CSCI 1510

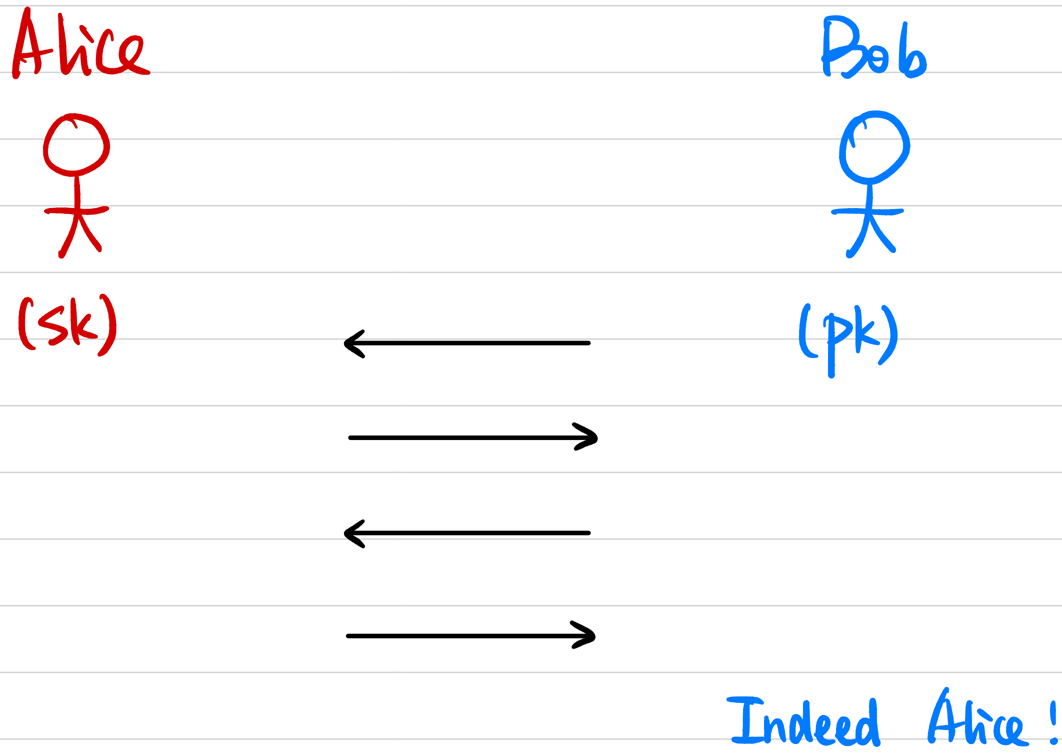
This Lecture:

- Schnorr's Identification / Signature Schemes (Continued)
- Definition of Zero-Knowledge Proofs
- Perfect ZKP for Diffie-Hellman Tuples

Signatures from DLOG

$$\begin{tikzcd}[column sep=huge] \text{1 Identification Scheme} \arrow[r, Rightarrow, "\text{2 Fiat-Shamir}", "\text{Transform}"'] & \text{Digital Signature} \\ \text{Discrete Log} \arrow[u, Rightarrow, "\text{3 Schnorr}"'] & \end{tikzcd}$$

