CSCI 1515 Applied Cryptography

This Lecture:

- Putting it Together: Anonymous Online Voting
- ElGamal Encryption: Homomorphism and Threshold Decryption
- Zero-Knowledge Proofs for All NP

Anonymous Online Voting

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

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

⋮

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

$\Downarrow$

$Enc(\Sigma v_i)$

$\Downarrow$

Decrypt to Σv_i

Additively Homomorphic Encryption

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

Additively Homomorphic

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

Multiplicatively Homomorphic

ElGamal Encryption: Cyclic group G with generator g, public key pk.

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

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

Exponential ElGamal:

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

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

Threshold Encryption

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

$\Rightarrow pk = \prod pk_i$

$sk = ?$

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

$ct = (c_1, c_2)$

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

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

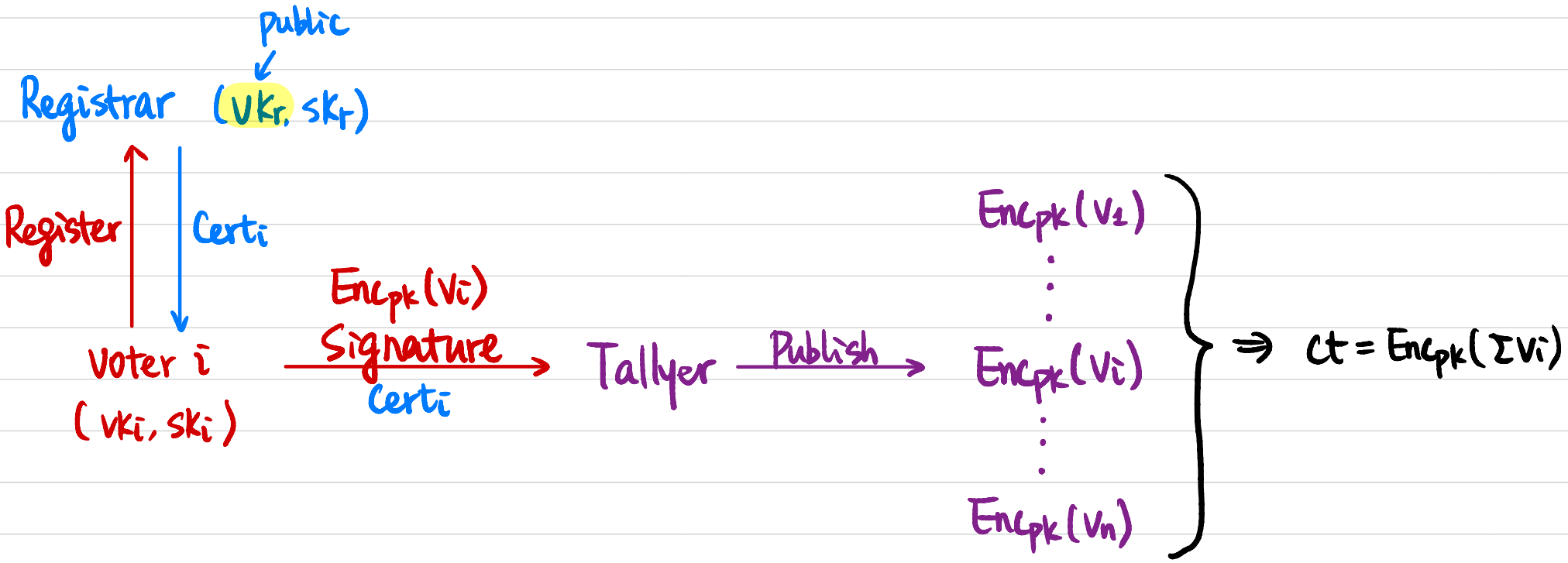
P_2 : $\alpha_2 = c_1^{sk_2}$ $\longrightarrow$ α_2

