COMMITMENTS

"Classical" commitments

Pair of algorithms (Com, Verify) where:

1) $\mathrm{com}(m; r) \to \mathrm{str}$ $\qquad m \in \{0,1\}^p,\ r \in \{0,1\}^\lambda$

2) $\mathrm{Verify}(\mathrm{str}, m'; r') \to 1/0$
Accept / Reject

and such that:

1) Correctness : $\mathrm{Verify}(\mathrm{Com}(m;r), m, r) = 1 \ [\forall m, \forall r]$

2) Binding : $\forall$ str, $\nexists\ (m, r, m', r')$ s.t. $m \neq m'$ and
$\mathrm{Verify}(\mathrm{str}, m, r) = \mathrm{Verify}(\mathrm{str}, m', r') = 1$.

3) Hiding : $\forall m, m'$,
$\mathrm{Com}(m; r) \approx_{\mathrm{negl}(\lambda)} \mathrm{com}(m'; r)$
$\hookrightarrow$ computational indistinguishability

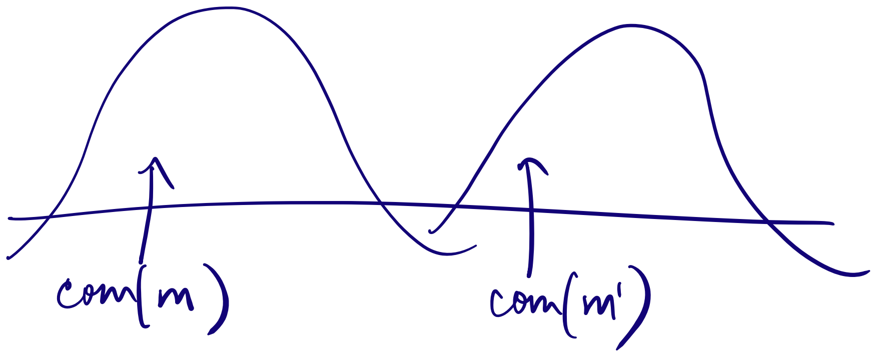
$\forall$ Quantum poly-sized circuit $\mathcal{D}$, $\forall m, \forall m'$,

$$\left| \Pr[\mathcal{D}(\mathrm{com}(m;r)) = 1] - \Pr[\mathcal{D}(\mathrm{com}(m';r)) = 1] \right| \leq \varepsilon$$

Typically, ε is reqd. to be $\boxed{\text{negligible}}$ in $\lambda = |r|$.

A <u>negligible function</u> is one that approaches 0 faster than $\frac{1}{\mathrm{poly}(\lambda)}$

$\boxed{\text{A function } \varepsilon(\cdot) \text{ is called negligible if } \forall c, \exists \lambda_0 \text{ s.t. } \forall \lambda > \lambda_0, \varepsilon(\lambda) < \frac{1}{\lambda^c}.}$



Is $\frac{1}{2^\lambda}$ negligible? Yes.

Is $\frac{1}{\lambda^{10}}$. " ? No.

Is $\frac{1}{2^{\log \lambda}} = \frac{1}{\lambda}$ " ? No

Is $\frac{1}{2^{\log^2 \lambda}} = \frac{1}{\lambda^{\log \lambda}}$ " ? Yes

CORRECT, SECURE AGAINST ALICE, INSECURE AGAINST BOB

Oblivious Transfer Secure Against Malicious Adversaries

$\forall i \in [n],\ x_i \xleftarrow{\$} \{0,1\}$

$\theta_i \xleftarrow{\$} \{0,1\}$

(m_0, m_1) bits

$\{|\psi_i\rangle = |x_i\rangle_{\theta_i}\}_{i\in[n]} \longrightarrow$

"I measured" $\longleftarrow$

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

$I_0, I_1 \longleftarrow$

$\cancel{q_0, q_1} \longrightarrow$

$\forall i \in [n]$, measure $|\psi_i\rangle$ in basis $\hat{\theta}_i \leftarrow \{0,1\} \mapsto \hat{x}_i$

(b)

$p_0 = \{\oplus x_i\}_{i \in I_0}$

$p_1 = \{\oplus x_i\}_{i \in I_1}$

$q_0 = p_0 \oplus m_0,\ q_1 = p_1 \oplus m_1$

$(I_b$ is $\{i : \theta_i = \hat{\theta}_i\})$

$\Rightarrow x_i = \hat{x}_i$

Bob computes $\hat{p} = \{\oplus \hat{x}_i\}_{I_b}$

$\hat{m} = q_b \oplus \hat{p} = q_b \oplus p_b = m_b$, $\hat{p} = p_b$

Oblivious Transfer Secure Against Malicious Adversaries

$\forall i \in [n],\ x_i \xleftarrow{\$} \{0,1\}$

$\theta_i \xleftarrow{\$} \{0,1\}$

$\{|\psi_i\rangle = |x_i\rangle_{\theta_i}\}_{i\in[n]} \longrightarrow$

didn't actually measure!

