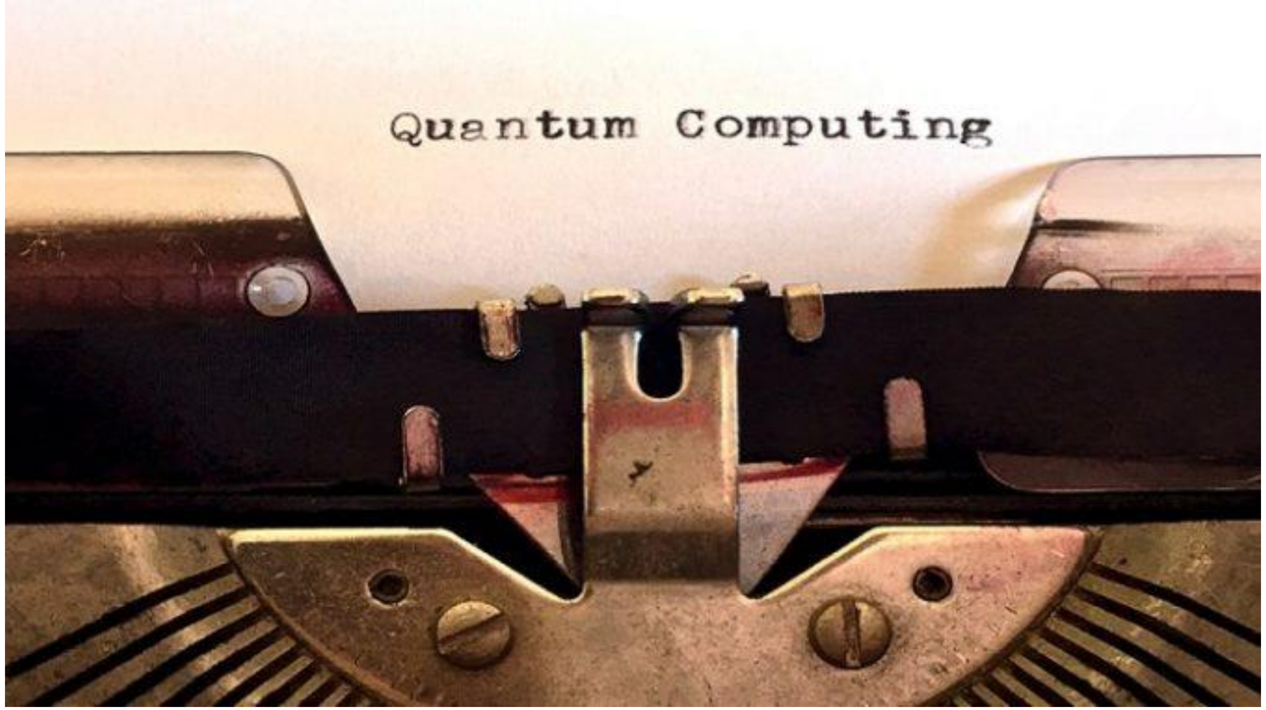
Quantum Computation and Key Distribution



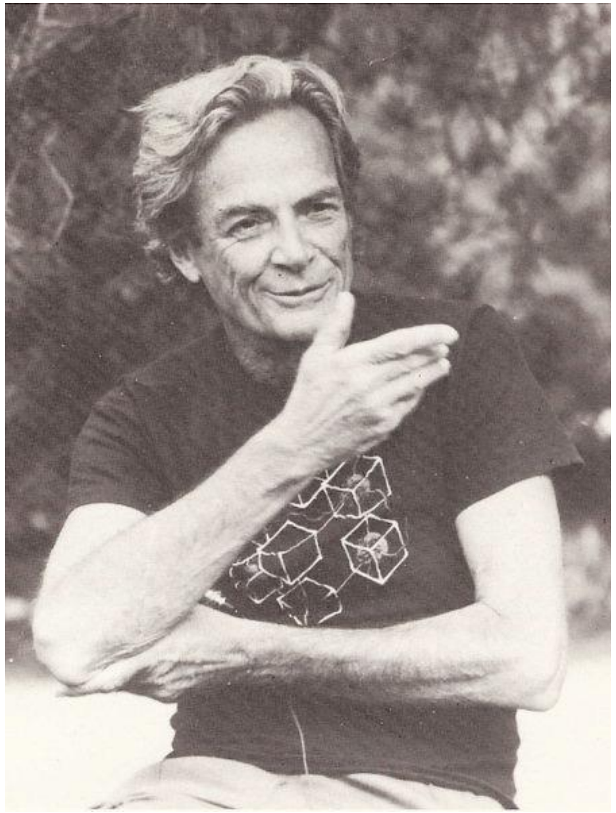
Hugo Zbinden

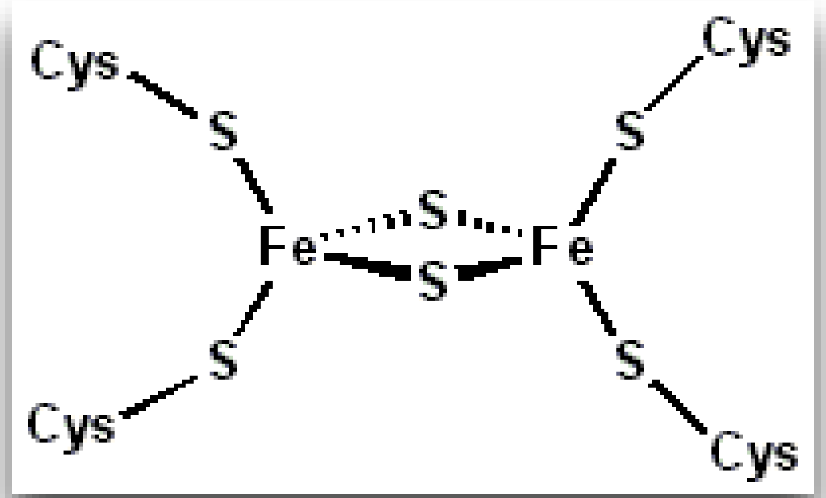
GAP – Quantum Technologies

UNIVERSITÉ DE GENÈVE

Quantum simulation

- Feynman's original motivation for proposing a quantum computer (1982)





Ferredoxin: Fe_2S_2-cluster:
16 valence electrons, 84 total

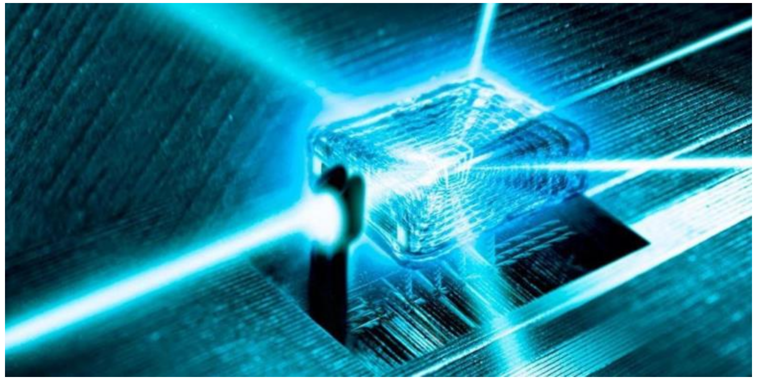
- problem setting: Given position of nuclei in a molecule, find ground state energy
- gives bond lengths, energetics etc.
- important for process optimization

The power of quantum

Classical computer

- Binary information
- Registers with well-defined binary value 0 or 1
- Commands on registers one-by-one
- Parallel operations = parallelized hardware

Quantum computer



- Binary information
- Qubits : |0>+|1>
- Superpositions of registers, entanglement
- Operations on complete state space
- intrinsic parallelism

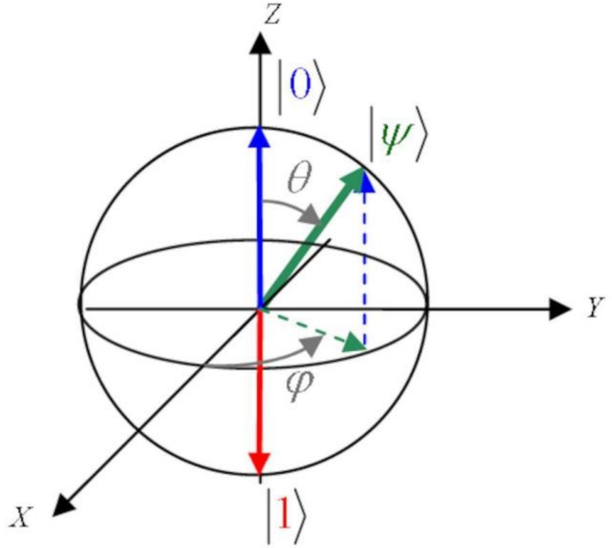
DiVincenzo-Criteria

- A scalable array of well-defined two level systems (qubits)
- A universal set of gates
- Initialization to a reference state
- A low error rate
  Low enough for error correction
- Qubit-specific measurement

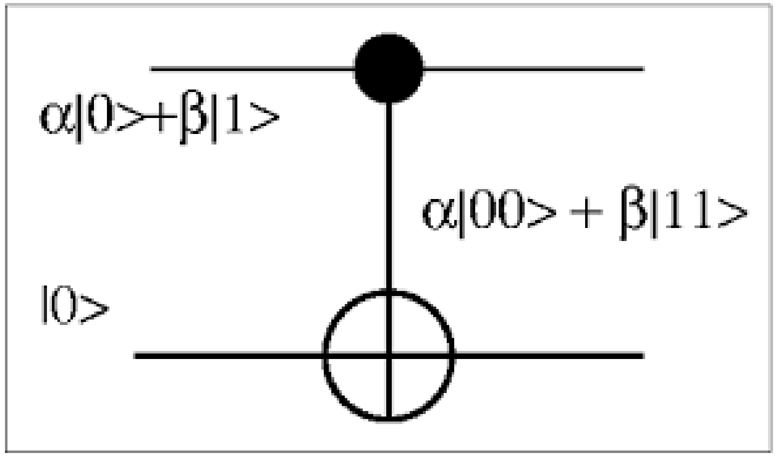
D.P. DiVincenzo, Fortschr. Phys. 2000

Gates

- Single qubit gates

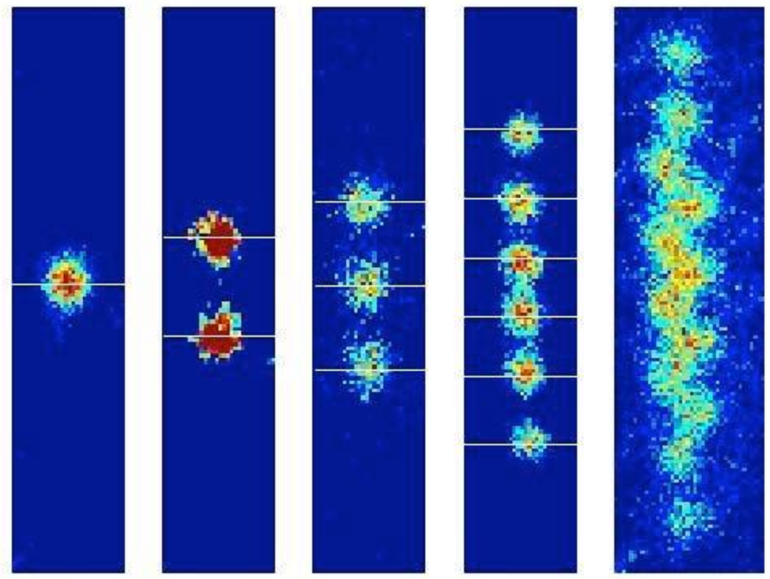


- CNOT (control-not gate): Flip target iff control = 1



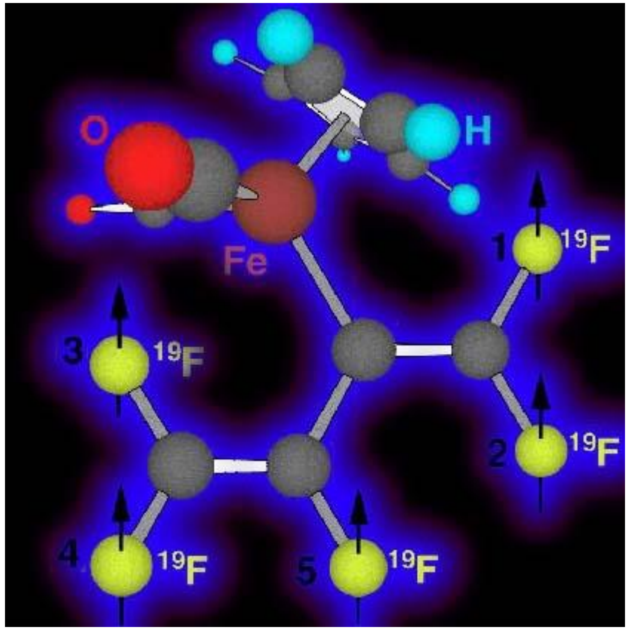
Qubit candidates

Atomic systems



up to 18 qubits in ion traps

Nuclei



Up to 12 qubits in liquid state

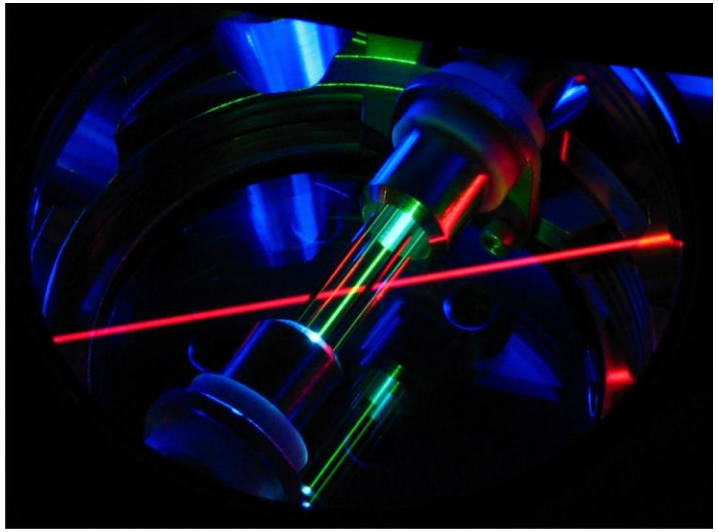
Natural quantum systems:

