Université Libre de Bruxelles

Synthèse

Quantum Information and Comutation
INFO-H514

Auteur :
Nicolas Englebert

Professeur :
Nicolas Cerf

Année 2017 - 2018

Appel à contribution

Synthèse Open Source

Ce document est grandement inspiré de l'excellent cours donné par Nicolas Cerf à l'EPB (École Polytechnique de Bruxelles), faculté de l'ULB (Université Libre de Bruxelles). Il est écrit par les auteurs susnommés avec l'aide de tous les autres étudiants et votre aide est la bienvenue ! En effet, il y a toujours moyen de l'améliorer surtout que si le cours change, la synthèse doit être changée en conséquence. On peut retrouver le code source à l'adresse suivante

`https://github.com/nenglebert/Syntheses`

Pour contribuer à cette synthèse, il vous suffira de créer un compte sur *Github.com*. De légères modifications (petites coquilles, orthographe, ...) peuvent directement être faites sur le site ! Vous avez vu une petite faute ? Si oui, la corriger de cette façon ne prendra que quelques secondes, une bonne raison de le faire !

Pour de plus longues modifications, il est intéressant de disposer des fichiers : il vous faudra pour cela installer LaTeX, mais aussi *git*. Si cela pose problème, nous sommes évidemment ouverts à des contributeurs envoyant leur changement par mail ou n'importe quel autre moyen.

Le lien donné ci-dessus contient aussi un `README` contenant de plus amples informations, vous êtes invités à le lire si vous voulez faire avancer ce projet !

Licence Creative Commons

Le contenu de ce document est sous la licence Creative Commons : *Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0)*. Celle-ci vous autorise à l'exploiter pleinement, compte- tenu de trois choses :

1. *Attribution* ; si vous utilisez/modifiez ce document vous devez signaler le(s) nom(s) de(s) auteur(s).
2. *Non Commercial* ; interdiction de tirer un profit commercial de l'œuvre sans autorisation de l'auteur
3. *Share alike* ; partage de l'œuvre, avec obligation de rediffuser selon la même licence ou une licence similaire

Si vous voulez en savoir plus sur cette licence :

`http://creativecommons.org/licenses/by-nc-sa/4.0/`

Merci !

Table des matières

Chapitre 1

Cours 1

1.1 Introduction

Le nombre des transistor sur les circuits intégrés double tous les 18 mois. Si on continue ainsi, les transistor auront atteint la taille d'un atome d'hydrogène d'ici 2030. On ne peut plus échapper à une vision quantique de la théorie de l'information.

La *théorie quantique* (début 1900), pour les physiciens, cherche à comprendre la matière à l'échelle atomique. D'autre part, la *théorie de l'information* (début 1940), pour les ingénieurs, cherche à caractériser l'information et à élaborer des moyens de communications. L'union des deux a donné naissance à la *théorie de l'information quantique*, où l'on a développé un équivalent quantique aux notions classiques

Quantum bits, quantum logic gates, quantum circuit, quantum computer, ...

Cette théorie concerne à la fois les physiciens *et* les ingénieurs quantiques. La motivation de l'ingénieur consiste à pousser les limites de la théorie de l'information quantique (des ordinateurs qui peuvent résoudre des problèmes difficiles, des moyens de communications basés sur la téléportation, un codage dense et de nouvelle techniques de cryptographie). Pour le physicien, c'est un nouveau champ passionnant (par exemple, la téléportation quantique théorisée en 1933 et démontrée en 1998).

Certains dispositifs basés sur des applications quantiques existent déjà aujourd'hui. La compagnie *ID Quantique* (Genève) commercialise un processus de cryptage des fibres optiques.

Outlines of this course

- De la théorique classique à quantique.
- Qu'est ce qui est vraiment spécial aux qbit (optiques) ? Application : algorithmes quantiques.
- Qu'est ce qui est si spéciale à l'intrication ? Application : téléportation quantique.

1.2 Théorie de l'information : du classique au quantique

1.2.1 Commençons classiquement : Shannon

La technologie actuelle se base sur la théorie de l'information élaborée par Shannon (1948 et 1949). Elle se base sur deux grands principes :

Mesure de l'information Chaque type d'information (texte, image, son) peut être associé à un **contenu d'information**, qui quantifie avec quelle efficacité elle peut être représentée par des 0 et 1.

Limite sur les communications Tout canal de communication imparfait (téléphone, radio, satellite) à une **capacité** qui quantifie la quantité d'information qui peut être transmise correctement sur un canal.

Source coding theorem (codage sans bruit)

Le plus grand taux de compression des données pour une source est donnée par l'**entropie de Shannon** $H = f$(statistique de la source).

$$01\cancel{1}010\cancel{01}1110\cancel{1}001 \quad \Rightarrow \quad 01|010|110|01 \tag{1.1}$$

→ Faire un "*code source*", c'est supprimer la redondance

Channel coding theorem (codage bruité)

Le plus grand taux de transmission possible via un canal est donné par la **capacité de Shannon** $C = f$(statistique du bruit).

$$0101011001 \quad \Rightarrow \quad 011010011101001 \tag{1.2}$$

→ Faire un "*code correcteur d'erreur*", c'est ajouter de la redondance.

Exemple: source coding.
La *source* est une variable aléatiore définie par

$$p(x) = \begin{cases} 1/2 & x = A \\ 1/4 & x = B \\ 1/8 & x = C \\ 1/8 & x = D \end{cases} \tag{1.3}$$

On lui associe le codage simple $A \to 00, B \to 01, C \to 10, D \to 11$. Ainsi, $L = 2$ bits par symbole. On peut calculer l'entropie

$$H(X) = -\sum_{x=A}^{D} p(x) \log_2 p(x) = \frac{1}{2} + \frac{2}{4} + \frac{3}{8} + \frac{3}{8} = \frac{7}{4} < 2 \tag{1.4}$$

La longueur moyenne d'un code L est supérieure où égale à l'entropie

$$L \geq H(X) \tag{1.5}$$

Avec un codage plus intelligent, on peut saturer la précédente inégalité. Le codage $A \to 0, B \to 10, C \to 110, D \to 111$ donne

$$L := \frac{1}{2} * 1 + \frac{1}{4} * 2 + \frac{1}{8} * 3 + \frac{1}{8} * 3 = \frac{7}{4} < 2 \tag{1.6}$$

Ici, $L = 7/4$ bits par symbole.

1.2.2 Information et physique

Rolf Landauer a donné de fortes implications liée au fait que l'**information est physique**. Il en découle deux grands principes

Il n'y a pas d'information sans représentation Chaque bit d'information doit être transporté par un *système physique*, ce n'est pas un concept immatériel.

Il n'y a pas de traitement sans processus Chaque traitement de l'information doit être réalisé par un *processus physique.*

Information de thermodynamique

Stocker un bit à un coût thermodynamique du à l'irréversibilité. Si l'on cherche à décrire un calcul classique, il sera irréversible et va ainsi dissiper de l'énergie. Par exemple, quand on veut effacer de l'information c'est quelque chose d'irréversible, qui coûte donc de l'énergie. On s'intéresse ici à l'effacement de "010010101110101001000101", qui correspond à une température T. On veut le changer en "000000000000000000000", correspondant à une température 0.

Principe de Landauer
Le coût thermodynamque de l'effacement d'un bit est (en joules)

$$\ln(2)kT \tag{1.7}$$

C'est un processus *irréversible.*

La notion d'un ordinateur classique réversible est précurseur à la notion de codage quantique.

Logique réversible et irréversible

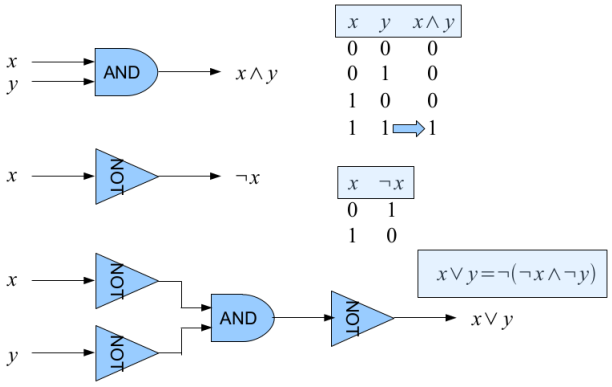

Figure 1.1

Ci-contre, les plus connues de portes logiques. La porte *AND* est irréversible car si la sortie est 0, il n'est pas possible de savoir quel était l'entrée. Par contre la porte *NOT* est réversible (on peut connaître l'entrée avec la sortie). La dernière est une composition des deux dernières portes avec une irréversibilité. Il s'agit d'une porte *OR*. Ceci signifie que l'on va dissiper de l'énergie à un moment donné. **Les portes *AND* et *NOT* forment un ensemble universel de portes irréversibles**.

Pour créer un porte universelle réversible, il faut avoir 3 bits. Si on parvient à faire quelque chose de totalement réversible, on pourrait créer un ordinateur sans coût ni énergie. La porte *Toffoli* copie x et y puis, pour z

$$z \to z \oplus (x \wedge y) \tag{1.8}$$

On peut voir $x \oplus y$ comme $\mod_2(x+y)$ (voir tableau ci-contre). Il s'agit du *NOT EXCLUSIF*. Si x **et** y valent 1, on effectue *NOT* z. Sinon, on copie z. On peut prouver que cette porte

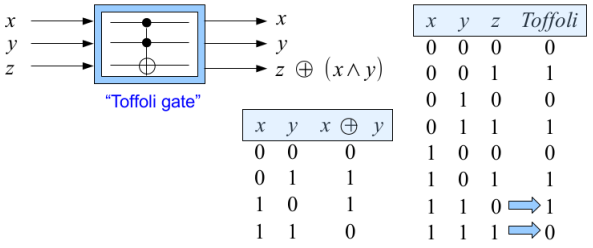

Figure 1.2

est suffisante pour implémenter chaque porte logique, elle est universelle. On a pensé que c'était le futur des ordinateurs car ils ne dissipent aucune énergie, mais on ne savait pas l'implémenter. C'est la première étape vers les ordinateurs quantiques. On a quelque chose d'universel et maintenant, on veut aller vers le quantique.

