Introduction au Calcul Quantique

1. La physique du qubit

Edouard Marchais[a]

[a] *EPITA, 14-16 Rue Voltaire, 94270 Le Kremlin-Bicêtre, France.*

E-mail: edouard.marchais@epita.fr

Abstract: Dans ce document un premier exemple de support physique pour transporter l'information par un système quantique, le photon, est donné. On montre que la polarisation de cette particule quantique est instrumentale afin d'encoder sans ambiguïté les valeurs binaires habituelles. Une première application de cet encodage quantique de l'information est également discutée dans le domaine de la cryptographie.

Table des Matières

1 Généralités

Introduction L'*informatique quantique* correspond à l'utilisation des lois et propriétés particulières de la **mécanique quantique** afin d'encoder et de transporter l'information. La *mécanique (ou physique) quantique* quant à elle correspond à une *théorie physique* cherchant à décrire un système dont la taille est typiquement de celle d'un atome ($\simeq 10^{-10}\mathsf{m}$) ou moindre.

1.1 Nécessité de l'approche quantique

Insuffisance de la description classique Pour des systèmes physiques à l'échelle *atomique ou microscopique* une approche classique, comme la mécanique newtonienne, décrit de manière incorrecte les phénomènes physiques mesurables par l'expérience. Un exemple simple est l'incapacité, pour la mécanique (newtonienne) classique, à décrire le mouvement de l'électron autour du noyau de l'atome d'hydrogène (formé d'un proton et d'un neutron).

Cette constatation a conduit à l'élaboration, au début du $\mathsf{XX}^{\text{ème}}$ siècle, d'une théorie quantique permettant donc de décrire les phénomènes physique à une échelle atomique et en deçà. Cette approche quantique repose sur un certain nombre de *postulats* et sur un *formalisme mathématique* distinct de celui de la mécanique classique.

Relation entre physique quantique et physique classique Malgré la distinction entre les domaines d'application de la *physique quantique* ($\lesssim 10^{-10}\mathsf{m}$) et la physique classique ($\gtrsim 10^{-10}\mathsf{m}$), tout système physique est ultimement un **object quantique**. En effet, une pomme, un tournevis, la terre, l'univers sont des objects macroscopiques qui, bien que décrit (dans une certaine approximation) par des lois classiques, sont constitués d'atomes et de molécules qui sont des objects microscopiques dont le comportement est décrit par la *mécanique quantique*.

Cette remarque est très importante puisque elle conduit à exiger de la mécanique quantique que celle-ci, malgré le *formalisme mathématique* qu'elle requiert, doit permettre de retrouver les lois classiques de la physique des objects *macroscopiques*. Cette limite classique de la mécanique quantique est usuellement retrouvée lorsque l'on considère que le système physique est formé d'un très grand nombre d'atomes (ou de particules de taille inférieure) et non plus que de quelques particules.

1.2 Exemples simples

Conduction électrique et transistors Pour illustrer notre propos, considérons l'exemple de la conduction électrique dans un matériau *conducteur* (servant à la fabrication de composant électronique par exemple). Les propriétés de conduction du courant électrique pour un tel matériau sont directement liées à la facilité avec laquelle les électrons se *propagent* dans le milieu cristallin qui forme le matériau. Bien que le comportement des électrons soit décrit correctement par la mécanique quantique, c'est le *comportement collectif* que l'on détecte à notre échelle sous la forme d'une intensité.

Un autre exemple intéressant est celui des transistors formant les circuits imprimés des ordinateurs actuels. C'est grâce à une compréhension précise du *comportement quantique* des électrons dans ces transistors que Bardeen, Brattain et Shockley ont pu mettre au point les premiers modèles en 1947. On voit que, bien qu'il ne soit pas quantique, votre ordinateur fonctionne suivant les *principes de la mécanique quantique*!

Bit classique Physiquement les valeurs binaires classiques 0 et 1 correspondent respectivement à un condensateur chargé et déchargé. Cette charge macroscopique correspond au niveau microscopique au déplacement de 10^4 à 10^5 électrons. C'est donc bien un comportement collectif d'objects microscopiques « quantiques » (les électrons) qui est à l'origine d'un effet macroscopique « classique » (0 ou 1).

1.3 Avancées techniques et miniaturisation

Progrès expérimentaux Depuis les années 1980, les physiciens ont développées des techniques afin de **manipuler** et d'**observer** des objects quantiques, ainsi que leur propriétés quantiques, tels que des atomes, des ions, des photons, etc... Cela a permis de construire physiquement des « bits » élémentaires d'information quantique, c'est-à-dire des « **Qubits** » (*quantum bits*). Il est intéressant de noter qu'aucun concept nouveau n'a été nécéssaire à cela et que, d'un certain point de vue, tout était prévu depuis 1930...

Grâçe aux techniques expérimentales il est donc devenu possible de changer les *propriétés quantiques individuelles* d'une particules telles que son énergie, sa polarisation, son « spin », etc... Ce sont ces propriétés physiques particulières qui vont servir à encoder notre information au niveau quantique, remplaçant les condensateurs chargé et déchargé utilisé auparavant.

