UNIVERSITÉ SAVOIE MONT BLANC

Rapport INFO 002

Cryptographie quantique

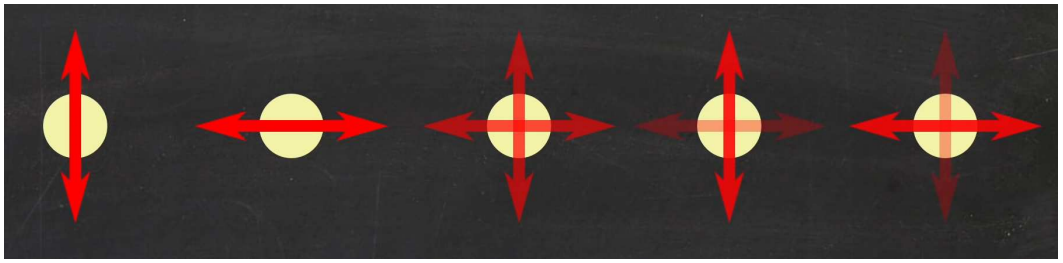
CHATEL Antoine, DEFLON Elodie

Sommaire

Définition

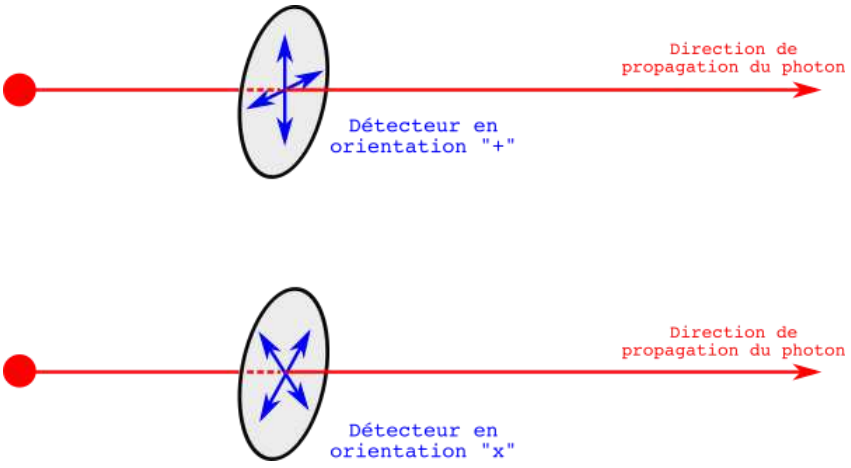
La cryptographie quantique consiste à utiliser les **propriétés de la physique quantique** pour établir des **protocoles de cryptographie**. Ils permettent d'atteindre des niveaux de sécurité qui sont inviolables à l'aide des méthodes classiques (non quantiques).

Pour comprendre le fonctionnement de la cryptographie quantique, il faut comprendre le principe de base de la physique quantique : le **principe de superposition**.
Si l'on prend une particule élémentaire comme un photon, il possède une propriété mesurable : sa **polarisation**. Elle peut être verticale, horizontale et avoir une orientation précise. Étant un objet quantique, le photon n'a pas une polarisation bien définie, il aura une superposition des différents états possibles.



De gauche à droite : polarisation verticale, horizontale et plusieurs superpositions possibles.

Lorsque l'on essaie de mesurer la polarisation d'un photon à un instant T, la mesure sera **aléatoire** : parfois horizontale, parfois verticale et l'orientation variera également.
Pour simplifier nos mesures dans nos exemples à venir, nous utiliserons 0 et 1 pour les axes "horizontal" et "vertical", et "+" et "x" pour les orientations possibles d'un photon.
Les mesures possibles seront donc : 0+, 1+, 0x et 1x, ce qui correspond à la polarisation selon chacun des axes.



En physique quantique, il y a un hasard qui se manifeste lorsque l'on essaie de mesurer les propriétés d'états superposés. Une fois la mesure effectuée, le photon perd sa superposition et se retrouve dans l'état mesuré : il s'agit de la projection ou réduction de l'état quantique.
Ces différentes spécificités de la physique quantique permettent, dans le cadre de l'informatique quantique, de savoir si un échange de message a été compromis.

