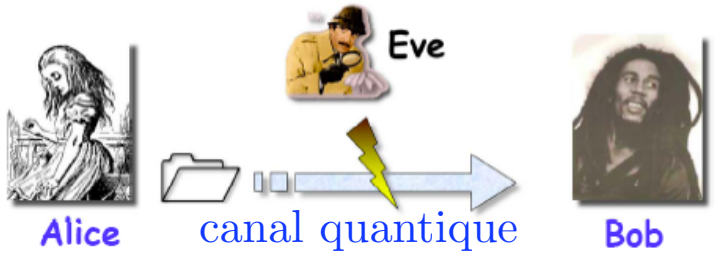
Mardi 24 octobre 2006

Cryptographie quantique
Réalisations expérimentales

Cryptographie quantique : ke za ko ?

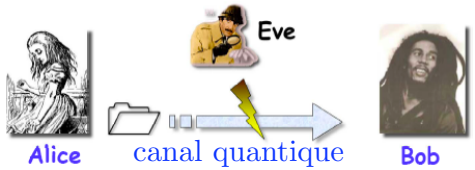


Sécurité assurée par les fondements de la physique quantique

- Avec le langage de la théorie de l'information :

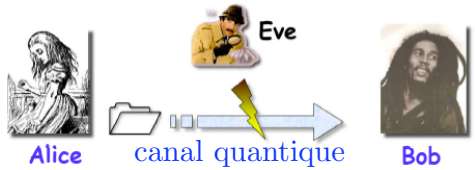
$\mathcal{I}_{AB} > \max\{\mathcal{I}_{AE}, \mathcal{I}_{BE}\}$ ➡ clef secrète !

Cryptographie quantique : principe



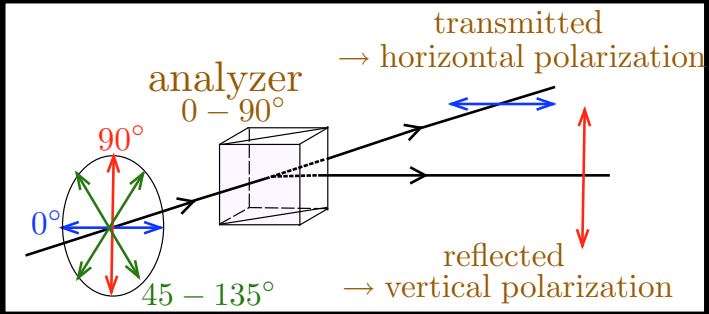
- Pour espionner un "canal de communication quantique", Eve doit effectuer des mesures sur des quantas individuels.
  - ex: impulsions à un photon
- Mais la physique quantique nous dit que "toute mesure effectuée sur un système quantique le perturbe"
- Donc "lire" le signal quantique diminue la corrélation entre les données partagées par Alice et Bob
- Alice et Bob peuvent détecter l'intervention d'Eve en comparant (via un canal de communication classique) un échantillon des données obtenues avec le signal quantique

Cryptographie quantique : remarques



- Le canal quantique n'est pas utilisé pour transmettre un message (c'est-à-dire une information existante). Seule une "clef" est transmise (pas d'information).
- S'il s'avère que la clef est corrompue, Alice et Bob la jettent (pas de perte d'information). Par contre, si la clef passe le test avec succès, alors Alice et Bob peuvent l'utiliser en toute confiance.
- La confidentialité de la clef doit être contrôlée avant que le message ne soit envoyé par Alice à Bob

Codage en polarisation d'un photon

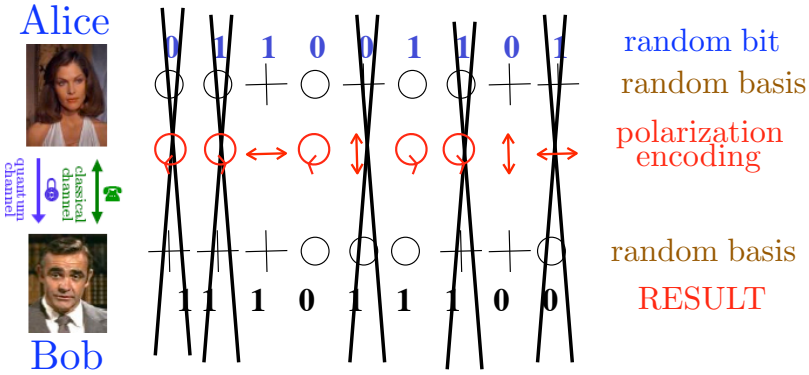


• Pour la même base de polarisation 0°–90°, la détection du photon sur une voie de sortie permet de connaître l'état de polarisation d'entrée du photon.

