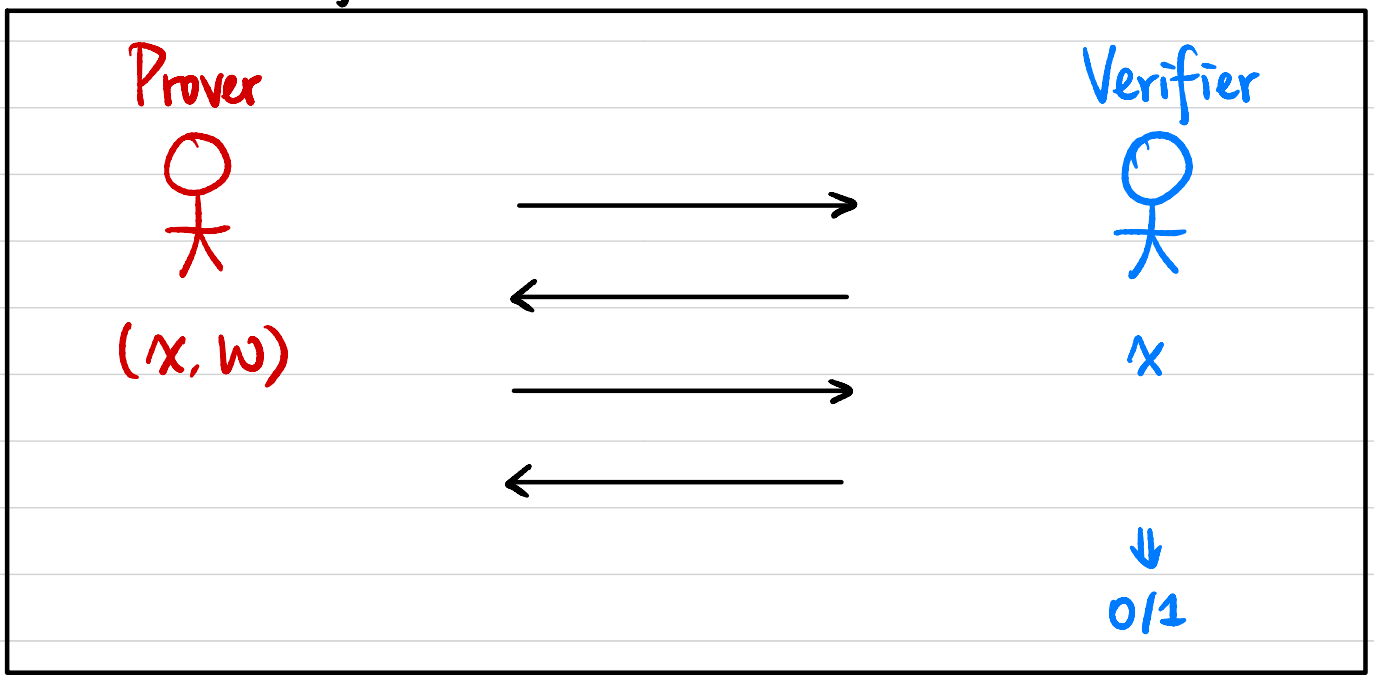
CSCI 1515 Applied Cryptography

This Lecture:

- Proof of Knowledge
- Schnorr's Identification Protocol
- Sigma Protocol and Examples

Zero-Knowledge Proof (ZKP)



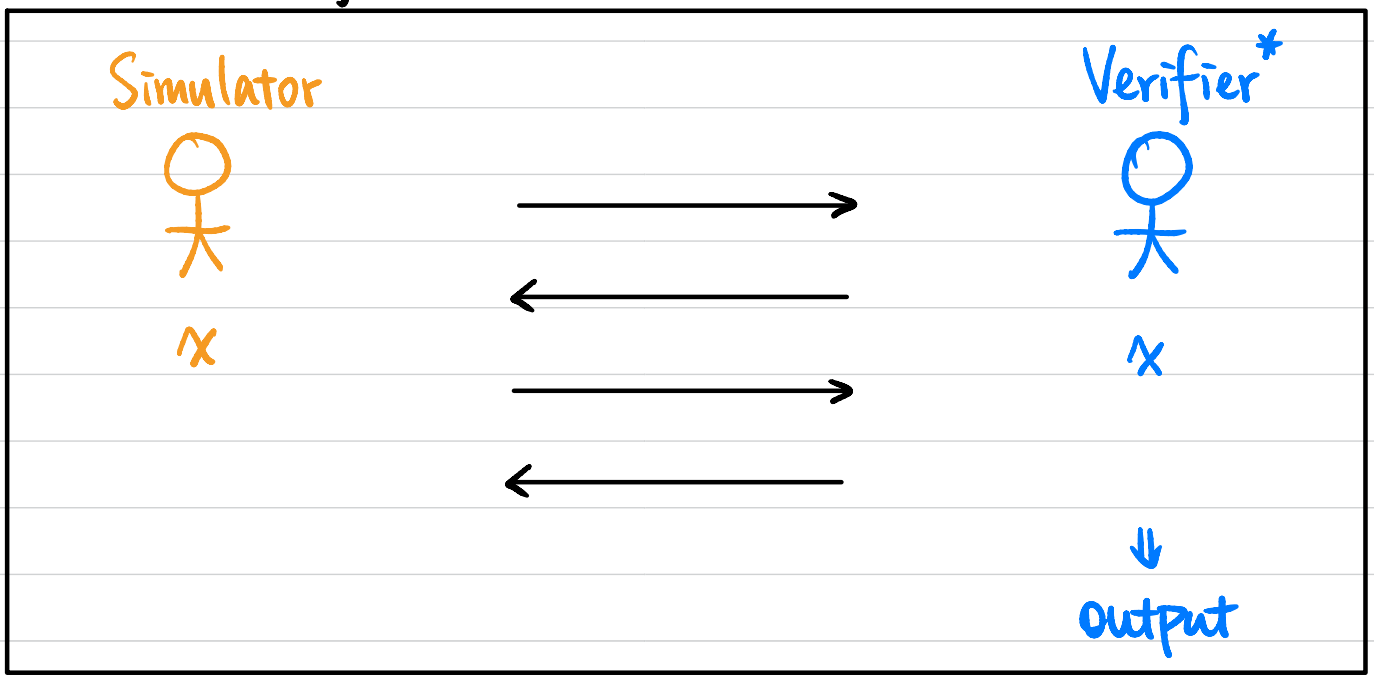
Let (P, V) be a pair of probabilistic poly-time (PPT) interactive machines.

