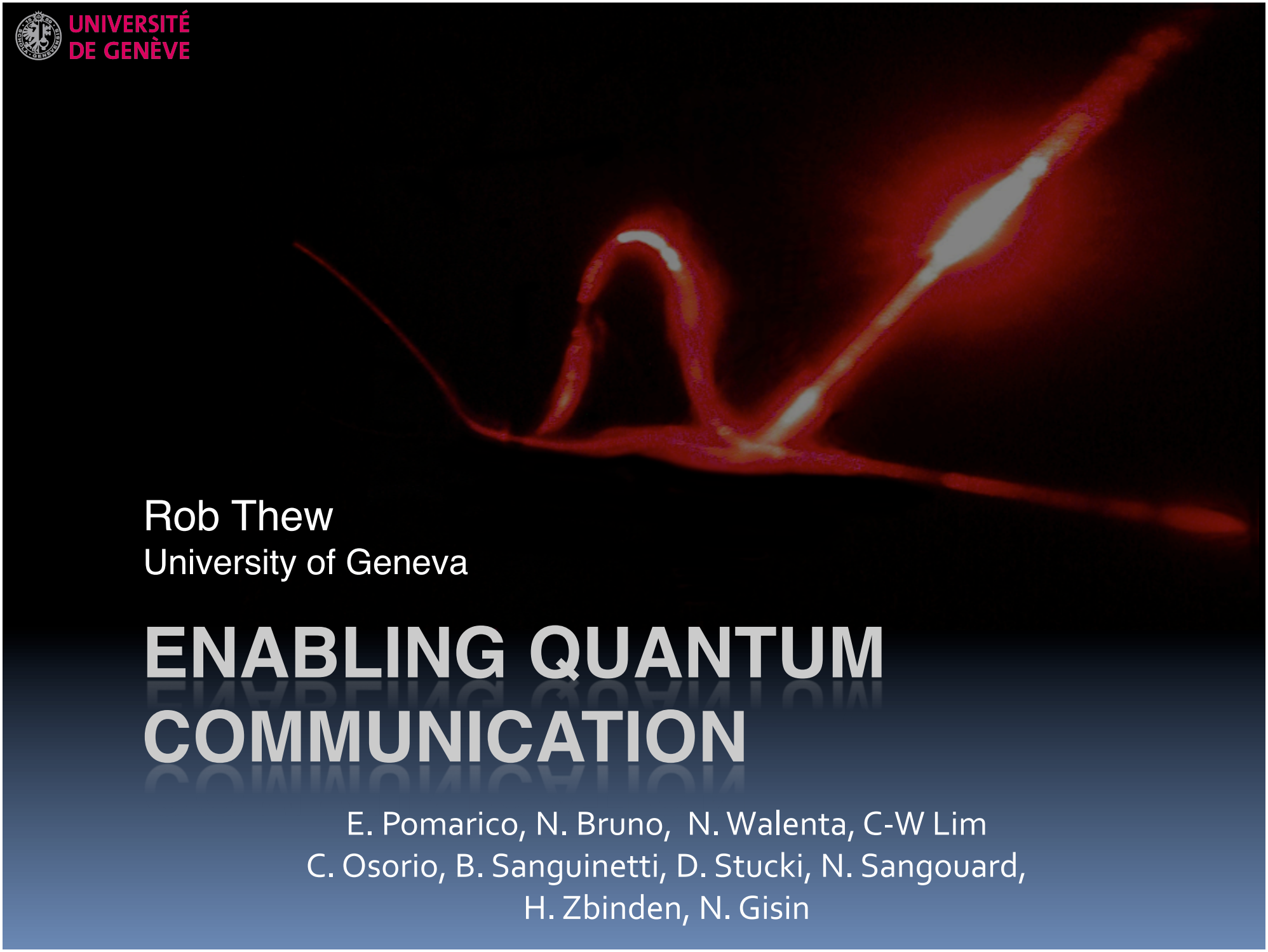


UNIVERSITÉ DE GENÈVE

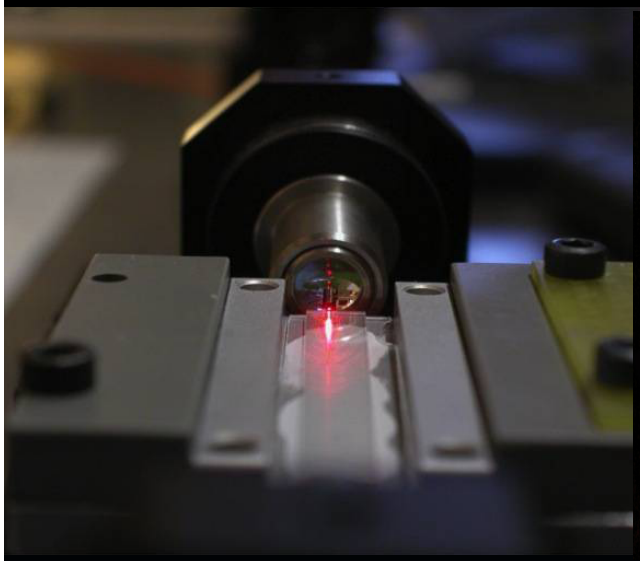
Rob Thew
University of Geneva

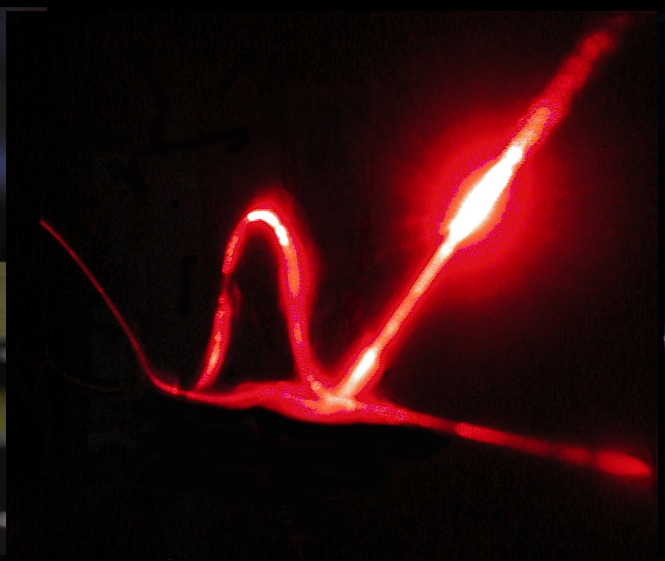
ENABLING QUANTUM COMMUNICATION

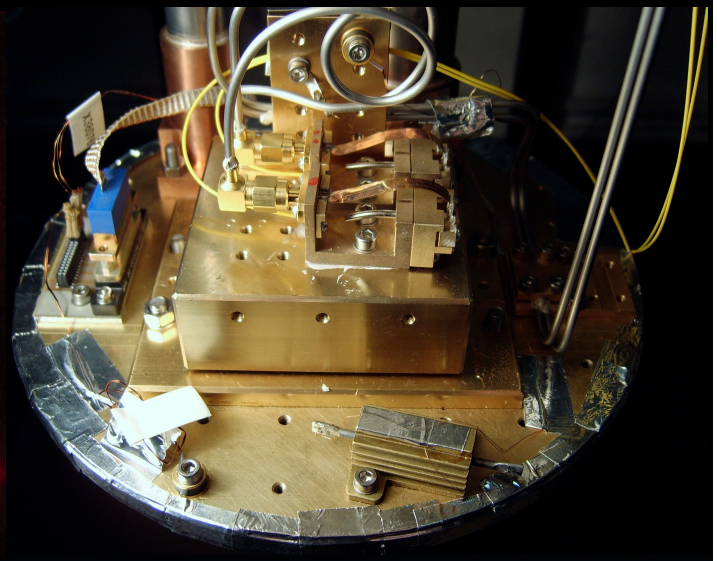
E. Pomarico, N. Bruno, N. Walenta, C-W Lim
C. Osorio, B. Sanguinetti, D. Stucki, N. Sangouard,
H. Zbinden, N. Gisin

