CSCI 1515 Applied Cryptography

This Lecture:

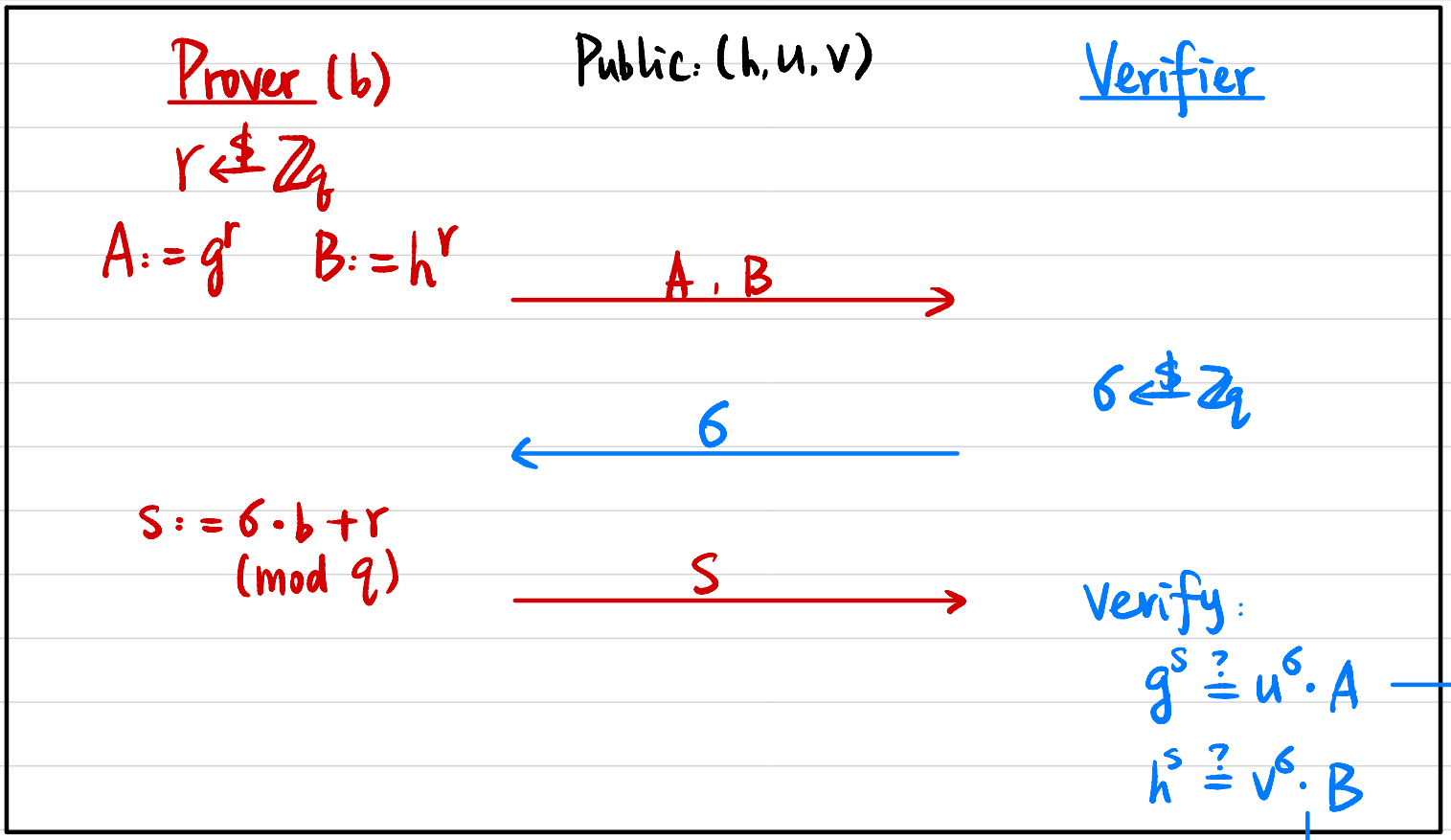
- Example: Diffie-Hellman Tuple
- Non-Interactive Zero-Knowledge (NIZK) Proof
- Fiat-Shamir Heuristic
- Anonymous Online Voting: More Details
- Homomorphism of ElGamal Encryption
- ZKP for OR Statements

Example: Diffie-Hellman Tuple

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

Prover's secret witness: b s.t. $u = g^b \wedge v = h^b$

$R_L = \{ ((h,u,v), b) \}$



Completeness? $\forall (x,w) \in R_L \quad \Pr[\, P(x,w) \longleftrightarrow V(x) \text{ outputs } 1 \,] = 1$

Zero-Knowledge Proof of Knowledge

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

  $\forall (x,w) \in R_L$, P can prove it.

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

  If P^* can prove it, $x \in L$.

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

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

  If P^* can prove it, P^* must know w.

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

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

  An honest V doesn't learn anything about w.

