlmann[1], Pascal Junod[4], Boris Korzh[1], Natalia Kulesza[2], Matthieu Legré[2], Charles Ci Wen Lim[1], Tommaso Lunghi[1], Laurent Monat[2], Christopher Portmann[1,6], Mathilde Soucarros[2], Patrick Trinkler[2], Gregory Trolliet[5], Fabien Vannel[5], Hugo Zbinden[1]



QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

Distributed-phase-reference QKD

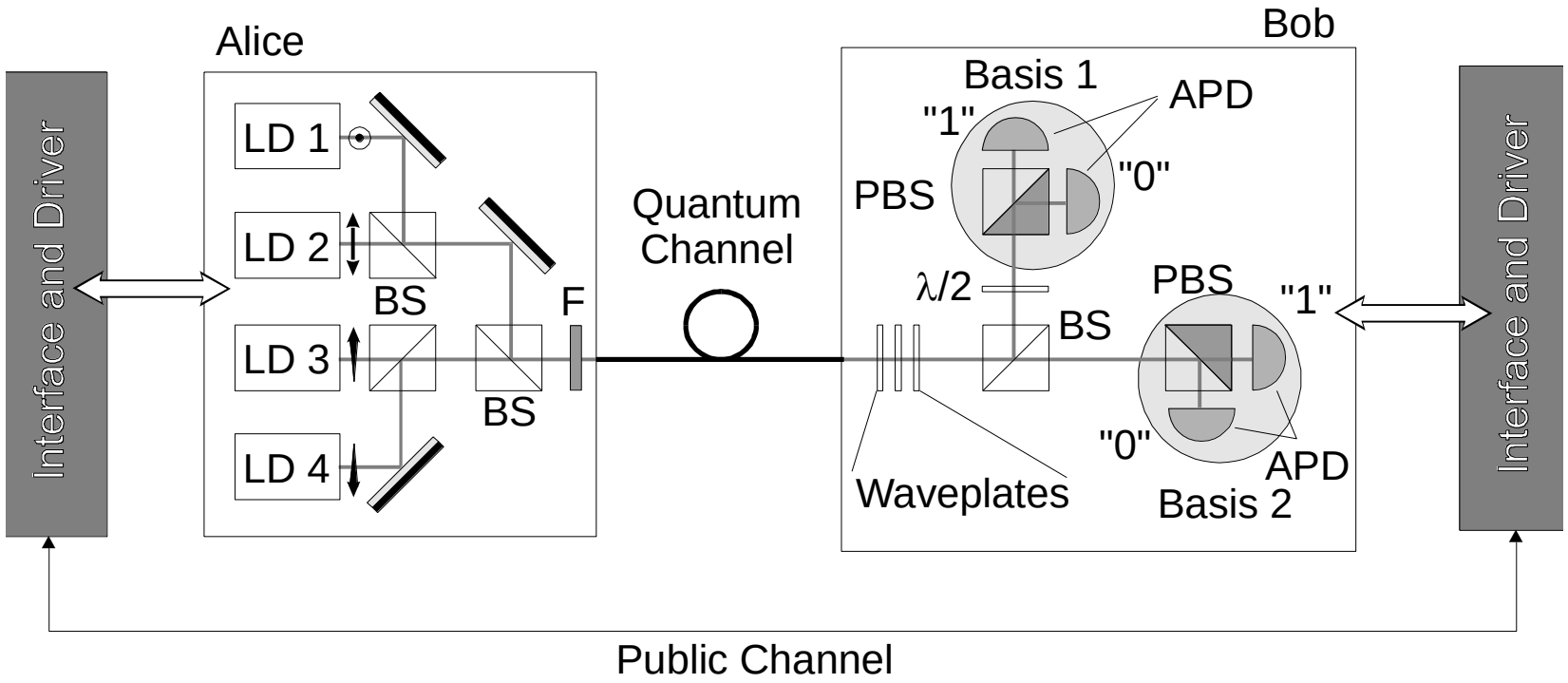


Interference between neighbor pulses will be broken in the case of the photon number splitting attack

K. Inoue, E. Waks, Y. Yamamoto, Phys. Rev. Lett. 89, 037902 (2002)

How to realize: Polarization Coding

Typical system



Polarization encoding can be low cost but it is questionable in vibrating fiber

Group in Bristol proposes to use polarization encoding but it is questionable in vibrating fiber

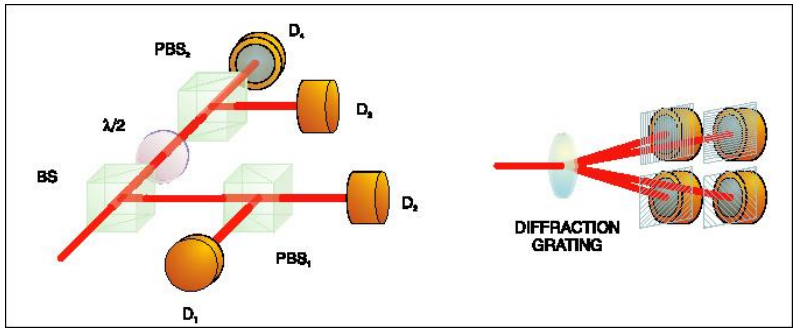
Low Cost and Compact Quantum Key Distribution

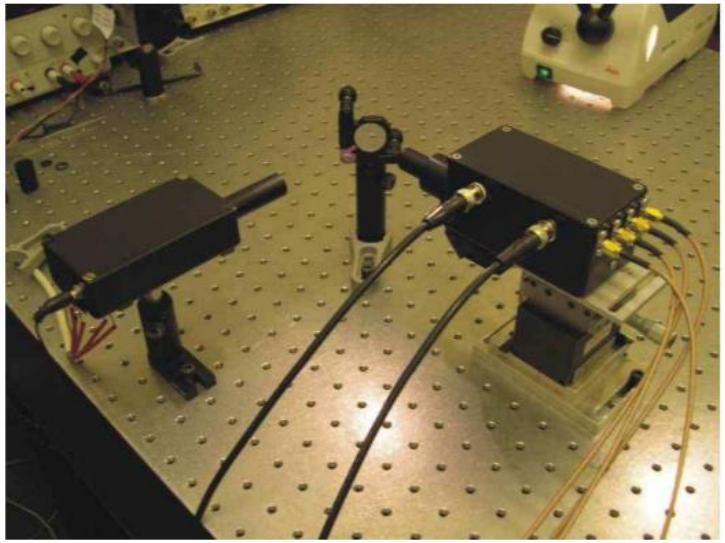
J L Duligall[1], M S Godfrey[1], K A Harrison[2], W J Munro[2] and J G Rarity[1]

[1] Department of Electrical and Electronic Engineering, University of Bristol, University Walk, Bristol, BS8 1TR

[2] Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol, BS34 8QZ

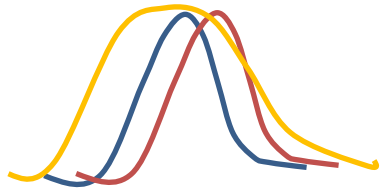
E-mail: joanna.duligall@bristol.ac.uk





Pulse difference is the issue:

- Wavelength
- Width
- Shape
- Time delay



Fiber polarization controllers operate at kHz frequency

QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

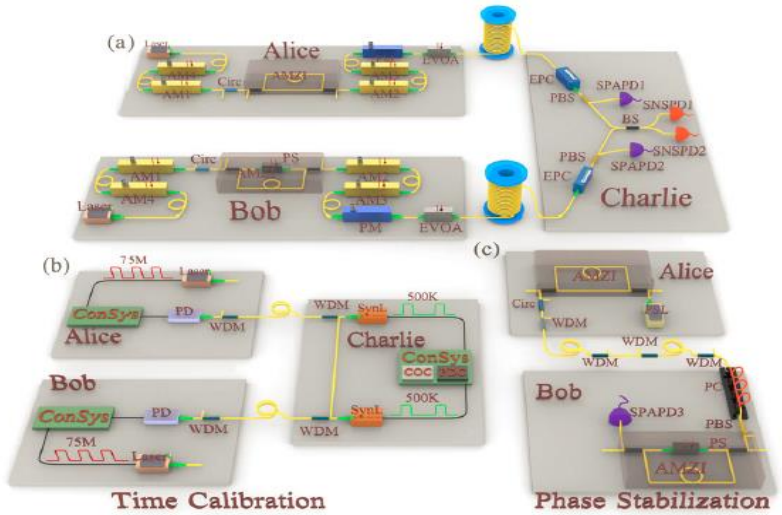
Is the polarization bad case for fiber channels?

Polarization is drifting in the fiber
Stability in the lab: minutes
Stability in the common fiber building-building: seconds.

Number of optical schemes are polarization sensitive
MDI QKD:

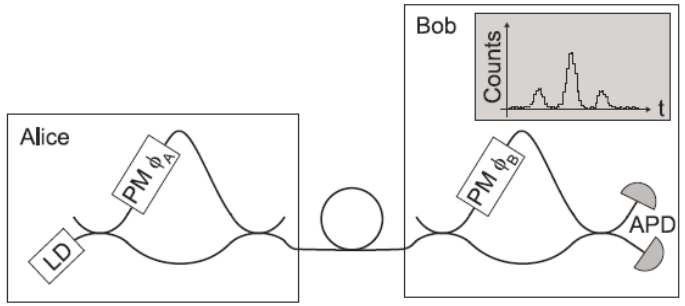
Yan-Lin Tang, et al., “Measurement-Device-Independent Quantum Key Distribution over 200 km”, PRL 113, 190501 (2014)

A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. 111, 130501 (2013).



Phase modulators are polarization sensitive. If Bob contains phase modulator most probably you need to control polarization

Marand, C., and P.D. Townsend, 1995, “Quantum key distribution over distances as long as 30 km”, Optics Letters 20, 1695-1697.



QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

How to prepare four BB84 polarization states?

One can use 4 lasers
Fast and convenient
Inseparability problem

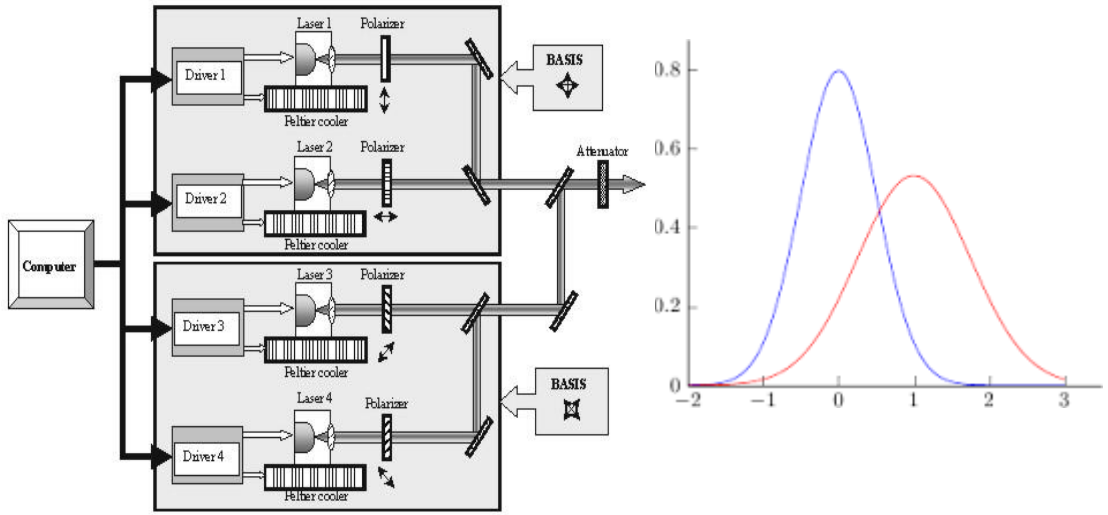
Lasers can be different in frequency, time or direction

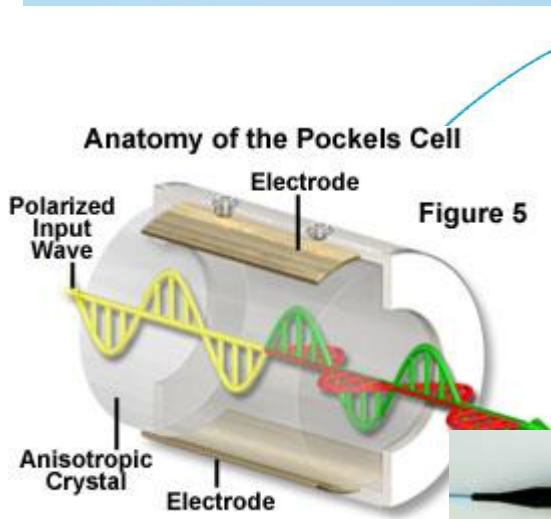
It is possible to construct full polarization controller from LiNbO3 crystals
Piezo driven polarization controllers are not fast enough for random state preparation

Pockels cell allows us to prepare four maximum nonorthogonal states

It was used in the first QKD experiment (Bennett, Ch.H., F. Bessette, G. Brassard, L. Salvail, and J. Smolin, 1992a, “Experimental Quantum Cryptography”, J. Cryptology 5, 3-28.

Modern LiNbO3 modulators work with much lower voltage and higher bandwidth





300V

40 GHz

QRATE QUANTUM COMMUNICATIONS

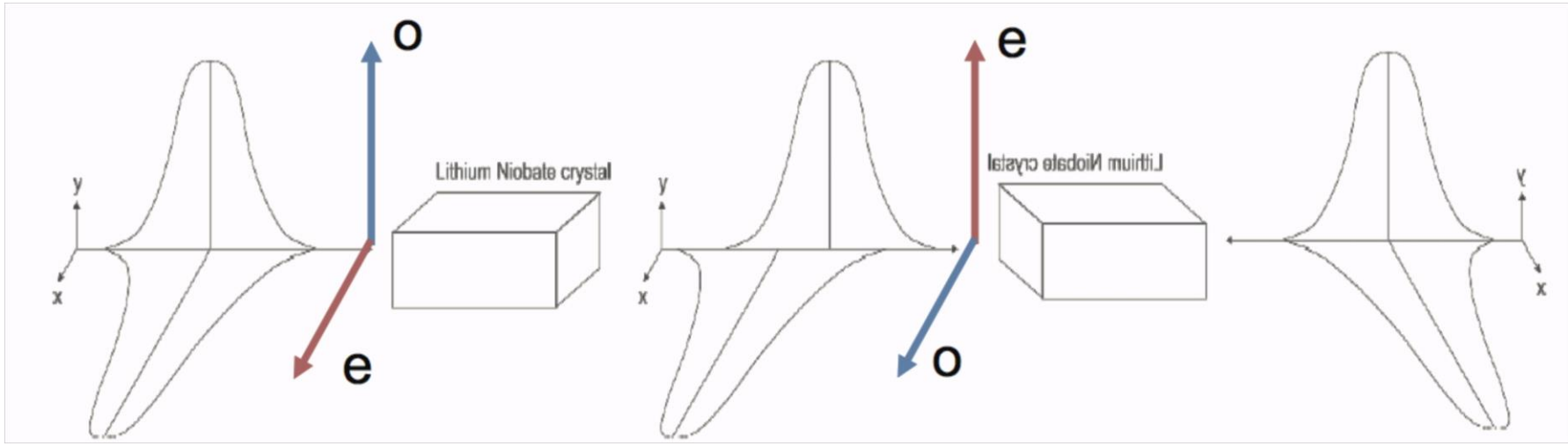
РКЦ Российский Квантовый Центр

How do we prepare states?

We decide to use modern 10GHz fiber phase modulator as Pockels cell

Even small time imbalance will break interference in the case of chirped pulse

We propose to use identical phase modulator on the Bob side rotated to π/2 to compensate the polarization mode dispersion.



Bob use this modulator for active basis choice

Two detectors are used instead of four

This scheme will allow to make QKD transmitter that of a USB stick size.

A. Duplinskiy, V. Ustimchik, A. Kanapin, V. Kurochkin, Y. Kurochkin. Low loss QKD optical scheme for fast polarization encoding // Opt. Express 25(23), 28886-28897 (2017).

QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

States prepared by Pockels cell

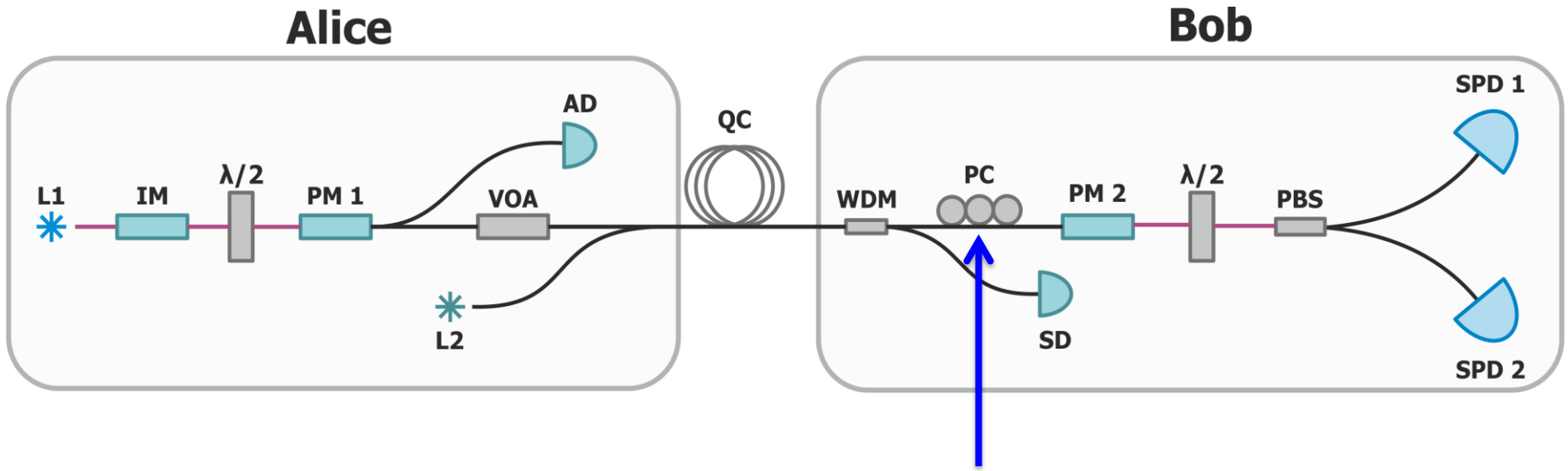
Polarization distortion induced by long quantum channel are compensated by polarization controller

At the entrance of Alice's polarization controller amplitudes of two polarization components should be equal (polarization is not obligatory linear)

BB84 states are not obligatory diagonal +45, diagonal -45, left and right. It can be any pair of maximally non orthogonal states combined by equal horizontal

Δφ	SOP	Δφ	SOP
0		0	
π/2		π/2	
π		π	
3π/2		3π/2	

Polarization tuning

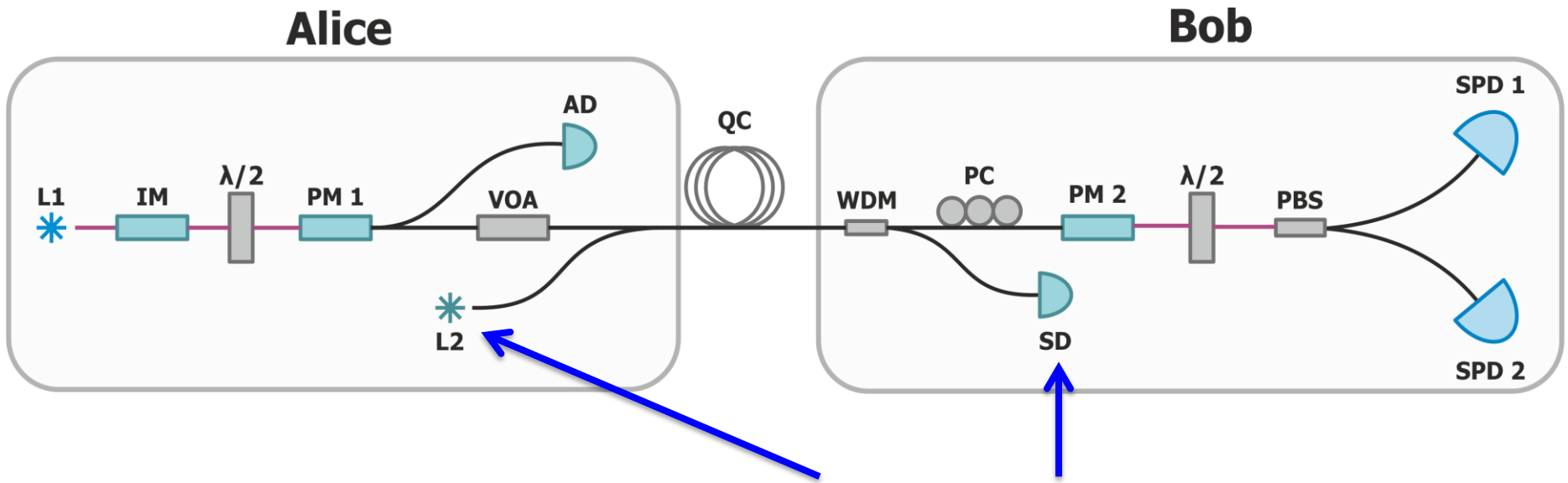


Polarization can be tuned with piezoelectric-polarization-controller
Alice and Bob can announce part of the key to monitor QBER (usually it is “decoy” state events)
If QBER exceeds threshold (for example 6%), Alice Increases Amplitude and sends predefined sequence to tune polarization controller
Bob tunes polarization to decrease QBER below required level (for example 3.5%)
Bob varies 3 parameters to tune polarization. It takes about 20-40 seconds.

QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

Clock tuning



To synchronize clock we use additional laser and syncrodetector
To reduce the effect on single photon detectors we use wavelength and time division
To remain good detector synchronization we need to keep Alice and Bob clock difference below 100-150 ps.
We send trains of syncropulses about 800 times a second

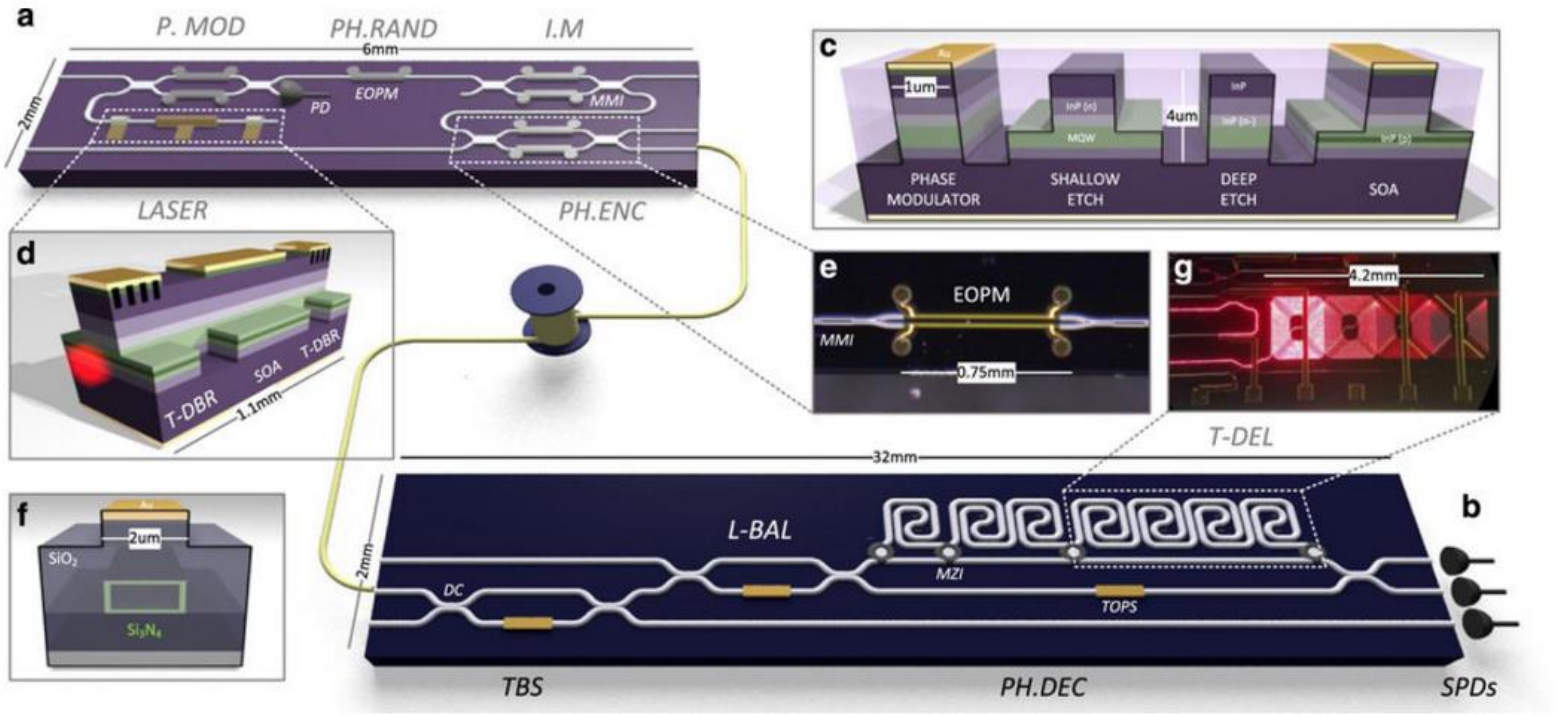
QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

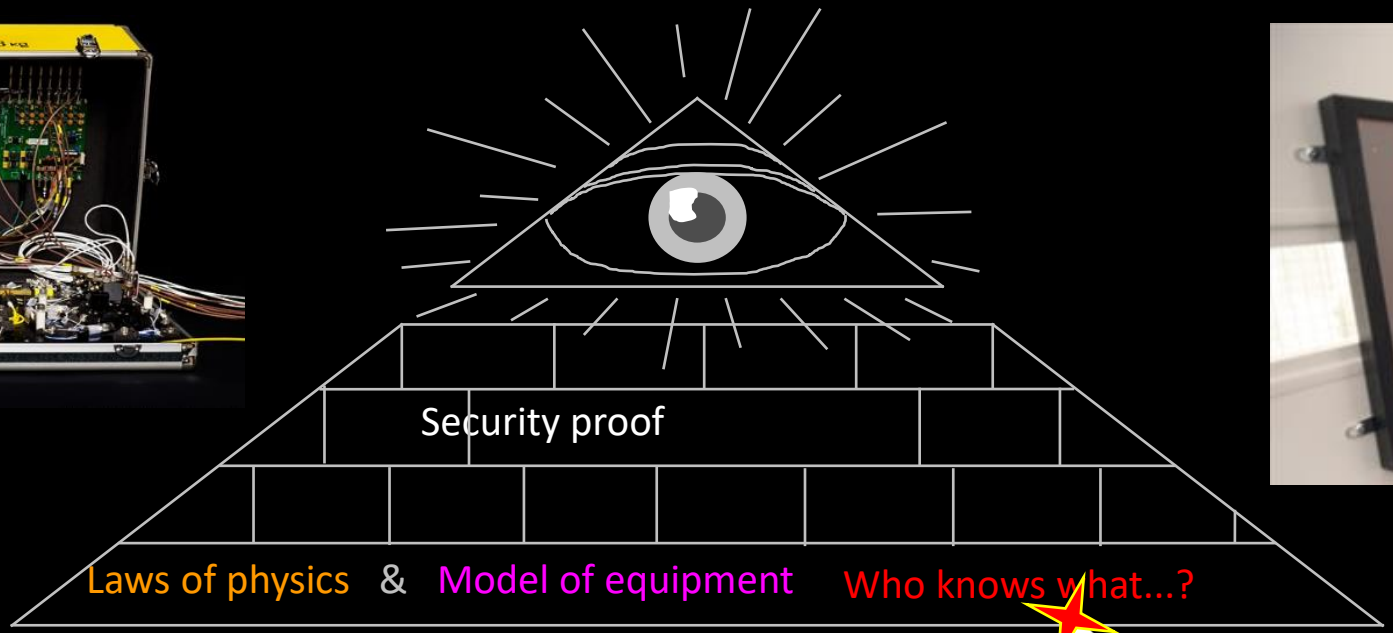
Photonic chips will dramatically change the QKD setup size

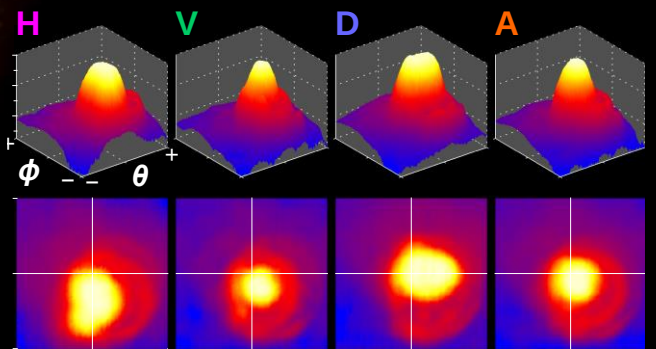
Using photonic chip all QKD optics can be made on centimeter size chip
The only problem is the current cost of such chip is 2-10 kEUR

From: Practical challenges in quantum key distribution



Limits on physical security

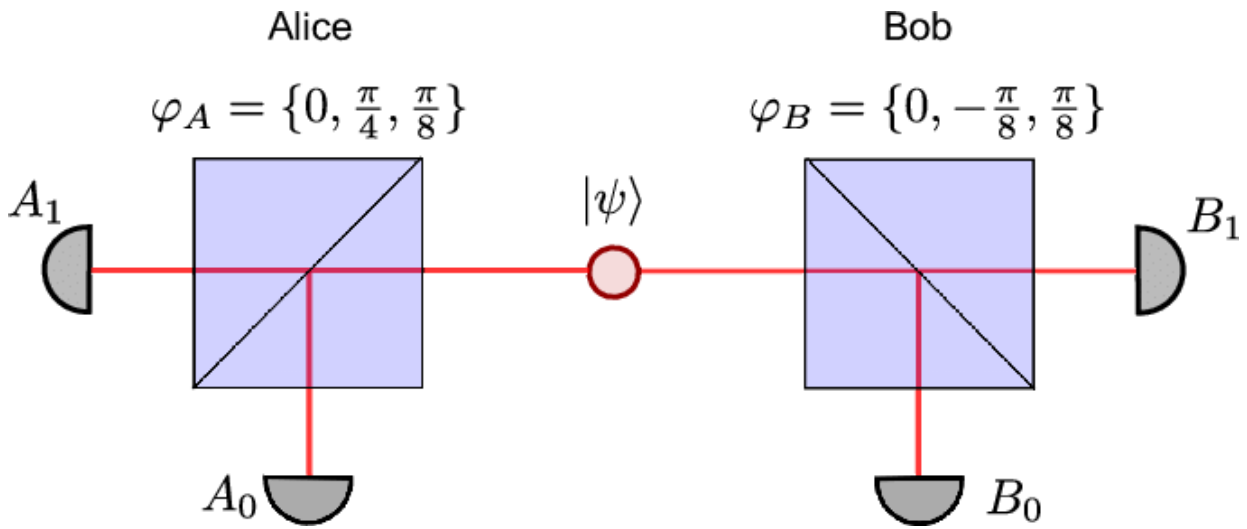




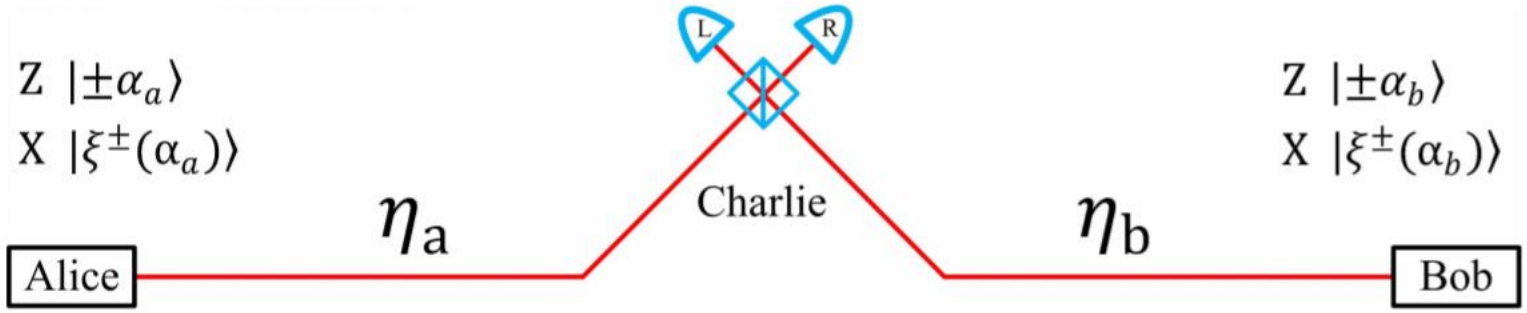
Physical access to equipment

Laser damage!

Time reverse helps to solve problem of detector blinding



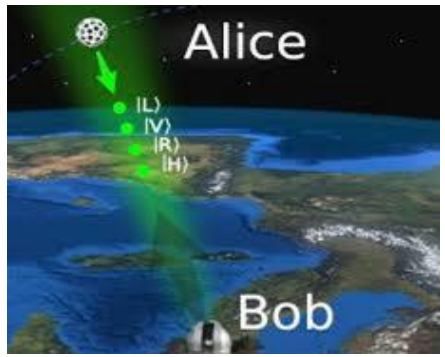
Entangled state
is distributed to make key
from non-classical correlations



Measurement is replaced
by state preparation

Preparation by measurement

Quantum key distribution provides a range of solutions for absolute information protection in various implementations



Optical fiber:

- There are commercial products in the world now
- Used in standard lines
- Practical distance is up to 100 km (in laboratories is up to 400 km.)
- Typical speed of key generation is 1-1000 kbit/s.