very coherent

challenging to scale

Machines

Ion trap



Optical table

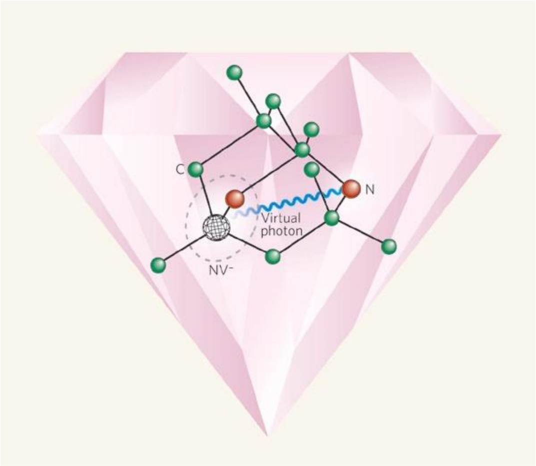
NMR:

Molecules in test tubes

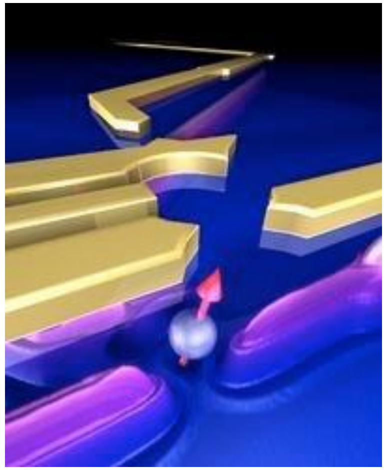
Spectrometer

Solid state qubits

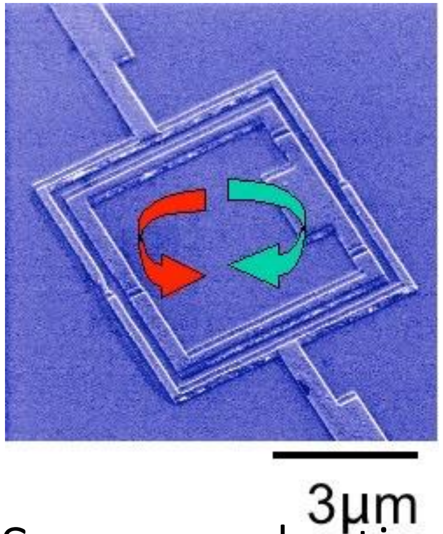
Spins controlled in solid matrix



Diamond



Quantum dot



Superconducting circuit

engineering flexibility, control
coherence

atom-like → engineered

Three paths to quantum computing

Universal fault-tolerant quantum computer:

- massive overhead from error correction
- long-term goal
- powerful tool
- potentially large time savings

Non error-corrected co-designed processor

- 50 qubits near?
- outperform supercomputer (in simulating quantum computers)
- gate number limited by physical errors
- potential memory savings

Quantum annealer / adiabatic quantum computer

- accessible technology
- quantum speedup?

IBM vient de dévoiler le premier ordinateur quantique commercial

Stéphanie Schmidt 9 janvier 2019 Technologie 3

L'ordinateur quantique IBM Q System One. | IBM

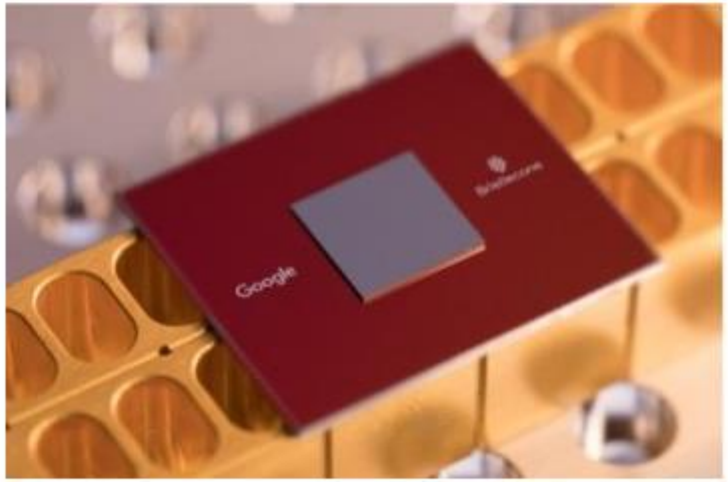
20 qubits

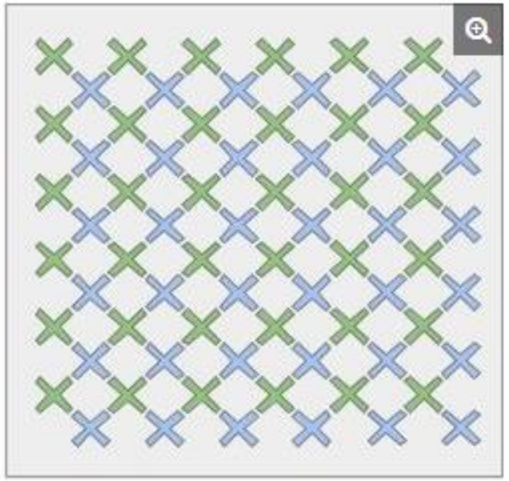
Google Unveils 72-Qubit Quantum Computer With Low Error Rates

22
COMMENTS

tom's HARDWARE

by Lucian Armasu March 5, 2018 at 12:00 PM - Source: Google Research





Google's Bristlecone quantum computer

Google announced a 72-qubit universal quantum computer that promises the same low error rates the company saw in its first 9-qubit quantum computer. Google believes that this quantum computer, called Bristlecone, will be able to bring us to an age of quantum supremacy.

Ready For Quantum Supremacy

see also https://www.microsoft.com/en-us/quantum/

Quantum „supremacy“ / advantage

Google and IBM Battle for Quantum Supremacy

Michael Feldman [/project/top500-news-team/] | May 30, 2017 03:19 CEST

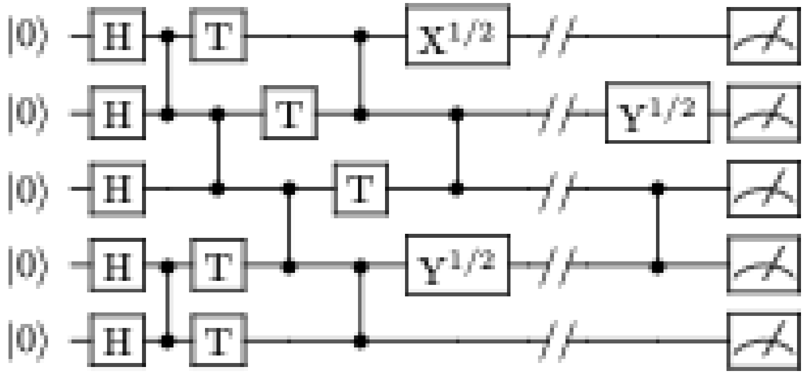
Revealed: Google's plan for quantum computer supremacy

The field of quantum computing is undergoing a rapid shake-up, and engineers at Google have quietly set out a plan to dominate

Key idea:

- Current classical supercomputers can simulate a quantum computer up to 47 qubits
- Build something larger and execute any algorithm
- Then find applications

Example: Simulation of quantum chaos



Boixo et al., 2016

D-Wave

A Unique Processor Environment

- Shielded to 50,000× less than Earth's magnetic field
- In a high vacuum: pressure is 10 billion times lower than atmospheric pressure
- 200 I/O and control lines from room temperature to the chip
- The system consumes less than 25 kW of power
- Power demand won't increase with successive processor generations

D-Wave 2000Q | Traditional Supercomputer

22.0kW | 2030.2kW

- "The Fridge" is a closed cycle dilution refrigerator
- The superconducting processor generates no heat
- Cooled to 180x colder than interstellar space (0.015 Kelvin)

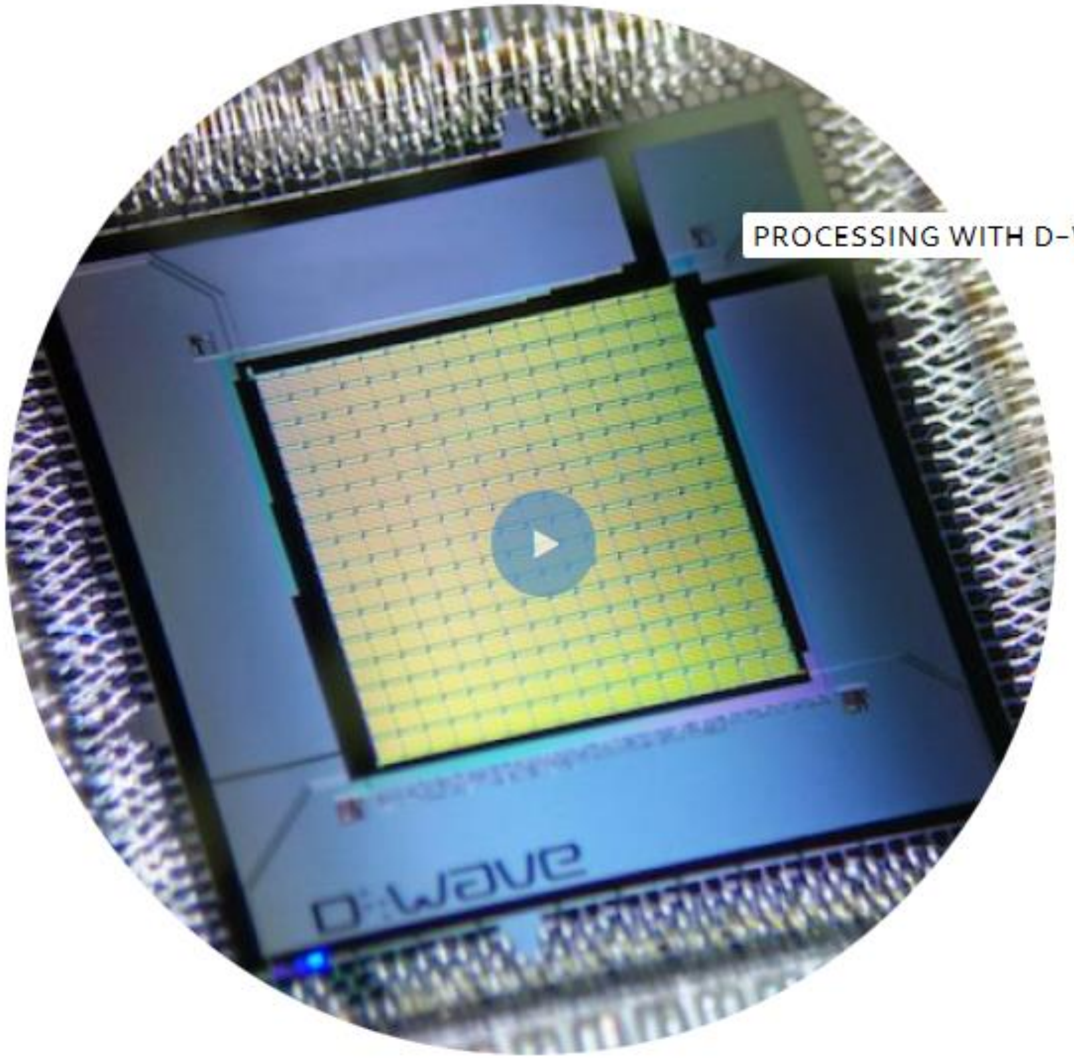
D-Wave Processor Environment

−273°C

0.015° above absolute zero

Processing with D-Wave

- A lattice of 2000 tiny superconducting devices, known as qubits, is chilled close to absolute zero to harness quantum effects
- A user models a problem into a search for the "lowest energy point in a vast landscape"
- The processor considers all possibilities simultaneously to determine the lowest energy and the values that produce it
- Multiple solutions are returned to the user, scaled to show optimal answers

