LECTURE - 17

* Quantum One-time Pad, continued
* Private-Key Encryption of Quantum states
* Public-Key Encryption of Quantum states

Classical One-time Pad idea.

$c \in \{0,1\}$. $\quad k \xleftarrow{\$} \{0,1\}$ $\quad otp(c,k) = c \oplus k$.

Pauli X : "classical NOT".

$$X|0\rangle \to |1\rangle$$
$$X|1\rangle \to |0\rangle$$
$$X(\alpha|0\rangle + \beta|1\rangle) \to \alpha|1\rangle + \beta|0\rangle$$

$$X|+\rangle \to |+\rangle$$
$$X|-\rangle \to -|-\rangle$$

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

$\boxed{\text{Sample } a \xleftarrow{\$} \{0,1\} \text{ and output } X^a|c\rangle}$

is an excellent one-time pad when qubit is classical"

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

$$X|+\rangle = |+\rangle \qquad |-\rangle$$

$X^a|+\rangle = |+\rangle$ (no matter what a is)

$X^a|-\rangle = (-1)^a|-\rangle.$

$$Z|+\rangle = |-\rangle \quad , \quad Z|-\rangle = |+\rangle$$

$\boxed{\text{Sample } b \xleftarrow{\$} \{0,1\} \text{ then output } Z^b(|\psi\rangle)}$

is a good ~~Q~~ One Time Pad when $|\psi\rangle \in \{|+\rangle, |-\rangle\}$.
and we're trying to hide which of the two it is.

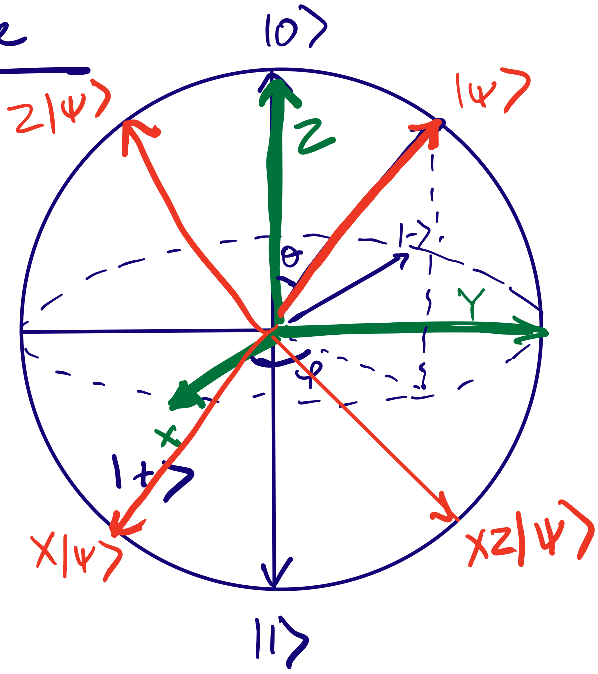
For a general quantum pure/mixed state,

$\boxed{\text{Sample } a,b \xleftarrow{\$} \{0,1\} \text{ then output } X^a Z^b |\psi\rangle}$

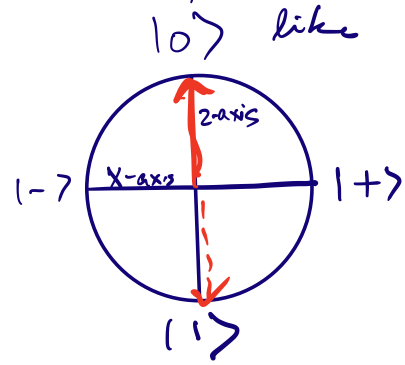
$Y = \begin{bmatrix} 0 & -i \end{bmatrix}$

$[\, i \quad 0 \,]$

Bloch Sphere



XZ-plane looks like



$$|\psi\rangle = \left(\cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)\left(\cos\varphi + i\sin\varphi\right)|1\rangle\right)$$

~~Complex number~~

$$\theta = 0 \Rightarrow \cos\left(\frac{\theta}{2}\right) = 1, \quad \sin\left(\frac{\theta}{2}\right) = 0$$

$$\therefore |\psi\rangle = |0\rangle$$

$$\theta = 180^\circ(\pi) \Rightarrow \cos\left(\frac{\theta}{2}\right) = 0, \quad \sin\left(\frac{\theta}{2}\right) = 1.$$

$$|\psi\rangle = e^{i\varphi}|1\rangle$$

$$\theta = \frac{\pi}{2} \Rightarrow |\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}e^{i\varphi}|1\rangle$$

$$\varphi = 0 \Rightarrow \quad = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = |+\rangle$$

$$\varphi = \pi \Rightarrow \quad = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) = |-\rangle$$

Exercise : Prove that

$$\forall \text{ D.M. } \rho, \ \frac{1}{4} \sum_{a,b} X^a Y^b \rho \left(X^a Y^b\right)^\dagger = \frac{\mathbb{I}}{2}$$

Private-key Encryption

Fixed key of size λ can be used to encrypt $\underline{\mathrm{poly}(\lambda)}$ messages with MULTI-MESSAGE SECURITY.

