Communication quantique: jongler avec des paires de photons dans des fibres optiques

Nicolas Gisin

GAP-Optique, University of Geneva

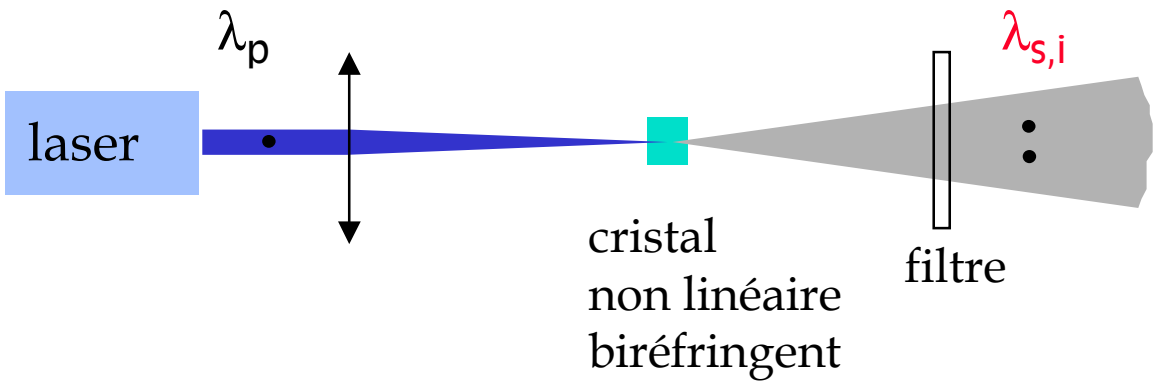
H. De Riedmatten, J.-D. Gautier, O. Guinnard, I. Marcikic, G. Ribordy,
V. Scarani, A. Stefanov, D. Stücki, S. Tanzilli, R. Thew, W. Tittel, H. Zbinden

- Thème: dialogue entre

  Physique de base et Physique appliquée

- Sources de paires de photons compatibles télécom
- Non-localité quantique
- Cryptographie Quantique et inégalités de Bell
- Applications futuristes

Source de paires de photons



- Fluorescence paramétrique
- Conservation de l'énergie et de l'impulsion

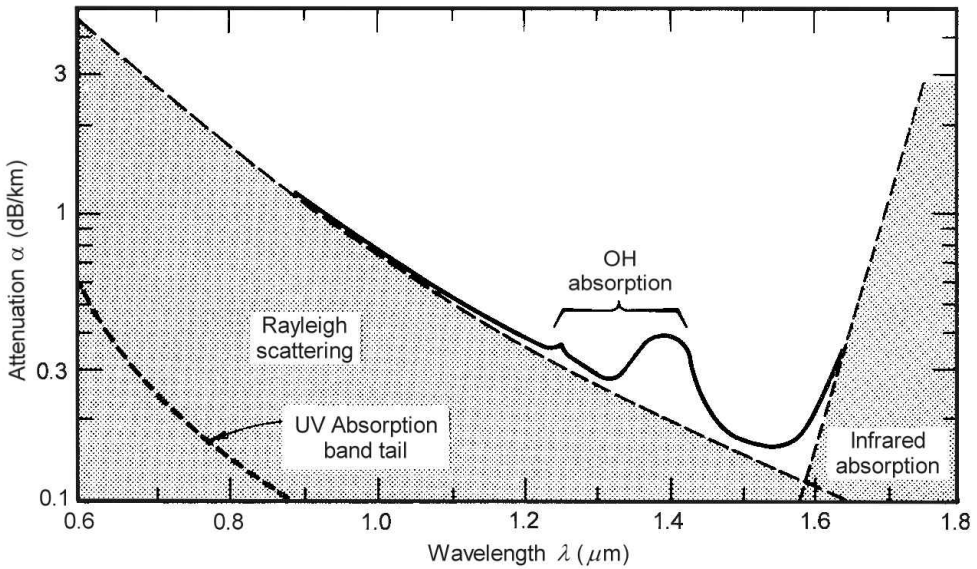
$$\omega_p = \omega_s + \omega_i \qquad \vec{k}_p = \vec{k}_s + \vec{k}_i$$

- L'accord de phase détermine les longueurs d'ondes et directions de propagations

Longueurs d'ondes Télécom

Atténuation

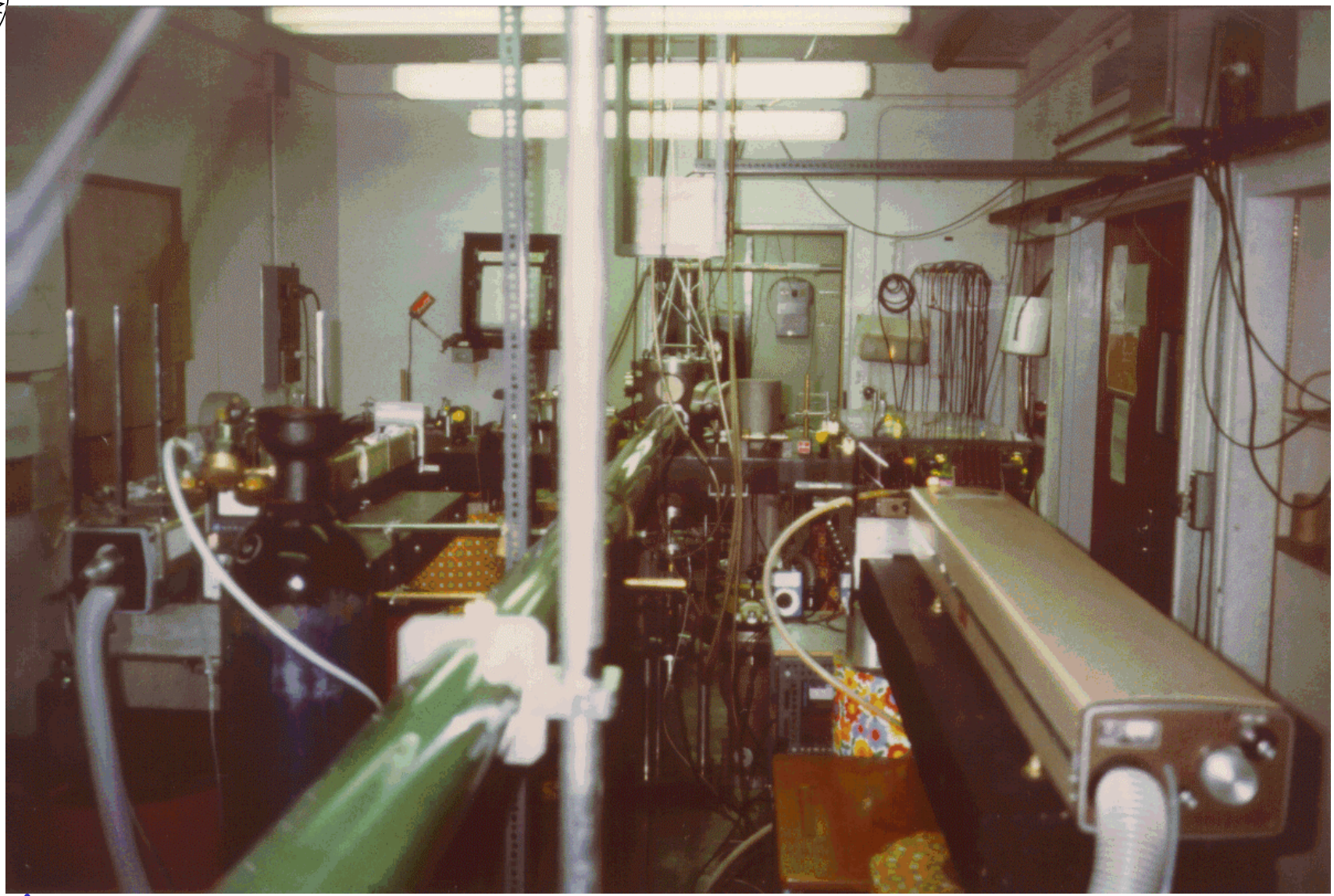
λ [µm]	α [dB/km]	T_{10km}
0.8	2	1%
1.3	0.35	44%
1.55	0.2	63%



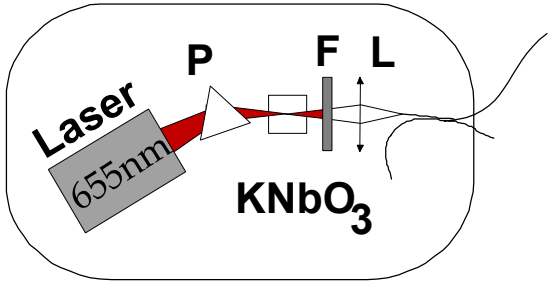
Dispersion chromatique

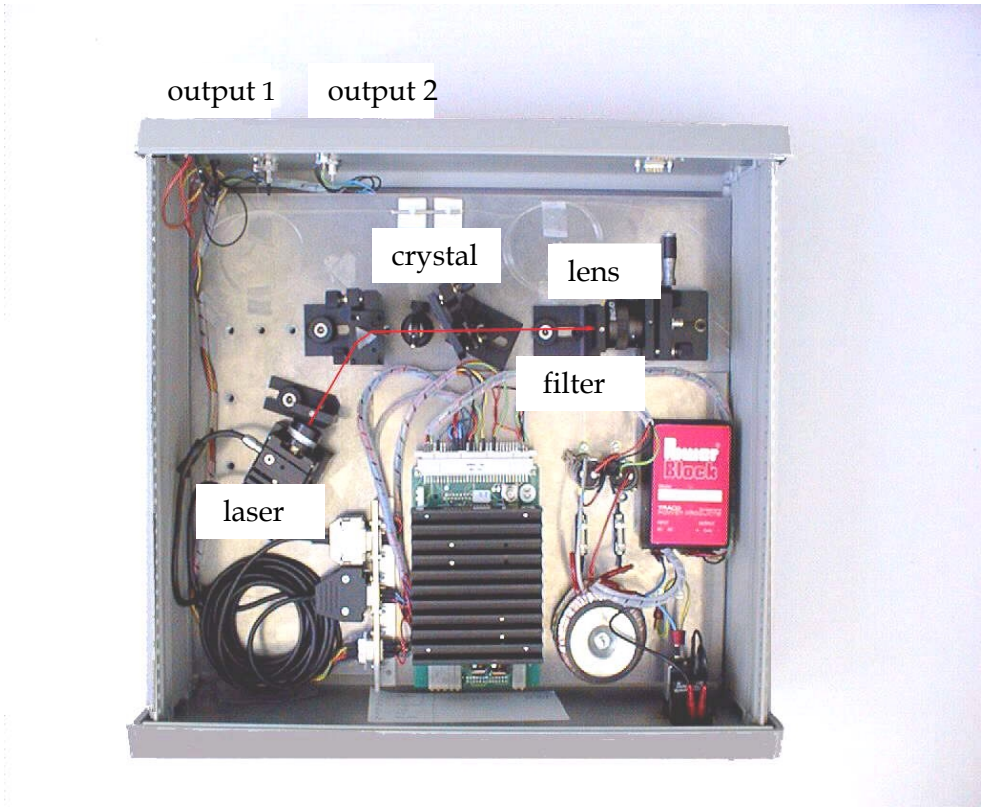
Composants disponibles

2-υ source of Aspect's 1982 experiment



Source de paires de photons (1997)





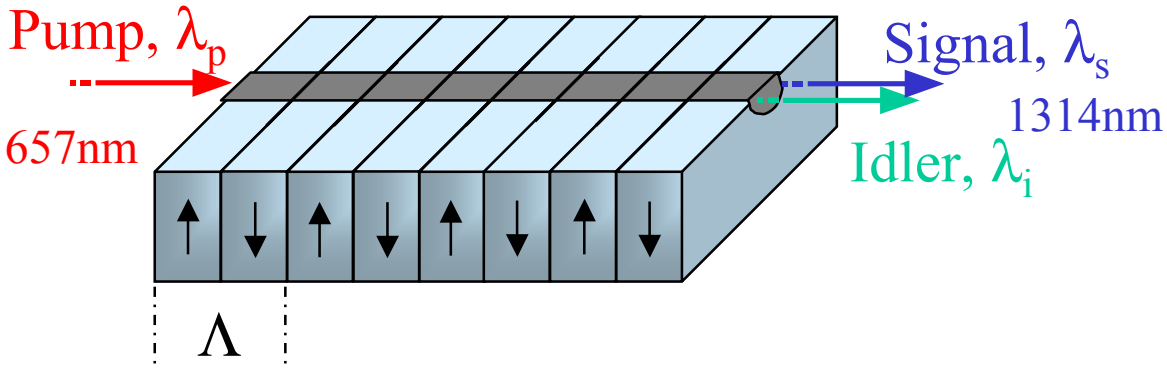
- Intrication énergie-temps
  - $\lambda_p = 655\,\text{nm};\ \overline{\lambda}_{s,i} = 1310\,\text{nm}$
- diode laser
- simple, petit, pratique

  40 x 45 x 15 cm^3
- I_{pump} = 8 mW
- avec guide dans $LiNbO_3$

  avec quasi accord phase,

  $I_{pump} \approx 8\ \mu W$

PPLN waveguide



QPM parameters :

