- Scribes?
- lecture recording

Non-interactive (ZK) proofs

- $\boxed{\text{Common random string or Common reference string}}$
- Random-oracle model

$crs \in \{0,1\}^{\ell(n)}$

$\underline{P}(x,w)$ $\qquad$ $\underline{V}(x)$ $\qquad$ $R(x,w)=1$

$L = \{x : \exists w\ R(x,w)=1\}$

$\pi \leftarrow P(crs, x, w) \xrightarrow{\ \pi\ } V(crs, x, \pi) \stackrel{?}{=} 1$

<u>Soundness</u>

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

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

<u>Adaptive soundness</u>

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

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

Extraction

$\exists$ PPT Ext s.t.

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

(2) $\forall$ PPT P^* $\Pr[(crs, td) \leftarrow Ext(1^n);\ (x, \pi) \leftarrow P^*;\ w \leftarrow Ext(td, x, \pi) :$
$V(crs, x, \pi) = 1 \wedge R(x, w) \neq 1] \leq negl(n)$

Adaptive Zero-Knowledge

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

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

&

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

- Define "hidden-bits model"
- Show that NIZK in hidden-bits model $\Longrightarrow$ NIZK in standard model, assuming trapdoor permutations
- Show NIZK in hidden-bits model

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

$\underline{P}(r_1, \ldots, r_\ell)$ $\qquad\qquad\qquad\qquad$ $\underline{V}$

$$\xrightarrow{\pi,\ I,\ \{r_i\}_{i \in I}}$$

<u>Trapdoor permutation</u> : f, f^{-1}, $f : \{0,1\}^n \to \{0,1\}^n$, permutation

anyone can compute f

only someone knowing a trapdoor can compute f^{-1}

<u>hard-core bit</u> : $h : \{0,1\}^n \to \{0,1\}$

For all PPT A :

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

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

$$\overset{r'_1}{\underbrace{r_{11}, r_{12}, \dots, r_{1n}}_{y_1}},\ \overset{r'_2}{\underbrace{r_{21}, r_{22}, \dots, r_{2n}}_{y_2}},\ \dots\ \overset{r'_\ell}{\underbrace{r_{\ell 1}, \dots, r_{\ell n}}_{y_\ell}}$$

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

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

$r'_i = \underline{h(f^{-1}(y_i))}$

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

$r'_i = h(x_i)$

run V for hidden-bits model

$$\underbrace{\boxed{0}\ \boxed{0}\ \boxed{0}\ \cdots\ \boxed{1}}$$

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

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

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

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

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

1) all $\{r_{ij}\}_{ij \in I}$ are opened
2) $r_{ij} = 0$ 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. $\frac{1}{n^6}$ 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