• Pour des bases différentes, le résultat devient aléatoire (50%–50% pour la base 45°–135°) et la détection n'apporte plus d'information sur la polarisation d'entrée.

• De plus, cette information a été effacée !

Protocole BB84



Charles BENNETT et Gilles BRASSART (1984)

Cryptographie quantique : questions...

Qu'est-ce qui est vraiment quantique dans la cryptographie quantique ?

→ théorème de "non-clonage"

- **Il est impossible de copier un état quantique arbitraire choisi parmi un ensemble d'états non orthogonaux**
- **Au delà de conséquences pour la sécurité de la cryptographie quantique, le clonage aurait des conséquences physiques inacceptables**
  - **violation des inégalités de Heisenberg**
  - **conflit avec la relativité restreinte (théorie locale)**

Comment mettre en œuvre en pratique ces belles idées ?

Propagation en espace libre

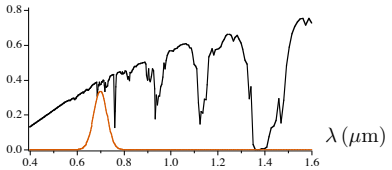
- $\lambda \sim 750 - 800$ nm
- Portée 2 km ⟶ satellite
- codage en polarisation

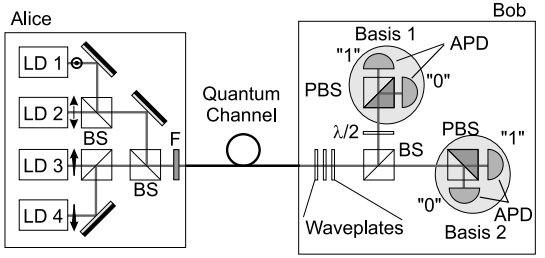
Photons uniques ≃ Laser atténué

$P_n = e^{-\mu}\frac{\mu^n}{n!} \simeq \frac{\mu^n}{n!}$ pour $\mu \ll 1$

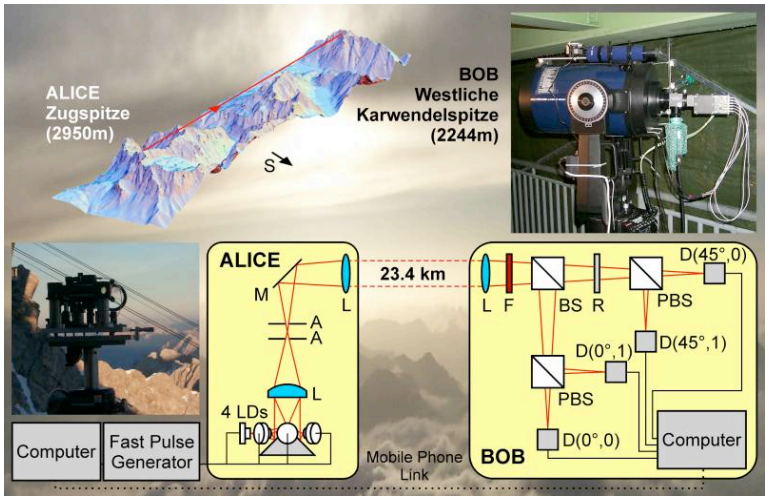
transmission rate $\propto \mathcal{P}(1) \simeq \mu$ $(\mu \leq 1)$

Atmospheric transmission (vertical direction, 99 km)





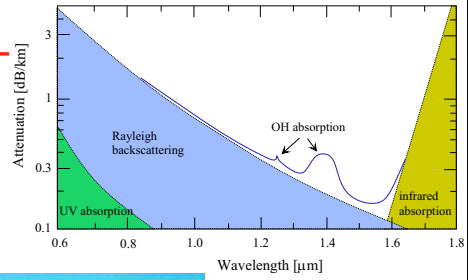
Démonstration de QKD en “espace libre”