$\longleftarrow$ "I measured"

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

(m_0, m_1)

bits

(b)

$\longleftarrow I_0, I_1$

$\forall i \in [n]$, measure $|\psi_i\rangle$ in basis $\theta_i \to \hat{x}_i$

Partitions $[n]$ into I_0, I_1 randomly.

$p_0 = \{\oplus x_i\}_{i \in I_0}$

$p_1 = \{\oplus x_i\}_{i \in I_1}$

$\cancel{q_0, q_1} \longrightarrow$

$q_0 = p_0 \oplus m_0,\ q_1 = p_1 \oplus m_1$

$m_0 = q_0 \oplus \{\hat{x}_i\}_{i\in I_0}$ problem!

$m_1 = q_1 \oplus \{\hat{x}_i\}_{i\in I_1}$

Oblivious Transfer Secure Against Malicious Adversaries

$\forall i \in [n],\ x_i \xleftarrow{\$} \{0,1\}$

$\theta_i \xleftarrow{\$} \{0,1\}$

$\xrightarrow{\{|\psi_i\rangle = |x_i\rangle_{\theta_i}\}_{i\in[n]}}$

$\forall i \in [n]$, measure $|\psi_i\rangle$ in basis $\hat{\theta}_i \leftarrow \{0,1\} :\to \hat{x}_i$

PROOF OF MEASUREMENT

$\longleftarrow$

(m_0, m_1) bits

(b)

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

$\xleftarrow{I_0,\ I_1}$

$(I_b$ is $\{i : \theta_i = \hat{\theta}_i\})$

$\Rightarrow x_i = \hat{x}_i$

$p_0 = \{\oplus x_i\}_{i\in I_0}$

$p_1 = \{\oplus x_i\}_{i\in I_1}$

$\xrightarrow{q_0,\ q_1}$

Bob computes $\hat{p} = \{\oplus \hat{x}_i\}_{I_b} = p_b$

$q_0 = p_0 \oplus m_0,\ q_1 = p_1 \oplus m_1$

$\hat{m} = q_b \oplus \hat{p} = q_b \oplus p_b = m_b$

Zooming into the proof of measurement.

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

$$\xrightarrow{\{|\psi_i\rangle\}_{i\in[n]}}$$

$\forall i$, sample $\hat{\theta}_i \leftarrow \{0,1\}$.

to obtain $\hat{x}_i$

$$\xleftarrow{str_i = Com\left((\hat{x}_i, \hat{\theta}_i); r_i\right)}$$

random $T \subseteq [n]$, $|T| = \frac{n}{2}$

$$\xrightarrow{T}$$

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

$\forall i \in T$

1> $Verify\left(str_i, (\hat{x}_i, \hat{\theta}_i), r_i\right) = 1$.

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

If check passes $\qquad \xrightarrow{\theta_i}$

I_0, I_1 as partitions of $[n]\setminus T$ s.t. $I_b = \{i : \theta_i = \hat{\theta}_i\}$.

$$\xleftarrow{I_0, I_1}$$

$q_0 = m_0 \oplus p_0$

$q_1 = m_1 \oplus p_1$

$$\xrightarrow{q_0, q_1}$$

$m_b = q_b \oplus \{\oplus \hat{x}_i\}_{I_b}$

Security against Bob.

Alice

x_i , θ_i

$\widetilde{\text{Bob}}$

EPR pair halves

$\xrightarrow{\cancel{|x_i\rangle}}$

$\hat{x}_i$, $\hat{\theta}_i$

$\xleftarrow{\boxed{\text{str}_1 \dots \text{str}_n}}$

Alice's EPR registers

for $T \subseteq [n]$, computer $(\hat{x}_i, \hat{\theta}_i)$,
Sample S.
measure her regs in basis $\hat{\theta}_i$
to obtain x_i. Matches x_i
against $\hat{x}_i$.

