La Cryptographie Quantique

Printemps des Sciences 2003

Dramaix Florence, van den Broek Didier, Wens Vincent

Prélude

Remerciements

Plusieurs personnes ont contribué à l'accomplissement de ce travail.

Nous tenons à remercier particulièrement Nicolas Cerf, Sofyan Iblisdir et Stefano Pironio qui nous ont supervisés tout au long de ce projet. Nous les remercions pour le temps qu'ils nous ont consacré quant aux apports théoriques, à la vérification de nos calculs (qui furent parfois laborieux) et à la mise en œuvre du tout.

Nous remercions aussi Jean-Louis Colot pour l'aide qu'il nous a apportée ; ainsi que Bénédicte pour les superbes illustrations qui décorent nos affiches.

Avis aux lecteurs

Ce rapport est conséquent car nous avons approfondi certains sujets sans réelle importance pour le thème abordé. Plusieurs passages peuvent être passés.

Table des matières

Chapitre 1

Introduction

Tout ce qui transite par les fibres optiques, le commerce électronique, les transactions bancaires, les messages électroniques, ... est concerné par cette technique prometteuse de la cryptographie quantique ou distribution de clefs secrètes. Et ce, parce qu'elle assure des communications inviolables.

Nous allons plus particulièrement nous intéresser au problème qui consiste en la transmission d'un message entre Alice et Bob, Alice étant la source et Bob, le destinataire. Ils sont reliés par un canal qui d'une part va propager de l'information et d'autre part sera la source de phénomènes perturbateurs. Ces perturbations qui altèrent le message transmis sont la principale propriété du canal. Il peut sembler étrange qu'on accorde une telle importance à ces phénomènes alors qu'ils passent la plupart du temps inaperçus. Mais il ne faut pas oublier que la réception du message envoyé par la source résulte d'une mesure physique dont la précision est limitée. Ce sont ces perturbations qui vont restreindre les possibilités de communication.

Chapitre 2

Théorie de l'information

2.1 Introduction

Avant d'aborder la cryptographie quantique, il est peut être utile de s'intéresser à la notion d'information.

Nous avons utilisé précédemment les termes propager de l'information mais qu'est-ce au juste l'information ? En 1948, Claude Elwood Shannon élabore et énonce sa théorie de l'information. Elle donne une mesure quantitative (mais en la restreignant) de l'information, étudie ses différents moyens de transmission et les dégradations qu'elle subit. Elle affirme la possibilité d'une communication sans erreur malgré la présence de bruits perturbateurs affectant la transmission pourvu qu'un codage approprié soit employé.

Le premier point de cette théorie est la conception d'une mesure quantitative de l'information. Mais il faut garder à l'esprit que l'objet de la théorie de l'information est un message dont la fonction est de transmettre un objet sans en connaître le contenu. L'information que peut porter cet objet n'a pas de conséquence sur les moyens utilisés pour la transporter. On en arrive donc à une définition de l'information qui ne prend pas en considération la sémantique du message, ni ses autres aspects qualitatifs. Cela peut paraître contradictoire car le sens du message semble être l'essence même de l'information et que donc si on retire la sémantique, le message semble se vider de son contenu. Mais la théorie de l'information ne se préoccupe pas de cet aspect.

Remarque 1 *Il est inutile de transmettre un message qui est certain, dont le contenu est connu à l'avance par le destinataire.*

On en tire deux conséquences. La première est qu'on ne va s'intéresser qu'à des sources aléatoires, le message émis est issu d'événements aléatoires. Dans le cas qui nous préoccupe, Alice envoie aléatoirement un photon polarisé horizontalement, verticalement, diagonalement ou anti-diagonalement qui selon des conventions établies préalablement par Alice et Bob représenteront des 0 ou des 1.

La deuxième porte sur la définition de la quantité d'information. Celle-ci va représenter la mesure de l'imprévisibilité du message.

On peut définir plusieurs types de quantités d'information.

L'information moyenne est la quantité d'information produite par une source (dont le message émis est issu d'événements répétitifs et stationnaires, ne dépendant pas de l'origine des temps choisie) et transmise par le message. C'est ce qu'on appelle aussi son entropie.

Une autre quantité est celle de l'information moyenne qu'apporte la connaissance du message reçu sur le message émis. Cette grandeur est symétrique. Elle mesure aussi la quantité d'information qu'apporte le message émis sur le message reçu. C'est l'information mutuelle moyenne ou information mutuelle.

On peut aussi mesurer la capacité d'un canal à transmettre de l'information, c'est le maximum de l'information mutuelle moyenne.

Lorsque les événements que nous utilisons pour décrire la source sont des choix d'éléments, appelés symboles (dans notre cas : un photon dans un état de polarisation), parmi un ensemble prédéterminé appelé alphabet (dans notre cas : les quatre états de polarisation possibles), supposé fini (pour que les symboles puissent être distingués), le message est constitué d'une suite de symboles et est dit numérique. On peut évidemment remplacer le message émis par tout autre qui s'en déduit de manière certaine et réversible (invariance de l'information).

La cryptographie n'est qu'un aspect des transformations que l'on peut effectuer sur un message numérique. On peut le transformer par codage de source, par codage de canal et par cryptographie.

Le codage de source vise à la concision maximale tout en assurant que

l'on peut retrouver le message initial.

Le codage de canal vise à protéger le message contre les perturbations du canal.

La cryptographie quant à elle présente plusieurs aspects, le chiffrage du message (c'est-à-dire le rendre inintelligible à tout autre que son destinataire), son authentification ou encore la détection de toute altération du message par effacement, insertion ou remplacement de certains symboles. Elle sert donc de manière générale à protéger un message.

2.2 Mesure quantitative de l'information

Comme nous l'avons dit précédemment, nous pouvons associer à la mesure de la quantité d'information, la mesure de l'improbable puisqu'un événement certain n'apporte aucune information.

- On mesure donc la quantité d'information $h(x)$ apporté par la réalisation d'un événement x de probabilité $p(x)$ par une fonction croissante de son improbabilité $\frac{1}{p(x)}$ (plus il est improbable plus il apporte d'information), soit :
$$h\left(x\right) = f\left[\frac{1}{p\left(x\right)}\right] \tag{2.1}$$
où f est une fonction croissante.

- Un événement certain apportera une information nulle, soit $f(1) = 0$.

- De plus, on veut que la réalisation de deux événements indépendants x et y apporte la somme de leurs quantités d'information individuelles, soit :
$$\begin{aligned} h\left(x,y\right) &= f\left[\frac{1}{p\left(x,y\right)}\right] = f\left[\frac{1}{p\left(x\right)\cdot p\left(y\right)}\right] \\ &= f\left[\frac{1}{p\left(x\right)}\right] + f\left[\frac{1}{p\left(y\right)}\right] = h\left(x\right) + h\left(y\right) \end{aligned} \tag{2.2}$$
puisque, pour des événements indépendants, $p\left(x,y\right) = p\left(x\right)\cdot p\left(y\right)$.

- On déduit donc de ces trois propriétés que la fonction f est la fonction logarithme et le choix de la base du logarithme définit l'unité d'information utilisée (bit ou Sh, nat, dit, ...).

– La base du logarithme ne sera donc pas précisée dans les définitions qui vont suivre. Mais lorsque nous les appliquerons au cas que nous traitons, nous travaillerons en base 2, de telle sorte que le choix entre deux alternatives équiprobables apporte l'unité d'information, appelé " bit " (abréviation pour binary unit, à ne pas confondre avec l'abréviation de binary digit).

– On associe donc à la réalisation d'un évènement x la quantité d'information (dite propre) :

$$h\left(x\right) = \log\left[\frac{1}{p\left(x\right)}\right] = -\log p\left(x\right) \tag{2.3}$$

Remarque 2 *$h(x)$ ne dépend pas de la valeur de x mais seulement de la probabilité qui lui est associée.*

– Soient deux événements x et y, en généralisant la formule précédente, on peut associer au couple (x,y) la quantité d'information suivante :

$$h\left(x,y\right) = \log\left[\frac{1}{p\left(x,y\right)}\right] = -\log p\left(x,y\right) \tag{2.4}$$

où $p(x,y)$ représente la probabilité conjointe des deux événements.

– On peut aussi définir la quantité d'information associée à x conditionnelle à la réalisation de y, c'est-à-dire sachant que y s'est produit :

$$h\left(x|y\right) = \log\left[\frac{1}{p\left(x|y\right)}\right] = -\log p\left(x|y\right) \tag{2.5}$$

où $p(x|y)$ est la probabilité de x conditionnellement à y.

Par Bayes :

$$p\left(x,y\right) = p\left(x|y\right) \cdot p\left(y\right) = p\left(y|x\right) \cdot p\left(x\right) \tag{2.6}$$

on a donc :

$$\begin{aligned} h(x,y) &= -\log\left(p(x,y)\right) = -\log\left(p(x|y).p(y)\right) \\ &= -\log\left(p(x,y)\right) - log\left(p(y)\right) \end{aligned} \tag{2.7}$$

$$h(x,y) = h(x|y) + h(y) = h(y|x) + h(x) \tag{2.8}$$

– Nous pouvons maintenant définir l'information mutuelle qui est la quantité d'information que la connaissance d'une des variables apporte sur l'autre. Soit $p(x)$ la probabilité a priori que x soit émis et $p(x/y)$ la probabilité que x ait été émis, sachant que y a été reçu. L'information mutuelle est donc :

$$\begin{aligned} i(x:y) &= h(x) - h(x|y) = \log\left(\frac{1}{p(x)}\right) - log\left(\frac{1}{p(x|y)}\right) \\ &= \log\left(\frac{p(x|y)}{p(x)}\right) \end{aligned} \tag{2.9}$$

Appliquons Bayes :

$$i(x:y) = \log\left(\frac{p(x|y)}{p(x)}\right) = \log\left(\frac{p(x,y)}{p(x).p(y)}\right) = i(y:x) \tag{2.10}$$

– Soit un alphabet de n symboles $(x_1,\ldots,x_n)$, X la variable aléatoire décrivant l'émission de la source et pouvant prendre comme valeur les symboles, x_i, de l'alphabet avec la probabilité :

$$p_i = P(X = x_i) \qquad i = 1,2,\ldots,n \tag{2.11}$$

avec $\sum_{i=1}^{n} p_i = 1$.

Remarque 3 *Nous supposons les choix successifs des x_i indépendants.*

– La quantité d'information moyenne associée à chaque symbole de cette source est la moyenne, l'espérance mathématique, de l'information propre de chacun des événements $X = x_i$:

$$H(X) = E\left(h(X)\right) \tag{2.12}$$

C'est l'entropie de la source.

Remarque 4 *Nous voyons immédiatement que le remplacement d'un symbole par un autre (tant qu'on ne touche pas aux probabilités) ne change pas la valeur de H.*

– Considérons maintenant deux variables aléatoires X à valeurs dans $(x_1,\ldots,x_n)$ et Y à valeurs dans $(y_1,\ldots,y_m)$. On peut définir l'entropie conjointe moyenne :

$$\begin{aligned} H(X,Y) &= E\left(h(X,Y)\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} p(x_i,y_j).\log\left(\frac{1}{p(x_i,y_j)}\right) \\ &= -\sum_{i=1}^{n}\sum_{j=1}^{n} p(x_i,y_j).\log\left(p(x_i,y_j)\right) \end{aligned} \tag{2.13}$$

On peut aussi définir l'entropie conditionnelle moyenne :

$$\begin{aligned} H(X|Y) &= E\left(h(X|Y)\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} p(x_i,y_j).\log\left(\frac{1}{p(x_i|y_j)}\right) \\ &= -\sum_{i=1}^{n}\sum_{j=1}^{n} p(x_i,y_j).\log\left(p(x_i|y_j)\right) \end{aligned} \tag{2.14}$$

On a :

$$p(x_i|y_j) = \frac{p(x_i,y_j)}{p(y_j)}$$

où

$$p(y_j) = \sum_{i=1}^{n} p(x_i,y_j))$$

est la probabilité marginale de y_j.

– On peut donc réécrire $H(X,Y)$ sous la forme :

$$\begin{aligned} H(X,Y) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p(x_i,y_j).\log\left(\frac{1}{p(x_i,y_j)}\right) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} p(x_i,y_j).\log\left(\frac{1}{p(x_i|y_j).p(y_j)}\right) \end{aligned} \tag{2.15}$$

$$\begin{aligned} H(X,Y) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p(x_i,y_j).\log\left(\frac{1}{p(x_i|y_j)}\right) \\ &\quad + \sum_{i=1}^{n}\sum_{j=1}^{n} p(x_i,y_j).\log\left(\frac{1}{p(y_j)}\right) \end{aligned} \tag{2.16}$$

$$H(X,Y) = H(X|Y) + H(Y) = H(X) + H(Y|X) \tag{2.17}$$

– Une autre grandeur très importante associée à un couple de variables aléatoires est l'information mutuelle moyenne :

$$I(X:Y) = E\left(i(X:Y)\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} p(x_i,y_j).\log\left(\frac{p(x_i|y_j)}{p(x_i)}\right) \tag{2.18}$$

$$I(X:Y) = \sum_{i=1}^{n}\sum_{j=1}^{n} p(x_i,y_j).\log\left(\frac{p(x_i,y_j)}{p(x_i).p(y_j)}\right) \tag{2.19}$$

$$\begin{aligned} I(X:Y) \quad &= H(X) - H(X|Y) = H(Y) - H(Y|X) \\ &= H(X) + H(Y) - H(X,Y) \end{aligned} \tag{2.20}$$

où $p(x_i)$ et $p(y_j)$ sont les probabilités marginales respectives de x_i et y_j.

$I(X:Y)$ est la réduction de l'entropie sur la variable aléatoire X qu'apporte la connaissance de la variable aléatoire Y.

Propriétés des grandeurs définies.

– L'entropie est non négative : $H(X) \geq 0$.

L'égalité est vérifiée lorsque la probabilité d'un des symboles est égale à 1 et donc toutes les autres probabilités sont égales à 0. Ce qui signifie qu'un des événements est certain. Sa réalisation n'apporte donc aucune information.

– Le maximum de $H(X)$ est atteint, pour n fixé, lorsque $p_i = \frac{1}{n}$, $\forall i$.

Démonstration : Soient deux distributions de probabilité sur le même ensemble fini, $(p_1, \ldots, p_n)$ et $(q_1, \ldots, q_n)$, avec

$$\sum_{i=1}^{n} p_i = \sum_{j=1}^{n} q_j = 1$$

On sait que

$$\ln(x) \leq x - 1$$

Soit

$$x = \frac{q_i}{p_i}$$

On a :

$$\ln\left(\frac{q_i}{p_i}\right) \leq \frac{q_i}{p_i} - 1$$

$$\Rightarrow \quad p_i \ln\left(\frac{q_i}{p_i}\right) \leq p_i\left(\frac{q_i}{p_i} - 1\right)$$

En faisant la somme sur tous les i, on a

$$\sum_{i=1}^{n} p_i \ln\left(\frac{q_i}{p_i}\right) \leq \sum_{i=1}^{n} p_i\left(\frac{q_i}{p_i} - 1\right) = \sum_{i=1}^{n} q_i - \sum_{i=1}^{n} p_i = 1 - 1 = 0$$

Cette inégalité reste donc vraie si on la multiplie par un facteur multiplicatif positif quelconque, donc quelle que soit la base du logarithme.

On a donc

$$\sum_{i=1}^{n} p_i . \log\left(\frac{q_i}{p_i}\right) \leq 0$$

Prenons $q_i = \frac{1}{n}\ \forall i$, on a :

$$\sum_{i=1}^{n} p_i \log\left(\frac{1}{np_i}\right) = \sum_{i=1}^{n} p_i \log\left(\frac{1}{p_i}\right) - \sum_{i=1}^{n} p_i \log(n) \leq 0$$

$$\Rightarrow \quad \sum_{i=1}^{n} p_i \log\left(\frac{1}{p_i}\right) \quad = H(p_1, \ \ldots \ , p_n) \leq \sum_{i=1}^{n} p_i \log(n) = \log n$$

$$= \sum_{i=1}^{n} \frac{1}{n} \log(n) = H\left(\frac{1}{n}, \ldots, \frac{1}{n}\right)$$

Le maximum de H est donc bien atteint lorsque $p_i = \frac{1}{n}$.

□

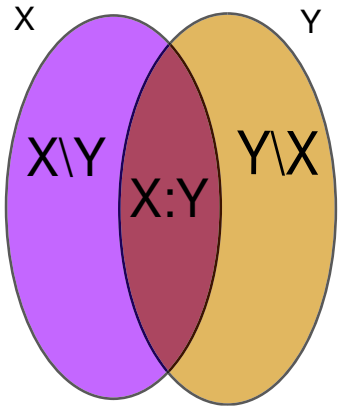
–

$$H(\lambda_1 p_1 + \lambda_2 p_2) \geq \lambda_1 H(p_1) + \lambda_2 H(p_2) \tag{2.21}$$

- Soit une variable aléatoire $X' = \{(x_1,p_1),\ \ldots,\ (x_n,p_n)\} \cup \{(x_{n+1},0)\}$, alors :
$$H(X') = H(X) \tag{2.22}$$

- $H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$

- On peut représenter les diverses quantités dont on a parlé précédemment sous la forme d'un diagramme, appelé diagramme de Venn :



Théorème 1 *La seule expression de l'entropie qui satisfait aux quatre propriétés suivantes :*

- $H(X) \geq 0$

- $H(\lambda_1.p_1 + \lambda_2.p_2) \geq \lambda_1.H(p_1) + \lambda_2.H(p_2)$

- *H ne dépend pas des valeurs des x_i mais uniquement des probabilités $p_i = P(X = x_i)$*

- $H(p_1,\ \ldots\ ,p_n,\ 0) = H(p_1,\ \ldots\ ,p_n)$

est l'entropie de Shannon,

$$H(X) = E[h(X)] = \sum_{i=1}^{n} p_i.log_2\left(\frac{1}{p_i}\right) \tag{2.23}$$

L'entropie de Shannon quantifie la quantité d'information.

La question que l'on se pose est de déterminer le nombre de bits qui sera nécessaire à l'encodage d'une information.

Prenons par exemple le tirage d'une pièce. Excluons les cas extrêmes où la probabilité d'apparition de face vaut 0, 1 ou ½. Dans les deux premiers cas, on n'a besoin d'aucun bit puisque c'est un événement certain. Dans le dernier cas, pour n lancers (n $\rightarrow \infty$), la quantité d'information est maximale (cf. deuxième propriété), il faudra donc n bits pour enregistrer l'information. Dans les cas intermédiaires, on aura np faces (p étant la probabilité d'apparition de face) et n(1 – p) piles.

Regardons le nombre de séquences typiques que l'on a :

$$m = \left(\begin{array}{c} np \\ n \end{array} \right) \tag{2.24}$$

et le nombre de bits qu'il faudra pour encoder m, c'est-à-dire

$$log_2\ m \tag{2.25}$$

On sait que

$$log\ (n\ !) = n\ log\ n - \frac{1}{n} + o(log\ n) \tag{2.26}$$

et que, pour $n \rightarrow \infty$,

$$n\ ! = \sqrt{2\ \pi}\ n^{n+1/2}\ e^{-n} \tag{2.27}$$

$$\begin{aligned} \log_2(m) \quad &= log_2 \frac{n!}{(n\ p)!\ n\ (1-p)!} = -n(p\ \log p + (1-p)\ \log(1-p)) \\ &= n\ H(p) \end{aligned} \tag{2.28}$$

$$m = 2^{-n\ H(p_i)} \tag{2.29}$$

On aura besoin de $n\ H(p)$ bits pour encoder l'information d'un tirage.