UNIVERSITÉ DE GENÈVE

Enabling Technologies for Quantum Communication







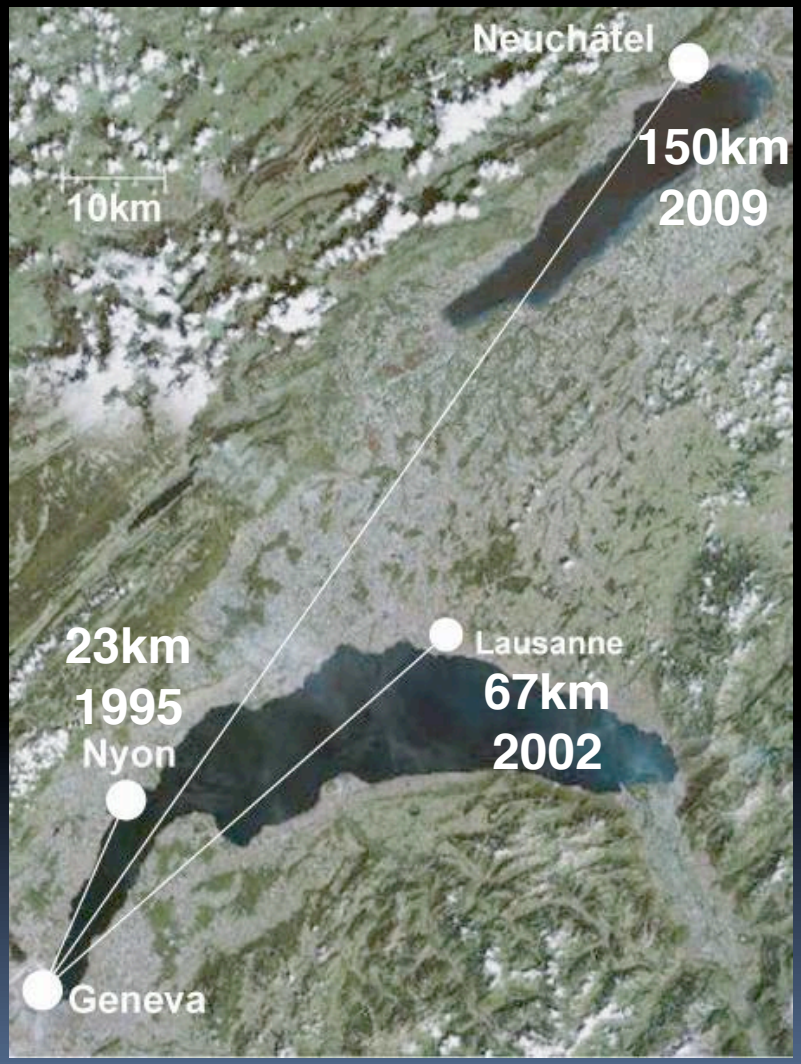
Sources

Interfaces

Detectors

UNIVERSITÉ DE GENÈVE

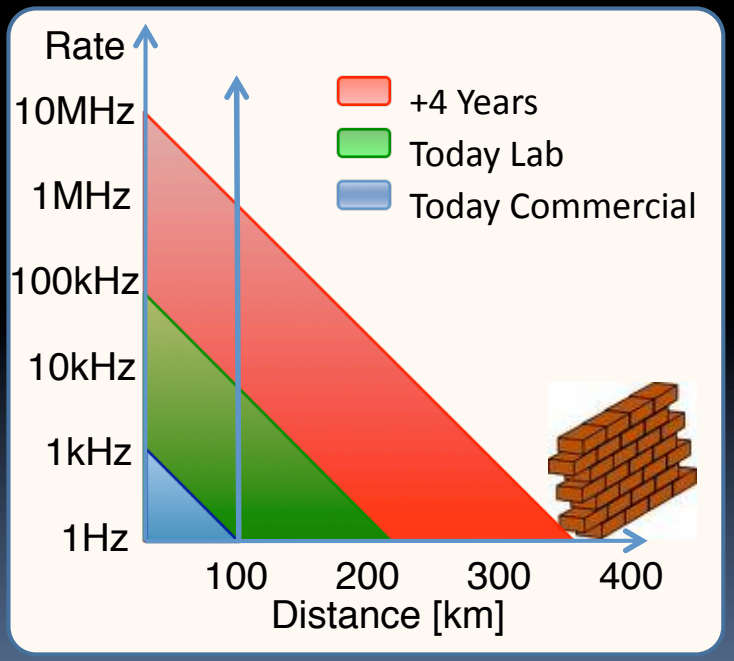
Quantum Communication Limitations



→ 2016: ~300-450km …. But….

¿ 10GHz single photon source
+ perfect detectors (& everything)?
< 1Hz @ 500km !

1 bit @ 1000km? ~ 300 years …



UNIVERSITÉ DE GENÈVE

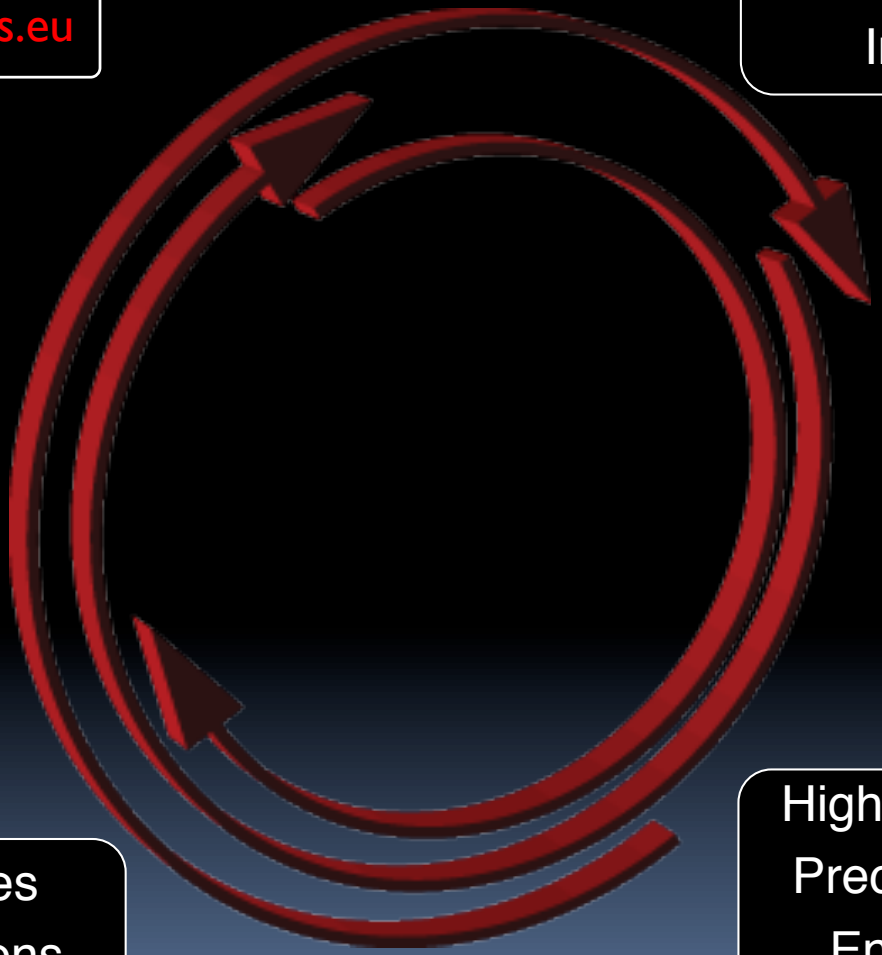
Quantum Communication Directions

Weak Pulse QKD

P2P / WDM / Networks
High Speed Electronics
InGaAs/InP APDs

http://quantumrepeaters.eu

QuReP



Quantum Repeaters

Quantum Memories
Narrow Band Photons
Entanglement based

Device Independent QKD

High Efficiency/Low Loss
Precision Q engineering
Entanglement based

UNIVERSITÉ DE GENÈVE

The next 20+ minutes…

- Applied QKD
  - Networks
  - Multiplexing
  - Faster & Farther
  - Detectors
    - InGaAs/InP Rapid Gating APDs

Weak pulse schemes

- Device Independent QKD
  - Heralded Qubit Amplification
  - Faithful Entanglement Swapping

Entanglement -based schemes

UNIVERSITÉ DE GENÈVE

Weak-Pulse QKD I

Networks, based on the trusted nodes, are a highly attractive business model …
they also provide an avenue for extending distances

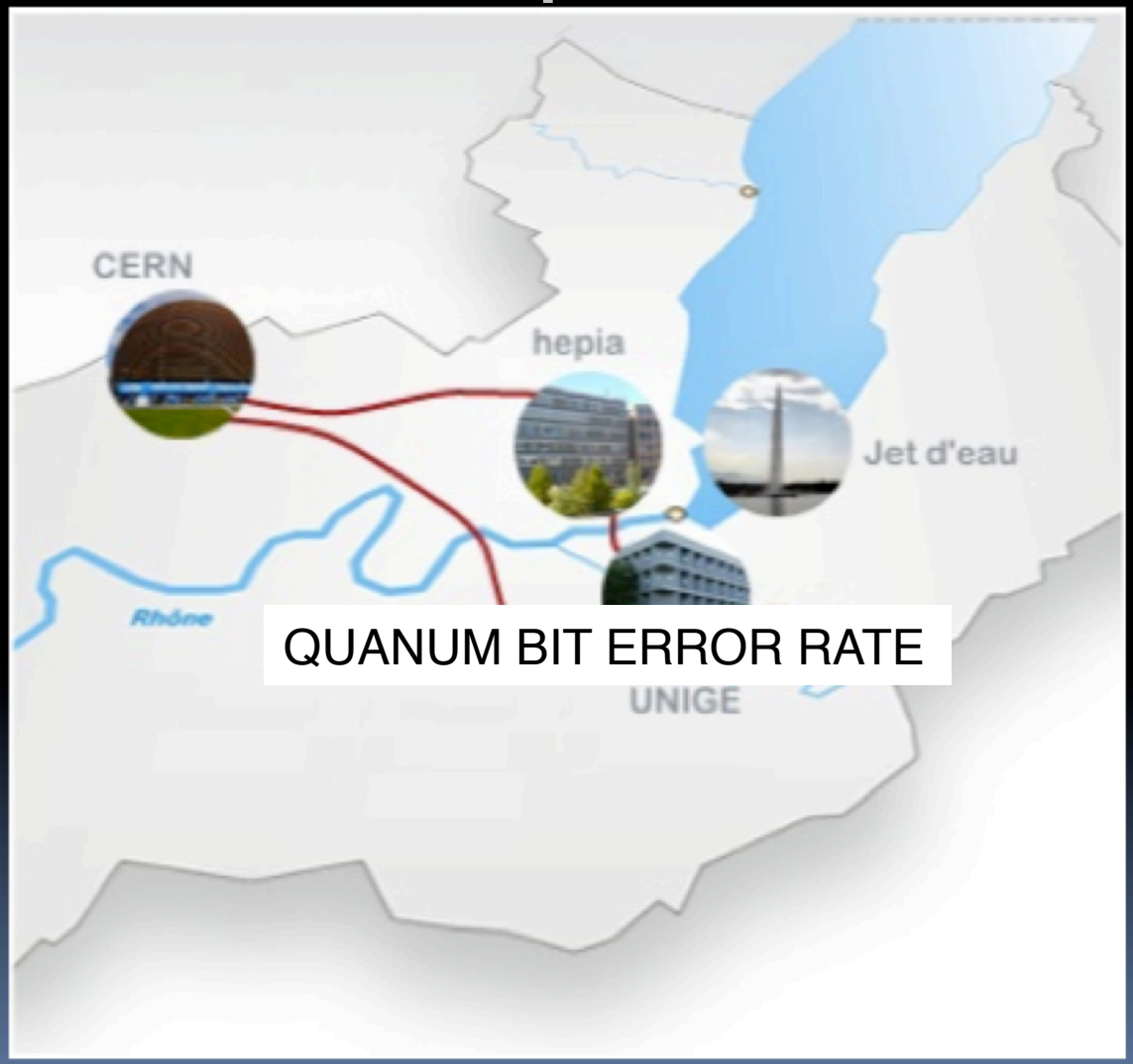
2010 FIFA World Cup
South Africa

UNIVERSITÉ DE GENÈVE

SwissQuantum Network

swiss QUANTUM

> 1.5 Years Operation: Online!



