Homework 4
Introduction to Quantum Information Processing

**Exercise 1** *Bennett 1992 Protocol for quantum key distribution*

The analysis of BB84 shows that the important point is the use of non-orthogonal states. BB92 retains this characteristic but simply uses two states instead of four.

- **Encoding by Alice**: Alice generates a random sequence $e_1, \ldots, e_N$ of bits that she keeps secret. She sends to Bob the quantum bits $|0\rangle$ if $e_i = 0$ and $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ if $e_i = 1$. The state of the quantum bit sent by Alice is thus $H^{e_i}|0\rangle$.
- **Decoding by Bob**: Bob generates a random sequence $d_1, \ldots, d_N$ of bits that he keeps secret. He measures the received quantum bit $H^{e_i}|0\rangle$ in the basis $\{|0\rangle, |1\rangle\}$ ($Z$ basis) or in the basis $\{H|0\rangle, H|1\rangle\}$ ($X$ basis) according to the value $d_i = 0$ or $d_i = 1$. So the measurement basis of Bob is $\{H^{d_i}|0\rangle, H^{d_i}|1\rangle\}$. He registers $y_i = 0$ if the outcome is $H^{d_i}|0\rangle$ (i.e. if it is $|0\rangle$ or $H|0\rangle$) and $y_i = 1$ if the outcome is $H^{d_i}|1\rangle$ (i.e. if it is $|1\rangle$ or $H|1\rangle$).
- **Public discussion phases**: Bob announces on a public channel his measurement outcome $y_1, \ldots, y_N$.
- **Secret key generation**: You will propose it in question 3).

1) Prove that just after Bob's measurements:

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

2) Deduce that $P(e_i = 1 - d_i|y_i = 1) = 1$.
Hint: You can convince yourself that this is necessarily the case from the above probabilities; but you can also prove it more in detail by using Bayes' rule $P(A|B) = \frac{P(A \cup B)}{P(B)} = \frac{P(B|A)P(A)}{P(B)}$.

3) Based on the result in 2) propose a secret key generation scheme. Show that the secret key has length $\approx N/4$.

4) Propose a security check.

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

Consider the BB84 protocol. Suppose the $i$-th qubit sent by Alice is $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and is captured by Eve. Eve wants to make a copy of the qubit and sends one of the copies to Bob. However she does not know what the preparation basis of Alice was: here we suppose that Eve uses the wrong machine $U_Z$ to copy this bit. Recall that $U_Z$ is defined by

$$U_Z |0\rangle \otimes |b\rangle = |0\rangle \otimes |0\rangle , \quad U_Z |1\rangle \otimes |b\rangle = |1\rangle \otimes |1\rangle .$$

Eve then keeps one of the photons and sends the other one to Bob. Suppose now that Bob uses the $X$-basis to measure the state of the photon. During the public communication phase Alice and Bob notice that their preparation and measurement basis were the same so they conclude that the $i$-th bit (of their secret key) must be the same under the hypothesis that Eve is not present (they don't know yet that Eve is present).

The goal of this problem is to show that there is a probability $1/2$ that the bit of Alice and Bob differs due to the presence of Eve. Therefore repeated such attacks of Eve over many qubits will be detectable during the security test.

1) What is the state of the two photons in the lab of Eve just after she made the copying operation.

2) The measurement process of Bob (we suppose Eve does not measure at this stage) is modeled by the two projectors:

$$\Pi_+ = I \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| + \langle 1|}{\sqrt{2}}\right), \quad \Pi_- = I \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| - \langle 1|}{\sqrt{2}}\right)$$

where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ expresses the fact that Eve does not measure and the second term of the tensor product expresses the fact that Bob's measurement basis is $\left\{ \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}} \right\}$.

a) What are the possible resulting states in Bob's lab? Hint: no calculation.

b) Compute now $p_\pm$ the probability of these outcoming states by using the appropriate form of the measurement postulate.

**Hint**: It may be a good idea to expand $\Pi_\pm$ by writing $I = |0\rangle\langle 0| + |1\rangle\langle 1|$. For example you should check this kind of identity:

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

**Exercise 3** *Quantum bank note*

In 1970's Wiesner had the idea of quantum bank notes that cannot be copied. A quantum bank note consists of one serial number $S$ and of $N$ small cavities each storing one quantum bit (say a polarized photon, or some magnetic moment). Each quantum bit is in a definite state

$$|\phi_i\rangle \in \left\{ |0\rangle \, ; \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right\}, i = 1 \ldots N.$$

The serial number $S$ (say $S =$ COM309HW7ISFUN) indicates to the bank the preparation $q_1, \ldots, q_N$ of the quantum bits where $q_i = 0$ if $|\phi_i\rangle = |0\rangle$ and $q_i = 1$ if $|\phi_i\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$. There is a mapping $f(S) = (q_1 \ldots q_N)$ that only the bank knows. Therefore the bank has access to the information $q_1, \ldots, q_N$ by reading $S$; but no one else has.

We decide to counterfeit the bill as follows:

- We first observe the state of each qubit using measurements in the $Z$ or $X$ basis at random (since we have no information about $q_i$). This necessarily leaves each qubit in a state $\in \{|0\rangle, |1\rangle\}$ or in a state $\in \left\{ \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}} \right\}$.
- If the measured qubit is left in state $|0\rangle$ or $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ we just copy it (with the correct copy machine!).
- If the measured qubit is left in state $|1\rangle$ then we prepare a new state as $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$. And if it is left in the state $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ we prepare a new state $|0\rangle$.

We thus get a "counterfeited" bill which we shall bring to the bank.

1) First suppose that a honest person brings a true bank note (not counterfeited) to the bank. Describe how the bank proceeds to make measurements in order to verify the bank note in such a way that the bank note is not destroyed.

2) Suppose that we bring a counterfeited note to the bank. What is the probability the bank detects a problem ?