(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 Proof (ZKP)



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

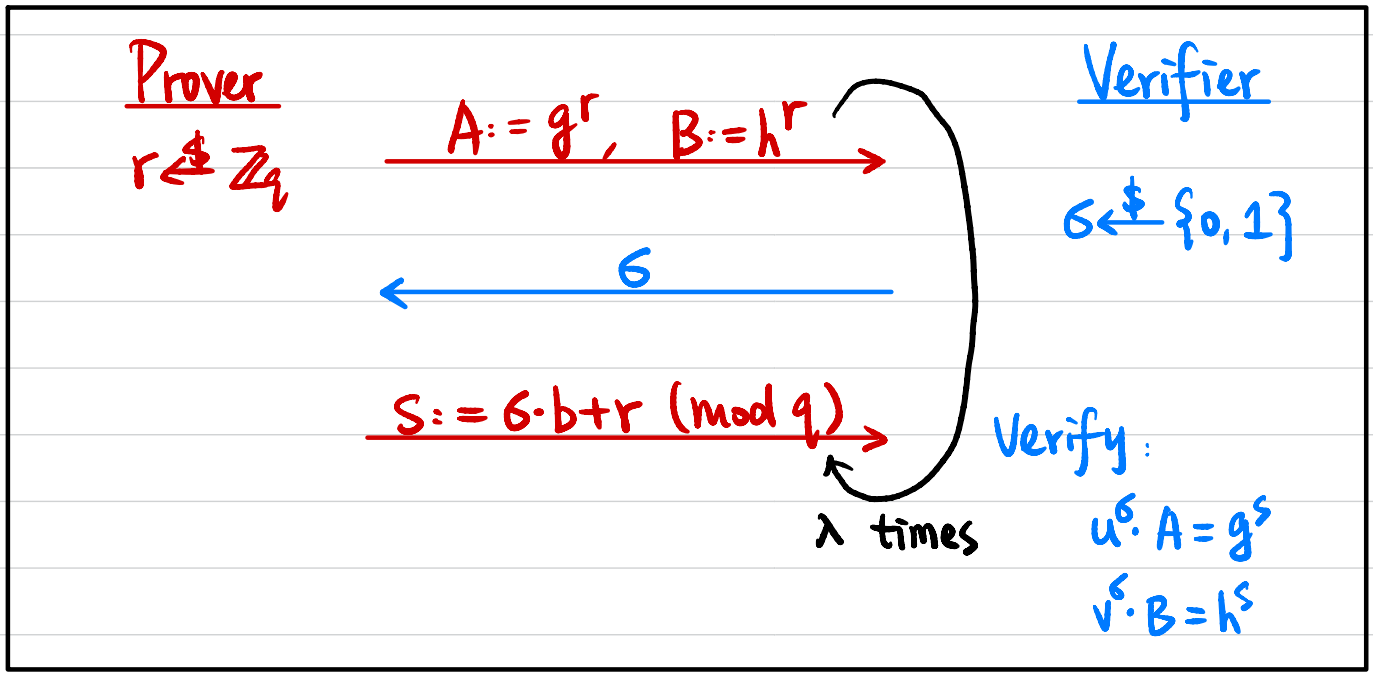
$$Output_{V^*}[P(x,w) \longleftrightarrow V^*(x)] \simeq S(x)$$

Example: Diffie-Hellman Tuple

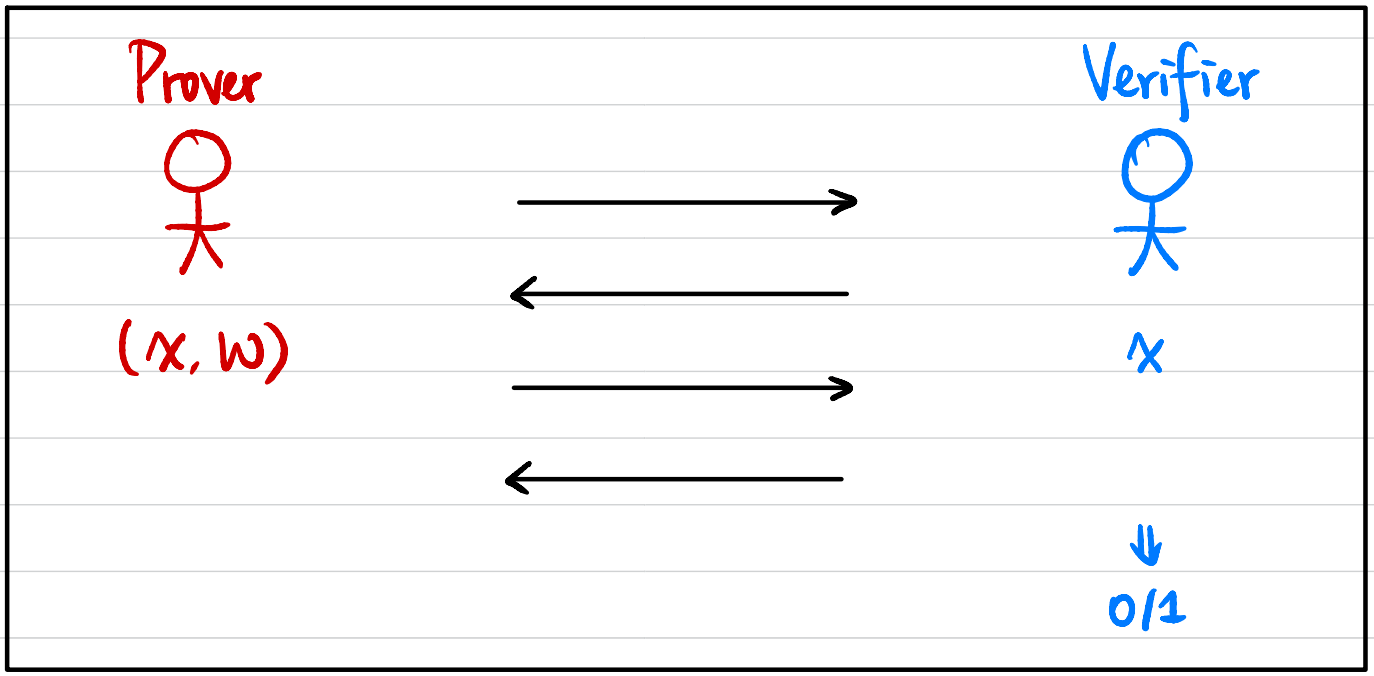
Input: Cyclic group G of order q, generator g, h, u, v
($h = g^a$, $u = g^b$, $v = g^{ab}$)

Witness: b

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



Proof of Knowledge (PoK)



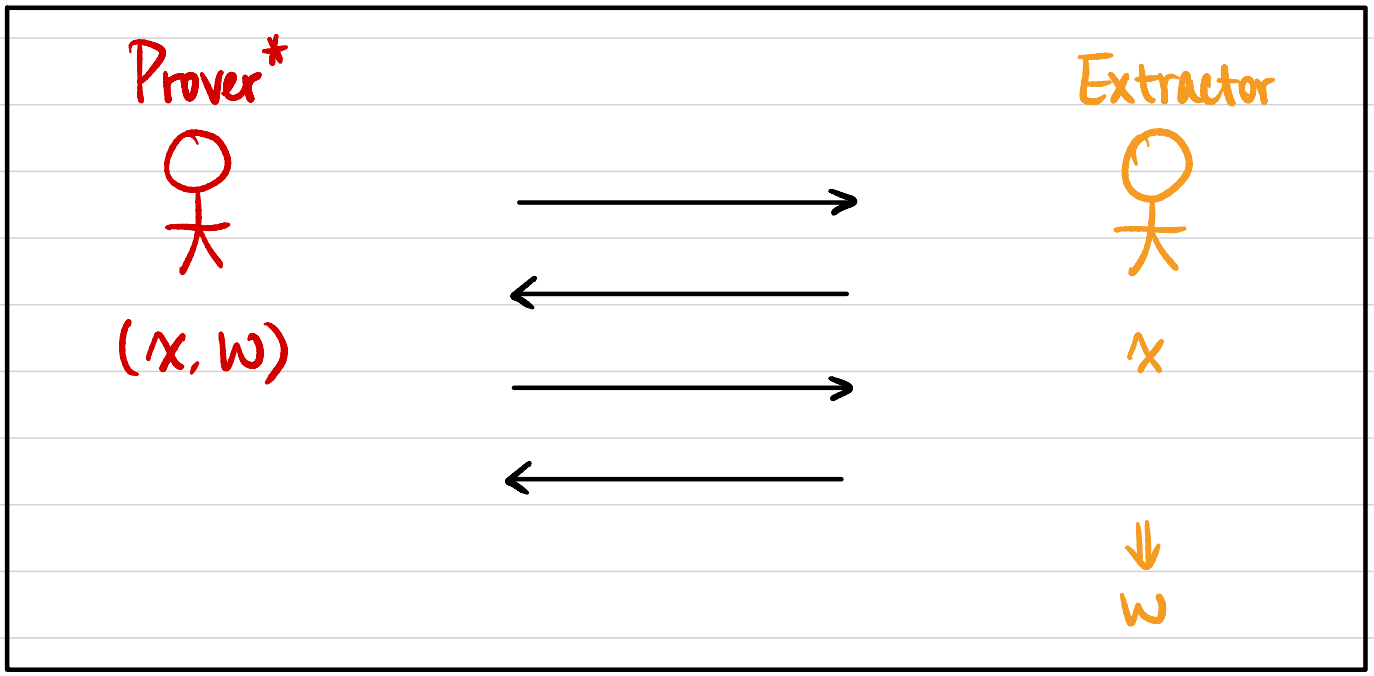
- **Soundness:** $\forall x \notin L$, $\forall$ (PPT) P^*, $Pr[P^*(x) \longleftrightarrow V(x) \text{ outputs } 1] \simeq 0$.