Identification Scheme



Special 3-Round Identification Scheme

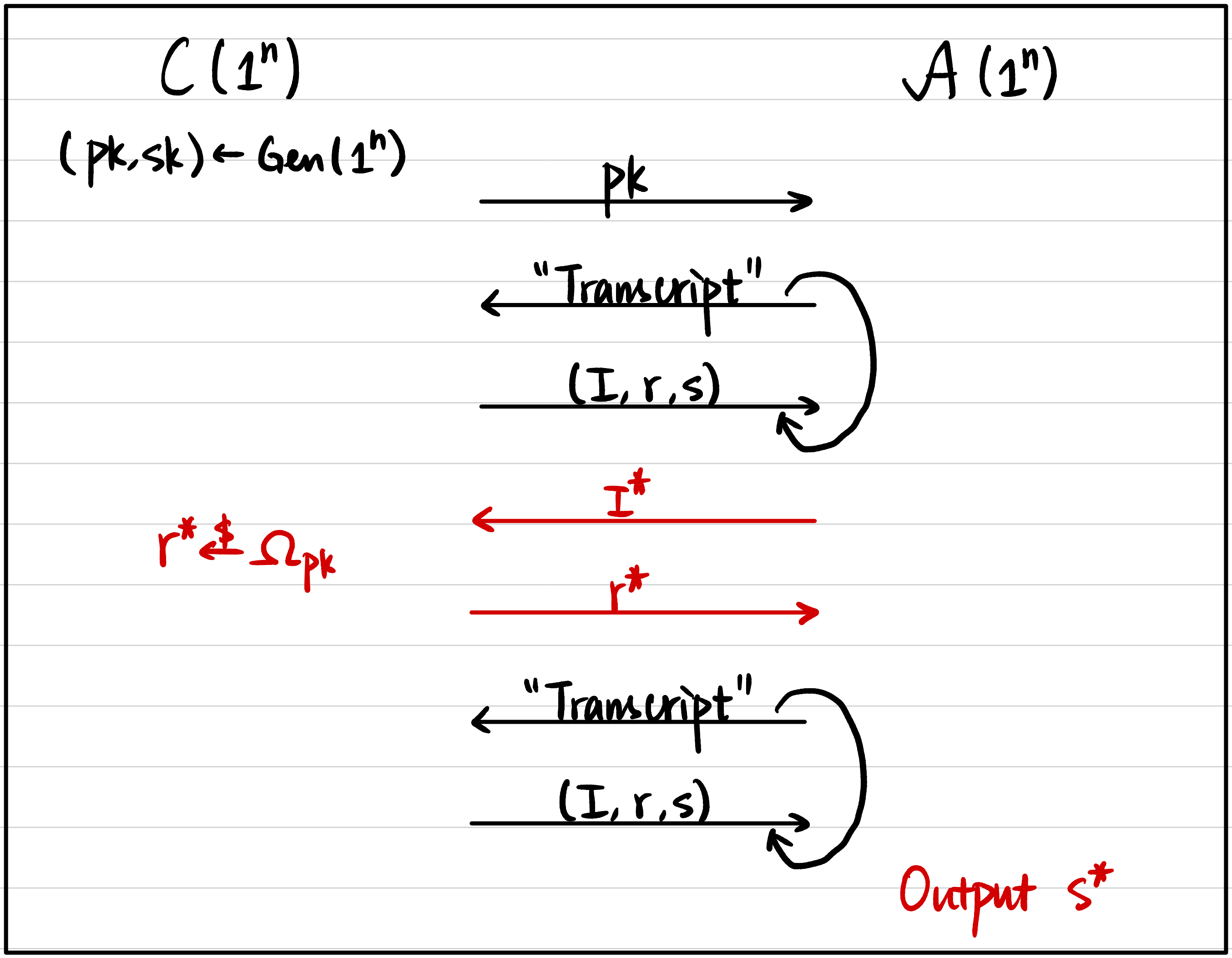
$$(pk, sk) \leftarrow Gen(1^n)$$

Prover (sk)		Verifier (pk)
$(I, st) \leftarrow P_1(sk)$	$\xrightarrow{\quad I \quad}$	
		$r \xleftarrow{\$} \Omega_{pk}$
	$\xleftarrow{\quad r \quad}$	
$s := P_2(sk, st, r)$	$\xrightarrow{\quad s \quad}$	
		$V(pk, r, s) \stackrel{?}{=} I$

Correctness: If both parties follow the protocol description, then the verifier accepts with probability 1.

Special 3-Round Identification Scheme

Def A 3-round identification scheme $\Pi = (Gen, P_1, P_2, V)$ is secure if $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[V(pk, r^*, s^*) = I^*] \le \varepsilon(n)$.



Schnorr's Identification Scheme

$$(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$$

$$x \xleftarrow{\$} \mathbb{Z}_q$$

$$h := g^x$$

Prover (x)		Verifier $(\mathbb{G}, q, g, h)$
$y \xleftarrow{\$} \mathbb{Z}_q$		
$I := g^y$	$\xrightarrow{\quad I \quad}$	
		$r \xleftarrow{\$} \mathbb{Z}_q$
	$\xleftarrow{\quad r \quad}$	
$s := (x \cdot r + y) \bmod q$	$\xrightarrow{\quad s \quad}$	
		$g^s / h^r \stackrel{?}{=} I$

$h^r = (g^x)^r = g^{xr}$

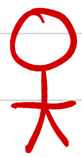
$g^s = g^{xr+y}$

$g^s / h^r = g^y = I$

Thm If DLOG is hard relative to $\mathcal{G}$, then this is a secure identification scheme.

