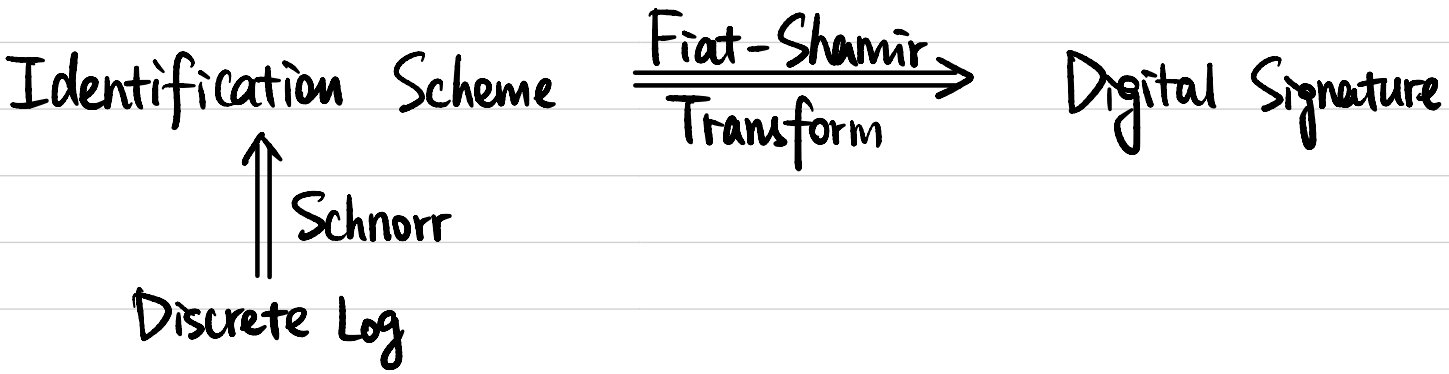
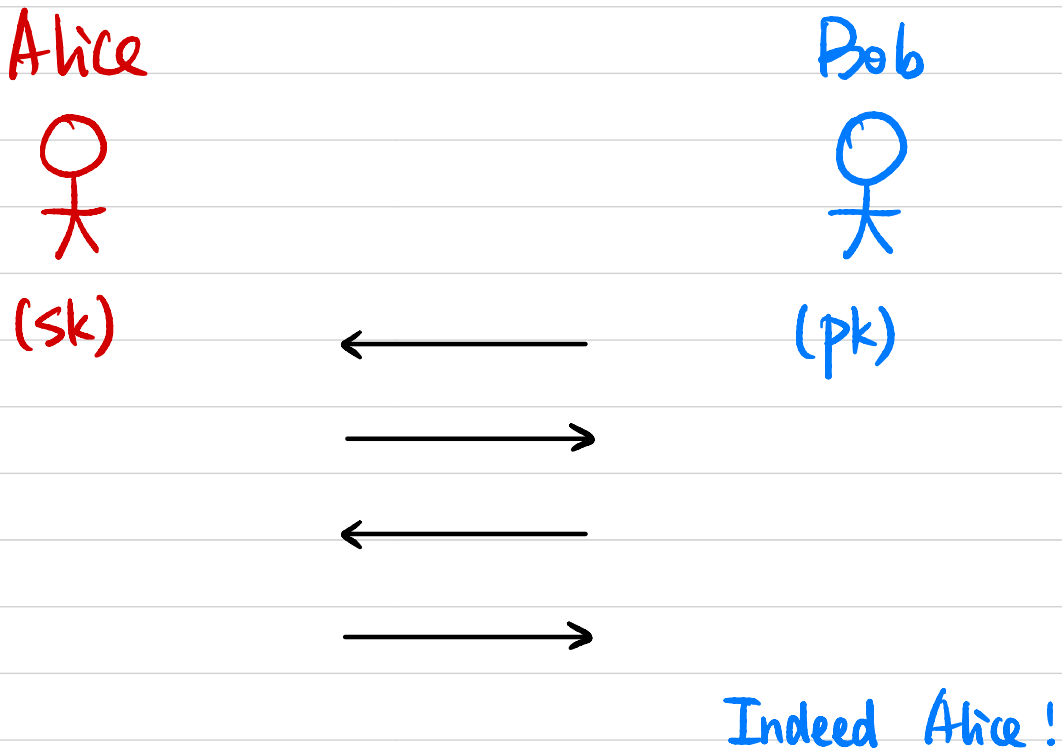
CSCI 1510

