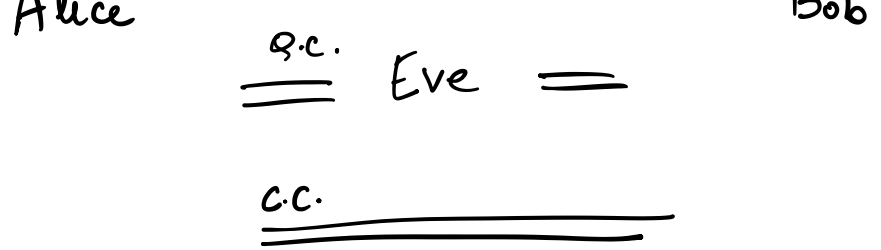
LECTURE -10.

QUANTUM KEY DISTRIBUTION



GOAL:

Alice and Bob agree on a shared key k, such that $(k, \text{Eve's view}) \approx_\varepsilon (\text{uniform}, \text{Eve's view})$

statistical indistinguishability

for any two distributions D_1 and D_2, we say that (D_1, D_2) are ε- stat- ind

$D_1 \approx_\varepsilon D_2 \iff \Delta(D_1, D_2) \leq \varepsilon$.

Equivalently, $\forall C$, $\left| \Pr_{d \leftarrow D_1}[C(d)=1] - \Pr_{d \leftarrow D_2}[C(d)=1] \right| \leq \varepsilon$

Attempt 0.

Alice Bob

$k \leftarrow \{0,1\}^n$

$k \xrightarrow{\text{c.c.}}$

But Eve can also observe k.

Attempt 1.

Alice Bob

$x \in \{0,1\}^n$

$\theta \in \{0,1\}^n$

$|\psi\rangle = |\psi_1\rangle \cdots |\psi_n\rangle$ where $|\psi_i\rangle = |x_i\rangle_{\theta_i}$

$|\psi\rangle$ (q.c.)

I received (c.c.)

$\theta = \theta_1 \cdots \theta_n$ (c.c.)

$\forall i$, measure $|\psi_i\rangle$ in basis $\theta_i \to x_i$

If $\theta_i = 0$ "computational basis" $= \{|0\rangle, |1\rangle\}$ (ordered)

$\theta_i = 1$ "Hadamard basis" $= \{|+\rangle, |-\rangle\}$

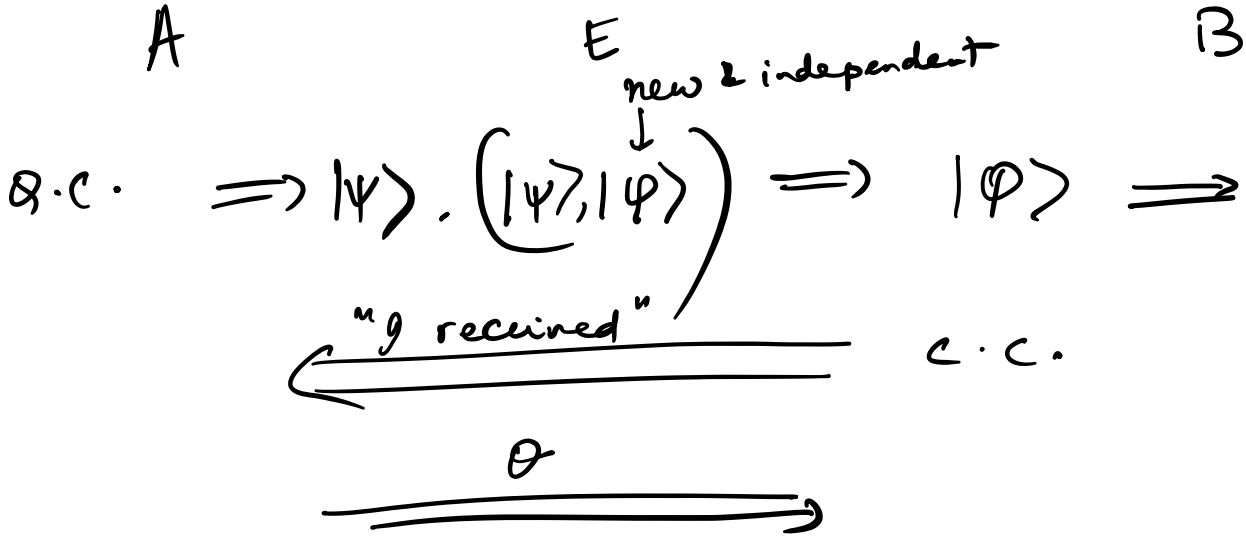
If $x_i = 0$, sample the first element in basis θ_i

