

# Physique Quantique

## Cours 2009-2010: Cinquième Leçon

### 15 Février 2010

Nous terminons aujourd'hui la série de leçons sur le clonage quantique en commençant (&V-A) par décrire *l'expérience de clonage par conversion paramétrique* de qubits codés dans la polarisation de photons dont le principe a été donné à la fin de la leçon 4. Cette expérience et d'autres du même genre ont permis de mettre en évidence l'effet d'amplification d'un mode du champ par émission stimulée et d'obtenir une fidélité de clonage en bon accord avec la théorie, mais elle est très délicate car elle demande beaucoup de soin dans l'alignement optique et l'accord temporel des modes. Elle repose surtout sur un processus de post-sélection qui ne retient qu'une toute petite fraction des événements.

Nous abordons ensuite (&V-B) l'analyse du clonage comme « *méthode d'attaque* » en *cryptographie*. Nous montrons comment les performances du clonage imposent une limite au taux de bruit acceptable sur un canal de communication quantique pour l'échange d'une clé cryptographique que l'on veut à l'abri de tout espionnage.

Nous revenons enfin au &V-C sur le *lien entre clonage et communication super-luminale* en montrant que la limite de fidélité du clonage optimal est précisément celle au-delà de laquelle la communication instantanée d'information basée sur l'intrication quantique deviendrait possible.

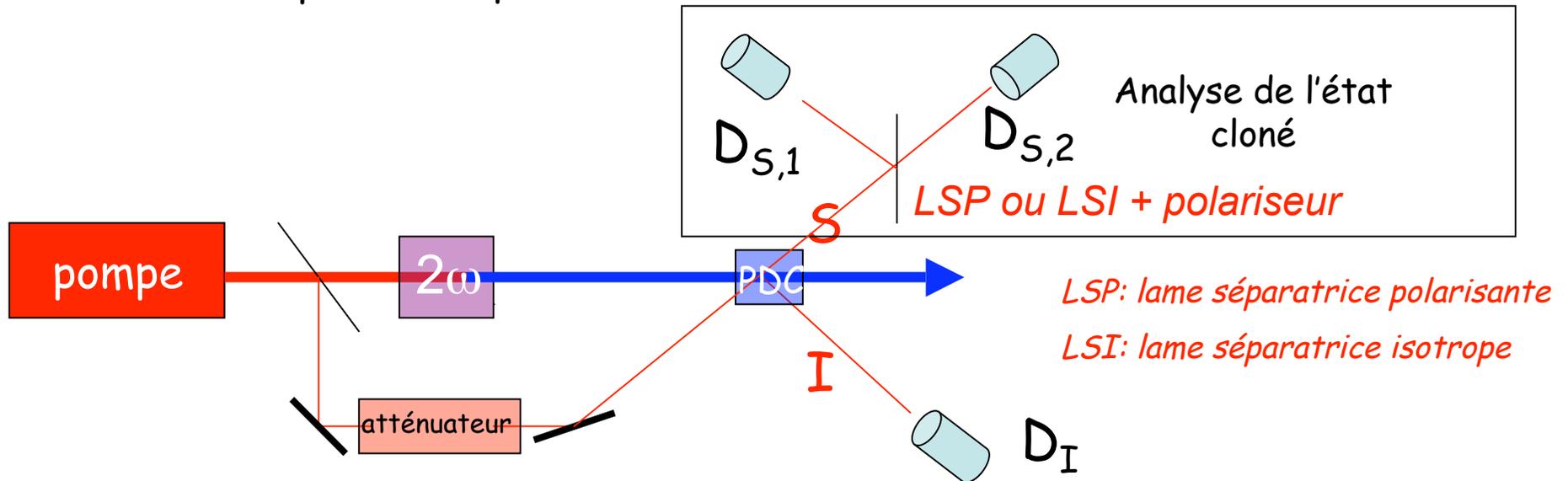
V-A

# Expérience de clonage de photon par amplification optique

A.Lamas-Linares, C.Simon, J.C.Howell et D.Bouwmeester,  
Science, 296, 712 (2002).

# Expérience de clonage par amplification

Le processus de clonage utilisé dans l'expérience de clonage de *Lamas Linares et al* est la conversion paramétrique dans un cristal non linéaire « PDC ».



La conversion paramétrique en impulsion temporelle crée des paires de photon suivant un mécanisme décrit par le hamiltonien:

$$H = \gamma a_p (a_{VS}^\dagger a_{HI}^\dagger - a_{HS}^\dagger a_{VI}^\dagger) + Hc \quad (5-1)$$

L'annihilation d'un photon pompe ( $a_p$ ) s'accompagne de la création d'une paire de photons «signal (S)» et «idler (I)» de fréquence moitié et polarisés soit H soit V. Une paire de photons intriqués est créée. Un signal faible, contenant au plus un photon par pulse est envoyé à travers le cristal PDC dans le mode S pour être amplifié et produire un second photon cloné. La pompe est obtenue par doublage de fréquence d'un laser primaire, dont une partie est dérivée pour générer le photon à cloner injecté dans le PDC. *L'alignement et l'accord des modes sont critiques.*

# Expérience de clonage par amplification (suite)

Le Hamiltonien  $H$  est invariant par rotation globale des polarisations  $H$  et  $V$ . Dans une rotation d'angle  $\theta$ , ces polarisations deviennent  $H'$  et  $V'$  et les opérateurs de création et d'annihilation de photons suivant les deux choix d'axes  $(H,V)$  et  $(H',V')$  sont reliés par les relations:

$$a_V^\dagger = \cos\theta a_{V'}^\dagger + \sin\theta a_{H'}^\dagger \quad ; \quad a_H^\dagger = -\sin\theta a_{V'}^\dagger + \cos\theta a_{H'}^\dagger \quad (5-2)$$

ce qui entraîne:

$$\begin{aligned} a_{VS}^\dagger a_{HI}^\dagger - a_{HS}^\dagger a_{VI}^\dagger &= (\cos\theta a_{V'S}^\dagger + \sin\theta a_{H'S}^\dagger) (-\sin\theta a_{V'I}^\dagger + \cos\theta a_{H'I}^\dagger) \\ &\quad - (-\sin\theta a_{V'S}^\dagger + \cos\theta a_{H'S}^\dagger) (\cos\theta a_{V'I}^\dagger + \sin\theta a_{H'I}^\dagger) \\ &= a_{V'S}^\dagger a_{H'I}^\dagger - a_{H'S}^\dagger a_{V'I}^\dagger \end{aligned} \quad (5-3)$$

