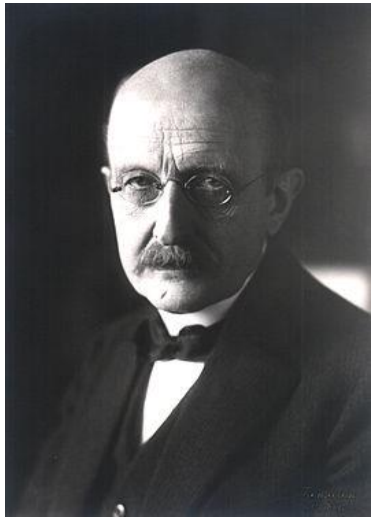
Lecture 2: Quantum optics at a glance.

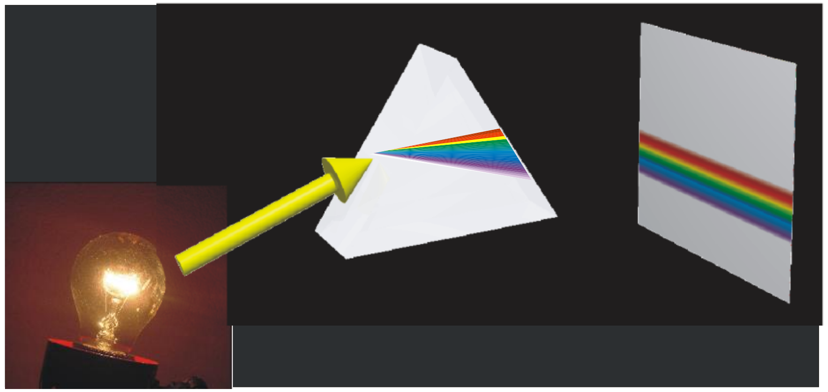
Content

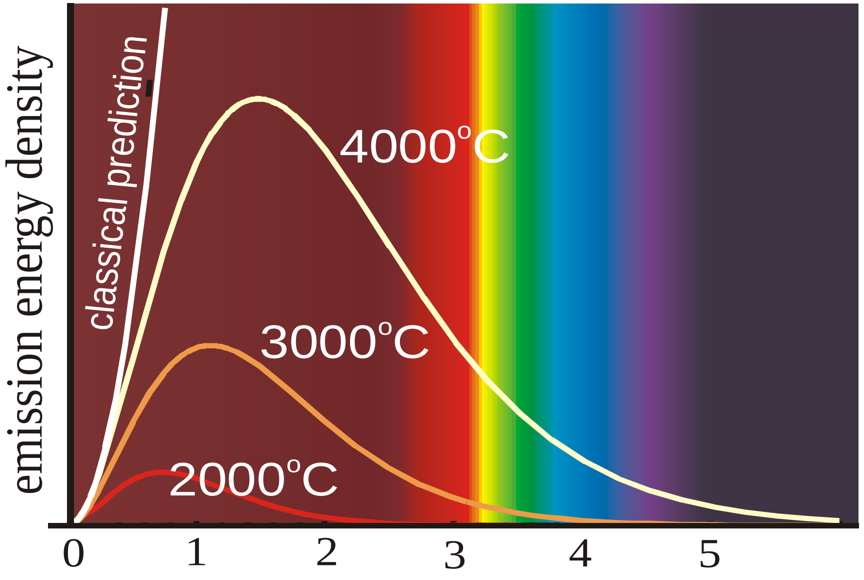
- Few words about light and states
- Wave and particle
- Quantum interference
- Beamsplitter
- States of light
- Entangled state
- Qubit concept
- Bloch sphere

Single photon is beautiful, but we expect from it some practical application

- Thermal radiation
  - All hot objects emit light
  - Emission spectrum can be measured
  - Classical physics predicts infinite intensity







Remind few words about light and states

Plain wave:

$$\vec{E}(\vec{r},t) = \vec{E}_0 e^{i\vec{k}\vec{r}-i\omega t} + c.c.$$

Combination of plain waves makes slowly-varying envelope :

A. I. Lvovsky. Nonlinear and Quantum Optics

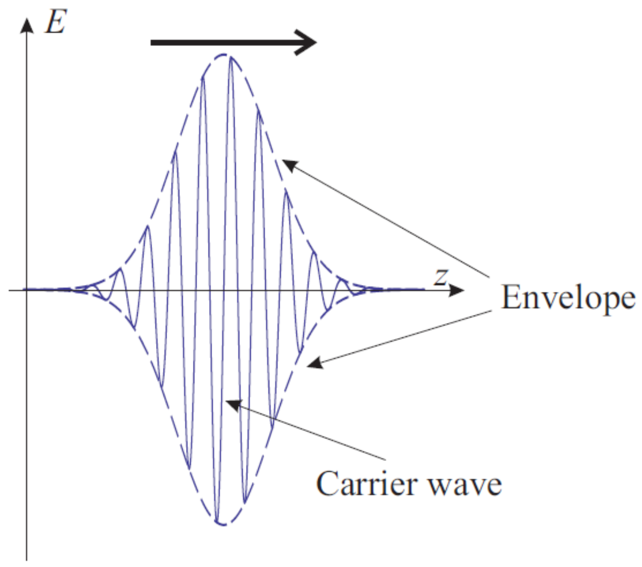
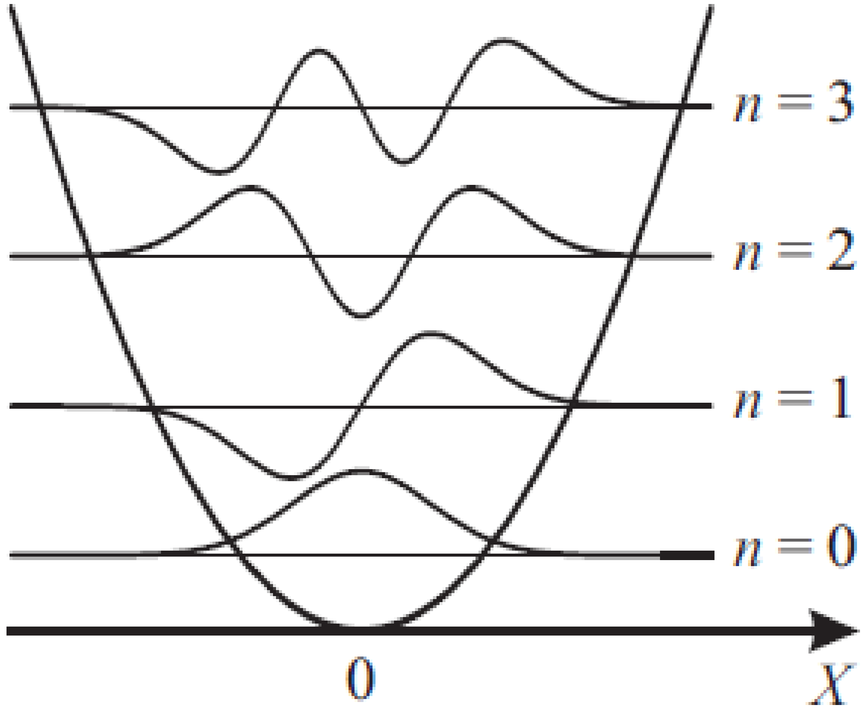


Figure 1.1: A pulse with a slowly varying envelope.

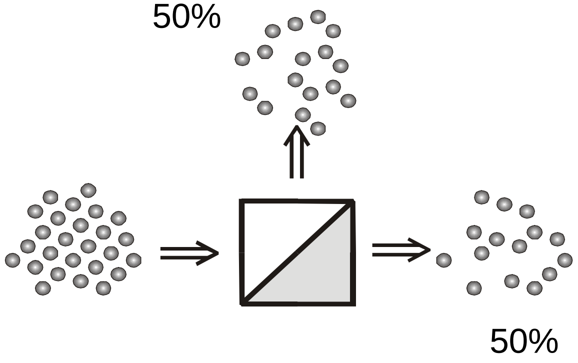
At the same time light can be qauntized:



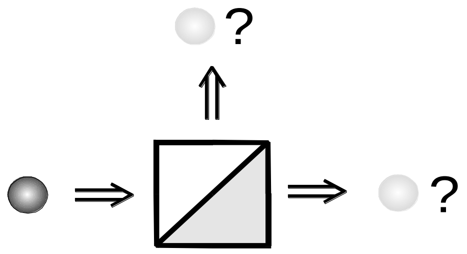
Single-Photons are Elementary Quantum Systems

- A single-photon constitutes an elementary quantum system

- Semi-transparent mirror



It cannot be split



What is the “shape” of the photon?

States of light

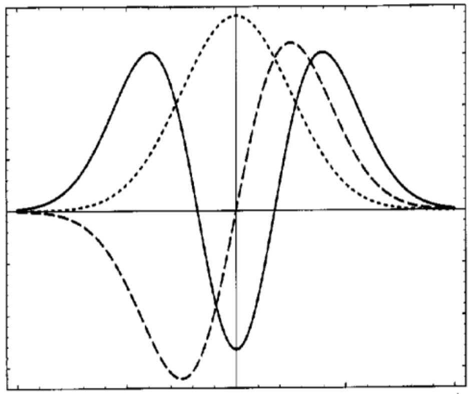
Fock state:
$|n\rangle$ - defined number of photons
Phase is not defined.
What about ΔEΔt ???

$$|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}|0\rangle$$

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}\,|n+1\rangle\,;$$

$$\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle\,;$$

$$\hat{n} = \hat{a}^\dagger\hat{a}$$



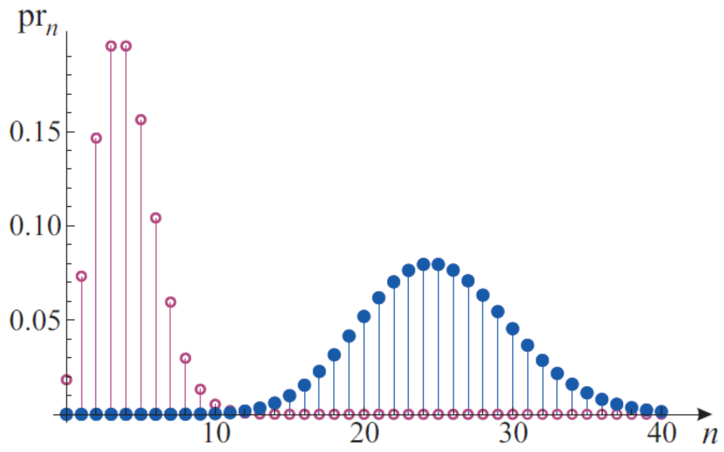
A. I. Lvovsky. *Nonlinear and Quantum Optics*

Coherent state: $|\alpha\rangle$

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_n \frac{\alpha^n}{\sqrt{n!}}|n\rangle$$

$$\hat{a}\,|\alpha\rangle = \ ?$$

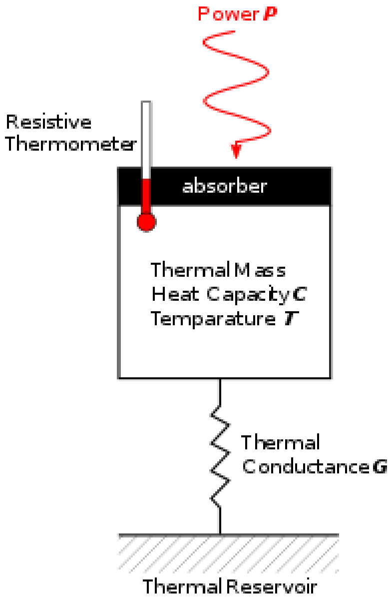
$$\langle n\rangle \ = ?$$



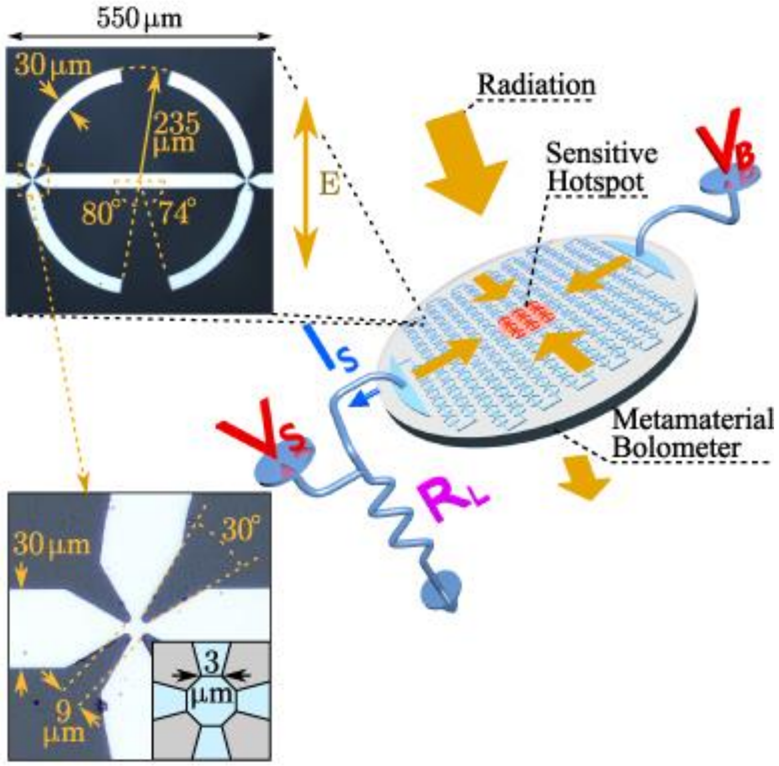
the Poisson distribution with $\langle n\rangle = 4$ (empty circles) and $\langle n\rangle = 25$ (filled circles).

