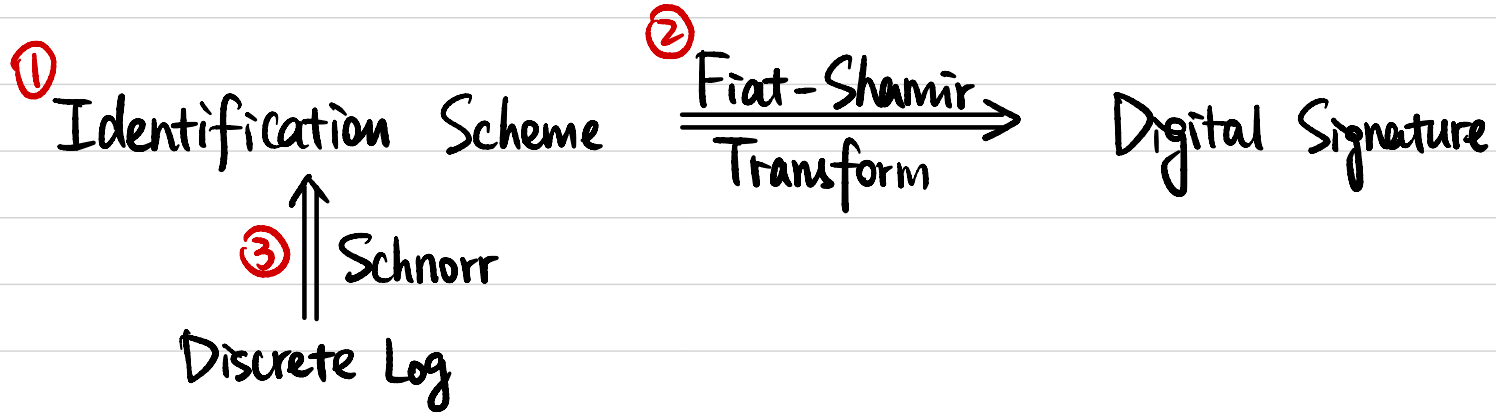
CSCI 1510

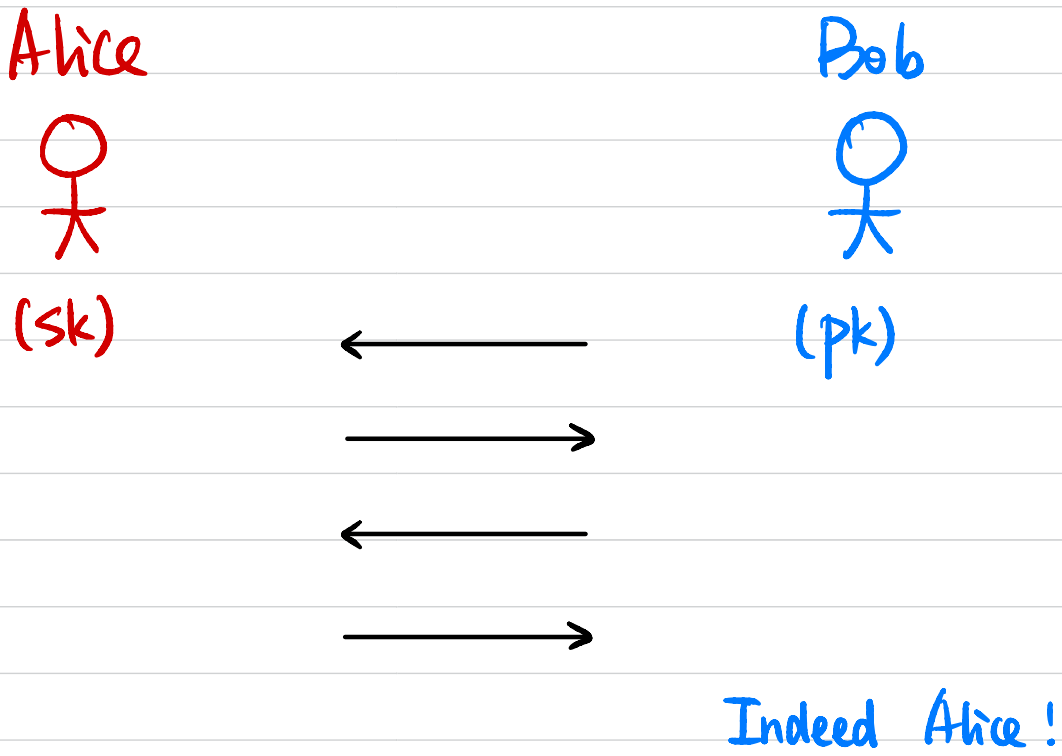
This Lecture:

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

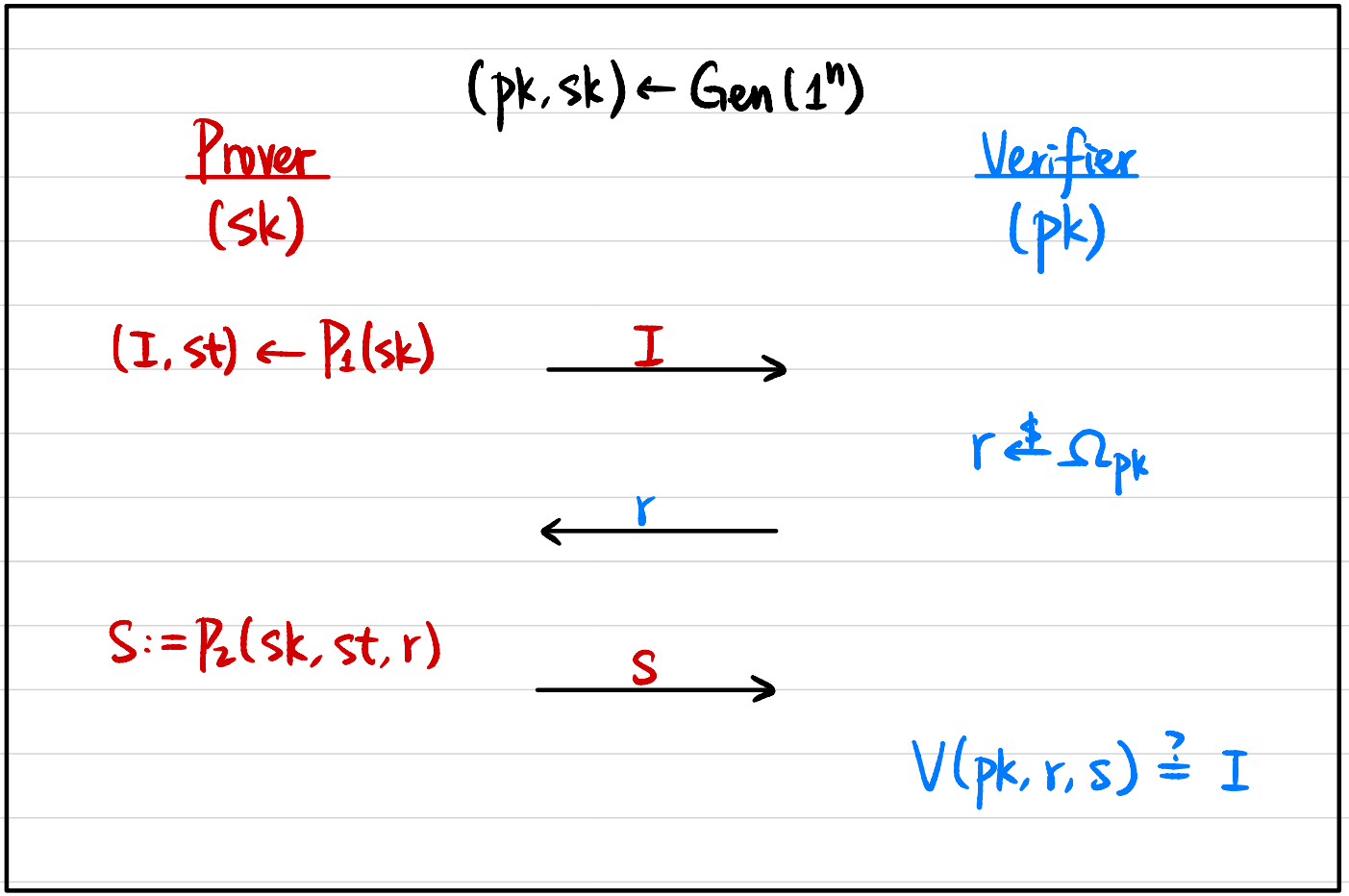
Signatures from DLOG



Identification Scheme



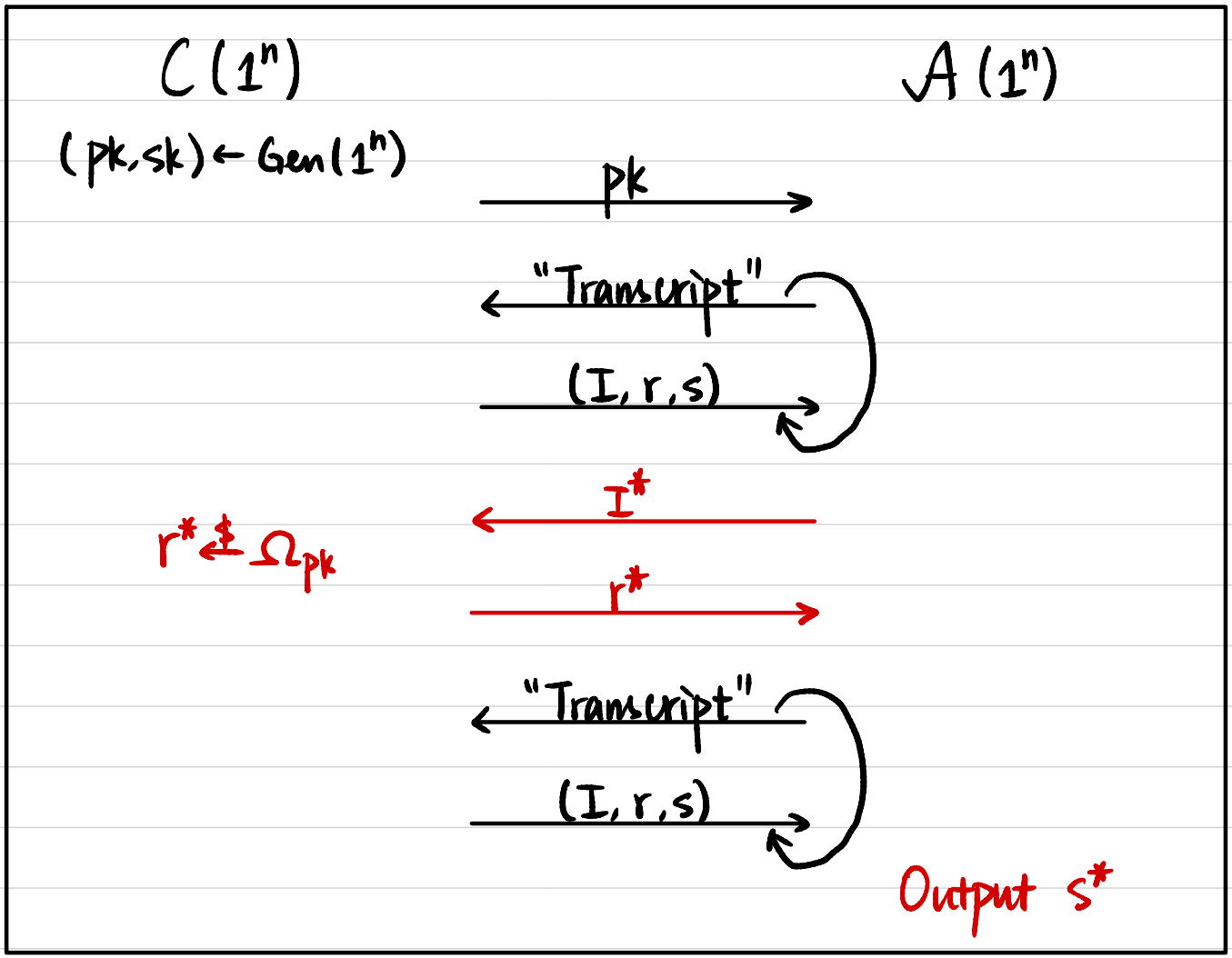
