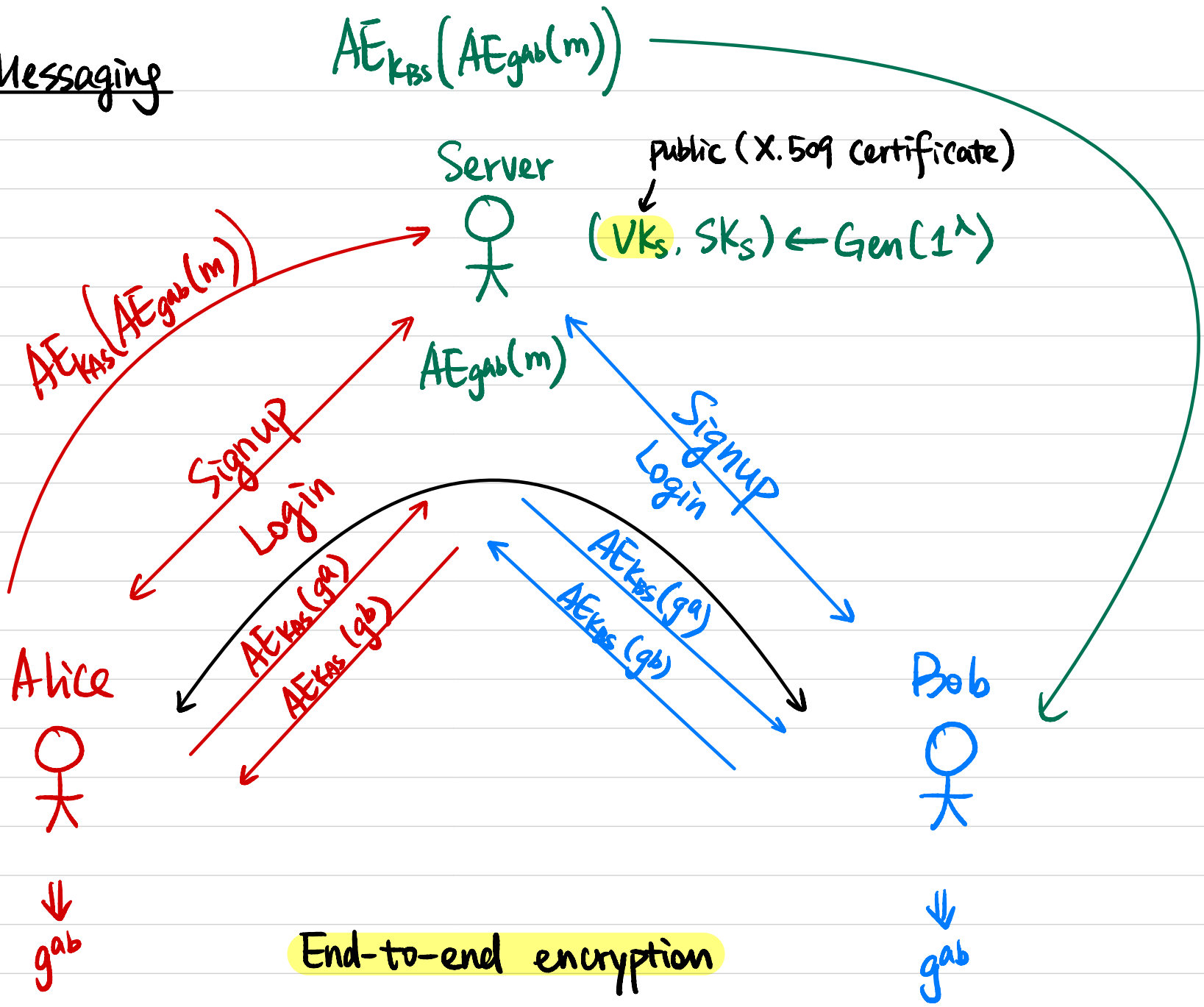
CSCI 1515 Applied Cryptography

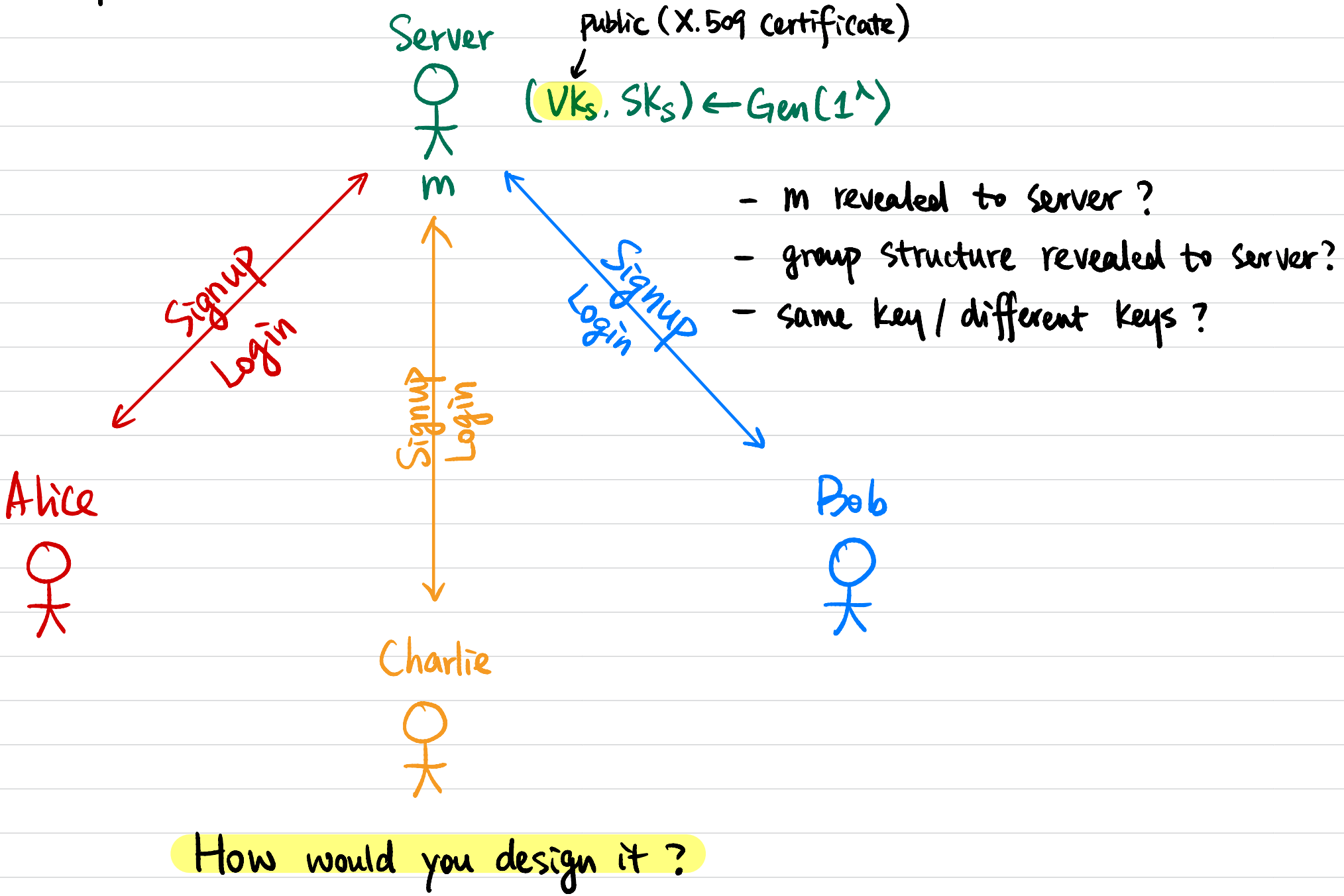
This Lecture:

- Case Study: Group Chat (Continued)
- Single Sign-On (SSO) Authentication
- Zero-Knowledge Proof (of Knowledge)
- Example: Diffie-Hellman Tuple

Secure Messaging



Group Chat ?



