

Cryptographie
quantique



Auteurs :

- Sylvain Guilley (sylvain.guilley@enst.fr)
- Sylvain Schwartz (sylvain.schwartz@enst.fr)

Table des matières

1	Fondements théoriques	3
1.1	La cryptographie classique	4
1.2	Le protocole BB84	6
2	La cryptologie « certifiée » quantique	10
2.1	Imperfections des canaux de communication réels	11
2.2	Test d'une inégalité de Bell	18
2.3	Cryptographie avec des paires de photons intriqués	24
3	Quelques expériences de cryptographie quantique	27
3.1	Principaux acteurs au niveau mondial	27
3.2	Etat de l'art des expériences actuelles	28
A	Rappels de mécanique quantique, liens avec le protocole BB84	30
A.1	Fonction d'onde et vecteur d'état	30
A.2	Le problème de la mesure en mécanique quantique	31
A.3	Une illustration des principes de superposition et de réduction du paquet d'onde : le "paradoxe" du chat de Schrödinger	32
A.4	Commutation des observables, compatibilité des mesures et relation d'incertitude ; application aux observables de BB84	33
A.5	Conclusion	34
A.6	Complément : le théorème de non clonage quantique	34
B	Théorie de l'information	36
B.1	Entropie : mesure de l'ordre et du désordre	36
B.2	Information : réduction de l'entropie	38
B.3	Liens entre théorie de l'information et mécanique quantique	38
C	Extraire de l'information d'une mesure quantique	39
C.1	Dans quelle mesure peut-on distinguer deux états quantiques?	39
C.2	Information codée dans deux états quantiques	39

Avant-propos

Ce cours propose une découverte de la cryptographie quantique et de ses enjeux. Il est rédigé de manière pédagogique de façon à faciliter l'approche de cette discipline à l'intersection de la physique quantique et de la théorie de l'information et du codage.

Les annexes rassemblent à la fois des aide-mémoire de mécanique quantique et de théorie de l'information et des quelques approfondissements.

Une riche bibliographie, qui reflète l'état de l'art des recherches, accompagne ce rapport.

Ce cours est périodiquement mis à jour. La version la plus récente est disponible en ligne à l'URL suivante :

http://www.enst.fr/~guilley/ressources/crypto_quantique/

Merci de faire parvenir à l'adresse sylvain.guilley@enst.fr toute remarque sur ce cours.

Sylvain Guilley et Sylvain Schwartz, septembre 2002.

Date	Version	Auteur	Commentaire
Juillet 2002	1.0	Sylvain Guilley et Sylvain Schwartz	Création du rapport. Publication.
07 Septembre 2002	1.1	Sylvain Guilley	Ajout de la section 2.1.3. sur le modèle de QBER.

TAB. 1 – *Table des modifications*

Chapitre 1

Fondements théoriques

1.1	La cryptographie classique	4
1.1.1	Les systèmes asymétriques	4
1.1.2	Les systèmes symétriques	5
1.1.3	Conclusion	6
1.2	Le protocole BB84	6
1.2.1	Un cas idéal : l'absence de bruit sur la ligne	6
1.2.2	Prise en compte du bruit et solutions envisageables	8
1.2.3	Conclusion	8

La cryptographie quantique repose sur l'un des axiomes fondamentaux de la mécanique quantique, à savoir que *toute mesure perturbe le système sur lequel elle est effectuée*.

Il est relativement simple (et utile) de se faire une idée intuitive de son principe de fonctionnement avant d'entrer dans les détails. Supposons, comme illustré dans la figure 1.1, que Alice désire envoyer un message à Bob sans qu'il ne soit intercepté par Eve (ces trois noms sont quasi universellement utilisés dans le domaine de la cryptographie quantique, bien qu'il arrive parfois que les deux derniers soient remplacés par Bernard et Erik). Pour tirer parti de l'axiome énoncé ci-dessus, Alice doit utiliser en guise de support de l'information des systèmes quantiques, comme par exemple des photons isolés (nous aurons l'occasion de revenir en détail sur ce point). Si Eve tente d'acquiescer de l'information donc de faire une mesure sur les systèmes quantiques envoyés par Alice, elle va perturber ces derniers, et ainsi révéler sa présence. En pratique, il suffit à Alice et Bob de comparer (publiquement) un échantillon de leurs données choisi aléatoirement pour se rendre compte de la présence (ou non) d'un espion sur leur canal de communication. Remarquons que cette présence n'est détectée qu'après l'envoi du message. Ce dernier ne doit donc pas directement contenir l'information confidentielle à transmettre, mais plutôt une suite de bits choisis aléatoirement par Alice qui constitueront ce que l'on appelle une clé. Si celle-ci parvient non perturbée à Bob, elle pourra être utilisée pour crypter (classiquement) le message qui sera alors transmis sur un canal de communication public. Si au contraire Alice et Bob détectent des perturbations dans la transmission de la clé, traduisant la présence d'un espion, ils ignorent simplement cette dernière et ne perdent aucune information puisque la clé n'en contenait pas.

On s'aperçoit au terme de cette introduction qu'un tel protocole ne permet pas directement de crypter un message mais plutôt de transmettre (de manière sûre) une clé qui pourra ensuite être utilisée dans un protocole de cryptographie classique (ainsi la cryptographie quantique porte-t-elle mal son nom, et devrait plutôt s'appeler *distribution quantique de clé*). Cela nous amène tout

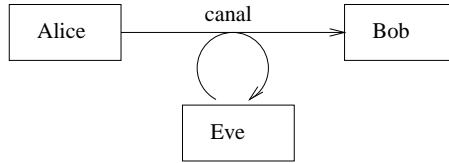


FIG. 1.1 – *Principe d'une communication sous menace d'espionnage. Alice envoie un message à Bob, pendant qu'Eve tente d'intercepter l'information échangée.*

naturellement, avant d'entrer plus en détail dans la description des protocoles de cryptographie quantique, à nous pencher plus avant sur la cryptographie dite classique, puisque cette dernière est indissociable de sa petite soeur quantique.

1.1 La cryptographie classique

La cryptographie, ou art de rendre un message inintelligible à une personne non autorisée à le lire, est probablement aussi vieille que l'écriture. Nous n'entrerons pas dans une revue historique, qui serait fort passionnante au demeurant.

Dans sa version moderne, la cryptographie est un algorithme qui combine un message avec une information supplémentaire appelée clé (c'est l'opération de cryptage). En théorie, pour que le cryptage soit sûr, il ne doit pas être possible de décoder le message crypté si l'on ne possède pas la clé. En pratique, cette contrainte est souvent moins forte : il est simplement extrêmement compliqué de décoder le message si l'on ne possède pas la clé, avec tous les aléas qu'implique une telle approximation. On peut par exemple dire que le système est sûr si le décryptage sans clé requiert plus de temps que la durée de validité de l'information cryptée.

Les systèmes de cryptographie peuvent se diviser en deux classes, appelées respectivement symétriques et asymétriques selon que Alice et Bob utilisent ou non la même clé.

1.1.1 Les systèmes asymétriques

Les systèmes asymétriques (plus connus sous le nom de systèmes à clé publique) mettent en jeu l'utilisation de clés différentes pour le cryptage et le décryptage. Si la première clé (la clé publique) est à la disposition de tous, il n'en est pas de même pour la seconde (la clé privée) dont seul dispose Bob. La version la plus connue de ce système, appelée RSA et développée en 1978 au MIT, est toujours largement utilisée, par exemple dans les opérations de paiement sécurisé.

Le détail mathématique de cet algorithme est hors du propos de ce rapport, mais nous allons tenter d'en résumer le principe. La clé publique est en général un entier N , produit de deux grands nombres premiers N_1 et N_2 , la clé privée étant par exemple l'entier N_1 . Il est d'autant plus difficile de calculer N_1 et N_2 à partir de N que les entiers mis en jeu sont grands. Appelons x le message à crypter, par exemple une succession de bits. L'algorithme RSA fournit une série d'opérations mathématiques permettant, à partir des entiers x et N de calculer l'entier $f_N(x)$. La clé publique N étant connue de tous, n'importe qui peut envoyer un message crypté à Bob (c'est ce qui se passe par exemple lorsque l'on tape son numéro de carte bancaire sur Internet). Par contre, la fonction f_N est construite de telle sorte que le calcul de x connaissant $f_N(x)$ ne peut s'effectuer que si l'on connaît un facteur premier de N , disons N_1 . Bob est donc en principe le seul capable de décrypter les messages.

La limite de ce protocole apparaît clairement : la sécurité n'est pas absolue, mais repose au contraire sur la "difficulté" à factoriser des grands nombres premiers, notion toute relative. Ainsi l'annonce un peu hâtive, il y a quelques années, de la mise au point imminente d'un ordinateur quantique capable de factoriser des entiers en un temps linéaire avait-elle provoqué un certain affolement (rapidement dissipé) dans les milieux bancaires. Malheureusement, au vu de l'état actuel des recherches sur l'ordinateur quantique, il semble que l'algorithme RSA a encore de beaux jours devant lui. Mais notre société, fondée de plus en plus sur l'information et la sécurité des communications, peut-elle se permettre une telle menace? Songeons qu'une avancée scientifique majeure brusquement révélée au monde pourrait rendre sans valeur tout l'argent électronique, ce qui entraînerait une catastrophe économique et sociale sans précédent...

Personne n'ayant jamais réussi à démontrer qu'un système de cryptographie asymétrique était sûr, il semble que la solution soit du côté des systèmes dits symétriques. Comme nous allons le voir, ceux-ci doivent être associés à un dispositif de distribution de clé. C'est dans ce domaine que la cryptographie quantique aura très certainement un rôle majeur à jouer dans les années à venir.

1.1.2 Les systèmes symétriques

Dans un système symétrique, Alice et Bob partagent la même clé. Alice crypte son message à l'aide de la clé en utilisant une opération involutive (c'est à dire dont la composée avec elle-même est l'identité). Bob effectue la même opération sur le message crypté à l'aide de la même clé. Comme l'opération est involutive, il retombe sur le message initial.

Une opération involutive simple agissant sur les bits est la fonction XOR ou addition modulo 2 (cette fonction prend 2 bits en argument et renvoie 1 si les deux bits sont différents et 0 s'ils sont identiques). Illustrons cet algorithme très simple sur un exemple. Supposons qu'Alice veuille faire parvenir à Bob le message *10010111* et que tous deux disposent de la clé secrète *00100100*. Le message crypté sera alors :

$$10010111 \text{ XOR } 00100100 = 10110011 \quad (1.1)$$

Ce dernier peut être transmis à Bob sur un canal public. L'opération de décryptage s'écrit :

$$10110011 \text{ XOR } 00100100 = 10010111 \quad (1.2)$$

On retrouve bien le message initial.

Si la clé utilisée est aussi longue que le message et est changée à chaque utilisation, un tel algorithme est sûr. En effet, le message crypté transmis est tout aussi aléatoire que la clé, donc ne contient *aucune* information. Par contre, si la clé est utilisée plusieurs fois ou si elle est plus courte que le message, des corrélations vont exister au sein du message transmis, ce qui donne à Eve la possibilité d'intercepter de l'information. Pour comprendre intuitivement ce fait, reprenons l'exemple simple de la fonction XOR. Si Alice utilise deux fois la même clé, disons pour crypter les messages m_1 et m_2 , elle va transmettre publiquement à Bob les données $m_1 \text{ XOR } cle$ et $m_2 \text{ XOR } cle$. Si Eve intercepte ces données et leur applique par exemple la fonction XOR, elle obtient :

$$\begin{aligned} (m_1 \text{ XOR } cle) \text{ XOR } (m_2 \text{ XOR } cle) &= (m_1 \text{ XOR } m_2) \text{ XOR } (cle \text{ XOR } cle) \\ &= m_1 \text{ XOR } m_2 \end{aligned}$$

ce qui *est une information* sur les messages.

En pratique, la fonction utilisée est bien plus complexe qu'une simple addition de bits modulo 2 (et est en particulier non commutative), ce qui permet d'utiliser la même clé plusieurs fois. Mais la sécurité du système n'est alors plus garantie, et ne repose que sur la complexité du calcul de décryptage. On est donc ramené au problème des algorithmes asymétriques. Signalons pour être complets qu'à longueur de clé donnée, on peut montrer que les systèmes de cryptographie symétriques sont plus sûrs que leurs équivalents asymétriques.

1.1.3 Conclusion

On peut résumer les principaux thèmes développés jusqu'ici comme suit :

1. la cryptographie quantique ne permet pas de transmettre un message mais une clé, la sécurité du protocole ne pouvant être garantie qu'après la transmission ;
2. le protocole quantique doit donc être combinée à un algorithme de cryptographie classique pour effectivement crypter le message, qui sera alors transmis sur un canal public ;
3. les algorithmes de cryptographie classiques se divisent en deux classes, les asymétriques et les symétriques ; ce sont ces derniers qui constituent le complément indispensable à un protocole de cryptographie quantique.

Il est maintenant temps de se pencher concrètement sur un protocole de cryptographie quantique. C'est le plus répandu d'entre eux, le protocole BB84, que nous allons étudier dans le paragraphe suivant.

1.2 Le protocole BB84

Ce protocole, dont l'apparition marque le début de la cryptographie quantique, a été développé en 1984 par Charles Bennett et Gilles Brassard, d'où son nom. Nous allons tout d'abord décrire en quoi il consiste, avant d'étudier son comportement face à l'action d'un espion et en présence de bruit. Nous invitons le lecteur peu familier avec la mécanique quantique à prendre connaissance des rappels formulés au début de l'annexe A avant la lecture de ce qui suit. On trouvera également dans cette annexe quelques réflexions sur les différentes manières de se représenter les concepts de BB84 à l'aide du formalisme des espaces de Hilbert.

1.2.1 Un cas idéal : l'absence de bruit sur la ligne

Alice veut transmettre à Bob une suite de bits aléatoires (dans le but de constituer une clé). Pour cela, elle va coder chaque bit sur un système quantique simple : le photon. Elle peut agir sur l'état de polarisation de chaque photon, ce qu'elle va faire selon l'algorithme qui suit.

Pour chaque bit à transmettre, Alice choisit aléatoirement d'utiliser l'une des deux bases suivantes : la base des états de polarisation circulaire (ou base a, notée $\{| \curvearrowright \rangle, | \curvearrowleft \rangle\}$) ou la base des états de polarisation rectiligne (ou base b, notée $\{| x \rangle, | y \rangle\}$). Si elle choisit la base a, elle émet l'état $| \curvearrowright \rangle$ si le bit à transmettre vaut +1 et l'état $| \curvearrowleft \rangle$ s'il vaut 0. Si elle choisit la base b, elle émet l'état $| x \rangle$ si le bit à transmettre vaut +1 et l'état $| y \rangle$ s'il vaut 0.

Pour effectuer sa mesure sur les photons qu'il reçoit, Bob choisit lui aussi, pour chaque photon et à l'aide d'un générateur de nombre aléatoire différent de celui d'Alice, la base a ou la base b. Il projette alors l'état du photon dans cette base. Quand il utilise la même base qu'Alice, il obtient le bon résultat avec une probabilité de 1. Par contre, quand ils utilisent des bases différentes, Bob a une chance sur deux de mesurer 0 ou 1, et ceci indépendamment de ce que lui a envoyé Alice.