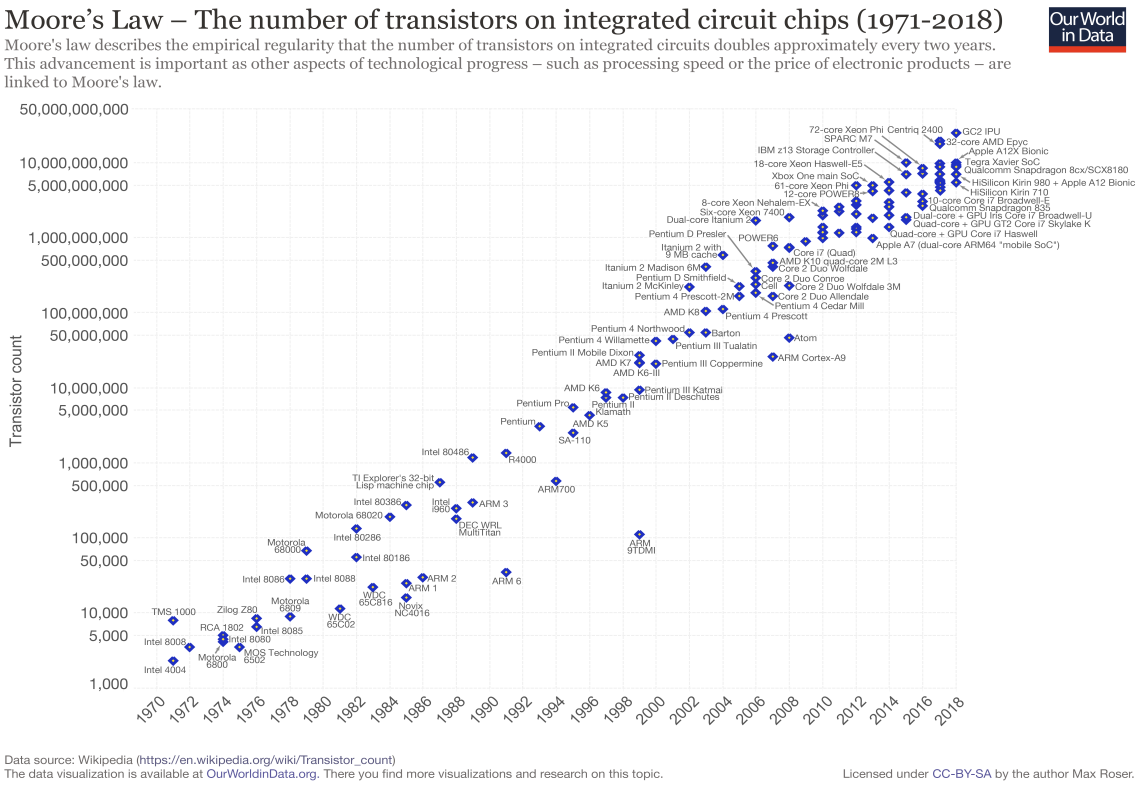

Figure 1: Évolution du nombre de transistors sur circuit

Loi de Moore Une autre raison, plus pragmatique, permet de s'attendre à l'émergence de l'informatique quantique. De fait la miniaturisation croissante de l'électronique va trouver ses limites physiques à cause effets quantiques. En effet la **Loi de Moore** postule que le nombre de transistors gravé sur une puce double tout les 18 mois (environ), voir **Figure 1**. Cette loi empirique indique que les dimensions caractéristiques d'une puce seront inférieures à 10 nm après 2020... À cette échelle les **propriétés quantiques** des atomes et des électrons vont devenir importantes.

1.4 Avantages et inconvénients du calcul quantique

Superposition Bien que l'avènement de l'informatique quantique semble inéluctable, il existe également un avantage fondamental de l'encodage **quantique** de l'information par rapport à sa

version **classique**. En effet, classiquement, un bit d'information peut (seulement) prendre les valeurs théoriques 0 ou 1. Cela pose des contraintes et des limites inhérentes quant aux possibilités de stockage et de calcul à partir de ces « bits classiques ».

En revanche, le **bit quantique** (ou *qubit*) peut prendre non seulement ces valeurs mais également toutes les valeurs intermédiaires. Ce **qubit**, en fait, est constitué de ce que l'on appelle une superposition linéaire des *états quantiques* correspondant aux bits (classiques) 0 et 1. Par superposition linéaire, on entend ici un certain type de combinaison linéaire au sens algébrique. Cela permet une **structure beaucoup plus riche** en terme de représentation de l'information qui décuple les capacités de calcul ainsi que de cryptage et de transport de l'information.

Intrication Cette structure plus complexe du qubit, par rapport au bit classique, se retrouve par exemple dans le phénomène d'**intrication quantique**. Dans ce contexte, deux objects quantiques intriqués (par exemple deux qubits) bien que séparés par une distance arbitraire, ne sont en fait qu'une seule et même entité. De fait on ne peut pas comprendre cette entité comme la réunion de deux objets indépendants. Si cela était le cas, on admettrait alors qu'un signal puisse se propager à une vitesse supérieure à celle de la lumière...

Parallélisme C'est la mise en oeuvre de ces propriétés de superposition et d'intrication qui permet (en théorie) à un ordinateur « quantique » de réaliser un nombre beaucoup plus grand d'opérations que son homologue « classique ». De plus, il y a maintenant un nombre croissant d'**algorithmes quantiques** qui exploitent ces aspects quantiques tels que l'**algorithme de Shor** [1] pour la factorisation des nombres premiers. C'est cet algorithme qui a véritablement propulsé l'informatique quantique et ouvert la voie à une nouvelle algorithmique. Pour citer un autre exemple, Il existe également l'**algorithme de Grover** [2, 3] qui permet de rechercher une entrée dans une *base non-structurée*, etc...

Décohérence Malgré les promesses de l'ordinateur quantique, il demeure néanmoins un **obstacle majeur** à sa réalisation physique et c'est celui de sa sensibilité à son environnement. Cette vulnérabilité se traduit par la propriété quantique dite de **décohérence** qui entraine une perte de relation de phase entre deux états quantiques. Cette relation est nécéssaire à la réalisation d'un calcul quantique. C'est l'interaction des qubits avec l'environnement qui brouille les délicates superpositions linéaires à l'origine de la cohérence d'un système quantique.

Afin de construire un ordinateur quantique fiable, il est donc nécéssaire de limiter un maximum ses interactions avec l'extérieur afin qu'il soit **parfaitement isolé**. Bien entendu, comme il impossible de réaliser ceci expérimentalement il faut s'attendre à des erreurs dues aux perturbations extérieures. C'est pourquoi des **codes correcteurs d'erreurs** ont été élaborés afin de palier à ces défauts d'isolation.

1.5 Perspectives

Malgré ces limitations, le **calcul quantique** recèle de très nombreuses applications à court, moyen et long termes. Parmi les domaines qui sont susceptibles d'être impactés par le calcul quantique on peut citer :

- *Chimie* : la simulation quantique de la chimie moléculaire permettrait d'optimiser et d'améliorer la production de produits chimiques (engrais, etc...)
- *Science des matériaux* : l'analyse des interactions physico-chimiques complexes permettrait de découvrir plus rapidement des nouveaux matériaux.
- *Médecine* : la modélisation les réactions chimiques à l'échelle moléculaire permettrait de prédire avec plus de précision l'interaction protéines-médicaments, ce qui mènerait à de nouvelles méthodologies pharmaceutiques.

- *Biologie* : La simulation de processus tels que la photosynthèse ou la modélisation des systèmes énergétiques.
- *Optimisation et logistique* : Accélération de la résolution de problèmes d'optimisation complexes (distribution d'énergie, traffic routier, etc...).
- *Apprentissage pour l'Intelligence Artificielle* : amélioration et accélération considérable de l'apprentissage à partir de modèles différentiels complexes (aéronautique, systèmes énergétiques ...)
- etc ...

1.6 Bibliographie

Il existe de très nombreux ouvrages, à des niveaux divers, qui peuvent servir de complément (ou de prolongation) à ce cours d'introduction.

Calcul Quantique Voici, en premier lieu, une sélection de trois ouvrages sur le thème du calcul quantique, de niveau de difficulté différent, qui sont particulièrement recommandés :

⇒ Livre de *vulgarisation* :

- « **Quantum Computing Since Democritus** » par Scott AARONSON

⇒ Livre d'*introduction* :

- « **A Short Introduction to Quantum Information and Quantum Computation** » par Michel LE BELLAC

⇒ Livre de *référence* :

- « **Quantum Computation and Quantum Information** »
  par Isaac CHUANG and Michael NIELSEN

Il existe également d'autres ouvrages intéressants, au niveau introductif, sur le vaste sujet du calcul quantique, en voici une sélection :

- « **Quantum Computer Science** » par David MERMIN
- « **Quantum Computing for Computer Scientists** »
  par Noson YANOVSKY et Mirco MANNUCCI
- « **Quantum Computing: An Applied Approach** » par Jack HIDARY
- « **Mathematics Of Quantum Computing: An Introduction** » par Wolfgang SCHERER
- « **Quantum Computing Explained** » par David MCMAHON

Physique Quantique Les outils et concepts de la mécanique quantique jouent également un rôle très important. Dans ce sens les livres suivants sont particulièrement recommandés :

⇒ Livre de *vulgarisation* :

- « **Initiation à la physique quantique** » par Valerio SCARANI

⇒ Livre d'*introduction* :

- « **Introduction à la physique quantique** » par Charles ANTOINE

⇒ Livre de *référence* :

- « **Mécanique quantique Tome I, II & III** »
  par Claude COHEN-TANNOUDJI, Bernard DIU et Franck LALOË

