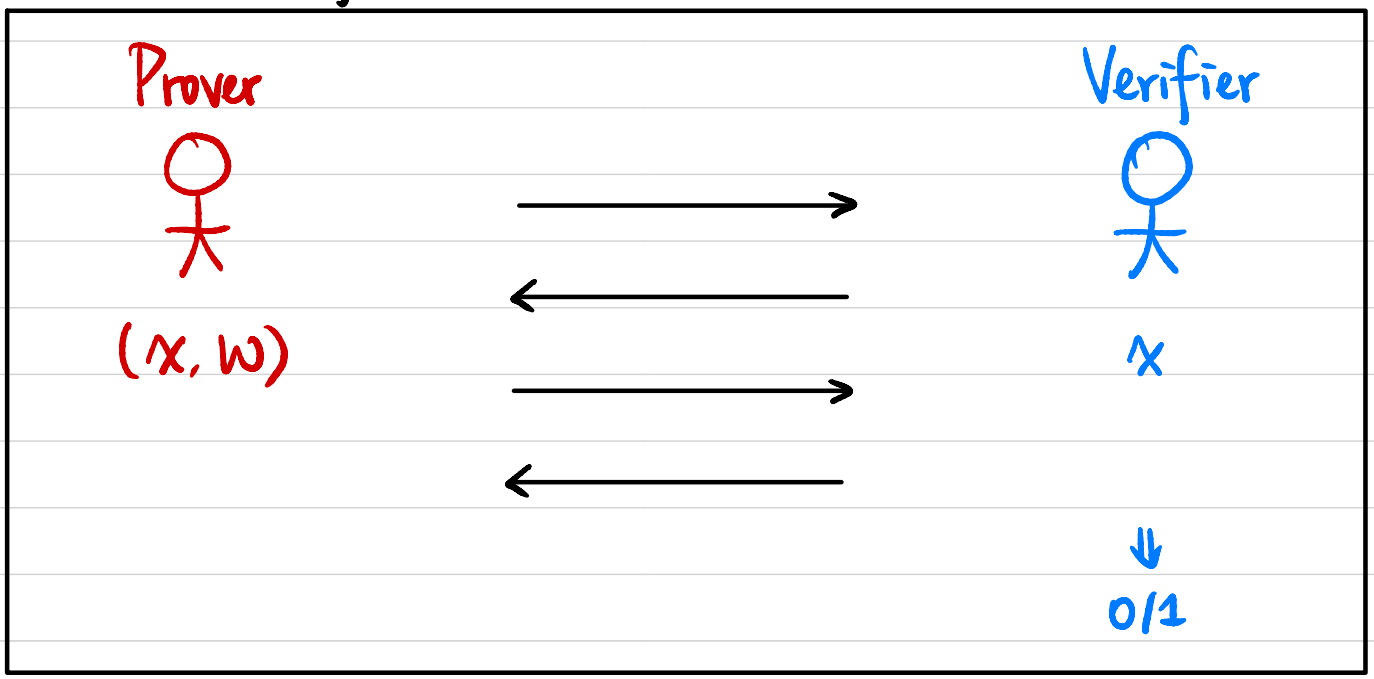
CSCI 1515 Applied Cryptography

This Lecture:

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

Zero-Knowledge Proof (ZKP)



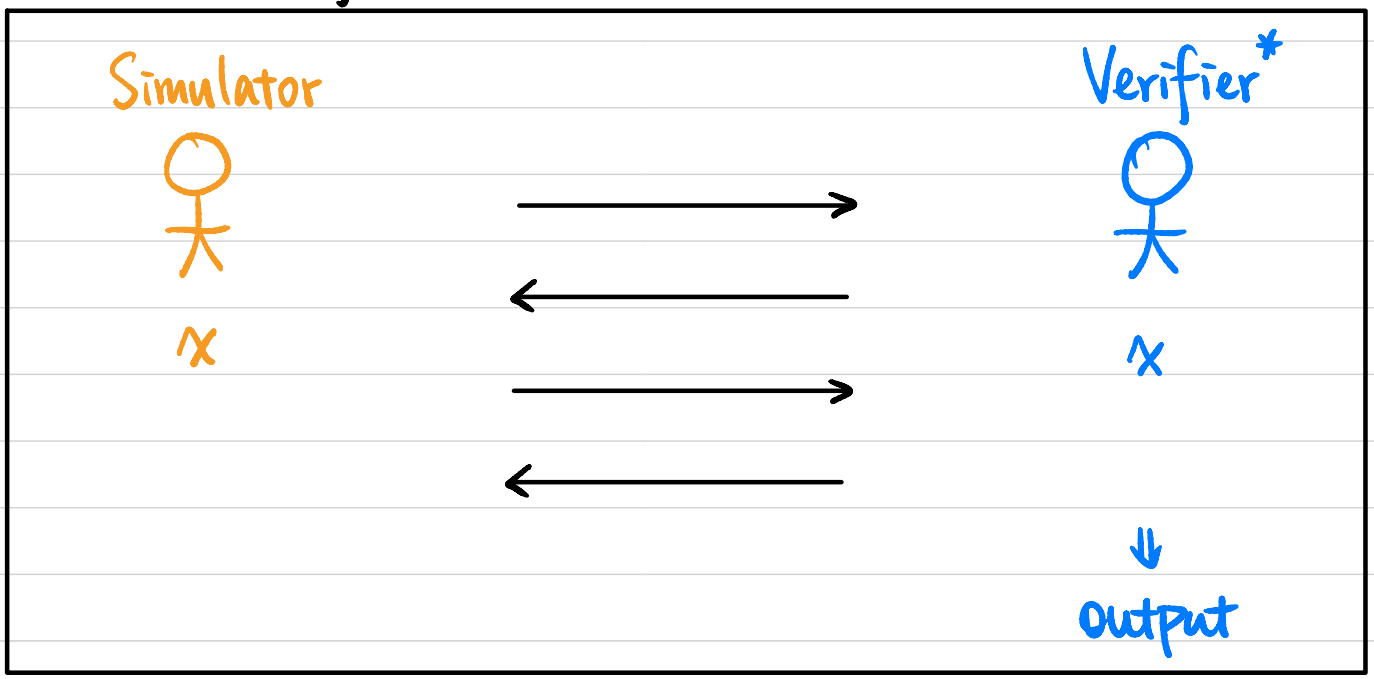
Let (P, V) be a pair of probabilistic poly-time (PPT) interactive machines.