Λ=12.1µm

W=4 µm

T=100°C

- Poling : E-field applied periodically

  Periodic reversal and use of d_{33} (= 7*d_{31}) ➔ QPM

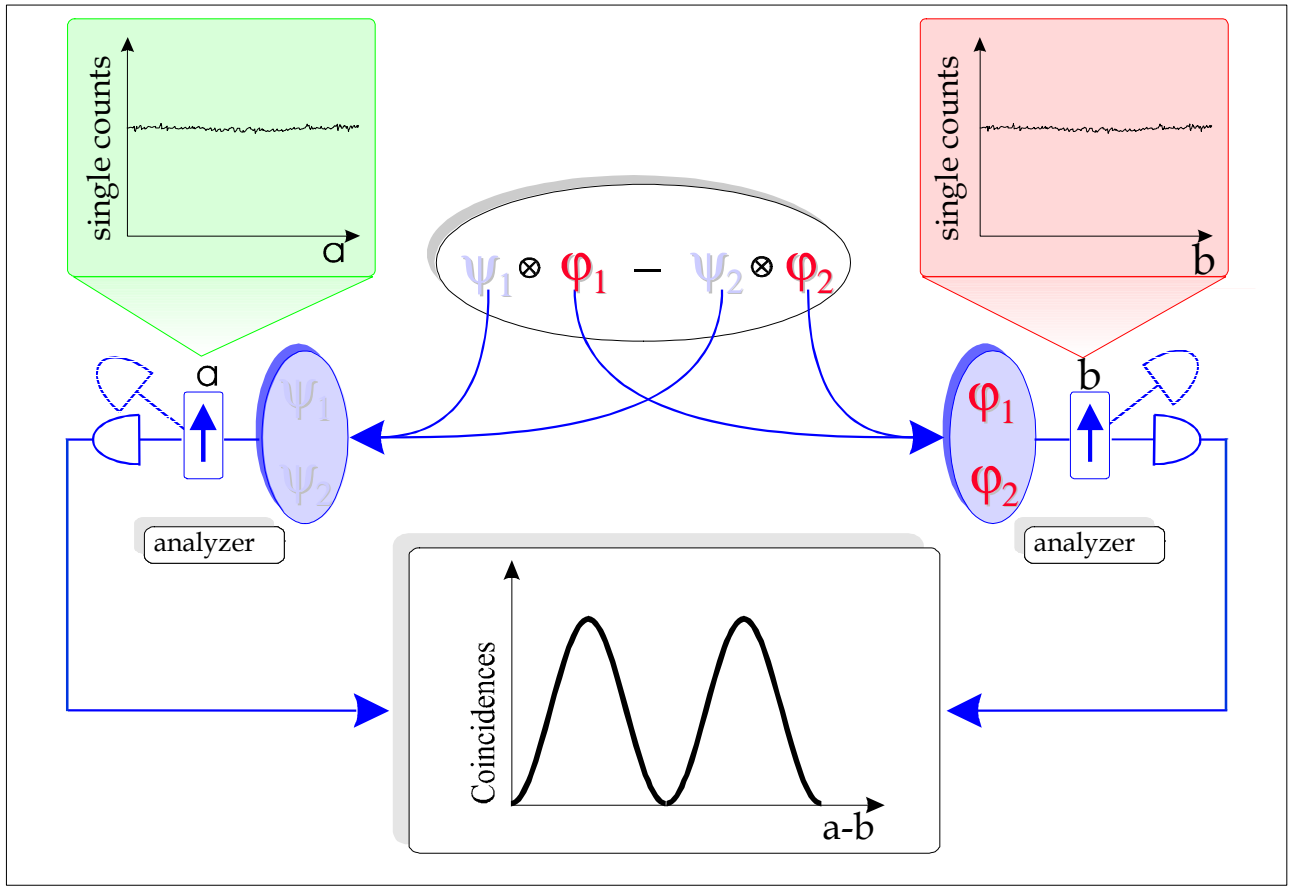
- Waveguide made by Soft Proton Exchange (SPE)

  $LiNbO_3$ + acid bath ➔ $\Delta n > 0$ trough the mask

$\Delta n \approx 0.03$ $\alpha \approx 0.5$ dB/cm

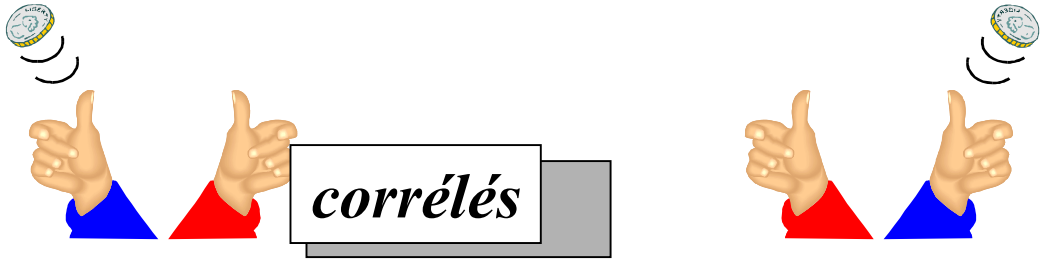
Probabilité ≈ 10^{-6}

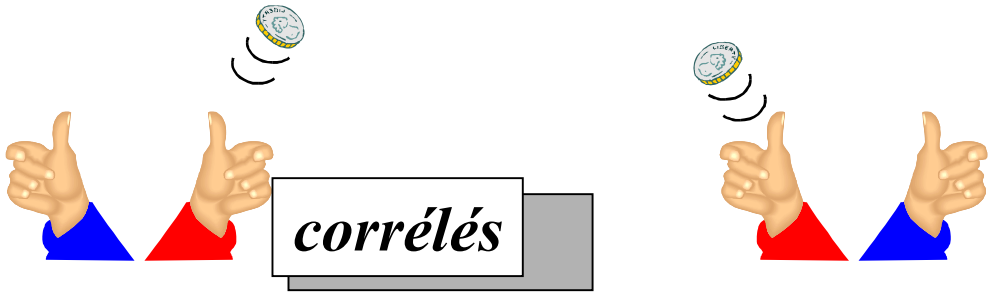
Non localité Quantique



La statistique des corrélations n'est pas descriptible à l'aide de variables locales ⇝ non localité quantique

Jeu de pile ou face à distance



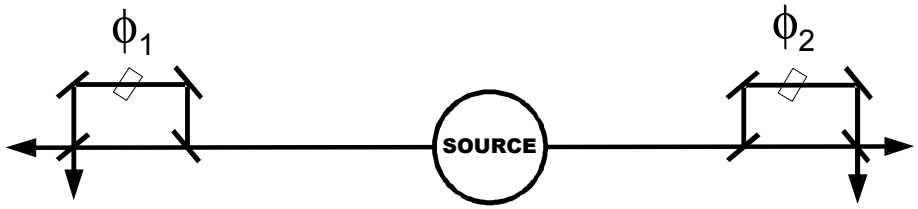


De chaque côté les résultats apparaissent aléatoires

La statistique des corrélations n'est pas descriptible à l'aide de

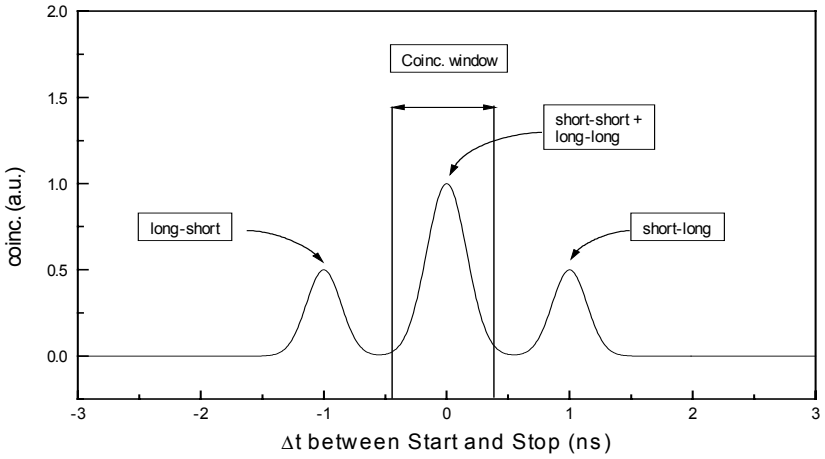
variables locales ⇝ **non localité quantique**

Interféromètre de Franson



2 interféromètres déséquilibrés $\Rightarrow$ pas d'interférences du 1er ordre

paires de photons $\Rightarrow$ possibilité de compter des coïncidences

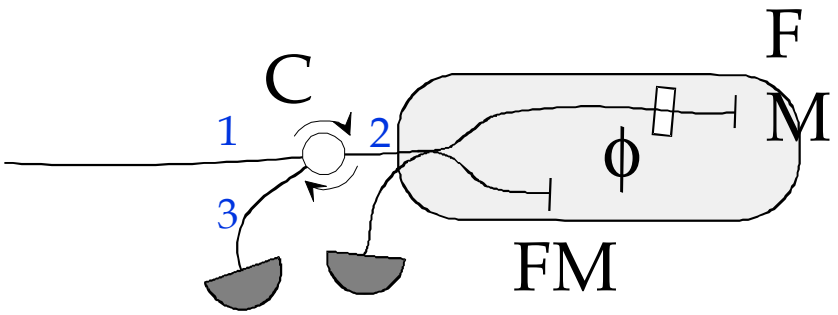


On ne peut pas distinguer entre "long-long" et "court-court"

Donc, la MQ nous dit que l'on doit additionner les amplitudes de probabilités

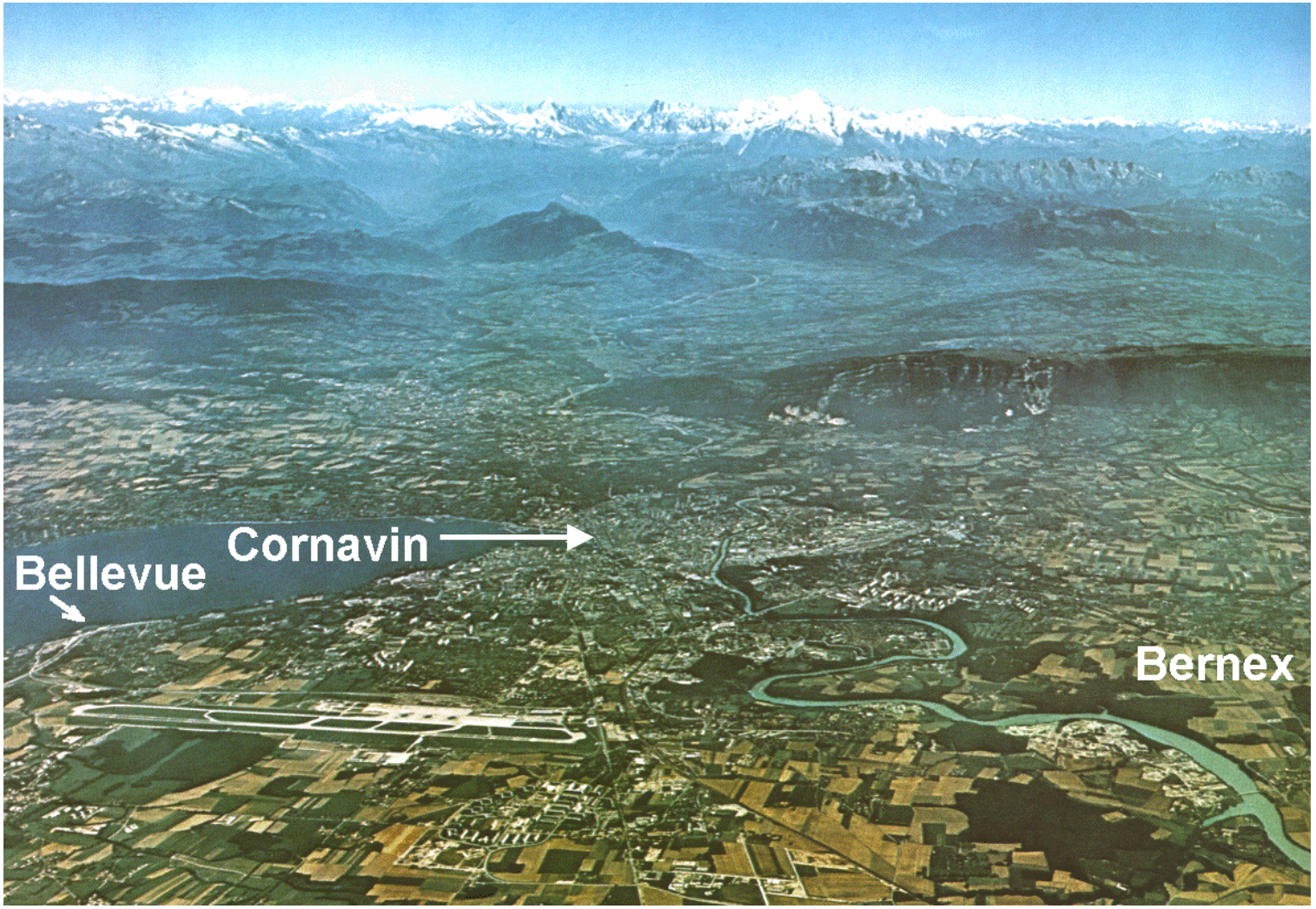
$\Rightarrow$ interférences (du 2ème ordre)

