Quantum Cryptography

Assignment - 1

(Submission on 18th Oct, 2022)

① Matrix of CC NOT gate

Sol^n: CC NOT gate has 3 bit input and output!

If the first two bits are 1, then it flips the third bit, else all the bits stay the same

$|000\rangle \mapsto |000\rangle$

$|001\rangle \mapsto |001\rangle$

$|010\rangle \mapsto |010\rangle$

$|011\rangle \mapsto |011\rangle$

$|100\rangle \mapsto |100\rangle$

$|101\rangle \mapsto |101\rangle$

$|110\rangle \mapsto |111\rangle$

$|111\rangle \mapsto |110\rangle$

$$\text{Matrix CCNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

② Matrix of CSWAP gate

CSWAP does controlled swap.

If the first bit is 1, then it swaps the second and third bit. Else, everything stays the same.

$|000\rangle \mapsto |000\rangle$
$|001\rangle \mapsto |001\rangle$
$|010\rangle \mapsto |010\rangle$
$|011\rangle \mapsto |011\rangle$
$|100\rangle \mapsto |100\rangle$
$|101\rangle \mapsto |110\rangle$
$|110\rangle \mapsto |101\rangle$
$|111\rangle \mapsto |111\rangle$

$$\text{Matrix CSWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

③ Quantum Entanglement of $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Sol^n: We have to basically show that given

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle$$

We can't have $|\psi_1\rangle, |\psi_2\rangle$ s.t. $|\psi\rangle = |\psi_1| \otimes |\psi_2|$

Let us assume such $|\psi_1\rangle, |\psi_2\rangle$ exist.

Then $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle \quad |\alpha_1|^2 + |\beta_1|^2 = 1$

$|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle \quad |\alpha_2|^2 + |\beta_2|^2 = 1$

$$\Rightarrow |\psi_1\rangle \otimes |\psi_2\rangle = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_1|01\rangle + \alpha_2\beta_1|10\rangle + \beta_1\beta_2|11\rangle$$

$\Rightarrow$ That'd mean

$$\alpha_1\alpha_2 = \frac{1}{\sqrt{2}}, \quad \beta_1\beta_2 = \frac{1}{\sqrt{2}}, \quad \alpha_1\beta_2 = \alpha_2\beta_1 = 0$$

$$(\beta_1\beta_2)^2 + (\alpha_2\beta_1)^2 = \frac{1}{2} + 0 = \frac{1}{2}$$

$$\Rightarrow |\beta_1^2|(|\alpha_2|^2 + |\beta_2|^2) = \frac{1}{2} \quad \Rightarrow |\beta_1^2| = \frac{1}{2}$$

$$|\alpha_2\beta_1|^2 = 0 \Rightarrow |\alpha_2|^2 \cdot |\beta_1|^2 = 0 \Rightarrow |\alpha_2|^2 = 0$$

Similarly $\Rightarrow$

$$|\alpha_1 \alpha_2|^2 + |\alpha_1 \beta_2|^2 = \frac{1}{2} + 0 = \frac{1}{2}$$

$$\Rightarrow |\alpha_1|^2 \left(|\alpha_2|^2 + |\beta_2|^2\right) = \frac{1}{2} \quad \Rightarrow |\alpha_1|^2 = \frac{1}{2}$$

$$\Rightarrow |\alpha_1 \beta_2|^2 = 0 \quad \Rightarrow |\beta_2|^2 = 0$$

We get $|\alpha_2|^2 + |\beta_2|^2 = 0 + 0 = 0$ $\hookrightarrow$ Contradiction

$\therefore$ It's not possible to find such $\alpha_2, \beta_2, \alpha_1, \beta_1$ values.

$\therefore$ $|\psi\rangle$ is entangled