Quantum Cryptology and Security

1. Hadamard Gate :-

This is a one qubit gate H. It is define by)

$$H = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

This gate is often use to put the standerd basis vectors into superposition

$$H(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

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

If $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ be any qubit then

$$H(|\psi\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$= \frac{1}{\sqrt{2}}\begin{pmatrix} \alpha+\beta \\ \alpha-\beta \end{pmatrix}$$

$$= \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$$

So $H(\alpha|0\rangle + \beta|1\rangle) = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$

2. For any qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha \\ \beta\end{pmatrix}$ Then output of ~~[illegible]~~ Hadamard gate is

$$H(|\psi\rangle) = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \begin{pmatrix}\alpha \\ \beta\end{pmatrix}$$

$$= \begin{pmatrix} \frac{\alpha+\beta}{\sqrt{2}} \\ \frac{\alpha-\beta}{\sqrt{2}} \end{pmatrix}$$

$$= \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$$

3. We know that two qubit $|a\rangle$ and $|b\rangle$ are orthogonal if and only if $\langle a|b\rangle = 0$

Here $|q_1\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha \\ \beta\end{pmatrix}$

~~[illegible]~~

$|q_2\rangle = \beta^*|0\rangle - \alpha^*|1\rangle = \begin{pmatrix}\beta^* \\ -\alpha^*\end{pmatrix}$

Where α^* and β^* are Complex Conjugate of α, β.

Then $\langle q_1| = \begin{pmatrix}\alpha^* \\ \beta^*\end{pmatrix}^T = (\alpha^* \ \beta^*) = \alpha^*\langle 0| + \beta^*\langle 1|$

~~[illegible]~~

So $\langle q_1|q_2\rangle = (\alpha^* \ \beta^*)\begin{pmatrix}\beta^* \\ -\alpha^*\end{pmatrix}$

$$= \alpha^*\beta^* - \beta^*\alpha^*$$

$$= 0$$

Therefore $|q_1\rangle$ and $|q_2\rangle$ are orthogonal.

another presentation

$$\langle q_1 | q_2 \rangle = \left(\left(\alpha^* \langle 0| + \beta^* \langle 1|\right) \left(\beta^* |0\rangle - \alpha^* |1\rangle\right) \right)$$

$$= \alpha^* \beta^* \langle 0|0\rangle - \alpha^* \alpha^* \langle 0|1\rangle + \beta^* \beta^* \langle 1|0\rangle - \beta^* \alpha^* \langle 1|1\rangle$$

$$= \alpha^* \beta^* - 0 + 0 - \beta^* \alpha^*$$

Since $\langle 0|0\rangle = 1$

$\langle 0|1\rangle = 0$

$\langle 1|0\rangle = 0$

$\langle 1|1\rangle = 1$

$$= 0$$

So $|q_1\rangle$ & $|q_2\rangle$ are orthogonal.

④ Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

let $|\psi^{\perp}\rangle = \gamma|0\rangle + \delta|1\rangle$

Then $\langle\psi|\psi^{\perp}\rangle = 0$

$\Rightarrow (\alpha^*\langle 0| + \beta^*\langle 1|)(\gamma|0\rangle + \delta|1\rangle) = 0$

$\Rightarrow \alpha^*\gamma + \beta^*\delta = 0$

$\Rightarrow \frac{\gamma}{\delta} = -\frac{\beta^*}{\alpha^*}$

$\Rightarrow \frac{\gamma}{\beta^*} = -\frac{\delta}{\alpha^*} = k$ (say) $\quad k \in \mathbb{C}$

$\Rightarrow \gamma = k\beta^*$ and $\delta = -k\alpha^*$

Since $|\gamma|^2 + |\delta|^2 = 1$

$\Rightarrow |k\beta^*|^2 + |-k\alpha^*|^2 = 1$

$\Rightarrow |k|^2(|\beta^*|^2 + |\alpha^*|^2) = 1$

$\Rightarrow |k|^2(|\alpha|^2 + |\beta|^2) = 1$

$\Rightarrow |k|^2 = 1$

$\Rightarrow |k| = 1$

Now $\frac{1}{\sqrt{2}}(|\psi\rangle + |\psi^{\perp}\rangle) = \frac{1}{\sqrt{2}}((\alpha|0\rangle + \beta|1\rangle) + (k\beta^*|0\rangle - k\alpha^*|1\rangle))$

$= \frac{1}{\sqrt{2}}((\alpha + k\beta^*)|0\rangle + (\beta - k\alpha^*)|1\rangle)$

Now we have ~~from eqn (2)~~ from ~~equation~~ question (2) we get

$$H(|\psi\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} \alpha+\beta \\ \alpha-\beta \end{pmatrix} \quad \text{——} \; (1)$$

~~By the~~ Given that $H(|\psi\rangle) = \frac{1}{\sqrt{2}}\left(|\psi\rangle + |\psi^{\perp}\rangle\right)$

$$= \frac{1}{\sqrt{2}}\begin{pmatrix} \alpha + K\beta^* \\ \beta - K\alpha^* \end{pmatrix} \quad \text{——} \; (2)$$

