How can Quantum Cryptography Contribute to Cyber-Security ?

Nicolas Gisin and Hugo Zbinden

GAP-Optique, University of Geneva

- Quantum as an entropy source :

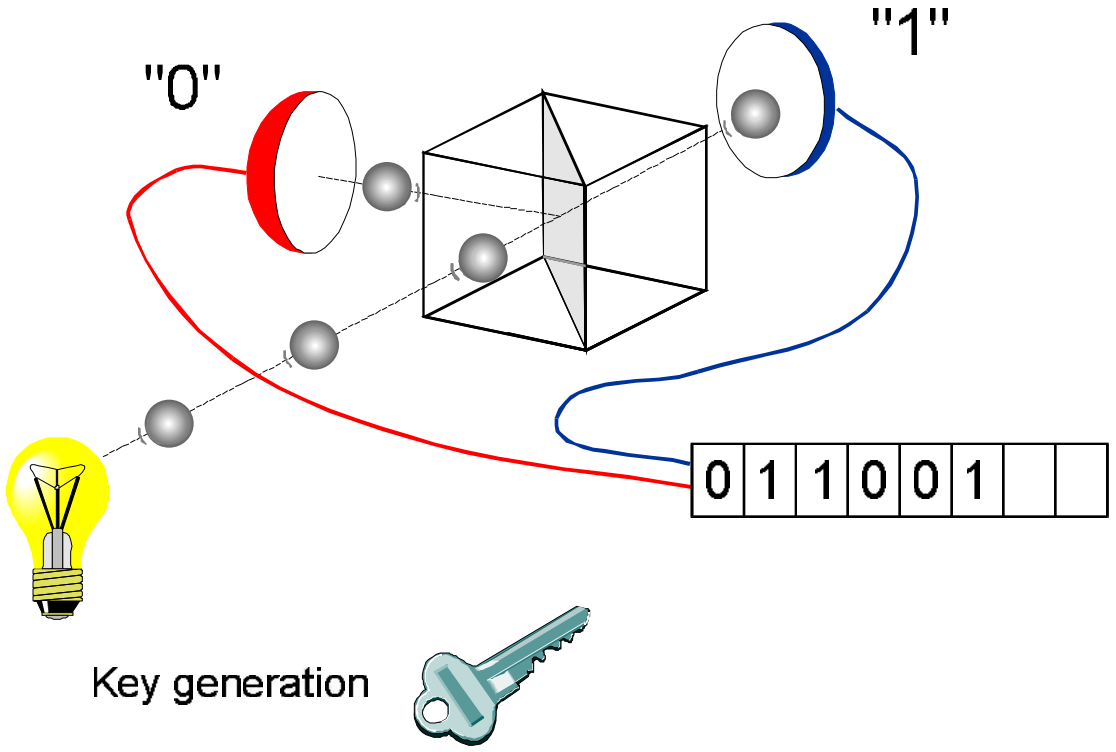
  Quantum Random number Generator QRNG

- Quantum as a building block for cryptography :

  Quantum Key distribution QKD

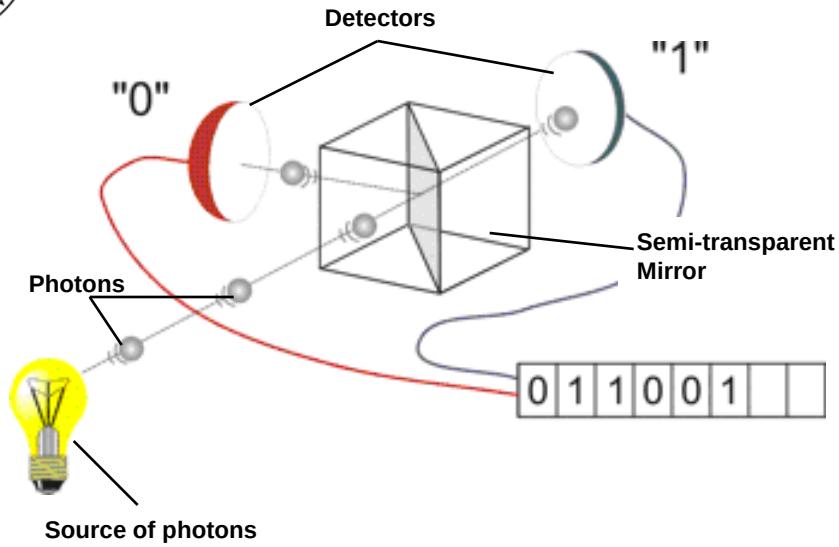
GAP Quantique

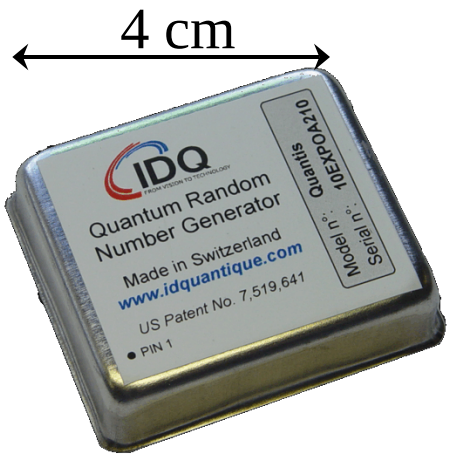
Physics of a beam-splitter

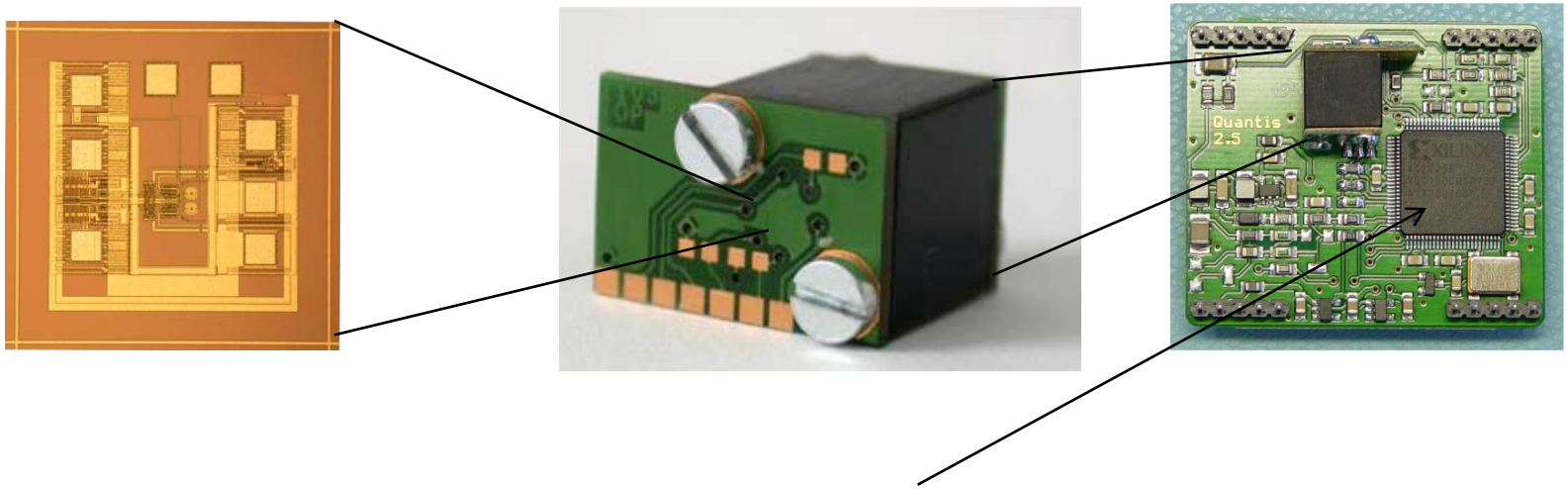


- A conceptually simple entropy source
- Only quantum physics offers fundamental randomness
- Easy to pindown the origine of the randomness
- A practical random number generator

Quantum Random Number Generator





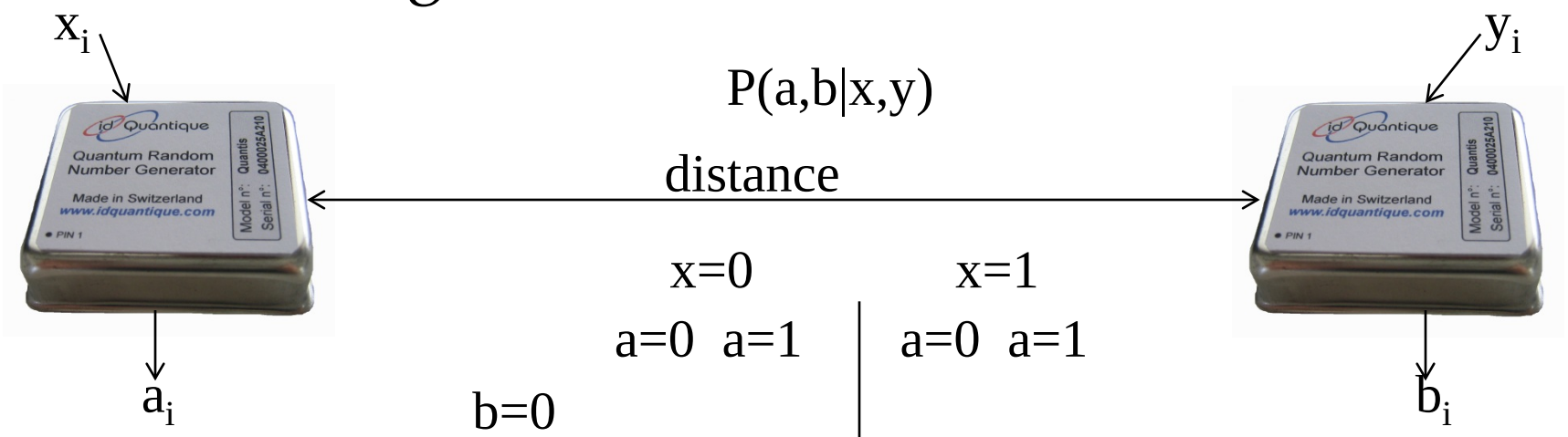


4 Mb per second of balanced random bits

GAP Quantique

Why are we convinced that the bits are truly random?

- The very same hardware can be used in a nonlocal game:

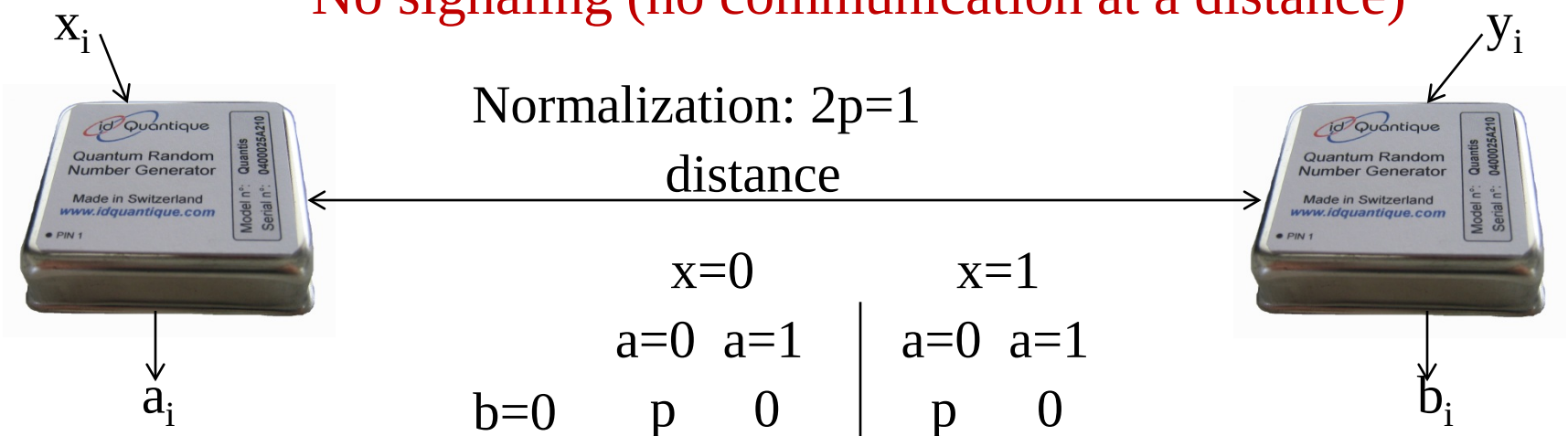


GAP Quantique

Why are we convinced that the bits are truly random?