Le processus d'amplification est donc invariant par rotation des axes de polarisation. Il suffit de l'analyser pour un choix de polarisation  $(H,V)$ . Appelons  $V$  la polarisation du photon à cloner. L'évolution du champ sous l'effet du hamiltonien  $H$  s'écrit au 1<sup>er</sup> ordre en  $\gamma$ :

$$\begin{aligned} e^{-iHt/\hbar} |N\rangle_p \otimes |1_V, 0_H\rangle_S |0_V, 0_H\rangle_I &\approx \\ |N\rangle_p \otimes |1_V, 0_H\rangle_S |0_V, 0_H\rangle_I - \frac{i\gamma t \sqrt{N}}{\hbar} |N-1\rangle_p \otimes & \left[ \sqrt{2} |2_V, 0_H\rangle_S |0_V, 1_H\rangle_I - |1_V, 1_H\rangle_S |1_V, 0_H\rangle_I \right] \end{aligned} \quad (5-4)$$

# Expérience de clonage par amplification (suite)

Sélectionnons (en détectant un clic de  $D_I$ ) les événements à deux photons dans le mode S. L'état de ce mode est décrit théoriquement par:

$$\rho_S = \frac{2}{3} |2_V, 0_H\rangle_S \langle 2_V, 0_H| + \frac{1}{3} |1_V, 1_H\rangle_S \langle 1_V, 1_H| \quad (5-5)$$

Une paire de photons identiques au photon initial est alors obtenue avec la probabilité  $2/3$  et une paire de photons corrélés avec des polarisations orthogonales est produite avec la probabilité  $1/3$ . Cette statistique indique que la probabilité de trouver un des deux photons du faisceau S dans le « mauvais » état H est  $(1/3)(1/2) = 1/6$ . La fidélité du clonage est donc  $F = 1 - (1/6) = 5/6$ .

Nous avons décrit une situation idéale: un photon « signal » arrive dans le PDC en coïncidence avec la paire EPR qui y est générée. En fait, pour éviter la présence de plusieurs photons dans le champ à cloner, celui-ci est préparé dans un état cohérent de faible amplitude, avec une probabilité de photon par impulsion  $\sim 5\%$ , ce qui rend négligeable la présence simultanée de deux photons. De plus, la probabilité de génération des paires EPR est également faible ( $\sim 0,1\%$  par pulse) et l'efficacité des détecteurs est  $\sim 10\%$ . L'expérience a un taux de répétition de  $8 \cdot 10^7 \text{s}^{-1}$ . On s'attend donc à 3 à 4 triples détections de photons dans  $D_I$ ,  $D_{S1}$  et  $D_{S2}$  par seconde et il faut quelques minutes pour accumuler une statistique significative.

# Mise en évidence de l'effet de stimulation

Lames-Linares et al ont sélectionné les signaux à 3 clics et les ont enregistrés en fonction du retard  $\Delta t$  du photon à cloner par rapport à l'instant de pompage du PDC. Pour  $\Delta t=0$ , l'indiscernabilité des photons conduit au terme d'amplification en  $\sqrt{2}$ . Pour  $\Delta t$  grand devant la durée des impulsions, le photon à cloner est dans un mode temporel  $S'$  discernable de  $S$ , spectateur d'une paire de photons intriqués émis spontanément par le PDC. Les états finals du champ sont respectivement:

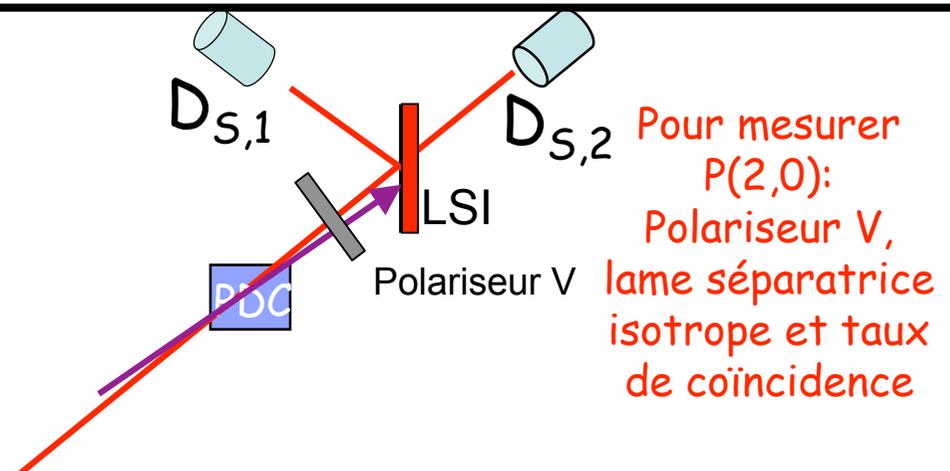
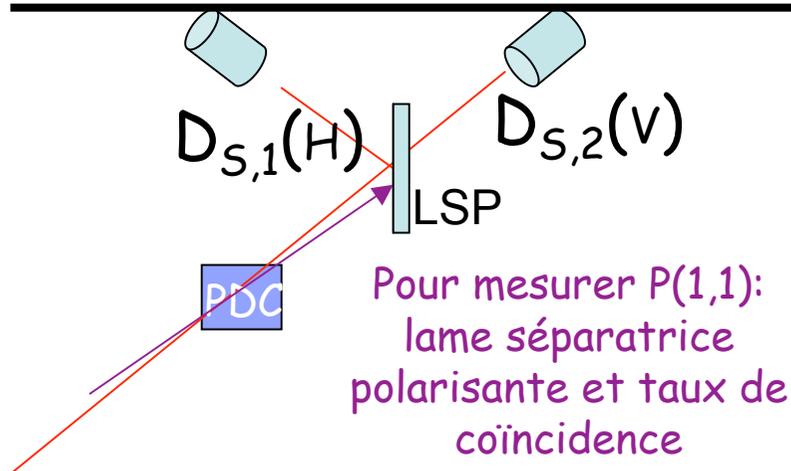
$\Delta t = 0$