Voici une courte sélection d'autres ouvrages (la littérature sur le sujet est extrêmement vaste et variée), regroupés par niveau, pouvant également être intéressant pour ceux qui veulent approfondir le sujet : ($\star$: Introduction, $\star\star$: Intermédiaire, $\star\star\star$: Avançé)

$\star$ « **15 leçons de mécanique quantique** » par Jean-Louis BASDEVANT

$\star$ « **Quantum Mechanics** » par Jim PEEBLES

$\star$ « **Essential Quantum Mechanics** » par Gary BOWMAN

$\star$ « **Introduction to Quantum Mechanics** » par David GRIFFITHS

$\star\star$ « **Physique quantique Tome I & II** » par Michel LE BELLAC

$\star\star$ « **Mécanique quantique** » par Jean-Louis BASDEVANT et Jean DALIBARD

$\star\star$ « **Mécanique Quantique Tome I, II & III** » par Claude ASLANGUL

$\star\star\star$ « **Mécanique Quantique Tome I & II** » par Albert MESSIAH

$\star\star\star$ « **Mécanique Quantique** » par Lev LANDAU et Evgeni LIFCHITS

Ressources Web Il existe, encore une fois, de *très* nombreuses sources d'information et d'enseignement en ligne sur le calcul quantique (*quantum computing*). En voici une petite sélection :

- **Quantum computing for the determined** par Michael NIESLEN.
- **Quantum Computing Since Democritus** par Scott AARONSON (blog).
- **Qubits, Quantum Mechanics, and Computers** par Birgitta WHALEY.
- **Theory of Quantum Information** par John WATROUS.
- **Lecture Notes on Quantum Computing** par John PRESKILL.
- **Quantum Computing** par IBM.
- **Where can I learn about quantum information?** par Aram HARROW.
- **Quantum Computation Lecture Notes** par David MERMIN.

2 Premier modèle physique d'un qubit : le photon

Introduction De manière simple, le *bit quantique* ou *qubit* correspond à la plus petite quantité d'information que l'on peut transporter ou stocker par l'intermédiaire d'un système quantique. Pour transporter cette entité élémentaire nous allons considérer un système quantique simple, le **photon** (*grain de lumière*). Plus précisément, C'est la **polarisation** de ce dernier qui va servir à encoder de manière quantique l'information que l'on cherche à manipuler. Cependant, avant d'aborder la description quantique de polarisation du photon, nous allons d'abord revenir sur le phénomène de polarisation d'un point de vue classique.

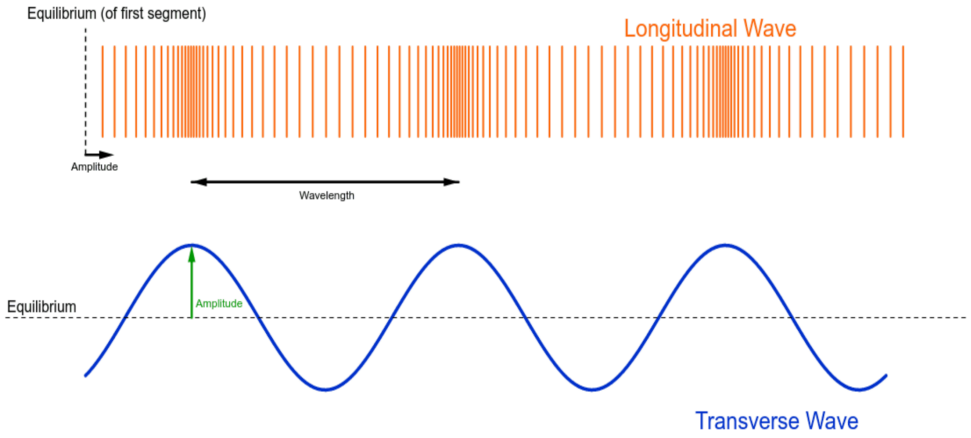

Figure 2: Ondes associées aux vibrations transverses (comme pour la lumière) et longitudinales (comme pour des ondes sismiques).

2.1 Approche classique de la polarisation

Rappel historique La polarisation de la lumière a été mis en évidence en 1809 par **Malus**. Celui-ci observa la double image du soleil donnée à travers un cristal de *spath d'Islande*. En faisant tourner ce cristal, une des deux images du soleil disparaissait. Ceci est du au fait que le *spath d'Islande* est un cristal **biréfringent**. Il décompose la lumière en deux rayons polarisés dans des directions perpendiculaires alors que la lumière incidente (qui est, dans ce cas précis, reflétée par une vitre) est (partiellement) polarisée.

Vibration transverse Pour une orientation convenable du cristal, on observera donc une extinction (ou une forte atténuation) d'un des deux rayons. Le phénomène de polarisation met en évidence le caractère vectoriel des vibrations lumineuses, c'est-à-dire que l'on peut représenter ce phénomène par un vecteur oscillant au cours du temps. Dans le cas de la lumière, ces vibrations sont **transverses** (orthogonales) à la direction de propagation. Ce phénomène de vibrations est similaire aux ondes mécaniques de cisaillement lors de secousses sismiques (**Figure 2**).

Modèle mathématique d'une onde transverse Avant de passer à l'aspect vectorielle de la polarisation de la lumière, rappelons d'abord la description mathématique d'une onde scalaire. Une telle onde (progressive) se propageant au cours du temps selon la direction Oz est décrite par la fonction scalaire suivante (qui représente l'amplitude de vibration) :

$$u(z,t) = u_0 \cos(\omega t - kz)$$

Plusieurs grandeurs physiques apparaissent dans cette expression : $\omega = ck = 2\pi/T = 2\pi f$ correspond à la fréquence angulaire de la vibration (en s^{-1}) et c est la vitesse de la lumière (en $\mathsf{m.s}^{-1}$), $k = 2\pi/\lambda$ est le module du vecteur d'onde (en m^{-1}) et λ est la longueur d'onde (en m^{-1}). Sans perdre de généralité, on se place dans un plan particulier, fixé en $z = 0$, ce qui conduit à

$$u(z=0,t) = u(t) = u_0 \cos(\omega t)$$

Vecteur polarisation Le modèle de l'onde scalaire peut se généraliser aux trois dimensions afin représenter le vecteur **champ électrique** qui caractérise une onde lumineuse que l'on écrira sous la forme (dans le plan $z = 0$)

$$\vec{E} = \vec{E}_0 \cos(\omega t)$$

C'est l'orientation spécifique de ce champ électrique (dans la plan perpendiculaire à la propagation de l'onde) que l'on appelle **polarisation** (linéaire) de la lumière. La lumière est donc perçue comme un **champ électromagnétique** dont la composante électrique est **orthogonale** à sa direction de propagation.

