Lectures 3 and 4:
Quantum optics at a glance
(continued)

Introduction to quantum cryptography

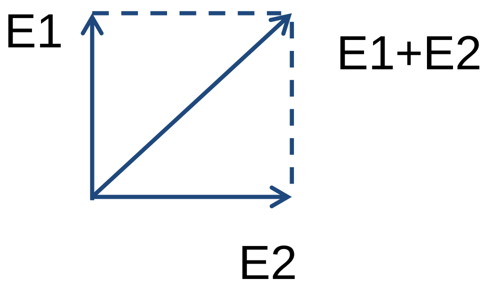
Content

- Bloch sphere
- No-cloning theorem
- Quantum measurements

- BB84 protocol
- Steps required for secret key extraction
- Source imperfection and decoy-state protocol
- Other protocols

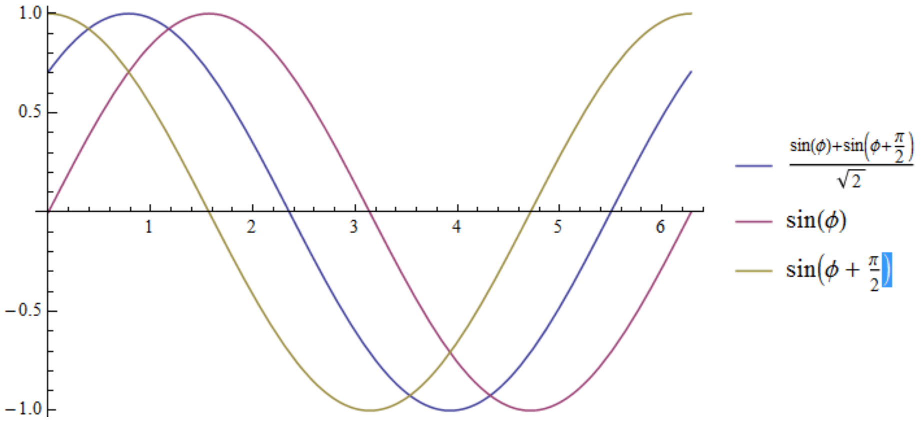
Superposition can be applied to different properties of quantum particle

Polarization



Phase

```
Plot[{(Sin[ϕ] + Sin[ϕ + π / 2]) / √2 , Sin[ϕ], Sin[ϕ + π / 2]}, {ϕ, 0, 2 π}, PlotLegends → "Expressions"]
```



QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

States prepared by Pockels cell

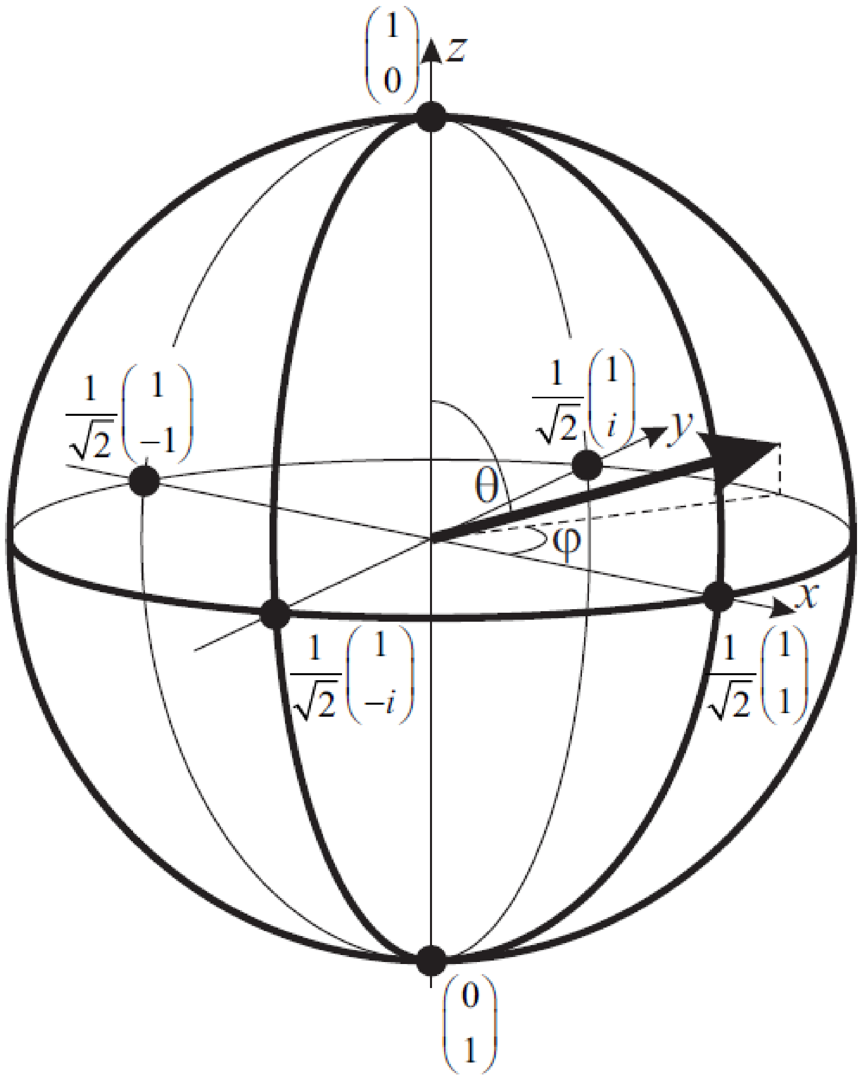
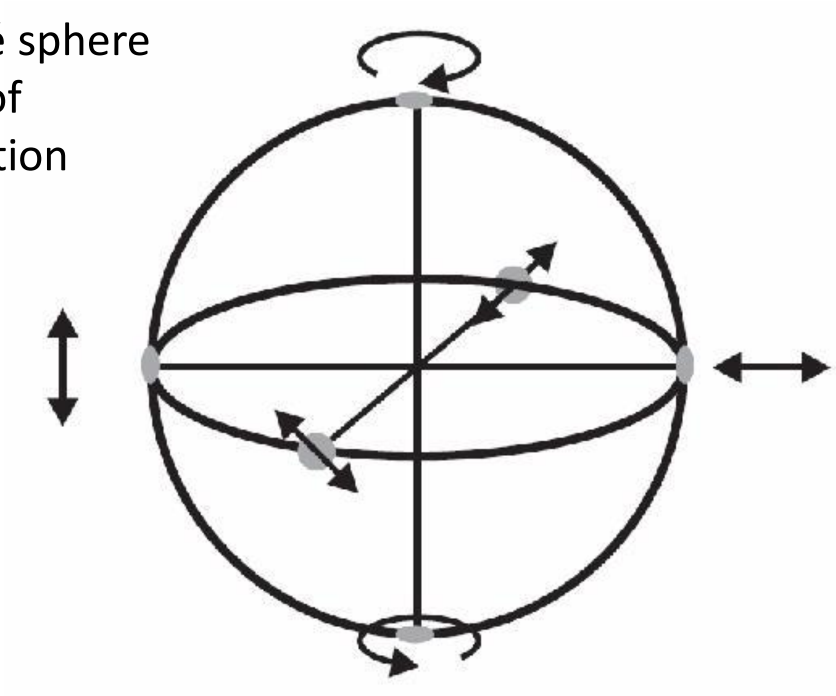
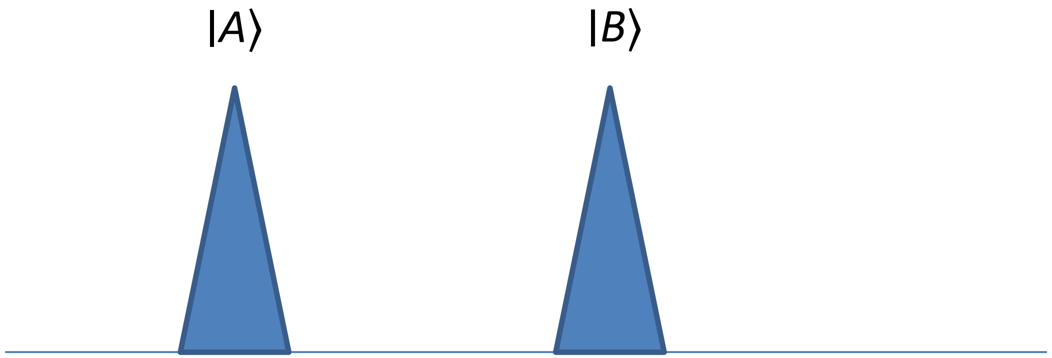


Figure 6.3: The Bloch sphere.

Poincaré sphere
in case of
polarization





$|0\rangle = |A\rangle + |B\rangle$
Other combinations?

Quantum No-Cloning Theorem

How to make quantum copy machine&

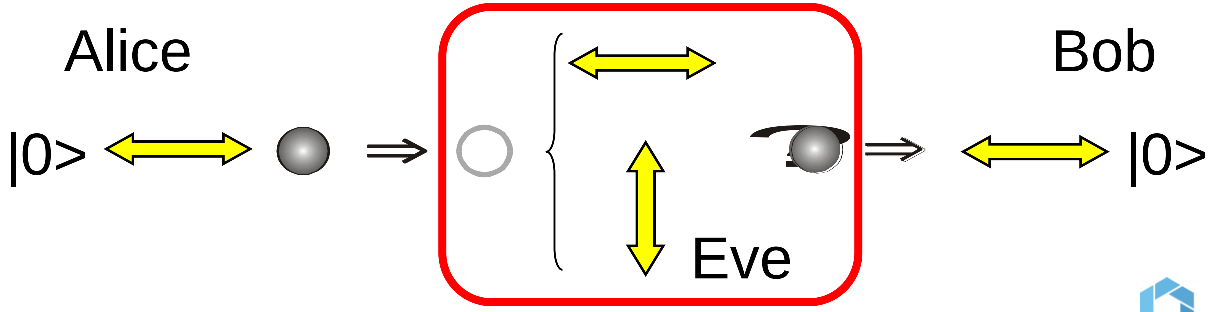
[W. K. Wootters and W. H. Zurek, Nature 299 (1982), pp. 802-803]

[S. Wiesner, SIGACT News, 15, 78 (1983)]

$$|0\rangle|blank\rangle|copy\_machine\rangle \Rightarrow |0\rangle|0\rangle|copy\_machine_0\rangle$$
$$|1\rangle|blank\rangle|copy\_machine\rangle \Rightarrow |1\rangle|1\rangle|copy\_machine_1\rangle$$

- $|blank\rangle = |0\rangle$ is an initial state of the copy particle
- The machine's operation must be unitary, so

$$|0+1\rangle|blank\rangle|copy\_machine\rangle \Rightarrow ?$$
$$|0\rangle|blank\rangle|copy\_machine\rangle + |1\rangle|blank\rangle|copy\_machine\rangle \Rightarrow ?$$

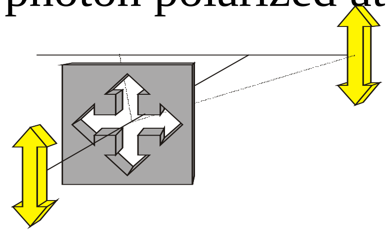


Why do we want the copy machine to be unitary?

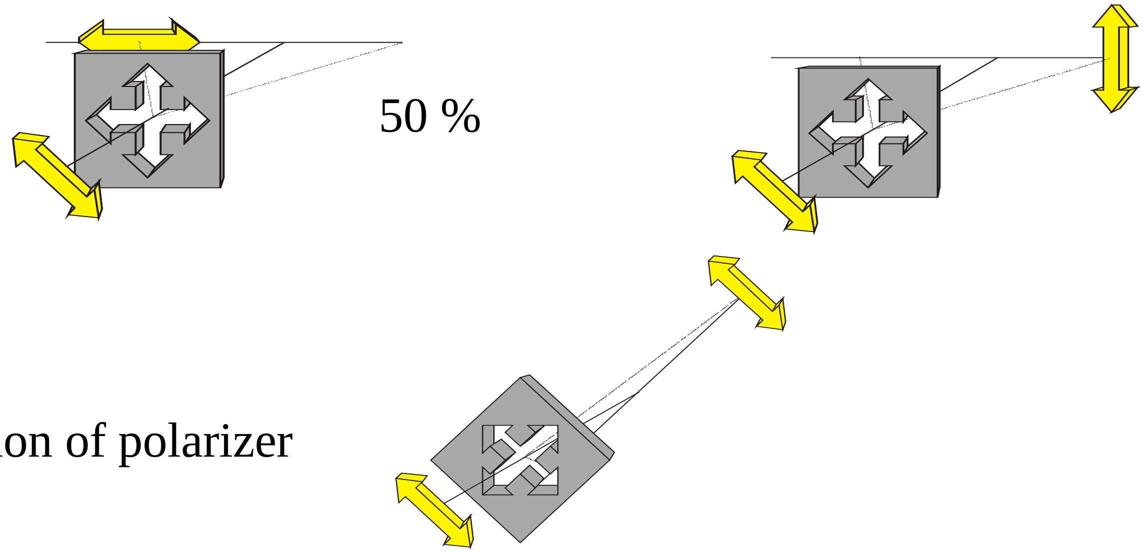
What non-unitary operators do you know?
How does it look like in the nature?

Irreversibility of Measurements

Incoming photon polarized at 90°



Incoming photon polarized at 45°



50 %

50 %

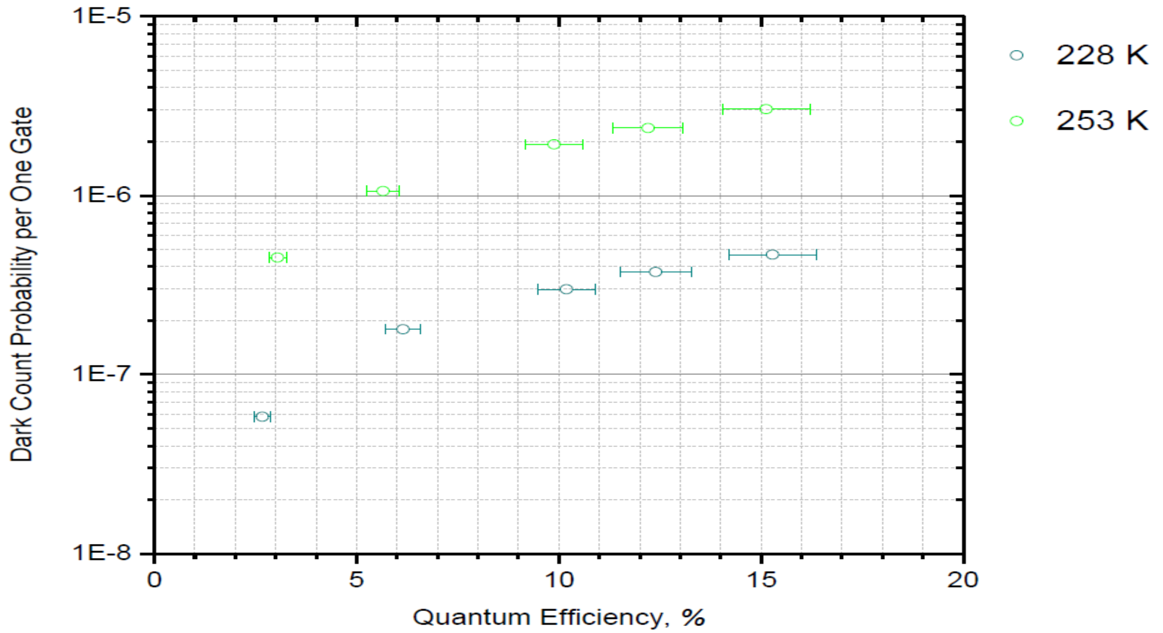
Rotation of polarizer

What interpretations do you know?

QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

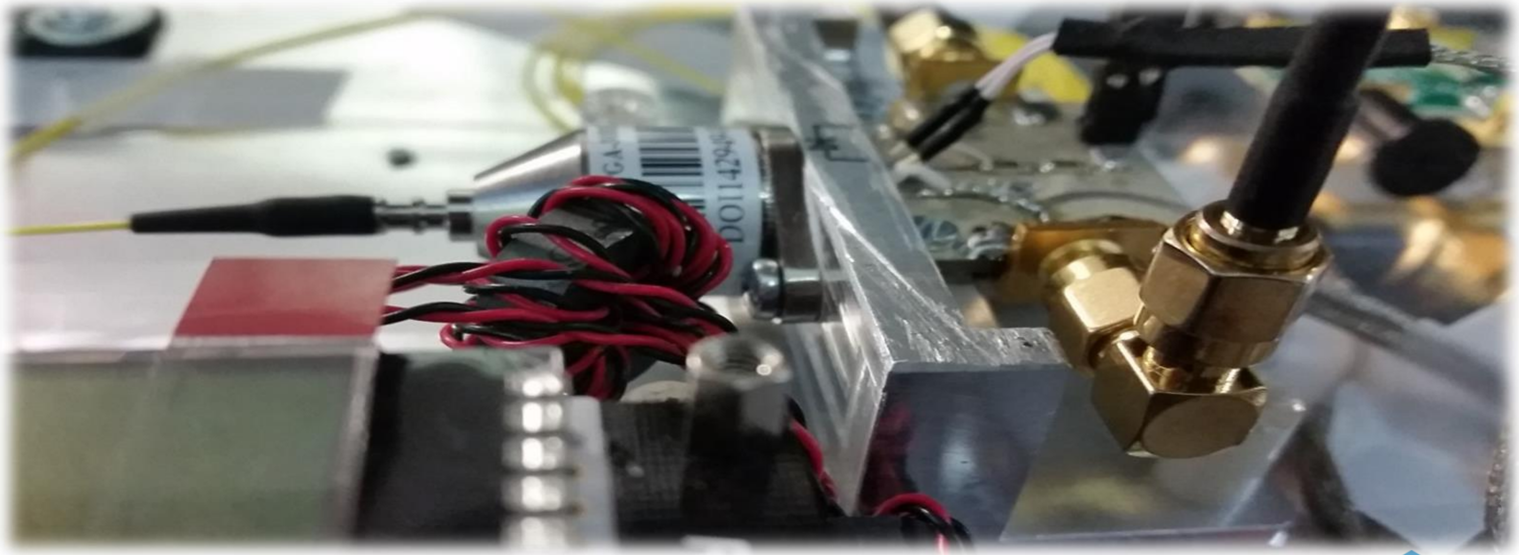
InGaAs avalanche photodiode based single photon detector



- 10% quantum efficiency
- Noises 3*10^(-7)
- Gating frequency

300 MHz.

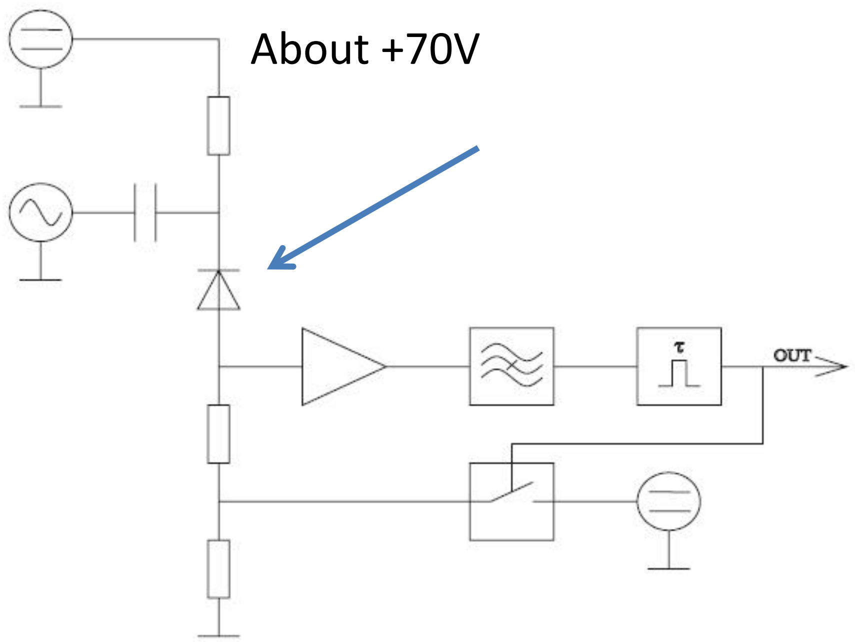
- Width of signal reception window 400 ps

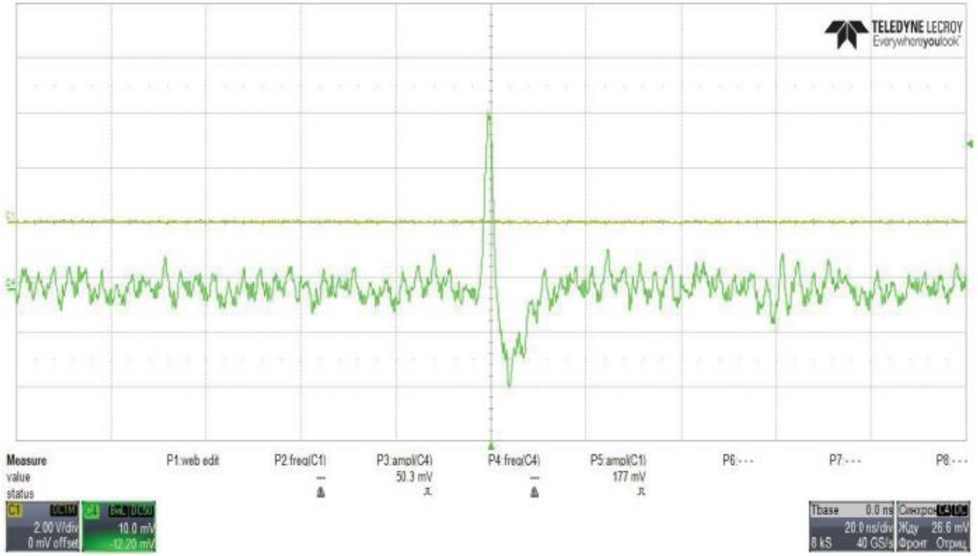


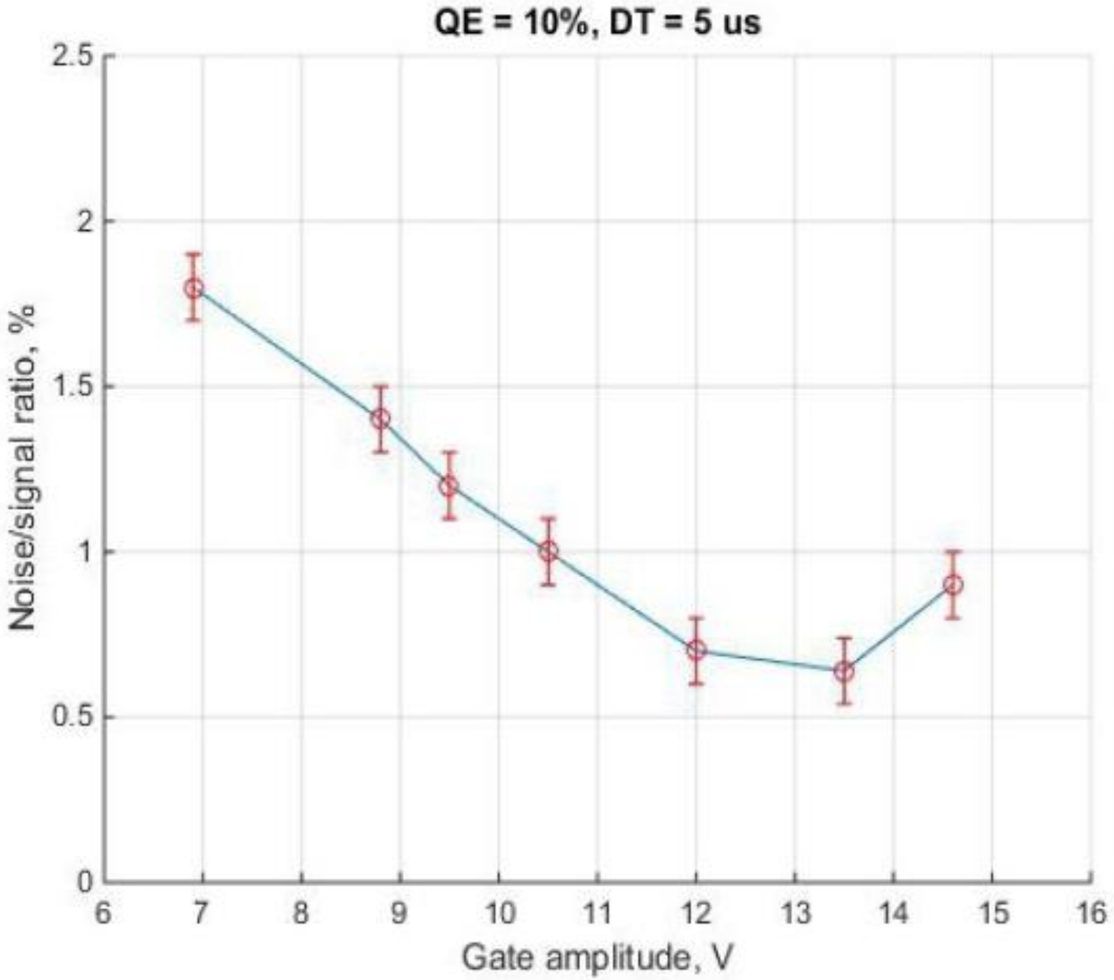
QRATE
QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

Basic principles of single photon detector







Single photon detector is the critical element of the QKD system

Quantum Efficiency. Probability to detect one photon. Signal rate is proportional to quantum efficiency.

Dark Count. Noisy count of the detector. Noisy clicks will be treated as Eve attack.

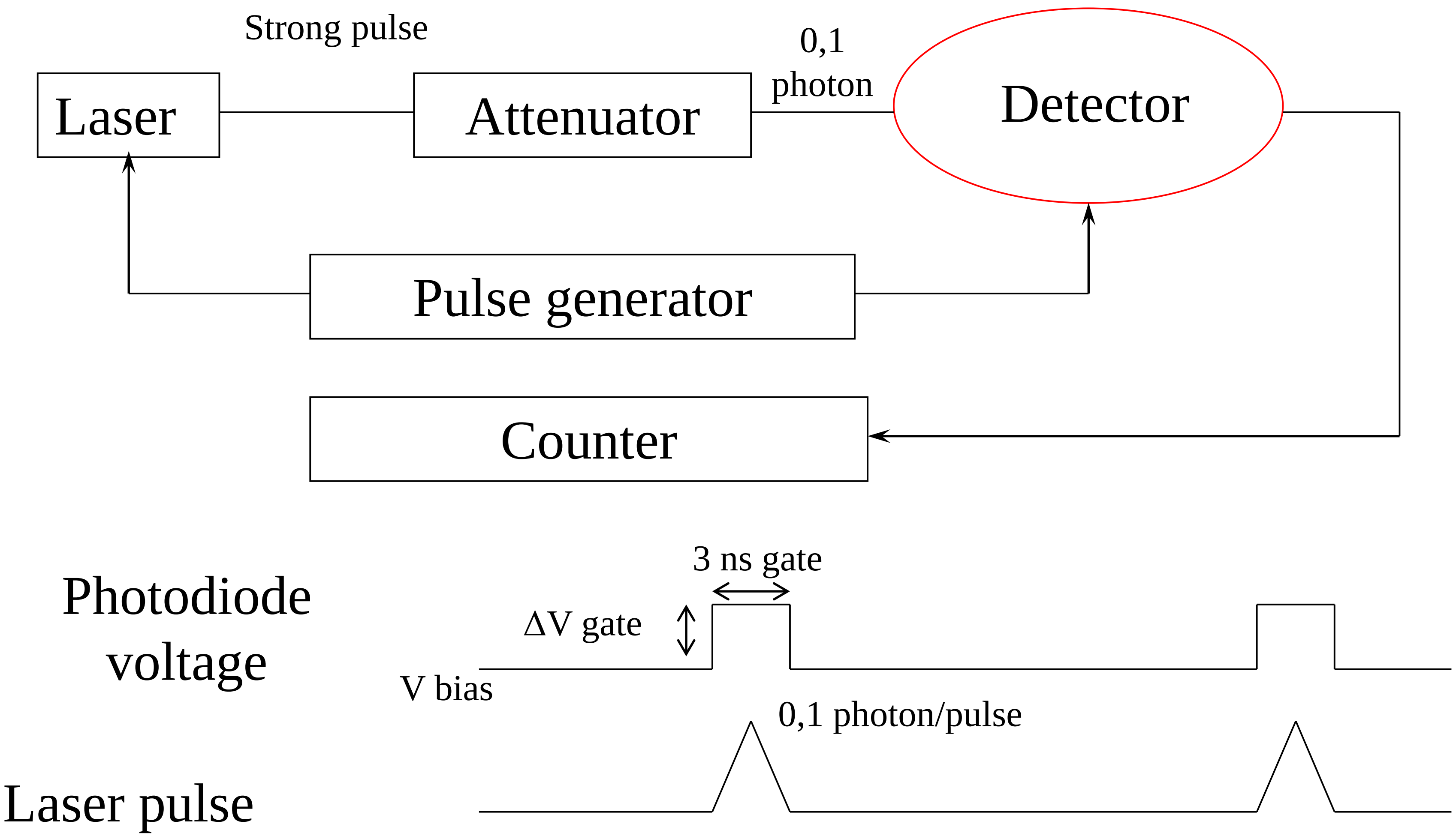
Afterpulsing. Probability to get noisy count some time after the detector click.