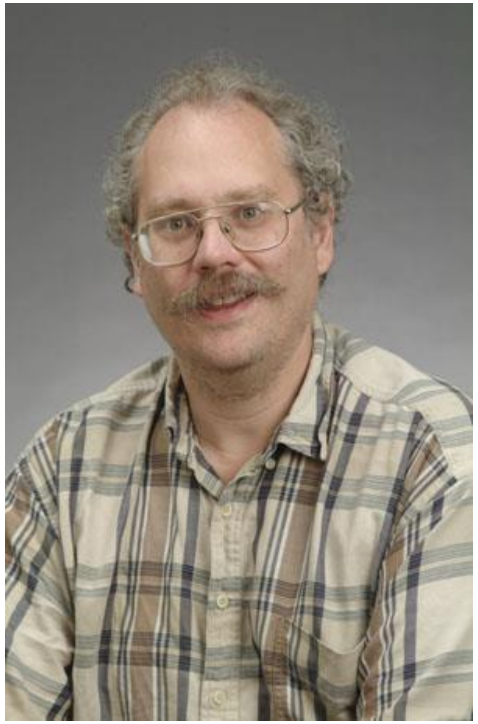


Applications

- Quantum simulation (chemistry, new drugs)

- Shor's algorithm: factoring

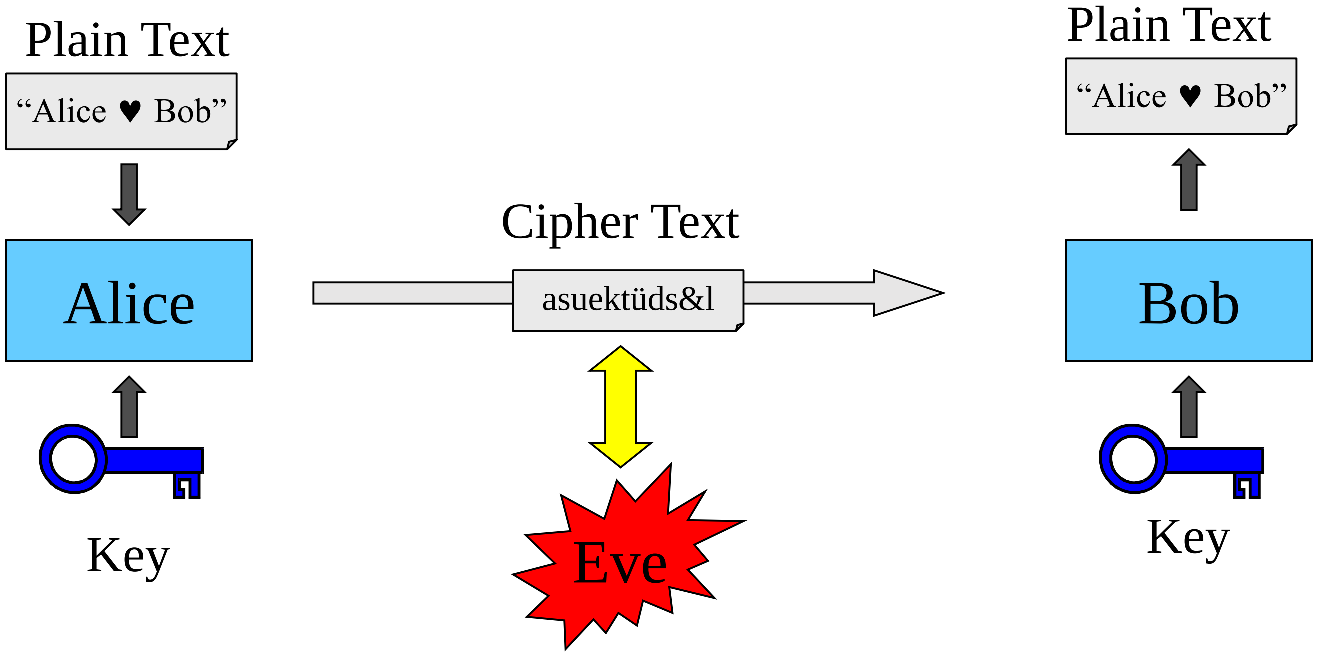
- Grover algorithm: data base search



Peter Shor

UNIVERSITÉ DE GENÈVE

Is the Quantum Computer a threat for the information security?



UNIVERSITÉ DE GENÈVE

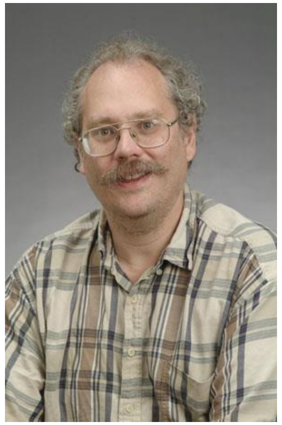
Classical Cryptography

A) Based on Complexity

DES, AES (secret key)

RSA (public key)

Security unproven



One-way functions

Integer factorisation

$107 \times 53 = x$

$5671 = y \times z$

Classical Cryptography

b) based on Information Theory

one time pad (Vernam)

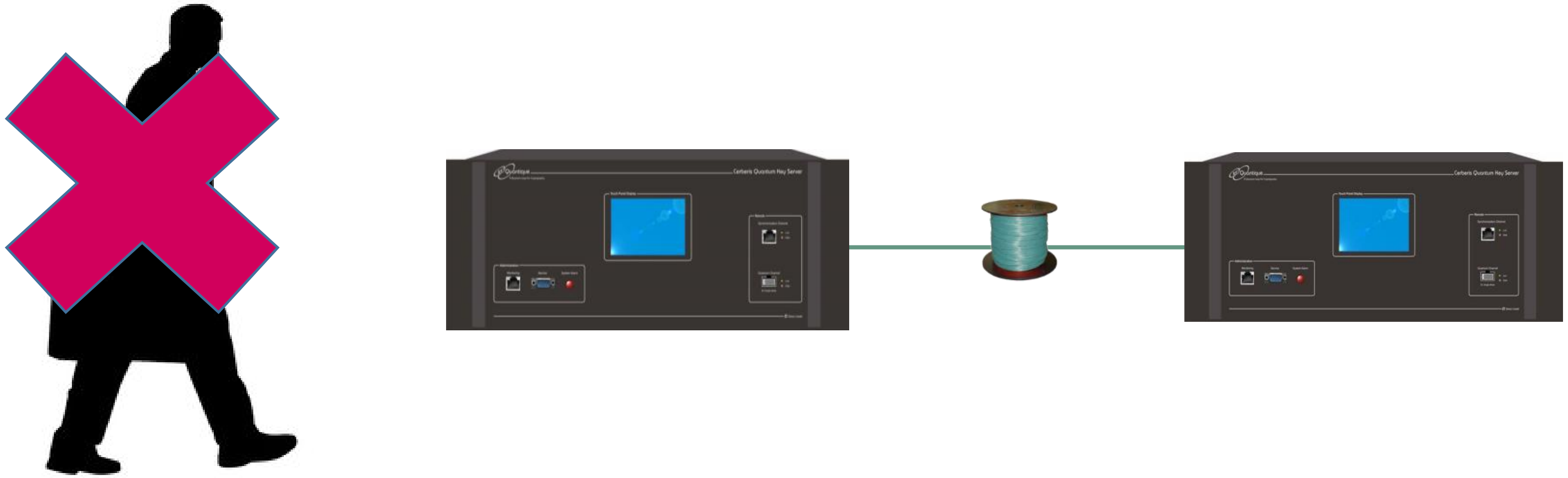
plaintext :	00101001001001110101000110101001
key:	+10101101101100101010011101010101
cyphertext:	10000100100101011111011011111100

security proven

problem: key distribution

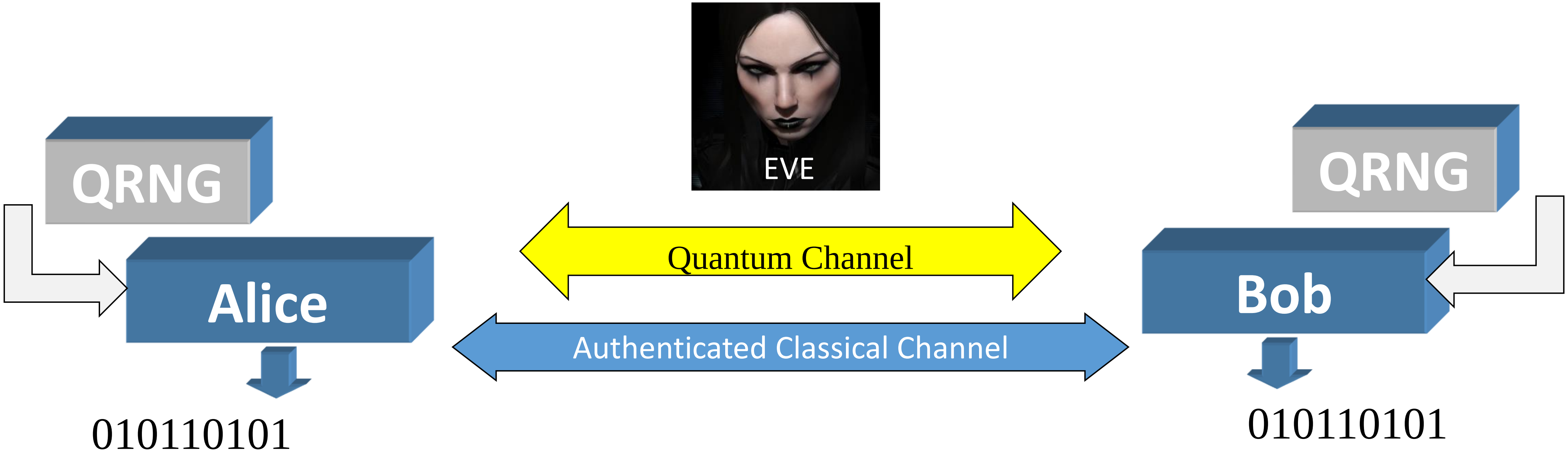
Quantum Key Distribution

- Quantum Crpytography is not a new coding method
- Send key with individual photons (quantum states)
- The eavesdropper may not measure without perturbation (Heisenbergs uncertainty principle)
- Eavesdropping can be detected by Alice and Bob!



