OFC 2017 © OSA 2017

Quantum Communication,

Nicolas Gisin and Hugo Zbinden

GAP-Quantique, University of Geneva

GAP Quantique Geneva University

Engineering

- Local Randomness for True Random Number generators
- Non-local Randomness for distribution of Cryptographic Keys
- Towards faster, longer distances and cheaper QKD engines
- Quantum Repeaters
- Device-Independent Quantum Information Processing

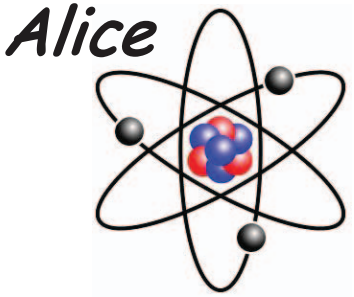
Fundamental Physics

978-1-943580-23-1/17/$31.00 ©2017 Optical Society of America

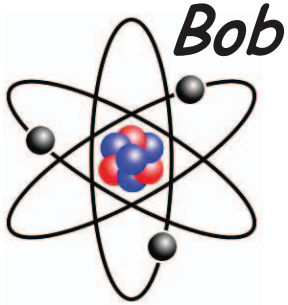
OFC 2017 © OSA 2017

Quantum communication

Quantum Communication is the art of transferring a quantum state from one location, Alice, to a distant one, Bob.



Ultimately, information is carried by the physical state of some quantum systems

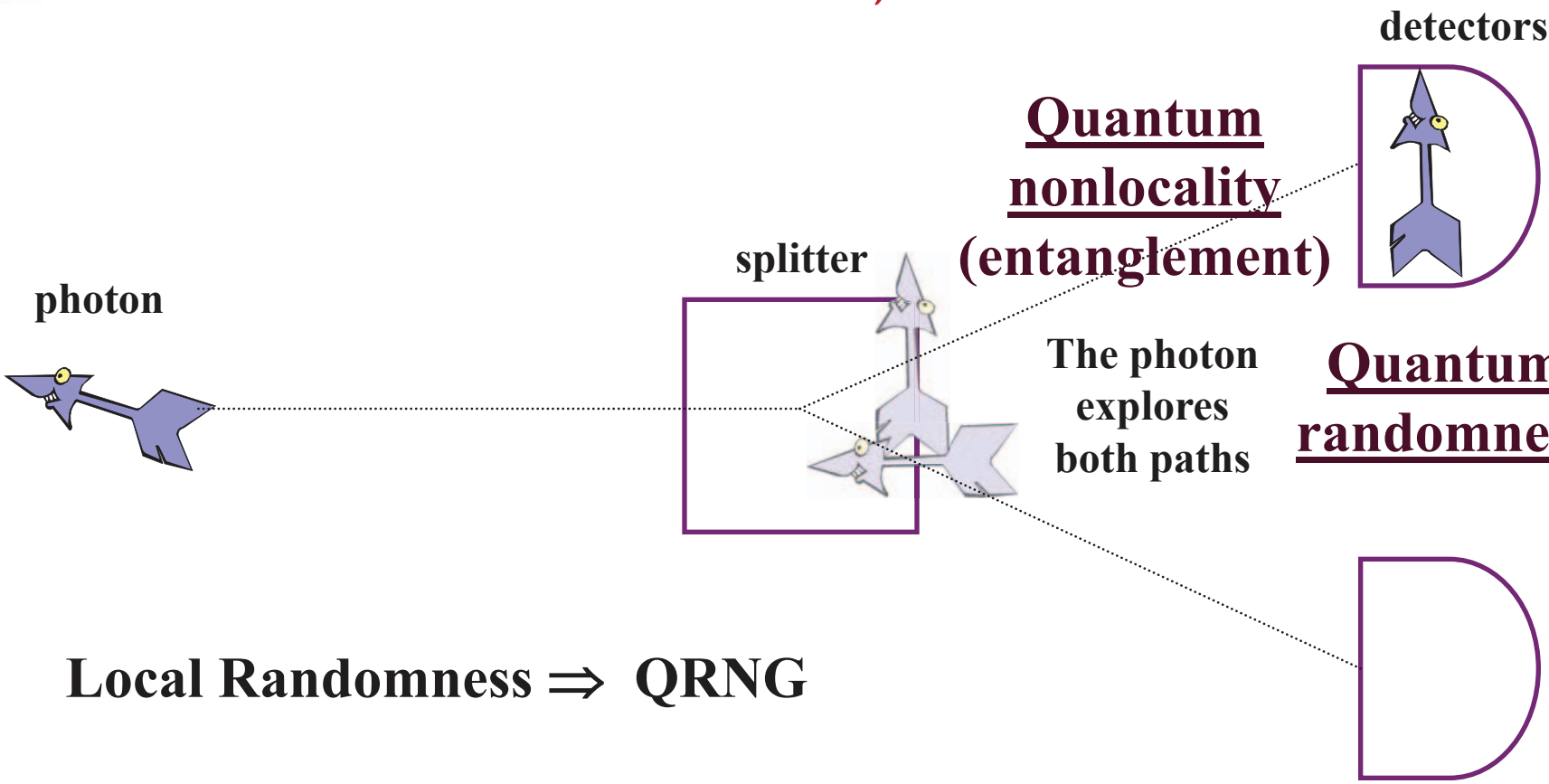


- **A quantum state can't be copied, hence the original is necessarily destroyed.**
- **Copying quantum states would violate both Heisenberg's uncertainty relations and the impossibility of faster than light signaling. Hence, the impossibility of "Q cloning" is one of the best established facts of Science.**

GAP Quantique Geneva University

OFC 2017 © OSA 2017

Quantum Communication is the art of transferring a quantum state from one location, Alice, to a distant one, Bob.



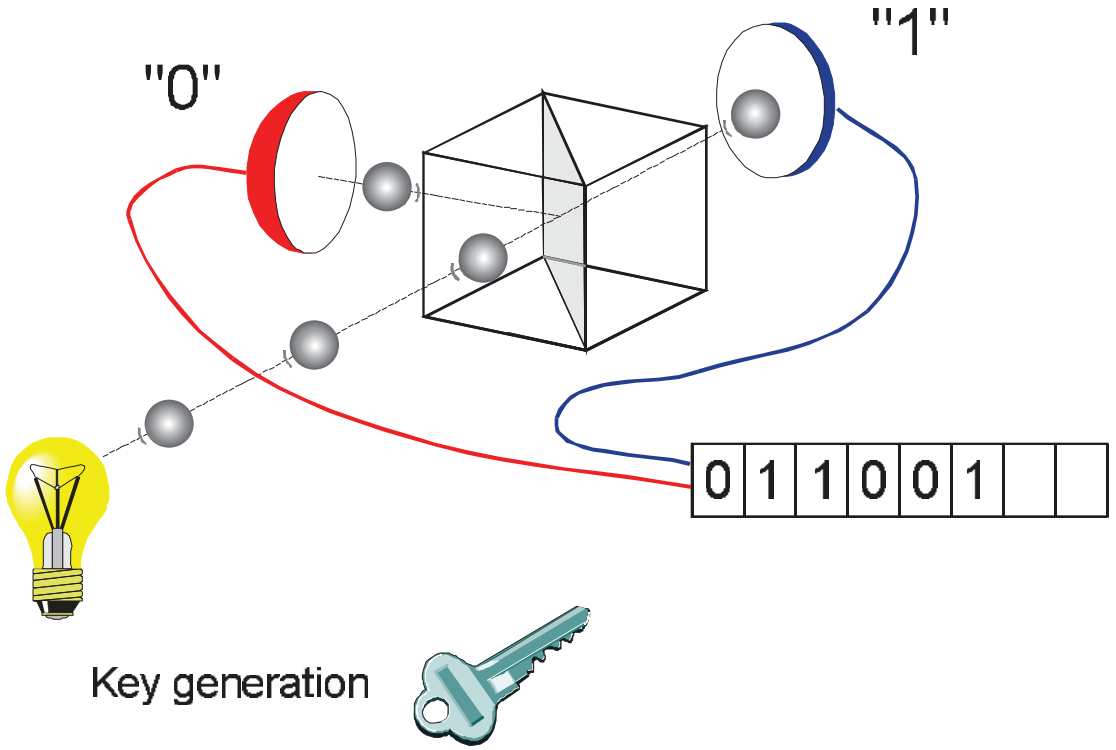
Local Randomness ⇒ QRNG

Non-local Randomness ⇒ QKD

GAP Quantique Geneva University

OFC 2017 © OSA 2017

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**

GAP Quantique Geneva University

OFC 2017 © OSA 2017

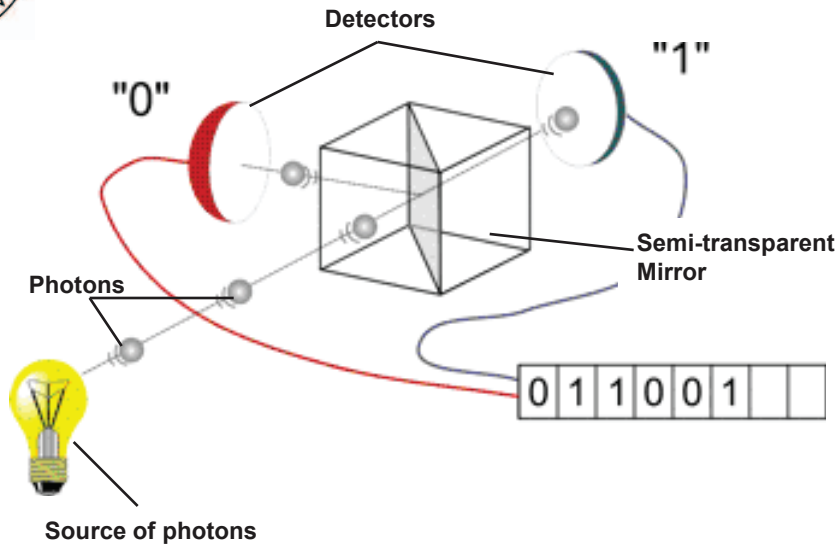
Danger of pseudo-random number generators

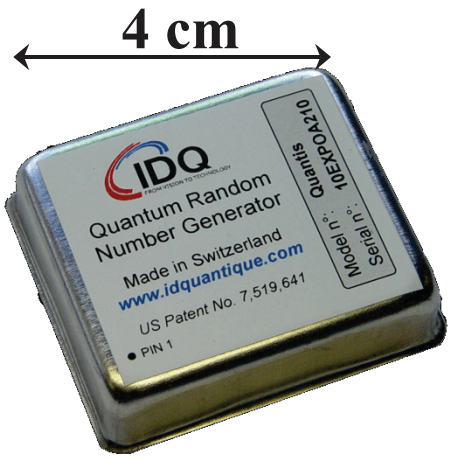
- There is no security without good randomness.
- Snowden taught us that one shouldn't trust pseudo-random number generators.
- They may even have on purpose build-in weaknesses !
- ⇒ go for good physical random number generators.
- Only quantum offers true randomness.

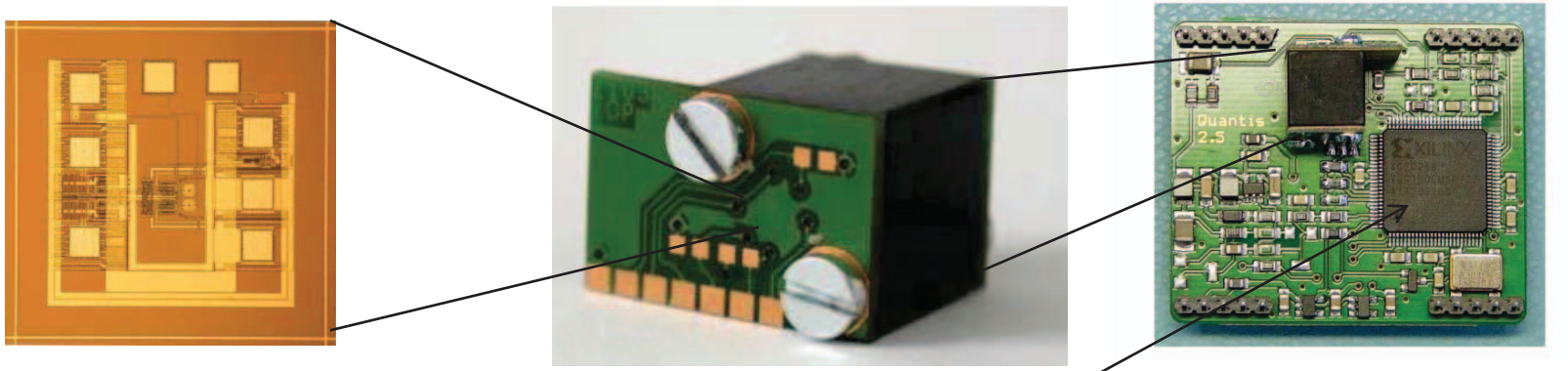
GAP Quantique Geneva University

OFC 2017 © OSA 2017

Quantum Random Number Generator







4 Mb per second of balanced random bits

GAP Quantique Geneva University

OFC 2017 © OSA 2017

Evaluation and Certification

GAP Quantique Geneva University

Non-Deterministic (Physical) RNG

- **PTG.1**

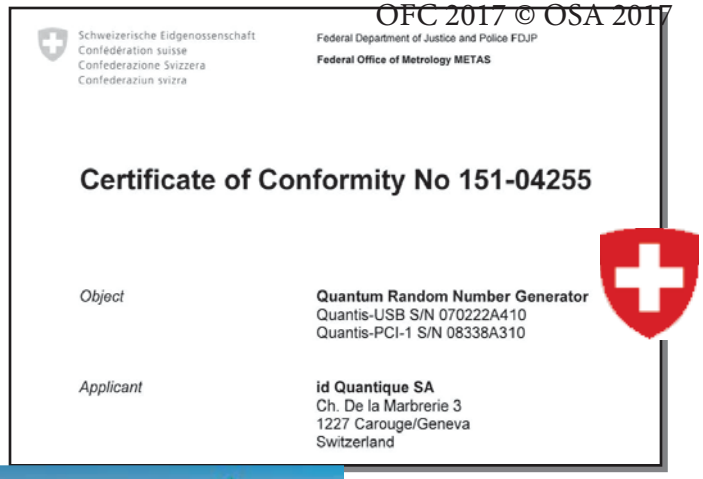
Physical RNG with internal tests that detect a total failure of the entropy source and non-tolerable statistical defects of the internal random numbers

- **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

CTL
Certificate of Compliance
Quantis-v10.10.08
ID Quantique SA
has been tested by
CTL, Compliance Testing Laboratory
Issue Date: 30.03.2011
CAST
BANGOR

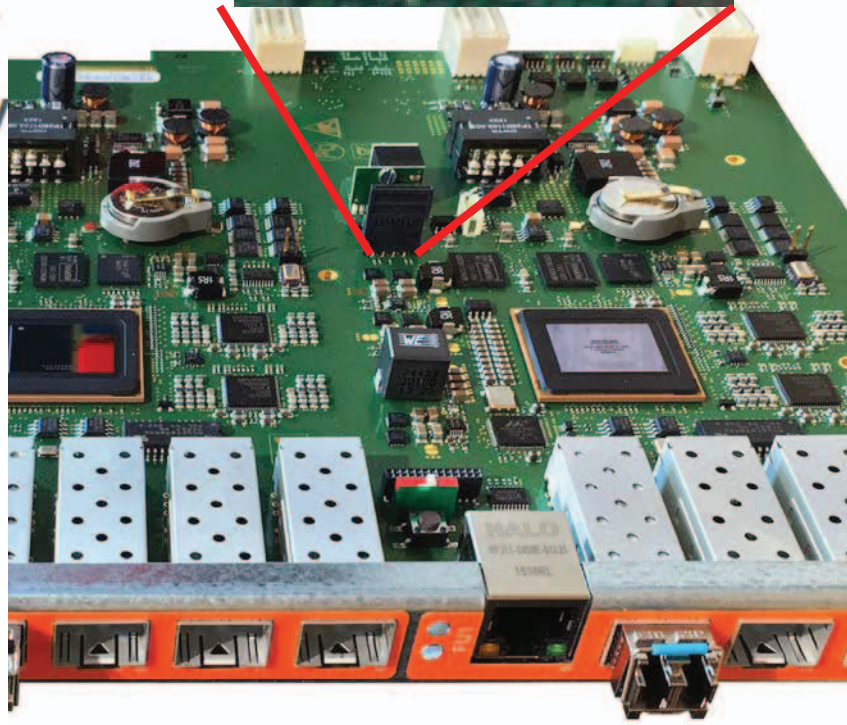
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

KEYMILE
because connectivity matters

Quantum physics are the base for key generation and distribution

For its encryption card, KEYMILE uses a hardware-based quantum random number generator (QRNG) which creates genuinely random numbers and extremely secure key

Solution Brief SECU1 (PDF | 4,12 MB)



OFC 2017 © OSA 2017

Quantum Physics has more to offer

1997

Nonlocal randomness:
a random event that manifests itself at several locations.

