CSCI 1515 Applied Cryptography

This Lecture:

- ZKP for OR Statements (Continued)
- Anonymous Online Voting (Continued)
- ElGamal Threshold Encryption
- RSA Blind Signature

Anonymous Online Voting

Public: Cyclic group $\mathbb{G}$ of order q with generator g

ElGamal public key pk

Exponential ElGamal　　　　　　　　ZKP

Voter 1 $\longrightarrow$ $Enc(v_1) = (g^{r_1}, pk^{r_1} \cdot g^{v_1})$　　$v_1 \in \{0,1\}$

Voter 2 $\longrightarrow$ $Enc(v_2) = (g^{r_2}, pk^{r_2} \cdot g^{v_2})$　　$v_2 \in \{0,1\}$

⋮

Voter n $\longrightarrow$ $Enc(v_n) = (g^{r_n}, pk^{r_n} \cdot g^{v_n})$　　$v_n \in \{0,1\}$

$$\Downarrow$$

$$Enc(\Sigma v_i) = (g^{\Sigma r_i}, pk^{\Sigma r_i} \cdot g^{\Sigma v_i})$$

$$\Downarrow$$

Decrypt to Σv_i

Correctness of Encryption

Given a cyclic group $\mathbb{G}$ of order q with generator g. (public)

Public key $pk \in \mathbb{G}$. ← public

Ciphertext $c = (c_1, c_2)$

ZKP for an OR statement:

$\boxed{c \text{ is an encryption of } 0}$ OR $\boxed{c \text{ is an encryption of } 1}$

Witness: randomness r used in encryption

↑ secret

$$R_L = \{ (\underbrace{(pk, c_1, c_2)}_{\substack{\text{(public)} \\ \text{Statement}}}, \underbrace{r}_{\substack{\text{(secret)} \\ \text{Witness}}}) : (c_1 = g^r \wedge c_2 = pk^r) \vee (c_1 = g^r \wedge c_2 = pk^r \cdot g) \}$$

Correctness of Encryption

$\boxed{c \text{ is an encryption of } 0}$

Witness: randomness r used in encryption

$$R_{L_0} = \{ (\underbrace{(pk, c_1, c_2)}_{\text{(public) statement}}, \underbrace{r}_{\text{(secret) witness}}) : c_1 = g^r \wedge c_2 = pk^r \}$$

$\boxed{c \text{ is an encryption of } 1}$

Witness: randomness r used in encryption

$$R_{L_1} = \{ (\underbrace{(pk, c_1, c_2)}_{\text{(public) statement}}, \underbrace{r}_{\text{(secret) witness}}) : c_1 = g^r \wedge c_2 = pk^r \cdot g \}$$

Proving AND/OR Statements

AND:

Statements: x_0, x_1

Witnesses: w_0, w_1

$$R_{AND} = \{ ((x_0, x_1), (w_0, w_1)) : (x_0, w_0) \in R_{L_0} \text{ AND } (x_1, w_1) \in R_{L_1} \}$$

OR:

Statements: x_0, x_1

Witness: w

$$R_{OR} = \{ ((x_0, x_1), w) : (x_0, w) \in R_{L_0} \text{ OR } (x_1, w) \in R_{L_1} \}$$

Example: Diffie-Hellman Tuple

Public: Cyclic group $\mathbb{G}$ 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. $u = g^b \wedge v = h^b$

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

Prover (b)	Public: (h,u,v)	Verifier
$r \xleftarrow{\$} \mathbb{Z}_q$		
$A := g^r \quad B := h^r$	$\xrightarrow{\quad A,\ B \quad}$	
		$\sigma \xleftarrow{\$} \mathbb{Z}_q$
	$\xleftarrow{\quad \sigma \quad}$	
$s := \sigma \cdot b + r \pmod q$	$\xrightarrow{\quad s \quad}$	Verify:
		$g^s \stackrel{?}{=} u^\sigma \cdot A$
		$h^s \stackrel{?}{=} v^\sigma \cdot B$

Proving OR Statement

$$R_{OR} = \{((x_0, x_1), w) : (x_0, w) \in R_{L_0} \text{ OR } (x_1, w) \in R_{L_1}\}$$

Prover — **Verifier**

$\xrightarrow{A_0, B_0}$ $\xrightarrow{A_1, B_1}$

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

$\xleftarrow{\sigma}$

σ_0 σ_1

$\xrightarrow{s_0}$ $\xrightarrow{s_1}$

Verify:

$\sigma_0 + \sigma_1 = \sigma \bmod q$

$((A_0, B_0), \sigma_0, s_0)$

$((A_1, B_1), \sigma_1, s_1)$

How does Prover compute response for both statements?

Say $(x_0, w_0) \in R_{L_0}$

Completeness?

