TD 8: IND-CCA Encryptions (corrected version)

Exercise 1. *CCA1 vs CCA2*

Let $\Pi_0 = (\mathsf{Keygen}_0, \mathsf{Encrypt}_0, \mathsf{Decrypt}_0)$ be an IND-CCA2-secure public-key encryption scheme which only encrypts single bits (i.e., the message space is $\{0,1\}$). We consider the following multi-bit encryption scheme $\Pi_1 = (\mathsf{Keygen}_1, \mathsf{Encrypt}_1, \mathsf{Decrypt}_1)$, where the message space is $\{0,1\}^L$ for some L polynomial in the security parameter λ.

$\mathsf{Keygen}_1(1^\lambda)$: Generate a key pair $(PK, SK) \leftarrow \Pi_0.\mathsf{Keygen}_0(1^\lambda)$. Output (PK, SK).

$\mathsf{Encrypt}_1(PK, M)$: In order to encrypt $M = M[1] \dots M[L] \in \{0,1\}^L$, do the following.

1. For $i = 1$ to L, compute $C[i] \leftarrow \Pi_0.\mathsf{Encrypt}_0(PK, M[i])$.
2. Output $C = (C[1], \dots, C[L])$.

$\mathsf{Decrypt}_1(SK, C)$ Parse the ciphertext C as $C = (C[1], \dots, C[L])$. Then, for each $i \in \{1, \dots, L\}$, compute $M[i] = \Pi_0.\mathsf{Decrypt}_0(SK, C[i])$. If there exists $i \in \{1, \dots, L\}$ such that $M[i] = \perp$, output $\perp$. Otherwise, output $M = M[1] \dots M[L] \in \{0,1\}^L$.

1. Show that Π_1 does not provide IND-CCA2 security, even if Π_0 is secure in the IND-CCA2 sense.

☞ Assume $L = 2$. Let $M_0 = 01$ and $M_1 = 10$. Given the challenge $C = (C_0, C_1)$, query (C_0, C_0) and (C_1, C_1), which are both different from C by perfect correctness, to the decryption oracle. Then deduce the value of b such that M_b was encrypted. if $L > 2$, then pad the messages with 0's.

Let $\Pi = (\mathsf{Keygen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ be an IND-CCA2-secure public-key encryption scheme with message space $\{0,1\}^L$ for some $L \in \mathbb{N}$. We consider the modified public-key encryption scheme $\Pi' = (\mathsf{Keygen}', \mathsf{Encrypt}', \mathsf{Decrypt}')$ where the message space is $\{0,1\}^{L-1}$ and which works as follows.

$\mathsf{Keygen}'(1^\lambda)$: Generate two key pairs $(PK_0, SK_0) \leftarrow \mathsf{Keygen}(1^\lambda)$, $(PK_1, SK_1) \leftarrow \mathsf{Keygen}(1^\lambda)$.
Define $PK := (PK_0, PK_1)$, $SK := (SK_0, SK_1)$.

$\mathsf{Encrypt}'(PK, M)$: In order to encrypt $M \in \{0,1\}^{L-1}$, do the following.

1. Choose a random string $R \leftarrow U(\{0,1\}^{L-1})$ and define $M_L = M \oplus R \in \{0,1\}^{L-1}$ and $M_R = R$.
2. Compute $C_L \leftarrow \Pi.\mathsf{Encrypt}(PK_0, 0||M_L)$ and $C_1 \leftarrow \Pi.\mathsf{Encrypt}(PK_1, 1||M_R)$.

Output $C = (C_L, C_R)$.

$\mathsf{Decrypt}'(SK, C)$ Parse C as (C_L, C_R). Then, compute $\tilde{M}_L = \Pi.\mathsf{Decrypt}(SK_0, C_L)$ and $\tilde{M}_R = \Pi.\mathsf{Decrypt}(SK_1, C_R)$. If $\tilde{M}_L = \perp$ or $\tilde{M}_R = \perp$, output $\perp$. If the first bit of M_L (resp. M_R) is not 0 (resp. 1), return $\perp$. Otherwise, parse $\tilde{M}_L$ as $0||M_L$ and $\tilde{M}_R$ as $1||M_R$, respectively, where $M_L, M_R \in \{0,1\}^{L-1}$, and output $M = M_L \oplus M_R \in \{0,1\}^{L-1}$.