Special 3-Round Identification Scheme



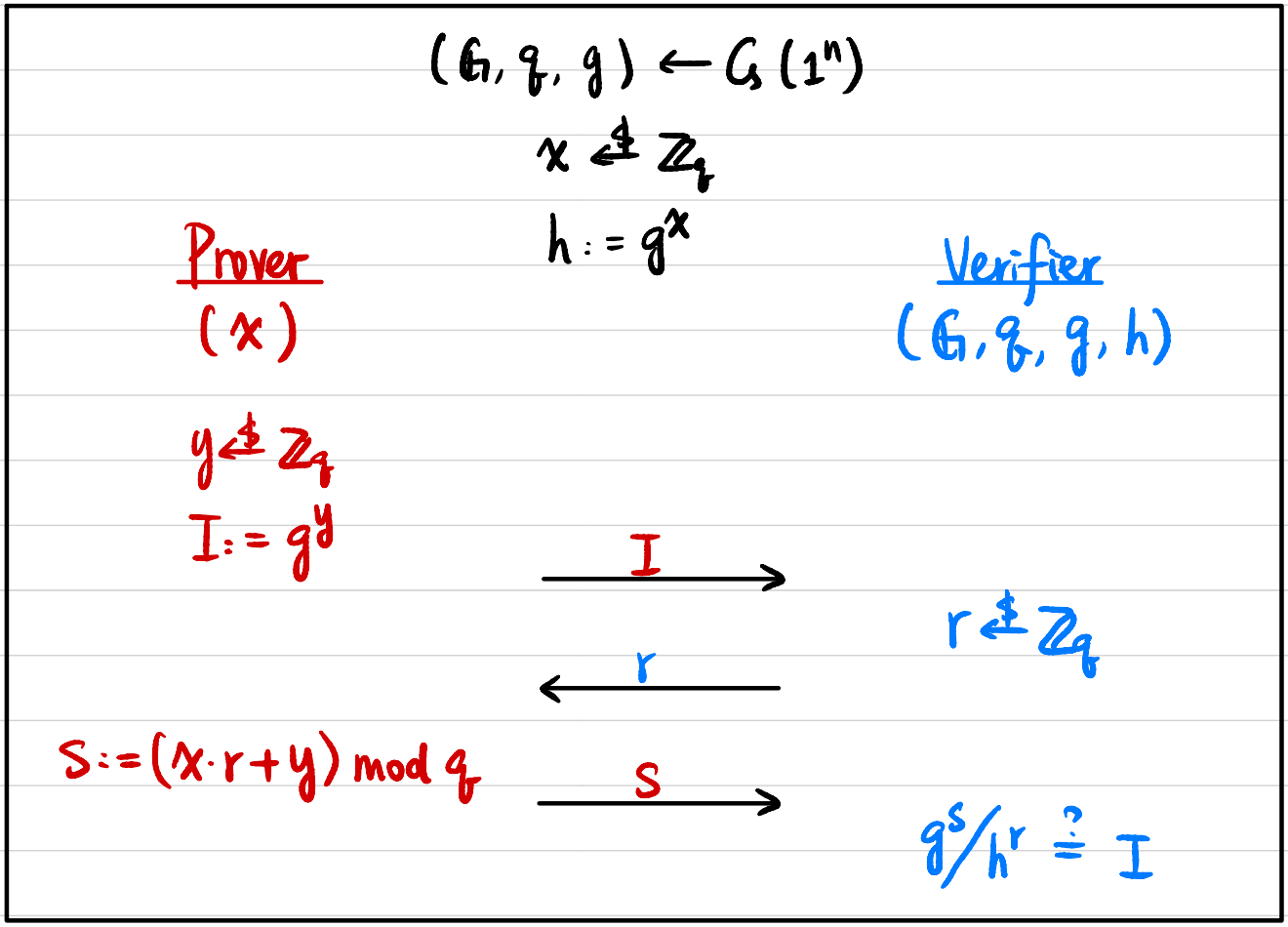
Correctness: If both parties follow the protocol description, then the verifier accepts with probability 1.