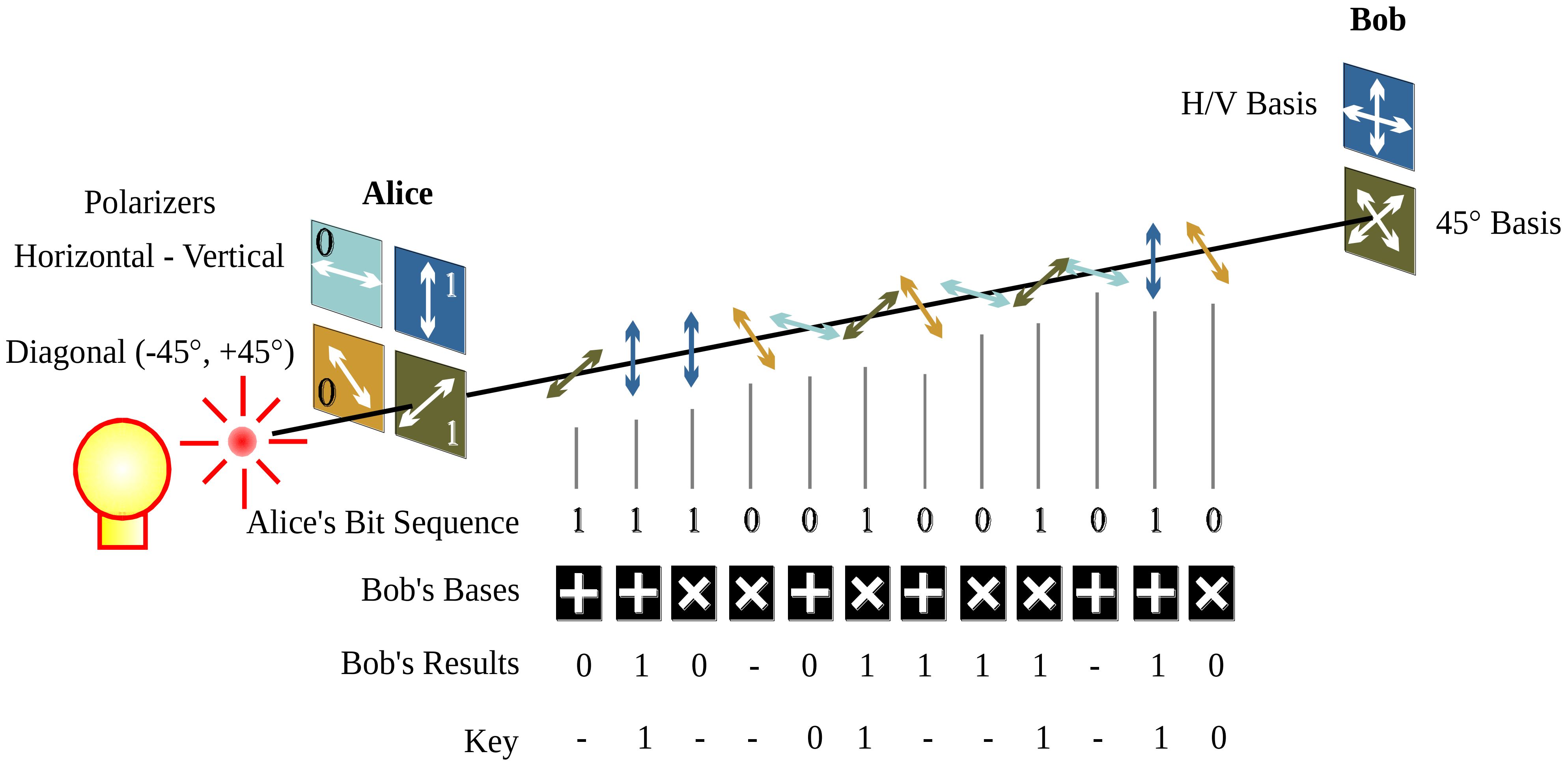
QKD is proven information theoretically secure!

Quantum Key Distribution

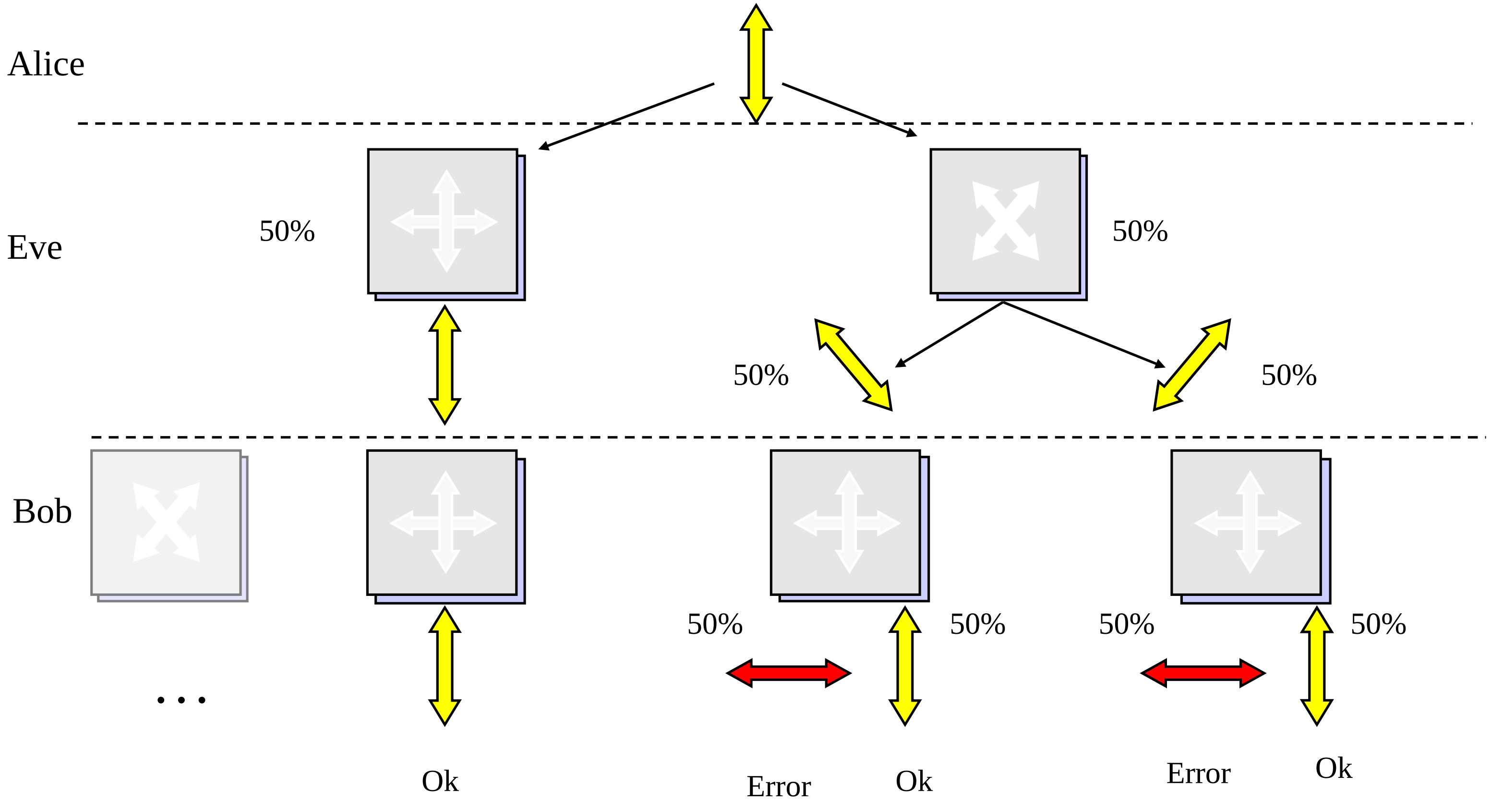


- Assumption: secure perimeters for Alice and Bob

BB84 protocol (Bennett, Brassard, 1984)



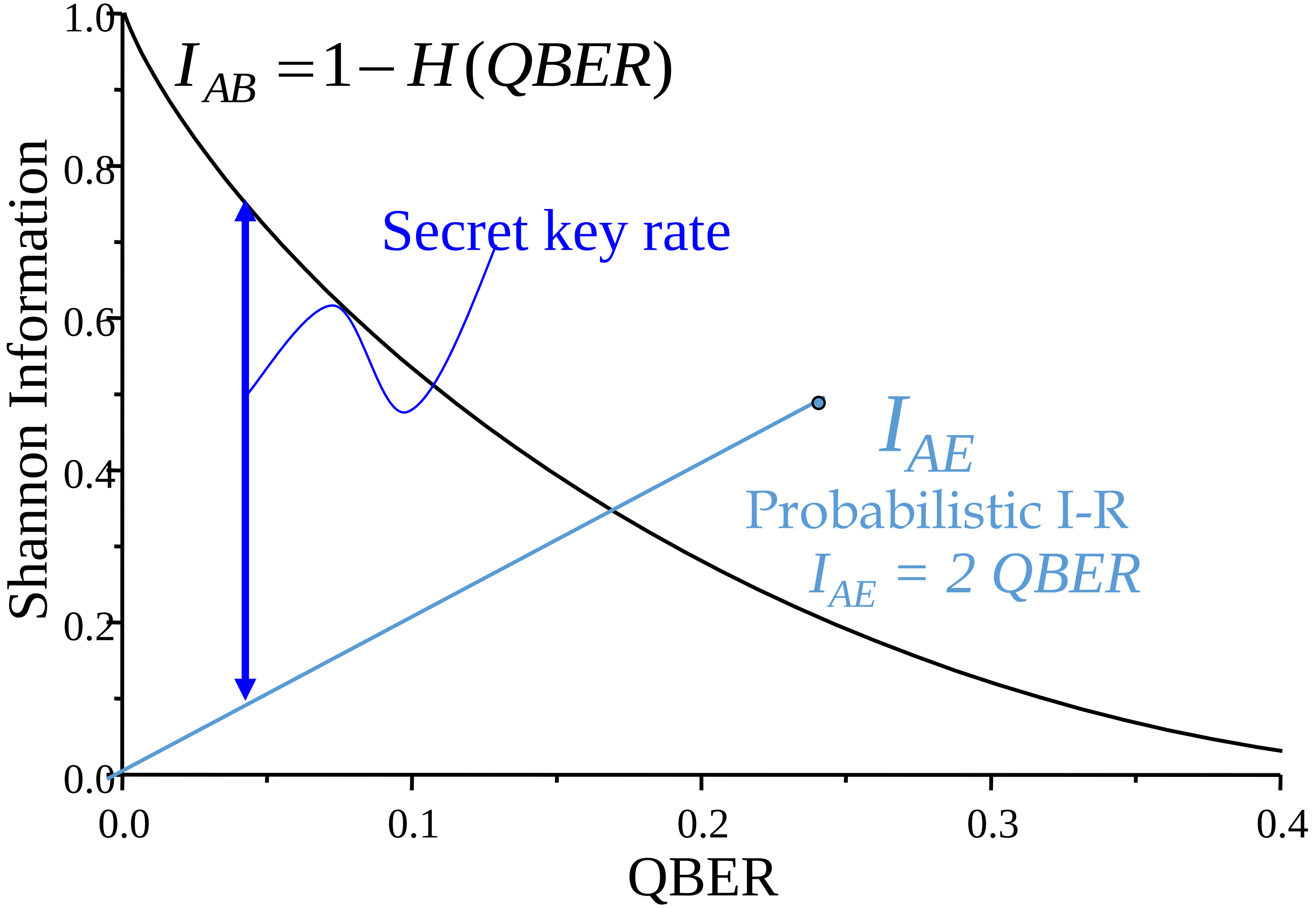
Eavesdropping (intercept-resend)



Error with 25 % probability

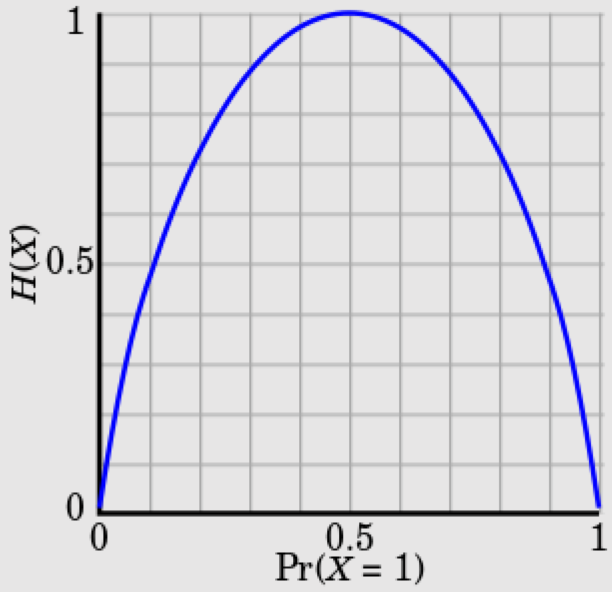
I_{AE} = *2 QBER (quantum bit error rate)*

