Exercise 1. CCA Security

We define the scheme "Encrypt and tag" by: for a message $m$, independent keys $k$ and $k'$, a CPA-secure encryption $Enc$ and a secure MAC $Sign$, let $c = Enc(k, m)$ and $t = Sign(k', m)$, return $(c, t)$. Is this scheme CCA-secure?

Exercise 2. MACs and CCA

Consider the following construction of symmetric encryption.

$Gen(1^\lambda)$: Choose a random key $K_1 \leftarrow U\{0,1\}^\lambda$ for an IND-CPA secure symmetric encryption scheme $(Gen', Enc', Dec')$. Choose a random key $K_0 \leftarrow U\{0,1\}^\lambda$ for a MAC $\Pi = (Gen, Mac, Verify)$.

The secret key is $K = (K_0, K_1)$

$Enc(K, M)$: To encrypt $M$, do the following.
1. Compute $c = Enc'(K_1, M)$.
2. Compute $t = \Pi.Mac(K_0, c)$.

Return $C = (t, c)$.

$Dec(K, C)$: Return $\bot$ if $\Pi.Verify(K_0, c, t) = 0$. Otherwise, return $M = Dec'(K_1, c)$.

1. Show that the scheme is not IND-CCA secure if the MAC $\Pi$ is only unforgeable (i.e., not strongly) under chosen-message attacks.

2. Prove that the scheme is IND-CCA secure assuming that: (i) $(Gen', Enc', Dec')$ is IND-CPA-secure; (ii) $\Pi$ is strongly unforgeable under chosen-message attacks.

Exercise 3. Repetitions

Let $(Gen, H)$ be a collision-resistant hash function. Is $(Gen, \widehat{H})$ defined by $\widehat{H}^\circ = \text{def} H^\circ(H^\circ(x))$ necessarily collision-resistant?

Exercise 4. HMAC

Before HMAC was invented, it was quite common to define a MAC by $\text{Mac}_t(m) = H^t(k \parallel m)$ where $H$ is a collision-resistant hash function. Show that this is not a secure MAC when $H$ is constructed via the Merkle-Damgård transform.

Exercise 5. SIS

Definition 1 (Learning with Errors). Let $\ell < k \in \mathbb{N}$, $n < m \in \mathbb{N}$, $q = 2^k$, $B = 2^\ell$, $A \leftarrow U(\mathbb{Z}_q^{n \times n})$. The Learning with Errors (LWE) distribution is defined as follows: $D_{\text{LWE},A} = (A, A \cdot s + e \mod q)$ for $s \leftarrow U(\mathbb{Z}_q^n)$ and $e \leftarrow U\left(\left[\begin{array}{c} -B \\ B \end{array}\right] \mathbb{Z}_q \cap \mathbb{Z}_q^n\right)$. 

1
The \textit{LWE}_A \textit{assumption} states that, given suitable parameters $k, \ell, m, n$, it is computationally hard to distinguish $D_{\text{LWE}_A}$ from the distribution $(A, U(Z_q^n))$.

Given a matrix $A \in \mathbb{Z}_q^{m \times n}$ with $m > n \log q$, let us define the following hash function:

$$H_A : \{0,1\}^m \rightarrow \{0,1\}^n \quad x \mapsto x^T \cdot A \mod q.$$ 

1. Why finding a sufficiently “short” non-zero vector $z$ such that $z^T \cdot A = 0$ is enough to distinguish $D_{\text{LWE}_A}$ from the distribution $(A, U(Z_q^n))$? Define “short”.

2. Show that $H_A$ is collision-resistant under the \textit{LWE}_A assumption.

3. Is it still a secure hash function if we let $H_A : x \mapsto x^T \cdot A$? (without the reduction modulo)