Les interféromètres

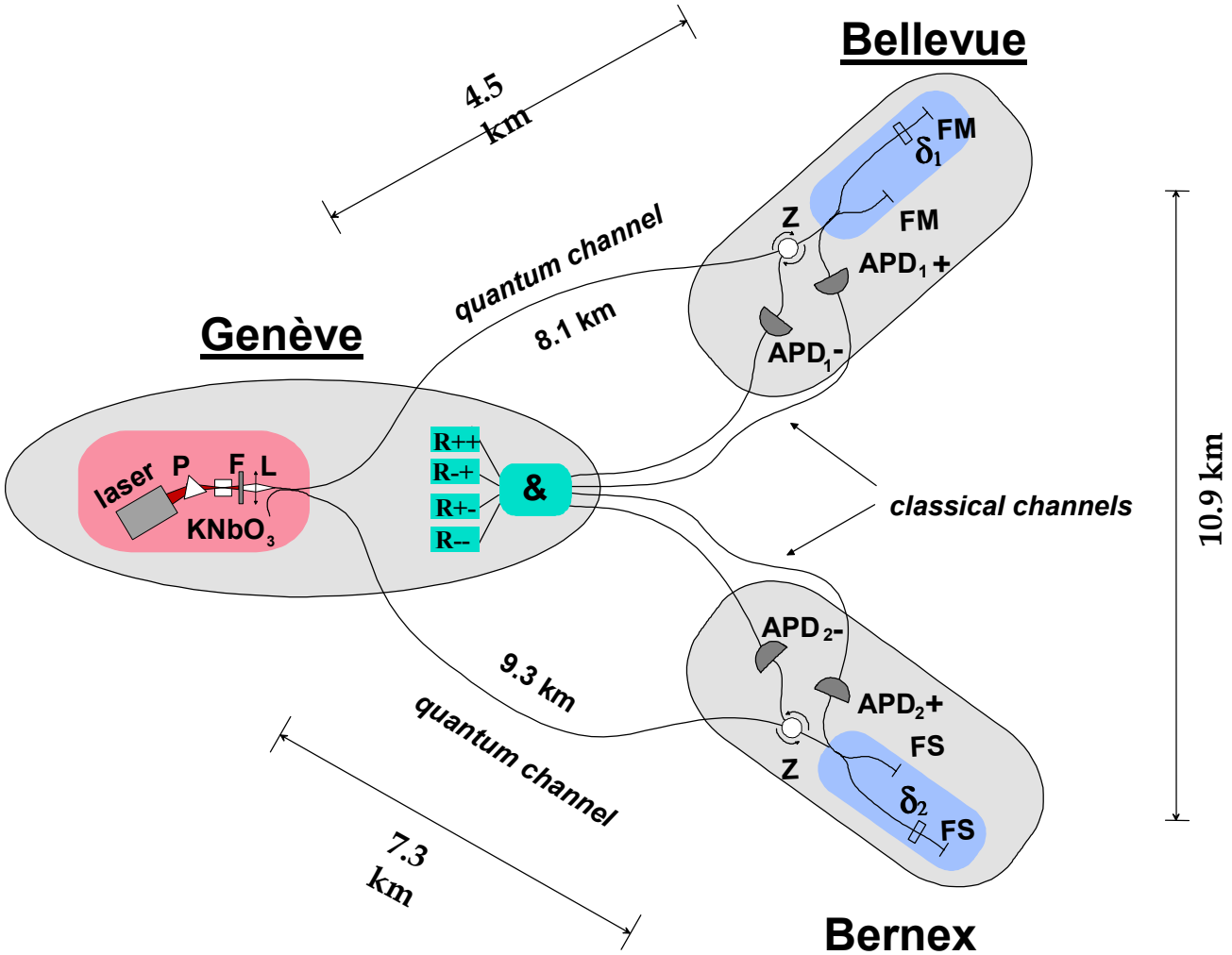


- Fibres optiques monomodes, standard telecom
- Configuration Michelson
- Circulateur C : donne accès au second port en sortie
- Miroirs de Faraday FM: compense la biréfringence
- Température ajustable pour le contrôle de la phase ϕ

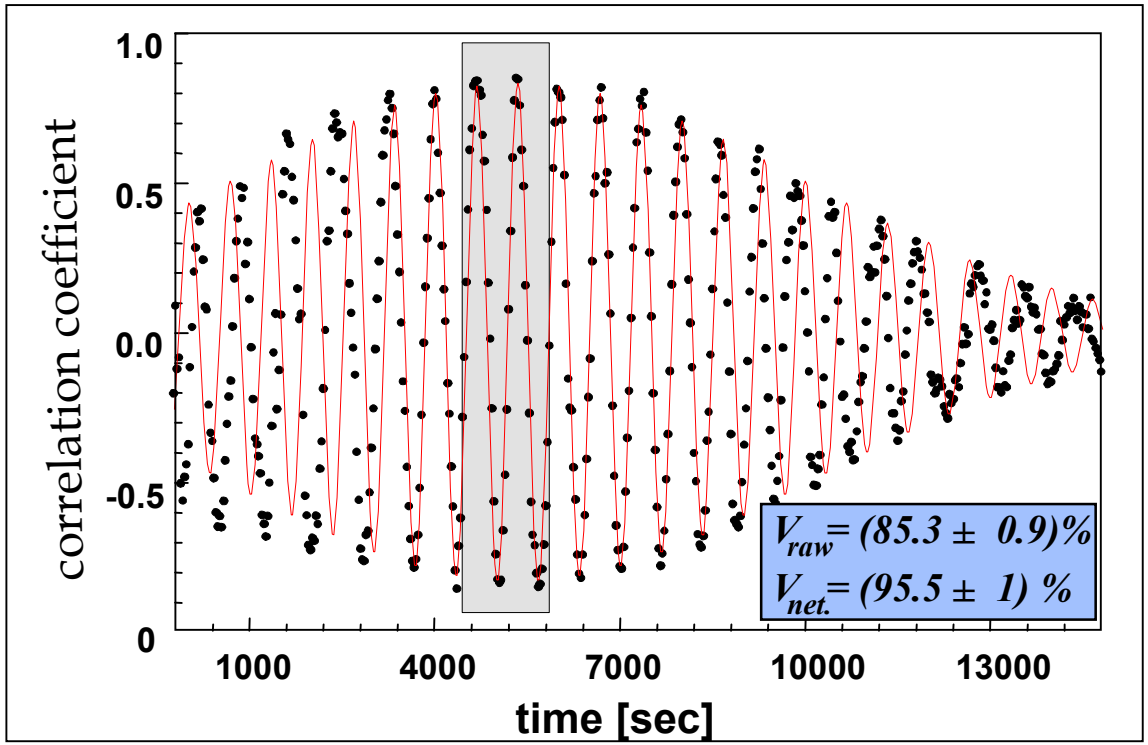
le labo



Test des inégalités de Bell sur 10 km



résultats



- 15 Hz coïncidences
- S_{raw} = 2.41
  S_{net} = 2.7
- violation des inégalités de Bell par 16 (25) déviations standards
- en bon accord avec les prédictions quantiques
- mêmes résultats qu'en labo

A quoi ça sert? … après tout, il n'y a pas de communication, seulement "jeu de hasard à distance"!

L 'intrication est paradoxale*

- **non-localité quantique**
- **⇒ tout est intriqué avec tout**
- **⇒ infinité d'univers parallèles (David Deutsch : Multivers)**
- **Le chat de Schrödinger est mort dans un univers et vivant dans un autre**

*En principe tout est intriqué avec tout, mais en pratique la décohérence rend impossible d'observer cette intrication généralisée!

L 'intrication est une ressource

- **La non-localité quantique est la matière première de la technologie de l'informatique quantique***
- **Les grandes agences internationales allouent des fonds substantiels à ce nouveau domaine de recherche**

*l'art de tourner les paradoxes quantiques en applications potentielles!

Cryptographie Quantique

- Pour espionner un "canal de communication quantique", Eve doit effectuer des mesures sur des quanta individuels (pulses à un photon).

- Mais, la mécanique quantique nous dit: toute mesure perturbe le système quantique.

- donc, "lire" le "signal quantique" réduit la corrélation entre les données d'Alice de Bob.

- Alice et Bob peuvent donc détecter l'intervention de toute tierce personne en comparant (à l'aide d'un canal de communication classique) un échantillon de leur "signal quantique".

- Le "canal de communication quantique" n'est pas utilisé pour transmettre un message (information), seule une "clé" est transmise (pas d'information).

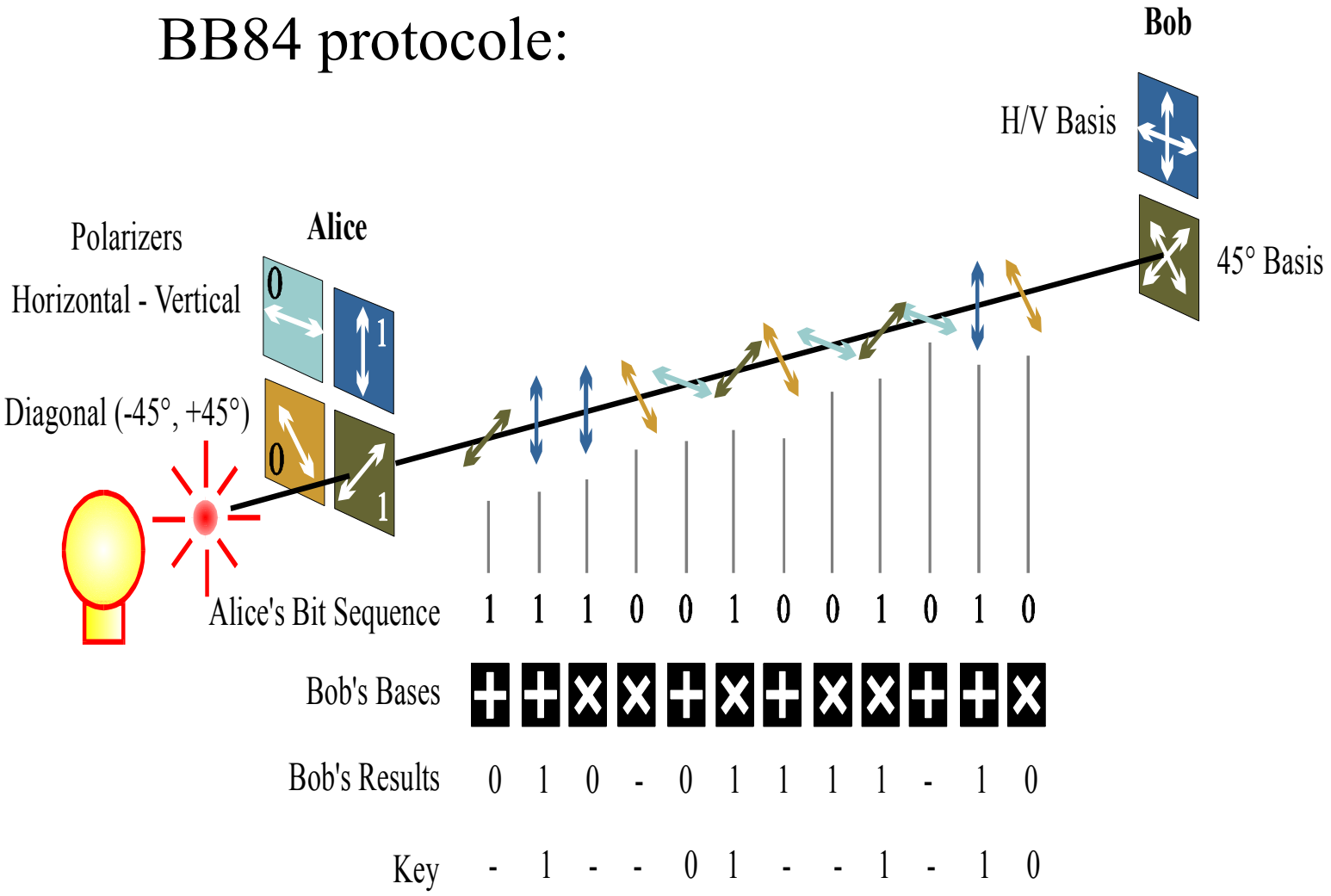
- S'il s'avère que la clé est corrompue, ils l'ignorent tout simplement (pas de perte d'information).

- Si la clé passe le test avec succès, Alice et Bob peuvent l'utiliser en toute confiance.

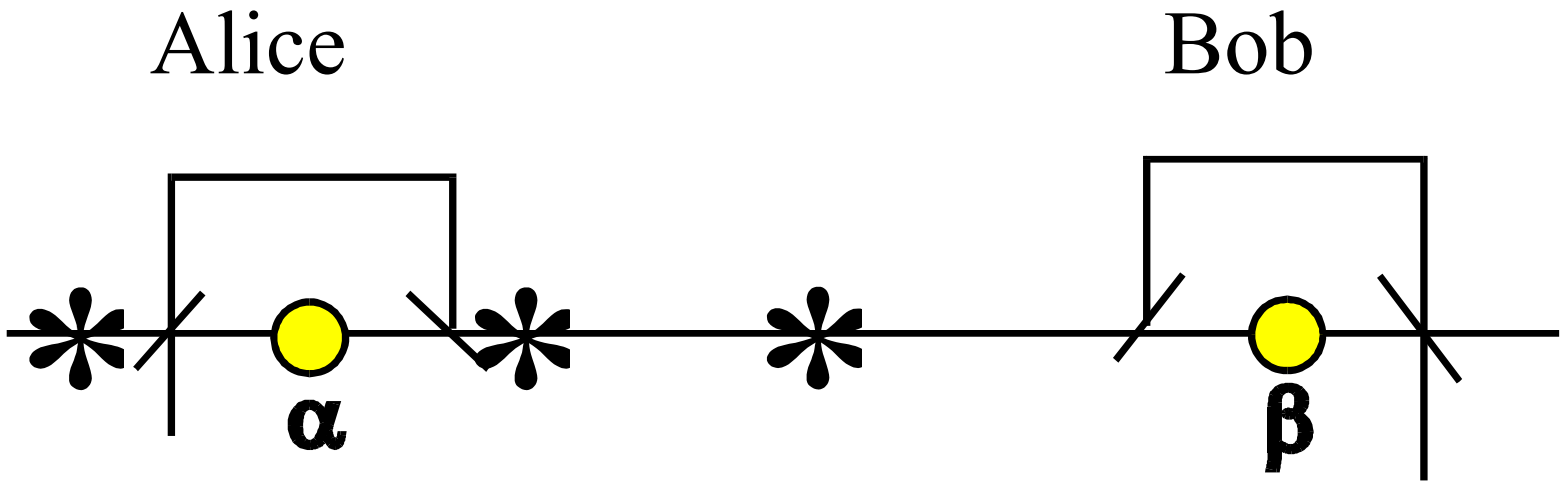
- La confidentialité de la clé est contrôlée avant que le message ne soit envoyé.