Champ électrique transverse Afin de décrire l'orientation du champ électrique $\vec{E}$, et donc la polarisation, de manière plus précise, on choisit un système d'axe Ox et Oy dans le plan transverse. En posant $||\vec{E_0}|| = E_0$, on peut écrire le champ électrique sous la forme

$$\vec{E} = \begin{pmatrix} E_x \\ E_y \end{pmatrix} = E_x\,\vec{u}_x + E_y\,\vec{u}_y \quad \Longrightarrow \quad \vec{E} = E_0\cos\theta\cos(\omega t)\,\vec{u}_x + E_0\sin\theta\cos(\omega t)\,\vec{u}_y \tag{2.1}$$

Dans cette forme, l'angle θ caractérise l'orientation de $\vec{E}$ dans xOy, donc il determine la **polarisation**. L'orientation θ de la polarisation peut être imposé, par exemple, par un filtre **polaroid** particulier. L'**intensité** (ou l'énergie) véhiculé par l'onde lumineuse est proportionnelle au carré (du module) du champ électrique, c'est-à-dire

$$I \propto E_0^2$$

Vecteur unitaire de polarisation Pour simplifier l'écriture du champ $\vec{E}$, il est commode d'introduire un **vecteur unitaire**, noté $\hat{p}$, appartenant au plan xOy de telle sorte que

$$\hat{p} = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} \quad \Longrightarrow \quad \vec{E} = E_0\cos(\omega t)\,\hat{p}$$

Le vecteur $\hat{p}$ caractérise donc l'orientation de la polarisation de l'onde lumineuse :

* Si $\theta = 0 \quad \Longrightarrow \quad$ Polarisation selon Ox $(\hat{p} = \vec{u}_x)$
* Si $\theta = \pi/2 \quad \Longrightarrow \quad$ Polarisation selon Oy $(\hat{p} = \vec{u}_y)$

Au passage on notera que la lumière naturelle est **non-polarisée**, elle est une superposition *incohérente* de 50% de lumière polarisé selon Ox et de 50% de lumière polarisée selon Oy.

2.2 Changement et mesure de la polarisation de la lumière

Polariseur et Analyseur Notre but est ici d'utiliser la polarisation de la lumière afin d'encoder de l'information. On a donc besoin, a priori, de pouvoir **changer** et **mesurer** l'orientation du champ $\vec{E}$ associé à l'onde lumineuse. On utilise dans ce cas un **système de deux polariseurs** consécutifs :

- Le polariseur « d'entrée » va orienter la polarisation de la lumière incidente selon un angle θ par rapport à Ox (voir **Figure 3**).
- Le polariseur « de sortie » (appelé l'*analyseur*) possède un axe de polarisation faisant un angle α avec Ox (voir **Figure 3**).

Si on utilise un vecteur unitaire $\hat{n}$ pour décrire la direction de polarisation de l'analyseur alors on peut écrire

$$\hat{n} = \cos\alpha\,\vec{u}_x + \sin\alpha\,\vec{u}_y = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}$$

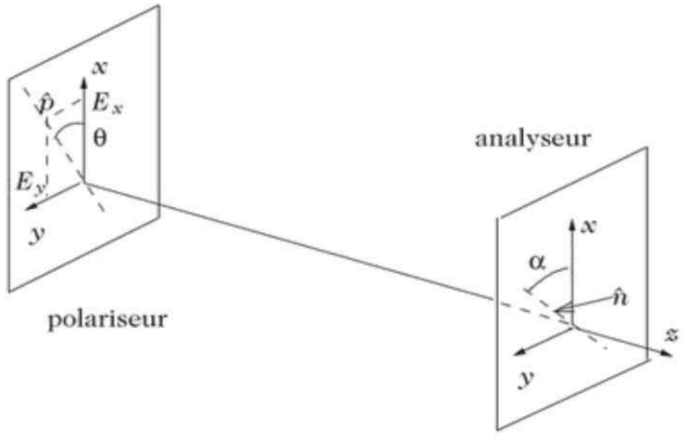

Figure 3: Schéma du système polariseur/analyseur

Loi de Malus D'après ce qui a été mentionné précédemment, si l'on veut **mesurer** la polarisation à la sortie de l'analyseur on doit déterminer l'orientation du champ électrique, noté $\vec{E}'$, à la sortie de l'*analyseur*. Pour cela on projette le champ électrique $\vec{E}$ (orienté selon $\hat{p}$) dans la direction $\hat{n}$

$$\begin{aligned}\vec{E}' &= (\vec{E}\cdot\hat{n})\,\hat{n}\\ &= E_0\,\cos(\omega t)\,(\hat{p}\cdot\hat{n})\,\hat{n}\\ &= E_0\,\cos(\omega t)\,(\cos\theta\cos\alpha+\sin\theta\sin\alpha)\,\hat{n}\\ \vec{E}' &= E_0\,\cos(\omega t)\,\cos(\theta-\alpha)\,\hat{n}\end{aligned}$$

On en déduit la *loi de Malus*, qui est une loi *classique*, pour l'intensité à la sortie de l'analyseur

$$I' = I\,\cos^2(\theta-\alpha) \tag{2.2}$$

Il est à noter que si l'on utilise une description quantique du phénomène, on parle alors plutôt de *photon* que d'*onde* pour décrire la lumière. Cette description doit néanmoins permettre de retrouver cette *loi de Malus*, d'où son rôle important dans notre présentation.

Polariseurs orthogonaux On considère un système polariseur/analyseur chacun avec une orientation orthogonale par rapport à l'autre. Le polariseur est selon Ox et l'analyseur selon Oy. Dans ce cas **aucune lumière** n'est transmise. En revanche Si on introduit un polariseur intermédiaire qui fait un angle θ avec Ox, alors une partie de la lumière est réstituée. Une première projection introduit un facteur $\cos\theta$ et une seconde un facteur $\sin\theta$, d'où une intensité de sortie $I' = I\,\cos^2\theta\,\sin^2\theta$ qui s'annule uniquement pour $\theta = \frac{\pi}{2}$ et $\theta = 0$.

Type de polarisation Dans l'expression (2.1), il est à noter que les deux composantes de $\vec{E}$ ont la même dépendance par rapport au temps. Il s'agit du *cas particulier de polarisation* dite **linéaire** (ou **rectiligne**) où le déphasage temporel entre les deux composantes du champ $\vec{E}$ est nul. En d'autres termes, les deux composantes de $\vec{E}$ « tournent » de manière *synchrone*. De manière générale, les composantes du champ $\vec{E}$ se notent avec une phase spécifique (pour chaque composante) qui n'est pas forcément la même. On écrit alors

$$\begin{cases} E_x = E_0\,\cos\theta\,\cos(\omega t-\delta_x)\\ E_y = E_0\,\cos\theta\,\cos(\omega t-\delta_y)\end{cases}$$

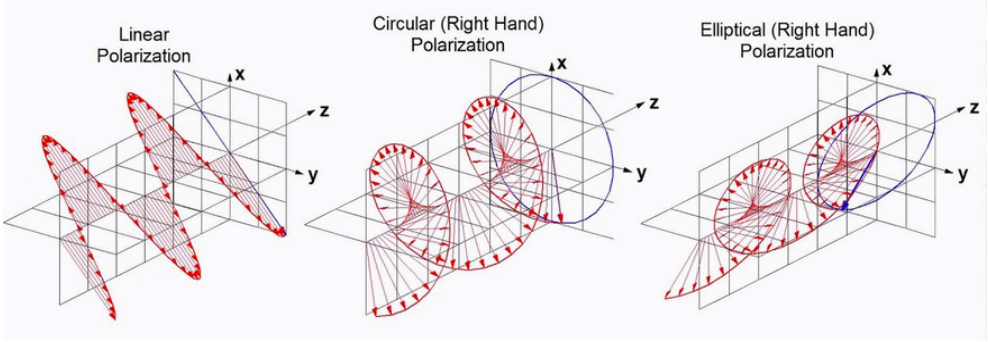

Figure 4: Les différents type de polarisation

On distingue alors trois type de polarisation en fonction de la différence de phase $\delta = \delta_x - \delta_y$:

- Si $\delta = 0$ ou $\delta = \pm\pi$ on parle de **polarisation rectiligne**. Dans ce cas, E_x et E_y oscillent (au cours du temps) dans un plan fixe faisant un angle θ avec Ox.
- Si $\delta = \pm\frac{\pi}{2}$ on parle de **polarisation circulaire** car l'extrémité du vecteur $\vec{E}$ décrit un cercle au cours du temps.
- Si $\delta \neq p\frac{\pi}{2}$ avec $p \in \mathbb{Z}$ alors il n'y a pas de relation particulière entre les phases des deux composantes et on parle de **polarisation elliptique**. L'extrémité de $\vec{E}$ décrit une *ellipse* au cours du temps.

