LECTURE 23

(AMA)

Prove : Non-interactive zero-knowledge is impossible in the "plain model".
for NP

HW : Prove "deterministic" ZK for NP is imp. in the plain model

Prover ~~random string~~ **Verifier**

$x \in L$

Suppose NIZK exists in the plain model.

$\Rightarrow \exists$ PPT Simulator Sim s.t.

$\mathrm{Sim}(x) \rightarrow \pi$ which is

indistinguishable from $P(x, w) \rightarrow \pi'$.

$\Rightarrow$ Consider P^* given $x \in L$

runs $\mathrm{Sim}(x) \rightarrow \pi$ s.t. $\mathrm{Ver}(\pi) = 1$

Hard problems in NP. where $x \in L \approx_c x \notin L$.

$\Rightarrow$ Consider P^* given $x' \notin L$.

runs $\mathrm{Sim}(x') \rightarrow \pi$.

s.t. $\mathrm{Ver}(\pi) = 1$.

$\Rightarrow$ This contradicts soundness.

NI Zero-knowledge for NP in the RO model

Graph 3-col is NP-hard $\Rightarrow$ Any x of an NP lang L can be transformed to graph G that is 3col iff $x \in L$.

Karp.

Prover

x, w, L

G c $\{3\text{-col graphs}\}$

RO

c $(i,j) = H(c)$.

$c = com(colors)$

Verifier

x, L

G $\{3\text{-col graphs}\}$

$c = com(colors),\ H(c) \to (i,j),\ (color_i, color_j)$

RGB

$c_1 = \text{com}(\text{fresh colors}) \longrightarrow$

$\longleftarrow (i,j)$

$\longrightarrow col_i, col_j$

GBR

$c_2 = \text{com}(\text{fresh colors}) \longrightarrow$

$\longleftarrow (i',j')$

$\longrightarrow col_{i'}, col_{j'}$

$\cdots$

$c_n = \text{com}(\text{fresh colors}) \longrightarrow$

$\longleftarrow (\tilde{i}, \tilde{j})$

$\longrightarrow col_{\tilde{i}}, col_{\tilde{j}}$

$R \longrightarrow G$

$G \longrightarrow B$

$B \longrightarrow R$

$\frac{1}{2^{n \log n}}$

$H: \{0,1\}^{n^2} \longrightarrow \{0,1\}^{n \log n}$

$c = c_1 c_2 \cdots c_n, \quad \overset{\log n}{(i,j)}, (i',j')(i'',j'') = H(c_1 c_2 \cdots c_n),$

$(col_i\, col_j\, col_{i'}\, col_{j'} \cdots)$

$H(c) \longrightarrow (i,j)$

$H: \{0,1\}^{n^2} \longrightarrow \{0,1\}^{\log n}$

$\frac{1}{2^{\log n}} \sim \frac{1}{n}$

$c = com(v; r)$

p.t. [c is a commitment to v s.t. $0 \le v \le 10$.]

NP instance $\longleftarrow$ $x := c$

NP lang. $\longleftarrow$ $L = \{ c' \text{ s.t. } \exists (v, r) \text{ s.t. } c' = com(v; r) \text{ where } 0 \le v \le 10 \}$

$x \in L$.

L is an <u>NP language</u>. Why?

poly-size

Def of NP lang:

① $\forall x \in L, \exists w$ s.t. $R_L(x, w) = 1$

poly. time computable.

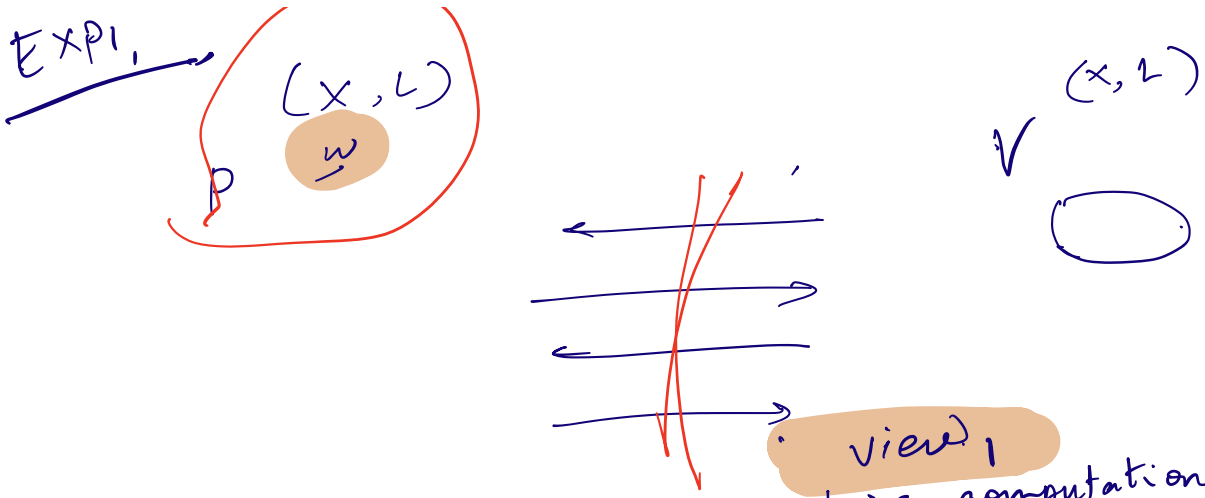
② $\forall x \notin L, \forall w, R_L(x, w) = 0$.

$R_L(x = c, w = (v, r))$:

if $c = com(v; r)$ and $0 \le v \le 10$, o/p 1

else o/p 0.

Exp1.

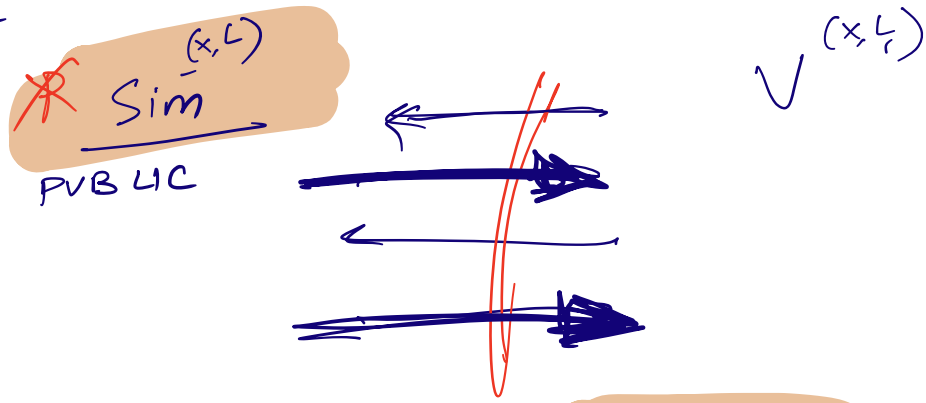


View1

contains computationally ~~about the witness~~

$\approx_c$

Exp2.



View2

contains no info. about w.