MÉMOIRE DE PREMIERE ANNÉE DE MAGISTÈRE - MAI 1993

CRYPTOGRAPHIE QUANTIQUE

Frédéric MAGNIEZ † auteur du sujet : Alain FINKEL ‡

† *ENS-Cachan ch. M464 61 av. du Pdt Wilson 94235 Cachan France, e-mail : magniez@ens-cachan.fr*
‡ *LIFAC ENS-Cachan 61 av. du Pdt Wilson 94235 Cachan France, e-mail : finkel@ens-cachan.fr*

MÉMOIRE DE PREMIERE ANNÉE DE MAGISTÈRE - MAI 1993

CRYPTOGRAPHIE QUANTIQUE

Frédéric MAGNIEZ † auteur du sujet : Alain FINKEL ‡

† *ENS-Cachan ch. M464 61 av. du Pdt Wilson 94235 Cachan France, e-mail : magniez@ens-cachan.fr*

‡ *LIFAC ENS-Cachan 61 av. du Pdt Wilson 94235 Cachan France, e-mail : finkel@ens-cachan.fr*

Résumé

Ce mémoire fait à la fois une présentation de la cryptographie quantique au lecteur et une synthèse des découvertes essentielles dans ce domaine, qui subit une expansion considérable depuis ces dernières années. Notre objectif essentiel sera de mettre en évidence des primitives s'appliquant à l'élaboration de protocoles cryptographiques et à la distribution de clefs secrètes utilisées pour le *one-time pad*[1]. Un souci d'introduction formelle et de justification des outils quantiques utilisés a été fait, néanmoins il n'est pas nécessaire de tous les assimiler pour comprendre les idées directrices de ce mémoire; le lecteur pourra donc dans une première approche passer sur le formalisme quantique le génant.

[1] ONE-TIME PAD, ou code de Vernam, inventé en 1917, est un système de codage qui utilise une clef de codage aussi longue que le message à coder que l'on ajoute terme à terme en utilisant l'addition cyclique (l'équivalent en binaire du *ou exclusif* : $\oplus$). C'est la seule méthode dont l'inviolabilité ait été prouvée sous l'hypothèse qu'une clef ne soit jamais utilisée deux fois.

Table des matières

Chapitre 1

Introduction

1.1 Présentation - Motivations

Dans les domaines se rapprochant plus ou moins de la cryptographie, on a de tous temps cherché des systèmes inviolables pour, par exemple, échanger des messages dans un secret absolu, la mise en gage d'informations, la comparaison de données sans révéler ces dernières, ou encore résoudre des problèmes se ramenant au tirage à pile ou face à distance. Hélas les solutions jusqu'alors avancées n'étaient pas mathématiquement inviolables ou supposaient des conditions initiales assez fortes, comme pour le *one-time pad* l'existence de données confidentielles, servant de clefs, entre les interlocuteurs (ce qui en pratique pose le problème de sécurité de stockage de ces données). Cependant, si on se place dans le modèle de la mécanique quantique, son principe d'incertitude donne une autre vision à ces problèmes en apportant des solutions (ou au moins de croire fortement en leur existence) quasi-idéales (en fait les attaques ont une probabilité de réussite exponentiellement faible en la complexité des protocoles (running time)), et réalisables pratiquement (à une échelle encore restreinte, mais qui ne peut que s'améliorer avec les technologies nouvelles et à venir). Dans toute la suite de ce mémoire, on supposera donc être dans un univers pour lequel le modèle de la mécanique quantique est vrai, ce qui semble acceptable comme hypothèse...

1.2 Historique

La naissance de la cryptographie quantique s'est faite dans la fin des années 60 avec Stephen Wiesner et son article "Conjucate Coding" [Wie83] qui, trop innovateur, ne fut pas publié à l'époque. Wiesner y expliquait comment le principe d'incertitude de la mécanique quantique pouvait être utilisé pour produire des données infalsifiables et pour implémenter une primitive de transfert équivoque[1]. Ce n'est qu'en 1979 que Charles H. Bennet et Gilles Brassard reprirent les travaux de Wiesner pour concevoir un système de distribution de clefs secrètes reposant sur la mécanique quantique [BBBW82]. L'article de Wiesner fut alors publié en 1983. L'un des principaux progrès fut d'utiliser les photons pour transmettre de l'information et non pour la stocker. Ce n'est cependant que vers 1991 que la cryptographie quantique ne fut plus considérée comme de la science fiction, et ce essentiellement grâce au succès du premier protocole expérimental de distribution de clefs quantiques [BBBSS90]... Depuis son développement est spectaculaire et son principe a été décrit dans la pluspart des magazines de vulgarisation comme *Scientific American* [Wal89, BBE92], *The Economist* [Got89], *New Scientist* [Deu89], *Science News* [Pet90], ou *Pour la science* [Del92].

[1] OBLIVIOUS TRANSFER, ou transfert équivoque, est une primitive permettant d'entremêler deux messages d'une façon telle qu'on ne puisse en lire qu'un, et qu'en le lisant, on rende l'autre illisible.

1.3 Résultats fondamentaux de mécanique quantique pour la suite...

1.3.1 Notions - Polarisation d'un photon

On considérera toujours des photons de même longueur d'onde.

Comme la lumière, on peut polariser des photons avec le même genre de matériel. Ainsi, on utilisera des lames (ou filtres) polarisantes et quart d'onde pour obtenir des polarisations dans une direction fixée ou circulaires... On supposera dans toute la suite des photons polarisés uniquement dans une direction fixée, par conséquent un photon sera entièrement caractérisé par son angle de polarisation.

Formellement, la mécanique quantique représente l'état interne d'un système quantique (comme la polarisation d'un photon) par un vecteur unitaire dans un espace de Hilbert. La dimension de l'espace de Hilbert dépend de la complexité du système. Chaque mesure physique pouvant être effectuée sur ce système correspond à un opérateur diagonalisant en base hilbertienne, appelé une *observable*, tel que les résultats possibles d'une mesure soient les valeurs propres de l'observable associée, et tel que l'état après une mesure soit sa projection normalisée avant mesure sur le sous-espace propre associé à la valeur propre du résultat. Le nombre de résultats possibles est donc limité par la dimension de l'espace de Hilbert.

L'espace de Hilbert d'un photon polarisé dans une direction et isolé est de dimension 2, identifié à R^2 muni du produit scalaire canonique $\langle | \rangle$. On caractérisera l'état d'un photon de polarisation θ (par rapport à l'horizontale) par le vecteur polarisation $\cos\theta|\leftrightarrow\rangle + \sin\theta|\updownarrow\rangle$ (où $(|\leftrightarrow\rangle, |\updownarrow\rangle)$ est la base canonique de R^2); on ira jusqu'à identifier un photon avec son vecteur polarisation, et on notera $|\theta\rangle$ l'état d'un photon polarisé suivant la direction θ et $\langle\theta| = |\theta\rangle^*$ (*cf.* appendice).

1.3.2 Définitions - Résultats

Pour mesurer la polarisation, θ, d'un photon, on peut le faire passer par une lame polarisante orientée de φ de laquelle il ressort (polarisé à φ) avec une probabilité de $\cos^2(\theta - \varphi)$. En fait on utilise un prisme de calcite de Wollaston orienté de φ duquel le photon ressort d'un coté (et polarisé à φ) avec une probabilité de $\cos^2(\theta - \varphi) = \langle\varphi|\theta\rangle$ ou de l'autre (et polarisé à $\varphi + \frac{\pi}{2}$) avec une probabilité de $\sin^2(\theta - \varphi) = \langle\varphi|\theta + \pi/2\rangle$.

PROPOSITION 1.1 — *Il est impossible de déterminer exactement la polarisation d'un photon sans d'autres informations supplémentaires sur ce photon. De plus, en accord avec la mécanique quantique, la méthode exposée ci-dessus est la meilleure qui puisse être pour mesurer la polarisation d'un unique photon.*

Démonstration:

Soit A l'observable associée à une certaine technique de mesure de la polarisation d'un photon. Il existe $\theta \in [0, 2\pi[$ tel que la matrice de A soit, dans la base orthonormée $(|\theta\rangle, |\theta + \pi/2\rangle)$, $diag(\alpha, \beta)$. Ceci correspond à prendre un calcite orienté de θ, et à associer le résultat α si le photon ressort polarisé à θ et β sinon. ■

DEFINITION 1.1 — *$(|\varphi\rangle, |\psi\rangle)$ est une* base *si il existe une mesure fiable permettant de dissocier les états $|\varphi\rangle$ et $|\psi\rangle$. On parlera de mesure dans la base $(|\varphi\rangle, |\psi\rangle)$ et on notera $\psi = \varphi^\perp$.*

Remarque : Si θ est un angle, alors $(|\theta\rangle, |\theta + \pi/2\rangle)$ est une base. Il suffit de considérer comme mesure celle du calcite orienté de θ.

DEFINITION 1.2 — *Soient $(|\varphi\rangle, |\varphi^\perp\rangle)$, $(|\psi\rangle, |\psi^\perp\rangle)$ deux bases. On dira qu'elles sont* conjuguées *si pour un photon dans $\{|\varphi\rangle, |\varphi^\perp\rangle\}$ (resp. $\{|\psi\rangle, |\psi^\perp\rangle\}$) une mesure dans la base $(|\psi\rangle, |\psi^\perp\rangle)$ (resp. $(|\varphi\rangle, |\varphi^\perp\rangle)$) est complètement aléatoire et entraîne la perte de toute information.*

Notations : On notera certains états de polarisation comme suit :

- polarisation horizontale définie par le vecteur $|\leftrightarrow\rangle$.
- polarisation verticale définie par le vecteur $|\updownarrow\rangle$.
- polarisation à $\frac{\pi}{4}$ définie par le vecteur $|\swarrow\!\!\!\!\!\nearrow\rangle$.
- polarisation à $\frac{3\pi}{4}$ définie par le vecteur $|\nwarrow\!\!\!\!\!\searrow\rangle$.
- polarisation à $\frac{\pi}{8}$ définie par le vecteur $|\mathcal{B}\rangle$. La base $(|\mathcal{B}\rangle, |\mathcal{B}^{\perp}\rangle)$ est appelée base de Breidbart. On notera par commodité $\kappa = \cos(\pi/8)$ (rq : $\kappa^2 \approx 85\%$).

On notera aussi les bases associées $\oplus = (|\leftrightarrow\rangle, |\updownarrow\rangle)$ et $\boxtimes = (|\swarrow\!\!\!\!\!\nearrow\rangle, |\nwarrow\!\!\!\!\!\searrow\rangle)$.

PROPOSITION 1.2 — *Les bases $\oplus$ et $\boxtimes$ sont conjuguées.*

1.3.3 Clônage d'un état quantique

THEOREME 1.1 (WOOTTERS-ZUREK [WZ82]) — *On ne peut pas clôner "directement" (sans faire de mesure) un état quantique.*

Démonstration:
On donne ici une démonstration simplifiée en oubliant quelques problèmes de formalisme... Soient $|\varphi\rangle, |\psi\rangle$ des états quantiques normés et U un opérateur unitaire de clônage de $(\mathcal{E}, \langle | \rangle)$.

On a donc :

$$U|\varphi\rangle = |\varphi\rangle|\varphi\rangle \quad : \text{vecteur de } \mathcal{E} \otimes \mathcal{E}$$
$$U|\psi\rangle = |\psi\rangle|\psi\rangle$$

D'où en faisant le produit scalaire des deux expressions et en utilisant le fait que U est unitaire on a :

$$\langle\varphi|\psi\rangle = \langle\varphi|\psi\rangle^2$$

Ce qui est absurde d'après l'inégalité de Schwarz si $|\varphi\rangle$ et $|\psi\rangle$ sont ni égaux, ni orthogonaux. ■

1.3.4 Le paradoxe d'E.P.R.

On pourra consulter pour plus d'informations [EPR35], voici néanmoins une première approche de ce paradoxe...

Il s'agit de l'existence de photons émergeant d'un même point (provenant de la désexcitation d'un atome), fuyant dans deux directions opposées, et surtout étant *corrélés*, c'est-à-dire qu'après toute mesure dans une certaine base de l'un des deux photons, la mesure de l'autre photon dans la même base donnera toujours le même résultat...