1.3 Information et physique quantique

Qu'est ce qui se passe si l'on encode l'information dans les états d'un système quantique ? N'importe quel système à deux niveaux (spin, polarisation des photons, ...) peut être utilisé pour faire un qbit. Alors qu'un bit ne peut prendre que 0 et 1 comme valeur, un qbit peut être dans une superposition.

$$\alpha\,|0\rangle + \beta\,|1\rangle \tag{1.9}$$

Cela signifie qu'il peut exister dans n'importe quel état combili de deux. Chaque état qbit peut être représenté par un vecteur dans une sphère. On peut ainsi être "entre le mode *on* et *off*" pour lequel il n'existe pas d'équivalent classique. La superposition n'est **pas** une mixture probabilistique (parfois 1, parfois 0). Si l'on a une superposition pour des milieurs de particules, on parlera d'intrication (plus qu'une corrélation classique).

Les qbits optiques sont des photons. Si on a une onde plane, on peut lui associer une polarisation linéaire. Si la polarisation est horizontale, c'est $|0\rangle$ et si elle est verticale $|1\rangle$. Un photon et son état de polarisation transporte un qbit. Il peut avoir une polarisation diagonale (45°) via superposition quatique

$$|0\rangle + |1\rangle \tag{1.10}$$

C'est bien le résultat d'une superposition et **pas** "parfois vertical, parfois horizontal". C'est un photon qui a une polarisation le long de la diagonale. En mesurant on aura l'un ou l'autre, mais avant il s'agit clairement d'une superposition.

Avec un McZehnder, un faisceau peut être spatialement séparé en deux. L'onde réfléchie gagne une phase de $\pi/2$ et il y a deux sorties possibles : l'une verra des interférence constructives, l'autre destructives (gauche). Diminuons l'intensité de la source pour n'avoir plus que un photon (ça existe !). A priori, si on envoie un photon, on ne devrait pas avoir de détection la ou il y avait des interférences destructives (centre). Si on mesure avec deux détecteurs, on n'a jamais de superposition : clic à gauche ou à droite (probabilité 1/2), mais pas les deux (droite). Ceci montre qu'il n'y a qu'un seul photon dans l'interféromètre.

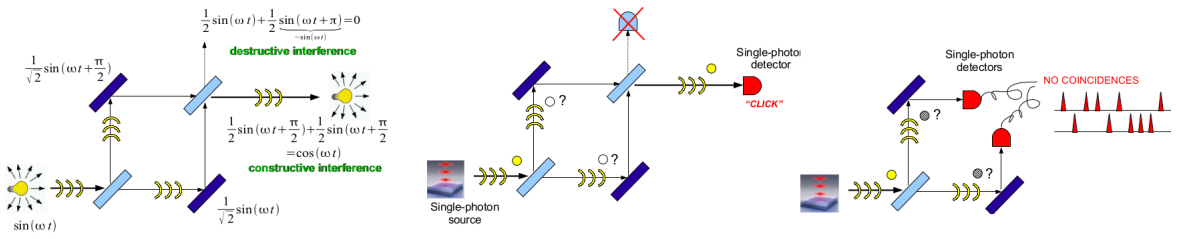

FIGURE 1.3

D'un point de vue physique **classique**, le photon est toujours détecté dans le même détecteur et ce peu importe le chemin qu'il emprunte comme le montre l'image ci-dessous

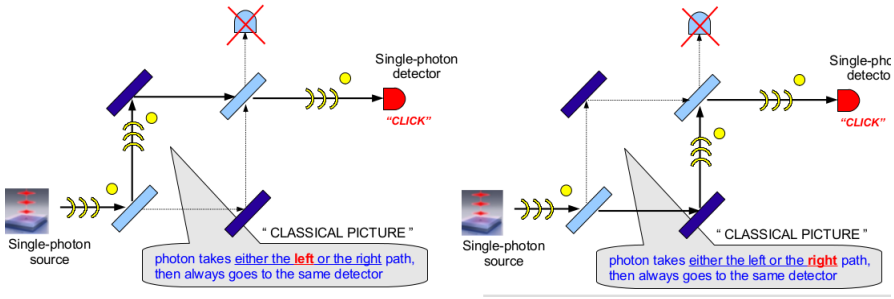

FIGURE 1.4

Insérons maintenant une lame de phase. Sa présence fait que ça interfère et l'on a maintenant des clic à l'autre détecteur (gauche). D'un point de vue **classique**, le clic est indépendant du chemin suivi. Un photon qui va tout droit va traverser la lame de phase et provoquer un clic dans le détecteur du haut (centre). Toujours classiquement, un photon qui prend le chemin de gauche doit aussi faire un clic sur le détecteur du haut (droite), mais **comment un photon du chemin de gauche peut-il sentir la lame de phase du "chemin droit"** ?

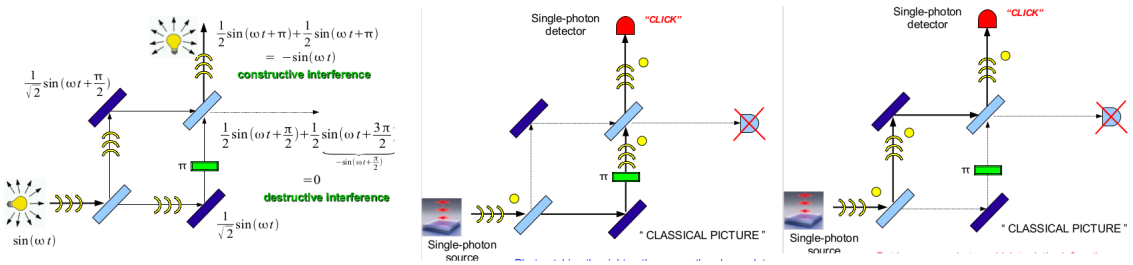

FIGURE 1.5

C'est possible par **dualité**. Le photon n'est pas "à gauche ou à droite", mais dans une superposition entre les deux.

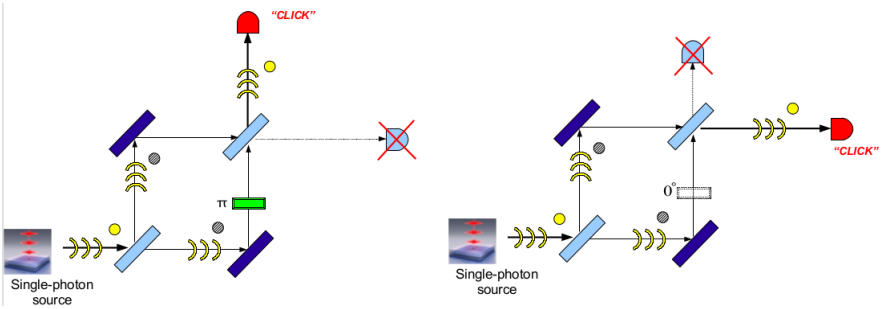

FIGURE 1.6

1.3.1 Dans un langage quantique

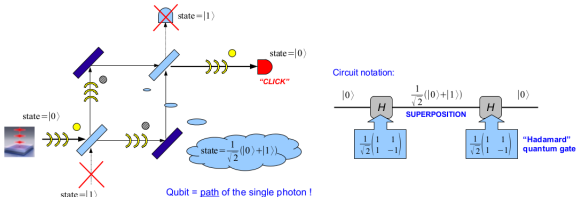

FIGURE 1.7

Dans l'interféromètre, entre les deux beamspliter, on peut noter l'état comme une superposition

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{1.11}$$

Le **qbit est le chemin d'un unique photon**. Adoptons la notation mathématique des vecteurs d'états (vecteurs complexes de dimension deux dans l'espace d'Hilbert)

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1.12}$$

On peut transcrire le McZehnder en circuit à l'aide des portes d'HADAMARD

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{1.13}$$

En effet, nous partons de $|0\rangle$ et nous passons la première porte (beamsplit)

$$H\,|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{1.14}$$

Il s'agit d'une superposition quantique. Ici, la probabilité d'avoir l'un ou l'autre (mesure) est de 1/2.L'état $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ passe alors la seconde porte (deuxième BS)

$$H\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right] = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \tag{1.15}$$

Nous avons bien décrit la situation de la figure 1.7, dans un langage quantique.

1.3.2 Parallélisme quantique

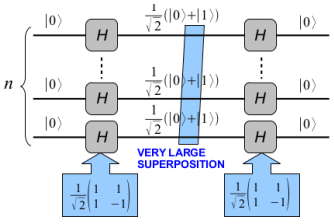

FIGURE 1.8

On aimerait cette fois avoir tous les états en même temps. A l'entrée et à la sortie, nous n'avons toujours que des $|0\rangle$. Entre les deux, c'est plus intéressant : nous avons une superposition qui donne un nombre exponentiel de terme. Avec seulement n qbits, on peut obtenir l'entièreté de $\mathcal{H}$. Chaque qbit à la même histoire, mais l'état joint peut être décrit comme une superposition exponentielle de 2^n états pour n qbits. Par exemple, si $n = 3$:

$$(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) = \underbrace{|0\rangle\,|0\rangle\,|0\rangle}_{'0'} + \underbrace{|0\rangle\,|0\rangle\,|1\rangle}_{'1'} + \underbrace{|0\rangle\,|1\rangle\,|0\rangle}_{'2'} + \cdots + \underbrace{|1\rangle\,|1\rangle\,|1\rangle}_{'7'} \tag{1.16}$$

1.3.3 Intrication quantique

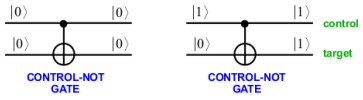

FIGURE 1.9

Ci-contre, une porte *CONTROL-NOT*. Il s'agit d'une porte qui agit sur deux bits (l'idée est la même que la porte sans pertes à 3 bits). Le qbit supérieur est celui de *contrôle*, il ne change pas. En dessous, c'est le qbit *cible* qui est inversé (*NOT*) si le qbit de contrôle est $|1\rangle$ (*CONTROL*).

