TD 10: Digital Signature

Exercise 0. [*Homework discussion*]

Exercise 1. [*RO does not exist*]

In this exercise we show a scheme that can be proven secure in the random oracle model, but is insecure when the random oracle model is instantiated with SHA-1 (or any fixed hash function). Let Π be a encryption scheme that is secure in the standard model.
Construct a signature scheme Π_y where the signing is carried out as follows: if $H(0) = y$ then output the secret key, if $H(0) \neq y$ then return a signature computed using Π.

1. Prove that for any value y, the scheme Π_y is secure in the random oracle model.
2. Show that there exists a particular y for which Π_y is insecure when the random oracle model is instantiated with SHA-1.

Exercise 2. [*Using collision resistant hashing for digital signature*]

Recall the definition of a digital signature scheme $\mathcal{S} = (G, S, V)$ given in the course. We present a similar approach as for MACs, that is called **hash-and-sign paradigm**. Let $H : \mathcal{M}' \to \mathcal{M}$ be a hash function where $|\mathcal{M}'| >> |\mathcal{M}|$. Define a new signature scheme $\mathcal{S}' = (G', S', V')$ for the message space $\mathcal{M}'$, as:

$$S'(sk, m) := S(sk, H(m)) \quad \text{and} \quad V'(pk, m, \tau) := V'(pk, H(m), \tau)$$

Show that the signature scheme $\mathcal{S}'$ is secure provided $\mathcal{S}$ is a secure signature scheme, and the hash function H is collision-resistant.

Exercise 3. [*Full domain hash signature scheme*]

Recall the definition of **full domain hash** $\mathcal{S}_{\text{FDH}}$ given in the course. This scheme can be proven to be secure in ROM as long as it uses a secure trapdoor permutation scheme $\mathcal{T}$. Consider a modified scheme, where the scheme does not apply the hash function H to the message, i.e., we define the signature on message $m \in \mathcal{X}$ as $\tau := I(sk, m)$. Could this modified scheme be secure?

Exercise 4. [*Secure pairing-based signature in the ROM*]

In this exercise, we assume we have two cyclic groups G and G_T of the same cardinality q, and a generator g of G. We also assume we have a pairing function $e : G \times G \to G_T$, with the following properties: It is non-degenerate, i.e., $e(g, g) \neq 1$; It is bilinear, i.e., $e(g^a, g^b) = e(g, g)^{ab}$ for all $a, b \in \mathbb{Z}/q\mathbb{Z}$; It is computable in polynomial-time. Note that the bilinearity property implies that $e(g^a, g) = e(g, g^a) = e(g, g)^a$ holds for all $a \in \mathbb{Z}/q\mathbb{Z}$.

1. Show that the Decision Diffie-Hellman problem (DDH) on G can be solved in polynomial-time.
2. We consider the following signature scheme (due to Boneh, Lynn and Shacham):
   - `KeyGen` takes as inputs a security parameter and returns G, g, q, G_T and a description of $e : G \times G \to G_T$ satisfying the properties above. All these are made publicly available. Sample x uniformly in $\mathbb{Z}/q\mathbb{Z}$. The verification key is $vk = g^x$, whereas the signing key is $sk = x$.

- `Sign` takes as inputs sk and a message $M \in \{0,1\}^*$. It computes $h = H(M) \in G$ where H is a hash function, and returns $\sigma = h^x$.
- `Verify` takes as inputs the verification key $vk = g^x$, a message M and a signature σ, and returns 1 if and only if $e(\sigma, g) = e(H(M), vk)$.

Show that this signature scheme is EU-CMA secure (same definition as in the course) under the Computational Diffie Hellman assumption (CDH) relative to G, when $H(\cdot)$ is modeled as a (full-domain hash) random oracle.

Remark. CDH assumption: given a cyclic group G of order q, (g, g^a, g^b) for randomly chosen generator g and $a, b \leftarrow \mathcal{U}(\mathbb{Z}/q\mathbb{Z})$, it is "hard" to compute g^{ab}.