- m revealed to server ?
- group structure revealed to server?
- same key / different keys ?

How would you design it ?

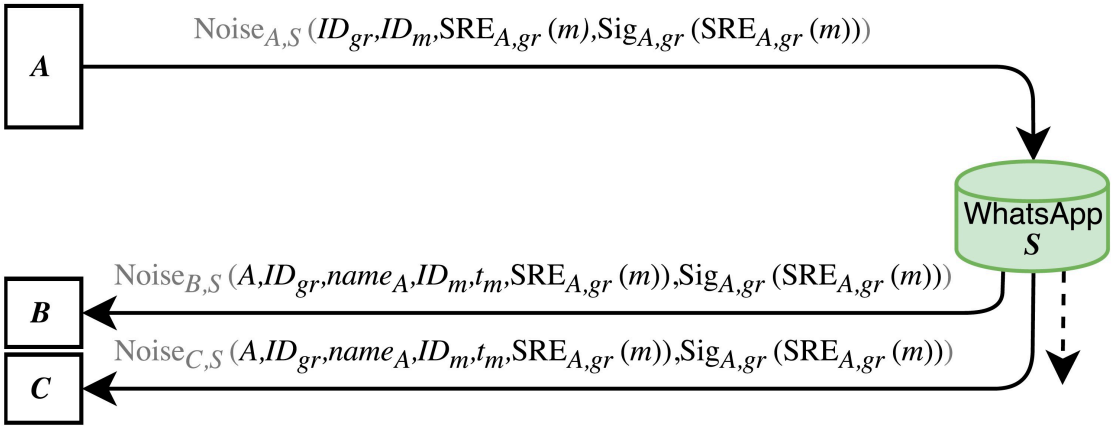


Figure 5. Schematic depiction of traffic, generated for a message m from sender A to receivers B, C in group gr with $\mathcal{G}_{gr} = \{A, B, C\}$ in WhatsApp.

