TD 10: Digital Signatures, pt2

Exercise 1. *Plenty of Fish in the Sea*

Let $H : \{0,1\}^{2n} \mapsto \{0,1\}^n$. We say that H is second-preimage resistant if for all efficient adversary $\mathcal{A}$, the probability that $\mathcal{A}$ succeeds in the following experiment is negligible. It is given $x \leftarrow U(\{0,1\}^{2n})$ and it has to find $x' \neq x$ such that $H(x') = H(x)$.

1. Recall the definition of collision resistance. Show that collision resistance implies second-preimage resistance.

2. Assume that there exists a second-preimage resistant $H : \{0,1\}^{2n} \mapsto \{0,1\}^n$. Show that there exists a second-preimage resistance H' that is not collision-resistant.

Exercise 2. *PRF and ROM*

Let $H : \{0,1\}^{2n} \to \{0,1\}^n$ be a random oracle. For $x \in \{0,1\}^n$ and $k \in \{0,1\}^n$, we define F_k as follows:

$$F_k(x) = H(k\|x).$$

The security of a PRF F_k is defined by the following game:

- A random function H, a random $k \in \{0,1\}^n$ and a uniform bit b are chosen.
- If $b = 0$, the adversary $\mathcal{A}$ is given access to an oracle for evaluating $F_k(\cdot)$. If $b = 1$ then $\mathcal{A}$ is given access an oracle for evaluating a random function mapping n-bit inputs to n-bit outputs (which is independent of H).
- $\mathcal{A}$ outputs a bit b', and succeeds if $b = b'$.

Note that during the second step, $\mathcal{A}$ can access H in addition to the function oracle provided by the experiment.
The function F_k is a PRF if for any polynomial-time adversary $\mathcal{A}$, the success probability of $\mathcal{A}$ in the preceding experiment is at most negligibly greater than $1/2$.

1. Show that F_k is a PRF.

Exercise 3. *(blblbl)>* ⋈

In this exercise, we assume we have two cyclic groups G and G_T of the same known prime cardinality p, 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 $a \in \mathbb{Z}/p\mathbb{Z}$.

1. Show that the Decision Diffie-Hellman problem (DDH) on G can be solved in polynomial-time.

We consider the BLS signature scheme (due to Boneh, Lynn and Shacham), which is as follows:

- `KeyGen` takes as inputs a security parameter and returns G, g, p, 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 $\mathbb{Z}/p\mathbb{Z}$. 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 $e(\sigma, g) = e(H(M), vk)$.

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

In cryptographic applications in which signing is performed very frequently (such as for cryptocurrencies), it is interesting to aggregate many signatures for multiple messages into significantly smaller space than required to store all these signatures.

3. Show that that the BLS signature scheme supports aggregation.

4. Propose formal definitions for the functionality and security of an aggregate signature scheme.