QUANUM BIT ERROR RATE

IDQ FROM VISION TO TECHNOLOGY

Hes·so Haute Ecole Spécialisée de Suisse occidentale University of Applied Sciences Western Switzerland

CERN

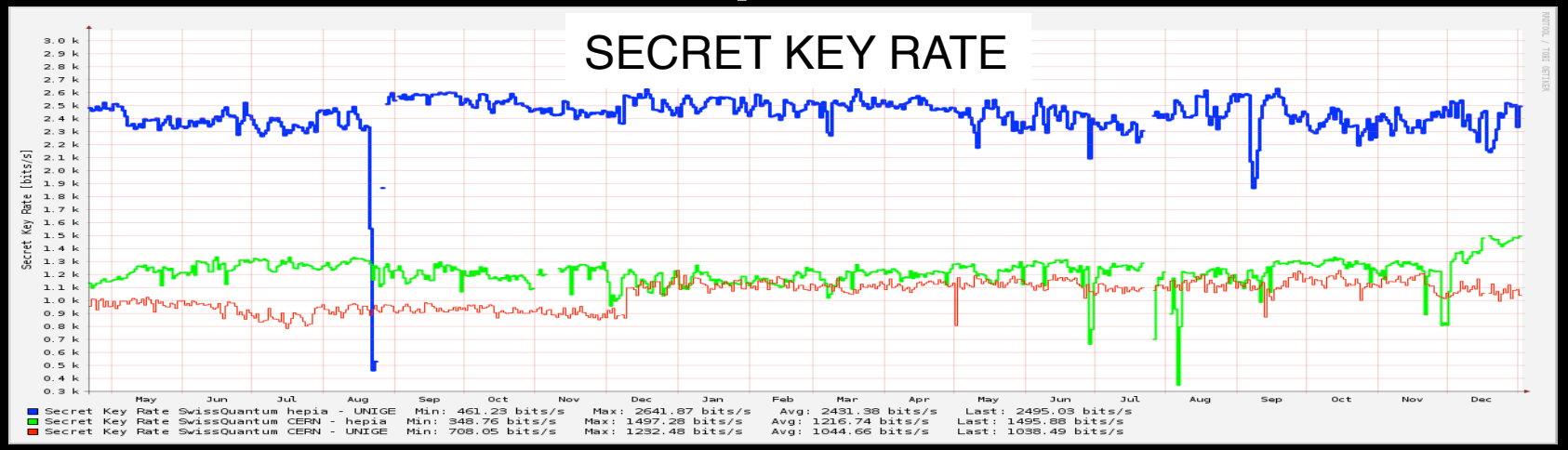
www.swissquantum.com

UNIVERSITÉ DE GENÈVE

SwissQuantum Network

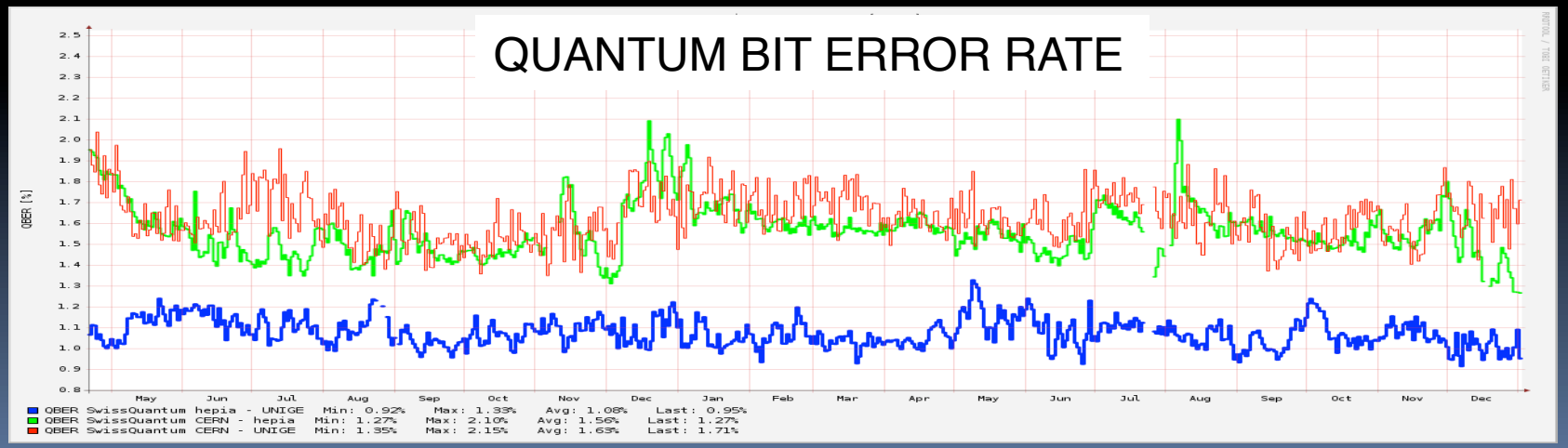
SWISS QUANTUM

> 1.5 Years Operation: Online!



April 2009

January 2011



IDQ FROM VISION TO TECHNOLOGY

Hes·so Haute Ecole Spécialisée de Suisse occidentale University of Applied Sciences Western Switzerland

CERN

www.swissquantum.com

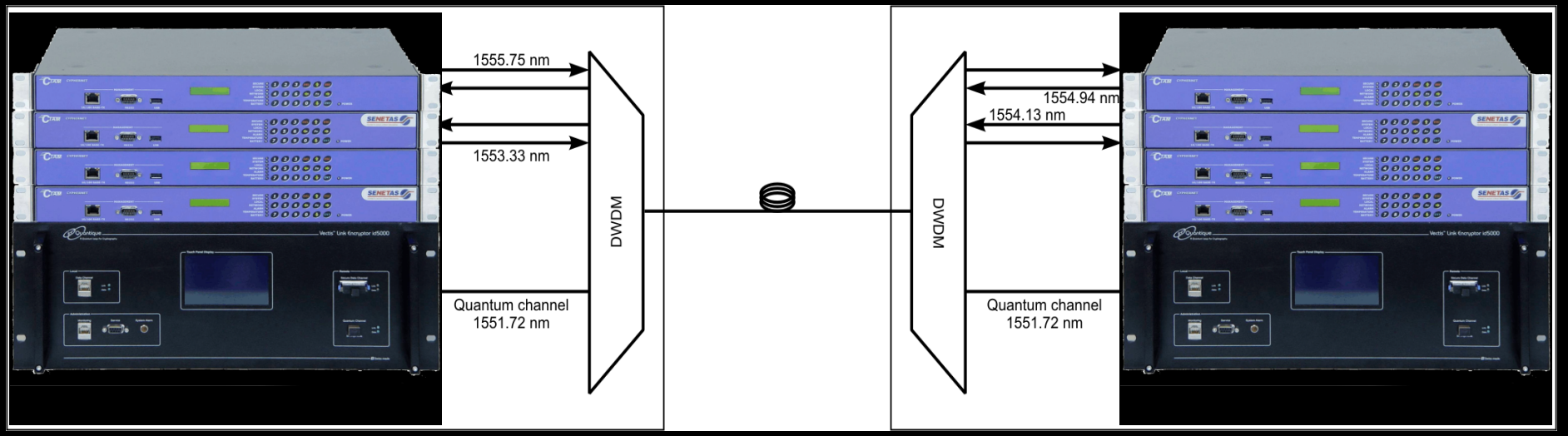
UNIVERSITÉ DE GENÈVE

Weak-Pulse QKD II

Multiplexing – Coarse/Dense/reconfigurable wavelength multiplexing, …

Fibre is expensive – need to put all the classical and quantum communication together

Qcrypt: Classical + Quantum Multiplexing



UNIVERSITÉ DE GENÈVE

ETH Zürich

Hes·so
Haute Ecole Spécialisée de Suisse occidentale
University of Applied Sciences Western Switzerland

IDQ
FROM VISION TO TECHNOLOGY

High-speed **Q**uantum Key Distribution

(1Mb/s OTP)

40 – 100Gbps en**CRYPT**ion

WDM for QKD

nano-tera.ch

FNSNF
Swiss National Science Foundation

UNIVERSITÉ DE GENÈVE

WDM-QKD – Managing the Noise

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

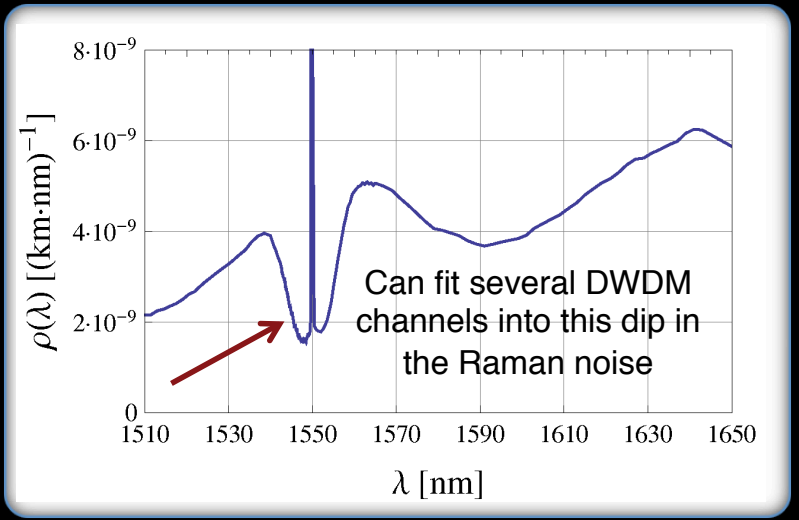
Channel crosstalk - "off-band noise" due to finite channel isolation → Filtering sufficient

