Cryptographie Quantique

I. Définition :

La "cryptographie quantique" est une expression médiatique, mais quelque peu trompeuse : en effet, il ne s'agit pas de chiffrer un message à l'aide de la physique quantique, mais d'utiliser celle-ci pour s'assurer que la transmission de la clé n'a pas été espionnée, donc il s'agit plutôt de la distribution quantique de clés.

Etant donné que la distribution de clés est un phénomène caractérisant la cryptographie symétrique, ainsi la cryptographie quantique est toujours combinée avec un algorithme de chiffrement symétrique (par bloc).

La cryptographie quantique a été fondée sur une idée originale de S. Wiesner, refusée en 1969 par une revue scientifique, puis s'est développée à partir de la publication par C.H. Bennett et G. Brassard, en 1984, d'un protocole d'échange quantique de clés. C'est aujourd'hui un domaine pluridisciplinaire en pleine expansion, a la veille d'applications commerciales et militaires

II. Principes de la cryptographie quantique :

Contrairement aux algorithmes de chiffrement symétrique et asymétrique qui s'appuient sur la complexité algorithmique (mathématique) de concevoir des méthodes ou des algorithmes permettant de casser le chiffre dans des délais raisonnables, même avec des machines très puissantes, la cryptographie quantique se base sur un phénomène (ou une loi) de la physique quantique.

L'idée fondamentale est d'exploiter le principe d'incertitude de Heisenberg pour interdire à un espion d'apprendre quoi que ce soit d'utile sur une transmission d'information. Ce principe a été souvent perçu comme une limitation fondamentale imposée par la mécanique quantique aux mesures physiques, ainsi la cryptographie quantique exploite cette limitation pour garantir un secret absolu sur des communications cryptées [1].

Principe d'incertitude de Heisenberg :

Le principe d'incertitude de Heisenberg a été découvert en 1920 suite à plusieurs expériences réalisées par plusieurs physiciens sur des particules microscopiques. Ce principe affirme qu'il était fondamentalement impossible de mesurer (observer) avec précision deux grandeurs physiques (appelés observables) simultanément pour un objet microscopique. Ainsi pour un photon la mesure précise de sa position par exemple détruit toute information sur sa vitesse et vice versa. La mesure simultanée des deux observables est toutefois possible, mais limitée à une précision « moyenne » [2].

En d'autres termes, ce « principe d'incertitude de Heisenberg » qui est une loi de la physique quantique limite la quantité d'information disponible sur les propriétés physiques de ces objets. De plus, il déclare qu'en général une mesure perturbe le système, ce qui limite la précision des mesures ultérieures [2].

Apport du principe sur la cryptographie :

L'exploitation du principe de Heisenberg en cryptographie quantique (distribution de clés) permet d'interdire à un espion d'apprendre quoi que ce soit d'utile sur une transmission d'information.

Appelons A et B les personnes qui veulent échanger un message secret et C l'espion. Si C veut intercepter les signaux envoyés par A, il doit effectuer une mesure sur ceux-ci et les perturber. Cette perturbation peut être évaluée par B et A, ce qui leur permet de détecter la présence de C et d'estimer la quantité d'informations qu'il a interceptés : moins la transmission entre A et B est bonne, plus le signal est perturbé, et plus C peut avoir d'informations sur ce qui a été transmis [1].

La cryptographie quantique est fondée sur l'utilisation de deux canaux : un canal quantique par lequel transitent des objets régis par les lois de la mécanique quantique (il s'agit en général d'une fibre optique par laquelle A envoie à B des impulsions lumineuses) et un canal classique que C peut écouter sans restriction, mais ne peut pas modifier. Des protocoles de cryptographie classiques permettent de réaliser un tel canal, authentifié de manière inconditionnellement sûre : A et B sont ainsi certains qu'ils se parlent bien l'un à l'autre. On ne peut pas empêcher C d'espionner le canal quantique, mais on peut savoir après la transmission s'il l'a fait. Il ne faut donc pas envoyer de message dans ce canal mais une suite d'éléments aléatoires, qui serviront ensuite à produire une clé s'ils n'ont pas été interceptés. Cette clé, parfaitement secrète, peut ensuite servir à chiffrer classiquement le message.

