Quantum Oblivious Transfer.

CHALLENGER

m_0, m_1

$\forall i \in [n]$,
sample EPR pair
$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$
on regs A_i, B_i

Bob

b

like to learn m_b.

$\xrightarrow{\text{Send } B_1 \ldots B_n}$

$\hat{\theta}_i \leftarrow \{0,1\}^n$

$\forall i$, $\hat{x}_i$ is the result of measuring $|\psi_i\rangle$ in basis θ_i

$\xleftarrow{\forall i,\ str_i := com(\hat{x}_i, \hat{\theta}_i; r_i)}$

$\xrightarrow{T \subset [n],\ |T| = n/2}$

$\xleftarrow{(\hat{x}_i, \hat{\theta}_i, r_i)_{i \in T}}$

$\forall i \in [n]$, $\theta_i \leftarrow \{0,1\}$
x_i is the result of measuring A_i in basis θ_i

$\forall i \in T$,
Check: $str_i = com(\hat{x}_i, \hat{\theta}_i; r_i)$

$\forall i \in T$ where $\theta_i = \hat{\theta}_i$, $x_i = \hat{x}_i$

CHALLENGER

Bob

m_0, m_1

b

like to learn m_b.

$\forall i \in [n]$, sample EPR pair $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ on regs A_i, B_i

Send $B_1 \ldots B_n$ →

$\hat{\theta}_i \leftarrow \{0,1\}^n$

$\forall i$, $\hat{x}_i$ is the result of measuring $|\psi_i\rangle$ in basis θ

$\forall i$, $str_i = com(\hat{x}_i, \hat{\theta}_i ; r_i)$ ←

Find $(\hat{x}_i, \hat{\theta}_i)$ $\forall i \in [n]$
Random $T \subset [n]$ of size $n/2$.
$\forall i \in T$, toss coin.

if coin = HEADS

measure A_i in basis $\hat{\theta}_i$

to obtain x_i.

Check $x_i = \hat{x}_i$

If checks pass $\forall i \in T$ s.t. coin = HEADS then $\forall i \in [n] \setminus T$, our regs A_i are "close to" $|\hat{x}_i\rangle_{\hat{\theta}_i}$

$\forall i$, w.p. $\frac{1}{2}$, $\theta_i \neq \hat{\theta}_i$, → uniform bit measured in θ_i
and then $|\hat{x}_i\rangle_{\hat{\theta}_i}$

T →

$(\hat{x}_i, \hat{\theta}_i, r_i)$ ←

~~Commitment checks~~

$\theta_i \leftarrow \{0,1\}$ $\forall i \in [n] \setminus T$, x_i

θ_i →

$I_b = \{ i \in [n] \setminus T : \theta_i = \hat{\theta}_i \}$

$I_{1-b} = \{ i \in [n] \setminus T : \theta_i \neq \hat{\theta}_i \}$

I_0, I_1 ←

$y_0 = m_0 \oplus \{x_i\}_{I_0}$ | $y_1 = m_1 \oplus \{x_i\}_{I_1}$

~~y_0, y_1~~ →

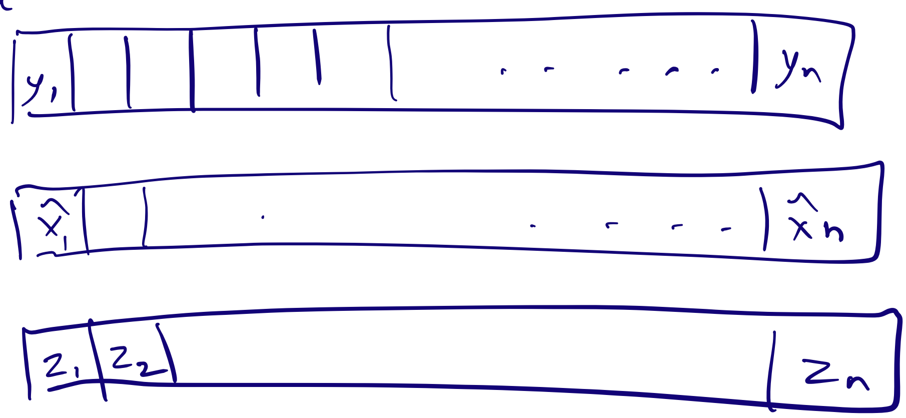
Claim: Define $|\psi_i'\rangle$ as:

$\forall\, i \in [n] \setminus T$, apply $H^{\hat{\theta}_i}$ on register A_i.

Then, $|\psi_1' \ldots \psi_n'\rangle$ is close to a superposition of terms that have $\boxed{\text{low hamming distance}}$ $(\leq \delta n)$ from $(\hat{x}_1 \ldots \hat{x}_n)$ in the computational basis.

[Proof via sampling]

Classical game



$z_i = y_i - \hat{x}_i$

$\Pr[\text{H.W.}(\{z_i\}_{i \in [n] \setminus T}) \geq \delta n] \lesssim 2^{-\delta f(n)}$

Sample $T \subset [n]$ of size $n/2$,

sample $S \subset T$ by picking each $i \in T$ w.p. $\frac{1}{2}$.