Cornavin

Bellevue

Bernex

swisscom

OFC 2017 © OSA 2017

Modern Cryptology
Secrecy is based on:

GAP Quantique Geneva University

Complexity theory

The key is public

The public key contains the decoding key, but it is very difficult to find (one way functions)

The security is not proven (no one knows whether one way functions exist)

Example:

127 x 229 = 29083

Difficult does not mean impossible

Information theory

The key is secrete

The key contains the decoding key: Only the two partners have a copy !

The security is proven (Shannon theorem)

Example:

Message:	**011001001**
Key:	**110100110**
Coded message:	**101101111**

Requires distribution of secrete keys

OFC 2017 © OSA 2017

NSA data center Utah
$3x10^{18}$ - 10^{24} bytes

Store ciphertexts now – decrypt later

Can probably decrypt a few hundreds of messages per day with large dedicated machines

GAP Quantique Geneva University

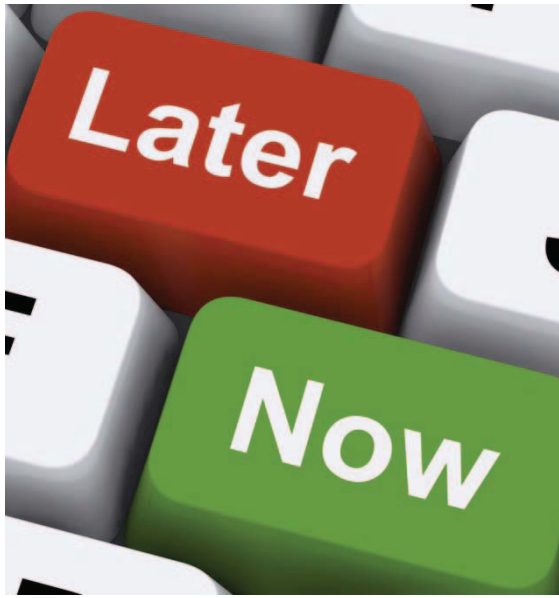
OFC 2017 © OSA 2017

How soon do we need to worry?

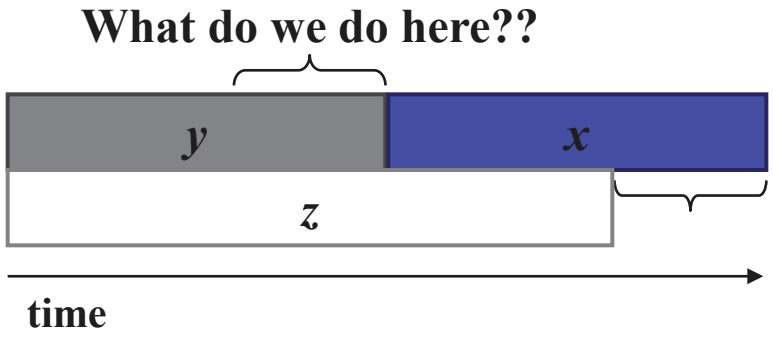
GAP Quantique Geneva University

Depends on:

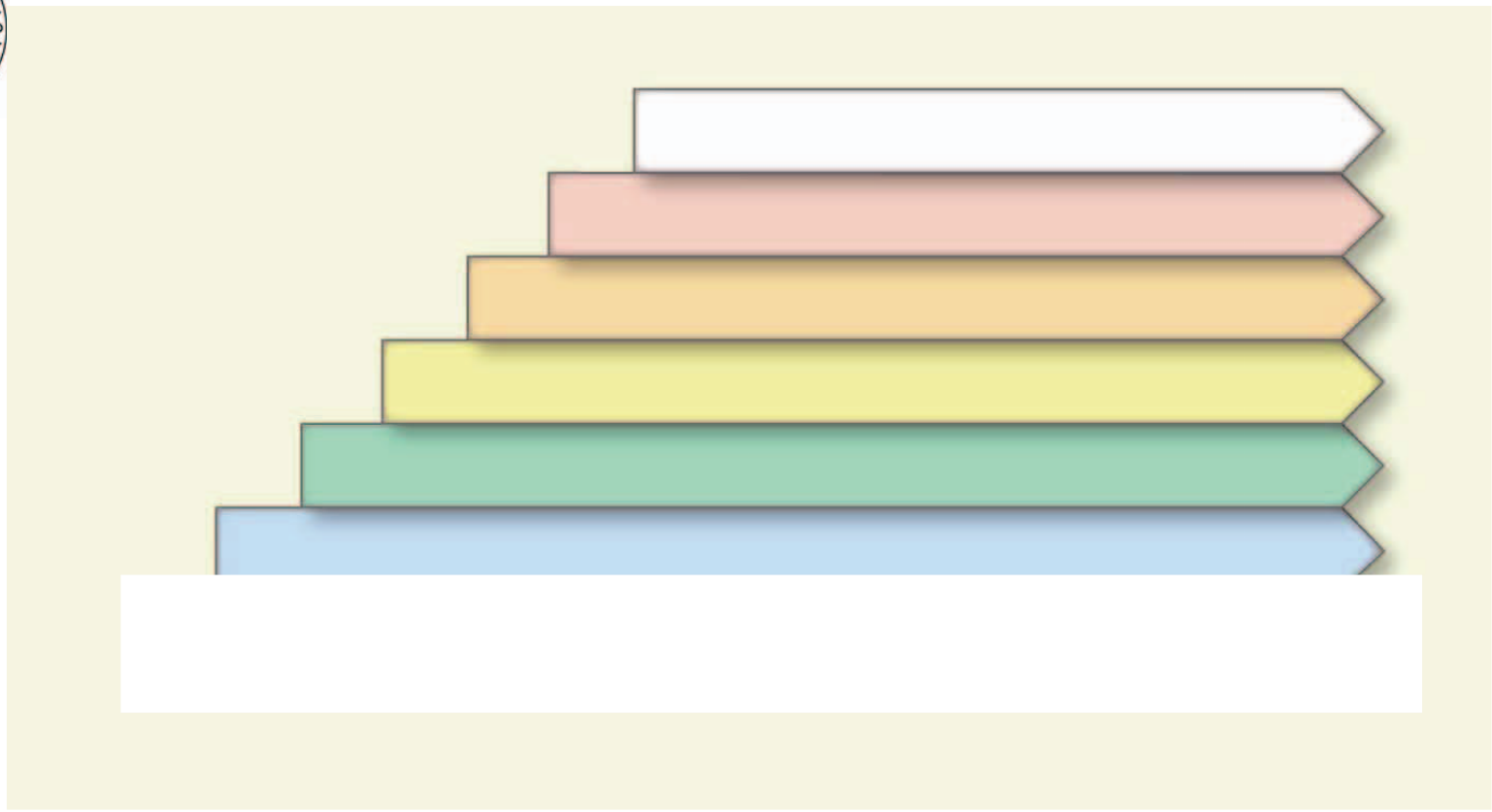
- How long do you need encryption to be secure? (x years)
- How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution? (y years)
- How long will it take for a large-scale quantum computer to be built (or for any other relevant advance? (z years)



- Theorem 1: If $x + y > z$, then worry.



OFC 2017 © OSA 2017



OFC 2017 © OSA 2017

Change in perception

OFC 2017 © OSA 2017

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 Geneva University

《中华人民共和国国民经济和社会发展第十三个五年规划纲要》

The 13th five-year plan for Economic and Social Development of the People's Republic of China

第二节 培育发展战略性产业

加强前瞻布局，在空天海洋、信息网络、生命科学、核技术等领域，培育一批战略性产业。大力发展新型飞行器及航行器、新一代作业平台和空天一体化观测系统，着力构建量子通信和泛在安全物联网，加快发展合成生物和再生医学技术，加速开发新一代核电装备和小型核动力系统、民用核分析与成像，打造未来发展新优势。

Chapter 23 Section 2 To Develop Cutting-Edge Industries

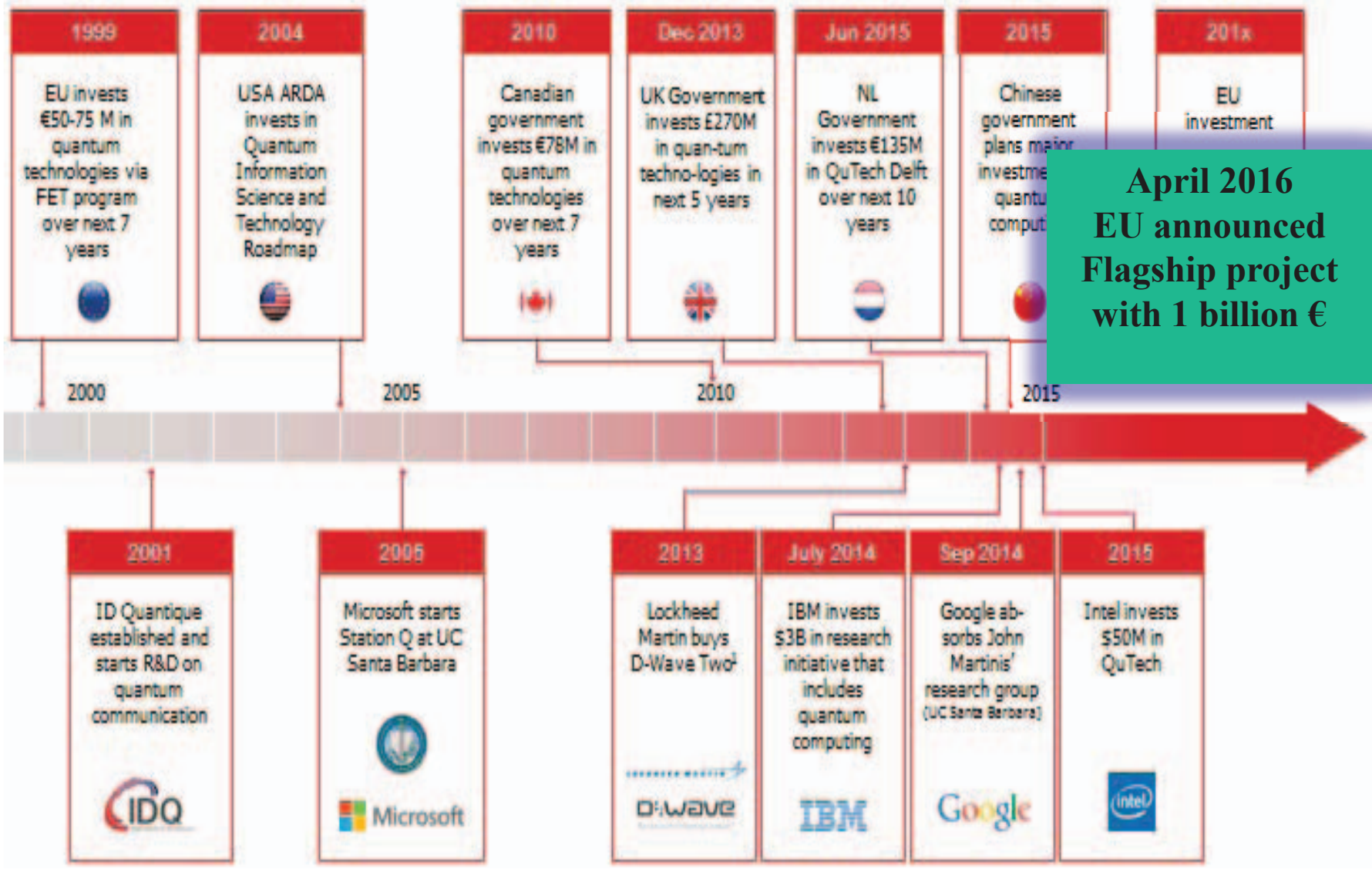
The technologies of aerospace and oceanography, information network, life sciences, nuclear technology should be strengthened. To develop new aircraft and aircraft, next-generation platforms and the integration of space observation system, concentrate on *quantum communication* and ubiquitous secure networking, accelerate the development of synthetic biology and regenerative medicine technology, accelerate the development of a new generation of small nuclear power and nuclear power equipment system, civil nuclear analysis and imaging, to create new advantages for future development.

GAP Quantique Geneva University

OFC 2017 © OSA 2017

Quantum Technologies

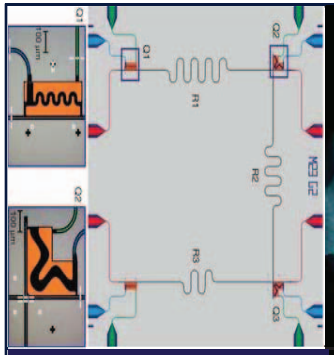
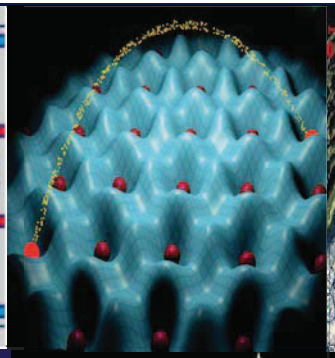
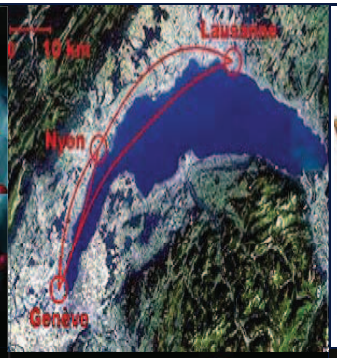
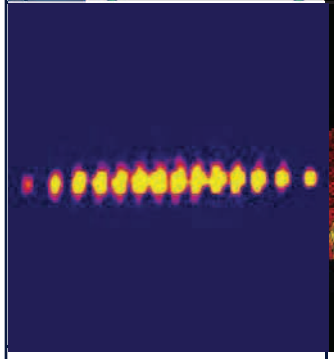
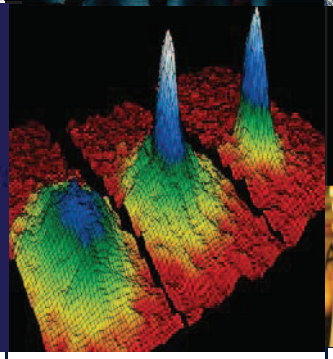
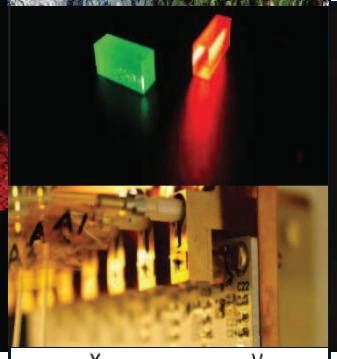
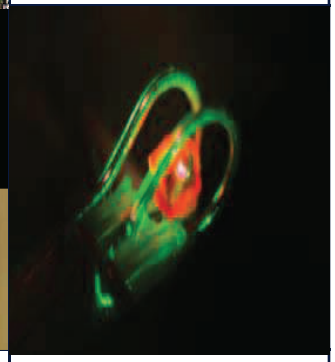
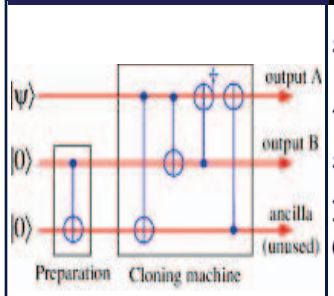
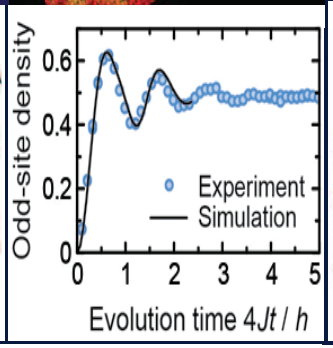
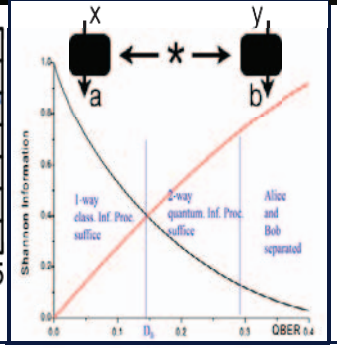
GAP Quantique Geneva University



OFC 2017 © OSA 2017

Quantum Technologies Flagship

GAP Quantique Geneva University

	Quantum Computers: Hardware & Software	Quantum Simulators	Quantum Communication: Devices & Systems	Quantum Sensing & Metrology
Quantum Engineering & Control				
Enabling Science				
Theory, Algorithms & Protocols				$\|\Psi\rangle \propto \|N,0\rangle - \|0,N\rangle$ $\mathrm{QFI} = 4\,\mathrm{var}_\psi(H)$

OFC 2017 © OSA 2017

QKD Engine ≈ standard telecom-box

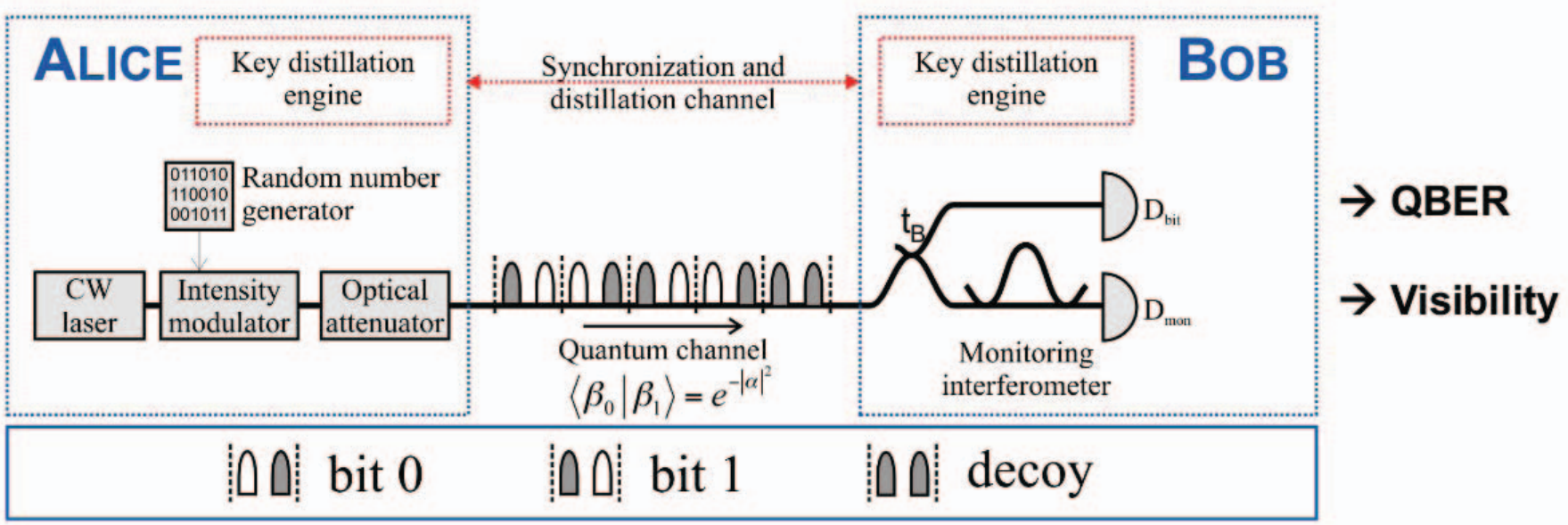
- Built on the Advanced Telecommunication Computing Architecture (ATCA).
- Provides standardized mechanical, power, and data interfaces.
- Provides network services, cooling, power supplies.
- Scalable architecture, familiar to potential clients.

