Experimental Quantum Key Distribution

QRATE
QUANTUM COMMUNICATIONS

MISIS
National University of Science and Technology

ROSATOM

RQC Russian Quantum Center

Sirius University

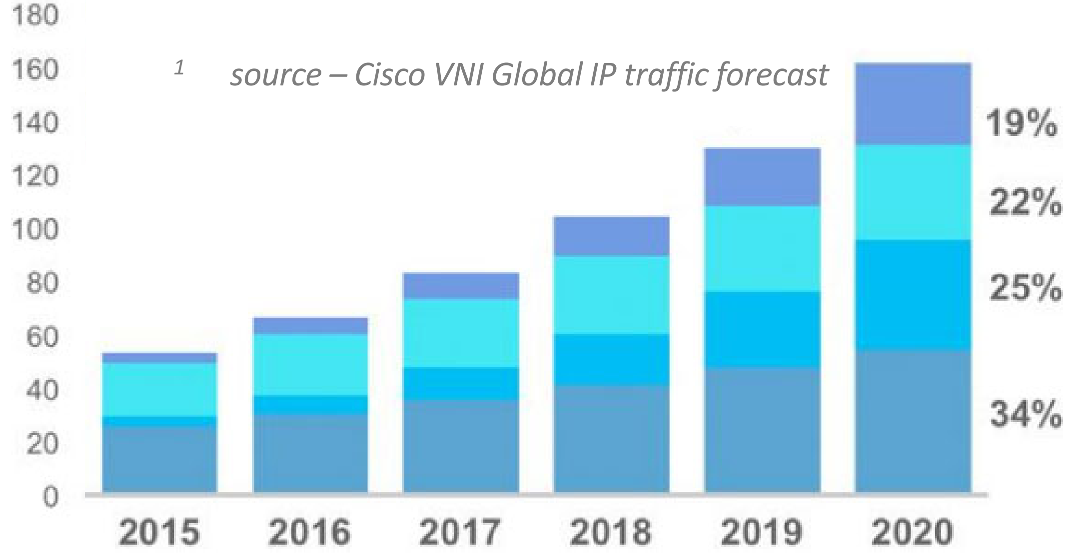
Yury Kurochkin, Director of NTI Quantum Communication Center in MISIS

“Huge” data

Data traffic growth in last 5 year:

All x3

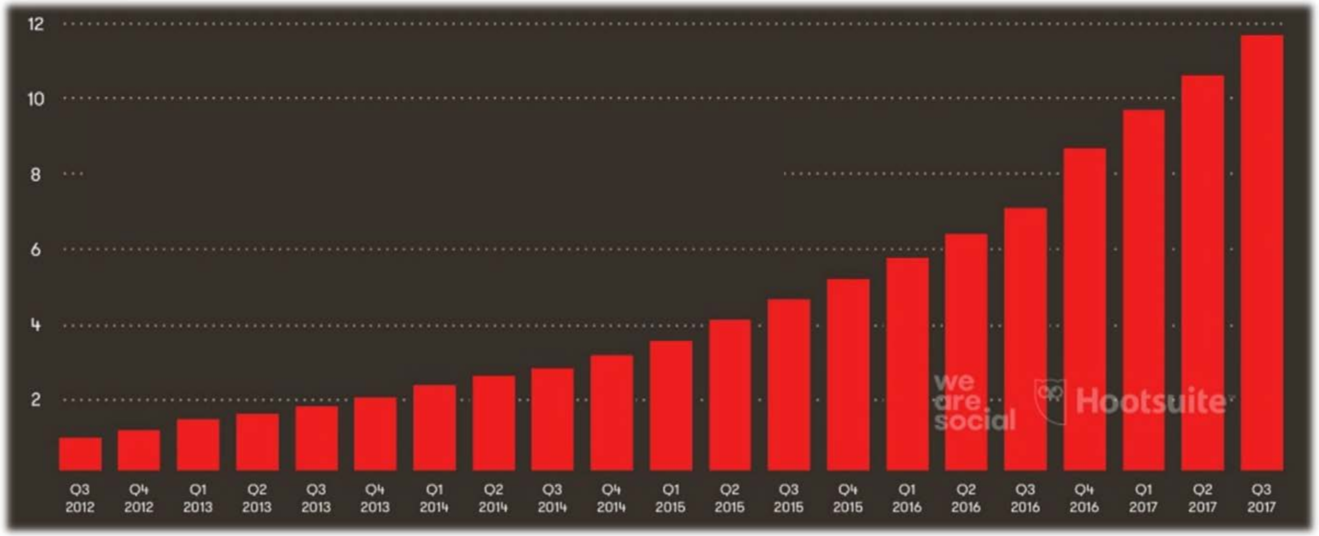
Global Internet traffic, exabytes/month and CAGR, %



- mobile data
- fixed/wired
- fixed/ Wi-Fi from mobile devices
- fixed / Wi-Fi from wi-fi only devices

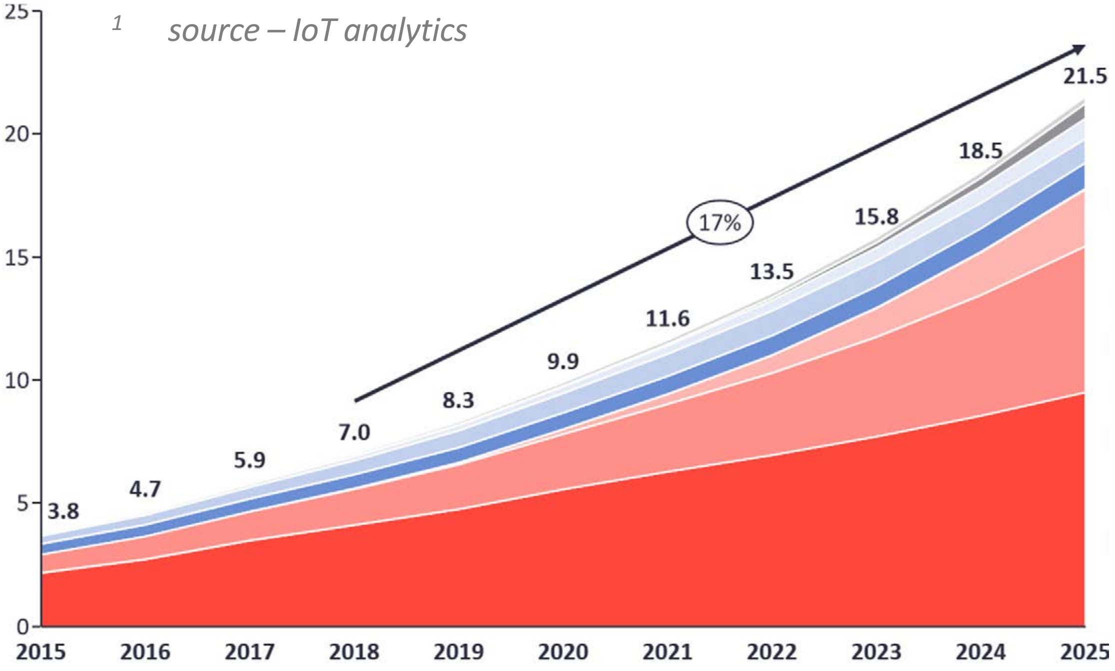
Mobile x12

Global mobile data, exabytes/month



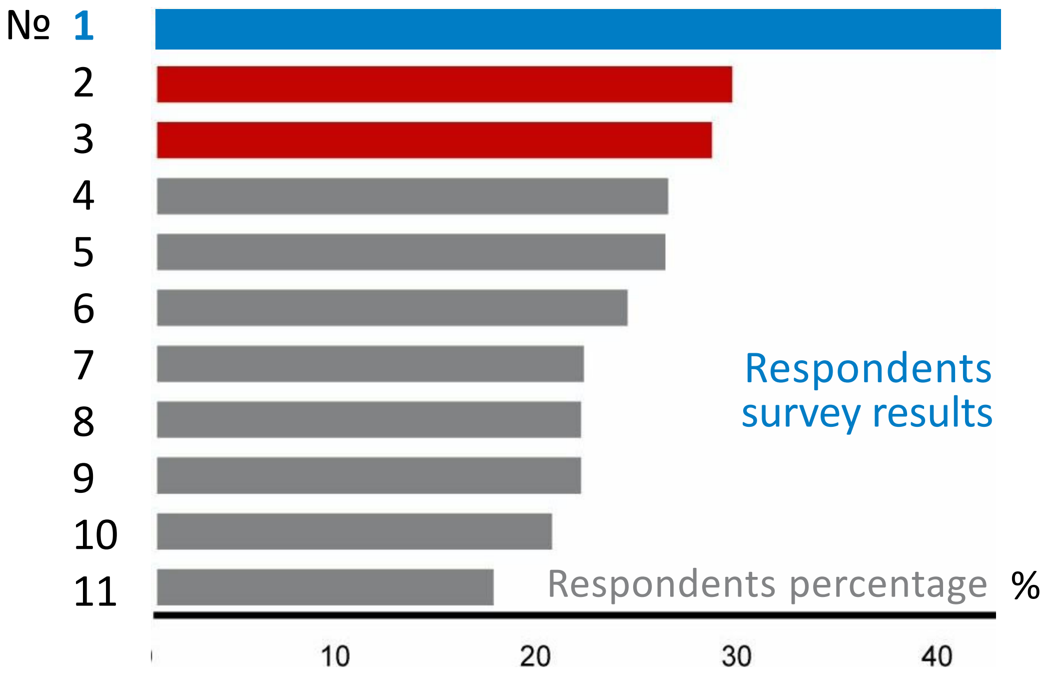
“Ocean” of devices

Global number of connected IoT devices, mn [1]



- WNAN (Wireless Neighborhood Area Network)
- 5G
- other
- cellular / M2M
- wired
- LPWA (Low-power Wide-area Network)
- WLAN (Wireless Local Area Network)
- WPAN (Wireless Personal Area Network)

Barriers, limiting adoption of IoT solutions [2]



1 - security
2 - IT/OT integration
3 - unclear ROI
4 - technical expertise
5 - interoperability
6 - data portability
7 - vendor risk
8 - transition risk
9 - legal/regulatory issues
10 - network constraints
11 - vendor lock-in

2 source – Bain IoT customer survey 2016

QRATE QUANTUM COMMUNICATIONS

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"

QRATE
QUANTUM COMMUNICATIONS

Cryptography new challenges

Quantum computer threat becomes real in 5-7 year –
existing crypto-algorithms with open key will loose their strength

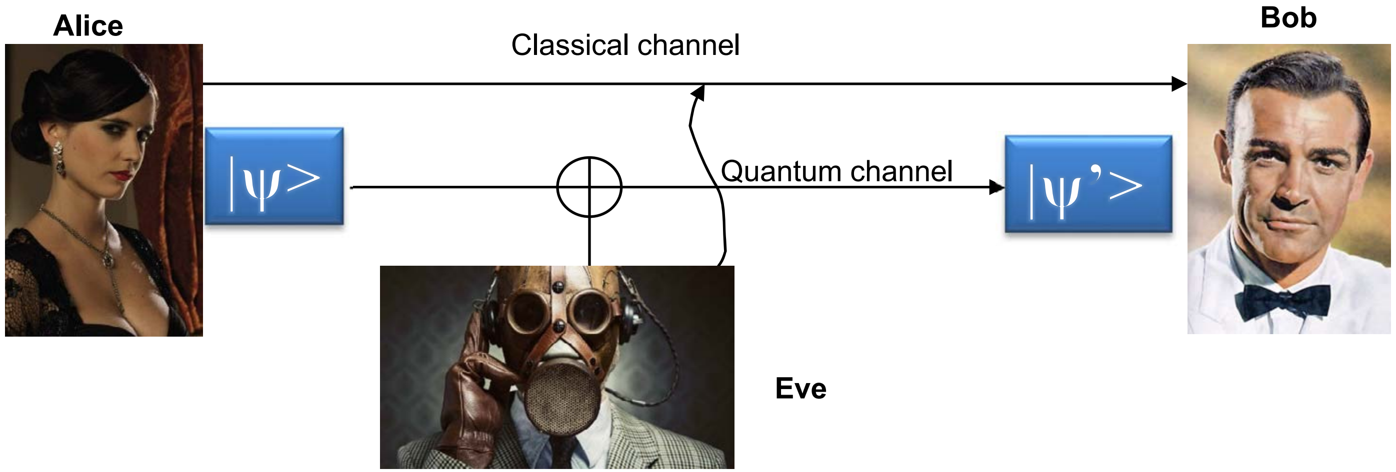
Sensitive data with 10+ years of guaranteed storage –
“hacking from the future” (data should be copied and encrypted today, then kept until de-encryption methods are ready)

As much data coming (traffic x2 per year) –
need to change keys more often

Number of IoT devices is rapidly growing (CAGR ≈20%) –
need oceans of new keys (Root-of-Trust)

Distributed computing hardware becomes more affordable (for instance, mining farms) –
anyone can build specialized highly-efficient crypto-equipment

