# Quantum Communication:

## QKD, teleportation into a solid-state quantum memory and Large entanglement

**Nicolas Gisin, Hugo Zbinden, Mikael Afzelius, Rob Thew and Félix Bussières**

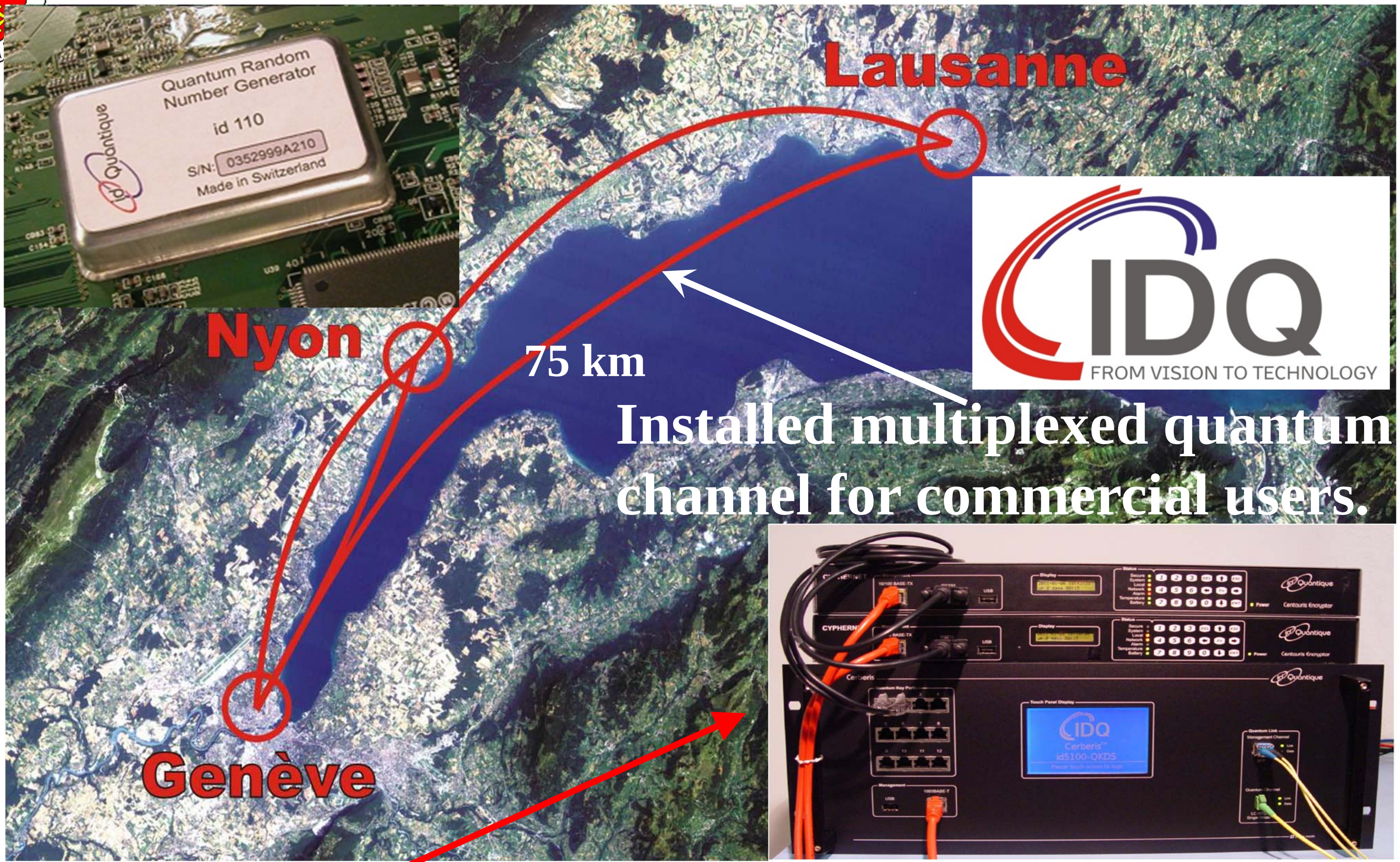
**GAP-Optique, University of Geneva**



- Commercial QKD system
- Why QKD ?
- Longer distances: networks based on trusted nodes
- Q memories for quantum repeaters and networks
- Large Entanglement

# Years of continuous commercial operation






Used daily by some commercial

# Why QKD ?




How much of a problem for QKD is quantum computing, really??

**Courtesy of Prof. Michele Mosca**

GAP Quantique Geneva University

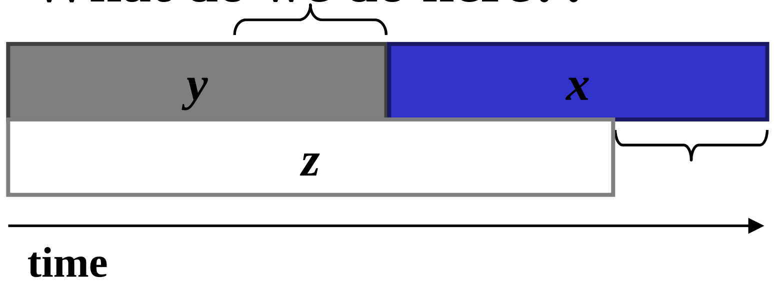
# How soon do we need to worry?

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.**

**What do we do here??**




**Courtesy of Prof. Michele Mosca**

GAP Quantique Geneva University

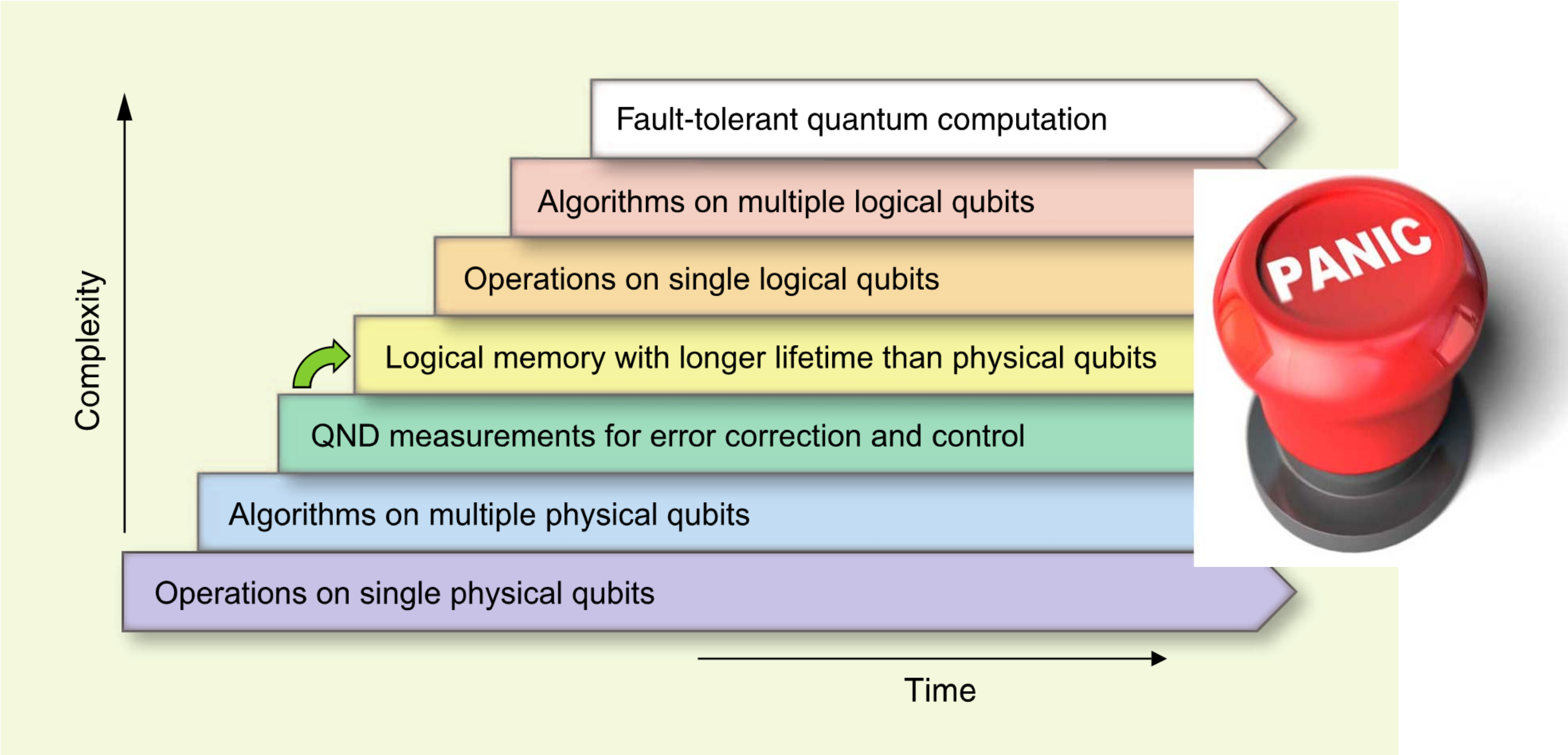
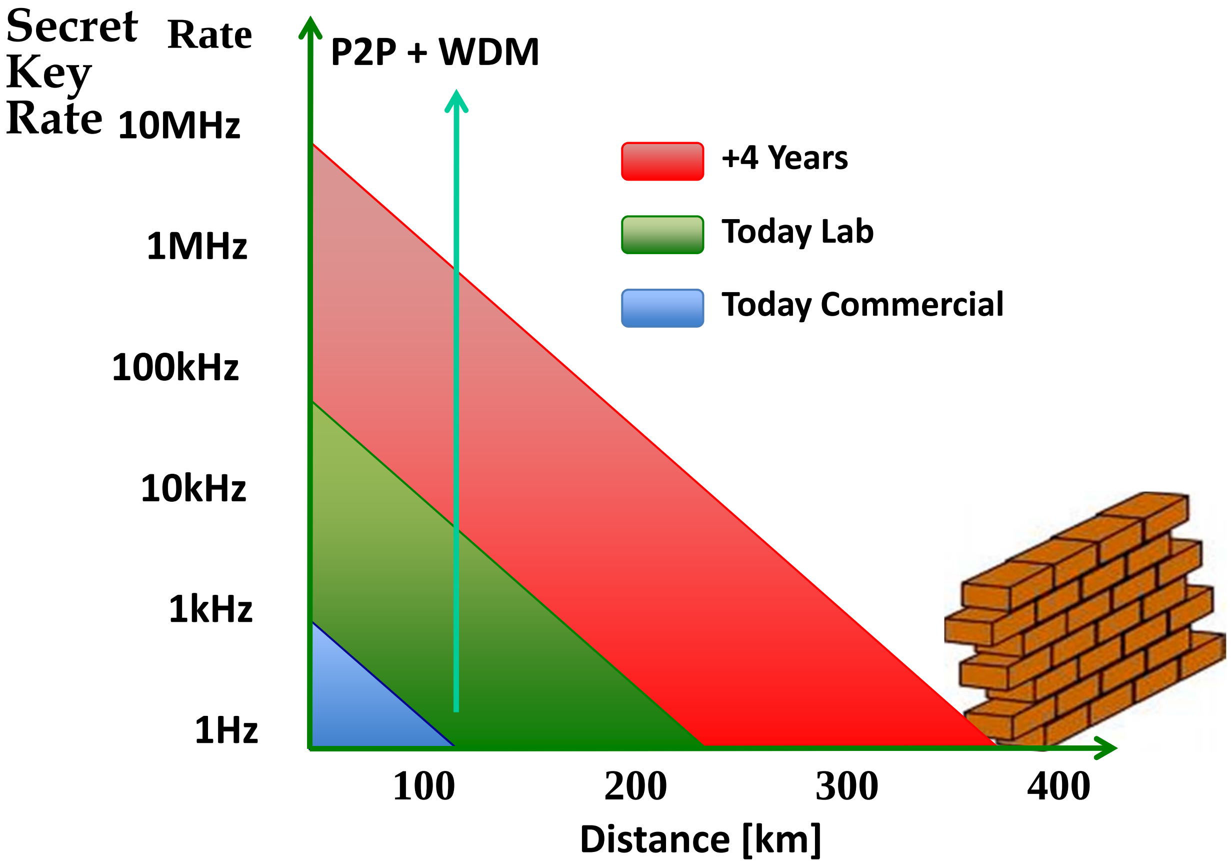



**Fig. 1.** Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third stage, and they now aim at reaching the fourth stage (green arrow). In the domain of atomic physics and quantum optics, the third stage had been previously attained by trapped ions and by Rydberg atoms. No implementation has yet reached the fourth stage, where a logical qubit can be stored, via error correction, for a time substantially longer than the decoherence time of its physical qubit components.

