

**CSCI971 Advance Computer Security:  
Homework #9**

**Mei Wangzhihui  
2019124044**

## Problem 1

This protocol is like ElGamal encryption mode.

The  $sk \leftarrow k, pk \leftarrow g^k$ .

Alice knows the public key  $pk$  and  $F(k, m) = H(m)^k$ , she chooses a random  $\rho \leftarrow Z_q$  and sends Bob  $\hat{m} = H(m) \cdot g^\rho$ .

We assume  $v \leftarrow g^\rho, \omega \leftarrow pk^\rho = g^{\rho k} = v^k$ .

When Bob gets the  $\hat{m}$ , he responds  $res = \hat{m}^k = H(m)^k \cdot g^{\rho k} = H(m)^k \cdot \omega$  to Alice, as  $H(m)$  is a random oracle, so Bob cannot know the  $m$  from  $H(m)$ .

When Alice gets the  $res$ , she knows  $\omega = g^{k\rho}$  so she just gets  $H(m)^k = res / (g^{k\rho})$ .

Because it is hard to get  $k$  from  $\hat{m}^k$  as it is a hard problem in number theory. So Alice doesn't know  $k$ .

## Problem 2

1)

### Game 0(DDH Game)

Challenger  $\mathcal{C}$ , generate random  $\alpha, \beta, \gamma$  from  $Z_q$ . Calculate  $u = g^\alpha, v = g^\beta, W_0 = g^{\alpha\beta}W_1 = g^\gamma$  and send  $(u, v, W_b)$  to Adversary, Adversary  $\mathcal{A}$  output  $\hat{b}$

### Game 1

Step1: Challenger  $\mathcal{C}_\infty$  generate  $pk = u \in G$  and  $E(pk, m) = [\beta \leftarrow Z_q, \gamma \leftarrow g^\alpha, e \leftarrow \mu^\beta * m]$ . Challenger send  $pk$  to Adversary.

Step2: Adversary  $\mathcal{A}$  generate  $m_0, m_1, |m_0| = |m_1|$  and send to Challenger.

Step3: Challenger generate  $e = \mu^\beta * m_b$  and send Adversary  $(v, e)$ . Adversary output  $b$ .

The Adversary knows  $g^\alpha, g^\beta, g^{\alpha\beta * m_b}$  because DDH assumption holds in  $G$ . The Adversary cannot distinguish  $g^{\alpha\beta}$  and  $g^\gamma$ .  $\mathcal{A}$  cannot distinguish  $g^{\alpha\beta * m}$  and  $g^\gamma * m$ . As  $g^\gamma$  is a random number, So  $g^\gamma * m$  is indistinguishable.

Assume  $W_b$  as the event, that Adversary output 1 in experiment  $b$ .

$Adv_S[\mathcal{A}, \mathcal{E}] = |Pr[W_0] - Pr[W_1]|$  is negligible.

2)

the CDH assumption is stronger than DDH assumption, so  $CDH \Rightarrow DDH$ .

If CDH problem is solvable, Adversary  $\mathcal{A}$  can compute  $g^{\alpha\beta}$  from  $g^\alpha$  and  $g^\beta$ . As  $\mathcal{A}$  can get  $u = g^\alpha, v = g^\beta$ , he can compute  $g^\alpha\beta * m_0$  and  $g^\alpha\beta * m_1$  by himself, so  $Adv_S[\mathcal{A}, \mathcal{E}] = 1$  is not negligible. So the  $E_{MEG}$  is not semantically secure.

3)

$$\because E(m_0) * E(m_1) = (v, e_0) * (v, e_1) = (v^2, e_0 * e_1) = E(m_1 * m_2)$$

$$D(E(m_0) * E(m_1)) = D(sk, (v^2, e_0 * e_1)) = e_0 * e_1 / (v^2)^\alpha = \frac{g^\alpha\beta * m_0 * g^\alpha\beta * m_1}{(g^{2\beta})^\alpha}$$

$\therefore$  it is possible to create a new ciphertext  $c$  which is an encryption of  $m_1 * m_2$ .

## Problem 3

## Problem 4

1) if Adversary  $\mathcal{A}$  knows  $g^\alpha$  and  $h^\beta$ . He can compute  $e(g, g)^{\alpha\beta} = e(g^\alpha, g^\beta)$ . In DDH, he can distinguish  $e(g, h)^{\alpha\beta}$  and  $e(g, h)^\gamma$  ( $\gamma \in \mathbb{Z}_q$ ) if  $\mathcal{A}$  know  $g^\alpha$  and  $g^\beta$ .

So  $\text{Adv}_{SS}[\mathcal{A}, \mathcal{E}] = 1$  is not negligible. DDH problem is easy in  $G$ .

2) CDH is hard to solve  $\Rightarrow \text{Pr}[\mathcal{A} \text{ know } g^{\alpha\beta} | \mathcal{A} \text{ know } (g^\alpha, g^\beta)]$  is negligible.

We can construct a game, Adversary  $\mathcal{A}$  attack in a BLS signature game. Adversary  $\mathcal{B}$  attack CDH assumption.  $\mathcal{B}$  is  $\mathcal{A}$ 's Challenger.

in CDH Attack Game, Challenger  $\mathcal{C}_1$  generate he generate  $x \leftarrow \mathbb{Z}_q, pk = g^x, sk = x, h = H(m)$  and send  $(g, g^x, h)$  to  $\mathcal{B}$ ,  $\mathcal{B}$  give back  $h^x$  and win if  $(g, g^x, h, h^x)$  is DH-tuple.

For  $\mathcal{B}$ , he challenge Adversary  $\mathcal{A}$  in BLS attack game.  $\mathcal{B}$  send  $pk = g^x, g$  to  $\mathcal{A}$ . A query  $\mathcal{B}$  with  $M_i, i \in \{0, 1, \dots, R_0\}$ ,  $\mathcal{B}$  give back  $H(M_i), \sigma$  and  $\mathcal{A}$  generate fogery  $M, \sigma$  to  $\mathcal{B}$ .

in each query step if  $i \neq i^*$   $\mathcal{B}$  would randomly choose  $x_i \in \mathbb{Z}_q$  and compute  $H(M_i) = g^{x_i}$  to  $\mathcal{A}$  only when  $i = i^*$   $\mathcal{B}$  send  $y$  to  $\mathcal{A}$ .  $\mathcal{A}$  know  $g, g^x$  does not know  $x$ .

So  $\text{Pr}[m = m_{i^*}] = 1/q_H$

$\text{Adv}_{CDH} \leq 1/q_H * \text{Adv}_{SIG}[\mathcal{A}, \text{BLS}]$

As  $\text{Adv}_{CDH}$  is negligible,  $\text{Adv}_{SIG}[\mathcal{A}, \text{BLS}]$  is also negligible, so BLS signature is secure.