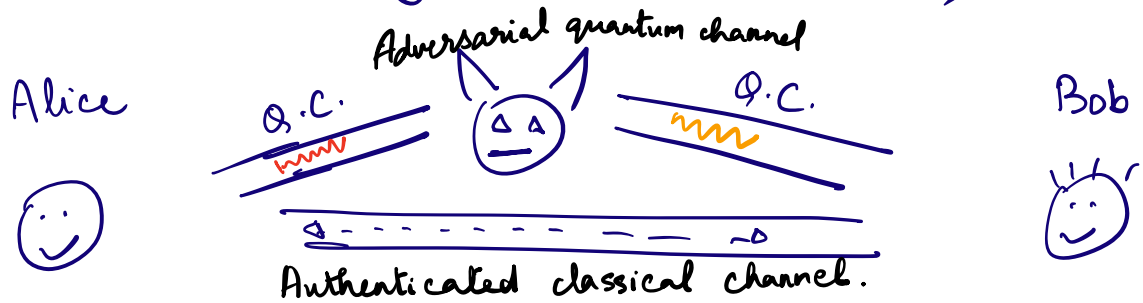
# LECTURE - 12

RECAP : Quantum Key Distribution (QKD)




Last time, we showed that :

Alice and Bob can agree on classical strings $X_1 \ldots X_n$ $Y_1 \ldots Y_n$ respectively, such that :

(1) "Weak" Agreement

$$Z_1 \ldots Z_n = (X_1 \oplus Y_1 \ \ldots\ldots \ X_n \oplus Y_n)$$

are derived from computational basis measurements of a state $\approx$ state with low H.W. terms,

i.e.

$$\Pr\left[ H.W.(Z_1 \ldots Z_n) > \delta n \right] \leq \sqrt{2}\, e^{-\frac{\delta^2 n}{2}}$$

(i.e. $X_i$ and $Y_i$ agree on $(1-\delta)$ fraction of $i$'s)

## ② "Weak" Privacy

$W_1 \ldots W_n :=$ [$\forall i \in [n]$, $W_i$ is either $X_i$ or $Y_i$]

(i.e. $W_i$ and $X_i$ agree on $(1-\delta)$ fraction of $i$'s)

where $W_1 \ldots W_n$ are obtained via Hadamard basis measurements on a state that is $\varepsilon$-close to the state

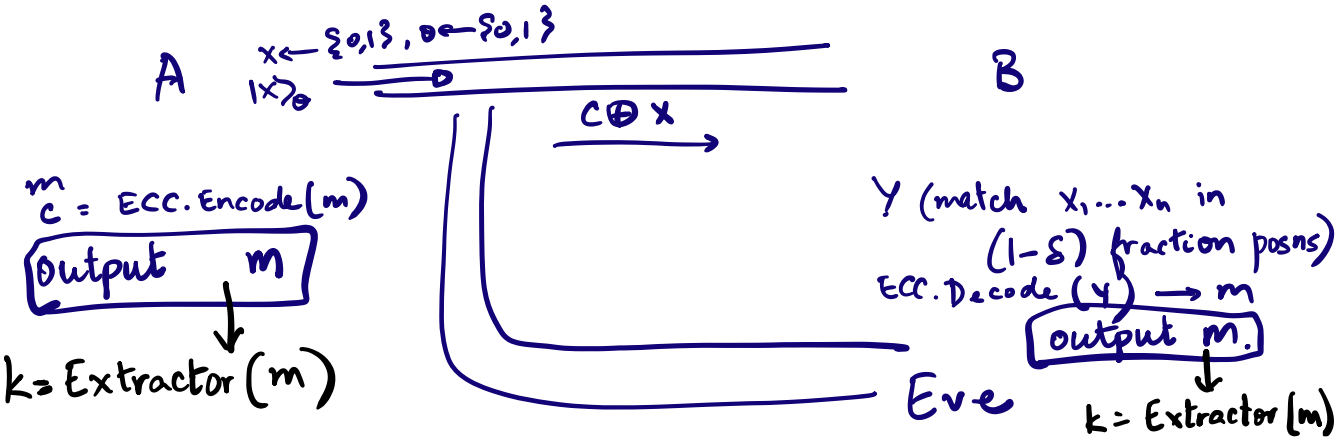
$$|\psi\rangle = \sum_{i \in \{0,1\}^n} \alpha_i |i\rangle_{AB} |\varphi_E^i\rangle_E \otimes (\text{residual})$$

where $\alpha_i = 0$ on all $|i\rangle$ with H.W. $> \delta n$.