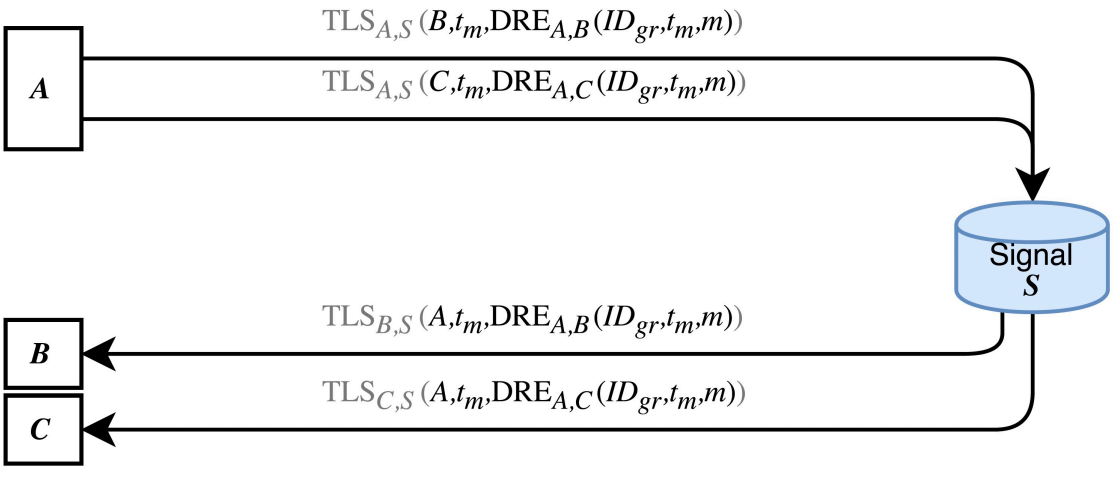
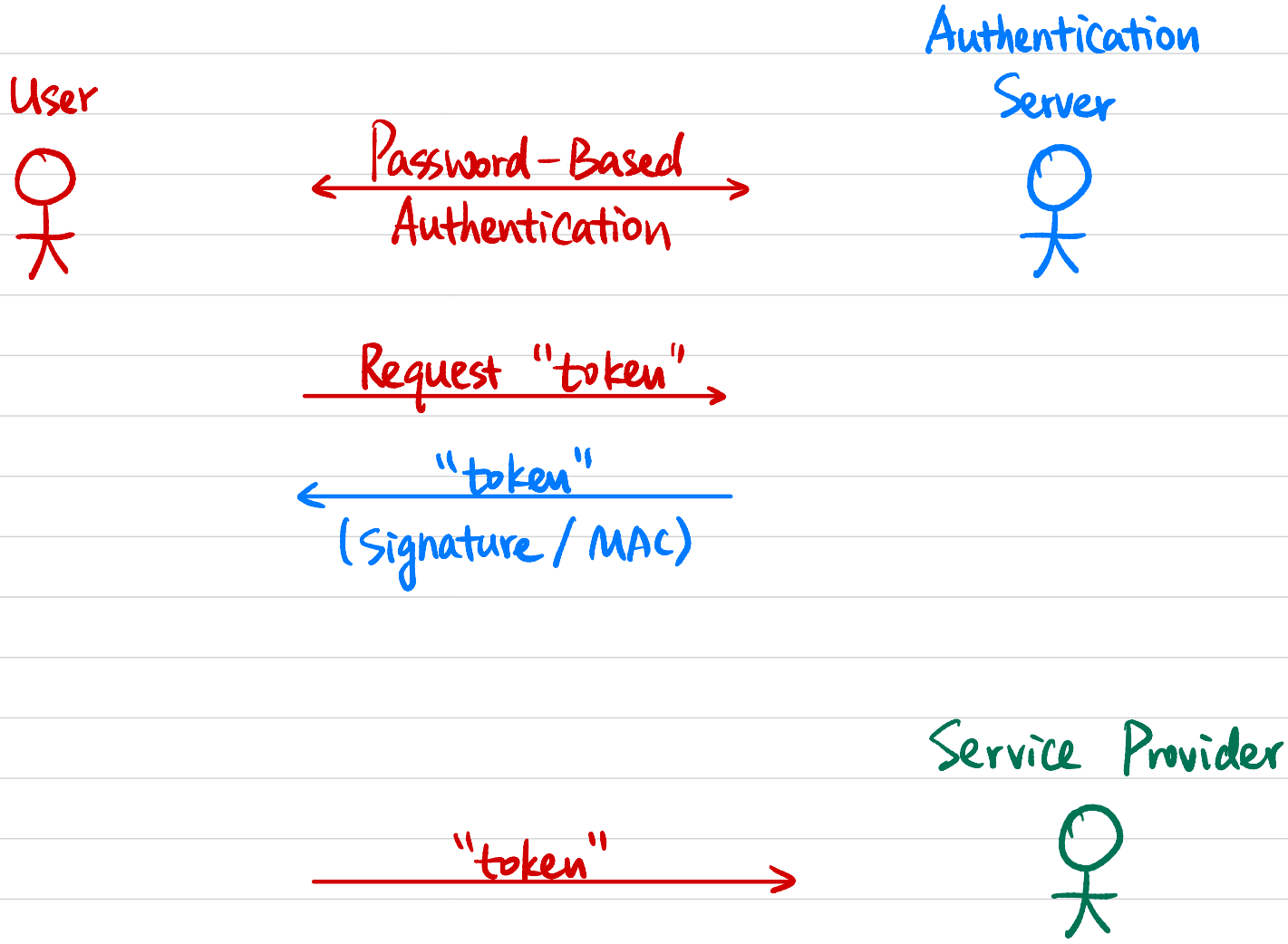


Figure 3. Schematic depiction of Signal's traffic, generated for a message m from sender A to receivers B and C in group gr with $\mathcal{G}_{gr} = \{A, B, C\}$. Transport layer protection is not in the analysis scope (gray).

