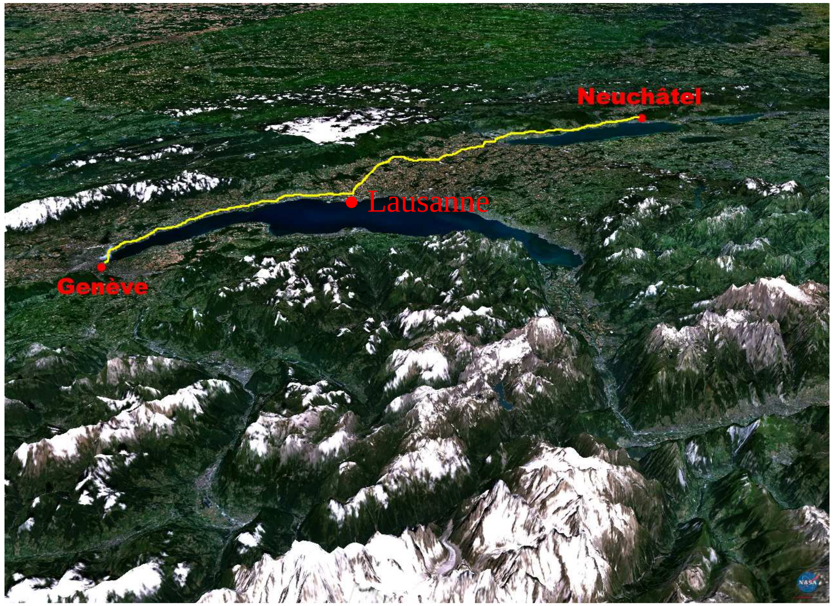
GAP Optique Geneva University

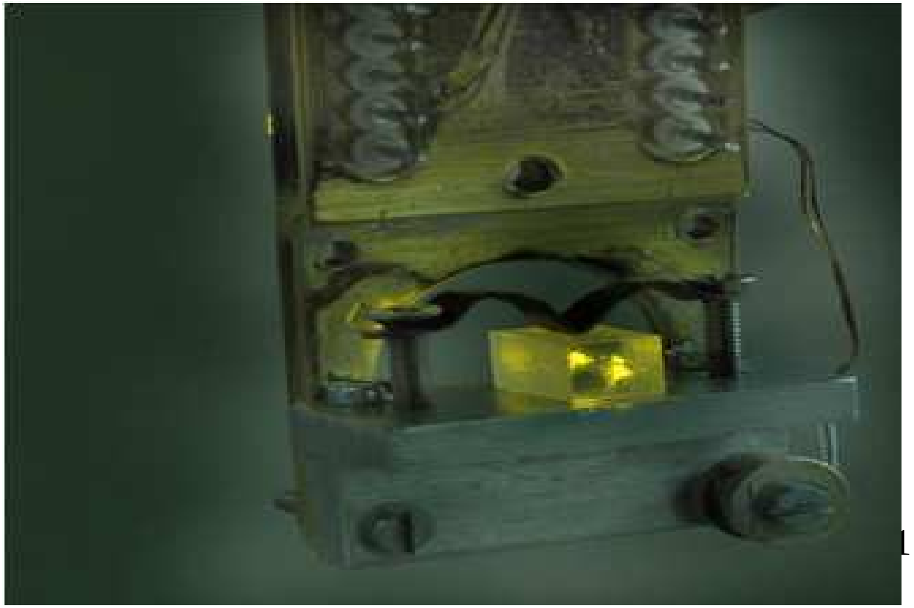
# Quantum memories for Quantum networks and device-Indep QKD

**Nicolas Gisin**
Group of Applied Physics
Geneva University, Switzerland

## 1. QKD

## 2. Quantum memories

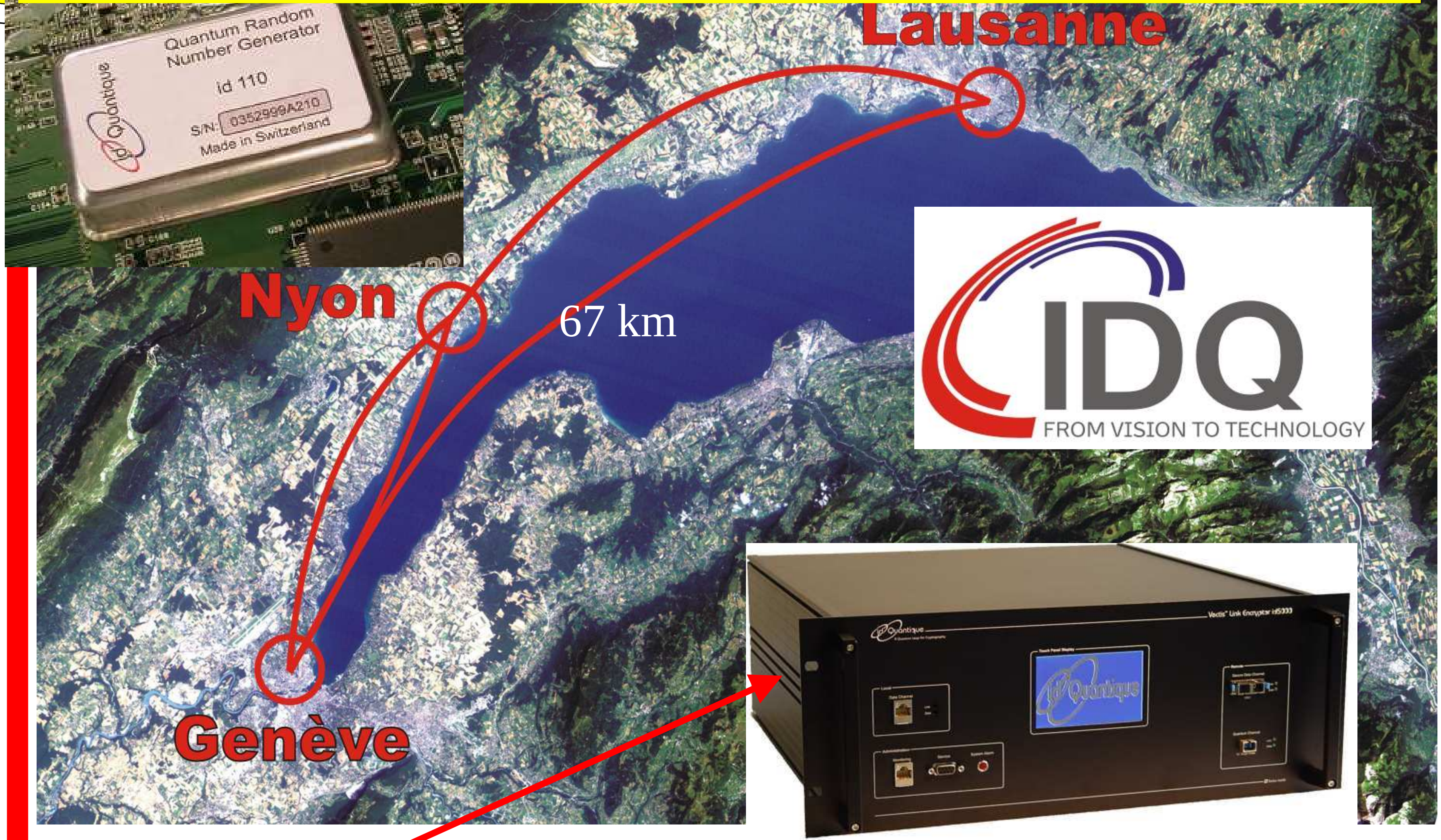


# Spin-off from the University of Geneva, 2001

**Industry Venture Session on Thursday 3.30 pm**

GAP Optique Geneva University




Used daily by some commercial customers

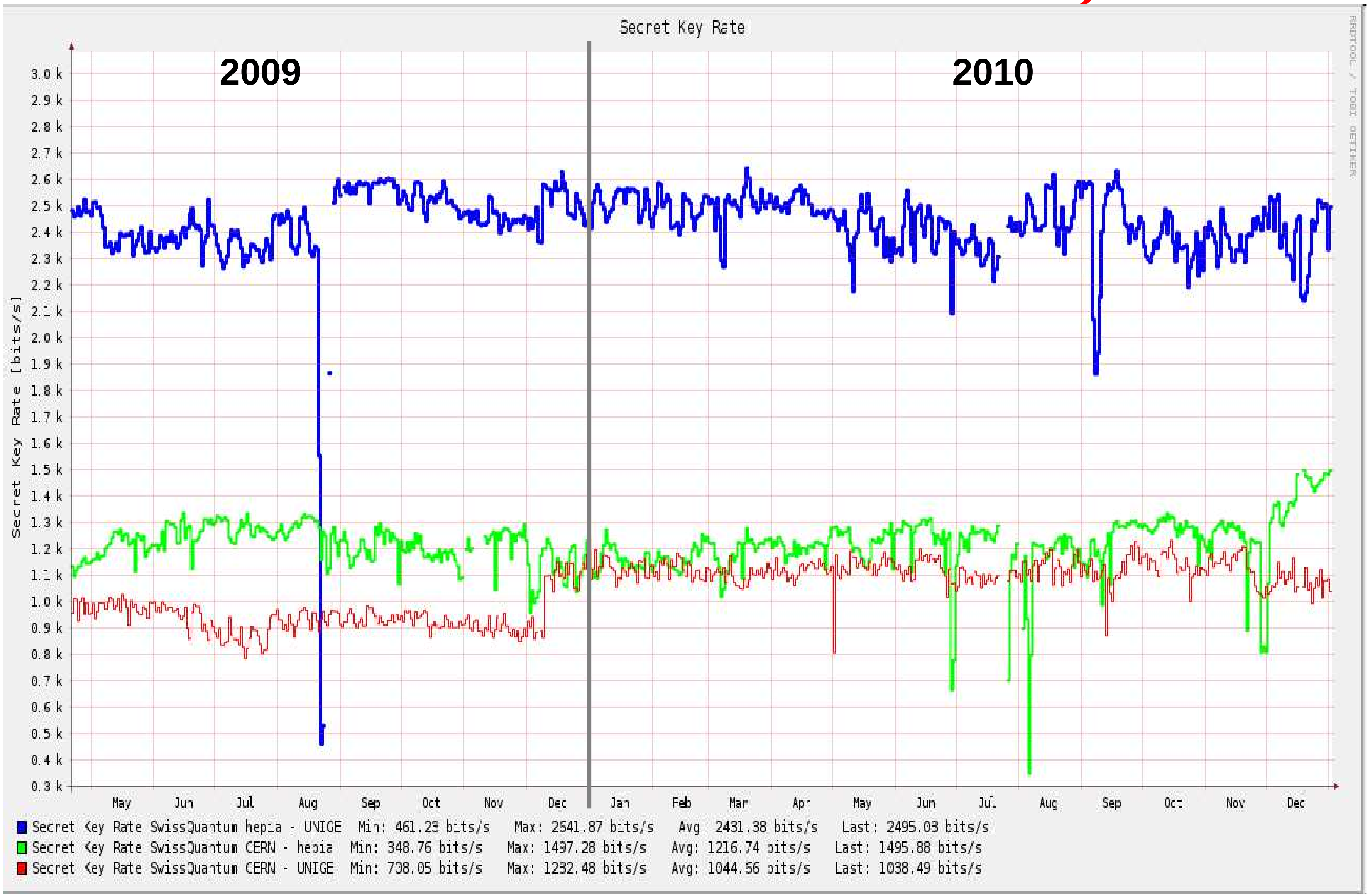
# Complete Solution


GAP Optique Geneva University

# Reliability: Swiss Quantum Network

**http://www.swissquantum.com**

**Run continuously during 20 months**
**Monitored by the University of Applied Science**




GAP Optique Geneva University

nature photonics

**Access**

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

nature.com > Journal home > Table of Contents

Letter

*Nature Photonics* **4**, 686 - 689 (2010)
Published online: 29 August 2010 | doi:10.1038/nphoton.2010.214

Subject Category: Quantum optics

Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen[1,2], Carlos Wiechers[3,4,5], Christoffer Wittmann[3,4], Dominique Elser[3,4], Johannes Skaar[1,2] & Vadim Makarov[1]

NTNU Norwegian University of Science and Technology

MPL

Friedrich-Alexander-Universität Erlangen-Nürnberg

IDQ FROM VISION TO TECHNOLOGY

**Press release**

# Vulnerability in commercial quantum cryptography tackled by international collaboration

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.**

# Quantum Hacking

1. *There is nothing like "unconditional security" !* (as emphasized in our 2002 RMP)
2. But it should not obscure the fact that *there is nothing like cracking QKD !*

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

In contrast, in classical crypto both the principle and the implementation can be attacked.

If the principle of classical crypto gets broken, then

- *All electronic money looses all value*
- *All past communications can be read*

# Device Independent Q Key Distribution
## Self-testing QKD

**Alice** | **Bob**

x=0 or 1 | y=0 or 1

**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 !**

*safe location, but untrusted equipment* | *safe location, but untrusted equipment*

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

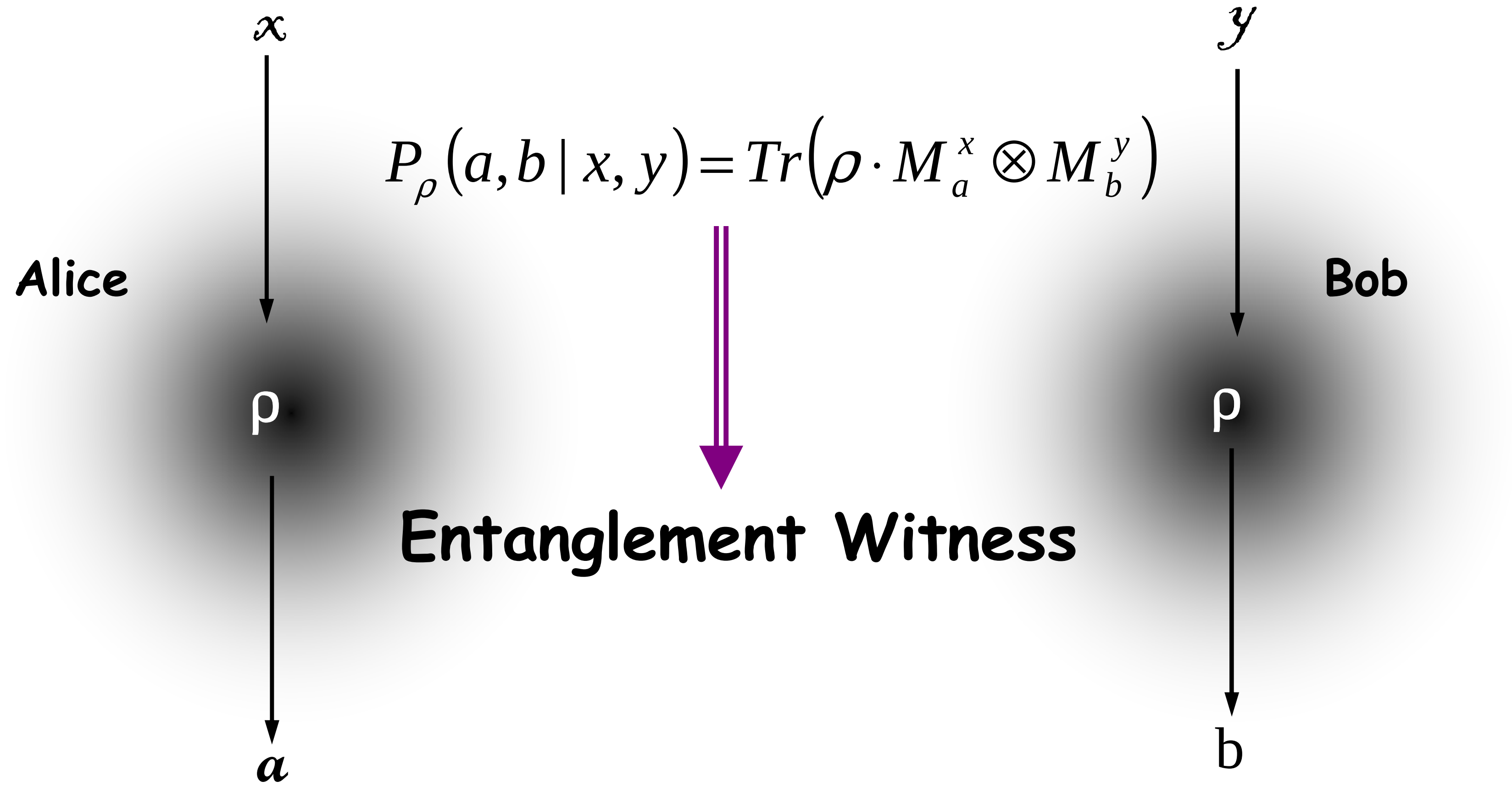
**p(a,b|x,y)**

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

# Another example of Device-Independent

ρ **is entangled** ⇔ ρ **not separable** ⇔ $\rho \neq \sum_j p_j \cdot \rho_A^j \otimes \rho_B^j$

$$P_\rho(a,b\,|\,x,y) = Tr\left(\rho \cdot M_a^x \otimes M_b^y\right)$$




**GAP Optique** **Geneva University**

# 3-party entanglement witnesses

$M = X_1 X_2 X_3 - X_1 Y_2 Y_3 - Y_1 X_2 Y_3 - Y_1 Y_2 X_3$

If $X = \sigma_x$ and $Y = \sigma_y$,
then $\langle\psi|M|\psi\rangle \leq 2$ for all biseparable $\psi = \psi_{AB} \otimes \psi_C$

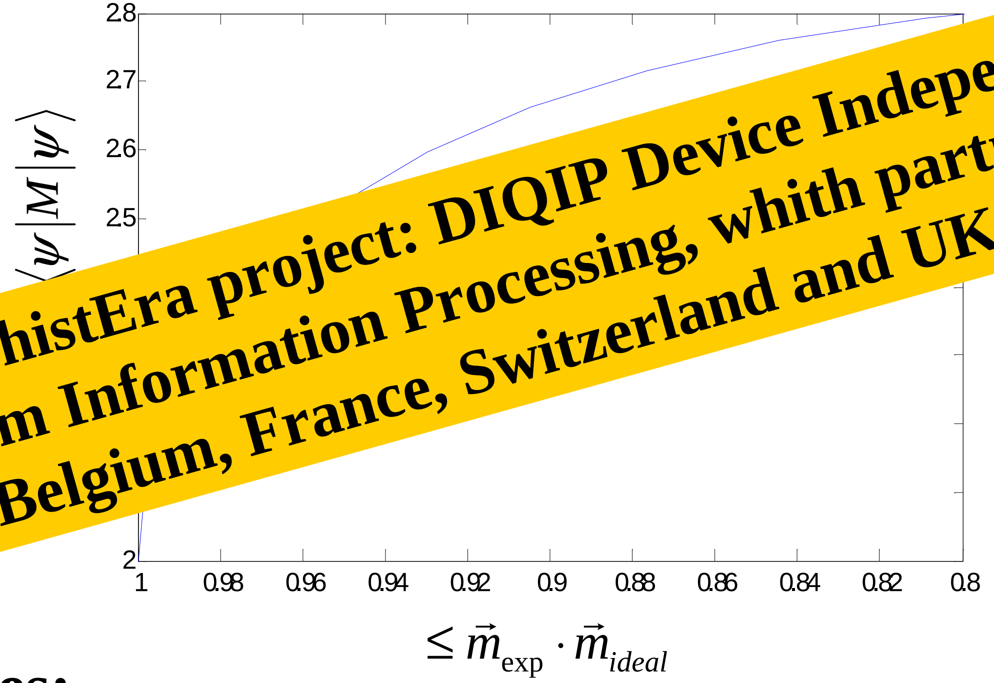
**But what if the settings are not perfectly under control:**
$X \approx \sigma_x$ and $Y \approx \sigma_y$ **?**