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

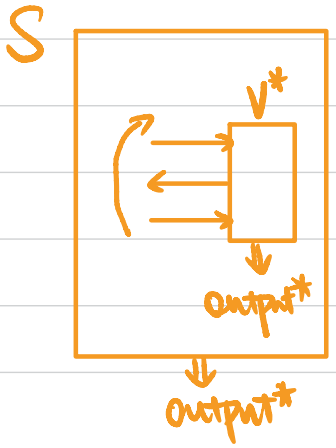
(PPT): argument

Zero-Knowledge Proof (ZKP)



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

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

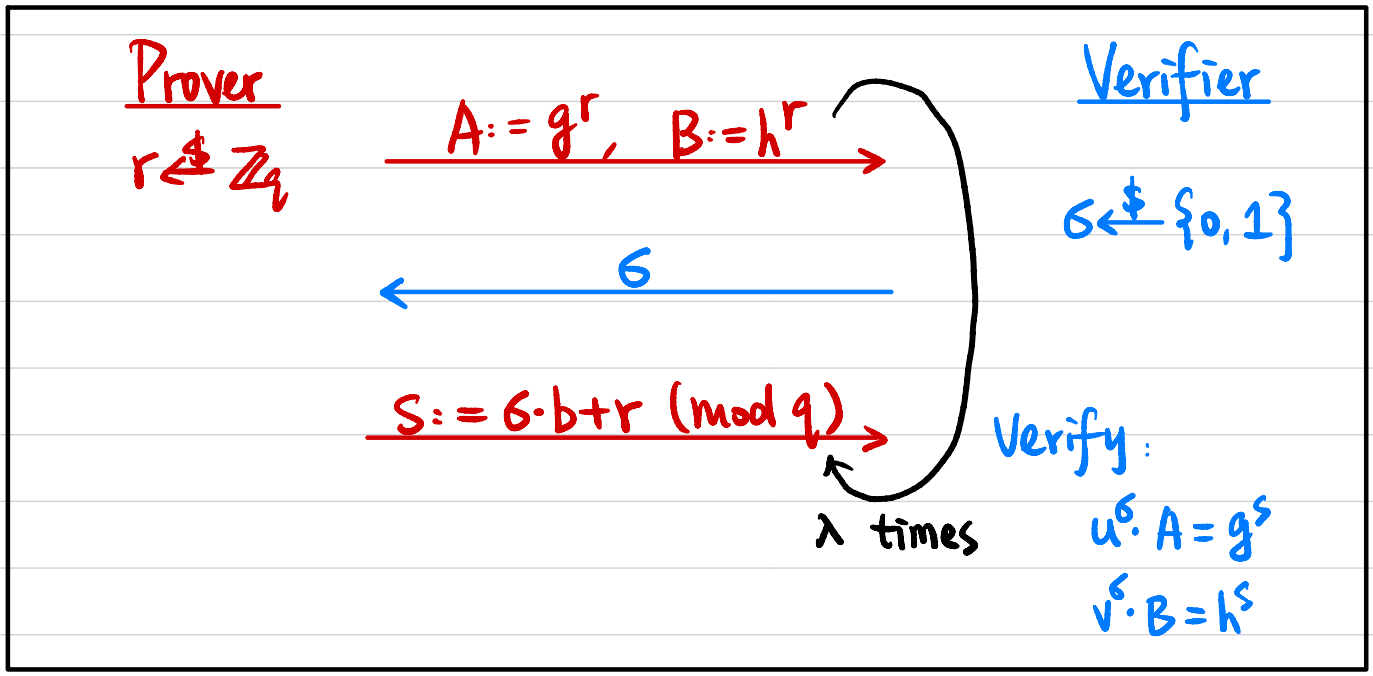


Example: Diffie-Hellman Tuple

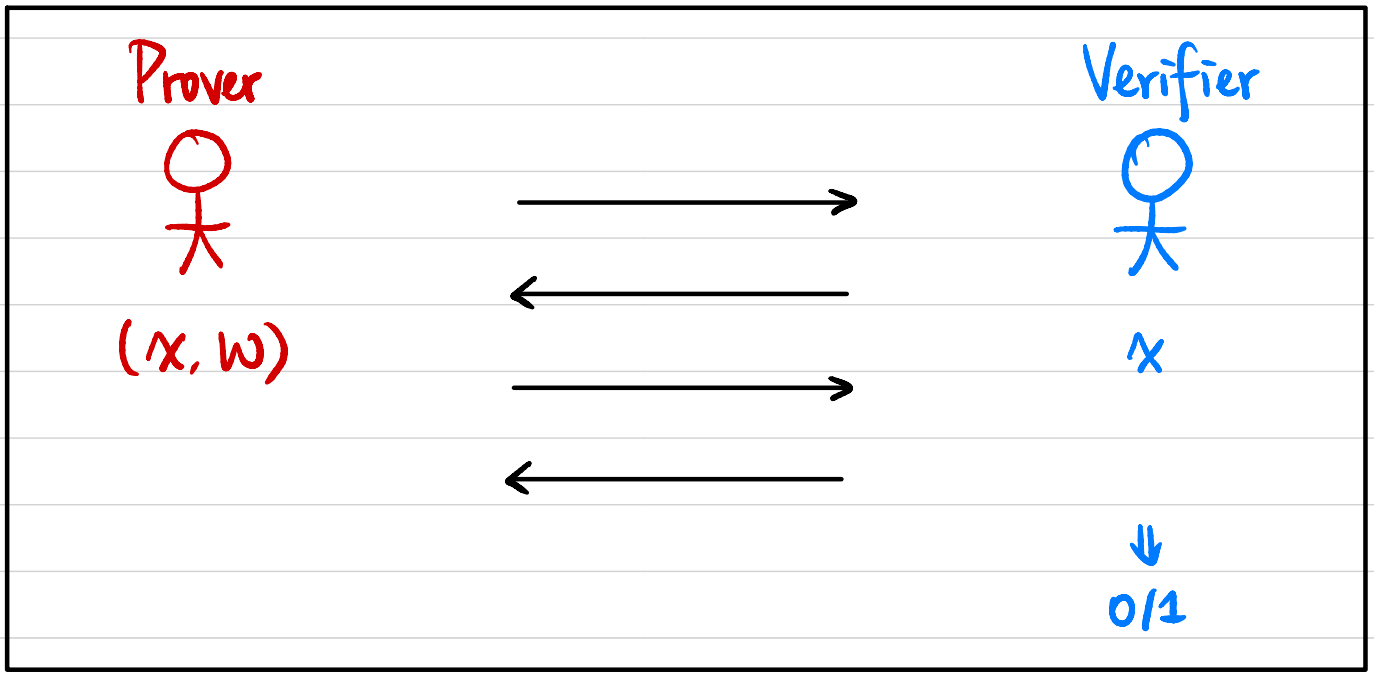
Input: Cyclic group G of order q, generator g, h, u, v
($h = g^a$, $u = g^b$, $v = g^{ab}$)

Witness: b

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



Proof of Knowledge (PoK)