On pourrait donc croire que l'information du résultat de la première mesure se propage instantanément (*i.e.* plus vite que la lumière). Or le résultat de la première mesure est aléatoire, donc on ne transmet pas une information voulue mais aléatoire, ce qui n'est pas en contradiction avec les fondements de la mécanique quantique!

On appellera une telle paire de photons corrélés des photons EPR, qui servirons dans la suite pour envisager certaines attaques des participants...

1.4 Le one-time pad (version binaire)

ALGORITHME 1.1 — *(codage(A, B))*

- *message binaire à coder* $A = a_1 a_2 \dots a_n$.
- *clef binaire de codage* $B = b_1 b_2 \dots b_n$.
- *renvoyer le message codé* $C = c_1 c_2 \dots c_n$ *avec* $\forall i \in \{1, 2, \dots, n\}, c_i = a_i \oplus b_i$.

ALGORITHME 1.2 — *(décodage(C, B))*

- *message binaire codé* $C = c_1 c_2 \dots c_n$.
- *clef binaire associée* $B = b_1 b_2 \dots b_n$.
- *renvoyer le message décodé* $A = a_1 a_2 \dots a_n$ *avec* $\forall i \in \{1, 2, \dots, n\}, a_i = c_i \oplus b_i$.

PROPOSITION 1.3 — *Dans le* one-time pad*, si la clef est aussi longue que le message à coder et si elle n'est utilisée qu'une seule fois, alors il est impossible de décoder le message sans connaître la clef.*

Démonstration:
Il suffit de remarquer que $B \mapsto$ *décodage*(B, C) est une bijection de $\{0, 1\}^n$, par conséquent, sans aucune information sur la clef de codage, il est impossible de décoder un message utilisant le *one-time pad*. ∎

Remarques :

1. L'inconvénient du *one-time pad* est qu'Alice et Bob doivent avoir chacun une copie de la clef secrète, et que cette copie est longue si l'on veut transmettre de longs messages... De plus, il faut pouvoir la garder secrète jusqu'au moment de son utilisation.
2. Son avantage réside dans le fait que la clef en elle même peut être quelconque, on peut donc remplacer le problême de transmission d'un message binaire secret *fixé* de longueur n en la distribution d'une clef *quelconque* de longueur n, ce que l'on va pouvoir faire grâce au principe d'incertitude de la mécanique quantique... Il suffira ensuite de transmettre par un canal infalsifiable *codage(message,clef)*, qui ne donne aucune information sur *message* si *clef* n'est pas révélée.
3. Pour simplifier, on notera *codage*(A, B)=*décodage*(A, B)=$A \oplus B$.

1.5 Le transfert quantique

Méthode

On suppose l'existence de canaux permettant le transit de photons sans interférences internes, mais ne garantissant pas leur sécurité vis-à-vis d'une éventuelle "écoute" de la ligne...

Alice envoie (et on suppose cela possible) à Bob un *unique* photon polarisé d'un angle θ fixé et connu d'Alice uniquement.

A la réception de ce photon, Bob lit l'information du photon, qui est sa polarisation, en le faisant passer dans un prisme de calcite de Wollaston orienté de φ. Bob considère avoir reçu le bit 0 si le photon ressort dans la direction de polarisation φ et 1 sinon.

Protocole

<u>PROTOCOLE</u> 1.1 — *(Quantum Transfert)*

– *Alice envoie à Bob un photon* $|\theta\rangle$.

– *Bob mesure le photon reçu dans une base* $(|\varphi\rangle, |\varphi^\perp\rangle)$.

– *Bob fixe le bit* $x \leftarrow \begin{cases} 0 & \textit{si la mesure donne } \varphi \\ 1 & \textit{sinon} \end{cases}$.

Modélisation

Tout se passe comme s'il éxistait une machine QT régissant les communications entre Alice et Bob de la manière suivante :

– Alice envoie un angle θ à QT.

– Bob envoie un angle φ à QT.

– QT envoie le bit x à Bob tel que $\Pr(x = 0) = \cos^2(\theta - \varphi)$.

<u>PROPOSITION</u> 1.4 — *QT est inviolable i.e. :*

– *Bob n'apprend rien sur* θ.

– *Alice n'apprend rien sur* φ *et* x.

Démonstration:

– D'après la proposition 1.1 Bob a le maximum d'informations en suivant le protocole, *i.e.* la variable x représente le maximum d'informations sur θ. Avant mesure, Bob n'a aucune information sur θ donc pour lui

$$\Pr(x = 0) = \int_0^{2\pi} \cos^2(\theta - \varphi)\, d\theta = \frac{1}{2} = \Pr(x = 1)$$

Donc le résultat est complètement aléatoire, donc aucune information n'est transmise.

– Citons le lemme suivant, que nous admettrons, et dont nous nous servirons dans le reste du mémoire.

<u>LEMME</u> 1.1 — *Le maximum d'informations qu'Alice peut avoir sur ce qu'advient un photon émis, qu'elle ne peut plus observer directement, est son photon corrélé dans une paire EPR.*

Alice pourrait donc stocker le photon corrélé à celui émis jusqu'à ce que Bob le mesure. Mais on se trouve alors dans la situation inverse : tout ce passe comme si Bob avait envoyé à Alice un photon de polarisation φ, qu'Alice ignore; la seule chose qu'elle peut faire étant de mesurer le photon gardé pour un θ choisi quelconque!

∎

Chapitre 2

Protocoles cryptographiques

2.1 Présentation

Deux participants (appelés *Alice* et *Bob*), qui ne se font pas confiance, veulent effectuer des tâches utilisant des informations secrètes provenant des deux parties, et ce sans pour autant se les révéler mutuellement. On modèlisera les participants par des machines de Turing probabilistes mais pas forcément bornées polynômialement par le temps, contrairement à ce qu'on fait généralement dans ce genre de situation. On aura donc en fait des preuves de sécurité même si $\mathcal{P} = \mathcal{NP}$, ce qui n'est pas habituellement le cas.

Nous allons donc expliciter des primitives cryptographiques fondamentales qui permettent d'établir de nombreux protocoles cryptographiques plus élaborés : *mise en gage d'un bit (bit commitment scheme)*$^{(1)}$, *transfert équivoque (oblivious transfer (OT))*$^{(2)}$, *transfert inconscient (one-out-of-two oblivious tansfer ($\binom{2}{1}$ -OT)).*

Exemples d'applications de ces primitives :

– (1) $\longrightarrow$ tirage à pile ou face à distance (coin tossing protocols).

– (1) $\longrightarrow$ preuve à divulgation nulle (zero-knowledge proofs): Alice veut prouver la validité d'un prédicat à Bob sans lui révéler d'informations sur le fait que le prédicat est juste.

– (2) $\longrightarrow$ Evaluation de fonctions avec sécurité des données des participants (secure two party computation) : On considère une fonction $(x, y) \mapsto f(x, y)$ à deux paramètres et calculable en un temps polynômial. Alice connait x et Bob y. On veut établir un protocole entre Alice et Bob leur permettant d'évaluer $f(x, y)$ sans révéler d'informations autre que $f(x, y)$ aux participants.

Signalons que nous allons travailler sur des bits, mais que l'implémentation sur des entiers quelconques et donc sur n'importe quel alphabet fini ne pose aucun problème. Enfin, le lecteur trouvera une vaste littérature sur les applications de ces primitives dont il trouvera une bibliographie représentative dans [Cré93].

2.2 Mise en gage d'un bit

2.2.1 Définition

DEFINITION 2.1 — *On dit qu'Alice met en gage un bit x à Bob quand Alice donne une représentation de x à Bob telle que :*

- *Bob ne peut en tirer aucune information sur x.*
- *Alice peut à tout moment révéler x avec preuve de sa bonne foi.*

Les conditions de mise en gage sont :
– la sécurité d'une Alice honnête face à un Bob malhonnête.
– la sécurité d'un Bob honnête face à une Alice malhonnête.

En effet, on ne cherche qu'à garantir les gens honnêtes face à des gens malhonnêtes, si tout le monde est malhonnête l'intérêt est nul. En fait on garantit la sécurité d'un participant s'il suit le protocole à la lettre. Il en sera de même pour les autres parties de ce chapitre...

Remarque : En fait, on montrera que les chances de réussites d'attaques des participants sont exponentiellement faibles en la complexité des protocoles.

2.2.2 Une version simplifiée

Nous proposons ici une des premières mises en gage quantiques explicitée par Bennett et Brassard dans [BB84].

Voici tout d'abord la première partie du protocole qui permet à Alice de mettre en gage un bit x à Bob; n est un entier très grand fixé. On notera $[a_0, a_1, \ldots, a_n]_i = a_i$.

PROTOCOLE 2.1 — *BB-commit(x)*

1. *Alice choisit aléatoirement un vecteur de* n *bits* $C \leftarrow (c_1, c_2, \ldots, c_n)$.
2. *Bob choisit aléatoirement un vecteur de* n *bits* $B' \leftarrow (b'_1, b'_2, \ldots, b'_n)$.
3. *Alice choisit sa base de polarisation* $(|\varphi\rangle, |\varphi^\perp\rangle) \leftarrow [\oplus, \boxtimes]_x$.
4. $\underset{i=1}{\overset{n}{DO}}$:
   - *Alice envoie un photon* π_i *de polarisation* $[|\varphi\rangle, |\varphi^\perp\rangle]_{c_i}$ *à Bob.*
   - *Bob mesure le photon* π_i *reçu dans la base* $(|\varphi'_i\rangle, |\varphi'^\perp_i\rangle) \leftarrow [\oplus, \boxtimes]_{b'_i}$.
   - *Bob fixe* $c'_i \leftarrow \begin{cases} 0 & \textit{si la mesure donne } \varphi'_i \\ 1 & \textit{sinon} \end{cases}$.
5. *Bob établie* $C' \leftarrow (c'_1, c'_2, \ldots, c'_n)$.

PROPOSITION 2.1 — *BB-commit a une complexité en* n.

THEOREME 2.1 — *Si Alice est honnête, Bob ne peut pas estimer la valeur de* x, *i.e.* $\Pr(x = 0 \mid C') = \Pr(x = 1 \mid C') = \frac{1}{2}$.

Démonstration:

Nous allons exposer deux démonstrations, la première, plus concrète, n'utilise pas beaucoup d'outils, la deuxième, plus élégante, utilise les matrices densités (*cf.* appendice). J'ai tenu à faire la démonstration de ce théorème en détails, que je n'ai trouvée nulle part, car je pense que sa compréhension permet de mieux assimiler celles qui suivent.

1. Bob ne peut que mesurer les photons arrivants : le fait de les conserver ne lui apporterait rien, de plus il ne peut pas les clôner. Ne supposons pas les $|\varphi_i\rangle_i$ dans $\{|\leftrightarrow\rangle, |\updownarrow\rangle, |\nearrow\rangle, |\nwarrow\rangle\}$, mais dans $\{|\theta\rangle; \theta \in [0, 2\pi[\}$. Avec ce modèle nous traitons toutes les attitudes possibles de Bob. Les seules informations qu'il peut tirer sont donc contenues dans C'.

   On suppose x fixé. Si $\Pr(c_i = 0) = \Pr(c_i = 1) = \frac{1}{2}$ alors :

$$\Pr(c'_i = 0) = \frac{\cos^2(\psi_i - \varphi) + \cos^2(\psi_i - \varphi^\perp)}{2} = \frac{1}{2} = \Pr(c'_i = 1)$$

Donc la i-ème mesure donne un résultat aléatoire pour Bob. Donc la valeur de x n'influe en rien la valeur de C'. Donc si on appelle ${C'}_0$ la valeur de la variable C', on a :

$$\Pr(C' = {C'}_0 \mid x = 0) = \Pr(C' = {C'}_0 \mid x = 1)$$

donc en utilisant la formule de Bayes on a :

$$\begin{aligned}
\Pr(x = 0 \mid C' = {C'}_0) &= \frac{\Pr(C' = {C'}_0 \mid x = 0) \times \Pr(x = 0)}{\Pr(C' = {C'}_0 \mid x = 0) \times \Pr(x = 0) + \Pr(C' = {C'}_0 \mid x = 1) \times \Pr(x = 1)} \\
&= \frac{1}{2} \\
&= \Pr(x = 1 \mid C' = {C'}_0)
\end{aligned}$$

2. Soit ρ_0 la matrice densité décrivant le mélange statistique des états envoyés à Bob pour représenter $x = 0$ à l'étape 4 du protocole BB-commit:

$$\rho_0 = \bigotimes_{i=1}^{n} \left(\frac{1}{2} |\leftrightarrow\rangle\langle\leftrightarrow| + \frac{1}{2} |\updownarrow\rangle\langle\updownarrow| \right) = \bigotimes_{i=1}^{n} \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$

et pour $x = 1$:

$$\rho_1 = \bigotimes_{i=1}^{n} \left(\frac{1}{2} |⤢\rangle\langle⤢| + \frac{1}{2} |⤡\rangle\langle⤡| \right) = \rho_0$$

On constate que la matrice obtenue pour BB-commit(0) coïncide à celle obtenue pour BB-commit(1). Un théorème de mécanique quantique dit que deux mélanges qui ont les mêmes matrices densités ne peuvent être distingués par aucune mesure quantique (*cf.* théorème 5.2).

