Homework 7: Solutions
Quantum Information Processing

Exercise 1 *Bennett 1992 Protocol for quantum key distribution*

1) When $d_i = e_i$, Bob measures the qubit in the same basis as the preparation basis used by Alice. In other words if $e_i = d_i = 0$ 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 if $e_i = d_i = 1$ and the transmitted qubit is $H|0\rangle$ and the measurement is in the X-basis which yields a measurement result $H|0\rangle$ with probability 1. Thus when $d_i = e_i$ we certainly have $y_i = 0$. So

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

When $d_i \neq e_i$ then, for example $e_i = 1$ and $d_i = 0$, 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

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

2) We observe from the above analysis that $y_i = 1$ only when $d_i \neq e_i$. Indeed if $y_i = 1$ then Alice and Bob know that $e_i = 1 - d_i$ for sure, i.e.

$$P(e_i = 1 - d_i|y_i = 1) = 1.$$

This can be proved more formally from Bayes' rule:

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

where for the denominator we used

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

Here we have assumed that $P(e_i \neq d_i) = P(e_i = d_i) = \frac{1}{2}$.

3) The secret key is then generated as follows: 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. The length of the resulting secret key is around $N \times P(y_i = 1) = N/4$, 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 halved with respect to BB84. However the main advantage of BB92 over BB84 is that in BB92 we manipulate only two non-orthogonal states instead of four in BB84.

4) Alice and Bob can do a security check by exchanging a small fraction $\epsilon N/4$, $0 < \epsilon \ll 1$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 should check that

$$P(e_i = 1 - d_i | y_i = 1) = 1.$$

In practice Alice and Bob check that

$$\#(i \text{ such that } e_i = 1 - d_i \text{ given that } y_i = 1) = \epsilon N/4$$

which means that the empirical probability is one.

Exercise 2 *Copying or unitary attack from Eve in BB84*

1) Given Alice sent $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, by linearity, the state of the two photons in the lab of Eve just after she made the copying operation is

$$\begin{aligned}
|\Psi\rangle &= U_Z \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |b\rangle \right) \\
&= U_Z \frac{|0\rangle \otimes |b\rangle}{\sqrt{2}} + U_Z \frac{|1\rangle \otimes |b\rangle}{\sqrt{2}} \\
&= \frac{|0\rangle \otimes |0\rangle}{\sqrt{2}} + \frac{|1\rangle \otimes |1\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.
\end{aligned}$$

2) In Bob's lab the outcome is $\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$ with probabilities $p_\pm = \langle \Psi | \Pi_\pm | \Psi \rangle$, where $|\Psi\rangle$ is given in Solution 3.1.

Following the hint, we have

$$\begin{aligned}
\Pi_\pm &= (|0\rangle \langle 0| + |1\rangle \langle 1|) \otimes \left(\frac{|0\rangle \pm |1\rangle}{\sqrt{2}} \right) \left(\frac{\langle 0| \pm \langle 1|}{\sqrt{2}} \right) \\
&= (|0\rangle \langle 0| + |1\rangle \langle 1|) \otimes \left(\frac{|0\rangle \langle 0| \pm |0\rangle \langle 1| \pm |1\rangle \langle 0| + |1\rangle \langle 1|}{2} \right) \\
&= \frac{1}{2} \big(|00\rangle \langle 00| \pm |00\rangle \langle 01| \pm |01\rangle \langle 00| + |01\rangle \langle 01| \\
&\qquad + |10\rangle \langle 10| \pm |10\rangle \langle 11| \pm |11\rangle \langle 10| + |11\rangle \langle 11| \big).
\end{aligned}$$

The rest of the calculation is

$$\begin{aligned}
\Pi_\pm |\Psi\rangle &= \frac{1}{2\sqrt{2}} \left(|00\rangle \pm |01\rangle \pm |10\rangle + |11\rangle \right), \\
p_\pm = \langle \Psi | \Pi_\pm | \Psi \rangle &= \frac{1}{\sqrt{2}} \cdot \frac{1}{2\sqrt{2}} \left(\langle 00| + \langle 11| \right) \left(|00\rangle \pm |01\rangle \pm |10\rangle + |11\rangle \right) \\
&= \frac{1}{4} \left(\langle 00|00\rangle + \langle 11|11\rangle \right) \\
&= \frac{1}{2}.
\end{aligned}$$

