Proofs of Security
TUT n°2 — Digital signatures

M2-SIF, M2-CRYPTO

Léo Ackermann

Answer all ▸ questions before looking at ⋆ questions.

We start by introducing a few cryptographic games that we will use through this tutorial.

Definition 1 (DL, CDH, DDH, k-SDH) *Let G be a cyclic group of order q, and g a generator of it. The Discrete Logarithm, Computation/Decisional/k-Strong Diffie-Hellmann problems are defined as follows.*

- ***DL.*** *Given (G, q, g, g^a) for $a \hookleftarrow_\$ [q]$, the goal is to recover a.*
- ***CDH.*** *Given (G, q, g, g^a, g^b) for $(a, b) \hookleftarrow_\$ [q]^2$, the goal is to compute g^{ab}.*
- ***DDH.*** *Given (G, q, g) and access to an oracle $\mathcal{O}^{\mathsf{samples}}$, decide whether $\mathcal{O}^{\mathsf{samples}}$ is returning samples of the form (g^a, g^b, g^{ab}) or (g^a, g^b, g^c) for $(a, b, c) \hookleftarrow_\$ [q]^3$.*
- ***k-SDH.*** *Given $(G, q, g, g^a, g^{a^2}, \cdots, g^{a^k})$ for $a \hookleftarrow_\$ \mathbb{Z}_q^\times$, the goal is to produce a tuple of the form $(w, g^{\frac{1}{a+w}})$.*

ElGamal signatures

In 1984, ElGamal proposed a signature scheme based on the discrete logarithm problem. We focus here on its *naive* version*, that consists in the following three algorithms.

- $\mathsf{KeyGen}(1^\lambda)$ takes p prime and compute g a generator of $\mathbb{Z}_p^\times$. It samples uniformly $x \hookleftarrow_\$ \mathbb{Z}_{p-1}^*$, and computes $y = g^x \mod p$. The public key is (p, g, y), the secret key is (p, g, x).
- $\mathsf{Sign}(sk, m \in \mathbb{Z}_{p-1})$ samples $k \hookleftarrow_\$ \mathbb{Z}_{p-1}^*$ and computes $r = g^k \mod p$, $s = (m - xr)/k \mod p - 1$. The signature is the couple (r, s).
- $\mathsf{Verify}(pk, m, (r, s))$ checks that both $r \in \mathbb{Z}_p$ and $s \in \mathbb{Z}_{p-1}$, and that $g^m \equiv y^r \cdot r^s \mod p$.

▸ **Question 1.** *Show that this scheme is correct.*

▸ **Question 2.** *The EUF-KOA security property stands for existentially-unforgeable-against-key-only-attacks, and capture the unability for an adversary to produce a valid message-signature couple without seeing any valid ones. Properly describe the corresponding cryptographic game, precising the advantage of an adversary.*

▸ **Question 3.** *Show that this scheme is not EUF-KOA secure.*

Boneh-Lynn-Shacham signatures

Pairing-based cryptography is the use of a pairing between elements of two cryptographic groups to a third group.

Definition 2 (Pairing) *Let G and G_T be two cyclic group of prime order q respectively written additively and multiplicatively. A (symmetric) pairing is an efficiently computable map $\pi : G \times G \to G_T$ such that*

1. *(Bilinearity)* $\forall (g_1, g_2) \in G^2, (a, b) \in \mathbb{Z}, \pi(g_1^a, g_2^b) = \pi(g_1, g_2)^{ab}$
2. *(Non-degeneracy)* $\forall (g, h) \in G^2, \pi(g, h) = 1$ *if and only if* $g = 1$ *or* $h = 1$.

The BLS signature – for Boneh, Lynn, Shacham – was introduced in 2001 and is as follows.

*In the real scheme, the message is replaced by a hash of the message during the signing and verification procedure.

- $\mathsf{KeyGen}(1^\lambda)$ generates two cyclic groups (G, G_T) of prime order $q = q(\lambda)$ together with a pairing $\pi : G \times G \to G_T$, and select $\mathcal{H}$ a hash function hashing into G. The secret key is $x \leftarrow\!\!\hookleftarrow_{\$} \mathbb{Z}_q^*$, and the public key is (g, g^x) for some generator g of G.
- $\mathsf{Sign}(sk, m)$ returns $\sigma = \mathcal{H}(m)^{sk}$.
- $\mathsf{Verif}(pk, m, \sigma)$ checks that $\pi(\sigma, g)$ and $\pi(\mathcal{H}(m), pk)$ are equal.