Zero-Knowledge Proof (ZKP)

Alice



Bob

[There is a bug in your code]

[I have the secret key for this ciphertext]

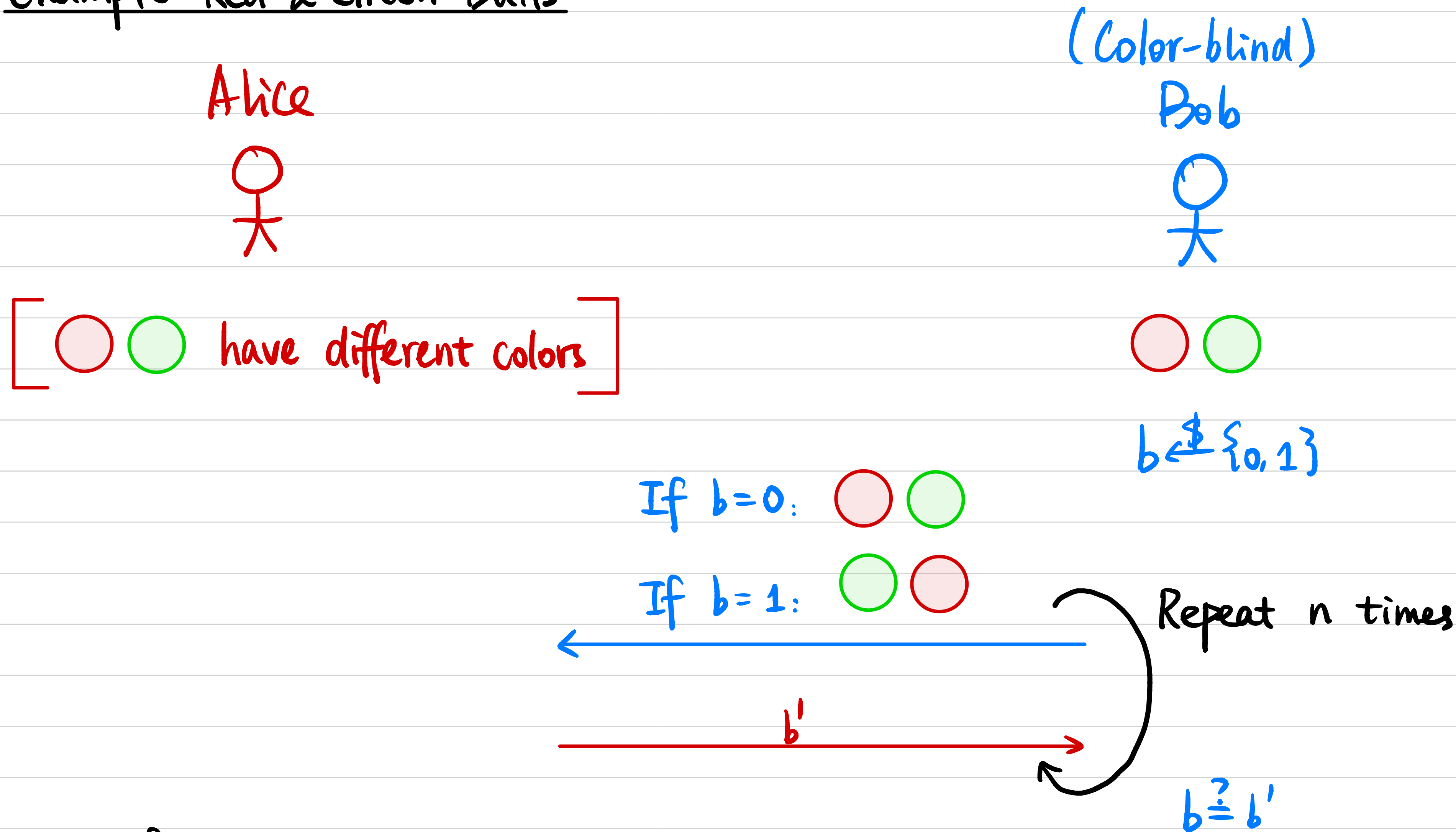
[There is enough balance in my Bitcoin account]

[ have different colors]

What is a proof?