On peut se convaincre de ce résultat en examinant l'exemple qui suit. Supposons qu'Alice veuille envoyer le bit 0 à Bob. Elle choisit (aléatoirement) la base a pour effectuer son codage. Elle va donc émettre à Bob un photon dans l'état $|\curvearrowright\rangle$. Si Bob choisit (par chance) lui aussi la base a, la probabilité qu'il mesure un bit égal à 0 vaut :

$$\mathcal{P}_a(0) = |\langle \curvearrowright | \curvearrowright \rangle|^2 = 1 \quad , \quad (1.3)$$

tandis que la probabilité qu'il mesure un bit égal à 1 vaut :

$$\mathcal{P}_a(1) = |\langle \curvearrowleft | \curvearrowright \rangle|^2 = 0 \quad . \quad (1.4)$$

Ses mesures sont donc parfaitement corrélées avec ce qu'Alice émet. Par contre, si Bob avait choisi la base b, la probabilité qu'il mesure un bit égal à 0 aurait été :

$$\begin{aligned} \mathcal{P}_b(0) &= |\langle y | \curvearrowright \rangle|^2 \\ &= |\langle y | (|x\rangle - i|y\rangle) / \sqrt{2} \rangle|^2 \\ &= 1/2 \quad , \end{aligned} \quad (1.5)$$

et la probabilité qu'il mesure un bit égal à 1 aurait été :

$$\begin{aligned} \mathcal{P}_b(1) &= |\langle x | \curvearrowright \rangle|^2 \\ &= |\langle x | (|x\rangle - i|y\rangle) / \sqrt{2} \rangle|^2 \\ &= 1/2 \quad , \end{aligned} \quad (1.6)$$

et ceci sans corrélation aucune avec l'information envoyée par Alice ! Bien sûr, il en va de même pour les autres choix de base et de bit à envoyer que peut faire Alice.

Cette transmission de bits entre Alice et Bob génère donc en moyenne un taux d'erreur de 25%. Mais Alice et Bob ont un moyen très simple de corriger ce taux, puisqu'ils ont noté pour chaque bit transmis leur choix de base respectif. Il leur suffit donc, après la transmission, de s'échanger publiquement ces choix de base, et de ne garder que les bits pour lesquels les deux bases coïncident. Ils obtiennent ainsi une clé dont la taille est réduite en moyenne de 50%, mais dont le taux d'erreur est nul. On parle de clé tamisée (*sifted key* en anglais).

Supposons maintenant qu'Eve puisse intercepter les photons émis par Alice avant qu'ils ne parviennent à Bob. Elle doit nécessairement choisir une base pour effectuer sa mesure. Dans les cas où cette base n'est pas la même que celle utilisée par Alice (ce qui arrive forcément puisqu'Alice change aléatoirement de base sans qu'Eve ne puisse le savoir), Eve va projeter le vecteur d'état du photon sur l'un des vecteurs de sa nouvelle base (les autres alternatives qui s'offrent à elle ne sont pas plus réjouissantes : elle peut choisir d'émettre un nouveau photon, mais il ne sera pas identique au photon qu'elle a reçu car elle n'a pas la possibilité de connaître avec certitude l'état de ce dernier ; elle peut ne rien émettre du tout, mais cela sera détecté par Bob ; enfin, elle pourrait tenter de dupliquer le photon avant d'effectuer sa mesure, mais ceci est interdit par le théorème de non clonage quantique). Les résultats de Bob ne seront alors pas corrélés avec les émissions d'Alice, même dans le cas où ils ont choisi la même base. Cela induira donc des erreurs dans la clé tamisée. Il suffit à Alice et à Bob de comparer publiquement un sous-ensemble de cette clé choisi au hasard (ce sous-ensemble sera ensuite abandonné) pour déterminer ce taux d'erreur, et ainsi en déduire la présence ou non d'un espion sur la ligne.

Le protocole que l'on vient de décrire est donc sûr dans le cas idéal (c'est-à-dire sans bruit), à la seule condition que le nombre de bits échangés par Alice et Bob soit suffisamment grand (pour ne pas être détectée, Eve doit choisir la même base qu'Alice à chaque fois, ce qui ne peut arriver au mieux -en supposant que Eve ait connaissance des conventions d'Alice et de Bob- qu'avec la probabilité $1/2^n$, où n est le nombre de bits de la clé tamisée). Pour 1000 bits échangés, Eve passe inaperçue dans seulement 1 cas sur environ 10^{150} .

1.2.2 Prise en compte du bruit et solutions envisageables

On vient de voir que, dans le cas idéal, la présence d'Eve est synonyme d'un taux d'erreur non nul dans la clé tamisée. Toutefois, une autre source d'erreur sur cette clé est le bruit inhérent au canal de communication. Il est donc possible pour Eve de passer inaperçue si elle ne prélève que peu d'information entre Alice et Bob, de telle sorte que les perturbations qu'elle engendre soient du même ordre de grandeur que le bruit de la ligne de communication. Ainsi Alice et Bob sont-ils obligés de tolérer la présence d'Eve tant que celle-ci reste peu gourmande d'information. Un critère plus formel peut être établi en théorie de l'information, voir par exemple Csiszar et Korner, 1978. Intuitivement, il dit que l'échange d'une clé de manière sûre est possible si Bob reçoit plus d'information de Alice. Bien sûr, la clé tamisée devra être traitée pour supprimer à la fois le bruit du canal et les éléments d'information détenus par Eve. Les algorithmes qui permettent ces traitements sont purement classiques et relativement compliqués. Nous allons en donner ici des versions simplistes afin de s'en faire une idée intuitive (on pourra consulter Brassard et Salvail, 1993 pour une description plus précise).

Tout d'abord, il est indispensable pour Alice et Bob de posséder des clés identiques, même au prix d'un filtrage de l'information vers Eve (qui sera corrigé dans un deuxième temps). Ils vont utiliser pour cela un algorithme de correction d'erreur. La version la plus simpliste d'un tel algorithme est la suivante : Alice choisit aléatoirement des paires de bits, et annonce publiquement pour chacune les numéros des bits et la valeur de leur somme modulo 2 (ou XOR). Bob répond "oui" si la somme modulo 2 de ses bits correspondant à la même paire est identique, et "non" sinon. Dans le premier cas, ils gardent le premier bit de la paire et jettent l'autre, dans le deuxième cas ils jettent les deux bits. Un tel algorithme n'augmente pas l'information d'Eve, et permet (dans l'hypothèse d'un faible taux d'erreurs, ce qui est toujours le cas quand la condition évoquée plus haut est satisfaite) de faire tendre le taux de différences entre les clés d'Alice et de Bob vers 0.

Une fois qu'Alice et Bob possèdent la même clé, il convient de réduire l'information d'Eve jusqu'à un niveau arbitrairement petit. Pour cela, des algorithmes dits de *privacy amplification* sont utilisés. Le plus simple d'entre eux consiste là encore à choisir une paire de bits aléatoirement, d'annoncer leurs numéros publiquement et de prendre leur somme modulo 2, mais sans cette fois annoncer la valeur de cette somme. Au lieu de cela, Alice et Bob remplacent simplement la valeur de ces deux bits par la valeur de cette somme modulo 2. Ainsi maintiennent-ils leur taux d'erreur à 0 tout en réduisant, au détriment de la longueur de leur clé, l'information d'Eve. En effet, supposons par exemple que celle-ci connaisse la valeur du premier bit et pas celle du deuxième. Alors elle n'a aucune information sur la valeur de leur somme modulo 2. De même, si elle connaît la valeur de chaque bit avec la probabilité p , elle connaîtra la valeur de leur somme modulo 2 avec la probabilité $p^2 + (1 - p)^2$, qui est strictement inférieur à p dès que p est plus grand que $1/2$ (ce qui est évidemment le seul cas pertinent).

En itérant cet algorithme, Alice et Bob disposent finalement d'une clé totalement libre d'erreur et sur laquelle Eve n'a aucune information.

1.2.3 Conclusion

Au terme de ce chapitre, il nous semble important de revenir sur deux points.

Premièrement, le protocole qui a été présenté ici n'est efficace concrètement que pour de très faibles taux d'erreur donc de bruit. Il sera présenté dans le chapitre qui suit un protocole plus robuste à l'addition de bruit sur le canal, fondé sur l'intrication quantique.

Deuxièmement, soulignons encore une fois la très grande interdisciplinarité de la cryptographie quantique, qui se situe au croisement de la mécanique quantique, de la théorie de l'informa-

tion et de l'informatique. C'est cette interdisciplinarité qui a initialement retardé son développement, mais qui rend son étude si riche et passionnante.

Chapitre 2

La cryptologie « certifiée » quantique

2.1	Imperfections des canaux de communication réels	11
2.1.1	Sources de bruits	11
2.1.2	Information en présence de bruit	11
2.1.3	Modèle d'évaluation du bruit	15
2.2	Test d'une inégalité de Bell	18
2.2.1	Intrication	19
2.2.2	Etats de Bell	20
2.2.3	Mécanique quantique <i>versus</i> théorie locale	20
2.2.4	Critère de violation d'une inégalité de Bell en environnement bruité	24
2.3	Cryptographie avec des paires de photons intriqués	24
2.3.1	Produire un état de Bell	25
2.3.2	Mesure des corrélations	25
2.3.3	Equivalence avec le protocole BB84	25

Le protocole BB84 décrit au chapitre 1 permet à deux partis, Alice et Bob, de se communiquer une série aléatoire de bits ne contenant pas d'information, en ayant la certitude que personne n'a intercepté le message. En effet, un acte d'espionnage (dont le plus simple est l'écoute et la réémission) se traduit par l'introduction d'erreurs, qu'Alice et Bob sont en mesure d'évaluer. De cette façon, la confidentialité de la communication est garantie par un argument probabiliste (voir la section 1.2.1) sur le taux d'erreur de transmission.

Cependant, la justification du protocole n'est que théorique. Comment peut-on montrer expérimentalement que la communication est belle et bien quantique?

Bien plus qu'un défi de physicien quantique, cette question est celle que se pose tout naturellement le client d'un système de cryptologie quantique¹. Une entreprise qui, pour des raisons de sécurité et de confidentialité, investit dans un tel système souhaite légitimement avoir un moyen de vérifier sa conformité aux spécifications.

En plus des limitations inhérentes aux appareils produisant et recevant les signaux optiques, il faut également jouer avec le bruit introduit durant la propagation. Les erreurs, comme sur tout canal de transmission, sont donc inévitables. Mais comment s'assurer que ces erreurs proviennent d'un bruit aléatoire et non d'un éventuel espion?

La réponse à cette question repose sur deux résultats *a priori* indépendants. En présence de bruit de suffisamment faible amplitude, une communication sécurisée est possible. De plus, tant que la communication est sécurisée, le canal reste quantique.

1. L'entreprise id-Quantique [1] met sur le marché un système de cryptologie quantique « plug and play ».

Comme nous allons le voir dans ce chapitre, on peut s'appuyer sur une expérience de preuve de la mécanique quantique pour prouver que la communication est quantique. La vérification expérimentale de la violation d'une inégalité de Bell démontre que la phénomène observé est de nature quantique.

Ainsi, observer la violation d'une inégalité de Bell sur un canal quantique assure que la communication est immunisée contre l'écoute par un espion.

L'implémentation d'un canal de cryptographie quantique avec test des inégalités de Bell requiert un dispositif expérimental plus sophistiqué que celui qui découle naturellement du protocole BB84. Néanmoins, cette façon de faire de la cryptographie peut être ramenée à une utilisation du protocole BB84.

2.1 Imperfections des canaux de communication réels

2.1.1 Sources de bruits

Le bruit aléatoire induit par l'environnement du système de communication quantique peut provenir des transducteurs (source de lumière, appareil de mesure) ainsi que du canal (bruit thermique, interactions avec le milieu).

- **Source de lumière :** Les signaux peuvent être composés de plusieurs photons. Ce cas de figure est gênant, car un espion pourrait prélever de l'information sur un des photons et laisser partir les autres vers le destinataire de droit, Bob qui n'a aucun moyen de s'apercevoir que le signal a été intercepté. L'utilisation de sources à photons uniques évite ce genre de désagréments.
- **Appareil de mesure :** Il peut arriver que des photons ne soient pas comptabilisés par la diode de mesure. Son efficacité n'est jamais exactement de 1. Par ailleurs, il peut aussi détecter des photons qui n'existent pas : c'est que l'on appelle les *dark counts*.
- **Canal de communication :** Que le signal lumineux se propage dans l'air libre ou dans une fibre optique, il peut y avoir des interactions, qui ont pour effet d'absorber le photon ou de modifier ses propriétés (polarisation, phase, etc.). Le milieu peut aussi émettre des photons spontanés, qui perturbent le signal.

En dépit du bruit engendré par l'environnement du canal, il n'est pas impossible de communiquer. Le handicap apporté par le bruit est mesurable. Voyons à quelles conditions sur l'intensité du bruit une communication quantique est possible avec la certitude que le message n'a pas été intercepté par un espion.

2.1.2 Information en présence de bruit

Les notions d'entropie et d'information qui sont utilisées dans cette section sont exposées dans l'annexe B. La sécurité d'un algorithme de cryptologie quantique est basée sur la protection de l'information. Dès lors que seuls Alice et Bob peuvent s'échanger de l'information sans qu'une Eve malveillante n'espionne la conversation, la communication est alors réputée sécurisée. En revanche, lorsqu'un espion est en mesure d'acquérir plus d'information que Bob, la crédibilité du système est à reconsidérer. Les trois parties qui suivent doivent aider à se convaincre à quel point les nouvelles technologies émergeant de la mécanique quantique doivent être scrupuleusement étudiées afin de dissuader les pirates de chercher à percer le mystère des conversations secrètes.

2.1.2.1 Information transmise d'Alice à Bob

Dans un canal parfait, toute l'information émise par Alice parvient à Bob. On dit que $I_{AB} = 1$ bit.

Un canal réel, comme par exemple les fibres optiques des équipementiers du secteur des télécommunications, est naturellement bruité. On caractérise le bruit par la valeur moyenne du taux d'erreur par bit transmis $QBER$ (pour *Quantum Bit Error Rate*). Ce taux moyen est la limite asymptotique du nombre d'erreur rapporté au nombre de bits transmis durant une transaction :

$$QBER = \frac{N_{erreur}}{N_{erreur} + N_{correct}} \quad (2.1)$$

où le nombre total de bits émis N se décompose en $N_{correct}$ bits reçus conformément à ce qui a été émis et en N_{erreur} bits reçus erronés.

En présence de bruit, l'entropie du signal est *a priori* maximale ($H_{a \text{ priori}} = 1$), mais elle est *a fortiori* réduite par le bruit $QBER$ du canal : $H_{a \text{ fortiori}} = H(QBER)$.

L'information mutuelle entre Alice et Bob est ainsi inférieure à 1 :

$$I_{AB} = 1 - H(QBER) \quad (2.2)$$

2.1.2.2 Information d'Alice prélevable par Eve

En l'absence de bruit, toute mesure d'Eve se manifeste par des discordances entre les mesures d'Alice et de Bob. C'est sur cet effet qu'est garantie la confidentialité du protocole BB84.

Néanmoins, lorsque le canal est bruité, Alice et Bob ne sont pas en mesure de connaître l'origine des erreurs. Certes la statistique du bruit du canal peut être connue ; cependant rien n'empêche Eve de mimer les caractéristiques du bruit « naturel » du canal. Effectivement, un principe fondamental de la cryptologie est de considérer que l'ennemi est omniscient et omnipotent. Il est par conséquent nécessaire de s'assurer par des arguments forts qu'aucun espion ne peut intercepter toute l'information d'une communication sans que son intervention ne soit décelée.

Il va de soi que plus le canal est bruité (plus $QBER$ est grand), plus un espion a de chance de prélever de l'information sans être découvert.

Néanmoins, pour une stratégie d'espionnage donnée, plus Eve tire d'information de ses observations, plus elle ajoute du bruit sur le signal que recevra Bob.

L'objectif d'Eve est par conséquent de trouver la meilleure stratégie qui lui permette de gagner le maximum d'information du signal quantique et aléatoire émis par Alice sous la contrainte que son action ne bruite pas le signal davantage que le bruit « naturel » $QBER$ du canal.