- Identification Schemes
- Fiat-Shamir Transform
- Schnorr's Identification / Signature Schemes
- Definition of Zero-Knowledge Proofs

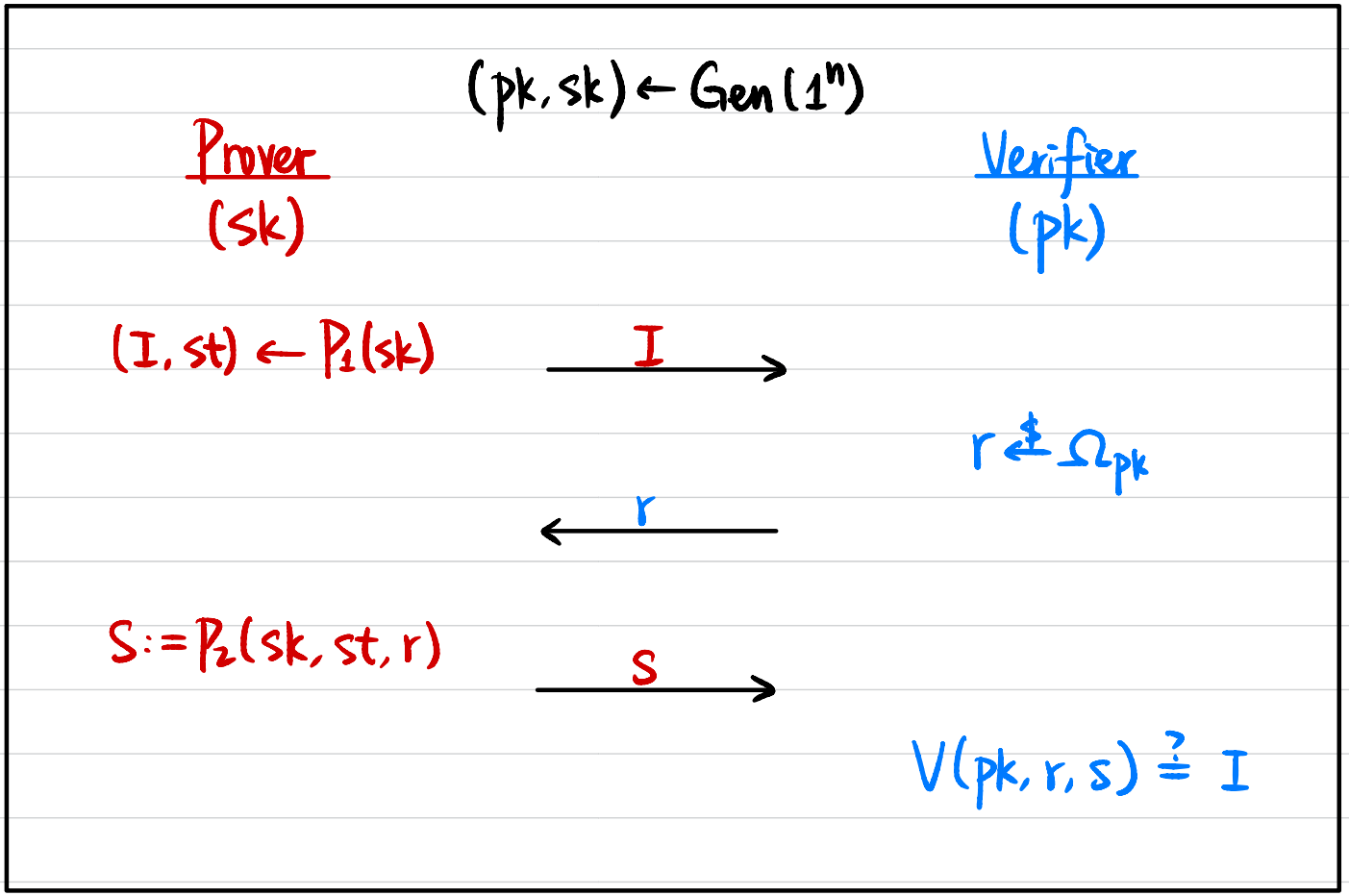
Signatures from DLOG