Remarque importante En pratique on ne peut pas mesurer expérimentalement la phase individuelle d'une composante de $\vec{E}$. Seule la différence de phase δ est accessible et est donc **physiquement importante**. On notera que l'on peut imposer $\delta_x = 0$ en redéfinissant l'origine des temps.

Remarque technique Le champ électrique $\vec{E}$ peut aussi s'écrire dans la notation complexe suivante :

$$\vec{E} = E_0 \,\mathsf{Re}\left[e^{-i\omega t} \begin{pmatrix} \lambda \\ \mu \end{pmatrix} \right] \quad \text{avec} \quad \begin{pmatrix} \mu \\ \lambda \end{pmatrix} = \begin{pmatrix} \cos\theta \, e^{i\delta_x} \\ \sin\theta \, e^{i\delta_y} \end{pmatrix}$$

où la polarisation est donnée par le vecteur complexe $\begin{pmatrix} \mu \\ \lambda \end{pmatrix}$ avec $\mu, \lambda \in \mathbb{C}$ et la condition de normalisation $|\lambda|^2 + |\mu|^2 = 1$ (la fonction $\mathsf{Re}[...]$ prend la partie réelle de $[...]$).

Dispositif expérimentaux Outre le système polariseur/analyseur, il existe d'autre moyen de manipuler la polarisation de la lumière. Lorsque qu'une lumière incidente contient deux états de polarisation orthogonaux (selon Ox et Oy par exemple), un filtre polaroïd **absorbera** une des deux polarisation et laissera passer l'autre. En revanche une lame biréfringente permet de **séparer** deux états de polarisation **orthogonaux**.

2.3 Approche quantique de la polarisation

Le photon Depuis Einstein en 1905, on sait que la lumière peut-être modélisée par des particules appelées **photons**. En réduisant l'intensité lumineuse suffisamment on peut étudier la polarisation rectiligne individuelle de chaque photons [1]. Dans ce contexte, la taille typique d'un photon est

[1] Ceux-ci sont détectables à l'aide de *photodétecteurs* contenus dans une caméra CDD par exemple

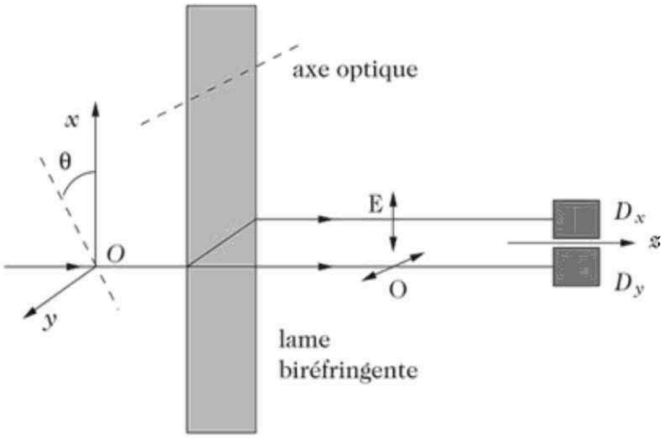

Figure 5: Dispositif de lame biréfringente permettant de séparer un faisceau lumineux de polarisation quelconque en deux faisceau polarisation orthogonalement.

donné par sa longueur d'onde qui est de l'ordre du nanomètre ce qui justifie de parler **polarisation quantique**.

Malgré ce passage au domaine quantique, il faut bien garder à l'esprit que si dans une expérience on détecte N photons, alors dans le cas où $N \to \infty$ on doit retrouver le comportement ondulatoire **classique** de la lumière. Reprenons le dispositif précédent de *lame biréfringente* (**Figure 5**) mais cette fois-ci dans le cas de photons incidents dont la polarisation *rectiligne* fait (toujours) un angle θ avec Ox.

Non-simultaneité En passant à travers la lame biréfringente, le faisceau constitué de photons est séparé en un faisceau d'intensité $I\cos^2\theta$ polarisé selon Ox et un autre faisceau d'intensité $I\sin^2\theta$ polarisé selon Oy. L'expérience montre que les détecteurs D_x et D_y ne **cliquent jamais simultanément** ! Un photon « *entier* » est détecté soit en D_x ou alors en D_y, **il ne se divise pas**. En répétant l'expérience on peut mesurer la probabilité de détection d'un photon individuel pour chaque détecteur. On obtient :

$$\mathsf{P}_x = \cos^2\theta \quad \text{et} \quad \mathsf{P}_y = \sin^2\theta$$

où P_x et P_y sont les probabilités de mesurer un photon polarisé selon Ox et Oy respectivement. Au passage on dit qu'une telle expérience met en valeur l'aspect corpusculaire de la lumière.

Recouvrement de la loi classique Si N photons sont envoyés dans le dispositif alors le nombre de photon détectés par chaque détecteur est :

$$D_x \ : \ N_x \simeq N\cos^2\theta \quad \text{et} \quad D_y \ : \ N_y \simeq N\sin^2\theta$$

Ici, Le signe $\simeq$ tient compte de fluctuations statistiques d'ordre $\sqrt{N}$ qui sont négligeables lorsque N est grand. On sait que l'intensité lumineuse est proportionnelle au nombre de photons. On retrouve donc la *loi de Malus* (2.2) lorsque $N \to \infty$. Cependant, malgré cette constatation positive, des changements majeurs sont intervenus par rapport à une expérience classique.

Nature probabiliste Tout d'abord, on observe que pour un photon individuel donné, il est **impossible** de prévoir à l'avance quel chemin il va prendre puisque l'on a au mieux que des probabilités (P_x et P_y) d'être passer par l'un ou l'autre détecteur. Cette constatation est en opposition flagrante

avec le déterminisme qui (semble) régir la mécanique classique. De plus cette nature probabiliste de ce phénomène quantique (la polarisation du photon) est **intrinsèque** à sa description. En d'autres mots, elle ne reflète pas un manque d'information de notre part ou une **incomplétude** de la théorie quantique qui contiendrait des *variables cachées*.

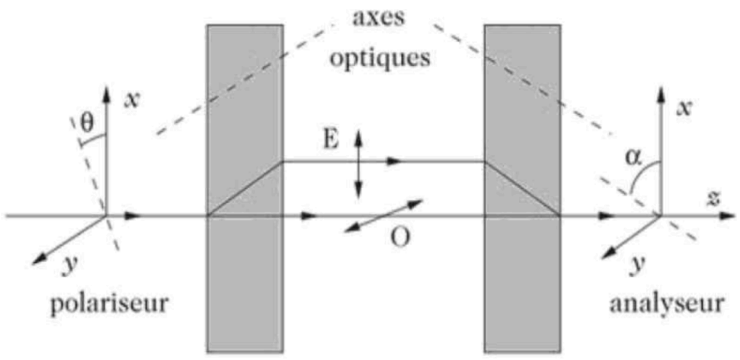

Figure 6: Recombinaison de faisceaux de photons de polarisation orthogonales.

