Foundations of Cryptography: Homework 10

(Deadline: Dec 6, 2018)

1. (20 points) Let $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be a length-preserving PRF. Define a MAC $\Pi = (\mathbf{Gen}, \mathbf{Mac}, \mathbf{Vrfy})$ for messages of length n as below:

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

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

2. (20 points) Let $\Pi = (\mathbf{Gen}, H)$ be a collision-resistant hash function. Let $\hat{\Pi} = (\mathbf{Gen}, \hat{H})$ be defined by $\hat{H}^s(x) = H^s(H^s(x))$. Is $\hat{\Pi}$ collision resistant? Prove your answer.