Single Sign-On (SSO) Authentication



- OAuth / OpenID: Sign-in with Google / Apple / ···
- Kerberos: enterprises

Zero-Knowledge Proofs

[Coca-Cola & Pepsi taste differently]

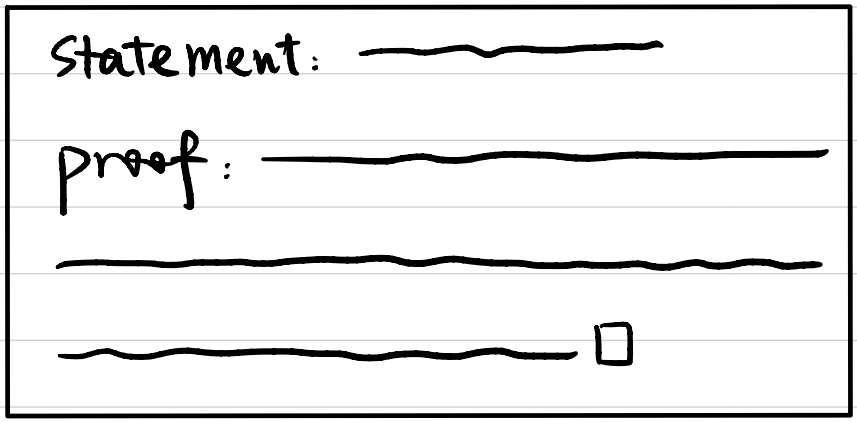
[There is a bug in your code]

[I have the secret key for this ciphertext]

What is a proof?

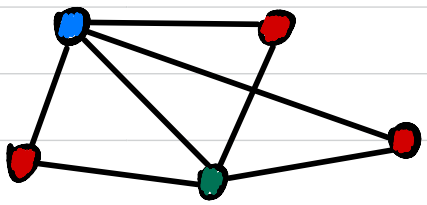
What does zero-knowledge mean?

What is a "proof system"?



NP as a Proof System

Ex: Gragh 3-Coloring



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

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

graph (↑ G) 3-coloring (↑ 3COL)