GAP Quantique Geneva University

OFC 2017 © OSA 2017

Coherent one-way QKD

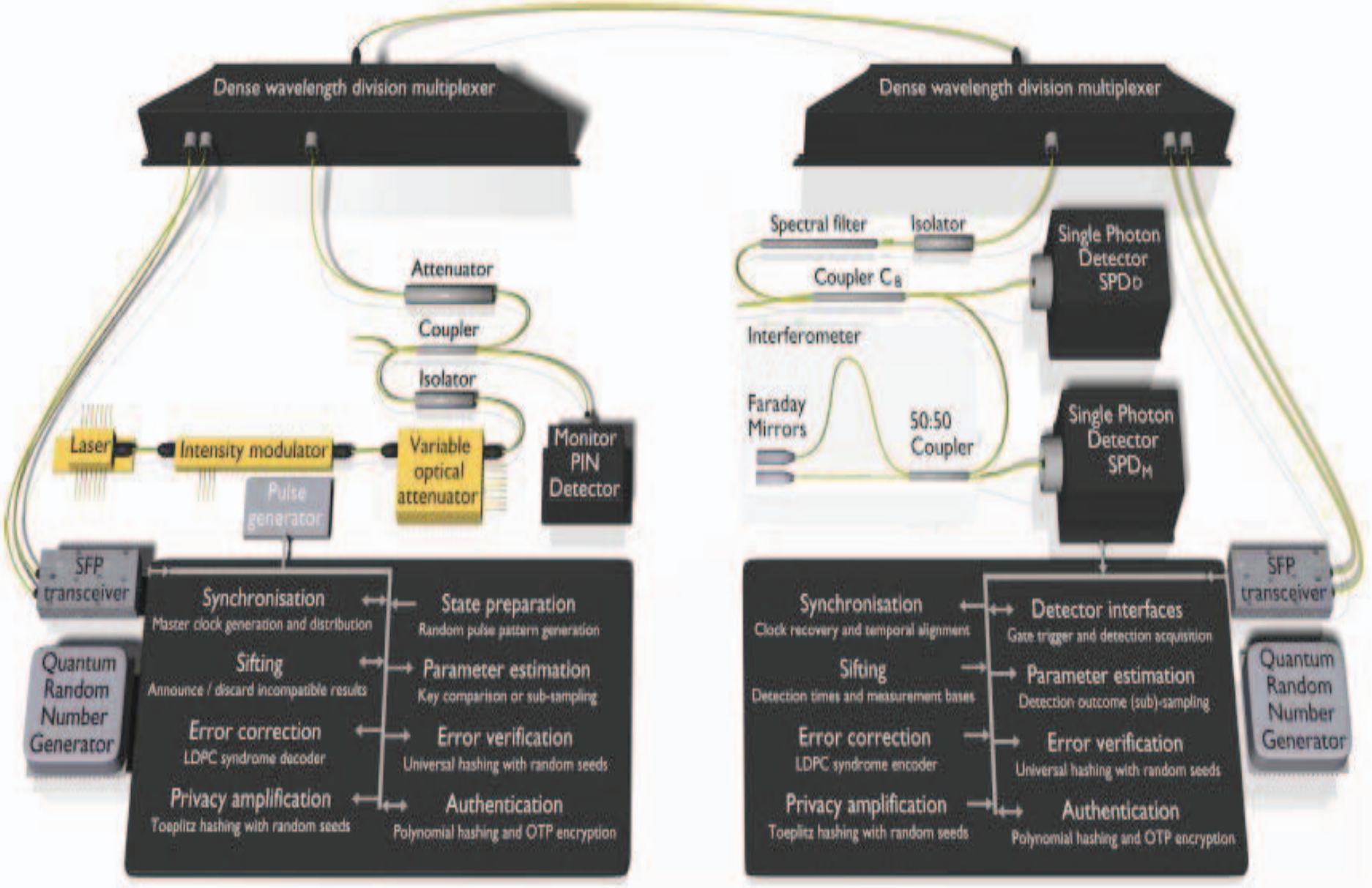
GAP Quantique Geneva University



- 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

OFC 2017 © OSA 2017

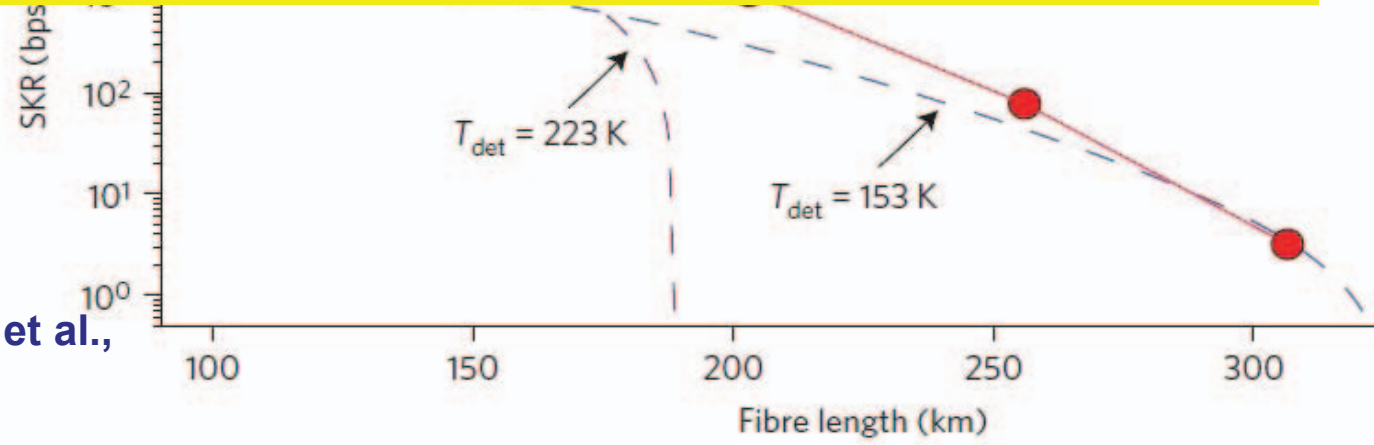


⇒ **QKD engines are very similar to standard telecom boxes, except for the 1-photon detectors.**

QKD over 307 km with real time secret key distillation, finite key analysis, InGaAs detect.

- **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 Geneva University

Spin-off from the University of Geneva, 2001

GAP Quantique Geneva University

Lausanne

Nyon

67 km

Genève

IDQ
FROM VISION TO TECHNOLOGY

Installed multiplexed quantum channel for commercial users.

Used daily by some commercial customers

OFC 2017 © OSA 2017

IDQ

- Geneva based
- Founded in 2001
- >50 employees
- Profitable
- Focuses on the opportunities of quantum photonics
- Three product ranges

Scientific Instrumentation

Quantum RNG

Quantum and conventional Cryptography

IDQ

OFC 2017 © OSA 2017

What does QKD achieve

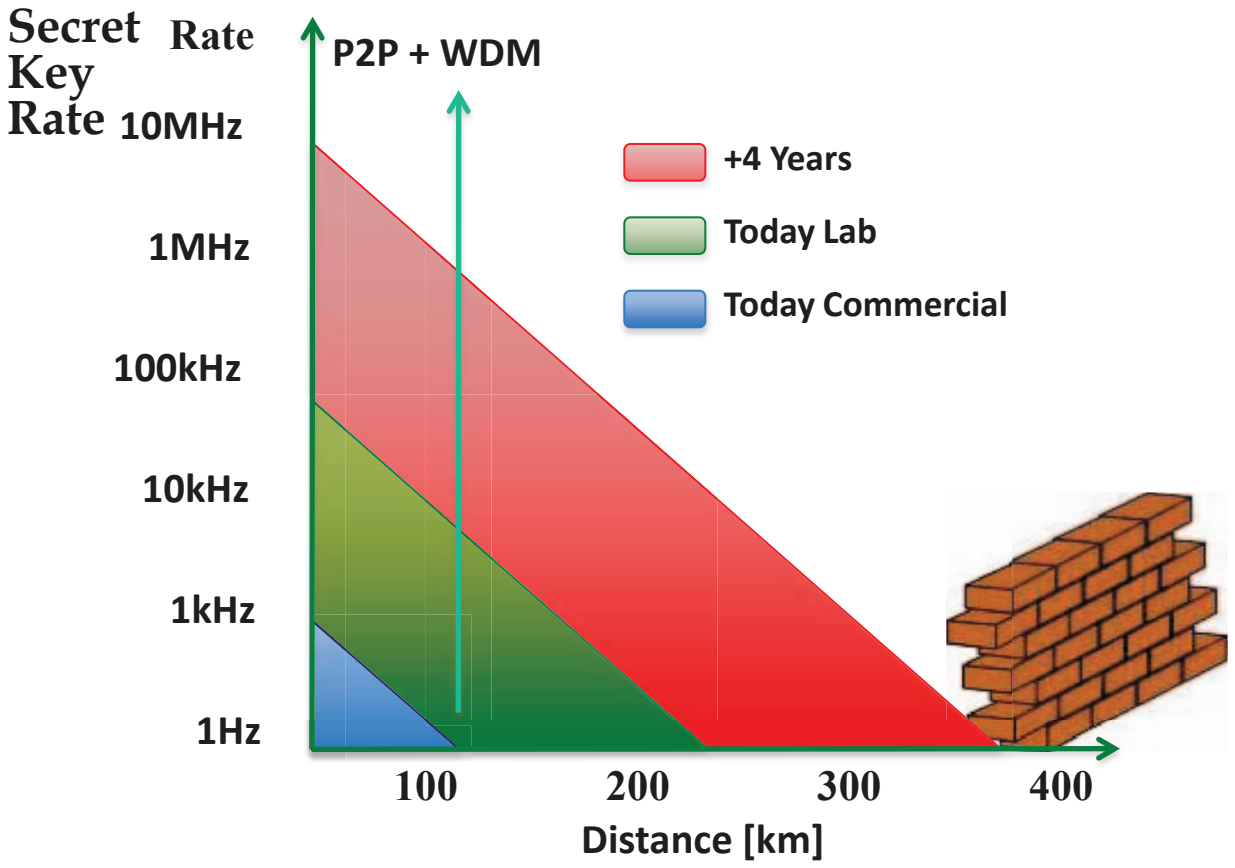
1. **Attacks have to be launched on the spot**
   ⇒ immune to future progress
2. With only the assumption of proper implementation
   ⇒ key expansion
3. Assuming short term secure of 1-way function
   ⇒ Cryptographic Key Distribution with long term security

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 Geneva University

OFC 2017 © OSA 2017

How far can one send a photon ?



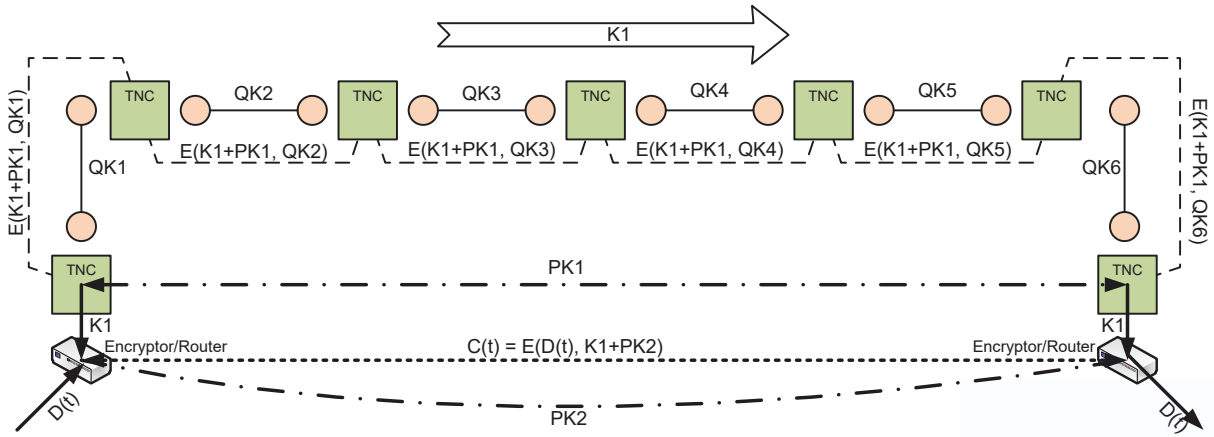
There is a hard wall around 400 km !

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 !

