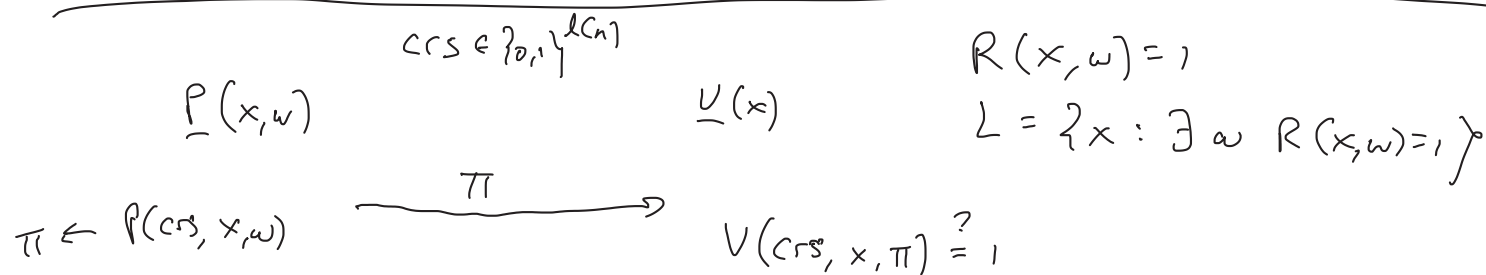


- scribes?
- lecture recording

Non-interactive (ZK) proofs

- Common random string or
Common reference string
- Random-oracle model



Soundness

$\forall x \notin L, \forall$ poly-time P^*

$$\Pr_{crs \leftarrow \{0,1\}^{\ell(n)}} \left[\pi \leftarrow P^*(crs, x) : V(crs, x, \pi) = 1 \right] \leq \text{negl}(n)$$

Adaptive soundness

$$\forall \text{ poly-time } P^*, \Pr \left(crs \leftarrow \{0,1\}^{\ell(n)} ; (x, \pi) \leftarrow P^*(crs) : V(crs, x, \pi) = 1 \wedge x \notin L \right) \leq \text{negl}(n)$$

Known how to convert proofs w/ soundness to proofs w/ adaptive soundness

Extraction

\exists PPT Ext s.t.

$$(1) \left\{ (crs, td) \leftarrow \text{Ext}(1^n) : crs \right\} \approx \left\{ crs \leftarrow \{0,1\}^{\ell(cn)} : crs \right\}$$

$$(2) \forall \text{PPT } P^* \Pr \left((crs, td) \leftarrow \text{Ext}(1^n); (x, \pi) \leftarrow P^*; w \leftarrow \text{Ext}(td, x, \pi) : \right. \\ \left. V(crs, x, \pi) = 1 \wedge R(x, w) \neq 1 \right) \leq \text{negl}(n)$$

Adapted

Zero-Knowledge

\exists PPT simulator Sim s.t. the following are indistinguishable
for any PPT A outputting (x, w) s.t. $R(x, w) = 1$

$$\left\{ crs \leftarrow \{0,1\}^{\ell(n)}; (x, w) \leftarrow A(crs); \pi \leftarrow P(crs, x, w) : (crs, \pi) \right\}$$

\approx

$$\left\{ (crs, td) \leftarrow \text{Sim}(1^n); (x, w) \leftarrow A(crs); \pi \leftarrow \text{Sim}(td, x) : (crs, \pi) \right\}$$

• Define "hidden-bits model"

• Show that NIZK in hidden-bits model \Rightarrow NIZK in standard model,
assuming trapdoor permutations

• Show NIZK in hidden-bits model

$$\boxed{0} \quad 0 \quad \boxed{1} \quad \dots \quad 0$$

$$\underline{P(c_1, \dots, c_\ell)}$$

$$\underline{\pi, \mathcal{I}, \{c_i\}_{i \in \mathcal{I}}}$$

\underline{V}

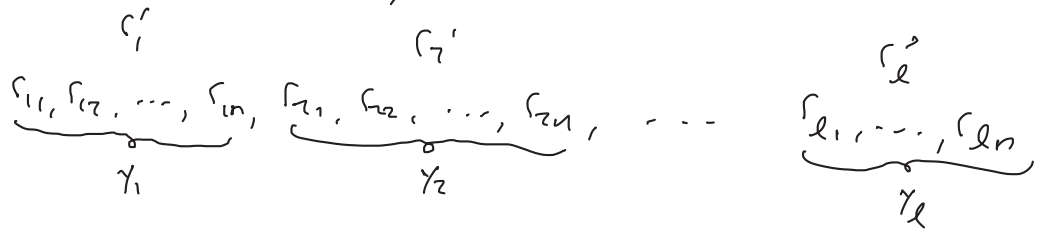
Trapdoor permutation : f, f^{-1} , $f: \{0,1\}^n \rightarrow \{0,1\}^n$ permutation
 anyone can compute f
 only someone knowing a trapdoor can compute f^{-1}

hard-core bit : $h: \{0,1\}^n \rightarrow \{0,1\}$

For all ppt A :

$$\Pr \left((f, f^{-1}) \leftarrow \text{Gen}(1^n); x \leftarrow \{0,1\}^n : A(f, f(x)) = h(x) \right) \leq \frac{1}{2} + \text{negl}(n)$$

Given NIZK in hidden-bits model, construct NIZK in standard model



$\underline{P}(C, w)$

$\underline{V}(C)$

$(f, f^{-1}) \leftarrow \text{Gen}(1^n) \xrightarrow{f}$

$c_i' = h(f^{-1}(y_i))$

$\pi, I, \{f^{-1}(y_i)\}_{i \in I} \xrightarrow{?}$ check $f(x_i) = y_i$

$c_i' = h(x_i)$

can U for hidden-bits model



n^2 bits, corresponding to adjacency matrix for Cycle graph

$P(G, w)$

$V(G)$

pick permutation π that maps the cycle in G to the cycle in the CRS.

$I = \{\text{non-edges in } \pi(G)\}$

$\xrightarrow{\pi, \{c_{ij}\}_{ij \in I}}$

1) all $\{c_{ij}\}_{ij \in I}$ are opened

2) $c_{ij} = 0$ for all $ij \in I$

Claim: This has perfect soundness.

Claim: This has perfect Zk.

Start w/ CRS where each bit is 1 w/ prob. $\frac{1}{nG}$ and 0 otherwise

look at $n^3 \times n^3$ matrix M

M is useful if it contains $n \times n$ submatrix that is a cycle graph, and all other entries of M are 0

Claim: w/ noticeable prob, M is useful