Le contrôle dit s'il faut inverser la cible, mais que se passe-t-il si le contrôle est une superposition quantique de ses deux états possibles ? Si $|0\rangle$ ça change rien, mais si $|1\rangle$ (contrôle) alors il faut que $|0\rangle \rightarrow |1\rangle$ (cible). Le nouvel état de sortie peut être écrit

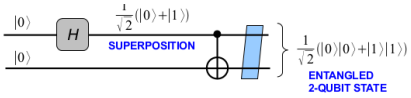

FIGURE 1.10

$$\frac{1}{\sqrt{2}}\left(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle\right) \tag{1.17}$$

Cet état est intéressant car même si on change de base ($|0\rangle, |1\rangle$ n'est qu'un choix) on ne sera jamais capable d'écrire cet état de sortie comme un produit. Il est dit **intriqué** : il n'est pas possible d'écrire chaque qbit séparément, on doit l'écrire comme tel.

À retenir*:* On peut construire n'importe quel circuit quantique en combinant la porte d'HADAMARD H et une porte quantique à 2-qbit (comme ci-dessus).

$$\text{Circuit quantique} = \{\text{Porte quantique à 1-bit, Portes quantique à 2-bit}\}$$

Ceci donne lieux à des états à n-qbit fortement intriqués. Pas besoin d'avoir 3 qbits ici.

1.3.4 Circuit quantique (exemple)

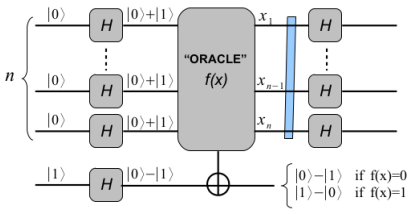

FIGURE 1.11

Nous avons un **oracle** $f(x)$, une boîte noire. Le but de l'algorithme est de dire ce que faire l'oracle de façon quantique en explorant toutes ses entrées possibles en même temps. Nous savons que nous aurons à la superposition de toutes les possibilités. Ainsi, le vecteur x est la superposition de toutes les entrées possibles !

D'abord, le vecteur x est copié (à droite de l'oracle). Ensuite, l'oracle va inverser le qbit $(n+1)$ si $f(x) = 0$ ou $f(x) = 1$. C'est comme ça qu'on défini l'oracle (c'est une sorte de grosse porte *CTRL-NOT*).

$$|0\rangle - |1\rangle \quad \Rightarrow \quad \begin{cases} |0\rangle - |1\rangle & \text{si } f(x) = 0 \\ |1\rangle - |0\rangle & \text{si } f(x) = 1 \end{cases} \tag{1.18}$$

On peut réécrire ce "flip" comme un facteur de phase. Avant la seconde porte d'HADAMARD (rectangle bleu), on a alors l'état suivant

$$\sum_{\vec{x}=00\ldots0}^{11\ldots1} (-1)^{f(\vec{x})}\,|x_1\rangle\,|x_2\rangle \ldots |x_n\rangle\,(|0\rangle - |1\rangle) \tag{1.19}$$

La somme est présente car nous avons bien toutes les possibilités d'entrées. Pour voir ce qui se passe après la deuxième "colonne de H", remarquons que nous pouvons réécrire la porte

d'HADAMARD de la façon suivante

$$\left.\begin{array}{ll} H|0\rangle & = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H|1\rangle & = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array}\right\} \quad \Rightarrow \quad H|x\rangle = \frac{1}{\sqrt{x}} \sum_{y=0}^{1} (-1)^{xy} |y\rangle \tag{1.20}$$

En utilisant cette dernière relation, on obtient en sortie

$$\sum_{\vec{x}=00\ldots0}^{11\ldots1} (-1)^{f(\vec{x})} \underbrace{\sum_{\vec{y}=00\ldots0}^{11\ldots1} (-1)^{\vec{x}\vec{y}} |y_1\rangle |y_2\rangle \ldots |y_n\rangle}_{\text{Effet des } H \text{ sur } |x_1\rangle|x_2\rangle\ldots|x_n\rangle} \tag{1.21}$$

où $\vec{x}\vec{y} = x_1y_1 + x_2y_2 + \cdots + x_ny_n$. Échangeons les deux sommations

$$\sum_{\vec{y}=00\ldots0}^{11\ldots1} \left[\sum_{\vec{x}=00\ldots0}^{11\ldots1} (-1)^{f(\vec{x})+\vec{x}\vec{y}} \right] |y_1\rangle |y_2\rangle \ldots |y_n\rangle \tag{1.22}$$

Nous avons maintenant une somme sur $\vec{y}$ pondérée par un coefficient qui donnera la probabilité d'amplitude de chaque sortie possible (entre crochets). Après mesure, nous aurons des 0/1.

1.3.5 Algorithme quantique (Deutsch-Josza)

L'idée principale de savoir si nous avons une fonction $f(x)$ constante ou *balanced*. Nous avons $f(x)$ et nous voulons savoir quelque chose sur lui en minimisant le nombre de requête.

Fonction constante

Si la fonction est constante, on remplace $f(\vec{x})$ par zéro. L'amplitude de probabilité devient

$$\left[\sum_{\vec{x}=00\ldots0}^{11\ldots1} (-1)^{\vec{x}\vec{y}} \right] = 0 \tag{1.23}$$

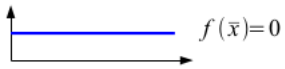

FIGURE 1.12

Sauf si $y_1 = y_2 = \cdots = 0$. On peut la réécrire

$$\underbrace{\sum_{x_1=0}^{1} (-1)^{x_1y_1}}_{y_1=0} \underbrace{\sum_{x_2=0}^{1} (-1)^{x_2y_2}}_{y_2=0} \ldots \tag{1.24}$$

On mesurera alors toujours $000\ldots0$ (seul état de probabilité non nulle).

Fonction "balanced"

Dans ce cas (autant de 0 que de 1), nous avons $f(\vec{x}) = x_1$. En remplaçant

$$\left[\sum_{\vec{x}=00\ldots0}^{11\ldots1} (-1)^{x_1+\vec{x}\vec{y}} \right] = 0 \tag{1.25}$$

FIGURE 1.13

Sauf si $y_1 = 1, y_2 = \cdots = y_n = 0$. On va alors mesurer $100\ldots0$.

En **un seul appel**, on peut distinguer si on a une fonction constante ou balancée (grâce au parallélisme quantique). En mesurant la sortie, on peut directement savoir ça. Classiquement, dans le pire des cas, il faudrait faire au moins la moitié de toutes les entrées [1] pour s'assurer qu'il n'y a pas de montée (elle serait alors constante) ce qui demanderait $2^n/2 = 2^{n-1}$ appels ! On comprend ici l'intérêt de l'algorithme quantique.

1. Voir schéma notes

Chapitre 2

What does entanglement have to do with computer science ?

2.1 Introduction

L'idée est d'utiliser les qbits pour avoir des algorithmes plus efficace, mais ceux-ci sont fragiles et se détruisent vite. A cause de la *décohérence* qui est une source forte d'erreurs, on perd rapidement toutes les belles propriétés quantiques comme la superposition.

Au début, à cause de la décohérence, tout était théorique. Mais après est venu l'idée de prolonger l'idée des codes correcteurs d'erreur au monde quantique. A cause du *théorème de non-clonage quantique* (cours 3) qui dit qu'un qbit ne peut pas être parfaitement cloné, on pourrait croire qu'on ne peut pas faire des codes correcteurs d'erreurs. Nous montrerons cependant que nous pouvons.

2.1.1 Correction d'erreur classique

Il s'agit du cas classique et trivial, c'est le codage répétitif (on introduit de la redondance). Le même bit est dupliqué trois fois et on l'envoie. Il peut y avoir des erreurs à cause de l'environnement que l'on peut corriger via cette redondance. Mais en quantique, on ne peut pas faire ça.

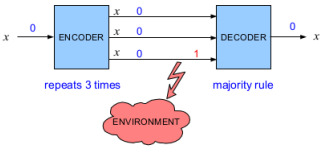

FIGURE 2.1

2.1.2 Correction d'erreur quantique

Soit un qbit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. On l'envoie dans un encodeur quantique U_{ENC} avec une superposition quantique, n'importe laquelle (ici $n = 4$). Nous allons faire une opération telle que les cinq états de qbits sont **intriqués** (on ne peut pas les décomposer dans un état pur de chaque qbit) : ils définissent un état pur pour les 5 qbits **ensemble**.

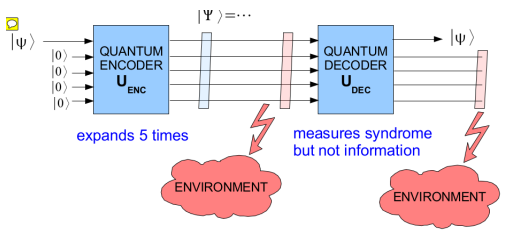

FIGURE 2.2

Il y a des interaction avec l'environnement et, imaginons, le 5^e qbit est touché. Vient le décodage avec U_{DEC} ou le *syndrome* est séparer de l'*information*. Le syndrome informe qu'il y a eu une erreur sur le 5^e qbit (par exemple, il a flip). Durant le décodage, on sépare donc le syndrome (quatre derniers qbits) et l'information (le premier).