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

h: x, α: w

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

Proof of Knowledge (PoK)



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

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

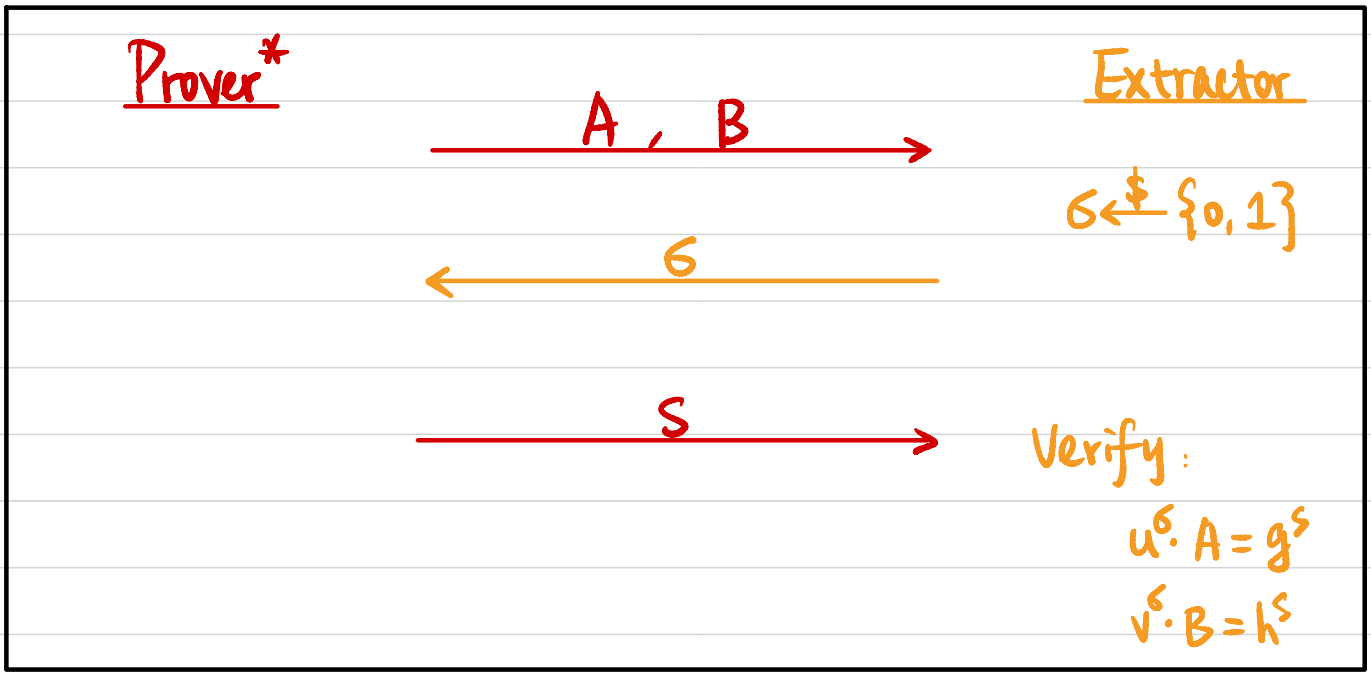
Zero-Knowledge Proof of Knowledge

- **Completeness:** $\forall (x, w) \in R_L$, $\Pr[P(x,w) \longleftrightarrow V(x) \text{ outputs } 1] = 1$.
- **Soundness:** $\forall x \notin L$, $\forall P^*$, $\Pr[P^*(x) \longleftrightarrow V(x) \text{ outputs } 1] \simeq 0$.
- **Zero-Knowledge:** $\forall \text{PPT } V^*$, $\exists \text{PPT } S$ s.t. $\forall (x, w) \in R_L$,
  $\text{Output}_{V^*}[P(x,w) \longleftrightarrow V^*(x)] \simeq S(x)$
- **Proof of Knowledge:** $\exists \text{PPT } E$ s.t. $\forall P^*$, $\forall x$,
  $\Pr[E^{P^*(\cdot)}(x) \text{ outputs } w \text{ s.t. } (x,w) \in R_L] \simeq \Pr[P^* \leftrightarrow V(x) \text{ outputs } 1]$.

Proof of Knowledge?

$(g, h, u, v) \in L$

Extract b s.t. $u = g^b \wedge v = h^b$?