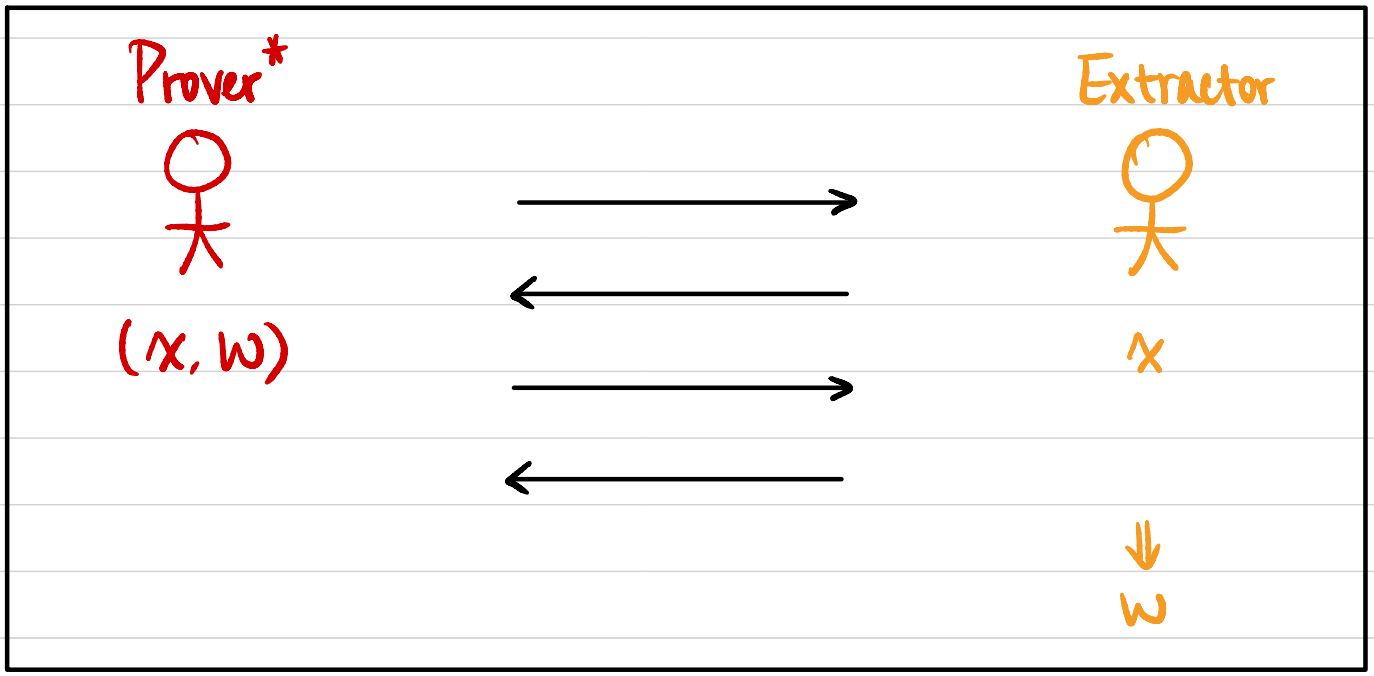
- **Soundness:** $\forall x \notin L$, $\forall$ (PPT) P^*, $Pr[P^*(x) \longleftrightarrow V(x) \text{ outputs } 1] \simeq 0$.

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

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. $\forall (x, w) \in R_L$,

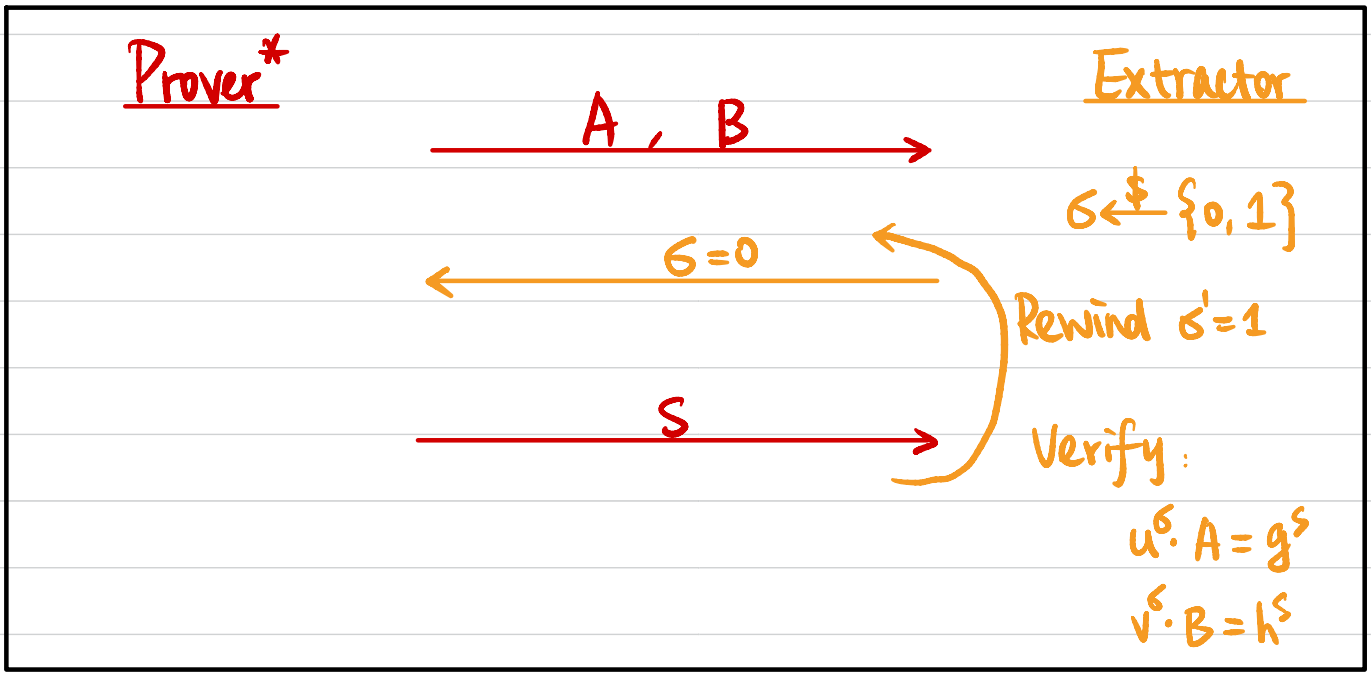
$$\text{Output}_{V^*}[P(x,w) \longleftrightarrow V^*(x)] \simeq S(x)$$

- **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. $u = g^b \wedge v = h^b$?