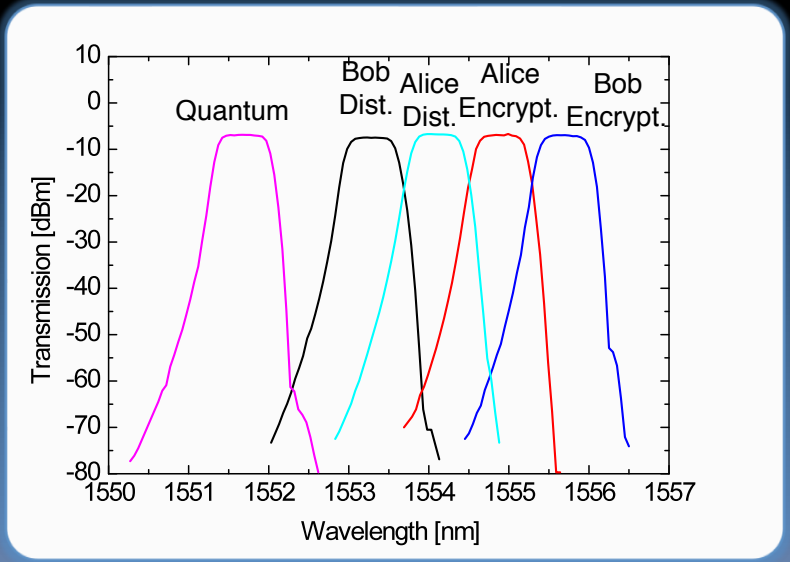
Raman

– We can easily measure and model the WDM impact for a QKD system

$$P_{forward} = P_{out} p(\lambda) \Delta\lambda L$$

$$P_{backward} = P_{out} p(\lambda) \Delta\lambda \frac{sinh(\alpha L)}{\alpha}$$





Four-wave mixing

– $\chi^{(3)}$ –process generates new frequencies by

– Stimulated processes eliminated by channel configuration

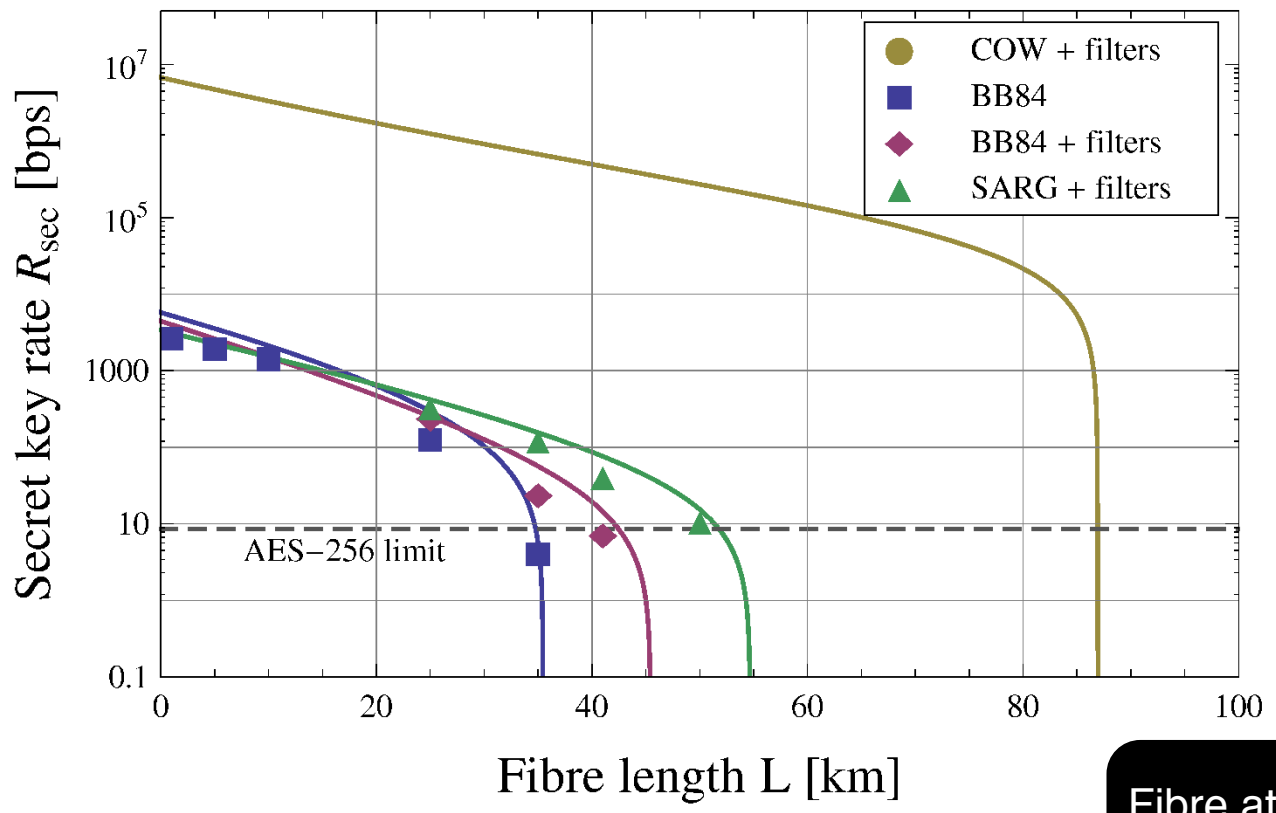
– Spontaneous processes can be neglected

$$\nu_- = 2\nu_2 - \nu_1$$
$$\nu_+ = 2\nu_1 - \nu_2$$
$$2\nu_1 = \nu_+ + \nu_-$$

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

UNIVERSITÉ DE GENÈVE

WDM-QKD: Experimental Results



Fibre 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

UNIVERSITÉ DE GENÈVE

Weak-Pulse QKD III

Faster & Farther – bottleneck has traditionally been detection, but we also require A LOT of integrated electronics

D. Stucki, *et al.,* Opt. Exp. 17, 13326 (2009)

UNIVERSITÉ DE GENÈVE

Weak-Pulse QKD III

Faster & Farther – bottleneck has traditionally been detection, but we also require A LOT of integrated electronics

D. Stucki, *et al.,* Opt. Exp. 17, 13326 (2009)

UNIVERSITÉ DE GENÈVE

InGaAs/InP APD = Applied

Compact,

Robust,

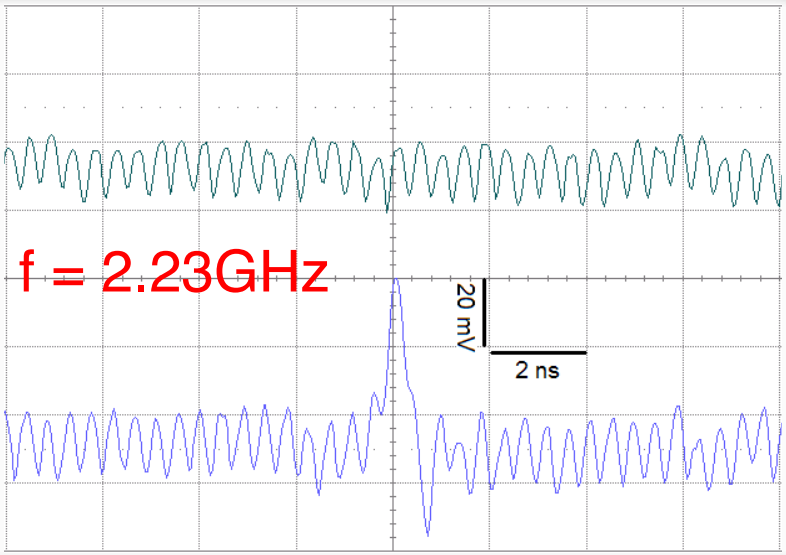
Thermo-electrically cooled

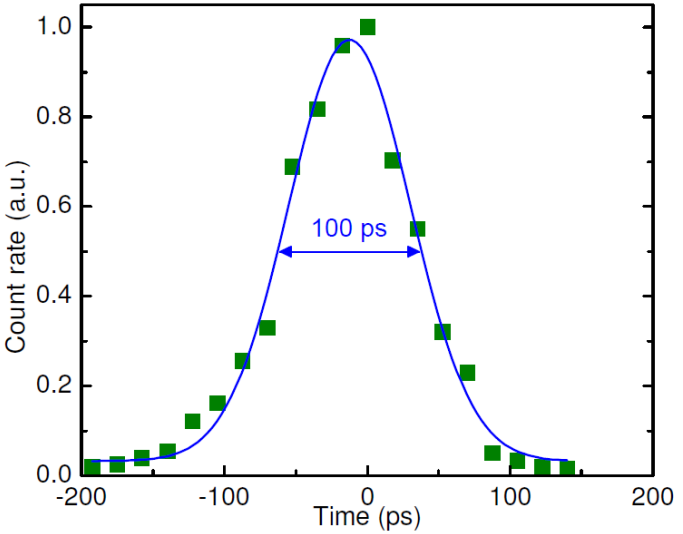
- But … InGaAs/InP are
  - SLOW
  - They suff
    Afte
  - are noisy
  - Did I mention that they are slow?