■

Voici maintenant la deuxième partie du protocole qui permet à Alice de révéler x à Bob:

<u>Protocole</u> 2.2 — *BB-unveil(x, C, B', C')*

1. *Alice révèle x et C à Bob.*
2. *Bob accepte si le prédicat $[\forall i \in \{1, 2, \ldots, n\}, [({b'}_i = x) \Rightarrow ({c'}_i = c_i)]]$ est vrai et refuse sinon.*

<u>Proposition</u> 2.2 — *BB-unveil a une complexité en n.*

Remarque : Si Alice est honnête et s'il n'y a pas d'erreurs de transmission, alors Bob acceptera toujours dans le protocole ci-dessus.

Exemple :

1.	⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕	⤡	⤢	⤢	↕
2.	⊕	⊠	⊠	⊕	⊕	⊠	⊠	⊕	⊠	⊕	⊠	⊠	⊠	⊠	⊕
3.	↕	⤢	⤡	↔	↕	⤢	⤢	↔	⤡	↕	⤡	⤡	⤢	⤢	↕
4.	?	?	√	√	√	?	?	√	√	?	?	√	√	√	√

1. Alice envoie à Bob une suite aléatoire de photons polarisés horizontalement (↔), verticalement (↕), à $\pi/4$ (⤢) ou à $3\pi/4$ (⤡).
2. Bob mesure la polarisation de chacun de ces photons aléatoirement, soit de façon rectiligne (⊕), soit de façon diagonale (⊠).

3. Résultat des mesures de Bob.

4. Alice révèle à Bob les bases et polarisations de chacun des photons envoyés. Bob teste alors, quand il avait fait le bon choix de base, s'il a la même polarisation que celle que lui a annoncée Alice. Si les tests sont concluants, Bob accepte.

On suppose Bob honnête mais Alice malhonnête, *i.e.* Alice veut être libre de révéler à sa guise 0 ou 1 (sans avoir à tenir compte de sa mise en gage). Quelles sont les chances de réussite d'Alice?

Modélisation d'une stratégie d'attaque pour Alice

On suppose qu'Alice envoie des photons π_i de polarisation intrinsèque $\varphi_i \in [0, 2\pi[$, et que pour révéler $x \in \{0,1\}$, Alice utilise le vecteur C^x dans BB-unveil.

On dira que la stratégie est *réussie* quand :

$$\forall i \in \{1,2,\ldots,n\}, \left[(b'_i = 0) \Rightarrow (c'_i = c_i^0)\right] \wedge \left[(b'_i = 1) \Rightarrow (c'_i = c_i^1)\right]$$

$$i.e. \text{ quand } \quad \forall i \in \{1,2,\ldots,n\}, c'_i = c_i^{b'_i}$$

<u>Theoreme</u> 2.2 — *Dans ce modèle, si Bob est honnête,* $\Pr($*stratégie réussie*$) \leq \kappa^{2n}$.

Démonstration:

Je me suis encore attaché ici à faire avec une démonstration propre dans ce cas simple car les mêmes méthodes seront réutilisées utltérieurement.

Traçons le tableau des probabilités de validité du prédicat $\left[c'_i = c_i^{b'_i}\right]$:

$\Pr(c'_i = c_i^{b'_i})$	$c_i^{b'_i} = 0$	$c_i^{b'_i} = 1$
$b'_i = 0$	$\cos^2 \varphi_i$	$\cos^2(\varphi_i - \pi/2)$
$b'_i = 1$	$\cos^2(\varphi_i - \pi/4)$	$\cos^2(\varphi_i - 3\pi/4)$

D'où une stratégie optimale :

- $c_i^0 = c_i^1 = 0$: Pour ne privilégier ni $x = 0$ ni $x = 1$, *i.e.* ni $b'_i = 0$ ni $b'_i = 1$ on prend $\varphi_i = \pi/8$.
- $c_i^0 = c_i^1 = 1 \longrightarrow \varphi_i = 5\pi/8$.
- $c_i^0 = \overline{c_i^1} \longrightarrow \varphi_i = 3\pi/8$.

Dans tous les cas on a donc : $\Pr(c'_i = c_i^{b'_i}) = \kappa^2 (= \cos^2(\pi/8))$. Donc la stratégie optimale est réussie avec une probabilité P:

$$P = \prod_{i=1}^{n} \Pr(c'_i = c_i^{b'_i}) = \kappa^{2n}$$

■

Une attaque possible d'Alice : l'attaque EPR

Supposons qu'Alice utilise des paires de photons EPR. Alice n'a qu'à suivre le protocole suivant pour avoir une stratégie réussie :

PROTOCOLE 2.3 — *BB-commit'*

1. *Alice choisit aléatoirement un vecteur de n bits $C \leftarrow (c_1, c_2, \ldots, c_n)$.*
2. *Bob choisit aléatoirement un vecteur de n bits $B' \leftarrow (b'_1, b'_2, \ldots, b'_n)$.*
3. $\overset{n}{\underset{i=1}{DO}}$:
   - *Alice produit une paire de photons EPR (π_i, π'_i) et envoie π_i à Bob tout en stoquant π'_i.*
   - *Bob mesure le photon π_i reçu dans la base $(|\varphi'_i\rangle, |\varphi'^{\perp}_i\rangle) \leftarrow [\oplus, \boxtimes]_{b'_i}$.*
   - *Bob fixe $c'_i \leftarrow \begin{cases} 0 & \text{si la mesure donne } \varphi'_i \\ 1 & \text{sinon} \end{cases}$.*
4. *Bob établie $C' \leftarrow (c'_1, c'_2, \ldots, c'_n)$.*

Lorsqu'Alice désire révéler $x \in \{0, 1\}$ de son choix à Bob, elle fait :

- Alice choisit sa base de polarisation $(|\varphi\rangle, |\varphi^{\perp}\rangle) \leftarrow [\oplus, \boxtimes]_x$
- $\overset{n}{\underset{i=1}{DO}}$:
  - Alice mesure le photon π'_i dans la base $(|\varphi\rangle, |\varphi^{\perp}\rangle)$.
  - Alice fixe $c_i \leftarrow \begin{cases} 0 & \text{si la mesure donne } \varphi_i \\ 1 & \text{sinon} \end{cases}$.
- Alice établie $C \leftarrow (c_1, c_2, \ldots, c_n)$.

Puis il suffit à Alice d'effectuer BB-unveil(x) avec Bob.

Remarque :

- Actuellement, le stoquage de photons est impossible sauf durant des temps très courts, donc cette attaque est irréalisable. Donc pratiquement, ce protocole est incassable des deux parties; néanmoins d'un point de vue théorique, il est important de trouver un protocole parfaitement incassable.
- Une solution pour lutter contre l'attaque EPR serait donc d'imposer une condition aux polarisations des photons envoyés pour forcer Alice à les polariser effectivement (*i.e.* d'avoir un unique état intrinsèque pour chaque photon envoyé). Une telle solution sera mise en évidence dans les protocoles qui suivent.

Bilan

THEOREME 2.3 *En théorie, la mise en gage de [BB84] est inviolable par Bob et est violable par Alice si et seulement si Alice peut générer des paires EPR et stocker des photons.*

Démonstration:
Il suffit de constater qu'après avoir envoyé les photons π_i, la seule trace qu'Alice peut en garder est leurs éventuels photons corrélés dans des paires EPR, et de rassembler ce qui précède.
■

Autres problèmes

Outre le problème théorique de l'attaque EPR, il y a des problèmes pratiques. On peut en éliminer certains facilement, d'autres non. Pour commencer, il n'est pas raisonnable de faire dans BB-unveil : $[\forall i \in \{1, 2, \ldots, n\}, [(b'_i = b) \Rightarrow (c_i = c'_i)]]$. En effet, les erreurs de transmission ne peuvent être absentes en pratique, d'autant plus que les appareils utilisés sont très sensibles (*cf.* paragraphe 3.2.3). On a constaté dans l'appareil actuel utilisé pour la distribution de clefs quantiques [BBBSS90] qu'il était raisonnable d'espérer 4% d'erreurs. Il faut donc mettre à la place dans BB-unveil $[\forall i \in \{1, 2, \ldots, n\}, [(b'_i = b) \Rightarrow_{90\%} (c'_i = c_i)]]$. Le seul prix à payer étant que le paramètre n, qui sécurise le protocole, doit être choisi plus grand pour atteindre la même infime probabilité de réussite de tricherie.

L'autre problème pratique est beaucoup plus sérieux : il est très difficile d'envoyer en pratique dans BB-commit des photons isolés. Il est beaucoup plus facile d'envoyer de faibles impulsions de photons polarisés comme dans l'appareil expérimental de distribution de clefs. Malheureusement, celles-ci contiennent parfois plus d'un photon, et tous les photons d'une même impulsion ont la même polarisation, et ceci est contraignant : quand Bob lit une impulsion qui contient plus d'un photon dans la base $(|\varphi\rangle, |\varphi^\perp\rangle)$, si Bob détecte des photons dans les deux directions du calcite alors l'impulsion est polarisée dans la base conjuguée à $(|\varphi\rangle, |\varphi^\perp\rangle)$ dans l'ensemble $\{⊕, ⊠\}$, sinon l'impulsion est polarisée dans la base $(|\varphi\rangle, |\varphi^\perp\rangle)$; donc dans les deux cas Bob découvre la valeur de x. Il n'y a pas de solutions à ce problème avec cette mise en gage, cependant le protocole qui suit restera fiable lorsqu'il n'y aura qu'un petit nombre de multiphotons émis.

2.2.3 Une version un peu plus évoluée

Cette version, tirée de [BC91], présente l'avantage de résister à l'attaque EPR et de rester fiable en présence de multiphotons.

PROTOCOLE 2.4 — *BC-commit(x)*

1. *Alice choisit aléatoirement une matrice booléenne $n \times n$ $C = (c_{i,j})$ telle que*

$$\forall i \in \{1, 2, \ldots, n\}, \bigoplus_{j=1}^{n} c_{i,j} = x$$

2. *Alice choisit aléatoirement une matrice booléenne $n \times n$ $B = (b_{i,j})$.*
3. *Bob choisit aléatoirement une matrice booléenne $n \times n$ $B' = (b'_{i,j})$.*
4. $\underset{i=1}{\overset{n}{DO}}\ \underset{j=1}{\overset{n}{DO}}$:
   - *Alice fixe la base $(|\varphi_{i,j}\rangle, |\varphi^\perp_{i,j}\rangle) \leftarrow [⊕, ⊠]_{b_{i,j}}$*
   - *Alice envoie un photon $\pi_{i,j}$ de polarisation $[|\varphi_{i,j}\rangle, |\varphi^\perp_{i,j}\rangle]_{c_{i,j}}$ à Bob.*
   - *Bob mesure le photon $\pi_{i,j}$ reçu dans la base $(|\varphi'_{ij}\rangle, |\varphi'^\perp_{ij}\rangle) \leftarrow [⊕, ⊠]_{b'_{i,j}}$.*
   - *Bob fixe $c'_{i,j} \leftarrow \begin{cases} 0 & \text{si la mesure donne } \varphi'_{i,j} \\ 1 & \text{sinon} \end{cases}$.*

PROPOSITION 2.3 — *BC-commit a une complexité en n^2.*

PROPOSITION 2.4 — *Si les deux participants sont honnêtes on a : $\Pr(c'_{i,j} = c_{i,j}) = \frac{3}{4}$.*

LEMME 2.1 — *Si Alice est honnête, Bob ne peut obtenir plus d'informations sur x que lire séparément chaque photon π_i reçu dans la base $(|\mathcal{B}\rangle, |\mathcal{B}^\perp\rangle)$.*

Démonstration:

Cette démonstration est très proche de celle du lemme 2.2, nous la ferons donc seulement à ce moment. Disons seulement que la démonstration utilise un deuxième protocole, qui révèle autant d'informations que celui-ci (preuve par les matrices densités), pour lequel le maximum d'informations est évidemment obtenu par la lecture séparée de chaque photon π_i reçu dans la base $(|\mathcal{B}\rangle, |\mathcal{B}^\perp\rangle)$. ■

THEOREME 2.4 — *Si Alice est honnête, il existe une constante $\alpha \in [0,1[$ telle que :*

$$\frac{1}{2} - \alpha^n \leq \left\{ \begin{array}{c} \Pr(x = 0 \mid C') \\ \Pr(x = 1 \mid C') \end{array} \right\} \leq \frac{1}{2} + \alpha^n$$

PROTOCOLE 2.5 — *BC-unveil(x, B, C, B', C')*

1. *Alice révèle x, B et C à Bob.*
2. *Bob accepte si*

$$\left\{ \begin{array}{l} \forall i \in \{1, 2, \ldots, n\}, \bigoplus_{j=1}^{n} c_{i,j} = x. \\ \forall (i,j) \in \{1, 2, \ldots, n\}^2, [(b'_{i,j} = b_{i,j}) \Rightarrow (c'_{i,j} = c_{i,j})]. \end{array} \right.$$

et refuse sinon.