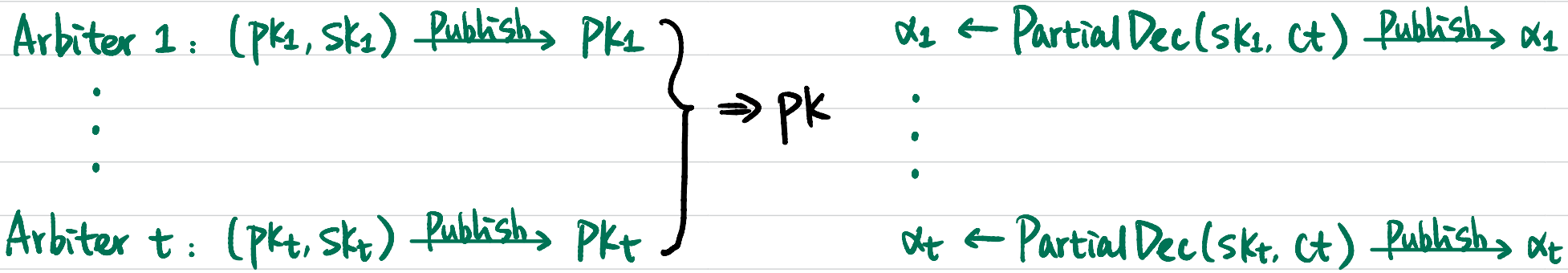
$\vdots$

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

$\Rightarrow m = ?$

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

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

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

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:

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

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) $\quad V_n \in \{0, 1, \cdots, k-1\}$

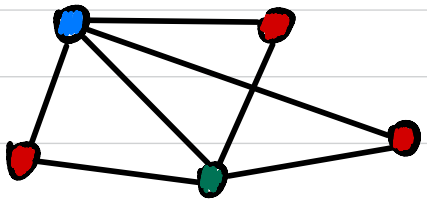
$\Downarrow$

Enc (ΣV_i)

