Chapter 4

Cryptographie Quantique

Une des premières applications de la MQ à la théorie de l'information quantique est le protocole inventé par Bennett et Brassard en 1984 pour la distribution d'une clé secrète entre deux acteurs distants (Alice et Bob). Depuis d'autres protocoles ont vu le jour et une nouvelle discipline "la cryptographie quantique" a émergée. A proprement parler, comme nous le verrons il ne s'agit pas vraiment de cryptographie, mais plutot de méthodes de génération de clé secrète commune.

L'idée générales du protocole BB84 est la suivante. Alice envoie une suite de bits classiques - la clé secrète - à Bob en utilisant des qubits intermédiaires[1]. Toute tentative, de la part d'un troisième acteur (Eve) d'extraction d'information, à propos de la clé nécessite d'observer les qubits. selon les postulats de la MQ cette observation perturbe l'état des qubits. Nous verrons qu'Alice et Bob sont capables de détecter cette perturbation, et donc la présence d'Eve. Dans un tel cas de figure la communication est arrétée.

Le sujet est bien plus compliqué que le traitement exposé dans ce chapitre. En réalité le canal de communication (la fibre optique) est bruité et il n'est pas évident de distinguer les perturbations d'Eve de celles associées au bruit. D'autrepart les opérations d'Alice et Bob ne sont pas parfaites, au niveau de la préparation des états ainsi qu'au niveau de leurs mesures. La preuve mathématique de la sécurité du protocole de BB84 repose sur des hypothèses qui peuvent en pratique être violées. Néanmoins si l'on accepte certaines hypothèses, on peut démontrer la sécurité du protocole. Une telle preuve est hautement non-triviale et dépasse largement le cadre de ce cours. Nous discuterons néanmoins deux attaques simplifiées de la part d'Eve ce qui sera suffisant pour comprendre pourquoi les principes de la MQ assurent la sécurité

[1]Ici nous pouvons penser au qubit associé à la polarisation du photon; bien qu'en pratique le protocole est implémenté avec des degrés de libertés associés à la phase des photons.

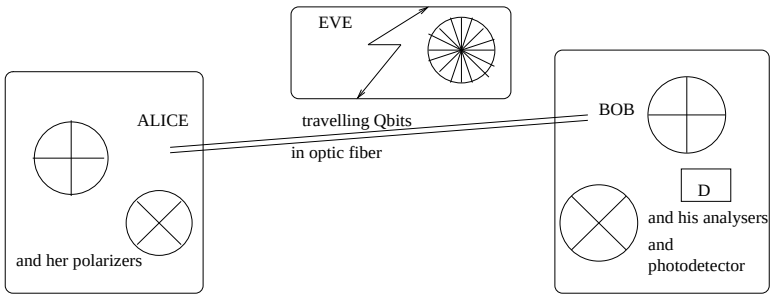

Figure 4.1: Alice et Bob génèrent une clśecrète sur le canal d'une fibre optique

de la clé.

La cryptographie quantique n'est pas seulement une idée théorique, c'est également un sujet véritablement expérimental. La génération de clé secrète commune à été réalisée dans les laboratoires (d'abord chez IBM en 1989, sur une distance de 32 cm!) et plus tard à l'extérieur des laboratoires sur des distances de quelques dizaines à des centaines de kilomètres (Genève, Los Alamos ...). Aujourd'hui, il existe des sociétés proposant des systèmes commerciaux [2]. Des implémentations récentes permettent la génération de clés secrètes communes sur des distance de 100 km (resp. 250 km) à un taux de de 6000 (resp. 15) bits par seconde. Celles-ci exigent une connaissance approfondie de l'optique et ne seront pas discutées ici. Récemment, ces systèmes ont été violés en exploitant les limites physiques des photo-détecteurs du coté de Bob. En illuminant un photodétecteur de facon appropriée celui-ci fonctionne alors en mode classique et les avantages liés à la MQ sont perdus.