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: STOP

Experimentalists: to maximize I_{AB}

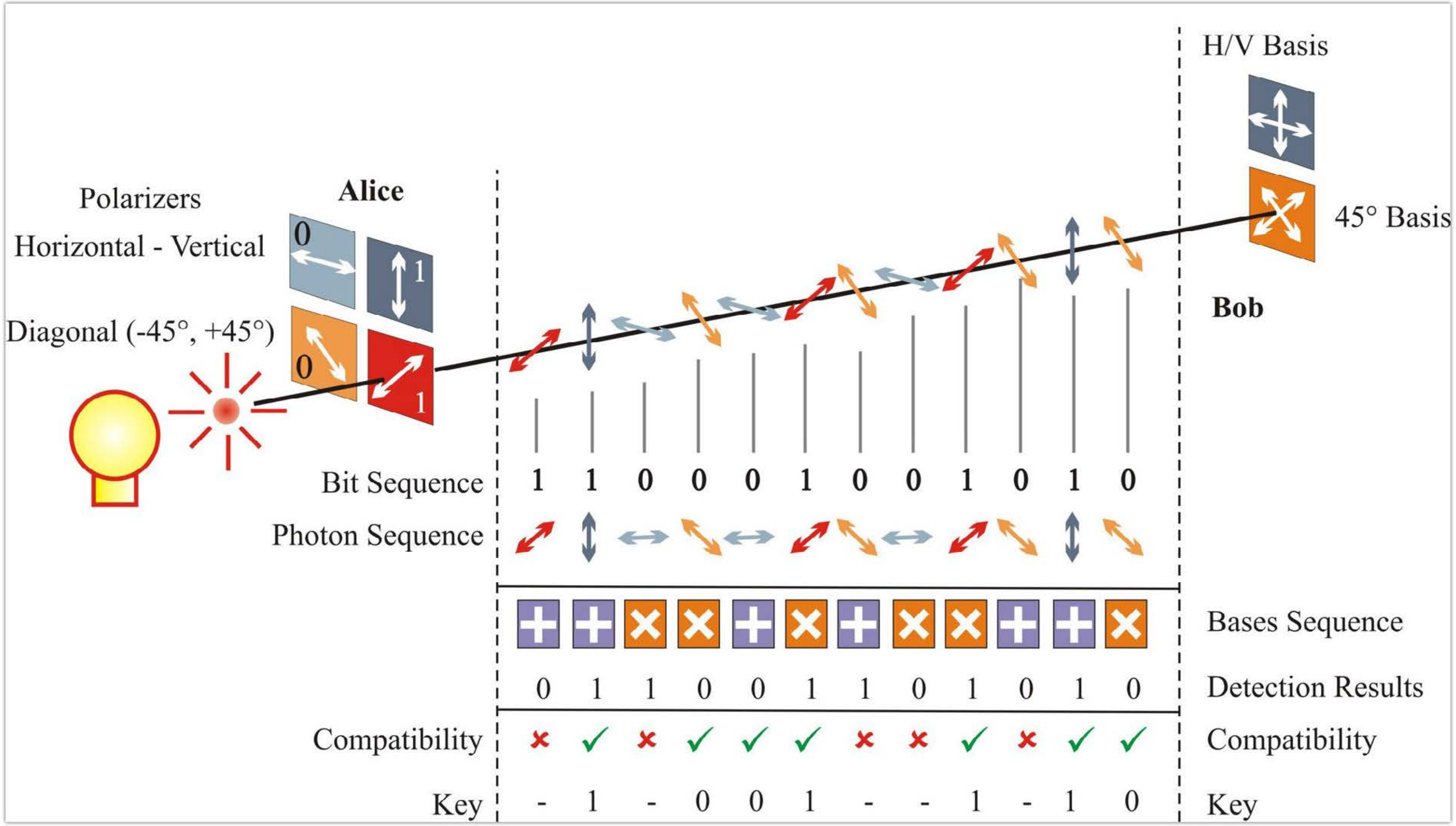
Theorists: to quantify I_{AE}

New protocols -> higher tolerance to noise, bit rate and distance growth

New methods to prepare and measure states -> reduce size and cost

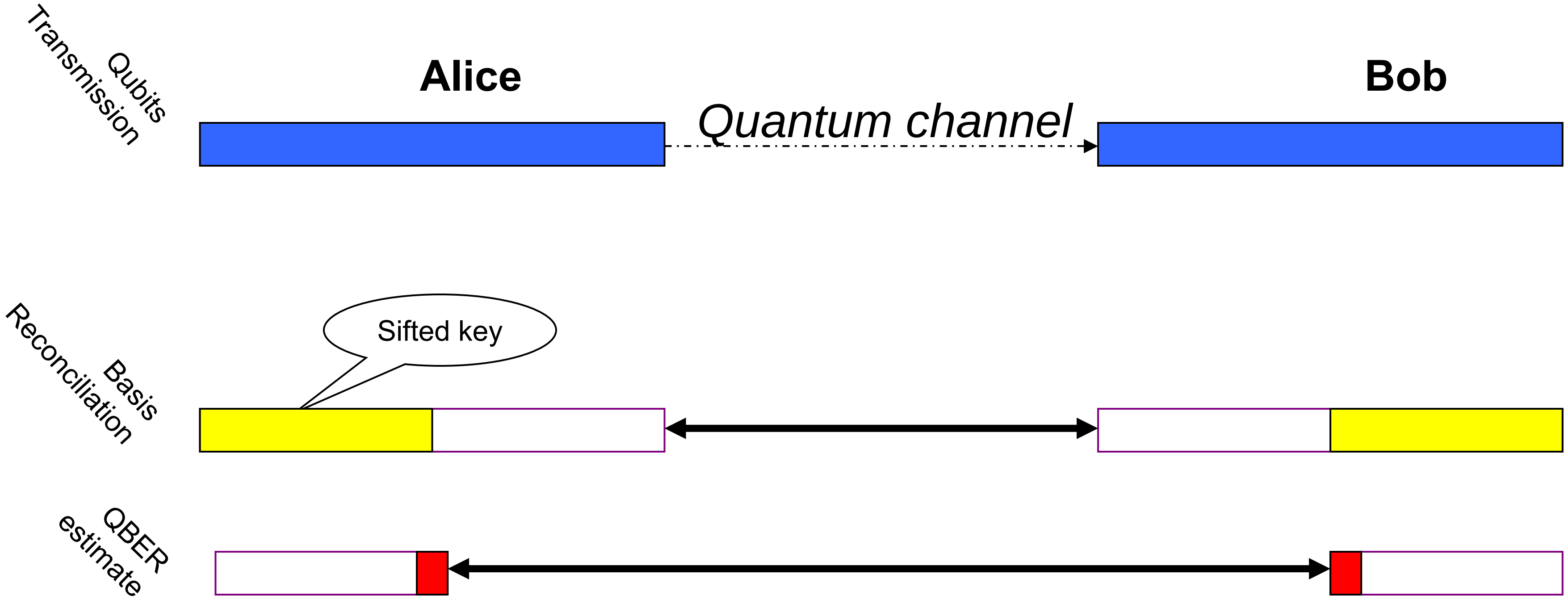
Security analysis and attacks -> search for good model of non-ideal components

BB84 is the first and most popular protocol



QUANTUM COMMUNICATIONS

Key Distillation (ideal case)



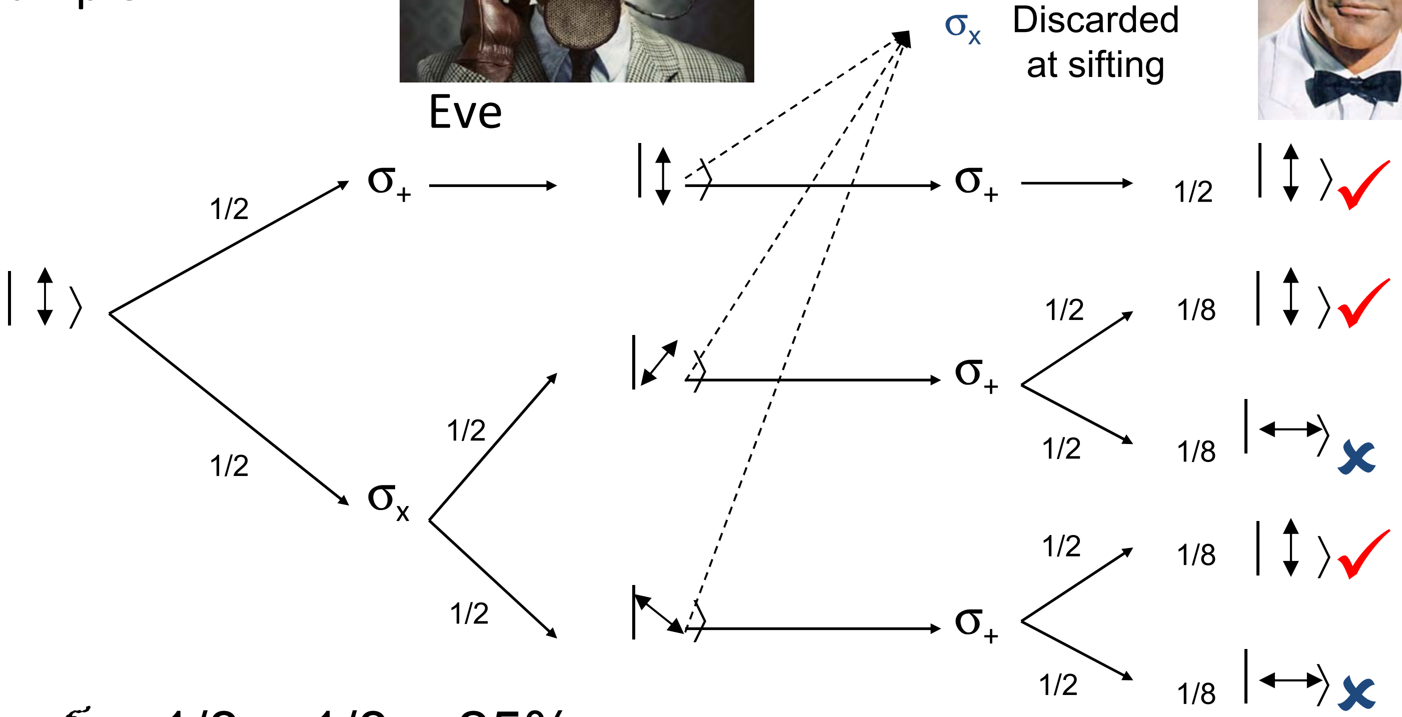
$$\text{QBER} = \begin{cases} 0 : \text{no eavesdropping} \\ > 0 : \text{eavesdropping} \end{cases}$$