Distribution quantique de clés

Il est possible de distribuer une clé de chiffrement secrète entre deux interlocuteurs distants en assurant la sécurité de la transmission grâce aux quelques **lois de la physique quantique**, que nous avons vu ci-dessus, et grâce à la **théorie de l'information**.
Cette clé secrète peut ensuite être utilisée dans un algorithme de chiffrement symétrique, afin de chiffrer et déchiffrer des données confidentielles.

La **théorie de l'information,** aussi appelée la théorie de l'information de Shannon, est une est une théorie visant à quantifier et qualifier la notion de contenu en information présent dans un ensemble de données.

Le tout premier protocole d'échange de clé quantique a été imaginé en 1984 par les cryptologues Charles Bennett et Gilles Brassard : le **protocole BB84**.
L'idée était de permettre l'échange sécurisé d'une clé de chiffrement de façon "quantique" pour ensuite chiffrer un message qui lui serait transmis sur un canal de communication classique.


Charles Bennett et Gilles Brassard

Pourquoi utiliser la cryptographie quantique ?

Aujourd'hui, nous utilisons différents algorithmes de cryptographie classiques pour **communiquer des données confidentielles** sur un canal de transmission (par exemple Internet). Dans ces algorithmes, nous retrouvons du chiffrement asymétrique, tel que RSA, ou du chiffrement symétrique (Triple DES, AES). Dans le cas du **chiffrement symétrique**, les deux interlocuteurs doivent posséder une **clé secrète**, c'est-à-dire qui ne soit connue que d'eux.

Un problème se pose : comment transmettre une clé de chiffrement entre deux interlocuteurs à distance, à la demande, et avec une sécurité démontrable ?
Actuellement, la technique répondant le mieux à cette problématique est une transmission physiquement sécurisée, de type **valise diplomatique**.

La cryptographie quantique cherche à répondre à ce problème en utilisant les lois de la physique quantique et la théorie de l'information pour **transmettre les données** entre les deux interlocuteurs tout en **détectant les intrusions**.
S'il n'y a pas eu d'espionnage, la clé non compromise peut alors être utilisée pour transmettre un message en toute sécurité.

Pourquoi ne pas transmettre directement le message ?

Selon les principes de la physique quantique, les **bits d'informations** communiqués par les mécanismes de la cryptographie quantique **ne peuvent être qu'aléatoires**. Ceci ne convient pas pour un message mais convient à une clé secrète qui doit être aléatoire.

Même si le mécanisme de la cryptographie quantique **garantit la détection de toute intrusion** dans la communication, il est possible que des bits d'informations soient interceptés par l'espion avant que celui-ci ne soit remarqué. Ceci n'est pas acceptable pour un message, mais sans importance pour une clé aléatoire, qui sera alors jetée en cas d'interception et remplacée par une nouvelle.

L’association avec le codage à masque jetable

En 1948, Claude Shannon montre qu’il est possible de démontrer formellement la sécurité d’un ensemble d’algorithmes de cryptographie. Parmi ces algorithmes, le plus simple est le codage à masque jetable ou aussi appelé chiffre de Vernam.

Cet algorithme consiste à combiner un message en clair avec une clé ayant des caractéristiques particulières notamment le fait qu’elle est à usage unique.
Combiné avec les techniques de cryptographie quantique, il est donc possible de démontrer la sécurité globale de la transmission d’un message confidentiel.