Satellite implementation:

- The movement of the satellite ensures the exchange of a secret key between any points on earth
- In 2016, China successfully launched the first satellite for the quantum cryptography technology

Open space:

- Potentially miniaturized solution for individual use
- Possibility of install on mobile platforms for hard-to-reach areas and highlands

QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

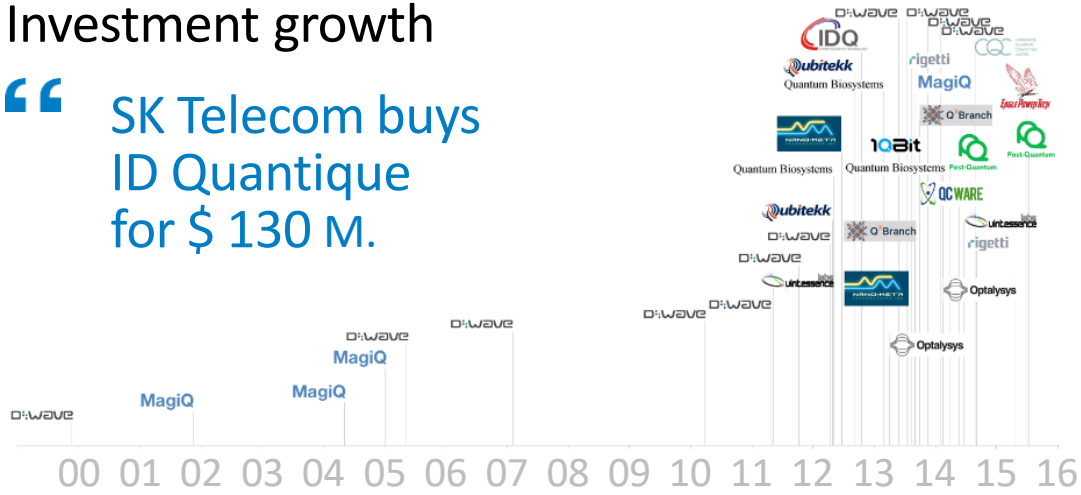
New market – new possibilities

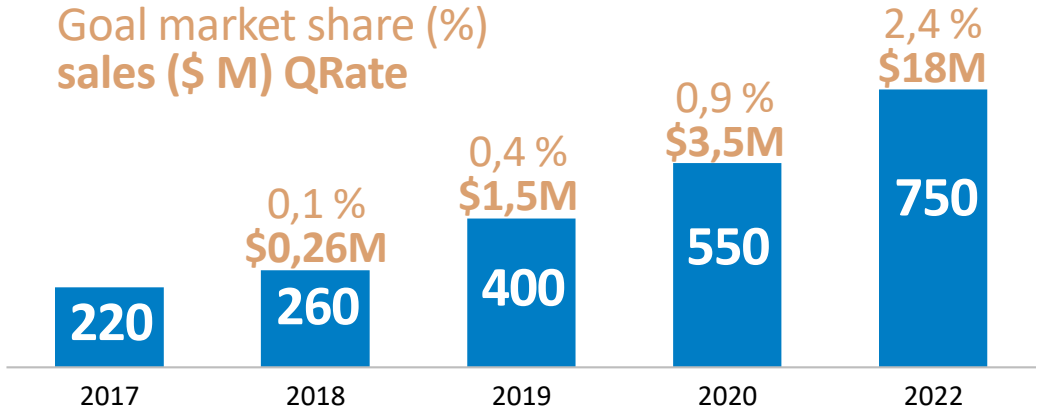
Today QKD market is the startup market

IDQ	market
QuantumCTek	market
ASKY	market
KETS	prototype
Quintessence Labs	prototype
TOSHIBA	Nor available for purchase *Best parameters*
QRATE	market
MSU/InfoTechs	market
ITMO/Kvanttelecom	market

Investment growth

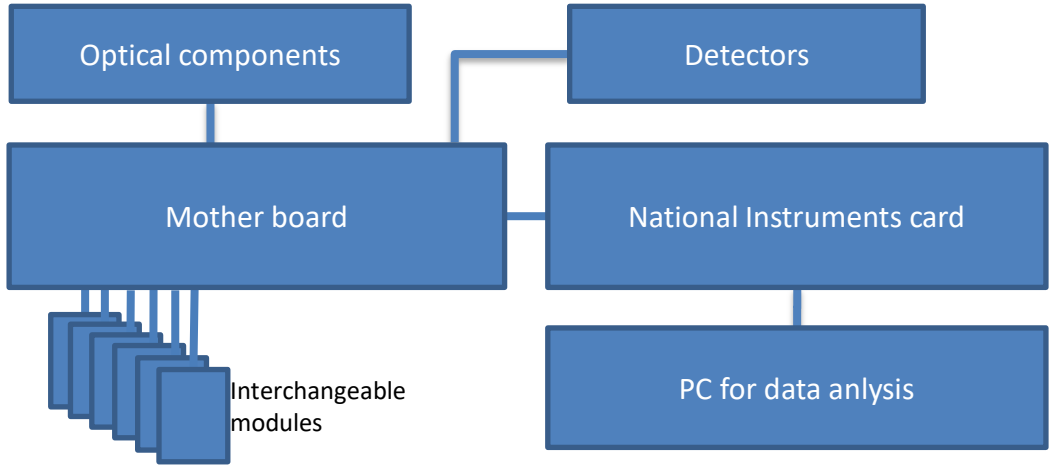
“ SK Telecom buys ID Quantique for $ 130 M.



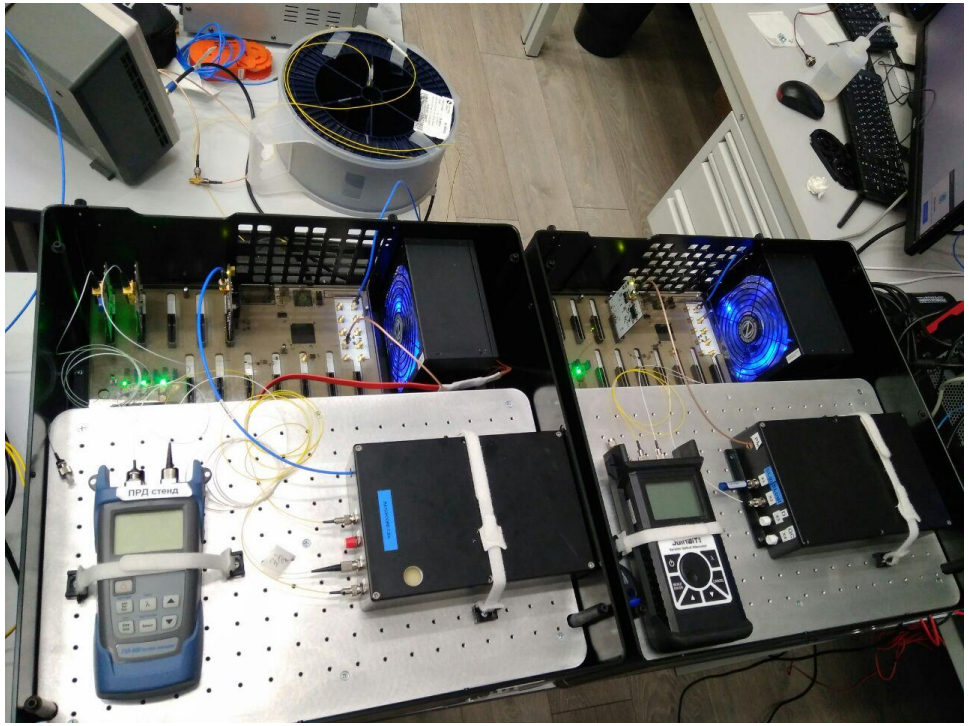


[1] **Markets&Markets**: Quantum cryptography market - 2017 to 2022

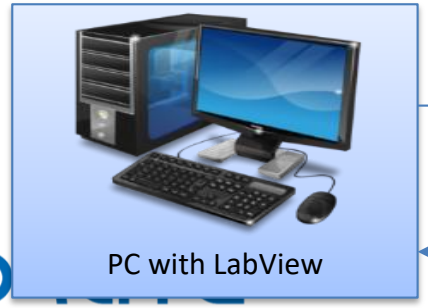
Fast prototyping with modular system is an opportunity for our group

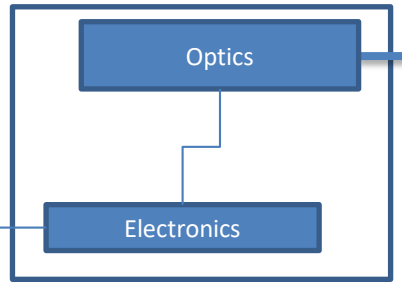


Modular system allows to change optical scheme, protocols and number of driving elements without knowledge in electronics



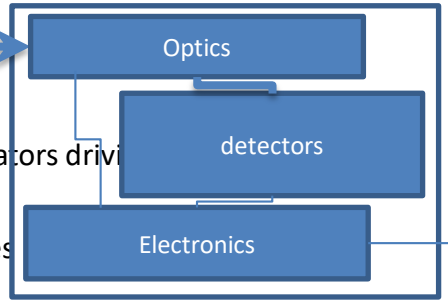
Alice





Motherboard can be equipped with:

- ✓ Up to 5 laser diodes
- ✓ Up to 5 single photon detectors
- ✓ Up to 5 fast DAC for phase/amplitude modulators drivi
- ✓ 2 ADC for fast analog signal collection
- ✓ Up to 7 slow DAC/ADC driven external devices



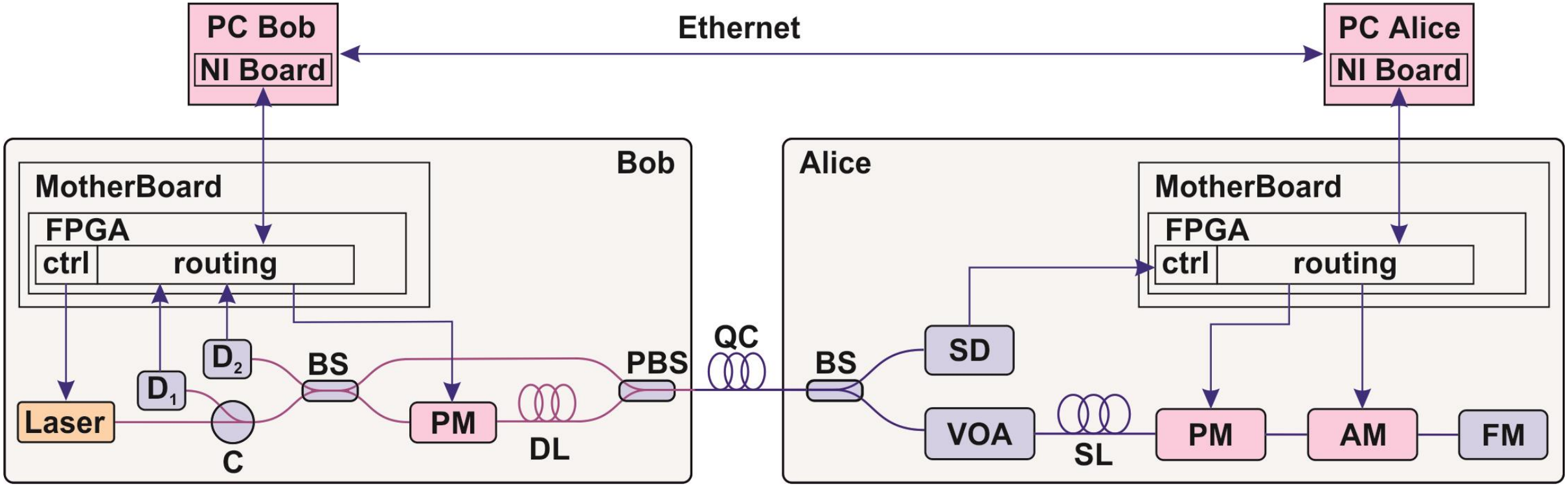
Bob

Driving software can be modified by “student” preparation level

QUANTUM COMMUNICATIONS

Российский Квантовый Центр

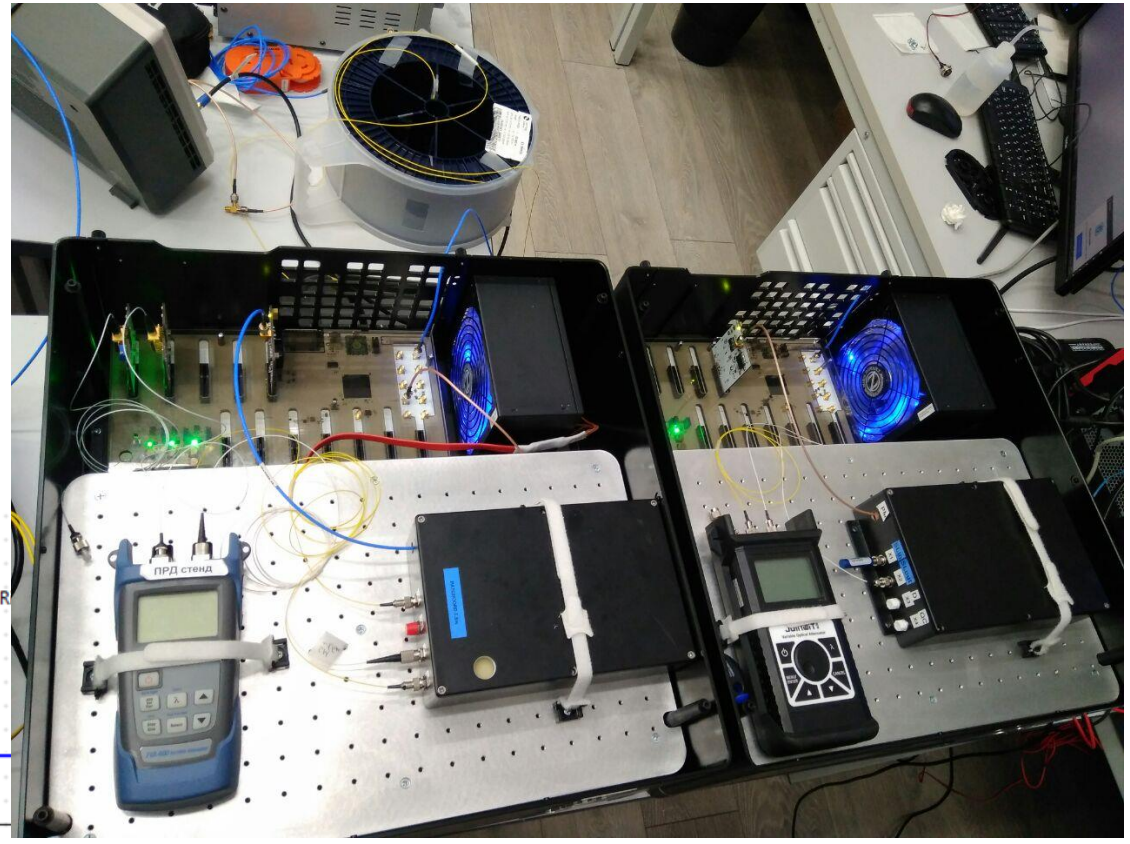
Plug&play QKD alignment is the basic task

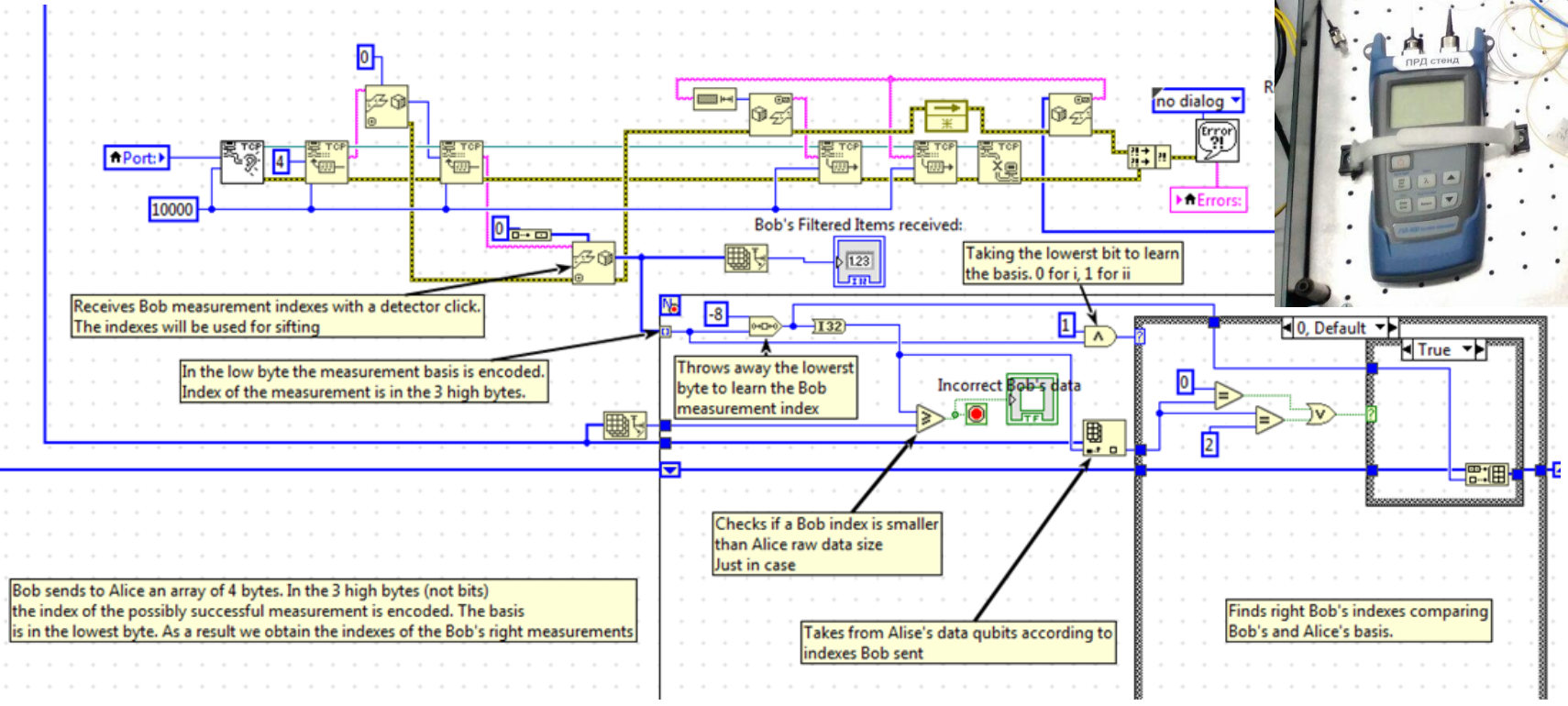


RQC’s solution for introducing quantum physics

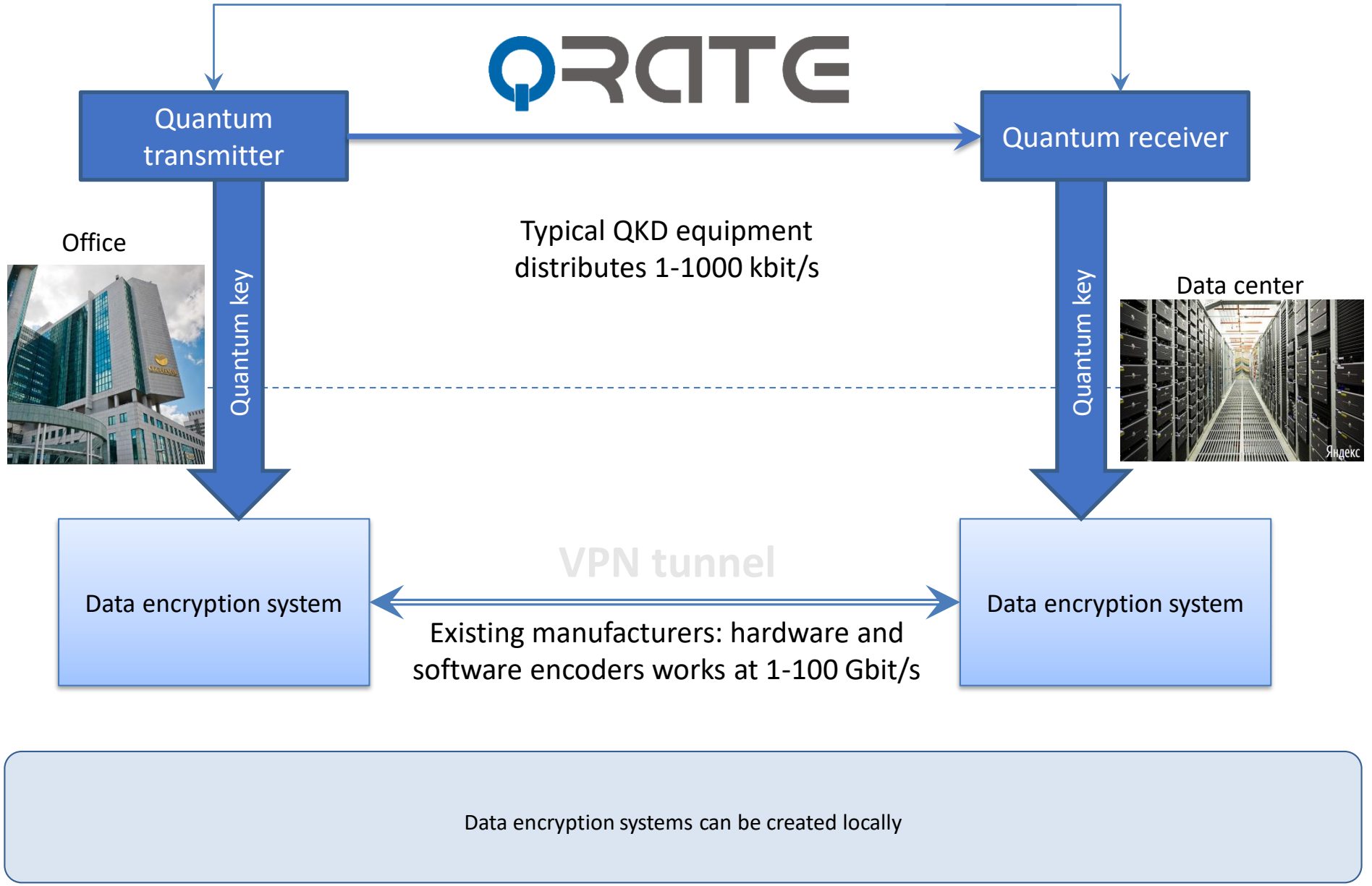
RQC’s solution is to use quantum cryptography as a tool for introducing quantum physics.