How to observe $\langle n \rangle$?

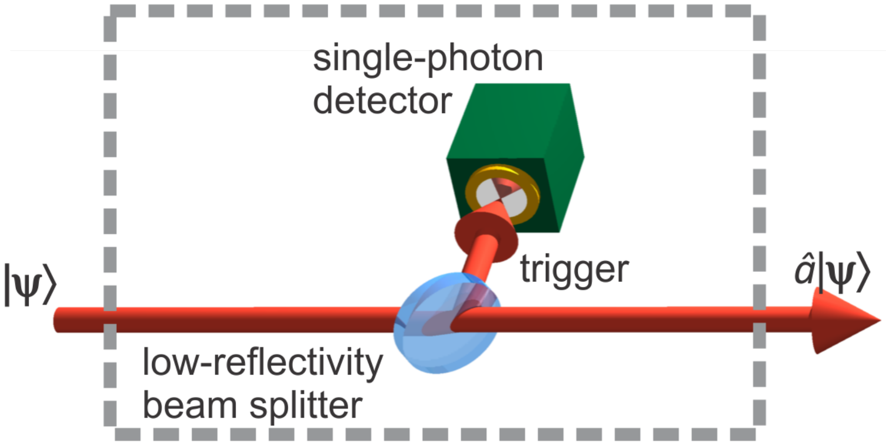
Threshold detector clicks on 1+ photons, we can put many of them



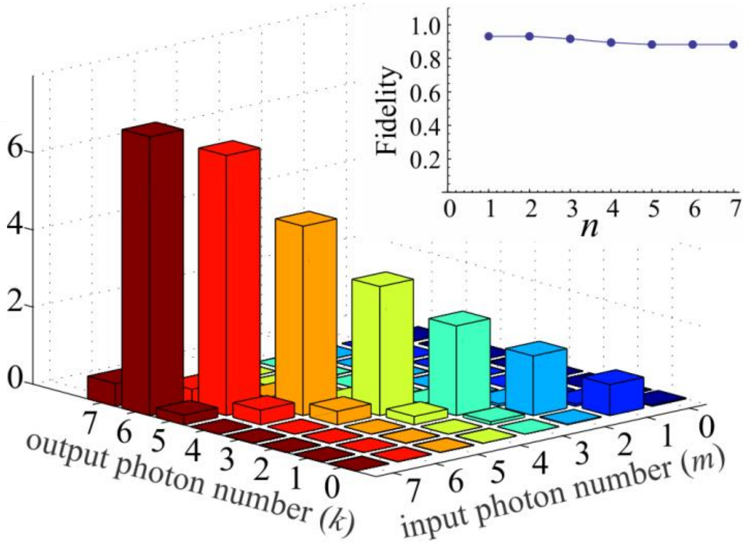
Superconducting nanowire bolometers can distinguish number of photons



How do we implement annihilation operator in the real experiment?



The scheme. A "click" indicates that a photon has been removed from $|\psi\rangle$



Experimental quantum process tomogralphy

R. Kumar, E. Barrios, C. Kupchak and A.L., PRL **110**, 130403 (2013)

Annihilation operator is non-deterministic

- Trace of the process output is given by the "click" probability
- The process involving the annihilation operator can change the state at a distance but cannot be used for faster than light communication because we need to transmit information about click

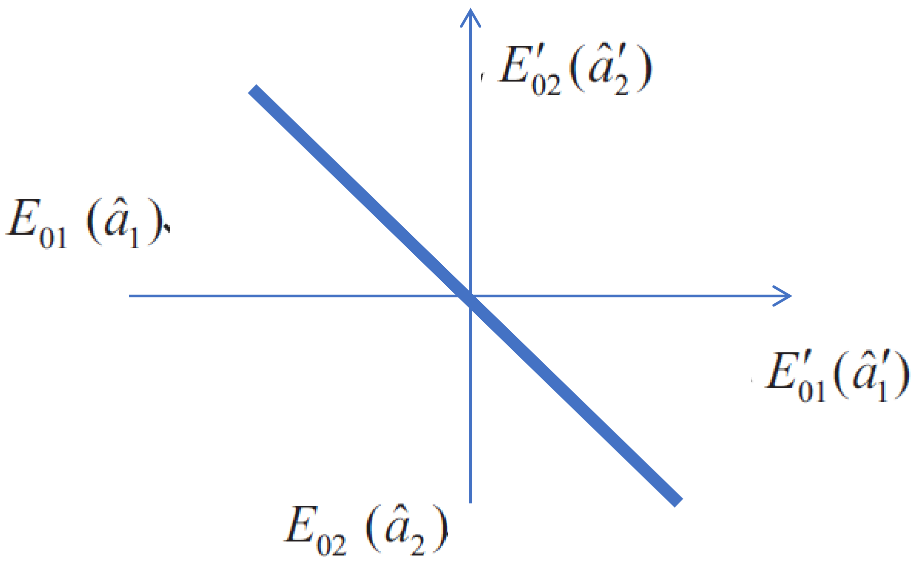
Beamsplitter

$$\begin{pmatrix} E'^{(+)}_{01} \\ E'^{(+)}_{02} \end{pmatrix} = \underline{B} \begin{pmatrix} E^{(+)}_{01} \\ E^{(+)}_{02} \end{pmatrix},$$

$$\underline{B} = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$$

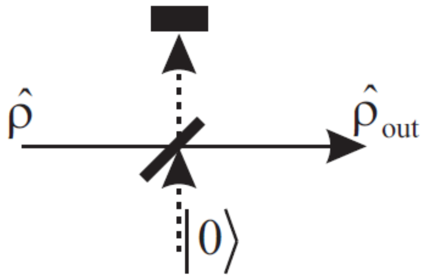
$$\underline{B} = \begin{pmatrix} t & -r \\ r & t \end{pmatrix},$$

$$\begin{pmatrix} \hat{a}'_1 \\ \hat{a}'_2 \end{pmatrix} = \underline{B} \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix}.$$



How does nature decides where is +r and where –r ?

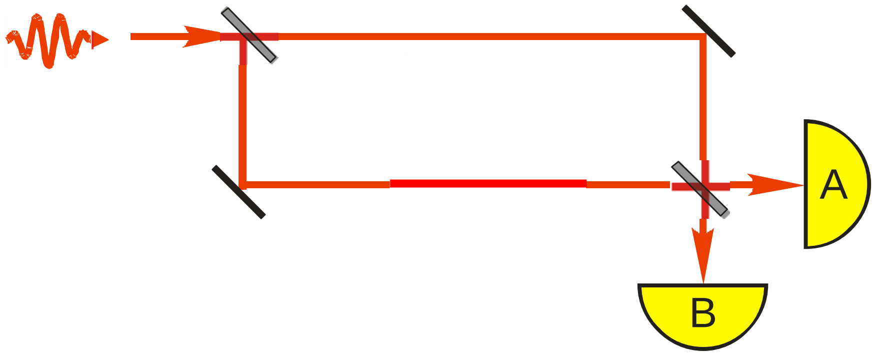
Beamsplitter represents an absorbtion:



The “bomb” paradox

[A. Elitzur and L. Vaidman (1993)]

- Mach-Zehnder interferometer tuned to get all signal on A

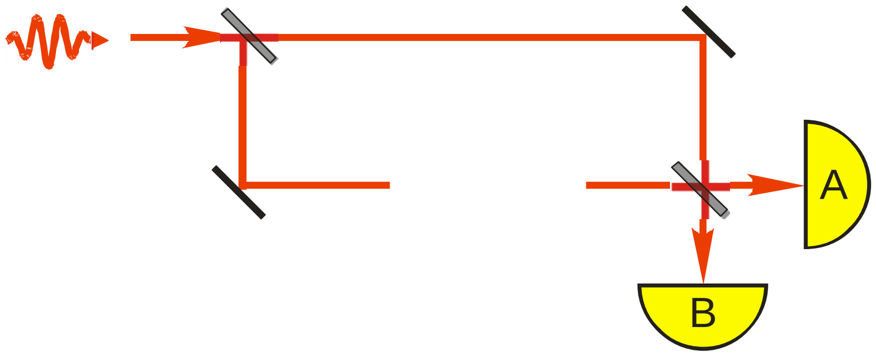


- If we move to single photon signal all clicks will still be on A

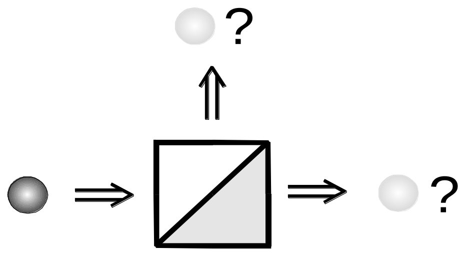
The “bomb” paradox

[A. Elitzur and L. Vaidman (1993)]