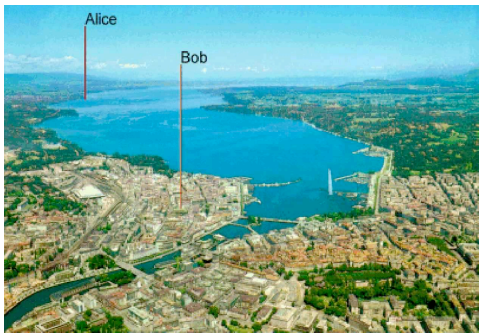


C. Kurtsiefer et al, (2002), *Nature*, **419**, 450.

Fibres optique

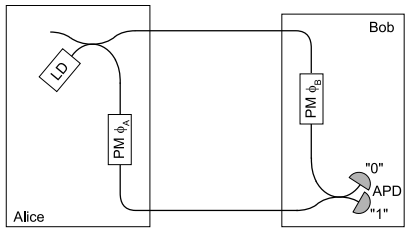
- $\lambda = 1550$ ou 1300 nm
  $T = 10^{-\alpha l}$ avec $\alpha = 0.25$ dB/km
- portée : 50 à 100 km

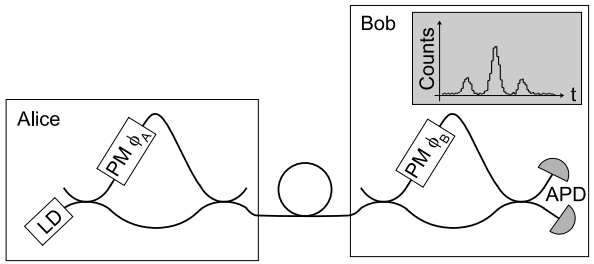




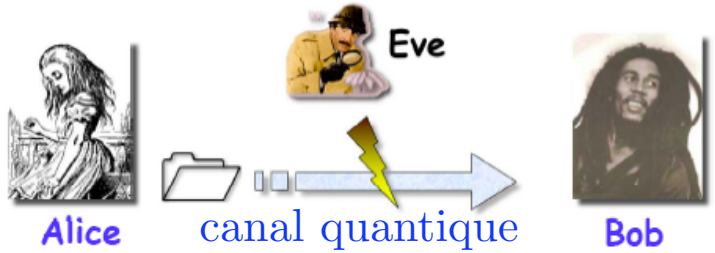
QKD et interférométrie (fibres optiques)

- $\lambda = 1550$ ou 1300 nm
  $T = 10^{-\alpha l}$ avec $\alpha = 0.25$ dB/km
- portée : 50 à 100 km
- codage en phase





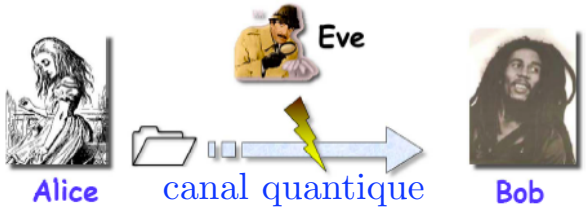
Crypto. quantique et inégalité de Bell



Utilisation des inégalités de Bell comme test de sécurité

A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991)

Cryptographie quantique : expériences



Influence des défauts

1. **Bruit des détecteurs (coups d'obscurité)**
2. **Statistique d'émission des photons**
3. **Utilisation de sources de photon unique**

Bruit des détecteurs

Probabilité de détection $\mu T \eta$
Probabilité de fausse détection p_{dark}

$$QBER = p_{\text{dark}}/\mu T\eta$$
$$T = 10^{-\alpha l/10} = p_{\text{dark}}/\mu\eta QBER$$
$$l = \frac{10}{\alpha}\log_{10}\frac{\mu\eta QBER}{p_{\text{dark}}}$$

λ	p_{dark}	α	η	$l_{\max}$	
800 nm	10^{-8}	2 dB/km	50 %	28 km	($\mu = 0.1$)
1300 nm	10^{-5}	0,35 dB/km	20 %	65 km	
1550 nm	10^{-5}	0,25 dB/km	10 %	80 km	

Attaque "PNS" : séparation des photons

Pour chaque impulsion, Ève mesure le nombre de photons n ;

si $n \geq 1$, Ève laisse passer $n-1$ photons jusqu'à Bob et en stocke 1 dans une mémoire quantique.
si $n = 1$, elle le bloque (si possible).