Eve attacks: information curves

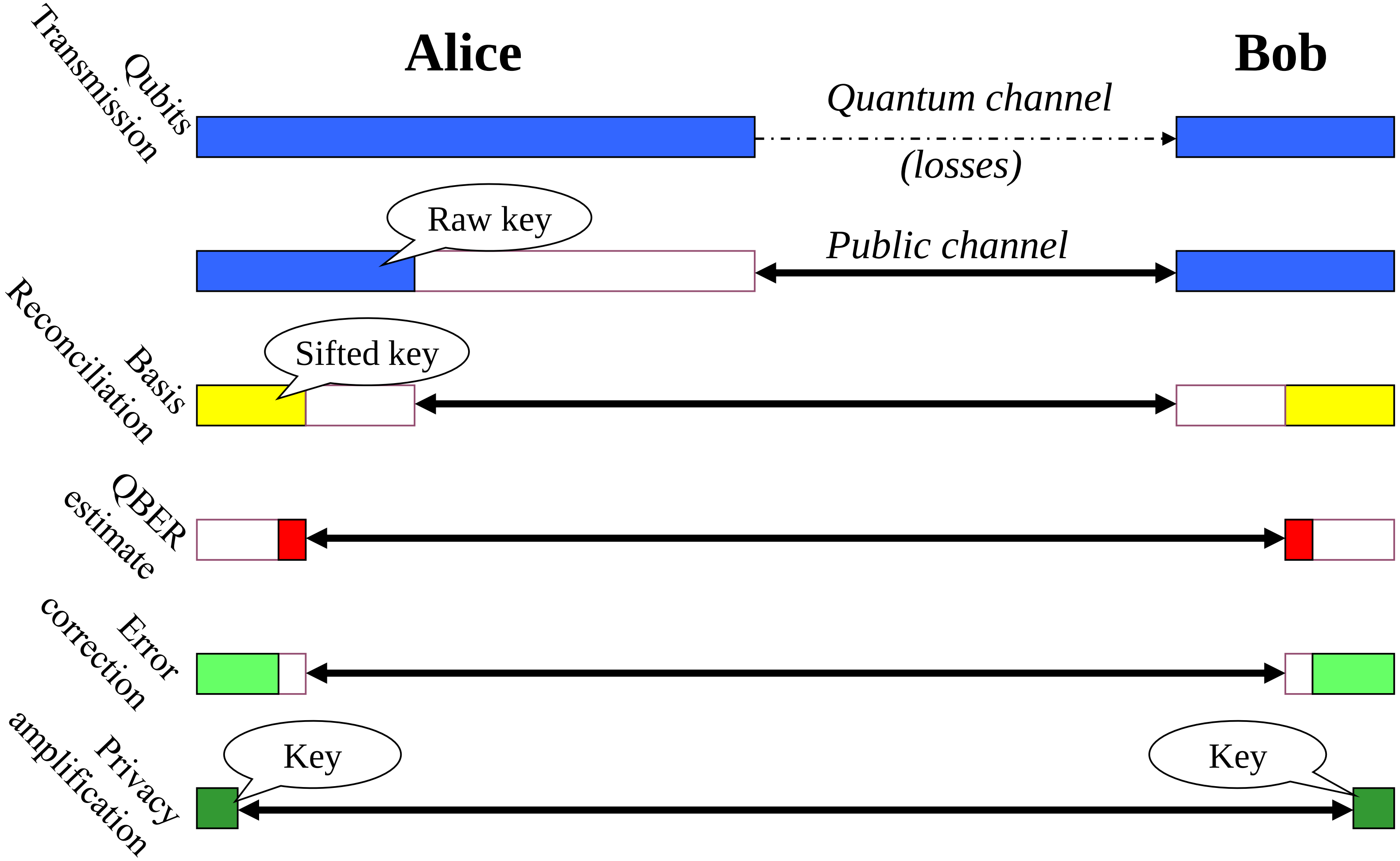


Binary Entropy function

$$H_b(p) = -p\log_2 p - (1-p)\log_2(1-p).$$

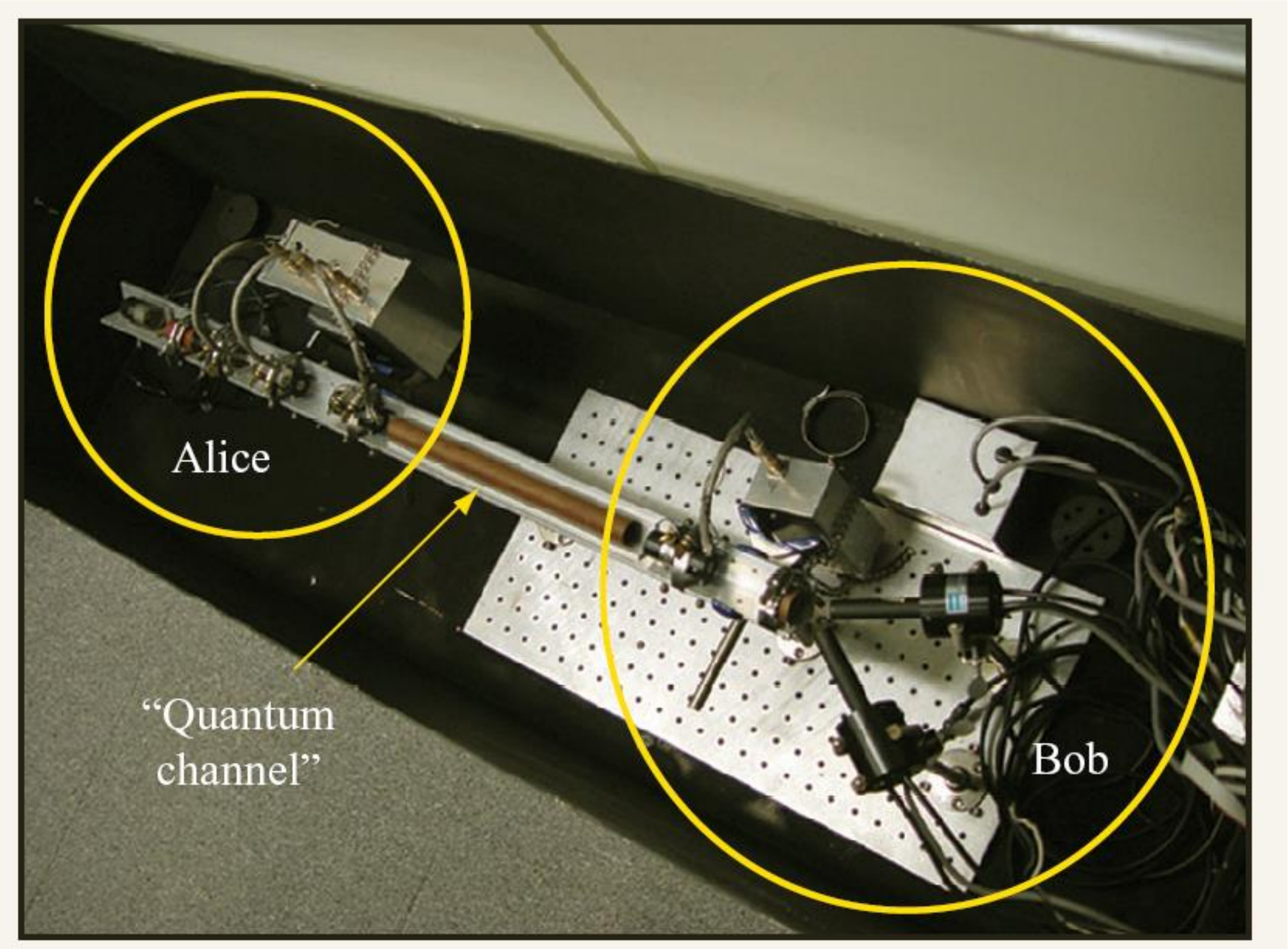


The steps to a secret key



+ Authentication!!!

Smolin and Bennett
IBM 1989



UNIVERSITÉ
DE GENÈVE

Swiss QCRYPT project (2013)

PHYSICAL REVIEW LETTERS **121,** 190502 (2018)

Editors' Suggestion | Featured in Physics

Secure Quantum Key Distribution over 421 km of Optical Fiber

Alberto Boaron,[1,*] Gianluca Boso,[1] Davide Rusca,[1] Cédric Vulliez,[1] Claire Autebert,[1] Misael Caloz,[1] Matthieu Perrenoud,[1] Gaëtan Gras,[1,2] Félix Bussières,[1] Ming-Jun Li,[3] Daniel Nolan,[3] Anthony Martin,[1] and Hugo Zbinden[1]

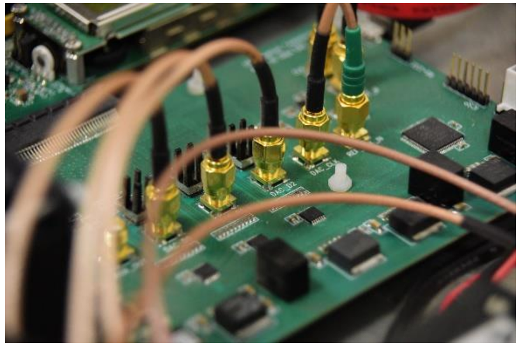
[1]*Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, 1211 Geneva 4, Switzerland*

[2]*ID Quantique SA, Chemin de la Marbrerie 3, 1227 Carouge, Switzerland*

[3]*Corning Incorporated, Corning, New York 14831, USA*

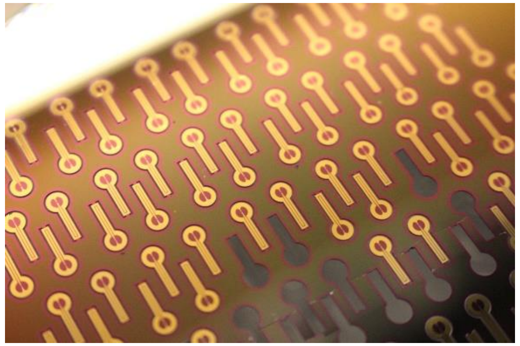
(Received 10 July 2018; published 5 November 2018)

New simple and efficient QKD protocol

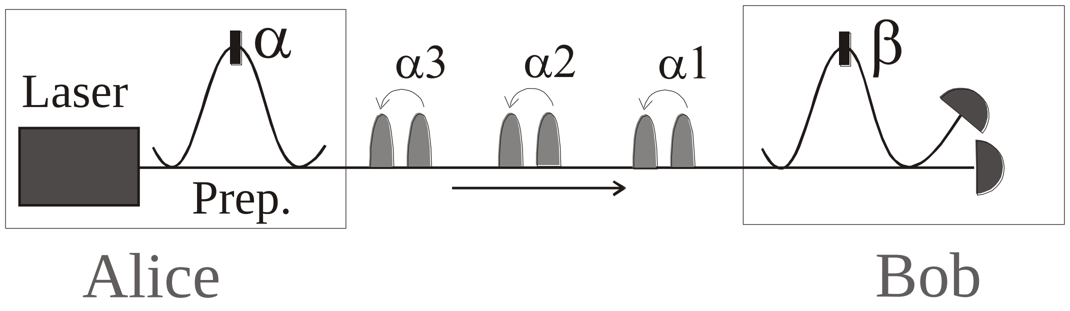


2.5 GHz repetition rate transmitter

Ultralow-loss fibers



Supeconducting detectors developed in QSIT

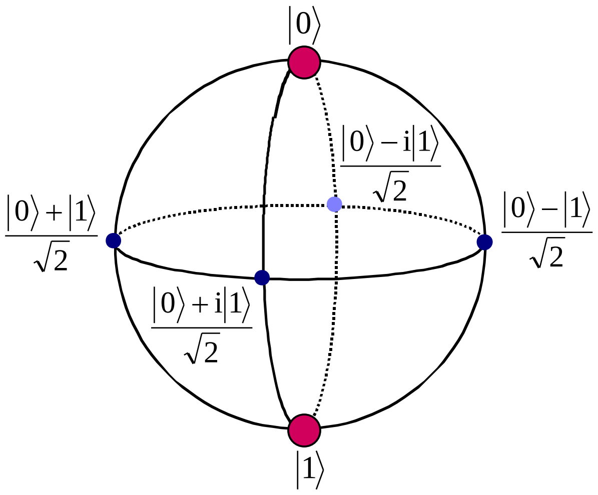


4 states $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\alpha}|1\rangle\right)$

2 bases

with probability 1/4:
α = 0, $\pi/2$, π, $3\pi/2$

with probability 1/2:
β = 0, $\pi/2$



Use the simplest basis for sending the key!