- Promise: $a \oplus b = x \cdot y$

No signaling (no communication at a distance)



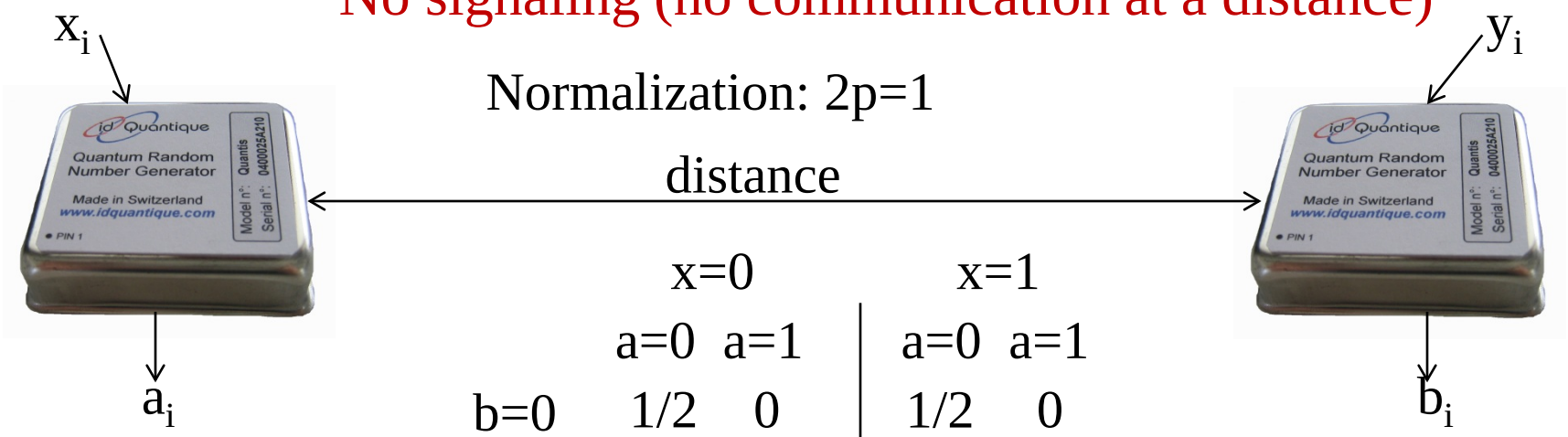
		x=0		x=1	
		a=0	a=1	a=0	a=1
y=0	b=0	p	0	p	0
	b=1	0	p	0	
y=1	b=0		0	0	
	b=1	0	p	p	0

GAP Quantique

Why are we convinced that the bits are truly random?

- Promise: $a \oplus b = x \cdot y$

No signaling (no communication at a distance)



		x=0		x=1	
		a=0	a=1	a=0	a=1
y=0	b=0	1/2	0	1/2	0
	b=1	0	1/2	0	1/2
y=1	b=0	1/2	0	0	1/2
	b=1	0	1/2	1/2	0

GAP Quantique

Random Sequences

Intuitive Definition

Sequence of numbers which are unpredictable

Rigorous Definition

Sequence for which a definition shorter than itself does not exist

00000…00000 = n x ‘0’

Concept applies only to an infinite sequence

Finite Random Sequences

- Impossible to prove randomness
- But possible to prove the existence of random processes.
- A random process produces with unit probability a sequence of maximal Kolmogorov complexity (Per Martin-Löf, Information and Control 9, 602-619, 1966)

When generating random numbers, it is very important to understand the method used.

Mind your Random Number Generator!

To appear in *Proceedings of the 21st USENIX Security Symposium*, August 2012. Initial public release; July 2, 2012.
For the newest revision of this paper, partial source code, and our online key-check service, visit **https://factorable.net**.

Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices

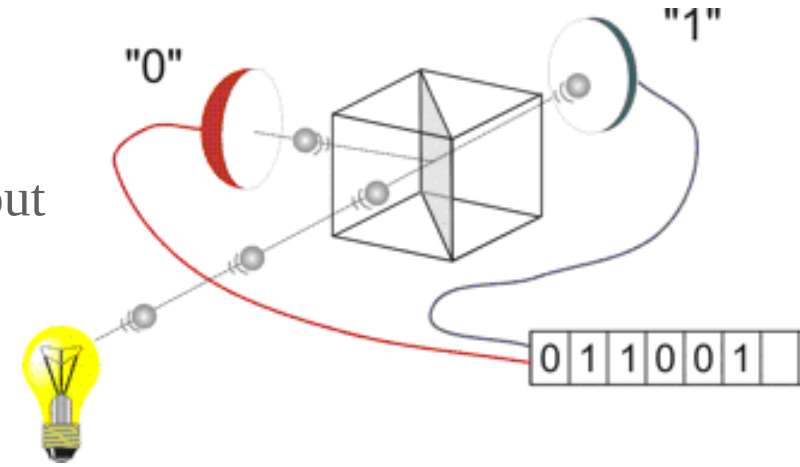
Nadia Heninger[†*] Zakir Durumeric[‡*] Eric Wustrow[‡] J. Alex Halderman[‡]

[†] *University of California, San Diego*
nadiah@cs.ucsd.edu

[‡] *The University of Michigan*
{zakir, ewust, jhalderm}@umich.edu

Advantages

- Truly random process
  → produces truly random sequences
- Simple process that can be modelled
  → influence of environment can be ruled out
- Live monitoring of elementary components
- Speed



GAP Quantique

Evaluation and Certification

Non-Deterministic (Physical) RNG

- PTG.1

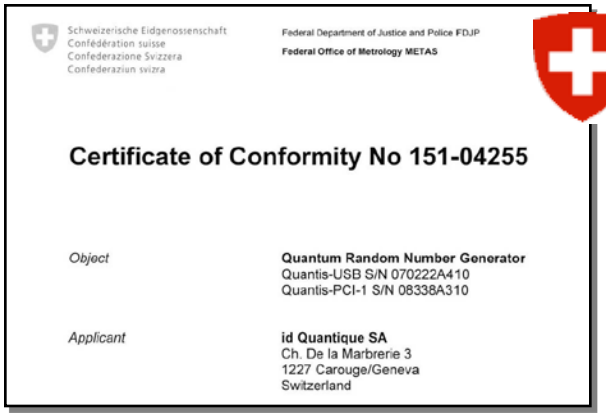
Physical RNG with internal tests that detect a total failure of the entropy source and non-tolerable statistical defects of the internal random numbers

- PTG.2

PTG.1, additionally a stochastic model of the entropy source and statistical tests of the raw random numbers

- PTG.3

PTG.2, additionally with cryptographic post-processing (hybrid PTRNG)



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP
Federal Office of Metrology METAS

Certificate of Conformity No 151-04255

Object — **Quantum Random Number Generator**
Quantis-USB S/N 070222A410
Quantis-PCI-1 S/N 08338A310

Applicant — **id Quantique SA**
Ch. De la Marbrerie 3
1227 Carouge/Geneva
Switzerland

Quantum Key Distribution (QKD)

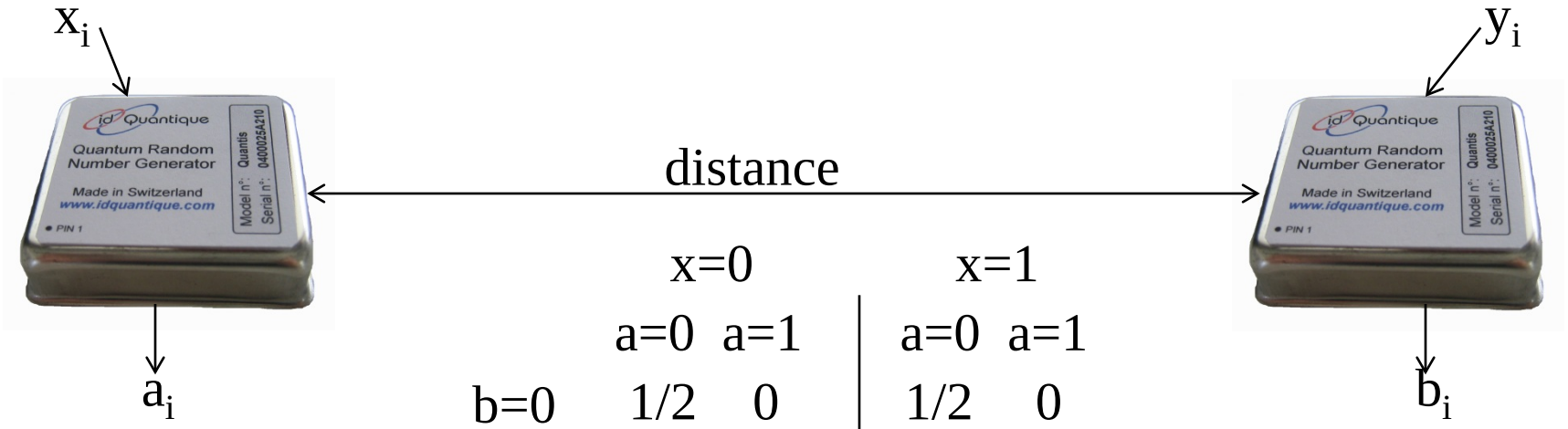
- Nature offers more than mere randomness:

Nonlocal distributed randomness:
a random event that manifest itself at more than one location.

- It looks like magic, but is well mastered physics.
- It would be absurd not to exploit this gift of nature.

