Solution de la série 5
Traitement Quantique de l'Information

Exercice 1 *Bennett 1992 Protocol.*

Key Generation : When $d_i = e_i$, i.e. Bob measures the qubit in the same basis than the preparation basis of Alice. In other words if the transmitted qubit state is $|0\rangle$ and the measurement is in the Z-basis then this yields a measurement result $|0\rangle$ with probability 1. A similar argument holds for if the transmitted quit is $H|0\rangle$. Thus when $d_i = e_i$ we certainly have $y_i = 0$. So

$$\mathbb{P}(y_i = 0|d_i = e_i) = 1, \qquad \mathbb{P}(y_i = 1|d_i = e_i) = 0.$$

When $d_i \neq e_i$ then, for example, the transmitted state is $|\psi\rangle = H|0\rangle$ but the measurement is done in the Z-basis which results in $|0\rangle$ or $|1\rangle$ with equal probability because $|\langle 0|\psi\rangle|^2 = |\langle 1|\psi\rangle|^2 = (1/\sqrt{2})^2 = 1/2$. So

$$\mathbb{P}(y_i = 0|d_i \neq e_i) = \frac{1}{2}, \qquad \mathbb{P}(y_i = 1|d_i \neq e_i) = \frac{1}{2}.$$

We observe from the abaove analysis that $y_i = 1$ only when $d_i \neq e_i$. The secret key is then generated as folllows : Alice and Bob reveal the y_i's and keep the $e_i = 1 - d_i$ such that $y_i = 1$ as their secret bits. The other e_i and d_i are discarded. Indeed if $y_i = 1$ then Alice and Bob know that $e_i = 1 - d_i$ for sure, i.e

$$\mathbb{P}(e_i = 1 - d_i|y_i = 1) = 1.$$

This can be proved more formally from Bayes rule :

$$\mathbb{P}(e_i = 1 - d_i|y_i = 1) = \frac{\mathbb{P}(y_i = 1|e_i = 1 - d_i)\mathbb{P}(e_i = 1 - d_i)}{\mathbb{P}(y_i = 1)} = \frac{\frac{1}{2} \times \frac{1}{2}}{\frac{1}{4}} = 1$$

In the last equality we used

$$\begin{aligned}\mathbb{P}(y_i = 1) &= \mathbb{P}(y_i = 1|e_i = d_i)\mathbb{P}(e_i = d_i) + \mathbb{P}(y_i = 1|e_i \neq d_i)\mathbb{P}(e_i \neq d_i) \\ &= 0 \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}.\end{aligned}$$

Here we have assumed that $\mathbb{P}(e_i \neq d_i) = \mathbb{P}(e_i = d_i) = \frac{1}{2}$ (but observe that the result holds in general even without this assumption).

The length of the resulting secret key is around $N\,\mathbb{P}(y_i = 1) = \frac{N}{4}$, a quarter of the length of the main sequence.

We observe a few differences with respect to BB84. First the common secret bits are here constituted from a subset of the encoding and decoding bits. Second the length of the secret

key is halfed with respect to BB84. However the main advantage of BB92 over BB84 is that in BB92 we have to manipulate only two (non-orthogonal states) instead of four in BB84.

Security Check : Alice and Bob can do a security check by exchanging a small fraction of the secure bits via public channel. If the test is successful they keep the rest of the common substring secure : thus they have succeeded in generating a common secure string. If there is no attack from Eve's side and the transmission channel is perfect, then as we explained we have $e_i = 1 - d_i$ whenever $y_i = 1$. The test is :

$$\mathbb{P}(e_i = 1 - d_i | y_i = 1) = 1.$$

Eve's Attack : Here we discuss only one plausible strategy of Eve. Note that we could devise other strategies for Eve but this will not help. If you wish you can devise your own strategy and see how the security criterion is affected.

Alice sends the states $H^{e_i}|0\rangle$ through the optic fiber. Suppose Eve captures a photon and makes a measurement in the Z or the X basis. Let $E_i = 0, 1$ denote the choice of Z or X basis for Eve.

If Eve chooses the Z basis ($E_i = 0$) she finds the result of the measurement $|0\rangle$ or $|1\rangle$. If she finds $|0\rangle$ she sends this state to Bob. If she finds $|1\rangle$ she deduces that certainly Alice did not send the state $|0\rangle$, and that Alice must have sent the state $H|0\rangle$ or that she (Eve) must have chosen the wrong measurement basis. She decides to send $H|0\rangle$ to Bob (another strategy would be to decide that the basis was wrong and that Alice sent $|0\rangle$).