$$-\frac{i\gamma t\sqrt{N}}{\hbar} \left[ \sqrt{2} |2_V, 0_H\rangle_S |0_V, 1_H\rangle_I - |1_V, 1_H\rangle_S |1_V, 0_H\rangle_I \right]$$

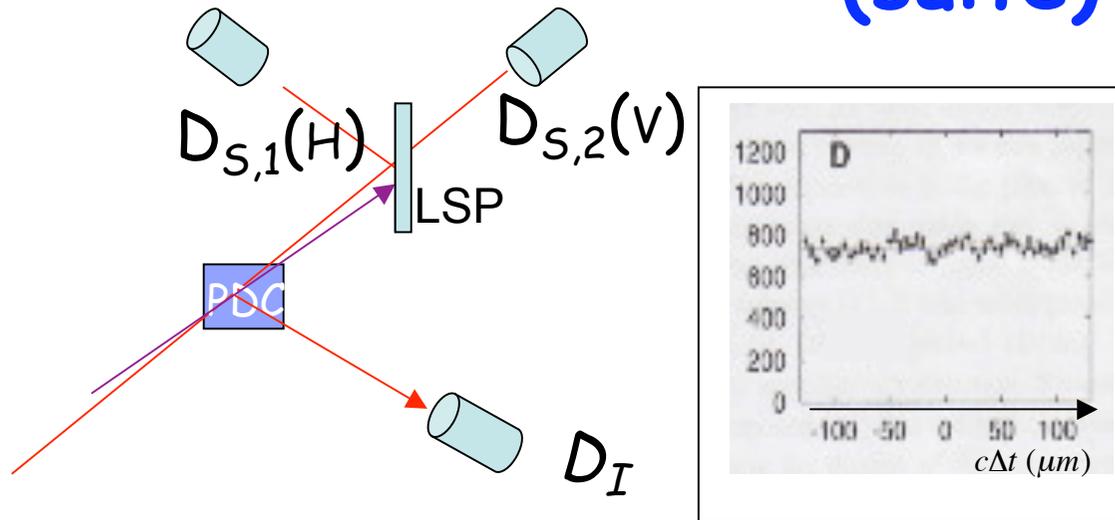
$\Delta t > \text{durée des impulsions}$

$$-\frac{i\gamma t\sqrt{N}}{\hbar} \left[ |1_V, 0_H\rangle_S |0_V, 1_H\rangle_I - |0_V, 1_H\rangle_S |1_V, 0_H\rangle_I \right] \otimes |1_V, 0_H\rangle_{S'}$$

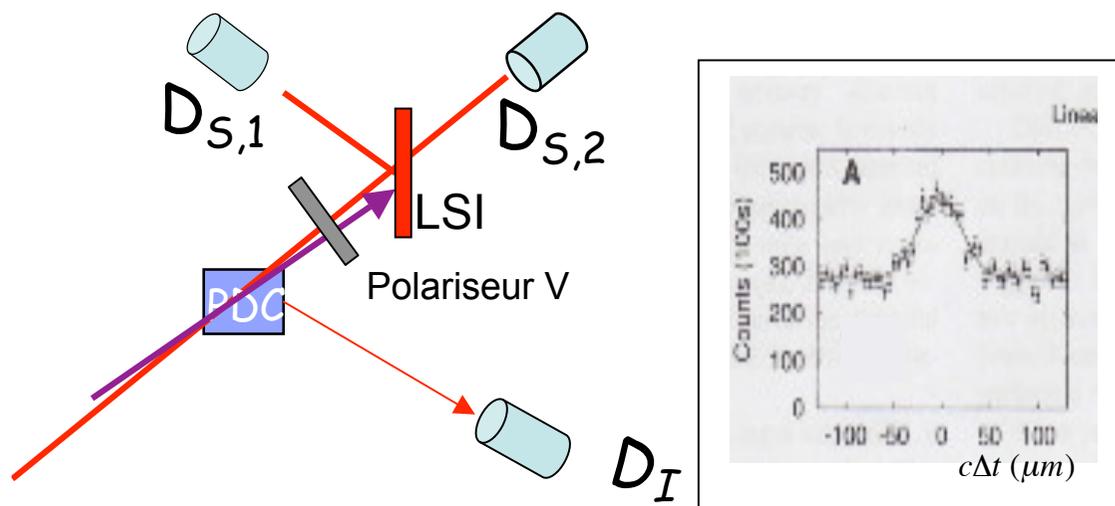
On voit que la probabilité  $P(1,1)$  d'avoir dans  $S+S'$  un photon V et un photon H (2<sup>nd</sup> terme de ces expressions) doit être insensible à  $\Delta t$ , alors que la probabilité  $P(2,0)$  d'avoir 2 photons V doit être maximum pour  $\Delta t=0$ . Les probabilités  $P(1,1)$  et  $P(2,0)$  sont mesurées à l'aide des deux dispositifs schématisés sur les figures ci-dessous.