Si on mesure les quatre bits à la fin, on verra le sydrome et ce qui est arrivé au qbit. Mais nous n'avons pas besoin de cette information : ce qui importe, c'est d'avoir $|\psi\rangle$ à la fin. C'est le rôle du décodeur, mais nous n'explicitons pas comment il procède. Nous ne voulons pas mesurer $|\psi\rangle$ car la mesure détruit l'information. Le truc, c'est qu'une erreur qui affecte un des cinq qbits peut être restaurée car quand l'environnement jour son rôle, le qbit est intriqué. L'idée est donc bien d'encoder un qbit dans cinq qbit et que celui-ci puisse survivre de l'erreur sur un des cinq qbits (interaction avec l'environnement) via l'opération de décodage.

This course
Que vient faire l'intrication quantique dans la science informatique ? Application : *distributed computing problem.*

2.2 What does entanglement have to do with computer science ?

Nous allosn réinterpréter un paradoxe quantique en langage de l'information. Nous allons ensuite l'appliquer sur un problème académique puis sur un problème "réel".

2.2.1 Problème académique

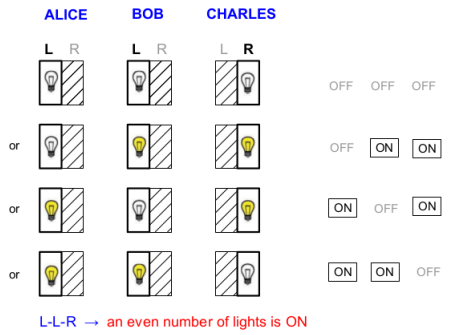

FIGURE 2.3

Alice, **B**ob et **C**harles achètent tous les trois une *magic box* dans une *magasin quantique* et ils s'en vont tous les trois dans des pays différents. Ensuite, chacun ouvre la moitié de sa boite (partie gauche L et droite R) pour y voir une ampoule allumée (*on*) ou éteinte (*off*).

Alice et Bob décident tous deux d'ouvrir la partie gauche tandis que Charles ouvre la partie de droite : configuration LLR. Il y a plusieurs possibilité (On/Off), mais dans tous les cas, un nombre **pair** de lumière est *on*. Dans la configuration RLL (permutation cyclique), le constat est le même : un nombre **pair** de lumière est *on*.

Dans les configuration LLR, RLL et LRL, nous devons avoir un nombre pair de *on*. Nous allons essayer de décrire mathématiquement ce que nous avons observés en définissant un bit de la sorte

$$\begin{cases} On & \equiv +1 \\ Off & \equiv -1 \end{cases} \qquad (-1)^{0,1} \tag{2.1}$$

Notre situation correspond donc à

$$\begin{array}{lll} LLR & \to A_L \times B_L \times C_R & = +1 \\ RLL & \to A_R \times B_L \times C_L & = +1 \\ LRL & \to A_L \times B_R \times C_L & = +1 \end{array} \tag{2.2}$$

Alice, Bob et Charles sont spatialement séparés : aucun d'eux ne sait si les deux autres ont regardés la partie gauche ou droite de leur boîte. Juste par causalité, Alice ne peut pas avoir des informations sur Bob et Charles : quand elle ouvre, elle est ignorante. Nous pouvons ainsi faire l'hypothèse que les variables L et R **existent** : Alice n'a peut-être pas regardé A_R, mais la variable existe (et c'est le cas pour les six variables).

Nous pouvons faire une prédiction grâce à ce modèle simple si l'on effectue la multiplication colonne par colonne. En effet, $A_L * A_L * A_R = A_L^2 * A_R = A_R$, on en tire donc

$$RRR \quad \rightarrow A_R \times B_R \times C_R = +1 \tag{2.3}$$

Le nombre de lumière allumée devrait être **pair** dans la configuration RRR. Malheureusement, l'expérience nous montre que c'est un nombre **impair** [1]. Il y a donc quelque chose de faux dans notre modèle.

Récapitulons. Nous avons six variables

$$A_L, A_R, B_L, B_R, C_L, C_R \in \{+1, -1\} \tag{2.4}$$

Prédiction $A_R \times B_R \times C_R = +1$. En **supposant** que ces variables existent simultanément.

Observation $A_R \times B_R \times C_R = -1$. En réalisant que ces boîtes magiques contiennent des **qbits**.

Supposer que les six variables existent en même temps ne peut être que faux. Comment s'en sortir ?

2.2.2 Quantum miracle

La physique classique ne parvient pas à expliquer l'observation, la solution sera un état intriqué. On assigne à A le bit 1, B le second et C le troisième mais nous les décrivons *ensemble*

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \left\{ |0,0,0\rangle_{A,B,C} - |1,1,1\rangle_{A,B,C} \right\} \qquad \text{"GHZ"} \tag{2.5}$$

Il s'agit de la superposition de deux états, mais intriqués. A, B et C ne peuvent pas être dans un état pur, on doit les décrire ensemble : on ne peut pas les exprimer comme un produit.

Choisissons la convention (base) suivante

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.6}$$

Il s'agit de deux vecteurs d'un espace 2D. Une mesure doit être associée à un observable. On va utiliser les matrices de Pauli qui correspondent à la mesure du spin. Ainsi, si le qbit est un spin 1/2, σ_x mesure la composante de spin dans l'axe x. Les trois matrices de Pauli sont les suivantes

$$\begin{array}{ccc} \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} & \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ \text{BIT FLIP} & \leftarrow \text{BOTH} \rightarrow & \text{SIGN FLIP} \\ \begin{cases} \sigma_x |0\rangle &= |1\rangle \\ \sigma_x |1\rangle &= |0\rangle \end{cases} & \begin{cases} \sigma_y |0\rangle &= i |1\rangle \\ \sigma_y |1\rangle &= -i |0\rangle \end{cases} & \begin{cases} \sigma_z |0\rangle &= |0\rangle \\ \sigma_z |1\rangle &= -|1\rangle \end{cases} \end{array} \tag{2.7}$$

On peut ainsi voir σ_x comme un *bit flip* : si on l'applique sur $|0\rangle$ on obtient un $|1\rangle$ et inversement. Ça correspond à une porte *NOT*. La matrice σ_z correspond au *sign flip* : $|0\rangle$ reste lui-même mais $|1\rangle$ change de signe. Les valeurs propres des matrices de Pauli sont les suivantes

$$\{+1, -1\} \equiv \{OFF, ON\} \tag{2.8}$$

1. C'est pas une explication ici, une observation

Supposons maintenant que l'action *ouvrir à gauche* L corresponde à mesurer σ_y et R corresponde à σ_x. Traduisons notre précédent système en langage quantique

$$\begin{aligned} LLR &\to \sigma_y \otimes \sigma_y \otimes \sigma_x \left|\Psi\right\rangle &= \left|\Psi\right\rangle \\ RLL &\to \sigma_x \otimes \sigma_y \otimes \sigma_y \left|\Psi\right\rangle &= \left|\Psi\right\rangle \\ LRL &\to \sigma_y \otimes \sigma_x \otimes \sigma_y \left|\Psi\right\rangle &= \left|\Psi\right\rangle \end{aligned} \tag{2.9}$$

avec $\left|\Psi\right\rangle = \frac{1}{\sqrt{2}}\left\{\left|0,0,0\right\rangle_{A,B,C} - \left|1,1,1\right\rangle_{A,B,C}\right\}$ et chaque matrice de Pauli porte sur un qbit différent. On retrouve bien à chaque fois $\left|\Psi\right\rangle$, ce qui signifie que le nombre de lumière allumée est **pair**. On peut dire que $\left|\Psi\right\rangle$ est un état propre commun du produit de ces trois observables avec comme valeur propre $+1$.

Une propriété importante des matrices de Pauli est leur anti-commutation : il faut placer un "-" lorsqu'on change l'ordre. C'est ce qui va produire le *miracle quantique*.

$$\{\sigma_x, \sigma_y\} \equiv \sigma_x\sigma_y + \sigma_y\sigma_x = 0 \tag{2.10}$$

Essayons de refaire notre prédiction. Nous allons refaire le produit mais cette fois-ci il s'agit d'un produit matriciel qui ne commute pas ! On va faire l'opérateur de la première lignes $\times$ celui de la seconde $\times$ celui de la troisième. Ceci est équivalent à faire le produit de la première colonne $\times$ celui de la seconde $\times$ celui de la troisième. Pour la première colonne, nous avons

$$\sigma_y\sigma_x\sigma_y = -\sigma_y\sigma_y\sigma_x = -\sigma_y \tag{2.11}$$

car $\sigma_y^2 = \hat{1}$ (le *double flip*, c'est l'identité). En faisant de même pour les deux autres colonnes (ou chaque fois nous avons directement un σ_y^2)

$$RRR \quad \to \sigma_x \otimes \sigma_x \otimes \sigma_x \left|\Psi\right\rangle = -\left|\Psi\right\rangle \tag{2.12}$$

C'est le *miracle quantique*, le nombre de lumière allumée est **impair** ! Ceci colle aux observations. Le $\left|\Psi\right\rangle$ est un étant propre de ce quatrième produit d'observable, mais de valeur propre -1.

