# Zero-Knowledge Protocols

## Review: NP problems

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

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 of DLog

$G$: cyclic group of prime order $q$

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

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

## Zero Knowledge Proof System for $L \in NP$

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

$P, V$

$$P(x, w) \quad \begin{matrix} \longrightarrow \\ \longleftarrow \\ \longrightarrow \end{matrix} \quad V(x) \hookrightarrow \text{yes or no}$$

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: $\forall x \notin L$, $\forall \hat{P}$: $\Pr[(\hat{P} \leftarrow V(x)) = \text{yes}] \leq$ negl.
   $\forall$all, incl exp. time, provers
   (cheating prover cannot convince verifier $x \in L$)

Trivial exs:

$P \xrightarrow{w} V$

$V$ 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 $L_{EDL}$

| $P(g, h, u, v; \alpha)$ | | $V(g, h, u, v)$ |
|---|---|---|
| $s \xleftarrow{R} \mathbb{Z}_q$ | $\xrightarrow{R_1 \leftarrow g^s,\ R_2 \leftarrow h^s}$ | $R_1, R_2$ |
| | $\xleftarrow{c \in \mathbb{Z}_q}$ | $c \xleftarrow{R} \mathbb{Z}_q$ |
| $z \leftarrow c\alpha + s \in \mathbb{Z}_q$ | | |
| | $\xrightarrow[z \in \mathbb{Z}_q]{}$ | accept if $g^z = u^c R_1$ and $h^z = v^c R_2$ |

note: verifier has no secrets $\rightarrow$ public coin protocol

Proof completeness: $(g, h, u = g^{\alpha}, v = h^{\alpha}) \in L_{EDL}$:

$$\begin{cases} g^{z} = g^{c\alpha + s} = (g^{\alpha})^{c} g^{s} = u^{c} R_1 \\ \text{same for } h^{z} \end{cases}$$

$\Rightarrow$ V outputs yes. $\checkmark$

Soundness: mal. prover $\hat{P}$

statement $u = g^{\alpha}$, $v = h^{\beta}$, $\alpha \neq \beta$

$\Rightarrow (g, h, u, v) \notin L_{EDL}$ ← desired outcome

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

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

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

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

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

Sim$(g, h, u, v)$ does:

1. choose $c, z \xleftarrow{R} \mathbb{Z}_q$
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 $s = z - c\alpha$

$c$ uniform in $\mathbb{Z}_q$

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

Same as transcript! $\checkmark$