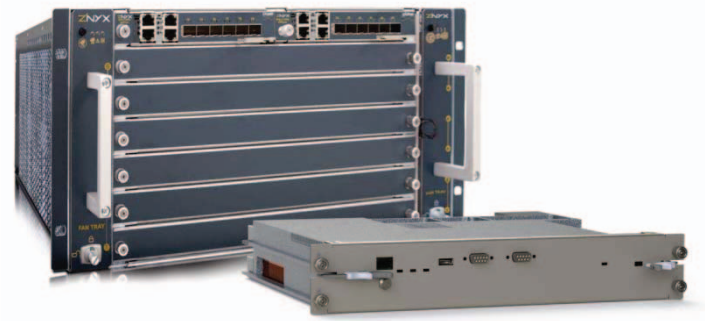
GAP Quantique Geneva University

OFC 2017 © OSA 2017

QKD Trusted Node



Keys move securely across the network in a piece-wise fashion

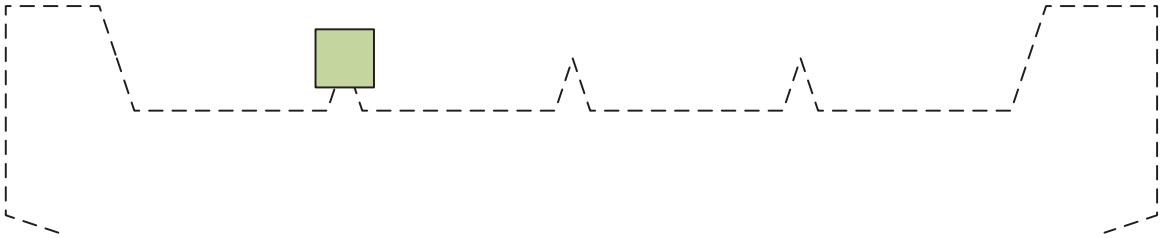


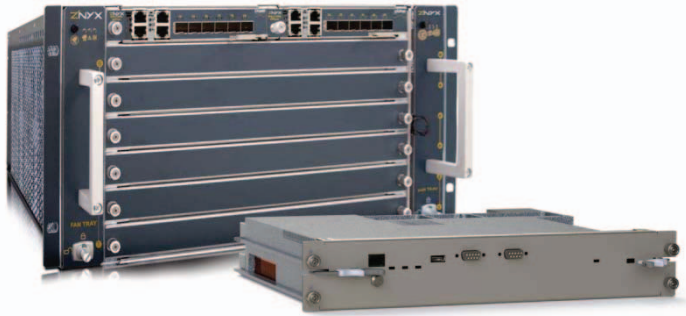
Telecom-compatible architecture (ATCA)
Up to 8 quantum blades per chassis

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

GAP Quantique Geneva University

QKD Trusted Node



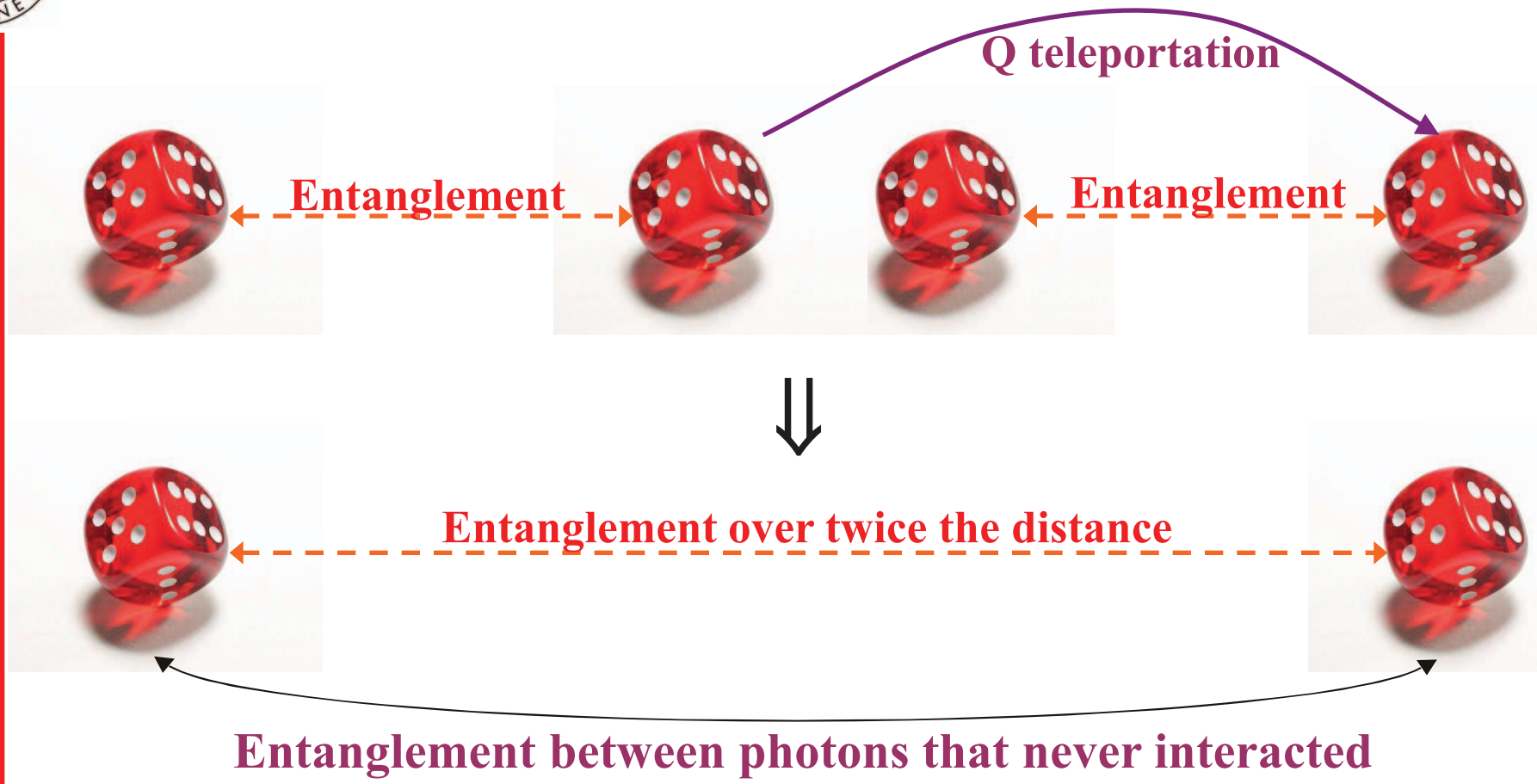


Telecom-compatible architecture (ATCA)
Up to 8 quantum blades per chassis

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

GAP Quantique Geneva University

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



This may look like magic, but it is well understood and mastered physics.

PRA 71, 05302, 2005

OFC 2017 © OSA 2017

N-photon quantum communication: quantum networks, quantum internet

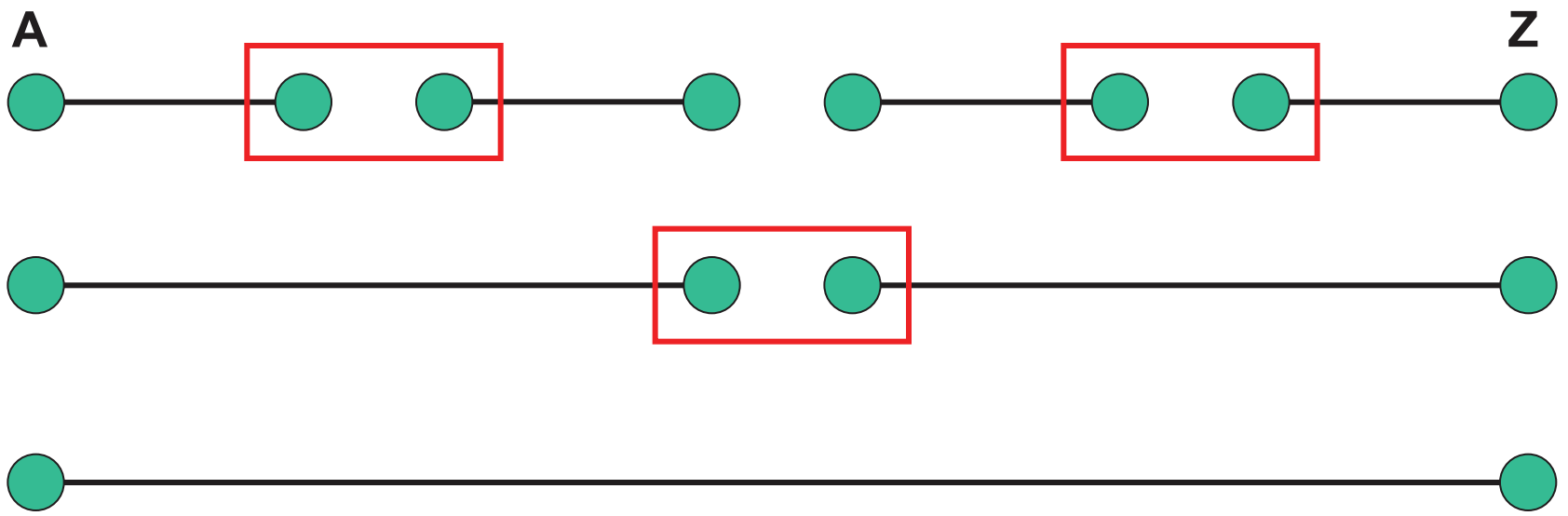
GAP Quantique Geneva University

- Q repeaters

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

OFC 2017 © OSA 2017

Quantum Repeater - Requirements



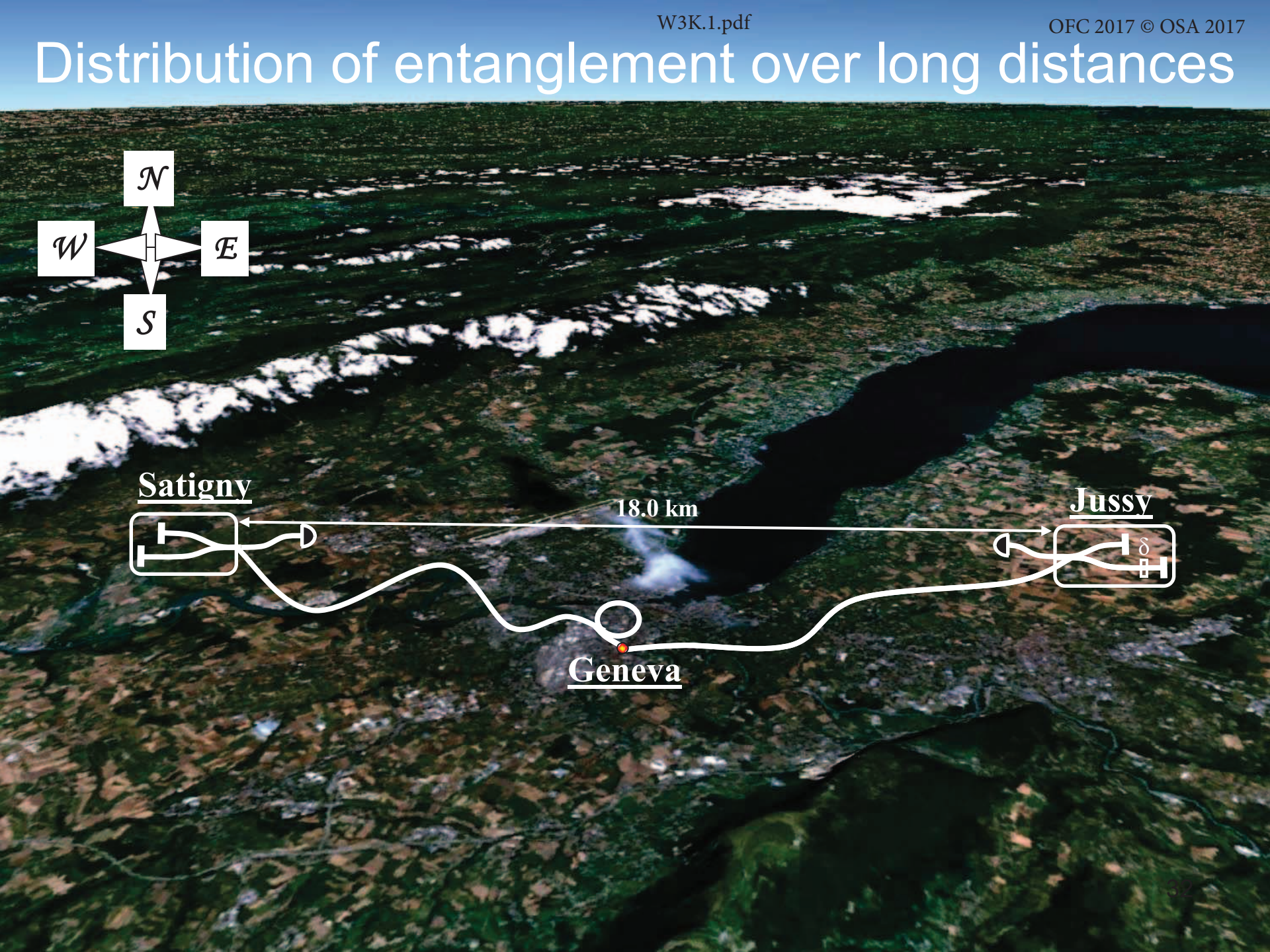
- Distribution of entanglement over long distances
- Multi-mode quantum memories
- Teleportation of entanglement @ telecom λ

C. Simon, H. de Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden and N. Gisin, Phys. Rev. Lett. 98, 190503 (2007)

GAP Quantique Geneva University

OFC 2017 © OSA 2017

Distribution of entanglement over long distances



OFC 2017 © OSA 2017

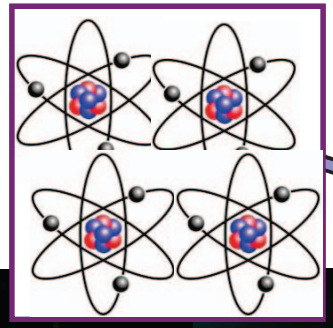
Quantum memory

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

University

photon in

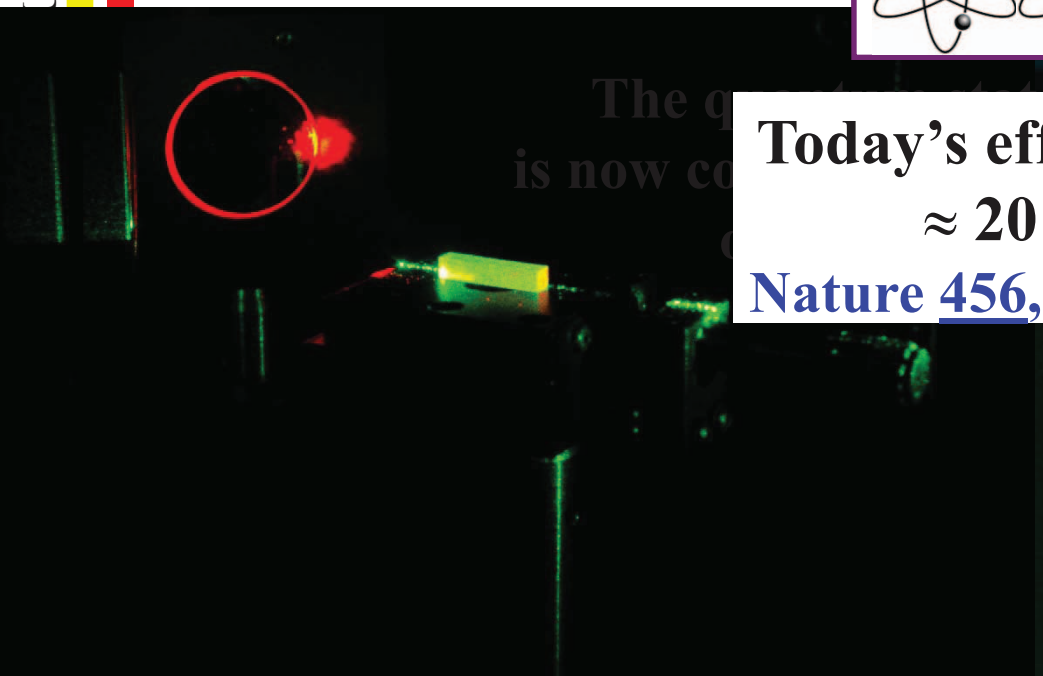
crystal doped with billions of ions

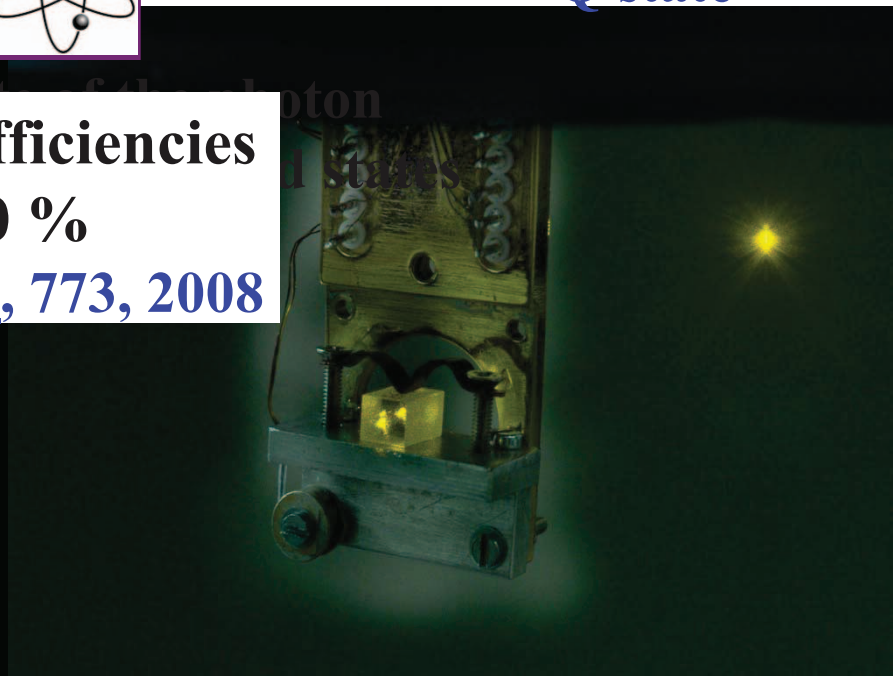


photon out at desired time in same Q state

Today's efficiencies ≈ 20 %

Nature 456, 773, 2008



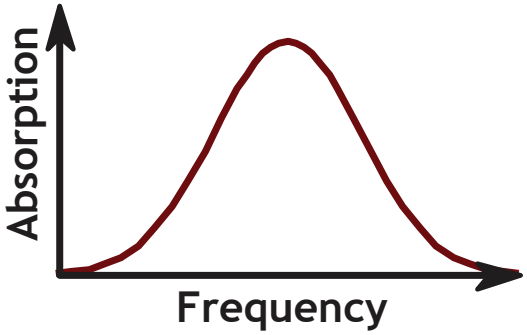


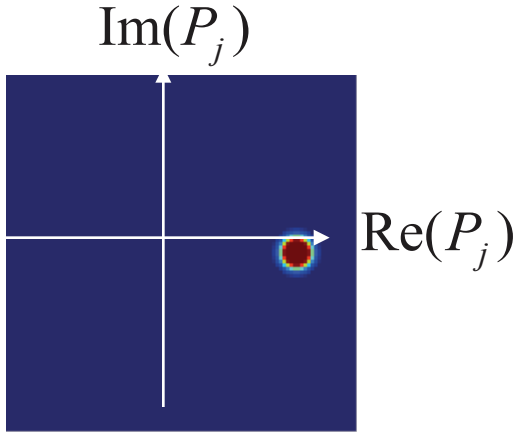
Controlling the Dephasing! Atomic Frequency Comb