PROPOSITION 2.5 — *BC-unveil a une complexité en n.*

Modélisation d'une stratégie d'attaque pour Alice

On suppose qu'Alice envoie des photons $\pi_{i,j}$ de polarisation intrinsèque $\varphi_{i,j} \in [0, 2\pi[$, et que pour révéler $x \in \{0,1\}$, Alice utilise les vecteurs B^x et C^x dans BC-unveil.

On dira que la stratégie est *réussie* quand :

$$\forall i \in \{1, 2, \ldots, n\}, \left[\bigoplus_{j=1}^{n} c^0_{i,j} = 0 \right] \bigwedge \left[\bigoplus_{j=1}^{n} c^1_{i,j} = 1 \right] \quad (2.1)$$

$$\text{et } \forall (i,j) \in \{1, 2, \ldots, n\}^2, \left[(b'_{i,j} = b^0_{i,j}) \Rightarrow (c'_{i,j} = c^0_{i,j})\right] \wedge \left[(b'_{i,j} = b^1_{i,j}) \Rightarrow (c'_{i,j} = c^1_{i,j})\right] \quad (2.2)$$

THEOREME 2.5 — *Dans ce modèle, si Bob est honnête,* $\Pr($*stratégie réussie*$) \leq \kappa^{2n}$.

Démonstration:

Tout d'abord, notons que le prédicat 2.1 implique que C^0 et C^1 diffèrent au moins d'une composante par ligne. Donc il y a au moins n bits différents dans ces deux matrices. Soit (i,j) tel que $c^0_{i,j} \neq c^1_{i,j}$. Deux cas se présentent :

1. $b^0_{i,j} = b^1_{i,j} = b$. Quand $b'_{i,j} = b$, le prédicat 2.2 n'est pas satisfait pour (i,j), sinon il l'est. Or $\Pr(b'_{i,j} = b) = \frac{1}{2}$, donc quelque soit le choix de $\varphi_{i,j}$, $\Pr(2.2 \text{ vrai pour } (i,j)) = \frac{1}{2}$.

2. $b^0_{i,j} = \overline{b^1_{i,j}}$. Donc une des deux égalitéd du prédicat 2.2 pour (i,j) sera à vérifier. Pour augmenter ses chances de réussite de vérifier 2.2 pour (i,j), Alice envoie un photon de polarisation $\varphi_{i,j}$ qui doit augmenter simultanément ses chances de réussite si $b'_{i,j} = 0$ ou $b'_{i,j} = 1$. On en déduit donc comme dans l'étude similaire au 2.2.2, qu'il y a deux sous cas :

   (a) $b^0_{i,j} = \overline{c^0_{i,j}} \Rightarrow \varphi_{i,j} = \frac{7\pi}{8}$.

   (b) $b^0_{i,j} = c^0_{i,j} \Rightarrow \varphi_{i,j} = \frac{\pi}{8}$.

   Ce qui entraine dans les deux cas $\Pr(2.2 \text{ vrai pour } (i,j)) = \kappa^2$.

Nous avons vu qu'il y avait au moins n paires (i,j) telles que $c^0_{i,j} \neq c^1_{i,j}$, on peut donc conclure.

■

Remarque : Quelques soient les photons envoyés, ils ont intérêt à être comme dans le cas idéal de la demonstration précédente pour augmenter les chances d'Alice, donc en particulier d'être polarisés de façon intrinsèque et de ne pas provenir par exemple d'une paire de photon EPR. Donc le théorème 2.5 est vrai pour n'importes quels photons envoyés.

Une attaque possible de Bob : mesures cohérentes

Nous connaissons l'existence de fonctions f telles que, étant donnés deux photons de polarisations φ_1 et φ_2, il existe un moyen d'avoir plus d'informations sur $f(\varphi_1, \varphi_2)$ qu'en appliquant directement f aux résultats des mesures séparées de φ_1 et φ_2. Ainsi s'il était possible de faire ceci avec l'opérateur $\oplus$, cette mise en gage serait non fiable pour Alice... Ce problème était ouvert à l'époque de la rédaction de [BC91], mais le lemme 2.1, établie dans [BCJL93] permet de répondre à ce problème par la négation.

Bilan

THEOREME 2.6 *En théorie, la mise en gage de [BC91] est inviolable par Alice et Bob.*

Comparaisons entre les deux protocoles

Une étude un peu plus poussée montre que ce protocole reste parfaitement fiable s'il y a quelques multiphotons (pour un n suffisament grand), de plus il résiste à l'attaque EPR. Cependant, il ne résiste pas aux erreurs de transmission car si Bob tolére occasionellement $c'_{i,j} \neq c_{i,j}$ lorsque $b'_{i,j} = b_{i,j}$, Alice peut facilement tricher (n est très grand, donc une erreur par ligne de C' est acceptable ce qui permet facilement de changer $\forall i \in \{1, 2, \ldots, n\}, \bigoplus_{j=1}^{n} c_{i,j} = x$).

Donc théoriquement ce protocole est inviolable, mais pratiquement les deux protocoles se complètent : le protocole de [BB84] souffre des multiphotons mais pas des erreurs de transmisson, et celui de [BC91] souffre de l'inverse!

2.2.4 Une application : le tirage à pile ou face à distance

Il s'agit donc d'une technique permettant de jouer à pile ou face par téléphone “quantique” en implémentant des primitives comme celles exposées précédemment.

Voici tout d'abord une première version étant donnée une primitive de mise en gage se décomposant en commit et unveil.

PROTOCOLE 2.6 — *BB-cointoss*

1. *Alice choisit aléatoirement un bit x_0 et utilise commit(x_0) avec Bob.*
2. *Bob choisit aléatoirement un bit x_1 et l'envoie (normalement) à Alice.*
3. *Alice utilise unveil(x_0) avec Bob.*
4. *Bob a gagné si et seulement si $x_1 = x_0$.*

PROPOSITION 2.6 — *BB-cointoss a la même complexité que celle de commit plus celle de unveil.*

THEOREME 2.7 — *Ce protocole peut être violé si et seulement si la primitive de mise en gage utilisée peut l'être.*

Citons cette autre version qui avait une importance lorsqu'on ne savait pas si l'attaque des mesures cohérentes avait lieu d'être:

PROTOCOLE 2.7 — *BC-cointoss*

1. *Alice choisit aléatoirement un bit x_0 et utilise BB-commit(x_0) avec Bob.*
2. *Bob choisit aléatoirement un bit x_1 et utilise BC-commit(x_1) avec Alice (les rôles d'Alice et Bob sont ici provisoirement interchangés).*
3. *Alice utilise BB-commit(x_0) avec Bob.*
4. *Bob utilise BC-commit(x_1) avec Alice.*
5. *Bob gagne si et seulement si $x_1 = x_0$.*

PROPOSITION 2.7 — *BC-cointoss a une complexité en n^2.*

THEOREME 2.8 — *Seule Alice peut violer ce protocole, et elle peut le violer si et seulement si elle peut implémenter l'attaque EPR (et l'attaque des mesures cohérentes).*

2.2.5 La dernière version actuelle

Ce protocole est extrait de [BCJL93], non encore publié, mais dont une première version m'a été donnée par Claude Crépeau que je remercie vivement. Il s'agit d'une amélioration du protocole décrit dans [BC91], qui permet une implémentation pratique et qui de plus solutionne le problème des mesures cohérentes du précédent protocole. Les démonstrations en étant d'autant plus pointues et faisant appel à des résultats de mécanique quantique et de probabilités, nous nous contenterons donc d'en exposer les grandes lignes.

On notera $X \odot Y$ le produit scalaire booléen, *i.e.* si $X = (x_1, x_2, \ldots, x_n)$ et $Y = (y_1, y_2, \ldots, y_n)$ alors

$$X \odot Y = \bigoplus_{i=1}^{n} x_i \wedge y_i$$

Soit ε un majorant du taux d'erreurs du canal quantique, *i.e.* la probabilité qu'un photon polarisé $|\varphi\rangle$ soit détecté comme étant $|\varphi^\perp\rangle$.

On note $d_H(X, Y) = |\{i \mid x_i \neq y_i\}|$, la distance de Hamming.

DEFINITION 2.2 — *On dira qu'une matrice binaire (booléenne) M vérifie la propriété $P(n,k,d)$, où n,k et d sont des entiers naturels, si elle vérifie les propriétés si dessous :*

- *M est de dimension $n \times k$.*
- $\forall (X,Y) \in \{0,1\}^k, [(X \neq Y) \Rightarrow (d_H(MX,MY) \geq d)]$

THEOREME 2.9 — *Une matrice binaire aléatoire M de dimension $n \times k$ vérifiera la propriété $P(n,k,d)$ sauf avec une probabilité $2^{-\alpha n}$ tant que*

$$k < n - H(d/n) - \alpha n$$

où H est la fonction d'entropie définie par $H(p) = p\lg(\frac{1}{p}) + (1-p)\lg(\frac{1}{1-p})$.

Démonstration:
cf. [MS77]. ∎

Appication : Si $\varepsilon < 1\%$, alors on prend $k/n = 0.52$ et on en déduit qu'en choisissant une matrice binaire M de dimension $n \times 0.52n$, M vérifie $P(n, 0.52n, 10\varepsilon n)$ sauf avec la probabilté $2^{-0.1n}$. Notons que dans le cas défavorable, trouver des vecteurs contradisant P est un problème d'autant plus difficile que n est grand.

La mise en gage proprement dite :

PROTOCOLE 2.8 — *BCJL-commit(x)*

1. *Bob choisit aléatoirement une matrice (n,k) booléenne M vérifiant $P(n,k,d)$, où (n,k,d) vérifie $d/n > 10\varepsilon$ et $k/n = 0.52$, et l'annonce à Alice.*
2. *Alice choisit aléatoirement un vecteur de n bits R et l'annonce à Bob.*
3. *Alice choisit aléatoirement un vecteur de k bits Y tel que $C \odot R = x$ où $C = DY$.*
4. $\underset{i=1}{\overset{n}{DO}}$:
   - *Alice choisit aléatoirement un bit b_i et définit sa base $(|\varphi_i\rangle, |\varphi_i^\perp\rangle) \leftarrow [\oplus, \boxtimes]_{b_i}$.*
   - *Alice envoie à Bob le photon π_i de polarisation $[|\varphi_i\rangle, |\varphi_i^\perp\rangle]_{c_i}$.*
5. $\underset{i=1}{\overset{n}{DO}}$:
   - *Bob choisit aléatoirement un bit ${b'}_i$ et mesure π_i dans $(|{\varphi'}_i\rangle, |{\varphi'}_i^\perp\rangle) \leftarrow [\oplus, \boxtimes]_{{b'}_i}$.*
   - *Bob fixe* ${c'}_i \leftarrow \begin{cases} 0 & \text{si la mesure donne } {\varphi'}_i \\ 1 & \text{sinon} \end{cases}$.

