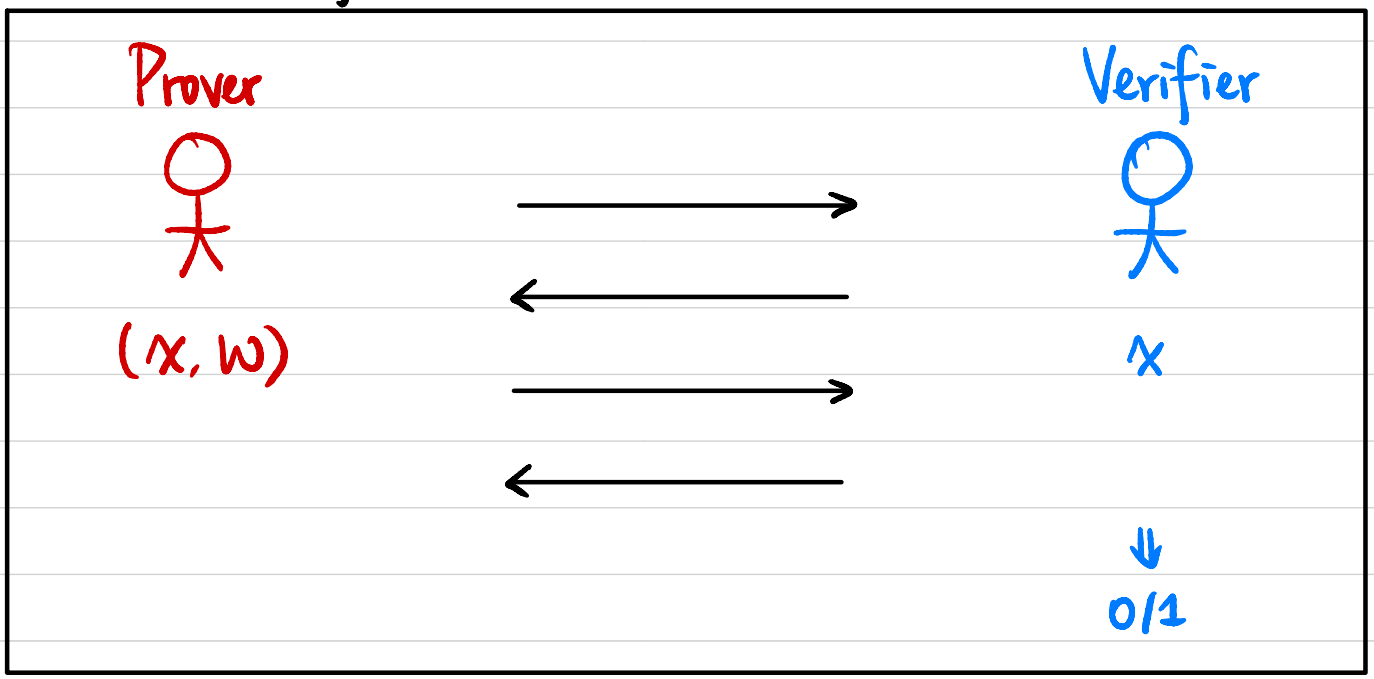
CSCI 1510

- Perfect ZKP for Diffie-Hellman Tuples (continued)
- Commitment Schemes
- ZKP for All NP
- Non-Interactive Zero-Knowledge Proofs

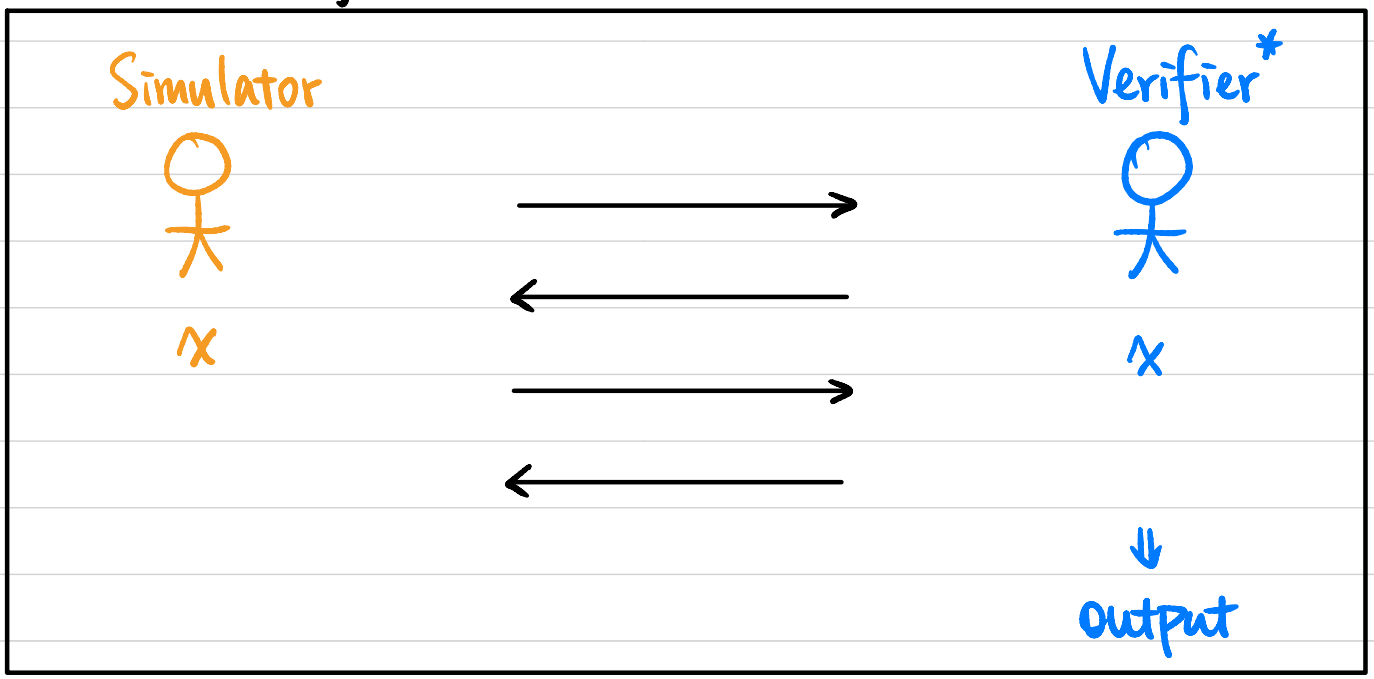
Zero-Knowledge Proof (ZKP)