It is an effective tool because it has the desired property set to intrigue students and demonstrate many basic quantum principles.





Integration with standard encryptor used in Sberbank and Rostelecom



World leaders are China and Europe

QRATE
LAUNCHING QUANTUM SECURITY

IDQ
FROM VISION TO TECHNOLOGY

QuantumCTek

- First product announced in 2001
- Demonstrated successful exit in 2018 with SK telecom

- Largest in the World production to supply network in China
- Number of products

Secure now.
Secure in the future.

QRATE

Working with potential customers is conducted at the stage of the prototyping

QRATE
LAUNCHING QUANTUM SECURITY

CISCO

HUAWEI

Data transmission protection

Main market

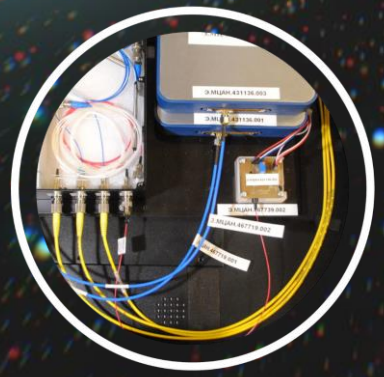
Data storage protection

Authentication

Trusted management of distributed infrastructure objects

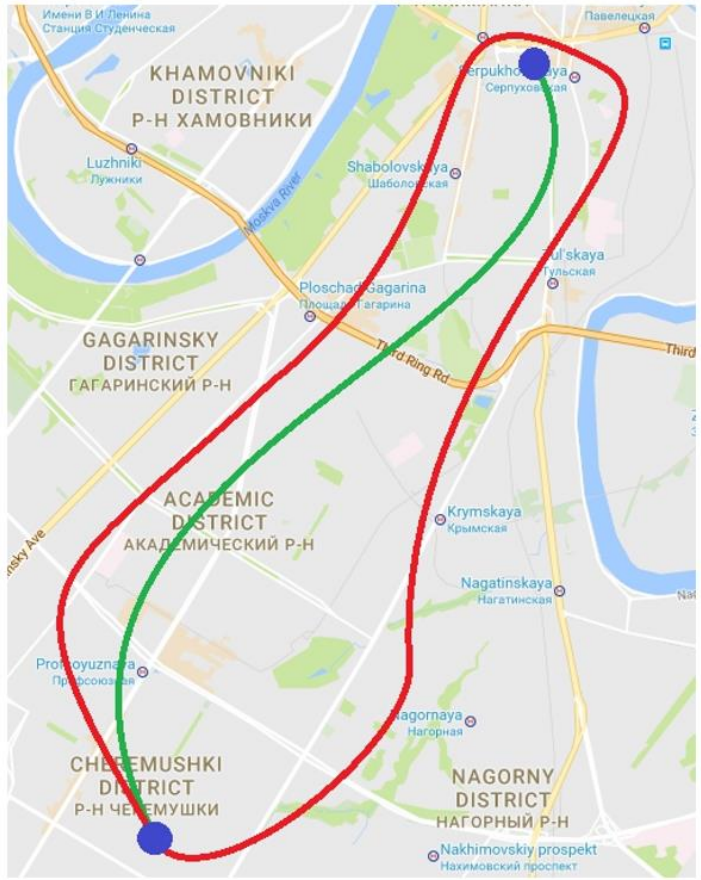
TESLA

QKD field test in 2016



GAZPROMBANK

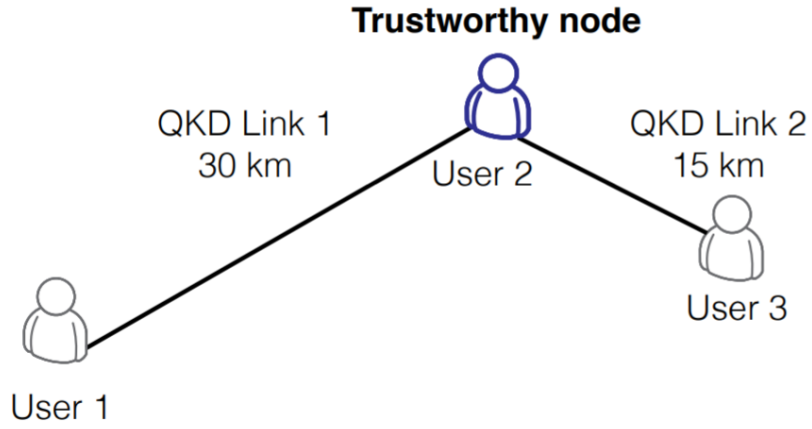
QKD networks are key to new quality provided by quantum technologies



Quantum network experiment (May 2017)

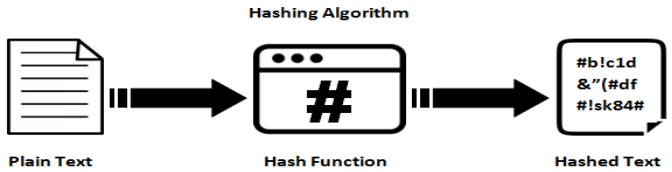
- Quantum keys transport between three users over an intermediate trusted node
- First link generates quantum keys using the polarization-encoding scheme
- Second link employs the phase-encoding scheme.

E.O. Kiktenko, et al. Demonstration of a quantum key distribution network in urban fibre-optic communication lines // Quantum Electronics 47 (9), 798-802 (2017).

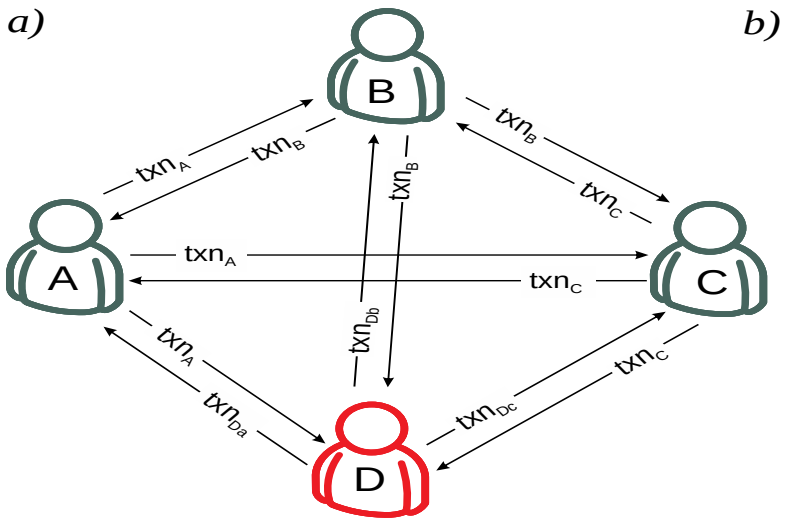


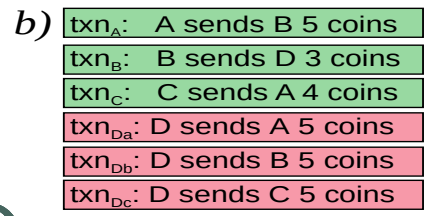
Quantum key protects blockchain

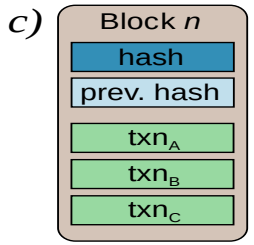
Digital signatures – Quantum-unsafe



Hash functions – Believed to be quantum-safe…?







Quantum-secure blockchain opens new opportunities for QKD

- QKD guarantees information-theoretically secure authentication between users.
- The unconfirmed transactions are aggregated into a block.
- We propose to create blocks in a decentralized fashion. To this end, we employ the "broadcast" protocol.
- This protocol allows achieving a Byzantine agreement in any network with pairwise authenticated communication.
- We believe this scheme to be robust against not only the presently known capabilities of the quantum computer, but also those that may potentially be discovered in the future to make post-quantum cryptography schemes vulnerable.

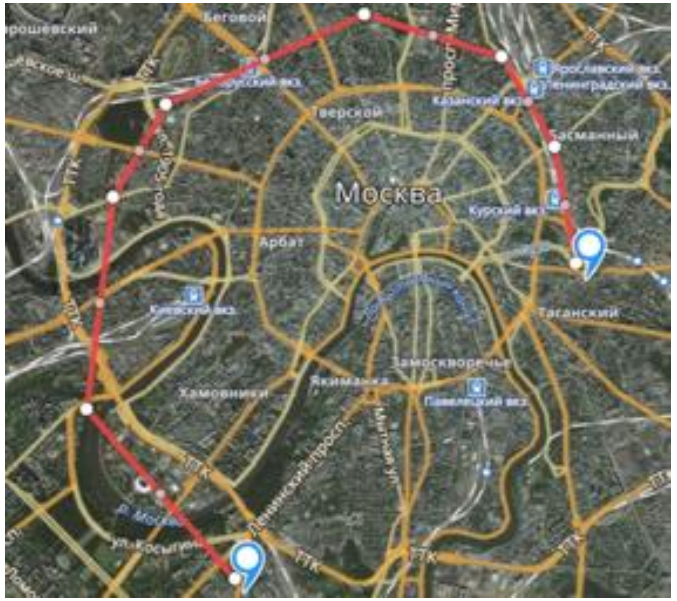
QRATE QUANTUM COMMUNICATIONS

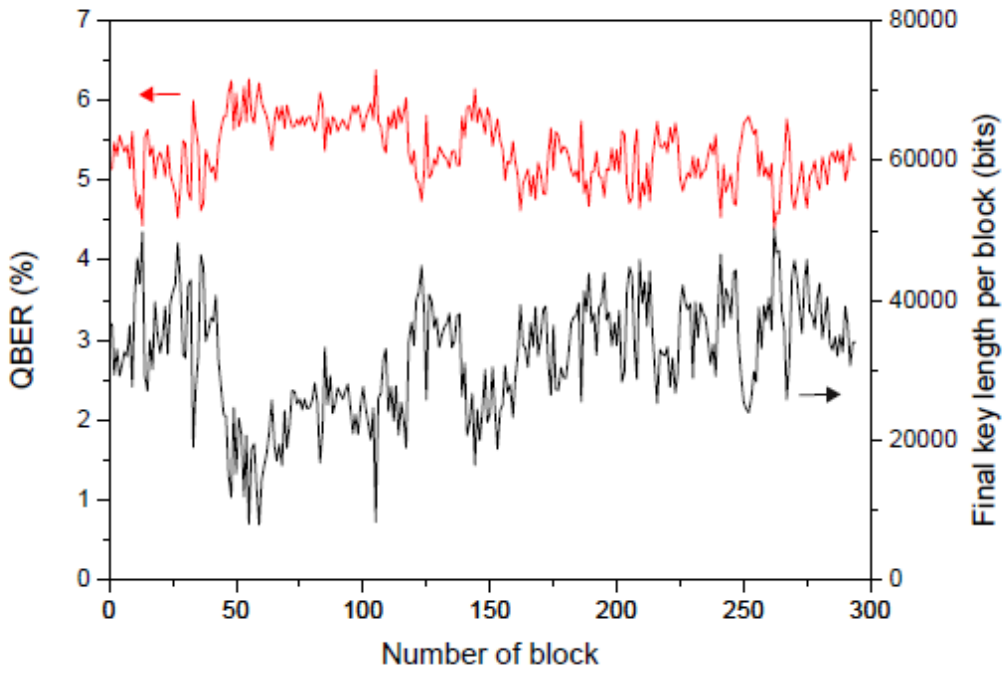
РКЦ Российский Квантовый Центр

2017-2018 Sberbank field tests

VPN

25 km, 14 dB loss.

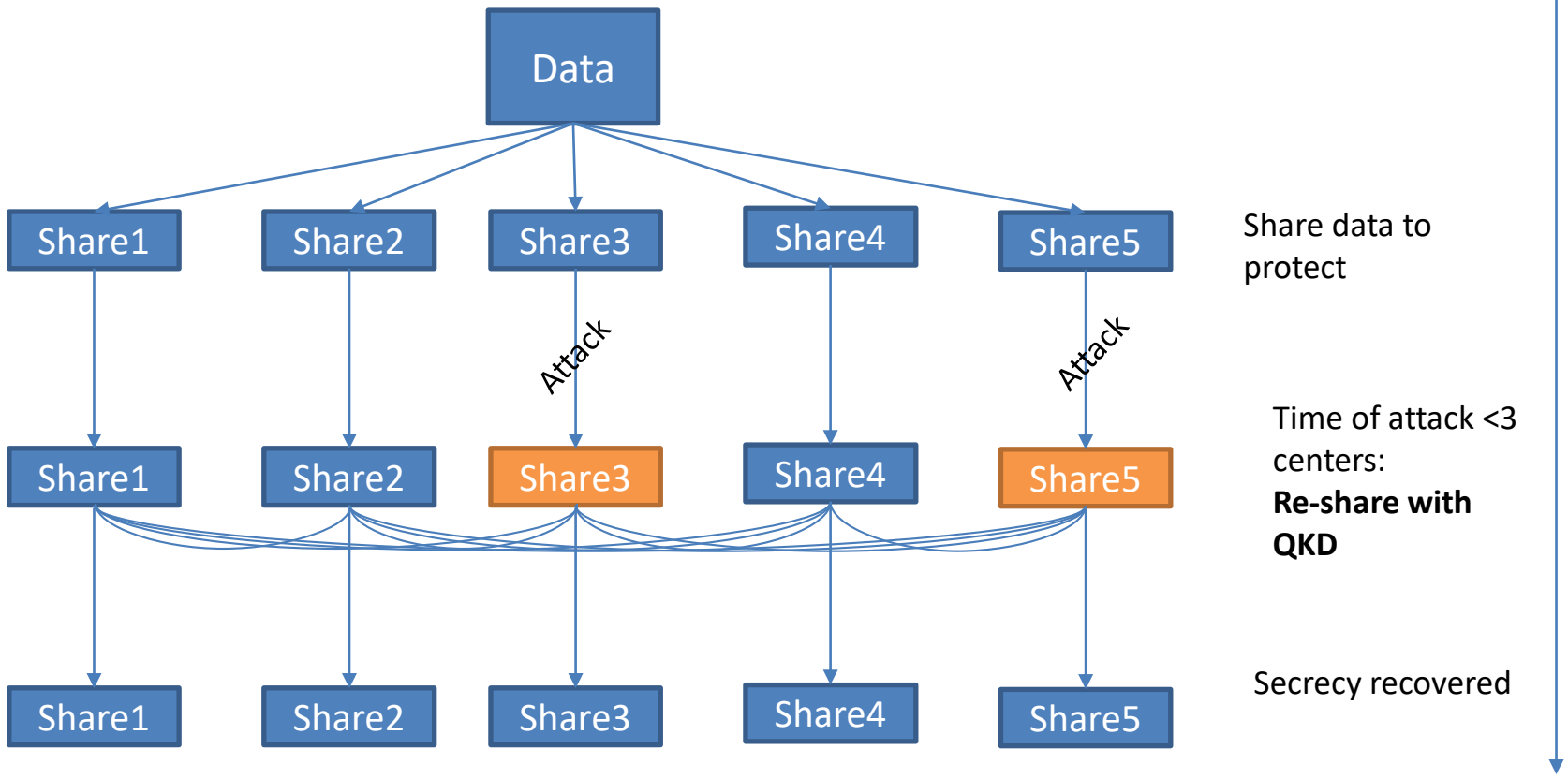




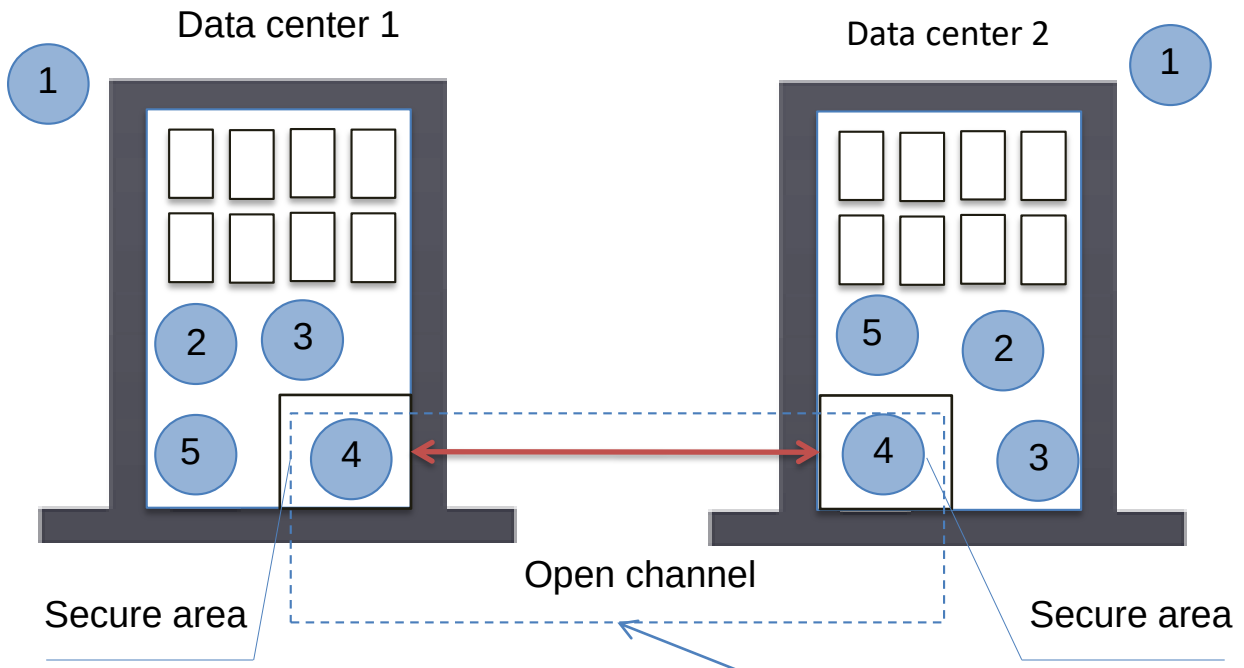
- Two Sberbank offices
- 25 km line, 8 segments, 14 dB loss
- 300 MHz pulse repetition rate
- BB84+ decoy
  - Signal 0,175 ph/pulse
  - Decoy 0,067 ph/pulse
- QBER 5,5 %
- 2 kbit/s raw key
- 0,1-0,9 kbit/s secret key
- Key consumption 256 bit per 400s.