- Mach-Zehnder interferometer tuned to get all signal on A



- If cut one arm the signal will be split 50/50

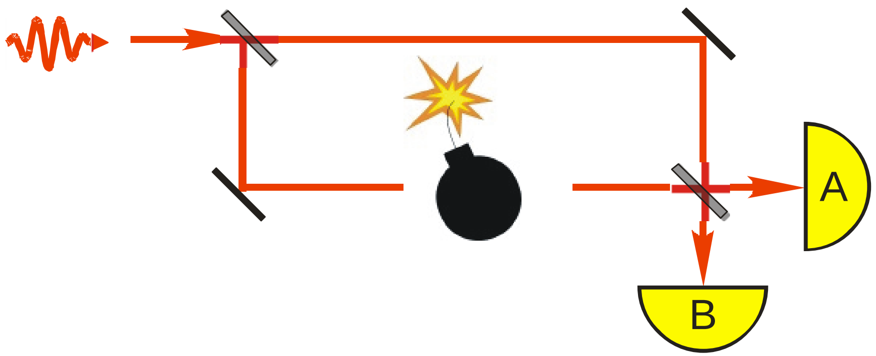


- *Single photon will click random detector*

The “bomb” paradox

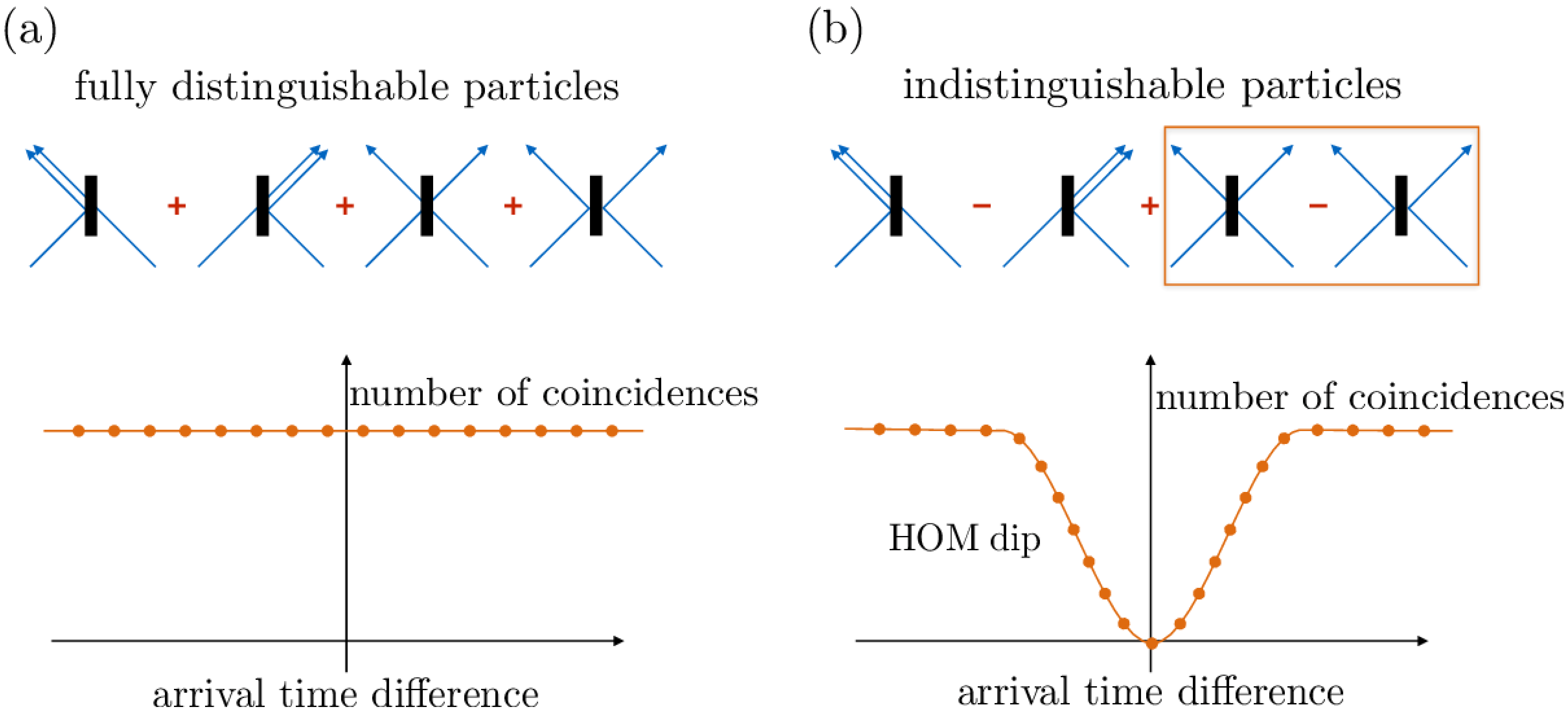
[A. Elitzur and L. Vaidman (1993)]

- Interaction-free weapons inspection
  - Insert a single-photon sensitive bomb into one of the interferometer arms

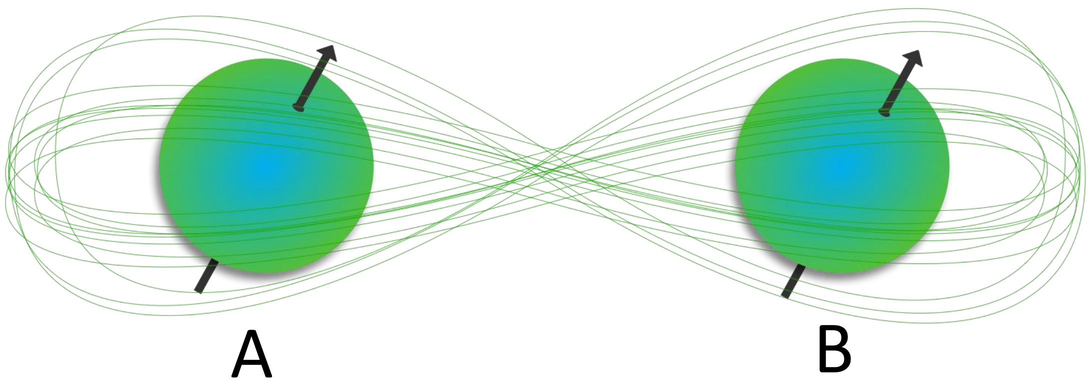


- Bomb absent
  → **interference observed: all photons emerge at A**
- Bomb present
  → **no interference: photons emerge at A or B**
  → **bomb may or may not explode**
- Photon detected at B (what probability ?)
  → **bomb is present**
  → *bomb has been detected without any interaction!*

Hong-Ou-Mandel effect



Entangled states



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

Can we use it to send information?

Einstein, A.; Podolsky, B.; Rosen, N. (1935). "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?". Physical Review. 47 (10): 777–780. Bibcode:1935PhRv...47..777E. doi:10.1103/PhysRev.47.777

Bell, John (1964). "On the Einstein Podolsky Rosen Paradox" (PDF). Physics. 1 (3): 195–200. doi:10.1103/PhysicsPhysiqueFizika.1.195

Freedman, Stuart J.; Clauser, John F. (1972). "Experimental Test of Local Hidden-Variable Theories" (PDF). Physical Review Letters. 28 (14): 938–941. Bibcode:1972PhRvL..28..938F. doi:10.1103/PhysRevLett.28.938.

Alain Aspect (1976)
Proposed experiment to test the nonseparability of quantum mechanics, Phys. Rev. D 14, 1944

$$a|0\rangle + b|1\rangle$$

Qubit

€3 bn

$20 bn

$12 bn

$400 m

Alibaba 阿里巴巴集团

$150 m

Google

IBM

Microsoft

$100 m

$75 m

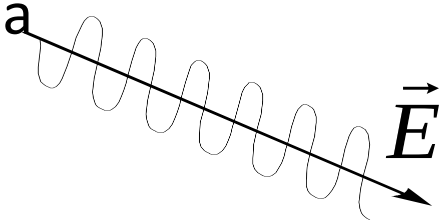
intel

$50 m

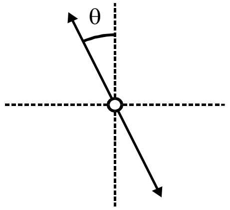

Stat
Attn
DDR

Polarization of Photons

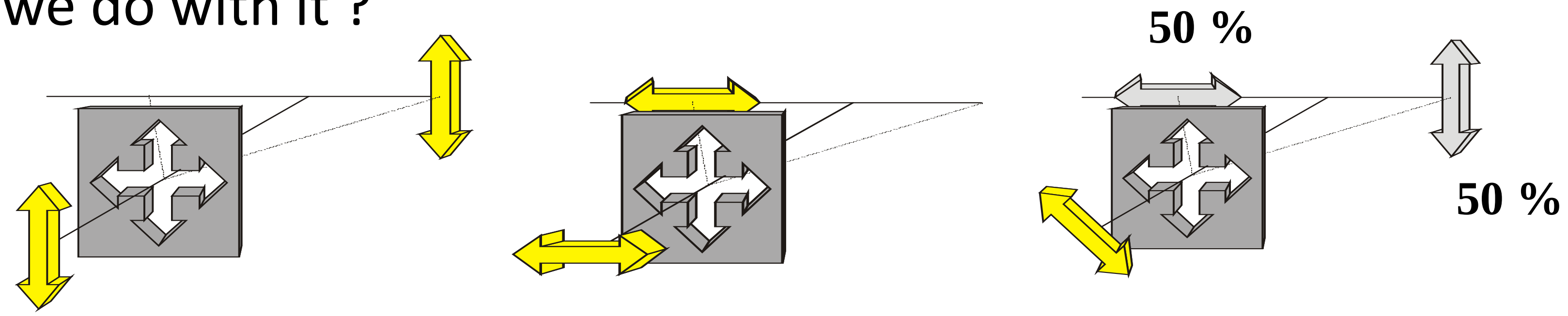
- Direction of oscillation of the electric field associated to a lightwave



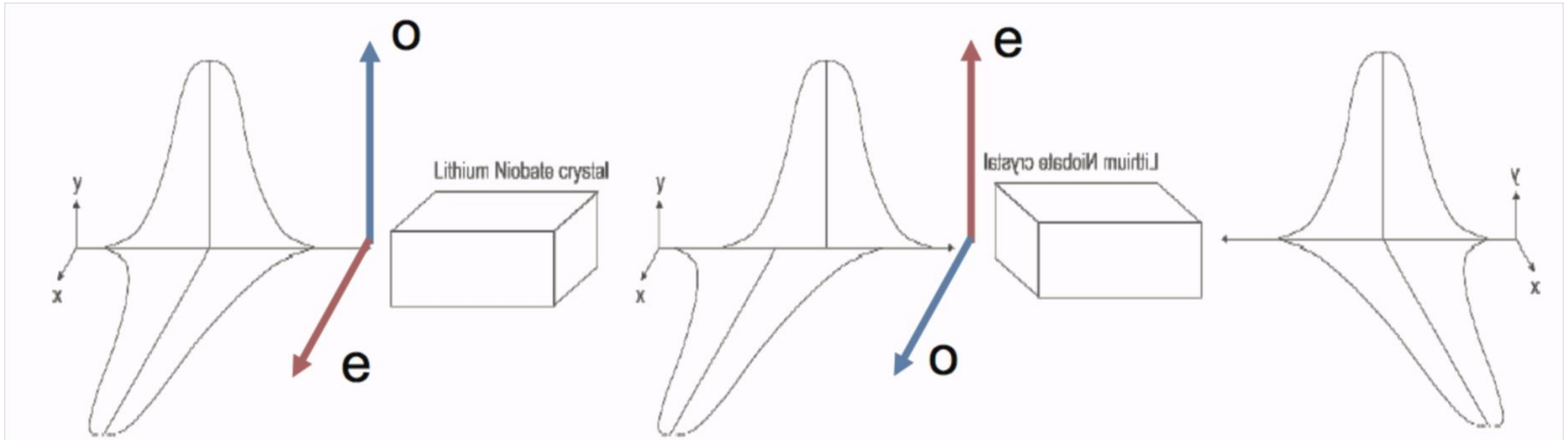
- Polarization states



- What can we do with it ?



How do we prepare states?

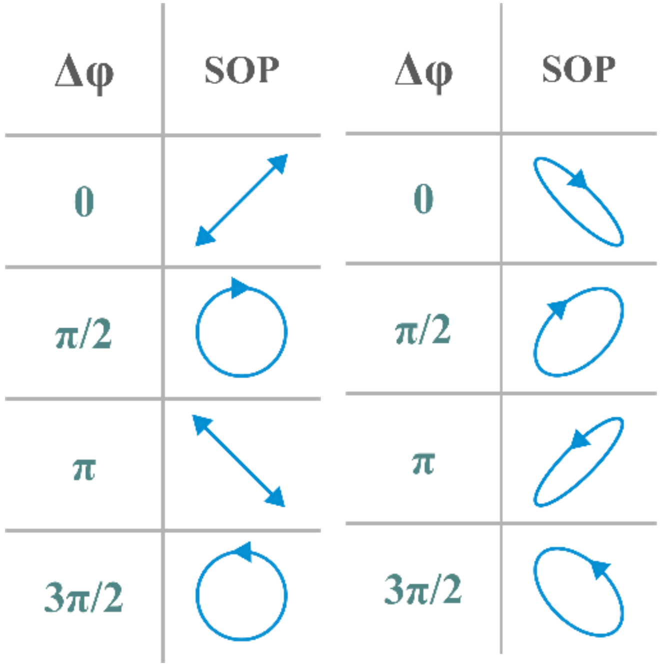
- We decide to use modern 10GHz fiber phase modulator as Pockels cell
- Even small time imbalance will break interference in the case of chirped pulse
- We propose to use identical phase modulator on the Bob side rotated to π/2 to compensate the polarization mode dispersion.
- 

- 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.