4.1 La génération des clés selon BB84

Le protocole comporte quatre phases essentielles: la procédure d'encodage d'Alice, la procédure de décodage de Bob, une communication publique entre les deux parties, et enfin la génération de la clé secrète commune. La figure 4.1 illustre le set-up général.

Procédure de codage d'Alice. Elle génère une suite binaire aléatoire $x_1, ..., x_n,\ x_i \in \{0, 1\}$ qu'elle garde secrète. La clé commune sera un sous-ensemble de ces bits. Elle génère également une deuxième suite binaire aléatoire $e_1, ..., e_N,\ e_i \in \{0, 1\}$ qu'elle garde secrète *pour l'instant*. Alice *encode* les bits classiques x_i en qubits comme suit:

- Pour $e_i = 0$ elle génère un qubit dans l'état $|x_i\rangle$. Concrètement, elle

[2] IdQuantique

Figure 4.2: Orientations des polariseurs pour la préparation des photons dans la base Z.

Figure 4.3: Orientations du polariseur pour la préparation des photons dans la base X.

prépare les photons avec un polariseur dans la base Z (figure 4.2).

$$\big\{|0\rangle, |1\rangle\big\}$$

Pour $x_i = 0$ (resp. $x_i = 1$) le polariseur est orienté horizontalement (resp. verticalement). Ainsi les photons sont préparés dans l'état de polarisation $|0\rangle$ (resp. $|1\rangle$). Un seul photon est ensuite sélectionné dans le faisceau sortant (ce qui bien-sûr est une idéalisation).

- Pour $e_i = 1$, elle génère un qubit dans l'état[3] $H|x_i\rangle$. Concrètement, cela peut se faire en envoyant des photons à travers un polariseur dans la base X (figure 4.3)

$$\big\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\big\}$$

Pour $x_i = 0$ (resp. $x_i = 1$) le polariseur est tourné vers la droite d'un angle $\pi/4$ (resp. à gauche d'un angle $-\pi/4$) et les photons sont préparés dans un état de polarisation $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (resp. $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

En résumé, Alice envoie une chaîne de qubits $|A_{e_i,x_i}\rangle = H^{e_i}|x_i\rangle$, $i = 1, ..., N$ par un canal (dans la pratique, une fibre optique).

Procédure de décodage de Bob . Bob génère une suite binaire aléatoire $d_1, ..., d_n$, $d_i \in \{0, 1\}$ qu'il garde secrète *pour l'instant* . Il décode les qubits reçus d'Alice comme suit:

[3]Ici H est la matrice de Hadamard $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

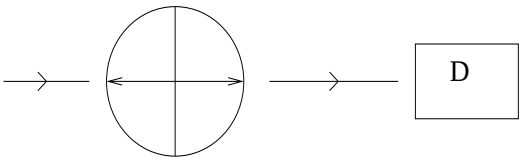

Figure 4.4: Dispositif analyseur-détecteur pour la mesure de la polarisation dans base Z.

- Si $d_i = 0$ il effectue une mesure des qubits reçus $|A_{e_i,x_i}\rangle$ dans la base Z

$$\Big\{|0\rangle, |1\rangle\Big\}.$$

L'état photon après la mesure

$$|y_i\rangle \in \{|0\rangle, |1\rangle\}.$$

est enregistré dans des bits classiques y_i. Pour ce faire, concrètement, il utilise l' appareil de mesure analyseur-détecteur décrit dans le premier chapitre: l'analyseur est placé horizontalement (figure 4.4); si le détecteur clique cela signifie que l' état des photons est projeté sur $|0\rangle$; et si le détecteur ne clique pas , cela signifie que l'état photon est projeté sur $|1\rangle$. Nous soulignons que, selon le postulat de la mesure, ces résultats sont *vraiment aléatoire* . C'est uniquement Bob qui les connaît.