Reveals rather than prevents eavesdropping

A better name: **quantum key distribution**

Eavesdropping (1): Intercept and resend

Simplest attack: example



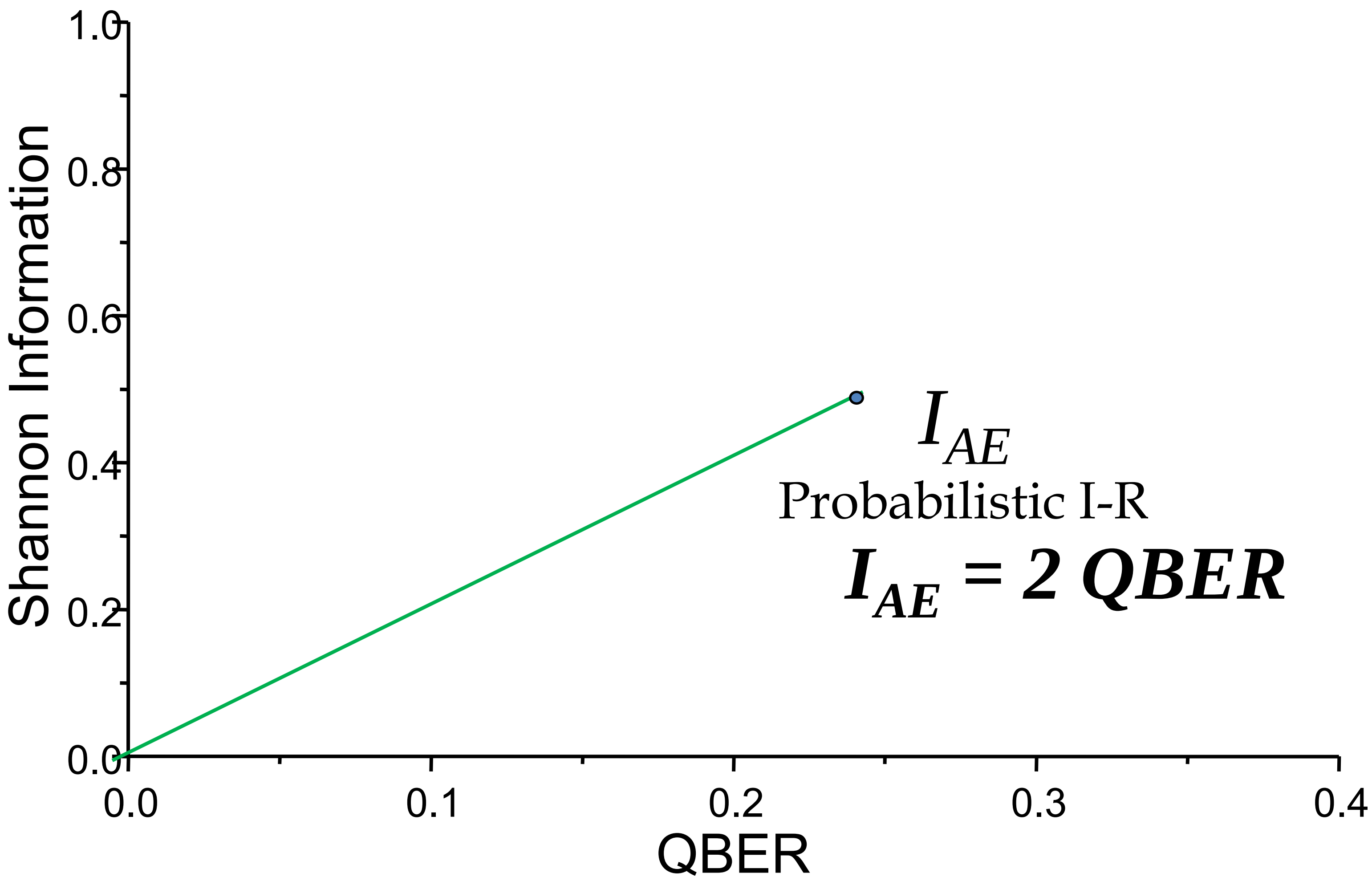
QBER = $\mathcal{D}$ = 1/8 + 1/8 = 25%

$I_{AE} = 2\ QBER$

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

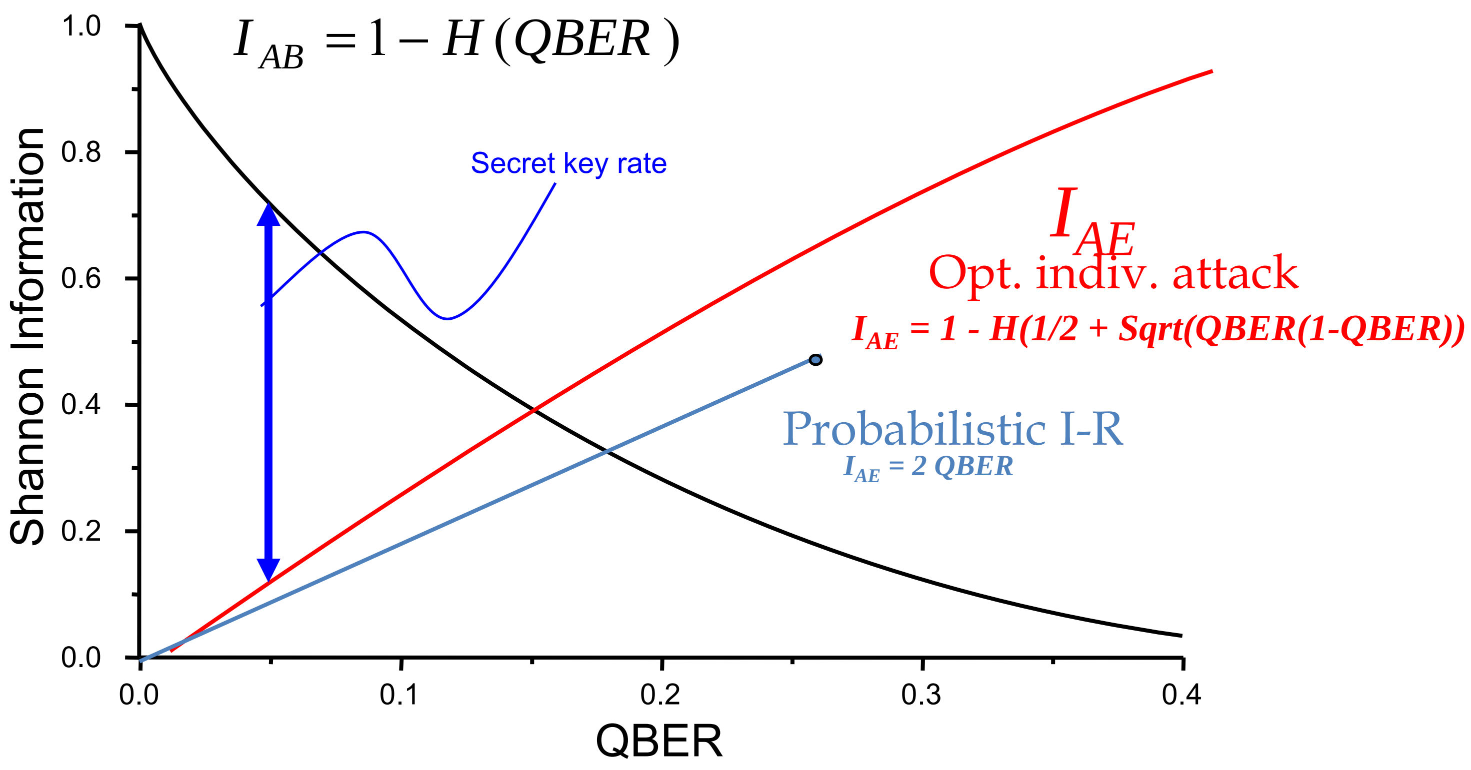
QRATE
QUANTUM COMMUNICATIONS

Incoherent attacks: information curves



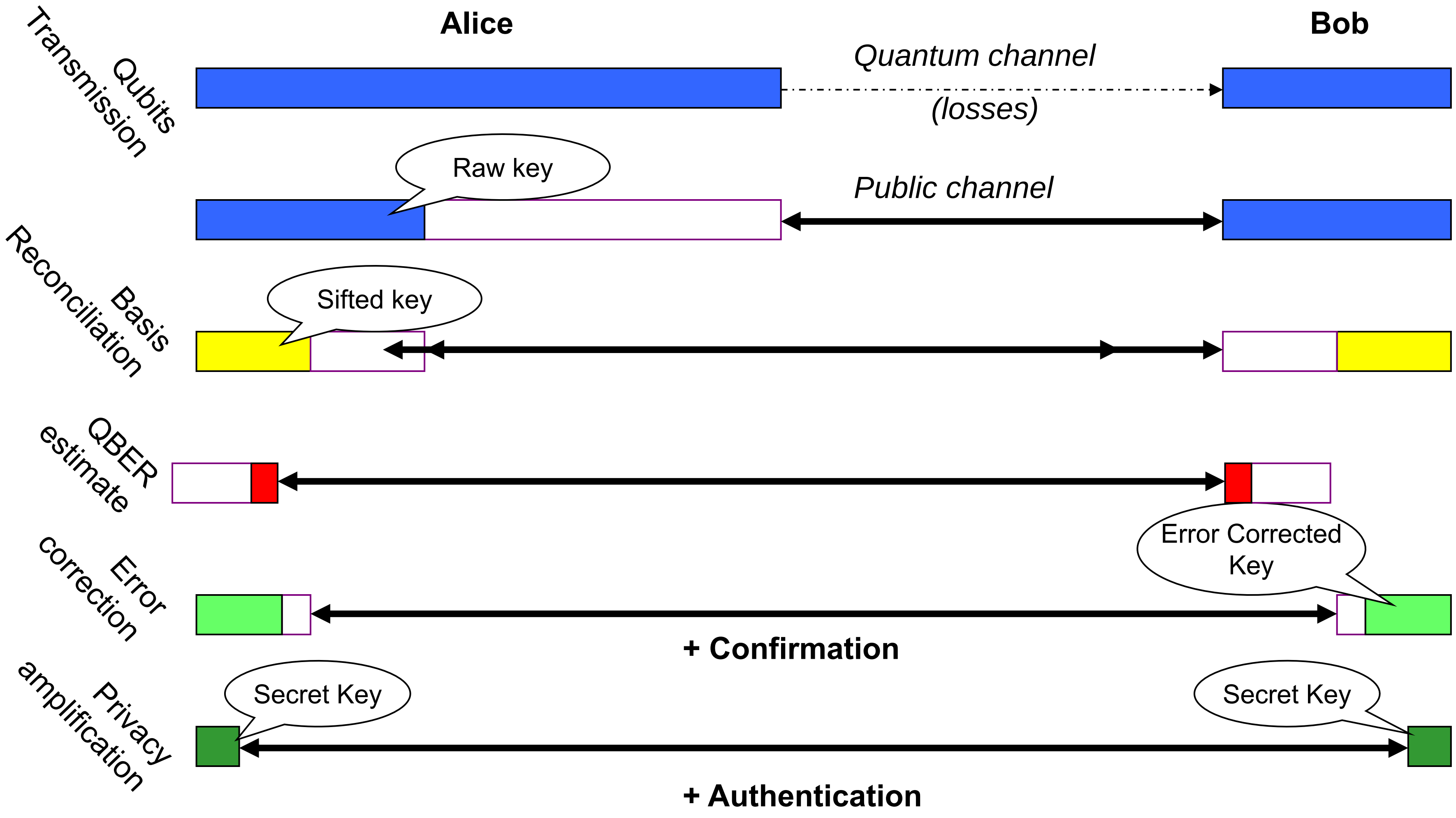
Information Theory and QKD

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

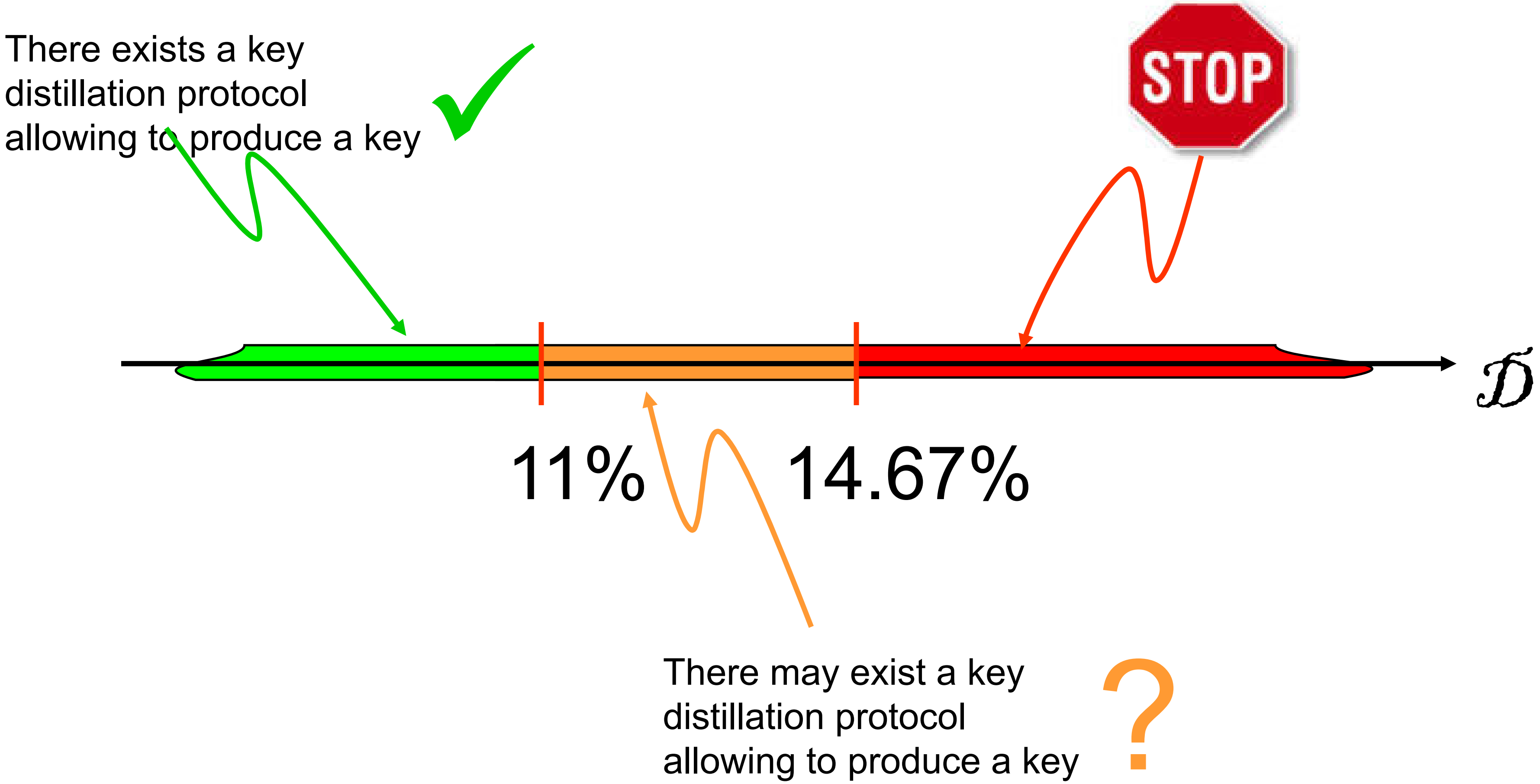


QRATE QUANTUM COMMUNICATIONS

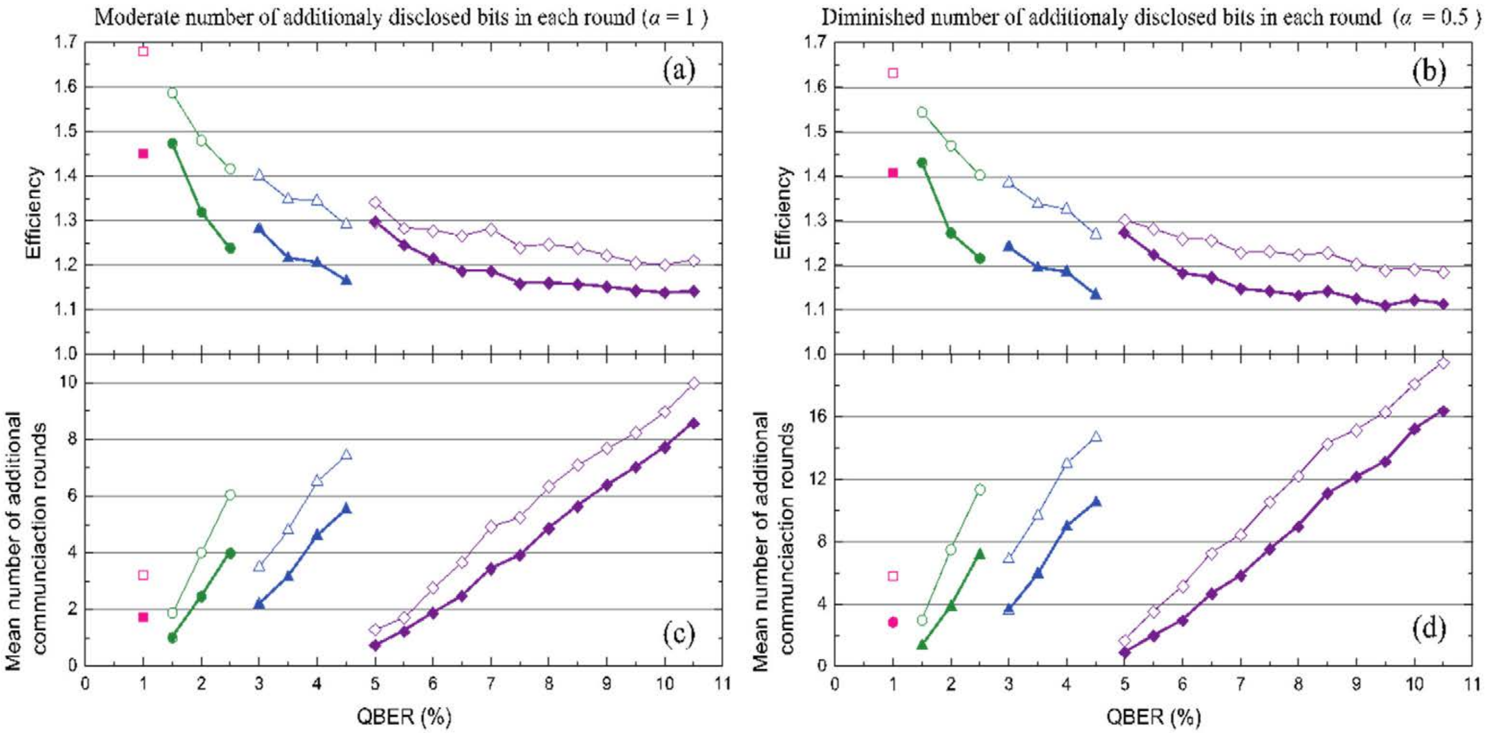
Key Distillation (realistic case)



Summary (single-photons)



Developed the advanced platform for processing quantum keys



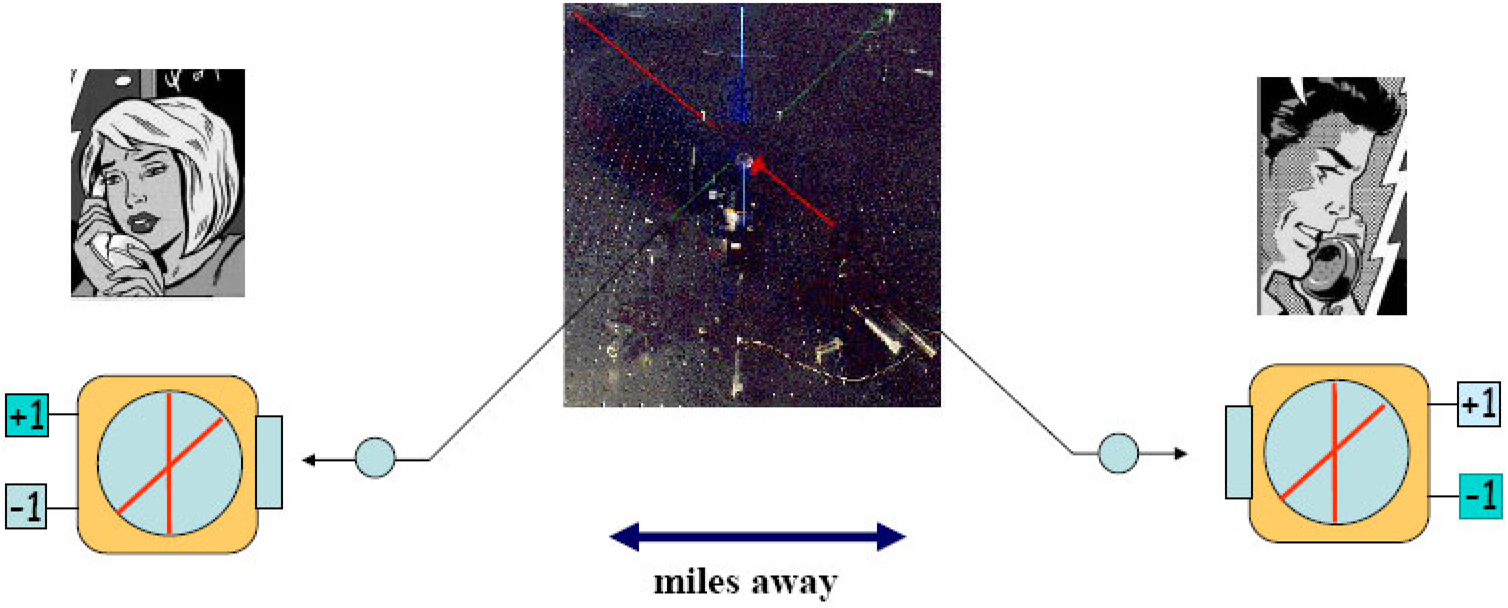
The most significant result is the creation of a record-breaking error correction algorithm. It exceeds the existing algorithms by an average of 10% in efficiency. It saves up to 30% of communication resources.

Common laboratory with SMI

The processing platform works In Open-Source mode

QRATE QUANTUM COMMUNICATIONS

Entanglement scheme



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

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

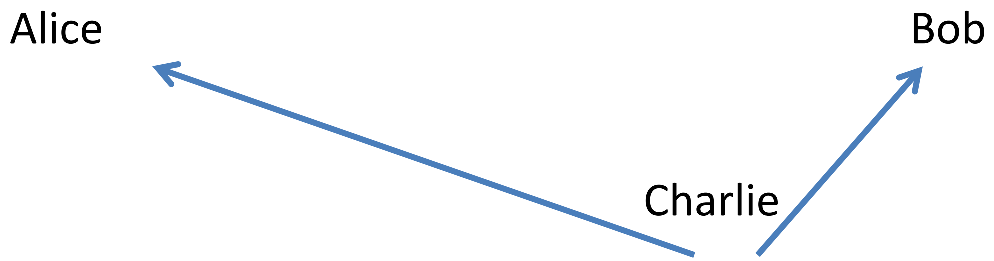
Where $|H'\rangle, |V'\rangle$ are the 45 degree Polarization

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

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

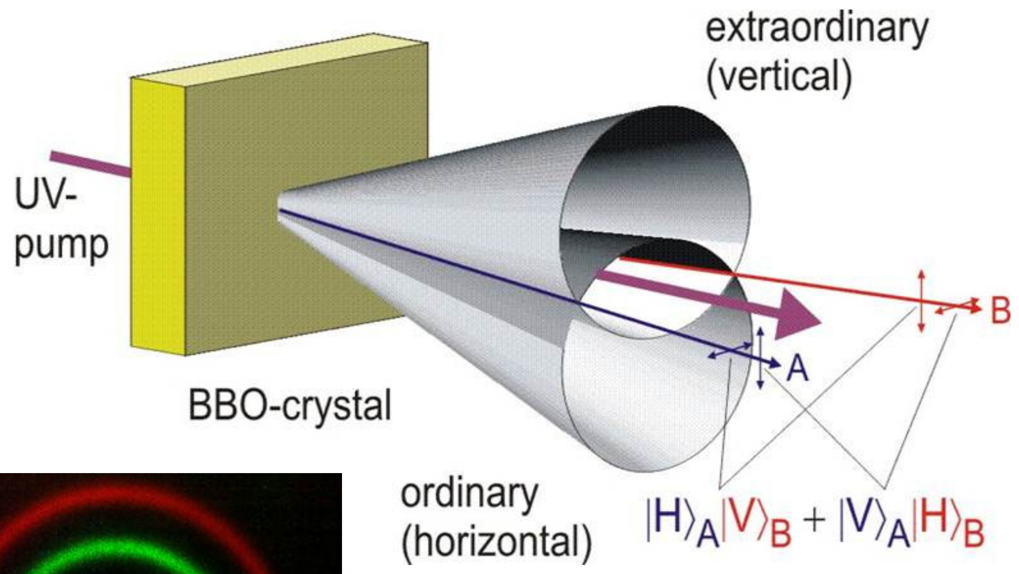
[A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991)]

