.

Solution de la série 6
Traitement Quantique de l'Information

Exercice 1 *Bennett 1992 Protocol.*

Key Generation : From the explanation, it is clear that when $d_i = e_i$, Bob measures the qubit in the same basis that they are transmitted, i.e. the transmitted qbit state is $|0\rangle$ and the measurement is done in Z-basis which gives $|0\rangle$ with probability 1. A similar argument holds for $H|0\rangle$. Thus when $d_i = e_i$ we certainly have $y_i = 0$. In other words $\mathbb{P}(y_i = 0|d_i = e_i) = 1$ and $\mathbb{P}(y_i = 1|d_i = e_i) = 0$. However, 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 $|\langle 0|\psi\rangle|^2 = |\langle 1|\psi\rangle|^2 = (1/\sqrt{2})^2 = 1/2$. In other words $\mathbb{P}(y_i = 0|d_i \neq e_i) = \frac{1}{2}$ and $\mathbb{P}(y_i = 1|d_i \neq e_i) = \frac{1}{2}$.

We observe 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 a secret key. The other e_i and d_i are discarded. Indeed if $y_i = 1$ the Alice and Bob know that $e_i = 1 - d_i$ for sure. This can be proved from the 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 equalirty 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 $\mathbb{P}(e_i \neq d_i) = \mathbb{P}(e_i = d_i) = \frac{1}{2}$.

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.

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 the measurement attack. 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. If she chooses the Z basis 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 Bob did not send the state $|0\rangle$, and that he must have sent the state $H|0\rangle$. She sends $H|0\rangle$ to Bob. If Eve chooses the X basis 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 Bob did not send the state $H|0\rangle$, and that he must have sent the state $|0\rangle$. She sends $|0\rangle$ to Bob. Let $E_i = 0, 1$ denote the choice of Z or X basis for Eve.

Note that we could devise other startegies for Eve but this will not help. If you wish you can devise your own strategy and see how the security criterion is affceted. Here we stick to the above strategy for Eve. Summarizing, we see that Bob receives the states $H^{e_i+E_i}|0\rangle$.

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

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

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

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

Thus

$$\begin{aligned}\mathbb{P}(y_i = 1|e_i = 1 - d_i) &= |\langle 1|H|0\rangle|^2 p(E_i = 0) + |\langle 1|H^2|0\rangle|^2 \mathbb{P}(E_i = 1) \\ &= \frac{1}{2}\mathbb{P}(E_i = 0)\end{aligned}$$

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)

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

For the numerator,

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

Putting these results alltogether we obtain :

$$\mathbb{P}(e_i = 1 - d_i|y_i = 1) = \frac{\frac{1}{2}\mathbb{P}(E_i = 0)\mathbb{P}(e_i = 1 - d_i)}{\frac{1}{2}} = \mathbb{P}(E_i = 0)\mathbb{P}(e_i = 1 - d_i)$$

Supposing that $\mathbb{P}(e_i \neq d_i) = \frac{1}{2}$ we see that $\mathbb{P}(e_i = 1 - d_i|y_i = 1) \leq \frac{1}{2}$ whatever is Eve's strategy for the choice of measurement basis $E_i = 0, 1$.

Exercice 2

1. One has to show that $\left\langle B_{x,y}\right| \left. B_{x',y'}\right\rangle = \delta_{x,x'}\delta_{y,y'}$. We show it explicitly for two cases :

$$\begin{aligned}\langle B_{00}|\ B_{00}\rangle &= \frac{1}{2}(\langle 00| + \langle 11|)(|00\rangle + |11\rangle) \\ &= \frac{1}{2}(\langle 00|\ 00\rangle + \langle 00|\ 11\rangle + \langle 11|\ 00\rangle + \langle 11|\ 11\rangle).\end{aligned}$$

   Now we have

$$\begin{aligned}\langle 00|\ 00\rangle = \langle 0|\ 0\rangle \langle 0|\ 0\rangle = 1, \langle 00|\ 11\rangle = \langle 0|\ 1\rangle \langle 0|\ 1\rangle = 0, \\ \langle 11|\ 00\rangle = \langle 1|\ 0\rangle \langle 1|\ 0\rangle = 0, \langle 11|\ 11\rangle = \langle 1|\ 1\rangle \langle 1|\ 1\rangle = 1.\end{aligned}$$

   Thus we get that $\langle B_{00}|\ B_{00}\rangle = \frac{1}{2}(1+0+0+1) = 1$. Now let us consider

$$\begin{aligned}\langle B_{00}|\ B_{01}\rangle &= \frac{1}{2}(\langle 00| + \langle 11|)(|01\rangle + |10\rangle) \\ &= \frac{1}{2}(\langle 00|\ 01\rangle + \langle 00|\ 10\rangle + \langle 11|\ 01\rangle + \langle 11|\ 10\rangle) \\ &= \frac{1}{2}(0+0+0+0) = 0.\end{aligned}$$

2. The proof is by contradiction. Suppose there exist a_1, b_1 and a_2, b_2 such that

$$|B_{00}\rangle = (a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle).$$

   Then we must have

$$\frac{1}{2}(|00\rangle + |11\rangle) = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + a_2b_2|11\rangle .$$

   Since the states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ form a basis one has

$$\frac{1}{2} = a_1a_2,\ \frac{1}{2} = b_1b_2,\ a_1b_2 = 0,\ b_1a_2 = 0.$$

   The third equality indicates that either $a_1 = 0$ or $b_2 = 0$ (or both). If $a_1 = 0$ we get a contradiction with the first equation. If on the other hand $b_2 = 0$, we get a contradiction with the second one. Therefore, there does not exist $|\psi_1\rangle$ and $|\psi_2\rangle$ such that $|B_{00}\rangle$ can be written as $|\psi_1\rangle \otimes |\psi_2\rangle$. Therefore, B_{00} is entangled.