- Si $d_i = 1$, il effectue une mesure des qubits reçus $|A_{e_i,x_i}\rangle$ dans la base X.

$$\Big\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle\Big\}.$$

L'état du photon après la mesure appartient à

$$H|y_i\rangle \in \Big\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\Big\}$$

Pour un état $H|y_i\rangle$, Bob enregistre le bit classique y_i . Pour ce faire, concrètement , il utilise l'appareil analyseur-détecteur décrit dans le premier chapitre : l'analyseur est tourné vers la droite (figure 4.5) à 45 degrés; si le détecteur clique cela signifie l'état des photons est projeté sur l'état $H|0\rangle$; tandis que si le détecteur ne clique pas cela signifie que l'état photon est projeté sur $H|1\rangle$. Nous soulignons à nouveau que, selon le postulat de la mesure ces résultats sont *vraiment aléatoire*. Seul Bob les connaît.

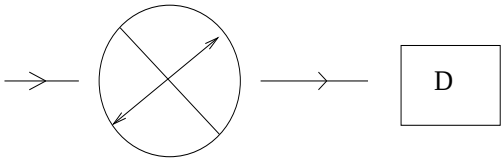

Figure 4.5: Dispositif analyseur-détecteur pour la mesure de la polarisation dans X base.

En résumé Bob a décodé les qubits envoyés par Alice, en une suite binaire classique $y_1, ..., y_n$. cette suite est le résultat des mesures de Bob et ne peut être prédite.

Communication Publique. Alice possède à sa disposition deux suites binaires: $e_1, ..., e_N$ utilisée pour encoder; et $x_1, ..., x_N$ qui est mappée sur les qubits. Bob aussi possède deux suites binaires: $d_1, ..., d_N$ pour choisir une base de mesure et $y_1, ..., y_N$ qui sont les résultats des mesures.

Alice et Bob communiquent $e_1, ..., e_N$ et $d_1, ..., d_N$ sur un canal public classique, et gardent les deux suites $x_1, ..., x_N$ et $y_1, ..., y_N$ secrètes. *Il importe que la communication publique ne commence qu'après la phase de mesures de Bob.* Alice et Bob peuvent déduire les informations suivantes (en fait quiconque entendant la communication publique peut déduire ces informations):

- Si $d_i = e_i$, c.a.d si ils ont utilisé la même base, alors certainement $y_i = x_i$ (on peut s'en convaincre avec quelques exemples; en fait si Bob et Alice ont utilisé la même base c'est comme s'ils vivaient dans un monde classique).

- Si $d_i \neq e_i$, c.a.d s'ils n'ont pas utilisé la même base, de véritables effets quantiques entrent en jeu quand Bob fait la mesure. Selon le postulat de la mesure $y_i \neq x_i$ avec probabilité $\frac{1}{2}$ et $y_i = x_i$ avec probabilité $\frac{1}{2}$. Prouvons le. Bob recoit le qubit

  $$|A_{e_i,x_i}\rangle = H^{e_i}|x_i\rangle$$

  et mesure dans la base

  $$\{H^{d_i}|0\rangle, H^{d_i}|1\rangle\}.$$

  Le résultat sera un des deux vecteurs de base:

  $$H^{d_i}|0\rangle, \qquad \text{avec prob } |\langle 0|H^{d_i}H^{e_i}|x_i\rangle|^2$$

ou bien

$$H^{d_i}|1\rangle, \qquad \text{avec prob } |\langle 1|H^{d_i}H^{e_i}|x_i\rangle|^2.$$

Le lecteur peut vérifier que si $e_i \neq d_i$ les deux probabilités correspondantes sont égales à $\frac{1}{2}$ (et si $e_i = d_i$ elles valent 0 ou 1).

