

# CS6846 – Quantum Algorithms and Cryptography

## Quantum Cryptography



Instructor: Shweta Agrawal, IIT Madras  
Email: shweta@cse.iitm.ac.in

## Road Ahead:

- Q K E.
- Q one time pads.
- Q SKE
- Q PKE .
- Try: Q FHE / q Money

## Mixed States

Let's say a device outputs

$$|\psi_1\rangle \text{ w.p. } p_1$$

$$|\psi_2\rangle \text{ w.p. } p_2$$

:

$$|\psi_n\rangle \text{ w.p. } p_n$$

Can represent such a state by  $\{p_i, |\psi_i\rangle\}$

---

Let us say that we measure the above device in basis  $|\nu_1\rangle, \dots, |\nu_d\rangle$ .

$$\Pr(|v_i\rangle \text{ is observed}) = \sum_j p_j |\langle v_i | \psi_j \rangle|^2$$

$$= \sum_j p_j \langle v_i | \psi_j \rangle \langle \psi_j | v_i \rangle$$

$$= \langle v_i | \underbrace{\left( \sum_j p_j \langle \psi_j \rangle \langle \psi_j | \right)}_S | v_i \rangle$$

$$= \langle v_i | \rho | v_i \rangle$$

Definition: The mixed state  $\{p_i, |\psi_i\rangle\}$  is represented by matrix  $\rho = \sum_j p_j |\psi_j\rangle \langle \psi_j|$ .

Example :

$$\begin{aligned}S_1 &= |0\rangle \quad w.p \ 1 \\&= |1\rangle \quad w.p \ 0\end{aligned}$$

$$P = |0\rangle \langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{aligned}S_2 &= -|0\rangle \quad w.p \ 1 \\&= |1\rangle \quad w.p \ 0\end{aligned}$$

$$\{ = (-|0\rangle)(-\langle 0|) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{aligned}S_3 &= |0\rangle \quad w.p \ \frac{1}{2} \\&= |1\rangle \quad w.p \ \frac{1}{2}\end{aligned}$$

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

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

Evolution: Suppose a mixed state  $S_1$ ,  $\{p_i, |\psi_i\rangle\}$  goes through unitary  $U$ , transforms to  $S_2 = \{p_i, U|\psi_i\rangle\}$ .

Let  $\rho_{S_b}$  be matrix corres. to  $S_b$ ,  
 $b \in \{1, 2\}$

$$\rho_{S_2} = ? \rho_{S_1} ? = U \rho_{S_1} U^\dagger$$

Proposition: If  $\rho$  represents a mixed state then  $\text{tr}(\rho) = 1$ ,  $\rho$  is positive semidefinite & hermitian.

PSD:  $\forall x \in \mathbb{C}^n, \langle x | \rho | x \rangle \geq 0$ .

Hermitian:  $\rho = \rho^\dagger$

Proof: Let's consider  $|\psi\rangle = \sum_{i=1}^d a_i |i\rangle$

$$\text{tr}(|\psi\rangle\langle\psi|) = \sum |a_i|^2 = 1.$$

Now consider mixed state:

$$\begin{aligned} \text{tr}\left(\sum_i p_i |\psi_i\rangle\langle\psi_i|\right) &= \sum_i p_i \underbrace{\text{tr}(|\psi_i\rangle\langle\psi_i|)}_1 \\ &= \sum p_i = 1. \end{aligned}$$

Hermitian: Exercise

PSD: Note for any  $|v\rangle$ ,

$$\langle v | \rho | v \rangle = \text{Pr}(\text{observe } |v\rangle) \geq 0.$$

$\Rightarrow \rho$  is PSD

Definition: We say that a matrix  $\rho$  is a density matrix iff  $\text{tr}(\rho) = 1$ ,  $\rho$  is PSD & Hermitian.