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 provides channel protection



- Technical Information security.
  1. Physical protection.
  2. Access protection.
  3. Protection against technical information lekage.
  4. **Data transmission protection.**
  5. Software protection.
- Organization security.

Quantum cryptography appplication

QKD already has number of business applications

Commercial networks	**2019**	> 150 km for 5G and LTE – SK Telecom
	2018	**2000 km , 32 nodes + 4 city networks** 12 banks, energy companies, government, Alibaba
Pilots	**2018**	> 120 km 13 nodes – British Telecom
	2018	3 nodes telecom – Telefonica
	2018	Smart Grid, energy, banks
Research networks	**2010**	70 km 6 nodes
	2009	184 km 6 nodes
	2004	30 km 3 nodes

National Quantum Communication Backbone in China

- Inter-city quantum communication backbone with 32 trusted relays (~2000km)
- Inter-connection of four intra-city metropolitan networks
- For financial applications, public affairs, etc.
- Test-bed for quantum foundations (e.g. frequency dissemination)


单模复用技术

One of 32 trusted nodes

Участники сети

Tokyo network built by different groups

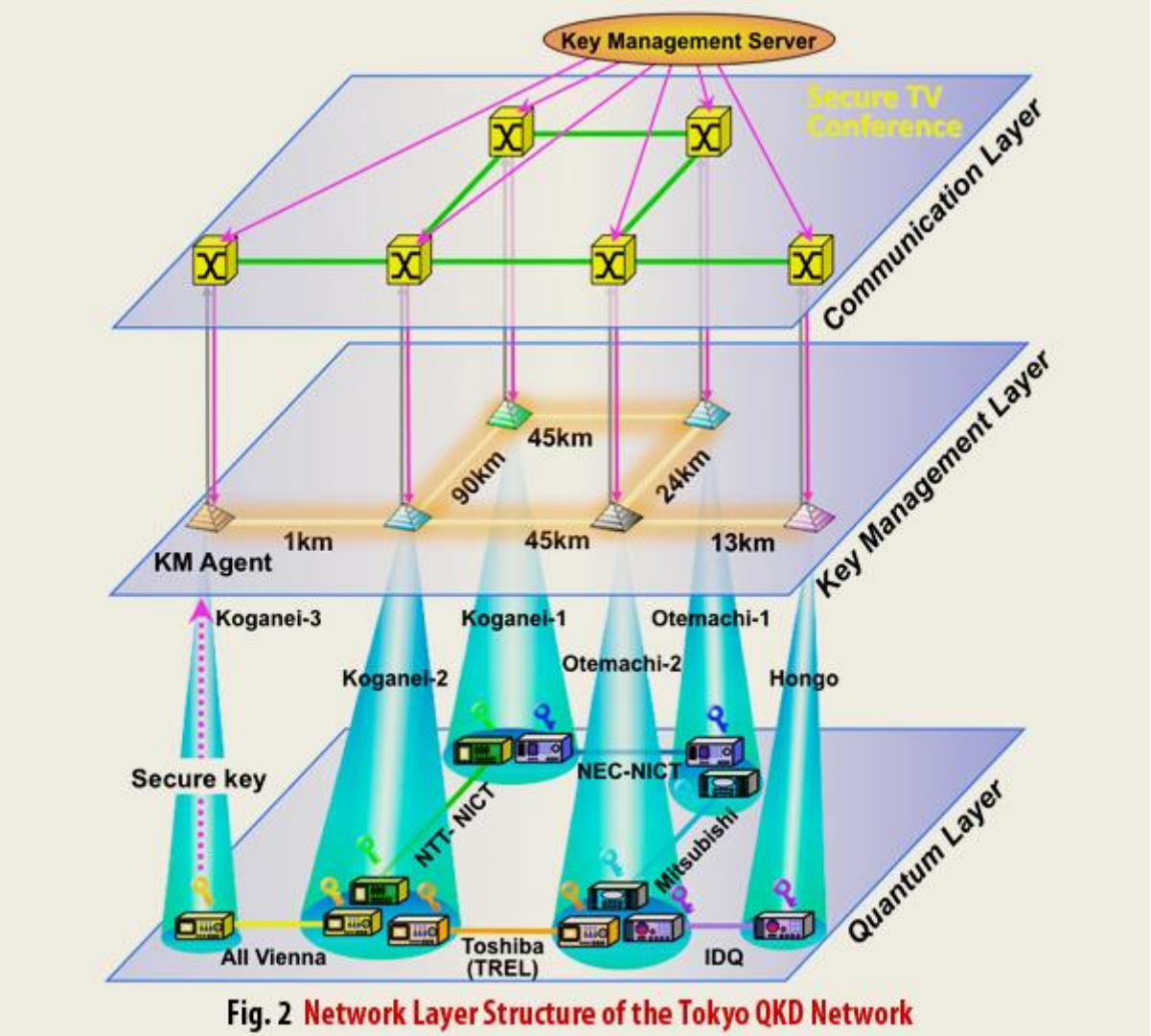


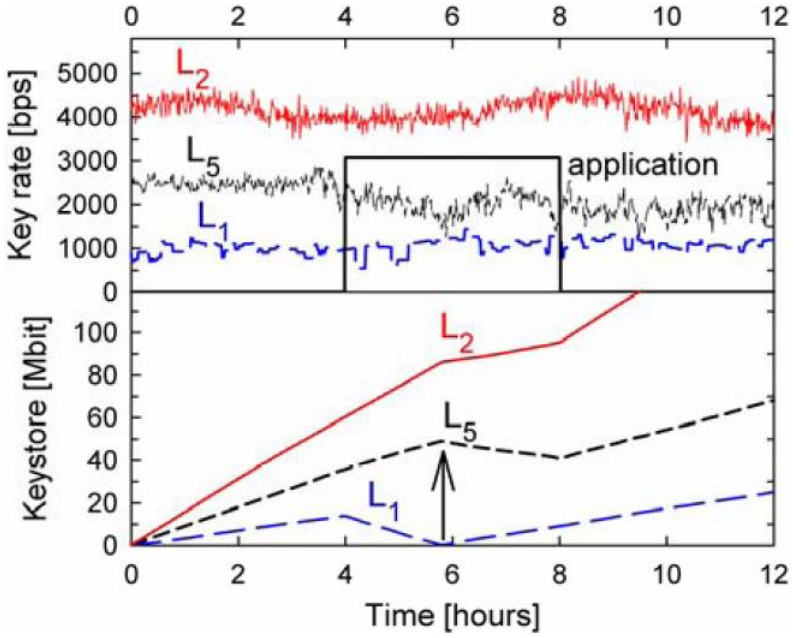
Fig. 2 Network Layer Structure of the Tokyo QKD Network

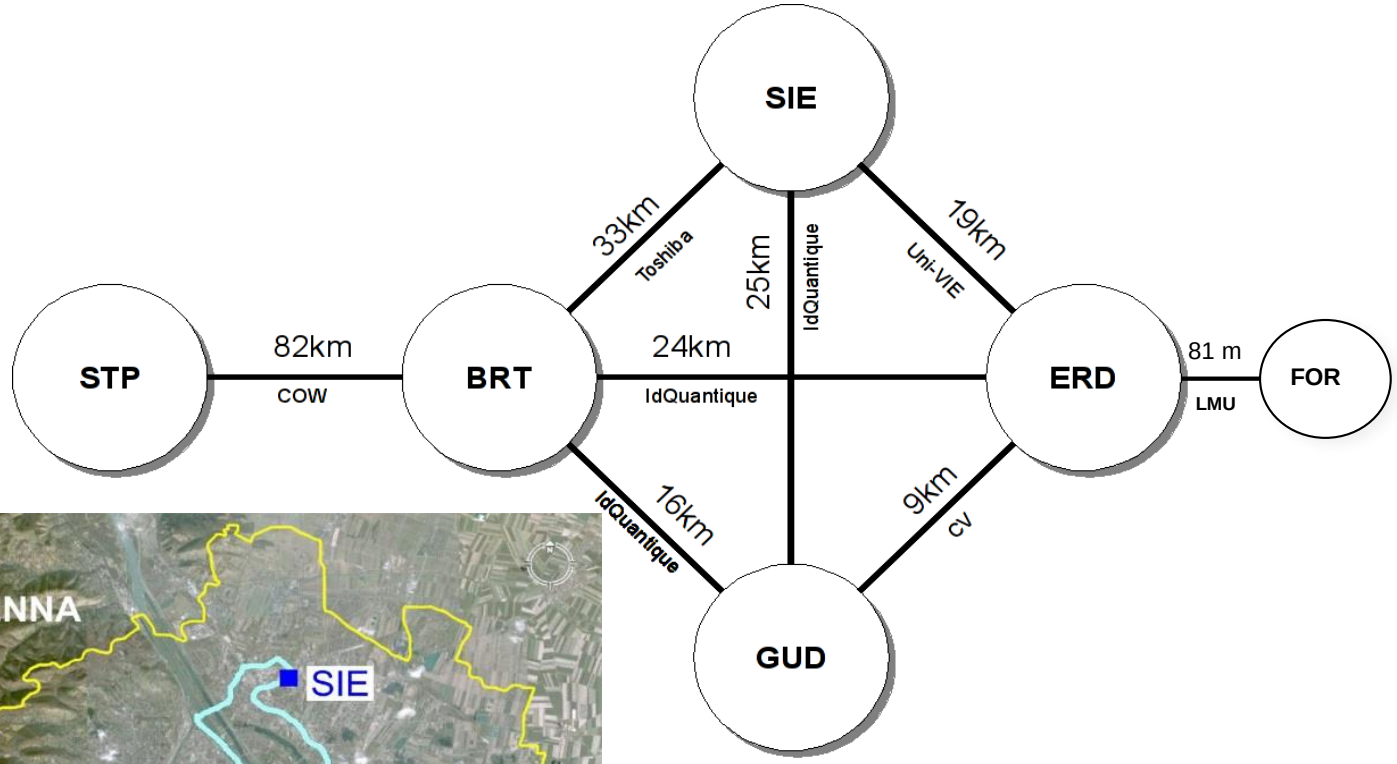
Communication layer

Key management layer

Quantum Layer

European network SECOQC was built in 2008





По материалам презентации участника проекта:
M. Peev, 2008

IDQuantique trusted node

Классические шифраторы:

L2, 2 Gbit/s

L2, 10 Gbit/s

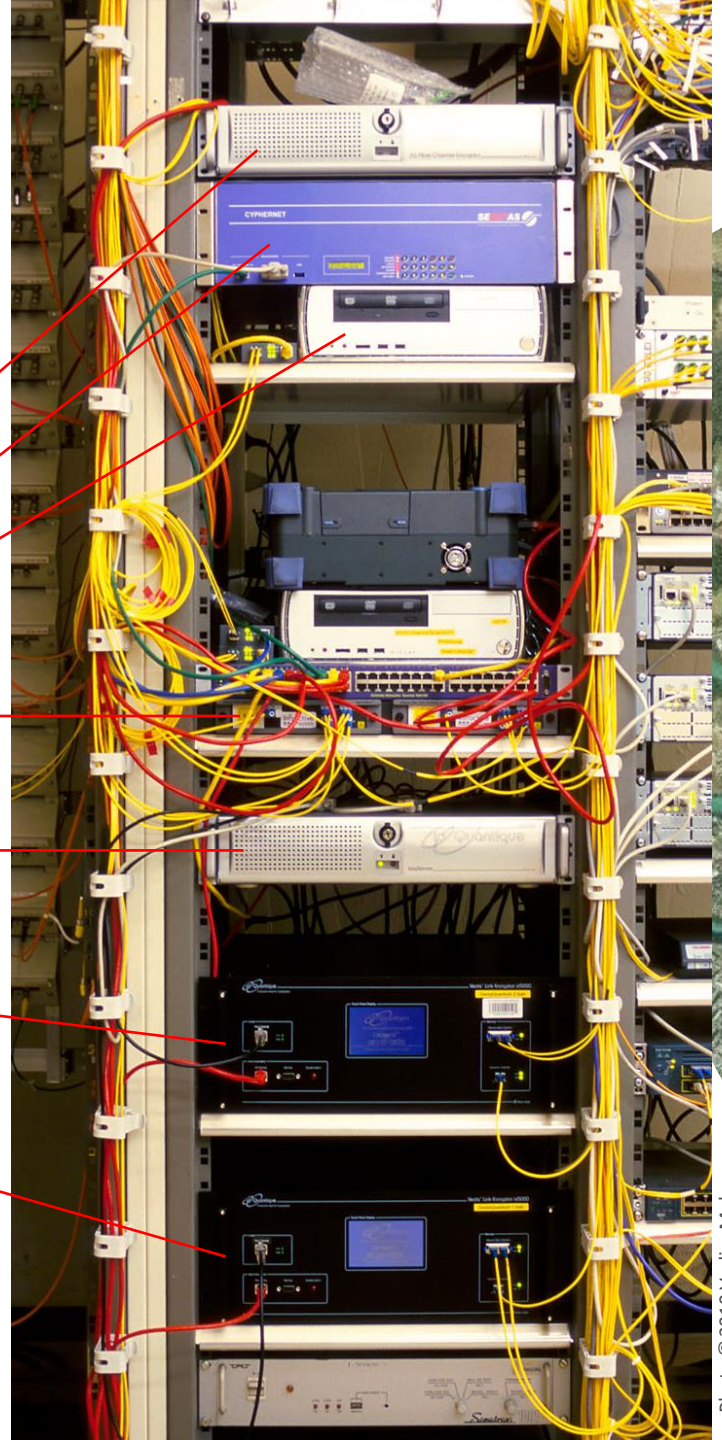
L3 VPN, 100 Mbit/s

WDMs

Управление ключом

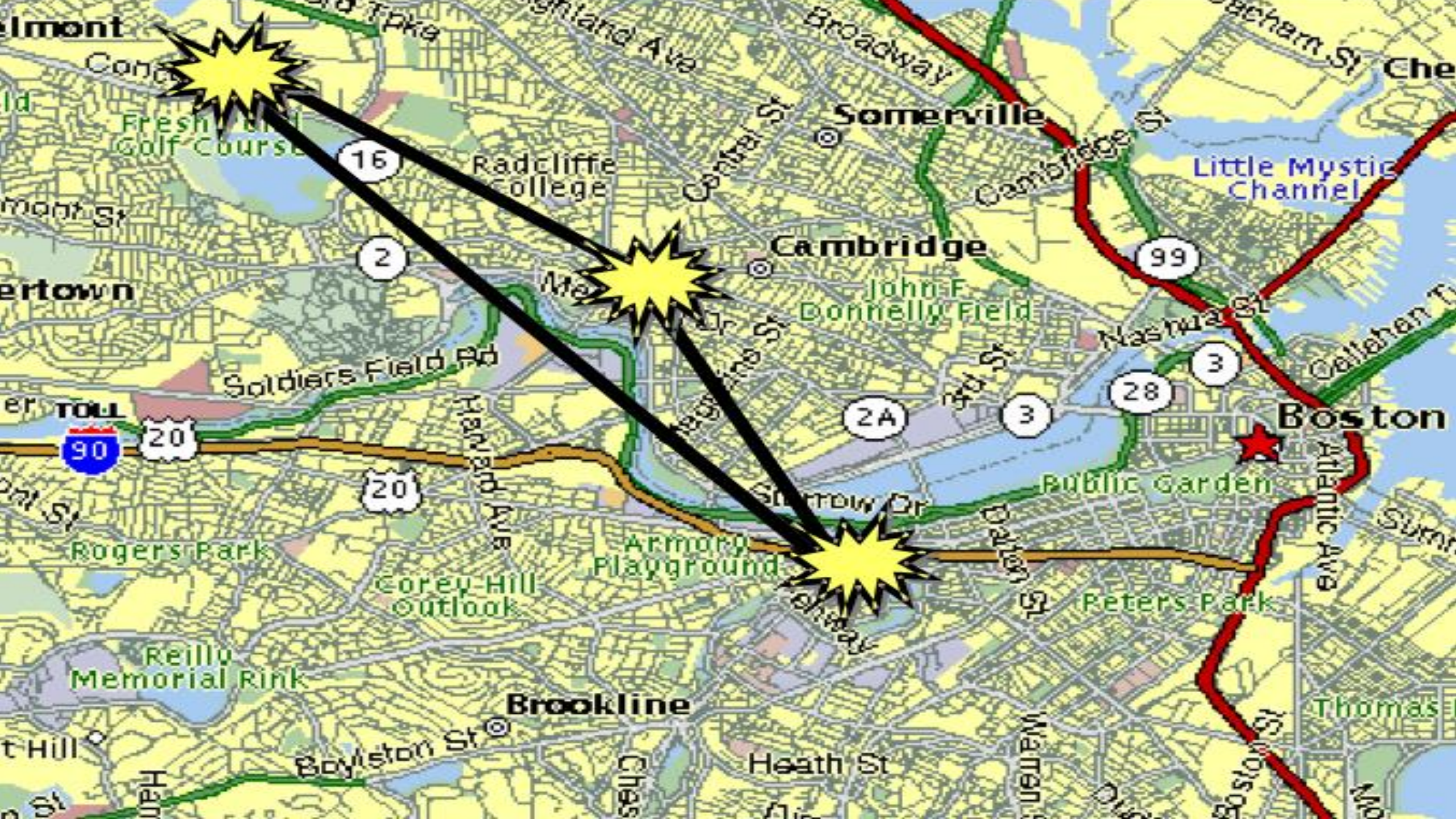
Квантовое распределение ключа на линии 4 km