III. Rappels des propriétés quantiques d'un photon polarisé :

La plus petite unité quantique de lumière, le photon, peut être assimilée à un minuscule champ électrique oscillant. La direction de l'oscillation est la polarisation du photon. La lumière ordinaire est constituée de photons dont les polarisations sont diverses. En faisant passer cette lumière à travers un filtre polariseur, comme ceux que l'on trouve dans les lunettes de soleil, ou bien ***lame biréfringente*** seuls les photons dont la polarisation n'est pas orthogonale à celle du filtre poursuivent leur chemin. La probabilité de passage augmente avec l'alignement de la polarisation et du filtre et, à la sortie, la lumière est ré-polarisée par rapport au filtre.

Polarisation du photon :

Dans le domaine de la cryptographie quantique les directions de polarisations utilisées sont limitées à deux directions uniquement :

- **Polarisation rectiligne** : dans ce cas les photons sont polarisés selon deux directions orthogonales (soit en horizontal 0° ou soit en vertical 90°).
- **Polarisation diagonale** : dans ce cas les photons sont polarisés selon deux directions différentes mais orthogonales aussi (soit penché vers la droite 45°, ou soit penché cers la gauche -45° (135°)).

Polarisation rectiligne		
	Horizontale (0°)	Verticale (90°)
Polarisation diagonale		
	Penché à gauche (-45°)	Penché à droite (45°)

Polarisations de photons en cryptographie quantique [5]

Pour pouvoir mesurer efficacement la polarisation d'un photon (sa valeur) il faut utiliser un filtre orienté dans la même direction de polarisation du photon, sinon le résultat n'est quasiment pas sûr (il est probabiliste), et on ne peut plus mesurer le photon à nouveau (principe de Heisenberg : l'observation modifie l'expérience). C'est-à-dire :

- Si le photon est polarisé en rectiligne et qu'on utilise un filtre rectiligne on peut efficacement l'évaluer, par contre si on utilise un filtre diagonal avec le même photon le résultat ne peut être sûr que dans certains cas.
- Si le photon a une polarisation diagonale on ne peut l'évaluer qu'à travers un filtre diagonal, sinon aussi le résultat n'est pas sûr.

Ce principe est dû aux caractéristiques suivantes :

- Un photon peut traverser un filtre s'il est orienté dans la même direction (le même angle), mais il ne peut jamais traverser un filtre orthogonal.
- Si un photon traverse un filtre qui n'est pas orienté dans sa direction mais qu'il n'est pas orthogonal avec lui, il peut le traverser des fois mais avec une polarisation déformée.

Qubit

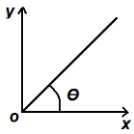
Dans l'information optique on parle de *qubit* au lieu de dire un bit. En effet un *qubit* est un bit (valeur 0 ou 1) codé sur un photon [4].

Comme cité précédemment un photon peut être polarisé selon différents angles, par convention on affecte :

- La valeur 0 à un photon polarisé en horizontal (0°, —) (suivant l'axe *Ox*) ;
- Et la valeur 1 à un photon polarisé en vertical (90°, |) (suivant l'axe *Oy*).

Cependant pour une polarisation selon un angle Θ différent de 0° et 90°, celle-ci est obtenue par superposition de deux photons l'un polarisé suivant Ox et l'autre suivant Oy.

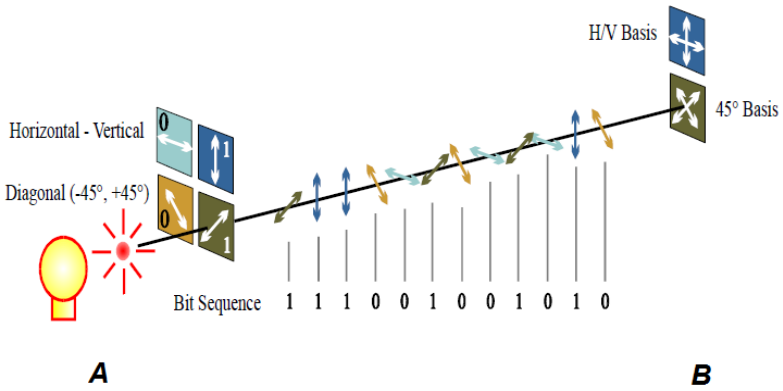
Un qubit est donc une entité beaucoup plus riche qu'un bit ordinaire, et il peut prendre théoriquement toutes les valeurs entre 0 et 1, mais pratiquement uniquement les valeurs 0 et 1 seront considérées.



Polarisation d'un photon

Pour cette raison un qubit est noté par : $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ avec $\alpha^2 + \beta^2 = 1$.

