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 $\mathsf{sk} = x \in \{0, \dots, q-1\}$ and $\mathsf{vk} = h = g^x$.

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 $g^{\alpha \cdot s^{-1} \bmod q} \cdot h^{r \cdot s^{-1} \bmod q} = \ell$.

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 key $\mathsf{sk} = x$, 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 signing 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. A *pairing* is an efficiently computable function $e : G \times G \to \Gamma$ such that $e(g^a, g^b) = \gamma^{ab}$ for all a, $b \in \{0, \dots, q-1\}$.

1. Prove that given a pairing, an adversary can win the DDH game in G with high probability.

Given a hash function $H : \{0,1\}^* \to G$, the BLS signature scheme[1] is:

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

2. Show that this signature scheme is correct.

Our goal is to show that the BLS signature scheme is EUF-CMA secure under the CDH assumption in G when H is a random oracle. Given an adversary $\mathcal{A}$ in the EUF-CMA game, we build an adversary $\mathcal{C}$ in the CDH game. The adversary $\mathcal{A}$ sends messages m_i, gets answer $\sigma_i \leftarrow \mathsf{Sign}_{\mathsf{sk}}(m_i)$, 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 play the role of the challenger in the EUF-CMA game against $\mathcal{A}$. It also plays the role of H.
The adversary $\mathcal{C}$ must answer the queries of $\mathcal{A}$, both to H and $\mathsf{Sign}_{\mathsf{sk}}$. It sets the keys $\mathsf{vk} = h_a$ and $\mathsf{sk} = a$. Let $m_1, \ldots, m_t$ be the queries made by $\mathcal{A}$ to H (in order). We make the strong assumption that $\mathcal{A}$ outputs a pair (m, σ) with $m = m_t$. To answer a query $H(m_i)$, $1 \leq i < t$, $\mathcal{C}$ samples $r_i \twoheadleftarrow \{0, \ldots, q-1\}$ and outputs $H(m_i) = g^{r_i}$. To answer $H(m_t)$, $\mathcal{C}$ outputs $H(m_t) = h_b = g^b$.

3. Show that if $\mathcal{A}$ outputs (m, σ) without querying $H(m)$, its advantage is $1/q$. *Hint. H is a random oracle.*

4. **i.** Show that $\mathcal{A}$ is able to answer a query $\mathsf{Sign}_{\mathsf{sk}}(m_i)$ although it does not know $\mathsf{sk} = a$, using its answers to H.

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 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.

5. **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 $\mathcal{A}$.

6. 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.