Examinons trois façons de procéder d'efficacité croissante :

1. La méthode la plus naïve consiste à mesurer selon un des deux axes utilisés par Alice, au hasard. Ceci suppose tout de même qu'Eve a pris soin de connaître le choix d'axes convenus entre Alice et Bob. Cette information étant publique, il n'y a aucune interdiction de principe à ce qu'Eve ait accès à cette information. Comme déjà expliqué dans la section 1.2.1 qui justifie le protocole BB84, cette stratégie correspond à une prise de risque élevée pour Eve : elle joue au poker. Si son choix de base coïncide avec celui d'Alice, son intervention passe inaperçue ! Elle mesure un état propre de son appareil de mesure et le réémet tel quel. Son gain d'information est 1, alors que le bruit que sa mesure engendre est nul. Cependant, lorsque Eve se trompe d'axes, elle gagne une information non pertinente (car aléatoire au sens quantique du terme) et émet un photon décorrélé de celui initialement émis par Alice, introduisant un rapport signal à bruit de $1/2$. Ainsi, en supposant qu'Alice utilise de manière équiprobable les deux bases, le bruit des mesures d'Eve est de $1/4$ en moyenne. Or aucun canal de communication ne présente de tel bruit. Typiquement, les taux d'erreurs binaires $QBER$ sont bien inférieurs au pourcent. L'action de Eve est donc facilement détectée.

La grande maladresse d'Eve dans cette tactique d'espionnage est de projeter le signal émis par Alice. Ce faisant, elle rend complètement aléatoire la moitié des bits.

2. Eve a donc tout intérêt à mesurer de manière plus fine le signal d'Alice. Son appareil de mesure peut être conçu pour ne se coupler que partiellement avec le signal. De cette façon, Eve peut ajuster précisément la perturbation qu'elle cause de telle sorte qu'elle reste sous le niveau de bruit *QBER*. Cette stratégie d'interception-réémission immédiate [2] permet à Eve d'espionner dans l'ombre.
3. Afin d'être la plus efficace possible, Eve a intérêt à ne pas chercher à connaître l'information que son appareil de mesure a prélevé sur le signal avant qu'Alice ne révèle ses choix de base. Cette information, diffusée publiquement, est très précieuse pour Eve. En retardant sa mesure et en s'assurant que son couplage avec le signal est imperceptible par Bob, Eve fait tout ce qui est en son pouvoir pour récupérer le maximum d'information. Cette stratégie est donc optimale. Dans le cadre de ce modèle [3], on représente l'appareil de mesure d'Eve par deux systèmes d'axes dont les directions et les longueurs sont optimisées pour obtenir la meilleure qualité d'espionnage. Eve dispose de deux degrés de liberté. L'un sert à maximiser l'information collectée par Eve à bruit donné et l'autre à ajuster le bruit induit par la mesure à son niveau maximal *QBER*.

Voilà le résultat de ce calcul :

- (a) Eve doit utiliser deux systèmes d'axes, chacun non-orthogonal. Chaque base est caractérisée par un recouvrement $\cos \alpha$ paramétré par un même angle α . En revanche, les deux systèmes d'axe sont orthogonaux entre eux.
- (b) La mesure a une fidélité \mathcal{F} de $(1 + \cos \alpha)/2$. Ou bien, du point de vue inverse, le bruit de la mesure est de :

$$1 - \mathcal{F} = (1 - \cos \alpha)/2 \quad (2.3)$$

- (c) L'information retirée par Eve est égale à sa capacité à discerner entre les deux états non-orthogonaux de ses bases. On montre que de manière optimale, on arrive à distinguer deux états de recouvrement $\cos \alpha$ avec une probabilité égale à $(1 + \sin \alpha)/2$. Eve se trompe donc avec une probabilité² de $(1 - \sin \alpha)/2$, ce qui, d'après (B.3), lui donne une augmentation d'information de :

$$I_{AE} = 1 - H((1 - \sin \alpha)/2) \quad (2.4)$$

On trouve ainsi l'information maximale que l'espionne Eve peut retirer des signaux d'Alice en limitant la fidélité de sa mesure de sorte que $QBER = 1 - \mathcal{F}$. En injectant (2.3) dans (2.4), on obtient :

$$I_{AE} = 1 - H\left(\frac{1 - \sqrt{1 - (1 - 2 QBER)^2}}{2}\right) \quad (2.5)$$

Cette stratégie peut être implémentée par un circuit à deux bits quantiques [4].

Pour de faibles valeur de *QBER*, l'information maximale qu'Eve peut acquérir est proportionnelle au taux d'erreur binaire *QBER* :

$$I_{AE} \approx 2,9 QBER \quad (2.6)$$

2.1.2.3 Bilan : *QBER* < 15 %

En faisant l'hypothèse qu'Alice et Bob disposent d'un temps infini pour échanger une clé commune, on arrive au résultat que la sécurisation de l'échange est assurée tant que l'information maximale prélevée par Eve est inférieure à l'information partagée entre Alice et Bob.

2. La démonstration de ce résultat est fournie en annexe C

Effectivement, du moment qu’Alice et Bob disposent d’un surplus d’information par rapport à Eve, ils peuvent s’assurer qu’après un certain nombre d’essai, un bit sera transmis sans qu’Eve n’ait pu le lire.

Ce critère ($I_{AE} < I_{AB}$) garantit la confidentialité d’un échange vis-à-vis d’un éventuel espion pourvu que le canal satisfasse à la condition :

$$\begin{aligned}
 1 - H\left(\left(\frac{1 - \sqrt{1 - (1 - 2QBER)^2}}{2}\right)\right) &< 1 - H(QBER) \Leftrightarrow \\
 \left(\frac{1 - \sqrt{1 - (1 - 2QBER)^2}}{2}\right) &> QBER \Leftrightarrow \\
 QBER &> \frac{1 - 1/\sqrt{2}}{2} \approx 15\% \quad (2.7)
 \end{aligned}$$

déduite des équations (2.2) et (2.5). Ce critère est illustré dans la figure 2.1.

Ainsi, dès lors que le bruit sur le canal est inférieur à 15 %, Eve n’a aucun moyen d’intercepter le message échangé entre Alice et Bob pour constituer leur clé secrète.

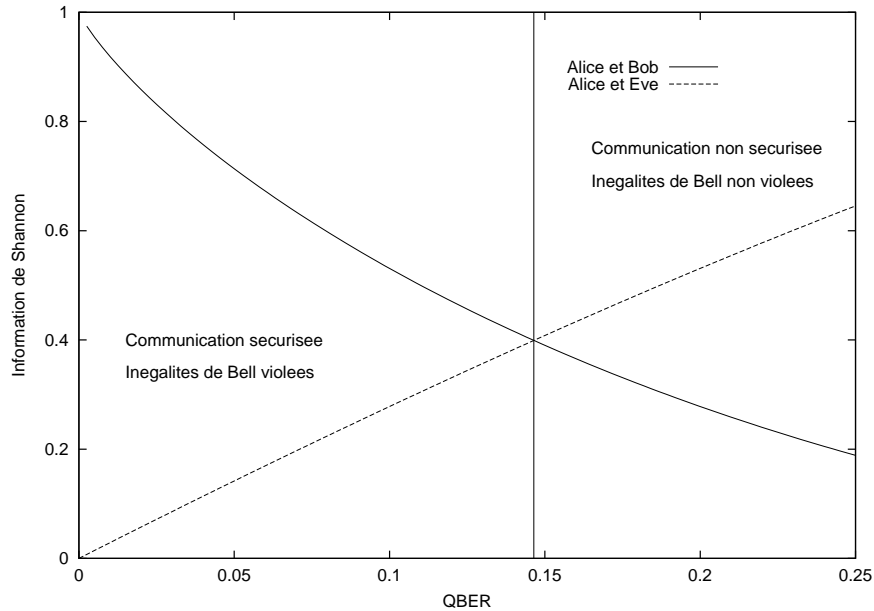


FIG. 2.1 – *Information mutuelle respectivement d’Alice et Bob et d’Alice et Eve. Lorsque le bruit dépasse $\approx 15\%$, Eve peut intercepter le message transmis d’Alice à Bob sans que son intervention ne soit détectable. Comme montré dans la section 2.2.4 (équation (2.28)), la même plage $QBER < 15\%$ correspond à l’assurance de la sécurisation de la communication et à la démonstration expérimentale, par violation d’une inégalité de Bell, de son caractère quantique.*

2.1.2.4 Stratégie optimale d’espionnage cohérent

L’étude menée en section 2.1.2.2 a fourni la borne supérieure théorique à l’information qu’Eve peut collecter en espionnant bit à bit le signal émis par Alice. Il est fort improbable que dans un futur proche un appareil d’écoute qui atteigne la limite théorique soit construit. La principale raison est que cet appareil doit pouvoir conserver de manière cohérente l’état de son appareil de mesure pendant un temps de l’ordre de la seconde, car la publication des choix de bases par Alice intervient en toute fin du protocole utilisé (par exemple BB84).

Néanmoins, il est rassurant de savoir qu'en prenant certaines précautions sur le bruit du canal, aussi drastiques soient-elles, on est sûr qu'aucun appareil ne pourra violer la confidentialité de l'échange.

Dans cette ligne d'idée, il est concevable d'améliorer davantage l'espionnage, mais de manière ultime cette fois-ci. L'idée consiste pour Eve à stocker de manière cohérente dans un registre long de la taille du nombre de bits échangés entre Alice et Bob.

On est alors en mesure de raffiner le modèle d'attaque sur des bits individuels de la section 2.1.2.2. Nous n'aborderons pas ce point, qui est expliqué dans la section VI-G de l'article de revue [3].

Le résultat est que, disposant d'une capacité de stockage infinie et cohérente, Eve peut collecter de l'information *incognito* jusqu'à un $QBER > 11\%$.

Toujours est-il que la meilleure parade est l'espionnage quantique est une ligne de communication peu bruitée. Cela signifie contrairement que les fibres optiques doivent présenter une faible atténuation et que les éventuels répéteurs (amplification et régénération du signal) doivent introduire le moins de bruit possible.

2.1.3 Modèle d'évaluation du bruit

Dans cette partie nous présentons un modèle simple qui permet d'estimer le bruit lors d'une communication sur un canal réel (avec ses défauts).

Etant données les technologies actuelles, nous montrerons que le bruit, exprimé en QBER (dont la définition figure dans l'équation (2.1)), reste inférieur aux 15 % (équation (2.7)) nécessaires à la confidentialité de l'échange pour une distance de l'ordre de 40 km.

Nous faisons l'hypothèse que la source de photons est parfaite: les photons sont tous émis un par un. En revanche, les erreurs de transmission proviennent du canal et du récepteur. Nous modéliserons le canal, par exemple une fibre optique, par un filtre d'atténuation linéique α . Le même modèle de canal s'applique également pour l'air. Le récepteur est susceptible de commettre deux types d'erreur de détection.

1. **Oubli de comptage:** Le détecteur, par exemple une photodiode, ne compte qu'une certaine fraction des photons incidents. Cette erreur est caractérisée par un taux η , appelé efficacité du détecteur. Ainsi, lorsque Alice et Bob sont séparés d'une distance z , l'atténuation du signal émis par Alice est de $t(z) = 10^{-\alpha z/10}$ au niveau du récepteur de Bob.
2. **Comptage en trop:** Il arrive que la photodiode détecte un photon qui n'ait pas été émis. On caractérise ces erreurs par un taux D de « dark counts ».

Les équipements actuels permettent de construire une liaison optique « Alice ↔ Bob » caractérisée par les paramètres suivants :

$$\begin{cases} \alpha &= 0,25 \text{ dB/km} \\ \eta &= 0,1 \\ D &= 10^{-4} \end{cases} \quad (2.8)$$

Nous allons examiner trois configurations de qualité croissante dans les sections qui suivent. Pour chacune d'elle, nous allons évaluer les deux quantités suivantes :

1. $C(z)$: Fraction de photons transmis par Alice arrivant effectivement à Bob.
2. $Q(z)$: Taux d'erreur commis par le dispositif détecteur de Bob.

Le taux d'erreur binaire, en fonction de la distance z qui sépare Alice et Bob, est alors donné par $QBER = \frac{C(z)}{C(z)+Q(z)}$, soit en dB :

$$QBER_{dB} = 10 (\log_{10}(C(z)) - \log_{10}(C(z) + Q(z))) \quad (2.9)$$

2.1.3.1 Configuration n° 1 : BB84

Dans cette première configuration, une unique fibre optique relie Alice directement à Bob. Ce dispositif, représenté dans la figure 2.2, est celui découlant naturellement du protocole BB84.

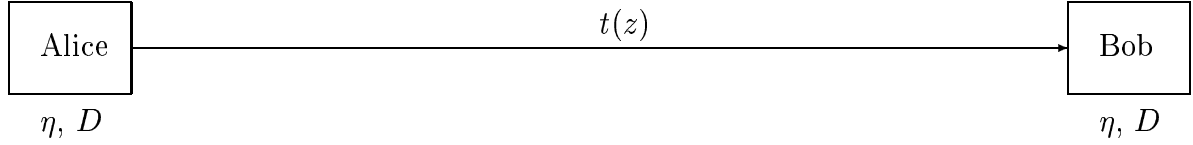


FIG. 2.2 – Configuration n° 1. Ce dispositif simple permet d’implémenter BB84. Alice et Bob sont séparés d’une distance z . Les paramètres $t(z) = 10^{-\alpha z/10}$, η et D sont ceux qui ont été définis dans l’équation (2.8).

Le taux de photons arrivant chez Bob et étant détectés vaut alors $C_1(z) = t(z) \cdot \eta$, car la fraction $t(z)$ est dissipée par la fibre durant la propagation et la fraction η est correctement comptabilisée par la photodiode de Bob.

Le taux d’erreur $Q_1(z)$ est égal à la fraction de photons détectés par Bob mais qui n’ont pas été émis par Alice. Ce nombre ne se ramène pas simplement au taux de « dark counts », puisqu’il faut en plus que l’instant du « dark count » corresponde à celui de la perte d’un photon (qu’il soit absorbé par la fibre optique ou non détecté par la photodiode de Bob). On a donc pour cette première configuration $Q_1(z) = D \cdot (1 - t(z) \cdot \eta)$, produit de D par le taux $1 - C_1(z)$ de perte de photons.

2.1.3.2 Configuration n° 2 : Source à paire de photons

Nous considérons maintenant un montage symétrique où une paire de photons est créée par un cristal se trouvant à égale distance $z/2$ d’Alice et de Bob. La configuration est schématisée dans la figure 2.3 et correspond à l’idée d’Ekert d’utiliser des photons intriqués pour réaliser une communication quantique³.

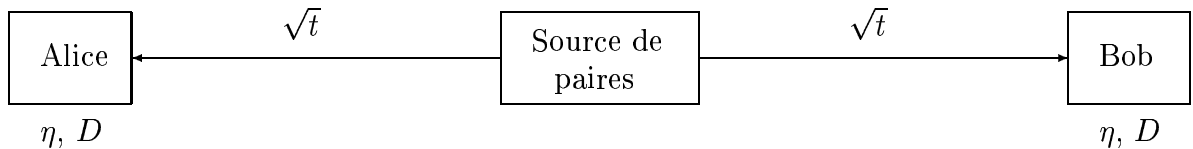


FIG. 2.3 – Configuration n° 2. Ce dispositif réalise une communication basée sur la cryptographie dite de Ekert.