Étendons ce résultat à un cas plus général. Soit un ensemble d'événements $\{x_i\}$ chacun de probabilité p_i, le nombre de séquences typiques est

$$\frac{n!}{\prod_{x_j}(n.p_j)!}$$

et le nombre de bits nécessaires est

$$n\ H(p_i)$$

2.3 La cryptographie

La cryptographie sert principalement à protéger des informations que l'on essaie de transmettre. Pour ce faire, on va chiffrer le message, c'est-à-dire le coder. Mais à l'heure actuelle les techniques de chiffrement et de déchiffrement sont assez bien connues. La sécurité d'un message réside donc dans le choix de la clef utilisée pour le chiffrer.

D'autre part, Shannon a démontré que la sécurité d'un message chiffré ne peut être totale que si chaque message (échangé entre deux personnes) est chiffré avec une clef aussi longue que celui-ci et que cette clef doit être différente pour chaque message.

Deux personnes peuvent, bien entendu, établir à chaque nouveau message à chiffrer une nouvelle clef, mais le problème est qu'elles doivent transmettre celle-ci sans que d'autres personnes en prennent connaissance. Cette clef ne peut donc pas être envoyée par un canal public qui est vulnérable à toutes sortes d'interceptions passives.

C'est à la physique que nous allons faire appel pour résoudre ce problème.

En effet, l'information échangée lors de la distribution d'une clef est toujours transmise par un moyen physique : la lumière (cf. le sujet que nous allons traiter), le son, les ondes radio ou encore des électrons. L'espionnage peut alors être vu comme l'acquisition de mesures faites sur le moyen physique utilisé pour la transmission. En théorie, l'acquisition de telles mesures perturbe l'état de ce moyen physique permettant ainsi aux utilisateurs d'effectuer leurs propres mesures afin de déterminer s'ils sont espionnés ou pas. En pratique, tous les canaux classiques peuvent être espionnés de façon passive sans que les utilisateurs (légitimes) ne puissent le déterminer. Ce que la mécanique quantique propose pour tenter de résoudre le problème est de concevoir des canaux de communication, les canaux quantiques, ayant la propriété d'être inviolables, c'est-à-dire que s'il y a espionnage sur un tel canal, celui-ci ne peut se faire sans être détecté.

Chapitre 3

Postulats de la Mécanique Quantique

Il est utile de rappeler ici les postulats de la mécanique quantique. Nous la présentons de façon purement axiomatique, sans "explication" sur les origines physiques car nous n'utiliserons que les postulats suivants.

3.1 Le cadre mathématique de la mécanique quantique.

La mécanique quantique se présente dans un espace de Hilbert, c'est-à-dire un espace fonctionnel $\mathcal{L}^2$ muni d'un produit scalaire.

Définition 1 *$\mathbb{H}$ est un espace de Hilbert si*

- *$\mathbb{H}$ est un espace $\mathcal{L}^2$, c'est-à-dire que $\forall f \in \mathcal{L}^2$, f :*
  $A \subset \mathbb{R}^3 \times \mathbb{R} \to \mathbb{C}$, f est mesurable et de carré sommable,

$$\int_A |f(x)|^2 dx \leq \infty \tag{3.1}$$

- *$\mathbb{H}$ est complet, c'est-à-dire que tout suite de Cauchy est convergente.*

- *$\mathbb{H}$ est muni d'un produit scalaire, défini par*

$$\langle f|g\rangle = \int_A dx f(x)^* g(x) \qquad \forall f,g \in \mathbb{H} \tag{3.2}$$

Les éléments de cet espace sont appelés des fonctions d'onde, et notés $\psi : A \to \mathbb{C}$.

Notons que $\langle \ | \ \rangle$ est un bon produit scalaire hermitien, c'est-à-dire qu'il vérifie les propriétés suivantes.
$\forall$ f, g, h $\in \mathbb{H}$, $\forall \alpha, \beta \in \mathbb{C}$:

$$\langle f|\alpha g + \beta h\rangle = \alpha\langle f|g\rangle + \beta\langle f|h\rangle \tag{3.3}$$

$$\langle f|g\rangle = \langle g|f\rangle^* \tag{3.4}$$

$$\langle f|f\rangle > 0 \tag{3.5}$$

$$\langle f|f\rangle = 0 \Leftrightarrow f \text{ est la fonction nulle} \tag{3.6}$$

3.2 Les notations de Dirac

On associe à toute fonction d'onde ψ un vecteur, noté $|\psi\rangle$ et appelé un *ket*. Ce vecteur d'état appartient à l'espace $\mathcal{E}$, appelé espace des états. C'est un sous-espace de l'espace d'Hilbert.

L'existence d'un *produit scalaire* nous permet aussi de prouver que le dual de $\mathcal{E}$, $\mathcal{E}^* = \{\text{application linéaire} : \mathcal{E} \to \mathbb{C}\ \}$, est isomorphe à $\mathcal{E}$.

Un élément de $\mathcal{E}^*$ est appelé un bra et est en fait associé à une fonction d'onde (ou à un ket) et est noté : $\langle\psi|$.

Théorème 1 *$\mathcal{E}^*$ est isomorphe à $\mathcal{E}$, c'est-à-dire à tout ket correspond un bra et réciproquement.*

En effet, $\forall|\psi\rangle$, $|\phi\rangle \in \mathcal{E}$, on a $\langle\phi|(|\psi\rangle) \equiv (|\phi\rangle\ ,\ |\psi\rangle)$ où (,) est le produit scalaire dans $\mathcal{E}$.

L'action de $\langle\phi|$ sur $|\psi\rangle$ est noté $\langle\phi|\psi\rangle$, c'est aussi le produit scalaire.

3.3 Les postulats

Axiome 1 *Tout état quantique peut être décrit par un ket. L'espace des états est un espace vectoriel complexe.*

On en tire en particulier le principe de superposition :

$$\forall|f\rangle\ ,\ |g\rangle \in \mathcal{E} \quad \forall\alpha\ ,\ \beta \in \mathbb{C} : \qquad \frac{\alpha|f\rangle + \beta|g\rangle}{\|\alpha|f\rangle + \beta|g\rangle\|} \in \mathcal{E} \tag{3.7}$$

Remarque 1 *On norme toujours les kets en vue d'avoir toujours une probabilité totale de 1.*

Axiome 2 *Toute quantité physique est représentée par une observable, c'est-à-dire un opérateur linéaire, $A : \mathcal{E} \to \mathcal{E}$, auto-adjoint (égale à sa conjuguée hermitique ; $A = A^\dagger$) pour lequel il existe toujours une base orthonormée de $\mathcal{E}$ formée par ses kets propres.*

Les seules quantités physiquement mesurables sont données par les valeurs propres de A.

Soit A une observable, $\mathrm{A} = \mathrm{A}^\dagger \equiv (A^T)^*$, soit $\{\lambda_i, |v_i\rangle\}$ l'ensemble de ses valeurs propres et vecteurs propres associés. Donc, $A|v_i\rangle = \lambda_i|v_i\rangle$ avec $\lambda_i \in \mathbb{C}$.

Axiome 3 *Axiome de calcul des probabilités (cas discret).*

La probabilité de mesurer λ_i est donnée par $P(\lambda_i) = |\langle v_i|\psi\rangle|^2$ où $|\psi\rangle$ est l'état du système considéré.

Remarque 2 *Cette écriture n'est valable que dans le cas où la base est discrète (le spectre est discret) et où les valeurs propres ne sont pas dégénérées, c'est-à-dire où la dimension de tous les sous-espaces propres est 1. Nous n'aurons besoin par la suite que de ce cas-ci, c'est pourquoi nous nous y limitons.*

Remarque 3 *Cet axiome justifie la normalisation des kets :*
$|\langle v_i|\psi\rangle|$ est la composante i de $|\psi\rangle$ sur la base $|v_i\rangle$.

En effet, $|\psi\rangle = c^i|v_i\rangle$

Nous sous-entendons la sommation sur la dimension de $\mathcal{E}$, quand un indice est répété.

Alors $\langle v_i|\psi\rangle = \langle v_i|c^j v_j\rangle = c^j\langle v_i|v_j\rangle = c^j\delta_{ij} = c^i$ (car $|v_i\rangle$ est orthonormé)

$$P(\lambda_i) = |\langle v_i|\psi\rangle|^2 = |c^i|^2 \tag{3.8}$$

La somme sur toutes les valeurs propres doit donner la probabilité de l'événement certain, c'est-à-dire un.

$$\sum_i P(\lambda_i) = \sum_i |c^i|^2 = \langle\psi|\psi\rangle = 1 \tag{3.9}$$

car $|\psi\rangle$ est normé.

Axiome 4 *Effet d'une mesure sur un état quantique.*

Soit $|\psi(t)\rangle$ un état à l'instant t et $\{\lambda_i\ ,|v_i\rangle\}$ le spectre de A. Si une mesure de A est effectuée à cet instant, l'état est projeté sur le vecteur propre correspondant à la mesure.

$$|\psi(t)\rangle \rightarrow |\psi'(t)\rangle = |v_i\rangle$$

Cet axiome, central pour la cryptographie quantique, nous dit finalement que si une mesure est effectuée, et que nous mesurons λ_i (avec une probabilité $P(\lambda_i)$), immédiatement après, nous savons que l'état sortant est $|v_i\rangle$; car si nous refaisons à nouveau cette mesure et si l'état n'a pas évolué dans le temps, nous sommes sûrs de trouver λ_i.

$$P(\lambda_i) = |\langle v_i|v_i\rangle|^2 = 1 \tag{3.10}$$

Axiome 5 *Evolution d'un état dans le temps.*

L'évolution dans le temps d'un ket $|\psi\rangle$ est décrit par une équation différentielle linéaire, l'équation de Schrödinger :

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle \tag{3.11}$$

où H est une observable représentant l'énergie du système, appelée hamiltonien ; $H = H^\dagger$.

Par exemple, pour une particule libre de masse m , $H = -\frac{\hbar^2}{2m}\triangle$.

Propriété 1 *L'évolution temporelle est unitaire, c'est-à-dire que $|\psi(t)\rangle = U(t,t_0)|\psi(t_0)\rangle$ où $UU^\dagger = 1$.*

En effet, une solution de l'équation de Schrödinger est donnée par :

$$|\psi(t)\rangle = \exp\left(-\frac{i}{\hbar}\int_{t_0}^{t} d\tau H(\tau)\right)|\psi(t_0)\rangle \tag{3.12}$$

$$U(t,t_0) = \exp\left(-\frac{i}{\hbar}\int_{t_0}^{t} d\tau H(\tau)\right) \tag{3.13}$$

où l'exponentielle d'une matrice est définie par

$$e^M \equiv \sum_{\nu=0}^{\infty}\frac{M^\nu}{\nu!} \tag{3.14}$$

Nous pouvons vérifier que c'est une solution. Nous sommes assurés que la soution est la seule pour une condition initiale donnée $|\psi(t_0)\rangle$ (théorème d'unicité pour les équations différentielles).

Cet opérateur exponentiel $U(t,t_0) = \exp\left(-\frac{i}{\hbar}\int_{t_0}^{t} d\tau H(\tau)\right)$ est effectivement unitaire.

En effet,

$$U(t,t_0)U^\dagger(t,t_0) = \exp\left(-\frac{i}{\hbar}\int_{t_0}^{t} d\tau H(\tau)\right)\exp\left(+\frac{i}{\hbar}\int_{t_0}^{t} d\tau H(\tau)^\dagger\right) = 1 \quad (3.15)$$

car

$$H = H^\dagger \quad (3.16)$$

et

$$e^A e^{-A} = 1 \quad (3.17)$$

car A et $(-A)$ commutent.

Remarque 4 *Notons que cette évolution est nécessairement unitaire car elle doit conserver le produit scalaire (c'est la définition des transformations unitaires en fait).*

En effet,

$$\begin{aligned} |\psi'\rangle &= U|\psi\rangle \\ |\phi'\rangle &= U|\phi\rangle \\ \langle\phi'|\psi'\rangle = \langle\phi|U^\dagger U|\psi\rangle &= \langle\phi|\psi\rangle \quad \text{car} \quad U^\dagger U = 1 \end{aligned} \quad (3.18)$$

où nous avons utilisé la définition de la conjugaison hermitique :

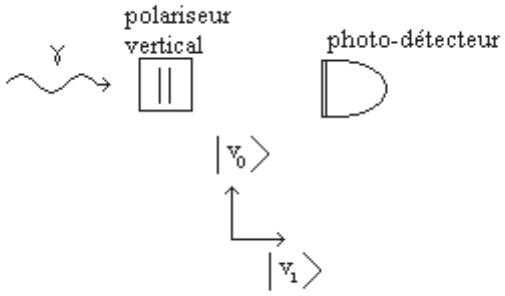
$$\langle\phi|U|\psi\rangle^* \equiv \langle\psi|U^\dagger|\phi\rangle \quad \text{ou} \quad \langle U\phi| \equiv \langle\phi|U^\dagger \quad (3.19)$$

Après cette liste axiomatique, considérons un exemple relation directe avec la cryptographie quantique.

3.4 Exemple : Polarisations de photons

1. Soit le dispositif expérimental suivant.

Plaçons un polariseur qui ne laisse passer que des photons polarisés verticalement suivi d'un photo-détecteur, qui fait 'clic' si un photon est détecté et 'pas clic' sinon. Ce dispositif nous permet seulement de détecter les photons polarisés verticalement.



Traduisons ceci dans le langage de la mécanique quantique.

Les états du système sont les état de polarisation d'un photon ; les mesure (de l'observable) auront aussi pour valeur ses état de polarisation.

Les mesures possibles sont :
- $\lambda_0 = 0$ = 'clic'
- $\lambda_1 = 1$ = 'pas clic'

On note les états correspondants $|v_0\rangle$,$|v_1\rangle$.
(λ_0,λ_1) sont les valeurs propres et ($|v_0\rangle$,$|v_1\rangle$) sont les vecteurs propres d'un opérateur, appelons-le P.

$\{|v_0\rangle$,$|v_1\rangle\}$ est une base orthonormée de l'espace des états (de polarisation). C'est la base H/V (Horizontale/Verticale).

Prenons plusieurs cas :

- Soit un photon dans l'état $|\psi\rangle = |v_0\rangle$.
  Alors, P $(\lambda = \lambda_0) = 1$; P $(\lambda = \lambda_1) = 0$.

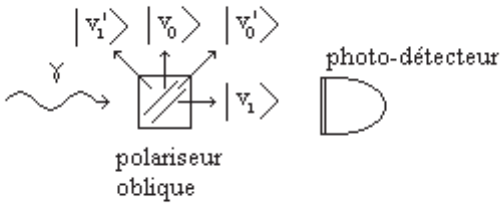
- Soit un photon dans l'état $|\psi\rangle = \frac{|v_0\rangle+|v_1\rangle}{\sqrt{2}}$ (normé, $\langle\psi|\psi\rangle = 1$).
  Alors,
  - $P(0) = |\langle v_0|\psi\rangle|^2 = |c_0|^2 = \frac{1}{2}$
  - $P(1) = |c_1|^2 = \frac{1}{2}$

  Notons que ce photon n'est pas polarisé dans la direction "$\vec{v}_0+\vec{v}_1$" (c'est-à-dire dans la direction oblique) mais est dans une superposition quantique de ces deux polarisations.

- Soit $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|v_0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|v_1\rangle$
  (normé, $\langle\psi|\psi\rangle = \left(\cos\left(\frac{\theta}{2}\right)\right)^2 + |e^{i\phi}|^2\left(\sin\left(\frac{\theta}{2}\right)\right)^2 = 1$).

  Alors
  - $P(0) = |\langle v_0|\psi\rangle|^2 = \left(\cos\left(\frac{\theta}{2}\right)\right)^2$
  - $P(1) = |\langle v_1|\psi\rangle|^2 = |e^{i\phi}\sin\left(\frac{\theta}{2}\right)|^2 = \left(\sin\left(\frac{\theta}{2}\right)\right)^2$

2. Changeons l'orientation du polariseur et tournons-le de $\frac{\pi}{4}$.



La nouvelle base est $|v_0'\rangle$et $|v_1'\rangle$, déterminée par une rotation d'angle $\frac{\pi}{4}$:

- $|v_0'\rangle = \frac{|v_0\rangle+|v_1\rangle}{\sqrt{2}}$: polarisation diagonale
- $|v_1'\rangle = \frac{|v_0\rangle-|v_1\rangle}{\sqrt{2}}$: polarisation anti-diagonale

C'est la base D/A (Diagonale/Anti-diagonale).

Effet et perturbation de la mesure :

Supposons que nous ayons deux polarisateurs qui se suivent, par exemple :

$$|v_0'\rangle = \text{donne} \begin{cases} \frac{1}{2}(\text{proba})|v_0\rangle \rightarrow \begin{cases} 1/2|v_0'\rangle \\ 1/2|v_1'\rangle \end{cases} \\ \frac{1}{2}(\text{proba})|v_1\rangle \rightarrow \begin{cases} 1/2|v_0'\rangle \\ 1/2|v_1'\rangle \end{cases} \end{cases}$$

Soit un photon dans un état $|\psi\rangle = |v_0'\rangle$.

Il y a une probabilité 1/2 pour le photon passe, c'est-à-dire soit dans l'état polarisé verticalement $|v_0\rangle$ et 1/2 pour que le photon soit dans l'état $|v_1\rangle$.

Si le photon passe dans l'état $|v_0\rangle$, il y a encore une probabilité 1/2 qu'il soit projeté sur l'état $|v_0'\rangle$ et que le photo-détecteur fasse 'clic' et 1/2 qu'il soit projeté sur l'état $|v_1'\rangle$.

On a donc une chance sur deux que le photon initialement préparé dans l'état $|v_0'\rangle$ soit détecté dans cet état par le photo-détecteur à la fin de l'expérience. Ce qui montre bien que la première mesure de la polarisation (dans la base H/V) a perturbé l'état de polarisation du photon. Toute mesure perturbe l'état du système.

Chapitre 4

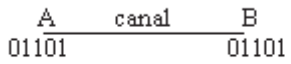
Cryptographie quantique

4.1 Généralités

Rappelons brièvement le problème que nous désirons traiter.

Si deux personnes, Alice (A) et Bob (B), veulent s'envoyer un message secrètement, ils devront élaborer des techniques permettant de coder et sécuriser la transmission du message : c'est la cryptographie. Cela revient essentiellement (comme nous l'avons dit précédemment) à transmettre une clef secrète, c'est-à-dire une suite de bits où un bit est un élément d'information prenant deux valeurs possibles (cf. théorie de l'information) qui permet, une fois cette clef connue par Alice et Bob, de transmettre un message secret codé.

Un exemple de protocole de transmission de codes secrets, une fois cette clef connue, est le code de Vernam, qui est le seul qui soit mathématiquement reconnu comme inviolable.



Soit 01101, la clef secrète connue de Alice et Bob seuls.

Le code de Vernam est le suivant : il faut effectuer un “ou exclusif” (XOR) (équivalent à une addition modulo 2 des bits correspondant) entre le message à coder et la clef secrète dont on dispose.

XOR	**0**	**1**
0	0	1
1	1	0

Le résultat est alors envoyé par un canal public. Ce message envoyé ne possède aucune information sauf pour Bob car personne d'autre que lui ne connaît la clef secrète.

Pour en connaître le contenu, il suffit à Bob de faire un XOR avec le message qu'il a reçu et la clef secrète qu'il a en sa possession. Il obtient ainsi le message originel car XOR est une opération involutive (c'est-à-dire dont la composée avec elle-même est l'identité).

Soit 00011 le message à transmettre.

Alice fait un XOR avec sa clef secrète : 01101 XOR 00011 = 01110.

Bob reçoit 01110 et veut retrouver le message transmis, il fait donc un XOR avec sa clef secrète : 01101 XOR 01110 = 00011.

Il a donc bien retrouvé le message originel qu'Alice voulait lui transmettre.