InGaAs -> 1550 nm (fiber wavelength)

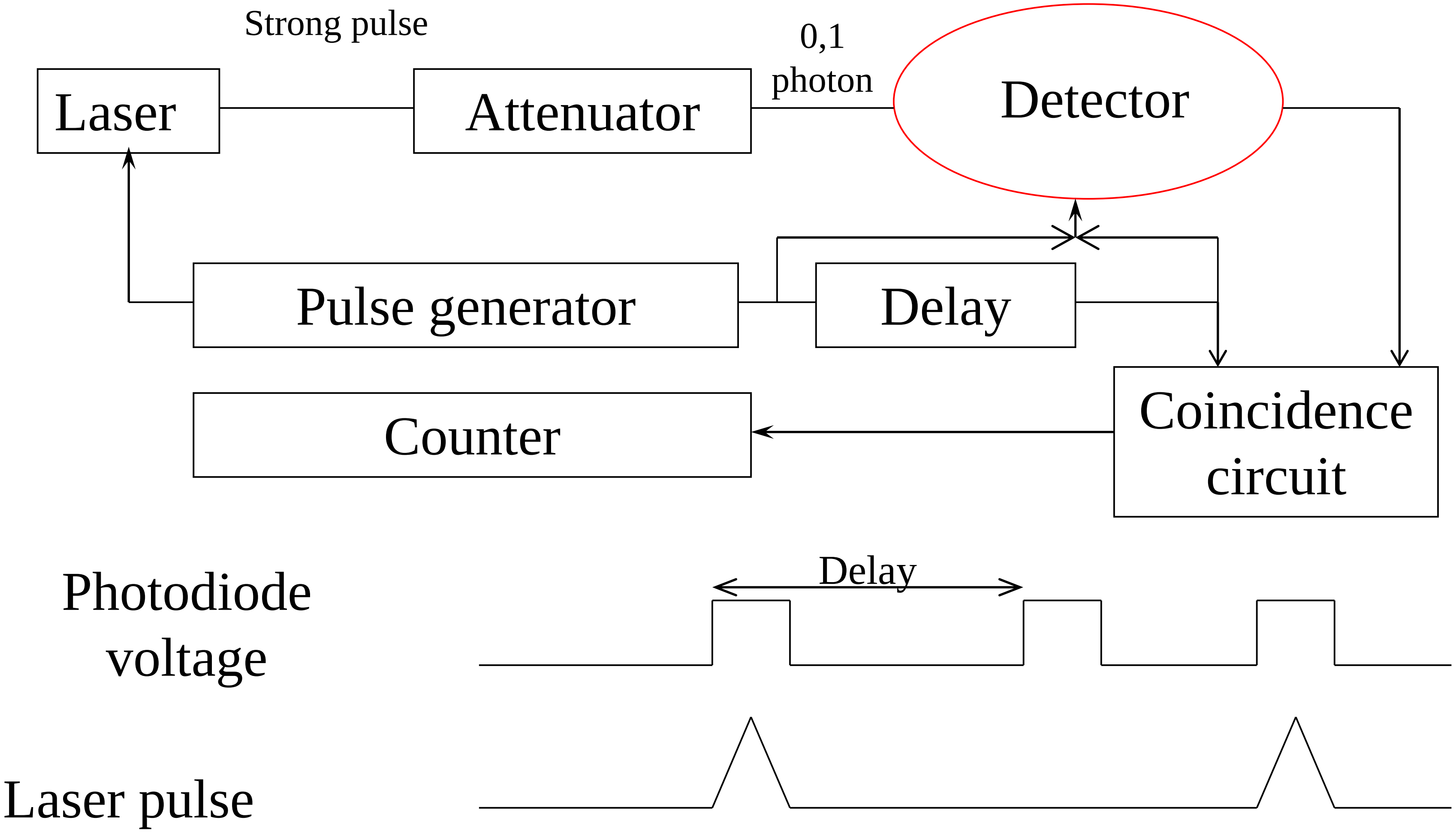
Si -> 800 nm (air transparency window)

InGaAs/InP avalanche photodiodes has much higher afterpulsing comparing to silicon detectors what cause large dead time

Measurement setup



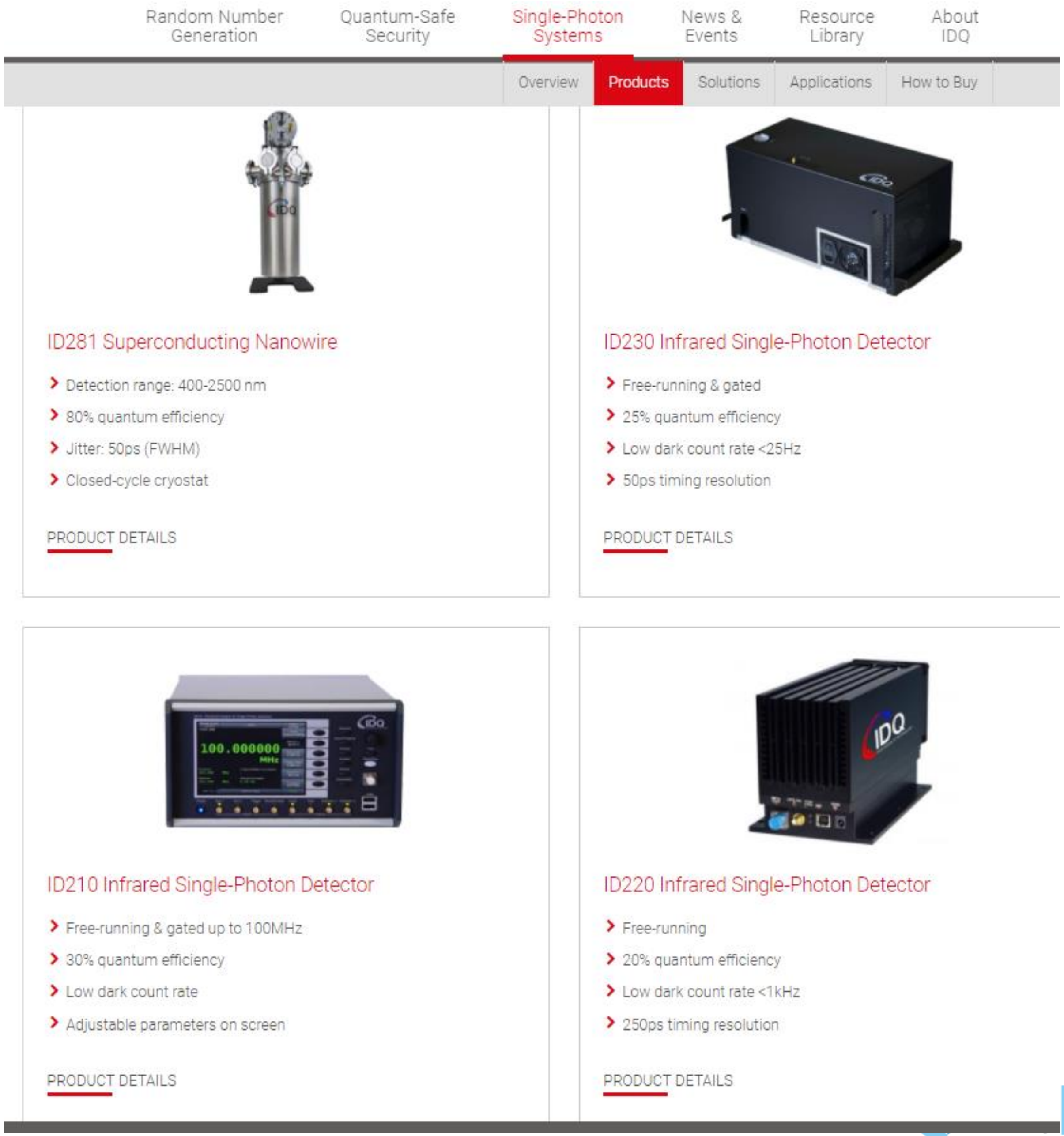
Afterpulsing measurement



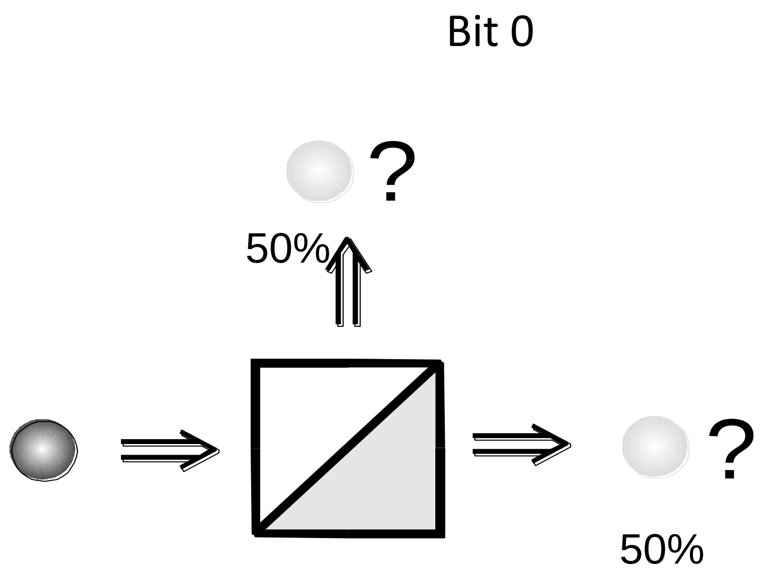
Best market available detectors are IDQuantique

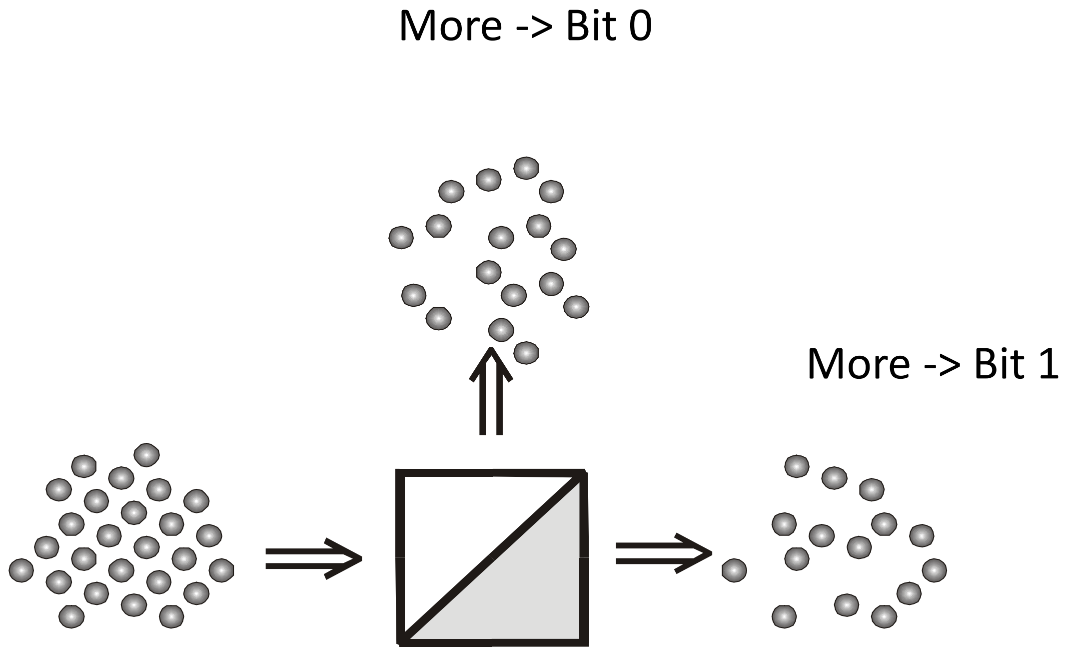
- There are about five single photon detector manufacturers in the World
- Market available single photon detectors are not suitable for high performance QKD
- IDQuantique uses Princeton Lightwave diodes (almost only OEM for high quality single photon diodes)

- Best gate rate has Toshiba research (1-1,5 GHz). But it is not on the market



Measuremensts and randmness





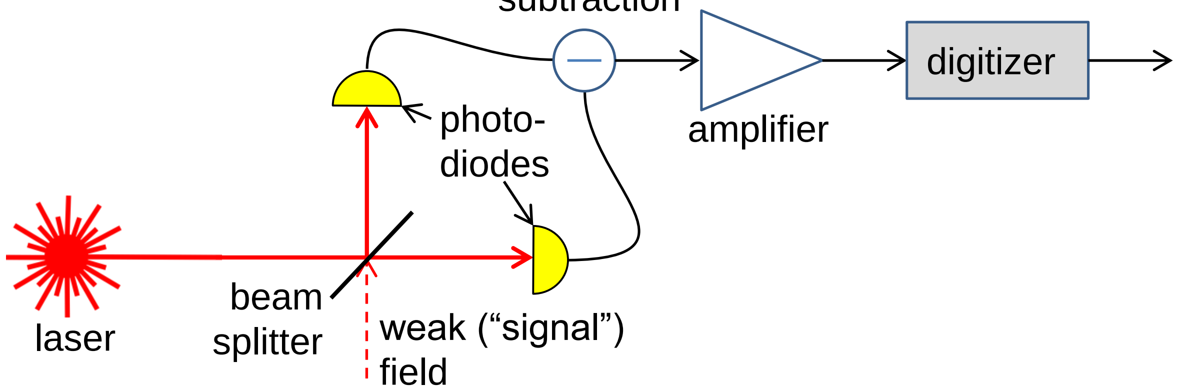
Estimate bit rate if the dead time is 5μs.

QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

Balanced detector to measure weak fields

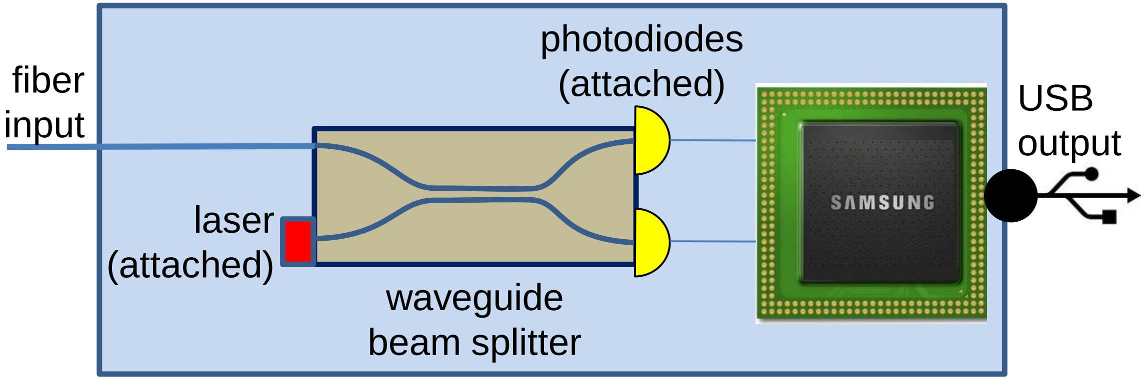
- **The principle**



- **Current prototype**

- Size: 5 cm
- Cost: ~ $100 + labor

- **What may look like in the future**



- Size: < 1 cm
- Cost: ~ $10

Our experience

Over 15 years of experience in constructing balanced detectors and using them for weak field detection[1]

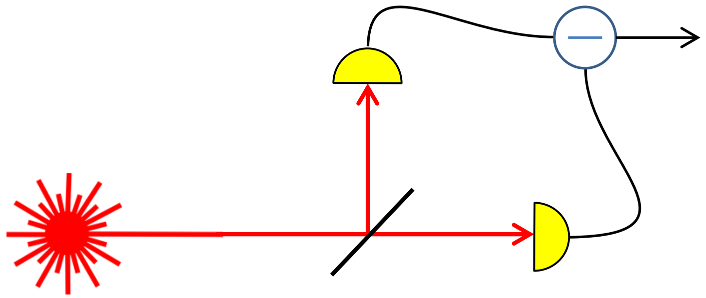
[1]H. Hansen et al., Optics Letters **26**, 1714 - 1716 (2001); R. Kumar et al., Optics Communications **285**, 5259 - 5267 (2012)

QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

Balanced detector as a cheap, fast, compact random number generator

The idea



Light consists of photons
- each photon has equal chance
  to transmit or reflect
- e. g. for N = 100,000,000 photon pulse,
  random disbalance on a scale of DN = √N = 10,000 photons
- the disbalance is present in the subtraction signal

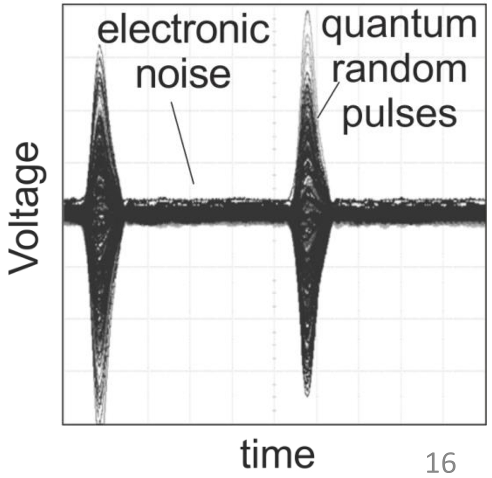
→**Fundamental quantum randomness in each output pulse**

Pulsed laser actually not required. Can use a cheap laser diode

Markets

Any cryptographic system uses a random number generator

- E-commerce
- Banks
- Cell phones
- Games



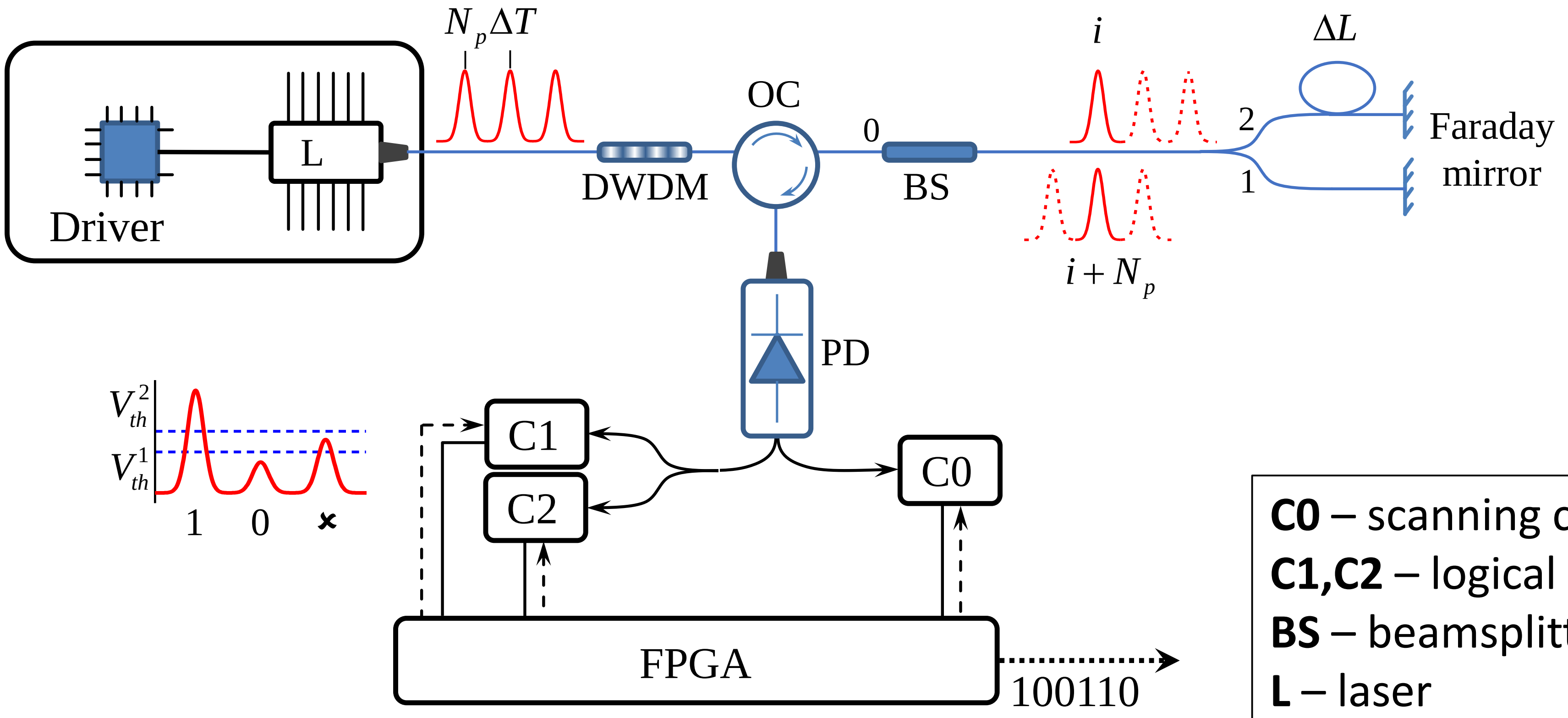
State of the art

Up to 2 Gb per second

QRATE QUANTUM COMMUNICATIONS

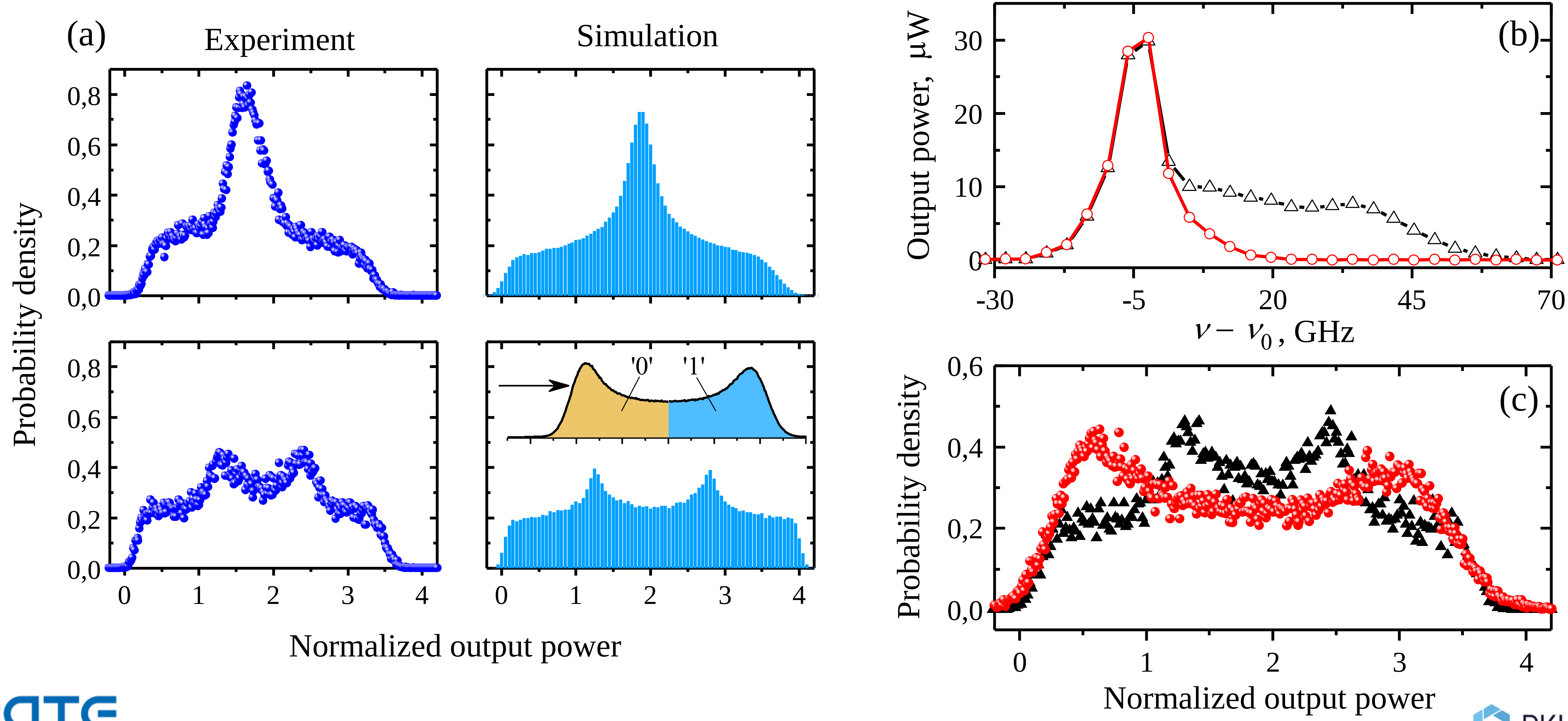
РКЦ Российский Квантовый Центр

Random number generator based on laser phase phase



C0 – scanning comparator
C1,C2 – logical comparator
BS – beamsplitter
L – laser
PD – photodiode
OC – optical circulator

Spectral properties affect the signal shape



QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

Quantum cryptography

Basics

One-time pad is proved to be secret

If Alice and Bob share a secret, random string of bits (the **key**), cryptography is easy.

original message 01101000..

XOR

secret key 01000101.. 01000101..

XOR

=

insecure channel

encrypted message 00101101.. 00101101..

=

01101000.. decrypted message

Check that it is unbreakable.
What other codes do you know?

QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

Public key encryption

$$C = E_x (P)$$
$$P = D_k (C) = D_k (E_x (P))$$

X: Public Key; K: Private Key

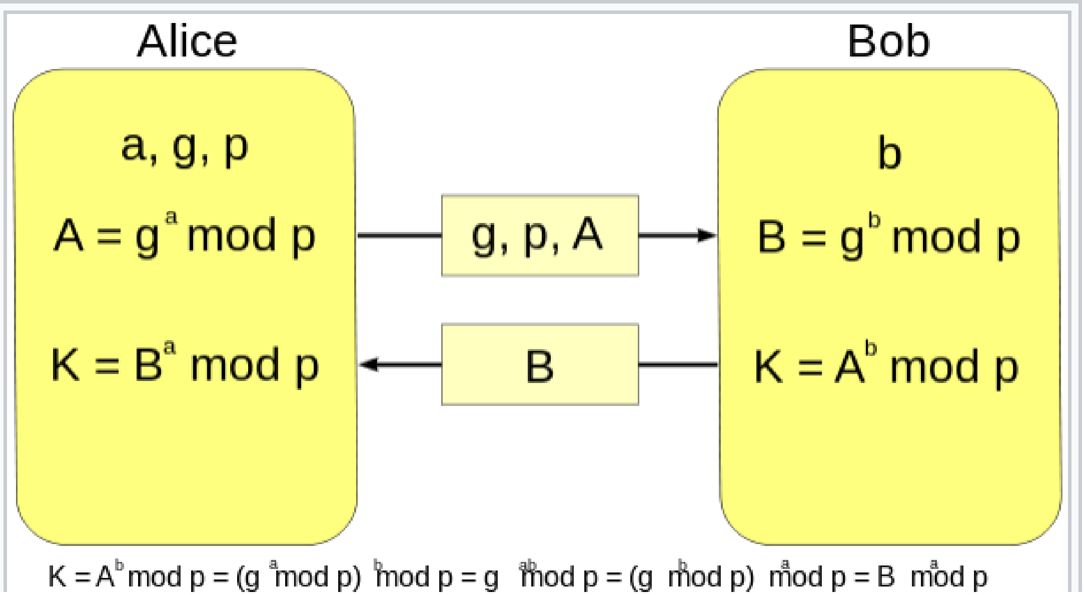
P: Plain Text; E: Encryption;
C: Ciphertext; D: Decryption.

RSA is based on factorization problem^

’ $N = n_1 \times n_2$

[R. Riverst, A. Shamir and L. Adleman, MIT/LCS/TR-212, Jan. 1979]

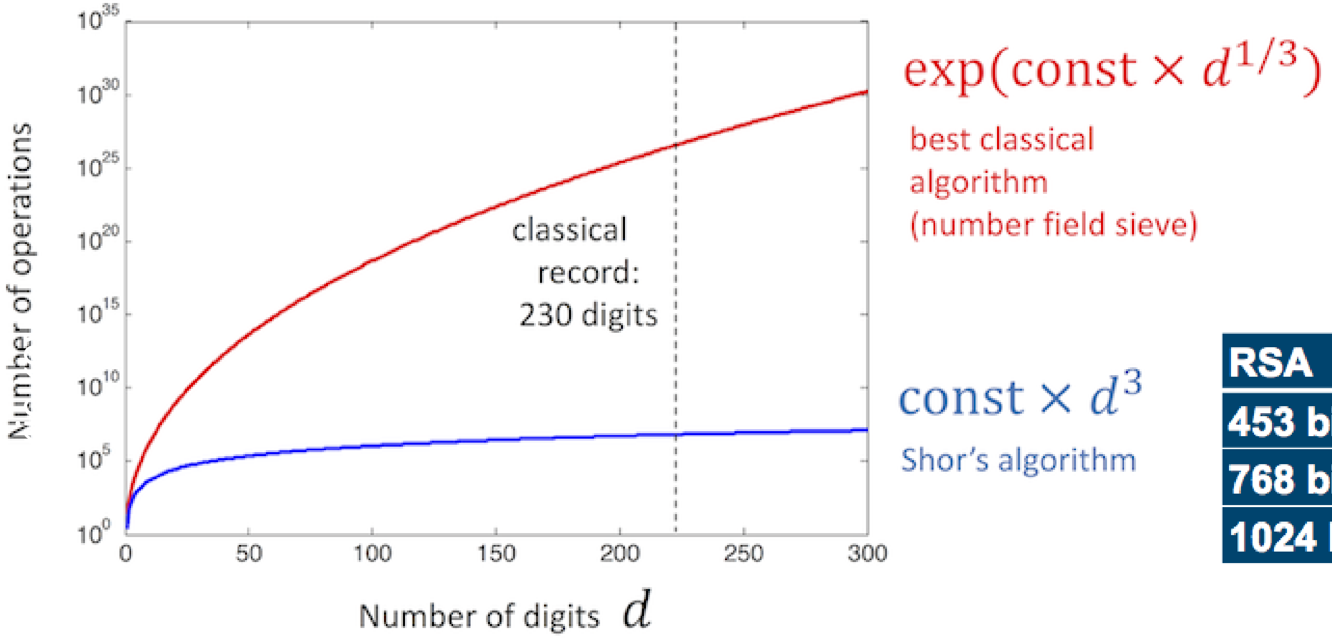
Diffie–Hellman key exchange



Alice		Bob		Eve	
Known	**Unknown**	**Known**	**Unknown**	**Known**	**Unknown**
$p = 23$		$p = 23$		$p = 23$	
$g = 5$		$g = 5$		$g = 5$	
$\mathbf{a = 6}$	b	$\mathbf{b = 15}$	a		a, b
$A = 5^a \bmod 23$		$B = 5^b \bmod 23$			
$A = 5^6 \bmod 23 = 8$		$B = 5^{15} \bmod 23 = 19$			
$\mathbf{B = 19}$		$\mathbf{A = 8}$		$A = 8$, $B = 19$	
$s = B^a \bmod 23$		$s = A^b \bmod 23$			
$s = 19^6 \bmod 23 = \mathbf{2}$		$s = 8^{15} \bmod 23 = \mathbf{2}$			s

Threat of quantum computers

Peter Shor



RSA	cracked in	CPU years	Shor
453 bits	1999	10	1 hour
768 bits	2009	2000	5 hours
1024 bits		1000000	10 hours

Lov Kumar Grover

Algorithm	Key Length	Effective Key Strength / Security Level	
		Conventional Computing	Quantum Computing
RSA-1024	1024 bits	80 bits	0 bits
RSA-2048	2048 bits	112 bits	0 bits
ECC-256	256 bits	128 bits	0 bits
ECC-384	384 bits	256 bits	0 bits
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

Applying Grover's algorithm to AES: quantum resource estimates

Markus Grassl[1], Brandon Langenberg[2], Martin Roetteler[3] and Rainer Steinwandt[2]

[1] Universität Erlangen-Nürnberg & Max Planck Institute for the Science of Light
[2] Florida Atlantic University
[3] Microsoft Research

February 24, 2016

Store ciphertexts now – decrypt later

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

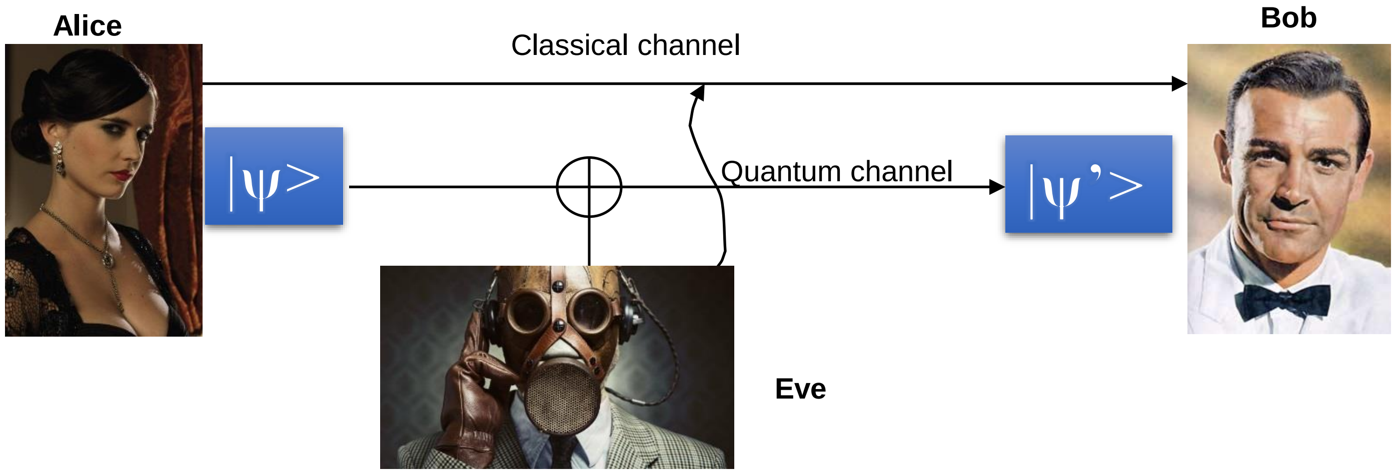
Figure 4 - Lead time required for quantum safety

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"

Quantum cryptography is beautiful application of single particle



Alice and Bob: to estimate the Eve's information I_{AE} on key

I_{AE} small: Error correction + Privacy amplification

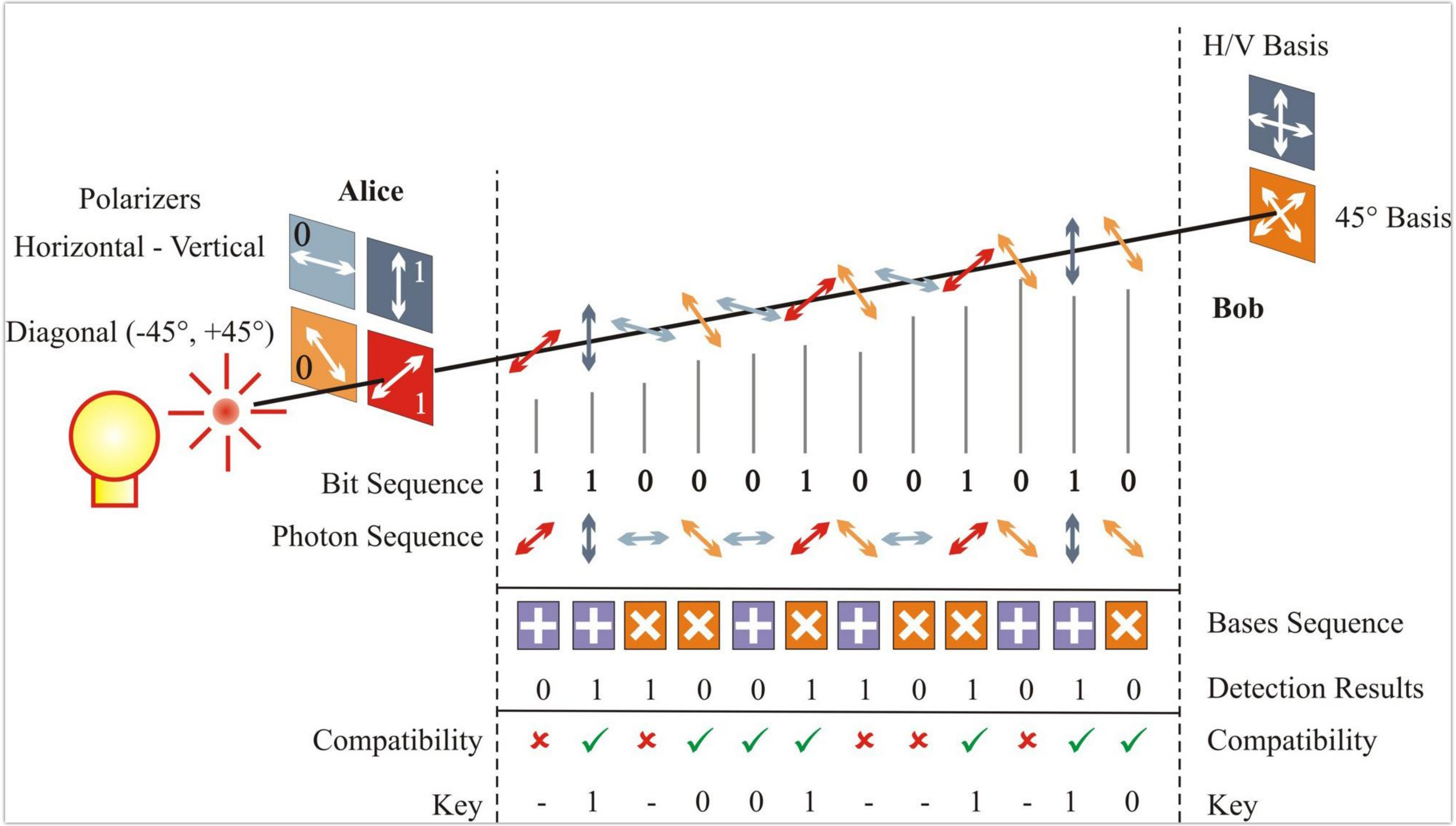
I_{AE} large: 

Experimentalists: to maximize I_{AB}

Theorists: to quantify I_{AE}

- New protocols -> higher tolerance to noise, bit rate and distance growth
- New methods to prepare and measure states -> reduce size and cost
- Security analysis and attacks -> search for good model of non-ideal components