Identification Scheme



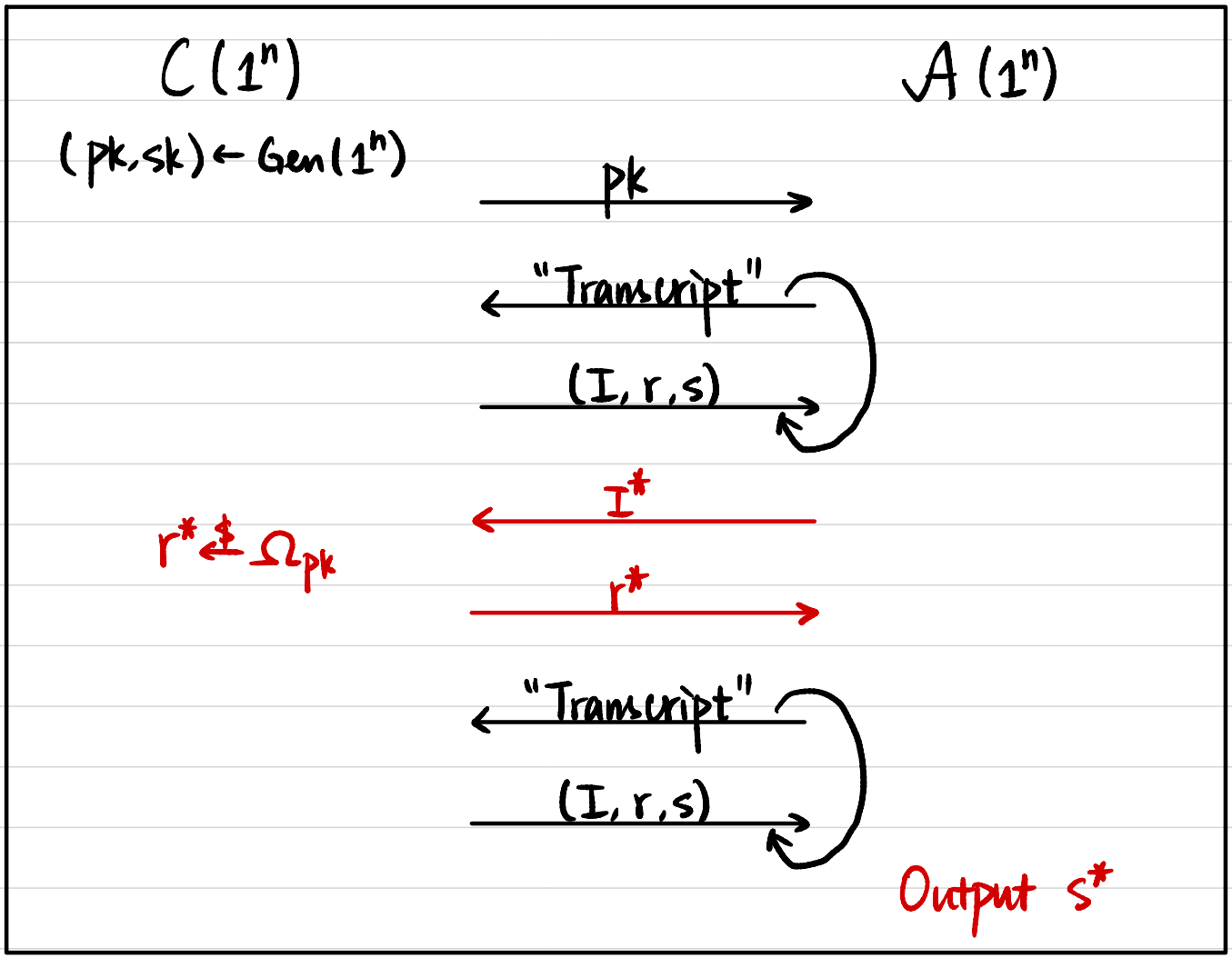
Special 3-Round Identification Scheme



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. $\Pr[V(pk, r^*, s^*) = I^*] \leq \varepsilon(n)$.