Une fois que Bob a révélé ses bases,
Ève peut connaître parfaitement les impulsions stockées

Bob reçoit $\sim T\mu$ impulsions,
Ève en intercepte $p_2 \simeq \frac{1}{2}\mu^2$.

$\longrightarrow$ portée maximale $T = \dfrac{p_2}{p_1} = \dfrac{1}{2} \times \mu$

$$l_{\max} = \underbrace{\frac{10}{\alpha}\log_{10} 2}_{12\text{ km}} - \underbrace{\frac{10}{\alpha}}_{40\text{ km}}\log_{10}\mu$$

Soit 52 km pour $\mu = 0.1$ et 92 km pour $\mu = 0.01$

Comment combattre l'attaque "PNS" ? (1)

Protocole SARG
Scarani Acín Ribordy Gisin 2002 (quant-ph/0211131)

- Physiquement identique à BB84
- Communications classiques différentes :
  Choix entre deux états non-orthogonaux.
- Débit divisé par 2.
- Ève n'a que 0.4 bit par impulsion $n = 2$.
- Elle a toute l'information uniquement pour $n = 3$, avec $p_{\text{OK}} = \frac{1}{2}$.

$$p_3 \simeq \tfrac{1}{6}\mu^3$$
$$T > \frac{p_3}{2p_1} = \tfrac{1}{12}\mu^2$$
$$l_{\max} = \frac{10}{\alpha}\log_{10} 12 - \frac{20}{\alpha}\log_{10}\mu$$

Comment combattre l'attaque "PNS" ? (2)

Protocoles à appâts
Decoy states

μ variable permet de repérer les attaques bloquantes

p_0	p_1	p_2
80%	20%	2%
90%	10%	0.5%
95%	5%	0.13%

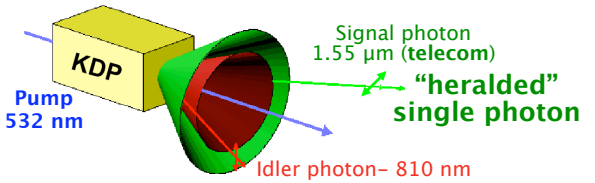
Ève ne peut moduler ses attaque qu'en fonction du nombre de photons, et non de μ.

Comment combattre l'attaque "PNS" ? (3)

Source de photon unique $\mu = 1$

- photon unique "annoncé"

Cristal non-linéaire génère des photons par paire, avec conservation de l'énergie et de l'impulsion



$$QBER = p_{\text{dark}}/\mu T\eta$$
$$T = 10^{-\alpha l/10} = p_{\text{dark}}/\mu\eta QBER$$
$$l = \frac{10}{\alpha}\log_{10}\frac{\mu\eta QBER}{p_{\text{dark}}}$$

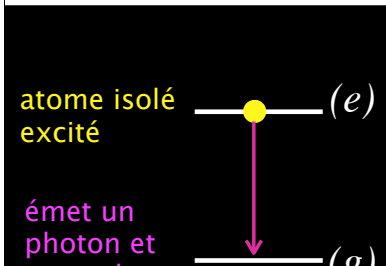
$\mu = 1 \longrightarrow$

λ	$l_{\max}$
800 nm	33 km
1300 nm	93 km
1550 nm	120 km

Comment combattre l'attaque "PNS" ? (3)

Source de photon unique $\mu = 1$

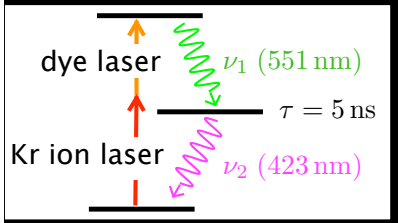
- photon unique "annoncé"
- photon unique "à la demande"



Dans les sources lumineuses classiques (lampe fluorescente, laser, LED, ...) un très grand nombre d'émetteurs sont excités simultanément.
Comment isoler un seul atome, ou plus généralement un seul centre émetteur excité ?