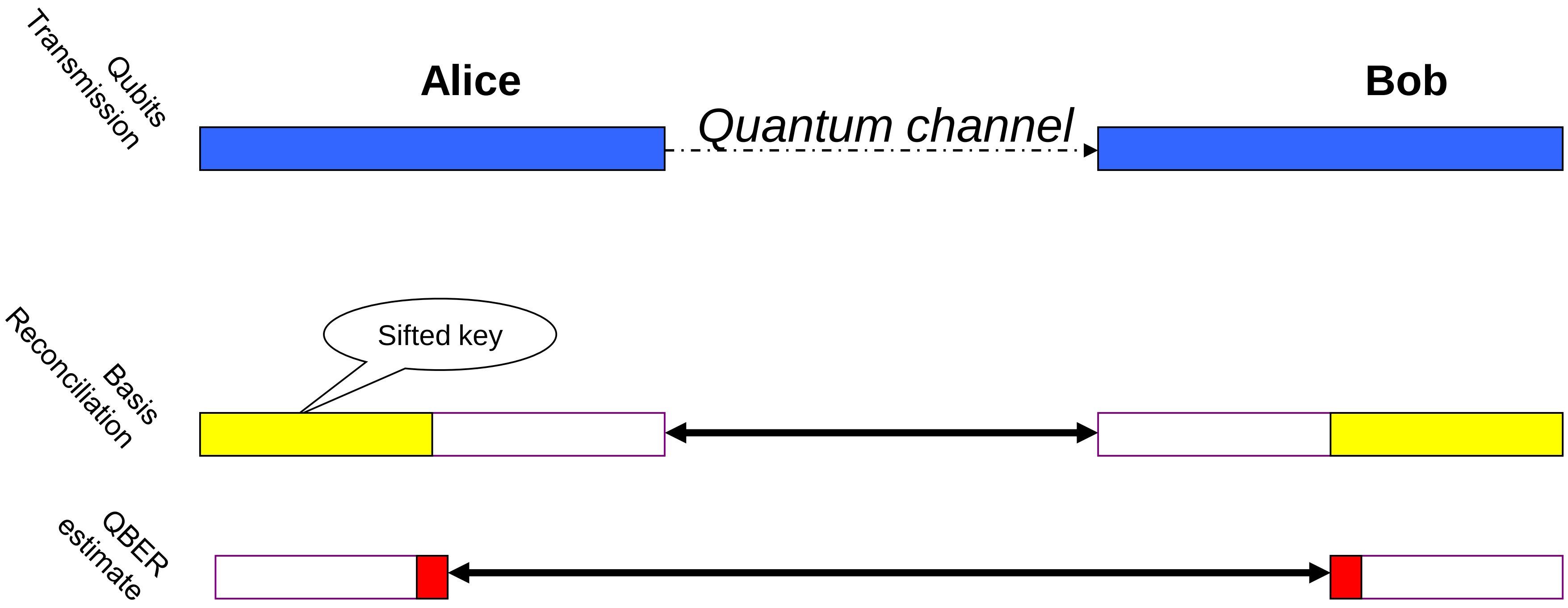
BB84 is the first and most popular protocol



QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

Key Distillation (ideal case)



QBER = { 0 : no eavesdropping ; > 0 : eavesdropping

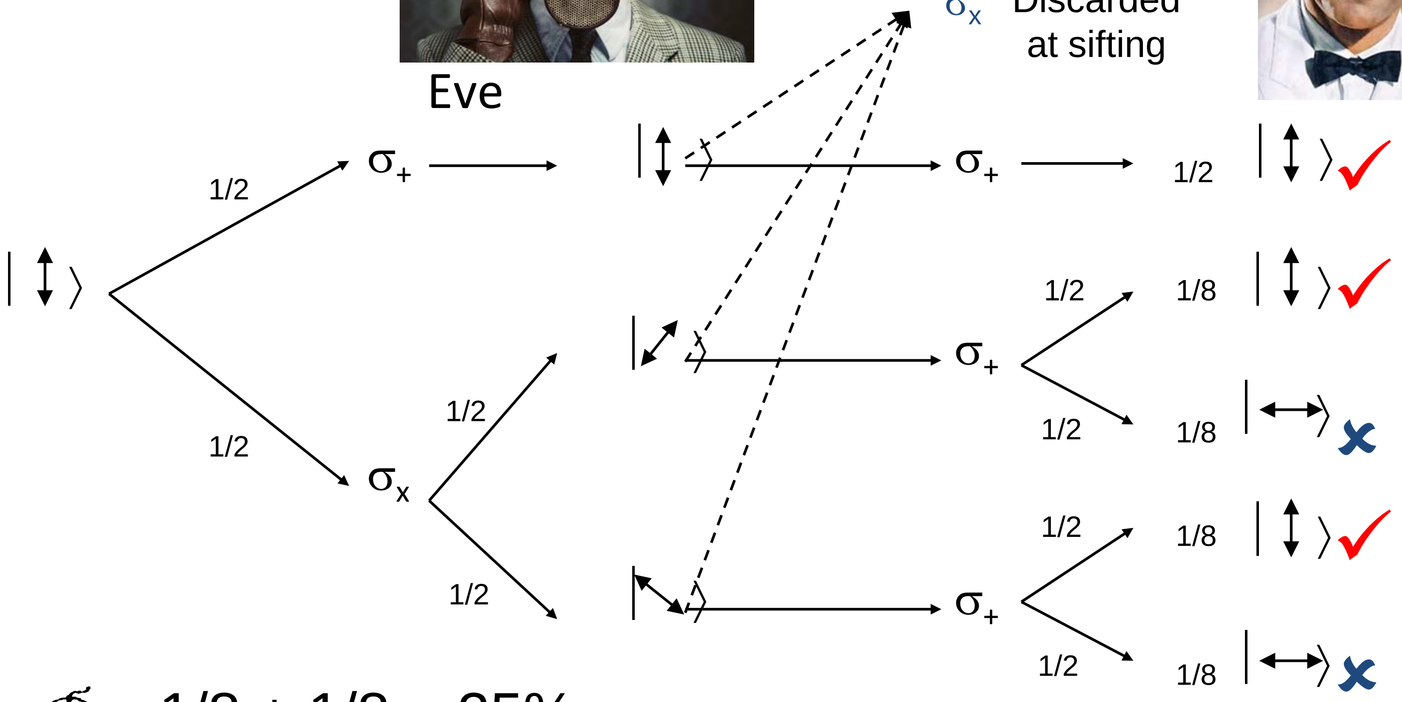
Reveals rather than prevents eavesdropping

A better name: **quantum key distribution**

Eavesdropping (1): Intercept and resend

Simplest attack: example

Eve

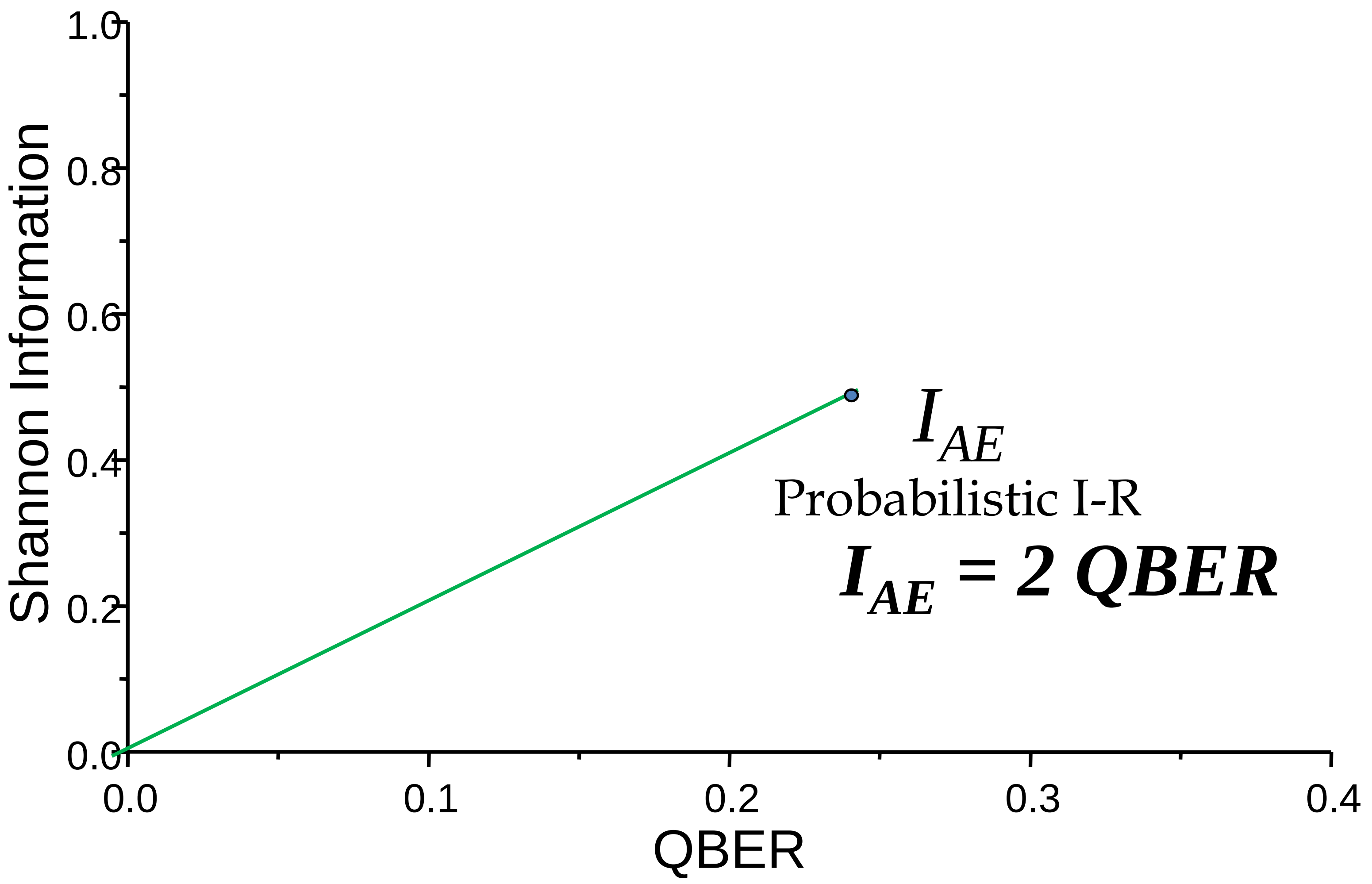


QBER = $\mathcal{D}$ = 1/8 + 1/8 = 25%

$I_{AE} = 2\ QBER$

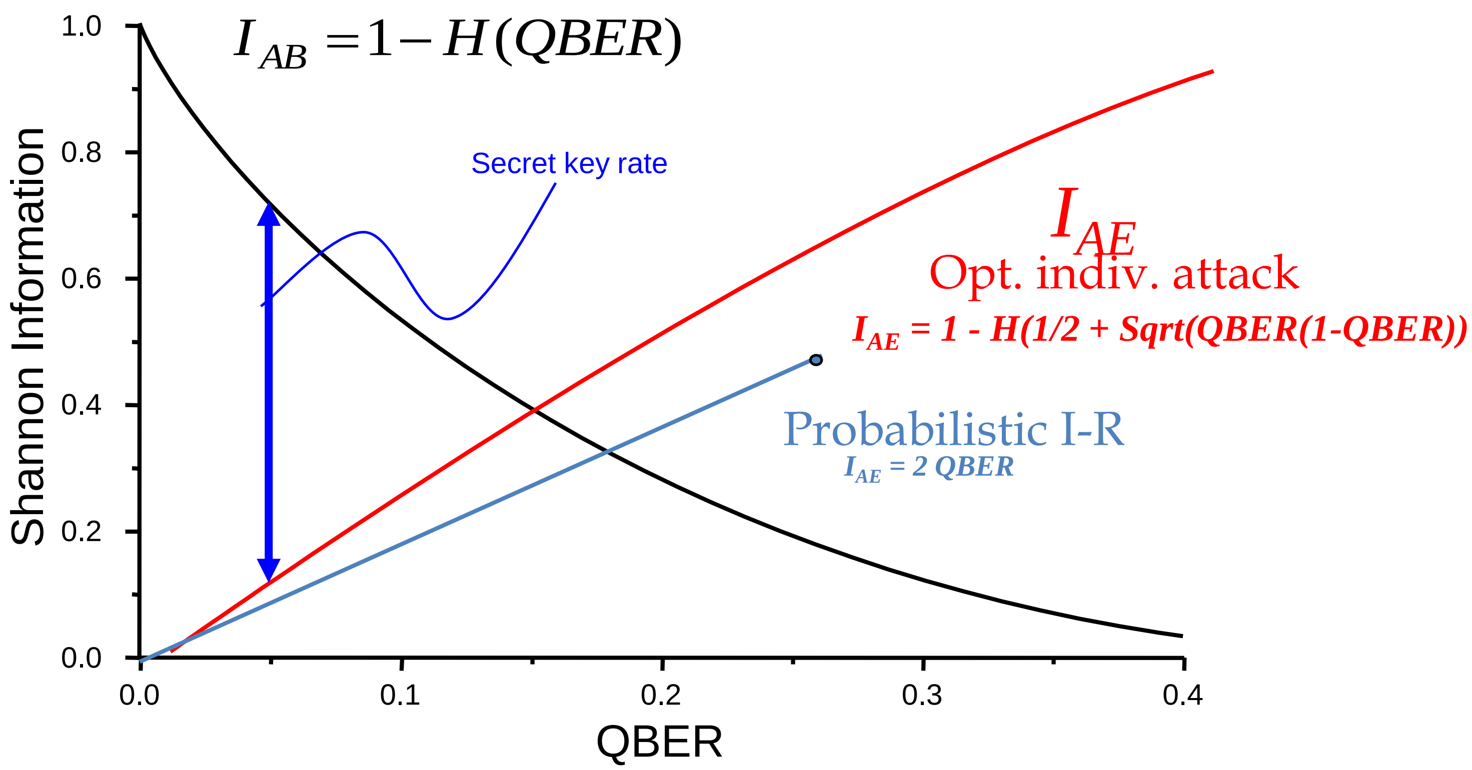
QBER Estimate: $\mathcal{D} \leftrightarrow I_{AE}$

Incoherent attacks: information curves

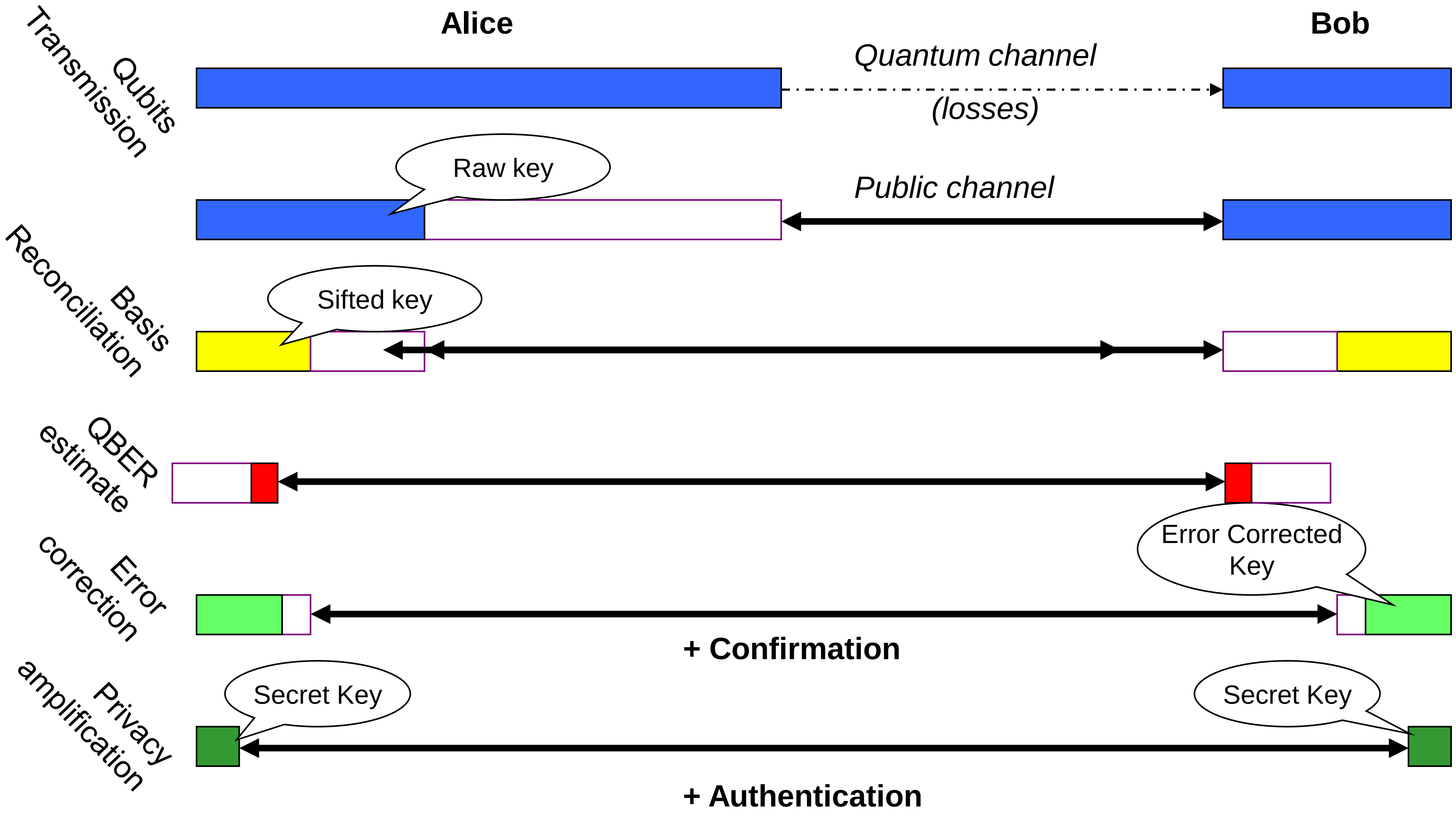


Information Theory and QKD

Shannon's Bound: $r = n - n\,(1 - I_{AB}) - n\,I_{AE} = n\,(I_{AB} - I_{AE})$

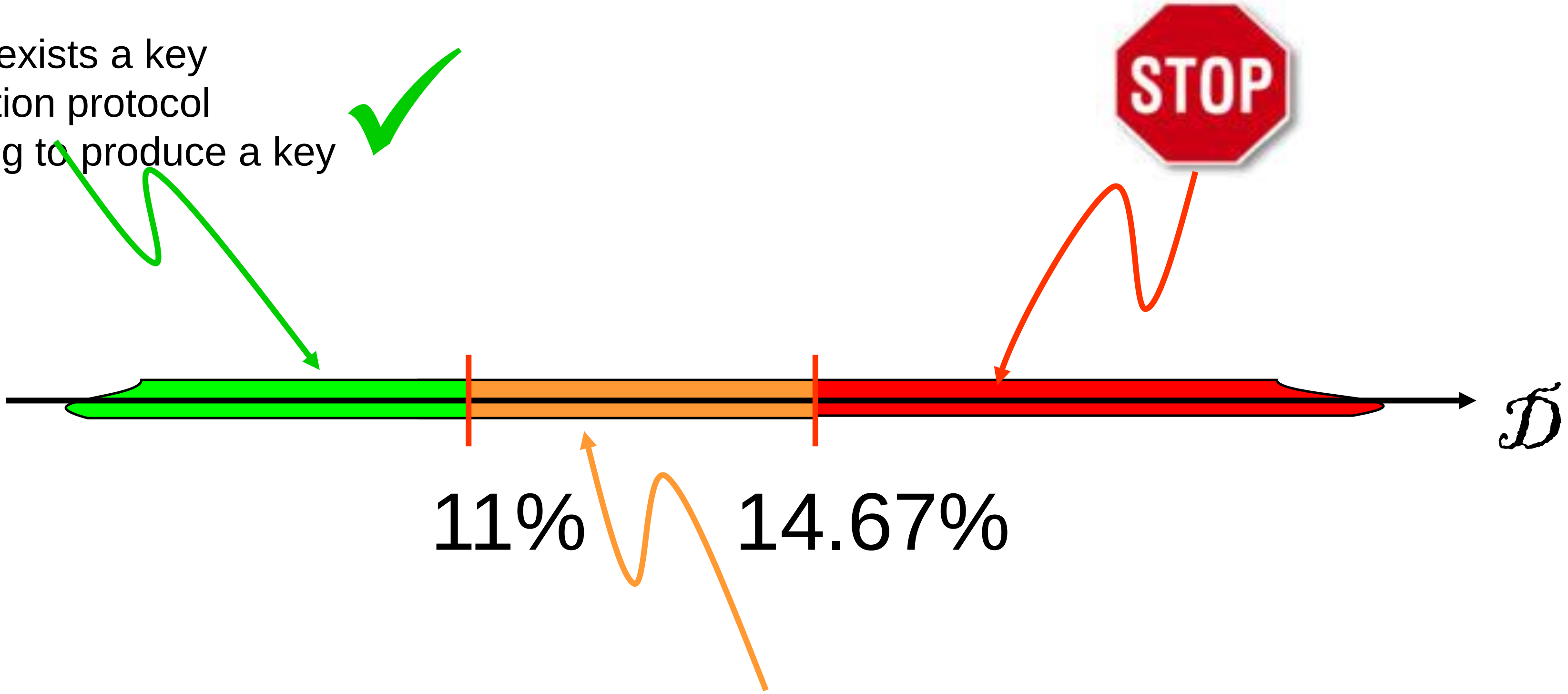


Key Distillation (realistic case)



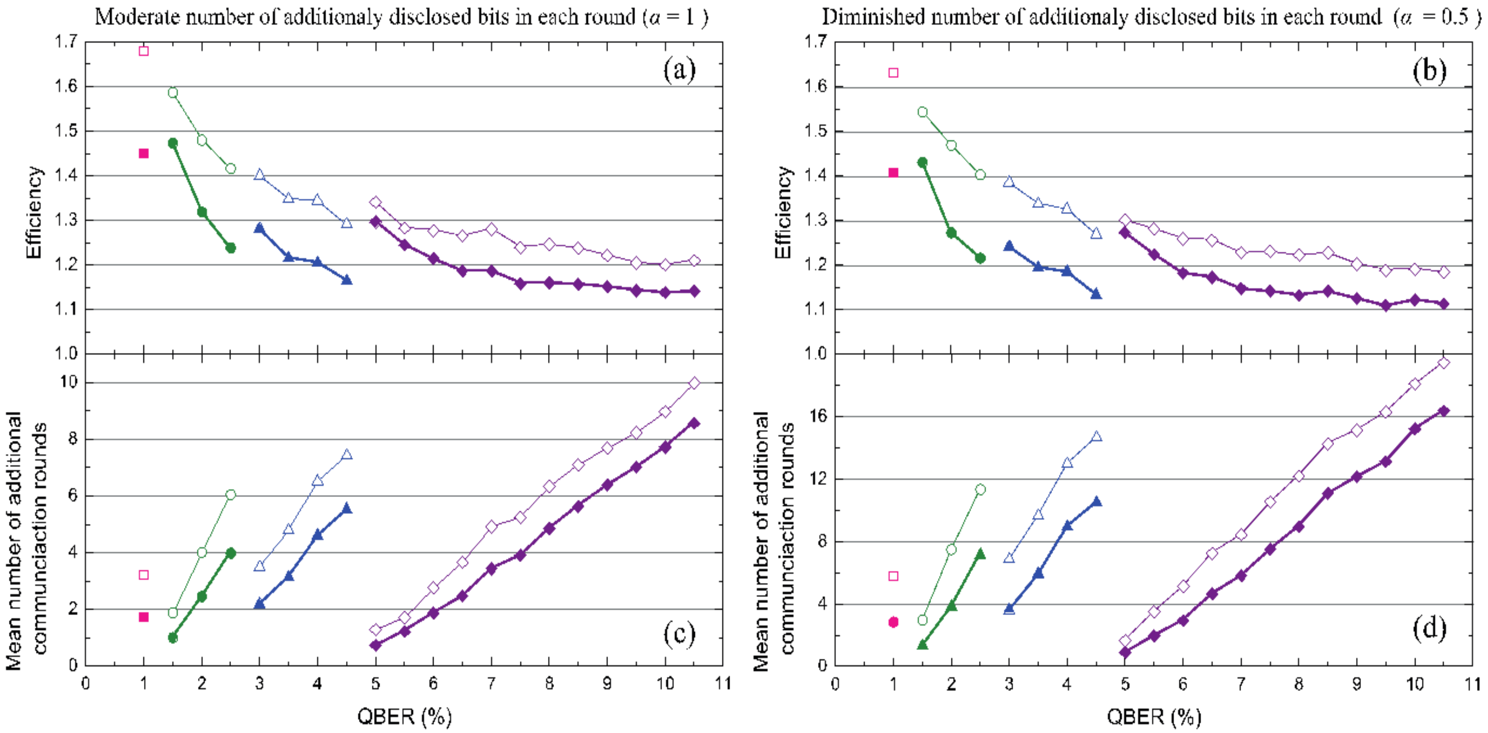
Summary (single-photons)

There exists a key
distillation protocol
allowing to produce a key



There may exist a key
distillation protocol
allowing to produce a key

Developed the advanced platform for processing quantum keys

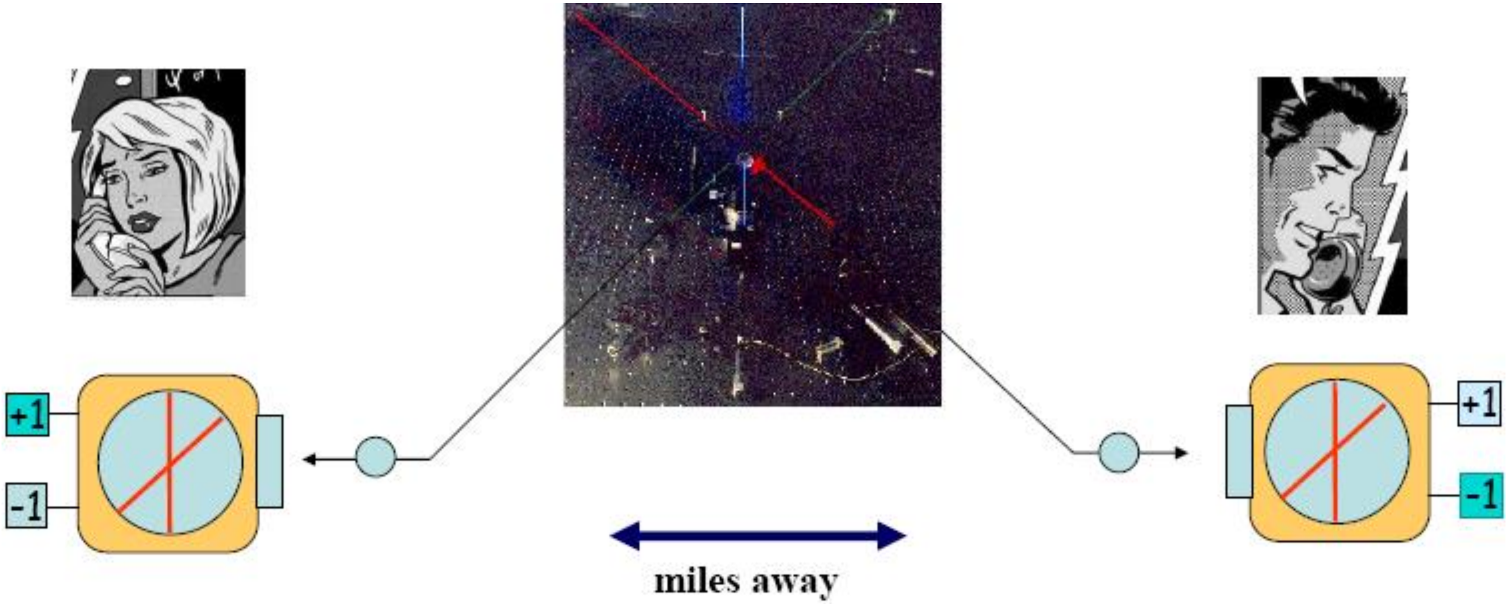


The most significant result is the creation of a record-breaking error correction algorithm. It exceeds the existing algorithms by an average of 10% in efficiency. It saves up to 30% of communication resources.

Common laboratory with SMI

The processing platform works
In Open-Source mode

Entanglement scheme



$$|\Psi^-\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1 |V\rangle_2 - |V\rangle_1 |H\rangle_2)$$

$$= \frac{1}{\sqrt{2}}(|H'\rangle_1 |V'\rangle_2 - |V'\rangle_1 |H'\rangle_2)$$

Where $|H'\rangle, |V'\rangle$ are the 45 degree Polarization

$$|H'\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$$

$$|V'\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$$

[A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991)]

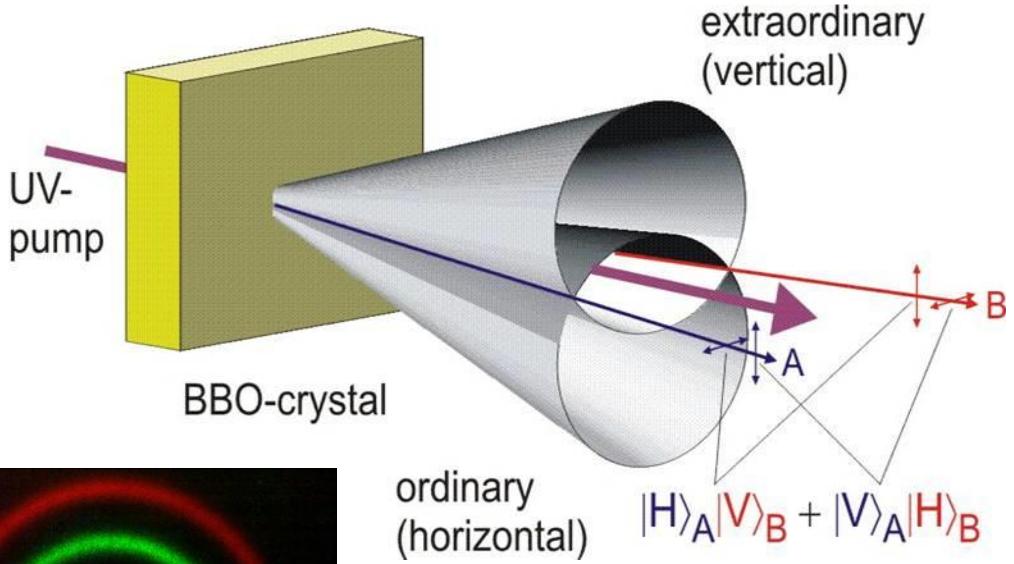
Ekert protocol and realization

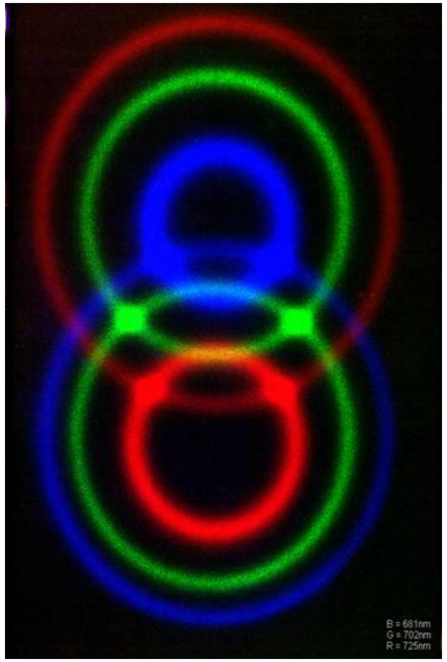
Alice

Bob

Charlie

$$\Psi = |\uparrow_A \uparrow_B\rangle + |\downarrow_A \downarrow_B\rangle == |0_A 0_B\rangle + |1_A 1_B\rangle$$





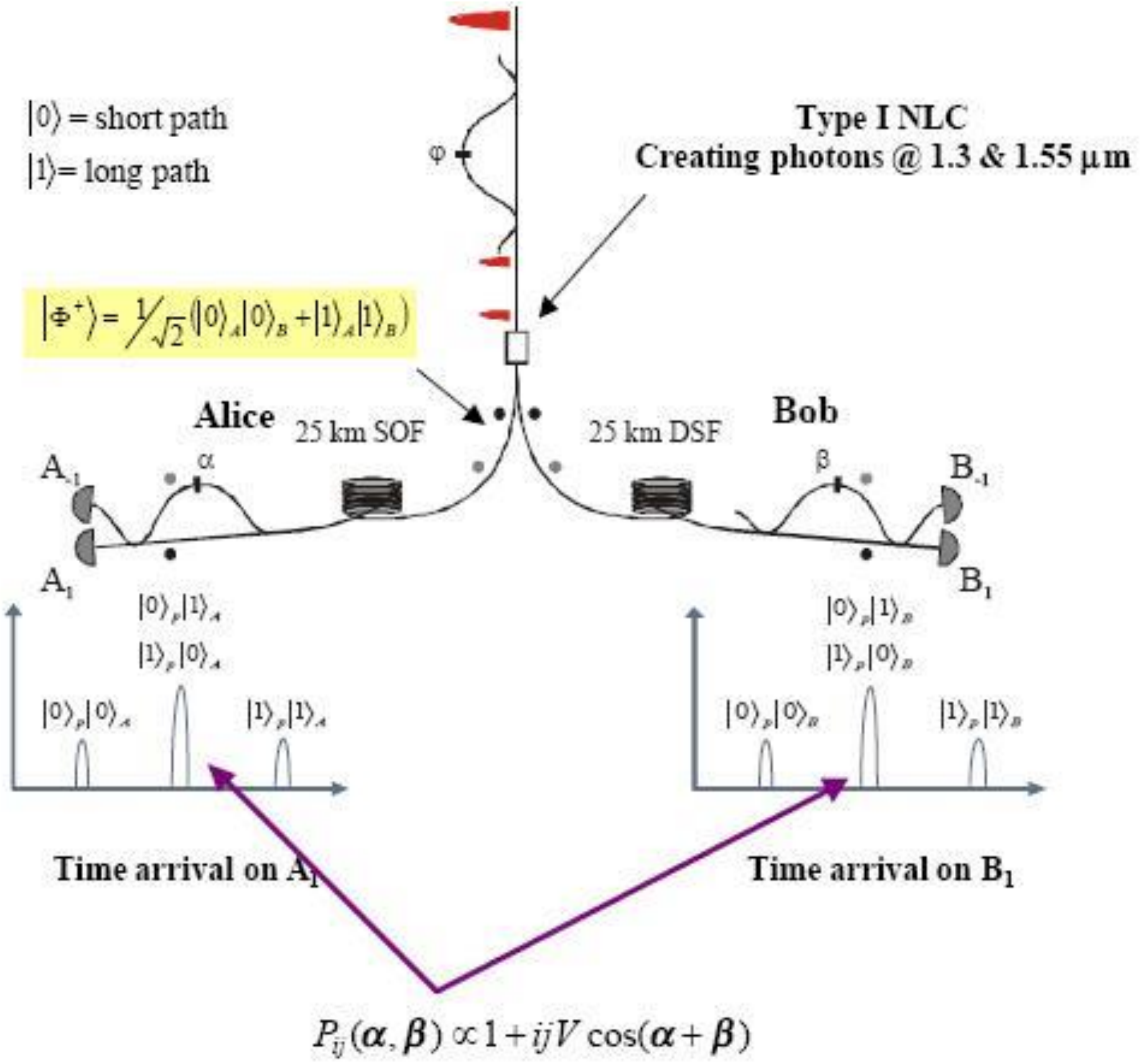
$$|\Phi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1 |H\rangle_2 \pm |V\rangle_1 |V\rangle_2\right)$$

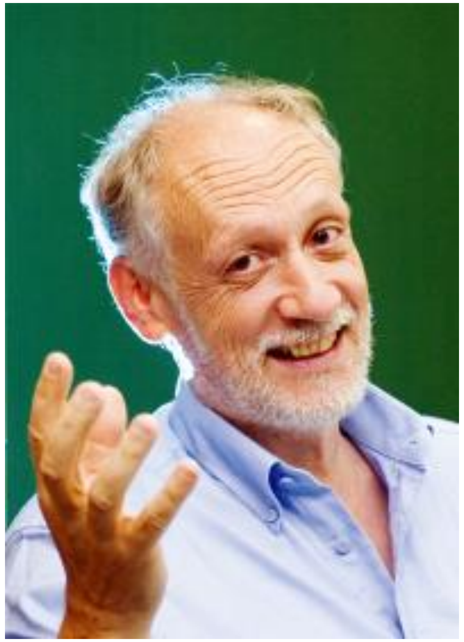
$$|\Psi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1 |V\rangle_2 \pm |V\rangle_1 |H\rangle_2\right)$$

[A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991)]

[P. G. Kwiat et al., Phys. Rev. Lett. 75, 4337 (1995).]