Proposition: If  $\rho$  is a density matrix, it corresponds to a mixed state

$$P = \sum_{i=1}^d \lambda_i |v_i\rangle \langle v_i| \quad \text{by spectral theorem.}$$

↓  
 real eigenvalues.  
 ↗ Form orthonormal basis

$$\text{tr}(P) = 1, \quad \sum \lambda_i = 1$$

Want  $\{\underline{P}_i, |\psi_i\rangle\} = \{\underline{\lambda}_i, |v_i\rangle\}$  for  $i \in [d]$

---

Maximally mixed state :

All eigenvalues  $\lambda_i$  are identical  
for  $i \in [N]$ ,  $\lambda_i = \frac{1}{N}$ .

Quantum Algos & Density Matrix:

In the HSP for group  $G$ , if " $f$ " hides subgroup  $H$ , then our algorithm outputs a uniformly random coset

$$|gh\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle$$

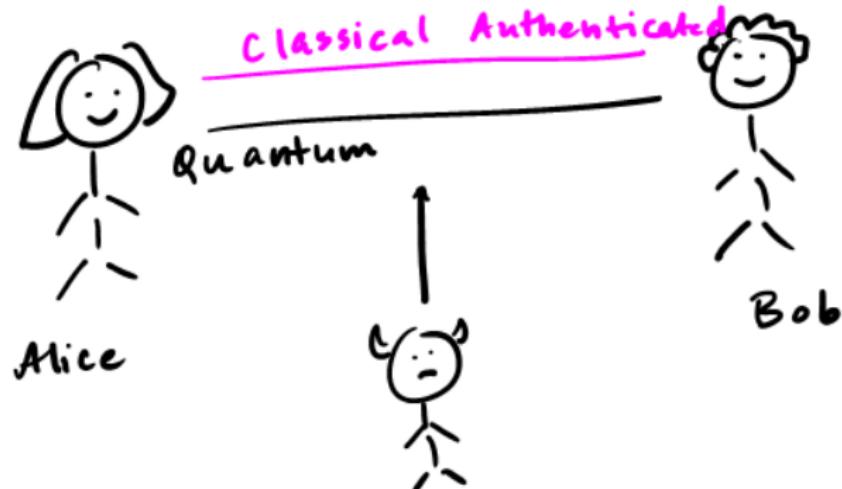
Each coset  $|gh\rangle$  is output w.p.  $\frac{1}{|G|}$ .

So the density matrix representing the mixed state is  $\rho_H = \sum_{g \in G} \frac{1}{|G|} |gh\rangle \langle gh|$

# Quantum Key Distribution

Bennett  
& Brassard  
1984

Information  
Theoretic  
Security.



Protocol:

1. Quantum State Preparation: Alice prepares a sequence of quantum states, which are sent through the channel to Bob. These states are chosen from an unknown basis.

2. Classical Authentication: Alice sends classical information to Bob via a secure channel, such as a public key or a previously shared secret.

3. Key Exchange: Alice and Bob use the shared quantum states and the classical authentication information to generate a shared key. Eve, who is intercepting the communication, cannot determine the key without disturbing the quantum states, which would be detected by Alice and Bob.

Main Property: If bit  $b$  is encoded in an unknown basis, Eve cannot get info abt  $b$  w/o disturbing the state.

1). Alice chooses  $n$  random bits  $a_1 \dots a_n$ ,  
&  $n$  random bases,  $b_1 \dots b_n$   
 $b_i \in \{\text{Comp, Head}\}$

$$\{\lvert 0 \rangle, \lvert 1 \rangle\} \quad b=0$$

$$\{\lvert + \rangle, \lvert - \rangle\} \quad b=1$$

Sends  $a_i$  in basis  $b_i$ .

$$a_i = 0, \quad b_i = 1 \quad \Rightarrow \lvert + \rangle$$

2). Bob chooses random bases  $b'_1 \dots b'_n$   
& measures received qubits in these.

Gets  $a'_1 \dots a'_n$ .

3) Bob sends  $\{b'_i\}$  to Alice, Alice sends  
 $\{b_i\}$  to Bob.

For "matching" positions  $a'_i = a_i$

IF Eve did not tamper.

4) Alice selects  $n/4$  locations in shared string & sends Bob  $a'_i$  & locations.

If fraction of errors is "high", they abort.

5) If not, they get  $n/4$  shared bits.