Première source de photon unique

Alain Aspect et Philippe Grangier – 1986

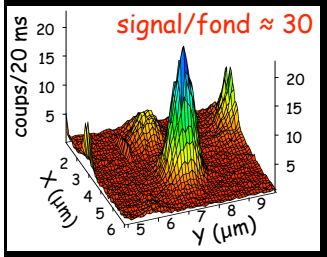


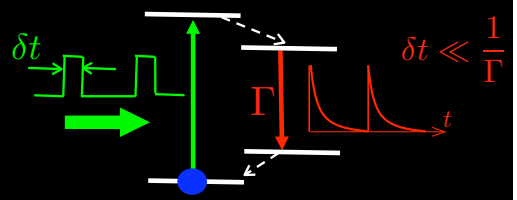
Cascade radiative atomique.
Atome unique isolé temporellement : pendant une durée de 5 ns suivant la détection de ν_1 un atome unique est pret à émettre un photon et un seul de fréquence ν_2.

- On utilise des atomes ou ions refroidis et piégés
- Il s'agit cependant de sources complexes à mettre en œuvre
- Peut-on imaginer des sources de photon unique plus "pratiques", (presque) "presse-bouton" ?

Utilisation de molécules uniques

Molécule isolée spatialement

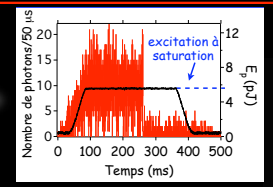




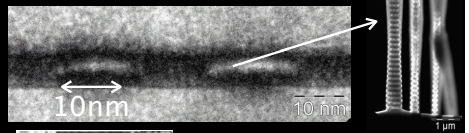
F. De Martini et al., *Phys. Rev. Lett.* **76**, 900 (1996)
B. Lounis & W. E. Moerner, *Nature* **407**, 491 (2000)

Quel émetteur peut-on choisir ?

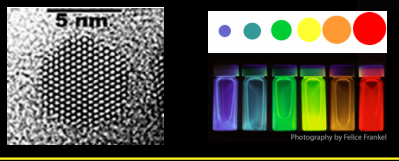
Molécules :
souplesse d'emploi, efficacité élevée, mais photoblanchiment (10^5 à 10^6 photons à T ambiant)



Boîtes quantiques d'InAs dans des micro-piliers



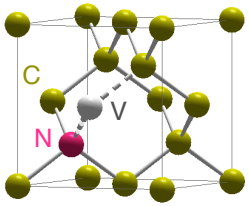
Nanocristaux de CdSe
Spectre d'émission étroit relié à la taille des nanocristaux

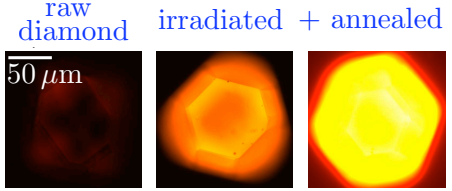


Centres colorés NV du diamant
"molécule artificielle" parfaitement photostable

Centres colorés NV du diamant

atome d'azote (N) comme impureté associé à une lacune (V) dans le site adjacent de la maille cristalline

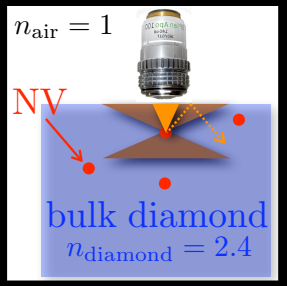




photoluminescence of a microcrystal
$\lambda_{exc} = 500 - 550\,nm$

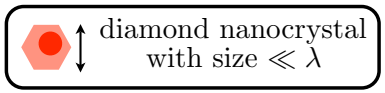
- Les impuretés d'azote sont naturellement présentes dans du diamant synthétique (type I)
- Irradiation électronique permettant de créer les lacunes V dans le cristal + recuit à 800°C

Emission des défauts dans le diamant

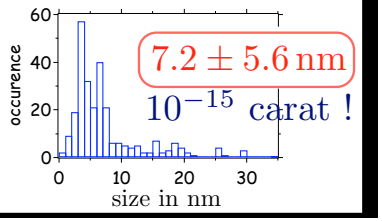


Limit angle ~ 24.5°
Photons are trapped in the crystal by internal reflection...
Optical aberrations induced by the strong mismatch of indexes of refraction