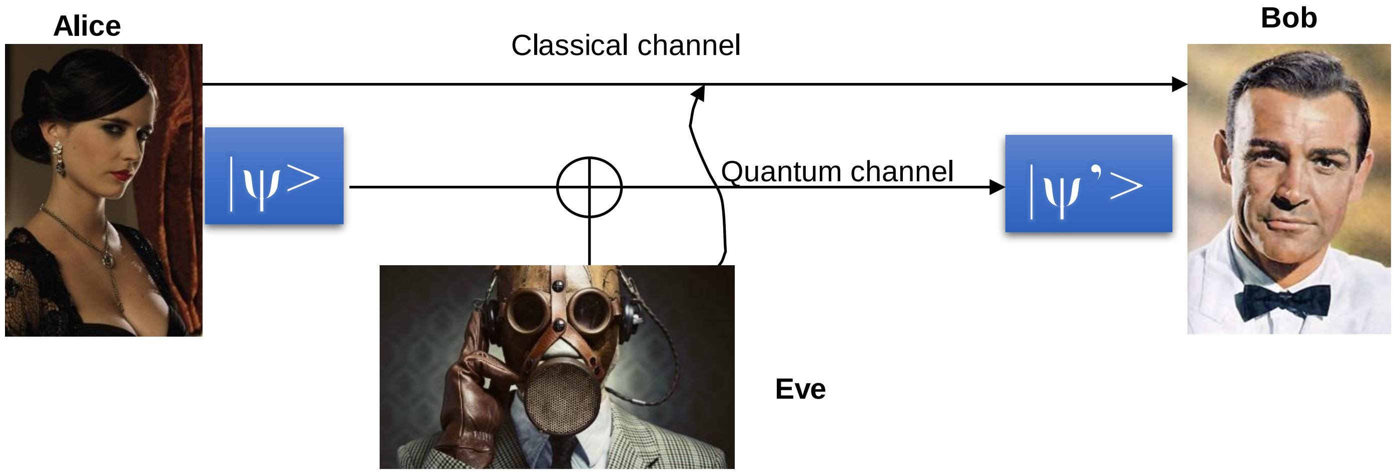
- *A. Duplinskiy, V. Ustimchik, A. Kanapin, V. Kurochkin, Y. Kurochkin. Low loss QKD optical scheme for fast polarization encoding // Opt. Express 25(23), 28886-28897 (2017).*

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



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

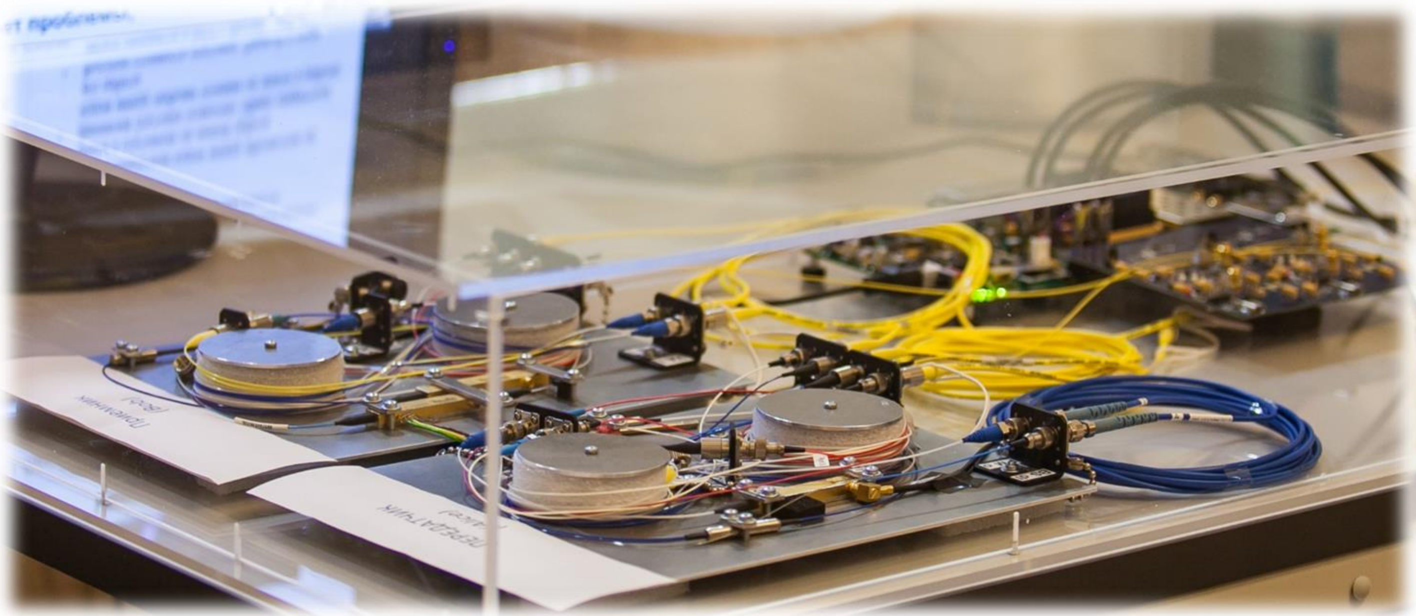
I_{AE} large: 

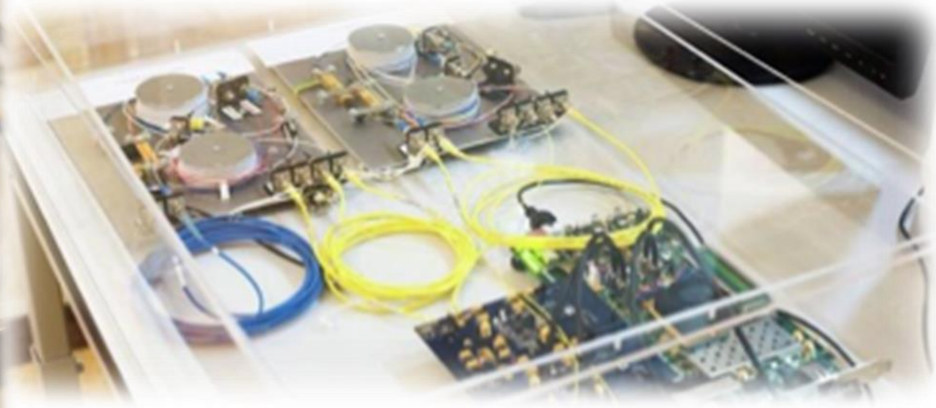
Experimentalists: to maximize I_{AB}

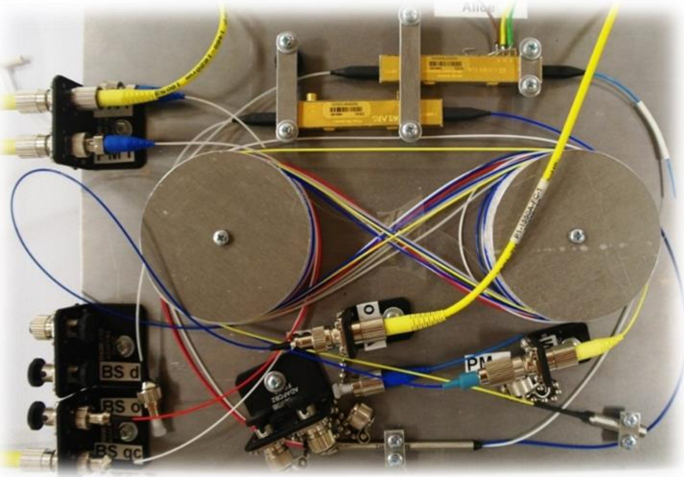
Theorists: to quantify I_{AE}

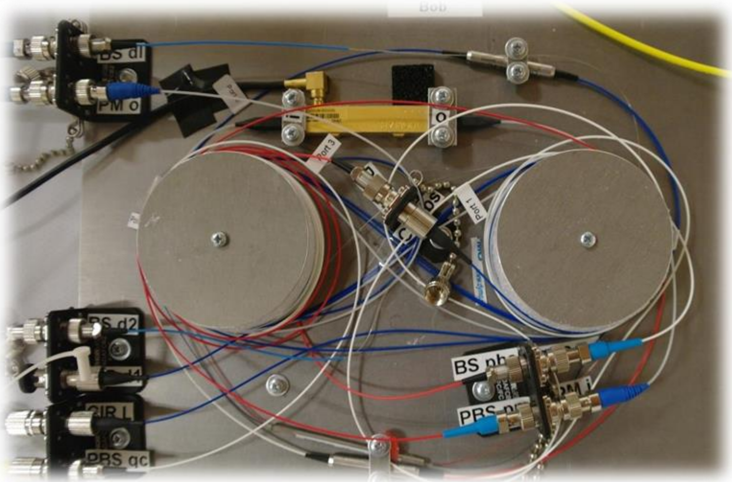
- New protocols -> higher tolerance to noise, bit rate and distance growth
- New methods to prepare and measure states -> reduce size and cost
- Security analysis and attacks -> search for good model of non-ideal components

How it looks









Secure now.
Secure in the future.

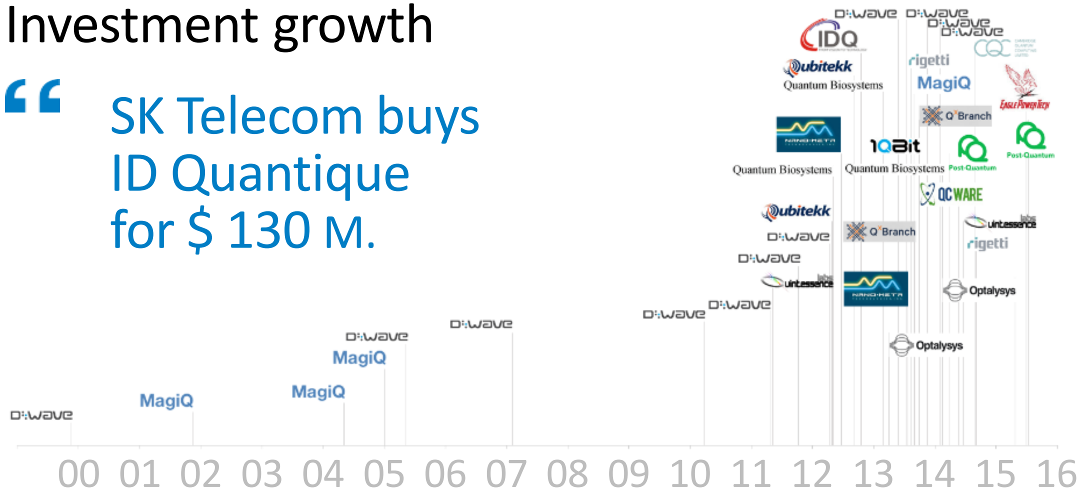
New market – new possibilities

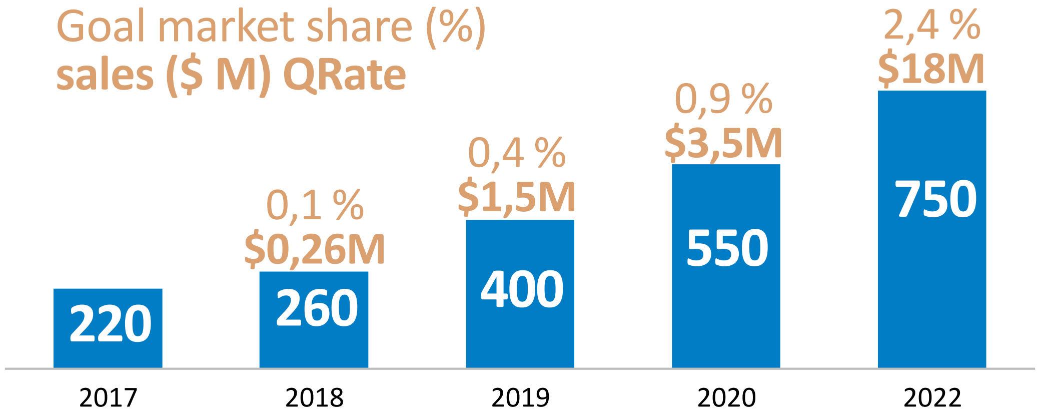
Today QKD market is the startup market

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]