2. Show that the modified scheme Π' does not provide IND-CCA2 security, even if the underlying scheme Π does.

☞ If C_0, C_1 is the challenge reply for any messages $M_0 \neq M_1$ we have chosen, then create $C_1' = Enc(pk_1, 1\|0^{L-1})$ and query $Dec(C_0, C_1')$. This gives $M_b \oplus R$. Similarly, create $C_0' = Enc(pk_0, 0\|0^{L-1})$ and query $Dec(C_0', C_1)$. This gives R. M_b is $M_b \oplus R \oplus R$.

3. Show that, if Π provides IND-CCA1 security, so does the modified scheme Π'. Namely, show that an IND-CCA1 adversary against Π' implies an IND-CCA1 adversary againt Π.

☞

Let us build a reduction $\mathcal{B}$ from an adversary $\mathcal{A}$ against the IND-CCA1 security of Π'. The reduction $\mathcal{B}$ is an adversary against the IND-CCA1 security of Π. On input a public key pk, it samples $pk_1, sk_1 \leftarrow Gen(1^\lambda)$ and sends pk, pk_1 to $\mathcal{A}$. Whenever $\mathcal{A}$ makes a decryption query $c = (C_L, C_R)$, the reduction $\mathcal{B}$ sends C_L to its decryption oracle, and it decrypts C_R using the secret key sk_1. Given these two decryptions, it can complete the decryption and it returns the message to $\mathcal{A}$. Given a challenge M_0, M_1, the reduction $\mathcal{B}$ samples R uniformly and sends $0||(M_0 \oplus R), 0||(M_1 \oplus R)$ as its own challenge and gets $C_L^\star$. Using pk_1, the reduction then encrypts $1||R$, gets $C_R^\star$ and returns the couple $(C_L^\star, C_R^\star)$ to $\mathcal{A}$. Note that this couple is a valid encryption of M_b, generated (in $\mathcal{A}$'s view) following the encryption algorithm of Π'. When the adversary outputs a bit, the reduction outputs the same.

It holds then that the advantage of the reduction is the same as the one of the adversary. This proves that if Π is IND-CCA1 secure, then so is Π'.

We have in particular proven that the existence of IND-CCA2 secure schemes implies the existences of IND-CCA1 secure schemes that are not IND-CCA2.

Exercise 2. *ElGamal Encryption*

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.

☞ we have $c_2 \cdot c_2' = (c_1 \cdot c_1')^x \cdot m \cdot m'$. This is a valid encryption for mm', i.e. the decryption algorithm called on this ciphertext returns $m \cdot m'$.

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.*

☞ Instead of encrypting an element of G, we choose to encrypt an element of $\mathcal{M}$. We keep the keygen and change the encryption scheme: $\mathsf{Enc}'(\mathsf{pk}, m) = \mathsf{Enc}(\mathsf{pk}, g^m)$. However, to decrypt, we need to do more: $\mathsf{Dec}'(\mathsf{sk}, c = \mathsf{Enc}'(\mathsf{pk}, m))$ recovers g^m with $\mathsf{Dec}(\mathsf{sk}, c)$. With our choice of message space, it is possible to brute force in polynomial time the Discrete Logarithm Problem, and recover m from g^m.

With the same trick as in the previous question, we get that our scheme is homomorphic, but this time additively: we get an encryption of $m + m'$, which is still polynomial in λ.

3. Show that the (genuine) ElGamal encryption scheme is not IND-CCA2 secure.

☞ Let $m_0 \neq m_1 \in G$. Let $c_1', c_2' = \mathsf{Enc}(\mathsf{pk}, g)$. When given c_1, c_2 encrypting either m_0 or m_1, it is still possible to query the decryption oracle for $(c_1 c_1', c_2 c_2')$ which returns either $m_0 g$ or $m_1 g$, which are different. It is then possible to win the IND-CCA2 security game with probability 1.

Remark: No homomorphic encryption scheme can be IND-CCA2 secure.

Exercise 3. *LPS Encryption*

Recall the LWE-based encryption scheme from the lecture.