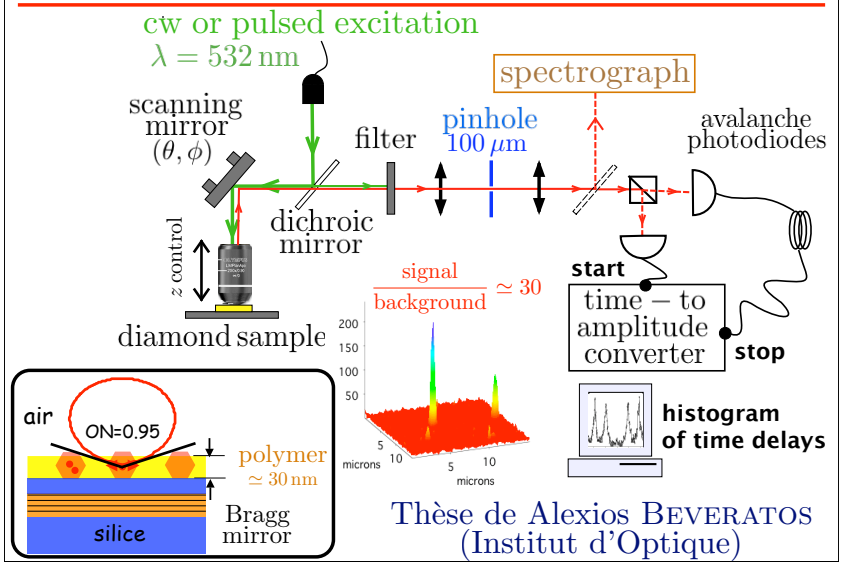
- **How to circumvent emission in bulk ?**



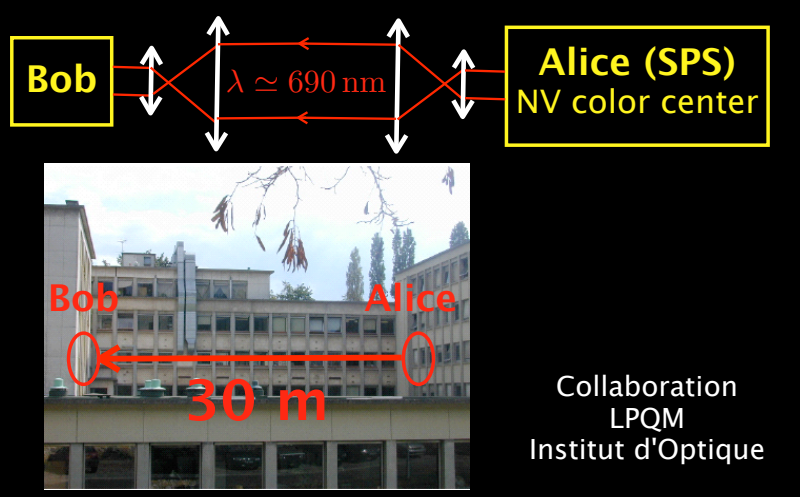
abrasive diamond powder dispersed in a polymer
size selection by centrifugation
Thierry GACOIN (PMC)



Détection par microscopie confocale

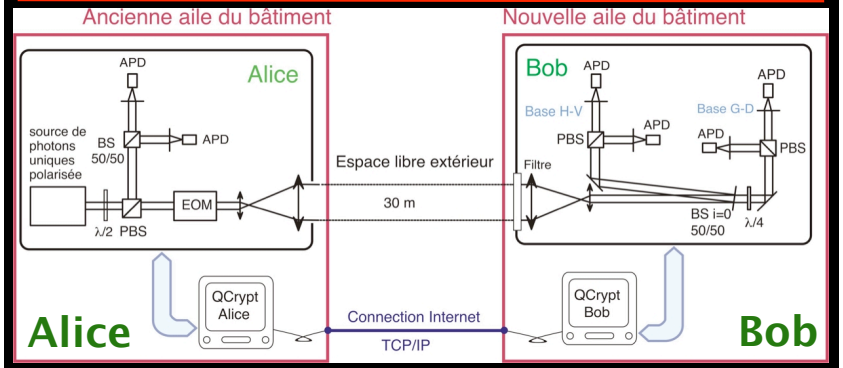


Single-photon QKD in open-air



Collaboration
LPQM
Institut d'Optique

QKD experimental setup



overall quantum efficiency $\mu = 0.0235$
repetition rate : 5.3 MHz
polarized single photon rate : 142×10^5 counts/s