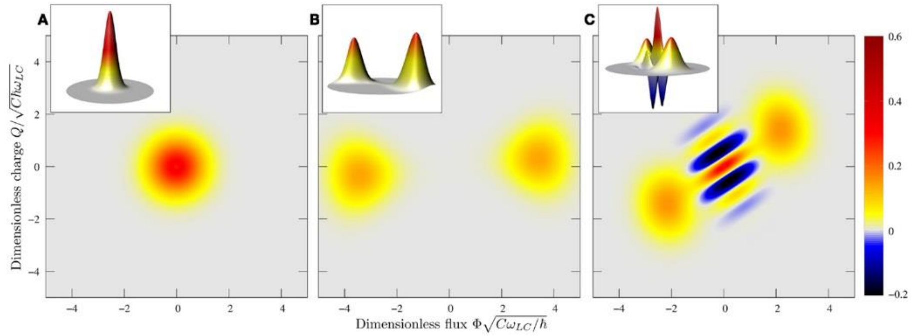
[1] **Markets&Markets**: Quantum cryptography market - 2017 to 2022

Optical implementations of a qubit

- **Single-rail qubit**

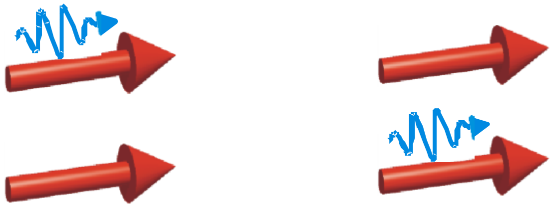
$$|0_L\rangle = |0\rangle \qquad |1_L\rangle = |1\rangle$$

CW qubits



- **Polarization qubit great for BB84 protocol**

- Dual-rail qubit

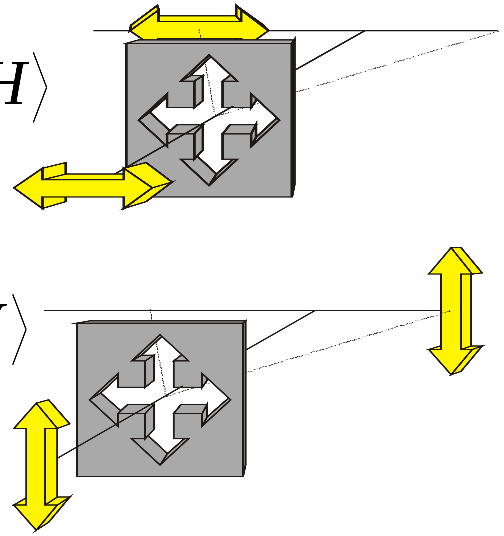


$$|0_L\rangle = |1,0\rangle \qquad |1_L\rangle = |0,1\rangle$$

Polarizing beam splitter

$$|0_L\rangle = |H\rangle$$

$$|1_L\rangle = |V\rangle$$



What methods of encoding you can propose?
Can we encode more than one bit?

States prepared by Pockels cell

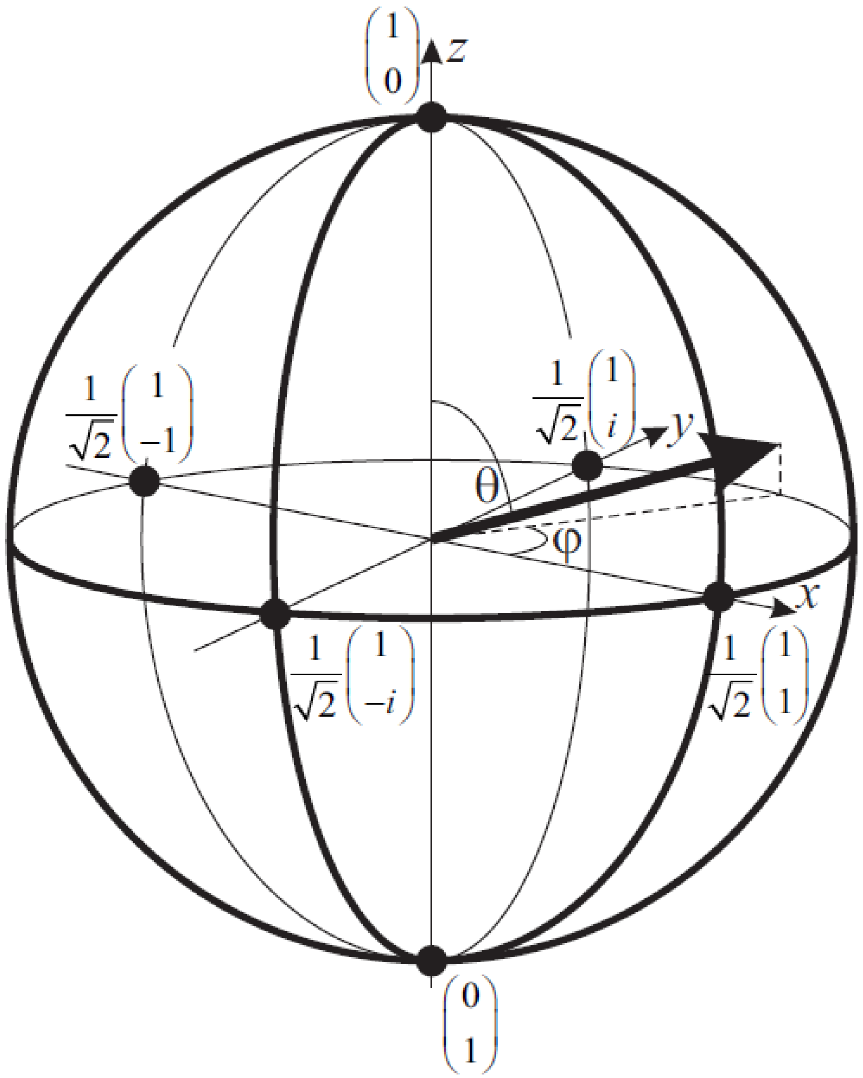
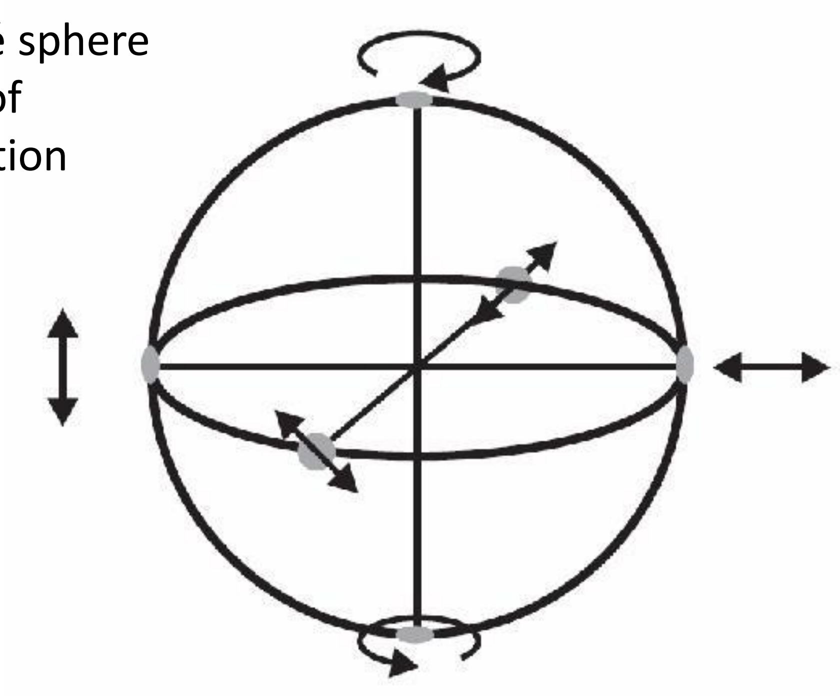
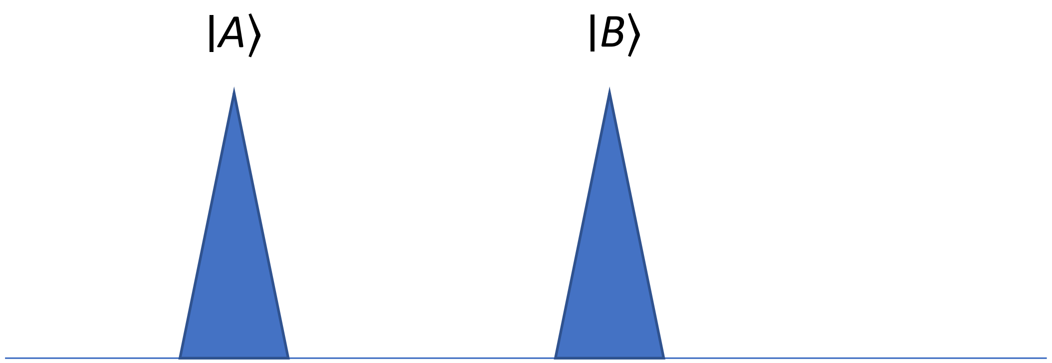


Figure 6.3: The Bloch sphere.

Poincaré sphere
in case of
polarization





|0⟩=|A⟩+|B⟩
Other combinations?

We're looking for talents!