CLASSICAL.

$\mathrm{KeyGen}(1^\lambda) \rightarrow k$ of size λ

$\mathrm{Enc}(k, m) \rightarrow ct$

$\mathrm{Dec}(k, ct) \rightarrow m$

Multi-message security : $n = \mathrm{poly}(\lambda)$

$\mathcal{A}$ Ch

$\vec{m_0} = m_0^1 \ldots m_0^n$

$\vec{m_1} = m_1^1 \ldots m_1^n \longrightarrow$

$\longleftarrow \mathrm{Enc}(m_b^1) \ldots \mathrm{Enc}(m_b^n)$ $b \xleftarrow{\$} \{0,1\}$

$\tilde{b} \longrightarrow$

$$\Pr\left[\tilde{b} = b\right] \leq \frac{1}{2} + \mathrm{negl}(\lambda)$$

QUANTUM

$\text{KeyGen}(1^\lambda) \rightarrow k$ of size λ

$\text{Enc}(k, \rho) \rightarrow \sigma$

$\text{Dec}(k, \sigma) \rightarrow \rho$

Multi - state security : $n = \text{poly}(\lambda)$

$\mathcal{A}$ $\quad$ Ch

$\rho_0^1 \ldots \rho_0^n$

$\rho_1^1 \ldots \rho_1^n \longrightarrow$

$\longleftarrow \text{Enc}(\rho_b^1) \ldots \text{Enc}(\rho_b^n)$ $\quad$ $b \xleftarrow{\$} \{0,1\}$

$\tilde{b} \longrightarrow$

$\Pr[\tilde{b} = b] \leq \frac{1}{2} + \text{negl}(\lambda)$

CONSTRUCTION $\rightarrow$ (Assume $(\text{Enc}_c, \text{Dec}_c, \text{KeyGen}_c)$ is a quantum-secure classical encryption scheme)

$\text{KeyGen}_Q(1^\lambda) \rightarrow \text{KeyGen}_c(1^\lambda) \rightarrow k_c$

$\text{Enc}_Q(k_c, \rho)$: Sample $a, b \xleftarrow{\$} \{0,1\}$.
Compute $\sigma = X^a Z^b \rho (X^a Z^b)^\dagger$
Compute $ct = \text{Enc}_c(k, (a, b))$.
Output $\boxed{(\sigma, ct)}$

$\text{Dec}_Q(k_c, (\sigma, ct))$: $\text{Dec}_c(k_c, ct) \rightarrow a, b$.
Output $(X^a Z^b)^\dagger \sigma (X^a Z^b)$

NEXT WEEK: PROOF OF SECURITY & Private KE

PUBLIC-KEY ENCRYPTION

(KeyGen, Enc, Dec)

$$\text{KeyGen}(1^\lambda) \rightarrow (pk, sk)$$

$$\text{Enc}(\underset{(k)}{pk}, m; r) \rightarrow ct$$

$$\text{Dec}(\underset{(k)}{sk}, ct) \rightarrow m$$

Correctness.

$$\forall\, m,\ (pk, sk) \in \text{Supp}(\text{KeyGen})$$

$$\Pr_{r}\left[\text{Dec}(sk, \text{Enc}(pk, m; r)) = m\right] = 1 - \text{negl}(\lambda)$$

Security.

$\mathcal{A}$ Ch

$\text{KeyGen}(1^\lambda) \rightarrow (pk, sk)$

$$\xleftarrow{\quad pk \quad}$$

$$\xrightarrow{m_0,\ m_1}$$

$$b \leftarrow^{\$} \{0,1\}$$

$$\xleftarrow{\mathrm{Enc}_{pk}(m_b)}$$

$$\xrightarrow{\tilde{b}}$$

$$\forall \text{ QPT } \mathcal{A}, \quad \Pr[\tilde{b} = b] \leq \frac{1}{2} + \mathrm{negl}(\lambda).$$

Single - message secure public - key encryption
$\Rightarrow$ Multi - message secure public - key encryption

Proof next time