Joffrey Duc
Alexandre Moreau

Cryptographie et physique quantique

Introduction

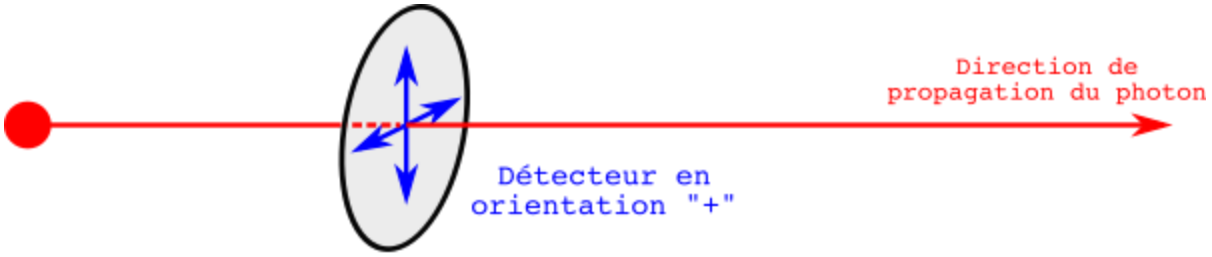
En cryptographie, il existe deux manières de chiffrer un message : il y a la manière symétrique et la manière asymétrique. En asymétrique, on dispose d'une clé publique destinée au chiffrement et d'une clé privée pour le déchiffrement de message, on peut ainsi partager la clé publique sans risque. En chiffrement symétrique c'est différent : on dispose d'une clé unique partagée entre des interlocuteurs pour chiffrer et déchiffrer des messages. Le problème dans cette méthode est que le partage de cette clé n'est pas garanti sans risque. On verra donc dans ce rapport comment on pourrait partager la clé de chiffrement / déchiffrement à des interlocuteurs de façon très sécurisée grâce à l'utilisation des lois de la physique quantique et du protocole BB84.

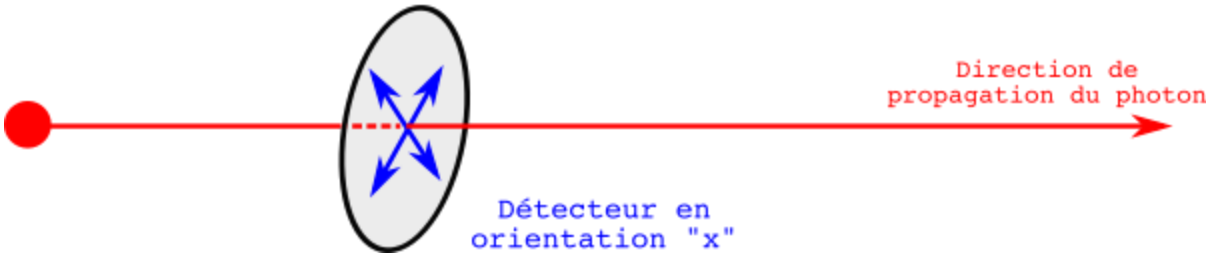
Le protocole BB84 est le tout premier protocole d'échange de clé quantique qui a été imaginé en 1984 par les cryptologues Charles Bennett et Gilles Brassard. L'idée de ce protocole est de permettre l'échange sécurisé d'une clé de chiffrement, clé qui pourra être ensuite utilisée pour chiffrer un message qui sera ensuite transmis sur un canal de communication classique. Il faut bien comprendre que ce n'est pas tout le message qui est transmis de façon quantique mais juste la clé de chiffrement.

La polarisation

En physique, quand on souhaite mesurer la polarisation d'un photon, on doit se fixer ce qu'on appelle une base de mesure, sous la forme de deux axes orthogonaux situés dans le plan perpendiculaire à la direction de propagation du photon (voir schéma ci-dessous). Une manière concrète de se le représenter, c'est d'imaginer un détecteur de polarisation à plat, placé perpendiculairement à la trajectoire du photon, et qui possède deux axes privilégiés, mais qu'on peut choisir de faire tourner.