Un tel niveau de sécurité est nommé sécurité inconditionnelle car aucune hypothèse n’est faite sur les capacités physiques de l’espion, contrairement à la sécurité calculatoire des algorithmes de cryptographie classique qui prend en compte le réalisme des capacités de calcul de l’espion.

```
ZDXWWW EJKAWO FECIFE WSNZIP PXPKIY URMZHI JZTLBC YLGDYJ
HTSVTV RRYYEG EXNCGA GGQVRF FHZCIB EWLGGR BZXQDQ DGGIAK
YHJYEQ TDLCQT HZBSIZ IRZDYS RBYJFZ AIRCWI UCVXTW YKPQMK
CKHVEX VXYVCS WOGAAZ OUVVON GCNEVR LMBLYB SBDCDC PCGVJX
QXAUIP PXZQIJ JIUWYH COVWMJ UZOJHL DWHPER UBSRUJ HGAAPR
CRWVHI FRNTQW AJVWRT ACAKRD OZKIIB VIQGBK IJCWHF GTTSSE
EXFIPJ KICASQ IOUQTP ZSGXGH YTYCTI BAZSTN JKMFXI RERYWE
```

Exemple de codage à masque jetable

Exemple du protocole BB84

Imaginons deux personnes souhaitant communiquer de façon sécurisée, et ayant besoin de partager une clé de chiffrement. Appelons-les Alice et Bob pour suivre la tradition en vigueur.

Pour partager leurs clés, Alice envoie une série de photons à Bob. Pour chacun de ces photons, Alice va tirer au hasard à la fois une base (+ ou x) (l'une verticale/horizontale, et l'autre qui est tournée de 45° degrés) et un bit 0 ou 1 (va correspondre à la polarité du photon, horizontale ou verticale). Chaque photon aura alors un de ces 4 états : 0+, 1+, 0x ou 1x.

Base Alice	+	x	x	+	+	+	x	+	…
Bit émis	0	0	1	1	0	1	1	0	…
Etat quantique	0+	0x	1x	1+	0+	1+	1x	0+	…

Bob va recevoir ces photons et va mesurer la polarisation de chacun d'entre eux. Pour ce faire, il va devoir choisir une base de mesure. Il va donc pour chaque proton la tirer au hasard (+ ou x) et noter le résultat de sa mesure.

Pour un photon donné, si Bob a choisi la bonne base (c'est-à-dire la même qu'Alice), il obtiendra à coup sur le bon bit (0 ou 1) envoyé par Alice. En revanche, s'il a choisi l'autre base, il obtiendra 0 ou 1 à 50% de probabilité.

Base Alice	+	x	x	+	+	+	x	+	…
Bit émis	0	0	1	1	0	1	1	0	…
Etat quantique	0+	0x	1x	1+	0+	1+	1x	0+	…

Base Bob	+	+	x	+	x	x	x	+	…
Bit mesuré	0	0 ou 1	1	1	0 ou 1	0 ou 1	1	0	…

Une fois que la transmission des photons est réalisée, Alice et Bob communiquent publiquement (sans besoin de sécuriser leur canal) la liste des bases qu'ils ont utilisé pour chacun des photons. Ils jettent ensuite de leur liste tous les photons pour lesquels les bases sont différentes (la moitié en moyenne).
Pour les photons restants, ils ont utilisé la même base et donc ont la certitude d'avoir les mêmes bits : 0 ou 1. Cette série de bits va donc constituer la clé de chiffrement qui est donc maintenant connue des deux.

Pourquoi l'échange est sécurisé ?
Imaginons que Eve pirate la communication et essaie de mesurer l'état de polarisation des photons pour découvrir la clé. On va se concentrer sur les photons pour lesquels Alice et Bob ont choisi la même base (les autres seront écartés). Comme Bob, Eve doit choisir à chaque photon une base de mesure x ou +. Dans 50% des cas elle va tomber juste, cependant les 50% restants elle choisira une base différente de la base d'Alice et Bob.