Proving OR Statement

Proof of Knowledge?

Prover* | **Extractor**

$\xrightarrow{A_0, B_0}$ $\xrightarrow{A_1, B_1}$

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

$\xleftarrow{\sigma}$

σ_0 σ_1

$\xrightarrow{s_0}$ $\xrightarrow{s_1}$

$\sigma_0 + \sigma_1 = \sigma \bmod q$

$((A_0, B_0), \sigma_0, s_0)$

$((A_1, B_1), \sigma_1, s_1)$

How to extract w s.t. $(x_0, w) \in R_{L_0}$ OR $(x_1, w) \in R_{L_1}$?

Proving OR Statement

Honest-Verifier Zero-Knowledge (HVZK)?

Simulator | **Verifier**

$$\xrightarrow{A_0,\, B_0} \quad \xrightarrow{A_1,\, B_1}$$

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

$$\xleftarrow{\quad \sigma \quad}$$

$$\sigma_0 \qquad \sigma_1$$

$$\xrightarrow{s_0} \quad \xrightarrow{s_1}$$

$$\sigma_0 + \sigma_1 = \sigma \bmod q$$

$$((A_0, B_0), \sigma_0, s_0)$$

$$((A_1, B_1), \sigma_1, s_1)$$

Anonymous Online Voting

Public: Cyclic group $\mathbb{G}$ of order q with generator g

ElGamal public key pk $(= g^{sk})$

Exponential ElGamal

ZKP

Voter 1 $\longrightarrow$ $Enc(V_1) = (g^{r_1}, pk^{r_1} \cdot g^{v_1})$ $\quad V_1 \in \{0, 1\}$

Voter 2 $\longrightarrow$ $Enc(V_2) = (g^{r_2}, pk^{r_2} \cdot g^{v_2})$ $\quad V_2 \in \{0, 1\}$

$\vdots$

Voter n $\longrightarrow$ $Enc(V_n) = (g^{r_n}, pk^{r_n} \cdot g^{v_n})$ $\quad V_n \in \{0, 1\}$

$\Downarrow$

$$Enc(\Sigma v_i) = (g^{\Sigma r_i}, pk^{\Sigma r_i} \cdot g^{\Sigma v_i}) = (C_1, C_2)$$

$\Downarrow$

Decrypt to Σv_i $\qquad\qquad$ $C_2 / C_1^{sk} = g^{\Sigma v_i}$

How? Who?

Threshold Encryption

t-out-of-t threshold

$$\left.\begin{array}{lll} P_1: & (pk_1, sk_1) \leftarrow \mathrm{PartialGen}(1^\lambda) & \longrightarrow pk_1 \\ P_2: & (pk_2, sk_2) \leftarrow \mathrm{PartialGen}(1^\lambda) & \longrightarrow pk_2 \\ \vdots & & \\ P_t: & (pk_t, sk_t) \leftarrow \mathrm{PartialGen}(1^\lambda) & \longrightarrow pk_t \end{array}\right\} \Rightarrow pk$$

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

$$\left.\begin{array}{lll} P_1: & d_1 \leftarrow \mathrm{PartialDec}(sk_1, ct) & \longrightarrow d_1 \\ P_2: & d_2 \leftarrow \mathrm{PartialDec}(sk_2, ct) & \longrightarrow d_2 \\ \vdots & & \\ P_t: & d_t \leftarrow \mathrm{PartialDec}(sk_t, ct) & \longrightarrow d_t \end{array}\right\} \Rightarrow m$$

Threshold Encryption: ElGamal

$$\left.\begin{array}{llll} P_1: & sk_1 \xleftarrow{\$} \mathbb{Z}_q & pk_1 = g^{sk_1} & \longrightarrow \ pk_1 \\ P_2: & sk_2 \xleftarrow{\$} \mathbb{Z}_q & pk_2 = g^{sk_2} & \longrightarrow \ pk_2 \\ \vdots & & & \\ P_t: & sk_t \xleftarrow{\$} \mathbb{Z}_q & pk_t = g^{sk_t} & \longrightarrow \ pk_t \end{array}\right\} \Rightarrow \begin{array}{l} pk = \prod pk_i \\ sk = ? \end{array}$$

$$ct = (c_1, c_2) = (g^r, \ pk^r \cdot g^m)$$

$$\left.\begin{array}{llll} P_1: & d_1 = c_1^{sk_1} & \longrightarrow & d_1 \\ P_2: & d_2 = c_1^{sk_2} & \longrightarrow & d_2 \\ \vdots & & & \\ P_t: & d_t = c_1^{sk_t} & \longrightarrow & d_t \end{array}\right\} \Rightarrow \begin{array}{l} \prod d_i = ? \\ m = ? \end{array}$$

Anonymous Online Voting

public

Registrar (vk_r, sk_r)