**Courtesy of Prof. Michele Mosca**

# How far can one send a photon ?



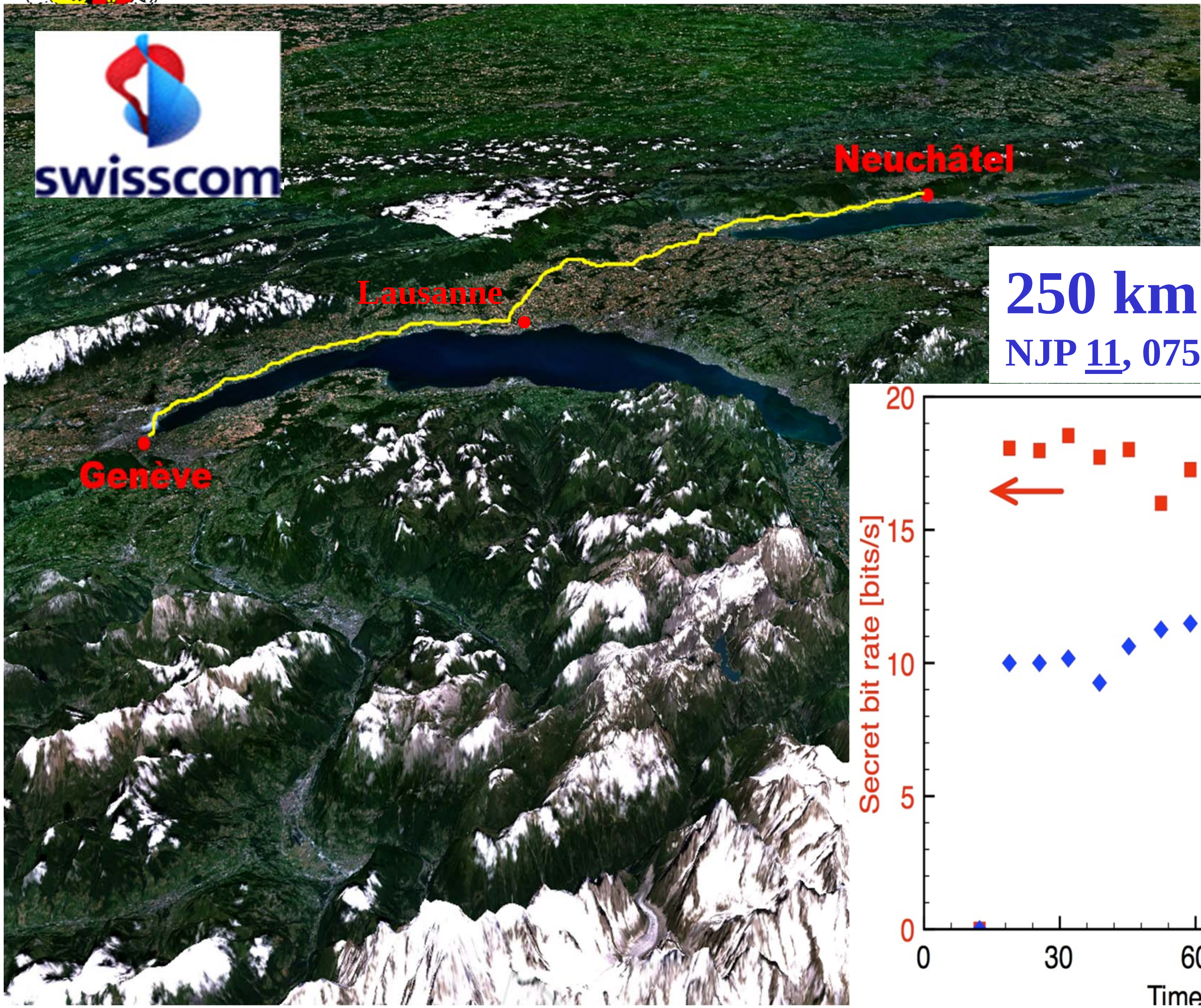

***There is a hard wall around 400 km !***

**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

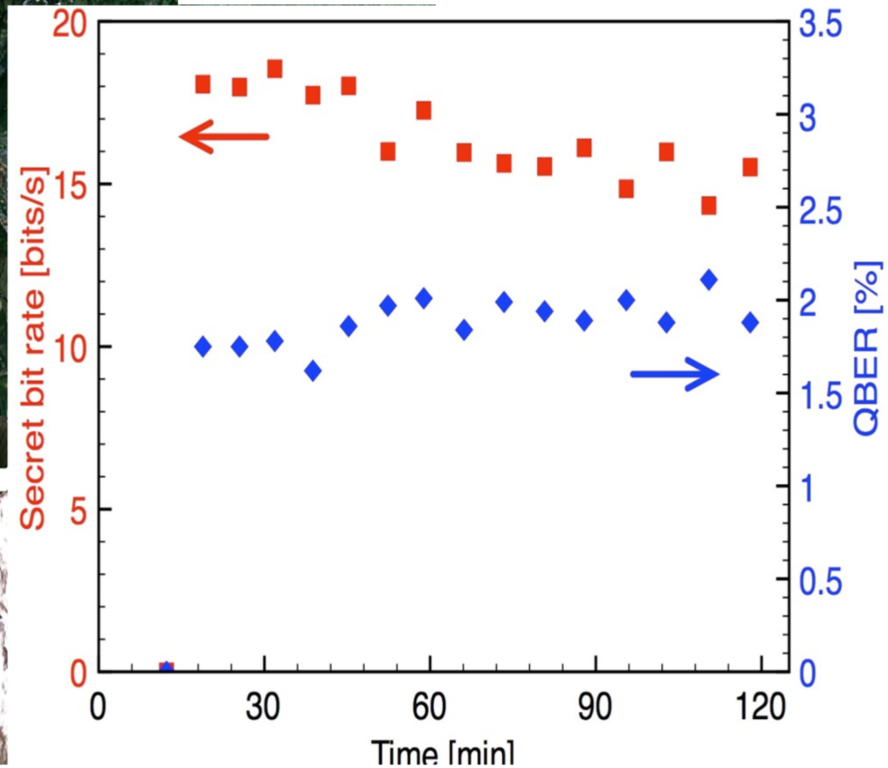
# Long distance QKD: World records

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



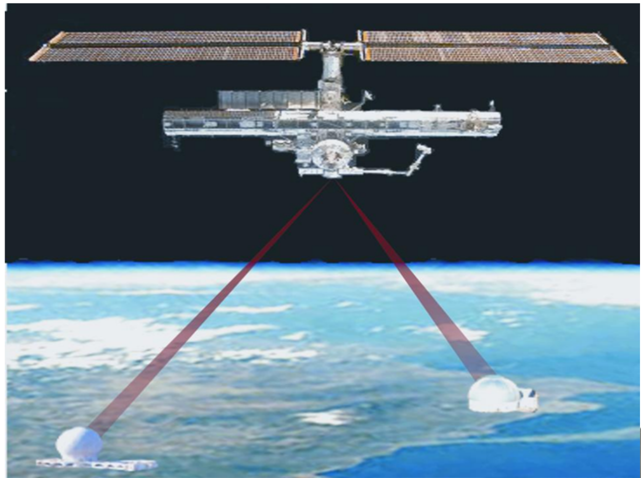

**250 km in the lab.**

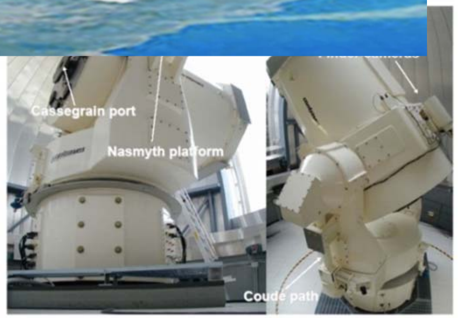
**NJP <u>11</u>, 075003 (2009)**



# Proposals for quantum communication in space

## Dual-downlink
## (ROM R&D 47 M€)

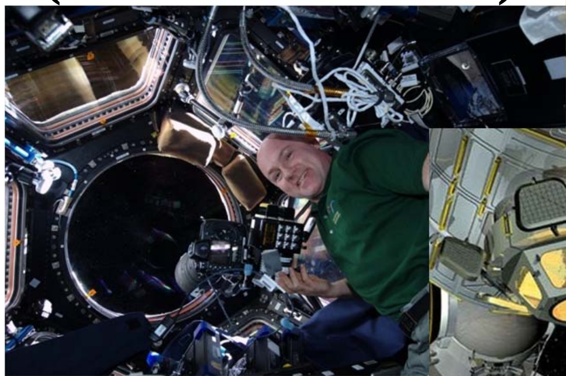


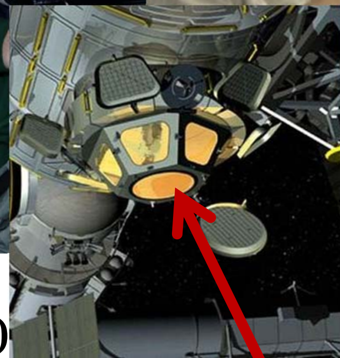



**Simultaneous optical downlink: 1400 km separation.**

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

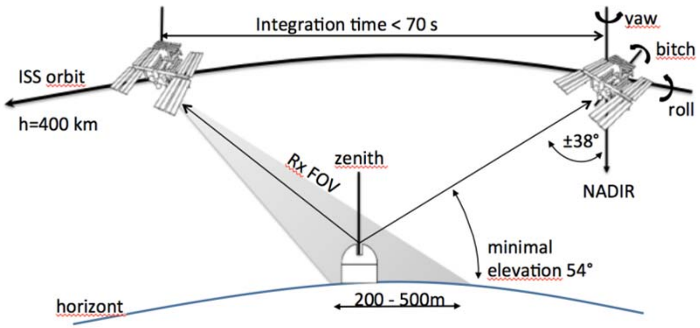
## Single-uplink
## (ROM R&D 1 M€)





**Astronaut A. Kuipers**

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

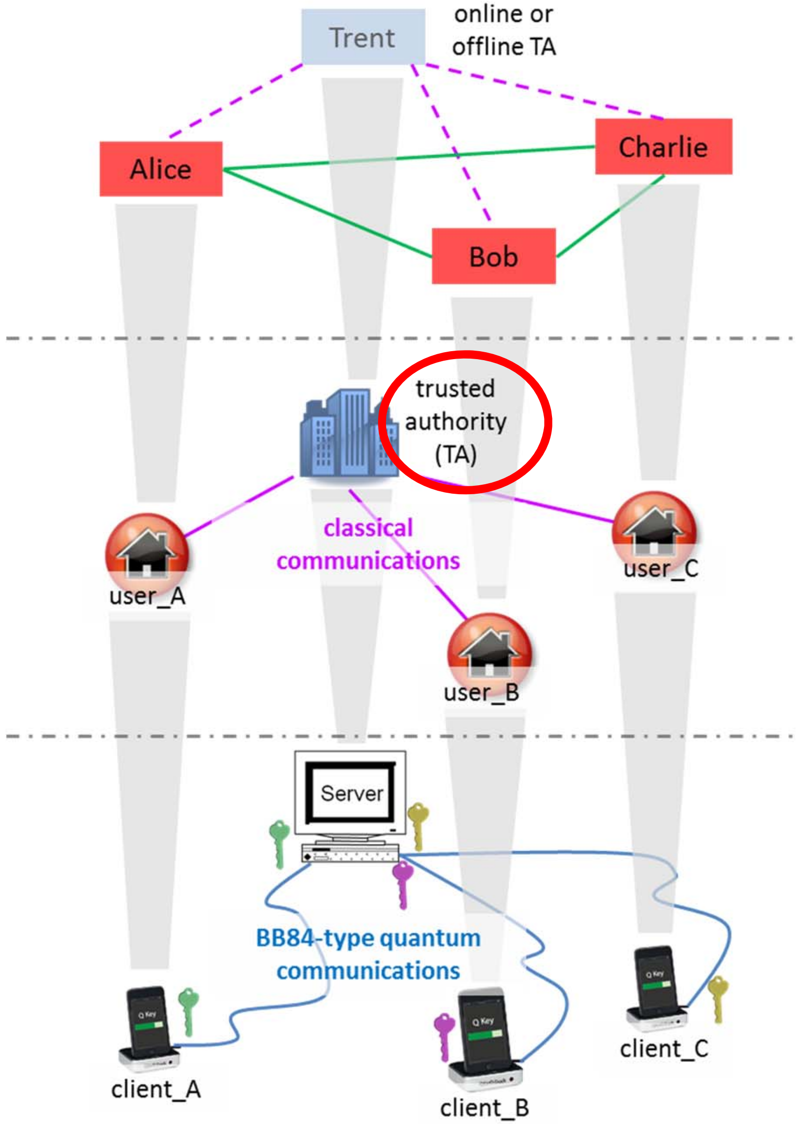



T. Scheidl, E. Wille, and R. Ursin, New Journal of Physics, 15, 043008 (2013)

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

# Network-centric Quantum Communications

Richard Hughes, Jane Nordholt and team
Los Alamos National Laboratory




**application layer:**
- **confidentiality**
- **authenticity**
- **integrity**
- **non-repudiation**
- **between users who may have no direct QC**

**quantum key management (QKM) layer:**
- **classical protocols built from quantum primitives**
  - **key establishment**
  - **signatures**
  - **certificates**

**quantum protocol layer:**
- **quantum identification (QID)**
- **quantum key distribution (QKD)**
- **quantum secret splitting (QSS)**

**quantum physical layer:**
- **novel BB84-type QC in fiber**
- **quantum multiple access (QMA)**
- **quantum random number gen.**

