Cryptography: Homework 6

(Deadline: 10am, 2022/11/4)

1. (20 points) Let F be a length-preserving PRF. Show that the following MACs are not EUF-CMA secure. (Let $\langle i \rangle$ denote the $n/2$-bit encoding of an 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. (30 points) Let F be a length-preserving PRF. Define a MAC $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ for messages of n bits as below:

   - $\mathsf{Gen}(1^n)$: choose $k \leftarrow \{0,1\}^n$;
   - $\mathsf{Mac}(k, m)$: for $m \in \{0,1\}^n$, output $t = F_k(m) \in \{0,1\}^n$.
   - $\mathsf{Vrfy}(k, m, t)$: output 1 if $t = F_k(m)$ or $t = F_k(m) \oplus 1^n$.

   Determine if Π is EUF-CMA secure or sEUF-CMA secure. Prove your answers.