PROPOSITION 2.8 — *Si on ne tient pas compte du choix de M, BCJL-commit a une complexité en n.*

LEMME 2.2 — *Si Alice est honnête, Bob ne peut obtenir plus d'informations sur x que lire séparément chaque photon π_i reçu dans la base $(|\mathcal{B}\rangle, |\mathcal{B}^\perp\rangle)$.*

Démonstration:
Considérons le protocole suivant différent du précédent à la 4-ième étape uniquement :

PROTOCOLE 2.9 — *BCJL-commit'(x)*

1. ...
2. ...
3. ...
4. $\underset{i=1}{\overset{n}{DO}}$:
   - *Alice choisit aléatoirement un bit* b_i *tel que* $\Pr(b_i = 0) = \kappa^2$.
   - *Alice envoie à Bob le photon* π_i *de polarisation* $(|\mathcal{B}\rangle, |\mathcal{B}^\perp\rangle)_{c_i \oplus b_i}$.
5. ...

Démonstration:

On calcule la matrice densité (*cf.* appendice) ρ_0 décrivant le mélange statistique des états envoyés à Bob pour représenter un bit 0 ($b_i = 0$) à l'étape 4 du protocole BCJL-commit :

$$\rho_0 = \frac{1}{2}|\leftrightarrow\rangle\langle\leftrightarrow| + \frac{1}{2}|\swarrow\!\!\!\nearrow\rangle\langle\swarrow\!\!\!\nearrow| = \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix}$$

et pour un bit 1 :

$$\rho_1 = \frac{1}{2}|\updownarrow\rangle\langle\updownarrow| + \frac{1}{2}|\nwarrow\!\!\!\searrow\rangle\langle\nwarrow\!\!\!\searrow| = \begin{pmatrix} \frac{1}{4} & -\frac{1}{4} \\ -\frac{1}{4} & \frac{3}{4} \end{pmatrix}$$

On procède de même pour BCJL-commit' :

$$\rho'_0 = \kappa^2|\mathcal{B}\rangle\langle\mathcal{B}| + (1-\kappa^2)|\mathcal{B}^\perp\rangle\langle\mathcal{B}^\perp| = \ldots = \rho_0$$

$$\rho'_1 = (1-\kappa^2)|\mathcal{B}\rangle\langle\mathcal{B}| + \kappa^2|\mathcal{B}^\perp\rangle\langle\mathcal{B}^\perp| = \ldots = \rho_1$$

Donc, si on appelle ρ_C la matrice densité associée au mélange des états utilisés pour envoyer C dans BCJL-commit et ρ'_C pour BCJL-commit' on a :

$$\rho_C = \rho_{c_1} \otimes \rho_{c_2} \otimes \ldots \otimes \rho_{c_n} = \rho'_{c_1} \otimes \rho'_{c_2} \otimes \ldots \otimes \rho'_{c_n} = \rho'_C$$

Donc enfin, les matrice densités ϱ_x et ϱ'_x correspondant respectivement à BCJL-commit(x) et à BCJL-commit'(x) sont :

$$\varrho_x = \frac{1}{\alpha_x} \sum_{C \in A_x} \rho_C = \frac{1}{\alpha_x} \sum_{C \in A_x} \rho'_C = \varrho'_x \text{ où } A_x = \{C \mid C \odot R = x\} \text{ et } \alpha_x = |A_x|$$

On constate que les matrices obtenues pour BCJL-commit coïncident à celles obtenues pour BCJL-commit'. D'aprés le théorème 5.2, on déduit donc que Bob est capable de tirer exactement la même information sur C (et sur x) dans les deux protocoles. Mais dans BCJL-commit', Bob obtient toute l'information possible sur C (et sur x) en mesurant les photons π_i dans la base $(|\mathcal{B}\rangle, |\mathcal{B}^\perp\rangle)$ puisqu'ils sont polarisés dans cette même base. Donc en particulier aucune mesure cohérente ne peut donner plus d'informations... ■

THEOREME 2.10 — *Si Alice est honnête, il existe une constante* $\alpha \in [0, 1[$ *telle que :*

$$\frac{1}{2} - \alpha^n \leq \left\{ \begin{array}{c} \Pr(x = 0 \mid C') \\ \Pr(x = 1 \mid C') \end{array} \right\} \leq \frac{1}{2} + \alpha^n$$

PROTOCOLE 2.10 — *BCJL-unveil(x, B, C, B', C')*

1. *Alice révèle x, B et C à Bob.*
2. *Bob calcule* $\delta \leftarrow \sum_{i \mid b'_i = b_i} \frac{c_i \oplus c'_i}{n/2}$.
3. *Si* $(\delta < 1.4\varepsilon)$ *et* $(x = C \odot R)$ *alors Bob accepte et refuse sinon.*

PROPOSITION 2.9 — *BCJL-unveil a une complexité en n.*

THEOREME 2.11 — *Si Bob est honnête, il existe une constante $\alpha \in [0, 1[$ telle que la probabilité qu'à Alice d'annoncer dans BCJL-unveil à sa guise $(0, B^0, C^0)$ ou $(1, B^1, C^1)$ et que Bob accepte soit majorée par α^n.*

THEOREME 2.12 *Si Alice est honnête, il existe une constante $\alpha \in [0, 1[$ telle que la probabilité qu'un honnête Bob rejete (B, C, x) dans BCJL-unveil soit majorée par α^n.*

Conclusion :

Il est clair que ce protocole de mise en gage est révolutionnaire en lui même et le premier en son genre. Il ne reste qu'à ajuster les constantes et à attendre que les techniques suivent pour pouvoir espérer une implémentation réelle à grande échelle : on ne peut guerre actuellement dépacer les 32cm et minimiser les erreurs de transmissions à moins de 4%... Mais cette version laisse tout de même entrevoir les choses de façon optimiste !

2.3 Transfert équivoque – Transfert inconscient

2.3.1 Définitions

DEFINITION 2.3 — *Un protocole P est un protocole de transfert équivoque s'il se résume en un protocole du type :*

- *Alice envoie un bit x à P.*
- *P envoie (t, x') à Bob tel que* $\begin{cases} x' = 0 & si\ t = 0 \\ x' = x & si\ t = 1 \end{cases}$ *avec* $\Pr(t = 0) = \Pr(t = 1) = \frac{1}{2}$.

et tel qu'Alice ne sait pas si Bob a reçu x (i.e. si $t = 1$) ou pas.

DEFINITION 2.4 — *Un protocole P est un protocole de transfert inconscient s'il se résume en un protocole du type :*

- *Alice envoie deux bit x_0 et x_1 à P.*
- *Bob envoie un bit c à P.*
- *P envoie x_c à Bob.*

et tel qu'Alice ne sait pas quel bit Bob a reçu, et Bob ne peut connaître qu'un seul des deux bits envoyés par Alice.

2.3.2 Un transfert équivoque faible

Le protocole :

PROTOCOLE 2.11 — *$OT_f(x)$*

1. *Alice choisit aléatoirement un bit b et fixe $(|\varphi\rangle, |\varphi^\perp\rangle) \leftarrow [\oplus, \boxtimes]_b$.*
2. *Bob choisit aléatoirement un bit b' et fixe $(|\varphi'\rangle, |\varphi'^\perp\rangle) \leftarrow [\oplus, \boxtimes]_b'$.*
3. *Alice envoie à Bob un photon π de polarisation $[|\varphi\rangle, |\varphi^\perp\rangle]_x$.*
4. *Bob mesure le photon π dans la base $(|\varphi'\rangle, |\varphi'^\perp\rangle)$.*
5. *Bob fixe $y \leftarrow \begin{cases} 0 & \text{si la mesure donne } \varphi' \\ 1 & \text{sinon} \end{cases}$.*
6. *Alice envoie à Bob b.*
7. *Bob établie $\begin{cases} (t, x') = (1, y) & \text{si } b' = b \\ (t, x') = (0, 0) & \text{sinon} \end{cases}$.*

PROPOSITION 2.10 — *OT_f a une complexité bornée.*

Etude :

PROPOSITION 2.11 *Si Alice et Bob sont honnêtes, alors OT_f est un transfert équivoque.*

Remarque : Alice n'a rien à gagner à tricher *i.e.* polariser dans une mauvaise base ou ne pas annoncer le b correcte ne lui apporte rien car elle ne sait pas la valeur que Bob a reçue. De plus utiliser des photons EPR n'apporte rien pour les mêmes raisons que pour QT défini en introduction. On ne regarde que le cas où Bob est malhonnête en supposant donc Alice honnête.

Une attaque possible pour Bob est de lire les photons dans la base $(|\mathcal{B}\rangle, |\mathcal{B}^\perp\rangle)$. Dans ce cas $\Pr(x' = x) \approx 85\%$ mais Bob ne sera jamais sur si $x' = x$. L'attaque redoutable, appelée *delayed measurements*, consiste pour Bob à stoquer le photon π jusqu'à ce qu'Alice lui annonce b. Pratiquement le stoquage des photons étant si délicat, comme nous l'avons déjà évoqué, que ceci ne pose guère de problèmes, mais tout de même... En fait, plus généralement pour les transferts équivoque et inconscient, les protocoles quantiques consistent à envoyer des informations partielles (à cause du principe d'incertitude) à Bob, dont il connait leur validité quand Alice lui transmet une certaine information (la base de polarisation). Si cela n'avait pas d'importance pour la mise en gage, Il faut donc ici forcer la lecture des photons par Bob à leur réception ou du moins avant de passer à l'étape révélatrice d'Alice. Une implémentation de la mise en gage est possible, mais elle doit être judicieuse pour ne rien révéler à Alice...

2.3.3 Un transfert inconscient

Nous allons à partir du transfert équivoque faible précédent construire un transfert inconscient...

Voici un théorème justifiant le bon fonctionnement du protocole qui suit, sauf avec une probabilité exponentiellement faible en n.

THEOREME 2.13 (BERNSTHEIN) — *Soit $X = (x_1, x_2, \ldots, x_n)$, un vecteur booléen, tel que $\forall i \in \{1, 2, \ldots, n\}, \Pr(x_i = 1) = p$, alors*

$$\forall \delta \in]0, p(p-1)], \Pr\left(\left|\frac{1}{n}\sum_{i=1}^{n} x_i - p\right| \geq \delta\right) \leq 2^{-n\delta^2}$$

Démonstration:
cf. [Kra86]. ■

Le protocole :

PROTOCOLE 2.12 — $\binom{2}{1}$ *-OT(x_0, x_1, c)*

1. *Alice choisit aléatoirement un vecteur de n bits R.*
2. $\underset{i=1}{\overset{n}{DO}}$ *: Alice effectue avec Bob $OT_f(r_i)$, Bob obtenant le couple (t_i, r'_i).*
3. *Bob selectionne aléatoirement deux ensembles disjoints $I_0 = \{i_1, i_2, \ldots, i_{n/3}\}$ et $I_1 = \{i_{n/3+1}, i_{n/3+2}, \ldots, i_{2n/3}\}$ tels que, si possible, $\forall i \in I_0, t_i = 1$.*
4. *Bob envoie à Alice $(J_0, J_1) \leftarrow (I_c, I_{1-c})$.*
5. *Alice stoppe si J_0 et J_1 ne sont pas disjoints ou de mauvaises tailles.*
6. *Alice effectue, pour $k = 0, 1$, $\tilde{x}_k \leftarrow x_k \oplus \bigoplus_{i \in J_k} r_i$*
7. *Alice envoie à Bob $\tilde{x}_0$ et $\tilde{x}_1$.*
8. *Bob effectue $x \leftarrow \tilde{x}_c \oplus \bigoplus_{i \in I_0} r'_i$.*

Remarque : Ce principe est un un principe général pour tranformer un transfert équivoque en transfert inconscient. Il est tiré de [Cré88, Cré90a].

PROPOSITION 2.12 — $\binom{2}{1}$ *-OT a une complexité en n.*

Etude :

On ne regarde que le cas où Bob est malhonnête et Alice honnête.

