Informatique quantique IFT6155

Distribution quantique de clef privée QKD

Motivation

Nous avons vu qu'il existe une technique cryptographique parfaite permettant à deux participants de communiquer secrètement un message de n bits s'ils partagent une clef secrète de n bits.

Nous avons aussi vu que cette technique est optimale.

Comment deux participants qui ne partagent pas de clef secrète peuvent-ils échanger un message secret?

Nous avons vu le protocole RSA qui permet de régler le problème mais ce protocole n'est plus sécuritaire advenant la réalisation de l'ordinateur quantique.

Pourquoi ne pas faire un échange de clef quantique?

Théorème fondamental

Toute acquisition d'information sur un état quantique inconnu perturbe l'état. L'ampleur de la perturbation est proportionnelle à la quantité d'information qui est extraite.

BB84

Alice et Bob ont accès à un canal quantique. Ève a accès au canal et peut espionner le canal. Elle peut faire n'importe quelle opération consistante avec la mécanique quantique sur les qubits qui sont échangés entre Alice et Bob. En particulier elle peut les mesurer.

Alice et Bob ont accès à un canal classique authentique. Ève peut espionner toutes les communications entre Alice et Bob mais Ève ne peut transmettre des messages à la place d'Alice ou de Bob.

Alice et Bob ne partagent pas de clef secrète et désirent obtenir un bit secret de telle façon qu'Ève ne possédera pratiquement aucune information à son sujet. Plus formellement, si X est la variable aléatoire décrivant l'information d'Ève sur le bit secret alors $H(X) \geq 1 - \frac{1}{2^{p(n)}}$.

BB84

Nous allons voir une version simplifiée du protocole permettant la génération d'un bit de clef secrète. Nous utilisons le codage suivant.

$$|0\rangle_0 = |0\rangle \quad |1\rangle_0 = |1\rangle \quad |0\rangle_1 = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad |1\rangle_1 = H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Protocole BB84
Alice choisit $x \in_R \{0,1\}^n$ et $b \in_R \{0,1\}^n$.
Bob choisit $c \in_R \{0,1\}^n$.
Pour i de 1 à n:
    Alice transmet à Bob $|\psi_i\rangle = |x_i\rangle_{b_i}$.
    Si $c_i = 0$ Bob mesure $y_i = M(|\psi_i\rangle)$.
    Si $c_i = 1$ Bob mesure $y_i = M(H|\psi_i\rangle)$.
Bob transmet c à Alice.
Alice transmet b à Bob.
Pour i de 1 à n si $b_i \neq c_i$ Alice transmet x_i à Bob qui remplace $y_i = x_i$.
Pour i de 1 à $n/4$:
    Alice choisit $z \in \{0,1\}^n$ et transmet z et $x \cdot z$ à Bob.
    Bob vérifie que $y \cdot z = x \cdot z$ sinon le protocole avorte.
Alice calcule $s = x \cdot 111\ldots1$.
Bob calcule $s' = y \cdot 111\ldots1$.

BB84

Alice			Bob	
x	b	$\|\psi_i\rangle$	c	y
1	0	$\|1\rangle$	0	$M(\|1\rangle) = 1$
0	1	$H\|0\rangle$	0	$M(H\|0\rangle) = 1$
1	1	$H\|1\rangle$	1	$M(HH\|1\rangle) = 1$
0	0	$\|0\rangle$	1	$M(H\|1\rangle) = 0$
1	0	$\|1\rangle$	0	$M(\|1\rangle) = 1$
0	1	$H\|0\rangle$	1	$M(HH\|0\rangle) = 0$

BB84

Lemme
Si Ève ne possède aucune information sur un des x_i alors Ève ne possède aucune information sur s.

Preuve
Supposons que Ève connaît tous les x sauf pour la position x_i pour laquelle elle ne possède *aucune* information. Clairement,

$$s = x \cdot 111\ldots1 = x_1 \oplus x_2 \oplus \cdots \oplus x_n = a \oplus x_i$$

mais Ève ne connaît pas x_i et x_i est uniformément distribué. Cela signifie que du point de vue d'Ève, $s = b$ avec probabilité $1/2$ et $s = b \oplus 1$ avec probabilité $1/2$. Peu importe la valeur de b, du point de vue d'Ève $s = 0$ ou 1 avec probabilité $1/2$.