Квантовое распределение ключа на линии 14 km

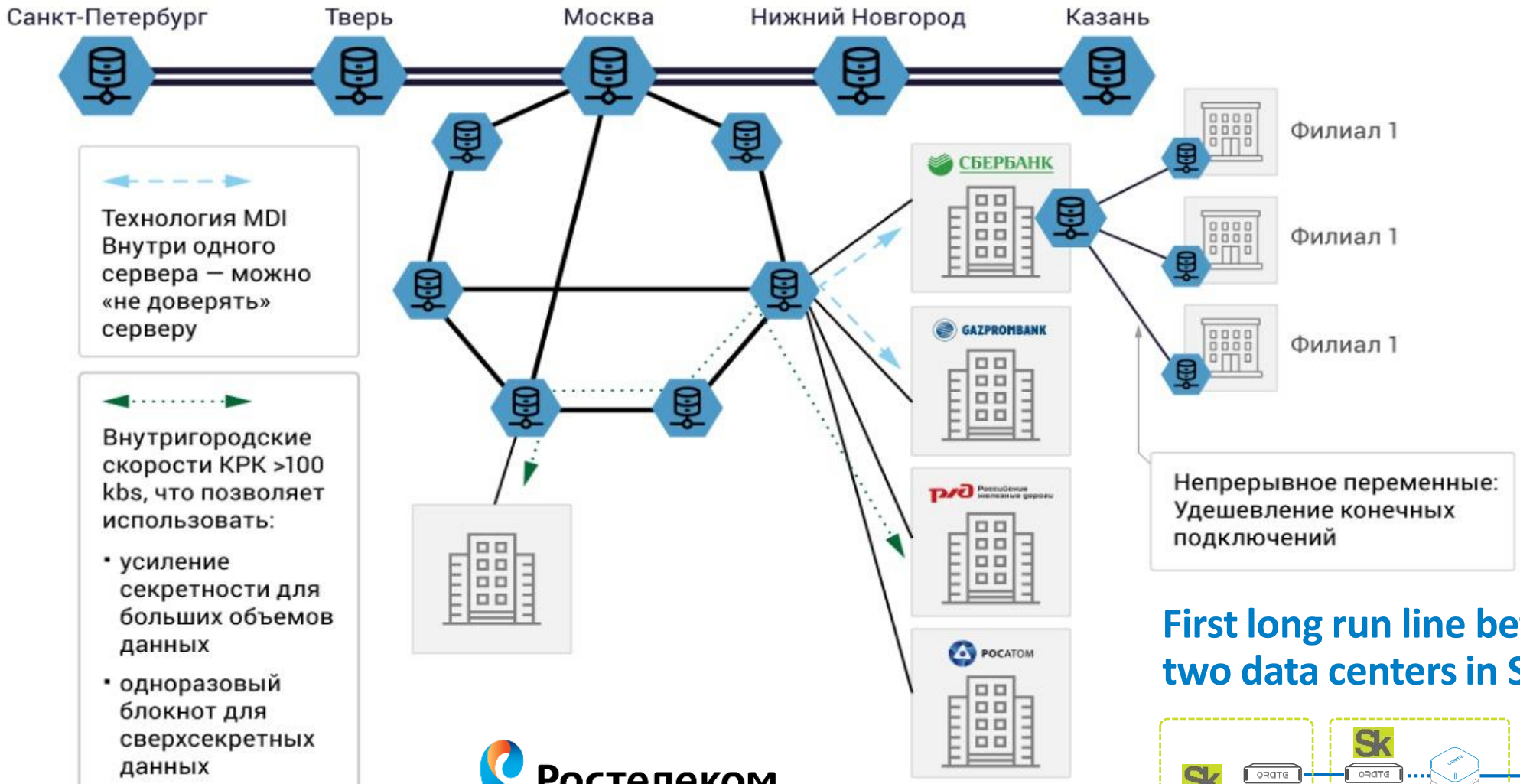


www.swissquantum.com

ID Quantique *Cerberis* system (2010)


Somerville
Cambridge
Boston
Brookline
Radcliffe College
John F. Donnelly Field
Soldiers Field Rd
Rogers Park
Corey Hill Outlook
Armory Playground
Public Garden
Peters Park
Reilly Memorial Rink
Little Mystic Channel
Broadway
Cambridge St
Boylston St
Heath St
TOLL
90
20
2
16
2A
3
28
99

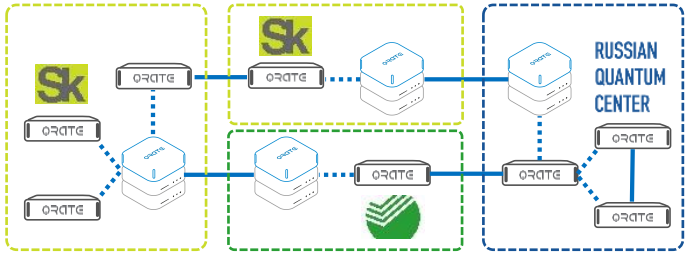
Russian quantum networks in 2024 will reach 10 000 km



Ростелеком

End of 2018 pilot project on 60 km line with 3 vendors

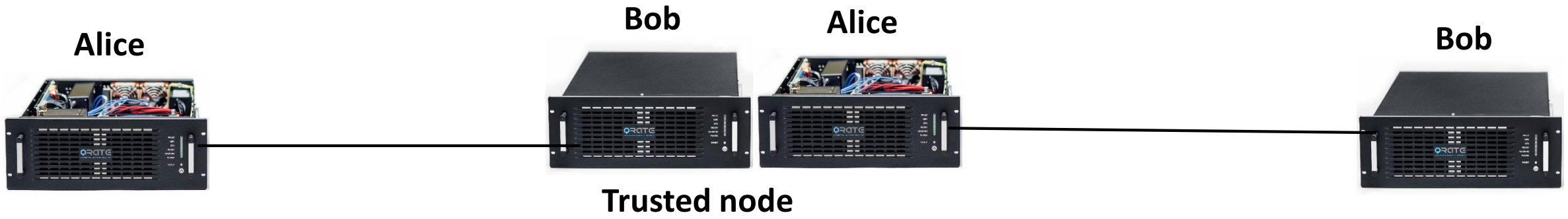
First long run line between two data centers in Sberbank

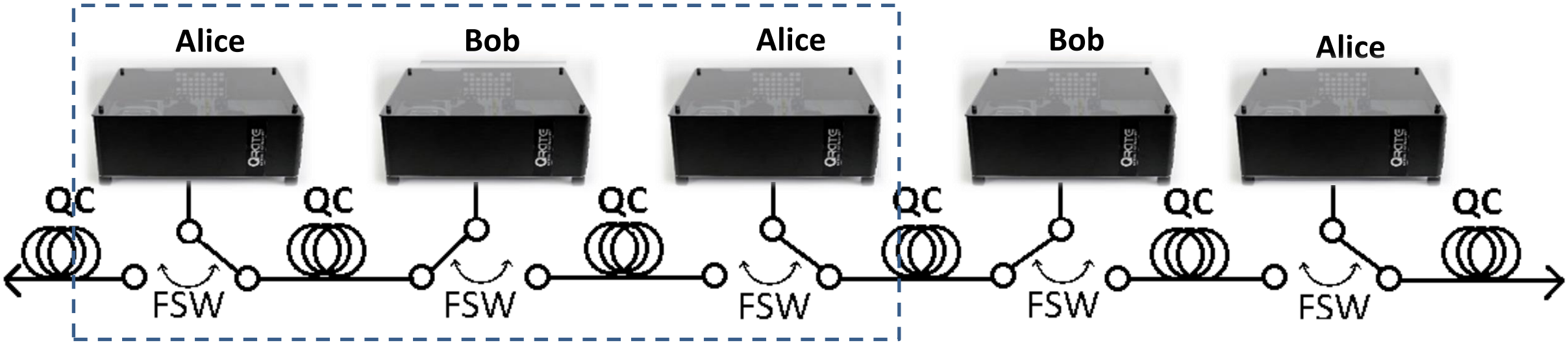


QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

Switch based network reduces number of equipment

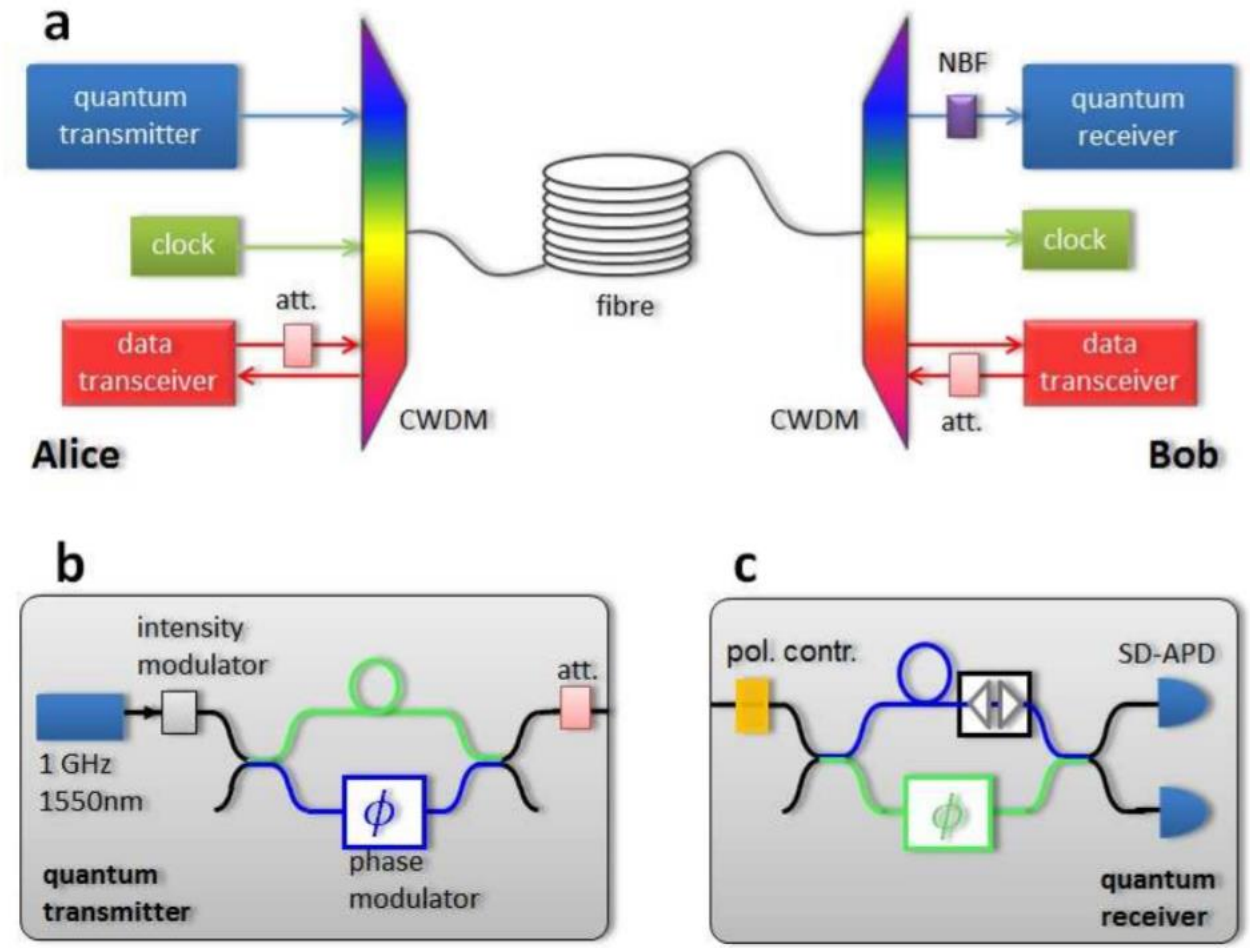


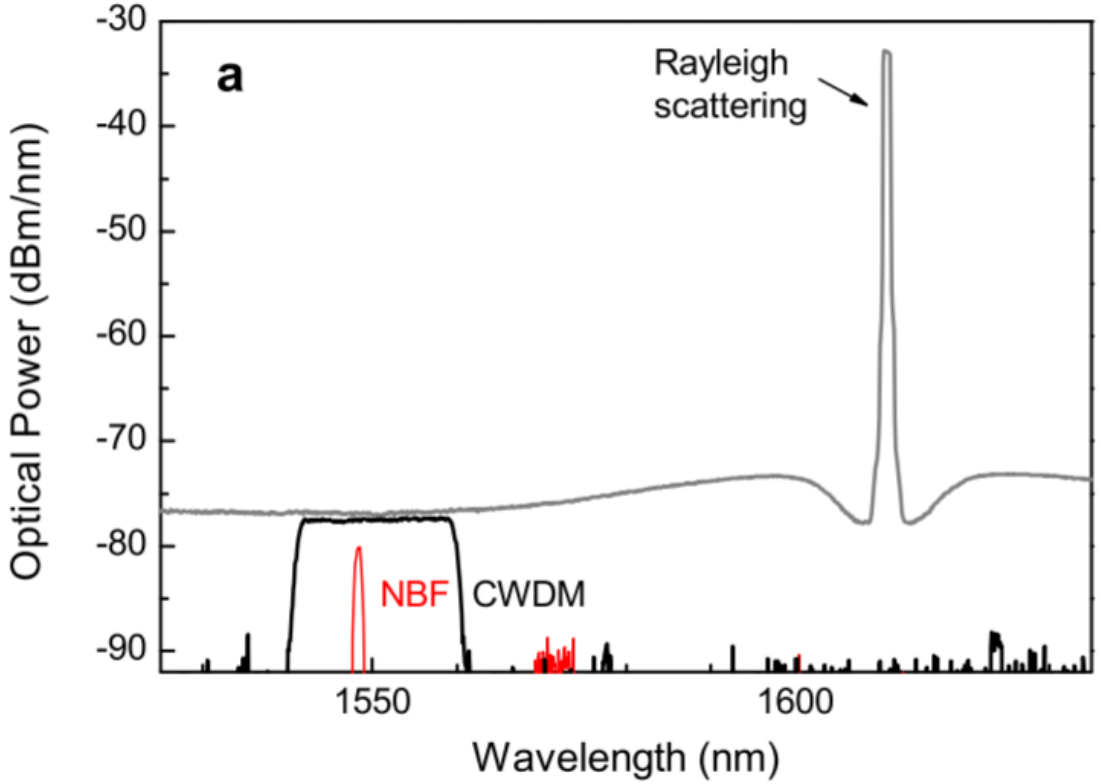


QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

Multiplexing of quantum and classical signals: Toshiba research example





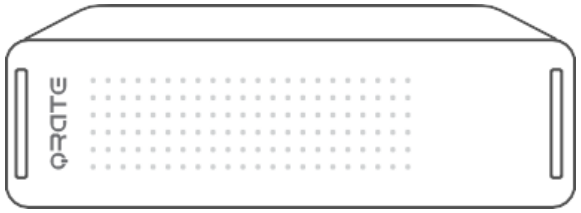
QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

How to miniaturize QKD

Existing QKD

Rack19” solution



One to one connection

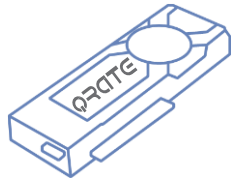
High price of one channel

Competitors:

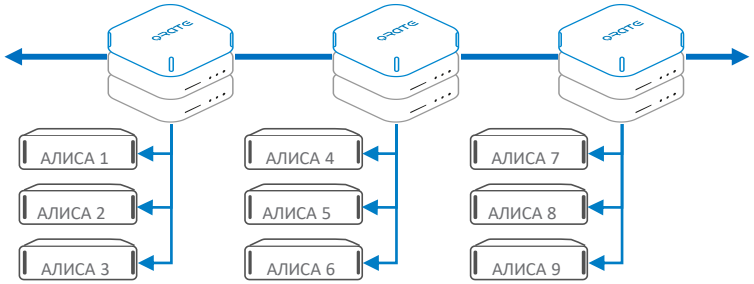
- ID Quantique
- Qubitekk
- QuantumCTek

New version with small alice and switch

Video card Alice



One to many connection (up to 1:128)