Statement: graph G

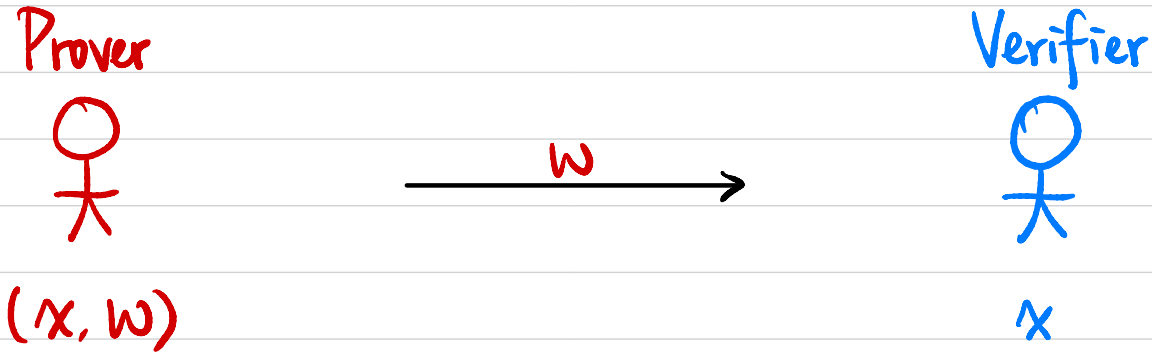
Proof: 3-coloring of G : 3COL

$(G, 3COL) \in R_L$

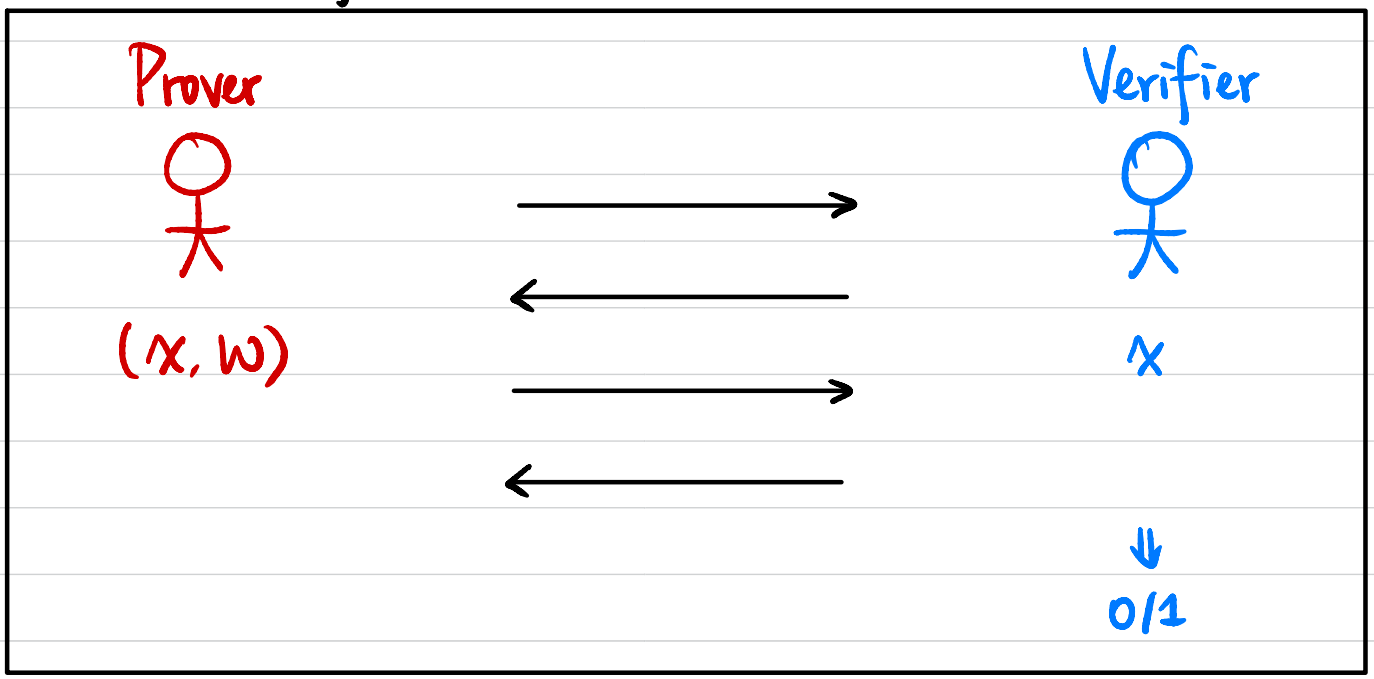
NP as a Proof System

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

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



Zero-Knowledge Proof (ZKP)



Let (P, V) be a pair of probabilistic poly-time (PPT) interactive machines.

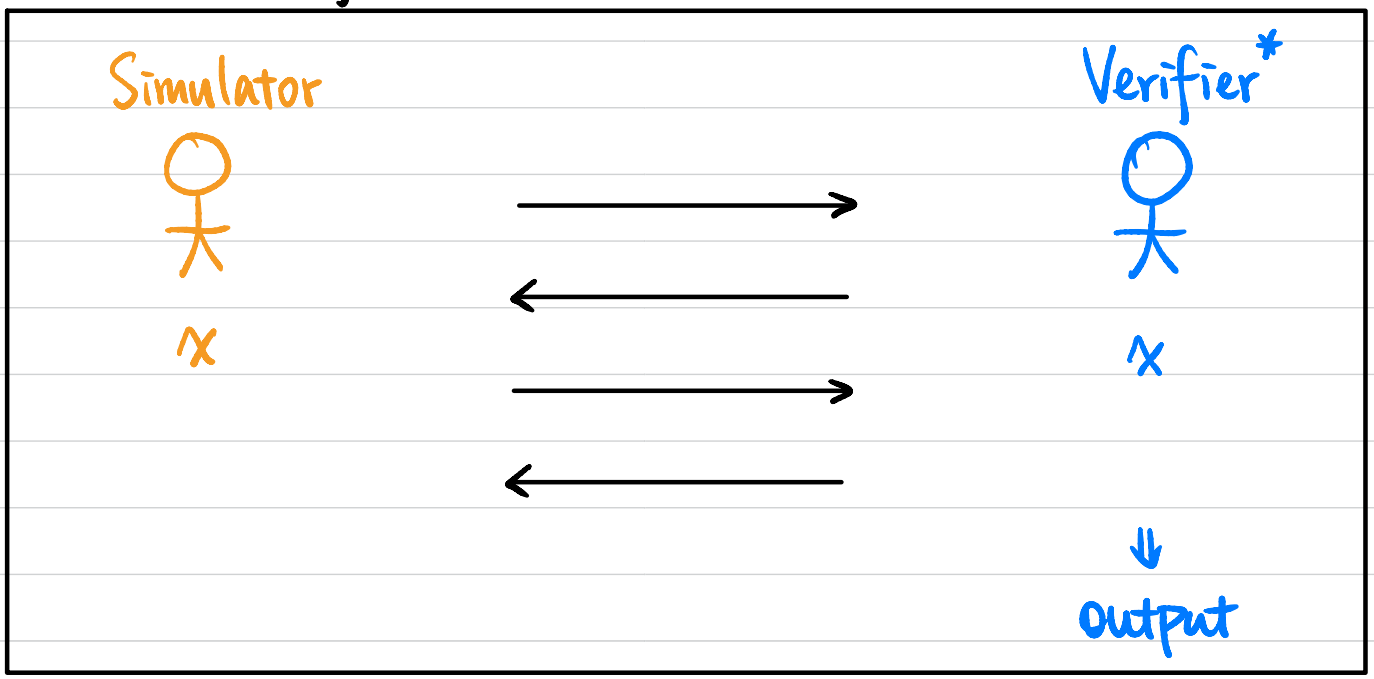
(P, V) is a **zero-knowledge proof system** for a language L with associated relation R_L if

- **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^*, $\Pr[P^*(x) \longleftrightarrow V(x) \text{ outputs } 1] \simeq 0$.

  (PPT): argument

- **Zero-Knowledge?**

Zero-Knowledge Proof (ZKP)