What does zero-knowledge mean?

Example: Red & Green Balls



If statement is true: $\Pr[b=b'] = 1$

If statement is false: $\Pr[b=b'] = (1/2)^n$

What is a "proof system"?

Statement:

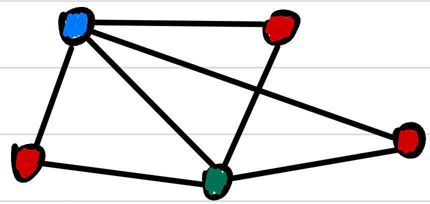
proof:

$\square$

- **Completeness:** If statement is true, then $\exists$ proof that proves it's true.
- **Soundness:** If statement is false, then $\forall$ proof can't prove it's true.

NP as a Proof System

Example: Gragh 3-Coloring



NP language $L = \{ G : G \text{ has 3-Coloring} \}$

NP relation $R_L = \{ (\underset{\uparrow \atop \text{graph}}{G}, \underset{\uparrow \atop \text{3-coloring}}{3COL}) \}$

Statement: graph G

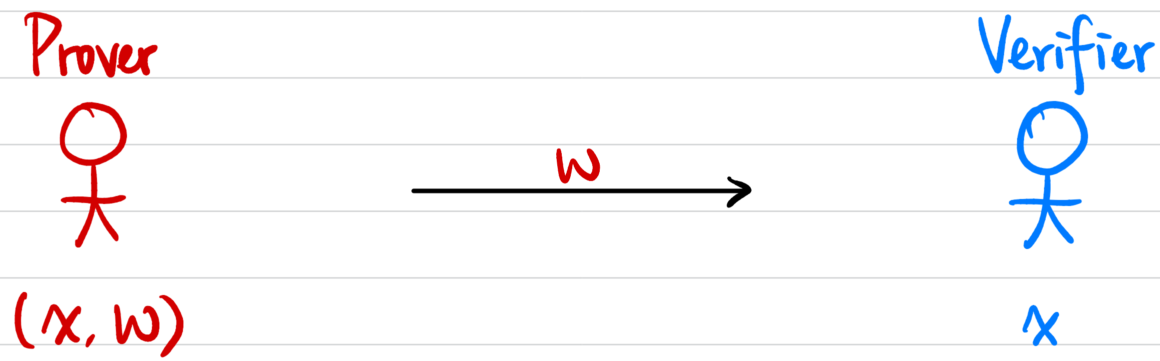
Proof: 3-coloring of G: 3COL

$(G, 3COL) \in R_L$

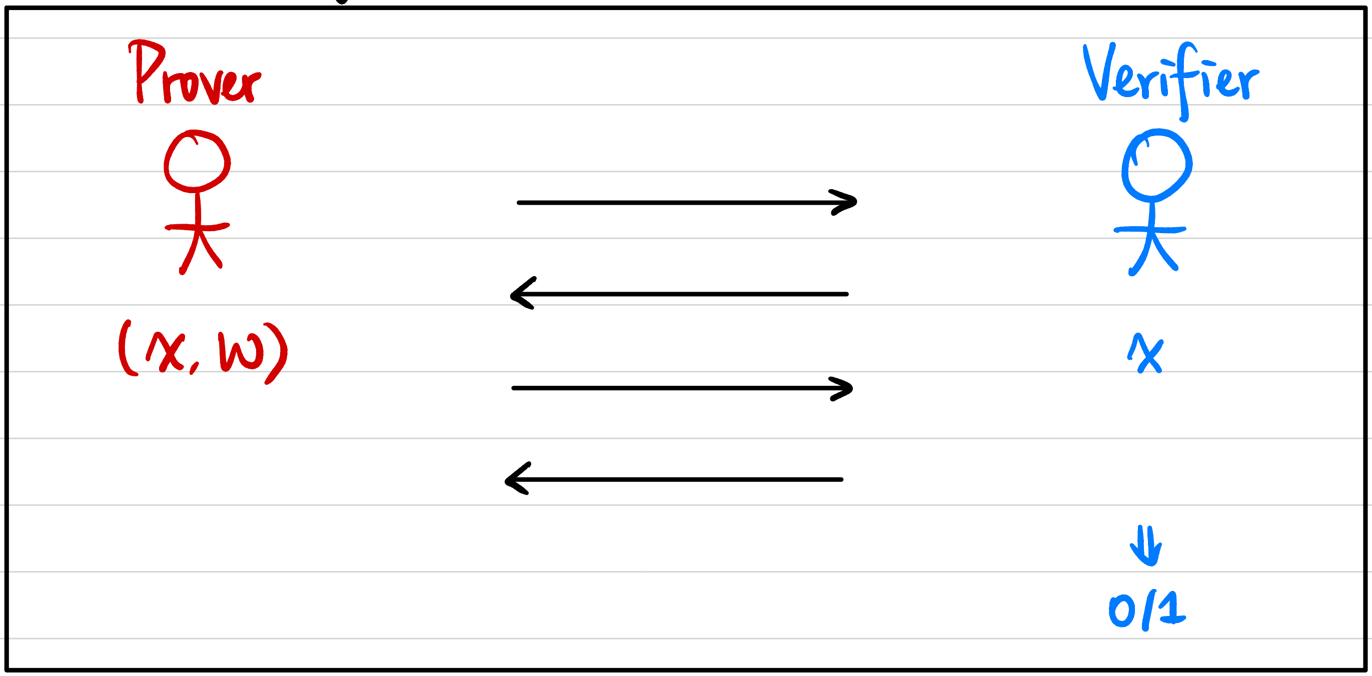
NP as a Proof System

A language L is in NP if $\exists$ poly-time V s.t.

- **Completeness:** $\forall x \in L$, $\exists w$ s.t. $V(x, w) = 1$
  witness
- **Soundness:** $\forall x \notin L$, $\forall w^*$, $V(x, w^*) = 0$



Zero-Knowledge Proof (ZKP)