Recombinaison de faisceaux Pour aller plus loin dans notre analyse et essayer de retrouver la *loi de Malus* malgré cette différentiation de chemin, on cherche maintenant à recombiner les deux faisceaux par un dispositif montré sur la **Figure 6**. Normalement, si on place un analyseur en fin de dispositif, on s'attend à retrouver une intensité de sortie proportionnelle à $\cos^2(\theta - \alpha)$. Cette intensité correspond également, dans notre approche quantique, à la probabilité de détecter un photon avec une polarisation selon Ox, c'est-à-dire également $\mathsf{P}_x = \cos^2(\theta - \alpha)$.

Analyse du trajet du photon Comme on peut le constater sur la **Figure 6**, le photon a deux chemins possibles :

(E) Il traverse d'abord le polariseur avec une probabilité de $\cos^2\theta$, puis l'analyseur avec une probabilité $\cos^2\alpha$. Dans ce cas la probabilité (totale) à la sortie de l'analyseur est juste le produit de ces probabilités $\cos^2\theta\cos^2\alpha$.

(O) En revanche, si il suit l'autre chemin alors il traverse le polariseur avec une probabilité de $\sin^2\theta$, puis l'analyseur avec une probabilité de $\sin^2\alpha$. On trouve alors une probabilité à la sortie de $\sin^2\theta\sin^2\alpha$.

Maintenant, en sommant les probabilités de chaque chemin, nous devrions retrouver la probabilité de sortie $\mathsf{P}_x = \cos^2(\theta - \alpha)$, or la probabilité totale pour un photon de sortir de l'analyseur est :

$$\mathsf{P}_{tot} = \cos^2\theta\cos^2\alpha + \sin^2\theta\sin^2\alpha \neq \cos^2(\theta - \alpha)$$

Le raisonnement que nous avons eu, en additionnant les probabilités associées à chaque chemin, est donc faux.

Amplitude de probabilité Pour retrouver la *loi de Malus* il faut en fait raisonner à partir de la notion d'**amplitudes de probabilité** pour chaque chemin (et non de probabilité). C'est le module au carré de cette amplitude (notée a) qui donne la probabilité associée tel que $|\mathsf{a}|^2 = \mathsf{P}$. On note ces amplitudes

$$\mathsf{a}(\theta \to x) = \cos\theta \qquad \mathsf{a}(x \to \alpha) = \cos\alpha$$
$$\mathsf{a}(\theta \to y) = \sin\theta \qquad \mathsf{a}(y \to \alpha) = \sin\alpha$$

Ici la quantité $\mathsf{a}(\theta \to x)$ est donc l'amplitude associé à la probabilité de détecter un photon polarisé selon Ox dans le polariseur. L'*amplitude totale* de sortie s'obtient en **superposant** les amplitudes pour des chemins **indiscernables** [2]:

$$\mathsf{a}_{tot} = \cos\theta\cos\alpha + \sin\theta\sin\alpha = \cos(\theta - \alpha)$$

Si on calcule maintenant la probabilité de sortie à partir de l'*amplitude de probabilité* total on retrouve bien :

$$\mathsf{P}_{tot} = |\mathsf{a}_{tot}|^2 = \cos^2(\theta - \alpha)$$

Les lois de composition des amplitudes de probabilité sont *identiques* à celles de l'optique ondulatoire classique. On retrouve donc les résultats de cette approche classique dans la limite où le nombre de photons est (très) grand.

Discernabilité Supposons un instant que l'on puisse savoir quel chemin est emprunté par chaque photon (même si cela est impossible...) On a alors deux catégories de photons : ceux qui prennent le chemin (E) et ceux qui prennent le chemin (O). Si on bloque le chemin (O) pour les photons empruntant le chemin (E) cela ne change rien et pareillement pour les photons prenant le chemin (O) en bloquant le chemin (E). Dans ce cas les chemins possibles sont **discernables** et on doit sommer les probabilités associés à chaque chemin pour obtenir la probabilité de sortie de l'analyseur :

$$\cos^2\theta\cos^2\alpha + \sin^2\theta\sin^2\alpha$$

De fait, on sait que ce résultat est faux et donc un photon ne fait aucune distinction entre les chemins (E) et (O), on parle d'indiscernabilité des chemins possibles.

Interprétation En conclusion, c'est donc bien l'*impossibilité expérimentale* de distinguer le chemin pris par un photon (E ou O) qui conduit à la notion d'**amplitude de probabilité**. On a deux interprétations possibles (et justes) :

(i) le photon emprunte les deux trajets à la fois;

(ii) la question « *quel trajet ?* » n'a aucun sens;

La deuxième interprétation est préférable au sens où il est impossible de différentier les chemins **expérimentalement**. En fait, de manière plus générale, la notion de trajectoire n'existe pas en mécanique quantique et elle est remplacé en quelque sorte par la notion de *probabilité de présence* d'une particule quantique dans un volume donnée. De plus la première interprétation sous-entend, si on la prend au pied de la lettre, qu'un photon puisse prendre **physiquement** les deux chemins possibles simultanément, ce qui est faux. Un photon ne peut prendre *physiquement* que l'un ou l'autre des trajets possibles mais ceux-ci sont impossibles à discerner ce qui peut conduit à l'interprétation (i) au premier abord.

Résumé Dans cette section nous avons décrit un premier système physique quantique qui permette de supporter un qubit, le **photon**. C'est la polarisation, c'est-à-dire l'orientation du champ électrique attaché au photon, qui permet d'encoder l'information puisqu'elle peut prendre deux valeurs correspondantes aux bits classiques **1** et **0**. On s'est appuyé sur les règles classiques qui gouvernent le comportement ondulatoire de la lumière afin de mettre en évidence les règles quantiques différentes qui régissent le comportement du **photon**.

[2] ce qui revient à additionner les amplitudes

3 Première application : la cryptographie quantique

Information et polarisation Précédemment, on a vu que la polarisation (rectiligne) pouvait être manipuler par des dispositifs expérimentaux relativement simples (au moins conceptuellement). Afin d'encoder l'information au niveau quantique, on décide alors d'attribuer arbitrairement une valeur de bit à une direction de polarisation :

- **Valeur 1** $\Leftrightarrow$ Photon polarisé selon Ox
- **Valeur 0** $\Leftrightarrow$ Photon polarisé selon Oy

Convention de communication Si deux personnes, conventionnellement appelés *Alice (A)* et *Bob (B)*, échangent des informations, à l'aide d'une fibre optique par exemple, sous **forme quantique** alors cela prend la forme d'une suite de photons polarisées, envoyé par *Alice*, selon :

$$y\, y\, x\, y\, x\, y\, y\, y\, x\, \ldots$$

Lorsque *Bob* reçoit l'information, il peut analyser la polarisation à l'aide d'une lame biréfringente et en déduit le message d'*Alice* [3]

$$0\,0\,1\,0\,1\,0\,0\,0\,1\,\ldots$$

Possibilité d'écoute Dans ce contexte, si une troisième personne, appelée *Eve*, tente d'intercepter le message, elle va devoir mesurer la polarisation quantique de l'un des photons. Or *Eve* ne sait pas quelle polarisation elle va mesurer, elle a 50% de chance de se tromper puisqu'il n'y a que deux polarisations possibles. Ensuite elle doit renvoyer le photon à *Alice*, là aussi avec 50% de chance de se tromper. Donc au final, si *Alice* et *Bob* comparent une partie de leur message, ils doivent pouvoir constater une plus grande quantité d'erreurs si leur message a été espionné. C'est cet aspect de la mécanique quantique qui est employé afin de protégé la transmission d'un message donné.

