- Scribes?
- lecture recording

- Commitment schemes
- A ZKPoK for all of NP
- WI; an $O(1)$-round WIPoK

Commitment schemes:

- Binding: After the commitment phase, there should be at most one m that S^* could validly decommit to
- Hiding: after the commitment phase, R^* has no information about m

ZKPoK for L_{HAM}

$\underline{P(G, w)}$ $\qquad\qquad\qquad\qquad$ $\underline{V(G)}$

randomly permute G

$$A = \begin{pmatrix} Com(G'_{1,1}) & \cdots & \\ \vdots & \ddots & \vdots \\ & \cdots & Com(G'_{n,n}) \end{pmatrix} \longrightarrow$$

$b \leftarrow \{0,1\}$

if $b=0$ $\quad \xleftarrow{\quad b \quad}$

open every commitment, reveal π $\quad \xrightarrow{\text{decommitments}}$ $\quad$ verify...

if $b=1$, open commitments corresponding to w

Repeat n times

Theorem

This protocol is zero knowledge

Proof

Fix some (cheating, poly-time) V^*. Construct Sim as follows:

Sim(G)

For $i = 1, \ldots, n$:

- for $j = 1, \ldots, n$ do:
  - guess $b_i' \leftarrow \{0,1\}$
  - generate committed adj. matrix A consistent w/ b_i'
  - run V^* on A to get b_i
  - if $b_i = b_i'$, send response and break
  - else, go back to step 1

Output the entire transcript

Ideal

Hybrid

For $i = 1, \ldots, n$:

- for $j = 1, \ldots, n$ do:
  - guess $b_i' \leftarrow \{0,1\}$
  - generate committed adj. matrix A honestly
  - run V^* on A to get b_i
  - if $b_i = b_i'$, send response and break
  - else, go back to step 1

Output the entire transcript

Claim

Hybrid is statistically close to Real

Proof

With overwhelming probability, Hybrid generates a complete transcript.
Conditioned on generating a complete transcript, Hybrid = Real.

Claim

Hybrid is comp. indistinguishable from Ideal

Proof

By hiding of commitment scheme.

H

For $i = 1, \ldots, n$

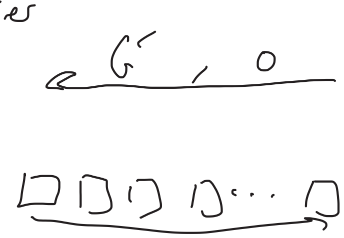
For $j = 1, \ldots, n$

$b_j^i \leftarrow \{0,1\}$

if $b_j^i = 0$, commit honestly

if $b_j^i = 1$

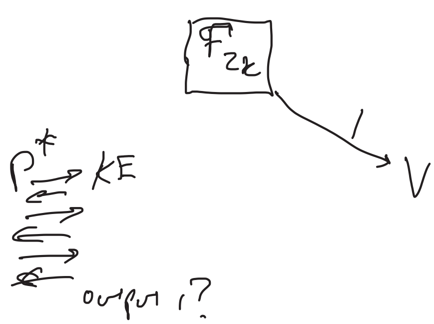
Committer



$$A = \begin{pmatrix} \square & \mathrm{Com}(1) & \square & \square \\ \square & \square & & \mathrm{Com}(1) \\ \mathrm{Com}(1) & \square & & \square \\ \square & \square & \mathrm{Com}(1) & \end{pmatrix}$$

Theorem

This protocol is a proof of knowledge.



P^*

$\xrightarrow{\quad A \quad}$

$\xleftarrow{\quad 0 \quad}$

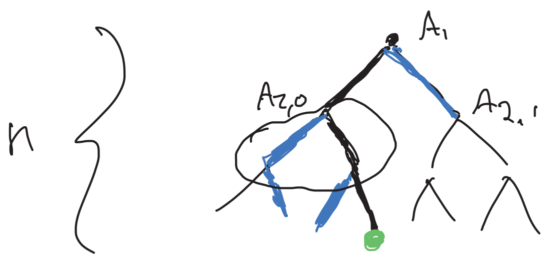
$\boxed{\text{open } A, \pi \rightarrow}$

$\xleftarrow{\quad 1 \quad}$

$\boxed{\text{open a cycle in } A \rightarrow}$

Proof

First interact w/ P^* exactly as an honest verifier would. If the execution results in 0, stop. If the execution gives 1, do:

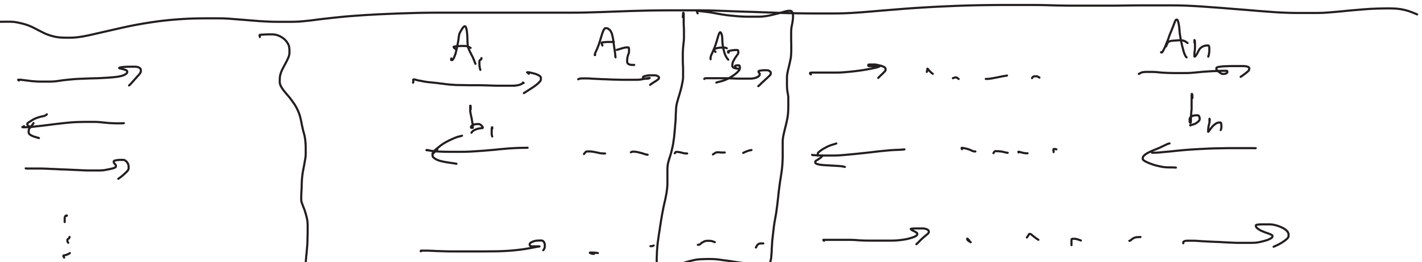


if $\Pr[P^* \text{ convinces } V] > 2^{-n}$,

this is guaranteed to extract a witness

if $\Pr[P^* \text{ convinces } V] = 2^{-n}$

$\Longrightarrow$ Simulation will be statistically close to a real-world execution



no proof of ZK!
it is a PoK

It is witness indistinguishable (WI)
$ZK \Rightarrow WI$