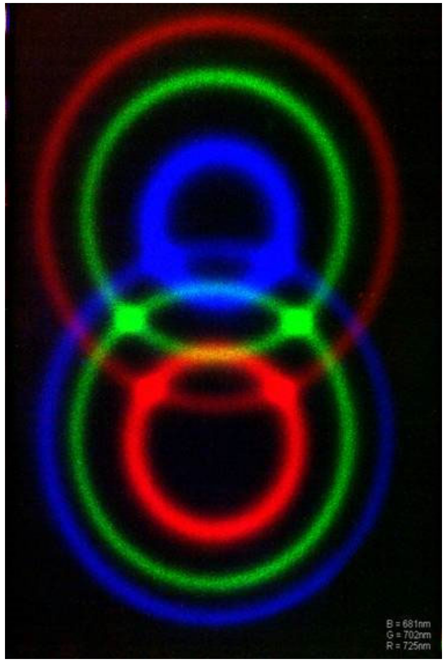
Ekert protocol and realization



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

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



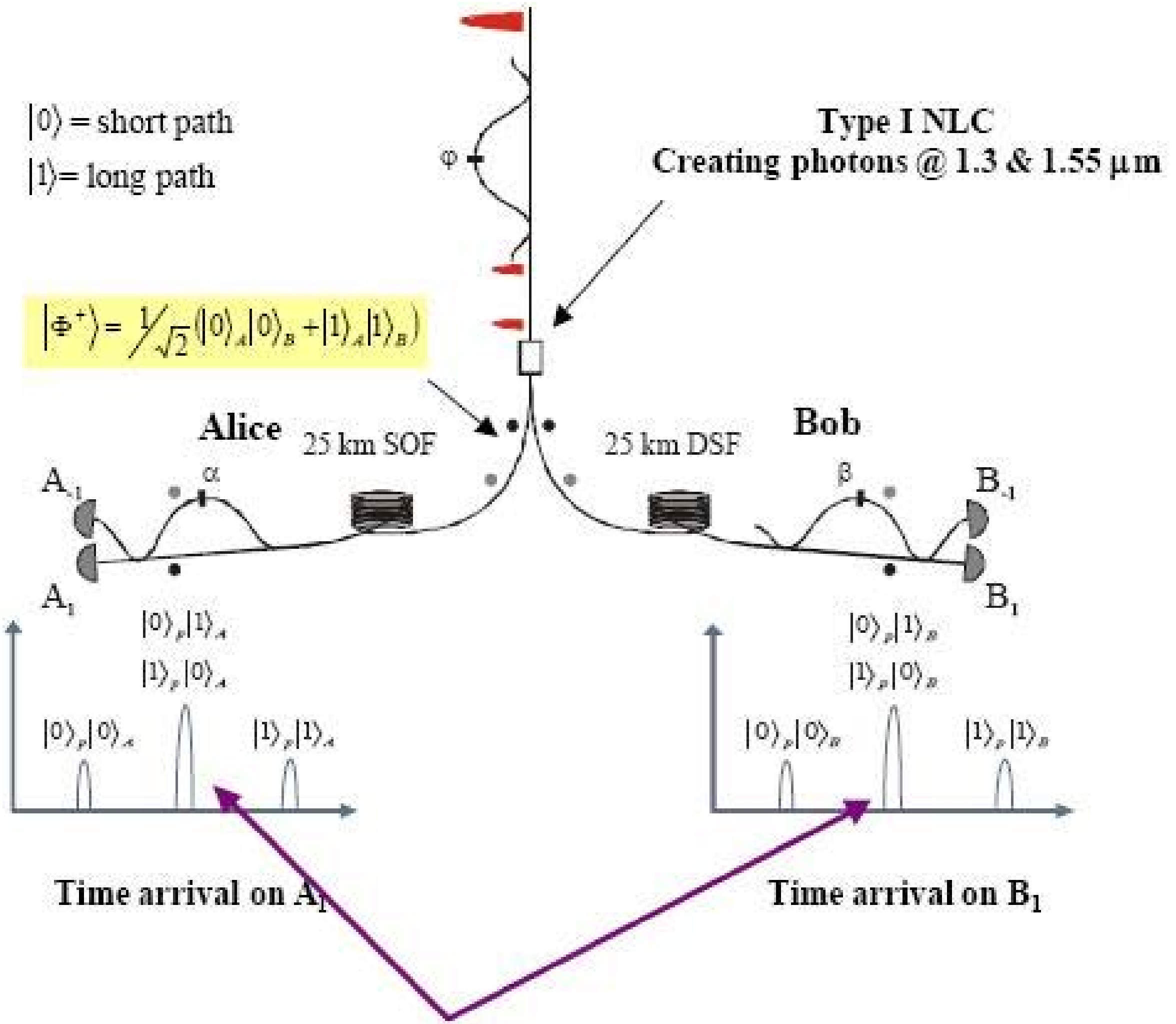


$$|\Phi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1 |H\rangle_2 \pm |V\rangle_1 |V\rangle_2\right)$$

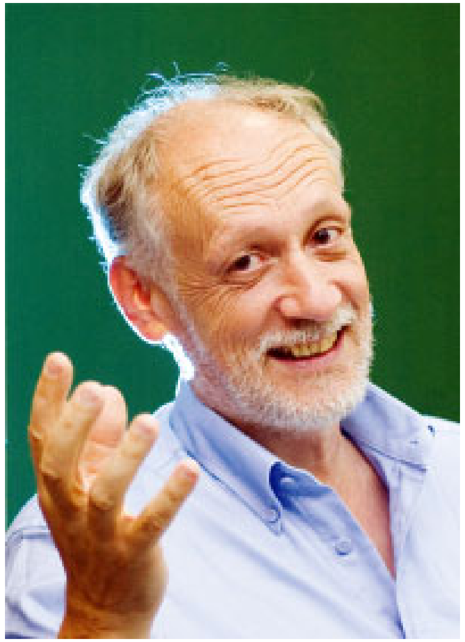
$$|\Psi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1 |V\rangle_2 \pm |V\rangle_1 |H\rangle_2\right)$$

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

Experimental realization: Time bin entanglement



$$P_{ij}(\alpha,\beta) \propto 1 + ijV\cos(\alpha+\beta)$$



QRATE
QUANTUM COMMUNICATIONS

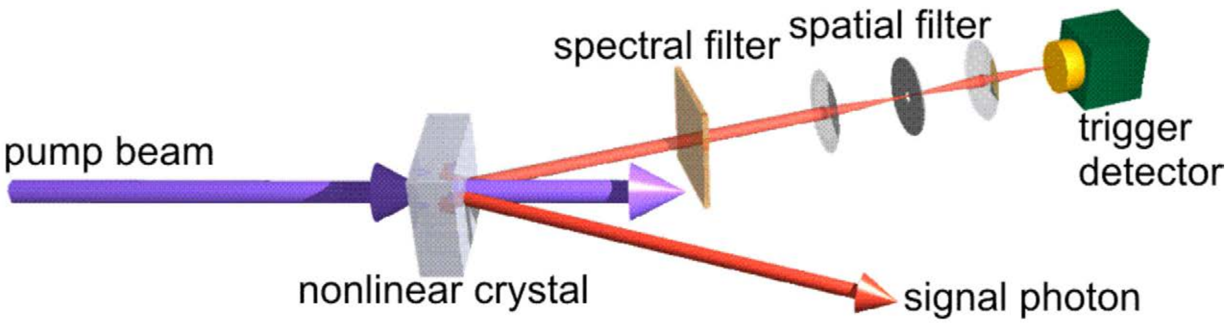
How to generate a photon?

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

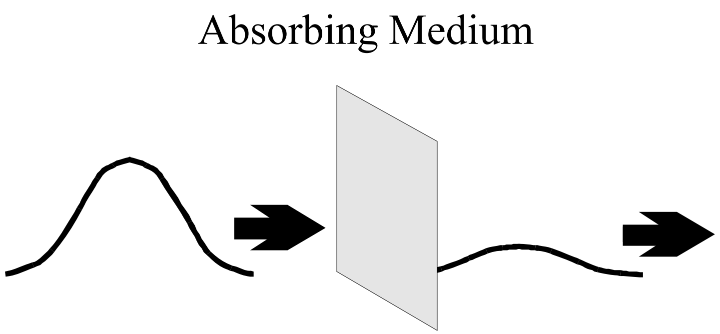


Not a single-photon “on demand”

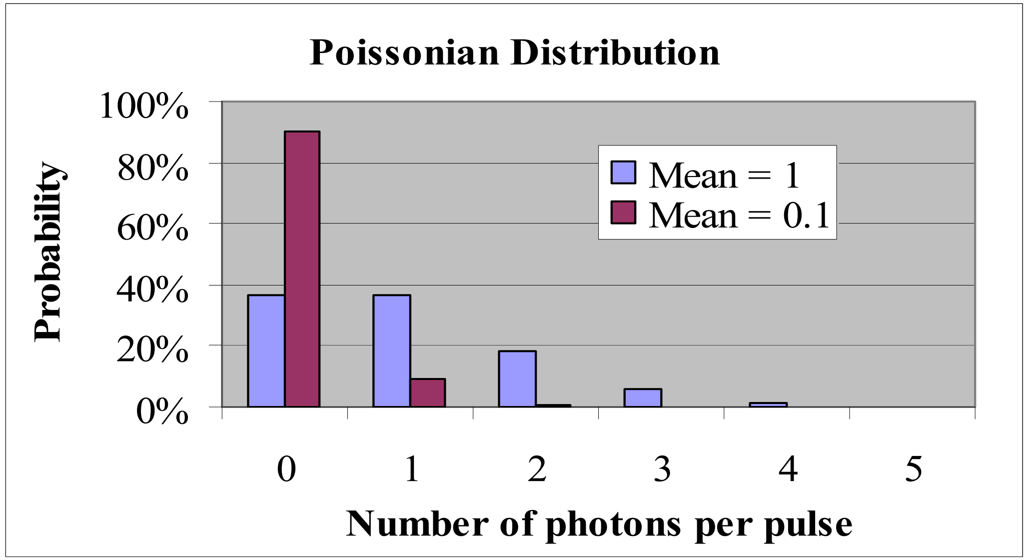
To date, this is the only method which provides a single photon with a high efficiency in a certain spatiotemporal mode

Other ways to find single-photons

Attenuated laser pulses



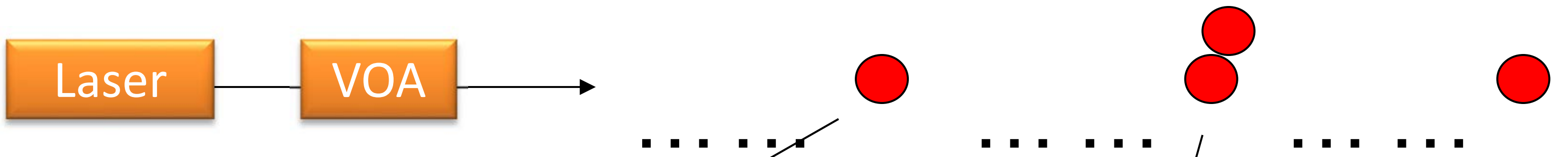
$$"|0\rangle \text{ or } |1\rangle \text{ or } |2\rangle \text{ or...}" \text{ rather than } |1\rangle$$



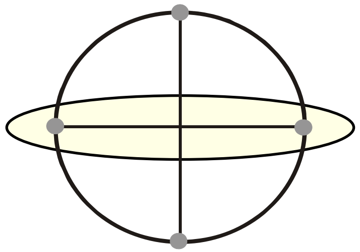
Calculate P(2)/P(1) for both sources with mean probability to generate photon P(1)=0,2.

Photon Number Splitting Attack – Lossless Channel

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



n=1: Nothing

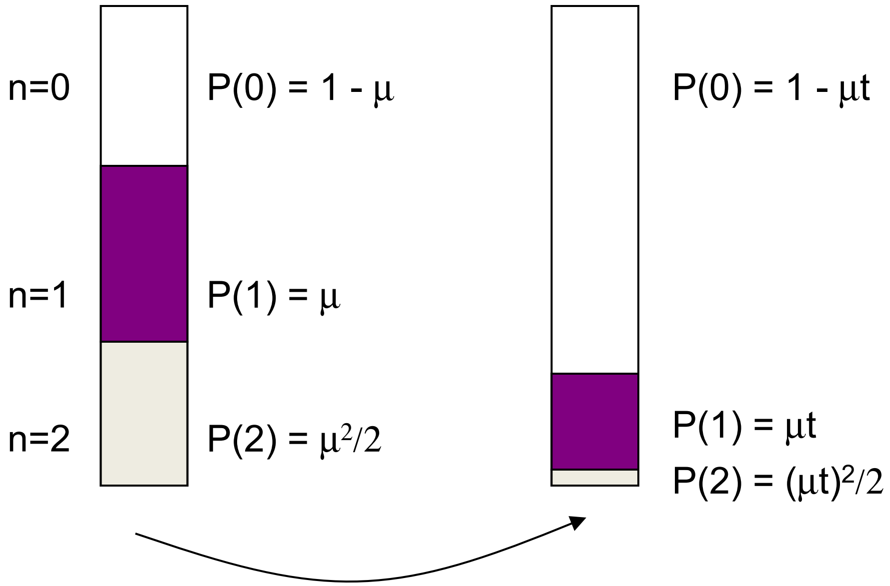


n=2: Stores one photon in quantum memory
Let the other pass through
Wait until sifting

QUANTUM COMMUNICATIONS

Photon Number Splitting Attack – Lossy Channel

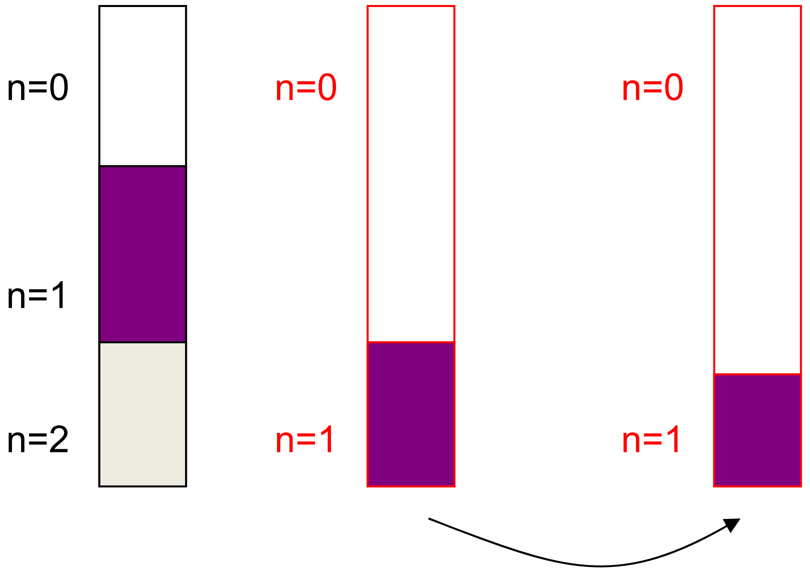
Without Eve



Transmission t

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

With Eve



Transmission τ

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

And $\tau = 2t/\mu$

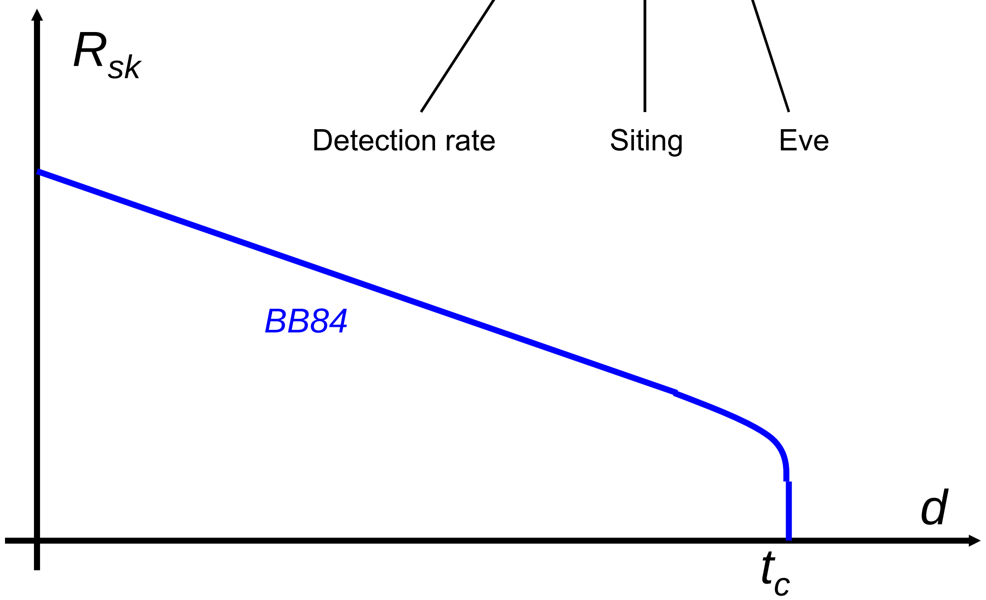
$P(2) = \mu^2/2 > \mu t$: 100% Information

Optimization of average photon number – BB84

Countermeasure to « PNS » attack

Optimization of the average number of photons per pulse μ

$\mu_{opt} = t$ $\qquad R_{sk} = \mu\, t\, \eta / 2 / 2 = \eta\, t^2 / 4$ $\qquad t_c = Sqrt(2\ ln2 \times p_{dark} / \eta)$



Remarks: Bob must…

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

Attenuation α = 0.25 [dB/km]

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

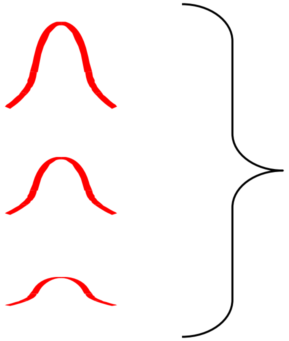
η = 10%

→ t_c = 97 km

QRATE QUANTUM COMMUNICATIONS

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.