- La sécurité de la cryptographie quantique est basée sur les fondements de la physique quantique.

BB84 protocole:



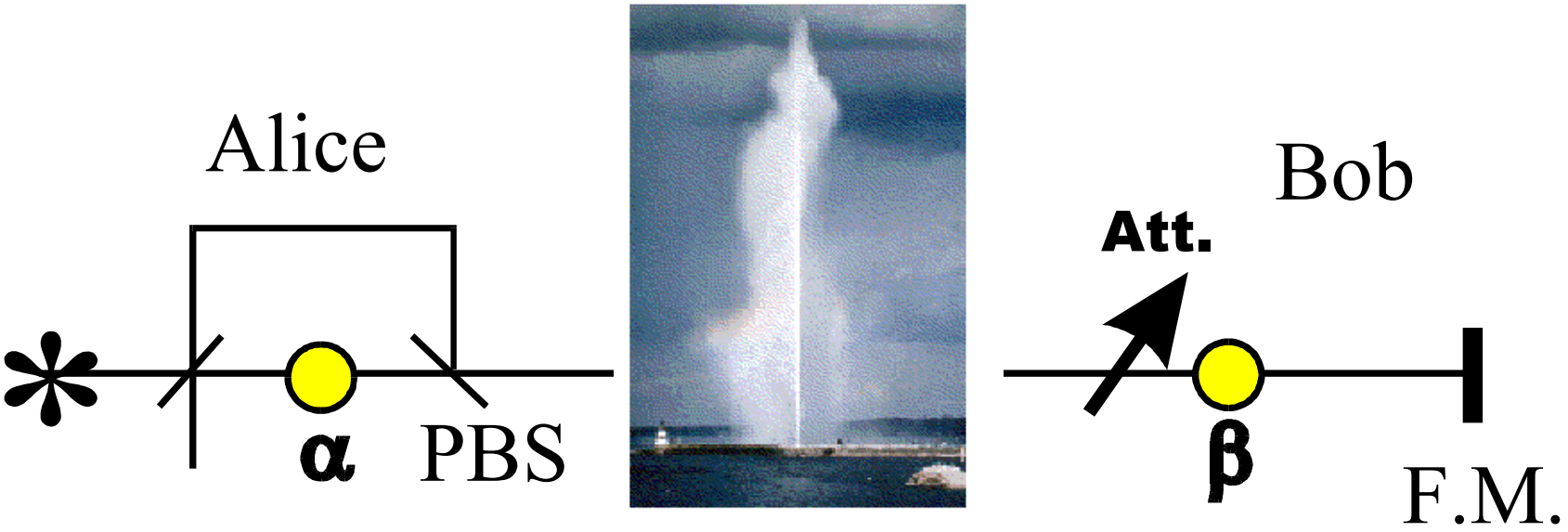
Des tests de Bell à la cryptographie Quantique



W. Tittel et al., PRL 81, 3563-3566, 1998
G. Ribordy et al., Phys. Rev. A 63, 012309, 2001

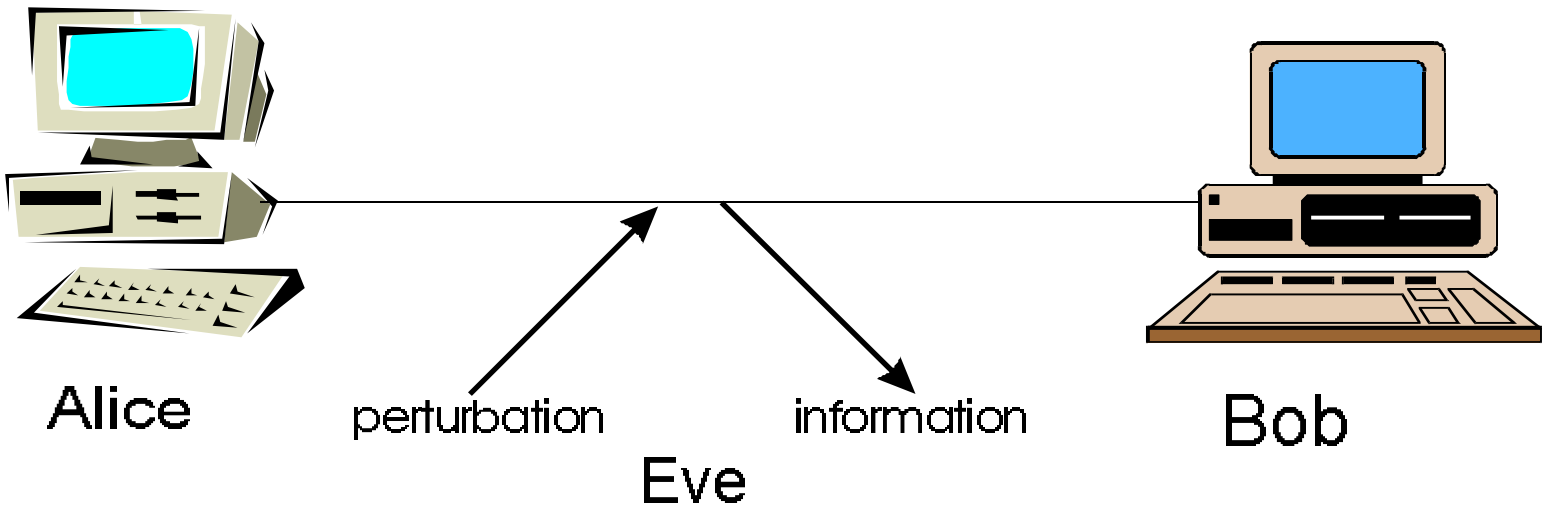
P.D. Townsend et al., Electr. Lett. 30, 809, 1994
R. Hughes et al., J. Modern Opt. 47, 533-547 , 2000

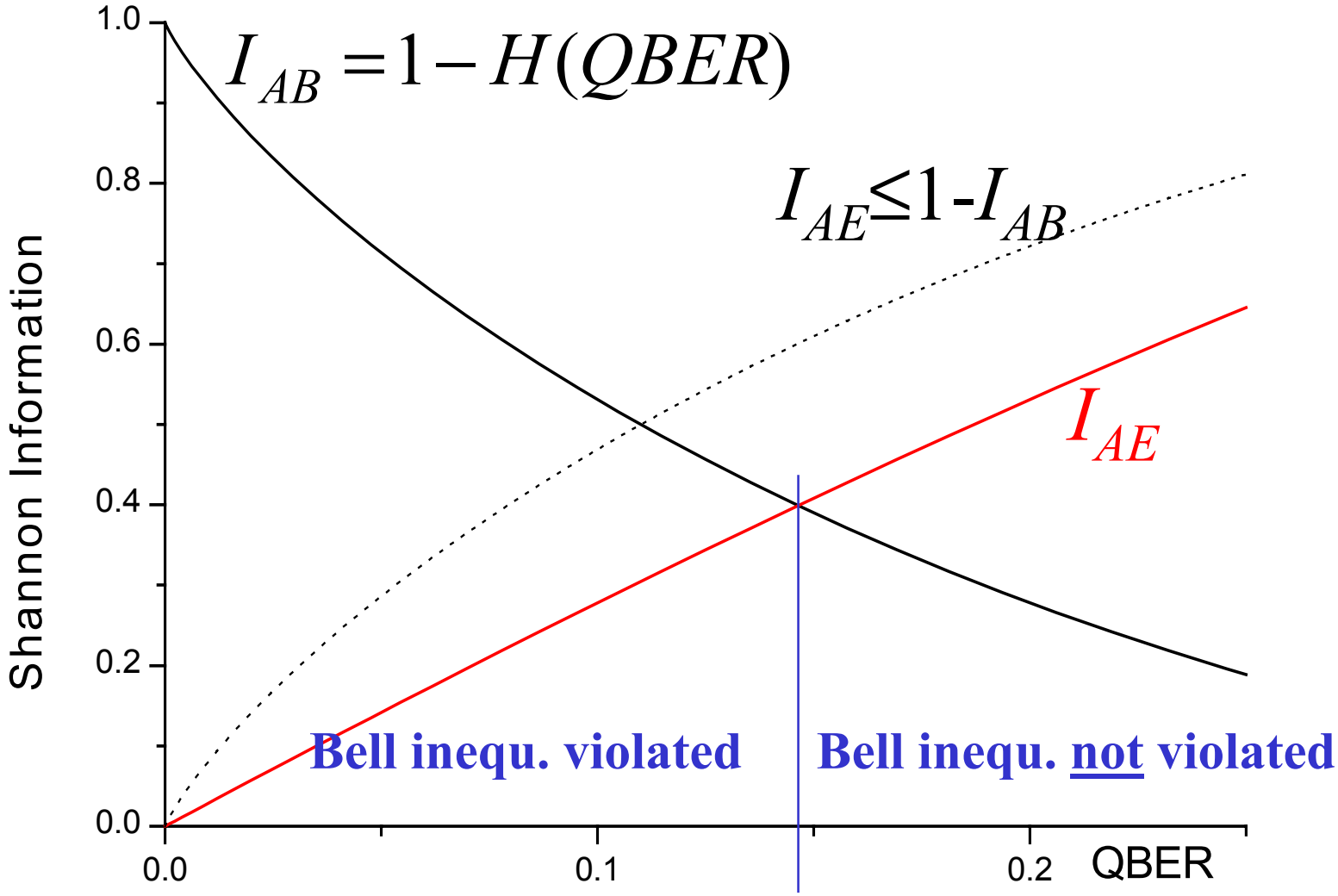
Cryptographie Quantique sous le lac de Genève

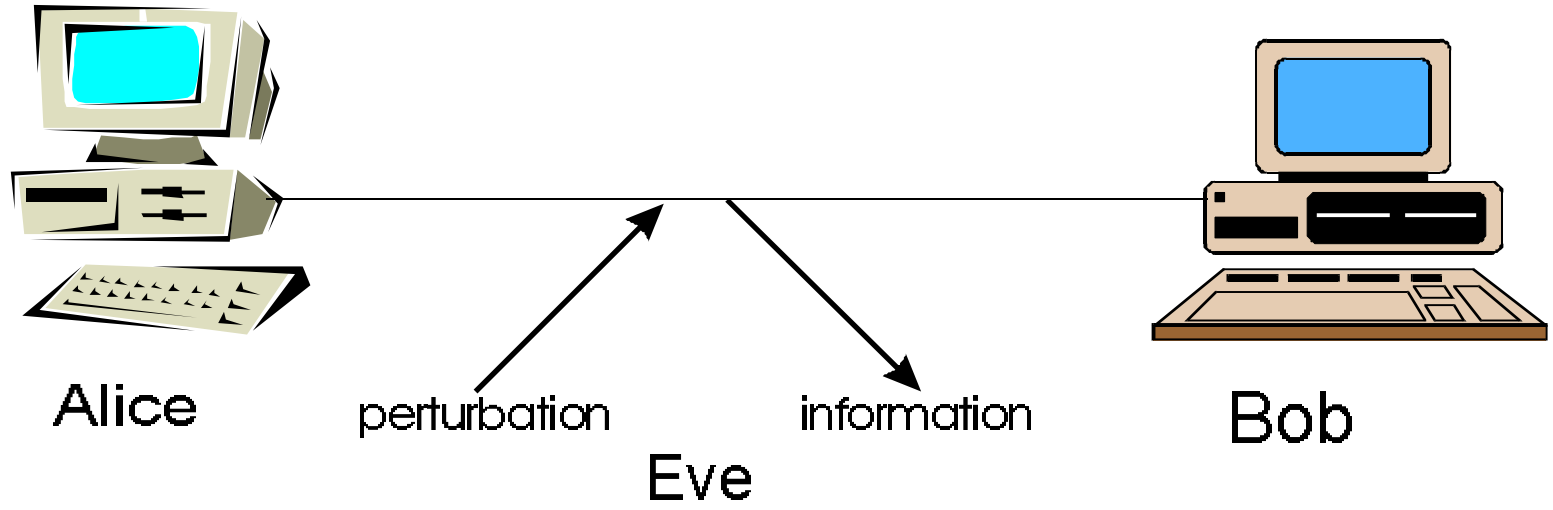


Applied Phys. Lett. 70, 793-795, 1997.
Electron. Letters 33, 586-588, 1997; 34, 2116-2117, 1998.
J. Modern optics 48, 2009-2021, 2001.