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:** $\forall (x, w) \in R_L, \quad \Pr[\, P(x,w) \longleftrightarrow V(x) \text{ outputs } 1 \,] = 1.$
- **Soundness:** $\forall x \notin L, \quad \forall \underset{\text{argument}}{(\text{PPT})} P^*, \quad \Pr[\, P^*(x) \longleftrightarrow V(x) \text{ outputs } 1 \,] \leq \text{negl}(n).$
- **Zero-Knowledge?**

Zero-Knowledge Proof (ZKP)



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

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

↑

perfect / statistical / computational

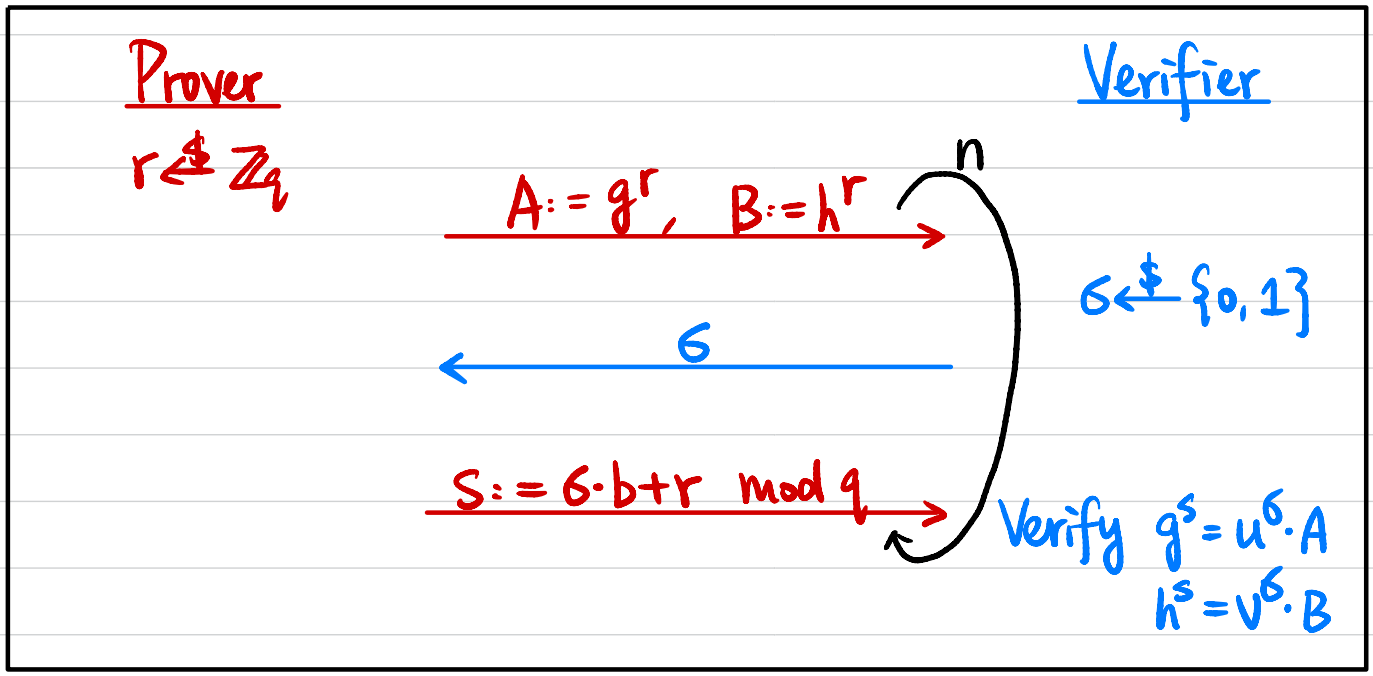
$\equiv$ $\quad$ $\overset{s}{\approx}$ $\quad$ $\overset{c}{\approx}$

Perfect ZKP for Diffie-Hellman Tuples

Input: Cyclic group G of order q, generator g, h, u, v
($h = g^a$, $u = g^b$, $v = g^{ab}$)

Witness: b

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



Completeness ?