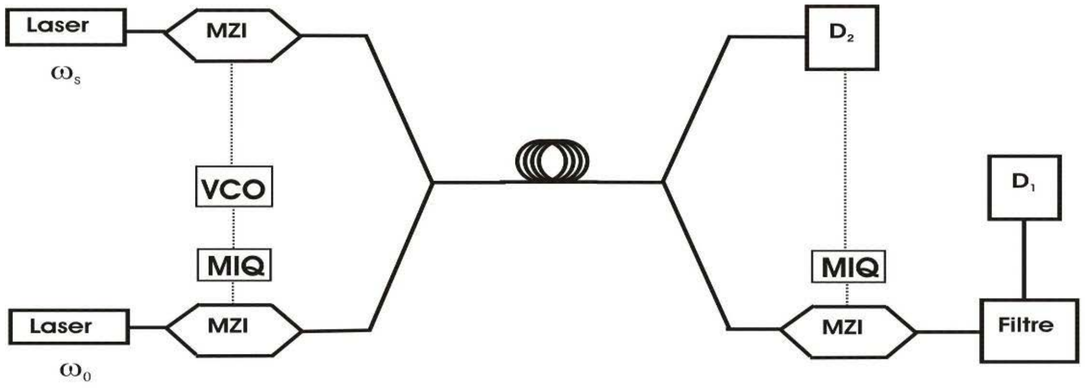
If Eve selectively transmits two-photons, an abnormally low fraction of the decoy state will be received by Bob. Eve will be caught.

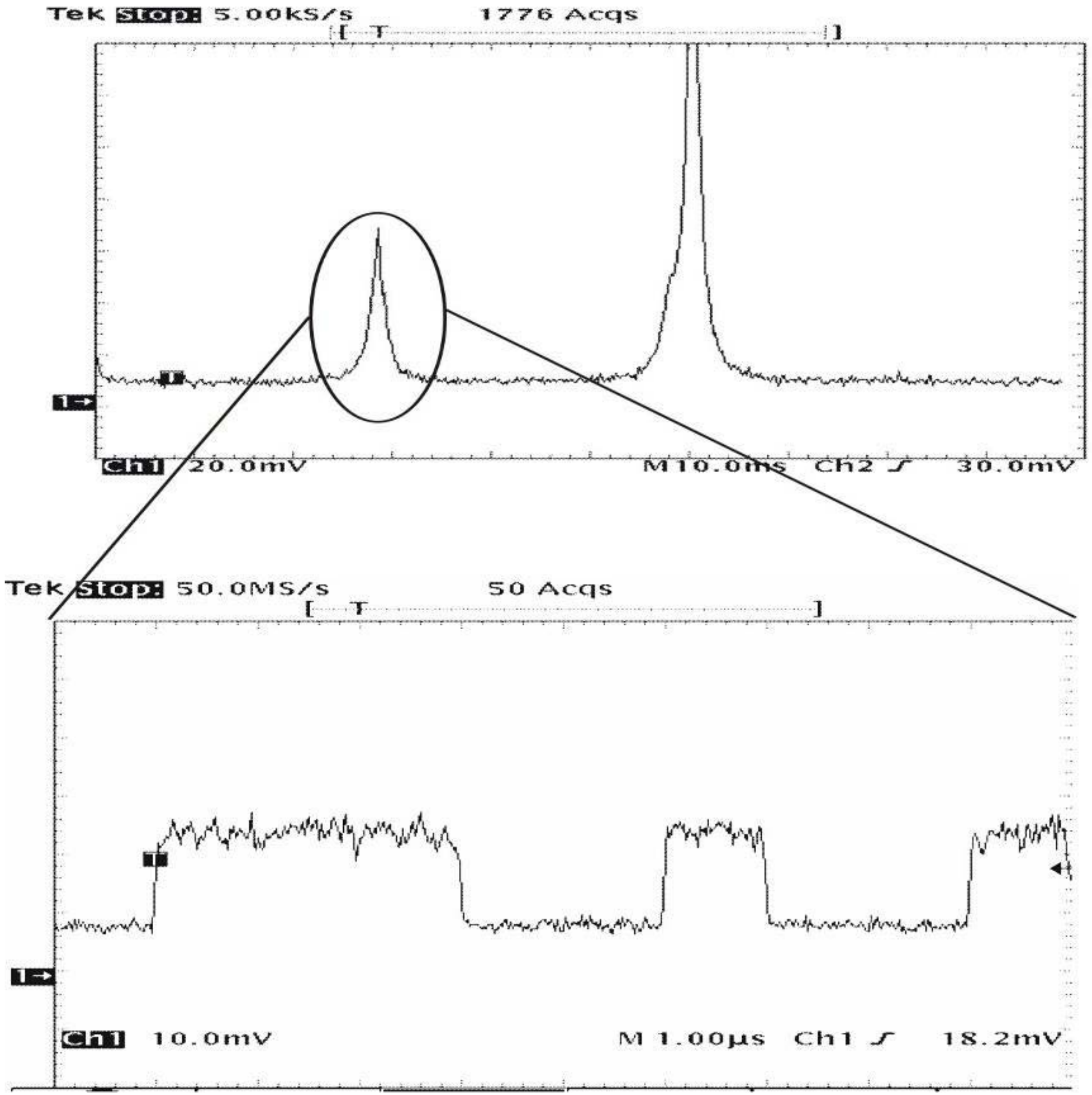
Decoy-state QKD can be as robust as implementations using ideal single-photon sources.

QRATE QUANTUM COMMUNICATIONS

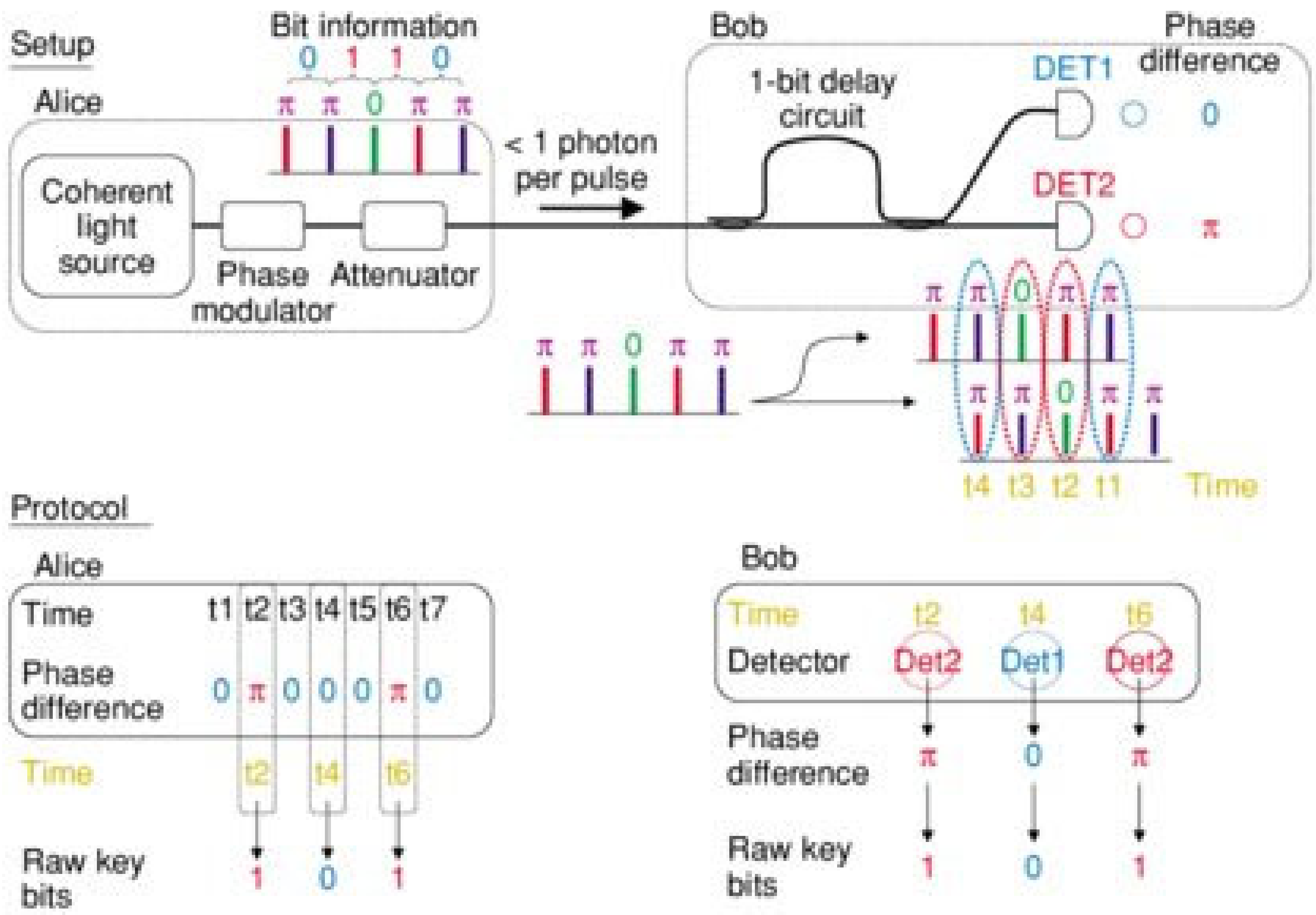
Strong reference

- 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

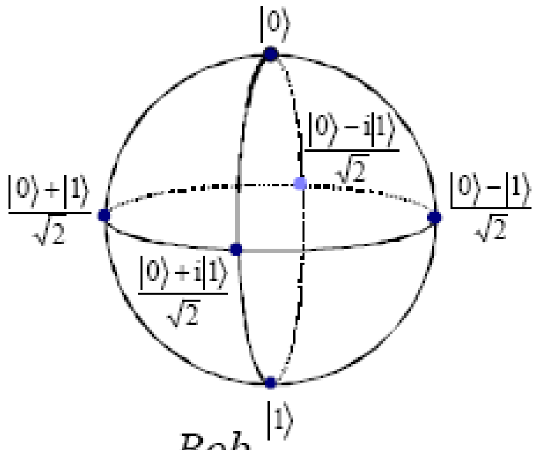


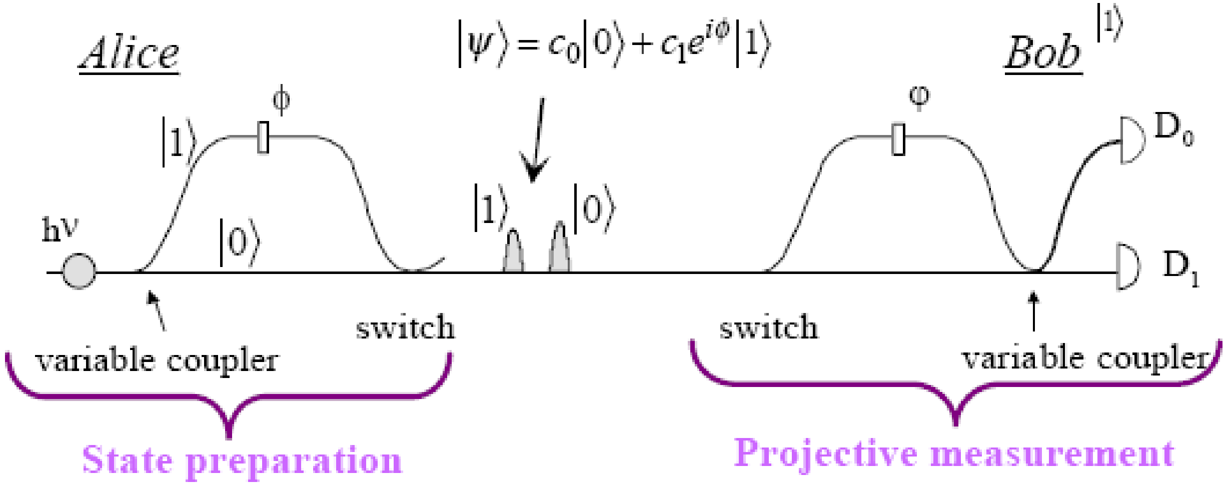
[Takesue, Hiroki & Honjo, Toshimori & Tamaki, Kiyoshi & Tokura, Yasuhiro. (2009). Differential phase shift-quantum key distribution. Communications Magazine, IEEE. 47. 102 - 106. 10.1109/MCOM.2009.4939284.]