Cryptographie Quantique sur des lignes réelles




$I_{AB} = 1 - H(QBER)$
$I_{AE} \leq 1 - I_{AB}$
I_{AE}
Shannon Information
1.0
0.8
0.6
0.4
0.2
0.0
0.0
0.1
0.2
QBER
Bell inequ. violated
Bell inequ. not violated



La cryptographie quantique garantit la confidentialité

⇔

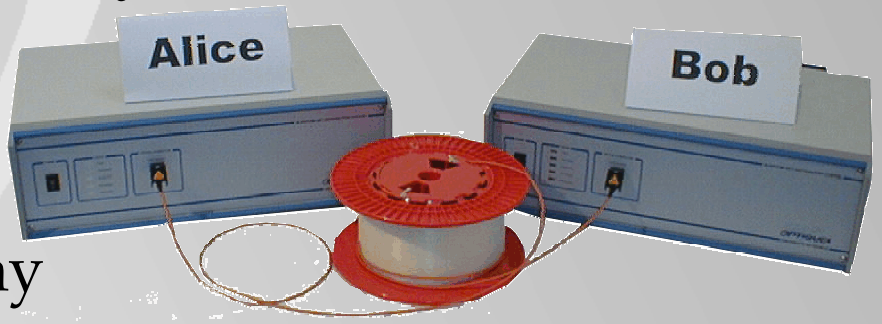
Les inégalités de Bell sont violées

⇔

Les corrélations quantiques ne peuvent pas être expliquées par des variables locales


Gare de Cornav
Pont de la Coulouvreniè
St-Gervais
Hôtel des Poste
Pointe à la Bi
Ile Rousseau
Grand Théât
Bains des Pâqu
Pont du Mont-Blan
Mur des
Genève -
Université
Cathédrale de St-Pierre
swisscom

- Company established in 2001
  - Spin-off from the University of Geneva



- Products
  - Quantum Cryptography (optical fiber system)
  - Quantum Random Number Generator
  - Single-photon detector module (1.3 μm and 1.55 μm)
- Contact information

email: info@idquantique.com

web: http://www.idquantique.com

Comment un client peut-il être certain que l'appareil qu'il achète est bien quantique?

- **Depuis la naissance de la MQ, des physiciens se sont questionnés à propos de la réalité du monde Q.**
- **Bientôt, ce seront les clients de crypto Q qui poseront la question:**

  Une question métaphysique expérimentale est devenue un problème de physique appliquée !!!

- **Même question ⇒ même réponse:**

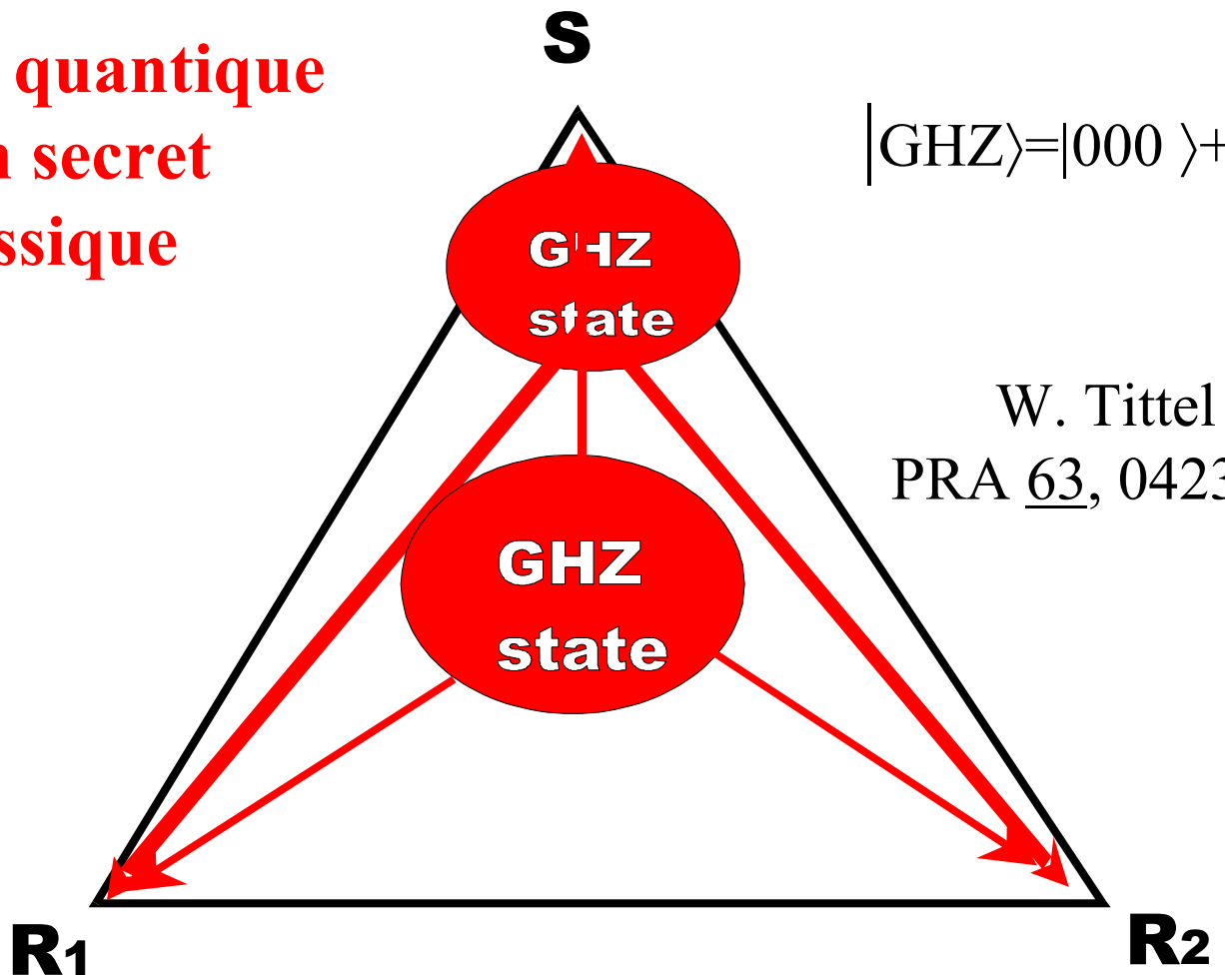
  Tester si l'appareil permet de violer les inégalités de Bell! (Mayers & Yao, 1998)

- **Même expérience ⇒ même problème:**

  l'inefficacité des détecteurs requière l'hypothèse que l'échantillon détecté est représentatif ! (N&B Gisin, Phys. Lett. A 260, 323, 1999)

Réseaux Quantiques

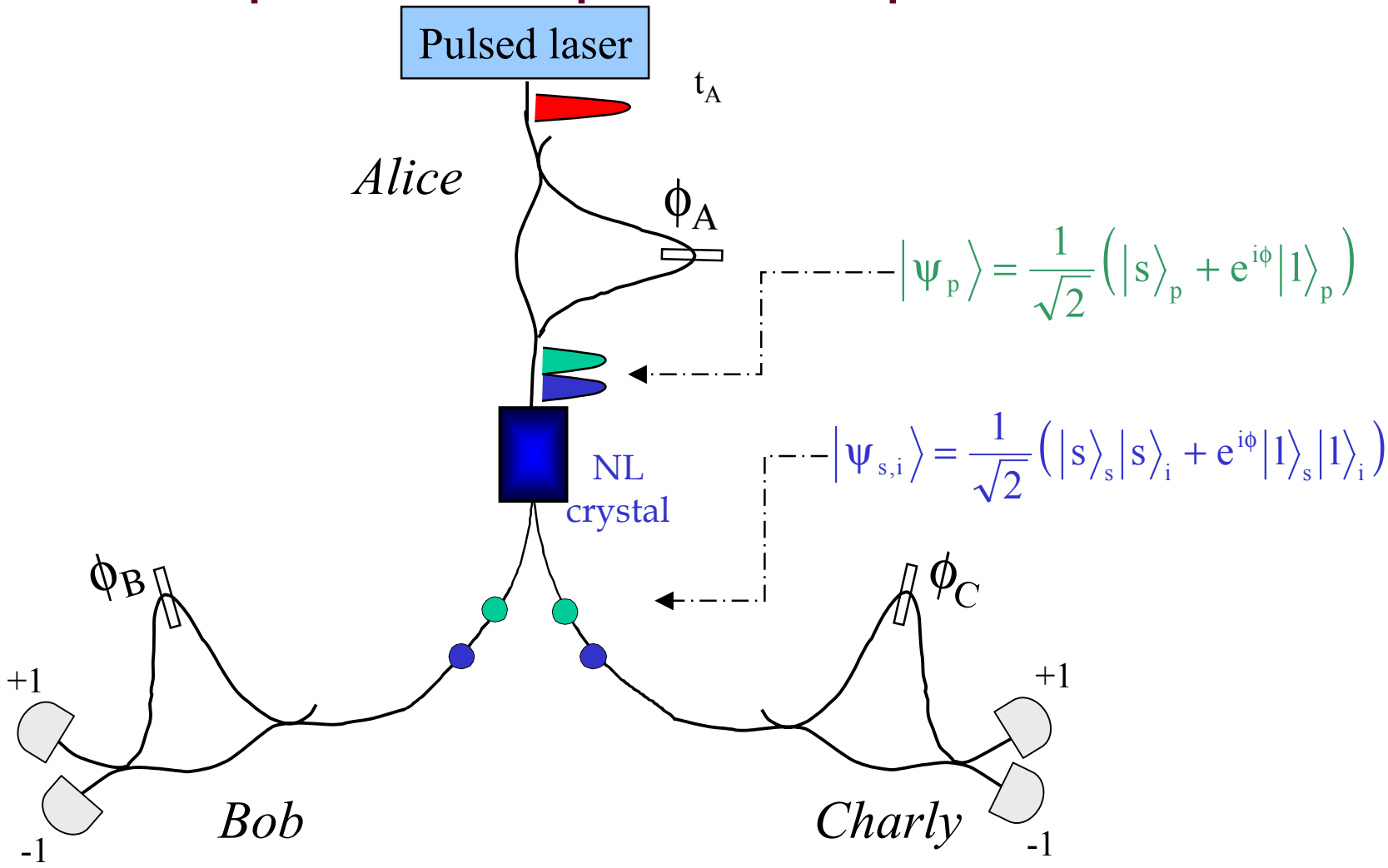
Partage quantique d'un secret classique



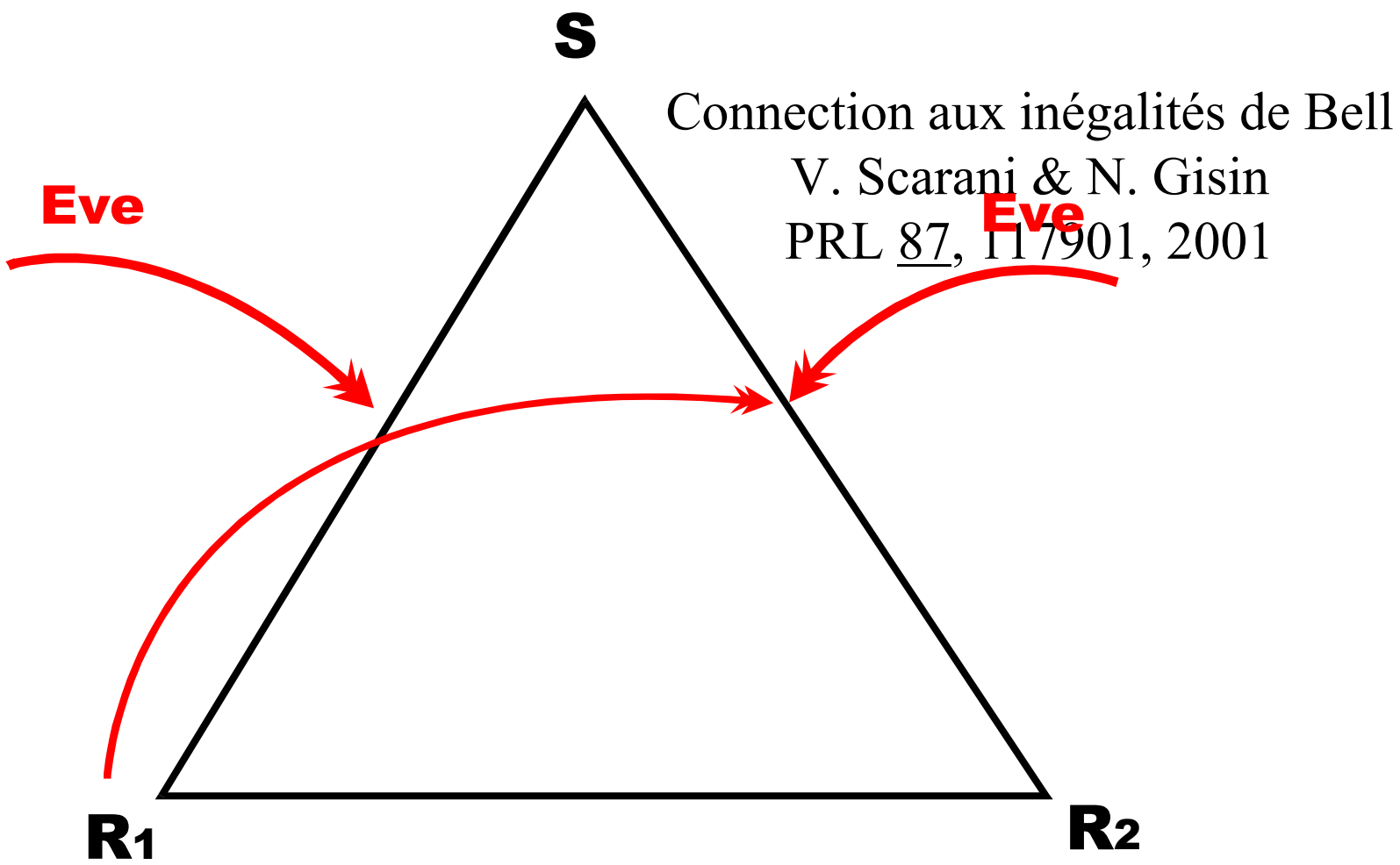
$|GHZ\rangle = |000\rangle + |111\rangle$