Les photons arrivant simultanément chez Alice et Bob présentent chacun une probabilité $C_1(z/2)$ d’être correctement détectés. Le taux $C_2(z)$ est donc égal au produit des deux probabilités $C_1(z/2)$, puisque les erreurs survenant sur le parcours vers Alice ou vers Bob sont *a priori*

3. Se reporter à la section 2.3

indépendantes. On a donc⁴ :

$$\begin{aligned} C_2(z) &= (C_1(z/2))^2 \\ &= t(z) \cdot \eta^2 \end{aligned}$$

Les erreurs de détections correspondent aux photons détectés par Alice et Bob mais non émis par le cristal du milieu. La plupart des erreurs vont arriver d'un côté ou de l'autre : soit Alice, soit Bob détecte un photon "virtuel" à la place du photon émis par le source de paires mais absorbé lors de son chemin. Ce genre d'erreur survient avec la probabilité :

$$2 \quad \underbrace{C_1(z/2)}_{1 \text{ photon bon}} \quad \underbrace{D \cdot (1 - C_1(z/2))}_{1 \text{ photon mauvais}}$$

Mais il se peut également que les erreurs arrivent concomitamment des deux côtés. Le taux d'erreur est alors le produit des deux probabilités (identiques) de détection d'un photon virtuel alors que le « vrai » photon a été « perdu » avant d'arriver chez Alice ou Bob. Cette erreur simultanée arrive avec un taux :

$$(D (1 - C_1(z/2)))^2$$

En factorisant la somme de ces deux termes, on obtient l'expression du taux d'erreur :

$$Q_2(z) = \left(\sqrt{t(z)} \cdot \eta + D \cdot (1 - \sqrt{t(z)} \cdot \eta) \right)^2 - t(z) \cdot \eta^2 \quad (2.10)$$

2.1.3.3 Configuration n° 3 : Téléportation d'un état de Bell

On considère une configuration composée de deux source à deux photons. Ces sources envoient un photon de chaque paire à Alice et à Bob. Le deuxième photon de chaque paire est envoyé vers un appareil qui mesure l'état conjoint des deux photons dans la base des états de Bell⁵

Ce dispositif, schématisé dans la figure 2.4, réalise la fonction de téléportation quantique. Le principe est que l'état de Bell mesuré communiqué publiquement à Alice et à Bob, qui arrivent alors à en déduire les corrélations entre les photons qu'ils ont chacun mesurés.

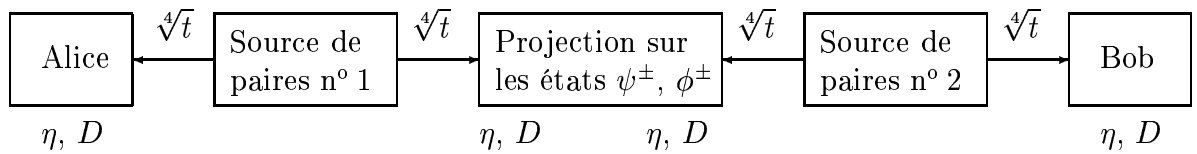


FIG. 2.4 – Configuration n° 3. Ce dispositif permet d'implémenter la téléportation quantique d'un état de Bell.

Nous allons considérer pour simplifier qu'Alice, la première source de paires, l'appareil de mesure d'états de Bell, la deuxième source de paires et Bob sont alignés dans cet ordre et séparés l'un de l'autre par la même distance $z/4$.

Pour le calcul des taux de réussite et d'échec dans la communication et la détection des photons, il faut désormais tenir compte du fait qu'il y a quatre détections pour un échange : Alice et Bob font une mesure ainsi que l'appareil qui réalise la projection sur la base des états de Bell.

4. En vertu de la décroissance exponentielle de $t(z)$, on a $t(z/2) = \sqrt{t(z)}$

5. Voir la définition dans l'équation (2.16).

Le taux de réussite $C_3(z)$ est donc égal à la probabilité de la coïncidence des quatre réussites dans les détections des quatre photons à mesurer. On a donc :

$$C_3(z) = C_3(z)^4 = t(z) \cdot \eta^4 \quad (2.11)$$

La façon d'évaluer le taux d'erreur $Q_3(z)$ est analogue à celle expliquée dans la section 2.1.3.2 précédente. On comptabilise les erreurs qui arrivent sur l'une et l'une seule des quatre mesures, plus celles qui arrivent sur exactement deux des mesures (il faut prendre en compte tous les couples), sur trois et enfin sur les quatre mesures à la fois. Tout dénombrement et tous calculs faits, on trouve une expression semblable à celle que $Q_2(z)$:

$$Q_3(z) = \left(\sqrt[4]{t(z)} \cdot \eta + D \cdot (1 - \sqrt[4]{t(z)} \cdot \eta) \right)^4 - t(z) \cdot \eta^4 \quad (2.12)$$

2.1.3.4 Conclusions du modèle

Les trois courbes donnant le $QBER$ en fonction de la distance z entre Alice et Bob sont représentées dans la figure 2.5.

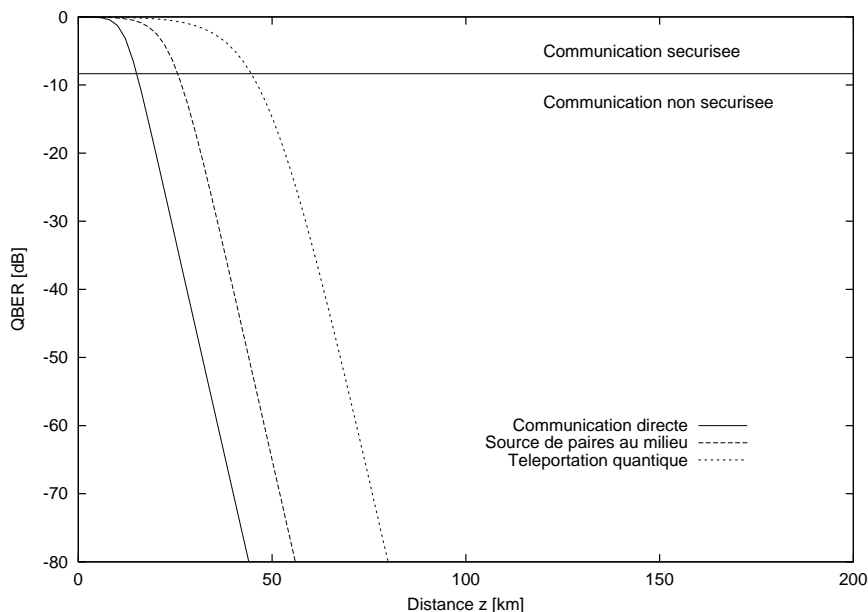


FIG. 2.5 – Taux d'erreur binaire pour trois configurations de communication entre les interlocuteurs Alice et Bob, décrites dans les figures 2.2, 2.3 et 2.4. Le taux d'erreur limite de 15 % au-delà duquel la communication n'est plus sécurisée est reportée comme une ligne horizontale. On peut lire la distance maximale autorisant une communication sécurisée : elle est de l'ordre de quelques dizaines de kilomètres environ (avec les données (2.8)).

2.2 Test d'une inégalité de Bell

Le bruit que l'on rencontre naturellement sur un canal de communication réel, comme une fibre optique commerciale, pourrait dissimuler l'écoute d'une espionne Eve. Cependant, comme expliqué dans la section précédente, Eve ne parvient pas à retirer suffisamment d'information dès lors que le taux d'erreur $QBER$ est inférieur à $\sim 11\%$. Ce résultat a été obtenu par des raisonnements sur les quantités maximales d'information accessibles par Eve ou Bob, en supposant que l'on pouvait toujours raisonner dans le cadre théorique du protocole BB84.

Or rien ne garantit qu'en présence de bruit la communication soit toujours « quantique ». Le but de cette section est de préciser cette notion. On montrera que les postulats de la mécanique quantique utilisés dans le protocole BB84 restent applicables tant qu'un test fondamental de la mécanique quantique (en l'occurrence la violation d'une inégalité de Bell) se montre concluant.

Il en découle le résultat remarquable (2.28) qu'une communication est sécurisée si et seulement si le canal est quantique.

2.2.1 Intrication

Un système composite de n particules sans interactions se décrit en physique classique par un « point » dans un espace des phases à n dimensions. Lorsque les particules n'interagissent pas entre elles, elles sont indépendantes les unes des autres.

Il en va autrement dans une description quantique : les n particules évoluent également dans un espace à n dimensions, mais, même en l'absence d'interactions, elles ne sont pas indépendantes. Les particules sont corrélées entre elles. C'est cette propriété de nature quantique que l'on appelle « intrication ».

L'amplitude des corrélations peut être évaluée par le nombre de Schmidt [5] ou l'entropie de von Neumann (voir l'annexe B). Les particules maximales intriquées, comme une paire de bits quantiques dans un état de Bell (section 2.16), ne peuvent être décrites que par une théorie quantique. C'est de type d'état qui permet de tester que le canal de communication entre Alice et Bob est bien quantique. A l'inverse, lorsque les particules sont peu intriquées, la description classique devient valide.

2.2.1.1 Cadre mathématique

En sciences physiques, on appelle « intrication » la propriété d'algèbre linéaire qu'un produit d'espaces de Hilbert conserve une structure d'espace de Hilbert.

Deux particules sont décrites en mécanique quantique dans deux espaces de Hilbert différents. L'état conjoint du système de deux particules appartient donc à l'espace produit tensoriel de deux espaces des particules individuelles.

Or d'après la linéarité de la mécanique quantique, deux particules peuvent être dans un état superposition linéaire d'états tensoriels.

Ainsi, en considérant le cas de 2 particules A et B à 2 états $|\uparrow\rangle$ et $|\downarrow\rangle$, chacune dans un état :

$$\begin{aligned} |\psi_A\rangle &= \alpha_A|\uparrow\rangle + \beta_A|\downarrow\rangle \\ |\psi_B\rangle &= \alpha_B|\uparrow\rangle + \beta_B|\downarrow\rangle \end{aligned} \quad (2.13)$$

L'état conjoint s'écrit :

$$\begin{aligned} |\psi_{AB}\rangle &= (\alpha_A|\uparrow\rangle + \beta_A|\downarrow\rangle) \otimes (\alpha_B|\uparrow\rangle + \beta_B|\downarrow\rangle) \\ &= \alpha_A\alpha_B|\uparrow\uparrow\rangle + \alpha_A\beta_B|\uparrow\downarrow\rangle + \beta_A\alpha_B|\downarrow\uparrow\rangle + \beta_A\beta_B|\downarrow\downarrow\rangle \end{aligned} \quad (2.14)$$

Il est superposition linéaire des états à deux particules : $|\uparrow\uparrow\rangle$, $|\uparrow\downarrow\rangle$, $|\downarrow\uparrow\rangle$, $|\downarrow\downarrow\rangle$. Ces états portent le nom d'états EPR⁶.

2.2.1.2 Non localité quantique

L'existence de ce type d'état implique qu'une mesure sur la particule A affecte l'état de la particule B . Par exemple, lorsque A est mesurée dans l'état $|\uparrow\rangle$, B se retrouve dans l'état

$$\langle\uparrow_A|\psi_{AB}\rangle = \alpha_A(\alpha_B|\uparrow\rangle + \beta_B|\downarrow\rangle) \quad (2.15)$$

6. Pour Einstein, Podolsky, Rosen [6].

Ceci reste valable même si les deux particules A et B sont éloignées. Il n'y a pas de transfert d'information entre A et B au moment où l'on touche A . La projection de l'état de A affecte instantanément l'état $|\psi_{AB}\rangle$ et par conséquent l'état partiel de la particule B . Ce phénomène est appelé *téléportation* quantique.

2.2.1.3 Différents aspects de l'intrication

A priori, dans n'importe quel système, tout est intriqué avec tout. Néanmoins, un système est toujours couplé à un environnement. De manière analogue à la thermalisation d'un système fermé couplé à un réservoir, il y a un transfert d'intrication du système vers l'environnement. Or l'environnement, classique, peut absorber infiniment d'intrication. Le système voit donc son intrication propre diminuer : on dit qu'il y a décohérence.

L'intrication est donc une ressource rare car fragile. Voilà quelques expériences d'intérêt scientifique qui tirent profit de l'intrication :

1. **Théorie de la mesure** : Intrication entre le mètre et le système.
2. **Complémentarité** : Expériences d'interférométrie où la particule s'intrique avec l'interféromètre.
3. **Téléportation** : Un état intriqué à plusieurs particules distantes est affecté de manière globale lorsqu'on affecte (projection, évolution) l'état d'une seule des particules. On parle aussi de non-localité quantique.
4. **Calcul quantique** : Intrication de registres de bits quantiques (aussi appelés *qubits*) afin de mener des calculs en parallèle. Les qubits doivent être manipulés de manière astucieuse de façon à ce qu'une mesure délivre un résultat pertinent : on parle de *distillation*⁷ quantique. Cette opération de concentration de l'intrication dans un état est opérée par les algorithmes quantiques, tel que celui de D. Deutsch et R. Jozsa [7] (premier algorithme quantique plus rapide que les algorithmes classiques) ou de P. Shor [8] (algorithme de factorisation des entiers en produit de facteurs premiers réalisable en temps polynomial). L'état de l'art du domaine du calcul quantique est traité dans l'ouvrage de référence de M. Nielsen et I. Chuang [9].

2.2.2 Etats de Bell

Dans le cas de systèmes à 2 bits quantiques, on utilise habituellement la base orthonormée suivante :

$$\begin{cases} |\phi^+\rangle = \frac{1}{\sqrt{2}}(|\downarrow\downarrow\rangle + |\uparrow\uparrow\rangle) \\ |\phi^-\rangle = \frac{1}{\sqrt{2}}(|\downarrow\downarrow\rangle - |\uparrow\uparrow\rangle) \\ |\psi^+\rangle = \frac{1}{\sqrt{2}}(|\downarrow\uparrow\rangle + |\uparrow\downarrow\rangle) \\ |\psi^-\rangle = \frac{1}{\sqrt{2}}(|\downarrow\uparrow\rangle - |\uparrow\downarrow\rangle) \end{cases} \quad (2.16)$$

des 4 états dits de Bell.

2.2.3 Mécanique quantique *versus* théorie locale

2.2.3.1 La mécanique quantique est-elle incomplète ?

« Dieu ne joue pas aux dés », disait Albert Einstein en parlant des implications philosophiques de la mécanique quantique alors naissante.

7. Dans la littérature, la *distillation* quantique sert à qualifier toute manipulation augmentant l'intrication. L'opération inverse est appelée *dilution* quantique.

La caractère aléatoire qui accompagne toute mesure quantique a déstabilisé plus d'un physicien : un monde déterministe serait intellectuellement plus satisfaisant.

Dans le formalisme quantique, une superposition d'états comme :

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|\uparrow\rangle + |\downarrow\rangle) \quad (2.17)$$

dont on évalue le spin selon la direction z donnera -1 ou $+1$ ⁸ alors que l'état $|\psi\rangle$ est parfaitement bien déterminé.

Il est donc légitime de se demander s'il n'existe pas une variable, cachée de l'expérimenteur, qui déterminerait le résultat de la mesure. On pourrait imaginer qu'un paramètre λ (voir la figure 2.6), propre au système, détermine l'état de la mesure : lorsque λ appartient à $[-\pi/2, +\pi/2]$ (respectivement à $[-\pi, -\pi/2] \cup [+\pi/2, +\pi]$), la mesure conduit au résultat $+1$ (respectivement -1). Une fonction $A(\lambda)$ binaire étendrait l'opérateur quantique $\widehat{\sigma}_z$ de projection de spin selon l'axe z .

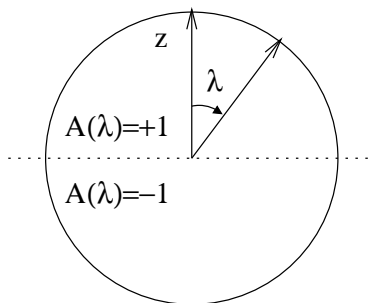


FIG. 2.6 – Un exemple de variable cachée (λ) pour le spin $\frac{1}{2}$ mesuré selon l'axe z

L'utilisation de variables cachées pourrait *a priori* permettre de trouver une super-théorie qui engloberait la mécanique quantique mais qui lui enlèverait son indéterminisme. Cette hypothétique théorie de variables cachées serait donc déterministe et locale. La localité découle du fait que la propagation de l'information (cachée) est limitée par la vitesse de la lumière : les mesures n'affectent de manière instantanée que la partie du système mesurée.