# Mise en évidence de l'effet de stimulation (suite)

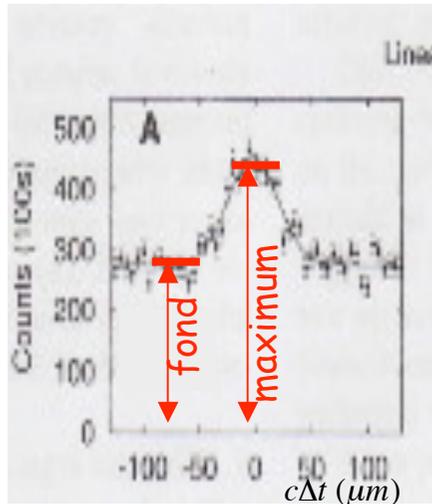


Les triples coïncidences mesurées avec le dispositif ci-contre correspondent aux événements où le photon V à cloner est « faussement » copié sur un photon H. Comme attendu, le taux de coïncidence, proportionnel à  $P(1,1)$  ne varie pas avec  $\Delta t$



Avec le dispositif ci-contre,  $D_{S,1}$  et  $D_{S,2}$  ne peuvent « cliquer » ensemble que quand le champ est dans la composante où le photon à cloner et sa copie ont la même polarisation V et le taux de coïncidence est alors proportionnel à  $P(2,0)$ . Comme prévu, ce taux varie avec  $\Delta t$ , avec un maximum pour  $\Delta t=0$

# Mesure de la fidélité du clonage par amplification optique



La constance de  $P(1,1)$  quand  $\Delta t$  varie montre que le pic observé sur  $P(2,0)$  est bien dû à l'effet de stimulation lié à l'indiscernabilité des photons. Le rapport  $R = \text{maximum}/\text{fond}$  de  $P(2,0)$  est directement lié à la fidélité de clonage. Il est clair que la ligne de base de  $P(2,0)$  correspond au signal plat de  $P(1,1)$ .  $R$  mesure donc le rapport  $P(2,0)/P(1,1)$  pour  $\Delta t=0$ . On en déduit les probabilités absolues que les deux photons aient la même polarisation ou des polarisations orthogonales:

$$P(V,V) = \frac{p(2,0)}{p(2,0) + p(1,1)} = \frac{R}{R+1} \quad ; \quad P(V,H) = \frac{p(1,1)}{p(2,0) + p(1,1)} = \frac{1}{R+1} \quad (5-6)$$

et la fidélité:

$$F = 1 \times P(V,V) + \frac{1}{2} P(V,H) = \frac{R}{R+1} + \frac{1}{2(R+1)} = \frac{2R+1}{2R+2} \quad (5-7)$$

L'expérience donne  $R = 1.50 \pm 0.05$  et  $F = 0.805 \pm 0.010$ , à comparer aux valeurs théoriques  $R=2$  et  $F=(5/6) = 0.833$ . D'autres expériences de clonage optique avec des résultats similaires ont été faites par DeMartini et al (Opt.Com, 179, 581 (2000); Phys.Rev.Lett. 92, 067901 (2004), Nature, 419, 815 (2002)). La préparation d'anticlones a été décrite dans certains de ces articles. Voir le séminaire suivant de *F.Sciarrino* pour la description d'expériences récentes du groupe de Rome.

V-B.

# Clonage et Cryptographie Quantique

# Rappels sur la cryptographie quantique BB84

Il s'agit d'établir le partage d'une clé aléatoire de bits 0/1 entre Alice et Bob, en évitant qu'elle ne tombe, sans qu'ils le sachent, entre les mains d'un espion (Eve). Le protocole de Brassard et Bennett de 1984 (BB84) est le suivant:

- ✓ Alice envoie à Bob des qubits préparés aléatoirement dans deux bases associées à des matrices de Pauli différentes, par exemple  $\sigma_x$  et  $\sigma_y$ .
- ✓ Bob mesure les qubits en choisissant aléatoirement sa base. Une fois sur deux, les bases d'Alice et Bob coïncident et leurs résultats doivent alors être identiques.
- ✓ Alice et Bob annoncent publiquement leur choix de base (sans les résultats) et extraient de leurs suites de bits le sous-ensemble associé au même choix.
- ✓ Si Eve intercepte un des qubits, le mesure et l'envoie ensuite à Bob, elle a une chance sur deux de choisir la mauvaise base, et Bob a alors une chance sur deux d'obtenir un résultat différent d'Alice. Alice et Bob comparent donc leurs résultats sur un sous-ensemble de la clé. S'ils diffèrent, il y a risque d'espionnage.
- ✓ En fait, il y a en pratique des erreurs dues au bruit. Comme il est impossible de distinguer le bruit statistique de la perturbation quantique induite par Eve, Alice et Bob font l'hypothèse pessimiste que toute perturbation vient d'Eve. Si le taux d'erreur est inférieur à un certain seuil, il existe une procédure classique de traitement de la clé en deux étapes (code de correction d'erreur par échange d'information et amplification de confidentialité) qui conduit à la distillation d'une clé plus courte sur laquelle Eve ne peut avoir aucune information.

# Clonage et stratégies d'espionnage de la clé

La sécurité de BB84 repose sur l'impossibilité du clonage parfait. Si Eve disposait d'une machine à cloner parfaite, il lui suffirait de cloner les qubits qu'elle intercepte, d'envoyer une copie à Bob et de garder l'autre jusqu'à ce qu'Alice et Bob annoncent leurs bases de mesure. Dans l'impossibilité de le faire, Eve peut décider de cloner les qubits de façon approchée optimale. Il est donc essentiel pour Alice et Bob de savoir ce que Eve peut faire de mieux comme clonage et les conséquences que cela a sur les corrélations qu'ils mesurent pour vérifier la sécurité de leur clé.