Joffrey Duc
Alexandre Moreau





Il existe donc une infinité de choix de base de mesure. On va donc prendre deux bases possibles, l'une verticale / horizontale, et l'autre qui est tournée de 45° degrés. On va appeler ces bases respectivement « + » et « x ». De plus, on va remplacer axes « horizontal » et « vertical » par axes 0 et 1.

Quand un photon vient traverser un détecteur, la réponse de la mesure sera soit 0, soit 1, désignant ainsi un des axes de la base de mesure. La notion de 0 ou 1 est donc toujours relative à la base de mesure, qui est pour rappel soit en forme de « + » soit en forme de « x ». On va noter les 4 états avec lesquels on va traiter de la façon suivante : 0+, 1+, 0x et 1x, correspondant à la polarisation selon chacun des 4 axes.

			
0+	1+	0x	1x

Imaginons un photon 0+, c'est à dire d'état 0 de la base +. Si on le mesure dans la base + la réponse du détecteur sera forcément 0.

Maintenant si on prépare un photon dans l'état 0+ et qu'on le mesure dans la base x, on obtiendra aléatoirement les réponses 0 ou 1 à 50% de probabilité. Une autre façon de le dire, c'est que l'état « pur » 0+ est un état « superposé » 50% de 0x et 50% de 1x dans la base x.

La notion d'état « pur » (on dit en fait « état propre ») ou « superposé » n'est donc pas absolue comme j'ai pu le sous-entendre, mais toujours relative à la base de mesure.

Dernier ingrédient à préciser : la projection de l'état quantique. Si vous mesurez un photon 0+ dans la base x, vous obtiendrez soit 0, soit 1. Mais à la suite de cette mesure, la polarisation sera dans l'état pur correspondant de la base x. Par exemple si vous obtenez 1, la polarisation sera changée en 1x. Et donc si vous le re-mesurez dans la base +, vous trouverez 0 ou 1 à 50/50 (et le re-changerez en 0+ ou 1+).

Le protocole BB84

Le protocole BB84 est basé sur une communication de photons entre deux noeuds. La propriété de réduction du paquet d'onde le rend résistant à l'écoute, un observateur va modifier les données interceptées, ce qui sera détecté plus tard.

Le fonctionnement du protocole est le suivant :

1 - Envoi de photons

Base d'Alice	+	x	x	+	x	x	+	+
Bit envoyé	0	0	1	0	0	0	1	1
Etat quantique	0+	0x	1x	0+	0x	0x	1+	1+

Dans un premier temps, Alice choisit une liste de bases (x ou +) et une liste de bits. La combinaisons de base et de bit donne un état quantique de photon. Ces photons sont envoyés à Bob via un canal non sécurisé.

Joffrey Duc
Alexandre Moreau

2 - Mesure des photons

Base de Bob	+	+	x	x	x	+	+	+
Bit reçu	0	0|1	1	0|1	0	0|1	1	1

Bob choisit aléatoirement une base pour chaque photon et mesure le photon dans cette base. Si il a choisi la même base qu'Alice il retrouve le bit d'origine, sinon il a 50% de probabilité de détecter 0 ou 1. Après avoir mesuré tous les photons, il envoie la liste des bases choisies, mais pas les bits trouvés.