Exercise 3 *Quantum bank note*

1) The bank finds the sequence $q_1, \ldots, q_N$ from S. The sequence $q_1, \ldots, q_N$ indicates the preparation basis of the true quantum bits $|\phi_1\rangle, \ldots, |\phi_N\rangle$. This allows the bank to measure the quantum bits using the preparation basis (so the measurement basis is Z if $p_i = 0$ and X if $q_i = 1$). If the bank note is authentic, each measurement on $|\phi_i\rangle$ does not destroy the quantum bit and the measurement certainly gives an output state $|\phi_i\rangle$. If the bank note is counterfeited, then the measurement does not guarantee to always give the output state $|\phi_i\rangle$.

2) Suppose the counterfeited bank note contains quantum bits in state $|\phi'_1\rangle \otimes \cdots \otimes |\phi'_N\rangle$. The bank detects a problem if for some i the measurement on $|\phi'_i\rangle$ does not give the state $|\phi_i\rangle$. Thus the probability that the bank detects a problem is

$$\begin{aligned} P(\text{detect a problem}) &= 1 - P(\text{not detect a problem}) \\ &= 1 - \prod_{i=1}^{N} P(\text{meas. on } |\phi'_i\rangle \text{ gives } |\phi_i\rangle) \end{aligned}$$

We expand $P(\text{meas. on } |\phi'_i\rangle \text{ gives } |\phi_i\rangle)$ into

$$\begin{aligned} &P(\text{meas. on } |\phi'_i\rangle \text{ gives } |\phi_i\rangle \,\big|\, |\phi'_i\rangle = |\phi_i\rangle) \cdot P(|\phi'_i\rangle = |\phi_i\rangle) \\ &\qquad + P(\text{meas. on } |\phi'_i\rangle \text{ gives } |\phi_i\rangle \,\big|\, |\phi'_i\rangle \neq |\phi_i\rangle) \cdot P(|\phi'_i\rangle \neq |\phi_i\rangle) \\ &= 1 \cdot (1 - P(|\phi'_i\rangle \neq |\phi_i\rangle)) + \frac{1}{2} \cdot P(|\phi'_i\rangle \neq |\phi_i\rangle) \end{aligned}$$

where $P(\text{meas. on } |\phi'_i\rangle \text{ gives } |\phi_i\rangle \,\big|\, |\phi'_i\rangle \neq |\phi_i\rangle) = 1/2$ can be checked explicitly for the two possible cases: $|\phi'_i\rangle = |0\rangle$ and $|\phi_i\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, or $|\phi'_i\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|\phi_i\rangle = |0\rangle$.

The event $|\phi'_i\rangle \neq |\phi_i\rangle$ happens in either of the following cases:

- The true quantum bit $|\phi_i\rangle$ is $|0\rangle$; the counterfeiter measures it with X basis; and upon the measurement the counterfeiter observes $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$. This happens with probability $\frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{8}$.
- The true quantum bit $|\phi_i\rangle$ is $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$; the counterfeiter measures it with Z basis; and upon the measurement the counterfeiter observes $|0\rangle$. This happens with probability $\frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{8}$.

We conclude that

$$\begin{aligned} P(|\phi'_i\rangle \neq |\phi_i\rangle) &= \frac{1}{8} + \frac{1}{8} = \frac{1}{4}, \\ P(\text{meas. on } |\phi'_i\rangle \text{ gives } |\phi_i\rangle) &= 1 \cdot \left(1 - \frac{1}{4}\right) + \frac{1}{2} \cdot \frac{1}{4} = \frac{7}{8}, \\ P(\text{detect a problem}) &= 1 - \left(\frac{7}{8}\right)^N. \end{aligned}$$