Nonlocal distributed randomness

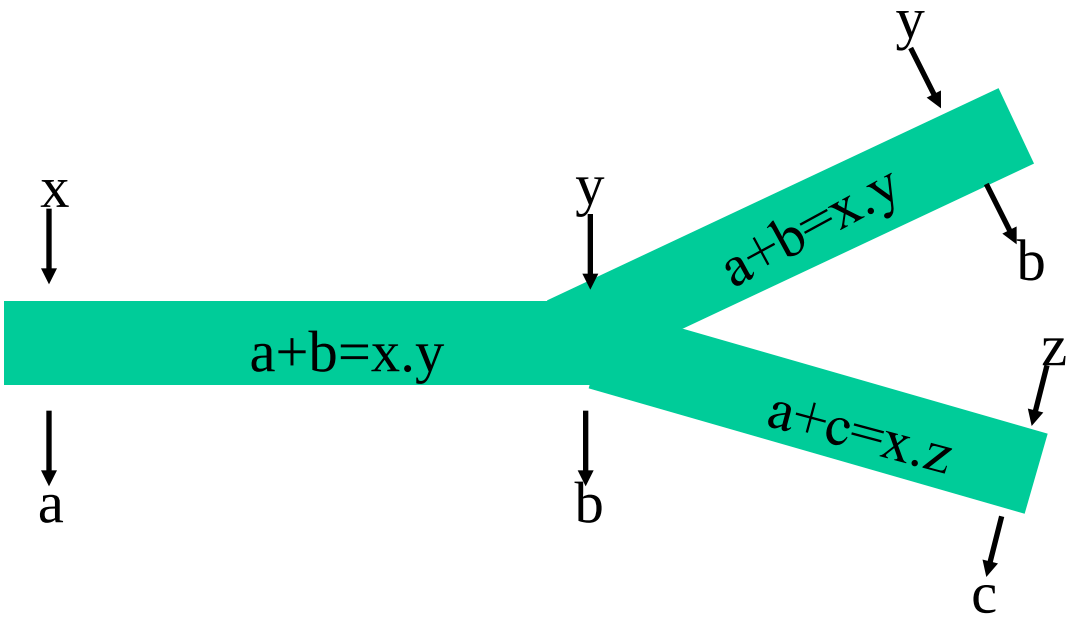
- The same random sequence of bits is produced at Alice and Bob sides:



		x=0		x=1	
		a=0	a=1	a=0	a=1
y=0	b=0	1/2	0	1/2	0
	b=1	0	1/2	0	1/2
y=1	b=0	1/2	0	0	1/2
	b=1	0	1/2	1/2	0

GAP Quantique

No-cloning from no-signaling



$\Rightarrow b+c = x.(y+z)$

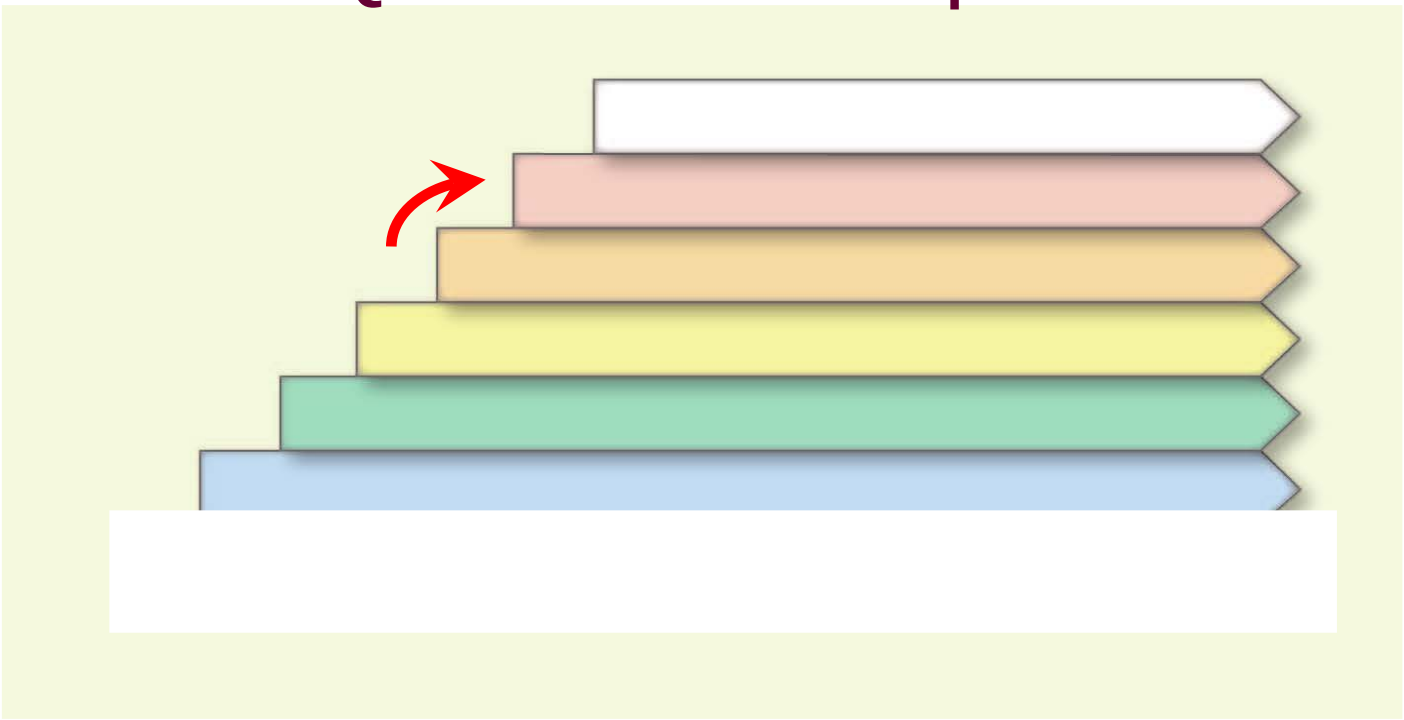
$\Rightarrow$ If $y+z=1$, Bob and Charly can deduce Alice's input out of their outputs

$\Rightarrow$ Signaling !!!

$\Rightarrow$ In a non-signaling world, quantum cloning is impossible.

GAP Quantique

When shall we have a Quantum Computer ?



Change in perception

Quantum Safe Crypto

- Post-Quantum Crypto
  = Complexity-based classical algorithms resistant to known Q attacks

+ not much change for the security experts.

- again a wild bet on the unknown.

- vulnerable backwards.

- QKD
  = Physics-based, proven resistant do Q attacks

+ provable security.

+ backward security.

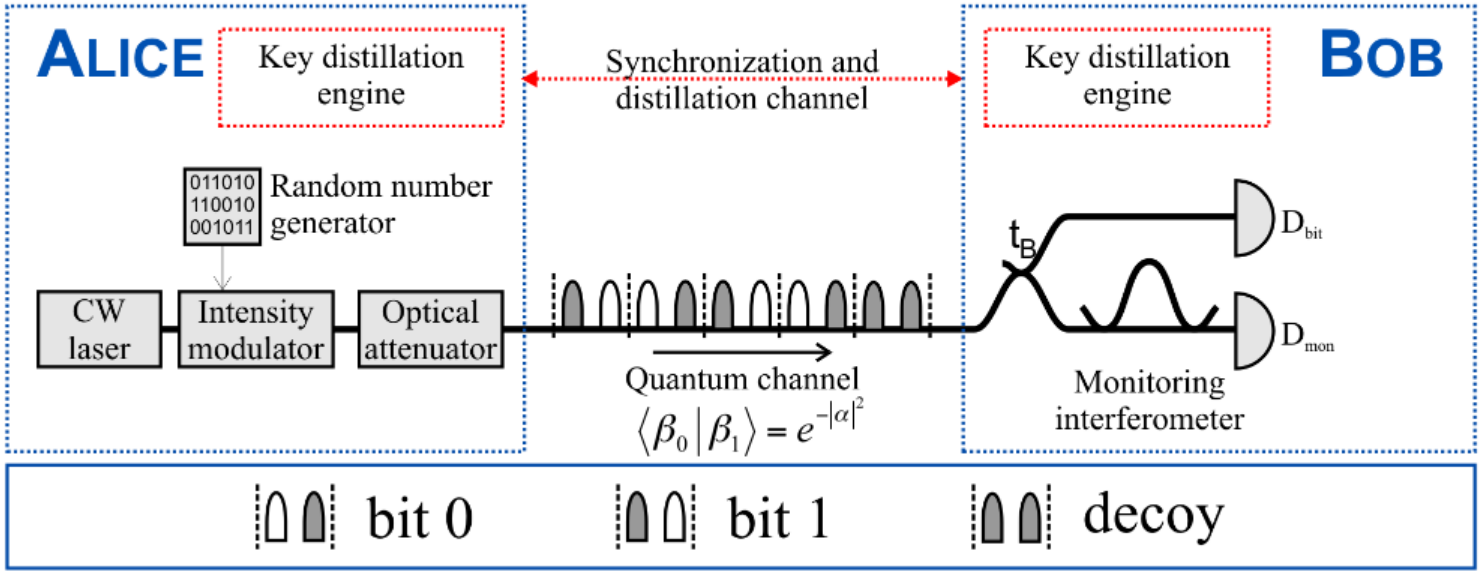
- expensive.

- big change of infrastructure and mentality.

- Likely that each will find some applications, the real question is about the size of each market.
- Each needs true random bits.

GAP Quantique

Coherent one-way QKD

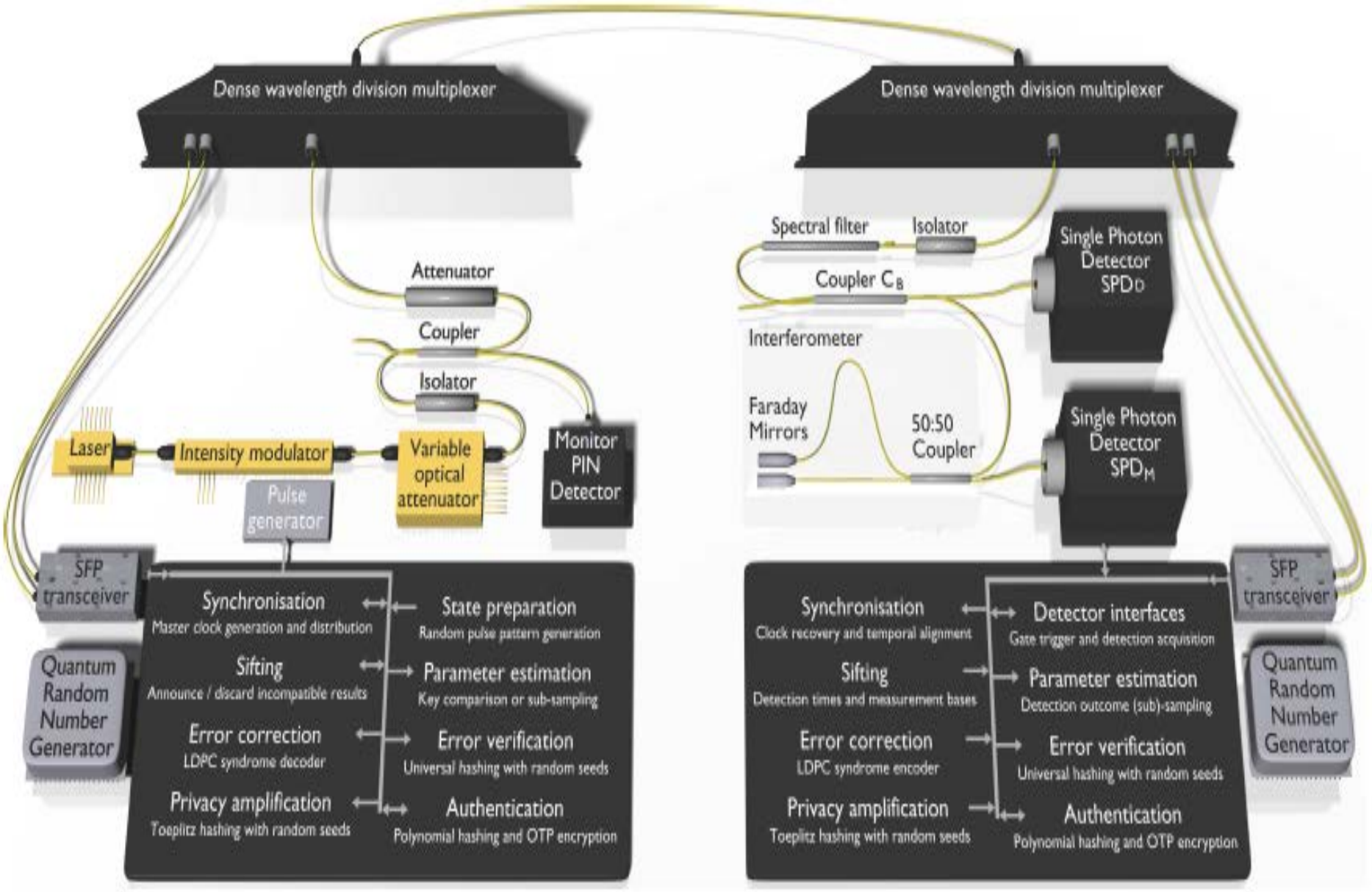


→ QBER

→ Visibility

- D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "*Fast and simple one-way quantum key distribution*," Appl. Phys. Lett. 87, 194108 (2005)
- C. Branciard, N. Gisin, and V. Scarani, "*Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography*," New J Phys. 10, 013031 (2008)
- N. Walenta et al, "*A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing*," New J. Phys. 16, 013047 (2014)
- T. Moroder et al., Security of Distributed-Phase-Reference Quantum Key Distribution, Phys. Rev. Lett. 109, 260501 (2012)