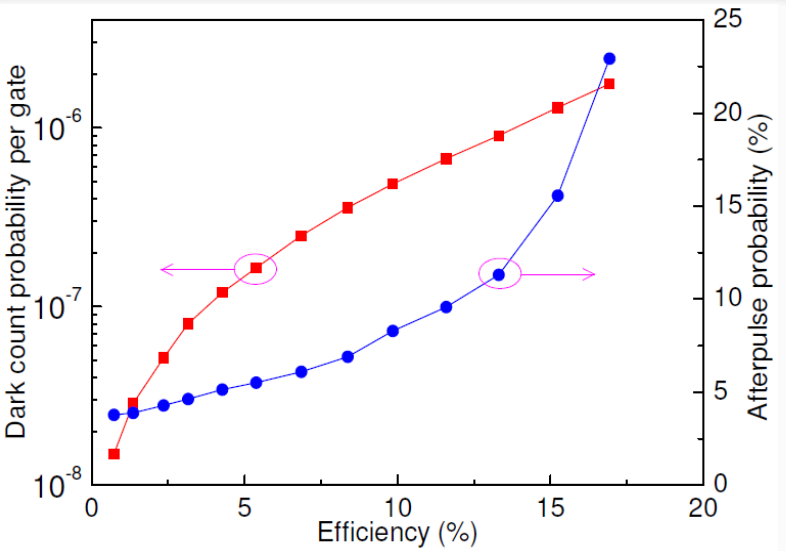
WRONG

UNIVERSITÉ DE GENÈVE

(Really) Rapid Gating Detectors





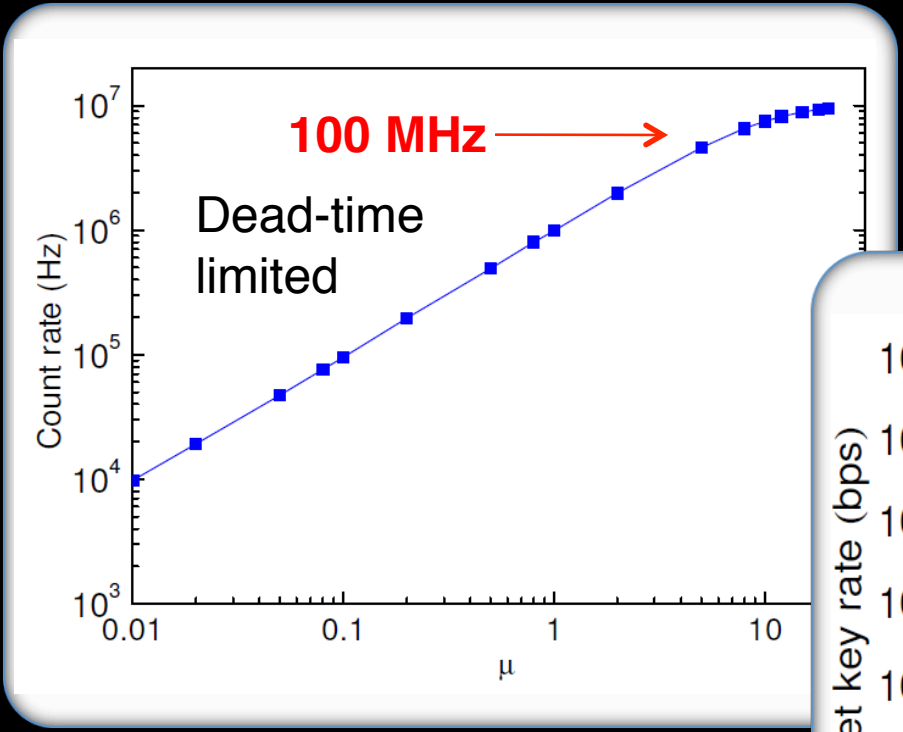


- Parameters
  - Gating freq.=2.23 GHz
  - Temperature=-40°C
  - η=10 %
  - P_{dc}=4.8E-6 /ns
  - P_{ap}=4E-5 /ns

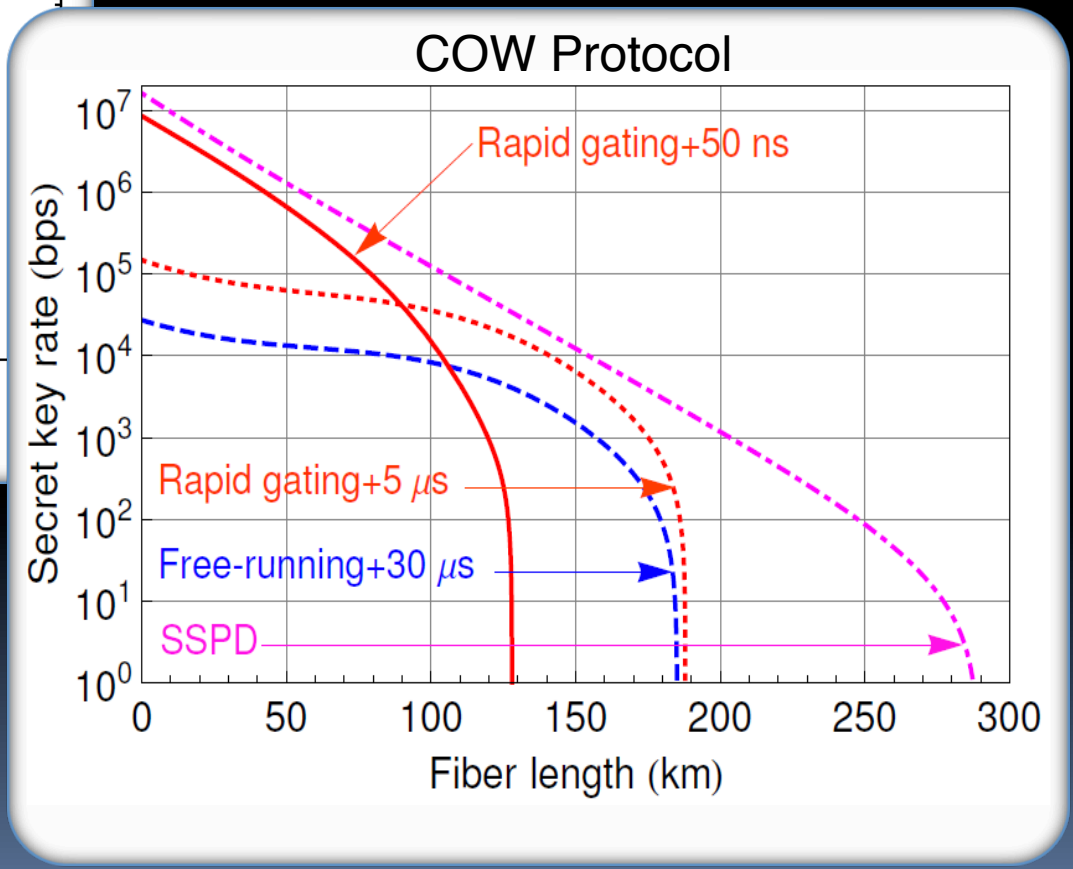
J. Zhang *et al.* SPIE 76810Z (2010)

UNIVERSITÉ DE GENÈVE

Rapid Gating Impact



In general, afterpulsing is no longer a limiting factor for QKD

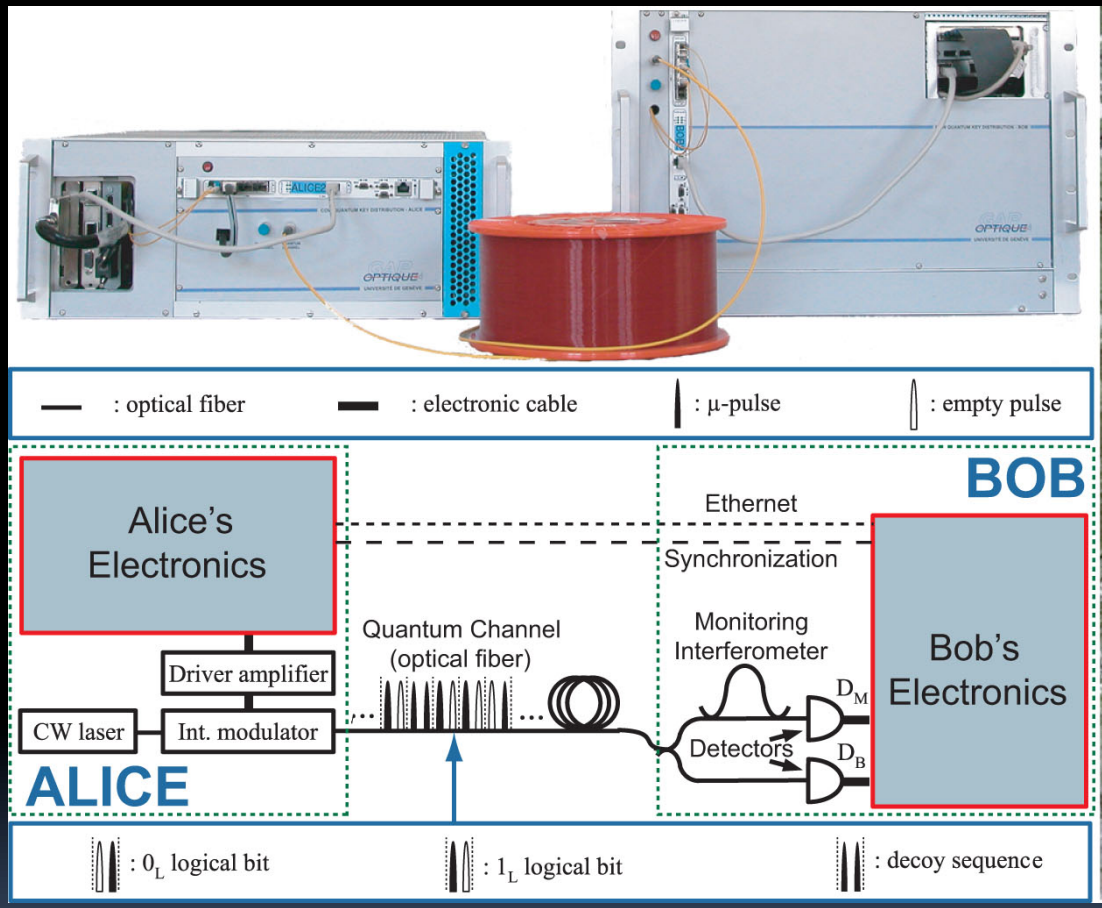


- RG APDs with small deadtime are well suited for high-rate QKD
- Both free-running and RG APDs are well suited for < 200 km applications.
- SSPDs remain advantageous for distances > 200 km