Experimental realization: Time bin entanglement





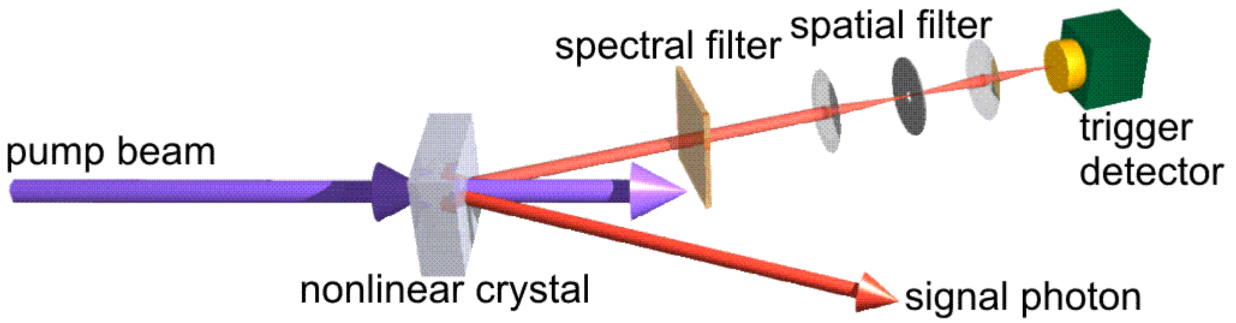
How to generate a photon?

Parametric down-conversion

“Red” photons are always born in pairs

Photon detection in one emission channel

$\rightarrow$ there must be a photon in the other channel as well

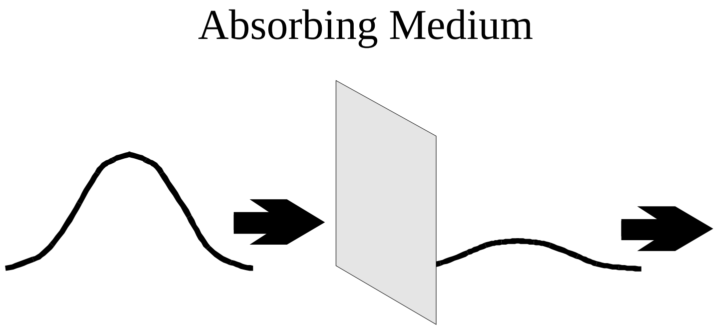


Not a single-photon “on demand”

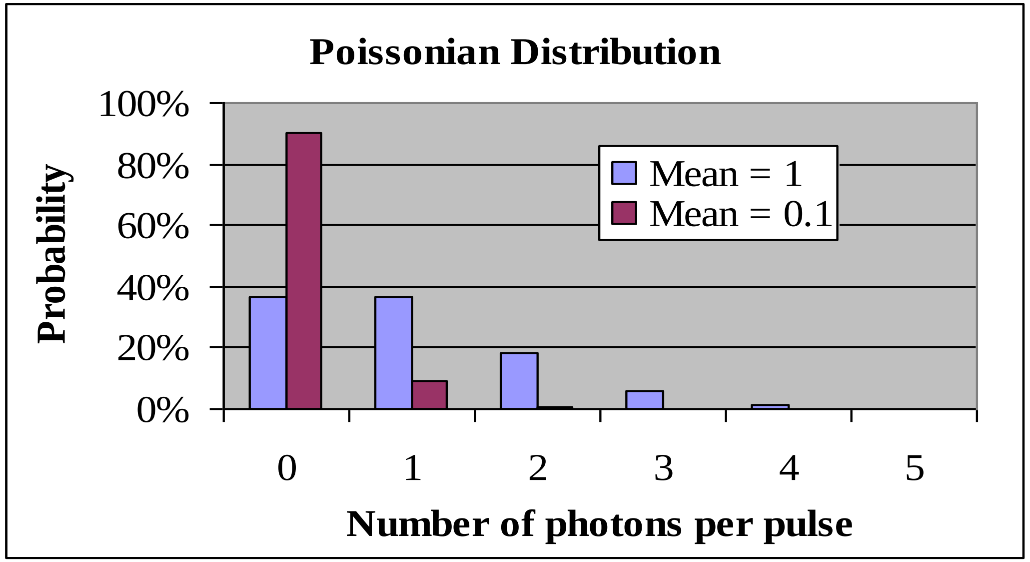
To date, this is the only method which provides a single photon with a high efficiency in a certain spatiotemporal mode

Other ways to find single-photons

Attenuated laser pulses



$$"|0\rangle \text{ or } |1\rangle \text{ or } |2\rangle \text{ or...}" \text{ rather than } |1\rangle$$



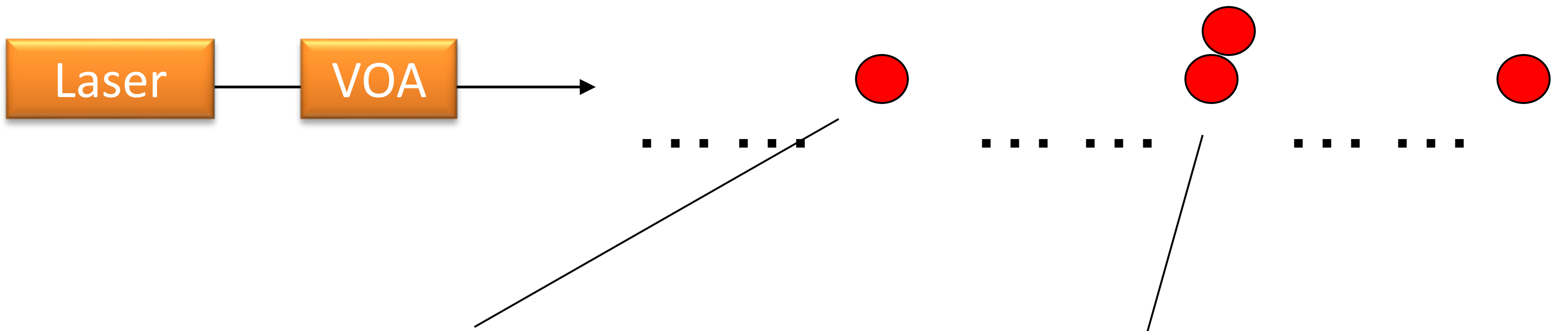
Calculate P(2)/P(1) for both sources with mean probability to generate photon P(1)=0,2.

QRATE QUANTUM COMMUNICATIONS

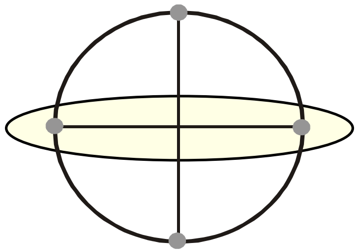
РКЦ Российский Квантовый Центр

Photon Number Splitting Attack – Lossless Channel

Eve takes advantage of statistical distribution of photon number in a pulse



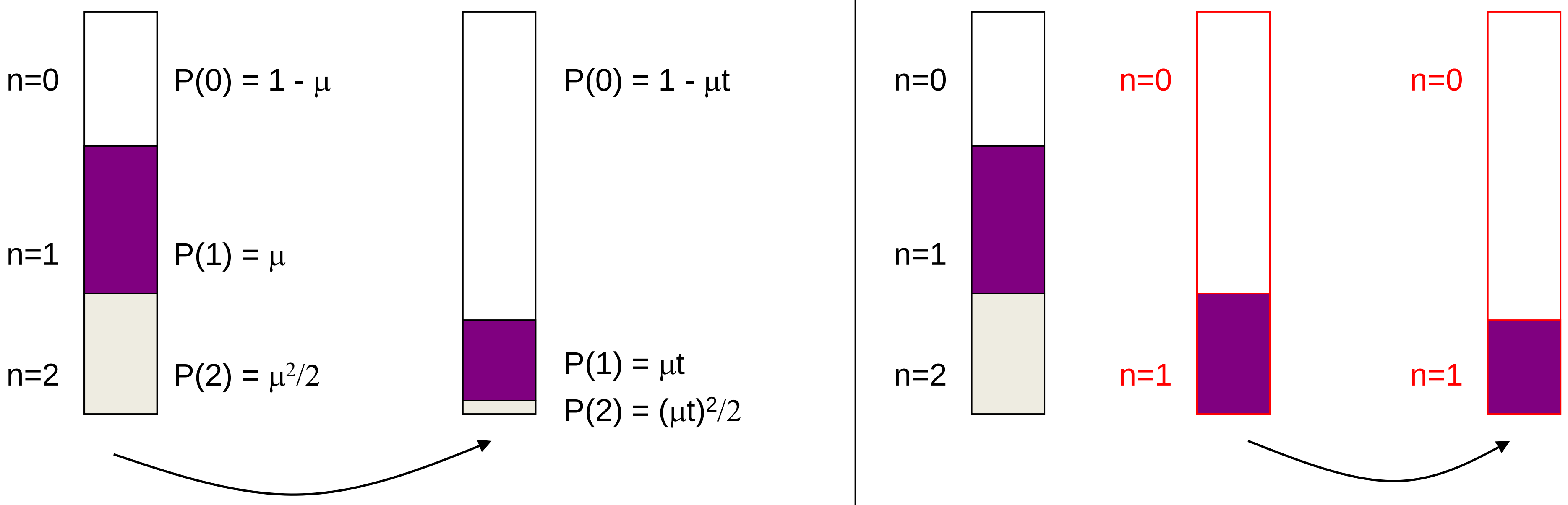
n=1: Nothing



n=2: Stores one photon in quantum memory
Let the other pass through
Wait until sifting

Photon Number Splitting Attack – Lossy Channel

Without Eve / With Eve



Transmission t

$P_{det} \approx \mu t \eta$

Transmission τ

$P_{det} \approx \tau\eta$

And $\tau = 2t/\mu$

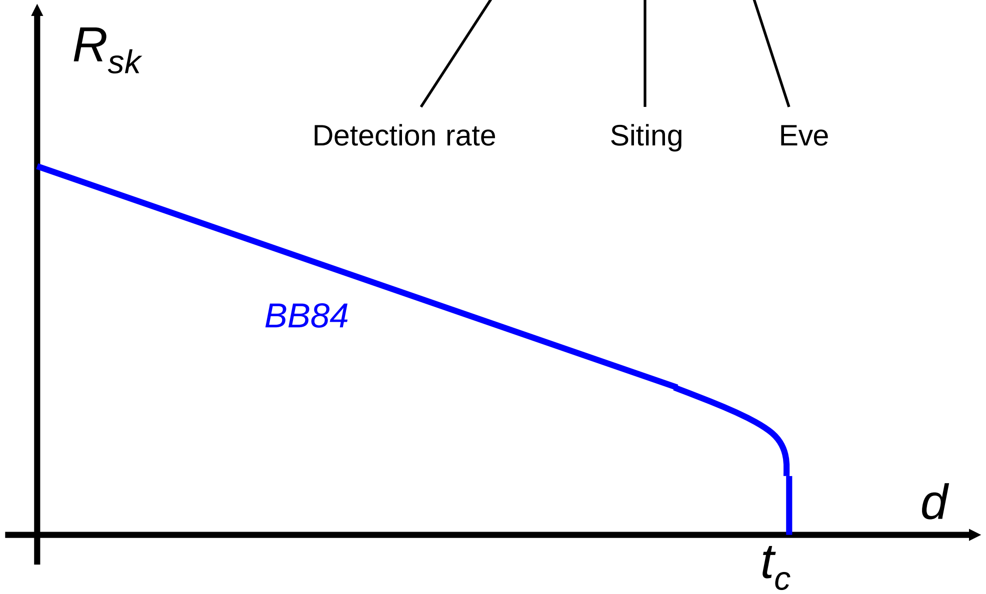
$P(2) = \mu^2/2 > \mu t$: 100% Information

Optimization of average photon number – BB84

Countermeasure to « PNS » attack

Optimization of the average number of photons per pulse μ

$\mu_{opt} = t$ $\qquad R_{sk} = \mu\, t\, \eta / 2 / 2 = \eta\, t^2 / 4$ $\qquad t_c = Sqrt(2 \ln 2 \times p_{dark} / \eta)$



Remarks: Bob must…

- check that rate is unchanged
- check that double clicks in incompatible basis are negligeable

Attenuation α = 0.25 [dB/km]

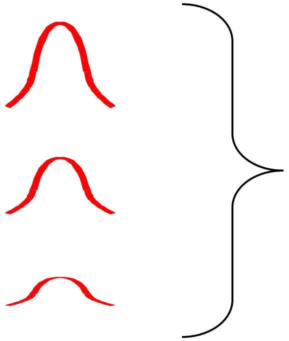
$p_{dark} = 10^{-6}$

η = 10%

→ t_c = 97 km

Decoy state QKD

Alice



Hwang

Alice uses sources of different amplitudes for the encoding.

Bob

1) Alice randomly sends either a signal state or decoy (usually weaker) state to Bob.

2) Bob acknowledges receipt of signals.

3) Alice publicly announces which are signal states and which are decoy states.

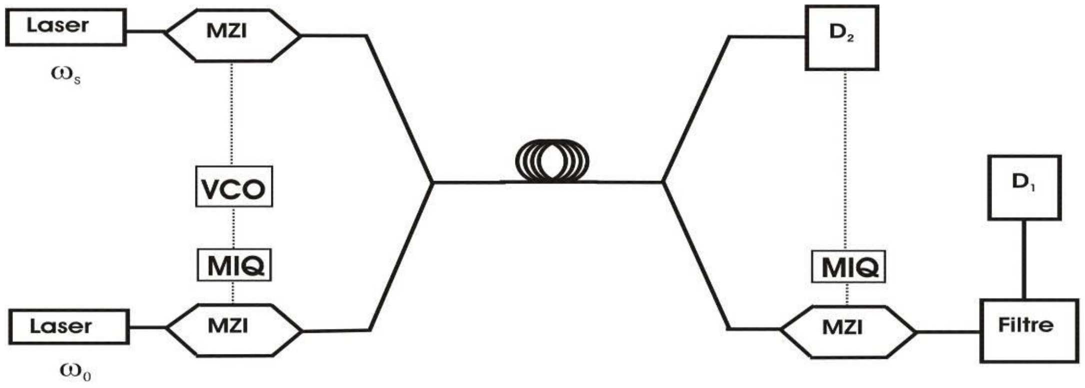
4) Alice and Bob compute the transmission probability for the signal states and for the decoy states respectively.

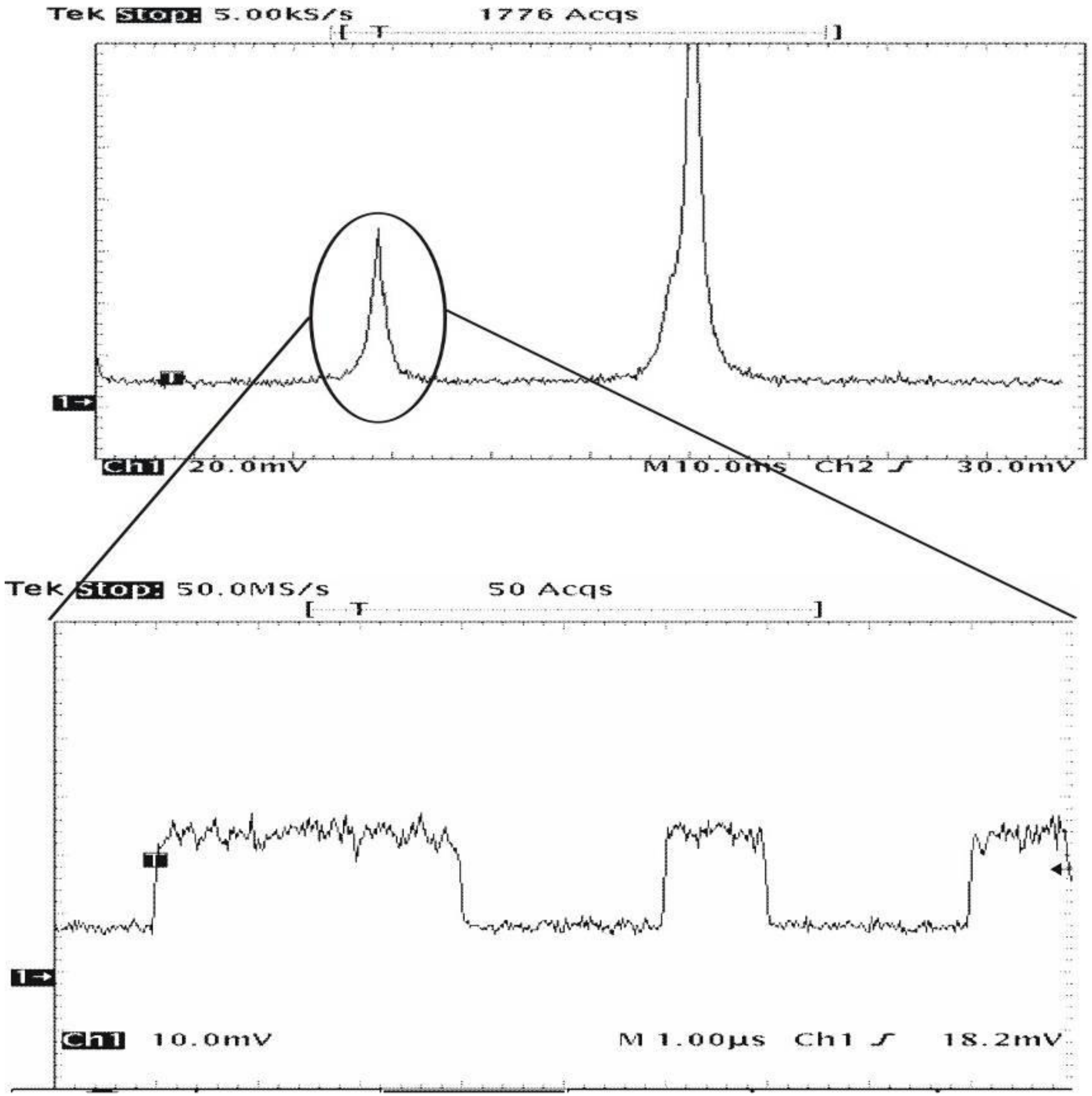
If Eve selectively transmits two-photons, an abnormally low fraction of the decoy state will be received by Bob. Eve will be caught.

Decoy-state QKD can be as robust as implementations using ideal single-photon sources.

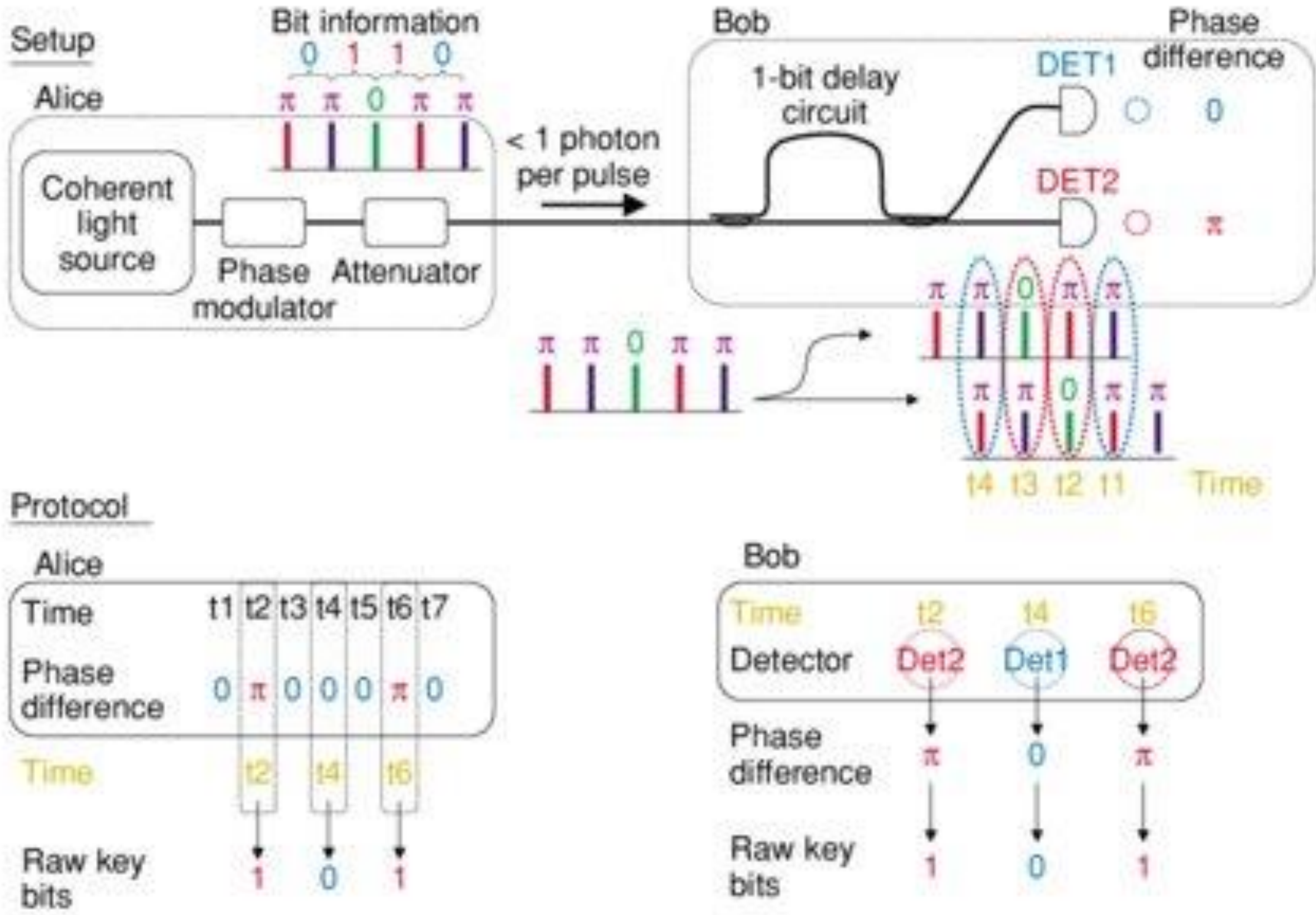
Strong reference

- One can measure interference between quantum signal and small fraction from the strong reference signal.
- Quantum signal block will cause the bit error because of strong signal fraction.
- It is important to control precisely the reference signal amplitude!
- Security proofs in progress.





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.]

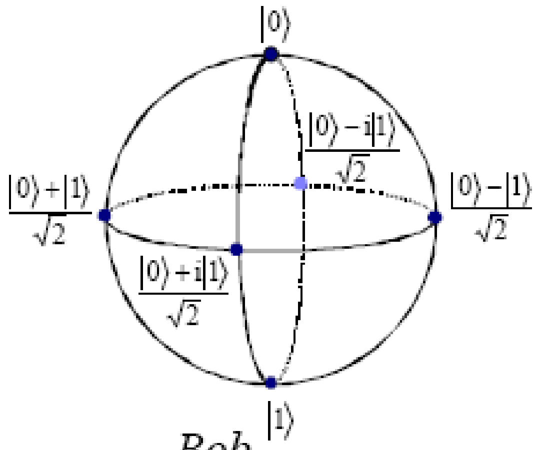
QUANTUM COMMUNICATIONS

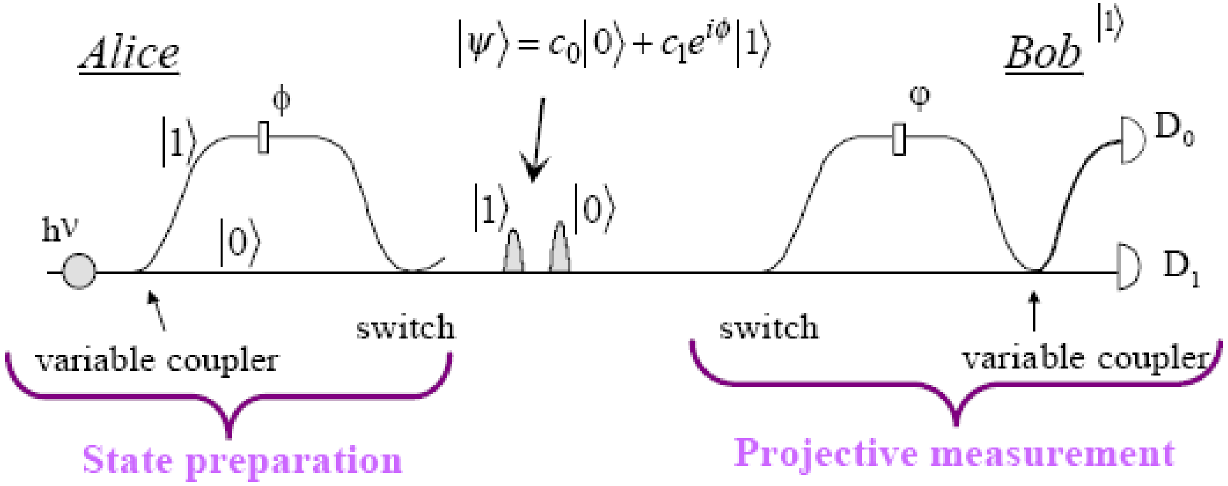
Российский Квантовый Центр

How to prepare states: Phase encoding

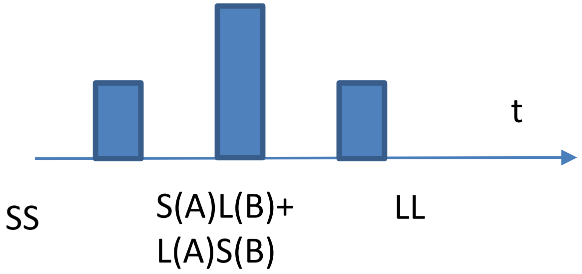
- qubit : $|\psi\rangle = c_0|0\rangle + c_1 e^{i\phi}|1\rangle$

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

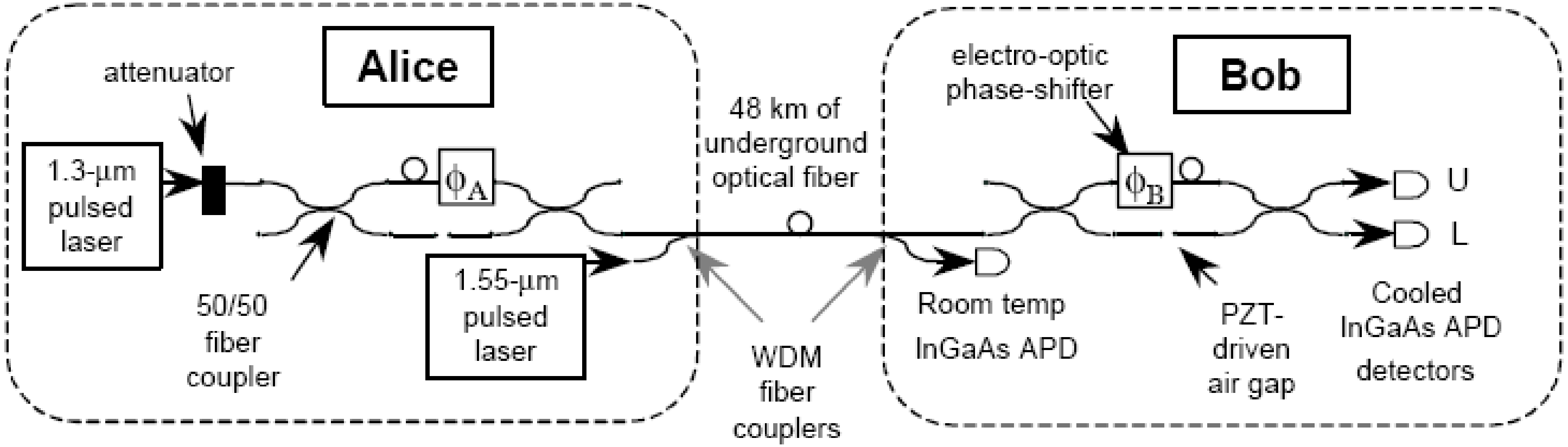




[C. H. Bennett, Phys. Rev. Lett. 68, 3121 (1992)]



Practical realization

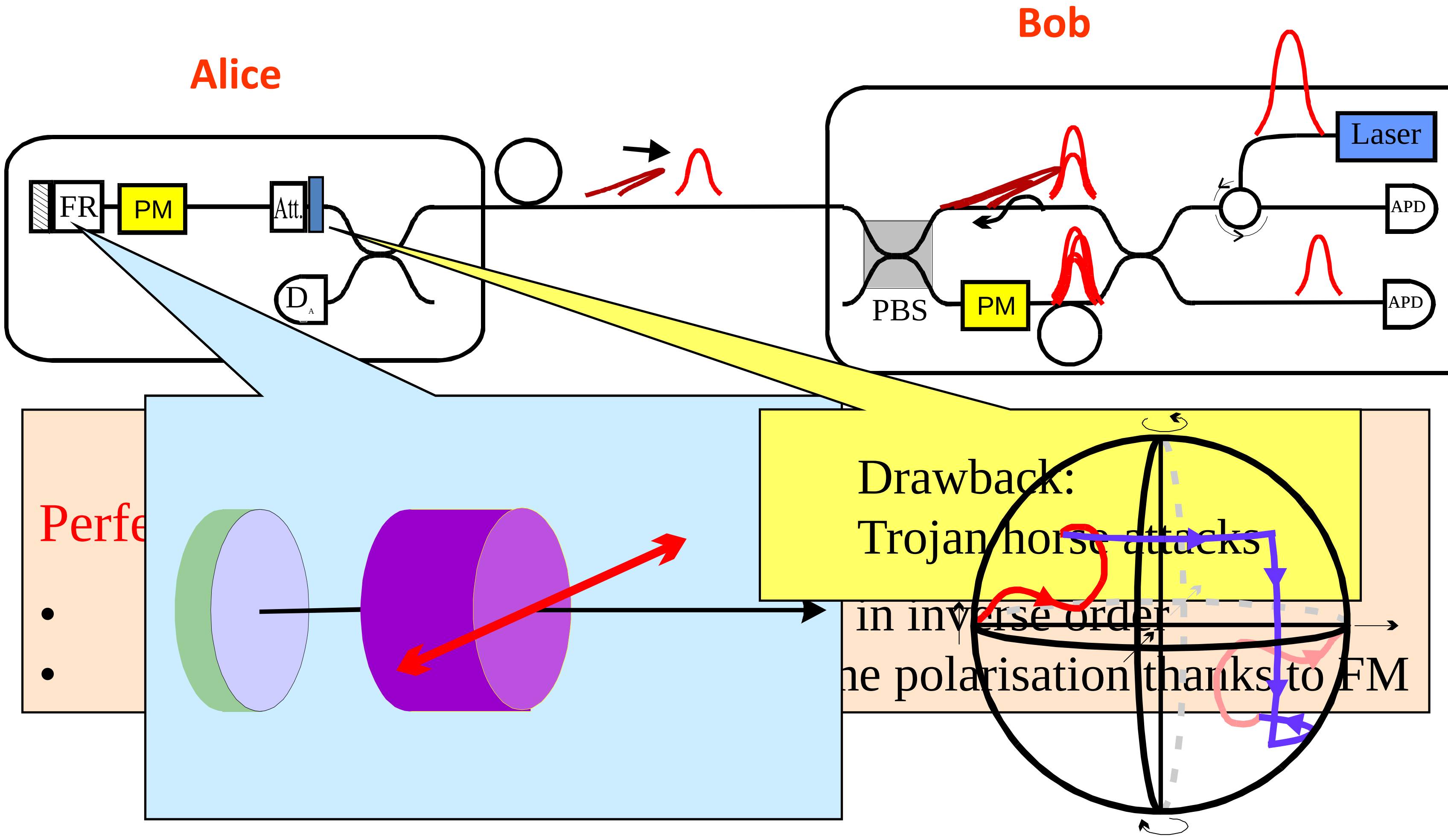


As the two coherent contributions are separated by a few nanoseconds but propagating along the same fiber, the are essentially no temperature or stress induced fluctuation.