Ève doit donc apprendre de l'information sur *tous* les x_i.

Si Ève est passive

Après l'envoi et la mesure, mais avant la réconciliation, on a que

$$b_i = c_i \quad \Rightarrow \quad y_i = x_i$$

$$b_i \neq c_i \quad \Rightarrow \quad P(y_i \neq x_i) = 1/2$$

Si Ève est passive, après la réconciliation nous avons que $x = y$ et donc la vérification de consistance va fonctionner et

$$s = x \cdot 111\ldots1 = y \cdot 111\ldots1 = s'$$

qui est le bit partagé par Alice et Bob.

Clairement, ce bit est secret puisqu'Ève ignore à peu près la moitié des bits des positions de x et donc elle n'a aucune information sur $x \cdot 111\ldots1$.

Si Ève est active

Premièrement, il est clair que Ève peut bloquer le canal quantique entre Alice et Bob et empêcher la réalisation de l'échange de clef.

Son objectif est d'apprendre s sans être détectée. Pour obtenir s avec certitude, Ève doit apprendre $x \cdot 111\ldots1$ et donc Ève doit apprendre x.

Notez qu'Ève apprend à peu près la moitié des positions lors de la réconciliation.

Si Ève est active

Lemme
Si Ève perturbe l'état de telle sorte que si $b_i = c_i$ alors $P(x_i = y_i) = 1 - \epsilon$ elle sera détectée avec probabilité

$$(1 - (1 - \epsilon)^{n/2})(1 - \frac{1}{2^{n/4}})$$

et en particulier, pour avoir une probabilité constante de passer le test, ϵ doit être exponentiellement petit en n.

Preuve
Il y a à peu près $n/2$ positions pour lesquelles $b_i = c_i$. Pour chacune de ces positions $P(x_i = y_i) = 1 - \epsilon$. La probabilité qu'au moins une position soit incorrecte est de $1 - (1 - \epsilon)^{n/2}$. Dans ce cas, nous avons vu que si $x \neq y$ alors la probabilité que $x \cdot z = y \cdot z$ est de $1/2$. La probabilité que les $n/4$ tests réussissent est de $\frac{1}{2^{n/4}}$. La probabilité qu'Ève soit détectée est donc

$$(1 - (1 - \epsilon)^{n/2})(1 - \frac{1}{2^{n/4}})$$

Une attaque simple

Ève garde le qubit envoyé par Alice et envoie un autre état à Bob. De cette façon, elle pourra mesurer les $|\psi_i\rangle$ après avoir appris la base et donc elle apprendra x au complet.

Le problème est qu'elle doit transmettre quelque chose à Bob en attendant. Elle n'a à ce moment aucune information sur le bit ni sur la base. De son point de vue, l'état est $S = \{(1/4, |0\rangle), (1/4, |1\rangle), (1/4, |0\rangle), (1/4, H|0\rangle), (1/4, H|1\rangle))\}$ et donc $\rho_s = \frac{1}{2}I$.

Supposons qu'Ève transmet l'état $\alpha|0\rangle + \beta|1\rangle$ et qu'Alice et Bob choisissent la même base. Il y a quatre cas (notez que $H(\alpha|0\rangle + \beta|1\rangle = (\frac{\alpha+\beta}{\sqrt{2}})|0\rangle + \frac{(\alpha-\beta)}{\sqrt{2}}|1\rangle)$:
$x = 0$ et $b = c = 0$, Bob obtient le bon bit avec probabilité $|\alpha|^2$,
$x = 1$ et $b = c = 0$, Bob obtient le bon bit avec probabilité $|\beta|^2$,
$x = 0$ et $b = c = 1$, Bob obtient le bon bit avec probabilité $|\frac{\alpha+\beta}{\sqrt{2}}|^2$,
$x = 1$ et $b = c = 1$, Bob obtient le bon bit avec probabilité $|\frac{\alpha-\beta}{\sqrt{2}}|^2$,
On obtient qu'en moyenne Bob aura le bon bit avec probabilité

$$\frac{1}{4}(|\alpha|^2 + |\beta|^2 + |\frac{\alpha+\beta}{\sqrt{2}}|^2 + |\frac{\alpha-\beta}{\sqrt{2}}|^2) = \frac{1}{4}(1+1) = \frac{1}{2}$$

