LECTURE - 11

RECALL:

(Alice, Bob) Eve

$$\xrightarrow[QC]{B_1 \dots B_n} \quad \text{Operation}(E_0)$$

$(A_1 \dots A_n)$

$$\xleftarrow[Q.C.]{C_1 \dots C_n}$$

C.C. $\xrightarrow{\theta,\, S,\, \{x_i\}_{i \in S}}$

- Measure $A_1 \dots A_n$ in basis $\theta_1 \dots \theta_n \rightarrow x_1 \dots x_n$
- Measure $C_1 \dots C_n$ in basis $\theta_1 \dots \theta_n$ to obtain $y_1 \dots y_n$
- Test if $\{x_i = y_i\}_{i \in S}$.

$\xrightarrow{\text{Pass / Fail}}$

If pass, output $\{x_i\}_{i \in \bar{S}}$ as Alice's "key".

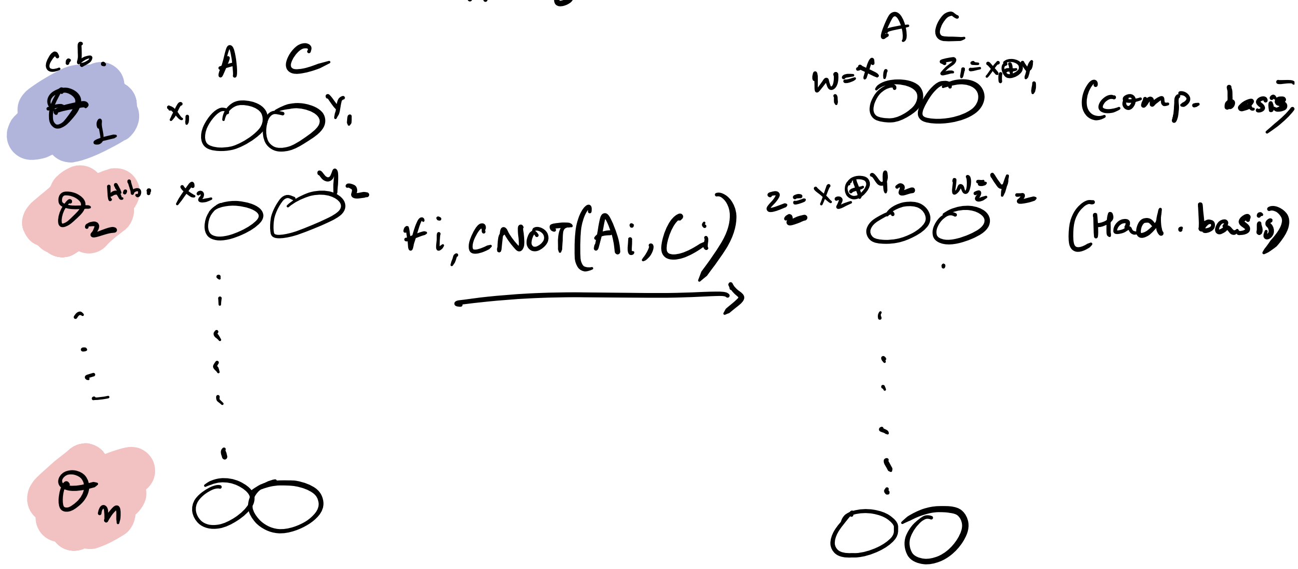
$\bar{S} = [n] \setminus S$

$\{y_i\}_{i \in \bar{S}}$ as Bob's "key".

$$|\psi\rangle_{ACE_0} \xrightarrow{\text{after the check}} |\psi\rangle_{\Theta XYE_0}$$

Hybrid classical-quantum state

Start with $|\psi\rangle_{ACE_0}$.



Equivalent state $|\psi\rangle_{\Theta WZE_0}$.