$\xrightarrow{T}$

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

1) Verify commitments

2) $\forall i \in [n]$ s.t. $\theta_i = \hat{\theta}_i$,
$x_i = \hat{x}_i$

(passes check)

$\xrightarrow{\{\theta_i\}_{i \in [n] \setminus T}}$

$\xleftarrow{I_0, I_1}$

$\xrightarrow{q_0, q_1}$

EQUIVALENT GAME.

Alice | Bob

$\left(\frac{|00+11\rangle}{\sqrt{2}}\right)^{\otimes n}$

$\xrightarrow{\text{EPR pair-halves}}$

$\xleftarrow{\{str_i\}_{i\in[n]}}$

$= (\hat{x}_i, \hat{\theta}_i)_{i\in[n]}$

Sample T.

$\forall str_i \ \exists$ at most one $(\hat{x}_i, \hat{\theta}_i)$ that Bob can open it to

00
01
10
11

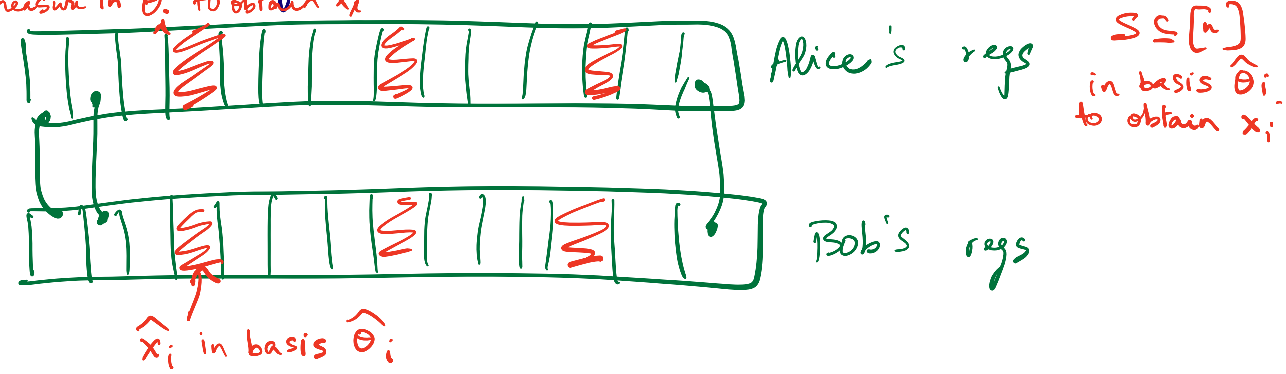
$\{(\hat{x}_i, \hat{\theta}_i)\}_{i\in T}$

$\{\theta_i \xleftarrow{\$} \{0,1\}\}_{i\in T}$, $S = \{i : \hat{\theta}_i = \theta_i\}$

Measure EPR registers for the set S in basis $\theta_i = \hat{\theta}_i$ to obtain $\{x_i\}_{i\in S}$. Check $\forall i \in S$, $x_i = \hat{x}_i$.

Leave other registers unmeasured

measure in $\hat{\theta}_i$ to obtain x_i

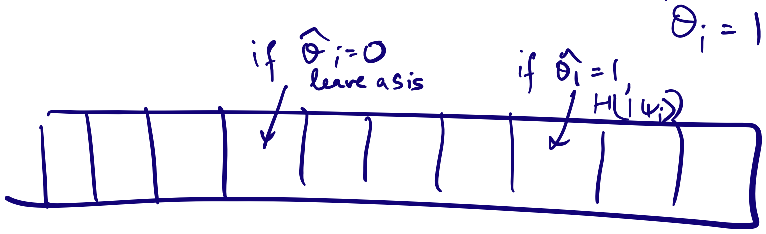


Suppose $\forall i \in S$, : $x_i = \hat{x}_i$.

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

$\forall\, i \in [n] \setminus T$, rotate reg holding $|\psi_i\rangle$ by $H^{\hat{\theta}_i}$

(i.e. if $\hat{\theta}_i = 0$, then leave as is,
$\hat{\theta}_i = 1$, then $H|\psi_i\rangle$)



$(\hat{x}_i, \hat{\theta}_i)_{i \in [n]}$.

Then conditioned on the check above passing, state $\{|\psi_i'\rangle\}_{i\in[n]}$ is close to a superposition over low Hamming weight terms.

Measure $\{|\psi_i'\rangle\}_{i \in [n]\setminus T}$ in basis $\theta_i \rightarrow x_i$

But θ_i's are sampled uniformly in {comp, Had}.

Thus, about half the positions are low H.W. Comp. basis terms measured in Had. basis.