- $\mathsf{KeyGen}(1^\lambda)$: Let m, n, q, B be integers such that $m > n$ and $q > 12mB^2$. Sample $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$, $\mathbf{s} \hookleftarrow U((-B, B]^n)$ and $\mathbf{e} \hookleftarrow U((-B, B]^m)$. Return
$$\mathsf{pk} := (\mathbf{A}, b = \mathbf{A}\mathbf{s} + \mathbf{e}) \text{ and } \mathsf{sk} := \mathbf{s}.$$
- $\mathsf{Enc}(\mathsf{pk}, m \in \{0, 1\})$: Sample $(\mathbf{t}, \mathbf{f}, f') \hookleftarrow U((-B, B]^m \times (-B, B]^n \times (-B, B])$ and output
$$(c_1, c_2) = (\mathbf{t}^\top \mathbf{A} + \mathbf{f}^\top, \mathbf{t}^\top \mathbf{b} + f' + \lfloor \frac{q}{2} \rfloor m).$$

- $\mathsf{Dec}(\mathsf{sk}, c_1, c_2)$: take the representative of $\mu = c_2 - c_1 \cdot \mathsf{sk}$ in $(-q/2, q/2]$ and return 0 if it has norm $< q/4$, 1 otherwise.

1. Show that this scheme is not IND-CCA2 secure.

   ☞ Let $\mathcal{A}$ be the adversary, that, given an encryption (c_1, c_2) of either 0 or 1, queries the decryption oracle for $(c_1, c_2 + 1 \bmod q)$ and returns its output. Let $\bar{\mu}$ denote the representative in $(-q/2, q/2]$ of $c_2 - c_1 \cdot \mathsf{sk}$. It fails if and only if $|\bar{\mu}| = \lfloor q/4 \rfloor - 1$ (it returns 1 when the message is 0) or $\bar{\mu} = \lfloor q/2 \rfloor - 1$ (it returns 0 when the message is 1). In terms of advantage, it holds:

   $$|1 - \Pr(\bar{\mu} = \lfloor q/4 \rfloor - 1 | m = 0) - \Pr(\bar{\mu} = \lfloor q/2 \rfloor - 1 | m = 1)| = \mathsf{Adv}(\mathcal{A}).$$

   The left hand side is non-negligible. Indeed, recall that $c_2 - c_1 \cdot \mathsf{sk} = \mathbf{t}^\top \cdot \mathbf{e} + f' - \mathbf{f}^\top \mathbf{s} + \lfloor \frac{q}{2} \rfloor \cdot m$, where $m = 0$ or 1. The probability of getting $\bar{\mu} = \lfloor q/4 \rfloor - 1$ or $\lfloor q/2 \rfloor - 1$ is not close to 1.

Exercise 4. *Fujisaki-Okamoto Transform*

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 $\ell = O(\log(\lambda))$?

   ☞ One can try to guess r: after a challenge phase where the adversary gets $c^\star$ which is an encryption of either m_0 or m_1, sample $r \hookleftarrow U(\{0,1\}^\ell)$ and compute $c_0 = \mathsf{Enc}(pk, m_0||r, H(m_0||r))$ and $c_1 = \mathsf{Enc}(pk, m_1||r, H(m_1||r))$. If there exists $b \in \{0,1\}$ such that $c_b = c^\star$, return it. Otherwise return a uniform bit.

   The advantage of this adversary is equal to the probability of guessing the right r which happens with probability $O(1/\lambda)$, which is non-negligible.

For the next questions, do not forget to look at the previous exercises.

2. Show that there exists an IND-CPA secure encryption scheme such that if we replace every instance of $H(m||r)$ with $H(r)$, then its FO transform is not IND-CCA2 secure.

   ☞ We use the Frodo encryption scheme here (LWE is not enough as its message space is not big enough). Given an encryption $(c_1^\star, c_2^\star)$ of either 0^k or $0^{k-1}1$, one can query the decryption oracle for $(c_1^\star, c_2^\star + \lfloor \frac{q}{2} \rfloor (0 \ldots 0\ 1\ 0))$. This a valid encryption of either $0^{k-2}10$ or $0^{k-2}11$ with the same randomness as $(c_1^\star, c_2^\star)$. Then the decryption oracle returns (almost) the encrypted challenge message. This adversary then has advantage 1 in the CCA2 game.

3. 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.

   ☞ We can for instance use the ElGamal encryption scheme. In this case, when we get $c^\star = (g^{H(m_b||r)}, pk^{H(m_b||r)} \cdot (m_b||r))$ we can query the decryption algorithm for $g \cdot g^{H(m_b||r)}, pk \cdot pk^{H(m_b||r)} \cdot (m_b||r)$, which will return m_b, letting us win the game with probability 1.