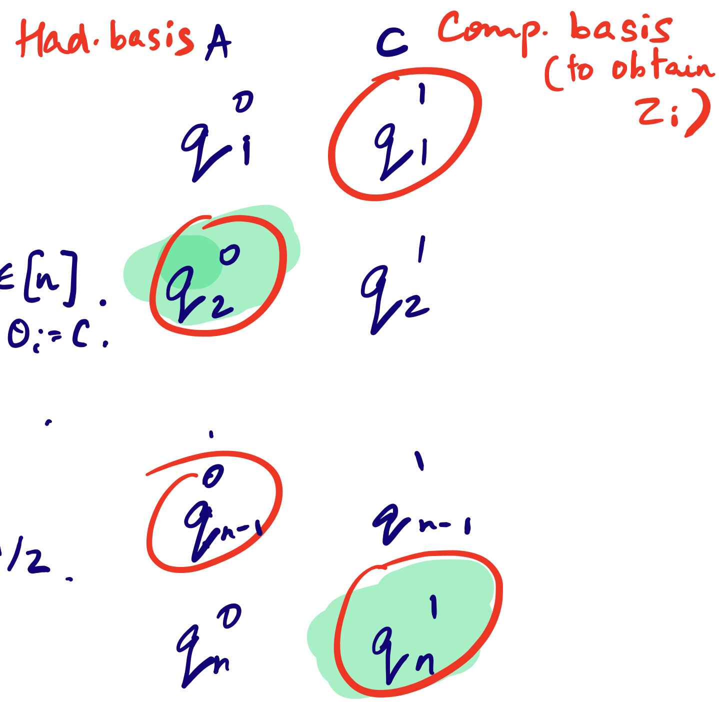
Can rewrite the test as:

* Sample $\{\Theta_i\}_{i\in[n]}$
* Sample $S \subset [n]$ of size $n/2$.
* Measure $\{Z_i\}_{i\in S}$, test if they are all 0

If test passed, then we want to claim

- Agreement: $\{i\in\bar{S} \mid X_i \sim Y_i\}$, equivalently $\{i\in\bar{S} \mid Z_i \sim 0\}$
- Secrecy: $\{X_i\}_{i\in\bar{S}} \sim \{Y_i\}_{i\in\bar{S}} \sim \{W_i\}_{i\in\bar{S}}$ is unguessable

Agreement.



1) Sample $\theta_i \leftarrow \{C, H\}$ $\forall i \in [n]$.
Set $j_i := 0$ if $\theta_i = H$, $j_i := 1$ if $\theta_i = C$.
$T = \{(i, j_i)\}_{i \in [n]}$.

Sample $S \subset T$ s.t. $|S| = n/2$.
(shaded)

Measure q_S in appropriate basis to obtain z_S.

Use this z_S to estimate $z_{T \setminus S}$.

When z_S are all 0s, what do expect on $z_{T\setminus S}$?
w.h.p., the registers $q_{T\setminus S}$ will "behave like"
$|\psi\rangle = \sum_{\substack{u \in \{0,1\}^n \\ \text{s.t. } w(u) \leq \delta n}} \alpha_u |u\rangle$ except with prob. ε.

ε is the "quantum error probability" in this sampling expmt.

Privacy

Z_i: Had. basis A W_i: comp. basis	C Comp. basis: Z_i Had. basis : Z_i
q_1^0	q_1^1
q_2^0	q_2^1
$\vdots$	$\vdots$
q_{n-1}^0	q_{n-1}^1
q_n^0	q_n^1

Analyze $\{W_i\}_{i \in T \setminus S}$

Recall W_i is obtained by measuring in conjugate bases as the ones used for Z_i.

$$Z_S = 0.$$

"most" left registers are close to $|+\rangle$.

"most" right registers are close to $|0\rangle$.

W is obtained by measuring non-circled regs. in purple bases.

Will show.

Non-circled regs must also be close to 0s (in Had. basis on left regs) (in Comp. basis on right regs).

Classical sampling and estimation.

2n-bit string

$n \times 2$ matrix

$$\begin{array}{cc} q_1^0 & q_1^1 \\ q_2^0 & q_2^1 \\ \vdots & \\ q_{n-1}^0 & q_{n-1}^1 \\ q_n^0 & q_n^1 \end{array}$$

$\forall i \in [n]$, sample $j_i \leftarrow \{0,1\}$.

$T = \{(i, j_i)\}_{i \in [n]}$, $\bar{T} = \{(i, 1-j_i)\}_{i \in [n]}$.

Sample $S \subset T$ of size $n/2$.

