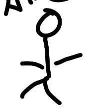
Zero Knowledge Proofs
Monday, September 27, 2021 4:40 PM

Zero Knowledge Proofs notation

Alice  x, $g^x = X$

private key — public key

Bulletin Board: X ← public key

"no one can compute x from X by DLOG"

ZKP is

Alice can say: "I know my secret key x s.t. $X = g^x$" ← "statement"

w/o revealing x

$$ZKP\{(x) : X = g^x\}$$

- witness
- statement
- relation/predicate

$X = g^x$

Alice^k sends $y = F_k(1)$

Can bob check y is actual $F_k(1)$ w/o knowing k?

Where's Waldo ZKP.

Language $L^{\in NP}$ is a set of strings

$$x \in L \iff \exists w. \text{ s.t. } L(x, w) = 1$$

statement — witness — predicate

* setup once per predicate, valid for many statements

Ideal Functionality

Prover Verifier

Alice $\xrightarrow{x, w}$ **Ideal Functionality**: Checks $L(x,w)$ if so, out x. $\xrightarrow{x}$ Bob

"learns $x \in L$, nothing else"

"protocol is secure iff it is as good as the IF"

(run the protocol) $\approx$ (interact with IF)

Interactive Protocol

Prover Alice — Verifier Bob

$P(x,w)$ $\xrightarrow{\text{"commit"}}$ $V(x)$

$\xleftarrow{\text{"challenge"}}$

$\xrightarrow{\text{"response"}}$

prover starts w/ wit & stmt

verifier starts w/ just statement

output Accept/Reject

- $\mathrm{out}_V[P(x,w) \leftrightarrow V(x)]$

means final output of V

- $\mathrm{View}_V[P(x,w) \longleftrightarrow V(x)]$

means a transcript of all
- messages received by V
- random choices made by V.

- Correctness: "verifier accepts if prover is honest"

$$\forall x, w.\ L(x,w)=1,\ \Pr\left[\mathrm{out}_V[P(x,w) \leftrightarrow V(x)] = 1\right] = 1$$

Soundness: "verifier only accepts $x \in L$"

$$\forall A, x \quad \Pr\left[\begin{array}{l} out_V[A(x) \leftrightarrow V(x)] = 1 \\ \text{and} \\ x \notin L \end{array}\right] \leq negl$$

Extraction (stronger than soundness)

"verifier only accepts if $x \in L$
and Prover "knows" witness w"

Zero Knowledge: "verifier knows no more information after the protocol than before"

"view of the verifier can be simulated even without interacting with the Prover"

$\forall x, w, L(x,w), \exists S$ ← simulator

$$View_V[P(x,w) \leftrightarrow V(x)] \approx S(x)$$

⇓ real transcript interacting w/ prover.

⇓ simulated transcript

Protocol for $ZK\{(x) : X = g^x\}$ $|G| = p$

$P(\cancel{X}, x)$: "commit" $V(\cancel{X})$

$k \xleftarrow{\$} \mathbb{Z}_p$

$K = g^k$ $\xrightarrow{\quad K \quad}$ $c \xleftarrow{\$} \mathbb{Z}_p$

"challenge"

$\xleftarrow{\quad c \quad}$

$s = xc + k$ "response"

$\xrightarrow{\quad s \quad}$ $g^s \stackrel{?}{=} X^c K$

- Correctness: $g^s = g^{xc+k} = (g^x)^c g^k = X^c K$

- Zero-knowledge:

$\text{View}_V [P(x,w) \leftrightarrow V(x)]$

$|G| \quad |\mathbb{Z}_p| \quad |\mathbb{Z}_p|$

(K, c, s) where $g^s = X^c K$

exactly equal distributions.

$$\Pr\left[\text{transcript} = (K, c, s)\right] = \begin{cases} 1/p^2 & \text{if } g^s = X^c K \\ 0 & \text{otherwise} \end{cases}$$

$S(X)$:

✗ $K \xleftarrow{\$} G,\ c \leftarrow \mathbb{Z}_p,\ s = \log_g K + c \log_g X$?

✓ $c \xleftarrow{\$} \mathbb{Z}_p,\ s \xleftarrow{\$} \mathbb{Z}_p,\ K = g^s / X^c$

- Extraction for next time.