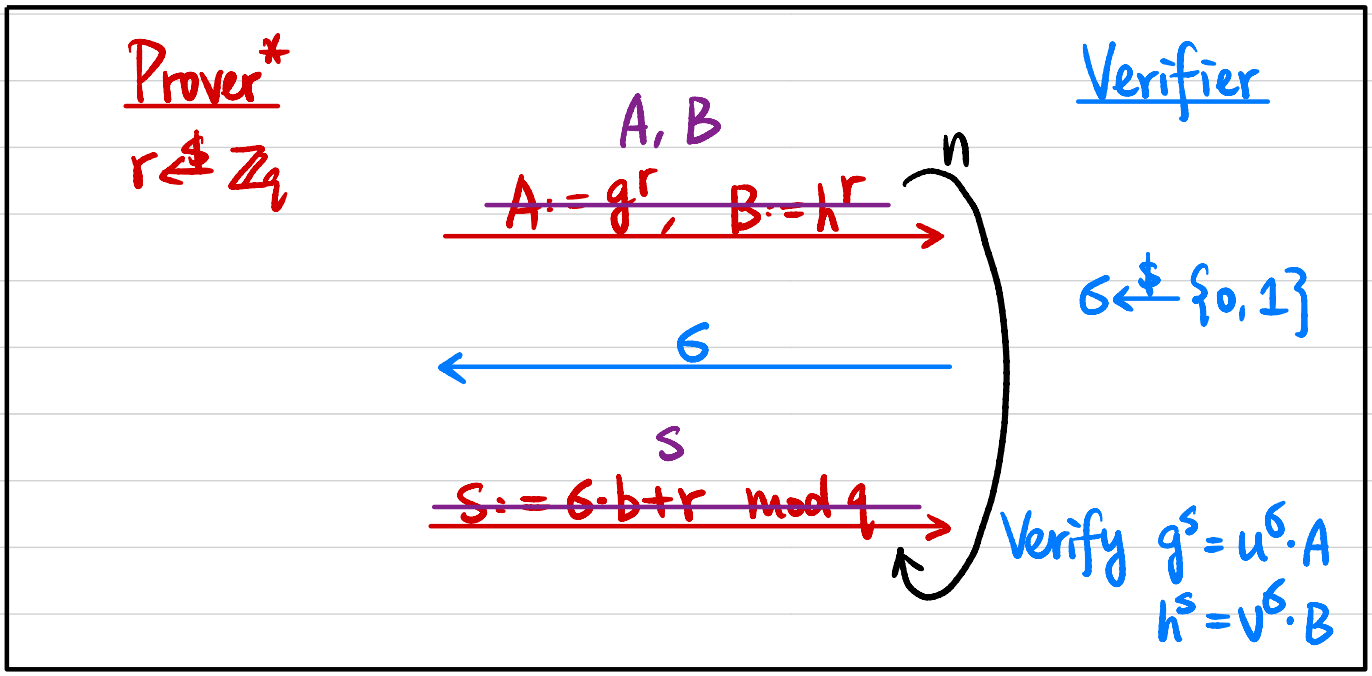
$$g^s = g^{c \cdot b + r} = (g^b)^c \cdot g^r = u^c \cdot A$$

$$h^s = h^{c \cdot b + r} = (h^b)^c \cdot h^r = v^c \cdot B$$

Soundness? $(g, h, u, v) \notin L$ $v = h^{b'}$ $b' \neq b$

g^a g^b g^c

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



$g^s = u^\sigma \cdot A \Leftrightarrow g^s = (g^b)^\sigma \cdot A \Leftrightarrow (g^s)^a = (g^b)^{\sigma \cdot a} \cdot A^a \Leftrightarrow h^s = h^{b \cdot \sigma} \cdot A^a$

$h^s = v^\sigma \cdot B \Leftrightarrow h^s = (h^{b'})^\sigma \cdot B$

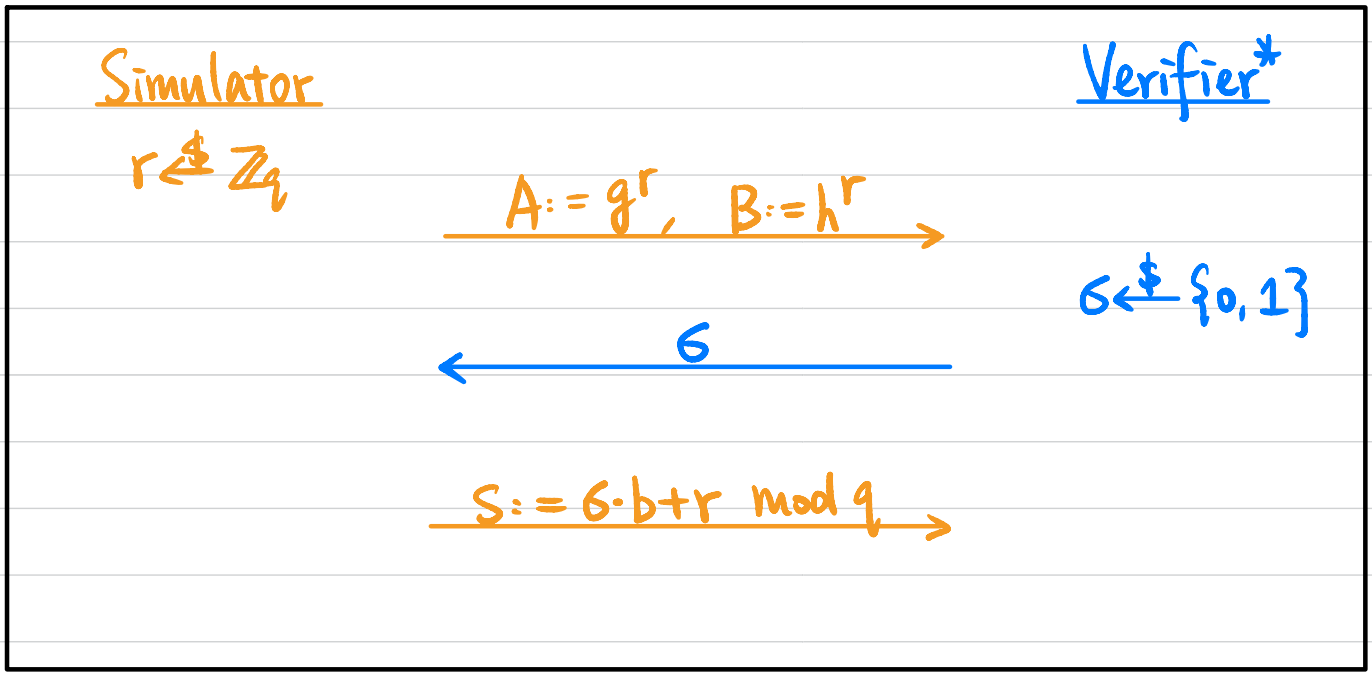
$\Pr[g^s = u^\sigma \cdot A \wedge h^s = v^\sigma \cdot B] = \Pr[h^{b \cdot \sigma} \cdot A^a = h^{b' \cdot \sigma} \cdot B] = \Pr[h^{(b'-b) \cdot \sigma} = B/A^a]$