If Eve chooses the X basis ($E_i = 1$) she finds the result of the measurement $H|0\rangle$ or $H|1\rangle$. If she finds $H|0\rangle$ she sends this state to Bob. If she finds $H|1\rangle$ she deduces that certainly Alice did not send the state $H|0\rangle$ and that he must have sent the state $|0\rangle$, or that she (Eve) chose the wrong measurement basis,. She decides to send $|0\rangle$ to Bob (another strategy would be to decide that the basis was wrong and that Alice sent $|0\rangle$).

Let us summarize what Bob receives. We see that when $E_i = e_i$ Bob certainly receives the states $H^{E_i}|0\rangle$. But when $E_i \neq e_i$ Bob receives $H^{E_i}|0\rangle$ with probability $1/2$ and $H^{e_i}|0\rangle$ with probability $1/2$.

Now Bob decodes and finds the states $\{H^{d_i}|y_i\rangle, y_i = 0, 1\}$ ($d_i = 0, 1$ fixed according to the measurement basis chosen). From the measurement postulate

$$\mathbb{P}(y_i | d_i, E_i = e_i) = |\langle y_i | H^{d_i + E_i} | 0 \rangle|^2$$

and

$$\mathbb{P}(y_i | d_i, E_i \neq e_i) = \frac{1}{2} |\langle y_i | H^{d_i + E_i} | 0 \rangle|^2 + \frac{1}{2} |\langle y_i | H^{d_i + e_i} | 0 \rangle|^2$$

In particular given $d_i = 1 - e_i$ we have

$$\mathbb{P}(y_i = 1 | d_i = 1 - e_i, E_i = e_i) = |\langle 1 | H | 0 \rangle|^2 = \frac{1}{2}$$

and

$$\mathbb{P}(y_i = 1 | d_i = 1 - e_i, E_i \neq e_i) = \frac{1}{2} |\langle 1 | H^0 | 0 \rangle|^2 + \frac{1}{2} |\langle 1 | H | 0 \rangle|^2 = \frac{1}{4}$$

Thus

$$\begin{aligned}\mathbb{P}(y_i = 1|e_i = 1 - d_i) &= \frac{1}{2}\mathbb{P}(E_i = e_i) + \frac{1}{4}\mathbb{P}(E_i \neq e_i) \\ &= \frac{1}{4} + \frac{1}{4}\mathbb{P}(E_i = e_i)\end{aligned}$$

Since Eve has no information on the Bernoulli choices of Alice the maximum is attained for $\mathbb{P}(E_i = e_i) \leq 1/2$ (see at the end for a detailed justification) so $\mathbb{P}(y_i = 1|e_i = 1 - d_i) \leq 3/8$.

Now let us look at the security criterion. By Bayes rule :

$$\mathbb{P}(e_i = 1 - d_i|y_i = 1) = \frac{\mathbb{P}(y_i = 1|e_i = 1 - d_i)\mathbb{P}(e_i = 1 - d_i)}{\mathbb{P}(y_i = 1)}$$

For the denominator we use (we asume that Eve's choice of E_i is independent of Alice's and Bob's choices of e_i and d_i)

$$\begin{aligned}\mathbb{P}(y_i = 1) &= \mathbb{P}(y_i = 1|d_i = e_i, E_i = e_i)\mathbb{P}(d_i = e_i)\mathbb{P}(E_i = e_i) \\ &+ \mathbb{P}(y_i = 1|d_i \neq e_i, E_i = e_i)\mathbb{P}(d_i \neq e_i)\mathbb{P}(E_i = e_i) \\ &+ \mathbb{P}(y_i = 1|d_i = e_i, E_i \neq e_i)\mathbb{P}(d_i = e_i)\mathbb{P}(E_i \neq e_i) \\ &+ \mathbb{P}(y_i = 1|d_i \neq e_i = 1 - e_i, E_i \neq e_i)\mathbb{P}(d_i \neq e_i)\mathbb{P}(E_i \neq e_i) \\ &= 0\,\mathbb{P}(d_i = e_i)\mathbb{P}(E_i = e_i) + \frac{1}{2}\mathbb{P}(d_i \neq e_i)\mathbb{P}(E_i = e_i) + \frac{1}{4}\mathbb{P}(d_i = e_i)\mathbb{P}(E_i \neq e_i) \\ &+ \frac{1}{4}\mathbb{P}(d_i \neq e_i)\mathbb{P}(E_i \neq e_i) \\ &= \frac{1}{4}\mathbb{P}(E_i = e_i) + \frac{1}{4}\mathbb{P}(E_i \neq e_i) \\ &= \frac{1}{4}\end{aligned}$$

where we suppose $\mathbb{P}(e_i = d_i) = \mathbb{P}(e_i \neq d_i) = 1/2$ and the strategy of Eve is arbitrary.