▸ **Question 4.** *Is the DDH problem hard in the group G used in BLS?*

▸ **Question 5.** *Show that if the DL problem is hard in G, then the DL problem is hard in G_T.*[†]

▸ **Question 6.** *Show that the BLS signature scheme is EUF-CMA in the random oracle model under the hypothesis that the CDH problem is hard.*

▸ **Question 7.** *Focusing solely on correctness, show how BLS signatures can be compressed in the context of multisignatures, that is a collection $\{\sigma_i\}_i$ of BLS signatures on a same message m – but under different verification keys – can be merged into a meta-signature σ^* that can be verified under a meta public key pk^*.*

Boneh-Boyen signatures

The weak version of the BB signature scheme was introduced by Boneh & Boyen in 2008 as follows. We show that the scheme is $(k-1)$-wEUF-CMA secure in the standard model under the k-SDH hypothesis.

- $\mathsf{KeyGen}(1^\lambda)$ generates keys as in the BLS signature scheme.
- $\mathsf{Sign}(sk, m)$ returns $\sigma \coloneqq g^{\frac{1}{x+m}}$ if $x + m \not\equiv 0 \mod q$, otherwise returns $\sigma \coloneqq 1$.
- $\mathsf{Verify}(pk, \sigma, m)$ checks that $\pi(\sigma, g^x \cdot g^m)$ and $\pi(g, g)$ are equal.

▸ **Question 8.** *The k-wEUF-CMA security property is a variant of EUF-CMA where the adversary only obtains signatures for k messages he chose before obtaining key materials. Properly define the associated game and advantage.*

▸ **Question 9.** *Show that, for $k > k' \in \mathbb{N}$, the k-SDH problem reduces to the k'-SDH problem.*[‡]

▸ **Question 10.** *(Simulation of KeyGen, 1/2). Given as input $(m_1, \cdots, m_k)$ from $\mathcal{A}_{\mathsf{wEUF\text{-}CMA}}$ ($\mathcal{A}$ for short), $\mathcal{B}_{\mathsf{SDH}}$ ($\mathcal{B}$ for short) needs to simulate the KeyGen step of the BB signature scheme. Let $P(X) = \prod_{i=1}^{k-1}(X + m_i)$. The algorithm $\mathcal{B}$ wants to ouput $\mathsf{pk} \coloneqq (g^{P(a)}, g^{aP(a)})$, where a is the random value from the SDH challenge. Show how $\mathcal{B}$ can compute such a public key. What is the associated secret key?*

▸ **Question 11.** *(Simulation of KeyGen 2/2). Is the distribution of the simulation of KeyGen equal to the distribution of the real KeyGen. This is crucial, as we want $\mathcal{A}$ to behave exactly as if it was really attacking the signature scheme.*

▸ **Question 12.** *(Simulation of Sign). Show how $\mathcal{B}$ can produce valid signatures $(\sigma_i)_i$ for the messages $(m_i)_i$.*

▸ **Question 13.** *(Extraction of the solution). Show how $\mathcal{B}$ can produce a valid solution for SDH given (m^*, σ^*), a valid forgery handed by $\mathcal{A}$. You may show that $\sigma^* = g^{P(a)/(a+s)}$*[§] *for some s, decompose $P(a)$ by Euclidean division, and finally show how to recover $g^{1/(a+s)}$ from σ^* (re-using the SDH group elements given as input).*

▸ **Question 14.** *Conclude.*

[†] In this case, we say that DL_G *reduces to* DL_{G_T}.

[‡] As a consequence, one can consider for simplicity that an adversary for k-wEUF-CMA makes exactly k signing requests. Indeed, if it asks for $k' < k$ signatures, the reduction will be from k'-SDH, and the later reduces from k-SDH.

[§] We denote by a the underlying secret quantity of the k-SDH instance we are dealing with.