Par convention aussi on affecte la valeur 0 pour un photon polarisé en -45° et 1 à un photon polarisé suivant 45°. La figure ci-dessous récapitule l'ensemble de cette notation :



Valeurs du qubit selon la polarisation du photon [5]

En notation quantique lors de l'envoi d'un photon on choisit la polarisation :

- Polarisation rectiligne : horizontale notée $|0\rangle$ (ou —), et verticale notée $|1\rangle$ (ou |).
- Polarisation diagonale : à 45° notée $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ (ou /), et -45° notée $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ (ou \).

Pour recevoir (mesurer) un photon on utilise une base (filtre) :

- Polariseur H/V (**+**) noté **+** = $|0\rangle\langle 0|$ - $|1\rangle\langle 1|$.
- Polariseur à 45 (X) noté X = $|1\rangle\langle 0| + |0\rangle\langle 1|$.

IV. Cryptographie quantique pratique :

Le protocole de cryptographie quantique le plus connu est désigné par l'acronyme BB84, et a été proposé par C.H. Bennett et G. Brassard en 1984. Ce protocole a inspiré de nombreuses variantes, qui sont largement utilisées dans les systèmes opérationnels à l'heure actuelle, en employant des compteurs de photons pour détecter les signaux lumineux transmis. Une autre famille de protocoles, que l'on appelle «protocoles a variables continues », utilise des méthodes interférométriques, que l'on appelle détections homodynes ou hétérodynes.

Protocole BB84 :

Soient A et B deux entités qui veulent échanger des messages chiffrés. Ils disposent de deux canaux de transmission comme cité au début de ce chapitre : un canal optique pour l'échange de clés et un canal ordinaire pour le chiffrement et la communication ordinaire [3][4].

Lorsque A et B veulent échanger une clé secrète ils doivent procéder comme suit :

1) A doit transmettre une suite de bits codés en qubits, en choisissant la polarisation rectiligne (+) ou diagonale (X) pour chaque qubit.
2) B mesure (observe) chaque qubit à travers un filtre au hasard + ou bien X.
3) En utilisant le canal ordinaire A et B s'échangent la suite des bases de polarisation utilisée par chacun. Ainsi ils vont garder uniquement les qubits pour lesquels B avait choisi la bonne base de mesure et ils rejettent les autres.
4) Après la construction de la suite des bits pour lesquels ils étaient d'accord, les deux partenaires doivent consacrer une partie de cette liste (en les échangeant sur le canal ordinaire) pour s'assurer qu'ils n'étaient pas espionnés. Dans le cas où ils détectent la présence d'un espion, ils doivent bien sûr tout annuler et reprendre le processus à nouveau.

Explication :

Lorsque B est entrain de recevoir les qubits, il ne connait pas la base de polarisation utilisée par A pour chaque qubit, donc il doit choisir les bases au hasard. En général il va se tromper sur la moitié des qubits.

En échangeant la liste des bases de polarisation par la suite, ils vont détecter tous les deux les qubits qui ont été mal mesurés et ainsi vont les ignorer et garder uniquement ceux qui ont été bien mesurés pour servir comme clé secrète. En général B va se tromper sur environ 50% de ces choix, et donc ils vont garder l'autre moitié pour s'en servir.

Si un espion C est en écoute entre eux, il doit lui aussi choisir sa liste de bases de polarisation à utiliser, et vu qu'il ne connait ni la liste utilisée par A ni celle utilisée par B, son choix sera automatiquement différents des autres, et lui aussi va se tromper sur la moitié des qubits. Ainsi et vu que C s'interpose entre A et B, chaque qubit mal mesuré par C sera modifié (principe de Heisenberg) et va provoquer des erreurs supplémentaires pour B, et c'est pour cette raison que vienne l'étape 4 qu'est une étape de réconciliation et qui a pour objectif d'obtenir des chaines identiques en discutant

via un canal classique authentifié, tout en révélant le moins d'informations possible, au moyen de techniques apparentées aux codes correcteurs d'erreurs.

Exemple 1:

On suppose tout d'abord qu'il n y a aucun espion entre A et B, et que B se trompe sur la moitié de ses choix :