R. J. Hughes et al., US Patent 8,483,394; US Patent Applications: US 20130083926 A1; US2013/055356

J. E. Nordholt, et al., US Patent Applications: 61/693,131, US20130101119 A1, US 20130084079 A1, US2013/055430

R. J. Hughes et al., arXiv:1305.0305

GAP Quantique Geneva University

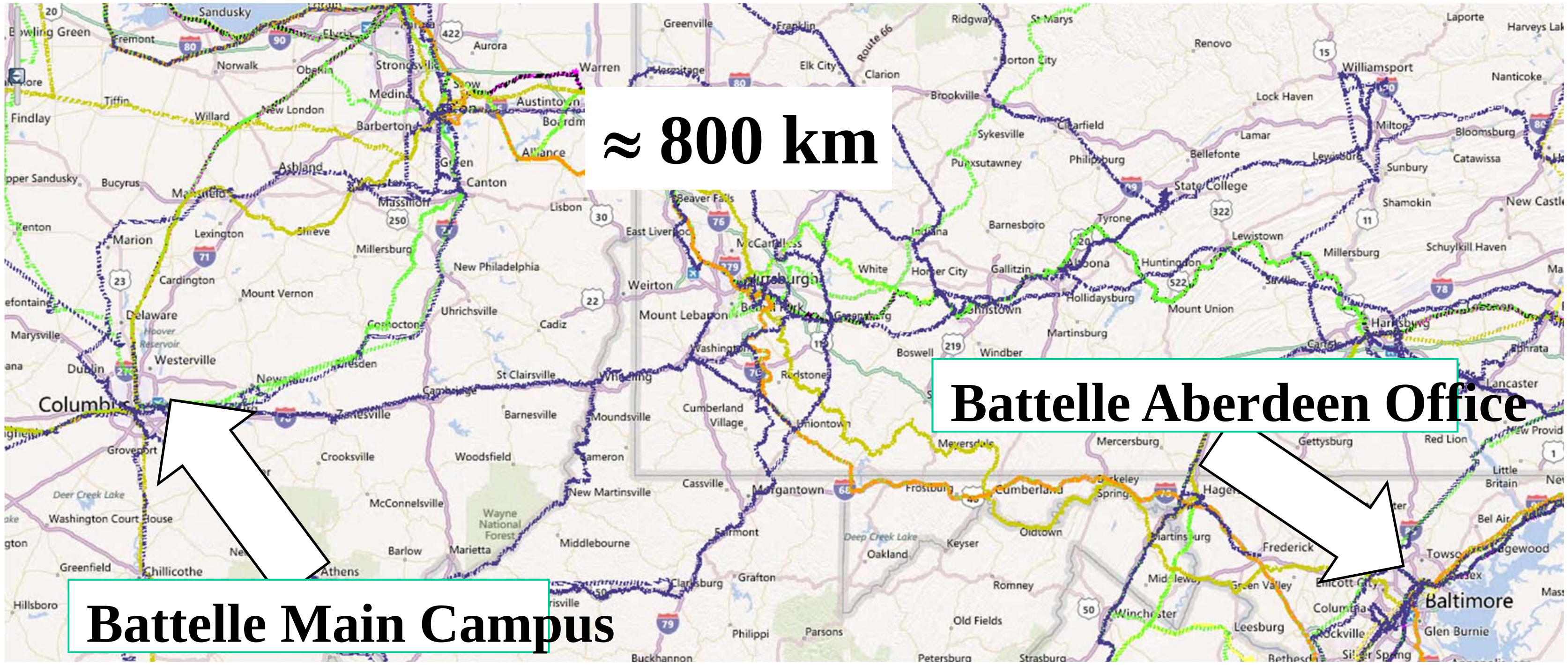
# Long Range QKD with trusted nodes

GAP Quantique Geneva University

Battelle
The Business of Innovation

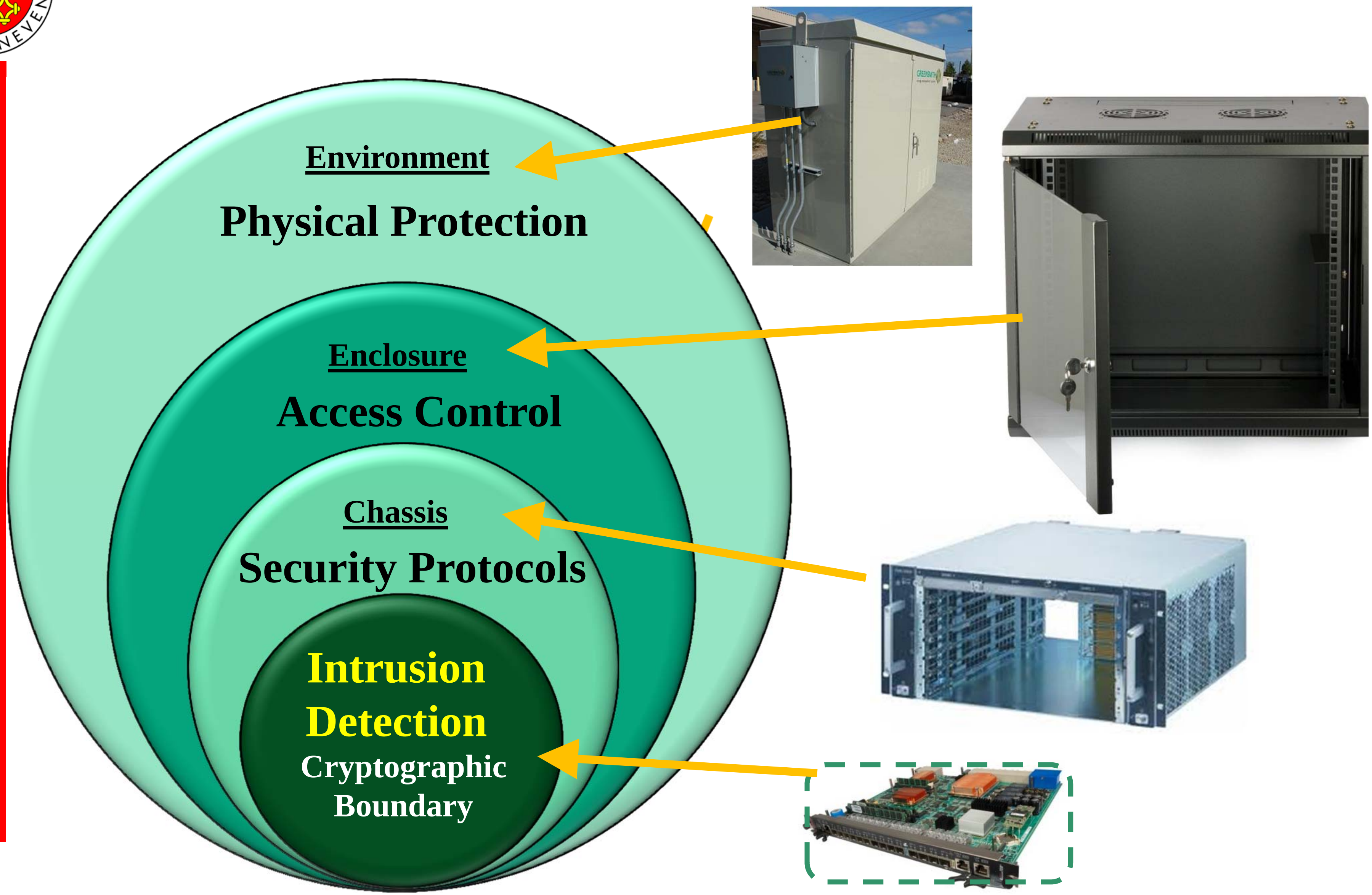
IDQ
FROM VISION TO TECHNOLOGY

**Battelle QKD Backbone**
- Columbus OH to Washington DC Area
- > 770 km
- Deployment targeted in 2015



# The Security Onion

Courtesy Dr Don Hayford
Battelle




GAP Quantique Geneva University

# N-photon quantum communication: quantum networks, quantum internet

GAP Quantique Geneva University

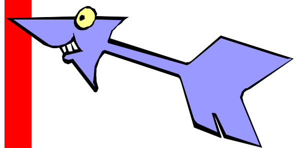

**We still miss the capability to store entanglement:**
**Developing <u>quantum memories</u> is a grand challenge !**

# Quantum memory

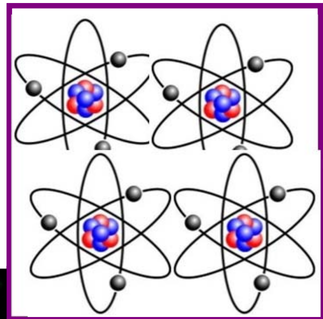
**Goal: controlled and reversible mapping of a photonic quantum state onto a long lived atomic ensemb**

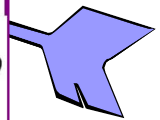
University

**photon in**

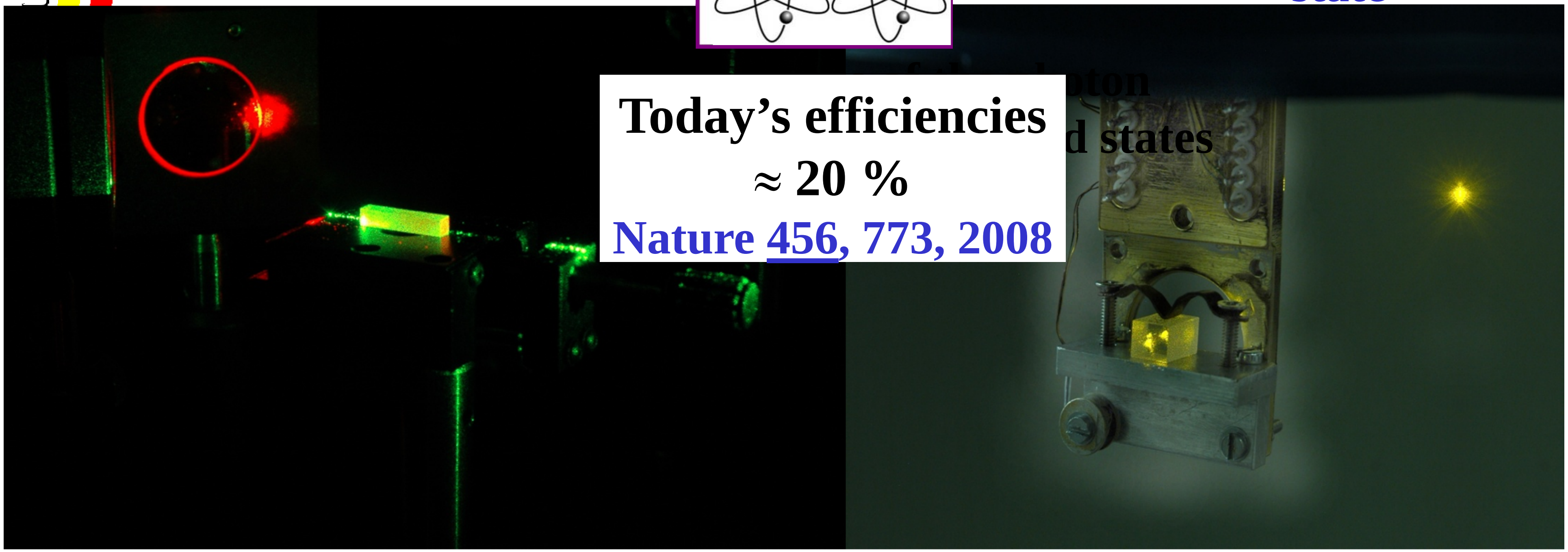


**crystal doped with billions of**





**photon out at desired time in same Q state**



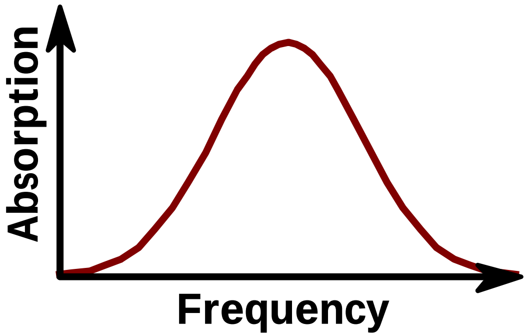
**Today's efficiencies ≈ 20 %**

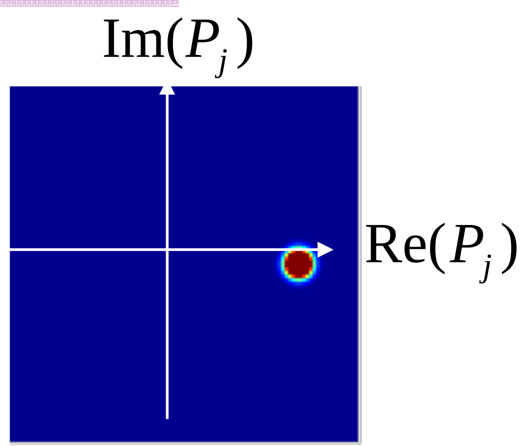
**Nature 456, 773, 2008**

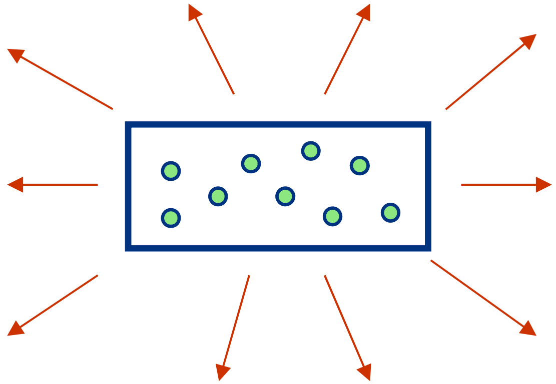
# Controlling the Dephasing! Atomic Frequency Comb

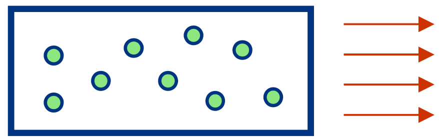
$$\sum_{j=1}^{N} e^{ikr_j} e^{-i\delta_j t} \left| g_1 \ldots e_j \ldots g_N \right\rangle \qquad P_j = e^{-i\delta_j t}$$

$\Delta$ continuous $\Rightarrow$ Dephasing



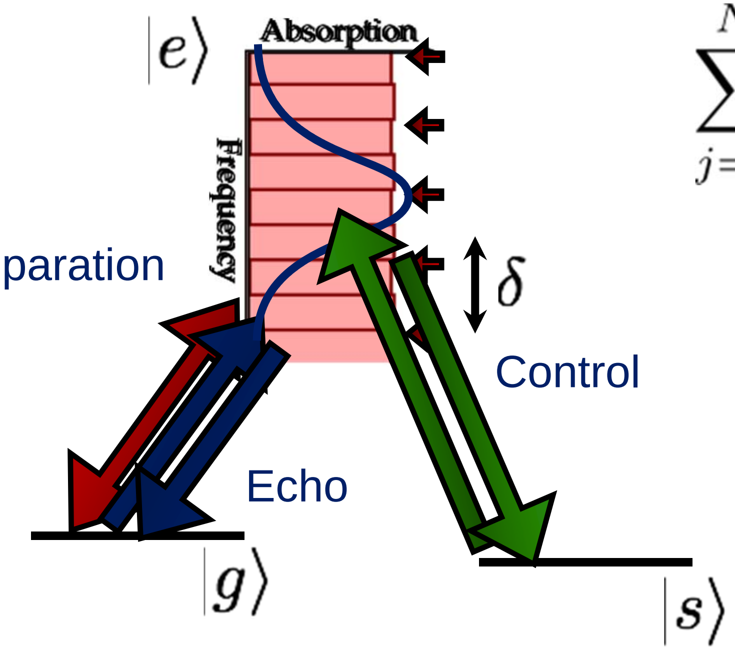





GAP Quantique Geneva University

# Atomic Frequency Comb (AFC) Quantum Memory



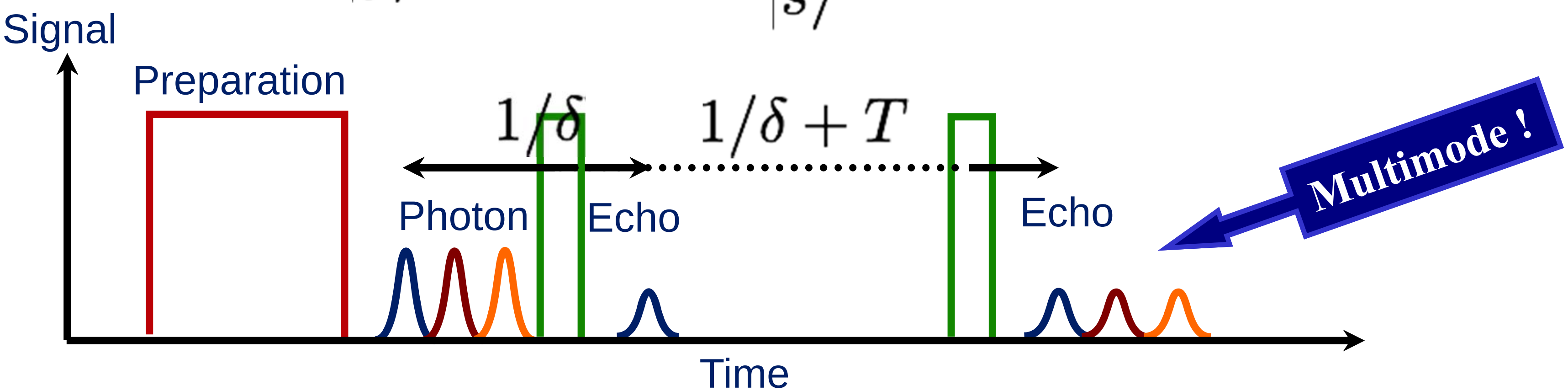



$$\sum_{j=1}^{N} e^{ikx_j} e^{i\delta_j t} |g_1 \ldots e_j \ldots g_N\rangle$$

Periodic!