$\leq \frac{1}{2}$

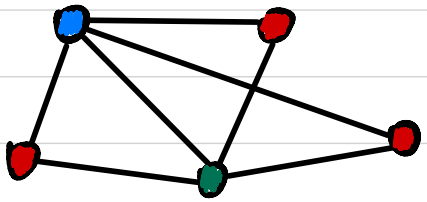
Zero-Knowledge?

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

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

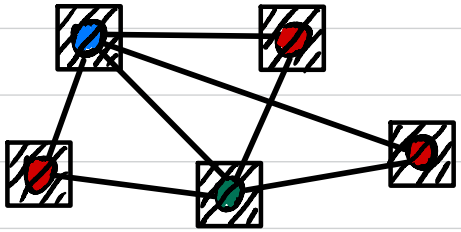


ZKP for Graph 3-Coloring (All NP)

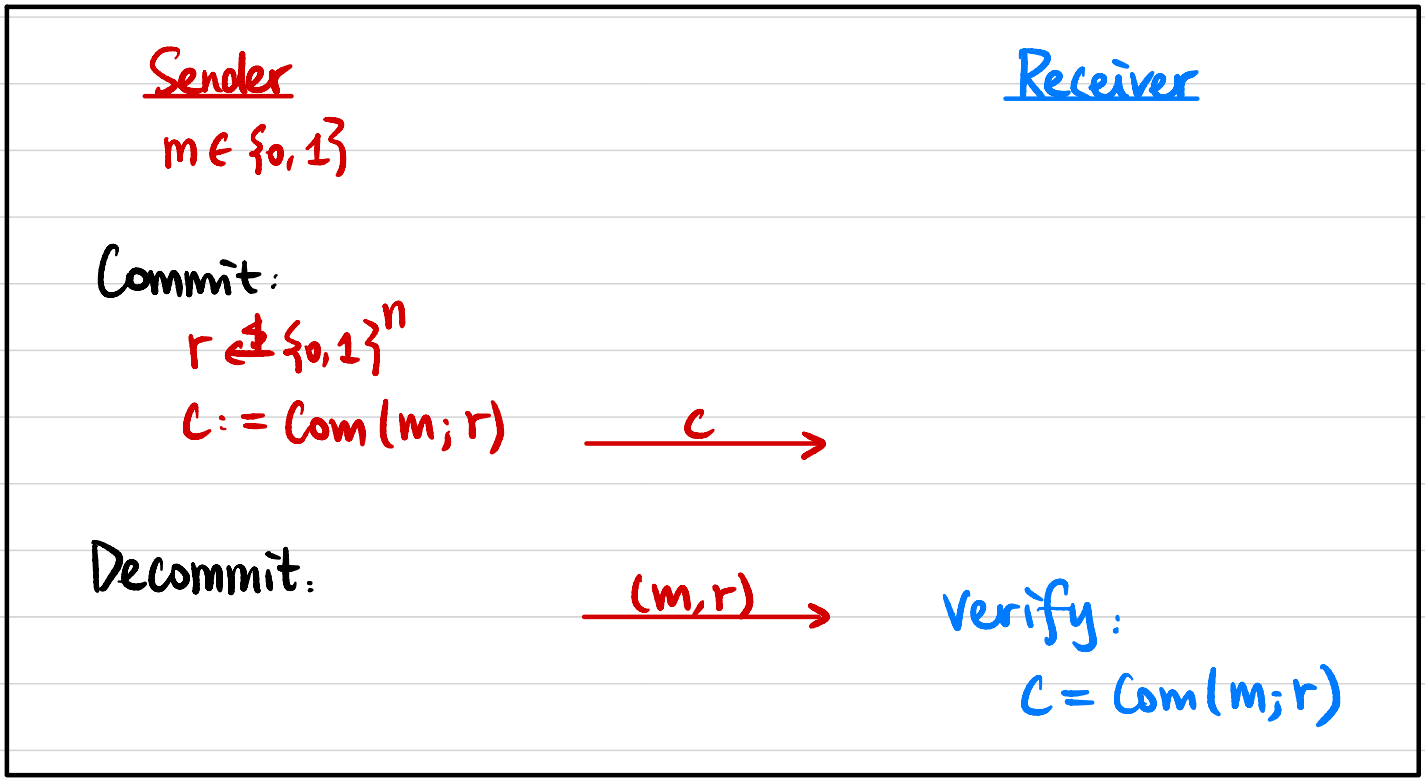


NP language $L = \{ G : G \text{ has 3-coloring} \}$

NP relation $R_L = \{ (G, 3COL) \}$



Commitment Scheme



Commitment Scheme

Def A non-interactive perfectly binding commitment scheme is a PPT algorithm Com statisfying:

- **Perfectly Binding:** $\forall r, s \in \{0,1\}^n$, $\mathrm{Com}(0; r) \neq \mathrm{Com}(1; s)$
- **Computationally Hiding:** $\mathrm{Com}(0; U_n) \overset{c}{\approx} \mathrm{Com}(1; U_n)$

A decommitment of a commitment value c is (b, r) s.t. $c = \mathrm{Com}(b; r)$.

Can a commitment scheme be both perfectly binding & perfectly hiding ?

Perfectly Binding Commitment Scheme