**But what if the measured $\langle M \rangle_\psi$ can be achieved with a biseparable state in dimension larger than 2?**
**$\Rightarrow$ The data can't be used for some quantum information tasks, like e.g. secret sharing.**

GAP Optique **Geneva University**

# 3-party entanglement witnesses

**A new ChistEra project: DIQIP Device Independent Quantum Information Processing, whith partners from Spain, Belgium, France, Switzerland and UK**

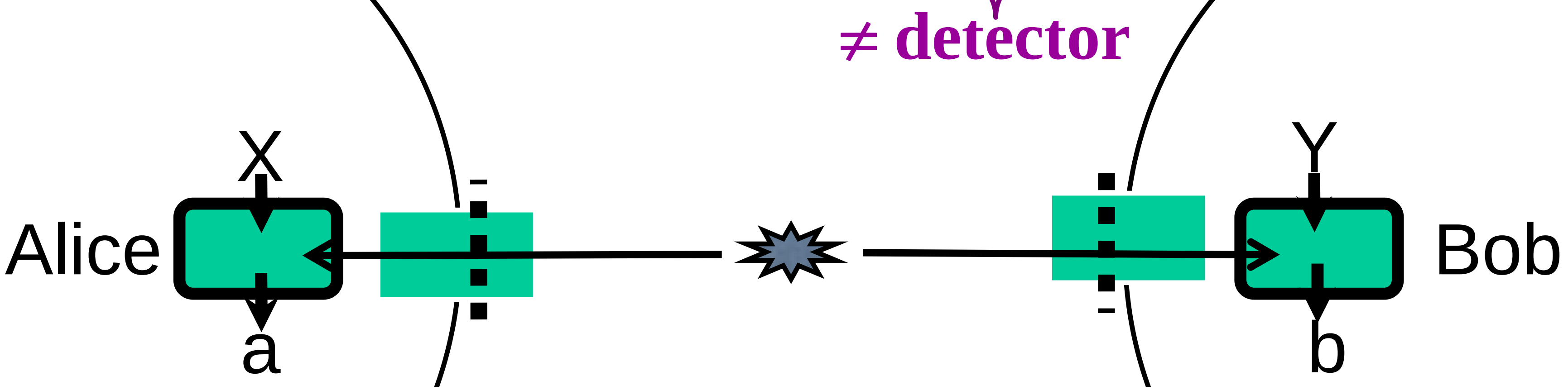



**<u>Two choices</u>:**

1. **Use device-independent entanglement witnesses (DIEWs) in a black-box scenario.** **Bancal et al., PRL <u>106</u>, 250404, 2011**
2. **Re-define entanglement witnesses with bounds that depend on the assumed experimental uncertainty: $\langle M \rangle_{\psi} \leq 2 + \mathrm{fct}(d, \text{experimental settings uncertainty})$**

# Bell violation guarantees entanglement independently of the devices !

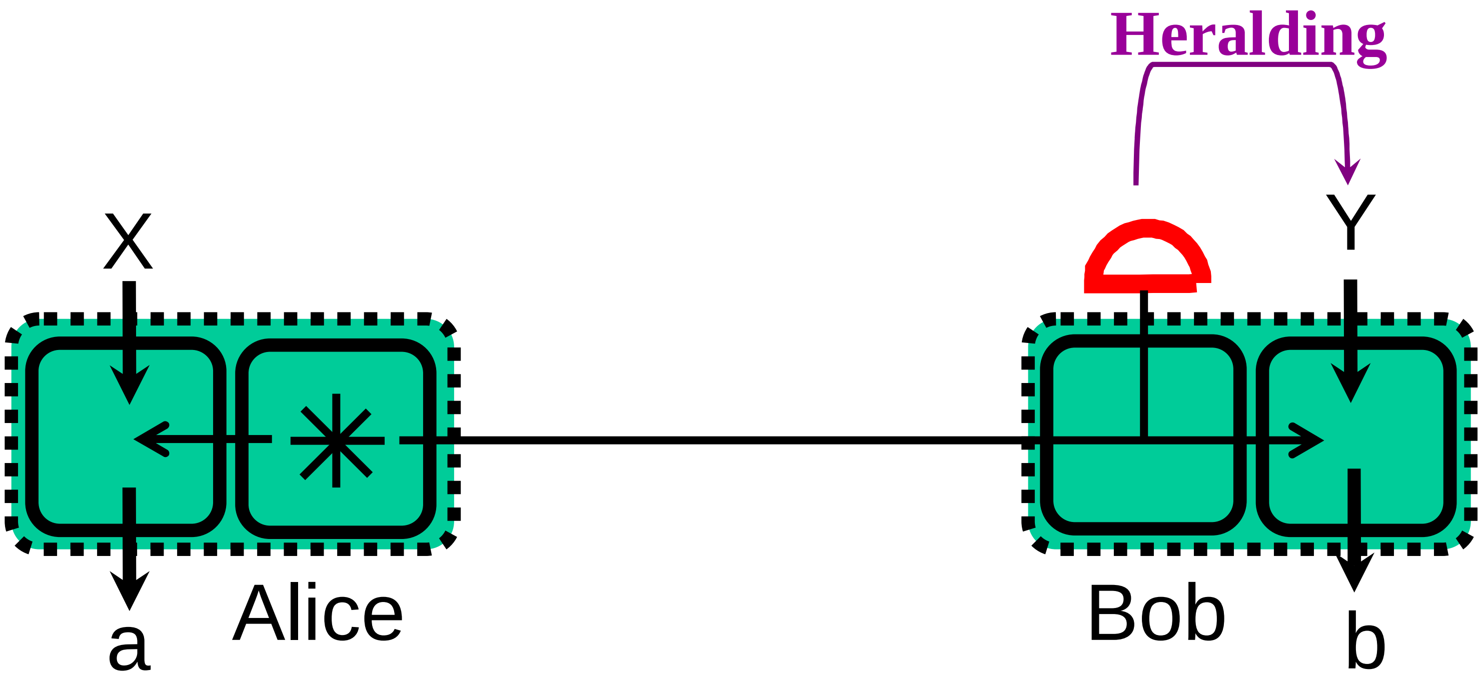
**Beautiful idea** ... but
it is crucial to close the detection loophole!




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 !!!**

# To overcome the transmission losses :
# Heralded signal

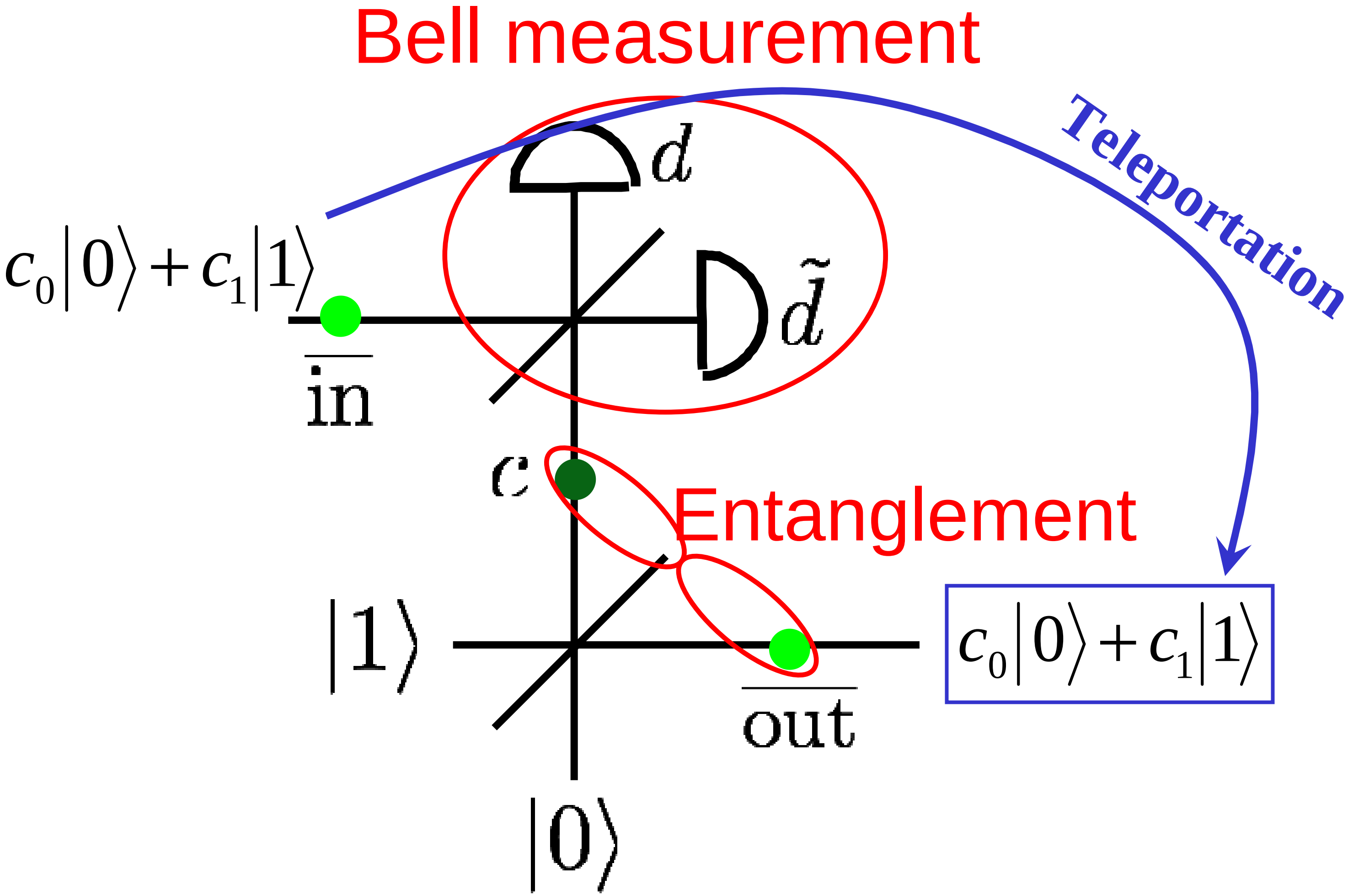



**NG, S. Pironio & N. Sangouard, PRL 105, 070501 (2010)**

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

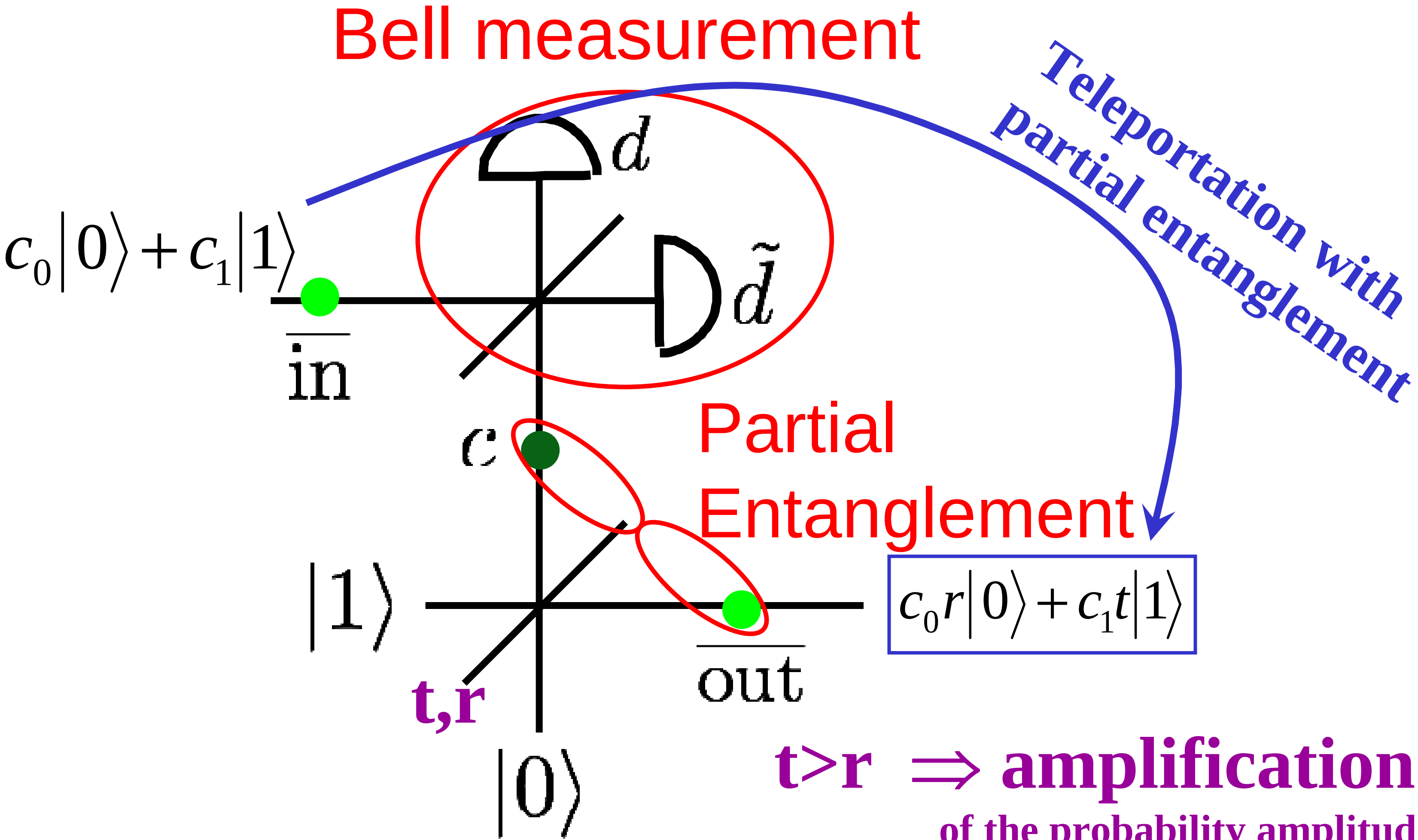
**T.C. Ralph & A.P. Lund, arXiv:0809.0326**

# « Photon Amplifier »




T.C. Ralph & A.P.Lund, arXiv:0809.0326; Ferreyrol F. et al. (Grangier), arXiv:0912.2065

# « Photon Amplifier »




**t>r ⇒ amplification**

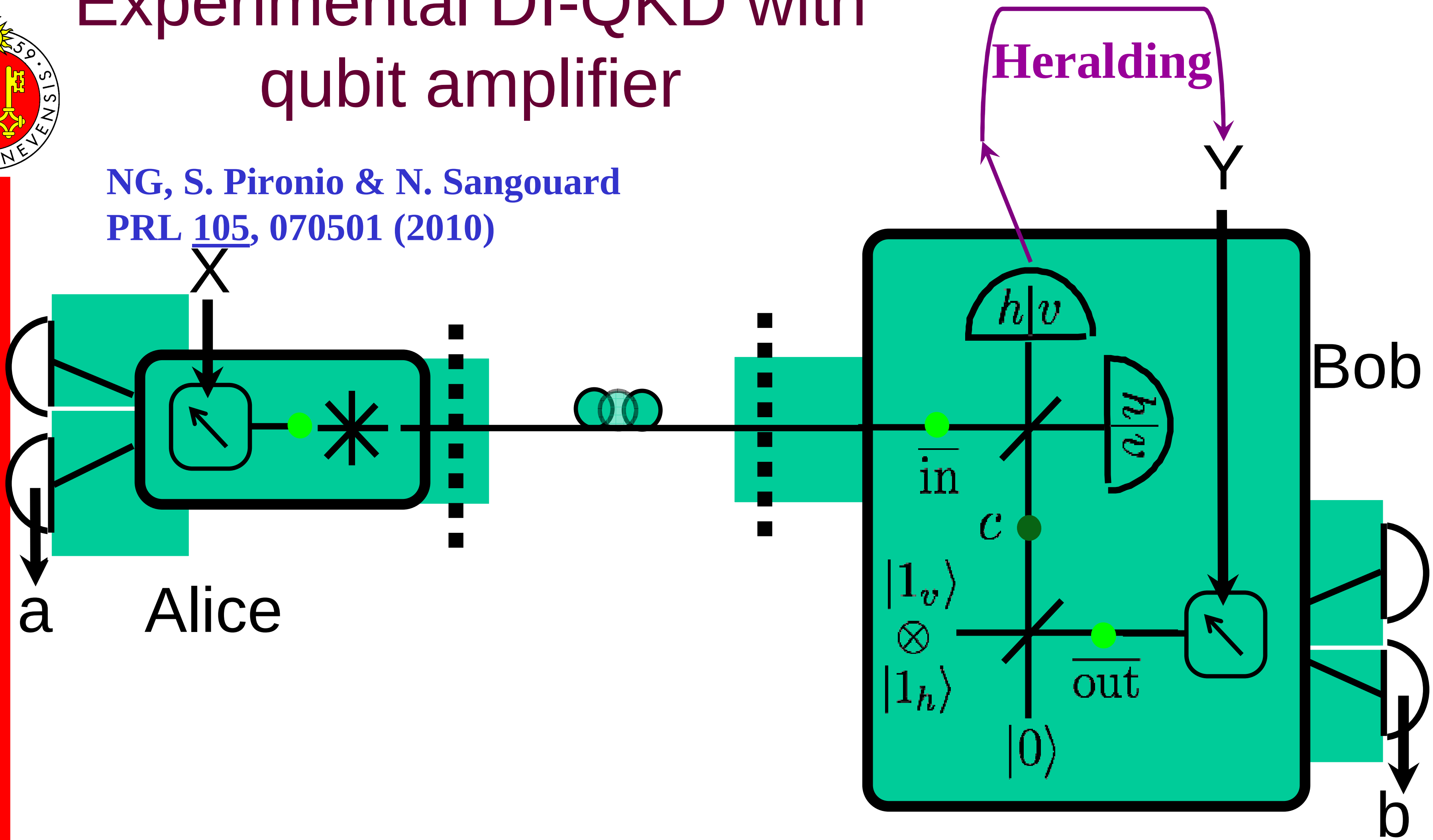
**of the probability amplitude that a photon is present**