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Envoi	Bit	0	1	1	0	0	1	0	0	0	0	1	0	1	1	0	0	0	0	1	1	1	0	0
	$Base_1$	+	+	x	+	x	x	x	x	x	x	x	+	x	x	+	+	x	x	+	x	+	+	+
	Qubit	-	|	/	-	\	/	\	\	\	\	/	-	/	/	-	-	\	\	|	/	|	-	-
	$Base_2$	+	+	+	x	x	x	x	+	+	+	+	+	x	+	+	+	x	+	+	x	+	x	x
	Clé	0	1			0	1	0					0	1		0	0	0		1	1	1		
	K_A = 0 1 0 1 0 0 1 0 0 0 1 1 1																							
Réception	$Base_2$	+	+	+	x	x	x	x	+	+	+	+	+	x	+	+	+	x	+	+	x	+	x	x
	Mesure	-	|	|	/	\	/	\	-	|	-	-	-	/	|	-	-	\	-	|	/	|	\	/
	Bit	0	1	1	1	0	1	0	0	1	0	0	0	1	1	0	0	0	0	1	1	1	1	0
	$Base_1$	+	+	x	+	x	x	x	x	x	x	x	+	x	x	+	+	x	x	+	x	+	+	+
	Clé	0	1			0	1	0					0	1		0	0	0		1	1	1		
	K_B = 0 1 0 1 0 0 1 0 0 0 1 1 1																							

Par la suite B va envoyer une partie de sa clé K_B à A, il décide par exemple d'envoyer le 1er, le 5ème, le 8ème et le 10ème. A doit ainsi les comparer avec ceux de sa propres clé, s'ils sont les mêmes (comme c'est le cas dans cet exemple) cette partie de la clé sera éliminée et la clé devienne K = 101010111.

Exemple 2:

On suppose qu'il y a un espion C entre A et B, et que B et C se trompent sur la moitié de leurs choix :

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Envoi	Bit	0	1	1	0	0	1	0	0	0	0	1	0	1	1	0	0	0	0	1	1	1	0	0
	$Base_1$	+	+	x	+	x	x	x	x	x	x	x	+	x	x	+	+	x	x	+	x	+	+	+
	Qubit	-	|	/	-	\	/	\	\	\	\	/	-	/	/	-	-	\	\	|	/	|	-	-
	$Base_2$	+	+	+	x	x	x	x	+	+	+	+	+	x	+	+	+	x	+	+	x	+	x	x
	Clé	0	1			0	1	0					0	1		0	0	0		1	1	1		
	K_A = 0 1 0 1 0 0 1 0 0 0 1 1 1																							
Espion	$Base_3$	+	x	+	x	x	+	x	x	+	x	+	x	+	x	x	+	x	+	x	+	x	+	x
	Bit	0	0	1	0	0	1	0	0	1	0	1	1	1	1	0	0	0	1	0	0	0	0	0
	$Base_1$	+	+	x	+	x	x	x	x	x	x	x	+	x	x	+	+	x	x	+	x	+	+	+
	$Base_2$	+	+	+	x	x	x	x	+	+	+	+	+	x	+	+	+	x	+	+	x	+	x	x
	Clé	0	0			0	1	0					1	1		0	0	0		0	0	0		
	K_C = 0 0 0 1 0 1 1 0 0 0 0 0 0																							
Réception	$Base_2$	+	+	+	x	x	x	x	+	+	+	+	+	x	+	+	+	x	+	+	x	+	x	x
	Bit	0	1	1	1	0	1	0	0	1	0	0	1	1	1	0	0	0	0	0	0	0	1	0

$Base_1$	+	+	x	+	x	x	x	x	x	x	x	+	x	x	+	+	x	x	+	x	+	+	+
Clé	0	1			0	1	0					1	1		0	0	0		0	0	0		
$K_B = 010101100000 0 0$																							

La mesure de quelques qubits par B est influencée par l'existence de C en intermédiaire, et de ce fait et lors de la phase de conciliation A et B vont remarquer cette différence entre leurs clés $K_A = 010100100011 1$ et $K_B = 010101100000 0 0$ ce qui mène à penser qu'ils ont été espionnés.

Références :

[1] F. Grosshans F. Granger« La cryptographie quantique : l'incertitude quantique au service de la confidentialité» Université Paris-sud .

[2] Wikipedia- Principe d'incertitude de Heisenberg « https://fr.wikipedia.org/wiki/Principe_d%27incertitude ».

[3] Matthieu Bloch « Algorithme de réconciliation et méthodes de distribution quantique de clés adaptées au domaine fréquentiel » Université de Franche-Comté 2006.

[4] Manuel Sabban « Sécurité en cryptographie quantique utilisant la détection homodyne d'états cohérents à faible énergie » Télécom ParisTech, 2009.

[5] Blog d'Olivier Ezratty « Comprendre l'informatique quantique – cryptographie » accessible sur « https://www.oezratty.net/wordpress/2018/comprendre-informatique-quantique-cryptographie/ » Publié le 3 septembre 2018 et mis à jour le 27 septembre 2018.