Assume one-way permutations exist.

Let $f: \{0,1\}^n \to \{0,1\}^n$ be a OWP and $hc: \{0,1\}^n \to \{0,1\}$ be a hard-core predicate of f.

$$Com(b; r) := (f(r), hc(r) \oplus b)$$

- Perfectly Binding?

- Computationally Hiding?

ZKP for Graph 3-Coloring

Input: $G = (V, E)$

Witness: $\phi: V \to \{0,1,2\}$

Given a perfectly binding commitment scheme Com.

Prover		Verifier
Randomly sample $\pi: \{0,1,2\} \to \{0,1,2\}$ $\forall v \in V$, $r_v \xleftarrow{\$} \{0,1\}^n$, $c_v := \mathsf{Com}(\pi(\phi(v)); r_v)$		
	$\xrightarrow{\{c_v\}_{v \in V}}$	
		Randomly pick an edge $(u,v) \in E$
	$\xleftarrow{(u,v)}$	
Reveal decommitments of c_u & c_v		
	$\xrightarrow[\beta = \pi(\phi(v)),\ r_v]{\alpha = \pi(\phi(u)),\ r_u}$	Verify: $c_u = \mathsf{Com}(\alpha; r_u)$ $c_v = \mathsf{Com}(\beta; r_v)$ $\alpha, \beta \in \{0,1,2\}$, $\alpha \neq \beta$

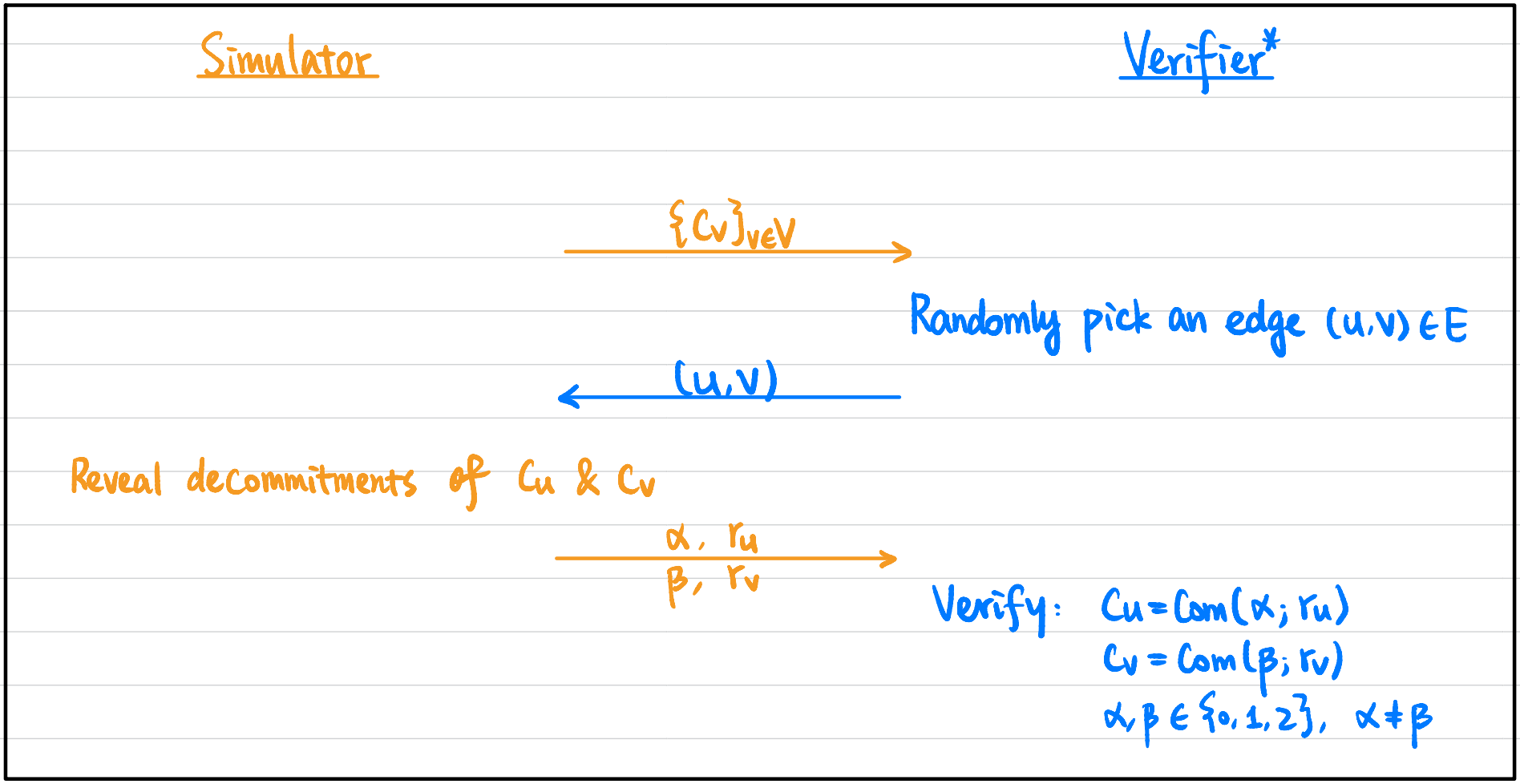
Completeness ?