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

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

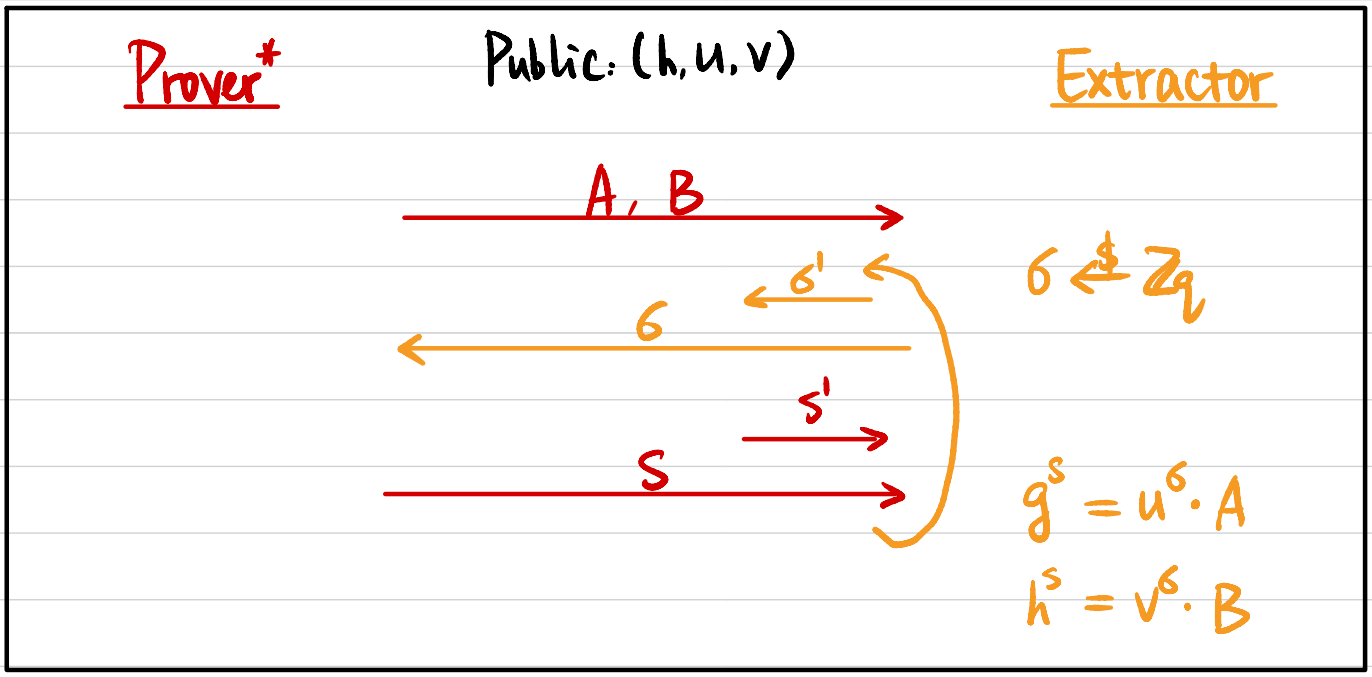
  A malicious V^* doesn't learn anything about w.

Example: Diffie-Hellman Tuple

Proof of Knowledge?

$\exists$ PPT E s.t. $\forall P^*$, $\forall x$,

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



How to extract b s.t. $u = g^b \wedge v = h^b$?

$$\frac{g^s}{g^{s'}} = \frac{u^\sigma \cdot A}{u^{\sigma'} \cdot A} \Rightarrow \left(g^{s-s'}\right)^{(\sigma-\sigma')^{-1}} = \left(u^{\sigma-\sigma'}\right)^{(\sigma-\sigma')^{-1}} \Rightarrow g^{(s-s')\cdot(\sigma-\sigma')^{-1}} = u$$

$$\Rightarrow b = (s-s')\cdot(\sigma-\sigma')^{-1} \bmod q$$

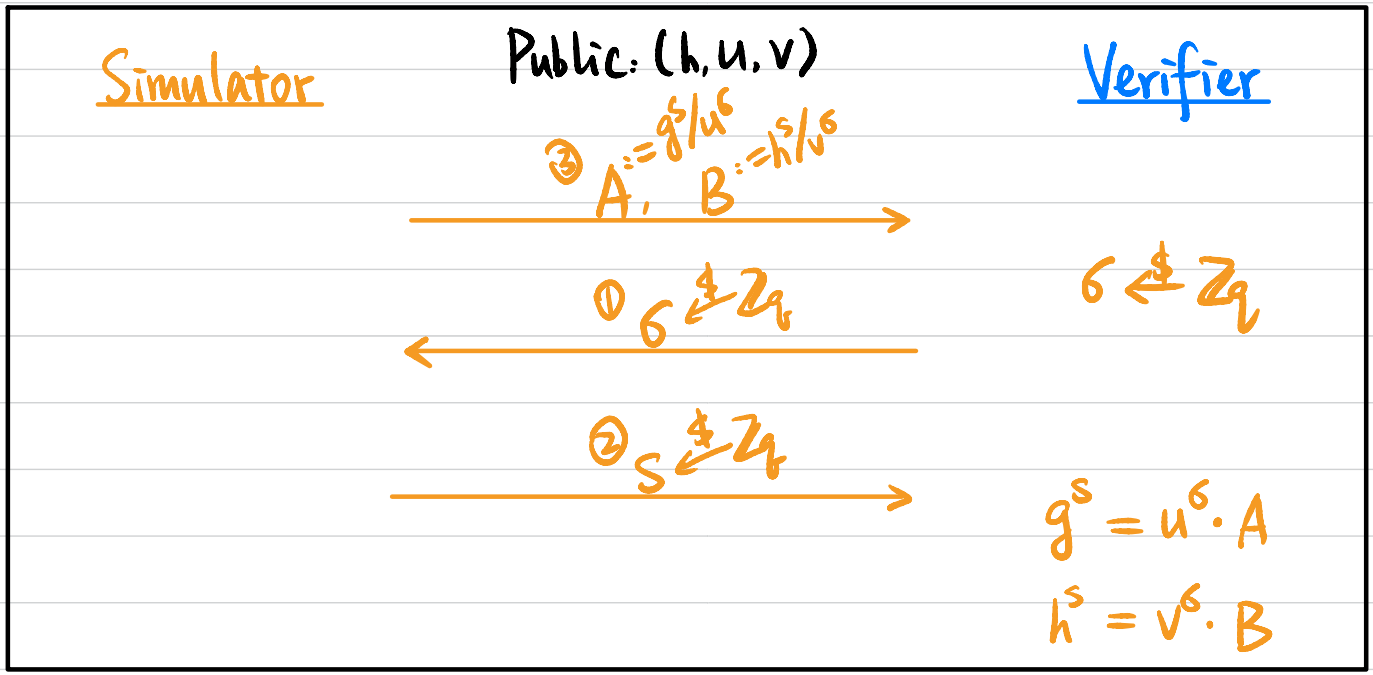
$$\frac{h^s}{h^{s'}} = \frac{v^\sigma \cdot B}{v^{\sigma'} \cdot B} \Rightarrow \left(h^{s-s'}\right)^{(\sigma-\sigma')^{-1}} = \left(v^{\sigma-\sigma'}\right)^{(\sigma-\sigma')^{-1}} \Rightarrow h^{(s-s')\cdot(\sigma-\sigma')^{-1}} = v$$

Example: Diffie-Hellman Tuple

Honest-Verifier Zero-Knowledge (HVZK)?