Putting these results all together we obtain :

$$\begin{aligned}\mathbb{P}(e_i = 1 - d_i|y_i = 1) &= \frac{(\frac{1}{4} + \frac{1}{4}\mathbb{P}(E_i = e_i))\mathbb{P}(e_i = 1 - d_i)}{\frac{1}{4}} \\ &= \frac{1}{2}(1 + \mathbb{P}(E_i = e_i))\end{aligned}$$

Since Eve has no information on the Bernoulli choices of Alice ($e_i = 0, 1$) we have $\mathbb{P}(E_i = e_i) \leq 1/2$. Indeed

$$\begin{aligned}\mathbb{P}(E_i = e_i) &= \mathbb{P}(E_i = 0, e_i = 0) + \mathbb{P}(E_i = 1, e_i = 1) \\ &= \mathbb{P}(E_i = 0)\mathbb{P}(e_i = 0) + \mathbb{P}(E_i = 1)\mathbb{P}(e_i = 1) \\ &= \frac{1}{2}(\mathbb{P}(E_i = 0) + \mathbb{P}(E_i = 1)) \\ &\leq \frac{1}{2}.\end{aligned}$$

Thus in the presence of Eve we always have :

$$\mathbb{P}(e_i = 1 - d_i|y_i = 1) \leq \frac{3}{4}$$

and Alice and Bob can detect her attack.

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

a) Pour passer de 0 à 2 il y a trois "chemins classiques" possibles (ou trois "transitions" possibles) $0 \to 0 \to 2$ ou $0 \to 1 \to 2$ ou $0 \to 2 \to 2$. Les probabilités associées à chaque chemin classique sont (respectivement) $Q_{20}P_{00}$, $Q_{21}P_{10}$, $Q_{22}P_{20}$. Donc la probabilité d'observer l'état 2 à la sortie est la somme des trois probabilités correspondantes :

$$\text{Prob}(2) = Q_{20}P_{00} + Q_{21}P_{10} + Q_{22}P_{20}.$$

b) Pour montrer que $|\langle j| U |i\rangle|^2 = R_{ji}$ est une matrice stochastique, il faut verifier que $\sum_{j=0}^{n-1} R_{ji} = 1$ et $0 \leq R_{ji} \leq 1$ (ici $U = U_1$ ou $U = U_2$; la preuve est la même).

$$\begin{aligned}\sum_{j=0}^{2} R_{ji} &= \sum_{j=0}^{2} |\langle j| U |i\rangle|^2 = \sum_{j=0}^{2} \langle i| U^\dagger |j\rangle \langle j| U |i\rangle \\ &= \langle i| U^\dagger \sum_{j=0}^{n-1} |j\rangle \langle j| U |i\rangle = \langle i| U^\dagger U |i\rangle \\ &= \langle i| i\rangle = 1\end{aligned}$$

Pour la deuxième égalité nous avons utilisé lídentité

$$\sum_{j=0}^{2} |j\rangle\langle j| = I$$

ou I est la matrice identité (ici l'identité 3×3). Cette relation discutée en cours s'appelle la "relation de fermeture" (dans la literature quantique) et suit simplement de l'orthonormalité de la base $\{|j\rangle, j = 0, 1, 2\}$. Pour l'avant dernière égalité nous avons utilisé l'unitarité de la matrice d'évolution : $U^\dagger U = UU^\dagger = I$.

Notez aussi que tous les termes $|\langle j| U |i\rangle|^2$ sont positifs et se somment à un. c'est pourquoi $0 \leq R_{ji} \leq 1$.

c) Dans le cas quantique létat évolue de facon unitaire. L'état initial est $|0\rangle$. Après la première étape létat est $U_1|0\rangle$. Après la deuxieme étape l'état est $U_2U_1|0\rangle$.