Special 3-Round Identification Scheme

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

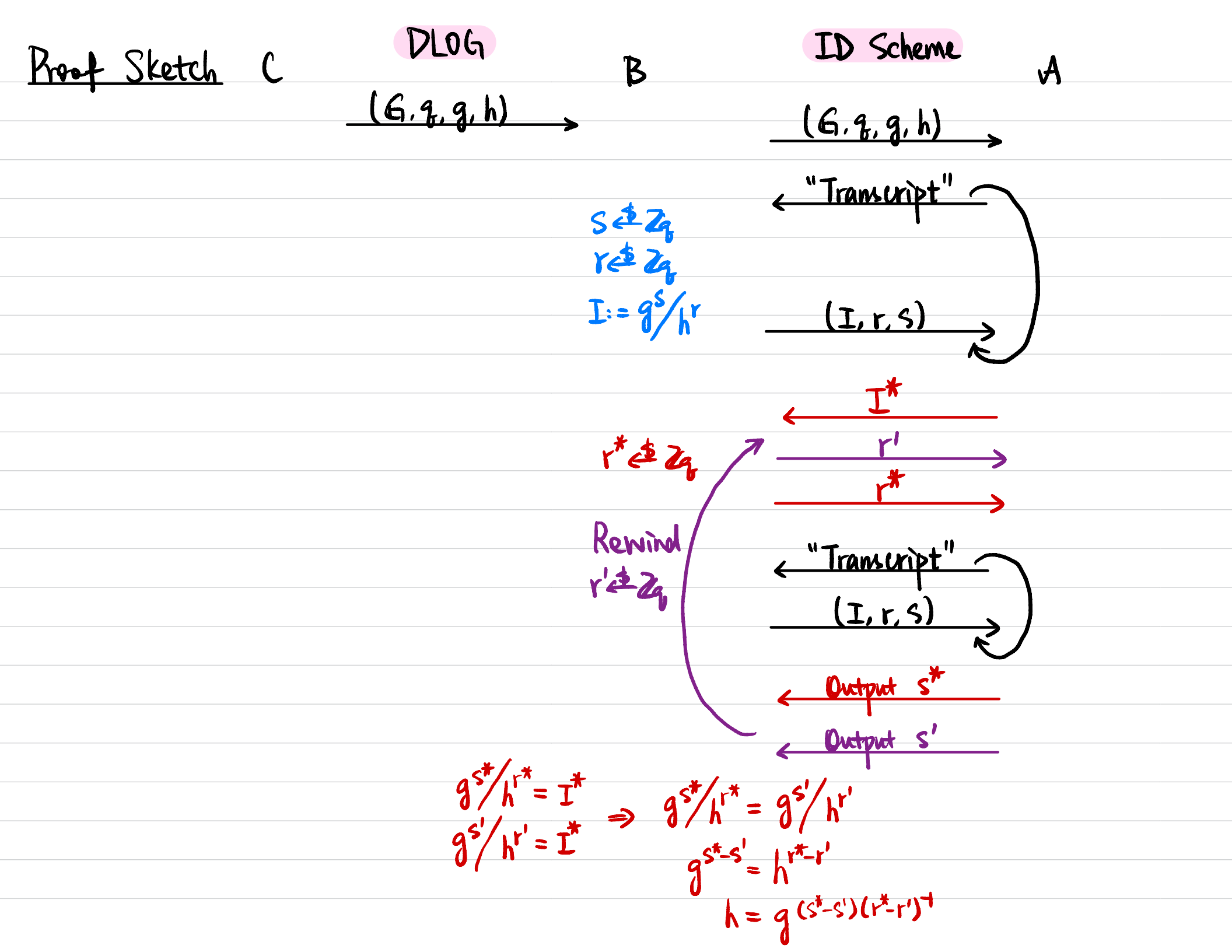


Schnorr's Identification Scheme



Thm If DLOG is hard relative to G, then this is a secure identification scheme.