Le taux d'erreur (ϵ) est donc de 1/2 et Ève sera très certainement détectée.

Une autre attaque

Plutôt que de garder l'état sans le mesurer, Ève peut essayer d'obtenir de l'information immédiatement sur le bit. Pour à la fois apprendre de l'information sur x_i et donner à Bob un état qui donne plus de chance de succès pour le test.

La base b_i

Ève peut-elle apprendre de l'information sur la Base b_i utilisée par Alice?

De son point de vue, comme le bit x_i est aléatoire et uniformément distribué, $b = 0$ se manifeste par

$$\frac{1}{2}|0\rangle_0 \langle 0|_0 + \frac{1}{2}|1\rangle_0 \langle 1|_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

et $b = 1$ se manifeste par

$$\frac{1}{2}|0\rangle_1 \langle 0|_1 + \frac{1}{2}|1\rangle_1 \langle 1|_1 = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} + \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

. Comme les deux matrices de densité sont identiques, aucune information n'est accessible à Ève sur la base avant qu'elle ne soit annoncée.

Le bit x_i

Ève peut-elle apprendre de l'information sur le bit x_i même si elle ignore la base b_i?

De son point de vue, comme la base est aléatoire et uniformément distribuée, $x = 0$ se manifeste par

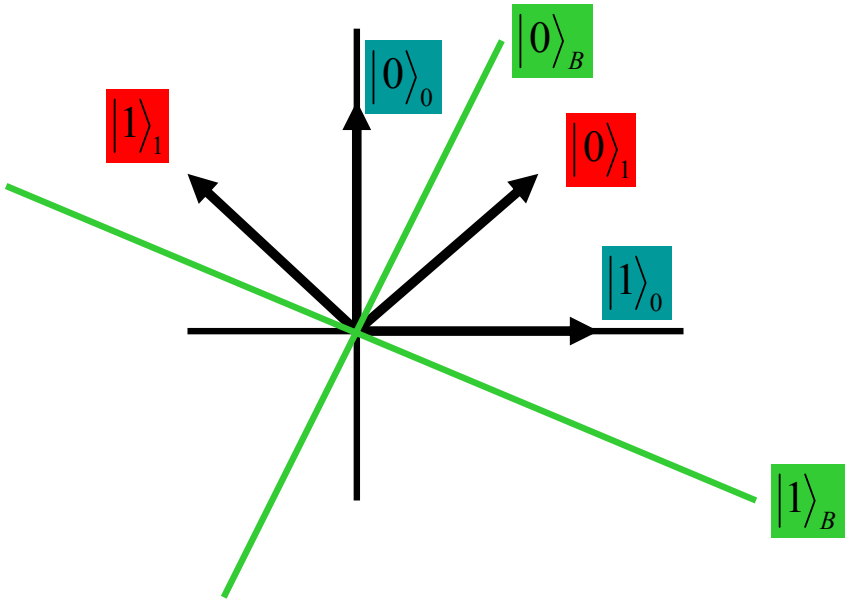
$$\frac{1}{2}|0\rangle_0 \langle 0|_0 + \frac{1}{2}|0\rangle_1 \langle 0|_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 1/4 \end{pmatrix} = \rho_0$$

et $x = 1$ se manifeste par

$$\frac{1}{2}|1\rangle_0 \langle 1|_0 + \frac{1}{2}|1\rangle_1 \langle 1|_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} 1/4 & -1/4 \\ -1/4 & 3/4 \end{pmatrix} = \rho_1$$

comme les deux matrices de densité sont différentes Ève peut partiellement distinguer les deux cas et obtenir de l'information sur x_i.