2.2.3.2 Une inégalité de Bell : critère CHSH

Une unique particule, comme un spin $\frac{1}{2}$, peut (voir la figure 2.6) être décrite par une variable cachée.

Qu'en est-il d'un système de plusieurs particules ? Nous allons voir que les corrélations quantiques sont plus fortes que les corrélations « classiques » d'une description par une théorie de variables cachées.

L'expérience décrite dans cette section a pour but de donner une quantité mesurable qui renseigne sur l'existence (ou non) de variables cachées. Elle s'inspire d'un raisonnement tenu par J.F. Clauser, M.A. Horne, A. Shimony et R.A. Holt [10].

Considérons deux particules A et B intriquées, dans l'état dit singulet de spin (ou encore état de Bell $|\psi^+\rangle$) :

$$|\psi_S\rangle = \frac{1}{\sqrt{2}} \left(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle \right) \quad (2.18)$$

8. En réalité, en unités de moment cinétique de spin, les valeurs propres sont $\pm\hbar/2$. Pour simplifier, on normalisera les opérateurs de moment cinétiques, de telle sorte que leurs valeurs propres soient ± 1 .

On définit la fonction $E(\vec{u}_A, \vec{u}_B)$ de corrélation du système $\{A, B\}$ dans une mesure du spin suivant les axes \vec{u}_A et \vec{u}_B comme la valeur moyenne du produit des mesures de la projection du spin de la particule A suivant \vec{u}_A et de B selon \vec{u}_B . La valeur moyenne s'entend respectivement dans les sens quantique et probabiliste.

1. Dans le formalisme quantique, l'issue des mesures est aléatoire: la valeur moyenne est la moyenne des résultats obtenus après la répétition d'un grand nombre de mesures. La fonction de corrélation $E(\vec{u}_A, \vec{u}_B)$ se calcule donc de la façon suivante:

$$E(\vec{u}_A, \vec{u}_B) = \langle \psi_S | \hat{S} \cdot \vec{u}_A \otimes \hat{S} \cdot \vec{u}_B | \psi_S \rangle$$

où \hat{S} est l'observable de spin. Tous calculs faits, on trouve que :

$$E(\vec{u}_A, \vec{u}_B) = -\vec{u}_A \cdot \vec{u}_B \quad (2.19)$$

On peut par exemple définir l'axe z comme l'axe \vec{u}_A . Le vecteur \vec{u}_B se décompose donc sous la forme $\vec{u}_B = \cos \alpha \vec{u}_z + \sin \alpha \vec{u}_x$. Les opérateurs de spins dans les deux directions s'écrivent par conséquent dans la base $\{|\uparrow\rangle, |\downarrow\rangle\}$ comme $\hat{S} \cdot \vec{u}_A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $\hat{S} \cdot \vec{u}_B = \begin{pmatrix} \cos \alpha & \sin \alpha \\ \sin \alpha & -\cos \alpha \end{pmatrix}$. Ainsi, la valeur moyenne des corrélations $\langle \psi_S | \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} \cos \alpha & \sin \alpha \\ \sin \alpha & -\cos \alpha \end{pmatrix} | \psi_S \rangle$ se décompose en 4 termes, dont $\langle \uparrow\downarrow | \dots | \uparrow\downarrow \rangle$ et $\langle \downarrow\uparrow | \dots | \downarrow\uparrow \rangle$ sont égaux, valant tous deux $-\cos \alpha/2$ et dont $\langle \uparrow\uparrow | \dots | \uparrow\uparrow \rangle$ et $\langle \downarrow\downarrow | \dots | \downarrow\downarrow \rangle$ sont nuls. La somme vaut donc $2 \times (-\cos \alpha/2)$, soit $-\vec{u}_A \cdot \vec{u}_B$.

2. Dans une théorie de variable(s) cachée(s), le paramètre λ , éventuellement vectoriel, détermine le résultat de la mesure. Néanmoins, étant « caché » de l'expérimentateur, ce paramètre est une grandeur inconnue. Nous faisons donc l'hypothèse que λ est une variable aléatoire de loi $\mu(\lambda)$. Les deux particules A et B étant supposées distantes, elles sont indépendantes pour une mesure simultanée. La fonction de corrélation vaut donc dans ce cadre :

$$E(\vec{u}_A, \vec{u}_B) = \int d\lambda \mu(\lambda) A(\lambda, \vec{u}_A) B(\lambda, \vec{u}_B) \quad (2.20)$$

où $A(\lambda, \vec{u}_A)$ et $B(\lambda, \vec{u}_B)$ sont les deux fonctions binaires qui donne le résultat des mesures de spin selon z pour chacune des particules A et B .

Etant donné que chacune des fonctions $A(\lambda, \vec{u}_A)$ et $B(\lambda, \vec{u}_A)$ ne prend que les valeurs ± 1 , la valeur moyenne (2.20) du produit des mesures de spins selon les directions \vec{u}_A et \vec{u}_B vérifie :

$$-1 \leq E(\vec{u}_A, \vec{u}_B) \leq +1 \quad (2.21)$$

Pour faire apparaître les corrélations, on considère une deuxième base $\{\vec{u}_{A'}, \vec{u}_{B'}\}$. On introduit alors la grandeur $S(\vec{u}_A, \vec{u}_B; \vec{u}_{A'}, \vec{u}_{B'})$, notée simplement S pour ne pas allourdir les notations :

$$S = E(\vec{u}_A, \vec{u}_B) + E(\vec{u}_A, \vec{u}_{B'}) - E(\vec{u}_{A'}, \vec{u}_B) + E(\vec{u}_{A'}, \vec{u}_{B'}) \quad (2.22)$$

Alors, en mécanique quantique, on peut donner à S des valeurs qui sont interdites par les théories à variables cachées :

1. En faisant le choix d'axes de la figure 2.7, les directions vérifient: $\vec{u}_A \cdot \vec{u}_B = \vec{u}_A \cdot \vec{u}_{B'} = -\vec{u}_{A'} \cdot \vec{u}_B = \vec{u}_{A'} \cdot \vec{u}_{B'} = \frac{1}{\sqrt{2}}$, de telle sorte que S prend la valeur :

$$S = -2\sqrt{2} \quad (2.23)$$

2. Quant aux théories à variables cachées, on a l'identité suivante :

$$A(\lambda, \vec{u}_A)B(\lambda, \vec{u}_B) + A(\lambda, \vec{u}_A)B(\lambda, \vec{u}_{B'}) + A(\lambda, \vec{u}_{A'})B(\lambda, \vec{u}_B) - A(\lambda, \vec{u}_{A'})B(\lambda, \vec{u}_{B'}) = A(\lambda, \vec{u}_A) \underbrace{(B(\lambda, \vec{u}_B) + B(\lambda, \vec{u}_{B'}))}_{\text{vaut 0 ou 2}} + A(\lambda, \vec{u}_{A'}) \underbrace{(-B(\lambda, \vec{u}_{B'}) + B(\lambda, \vec{u}_B))}_{\text{vaut 2 ou 0}} \quad (2.24)$$

Ainsi, seul un des deux termes de la factorisation est non nul. On en déduit que l'issue de la mesure de (2.24) ne peut être que -2 ou $+2$. Ainsi, en prenant la valeur moyenne $\int d\lambda \mu(\lambda) \cdot$, l'on aboutit à un encadrement de S :

$$|S| \leq 2 \quad (2.25)$$

qui exprime que les corrélations dans les théories à variables cachées sont limitées.

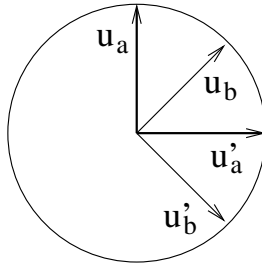


FIG. 2.7 – Choix des directions de mesure pour une expérience CHSH de violation d'une inégalité de Bell

L'inégalité (2.23) peut ainsi être violée par des systèmes quantiques fortement intriqués, comme le système de 2 spins $\frac{1}{2}$ dans l'état singulet (2.18).

La mécanique quantique permet de superposer des états produits, ce qui permet de produire des états à plusieurs particules très corrélés. Certaines corrélations quantiques, dont celles mesurées par (2.23), ne sont pas envisageables dans une théorie déterministe locale à variables cachées.

La portée de ce résultat est universelle : nous vivons dans un monde où les événements sont intrinsèquement aléatoires. Pis encore, il n'est de aucun moyen de réduire cette indétermination, aussi précise soit notre connaissance du monde.

Une telle percée théorique se doit d'être observée expérimentalement afin qu'il soit validé. Les inégalités de Bell sous la forme CHSH (2.23) et (2.25), se prêtent justement bien à une implémentation expérimentale.

2.2.3.3 Victoire de la mécanique quantique

Les premières expériences recherchant une violation de l'inégalité (2.25) de Bell commencèrent dans les années 1970. Fry et Thomson au Texas, puis A. Aspect à Orsay [11]-[12], permirent de mesurer le nombre S dans la configuration de la figure 2.7 sur des paires de photons produites par des atomes de calcium :

$$S = 2,697 \pm 0,015$$

La super-théorie déterministe et locale n'existe donc pas, du moins pour ce système. Nous devons admettre l'indéterminisme fondamental de la mécanique quantique : « Dieu joue aux dés ».

2.2.4 Critère de violation d'une inégalité de Bell en environnement bruité

L'expérience d'Aspect *et al.* démontrant la violation de l'inégalité (2.25) de Bell a été menée en laboratoire, où les sources de bruit ont soigneusement été réduites au maximum.

Lorsque l'on cherche à réaliser la même expérience dans un environnement réel, comme par exemple en utilisant une fibre optique à usage de télécommunications, il faut tenir compte du bruit ambiant.

Le bruit va tout naturellement affaiblir la relation (2.23). Néanmoins nous disposons d'une certaine marge de manœuvre : entre (2.23) et (2.25), il y a un facteur $\sqrt{2}$ qui garantit que l'on peut observer la violation d'une inégalité de Bell, même dans un environnement bruité.

Pour étudier l'influence du bruit sur les corrélations entre deux particules A et B , nous introduisons la quantité $E(\vec{u}_A, \vec{u}_B | QBER)$. Elle est égale est la corrélation des produits des polarisations selon \vec{u}_A et \vec{u}_B en présence d'une probabilité d'erreur de $QBER$.

Pour chaque mesure du produit des polarisations, deux classes de cas de figures se présentent :

1. La mesure n'est pas affectée par le bruit. Ceci survient avec une probabilité de $(1 - QBER)$. A ce moment-là, la corrélation mesurée est égale à la corrélation que l'on mesurerait en l'absence de bruit.
2. Le bruit a perturbé la mesure : cet événement a une probabilité égale à $QBER$. Dans ce cas, le résultat de la mesure est faux. Comme chaque issue est -1 ou $+1$, la corrélation mesurée est donc opposée à la vraie corrélation.

Le bruit modifie donc la corrélation selon une loi linéaire :

$$\begin{aligned}
 E(\vec{u}_A, \vec{u}_B | QBER) &= (1 - QBER) \underbrace{E(\vec{u}_A, \vec{u}_B)}_{\text{résultat juste}} + QBER \underbrace{(-E(\vec{u}_A, \vec{u}_B))}_{\text{résultat faux}} \\
 &= (1 - 2 QBER) E(\vec{u}_A, \vec{u}_B) \\
 &= 2\sqrt{2} (1 - 2 QBER) \text{ (Dans la configuration la figure 2.7)} \quad (2.26)
 \end{aligned}$$

Evaluons le niveau bruit qui ne permet plus d'observer la violation de l'inégalité de Bell :

$$\underbrace{2\sqrt{2} (1 - 2 QBER)}_{(2.26)} < \underbrace{2}_{(2.25)} \Leftrightarrow QBER > \frac{1 - 1/\sqrt{2}}{2} \quad (2.27)$$

On constate que le critère sur le bruit (2.27) et le même que celui qui garantit la sécurité de la communication par rapport à « l'écoute quantique » (2.7) :

$$\boxed{\text{sécurité de la communication} \Leftrightarrow \text{violation d'une inégalité de Bell}} \quad (2.28)$$

Ce résultat remarquable [13] intrigue énormément les chercheurs. Est-il fortuit ou y a-t-il une raison fondamentale qui expliquerait la coïncidence de ces deux critères ?

2.3 Cryptographie avec des paires de photons intriqués

Les deux sections 2.1 et 2.2 ont montré que lorsque le bruit sur le canal de communication est inférieur à 15 %,

- on peut assurer, grâce à un bilan (classique) sur les informations disponibles, qu'un espion Eve ne peut pas acquérir toute l'information échangée par Alice et Bob. Il est donc possible pour Alice et Bob moyennant un certain nombre de rémissions, d'échanger des bits de manière sûre, vis-à-vis d'Eve.
- on peut mesurer la violation d'une inégalité de Bell.

La méthode de cryptologie proposée par A. K. Ekert en 1992 [14] consiste à générer des paires de photons intriqués entre Alice et Bob. Toute intervention d'Eve diminuerait *de facto* les corrélations entre les mesures d'Alice et de Bob. Une intervention suffisamment légère peut ne pas suffire à empêcher la violation des inégalités de Bell. Mais rappelons que le test d'une inégalité de Bell ne consiste pas à déceler la présence d'un espion, mais de garantir que le transfert se fait de manière quantique. C'est par exemple au protocole BB84 dont nous verrons qu'il s'applique dans ce cas, de vérifier l'absence d'espion sur le canal.

Le type de mesures effectuées sur les photons par Alice et Bob peuvent être très diverses. Nous donnons dans le chapitre 3 un état de l'art dans les méthodologies de cryptographie quantique.

2.3.1 Produire un état de Bell

Certains cristaux possèdent des propriétés non-linéaires qui se manifestent par la génération de nouvelles fréquences. Un phénomène typique d'optique non-linéaire est la division de fréquence: un photon de pompe de fréquence ν_P donne naissance à deux photons de fréquence ν_S et ν_I satisfaisant à:

$$\begin{array}{rcl} \nu_P & = & \nu_S + \nu_I \\ \text{Pompe} & \longrightarrow & \text{Signal} + \text{Idler} \end{array} \quad (2.29)$$

Les deux photons créés sont corrélés. En assurant un accord de phase tout au long du cristal, on garantit que la production de paires de photons est cohérente. En tout point du cristal, les photons créés interfèrent constructivement avec l'onde de leur fréquence (*signal* ou *idler*): les deux nouvelles fréquences sont amplifiées.

2.3.2 Mesure des corrélations

Du côté d'Alice comme de Bob, la polarisation peut être mesurée selon deux axes. Une lame séparatrice permet de sélectionner la polarisation à mesurer, c'est-à-dire la base à utiliser. Pour chaque base, une lame séparatrice de polarisation permet de distinguer les deux codes (0 ou 1). Ce dispositif, application directe du protocole BB84, est illustré dans la figure 2.8.

Pour mesurer les corrélations de polarisation du type $E(\vec{u}_A, \vec{u}_B)$, introduites dans la section 2.2.3.2, Alice et Bob commencent par fixer leur base respective. Après une série de mesures, ils dépouillent leurs résultats et évaluent de manière statistique la corrélation recherchée.

2.3.3 Equivalence avec le protocole BB84

Sur la plupart des schémas, la source à paires de photons est placée entre Alice et Bob, pour insister sur la symétrie du dispositif. Néanmoins, il est habituel dans la pratique de déplacer la source des paires chez Alice par exemple.

Les résultats de ce chapitre sont alors toujours valables. On retrouve alors un schéma de communication élémentaire, du type de celui de la figure 1.1.