$\sigma = 0 \Rightarrow s$ s.t. $A = g^s$, $B = h^s$

$\sigma' = 1 \Rightarrow s'$ s.t. $u \cdot A = g^{s'}$, $v \cdot B = h^{s'}$

$\Downarrow$

$u = g^{s-s'}$ $v = h^{s-s'}$

$\Downarrow$

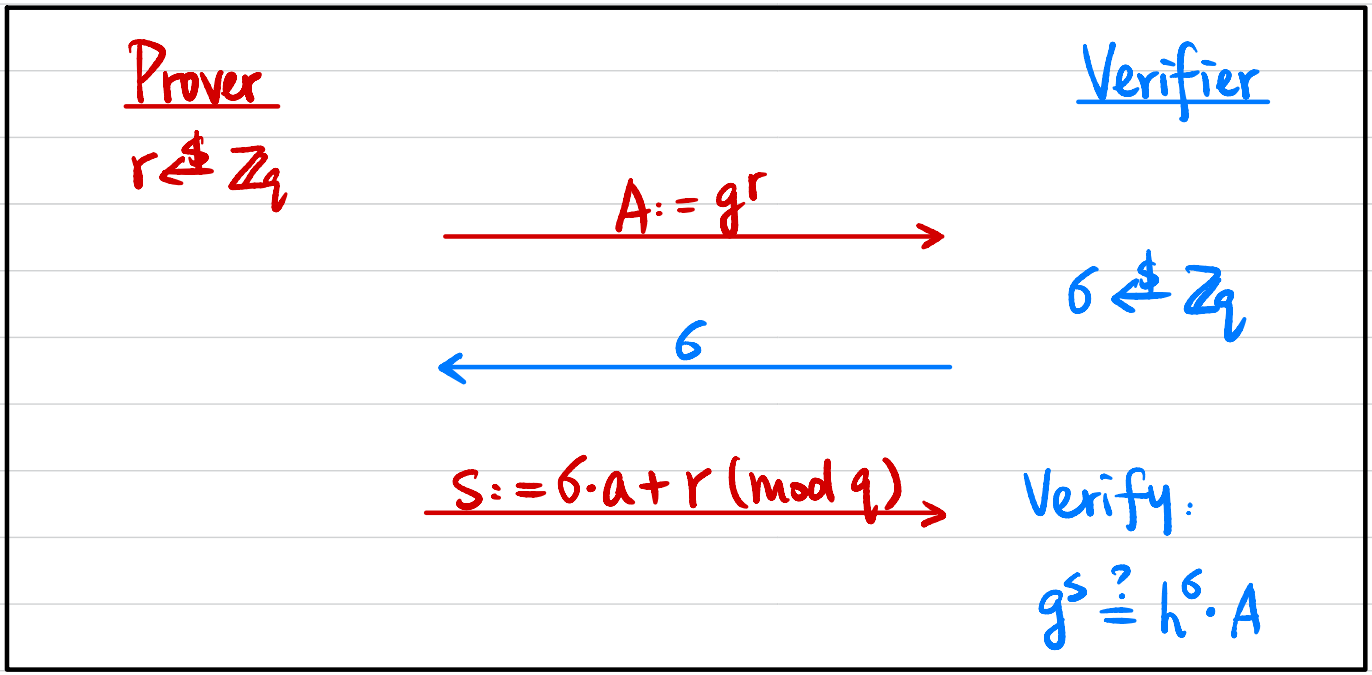
$b = s - s' \pmod q$

Example: Schnorr's Identification Protocol

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

Witness: a

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



Completeness?

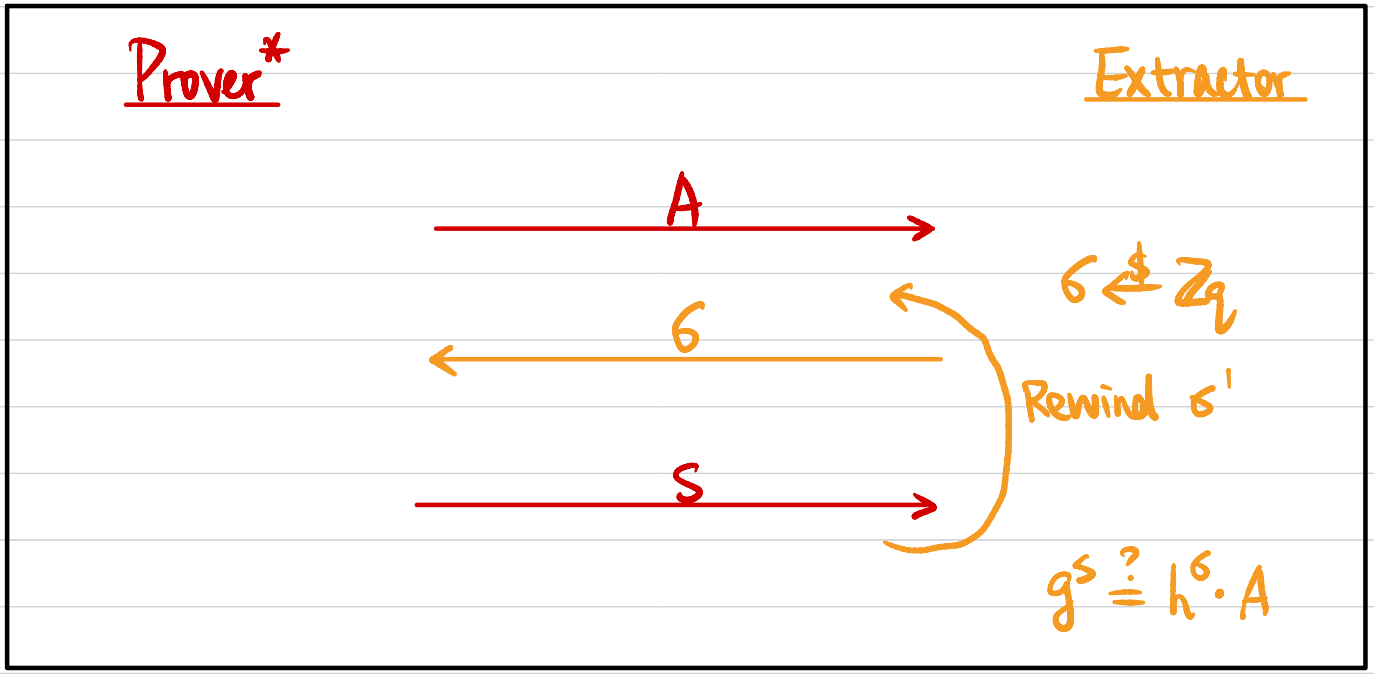
$g^s = g^{\sigma \cdot a + r}$

$h^\sigma \cdot A = (g^a)^\sigma \cdot g^r = g^{\sigma \cdot a + r}$

$\Rightarrow$ Verifier always outputs 1

Proof of Knowledge?