**T.C. Ralph & A.P.Lund, arXiv:0809.0326; Ferreyrol F. et al. (Grangier), arXiv:0912.2065**

# Experimental DI-QKD with qubit amplifier

**NG, S. Pironio & N. Sangouard**

**PRL 105, 070501 (2010)**

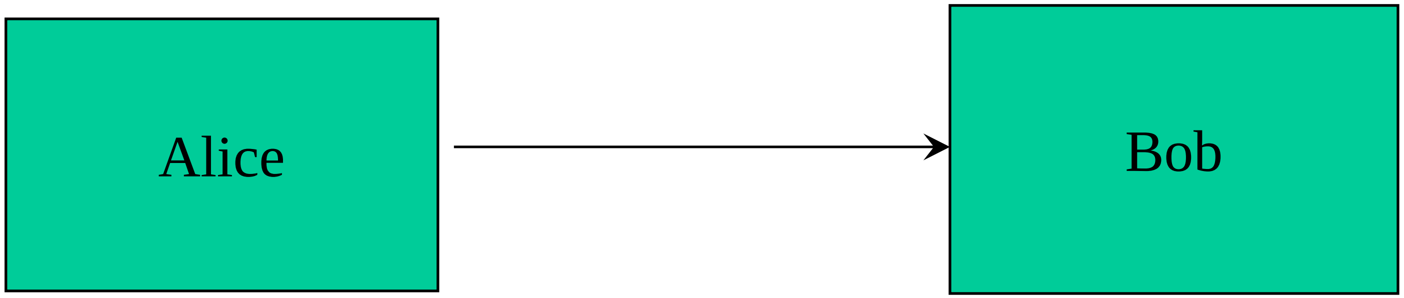



**Each individual step has already been demonstrated, though with close-but-yet-insufficient specs.**

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

# Back to "standard" QKD: quantum engineering feeds back to theory

## Higher bit rates & longer distances




bit rate at emission
goal: > 1 Gbit/s

channel
loss

« no » loss in
Bob's
optics

Efficient
detector

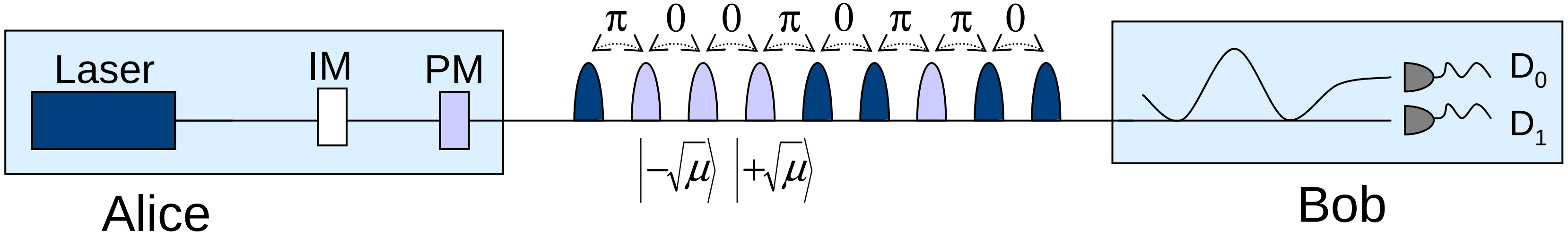
+ noise ⇒ secret bit rate
goal: > 1 Mbit/s

# Examples of practical protocols

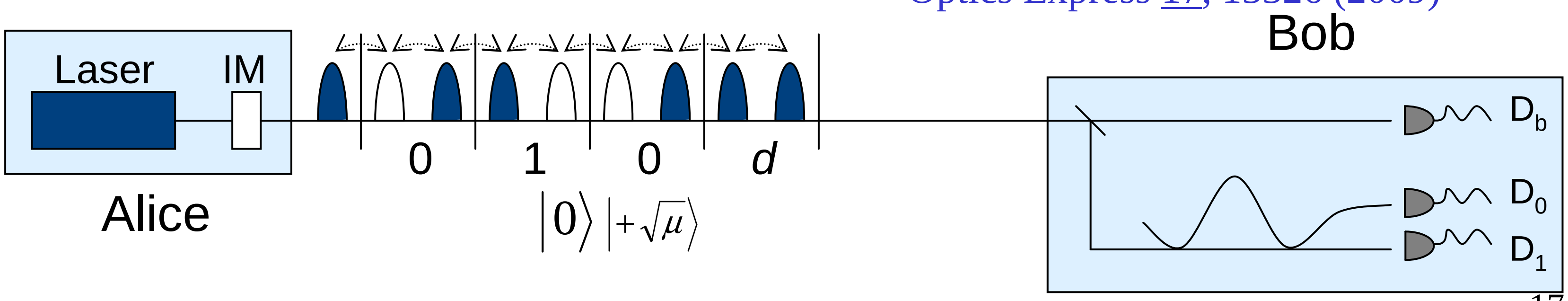
***Common feature: bits are not coded in qubits***

**This is quantum engineering, but raises the long standing open problem "how to analyse QKD security when the bit string can't be decomposed into many subsystems?"**

- DPS: Differential Phase Shift Phys. Rev. Lett. 89, 037902 (2002).

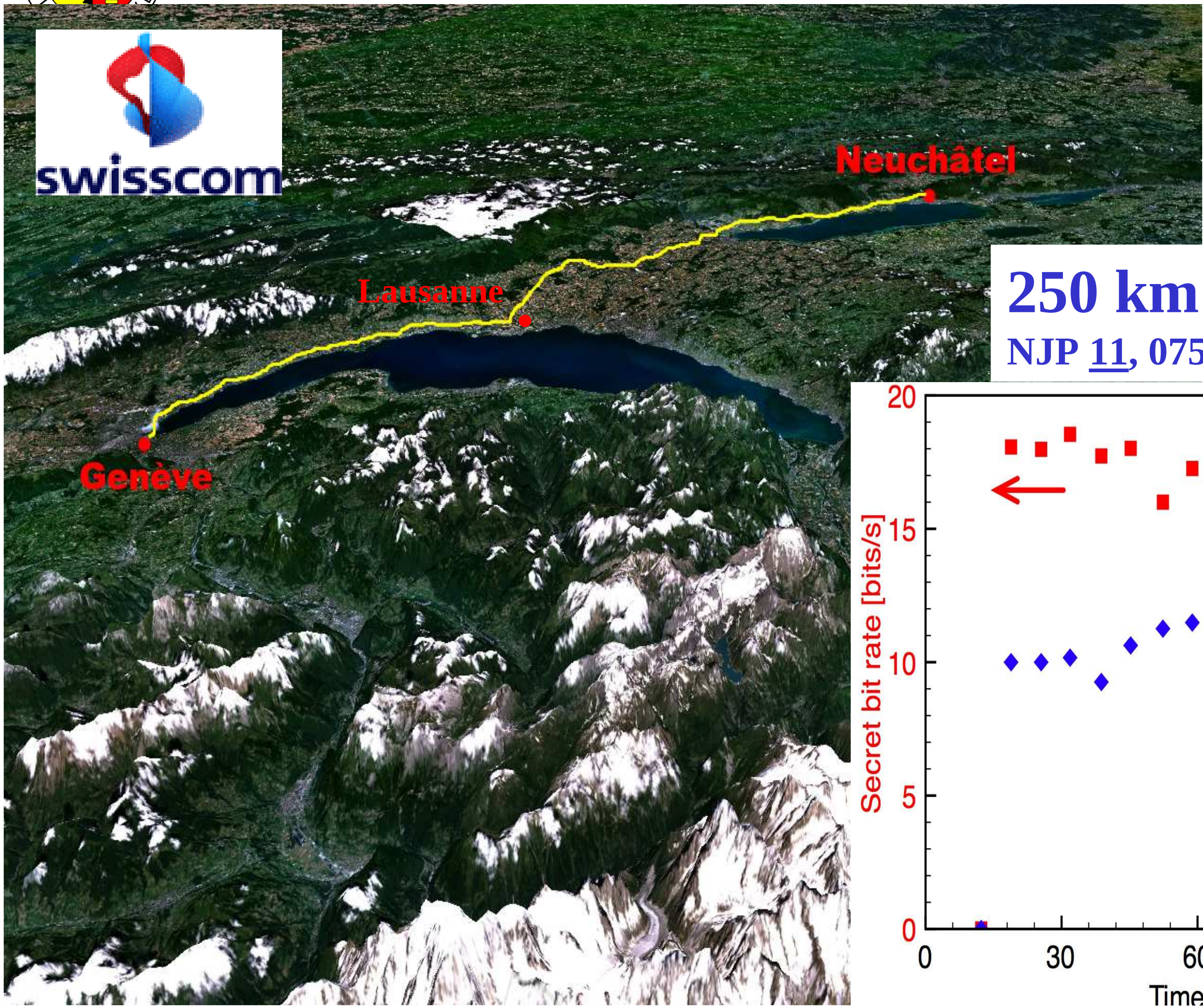



- COW: Coherent One-Way APL 87, 194105 (2005) Optics Express 17, 13326 (2009)