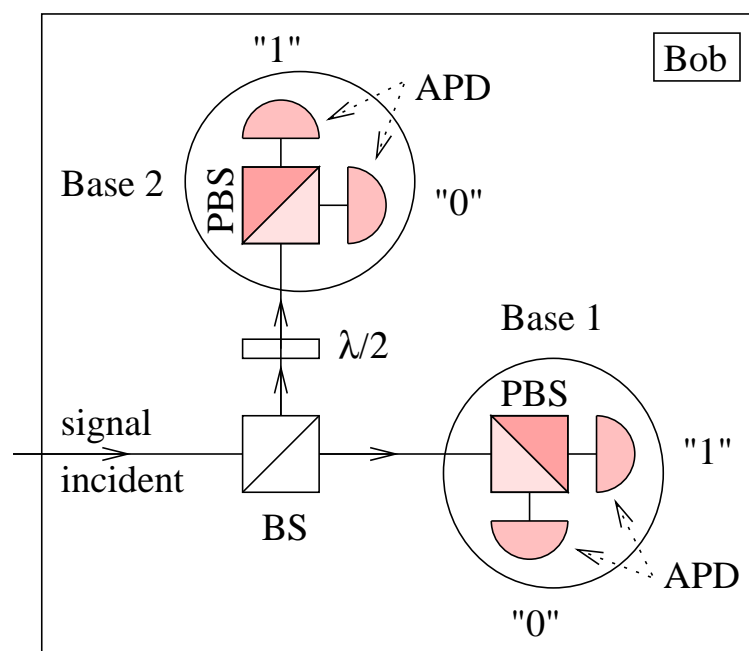


FIG. 2.8 – *Système typique de mesure de la polarisation. BS : séparateur de faisceau (beamsplitter), PBS : séparateur de faisceau en polarisation (polarisation beamsplitter), PBS : séparateur de faisceau en polarisation (polarisation beamsplitter), APD : photodiode à avalanche (avalanche photodiode), $\lambda/2$: lame à retard demi-onde.*

Chapitre 3

Quelques expériences de cryptographie quantique

3.1	Principaux acteurs au niveau mondial	27
3.2	Etat de l'art des expériences actuelles	28
3.2.1	Application directe du protocole BB84	28
3.2.2	Utilisation de paires de photons intriqués en polarisation	28
3.2.3	Utilisation de paires de photons intriqués en phase	29
3.2.4	Conclusion	29

Nous présentons dans ce chapitre les différentes expériences menées par les principaux groupes en lien avec la cryptographie quantique. Le lecteur désireux d'en savoir plus trouvera dans chaque paragraphe des références lui permettant d'approfondir les sujets traités.

3.1 Principaux acteurs au niveau mondial

La cryptographie quantique est actuellement très en vogue aux Etats-Unis, ce qui fait qu'elle bénéficie du soutien de nombreuses universités. Le groupe de recherche le plus actif sur ce sujet dans le pays est probablement celui de Los Alamos. Il convient aussi de citer les entreprises privées comme HP ou IBM (c'est dans cette dernière que travaillait Charles H. Bennet quand il a mis au point le protocole BB84).

L'Union Européenne, dans le 5ème PCRD, place les technologies quantiques au cœur de ses préoccupations et leur apporte un soutien important (IST/FET/QIPC).

Plusieurs groupes de recherche européens ainsi que celui de Los Alamos se sont associés pour former le QUCOMM consortium (communications quantiques). Il s'agit des universités de Munich, Vienne, Oxford, Genève et Stockholm (KTH) ainsi que des laboratoires de DERA Malvern (British Telecom) et de Thales Research and Technology (LCR).

Enfin, le GDR regroupe les principaux acteurs français du domaine, comme par exemple l'Ecole Normale Supérieure, l'Institut d'Optique Théorique et Appliquée ou les anciens laboratoires du CNET.

Voyons maintenant comment ces acteurs se répartissent en fonction des différents types d'expériences menées.

3.2 Etat de l'art des expériences actuelles

3.2.1 Application directe du protocole BB84

Le groupe QinetiQ (DERA Malvern, Royaume Uni) a réalisé une mise en œuvre directe du protocole BB84 en polarisant selon les besoins d'Alice un groupe de photons, avant de l'atténuer pour qu'il n'en reste plus qu'un puis de l'envoyer en propagation aérienne libre à Bob [15]. Celle-ci effectue sa mesure à l'aide de cube séparateurs (voir la figure 3.1). Les résultats sont une efficacité de détection de 5 à 10%. Ainsi, pour une source à 10 MHz, une clé a pu être échangée sur 23 km au taux de 700 bits/s. Le groupe développe également des méthodes quantiques de génération de nombres aléatoires appliquées à la cryptographie [16].

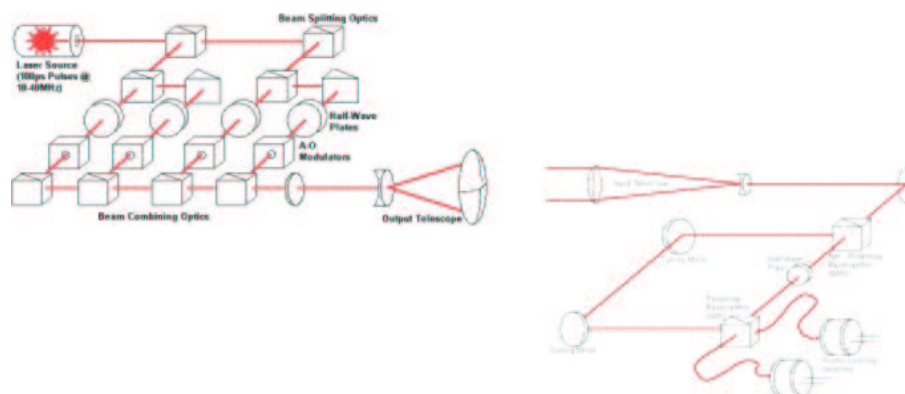


FIG. 3.1 – *Système de cryptographie quantique avec codage en polarisation. Expérience menée au DERA de Malvern.*

3.2.2 Utilisation de paires de photons intriqués en polarisation

Le groupe de Anton Zeilinger de l'université d'Innsbruck (Autriche) a réalisé une démonstration d'un crypto-système utilisant l'intrication de photons en phase incluant la correction d'erreurs sur une distance de 360 m [17].

Des fibres optiques monomodes ont été utilisées pour tester les inégalités de Bell sous la forme d'inégalités de Wigner.

L'ensemble du protocole de cryptographie « Ekert », décrit dans la section 2.3 a été implémenté à Los Alamos par le groupe de Paul Kwiat [18]. Plusieurs stratégies d'espionnage ont été testées sur ce système. Comme le montre la théorie (voir par exemple la section 2.2.4), ils observèrent une augmentation du taux d'erreur binaires lorsque l'espion opère sur le canal.

Enfin, le groupe de l'université de Genève, mené par Nicolas Gisin, a réalisé un système autocompensé dans lequel les photons, émis par Bob, effectuent un aller et retour dans une fibre [19]-[20]-[21]-[22]. Alice leur transmet l'information « au vol » à l'aide de rotateurs de Faraday. Une liaison Lausanne-Genève a ainsi été réalisée (distance : 67 km) et une clé de 20 kbits a été transmise à la fréquence de 1 kHz avec un taux d'erreur de 1,35%. Le dispositif expérimental est illustré dans la figure 3.2.

L'avantage de l'intrication en polarisation réside dans le fait que les analyseurs sont simples et efficaces. Cependant, la polarisation n'est pas assez robuste à la décohérence dans les fibres télécoms usuelles.

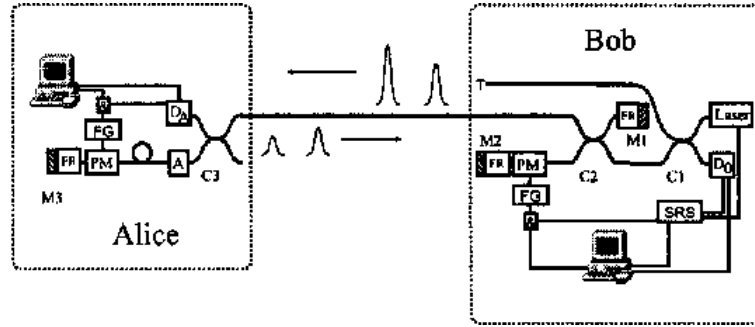


FIG. 3.2 – Montage expérimental d'un système de cryptographie quantique interférométrique avec compensation des fluctuations de polarisation par miroirs de Faraday. $C1, C2, C3$: coupleurs $M1, M2, M3$: miroirs de Faraday. Miroirs ordinaires avec des rotateurs de Faraday (FR) PM : Modulateur de phase A : Atténuateur D_0 : Compteur de photons D_A : Photodiode T : Sortie optionnelle de déclenchement SRS : Générateur de retard FG : Générateur de fonction & : Porte ET

3.2.3 Utilisation de paires de photons intriqués en phase

L'intrication en phase, si elle dérive beaucoup, peut quant-à elle être compensée localement chez Alice et Bob à l'aide d'interféromètres. C'est ce qui explique le développement de ce type d'expérience.

Une source émet à chaque instant plusieurs paires de photons dont les phases sont identiques mais aléatoires. Alice et Bob ajuste la phase de leur interféromètre pour que leurs photons parcourent le même chemin.

Cette idée a été mise en œuvre courant 2000 par le groupe de Nicolas Gisin (Genève), en vue de réaliser un système de cryptographie quantique asymétrique [23].

Enfin, les laboratoires de British Telecom ont réalisé un tel dispositif de codage sur fibre optique à $1,3 \mu\text{m}$, avec un débit de $1,4 \text{ kbits/s}$ sur 10 km [24].

3.2.4 Conclusion

A ce jour, une entreprise privée a réussi à commercialiser des cryptosystèmes. Il s'agit d'une spin-off de l'université de Genève créée en 2001, appelée id Quantique [1] et ayant pour clients des banques suisses.

Annexe A

Rappels de mécanique quantique, liens avec le protocole BB84

A.1	Fonction d'onde et vecteur d'état	30
A.2	Le problème de la mesure en mécanique quantique	31
A.3	Une illustration des principes de superposition et de réduction du paquet d'onde : le "paradoxe" du chat de Schrödinger	32
A.4	Commutation des observables, compatibilité des mesures et relation d'incertitude ; application aux observables de BB84	33
A.5	Conclusion	34
A.6	Complément : le théorème de non clonage quantique	34

Avertissement

Nous présentons dans cette annexe certaines notions de mécanique quantique utiles à la bonne compréhension des protocoles de cryptographie présentés dans ce rapport.

Ce qui suit n'est en aucun cas un cours de mécanique quantique, mais plutôt un rappel destiné à rafraîchir la mémoire du lecteur, à préciser certaines notations et à mettre en valeur les problèmes fondamentaux intéressant notre sujet. Pour un cours de mécanique quantique, on pourra se reporter à l'ouvrage de Jean-Louis Basdevant et Jean Dalibard (éditions de l'Ecole Polytechnique [25]) ou à celui de Claude Cohen-Tannoudji, Bernard Diu et Franck Lalœ (éditions Hermann [26]).

A.1 Fonction d'onde et vecteur d'état

En mécanique quantique, il y a en général indétermination sur la position d'une particule. Celle-ci est décrite par une fonction d'onde complexe $\psi(\vec{r}, t)$, dont le module carré est la densité de probabilité de présence de la particule au point \vec{r} à l'instant t . Cela implique la relation de normalisation suivante :

$$\int |\psi(\vec{r}, t)|^2 d^3r = 1 . \quad (\text{A.1})$$

Par ailleurs, l'évolution temporelle de la fonction d'onde d'une particule placée dans un potentiel $V(\vec{r})$ est régie par l'équation de Schrödinger, qui s'écrit :

$$i\hbar \frac{\partial \psi(\vec{r}, t)}{\partial t} = -\frac{\hbar^2}{2m} \Delta \psi(\vec{r}, t) + V(\vec{r}) \psi(\vec{r}, t) . \quad (\text{A.2})$$

Cette équation est linéaire, ce qui veut dire que toute combinaison linéaire de fonctions d'ondes qui respecte la condition de normalisation est également une fonction d'onde admissible pour la particule. Ce résultat est connu sous le nom de principe de superposition. Il joue un rôle central dans la mécanique quantique en général et dans la cryptographie quantique en particulier. Nous aurons l'occasion d'y revenir un peu plus loin dans cette annexe.

Pour l'instant, contentons nous de remarquer que, d'après ce qui précède, les fonctions d'onde appartiennent à chaque instant à un espace de Hilbert (l'espace $\mathcal{L}^2(\mathbb{R}^3)$ des fonctions de carré sommable). Dans cette espace, le produit scalaire d'une fonction $\psi_1(\vec{r})$ par une fonction $\psi_2(\vec{r})$, noté $\langle \psi_2 | \psi_1 \rangle$, s'écrit :

$$\langle \psi_2 | \psi_1 \rangle = \int \psi_2^*(\vec{r}) \psi_1(\vec{r}) d^3 r . \quad (\text{A.3})$$

Par ailleurs, la description d'une particule en termes de fonction d'onde n'est pas unique : on aurait très bien pu par exemple décrire la même particule par la transformée de Fourier de $\psi(\vec{r}, t)$, notée $\phi(\vec{p}, t)$, dont le module carré représente la densité de probabilité en impulsion de la particule. Tout comme en géométrie plusieurs systèmes de coordonnées différents permettent de situer le même point dans l'espace, ces différentes fonctions décrivent en réalité le même objet $|\psi(t)\rangle$. Cet objet, appelé vecteur d'état, décrit entièrement l'état du système à un instant t .

Comme nous l'avons vu un peu plus haut, $|\psi(t)\rangle$ est élément d'un espace de Hilbert \mathcal{E}_H . On notera $\langle \psi_2 | \psi_1 \rangle$ le produit scalaire de $|\psi_1\rangle$ par $|\psi_2\rangle$ dans cet espace. La condition de normalisation s'écrit alors :

$$\| |\psi(t)\rangle \|^2 = \langle \psi(t) | \psi(t) \rangle = 1 . \quad (\text{A.4})$$

Le principe de superposition peut se reformuler de la manière suivante : si $\{|\psi_i\rangle\}_i$ est une famille de vecteurs d'états et $\{C_i\}_i$ un ensemble de nombre complexes vérifiant $\sum |C_i|^2 = 1$, alors $|\psi\rangle = \sum C_i |\psi_i\rangle$ est un vecteur d'état.

Signalons que la description d'une particule en termes de vecteurs d'états permet de prendre en compte non seulement la fonction d'onde spatiale de la particule, mais aussi ses degrés de liberté internes comme par exemple l'état de spin.

A.2 Le problème de la mesure en mécanique quantique

Dans le formalisme que nous sommes en train de décrire, qui associe à tout état de la particule un vecteur d'un espace de Hilbert \mathcal{E}_H , il convient maintenant de préciser la manière d'exploiter l'information sur la particule contenue dans ce vecteur d'état. En d'autres termes, comment peut-on prévoir le résultat de la mesure d'une grandeur physique connaissant le vecteur d'état ? Par ailleurs, on se rappelle du postulat fondamental pour la cryptographie quantique donné dans l'introduction au chapitre 1, à savoir que *toute mesure perturbe le système*. On peut se demander comment préciser de manière quantitative ce postulat afin de l'appliquer à un protocole de type BB84. C'est à ces deux questions que nous allons tenter d'apporter des éléments de réponse dans ce paragraphe.

