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:
\[
\begin{align*}
P(y_i = 0 | e_i = d_i) &= 1 \\
P(y_i = 1 | e_i = d_i) &= 0 \\
P(y_i = 0 | e_i \neq d_i) &= \frac{1}{2} \\
P(y_i = 1 | e_i \neq d_i) &= \frac{1}{2}
\end{align*}
\]

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 \( P(A|B) = \frac{P(A,B)}{P(B)} = \frac{P(B|A)P(A)}{P(B)} \).

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

4) Propose a security check.

Exercise 2 No-cloning theorem

In class we saw that unitarity and tensor product structure imply the no-cloning theorem. Here we show that linearity and tensor product structure also imply the no-cloning theorem.

Suppose a common cloning machine \( U \) exists for all inputs \( |\Psi\rangle \in \mathbb{C}^2 \) in the Hilbert space. In other words we suppose that there exist \( U \) a 4 \( \times \) 4 matrix acting on \( \mathbb{C}^2 \otimes \mathbb{C}^2 \) such that \( U|\Psi\rangle \otimes |0\rangle = |\Psi\rangle \otimes |\Phi\rangle \).
Let $|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle$ where $|\alpha|^2 + |\beta|^2 = 1$. You apply the definition of the copying operator and claim that

$$U |\Psi\rangle \otimes |\text{blank}\rangle = \alpha |0\rangle \otimes |0\rangle + \beta |1\rangle \otimes |1\rangle.$$ 

But your neighbor, just with the same definition of the copying operator, claims that

$$U |\Psi\rangle \otimes |\text{blank}\rangle = \alpha^2 |0\rangle \otimes |0\rangle + \alpha \beta |0\rangle \otimes |1\rangle + \alpha \beta |1\rangle \otimes |0\rangle + \beta^2 |1\rangle \otimes |1\rangle.$$ 

1) Elaborate in detail the mathematical steps that you and your neighbor each have in mind to reach these two conclusions.

2) Under what condition on $\alpha$ and $\beta$ are the two conclusions equivalent? What does this mean with respect to cloning?

**Exercise 3 On the Bell states**

We recall from the lecture that the four Bell states $|B_{00}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$, $|B_{01}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle)$, $|B_{10}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle)$, $|B_{11}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle)$, form an orthonormal basis.

Let $U = (CNOT)H \otimes I$ the $4 \times 4$ unitary matrix. Here the control-NOT operation is defined by $CNOT(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus x\rangle$, for any $x, y \in \{0, 1\}$ ($x$ is called the control bit, $y$ is called the target bit, and $y \oplus x$ is the modulo 2 sum). We recall that the Hadamard matrix is $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $I$ the $2 \times 2$ identity matrix.

1) Compute the following states: $U|0\rangle \otimes |0\rangle = ?$, $U|0\rangle \otimes |1\rangle = ?$, $U|1\rangle \otimes |0\rangle = ?$, $U|1\rangle \otimes |1\rangle = ?$. You should recognize the four Bell states.

2) Based on the fact that the Bell states are entangled (i.e., there does not exist $|\phi_1\rangle \in \mathbb{C}^2$, $|\phi_2\rangle \in \mathbb{C}^2$ such that a Bell state can be factored into $|\phi_1\rangle \otimes |\phi_2\rangle$), show that the CNOT operation cannot be written as a tensor product of two $2 \times 2$ unitary matrices. In other words show there does not exist $U_1$ and $U_2$ such that $CNOT = U_1 \otimes U_2$. 

2