Comparing (1) and 2 we get

$\alpha+\beta = \alpha + K\beta^*$ and $\alpha - \beta = \beta - K\alpha^*$

$\Rightarrow \beta = K\beta^*$

$\Rightarrow K = \beta/\beta^*$

$K = \dfrac{2\beta - \alpha}{\alpha^*}$

$\therefore \dfrac{\beta}{\beta^*} = \dfrac{2\beta-\alpha}{\alpha^*}$

$\Rightarrow \beta\alpha^* = 2\beta\beta^* - \alpha\beta^*$

$\Rightarrow \alpha^*\beta + \alpha\beta^* = 2|\beta|^2 \quad \text{——} \; (3)$

④ Let $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$

$|\varphi^{\perp}\rangle = \gamma|0\rangle + \delta|1\rangle$

Then $\frac{1}{\sqrt{2}}\left(|\varphi\rangle + |\varphi^{\perp}\rangle\right) = \frac{1}{\sqrt{2}}\left((\alpha+\gamma)|0\rangle + (\beta+\delta)|1\rangle\right)$

$= \frac{1}{\sqrt{2}}\begin{pmatrix}\alpha+\gamma \\ \beta+\delta\end{pmatrix}$

~~Now~~

and $\frac{1}{\sqrt{2}}\left(|\varphi\rangle - |\varphi^{\perp}\rangle\right) = \frac{1}{\sqrt{2}}\left((\alpha-\gamma)|0\rangle + (\beta-\delta)|1\rangle\right)$

$= \frac{1}{\sqrt{2}}\begin{pmatrix}\alpha-\gamma \\ \beta-\delta\end{pmatrix}$

Now $H(|\varphi\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}\alpha+\beta \\ \alpha-\beta\end{pmatrix}$

By the given condition $H(|\varphi\rangle) = \frac{1}{\sqrt{2}}\left(|\varphi\rangle + |\varphi^{\perp}\rangle\right)$

$\Rightarrow \frac{1}{\sqrt{2}}\begin{pmatrix}\alpha+\beta \\ \alpha-\beta\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}\alpha+\gamma \\ \beta+\delta\end{pmatrix}$

$\Rightarrow \alpha+\beta = \alpha+\gamma$ and $\alpha-\beta = \delta+\beta$

$\Rightarrow \gamma = \beta$ $\quad \delta = \alpha - 2\beta$

~~There~~

⑤ given $|\varphi\rangle = \frac{\sqrt{7}}{2\sqrt{3}}|0\rangle - \frac{2+i}{2\sqrt{3}}|1\rangle$

Then $\langle\varphi| = \frac{\sqrt{7}}{2\sqrt{3}}\langle 0| - \frac{2-i}{2\sqrt{3}}\langle 1|$

Then the probable state of observation are.

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

out come "$|+\rangle$" is $\quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$P_+ = |\langle\varphi|+\rangle|^2$$

$$= \left|\left(\frac{\sqrt{7}}{2\sqrt{3}}\langle 0| - \frac{2-i}{2\sqrt{3}}\langle 1|\right)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right|^2$$

$$= \left|\frac{\sqrt{7}}{2\sqrt{6}} - \frac{2-i}{2\sqrt{6}}\right|^2$$

Since $\langle 0|0\rangle = 1$

$\langle 1|1\rangle = 1$

$\langle 0|1\rangle = 0$

$\langle 1|0\rangle = 0$

$$= \left|\frac{\sqrt{7}-2}{2\sqrt{6}} + \frac{i}{2\sqrt{6}}\right|^2$$

$$= \left(\frac{\sqrt{7}-2}{2\sqrt{6}}\right)^2 + \left(\frac{1}{2\sqrt{6}}\right)^2$$

$$= \frac{(\sqrt{7}-2)^2+1}{24} = \frac{12-4\sqrt{7}}{24} = \frac{3-\sqrt{7}}{6}$$

out ~~of~~ come "$|-\rangle$" is

$$P_- = |\langle\psi|-\rangle|^2$$

$$= \left|\left(\frac{\sqrt{7}}{2\sqrt{3}}\langle 0| - \frac{2-i}{2\sqrt{3}}\langle 1|\right)\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right|^2$$

$$= \left|\frac{\sqrt{7}}{2\sqrt{6}} + \frac{2-i}{2\sqrt{3}}\right|^2$$

$$= \left|\frac{\sqrt{7}+2}{2\sqrt{6}} - \frac{i}{2\sqrt{6}}\right|^2$$

$$= \left(\frac{\sqrt{7}+2}{2\sqrt{6}}\right)^2 + \left(\frac{1}{2\sqrt{6}}\right)^2$$

$$= \frac{12+4\sqrt{7}}{24} = \frac{3+\sqrt{7}}{6}$$

(6) Let V_1 ~~be~~ and V_2 be two basis.

~~and so $|p\rangle, |q\rangle$ are in entangled state~~

Let $|\psi\rangle = \alpha|p\rangle + \beta|q\rangle$ is in n qubit entangled state.
Then $|\psi\rangle$ can not be written as a tensor product
~~Let U be~~ ~~them~~ of lower qubit state.

Let U be the unitary transformation which transform the basis V_1 to V_2. Then.

$U|\psi\rangle = |\psi'\rangle$ (say)

If possible let $|\psi'\rangle$ is not in entangled state. Then $|\psi'\rangle$ can be written as a tensor product of two lower qubit state. which is a contradiction, Since if $|\psi'\rangle$ can written as tensor product of lower qubit space the $|\psi\rangle$ can also written as tensor product of lower qubit stat so $|\psi\rangle$ is not in entangled state,