Exercice 1 *Protocole de téléportation quantique*

1. L'opération CNOT permet de changer l'état du second qu-bit seulement si l'état du premier qu-bit est $|1\rangle$. L'état $|\Psi_1\rangle$ obtenu après application de cette opération sur $|\Psi_0\rangle$ est :

$$|\Psi_1\rangle = \alpha|0\rangle \otimes \frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}} + \beta|1\rangle \otimes \frac{|1\rangle|0\rangle + |0\rangle|1\rangle}{\sqrt{2}}. \tag{1}$$

2. L'état $|\Psi_2\rangle$ obtenu après application d'une porte de Hadamard sur la premier qu-bit est :

$$\begin{aligned}|\Psi_2\rangle &= \alpha\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|1\rangle|0\rangle + |0\rangle|1\rangle}{\sqrt{2}} \\ &= \frac{1}{2}|00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}|01\rangle \otimes (\alpha|1\rangle + \beta|0\rangle) \\ &\quad + \frac{1}{2}|10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) + \frac{1}{2}|11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle)\end{aligned} \tag{2}$$

3. Le processus de mesure projette l'état $|\Psi_2\rangle$ sur le résultat mesuré.
   - Pour $(x, y) = (0, 0)$, l'état après la mesure est $|0\rangle_1|0\rangle_2(\alpha|0\rangle_3 + \beta|1\rangle_3)$
   - Pour $(x, y) = (0, 1)$, l'état après la mesure est $|0\rangle_1|1\rangle_2(\alpha|1\rangle_3 + \beta|0\rangle_3)$
   - Pour $(x, y) = (1, 0)$, l'état après la mesure est $|1\rangle_1|0\rangle_2(\alpha|0\rangle_3 - \beta|1\rangle_3)$
   - Pour $(x, y) = (1, 1)$, l'état après la mesure est $|1\rangle_1|1\rangle_2(\alpha|1\rangle_3 - \beta|0\rangle_3)$
4. Le qu-bit de Bob sera dans l'état $|\psi\rangle$ si $(x, y) = (0, 0)$. Il est facile de voir qu'il devra par contre appliquer σ_x si $(x, y) = (0, 1)$, σ_z si $(x, y) = (1, 0)$, et $\sigma_z\sigma_x$ si $(x, y) = (1, 1)$, afin de placer son qu-bit dans l'état $|\psi\rangle$. De manière générale, Bob doit donc appliquer l'opération $\sigma_z^x\sigma_x^y$ à son qu-bit.
5. Le téléportation se fait sans transfert de matière dans le sens où Alice garde ses qu-bits physiques ; c'est l'état $|\psi\rangle$ (autrement dit l'information quantique) qui est transmise d'Alice vers Bob.
6. Un théorème fondamental de théorie de l'information quantique stipule qu'il est impossible de dupliquer ("cloner") de l'information quantique ; ici, on vérifie qu'à aucun moment du protocole deux qu-bits distincts ne sont dans l'état $|\psi\rangle$ au même moment : en effet, lorsque Bob a reconstitué $|\psi\rangle$ sur son qu-bit, Alice a perdu toute l'information relative aux coefficients α et β, puisqu'elle ne dispose plus que de $|00\rangle$, ou de $|01\rangle$, etc.
7. Le transfert d'information n'est pas supraluminique. Il est limité par la vitesse de transfert à Bob du résultat (x, y) de la mesure effectuée par Alice.

Exercice 2 *Protocle cryptographique BB84*

Remarque : Notez que l'on a associé les 0,1 aux états $|+\rangle$ et $|-\rangle$ respectivement, contrairement à la série originale traitée en séance d'exercices. Il s'agit simplement de la convention la plus usuelle, mais ceci ne change pas les résultats de l'exercice. L'énoncé de la série 11 a été mis à jour conformément à cette convention.