Génération de la clé commune. Bob et Alice effacent tous les bits x_i et y_i correspondant à i tel que $e_i \neq d_i$. Ils gardent les bits x_i et y_i restants indexés par i tels que $e_i = d_i$. Ils sont assurés que ces deux suites de bits sont identiques $x_i = y_i$, donc cela peut potentiellement constituer la clé secrète commune. La longueur de cette sous-suite est proche de $\frac{N}{2}$, car prob(e_i $neq d_i$) $= \frac{1}{2}$. Enfin, Alice et Bob effectuent un test de sécurité: selon la mécanique quantique on doit avoir[4]

$$\text{Prob}(x_i = y_i | e_i = d_i) = 1$$

Alice et Bob testent cette condition en échangant une petite fraction (disons $\epsilon\frac{N}{2}$) de la sous-suite commune sur le canal public. Si le test réussi, ils gardent le reste de sous suite commune: ils ont réussi à générer une clé secrète commune de longueur $(1-\epsilon)\frac{N}{2}$.

4.2 Attaques de la part d'Eve - discussion simplifiée

Nous supposons que Alice a une source de photon unique parfait, que la préparation des qubits est parfaite , qu'il n'y a pas de bruit, que les appareils de mesure de Bob sont parfaits. Dans ces conditions, lorsque Eve est absente le critère de sécurité absolue Prob($x_i = y_i | e_i = d_i$) $= 1$ est satisfait.

En outre, nous supposons qu'Eve peut seulement attaquer en effectuant des opérations sur un qubit à la fois, sur les photons capturés le long de la fibre optique et qu'elle n'a pas accès aux laboratoires d'Alice et Bob. Nous supposons néanmoins qu'Eve a une connaissance parfaite des orientatins X et Z des polariseurs et analyseurs d'Alice et Bob (mais pas des choix aléatoires successifs).

Nous considérons deux attaques possibles: "l'attaque basée sur une mesure" et "l'attaque basée sur des opérations unitaires ". Les deux attaques se composent de deux étapes. Premièrement Eve capture un photon, fait une mesure ou applique une opération unitaire, puis transmet le photon à Bob, ou alors lui transmet un autre photon (voir figure 4.6). Nous allons voir que

[4]Sans bruit et sans la présence d'Eve.

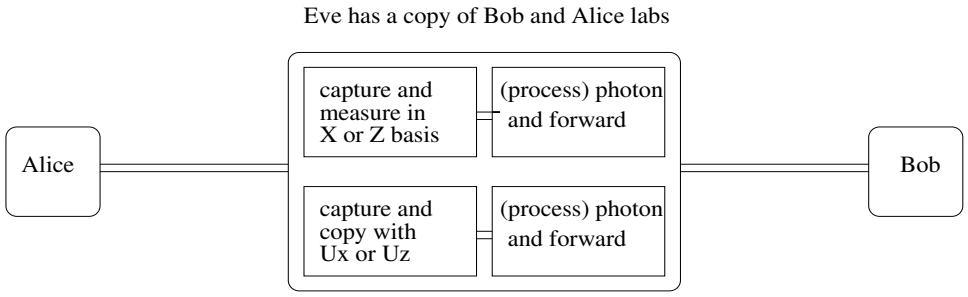

Figure 4.6: Laboratoire d'interception de photons d'Eve's sur le chemin de la fibre optique

les postulats de base de QM impliquent que le critère de sécurité est violé. Lorsqu'Alice et Bob constatent cette violation ils découvrent la présence d'Eve et interrompent la communication.

Attaque de type mesure. Supposons qu'Eve capture un photon dans la fibre optique. Le photon capturé est dans l'un des états

$$|A_{e_i,x_i}\rangle \in \big\{|0\rangle, |1\rangle, H|0\rangle, H|1\rangle\big\}$$

Eve effectue une mesure. Si elle utilise la base Z le résultat appartient à $\{|0\rangle, |1\rangle\}$ et elle enregistre un bit $y_i^E \in \{0, 1\}$. Si elle utilise la base X son résultat est dans $\{H|0\rangle, H|1\rangle\}$ et elle enregistre le bit correspondant $y_i^E \in \{0, 1\}$. Une fois qu'elle a terminé la mesure, elle envoie le photon à Bob dans le nouvel état laissé par la mesure [5]. Deux possibilités peuvent se présenter:

- Eve a utilisé la même base qu'Alice: alors $y_i^E = x_i$ et le photon est reçu par Bob dans l'état correct.