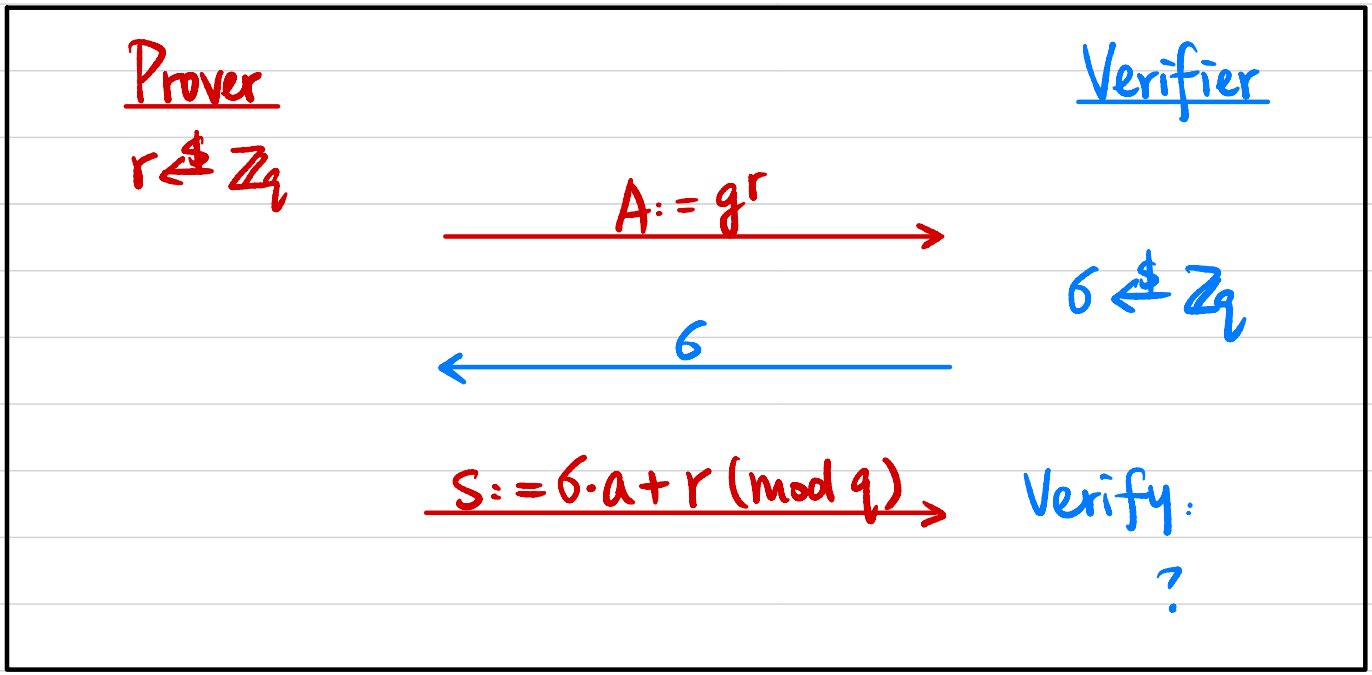


Example: Schnorr's Identification Protocol

Input: Cyclic group G of order q, generator g, $h = g^a$

Witness: a

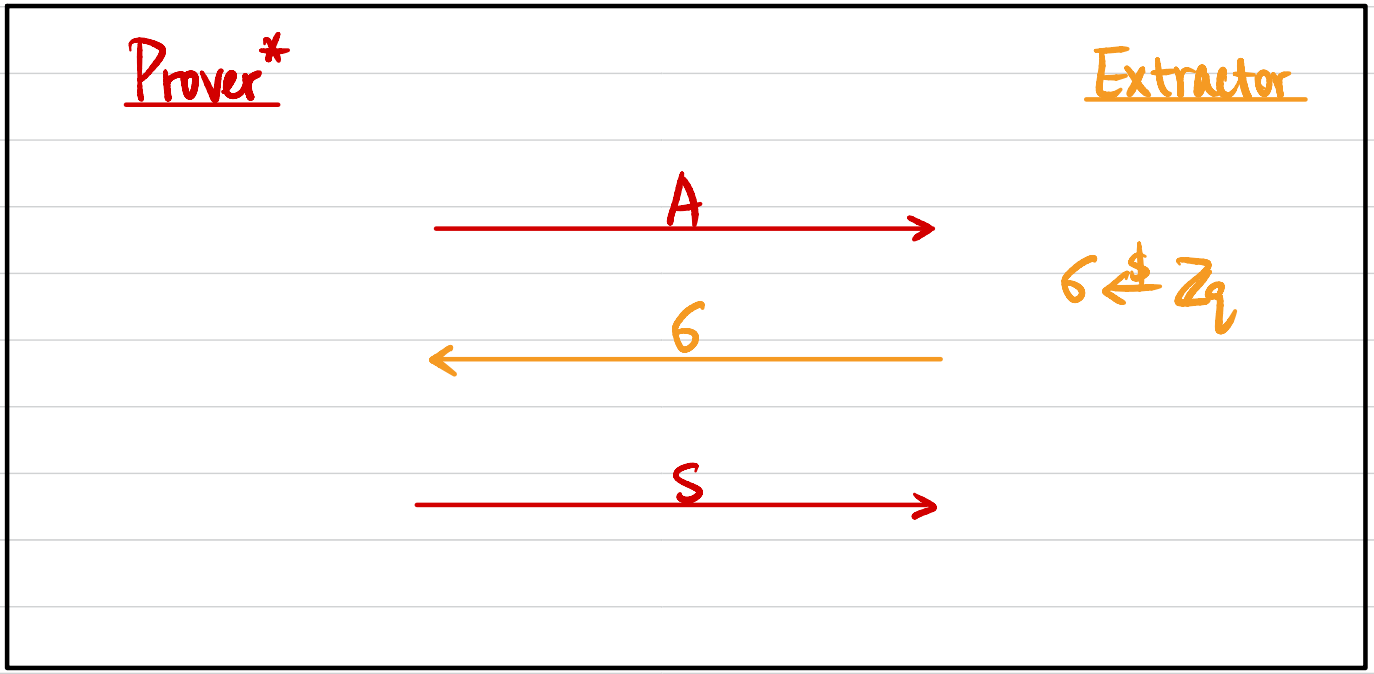
$R_L = \{ (h = g^a, a) \}$



Completness?

Proof of Knowledge?

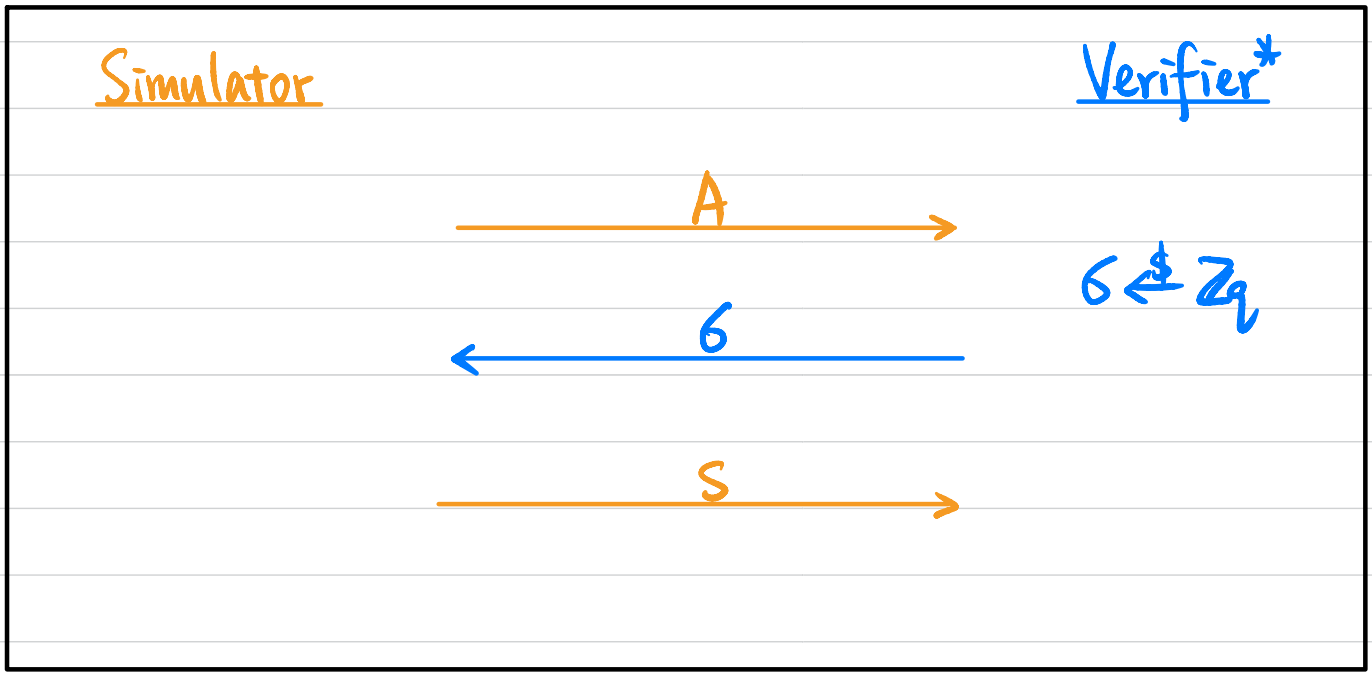
Extract a s.t. $h = g^a$?