- 3-state time bin encoding
- 1-decoy level scheme

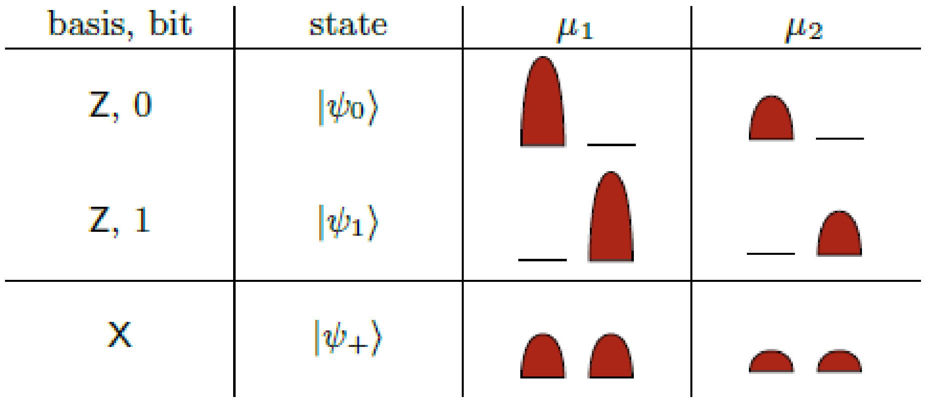
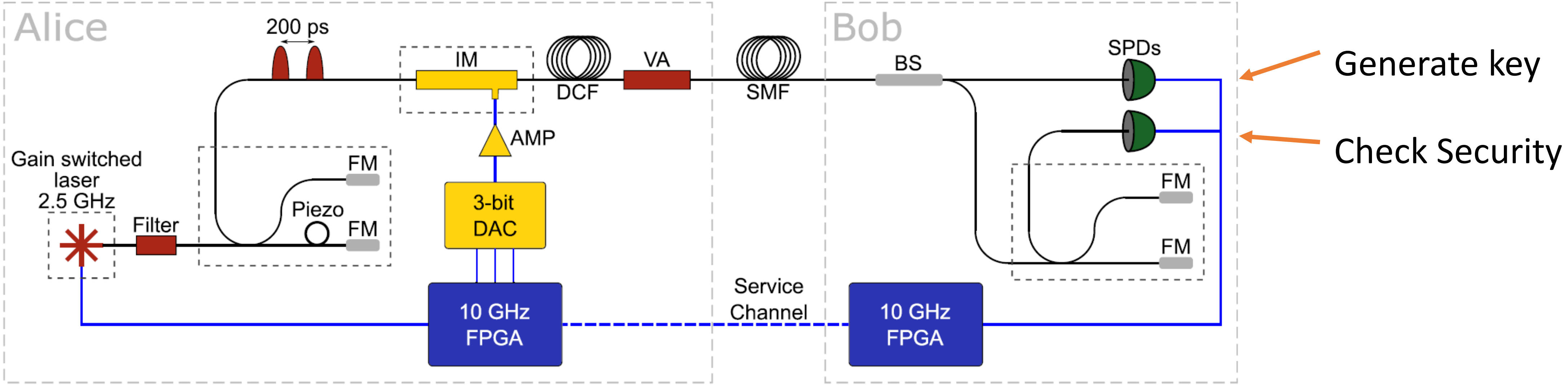


FIG. 1. Encoding of the states sent by Alice.



- Pulse rate 2.5 GHz
- Realtime error correction and privacy amplification

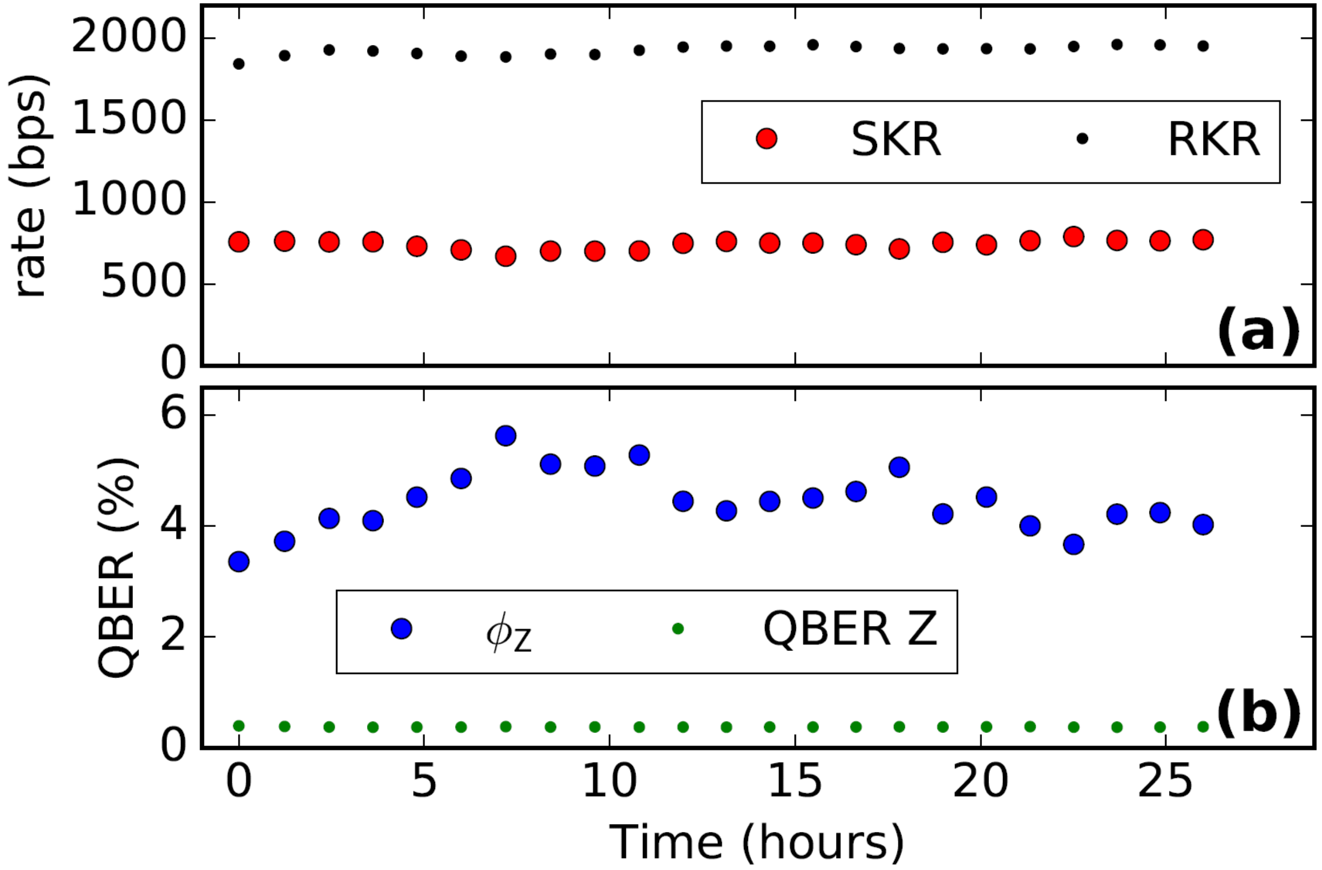
UNIVERSITÉ DE GENÈVE

QBER and stability over time

ArXiv 1807.03222

Channel length fluctuations

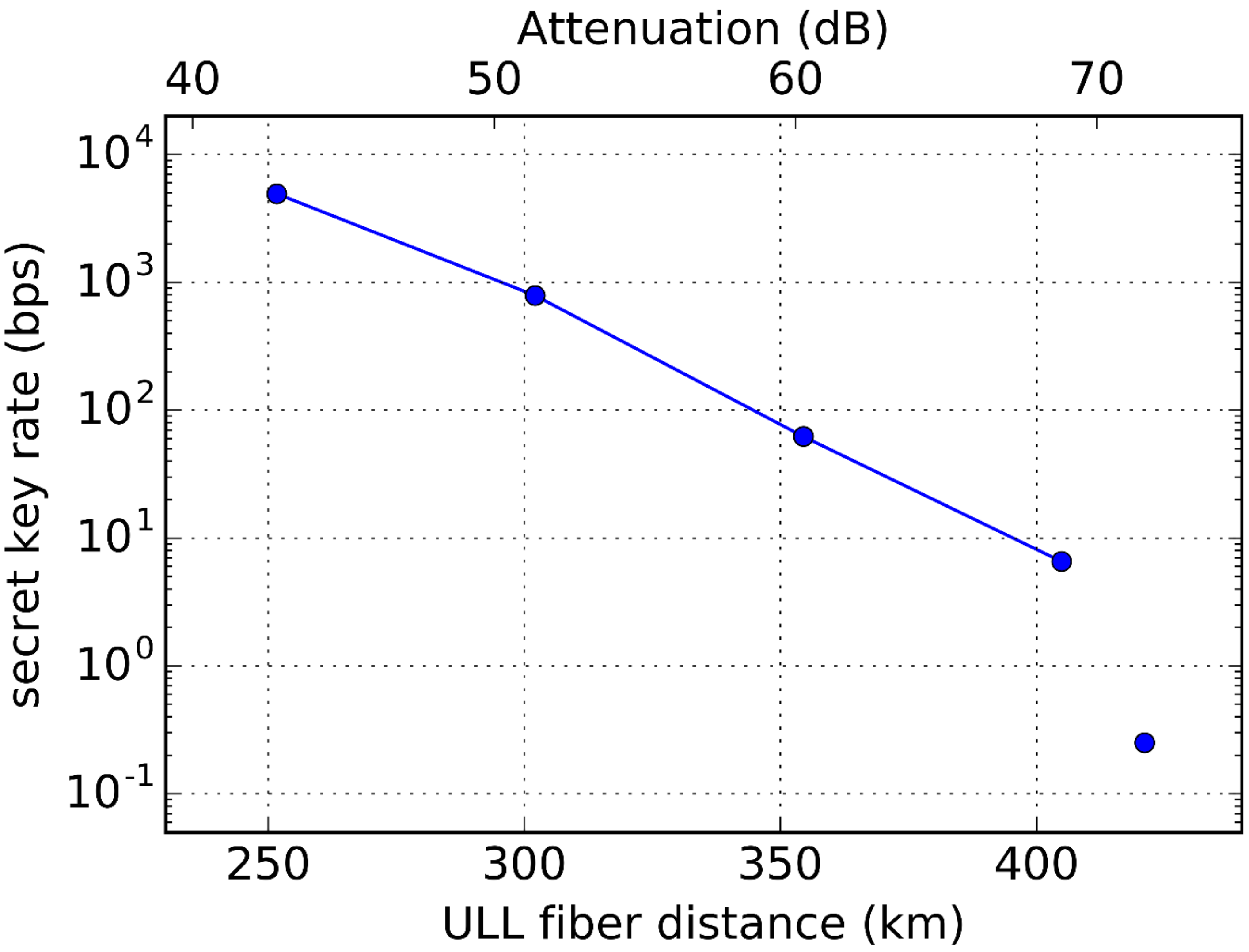
Interferometers phase fluctuations



Distance: 300 km

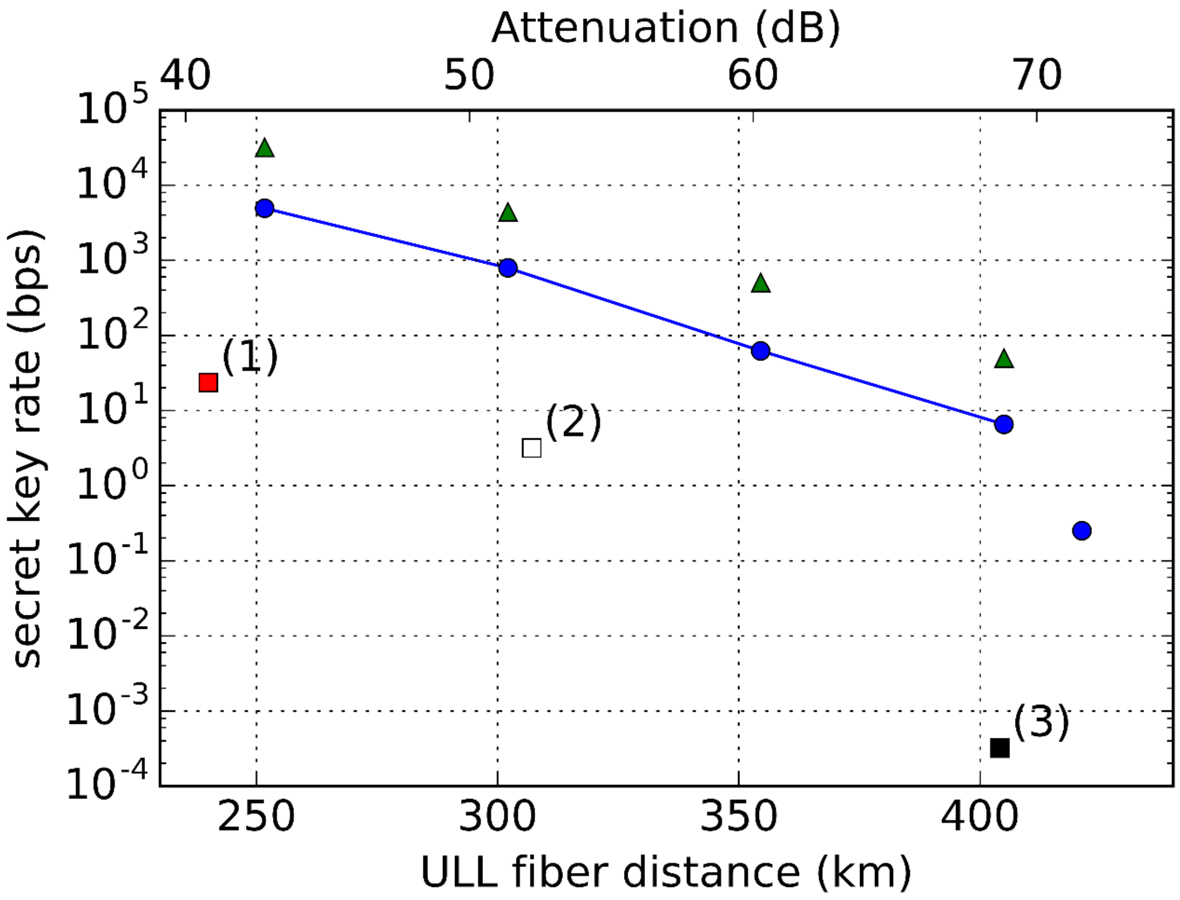
Secret key rate vs distance

ArXiv 1807.03222



UNIVERSITÉ DE GENÈVE

How close are we from an ideal system ?