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

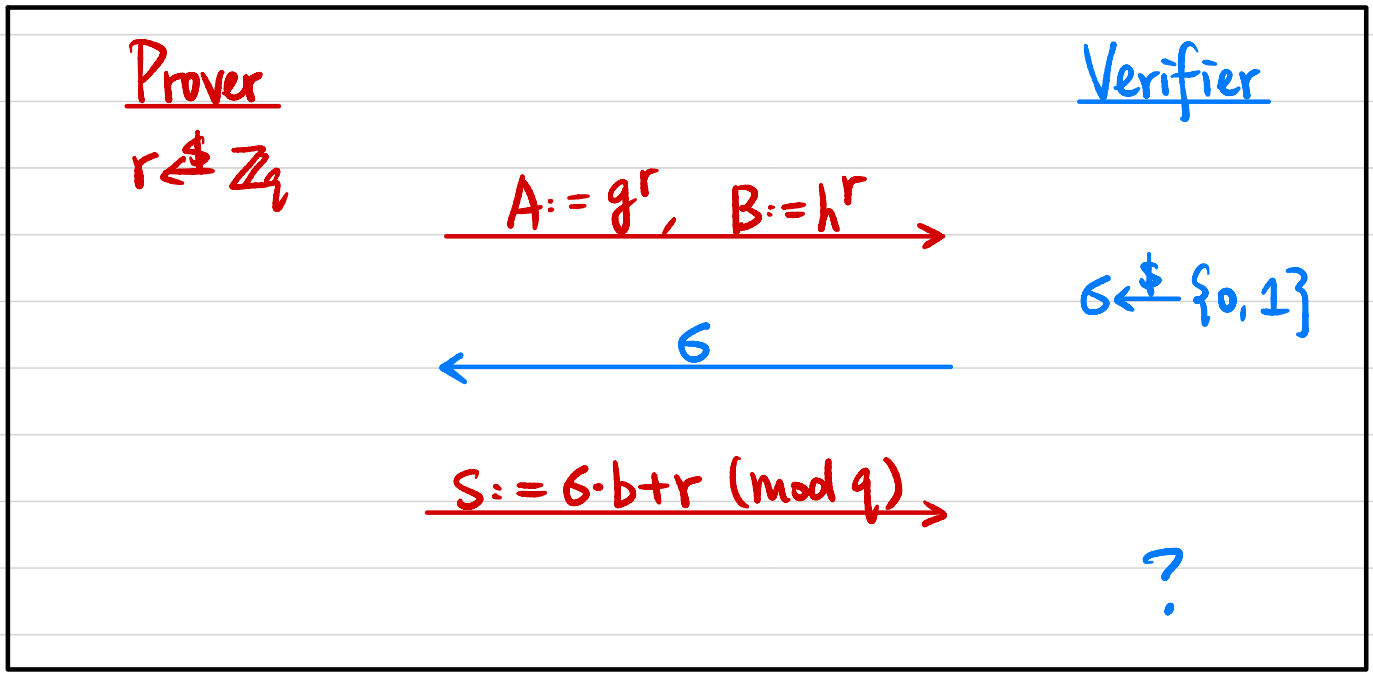
$$Output_{V^*}[P(x,w) \longleftrightarrow V^*(x)] \simeq S(x)$$

Example: Diffie-Hellman Tuple

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. $u = g^b \wedge v = h^b$



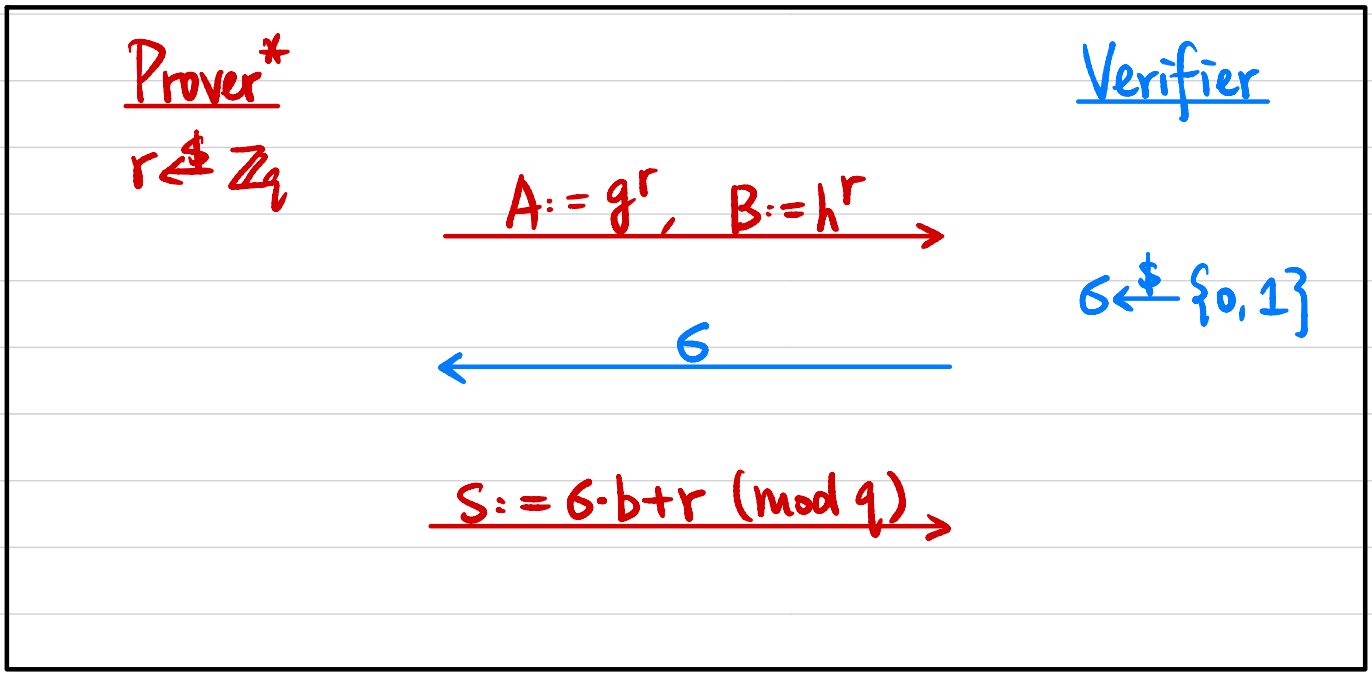
If $\sigma = 0 \Rightarrow s = r \Rightarrow$