If $x_i = 1$, sample the second element in basis θ_i

x_i \ θ_i	$\theta_i = 0$	$\theta_i = 1$
0	$\lvert x_i\rangle_{\theta_i} = \lvert 0\rangle$	$\lvert +\rangle$
1	$\lvert 1\rangle$	$\lvert -\rangle$

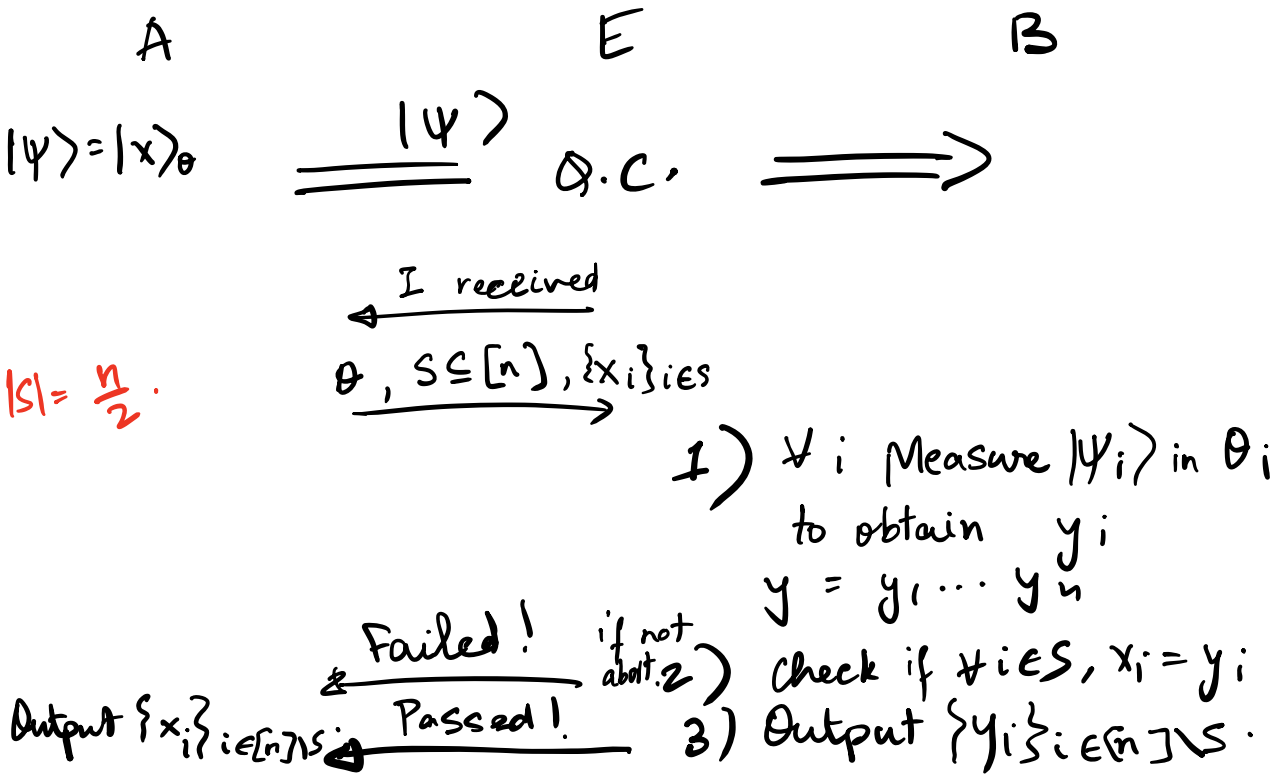
$|x_i\rangle_{\theta_i}$

"Conjugate coding"



E measures $|\psi\rangle$ in basis θ.
E and A share a key. E and B share a key.

