Série 6
Traitement Quantique de l'Information

Exercice 1 *Protocole de Bennet 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 deux états non-orthogonaux sont utilisés au lieu de 4. Voici les phases principales du protocole :

Alice encode. Alice genère une suite binaire aléatoire $e_1, ..., e_N$. Elle envoie à Bob $|A_{e_i}\rangle = |0\rangle$ if $e_i = 0$ and $|A_{e_i}\rangle = H|0\rangle = \frac{1}{2}(|0\rangle + |1\rangle)$ if $e_i = 1$. Létat du qubit envoyé est donc $H^{e_i}|0\rangle$.

Bob decode. Bob genère une binaire aléatoire $d_1, ..., d_N$ et measure le qubit recu selon la valeur de d_i dans la base Z ou X et obtient un état dans $\{|0\rangle, |1\rangle\}$ ou dans $\{H|0\rangle, H|1\rangle\}$. Il décode le qubit comme $y_i = 0$ si le résultat de la mesure est $|0\rangle$ or $H|0\rangle$ et $y_i = 1$ si le résultat de la mesure est $|1\rangle$ or $H|1\rangle$.

Discussion Publique. Bob annonce sur un canal public ses résultats y_i. 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 $d_i = 1 - e_i$.

Génération de la clé. Alice et Bob gardent secrets les bits $(e_i, d_i = 1 - e_i)$ pour i tels que $y_i = 1$ et rejettent les autres bits. Expliquez pourquoi cela constitue leur clé secrete. Quelle est la longeur de cette clé. Proposez un test de sécurité qu'ils pourraient faire sur une petite fraction de ces bits.

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 and forward".

Exercice 2 *Etats de Bell.*

Le but de cet exercice est de se familiariser avec certains calculs relatifs aux états de Bell : les calculs des trois premières questions sont à faire en notation de Dirac.

1. Montrez que 4 les états de Bell introduits en cours forment une base orthonormée de $\mathbf{C}^2 \otimes \mathbf{C}^2$.
2. Montrez que l'état $|B_{00}\rangle$ (ou bien prenez en un autre) est intriqué. C'est à dire qu'il n'existe pas $|\psi_1\rangle \in \mathbf{C}^2$ et $|\psi_2\rangle \in \mathbf{C}^2$ tels que $|B_{00}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \in \mathbf{C}^2$.
3. Soit $|\gamma\rangle = (\cos\gamma|0\rangle + \sin\gamma|1\rangle)$. Montrez l'identité (pour tout $|\gamma\rangle$)
$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|\gamma\rangle \otimes |\gamma\rangle + |\gamma_\perp\rangle \otimes |\gamma_\perp\rangle)$$
4. Représentez les 4 états de Bell en coordonnées. Utilisez la représentation canonique $|0\rangle = (1,0)^T$ et $|1\rangle = (0,1)^T$.

Exercice 3 *Opération unitaire créant l'intrication.*

Soit $|x\rangle \otimes |y\rangle$ avec $x, y = 0, 1$ les 4 états de la "base computationnelle" (ou cacnonique) pour deux 2 qubits. On définit l'opération unitaire $CNOT$ (appelée "control-not")

$$CNOT|x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus x\rangle$$

où $y \oplus x$ est l'addition modulo 2. Cette opération modélise certaines interactions entre degrés de liberté de spin, et est responsable de l'intrication.

1. Vérifiez que
$$|B_{xy}\rangle = (CNOT)(H \otimes I)|x\rangle \otimes |y\rangle$$
Faites le calcul en notation de Dirac. Est ce que la partie $(H \otimes I)|x\rangle \otimes |y\rangle$ est déja intriquée ? Justifiez.
2. Donnez le tableau des composantes des matrices $CNOT$ et $H \otimes I$ ainsi que leur produit dans la base computationnelle. Vérifiez que les matrices sont unitaires.
3. A partir de l'unitarité des matrices, donnez une preuve compacte en cinq lignes maximum de l'orthonormalité des états $|B_{xy}\rangle$.