QKD engine @ 625 MHz



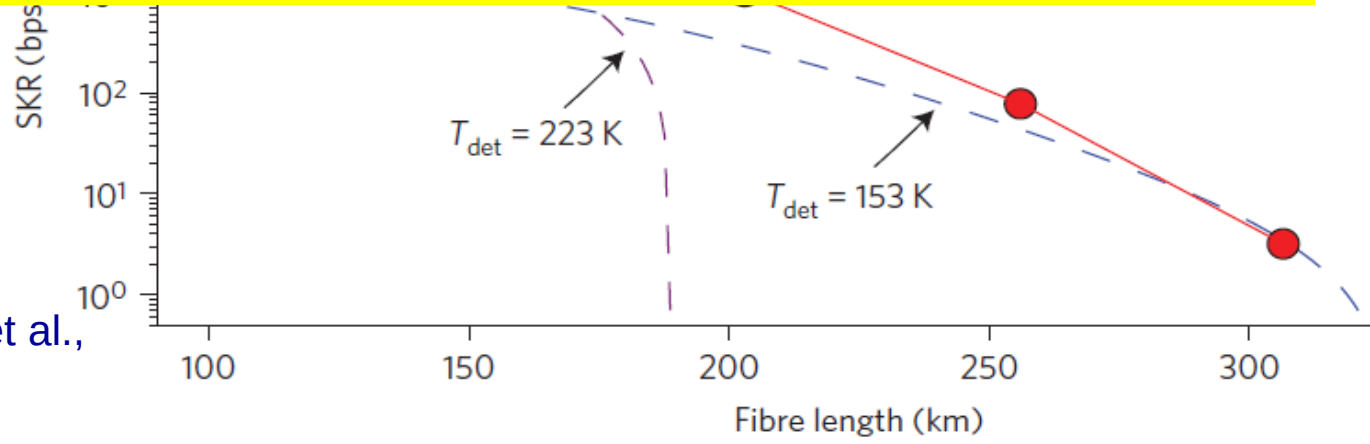
Integrated QKD Engine

- Built on the Advanced Telecommunication Computing Architecture (ATCA).
- Provides standardized mechanical, power, and data interfaces.
- Provides network services, cooling, power supplies.
- Scalable architecture, familiar to potential clients.

GAP Quantique

QKD over 307 km with real time secret key distillation and finite key analysis

- Integration into ATCA blades
- A vision of a QKD engine producing 1 Gb/s of provably secret bits is on the horizon.



B. Korzh, C. W. Lim et al.,
Nature Photonics
9, 163-168 (2015)

GAP Quantique

Example of a commercial link running continuously since 2011

Lausanne

Nyon

67 km

Genève

IDQ
FROM VISION TO TECHNOLOGY

Installed multiplexed quantum channel for commercial users.

GAP Quantique

What does QKD achieve

1. Attacks have to be launched on the spot
   ⇒ immune to future progress
2. With only the assumption of proper implementation
   ⇒ key expansion
3. Assuming short term secure of 1-way function
   ⇒ Cryptographic Key Distribution with long term security

1. QKD with one-time-pad (limited to the bit rate of QKD, i.e. Mb/s)
   ⇒ allows for information theoretical everlasting security.
2. QKD allows to change the session key of AES very frequently
   ⇒ limited data available for cryptanalysing and limited motivation for an adversary.

GAP Quantique

QKD versus AES

1. Today's commercial QKD engines are slow
   ⇒ they only provide cryptographic keys for AES sessions.
2. Why not merely use another AES system to distribute the session keys (re-keying)?

1. The keys should be produced by the best random number generators, i.e. by Quantum RNG.
2. AES is vulnerable forwards and backwards, QKD is immune backwards (and forwards the adversary can't miss a single photon).
3. The security of the principle of QKD is based on a well tested mathematical model.
   The security of the principle of AES rests on faith.

GAP Quantique

nature photonics

Access

To read this story in full you will need to login or make a payment (s

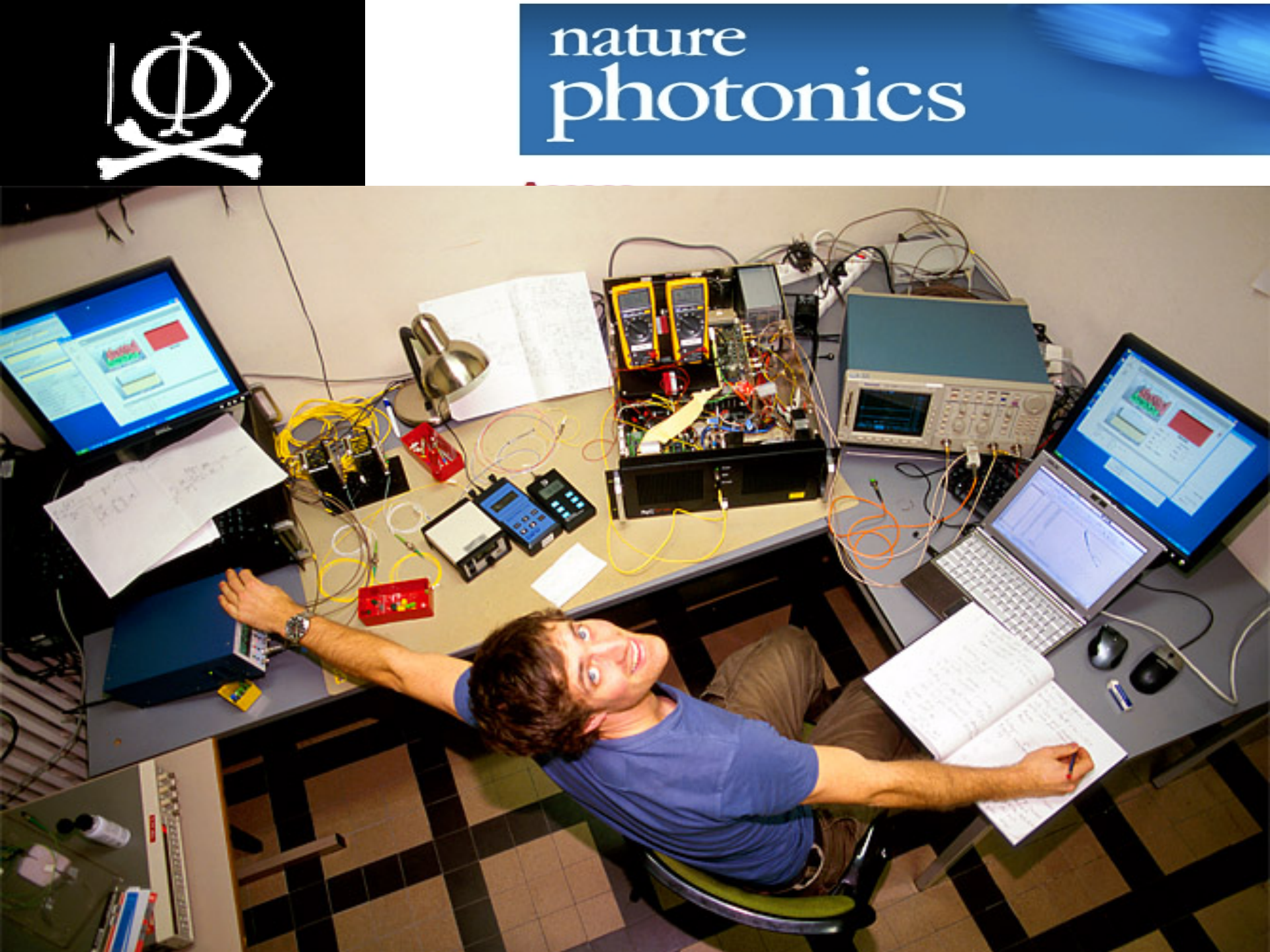
There is nothing like cracking QKD !

The principle of QKD will never be attacked, only the implementation may be faulty.

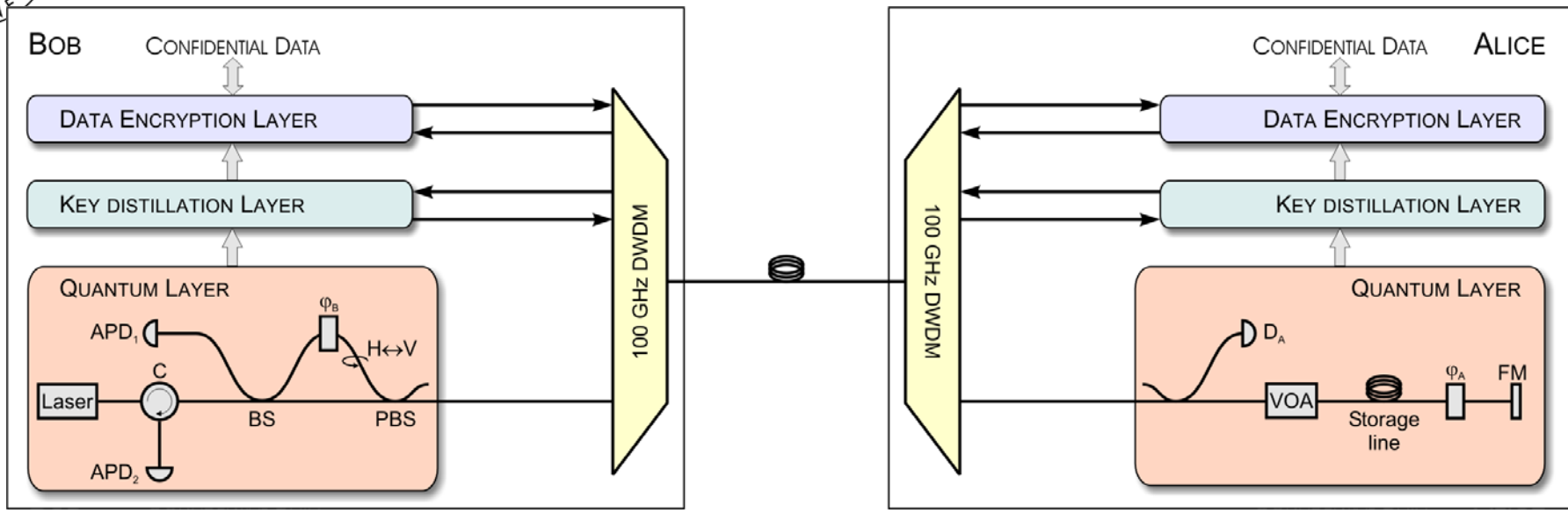
The implementation must be checked, as is the case for all hardware and all software.