Proof Sketch



Zero-Knowledge Proof (zkp)

Alice

Bob

[There is a bug in your code]

[I have the secret key for this ciphertext]

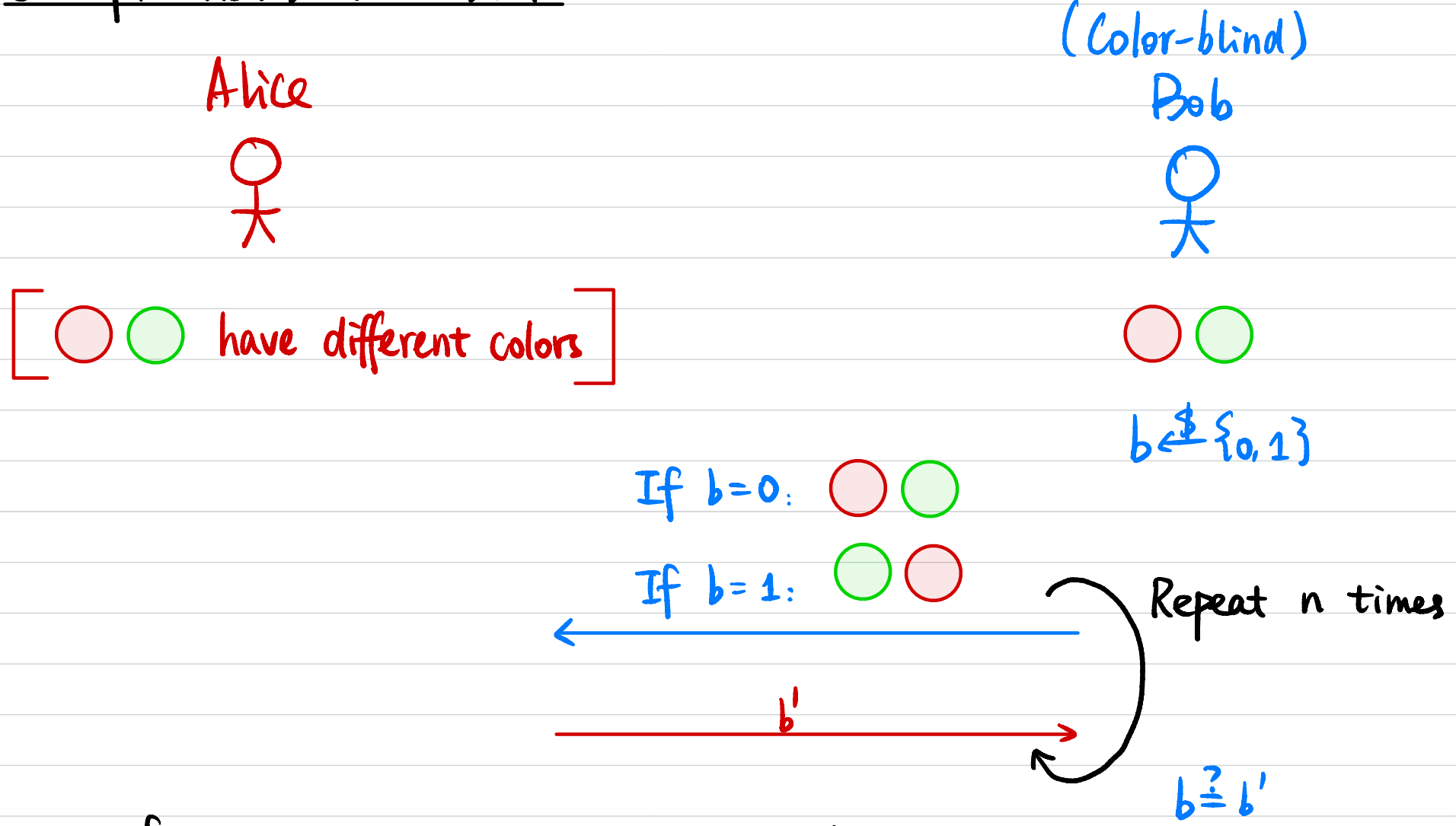
[There is enough balance in my Bitcoin account]

[ have different colors]

What is a proof?

What does zero-knowledge mean?

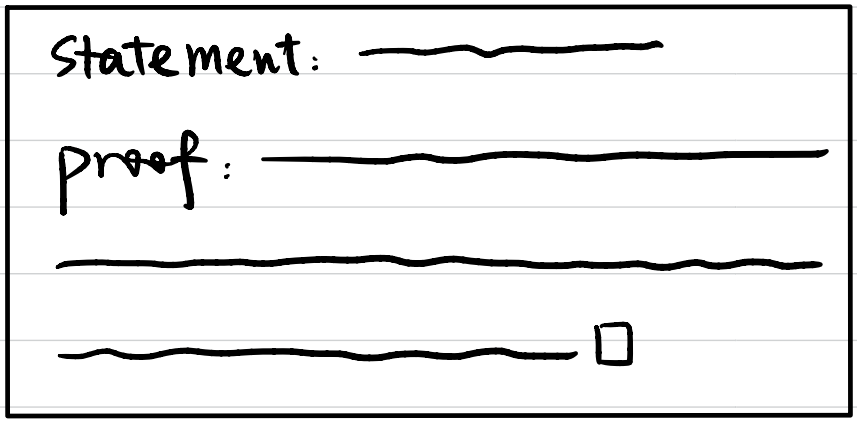
Example: Red & Green Balls



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

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

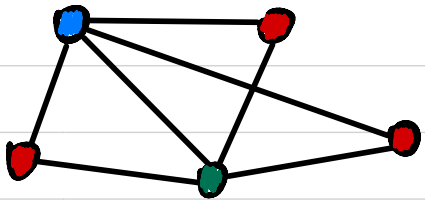
What is a "proof system"?