Solution au miracle quantique

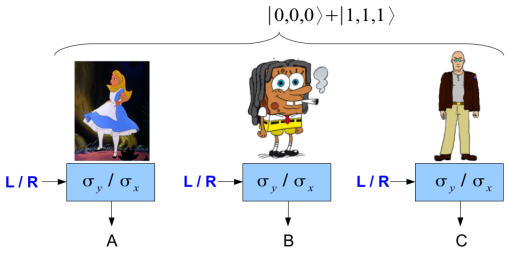

FIGURE 2.4

On peut prendre un des états GHZ préparé et on met un qbit dans chacune des boîtes. En fonction de ce qu'ils ouvrent, ils utilisent σ_x ou σ_y. Tout est réglé car les deux possibilités (L ou R) correspondent aux deux mesures. On dit que σ_x et σ_y sont **incompatibles** : on ne peut pas les définir ensemble car ils anticommutent. Si l'on a un spin 1/2, on ne peut pas lui associer un σ_x et un σ_y en même temps. On peut en connaître un, mais pas le second. En mécanique quantique, on ne peut pas donner une valeurs aux "deux ensembles". Alice a un qbit : on ne peut pas avoir à la fois précisément la valeur donnée par σ_y et celle par σ_x car cela violerait le principe d'incertitude.

2.2.3 Problème réel : distributed computing

Comment est-ce que ceci peut être utilisé dans un contexte informationnel ? Supposons que nous avons à nouveau trois parties A, B et C et que chacune d'elles reçoit une chaîne de bits

$$x = \underbrace{010110\ldots}_{n\ bits} \to A, \qquad y = \underbrace{111001\ldots}_{n\ bits} \to B, \qquad z = \underbrace{010000\ldots}_{n\ bits} \to C \tag{2.13}$$

Alice aimerait bien calculer l'addition modulo 2 suivante

$$f(x,y,z) = x_1y_1z_1 \oplus x_2y_2z_2 \oplus \cdots \oplus x_ny_nz_n \tag{2.14}$$

sachant que $x \oplus y \oplus z = (x_1 \oplus y_1 \oplus z_1, x_2 \oplus y_2 \oplus z_2, \ldots, x_n \oplus y_n \oplus z_n) = (1,1,\ldots,1)$. On veut calculer $f(x,y,z)$ en minimisant au maximum la communication, sinon B n'aura qu'a tout envoyer à A et ce serait fini.

C'est le *distributed computing problem* : comment calculer $f(x,y,z)$ qui a des entrées distribuées dans les trois parties en gardant la communication entre les parties la plus faible que possible ? Il existe des algorithmes classiques dont la complexité de cet algorithme est de $C = 3\text{bits}$ [2]

Comment faire mieux ?

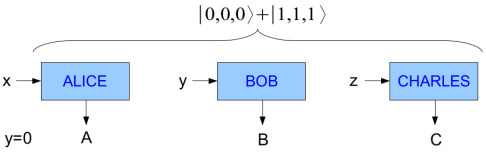

FIGURE 2.5

On prépare un état GHZ global pour A, B et C à qui on donne un chaîne de qbit, comme précédemment (resp. x, y et z). On regarde chacun des bits de la chaîne, un à un. Si la variable d'entrée est nulle ($x = 0, y = 0$ ou $z = 0$) cela correspond à l'action L (définie par σ_y). Sinon, c'est R (définie par σ_x).

Nous avons comme précédemment [3]

$$\begin{array}{lll} LLR & \to A \oplus B \oplus C & = 0 \\ RLL & \to A \oplus B \oplus C & = 0 \\ LRL & \to A \oplus B \oplus C & = 0 \\ RRR & \to A \oplus B \oplus C & = 1 \end{array} \tag{2.15}$$

Ce tableau nous donne les entrées et les sorties. Il peut être résumé [4]

$$A \oplus B \oplus C = x.y.z \tag{2.16}$$

Nous avons toujours

$$x \otimes y \otimes z = 1 \tag{2.17}$$

où il s'agit bien de l'addition modulo 2 [5]. Nous allons répéter cette procédure pour chacun des n bits d'Alice, Bob et Charles.

Protocole quantique

En envoie n bits chez A, B et C et ils produisent chacun une sortie de n bits

$$A = A_1A_2\ldots A_n, \qquad A = B_1B_2\ldots A_n, \qquad A = C_1C_2\ldots A_n \tag{2.18}$$

Ensuite, chacun d'entre-eux calculent la quantité suivante (chaque fois un bit)

$$a = \sum_{i=1}^{n} A_i, \qquad b = \sum_{i=1}^{n} B_i, \qquad c = \sum_{i=1}^{n} C_i \tag{2.19}$$

Bob envoie ensuite b à Alice et Charles envoie c à Alice également qui calcule la quantité suivante

$$a + b + c = \sum_{i=1}^{n}(A_i + B_i + C_i) = \sum_{i=1}^{n} x_iy_iz_i = f(x,y,z) \tag{2.20}$$

La complexité quantique n'est ainsi que de $C = 2$ bits !

2. Par exemple, C envoie 1 bit à A qui en envoie 2 à B.
3. Comment ?! Pourquoi des addition maintenant ?! Quel est l'avantage d'être quantique alors ?
4. Par exemple, pour LLR on a $x = 0, y = 0$ et $z = 1$, soit $0 * 0 * 1 = 0$.
5. $(1 + 1 + 1)\%2 = 1$

Qu'avons-nous appris ?

Si Alice, Bob et Charles partagent n état (GHZ) intriqués, ils peuvent **économiser un bits de communication** pour calculer $f(x, y, z)$. C'est **remarquable** car l'intrication ne peut pas être utilisée pour violer le principe de causalité (soit communiquer plus vite que la célérité) : on ne peut pas toucher à un qbit et avoir instantanément l'autre qui réagit.

2.3 Téléportation quantique

Le fait qu'Alice et Bob aient deux photons intriquée les autorisé à "téléporter" l'état d'une particule (un qbit).

2.3.1 Intrication de deux qbits (Etat de Bell)

Il existe quatre états particulièrement intéressants pour le traitement de deux qbits : les états de Bell. Ils sont maximalement intriqués, orthogonaux et normalisés.

À retenir*:* États de Bell

$$\left|\Phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right), \qquad \left|\Psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right) \tag{2.21}$$

Rappelons l'opération *SIGN FLIP* σ_z et l'opération *BIT FLIP* σ_x

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.22}$$

Qui ensemble donnent σ_y, à une constante près

$$\sigma_x\sigma_z = -i\sigma_y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{2.23}$$

L'application de $\sigma_x\sigma_z$ permet d'inverser le bit ainsi que son signe

$$\begin{cases} \sigma_x\sigma_z\,|0\rangle &= |1\rangle \\ \sigma_x\sigma_z\,|1\rangle &= -\,|0\rangle \end{cases} \tag{2.24}$$

Voyons l'application de nos opérateurs sur les états de Bell. Le premier $I\times$ signifie "ne rien faire" sur le premier qbit

À retenir*:*

$$\begin{aligned} (I\times I) \quad \left|\Phi^+\right\rangle &= \left|\Phi^+\right\rangle \quad \text{(Alice rien, Bob rien)} \\ (I\times \sigma_z) \quad \left|\Phi^+\right\rangle &= \left|\Phi^-\right\rangle \quad \text{(Alice rien, Bob SIGN-FLIP)} \\ (I\times \sigma_x) \quad \left|\Phi^+\right\rangle &= \left|\Psi^+\right\rangle \quad \text{(Alice rien, Bob BITFLIP)} \\ (I\times \sigma_x\sigma_z) \quad \left|\Phi^+\right\rangle &= \left|\Psi^-\right\rangle \quad \text{(Alice rien, Bob BOTH)} \end{aligned} \tag{2.25}$$

On comprends ainsi l'intérêt de ces états quand on voit la faciliter du passage de l'un à l'autre, à l'aide des matrices de Pauli.

Alice n'a ici jamais rien fait, mais bien Bob. Leurs qbit peuvent être séparés loin l'un de l'autre et Alice ne sait pas ce que Bob fait, mais le résultat final est quatre états orthogonaux qui peuvent former une base. Ceci semble violer la causalité.

Heureusement, ce n'est pas le cas. Explicitons

$$\Phi^{\pm} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & \pm 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \pm 1 & 0 & 0 & 1 \end{pmatrix}, \qquad \Psi^{\pm} = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & \pm & 0 \\ 0 & \pm 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{2.26}$$

Le calcul des traces (partielles ? Revoir) montre que

$$\mathrm{Tr}_1 \Phi^{\pm} = \mathrm{Tr}_1 \Psi^{\pm} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \mathrm{Tr}_2 \Phi^{\pm} = \mathrm{Tr}_2 \Psi^{\pm} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{2.27}$$

Ceci montre que peu importe ce que fait Bob (c'est-à-dire l'application d'une matrice de Pauli), l'état d'Alice reste le même. Alice ne voit donc pas de différence et heureusement car sinon, la causalité serait violée.

Ces états permettent surtout la création d'un protocole particulièrement intéressant. En effet, comme nous allons le voir, quatre opérations possibles (2 bits) peuvent être virtuellement encodées dans un seul qbit.

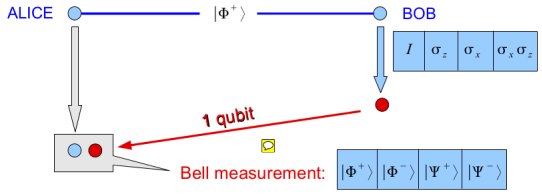

Figure 2.6

Supposons qu'Alice et Bob se partagent un état $|\Phi^+\rangle$, mais ils ne peuvent communiquer avec lui. Bob applique une des quatre opérations possible $(I, \sigma_z, \sigma_x, \sigma_x\sigma_z)$. Ce qui l'intéresse c'est transmettre deux bits (soit quatre possibilités).