August 29, 2010

The Norwegian University of Science and Technology (NTNU) and the University of Erlangen-Nürnberg together with the Max Planck Institute for the Science of Light in Erlangen have recently developed and tested a technique exploiting imperfections in quantum cryptography systems to implement an attack. Countermeasures were also implemented within an ongoing collaboration with leading manufacturer ID Quantique.


nature
photonics

WDM: multiplex the Quantum and Classical ≈ 10^9 times more intense !!!



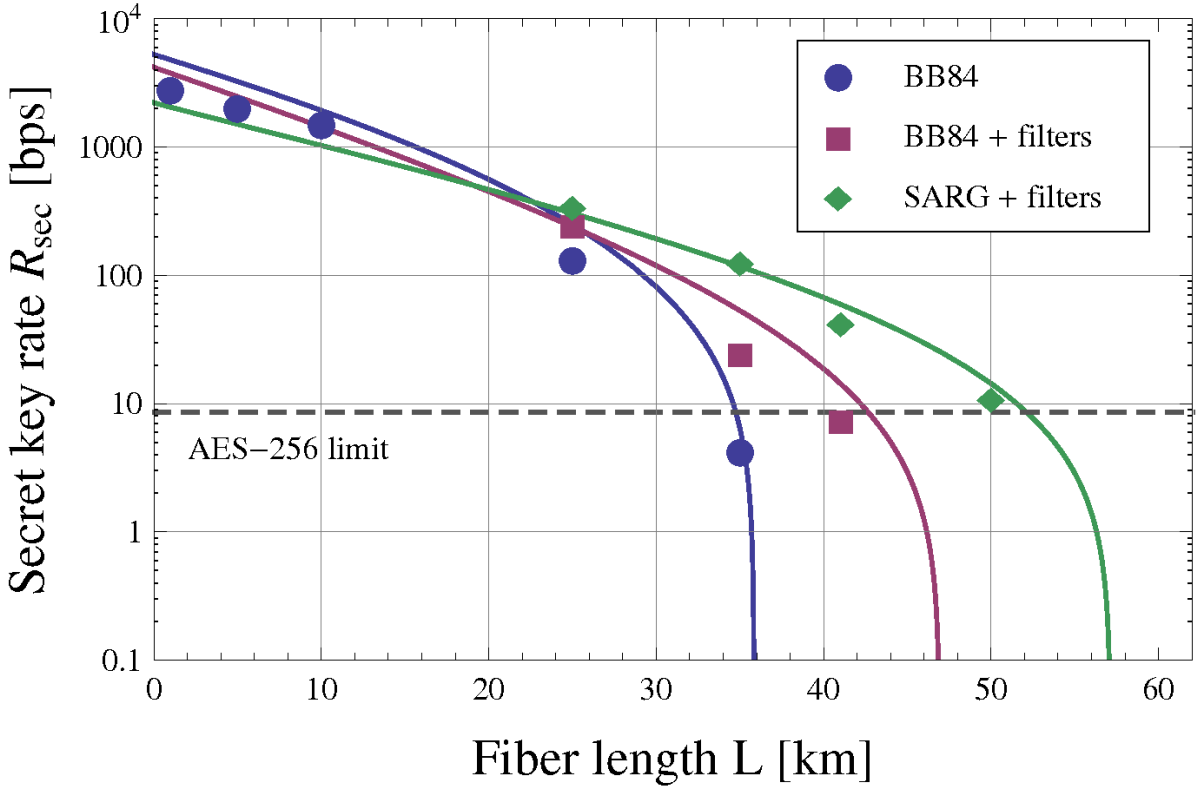
$$QBER = QBER_{opt} + QBER_{det} + QBER_{noise/WDM}$$

What are the noise sources?

- Crosstalk of other wavelengths into quantum channel
- Generation of parasitic light at the wavelength of the Q channel
  - by Raman scattering (dominant for lengths > 10 km)
  - by Four Wave Mixing (FWM)

GAP Quantique

Experimental Results

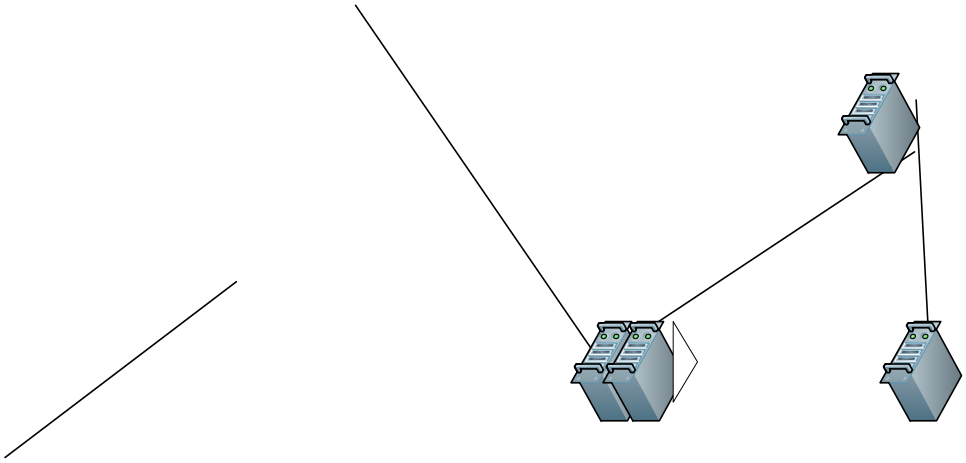


Eraerds et al., NJP 12, 063027 (2010)

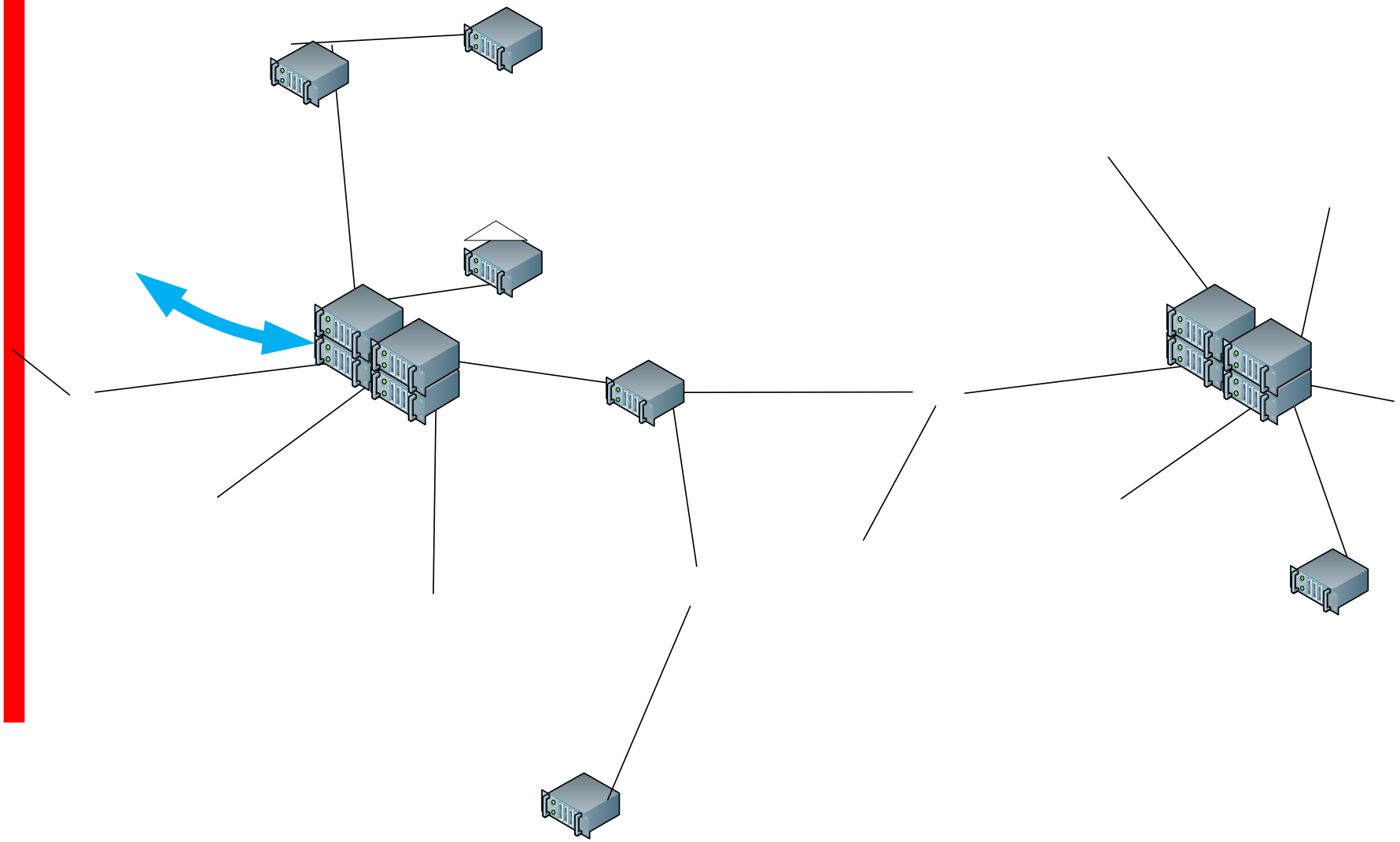
Fiber attenuation:	-0.207 dB/km
Detection efficiency:	0.07
Dark count rate:	$5 \cdot 10^{-6}$ ns^{-1}
Dead time:	10 µs
DWDM isolation:	82 dB

GAP Quantique

GAP Quantique

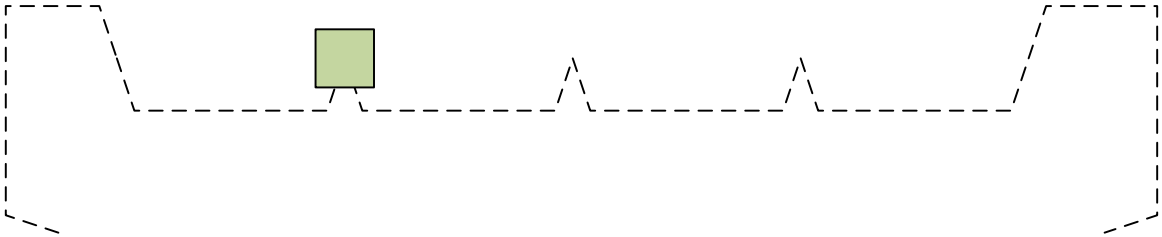


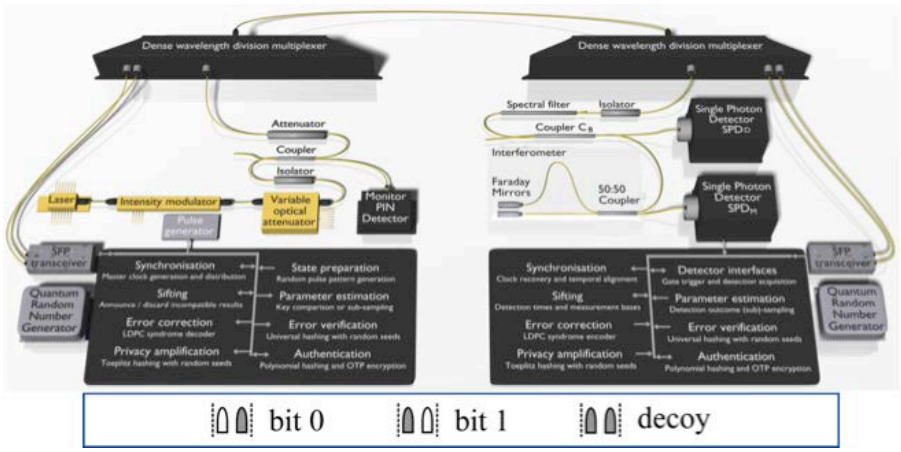
Quantum Network Architecture With Trusted Node