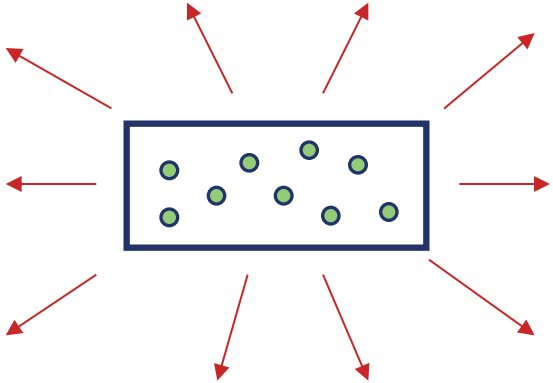
$$\sum_{j=1}^{N} e^{ikr_j} e^{-i\delta_j t} \left| g_1 \ldots e_j \ldots g_N \right\rangle$$

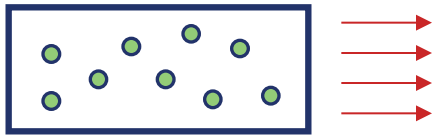
$$P_j = e^{-i\delta_j t}$$

Δ continuous $\Rightarrow$ Dephasing







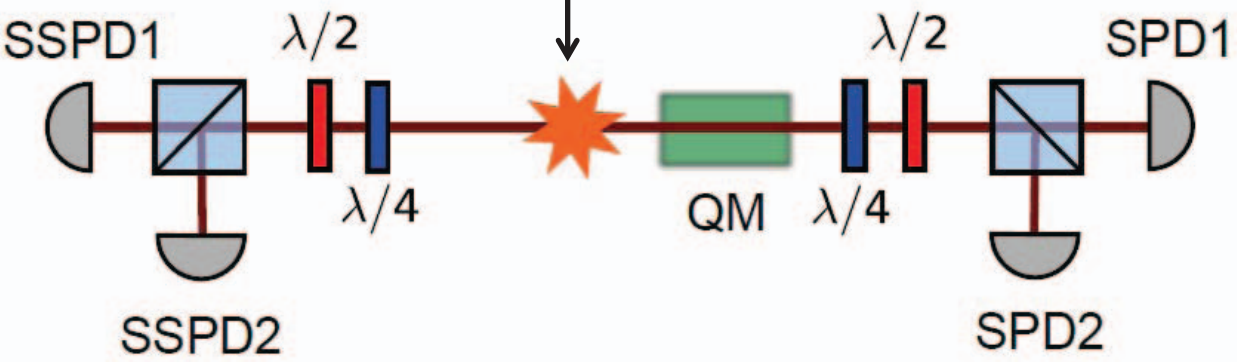


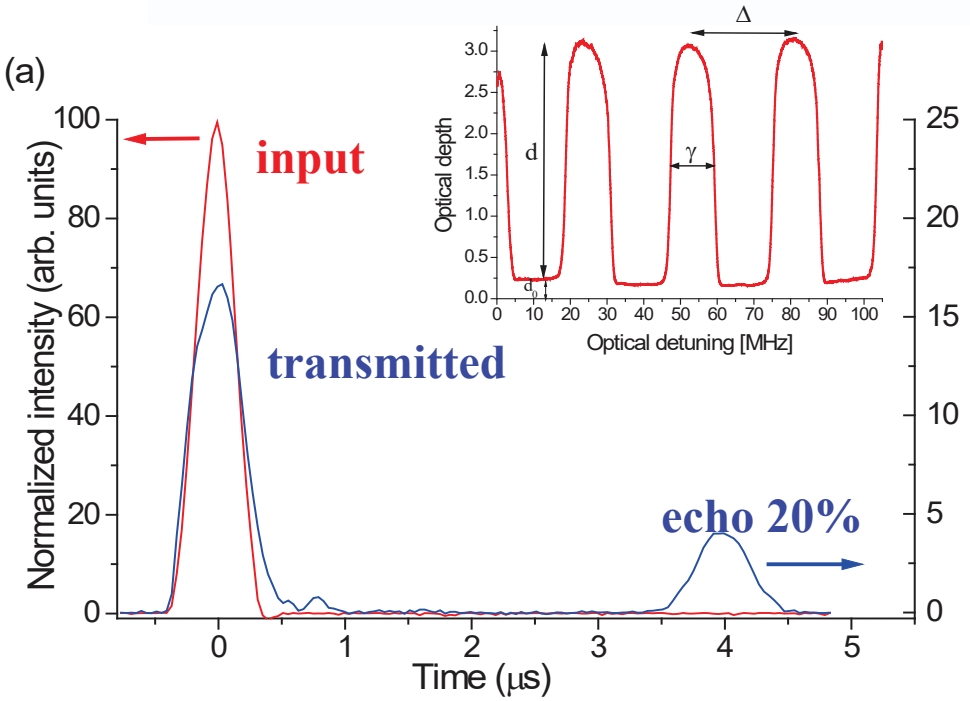
GAP Quantique Geneva University

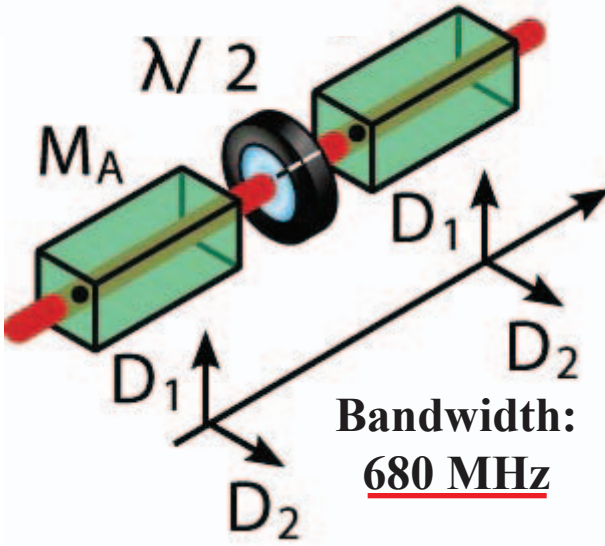
Entanglement-preserving quantum memory

GAP Quantique Geneva University

$$\left|\Phi^{+}\right\rangle = \left|H\right\rangle_{1338}\left|H\right\rangle_{883} + \left|V\right\rangle_{1338}\left|V\right\rangle_{883}$$



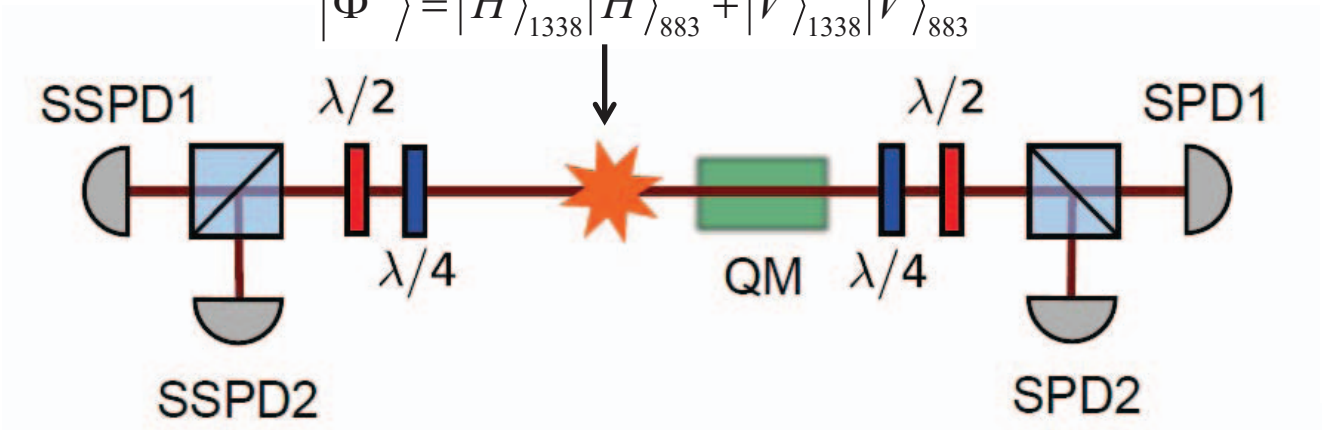


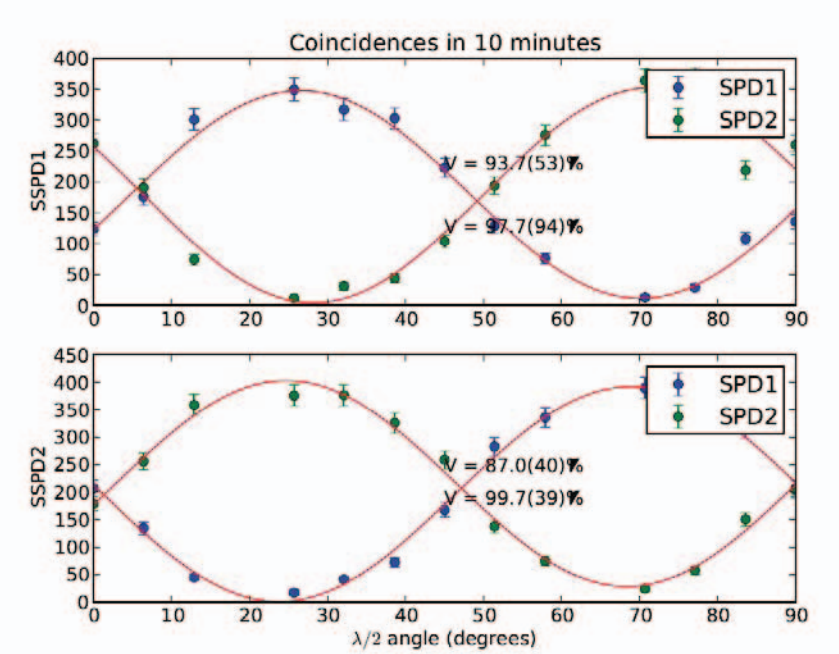


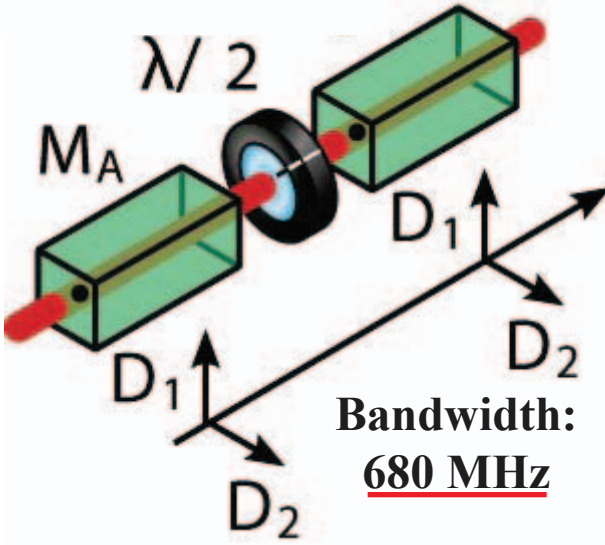
Entanglement-preserving quantum memory

GAP Quantique Geneva University

$$\left|\Phi^{+}\right\rangle = \left|H\right\rangle_{1338}\left|H\right\rangle_{883} + \left|V\right\rangle_{1338}\left|V\right\rangle_{883}$$



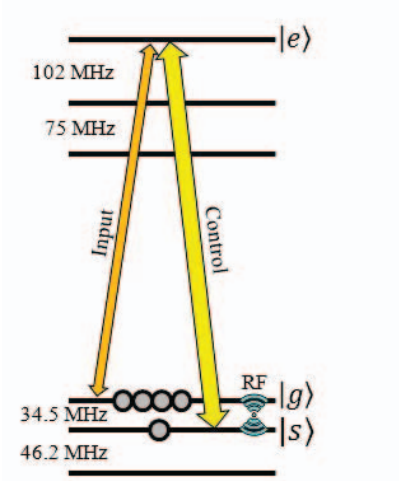


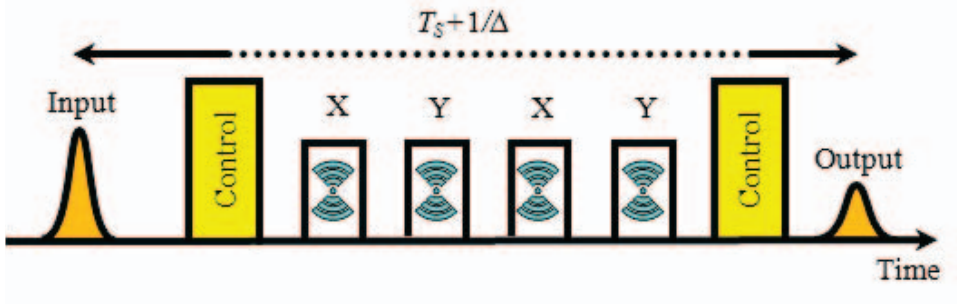


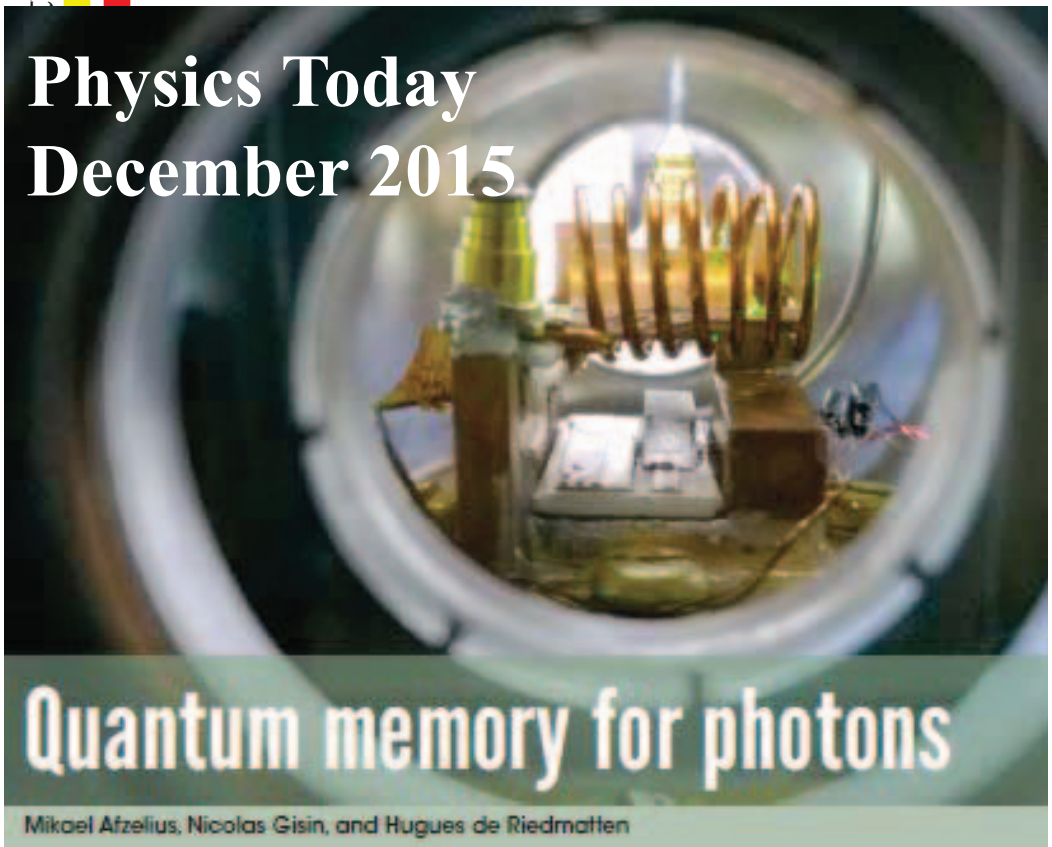
CHSH = 2.52±0.13 ⇒ nonlocal quantum randomness

