# Homework (due before April, 8th. 3.45pm)

**Exercise 1.** *multi-bit Encryption with LWE*

Let four integers $n, m, q, B$. Recall the Learning with Errors (with small secret) assumption[1] $\mathsf{LWE}_{n,m,q,B}$: the distributions $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e})$ and $(\mathbf{A}, \mathbf{b})$ are computationally indistinguishable, where $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m\times n})$, $\mathbf{s} \hookleftarrow U((-B, B]^n)$, $\mathbf{e} \hookleftarrow U((-B, B]^m)$ and $\mathbf{b} \hookleftarrow U(\mathbb{Z}_q^m)$.

Let $k$ be another nonzero integer. We define the multi-secret Learning with Errors (with small secret) assumption $\mathsf{msLWE}_{n,m,q,B,k}$ as follows: the distributions $(\mathbf{A}, \mathbf{A}\mathbf{s}_1 + \mathbf{e}_1, \mathbf{A}\mathbf{s}_2 + \mathbf{e}_2, \ldots, \mathbf{A}\mathbf{s}_k + \mathbf{e}_k)$ and $(\mathbf{A}, \mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$ are computationally indistinguishable, where $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m\times n})$, $\mathbf{s}_i \hookleftarrow U((-B, B]^n)$, and $\mathbf{e}_i \hookleftarrow U((-B, B]^m)$ and $\mathbf{b}_i \hookleftarrow U(\mathbb{Z}_q^m)$ for any $i \leq k$.

1. Prove that, under the $\mathsf{LWE}_{n,m,q,B}$ assumption, the $\mathsf{smLWE}_{n,m,q,B,k}$ assumption holds for any polynomial $k$. *Hint: use an hybrid argument.*

2. Adapt the LWE-based encryption scheme from the lecture and propose a public encryption scheme with message space $\{0, 1\}^k$. Under which constraint is it correct? Prove that it is CPA-secure under the $\mathsf{msLWE}_{n,m,q,B,k}$ assumption.

3. Is this scheme IND-CCA2 secure? If not, what can we do to turn it into an IND-CCA2 secure scheme?

**Exercise 2.** *OW-CPA implies IND-CPA*

Let $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme with message space $\{0, 1\}^n$ and a hash function $H : \{0, 1\}^n \to \{0, 1\}^n$ modelled as a Random Oracle. We build the following encryption scheme $\mathsf{PKE}'$:

$\mathsf{Gen}'(1^\lambda)$**:** Run and return $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$.

$\mathsf{Enc}'(1^\lambda)$**:** Sample $x \leftarrow \{0, 1\}^n$. Return $c_0 := m \oplus H(x)$ and $c_1 := \mathsf{Enc}(\mathsf{pk}, x)$.

1. Give a decryption algorithm. Prove that the scheme is correct, assuming that PKE is correct.

We briefly recall the OW-CPA security game: the adversary is given a ciphertext, which is an encryption of an uniformly sampled message among the (finite) message space. The adversary wins if and only if it outputs the message. A PKE scheme is OW-CPA secure if no ppt adversary has non-negligible probability of winning.

2. Let $\mathcal{A}$ be an adversary against the IND-CPA security of the scheme. Let $c_0 := m_b \oplus H(x^*)$ and $c_1 := \mathsf{Enc}(\mathsf{pk}, x^*)$ be the challenge ciphertext. Let $QUERY$ be the event "$\mathcal{A}$ queries the random oracle on input $x^*$". Give an upper bound on the advantage of $\mathcal{A}$ as a function of $\Pr(QUERY)$.

3. Assuming that PKE is OW-CPA secure, show that $\mathsf{PKE}'$ is IND-CPA secure.

**Exercise 3.** *Lamport's signature*

The notion of existential unforgeability under single-message attack for a signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{V})$ states that no adversary can output a valid tuple $(m', \sigma)$ with non-negligible probability by only querying once the signing oracle for $m$ with $m \neq m'$.

1. Give a formal definition of the euSMA-security.

[1] We used to call it $\mathsf{ssLWE}_{n,m,q,B}$ in the previous tutorials

Let $H : \{0,1\}^n \to \{0,1\}^k$ with $k < n/2$ be a collision resistant hash function. We say that $H$ is preimage resistant if no ppt adversary, given $y = H(x)$ for $x$ uniformly sampled, is able to compute $x'$ such that $H(x') = y$ with non-negligible probability.

2. Show that if $H$ is collision-resistant then it is preimage resistant.

Lamport's signature scheme for messages of length $\ell$ is as follows:

$\mathsf{Gen}(1^\lambda)$**:** Choose uniformly $x_{i,b} \hookleftarrow U(\{0,1\}^n)$ for any $(i,b) \in [1,\ell] \times \{0,1\}$. Return $vk := \{y_{i,b} := H(x_{i,b}), (i,b) \in [1,\ell] \times \{0,1\}\}$ and $sk := \{x_{i,b}, (i,b) \in [1,\ell] \times \{0,1\}\}$.

$\mathsf{Sign}(sk, m)$**:** To sign $m = (m_1, \ldots, m_\ell) \in \{0,1\}^\ell$, return $(x_{1,m_1}, \ldots, x_{\ell,m_\ell})$.

$\mathsf{V}(vk, m, (x_1, \ldots, x_\ell))$**:** To verify a signature, compute $H(x_i) =: y'_i$ for any $i \in [1,\ell]$. Return 1 if and only if $y'_i = y_{i,m_i}$ for all $i \in [1,\ell]$.

3. Is this scheme euCMA-secure?

4. Assuming that the hash function is preimage resistant, show the euSMA-security of the scheme.

**Exercise 4.** *Attacks on ElGamal*

We consider the following signature scheme. Let $p$ be a prime integer and $g$ be a generator of $\mathbb{Z}_p^\star$. The element $x \in \mathbb{Z}_{p-1}$ is uniformly chosen, and we compute $y = g^x \bmod p$. The public key is $(p, g, y)$ and the secret key is $x$.

- To sign $m \in \mathbb{Z}_{p-1}$, choose $k \in \mathbb{Z}_{p-1}^\star$ uniformly at random and compute $r = g^k \bmod p$ as well as $s = (m - xr)/k \bmod p - 1$. The signature is $(r, s)$.
- To verify $(m, (r, s))$, accept if and only if $(r, s) \in \mathbb{Z}_p^\star \times \mathbb{Z}_{p-1}$ and $g^m = y^r r^s \bmod p$.

We now study the security of this scheme.

1. Show the correctness of this scheme.

2. Give a key only attack (i.e. without querying a signature) against the existential unforgeability.

   *Hint: try with* $r = g^a y^b \bmod p$ *for some well-chosen* $a$ *and* $b$ *and then find* $s$ *and* $m$ *such that* $(r, s)$ *is a valid signature for* $m$*.*