Selon la théorie de Shannon, si la clef est aussi longue que le message et changée à chaque nouvelle utilisation, alors cet algorithme utilisant le code de Vernam est sûr. En effet, lorsque Alice crypte son message, celui-ci devient aussi aléatoire que la clef. Il ne contient donc aucune information pour toute personne ne connaissant pas la clef. Par contre, si Alice utilise plusieurs fois la même clef ou si la clef est plus petite que le message à crypter, des corrélations vont apparaître à l'intérieur du message transmis. Ce qui donne à un éventuel espion la possibilité d'intercepter de l'information.

En effet, si Alice utilise deux fois la même clef pour crypter deux messages, m_1 et m_2, elle envoie publiquement à Bob (m_1 XOR clef) et (m_2 XOR clef). Si l'espion intercepte les données et leur applique, par exemple, l'opération XOR, elle obtient :

$$\begin{aligned}(m_1\ XOR\ clef)\ XOR\ (m_2\ XOR\ clef)\\ &= [(m_1\ XOR\ m_2)\ XOR\ clef]\ XOR\ clef\\ &= m_1\ XOR\ m_2\end{aligned}$$

Ce qui est une information sur le message.

Tout le problème est donc de transmettre cette fameuse clef sans qu'un espion ne puisse l'intercepter.

La cryptographie quantique permet, sur base seule de la théorie quantique, de transmettre une telle clef en toute sûreté et aucune technologie ne peut, en principe, réussir à la contrer.

4.2 BB84, sans espion

Le protocole que nous étudierons est le protocole BB84 (Bennett & Brassard, 1984) qui est le plus utilisé à l'heure actuelle.

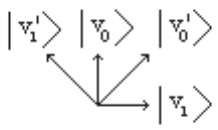
Alice utilise des photons pour transmettre un message à Bob et code ses bits dans un état de polarisation, notons 0 si le photon est polarisé verticalement et 1 s'il est polarisé horizontalement.

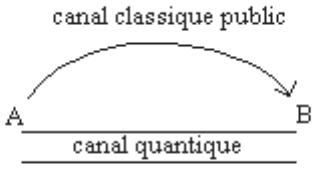
Alice choisit l'une des deux bases suivantes :

$$\begin{cases} |v_0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv \text{polarisation verticale} \\ |v_1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \equiv \text{polarisation horizontale} \\ |v'_0\rangle = \begin{pmatrix} 1' \\ 0' \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \text{polarisation diagonale} \\ |v'_1\rangle = \begin{pmatrix} 0' \\ 1' \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \equiv \text{polarisation antidiagonale} \end{cases}$$

La polarisation de photons permet alors d'envoyer des bits.

Le dispositif est le suivant.





Alice choisit comme clef une suite quelconque de bits et elle choisit aléatoirement la base dans laquelle elle va envoyer chacun de ses photons.

Un exemple. Alice envoie : 0, 0', 1 (c'est à dire vertical, diagonal et horizontal). Bob choisit aléatoirement la base avec laquelle il mesure la polarisation de ces photons. Supposons qu'il choisisse les bases $(|v_0\rangle\ ,|v_1\rangle)$; $(|v_0\rangle\ ,|v_1\rangle)$; $(|v_0'\rangle\ ,|v_1'\rangle)$. Les deux dernières bases choisies par Bob sont donc différentes de celles d'Alice.

Les mesures possibles de Bob sont alors :

- 0 ($P = 1$ car Alice et Bob ont la même base) pour le premier photon;
- 0 ou 1 ($P = 1/2$ pour chaque résultat possible) pour le deuxième photon;
- $0'$ ou $1'$ ($P = 1/2$ pour chaque résultat possible) pour le troisième photon.

Ensuite, Alice et Bob passent à la suite du protocole, le *sifting*. Alice et Bob se disent, sur un canal public, quelles bases ils ont utilisées, et ils se débarrassent des bases mal choisies (car sinon Bob n'est pas sûr de son résultat concorde avec ce qu'a envoyé Alice). On parle alors de clef tamisée.

TAB. 4.1 – Tableau récapitulatif

Bases d'Alice	$(\|v_0\rangle, \|v_1\rangle)$	$(\|v'_0\rangle, \|v'_1\rangle)$	$(\|v_0\rangle, \|v_1\rangle)$
Photons envoyés par Alice	0	0	1
Bases de Bob	$(\|v_0\rangle, \|v_1\rangle)$	$(\|v_0\rangle, \|v_1\rangle)$	$(\|v'_0\rangle, \|v'_1\rangle)$
Photons reçus par Bob	0	0,1	0,1
Probabilité de recevoir le bon photon	1	1/2, 1/2	1/2, 1/2

Dans notre exemple, il laisse donc tomber les deux dernières mesures.

Il convient donc de transmettre un nombre de photons bien plus important que dans cet exemple pour avoir à la fin une clef suffisamment longue.

4.3 BB84, avec espion

Intéressons-nous au cas où un espion essaierait de connaître cette clef.

Appelons cet espion Ève (E).

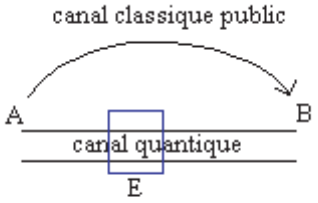
Nous supposons ici qu'Ève ne peut mener qu'une attaque passive sur le canal classique et donc ne peut pas modifier les messages qu'Alice et Bob doivent s'échanger par ce canal classique pour compléter le protocole. On dit que le canal est authentifié. De plus, on suppose qu'Ève ne coupe pas le canal quantique entre Alice et Bob, son but étant de connaître (au moins le plus possible) la clef transmise par Alice à Bob sans se faire remarquer. Toutefois Ève devra, pour obtenir une information quelconque, faire une mesure sur ces photons, porteurs de bits, ou effectuer une tranfsormation. Or c'est ici que la mécanique quantique intervient : *toute mesure d'un état le perturbe* et Ève pourra donc être détectée par Alice et Bob.

En effet, quel que soit le stratagème utilisé, Ève devra effectuer une mesure de la polarisation des photons ou une tranformation sur les photons et donc induira des changements d'états de polarisation des photons qui pourront être détectés par Alice et Bob.

Selon l'attaque utilisée, Ève pourra retirer une certaine quantité d'information ; Bob en aura alors d'autant moins.

Nous pourrons calculer la probabilité d'erreur maximale acceptée par Bob et Alice avant d'abandonner le protocole. En effet, à partir de leur clef tamisée, Alice et Bob utiliseront une partie de leurs photons, compareront les états de polarisation mesurés et détermineront alors cette probabilité d'erreur, donnée par :

$$P_{\text{erreur}} = \frac{\text{nombre de résultats différents}}{\text{nombre de photons}} \tag{4.1}$$



Exemple : Alice envoie 2000 photons en choisissant aléatoirement les bases et la polarisation de chaque photon. Bob mesure les 2000 photons qu'il reçoit ; Ève a mesuré certains de ces photons et a donc induit certaines erreurs.

Ensuite, Alice et Bob comparent leurs bases et éliminent celles qui ne sont pas les mêmes. Bob a choisit une fois sur deux la mauvaise base, il leur reste donc 1000 photons. Ils en utilisent par exemple 250 pour calculer leur probabilité d'erreur. Ils se communiquent par le canal public les résultats, et trouvent P_{erreur}. La communication de ces résultats ne pose pas problème s'ils rejettent les photons dévoilés pour construire la clef.

Supposons que 25 photons parmi ces 250 sont faux alors qu'ils ont utilisé la même base.

Alors

$$P_{\text{erreur}} = \frac{25}{250} = 0.1$$

Si cette probabilité est inférieure à une borne que l'on calculera, ils utiliseront les 750 photons restants pour la clef. Sinon, ils savent qu'Ève a trop d'information et ils recommencent le protocole.

Nous avons donc, par la mécanique quantique seulement, un moyen sûr de transmettre une clef (ou en tout cas si nous arrivons à l'envoyer, nous sommes sûrs que Ève n'a pas assez d'information pour pouvoir l'utiliser).

4.4 Théorème central

Comment cette P_{erreur} limite est-elle déterminée ? Et pourquoi Alice et Bob acceptent-ils d'utiliser une clef alors qu'Ève a un peu d'information ?

La théorie de l'information définit les informations mutuelles, I_{AB} (entre Alice et Bob) et I_{AE} (entre Alice et Ève). Ces deux quantités sont calculées à partir de cette P_{erreur}. La P_{erreur} limite est la probabilité pour laquelle $I_{AE} = I_{AB}$.

Alice et Bob acceptent de s'envoyer la clef à la condition que $I_{AB} \geq I_{AE}$, c'est-à-dire que Ève ait moins d'information que Bob. En effet, il existe un théorème disant que si $I_{AB} \geq I_{AE}$, il est toujours possible à Alice et Bob de s'envoyer une clef au moyen de la cryptographie classique.

Théorème 1 *Si $I_{AB} \geq I_{AE}$, alors il existe un protocole de communication classique permettent à Alice et Bob de distiller une clef secrète.*

Nous étudierons deux techniques d'espionnages, dites attaques :

1. Intercept and resend (non optimal)
2. Cloning (optimal)

Aucune de ces deux attaques n'est parfaite et Alice et Bob pourront toujours détecter la présence d'un espion.

4.5 Intercept and resend

Ève va placer sur le canal quantique un polariseur à orientation variable (pour le choix de la base) suivi d'un photo-détecteur. Elle va donc intercepter certains photons, les mesurer, puis envoyer à Bob des photons dont l'état de polarisation est celui qu'elle a mesuré. Si Ève a choisi la même base qu'Alice, elle ne sera pas détectée car l'état de polarisation du photon ne sera pas perturbé. Par contre, si Ève choisit une base différente, elle aura une chance égale de mesurer une polarisation ou l'autre ($p = 1/2$) et aura de plus perturbé l'état.

La suite dépend de Bob. Si Bob a choisi une base différente de celle d'Alice, cette mesure sera de toute façon abandonnée. S'il utilise la même base qu'Alice et Ève, rien ne permet de détecter l'intrusion d'Ève. Si Alice et Bob utilisent la même base et Ève une base différente, Ève aura perturbé le photon envoyé et Bob aura une chance sur deux d'avoir une mesure erronée et l'erreur est détectable.

4.5.1 Le protocole en résumé

Alice envoie une séquence de photons à Bob en choisissant aléatoirement d'envoyer un 1 ou un 0 dans la base H/V ou D/A. Bob, quant à lui, choisit aléatoirement de mesurer le photon reçu dans la base H/V ou D/A. Entre eux, se trouve une espionne, Ève, qui intercepte certains photons avec une probabilité ω, mesure leur polarisation en choisissant aléatoirement une base et les renvoie à Bob dans l'état de polarisation qu'elle a mesuré. À la place des photons qu'elle ne mesure pas, elle met aléatoirement un 0 ou un 1 dans sa chaîne de bits. Ensuite, Alice et Bob s'échangent de manière classique les bases qu'ils ont utilisées, suppriment dans leur chaîne de bits ceux pour lesquels ils ont utilisé des bases différentes. Dans les bits restants, ils prennent un petit échantillon de bits et comptent le nombre d'erreurs qu'ils ont, bien qu'ils aient choisi la même base pour mesurer le photon. À partir de ce nombre d'erreurs, ils peuvent déterminer la quantité maximale d'information que possède Ève.

4.5.2 Calculs des informations mutuelles entre Alice et Bob et entre Alice et Ève.

- Soient x l'état de polarisation qu'envoie Alice, y ce que reçoit Bob et z ce qu'espionne Ève. Les valeurs possibles de x, y et z sont : x, y, z = {0,1}.
- On sait que l'information mutuelle entre Alice et Bob vaut

$$I_{AB} = H(A:B) = \sum_{x,y} p(x,y) \log_2 \frac{p(x,y)}{p(x)p(y)} \tag{4.2}$$

où $p(x) = \sum_y p(x,y)$ et $p(y) = \sum_x p(x,y)$.

De plus, on a : $p(x,y) = p(x)p(y|x)$.

$p(x) = \frac{1}{2}$

– On se trouve dans le cas où tous les photons qui ont été mesurés dans une mauvaise base ont été éliminés.

1. $\underline{p(z|x)}$
   – $p(0|0)$: probabilité qu'Ève mesure un 0 sachant qu'Alice a envoyé un 0. Deux cas se présentent. Soit Ève mesure le photon, soit elle ne le mesure pas.
     (a) Ève fait la mesure. Alors,

$$p(0|0) = \omega\frac{1}{2}\left(1 + \frac{1}{2}\right)$$

     Elle a une probabilité ω de choisir de faire la mesure, une probabilité $1/2$ de choisir la bonne base. Si elle choisit la bonne base, elle a une probabilité 1 d'avoir un 0 ou si elle choisit la mauvaise base, elle a une probabilité $1/2$ d'obtenir un 0.
     (b) Ève ne fait pas de mesure. Alors,

$$p(0|0) = (1 - \omega)\frac{1}{2}$$

     Elle a une probabilité $(1 - \omega)$ de choisir de ne pas faire la mesure et une probabilité $1/2$ de choisir de mettre un 0 dans sa chaîne de bits.
     $\Rightarrow p(z = 0|x = 0) = \frac{\omega}{2}\left(1 + \frac{1}{2}\right) + \frac{1}{2}(1 - \omega)$
     $\Rightarrow p(0|0) = \frac{1}{2} + \frac{\omega}{4}$
   – $p(1|0)$: probabilité qu'Ève mesure un 1 sachant qu'Alice a envoyé un 0. Deux cas se présentent. Soit Ève mesure le photon, soit elle ne le mesure pas.
     (a) Ève fait la mesure :

$$p(1|0) = \omega\frac{1}{2}\left(0 + \frac{1}{2}\right)$$

     Elle a une probabilité ω de choisir de faire la mesure, une probabilité $1/2$ de choisir la bonne base. Si elle choisit la bonne base, elle a une probabilité 0 d'avoir un 1 ou si elle choisit la mauvaise base, elle a une probabilité $1/2$ d'obtenir un 1.

(b) Ève ne fait pas de mesure :

$$p(1|0) = (1-\omega)\frac{1}{2}$$

Elle a une probabilité $(1-\omega)$ de choisir de ne pas faire la mesure et une probabilité $1/2$ de choisir de mettre un 1 dans sa chaîne de bits.

$$\Rightarrow p(z=1|x=0) = \frac{1}{2} - \frac{\omega}{2} + \frac{\omega}{4}$$
$$\Rightarrow p(1|0) = \frac{1}{2} - \frac{\omega}{4}$$
$$\Rightarrow \begin{cases} p(0|0) = p(1|1) = \frac{1}{2} + \frac{\omega}{4} \\ p(1|0) = p(0|1) = \frac{1}{2} - \frac{\omega}{4} \end{cases}$$

Remarque 1 *Les limites pour* $\omega \rightarrow 0$ *des l'informations conditionnelles, sont* $1/2$ *et* $1/2$.

C'est une valeur tout à fait logique puisque, si Ève ne mesure rien, elle va choisir aléatoirement de mettre un 0 ou un 1 dans sa chaîne de bits.
Considérons à présent les limites pour $\omega \rightarrow 1$ des informations conditionnelles, on trouve $3/4$ et $1/4$. Ce qui est tout aussi logique puisque, si Ève mesure tous les photons, elle a une chance sur deux d'avoir choisi la bonne base et une chance sur deux d'avoir la mauvaise, auquel cas elle a encore une chance sur deux de recevoir le bon état de polarisation ou non.

Entre Alice et Ève

$$p(0,0) = p(1,1) = \frac{1}{4} + \frac{\omega}{8} \tag{4.3}$$
$$p(1,0) = p(0,1) = \frac{1}{4} - \frac{\omega}{8} \tag{4.4}$$

2. $\underline{p(y|x)}$
   - $p(0|0)$: probabilité que Bob mesure un 0 sachant qu'Alice a envoyé un 0. Deux cas se présentent. Soit Ève a mesuré le photon, soit elle ne l'a pas mesuré avant de l'envoyer à Bob.
     (a) Ève fait la mesure :

$$p(0|0) = \omega\frac{1}{2}\left[1 + \frac{1}{2}\left(\frac{1}{2} + \frac{1}{2}\right)\right]$$

Elle a une probabilité ω de choisir de faire la mesure, une probabilité 1/2 de choisir la bonne base. Si elle choisit la bonne base, elle renvoie le bon photon et Bob a une probabilité 1 d'avoir un 0 ou si elle choisit la mauvaise base, elle a une probabilité 1/2 d'obtenir un 0 ou un 1 et dans chacun de ces cas, Bob a une probabilité 1/2 de recevoir un 0.

(b) Ève ne fait pas de mesure :

$$p(0|0) = (1-\omega)1$$

Elle a une probabilité (1-ω) de choisir de ne pas faire la mesure et Bob a une probabilité de 1 d'obtenir un 0.

$$\Rightarrow p(y=0|x=0) = 1-\omega+\frac{\omega}{2}\frac{3}{2}$$
$$\Rightarrow p(0|0) = 1-\frac{\omega}{4}$$

– $p(1|0)$: probabilité que Bob mesure un 1 sachant qu'Alice a envoyé un 0. Deux cas se présentent. Soit Ève a mesuré le photon, soit elle ne l'a pas mesuré avant de l'envoyer à Bob.

(a) Ève a fait la mesure :

$$p(1|0) = \omega\frac{1}{2}\left(0+\frac{1}{2}\left(\frac{1}{2}+\frac{1}{2}\right)\right)$$

Elle a une probabilité ω de choisir de faire la mesure, une probabilité 1/2 de choisir la bonne base. Si elle choisit la bonne base, elle a une probabilité 0 d'avoir un 1 ou si elle choisit la mauvaise base, elle a une probabilité 1/2 d'obtenir un 0 ou un 1 et, dans chacun des cas, Bob a une probabilité 1/2 de recevoir un 1 .

(b) Ève ne fait pas de mesure :

$$p(1|0) = (1-\omega)0$$

Elle a une probabilité $(1-\omega)$ de choisir de ne pas faire la mesure et Bob a une probabilité 0 de mesurer un 1.

$$\Rightarrow p(y=1|x=0) = \frac{\omega}{4}$$

$$\Rightarrow \begin{cases} p(0|0) = p(1|1) = 1-\frac{\omega}{4} \\ p(1|0) = p(0|1) = \frac{\omega}{4} \end{cases}$$

Remarque 2 *Les limites pour $\omega \rightarrow 0$ des informations conditionnelles, sont 1 et 0.*

C'est une valeur tout à fait logique puisque si Ève ne mesure rien, sachant qu'Alice a envoyé un photon dans un état de polarisation, Bob va recevoir avec une probabilité 1 un photon dans le même état de polarisation et avec une probabilité 0 un photon dans un autre état de polarisation.
Considérons maintenant les limites pour $\omega \rightarrow 1$ des informations conditionnelles, on trouve 3/4 et 1/4.

