TD 8 – Digital signatures

Exercise 1. *DSA*

The *Digital Signature Algorithm* (DSA) is a standardized signature scheme based on the discrete logarithm problem. It uses an indentification protocol, which is transformed into a signature scheme (though not through Fiat-Shamir transform). In the exercise, p is a prime number and $G = \langle g \rangle$ is a (cyclic) subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ of prime order q. We define a pair keys $sk = x \in \{0, \dots, q-1\}$ and $pk = h = g^x$.

1. The identification protocol works as follows:
- The prover chooses $k \twoheadleftarrow \{1, \dots, q-1\}$ and sends $\ell \leftarrow g^k$;
- The verifier chooses α, $r \twoheadleftarrow \{0, \dots, q-1\}$ and sends them;
- The prover computes $s = k^{-1} \cdot (\alpha + xr) \bmod q$;
- The verifier accepts iff $s \neq 0$ and $g^{\alpha \cdot s^{-1}} \cdot h^{r \cdot s^{-1}} = \ell$ (where s^{-1} is the inverse of s modulo q).

i. Prove that if $s \neq 0$, the protocol is correct.

ii. Compute the probability that $s = 0$.

2. To define the DSA signature scheme, we consider a hash function $H : \{0,1\}^* \to \{0, \dots, q-1\}$. To sign with the private key x, the signer simulates the identification protocol, replacing the random choices of α and r by $\alpha \leftarrow H(m)$ and $r \leftarrow \ell \bmod q$. If $s = 0$, the signer restarts with a new value k.

i. Write the algorithm Sign formally. *What should be the output?*

ii. Describe the verification algorithm Vrfy and prove that it is correct.

iii. We define a variant of DSA where the message space is $\{0, \dots, q-1\}$, and where H is simply omitted. Show that this variant is insecure, that is one can forge a signature without knowing the private key. Is this an existential or a universal forgery?

Exercise 2. *BLS signatures*

Let $G = \langle g \rangle$ and $\Gamma = \langle \gamma \rangle$ be two cyclic groups of the same prime order q. We are also given a *pairing*, namely a(n efficiently computable) function $e : G \times G \to \Gamma$ which is *non-degenerate*, i.e., $e(g, g) = \gamma$, and *bilinear*, i.e., $e(g^a, g^b) = \gamma^{ab}$ for all $a, b \in \{0, \ldots, q-1\}$, and a hash function $H : \{0,1\}^* \to G$. The BLS signature scheme[1] is defined by:

- Gen samples $x \twoheadleftarrow \mathbb{Z}/q\mathbb{Z}$ and outputs $(pk, sk) = (g^x, x)$;
- $\mathsf{Sign}_{sk}(m) = H(m)^x$ for a message $m \in \{0,1\}^*$;
- $\mathsf{Vrfy}_{pk}(m, \sigma) = 1$ if and only if $e(\sigma, g) = e(H(m), pk)$.

1. Show that this signature scheme is correct.

We aim to show that the BLS signature scheme is EUF-CMA secure under the CDH assumption in G, when $H(\cdot)$ is modeled as a random oracle. To this end, we prove that any adversary $\mathcal{A}$ in the EUF-CMA game can be used to build an adversary $\mathcal{C}$ in the CDH game.

The adversary $\mathcal{A}$ is given oracle access to $\mathsf{Sign}_{sk}(\cdot)$ by means of oracle accesses to both $H(\cdot)$ and $(\cdot)^{sk}$ and must output a valid pair (m, σ). The goal of $\mathcal{C}$ is, given $h_a = g^a$ and $h_b = g^b$, to compute $h = g^{ab}$. The idea is for $\mathcal{C}$ to simulate the EUF-CMA game, playing the role of the challenger against $\mathcal{A}$.

The adversary $\mathcal{C}$ sets $pk = h_a$ and $sk = a$, even though it does not know its value, and has to answer $\mathcal{A}$'s queries. Let $m_1, \ldots, m_t$ be the queries made by $\mathcal{A}$ to $H(\cdot)$ (in order). We make the strong assumption that the pair (m, σ) output by $\mathcal{A}$ satisify $m = m_t$. To answer a query $H(m_i)$, $1 \leq i < t$, $\mathcal{C}$ samples $r_i \twoheadleftarrow \{0, \ldots, q-1\}$ and outputs $H(m_i) = g^{r_i}$ (retaining the value r_i). To answer $H(m_t)$, $\mathcal{C}$ outputs $H(m_t) = h_b = g^b$.

2. Show that if $\mathcal{A}$ outputs (m, σ) without querying $H(m)$, its advantage is $1/q$.

3. **i.** If $\mathcal{A}$ makes a queries $\mathsf{Sign}_{sk}(m_i)$, show that $\mathcal{C}$ is able to answer the query correctly.

ii. Assume that $\mathcal{A}$ outputs a valid pair (m, σ) where $m = m_t$. Prove that $\mathcal{C}$ can use this result to compute $h = g^{ab}$.

We now want to remove the strong assumption: the message m in the pair output by $\mathcal{A}$ can be any m_i, $1 \leq i \leq t$. As a first step, $\mathcal{C}$ now *guesses* the value of i.[2] The rest remains the same, replacing m_t by m_i. If the guess is incorrect, $\mathcal{C}$ returns FAILURE.

4. **i.** What is the probability that the guess of $\mathcal{C}$ is correct?

ii. Express the advantage and the running time of $\mathcal{C}$ in terms of those of $\mathcal{A}$.

5. Draw a conclusion: Why do the previous questions allow to conclude that if the CDH is hard in G and H is modeled as a random oracle, then the BLS signature scheme is EUF-CMA secure?

[1] Due to Boneh, Lynn and Shacham.

[2] Here we assume that $\mathcal{C}$ knows the value of t and samples $i \twoheadleftarrow \{1, \ldots, t\}$. It is actually possible to perform the same task without knowing t beforehand.