Le qbit d'Alice ne change pas, elle ne peut pas savoir ce qui se passe du côté de Bob, mais Bob envoie son qbit à Alice. Une fois qu'Alice le reçoit, elle est en possession de deux qbits et peut faire une **mesure de Bell**[6]. Alice sait ce qu'elle a, partage un état intriqué avec Bob et la mesure de Bell lui donne un des quatre états de Bell possibles

$$|\Phi^+\rangle, \qquad |\Phi^-\rangle, \qquad |\Psi^+\rangle, \qquad |\Psi^-\rangle \tag{2.28}$$

Elle est donc en mesure de savoir ce qu'a appliqué Bob sur l'état de Bell partagé. L'information de ce qu'a appliqué Bob tenant dans deux bits, nous avons bien transféré deux bits à l'aide d'un seul qbit à l'aide de l'intrication. On ne peut donc pas transmettre d'information via cet état, mais on peut l'utiliser pour faire du codage dense. La causalité n'a ici pas été violée car Bob a du envoyer son qbit à Alice via un système physique, causal[7].

2.3.2 Téléportation quantique

Alice reçoit un qbit $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ et partage un état de Bell $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ avec Bob.

Figure 2.7

6. Mesure qui nous dit dans lequel des quatre états de Bell on se trouve.
7. Voir slide 44 (cours1) sur les EPR. Je n'ai pas de notes dessus.

Faisons le produit des deux états d'Alice (à gauche le qbit que l'on souhaite téléporter, à droite l'intriqué)

$$\begin{aligned} |\Psi\rangle \left|\Phi^+\right\rangle &= \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right) \left(\alpha |0\rangle + \beta |1\rangle\right) \\ &= \frac{1}{\sqrt{2}} \left(\alpha \underbrace{|00\rangle}_{\frac{\Phi^+ + \Phi^-}{\sqrt{2}}} |0\rangle + \alpha \underbrace{|01\rangle}_{\frac{\Psi^+ + \Psi^-}{\sqrt{2}}} |1\rangle + \beta \underbrace{|10\rangle}_{\frac{\Psi^+ - \Psi^-}{\sqrt{2}}} |0\rangle + \beta \underbrace{|11\rangle}_{\frac{\Phi^+ - \Phi^-}{\sqrt{2}}} |1\rangle \right) \end{aligned} \tag{2.29}$$

Il est important de remarquer ici que le premier produit correspond à

$$\frac{\alpha}{\sqrt{2}} |00\rangle_{AC} |0\rangle_B \tag{2.30}$$

où C désigne le qbit à téléporter. Les qbits $|..\rangle$ correspondent à AC (les deux qubits de A) tandis que les $|.\rangle$ correspondent aux qubit que B à en sa possession ! On peut regrouper les termes en Φ^+ ce qui fait apparaître $|\Psi\rangle = (\alpha |0\rangle_B + \beta |1\rangle_B)$, l'état à téléporter. En faisant de même pour les autres états de Bell

$$|\Psi\rangle \left|\Phi^+\right\rangle = \frac{1}{2} \left(\left|\Phi^+\right\rangle \underbrace{(\alpha |0\rangle + \beta |1\rangle)}_{|\Psi\rangle} + \left|\Phi^-\right\rangle \underbrace{(\alpha |0\rangle - \beta |1\rangle)}_{\sigma_z|\Psi\rangle} \right) + \frac{1}{2} \left(\left|\Psi^+\right\rangle \underbrace{(\alpha |1\rangle + \beta |0\rangle)}_{\sigma_x|\Psi\rangle} + \left|\Psi^-\right\rangle \underbrace{(\alpha |1\rangle - \beta |0\rangle)}_{\sigma_x\sigma_z|\Psi\rangle} \right) \tag{2.31}$$

Nous voyons apparaître dans l'ordre le qbit à téléporter, le qbit à téléporter avec un *SIGN-FLIP*, toujours le même avec un *BIT-FLIP* et enfin la combinaison des deux. Nous avons ici juste ré-écrit l'état original. Réécrivons-le

$$|\Psi\rangle \left|\Phi^+\right\rangle = \frac{1}{2} \left(\left|\Phi^+\right\rangle |\Psi\rangle + \left|\Phi^-\right\rangle \sigma_z |\Psi\rangle + \left|\Psi^+\right\rangle \sigma_x |\Psi\rangle + \left|\Phi^-\right\rangle \sigma_x\sigma_z |\Psi\rangle \right) \tag{2.32}$$

Alice va faire une **mesure de Bell** sur les **deux** qbits qu'elle possède (celui à téléporter et l'intriqué) : c'est la que va véritablement se faire la téléportation. En effet, en effectuant la mesure, le résultat d'Alice est que l'état à trois particules va se réduire à l'un des quatre états suivant (probabilité identique)

$$\left|\Phi^+\right\rangle |\Psi\rangle , \qquad \left|\Phi^-\right\rangle \sigma_z |\Psi\rangle , \qquad \left|\Psi^+\right\rangle \sigma_x |\Psi\rangle , \qquad \left|\Phi^-\right\rangle \sigma_x\sigma_z |\Psi\rangle \tag{2.33}$$

Les qbits d'Alice sont maintenant intriqués dans l'un des quatre états de Bell [8] et l'intrication initialement partagée par Alice et Bob est cassée : le qbit de Bob est dans un des états (2.33). [9] Le qbit de Bob ressemble maintenant à celui qui doit être téléporté, mais il n'est le même que dans 1/4 des cas.

Lorsque Alice a effectué la mesure de Bell sur ses qbits, elle a mesuré l'état de Bell dans lequel elle se trouve. Par exemple, si Alice a mesuré $\left|\Psi^+\right\rangle$, elle sait que l'on a appliqué σ_x sur $|\Psi\rangle$. Il y a quatre mesures possibles, qui correspondent à quatre opérations distinctes faite sur $|\Psi\rangle$

$$I, \qquad \sigma_z, \qquad \sigma_x, \qquad \sigma_x\sigma_z \tag{2.34}$$

8. Lorsque l'on fait une mesure de Bell sur des états qui n'étaient pas de Bell avant, ils sont projeter sur un état de Bell et ils deviennent intriqués.

9. Ca ne viole pas la causalité ? C'est bien le principe de réduction de la fonction d'onde ? Un peu étrange. En fait, non : les qbits de Psi dans 2.31 sont ceux de Bob ! Voir page eng Wiki ou c'est explicité (ou ce que j'ai rajouté). C'est juste que les psi et psi modifié par les matrices sont le qbit de bob : on se réduit à une des fonctions et pour retrouver le bit (bob a un bit modifié) il doit appliquer la transfo que lui dit alice

Ces opérations se codent en deux bits. Alice va envoyer ces deux bits à Bob ce qui permettra de savoir à Bob "ce qu'il a entre les mains" et de retrouver exactement $|\Psi\rangle$ (et pas quelque chose qui "lui ressemble", comme dans 3/4 des cas). Quelques exemples :

- Si Alice dit '00', Bob est en $|\Psi\rangle$: il doit appliquer I, soit ne rien faire.
- Si Alice mesure $|\Phi^-\rangle$, elle envoie '01' ce qui correspond aux second terme. Bob sait que l'état téléporté (qu'il "a entre les mains) à eu un *SIGN-FLIP* : il en réapplique un autre pour retrouver l'état à téléporter.

Alice envoie donc deux bits, Bob applique une transformation et grâce à ça il le "re-matérialise" sur une autre particule.

Remarques :

— Ca ne viole pas le principe du non-clonage car le qbit d'Alice est détruit
— Le qbit de Bob ne contient pas d'information (pas causalement lié à celui d'Alice)
— Les bits transmis classiquement ne cotiennent pas d'information (sinon le qubit serait perturbé)

La section "Performing a Bell measurement using a BS" a été passée. Il reste la démonstration expérimentale au slide 53, mais comme c'est l'article que j'ai choisi je ne détaille pas ici.

Chapitre 3

Quantum no-cloning theorem and cryptography

3.1 Quantum no-cloning theorem

3.1.1 Indistinguabilité des états non-orthogonaux

À retenir*:* Les états quantiques non-orthogonaux ne sont pas parfaitement distinguables.

En effets, des bits classiques sont, *en principe*, complètement distinguables

$$\langle 0|1\rangle = (0\ 1)\begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0 \tag{3.1}$$

Mais pour les qubits

$$\langle \phi|\psi\rangle \equiv (\gamma^*\ \delta^*)\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha\gamma^* + \beta\gamma^* \neq 0 \tag{3.2}$$

où $|\psi\rangle \equiv \alpha\,|0\rangle + \beta\,|1\rangle$ et $|\phi\rangle \equiv \gamma\,|0\rangle + \delta\,|1\rangle$. Dès lors, lorsqu'ils ne sont **pas** orthogonaux, ils sont *intrinsèquement indistinguables*. Ceci a plusieurs applications : codages quantiques, "quantum money", principe de non-clonage quantique, ...

Quantum coding (compression of quantum info)

Soit une source qui émets une séquence de qubits identiquement distribué (probabilité 1/2)

$$\begin{cases} |\psi\rangle & p = 1/2 \quad |\psi\rangle = |0\rangle \\ |\phi\rangle & p = 1/2 \quad |\phi\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \end{cases} \tag{3.3}$$

FIGURE 3.1

Il s'agit d'un mélange d'états **non-orthogonaux** et donc indistinguables (produit scalaire entre les deux de $1/\sqrt{2}$). Il n'est pas possible de compresser une séquence de bits identiquement distribué, mais avec les qubits c'est possible. En effet, $|\psi\rangle = |0\rangle$ mais $|\phi\rangle$ est une combinaison linéaire de $|1\rangle$ et $|2\rangle$: c'est une superposition quantique qui n'a pas d'équivalent classique.

