Cryptographie quantique

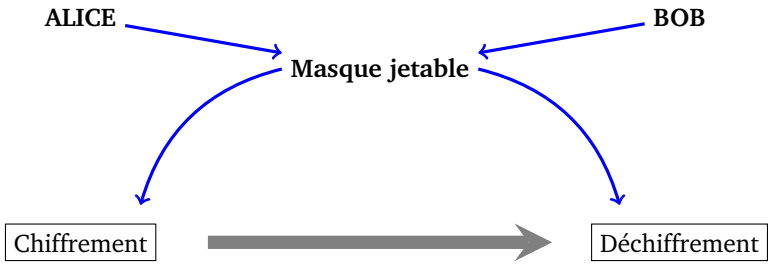
Vidéo ■ partie 16. Cryptographie quantique

Nous étudions le protocole BB84 qui permet le partage d'un secret commun entre deux personnes grâce à la physique quantique.

1. Le chiffrement parfait existe

Commençons par comprendre qu'un secret commun entre deux personnes permet une communication parfaitement sûre. C'est d'ailleurs ce protocole qui était utilisé par le « téléphone rouge » reliant les USA et l'URSS pendant la guerre froide.

1.1. Masque jetable



- Alice veut envoyer un message à Bob. Ce message est composé de 0 et de 1 (par exemple pour un nombre, on utiliserait son écriture binaire : 14 serait codé 1.1.1.0 ; pour une lettre on utiliserait le code ASCII : « A » serait codé 1.0.0.0.0.0.1).
  Exemple : le message est $x = 1.0.1.1.0.1.1$.
- Alice et Bob s'étaient au préalable partagé un « masque jetable », qui est une suite secrète et aléatoire de 0 et de 1.
  Exemple : le masque est $m = 0.0.1.0.1.1.1$.

$$x \xrightarrow[\text{chiffrement } y = x \oplus m]{\text{Alice}} y \xrightarrow[\text{transmission}]{} y \xrightarrow[\text{déchiffrement } x = y \oplus m]{\text{Bob}} x$$

- Alice envoie le message chiffré y obtenu par addition bit à bit (sans retenue) $y = x \oplus m$ (c'est un « ou exclusif » bit à bit).

$$\begin{array}{rr} & 1.0.1.1.0.1.1 \\ \oplus & 0.0.1.0.1.1.1 \\ \hline & 1.0.0.1.1.0.0 \end{array}$$

Exemple : $y = x \oplus m = 1.0.0.1.1.0.0$.

- Bob déchiffre le message en ajoutant de nouveau le masque m à y : il obtient x. En effet $y \oplus m = x \oplus m \oplus m = x$ (car $0 \oplus 0 = 0$ et $1 \oplus 1 = 0$).
  Exemple : $y \oplus m = 1.0.1.1.0.1.1 = x$.

$$\begin{array}{rr} & 1.0.0.1.1.0.0 \\ \oplus & 0.0.1.0.1.1.1 \\ \hline & 1.0.1.1.0.1.1 \end{array}$$

Voici les conditions que doit respecter le masque jetable m :

- il doit être un choix aléatoire,
- il doit rester secret,
- il doit être de la même longueur que le message,
- il ne doit servir qu'une seule fois.

1.2. Avantages et inconvénients

Avantages. Ce chiffrement est parfaitement sûr : un espion qui intercepterait le message chiffré y sans connaître le masque jetable m ne serait pas capable ici de décrypter le message. En effet, un 0 du message y peut correspondre aussi bien à 0 ou 1 du message original, de même pour un 1.

	$m = 0$	$m = 1$
$x = 0$	0	1
$x = 1$	1	0

Un espion n'a pas de meilleure méthode que de deviner au hasard si le message original contenait 0 ou 1. Si le message est de longueur n alors la probabilité qu'il décrypte le message complet est $\frac{1}{2^n}$ (ce qui revient à tirer au hasard un message parmi les 2^n messages possibles).

