Traitement quantique de l'information I (automne 2009)
Série 7: Stratégie optimale pour la cryptographie quantique

Supposons que Alice choisit de manière aléatoire (avec 50% de probabilité) une parmi les deux bases $\{|x\rangle, |y\rangle\}$ et $\{|\theta\rangle, |\theta_\perp\rangle\}$. Eve détecte toujours avec un polariseur orienté selon **x**. Considérer seulement les cas où Bob a choisi la même base que Alice (donc ceux qui seront retenus). Quelle est la probabilité que un bit de la clé de Bob soit différent de celui de la clé de Alice? Cette probabilité correspond à la probabilité pour Eve de commettre une erreur dans sa stratégie, et donc d'être découverte par Alice et Bob. Montrer que cette probabilité est

$$p = \frac{1}{4}\sin^2(2\theta)$$

On comprend donc pourquoi le choix optimal pour les deux bases est $\theta = \pi/4$.

$$P_{\text{erreur}} = P(\overset{B}{1} \mid \overset{A}{0}) \cdot P(\overset{A}{\theta})$$

$$= P(\overset{E}{x} \mid \overset{A}{0})\, P(\overset{B}{1} \mid \overset{E}{x}) \cdot \frac{1}{2}$$

$$+ P(\overset{E}{y} \mid \overset{A}{0})\, P(\overset{B}{1} \mid \overset{E}{y}) \cdot \frac{1}{2}$$

$$= \frac{1}{2} \cdot 2 \sin^2\theta \cos^2\theta = \frac{1}{4} \sin^2 2\theta .$$