Entre Alice et Bob

$$p(0,0) = p(1,1) = \frac{1}{2} - \frac{\omega}{8} \tag{4.5}$$

$$p(1,0) = p(0,1) = \frac{\omega}{8} \tag{4.6}$$

4.5.3 L'information mutuelle entre Alice et Ève

En vertu de la formule (2.19) :

$$I_{AE} = p(0,0)\log_2\frac{p(0,0)}{p(0)p(0)} + p(1,1)\log_2\frac{p(1,1)}{p(1)p(1)} + p(0,1)\log_2\frac{p(0,1)}{p(0)p(1)} + p(1,0)\log_2\frac{p(1,0)}{p(1)p(0)}$$

$$I_{AE} = 2\left[\left(\frac{1}{4}+\frac{\omega}{8}\right)\log_2\left(1+\frac{\omega}{2}\right) + \left(\frac{1}{4}-\frac{\omega}{8}\right)\log_2\left(1-\frac{\omega}{2}\right)\right]$$

$$I_{AE} = \frac{1}{2}\log_2\left(1-\frac{\omega^2}{4}\right) + \frac{\omega}{4}\log_2\left(\frac{1+\frac{\omega}{2}}{1-\frac{\omega}{2}}\right) \tag{4.7}$$

4.5.4 L'information mutuelle entre Alice et Bob

De même,

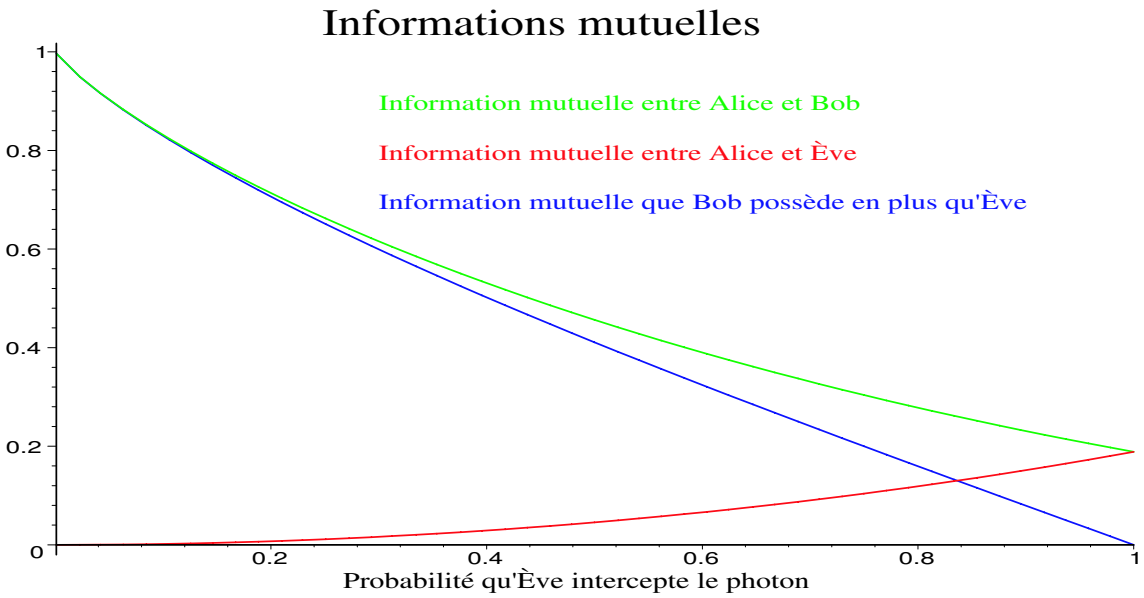
$$I_{AB} = p(0,0)\log_2\frac{p(0,0)}{p(0)p(0)} + p(1,1)\log_2\frac{p(1,1)}{p(1)p(1)} + p(0,1)\log_2\frac{p(0,1)}{p(0)p(1)} + p(1,0)\log_2\frac{p(1,0)}{p(1)p(0)}$$

$$I_{AB} = 2\left[\left(\frac{1}{2} - \frac{\omega}{8}\right)\log_2\left(2 - \frac{\omega}{2}\right) + \frac{\omega}{8}\log_2\left(\frac{\omega}{2}\right)\right]$$

$$I_{AB} = \log_2\left(2 - \frac{\omega}{2}\right) - \frac{\omega}{4}\log_2\left(\frac{4}{\omega} - 1\right) \tag{4.8}$$

4.5.5 Résultats

Les informations mutuelles
$I_{AE} = \frac{1}{2}\log_2\left(1 - \frac{\omega^2}{4}\right) + \frac{\omega}{4}\log_2\left(\frac{1+\frac{\omega}{2}}{1-\frac{\omega}{2}}\right)$
$I_{AB} = \log_2\left(2 - \frac{\omega}{2}\right) - \frac{\omega}{4}\log_2\left(\frac{4}{\omega} - 1\right)$

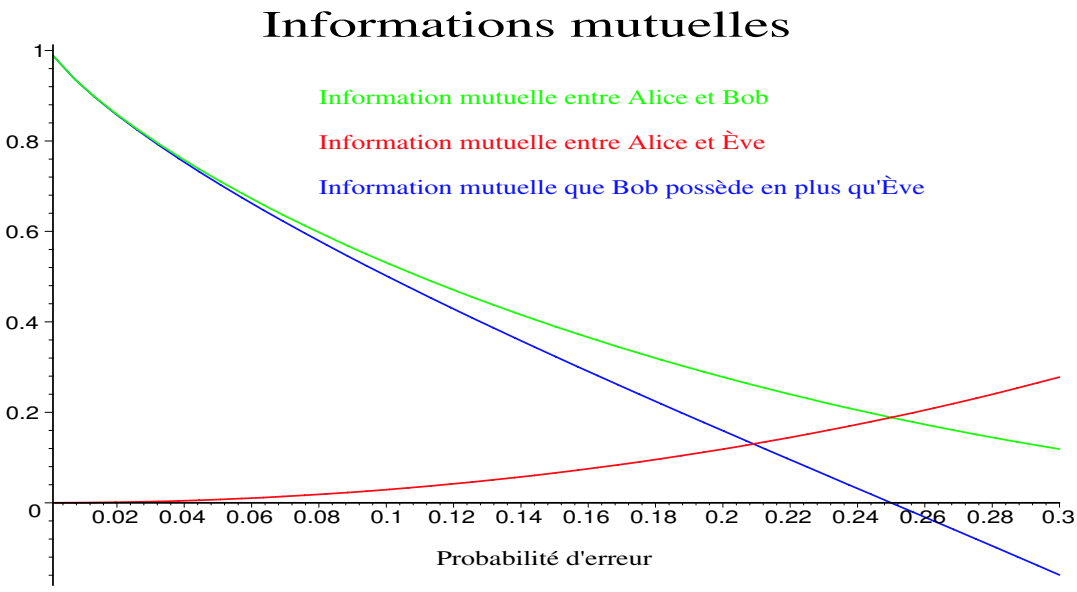


Nous avons évalué ω tel que $I_{AE} = I_{AB}$ à l'aide de Maple[1].

$$I_{AB} = I_{AE} \Leftrightarrow \omega = 1 \tag{4.9}$$

Tant que $\omega < 1$ (ce qui est souvent le cas, Ève ne va pas intercepter tous les photons), le théorème central nous assure qu'Alice et Bob pourront toujours se transmettre une clef.

1. Les calculs sont fournis dans l'annexe D



Cette attaque n'est donc pas très efficace puisque, Ève ne pourra jamais obtenir complètement une clef.

Nous avons aussi montré la proposition suivante.

Proposition 1 *Soit ω la probabilité qu'Ève intercepte un photon en utilisant l'attaque " intercept et resend ".*

1. *Si $\omega < 1$, alors une clef qu'Ève ne pourra jamais connaître pourra être transmise entre Alice et Bob.*
2. *Si $\omega = 1$, alors l'envoi d'une clef est abandonné.*

La probabilité d'erreur pour $\omega = 1$ est $p_{erreur} = 25$ %.

En effet, $\begin{cases} p(0,0) = p(1,1) = \frac{1}{2} - \frac{\omega}{8} \\ p(1,0) = p(0,1) = \frac{\omega}{8} \end{cases}$ (entre Alice et Bob), nous avons donc un bruit de

$$P_{\text{erreur}} = 2\frac{\omega}{8} \tag{4.10}$$

le bruit étant la probabilité d'erreurs qu'engendre la mesure effectuée par Ève. Ce bruit est la somme des différence des probabilités qu'Alice envoie tel état et que Bob reçoive tel état à $\omega = 0$ et celles à ω. Donc,

$$\begin{aligned} \text{bruit} &= \left[p(0,0)_{|\omega=0} - p(0,0)\right] + \left[p(1,0)_{|\omega=0} - p(1,0)\right] \\ &= \left[\frac{1}{2} - \left(\frac{1}{2} - \frac{\omega}{8}\right)\right] + \left[0 - \frac{\omega}{8}\right] = 2.\frac{\omega}{8} \end{aligned} \tag{4.11}$$

Pour $\omega = 1$, nous retrouvons la valeur 1/4.

4.6 BB84 dans le cas non idéal

4.6.1 Algorithmes de correction d'erreur

Le protocole que nous venons de décrire est donc sûr dans le cas idéal, c'est-à-dire sans les bruits inhérents au canal (différents des bruits engendrés par la mesure d'Ève), à la condition qu'Alice envoie un nombre suffisamment grand de photons. En effet, pour ne pas être détectée, Ève devrait choisir à chaque fois la même base qu'Alice, ce qui peut arriver au mieux $\frac{1}{2^n}$ fois où n est le nombre de bits de la clef tamisée. Si Alice et Bob ont une clef tamisée de 1000 bits, Ève passera inaperçue dans environ 1 cas sur 10^{300}.

Dans le cas idéal, si Ève effectue des mesures, alors Alice et Bob auront un taux d'erreur non nul dans leur clef tamisée. Mais, une autre source d'erreur est, comme nous l'avons dit plus haut, le bruit lié au canal de communication. Il devient donc possible pour Ève de passer inaperçue si elle ne mesure que peu de photons de telle sorte que les perturbations qu'elle engendre soient du même ordre de grandeur que le bruit du canal de communication. La clef tamisée devra donc être traitée pour supprimer à la fois le bruit du canal et les éléments d'information détenus par Ève et cela de manière classique.

Alice et Bob vont devoir utiliser un algorithme de correction d'erreur car il est primordial pour eux de posséder la même clef même au prix d'un petit gain d'information pour Ève. Ils supprimeront l'information que possède Ève dans un deuxième temps. Étudions une version simplifiée d'un algorithme qui permettrait à Alice et Bob d'avoir la même clef. Alice choisit aléatoirement des paires de bits et divulgue publiquement le numéros de ces bits et leur somme XOR. Si Bob obtient le même résultat, ils gardent le premier bit de la paire et jettent le second. Si Bob n'obtient pas le même résultat, ils jettent les deux bits. Cet algorithme permet de faire tendre le taux de différences entre les clefs d'Alice et Bob vers 0.

Maintenant qu'Alice et Bob ont la même clef, ils vont essayer de réduire l'information que possède Ève. Ils vont alors utiliser un algorithme dit de *privacy amplification*. Considérons à nouveau le cas le plus simple. Alice choisit à nouveau des paires de bits dont elle prend leur somme XOR, mais cette fois-ci, elle annonce seulement le numéro des bits. Alice et Bob remplacent simplement la valeur de chacun de ces deux bits par la valeur de leur somme

XOR. Ainsi, Alice et Bob n'engendrent pas de nouvelles différences entre leur clef et réduisent l'information d'Ève au détriment bien sûr de la longueur de leur clef. En effet, si Ève ne connaît que la valeur du premier bit mais pas du deuxième, elle n'a aucune information sur leur somme XOR.

Alice et Bob disposent finalement d'une clef sans erreur à propos de laquelle Ève n'a aucune information.

4.6.2 Les sources de bruit

Il y a plusieurs sources de bruits : la source lumineuse en elle-même, les appareils de mesure et le canal, c'est-à-dire le bruit thermique et les interactions avec le milieu.

La source de lumière Nous avons considéré le cas où Alice envoyait photon par photon à Bob. Ceci veut dire que chaque impulsion lumineuse qu'elle envoie ne contient qu'un seul photon. En effet, si l'impulsion contient plus d'un photon, il suffit à Ève de prélever l'information sur un des photons et de laisser passer l'autre ou les autres photons. Cette attaque est connue sous le nom de *beam splitting attack*. Dans ce cas, Alice et Bob ne s'apercevraient jamais qu'ils sont espionnés.

Les appareils de mesure. Les photo-détecteurs ne sont pas efficaces à 100%. Il peut arriver qu'ils ne détectent pas un photon ou en comptabilisent un alors qu'il n'existe pas. C'est ce qu'on appelle le *dark count*.

Le canal de communication. Il peut y avoir des interactions avec le milieu, que le photon se propage à l'air libre ou dans une fibre optique. Ces interactions ont pour effet d'absorber le photon ou de modifier ses propriétés (polarisation, phase, ...). Le milieu peut aussi émettre des photons spontanément.

4.6.3 Cas réel

Un canal réel est naturellement bruité. Le bruit est caractérisé par la valeur moyenne du taux d'erreur par bit transmis QBER (pour Quantum Bit Error Rate).

$$QBER = \frac{N_{erreur}}{N_{erreur} + N_{correct}}$$

où N_{erreur} (nombre d'erreurs) $+N_{correct}$ (nombre de bits corrects) $= N$ (nombre de bits émis).

L'information mutuelle entre Alice et Bob, quand il n'y a pas d'espion, n'est pas de 1 mais vaut

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

Lorsque le canal est bruité, Alice et Bob ne peuvent pas connaître l'origine des erreurs. Ils peuvent bien sûr connaître la statistique du bruit du canal mais Ève aussi et elle peut donc imiter le bruit naturel du canal. L'objectif d'Ève est donc bien de gagner le maximum d'information en n'ajoutant pas de bruit supplémentaire au bruit naturel QBER du canal.

Reprenons le cas de l'attaque intercept and resend, lorsque $\omega = 1$, Ève engendre un bruit de $\frac{1}{4}$. Or un canal de communication ne présente jamais un tel bruit. Ève sera donc très facilement détectée. Elle va donc devoir contrôler ce paramètre ω de telle sorte que le bruit qu'elle produit reste inférieur au niveau de bruit QBER.

4.7 "Cloning" ou attaque par duplication

4.7.1 Prélude : Systèmes quantiques à deux états

L'attaque du cloning et son analyse sont basés sur les systèmes quantiques à deux états.

Soit $\mathcal{E}_1$ l'espace vectoriel des états d'une particule 1.
Soit $\mathcal{E}_2$ l'espace vectoriel des états d'une particule 2.

Si nous voulons étudier ces deux particules interagissant comme un seul système quantique, l'espace des états de ce nouveau système est le produit tensoriel de $\mathcal{E}_1$ et $\mathcal{E}_2$ et les éléments de cet espace sont des tenseurs d'ordre deux.

$$\mathcal{E}_{12} = \mathcal{E}_1 \otimes \mathcal{E}_1$$

Soient $|\psi_1\rangle \in \mathcal{E}_1$ et $|\psi_2\rangle \in \mathcal{E}_2$. Nous sommes amenés à prendre le produit tensoriel, dfini par:

$$|\psi_1\rangle \otimes |\psi_2\rangle \equiv |\psi_1\rangle\,|\psi_2\rangle \equiv |\psi_1\psi_2\rangle \tag{4.12}$$

Remarque 3 *Un bit d'information est appelé qubit s'il est dans une superposition quantique de 0 et de 1.*

On le représente par un vecteur normalisé $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ dans $\mathbb{H}$, où α, $\beta \in \mathbb{C}$ et $||\alpha||^2 + ||\beta||^2 = 1$. Il s'agit donc d'une superposition de deux états orthogonaux.

Si $|v_{j\,1}\rangle$est une base orthonormée de $\mathcal{E}_1$ et $|v_{j\,2}\rangle$ une base orthonormée de $\mathcal{E}_2$, alors $|v_{j\,1}\rangle\,|v_{j\,2}\rangle$ est une base orthonormée de $\mathcal{E}_{12}$. Un élément général de $\mathcal{E}_{12}$ est donc

$$|\phi\rangle \in \mathcal{E}_{12} \Leftrightarrow |\phi\rangle = c^{j_1 j_2}|v_{j_1}\rangle|v_{j_2}\rangle \quad , \quad c^{j_1 j_2} \in \mathbb{C} \tag{4.13}$$

La même chose peut être faite pour les duals de $\mathcal{E}_1$ et $\mathcal{E}_2$. On a de la même façon.

$$\langle\phi| \in \mathcal{E}_{12}^* \Leftrightarrow \langle\phi| = c^{j_1 j_2}\langle v_{j_1}|\langle v_{j_2}| \tag{4.14}$$

Le même isomorphisme existe entre $\mathcal{E}_{12}$ et $\mathcal{E}_{12}^*$ que celui entre $\mathcal{E}$ et $\mathcal{E}^*$.

Définition 1 *Le produit scalaire sur* $\mathcal{E}_{12}$ *est*
$\forall|\phi_1\rangle,|\psi_1\rangle \in \mathcal{E}_1$, $\forall|\phi_2\rangle,|\psi_2\rangle \in \mathcal{E}_2$,

$$\langle\phi_1\phi_2|\psi_1\psi_2\rangle_{12} = \langle\phi_1|\psi_1\rangle_1\langle\phi_2|\psi_2\rangle_2 \tag{4.15}$$

Cette définition s'étend par linéarité à tout tenseur $\in \mathcal{E}_{12}$.

$$\langle\phi|\psi\rangle = \langle c^{i_1 i_2} v_{i_1} v_{i_2}| d^{j_1 j_2} v_{j_1} v_{j_2}\rangle = \left(c^{i_1 i_2}\right)^* d^{j_1 j_2}\langle v_{i_1}|v_{j_1}\rangle\langle v_{i_2}|v_{j_2}\rangle = \sum_{i_1 i_2}\left(c^{i_1 i_2}\right)^* d^{i_1 i_2} \tag{4.16}$$

Un opérateur $A_1 : \mathcal{E}_1 \to \mathcal{E}_1$ possède une extension homomorphique à un opérateur $\mathcal{E}_{12} \to \mathcal{E}_{12}$ défini par :

$$A_1|\psi_1\psi_2\rangle \equiv (A_1|\psi_1\rangle) \otimes |\psi_2\rangle \tag{4.17}$$

Il est de même pour un opérateur $A_2 : \mathcal{E}_2 \to \mathcal{E}_2$.

La même extension existe pour les bras.

Définition 2 *L'extension homomorphique de tout bra* $\langle\psi_1| : \mathcal{E}_1 \to \mathbb{C}$ *à* $\langle\psi_2| : \mathcal{E}_{12} \to \mathcal{E}_2$ *est définie par.*

$$\langle\phi_1|\psi_1\psi_2\rangle \equiv \langle\phi_1|\psi_1\rangle|\psi_2\rangle \tag{4.18}$$

De même, l'extension de tout bra $\langle\psi_2| : \mathcal{E}_2 \to \mathbb{C}$ *à* $\langle\psi_2| : \mathcal{E}_{12} \to \mathcal{E}_1$ *est définie par.*

$$\langle\phi_2|\psi_1\psi_2\rangle \equiv \langle\phi_2|\psi_2\rangle|\psi_1\rangle \tag{4.19}$$

$\forall|\psi\rangle_1 \in \mathcal{E}_1$, $\forall|\phi\rangle_2$, $|\psi\rangle_2 \in \mathcal{E}_2$

Cette définition s'étend encore une fois à tout tenseur de $\mathcal{E}_{12}$ par linéarité.

4.7.2 Cloning: "l'attaque des clones"

Alice envoie un photon dans un état quantique $|\phi\rangle$ (c'est-à-dire soit $|v_0\rangle$, soit $|v_1\rangle$, soit $|v_0'\rangle$ ou soit $|v_1'\rangle$). Ève va créer un clone de chaque photon transmis et renvoie un photon (supposé identique) à Bob. Remarquons qu'Ève n'a pas encore fait de mesure et n'a donc pas choisi de base.

Ensuite, Alice et Bob se communiquent leurs bases et ne gardent que celles qu'ils ont en commun. Ève, ayant écouté cela, peut donc choisir à chaque fois la bonne base pour mesurer ses photons, ce qui représente déjà un gros avantage par rapport à la première attaque.

Cette attaque serait sans défaut si l'on pouvait cloner parfaitement des états quantiques. Mais à nouveau, la mécanique quantique introduit la restriction suivante.

Théorème de non-clonage 1 *On ne peut cloner un ensemble d'états non orthogonaux.*
Donc, comme l'état envoyé est inconnu, il est impossible de cloner parfaitement un état[2]*.*

Comme toutes les bases ont été choisies, nous pouvons choisir une base unique de notre espace des états. Prenons la base ortonormée ($|0\rangle$,$|1\rangle$).

