Cryptography: Homework 7

(Deadline: 11:59am, 2019/11/13)

1. (30 points) Let F be a pseudorandom function. Show that the following MACs are not EUF-CMA. (Let $\langle i \rangle$ denote an $n/2$-bit encoding of the integer i.)

   (a) A fixed-length MAC that authenticates messages of $3n/2$ bits.

   - $\mathsf{Gen}(1^n)$: choose $k \leftarrow \{0,1\}^n$ uniformly as the secret key.
   - $\mathsf{Mac}(k, m)$: To authenticate a message $m = m_1 m_2 m_3$, where $m_i \in \{0,1\}^{n/2}$ for every $i \in \{1, 2, 3\}$, compute and output the tag

   $$t = F_k(\langle 1 \rangle \| m_1) \oplus F_k(\langle 2 \rangle \| m_2) \oplus F_k(\langle 3 \rangle \| m_3).$$

   - $\mathsf{Vrfy}(k, m, t)$: for a message $m = m_1 m_2 m_3 \in \{0,1\}^{3n/2}$ and a tag $t \in \{0,1\}^n$, output 1 if and only if $t = F_k(\langle 1 \rangle \| m_1) \oplus F_k(\langle 2 \rangle \| m_2) \oplus F_k(\langle 3 \rangle \| m_3)$.

   (b) A fixed-length MAC that authenticates messages of $n/2$ bits.

   - $\mathsf{Gen}(1^n)$: choose $k \leftarrow \{0,1\}^n$ uniformly as the secret key.
   - $\mathsf{Mac}(k, m)$: To authenticate a message $m \in \{0,1\}^{n/2}$, choose $r \leftarrow \{0,1\}^n$ uniformly, compute $s = F_k(r) \oplus F_k(\langle 1 \rangle \| m)$, output the tag $t = (r, s)$.
   - $\mathsf{Vrfy}(k, m, t)$: for a message $m \in \{0,1\}^{n/2}$ and a tag $t = (r, s)$, output 1 if and only if $s = F_k(r) \oplus F_k(\langle 1 \rangle \| m)$.

2. (20 points) Define a MAC for arbitrary-length messages by $\mathbf{Mac}((s, k), m) = H^s(k \| m)$ where $k \in \{0,1\}^n$ is an n-bit secret key and H^s is the collision-resistant hash function on page 2, lecture 16, i.e., the Merkle-Damgård transform of the hash function $h^s : \{0,1\}^{2n} \to \{0,1\}^n$. Show that **Mac** is not EUF-CMA. (The s is public and known to the adversary. The k is secret and not known to the adversary.)