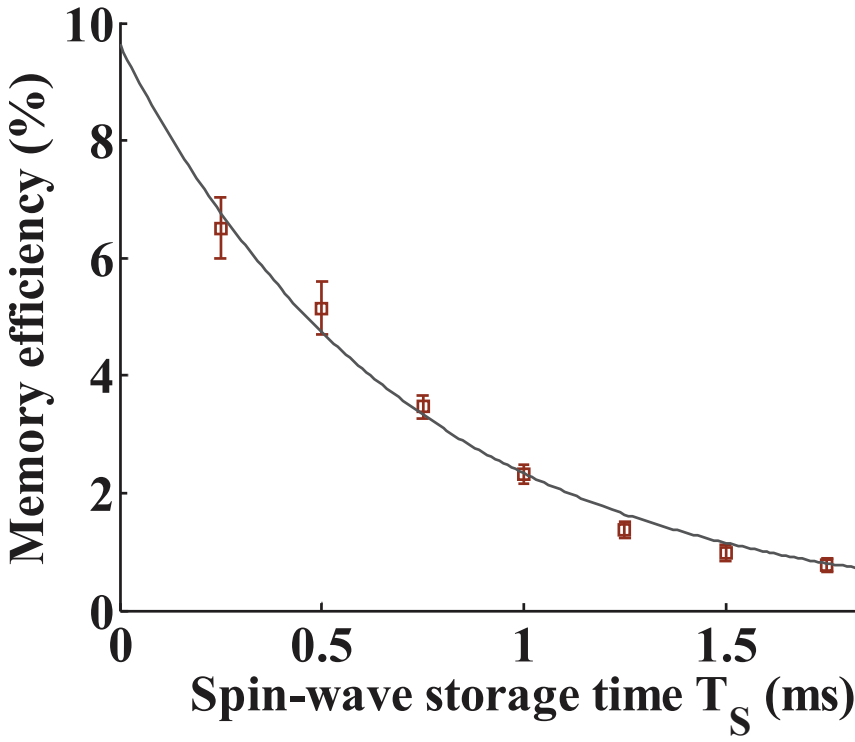
OFC 2017 © OSA 2017

Longuest read-write quantum memory in solid ≈ 1ms



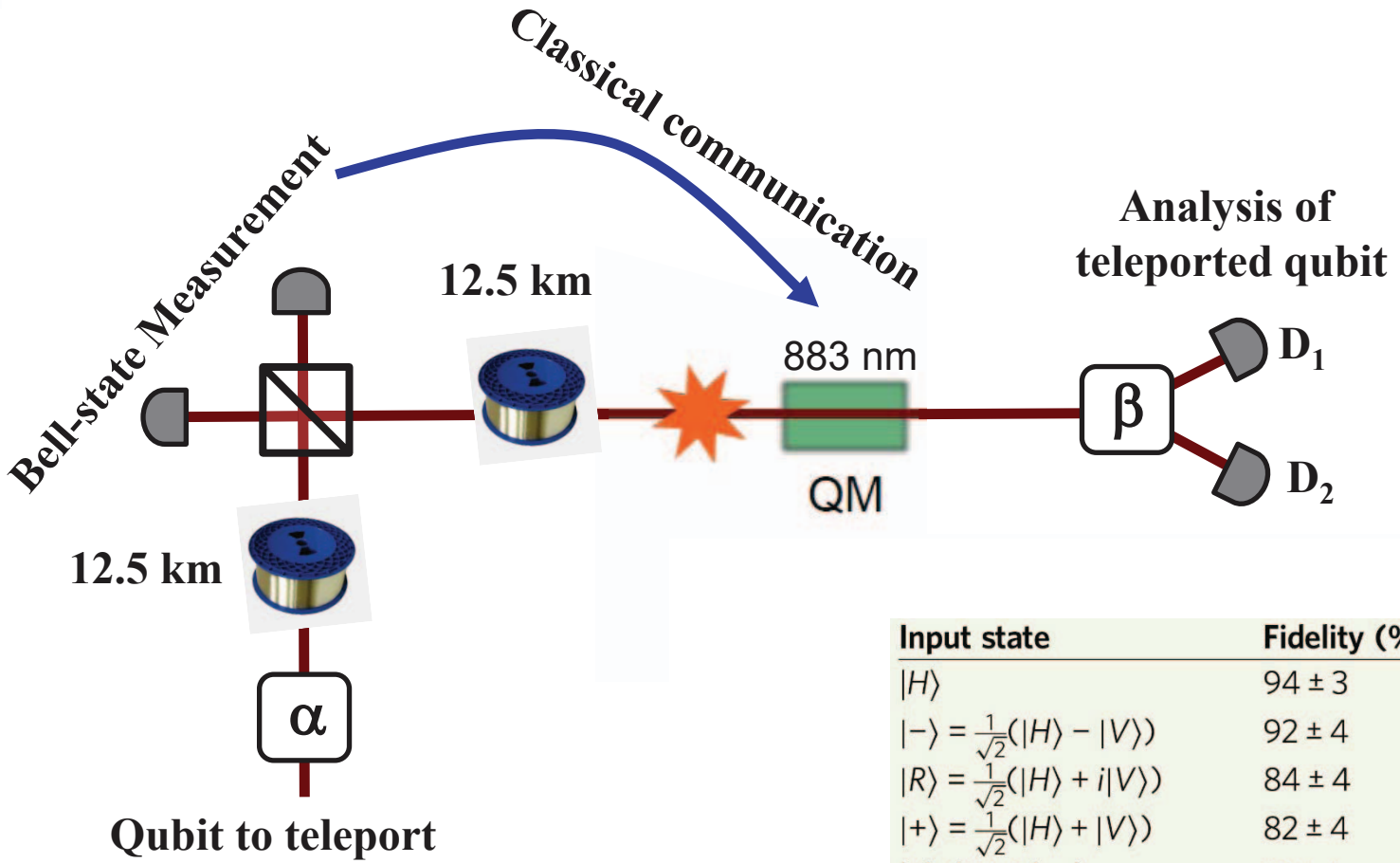






OFC 2017 © OSA 2017

Teleportation from a telecom photon to a memory over 25 km



Input state	Fidelity (%)
$\|H\rangle$	94 ± 3
$\|-\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$	92 ± 4
$\|R\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + i\|V\rangle)$	84 ± 4
$\|+\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$	82 ± 4
$\|+\rangle$ (24.8 km)	81 ± 4

C. Clausen, F. Bussières, A. Tiranov, M. Afzelius et. al., Nature Photonics 8, 775 (2014)

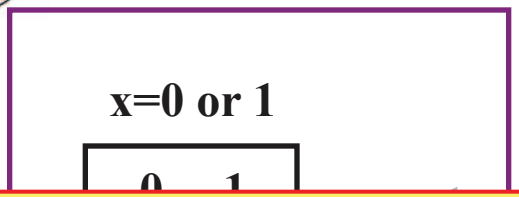
GAP Quantique Geneva University

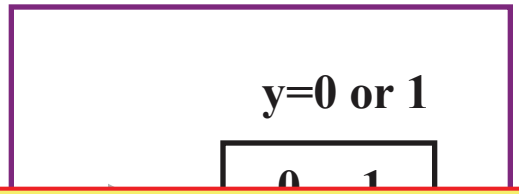
Academic research: DI-QKD

OFC 2017 © OSA 2017

Alice

Bob





If p(a,b|x,y) violates some Bell inequality, then p(a,b|x,y) contains secrecy irrespective of any detail of the implementation !

After publicly announcing a fair sample of their data, Alice and Bob's information is entirely contained in the conditional probability

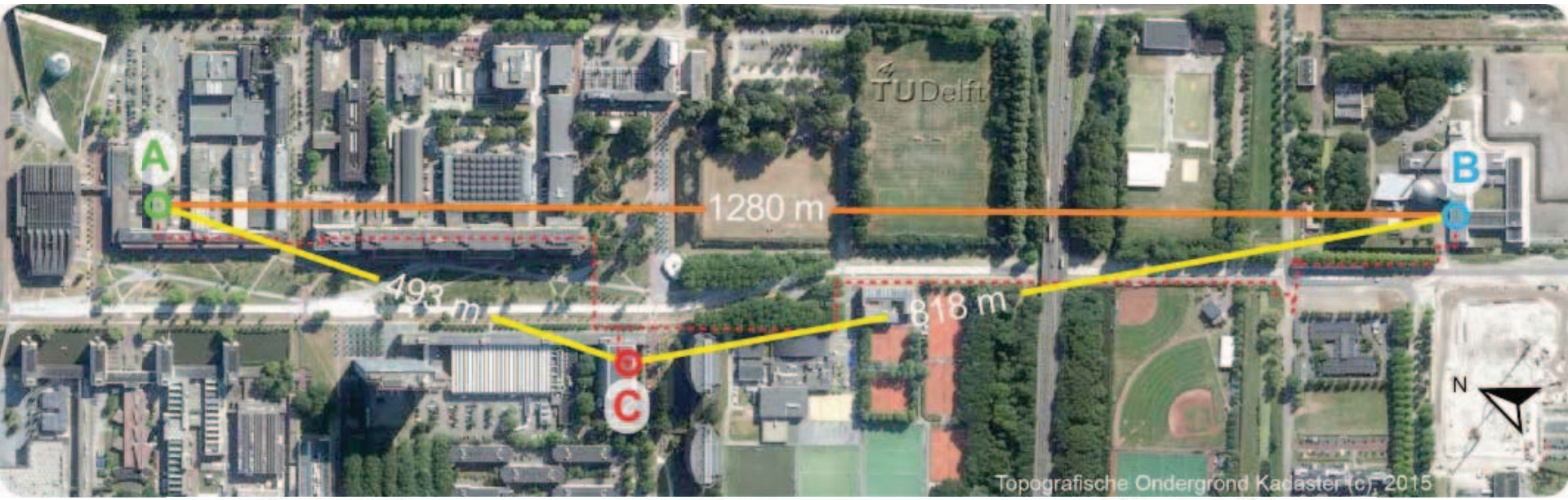
p(a,b|x,y)

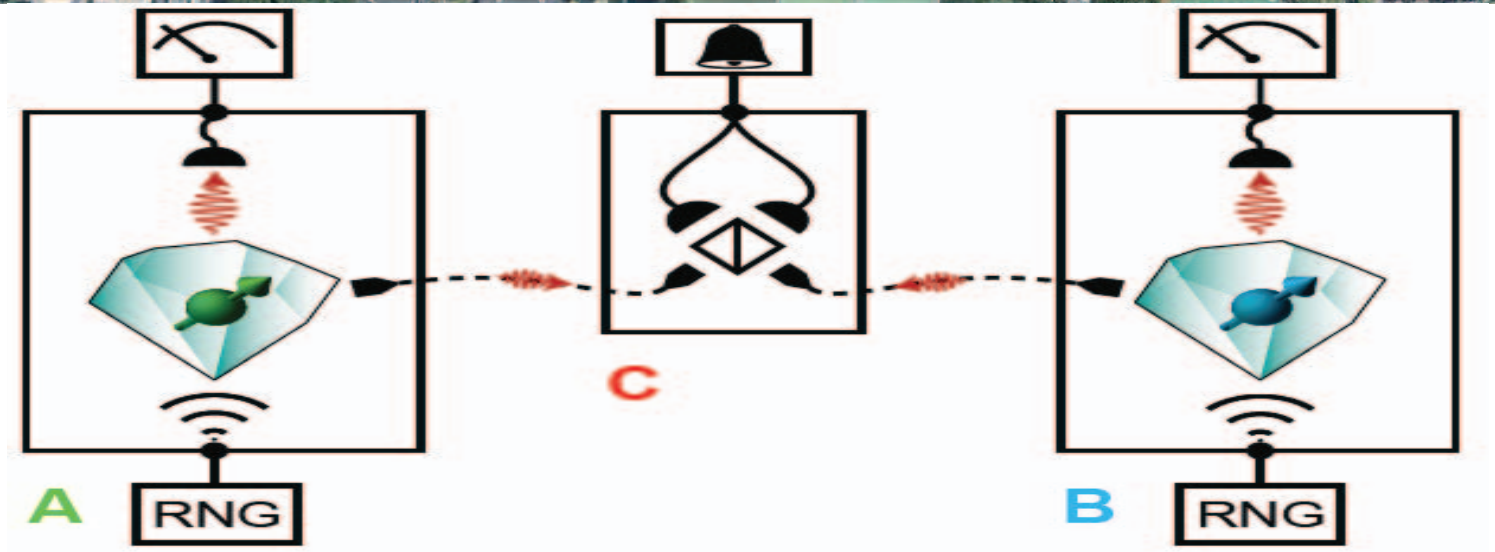
PRL 98, 230501, 2007; PRL 97, 120405, 2006; NJP 11, 1, 2009

QCEC 2017 © OSA 2017

A loophole-free Bell test in Delft

Ronald Hanson's group



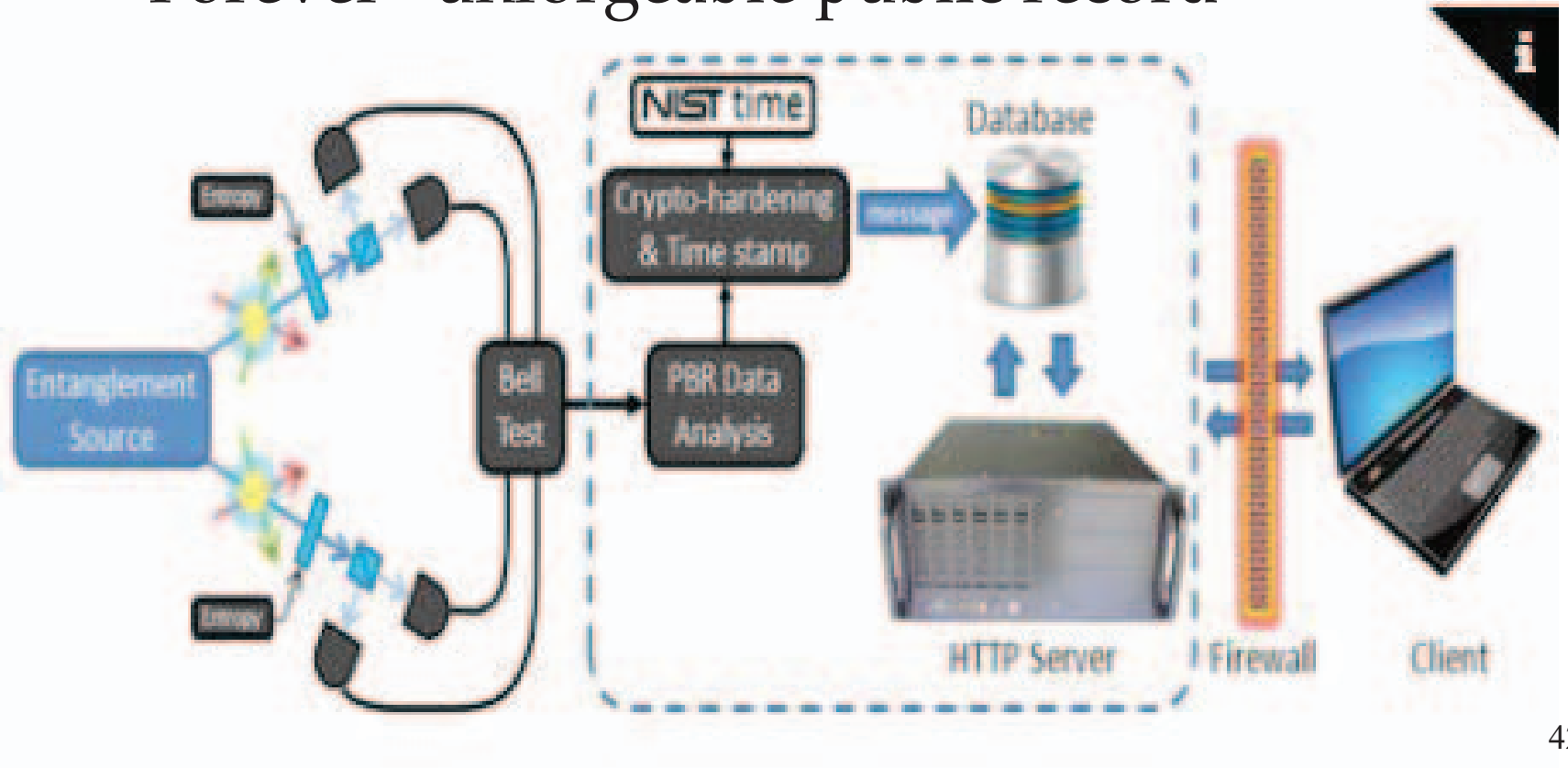


4 loophole-free Bell tests:

1. **Delft with e-spins in diamonds**
2. **NIST and Vienna with photons and supraconducting detectors**
3. **Münich with entangled atoms**

Public Randomness: https://beacon.nist.gov/home

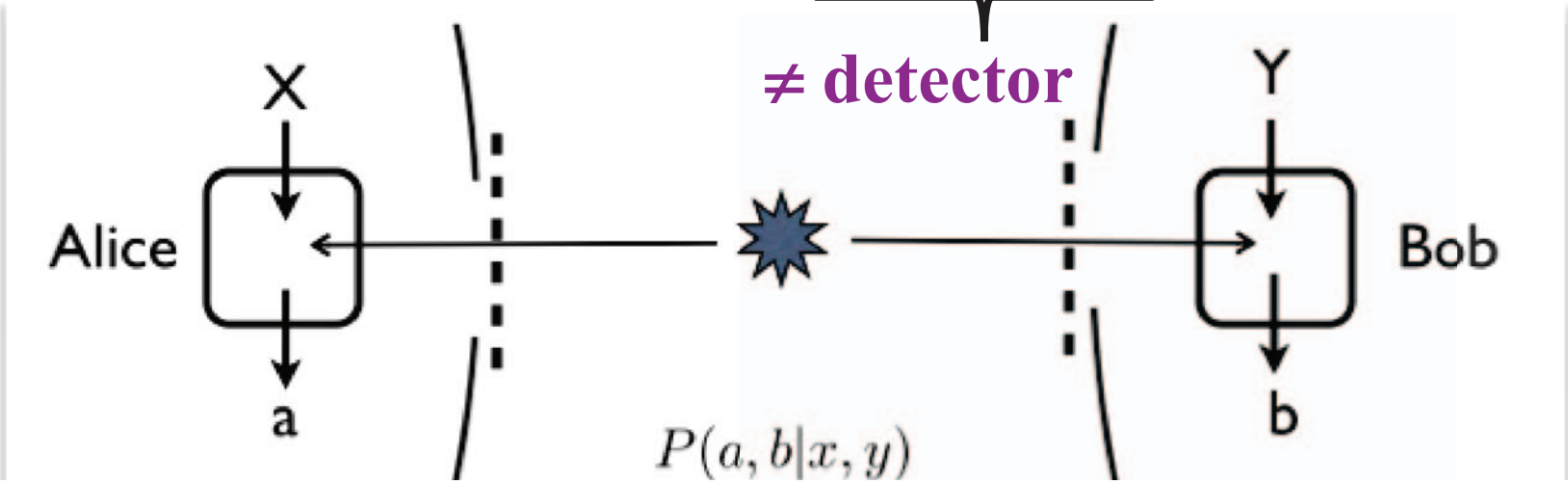
- Public, time-bound randomness
- Unpredictability, Autonomy, Consistency
- "Forever" unforgeable public record



OFC 2017 © OSA 2017

Bell violation guarantees entanglement independently of the devices !

