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 construir un protocole efficace, si Alice et Bob choisissent d'orienter le polariseur parmi trois orientations différentes.

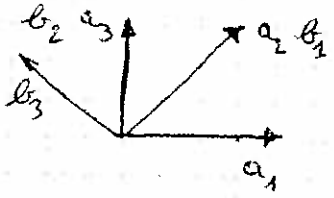
   Pour Alice: $\theta_A = 0,\ \pi/8,\ \pi/4$

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

   Illustrer le fonctionnement du protocole.

2. Discuter comment Eve pourrait obtenir de l'information sur la clé, et comment Alice et Bob peuvent détecter son intrusion.

Serie 12.



clé:

a_1 b_2
a_2 b_1
a_2 b_3
a_3 b_2

} → 4 (4/9 : info)

Bell:

a_1 b_1
a_1 b_3
a_3 b_1
a_3 b_3

} → 4 (4. 9. check)

pas utilisé

a_2 b_2

$$E(a_i, b_j) = -a_i \cdot b_j$$

$$S = E(a_1, b_1) - E(a_1, b_3) + E(a_3, b_1) + E(a_3, b_3)$$

$$= \frac{\sqrt{2}}{2} - \left(-\frac{\sqrt{2}}{2}\right) + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} = 2\sqrt{2}$$

$$E(a_i, b_j) = P_{++}(a_i, b_j) + P_{--}(a_i, b_j) - P_{+-}(a_i, b_j) - P_{-+}(a_i, b_j)$$

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

a mesuré selon (x) / (y)

b mesuré selon $|\theta\rangle |\theta_\perp\rangle$ $\quad |\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$

$|\theta_\perp\rangle = \sin\theta|0\rangle - \cos\theta|1\rangle$

$$P_{++} = |\langle 0\,\theta|\psi\rangle|^2 = \left|\frac{1}{\sqrt{2}}(\sin\theta)\right|^2$$

$$P_{--} = |\langle 1\,\theta_\perp|\psi\rangle|^2 = \frac{1}{2}(\sin\theta)^2$$

$$P_{+-} = |\langle 0\,\theta_\perp|\psi\rangle|^2 = \frac{1}{2}(\cos\theta)^2$$

$$P_{-+} = |\langle 1\,\theta|\psi\rangle|^2 = \frac{1}{2}(\cos\theta)^2$$

$$E = \frac{1}{2}(2\sin^2\theta - 2\cos^2\theta) = -\cos(2\theta)$$

Après eavesdropping

$$|\psi\rangle = |\theta_{ea}\ \theta_{eb}\rangle$$

$$E_{ee}(a_i, b_j) = ?$$

$$P_{++}(a_i, b_j) = |\langle \theta_i \theta_j | \theta_{ea}\ \theta_{eb}\rangle|^2$$

$$= |\langle \theta_{a_i} | \theta_{ea}\rangle|^2 |\langle \theta_{b_j} | \theta_{eb}\rangle|^2$$

$$= (\cos\theta_{a_i}\cos\theta_{ea} + \sin\theta_i \sin\theta_{ea})^2 (\ \ldots\ )^2$$

$$= \cos^2(\theta_{a_i} - \theta_{ea})\cos^2(\theta_{b_j} - \theta_{eb})$$

$$P_{--}(a_i, b_j) = |\langle \theta_{a_i \perp} | \theta_{ea}\rangle|^2 |\langle \theta_{b_j \perp} | \theta_{eb}\rangle|^2$$

$$= (-\sin(\theta_{a_i})\cos(\theta_{ea}) + \cos(\theta_{a_i})\sin(\theta_{ea}))^2$$

$$(\quad\quad)^2$$

$$= \sin^2(\theta_{a_i} - \theta_{ea})\sin^2(\theta_{b_j} - \theta_{eb})$$

$$P_{+-}(a_i, b_j) = \cos^2(\theta_{a_i} - \theta_{ea})\ \sin^2(\theta_{b_j} - \theta_{eb})$$

$$P_{-+}(a_i, b_j) = \sin^2(\theta_{a_i} - \theta_{ea})\ \cos^2(\theta_{b_j} - \theta_{eb})$$

$$E(a_i, b_j) = \cos^2(\overbrace{\theta_{a_i} - \theta_{ea}}^{\Delta\theta_a})\left(\cos^2\Delta\theta_b - \sin^2\Delta\theta_b\right)$$

$$+ \sin^2(\Delta\theta_a)\left(\cos^2\Delta\theta_b - \sin^2\Delta\theta_b\right)$$

$$= \cos 2\Delta\theta_a \cos 2\Delta\theta_b$$

$$S = \int \rho(\theta_{ea}, \theta_{eb}) \Big[\cos\theta_{ea} \cos\left(\theta_{eb} - \frac{\pi}{4}\right) - \cos\theta_{ea} \cos\left(\theta_{eb} - \frac{3\pi}{4}\right) + \cos\left(\theta_{ea} - \frac{\pi}{2}\right) \cos\left(\theta_{eb} - \frac{\pi}{4}\right) + \cos\left(\theta_{ea} - \frac{\pi}{2}\right) \cos\left(\theta_{eb} - \frac{3\pi}{4}\right) \Big] d\theta_{ea} d\theta_{eb}$$

(Mathematica)

$$= \int \rho(\theta_{ea}, \theta_{eb}) \sqrt{2} \cos(\theta_{ea} - \theta_{eb}) \, d\theta_{ea} \, d\theta_{eb}$$

$$\Rightarrow -\sqrt{2} < S < \sqrt{2}$$