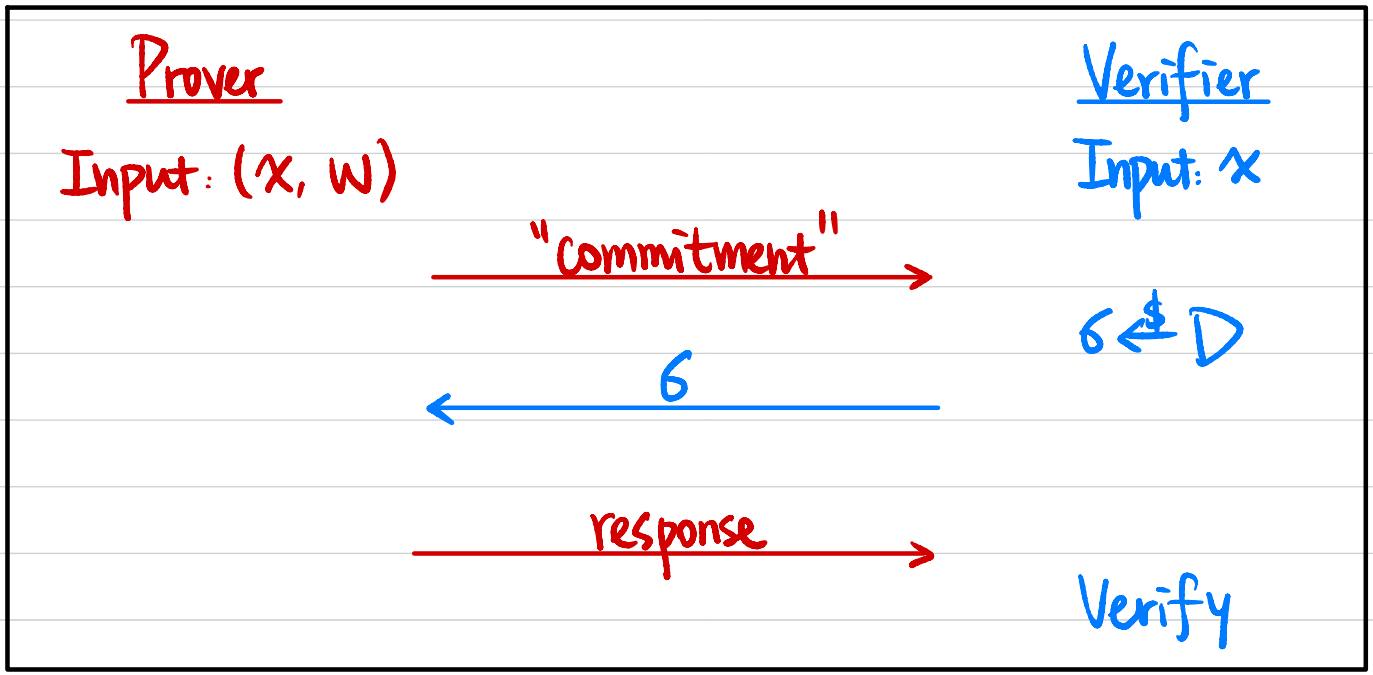
$\exists$ PPT S s.t. $\forall (x, w) \in R_L$,

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

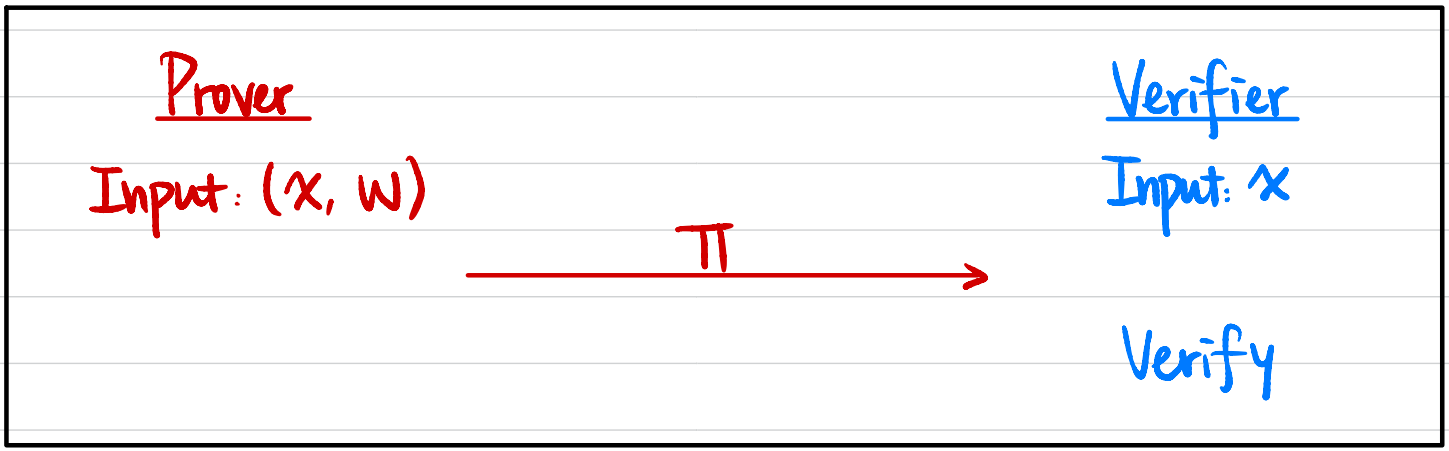


How to generate (A, B, s) s.t. $g^s = u^\sigma \cdot A \wedge h^s = v^\sigma \cdot B$?

