TD 9: IND-CCA Security - Signature

Exercise 1.
Recall the ElGamal public key encryption scheme from the lecture.

- $\mathsf{KeyGen}(1^\lambda)$: Choose a group G with generator g and order $p = O(2^\lambda)$. Sample $x \hookleftarrow U(\mathbb{Z}_p)$ and return:
$$\mathsf{pk} := (G, g, p, g^x) \text{ and } \mathsf{sk} := x.$$
- $\mathsf{Enc}(\mathsf{pk}, m \in G)$: Sample $r \hookleftarrow U(\mathbb{Z}_p)$ and output $(c_1, c_2) = (g^r, (g^x)^r \cdot m)$.
- $\mathsf{Dec}(\mathsf{sk}, c_1, c_2)$: output $m = c_2 \cdot c_1^{-\mathsf{sk}}$.

1. Show that for any $m, m' \in G$, and $(c_1, c_2) := \mathsf{Enc}(\mathsf{pk}, m)$ and $(c_1', c_2') := \mathsf{Enc}(\mathsf{pk}, m')$, it holds that $(c_1 \cdot c_1', c_2 \cdot c_2')$ is a valid ciphertext for $m \cdot m'$. We say that the scheme is homomorphic for multiplication.
2. Provide a modification of the scheme such that it is now *additively* homomorphic instead of multiplicatively. *Hint: you may want to choose $\mathcal{M} = \{m \in \mathbb{Z}_p, |m| \leq \mathsf{poly}(\lambda)\}$ as your message space.*
3. Show that the (genuine) ElGamal encryption scheme is not IND-CCA2 secure.
Remark: No homomorphic encryption scheme can be IND-CCA2 secure.

Exercise 2.
We are looking here at different modifications of the Fujisaki-Okamoto (FO) transform that fail at providing CCA2 security. Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme assumed to be IND-CPA secure with message space $\{0,1\}^{k+\ell}$. We recall the FO transform, where H is a hash function that is modeled as a RO.

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

$\mathsf{Enc}'(pk, m \in \{0,1\}^k)$**:** Sample $r \hookleftarrow U(\{0,1\}^\ell)$ and return $c = \mathsf{Enc}(pk, m||r; H(m||r))$, where $H(m||r)$ is the randomness used by the algorithm.

$\mathsf{Dec}'(sk, c)$**:** Compute $m||r \leftarrow \mathsf{Dec}(sk, c)$ and return m if $c = \mathsf{Enc}(pk, m||r; H(m||r))$. Otherwise, return $\perp$.

1. What happens if $\ell = O(\log(\lambda))$?
2. Show that there exists an IND-CPA secure encryption scheme such that if we always return m in the decryption algorithm, without checking the consistency of the randomness used in the ecnryption, then its FO transform is not IND-CCA2 secure.

Exercise 3.
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 Π be a signature scheme that is euCMA-secure in the standard model.
Let $y \in \{0,1\}^n$ and define the following signature scheme Π_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 Π_y is euCMA-secure in the random oracle model.
2. Show that there exists a particular y for which Π_y is insecure when the hash function is not modeled as a random oracle anymore.