Zero-Knowledge?

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

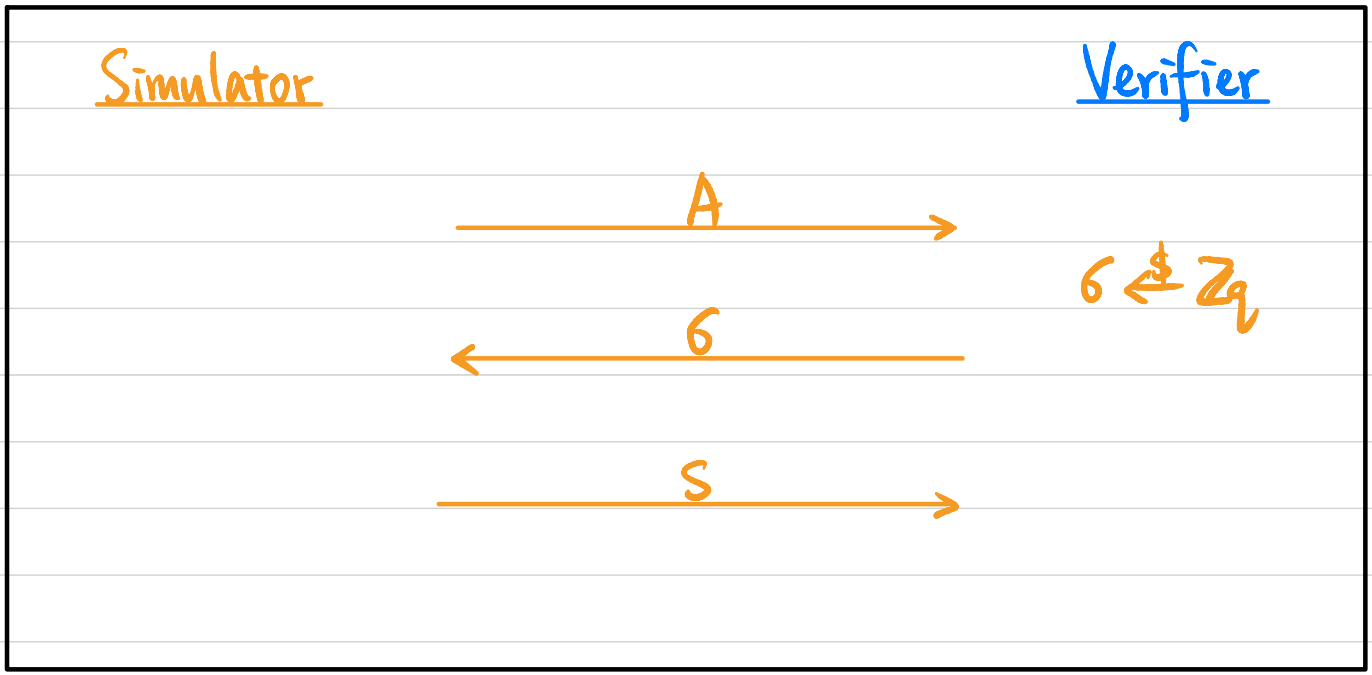
$$\text{Output}_{V^*}[P(x,w) \longleftrightarrow V^*(x)] \simeq S(x)$$



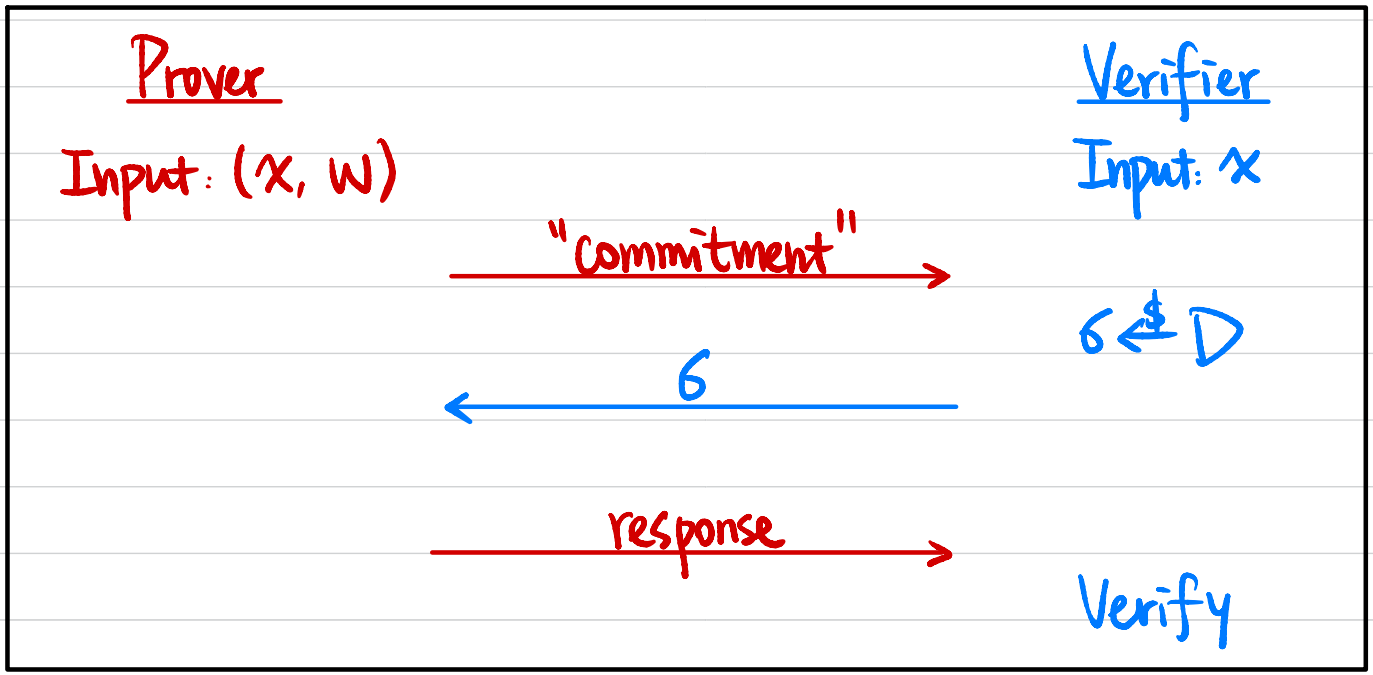
Honest Verifier Zero Knowledge (HVZK)

