

Zero-Knowledge Protocols

Review: NP problems

Def. $L \in \text{NP}$ if $L \subseteq \{0,1\}^*$

and \exists poly-time M s.t.

$$x \in L \iff \exists w \in \{0,1\}^n : M(x,w) = 1$$

x : statement

w : witness

e.g. equality or Dlog

G : cyclic group of prime order q

$$L_{\text{EDL}} = \{ (g, h, g^d, h^d) \in G^4 : \begin{matrix} d \in \mathbb{Z}_q \\ h, g \neq 1 \end{matrix} \}$$

Given witness d , easy to check $(g, h, u, v) \in L_{\text{EDL}}$

Zero Knowledge Proof System for $L \in \text{NP}$

Def. Proof System: pair of prob. poly time (PPT) algs.

P, V

$$\begin{array}{ccc} P(x, w) & \longrightarrow & V(x) \\ & \longleftarrow & \\ & \longrightarrow & \text{yes or no} \end{array}$$

s.t.

1. Complete: $\forall x, w$: if $M(x, w) = 1$ (i.e. $x \in L$):
then $\Pr [(P(x, w) \leftrightarrow V(x)) = \text{yes}] = 1$

2. Sound: $\forall x \notin L, \forall \hat{P}$: $\Pr [(\hat{P} \leftarrow V(x)) = \text{yes}] \leq \text{negl.}$

*(all, incl. exp. time, provers
cheating prover cannot convince verifier $x \notin L$)*

Trivial case:

$$P \xrightarrow{w} V$$

V accepts if $m(x, w) = 1$

Honest verifier zero knowledge (HVZK):

Protocol should reveal nothing except that $x \in L$

For x, w , let $\text{transcript}(P(x, w) \leftrightarrow V(x))$

be seq. of msgs between $P(x, w)$ and $V(x)$
(random vars).

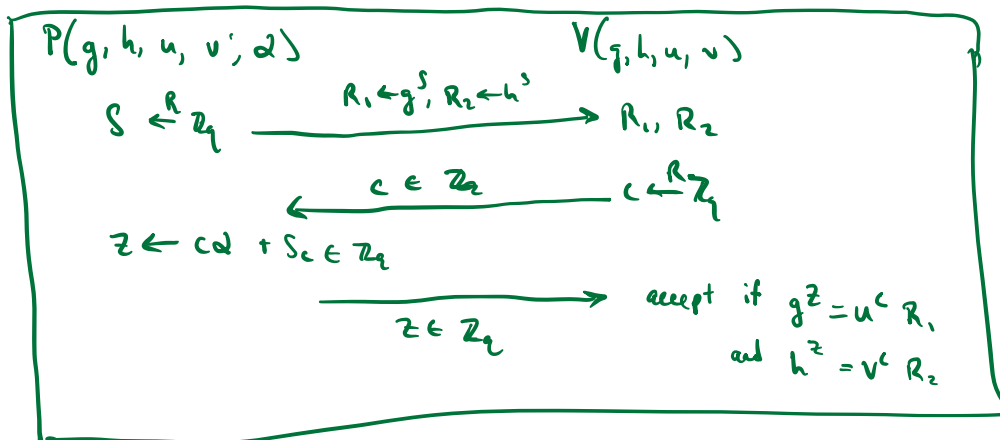
Def. (P, V) is HVZK for L if

\exists PPT alg S . (simulator) s.t. $\forall x \in L$:

Distr. $\{S(x)\}$ is computationally indistinguishable
from Distr. $\{\text{transcript}(P(x, w) \leftrightarrow V(x))\}$

\Rightarrow Sim. shows V learns nothing from transcript b/c
it can gen. transcript on its own.

Language example: HVZK proof system for L_{EDL}



note: verifier has no secret \Rightarrow public coin protocol

Proof completeness: $(g, h, u = g^d, v = h^d) \in \mathcal{L}_{EDL}$:

$$\begin{cases} g^z = g^{cd + s} = (g^d)^c g^s = u^c v, \\ \text{same for } h^z \end{cases}$$

$\Rightarrow V$ outputs yes. \checkmark

Soundness: Mal. prover \hat{P}

statement $u = g^d, v = h^d, d \neq \beta$

$\Rightarrow (g, h, u, v) \notin \mathcal{L}_{EDL}$ \leftarrow desired outcome

$$\text{transcript} = (R_1 = g^{s_1}, R_2 = h^{s_2}, c, z)$$

$$\Pr[V \text{ acc.}] = \Pr[z = \alpha c + s_1, z = \beta c + s_2]$$

$$= \Pr[\alpha c + s_1 = \beta c + s_2] = \Pr[c = \frac{s_1 - s_2}{\alpha - \beta}] = \frac{1}{q} \leq \text{negl.} \checkmark$$

HVZK: if $(g, h, u, v) \in \mathcal{L}_{EDL}$,

then Sim needs to output (R_1, R_2, c, z)

$\text{Sim}(g, h, u, v)$ does:

1. choose $c, z \leftarrow \mathbb{Z}_q$
2. Set $R_1 \leftarrow g^z / u^c, R_2 \leftarrow h^z / v^c$
3. output (R_1, R_2, c, z)

Then: $R_1 = g^s$ and $R_2 = h^s$ where $s = z - cd$

c uniform in \mathbb{Z}_q

$z \in \mathbb{Z}_q$ s.t. cond (1), (2) hold

Same as transcript! \checkmark