Sigma Protocols Σ



Non-Interactive Zero-Knowledge (NIZK) Proof



- **Completeness:** $\forall (x,w) \in R_L, \quad Pr[\, P(x,w) \longrightarrow V(x) \text{ outputs } 1\,] = 1.$
- **Soundness:** $\forall x \notin L, \ \forall P^*, \quad Pr[\, P^*(x) \longrightarrow V(x) \text{ outputs } 1\,] \simeq 0.$
- **Zero-Knowledge:** $\forall PPT\ V^*, \ \exists PPT\ S \quad s.t. \quad \forall (x,w) \in R_L,$

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

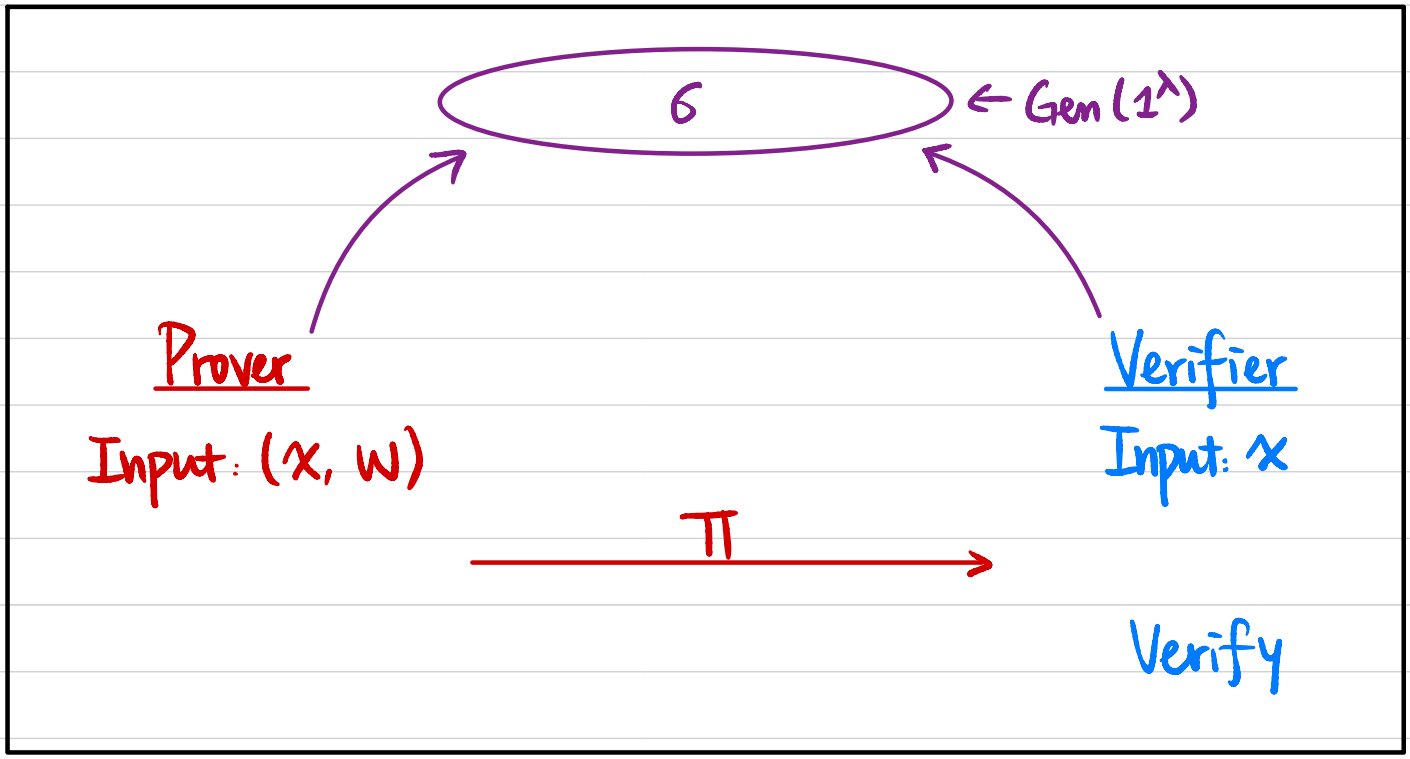
Is it possible? NOT in the "plain" model

Example: Diffie-Hellman Tuple (h,u,v)

If (h,u,v) is a DH tuple, then $S(h,u,v)$ outputs → valid pmf → V outputs 1 ⇒ Break DDH

If (h,u,v) is not a DH tuple, then $S(h,u,v)$ outputs → invalid pmf → V outputs 0

Model 1: Common Random String / Common Reference String (CRS)



- **Soundness:** $\forall x \notin L,\ \forall P^*,\ Pr[\sigma \leftarrow Gen(1^\lambda),\ P^*(\sigma, x) \longrightarrow V(\sigma, x) \text{ outputs } 1] \simeq 0.$