THEOREME 2.14 — *Si Bob mesure indépendamment chaque photon reçu dans une base, alors Bob ne peut pas avoir plus d'informations qu'un des deux bits d'Alice à une probabilité exponentiellement fiable en n près.*

Démonstration:
Etant donné que $\Pr[\forall i \in I_1, t_i = 1]$ est exponentiellement faible en n, si Bob suit le protocole, il ne peut tirer aucune information de $\tilde{x}_{\overline{c}}$ sauf dans une situation de probabilité d'existence exponentiellement faible en n. La tactique optimale de Bob serait de mesurer chaque photon dans la base $(|\mathcal{B}\rangle, |\mathcal{B}^\perp\rangle)$. Or la proposition suivante nous permet de conclure (sa démonstration se fait par récurence) avec $p_i = \kappa^2$:

PROPOSITION 2.13 — *Soient $2n$ bits aléatoires $c_1, c_2, \ldots, c_n, c'_1, c'_2, \ldots, c'_n$. Si pour tout $i \in \{1, 2, \ldots, n\}$ on a $\Pr(c_i = c'_i) = p_i$ alors*

$$\Pr\left(\bigoplus_{i=1}^{n} c_i = \bigoplus_{i=1}^{n} c'_i\right) = \frac{1}{2} + \frac{\prod_{i=1}^{n}(2p_i - 1)}{2}$$

■

Pour empêcher Bob de stocker les photons reçus, il suffit qu'Alice demande à Bob, après l'étape 4 de OT_f, de mettre en gage à chaque photon reçu le bit lu et le bit correspondant au choix de base de Bob, qu'Alice demandera avec la probabilité $1/2$ de révéler a la fin de OT_f. Lorsque cela ne correspondera pas, Alice mettra fin au protocole.

En ce qui concerne les mesures cohérentes, une étude similaire à celle de [BCJL93] montre qu'elles n'apportent rien.

Bilan

THEOREME 2.15 — *Ce transfert inconscient est inviolable par Bob.*

THEOREME 2.16 — *Disposant d'un protocole de mise en gage et un protocole de transfert inconscient, on peut construire un protocole de transfert inconscient de bits mis en gage, i.e. contraindre les participants à utiliser tout au long du protocole les bonnes entrées* (x_0, x_1, c).

Démonstration:
cf. [Cré90b] qui met en évidence un algorithme de passage des deux protocoles de départ à celui d'arriver de complexité en m^3, où m est tel que les probabilités de réussites de fraudes des protagonistes sont exponentiellement faible en m. ■

Problèmes pratiques :

- Le problème des multiphotons donne un avantage pour Bob. Ce n'est pas très grave en pratique, on a un transfert équivoque à $50\% + \varepsilon$ et $\varepsilon \approx 1\%$ si la probabilité d'envoyer plusieurs photons est faible.
- Le problème du "zero-photon" : Bob annonce à Alice qu'il n'a pas reçu de photon avant qu'Alice ne lui annonce la base de polarisation. Si Bob dit qu'il ne reçoit pas de photon alors qu'il en reçoit, on se retrouve dans le cas précédent. Donc Alice doit faire des statistiques de son dispositif...
- Erreurs de transmission. C'est le plus gros problème, car même si on n'a qu'1% d'erreurs, d'après la proposition 2.13, on aura au résultat quelque chose de quasi aléatoire! Il faut donc un système de codes correcteurs qui permette de corriger $(r_i)_{i \in I_0}$ et non $(r_i)_{i \in I_1}$.

Pour plus de précisions quant à l'implémentation pratique de ce protocole, on consultera [BBCS92].

2.3.4 Comment avoir un transfert équivoque fort?

Nous allons en fait reprendre le principe du protocole précédent pour pouvoir à partir de OT_f faire un transfert équivoque (fort) en implémentant des mises en gage. Je n'ai trouvé ce protocole nulle part, mais il n'est pas inintéressant de le citer :

PROTOCOLE 2.13 — *OT(x)*

1. *Alice choisit aléatoirement un vecteur de* n *bits* R.
2. $\underset{i=1}{\overset{n}{DO}}$: *Alice effectue avec Bob* $OT_f(r_i)$, *Bob obtenant le couple* (t_i, r'_i).
3. *Bob selectionne aléatoirement deux ensembles disjoints* $I_0 = \{i_1, i_2, \ldots, i_{n/3}\}$ *et* $I_1 = \{i_{n/3+1}, i_{n/3+2}, \ldots, i_{2n/3}\}$ *tels que, si possible,* $\forall i \in I_0, t_i = 1$.
4. *Bob choisit aléatoirement un bit* c.
5. *Bob envoie à Alice* $(J_0, J_1) \leftarrow (I_c, I_{1-c})$.
6. *Alice stoppe si* J_0 *et* J_1 *ne sont pas disjoints ou de mauvaises tailles.*
7. *Alice choisit aléatoirement* c'
8. *Alice effectue* $\tilde{x} \leftarrow x \oplus \bigoplus_{i \in J_{c'}} r_i$.
9. *Alice envoie à Bob* $(c', \tilde{x})$.
10. *Bob effectue* $y \leftarrow \tilde{x} \oplus \bigoplus_{i \in I_0} r'_i$.
11. *Bob établie* $\begin{cases} (t, x') = (1, y) & \text{si } c' = c \\ (t, x') = (0, 0) & \text{sinon} \end{cases}$.

Remarque : Alice s'assure donc que Bob mesure les photons au fur et à mesure en lui demandant, après l'étape 4 de OT_f, de mettre en gage à chaque photon reçu son bit lu et son choix de base qu'Alice demandera avec la probabilité 1/2 de révéler a la fin de OT_f.

Chapitre 3

Distribution de clefs quantiques

3.1 Introduction

Deux participants, appelés *Alice* et *Bob*, n'ayant aucune information secrète en commun intialement, désirent échanger des messages secrets résistants aux attaques d'un troisième protagoniste que nous appellerons *Eve*. Ils vont donc établir une clef secrète dont ils se serveront dans algorythme de codage sûr comme le one-time pad. On suppose dans cette partie qu'Alice et Bob sont honnêtes, et de plus l'existence d'un canal public classique dans le sens qu'il n'offre aucune sécurité contre l'espionnage, mais qu'il peut être utilisé sans craintes que les données transmises ne soit modifiées par Eve (existence justifiée dans [Bra92]).

3.2 Un Protocole de distribution de clefs quantiques

3.2.1 Le protocole théorique

<u>PROTOCOLE</u> 3.1 —

1. *Alice choisit aléatoirement un vecteur de n bits B.*
2. *Alice choisit aléatoirement un vecteur de n bits C.*
3. *Bob choisit aléatoirement un vecteur de n bits B'.*
4. $\underset{i=1}{\overset{n}{DO}}$:
   - *Alice envoie dans la base* $(|\varphi_i\rangle, |\varphi_i^\perp\rangle) \leftarrow [\oplus, \boxtimes]_{b_i}$ *le photon* π_i *de polarisation* $[|\varphi_i\rangle, |\varphi_i^\perp\rangle]_{c_i}$ *à Bob.*
   - *Bob lit dans la base* $(|\varphi'_i\rangle, |{\varphi'}_i^\perp\rangle) \leftarrow [\oplus, \boxtimes]_{b'_i}$ *le photon* π_i *reçu.*
   - *Bob fixe* $c'_i \leftarrow \begin{cases} 0 & \text{si la mesure donne } \varphi'_i \\ 1 & \text{sinon} \end{cases}$.
5. *Bob envoie publiquement à Alice B'.*
6. *Alice envoie publiquement à Bob $I = \{i \mid b_i = b'_i\}$.*
7. *Alice et Bob fixent aléatoirement et publiquement un ensemble $I' \subset I$ et comparent publiquement si $\forall i \in I', b_i = b'_i$.*
8. *Si le test précédent est concluant, Alice et Bob établissent la clef $\leftarrow (c_i)_{i \in I \setminus I'}$, sinon ils concluent qu'ils ont été espionnés.*

Remarque : On peut améliorer le test de l'étape 7. Par exemple on peut uniquement comparer la parité du nombre de bits $b_i = 1$ et de bits $b'_i = 1$ en faisant varier I'. Ainsi il n'est pas nécessaire de retrancher I' de I à l'étape 8.

Exemple :

1.	⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕	⤡	⤢	⤢	↕
2.	⊕	⊠	⊠	⊕	⊕	⊠	⊠	⊕	⊠	⊕	⊠	⊠	⊠	⊠	⊕
3.	↕	⤢	⤡	↔	↕	⤢	⤢	↔	⤡	↕	⤡	⤡	⤢	⤢	↕
4.	⊕	⊠	⊠	⊕	⊕	⊠	⊠	⊕	⊠	⊕	⊠	⊠	⊠	⊠	⊕
5.			√	√	√			√	√			√	√	√	√
6.			1	0	1			0	1			1	0	0	1

1. Alice envoie à Bob une suite aléatoire de photons polarisés horizontalement (↔), verticalement (↕), à $\pi/4$ (⤢) ou à $3\pi/4$ (⤡).
2. Bob mesure la polarisation de chacun de ces photons aléatoirement, soit de façon rectiligne (⊕), soit de façon diagonale (⊠).
3. Résultat des mesures de Bob.
4. Bob révèle publiquement à Alice les mesures effectuées pour chacun des photons détectés, mais pas le résultat de ces mesures.
5. Alice dit à Bob lesquelles de ses mesures étaient adéquates.
6. Ces données sont interprétées comme une suite de bits selon la convention arbitraire ↔=⤢= 0 et ↕=⤡= 1.

3.2.2 Etude de l'attaque d'Eve

Attaque primaire

On suppose ici qu'Eve mesure les photons qu'elle décide d'intercepter dans $\oplus$ ou $\boxtimes$ et en les réémettant dans l'une de ces bases. Il est très aisé de voir qu'Alice a une chance sur deux d'avoir lu le bon bit (Eve ne le sait qu'après la révélation des bases communes d'Alice et Bob), *i.e.* Eve obtient un demi-bit espéré d'information, et une chance sur quatre de se faire détecter par Alice et Bob si ce bit donne lieu à un bit de la clef.

Attaque de Breidbart

Eve mesure les photons qu'elle intercepte dans la base de Breidbart, et renvoie un photon de même polarisation que le résultat de la mesure précédente. Dans ce cas, Eve lit le bon bit avec une probabilité de $\kappa^2 \approx 85\%$, mais elle ne sera jamais sure de la bonne valeur de ce bit. Ceci représente donc au sens de Shannon une information de $1+\kappa^2\log_2(\kappa^2)+(1-\kappa^2)\log_2(1-\kappa^2) \approx 0.399$bit espéré d'information. De plus, la probabilité $\mathcal{P}$ de se faire détecter est définie par :

$$\begin{aligned}
\mathcal{P} &= \Pr(\text{Eve lit bon bit et Bob lit bit opposé d'Eve}) + \Pr(\text{Eve lit mauvais bit et Bob lit même bit qu'Eve}) \\
&= (1-\kappa^2)\kappa^2 + \kappa^2(1-\kappa^2) \\
&= \frac{1}{4}
\end{aligned}$$

Attaque plus générale

On suppose ici qu'Eve mesure les photons interceptés dans une base fixée $(|\varphi\rangle, |\varphi^\perp\rangle)$, et les réemet dans une autre base fixée $(|\varphi'\rangle, |\varphi'^\perp\rangle)$. Donc on peut définir $\mathcal{P} = \Pr(\text{Eve lise bon bit})$, et $\mathcal{P}' = \Pr(\text{Bob lise même bit qu'Eve})$ comme suit : $P = (\langle\varphi| \leftrightarrow\rangle + \langle\varphi| \nearrow\!\!\swarrow\rangle)/2 = (\cos^2(\theta) + \cos^2(\theta-\pi/4))/2$, et de même $\mathcal{P}'$ avec un θ' bien choisi; donc $(\mathcal{P}, \mathcal{P}') \in [1/4, \kappa^2]^2$.

- <u>Détection de l'espionnage d'Eve :</u>
  La probabilité pour qu'Eve se fasse détecter est donnée par $\mathcal{P}(1-\mathcal{P}') + (1-\mathcal{P})\mathcal{P}' = \mathcal{P} + \mathcal{P}'(1-2\mathcal{P})$. Trois cas se présentent :
  1. $\mathcal{P} = 1/2$: la valeur de $\mathcal{P}'$ n'importe pas.
  2. $\mathcal{P} > 1/2$: il faut maximiser $\mathcal{P}'$.
  3. $\mathcal{P} < 1/2$: ceci revient au cas 1 où prendrait l'opposé du bit lu, ce qui ne change rien quant à la détection d'Eve.