1. Le tableau des séquences et des résultats possibles :

a_i	0	1	1	0	1	1	0	0	0
b_i	0	0	1	0	1	1	1	0	1
Etat	$\|+_z\rangle$	$\|-_z\rangle$	$\|-_x\rangle$	$\|+_z\rangle$	$\|-_x\rangle$	$\|-_x\rangle$	$\|+_x\rangle$	$\|+_z\rangle$	$\|+_x\rangle$
b'_i	0	1	0	0	1	1	0	0	1
Base de mesure (Bob)	z	x	z	z	x	x	z	z	x
Résultats possibles	0	0 ;1	0 ;1	0	1	1	0 ;1	0	0
Probabilités	1	0.5 ;0.5	0.5 ;0.5	1	1	1	0.5 ;0.5	1	1

2. Le tableau précédent montre que $a'_i = a_i$ lorsque $b'_i = b_i$. Ainsi, dans les séquences retenues par Alice et Bob, $a'_i = a_i$, $\forall i$. Cette procédure leur permettra donc de partager une séquence commune en guise de clé.

3. La longueur de la clé partagée est donnée par $\#\{i|b_i = b'_i\}$. Si X désigne la variable aléatoire donnant la longueur de la clé, alors la probabilité que $X = k$ correspond à la probabilité de choisir k indices i tels que $b'_i = b_i$ et de choisir différemment les $N - k$ composantes restantes. Les choix 0 ou 1 étant équiprobables, la probabilité que $X = k$ pour une configuration donnée est de $\left(\frac{1}{2}\right)^k \left(\frac{1}{2}\right)^{N-k}$. Pour tenir compte des multiples configurations possibles de longueur k, il faut multiplier le tout par $\binom{N}{k}$. Ainsi, la probabilité $P(X = k)$ s'écrit finalement :

$$P(X = k) = \binom{N}{k} \left(\frac{1}{2}\right)^k \left(\frac{1}{2}\right)^{N-k} \tag{3}$$

ce qui est bien une loi binomiale $B(N, \frac{1}{2})$. L'espérance de X est ainsi N/2. Ceci est le résultat intuitivement attendu. De plus, pour N grand, la largeur relative de la distribution $\frac{\sqrt{Var(X)}}{E(X)} \to 0$, c.à.d qu'on doit obtenir presque toujours N/2 coïncidences, ce qui corrobore le résultat attendu.

4. La probabilité $P(b''_i \neq b_i)$ pour un i donné est $1/2$.

5. On considère le cas $b_1 = b'_1 = 0$, $a_1 = 0$. Sans intervention d'Eve, le résultat de Bob est $a'_1 = 0$ avec probabilité 1. Eve ayant $b''_1 = 1$, le résultat de sa mesure est 0 ou 1 avec probabilité $1/2$. Eve envoie ensuite à Bob un état propre de $\hat{S}_x$, résultat de sa mesure. Bob mesurera ainsi, après intervention d'Eve, 0 ou 1 avec probabilité $1/2$, puisque sa base de mesure est z. L'intervention d'Eve modifie donc la distribution de probabilité des résultats possibles de Bob. Dans un système supposé parfait, seul un espionnage justifie l'obtention de $P(a'_i \neq a_i|b'_i = b_i) \neq 0$.

6. Il est facile de constater tout d'abord que $P(a'_i \neq a_i|b'_i = b_i) = 1/4$ pour i appartenant à la séquence des indices tels que $b'_i = b_i$. En effet, pour un indice i, Eve a une probabilité $1/2$ de choisir une base différente de la base commune de Bob et Alice. De plus, Bob a une probabilité $1/2$ de mesurer "la mauvaise projection" de l'état propre envoyé par Eve, et donc d'obtenir $a'_i \neq a_i$. D'où le résultat. Ainsi, $P(a'_i = a_i|b'_i = b_i) = 3/4$. Et donc pour une séquence de longueur n, $P(\forall i, a'_i = a_i|b'_i = b_i) = (3/4)^n \underset{n\to\infty}{\longrightarrow} 0$. Ainsi plus n est grand, plus il sera difficile pour Eve d'espionner sans être détectée.