TD 5: MACs and CCA-encryption

Exercise 1. *CBC-MAC*

Let $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a PRF, $d > 0$ and $L = nd$. Prove that the following modifications of CBC-MAC (recalled in Figure 1) do not yield a secure fixed-length MAC. Define $t_i := F(K, t_{i-1} \oplus m_i)$ for $i \in [1, d]$ and $t_0 := IV = 0$.

1. Modify CBC-MAC so that a random $IV \hookleftarrow U(\{0,1\}^n)$ (rather than $IV = \mathbf{0}$) is used each time a tag is computed, and the output is (IV, t_d) instead of t_d alone.

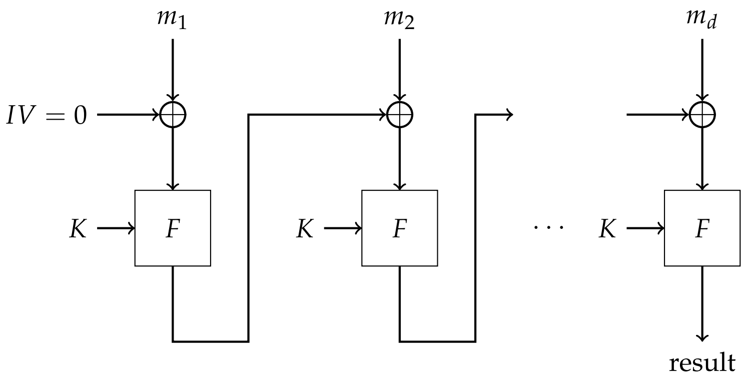

Figure 1: CBC-MAC

2. Modify CBC-MAC so that all the outputs of F are output, rather than just the last one.

We now consider the following ECBC-MAC scheme: let $F : K \times X \to X$ be a PRF, we define $F_{ECBC} : K^2 \times X^{\leq L} \to X$ as in Figure 2, where K_1 and K_2 are two independent keys.
If the message length is not a multiple of the block length n, we add a pad to the last block: $m = m_1 | \ldots | m_{d-1} | (m_d \| \mathrm{pad}(m))$.

3. Show that there exists a padding for which this scheme is not secure.

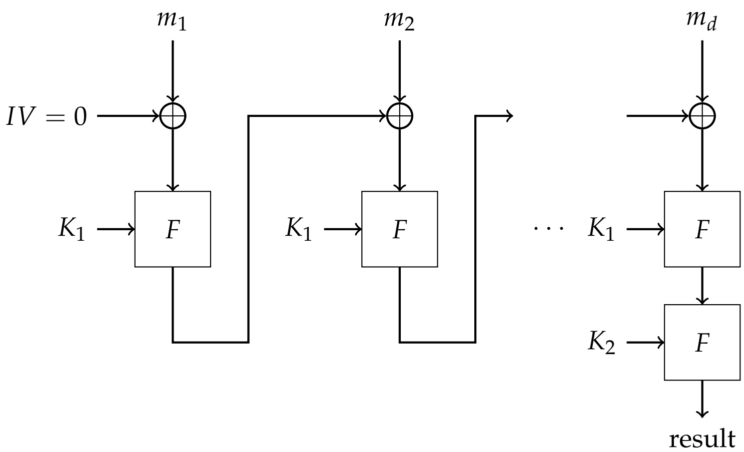

Figure 2: ECBC-MAC

For the security of the scheme, the padding must be invertible, and in particular for any message $m_0 \neq m_1$ we need to have $m_0 || \text{pad}(m_0) \neq m_1 || \text{pad}(m_1)$. In practice, the ISO norm is to pad with $10 \cdots 0$, and if the message length is a multiple of the block length, to add a new "dummy" block $10 \cdots 0$ of length n.

4. Prove that this scheme is not secure if the padding does not add a new "dummy" block if the message length is a multiple of the block length.