Ève utilise pour le clonage un état, appelons-le $|0\rangle_E$. Elle reçoit d'Alice l'état $|\phi\rangle_A$ ($= |0\rangle_A$ ou $= |1\rangle_A$). Ce dernier va interagir avec le photon-clone $|0\rangle_E$.

2. La démonstration de ce théorème est fournie dans l'annexe A

Dans l'espace tensoriel $\mathcal{E}_A \otimes \mathcal{E}_E$, l'état que reçoit Ève est donc $|\phi\rangle_A|0\rangle_E$.

Ève va alors utiliser l'opérateur unitaire $U : \mathcal{E}_{AE} \to \mathcal{E}_{AE}$, défini par :

$$U\left(|0\rangle_A|0\rangle_E\right) = |0\rangle_A|0\rangle_E \tag{4.20}$$
$$U\left(|1\rangle_A|0\rangle_E\right) = |1\rangle_A|1\rangle_E \tag{4.21}$$

Donc, U copie dans $\mathcal{E}_E$ le photon d'Alice.

Constatons que cela ne fonctionne pas si l'état reçu n'est pas perpendiculaire à $|0\rangle_E$. Rappelons que $|0\rangle_E$ est choisi une fois pour toutes par Ève au départ et n'est donc pas nécessairement perpendiculaire aux états arrivants.

Par exemple,

$$|\phi\rangle_A = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{4.22}$$

Alors, l'action de U donne

$$|\phi\rangle_{AE} = U\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle\right) = \frac{1}{\sqrt{2}}U\left(|00\rangle + |10\rangle\right) = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \tag{4.23}$$

par linéarité de U. Mais ce que Ève souhaite, ce serait un état sortant $|\phi\rangle_{AE}$ tel que

$$|\phi\rangle_{AE} = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) \tag{4.24}$$

Ève ne peut donc cloner un état quelconque.

L'état à la sortie est en général :

$$|\phi\rangle_{AE} = c_{00}|00\rangle + c_{10}|10\rangle + c_{01}|01\rangle + c_{11}|11\rangle \tag{4.25}$$

où

$$|c_{00}|^2 + |c_{10}|^2 + |c_{01}|^2 + |c_{11}|^2 = 1 \tag{4.26}$$

puisque $|\phi\rangle_{AE}$ est normé.

Remarque 4 $\{|00\rangle,|10\rangle,|01\rangle,|11\rangle\}$ *est une base orthonormée de* $\mathcal{E}_{AE}$.

En effet,

$$\langle i_A i_E | j_A j_E \rangle = \langle i_A | j_A \rangle \langle i_E | j_E \rangle = \delta_{i_A j_A} \delta_{i_E j_E} \tag{4.27}$$

où i_A,i_E,j_A,$j_E = \{0,1\}$.

Comme la première tranformation n'est pas efficace, Ève utilise une autre transformation unitaire.

Définissons plusieurs bases :

– la base z (polarisation verticale/horizontale) :

$$\{|0\rangle_z, |1\rangle_z\} \tag{4.28}$$

– la base x (polarisation diagonale/anti-diagonale) :

$$|0\rangle_x = \frac{|0\rangle_z + |1\rangle_z}{\sqrt{2}} \tag{4.29}$$

$$|1\rangle_x = \frac{|0\rangle_z - |1\rangle_z}{\sqrt{2}} \tag{4.30}$$

– la base y :

$$|0\rangle_y = \frac{|0\rangle_z + i|1\rangle_z}{\sqrt{2}} \tag{4.31}$$

$$|1\rangle_y = \frac{|0\rangle_z - i|1\rangle_z}{\sqrt{2}} \tag{4.32}$$

Remarque 5 *On peut montrer que ces états sont en fait les kets propres des opérateurs de Pauli*[3].

Proposition 2 *La meilleure transformation unitaire de clonage est*

$$U : \mathcal{E}_{AE} \to \mathcal{E}_{AE}$$

définie dans la base y par

$$U(|0\rangle_{yA}|0\rangle_{yE}) = |0\rangle_{yA}|0\rangle_{yE} \tag{4.33}$$

$$U(|1\rangle_{yA}|0\rangle_{yE}) = \cos(\theta)|1\rangle_{yA}|0\rangle_{yE} + \sin(\theta)|0\rangle_{yA}|1\rangle_{yE} \tag{4.34}$$

où $\theta \in \left[0, \frac{\pi}{2}\right]$.

3. cf. annexe B

Remarque 6 *Ce θ est un paramètre contrôlé par Ève et mesure la force de l'attaque.*

Si $\theta = 0$, $|1\rangle|0\rangle \rightarrow |1\rangle|0\rangle$: Ève ne fait rien et aucun bruit (aucune perturbation) n'est produit.

Si $\theta = \frac{\pi}{2}$, $|1\rangle|0\rangle \rightarrow |0\rangle|1\rangle$: Ève intercepte toute l'information mais renvoie une erreur à Bob. Cette attaque n'est pas discrète !

Ève doit donc choisir un θ intermédiaire.

Après le clonage, Ève garde le photon qui appartient originellement à son espace $\mathcal{E}_E$, et renvoie à Bob le photon qui appartenait à $\mathcal{E}_A$.

4.7.3 Calculs des informations mutuelles entre Alice et Bob et entre Alice et Ève.

Rappels

- L'information mutuelle entre Alice et Bob vaut

$$I_{AB} = H(A:B) = \sum_{x,y} p(x,y) \log_2 \frac{p(x,y)}{p(x)p(y)} \tag{4.35}$$

$$p(x) = \sum_{y} p(x,y) \tag{4.36}$$

$$p(y) = \sum_{x} p(x,y) \tag{4.37}$$

- De plus

$$p(x,y) = p(x)p(y|x) \tag{4.38}$$

- On a aussi

$$p(x) = \frac{1}{2} \tag{4.39}$$

  où $x = \{0,1\}$.
- Tous les photons qui ont été mesurés dans une mauvaise base ont été éliminés.

– Pour calculer cette information mutuelle, nous déterminons la probabilité que Bob reçoive l'état $|\phi\rangle_B$ sachant qu'Alice a envoyé l'état $|\phi\rangle_A$ ($|0\rangle$,$|1\rangle$). Ce qui revient à calculer

$$|_B\langle\phi|\psi\rangle_{BE}|^2 \tag{4.40}$$

avec

$$|\psi\rangle_{BE} = |\psi\rangle_{AE} = U\left(|\phi\rangle_A|0\rangle_E\right) = c_{00}|00\rangle + c_{10}|10\rangle + c_{01}|01\rangle + c_{11}|11\rangle \tag{4.41}$$

– Le photon-clone utilisé par Ève est préparé dans la base y et le photon envoyé par Alice est soit dans la base x, soit dans la base z.
– Intéressons-nous d'abord au cas où le photon envoyé par Alice est dans la base z et effectuons nos calculs dans la base y.

$$|\psi\rangle_A = \begin{cases} |0\rangle_z \\ |1\rangle_z \end{cases} \tag{4.42}$$

Transformation de base

On a

$$|0\rangle_x = \frac{|0\rangle_z + i|1\rangle_z}{\sqrt{2}} \tag{4.43}$$

$$|1\rangle_x = \frac{|0\rangle_z - i|1\rangle_z}{\sqrt{2}} \tag{4.44}$$

Donc, sous forme matricielle

$$\begin{pmatrix} |0\rangle_y & |1\rangle_y \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} |0\rangle_z & |1\rangle_z \end{pmatrix} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \tag{4.45}$$

Ceci s'inverse facilement en

$$\begin{pmatrix} |0\rangle_z & |1\rangle_z \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} |0\rangle_x & |1\rangle_x \end{pmatrix} \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix} \tag{4.46}$$

On trouve donc:

$$|0\rangle_z = \frac{|0\rangle_y + |1\rangle_y}{\sqrt{2}} \tag{4.47}$$

$$|1\rangle_z = \frac{|0\rangle_y - |1\rangle_y}{\sqrt{2}i} = \frac{i}{\sqrt{2}}\left(-|0\rangle_y + |1\rangle_y\right) \tag{4.48}$$

Entre Alice et Bob

(A) Soit Alice envoie :

$$|0\rangle_z = \frac{|0\rangle_y + |1\rangle_y}{\sqrt{2}} \tag{4.49}$$

On calcule alors l'action de la transformation de clonage :

$$|0\rangle_{zA}|0\rangle_{yE} = \left(\frac{|0\rangle_y + |1\rangle_y}{\sqrt{2}}\right) \otimes |0\rangle_y = \frac{1}{\sqrt{2}}\left(|00\rangle_y + |10\rangle_y\right) \tag{4.50}$$

$$|\phi\rangle_{AE} = U\left(|0\rangle_{zA}|0\rangle_{yE}\right) = U\left(\frac{1}{\sqrt{2}}\left(|00\rangle_y + |10\rangle_y\right)\right) \tag{4.51}$$

$$|\phi\rangle_{AE} = \frac{1}{\sqrt{2}}\left(|00\rangle_y + \cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y\right) \tag{4.52}$$

Déterminons la probabilité que Bob reçoive un 0 sachant qu'Alice a envoyé un 0.

$$|\psi\rangle_B = |0\rangle_{zB} = \frac{1}{\sqrt{2}}\left(|0\rangle_y + |1\rangle_y\right) \tag{4.53}$$

$$P = |{}_B\langle 0_z|\phi\rangle_{BE}|^2 \tag{4.54}$$

$${}_B\langle 0_z|\phi\rangle_{BE} = \frac{1}{2}\left[\left(\langle 0|_y + \langle 1|_y\right)|\left(|0\rangle_{yB}|0\rangle_{yE} + \cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y\right)\right] \tag{4.55}$$

$${}_B\langle 0_z|\phi\rangle_{BE} = \frac{1}{2}\left(|0\rangle_y + \sin(\theta)|1\rangle_y + \cos(\theta)|0\rangle_y\right) \tag{4.56}$$

$$P = \frac{1}{4}\left[(1+\cos(\theta))^2 + (\sin(\theta))^2\right] = \frac{1+\cos(\theta)}{2} \tag{4.57}$$

Déterminons la probabilité que Bob reçoive un 1 sachant qu'Alice a envoyé un 0.

$$|\psi\rangle_B = |1\rangle_{zB} = \frac{1}{\sqrt{2}i}\left(|0\rangle_y - |1\rangle_y\right) \tag{4.58}$$

$$P = |{}_B\langle 1_z|\phi\rangle_{BE}|^2 \tag{4.59}$$

$$ {}_B\langle 1_z|\phi\rangle_{BE} = -\frac{1}{2i}\left[(\langle 0|_y - \langle 1|_y)\,|\,(|00\rangle_y + \cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y)\right] \quad (4.60) $$

$$ {}_B\langle 1_z|\phi\rangle_{BE} = -\frac{1}{2i}\left(|0\rangle_y + \sin(\theta)|1\rangle_y - \cos(\theta)|0\rangle_y\right) \quad (4.61) $$

$$ P = \frac{1}{4}\left[(1-\cos(\theta))^2 + (\sin(\theta))^2\right] = \frac{1-\cos(\theta)}{2} \quad (4.62) $$

(B) Soit Alice envoie

$$ |1\rangle_z = \frac{|0\rangle_y - |1\rangle_y}{\sqrt{2}i} \quad (4.63) $$

On calcule alors l'action de la transformation de clonage :

$$ |1\rangle_{zA}|0\rangle_{yE} = \left(\frac{|0\rangle_y - |1\rangle_y}{\sqrt{2}i}\right) \otimes |0\rangle_y = \frac{1}{\sqrt{2}i}\left(|00\rangle_y - |10\rangle_y\right) \quad (4.64) $$

$$ |\phi\rangle_{AE} = U\left(|1\rangle_{zA}|0\rangle_{yE}\right) = U\left(\frac{1}{\sqrt{2}i}\left(|00\rangle_y - |10\rangle_y\right)\right) \quad (4.65) $$

$$ |\phi\rangle_{AE} = \frac{1}{\sqrt{2}i}\left(|00\rangle_y - \cos(\theta)|10\rangle_y - \sin(\theta)|01\rangle_y\right) \quad (4.66) $$

Déterminons la probabilité que Bob reçoive un 0 sachant qu'Alice a envoyé un 1.

$$ |\psi\rangle_B = |0\rangle_{zB} = \frac{1}{\sqrt{2}}\left(|0\rangle_y + |1\rangle_y\right) \quad (4.67) $$

$$ P = |{}_B\langle 1_z|\phi\rangle_{BE}|^2 \quad (4.68) $$

$$ {}_B\langle 0_z|\phi\rangle_{BE} = \frac{i}{2}\left[(\langle 0|_y + \langle 1|_y)\,|\,(-|00\rangle_y + \cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y)\right] \quad (4.69) $$

$$ {}_B\langle 0_z|\phi\rangle_{BE} = \frac{i}{2}\left(-|0\rangle_y + \sin(\theta)|1\rangle_y + \cos(\theta)|0\rangle_y\right) \quad (4.70) $$

$$ P = \frac{1}{4}\left[(\cos(\theta)-1)^2 + (\sin(\theta))^2\right] = \frac{1-\cos(\theta)}{2} \quad (4.71) $$

Déterminons la probabilité que Bob reçoive un 1 sachant qu'Alice a envoyé un 1.

$$|\psi\rangle_B = |1\rangle_{zB} = \frac{1}{\sqrt{2}i}\left(|0\rangle_y - |1\rangle_y\right) \tag{4.72}$$

$$P = |{}_B\langle 1_z|\phi\rangle_{BE}|^2 \tag{4.73}$$

$${}_B\langle 1_z|\phi\rangle_{BE} = \frac{1}{2}\left[\left(\langle 0|_y - \langle 1|_y\right)|\left(-|00\rangle_y + \cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y\right)\right] \tag{4.74}$$

$${}_B\langle 1_z|\phi\rangle_{BE} = \frac{1}{2}\left(-|0\rangle_y + \sin(\theta)|1\rangle_y - \cos(\theta)|0\rangle_y\right) \tag{4.75}$$

$$P = \frac{1}{4}\left[(1+\cos(\theta))^2 + (\sin(\theta))^2\right] = \frac{1+\cos(\theta)}{2} \tag{4.76}$$

Les probabilités conditionnelles sont donc

$$p(\text{Bob mesure } 0_z|\text{Alice envoie } 0_z) = \frac{1+\cos(\theta)}{2} \tag{4.77}$$

$$p(\text{Bob mesure } 0_z|\text{Alice envoie } 1_z) = \frac{1-\cos(\theta)}{2} \tag{4.78}$$

$$p(\text{Bob mesure } 1_z|\text{Alice envoie } 0_z) = \frac{1-\cos(\theta)}{2} \tag{4.79}$$

$$p(\text{Bob mesure } 1_z|\text{Alice envoie } 1_z) = \frac{1+\cos(\theta)}{2} \tag{4.80}$$

Entre Alice et Ève

(A) Soit Alice envoie

$$|0\rangle_z = \frac{|0\rangle_y + |1\rangle_y}{\sqrt{2}} \tag{4.81}$$

On calcule alors l'action de la transformation de clonage :

$$|0\rangle_{zA}|0\rangle_{yE} = \left(\frac{|0\rangle_y + |1\rangle_y}{\sqrt{2}}\right) \otimes |0\rangle_y = \frac{1}{\sqrt{2}}\left(|00\rangle_y + |10\rangle_y\right) \tag{4.82}$$

$$|\phi\rangle_{AE} = U\left(|0\rangle_{zA}|0\rangle_{yE}\right) = U\left(\frac{1}{\sqrt{2}}\left(|00\rangle_y + |10\rangle_y\right)\right) \tag{4.83}$$

$$|\phi\rangle_{AE} = \frac{1}{\sqrt{2}}\left(|00\rangle_y + \cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y\right) \tag{4.84}$$

Déterminons la probabilité qu' Ève reçoive un 0 sachant qu'Alice a envoyé un 0.

$$|\psi\rangle_E = |0\rangle_{zE} = \frac{1}{\sqrt{2}}\left(|0\rangle_y + |1\rangle_y\right) \tag{4.85}$$

$$P = |{}_E\langle 0_z|\phi\rangle_{AE}|^2 \tag{4.86}$$

$${}_E\langle 0_z|\phi\rangle_{AE} = \frac{1}{2}\left[\left(\langle 0|_y + \langle 1|_y\right)|\left(|0\rangle_{yA}|0\rangle_{yE} + \cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y\right)\right] \tag{4.87}$$

$${}_E\langle 0_z|\phi\rangle_{AE} = \frac{1}{2}\left(|0\rangle_y + \sin(\theta)|0\rangle_y + \cos(\theta)|1\rangle_y\right) \tag{4.88}$$

$$P = \frac{1}{4}\left[(1+\sin(\theta))^2 + (\cos(\theta))^2\right] = \frac{1+\sin(\theta)}{2} \tag{4.89}$$

Détermninons la probabilité qu' Ève reçoive un 1 sachant qu'Alice a envoyé un 0.

$$|\psi\rangle_E = |1\rangle_{zE} = \frac{1}{\sqrt{2}i}\left(|0\rangle_y - |1\rangle_y\right) \tag{4.90}$$

$$P = |{}_E\langle 1_z|\phi\rangle_{AE}|^2 \tag{4.91}$$

$${}_E\langle 1_z|\phi\rangle_{AE} = \frac{i}{2}\left[\left(\langle 0|_y - \langle 1|_y\right)|\left(|00\rangle_y + \cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y\right)\right] \tag{4.92}$$

$${}_E\langle 1_z|\phi\rangle_{AE} = \frac{i}{2}\left(|0\rangle_y - \sin(\theta)|0\rangle_y + \cos(\theta)|1\rangle_y\right) \tag{4.93}$$

$$P = \frac{1}{4}\left[(1-\sin(\theta))^2 + (\cos(\theta))^2\right] = \frac{1-\sin(\theta)}{2} \tag{4.94}$$

(B) Soit Alice envoie

$$|1\rangle_z = \frac{|0\rangle_y - |1\rangle_y}{\sqrt{2}i} \tag{4.95}$$

On calcule alors l'action de la transformation de clonage

$$|1\rangle_{zA}|0\rangle_{yE} = \left(\frac{|0\rangle_y - |1\rangle_y}{\sqrt{2}i}\right) \otimes |0\rangle_y = \frac{1}{\sqrt{2}i}\left(|00\rangle_y - |10\rangle_y\right) \tag{4.96}$$

$$|\phi\rangle_{AE} = U\left(|1\rangle_{zA}|0\rangle_{yE}\right) = U\left(\frac{1}{\sqrt{2}i}\left(|00\rangle_y - |10\rangle_y\right)\right) \tag{4.97}$$

$$|\phi\rangle_{AE} = \frac{1}{\sqrt{2}i}\left(|00\rangle_y - \cos(\theta)|10\rangle_y - \sin(\theta)|01\rangle_y\right) \tag{4.98}$$

Déterminons la probabilité qu' Ève reçoive un 0 sachant qu'Alice a envoyé un 1.

$$|\psi\rangle_E = |0\rangle_{zE} = \frac{1}{\sqrt{2}}\left(|0\rangle_y + |1\rangle_y\right) \tag{4.99}$$

$$P = |{}_E\langle 0_z|\phi\rangle_{AE}|^2 \tag{4.100}$$

$${}_E\langle 0_z|\phi\rangle_{AE} = \frac{i}{2}\left[\left(\langle 0|_y + \langle 1|_y\right)|\left(-|00\rangle_y + \cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y\right)\right] \tag{4.101}$$

$${}_E\langle 0_z|\phi\rangle_{AE} = \frac{i}{2}\left(-|0\rangle_y + \sin(\theta)|0\rangle_y + \cos(\theta)|1\rangle_y\right) \tag{4.102}$$

$$P = \frac{1}{4}\left[(\sin(\theta) - 1)^2 + (\cos(\theta))^2\right] = \frac{1 - \sin(\theta)}{2} \tag{4.103}$$