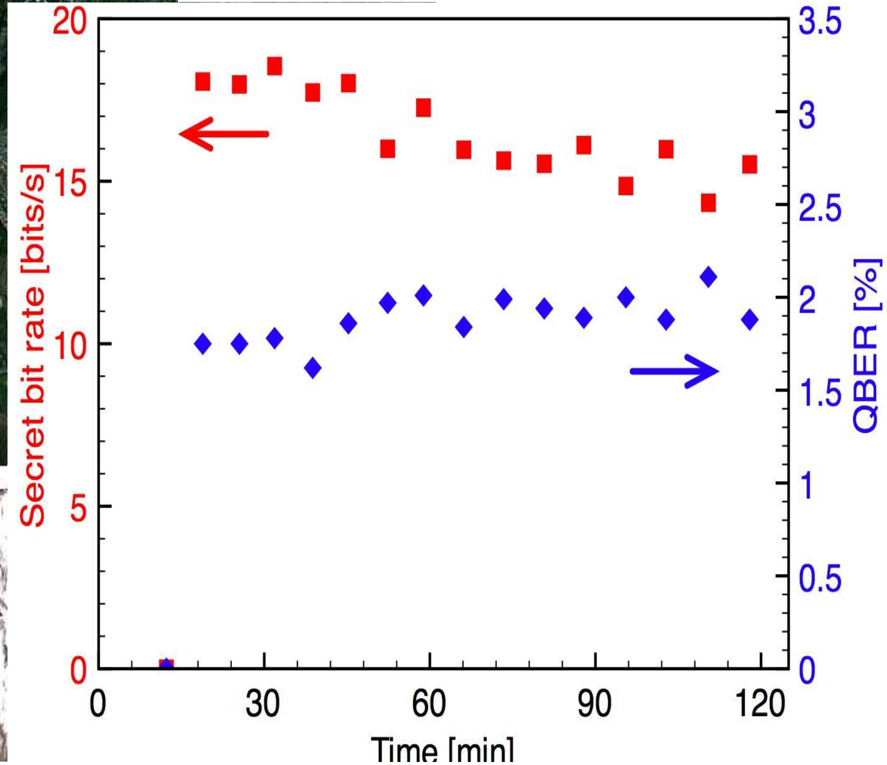
# Long distance QKD: World records

**150 km of installed fibers**, **Optics Express <u>17</u>, 13326 (2009)**

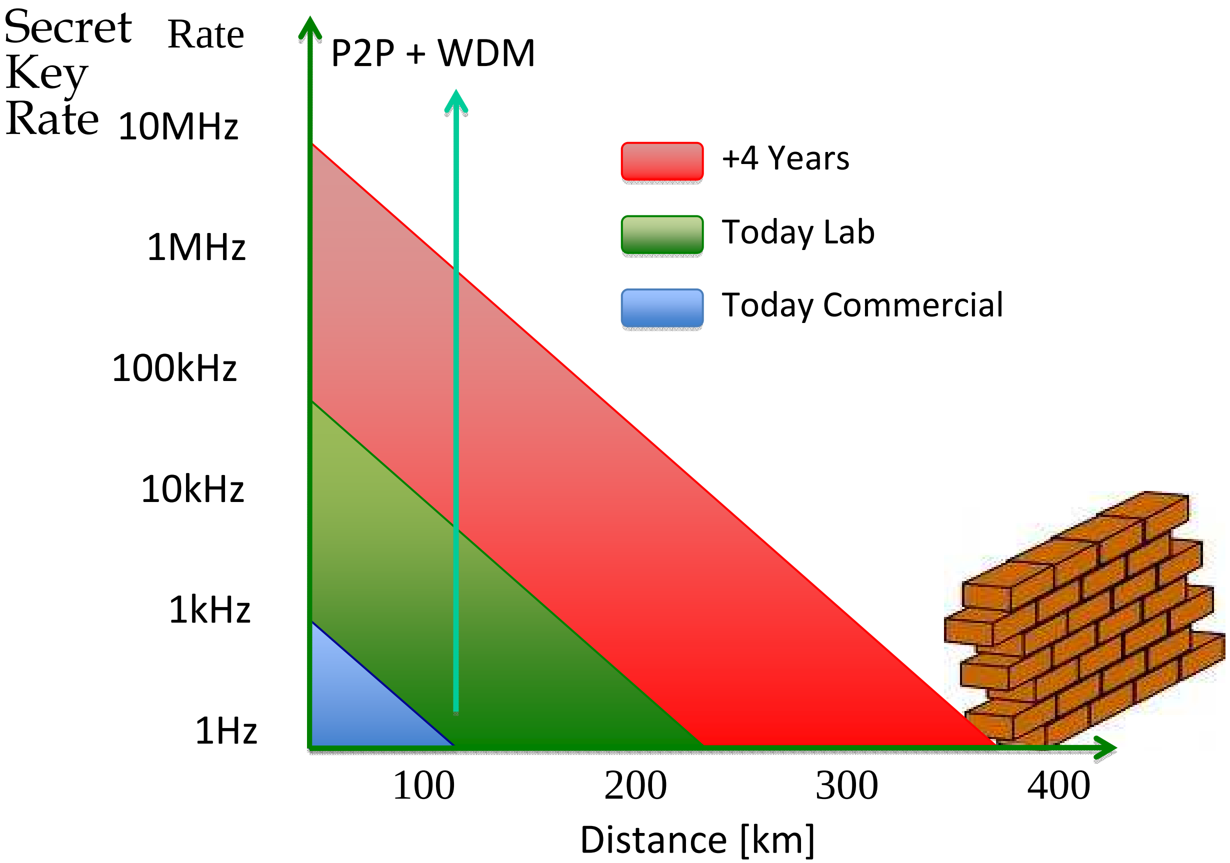



**250 km in the lab.**

**NJP <u>11</u>, 075003 (2009)**



# How far can one send a photon ?

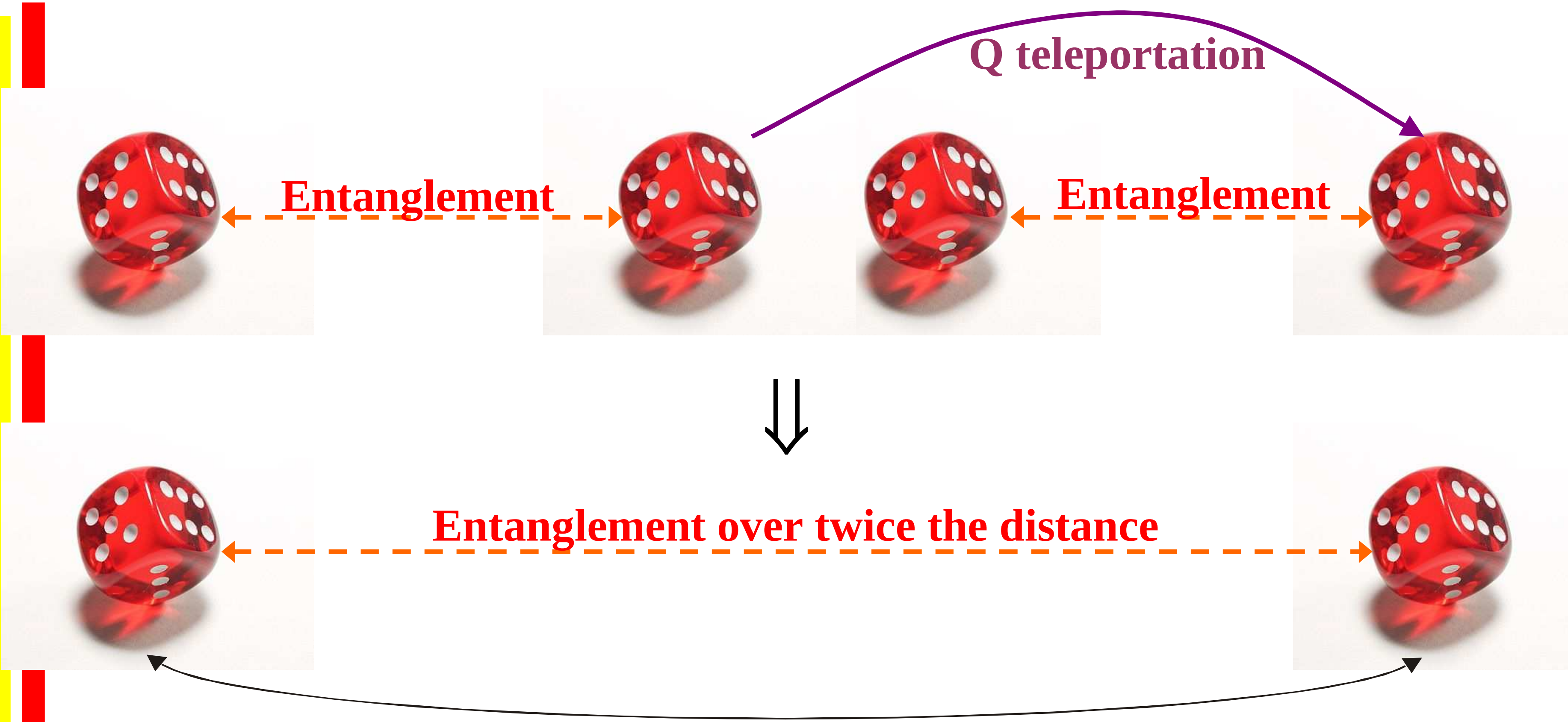



*There is a hard wall around 400 km !*

**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 Optique Geneva University

# Beating the hard wall: Teleportation of entanglement



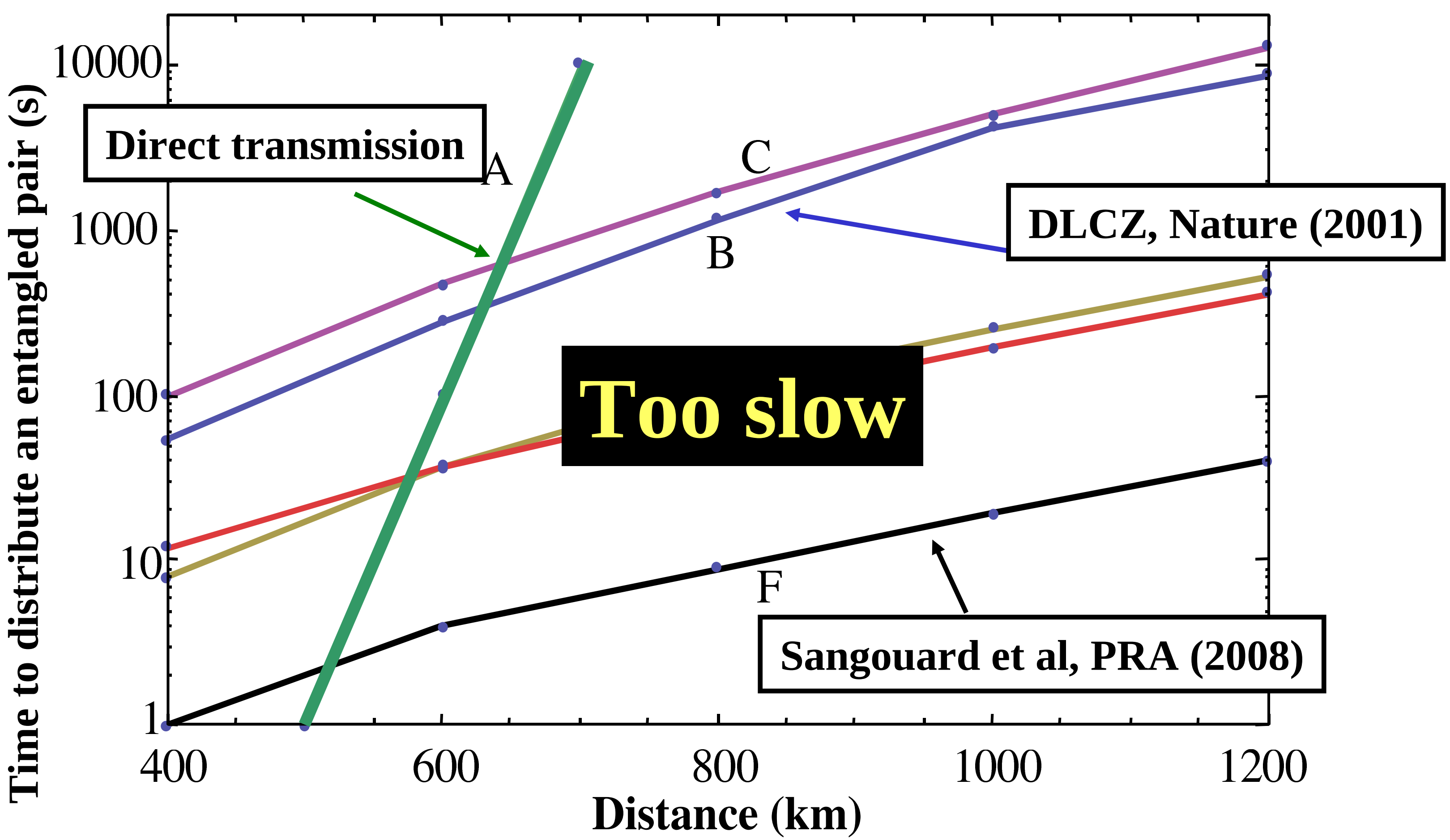

**Entanglement between photons that never interacted**

**PRA 71, 05302, 2005**

# How far can one send a photon ?

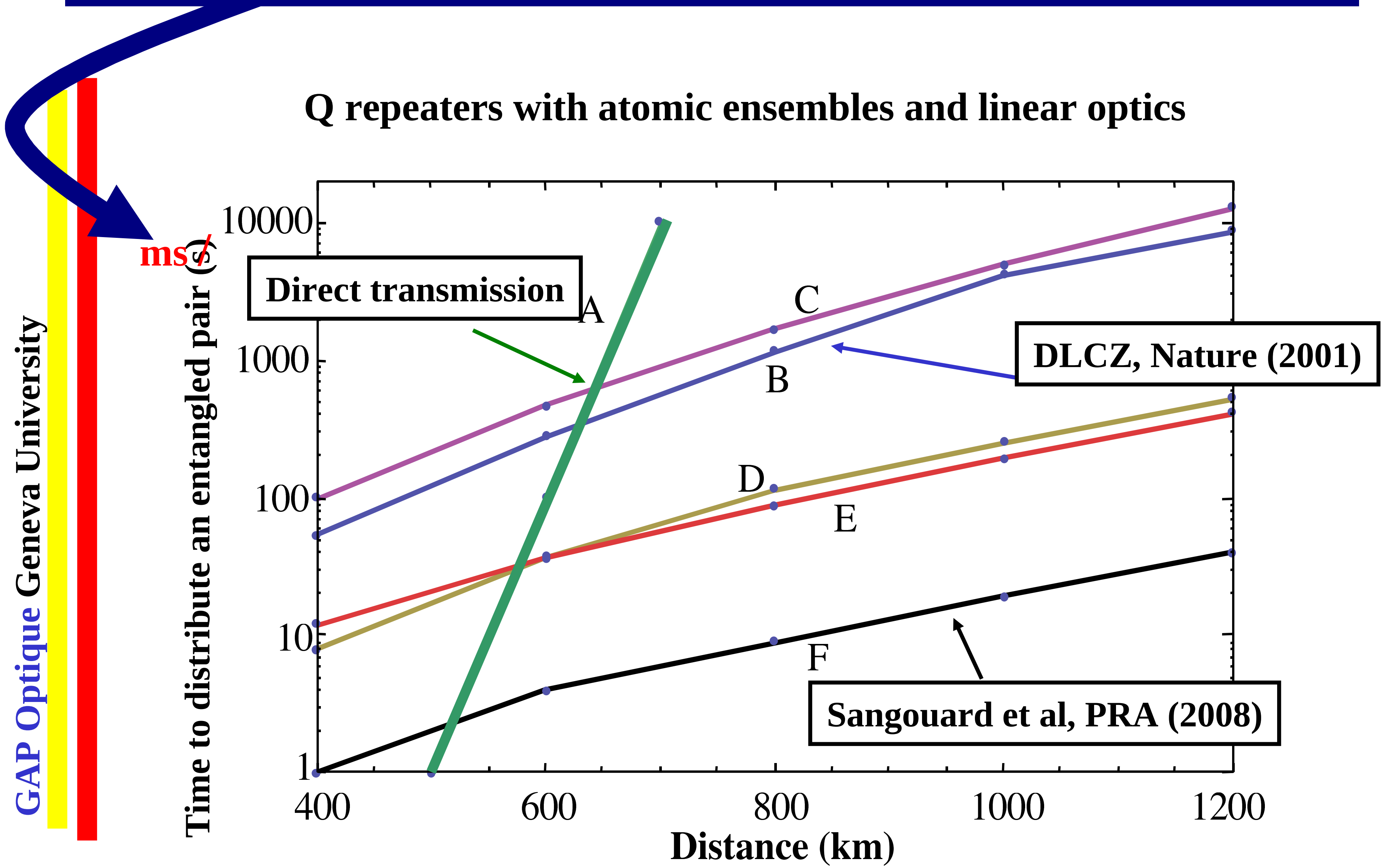
GAP Optique Geneva University

**Q repeaters with atomic ensembles and linear optics**



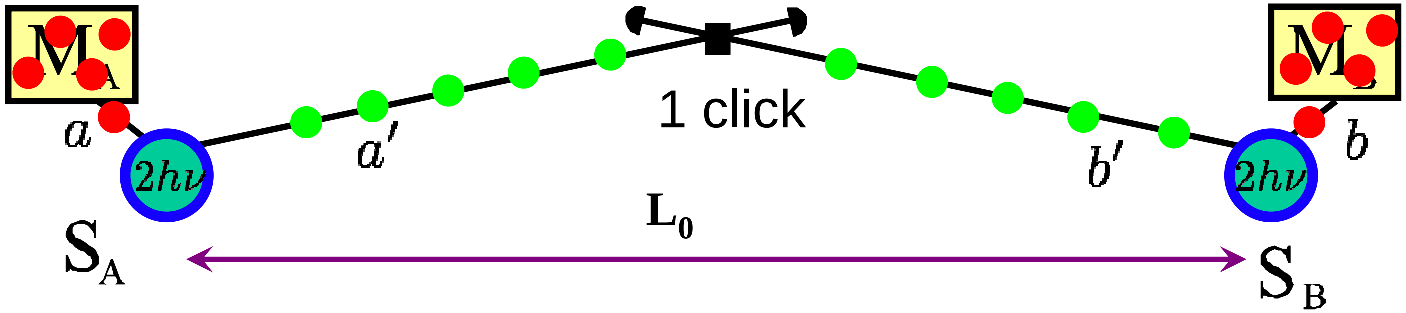
**Storing N modes in <u>ONE</u> memory using <u>*time*</u>, spatial or frequency multiplexing will reduce this time with a factor N**

## Q repeaters with atomic ensembles and linear optics




GAP Optique Geneva University

# Increasing $P_0$ using multi-mode memories




Conventional memory: have to wait time $L_0/c$ before trying again. (Ex. For 100 km, $L_0/c$=500 μs, R=2 kHz)

$$P_0 = p\eta_{L_0}\eta_D$$

Low success probability! (Typ. $10^{-3}$ - $10^{-4}$)

Memories that can store *N* temporal modes.

*N* attempts per time interval $L_0/c$

$$P_0^{(N)} = 1-(1-P_0^{(1)})^N \approx N P_0^{(1)}$$

***(N > 100 possible)***

Speedup by factor of *N.*


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


**GAP Optique** **Geneva University**

# Requirements for Quantum Repeaters

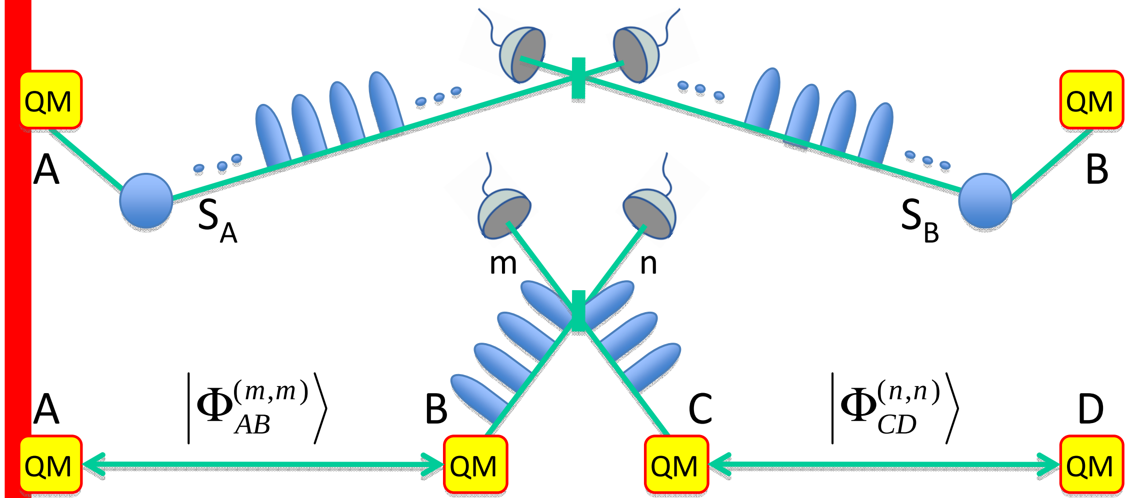
1. **Distribution of entanglement over long distances**
2. **Multi-mode quantum memories**
3. **Entanglement swapping @ telecom λ**

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

# Quantum Repeaters for Long Distance Fibre-Based Quantum Communication

**2010 – 2012 : 2 M€**

GAP **Optique** Geneva University



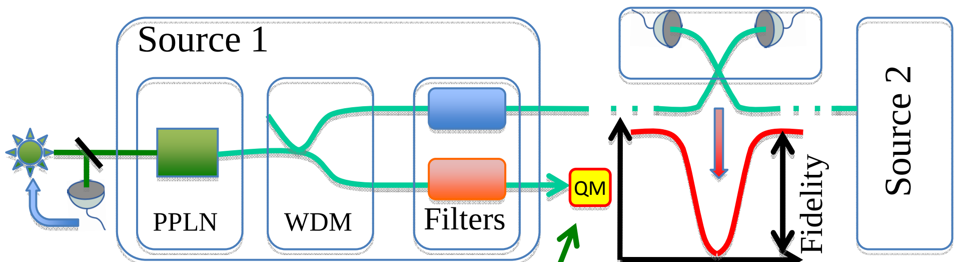

The goal of QuReP is to develop a Quantum Repeater - the elementary building block required to overcome current distance limitations for long-distance quantum communication.

Switzerland: - Université de Genève
- ID Quantique SA

Sweden: - Lunds Universitet

France: - Laboratoire Aimé Cotton
- Laboratoire de Chimie de la Matière Condensée de Paris
- Université Pierre et Marie Curie

Germany: - Universität Paderborn, DE




Integrated Photon pair sources

High Fidelity BSMs

Multi-Mode Q Memories Rare-Earth Ion Doped Solids

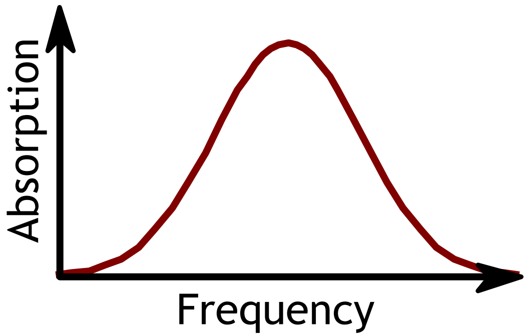
Multiple Systems

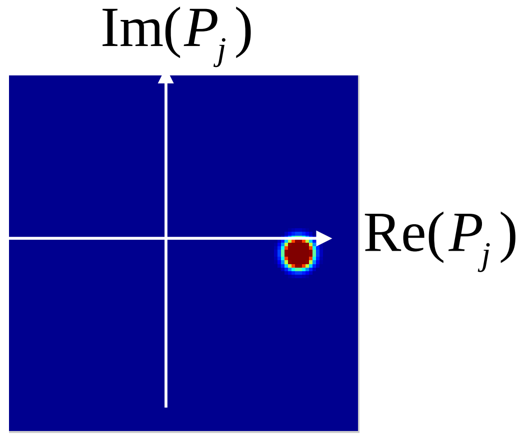
http://quantumrepeaters.eu

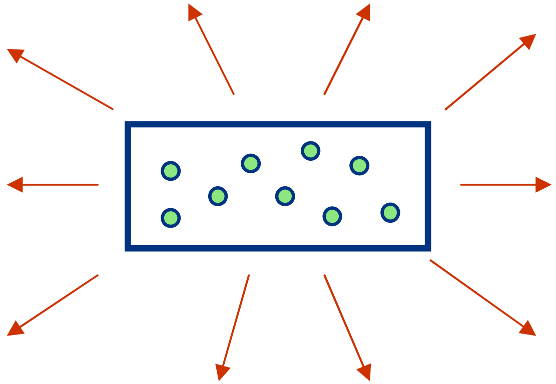
# Controlling the Dephasing! Atomic Frequency Comb

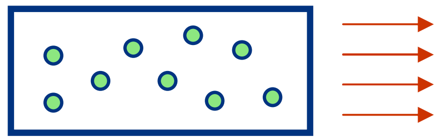
$$\sum_{j=1}^{N} e^{ikr_j} e^{-i\delta_j t} \left| g_1 \ldots e_j \ldots g_N \right\rangle \qquad P_j = e^{-i\delta_j t}$$

