CS 409M : Introduction to Cryptography Fall 2024

Quiz II

Full Marks: 20, **Time**: 1 hour (+ 15 minutes)

Roll Number: _____ **Name:** _____

1. Answer each question on a new page of the answer booklet.
2. Do not use pencils. Pens only!
3. Use me as your cheat sheet and ask me for defintions, if you want.

Problem 1: [6 marks (3+3)]

Let F, $F^{(1)}$ and $F^{(2)}$ be a length-preserving pseudorandom functions. For the following constructions of a keyed function F', state whether F' is a pseudorandom function. If yes, prove it; if not, show an attack.

a) $F' : \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$, where $F'_k(x) := F_k(0||x)||F_k(x||1)$.

b) $F' : \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^{2n}$, where $F'_{k_1||k_2}(x) = F^{(1)}_{k_1}(x)||F^{(2)}_{k_2}(x)$.

Problem 2: [3 marks (1+2)]

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a length-preserving pseudorandom function. Define the function G as

$$G(s) := F_s(1)||F_s(2)||\cdots||F_s(\ell-1)||F_s(\ell).$$

State its expansion factor and whether it is a pseudorandom generator or not. If you claim it is a pseudorandom generator, prove the same. If you claim it is not a pseudorandom generator, provide a distinguisher with a non-negligible advantage.

Problem 3: [6 marks (3+3)]

1. Let F be a pseudorandom permutation. Consider the mode of operation in which you choose a $\mathsf{ctr} \in_R \{0,1\}^n$ (uniformly at random), and the i-th ciphertext block c_i is generated as $c_i := F_k(\mathsf{ctr} + i + m_i)$. Show that this scheme is not secure against a ciphertext only attack against an eavesdropper (i.e., not COA secure).

2. Show a chosen ciphertext attack (CCA) on the output feedback (OFB) mode of operation for encryptions.

Problem 4: [5 marks]

Let $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ be message authentication code that is existentially unforgeable against a strong chosen message attack (EU-SCMA secure). Define $\Pi' = (\mathsf{Gen}', \mathsf{Mac}', \mathsf{Vrfy}')$ as follows.

- $\mathsf{Gen}'(1^n)$: output $k \leftarrow \mathsf{Gen}(1^n)$
- $\mathsf{Mac}'_k(m) := \mathsf{Mac}_k(m)||0$
- $\mathsf{Vrfy}'_k(m, t||b) := \mathsf{Vrfy}_k(m, t)$ (i.e., ignores the last bit of the tag).

Answer the following questions:

1. Is Π' existentially unforgeable against a chosen message attack (EU-CMA)? If yes, prove it. If no, show an attack.
2. Is Π' existentially unforgeable against a strong chosen message attack (EU-SCMA)? If yes, prove it. If no, show an attack.

Problem 5 (bonus): [4 marks]

Let F be a pseudorandom function. Consider the following scheme $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$:

- $\mathsf{Gen}(1^n)$: Generate a $k \in_R \{0,1\}^n$.
- $\mathsf{Mac}_k(m)$: On message $m = m_1, m_2, ..., m_d$, where $m_i \in \{0,1\}^n$ for each i, compute: $t_1 = F_k(m_1)$, $t_2 = F_k(t_1 \oplus m_2)$, $\cdots$, $t_d = F_k(t_{d-1} \oplus m_d)$, $t_{d+1} = F_k(t_d \oplus |m|)$. Output $t = t_{d+1}$. (see Figure 1)

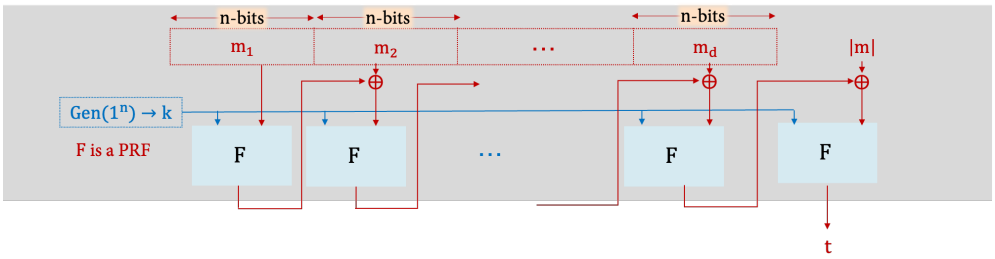

Figure 1: $\mathsf{Mac}_k(m) = t$

- $\mathsf{Vrfy}_k(m, t)$: Compute $t_1 = F_k(m_1)$, $\cdots$, $t_d = F_k(t_{d-1} \oplus m_d)$. If $t = F_k(t_d \oplus |m|)$, then output 1, else output 0.

Show a chosen message attack against Π (i.e., show that it is not EU-CMA secure).