Inconvénients.
Tout d'abord il faut respecter scrupuleusement les consignes pour l'utilisation du masque jetable (choix aléatoire, usage unique,...). Une difficulté réside dans le fait qu'il faut que le masque reste un secret uniquement connu d'Alice et Bob : la méthode la plus simple est qu'Alice et Bob puissent se rencontrer physiquement pour déterminer ensemble le masque jetable. Pour le « téléphone rouge », les masques jetables étaient des listes de nombres transmis régulièrement via une valise diplomatique. Cet échange de masque est un problème pratique majeur puisqu'il nécessite une rencontre entre Alice et Bob. C'est pourquoi d'autres protocoles cryptographiques sont utilisés, comme par exemple RSA, pour permettre des communications chiffrées sans aucune rencontre physique, mais ils ne sont pas parfaitement sûrs.

2. BB84 : un secret commun

Nous présentons maintenant le protocole BB84 (dû à Bennett et Brassard en 1984) qui n'est pas vraiment un protocole cryptographique mais qui permet la création d'un secret commun sous la forme d'une suite de 0 et de 1. Cette suite peut ensuite, par exemple, être utilisée comme masque jetable pour un chiffrement parfait. Ce secret commun peut se construire à distance et on peut être sûr avec une forte probabilité que personne n'a intercepté le secret.

2.1. Deux bases

Alice souhaite envoyer à Bob une information 0 ou 1. Pour réaliser cela, elle va lui envoyer un qubit. Elle a le choix de deux codages différents.

Première base d'envoi « ⊕ ».
Dans cette base deux qubits sont possibles : $|\uparrow\rangle$ et $|\rightarrow\rangle$.
- $|\uparrow\rangle = |0\rangle$ représente l'information 0,
- $|\rightarrow\rangle = |1\rangle$ représente l'information 1.

Seconde base d'envoi « ⊗ ».
Dans cette base deux qubits sont possibles : $|\nearrow\rangle$ et $|\searrow\rangle$.
- $|\nearrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ représente l'information 0,
- $|\searrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ représente l'information 1.

D'un point de vue physique ces qubits correspondent à des polarisations de photons : la polarisation à 90° pour la base « ⊕ » et la polarisation à 45° pour la base « ⊗ ». Selon le choix de base et selon l'information 0/1, Alice envoie un des quatre qubits $|\uparrow\rangle$, $|\rightarrow\rangle$, $|\nearrow\rangle$, $|\searrow\rangle$.

On retrouve aussi ces deux mêmes bases lors de la réception qui correspond à une mesure.

Première base de mesure « ⊕ ».
Voici l'information que Bob obtient lorsqu'il mesure le qubit reçu dans la base « ⊕ ».

qubit	$\|\uparrow\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$	$\|\searrow\rangle$
information	0	1	0 ou 1 (50% chaque)	0 ou 1 (50% chaque)

Seconde base de mesure « ⊗ ».
Voici l'information que Bob obtient lorsqu'il mesure le qubit reçu dans la base « ⊗ ».

qubit	$\|\uparrow\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$	$\|\searrow\rangle$
information	0 ou 1 (50% chaque)	0 ou 1 (50% chaque)	0	1

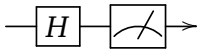
Conclusion. Si Bob effectue la mesure dans la même base que celle d'envoi alors il obtient exactement l'information 0 ou 1 envoyée par Alice. Par contre s'il mesure dans l'autre base que celle d'envoi, il obtient alors un bit 0 ou 1 aléatoire qui n'a rien à voir avec l'information envoyée par Alice.

Circuits quantiques
Base « ⊕ ». Pour l'envoi il n'y a rien à faire, le qubit est $|0\rangle$ ou $|1\rangle$. Pour la réception, il s'agit juste d'une mesure classique :

On retrouve bien que, par exemple, $|\nearrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ se mesure en 0 ou 1 avec chacun une probabilité $\frac{1}{2}$.

Base « ⊗ ». Pour l'envoi, l'information 0 est codée par $H|0\rangle = |\nearrow\rangle$ et l'information 1 est codée par $H|1\rangle = |\searrow\rangle$. Donc une porte H de Hadamard suffit.