Déterminons la probabilité qu' Ève reçoive un 1 sachant qu'Alice a envoyé un 1.

$$|\psi\rangle_E = |1\rangle_{zE} = \frac{1}{\sqrt{2}i}\left(|0\rangle_y - |1\rangle_y\right) \tag{4.104}$$

$$P = |{}_E\langle 1_z|\phi\rangle_{AE}|^2 \tag{4.105}$$

$$ {}_E\langle 1_z|\phi\rangle_{AE} = \frac{-1}{2}\left[(\langle 0|_y - \langle 1|_y)\,|\,(-|00\rangle_y + \cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y)\right] \tag{4.106} $$

$$ {}_E\langle 1_z|\phi\rangle_{AE} = \frac{-1}{2}\left(-|0\rangle_y - \sin(\theta)|0\rangle_y + \cos(\theta)|1\rangle_y\right) \tag{4.107} $$

$$ P = \frac{1}{4}\left[(1+\sin(\theta))^2 + (\cos(\theta))^2\right] = \frac{1+\sin(\theta)}{2} \tag{4.108} $$

Les probabilités conditionnelles sont donc

$$ p(\text{Ève mesure } 0_z|\text{Alice envoie } 0_z) = \frac{1+\sin(\theta)}{2} \tag{4.109} $$

$$ p(\text{Ève mesure } 0_z|\text{Alice envoie } 1_z) = \frac{1-\sin(\theta)}{2} \tag{4.110} $$

$$ p(\text{Ève mesure } 1_z|\text{Alice envoie } 0_z) = \frac{1-\sin(\theta)}{2} \tag{4.111} $$

$$ p(\text{Ève mesure } 1_z|\text{Alice envoie } 1_z) = \frac{1+\sin(\theta)}{2} \tag{4.112} $$

4.7.4 L'information mutuelle entre Alice et Bob

$$ p(x,y) = p(y|x)p(x) \tag{4.113} $$

$$ p(0,0) = p(1,1) = \frac{1+\cos(\theta)}{4} \tag{4.114} $$

$$ p(0,1) = p(1,0) = \frac{1-\cos(\theta)}{4} \tag{4.115} $$

Remarque 7 *On a bien*

$$ p(x) = \sum_y p(x,y) = \frac{1}{2} $$

Par l'équation (2.19)

$$ I_{AB} = \sum_{x,y} p(x,y)\log_2\frac{p(x,y)}{p(x)p(y)} = \sum_{x,y} p(x,y)\log_2\left[4.p(x,y)\right] \tag{4.116} $$

$$I_{AB} = 2\left(p(0,0)\log_2\left[4.p(0,0)\right] + p(1,0)\log_2\left[4.p(1,0)\right]\right) \tag{4.117}$$

On trouve donc :

$$I_{AB} = \frac{1}{2}\left[(1+\cos(\theta))\log_2(1+\cos(\theta)) + (1-\cos(\theta))\log_2(1-\cos(\theta))\right] \tag{4.118}$$

4.7.5 L'information mutuelle entre Alice et Ève

$$p(x,z) = p(z|x)p(x) \tag{4.119}$$

$$p(0,0) = p(1,1) = \frac{1+\sin(\theta)}{4} \tag{4.120}$$

$$p(0,1) = p(1,0) = \frac{1-\sin(\theta)}{4} \tag{4.121}$$

Remarque 8 *On a bien*

$$p(x) = \sum_z p(x,z) = \frac{1}{2}$$

Et un bruit de

$$\frac{1}{2}(1-\sin(\theta)) \tag{4.122}$$

Par l'équation (2.19) :

$$I_{AB} = \sum_{x,z} p(x,z)\log_2\frac{p(x,z)}{p(x)p(z)} = \sum_{x,z} p(x,z)\log_2\left[4.p(x,z)\right] \tag{4.123}$$

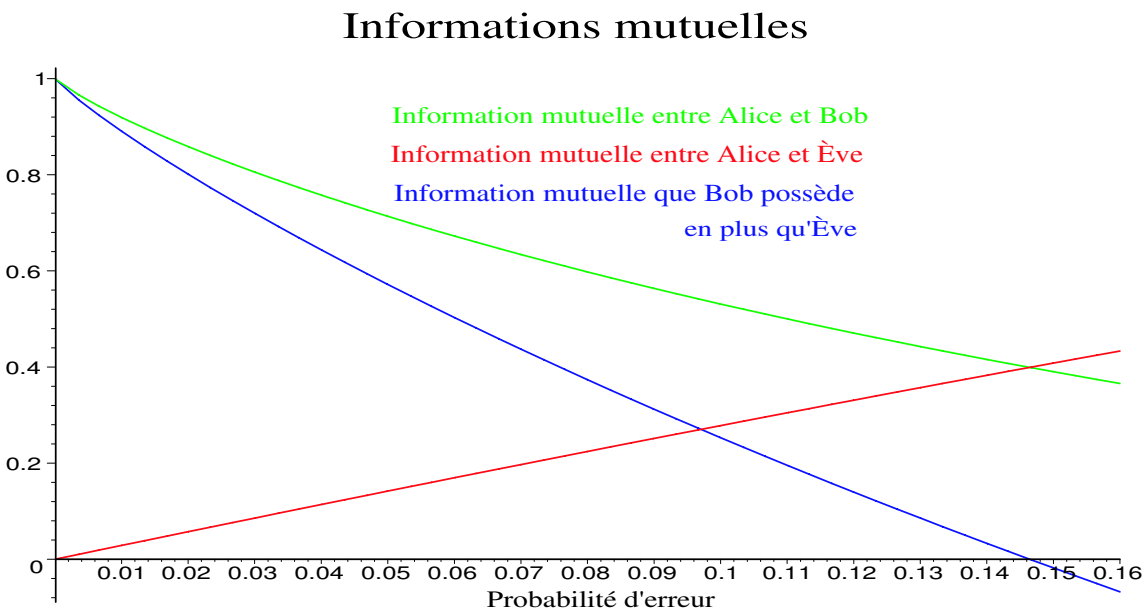
$$I_{AB} = 2\left(p(0,0)\log_2\left[4.p(0,0)\right] + p(1,0)\log_2\left[4.p(1,0)\right]\right) \tag{4.124}$$

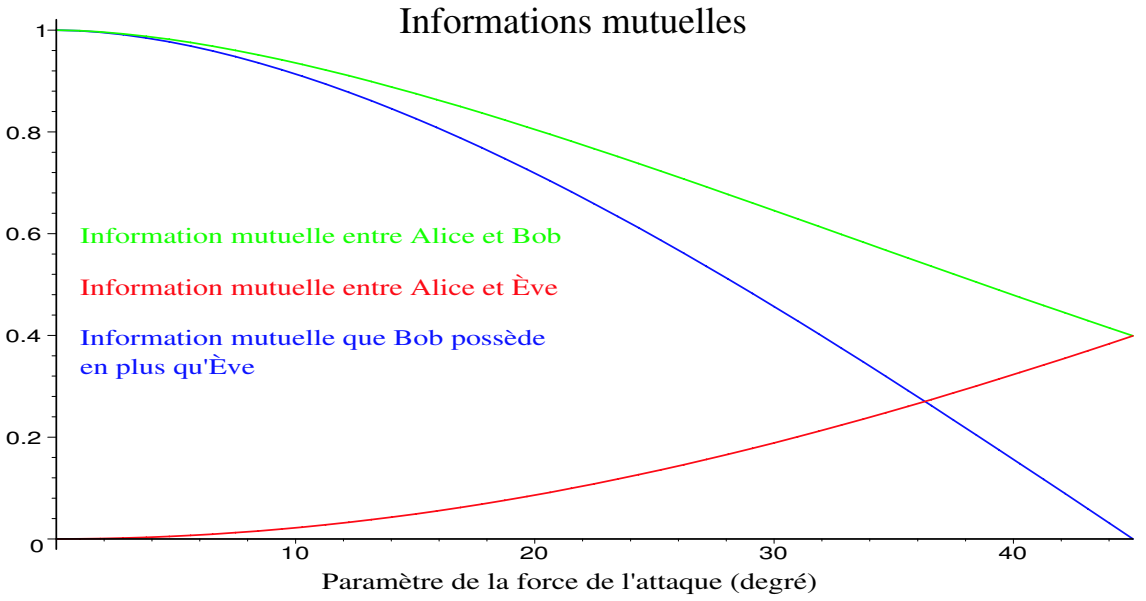
On trouve donc :

$$I_{AB} = \frac{1}{2}\left[(1+\sin(\theta))\log_2(1+\sin(\theta)) + (1-\sin(\theta))\log_2(1-\sin(\theta))\right] \tag{4.125}$$

4.7.6 Résultats

En raison de la symétrie entre l'expression de I_{AE} et celle de I_{AB}, on voit immédiatement que $\mathrm{I}_{AE} = \mathrm{I}_{AB}$ pour $\sin(\theta) = \cos(\theta)$, c'est-à-dire pour $\theta = \frac{\pi}{4}$.


Informations mutuelles
Information mutuelle entre Alice et Bob
Information mutuelle entre Alice et Ève
Information mutuelle que Bob possède
en plus qu'Ève
1
0.8
0.6
0.4
0.2
0
0.01 0.02 0.03 0.04 0.05 0.06 0.07 0.08 0.09 0.1 0.11 0.12 0.13 0.14 0.15 0.16
Probabilité d'erreur


Informations mutuelles
Information mutuelle entre Alice et Bob
Information mutuelle entre Alice et Ève
Information mutuelle que Bob possède
en plus qu'Ève
1
0.8
0.6
0.4
0.2
0
10
20
30
40
Paramètre de la force de l'attaque (degré)

Nous avons donc montré la proposition suivante :

Proposition 3 *Soit θ le paramètre de la force de l'attaque " cloning ", contrôlé par Ève.*

1. *Si $\theta < \frac{\pi}{4}$, alors une clef pourra être transmise entre Alice et Bob.*
2. *Si $\theta \geq \frac{\pi}{4}$, alors l'envoi d'une clef est abandoné.*

La probabilité d'erreur pour $\theta = \frac{\pi}{4}$ est

$$P_{erreur} = 0.1464 \tag{4.126}$$

En effet, le bruit est de $\frac{1}{2}(1-\sin(\theta))$, donc pour $\theta = \frac{\pi}{4}$, on a bien 14,64% d'erreur.

Remarque 9

$$|00\rangle_y = \frac{|0\rangle_z + i|1\rangle_z}{\sqrt{2}} \otimes \frac{|0\rangle_z + i|1\rangle_z}{\sqrt{2}} = \frac{1}{2}\left(|00\rangle_z + i|01\rangle_z + i|10\rangle_z - |11\rangle_z\right) \tag{4.127}$$

$$|10\rangle_y = \frac{|0\rangle_z - i|1\rangle_z}{\sqrt{2}} \otimes \frac{|0\rangle_z + i|1\rangle_z}{\sqrt{2}} = \frac{1}{2}\left(|00\rangle_z + i|01\rangle_z - i|10\rangle_z + |11\rangle_z\right) \tag{4.128}$$

$$|01\rangle_y = \frac{|0\rangle_z + i|1\rangle_z}{\sqrt{2}} \otimes \frac{|0\rangle_z - i|1\rangle_z}{\sqrt{2}} = \frac{1}{2}\left(|00\rangle_z - i|01\rangle_z + i|10\rangle_z - |11\rangle_z\right) \tag{4.129}$$

Calculons $|\phi\rangle_{AE}$ dans la base z quand Alice envoie $|0\rangle_z$.

$$|\phi\rangle_{AE} = U\left(|0\rangle_{zA}|0\rangle_{yE}\right) = U\left(\frac{|00\rangle_y + |10\rangle_y}{\sqrt{2}}\right) = \frac{\left(|00\rangle_y + \cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y\right)}{\sqrt{2}} \tag{4.130}$$

$$\begin{aligned} |\phi\rangle_{AE} = \frac{1}{2\sqrt{2}}\{&(1+\cos(\theta)+\sin(\theta))|00\rangle_z + i(1+\cos(\theta)-\sin(\theta))|01\rangle_z \\ &+ i(1-\cos(\theta)+\sin(\theta))|10\rangle_z + (-1+\cos(\theta)+\sin(\theta))|11\rangle_z\} \end{aligned} \tag{4.131}$$

Calculons $|\phi\rangle_{AE}$ dans la base z quand Alice envoie $|1\rangle_z$.

$$|\phi\rangle_{AE} = \frac{1}{2\sqrt{2}}\{i(-1+\cos(\theta)+\sin(\theta))|00\rangle_z + (1-\cos(\theta)+\sin(\theta))|01\rangle_z + (1+\cos(\theta)-\sin(\theta))|10\rangle_z + i(1+\cos(\theta)+\sin(\theta))|11\rangle_z\} \quad (4.132)$$

Or, les informations mutuelles sont égales pour $\theta = \frac{\pi}{4}$. Ce qui se vérifie.

Le terme dominant de $|\phi\rangle_{AE}$ quand Alice envoie $|0\rangle_z$ et que $\theta = \frac{\pi}{4}$ est $|00\rangle_z$. Alice, Bob et Ève ont donc bien tous les trois un photon dans le même état de polarisation. L'attaque n'est cependant pas parfaite vu qu'il y a encore d'autres termes en $|01\rangle_z$, $|10\rangle_z$ et $|11\rangle_z$.

Il en est de même quand Alice envoie $|1\rangle_z$. Le terme dominant de $|\phi\rangle_{AE}$ est alors, pour $\theta = \frac{\pi}{4}$, $|11\rangle_z$. Alice, Bob et Ève ont donc bien tous les trois un photon dans le même état de polarisation, $|1\rangle_z$. Mais, l'attaque n'est toujours pas parfaite pour les mêmes raisons.

4.7.7 Cas réel

Dans le cas réel, Alice et Bob doivent tenir compte du bruit inhérent au canal de communication. On voit que, dès que le bruit de ce canal est inférieur à 15 %, Ève n'a aucun moyen d'intercepter la clef sans que son intervention soit détectable. Si ce bruit dépasse 15 %, elle pourra prendre de l'information en simulant le bruit du canal et passée inaperçue. QBER < 15 % assure donc la sécurisation de la communication.

En pratique, cette attaque présente un inconvénient. Ève doit pouvoir conserver de manière cohérente l'état du photon qu'elle a dupliqué pendant un temps de l'ordre de la seconde, puisqu'elle doit attendre le moment où Alicedivulgue ses choix de bases à la fin du protocole.

Concrètement, pour lutter contre l'espionnage, il faut disposer d'une fibre optique introduisant le moins de bruit possible et présentant une faible atténuation.

4.7.8 Calculs des probabilités en base x : même combat

Reprenons maintenant tous les calculs en considérant qu'Alice envoie son photon dans la base x et vérifions que l'information mutuelle est symétrique pour les bases x et z.

Nous allons effectuer nos calculs dans la base y.

$$|\psi\rangle_A = \begin{cases} |0\rangle_x \\ |1\rangle_x \end{cases} \tag{4.133}$$

et

$$\begin{cases} |0\rangle_x = \frac{|0\rangle_z + |1\rangle_z}{\sqrt{2}} = \frac{1}{2}\left((1-i)|0\rangle_y + (1+i)|1\rangle_y\right) \\ |1\rangle_x = \frac{|0\rangle_z - |1\rangle_z}{\sqrt{2}} = \frac{1}{2}\left((1+i)|0\rangle_y + (1-i)|1\rangle_y\right) \end{cases} \tag{4.134}$$

Entre Alice et Bob

(A) Soit Alice envoie

$$|0\rangle_x = \frac{(1-i)|0\rangle_y + (1+i)|1\rangle_y}{2} \tag{4.135}$$

On calcule alors l'action de la transformation de clonage

$$\begin{aligned} |0\rangle_{xA}|0\rangle_{yE} &= \left(\frac{(1-i)|0\rangle_y + (1+i)|1\rangle_y}{2}\right) \otimes |0\rangle_y \\ &= \frac{1}{2}\left((1-i)|00\rangle_y + (1+i)|10\rangle_y\right) \end{aligned} \tag{4.136}$$

$$|\phi\rangle_{AE} = U\left(|0\rangle_{xA}|0\rangle_{yE}\right) = U\left(\frac{1}{2}\left((1-i)|00\rangle_y + (1+i)|10\rangle_y\right)\right) \tag{4.137}$$

$$|\phi\rangle_{AE} = \frac{1}{2}\left((1-i)|00\rangle_y + (1+i)(\cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y)\right) \tag{4.138}$$

Déterminons la probabilité que Bob reçoive un 0 sachant qu'Alice a envoyé un 0.

$$|\psi\rangle_B = |0\rangle_{xB} = \frac{1}{2}\left((1-i)|0\rangle_y + (1+i)|1\rangle_y\right) \tag{4.139}$$

$$P = |{}_B\langle 0_x|\phi\rangle_{BE}|^2 \tag{4.140}$$

$${}_B\langle 0_x|\phi\rangle_{BE} = \frac{1}{4}\left[\left((1+i)\langle 0|_y + (1-i)\langle 1|_y\right)|(1-i)|00\rangle_y + (1+i)(\cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y)\right] \tag{4.141}$$

$${}_B\langle 0_x|\phi\rangle_{BE} = \frac{1}{2}\left(|0\rangle_y + i\sin(\theta)|1\rangle_y + \cos(\theta)|0\rangle_y\right) \tag{4.142}$$

$$P = \frac{1}{4}\left[(1+\cos(\theta))^2 + (\sin(\theta))^2\right] = \frac{1+\cos(\theta)}{2} \tag{4.143}$$

Déterminons la probabilité que Bob reçoive un 1 sachant qu'Alice a envoyé un 0.

$$|\psi\rangle_B = |1\rangle_{xB} = \frac{1}{2}\left((1+i)|0\rangle_y + (1-i)|1\rangle_y\right) \tag{4.144}$$

$$P = |{}_B\langle 1_x|\phi\rangle_{BE}|^2 \tag{4.145}$$

$${}_B\langle 1_x|\phi\rangle_{BE} = \frac{1}{4}\left[\left((1-i)\langle 0|_y + (1+i)\langle 1|_y\right)|(1-i)|00\rangle_y + (1+i)(\cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y)\right] \tag{4.146}$$

$${}_B\langle 1_x|\phi\rangle_{BE} = \frac{1}{2}\left(-i|0\rangle_y + \sin(\theta)|1\rangle_y + i\cos(\theta)|0\rangle_y\right) \tag{4.147}$$

$$P = \frac{1}{4}\left[(\cos(\theta)-1)^2 + (\sin(\theta))^2\right] = \frac{1-\cos(\theta)}{2} \tag{4.148}$$

(B) Soit Alice envoie

$$|1\rangle_x = \frac{(1+i)|0\rangle_y + (1-i)|1\rangle_y}{2} \tag{4.149}$$

On calcule alors l'action de la transformation de clonage

$$\begin{aligned} |1\rangle_{xA}|0\rangle_{yE} &= \left(\frac{(1+i)|0\rangle_y + (1-i)|1\rangle_y}{2}\right) \otimes |0\rangle_y \\ &= \frac{1}{2}\left((1+i)|00\rangle_y + (1-i)|10\rangle_y\right) \end{aligned} \tag{4.150}$$

$$|\phi\rangle_{AE} = U\left(|1\rangle_{xA}|0\rangle_{yE}\right) = U\left(\frac{1}{2}\left((1+i)|00\rangle_y + (1-i)|10\rangle_y\right)\right) \tag{4.151}$$

$$|\phi\rangle_{AE} = \frac{1}{2}\left((1+i)|00\rangle_y + (1-i)(\cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y)\right) \tag{4.152}$$

Déterminons la probabilité que Bob reçoive un 0 sachant qu'Alice a envoyé un 1.

$$|\psi\rangle_B = |0\rangle_{xB} = \frac{1}{2}\left((1-i)|0\rangle_y + (1+i)|1\rangle_y\right) \tag{4.153}$$

$$P = |{}_B\langle 0_x|\phi\rangle_{BE}|^2 \tag{4.154}$$

$$ {}_B\langle 0_x|\phi\rangle_{BE} = \frac{1}{4}\left[((1+i)\langle 0|_y + (1-i)\langle 1|_y)\,|(1+i)|00\rangle_y + (1-i)(\cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y)\right] \tag{4.155} $$

$$ {}_B\langle 0_x|\phi\rangle_{BE} = \frac{1}{2}\left(i|0\rangle_y + \sin(\theta)|1\rangle_y - i\cos(\theta)|0\rangle_y\right) \tag{4.156} $$

$$ P = \frac{1}{4}\left[(1-\cos(\theta))^2 + (\sin(\theta))^2\right] = \frac{1-\cos(\theta)}{2} \tag{4.157} $$

Déterminons la probabilité que Bob reçoive un 1 sachant qu'Alice a envoyé un 0.

$$ |\psi\rangle_B = |1\rangle_{xB} = \frac{1}{2}\left((1+i)|0\rangle_y + (1-i)|1\rangle_y\right) \tag{4.158} $$

$$ P = |{}_B\langle 1_x|\phi\rangle_{BE}|^2 \tag{4.159} $$

$$ {}_B\langle 1_x|\phi\rangle_{BE} = \frac{1}{4}\left[((1-i)\langle 0|_y + (1+i)\langle 1|_y)\,|(1+i)|00\rangle_y + (1-i)(\cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y)\right] \tag{4.160} $$

$$ {}_B\langle 1_x|\phi\rangle_{BE} = \frac{1}{2}\left(|0\rangle_y - i\sin(\theta)|1\rangle_y + \cos(\theta)|0\rangle_y\right) \tag{4.161} $$

$$ P = \frac{1}{4}\left[(1+\cos(\theta))^2 + (\sin(\theta))^2\right] = \frac{1+\cos(\theta)}{2} \tag{4.162} $$

Conclusion. Les probabilités conditionnelles sont bien les mêmes.