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

$$View_V[P(x,w) \longleftrightarrow V(x)] \simeq S(x)$$



Sigma Protocols Σ



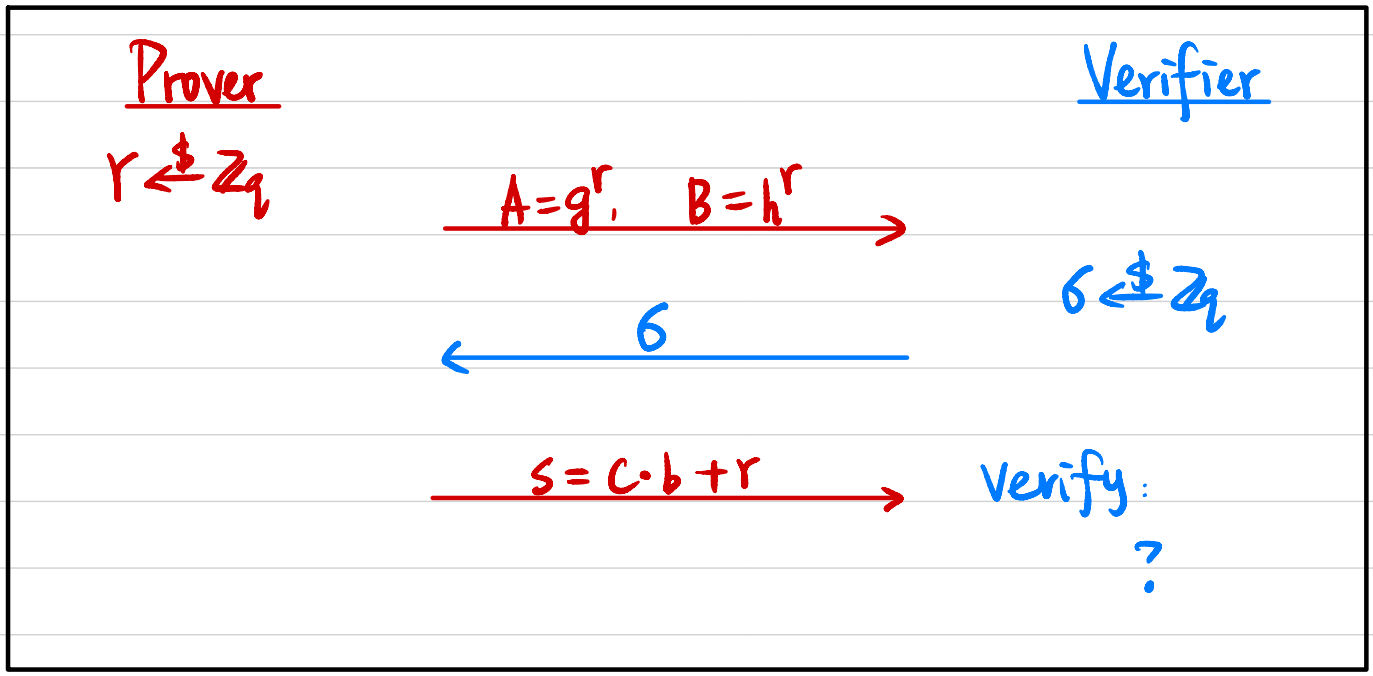
Example: Chaum-Pedersen Protocol for DH Tuple

Input: Cyclic group G of order q, generator g, h, u, v

$h = g^a$, $u = g^b$, $v = g^{ab}$

Witness: b

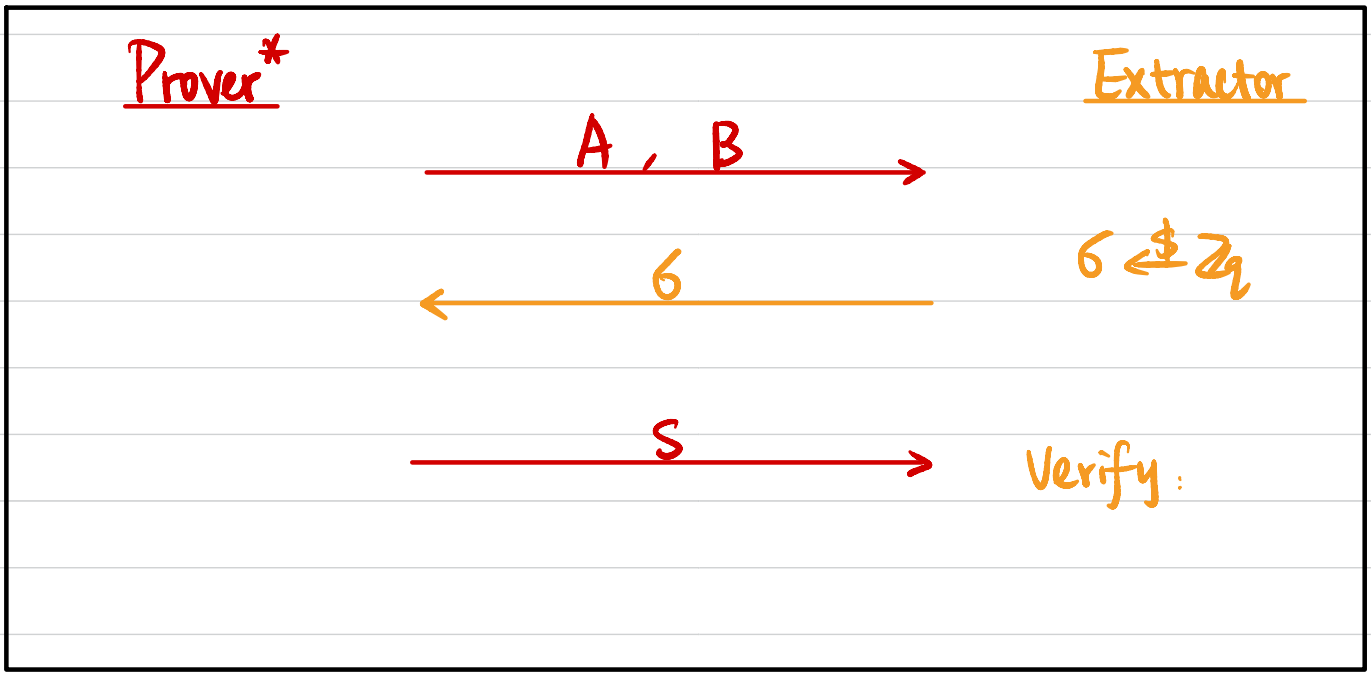
Statement: $\exists\, b \in \mathbb{Z}_q$ s.t. $u = g^b \wedge v = h^b$



Completeness ?