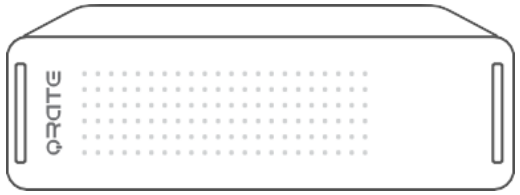


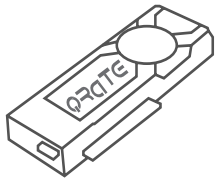
Channel cost drops more than 10times

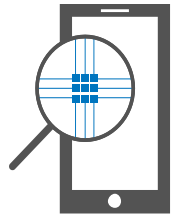
No competitors up to year 2019

We're on the road to quantum internet

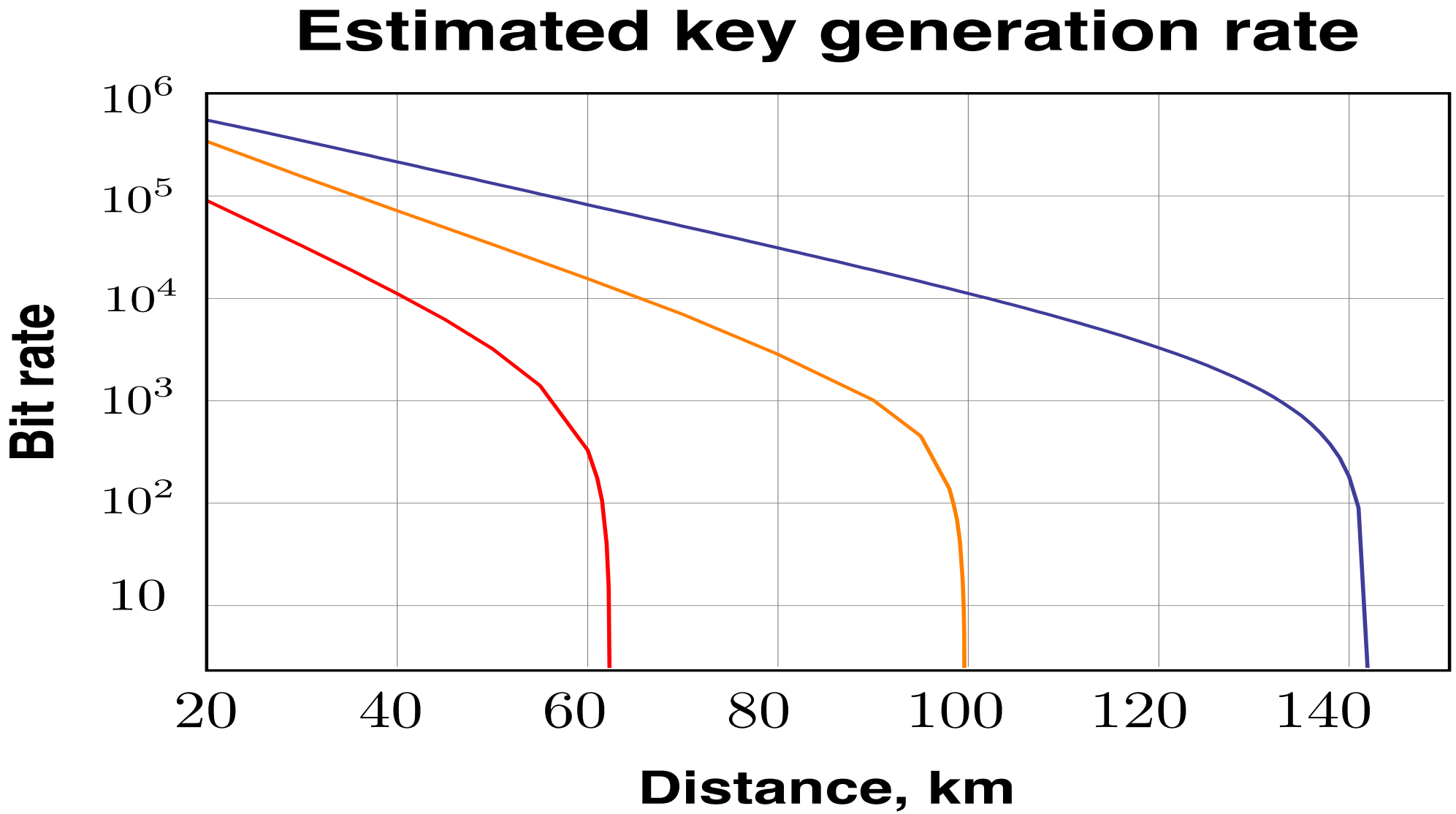
Now	5 Years	10-15 Years
Quantum Security	Quantum-secure IoT	Quantum Internet



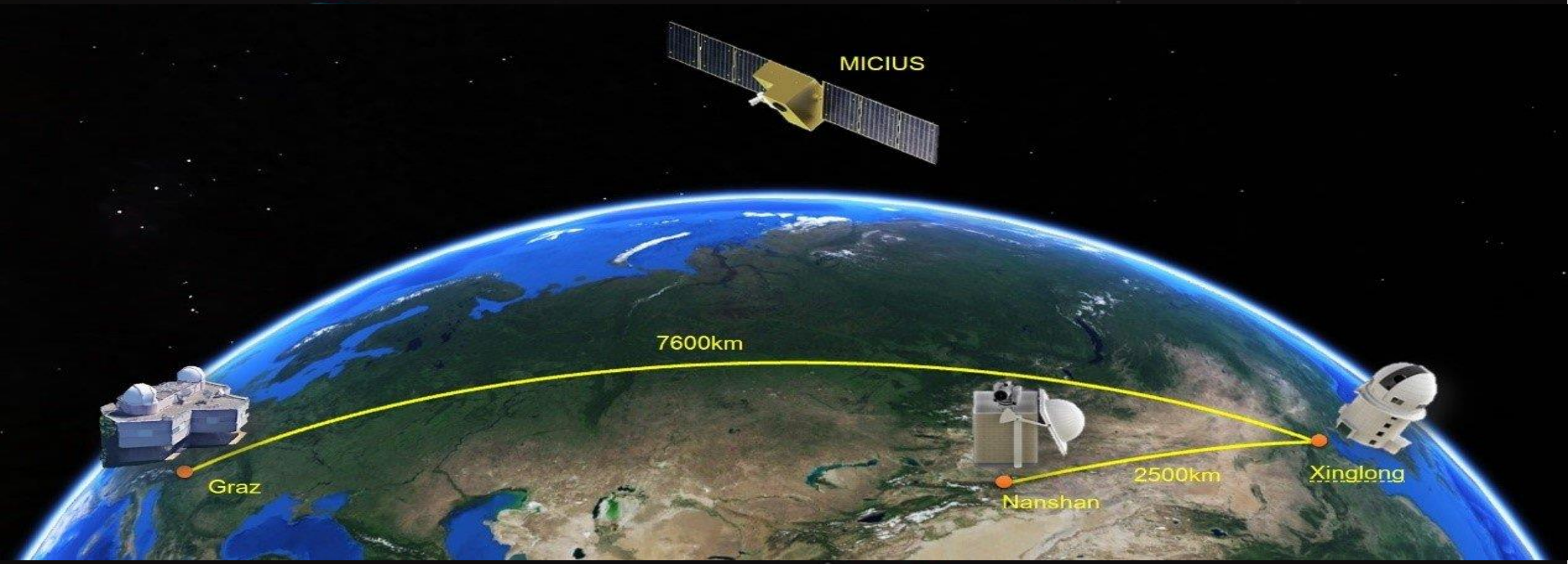




QKD distance limit is driven by exponential loss

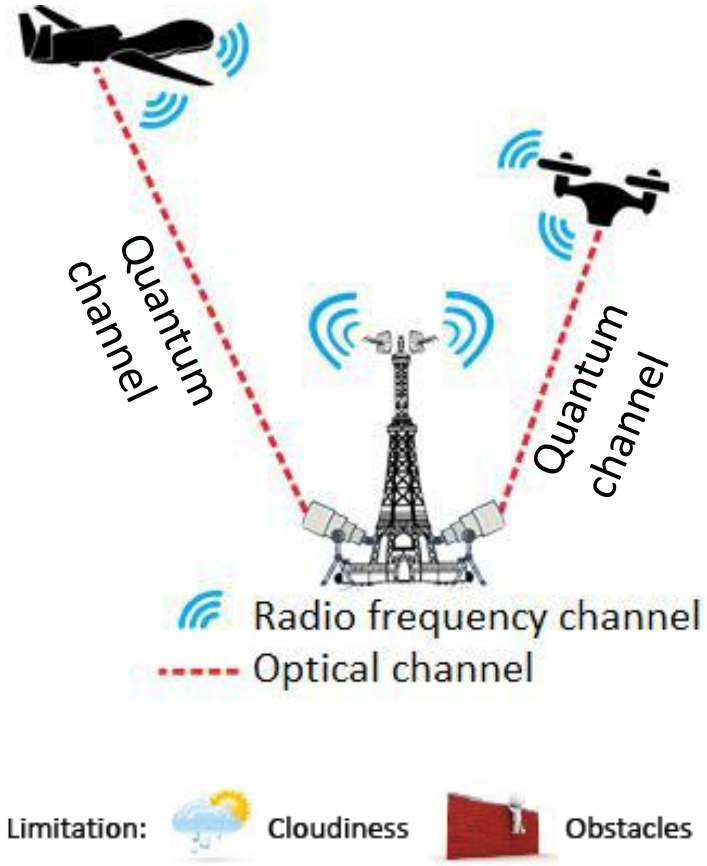


China is the only country with quantum satellite but may other are in the competition

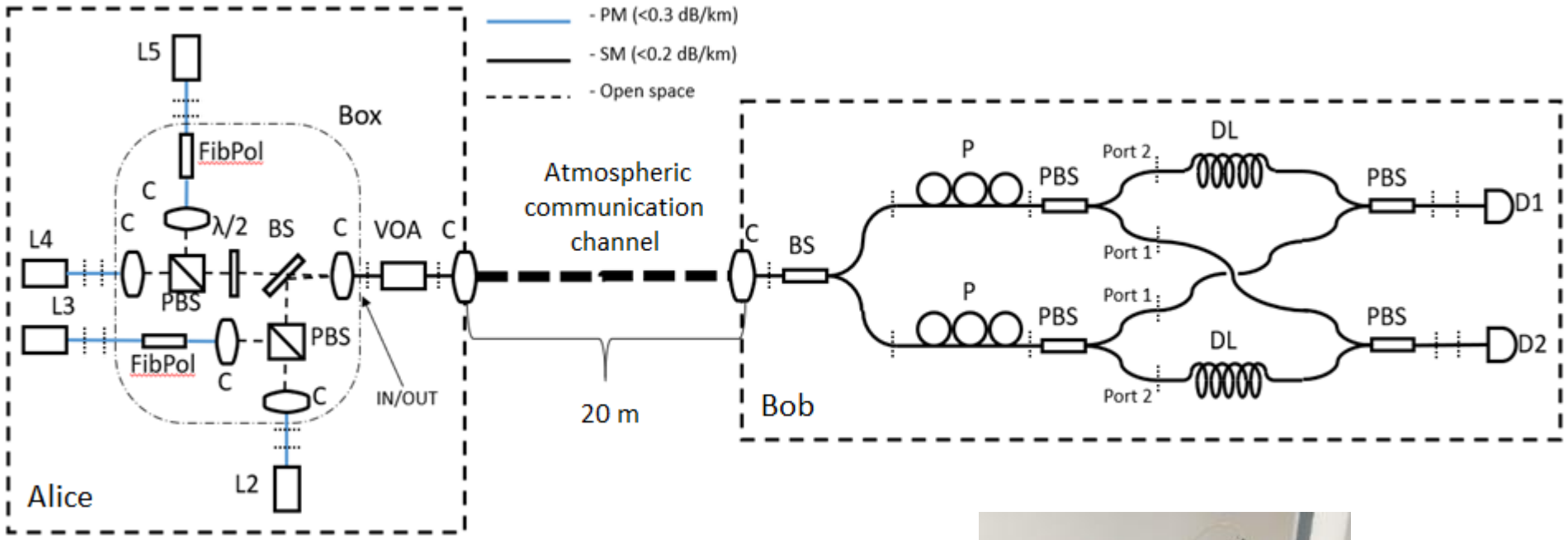


– Unmanned or manned aircraft can distribute secret key bits through free-space optical quantum channel

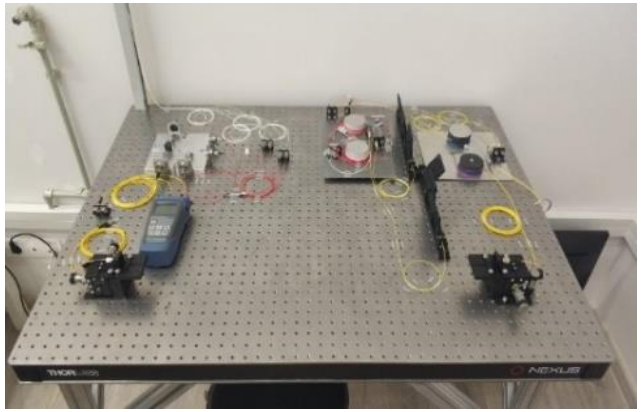
– Information, encrypted by secret key, then can be transmitted through classical RF-channel or free-space optics communication



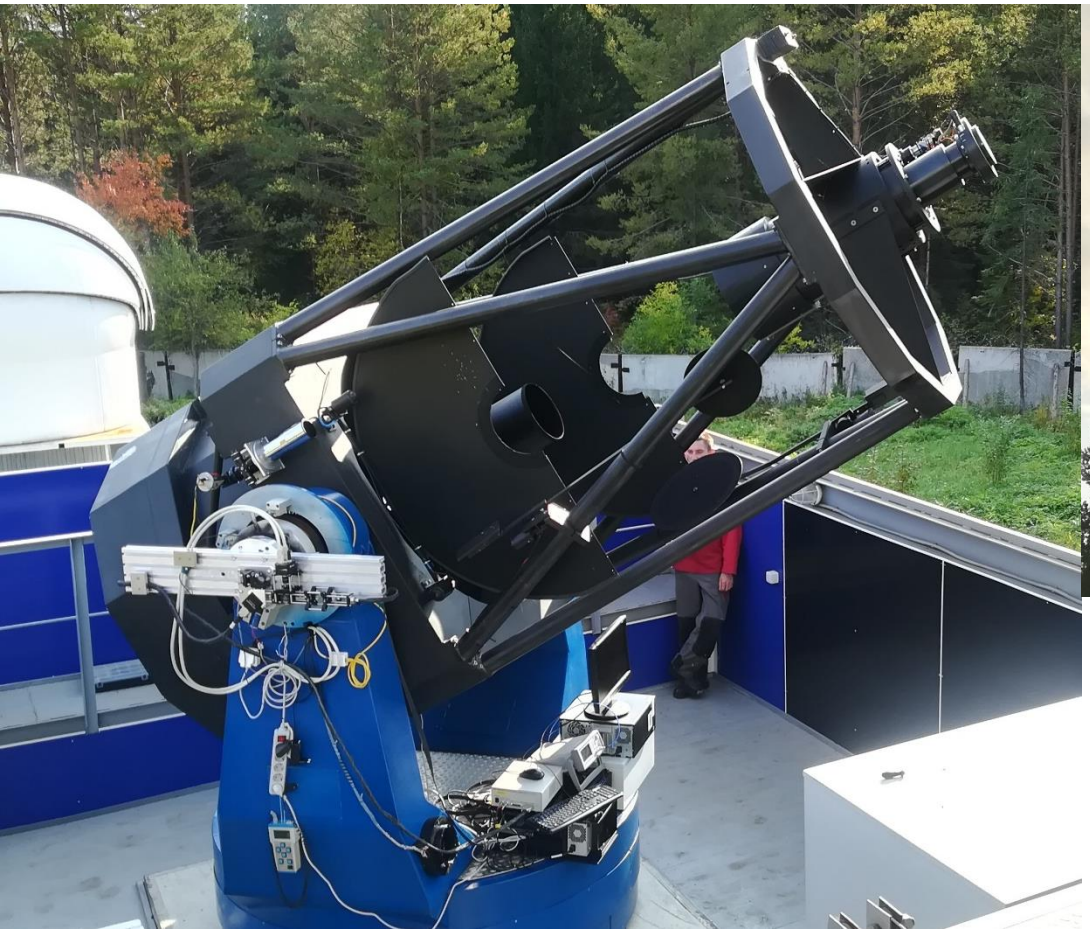
Free space QKD initiative: prototyping for drones application

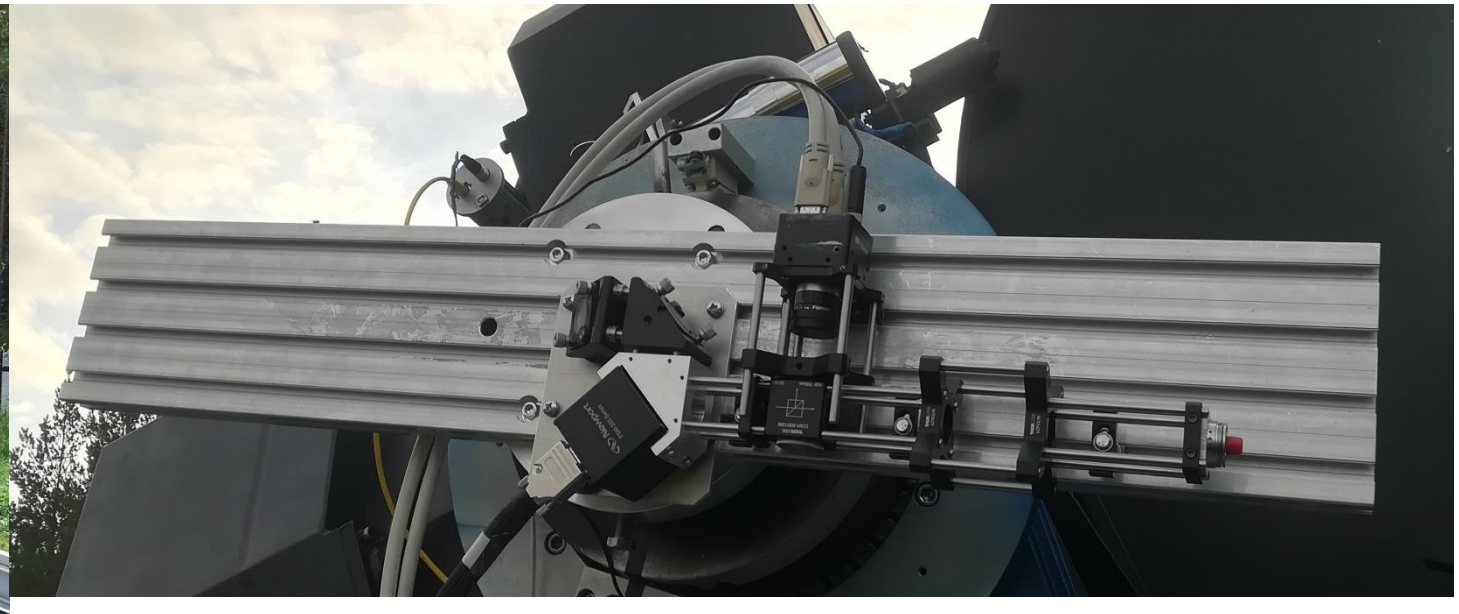


Information coding method, optical power level	Sifted key generation rate, kbit/s	Sifted quantum key error level, %
Phase coding, μ = 0.20	0.26	6.0
Polarization coding, μ = 0.20	170	1.4
Polarization coding, μ = 0.020	77	1.5
Polarization coding, μ = 0.0020	14	4.7