Différentes bases



Mesurer dans la base intermédiaire

Voici la base intermédiaire:

$$|0\rangle_B = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$$

$$|1\rangle_B = \sin(\pi/8)|0\rangle - \cos(\pi/8)|1\rangle$$

et la transformation unitaire

$$U_B = \begin{pmatrix} \cos(\pi/8) & \sin(\pi/8) \\ \sin(\pi/8) & -\cos(\pi/8) \end{pmatrix}$$

Nous avons que

$$U_B \rho_0 U_B^\dagger = \begin{pmatrix} \cos(\pi/8)^2 & 0 \\ 0 & \sin(\pi/8)^2 \end{pmatrix}$$

$$U_B \rho_1 U_B^\dagger = \begin{pmatrix} \sin(\pi/8)^2 & 0 \\ 0 & \cos(\pi/8)^2 \end{pmatrix}$$

et donc si $x_i = 0$ la probabilité d'observer $|0\rangle$ est $\cos(\pi/8)^2 \simeq 85\%$ et si $x_i = 1$ la probabilité d'observer $|1\rangle$ est $\cos(\pi/8)^2 \simeq 85\%$ Ève peut donc apprendre avec probabilité 85% la valeur de x_i en mesurant (détruisant) le qubit $|\psi_i\rangle$.

Mesurer dans la base intermédiaire

Maintenant que l'information est obtenue Ève doit transmettre un qubit à Bob. Même si Ève pense connaître la valeur de x_i, elle n'a aucune information sur b_i. Appelons x'_i la valeur supposée par Ève.

Plusieurs stratégies équivalentes s'offrent à elle. Elle peut essayer de deviner $b_i(b'_i)$ et envoyer $|x'_i\rangle_{b'_i}$. Si Alice et Bob choisissent la même base, alors avec probabilité 1/2 Ève choisira la même base et avec probabilité $\cos(\pi/2)^2$ le bon bit auquel cas aucune erreur ne survient, et avec probabilité $\sin(\pi/2)^2$ le mauvais bit auquel cas une erreur survient. Si elle choisit la mauvaise base, on calcule facilement que $x_i \neq y_i$ avec probabilité 1/2. En combinant ces probabilités on obtient que le bit sera erroné avec probabilité

$$\frac{\sin(\pi/8)}{2} + \frac{1}{4} \simeq 32\%$$

Ève pourrait aussi envoyer une superposition quelconque des deux états possibles et le résultat serait exactement le même. Elle peut évidemment faire pire mais il n'y a pas de façon évidente de faire mieux.

La stratégie optimale pour Ève

La stratégie optimale pour Ève consiste a interagir avec chaque $|\psi_i\rangle$ transmis par Alice juste ce qu'il faut pour obtenir de l'information sans trop perturber l'état.

Il existe toute une série d'attaques qu'Alice peut faire. On ne connaît pas l'attaque optimale, mais on sait que toute attaque donnant une quantité significative d'information sur s sera détecté avec probabilité très très proche de 1.

Peut-on faire mieux?

Qu'arrive t'il s'il y a des erreurs de transmission de qubits? Cela signifie que des erreurs vont être détectées même si l'espion n'espionne pas. Peut-on utiliser la correction d'erreur?

Avec le protocole présenté on produit 1 bit secret en utilisant $\Omega(n)$ qubits de communication quantique et $\Omega(n)$ bits de communication classique. Peut-on faire mieux?

Amplification de confidentialité

Définition
Une famille de fonctions de hachage universelles est $\mathcal{F} = \{f : \{0,1\}^n \to \{0,1\}^k\}$ telle que si f est choisit uniformément dans $\mathcal{F}$ alors $Prob(f(x) = g(x)) \leq \frac{1}{2^k}$.

Théorème:
Soit $p \geq 2^k$ $\mathcal{F} = \{f(x) = (ax + b(mod\ p))mod\ 2^k) | a \in \{1, \ldots, p-1\}, b \in \{0, \ldots, p-1\}\}$ est une famille de fonctions de hashage universelles.