Fiat-Shamir Transform

Let $\Pi = (Gen_{ID}, P_1, P_2, V)$ be a secure identification scheme.

Construct a signature scheme $\Pi' = (Gen, Sign, Vrfy)$:

- $Gen(1^n)$:

  $(pk, sk) \leftarrow Gen_{ID}(1^n)$

  Specify a hash function $H: \{0,1\}^* \to \Omega_{pk}$

- $Sign_{sk}(m)$: $m \in \{0,1\}^*$

  $(I, st) \leftarrow P_1(sk)$

  $r := H(I \| m)$

  $s := P_2(sk, st, r)$

  Output $\sigma = (I, r, s)$

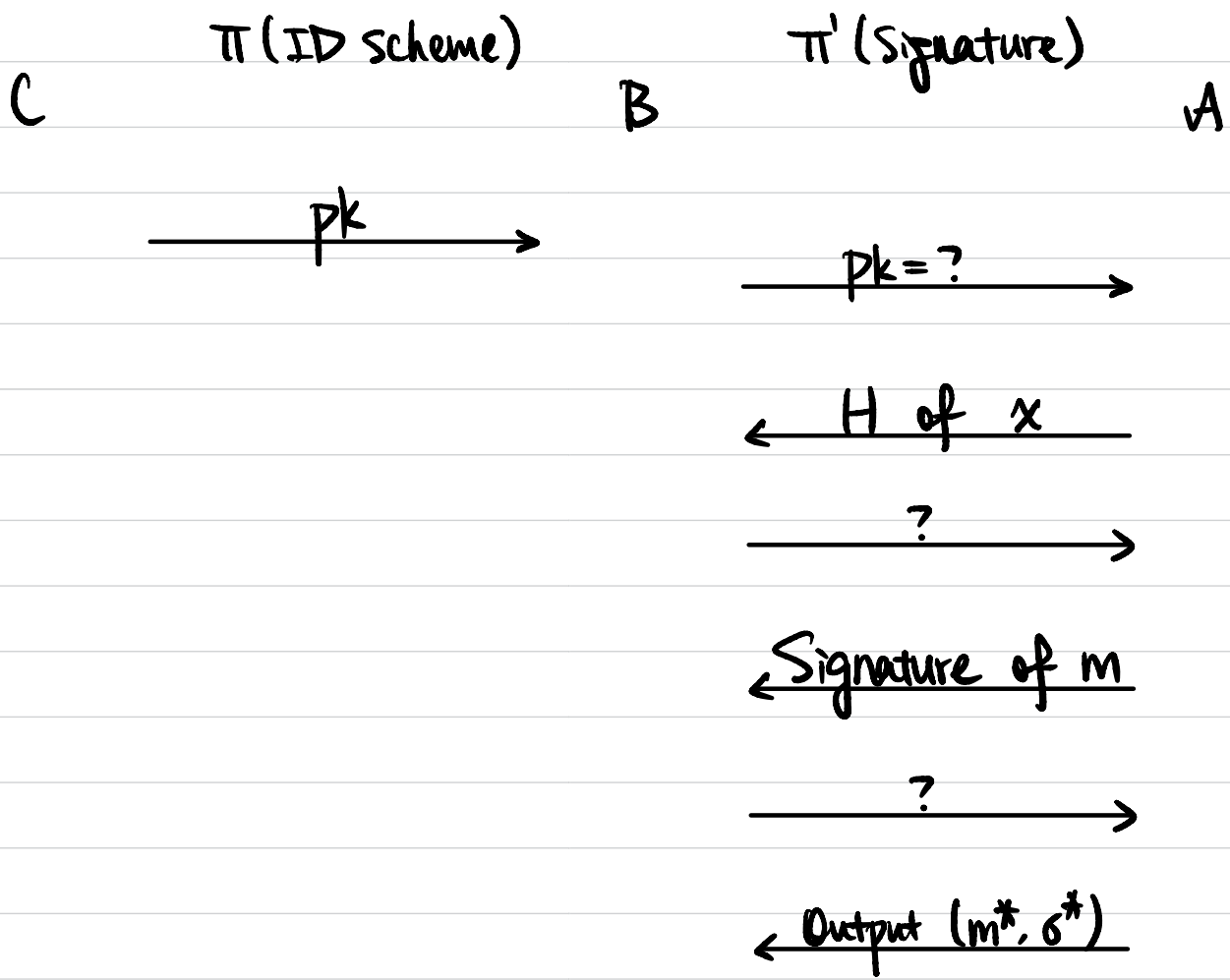
- $Vrfy_{pk}(m, \sigma)$:

  $I := V(pk, r, s)$

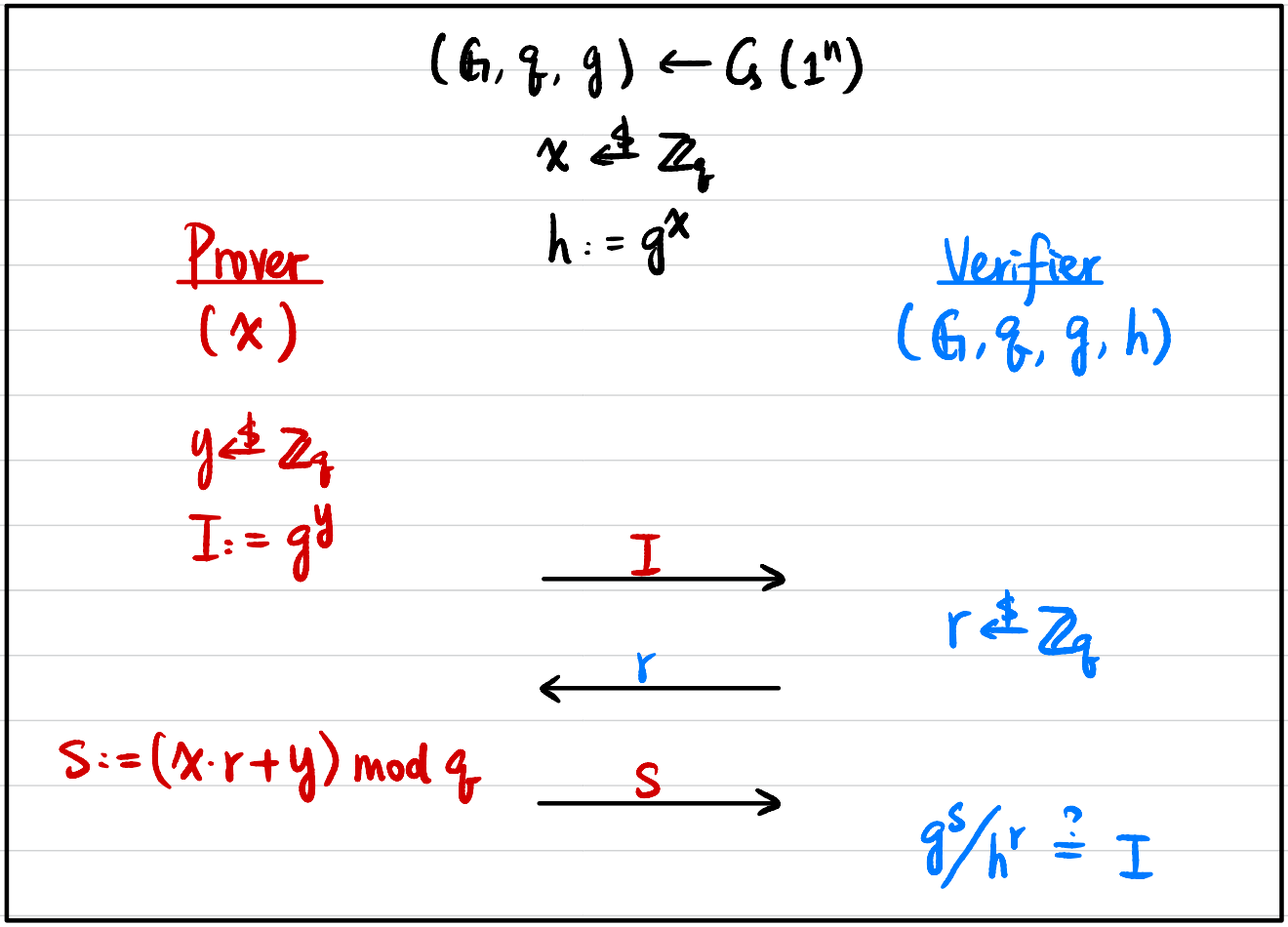
  Output 1 iff $H(I \| m) = r$.