Soundness ?

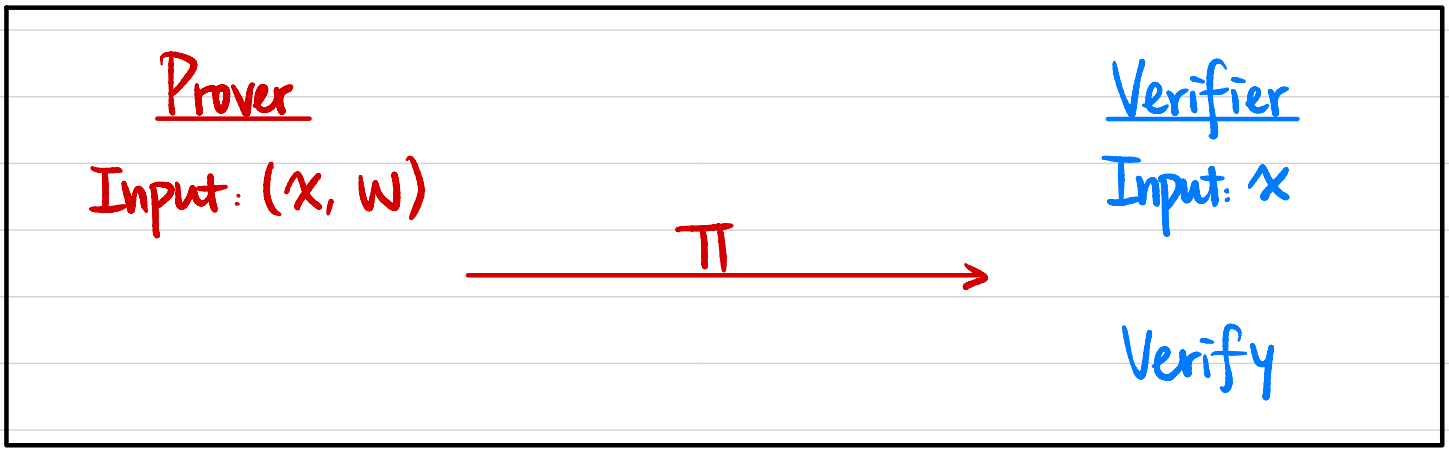
Zero-Knowledge?

