CRS 2017

Quantum Cryptography
Assignment 6

Q1 Create an unitary gate G such that:

$G(\alpha|0\rangle + \beta|1\rangle) \longrightarrow |0\rangle$

$G(\beta^*|0\rangle - \alpha^*|1\rangle) \longrightarrow |1\rangle$

Also prove that $(\alpha|0\rangle+\beta|1\rangle)$ & $(\beta^*|0\rangle-\alpha^*|1\rangle)$ are orthogonal

Sol^n: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

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

$\langle\psi|\psi^*\rangle = [\alpha^* \;\; \beta^*]\begin{bmatrix}\beta^* \\ -\alpha^*\end{bmatrix} = \alpha^*\beta^* - \beta^*\alpha^* = 0 \Rightarrow |\psi\rangle$ & $|\psi^*\rangle$ are orthogonal

Let $G = \begin{bmatrix} a & b \\ c & d\end{bmatrix} \Rightarrow G|\psi\rangle \to |0\rangle \Rightarrow \begin{bmatrix} a & b \\ c & d\end{bmatrix}\begin{pmatrix}\alpha \\ \beta\end{pmatrix} = \begin{pmatrix}1 \\ 0\end{pmatrix} \Rightarrow a\alpha + b\beta = 1 \Rightarrow$ One a, b which satisfies this $a=\alpha^*,\ b=\beta^*$

Similarly $G|\psi^*\rangle \to |1\rangle \Rightarrow \begin{bmatrix} a & b \\ c & d\end{bmatrix}\begin{pmatrix}\beta^* \\ -\alpha^*\end{pmatrix} = \begin{pmatrix}0 \\ 1\end{pmatrix} \Rightarrow c\beta^* - d\alpha^* = 1$

$\hookrightarrow$ If $c=\beta,\ d=-\alpha$ would satisfy this

$\therefore G = \begin{bmatrix}\alpha^* & \beta^* \\ \beta & -\alpha\end{bmatrix}$

Q2 Prove that the quantum bits cannot be cloned.

Sol^n: Let us assume that quantum bits can be cloned.
That'd mean that there exists an unitary matrix U which would transform:

$$U\left(|\psi\rangle|x\rangle\right) = e^{i\theta}|\psi\rangle|\psi\rangle,$$ where $|x\rangle$ is a normalised state, θ = phase

Let us take two non-orthogonal states $|\psi\rangle, |\phi\rangle$ and let us use this circuit to copy the qubits:

$U(|\psi\rangle|x\rangle) = e^{i\alpha}|\psi\rangle|\psi\rangle$

$U(|\phi\rangle|x\rangle) = e^{i\beta}|\phi\rangle|\phi\rangle$

} Basically changing $|x\rangle$ to $|\psi\rangle, |\phi\rangle$

Using $UU^+ = I = U^+U \Rightarrow$ As $U(|\psi\rangle|x\rangle) = e^{i\alpha}|\psi\rangle|\psi\rangle$

$\hookrightarrow \langle\psi|\langle x|U^+U|\psi\rangle|x\rangle = 1$

$\Rightarrow \therefore \langle\psi|\langle x|U^+ = e^{-i\alpha}\langle\psi|\langle\psi|$

$\therefore$ If we try this : $\langle\psi|\langle x|U^+U|\phi\rangle|x\rangle = e^{-i\alpha}\langle\psi|\langle\psi|e^{i\beta}|\phi\rangle|\phi\rangle$

$\Rightarrow |\langle\psi|\phi\rangle\langle x|x\rangle| = |e^{i(\beta-\alpha)}\langle\psi|\phi\rangle\langle\psi|\phi\rangle|$

$\Rightarrow \therefore |\langle\psi|\phi\rangle| = |\langle\psi|\phi\rangle|^2 \longrightarrow$ The only sol^n to this is either $|\langle\psi|\phi\rangle| = 0$ OR $|\langle\psi|\phi\rangle| = 1$

This would mean $|\psi\rangle$ and $|\phi\rangle$ are orthogonal to each other.

This would mean $|\psi\rangle$ and $|\phi\rangle$ are the same state (or states with 180° phase difference.