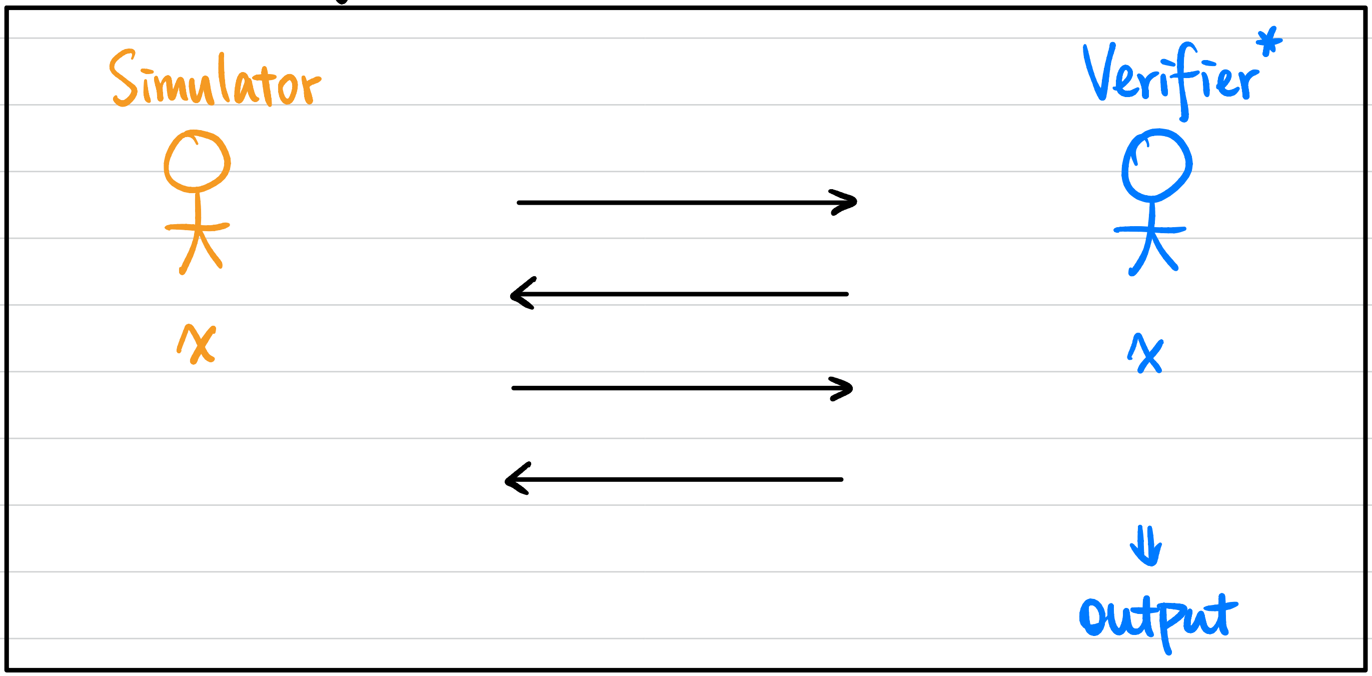


Let (P, V) be a pair of PPT interactive machines. (P, V) is a zero-knowledge proof system for a language L with associated relation R_L if

- **Completeness:** $\forall (x, w) \in R_L$, $\Pr[P(x,w) \longleftrightarrow V(x) \text{ outputs } 1] = 1$.
- **Soundness:** $\forall x \notin L$, $\forall$ (PPT) P^*, $\Pr[P^*(x) \longleftrightarrow V(x) \text{ outputs } 1] \le \mathrm{negl}(n)$.

  ↑ argument
- **Zero-Knowledge?**

Zero-Knowledge Proof (ZKP)



• **Zero-Knowledge:** $\forall$ PPT V^*, $\exists$ PPT S s.t. $\forall (x, w) \in R_L$,

$$\text{Output}_{V^*}[P(x,w) \longleftrightarrow V^*(x)] \simeq S(x)$$

perfect / statistical / computational

$\equiv$ $\quad \overset{s}{\simeq}$ $\quad \overset{c}{\simeq}$

Perfect ZKP for Diffie-Hellman Tuples

Input: Cyclic group G of order q, generator g, $\underset{g^a}{\underset{\parallel}{h}}$, $\underset{g^b}{\underset{\parallel}{u}}$, $\underset{g^{ab}}{\underset{\parallel}{v}}$

Witness: b

Statement: $\exists b \in \mathbb{Z}_q$ s.t. $u = g^b \wedge v = h^b$

Prover		Verifier