3.1 Protection de clé publique

Clé de chiffrage La cryptographie repose sur une **clé de chiffrage** connu seulement de l'expéditeur (*Alice*) et du destinataire (*Bob*). Cette clé est le plus souvent une *clé publique* (par opposition à une *clé secrète*) accessible au public. Un exemple de système de clé publique est celui basé sur la factorisation de grand nombre en **facteur premiers**. En fait, trouver deux nombres premiers p et q tels que $pq = N$ entraîne un temps de calcul de l'ordre de

$$\simeq e^{(1.9)(\ln N)^{1/3}(\ln\ln N)^{2/3}}$$

C'est ce temps de calcul qui est le principal obstacle que doit franchir toute personne (communément appelée *Eve*) cherchant à déchiffrer le message entre (*Alice*) et destinataire (*Bob*). Cependant, il n'est pas exclu de tels calculs soient exécutés plus rapidement, notamment par une approche quantique !

Cryptographie quantique Dans le cadre de la cryptographie quantique il ne s'agit pas, en fait, de protéger le message transmit à l'aide de la *physique quantique* mais plutôt la clé de chiffrage (publique dans ce cas) qui permet de décoder le message lui-même. En particulier, on cherche à s'assurer que la transmission d'une clé n'a pas été espionnée (on parle de *distribution quantique d'une clé*). Une procédure particulière qui permet d'effectuer une telle opération est le protocole BB84 du nom de leur auteurs, Charles Bennett and Gilles Brassard, et de l'année de publication de ce protocole [4].

[3] Ce protocole, bien que peu efficace, est la base de la *cryptographie quantique*

3.2 Protocole BB84

Choix de polarisation On a vu que la transmission d'une telle clé peut se faire sous la forme d'une suite de photons (transmis) polarisés. On suppose donc qu'*Alice* peut envoyer 4 types de photons avec des **polarisations rectilignes** différentes :

$$0° : \longleftrightarrow \quad , \quad +45° : \nearrow \quad , \quad +90° : \updownarrow \quad , \quad -45° : \nwarrow$$

On peut alors regrouper les polarisation en deux ensembles différents, chaque ensemble étant attribué à une valeur de bit selon :

$$\mathfrak{E}_1 = \left\{ \updownarrow , \nwarrow \right\} \implies \mathbf{1} \quad \text{et} \quad \mathfrak{E}_0 = \left\{ \longleftrightarrow , \nearrow \right\} \implies \mathbf{0}$$

On remarque que pour chaque valeur de bit 1 ou 0, on peut lui associé une polarisation qui appartient soit à $\mathfrak{E}_1$, soit à $\mathfrak{E}_0$. On a alors 50% de chance de se tromper.

Transmission À chaque fois que *Alice* va envoyer un photon elle va également **choisir au hasard** une des deux bases utilisées pour émettre/recevoir les photons :

$$\left\{ \boxplus , \boxtimes \right\}$$

Au niveau physique, ces bases $\boxplus$ et $\boxtimes$ sont constitués par des systèmes similaires au dispositif de lame biréfringente que l'on a introduit précédemment. Il est important de remarquer que si *Alice* veut émettre le bit $\mathsf{bit}_A = \mathbf{0}$ elle peut choisir une des deux bases $\boxplus$ ou $\boxtimes$ indistinctement. Lorsque *Bob* va recevoir un photon, il va aussi choisir parmi une des deux bases **aléatoirement**. Il va ensuite analyser la polarisation du photon reçu, grâce à cette base, pour en déduire sa valeur en bit (0 ou 1). Le processus, pour une émission de plusieurs photon est illustré sur le tableau suivant.

bit_A	0	1	1	0	1	0	0	1
$\mathfrak{B}_A$	$\boxplus$	$\boxplus$	$\boxtimes$	$\boxplus$	$\boxtimes$	$\boxtimes$	$\boxtimes$	$\boxplus$
$\mathcal{P}_A$	$\longleftrightarrow$	$\updownarrow$	$\nwarrow$	$\longleftrightarrow$	$\nwarrow$	$\nearrow$	$\nearrow$	$\updownarrow$
$\mathfrak{B}_B$	$\boxplus$	$\boxtimes$	$\boxtimes$	$\boxtimes$	$\boxplus$	$\boxtimes$	$\boxplus$	$\boxplus$
$\mathcal{P}_B$	$\longleftrightarrow$	$\nwarrow$ ou $\nearrow$	$\nwarrow$	$\nwarrow$ ou $\nearrow$	$\longleftrightarrow$ ou $\updownarrow$	$\nearrow$	$\nwarrow$ ou $\nearrow$	$\updownarrow$
$\mathcal{I}_B$	0	Jeté	1	Jeté	Jeté	0	Jeté	1

Table 1: Exemple de déroulé du protocole BB84

Reception Parfois la base de réception de *Bob* $\mathfrak{B}_B$ n'est pas « aligné » avec la polarisation du photon qu'il reçoit. Dans ce cas, l'état de polarisation du photon est projeté sur l'une des deux directions qui forment la base $\mathfrak{B}_B$. Par exemple on peut avoir un photon incident polarisé selon $\nearrow$ et la base de réception est $\mathfrak{B}_B = \boxplus$. Dans ce cas *Bob* a 50% de chance de mesurer une polarisation selon $\updownarrow$ ou selon $\longleftrightarrow$, il a donc 50% de chance de se tromper!

Comparaison Afin d'indiquer à *Bob* les photons reçus dont la polarisation n'était pas aligné avec sa base de réceptions $\mathfrak{B}_B$, *Alice* rend publique sa base d'émission $\mathfrak{B}_A$ qu'elle a utilisé pour émettre ses photons. Si $\mathfrak{B}_B \neq \mathfrak{B}_A$ pour un photon, cela indique qu'il y a eu projection à cause d'une polarisation non-alignée. Dans ce cas le photon reçu est rejeté (voir tableau) et *Bob* ne conserve que les photons pour lesquels la base de réception $\mathfrak{B}_B$ était en accord avec la base d'émission $\mathfrak{B}_A$. Dans l'exemple montré dans le tableau, la partie de la clé conservée est $0\,1\,0\,1\ldots$, elle aussi appelée **clé réconciliée**. On peut facilement imaginer que cette clé continue pour un message plus long...

Interception Comme mentionné précédemment, l'avantage de cryptographie quantique est la protection unique qu'elle offre par rapport à l'interception d'une **clé réconciliée** constitué physiquement d'une suite de photons polarisés (échangés entre *Bob* et *Alice*). Par principe, une personne qui souhaite intercepter un tel message, appelée conventionnellement *Eve*, doit recevoir d'*Alice* puis renvoyé à *Bob* chaque photon intercepté. Deux cas se présente alors pour *Eve* :

- La base $\mathfrak{B}_E$ de réception de *Eve* est alignée avec la polarisation du photon qu'elle reçoit. Par exemple $\mathfrak{B}_E = \updownarrow\!\!\leftrightarrow$ pour un photon polarisé selon $\updownarrow$. Dans ce cas, *Eve* a 0% de chance de se tromper sur la polarisation du photon et donc de deviner la valeur correcte du bit intercepté (ici **1**).
- La base $\mathfrak{B}_E$ de réception de *Eve* est non-alignée avec la polarisation du photon qu'elle reçoit. Par exemple $\mathfrak{B}_E = \nwarrow\!\!\nearrow$ pour un photon polarisé selon $\longleftrightarrow$. Dans ce cas *Eve* a 50% de chance de se tromper sur la valeur du bit intercepté (ici **0**).