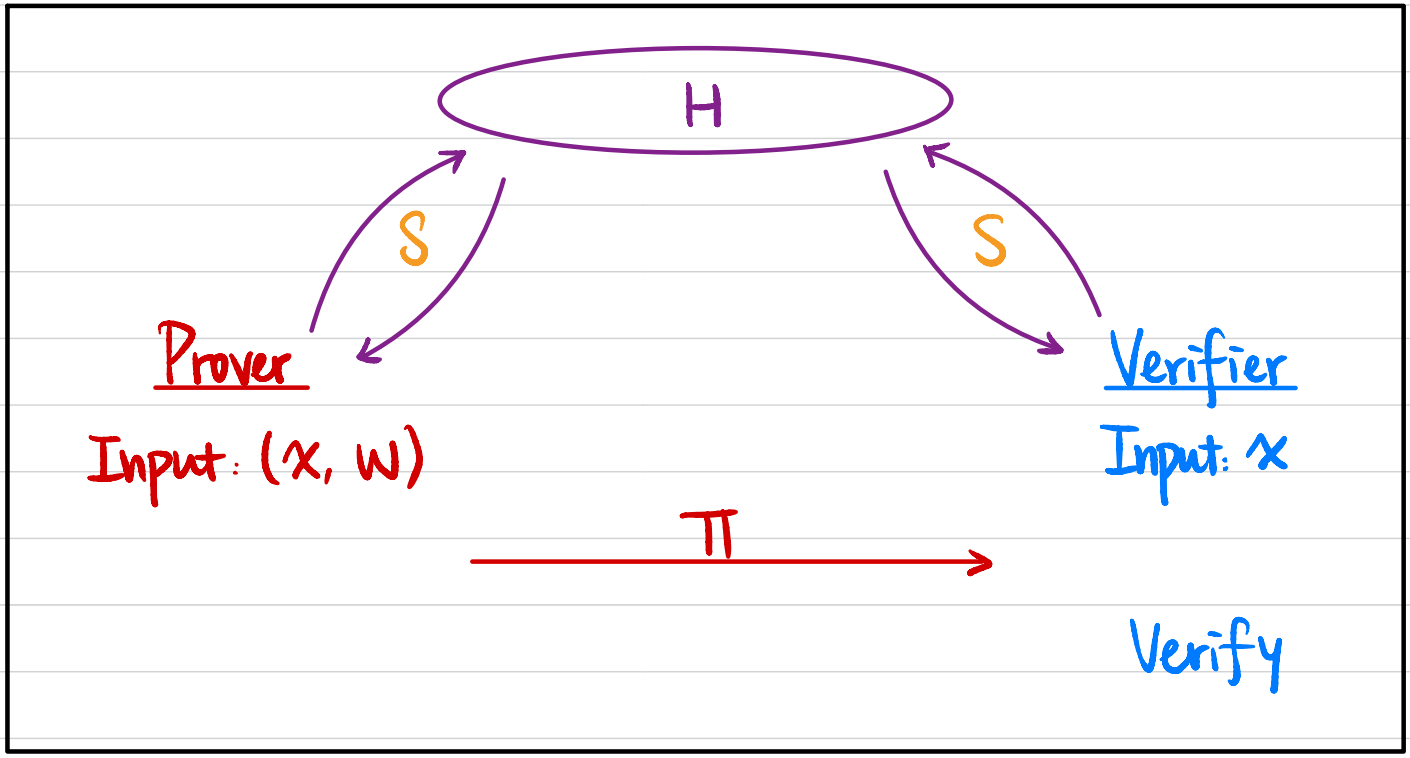
- **Zero-Knowledge:** $\forall PPT\ V^*,\ \exists PPT\ S$ s.t. $\forall (x, w) \in R_L,$

$$Output_{V^*}[\sigma \leftarrow Gen(1^\lambda),\ P(x, w, \sigma) \longrightarrow V^*(x, \sigma)] \simeq S(x)$$

Alternatively: $(\sigma \leftarrow Gen(1^\lambda),\ P(x, w, \sigma)) \simeq S(x)$

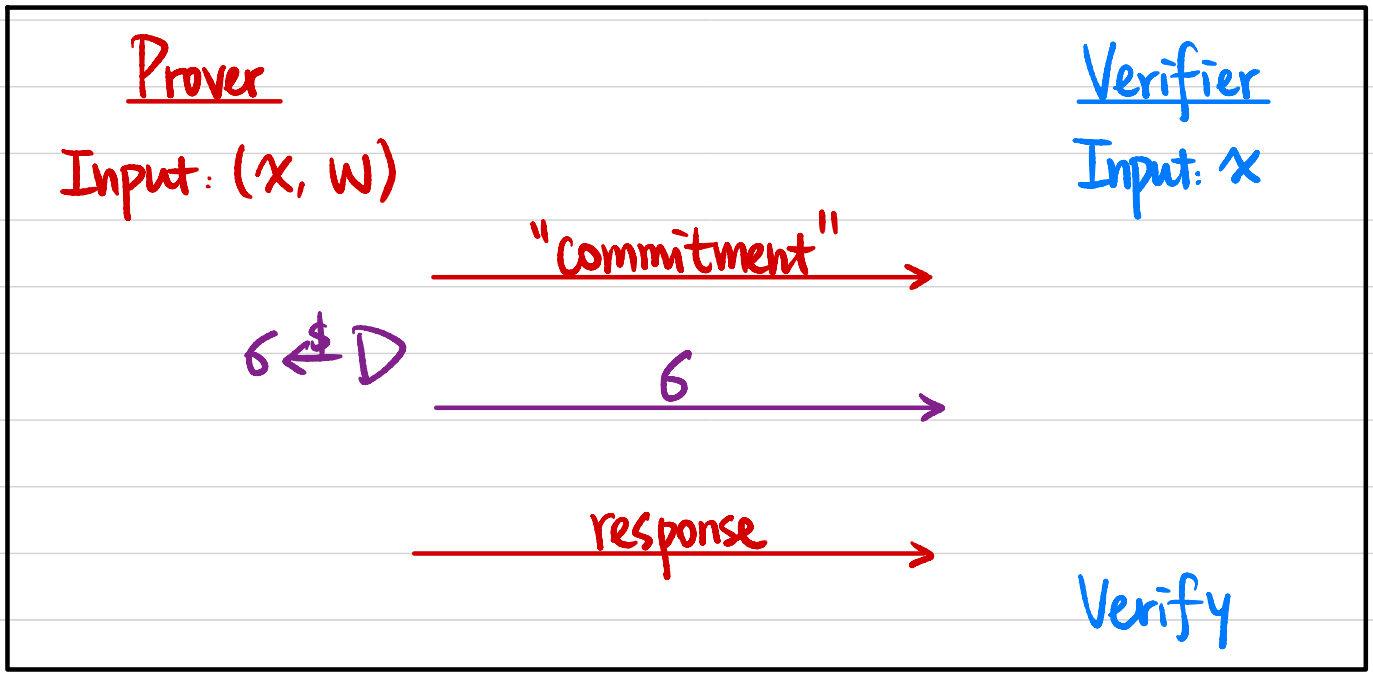
$S(x)$ generates both (σ, π)

