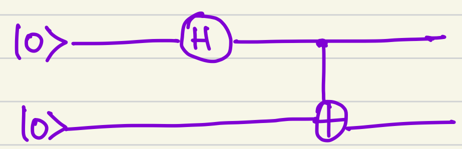
Quantum Cryptography

Assignment 5

Q1



$\Big\} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

What is the matrix representation of this circuit

Sol^n:

We know that Hadamard gate H applied on $|0\rangle$ gives $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

So when we apply H to $|00\rangle$ (applied to the first $|0\rangle$) gives $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$

Now apply CNOT gate to this output, you have $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

In matrix form, this would be as follows:

Since we are applying H only to the first qubit and the second qubit stays the same: It'd be $H \otimes I$. And then we apply M_{CNOT} to it. Final matrix would be $M_{CNOT} \cdot (H \otimes I)$

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow H \otimes I = \begin{bmatrix} \frac{1}{\sqrt{2}} \cdot 1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \frac{1}{\sqrt{2}} \cdot 1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ \frac{1}{\sqrt{2}} \cdot 1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \frac{1}{\sqrt{2}} \cdot (-1) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{bmatrix}$$

$$\Rightarrow H \otimes I = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \Rightarrow \text{As } M_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$M_{CNOT} \cdot H \otimes I = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix} = M$$

$\Rightarrow$ We have $M|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Q2 How would you generate $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

Sol^n: The above matrix M applied to various two qubit states would be:

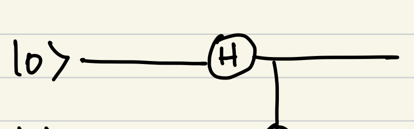
$$M|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \; ; \quad M|01\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$M|10\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$M|11\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

As we see applying M on $|01\rangle$ gives us $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

$\therefore$



$\Big\} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

Q3 Find another matrix M' which generates the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ from $|00\rangle$. M' is unitary.

Sol^n: So basically:

$$\underbrace{\begin{pmatrix} & & & \\ & & & \\ & & & \\ & & & \end{pmatrix}}_{M'} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{pmatrix} \Rightarrow \text{Let us check this following matrix: } \begin{pmatrix} 1/\sqrt{2} & 0 & 0 & -1/\sqrt{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1/\sqrt{2} & 0 & 0 & 1/\sqrt{2} \end{pmatrix} = A$$

Firstly, does this new matrix generate $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$$\Rightarrow \begin{pmatrix} 1/\sqrt{2} & 0 & 0 & -1/\sqrt{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1/\sqrt{2} & 0 & 0 & 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{pmatrix} \checkmark$$

Now is it a unitary matrix? $\Rightarrow A \cdot (A^*)^T = I$

$$\begin{pmatrix} 1/\sqrt{2} & 0 & 0 & -1/\sqrt{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1/\sqrt{2} & 0 & 0 & 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} & 0 & 0 & -1/\sqrt{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1/\sqrt{2} & 0 & 0 & 1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \checkmark$$

$\therefore$ The above A is a unitary matrix which generates $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ from $|00\rangle$