Beautiful idea ... but it is crucial to close the detection loophole!



Required detection efficiency > 82.8%

But the transmission efficiency of 10 km of telecom fiber is roughly 60% !

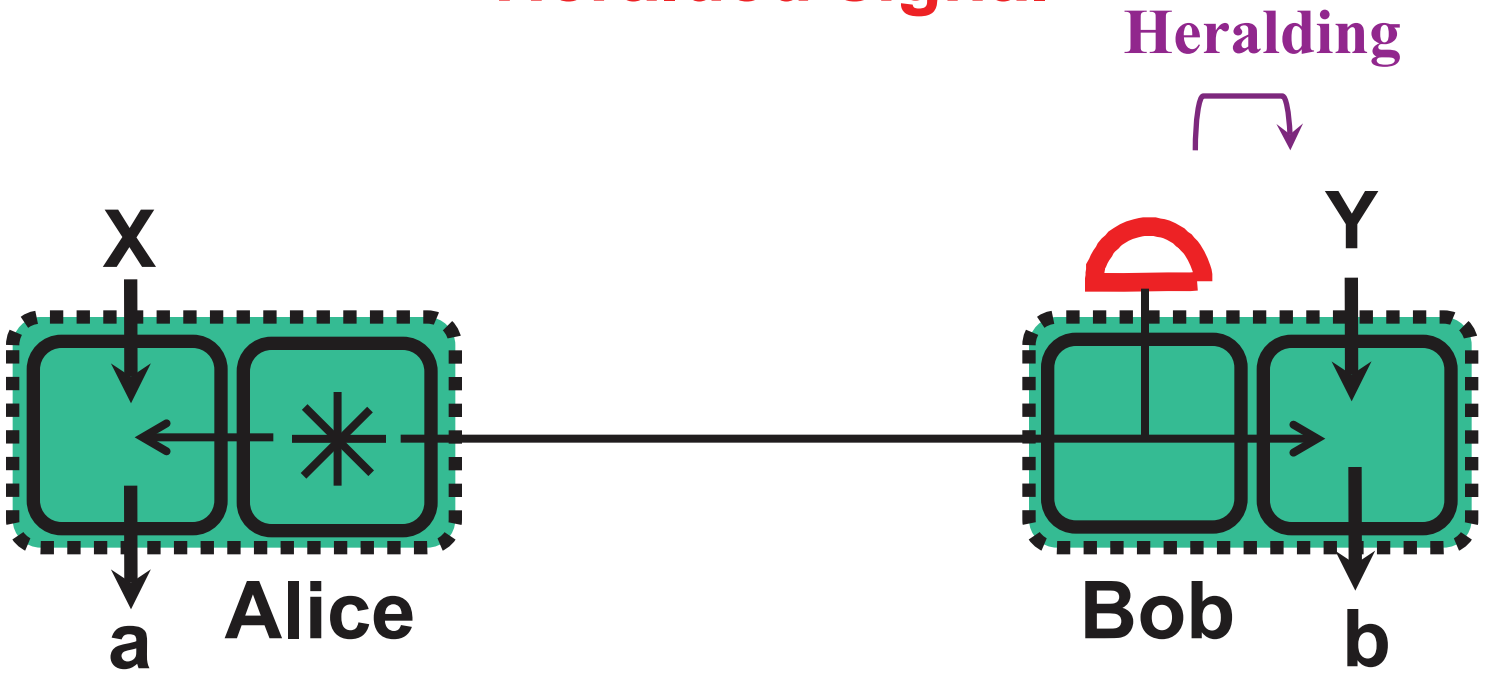
The infamous Detection Loophole is now part of Applied Physics !!!

GAP Quantique Geneva University

OFC 2017 © OSA 2017

To overcome the transmission losses :

Heralded signal



NG, S. Pironio & N. Sangouard, PRL 105, 070501 (2010)

Experimental DI-QKD is a new Grand Challenge for Quantum communication !

T.C. Ralph & A.P. Lund, arXiv:0809.0326

4

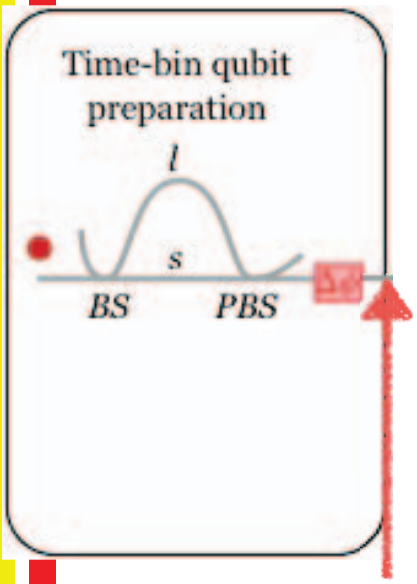
GAP Quantique Geneva University

OFC 2017 © OSA 2017

Heralded Qubit Amplification

Telecom – Fiber – Time-bin

GAP Quantique Geneva University



$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\ell_H\rangle + e^{i\Delta\phi}|s_V\rangle\right)$$

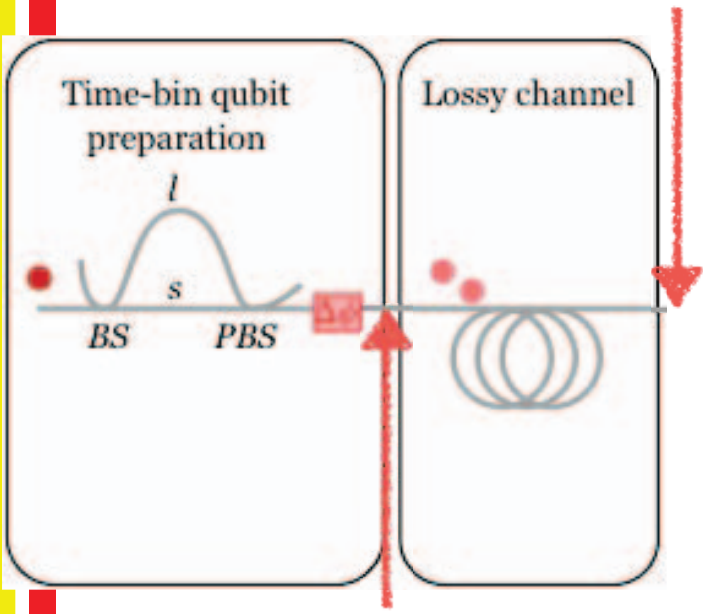
Optics Express 24, 125 (2016)

OFC 2017 © OSA 2017

Heralded Qubit Amplification

Telecom – Fiber – Time-bin

$$\rho_{in} = (1-p)|0\rangle\langle 0| + p|\psi\rangle\langle\psi|$$



$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\ell_H\rangle + e^{i\Delta\phi}|s_V\rangle\right)$$

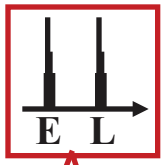
GAP Quantique Geneva University

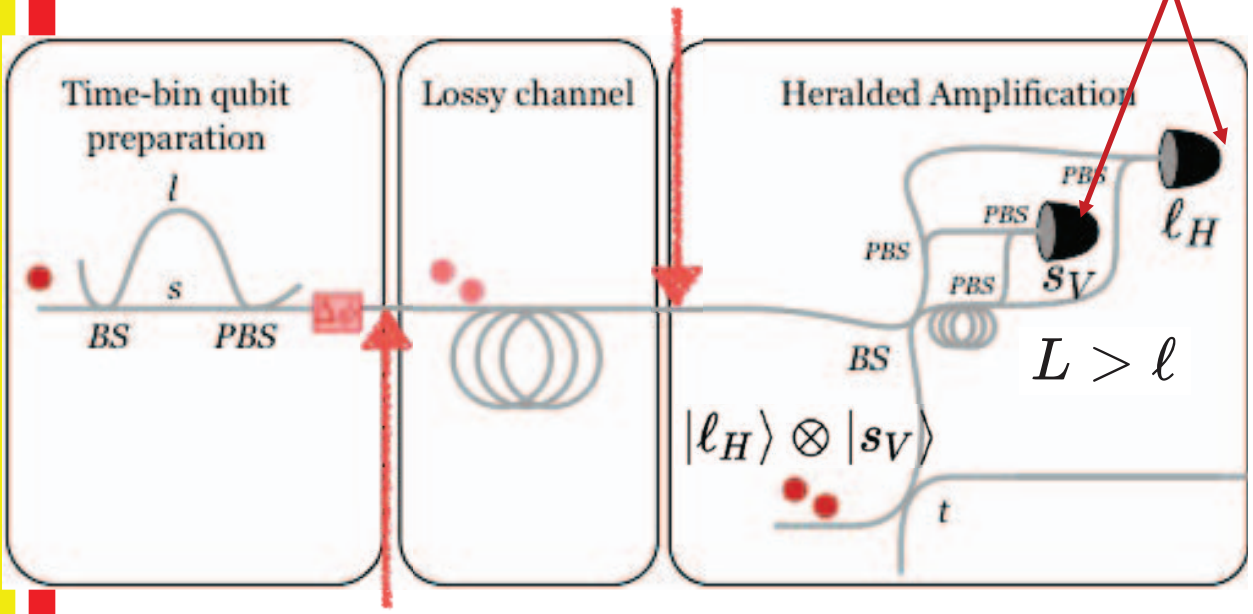
Optics Express 24, 125 (2016)

Heralded Qubit Amplification

Telecom – Fiber – Time-bin

$$\rho_{in} = (1-p)|0\rangle\langle 0| + p|\psi\rangle\langle\psi|$$





$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\ell_H\rangle + e^{i\Delta\phi}|s_V\rangle\right)$$

GAP Quantique Geneva University

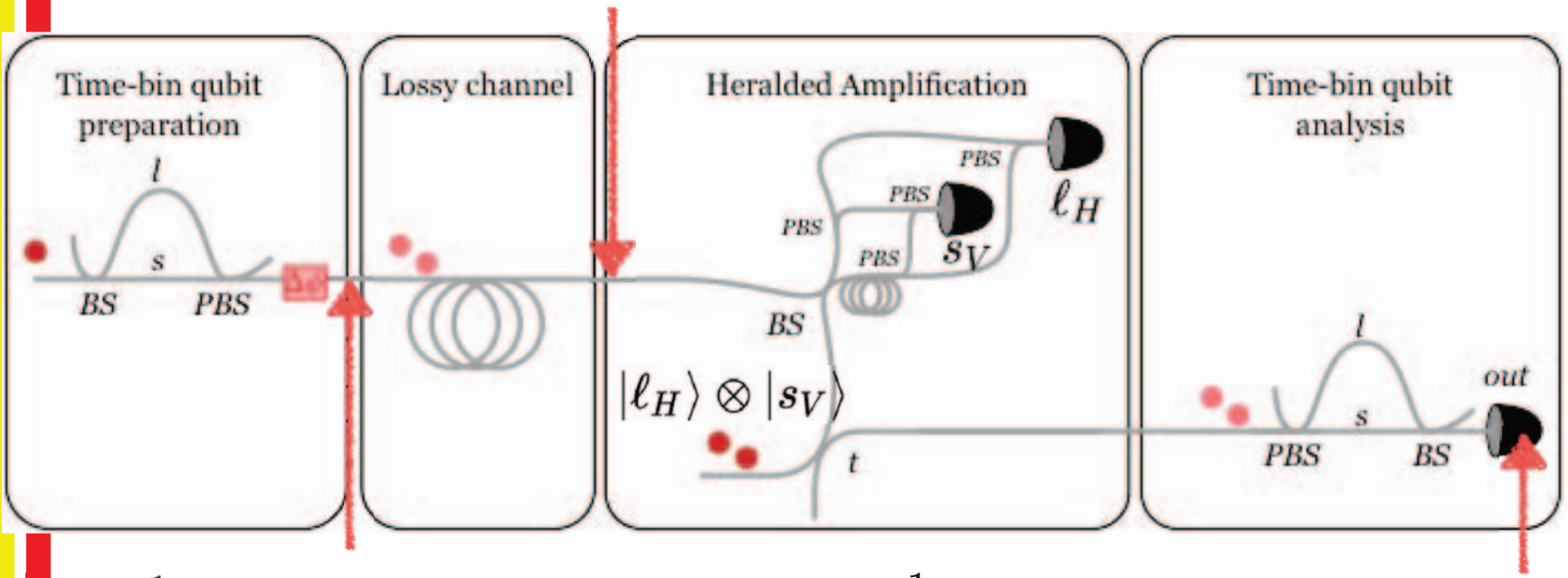
Optics Express 24, 125 (2016)

OFC 2017 © OSA 2017

Heralded Qubit Amplification

Telecom – Fiber – Time-bin

$$\rho_{in} = (1-p)|0\rangle\langle 0| + p|\psi\rangle\langle\psi|$$



$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\ell_H\rangle + e^{i\Delta\phi}|s_V\rangle\right)$$

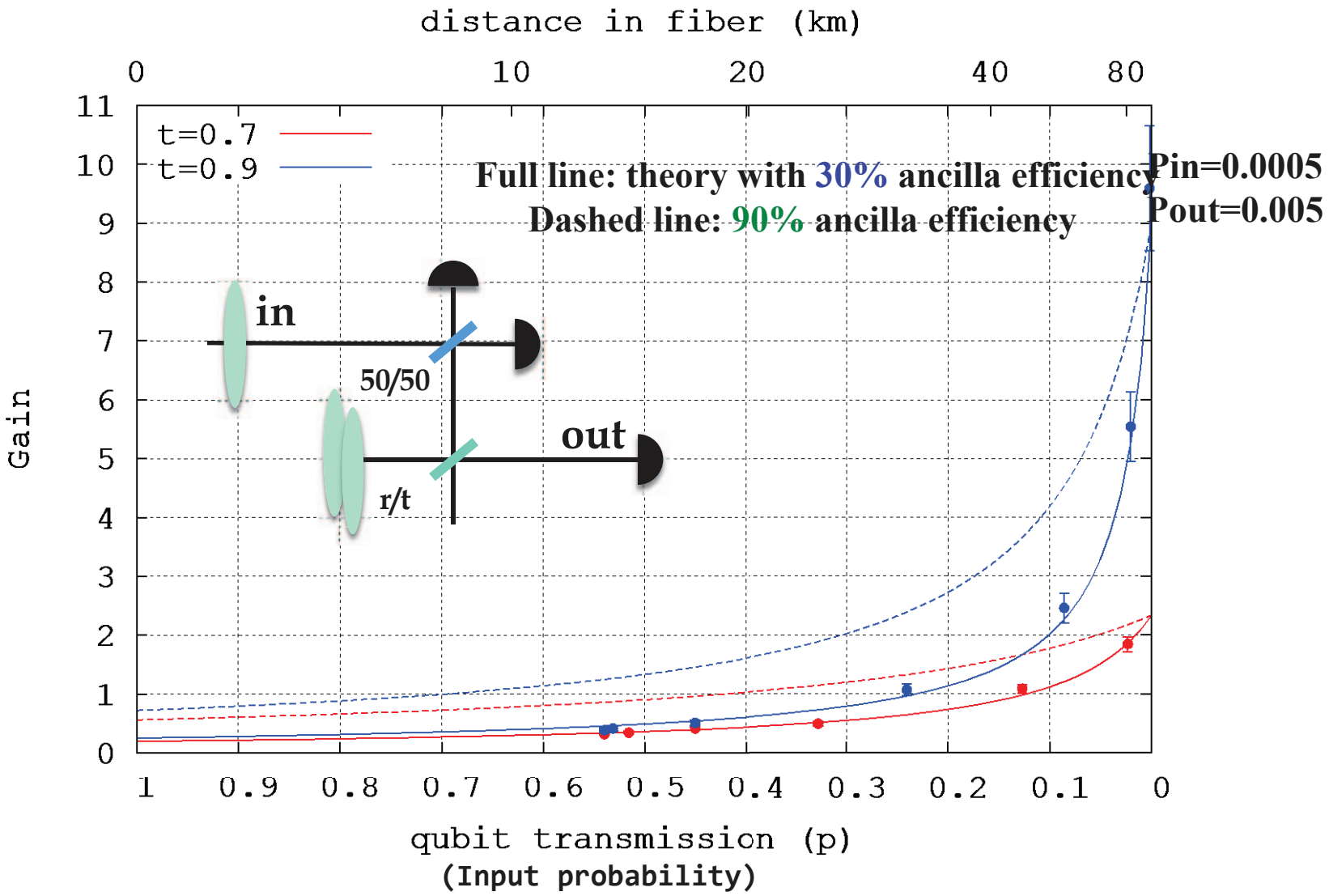
$$\rho_{out} = \frac{1}{N(t)}\left[(1-p)|0\rangle\langle 0| + g(t)\,p\,U|\psi\rangle\langle\psi|U^{-1}\right]$$