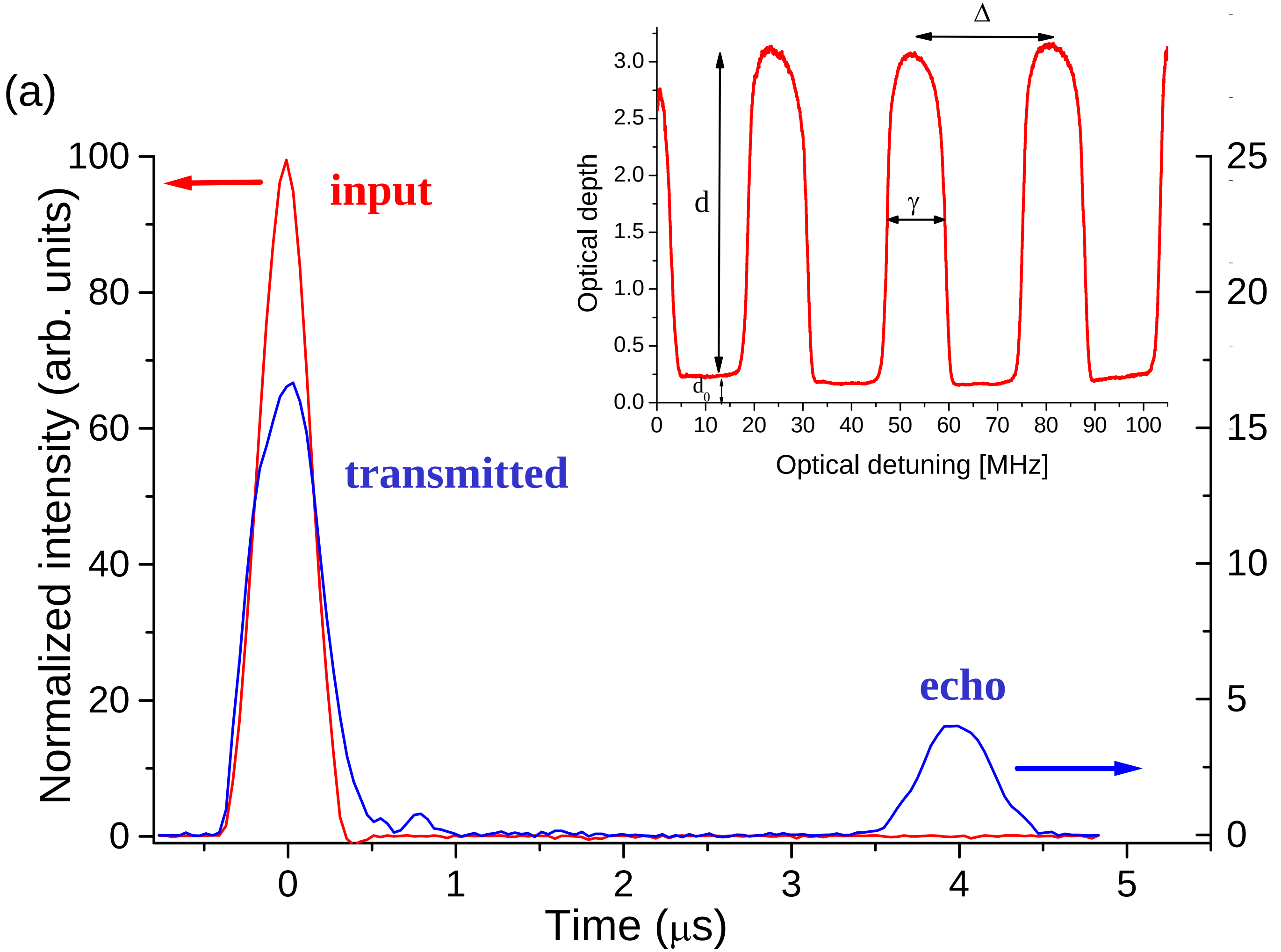
2 levels: preprogrammed delay (AFC echo)

3 levels: ***on-demand*** re-emission (spin wave storage)




*M. Afzelius et al. PRA 79, 052329 (2009)*

# AFC echo

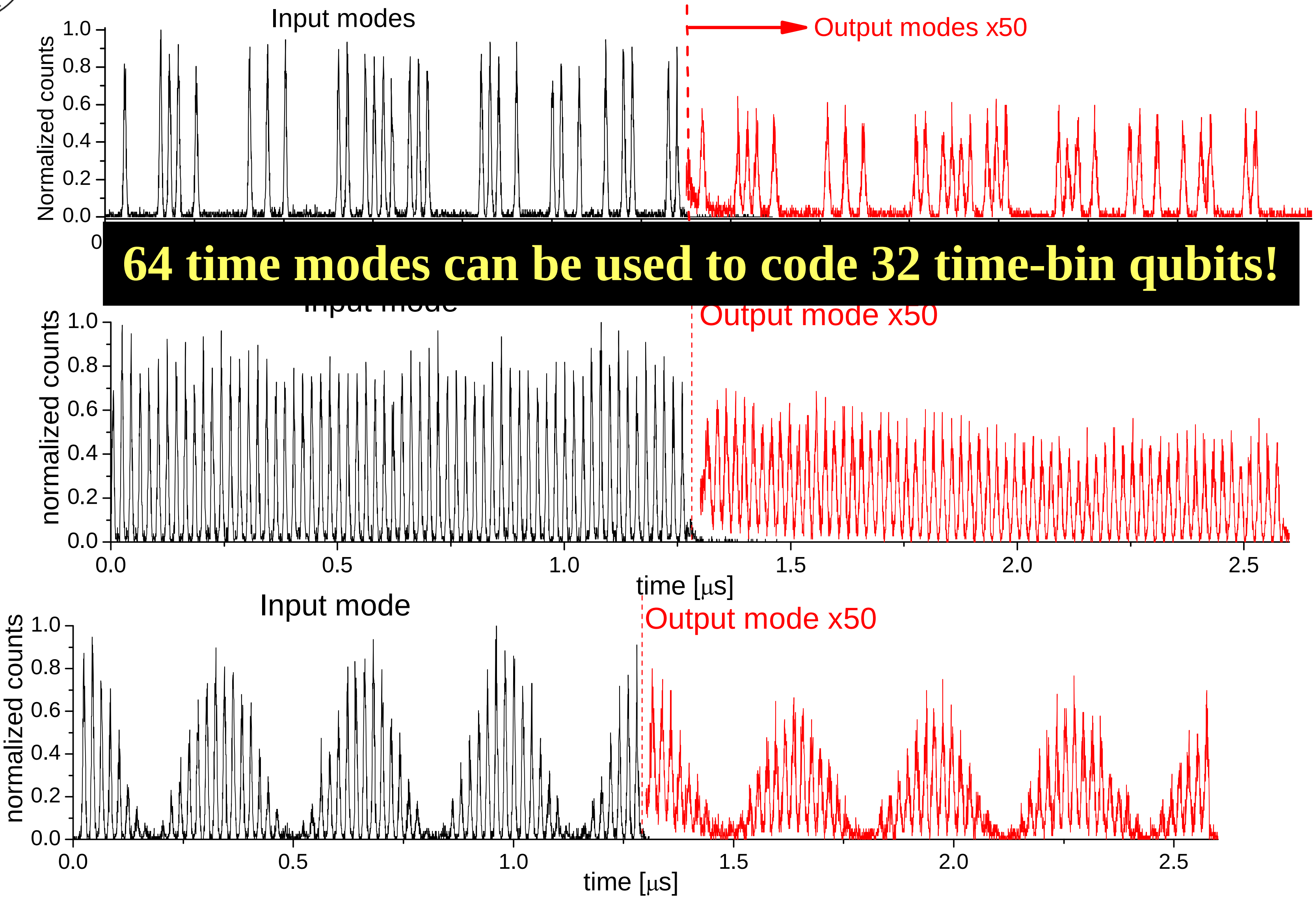



GAP Quantique Geneva University

# 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!**

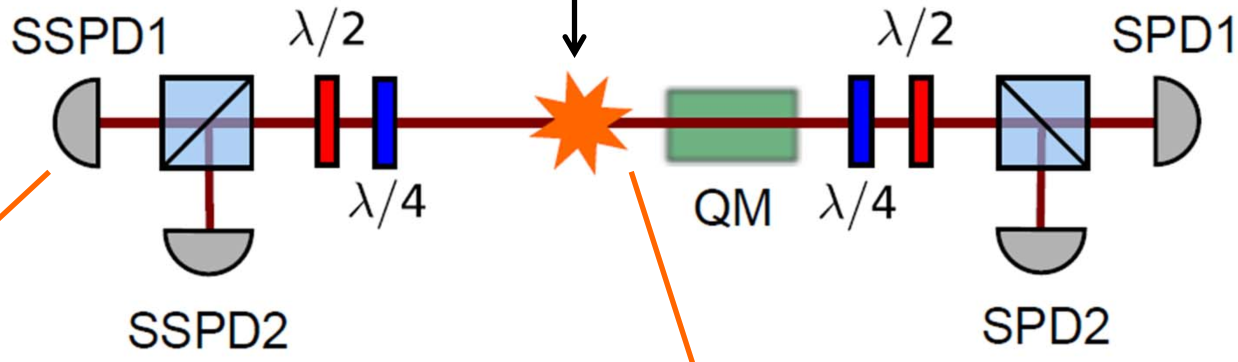
**GAP Quantique Geneva University**

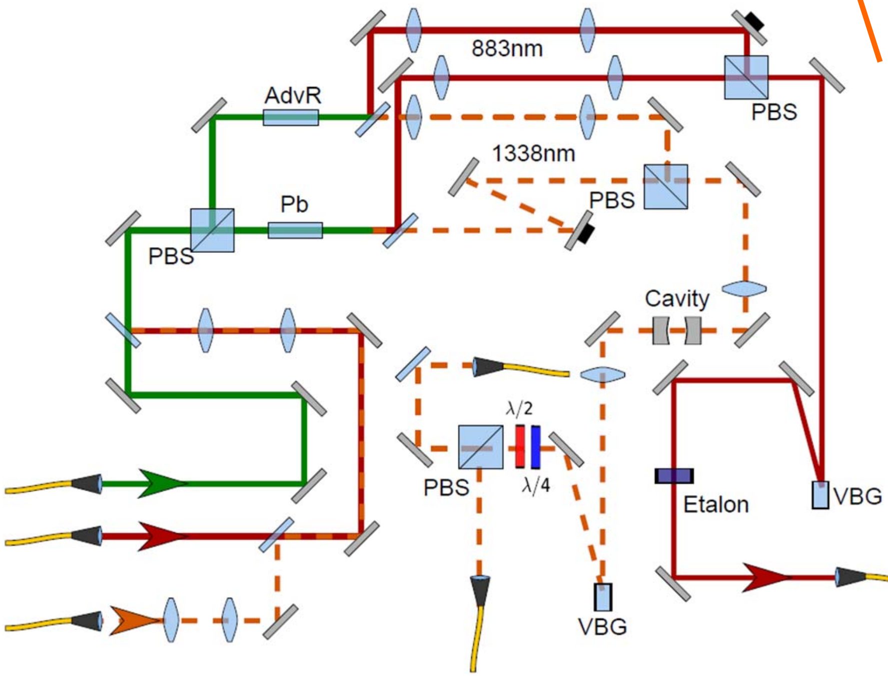
**I. Usmani et al., Nature Communications 1,12 (2010)**