J. Zhang *et al.* SPIE 76810Z (2010)

UNIVERSITÉ DE GENÈVE

P2P QKD: Long Distance Geneva-Neuchâtel Experiment



- Academic prototype system – continuous, automated operation
- **150 km** of installed standard fibres (43dB of loss)
- **250km** in the lab
- Self-synchronisation over distance

D. Stucki *et al.*, Opt. Exp., **17**, 13326 (2009)
D. Stucki *et al.*, New J. Phys., **11**, 075003 (2009)

UNIVERSITÉ DE GENÈVE

Quantum Communication & Entanglement

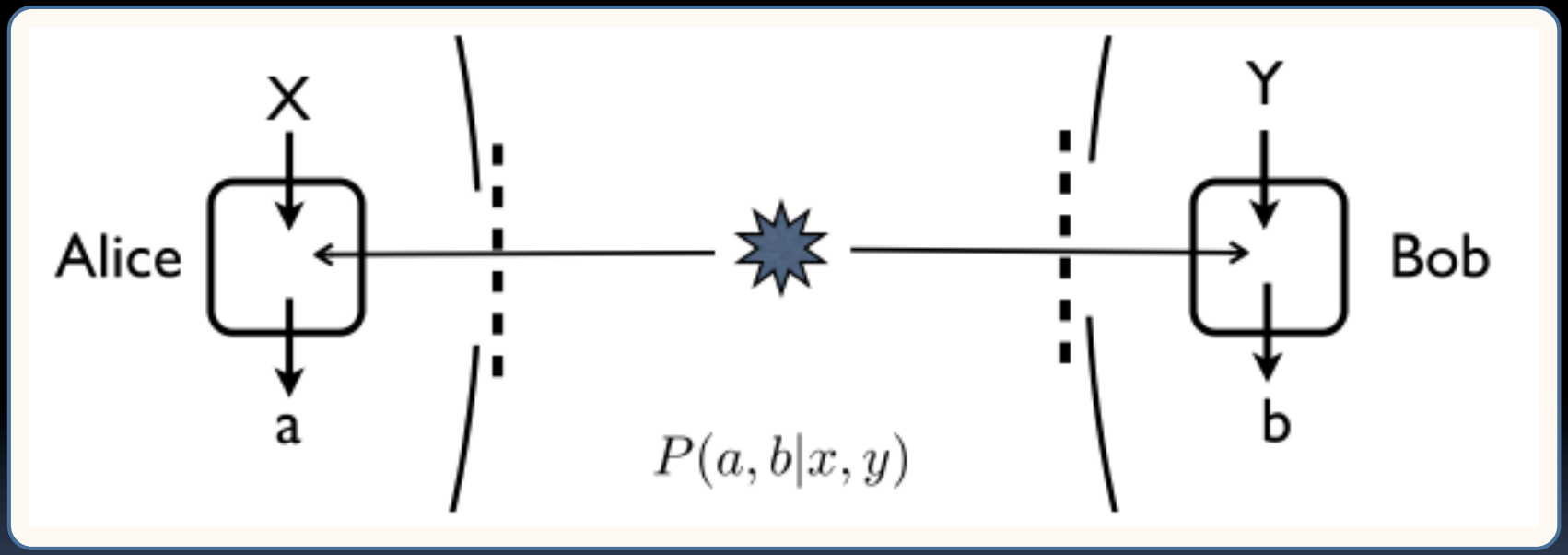
- Some new ideas
  - Heralded Qubit Amplification
  - Faithful Entanglement Swapping

Device Independent QKD

UNIVERSITÉ DE GENÈVE

Device Independent QKD

In Device-Independent quantum key distribution, the violation of a Bell inequality is exploited to establish a shared key that is secure independently of the internal workings of the QKD devices.

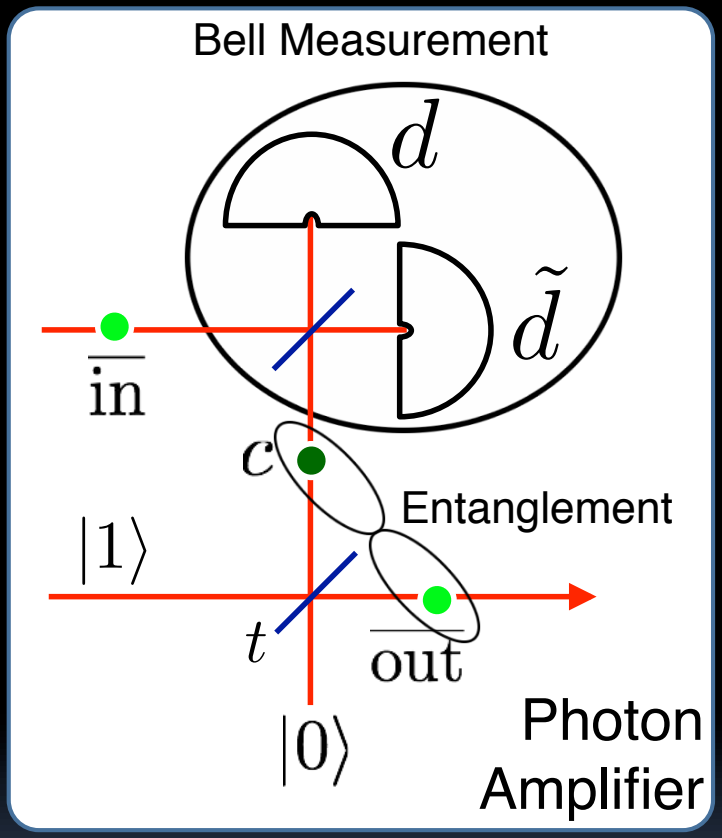


Need to overcome the detection loophole problem

We can overcome transmission loss if we can herald the arrival of a photon

UNIVERSITÉ DE GENÈVE

Heralded Photon Amplification



Input

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Conditional output

$$\sqrt{1-t}|0\rangle + \sqrt{t}|1\rangle$$

Teleportation with single-photon entanglement

Photon amplifier if

$$t > 1/2$$

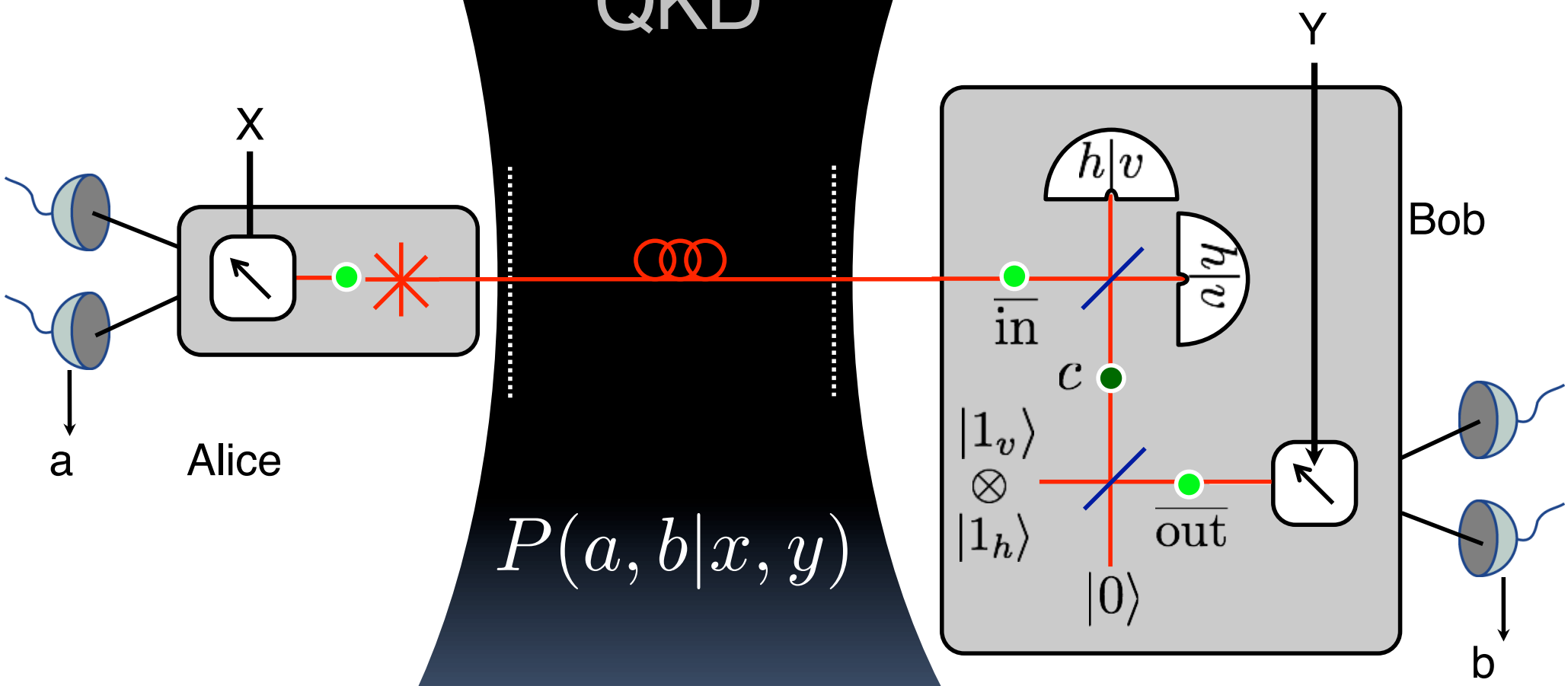
We can use single photon entanglement for teleportation …