  Donc Eve a intérêt à prendre dans tous les cas $\mathcal{P}' = \kappa^2$, *i.e.* à renvoyer les photons dans la base $(|\mathcal{B}\rangle, |\mathcal{B}^\perp\rangle)$, alors sa probabilité de se faire détecter est $\mathcal{P}(1-2\kappa^2) + \kappa^2 \geq \mathcal{P}/4$. Et donc à $\mathcal{P}'$ fixé, si $\mathcal{P} \neq 1/2$ Eve a intérêt à maximiser $\mathcal{P}$. En conclusion, Eve se fait le moins repérer (avec une probabilité de $1/4$ sur les bits en communs entre Alice et Bob) en applicant l'attaque primaire ou de Breidbart.
- <u>Quantité de bit espéré d'information révélée :</u>
  En moyenne, Eve lit un bit avec une probabilité d'authenticité de $\mathcal{P}$, et donc en terme d'information de Shannon la quantité de bit espéré d'information est $1+\mathcal{P}\log_2(\mathcal{P})+(1-\mathcal{P})\log_2(1-\mathcal{P}) \leq \mathcal{P}/2$.

Conclusion

Aucune mesure d'un photon en cours de route, effectuée par Eve qui ne sera informé qu'après coup de la bonne mesure à faire, ne peut révéler plus qu'un demi-bit espéré d'information à propos du bit effectivement codé par ce photon, même si Eve effectue une mesure non standart sur le photon. De plus, toute mesure produisant b bit d'information espérée ($b \leq 1/2$) doit introduire un désaccord entre le bit envoyé par Alice et celui reçu par Bob avec une probabilité d'au moins $b/2$, si bien sûr ce photon donne lieu à un bit de la clef à l'issue du protocole.

3.2.3 L'implémentation pratique

Problèmes pratiques:

1. Utilisation délicate de photons isolés.
2. Erreurs de transmissions même en l'absence d'espionnage sur le canal quantique.

Des solutions sont apportées dans [BBBSS90] où il est fait un description du premier montage expérimental de cryptographie quantique effectivement réalisé. Nous allons en exposer les idées de base ci-dessous.

1. On utilise des impulsions dans lesquelles le nombre de photons suit une loi de distribution de Poisson de moyenne contrôlable. D'un point de vue pratique, cette utilisation est plus aisée car elle permet de fixer des polarisations bien définies par des polariseurs, et grâce à une cellule de Pockels, on peut alterner facilement de polarisation entre deux pulsations. Cependant, on se trouve confronté à un problème de multiphotons, qui favorise l'attaque d'Eve. Pour y lutter on fixe par exemple un nombre moyen de photons par impulsion de 1/10. En moyenne, Eve peut trouver alors jusqu'à 10% de bits de la *clef* finale en utilisant les multiphotons ainsi produits.
2. On peut utiliser un code correcteur suffisamment redondant pour que Bob puisse corriger sans ambiguïté sa *clef*, mais aussi suffisamment non redondant pour pas dévoiler trop d'informations à Eve.

Le résultat de l'expérience de [BBBSS90] du 27 février 1991

715 000 impulsions d'intensité moyenne 0.12 photon par impulsion ont été transmises d'Alice vers Bob distants de 32cm. On a pu obtenir une clef de 2000 bits contenant 79 erreurs, soit environ 4% d'erreurs de transmission. La correction d'erreurs a permis de corriger toutes les erreurs en ne révélant que 550 bits à Eve suite à l'espionnage du canal publique uniquement. On a de plus estimé qu'Eve avait une probabilité infime d'avoir obtenu plus de 601 des 2000 bits avant la correction d'erreurs. Donc en sacrifiant 1172 bits, Alice et Bob ont obtenu une clef finale de 828 bits, avec un rythme de transmission d'environ un bit par seconde, telle que la probabilité qu'Eve en connaisse un bit soit inférieure à 10^{-6}.

3.3 Autres méthodes

3.3.1 Photons EPR

cf. [Eke91] et [BBM92].

Dans le protocole précédent, il reste un petit problème : où stoquer la clef ainsi construite pour qu'elle ne soit pas espionnée? Même si elle est utilisée tout de suite, théoriquement on peut envisager une maneuvre d'Eve lui révélant des informations sur cette clef. Pour contrer cette ultime attaque, Artur Ekert a imaginé un protocole à base de photons EPR. Grâce à cette approche, la clef ne prend forme classique qu'au moment précis où elle sera utilisée comme masque jetable. Cependant cette sophistication n'est toutefois pas à la portée de la technologie actuelle.

3.3.2 Interférométrie

cf. [ERTP92].

Comme nous l'avons vu, l'un des problèmes du montage expérimental pour la distribution de clefs est la distance maximale entre Alice et Bob de 32cm. Néanmoins, Artur Ekert, John Rarity, Paul Tapster et Massino Palma travaillent actuellement sur une approche utilisant l'interférométrie et des fibres optiques, ce qui permettrait d'espérer une distance d'une centaine de kilomètres.

Chapitre 4

Conclusion

Nous avons montré à quel point la mécanique quantique apportait un nouveau regard aux problèmes de cryptographie. La perfection mathématique de la mécanique quantique semble se transporter vers la cryptogaphie, et permet ainsi d'envisager des solutions parfaites. Les obstacles restants sont essentiellement pratiques et leur levées nécessitent d'une part l'assouplissement des solutions existantes, ce qui les rend plus complexes et plus techniques, par l'implémentation de codes correcteurs, dont la maîtrise devient donc fondamentale, et d'autre part des progrès de physique expérimentale envisageables comme par exemple une amélioration du taux d'erreurs des detecteurs de photons, de la production de photons isolés, et surtout de la distance entre Alice et Bob. Notons que les protocoles cryptographiques quantiques évoqués dans ce mémoire ont déjà une utilité puisque leur implémentation pratique serait utile même sur une courte distance.

Dans ce mémoire, nous n'avons fait que citer l'une des applications de la mécanique quantique à l'informatique. La cryptographie quantique a pour fondements l'information quantique dont on pourra trouver une introduction aux principaux concepts dans l'appendice de ce mémoire. Citons aussi, le concept de *l'ordinateur quantique* de David Deutsch [Deu85, Deu86] qui permet en théorie l'accélération exponentielle de certains calculs [DJ91, Joz91, BB92]. Si l'ordinateur quantique parvenait un jour à factoriser très rapidement de grands entiers, la mécanique quantique pourrait d'une part probablement mettre en échec les systèmes de codages à clef publique, mais d'autre part apporterait, comme nous l'avons vu, de nouvelles solutions effectivement inviolables.

Pour conclure, je remercie Alain Finkel pour m'avoir fait découvrir ce sujet et m'avoir permis de rencontrer Claude Crépeau dont les cours de DEA et documentations fournies par lui-même m'ont été d'une utilité fondamentale, les bibliothèques d'Orsay et d'Ulm, AleX pour son initiation TEX, et tous ceux que j'oublie.

Chapitre 5

Appendice : l'information quantique

Source principale : [CTDL]

5.1 Généralités - Postulats

POSTULAT 5.1 — *A un instant t_0 fixé, l'état d'un système physique est défini par la donnée d'un vecteur d'état (fonction d'onde solution de l'équation de Schröninger) appartenant à l'espace de Hilbert des états $(\mathcal{E}, \langle | \rangle)$.*

Notations : on appelle *ket* un vecteur $|\psi\rangle$ et *bra* sa forme linéaire associée

$$\langle\psi| : \varphi \mapsto \langle\psi|\varphi\rangle$$

Remarque : le vecteur d'état ayant une interprétation probabiliste, on le supposera normé par défaut.

POSTULAT 5.2 — *A toute grandeur physique mesurable (position, vitesse, polarisation...) $\mathcal{A}$ est associée un opérateur A agissant dans $\mathcal{E}$; cet opérateur est hermitien.*

Remarques :

1. en fait l'opérateur est une *observable*, ce qui représente une notion plus forte en dimension ∞ et qui assure entre autre l'existence d'une base de Hilbert de vecteurs propres...
2. Contrairement à la mécanique classique, la mécanique quantique décrit de façon fondamentalement différente l'état d'un système et les grandeurs physiques associées : un état est représenté par un vecteur normé, une grandeur physique par un opérateur.

5.2 Mesure des grandeurs physiques

POSTULAT 5.3 — *La mesure d'une grandeur physique $\mathcal{A}$ ne peut donner comme résultat qu'une des valeurs propres de l'observable A correspondante.*

Remarques :

1. Une mesure de $\mathcal{A}$ donnera toujours une valeur réelle, puisque A est par définition hermitien.
2. Si le spectre de A est discret, les résultats que l'on peut obtenir en mesurant $\mathcal{A}$ sont quantifiés.

Exemples d'observables :

1. coordonnée x du vecteur position : opérateur X qui est l'opérateur multiplication par x.
2. coordonnée p_x du vecteur quantité de mouvement : opérateur P_x qui est $\frac{\hbar}{i}\frac{\partial}{\partial x}$.
3. tester si un photon passe ou pas par un filtre polarisant orienté horizontalement est traduit par l'observable $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

POSTULAT 5.4 — *(cas d'un spectre discret) Lorsqu'on mesure la grandeur physique $\mathcal{A}$ sur un système dans l'état $|\psi\rangle$ normé, la probabilité $\mathcal{P}(a_n)$ d'obtenir comme résultat la valeur propre a_n de l'observable A correspondante vaut :*

$$\mathcal{P}(a_n) = \sum_{i=1}^{g_n} \left|\langle u_n^i|\psi\rangle\right|^2$$

où g_n est la multiplicité de a_n, et $(|u_n^i\rangle)_{i=1,2,\ldots,g_n}$ est un système orthonormé de vecteurs formant une base dans le sous-espace propre $\mathcal{E}_n$ associé à la valeur propore a_n de A.

Remarque : Dans le cas d'un spectre continu, on généralise ceci en parlant de densité de probabilité...

5.3 Réduction du paquet d'ondes (cas d'un spectre discret)

Supposons que l'on veuille mesurer, à un instant donné, la grandeur physique $\mathcal{A}$. Si l'on connaît le ket $|\psi\rangle$ qui représente l'état du système avant la mesure, le postulat 5.4 permet de prédire les probabilités d'obtenir les divers résultats possibles. Mais, lorsqu'on effectue réellement la mesure, on obtient évidemment un seul de ces résultats possibles. Immédiatement après cette mesure, on sait quelle valeur a été effectivement obtenue. On possède donc une information supplémentaire, et il est compréhensible que l'état du système après la mesure, qui doit incorporer cette information, soit différent de $|\psi\rangle$. Il vient donc naturellement le postulat suivant...

POSTULAT 5.5 — *Si la mesure de la grandeur physique $\mathcal{A}$ sur le système dans l'état $|\psi\rangle$ donne le résultat a_n, l'état du système immédiatement après la mesure est la projection normée de $|\psi\rangle$ sur le sous-espace propre associé à a_n, soit $\frac{P_n|\psi\rangle}{\sqrt{\langle\psi|Pn|\psi\rangle}}$.*

5.4 Quelques conséquences

<u>Proposition</u> 5.1 — *La valeur moyenne de l'observable A dans l'état $|\psi\rangle$ est*

$$\langle A\rangle_\psi = \langle\psi|A|\psi\rangle$$

<u>Proposition</u> 5.2 — *Lorsque deux observables A et B commutent, la mesure de B ne fait pas perdre les informations préalables fournies par une mesure de A (et réciproquement), mais au contraire les complète; de plus, l'ordre dans lequel on mesure les deux observables A et B est sans importance..*

Remarque: dans le cas contraire, on peut ,par exemple, en considérant X et P_x démontrer le principe d'incertitude de Heisenberg.

5.5 L'opérateur densité

5.5.1 Position

Dans cette partie, nous ne considérons plus un sytème d'état ψ déterminé, mais défini de façon statistique *i.e.*:

$$\exists\,(\psi_i)_{i\in I}\,, \psi \in \{\psi_i\}_{i\in I} \text{ et } \Pr(\psi = \psi_i) = p_i \text{ avec bien sûr } \sum_{i\in I} p_i = 1$$

On dit qu'on a affaire à un *mélange statistique* des états $(\psi_i)_{i\in I}$ avec les probabilités $(p_i)_{i\in I}$.