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

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



Non-Interactive Zero-Knowledge (NIZK) Proof

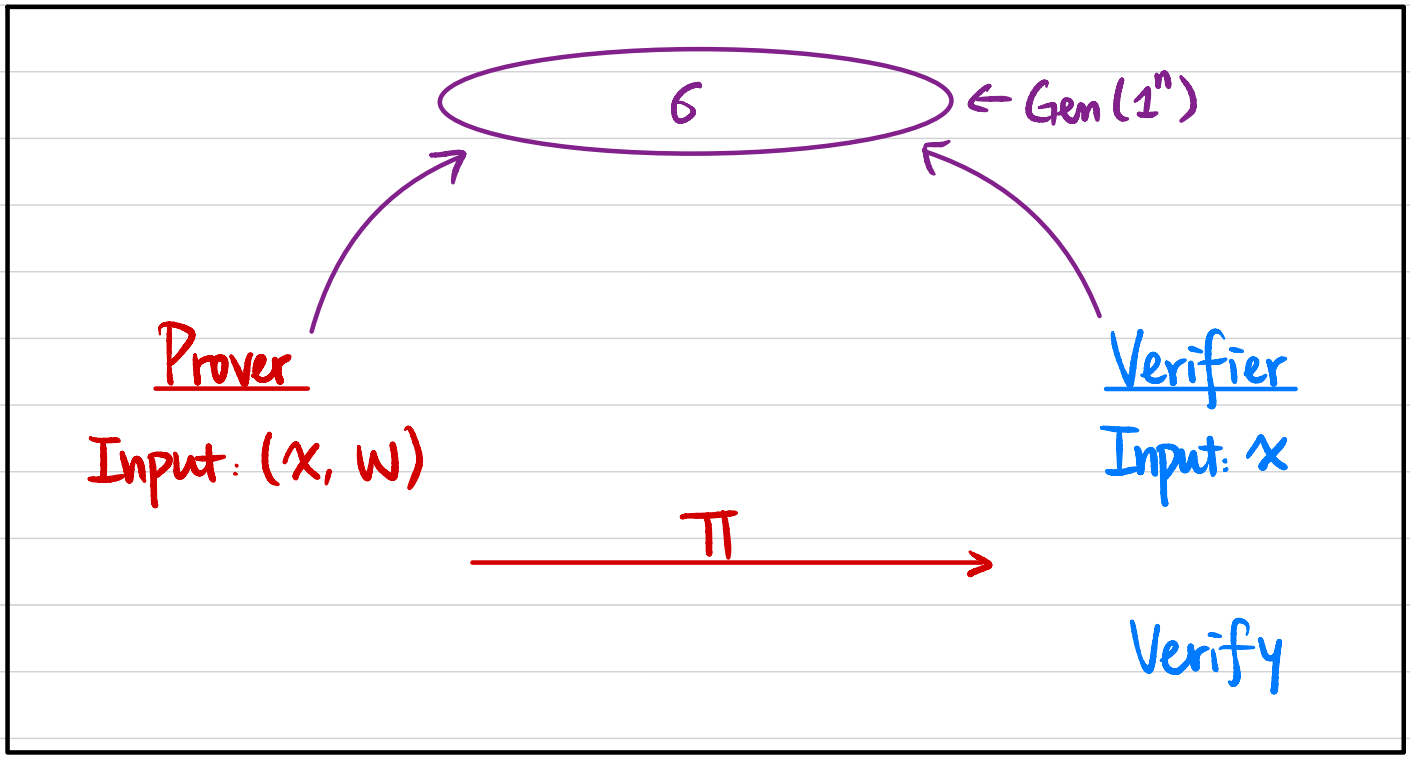


- **Completeness:** $\forall (x,w) \in R_L, \quad Pr[\, P(x,w) \longrightarrow V(x) \text{ outputs } 1\,] = 1.$
- **Soundness:** $\forall x \notin L, \ \forall P^*, \quad Pr[\, P^*(x) \longrightarrow V(x) \text{ outputs } 1\,] \leq negl(n)$
- **Zero-Knowledge:** $\forall PPT\ V^*, \ \exists PPT\ S \quad s.t. \quad \forall (x,w) \in R_L,$

$$Output_{V^*}[P(x,w) \longrightarrow V^*(x)] \simeq S(x)$$

Is it possible ?

Model 1: Common Random String / Common Reference String (CRS)



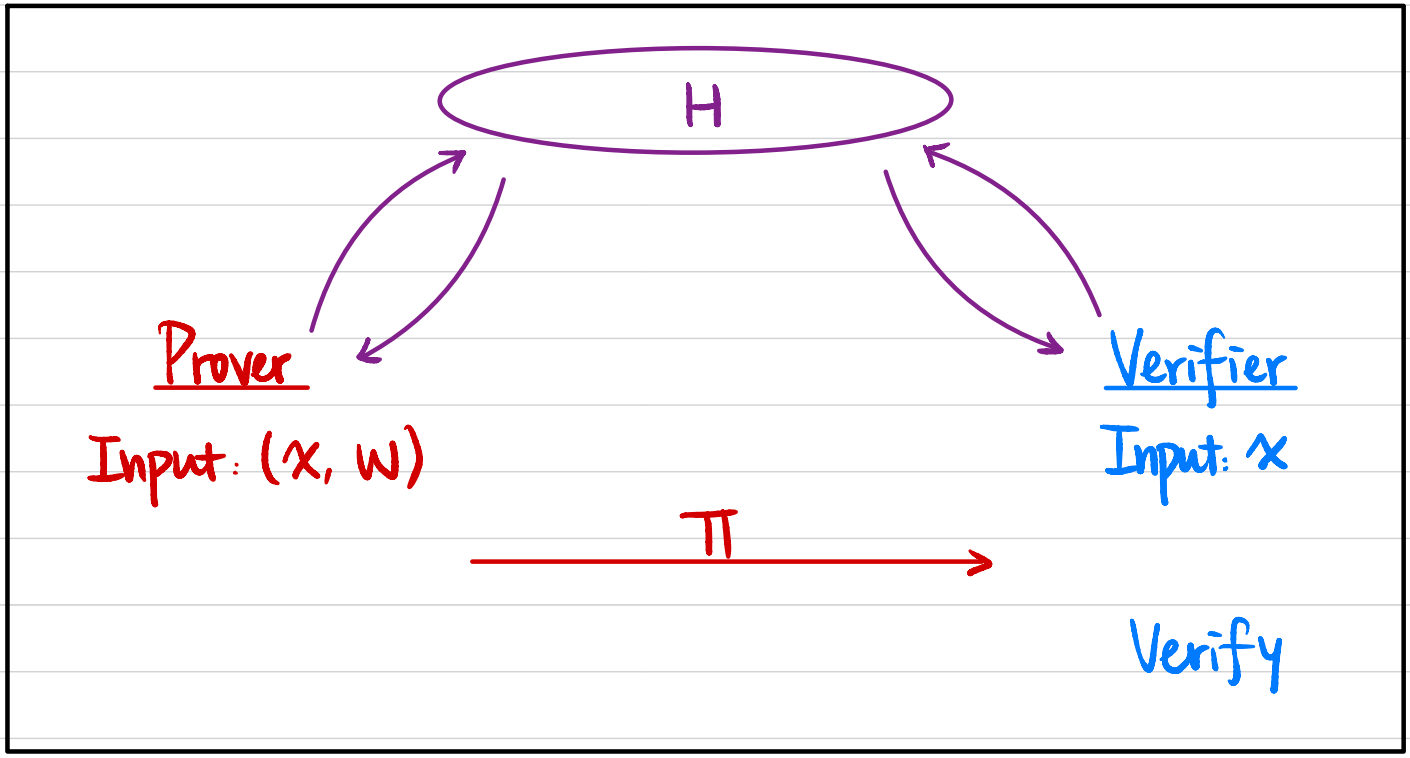
S(x) generates both (σ, π)