ID_i

$Vote_i$

$\sigma_i \leftarrow Sign_{sk_r}(Vote_i)$

(NI)ZKP$_i$ for OR

Voter i $\xrightarrow{(Vote_i,\ \sigma_i)}$ Tallyer $\xrightarrow[\text{(Sign)}]{\text{Publish}}$

$Vote_i \leftarrow Enc_{pk}(v_i)$

$v_i \in \{0,1\}$

(vk_t, sk_t)

public

$$\left.\begin{array}{l} (Vote_1, \sigma_1, ZKP_1), \sigma_1^T \\ \vdots \\ (Vote_i, \sigma_i, ZKP_i), \sigma_i^T \\ \vdots \\ (Vote_n, \sigma_n, ZKP_n), \sigma_n^T \end{array}\right\} \Rightarrow ct = Enc_{pk}(\Sigma v_i)$$

public

(NI)ZKP

$$\left.\begin{array}{l} \text{Arbiter } 1:\ (pk_1, sk_1) \xrightarrow{\text{Publish}} pk_1 \\ \vdots \\ \text{Arbiter } t:\ (pk_t, sk_t) \xrightarrow{\text{Publish}} pk_t \end{array}\right\} \Rightarrow pk$$

$$\left.\begin{array}{l} d_1 \leftarrow PartialDec(sk_1, ct) \xrightarrow{\text{Publish}} d_1 \\ \vdots \\ d_t \leftarrow PartialDec(sk_t, ct) \xrightarrow{\text{Publish}} d_t \end{array}\right\} \Rightarrow \Sigma v_i$$

Correctness of Partial Decryption

Given a cyclic group $\mathbb{G}$ of order q with generator g. (public)

Partial public key $pk_i \in \mathbb{G}$.

Ciphertext $c = (c_1, c_2)$. ← public

Partial decryption d_i

Witness: partial secret key sk_i ← private

ZKP for partial decryption:

$$R_L = \{ (\underbrace{(c_1, pk_i, d_i)}_{x}, \underbrace{sk_i}_{\text{witness}}) : pk_i = g^{sk_i} \wedge d_i = c_1^{sk_i} \}$$

Blind Signature

Signer

public

$(vk, sk) \leftarrow Gen(1^\lambda)$

Requester

m=?

$(m', r) \leftarrow Blind(m)$

$\xleftarrow{\quad m' \quad}$

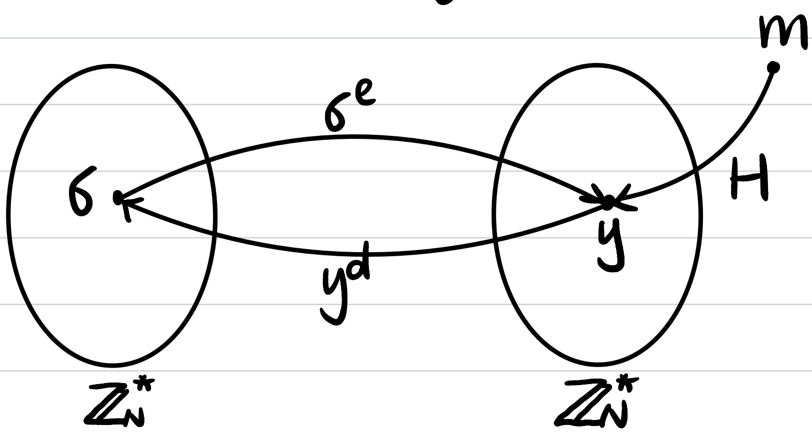
$\sigma' \leftarrow SignBlind_{sk}(m')$

$\xrightarrow{\quad \sigma' \quad}$

$\sigma := Unblind(\sigma', r)$

$Vrfy_{vk}(m, \sigma) = 1$

RSA Blind Signature



$vk = (N, e)$ $sk = d$

$\mathrm{Sign}_{sk}(m) = H(m)^d \bmod N$

$\mathrm{Vrfy}_{vk}(m, \sigma)$: $\sigma^e \stackrel{?}{\equiv} H(m) \pmod N$

Signer

$(vk, sk) \leftarrow \mathrm{Gen}(1^\lambda)$

Requester

$\mathrm{Blind}(m)$:

$r \xleftarrow{\$} \mathbb{Z}_N^*$

$m' := H(m) \cdot r^e \bmod N$

$m = ?$

$\downarrow$

$\xleftarrow{\quad m' \quad}$

$\mathrm{SignBlind}_{sk}(m')$:

$\sigma' := (m')^d$

$\xrightarrow{\quad \sigma' \quad}$

$\mathrm{Unblind}(\sigma', r)$:

$\sigma := \sigma' \cdot r^{-1} \bmod N$