GAP Quantique Geneva University

Optics Express 24, 125 (2016)

OFC 2017 © OSA 2017

Result

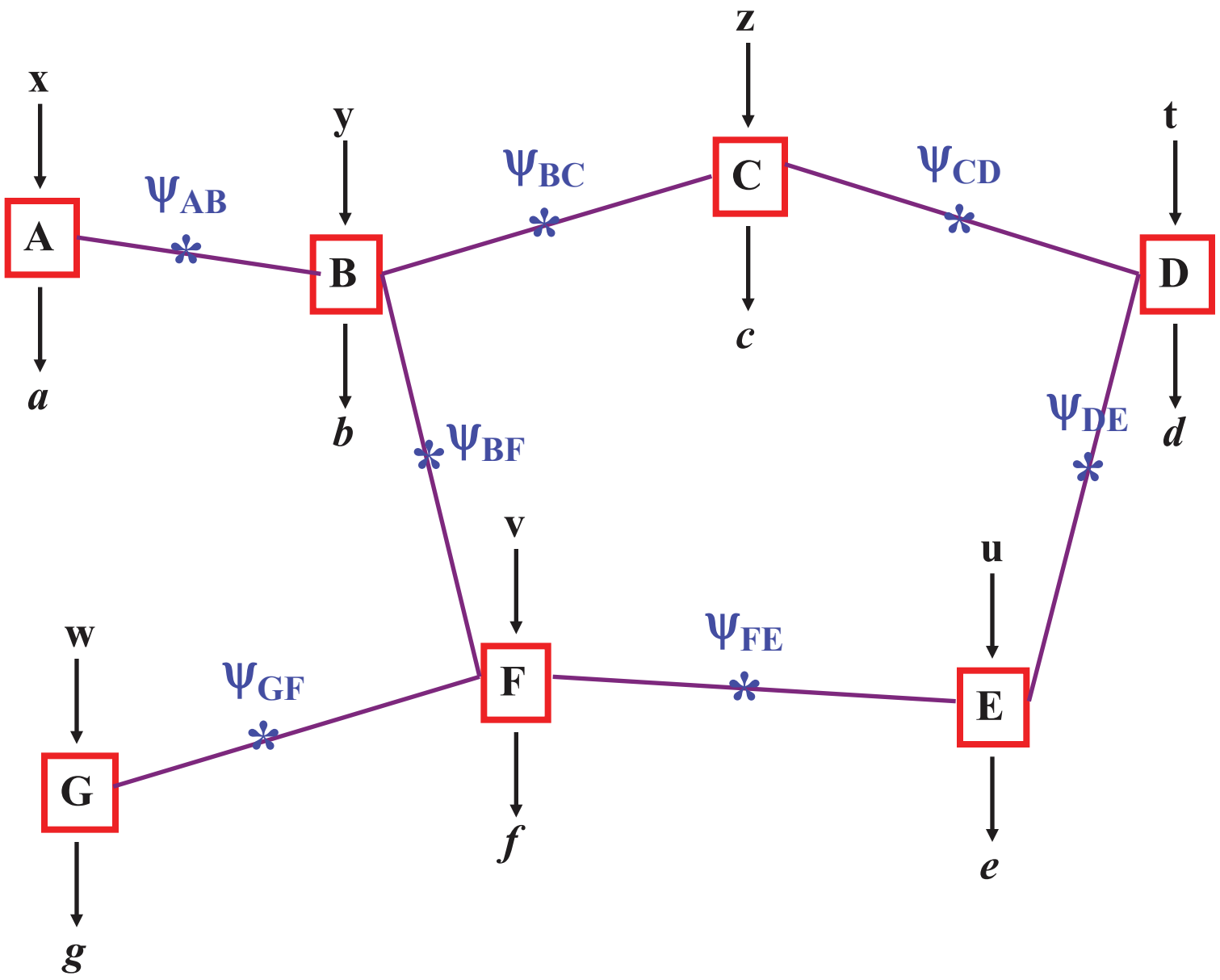


GAP Quantique Geneva University

Optics Express 24, 125 (2016)

OFC 2017 © OSA 2017

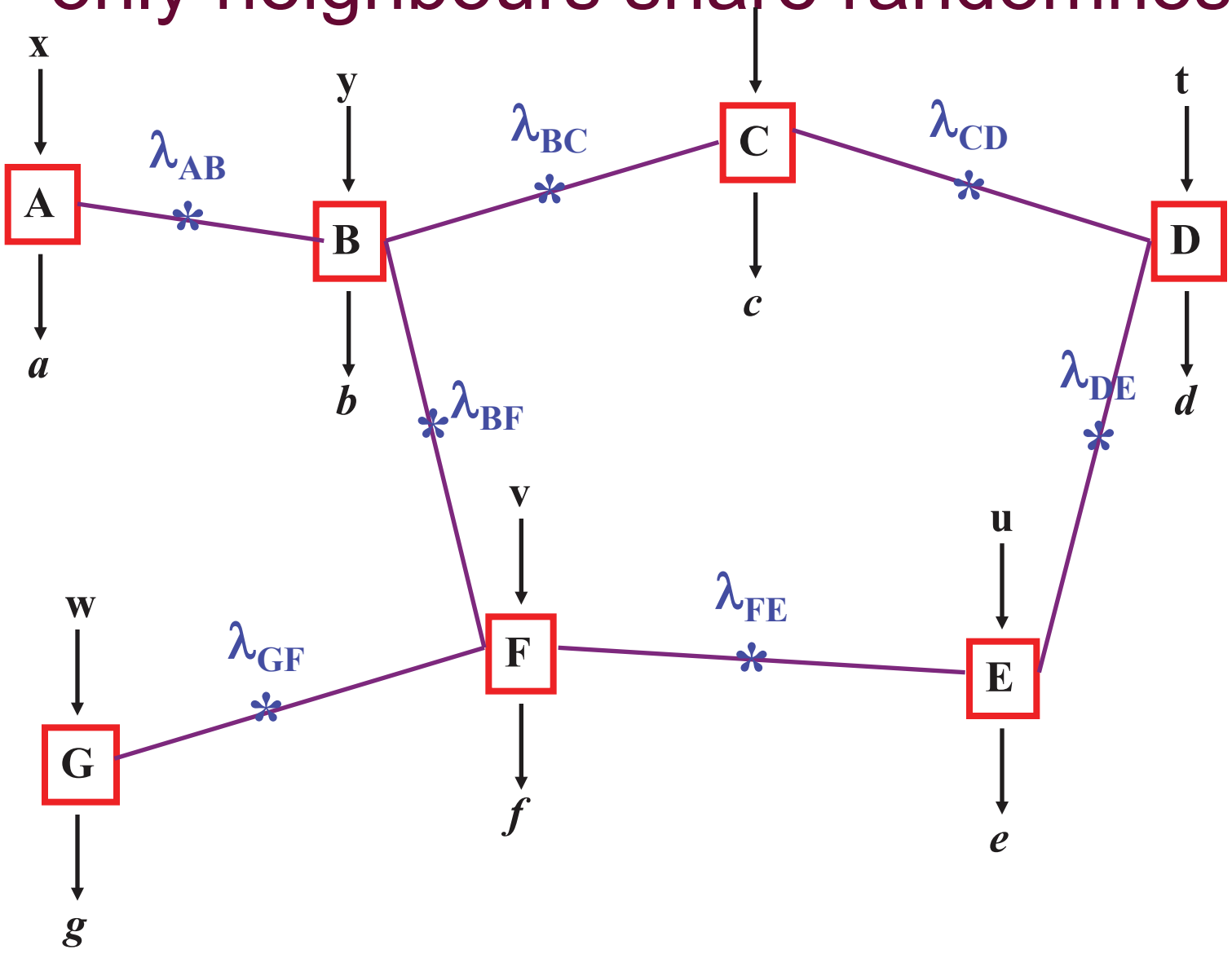
N independent sources: product state $\psi^{\otimes N}$



GAP Quantique Geneva University

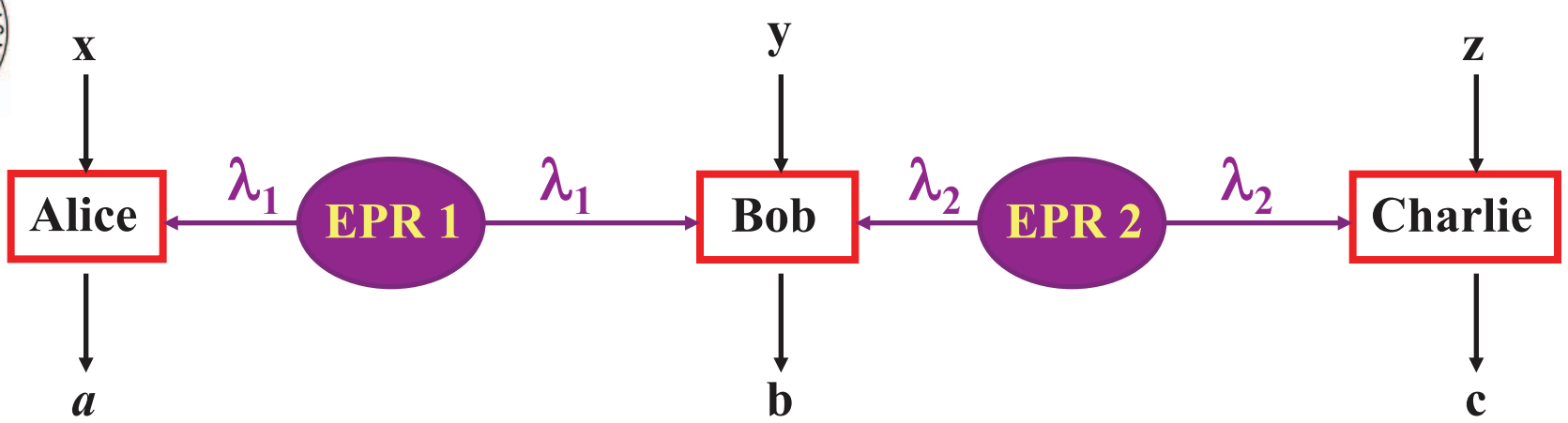
OFC 2017 © OSA 2017

⇒N independent local variables : only neighbours share randomness



Bi-locality

Branciard, NG, Pisanic
QFC 2017 © USA 2017
PRL 104, 170401-1/4, 2010



$\Rightarrow$ P(a,b,c|x,y,z)

Independent locality (bi-locality) : $I(\lambda_1:\lambda_2) = 0$, or $P(\lambda 1,\lambda 2)=P(\lambda_1)\cdot P(\lambda_2)$

$$P_{biloc.}(a,b,c|x,y,z,\lambda_1,\lambda_2) = p(a|x, \lambda_1) \cdot p(b|y, \lambda_1, \lambda_2) \cdot p(c|z, \lambda_2)$$

$\Rightarrow$??? Bell-like inequalities ???

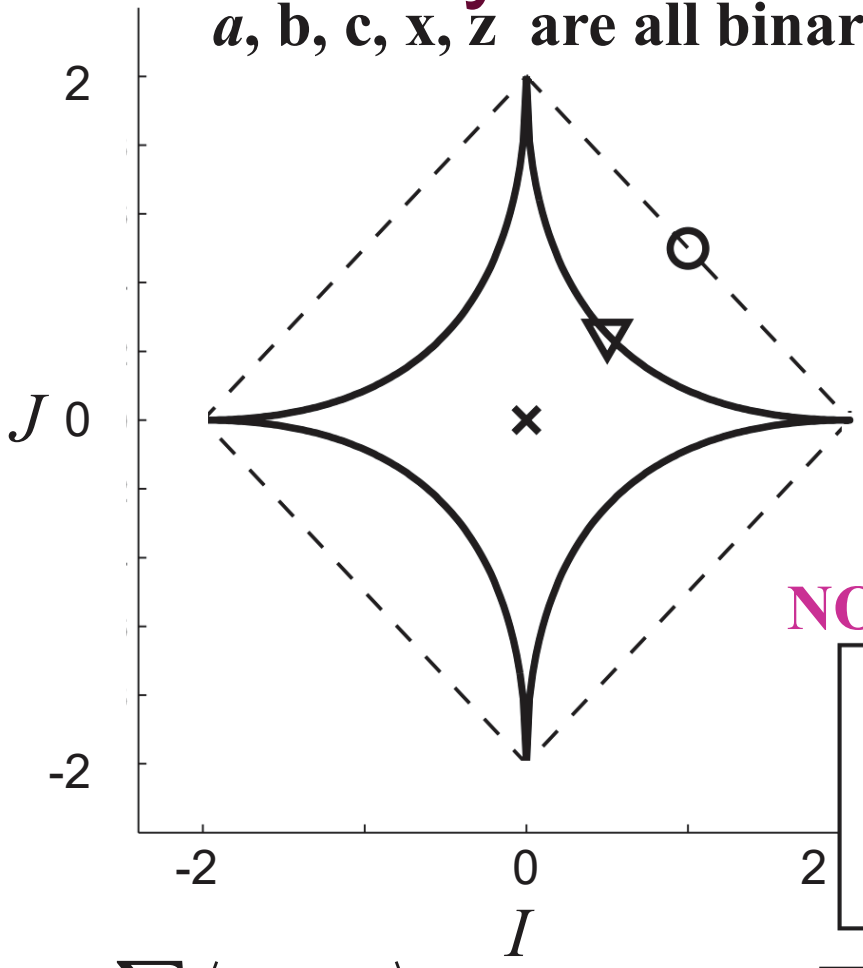
The set of bilocal $p_{biloc}(a,b,c\,|\,x,y,z)$ is not convex:
The deterministic strategy *a*=c=0 is bi-local
The deterministic strategy *a*=c=1 is bi-local
But the probabilistic strategy *a*=c is not bi-local !

GAP Quantique Geneva University

Bi-locality: an example

Branciard, NG, Pironio PRL 104, 170401-1/4, 2010

Rosset +Branciard et al. PRL 116, 010403, 2016



NONLINEAR INEQUALITY:

$$\sqrt{|I|}+\sqrt{|J|}\leq 2$$

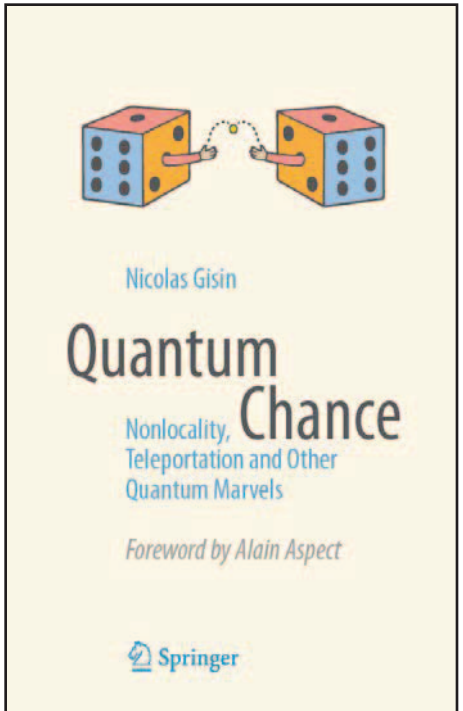
$$I=\sum_{x,z}\langle a_x b_0 c_z\rangle \qquad J=\sum_{x,z}(-1)^{x+z}\langle a_x b_1 c_z\rangle$$

Critical visibility V_{th}=1/2, significantly lower than for CHSH, hence it is easier to experimentally demonstrate quantumness.

GAP Quantique Geneva University

OFC 2017 © OSA 2017

Conclusions

GAP Quantique Geneva University

- Quantum Physics offers True Randomness:
  - ⇒ Quantum Random Number Generator.
- Quantum Physics offers nonlocal Randomness:
  - ⇒ Distribution of Cryptographic Keys (QKD).
- In the Future we'll have:
  - ✓ Longer Distances
  - ✓ Faster Key Distribution
  - ✓ Cheaper QKD
- Quantum repeaters are promising, but still in the laboratories
- Device-Independent Quantum Info. Processing is fascinating and not that far in the future.