Model 2: Random Oracle Model



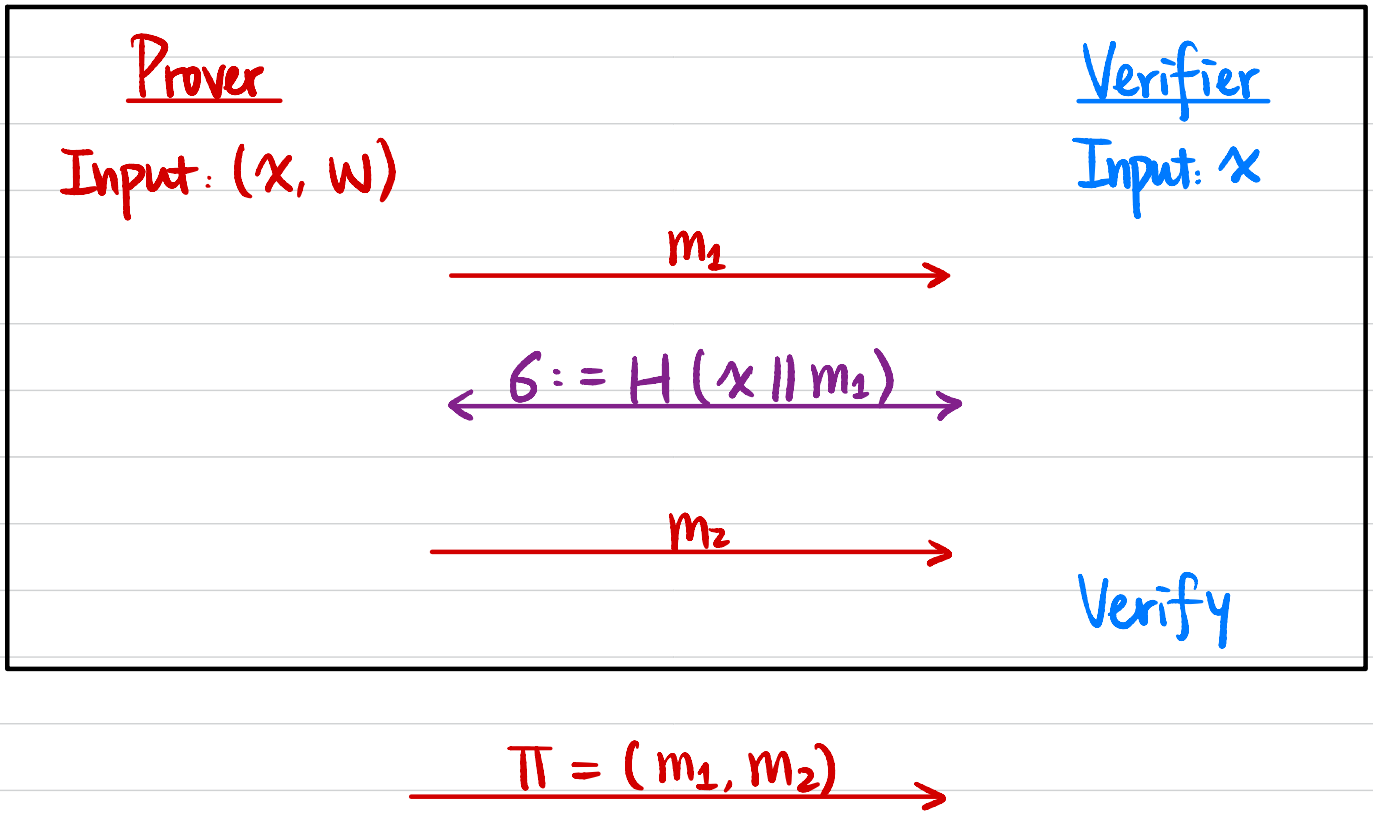
S controls input/output behavior of RO

Sigma Protocol ⇒ NIZK?