- Consider $|\psi\rangle = |0^n\rangle_{AB} \otimes |\varphi_E^i\rangle_E$.

then measuring $|0^n\rangle_{AB}$ in the Hadamard basis results in a uniform $n$-bit string in $\{\underset{=0}{+}, \underset{=1}{-}\}^n$.

- Next H.W.: prove that measuring $|\psi\rangle$ in the Hadamard basis [i.e. $H(|\psi\rangle)$ then measure in c.b.] then XORing all $n$ bits yields a uniform bit.




1) For $(1-\delta)n$ indices $i \in [n]$, $x_i = y_i$.

Use ERROR CORRECTING CODES. ECC that corrects $\delta n$. errors.

Alice picks $m = m_1 \ldots m_k$ $(k < n)$

$c = c_1 \ldots c_n \leftarrow \text{ECC.Encode}(m)$.

Set $x_i = c_i \quad \forall\ i \in [n]$.

Bob obtains $y = y_1 \ldots y_n$ that agrees with $c$ in $(1-\delta)n$ positions

$\text{Dec}(y_1 \ldots y_n) = m$ as long as $\text{H.W.}(x \oplus y) \leq \delta n$.

2) Secrecy.

Eve has "uncertainty" about most $x_i$.

formally described via quantum conditional min-entropy.

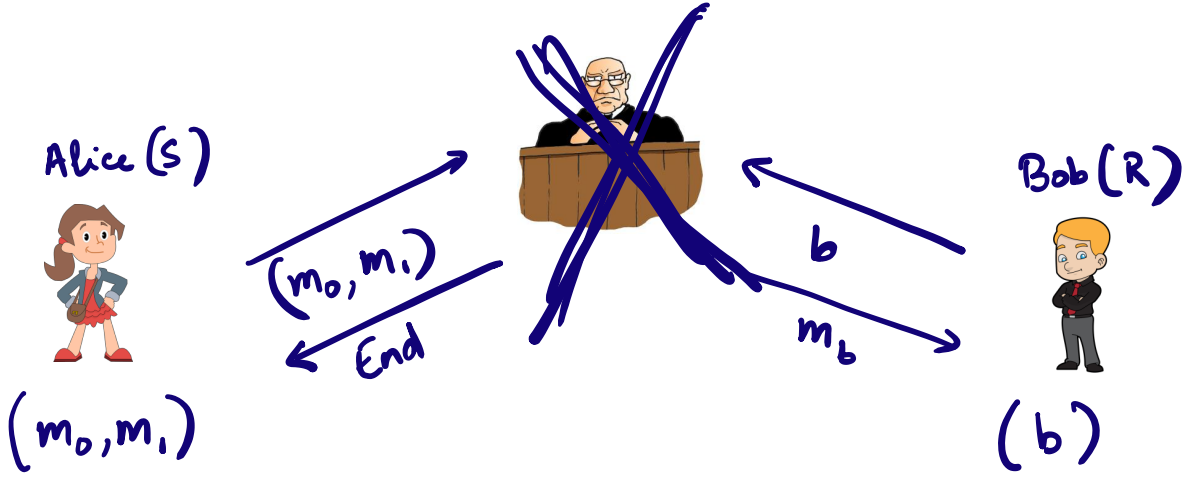
$$\Pr_{\text{Eve} \to m' = (m_1', \ldots, m_k')} [m' = m] \leq 2^{-\boxed{O(n)}}$$

$$\boxed{H_{min}(m \mid \text{Eve's view}) \geq O(n) \quad [-\log(2^{-O(n)})]}$$

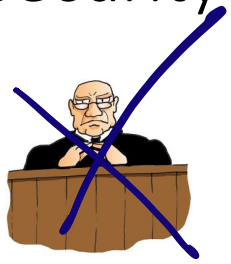
## Leftover Hash Lemma.

Extractor$(m)$ can be a pairwise independent hash function.