GAP Quantique

QKD Trusted Node





Telecom-compatible architecture (ATCA)
Up to 8 quantum blades per chassis

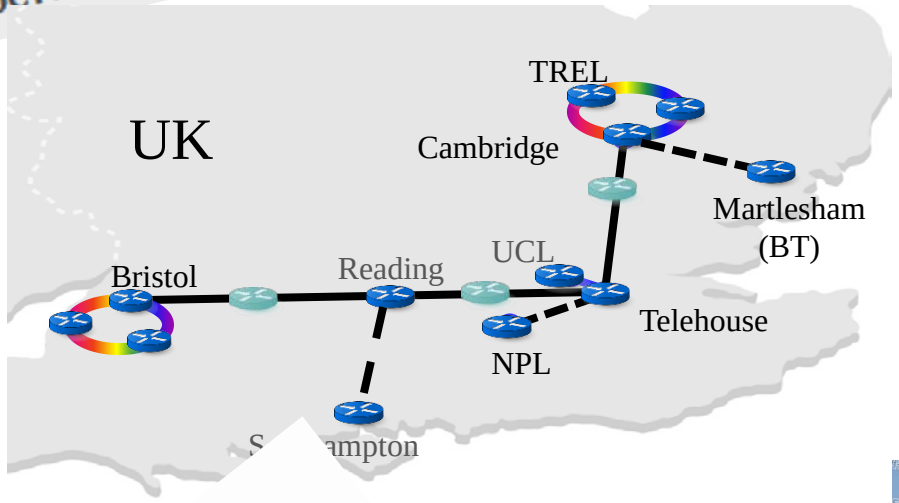
FIPS 140-2 Certification (Planned)
CC Evaluation (Planned)

GAP Quantique

3rd ETSI/IQC Workshop on Quantum-Safe Cryptography

ADD THIS TO MY CALENDAR

5-7 OCTOBER 2015



Quantique

Battelle

The Business of Innovation

Chinese Trusted Node Quantum Network

Chinese Trusted node Quantum network

- Total Length 2000 km
- 2013.6-2016.12
- 32 trustable relay nodes

  31 fiber links
- Metropolitan networks

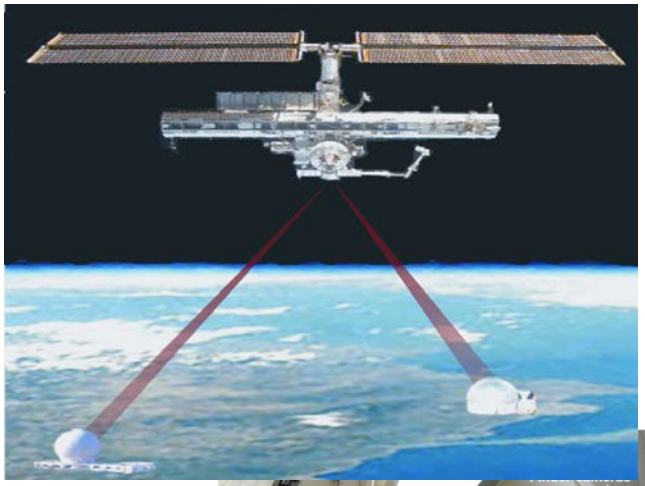
  Existing: Hefei, Jinan

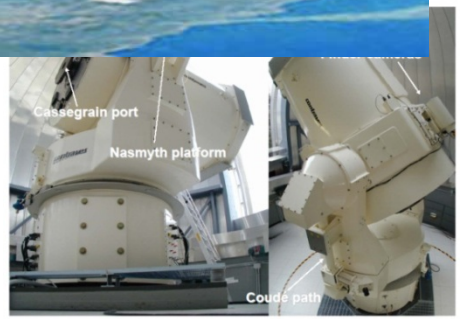
  New: Beijing, Shanghai
- Total Investment: 560 M RMB. Half by NDRC, Half by Local government
- Customer: China Industrial & Commercial Bank; Xinhua News Agency; CBRC

GAP Quantique

Proposals for quantum communication in space

Dual-downlink
(ROM R&D 47 M€)

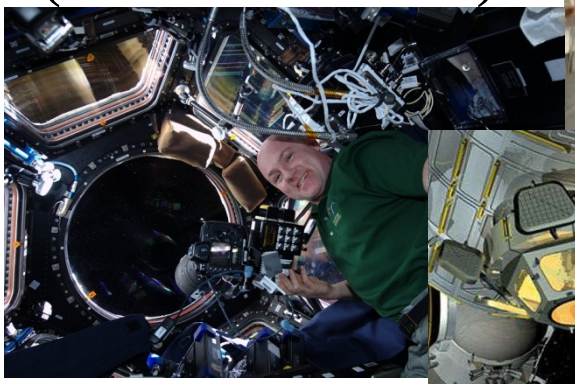




Simultaneous optical downlink: 1400 km separation.

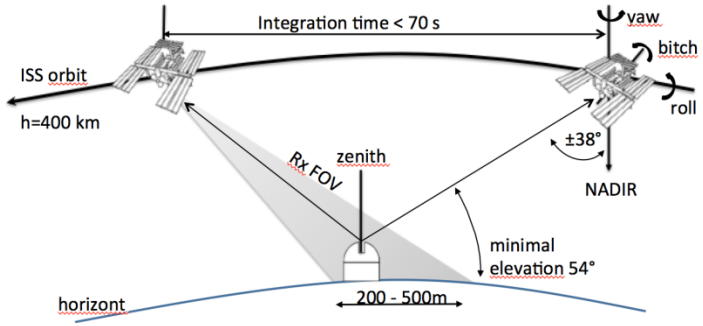
R. Ursin et al., Europhysics News, 26-29, 40–40 (3) (2009)

Single-uplink
(ROM R&D 1 M€)



Using a motorized photo-lens-pod (existing) and a dedicated quantum detector as “camera”.

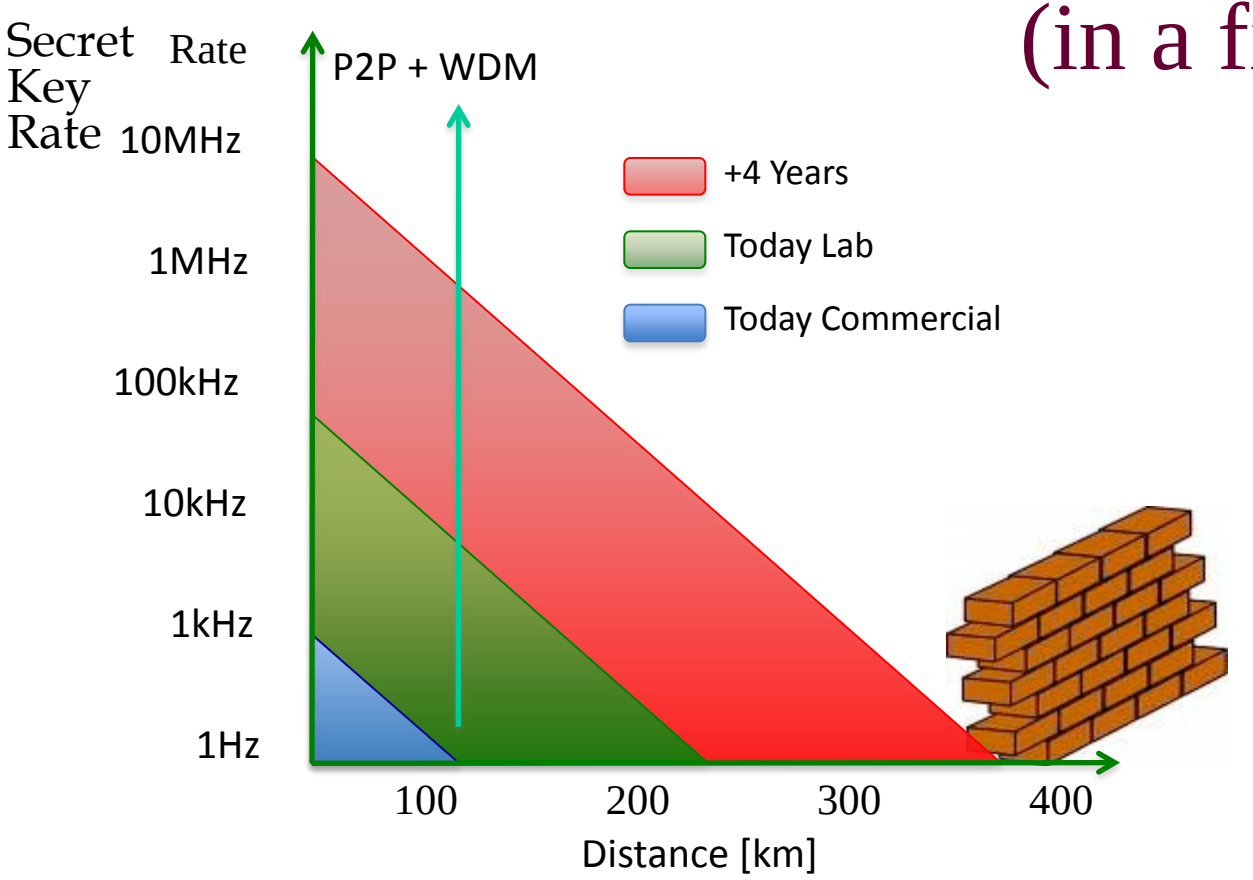
Astronaut: A. Kuipers



T. Scheidl, E. Wille, and R. Ursin, New Journal of Physics, 15, 043008 (2013)

Rupert.Ursin@oeaw.ac.at - Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences

How far can one send a photon ? (in a fiber)