W. Tittel et al.
PRA 63, 042301, 2001

Cryptographie quantique avec une source pulsée de paires de photons



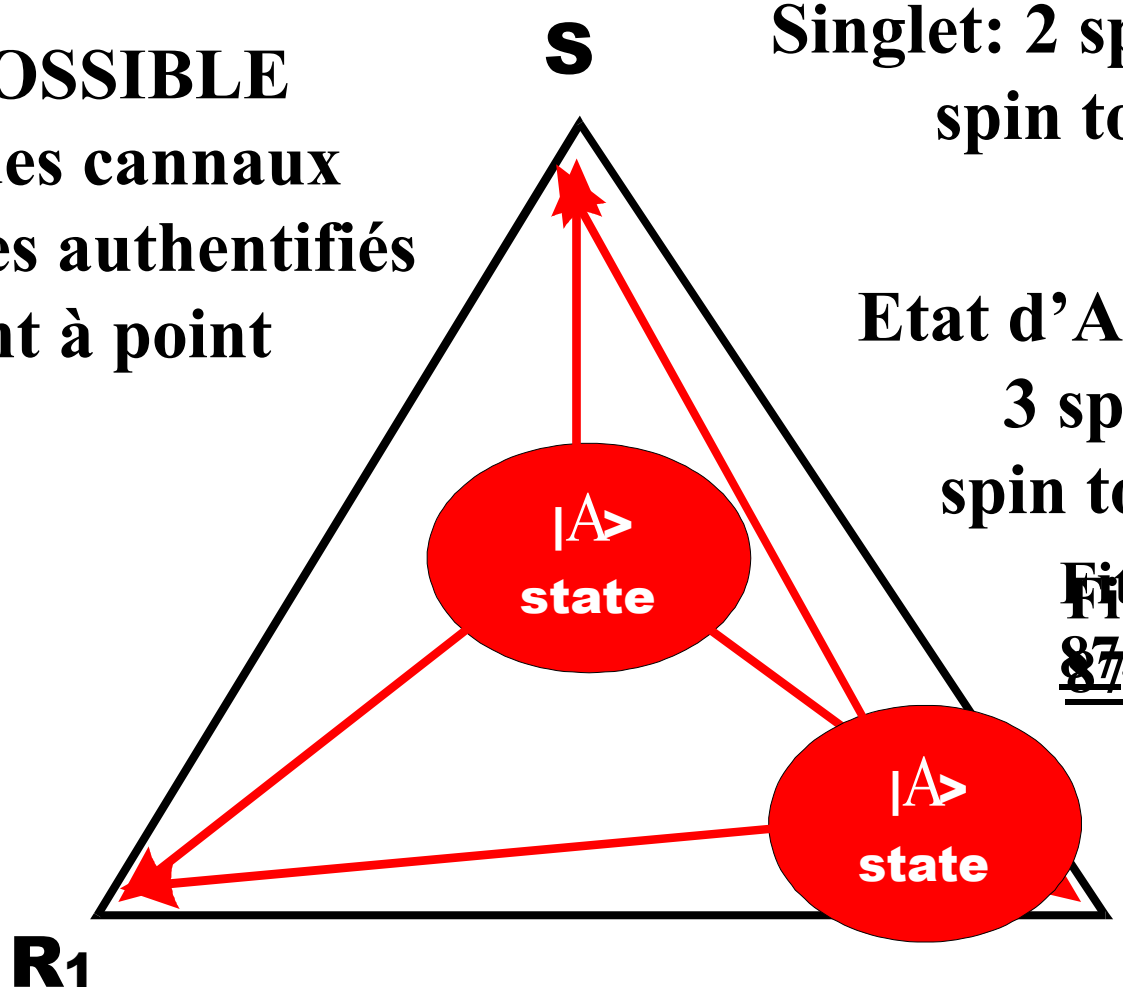
Partage quantique d'un secret: espionnage



Connection aux inégalités de Bell
V. Scarani & N. Gisin
PRL 87, 117901, 2001

Accord Byzantin

IMPOSSIBLE
avec des cannaux classiques authentifiés point à point



Singlet: 2 spin ½, spin total =0

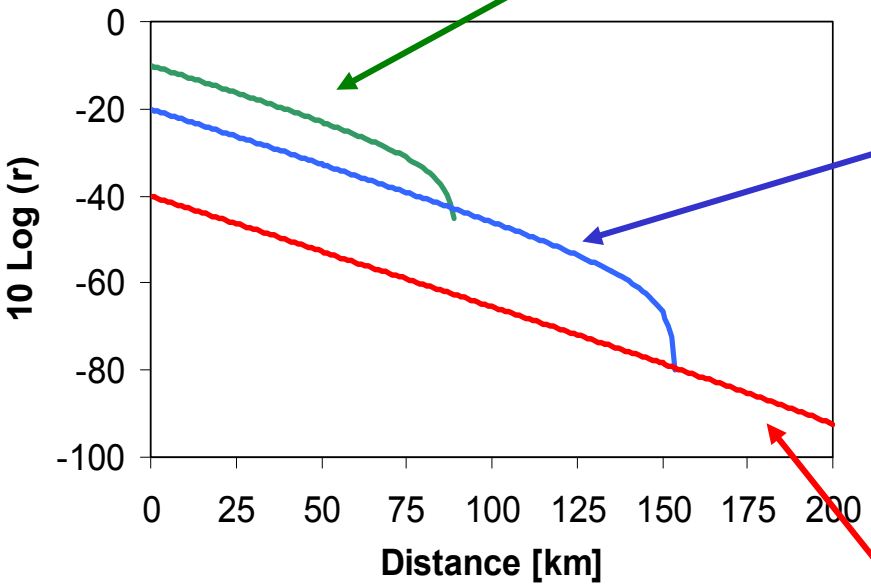
Etat d'Aharonov: 3 spin 1, spin total =0

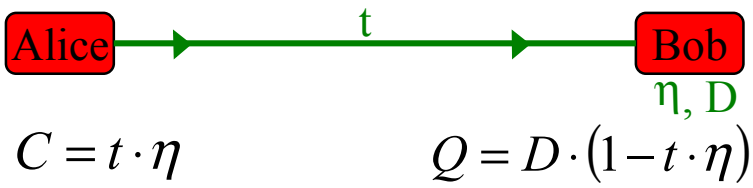
Fitzi et al., PRL 87, 217910, 2001

Répéteurs Quantiques

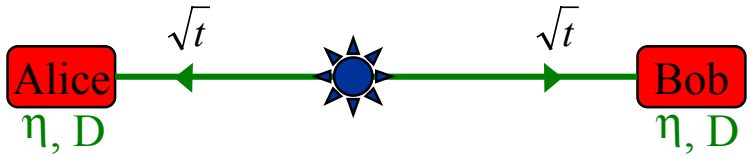
- Pour contrer la décohérence …
  - Mais la décohérence en communication quantique n'est pas un problème!
- Les vrais problèmes sont l'atténuation et le bruit des détecteurs:

  $\Rightarrow$ faible signal / bruit
- Problème: comment lutter contre l'atténuation?
  - De meilleures fibres optiques sont illusoires
  - propagation à l'air libre
  - ou …





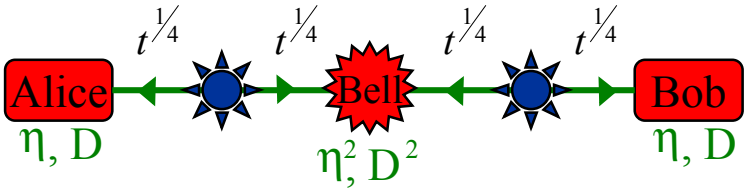
$$C = t \cdot \eta \qquad Q = D \cdot (1 - t \cdot \eta)$$



$$C = t \cdot \eta^2$$

$$Q = \left(1-\sqrt{t\eta}\right)^2 + 2\sqrt{t\eta}\left(1-\sqrt{t\eta}\right)\cdot D$$

$$= \left(\sqrt{t\eta} + \left(1-\sqrt{t\eta}\right)D\right)^2 - t\eta^2$$



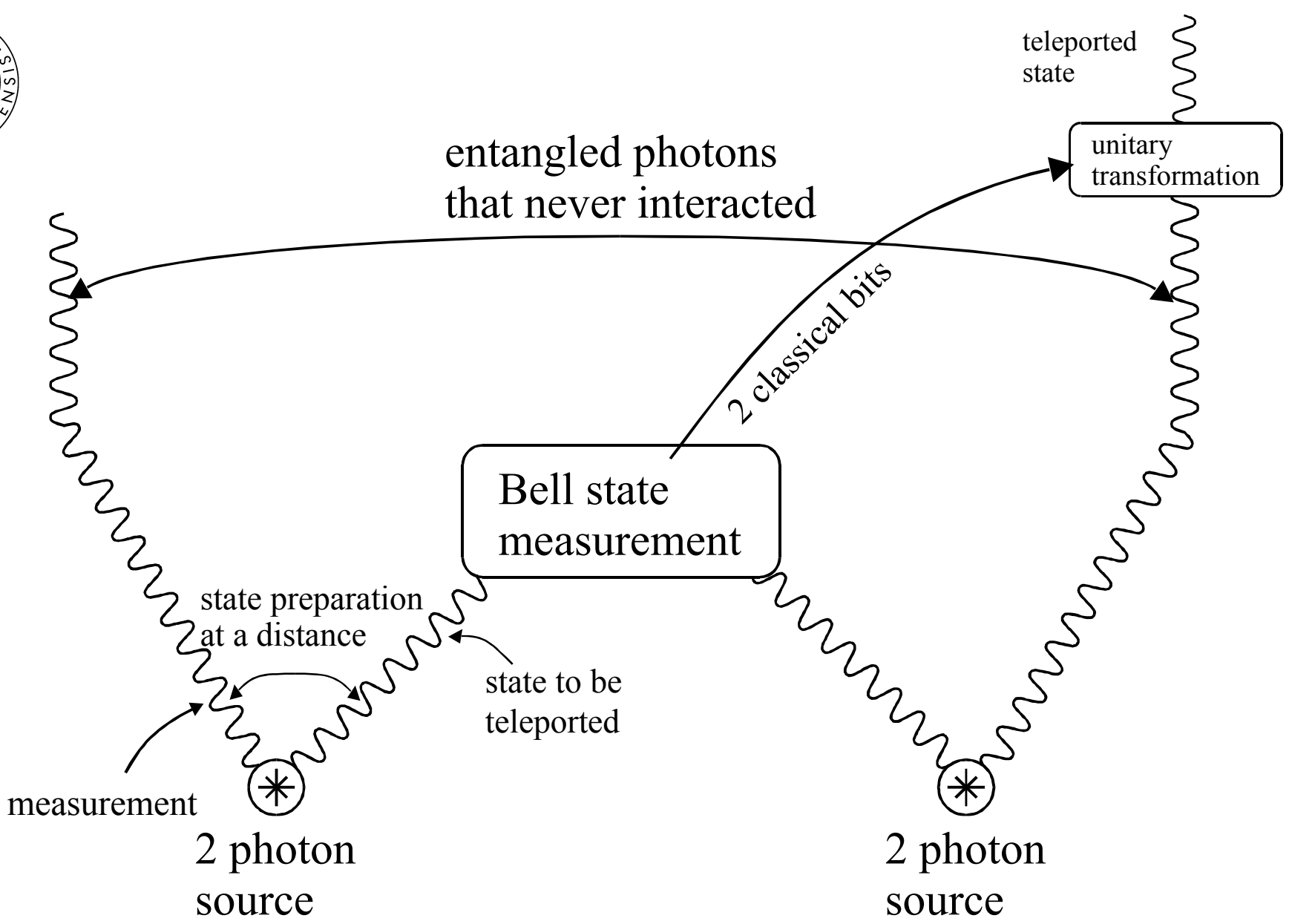
$$C = t \cdot \eta^4$$

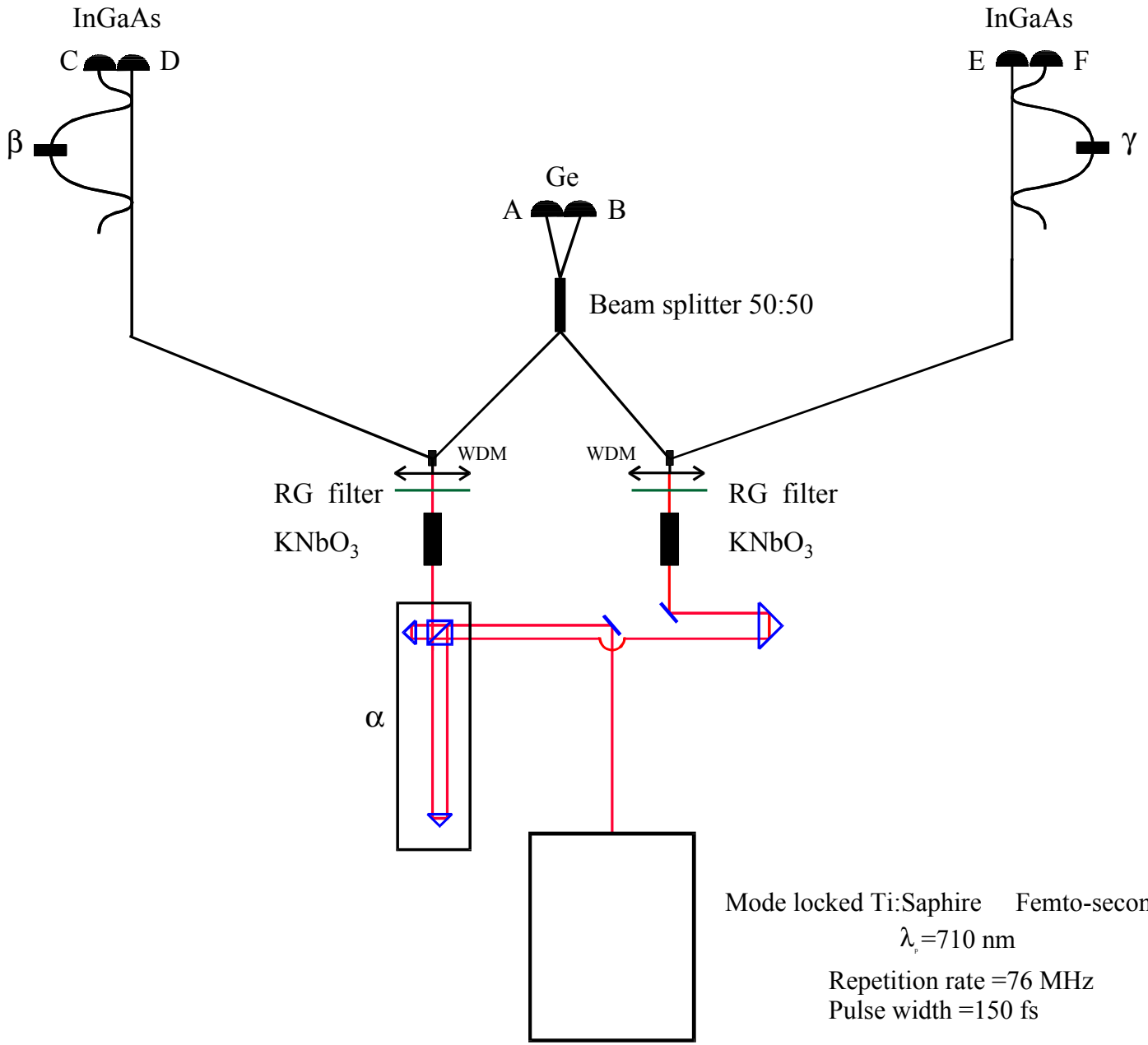
$$Q = \left(t^{1/4}\eta + \left(1 - t^{1/4}\eta\right)D\right)^4 - t\eta^4$$