Calculons l'opérateur densité moyen. Il est nécessaire de la diagonaliser pour appliquer l'entropie de VON NEUMANN (qui est l'entropie de SHANNON des valeurs propres)

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} 3/4 & 1/4 \\ 1/7 & 1/4 \end{pmatrix} \quad \Rightarrow \quad \begin{pmatrix} 0.85 & 0 \\ 0 & 0.85 \end{pmatrix} \tag{3.4}$$

L'entropie de VON NEUMANN vaut alors

$$S(\rho) = -\mathrm{Tr}[\rho \log(\rho)] = 0.6 < 1 \text{ bit} \tag{3.5}$$

Celle-ci est inférieur à 1 bit, on peut donc faire une compression même avec $p = 1/2$. C'est la **redondance quantique**. Classiquement, ce n'est pas compressible mais le fait qu'ils soient indistinguables et que c'est un mélange, cela donne la possibilité de faire mieux. C'est le mélange qui a introduit la redondance.

Théorème de non-clonage quantique

On aimerait avoir

$$\begin{cases} |\psi\rangle & = \alpha\,|0\rangle + \beta\,|1\rangle \\ |0\rangle & \end{cases} \quad \Rightarrow \quad \begin{cases} |\psi\rangle & = \alpha\,|0\rangle + \beta\,|1\rangle \\ |\psi\rangle & = \alpha\,|0\rangle + \beta\,|1\rangle \end{cases} \tag{3.6}$$

où $|0\rangle$ est l'état sur lequel on veut faire la copie ("page blanche"). On peut montrer que ceci est **interdit par la physique**. C'est une conséquence du fait que deux états non-orthogonaux ne sont pas distinguables.

Quantum money

Si on attribue un numéro de série qui est une séquence de spin 1/2 provenant d'atomes isolés dans des états non-orthogonaux, on ne serait pas habilité à lire ni cloner le billet.

Cryptographie quantique (QKD)

Il s'agit d'un des protocoles les plus connu (distribution de clef). Il y a deux parties autorisées (A, B) et un espion E. Grâce au théorème de non-clonage quantique, on peut assurer la sécurité de la ligne malgré qu'elle soit "écoutée". Ce genre de dispositif est déjà commercialisé (pour les communications par fibre optique sur 50 km).

3.1.2 Optical qubits

On reprends l'interféromètre du premier chapitre. Lire *slides 8-15*, brièvement résumé ici.

- *Interféromètre à un photon, $\theta = 0$.* Si pas de lame de phase, c'est toujours le même détecteur qui va cliquer. L'état du photon est dans une superposition des deux chemins.
- *Interféromètre à un photon, $\theta = \pi$.* Si l'on place une lame de phase de π on a toujours que un seul clic, mais dans l'autre détecteur.
- *Interféromètre à un photon, $\theta = \pi/2$.* Si l'on place une lame de phase de $\pi/2$. Classiquement, cela correspond à une intensité 50/50 sur chaque détecteur. En quantique, on aura maximum un clic : "*quantum randomness*". Il va y avoir un clic sur le premier ou le deuxième détecteur, avec une probabilité de 50% : c'est bien aléatoire. Ce n'est pas un manque de connaissance, mais du à la nature même de la mécanique quantique.

Il est donc **impossible de déterminer la lame de phase** insérée à partir de la connaissance du détecteur qui a cliquer. L'espion sera dans cette situation : il voit quelque chose, mais ne sait pas la situation dans laquelle on se trouve.

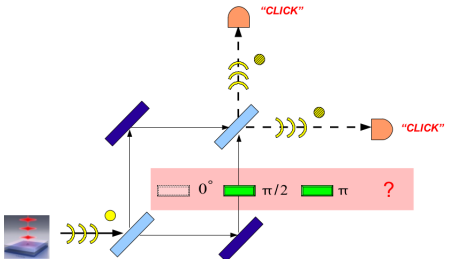

FIGURE 3.2

On peut ré-écrire les précédentes équations (chapitre 1), mais en présence d'une lame de phase. La superposition entre les deux BS s'écrit cette fois-ci

$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right) \tag{3.7}$$

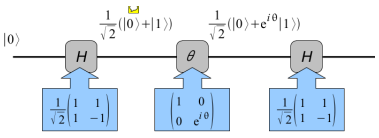

FIGURE 3.3

Avec les portes d'HADAMARD, ré-écrivons notre circuit

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{3.8}$$

Appliquons la porte "quantum phase"

$$\Phi\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right] = \begin{pmatrix}1 & 0\\ 0 & e^{i\theta}\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\e^{i\theta}\end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle) \tag{3.9}$$

En appliquant une nouvelle fois HADAMARD, on trouve finalement l'état de sortie

$$\frac{1+e^{i\theta}}{2}|0\rangle + \frac{1-i\theta}{2}|1\rangle \tag{3.10}$$

La probabilité de mesurer $|0\rangle$ est donnée par $\left|\frac{1+e^{i\theta}}{2}\right|^2 = \cos^2\frac{\theta}{2}$ et la probabilité de mesurer $|1\rangle$ est de $\sin^2\frac{\theta}{2}$.

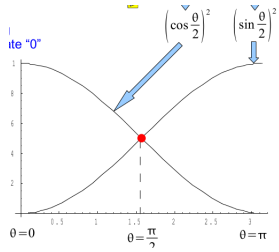

FIGURE 3.4

Mais qu'est ce que ceci vient faire pour le théorème de non-clonage quantique ? Il va nous montrer pourquoi le clonage est interdit. L'origine de ce principe est la linéarité de la mécanique quantique. Donnons nous deux bases

Computational basis $\{|0\rangle, |1\rangle\}$ (convention)

Dual basis $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$

Supposons que les états $\{|0\rangle, |1\rangle\}$ puissent être clonés

$$\begin{aligned}|0\rangle &\to |0\rangle|0\rangle\\ |1\rangle &\to |1\rangle|1\rangle\end{aligned} \tag{3.11}$$

Si c'est le cas, les états $\{|+\rangle, |-\rangle\}$ ne peuvent pas l'être

$$|0\rangle + |1\rangle \to |0\rangle|0\rangle + |1\rangle|1\rangle \neq (|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \tag{3.12}$$

La première égalité est un état intriqué (état de BELL, $|P\rangle\, hi^+$), ce n'est pas ce qu'on voulait car nous voulions le produit (seconde (non-)égalité). **Donc**

$$|\pm\rangle \nrightarrow |\pm\rangle|\pm\rangle \tag{3.13}$$

Si on peut cloner l'un, on ne peut pas cloner l'autre. Le choix de la base étant arbitraire, on comprend l'origine du théorème.

Exemple : qubit optique

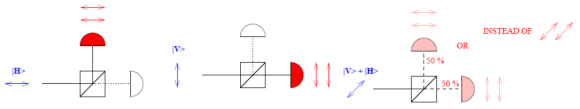

FIGURE 3.5

On a deux photons identiques dans la même polarisation. Si l'on vient avec $|V\rangle$, les deux photons vont sortir du même côté et inversement avec $|H\rangle$. Si par contre on vient avec $|V\rangle + |H\rangle$, on n'aura pas deux fois $|V\rangle + |H\rangle$ en sortie mais l'un des résultats précédents avec une probabilité de 50%.

On pourrait croire que l'amplification optique par émission stimulée viole le théorème. Mais l'émission stimulée s'accompagne toujours d'émission spontanée : les polarisation ne seront dès lors pas indépendantes et le théorème ne sera pas violé.

Causalité

On peut montrer que si le clonage était possible, la causalité serait violée. Créons un état de BELL $|\Psi^-\rangle$. On envoie un des qbits de cet état à gauche, l'autre à droite. A gauche, on va le mesurer dans la base de référence ou dans la base duale. Je peux ainsi calculer les deux opérateurs densité : l'un dans la base de référence ρ et l'autre dans la base duale ρ'. Le problème c'est que $\rho \neq \rho'$ est **distinguable**. En effet, en mesurant l'original et le clone, on sait que c'est plus probable d'avoir ρ ou ρ'. En effectuant la mesure, on a un état cloné. Si on peut dire lequel, on peut transmettre instantanément l'information ce qui viole la causalité.

On peut montrer que le "meilleur" clonage possible correspond à une fidélité de 5/6 : on peut presque bien cloner, mais pas parfaitement.

3.2 Quantum cryptography

Avec des bits classiques, Eve peut écouter ce qui se passe sur la ligne entre A et B. Comment être sur de la confidentialité ? C'est très simple, on utilise une clef secrète. Alice a le message, elle y ajoute une clef pour donner un *cipher* puis envoie ce dernier à Bob. Si Bob à la clef, il peut retrouver le message. C'est parfait, mais une clef ne peut pas être utilisée deux fois sinon on perd la sécurité. Il existe d'autres techniques, comme avec la clef publique E pour l'encodage et une clef privée D pour le décodage. C'est difficile de décoler l'information car déduire D et E nécessite une factorisation ce qui est un "calcul difficile". Le problème c'est que un ordinateur quantique sait faire ça efficacement (temps polynomial), ce qui rendrait le protocole non sécurisé.

Il existe une solution quantique, le protocole BB84. Dans ce protocole, l'encodage est classique mais la distribution de la clef est quantique. On peut prouver que c'est sécurisé si

- La clef secrète est générée totalement aléatoirement. Si pseudo-aléatoire ça devient prédictible et c'est foutu.
- La clef secrète doit être aussi longue que le message.
- La même clef secrète ne peut pas être utilisée pour différents messages.

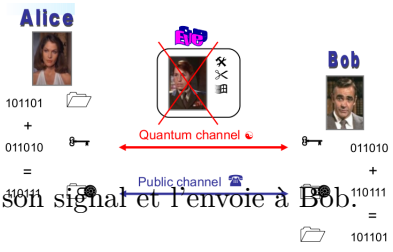

FIGURE 3.6

Ce qui est intéressant c'est que la **clef secrète** est **inconnue de Eve** : c'est garanti par la mécanique quantique ! Si Eve essaye d'espionner, cela va causer des erreurs de transmission ! S'il n'y a pas d'erreur, c'est que personne n'a essayé d'espionner. Avec la base de codage, Alice code son signal et l'envoie à Bob.