Yury Kurochkin
yk@goqrate.com

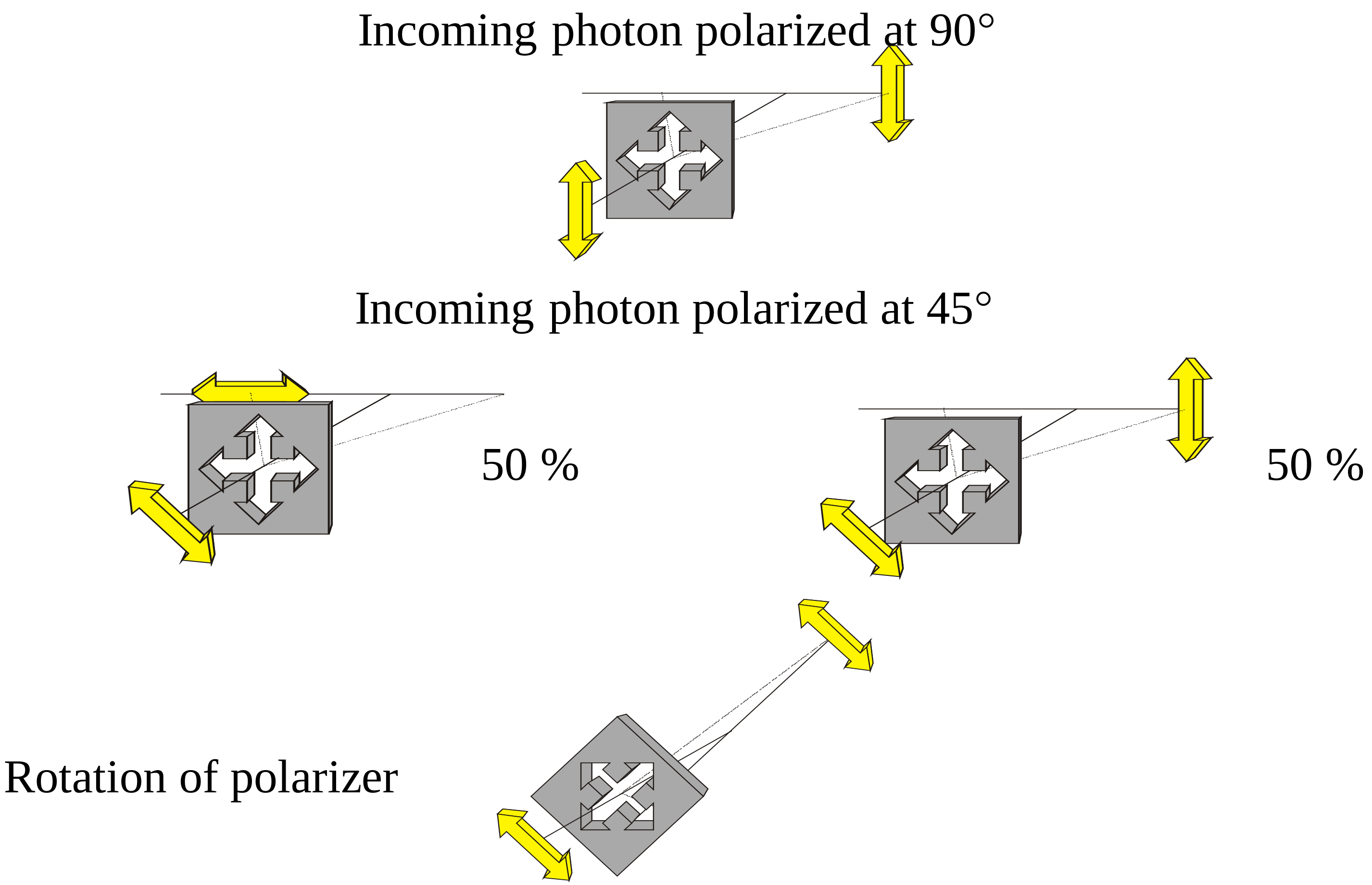
QUANTUM COMMUNICATIONS

GAZPROMBANK

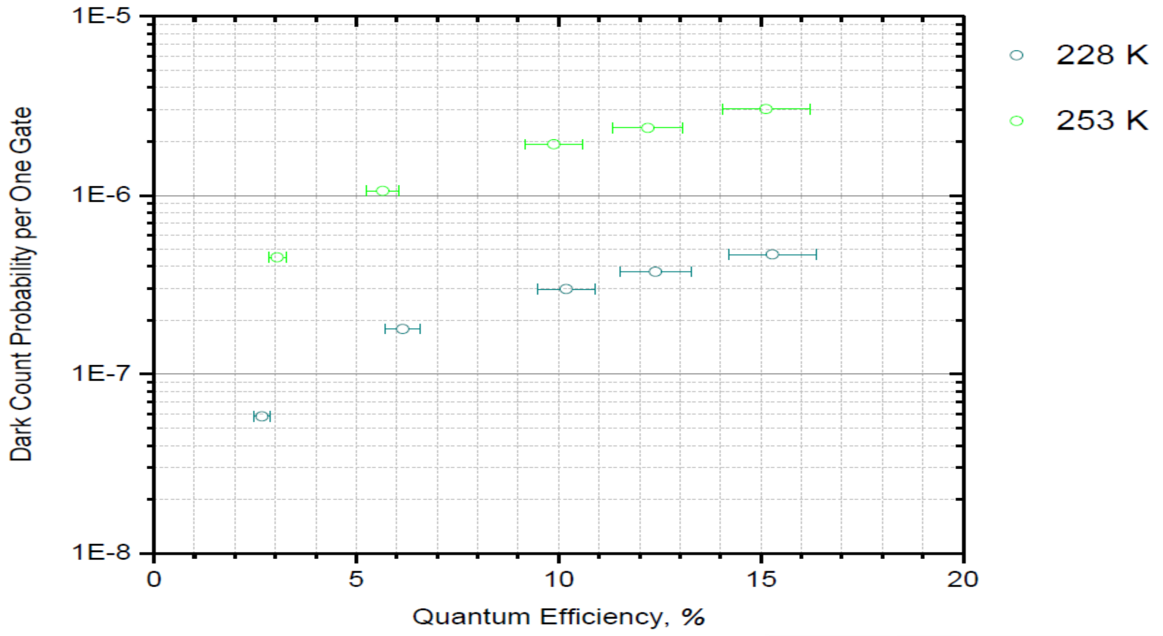
RQC Russian Quantum Center

MINISTRY OF
EDUCATION AND SCIENCE

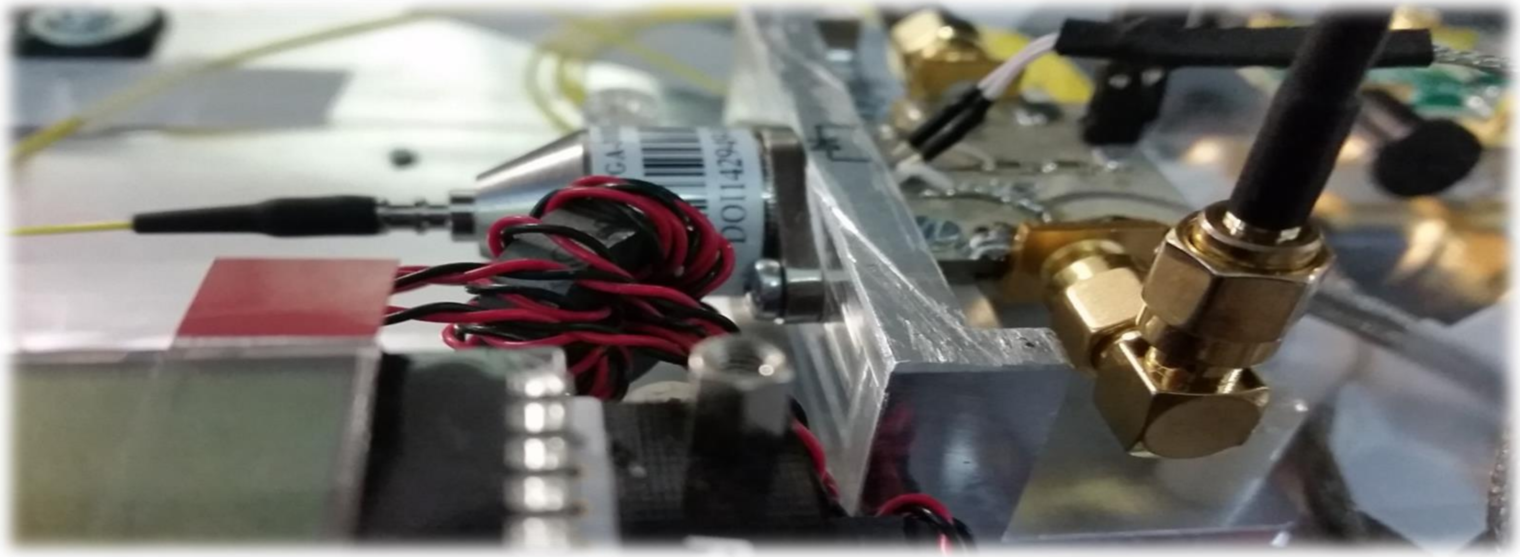
Irreversibility of Measurements



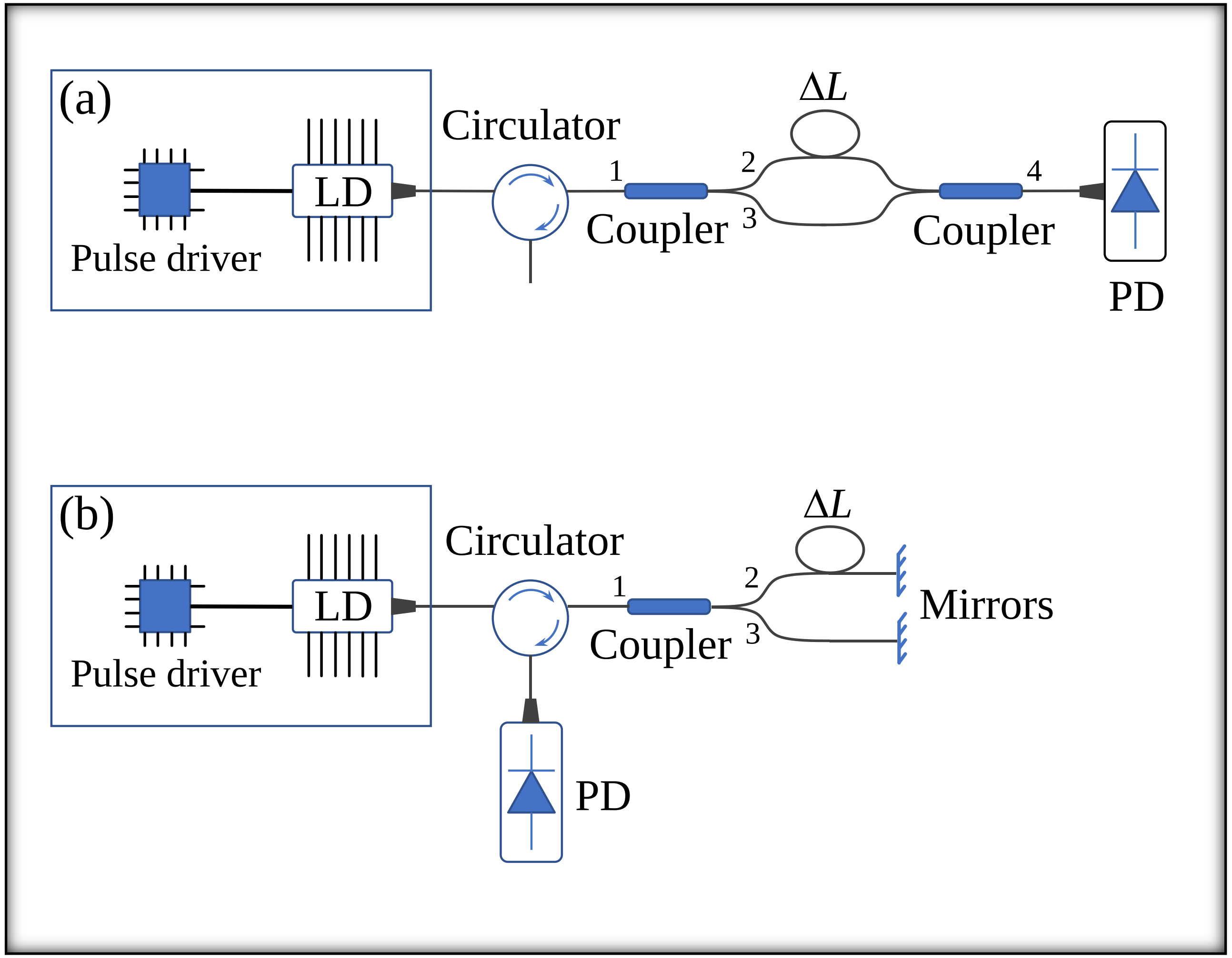
Детектор одиночных фотонов – ключевой элемент