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

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

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

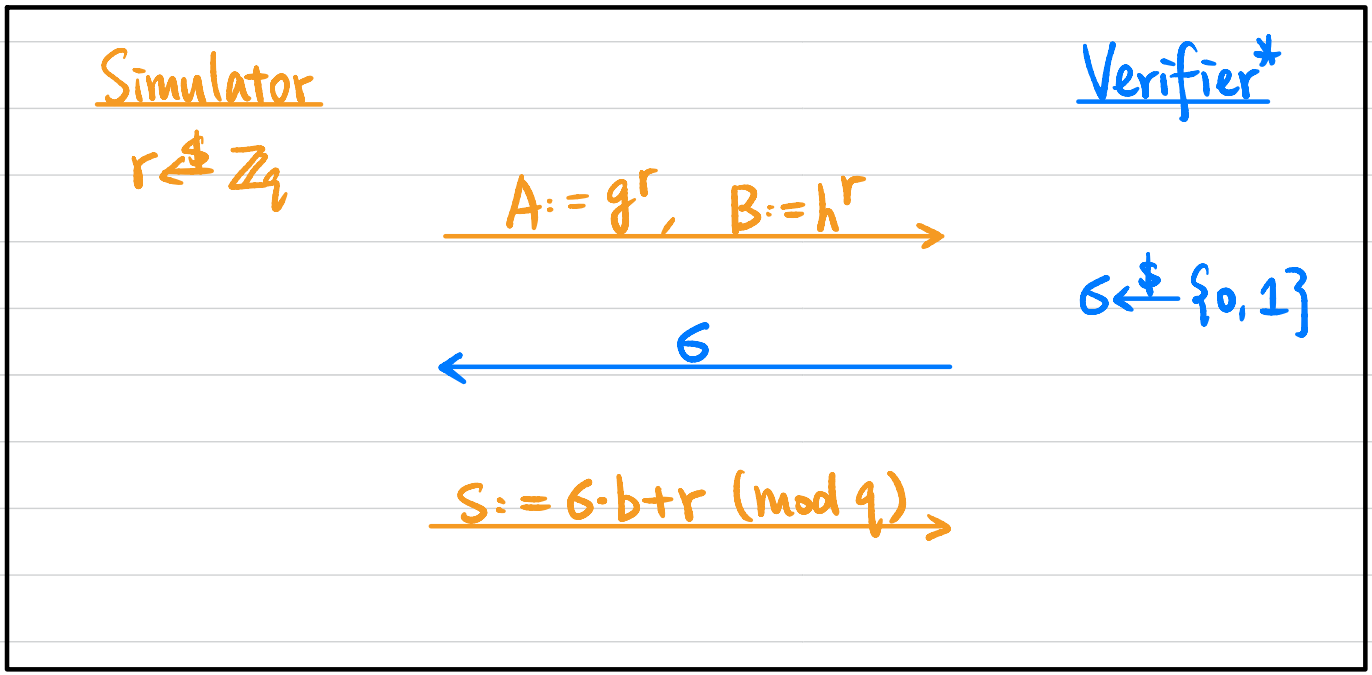
$\forall x \notin L, \forall p^*, \Pr[p^*(x) \longleftrightarrow V(x) \text{ outputs } 1] \simeq 0.$



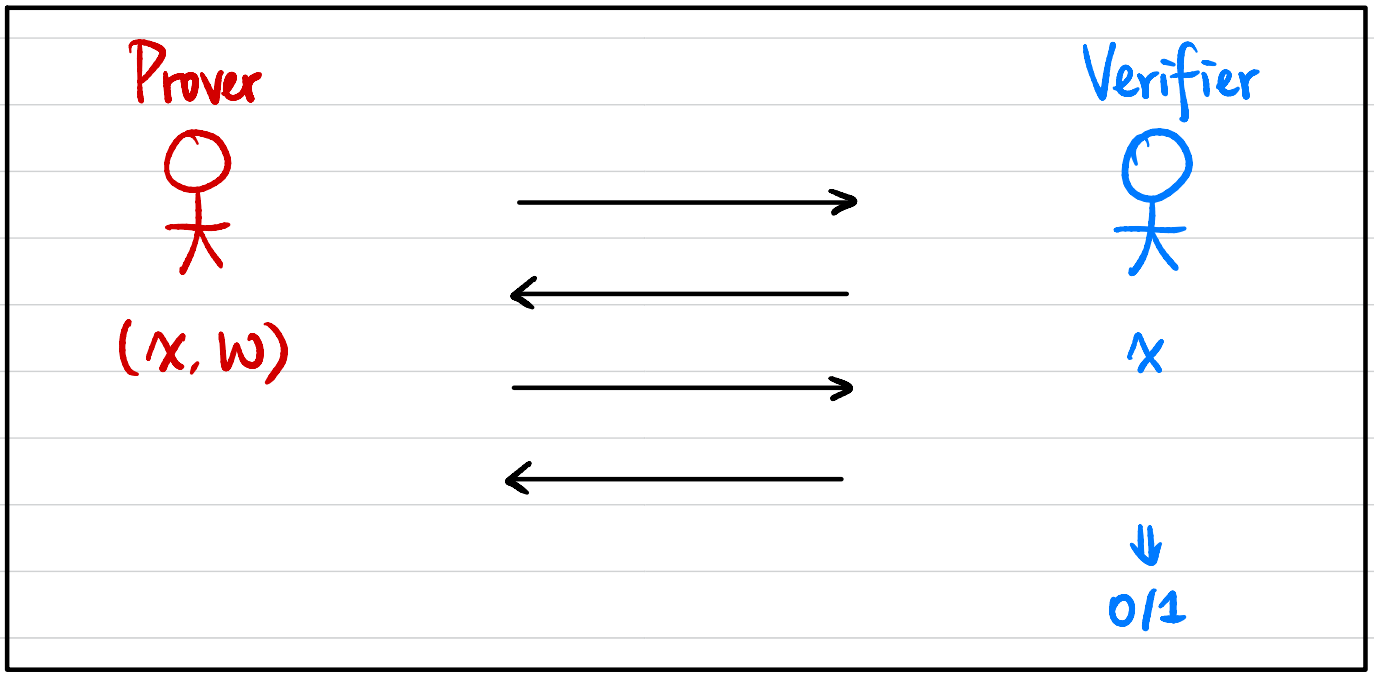
Zero-Knowledge?

