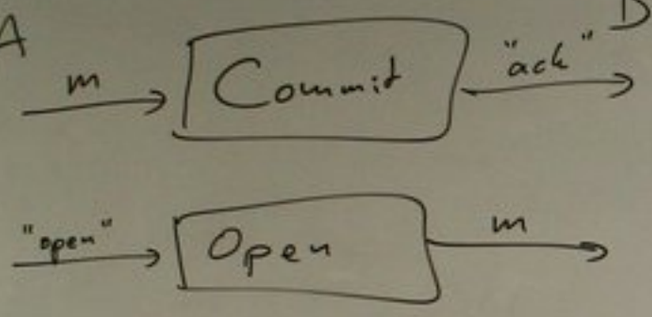
Commitment



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.

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

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

Quantumly?

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

→ But: broken

→ Later: General imposs.

2020-05-18_3927.jpg

Definitions (for case $m \in \{0,1\} \triangleq$ bit commitments)

① **Correctness**: Com proto is ε_{corr}-correct iff:

When A&B exec. honestly commit & open phase
and A uses input m,
then $R[B \text{ outputs } m] \geq 1 - \varepsilon_{corr}$

② **Hiding**: Com proto is ε_{hid}-hiding iff:

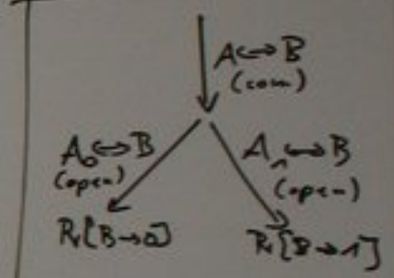
Fix some algo B.
Let ρ^m_{AB} be the state of A&B after commit phase (A gets input m, A honest)
Then: $TD(tr_A \rho^0_{AB}, tr_A \rho^1_{AB}) \leq \varepsilon_{hid}$

③ **Binding**: Com proto is ε_{bind}-binding if:

Fix A, A_0, A_1
$P_0 := R[B \text{ outputs } 0 \text{ after running with } A \text{ in com \& } A_0 \text{ in open phase}]$
$P_1 := R[B \text{ outputs } 1 \text{ after running with } A \text{ in com \& } A_1 \text{ in open phase}]$
Then $P_0 + P_1 \leq 1 + \varepsilon_{bind}$.

Thm: $\exists \varepsilon > 0$ s.t.
$\nexists$ com proto that is
ε-corr, ε-binding, ε-hiding.

Thm: For any 0-hiding, 0-correct com proto, we have that the proto is not ε-binding (for any $\varepsilon < 1$)



2020-05-18_3928.jpg

Mathematical tool:

Schmidt decomposition

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

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

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 decomp:

If $\mathrm{tr}_A |\psi\rangle\langle\psi| = \mathrm{tr}_A |\hat{\psi}\rangle\langle\hat{\psi}|$,

then $\exists$ Schmidt decomps of $|\psi\rangle, |\hat{\psi}\rangle$

s.t. $|\beta_i\rangle = |\hat{\beta}_i\rangle$, $\lambda_i = \hat{\lambda}_i$ (but possibly $|\alpha_i\rangle \neq |\hat{\alpha}_i\rangle$)

Impossibility proof

Assume some com protocol with A, B.

Assume protocol is 0-correct, 0-hiding.

WLOG: A & B are unitary $\mathcal{O}$-circuits

Let ρ_{AB}^m be state after commit phase with honest A&B.

A&B unitary $\Rightarrow$ $\rho_{AB}^m = |\psi^m\rangle\langle\psi^m|$

0-hiding $\Rightarrow$ $\mathrm{tr}_A \rho_{AB}^0 = \mathrm{tr}_A \rho_{AB}^1$

$\Rightarrow \mathrm{tr}_A |\psi^0\rangle\langle\psi^0| = \mathrm{tr}_A |\psi^1\rangle\langle\psi^1|$

Simult. Schmidt decomp:

$$|\psi^0\rangle = \sum \lambda_i \, |\alpha_i\rangle |\beta_i\rangle \quad (\{|\alpha_i\rangle\}, \{|\beta_i\rangle\} \text{ ONB})$$

$$|\psi^1\rangle = \sum \lambda_i \, |\hat{\alpha}_i\rangle |\beta_i\rangle \quad (\{|\hat{\alpha}_i\rangle\} \text{ ONB})$$

$\exists$ unitary U: $|\hat{\alpha}_i\rangle = U|\alpha_i\rangle \; \forall_i$

Attack against binding

Com-phase A: Honest A with $u=0$

Open-phase A_0: Honest A

0-correctness $\Rightarrow P_0 = R_1[B \text{ outputs } 0] = 1$

Open-phase A_1:

State after com-phase: $|\psi^0\rangle = \sum_i \lambda_i |\alpha_i\rangle |\beta_i\rangle$

A_1 applies U to A's register

$\rightsquigarrow$ state is: $\sum_i \lambda_i U|\alpha_i\rangle |\beta_i\rangle$

$= \sum_i \lambda_i |\tilde{\alpha}_i\rangle |\beta_i\rangle = |\psi^1\rangle$

A&B hold the state they would have had after honest com to $u=1$.

A runs honest A open phase

0-correctness $\Rightarrow P_1 = R_1[B \text{ outputs } 1] = 1$

$\Rightarrow P_0 + P_1 = 2 \not\leq 1 + \varepsilon_{hid}$ for any $\varepsilon_{hid} < 1$

2020-05-18_3930.jpg