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

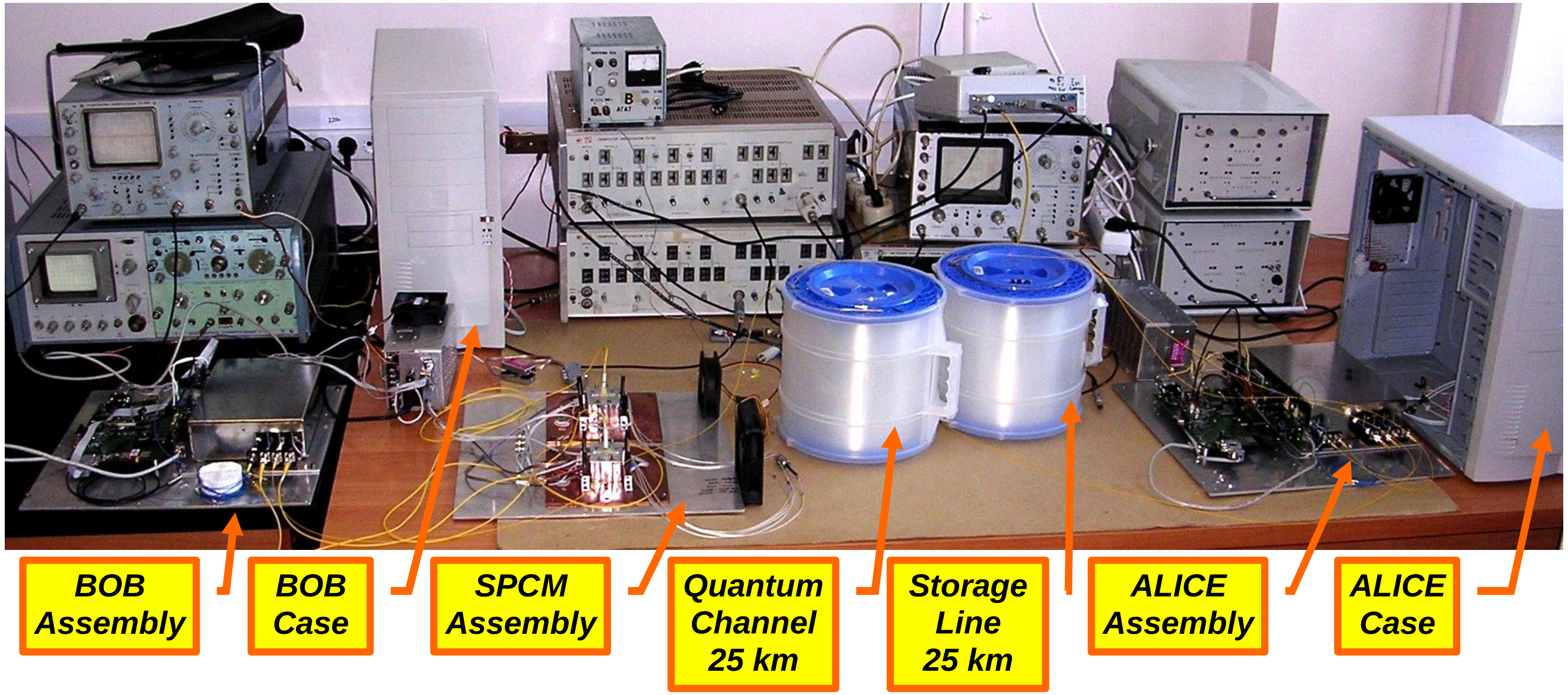
Plug & Play

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



First commercial product by ID Quantique used this scheme

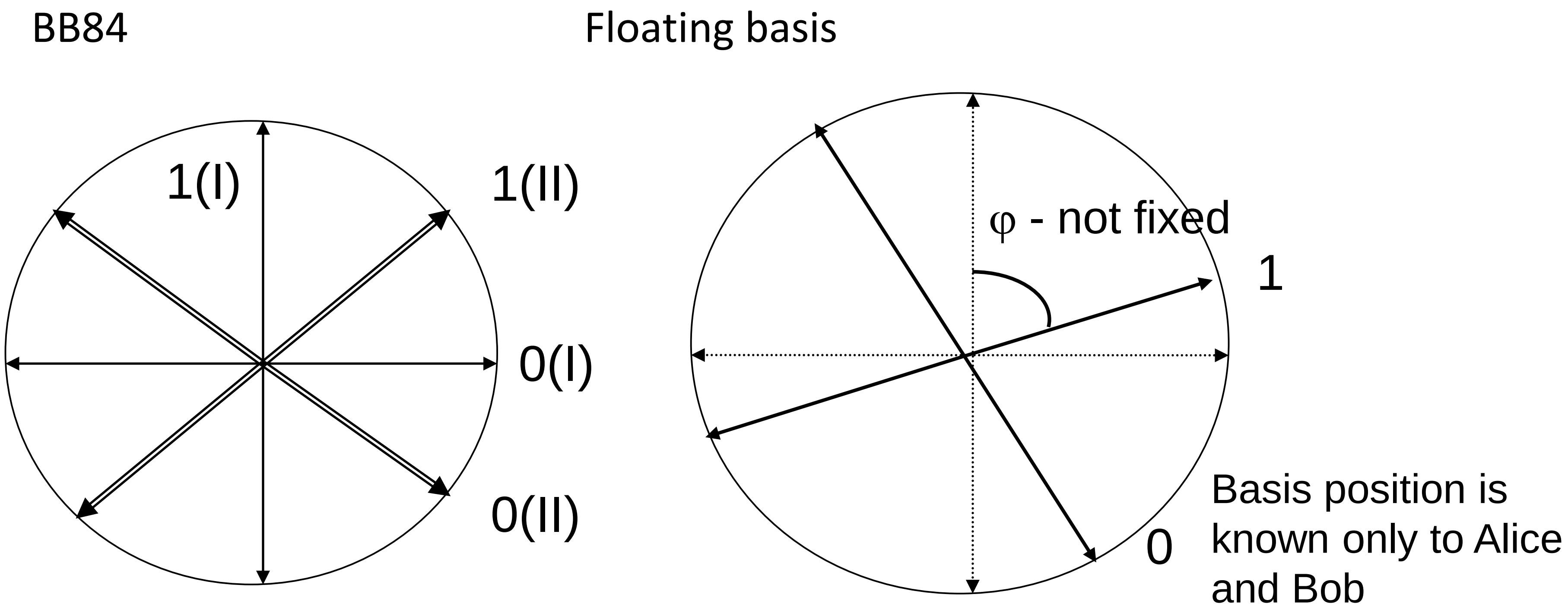
First in Russia fiber based quantum cryptography setup developed in ISP



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

Floating basis protocol

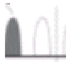
New quantum key distribution protocol which refuses from fixed basis. Absence of the fixed basis allows to make setup tolerant to detector blinding attack and increase key generation rate

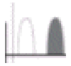


Basis shift also protects from the detector manipulation attack

Coherent one way protocol is inspired by classical communication

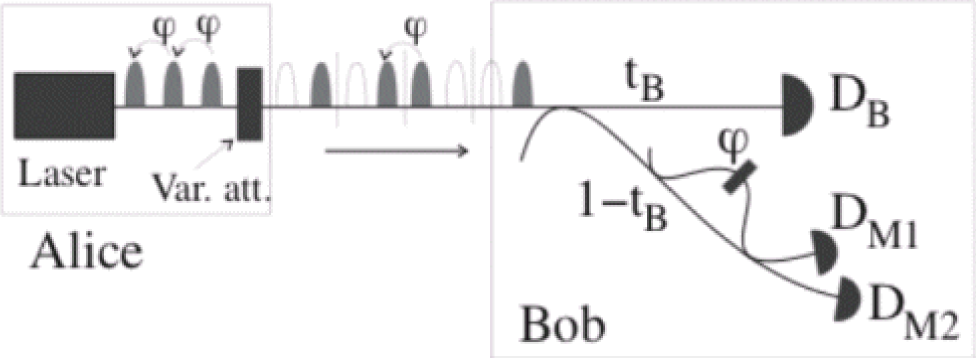
Coherent one way (COW) protocol (currently used by ID Quantique and University of Geneva)

Logical “0” 

Logical “1” 

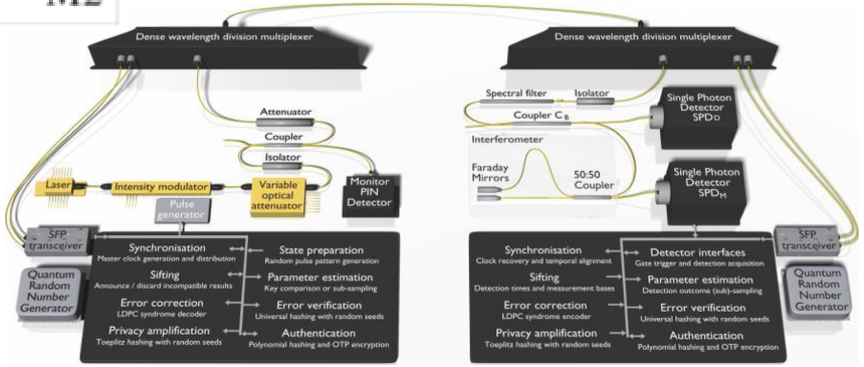
Decoy state  is used to monitor the attempt to unauthorized measurement

Unconditional proofs in process

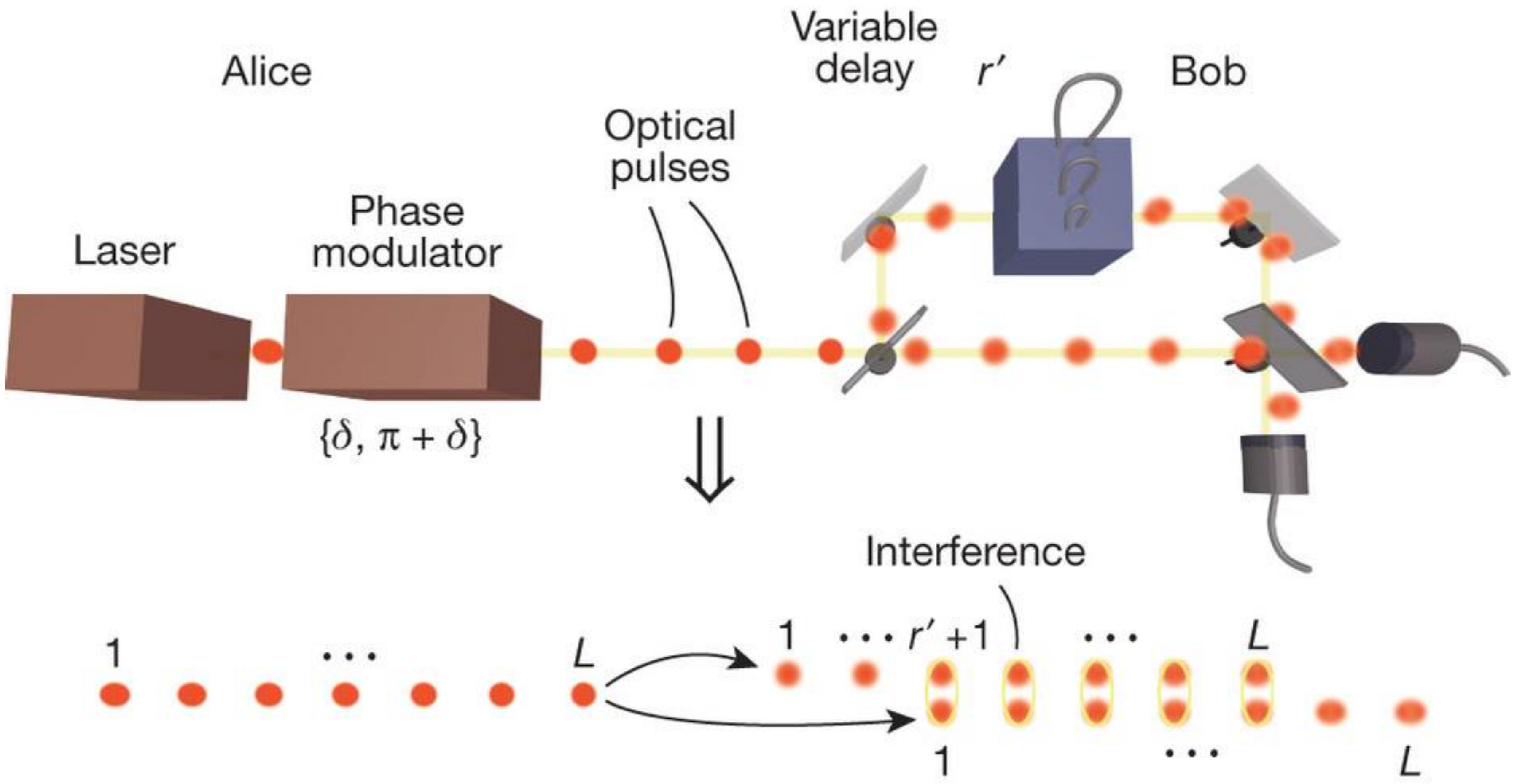


A fast and versatile QKD system with hardware key distillation and wavelength multiplexing

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]



Distributed-phase-reference QKD

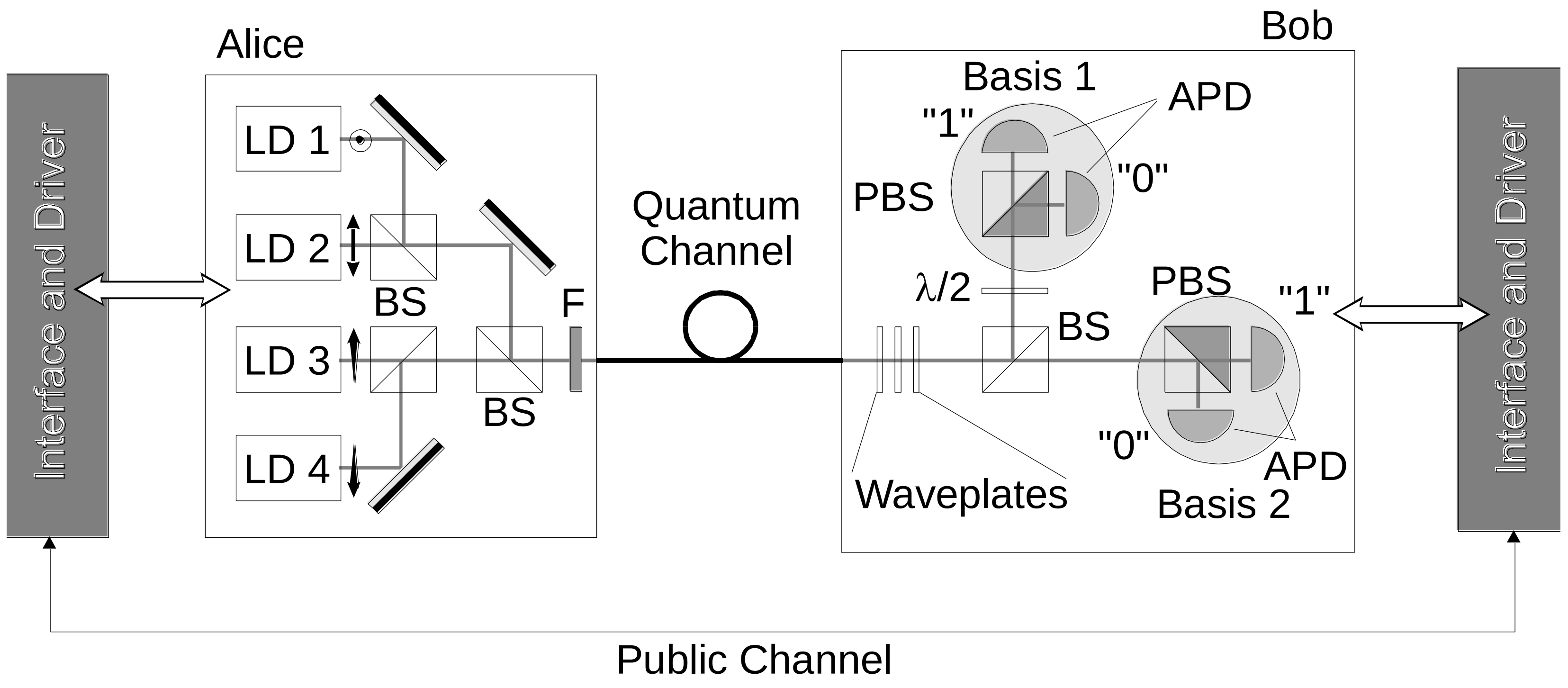


Interference between neighbor pulses will be broken in the case of the photon number splitting attack

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

How to realize: Polarization Coding

Typical system



QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

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

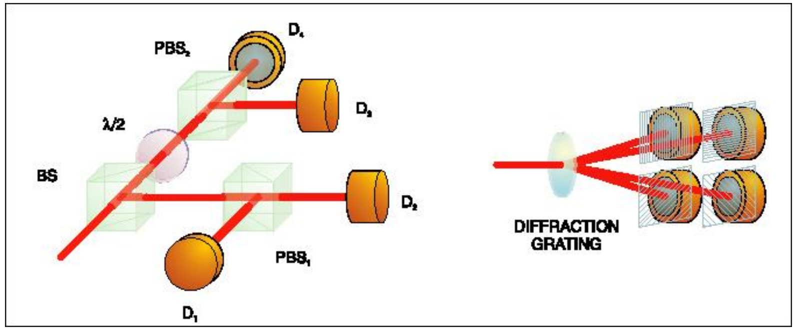
Low Cost and Compact Quantum Key Distribution

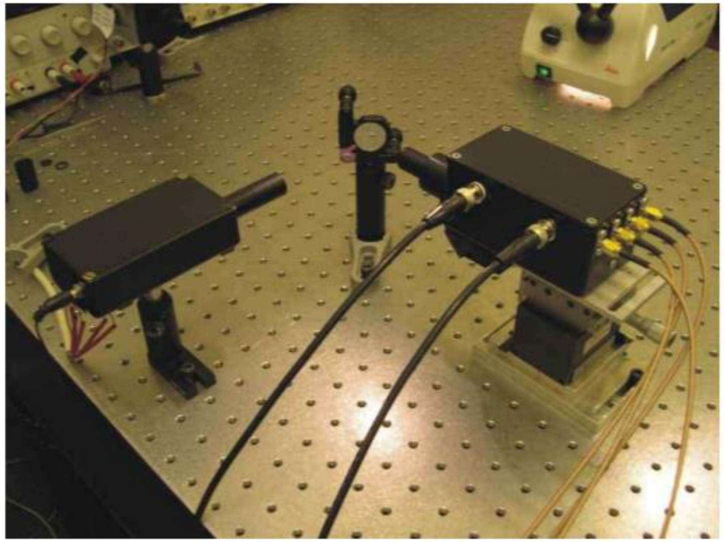
J L Duligall[1], M S Godfrey[1], K A Harrison[2], W J Munro[2] and J G Rarity[1]

[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

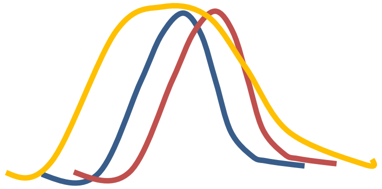
E-mail: joanna.duligall@bristol.ac.uk





Pulse difference is the issue:

- Wavelength
- Width
- Shape
- Time delay



Fiber polarization controllers operate at kHz frequency

QRATE QUANTUM COMMUNICATIONS

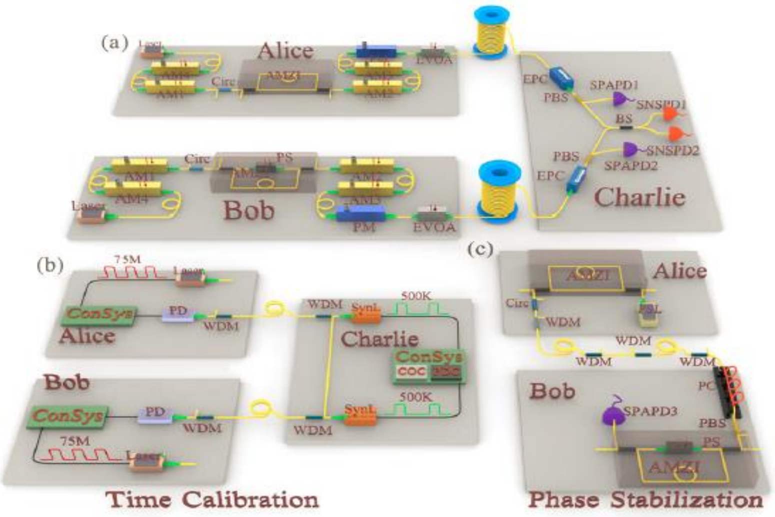
РКЦ Российский Квантовый Центр

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.

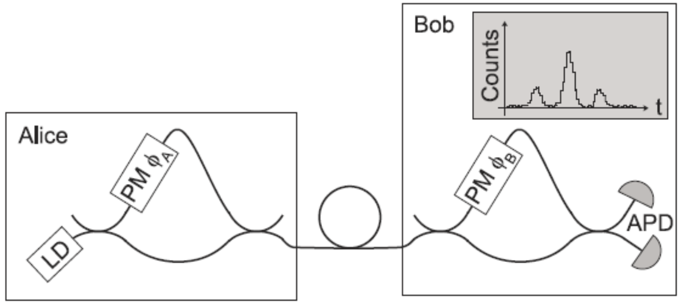
Number of optical schemes are polarization sensitive
MDI QKD:

> 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.



How to prepare four BB84 polarization states?

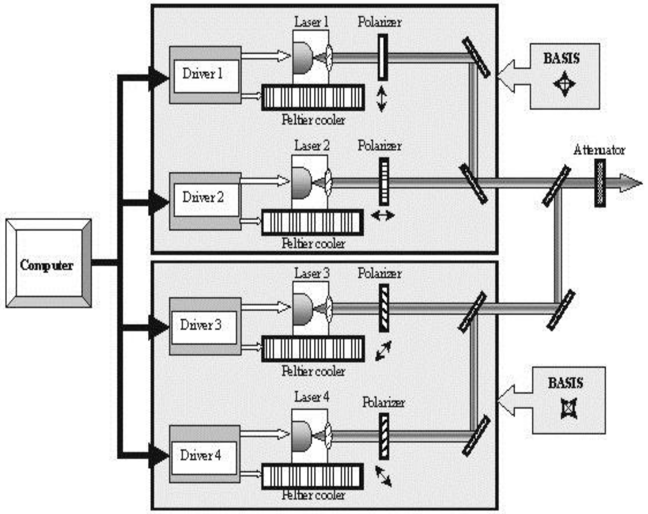
One can use 4 lasers
Fast and convenient
Inseparability problem

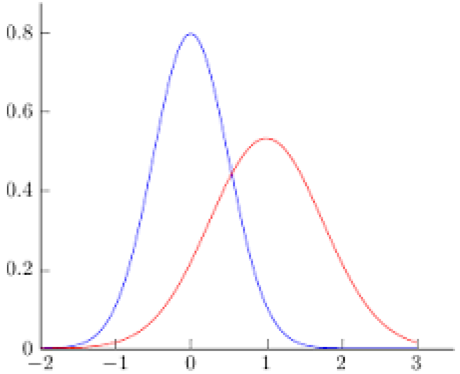
- Lasers can be different in frequency, time or direction

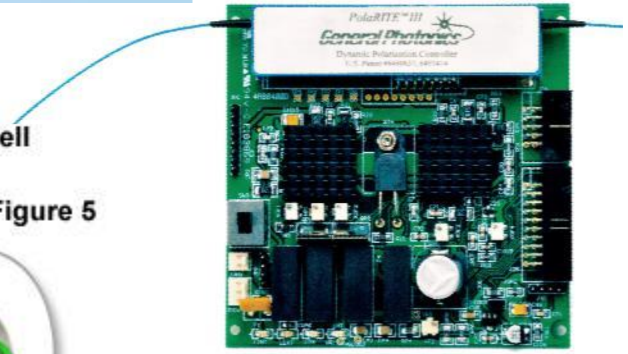
It is possible to construct full polarization controller from LiNbO3 crystals
Piezo driven polarization controllers are not fast enough for random state preparation

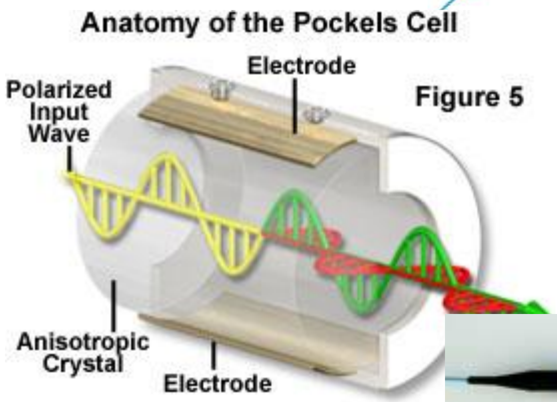
Pockels cell allows us to prepare four maximum nonorthogonal states

- 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

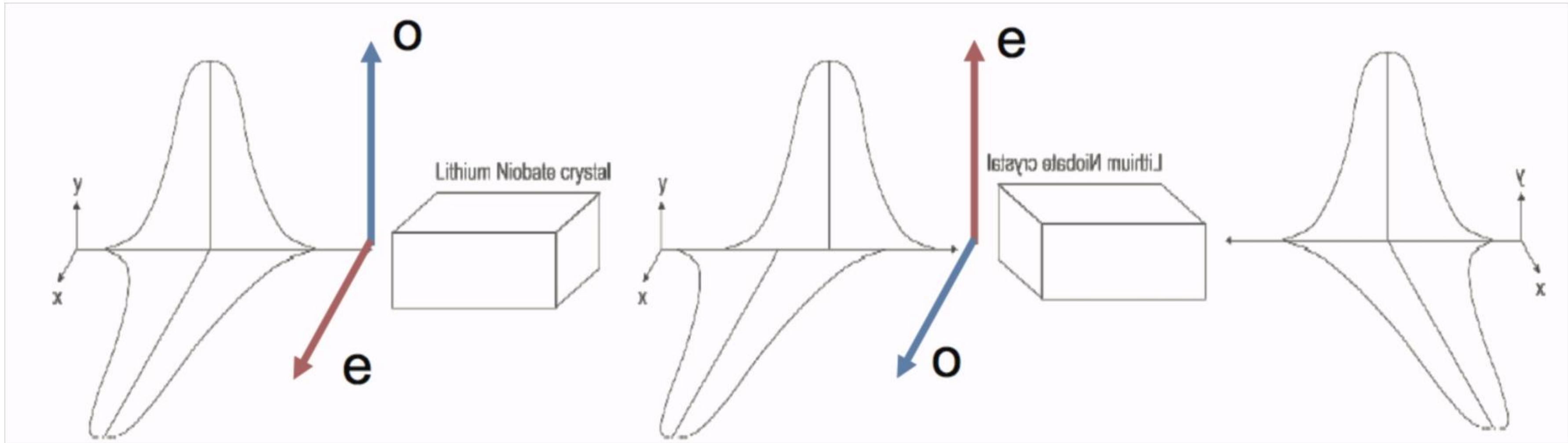
40 GHz

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).

QRATE QUANTUM COMMUNICATIONS

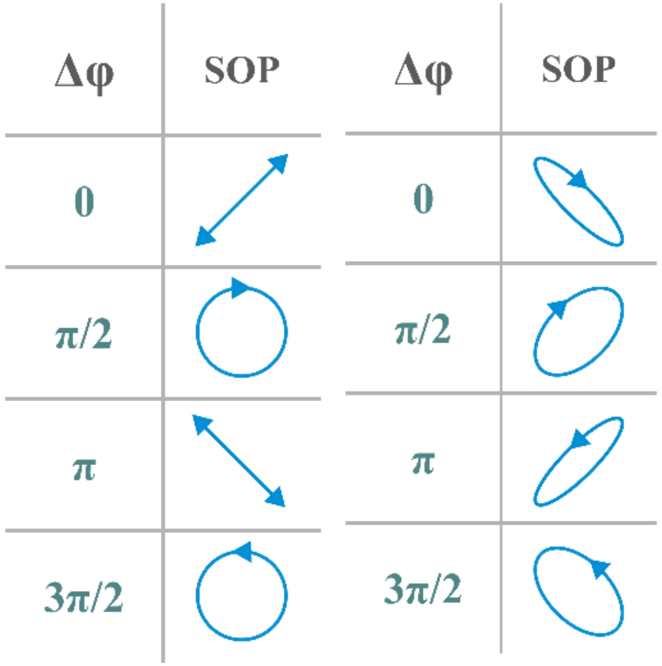
РКЦ Российский Квантовый Центр

States prepared by Pockels cell

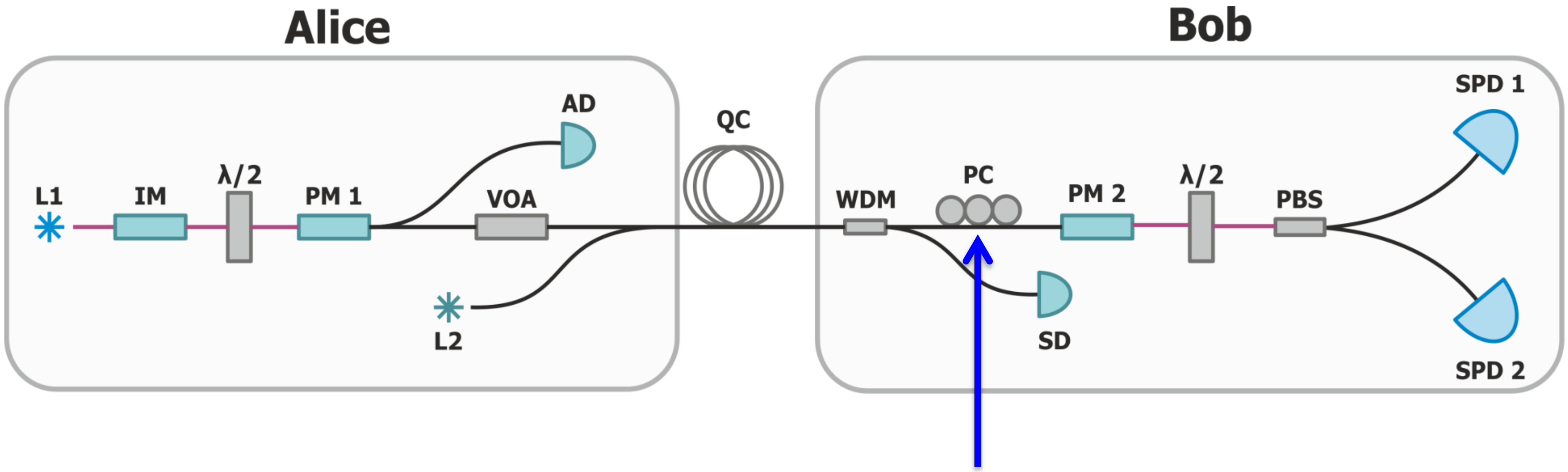
Polarization distortion induced by long quantum channel are compensated by polarization controller

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



Polarization tuning

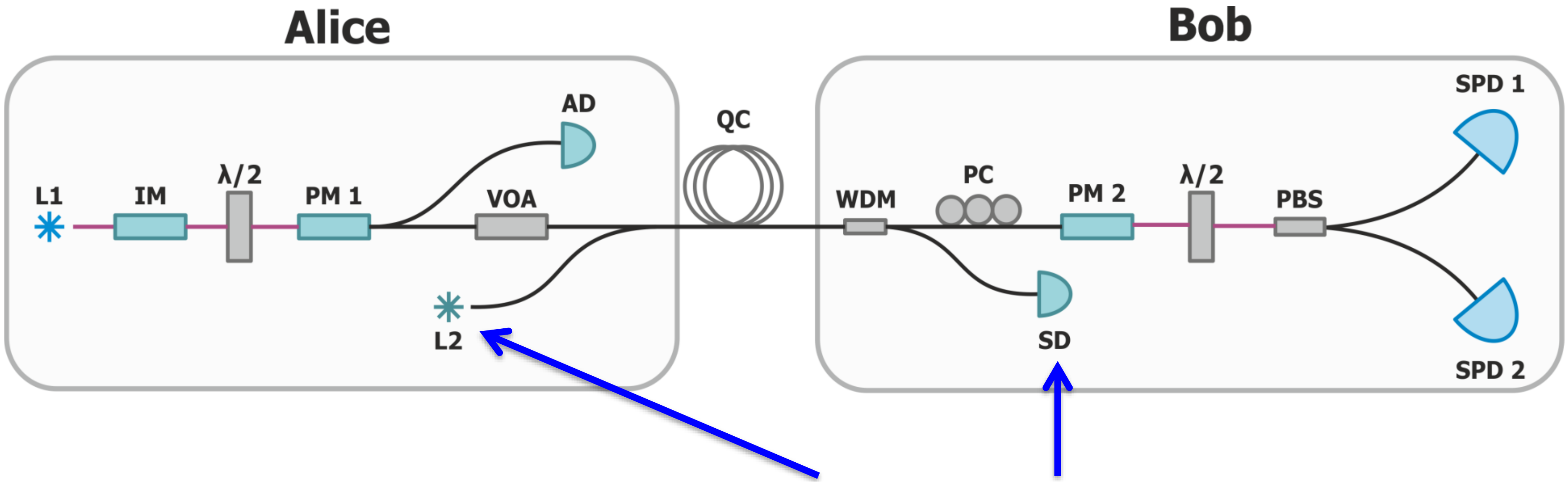


Polarization can be tuned with piezoelectric-polarization-controller
Alice and Bob can announce part of the key to monitor QBER (usually it is “decoy” state events)
If QBER exceeds threshold (for example 6%), Alice Increases Amplitude and sends predefined sequence to tune polarization controller
Bob 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

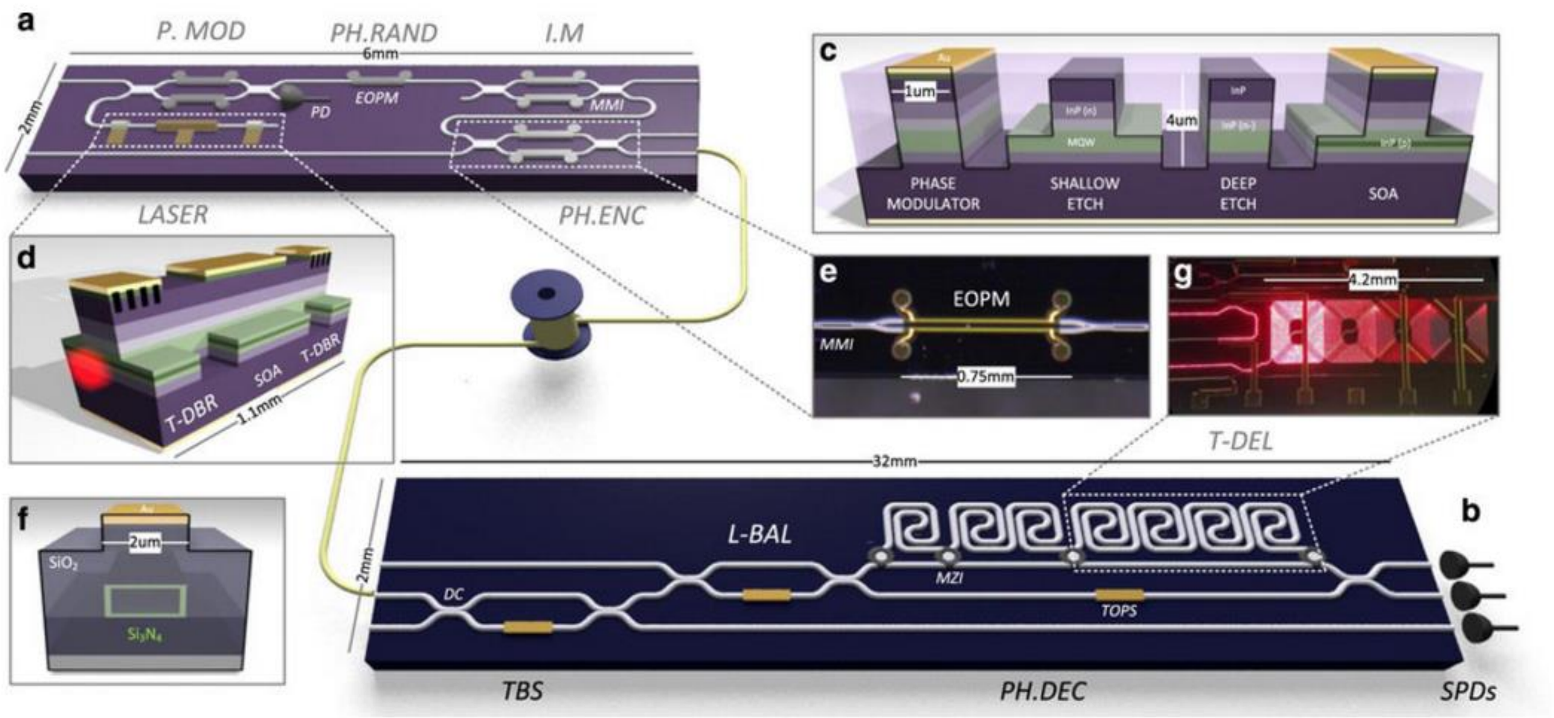


To synchronize clock we use additional laser and syncrodetector
To reduce the effect on single photon detectors we use wavelength and time division
To remain good detector synchronization we need to keep Alice and Bob clock difference below 100-150 ps.
We send trains of syncropulses about 800 times a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