Pour la réception, le circuit est composé d'une porte H suivi d'une mesure :



Par exemple si le qubit reçu est $|\searrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, alors la porte de Hadamard l'envoie sur $|1\rangle$ qui se mesure en 1. (On pourrait aussi utiliser que $H \circ H|\psi\rangle = |\psi\rangle$.)

2.2. Protocole

Voici le protocole de partage d'un secret commun.

1. Alice – envoi.

- Alice choisit des bits 0 ou 1 au hasard.
- Par chaque bit, elle choisit au hasard une base d'envoi $\oplus$ ou $\otimes$.
- Pour chaque bit, elle a donc quatre situations et elle envoie le qubit correspondant :

bit/base	$(0,\oplus)$	$(1,\oplus)$	$(0,\otimes)$	$(1,\otimes)$
qubit	$\lvert\uparrow\rangle$	$\lvert\rightarrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\searrow\rangle$

2. Bob – réception.

- Bob reçoit une liste de qubits.
- Pour chaque qubit il choisit au hasard une base de mesure $\oplus$ ou $\otimes$.
- Bob mesure chaque qubit reçu parmi $\lvert\uparrow\rangle$, $\lvert\rightarrow\rangle$, $\lvert\nearrow\rangle$, $\lvert\searrow\rangle$ dans la base choisie $\oplus$ ou $\otimes$.

3. Alice & Bob – mise en commun.

- Alice et Bob établissent la liste de leurs bases identiques (les deux ont choisi $\oplus$ ou les deux ont choisi $\otimes$). Cette discussion peut être publique.
- Alice et Bob ne conservent que les rangs où les choix de base sont identiques. Les autres sont oubliés.
- Alice ne conserve que les bits correspondant à ces rangs.
- Pour chacun de ces rangs, Bob mesure dans la base (commune) et obtient le même bit qu'Alice.

2.3. Exemple

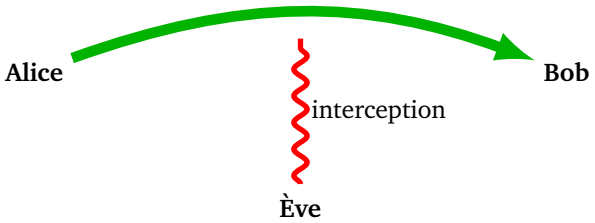
Voici un exemple. À vous de terminer de compléter ce tableau.

Alice bit	1	0	0	1	1	1	0	1	0
Alice base	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$
Qubit	$\lvert\rightarrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\uparrow\rangle$	$\lvert\searrow\rangle$	$\lvert\searrow\rangle$				
Bob base	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$
Base commune ?	oui	non	oui	oui	non				
Bit commun	1		0	1					

Le message commun est 1.0.1…

2.4. Sûreté

Pour l'instant Alice et Bob partagent un message commun. Mais celui-ci est-il secret ? Il faut s'assurer que le message n'a pas été intercepté ou modifié en cours de transmission.



La sécurité repose sur le théorème de non clonage quantique (voir le chapitre « Portes quantiques »). Ève ne peut pas lire un qubit puis le renvoyer à Bob. En effet, toute mesure modifie irrémédiablement le qubit.

Expliquons sur un exemple : Alice envoie l'information 0 dans la base $\otimes$, c'est-à-dire qu'elle transmet le qubit $\lvert\nearrow\rangle$. Ève doit choisir une base pour sa lecture (car elle ne connaît pas la base d'envoi d'Alice).

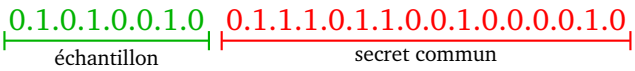
- Si elle choisit la base $\otimes$, alors la mesure de $\lvert\nearrow\rangle$ donne toujours 0, son interception est réussie ;

- si elle choisit la base $\oplus$, alors la mesure de $|\nearrow\rangle$ donne 0 (avec probabilité $\frac{1}{2}$, interception réussie) ou 1 (avec probabilité $\frac{1}{2}$, interception ratée).

