CSCI 1515 Applied Cryptography

This Lecture:

- Putting it Together: Anonymous Online Voting
- ElGamal Encryption: Homomorphism and Threshold Decryption

Zero-Knowledge Proof of Knowledge

- **Completeness:** $\forall (x, w) \in R_L$, P can prove it.

- **Soundness:** $\forall x \notin L$, no P^* can prove it.
- **Proof of Knowledge:** $\forall x$, no P^* can prove it without w.

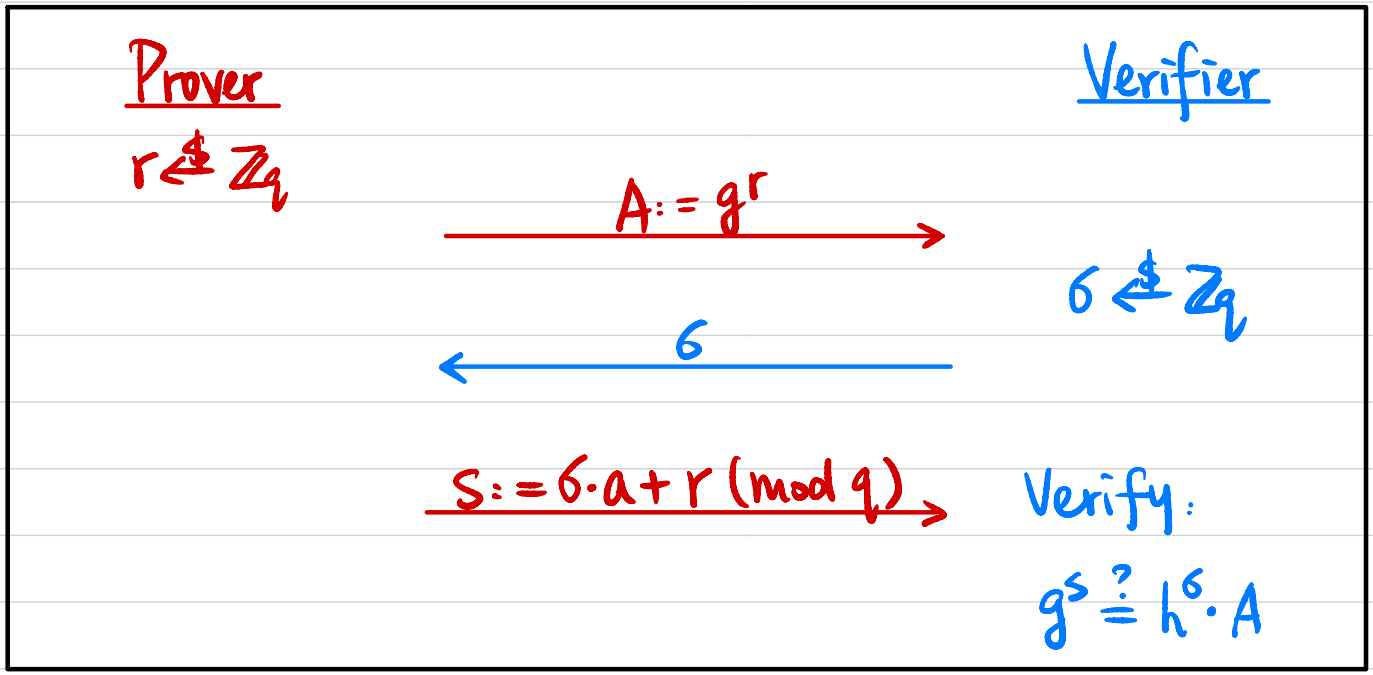
- **Honest-Verifier Zero-Knowledge:** An honest V can't learn anything.
- **Zero-Knowledge:** A malicious V^* can't learn anything.

Example: Schnorr's Identification Protocol

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

Witness: a

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



Anonymous Online Voting

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

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

⋮

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

$\Downarrow$ How?

$Enc(\Sigma v_i)$

$\Downarrow$

Decrypt to Σv_i ← Who?

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.

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

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

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

Exponential ElGamal:

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

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

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

$pk = g^{sk}$

$g^{r_1+r_2} = c_1$, $pk^{r_1+r_2} \cdot g^{m_1+m_2} = c_2$

$c_2 / c_1^{sk} = g^{m_1+m_2}$

$m \in \{0, 1, \cdots, n\}$

Threshold Encryption

t-out-of-t threshold

P_1: $(pk_1, sk_1) \leftarrow \text{PartialGen}(1^\lambda) \longrightarrow pk_1$

P_2: $(pk_2, sk_2) \leftarrow \text{PartialGen}(1^\lambda) \longrightarrow pk_2$

$\vdots$

P_t: $(pk_t, sk_t) \leftarrow \text{PartialGen}(1^\lambda) \longrightarrow pk_t$

$\Rightarrow pk$

$ct \leftarrow \text{Enc}_{pk}(m)$

P_1: $\alpha_1 \leftarrow \text{PartialDec}(sk_1, ct) \longrightarrow \alpha_1$

P_2: $\alpha_2 \leftarrow \text{PartialDec}(sk_2, ct) \longrightarrow \alpha_2$

$\vdots$

P_t: $\alpha_t \leftarrow \text{PartialDec}(sk_t, ct) \longrightarrow \alpha_t$

$\Rightarrow m$

Threshold Encryption : ElGamal

P_1 : $sk_1 \xleftarrow{\$} \mathbb{Z}_q$ $\quad pk_1 = g^{sk_1}$ $\longrightarrow$ pk_1

P_2 : $sk_2 \xleftarrow{\$} \mathbb{Z}_q$ $\quad pk_2 = g^{sk_2}$ $\longrightarrow$ pk_2

$\vdots$

P_t : $sk_t \xleftarrow{\$} \mathbb{Z}_q$ $\quad pk_t = g^{sk_t}$ $\longrightarrow$ pk_t

$\Rightarrow pk = \prod pk_i = \prod g^{sk_i} = g^{\sum sk_i}$

$sk = \sum sk_i \pmod q$

$ct \leftarrow Enc_{pk}(m)$

$ct = (c_1, c_2)$

$= (g^r,\ pk^r \cdot g^m)$

P_1 : $\alpha_1 = c_1^{sk_1}$ $\longrightarrow$ α_1

P_2 : $\alpha_2 = c_1^{sk_2}$ $\longrightarrow$ α_2

$\vdots$

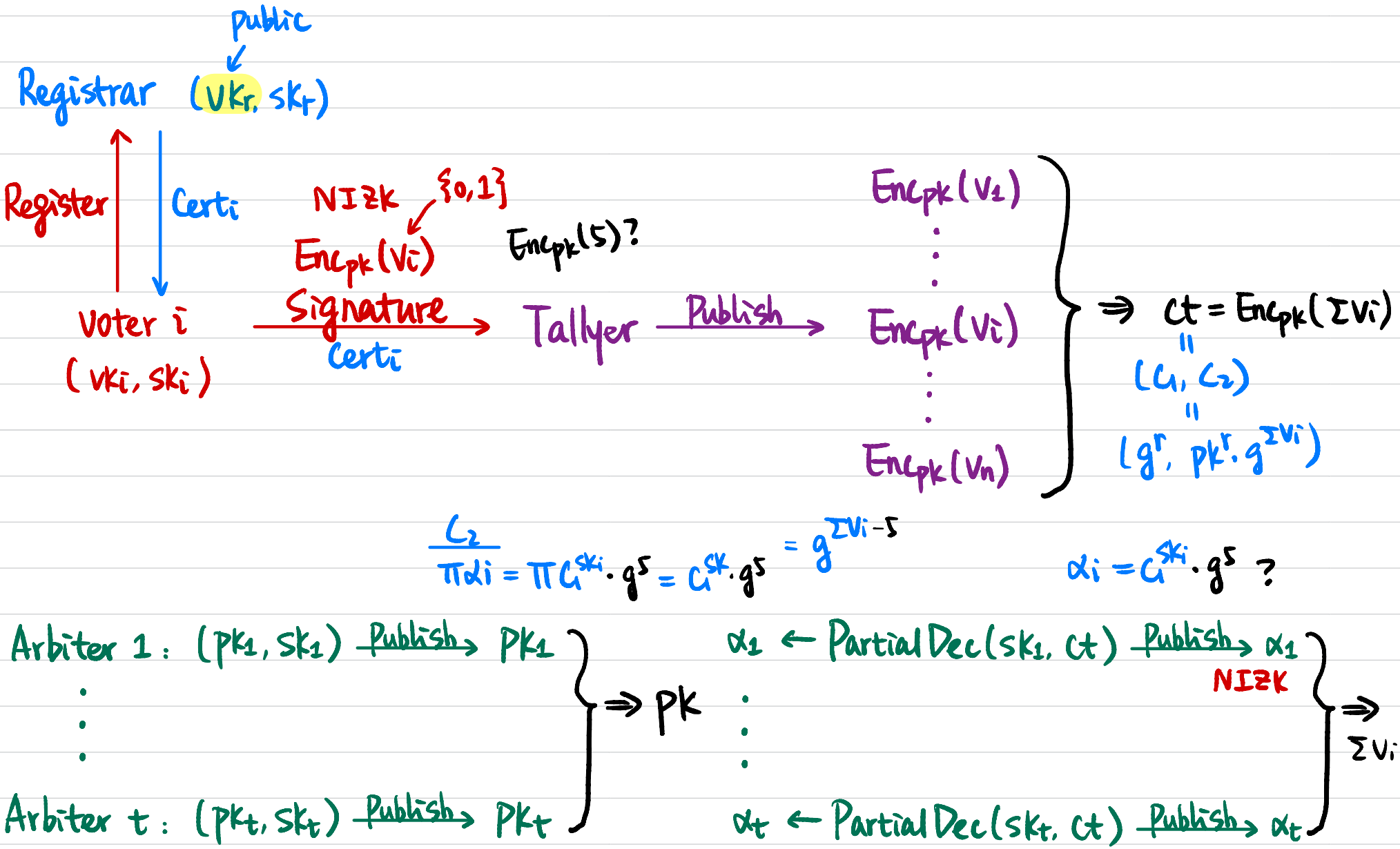
P_t : $\alpha_t = c_1^{sk_t}$ $\longrightarrow$ α_t