Ideal system

- BB84 with decoy state
- 2.5 GHz repetition rate
- No detector noise
- 100% detection efficiency
- Same block size than exp. points

(1) **BB84**, Fröhlich et al., Optica **4**, 163 (2017)

(2) **COW**, Korzh et al., Nat. Phot. **9**, 163 (2015)

(3) **MDI**, Yin et al. Phys. Rev. Lett. **117**, 190501 (2016)

UNIVERSITÉ DE GENÈVE

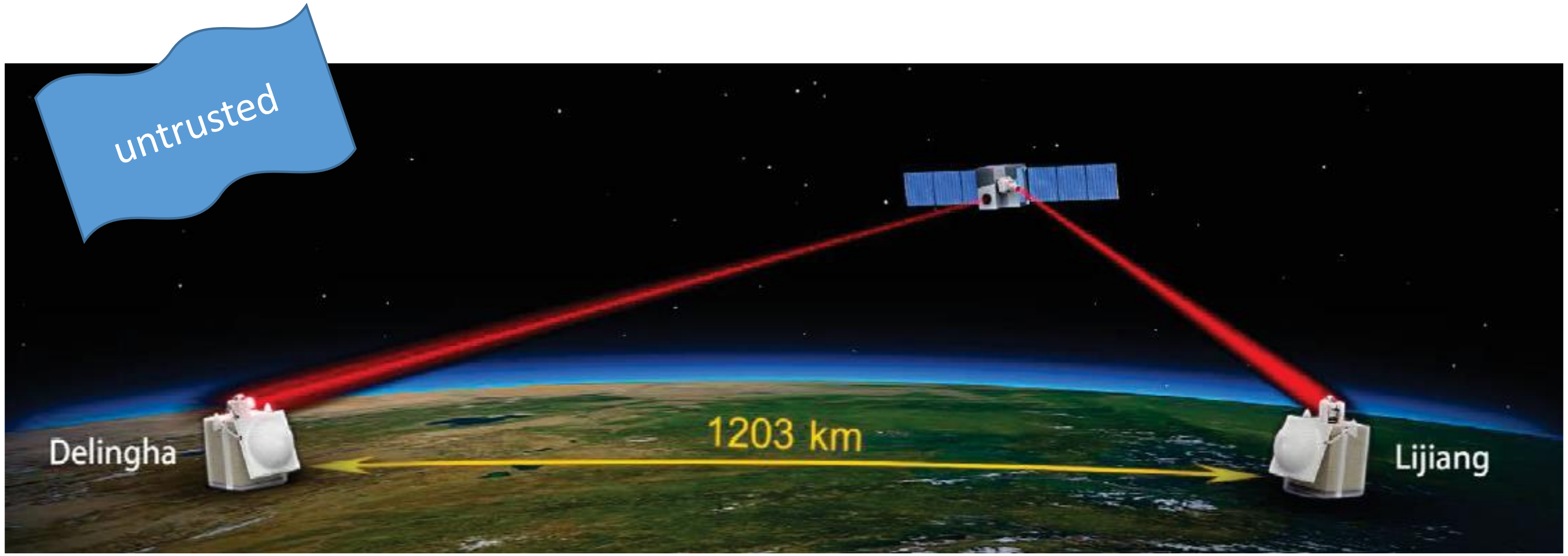
Current issues/developments

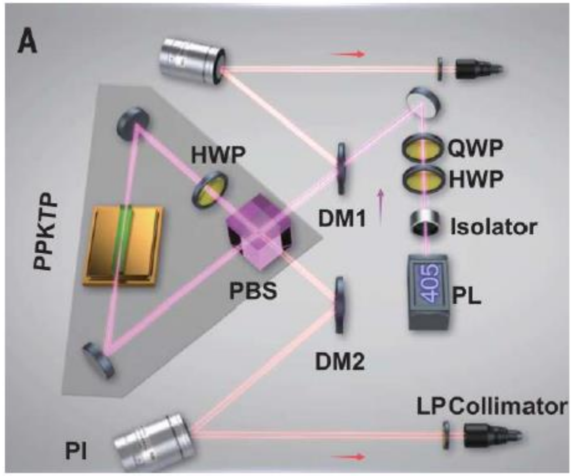
- Make it smaller, make it cheaper (integrated optics)

- Integration into telecom networks
- Longer distances (quantum repeater, satellite)
- Make it safer? Hacking

UNIVERSITÉ DE GENÈVE

UNIVERSITÉ DE GENÈVE





SPDC source:
810 nm
6 MHz pair generation rate

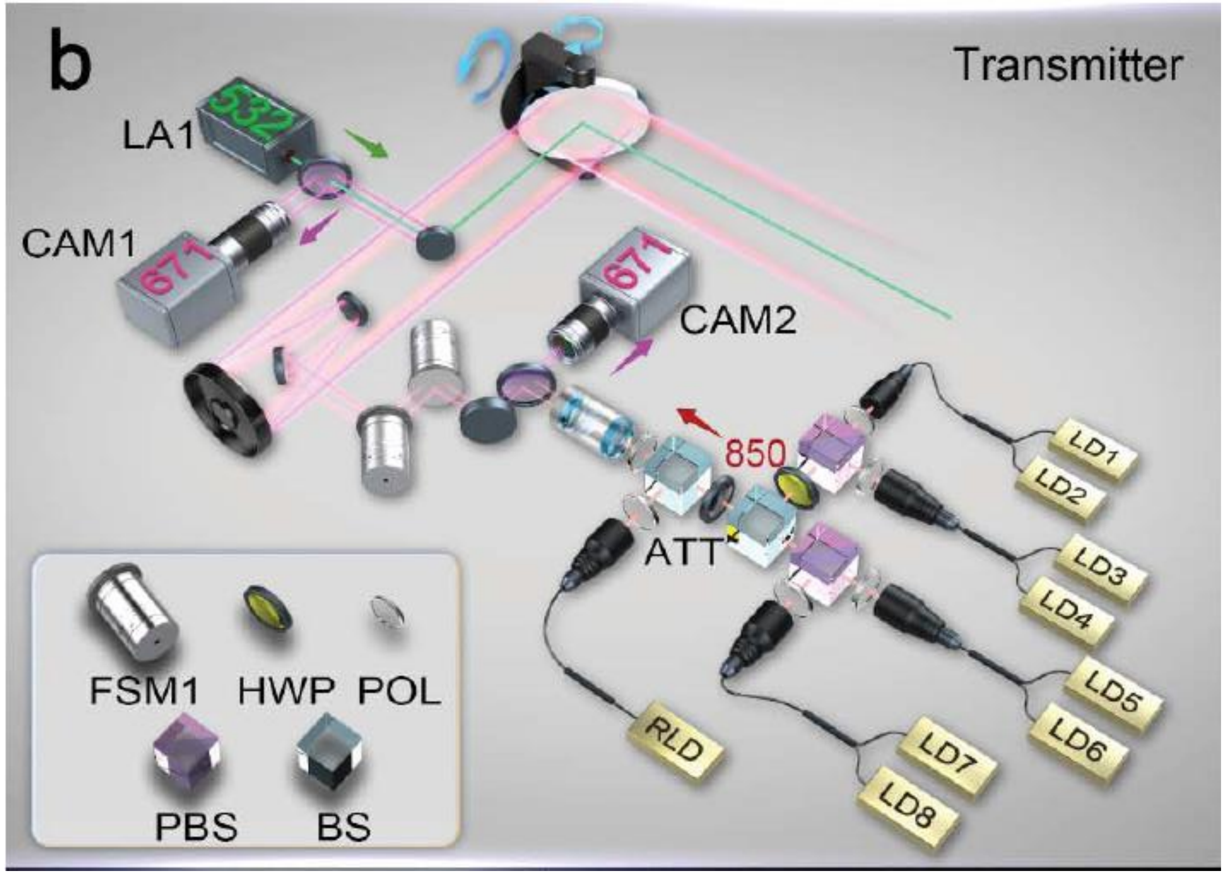
Total loss: ~65dB
Average coincidence count rate: 1Hz
275s coverage time
S=2.37 ± 0.09