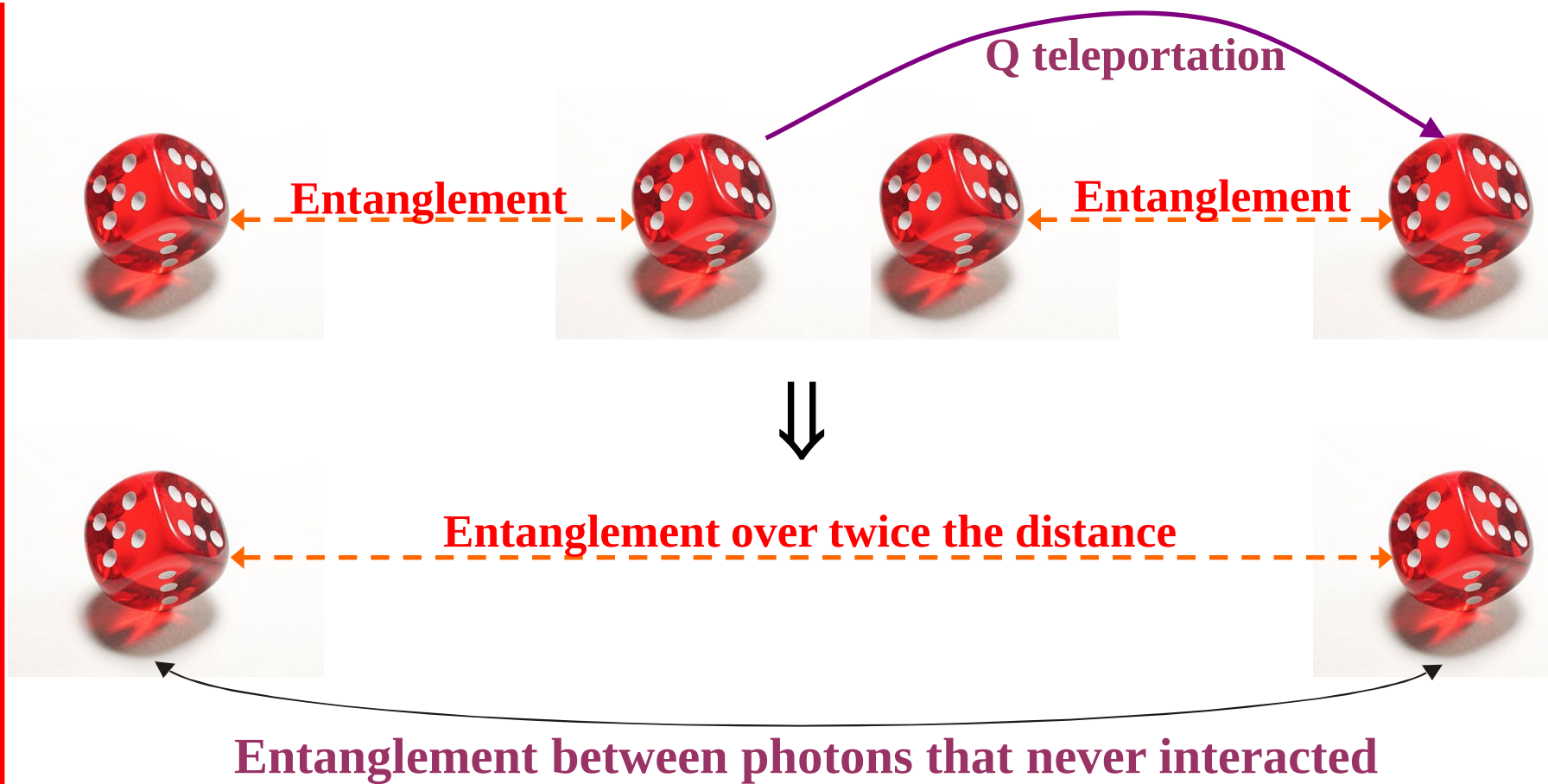


There is a hard wall around 400 km !

With the best optical fibers, perfect noise-free detectors and ideal 10 GHz single-photon sources, it would take centuries to send 1 qubit over 1000 km !

GAP Quantique

Quantum Repeaters: beating the hard wall thanks to Teleportation of entanglement

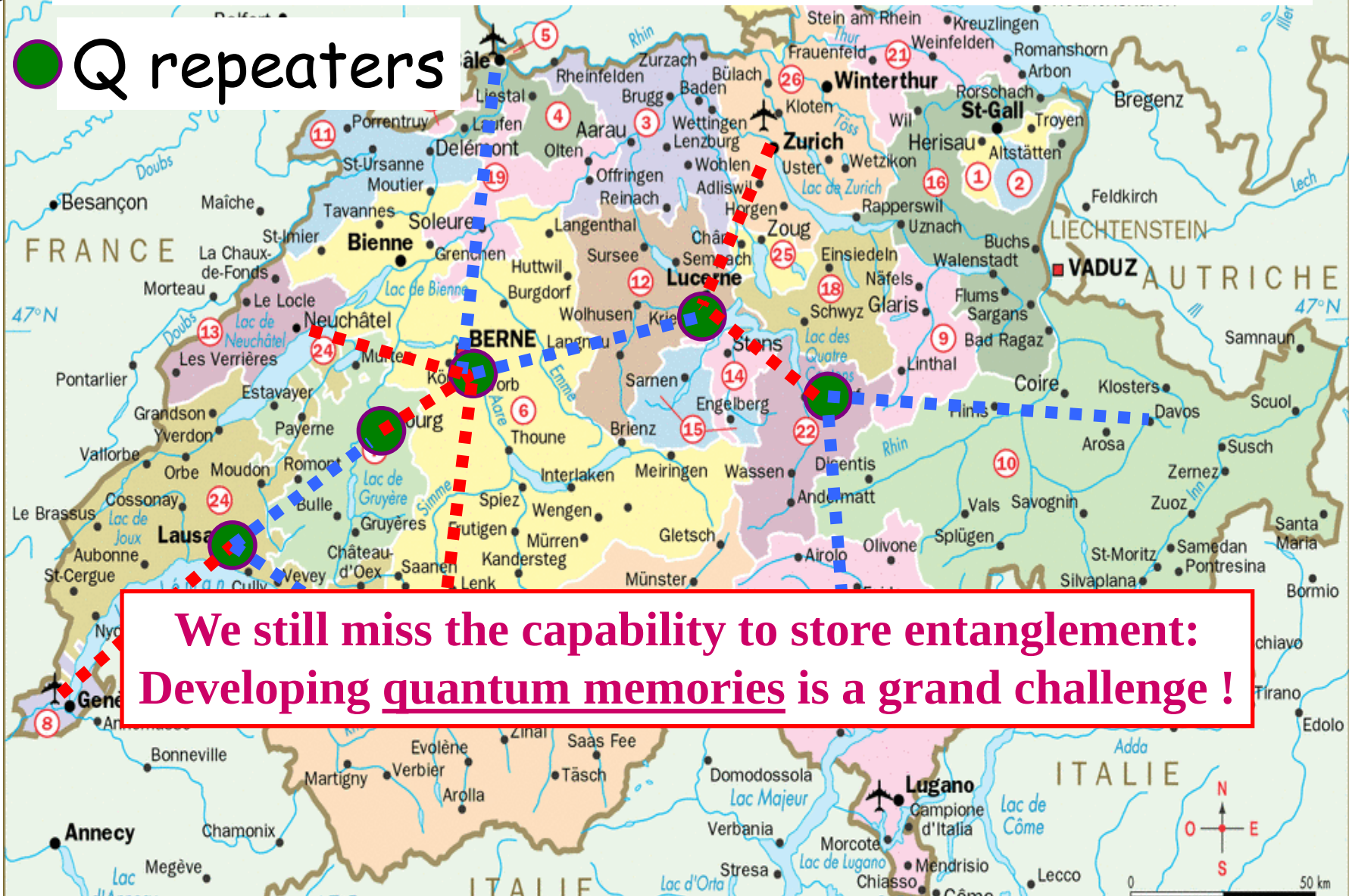


GAP Quantique

PRA 71, 05302, 2005

N-photon quantum communication: quantum networks, quantum internet

- Q repeaters



We still miss the capability to store entanglement: Developing quantum memories is a grand challenge !

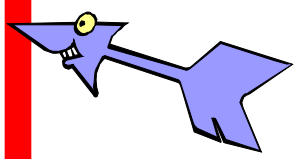
GAP Quantique

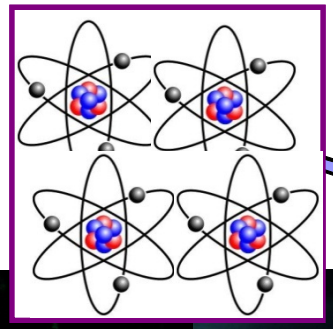
Quantum memory

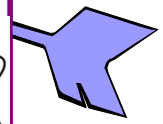
Goal: controlled and reversible mapping of a photonic quantum state onto a long lived atomic ensemble.