How to prepare states: Phase encoding

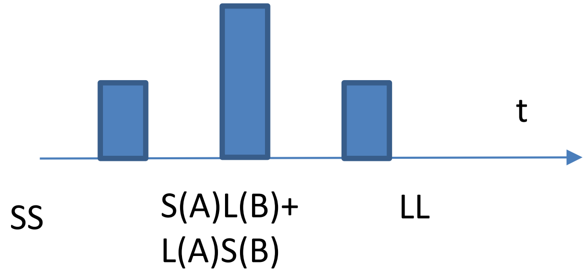
- **qubit** : $|\psi\rangle = c_0|0\rangle + c_1 e^{i\phi}|1\rangle$

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

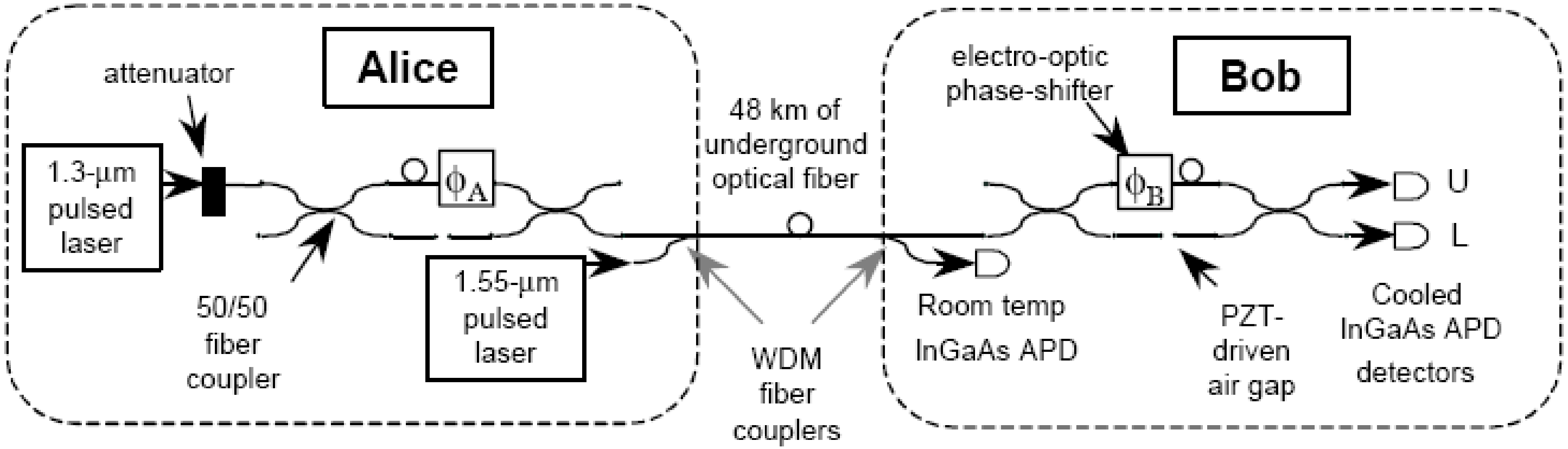




[C. H. Bennett, Phys. Rev. Lett. 68, 3121 (1992)]



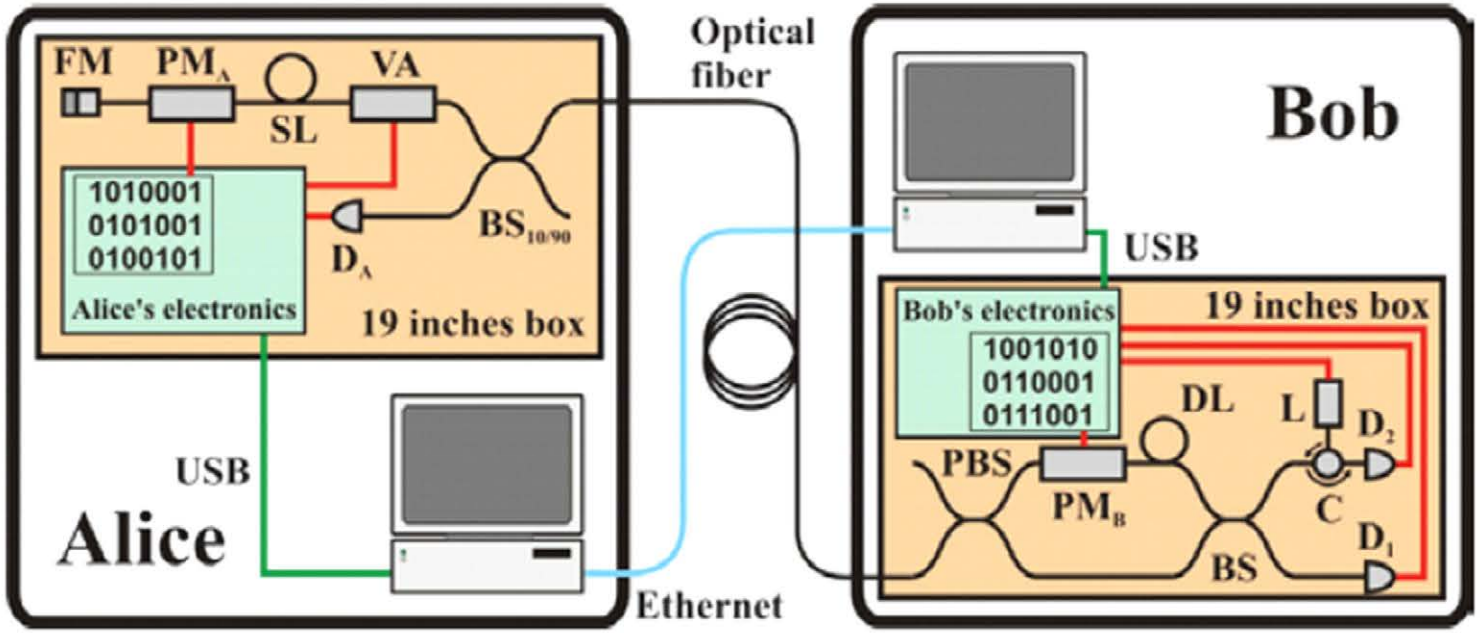
Practical realization



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)]

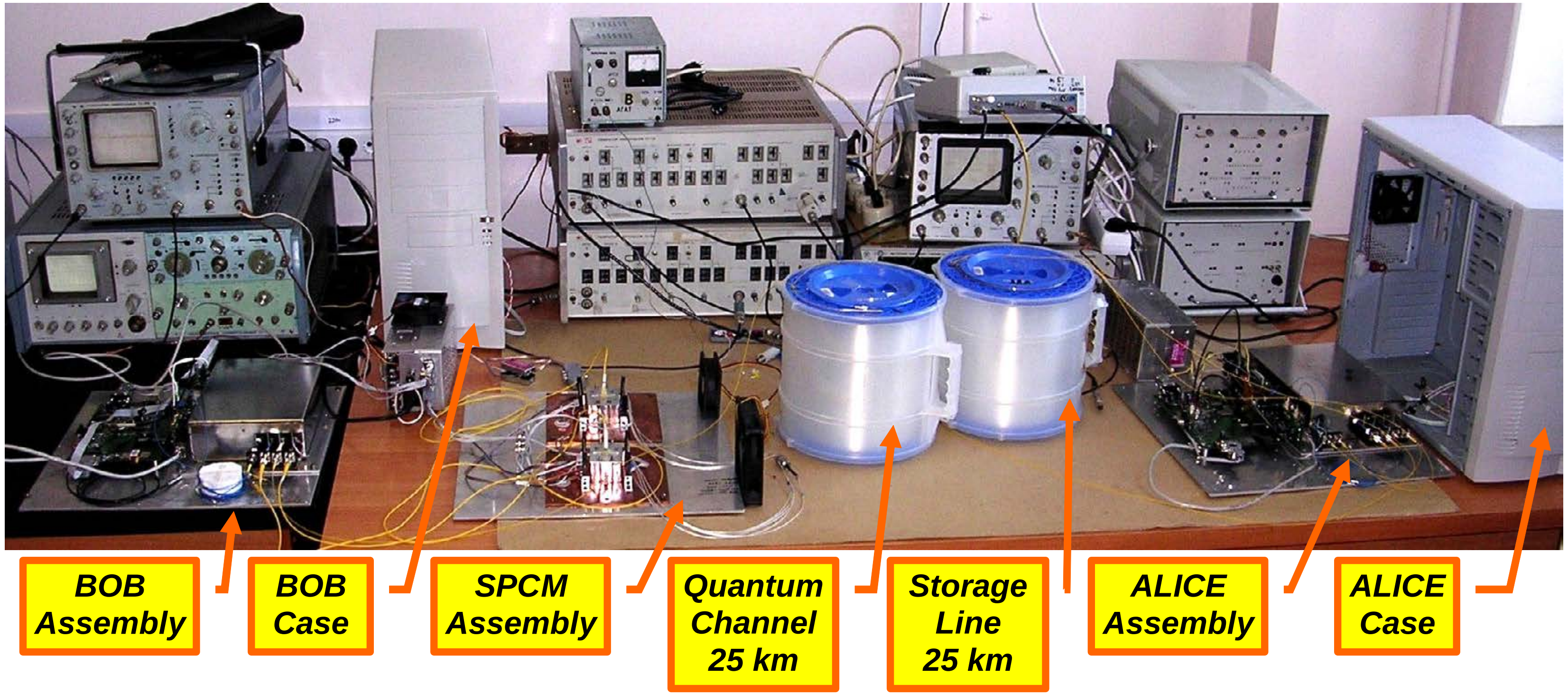
First commercial product by ID Quantique used phase coding



D.Stucki, N.Gisin, O.Guinnard, G.Ribordy, and H.Zbinden, "Quantum key distribution over 67 km with a plug&play system", New Journal of Physics 2002, v.4, p.41

QRATE
QUANTUM COMMUNICATIONS

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

Coherent one way protocol is inspired by classical communication

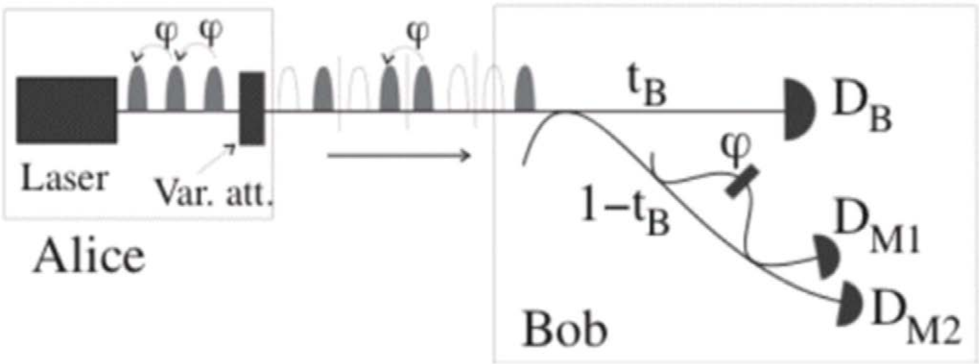
Coherent one way (COW) protocol (currently used by ID Quantique and University of Geneva)

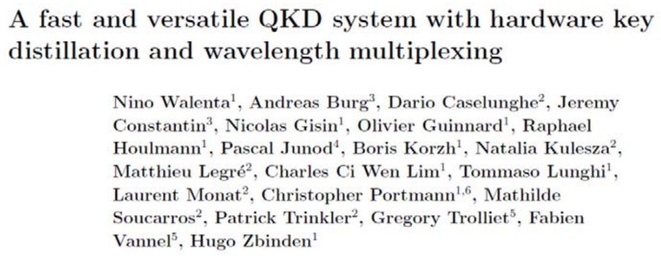
Logical "0" 

Logical "1" 

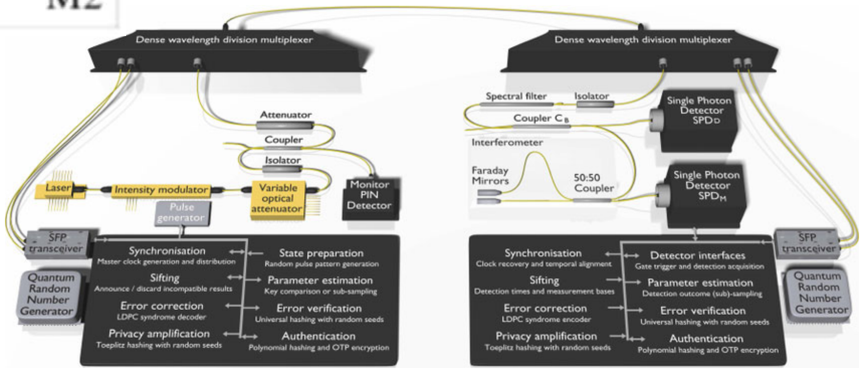
Decoy state  is used to monitor the attempt to unauthorized measurement

Unconditional proofs in process

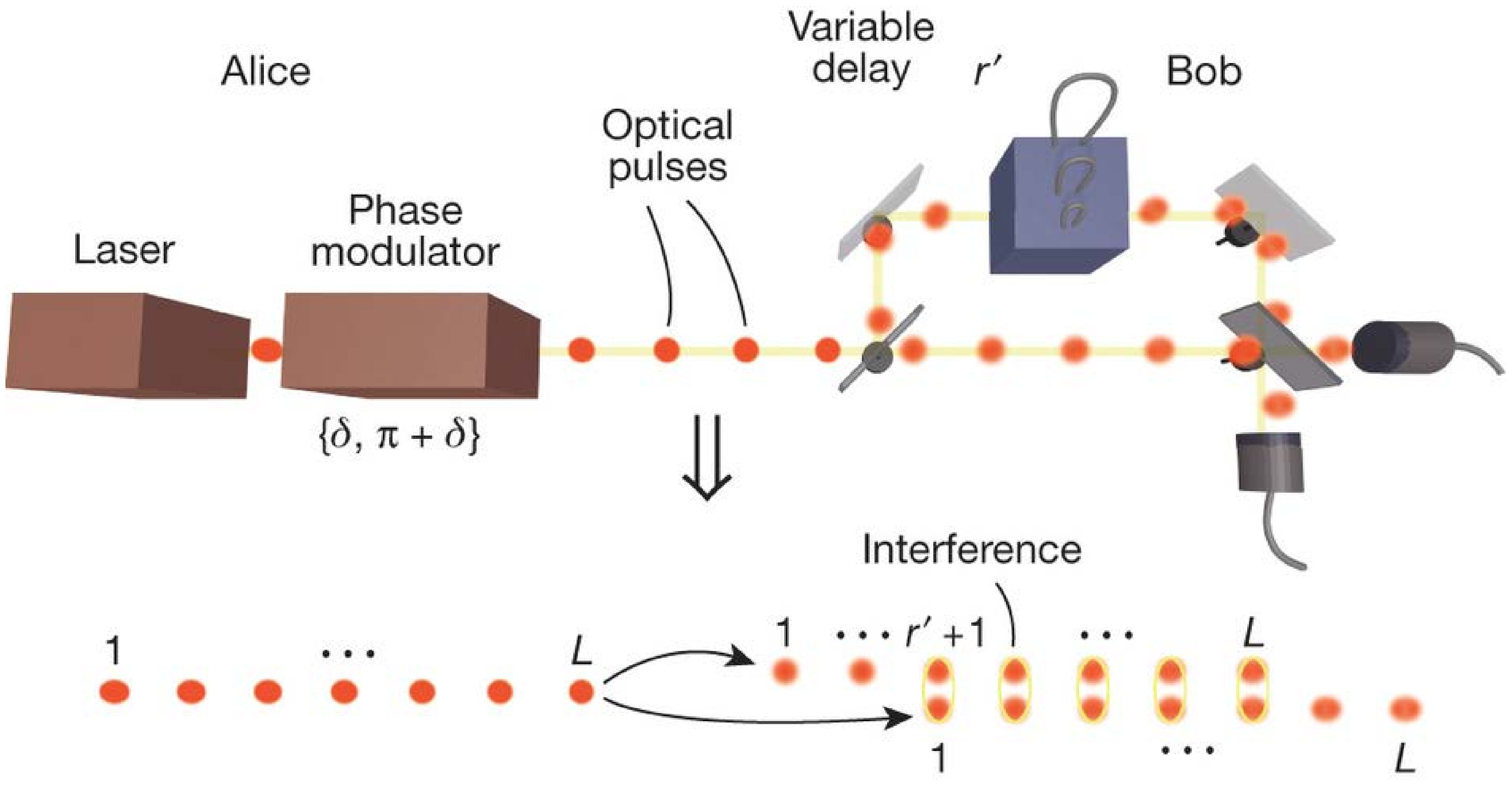



A fast and versatile QKD system with hardware key distillation and wavelength multiplexing

