Quantum Cryptography

Assignment 4

Matta Uma Maheswara Reddy
CRS 2017

Solution- 1

(a) Inner product b/w $(0,1,0,1)$ & $(0,1,1,1)$

$\Rightarrow (0,1,0,1) \cdot (0,1,1,1) = 0\cdot 0 + 1\cdot 1 + 0\cdot 1 + 1\cdot 1 = \underline{\underline{2}}$

(b) Inner product between states $|0101\rangle$ & $|0111\rangle$

$\hookrightarrow |0101\rangle = |0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle$

$= |01\rangle \otimes |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

$|0111\rangle = |01\rangle \otimes |11\rangle$

$= \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

Inner product =

$(0000010000000000) \cdot (0000000100000000) = \underline{\underline{0}}$

Solution 2

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \Rightarrow H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

The question asks us to apply Hadamard transformation to both the qubits (which we have done)

$\Rightarrow$

$$H|0\rangle \otimes H|1\rangle$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

$$= \frac{1}{2}\left(|00\rangle + |10\rangle - |01\rangle - |11\rangle\right)$$

$$= \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}$$

What is $H \otimes H$

$$= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

$$\Rightarrow (H \otimes H)\left(|0\rangle \otimes |1\rangle\right)$$

$$\Rightarrow \left(\frac{1}{2}\right)\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}$$

We see LHS = RHS

$$\therefore H|0\rangle \otimes H|1\rangle = (H \otimes H)\left(|0\rangle \otimes |1\rangle\right)$$

Solution - 3

Here we need to prove that

$$HXH = Z$$

$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ - Hadamard transform

$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ - Bit flip $\quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ - phase flip

$$HXH = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z$$

$\therefore$ A bitflip operation preceded and succeeded by a Hadamard transform equals a phaseflip operation.

$$\underline{\underline{HXH = Z}}$$

Solution 4

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H \otimes H = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$\Rightarrow (H \otimes H)\, CNOT\, (H \otimes H)$$

$$\Rightarrow \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$\Rightarrow \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix} = \frac{1}{4}\begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 4 & 0 \\ 0 & 4 & 0 & 0 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = A$$

Now let us check what this operation does $\Rightarrow$

$$A|00\rangle = A\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle$$

$$A|01\rangle = A\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11\rangle$$

$$A|10\rangle = A\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle$$

$$A|11\rangle = A\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle$$

As we see, based on the second bit, the first bit flips. If the second bit is 1, then the first bit flips. If the second bit is 0, then the first bit does not flip.

Solution 5

Simplify $(\langle 0| \otimes I)(\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle)$

$\Rightarrow \langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\Rightarrow \therefore \langle 0| \otimes I = \begin{pmatrix} 1 \\ 0 \end{pmatrix}^T \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\Rightarrow (1 \quad 0) \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$

$\alpha_{00}|00\rangle = \begin{pmatrix} \alpha_{00} \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad \alpha_{01}|01\rangle = \begin{pmatrix} 0 \\ \alpha_{01} \\ 0 \\ 0 \end{pmatrix}$

$\alpha_{10}|10\rangle = \begin{pmatrix} 0 \\ 0 \\ \alpha_{10} \\ 0 \end{pmatrix} \qquad \alpha_{11}|11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \alpha_{11} \end{pmatrix}$

$\therefore$ Summing them $\Rightarrow \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$

$\Rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \end{pmatrix}$

$G = \alpha_{00} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_{01} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$= \alpha_{00}|0\rangle + \alpha_{01}|1\rangle$