η = 0.1 det. efficiency;

D = 10^{-4}dark count;

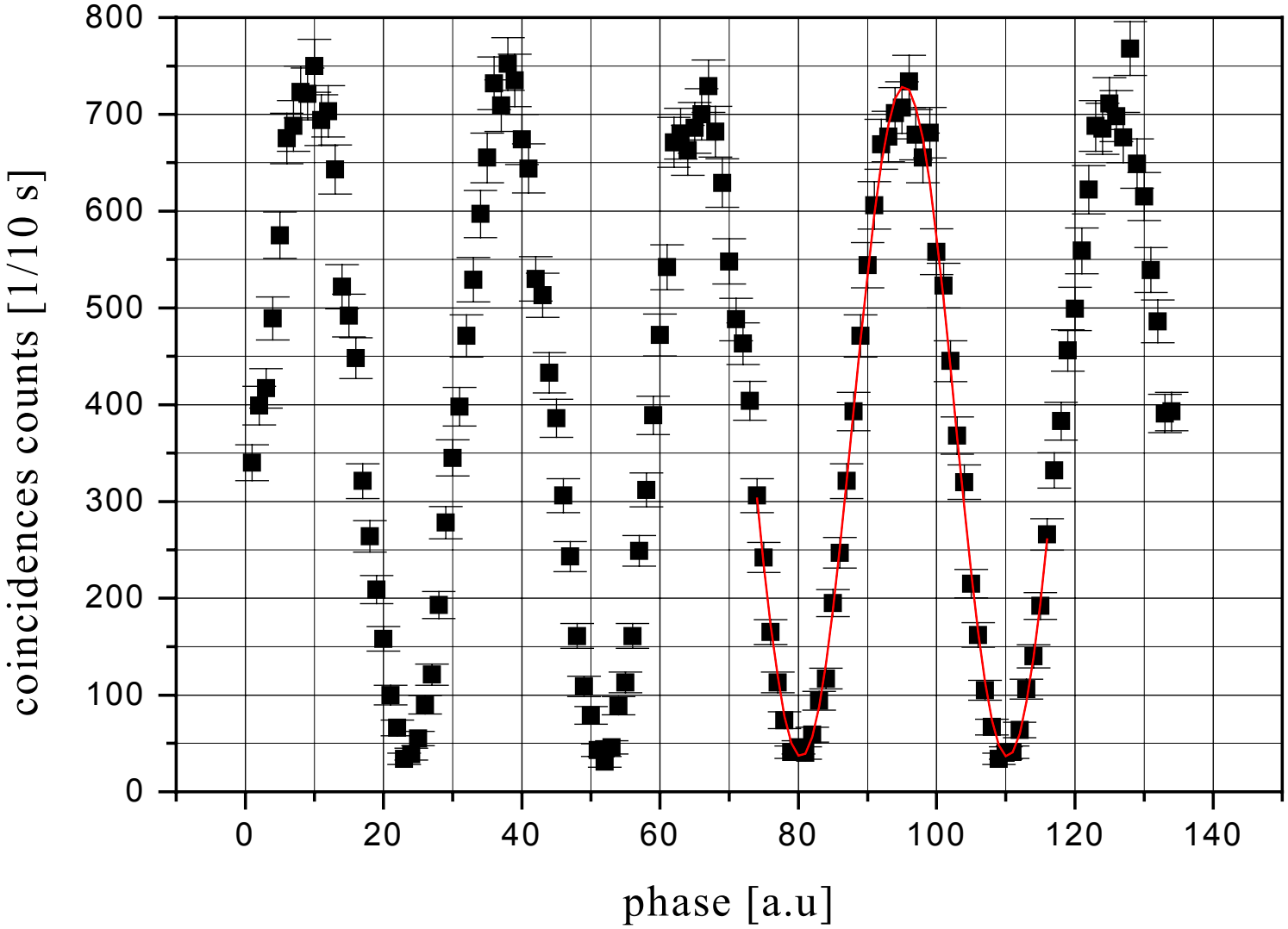
α = 0.25 dB/km attenuation


teleported
state
entangled photons
that never interacted
unitary
transformation
2 classical bits
Bell state
measurement
state preparation
at a distance
state to be
teleported
measurement
2 photon
source
2 photon
source

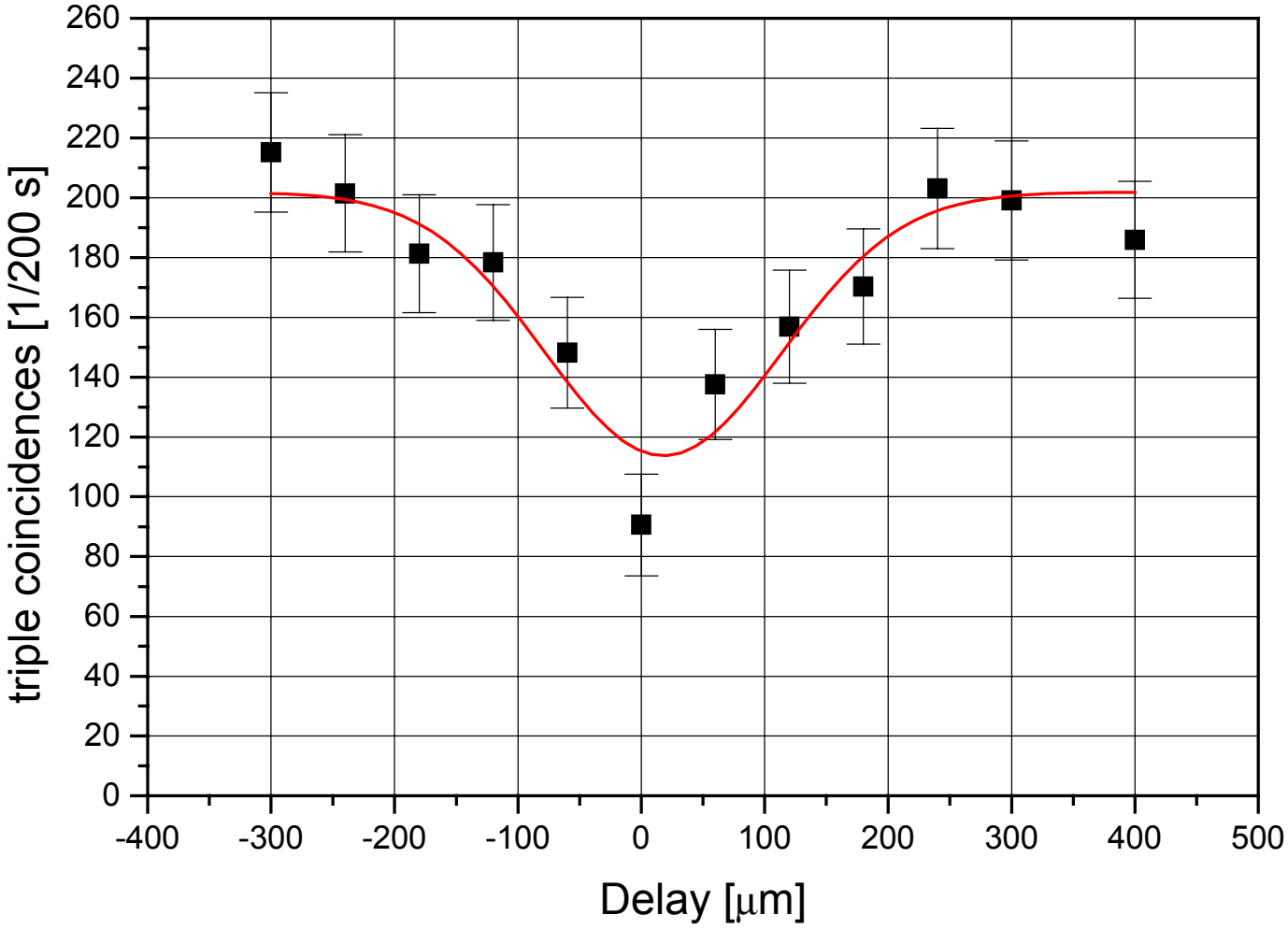

InGaAs
C
D
β
Ge
A
B
InGaAs
E
F
γ
Beam splitter 50:50
WDM
WDM
RG filter
KNbO3
RG filter
KNbO3
α
Mode locked Ti:Saphire Femto-second laser
λp=710 nm
Repetition rate =76 MHz
Pulse width =150 fs

Visibility of 91 ± 0.8 %

Violation of the critical visibility as given by Bell's inequalities by more than 23 standard deviations



« Mandel dip » with two spatially separated sources



Visibility 44.7 ± 5.5 [%]
FWHM 234 ± 3.5 [μm]

Conclusions

- Créer des paires de photons-télécom n'est pas difficile.
- Les fibres optiques protègent bien les photons durant leur propagation.
- La détection reste délicate (bien qu'un premier détecteur commercial existe!) .
- Des expériences de pensées et les principaux protocoles de communications quantiques peuvent être réalisés.
- La cryptographie quantique est une idée magnifique!
- Les communications quantiques relient la physique de base à l'industrie des télécom:
  des corrélations quantiques aux fibres optiques,
  des inégalités de Bell à la confidentialité,
  des relations d'incertitudes à l'information de Shannon.

Références

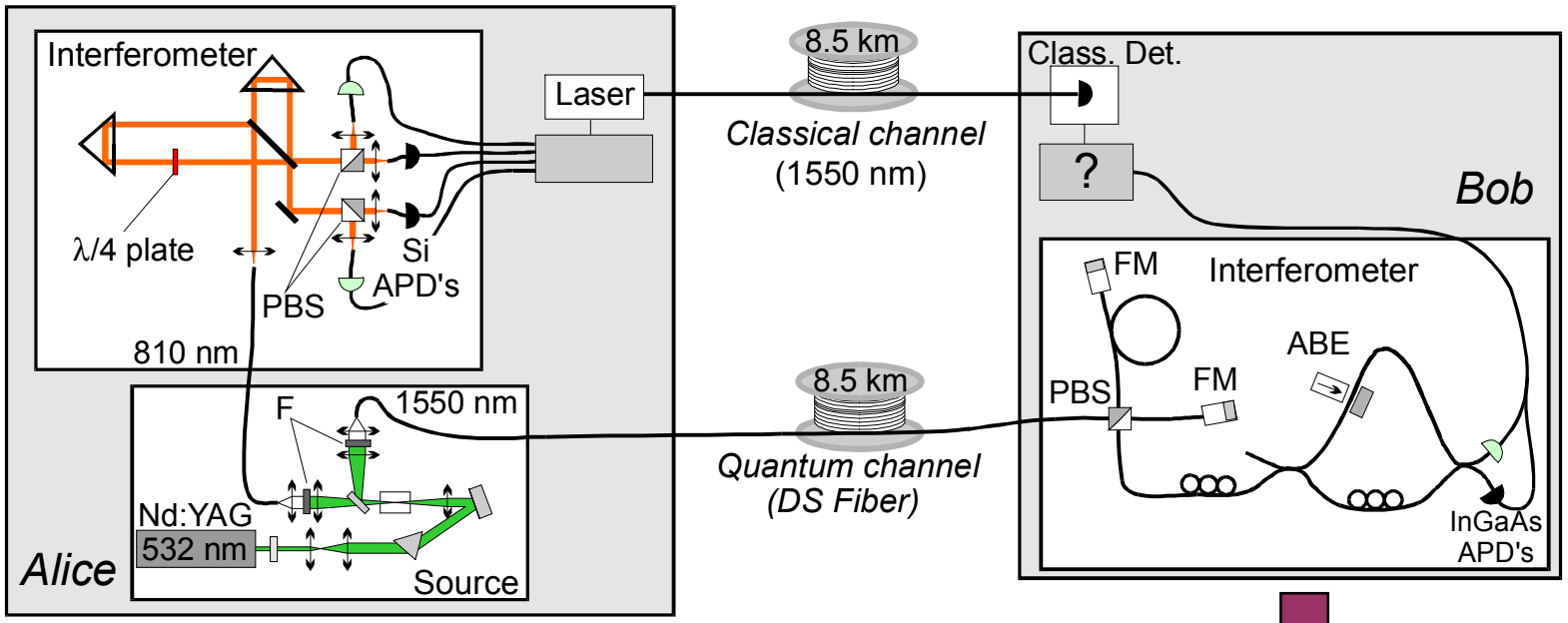
- Quantum Cryptography
  - N. Gisin, G. Ribordy, H. Zbinden, and W. Tittel, "Quantum Cryptography", e-print: http://xxx.lanl.gov/abs/quant-ph/0101098, to appear in Rev. Mod. Phys.