Entre Alice et Ève

(A) Soit Alice envoie

$$ |0\rangle_x = \frac{(1-i)|0\rangle_y + (1+i)|1\rangle_y}{2} \tag{4.163} $$

On calcule alors l'action de la transformation de clonage

$$ \begin{aligned} |0\rangle_{xA}|0\rangle_{yE} &= \left(\frac{(1-i)|0\rangle_y + (1+i)|1\rangle_y}{2}\right) \otimes |0\rangle_y \\ &= \frac{1}{2}\left((1-i)|00\rangle_y + (1+i)|10\rangle_y\right) \end{aligned} \tag{4.164} $$

$$|\phi\rangle_{AE} = U\left(|0\rangle_{xA}|0\rangle_{yE}\right) = U\left(\frac{1}{2}\left((1-i)|00\rangle_y + (1+i)|10\rangle_y\right)\right) \tag{4.165}$$

$$|\phi\rangle_{AE} = \frac{1}{2}\left((1-i)|00\rangle_y + (1+i)(\cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y)\right) \tag{4.166}$$

Déterminons la probabilité qu'Ève reçoive un 0 sachant qu'Alice a envoyé un 0.

$$|\psi\rangle_E = |0\rangle_{xE} = \frac{1}{2}\left((1-i)|0\rangle_y + (1+i)|1\rangle_y\right) \tag{4.167}$$

$$P = |{}_E\langle 0_x|\phi\rangle_{AE}|^2 \tag{4.168}$$

$${}_E\langle 0_x|\phi\rangle_{AE} = \frac{1}{4}\left[\left((1+i)\langle 0|_y + (1-i)\langle 1|_y\right)|(1-i)|00\rangle_y + (1+i)(\cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y)\right] \tag{4.169}$$

$${}_E\langle 0_x|\phi\rangle_{AE} = \frac{1}{2}\left(|0\rangle_y + i\cos(\theta)|1\rangle_y + \sin(\theta)|0\rangle_y\right) \tag{4.170}$$

$$P = \frac{1}{4}\left[(1+\sin(\theta))^2 + (\cos(\theta))^2\right] = \frac{1+\sin(\theta)}{2} \tag{4.171}$$

Déterminons la probabilité qu'Ève reçoive un 1 sachant qu'Alice a envoyé un 0.

$$|\psi\rangle_E = |1\rangle_{xE} = \frac{1}{2}\left((1+i)|0\rangle_y + (1-i)|1\rangle_y\right) \tag{4.172}$$

$$P = |{}_E\langle 1_x|\phi\rangle_{AE}|^2 \tag{4.173}$$

$${}_E\langle 1_x|\phi\rangle_{AE} = \frac{1}{4}\left[\left((1-i)\langle 0|_y + (1+i)\langle 1|_y\right)|(1-i)|00\rangle_y + (1+i)(\cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y)\right] \tag{4.174}$$

$${}_E\langle 1_x|\phi\rangle_{AE} = \frac{1}{2}\left(-i|0\rangle_y + \cos(\theta)|1\rangle_y + i\sin(\theta)|0\rangle_y\right) \tag{4.175}$$

$$P = \frac{1}{4}\left[(\sin(\theta)-1)^2 + (\cos(\theta))^2\right] = \frac{1-\sin(\theta)}{2} \tag{4.176}$$

(B) Soit Alice envoie

$$|1\rangle_x = \frac{(1+i)|0\rangle_y + (1-i)|1\rangle_y}{2} \tag{4.177}$$

On calcule alors l'action de la transformation de clonage

$$\begin{aligned} |1\rangle_{xA}|0\rangle_{yE} &= \left(\frac{(1+i)|0\rangle_y + (1-i)|1\rangle_y}{2}\right) \otimes |0\rangle_y \\ &= \frac{1}{2}\left((1+i)|00\rangle_y + (1-i)|10\rangle_y\right) \end{aligned} \tag{4.178}$$

$$|\phi\rangle_{AE} = U\left(|1\rangle_{xA}|0\rangle_{yE}\right) = U\left(\frac{1}{2}\left((1+i)|00\rangle_y + (1-i)|10\rangle_y\right)\right) \tag{4.179}$$

$$|\phi\rangle_{AE} = \frac{1}{2}\left((1+i)|00\rangle_y + (1-i)(\cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y)\right) \tag{4.180}$$

Déterminons la probabilité qu'Ève reçoive un 0 sachant qu'Alice a envoyé un 1.

$$|\psi\rangle_E = |0\rangle_{xE} = \frac{1}{2}\left((1-i)|0\rangle_y + (1+i)|1\rangle_y\right) \tag{4.181}$$

$$P = |{}_E\langle 0_x|\phi\rangle_{AE}|^2 \tag{4.182}$$

$${}_E\langle 0_x|\phi\rangle_{AE} = \frac{1}{4}\left[\left((1+i)\langle 0|_y + (1-i)\langle 1|_y\right)|(1+i)|00\rangle_y + (1-i)(\cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y)\right] \tag{4.183}$$

$${}_E\langle 0_x|\phi\rangle_{AE} = \frac{1}{2}\left(i|0\rangle_y + \cos(\theta)|1\rangle_y - i\sin(\theta)|0\rangle_y\right) \tag{4.184}$$

$$P = \frac{1}{4}\left[(1-\sin(\theta))^2 + (\cos(\theta))^2\right] = \frac{1-\sin(\theta)}{2} \tag{4.185}$$

Déterminons la probabilité qu'Ève reçoive un 1 sachant qu'Alice a envoyé un 0.

$$|\psi\rangle_E = |1\rangle_{xE} = \frac{1}{2}\left((1+i)|0\rangle_y + (1-i)|1\rangle_y\right) \tag{4.186}$$

$$P = |{}_E\langle 1_x|\phi\rangle_{AE}|^2 \tag{4.187}$$

$$ {}_E\langle 1_x|\phi\rangle_{AE} = \frac{1}{4}\left[((1-i)\langle 0|_y + (1+i)\langle 1|_y)\,|(1+i)|00\rangle_y + (1-i)(\cos(\theta)|10\rangle_y + \sin(\theta)|01\rangle_y)\right] \tag{4.188} $$

$$ {}_E\langle 1_x|\phi\rangle_{AE} = \frac{1}{2}\left(|0\rangle_y - i\cos(\theta)|1\rangle_y + \sin(\theta)|0\rangle_y\right) \tag{4.189} $$

$$ P = \frac{1}{4}\left[(1+\sin(\theta))^2 + (\cos(\theta))^2\right] = \frac{1+\sin(\theta)}{2} \tag{4.190} $$

Conclusion. Les probabilités conditionnelles sont également les mêmes.

4.8 L'intrication

4.8.1 Qu'est-ce qu'un état intriqué?

Nous avons jusqu'à présent considéré le cas où l'état d'un système global est représenté par un produit tensoriel de qubits, c'est-à-dire que l'état $|\psi\rangle$ peut être décrit sous la forme $|\psi\rangle = |\phi\rangle \otimes |\chi\rangle$ où $|\phi\rangle$ est le vecteur d'état associé au système 1 et $|\chi\rangle$ est le vecteur d'état associé au système 2. Mais ce n'est pas toujours le cas.

Prenons par exemple,

$$ |\Psi^-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle $$

C'est bien un état de $\mathbb{H}^2$ ($||\frac{1}{\sqrt{2}}||^2 + ||\frac{1}{\sqrt{2}}||^2 = 1$) où $\mathbb{H}^2 = \mathbb{H} \otimes \mathbb{H}$.

Recherchons $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ et $|\chi\rangle = \gamma|0\rangle + \delta|1\rangle$ tels que $|\Psi^-\rangle = |\phi\rangle \otimes |\chi\rangle$?

$$ \begin{aligned} |\phi\rangle \otimes |\chi\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) \\ &= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \end{aligned} $$

$$ \begin{aligned} &\Rightarrow |\Psi^-\rangle = |\phi\rangle \otimes |\chi\rangle \\ &\Leftrightarrow \alpha\gamma = \beta\delta = 0 \\ &\alpha\delta = \frac{1}{\sqrt{2}} \\ &\beta\gamma = -\frac{1}{\sqrt{2}} \end{aligned} $$

Puisque $\alpha\gamma = \beta\delta = 0 \Rightarrow$, au moins deux des cœficients α, β, γ, δ sont nuls. Or, $\alpha\delta \neq 0$ et $\beta\gamma \neq 0 \Rightarrow$ nous aboutissons donc à une contradiction.

□

Nous ne pouvons donc pas factoriser (séparer en produit tensoriel) l'état $|\Psi^-\rangle$. On dit alors que l'état est *intriqué*.

Définition 1 *Soit $|\psi\rangle \in \mathbb{H}^q$. L'état $|\psi\rangle$ est intriqué s'il n'existe pas de $|\phi\rangle \in \mathbb{H}^m$ et $|\chi\rangle \in \mathbb{H}^n$ tels que $|\psi\rangle = |\phi\rangle \otimes |\chi\rangle$ et $q = m + n$.*

Remarque 10 *Un état qui n'est pas intriqué est dit séparable.*

Remarque 11 *Le choix de cet exemple n'est pas anodin. En effet, l'état $|\Psi^-\rangle$ a une importance en information quantique. C'est l'un des quatre états de Bell, qui sont définis comme suit :*

$$\begin{cases} |\Psi^+\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle \\ |\Psi^-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle \\ |\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \\ |\Phi^-\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle \end{cases} \tag{4.191}$$

Remarque 12 *Les états de Bell forment une base orthonormée de $\mathbb{H}^2$.*

En effet, tout $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \in \mathbb{H}^2$ peut être exprimé comme :

$$|\psi\rangle = |\Phi^+\rangle\langle\Phi^+|\psi\rangle + |\Phi^-\rangle\langle\Phi^-|\psi\rangle + |\Psi^+\rangle\langle\Psi^+|\psi\rangle + |\Psi^-\rangle\langle\Psi^-|\psi\rangle$$

$$|\psi\rangle = \frac{(\alpha+\delta)}{\sqrt{2}}|\Phi^+\rangle + \frac{(\alpha-\delta)}{\sqrt{2}}|\Phi^-\rangle + \frac{(\beta+\gamma)}{\sqrt{2}}|\Psi^+\rangle + \frac{(\beta-\gamma)}{\sqrt{2}}|\Psi^-\rangle$$

Mais nous ne nous étendrons pas sur le sujet.

4.8.2 Application à la cryptographie quantique

Reprenons notre état intriqué, $|\psi\rangle$.

Les prévisions des résultats de mesure portant sur un seul des deux systèmes ne peuvent plus s'exprimer en fonction d'un vecteur $|\phi\rangle$ ou $|\chi\rangle$. Nous devons utiliser la formule générale :

$$\langle A\rangle = \frac{\langle\psi|A|\psi\rangle}{\langle\psi|\psi\rangle} \tag{4.192}$$

qui donne la valeur moyenne de l'observable A dans l'état $|\psi\rangle$.

Nous dirons que les systèmes 1 et 2 sont corrélés, c'est-à-dire que les résultats de mesure portant soit sur le système 1, soit sur le système 2, présentent des corrélations.

Le vecteur d'état $|\chi\prime\rangle$ associé au système 2 après la mesure dépend, lorsque l'état $|\psi\rangle$ avant la mesure est un état *intriqué*, du résultat de l'ensemble complet des mesures faites sur le système 1 même si le sytème 2 est, au moment de la mesure, déjà très loin du système 1 et n'interagit plus avec lui.

On appelle cela le *paradoxe d'EPR* pour Einstein, Podolsky et Rosen.

L'intrication est donc une corrélation qui lie les deux particules à travers l'espace.

Pour vérifier ceci, prenons un cas plus simple où nous faisons interagir deux particules. Les deux particules sont alors corrélées.

Soient deux particules A et B à deux états $|0\rangle$ et $|1\rangle$, chacune dans un état :

$$|\psi_A\rangle = \alpha|0\rangle + \beta|1\rangle$$
$$|\psi_B\rangle = \gamma|0\rangle + \delta|1\rangle$$

L'état conjoint s'écrit :

$$\begin{aligned}|\psi_{AB}\rangle &= |\psi_A\rangle|\psi_B\rangle \\ &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) \\ &= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle\end{aligned}$$

La mesure sur la particule A affecte l'état de la particule B. Ainsi, lorsque A est mesuré dans l'état $|0\rangle$, B se trouve dans l'état :

$$\langle 0|\psi_{AB}\rangle = \alpha(\gamma|0\rangle + \delta|1\rangle)$$

Ceci reste valable même si les deux particules A et B sont éloignées. La projection de l'état de A affecte instantanément l'état $|\psi_{AB}\rangle$ et par conséquent, l'état partiel de la particule B.

Proposition 4 *Si n paires d'états intriqués sont séparées entre Alice et Bob (par exemple, pour chaque paire Alice a la première particule (le premier qubit) et Bob, la deuxième) alors, la mesure complète de chaque photon dans la même base donnera la même chaîne de bits.*

Le protocole est tout à fait similaire au protocole que nous avons étudié dans ce chapitre. La seule différence est qu'Alice et Bob partagent des paires EPR. Donc, si Ève effectue des mesures ou des transformations sur les photons, elle engendre des perturbations qui pourront être détectées par Alice et Bob lorsqu'ils compareront une partie de leurs clefs tamisées puisqu'elles devraient être identiques.

Chapitre 5

Expériences

Nous consacrons ce dernier chapitre aux principales expériences qui ont été réalisées jusqu'à maintenant.

Ces expériences nous montrent que les problèmes les plus importants, avec les sources de bruit que nous avons traitées au paragraphe 4.6.2, sont l'atténuation et l'effet de décohérence dans les fibres. Ceux-ci sont proportionnels à la distance à laquelle on désire transmettre les photons. Les chercheurs sont donc limités quant à la distance séparant Alice et Bob. À l'heure actuelle, elle atteint environ 70 km.

Contrairement à un signal classique, un signal quantique ne peut être amplifié par des répétiteurs et ceci en vertu des lois de la mécanique quantique. Cependant, des recherches portent actuellement sur l'utilisation de répétiteurs quantiques.

Voici quelques expériences. Nous indiquons la distance sur laquelle la clef a été transmise.

1989 Première expérience basée sur le protocole BB84 et réalisée au laboratoire de recherche IBM T.J. Watson par Bennet, Brassard et certains de leurs élèves, qui a permis de montrer qu'il était possible grâce à un canal quantique (ici, un canal optique sous vide et rectiligne) de transmettre des clefs secrètes de plusieurs centaines de bits à une vitesse de 10 bit/s, entre deux points distants de 32 cm, et ce même si ce canal est espionné (attaques : *intercept and resend* et *beam splitting*) tout au long de la transmission. Les photo-détecteurs étaient efficaces à 9 % et l'intensité des implusions lumineuses étaient de 0,17 photon par impulsion.

1993 Réalisation, à Genève du protocole BB84, sur un solénoïde de 1 km de fibre optique (Muller, Breguet et Gisin).
Réalisation sur 10 km de fibre optique du protocole basé sur les paires de photons intriqués (Townsend, Rarity et Tapster).

1995 Expérience effectuée sur une fibre optique de 23 km sous le lac de Genève.

1999 Expérience réalisée à Los Alamos par le groupe de Paul Kwiat (protocole basé sur les paires EPR) qui a permis d'échanger des clefs par une fibre optique de 48 km.

2000 Distribution quantique de clefs en plein air et en plein jour sur une distance de 1,6 km. Ceci laisse espérer que le protocole pourrait être un jour utilisé pour les communications satellites.

2001 Un groupe anglais a réalisé le protocole BB84 à l'air libre sur une distance de 23 km. Il a transmis une clef à la vitesse de 700 bits/s. Les photo-détecteurs avaient une efficacité de 5 à 10 %.

2002 Liaison Lausanne-Genève réalisée par le groupe de l'université de Genève, mené par Nicolas Gisin, sur 67 km. Une clef a été transmise à raison de 20 kbits/s (utilisation de paires de photons intriqués).

Conclusion

Nous avons montré que la cryptographie quantique est conceptuellement "simple" (dans le sens qu'elle applique les principes de la mécanique quantique sans autre moyen technologique) mais d'un point de vue pratique, elle doit encore faire face à plusieurs problèmes que les techniques actuelles ne peuvent pas encore résoudre (bien que des réussites expérimentales existent).

Tant que ces problèmes de communication sécurisée à longue distance ne seront pas résolus, il ne pourra pas y avoir de véritables applications (commerciales) de la cryptographie quantique.

Annexe A

Théorème de non-clonage

Théorème 1 *Soient $|\psi\rangle$ un état quelconque et $|u\rangle$ l'état clonant. Il n'existe pas de transformation qui permette de cloner parfaitement $|\psi\rangle$;*
c'est-à-dire : il n'existe pas de $U : \mathcal{E} \otimes \mathcal{E} \to \mathcal{E} \otimes \mathcal{E}$ tel que

$$U(|\psi\rangle|u\rangle) = |\psi\rangle|\psi\rangle)$$

Démonstration :

Première étape
Soient $|\psi\rangle \in \mathcal{E}$ et $|u\rangle \in \mathcal{E}$.
Localement, il existe toujours une base orthonormée de $\mathcal{E}$ avec $|u\rangle$ comme premier vecteur de base. Soit $|u_j\rangle$ cette base et $|u\rangle = |u_1\rangle$.

$$|\psi\rangle = c^j|u_j\rangle \tag{A.1}$$

Supposons qu'il existe $U : \mathcal{E} \otimes \mathcal{E} \to \mathcal{E} \otimes \mathcal{E}$ tel que :

$$U(|\phi\rangle|u\rangle) = |\phi\rangle|\phi\rangle \qquad , \qquad \forall|\phi\rangle \in \mathcal{E} \tag{A.2}$$

C'est vrai pour tout ket, donc en particulier

1. Pour $|\psi\rangle$:
$$|\Theta\rangle = U\left(|\psi\rangle|u\rangle\right) = |\psi\rangle|\psi\rangle \tag{A.3}$$
2. Pour chaque $|u_k\rangle$:
$$|\Theta\rangle = U\left(|\psi\rangle|u\rangle\right) = U\left(c^k|u_k\rangle|u_1\rangle\right) \tag{A.4}$$
$$|\Theta\rangle = \sum_k c^k|u_k\rangle|u_k\rangle \tag{A.5}$$

Or, dans (A.3),

$$|\Theta\rangle = |\psi\rangle|\psi\rangle = |c^k u_k\rangle|c^m u_m\rangle = c^k c^m|u_k\rangle|u_m\rangle \tag{A.6}$$

Ce qui est différent de l'expression (A.5).