# Oblivious Transfer



# Oblivious Transfer: Security



$(m_0, m_1)$

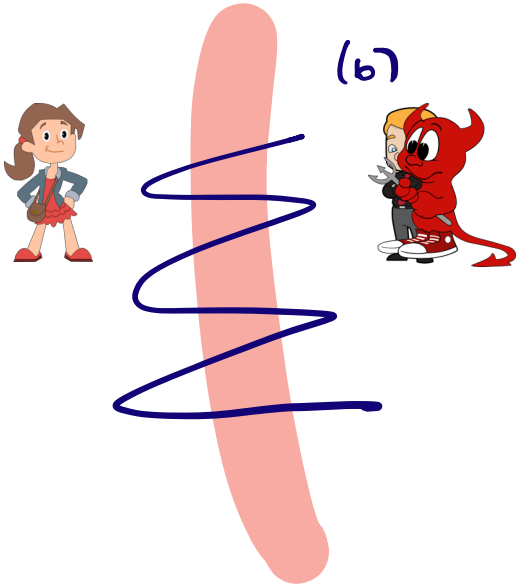
$b$

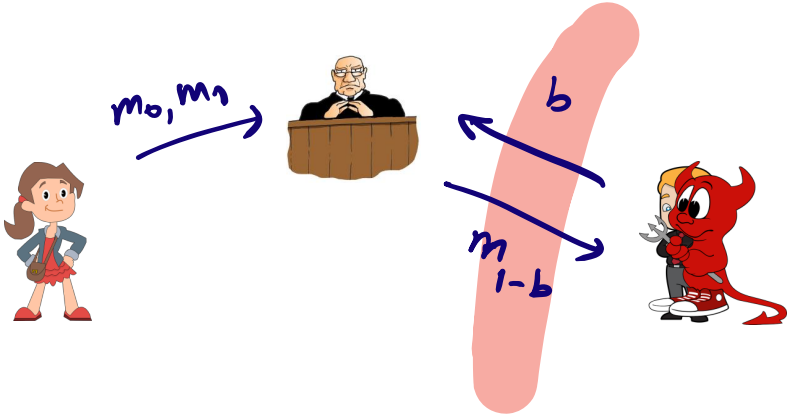
$m_b$

(Does not learn $b$)

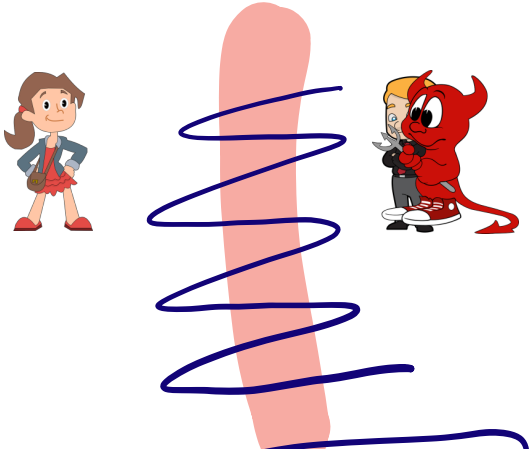
(Does not learn $m_{1-b}$)

# OT: Security against Malicious Receivers



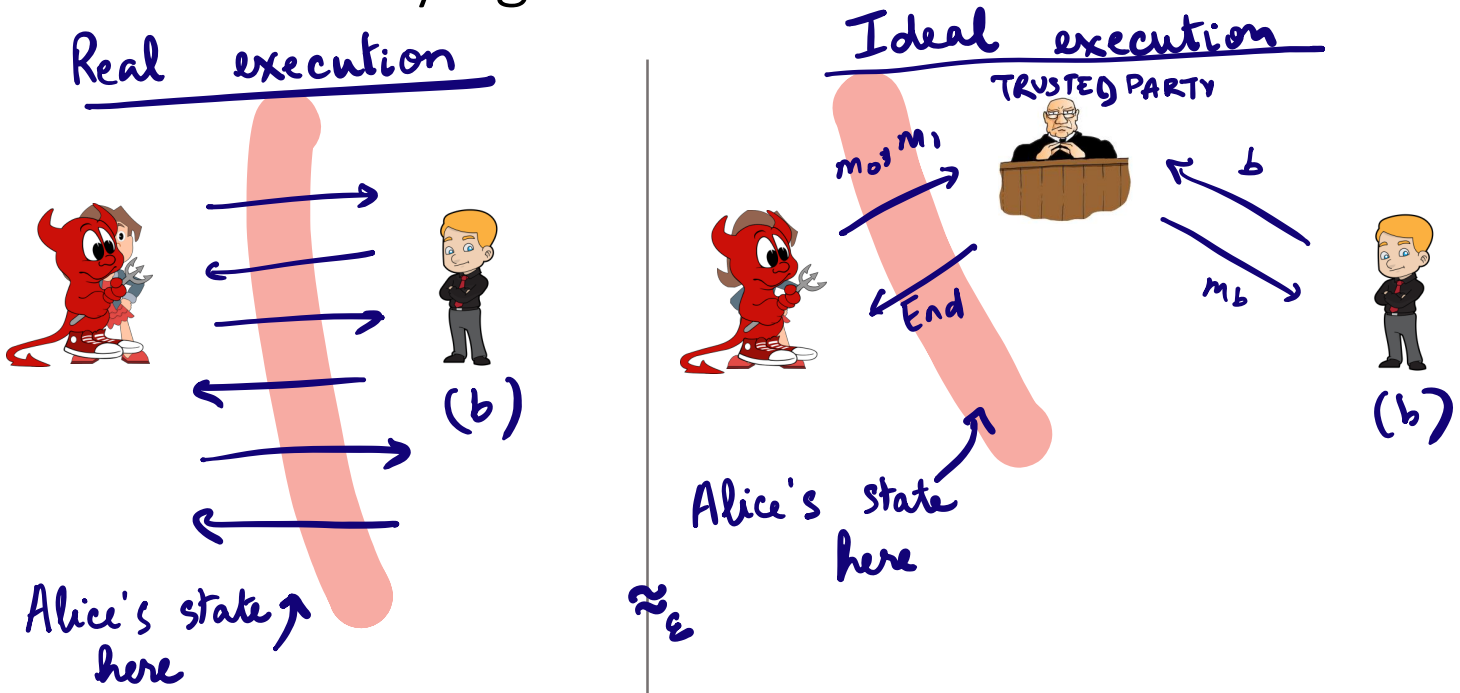
# OT: Security against Malicious Receivers