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

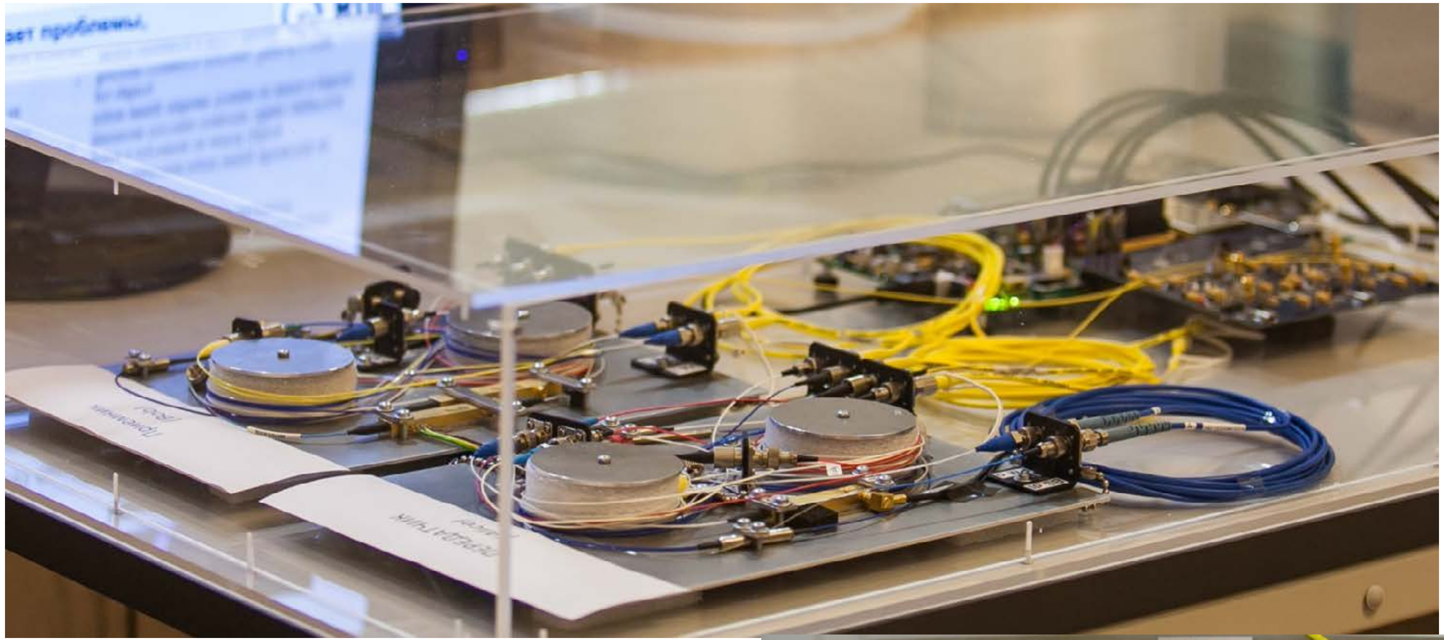


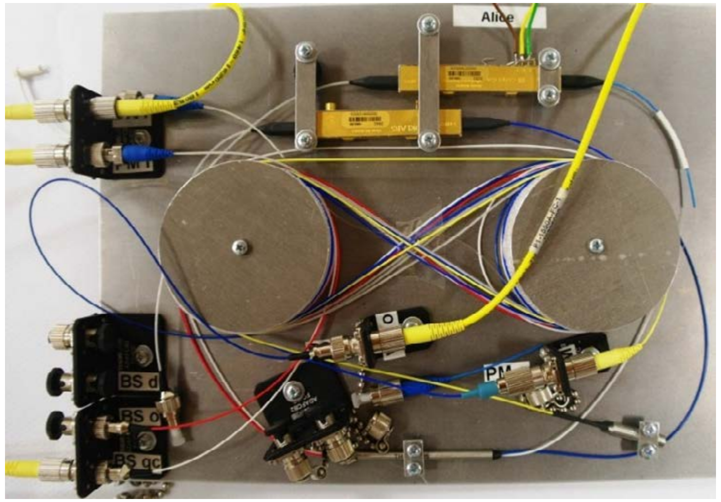
Interference between neighbor pulses will be broken in the case of the photon number splitting attack

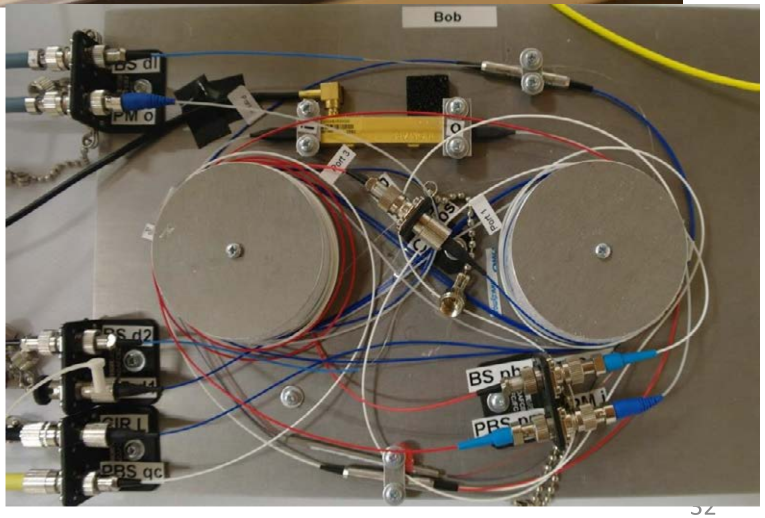
K. Inoue, E. Waks, Y. Yamamoto, Phys. Rev. Lett. 89, 037902 (2002)

QRATE
QUANTUM COMMUNICATIONS

How fiber optical scheme looks like





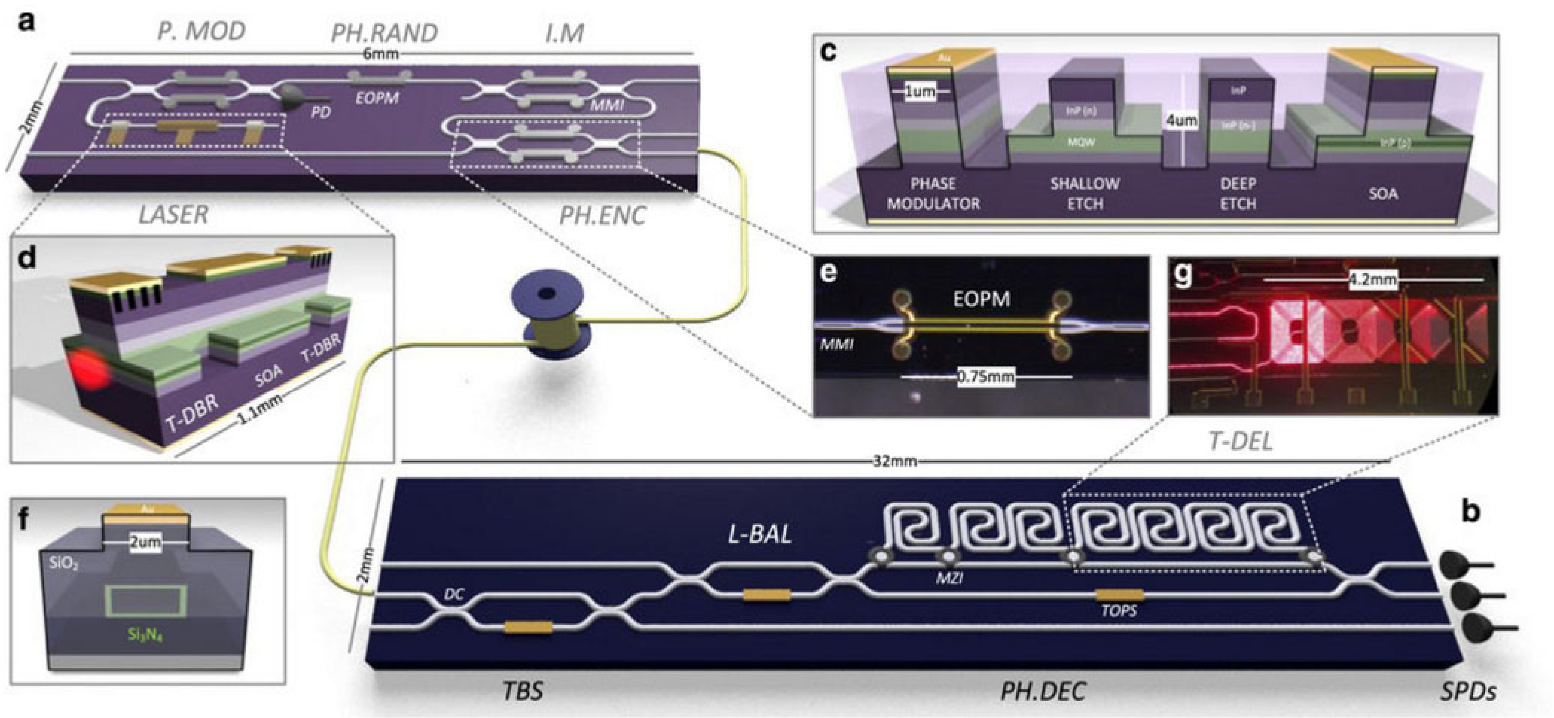


QRATE
QUANTUM COMMUNICATIONS

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



QRATE
QUANTUM COMMUNICATIONS

How to prepare four BB84 polarization states?

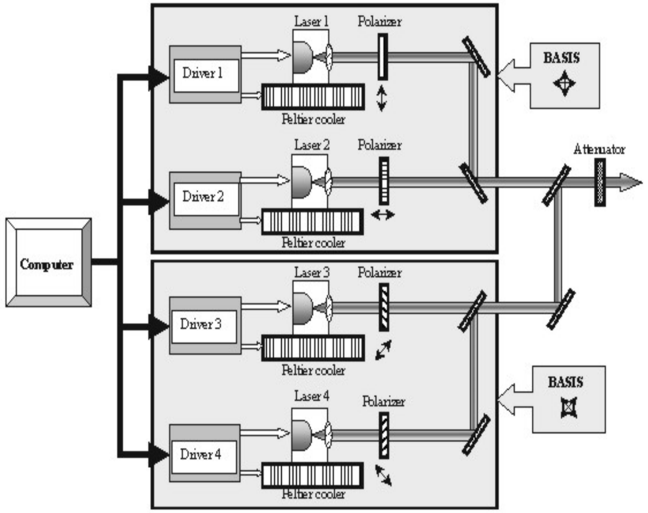
One can use 4 lasers
Fast and convenient
Inseparability problem

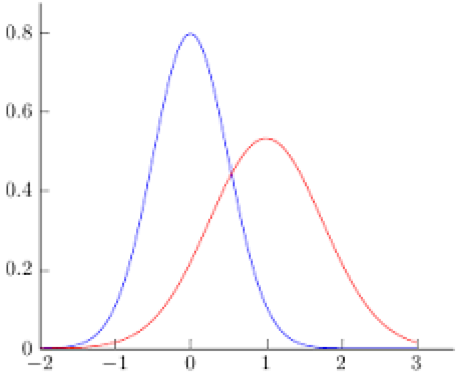
- Lasers can be different in frequency, time or direction

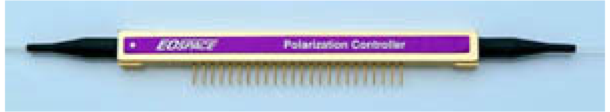
It is possible to construct full polarization controller from $LiNbO_3$ crystals
Piezo driven polarization controllers are not fast enough for random state preparation

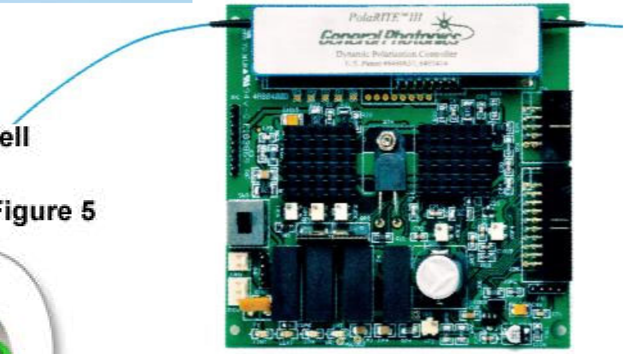
Pockels cell allows us to prepare four maximum nonorthogonal states

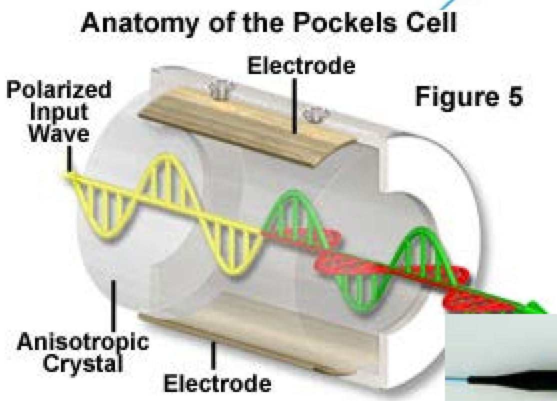
- It was used in the first QKD experiment (Bennett, Ch.H., F. Bessette, G. Brassard, L. Salvail, and J. Smolin, 1992a, “Experimental Quantum Cryptography”, J. Cryptology 5, 3-28.
- Modern $LiNbO_3$ modulators work with much lower voltage and higher bandwidth











300V

40 GHz

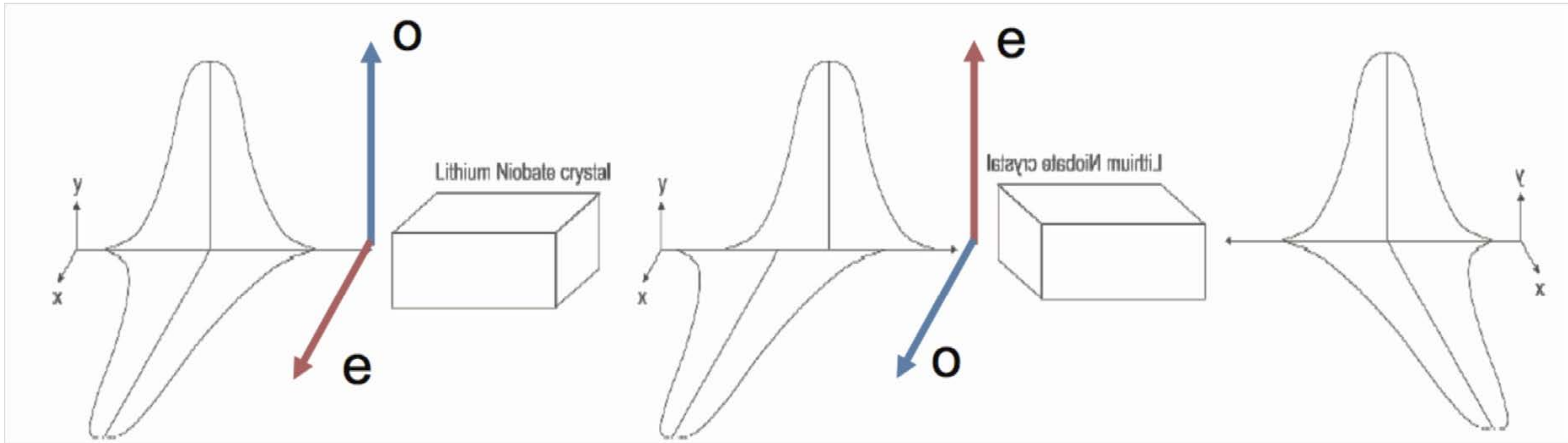
QRATE QUANTUM COMMUNICATIONS

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).