# Entanglement-preserving quantum memory

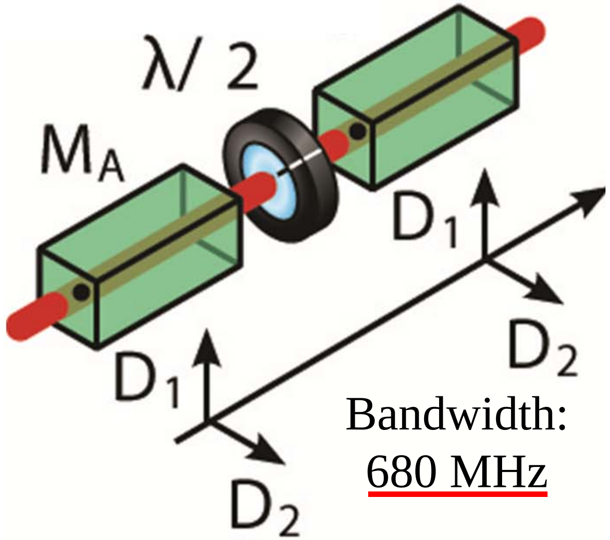
GAP Quantique Geneva University

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



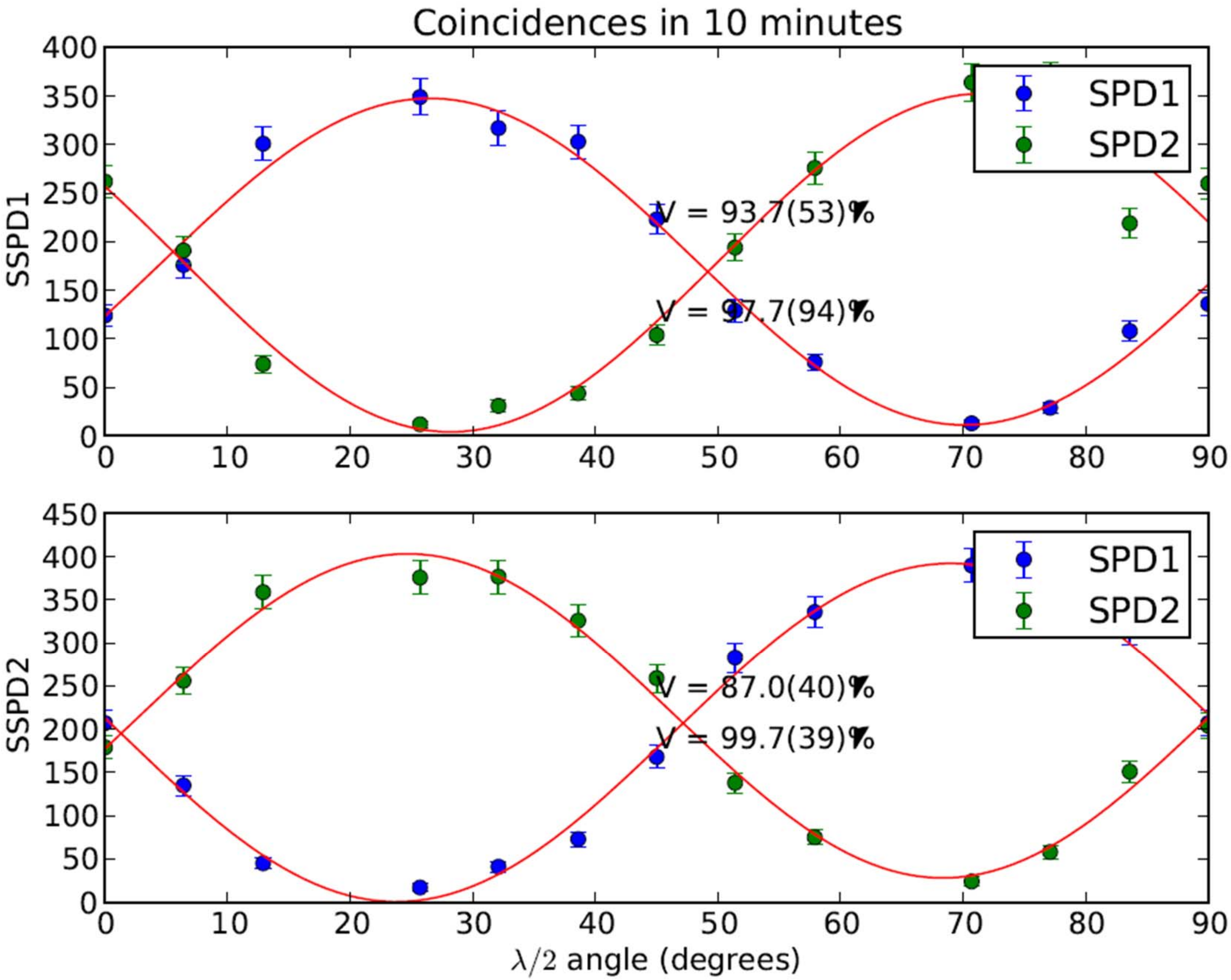




*to Quantum Memory then to measurement device*




Bandwidth:
680 MHz

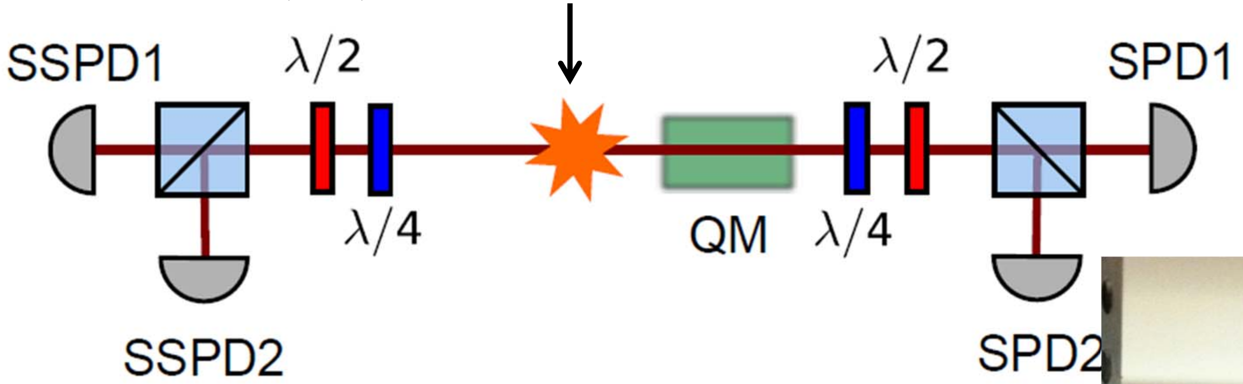
# Entanglement-preserving quantum memory

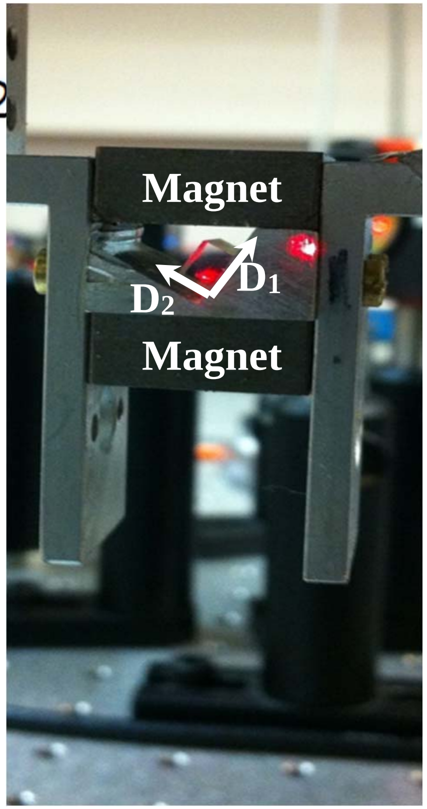



GAP Quantique Geneva University

# Entanglement-preserving quantum memory

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




**Using Bell test as Entanglement Witness**

$$E(A_1, B_1) = 0.68 \pm 0.06$$

$$E(A_1, B_2) = 0.51 \pm 0.06$$

$$E(A_2, B_1) = 0.54 \pm 0.06$$

$$E(A_2, B_2) = -0.79 \pm 0.08$$

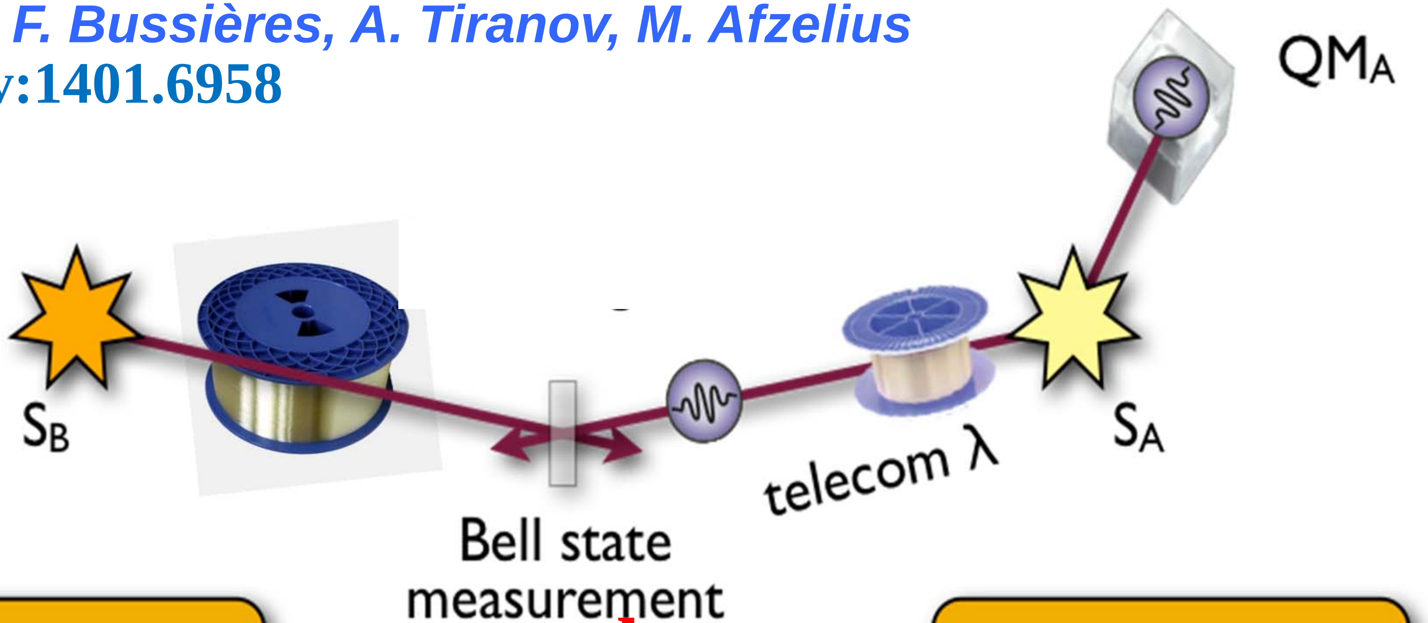
$$S = 2.52 \pm 0.13$$

**S larger than local bound of 2 ➡ Device-Independent Entanglement!**

**GAP Quantique Geneva University**

# Teleportation of a polarization qubit from a *weak coherent state*

*C. Clausen, F. Bussières, A. Tiranov, M. Afzelius et. al*. **arXiv:1401.6958**




$\alpha|H\rangle + \beta|V\rangle$

**sspd from NIST**

$|HH\rangle + e^{i\phi}|VV\rangle$

GAP Quantique Geneva University

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

**Partial Bell State Measurement and post-selected fidelity**

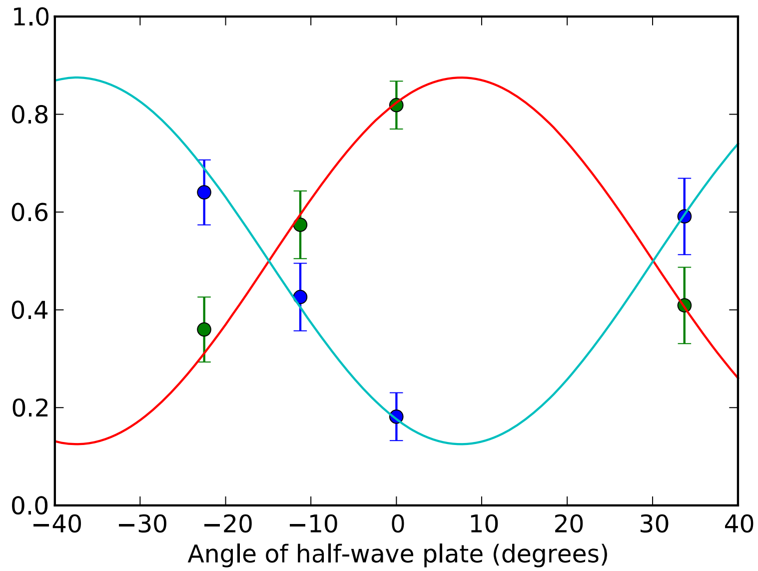
**F. Bussières, Ch.Clausen et al., arXiv:1401.6958**

***Tomographic reconstruction (short link)***

| State | Fidelity (%) |
|---|---|
| $\vert$ | |
| $\vert$ | |
| $\vert$ | |
| $\vert$ | |
| Ave | |