Thm If π is secure and H is modeled as a random oracle, then π' is secure.

Proof Attempt



Schnorr's Identification Scheme



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

Zero-Knowledge Proof (zkp)

Alice

Bob

[Coke & Pepsi taste differently]

[There is a bug in your code]

[I have the secret key for this ciphertext]

What is a proof?

What does zero-knowledge mean?

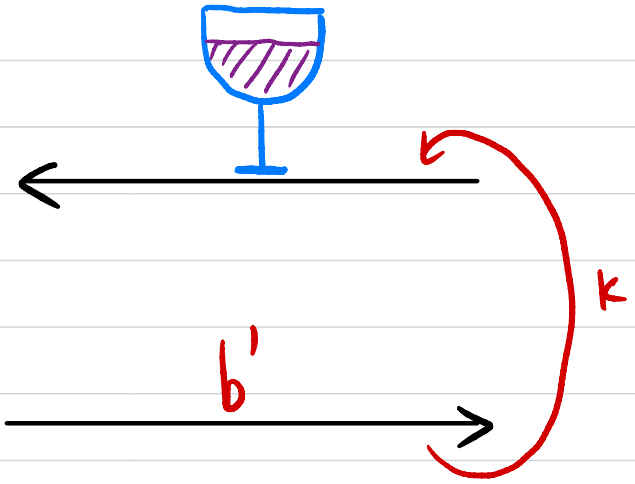
Coke & Pepsi

Alice

Bob

[Coke & Pepsi taste differently]

$b \xleftarrow{\$} \{0,1\}$



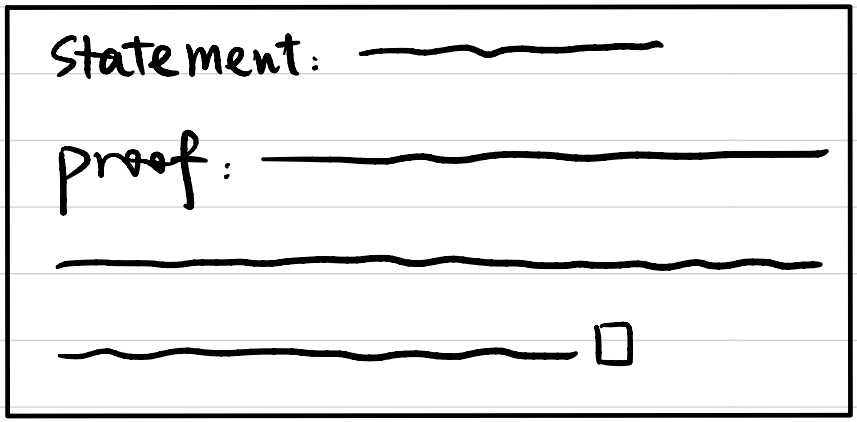
b = 0, Coke

b = 1, Pepsi

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

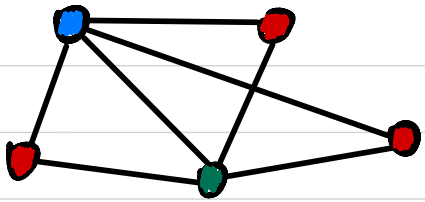
If statement is false: $Pr[b = b'] = (1/2)^k$

What is a "proof system"?