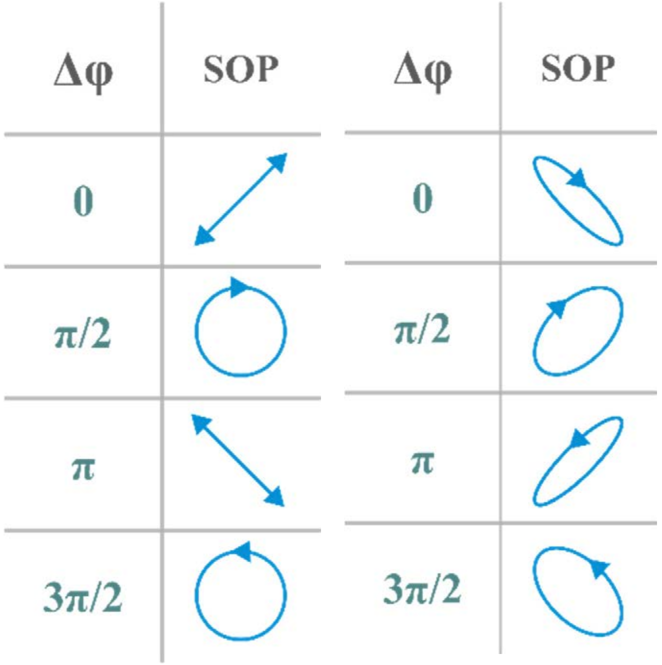
QRATE QUANTUM COMMUNICATIONS

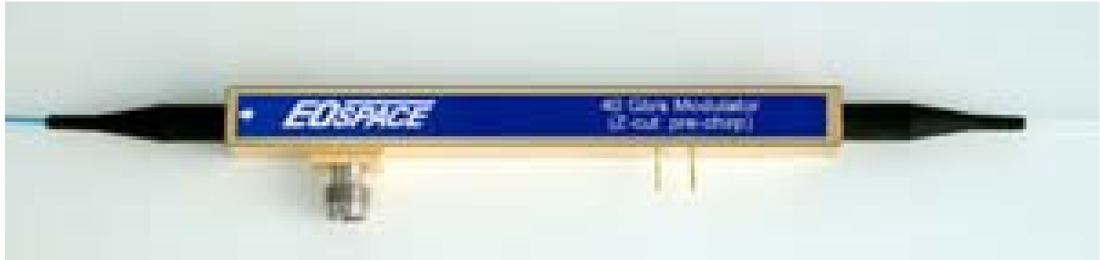
States prepared by Pockels cell

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)

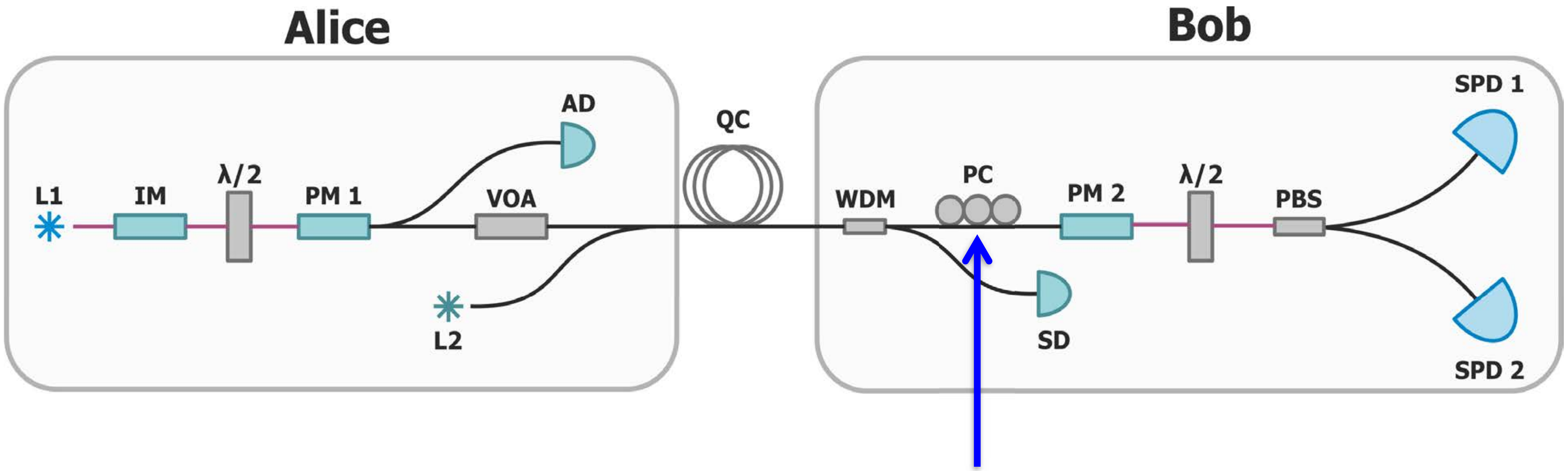
BB84 states are not obligatory diagonal +45, diagonal -45, left and right. It can be any pair of maximally non orthogonal states combined by equal horizontal





ORATE
QUANTUM COMMUNICATIONS

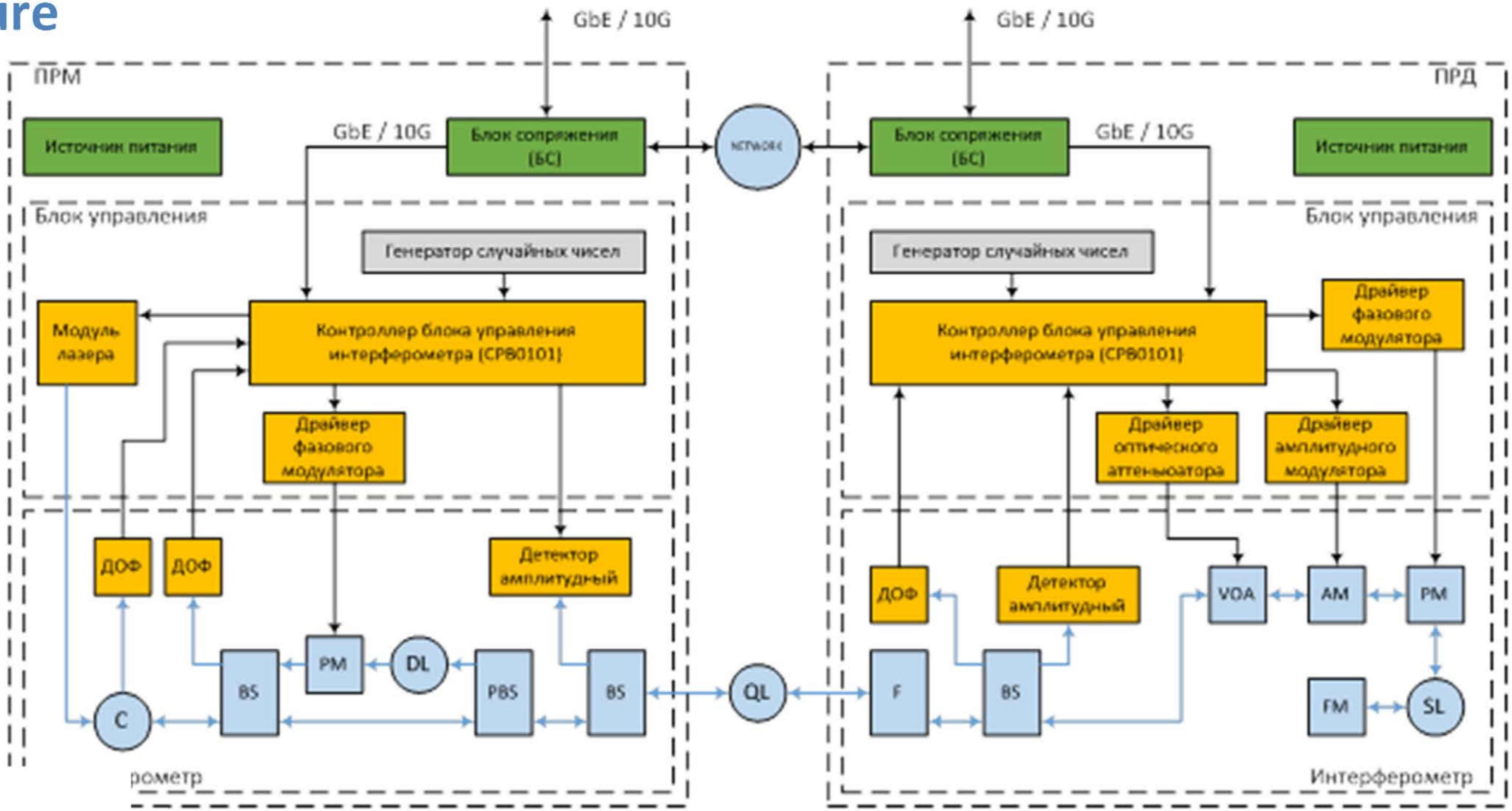
Polarization tuning

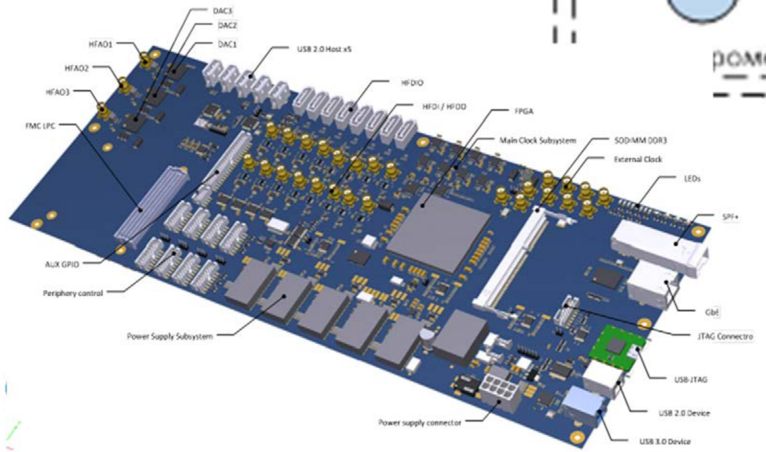


Polarization can be tuned with piezoelectric-polarization-controller
Alice and Bob can announce part of the key to monitor QBER (usually it is “decoy” state events)
If QBER exceeds threshold (for example 6%), Alice Increases Amplitude and sends predefined sequence to tune polarization controller
Bob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

Real QKD structure

Структурная схема УК БПД. C – Circulator; PM – Phase Modulator; DL – Delay Line; PM – Phase Modulator; PBS – Polarization Beam Splitter; BS – Beam Splitter; QL – Quantum Line; F – Filter; VOA – Variable Optic Attenuator; AM – Amplitude Modulator; FM – Faraday Mirror; SL – Storage Line.

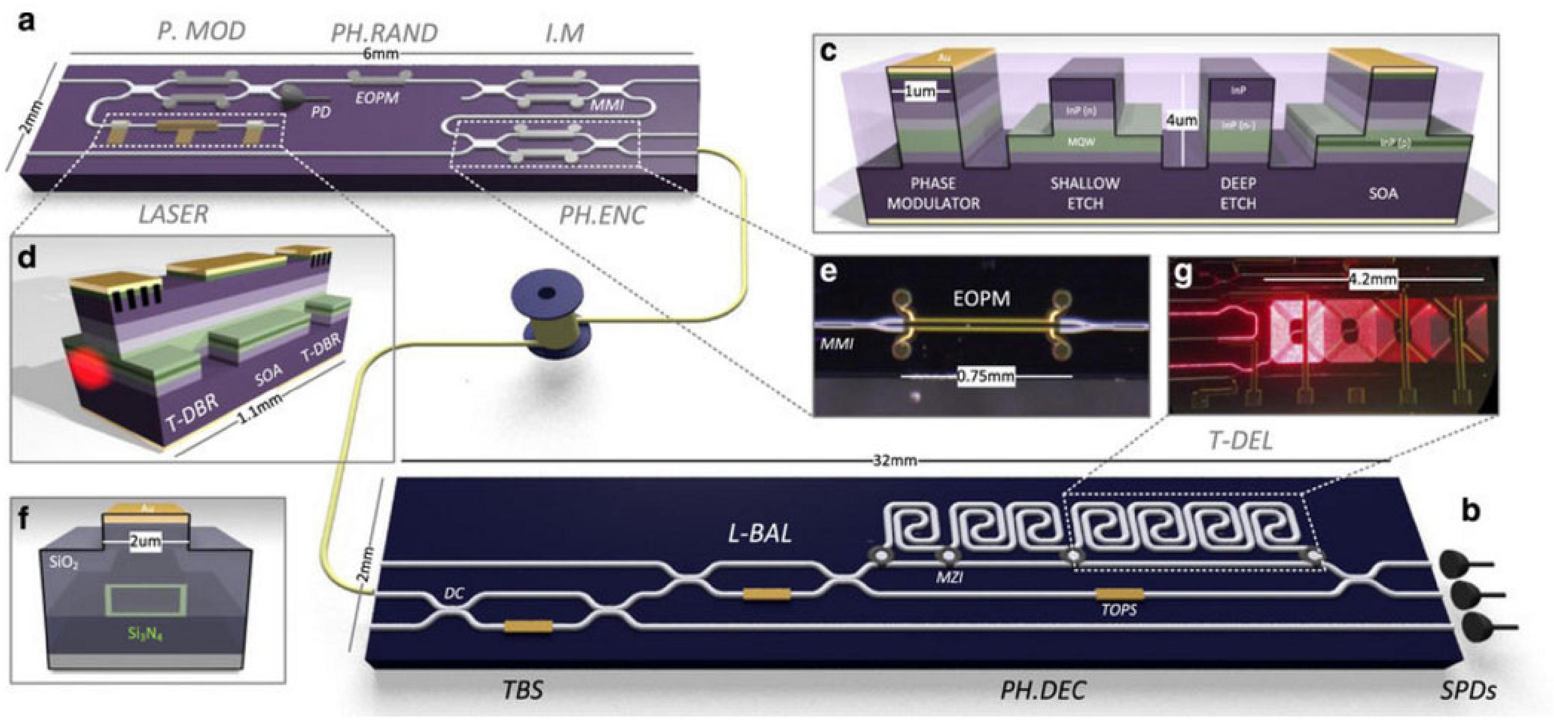




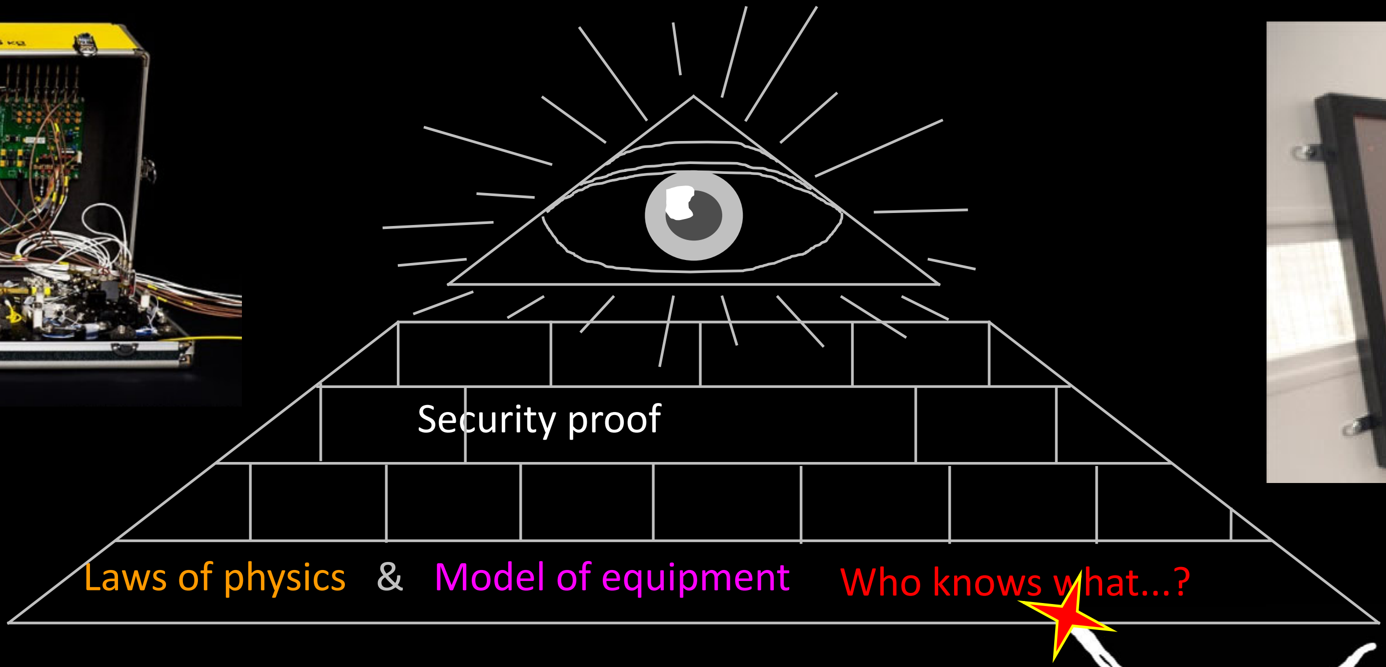
Photonic chips will dramatically change the QKD setup size

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

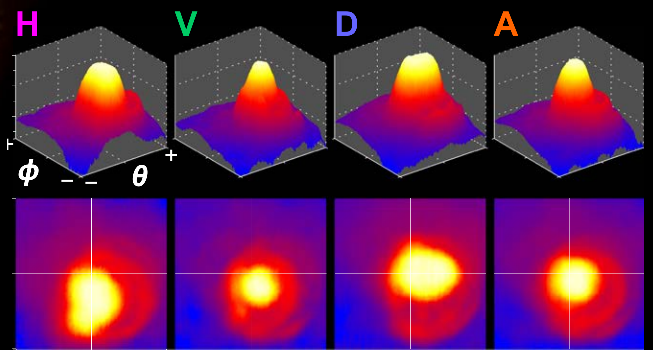
From: Practical challenges in quantum key distribution



Limits on physical security



Physical access to equipment



Laser damage!