Traitement quantique de l'information I (automne 2009)
Série 12: Protocole E91 de cryptographie quantique

Etablir un protocole de partage quantique de clé qui soit basé sur des paires de photons dans un état de Bell

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Les deux photons sont préparés par Charlie et envoyés le premier à Alice et le deuxième à Bob. Alice et Bob disposent chacun d'un filtre polariseur qu'ils peuvent orienter. Si le filtre laisse passer le photon on mesure $+1$. Si non, on mesure -1.

1. Montrer qu'on peut construire un protocole efficace, si Alice et Bob choisissent d'orienter le polariseur parmi trois orientations différentes.

   Pour Alice: $\theta_A = 0$, $\pi/8$, $\pi/4$.

   Pour Alice: $\theta_B = \pi/8$, $\pi/4$, $3\pi/8$.

   Illustrer le fonctionnement du protocole. En particulier:

   (a) Qu'arrive-t-il si Alice et Bob choisissent la meme orientation pour les polariseurs? Ecrire un tableau des possibles résultats des deux mesures, avec probabilités respectives.

   (b) Qu'arrive-t-il si Alice et Bob choisissent deux orientations différentes pour leurs polariseurs? Ecrire un tableau des possibles résultats des deux mesures, avec probabilités respectives.

   (c) Dans quel cas on a corrélation entre les mesures d'Alice et Bob?

   (d) Comment font Alice et Bob pour choisir les mesures corrélées?

2. Discuter comment Eve pourrait obtenir de l'information sur la clé, et comment Alice et Bob peuvent détecter son intrusion. Idée: on pourrait utiliser les mesures qu'on a exclu avant. Quelle condition doivent remplir ces mesures si Eve ne fait rien? Quel est l'état après une éventuelle mesure effectuée par Eve? Comment change la condition d'avant?