$r \xleftarrow{\$} \mathbb{Z}_q$		
	$\xrightarrow{A := g^r,\ B := h^r}$	
		$\sigma \xleftarrow{\$} \{0,1\}$
	$\xleftarrow{\sigma}$	
	$\xrightarrow{s := \sigma \cdot b + r \bmod q}$	
		?

Completeness ?

If $\sigma = 0 \Rightarrow s = r \quad \Rightarrow$

If $\sigma = 1 \Rightarrow s = b + r \quad \Rightarrow$

Soundness? $(g, h, u, v) \notin L$

$h = g^a, \quad u = g^b, \quad v = g^c$

$\forall x \notin L, \ \forall P^*, \quad \Pr[P^*(x) \longleftrightarrow V(x) \text{ outputs } 1] \leq \text{negl}(n)$

Prover*		Verifier
$r \xleftarrow{\$} \mathbb{Z}_q$		
	$\xrightarrow{A := g^r, \ B := h^r}$	
		$\sigma \xleftarrow{\$} \{0,1\}$
	$\xleftarrow{\ \sigma\ }$	
	$\xrightarrow{S := \sigma \cdot b + r \bmod q}$	

Zero-Knowledge?

$\forall$ PPT V^*, $\exists$ PPT S s.t. $\forall (x, w) \in R_L$,

$$\text{Output}_{V^*}[P(x,w) \longleftrightarrow V^*(x)] \equiv S(x)$$

Simulator		Verifier*
$r \xleftarrow{\$} \mathbb{Z}_q$		
	$\xrightarrow{A := g^r,\ B := h^r}$	
		$\sigma \xleftarrow{\$} \{0,1\}$
	$\xleftarrow{\sigma}$	
	$\xrightarrow{s := \sigma \cdot b + r \bmod q}$	