Non-clonage Il est absolument impossible pour *Eve* de procéder autrement que la manière qui est décrite. Elle est obligée de projeter la polarisation des photons interceptés afin de mesurer celle-ci. Cette particularité de la **mesure quantique** implique que, de manière générale, il est impossible d'interagir avec un « état quantique » (ici la polarisation du photon) sans le modifier. Cette propriété est souvent mentionné sous la forme d'un **théorème de non-clonage** stipulant qu'un état quantique ne peut être « copier ». Nous reviendrons dans la suite du cours sur cette notion.

En conclusion, si *Bob* et *Alice* compare une partie de leur clé réconciliée (publiquement), en cas d'écoute, il devrait y avoir 25% (c'est-à-dire la moyenne des probabilités pour que *Eve* se trompe) des bits qui sont différents. Dans un ce cas, il n'utilise pas le reste de leur message compromis. De manière générale, en sacrifiant n bits de la clé de réconciliation, *Alice* et *Bob* peuvent détecter un éventuel espion sur le canal avec une probabilité $1 - (3/4)^n$.

Résumé Dans cette section nous avons décrit comment l'on pouvait utiliser les règles quantiques qui décrivent la polarisation du photon et sa mesure afin de crypter la transmission d'une clé de chiffrage. Le protocole `BB84` que nous avons utiliser permet, en principe, de détecter si un message, constitué d'une série de photons polarisées, a été intercepté et ceci de manière absolue. Cette inviolabilité est la conséquence d'un résultat général connu sous le nom de **théorème de non-clonage**.

A Exercices

A.1 Polarisation

On a vu que l'on pouvait utiliser une notation complexe pour représenter le champ électrique associé à une onde électromagnétique progressive :

$$E_x(t) = E_{0x}\,\cos(\omega t - \delta_x) = \mathsf{Re}\left[E_{0x}\,e^{i\delta_x}\,e^{-i\omega t}\right] = \mathsf{Re}\left[\mathcal{E}_x\,e^{-i\omega t}\right]$$
$$E_y(t) = E_{0y}\,\cos(\omega t - \delta_y) = \mathsf{Re}\left[E_{0y}\,e^{i\delta_y}\,e^{-i\omega t}\right] = \mathsf{Re}\left[\mathcal{E}_y\,e^{-i\omega t}\right]$$

Soient deux nombres, λ réel et μ complexe, paramétrés par

$$\lambda = \cos\theta \qquad \mu = \sin\theta\,e^{i\delta_y}$$

Un polariseur (λ, μ) est constitué de trois éléments :

- Une première lame biréfringente qui déphase $\mathcal{E}_y$ de $-\eta$ en laissant $\mathcal{E}_x$ inchangé soit

$$\mathcal{E}_x \to \mathcal{E}_x^{(1)} = \mathcal{E}_x \qquad \text{et} \qquad \mathcal{E}_y \to \mathcal{E}_y^{(1)} = \mathcal{E}_y\,e^{-i\eta}$$

- Un polariseur linéaire qui projette suivant $\hat{n}_\theta$ selon

$$\mathcal{E}^{(1)} \to \mathcal{E}^{(2)} = \left(\mathcal{E}_x^{(1)}\cos\theta + \mathcal{E}_y^{(1)}\sin\theta\right)\,\hat{n}_\theta = \left(\mathcal{E}_x\cos\theta + \mathcal{E}_y\sin\theta\,e^{-i\eta}\right)\,\hat{n}_\theta$$

- Une seconde lame biréfringente qui laisse $\mathcal{E}_x^{(2)}$ inchangé et déphase $\mathcal{E}_y^{(2)}$ de η soit

$$\mathcal{E}_x^{(2)} \to \mathcal{E}'_x = \mathcal{E}_x^{(2)} \qquad \text{et} \qquad \mathcal{E}_y^{(2)} \to \mathcal{E}'_y = \mathcal{E}_y^{(2)}\,e^{i\eta}$$

La combinaison des trois opérations est représentée par $\mathcal{E} \to \mathcal{E}'$.

1. Calculer les composantes $\mathcal{E}'_x$ et $\mathcal{E}'_y$ en fonction de $\mathcal{E}_x$ et $\mathcal{E}_y$.

2. On décide de représenter les polarisations $\mathcal{E}$ et $\mathcal{E}'$ par des vecteurs, que l'on note $|\mathcal{E}\rangle$ et $|\mathcal{E}'\rangle$, qui s'expriment dans la base orthogonale $\{|x\rangle, |y\rangle\} = \{\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)\}$ selon

$$|\mathcal{E}\rangle = \mathcal{E}_x|x\rangle + \mathcal{E}_y|y\rangle \qquad \text{et} \qquad |\mathcal{E}'\rangle = \mathcal{E}'_x|x\rangle + \mathcal{E}'_y|y\rangle$$

   Déterminer la matrice $\mathcal{P}$ telle que $|\mathcal{E}'\rangle = \mathcal{P}\,|\mathcal{E}\rangle$.

A.2 Cryptographie

Alice envoie un bit **1** grâce à un photon polarisé selon $\updownarrow$ et celui-ci est intercepté par *Eve*. Si celle-ci utilise, par chance, la base de réception correcte, c'est-à-dire $\leftrightarrow\!\!\updownarrow$, elle a alors 100% chance de détecter de trouver la valeur (correcte) **1** envoyer par *Alice*. En revanche, si *Eve* utilise la base de réception $\nwarrow\!\!\nearrow$, alors elle aura seulement 50% de chance de trouver cette valeur correcte. La probabilité, notée P, pour *Eve* de mesurer la valeur correcte envoyée par *Alice* est donc

$$\mathsf{P} = \frac{1}{2}\left(1 + \frac{1}{2}\right) = \frac{3}{4} = 75\%$$

On suppose maintenant que la base de réception de *Eve* fait un angle ϕ, au lieu de $\pm 45°$, par rapport à l'axe Ox.

1. Montrer que la probabilité P_ϕ de succès pour *Eve* de mesurer le bit **1** est maintenant

$$\mathsf{P}_\phi = \frac{1}{4}\Big(2 + \cos(2\phi) + \sin(2\phi)\Big)$$

2. Montrer que pour un choix d'angle optimal $\phi = \phi_0$, que l'on déterminera, on obtient une probabilité de succès supérieur à 75% (il n'est pas nécessaire de faire un calcul).

3. Maintenant on suppose que *Alice* utilise une base d'émission qui fait un angle θ avec Ox et *Eve* utilise à nouveau les bases de réception $\{\updownarrow\!\!\leftrightarrow, \nwarrow\!\!\searrow\}$. Montrer que la probabilité pour *Eve* de se tromper est alors

$$\mathsf{P} = \frac{1}{4}\sin^2(2\theta)$$

References

[1] P. W. Shor, "Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM J. Sci. Statist. Comput.* **26** (1997) 1484, arXiv:quant-ph/9508027.

[2] L. K. Grover, "A Fast quantum mechanical algorithm for database search", arXiv:quant-ph/9605043.

[3] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack", *Phys. Rev. Lett.* **79** (1997) 325–328, quant-ph/9706033.

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", *Theoretical Computer Science* **560** (2014) 7 – 11, Theoretical Aspects of Quantum Cryptography & celebrating 30 years of BB84.