$\boxed{\text{View}_{\text{Bob, real}}} \approx_\varepsilon$


$\boxed{\text{View}_{\text{Bob, Sim}}}$

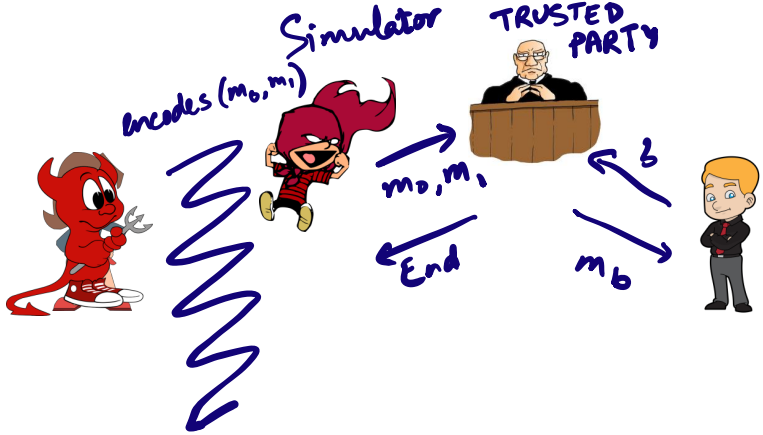
# OT: Security against Malicious Senders



# OT: Security against Malicious Senders


$View_{Alice,\,real}$

$\approx$




$View_{Alice,\,Sim}$

# Oblivious Transfer Secure Against Malicious Adversaries

Simpler goal: set up 2 communication channels s.t. Bob only recovers info on $\leq 1$ channel.

BB84 states

Recall: conjugate encodings

Classical $x \in \{0,1\}^n$, $\theta \in \{C, H\}^n$

$$|\psi_i\rangle = |x_i\rangle_{\theta_i}$$

$$|0\rangle_C = |0\rangle, \; |1\rangle_C = |1\rangle, \; |0\rangle_H = |+\rangle, \; |1\rangle_H = |-\rangle.$$

Sample uniformly in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to obtain $|\psi_i\rangle$ for $i \in [n]$.

Send $|\psi\rangle = \{|\psi_i\rangle\}_{i \in [n]}$ to Bob.

# Oblivious Transfer Secure Against Malicious Adversaries

BB84 states $|\psi\rangle \longrightarrow$

$\forall i \in [n]\ \theta_i' \xleftarrow{\$} \{C, H\}$

$x_1 \ldots x_n$

$\forall i \in [n]$, measure $|\psi_i\rangle$ in basis $\theta_i'$ to obtain $y_i$

$$\boxed{\begin{array}{l} \text{if } \theta_i = \theta_i', \text{ then } y_i = x_i \\ \theta_i \neq \theta_i', \text{ then } y_i \text{ ind } x_i \end{array}}$$

$\longleftarrow$ ok, I measured

$\{\theta_i\}_{i \in [n]} \longrightarrow$

$S_1 = \{i : \theta_i = \theta_i'\} \rightarrow \therefore y_i = x_i$

$S_2 = \{i : \theta_i \neq \theta_i'\}$

$\longleftarrow I_0, I_1$

let $I_b = S_1$, $I_{1-b} = S_2$

$y_0 = m_0 \oplus \{x_i\}_{i \in I_0}$

$y_1 = m_1 \oplus \{x_i\}_{i \in I_1}$

$\longrightarrow y_0, y_1$

$m_b = y_b \oplus \{x_i\}_{i \in I_b} = y_b \oplus \{y_i\}_{i \in I_b}$

# Oblivious Transfer Secure Against Malicious Adversaries

INGREDIENT :

commitment scheme :

(commit, decommit)

commit (b) → com , state

state

com →

b, state →

decommit (com, state, b) → 0/1