On supposera de plus tous les vecteurs d'états normés.

5.5.2 Cas pur

<u>Definition</u> 5.1 — *On appelle* opérateur densité *associé à l'état ψ l'opérateur ρ défini par*

$$\rho = |\psi\rangle\langle\psi|$$

<u>Proposition</u> 5.3 — *Les propriétés suivantes sont vraies :*

- $tr(\rho) = 1$.
- $\langle A\rangle_\psi = tr(\rho A)$.
- $\mathcal{P}(a_n) = tr(P_n\rho)$.
- *ρ est un opérateur hermitien positif.*

Démonstration:

Plaçons nous dans une base hilbertienne $(|u_n\rangle)_n$. On a donc

$$|\psi\rangle = \sum_n c_n|u_n\rangle \text{ avec } \sum_n |c_n|^2 = 1$$

$$\langle u_i|A|u_j\rangle = a_{i,j}$$

$$\langle A\rangle_\psi = \langle\psi|A|\psi\rangle = \sum_{i,j} \overline{c_i}c_j a_{i,j}$$

$$\rho_{i,j} = \langle u_i|\rho|u_j\rangle = \overline{c_i}c_j$$

Il suffit de réécrire les propriétés avec ces notations pour les démontrer... ■

Remarque : Donc dans un cas pur, un système peut être décrit aussi bien par un opérateur densité que par un vecteur d'état. De plus on y gagne quelques avantages comme la linéarité ds formules utilisant cet opérateur.

5.5.3 Cas non-pur : mélange statique d'états

DEFINITION 5.2 — *Soit un systéme défini par le mélange statistique* $(\psi_i, p_i)_{i\in I}$ *comme au 5.5.1. Alors on définit l'opérateur densité du système comme suit*

$$\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k| \qquad \left(= \sum_k p_k \rho_k\right)$$

PROPOSITION 5.4 — *Les propriétés suivantes sont vraies :*

- $tr(\rho) = 1$.
- $\langle A\rangle_\psi = tr(\rho A)$.
- $\mathcal{P}(a_n) = tr(P_n\rho)$.
- ρ *est un opérateur hermitien positif.*

THEOREME 5.1 — *Il est impossible de distinguer physiquement les divers types de mélanges statistiques qui conduisent à la même matrice densité.*

Démonstration:
Il suffit de voir que toutes les prévisions physiques ne dépendent que de la matrice densité, ce qui a été établi à la proprosition 5.4. ∎

Remarque : $\rho_{n,n} = \sum_k p_k \left|c_n^k\right|^2$ (où $c_n^k = \langle u_n|\psi_k\rangle$) représente la probabilité moyenne de trouver le système dans l'état $|u_n\rangle$ après mesure par l'observable A.

5.6 Produit tensoriel d'états

5.6.1 Introduction

La notion de produit tensoriel d'espaces d'états permet, entre autre, de résoudre le problème suivant. Soit deux systèmes physiques isolés (S_1) et (S_2) d'espaces d'états correspondants respectifs $\mathcal{E}_1$ et $\mathcal{E}_2$. Si nous considérons maintenant l'ensemble de ces deux systèmes comme un unique système (S), quel est l'espace des états $\mathcal{E}$ associé?

5.6.2 Définitions

DEFINITION 5.3 — *Par définition, l'espace vectoriel* $\mathcal{E}$ *est appelé* produit tensoriel *de* $\mathcal{E}_1$ *et* $\mathcal{E}_2$, *noté* $\mathcal{E} = \mathcal{E}_1 \otimes \mathcal{E}_2$, *si à tout couple de vecteurs,* $(|\psi_1\rangle, |\psi_2\rangle) \in \mathcal{E}_1 \times \mathcal{E}_2$, *on associe un vecteur de* $\mathcal{E}$, *noté* $|\psi_1\rangle \otimes |\psi_2\rangle$ *et appelé produit tensoriel de* $|\psi_1\rangle$ *et* $|\psi_2\rangle$, *tel que cette correspondance soit* *linéaire par rapport à la multiplication par des scalaires, et distributive par rapport à l'addition vectorielle :*

$$[\lambda|\psi_1\rangle] \otimes |\psi_2\rangle = \lambda\,[|\psi_1\rangle \otimes |\psi_2\rangle] = |\psi_1\rangle \otimes [\lambda|\psi_2\rangle]$$

$$[|\psi_1\rangle + |\psi'_1\rangle] \otimes |\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle + |\psi'_1\rangle \otimes |\psi_2\rangle$$

$$|\psi_1\rangle \otimes [|\psi_2\rangle + |\psi'_2\rangle] = |\psi_1\rangle \otimes |\psi_2\rangle + |\psi_1\rangle \otimes |\psi'_2\rangle$$

et tel que si $(|u_1^i\rangle)_i$ *et* $(|u_2^j\rangle)_j$ *sont respectivement des bases de* $\mathcal{E}_1$ *et* $\mathcal{E}_2$*, alors* $(|u_1^i\rangle \otimes |u_2^j\rangle)_{i,j}$ *est une base de* $\mathcal{E}$*.*

Notation : On note plus généralement $|\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\rangle|\psi_2\rangle = |\psi_1\psi_2\rangle$.

<u>Definition</u> 5.4 — *On peut définir sur* $\mathcal{E} = \mathcal{E}_1 \otimes \mathcal{E}_2$ *le produit scalaire suivant :*

$$\langle\psi_1\psi_2|\psi'_1\psi'_2\rangle = \langle\psi_1|\psi'_1\rangle\langle\psi_2|\psi'_2\rangle$$

Remarque : on définit de même le produit tensoriel d'opérateurs.

5.6.3 Application

<u>Theoreme</u> 5.2 — *On peut considérer qu'un état produit* $|\psi_1\rangle \otimes |\psi_2\rangle$ *représente la simple juxtaposition de deux systèmes, l'un dans l'état* $|\psi_1\rangle$*, l'autre dans l'état* $|\psi_2\rangle$*. On dit encore que, dans un tel état, les deux systèmes sont* sans corrélations *(de manière plus précise, les résultats de deux types de mesures portant soit sur un système, soit sur l'autre, correspondent à des variables aléatoires indépendantes). Une telle situation est réalisée lorsque les deux systèmes ont été préparés séparément dans les états* $|\psi_1\rangle$ *et* $|\psi_2\rangle$ *et qu'on les réunit ensuite, sans qu'ils interagissent.*

<u>Proposition</u> 5.5 — *Si le système global est dans un état produit* $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$*, alors son opérateur densité sécrit* $\rho = \rho_1 \otimes \rho_2$*, où* ρ_1 *et* ρ_2 *sont respectivement les opérateurs densités de* ψ_1 *et* ψ_2*.*

Références

[BB84] C.H. Bennet, G. Brassard. Quantum cryptography : Public key distribution and coin tossing, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, 1984, pp. 175-179.

[BB92] A. Berthiaume, G. Brassard. The quantum challenge to structural complexity theory, *Proceedings of 7th Annual IEEE Conference on Structure in Complexity Theory*, juin 1992, pp. 132-137.

[BBBSS90] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, et J. Smolin. Experimental quantum cryptography, *Advances in Cryptology - Eurocrypt' 90 Proceedings*, avril 1990, Springer-Verlag, pp. 253-265. Nouvelle édition dans *Journal of Cryptology*, vol. 5, no. 1, 1992, pp. 3-28.

[BBBW82] C.H. Bennett, G. Brassard, S. Breidbart, et S. Wiesner. Quantum cryptography, or unforgeable subway tokens, *Advances in Cryptology : Proceedings of Crypto' 82*, août 1982, Plenum, New York, pp. 267-275.

[BBCS92] C.H. Bennett, G. Brassard, C. Crépeau, M.-H. Skubiszewska. Pratical quantum oblivious transfer protocols, *Advances in Cryptology : Proceedings of Crypto' 91*, vol. 576 de *Lecture Notes in Computer Science*, pp. 351-366. Springer-Verlag, 1992.

[BBE92] C.H. Bennett, G. Brassard, A.K. Ekert. Quantum cryptography, *Scientific American*, octobre 1992, pp. 50-57.

[BBM92] C.H. Bennett, G. Brassard, N.D. Mermin. Quantum cryptography without Bell's theorem, *Physical Review Letters*, vol. 68, 3 février 1992, pp. 557-559.

[BC91] G. Brassard, C. Crépeau. Quantum bit commitment and coin tossing protocols, *Advances in Cryptology : Proceedings of Crypto' 90*, vol. 537 de *Lecture Notes in Computer Science*, pp. 49-61. Springer-Verlag, 1991.

[BCJL93] G. Brassard, C. Crépeau, Richard Jozsa, Denis Langlois. A quantum bit commitment scheme provably unbreakable by both parties, *en préparation*, 1993.

[Bra92] G. Brassard. Cryptologie contemporaine, chez *Masson*.

[Cré88] C. Crépeau. Equivalence between two flavours of oblivious transfers, *Advances in Cryptology : Proceedings of Crypto' 87*, vol. 293 de *Lecture Notes in Computer Science*, pp. 350-354. Springer-Verlag, 1988.

[Cré90a] C. Crépeau. *Correct and Private Reductions among Oblivious Transfers*. PhD thesis, Department of Elec. Eng. and Computer Science, Massachusetts Institute of Technology, 1990. Supervisée par Silvio Micali.

[Cré90b] C. Crépeau. Verifiable disclosure of secrets and applications, *Advances in Cryptology : Proceedings of Eurocrypt' 89*, vol. 434 de *Lecture Notes in Computer Science*, pp.181-191. Springer-Verlag, 1991.

[Cré93] C. Crépeau. Cryptographic primitives and quantum theory, *Proceedings of the second Physics of Computation Workshop, PhysComp' 92*, pp. 200-204, 1993.

[CTDL] C. Cohen-Tannoudji, B. Diu, F. Laloë. Mécanique quantique.

[Del92] J.-P. Delahaye. Cryptographie quantique, *Pour la science*, no. 178, août 1992, pp. 101-106.

[Deu85] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer, *Proceedings of the Royal Society*, Londres, vol. A400, 1985, pp. 97-117.

[Deu86] D. Deutsch. Three connections between Everett's interpretation and experiment, *Quantum Concepts in Space and Time*, R. Penrose et C. Isham, Clarendon Press, Oxford, 1986, pp. 215-225.

[Deu89] D. Deutsch. Quantum communication thwarts eavesdroppers, *New Scientist*, 9 décembre 1989, pp. 25-26.

[DJ91] D. Deutsch, R. Jozsa. Rapid solution of problems by quantum computation, distribué par les auteurs, décembre 1991.

[Eke91] A.K. Ekert. Quantum cryptography based on Bell's theorem, *Physical Review Letters*, vol. 67, 5 août 1991, pp. 661-663.

[EPR35] A. Einstein, P. Podolsky, N. Rosen. Can quantum-mechanical description of physical reality be considered complete?, *Physical Review*, vol. 47, 1988, pp. 42-52.

[ERTP92] A.K. Ekert, J. Rarity, P. Tapster, G.M. Palma. Practical quantum cryptography based on two-photon interferometry, *Physical Review Letters*, vol. 69, 31 août 1992, pp. 1293-1296.

[Joz91] R. Jozsa. Characterizing classes of functions computable by quantum parallelism, *Proceedings of the Royal Society*, Londres, vol. A435, 1991, pp. 563-574.

[Got89] A. Gottlieb. Conjugal secrets - The untappable quantum telephone, *The Economist*, vol. 311, no. 7599, 22 avril 1989, p. 81.

[Kra86] E. Kranakis. Primality and cryptography. John Wiley and Sons, 1986.

[MS77] F.J MacWilliams, N.J.A Sloane. *The THeory of Error-Correcting Codes*, North-Holland, 1977.

[Pet90] I. Peterson. Bits of uncertainly : Quantum security, *Science News*, vol. 137, 2 juin 1990, pp. 342-343.

[Wal89] P. Wallich. Quantum cryptography, Scientific American, vol. 260, no. 5, mai 1989, pp. 28-30.

[Wie83] S. Wiesner. Conjugate coding, écrit vers 1970, non publié jusqu'en 1983 dans *Sigact News*, vol. 15, no. 1, 1983, pp. 78-88.

[WZ82] W.K. Wootters, W.H. Zurek. A single quantum state cannot be cloned, *Nature*, vol. 299, 1982, pp. 802-803.