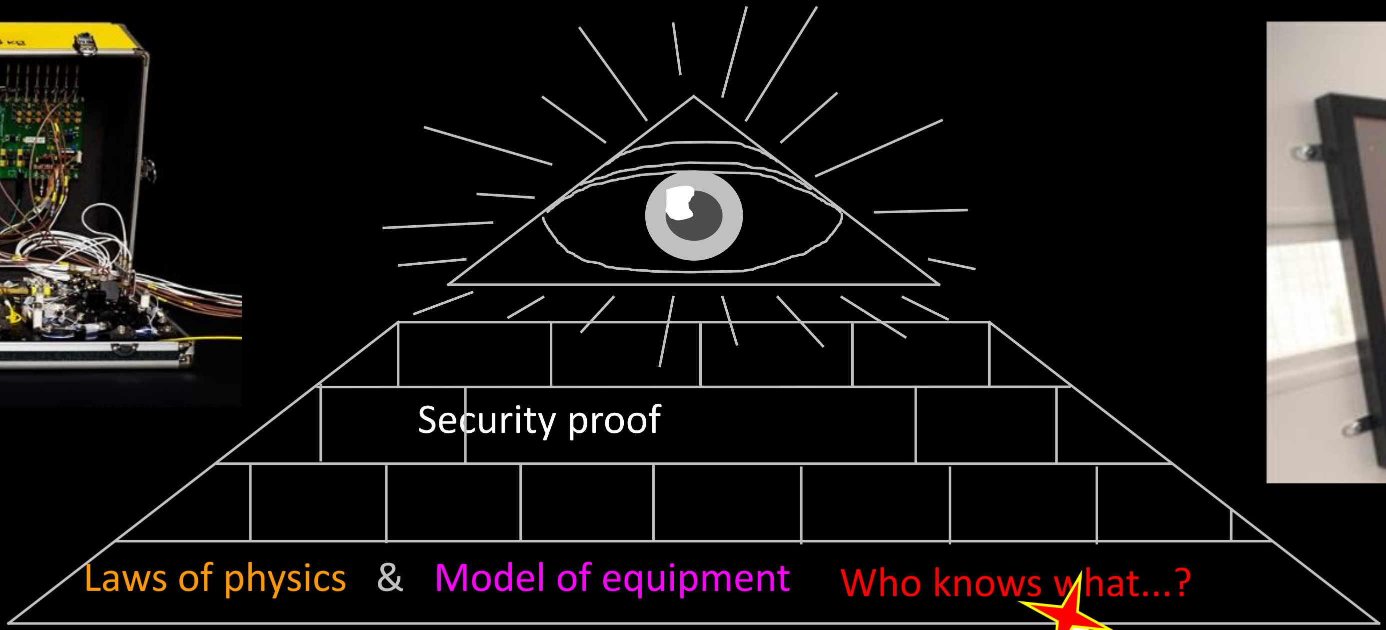
Photonic chips will dramatically change the QKD setup size

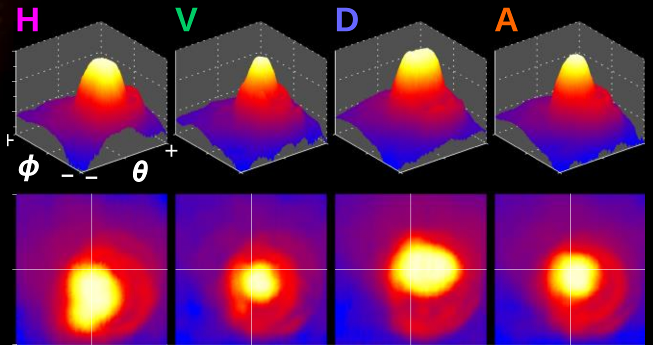
Using photonic chip all QKD optics can be made on centimeter size chip
The only problem is the current cost of such chip is 2-10 kEUR

From: Practical challenges in quantum key distribution



Limits on physical security

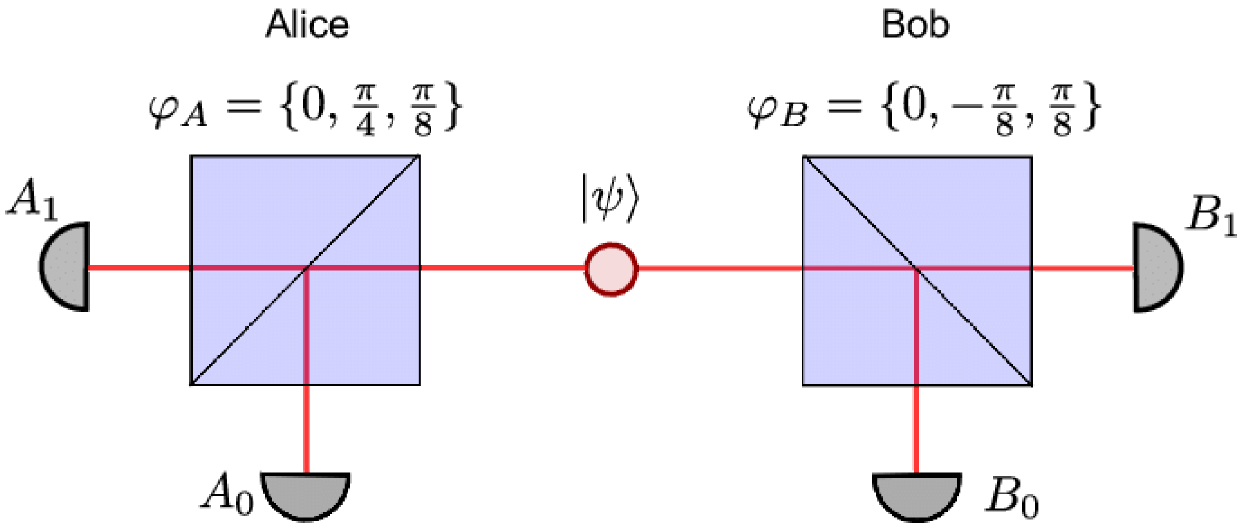




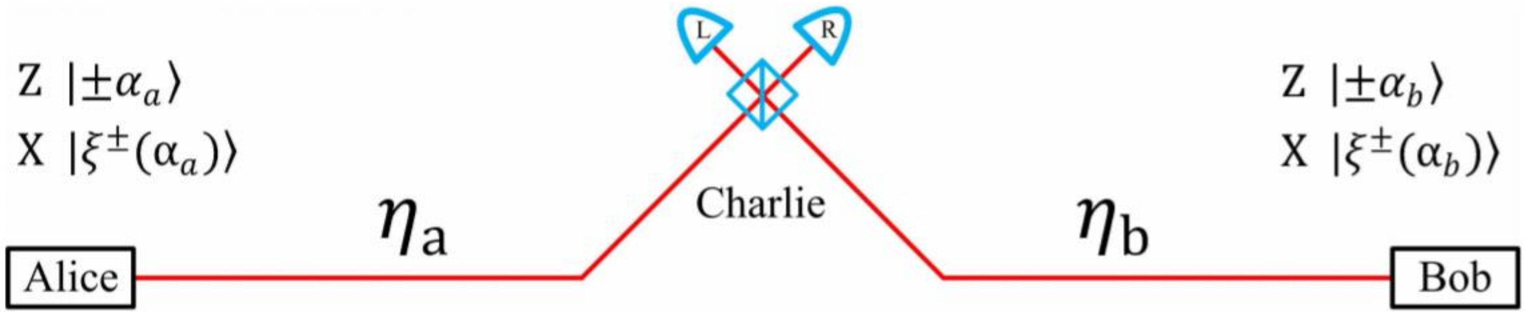
Physical access to equipment

Laser damage!

Time reverse helps to solve problem of detector blinding



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



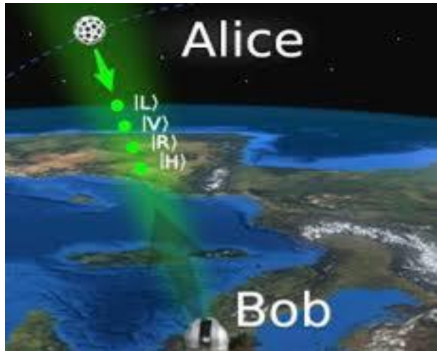
Measurement is replaced
by state preparation

Preparation by measurement

QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

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

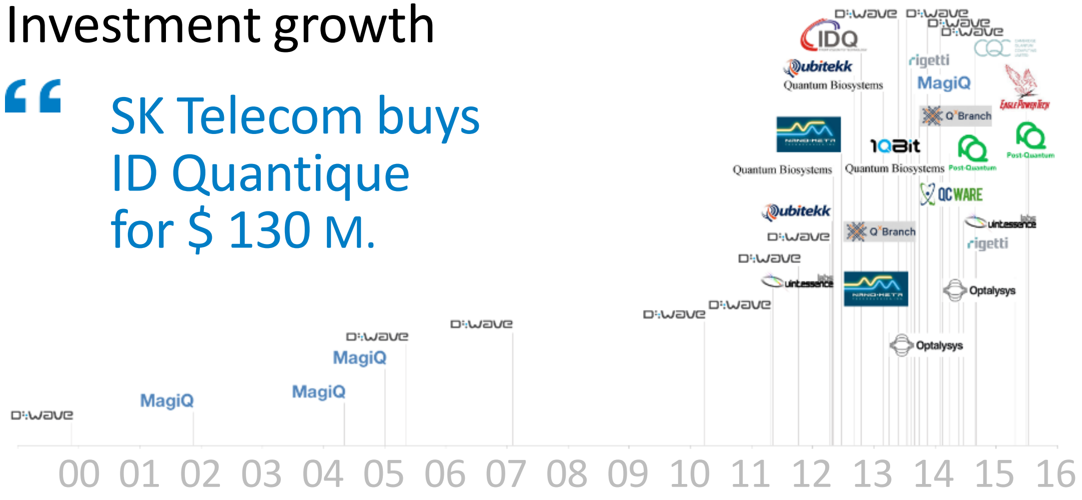
New market – new possibilities

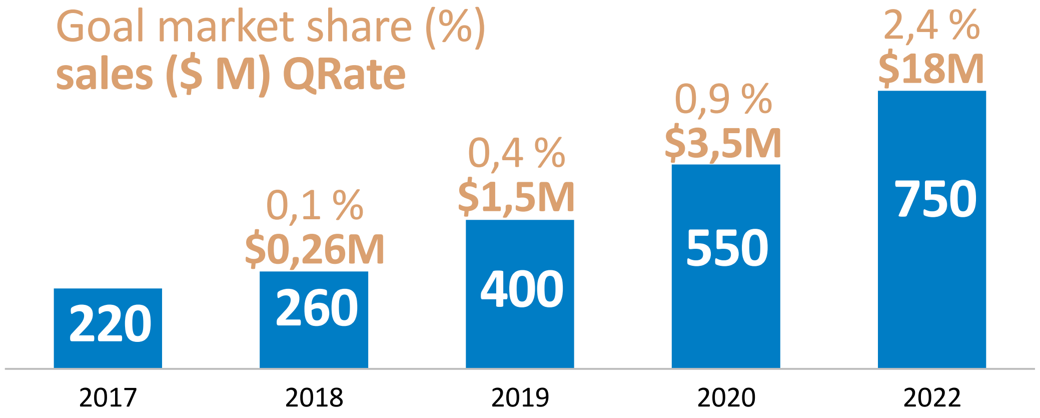
Today QKD market is the startup market

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.

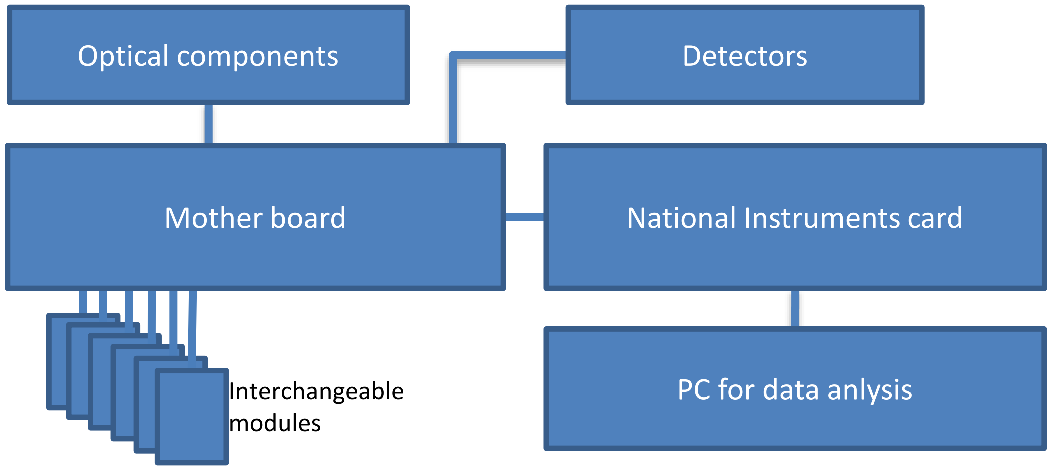




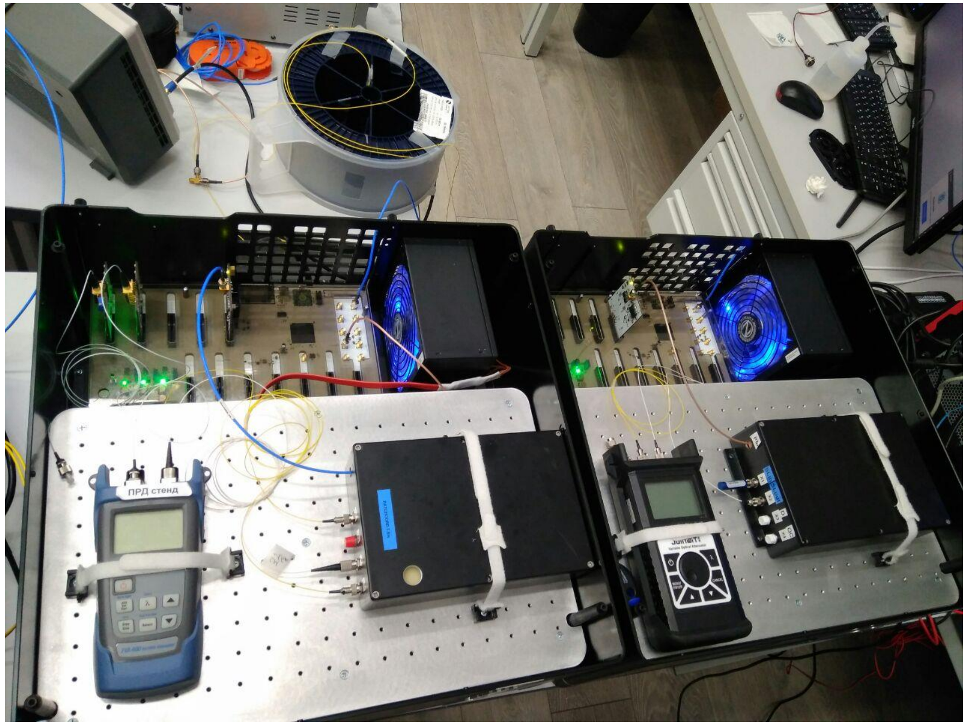
QKD market, $ M [1]

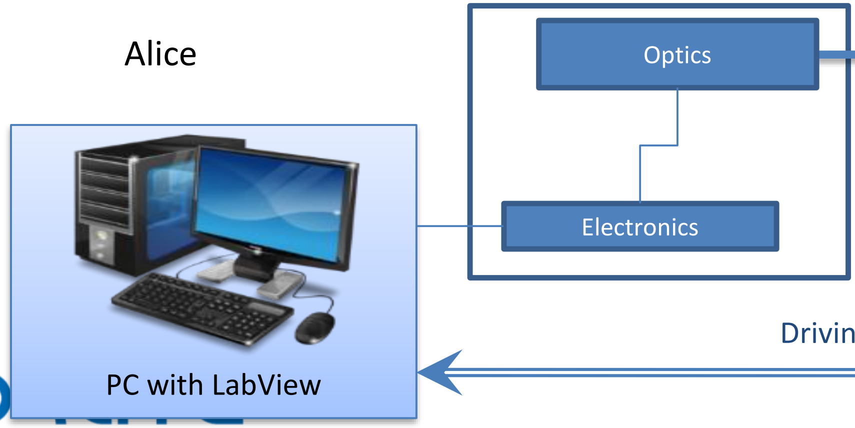
[1] **Markets&Markets**: Quantum cryptography market - 2017 to 2022

Fast prototyping with modular system is an opportunity for our group



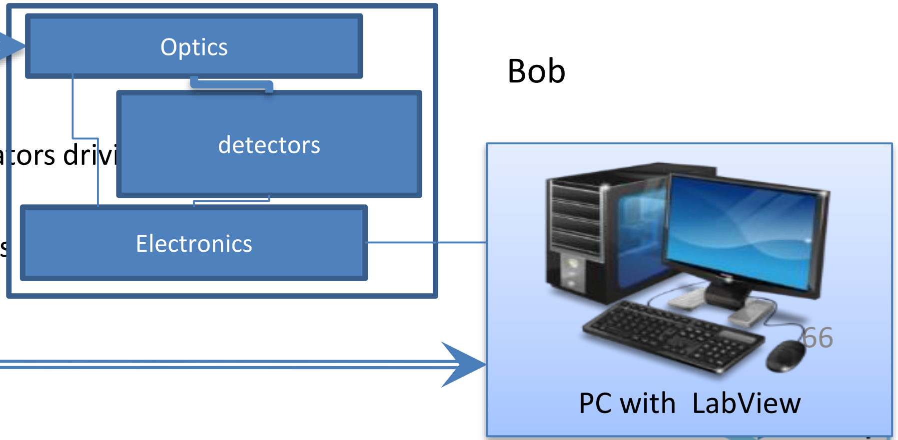
Modular system allows to change optical scheme, protocols and number of driving elements without knowledge in electronics





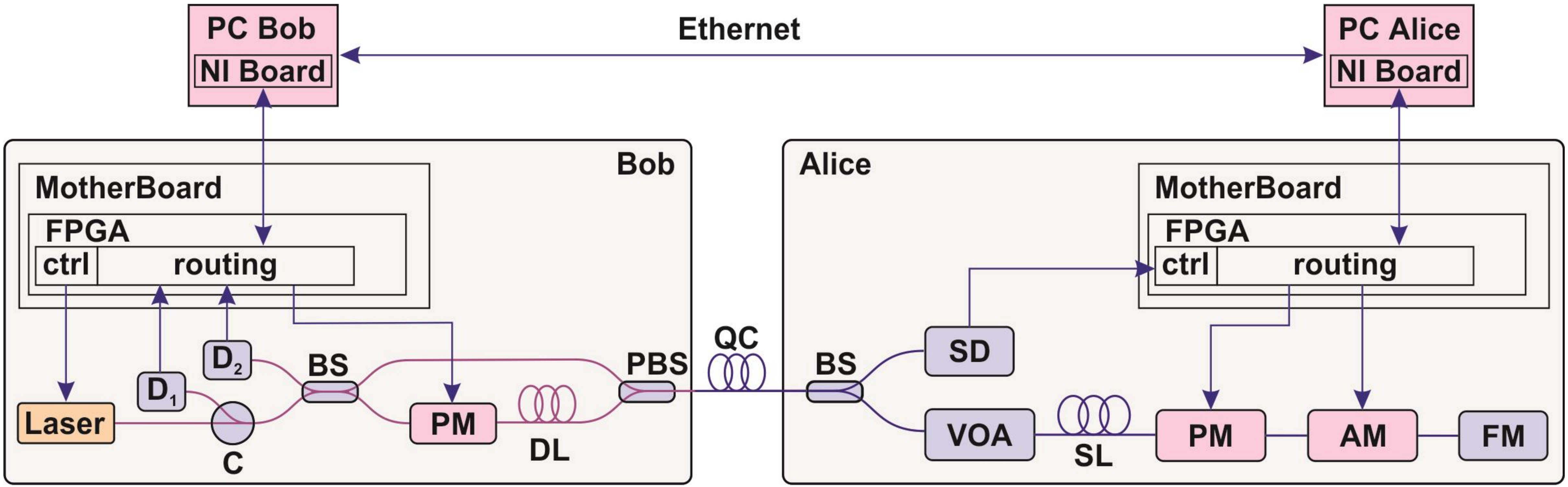
Motherboard can be equipped with:

- ✓ 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



Driving software can be modified by “student” preparation level

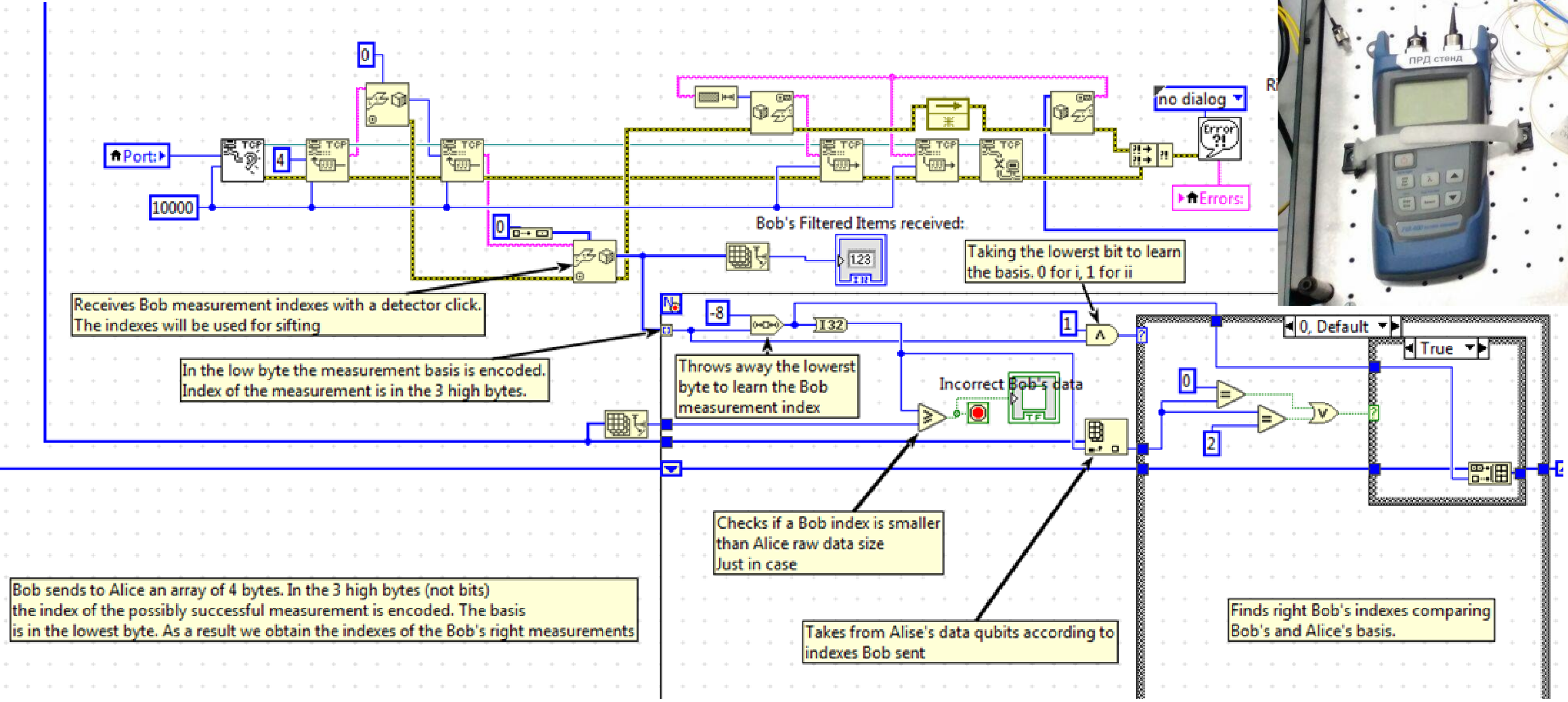
Plug&play QKD alignment is the basic task

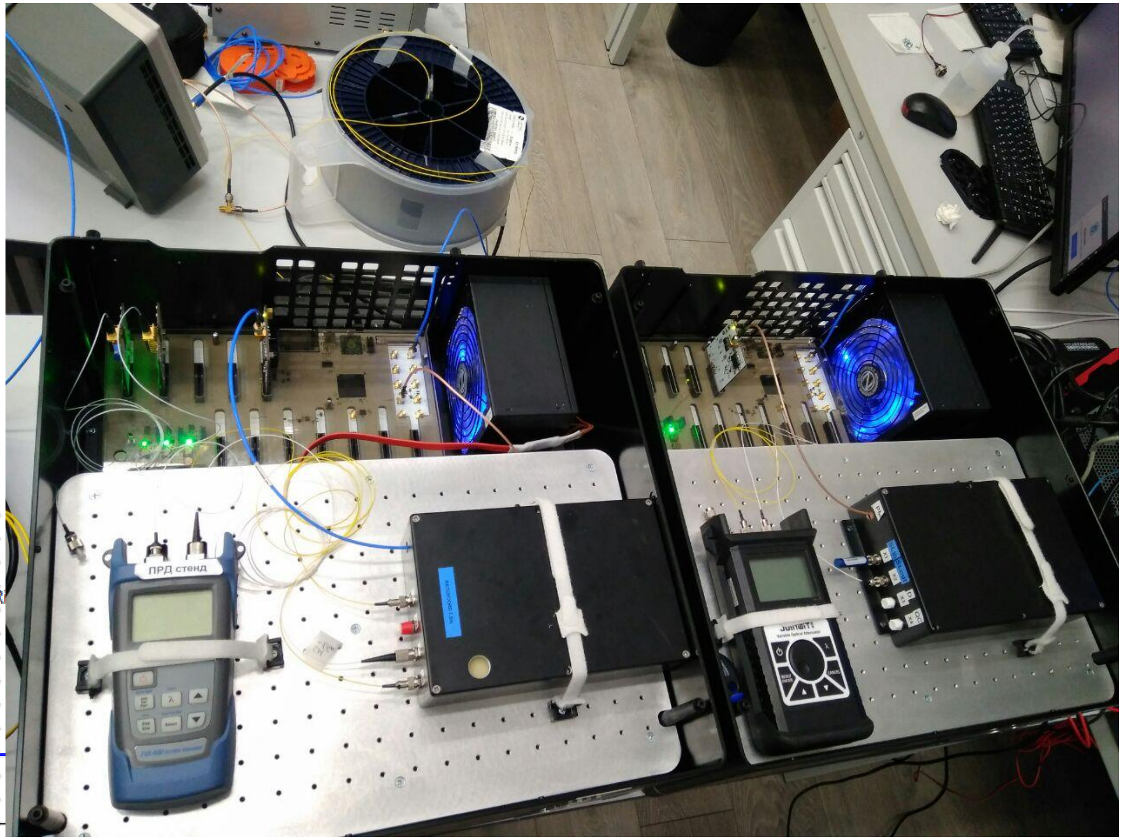


RQC’s solution for introducing quantum physics

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

QRATE

Quantum transmitter → Quantum receiver

Typical QKD equipment distributes 1-1000 kbit/s

Office

Quantum key

Data center

Quantum key

Data encryption system ⟷ Data encryption system

VPN tunnel

Existing manufacturers: hardware and software encoders works at 1-100 Gbit/s

Data encryption systems can be created locally

World leaders are China and Europe

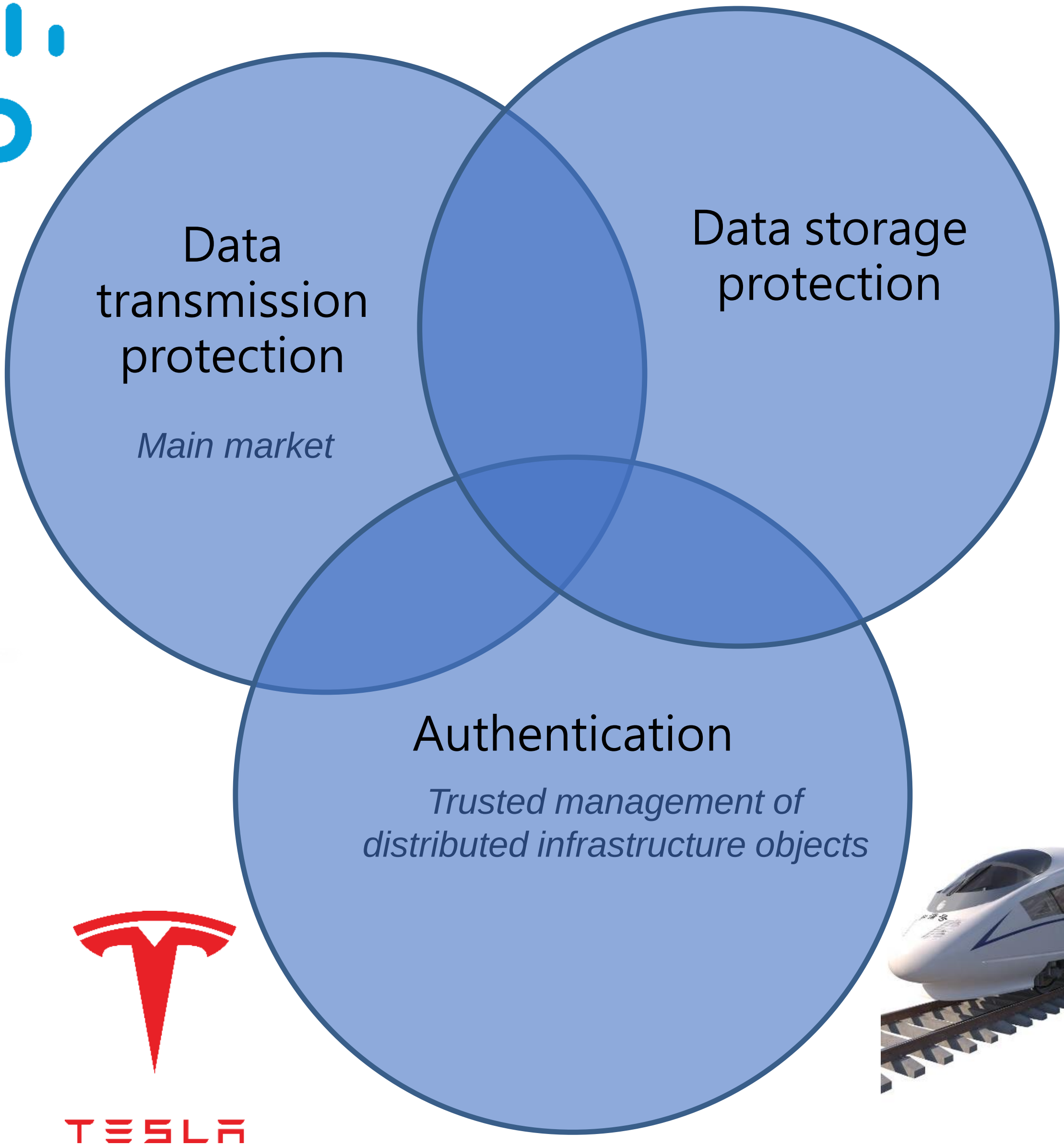
- First product announced in 2001
- Demonstrated successful exit in 2018 with SK telecom

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

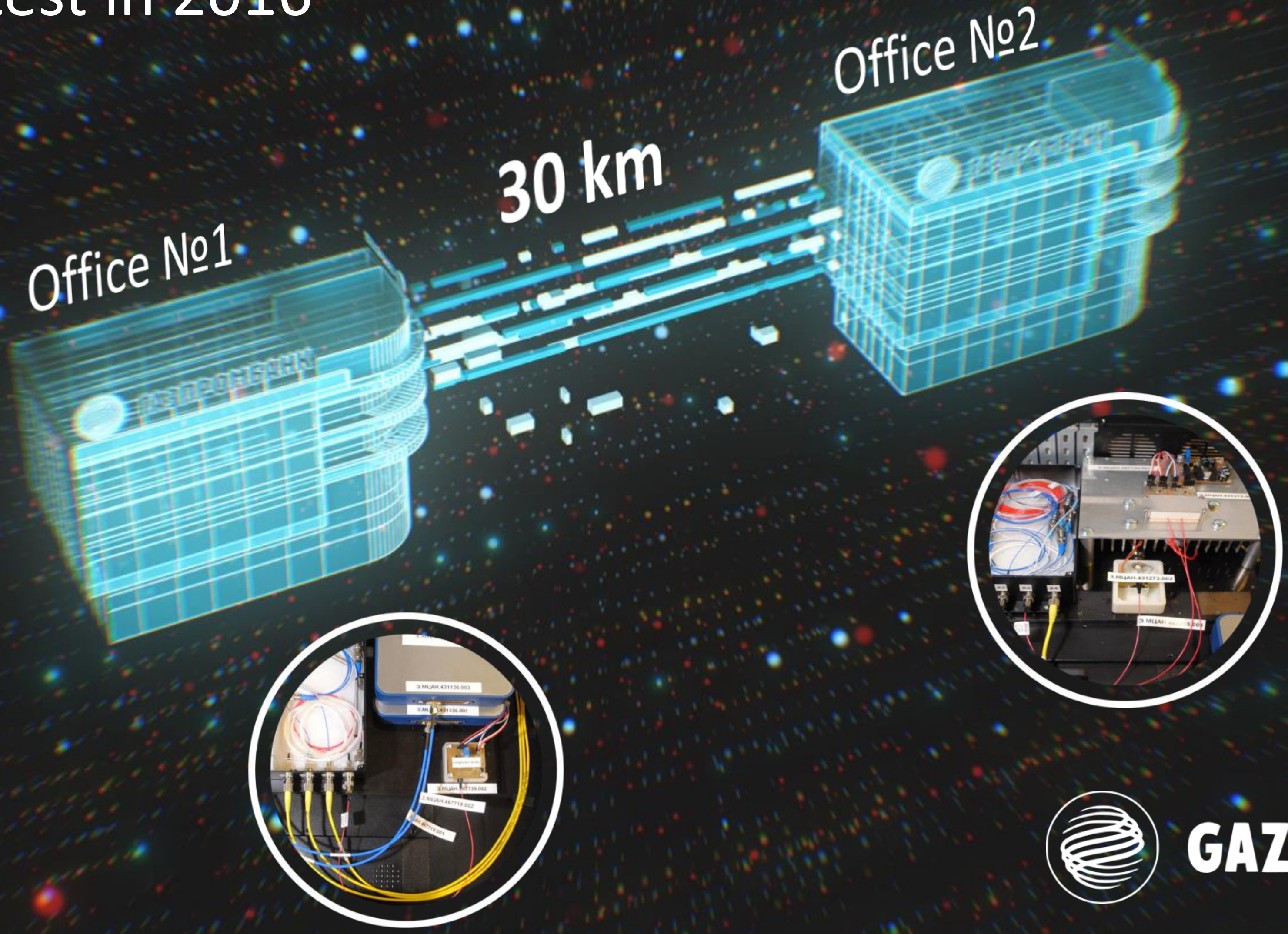
Secure now.
Secure in the future.

