# TD 10: Digital Signatures

**Exercise 1.**
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-3 (or any fixed (unkeyed) hash function $H : \{0,1\}^* \to \{0,1\}^n$). Let $\Pi$ be a signature scheme that is euCMA-secure in the standard model.
Let $y \in \{0,1\}^n$ and define the following signature scheme $\Pi_y$. The signing and verifying keys are obtained by running $\Pi.\mathsf{Gen}(1^\lambda)$. Signature of a message $m$ is computed out as follows: if $H(0) = y$ then output the secret key, if $H(0) \neq y$ then return a signature computed using $\Pi.\mathsf{Sign}$. To verify a message, if $y = H(0)$ then accept any signature for any message and otherwise, verify it using $\Pi.\mathsf{Verify}$.

1. Prove that for any value $y$, the scheme $\Pi_y$ is euCMA-secure in the random oracle model.
2. Show that there exists a particular $y$ for which $\Pi_y$ is insecure when the hash function is not modeled as a random oracle anymore.

**Exercise 2.**
Define a lattice-based Schnorr-like signature scheme as follows:

$\mathsf{Gen}(1^\lambda)$**:** Sample $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{n\times n})$, $\mathbf{S}, \mathbf{E} \hookleftarrow U((-B,B]^{n\times n})$. Return $vk = (\mathbf{A}, \mathbf{T} = \mathbf{AS} + \mathbf{E}, H)$ with $H$ a hash function modeled as a random oracle with values in $\{0,1\}^{n\times n}$ and $sk = (\mathbf{S}, \mathbf{E})$.

$\mathsf{Sign}(sk, \mu)$**:** To sign a message $\mu \in \{0,1\}^\star$, do the following:

1. (Commit) Sample $\mathbf{S}', \mathbf{E}' \hookleftarrow U((-B,B]^{n\times n})$ and compute $\mathbf{T}' = \mathbf{AS}' + \mathbf{E}'$;
2. (Challenge) Compute $\mathbf{C} = H(\mu||\mathbf{T}')$;
3. (Response) Compute $\mathbf{Z}_1 = \mathbf{S}' + \mathbf{SC}, \mathbf{Z}_2 = \mathbf{E}' + \mathbf{EC}$.
4. Output $(\mathbf{C}, \mathbf{Z}_1, \mathbf{Z}_2)$.

$\mathsf{V}(vk, (\mathbf{C}, \mathbf{Z}_1, \mathbf{Z}_2), \mu)$**:** To verify the signature:

1. Compute $\mathbf{T}' = \mathbf{AZ}_1 + \mathbf{Z}_2 - \mathbf{TC}$;
2. Accept if $\mathbf{C} = H(\mu||\mathbf{T}')$.

1. Would the scheme be euCMA secure if $\mathbf{S}$ and $\mathbf{E}$ were sampled as vectors in $(-B,B]^n$ instead of $(-B,B]^{n\times n}$?
2. Is it hard to find a forgery for this scheme?
3. Explain how to tweak to above scheme to prevent the above attack by imposing an additional validity check regarding the norm of $\mathbf{Z}_1, \mathbf{Z}_2$. Show that the secret key owner can still sign.
4. Show that if the resulting scheme is still not euCMA secure.

The solution to make the scheme secure is to force the distribution of $\mathbf{Z}_1, \mathbf{Z}_2$ to be independent of the secret key. This is done by a technique called rejection sampling, or by noise flooding.

**Exercise 3.**
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 $\sigma$, 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.