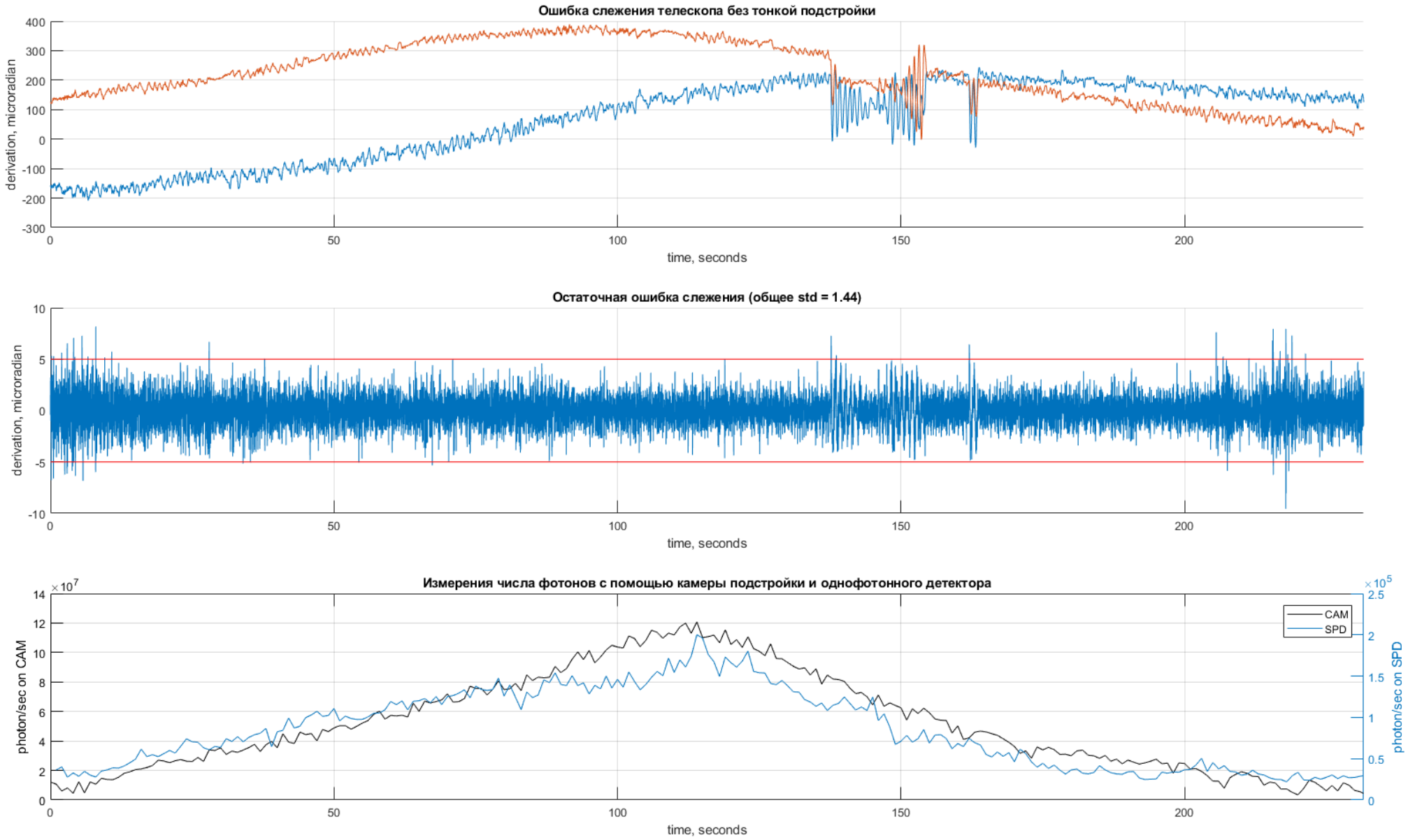


Satellite tracking



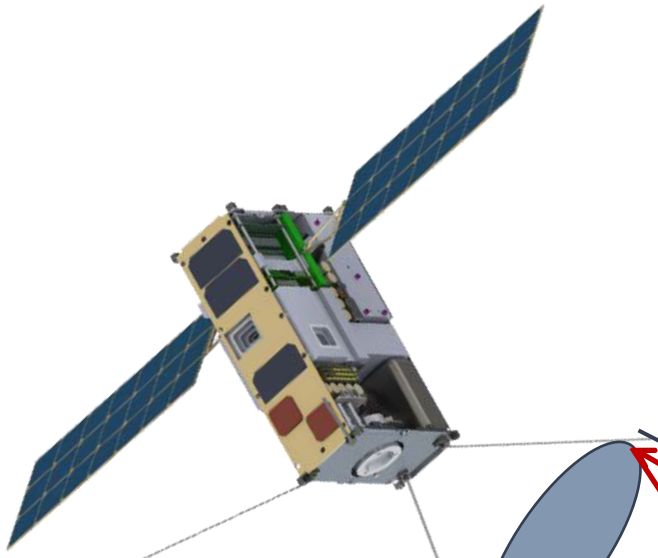


Active mirror stabilization



QSpace project

Diameter of light beam (information link) on the Earth - more than 10 m
Diameter of light beam (sync. channel) on ground - more than 40 m
Pointing accuracy - up to 40 m
Receiver telescope aperture - more than 0,6 m
4-6 communication sessions per day, 5-10 min each



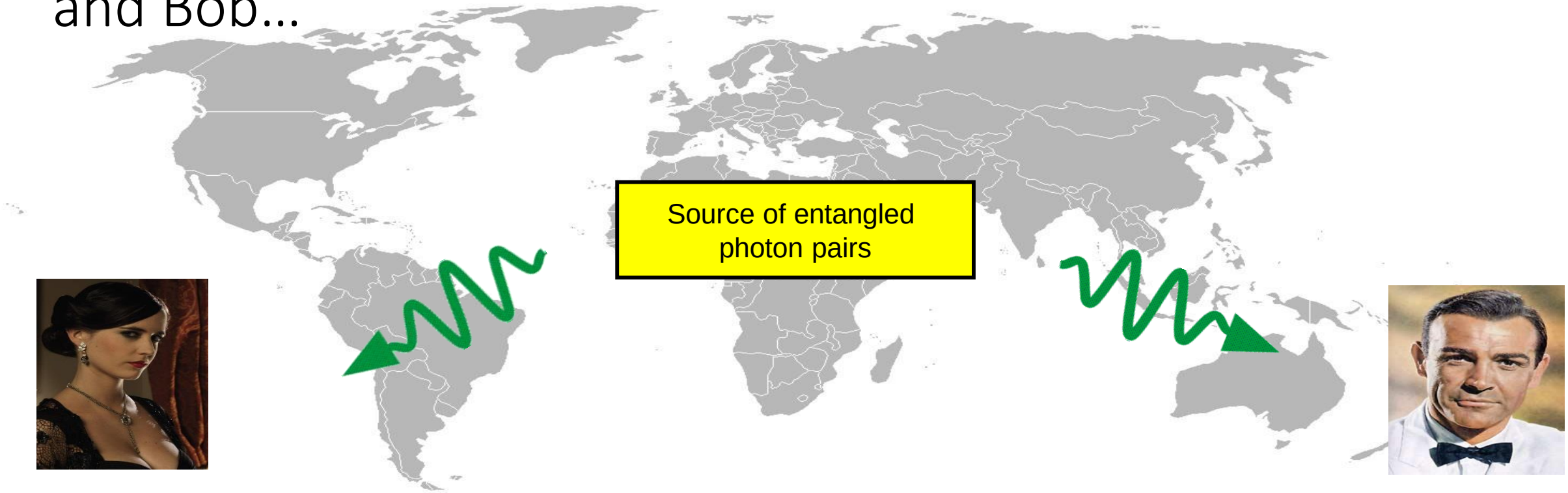
10 DFB lasers for different application tasks

CubeSat 6U
Power consumption 10-15 W
Satellite telescope aperture 80 mm
Pointing accuracy 15”
Orbit height 400-600 km

Quantum repeaters

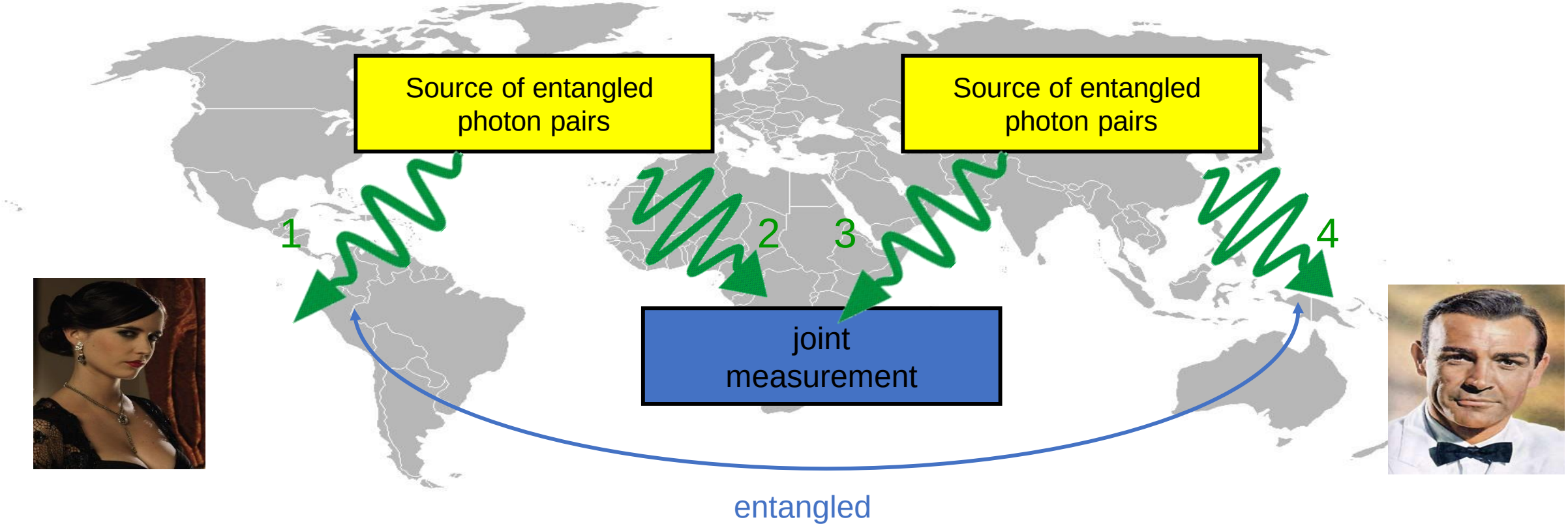
- Problem: to get 1 photon after 1000 km line you need to make ~ 10^{20} ts what is not practical
- Practical distances are within 100 km in the external lines and within 400 km in the lab (less than 1 bit/s)
- Solution comes from classical communication, we need a repeater
- What is a repeater
  - Device that captures a signal, regenerates it, and sends it further
- Classical repeater will inevitably cause noise
- Quantum repeater
  - Must capture and regenerate a photon without measuring its polarization
  - Requires *memory* for efficient operation
  - Requires entangled states

We need to create quantum correlations between Alice and Bob…



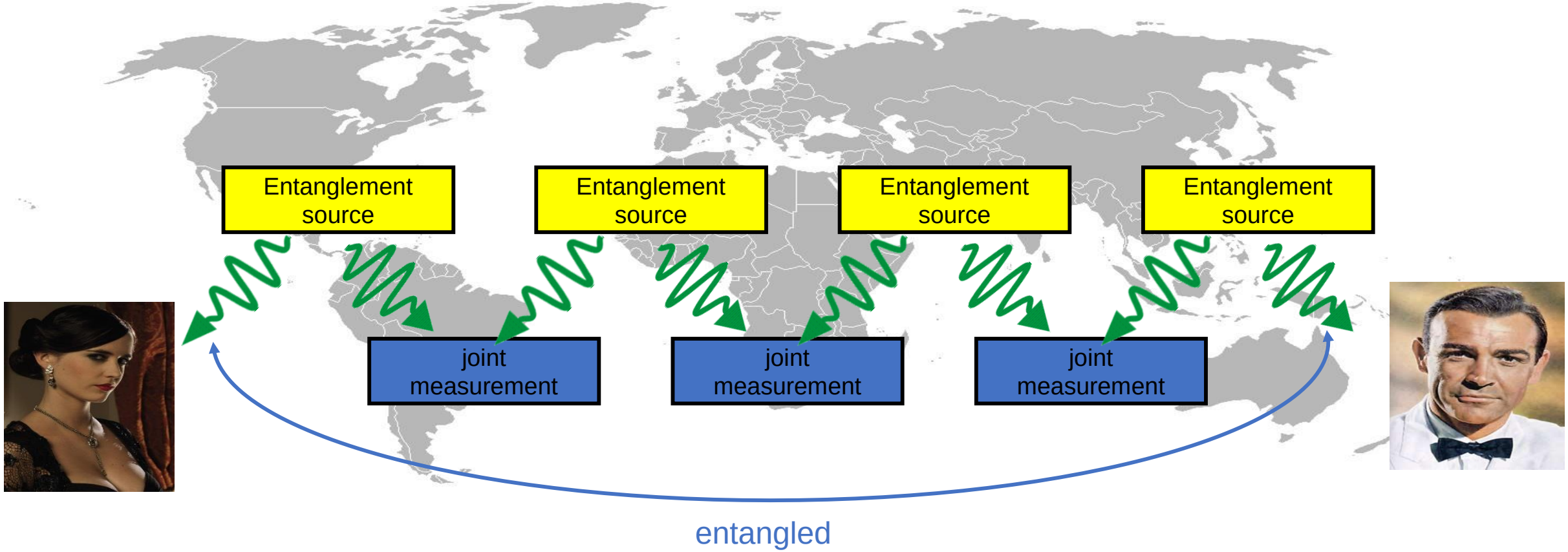
☹ The photons are likely to get lost on their way

Entanglement swapping



- Long-distance entanglement can be created by *entanglement swapping*
  - A Bell measurements on modes 2 and 4 entangles modes 1 and 4
  - This protocol has much in common with teleportation

Quantum relay

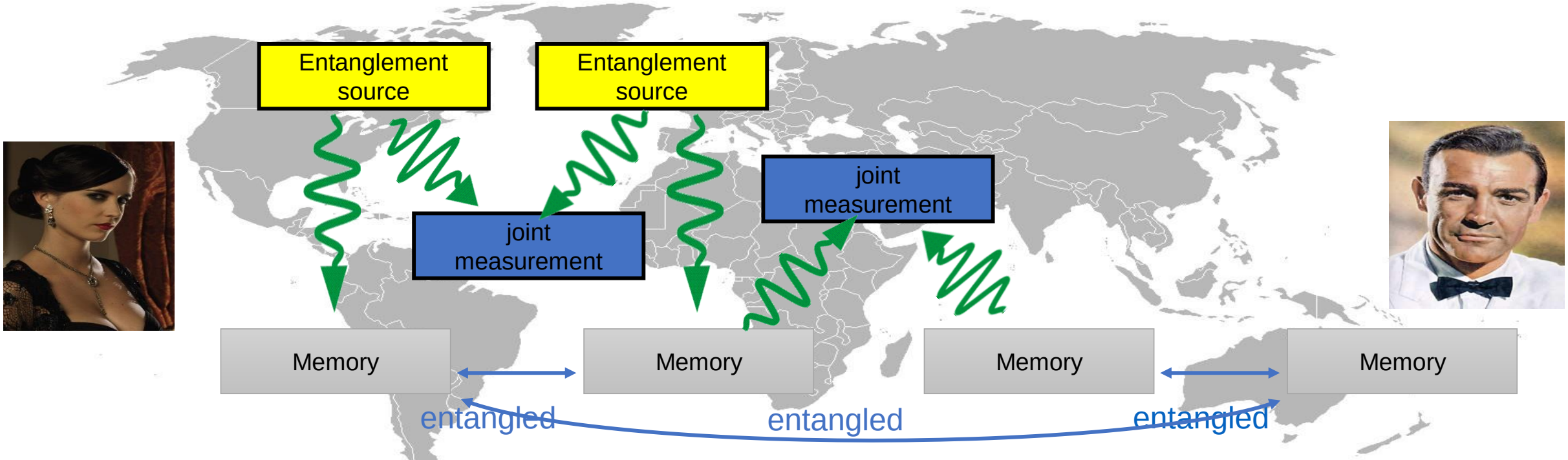


Long-distance entanglement can be created by *entanglement swapping*

☹ but to succeed, all links must work simultaneously.

→ success probability still decreases exponentially with distance.

The role of memory



- **But if we had quantum memory,**
  - entanglement in a link could be stored…
    until entanglement in other links has been created, too.
  - Bell-measurement on adjacent quantum memories...
    will create the desired long-distance entanglement.
  - Alice can teleport her photon to Bob

Quantum repeater

Memory | Memory | Memory | Memory

entangled

- **This technology is called *quantum repeater***
  - Initial idea: H. Briegel *et al.*, 1998
  - In application to EIT and quantum memory: L.M. Duan *et al.*, 2001
- Quantum memory for light is essential for long-distance quantum communications.

We're looking for talents!

Yury Kurochkin
yk@goqrate.com

QUANTUM COMMUNICATIONS

GAZPROMBANK

RQC
Russian Quantum Center

MINISTRY OF
EDUCATION AND SCIENCE