$\Delta$ continuous $\Rightarrow$ Dephasing



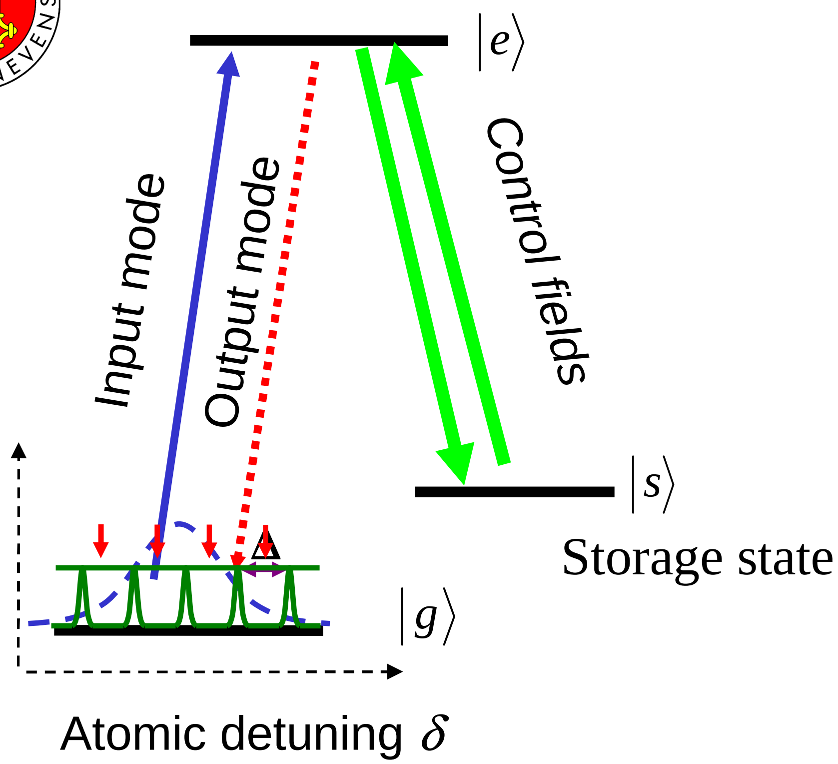





GAP Optique Geneva University

# Atomic Frequency Comb (AFC) Quantum Memory

Ensemble of inhomogeneously broadened atoms




State after absorption
**(superradiant Dicke state)**

$$\sum_{k=1}^{N} c_k |g_1 g_2 ... e_k ... g_N\rangle$$

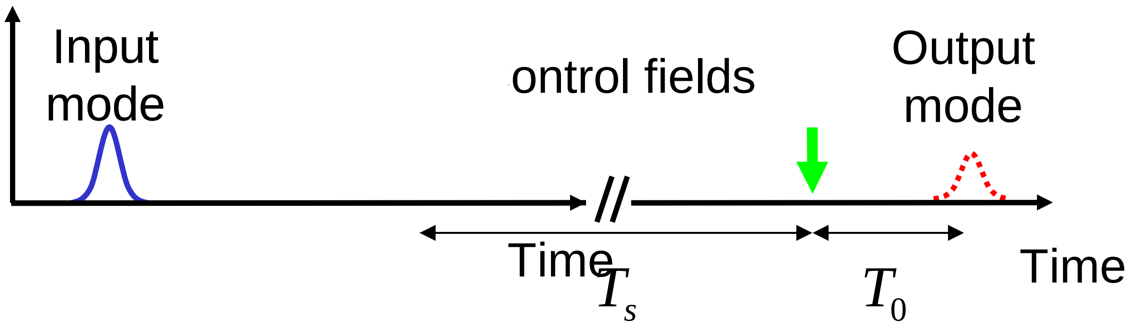
Dephasing

$$\sum_{k=1}^{N} c_k e^{-i\delta_k t} |g_1 g_2 ... e_k ... g_N\rangle$$

$$\delta_k = m_k \Delta$$

Periodic structure =>
Rephasing after a time

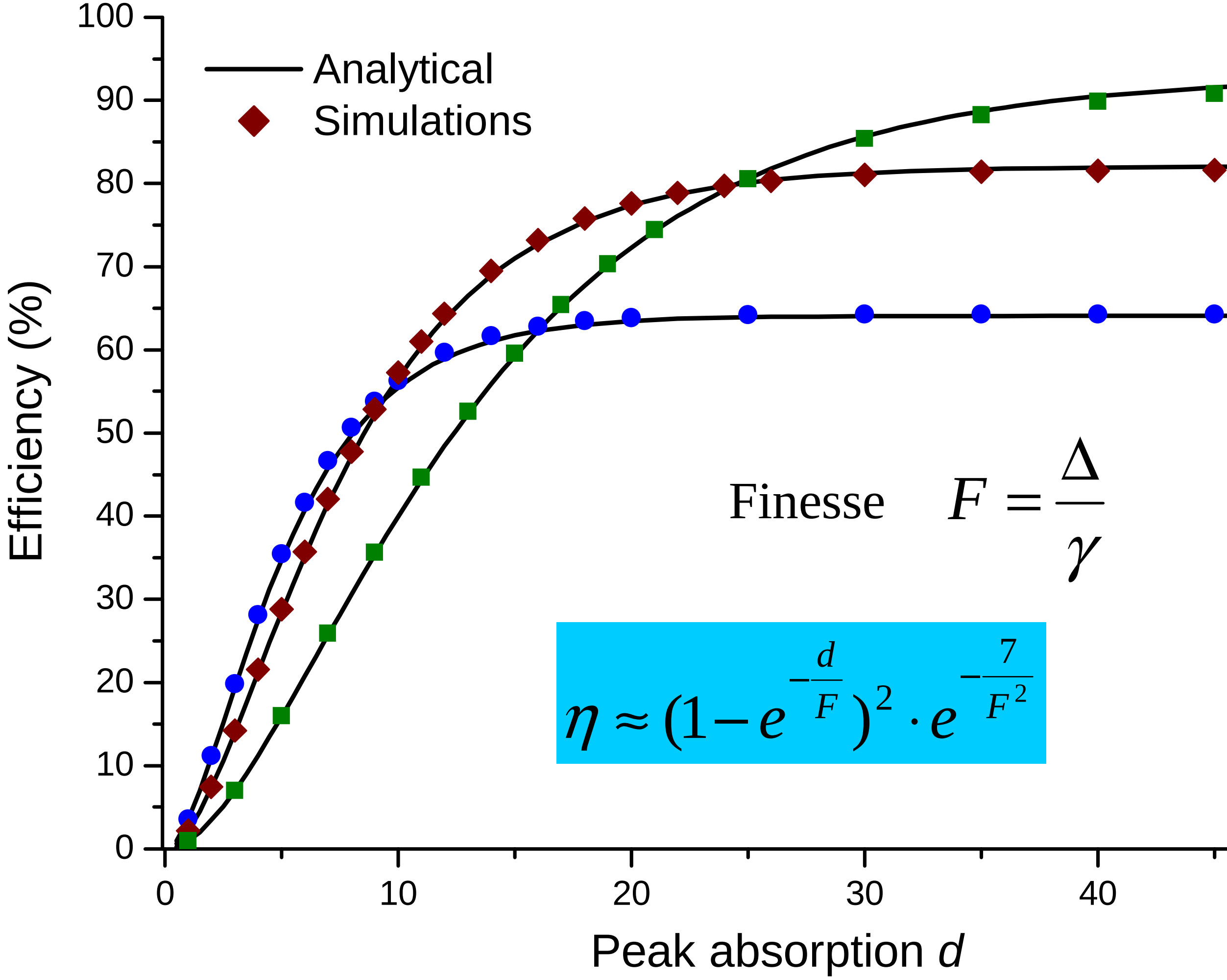
$$t_e = \frac{2\pi}{\Delta}$$




Collective emission in the forward BACKWARD Photon echo like emission

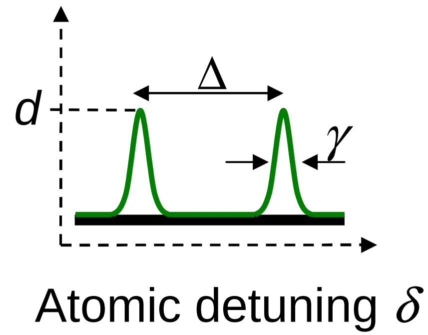
**M.Afzelius, C.Simon, H. de Riedmatten and N.Gisin, Phys Rev A 79, 052329 (2009)**

# Efficiency vs optical depth (theory)




Finesse $F = \frac{\Delta}{\gamma}$

$$\eta \approx \left(1 - e^{-\frac{d}{F}}\right)^2 \cdot e^{-\frac{7}{F^2}}$$




GAP Optique Geneva University

M.Afzelius, C.Simon, H. de Riedmatten and N.Gisin, Phys Rev A 79, 052329 (2009)

# Time multiplexing (multi-mode)



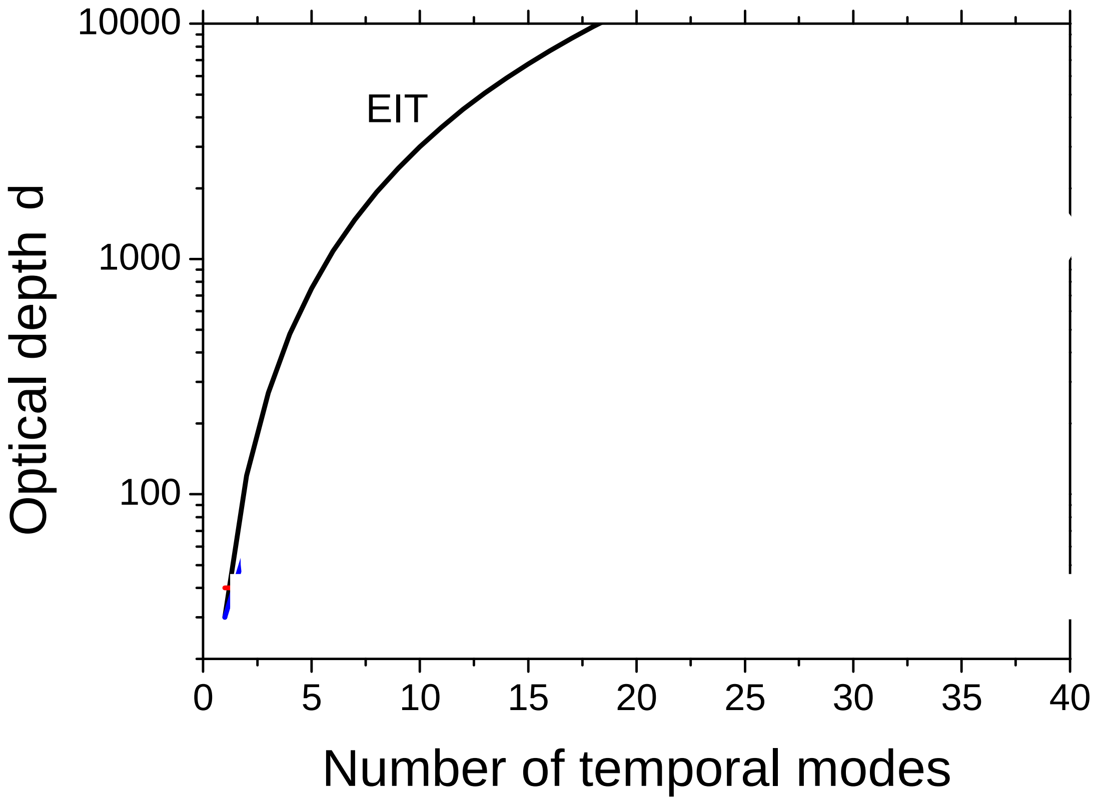
- **EIT based memory (stopped light)** $d \propto N^2$

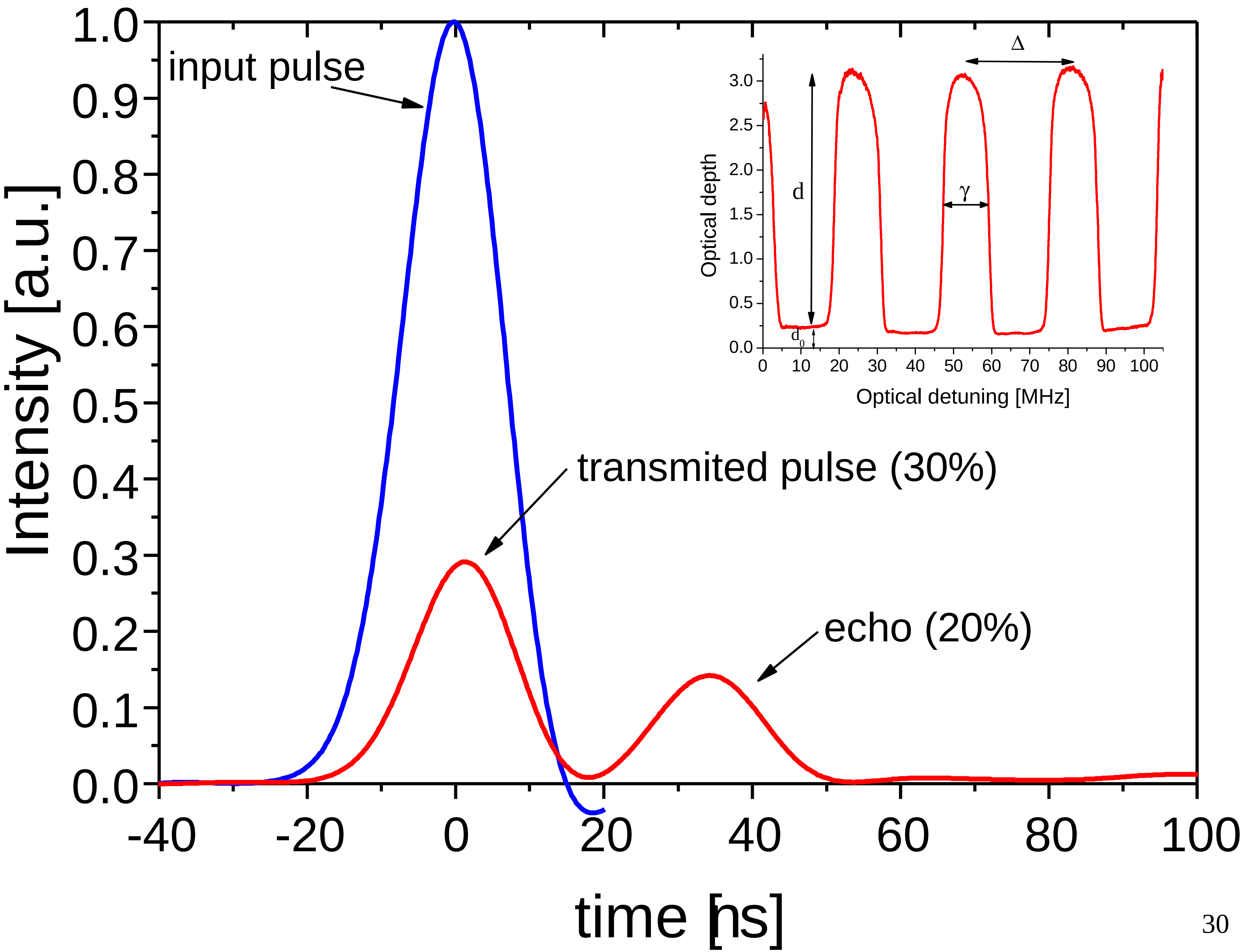
J. Nunn et al, arXiv:0807.1250 (2008)

- **Controlled Reversible Inhomogeneous Broadening (CRIB) based memory** $d = 30 \cdot N$

C. Simon et al, PRL 98, 190503 (2007), J. Nunn et al, arXiv:0807.1250 (2008)

- **AFC based memory** **d independent of N**





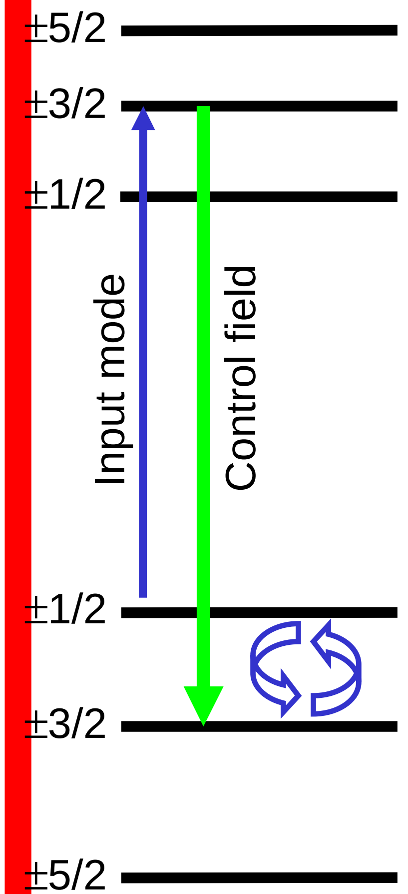

GAP Optique Geneva University

# AFC storage experiment in $Pr^{3+}:Y_2SiO_5$

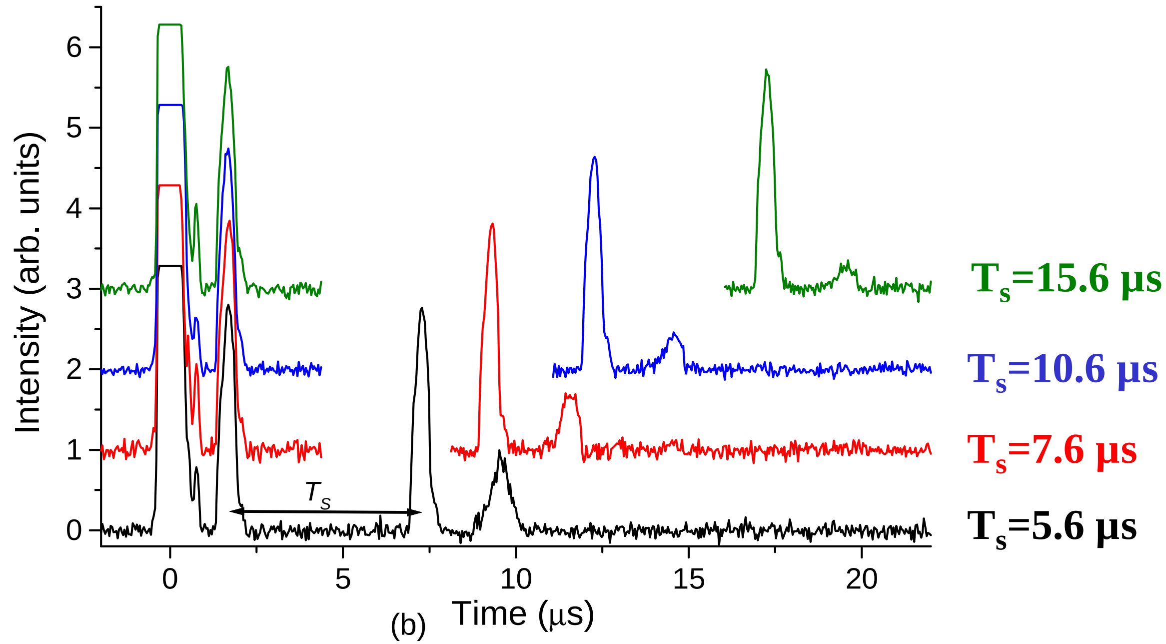
**Geneva-Lund collaboration**

**PRL <u>104</u>, 040503, 2010**

**GAP Optique Geneva University**



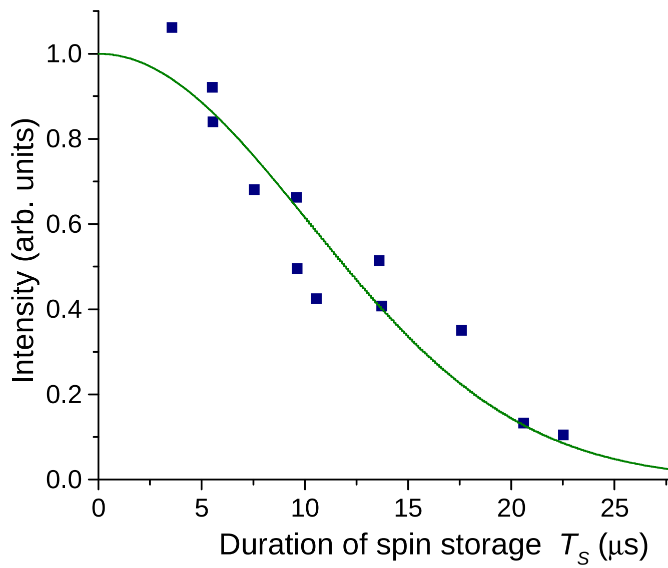

(a)




*Decay of coherence due to inhomogeneous spin dephasing.*

*Fitted spin distribution Gaussian FWHM: 26 kHz*

(b)