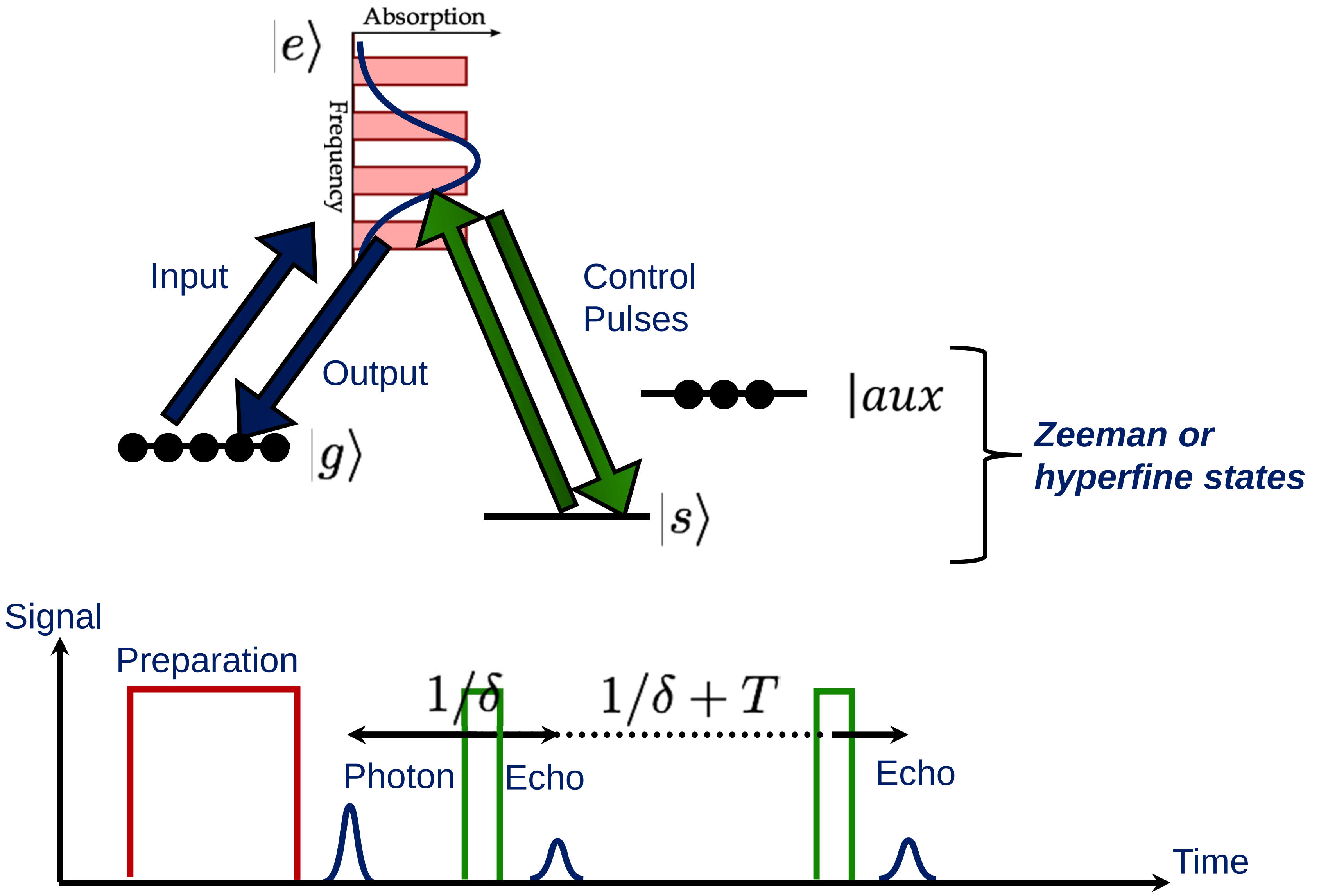
***Fidelit (2x12.***

**Analysis on a great circle of**




GAP Quantique Geneva University

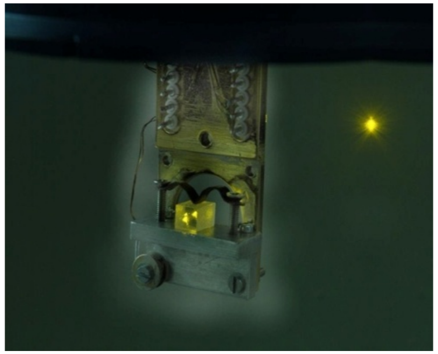
# What do we need to do the full AFC memory scheme?



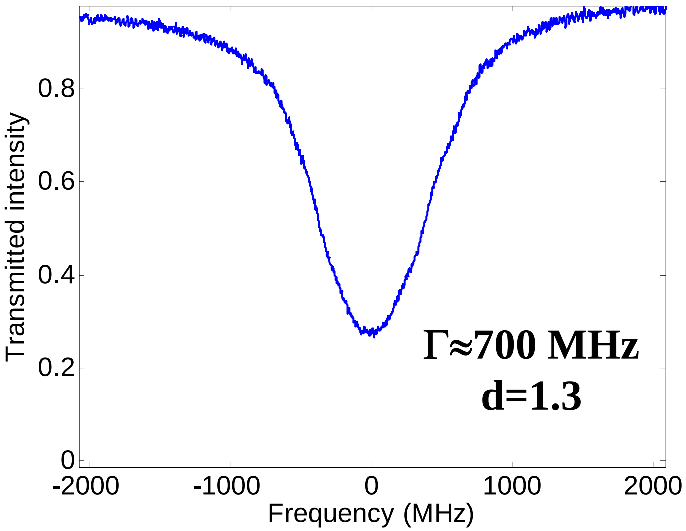

GAP Quantique Geneva University

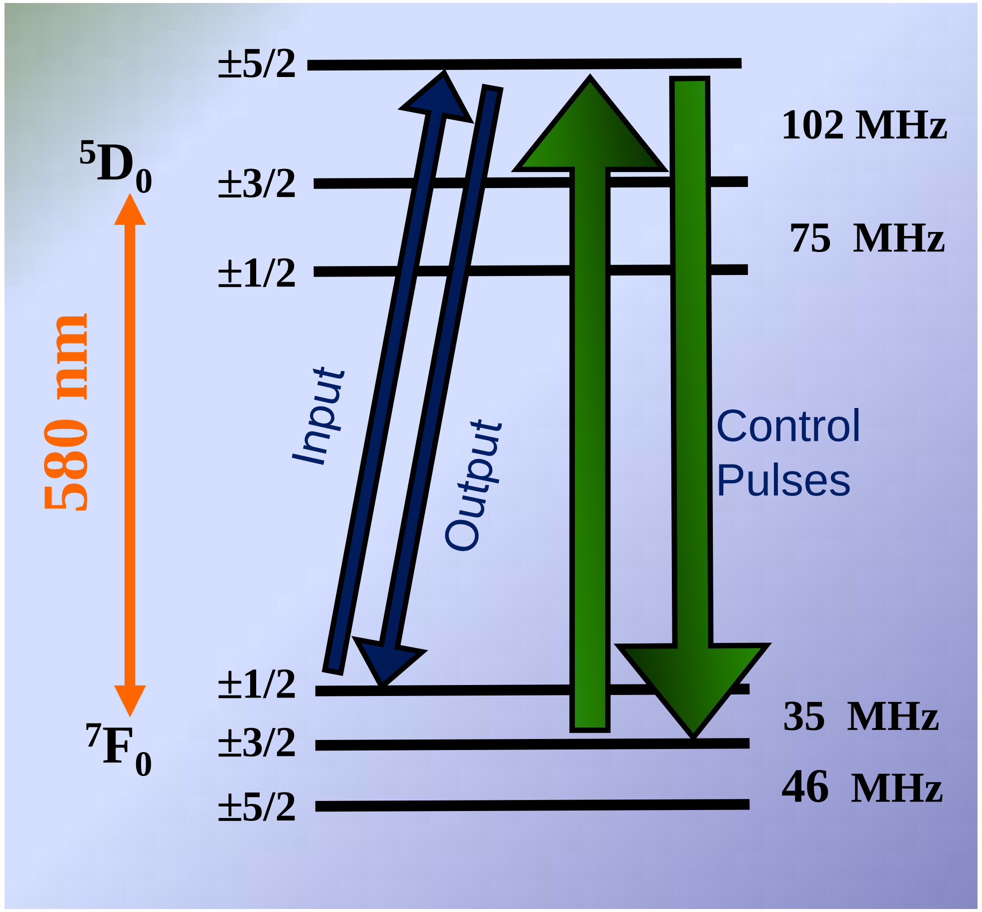
# Some Basic $^{151}Eu^{3+}:Y_2SiO_5$ Spectroscopy

GAP Quantique Geneva University



*Inhomogeneous absorption spectrum*
**(100 ppm $^{153}$Eu)**




*N. Timoney, I. Usmani, P. Jobez, MA, N. Gisin, arXiv:1301.6924*
*PRA 88, 02324 (2013)*

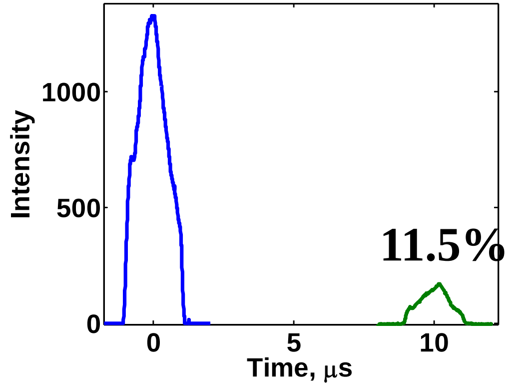
**-Excited state life time 2 ms**
**- Max. absorption coefficient 3-4 $cm^{-1}$**
**- Spin coherence time 15 ms for $^{151}$Eu (B=0)**

# Towards high SNR and long-lived Quantum Memory
# Work in progress...

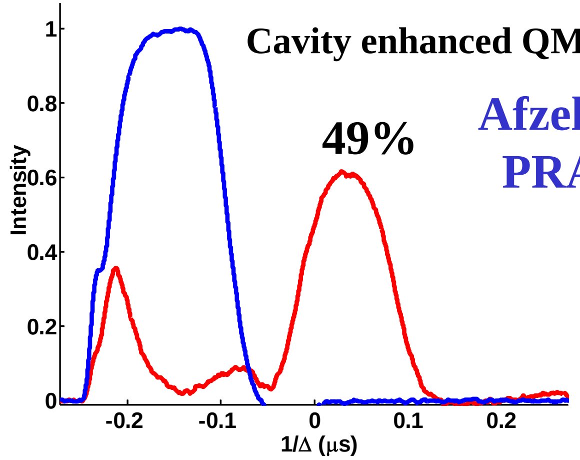
GAP Quantique Geneva University

## 1. Higher two-level AFC efficiency Method 1

Frequency stable laser, optimized comb preparation

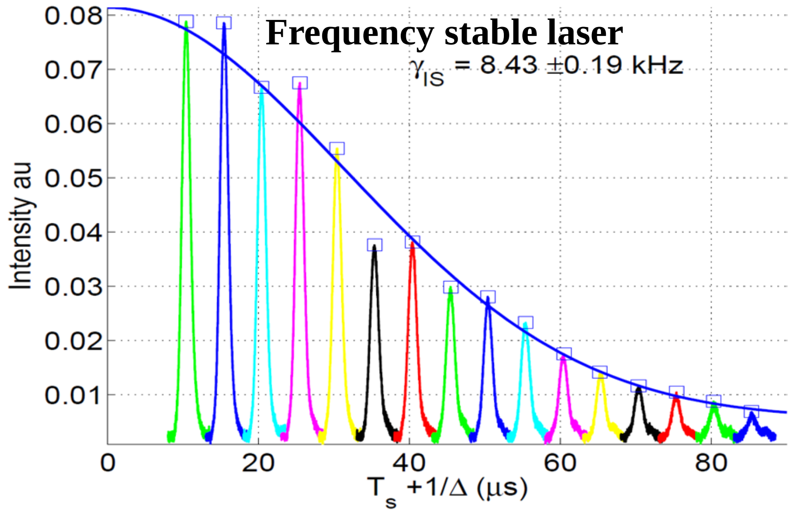



## 2. Higher two-level AFC efficiency Method 2

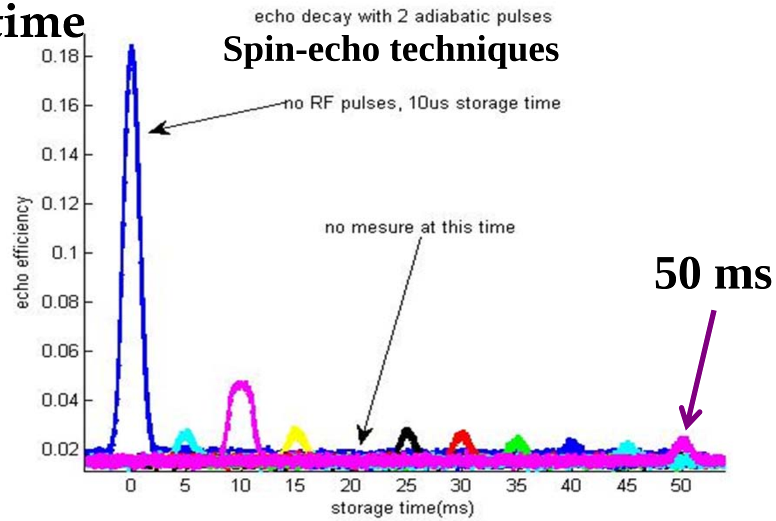



Afzelius & Simon
PRA 82, 022310 (2010)