Définitio:n
L'entropie de collision d'une variable aléatoire X est donnée par

$$H_c = -\log\left(\sum_{x \in X} prob(x)^2\right)$$

Théorème: $H(X) \geq H_c(X)$.

Théorème:
Soit $\mathcal{F}$ une famille de fonctions de hachage universelles de n bits dans k bits et X une variable aléatoire. Alors

$$H(f(X)|f) \geq H_c((f(X)|f)) \geq k - 2^{k - H_c(X)}$$

.

En particulier si Alice et Bob partagent une chaîne x de n bits telle que du point de vue d'Ève $H(X) = n - s$, c'est-à-dire qu'Ève connaît en gros s bits d'information sur x, alors en choisissant $k < n - s$ l'application d'une fonction de hachage universelle n dans k produit une chaîne y de k bits telle que $H(y) \simeq k$.

Réconciliations

Supposons qu'Alice et Bob ont une chaîne en commun mais que certaines positions sont erronées. Alice possède a et Bob b tels que $D(a,b) \leq t$.

Alice et Bob veulent réconcilier leurs chaînes. Ils veulent obtenir une chaîne commune x en révélant le moins d'information possible à Ève.

Premièrement, Alice et Bob peuvent facilement détecter si $t = 0$. Alice choisit z et transmet $z, a \cdot z$ à Bob, qui vérifie que $a \cdot z = b \cdot z$. Si $a = b$ alors le test réussira avec probabilité 1; mais si $a \neq b$ alors le test détectera une erreur avec probabilité exactement 1/2.

Alice et Bob savent maintenant que le nombre de positions où $z_i = 1$ et $a_i \neq b_i$ est impair.

Soit maintenant a' et b' les sous-chaînes de a et b pour lesquelles $z_i = 1$ ($|a'| = |b'| = n'$). Clairement $a' \neq b'$ si $n' = 1$ alors Alice et Bob ont détecté une position pour laquelle $a \neq b$ et peuvent corriger l'erreur.

Si $n > 1$ alors Alice choisit z', une chaîne aléatoire de n' bits, et transmet $z', a' \cdot z'$ à Bob. Ce dernier compare $a' \cdot z'$ avec $b' \cdot z'$. Si cette valeur est différente alors Bob sait qu'il y a un nombre impair d'erreurs dans la sous-chaîne de a' et b' pour laquelle $z'_i = 1$. Alice et Bob recommencent le même procédé avec les sous chaines.

Si $a' \cdot z'$ avec $b' \cdot z'$, comme il y a un nombre impair d'erreurs on sait que les sous-chaînes de a' et b' pour lesquelles $z'_i = 0$ contiennent un nombre impair d'erreurs. Alice et Bob continuent le protocole de réconciliation avec ces sous-chaînes.

On voit bien qu'Alice et Bob vont réconcilier leurs chaînes avec très bonne probabilité. Le nombre de bits transmis au sujet des chaînes est dans $O(t \log n)$.

Réconciliation

Exemple au tableau...

Le vrai protocole BB84

Protocole BB84
Alice choisit $x \in_R \{0,1\}^n$ et $b \in_R \{0,1\}^n$.
Bob choisit $c \in_R \{0,1\}^n$.
Pour i de 1 à n:
    Alice transmet à Bob $|\psi_i\rangle = |x_i\rangle_{b_i}$.
    Si $c_i = 0$ Bob mesure $y_i = M(|\psi_i\rangle)$.
    Si $c_i = 1$ Bob mesure $y_i = M(H|\psi_i\rangle)$.
Bob transmet c à Alice.
Alice transmet b à Bob.
Pour i de 1 à n, si $b_i \neq c_i$ Alice transmet x_i à Bob, qui remplace $y_i = x_i$
Alice et Bob effectuent la réconciliation de leurs chaînes.
Si le taux d'erreur est suffisamment faible ils effectuent l'amplification de confidentialité et obtiennent une clef secrète s.