Commitment

\[ A \rightarrow \text{Commit} \rightarrow \text{"ack"} \rightarrow B \]

\[ \text{"open"} \rightarrow \text{Open} \rightarrow m \]

Hiding: B does not learn \( m \) during commit phase.

Binding: A cannot change her mind (i.e., \( m \) in open phase \( = m \) in commit phase).

Correctness: If A & B honest, commit & open phase succeed & B gets \( m \).

Com's occur in many crypto protos.

Classically: Impossible to conduct com that is inf-theo hiding & binding.

Quantumly?

In early 90s, an inf-theo hiding & binding Q-com was proposed.

In a setting, given a com, we can perform arb. secure function eval. (with inf-theo sec)

Later: General imposs.
Definitions (for case $m \in \{0, 1\} \equiv \# commitments)

1. Correctness: Com proto is $E_{\text{corr}}$-correct iff:
   When $A \& B$ exec. commit & open phase
   and $A$ uses input $x$,
   then $R[A]$ outputs $m = \frac{1}{2} - E_{\text{corr}}.$

2. Hiding: Com proto is $E_{\text{hiding}}$-hiding iff:
   Fix some also $B$.
   Let $s_{AB}$ be the state of $A \& B$
   after commit phase ($A$ gets input $x$)
   Then: $TV(T_{s_{AB}}, T_{s_{AB}^*}) \leq E_{\text{hiding}}$

3. Binding: Com proto is $E_{\text{binding}}$-binding iff:
   Fix $A, A_0, A_1$
   $P_0 = R[B]$ outputs 0 after running with
   $A$ in com & $A_0$ in open phase
   Then $P_0 + P_1 \leq 1 + E_{\text{binding}}.$
   Fix $A, A_0, A_1$
   $P_1 = R[B]$ outputs 1 after running with
   $A$ in com & $A_1$ in open phase
   Then $P_0 + P_1 \leq 1 + E_{\text{binding}}.$

Thus: $\exists \epsilon > 0$ s.t.
$\forall$ com proto that is
$E_{\text{corr}}, E_{\text{binding}}, E_{\text{hiding}}.
$Thm.$: For any $O_{\text{hiding}}, O_{\text{correct}}$ com proto,
we have that the proto is not
$E_{\text{binding}}$ (for any $\epsilon < 1$)
Mathematical tool: Schmidt decomposition

Thm: Fix a vector $|\psi\rangle \in \mathcal{L}_A \otimes \mathcal{L}_B$

Then there are ONBs $\{ |\alpha_i\rangle \}$ of $\mathcal{L}_A$ and $\{ |\beta_i\rangle \}$ of $\mathcal{L}_B$

and some scalars $\lambda_i \geq 0$, and set $I$ s.t.:

$$|\psi\rangle = \sum_{i \in I} \lambda_i |\alpha_i\rangle \otimes |\beta_i\rangle$$

Simultaneous Schmidt decomposition:

If $\delta_A 14 = \delta_A 14$, then $\exists$ Schmidt decomps of $|14\rangle$, $|14\rangle$

s.t. $|\alpha\rangle = |\beta\rangle$, $\lambda_i = \lambda_i$ (but possibly $|\alpha\rangle \neq |\beta\rangle$)

Impossibility proof

Assume some com protocol with A, B.

Assume protocol is $O$-correct, $O$-hiding.

Why: A&B are unitary $O$-circuits

Let $s_{AB}$ be state after commit phase

with honest A&B.

$A&B$ unitary $\Rightarrow s_{AB}^m = 14^m \times 4^m$

$O$-hiding $\Rightarrow \delta_A s_{AB}^0 = \delta_A s_{AB}^1$

$\Rightarrow \delta_A 14^0 \times 4^1 = \delta_A 14^1 \times 4^1$

Simult. Schmidt decomp:

$|14^0\rangle = \sum |\alpha_i\rangle \otimes |\beta_i\rangle$ (with $\langle \alpha_i | \alpha_i \rangle = \langle \beta_i | \beta_i \rangle$)

$|14^1\rangle = \sum |\alpha_i\rangle \otimes |\beta_i\rangle$ (with $\langle \alpha_i | \alpha_i \rangle = \langle \beta_i | \beta_i \rangle$)

$\exists$ unitary $U$: $|\alpha_i\rangle = U |\alpha_i\rangle \ \forall i$
Attack against binding

Com-phase A: Honest A with m=0

Open-phase A₀: Honest A

\[ P₀ = R₁[B \text{ output}, 0] = 1 \]

Open-phase A₁:

State after com-phase: \( 14° = \sum _i \chi _i | \alpha _i > | \beta _i > \)

Aₙ applies U to A's register

New state is:

\[ \sum _i | \alpha _i > U | \alpha _i > | \beta _i > = \sum _i | \beta _i > = 14° \]

A₂₀ hold the state they would have had after honest com to m=1.

A runs honest A open phase

\[ \text{0-correctness} \Rightarrow P₁ = R₁[B \text{ output}, 1] = 1 \]

\[ P₀ + P₁ = 2 \neq 1 + ε_{bid} \text{ for any } ε_{bid} < 1 \]