INSECURE!



Equivalent experiment

A

B

EPR pairs

$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = A_1 B_1$

$\vdots$

$= A_n B_n$

Keeps $A_1 \dots A_n$

$B_1 \dots B_n$ ⟹ (QC)

$\frac{1}{2^n} I_n$

"I received"

$\theta = \theta_1 \dots \theta_n$

measure $A_1 \dots A_n$ in basis $\theta_1 \dots \theta_n$

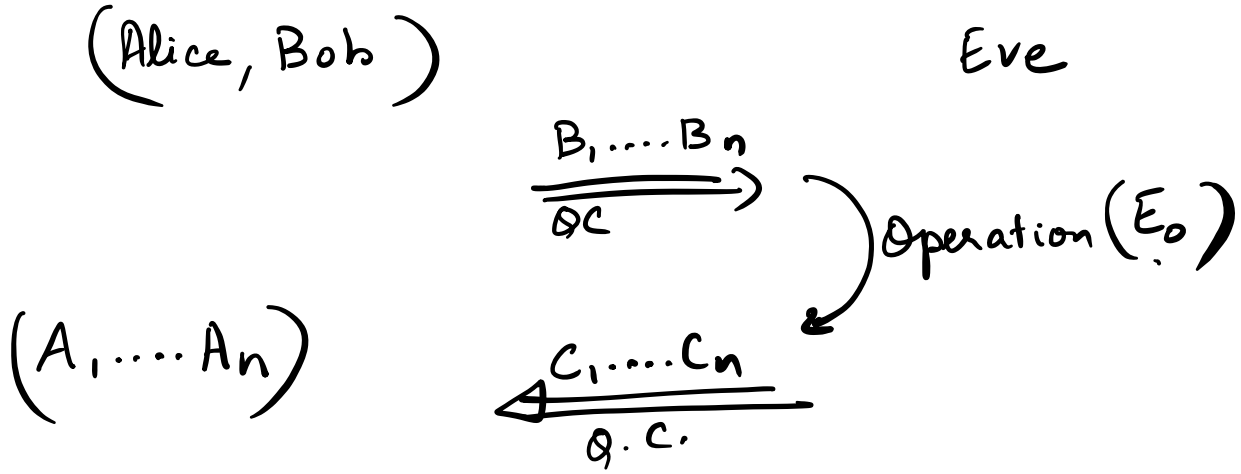
$\{x_i\}_{i \in [n] \setminus S}$

$\{\theta_i\}_{i \in [n]}, S, \{x_i\}_{i \in S}$ →

← Fails / Passes

measure in θ, same check as before.

$\{y_i\}_{i \in [n] \setminus S}$



C.C. $\theta, S, \{x_i\}_{i \in S}$ →

* Measure $A_1 \dots A_n$ in basis $\theta_1 \dots \theta_n \to x_1 \dots x_n$
* Measure $C_1 \dots C_n$ in basis $\theta_1 \dots \theta_n$
  to obtain $Y_1 \dots Y_n$
* Test if $\{x_i = y_i\}_{i \in S}$.

→ 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".