QRATE

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



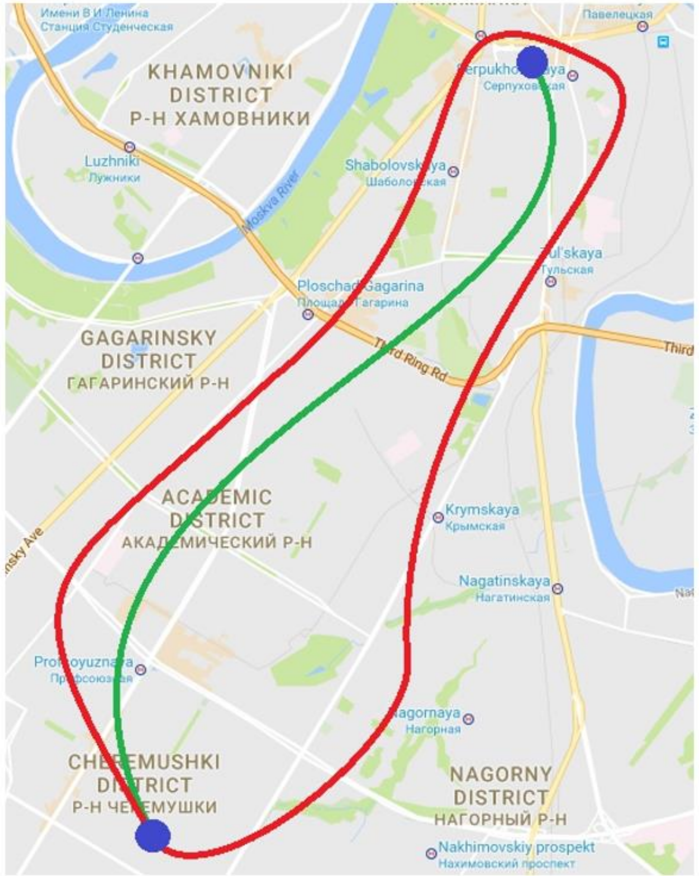
QKD field test in 2016



RQC RUSSIAN QUANTUM CENTER

GAZPROMBANK

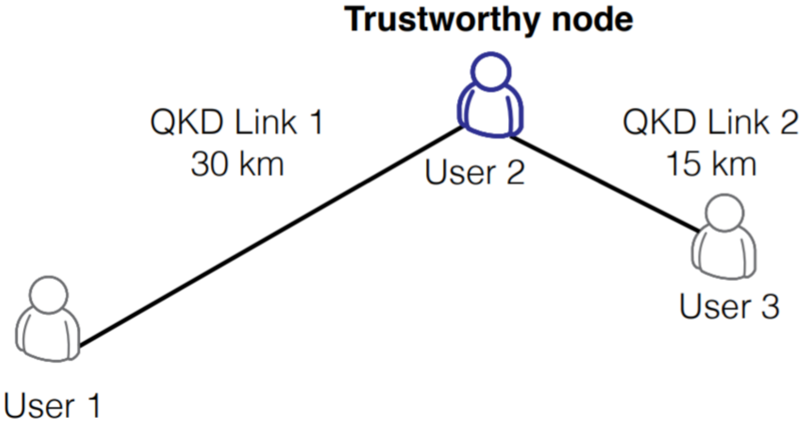
QKD networks are key to new quality provided by quantum technologies



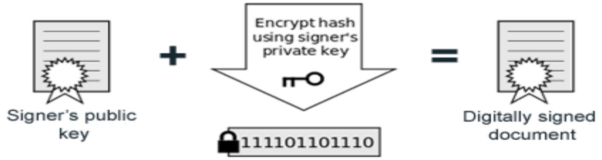
Quantum network experiment (May 2017)

- 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.

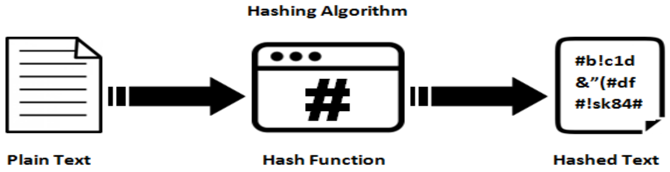
E.O. Kiktenko, et al. Demonstration of a quantum key distribution network in urban fibre-optic communication lines // Quantum Electronics 47 (9), 798-802 (2017).



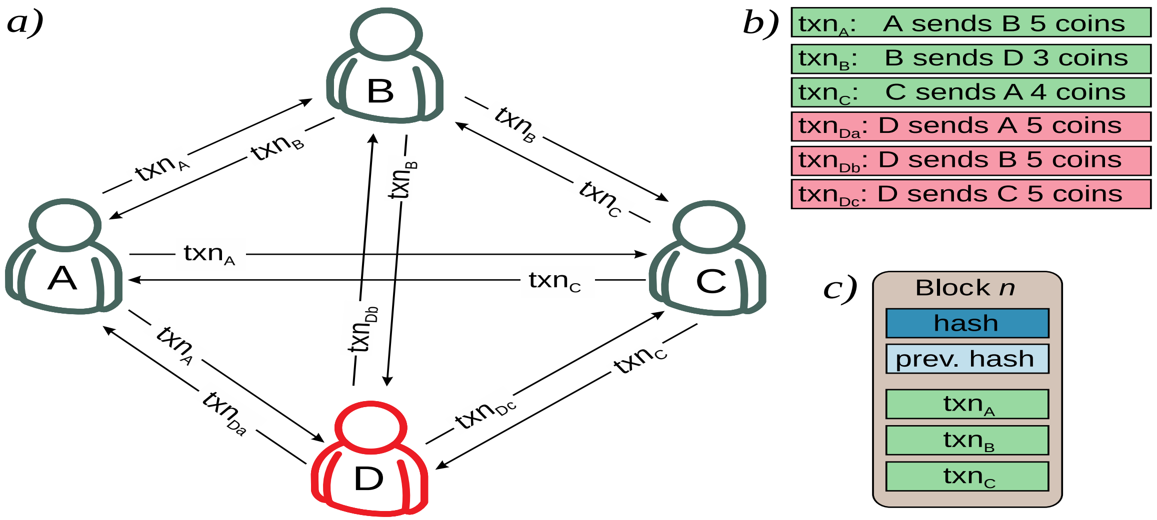
Quantum key protects blockchain



Digital signatures – Quantum-unsafe



Hash functions – Believed to be quantum-safe...?



Quantum-secure blockchain opens new opportunities for QKD

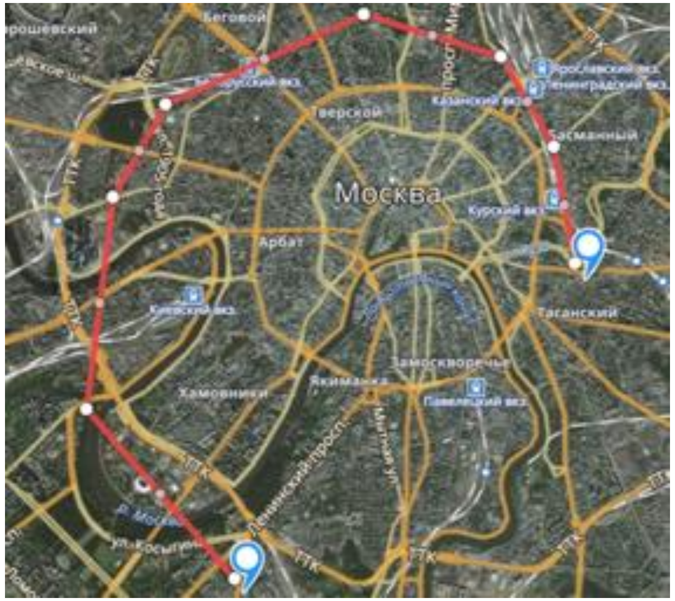
- QKD guarantees information-theoretically secure authentication between users.
- The unconfirmed transactions are aggregated into a block.
- We propose to create blocks in a decentralized fashion. To this end, we employ the "broadcast" protocol.
- This protocol allows achieving a Byzantine agreement 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.

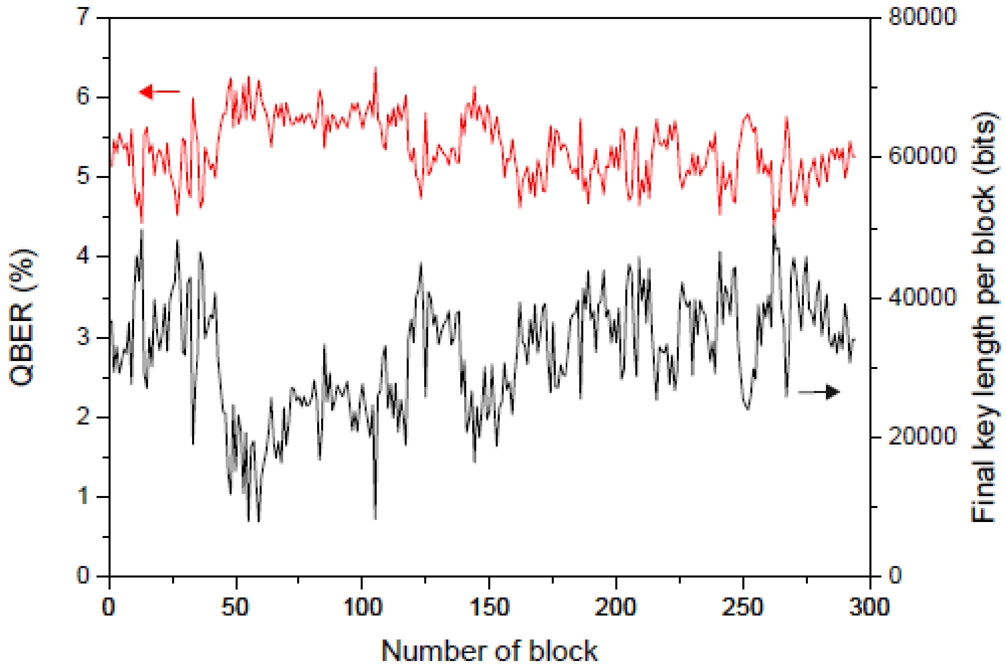
2017-2018 Sberbank field tests

LAUNCHING QUANTUM SECURITY

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.

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)

Presentation by Jian-Wei Pan at TyQI conference, Shanghai, June 27–30, 2016


视频会议
数据库
视频会议
数据库
量子信道
经典信道
用户节点
单模复用技术

One of 32 trusted nodes

Участники сети

Photo ©2016 Vadim Makarov

Tokyo network built by different groups

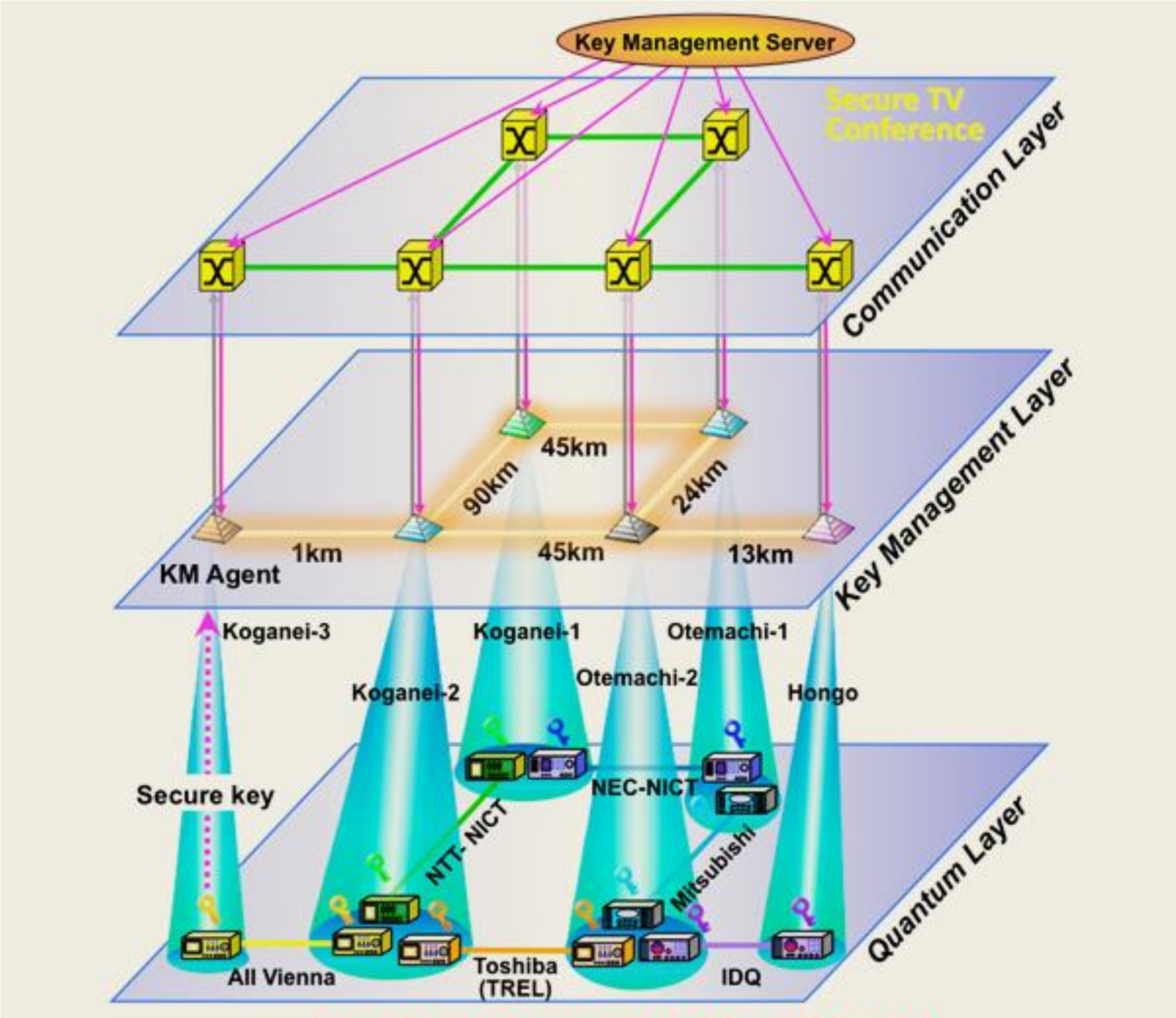


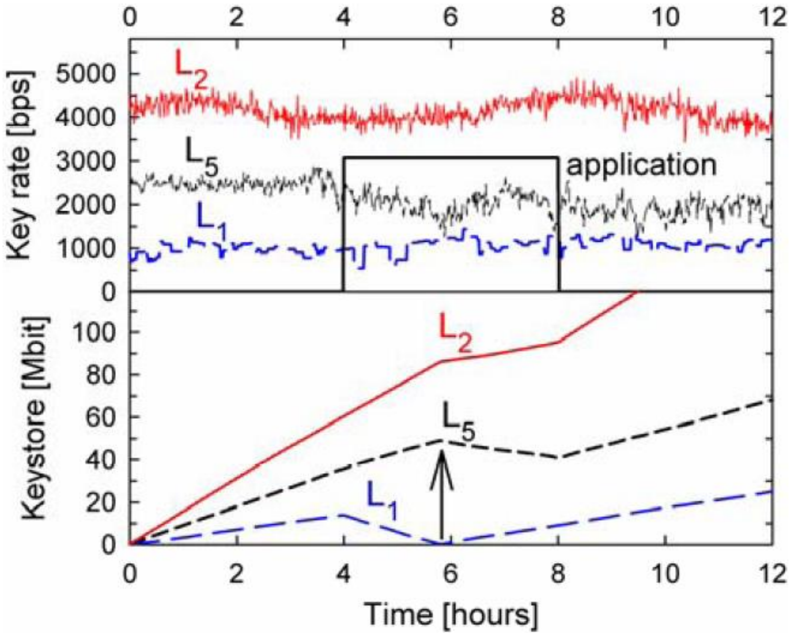
Fig. 2 Network Layer Structure of the Tokyo QKD Network

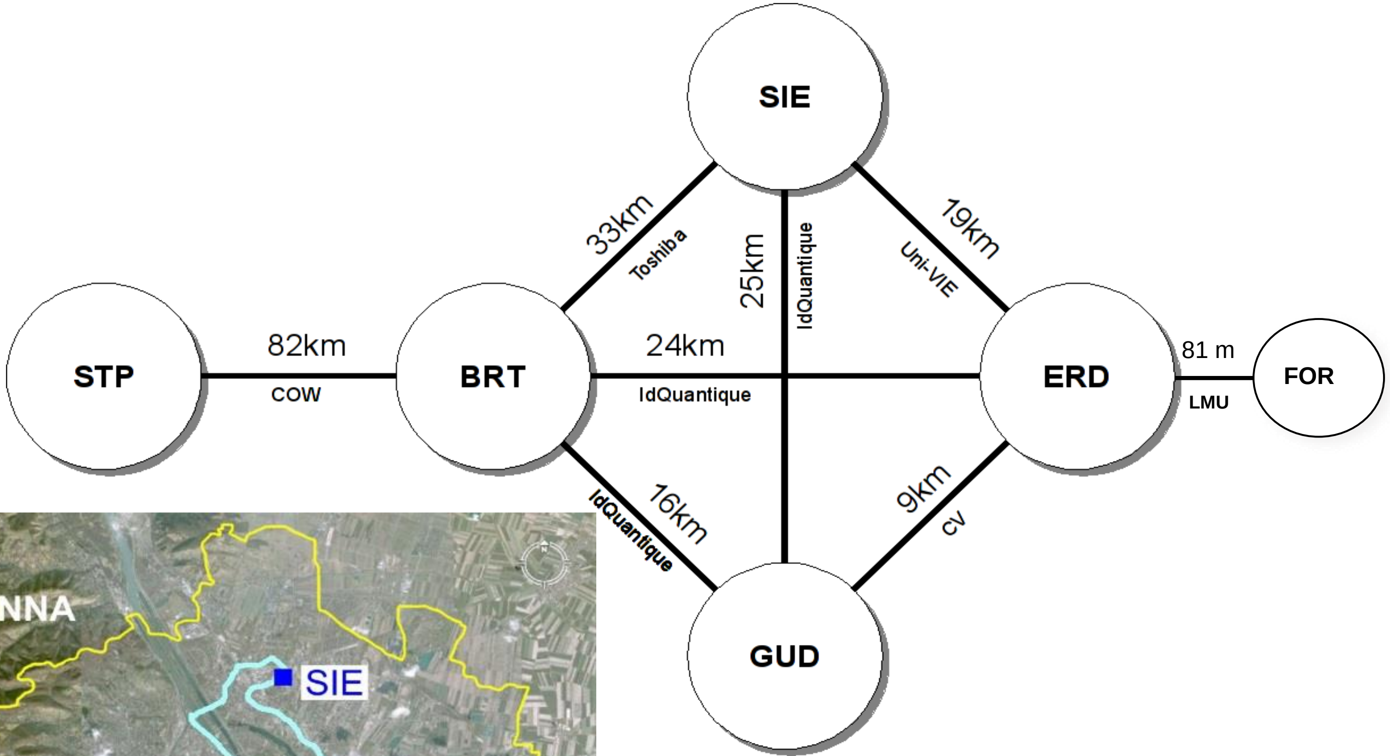
Communication layer

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

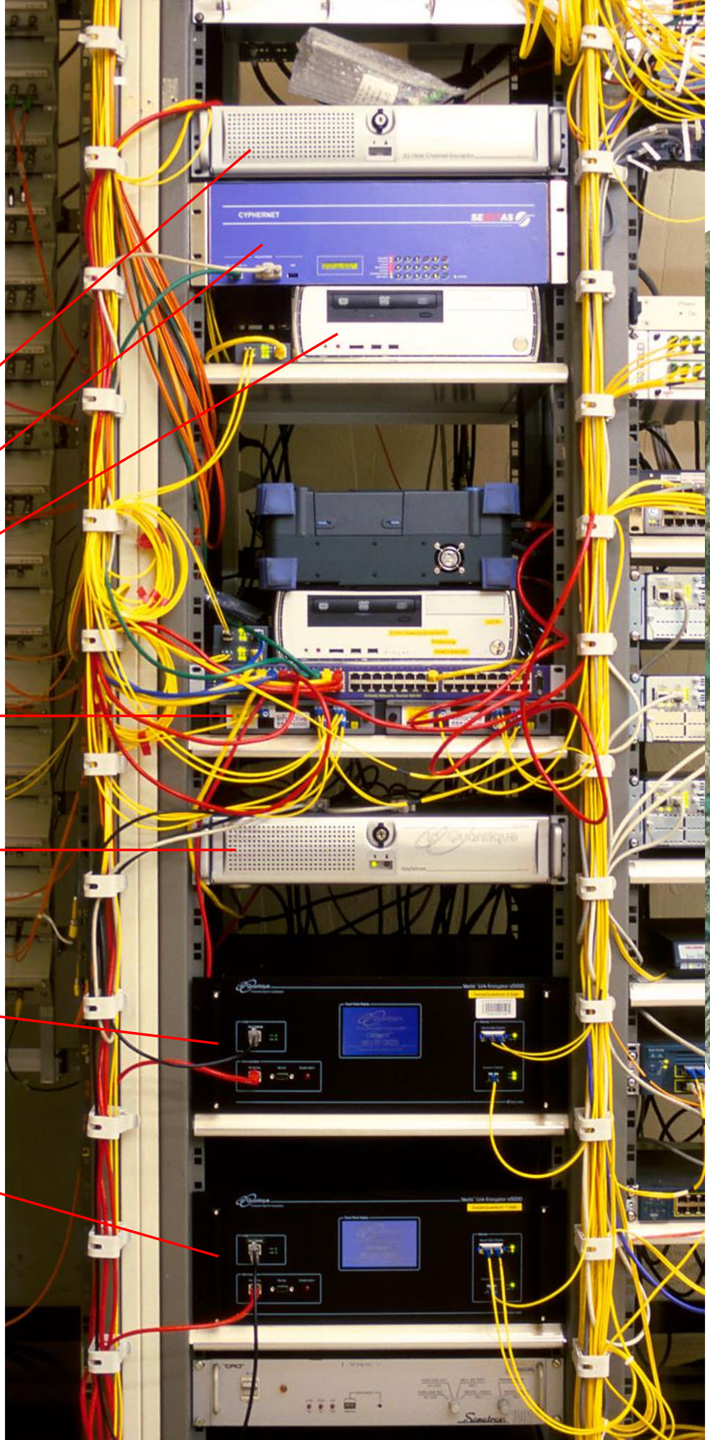
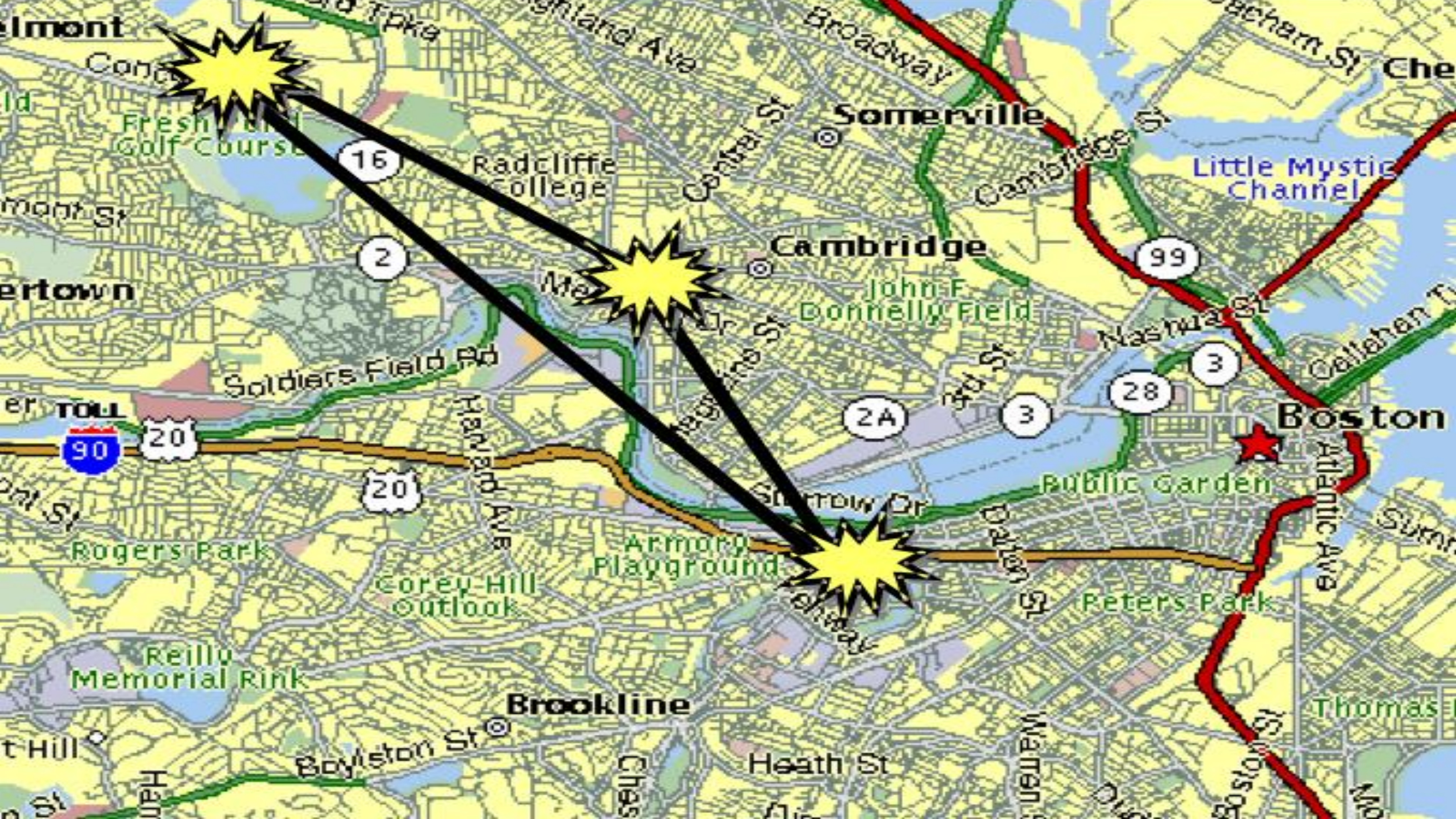


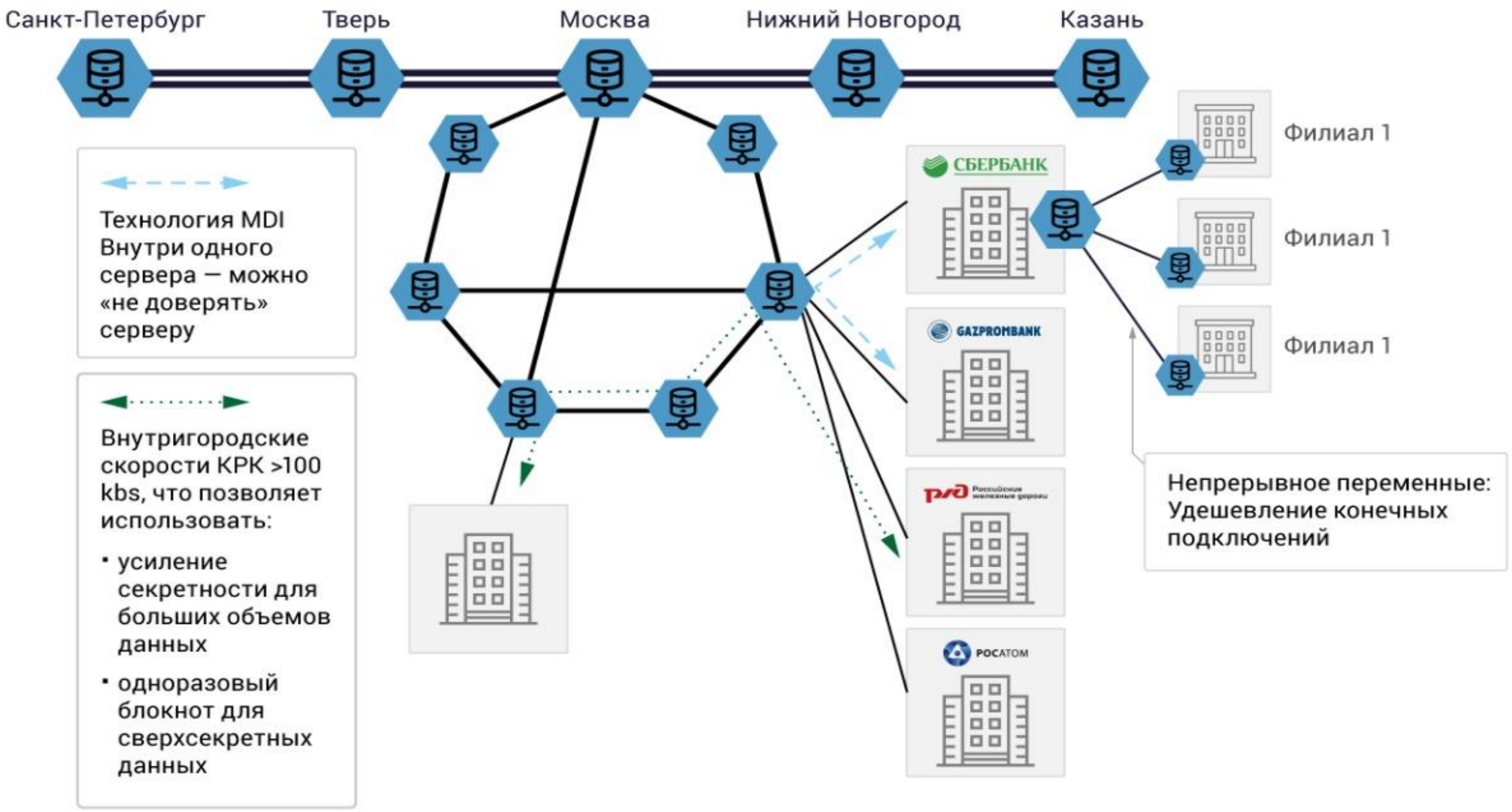
Photo ©2010 Vadim Makarov

www.swissquantum.com
ID Quantique *Cerberis* system (2010)

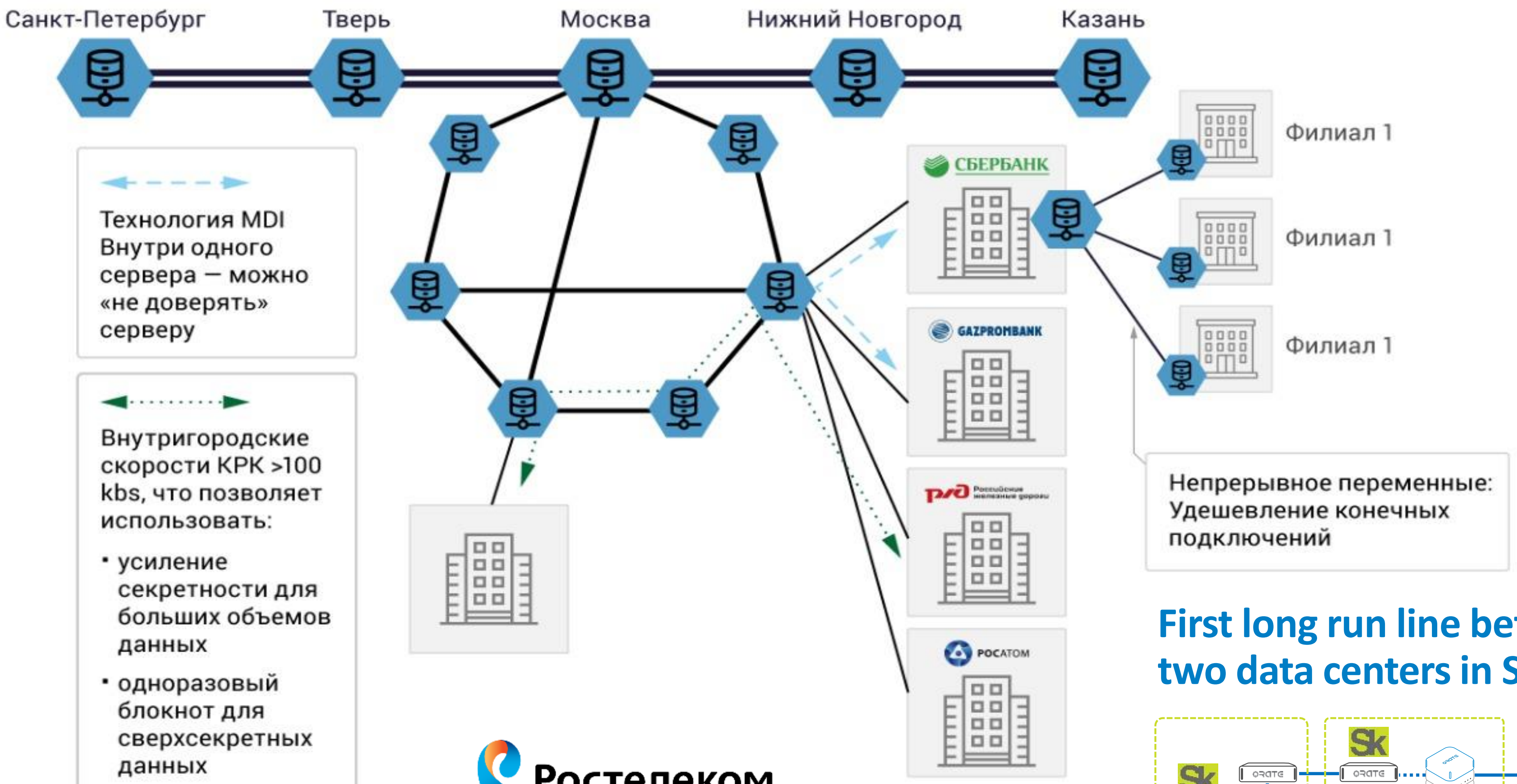


Somerville
Radcliffe College
Little Mystic Channel
Cambridge
John F. Donnelly Field
Soldiers Field Rd
Boston
TOLL
90
20
16
2
99
3
28
2A
Public Garden
Storrow Dr
Armory Playground
Rogers Park
Corey Hill Outlook
Peters Park
Reilly Memorial Rink
Brookline
Boylston St
Heath St
Harvard Ave
Atlantic Ave
Broadway
Cambridge St
Central St
Nashua St
Fresh Pond Golf Course
Highland Ave