$\Downarrow$

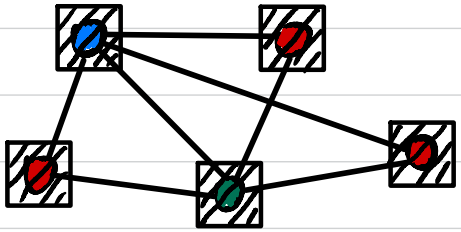
Decrypt to ΣV_i

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

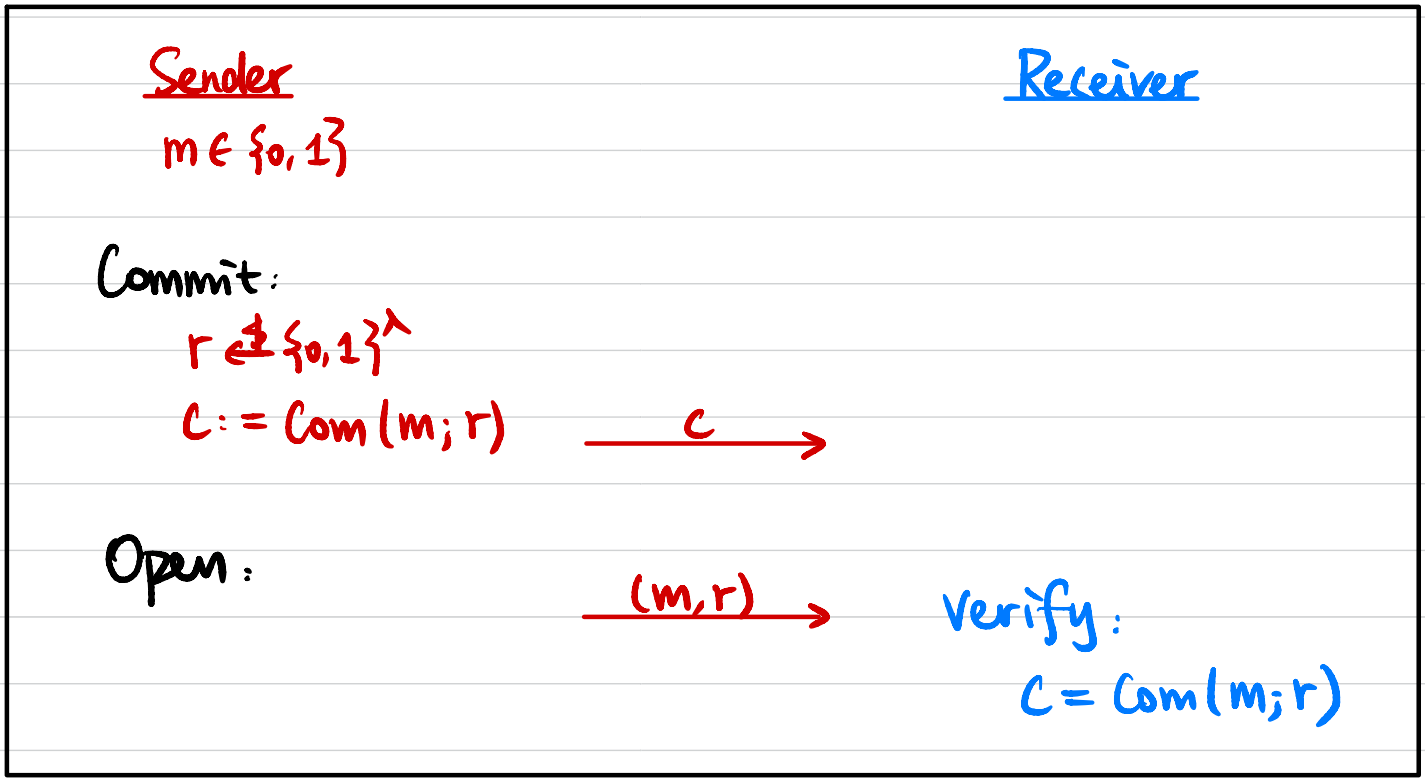


NP language $L = \{ G : G \text{ has 3-coloring} \}$

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



Commitment Scheme



Example: Pedersen Commitment

Cyclic group G of order q with generator g. $h \xleftarrow{\$} G$ ← can be generated by Receiver

$r \xleftarrow{\$} \mathbb{Z}_q$

$Com(m;r) = g^m \cdot h^r$

Commitment Scheme

- **Hiding:** $\mathsf{Com}(0; r) \simeq \mathsf{Com}(1; s)$
  - **Perfectly hiding:** $\mathsf{Com}(0; r) \equiv \mathsf{Com}(1; s)$
  - **Computationally hiding:** $\mathsf{Com}(0; r) \overset{c}{\simeq} \mathsf{Com}(1; s)$

- **Binding:** Hard to find r, s s.t. $\mathsf{Com}(0; r) = \mathsf{Com}(1; s)$
  - **Perfectly binding:** $\forall r, s,\ \mathsf{Com}(0; r) \neq \mathsf{Com}(1; s)$
  - **Computationally binding:** Any PPT sender cannot find r, s s.t. $\mathsf{Com}(0; r) = \mathsf{Com}(1; s)$

What does Pedersen commitment scheme satisfy?

Can a commitment scheme be both perfectly hiding & perfectly binding?

Zero-Knowledge Proof for Graph 3-Coloring

Input: $G = (V, E)$

Witness: $\phi: V \to \{0,1,2\}$

Given a computationally hiding, perfectly binding commitment scheme.

Prover

Randomly sample $\pi: \{0,1,2\} \to \{0,1,2\}$

$\forall v \in V$, $r_v \xleftarrow{\$} \{0,1\}^\lambda$, $c_v := \mathrm{Com}(\pi(\phi(v)); r_v)$

$\xrightarrow{\{c_v\}_{v \in V}}$

Verifier

Randomly pick an edge $(u,v) \in E$

$\xleftarrow{(u,v)}$

Open commitments c_u & c_v

$\xrightarrow{\alpha = \pi(\phi(u)),\ r_u \quad \beta = \pi(\phi(v)),\ r_v}$

Verify: $c_u = \mathrm{Com}(\alpha; r_u)$

$c_v = \mathrm{Com}(\beta; r_v)$

$\alpha, \beta \in \{0,1,2\}$, $\alpha \neq \beta$

Completeness ?

Soundness

Given a computationally hiding, perfectly binding commitment scheme.

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

Prover		Verifier
Randomly sample $\pi: \{0,1,2\} \to \{0,1,2\}$		
$\forall v \in V, \ r_v \xleftarrow{\$} \{0,1\}^\lambda, \ C_v := \mathsf{Com}(\pi(\phi(v)); r_v)$		
	$\xrightarrow{\{C_v\}_{v \in V}}$	
		Randomly pick an edge $(u,v) \in E$
	$\xleftarrow{(u,v)}$	
Open commitments C_u & C_v		
$\alpha = \pi(\phi(u)), \ r_u$ $\beta = \pi(\phi(v)), \ r_v$	$\xrightarrow{\quad}$	Verify: $C_u = \mathsf{Com}(\alpha; r_u)$ $C_v = \mathsf{Com}(\beta; r_v)$ $\alpha, \beta \in \{0,1,2\}, \ \alpha \neq \beta$

Zero-Knowledge

Given a computationally hiding, perfectly binding commitment scheme.

$$\forall \text{PPT } V^*,\ \exists \text{PPT } S \text{ s.t. } \forall (x,w) \in R_L,$$
$$\text{Output}_{V^*}[P(x,w) \longleftrightarrow V^*(x)] \simeq S(x)$$