Comme la clé repose sur les mesures de qubits suivant deux axes orthogonaux du plan équatorial de la sphère de Bloch, Eve n'a pas besoin d'une machine à cloner universelle. Il suffit qu'elle clone au mieux, avec la même fidélité les états de la forme  $|0\rangle + e^{i\varphi}|1\rangle$  pour  $\varphi=0, \pi/2, \pi$  et  $3\pi/2$ . En fait nous allons montrer qu'on peut réaliser un clonage « covariant de phase » qui clone, en **rétrécissant par le même facteur  $\eta$**  leur vecteur de Bloch, tous les états dans le plan équatorial de la sphère de Bloch (et pas seulement ceux correspondant à quatre directions). Ce clonage covariant de phase, n'étant pas universel (il ne cherche pas à bien reproduire les états suivant Oz), a **pour les états  $(|0\rangle + e^{i\varphi}|1\rangle)/\sqrt{2}$  une fidélité supérieure à 5/6.**

# Clonage covariant de phase

Pour cloner symétriquement l'état  $|\psi\rangle = (|0\rangle + e^{i\varphi}|1\rangle)/\sqrt{2}$  d'un qubit a sur un qubit b, envisageons une opération unitaire sur (a,b) et sur un qubit auxiliaire m réalisant les transformations (les chiffres correspondent de gauche à droite à a,b et m):

$$|0,0,0\rangle \rightarrow |0,0,0\rangle \quad ; \quad |1,0,0\rangle \rightarrow \frac{1}{\sqrt{2}}[|1,0\rangle + |0,1\rangle]|0\rangle \quad ; \quad |0,1,1\rangle \rightarrow \frac{1}{\sqrt{2}}[|1,0\rangle + |0,1\rangle]|1\rangle \quad ; \quad |1,1,1\rangle \rightarrow |1,1,1\rangle \quad (5-8)$$

Si a est initialement dans  $|\psi\rangle$  et {b,m} dans  $|\Phi^+\rangle_{bm} = (1/\sqrt{2})(|00\rangle + |11\rangle)_{bm}$ , on a par superposition linéaire:

$$\begin{aligned} \frac{1}{2} [ |0\rangle + e^{i\varphi} |1\rangle ] \otimes [ |0,0\rangle + |1,1\rangle ] &= \frac{1}{2} [ |0,0,0\rangle + |0,1,1\rangle ] + \frac{e^{i\varphi}}{2} [ |1,0,0\rangle + |1,1,1\rangle ] \rightarrow \\ \frac{1}{2} |0,0,0\rangle + \frac{1}{2\sqrt{2}} [ |1,0\rangle + |0,1\rangle ] |1\rangle + \frac{e^{i\varphi}}{2\sqrt{2}} [ |1,0\rangle + |0,1\rangle ] |0\rangle + \frac{e^{i\varphi}}{2} |1,1,1\rangle & \quad (5-9) \end{aligned}$$

L'expression identique des états clonés sur a et b obtenus par trace partielle est:

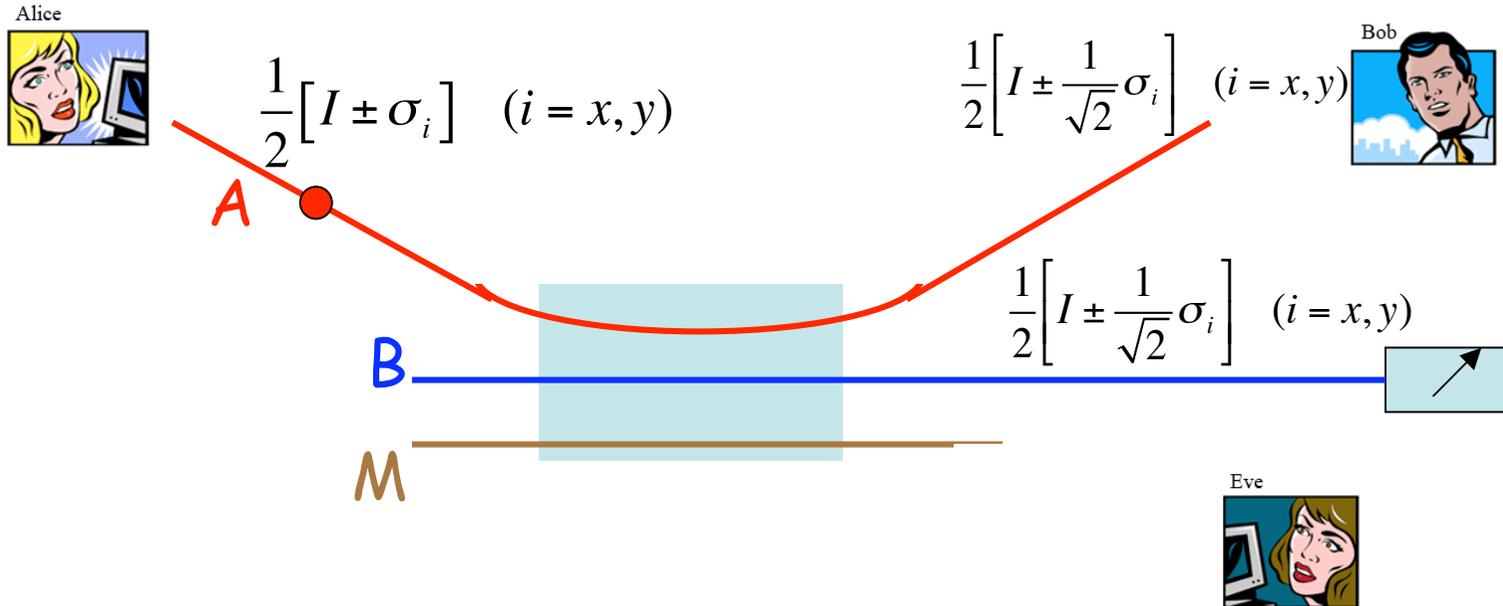
$$\rho_a = \rho_b = \frac{1}{2} [ |0\rangle\langle 0| + |1\rangle\langle 1| ] + \frac{1}{2\sqrt{2}} [ e^{-i\varphi} |0\rangle\langle 1| + e^{i\varphi} |1\rangle\langle 0| ] = \frac{1}{2} \begin{pmatrix} 1 & e^{-i\varphi} / \sqrt{2} \\ e^{i\varphi} / \sqrt{2} & 1 \end{pmatrix} = \frac{1}{2} \left[ I + \frac{\cos \varphi \sigma_x + \sin \varphi \sigma_y}{\sqrt{2}} \right] \quad (5-10)$$