Seconde étape

On a supposé que U était unitaire. (On a en effet supposé qu'elle envoie une base orthonormée sur une autre base orthonormée.)
Pour être plus géneral, on étend U à $\tilde{U} : \mathcal{E} \otimes \mathcal{E} \otimes \mathcal{E} \rightarrow \mathcal{E} \otimes \mathcal{E} \otimes \mathcal{E}$.
$\tilde{U}$ n'est alors plus unitaire.
Alors, $\forall |\xi\rangle \in \mathcal{E}$, on suppose

$$\tilde{U}\left(|\phi\rangle|u\rangle|\xi\rangle\right) = |\phi\rangle|\phi\rangle|\xi\rangle \tag{A.7}$$

1.
$$|\Theta\rangle = \tilde{U}\left(|\psi\rangle|u\rangle|\xi\rangle\right) = \sum_k c^k |u_k\rangle|u_k\rangle|\xi\rangle \tag{A.8}$$

2.
$$|\Theta\rangle = \tilde{U}\left(|\psi\rangle|u\rangle|\xi\rangle\right) = |\psi\rangle|\psi\rangle|\xi\rangle = c^k c^m |u_k\rangle|u_m\rangle|\xi\rangle \tag{A.9}$$

Les équations (A.8) et (A.9) sont vraies $\forall |\xi\rangle \Rightarrow$ contradiction.

□

C'est donc la linéarité de la mécanique quantique qui interdit le clonage.

Annexe B

Matrices de Pauli

[1] Nous avons cité au chapitre 4 le fait qu'il existe 3 bases principalement utilisées : les bases x, y, et z (définies par les équations (4.28) à (4.32)). Nous nous proposons ici de montrer que ces kets sont kets propres des opérateurs de Pauli, et puisqu'elles apparaissent souvent en mécanique quantique, nous déduirons quelques propriétés, juste pour l'amusement.

B.1 Définition

Les matrices de Pauli apparaissent dans la théorie des moments angulaires en physique quantique, en particulier dans la description des systèmes de spin 1/2.
En effet, on définit l'opérateur moment angulaire $\bar{J} = \bar{x} \times \bar{p} = -i\hbar\bar{x} \times \bar{\nabla}$, dont les valeurs propres pour une particule de spin 1/2 sont $(\hbar/2\ ,\ -\hbar/2)$.
On écrit ces matrices

$$J_k = \frac{\hbar}{2}\sigma_k \qquad \Leftrightarrow \qquad \bar{J} = \frac{\hbar}{2}\bar{\sigma} \tag{B.1}$$

Définition 1 *Les matrices de Pauli sont définies par :*

$$\sigma_x \equiv \sigma_1 = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \tag{B.2}$$

$$\sigma_y \equiv \sigma_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{B.3}$$

$$\sigma_z \equiv \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{B.4}$$

1. Cette annexe a été ajoutée pour notre propre plaisir et n'a que peu d'intérêt pour le sujet présenté, elle peut donc être passée sans honte.

B.2 Les matrices de Pauli comme base

Dans le problème de la cryptographie quantique, l'espace des états $\mathcal{E}$ qui nous intéresse est simplement l'ensemble des couples de nombres complexes. $\mathcal{E}$ est donc isomorphe à $\mathbb{C} \times \mathbb{C}$.

$$\mathcal{E} \simeq \mathbb{C}^2$$

Les matrices de Pauli (σ_k) peuvent être vues comme des opérateurs de $\mathbb{C}^2 \to \mathbb{C}^2$. Une propriété intéressante, qui permet de retenir facilement ces matrices, est la suivante.

Propriété 1 *Soit* $\mathcal{M} = \{M \in \mathbb{C}^{2\times 2} : M = M^\dagger\}$ *l'ensemble des matrices complexes hermitiques* 2×2*. Alors*

$$\{\sigma_\mu\} = \{\sigma_0 = I, \sigma_1, \sigma_2, \sigma_3\} \tag{B.5}$$

forme une base de $\mathcal{M}$*.*

$\mathcal{M}$ peut être considéré comme un espace vectoriel réel de dimension 4.

Soit $M \in \mathcal{M}$, on sait que $M = M^\dagger$, c'est-à-dire

$$M_{kl} = M^*_{lk} \tag{B.6}$$

Donc, les deux éléments diagonaux sont réels et les deux éléments non diagonaux sont complexes conjugués. En choisissant a, b $\in \mathbb{R}$ et $z = x + iy$ un complexe, on peut écrire en général :

$$M = \begin{pmatrix} a & x+iy \\ x-iy & b \end{pmatrix} \tag{B.7}$$

$$M = a \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} + x \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + y \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \tag{B.8}$$

$$M = \frac{a+b}{2} I + \frac{a-b}{2} \sigma_3 + x\sigma_2 + y\sigma_1 \tag{B.9}$$

Toute matrice de $\mathcal{M}$ se décompose donc de façon unique sur la matrice unité et les trois σ_k, ce qui démontre la propriété.

B.3 Valeurs propres - vecteurs propres

Résolvons le problème aux valeurs et vecteurs propres des σ_k.

B.3.1 Valeurs propres

Résultat 1 *Les 3 σ_k ont le même spectre :* $\{-1,1\}$

En effet, les valeurs propres sont déterminées par l'équation caractéristique

$$det\,(\sigma_k - \lambda I) = 0 \tag{B.10}$$

$$det\,(\sigma_1 - \lambda I) = 0 \Leftrightarrow det \begin{pmatrix} -\lambda & i \\ -i & -\lambda \end{pmatrix} = \lambda^2 - 1 = 0 \tag{B.11}$$

$$det\,(\sigma_2 - \lambda I) = 0 \Leftrightarrow det \begin{pmatrix} -\lambda & 1 \\ 1 & -\lambda \end{pmatrix} = \lambda^2 - 1 = 0 \tag{B.12}$$

$$det\,(\sigma_3 - \lambda I) = 0 \Leftrightarrow det \begin{pmatrix} 1-\lambda & 0 \\ 0 & -1-\lambda \end{pmatrix} = 1 - \lambda^2 = 0 \tag{B.13}$$

Les trois matrices ont la même équation caractéristique, donc les mêmes valeurs propres, qui sont -1 et 1.

B.3.2 Vecteurs propres

Résultat 2 *Les bases x, y, z sont des bases ortonormées de vecteurs propres respectivement de σ_1, σ_2, σ_3.*

Partons de σ_3 :

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \quad \Rightarrow \quad a = a \quad ; \quad b = -b$$

On a donc un premier vecteur propre (normé) ,

$$|0\rangle_z = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{B.14}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = -\begin{pmatrix} a \\ b \end{pmatrix} \quad \Rightarrow \quad a = -a \quad ; \quad -b = -b$$

Donc, le deuxième vecteur propre (normé) est

$$|1\rangle_z = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{B.15}$$

Ensuite, pour σ_2, on trouve de façon similaire

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \quad \Rightarrow \quad a = b$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = - \begin{pmatrix} a \\ b \end{pmatrix} \quad \Rightarrow \quad b = -a$$

Les vecteurs propres sont donc

$$|0\rangle_y = \frac{|0\rangle_z + |1\rangle_z}{\sqrt{2}} \tag{B.16}$$

$$|1\rangle_y = \frac{|0\rangle_z - |1\rangle_z}{\sqrt{2}} \tag{B.17}$$

Enfin, pour σ_3

$$\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \quad \Rightarrow \quad a = ib$$

$$\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = - \begin{pmatrix} a \\ b \end{pmatrix} \quad \Rightarrow \quad a = -ib$$

Les vecteurs propres sont donc

$$|0\rangle_x = \frac{|0\rangle_z + i|1\rangle_z}{\sqrt{2}} \tag{B.18}$$

$$|1\rangle_x = \frac{|0\rangle_z - i|1\rangle_z}{\sqrt{2}} \tag{B.19}$$

Ce qui finit la démonstration.

B.4 Propriétes supplémentaires

Voici quelques propriétés immédiates :

$$Tr(\sigma_k) = 0 \tag{B.20}$$

$$det(\sigma_k) = -1 \tag{B.21}$$

Ensuite, calculons le commutateur de deux matrices de Pauli; on trouve aisément

$$[\sigma_k \ , \ \sigma_l] = \sigma_k\sigma_l - \sigma_l\sigma_k = 2i\varepsilon_{klm}\sigma_m \tag{B.22}$$

De même, on calcule facilement l'anti-commutateur :

$$\{\sigma_k \ , \ \sigma_l\}_+ = \sigma_k\sigma_l + \sigma_l\sigma_k = 2\delta_{kl}I \tag{B.23}$$

En particulier, $\sigma_k^2 = I$ et $\sigma_k\sigma_l = -\sigma_l\sigma_k$ pour $k \neq l$.

En prenant la somme de (C.22) et (C.23), on trouve

$$\sigma_k\sigma_l = \delta_{kl}I + i\varepsilon_{klm}\sigma_m \tag{B.24}$$

On prouve aussi, pour $\bar{a}$, $\bar{b}$ deux vecteurs de $\mathbb{R}^3$ (ou deux opérateurs vectoriels commutant avec les trois σ_k) :

$$(\bar{a}\cdot\bar{\sigma})(\bar{b}\cdot\bar{\sigma}) = (\bar{a}\cdot\bar{b})I + i\bar{\sigma}\cdot(\bar{a}\times\bar{b}) \tag{B.25}$$

En effet,

$$(\bar{a}\cdot\bar{\sigma})(\bar{b}\cdot\bar{\sigma}) = \sigma_k a^k\sigma_l b^l = a^k b^l\sigma_k\sigma_l = a^k b^l(\delta_{kl}I + i\varepsilon_{klm}\sigma_m)$$

$$(\bar{a}\cdot\bar{\sigma})(\bar{b}\cdot\bar{\sigma}) = \sum_k a^k b^k I + i\sum_m \sigma_m a^k b^l \varepsilon_{klm} = \bar{a}\cdot\bar{b}I + i\sum_m \sigma_m(\bar{a}\times\bar{b})^m = \bar{a}\cdot\bar{b}I + i\bar{\sigma}\cdot(\bar{a}\times\bar{b})$$

□

B.5 Algèbre de Clifford

Notons enfin une petite proptiété amusante des matrices de Pauli. L'ensemble des matrices complexes 2×2 formées par combinaison linéaire des σ_k forme un sous-espace vectoriel de dimension 3 de $\mathcal{M}$ (avec σ_k comme base), notons le $\mathcal{D}$.

Définition 1 *Soit V un espace vectoriel réel. S'l existe un produit $[\ ,\ ] : V\times V\to V$ tel que, $\forall\bar{a}$, $\bar{b}$, $\bar{c}\in V$, $\forall\lambda$, $\mu\in\mathbb{R}$:*

1. $[\bar{a},\lambda\bar{b}+\mu\bar{c}] = \lambda[\bar{a},\bar{b}] + \mu[\bar{a},\bar{c}]$ *(linéarité)*
2. $[\bar{a},\bar{b}] = -[\bar{b},\bar{a}]$ *(antisymmétrie)*
3. $\big[[\bar{a},\bar{b}],\bar{c}\big] + \big[[\bar{b},\bar{c}],\bar{a}\big] + \big[[\bar{c},\bar{a}],\bar{b}\big] = 0$ *(identité de Jacobi)*

alors on dit que V, muni de ce produit, forme une algèbre de Lie réelle, notée $\mathcal{V}$.

Par exemple, E_0^3, muni du produit vectoriel, forme une telle algèbre.

On en déduit l'existence de *constantes de structures* (f_{klm}).

Si $\bar{e}_k$ forme une base de V, alors

$$[\bar{e}_k,\bar{e}_l] = \sum_m f_{klm}\bar{e}_m \qquad \text{où} \qquad f_{klm} = -f_{lkm} \tag{B.26}$$

On voit immédiatement que $\mathcal{D}$, avec le commutateur comme produit interne, forme une telle algèbre de Lie, et les constantes sont données par (C.22) et sont donc $2i\varepsilon_{klm}$.

Définition 2 *Une algèbre de Clifford est une algèbre telle que, si γ_k forme une base,*

$$\{\gamma_k,\gamma_l\}_+ = 2\delta_{kl}I \tag{B.27}$$

Nous avons donc que $\mathcal{D}$ est une algèbre de Clifford de dimension 3, notée $\mathcal{C}_3$. En effet, cela découle de la propriété (C.23)

$$\{\sigma_k\ ,\ \sigma_l\}_+ = \sigma_k\sigma_l + \sigma_l\sigma_k = 2\delta_{kl}I$$

Annexe C

Affiches

Cryptographie quantique

ou distribution de clefs secrètes

Printemps des Sciences 2003 : La communication de l'électron au papillon

Présentation : Dramaix Florence, van den Broek Didier, Wens Vincent

Comment Alice et Bob peuvent-ils secrètement se transmettre un message?

Alice et Bob devront d'abord s'envoyer une clef (c'est-à-dire une suite de bits) connue d'eux seuls, qui leur permettra de coder et de déchiffrer un message. Ils utilisent cette clef et le code de Vernam pour le crypter.

Code de Vernam

XOR :

$\oplus$	0	1
0	0	1
1	1	0

message à crypter		10100	message reçu(crypté)		11001
clef	$\oplus$	01101	clef	$\oplus$	01101
message crypté		11001	message initial		10100

Pour mettre tout ceci en œuvre, Alice et Bob vont faire appel à la *cryptographie quantique* qui se base sur la *mécanique quantique*.

Les trois propriétés principales utilisées sont :
- Les résultats d'une mesure quantique sont distribués de manière probabiliste.
- Le principe de superposition empêche la *duplication parfaite*.
- Toute mesure perturbe le système.

Principe de la cryptographie quantique

Toute écoute d'un canal quantique provoque des perturbations. (erreurs chez Bob)

Le protocole utilisé: Bennett et Brassard 1984 (BB84)

Alice utilise des photons polarisés soit horizontalement, soit verticalement (base H/V), soit diagonalement ou anti-diagonalement (base D/A), pour envoyer des bits à Bob.

Plusieurs cas se présentent :
- Bob a choisi la même orientation du polariseur (même base), alors il est sûr de trouver l'état de polarisation envoyé par Alice;
- Bob a choisi l'autre orientation, il a alors une chance sur deux de trouver l'état de polarisation envoyé par Alice.

Les attaques

Ève veut espionner Alice et Bob et découvrir leur clef.

Alice et Bob envoient leurs photons via un canal quantique. Alice choisit aléatoirement ses bases et l'état de polarisation des photons; Bob fait de même pour ses bases et mesure les photons. Via un canal classique authentifié, ils s'échangent le choix des bases et gardent les bases communes.

Théorème 1 *Alice et Bob abandonnent leur clef dès que Ève possède autant d'information que Bob sur celle-ci.*

Étudions deux types d'attaque :

Interception et réémission : "Intercept and resend"

Avec une probabilité ω, Ève choisit une base, mesure et envoie l'état de polarisation trouvé à Bob. Comme elle *mesure*, elle perturbe la polarisation du photon et Bob aura des erreurs dans sa chaîne de bits.

Les informations de Bob $\mathbf{I_{AB}}$ et d've $\mathbf{I_{AE}}$ sont	Si $\omega < 1 \Rightarrow$ clef pas connue d'Eve
$I_{AB} = \log_2\left(2 - \frac{\omega}{2}\right) + \frac{\omega}{4}\log_2\left(\frac{4}{\omega} - 1\right)$	Si $\omega = 1 \Rightarrow$ clef abandonnée
$I_{AE} = \frac{1}{2}\log_2\left(1 - \frac{\omega^2}{4}\right) + \frac{\omega}{4}\log_2\left(\frac{1+\frac{\omega}{2}}{1-\frac{\omega}{2}}\right)$	$P_{\text{erreur}} = 0.25 \quad \text{pour} \quad \omega = 1$

Duplication : "L'attaque des clones"

Ève possède une machine qui *clone* les photons. Après avoir éliminé les mauvaises bases, elle a en principe autant d'information que Bob. Cependant...

Théorème 2 *On ne peut cloner un ensemble d'états non orthogonaux; la duplication parfaite d'un photon est impossible.*

Ève utilise comme transformation "cloneuse":

$$U\left(|0\rangle_{yA}|0\rangle_{yE}\right) = |0\rangle_{yA}|0\rangle_{yE}$$
$$U\left(|1\rangle_{yA}|0\rangle_{yE}\right) = \cos(\theta)|1\rangle_{yA}|0\rangle_{yE} + \sin(\theta)|0\rangle_{yA}|1\rangle_{yE}$$

Par ce théorème, Ève perturbe encore le photon d'Alice, et pourra alors être détectée.

Les informations de Bob $\mathbf{I_{AB}}$ et d'Ève $\mathbf{I_{AE}}$ sont
$I_{AB} = \frac{1}{2}\left[(1+\cos\theta)\log_2(1+\cos\theta) + (1-\cos\theta)\log_2(1-\cos\theta)\right]$
$I_{AE} = \frac{1}{2}\left[(1+\sin\theta)\log_2(1+\sin\theta) + (1-\sin\theta)\log_2(1-\sin\theta)\right]$
Si $\theta < \frac{\pi}{4} \Rightarrow$ clef pas connue d'Ève
Si $\theta \geq \frac{\pi}{4} \Rightarrow$ clef abandonnée
$P_{\text{erreur}} = 0.1464 \quad \text{pour} \quad \theta = \frac{\pi}{4}$

où θ est un paramètre contrôlé par Ève représentant la force de l'attaque.

Pour une quantité d'information donnée, Ève introduit plus d'erreur chez Bob avec "intercept and resend" qu'avec la duplication.

Annexe D

Documents autres que LaTeX

Cette dernière annexe est constituée des pages *Maple* que nous avons utilisées pour réaliser certains de nos calculs et nos graphiques.

De plus, nous avons joint le programme de notre simulation qui a été réalisée au moyen de *LabVIEW* et que les visiteurs ont pu utiliser. Nous n'avons imprimé que quelques cas intéressants.

Bibliographie

[1] Gérard Battail, *Théorie de l'information : application aux techniques de communication*, Collection Pédagogique de Télécommunication (1997).

[2] Thomas M. Cover, Joy A. Thomas, *Elements of information theory*, Wiley series in telecommunications (1991).

[3] Claude Cohen-Tannoudji, Bernard Diu, Franck Laloë, *Mécanique quantique*, volumes 1 et 2, collection enseignement des sciences (2000).

[4] A. Messiah, *Mécanique quantique*, Dunod (1969).

[5] P. Gaspard, cours de *Mécanique quantique*, 1$^{\text{er}}$ et 2$^{\text{ème}}$ fascicule (2001-2002) et le cours oral de J. Turner.

[6] P. Godin, J-P. Gossez et L. Lemaire, cours de *Calcul différentiel et intégral*, 1$^{\text{er}}$ et 2$^{\text{ème}}$ partie.

[7] http://www.qubit.org

[8] http://www.idquantique.com

[9] http://www.gap-optique.unige.ch

[10] www.comelec.enst.fr