- Eve a utilisé une base différente qu'Alice: alors $y_i^E = x_i$ seulement la moitié du temps, et elle envoie à Bob le photon dans un état "correct" seulement la moitié du temps.

Voyons ce que Alice et Bob trouvent quand ils effectuent le test de sécurité.

[5] Elle pourrait aussi envoyé un autre photon dans cet état ou un autre état mais cela ne peut pas améliorer sa performance.

On note EA pour l'évènement "Eve utilise la même base que Alice".

$$\begin{aligned}\text{prob}(x_i = y_i | e_i = d_i) &= \text{prob}(x_i = y_i | e_i = d_i, EA)\text{prob}(EA) \\ &\quad + \text{prob}(x_i = y_i | e_i = d_i, \text{not } EA)\text{prob}(\text{not } EA) \\ &= 1 \cdot \text{prob}(EA) + \frac{1}{2} \cdot (1 - \text{prob}(EA)) \\ &= \frac{1}{2}(1 + \text{prob}(EA))\end{aligned}$$

où nous avons utilisé

$$\text{prob}(x_i = y_i | e_i = d_i, EA) = 1, \qquad \text{prob}(x_i = y_i | e_i = d_i, \text{not EA}) = \frac{1}{2} \quad (4.1)$$

En supposant qu' Eve n'a aucune information sur les choix de base d'Alice que nous prenons $\text{prob}(EA) = \frac{1}{2}$. Alors

$$\text{prob}(x_i = y_i | e_i = d_i) = \frac{3}{4}.$$

Alice et Bob savent qu'un quart des bits ne sont pas corrects même quand ils ont utilisés la même base: ils concluent qu'un espion est à l'oeuvre!

Attaque unitaire. Avec l'attaque précédente lorsqu'Eve fait une mesure, elle n'a aucune information sur la base qu'Alice a choisi. Une solution possible serait de copier les qubits $|A_{e_i,x_i}\rangle$, et laisser le photon dans l'état original arriver à Bob. La copie pourra être utilisée par eve (du moins croit-elle) après la phase de communication publique. Quand Alice et Bob entrent dans la phase de communication publique, Eve connait les choix de base de Bob. Donc pour i tel que $e_i = d_i$ elle obtient les mêmes résultat que Bob $y_i^E = y_i = x_i$. Elle partage donc le secret d'Alice et Bob.

Toutefois il y a une erreur dans le raisonnement ci-dessus. Le *théorème de non-clonage* (qui est une conséquence du postulat de l'évolution unitaire) garanti qu'il n'existe pas de machine (unitaire) telle que

$$U(|A_{e_i,x_i}\rangle \otimes |\text{blank}\rangle) = |A_{e_i,x_i}\rangle \otimes |A_{e_i,x_i}\rangle$$

Le point important est que $|A_{e_i,x_i}\rangle$ appartient à

$$\{|0\rangle,\ |1\rangle,\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

qui est un ensemble d'états non-orthogonaux! (A et B ont bien travaillé leur MQ).

Eve pourrait essayer d'utiliser deux machines de copie: une pour la copie des deux états de la base Z et une autre pour la copie des deux états de la base X. Mais cette fois, elle n'a aucun moyen de savoir laquelle des deux utiliser quand un photon est capturé. Elle utilisera la mauvaise machine la moitié du temps. Une analyse similaire à la précédente montre qu'à nouveau

$$\text{prob}(x_i = y_i | e_i = d_i) = \frac{3}{4}.$$

Le critère de sécurité est violé: le quart des bits communs sont corrompus.

4.3 Le protocole de Bennet 1992

Dans BB84 Alice prépare les photons dans 4 états possibles. En fait l'analyse précédente montre que le point impiortant est que ces états ne sont pas deux à deux tous orthogonaux. Bennet inventa en 1992 un protocole qui utilise uniquement deux états non-orthogonaux: $|0\rangle$ et $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Ce protocole ainsi qu'une analyse détaillée de sa sécurité est l'objet d'un exercice.