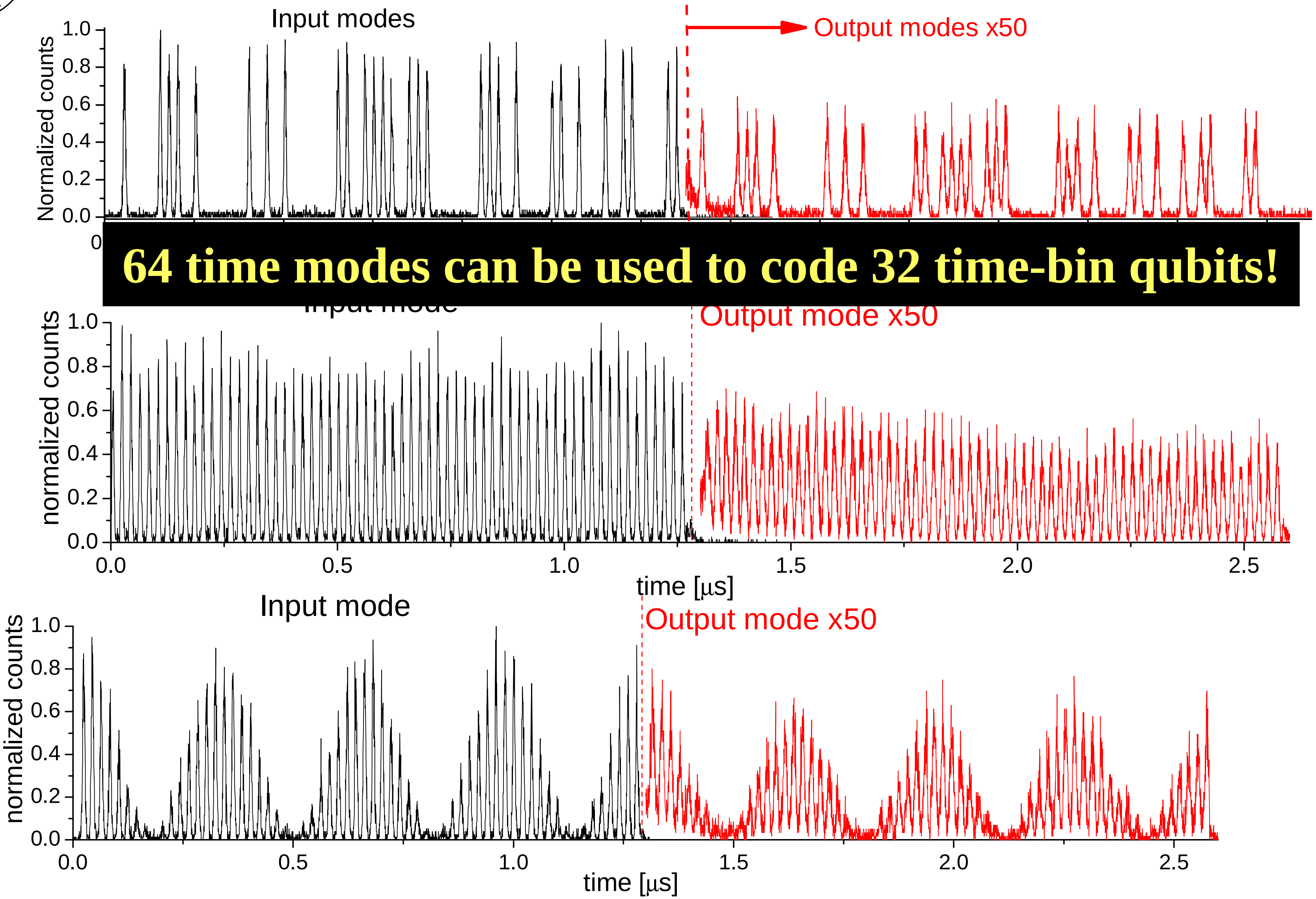



**Solution: Spin echo ⇒ 1 s spin coherence !**

# Multi-mode storage in $Nd^{3+}:Y_2SiO_5$

⟨n⟩ < 1 per mode

**Mapping 64 input modes onto _one_ crystal**



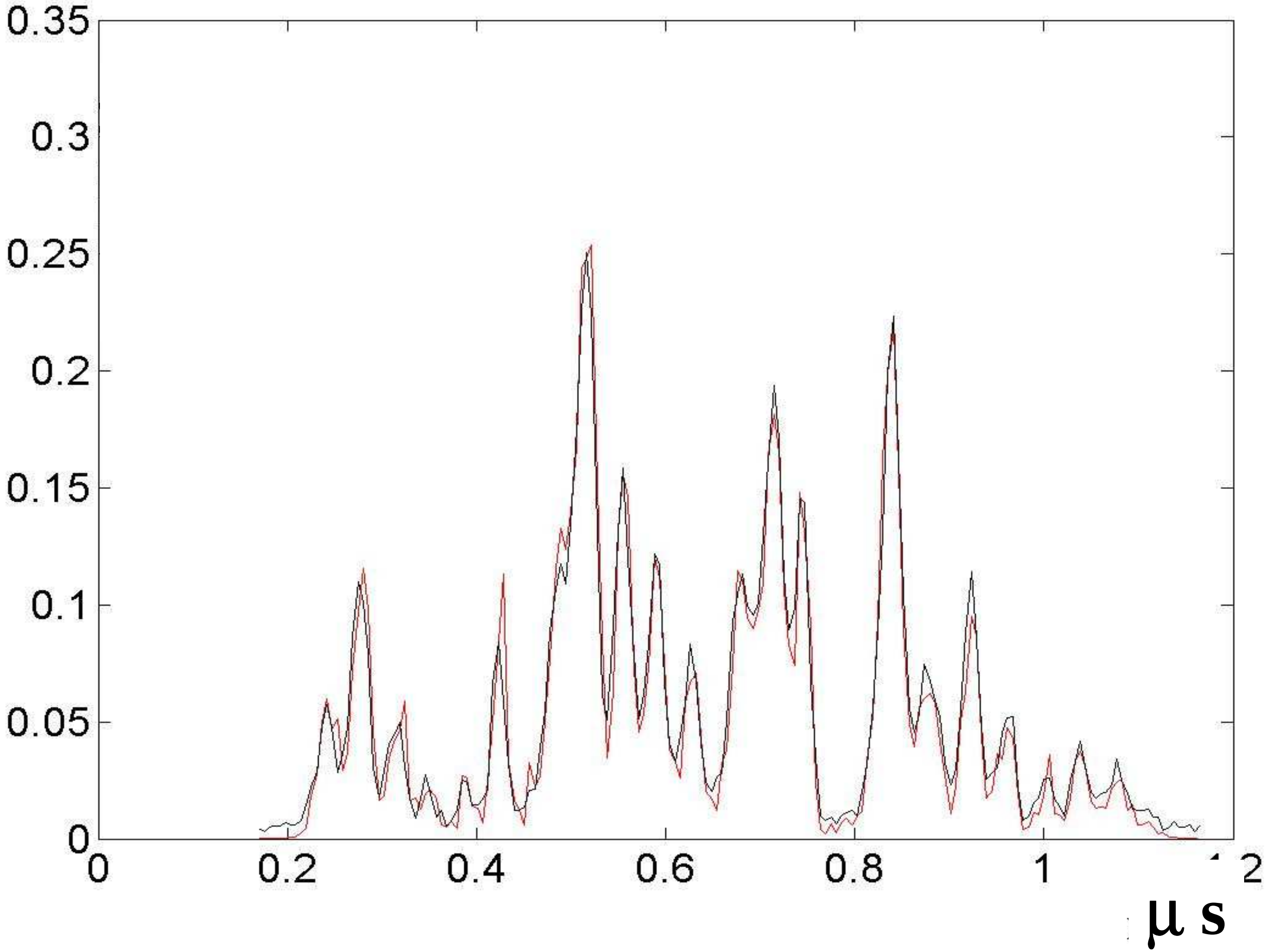

**64 time modes can be used to code 32 time-bin qubits!**

GAP Optique Geneva University

**I. Usmani et al., Nature Communications 1,12 (2010)**

# Storage of arbitrary waveform (Nd:YSO)

Overlap between input and output

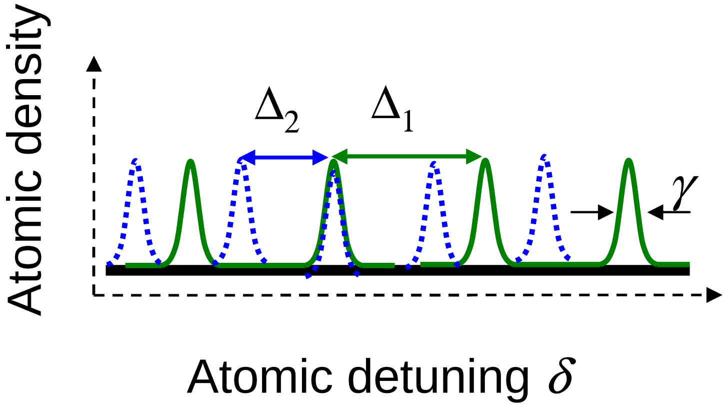



I. Usmani et al., Nature Communications, 1:12, 2010

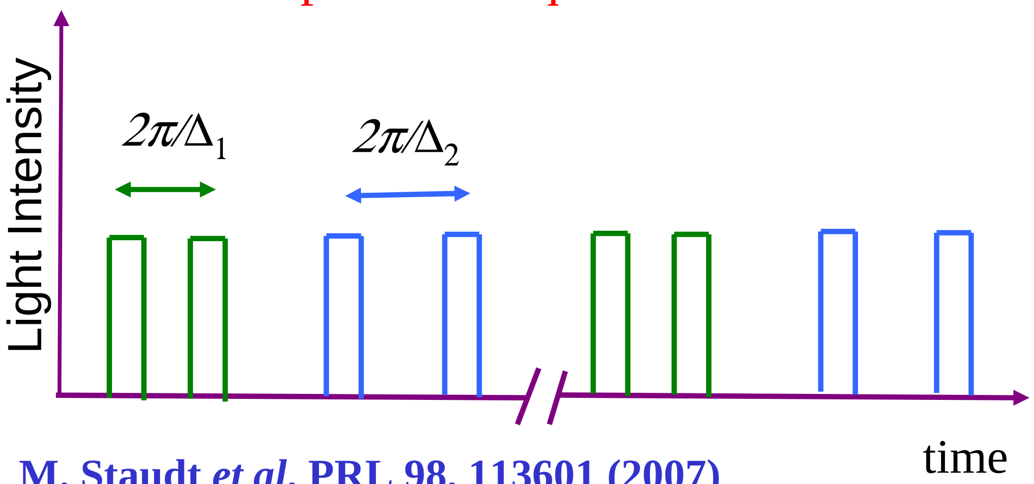
# Probing the coherence of the storage

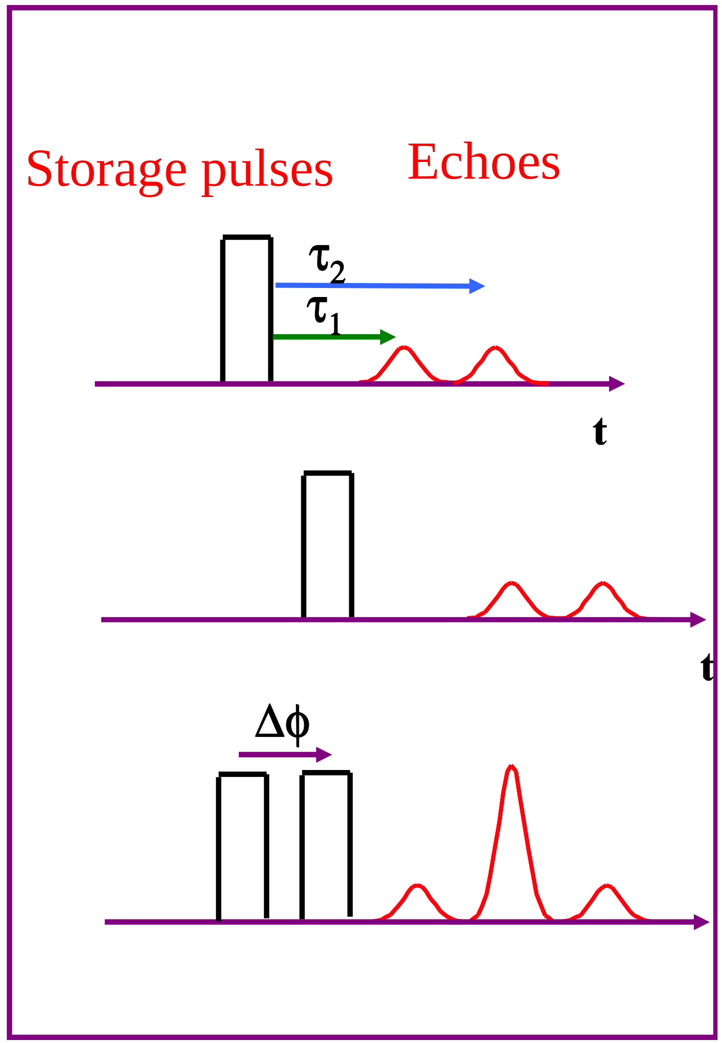
By preparing two gratings, it is possible to read out twice:

Spectral gratings




Preparation sequence



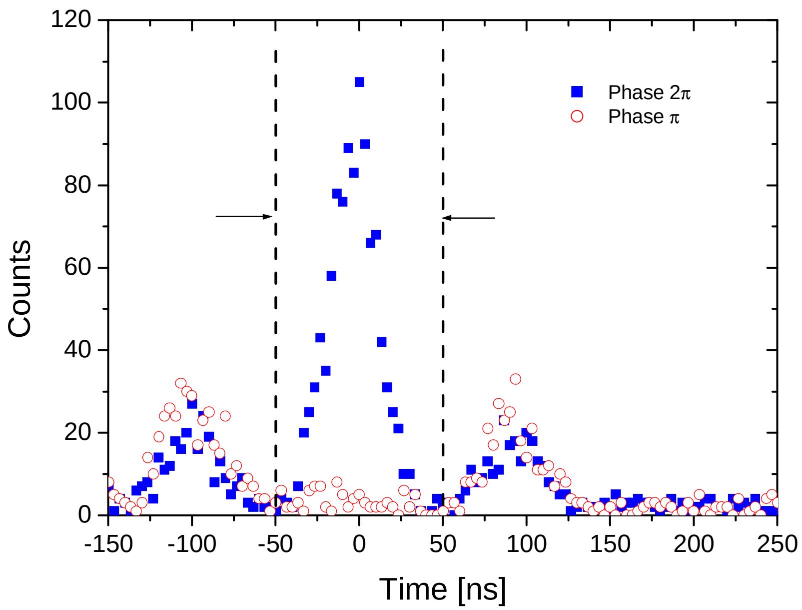



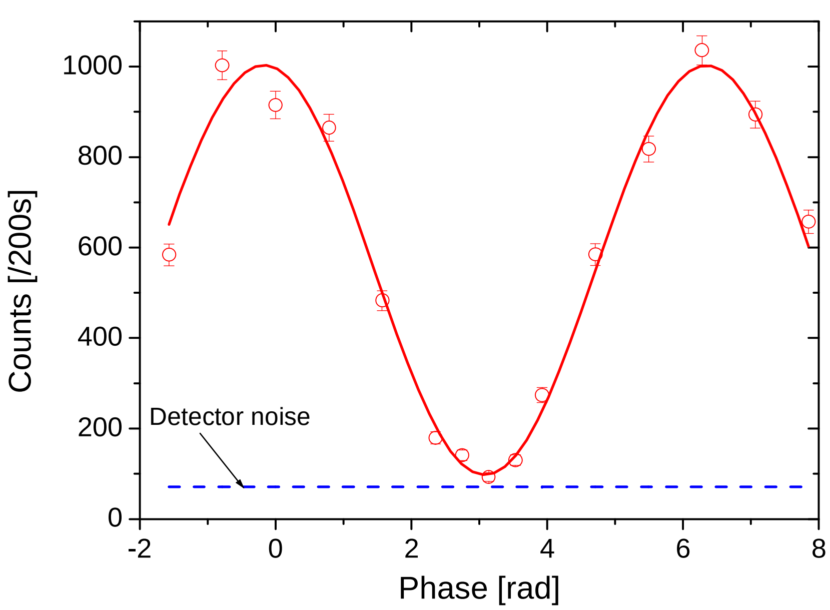

GAP Optique Geneva University

**M. Staudt *et al*, PRL 98, 113601 (2007)**

# Probing the coherence of the storage

**Incident pulses: 0.8 photon per pulse on average**



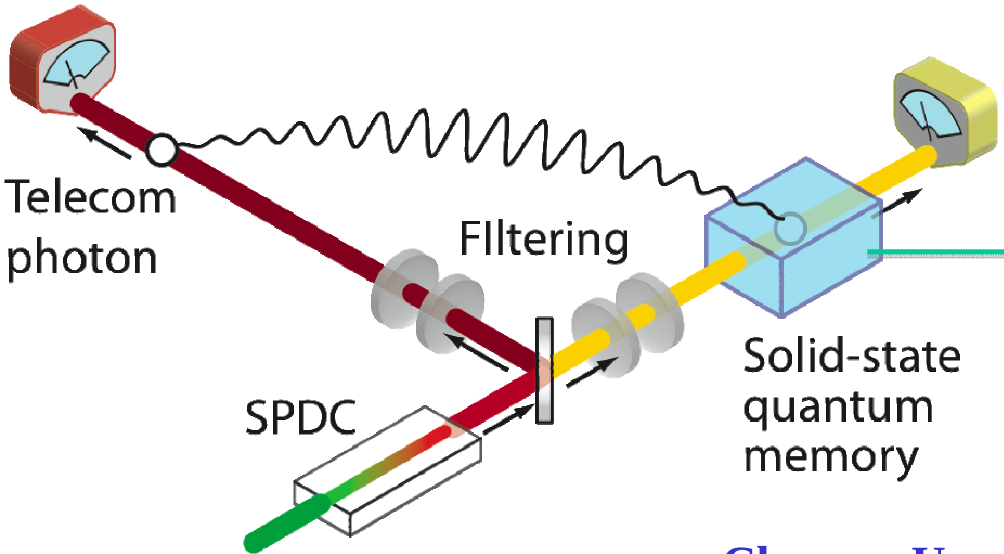



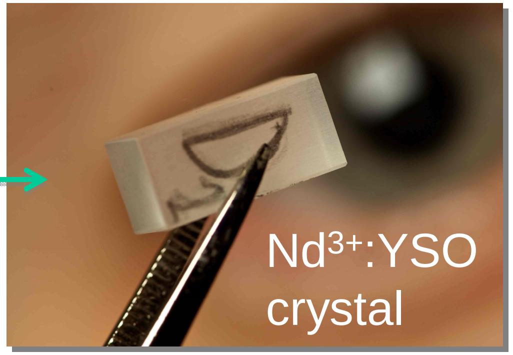

**Storage times: 200 ns and 300 ns**

**Visibility : 95 ±3 %**

**H. De Riedmatten, M. Afzelius et al, Nature 456, 773, 2008**

# Demonstration of entanglement between a telecom photon and an excitation stored in a crystal

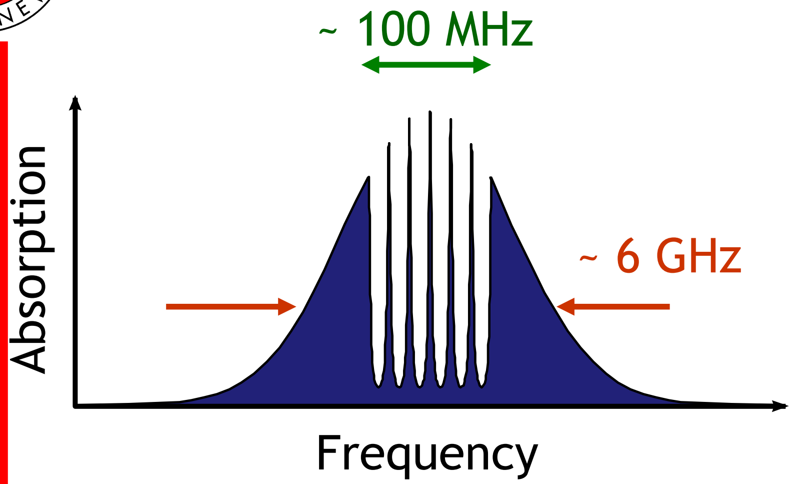


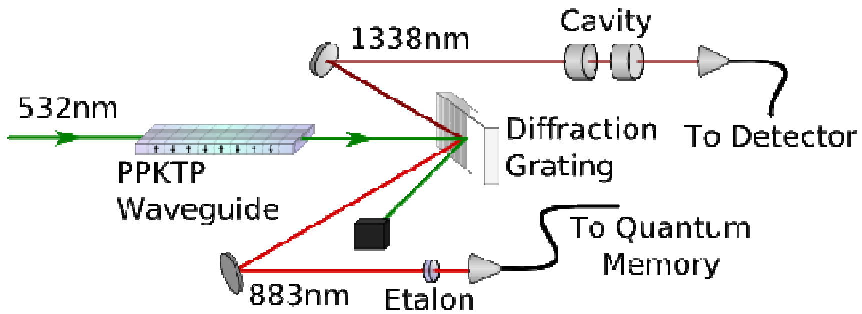




**Clausen, Usmani et al, Nature 469, 508-511, 2011**

GAP Optique Geneva University

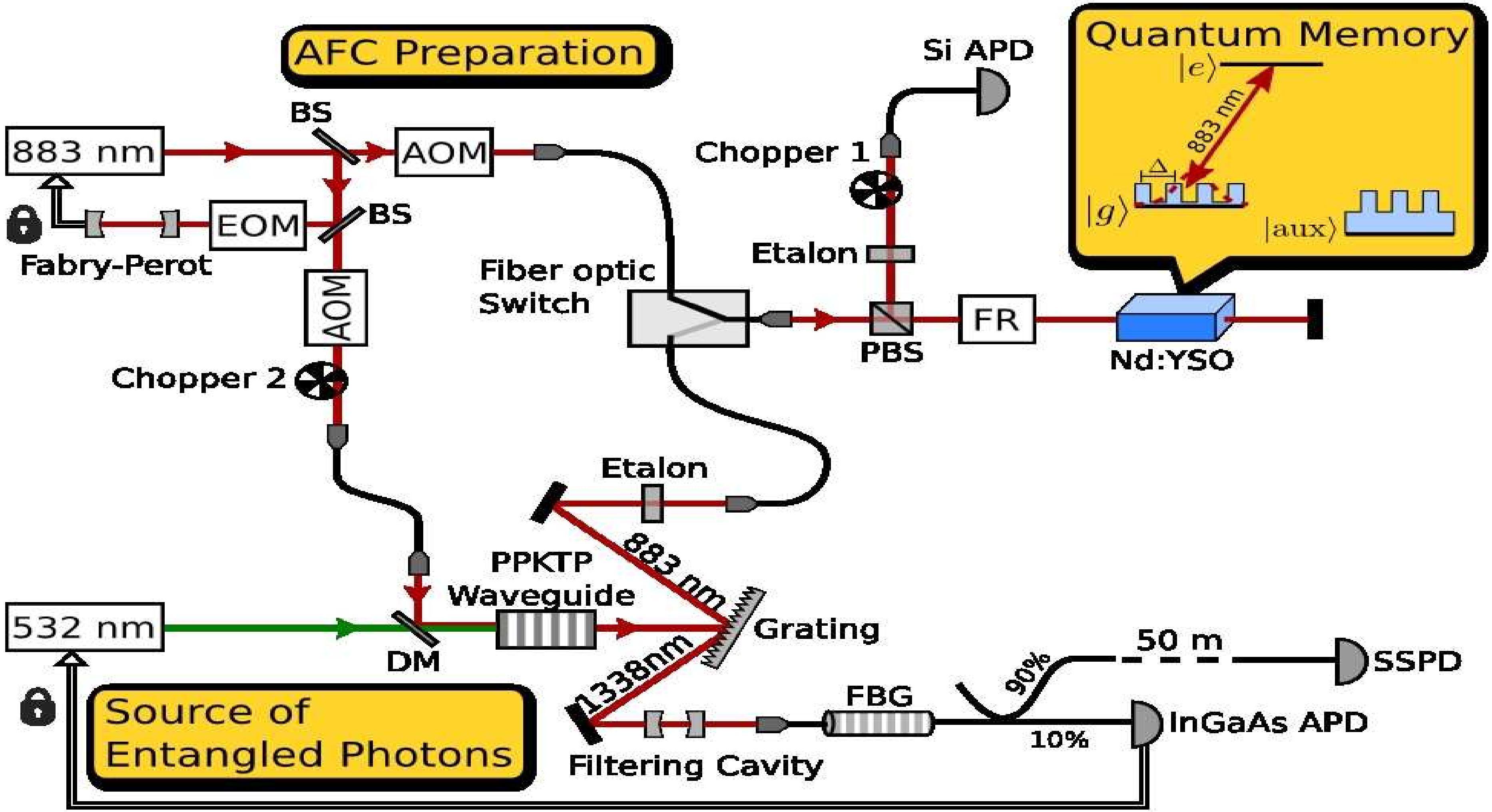
# Filtering




| | 883 nm | 1338 nm |
|---|---|---|
| ◆ Photon from guide | 1.5 THz | 1.5 THz |
| ◆ Diffraction grating | 90GHz | 60 GHz |
| ◆ Fabry-Perot Cavity | | FSR = 24 GHz<br>$\Gamma$ = 45 MHz |
| ◆ 2 Etalons | FSR = 42, 50 GHz<br>$\Gamma$ = 600 MHz | |

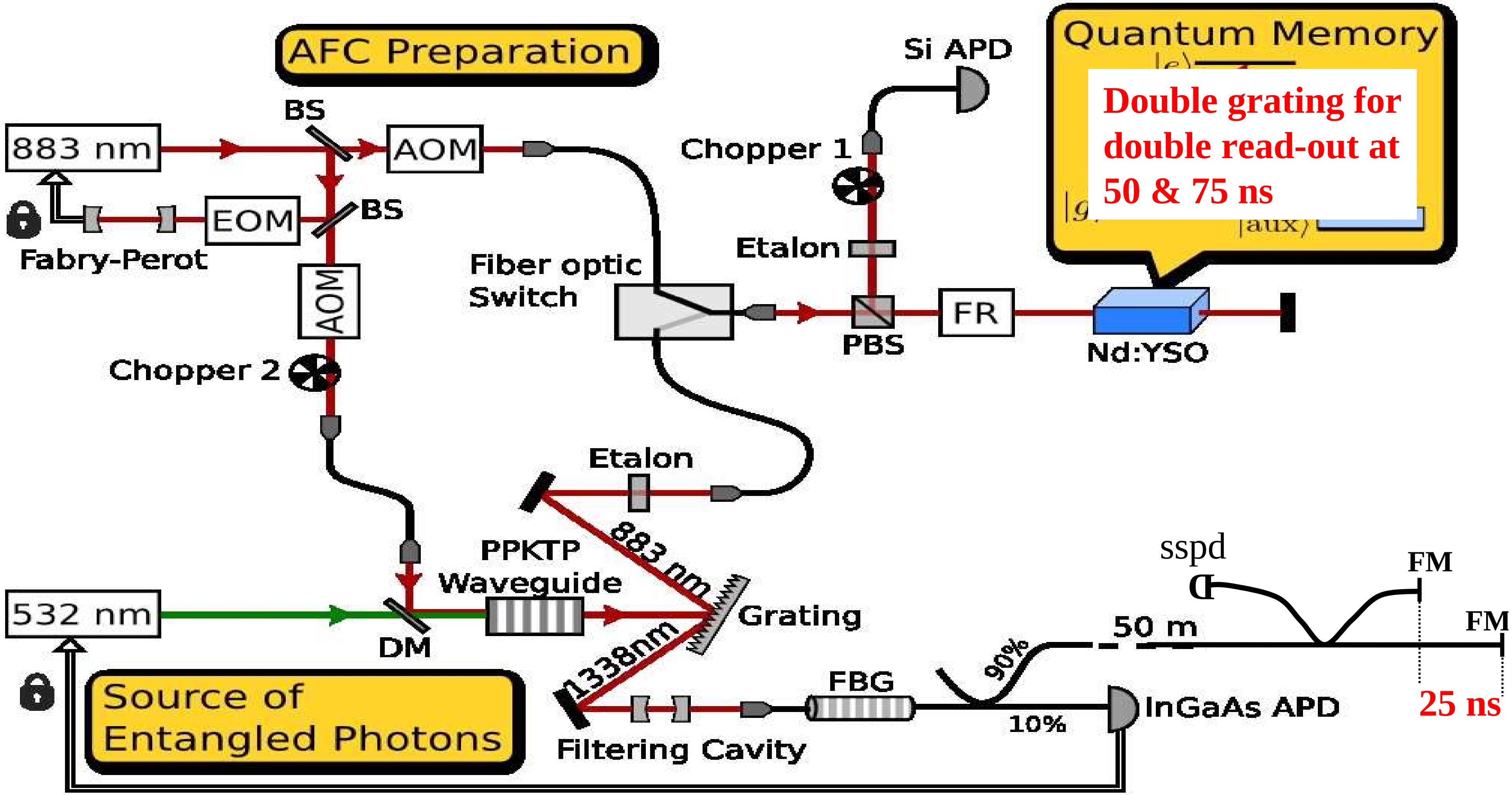
# Photon-Crystal Entanglement




EOM: Electro-optic modulator
AOM: Acousto-optic modulator
PBS: Polarizing beam splitter
FBG: Fiber Bragg grating
SSPD: Superconducting single-photon detector

BS: Beam splitter
FR: Faraday rotator
DM: Dichroic Mirror
: Feedback for stabilization

# Photon-Crystal Entanglement

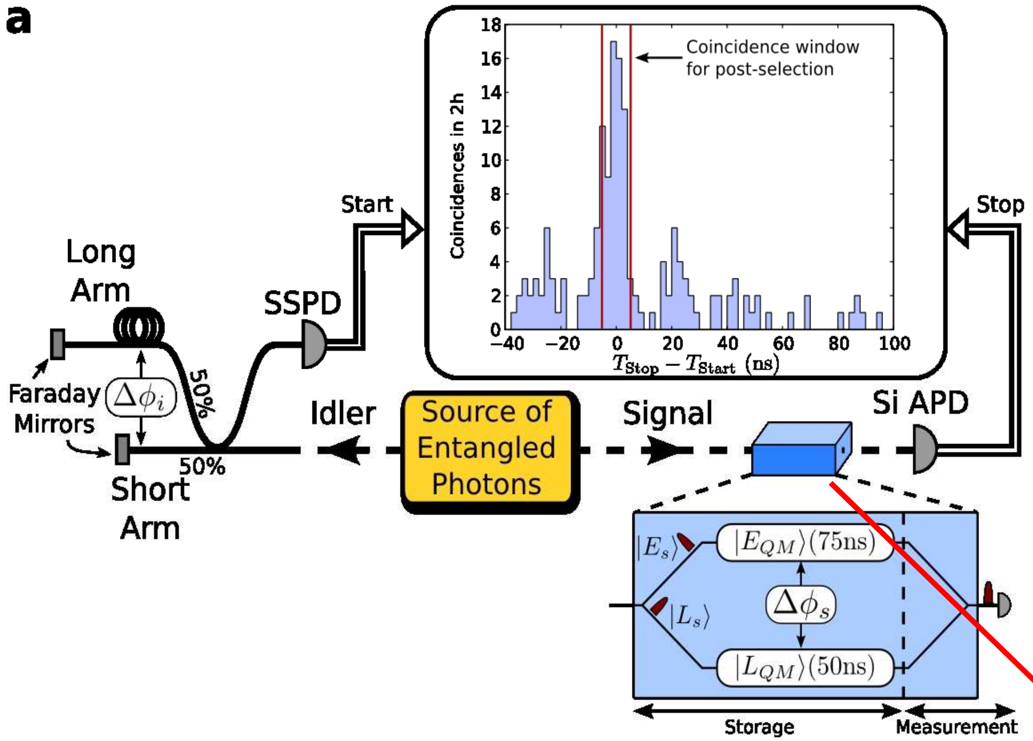


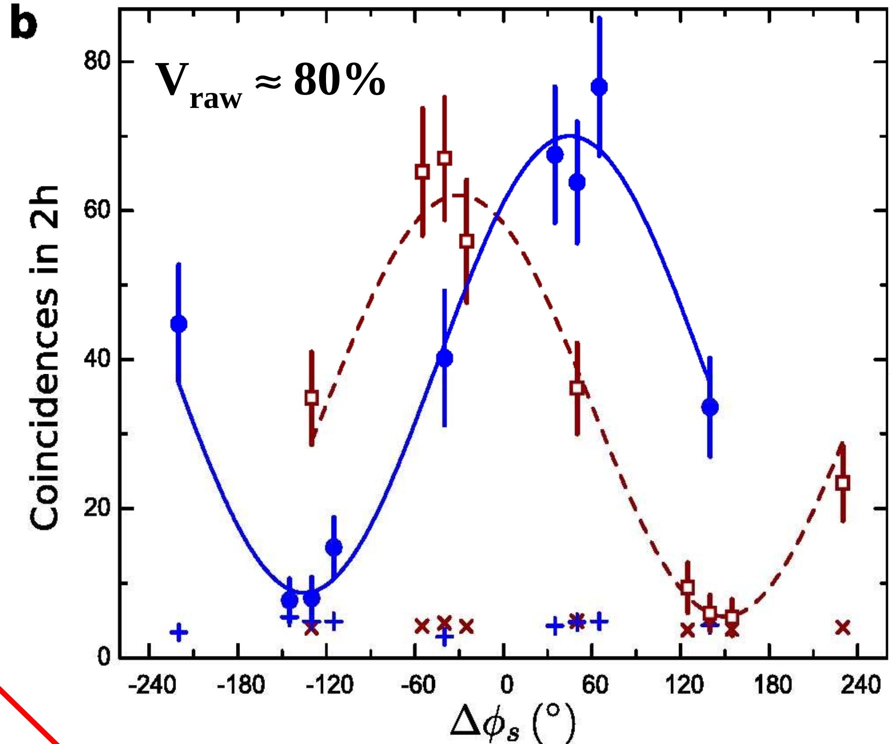

EOM: Electro-optic modulator
AOM: Acousto-optic modulator
PBS: Polarizing beam splitter
FBG: Fiber Bragg grating
SSPD: Superconducting single-photon detector

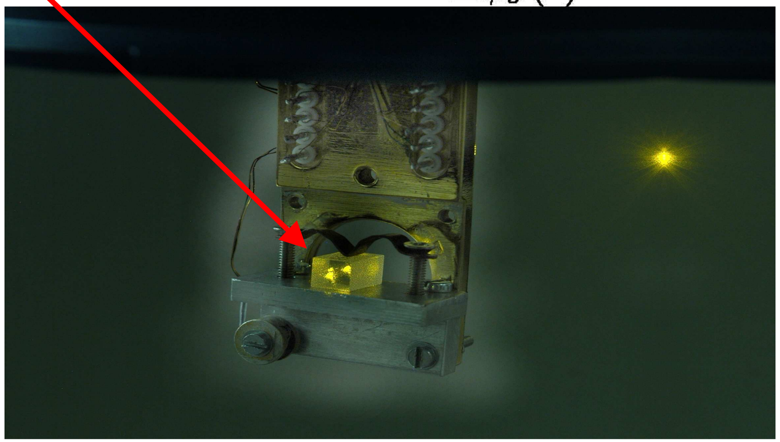
BS: Beam splitter
FR: Faraday rotator
DM: Dichroic Mirror
: Feedback for stabilization

# Photon – Crystal Entanglement

**Clausen, Usmani et al, Nature 469, 508-511, 2011**



**Photon-Crystal entanglement with a violation of the CHSH-Bell inequality: S=2.64 > 2**

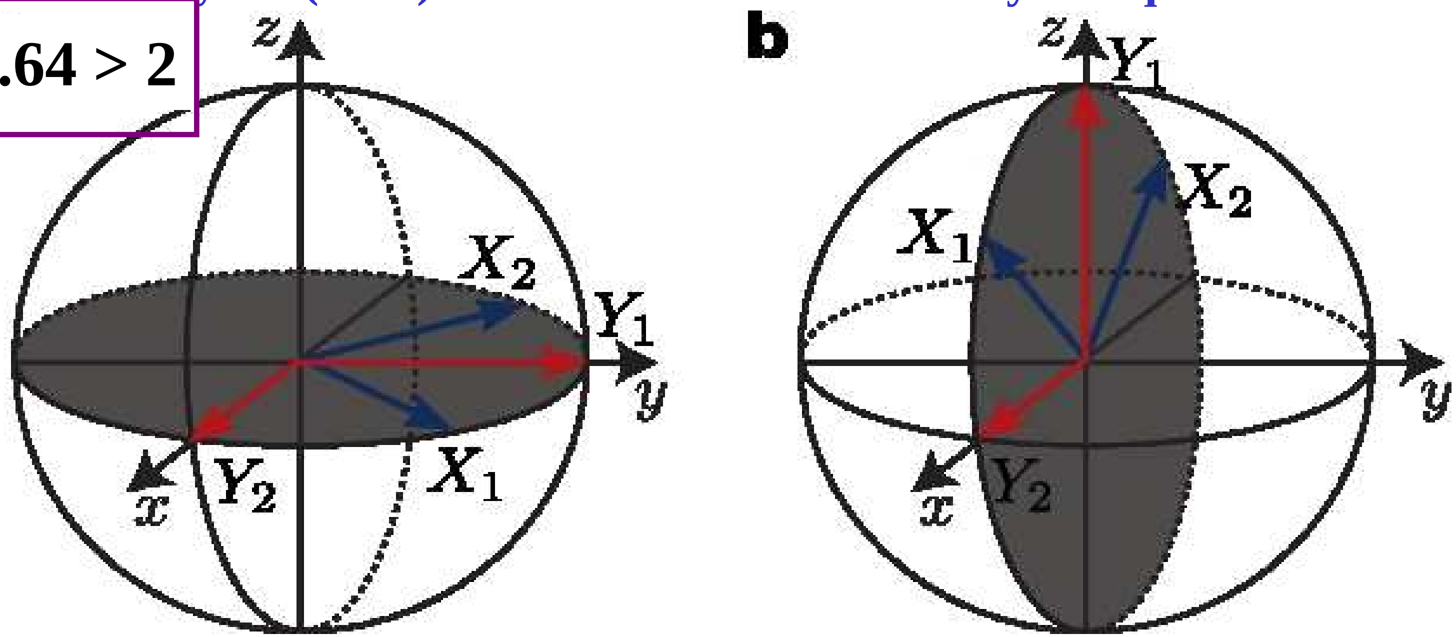
# Photon-Hybrid qubit Entanglement

GAP Optique Geneva University

**S = 2.64 > 2**

**Red: photon (interferometer)**
**Blue: crystal (AFC)**

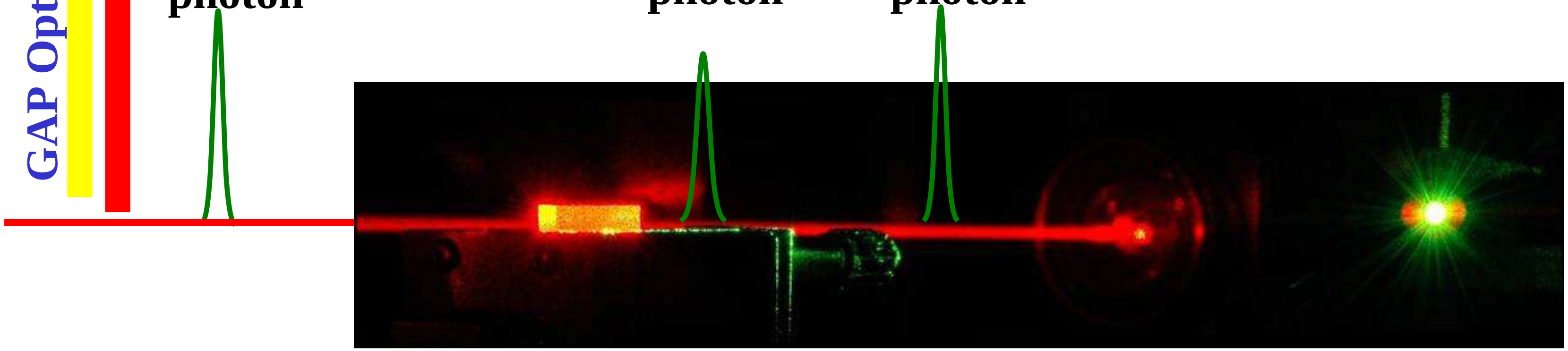
**Red: photon (interferometer)**
**Blue: Hybrid qubit**