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

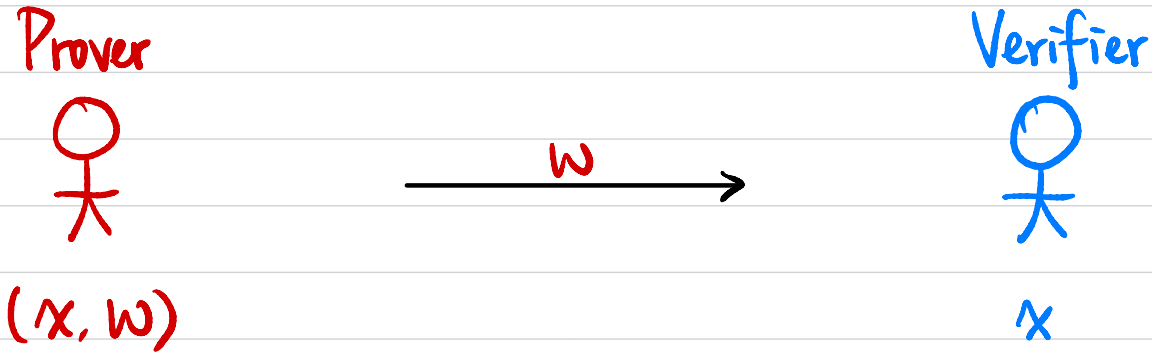
Proof: 3-coloring of G: $3COL$

$(G, 3COL) \in R_L$

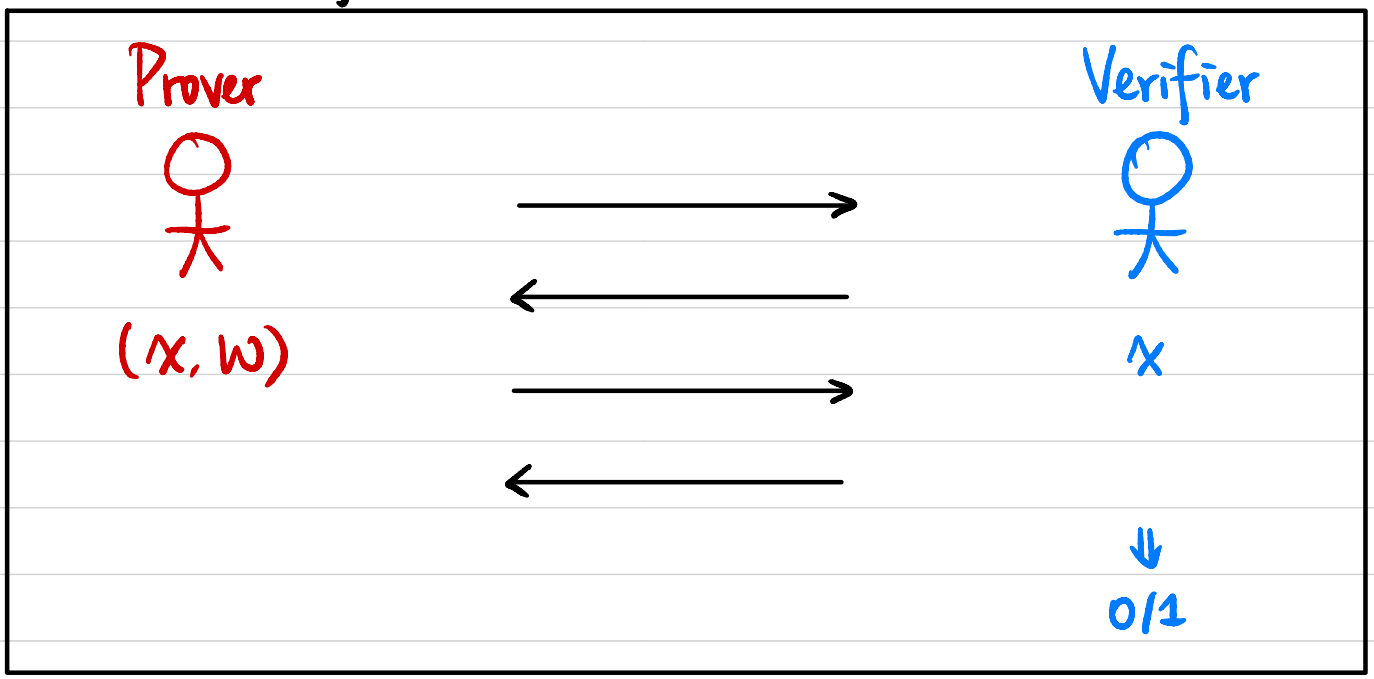
NP as a Proof System

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:** $\forall