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



$\sigma \Rightarrow s$ s.t. $g^s = h^\sigma \cdot A$

$\sigma' \Rightarrow s'$ s.t. $g^{s'} = h^{\sigma'} \cdot A$

$\Rightarrow g^{s-s'} = h^{\sigma-\sigma'}$

$\Downarrow$

$g^{(s-s')(\sigma-\sigma')^{-1}} = h$

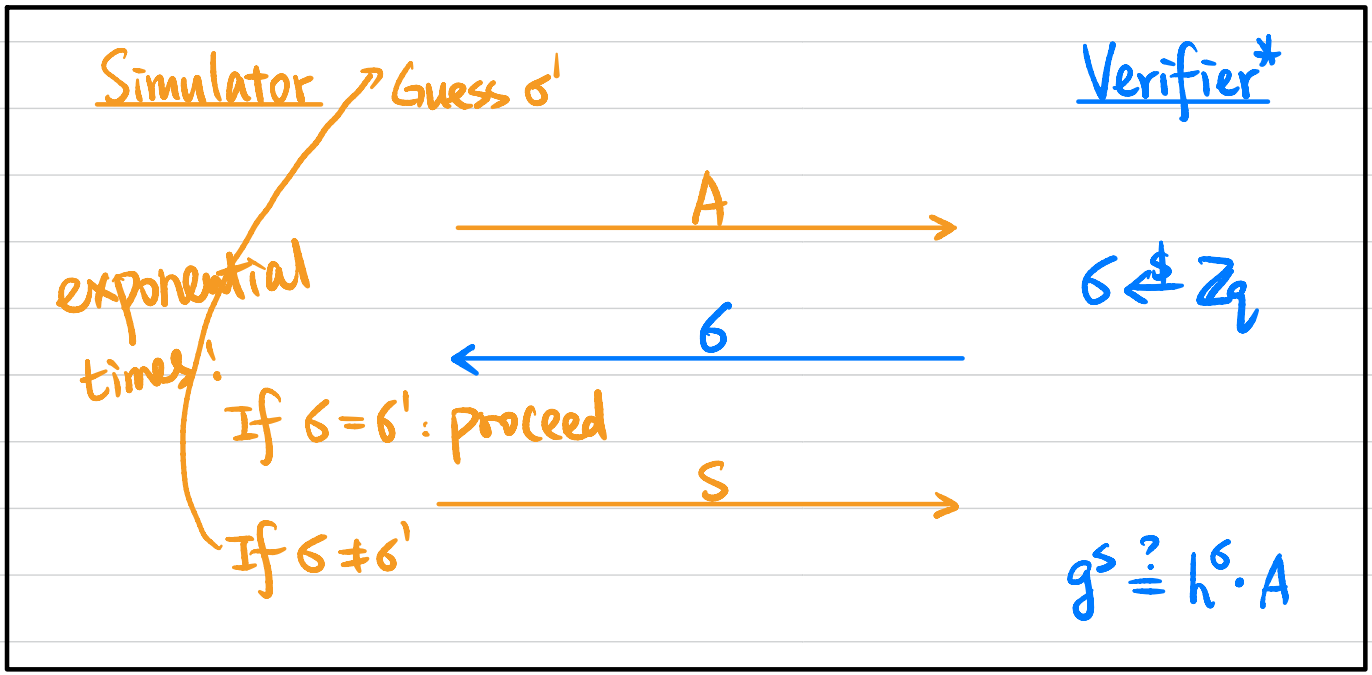
$\Downarrow$

$a = (s-s')(\sigma-\sigma')^{-1} \pmod q$

Zero-Knowledge?

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

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



We know σ'

We want A, s s.t.