$|\psi\rangle_{ACE_0}$ —after the check→ $|\psi\rangle_{\Theta XYE_0}$

Hybrid classical-quantum state

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

c.b. Θ_1 x_1 y_1

H.b. Θ_2 x_2 y_2

Θ_n

$\forall i, \mathrm{CNOT}(A_i, C_i)$

A C

$w_1 = x_1$ $z_1 = x_1 \oplus y_1$

$z_2 = x_2 \oplus y_2$ $w_2 = y_2$

$00 \to 00$
$01 \to 01$
$10 \to 11$
$11 \to 10$

$$H^{\otimes 2}\left(\mathrm{CNOT}\left(H^{\otimes 2}(x_2 y_2)\right)\right)$$

$$= H^{\otimes 2}\left(\mathrm{CNOT}\left(\sum_{\sigma_1,\sigma_2}(-1)^{\langle \sigma_1\sigma_2, x_2y_2\rangle}|\sigma_1\sigma_2\rangle\right)\right)$$

$$= H^{\otimes 2}\left(\sum_{\sigma_1\sigma_3}(-1)^{\langle \sigma_1 \sigma_1\oplus\sigma_3, x_2y_2\rangle}|\sigma_1\ \sigma_1\oplus\sigma_3\rangle\right)$$

$$= \sum_{p,q}\left(\sum_{\sigma_1\sigma_3}\left((-1)^{\langle pq,\sigma_1\sigma_3\rangle}\cdot(-1)^{\langle \sigma_1\sigma\oplus\sigma_3, x_2y_2\rangle}\right)|p,q\rangle\right)$$

$$= \sum_{p,q} \left(\sum_{\sigma_1 \sigma_3} \left((-1)^{\langle pq, \sigma_1 \sigma_3 \rangle} \cdot (-1)^{\langle \sigma_1 \sigma_2 \oplus \sigma_3, x_2 y_2 \rangle} \right) \right) |p, q\rangle$$

$$\sigma_1 x_2 \oplus \sigma_1 y_2 \oplus \sigma_3 y_2$$
$$= \sigma_1 (x_2 \oplus y_2) \oplus \sigma_3 (y_2)$$

$$\sum_{\sigma_1 \sigma_3} (-1)^{\langle pq, \sigma_1 \sigma_3 \rangle \oplus \langle \sigma_1 (x_2 \oplus \sigma_3), x_2 y_2 \rangle}$$

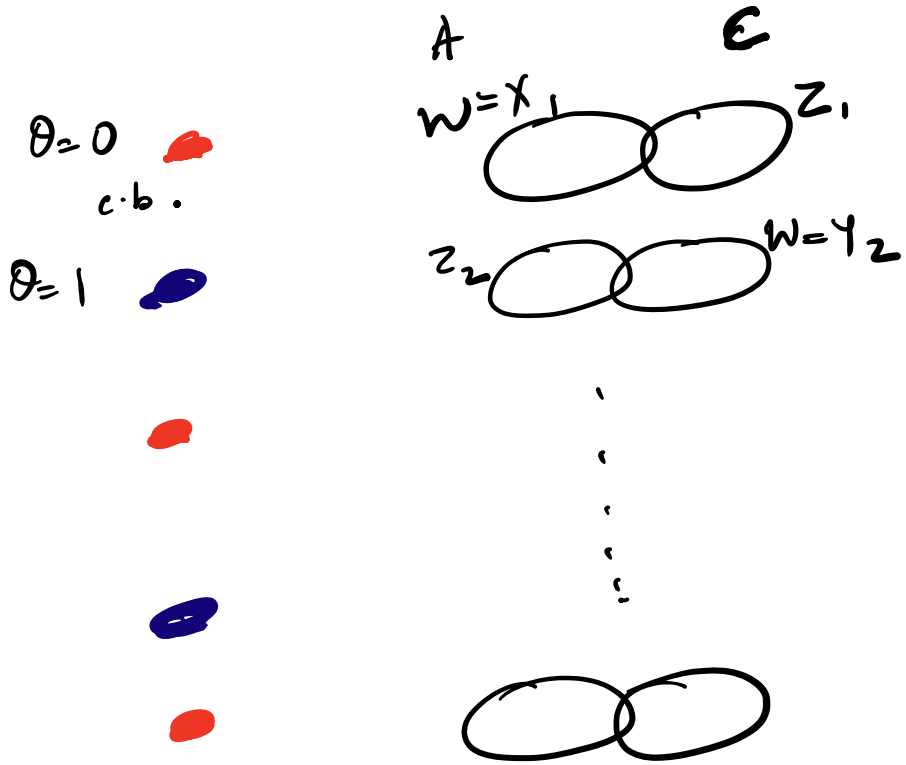
$= 0$ when the term in exponent is NOT identically 0 $\forall \sigma_1 \sigma_3$.