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

$$\text{Output}_{V^*}\left[\sigma \leftarrow \text{Gen}(1^n),\ P(x, w, \sigma) \longrightarrow V^*(x, \sigma)\right] \simeq S(x)$$

Alternatively: $\left(\sigma \leftarrow \text{Gen}(1^n),\ P(x, w, \sigma)\right) \simeq S(x)$

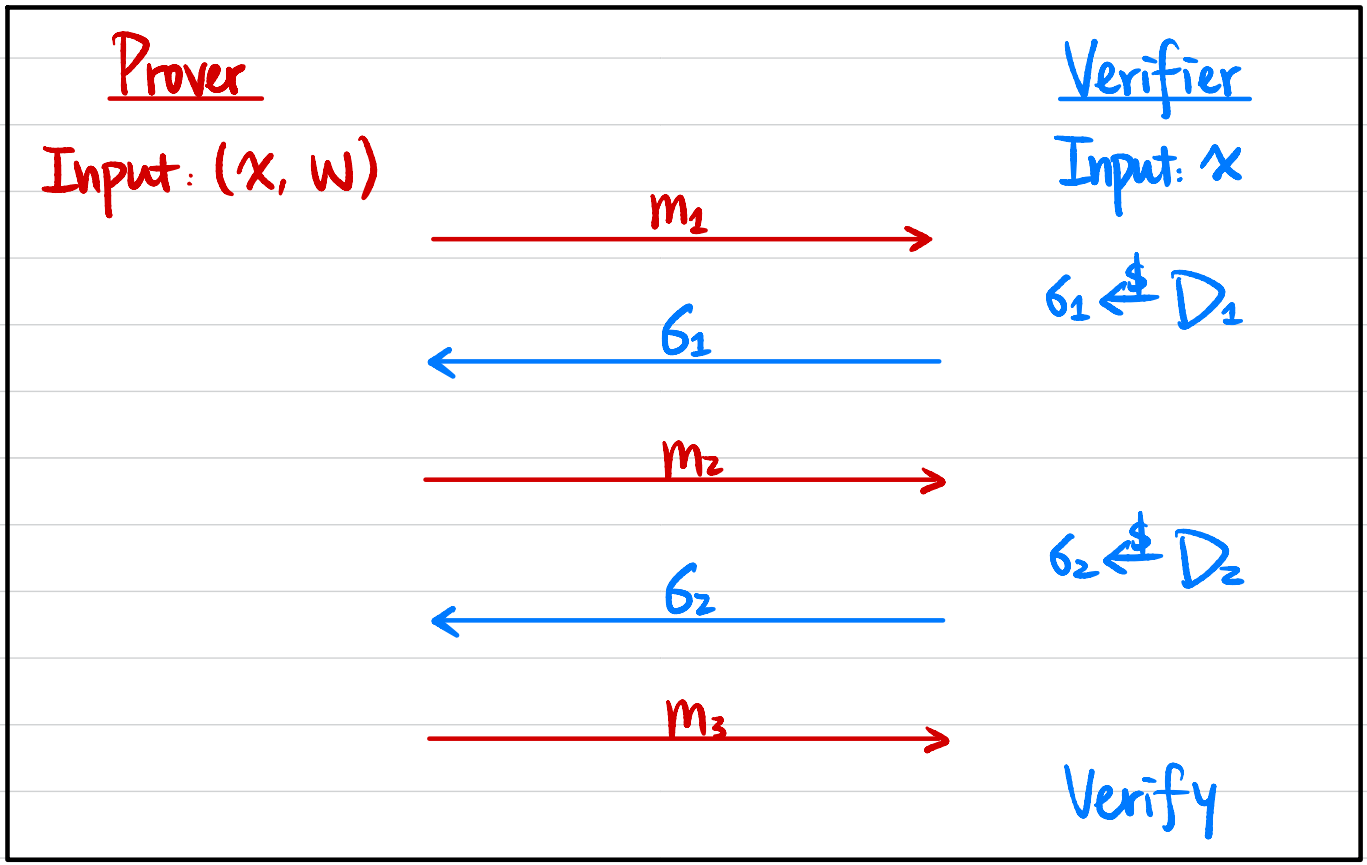
Model 2: Random Oracle Model



S controls input/output behavior of RO

Fiat-Shamir Heuristic

Public-Coin Honest-Verifier ZK (HVZK) $\Rightarrow$ NIZK in the RO model



$\sigma_1 := H(x \| m_1)$

$\sigma_2 := H(x \| m_1 \| m_2)$