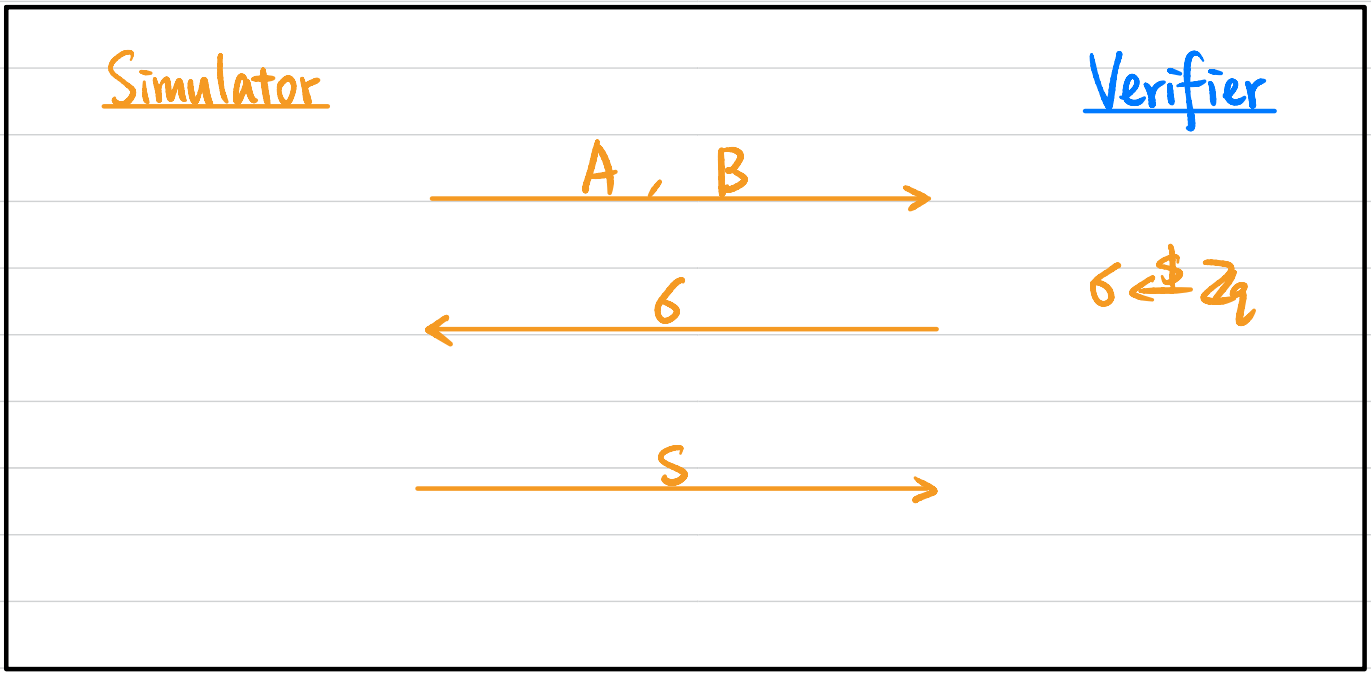
Proof of Knowledge?

Extract b s.t. $u = g^b \wedge v = h^b$?



Honest Verifier Zero Knowledge ?

$\forall (x, w) \in R_L, \quad \text{View}_V[P(x,w) \longleftrightarrow V(x)] \simeq S(x)$

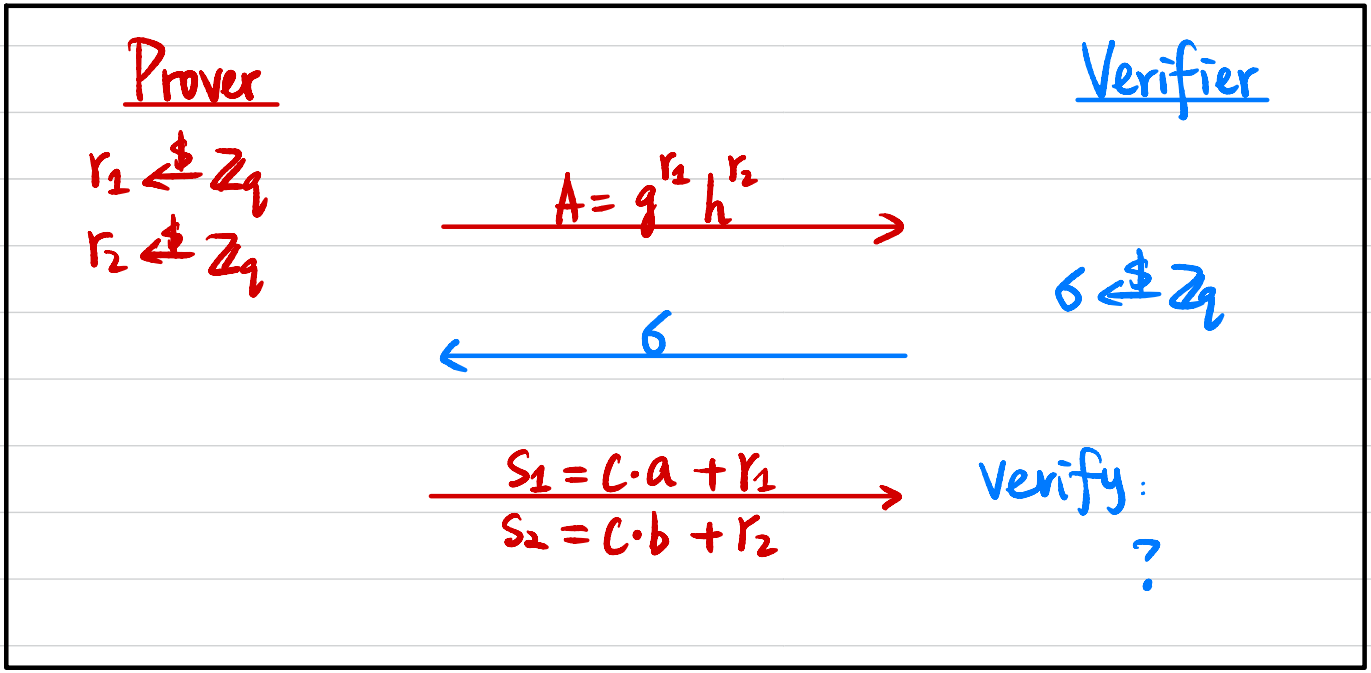


Example: Okamoto's Protocol for Representation

Input: Cyclic group G of order q, generator g, h, $u = g^a h^b$

Witness: (a, b)

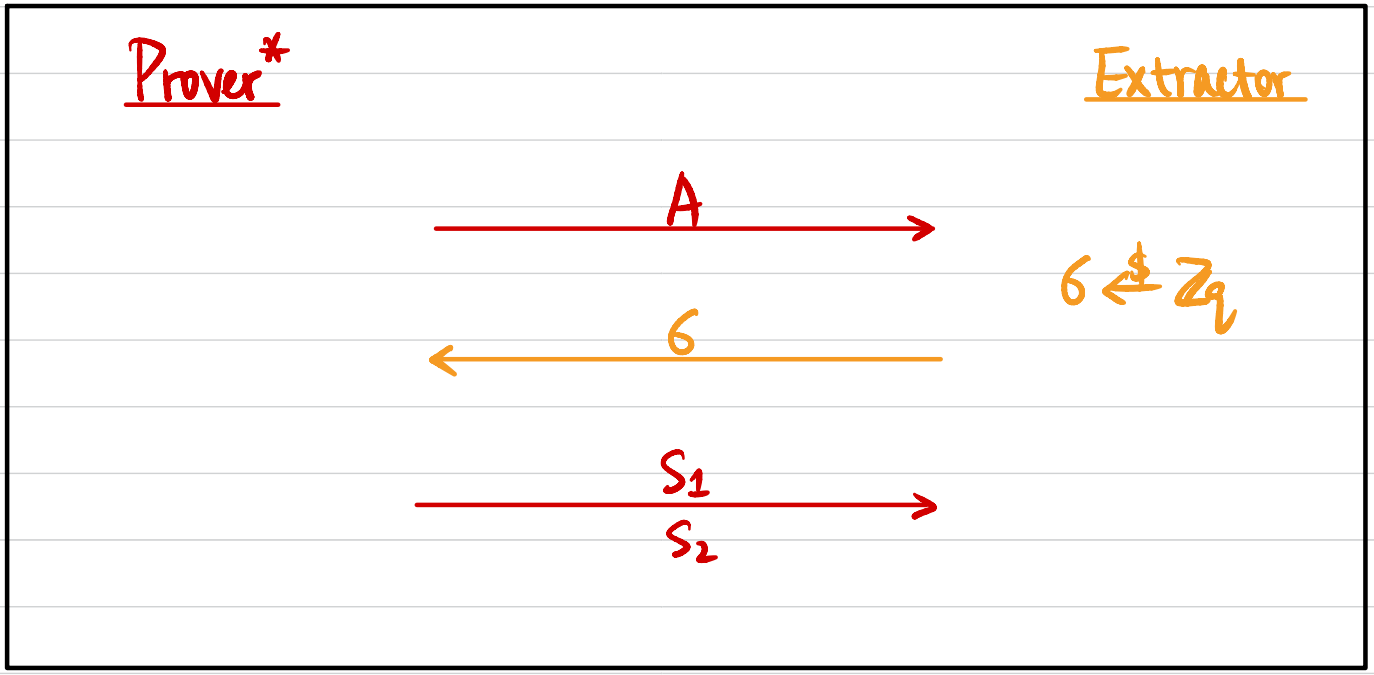
$R_L = \{ (u = g^a h^b, \ (a, b)) \}$



Completeness ?

