Série 5 : 15 Octobre 2015
Traitement Quantique de l'Information

Exercice 1 *Protocole de Bennett 1992.*

L'analyse de BB84 montre que le point important du protocole est l'utilisation d'états de qubits non-orthogonaux. Le protocole B92 retient cette caractéristique mais est plus simple à implémenter que BB84. En effet seulement deux états non-orthogonaux sont utilisés au lieu de 4. Voici les phases principales du protocole :

Alice encode. Alice génère une suite binaire aléatoire $e_1, ..., e_N$ qu'elle garde secrète. Elle envoie à Bob $|A_{e_i}\rangle = |0\rangle$ si $e_i = 0$ et $|A_{e_i}\rangle = H|0\rangle = \frac{1}{2}(|0\rangle + |1\rangle)$ si $e_i = 1$. L'état du qubit envoyé est donc $H^{e_i}|0\rangle$.

Bob décode. Bob génère une suite binaire aléatoire $d_1, ..., d_N$ qu'il garde secrète, et mesure le qubit recu selon la valeur de $d_i = 0$ ou $d_i = 1$ dans la base Z ou X. Il obtient alors un état après la mesure dans $\{|0\rangle, |1\rangle\}$ ou dans $\{H|0\rangle, H|1\rangle\}$. Puis enregistre le bit $y_i = 0$ si le résultat de la mesure est $|0\rangle$ ou $H|0\rangle$ et $y_i = 1$ si le résultat de la mesure est $|1\rangle$ ou $H|1\rangle$.

Discussion Publique. Bob annonce sur un canal public ses résultats $y_1, \ldots, y_N$. Si $e_i = d_i$ on a $y_i = 0$ avec probabilité 1 : prouvez le. Si par contre $e_i \neq d_i$ on a $y_i = 0$ avec probabilité $\frac{1}{2}$ et $y_i = 1$ avec probabilité $\frac{1}{2}$: prouvez le. A partir de cette discussion publique Alice et Bb deduisent que si $y_i = 1$, alors certainement $d_i = 1 - e_i$.

Génération de la clé secrète commune. Alice et Bob gardent secrets les bits e_i et $d_i = 1 - e_i$ pour les i tels que $y_i = 1$. Ils rejettent tous les autres bits. Expliquez pourquoi cela constitue leur clé secrète. Quelle est la longueur de cette clé ? Proposez un test de sécurité qu'Alice et Bob pourraient faire.

Attaques de la part d'Eve. Discutez dans le même esprit que dans le cours pourquoi le test de sécurité est violé si Eve capture un photon et essaye une attaque de type "mesure" ou de type "unitaire".

Exercice 2 *Processus stochastique classique versus évolution unitaire et mesure quantique.*

Une matrice P est dite stochastique si $0 \leq P_{kl} \leq 1$ et $\sum_{k=0}^{n-1} P_{kl} = 1$. Ici P_{kl} représente une probabilité de transition $l \to k$. On considère le processus stochastique classique donné par la figure 1. On initialise le registre d'entrée dans l'état 0. Lors de la première étape, l'état transite vers 0, 1, 2 avec probabilité P_{j0}. Lors de la deuxième étape, l'état transite vers 0, 1, 2 avec probabilité Q_{kj}.

a) Calculez la probabilité d'observer l'état 2 à la sortie.

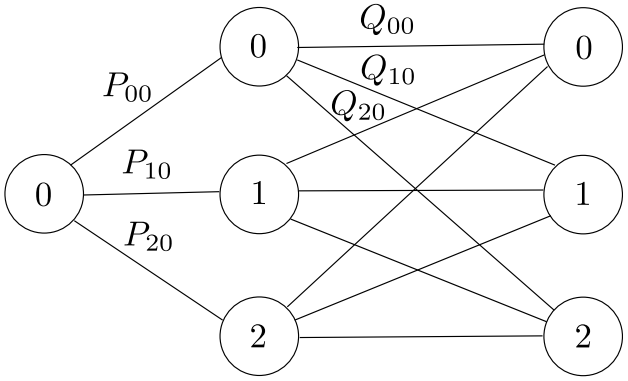

FIGURE 1 – processus classique

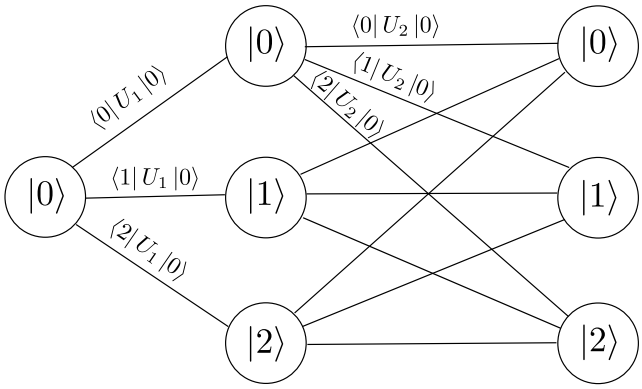

FIGURE 2 – processus quantique

On considère l'analogue quantique :voir figure 2. Ici le registre peut être dans 3 états quantiques qui forment une base orthonormée. $|0\rangle$, $|1\rangle$ et $|2\rangle$. La première transition est décrite par une matrice d'évolution unitaire U_1 et la deuxième transition par U_2. On suppose que $|\langle j|\,U_1\,|i\rangle|^2 = P_{ji}$ et $|\langle j|\,U_2\,|i\rangle|^2 = Q_{ji}$.

b) Montrez d'abord que P_{ji} et Q_{ji} sont des matrices stochastiques (utilisez l'orthonormalité des états de base). Interprétez la signification physique de ces matrice.

c) Calculez la probabilité d'observer l'état $|2\rangle$ à la sortie si l'état d'entrée est $|0\rangle$. Comparez le résultat avec le cas classique.

d) Supposons que l'on fasse une mesure intermédiaire après la première étape. Quelle est la probabilité d'observer l'état final $|2\rangle$ à la sortie, si l'état initial est $|0\rangle$. Y-a-t'il une différence avec le cas classique ?

e) Réfléchissez à une analogie entre cet exercice et l'expérience des fentes Young (qu'est ce qui joue le role de fentes ? qu'est ce qui joue le role de l'écran ? discutez !).