3 - Comparaison et suppression

Bases conservées	+		x		x		+	+
Bit conservé	0	-	1	-	0	-	1	1

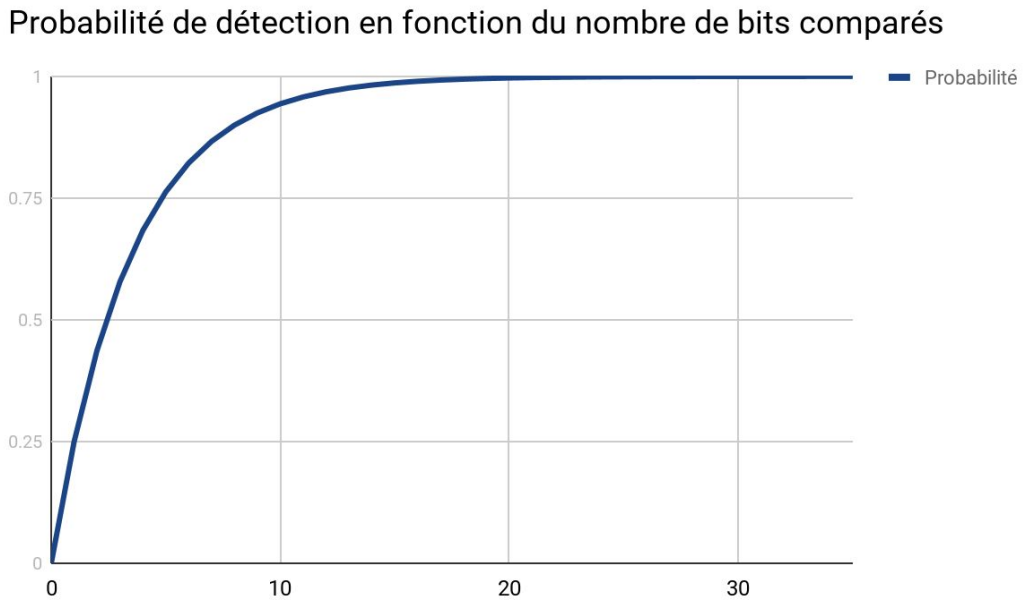
Alice compare les bases envoyées par Bob aux siennes. Elle lui envoie la liste des bases différentes, et les deux suppriment ces bases et les bits liés. Les bits restants sont en commun.

4 - Detection de suppression

Si Eve a essayé de mesurer les photons entre Alice et Bob, elle a 50% de probabilité d'avoir choisi une mauvaise base. Dans ce cas, elle obtient une mauvaise lecture du bit dans 50% des cas, ce qui a pour conséquence de modifier 1 photon sur 4 avant qu'il arrive à Bob. Une façon de détecter cette altération est de rendre publique un certain nombre de bits. Si Bob et Alice comparent un de leurs bits finaux, ils ont 25% de probabilité de détecter une écoute. Si les bits comparés ne sont pas tous égaux, la communication a été interceptée, et on doit recommencer l'échange de clé.

La probabilité augmente avec le nombre de bits comparés, avec une probabilité de $1-(3/4)^n$ où n est le nombre de bits rendus publics.

Nombre de bits comparés	Probabilité de détection
1	0,25
3	> 0,5
9	> 0,9
17	> 0,99
25	> 0,999
33	> 0,9999
41	> 0,99999



Conclusion

L’utilisation de la physique quantique pour la génération et l’échange de clé lors d’une cryptographie symétrique peut réellement renforcer la sécurité de la communication, car il y a quasiment 100% de chance de détecter si la clé a été interceptée ou non grâce au concept de la réduction du paquet d’ondes appliqué aux photons.

Cependant, même si on peut transporter les photons en utilisant la fibre optique, les technologies pour les envoyer et les détecter ne sont pas encore parfaites et encore moins grand public : il est plus facile de créer un paquet de photon qu’un photon unique, et les détecteurs de photons ne sont pas parfaits : du bruit électromagnétique ou des erreurs de mesure peuvent causer de mauvais résultats, même en l’absence d’une personne qui intercepte la communication.

C’est sur ces questions que travaillent les chercheurs de l'équipe PIQ (Photonique & Information Quantique) de l'institut de physique de Nice. Ils réalisent et étudient les systèmes miniaturisés qui permettent de générer, manipuler et mesurer des photons dont l'état quantique est très bien contrôlé. En ce moment (novembre 2019), cette équipe travaille sur une expérience ambitieuse visant à réaliser une communication sécurisée par fibre optique entre Nice et Sophia Antipolis sur une distance de 25 km. Et les technologies qui seront développées pourraient un jour assurer une sécurité renforcée de toutes nos communications chiffrées sur des distances beaucoup plus grandes.

Bibliographie

https://fr.wikipedia.org/wiki/Protocole_BB84
https://fr.wikipedia.org/wiki/Cryptographie_sym%C3%A9trique
http://physique.unice.fr/sem6/2014-2015/PagesWeb/PT/Tomographie/?page=bb84
https://www.futura-sciences.com/sciences/definitions/physique-photon-3500/
https://inphyni.cnrs.fr/sites/teams/quantum-photonics-and-information/