CS 171: Discussion Section 6 (2/26)

1 Insecure Candidates for MACs

Two candidate constructions of MACs are given below. The schemes use a pseudrandom function function F that maps $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$. The differences between schemes 1 and 2 are shown in red.

Show that each of the following MAC schemes is insecure.

Scheme 1:

1. $\mathsf{Gen}(1^n)$: Output $k \leftarrow \{0,1\}^n$.
2. $\mathsf{Mac}(k,m)$: Let $m = m_0||m_1$, where $m_0, m_1 \in \{0,1\}^n$. Then Mac outputs
$$t = F(k, m_0) \oplus F(k, m_1)$$
3. $\mathsf{Verify}(k,m,t)$: Output 1 if $t = \mathsf{Mac}(k,m)$, and output 0 otherwise.

Scheme 2:

1. $\mathsf{Gen}(1^n)$: Output $k \leftarrow \{0,1\}^n$.
2. $\mathsf{Mac}(k,m)$: Let $m = m_0||m_1$, where $m_0, m_1 \in \{0,1\}^n$. Then Mac outputs
$$t = F(k, m_0)||F(k, m_1)$$
3. $\mathsf{Verify}(k,m,t)$: Output 1 if $t = \mathsf{Mac}(k,m)$, and output 0 otherwise.

2 Difference Between Regular and Strong Security for MACs

Construct a MAC $\mathsf{MAC}' := (\mathsf{Gen}', \mathsf{Mac}', \mathsf{Verify}')$ that is secure but not strongly secure. In your construction, you may start with a secure MAC, $\mathsf{MAC} := (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Verify})$.

3 MACs and Pseudorandom Functions

In the construction of a fixed-length MAC that we saw in lecture (and in construction 4.5 in the textbook), Mac is a pseudorandom function. However we will show that this feature is not necessary.

Construct a secure deterministic MAC for n-bit messages such that Mac is not a pseudorandom function. Note: you may use a pseudorandom function in your construction.