- **Completeness:** If statement is true, then ∃ proof that proves it's true.
- **Soundness:** If statement is false, then ∀ 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 $R_L = \{ (G, 3COL) \}$

G: graph; $3COL$: 3-coloring

Statement: graph G

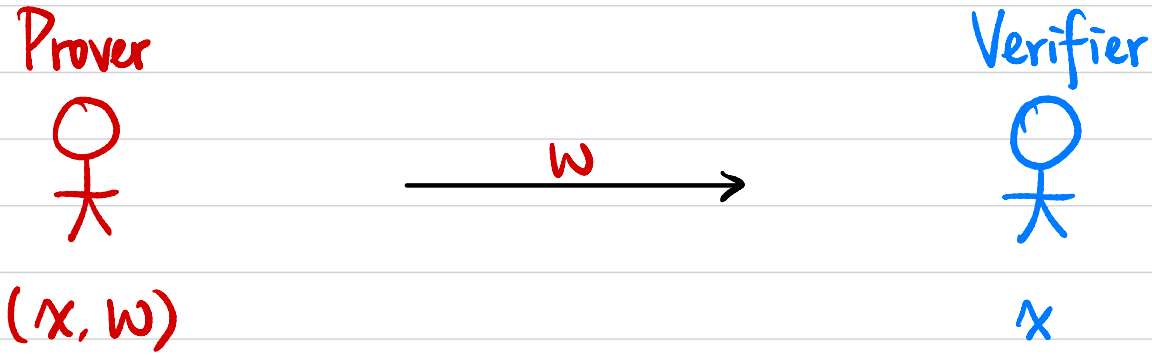
Proof: 3-coloring of G: $3COL$

$(G, 3COL) \in R_L$

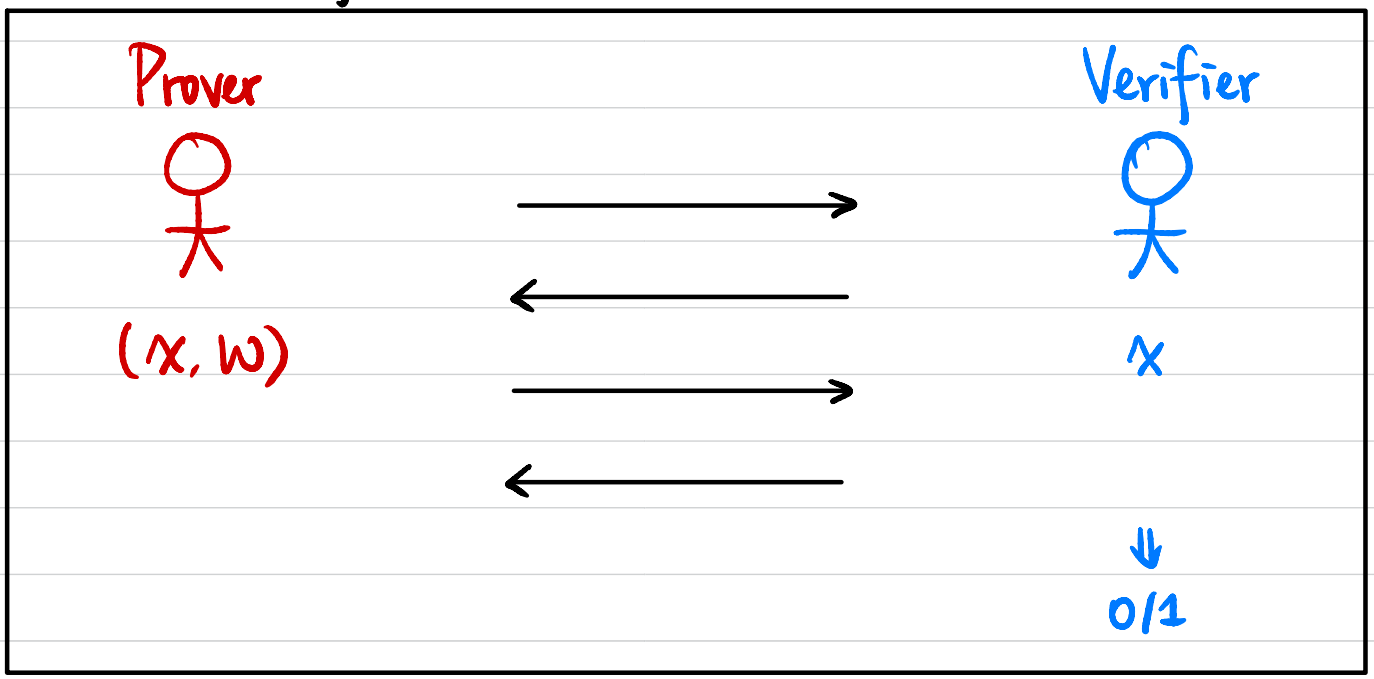
NP as a Proof System