Check that $z_i = 0 \quad \forall\, i \in S$.

$z_1 \ldots z_n$ has low Hamming weight $\Rightarrow \{z_i\}_{i \in [n] \setminus T}$ also

APPLICATIONS OF OBLIVIOUS TRANSFER

"Securely compute arbitrary functions" on distributed inputs

A   B

$a_1 \ldots a_n$ $b_1 \ldots b_n$

Classical $\boxed{C(a_1, \ldots a_n, b_1, \ldots b_n)}$

XOR

A   B

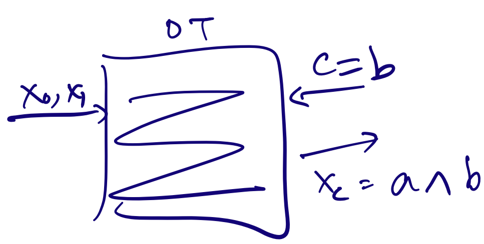
Inputs : a b

$\xrightarrow{\text{Send } a \text{ to Bob}}$

Outputs :   out: $(a \oplus b)$

AND

A   B



a b

$x_0 = a \wedge 0$,
$x_1 = a \wedge 1$

out: $(a \wedge b)$

Securely evaluate

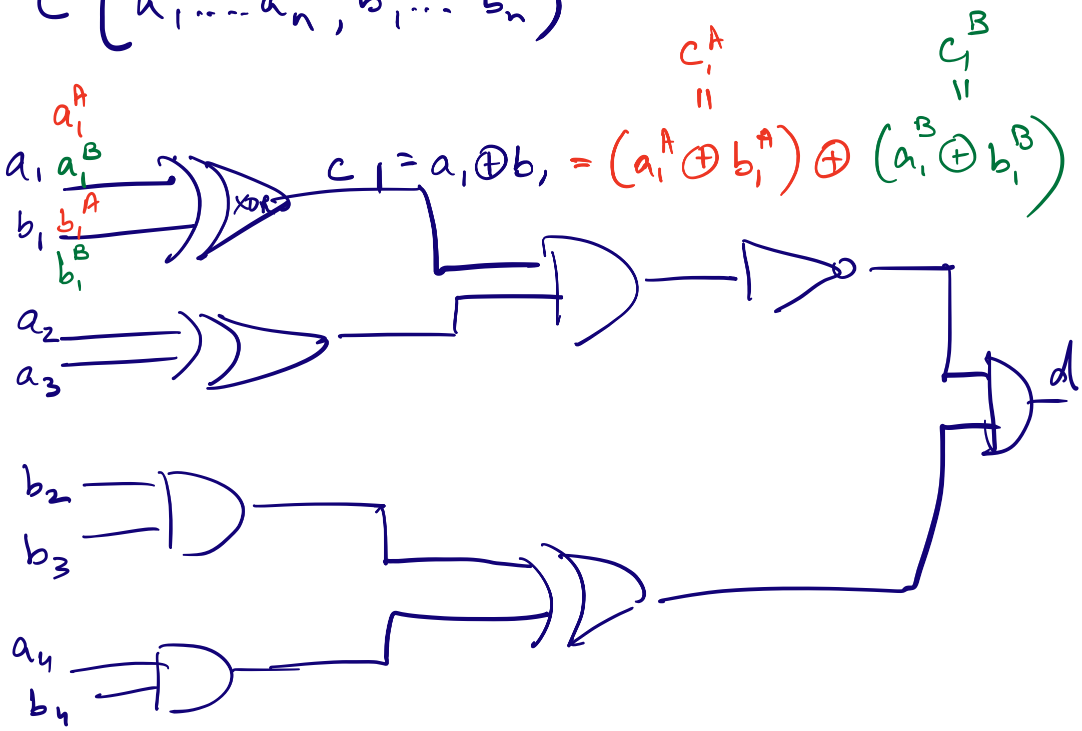
Single-bit output circuits (with polynomial overhead)

$$C(x_1, \dots x_n, y_1, \dots y_n) \to 0/1.$$

A $\qquad\qquad\qquad\qquad$ B

$a_1, \dots a_n$ $\qquad\qquad\qquad$ $b_1, \dots b_n$

$$C(a_1, \dots a_n, b_1, \dots b_n)$$



<u>Secret sharing</u> of each bit $(a_1 \dots a_n)$.

Secret sharing of 0 is a uniform sample from $\{00, 11\}$

$\qquad\qquad\qquad\qquad\quad$ 1 $\qquad\qquad\qquad\qquad\qquad\qquad$ $\{01, 10\}$

$\forall i,$

Secret shares $\qquad a_i \longrightarrow a_i^A, a_i^B$

A

$\forall i, SS(a_i) \longrightarrow a_i^A, a_i^B$

$$\xrightarrow{a_1^B \cdots a_n^B}$$

$\forall i, SS(b_i) \rightarrow b_i^A, b_i^B$

$$\xleftarrow{b_1^A \ldots b_n^A}$$

then evaluate gate-by-gate as on the previous slide.

See linked lecture notes from a previous offering for a detailed description.