$= 1$ o/w.

term in exponent is identically 0 when.

$$\langle pq, \sigma_1 \sigma_3 \rangle = \sigma_1 (x_2 \oplus y_2) \oplus \sigma_3 (y_2)$$

identically 0 $\Leftrightarrow$ $p = x_2 \oplus y_2$, $q = y_2$.



then sample $S \subseteq [n]$.

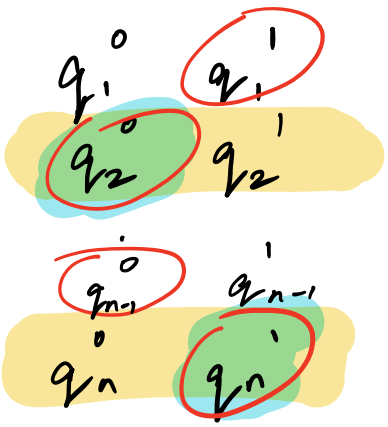
Check if $\{Z_i\}_{i \in S} = 0$.

If it is 0, then sample $\{W_i\}_{i \in \bar{S}}$.

Classical Sampling and estimation

2n-bit string

Write as $n \times 2$ matrix



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

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

Sample $S \subseteq T$ (of size $n/2$), then count #1s in q_S $= W[q_S]$

Use this to estimate $W[q_T] \cdot W[q_{\bar{T}}] \leq 2W[q_S] + \text{small}$

Step 1: Relate q_T and $q_{\bar{T}}$.

Let $L = \{i : q_i^{\cancel{i}^0} \neq q_i^{\cancel{1-i}^1}\}$ Let $\ell = |L|$.

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

$\because W[q_{T|L}] + W[q_{\bar{T}|L}] = \ell$ (because 1 is 0, other is 1 in each row)

$$\Pr\left[\,|w[q_T] - w[q_{\bar{T}}]| \geq n\varepsilon\right] \quad \text{(later)} \leq 2e^{-n\varepsilon^2/2}$$

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

$$= \Pr\left[|w[q_{T|L}] - \ell/2)| \geq \frac{n\varepsilon}{2}\right]$$

$q_{T|L}$ is T restricted to positions where $q_i^0 \neq q_i^1$
So one of them is 0 & the other is 1.
Because T was chosen randomly, every entry in the set $q_{T|L}$ is 0 w.p. $\frac{1}{2}$ & 1 w.p. $\frac{1}{2}$ independently

ℓ such entries, so

$$\mathbb{E}\left[w[q_{T|L}]\right] = \ell/2.$$

Hoeffding's inequality:

For r.v.s $X_1 \ldots X_m$ s.t. $0 \leq X_i \leq 1$,
let $S = X_1 + X_2 \ldots + X_m$

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

Substituting $S = w[q_{T|L}]$, $t = \frac{n\varepsilon}{2}$, $\Rightarrow 2t^2 = \frac{n^2\varepsilon^2}{2}$

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

$$\leq 2^{e^{-n\varepsilon^2/2}}$$

Step 2: relate $W[q_T]$ and $W[q_S]$

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

Recall,

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

$$\Pr\left[\left|\frac{W[q_S]}{|S|} - \frac{W[q_{\bar{T}}]}{|T|}\right| \geq (\varepsilon + \delta)\right]$$

$$\leq 2e^{-\delta^2 n} + 2e^{-\varepsilon^2 n/2}$$

Set ε s.t. $\varepsilon^2/2 = \delta^2$. Then $\leq 4e^{-\delta^2 n}$

$\varepsilon = \sqrt{2}\,\delta$

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

w.p. $4e^{-\delta^2 n}$, $W[q_{\bar{T}}] \leq \delta(1+\sqrt{2}) \cdot n$