Les vecteurs de Bloch du plan équatorial sont réduits dans le rapport  $\eta=1/\sqrt{2}$ . Ce clonage a, pour les états concernés, une fidélité supérieure au clonage universel:

$$\eta = \frac{1}{\sqrt{2}} > \frac{2}{3} \quad ; \quad F = \frac{1+\eta}{2} = \frac{1}{2} + \frac{1}{2\sqrt{2}} = 0.853.. > \frac{5}{6} \quad (5-11)$$

On montre par contre que la fidélité de ce clonage pour  $|0\rangle$  et  $|1\rangle$  est  $(3/4) < (5/6)$ .

# Sécurité de la cryptographie quantique



Supposons qu'Eve intercepte les qubits envoyés par Alice et les clone de façon covariante de phase, gardant une copie et envoyant l'autre à Bob. Les qubits gardés par Eve et reçus par Bob sont décrits, dans la base de mesure d'Alice, par l'un des deux opérateurs densité suivants, selon le résultat de la mesure d'Alice ( $\varepsilon_A = 0$  ou  $1$ ):

$$\rho = \begin{pmatrix} \frac{1+\eta}{2} - \varepsilon_A \eta & 0 \\ 0 & \frac{1-\eta}{2} + \varepsilon_A \eta \end{pmatrix} ; \quad (\eta = 1/\sqrt{2} ; \quad \varepsilon_A = 0, 1) \quad (5-12)$$

Quel que soit le résultat d'Alice, Eve et Bob, s'ils choisissent la même base de mesure qu'Alice, ont donc une probabilité d'erreur de mesure  $(1-\eta)/2 = 0,147$ .

# Sécurité de la cryptographie quantique (fin)

Le taux d'erreur  $r$  constaté par Alice et Bob après avoir sélectionné les mesures associées au même choix de base provient d'une combinaison des effets du bruit technique et d'un possible espionnage. Si  $r$  est supérieur à 25%, il est possible qu'Eve ait intercepté de façon triviale les qubits avant de les renvoyer à Bob après mesure. Alice et Bob se doutent alors que leur canal quantique n'est pas sûr et décident de ne pas l'utiliser. Si  $0,25 > r > 0,147$ , il est possible qu'Eve ait utilisé une machine de clonage covariant de phase. Elle posséderait alors autant d'information sur la clé que Bob et là encore, Alice et Bob ne peuvent communiquer de façon sûre. Enfin, si  $r < 0,147$  Alice et Bob peuvent être assurés qu'aucun espion n'a pu cloner et mesurer successivement tous les qubits échangés. En conséquence Alice et Bob possèdent davantage d'information que Eve. La théorie de l'information classique fournit alors des algorithmes de corrections d'erreurs et d'amplification de confidentialité qui permettent, en deux étapes, de «distiller» une clé plus courte que la clé initiale, sur laquelle Eve ne peut pratiquement avoir aucune information.

Dans l'analyse précédente, Bob et Alice font l'hypothèse qu'Eve a fait des mesures *individuelles* sur les qubits clonés après que Alice a révélé son choix de base, mais avant tout échange classique (et donc possiblement intercepté) entre Alice et Bob pour corriger les erreurs. Il existe des scénarii plus subtils *d'attaques collectives* dans lesquels Eve conserve les qubits clonés et effectue sur eux des mesures d'ensemble après les procédures d'Alice et Bob, tenant éventuellement compte des communications classiques qu'ils ont échangées. On montre qu'alors, le taux d'erreurs acceptables pour pouvoir obtenir une clé sûre doit satisfaire  $r < 0,11$ .

V-C.

# Clonage et superluminalité

Cette partie développe le raisonnement et les calculs de  
N.Gisin, Phys.Lett.A 242, 1 (1998)

# Clonage approché et causalité

Nous avons vu à la leçon 3 que le clonage parfait  $1 \rightarrow 2$  permettrait la communication superluminale, qui est en contradiction avec le principe de causalité relativiste. Nous allons montrer maintenant que la limite  $F=5/6$  de la fidélité de clonage universel  $1 \rightarrow 2$  est précisément celle au-delà de laquelle la communication superluminale deviendrait possible. Ainsi, le respect de la causalité qui impose que la vitesse maximale de propagation des signaux est celle de la lumière est compatible avec la théorie quantique non-relativiste, un résultat qui n'était pas évident a priori.

En reprenant le raisonnement développé au début de la leçon 3, Nous allons supposer que Alice et Bob cherchent à communiquer en effectuant des mesures sur une paire de particules intriquées. L'information est contenue dans le choix de base effectué par Alice. Nous avons vu que l'opérateur densité de la particule de Bob ne dépend pas de ce choix, ce qui empêche toute communication superluminale directe. Nous avons également montré que par clonage parfait, Bob aurait la possibilité de produire une paire de clones dans des états différents suivant le choix d'Alice. Nous allons maintenant voir ce que devient cette possibilité dans le cas d'un clonage universel symétrique tel que nous l'avons décrit à la leçon 3.