Then count # 1s in q_S. $\rightarrow W[q_S]$

We want to use $W[q_S]$ to estimate $W[q_T]$

$$W[q_{T \setminus S}] = W[q_T] - W[q_S]$$

$W[q_{\bar{T}}]$

Step 1. Relate $W[q_T]$ and $W[q_S]$.

$$\Pr\left[\left|\frac{W[q_S]}{|S|} - \frac{W[q_T]}{|T|}\right| \geq \delta\right] \leq 2e^{-2\delta^2|S|}$$

$|S| = \frac{n}{2}$, $|T| = n$

$$\Pr\left[\left|2W[q_S] - W[q_T]\right| \geq \delta n\right] \leq 2e^{-\delta^2 n}$$

(Hoeffding's inequality).

In particular, when $W[q_S] = 0$,

$$\Pr\left[W[q_T] \leq \delta n\right] \geq 1 - \boxed{2e^{-\delta^2 n}}.$$

This is the classical analogue of the agreement game.

[Bouman-Fehr 10]: Quantum error

$$\varepsilon_q \leq \sqrt{\varepsilon_{class.}} \leq \sqrt{2}\, e^{-\frac{\delta^2 n}{2}}$$

Step 2. $W[q_T]$ and $W[q_{\bar{T}}]$.

Let $L = \{ i : q_i^{j_i} \neq q_i^{1-j_i} \}$.

Let $\ell = |L|$.

$$W[q_T] - W[q_{\bar{T}}] = W[q_{T|L}] - W[q_{\bar{T}|L}]$$
$$= 2W[q_{T|L}] - \ell$$

$\left(\text{because } W[q_{T|L}] + W[q_{\bar{T}|L}] = \ell \right)$

$$\Pr\left[|W[q_T] - W[q_{\bar{T}}]| \geq \varepsilon n \right]$$

$$= \Pr\left[|2W[q_{T|L}] - \ell| \geq \varepsilon n \right] \ldots$$

$$= \left(\Pr\left[|W[q_{T|L}] - \ell/2| \geq \frac{\varepsilon n}{2} \right] \right) \leq 2e^{-\frac{n\varepsilon^2}{2}}$$

For r.v.s $X_1 \ldots X_m$ s.t. $0 \leq X_i \leq 1$,
let $S = X_1 \ldots X_m$

$$\Pr\left[|S - \mathbb{E}[S]| \geq t \right] \leq 2e^{-\frac{2t^2}{m}}$$

$S = W[q_{T|L}]$, $t = \frac{\varepsilon n}{2}$.

Recall:

$$\Pr\left[\left|\frac{W[q_S]}{|S|} - \frac{W[q_T]}{|T|}\right| \geq \delta\right] \leq 2e^{-\delta^2 n}$$

$$\Pr\left[\frac{W[q_T]}{|T|} - \frac{W[q_{\bar{T}}]}{|\bar{T}|} \geq \varepsilon\right] \leq 2e^{-\frac{n\varepsilon^2}{2}}$$

$$\Pr\left[\left|\frac{W[q_S]}{|S|} - \frac{W[q_{\bar{T}}]}{|\bar{T}|}\right| \geq \varepsilon + \delta\right] \leq 2e^{-\delta^2 n} + 2e^{-\frac{\varepsilon^2 n}{2}}$$

$\varepsilon = \delta = 0.001$

$$\Pr\left[\left| \qquad \right| \geq 2\delta\right] \leq 4e^{-\frac{\delta^2 n}{2}}$$

$\varepsilon_{class} =$

$$\Pr\left[W[q_{\bar{T}}] \geq 0.002n\right] \leq \left(4e^{-\frac{n}{2\times10^6}}\right)$$

$$\varepsilon_q \leq \sqrt{4e^{-\frac{n}{2\times10^6}}} = 2 \cdot e^{-\frac{n}{4\times10^6}}.$$

Except with prob. $\varepsilon_q = 2 \cdot e^{-\frac{n}{4\times 10^6}}$.

Hadamard first

$Z \rightarrow$ comp. basis

$W \rightarrow$ Had. basis

~~$Z \rightarrow$ Had. basis~~

~~$W \rightarrow$ Comp. basis~~

Comp. basis $\leftarrow Z$

Had. basis $\leftarrow W$

A	C
q_1^0	q_1^1
q_2^0	q_2^1
$\vdots$	$\vdots$
q_{n-1}^0	q_{n-1}^1
q_n^0	q_n^1

We infer that $q_{T\setminus S}$ are ε_q-close to a "mixed" state with terms

$$\sum_{T,S} |T,S\rangle\langle S,T| \sum_{i\in\{0,1\}^n} \alpha_i |i\rangle |\varphi_E^i\rangle$$

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