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

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



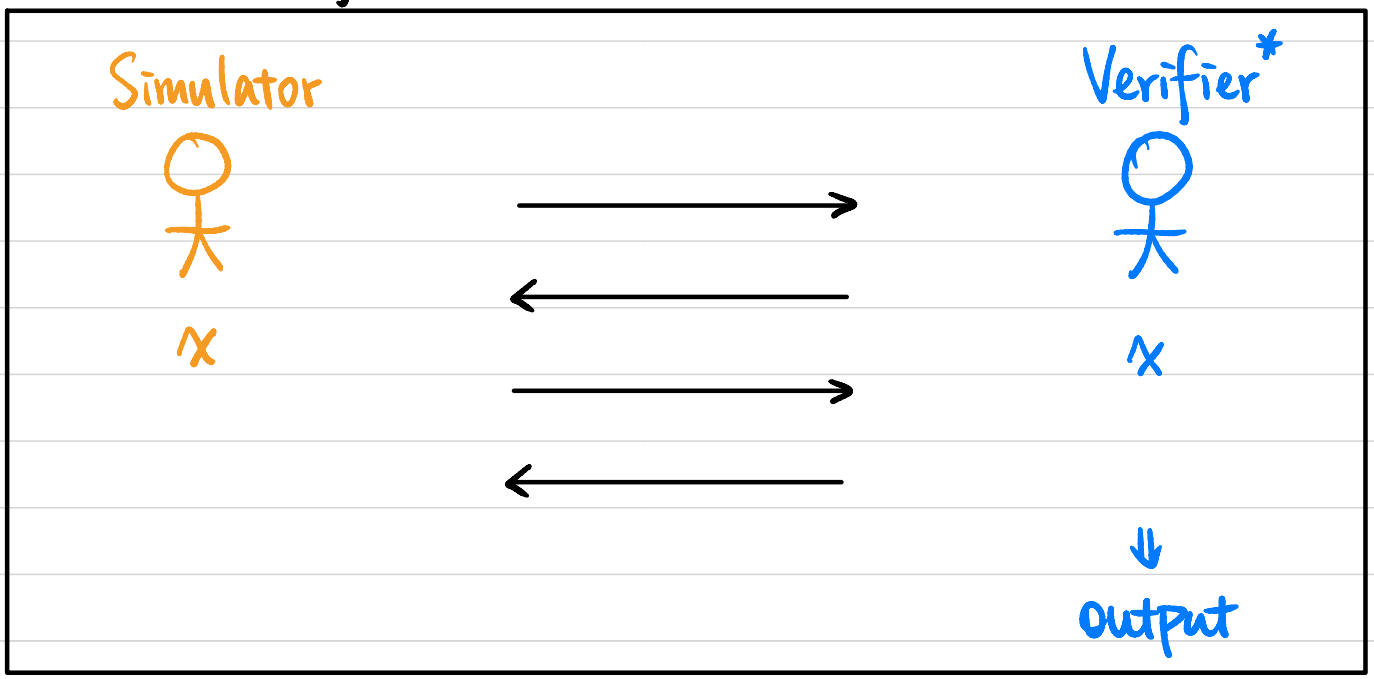
Zero-Knowledge Proof (ZKP)



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:** $\forall (x, w) \in R_L, \quad \Pr[\, P(x,w) \longleftrightarrow V(x) \text{ outputs } 1 \,] = 1.$
- **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