$\Rightarrow m = ?$

$$\frac{c_2}{\prod \alpha_i} = g^m$$

$$\prod \alpha_i = \prod c_1^{sk_i} = c_1^{\sum sk_i} = c_1^{sk}$$

Anonymous Online Voting



Correctness of Encryption

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

Public key $pk \in G$.

Ciphertext $C = (c_1, c_2)$

ZKP for an OR statement:

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

Witness: randomness r used in encryption

$$R_{L_0} = \{ ((pk, \underset{\downarrow}{c_1}, c_2), \underset{\downarrow}{r}) : c_1 = g^r \wedge c_2 = pk^r \}$$

(x: $pk = g^a$, $c_1 = g^r$, $c_2 = g^{ar}$; w: r)

$$Enc_{pk}(0) = (g^r, pk^r \cdot g^0)$$

$$R_{L_1} = \{ ((pk, c_1, c_2), r) : c_1 = g^r \wedge c_2 = pk^r \cdot g \}$$

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

$$Enc_{pk}(1) = (g^r, pk^r \cdot g^1)$$

Correctness of Partial Decryption

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

Partial public key $pk_i \in G$.

Ciphertext $C = (C_1, C_2)$.

Partial decryption α_i

Witness: partial secret key sk_i

ZKP for partial decryption:

$$R_L = \{ ((pk_i, C_1, \alpha_i), sk_i) : pk_i = g^{sk_i} \wedge \alpha_i = C_1^{sk_i} \}$$

x: $pk_i = g^{sk_i}$, $C_1 = g^r$, $\alpha_i = g^{r \cdot sk_i}$

w: sk_i

Multiple Candidates ?

k candidates

Voter 1 $\longrightarrow$ Enc (V_1) $\quad V_1 \in \{0, 1, \cdots, k-1\}$

Voter 2 $\longrightarrow$ Enc (V_2) $\quad V_2 \in \{0, 1, \cdots, k-1\}$

$\vdots$

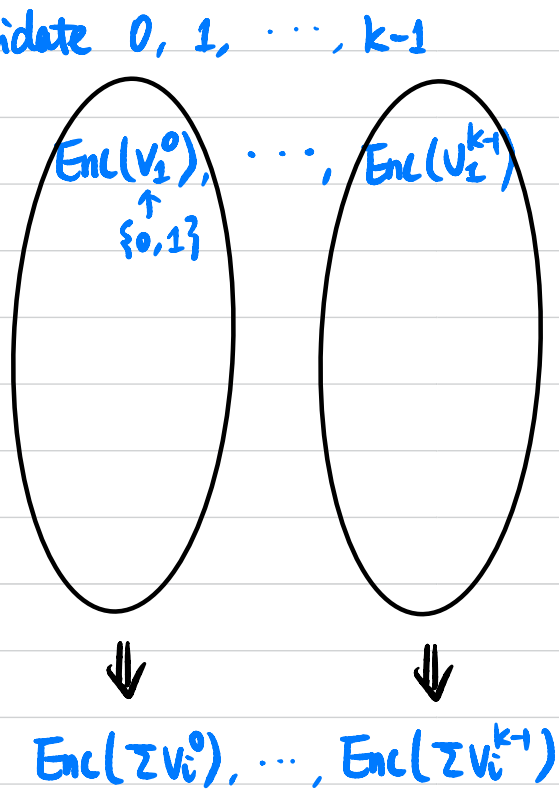
Voter n $\longrightarrow$ Enc (V_n) $\quad V_n \in \{0, 1, \cdots, k-1\}$

$\Downarrow$

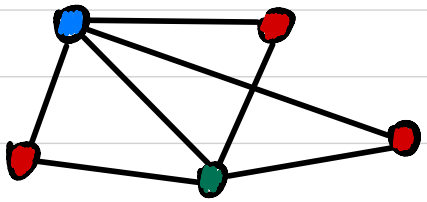
Enc (ΣV_i)

$\Downarrow$

Decrypt to ΣV_i



Zero-Knowledge Proof for Graph 3-Coloring (All NP)



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

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