Russian quantum networks in 2024



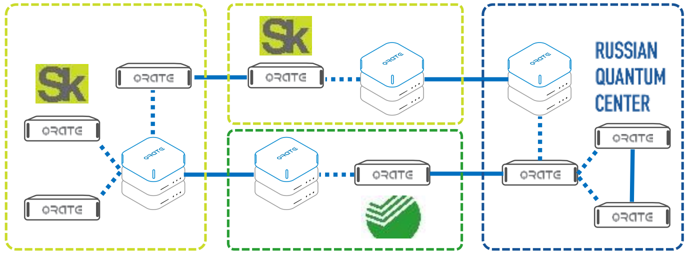
Russian quantum networks in 2024 will reach 10 000 km



Ростелеком

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

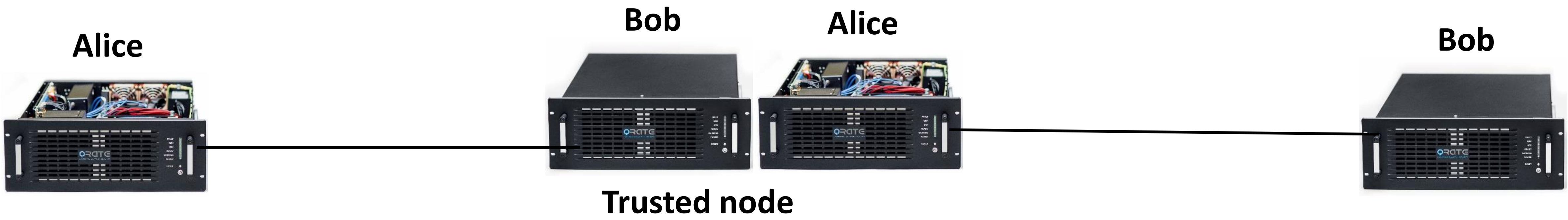
First long run line between two data centers in Sberbank

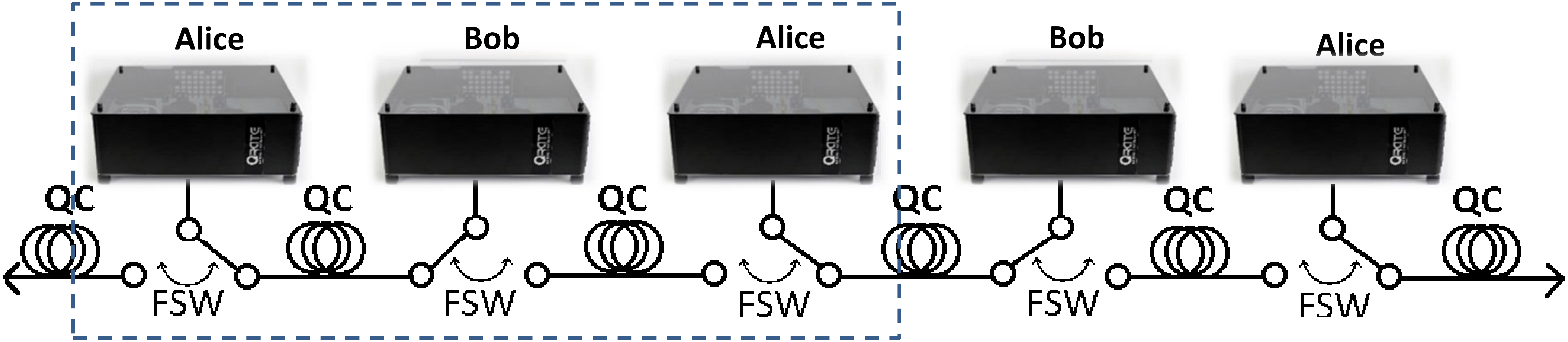


QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

Switch based network reduces number of equipment





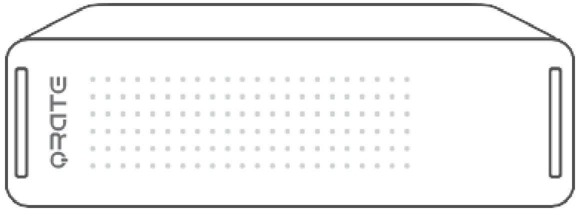
QRATE QUANTUM COMMUNICATIONS

РКЦ Российский Квантовый Центр

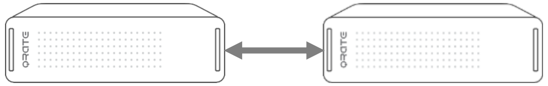
How to miniaturize QKD

Existing QKD

Rack19” solution



One to one connection



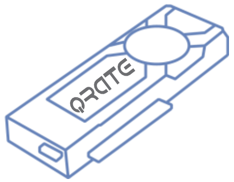
High price of one channel

Competitors:

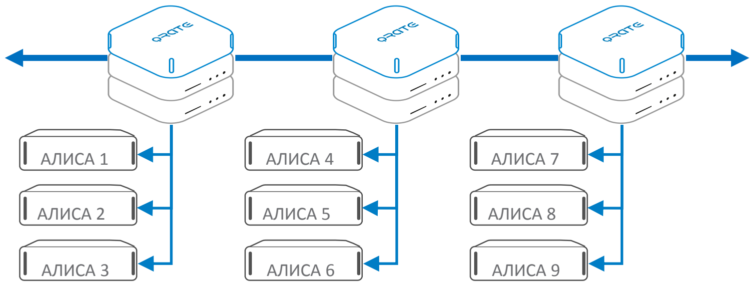
- ID Quantique
- Qubitekk
- QuantumCTek

New version with small alice and switch

Video card Alice



One to many connection (up to 1:128)

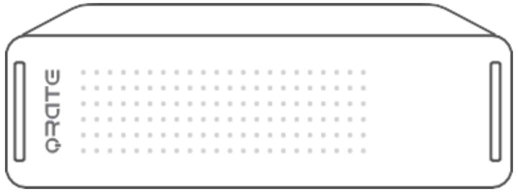


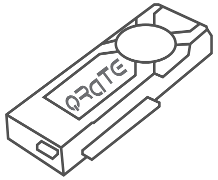
Channel cost drops more than 10times

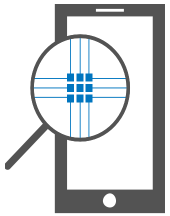
No competitors up to year 2019

We're on the road to quantum internet

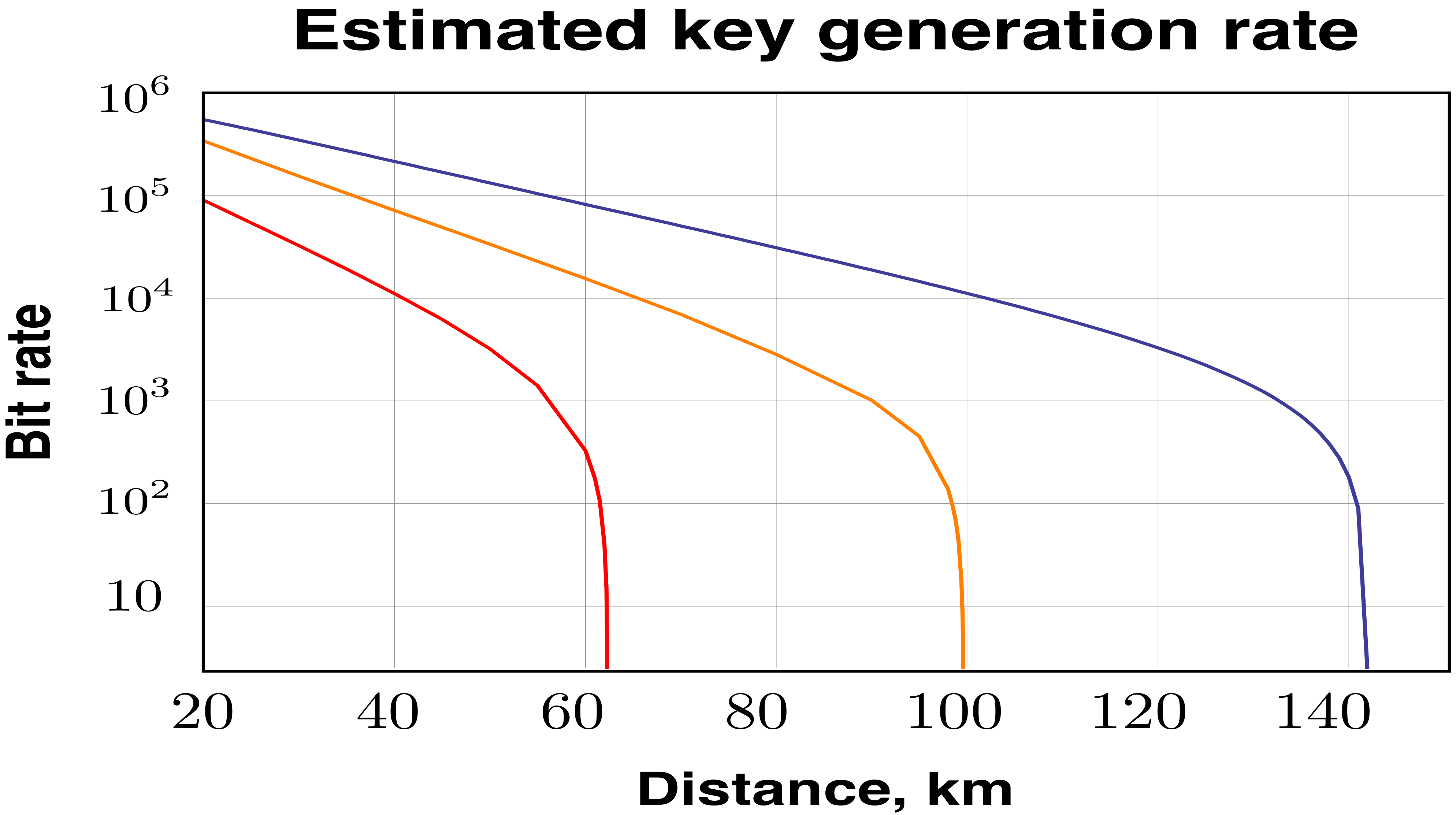
Now	5 Years	10-15 Years
Quantum Security	Quantum-secure IoT	Quantum Internet



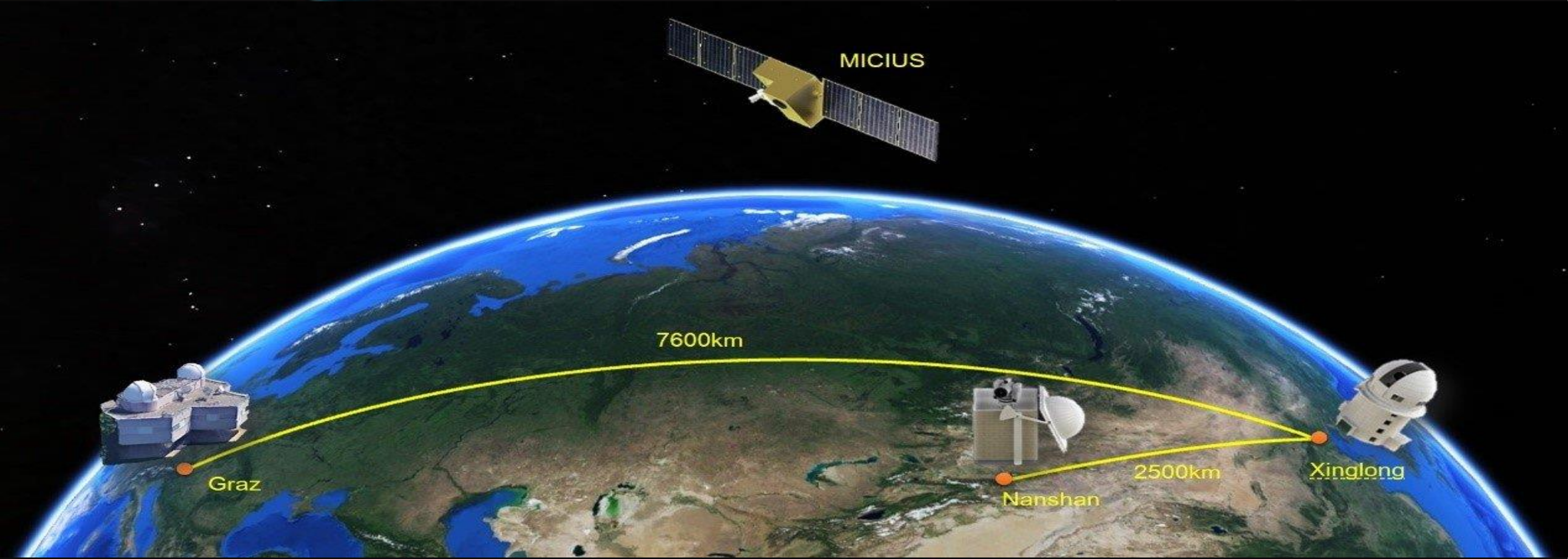




QKD distance limit is driven by exponential loss

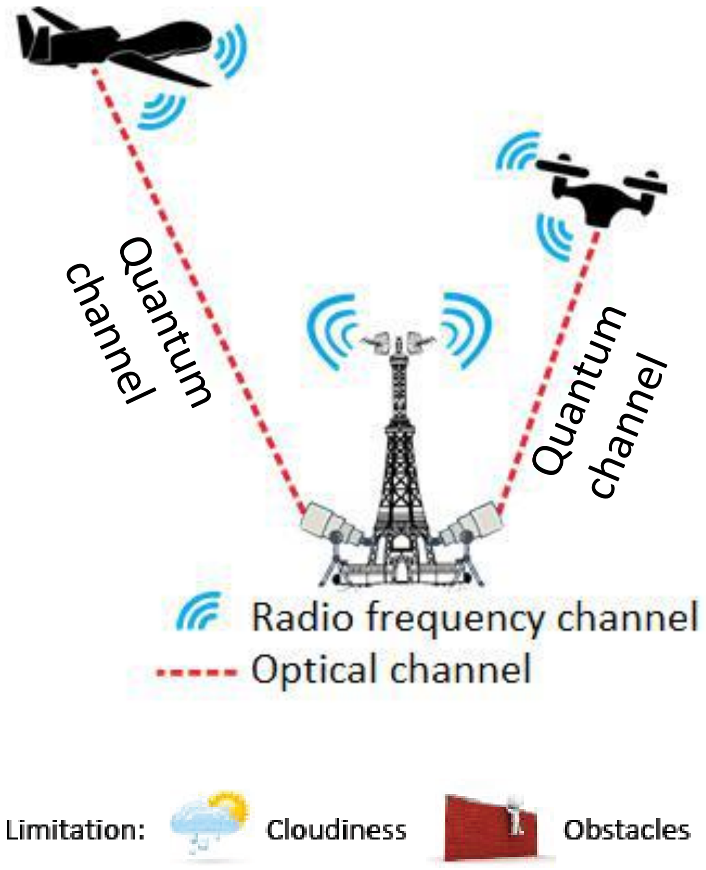


China is the only country with quantum satellite but may other are in the competition

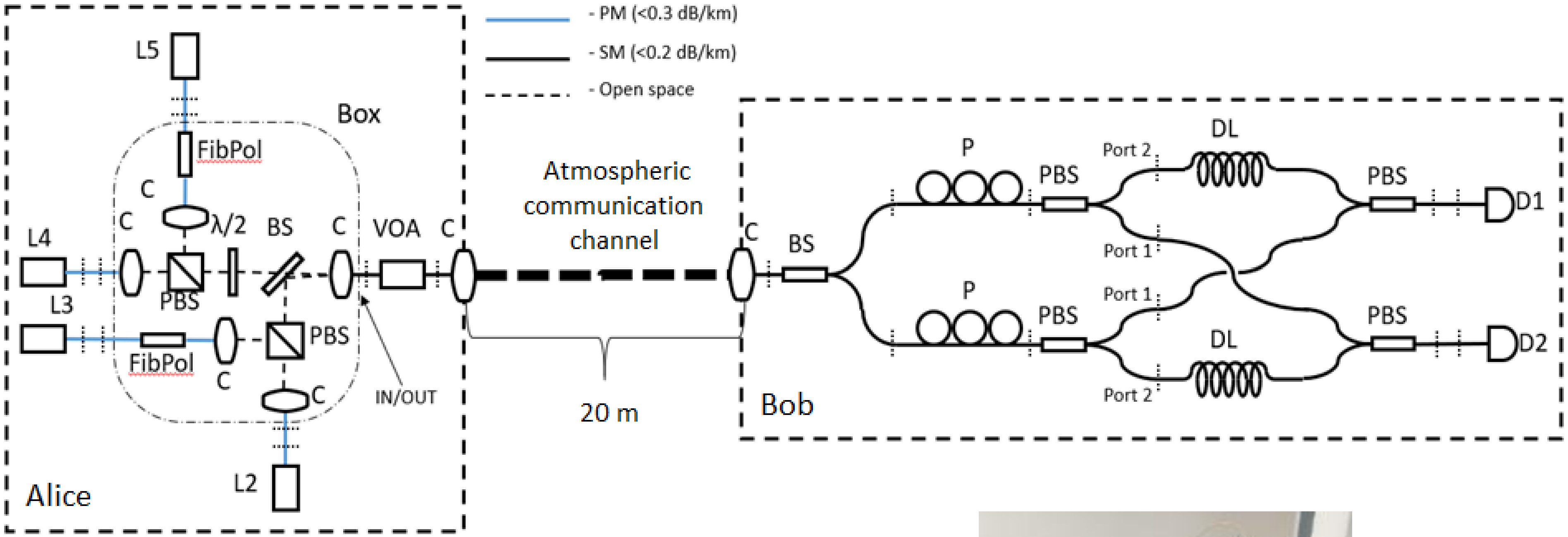


– Unmanned or manned aircraft can distribute secret key bits through free-space optical quantum channel

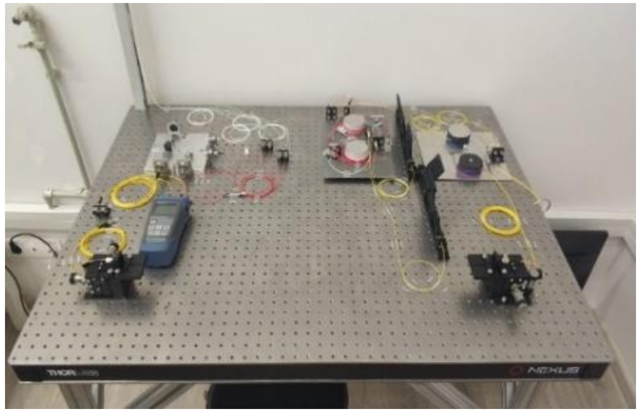
– Information, encrypted by secret key, then can be transmitted through classical RF-channel or free-space optics communication



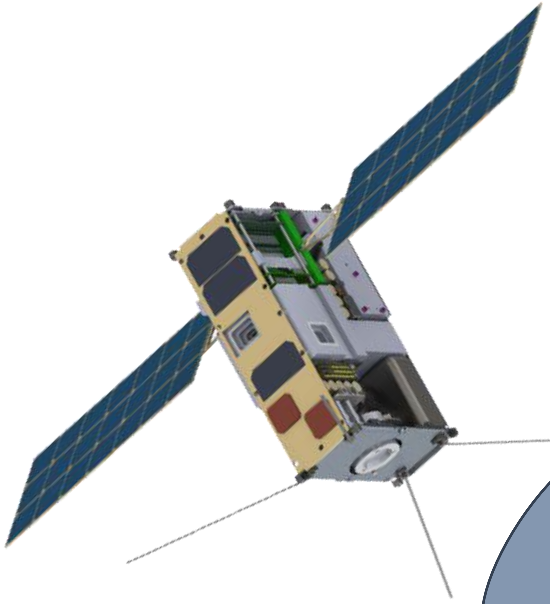
Free space QKD initiative: prototyping for drones application



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



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

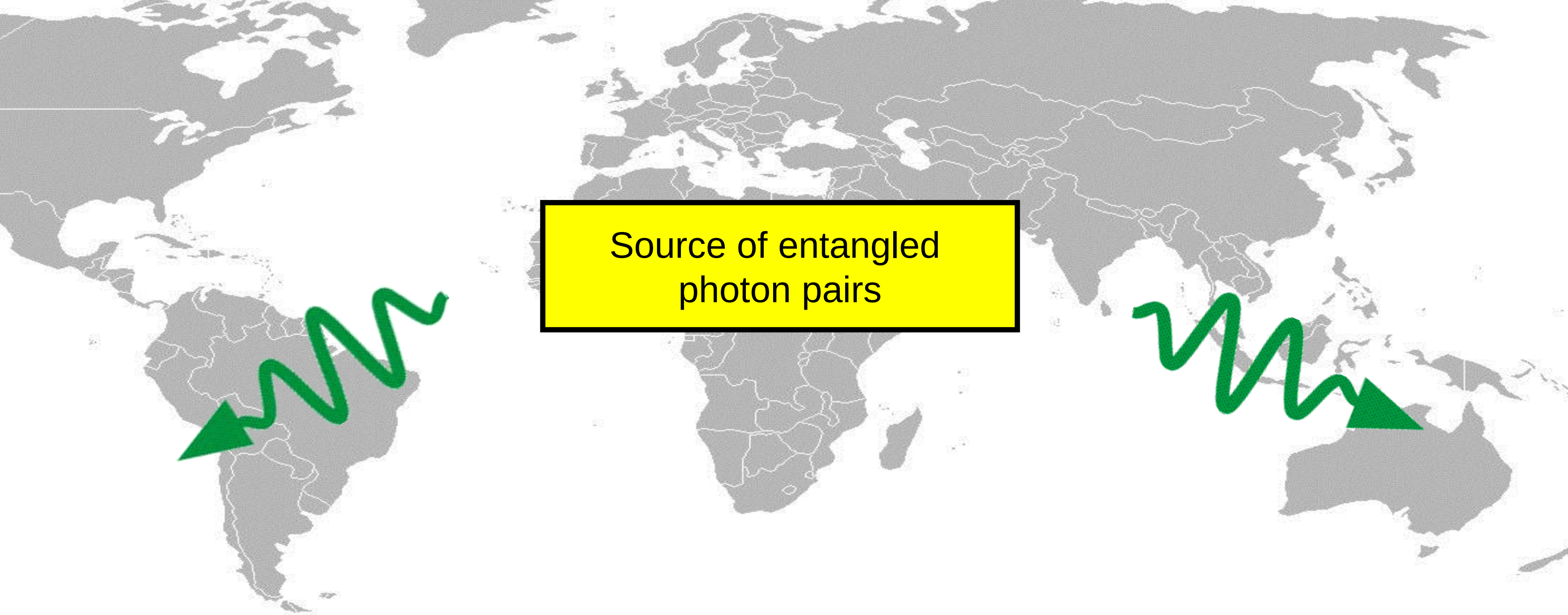
10 DFB lasers for different application tasks

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

Quantum repeaters

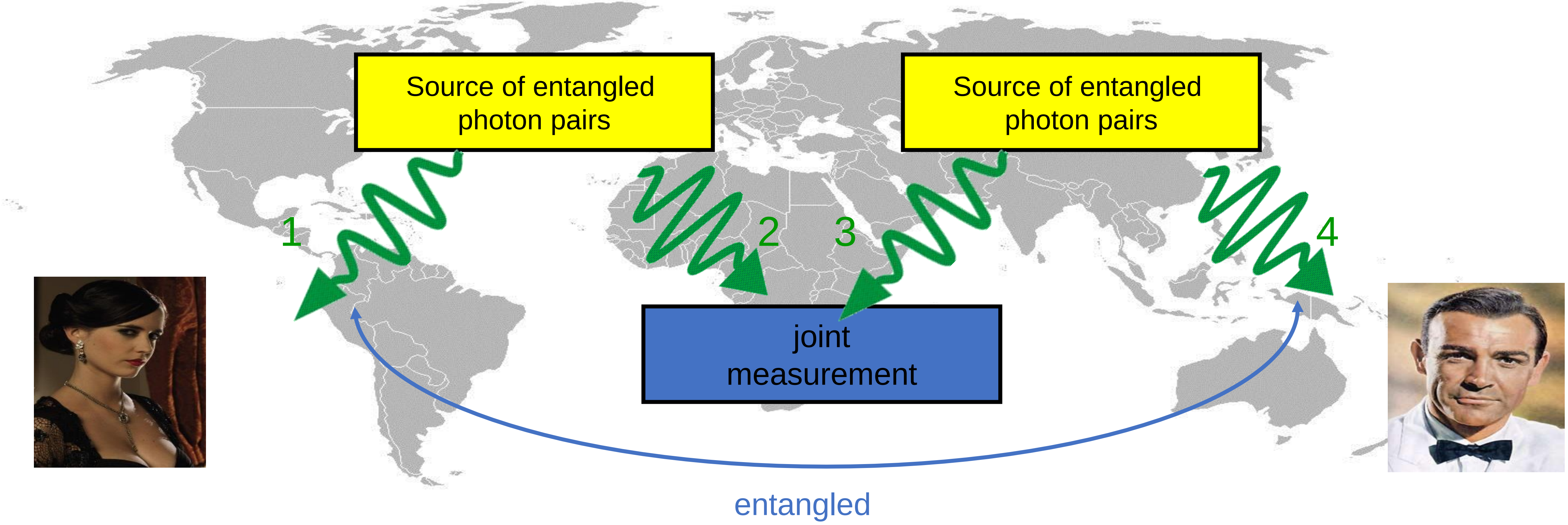
- Problem: to get 1 photon after 1000 km line you need to make 10^{20} ts what is not practical
- Practical distances are within 100 km in the external lines and within 400 km in the lab (less than 1 bit/s)
- Solution comes from classical communication, we need a repeater
- What is a repeater
  - Device 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…



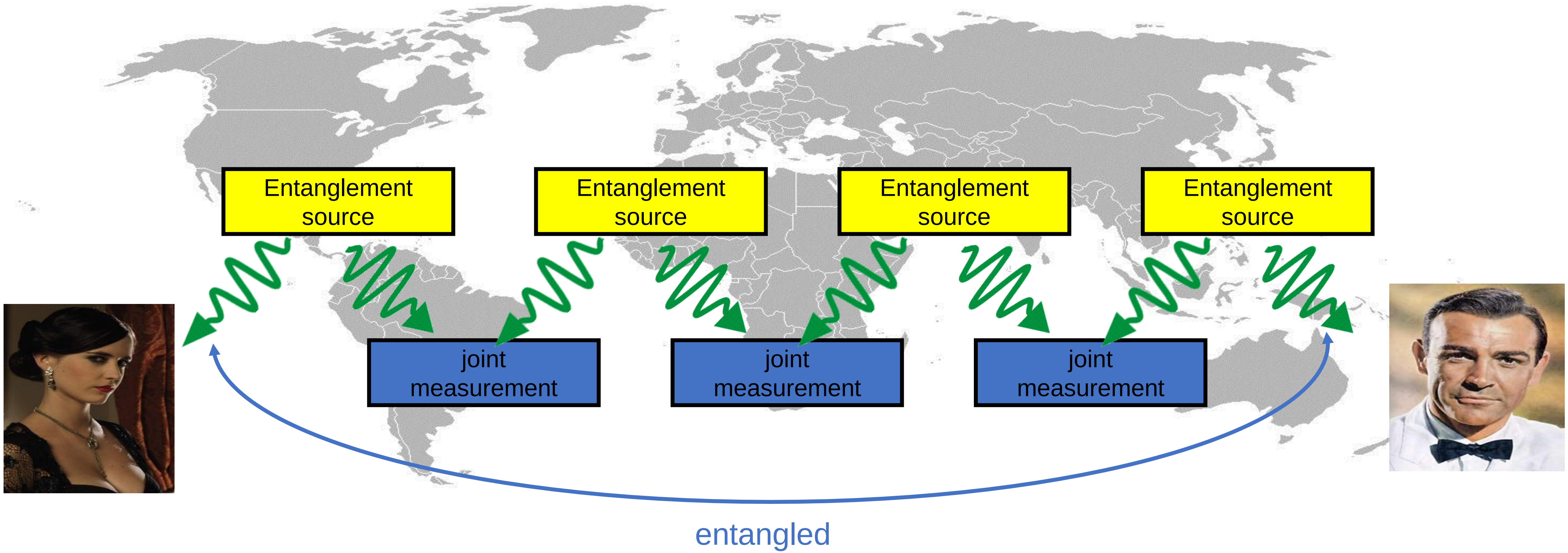
The photons are likely to get lost on their way

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

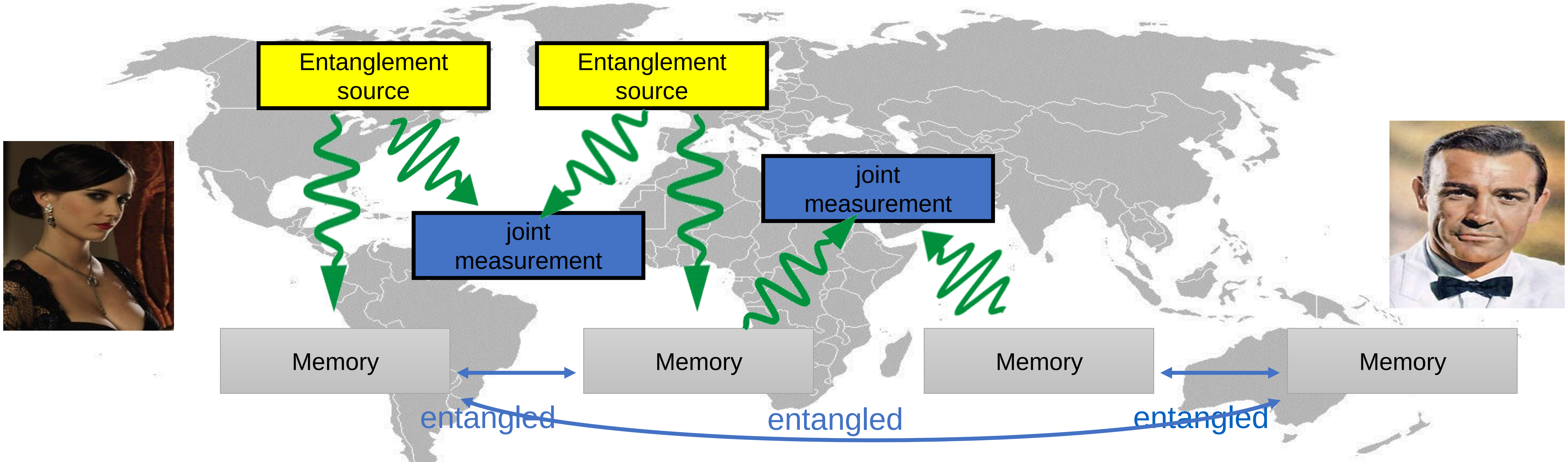


Long-distance entanglement can be created by *entanglement swapping*

but to succeed, all links must work simultaneously.

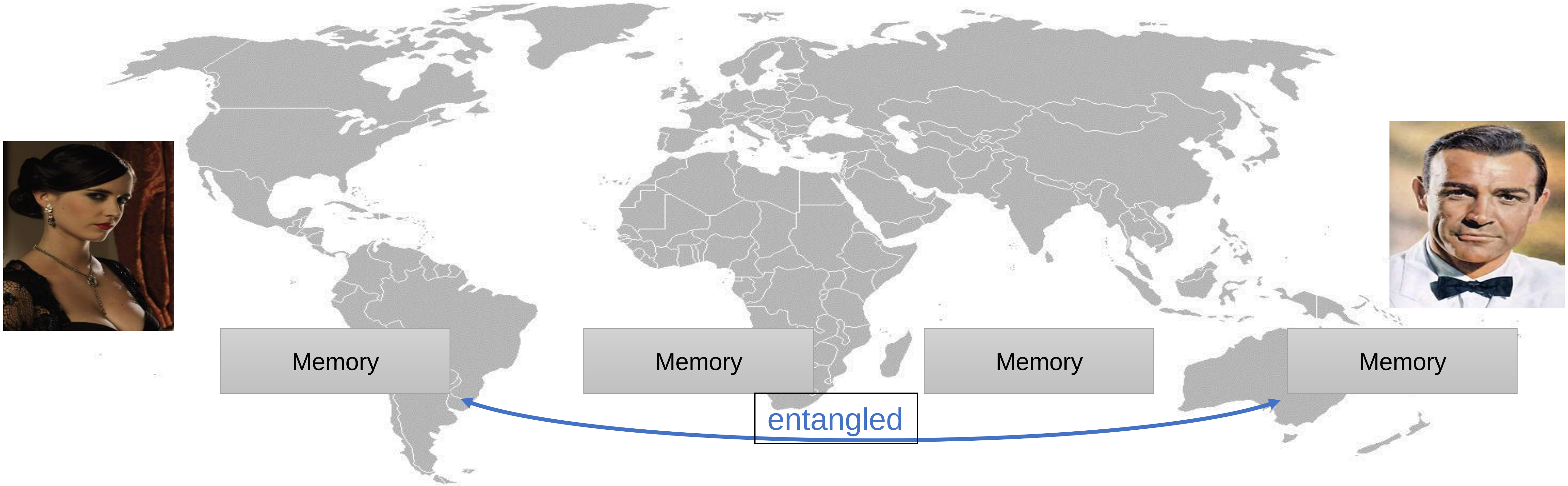
→ success probability still decreases exponentially with distance.

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



- **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