crystal doped with billions of ions

photon in



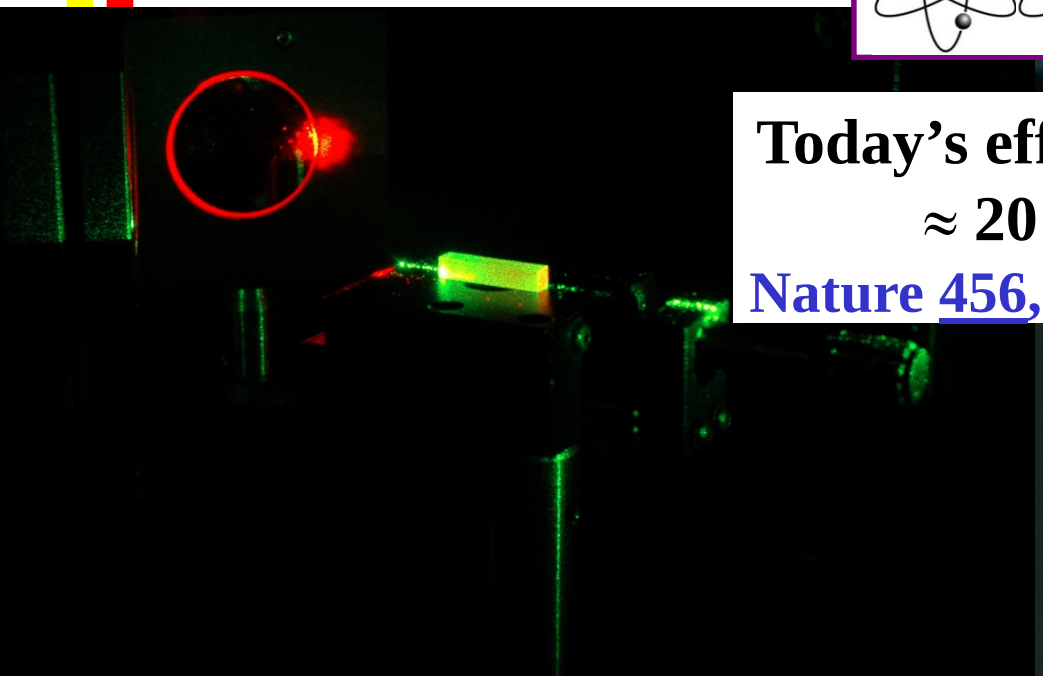




photon out at desired time in same Q state

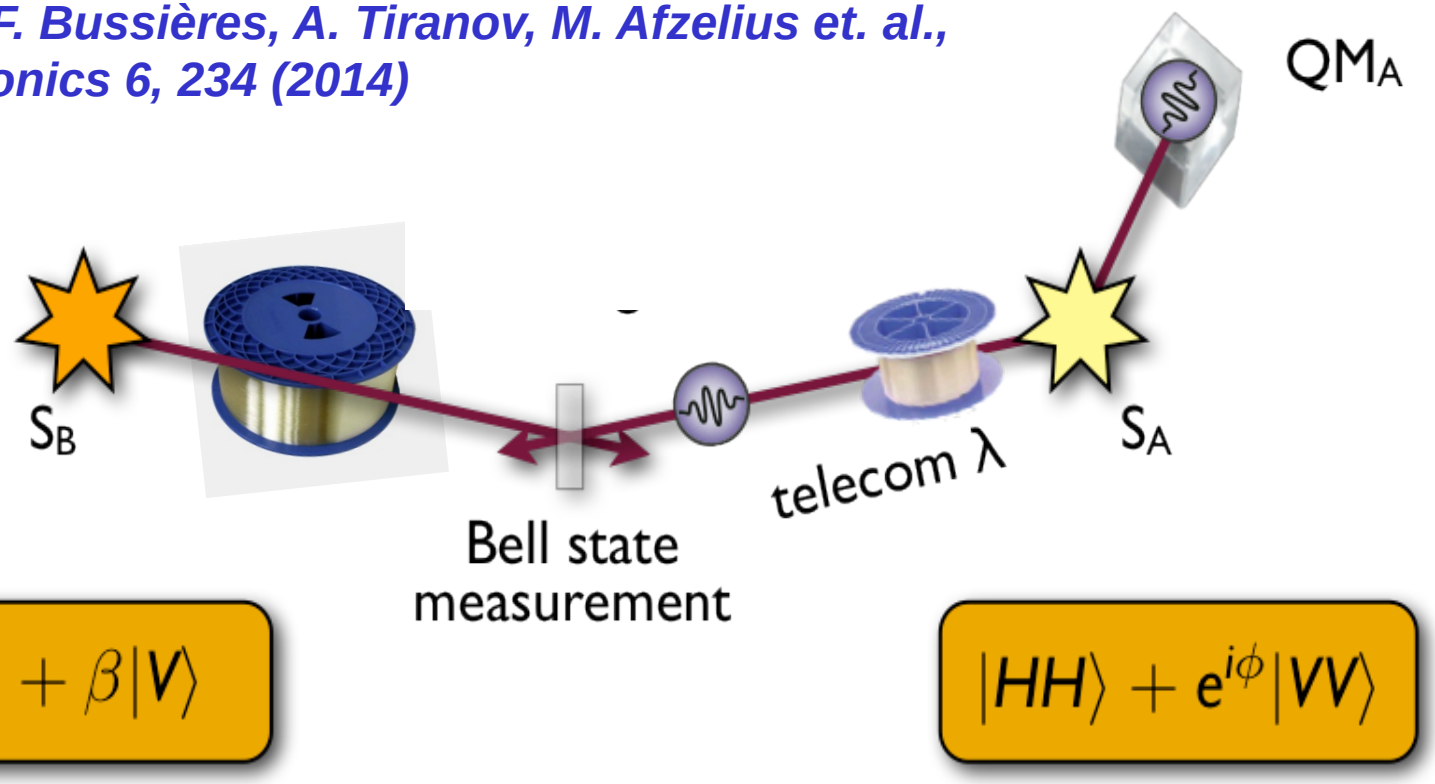
Today's efficiencies ≈ 20 %

Nature 456, 773, 2008



Teleportation of a polarization qubit over 25 km from a *weak coherent state*

C. Clausen, F. Bussières, A. Tiranov, M. Afzelius et. al., Nature Photonics 6, 234 (2014)



Quantum teleportation of a telecom-wavelength photon to a solid-state quantum memory

GAP Quantique

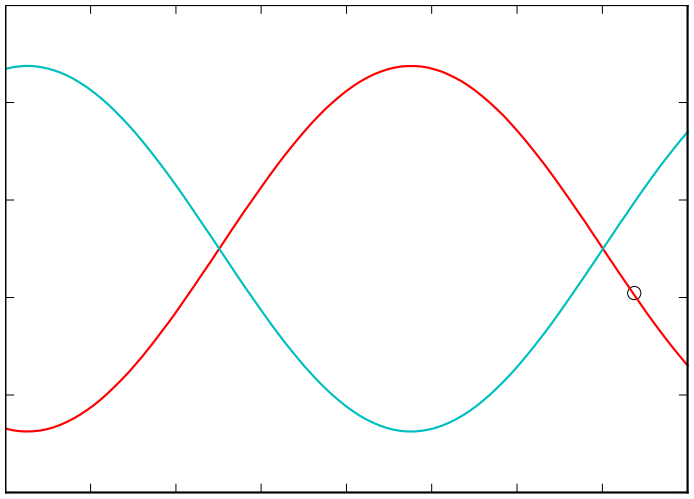
Partial Bell State Measurement and post-selected fidelity

Tomographic reconstruction (short link)

State	Fidelity (%)
$\|H\rangle$	94 ± 3
$\|-\rangle$	92 ± 4
$\|R\rangle$	82 ± 4
$\|+\rangle$	82 ± 4
Average	88 ± 4

Fidelity of $|+\rangle$ teleportation (2x12.4 km) $81 \pm 5\%$

Analysis on a great circle of the Poincaré sphere



Quantum memory - dream and reality

Property	Desired performance	State-of-the-art (quantum & classical state storage)
Efficiency	≈0.9	0.87
Fidelity*	≈0.95	0.92-0.98
Multi-mode storage capacity	high	64 (1000) modes
Pulse duration	≤ ns	~100 ps
Storage time	> sec	>2 sec
Universal	entanglement-preserving	atomic vapor & RE-crystal
Complexity	simple	…

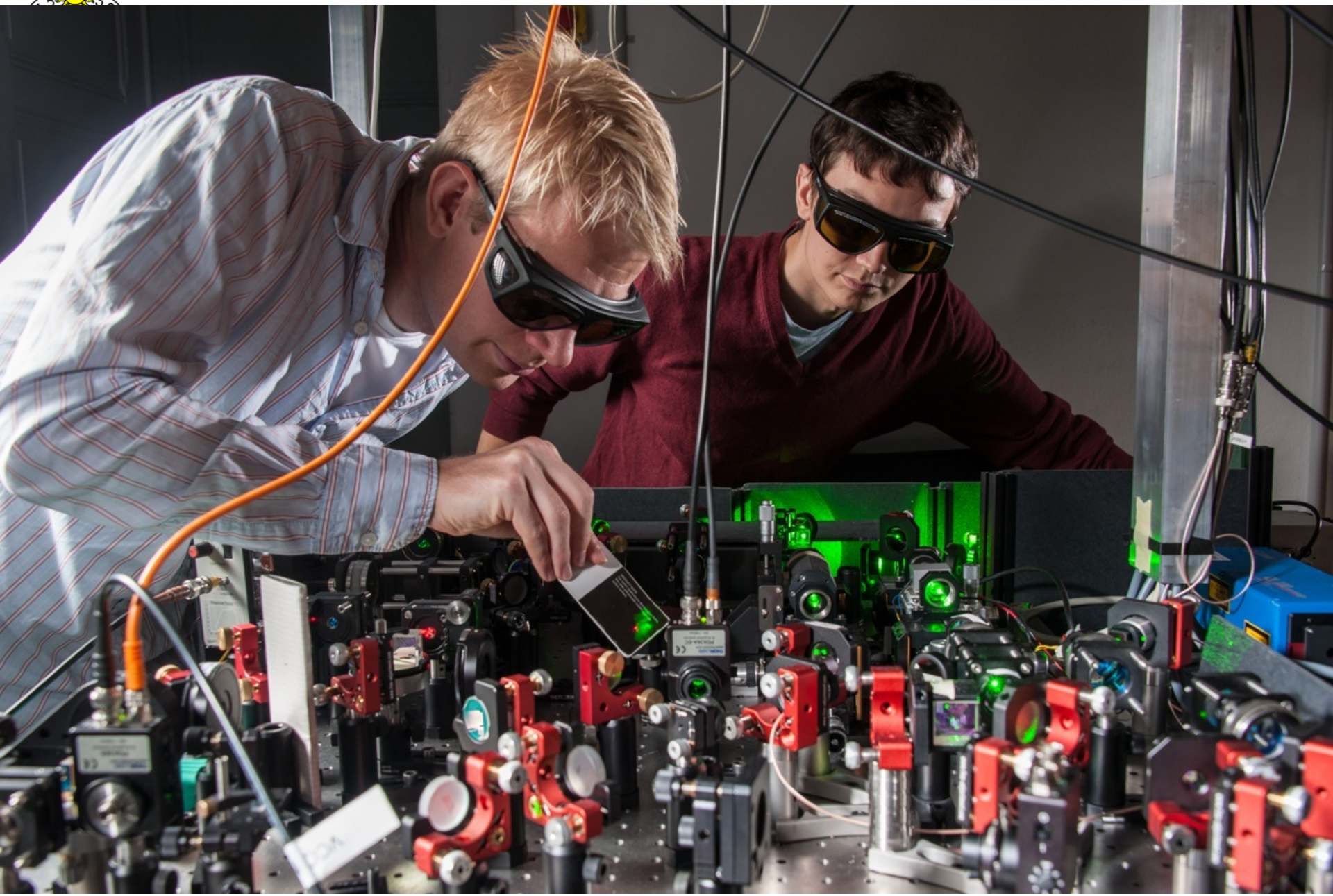
(for qubits)

* post selected

Different storage media and protocols

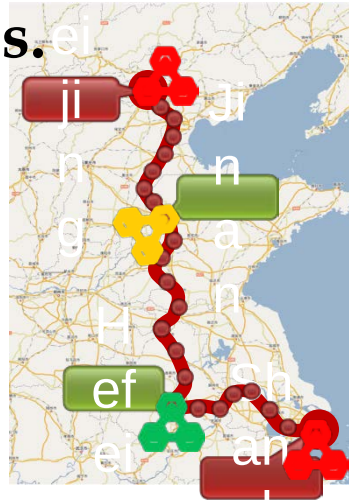
GAP Quantique

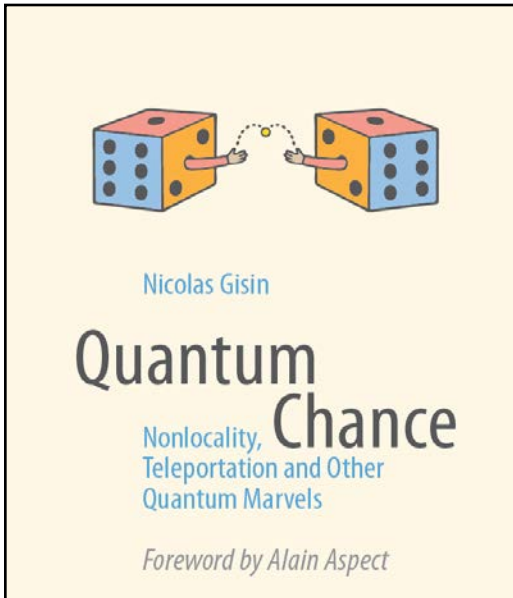
Hedges *et al*, Nature (2010); Hosseini *et al*, Nature Phys. (2011), Usmani *et al*, Nature Comm (2010), Saglamyurek, WT *et al*, Nature (2011), Longdell *et al*, Phys Rev Lett. (2005), Jin *et al*, quant-ph (2010), Clausen *et al*, Nature (2011), Rempe *et al.*, Nature (2011), Lvovsky, Sanders, WT, Nature Phot. (2010)



Conclusions

- Quantum offers truly random processes, hence truly random sequences of bits.
- Quantum offers secret & shared randomness.
- **Quantum physicists and cryptographers should work together to exploit this gift of Nature.**
- Quantum Networks based on Trusted Nodes are under advanced developments in several countries.
- Quantum Key Distribution Devices exists: you can buy it !
- Quantum Repeaters require teleportation and quantum memories. They are still in the lab.





GAP Quantique