$g^s = h^{\sigma'} \cdot A$

$s \xleftarrow{\$} Z_q$ $\quad A = g^s / h^{\sigma'}$

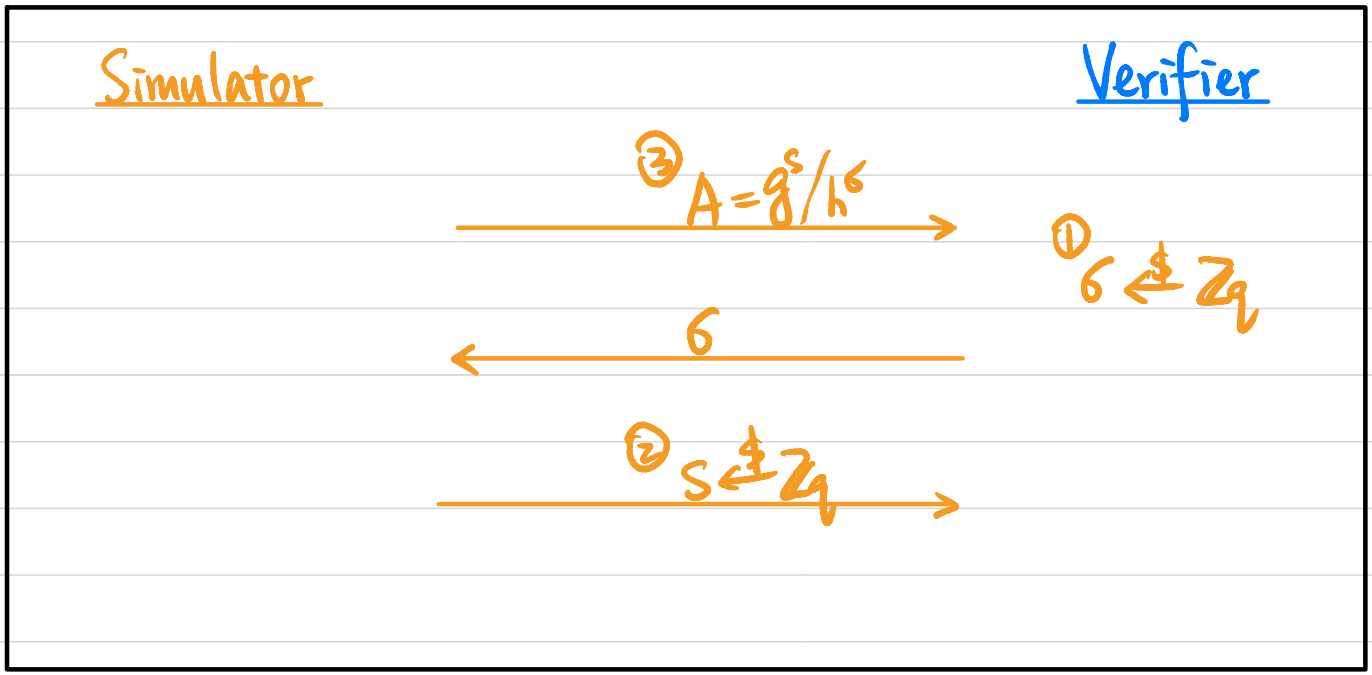
$\Pr[\sigma = \sigma'] = \frac{1}{q}$

↑ negligible

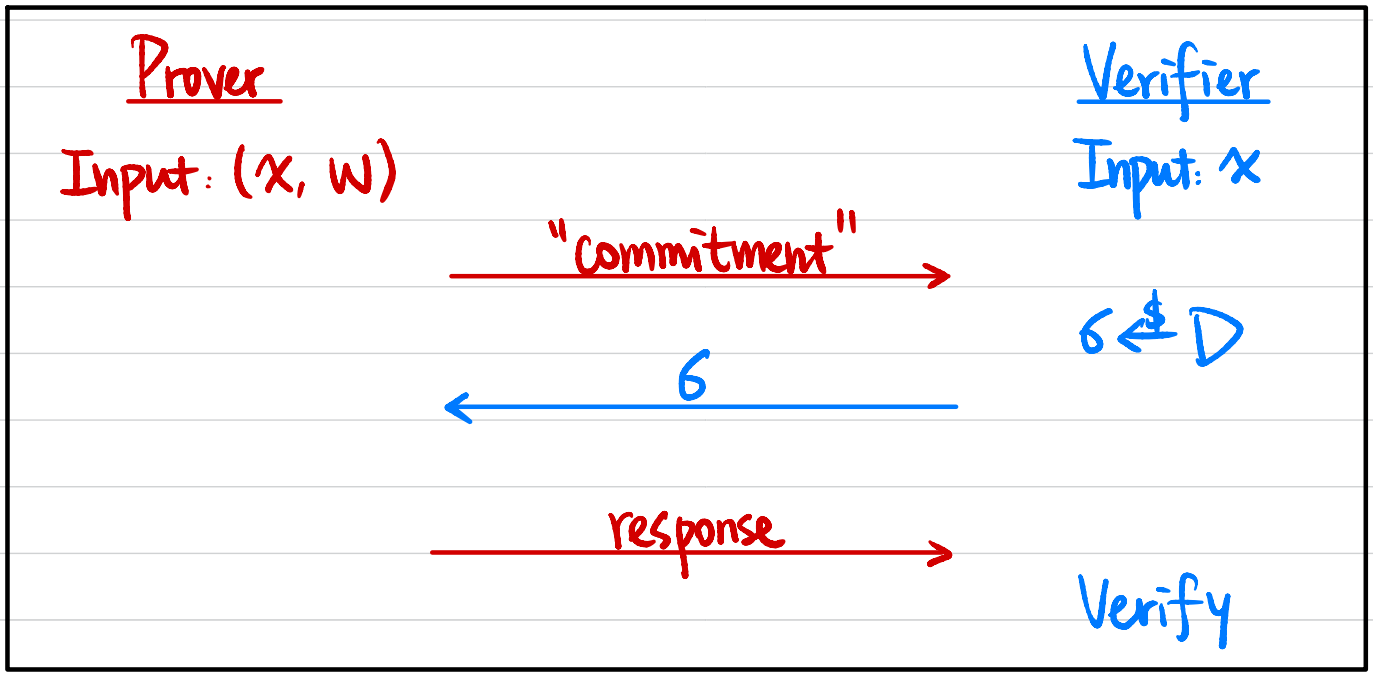
Honest Verifier Zero Knowledge (HVZK)

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

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



Sigma Protocols Σ



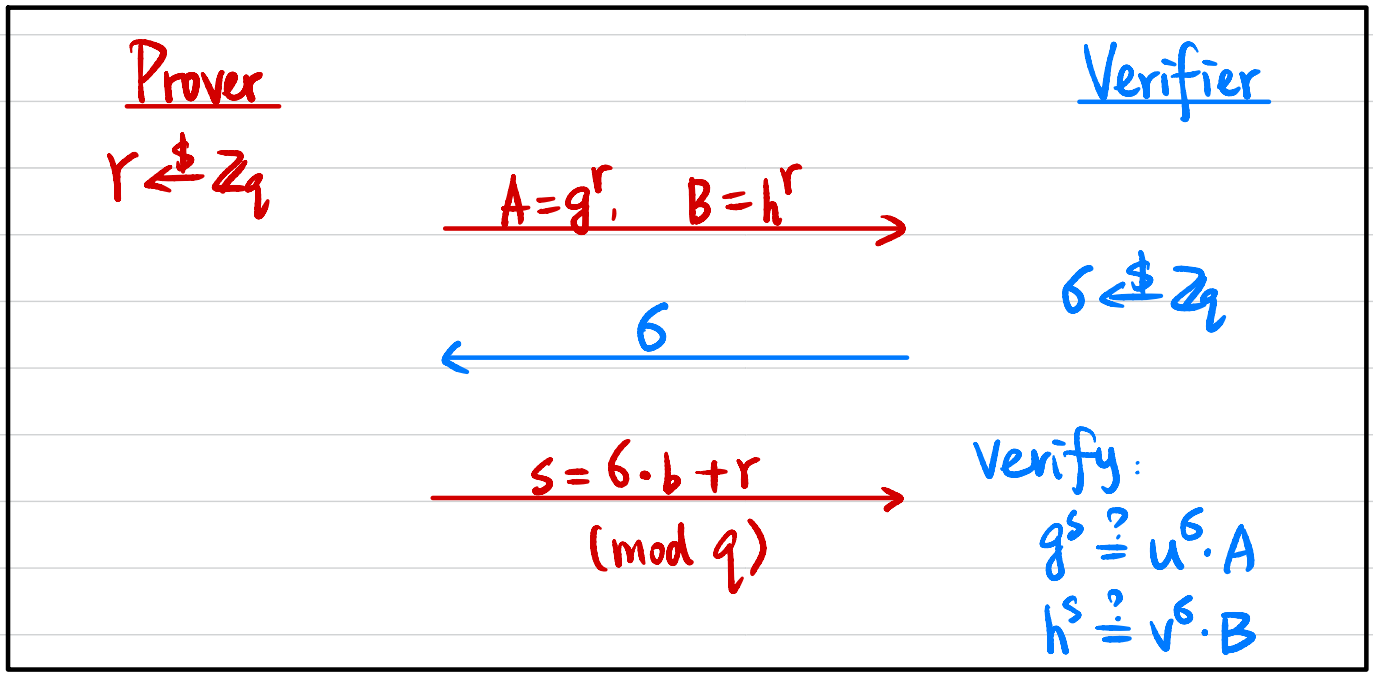
Example: Chaum-Pedersen Protocol for DH Tuple

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 ?