# Clonage et causalité (suite)

La machine à cloner de Bob, agissant sur un qubit  $b$  dans un état pur de vecteur de Bloch  $\vec{P}$ , produit deux qubits  $b$  et  $c$  dont les opérateurs densité partiels ont des vecteurs de Bloch réduits dans le rapport  $\eta$ :

$$\rho = \frac{1}{2} [I + \eta \vec{P} \cdot \vec{\sigma}] \quad (5-13)$$

Nous savons que la valeur  $\eta=1$  est incompatible avec la causalité. Nous allons déterminer la valeur maximale de  $\eta$  qui n'est pas en contradiction avec ce principe. L'opérateur densité  $\rho_{bc}$  des deux qubits clonés se développe sur les produits de matrice de Pauli et de matrice unité sous la forme générale (où les  $t_{jk}$  sont des coordonnées tensorielles réelles):

$$\rho_{bc} = \frac{1}{4} \left[ I_{bc} + \eta (\vec{P} \cdot \vec{\sigma}_b \otimes I_c + I_b \otimes \vec{P} \cdot \vec{\sigma}_c) + \sum_{j,k=x,y,z} t_{jk} \sigma_{jb} \sigma_{kc} \right] \quad (5-14)$$

Pour préciser la forme de  $\rho_{bc}$ , nous allons tenir compte du **caractère universel** du clonage, qui opère de la même façon sur tous les états, quelle que soit la direction de leur vecteur de Bloch. En appelant  $R$  une opération de rotation arbitraire sur l'état des qubits (ou sur leurs vecteurs de Bloch), l'universalité entraîne **la propriété de covariance** qui exprime que tourner le qubit avant de le cloner ou le cloner puis tourner les deux clones doivent revenir au même:

$$\rho_{bc} [R(P_\psi)] = R_b R_c \rho_{bc} (P_\psi) R_b^\dagger R_c^\dagger \quad (5-15)$$

# Clonage et causalité (suite)

Analysons les conséquences de cette covariance sur l'expression générale de l'état des clones b et c pour un qubit dont le vecteur de Bloch est aligné le long de Oz:

$$\begin{aligned} \rho_{bc}(\vec{e}_z) = & \frac{1}{4} [ I_{bc} + \eta(\sigma_{za} \otimes I_b + \sigma_{zb} \otimes I_a) \\ & + t_{xx} \sigma_{xa} \sigma_{xb} + t_{yy} \sigma_{ya} \sigma_{yb} + t_{zz} \sigma_{za} \sigma_{zb} \\ & + t_{xy} \sigma_{xa} \sigma_{yb} + t_{yx} \sigma_{ya} \sigma_{xb} \\ & + t_{yz} \sigma_{ya} \sigma_{zb} + t_{zy} \sigma_{za} \sigma_{yb} \\ & + t_{zx} \sigma_{za} \sigma_{xb} + t_{xz} \sigma_{xa} \sigma_{zb} ] \end{aligned} \quad (5-16)$$

L'invariance de  $\rho_{bc}(\vec{e}_z)$  dans la rotation de  $\pi/2$  autour de Oz (qui change x en y et y en -x) entraîne:

$$t_{xx} = t_{yy} ; t_{xy} = -t_{yx} \quad (5-17)$$

et l'invariance dans la rotation de  $\pi$  autour du même axe (qui change x en -x et y en -y) conduit à:

$$t_{xz} = t_{yz} = t_{zx} = t_{zy} = 0 \quad (5-18)$$

# Clonage et causalité (suite)

D'où l'expression simplifiée:

$$\begin{aligned} \rho_{bc}(\vec{e}_z) = & \frac{1}{4} [I_{bc} + \eta(\sigma_{za} \otimes I_b + \sigma_{zb} \otimes I_a) \\ & + t_{xx}(\sigma_{xa} \sigma_{xb} + \sigma_{ya} \sigma_{yb}) + t_{zz} \sigma_{za} \sigma_{zb} \\ & + t_{xy}(\sigma_{xa} \sigma_{yb} - \sigma_{ya} \sigma_{xb})] \end{aligned} \quad (5-19)$$

et par rotation  $R_x(\pi)$  qui change  $z$  en  $-z$  et  $y$  en  $-y$ :

$$\begin{aligned} \rho_{bc}(-\vec{e}_z) = & \frac{1}{4} [I_{bc} - \eta(\sigma_{za} \otimes I_b + \sigma_{zb} \otimes I_a) \\ & + t_{xx}(\sigma_{xa} \sigma_{xb} + \sigma_{ya} \sigma_{yb}) + t_{zz} \sigma_{za} \sigma_{zb} \\ & - t_{xy}(\sigma_{xa} \sigma_{yb} - \sigma_{ya} \sigma_{xb})] \end{aligned} \quad (5-20)$$

soit par addition:

$$\frac{1}{2} [\rho_{bc}(\vec{e}_z) + \rho_{bc}(-\vec{e}_z)] = \frac{1}{4} [I_{bc} + t_{xx}(\sigma_{xa} \sigma_{xb} + \sigma_{ya} \sigma_{yb}) + t_{zz} \sigma_{za} \sigma_{zb}] \quad (5-21)$$

et enfin par rotation  $R_y(\pi/2)$  qui change  $z$  en  $x$ :

$$\frac{1}{2} [\rho_{bc}(\vec{e}_x) + \rho_{bc}(-\vec{e}_x)] = \frac{1}{4} [I_{bc} + t_{xx}(\sigma_{za} \sigma_{zb} + \sigma_{ya} \sigma_{yb}) + t_{zz} \sigma_{xa} \sigma_{xb}] \quad (5-22)$$

La comparaison des expressions (5-21) et (5-22) nous permet de contraindre encore plus le tenseur  $t_{ij}$ .

# Clonage et causalité (suite)

Les deux expressions (5-21) et (5-22) sont les opérateurs densité obtenus par Bob lorsque Alice effectue une mesure soit suivant Oz soit suivant Ox de son qubit. Pour qu'il n'y ait pas superluminalité, il faut que ces deux expressions soient identiques, ce qui impose:

$$t_{xx} = t_{yy} = t_{zz} = t \quad (5-23)$$

d'où l'expression imposée pour  $\rho_{bc}(\vec{e}_z)$ :

$$\begin{aligned} \rho_{BC}(\vec{e}_z) &= \frac{1}{4} [I_{BC} + \eta(\sigma_{zA} \otimes I_B + \sigma_{zB} \otimes I_A) \\ &\quad + t(\sigma_{xA} \sigma_{xB} + \sigma_{yA} \sigma_{yB} + \sigma_{zA} \sigma_{zB}) \\ &\quad + t_{xy}(\sigma_{xA} \sigma_{yB} - \sigma_{yA} \sigma_{xB})] \\ &= \frac{1}{4} \begin{pmatrix} 1+2\eta+t & 0 & 0 & 0 \\ 0 & 1-t & 2t+2it_{xy} & 0 \\ 0 & 2t-2it_{xy} & 1-t & 0 \\ 0 & 0 & 0 & 1-2\eta+t \end{pmatrix} \quad (5-24) \end{aligned}$$

Il nous reste à voir à quelles conditions cette matrice est positive.