→ single photon entanglement is a resource for quantum communication

Pegg *et al.* 1998, Ralph and Lund 2008

UNIVERSITÉ DE GENÈVE

Device Independent QKD

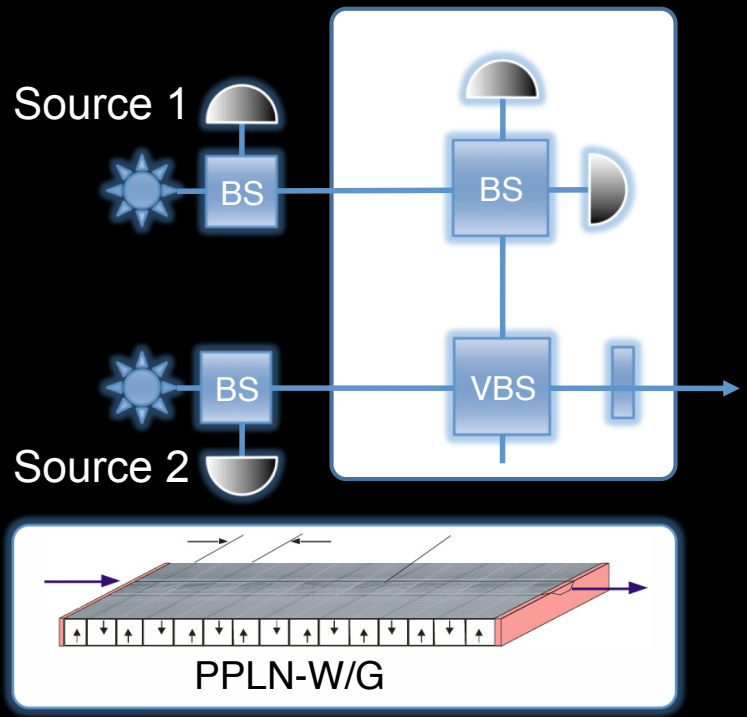


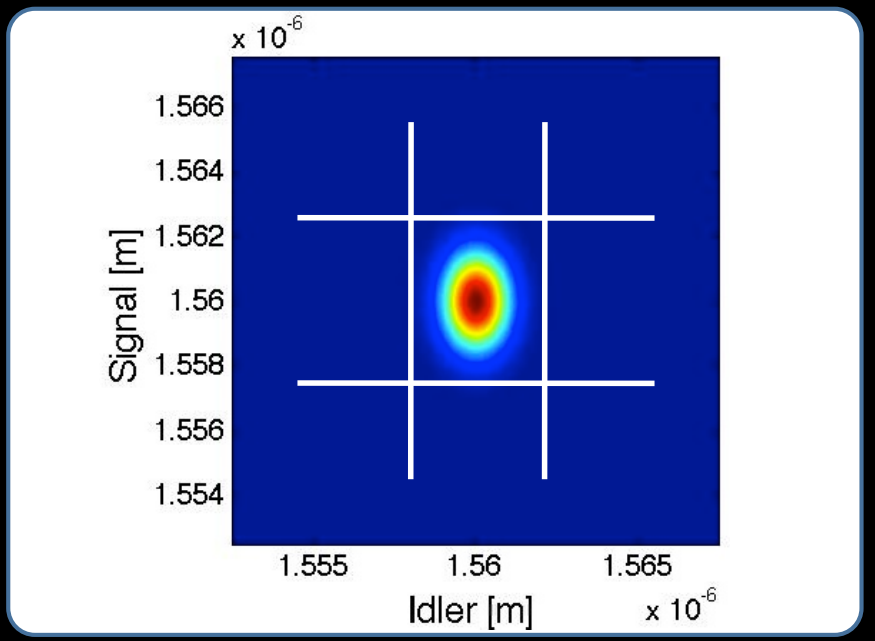
$P(a, b|x, y)$

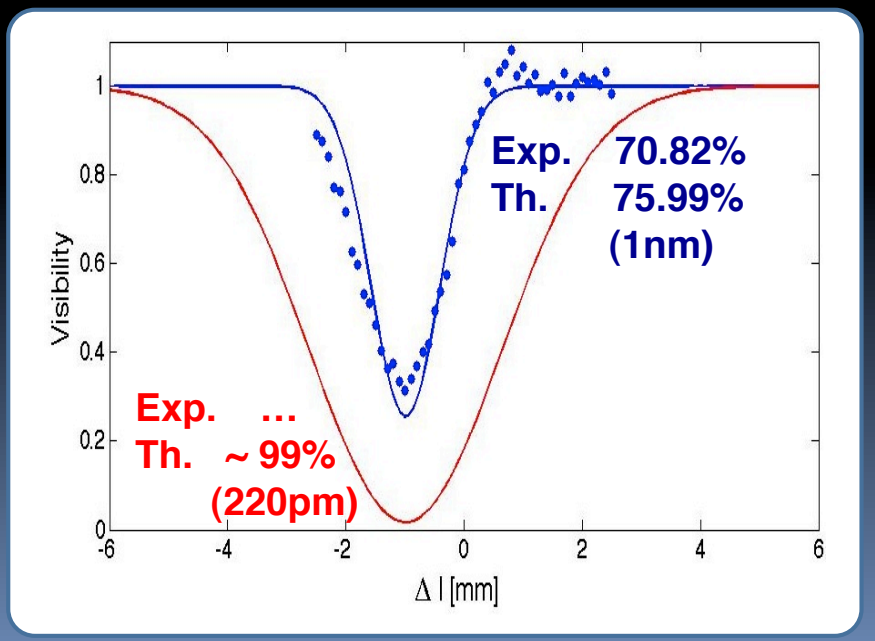
N. Gisin *et al.*, PRL 105, 070501 (2010)

UNIVERSITÉ DE GENÈVE

How good are your SPDC sources?







Constraints

Coupling losses (including filtering) will reduce the amplification

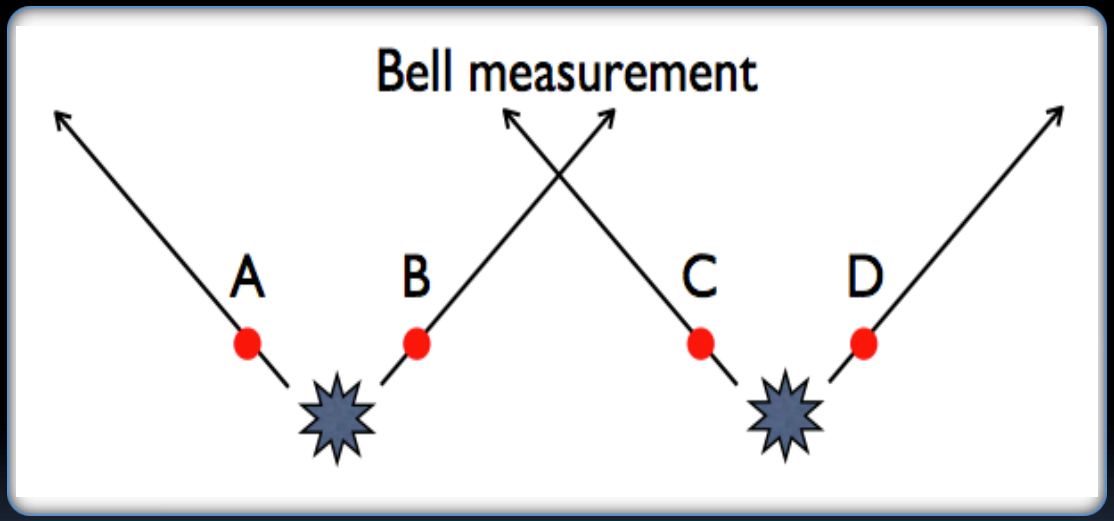
- they need to be better than the losses we are trying to overcome
- they need to be pure & indistinguishable

UNIVERSITÉ DE GENÈVE

Entanglement Swapping

(Teleporting Entanglement)

Only works with post-selection of all 4 photons



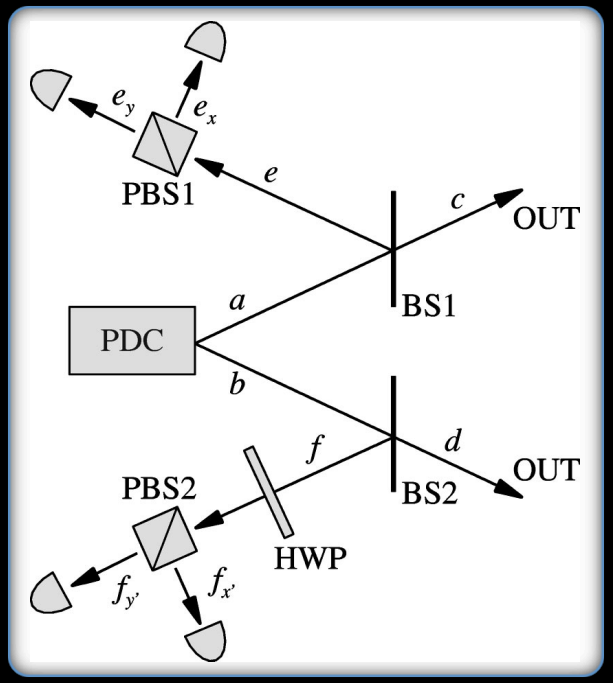
Probability to get a pair from each source = Probability to get 2 pairs from one source!