## 3. Longer two-level AFC storage time




## 4. Milliseconds spin-wave storage time

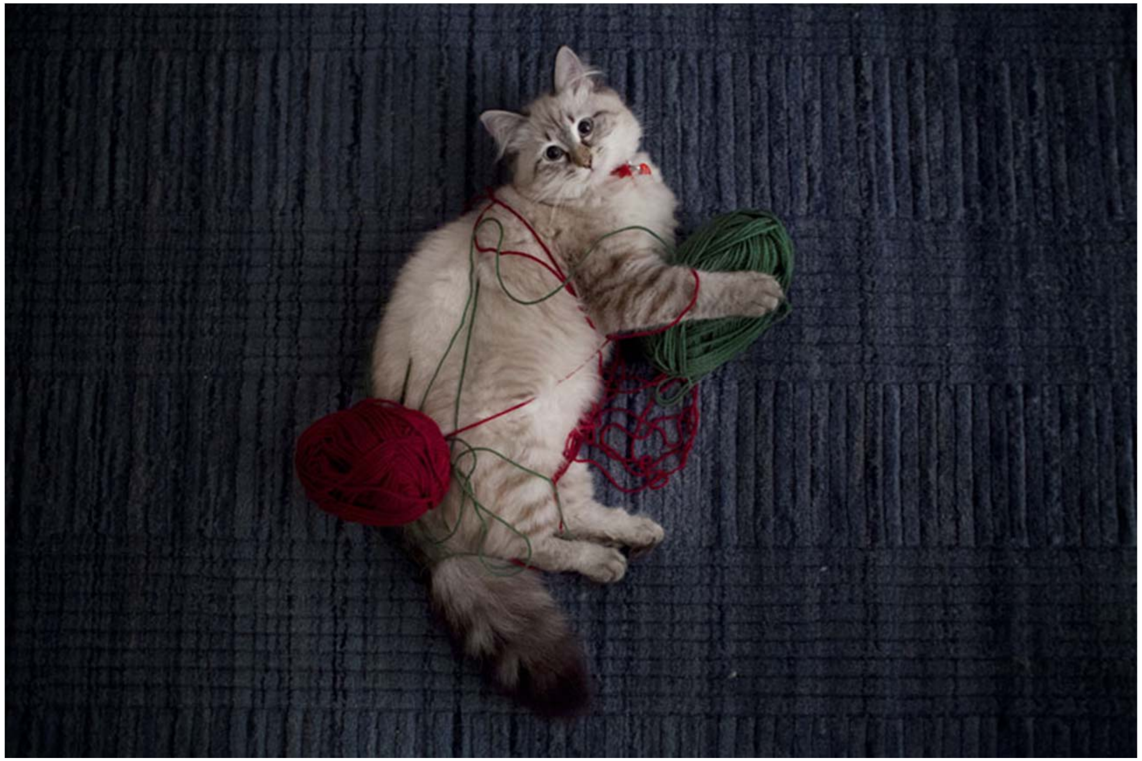


GAP Quantique Geneva University

# 3. Large Entanglement

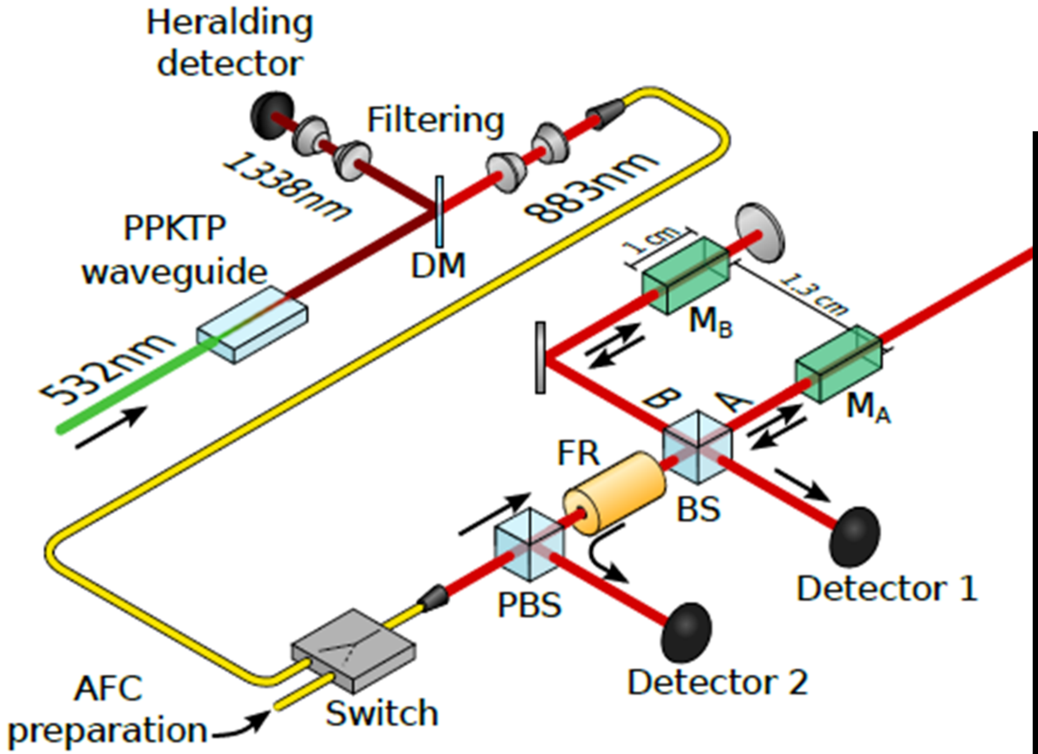

**Natalia Bruno, Anthony Martin, Pavel Sekatski, Nicolas Sangouard, Rob Thew and Nicolas Gisin**

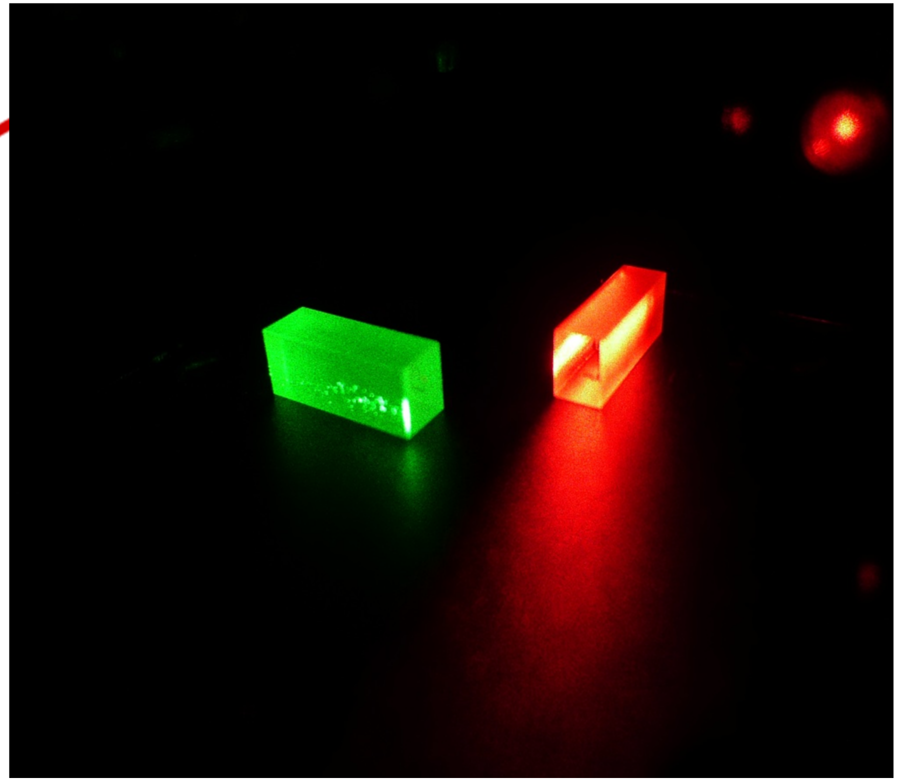
Group of Applied Physics
Geneva University, Switzerland

# Do these entangled crystals count as macroscopic entanglement ?

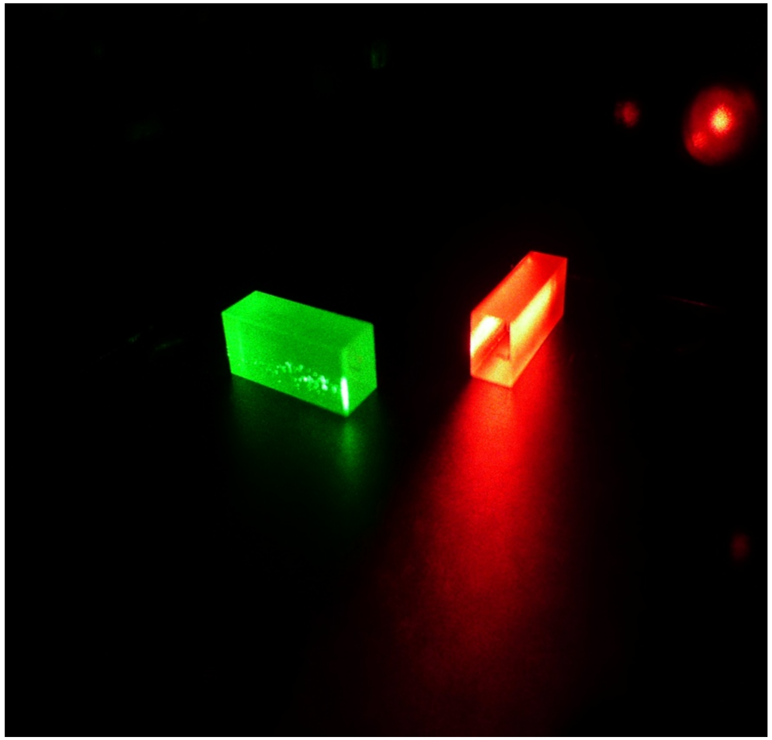
**Nature Photonics**
**<u>6</u>, 234-7, 2012**



# What is macroscopic ?
# What is quantum ?

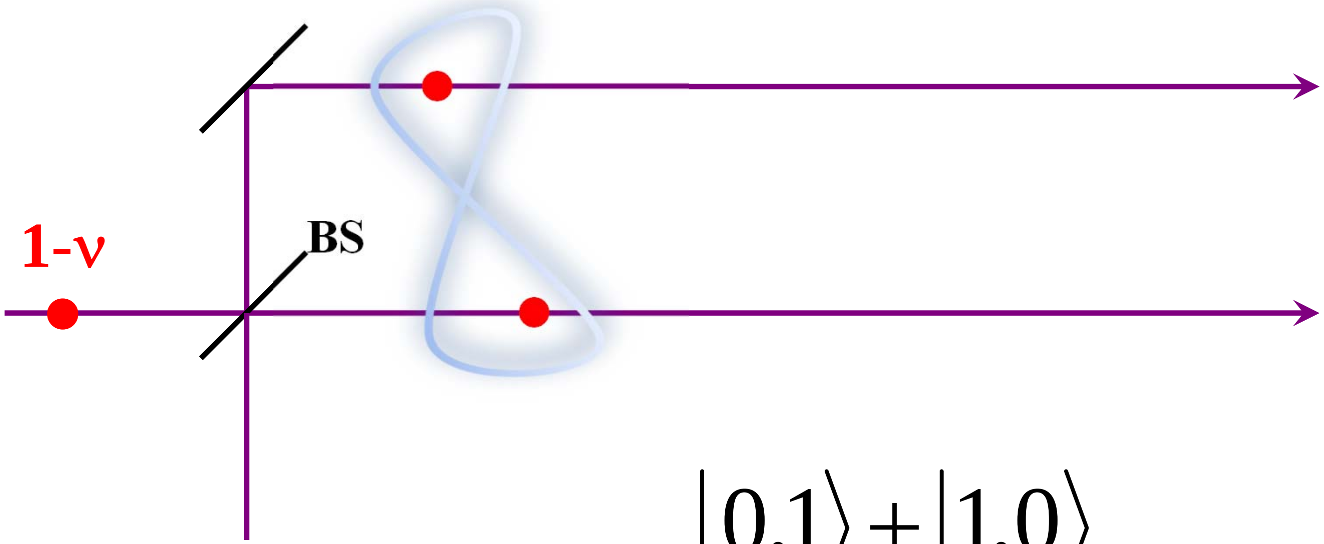
- Do these 2 crystals count as large entanglement?
  No !
- Billions of ions in a macroscopic object, but "only" one - delocalized - excitation
- Quantum = entanglement.



Nature Photonics 6, 234-7, 2012

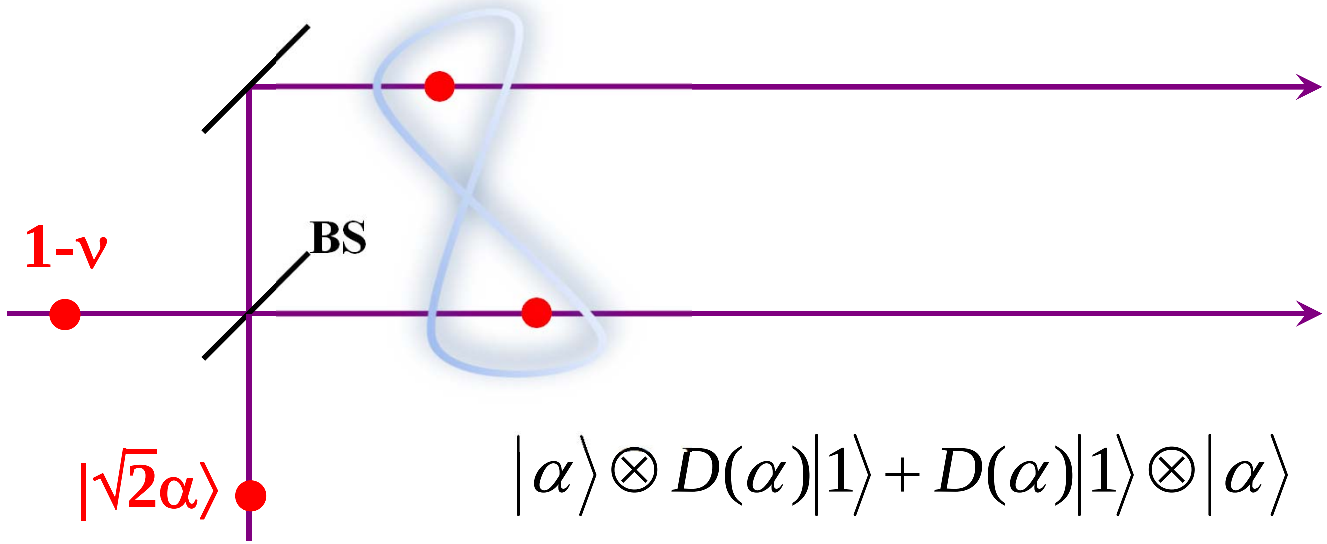
# Example: 1-photon entanglement






$$|0,1\rangle + |1,0\rangle$$

# Example: displaced 1-ν entanglement




$$\left|\alpha\right\rangle \otimes D(\alpha)\left|1\right\rangle + D(\alpha)\left|1\right\rangle \otimes \left|\alpha\right\rangle$$

**The components of this entangled state can easily be distinguished using classical detectors because** $\Delta n_{D(\alpha)|1\rangle} \approx 3\,\Delta n_{|\alpha\rangle}$

**Pavel Sekatski, Nicolas Sangouard et al., PRA 86, 060301 (2012)**

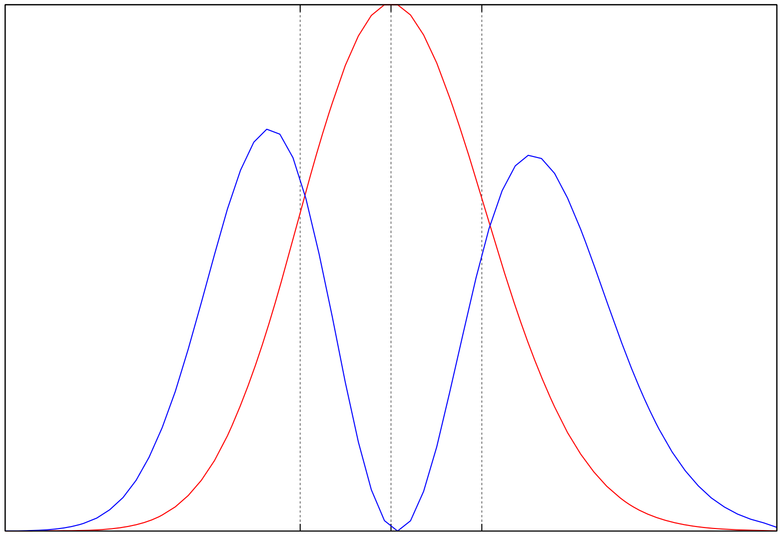
GAP Quantique Geneva University

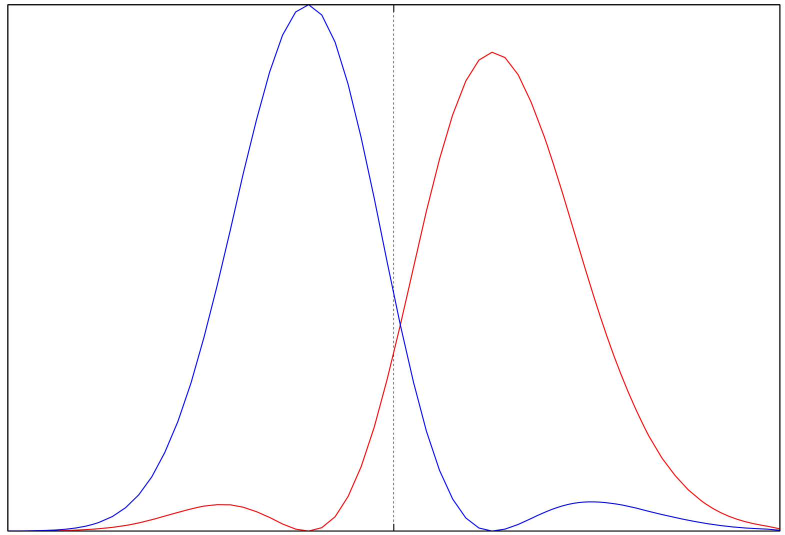
# Distinguishability

$$|0\rangle\otimes D(\alpha)|1\rangle + |1\rangle\otimes|\alpha\rangle \quad = |+\rangle\otimes\Psi_{-} + |-\rangle\otimes\Psi_{+}$$

