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 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

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

statement — witness — predicate

A setup once per predicate, valid for many statements

Ideal Functionality

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

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

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

$\begin{pmatrix}\text{run the} \\ \text{protocol}\end{pmatrix} \approx \left(\text{interact with } I_F\right)$

Interactive Protocol

Prover Alice		Verifier Bob
$P(X,w)$	"commit" $\longrightarrow$	$V(X)$
	$\longleftarrow$ "challenge"	
	"response" $\longrightarrow$	

prover starts w/ wit & stmt

verifier starts w/ just statement

output Accept/Reject

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

means final output of V

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

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

- Correctness: "verifier accepts if prover is honest"

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

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

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

- 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

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

$\Downarrow$ real transcript interacting w/ Prover.

$\Downarrow$ Simulated transcript

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

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

"Commit"

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

$K = g^k$ $\qquad \xrightarrow{K}$

Σ sigma protocols

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

"challenge"

$\xleftarrow{c}$

$s = xc + k$

"response"

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

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

- Zero-knowledge:

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

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

$\Downarrow$

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

exactly equal distributions.

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

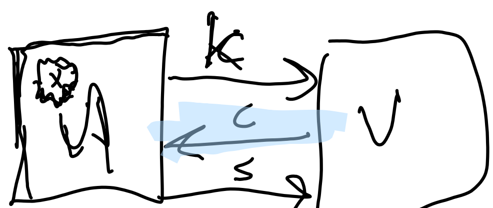
$S(X)$: ✗ $K \xleftarrow{\$} G$, $c \in \mathbb{Z}_p$, $s = \log_g K + c \log_g X$?

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

- Extraction for next time.

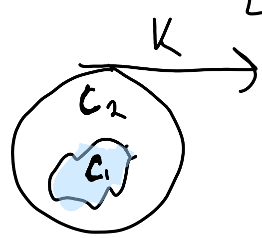
"If A (possibly randomized prover) produces a valid proof for X, with high prob then we can use A (run A multiple times) to output a witness"

- extractability



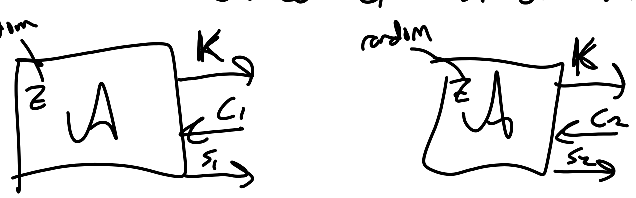
V says OK

Possible values of c



$A(1^\lambda, X; z)$ rand bits. $c \in C_1 \Rightarrow A$ outputs valid s

Success set C_1 must be nonnegligible.



$[A \leftrightarrow P]$

"run A twice, with two different challenges."

We construct an extractor $\mathcal{E}_A(1^\lambda, X)$:

$z \xleftarrow{\$} \{0,1\}^{q(\lambda)}$ ← however many bits A needs

run A until it outputs first message K

$A(1^\lambda, X; z) \to K$.

(I) $c_1 \xleftarrow{\$} \mathbb{Z}_p$

Send c_1 to A, run until receiving s_1.

run $\mathcal{A}(1^n, X; Z)$ a second time and outputs K.

(II) $\underline{c_2} \xleftarrow{\$} \mathbb{Z}_p$

Send c_2 to $\mathcal{A}$, receive s_2.

IF $out_V[\mathcal{A} \leftrightarrow V] = 1$ with prob $\underline{d}_2$

then $g^{s_1} = X^{c_1} K$ w/ prob at least $\underline{d^2}$

and $g^{s_2} = X^{c_2} K$

$g^{s_1} / g^{s_2} = X^{c_1} K / X^{c_2} K$

$g^{s_1 - s_2} = \cancel{X}^{c_1 - c_2}$ ← size $|G| = p$

division mod p.

$\left(g^{s_1 - s_2}\right)^{c_1 - c_2}$ $\left(X^{c_1 - c_2}\right)^{\left(1/\underline{c_1 - c_2}\right)}$

Solve for $x = (s_1 - s_2)/(c_1 - c_2)$. ← division mod p

Commitments.

Exercise: Come up with a protocol for

$$ZK\{(x, r) : C = g^x h^r\}$$