Remark: The NIST standard is called CMAC, it is a variant of CBC-MAC with three keys (k, k_1, k_2). If the message length is not a multiple of the block length, then we append the ISO padding to it and then we also XOR this last block with the key k_1. If the message length is a multiple of the block length, then we XOR this last block with the key k_2. After that, we perform a last encryption with $F(k, .)$ to obtain the tag.

Exercise 2. *Insecure MACs*

Let $F : \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$ be a secure pseudo-random function (PRF). Show that each one of the following message authentication codes (MAC) is insecure:

1. To authenticate $m = m_1 \| \ldots \| m_d$ where $m_i \in \{0,1\}^n$ for all i, compute $t = F(k, m_1) \oplus \ldots \oplus F(k, m_d)$.

2. To authenticate $m = m_1 \parallel \ldots \parallel m_d$ with $d < 2^{n/2}$ and $m_i \in \{0,1\}^{n/2}$ for all i, compute

$$t = F(k, \underline{1} \parallel m_1) \oplus \ldots \oplus F(k, \underline{d} \parallel m_d),$$

where $\underline{i}$ is an $n/2$-bit long representation of i, for all $i \leq d$.

Exercise 3. *CPA + MAC implies CCA*

Consider the following construction of symmetric encryption, where $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Verify})$ is a MAC.

Gen(1^λ)**:** Choose a random key $K_1 \leftarrow \mathsf{Gen}'(1^\lambda)$ for an IND-CPA secure symmetric encryption scheme $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$. Choose a random key $K_0 \leftarrow \Pi.\mathsf{Gen}(1^\lambda)$ for the MAC Π. The secret key is $K = (K_0, K_1)$.

Enc(K, M)**:** To encrypt M, do the following.

1. Compute $c = \mathsf{Enc}'(K_1, M)$.
2. Compute $t = \Pi.\mathsf{Mac}(K_0, c)$.

Return $C = (t, c)$.

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

1. Assume that the MAC is weakly unforgeable. Assume however that there exists an algorithm $\mathcal{F}$, which on input a valid message for the MAC and a tag (M, t), outputs a forgery (M, t') such that $t \neq t'$. In particular, the MAC is not strongly unforgeable. Show that the scheme is not IND-CCA secure.

2. We assume that: (i) $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ is IND-CPA-secure; (ii) Π is strongly unforgeable under chosen-message attacks. We will prove in this question the IND-CCA security of the new encryption scheme under these assumptions. Let $\mathcal{A}$ be an adversary against the IND-CCA security of the scheme.

(a) Define the event Valid as the event where $\mathcal{A}$ makes a valid (i.e. accepted by the MAC) decryption query for (c, t) where the ciphertext c was not encrypted by the encryption oracle nor is (c, t) the challenge ciphertext. Prove that if $\Pr(\mathsf{Valid})$ is non-negligible then there exists an adversary with non-negligible advantage against the strong unforgeability of the MAC.

The intuition is that since this event has negligible probability, the decryption oracle is useless to an attacker $\mathcal{A}$.

(b) Prove that if $|\Pr(\mathcal{A} \text{ wins} \wedge \overline{\mathsf{Valid}}) - 1/2|$ is non-negligible, then there exists an efficient adversary against the IND-CPA security of the encryption scheme $(\mathsf{Gen}, \mathsf{Enc}', \mathsf{Dec}')$.

(c) Conclude.

Exercise 4. *Insecure encryption*

Let us consider the following symmetric encryption scheme, where $F : \{0,1\}^s \times \{0,1\}^n \to \{0,1\}^\ell$ is a secure PRF. To encrypt a message $m \in \{0,1\}^\ell$ for $\ell \in \mathbb{N}$:

KeyGen(1^λ): Output $k \hookleftarrow U(\{0,1\}^s)$.

Enc(k, m): Sample $r \hookleftarrow U(\{0,1\}^n)$ and output $c := (r, F(k,r) \oplus m)$.

Dec$(k, c := (c_1, c_2))$: Output $m = c_2 \oplus F(k, c_1)$.

1. Recall the security definition of the CCA-security of an encryption scheme.

2. Is this scheme CCA-secure?