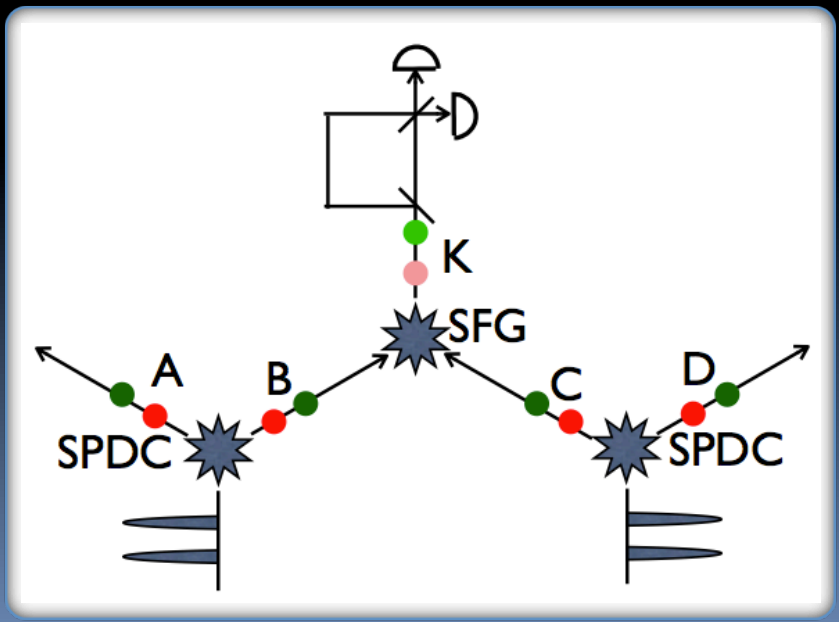
Without postselection Fidelity ≤ 1/2

UNIVERSITÉ DE GENÈVE

Faithful Entanglement Swapping

- 6 photons + 4 heralding detections
  - Theory
    - Sliwa & Banaszek, PRA 67, 030101(R) (2003)
  - Experiment
    - Wagenknecht *et al.*, Nature Phot. 4, 549 - 552 (2010)
    - Barz *et al.*, Nature Phot. 4, 553 - 556 (2010)





- 4 photons + 1 heralding detection
  - Sangouard *et al.*,
    - Phys. Rev. Lett. 106, 120403 (2011)

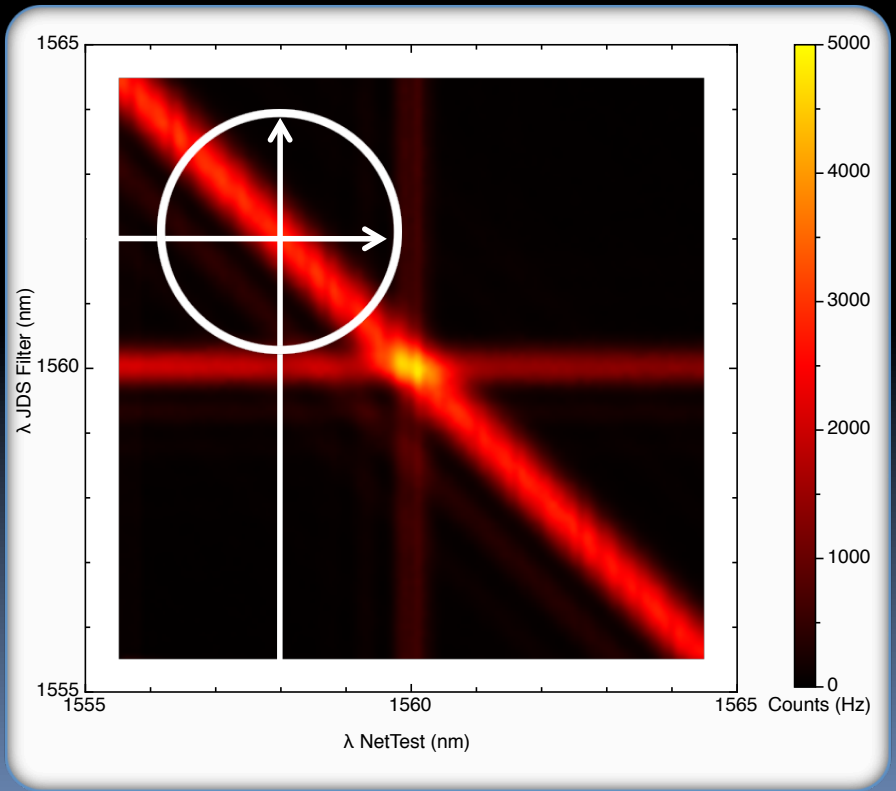
Already for $\eta_d \sim 0.4$, & $\eta_{nl} \sim 10^{-9}$
this outperforms the previous proposal

UNIVERSITÉ DE GENÈVE

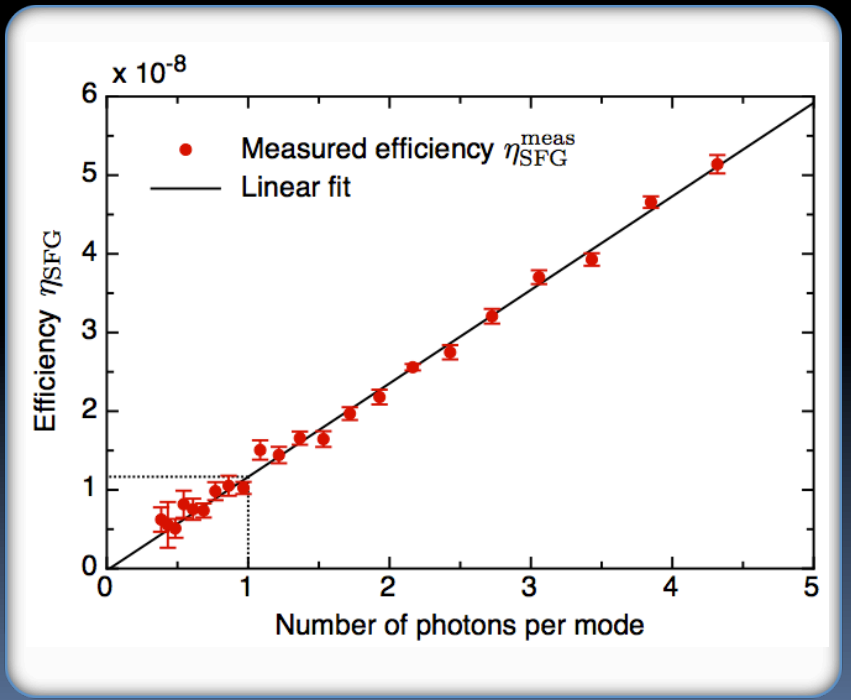
Single Photon Level SFG

SFG = sum-frequency generation

- Why does it work?
  - Non-degenerate photons from one source will not satisfy the SFG phase matching conditions



- …and at the single photon level?
  - Two attenuated input beams test the linearity of the nonlinear conversion

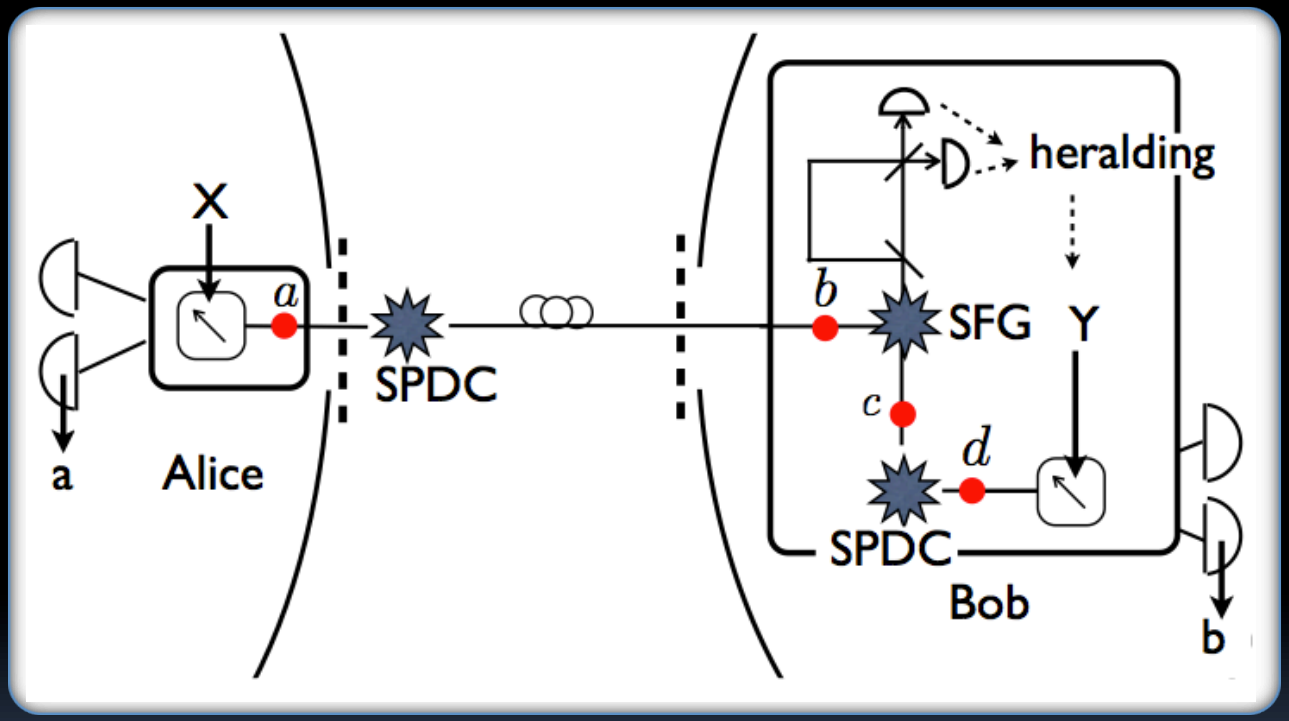


N. Sangouard *et al.*, PRL **106**, 120403 (2011)

UNIVERSITÉ DE GENÈVE

Up-Conversion Heralding Amplifier

- Potential application - DIQKD



Unlike recent single photon SPDC proposals
this provides a heralding signal over
extended - Quantum Communication - distances

N. Sangouard *et al.*, PRL **106**, 120403 (2011)

UNIVERSITÉ DE GENÈVE

What happened?

- Applied QKD
  - Robust Long term operation of a QKD network
  - Standard fibre and InGaAs detectors: 150 km
  - With ULL fibre and SSPD detector: 250 km
  - Key exchange and high speed encryption (1Gbps) using a single dark fibre: 60 km
- Device Independent QKD
  - Heralded Qubit amplification (concept)
  - Faithful Entanglement Swapping via SFG (Proof of principle)

Opens the door to experimental DIQKD

UNIVERSITÉ DE GENÈVE

Thanks

QKD

Nino Walenta Ci Wen Lim
Damien Stucki

Quantum Communication

Natalia Bruno Enrico Pomarico
Clara Osorio Bruno Sanguinetti

Theory

Nicolas Sangouard

Hugo Zbinden

Nicolas Gisin