Lors d'une mesure dans la base $\{|0\rangle, |1\rangle, |2\rangle\}$ la probabilité d'observer l'état $|2\rangle$ à la sortie est :

$$\text{Prob}(|2\rangle) = |\langle 2| U_2U_1 |0\rangle|^2$$

Regardons cette expressiond de plus près. On a

$$\begin{aligned}\text{Prob}(|2\rangle) = |\langle 2| U_2U_1 |0\rangle|^2 &= \langle 2| U_2U_1 |0\rangle \langle 0| U_1^\dagger U_2^\dagger |2\rangle \\ &= \sum_{i=0}^{2}\sum_{j=0}^{2} \langle 2| U_2 |i\rangle \langle i| U_1 |0\rangle \langle 0| U_1^\dagger |j\rangle \langle j| U_2^\dagger |2\rangle \\ &= \sum_{i=j} \langle 2| U_2 |i\rangle \langle i| U_1 |0\rangle \langle 0| U_1^\dagger |i\rangle \langle i| U_2^\dagger |2\rangle \\ &\quad + \sum_{i\neq j} \langle 2| U_2 |i\rangle \langle i| U_1 |0\rangle \langle 0| U_1^\dagger |j\rangle \langle j| U_2^\dagger |2\rangle\end{aligned}$$

Notez dans ce résultat final que la première somme sur $i = j$ est la probabilité d'observer l'état 2 à la sortie dans le cas classique. En effet :

$$\sum_{i=0}^{2} \langle 2| U_2 |i\rangle \langle i| U_1 |0\rangle \langle 0| U_1^\dagger |i\rangle \langle i| U_2^\dagger |2\rangle = \sum_{i=0}^{2} |\langle 2| U_2 |i\rangle|^2 |\langle i| U_1 |0\rangle|^2$$
$$= P_{00}Q_{20} + P_{10}Q_{21} + P_{20}Q_{22}$$

La deuxième somme sur $i \neq j$ est un terme d'interférence purement quantique qui est du au fait que la dynamique quantique (l'évolution unitaire) explore tous les états du système à la fois.

d) En faisant la mesure intermédiaire après la première étape on observe :

- $|0\rangle$ avec la probabilité $|\langle 0| U_1 |0\rangle|^2$,
- $|1\rangle$ avec la probabilité $|\langle 1| U_1 |0\rangle|^2$,
- $|2\rangle$ avec la probabilité $|\langle 2| U_1 |0\rangle|^2$.

Ensuite

- Quand létat à la prmi‘ere mesure est réduit à $|0\rangle$ alors à la deuxième étape létat sera $U_2|0\rangle$. La probabilité d'observer $|2\rangle$ est alors $|\langle 2|U_2|0\rangle|^2$.
- Quand létat à la prmi‘ere mesure est réduit à $|1\rangle$ alors à la deuxième étape létat sera $U_2|1\rangle$. La probabilité d'observer $|2\rangle$ est alors $|\langle 2|U_2|1\rangle|^2$.
- Quand létat à la prmi‘ere mesure est réduit à $|2\rangle$ alors à la deuxième étape létat sera $U_2|2\rangle$. La probabilité d'observer $|2\rangle$ est alors $|\langle 2|U_2|2\rangle|^2$.

Ainsi la probabilité totale d'observer $|2\rangle$ lors de la mesure finale, étant donné que l'on a fait une mesure intermédaire, est

$$|\langle 0| U_1 |0\rangle|^2 |\langle 2| U_2 |0\rangle|^2 + |\langle 1| U_1 |0\rangle|^2 |\langle 2| U_2 |1\rangle|^2 + |\langle 2| U_1 |0\rangle|^2 |\langle 2| U_2 |2\rangle|^2$$

Ce résultat est le même que dans le cas classique.

e) Cet exercice est un analogue discret de l'expérience des franges d'interférence de Young sauf qu'il y a trois fentes (les états intermédiaires). L'écran est ici représenté par les trois états finaux. Lorsque on laisse évoluer le système sans l'observer (le système est complètement isolé de l'environement) la probabilité finale comporte un terme classique plus un terme d'interférence. Lorsque le systeème n'est pas isolé de son environement et que nous observons létat intermédiaire (en faisant une mesure) le terme d'interférence est détruit. Lors de l'observation intermédiaire nous détruisons la superposition quantique (on dit aussi que l'on détruit la “cohérence” quantique) de l'état intermédiaire $U_1|0\rangle$.