$g^s = g^{\sigma \cdot b + r}$

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

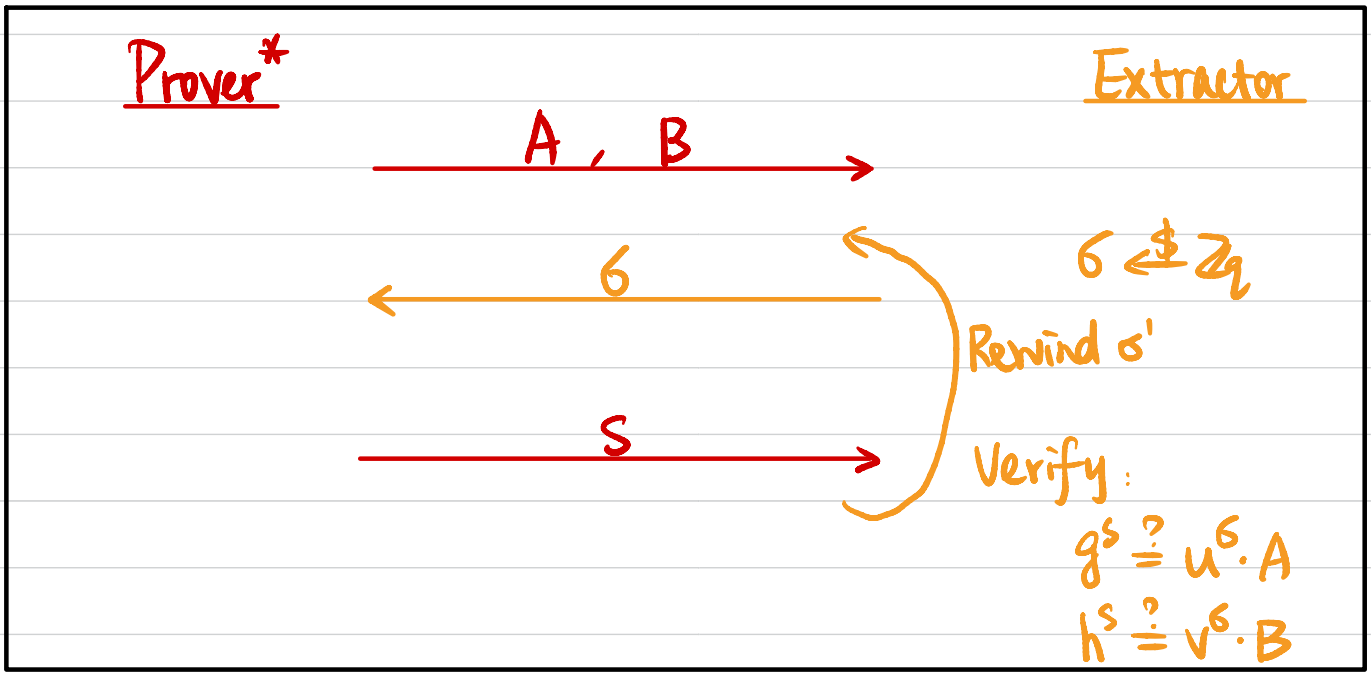
$h^s = h^{\sigma \cdot b + r}$

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

$\Rightarrow$ always output 1

Proof of Knowledge?

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



$\sigma \Rightarrow s$ s.t. $g^s = u^\sigma \cdot A$, $h^s = v^\sigma \cdot B$

$\sigma' \Rightarrow s'$ s.t. $g^{s'} = u^{\sigma'} \cdot A$, $h^{s'} = v^{\sigma'} \cdot B$

$\Downarrow$

$g^{s-s'} = u^{\sigma-\sigma'}$, $h^{s-s'} = v^{\sigma-\sigma'}$

$\Downarrow$

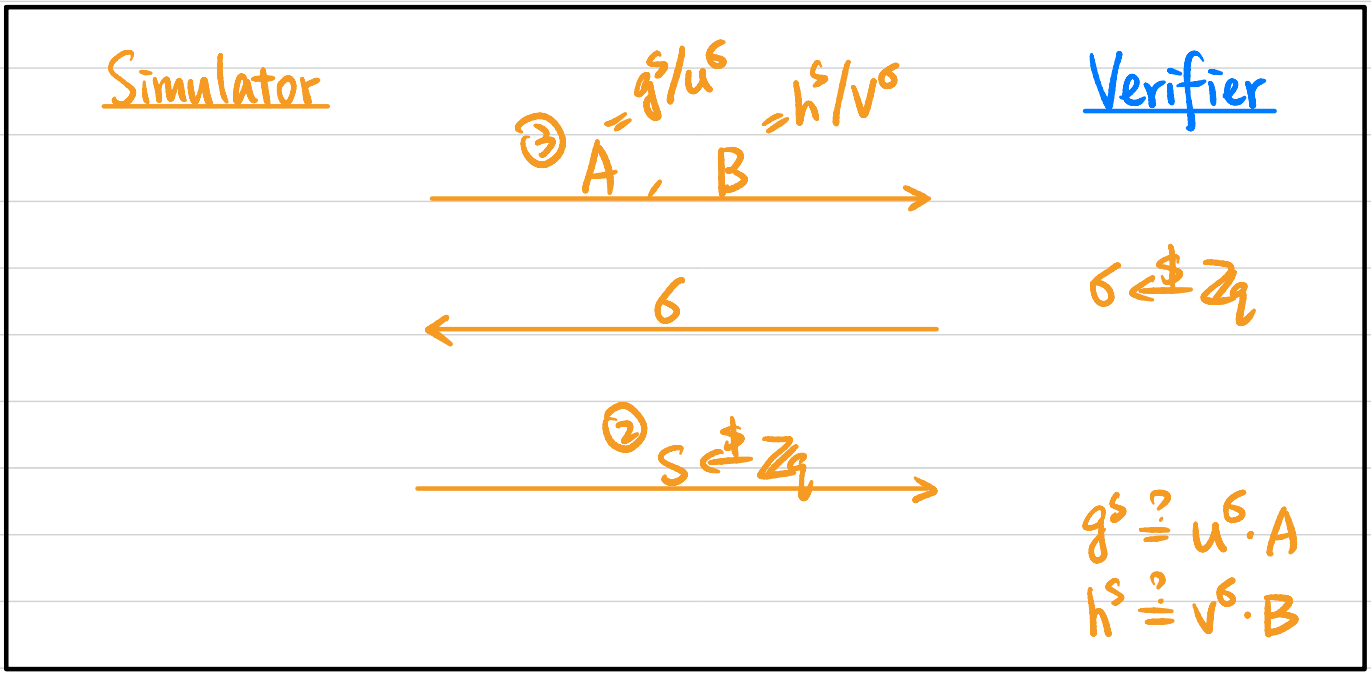
$g^{(s-s')(\sigma-\sigma')^{-1}} = u$, $h^{(s-s')(\sigma-\sigma')^{-1}} = v$

$\Downarrow$

$b = (s-s')(\sigma-\sigma')^{-1} \pmod q$

Honest Verifier Zero Knowledge ?