x \notin L$, $\forall w^*$, $V(x, w^*) = 0$



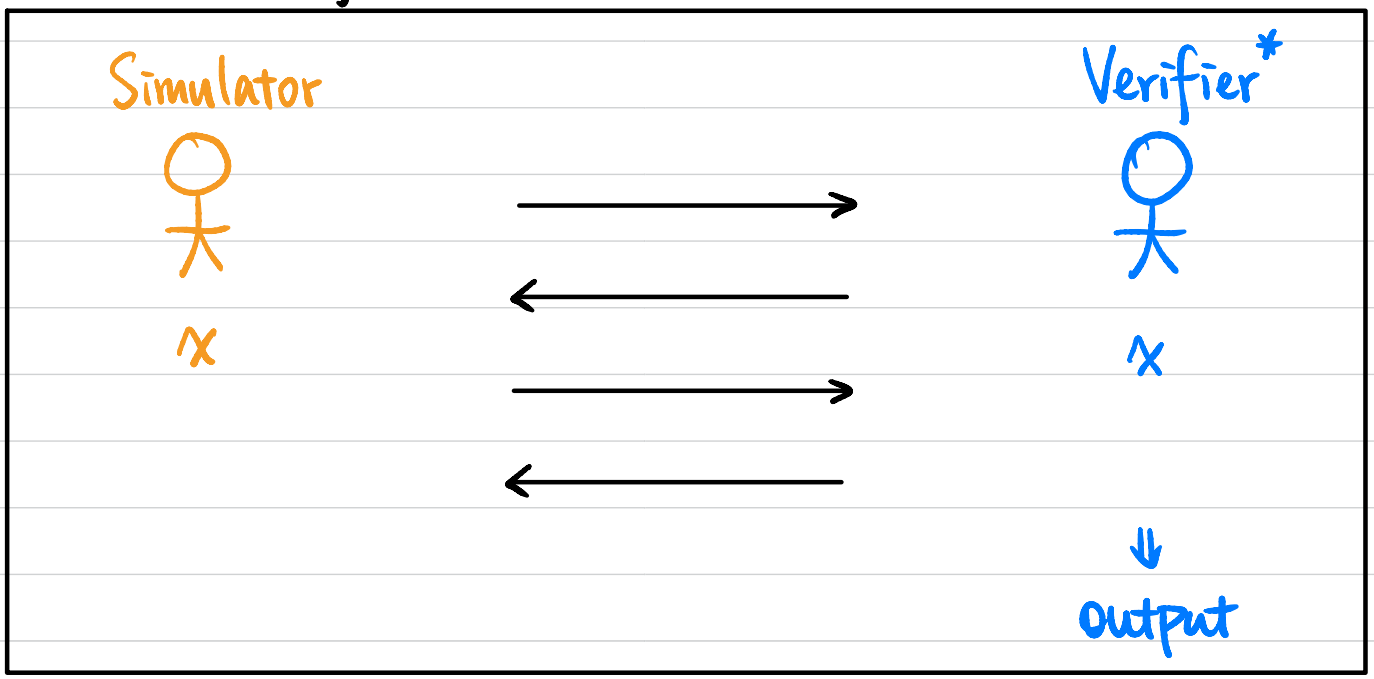
Zero-Knowledge Proof (ZKP)



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

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