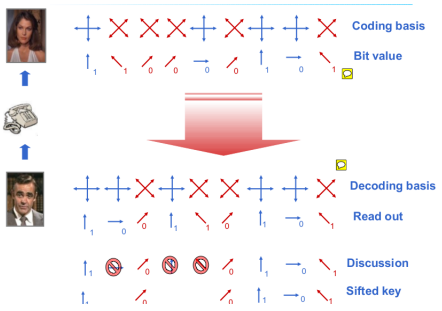

FIGURE 3.7

Le protocole BB84 nécessite l'utilisation de deux bases conjuguées. Alice a à sa disposition la base de codage, composée de quatre états non-orthogonaux. Supposons pour le moment que la ligne est parfaite, personne n'écoute.

Bob reçoit le bit codé. Il va prendre une base **aléatoire** pour décoder le signal, puis il va essayer de distinguer horizontal, vertical, diagonal ou anti-diagonal. Évidemment, en faisant ça, beaucoup sont faux. Vient ensuite une étape de discussion ou Alice et Bob vont parler des bases utilisées et voir directement ce qui est faux. On obtient alors une **shifted key** : elle est plus petite que la clef, mais elle est parfaite. Regardons maintenant s'il y a un espion.

Cette fois-ci, Eve est entre les deux. Elle va essayer de faire comme Bob et choisir une base au hasard. Elle va décoder avec et envoyer le résultat à Bob en espérant que ce soit exact. Bob choisi une base au hasard et essaye de décoder. Dans la première colonne, l'action de Eve est invisible car elle a choisie la bonne base et Bob aussi. Dans la deuxième, c'est trouvé par Eve mais Bob a aussi choisi la mauvaise base. Vient ensuite la troisième colonne : Alice à envoyé un 0, Eve utilise la mauvaise base (H/V) et envoie un H à Bob. Bob utilise la bonne base, mais E l'a modifié : cela cause une erreur, entourée en vert. Ainsi, dans les six bits de la shifted key, deux sont faux.

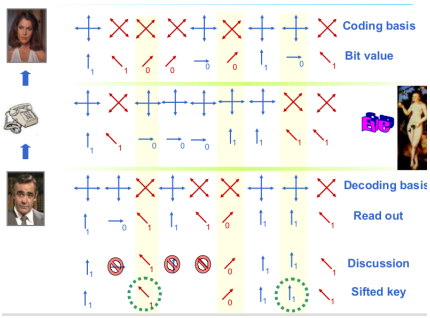

FIGURE 3.8

Nous allons voir que l'interception d'Eve est limitée par la physique quantique. En effet, Eve doit faire une mesure sans savoir la base utilisée par Alice. Elle doit intercepter/renvoyer avec la base + ou ×, garder une copie de son coté, faire des mesures qui ne démolissent pas l'état quantique, . . .Toutes ces opérations vont causer des erreurs de transmission : plus Eve en sait, plus il y a d'erreurs.

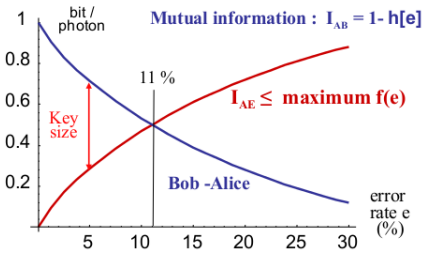

FIGURE 3.9

Analysons la pire situation, soit celle ou Eve applique la meilleur stratégie autorisée par la mécanique quantique (courbe rouge). Il y a une intersection avec le taux d'erreur autour de 11% : tant que l'on est en dessous d'un taux d'erreur de 11%, Bob en sait plus que Eve, il a un avantage. En pratique, il existe un algorithme qui permet d'extraire une clef basé sur la différence entre le taux d'erreur ce ce que sait Eve tant que l'on a un avantage. Dès lors, tant que le rouge est en dessous de 11%, on peut extraire une clef totalement secrète garantie par la mécanique quantique.

Procédure réelle

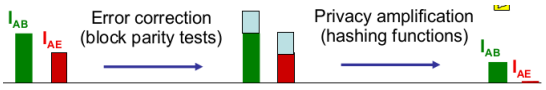

FIGURE 3.10

Après l'échange initial entre Alice et Bob, ils mesurent le taux d'erreur en comparant publiquement une petite partie de la clé brute. Ceci permet d'évaluer le montant de l'information que Eve a (possiblement) à disposition. Ensuite (et seulement si Bob en sait plus que Eve, soit si $QBER < 0.11$) on applique une correction d'erreur et une amplification privée : A et B extraient la clef disponible en corrigeant les erreurs et en annulant quasiment toute l'information que E avait. Un premier setup mettant ça en application a été proposé par *ID Quantique*.

3.2.1 Implémentation optique (codage en phase)

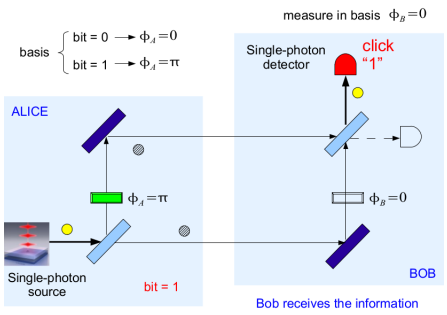

FIGURE 3.11

On cherche a déterminer l'état d'un photon. Pour y arriver, on va tout faire avec un McZehnder pour le codage de l'information en phase. On se place dans la base

$$\begin{cases} \text{bit} = 0 & \to \Phi_A = 0 \\ \text{bit} = 1 & \to \Phi_A = \pi \end{cases} \tag{3.14}$$

Alice va utiliser une phase de 0 ou π si elle désire un 0 ou 1. Alice veut envoyer un zéro et choisi alors $\Phi_A = 0$. Si Bob mesure dans la base $\Phi_B = 0$, il va avoir un clic '0' (il ne met pas de phase de son côté). Si Alice veut transmettre 1, elle va utiliser $\Phi_A = \pi$. Si Bob mesure dans la base $\Phi_B = 0$ il aura un clic '1'. Dans les deux cas précédent, Bob reçoit l'information.

Si maintenant Alice envoie '0' ($\Phi_A = 0$) et que Bob choisi de mesurer dans l'autre base $\Phi_B = \pi/2$, il a 50% de chance de clic '0' ou clic '1'. Le résultat est identique si Alice envoie '1' ($\Phi_A = \pi$). Dans les deux cas, Bob observe un bit aléatoire et n'a aucune information : c'est parce qu'il a choisi la mauvaise base.

Troisième situation, Alice utilise maintenant la base

$$\begin{cases} \text{bit} = 0 & \to \Phi_A = \pi/2 \\ \text{bit} = 1 & \to \Phi_A = 3\pi/2 \end{cases} \tag{3.15}$$

Si Alice envoie '0' ou '1' et que Bob utilise la base $\Phi_B = \pi/2$, il reçoit l'information dans les deux cas car il est dans la bonne base. Si par contre Bob chance de base $\Phi_B = 0$, il a de nouveau un bit aléatoire peu importe ce qu'envoie Alice. Il n'a pas d'information : il a choisi la mauvaise base.

Ceci nous montre comment implémenter le "choix de base" présenté précédemment. Mais ce protocole n'est pas pratique, car il nécessite l'existence d'un interféromètre qui peut être long d'une centaine de kilomètres. Comment éviter l'interféromètre ?

3.2.2 Implémentation optique (multiplexage temporel)

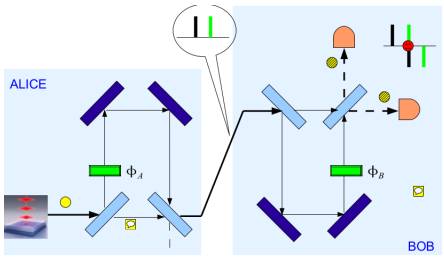

FIGURE 3.12

Pour l'éviter, on va multiplexer : on a maintenant à disposition deux petits interféromètres. Le chemin peut être plus petit en fonction du bras emprunté et il en résulte un délai temporel. Le trait vert supérieur correspond à celui qui passe dans Φ_A tandis que le trait vers inférieur celui que passe dans Φ_B. Ils arrivent en retard, alors que le trait noir correspond au chemin "court" (arrive avant).

3.2.3 Implémentation optique (codage en phase)

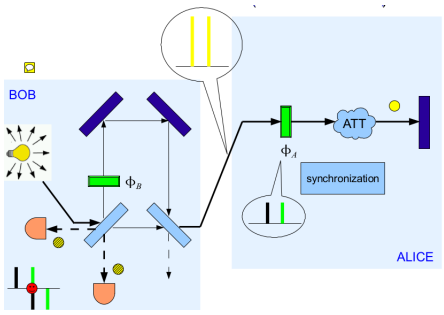

FIGURE 3.13

Il est possible de faire mieux et n'avoir qu'un seul interféromètre. Bob envoie une impulsion lumineuse, pas du tout quantique, qui se propage dans l'interféromètre. Il en ressort deux impulsions : une en avance et une en retard (les deux jaunes). On les atténue (ATT) pour n'avoir qu'un seul photon et on les renvoie du côté de Bob. Avant de les renvoyer, on va imposer une phase différente aux deux photons (par synchronisation via l'électronique rapide). Par exemple, pas de phase sur un photon (photon noir) et une phase sur l'autre (photon vert) : on reconstruit ainsi les deux photons du premier interféromètre du cas précédent. Une fois chez Alice, tout se passe comme au précédent montage. Tout est identique, mais avec un interféromètre de moins. Voir *slide 50* pour l'implémentation réelle (et commentaires).