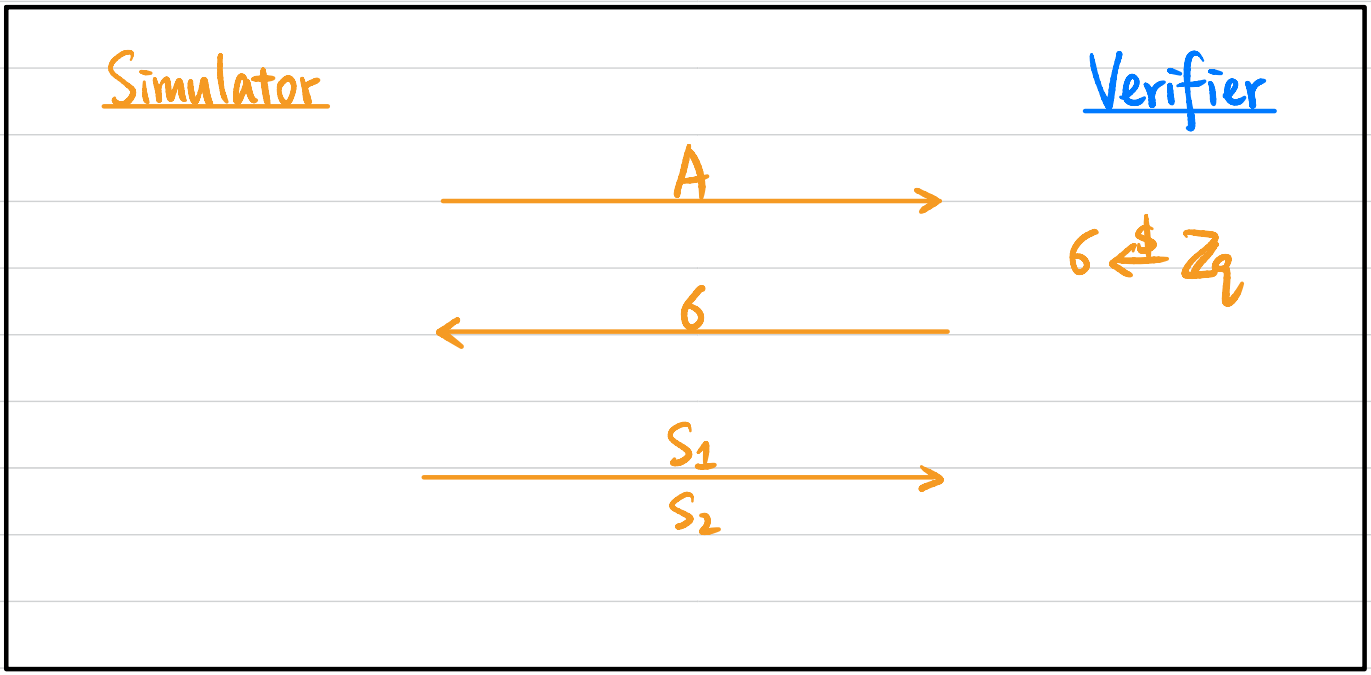
Proof of Knowledge ?

Extract (a,b) s.t. $u = g^a h^b$?



Honest Verifier Zero Knowledge ?

$$\forall (x, w) \in R_L, \quad \text{View}_V[P(x,w) \longleftrightarrow V(x)] \simeq S(x)$$



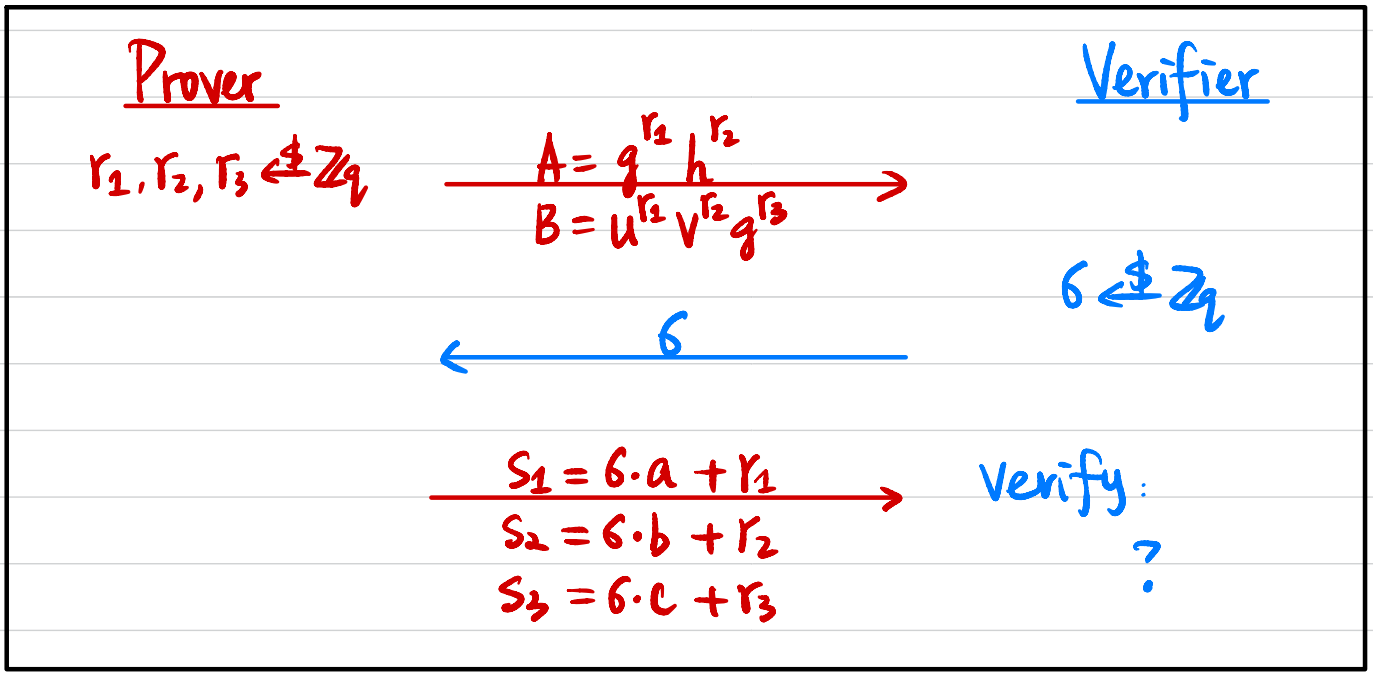
Example: Arbitrary Linear Equations

Input: Cyclic group G of order q, generator g, h, u, v

Witness: (a, b, c)

$u = g^a h^b$

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



Completeness?

PoK?

HVZK?