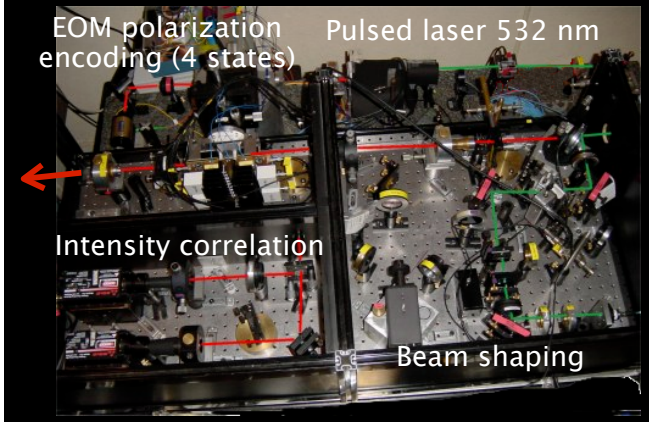
key : sequence of 10^6 bits sent Alice (0.2 s)

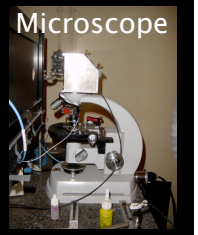
BB84 initial random sequence

- Sequence of encoded polarization bits generated with hardware electronics, using two programmable electronic linear shift registers in Fibonacci configuration.
- Each register gives a pseudo-random sequence of $2^{20}-1=1048575$ bits.
- "BB84" 4-polarization states are coded with two bits. Each of them belongs to one of the two (pseudo) random sequences.

ALICE : experimental set-up

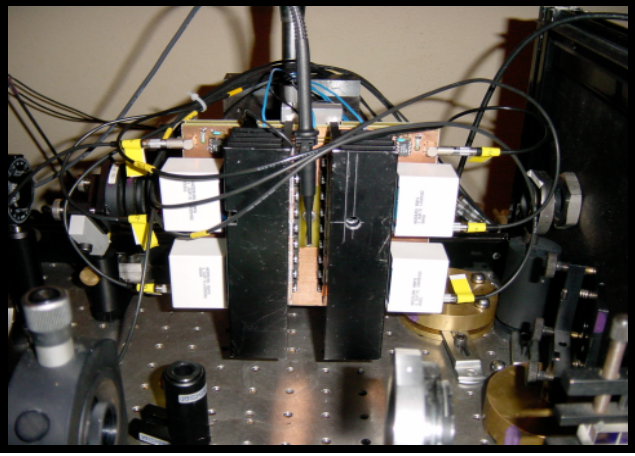
Single photon source and polarization encoding