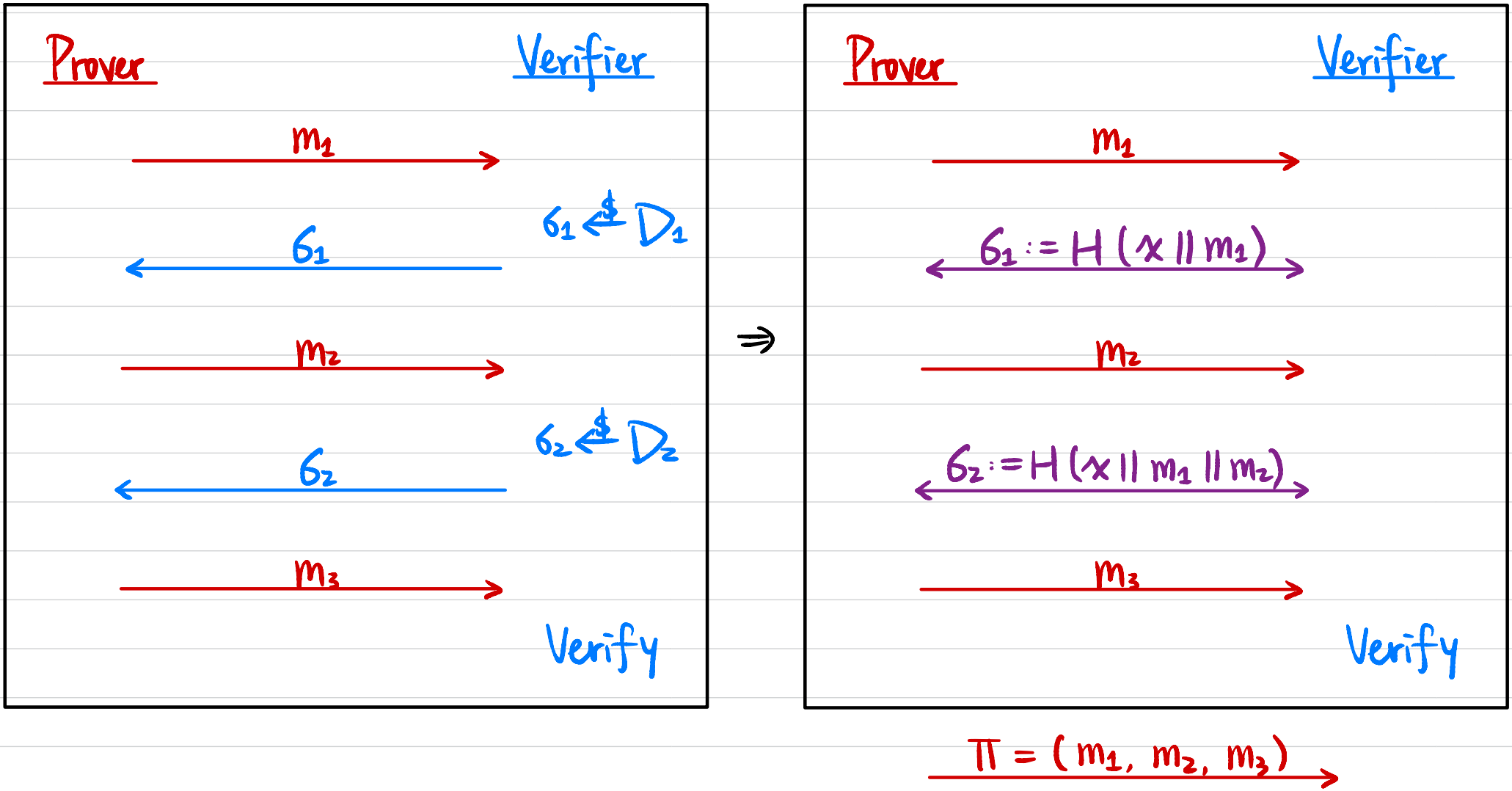
Fiat-Shamir Heuristic

Sigma Protocol $\Rightarrow$ NIZK in the RO model



Fiat-Shamir Heuristic

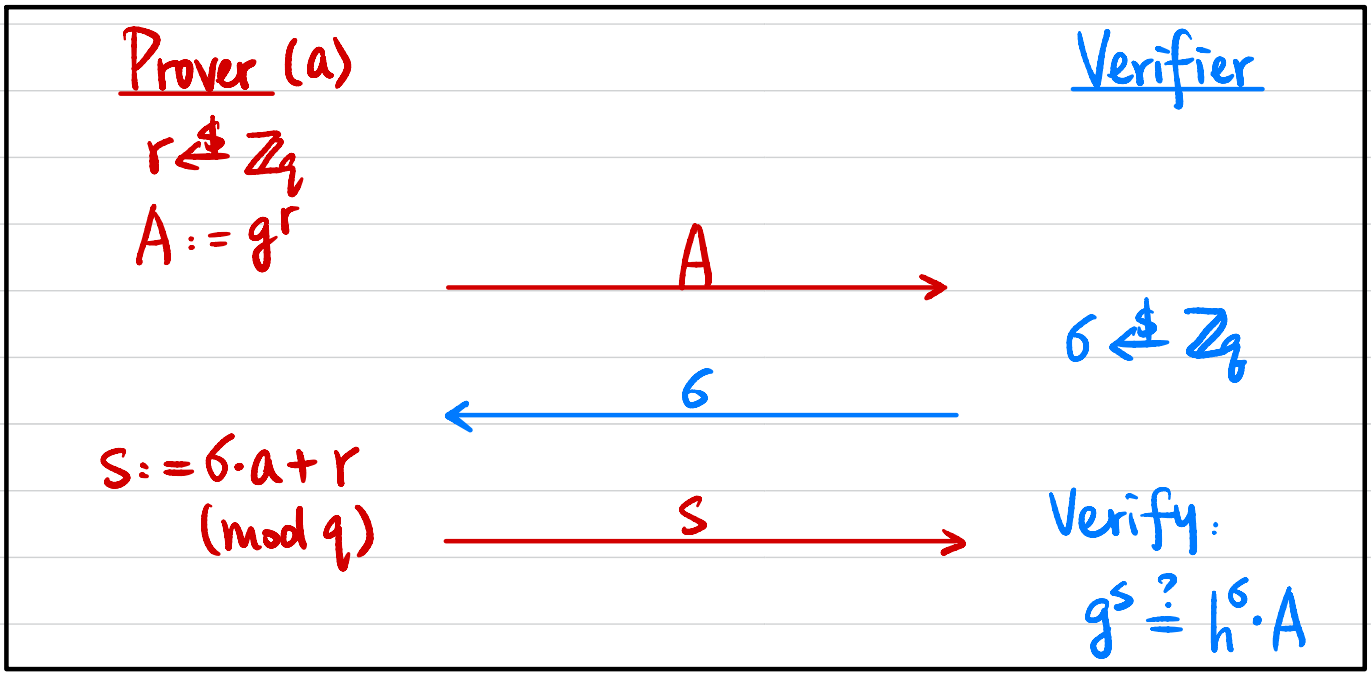
Public-Coin HVZK $\Rightarrow$ NIZK in the RO model