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

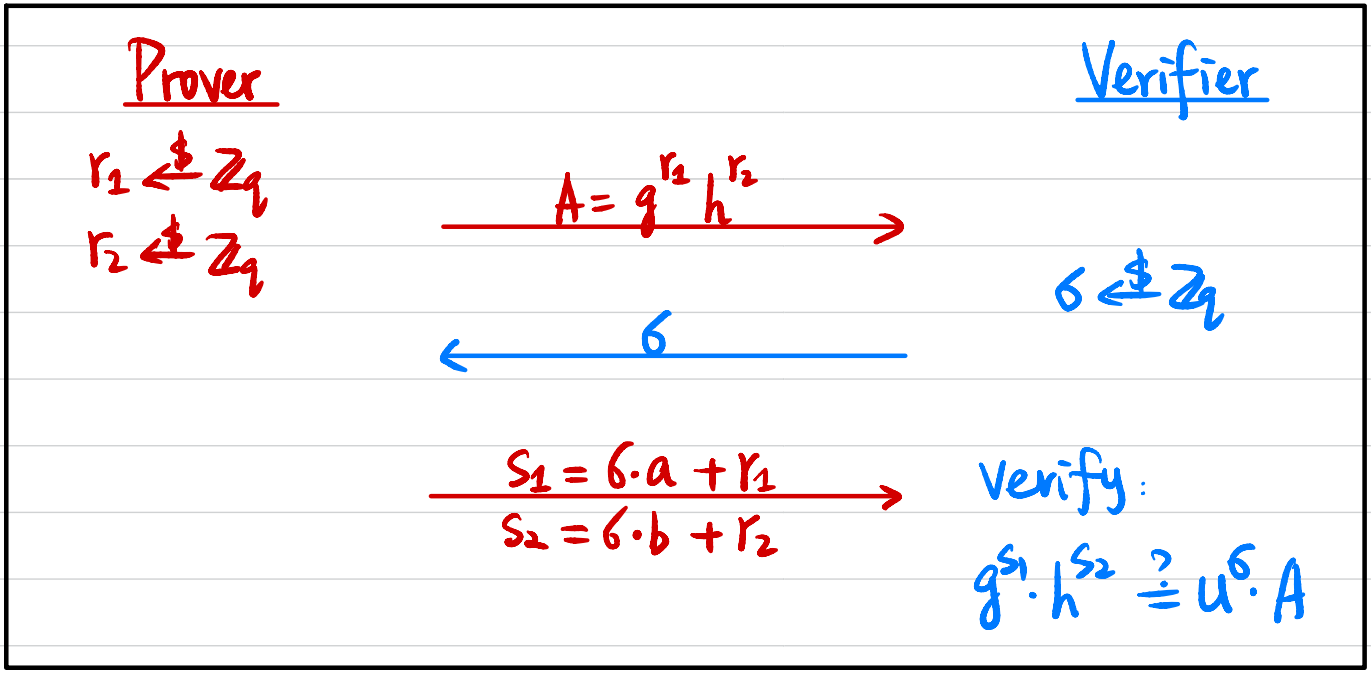


Example: Okamoto's Protocol for Representation

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 ?

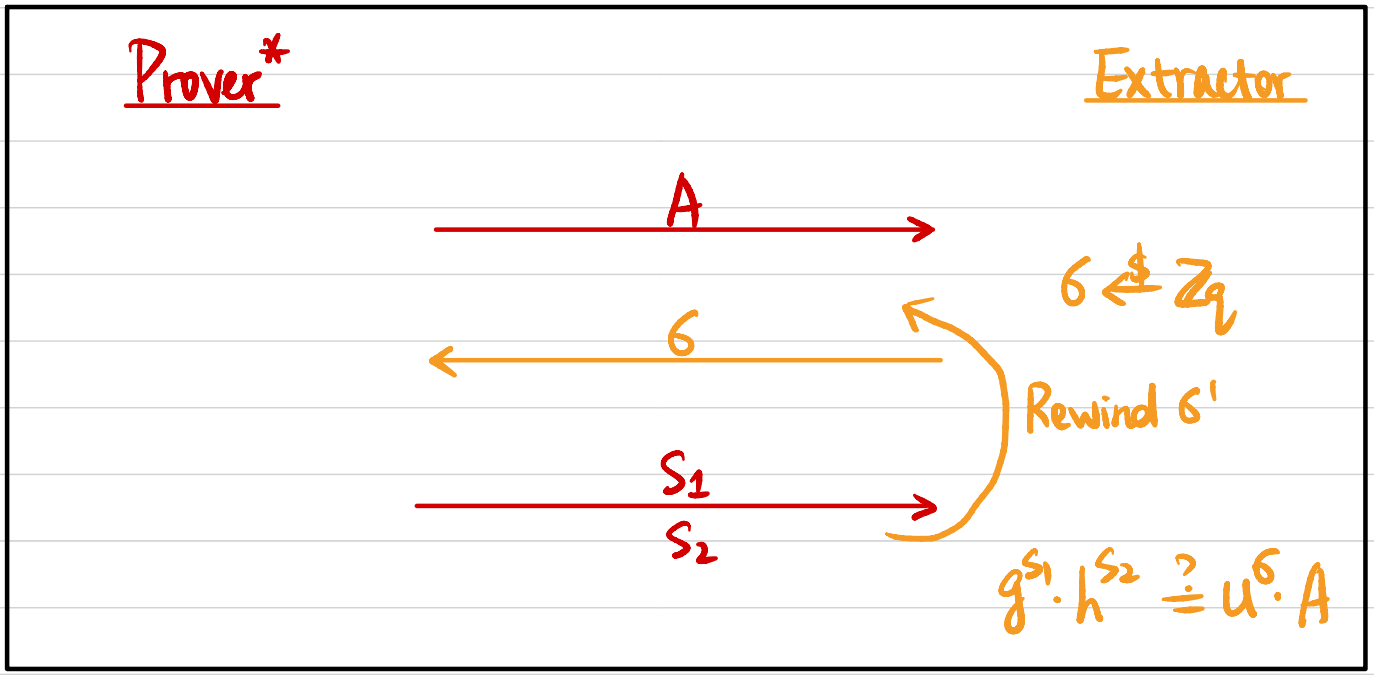
$g^{s_1} \cdot h^{s_2} = g^{\sigma \cdot a + r_1} \cdot h^{\sigma \cdot b + r_2}$

$u^{\sigma} \cdot A = (g^a h^b)^{\sigma} \cdot g^{r_1} h^{r_2} = g^{\sigma a + r_1} \cdot h^{\sigma b + r_2}$

$\Rightarrow$ always output 1

Proof of Knowledge ?

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



$\sigma \Rightarrow s_1, s_2$ s.t. $g^{s_1} \cdot h^{s_2} = u^{\sigma} \cdot A$

$\sigma' \Rightarrow s_1', s_2'$ s.t. $g^{s_1'} \cdot h^{s_2'} = u^{\sigma'} \cdot A$

$\Downarrow$

$$g^{s_1 - s_1'} \cdot h^{s_2 - s_2'} = u^{\sigma - \sigma'}$$

$\Downarrow$

$$g^{(s_1 - s_1')(\sigma - \sigma')^{-1}} \cdot h^{(s_2 - s_2')(\sigma - \sigma')^{-1}} = u$$

$\Downarrow$

$$a = (s_1 - s_1')(\sigma - \sigma')^{-1}, \quad b = (s_2 - s_2')(\sigma - \sigma')^{-1} \pmod q$$

Honest Verifier Zero Knowledge ?

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