# Clonage et causalité (suite)

L'équation aux valeurs propres:

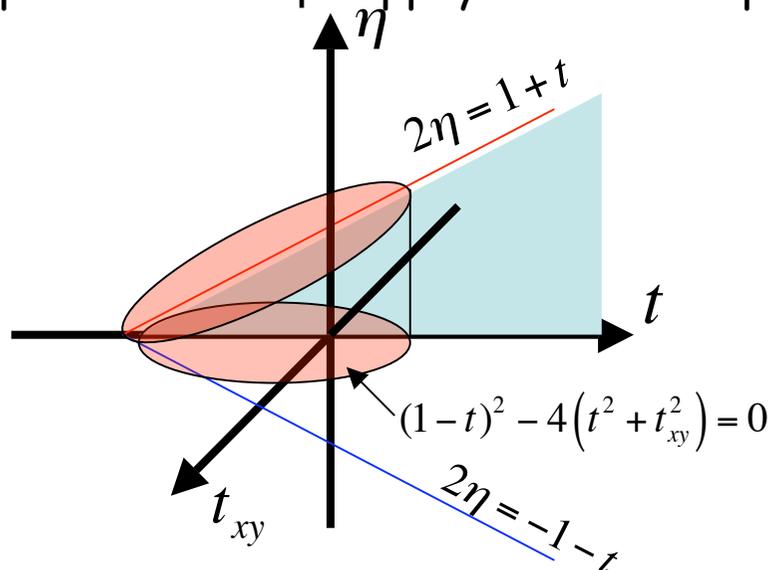
$$(1 + 2\eta + t - \lambda)(1 - 2\eta + t - \lambda)[(1 - t - \lambda)^2 - 4(t^2 + t_{xy}^2)] = 0 \quad (5-25)$$

admet les racines:

$$\lambda_1 = \frac{1}{4}(1 + 2\eta + t); \lambda_2 = \frac{1}{4}(1 - 2\eta + t); \lambda_3 = \frac{1}{4}\left(1 - t + 2\sqrt{t^2 + t_{xy}^2}\right); \lambda_4 = \frac{1}{4}\left(1 - t - 2\sqrt{t^2 + t_{xy}^2}\right) \quad (5-26)$$

qui dépendent des 3 paramètres  $t$ ,  $t_{xy}$  et  $\eta$ . Pour discuter le signe de ces racines, associons à ces paramètres le point les ayant comme coordonnées dans un repère orthonormé (voir fig) et déterminons la région du demi-espace  $\eta \geq 0$  pour laquelle les quatre  $\lambda_i$  sont positifs. On a  $\lambda_1, \lambda_2 \geq 0$  pour les points à l'intérieur du dièdre formé par le plan  $\eta=0$  et le plan parallèle à l'axe  $Ot_{xy}$  d'équation  $2\eta=1+t$  (zone en bleu sur la figure). On a  $\lambda_3, \lambda_4 \geq 0$  pour les points à l'intérieur d'un cylindre d'axe parallèle à  $O\eta$  s'appuyant sur l'ellipse du plan  $Ot, t_{xy}$  d'équation:

$$(1-t)^2 - 4(t^2 + t_{xy}^2) = 0 \quad (5-27)$$



On voit sur la figure que la valeur la plus grande de  $\eta$  compatible avec ces contraintes correspond au point sur la génératrice du cylindre de plus grande valeur de  $t$  ( $t=1/3$ ). La valeur maximale de  $\eta$  est donc  $(1+1/3)/2 = 2/3$ , ce qui correspond à la fidélité de clonage  $F=(1+\eta)/2=5/6$ .

# Clonage et causalité (conclusion)

Nous avons montré, en suivant l'analyse de Nicolas Gisin que le clonage universel symétrique de qubits  $1 \rightarrow 2$  ne peut avoir une fidélité supérieure à  $5/6$  si on impose au système la condition de non-communication superluminale. En d'autres termes, la fidélité optimale de clonage universel établie à la leçon 3 est une condition nécessaire pour assurer la « coexistence pacifique » entre les principes de la relativité et ceux de la physique quantique non-relativiste. Cette coexistence n'a en soi rien d'évident. Le fait que les propriétés de l'intrication, basées sur une physique où la vitesse de la lumière ne joue aucun rôle fondamental, sont compatibles avec le principe de causalité relativiste est remarquable.

**Remarque:** Le raisonnement ci-dessus repose sur l'éq. (5-15) qui exprime le caractère covariant dans une *rotation arbitraire* du clonage universel. Si Bob utilise le clonage covariant de phase restreint à un plan de la sphère de Bloch décrit au §V-B, les contraintes sur la décomposition tensorielle de  $\rho_{bc}$  sont différentes car l'éq. (5-15) n'est plus valable pour  $R$  quelconque. Le calcul des pages précédentes ne s'applique donc pas. Une démarche analogue permet cependant de montrer que la causalité serait violée avec un clonage covariant de phase symétrique ayant une fidélité supérieure à  $F = (1/2) + 1/(2\sqrt{2}) = 0,854$  (voir P.Navez et N.Cerf, *Phys.Rev.A* 68, 032313 (2003) et refs.in). Ici encore, la limite de fidélité quantique correspond à la condition de « coexistence » de la théorie quantique non relativiste avec le principe de causalité.