École normale supérieure **2022-2023**
Département d'informatique

Introduction à la cryptologie
TD n° 7 : Cryptography via Pairings and Lattices.

Exercice 1 (BLS Signatures)**.** Let $\mathbb{G}$ be a group with generator g and bilinear pairing $e : \mathbb{G} \times \mathbb{G} \mapsto \mathbb{G}_T$. Recall that to sign a message m, the signer outputs $\sigma = H(m)^x$, where $y = g^x$ is the public key.

1. Recall the verification algorithm.
2. Show that it is hard to output a signature on an arbitrary message m^* under the CDH assumption, even given access to a signature oracle, provided m^* was never queried. For this, we model the H as a programmable random oracle. That is, the challenger can program the oracle output in the security game with chosen random values.

Next, we to construct a signature issuance protocol, where the signer does not learn the message it signed. The scheme should remain unforgeable, that is a user should obtain at most Q valid signatures from Q signing sessions.

3. Propose such a protocol.
   Hint : The user sends $A = rand(H(m), r)$ to the signer, where $rand$ is an appropriate randomization function that allows to recover a valid signature given $B = A^x$ and r.
4. Show that the scheme is blind, i.e., the user cannot distinguish between signing m_0 or m_1 first, when presented signatures σ_0 and σ_1 on m_0 and m_1, respectively.
5. Show that the scheme is unforgeable if H is modeled as a programmable random oracle, assuming the One-more CDH assumption holds. That is, the adversary $\mathcal{A}$ has access to two oracles, the first oracle $(\cdot)^x$ outputs h^x given h and the second oracle outputs challenges h_i. The assumption is that $\mathcal{A}$ cannot compute h_i^x for $Q+1$ different h_i efficiently, given $(\cdot)^x$ was queried at most Q times.
6. Is the One-more CDH assumption reasonable ?

Exercice 2 (IBE-based signatures)**.** Recall that identity-based encryption allows to encrypt a message under unstructured public key, for example an email address. An IBE scheme consists of algorithms ($Setup, Extract, Encrypt, Decrypt$). $Setup$ generates system parameters, denoted by $params$, and a master key mk. $Extract$ receives an identity id and the master key mk as input and outputs a private key pk_{id}. $Encrypt$ encrypts messages for a given identity id (via $params$) and $Decrypt$ decrypts ciphertexts using the private key.

1. What should be hard for an adversary in the context of IBE ?
2. Give a generic construction of a signature scheme given any IBE scheme.
   Hint : Identify the identities with messages.
3. Apply the transformation to Boneh-Franklin IBE and simplify the verification algorithm. Is the scheme familiar ?

Again, let $\mathbb{G}$ be a group with generator g and bilinear pairing $e : \mathbb{G} \times \mathbb{G} \mapsto \mathbb{G}_T$. A well-known signature scheme obtained via this transformation are Boneh-Boyen signatures :

— $KeyGen()$: samples $\alpha, \beta, \gamma \leftarrow \mathbb{Z}_p$, and sets $u = g^\alpha, h = g^\gamma, v = e(g,g)^{\alpha\beta}$, and outputs $pk = (u, h, v)$ and $sk = g^{\alpha\beta}$,
— $Sign(sk, m)$: samples $r \in \mathbb{Z}_p$ and outputs $(\sigma_1, \sigma_2) = (sk \cdot (u^m h)^r, g^r) \in \mathbb{G}^2$,
— $Verify(pk, m, (\sigma_1, \sigma_2))$: outputs 1 if $e(\sigma_1, g) = v \cdot e(\sigma_2, u^m h)$, and otherwise outputs 0.

The rest of the exercise is about Boneh-Boyen signatures.

4. We want to show selective unforgeability : the user should not be able to forge a signature for a message fixed m^* chosen before seeing the public key. Given the structure of the scheme, what seems to be the underlying hardness assumption ?
5. Show that given $A = g^\alpha, B = g^\beta$, the public key $pk = (A, A^{-m^*} \cdot g^\delta)$ is indistinguishable from a public key output by $KeyGen$.

6. Show that the scheme is selectively unforgeable under the CDH assumption.

   Hint : Setup the public key as above for a CDH challenge (A, B). To sign a message $m_i \neq m^*$, draw $\tilde{r}_i \leftarrow \mathbb{Z}_p$, set $\sigma_2 = g_1^{\tilde{r}_i} \cdot B^{-1(m_i - m^*)}$, and recompute an appropriate σ_1. Finally, show that a valid signature on m^* allows to break CDH.

7. Is selective security satisfying in practice ?

8. Show that the scheme is rerandomizable, i.e., given a signature on a message m you can make it look like a random signature on message m.

9. Modify the Boneh-Boyen scheme such that it unforgeable (for arbitrary messages). Feel free to use a programmable random oracle.

Exercice 3 (Lattice-based encryption)**.** We consider the Regev encryption system given below :

— *KeyGen*(1^λ) : set $A = \begin{bmatrix} \bar{A} \\ \bar{s}^T \bar{A} + e^T \end{bmatrix} \in Z_p^{n \times m}$ and $s^T = [-\bar{s}^T \mid 1]$, and output public key A and secret key s. Note that e is a small random error and $\bar{A}, \bar{s}$ are random values.

— *Encrypt*(μ) : for $\mu \in \{0, 1\}$, sample $r \leftarrow \{0, 1\}^m$ and output $c = Ar + \begin{bmatrix} 0^{n-1} \\ \lfloor q/2 \rceil \cdot \mu \end{bmatrix}$.

1. How would you decrypt the ciphertext c ?

2. Argue that the scheme is secure under the LWE assumption.

   Hint : Ar is (almost) uniform if A and r is drawn at random.

3. Show that the scheme is additively homomorph.

4. What happens if you multiply ciphertexts ? Can you still decrypt ?

5. Assume we have an encryption scheme that allows for N additions and M multiplications, and that decryption can be implemented with less than N additions and M multiplications [1]. Propose a scheme that allows for an unbounded number of multiplications and additions.

   Hint : Add an encryption of the secret key to the public key.

1. The Regev encryption scheme can be adapted to fulfil this property.