Les principes de la mécanique quantique concernant la mesure peuvent se résumer comme suit. A chaque grandeur physique A susceptible d'être mesurée est associé un opérateur linéaire auto-adjoint \hat{A} agissant dans \mathcal{E}_H et appelé observable. Les résultats possibles de la mesure de A sont les valeurs propres de l'observable \hat{A} (notons que comme \hat{A} est auto-adjoint, ses valeurs propres sont réelles). Pour simplifier un peu la discussion, nous ferons l'hypothèse dans la suite que tous les sous espaces propres de \hat{A} sont de dimension 1 (ce cas étant le seul susceptible de

nous servir), et nous noterons $|\alpha\rangle$ un vecteur propre de \hat{A} de norme 1 associé à la valeur propre α (notons qu'il y a une infinité de choix possible pour ce vecteur propre). La probabilité de trouver la valeur α lors d'une mesure de A effectuée sur un système dans l'état $|\psi\rangle$ est alors :

$$\mathcal{P}(\alpha) = |\langle\alpha|\psi\rangle|^2 . \quad (\text{A.5})$$

De plus, juste après une mesure de A ayant donné α comme résultat, le nouvel état du système est égal à la projection (normalisée à 1) de $|\psi\rangle$ sur le sous-espace propre associé à α , qui peut s'écrire :

$$\frac{P_\alpha(|\psi\rangle)}{\|P_\alpha(|\psi\rangle)\|} = \frac{\langle\alpha|\psi\rangle|\alpha\rangle}{|\langle\alpha|\psi\rangle|} . \quad (\text{A.6})$$

Remarquons que si l'on effectue une deuxième mesure dans la foulée, on retrouve α avec une probabilité de 1, ce qui est conforme à l'intuition. Ainsi une mesure physique induit-elle une projection du vecteur d'état sur un sous-espace propre (choisi aléatoirement) de l'observable associée à la mesure. C'est en cela que l'on peut dire que la mesure perturbe l'état du système, on parle de réduction du paquet d'onde.

Le protocole BB84 exploite ce phénomène en codant l'information de telle sorte qu'Eve soit forcée environ une fois sur deux de perturber l'information lorsqu'elle la mesure (voir le chapitre 1), permettant ainsi à Alice et Bob de détecter sa présence. Nous allons étudier un peu plus loin un autre point de vue sur ce protocole, en terme cette fois de non compatibilité d'observables qui ne commutent pas. Mais avant cela, illustrons pour fixer les idées les principes que nous venons d'exposer par un exemple célèbre...

A.3 Une illustration des principes de superposition et de réduction du paquet d'onde : le "paradoxe" du chat de Schrödinger

Si on applique les postulats de la mécanique quantique à des objets macroscopiques, on tombe sur d'étranges paradoxes. Considérons par exemple un chat (cette expérience de pensée, très célèbre, est due au physicien Erwin Schrödinger) enfermé dans une boîte avec un dispositif destiné à le tuer et qui se met en marche lorsqu'il détecte la désintégration d'un atome. On suppose que l'on a introduit dans la boîte une substance peu radioactive, de telle sorte qu'en une heure, on ait une chance sur deux qu'un atome se désintègre. La mécanique quantique prédit alors que cette substance radioactive est, une fois l'heure écoulée, dans la superposition linéaire à poids égal des états {un atome s'est désintégré} et {aucun atome ne s'est désintégré}, si bien que notre chat se trouve quant-à lui dans la superposition des états {chat vivant} et {chat mort} : il est devenu quantique ! Si on ouvre la boîte pour observer le chat, on a une chance sur deux de le trouver dans l'état {chat mort} et une chance sur deux de le trouver dans l'état {chat vivant}. Par cette mesure, on réduit le paquet d'onde, ce qui veut dire que le chat reste dans cet état aux temps ultérieurs : soit on l'a tué pour de bon, soit on l'a définitivement sauvé, et ceci simplement en ouvrant la boîte !

En pratique, s'il est très facile de réaliser des superpositions linéaires d'états quantiques pour des systèmes simples (c'est ce que l'on fait avec les photons en cryptographie quantique), cela devient très difficile pour des objets macroscopiques, car la moindre interaction avec le milieu extérieur détruit cette superposition (c'est le phénomène de décohérence).

A.4 Commutation des observables, compatibilité des mesures et relation d'incertitude ; application aux observables de BB84

Les observables associées aux différentes grandeurs physiques étant des opérateurs, elles ne commutent pas forcément. Nous allons étudier dans ce chapitre les conséquences physiques de leurs relations de commutation, avant de voir comment celles-ci entrent en jeu dans la mise en œuvre du protocole BB84. On s'intéresse à la situation où un observateur tente de mesurer successivement deux grandeurs physiques différentes A et B pour un même système.

Commençons par considérer le cas où les observables \hat{A} et \hat{B} commutent. D'après le théorème de diagonalisation simultanée, leurs sous-espaces propres coïncident. Si l'observateur effectue une mesure de A et trouve comme résultat la valeur α_A , alors le vecteur d'état du système sera à l'issue de la mesure dans le sous-espace propre de \hat{A} associé à α_A . Mais on vient de voir que cet espace est aussi un sous-espace propre de \hat{B} . Soit α_B la valeur propre de \hat{B} associée à cet espace. Si l'observateur effectue une mesure de B immédiatement après celle de A, il est sûr d'obtenir comme résultat la valeur α_B . Il est donc possible dans ce cas de mesurer simultanément et avec une précision infinie les grandeurs A et B. Ces dernières sont dites compatibles.

Considérons maintenant le cas où les observables ne commutent pas. On notera $[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}$ leur commutateur. Dans ce cas, la mesure de A ayant pour résultat α_A va mettre le vecteur d'état du système dans le sous-espace propre de \hat{A} associé à α_A . Cet espace n'étant pas un sous-espace propre de \hat{B} , le vecteur d'état est une superposition linéaire d'états propres de \hat{B} . Le résultat de la mesure de B qui va suivre celle de A est donc incertain. Plus précisément, si le système est dans un état $|\psi\rangle$ avant la série de mesures, on peut montrer par un argument du type inégalité de Schwarz que les incertitudes sur les valeurs mesurées de A et B (notées respectivement Δa et Δb) vérifient la relation suivante :

$$\Delta a \Delta b \geq \frac{1}{2} |\langle \psi | [\hat{A}, \hat{B}] | \psi \rangle| . \quad (\text{A.7})$$

Dans le cas très classique des grandeurs position et impulsion (dont le commutateur des observables vaut $i\hbar$), on retrouve l'inégalité de Heisenberg $\Delta x \Delta p_x \geq \hbar/2$.

Dans le cas (moins classique!) du protocole BB84, on va tenter de définir des observables "valeur du bit dans la base a" et "valeur du bit dans la base b". Pour cela, il faut choisir une manière de coder l'information (les bits) sur leur support (les photons). On trouve souvent dans la littérature des références (plus ou moins claires) au formalisme du spin $\frac{1}{2}$, dont le lien avec les photons n'est pas si évident. En fait, la définition du spin du photon est un problème délicat. En effet, pour définir le spin d'une particule de manière classique, il faut se placer dans un repère pour lequel celle-ci est au repos, ce qui est impossible pour le photon. La théorie de la relativité, en remplaçant les rotations par les transformations de Lorentz (le lecteur intéressé pourra se reporter à André Rougé, *Introduction à la Physique Subatomique*, éditions de l'Ecole Polytechnique [27]), montre que le photon est une particule de spin 1 qui ne possède que deux états de projection de spin le long de son axe d'impulsion, $\lambda = +1$ et $\lambda = -1$. Ces deux états, appelés états d'hélicité, correspondent aux polarisations circulaires gauche $|\curvearrowleft\rangle$ et droite $|\curvearrowright\rangle$ du champ électromagnétique associé. Les états de polarisation linéaire sont des superpositions de ces états de polarisation circulaire, selon les relations :

$$\begin{cases} |x\rangle &= (|\curvearrowleft\rangle + |\curvearrowright\rangle)/\sqrt{2} \\ |y\rangle &= i(|\curvearrowright\rangle - |\curvearrowleft\rangle)/\sqrt{2} \end{cases} . \quad (\text{A.8})$$

En inversant ces relations, on peut exprimer les états de polarisation circulaire en fonction des états de polarisation linéaire comme suit :

$$\begin{cases} |\curvearrowright\rangle &= (|x\rangle + i|y\rangle)/\sqrt{2} \\ |\curvearrowleft\rangle &= (|x\rangle - i|y\rangle)/\sqrt{2} \end{cases} . \quad (\text{A.9})$$

Rappelons les conventions de codage d'Alice et Bob dans les différentes bases (voir le chapitre 1). Dans la base a (qui n'est autre que $\{|\curvearrowright\rangle, |\curvearrowleft\rangle\}$), un photon dans l'état $|\curvearrowright\rangle$ correspond au bit +1 et un photon dans l'état $|\curvearrowleft\rangle$ au bit -1 (on prend -1 et pas 0 pour simplifier l'expression des observables). Dans la base b (à savoir $\{|x\rangle, |y\rangle\}$), $|x\rangle$ correspond à +1 et $|y\rangle$ à -1. Ecrivons dans la base a les matrices des observables "valeur du bit dans la base a" et "valeur du bit dans la base b". La matrice de l'observable "valeur du bit dans la base a" est bien évidemment diagonable dans cette base et s'écrit $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. La matrice de l'observable "valeur du bit dans la base b" n'est autre que $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, car ses vecteurs propres sont $|x\rangle = (|\curvearrowright\rangle + |\curvearrowleft\rangle)/\sqrt{2}$ pour la valeur propre +1 et $|y\rangle = i(|\curvearrowright\rangle - |\curvearrowleft\rangle)/\sqrt{2}$ pour la valeur propre -1.

Ces matrices ne commutent pas (la vérification est laissée au lecteur). C'est ce qui fait que si Eve effectue sa mesure dans une base différente de celle de Bob, elle va rendre la mesure de ce dernier imprécise, ce qu'il va pouvoir détecter à coup sûr en étudiant un grand nombre d'échantillon.

Remarquons que les matrices des observables "valeur du bit dans la base a" et "valeur du bit dans la base b" sont des matrices de Pauli, qui sont utilisées entre autres pour représenter les observables σ_z et σ_x d'un spin $\frac{1}{2}$. C'est cette observation qui est souvent à l'origine de l'utilisation du formalisme du spin $\frac{1}{2}$ pour décrire le protocole BB84.

A.5 Conclusion

Au terme de cette annexe, on dispose de deux angles différents sous lesquels observer le protocole BB84. On peut tout d'abord dire qu'Eve, en mesurant la valeur d'un bit codé sur un photon, réduit le paquet d'onde, ce qui peut perturber l'information reçue par Bob. On peut également dire que Eve et Bob, lorsqu'ils choisissent des bases différentes, effectuent sur un même système deux mesures successives de grandeurs dont les observables ne commutent pas. Ils ne peuvent donc pas tous les deux connaître l'information codée sur le photon (la valeur du bit) avec une précision infinie (ce qui serait la condition d'un espionnage réussi).

Bien entendu, ces modèles ne sont que deux visions différentes du même phénomène physique.

A.6 Complément : le théorème de non clonage quantique

Supposons que Eve, lasse de toutes ces contraintes sur la mesure, décide tout simplement de dupliquer chaque photon qu'elle reçoit, afin d'en envoyer un à Bob et d'utiliser l'autre pour acquérir de l'information. Cela constituerait une menace imparable pour Alice et Bob mettant en défaut tout protocole de cryptographie quantique. Fort heureusement, on peut démontrer qu'une machine à cloner les photons n'existe pas et n'existera jamais. C'est le théorème de non clonage quantique, dû à Wootters et Zurek (1982). En effet, supposons qu'une telle machine existe. Soit $|\psi\rangle$ l'état du photon, $|b\rangle$ l'état du "photon vierge" (l'équivalent du papier blanc de la photocopieuse) et $|i\rangle$ l'état initial de la machine. Par définition, cette dernière opère la transformation suivante :

$$|\psi\rangle \otimes |b\rangle \otimes |i\rangle \longrightarrow |\psi\rangle \otimes |\psi\rangle \otimes |f_\psi\rangle , \quad (\text{A.10})$$

où $|f_\psi\rangle$ décrit l'état de la machine après la copie d'un photon dans l'état $|\psi\rangle$ (et où nous avons introduit le produit tensoriel noté *otimes* qui peut être vu en première approche comme une simple juxtaposition de vecteurs d'espaces de Hilbert différents permettant de décrire des systèmes complexes). Ainsi, si l'on considère les états intéressants le protocole BB84, on a :

$$\begin{aligned}
|\curvearrowright\rangle \otimes |b\rangle \otimes |i\rangle &\longrightarrow |\curvearrowright\rangle \otimes |\curvearrowright\rangle \otimes |f_{\curvearrowright}\rangle \\
|\curvearrowleft\rangle \otimes |b\rangle \otimes |i\rangle &\longrightarrow |\curvearrowleft\rangle \otimes |\curvearrowleft\rangle \otimes |f_{\curvearrowleft}\rangle \\
|x\rangle \otimes |b\rangle \otimes |i\rangle &\longrightarrow |x\rangle \otimes |x\rangle \otimes |f_x\rangle \\
|y\rangle \otimes |b\rangle \otimes |i\rangle &\longrightarrow |y\rangle \otimes |y\rangle \otimes |f_y\rangle .
\end{aligned} \tag{A.11}$$

Mais par linéarité, on a aussi :

$$\begin{aligned}
|x\rangle \otimes |b\rangle \otimes |i\rangle &= (|\curvearrowright\rangle + |\curvearrowleft\rangle)/\sqrt{2} \otimes |b\rangle \otimes |i\rangle \\
&\longrightarrow (|\curvearrowright\rangle \otimes |\curvearrowright\rangle \otimes |f_{\curvearrowright}\rangle + |\curvearrowleft\rangle \otimes |\curvearrowleft\rangle \otimes |f_{\curvearrowleft}\rangle)/\sqrt{2} .
\end{aligned} \tag{A.12}$$

Ce dernier état diffère de l'état copié $|x\rangle \otimes |x\rangle \otimes |f_x\rangle$ et ceci quels que soient les états $|f_\psi\rangle$, d'où l'on conclut à la non existence de la machine à cloner les photons.

Annexe B

Théorie de l'information

B.1 Entropie: mesure de l'ordre et du désordre	36
B.1.1 Entropie statistique	36
B.1.2 Entropie en théorie de l'information	37
B.1.3 Interprétation de l'entropie	37
B.2 Information: réduction de l'entropie	38
B.3 Liens entre théorie de l'information et mécanique quantique	38

B.1 Entropie: mesure de l'ordre et du désordre

La définition de l'entropie remonte à Boltzmann. L'idée était alors de définir une variable extensive qui rende compte quantitativement du désordre d'un système.

B.1.1 Entropie statistique

Dans la version « physique statistique » de l'entropie, on considère un espace des phases qui constitue un ensemble de configurations envisageables pour le système. L'argument fondateur de la physique statistique est de considérer chaque état comme une issue d'un tirage aléatoire uniforme sur l'espace des phases.

En présence de certaines contraintes, comme par exemple sur l'énergie moyenne du système, la distribution des configurations devient originale. Son ordre est mesuré par la quantité « entropie » S , sous les contraintes du modèle, qui est définie comme :

$$S = \sum_{\substack{W : \text{configuration} \\ \text{de probabilité } p}} p \ln \frac{1}{p} \quad (\text{B.1})$$

De la concavité de la fonction $p \rightarrow p \log p$ on déduit la sous-additivité de l'entropie.

La même définition, *a priori* statique, s'applique également à un système dynamique. Il suffit de considérer que l'espace des phases à une dimension supplémentaire qui représente le temps. On peut aussi invoquer l'ergodisme d'une variable aléatoire markovienne: conduire de nombreuses expériences en parallèle est équivalent à prendre la moyenne temporelle d'un seul processus sans mémoire¹.

1. C'est de cette façon que l'on arrive à retracer les différentes étapes de la vie d'une étoile, ainsi que le temps

B.1.2 Entropie en théorie de l'information

C'est donc tout naturellement que le concept d'entropie a été importé à l'étude des signaux de télécommunication. La définition (B.1) tient toujours. Par convention, l'entropie des signaux sera désignée par la lettre H au lieu de S et exprimée en base 2.