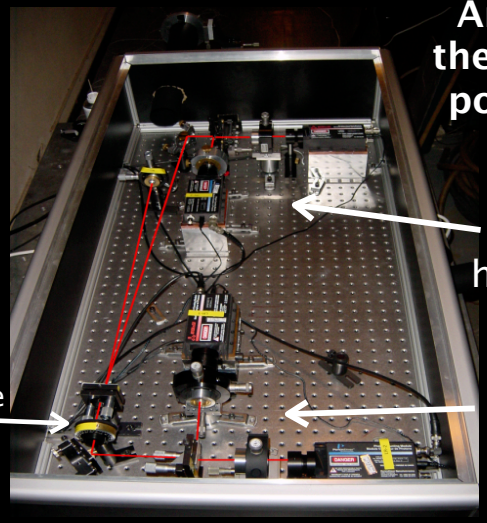


Electro-optical modulator

4 states (H,V,L,R) – switches 500 V in 30 ns
Transmission of 90% @ λ=632 nm



BOB : experimental set-up



Analysis of the four BB84 polarization states

Linear
horizontal
vertical

Circular
left
right

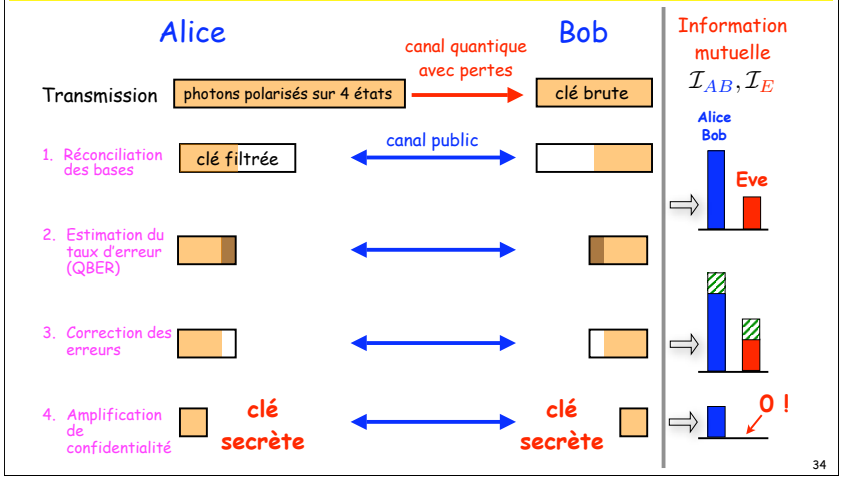
Alice by night…

Exchanging photons with Bob…

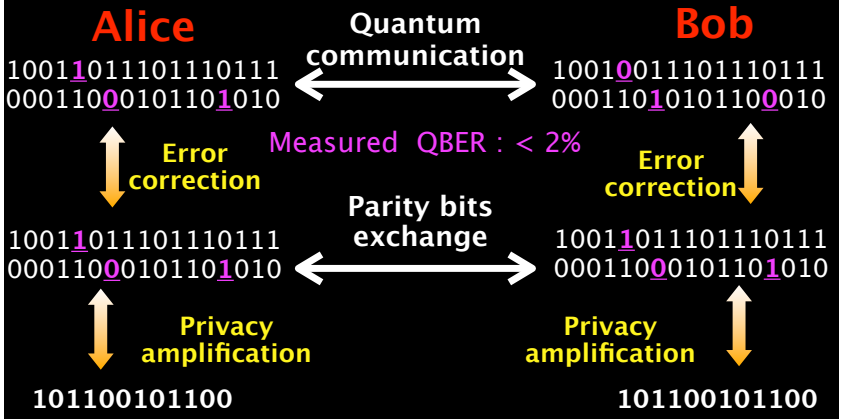
The two wings
of the Institut d'Optique building in Orsay
about 35 meters away

Distillation de la clé secrète (1)

$\mathcal{I}_{AB} > \max\{\mathcal{I}_{AE}, \mathcal{I}_{BE}\}$ ➡ clef secrète !



Distillation de la clé secrète (1)

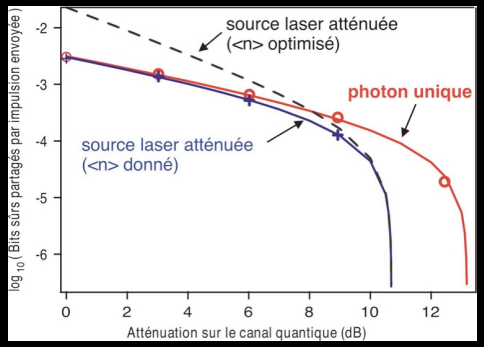


Error correction and privacy amplification : software « QUCRYPT », Louis Salvail (http://www.cki.au.dk/)

Secret bit rate > 16 kbits /s

Long distance transmission

Secure bit rate per pulse between Alice and Bob,
as a function of attenuation on the quantum channel



When $P(2) = P_{\text{detection}}$ secure bit rate vanishes

Use of pure single photon states gives measurable advantage over systems with weak coherent pulses

Potentiel industriel à moyen et long terme

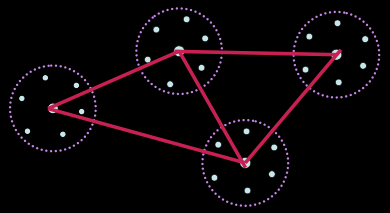
MagiQ (Boston, USA)
www.magiqtech.com

IdQuantique
(Genève, Suisse)
www.idquantique.com

SmartQuantum
(Lannion/Metz, France)
www.smartquantum.com

Conclusion

- **La cryptographie quantique progresse régulièrement**
  - des systèmes sont disponibles commercialement
  - défi actuel : mise en oeuvre et évaluation en réseau



SECOQC

Secure communication based on quantum cryptography

- **Ne pas croire que tout s'arrête au protocole imaginé par Bennett et Brassard, qu'on ne pourrait que raffiner !**

→ cryptographie quantique à "variables continues"