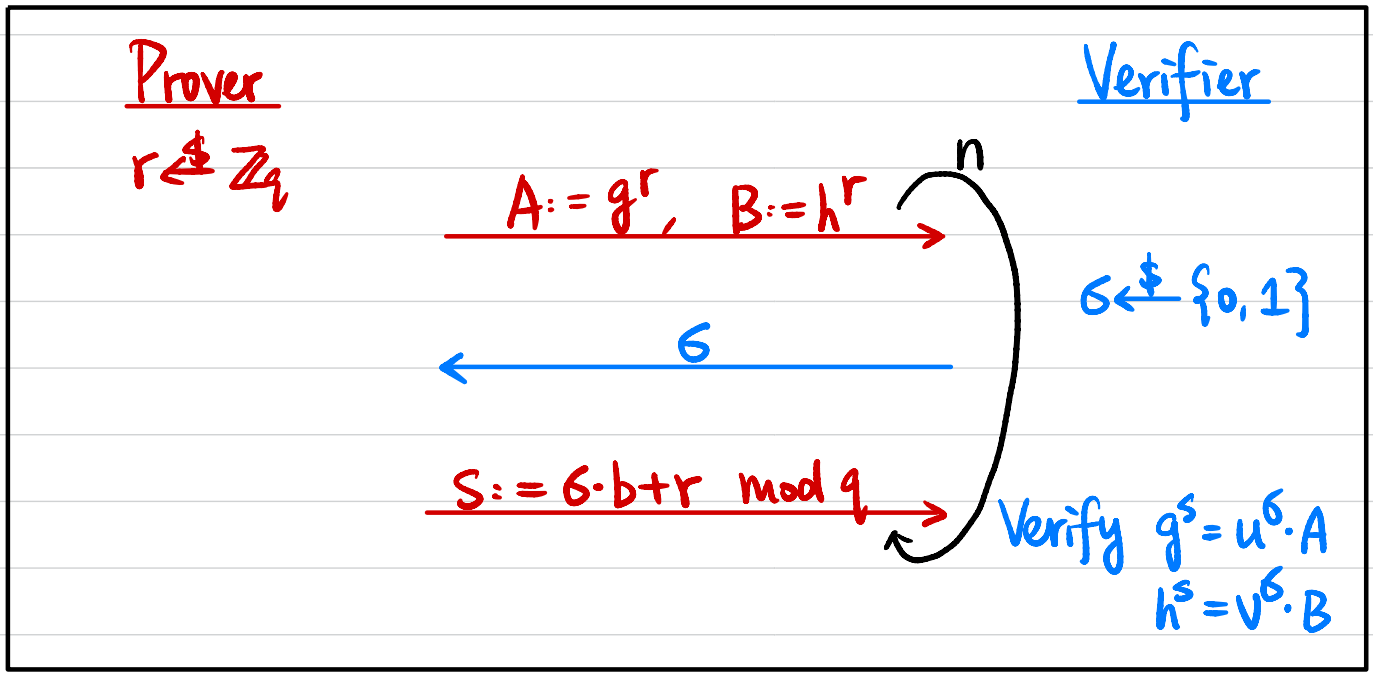
$\equiv$ $\quad$ $\overset{s}{\approx}$ $\quad$ $\overset{c}{\approx}$

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 ?

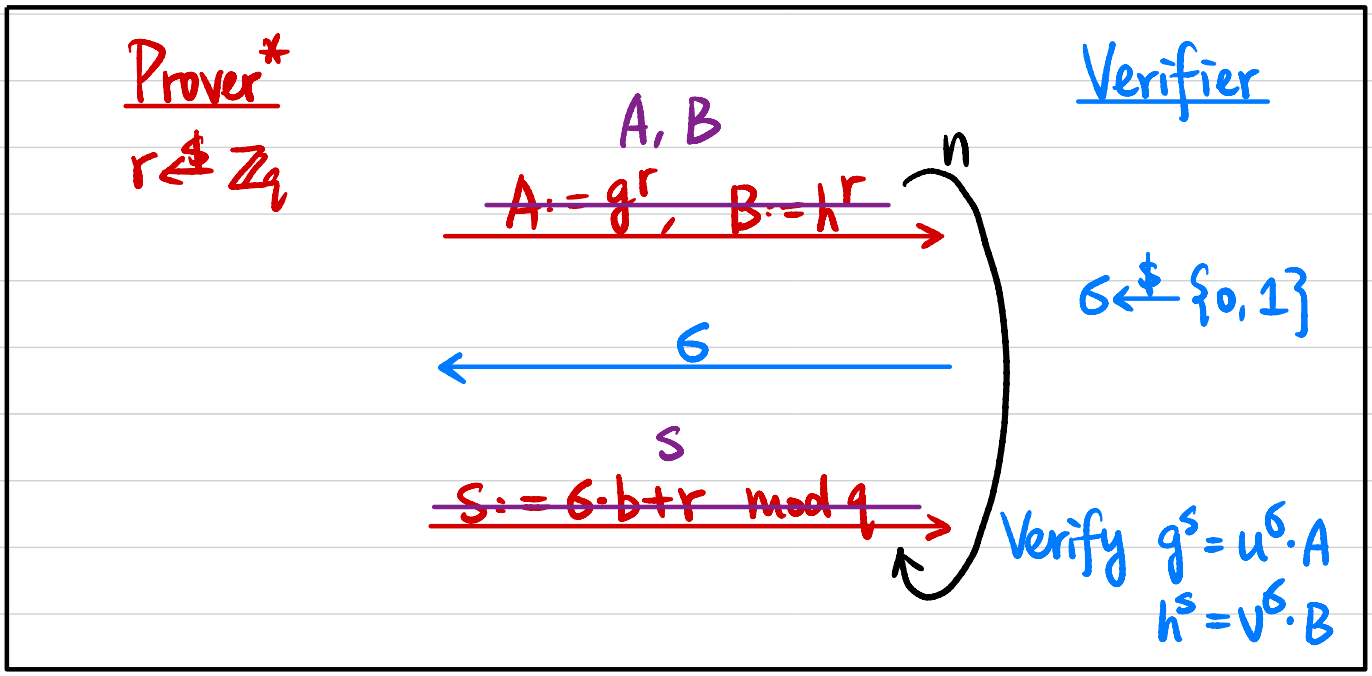
$$g^s = g^{c \cdot b + r} = (g^b)^c \cdot g^r = u^c \cdot A$$

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

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?

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

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