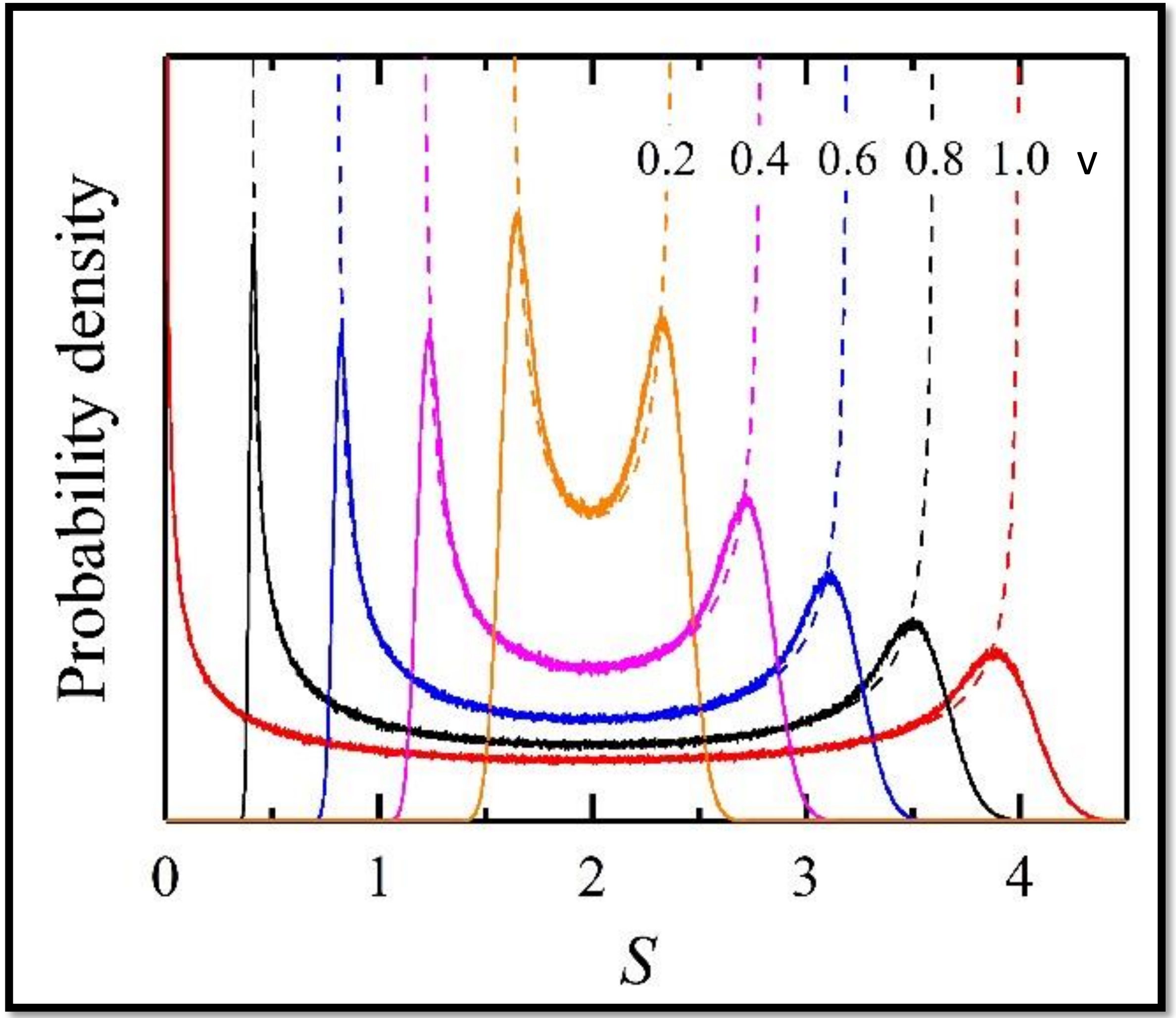


- Квантовая эффективность 10%
- Шумы 3*10^(-7)
- Частота повторения стробов 300 MHz.
- Ширина окна приема сигнала 400 ps



High bit rate quantum random number generator

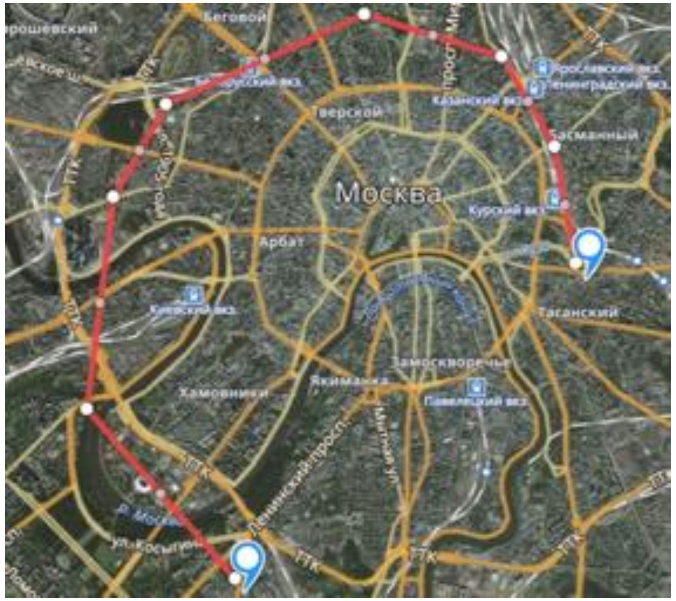


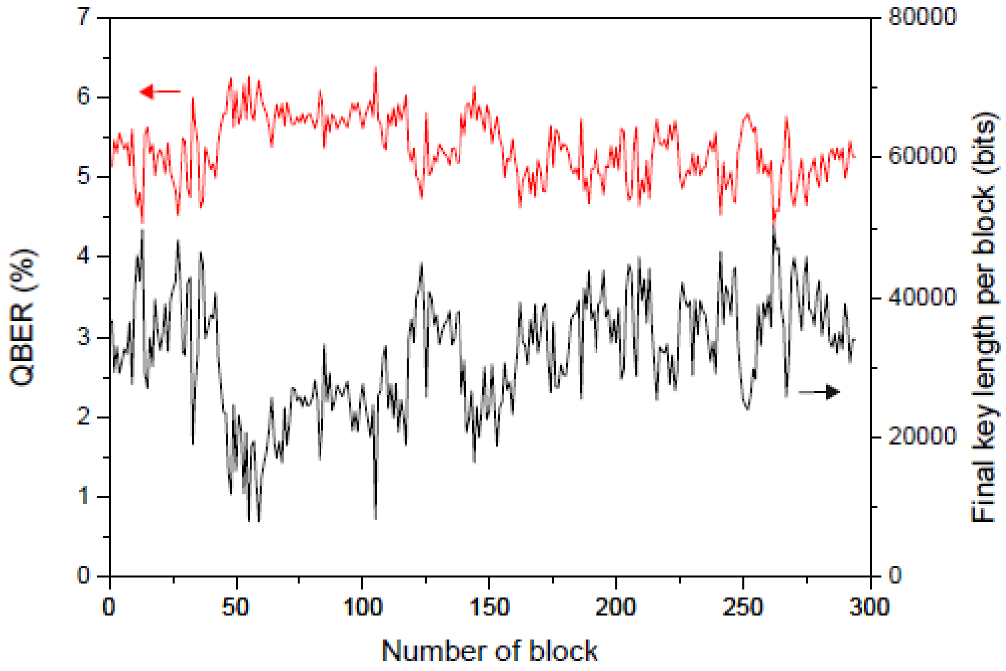


2017-2018 Sberbank field tests

VPN

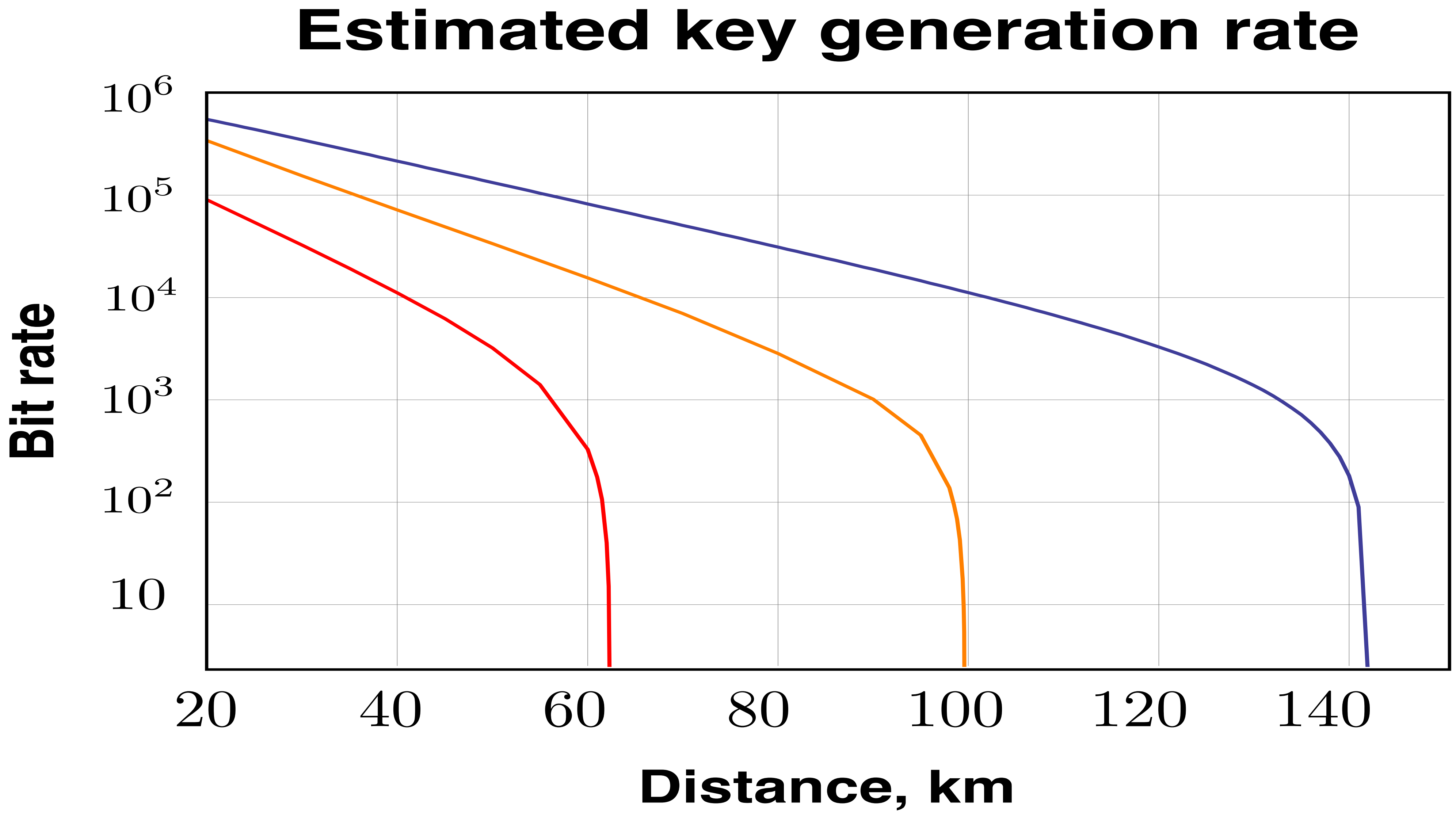
25 km, 14 dB loss.





- 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.