Ève ne sait pas si elle a choisi la bonne base. Si elle a choisi la bonne base alors elle pourrait renvoyer le bon qubit à Bob. Mais si elle a choisi la mauvaise base elle va renvoyer $|\uparrow\rangle$ ou $|\rightarrow\rangle$ à Bob. Lorsque Bob va vérifier avec Alice qu'il a la bonne base, alors la lecture de $|\uparrow\rangle$ ou $|\rightarrow\rangle$ dans la base $\otimes$ va donner 0 ou 1, et le bit sera faux dans la moitié des cas.
Bilan : Ève obtient la bonne information 0/1 dans les $\frac{3}{4}$ des cas (mais sans savoir quand c'est bon ou mauvais). Mais surtout si Ève intervient lors de la transmission, alors Bob obtient un mauvais bit d'information avec une probabilité $\frac{1}{4}$ (parmi les bits du message commun).

Voici donc la fin du protocole.
4. Alice & Bob – vérification de la sécurité.

- Alice et Bob se communiquent publiquement un échantillon de n bits du message commun (par exemple les n premiers bits).
- Si les échantillons ne sont pas exactement les mêmes alors un espion est intervenu, l'ensemble du message est compromis et il faut tout recommencer.
- Si les échantillons sont exactement identiques, alors la transmission est considérée comme sûre (d'autant plus sûre que n est grand). Le reste du message constitue alors le secret commun.



Détaillons les calculs de la sécurité de la transmission.

- Si aucun espion intervient, alors les échantillons d'Alice et Bob sont toujours identiques (probabilité 1, quelle que soit la taille n de l'échantillon).
- Si un espion intervient entre Alice et Bob alors, pour chaque bit, la probabilité qu'il parvienne correctement à Bob est de $\frac{3}{4}$. Donc les échantillons de n bits d'Alice et Bob sont complètement identiques avec probabilité $\left(\frac{3}{4}\right)^n$. Si n est assez grand, alors cette probabilité est presque nulle. Ce qui signifie qu'on détecte presque sûrement la présence d'un espion.
- Voici des exemples :
  — $n = 10$: $\left(\frac{3}{4}\right)^{10} = 0.0563$, donc dans environ 95% des cas l'espion est repéré,
  — $n = 20$: $\left(\frac{3}{4}\right)^{20} = 0.003\ldots$ donc dans 99.7% des cas l'espion est repéré,
  — $n = 100$: $\left(\frac{3}{4}\right)^{100} \simeq 3 \cdot 10^{-13}$ donc l'espion est repéré sauf 1 fois sur 1 000 000 000 000.

Bilan.

- Alice et Bob partagent un secret commun,
- ils sont raisonnablement certains de ne pas avoir été espionnés,
- ce secret commun peut servir de masque jetable pour une communication chiffrée.

3. Alice et Bob divorcent : qui garde le chien ?

Alice et Bob ne se font plus confiance, et ils doivent décider par téléphone qui garde le chien. L'un pourrait tirer à pile ou face et annoncer le résultat à l'autre mais chacun pense que l'autre peut tricher. Comment faire ?
Nous allons voir la simulation d'un tirage à pile ou face à distance dans le monde quantique. Voici le protocole expliqué simplement : Alice et Bob tirent chacun de leur côté une pièce à pile ou face. S'ils obtiennent tous les deux « pile » ou tous les deux « face » c'est Bob qui gagne, sinon c'est Alice. Le point crucial est de se débrouiller pour qu'aucun des deux ne puisse mentir en annonçant son résultat.