Where $\Psi_{\pm} = D(\alpha)|1\rangle \pm |\alpha\rangle$

**Photon number distribution**

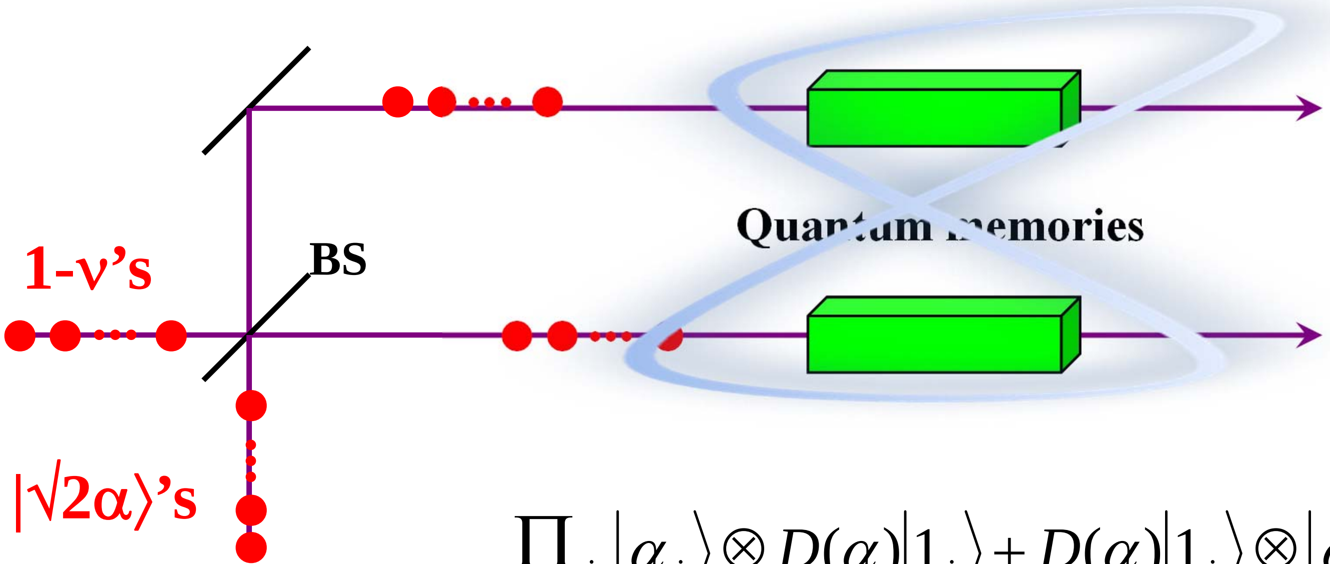


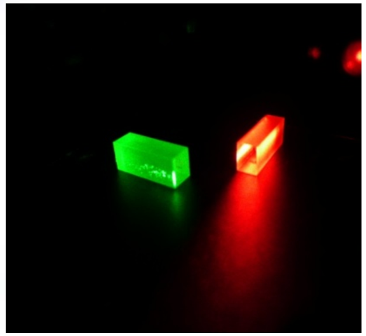


For $|\alpha|^2 >> \Delta$, Pguess $\cong 74\%$ For $|\alpha|^2 >> \Delta$, Pguess $\cong 89\%$

**Pavel Sekatski, Nicolas Sangouard et al., PRA 86, 060301 (2012)**

# Toward truly Large Entanglement



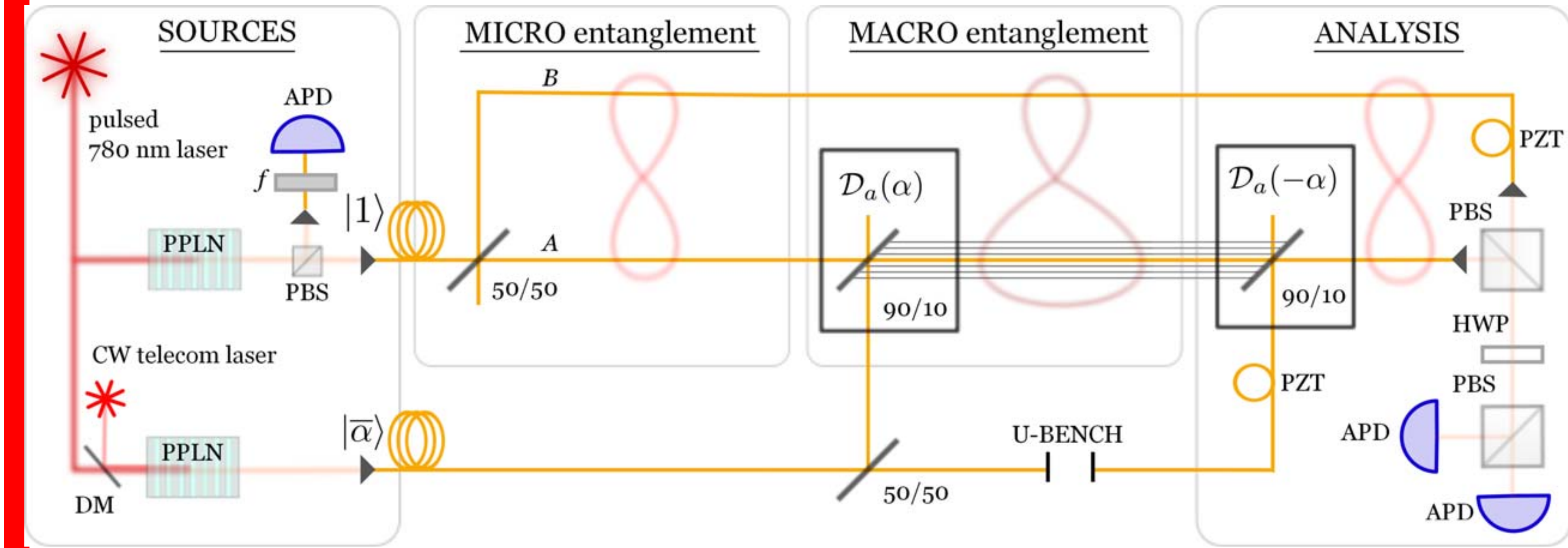
$$\Pi_j \left|\alpha_j\right\rangle \otimes D(\alpha)\left|1_j\right\rangle + D(\alpha)\left|1_j\right\rangle \otimes \left|\alpha_j\right\rangle$$

**Inside the crystal, no longer a product state, But a complex sort of Dicke state with involved Phase relations.**

**billions of atoms**
**thousands of excitations**
**hundreds of e-bits**

GAP Quantique Geneva University

# Experiment: demonstrate Large Size Entanglement

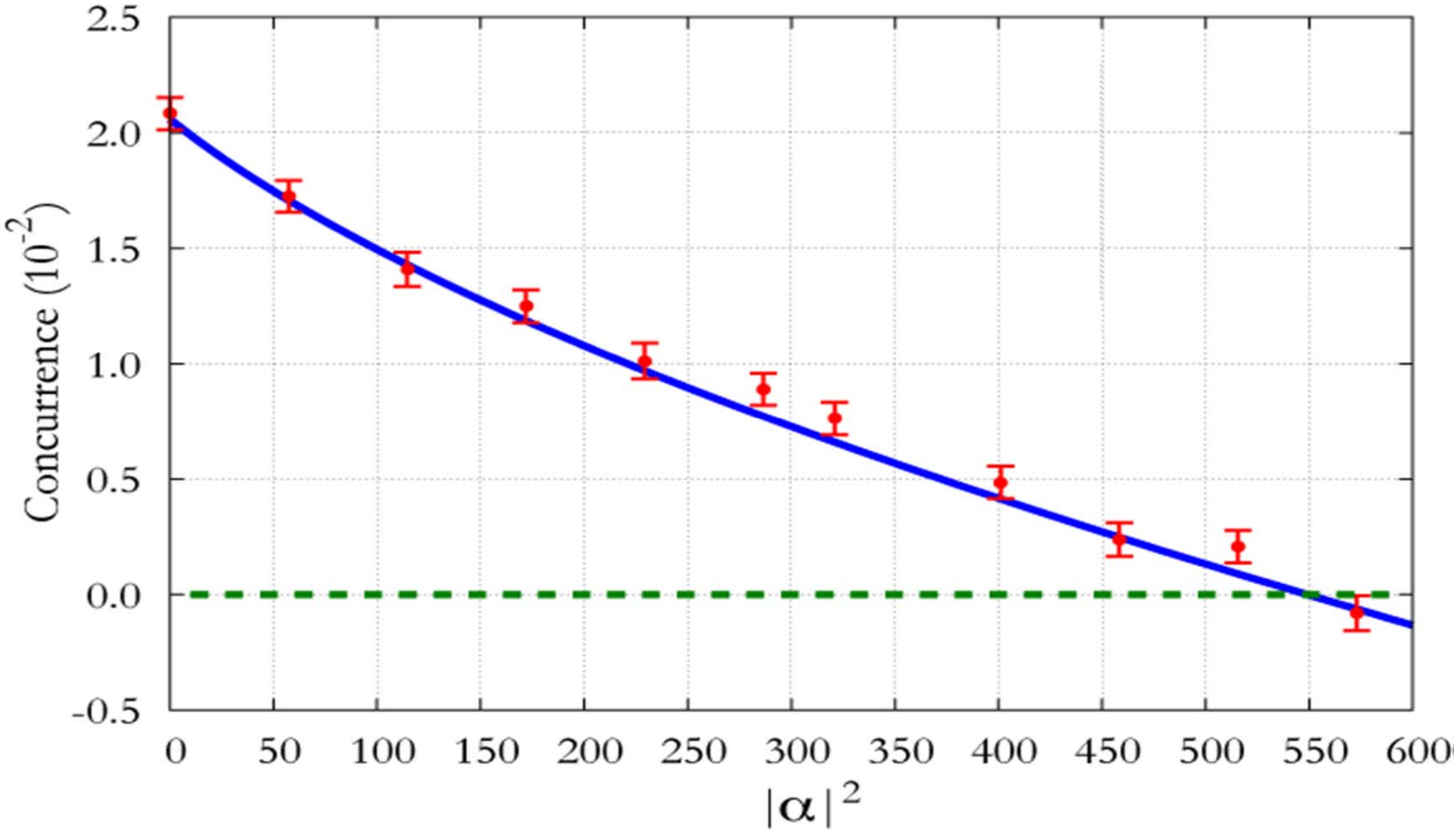



*N.Bruno et al. , arXiv:1212.3710, Nature Physics 9, 545 (2013)*

# Experiment (one mode, no crystal): Result

**We measured the concurrence C (a measure of entanglement):**

$$C \geq V(p_{10} + p_{01}) - 2\sqrt{p_{00}p_{11}}$$




*N.Bruno et al., arXiv:1212.3710, Nature Physics 9, 545 (2013)*
*A.I. Lvovski et al., Nature Physics 9, 541 (2013)*

GAP Quantique Geneva University

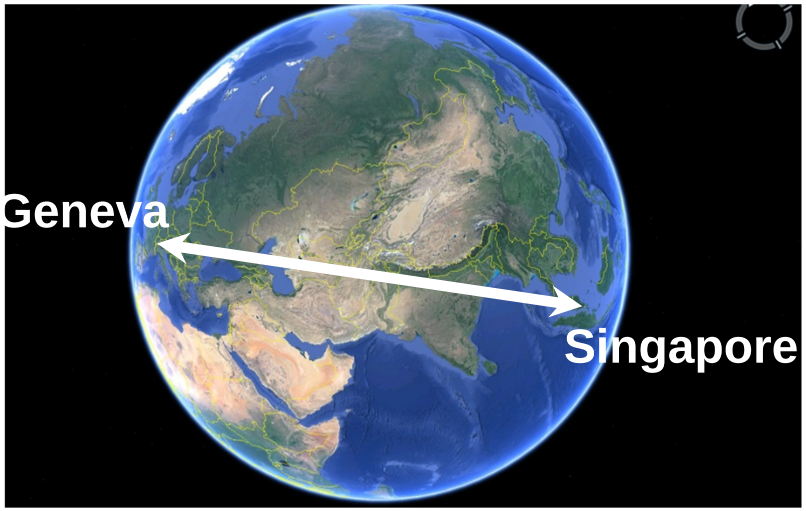
GAP Quantique Geneva University

# Conclusions

- Quantum cryptography exists since years, though only in niche markets.
- z > x+y $\Rightarrow$ Panic today !


- Trusted nodes make a lot of sense.
- Quantum repeaters require teleportation and quantum memories.

- Decoy detectors are practical again "quantum hacking" on detectors
- Large entanglement is fascinating Nature Physics 9, 545 (2013)




- Relativistic bit commitment: PRL 111, 180504 (2013)