Impossible to extract a key with small ε

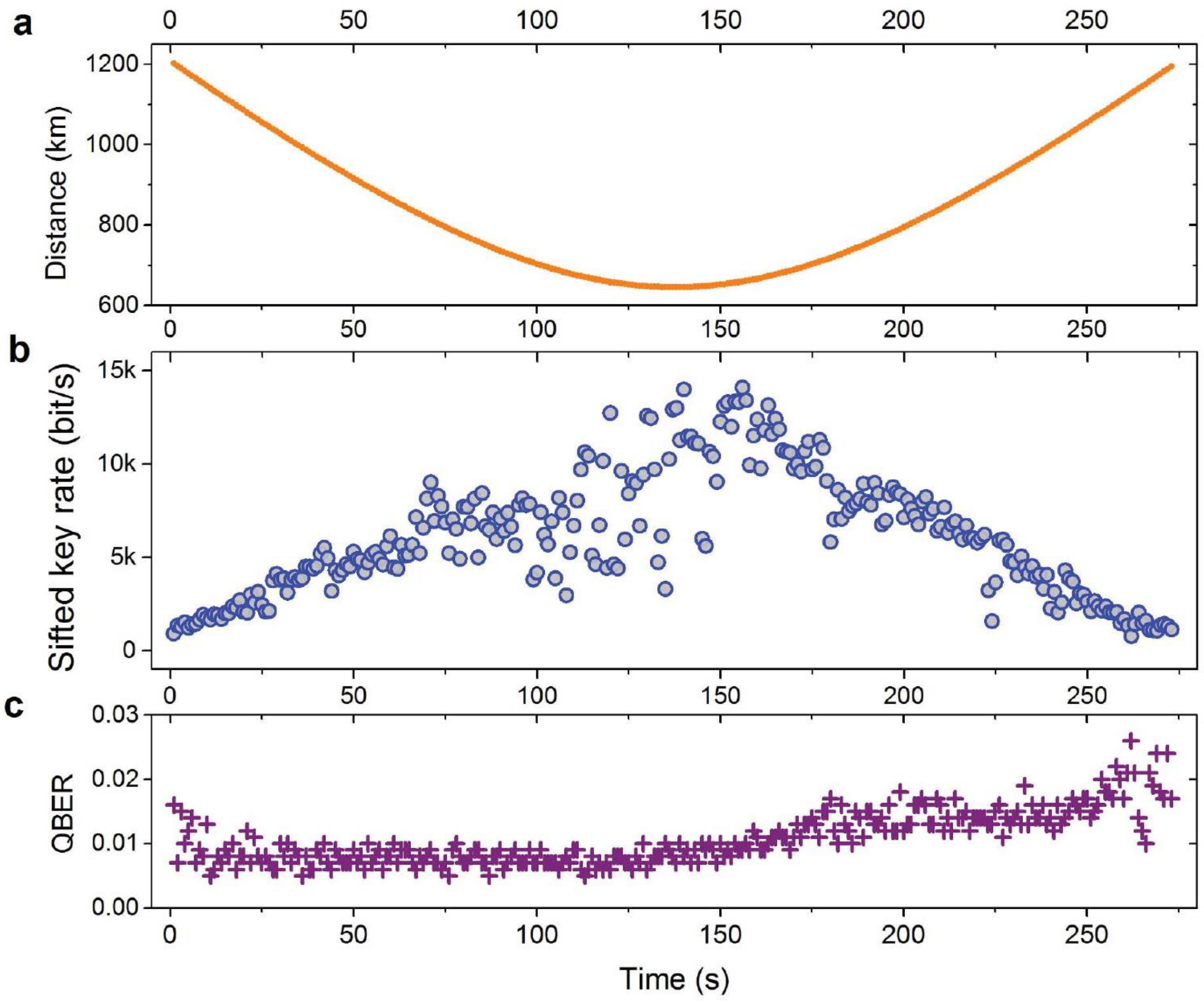
UNIVERSITÉ DE GENÈVE

Satellite to ground QKD

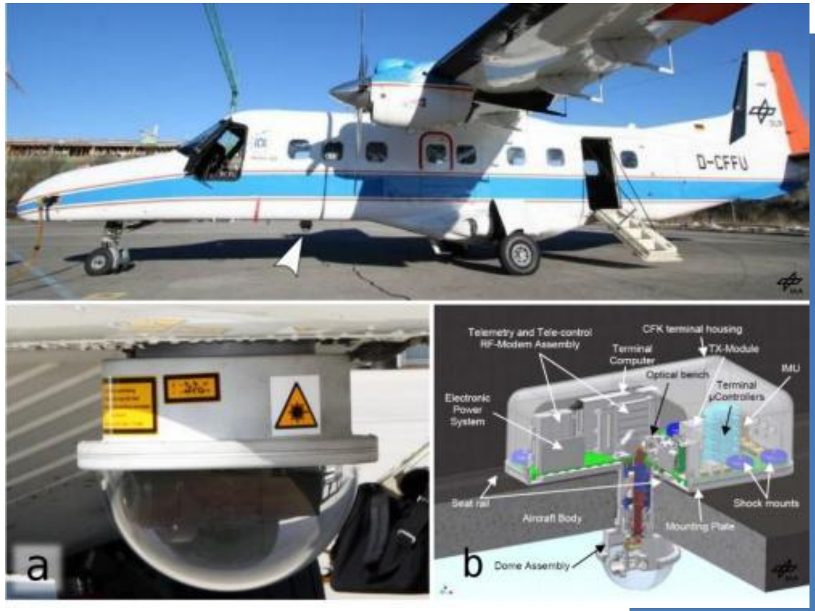
- just one downlink with decoy-state faint laser pulses (polarisation BB84)



Results


a
Distance (km)
1200
1000
800
600
b
Sifted key rate (bit/s)
15k
10k
5k
0
c
QBER
0.03
0.02
0.01
0.00
0
50
100
150
200
250
Time (s)

More accessible alternative: Drones ?

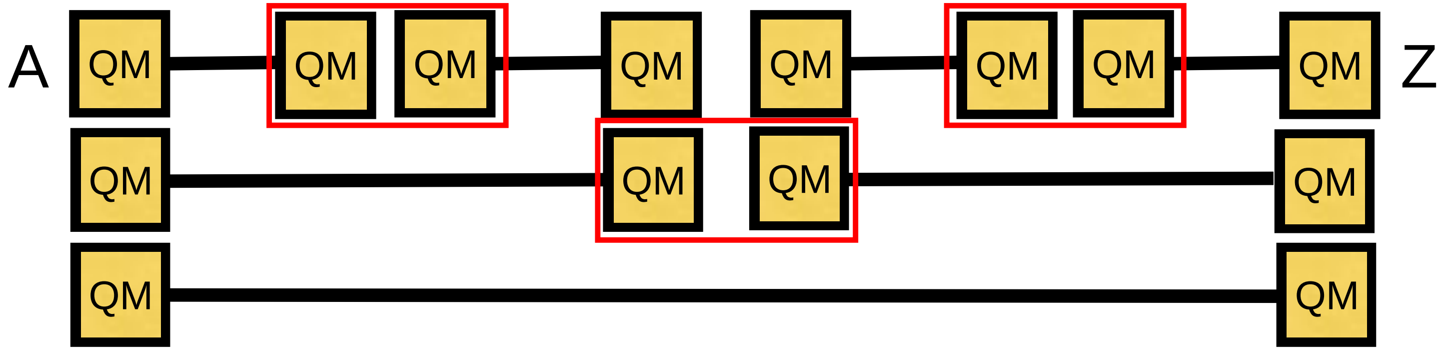


Conclusions

- State of the art of QKD: 400 km
- Higher distances with trusted repeaters or satellites /drones
- Quantum Repeaters are waiting for a quantum leap….

Quantum repeater

Create remote entanglement independently for each link.
Extend by swapping



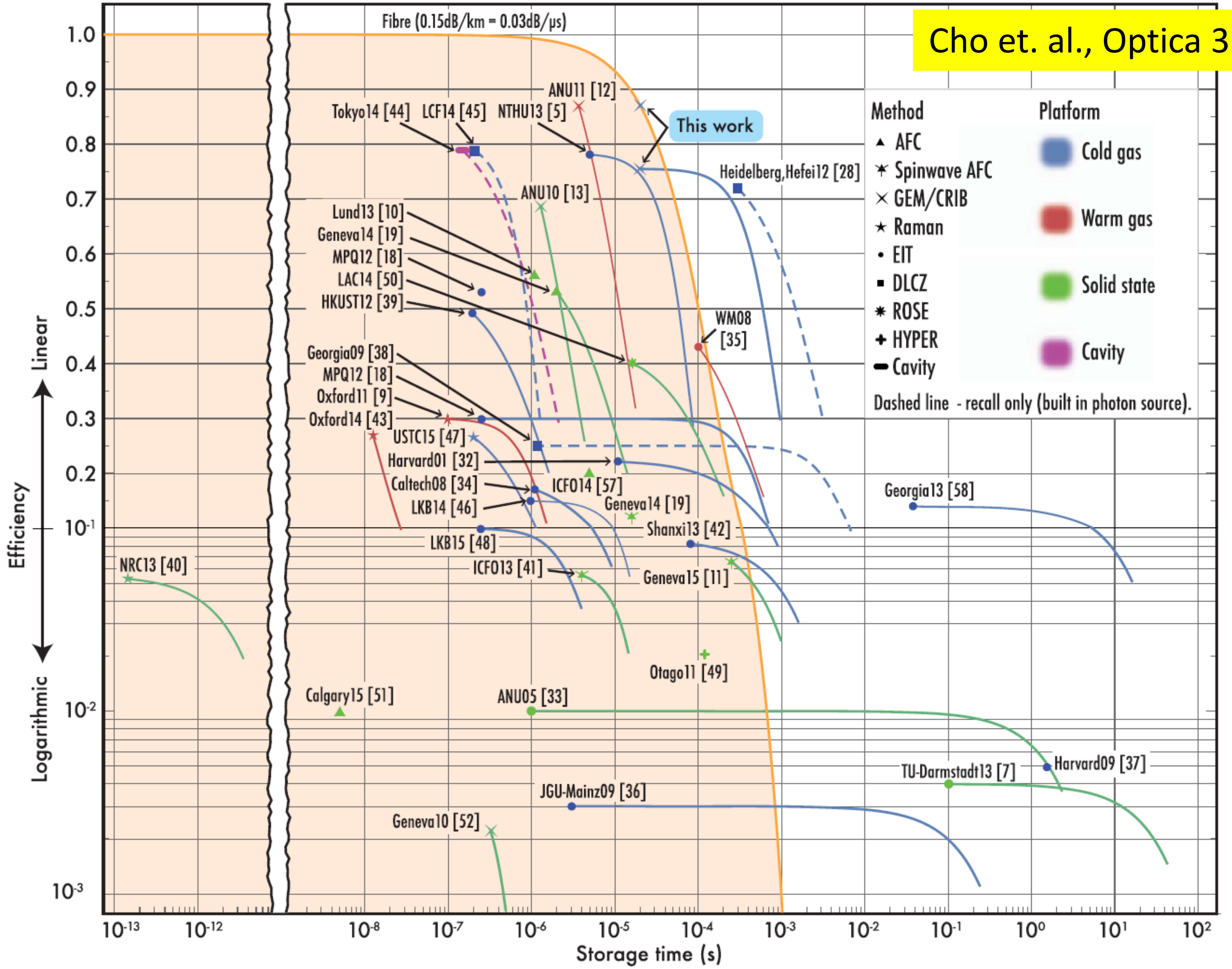
Direct transmission $T \sim \left(\frac{1}{\eta_t}\right)^n$

Repeater $T \sim \frac{1}{\eta_t}$

Requires heralded entanglement creation, storage and swapping of entanglement

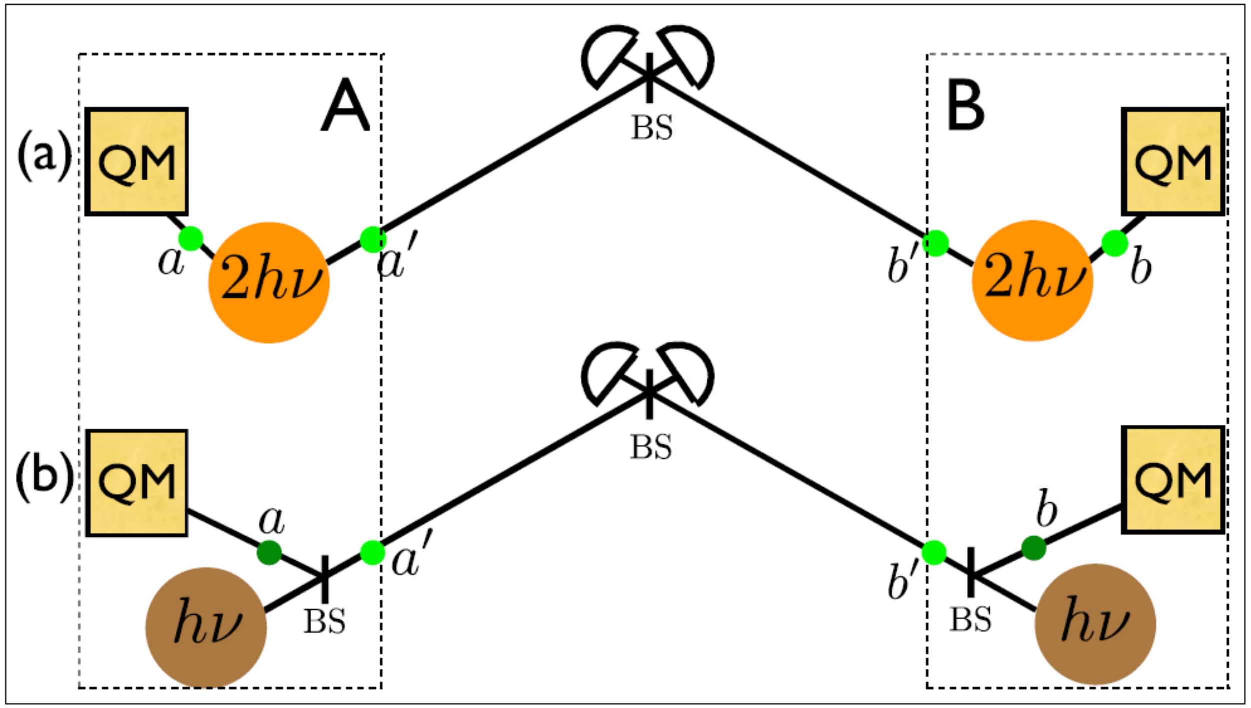
The quantum memory zoo

Cho et. al., Optica 3 (1), 2016



UNIVERSITÉ DE GENÈVE

DLCZ (entangled photon pairs) vs single photon scheme



1000km	Direct (1 link)	DLCZ (3 links)	SPS (3 links)
Time to transmit 1 bit	10^{10}s	4600s	250s

For p(1) = 95% , $\eta_{memory} = \eta_{det}$ = 90%, f = 10GHz

Sangouard et al. PRA **76**, 050301R 2007

UNIVERSITÉ DE GENÈVE

Long distance QKD
Comparison Satellite / quantum repeater

	Quantum repeater	Satellite untrusted	Trusted repeater	Satellite trusted
Operating conditions	24h/24h complex untrusted network	273s/24h weather dependent Telescopes in "dark zones"	24h/24h trusted network	273s/24h weather dependent Telescopes in "dark zones"
Rate (~1000 km)	0.005 Hz	1 Hz 0.003 Hz (24h average)	1kbit/s (5 links)	1kbit/s (unlimited distance) 3bit/s (24h average)
Available today?	no!	Yes!	Yes!	Yes!
Cost	10-20 M$ + infrastructure	200 M$? + infrastructure	500 k$ + infrastructure	200 M$? + infrastructure

UNIVERSITÉ DE GENÈVE