Assignment 9 – 2021.11.24

Submission deadline: 2021.12.01

BLS signature

Let $e: G_0 \times G_1 \to G_T$ be a pairing where G_0, G_1 and G_T are cyclic groups of prime order q, and $g_0 \in G_0, g_1 \in G_1$ are two generators in the corresponding groups. H is a hash function maps messages to elements in G_0. BLS works as follows:

- $G()$: The key generation algorithm runs as follows

$$\alpha \leftarrow \mathbb{Z}_q, \quad u \leftarrow g_1^\alpha \in \mathbb{G}_1$$

The public key is $pk := u$, and the secret key is $sk := \alpha$.

- $S(sk, m)$: To sign a message $m \in \mathcal{M}$ using a secret key $sk = \alpha \in \mathbb{Z}_q$, do:

$$\sigma \leftarrow H(m)^\alpha \in \mathbb{G}_0, \quad \text{output } \sigma$$

- $V(pk, m, \sigma)$: To verify a signature $\sigma \in \mathbb{G}_0$ on a message $m \in \mathcal{M}$, output accept if

$$e(H(m), u) = e(\sigma, g_1)$$

It can be shown that BLS signature scheme is secure under the co-CDH problem which is described as follows.

co-CDH Problem.

For a given adversary A, the attack game is defined as follows:

- The challenger computes

  $$\alpha, \beta \leftarrow \mathbb{Z}_q, \quad u_0 \leftarrow g_0^{\alpha}, \quad u_1 \leftarrow g_1^{\alpha}, \quad v_0 \leftarrow g_0^{\beta}, \quad z_0 \leftarrow g_0^{\alpha\beta}$$

  And gives the tuple (u_0, u_1, v_0) to the adversary. Notice here α is used twice, once in group G_0 and once in group G_1.

- The adversary outputs some $\widehat{z_0} \in G_0$

The advantage of the attack is defined as coCDHadv[A, e] = Pr($\widehat{z_0} = z_0$)

We say that the co-CDH assumption holds for pairing e if for all efficient adversary A the coCDHadv[A, e] is negligible.

a). Confirm the correctness of the verification step of the BLS signature scheme.

b). Prove BLS signature scheme is secure assuming co-CDH assumption holds in pairing e and H is modeled as a random oracle. (Hint: apply the similar strategy as RSA-FDH)