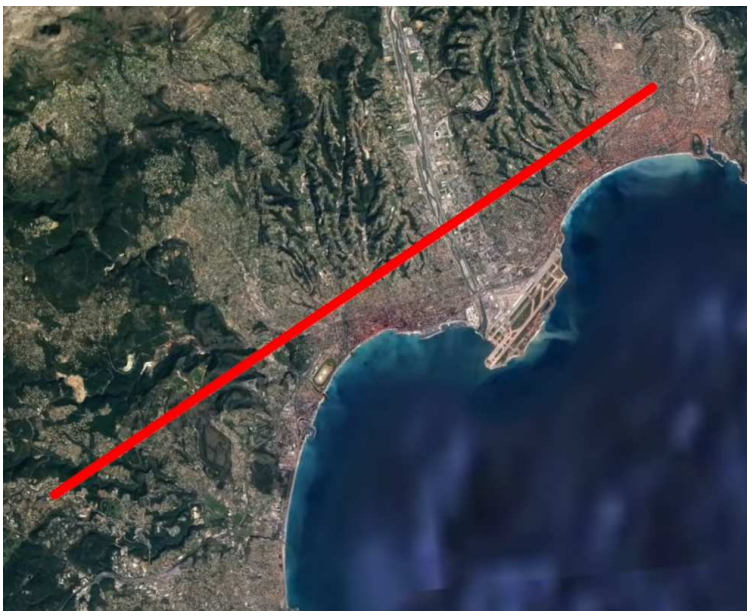
Imaginons un photon 0+ qu'Eve intercepte et mesure dans la base x. La mesure va le projeter dans l'état 0x ou 1x, et quand Bob mesurera à son tour dans la base +, il obtiendra 0 ou 1 à 50% de probabilité. S'il obtient 0 (ce qu'Alice avait envoyé), tout se passera comme si Eve n'avait pas été là, mais s'il obtient 1 il obtiendra un bit différent de ce qu'Alice avait envoyé alors que leurs bases sont pourtant identiques.

Voici donc comment détecter la présence d'Eve. Comme expliqué précédemment : Alice envoie ses photons, Bob les mesure, ils comparent publiquement leurs bases et ne conservent que les cas où les bases coïncident. Mais il n'en font pas tout de suite une clé : d'abord, ils décident de sacrifier une partie de ces photons pour vérifier qu'ils ne sont pas espionnés. Pour cela ils révèlent (publiquement) les bits qu'ils ont respectivement envoyé et mesuré, et qui en principe devraient coïncider complètement. Si Eve était à l'écoute au milieu de la ligne, environ 25% de ces bits devraient différer, du fait des projections quantiques opérées par les mesures. Si c'est le cas, Alice et Bob peuvent jeter leur clé et tenter de recommencer. Si ça n'est pas le cas, ils ont l'assurance que l'échange de clé n'aura pas été intercepté

Adaptation possible au réseau existant

Un des gros avantages d'utiliser des photons pour réaliser ce protocole d'échange de clés est que les photons sont de la lumière, ils peuvent donc voyager par de la fibre optique classique, celle que l'on utilise déjà sur certains réseaux d'Internet, en théorie.

En pratique, des instituts de recherche essaient aujourd'hui de concevoir des systèmes miniaturisés permettant de générer, manipuler et mesurer des photons dont l'état quantique est très bien contrôlé. Si les recherches aboutissent à un succès, les protocoles utilisant des photons pourraient être utilisés par les machines ayant accès à la fibre optique.



Exemple d'utilisation d'un système miniaturisé de 25 km entre Nice et Sophia-Antipolis

Conclusion

Nous avons vu les principes de la cryptologie quantique en se basant sur l'utilisation des photons, ses avantages et ses applications potentielles. Il existe d'autres protocoles que le BB84 que nous vous avons présenté, certains utilisent des états quantiques intriqués et seraient compliqués à expliquer brièvement, mais il existe donc de nombreuses possibilités pour crypter nos communications de manière quantique.
En continuant les recherches, les technologies développées par les instituts pourraient un jour nous fournir une sécurité renforcée pour nos communications à travers le monde.

Sources

https://fr.wikipedia.org/wiki/Cryptographie_quantique
https://fr.wikipedia.org/wiki/Théorie_de_l%27information
https://www.cea.fr/comprendre/Pages/nouvelles-technologies/essentiel-sur-ordinateur-quantique.aspx#:~:text=Le%20qubit%20à%20ions%20piégés%20correspond%20à%20des%20orientations%20magnétiques,ions%20excités%20par%20le%20laser.
https://www.techno-science.net/definition/6157.html
https://scienceetonnante.com/2019/02/14/bb84/