3. We have

$$\begin{aligned}|\gamma\rangle \otimes |\gamma\rangle &= (\cos(\gamma)|0\rangle + \sin(\gamma)|1\rangle) \otimes (\cos(\gamma)|0\rangle + \sin(\gamma)|1\rangle) \\ &= \cos^2(\gamma)|00\rangle + \cos(\gamma)\sin(\gamma)|01\rangle + \sin(\gamma)\cos(\gamma)|10\rangle + \sin^2(\gamma)|11\rangle .\end{aligned}$$

   Similarly,

$$|\gamma_\perp\rangle \otimes |\gamma_\perp\rangle = \cos^2(\gamma_\perp)|00\rangle + \cos(\gamma_\perp)\sin(\gamma_\perp)|01\rangle + \sin(\gamma_\perp)\cos(\gamma_\perp)|10\rangle + \sin^2(\gamma_\perp)|11\rangle .$$

   A picture shows that $\cos(\gamma_\perp) = -\sin(\gamma)$ and $\sin(\gamma_\perp) = \cos(\gamma)$ (this also allows to check that $\langle\gamma|\ \gamma_\perp\rangle = 0$). Therefore, $\cos^2(\gamma_\perp) = \sin^2(\gamma)$, $\sin^2(\gamma_\perp) = \cos^2(\gamma)$ and $\cos(\gamma_\perp)\sin(\gamma_\perp) = -\cos(\gamma)\sin(\gamma)$. We find that

$$|\gamma\rangle \otimes |\gamma\rangle + |\gamma_\perp\rangle \otimes |\gamma_\perp\rangle = (\cos^2(\gamma) + \sin^2(\gamma))|00\rangle + (\sin^2(\gamma) + \cos^2(\gamma))|11\rangle ,$$

   and the terms $|01\rangle$ and $|10\rangle$ cancel. Finally,

$$\frac{1}{\sqrt{2}}(|\gamma\rangle \otimes |\gamma\rangle + |\gamma_\perp\rangle \otimes |\gamma_\perp\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |B_{00}\rangle .$$

4. From the rule for the tensor product

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a \begin{pmatrix} c \\ d \end{pmatrix} \\ \\ b \begin{pmatrix} c \\ d \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix},$$

we get for the basis states

$$|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \qquad |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$|1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \qquad |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Thus,

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix},$$

$$|B_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix},$$

$$|B_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix},$$

$$|B_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}.$$

Exercice 3

1. By definition of the tensor product :

$$(H \otimes I) |x\rangle \otimes |y\rangle = H |x\rangle \otimes I |y\rangle = H |x\rangle \otimes |y\rangle .$$

Also, one can use that $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ to show that always

$$H |x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x |1\rangle).$$

Thus,

$$(H \otimes I) |x\rangle \otimes |y\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |y\rangle + (-1)^x |1\rangle \otimes |y\rangle).$$

Now we apply *'CNOT'*. By linearity, we can apply it to each term separately. Thus,

$$\begin{aligned}(CNOT)(H \otimes I) |x\rangle \otimes |y\rangle &= \frac{1}{\sqrt{2}}((CNOT) |0\rangle \otimes |y\rangle + (-1)^x (CNOT) |1\rangle \otimes |y\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle \otimes |y\rangle + (-1)^x |1\rangle \otimes |y \oplus 1\rangle) \\ &= |B_{xy}\rangle .\end{aligned}$$

2. Let us first start with $H \otimes I$. We use the rule

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae & af & be & bf \\ ag & ah & bg & bh \\ ce & cf & de & df \\ cg & ch & dg & dh \end{pmatrix},$$

Thus we have

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

For (CNOT), we use the definition :

$$(CNOT) |x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus x\rangle ,$$

which implies that the matrix elements are

$$\langle x'y' | \, CNOT \, |xy\rangle = \langle x', y' | x, y \otimes x\rangle = \langle x' | \, x\rangle \, \langle y' | \, y \oplus x\rangle = \delta_{xx'} \delta_{y \oplus x, y'}.$$

We obtain the following table with columns xy and rows $x'y'$:

	00	01	10	11
00	1	0	0	0
01	0	1	0	0
10	0	0	0	1
11	0	0	1	0

For the matrix product $(CNOT)(H \otimes I)$, we find that

$$\begin{aligned}(CNOT)H \otimes I &= \frac{1}{\sqrt{2}} \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix} \begin{pmatrix} I & I \\ I & -I \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} I & I \\ X & -X \end{pmatrix},\end{aligned}$$

where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Thus,

$$(CNOT)(H \otimes I) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}.$$

One can check that for example $|B_{00}\rangle = (CNOT)(H \otimes I)\,|0\rangle \otimes |0\rangle$. Finally to check the unitarity, we have to check that $UU^\dagger = U^\dagger U = I$ for $U = H \otimes I$, $CNOT$ and $(CNOT)(H \otimes I)$. We leave this to the reader.

3. Let $U = (CNOT)(H \otimes I)$. We have

$$|B_{xy}\rangle = U\,|x\rangle \otimes |y\rangle\,, \langle B_{x'y'}| = \langle x'| \otimes \langle y'|\, U^\dagger.$$

Thus,

$$\begin{aligned}\langle B_{x'y'}|\, B_{xy}\rangle &= \langle x'| \otimes \langle y'|\, U^\dagger U\,|x\rangle \otimes |y\rangle \\ &= \langle x'| \otimes \langle y'|\, I\,|x\rangle \otimes |y\rangle \\ &= \langle x'|\, x\rangle\, \langle y'|\, y\rangle = \delta_{xx'}\delta_{yy'}.\end{aligned}$$