Appliquée à une communication de bits² décorrélés entre eux, on trouve l'expression de la fonction d'entropie dite binaire (tracée dans la figure B.1 :

$$H_2(p) = p \log_2 \left(\frac{1}{p} \right) + (1 - p) \log_2 \left(\frac{1}{1 - p} \right) \quad (\text{B.2})$$

puisque seuls deux événements sont susceptibles d'arriver :

1. transmission d'un bit 1, par exemple, avec une certaine probabilité p ,
2. transmission de l'autre bit, 0, avec une certaine probabilité $1 - p$ complémentaire.

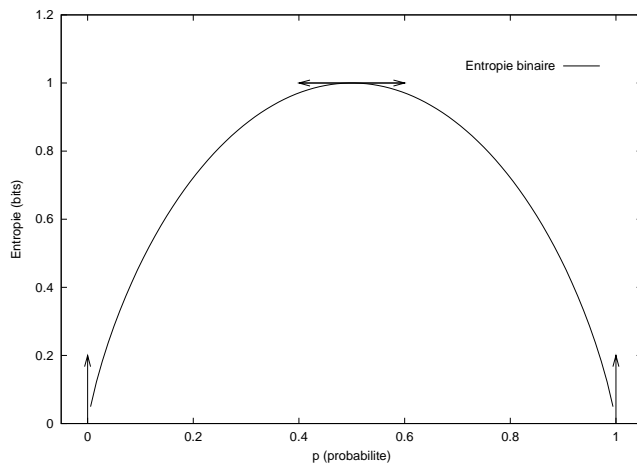


FIG. B.1 – Entropie binaire $H_2(p)$ en fonction de la part d'aléatoire p du signal.

B.1.3 Interprétation de l'entropie

Les cas limites de l'entropie binaire (B.2) s'expliquent de la façon suivante :

- $H(0) = 0$: Un événement certain ne contient pas d'information. On n'apprend rien de quelque chose de normal.
- $H(1/2) = 1$: L'entropie est maximale quand les événements sont aléatoires avec la même probabilité pour les deux issues possibles. Les surprises sont imprévisibles.

En résumé, l'entropie mesure :

- le caractère aléatoire du signal,
- son incertitude moyenne (avant mesure),
- ou l'étonnement moyen quand on le découvre (après mesure).

qu'elle passe dans chacune d'entre elles, en réalisant une étude statistique des étoiles observables. On recense par exemple de nombreuses étoiles dans la « séquence principale » mais très peu de super-géantes. Par érgodicité, on peut traduire cette observation par le fait que chaque étoile (comme notre soleil) passe le plus clair de sa vie dans la phase de la séquence principale mais que lorsqu'elle devient super-géante, les choses se passent très vite.

2. le terme bit signifie « binary digit », c'est-à-dire élément d'information binaire.

B.2 Information : réduction de l'entropie

L'information est une quantité qui mesure un bilan lors d'une communication. Après avoir reçu un message, on espère avoir gagné de l'information. Cela signifie que notre méconnaissance a été réduite. Le lien avec l'entropie est alors direct : l'information acquise après une communication, décrite par un processus stochastique, est égale à la diminution de l'entropie résultat du processus Y .

On définit donc l'information de Shannon comme :

$$I(X,Y) = \underbrace{H(X)}_{\text{Entropie initiale}} - \underbrace{H(X|Y)}_{\substack{\text{Entropie finale,} \\ \text{après communication}}} \quad (\text{B.3})$$

Dans le cas où l'entropie est *a priori* maximale (X complètement aléatoire, soit $H(X) = 1$ bit), on ne tire de l'information que de la communication. L'information apportée par le message s'exprime donc comme :

$$I(Y) = 1 - H(Y) \quad (\text{B.4})$$

B.3 Liens entre théorie de l'information et mécanique quantique

L'objectif de cette section est de définir le terme d'information quantique [9]-[5].

Comme expliqué dans la section C, les résultats des mesures quantiques sont aléatoires, ce qui permet de connecter la théorie quantique à la théorie de l'information.

Une mesure quantique qui se fait avec une probabilité d'erreur, de nature quantique, de valeur p , est porteuse d'une entropie (B.2).

On peut donc évaluer l'information engendrée par une mesure quantique grâce au formalisme présenté dans cette annexe.

Ce outil nous sert à évaluer quantitativement l'information partagée entre Alice et Bob dans le cas de la cryptologie en milieu bruité (section 2.1.2.1) ainsi que l'information que peut acquérir une espionne Eve sans qu'elle ne se fasse démasquer (section 2.1.2.2)

Annexe C

Extraire de l'information d'une mesure quantique

C.1	Dans quelle mesure peut-on distinguer deux états quantiques? . . .	39
C.2	Information codée dans deux états quantiques	39
C.2.1	Cas de deux états orthogonaux	39
C.2.2	Recouvrement : une méthode	40
C.2.3	Recouvrement : la méthode optimale	40

C.1 Dans quelle mesure peut-on distinguer deux états quantiques?

Comme exposé dans la section A.2, la mesure en mécanique quantique présente deux caractéristiques remarquables :

1. Elle donne lieu à un résultat aléatoire. On a beau connaître l'état du système avec une précision arbitrairement grande, on ne pourra jamais échapper à cet indéterminisme fondamental. La violation expérimentale d'une inégalité de Bell dans les années 1970 (voir la section 2.2.3) clôt le débat : il n'existe pas de super-théorie déterministe.
2. L'état d'un système est affecté par la mesure. Une fois l'issue de la mesure obtenue, l'état devient état propre de la grandeur mesurée. La mesure en mécanique quantique est projective.

Bien souvent, la problématique est d'obtenir une valeur moyenne de la mesure. Il suffit alors de réaliser un grand nombre d'expériences partant de conditions initiales identiques.

Nous nous intéressons ici à la détermination en un coup de l'état d'un système. Pour simplifier le problème, nous considérons un système à deux niveaux, appelé bit quantique. Pour l'application aux communications quantiques, ce cadre est adapté, vu que les informations s'échangent habituellement sous forme de bits.

On se donne deux états, que l'on peut visualiser comme deux polarisations. L'objectif est de distinguer ces deux états en commettant l'erreur la plus faible possible.

C.2 Information codée dans deux états quantiques

C.2.1 Cas de deux états orthogonaux

Commençons par constater que si les deux états sont orthogonaux, une mesure de la polarisation selon un des deux axes, disons le premier, permet de conclure sans ambiguïté. Si le résultat

est non nul (i.e. égal à 1), on a affaire à la première polarisation. Sinon, l'état est polarisé selon la deuxième direction.

La solution est facile puisque les deux états sont indépendants : ils ne se recouvrent pas.

C.2.2 Recouvrement : une méthode

Analysons la situation où les deux polarisations ont un recouvrement de $\cos \alpha$. La figure C.1 illustre la configuration.

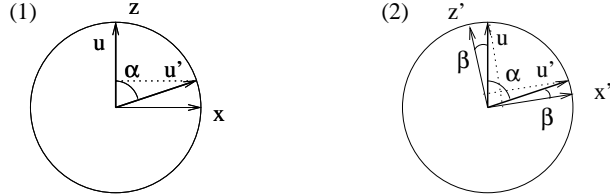


FIG. C.1 – Illustration de deux polarisations \vec{u} et \vec{u}' non-orthogonales que l'on cherche à distinguer en une mesure unique. Dans le dessin (1), la mesure est la projection le long de l'axe z . Dans le dessin (2), la mesure consiste en la projection le long d'axe z' , tel que $\{z', x'\}$ et $\{\vec{u}, \vec{u}'\}$ aient la même bissectrice. Ce deuxième cas est la meilleure mesure pour discerner les deux états.

Si l'on procède de manière analogue à celle du cas où les deux polarisation \vec{u} et \vec{u}' sont orthogonales, on peut choisir de faire une projection selon l'axe z , défini comme colinéaire à \vec{u} . Mais à ce moment-là, lorsque l'on mesure 1, on a une probabilité non nulle d'observer le deuxième état de polarisation (selon \vec{u}'), qui se projette sur l'axe z . Cette probabilité d'erreur est égale au module carré du recouvrement : $\cos^2 \alpha$. Elle survient en moyenne 1 fois sur 2, si l'on suppose que les bases sont choisies de manière équiprobables. Ainsi, avec telle mesure, on atteint un taux d'erreur de :

$$P_{\text{erreur}}^{(1)} = \frac{\cos^2 \alpha}{2} \quad (\text{C.1})$$

C.2.3 Recouvrement : la méthode optimale

Une meilleure stratégie consiste à ne pas prendre une polarisation comme axe de l'appareil de mesure, mais de couper la poire en deux. En procédant comme indiqué dans le deuxième dessin de la figure C.1, on commet des erreurs à la fois quand on mesure 0 et 1, mais globalement on gagne. On choisit donc la projection selon l'axe z' comme mesure. Les coordonnées des deux polarisations sont alors :

$$\begin{aligned} \vec{u} &= \cos \beta z' + \sin \beta x' \\ \vec{u}' &= \sin \beta z' + \cos \beta x' \end{aligned}$$

où x' complète z' pour former une base orthonormale du plan et où β est l'angle $(\frac{\pi}{2} - \alpha)/2$.

Les amplitudes de probabilité des deux types d'erreurs, à savoir :

1. Penser que l'on a \vec{u} quand la mesure donne 1 alors que l'on mesure en fait le recouvrement de \vec{u}' sur z' . L'amplitude de probabilité de cet événement est égale au produit scalaire de \vec{u}' et de z' : $\sin \beta$.
2. Penser que l'état est \vec{u}' quand on mesure 0. L'amplitude de l'erreur commise est la même que précédemment, par symétrie de la configuration.

La probabilité d'erreur, tenant compte du choix aléatoire des axes, vaut $1/2 \sin^2 \beta + 1/2 \sin^2 \beta = \sin^2 \beta$. En fonction de l'angle de recouvrement α , cette probabilité s'écrit :

$$\begin{aligned}
 P_{\text{erreur}}^{(2)} &= \sin^2 \beta \\
 &= \sin^2 \left(\frac{\pi}{2} - \frac{\alpha}{2} \right) \\
 &= \left(\frac{1}{\sqrt{2}} \cos \frac{\alpha}{2} - \frac{1}{\sqrt{2}} \sin \frac{\alpha}{2} \right)^2 \\
 &= \frac{1 - \sin \alpha}{2}
 \end{aligned} \tag{C.2}$$

Les probabilités d'erreurs (C.1) et (C.2) des deux configurations (1) et (2) de la figure C.1 sont tracées dans la figure C.2.

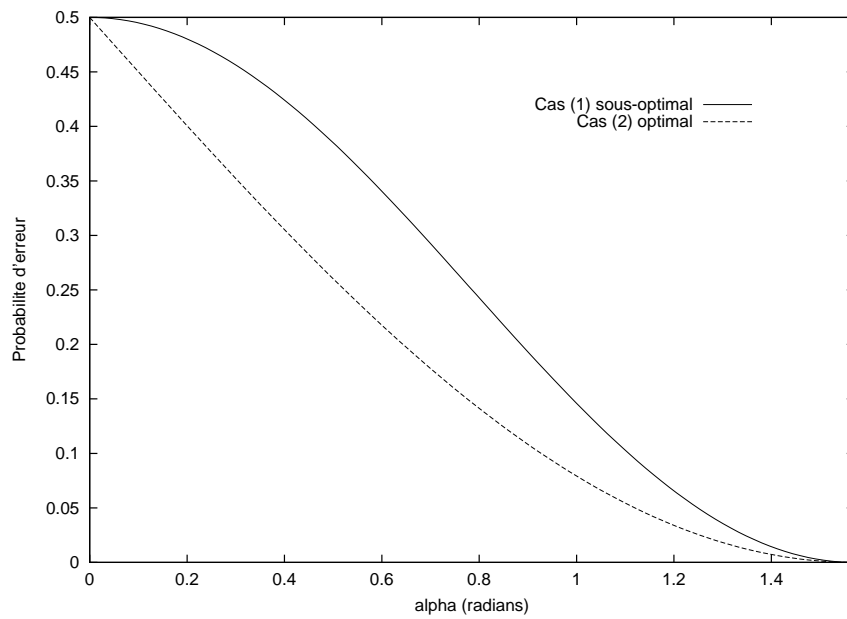


FIG. C.2 – Probabilités d'erreur des deux dispositifs de la figure C.1 pour le problème de la distinction en un coup de deux états se recouvrant de $\cos \alpha$.

On peut vérifier à titre d'exercice que le choix de la base (2) $\{z', x'\}$ conduit à la plus petite probabilité d'erreur pour la question de la distinction entre deux états de polarisation donnée.

Bibliographie

- [1] Id-Quantique, (entreprise) , information en ligne : <http://www.idquantique.com/>.
- [2] A. K. Ekert and B. Huttner, *J. Mod. Opt.* **41**, 2455 (1994).
- [3] C. A. Fuchs *et al.*, *Phys. Rev. A* **56**, 1163 (1997), disponible en ligne : <http://www.gap-optique.unige.ch/Publications/Pdf/PRA01163.pdf>.
- [4] R. B. Griffiths and C.-S. Niu, *Phys. Rev. A* **56**, (1997), disponible en ligne : <http://xxx.lanl.gov/abs/quant-ph/9702015>.
- [5] S. Haroche, (2001-2002), supports du cours de physique quantique sur le thème de l'information quantique au Collège de France. Disponibles en ligne : <http://www.lkb.ens.fr/recherche/qedcav/college/college.html>.
- [6] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev. Lett.* **47**, 777 (1935).
- [7] D. Deutsch and R. Jozsa, *Proc. R. Soc. Lond. A* **439**, 553 (1992).
- [8] P. Shor, *IEEE* **124**, (1994).
- [9] M. Nielsen and I. Chuang, Cambridge University Press (2000), numéro ISBN : 0-521-63235-8.
- [10] J. Clauser, M. Horne, A. Shimony, and R. Holt, *Phys. Rev. Lett.* **23**, 880 (1969).
- [11] A. Aspect, P. Grangier, and G. Roger, *Phys. Rev. Lett.* **49**, 91 (1982).
- [12] A. Aspect, J. Dalibard, and G. Roger, *Phys. Rev. Lett.* **49**, 1804 (1982).
- [13] A. Zeilinger, *Rev. Mod. Phys.* S288 (1999), in «More Things in Heaven and Earth, A Celebration of Physics at the Millenium», American Physical Society, B. Bederson (Ed.),.
- [14] A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, *Phys. Rev. Lett.* **69**, 1293 (1992).
- [15] J. G. Rarity and al, *Electronics Letters* (2001).
- [16] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, *J. Mod. Opt.* 2435 (1994).
- [17] T. Jennewein *et al.*, *Phys. Rev. Lett.* **84**, 4729 (2000).
- [18] D. Naik *et al.*, *Phys. Rev. Lett.* **84**, 4733 (2000).
- [19] N. Gisin and al., *Applied Phys. Lett.* **70**, 793 (1997).
- [20] N. Gisin and al, *Electron. Letters* **33**, 586 (1997).
- [21] N. Gisin and al, *Electron. Letters* **34**, 2116 (1998).
- [22] N. Gisin and al, *J. Mod. Opt.* **48**, 2009 (2001).
- [23] G. Ribordy *et al.*, *J. Mod. Opt.* **47**, 517 (2000).
- [24] P. D. Townsend, *Optical Fibre Technology* **4**, 345 (1998).
- [25] J.-L. Basdevant and J. Dalibard, Editions de l'Ecole Polytechnique (2001), numéro ISBN : 2-7302-0507-2.
- [26] C. Cohen-Tannoudji, B. Diu, and F. Laloë, Editions Hermann, collection enseignement des sciences (1998), numéro ISBN : 2-7056-6074-7.
- [27] A. Rougé, Editions de l'Ecole Polytechnique (2001), numéro ISBN : 2-7302-0495-1.