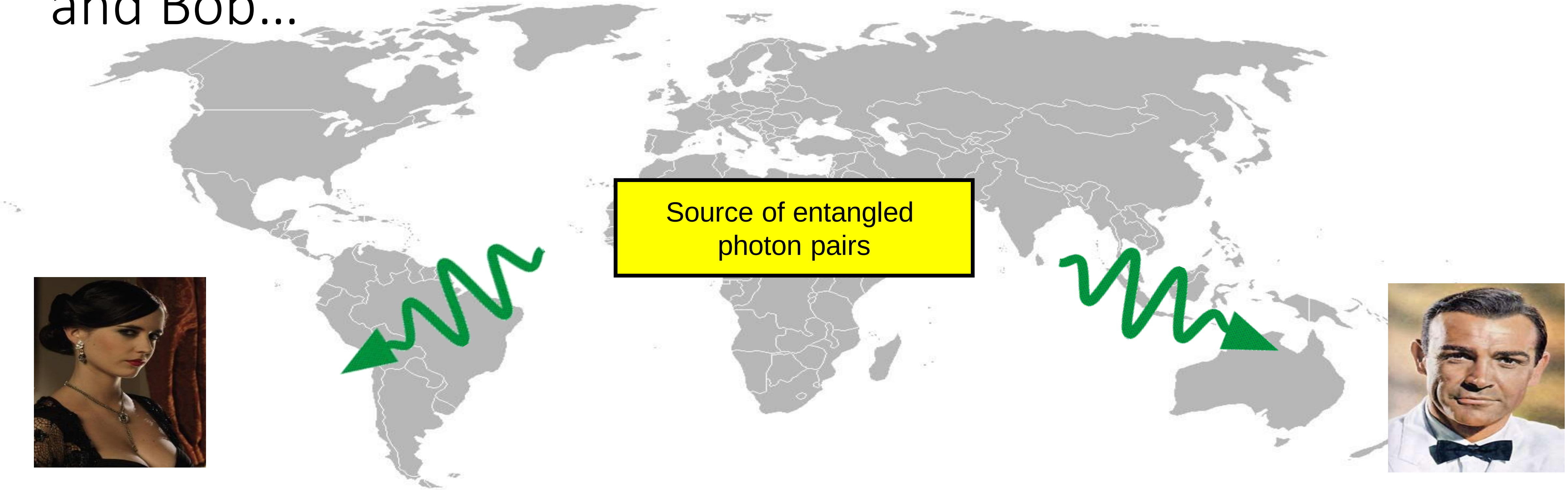
QKD distance limit is driven by exponential loss



Quantum repeaters

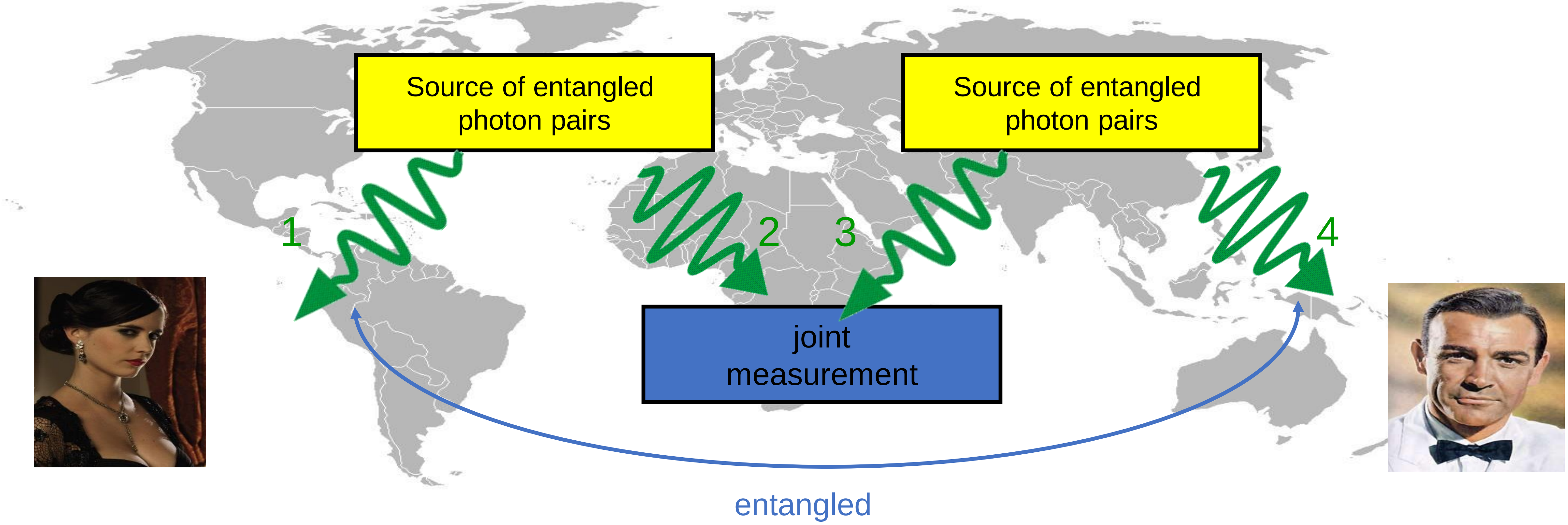
- Problem: to get 1 photon after 1000 km line you need to make a 10^{20} ts what is not practical
- Practical distances are within 100 km in the external lines and within 400 km in the lab (less than 1 bit/s)
- Solution comes from classical communication, we need a repeater
- What is a repeater
  - Device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



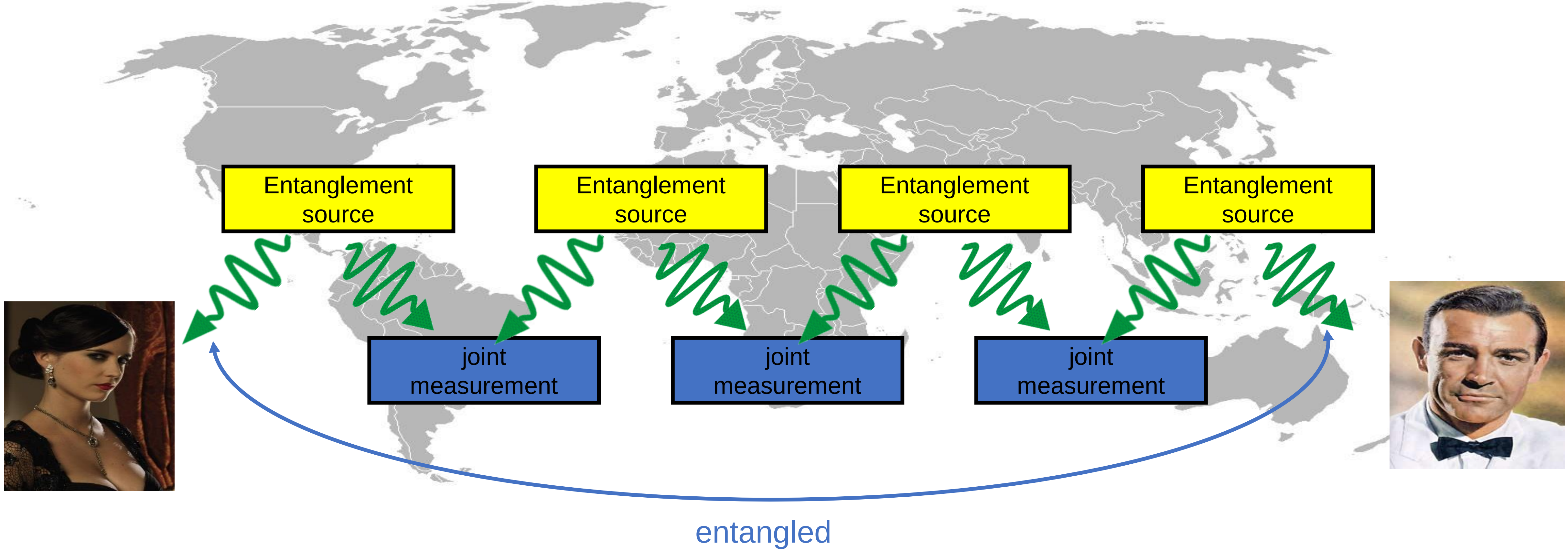
The photons are likely to get lost on their way

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

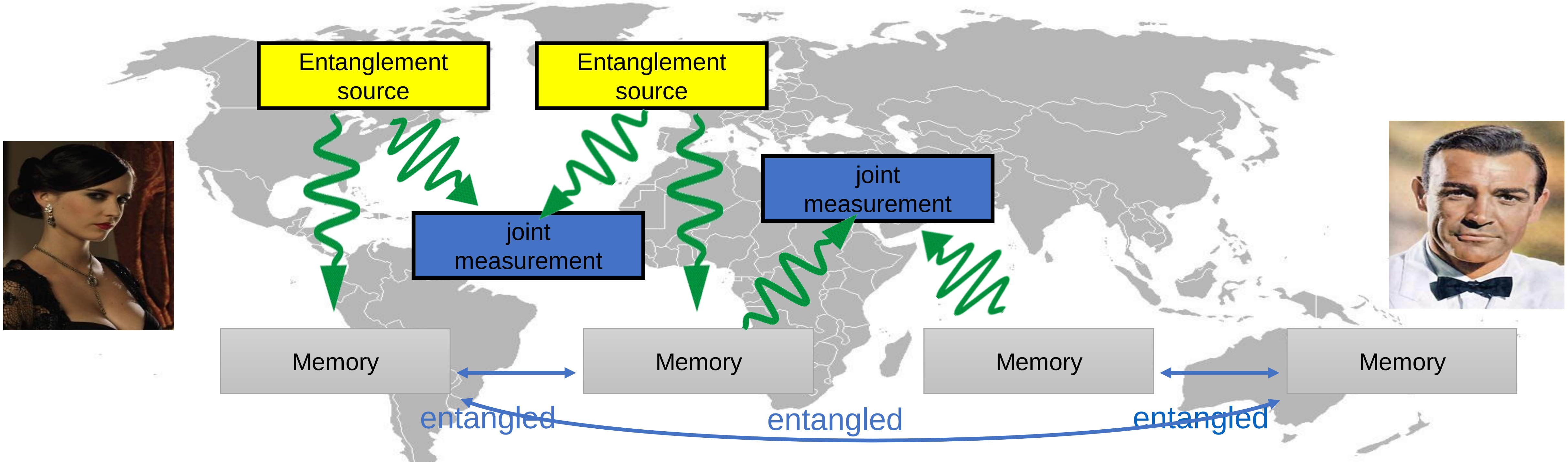


Long-distance entanglement can be created by *entanglement swapping*

but to succeed, all links must work simultaneously.

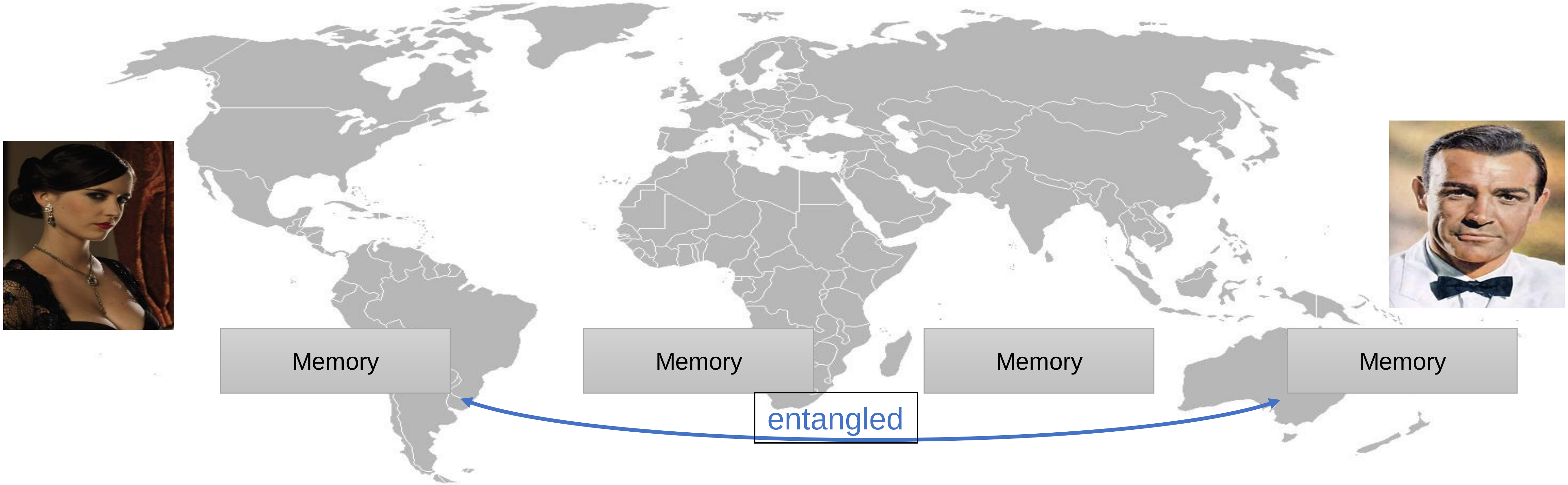
→ success probability still decreases exponentially with distance.

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.