Example: Schnorr's Identification Protocol

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

Prover's secret: a

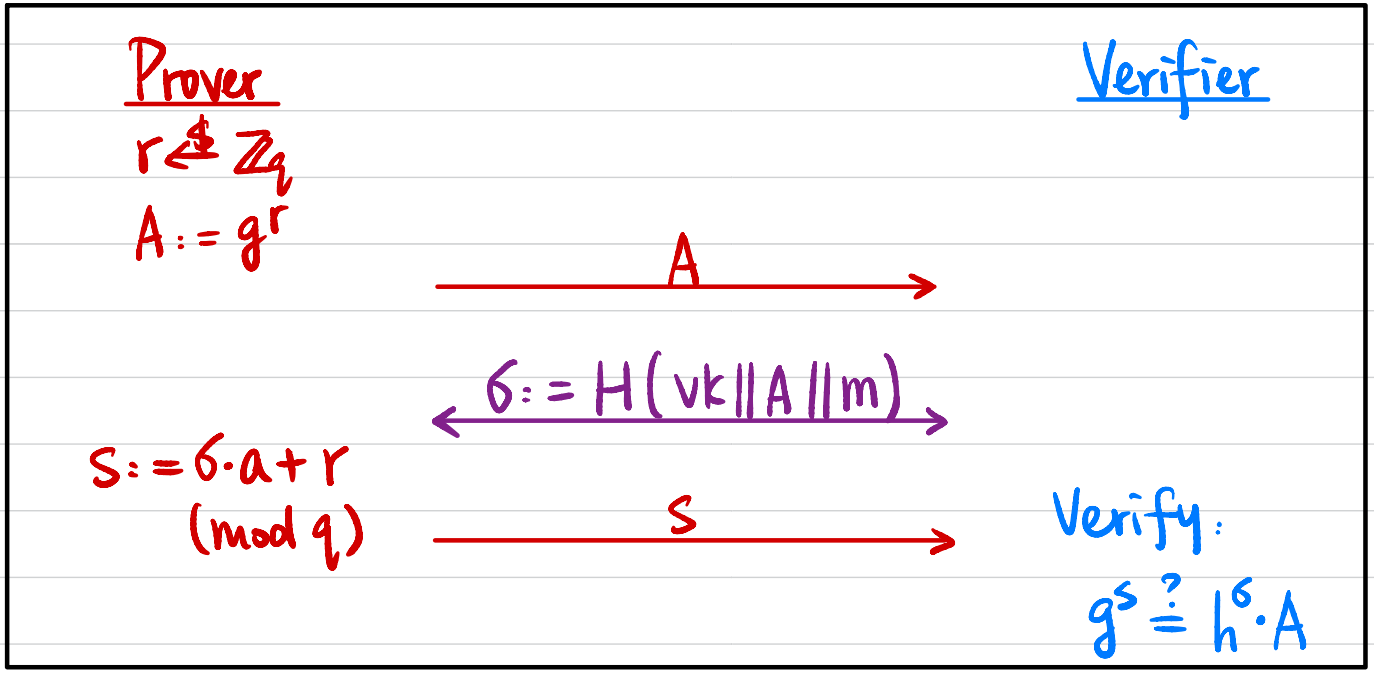


Fiat-Shamir Heuristic

Schnorr's Identification Protocol ⇒ Schnorr's Signature in the RO model

Cyclic group G of order q, generator g — $Gen(1^\lambda)$

Public verification key $vk = g^a$; Secret signing key $sk = a$



To sign a message m: output (A, s)

Anonymous Online Voting

ElGamal ZKP

Voter 1 $\longrightarrow$ $Enc(v_1)$ $v_1 \in \{0, 1\}$

Voter 2 $\longrightarrow$ $Enc(v_2)$ $v_2 \in \{0, 1\}$

⋮

Voter n $\longrightarrow$ $Enc(v_n)$ $v_n \in \{0, 1\}$

$\Downarrow$

$Enc(\Sigma v_i)$

$\Downarrow$

Decrypt to Σv_i

Additively Homomorphic Encryption

$Enc(m_1)$, $Enc(m_2)$ → $Enc(m_1 + m_2)$

Additively Homomorphic

$Enc(m_1)$, $Enc(m_2)$ → $Enc(m_1 \cdot m_2)$

Multiplicatively Homomorphic

ElGamal Encryption: Cyclic group G with generator g, public key $pk = g^{sk}$.

$Enc_{pk}(m_1) = (g^{r_1}, pk^{r_1} \cdot m_1)$

$Enc_{pk}(m_2) = (g^{r_2}, pk^{r_2} \cdot m_2)$

→ $Enc(m_1 \cdot m_2)$? $\quad (g^{r_1+r_2}, pk^{r_1+r_2} \cdot m_1 \cdot m_2)$

Exponential ElGamal:

$Enc_{pk}(m_1) = (g^{r_1}, pk^{r_1} \cdot g^{m_1})$

$Enc_{pk}(m_2) = (g^{r_2}, pk^{r_2} \cdot g^{m_2})$

→ $Enc(m_1 + m_2)$? $\quad (g^{r_1+r_2}, pk^{r_1+r_2} \cdot g^{m_1+m_2})$

Correctness of Encryption

Given a cyclic group G of order q with generator g.

Public key $pk \in G$. ← public

Ciphertext $C = (c_1, c_2)$ ← public

ZKP for an OR statement:

C is an encryption of 0 OR C is an encryption of 1

Witness: randomness r used in encryption

↑ secret

$$R_L = \{ ((pk, c_1, c_2), r) : (c_1 = g^r \wedge c_2 = pk^r) \vee (c_1 = g^r \wedge c_2 = pk^r \cdot g) \}$$

↑ (public) statement — ↑ (secret) witness