**Incoming photon**

**AFC-echo photon**

**Transmitted photon**

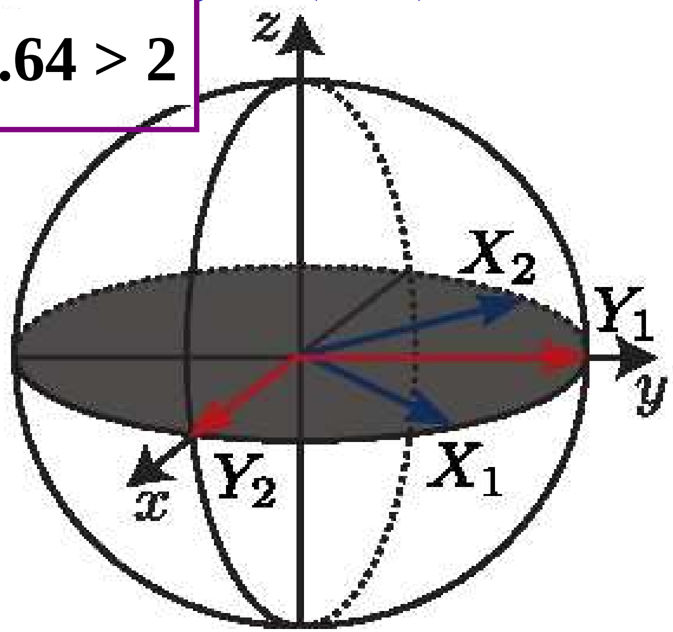


# Photon-Hybrid qubit Entanglement

**GAP Optique Geneva University**

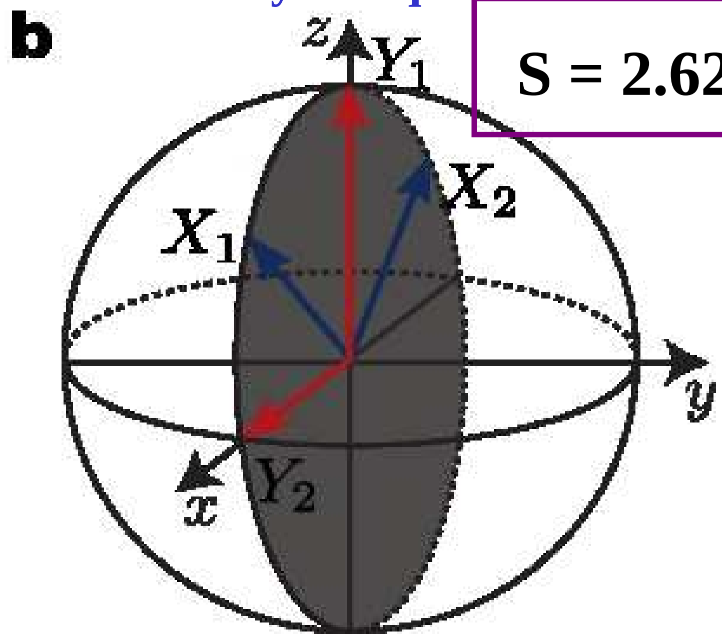
**Red: photon (interferometer)**
**Blue: crystal (AFC)**

**S = 2.64 > 2**



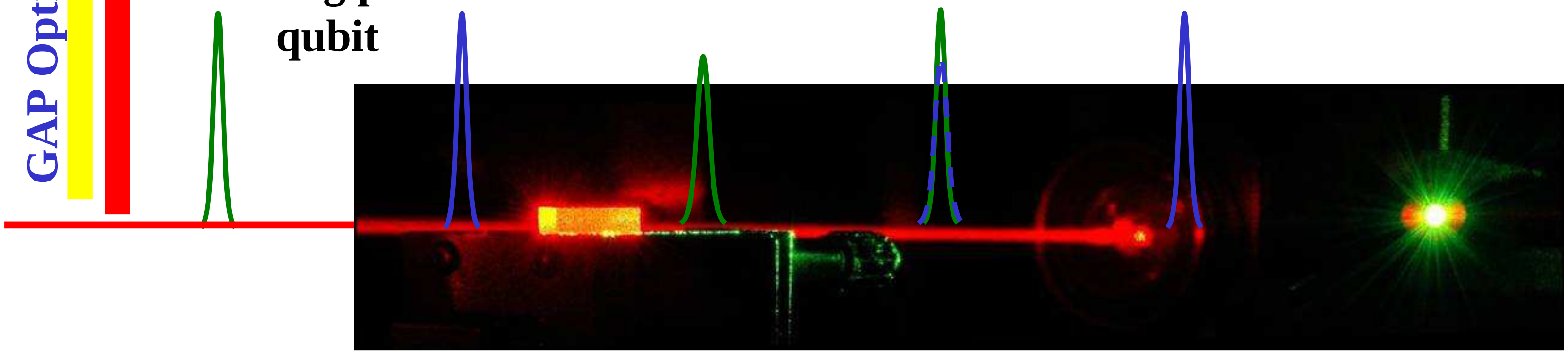

**Red: photon (interferometer)**
**Blue: Hybrid qubit**

**S = 2.62 > 2**




**Incoming photon qubit**

**Interference**

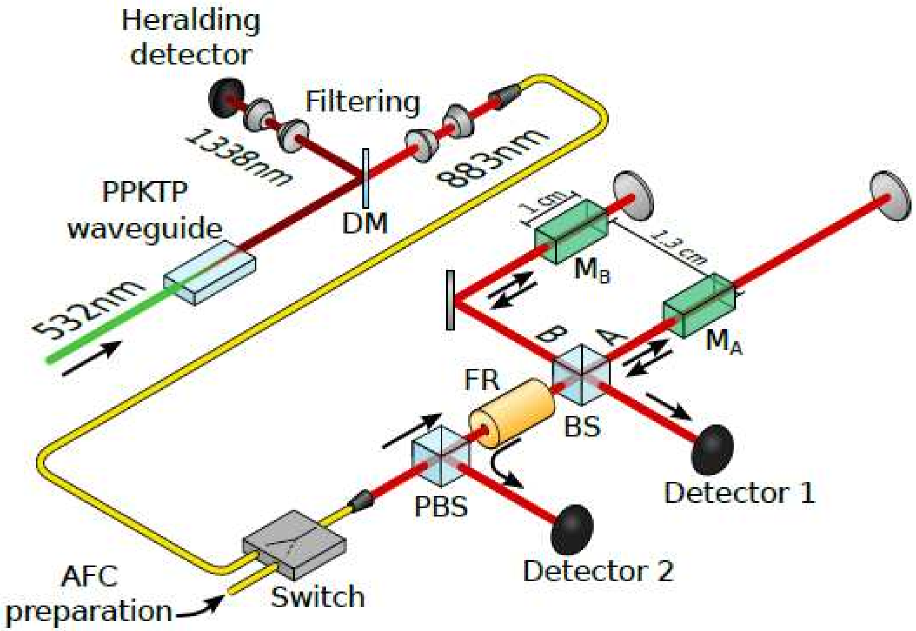


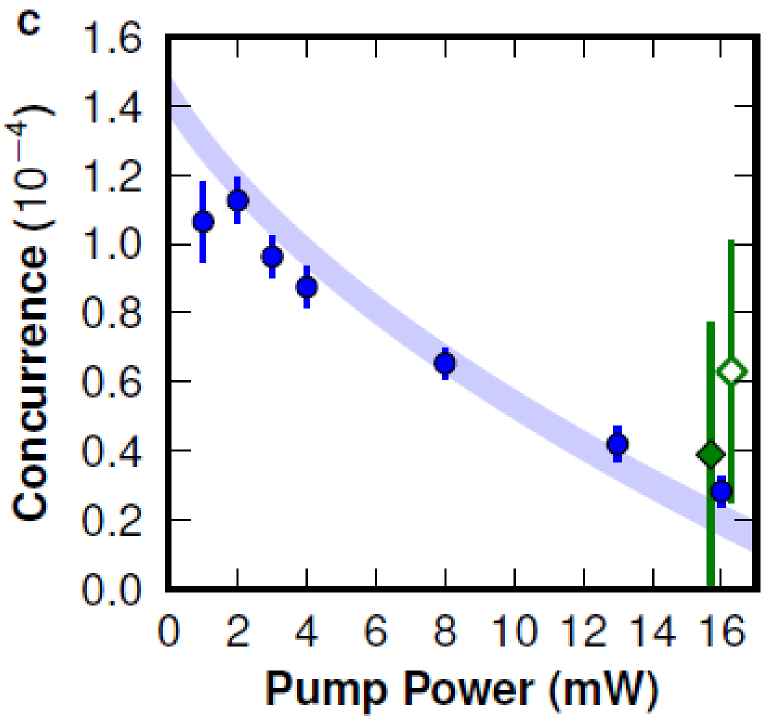
# Heralded quantum entanglement between two crystals

Imam Usmani, Christoph Clausen, Félix Bussières, Nicolas Sangouard, Mikael Afzelius, and Nicolas Gisin

Group of Applied Physics, University of Geneva, Switzerland

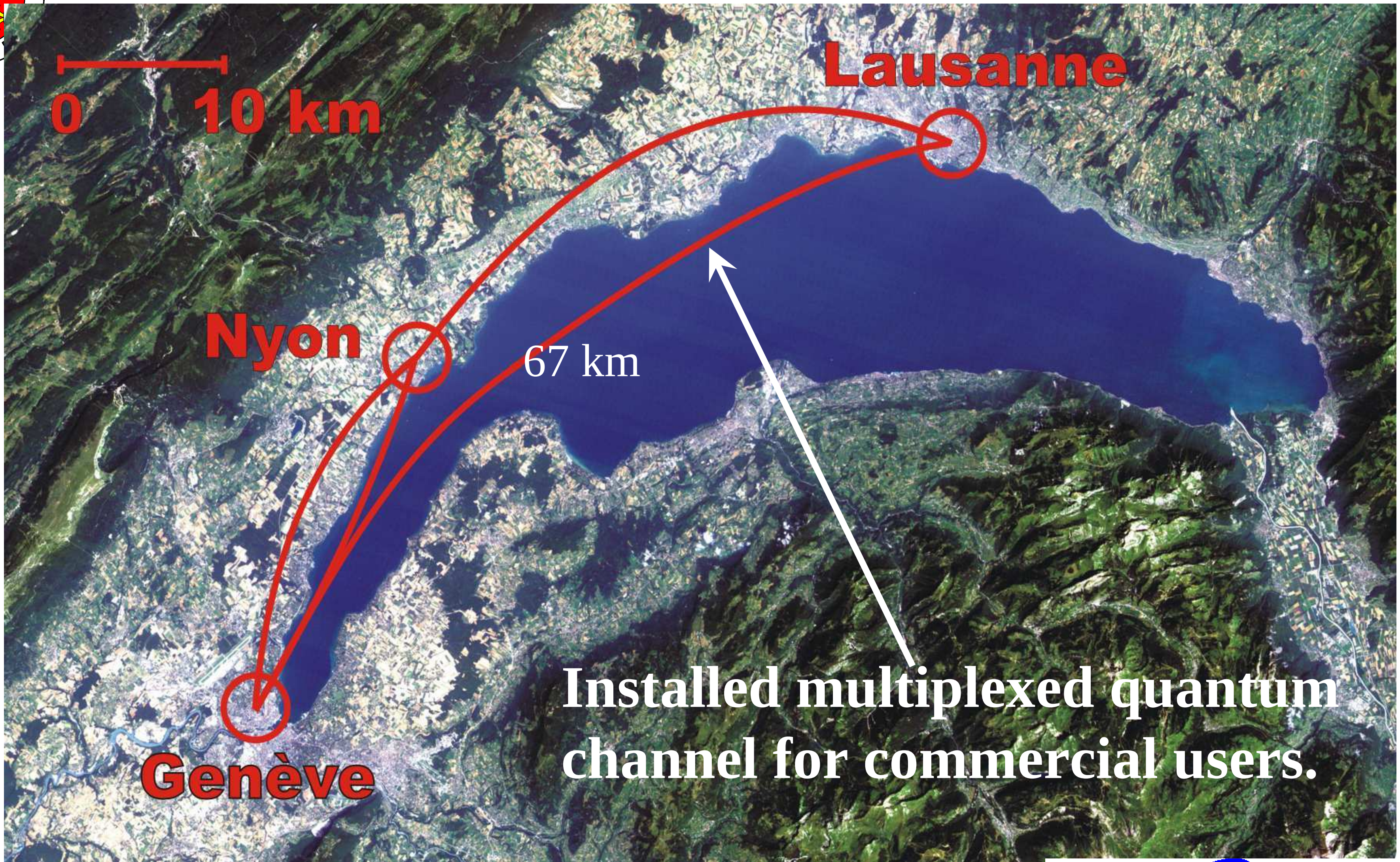
arXiv:1109.0440




GAP Optique Geneva University

# Industry Venture Session on Thursday at 3.30 pm



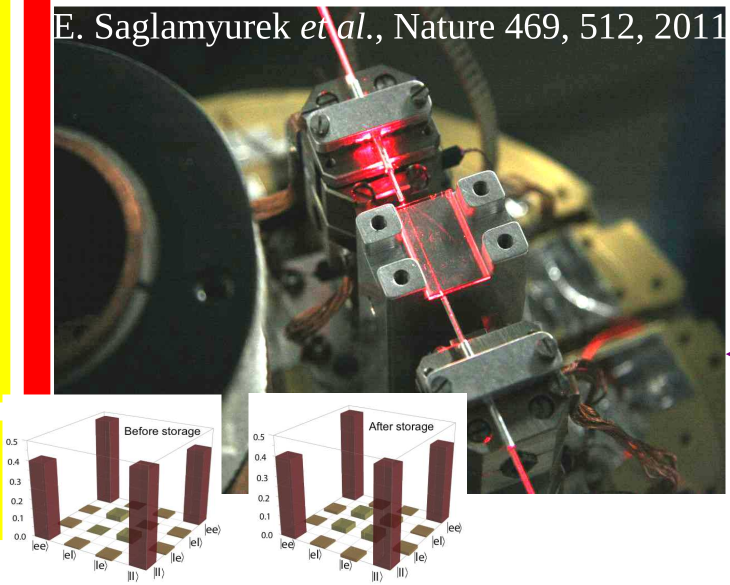

GAP Optique Geneva University

id Quantique

GAP Optique Geneva University

# Conclusions

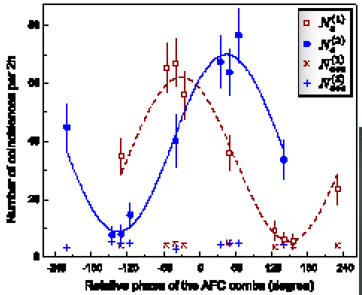
- Quantum Engineering opens new theory questions.
- Experimental DI-QKD is a Grand Challenge.
- The AFC protocol is very promising for a solid-state multimode Q memory.




E. Saglamyurek *et al.*, Nature 469, 512, 2011

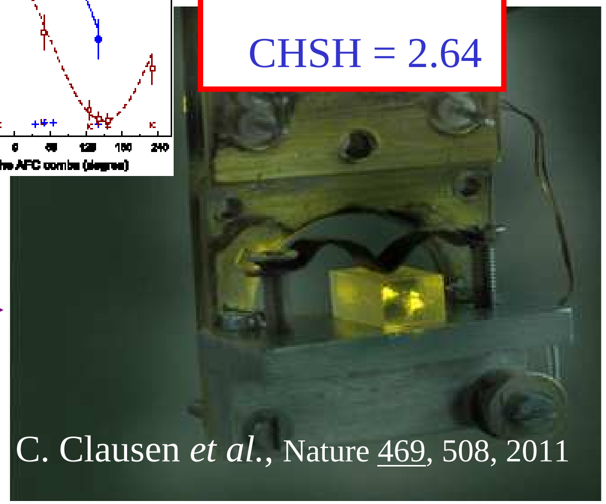
Calgary

Geneva



Photon-Crystal

CHSH = 2.64



C. Clausen *et al.*, Nature 469, 508, 2011

# January 2012

## 4th Winter School on Practical Quantum Cryptography

**Dates:** Monday January 23 to Thursday January 26, 2012

**Location:** Les Diablerets, Switzerland

**More:** **www.idquantique.com or info@idquantique.com**

Scholarships Available:
Contact us by email

Pictures from the Winter School 2nd Edition

Key note speakers include:
- Nicolas Gisin
- Renato Renner
- Vadim Makarov

Winter School 1 – 3:
- over 45 participants
- from industry and academia
- from 5 continents


46

# Scientific Instrumentation




June 2011: id210
InGaAs APD SPD
Free Running Operation
Gating up to 100MHz