3.1. Protocole

1. Alice choisit une base d'envoi ⊕ ou ⊗.

- Alice décide au hasard d'une base d'envoi ⊕ ou ⊗ (c'est son tirage à pile ou face).
- Elle envoie une série aléatoire de bits, par exemple 0.0.1.0.1.1.
- Elle envoie les qubits correspondant dans la base qu'elle a choisie. Par exemple :
  — si elle a choisi la base ⊕ : $|\uparrow\rangle$, $|\uparrow\rangle$, $|\rightarrow\rangle$, $|\uparrow\rangle$, $|\rightarrow\rangle$, $|\rightarrow\rangle$,
  — si elle a choisi la base ⊗ : $|\nearrow\rangle$, $|\nearrow\rangle$, $|\searrow\rangle$, $|\nearrow\rangle$, $|\searrow\rangle$, $|\searrow\rangle$.

2. Bob choisit une base de mesure ⊕ ou ⊗.

- Bod décide au hasard d'une base de mesure ⊕ ou ⊗ (c'est son tirage à pile ou face).
- Il effectue la mesure des qubit reçus dans la base qu'il a choisie.
- Il obtient une suite de mesures 0 ou 1.

3. Bob annonce la base qu'il a choisie pour la mesure.

4. Alice dévoile la base qu'elle avait choisie pour l'envoi ainsi que les bits transmis.

5. Gagnant : si les deux bases coïncident Bob a gagné, sinon c'est Alice.

6. Vérification : Bob vérifie qu'Alice n'a pas menti. Bob a annoncé son choix avant Alice il doit donc vérifier qu'Alice n'a pas triché, pour cela il compare sa mesure avec les bits d'Alice :

- s'il a trouvé la bonne base, alors sa mesure est exactement la même que les bits d'Alice,
- s'il n'a pas trouvé la bonne base, alors il doit avoir en moyenne la moitié des bits corrects et la moitié des bits faux.

Il sait donc s'il a trouvé la bonne base ou pas. Plus de détails sur la vérification sont donnés ci-dessous.

3.2. Vérifications

Tout d'abord Bob ne peut pas tricher, d'une part les mesures qu'il effectue ne permettent pas de déduire quelle base d'envoi Alice avait choisie et d'autre part Bob annonce en premier sa base à Alice.
Voyons comment Bob vérifie le résultat annoncé par Alice.
Imaginons qu'Alice ait choisi la base ⊕ et les bits 0.0.1.0.1.1 elle transmet donc les qubits $|\uparrow\rangle$, $|\uparrow\rangle$, $|\rightarrow\rangle$, $|\uparrow\rangle$, $|\rightarrow\rangle$, $|\rightarrow\rangle$.
Si Bob a choisi de mesurer les qubits dans la même base ⊕ alors il va obtenir après mesure la même suite de bits 0.0.1.0.1.1. Donc dans le cas où il gagne les bits d'Alice et de Bob sont identiques.
Si Bob a choisi l'autre base, ici ⊗, alors la mesure de $|\uparrow\rangle$, $|\rightarrow\rangle$, conduit à 0 ou 1 aléatoirement. Il va donc, en moyenne, avoir la moitié de bits faux et l'autre moitié corrects. La probabilité que les n bits de Bob coïncident exactement avec les n bits d'Alice est $\frac{1}{2^n}$ et est donc très faible (si n est assez grand).
Bilan : Bob sait s'il a choisi la même base qu'Alice juste en comparant les bits mesurés avec les bits annoncés par Alice.
Par contre, Alice pourrait essayer de tricher : si Bob choisit la base ⊕, elle pourrait mentir pour faire perdre Bob et dire « J'avais choisi la base ⊗ » ou inversement. Mais dans ce cas, elle va être démasquée car elle a déjà envoyé les qubits qui ont déjà été mesurés pars Bob et ne peut donc plus rien modifier. Or, comme on l'a déjà vu, la mesure des qubits $|\uparrow\rangle$, $|\uparrow\rangle$, $|\rightarrow\rangle$, $|\uparrow\rangle$, $|\rightarrow\rangle$, $|\rightarrow\rangle$ dans la base ⊗ a très peu de chance de donner exactement 0.0.1.0.1.1.

La cryptographie quantique n'en est encore qu'à ces débuts, c'est tout un domaine à découvrir !