**Zero Knowledge Proofs notation**

- Alice: \( x, g^x = X \)  
  \[ \text{public key} \]  
  \[ \text{private key} \]

- Bob: \( X \)  
  \[ \text{public key} \]  
  \[ \text{private key} \]

**ZKP is**

- Alice can say:  
  \[ \text{"I know my secret key } x \text{ s.t. } X = g^x \" } \]

- **Statement**: \( X \)  
  \[ \text{public key} \]  
  \[ \text{private key} \]

**ZKP \( \exists (\exists ) : X = g^x \)**

- witness
- statement
- relation/predicate: \( X = g^x \)

**Where's the ZKP?**

- Language \( L \in NP \) is a set of strings
  \[ x \in L \iff \exists w \text{ s.t. } L(x, w) = 1 \]
  
**Ideal Functional**

- A sequence of predicates
- valid for
- statements
- witness
- predicate

- monix statements
Interactive Protocol

Verifier

Bob

"commits"

Verifier

Bob

V(X)

Verifier starts with

Just statement

output Accept/Reject

- Output [P(X,w) ⇆ V(X)]
  | means output of V

- View V[P(X,w) ⇆ V(X)]
  means a transcript of all
  messages received by V
  - random choices made by V.

- Correctness: "Verifier accepts if prover is honest"

\[ \forall X, w. L(X,w) = 1, \Pr \left[ \text{Output} \left[ P(X,w) \leftrightarrow V(X) \right] \right] = y \]
Soundness: "verifier only accepts $x \in L$"

$$\forall A, x \in \Pr \left[ \text{out}_v[A(x) \leftrightarrow V(x)] = 1 \quad \text{and} \quad x \notin L \right] \leq \text{negl}$$

**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"

$$\forall x, v, L(x), \exists S \epsilon \text{-similar}$$

$$\text{View}_v[P(x,v) \leftrightarrow V(x)] \approx \leq (x)$$

real transcript interacting
with prover.

Simulated transcript

---

Protocol for $ZK(\frac{1}{3})$:

$X = g^x, |G| = p$

$P(X, x)$:

"assert" $V(x)$
\[ k \in \mathbb{Z}_p \quad K = g^k \]

**Challenge**

\[ c \in \mathbb{Z}_p \]

\[ s = xc + k \]

**Response**

\[ g^s = x^c \]

**Correctness:** \[ g^s = g^{xc + k} = (g^x)^c g^k = x^c K \]

**Zero-knowledge:**

\[
\mathsf{View}_V \left[ p(x, w) \leftrightarrow V(x) \right]
\]

\[ \mathsf{Transcript} = (K, c, s) \text{ when } g^s = x^c K \]

\[ \mathsf{Equal Distribution:} \quad P \left[ \mathsf{Transcript} = (K, c, s) \right] = \begin{cases} \frac{1}{|\mathbb{Z}_p|} & \text{if } g^s = x^c K \\ 0 & \text{otherwise} \end{cases} \]

**S(X):**

\[ K \in G_1, c \in \mathbb{Z}_p, \quad s = \log_g K + c \log_g X \]

\[ c \in \mathbb{Z}_p, s \in \mathbb{Z}_p, K = g^s / x^c \]

**Extraction for next time.**