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

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



Proof of Knowledge (PoK)



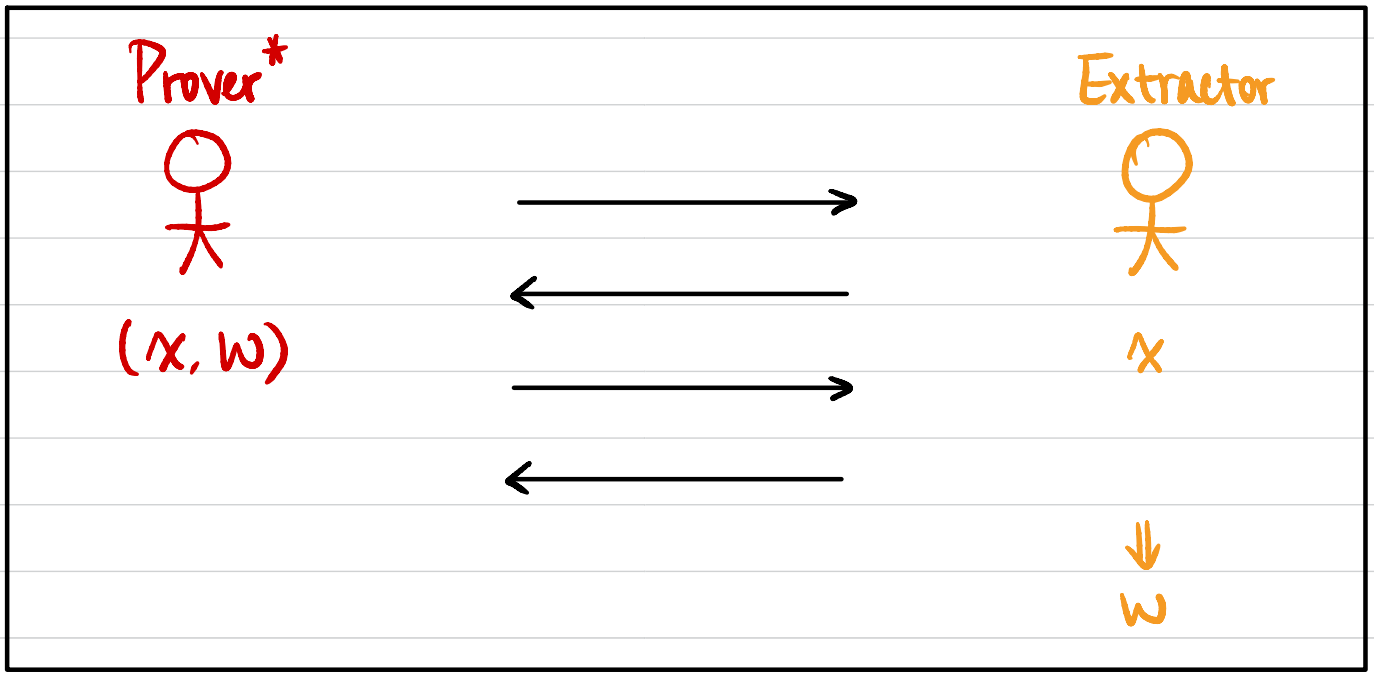
- **Soundness:** $\forall x \notin L$, $\forall$ (PPT) P^*, $Pr[P^*(x) \longleftrightarrow V(x) \text{ outputs } 1] \simeq 0$.

$$R_L = \{ (h = g^{\alpha}, \alpha) \}$$

h: x, α: w

$\forall x, \; x \in L$

Proof of Knowledge (PoK)



- **Proof of Knowledge:** $\exists$ PPT E s.t. $\forall$ PPT P^*, $\forall x \in L$,

$$\Pr\left[E^{P^*(\cdot)}(x) \text{ outputs } w \text{ s.t. } (x,w) \in L\right] \simeq \Pr\left[P^* \leftrightarrow V(x) \text{ outputs } 1\right].$$

Proof of Knowledge? $(g, h, u, v) \in L$