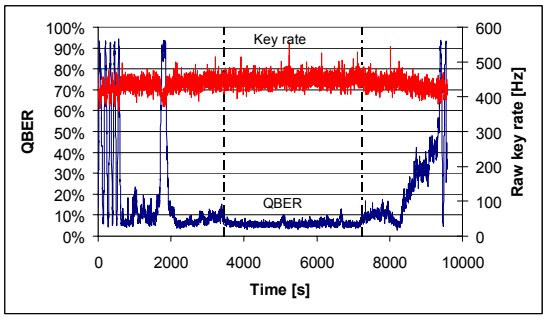
- Single-photon detection with InGaAs/InP APD's
  - P. A. Hiskett *et al.* "Performance and Design of InGaAs/InP Photodiodes for Single-Photon Counting at 1.55 μm", Appl. Opt. **39**, 6818 - 6829 (2000)

  - D. Stucki *et al.*, "Photon counting for quantum key distribution with Peltier cooled InGaAs/InP APD's", e-print: http://xxx.lanl.gov/abs/quant-ph/0106007,

- 2-photon Quantum cryptography
  - G. Ribordy et al., Long distance entanglement based quantum key distributionts using energy-time entangled photons, Phys. Rev. A 63, 012309, 2001

2-υ QC with the source at Alice side



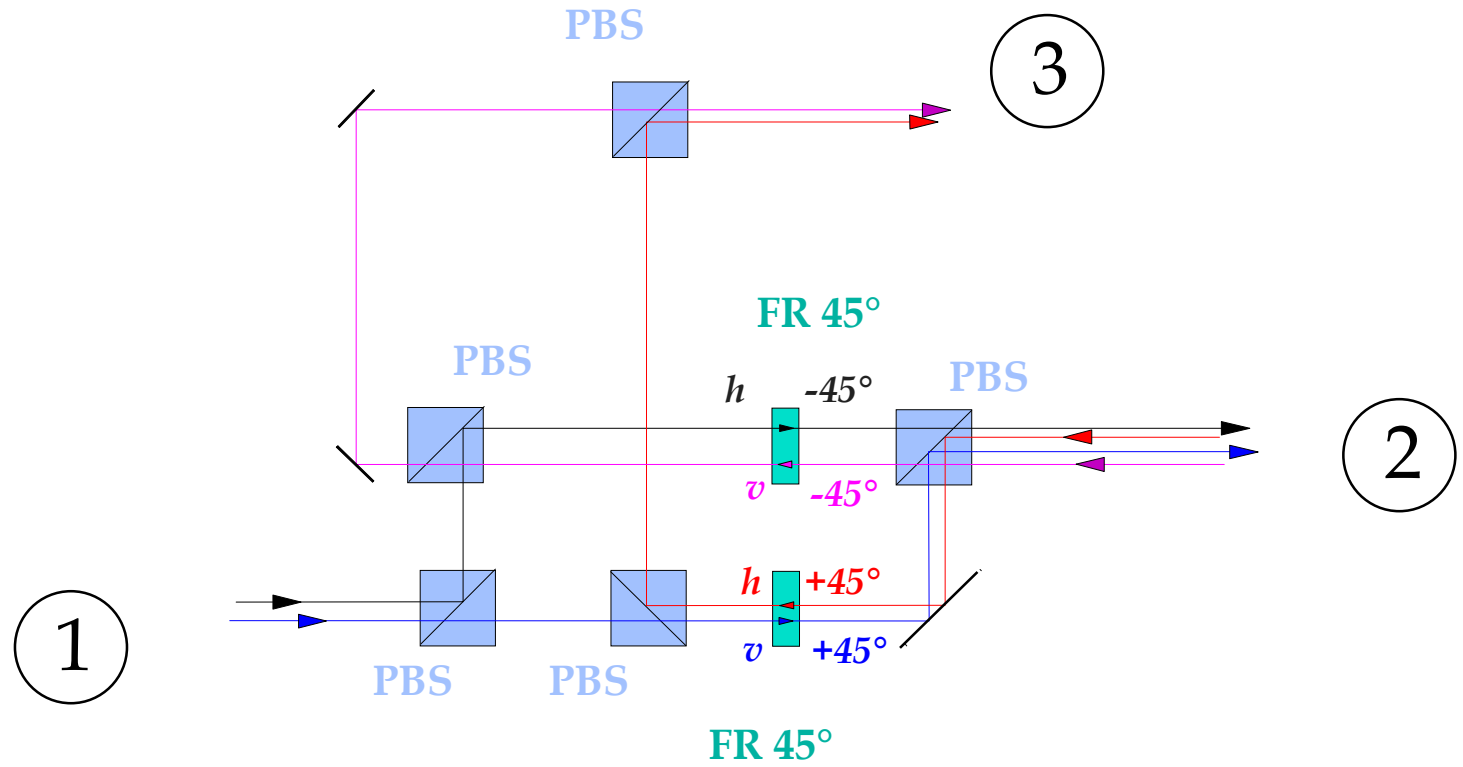


Key Exchange

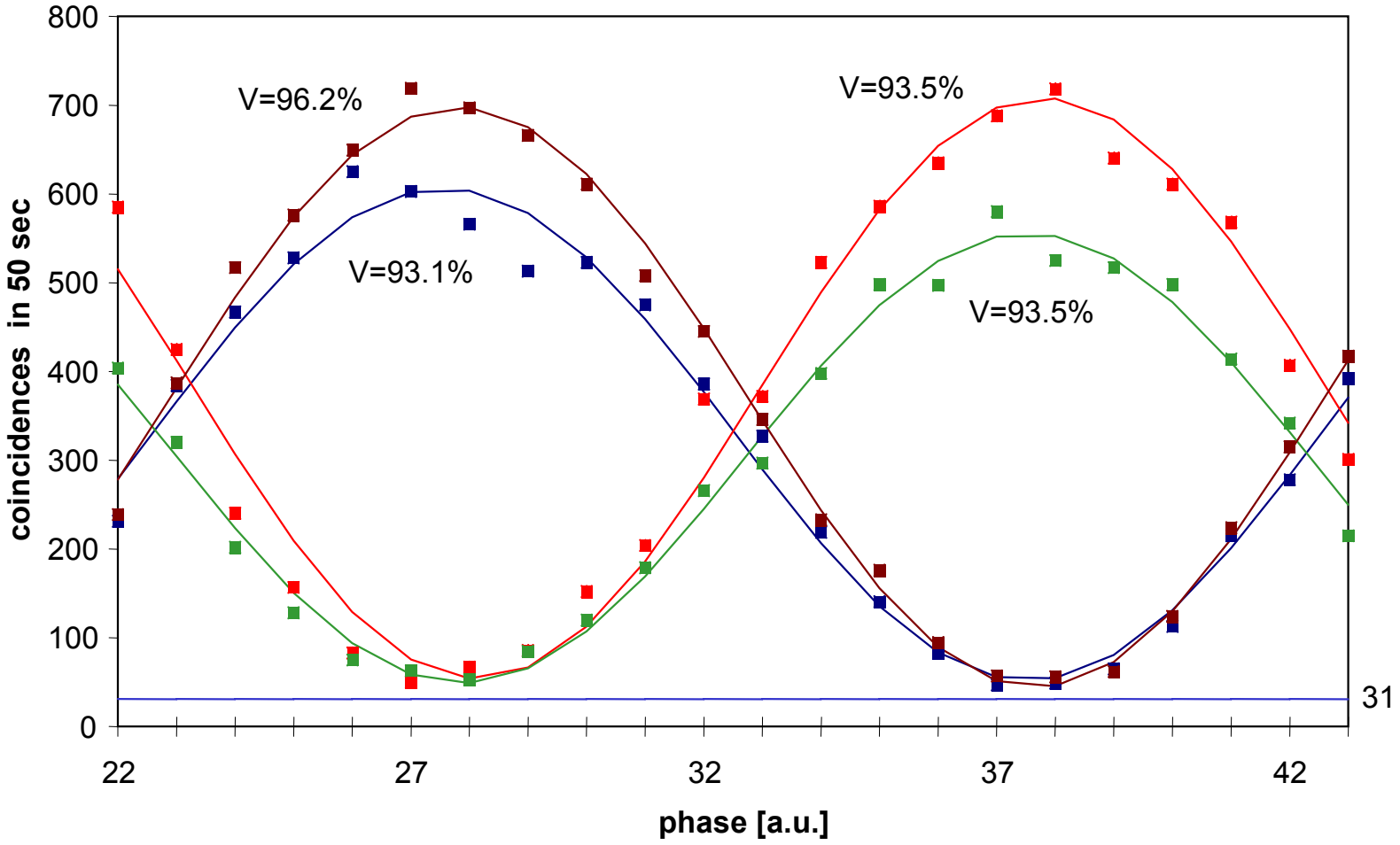
20 m: 1.7 Mbits @ 178 bits/s

8500 m: 0.4 Mbits @ 32 bits/s

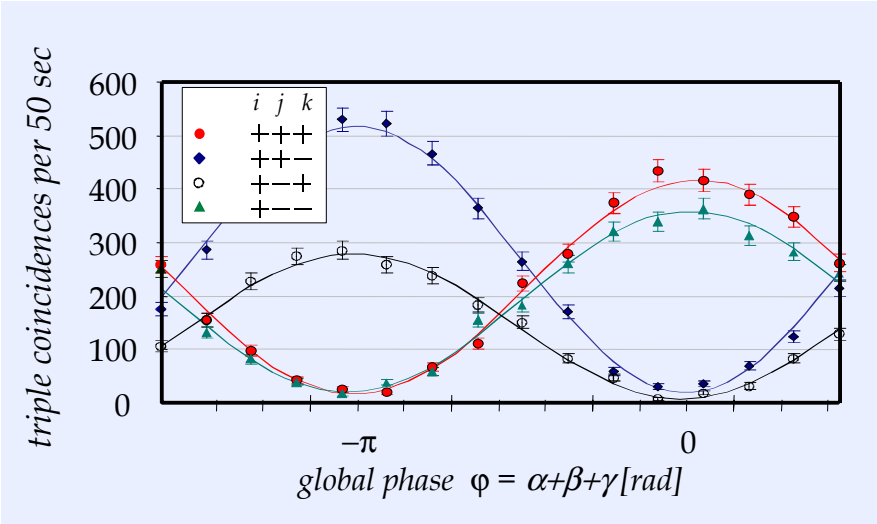
circulateur



Taux de coïncidences



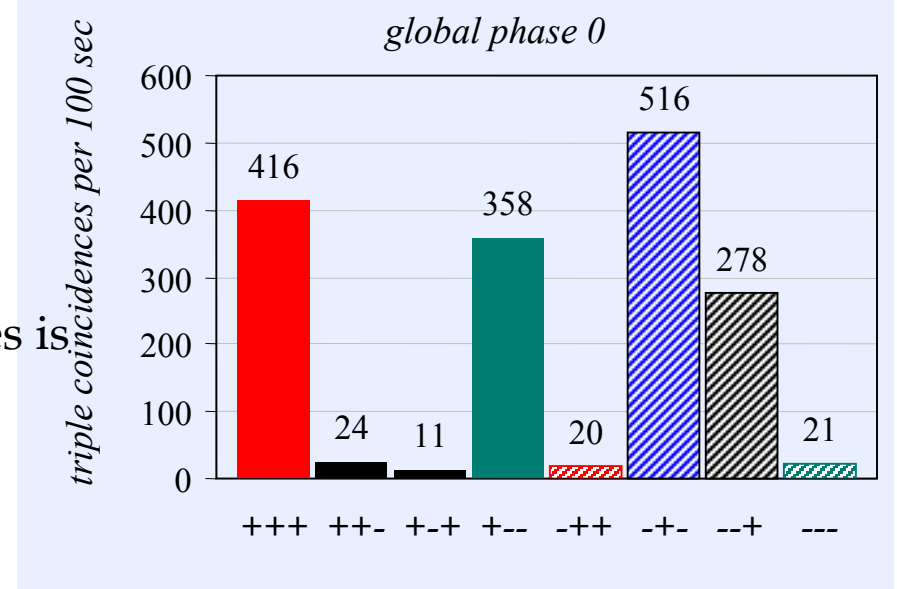
quantum secret sharing : results



- visibility : 89.3 – 94.5 %
- $\alpha+\beta+\gamma = 0$ (I=+1) $ijk = 1$

  and j,k = +1 i =+1

- Bit rate ≈ 15 Hz
- QBER ≈ 4%
- extension to long distances is possible



Répéteurs Quantiques

t = coefficient de transmission
η = efficacité de détection
D = bruit du détecteur

Q = taux de bits incorrects **C = taux de bits corrects**

$\Rightarrow$ **Q + C = taux brut**

$$\text{QBER} = \frac{Q}{Q + C}$$

$$\text{Taux net} = r = (Q+C) \cdot fct(QBER) \approx (Q + C) \cdot \left(1 - \frac{\text{QBER}}{15\%}\right)$$

$$\Rightarrow r = C - \frac{85}{15} Q$$