

Assignment 2

PRFs, CPA Security, Modes of Operation

Instructor: Sruthi Sekar

Problem 1 (PRF or not?). Let $\mathcal{F}^{(1)} = \{f_k^{(1)} : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ and $\mathcal{F}^{(2)} = \{f_k^{(2)} : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ be length-preserving pseudorandom functions [Def 1 or 2, Lec7]. For the following constructions, state whether $\mathcal{F}'$ is a pseudorandom function. If yes, prove it; if not, show an attack.

- $\mathcal{F}' = \{f'_k : \{0, 1\}^{n-1} \rightarrow \{0, 1\}^{2n}\}_{k \in \{0, 1\}^n}$, where $f'_k(x) := f_k^{(1)}(0||x)||f_k^{(1)}(1||x)$.
- $\mathcal{F}' = \{f'_k : \{0, 1\}^{n-1} \rightarrow \{0, 1\}^{2n}\}_{k \in \{0, 1\}^n}$, where $f'_k(x) := f_k^{(1)}(0||x)||f_k^{(1)}(x||1)$.
- $\mathcal{F}' = \{f'_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$, where $f'_k(x) = f_k^{(1)}(f_k^{(2)}(x))$.
- $\mathcal{F}' = \{f'_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$, where $f'_k(x) := \overline{f_k^{(1)}(x)}$ (overline denoted bit-string complement).
- $\mathcal{F}' = \{f'_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$, where $f'_k(x) := f_k^{(1)}(\bar{x})$.
- Recall the tree-based construction of PRF from length-doubling PRF [GGM, Lec 7]. Recall that the value $f_k(x)$, $x \in \{0, 1\}^n$, was computed by taking the key k as the seed of the root PRG, and computing the leaf output y_x (taking the path given by x). Consider the “dual” construction $\mathcal{F}' = \{f'_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$: to compute $f'_k(x)$, you use the input x as the seed of the root PRG, and then output the leaf value y_k .
- $\mathcal{F}' = \{f'_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ as ($||$ denotes concatenation):

$$f'_k(x) := \begin{cases} f_k^{(1)}(x), & \text{if } \bigoplus_{i=1}^n x_i = 0 \\ f_k^{(1)}(x \oplus 0^{n-1}||1), & \text{if } \bigoplus_{i=1}^n x_i = 1 \end{cases}$$

Note that when x has odd number of 1's, you are just flipping the last bit to make it even.

Problem 2 (COA secure, CPA secure or Both?). Let F be a pseudorandom function [Def 1 or 2, Lec7] and G be a pseudorandom generator with expansion factor $\ell(n) = n+1$ [Def 1 or 2, Lec 4]. For each of the following encryption schemes, state whether the scheme has indistinguishable encryptions in the presence of an eavesdropper, i.e., COA secure [Def 7, Lec 3] and whether it is CPA-secure [Def 3, Lec 8]. (In each case, the shared key is a uniform $k \in \{0, 1\}^n$.) Explain your answer.

- To encrypted $m \in \{0, 1\}^{n+1}$, choose uniform $r \in \{0, 1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$.
- To encrypt $m \in \{0, 1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.
- To encrypt $m \in \{0, 1\}^{2n}$, parse m as $m_1||m_2$ with $|m_1| = |m_2|$, then choose uniform $r \in \{0, 1\}^n$ and send $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$.

Problem 3 (Understanding CPA). For a symmetric-key encryption (SKE) scheme, refer to [Def 7, Lec 3] for indistinguishability against an eavesdropper (or COA-security), [Definition 3.18, Katz Lindell] for security of multiple encryptions against an eavesdropper, and [Def 3, Lec 8] for CPA security.

- A) **Gap b/w Multiple-EAV- and CPA-Securities:** Assuming the existence of pseudorandom functions, prove that there is an encryption scheme that has indistinguishable multiple encryptions in the presence of an eavesdropper, but is not CPA-secure.

Hint: The scheme need not be “natural”. You will need to use the fact that in a chosen-plaintext attack, the adversary can choose its queries to the encryption oracle adaptively.

- B) **Combiners:** Let $\Pi_1 = (\text{Gen}_1, \text{Enc}_1, \text{Dec}_1)$ and $\Pi_2 = (\text{Gen}_2, \text{Enc}_2, \text{Dec}_2)$ be two SKE schemes for which it is known that at least one is CPA-secure (and we don't know which one). Construct a SKE scheme Π that is CPA-secure as long as Π_1 or Π_2 is secure. (Such a construction is called a “combiner”.)

Hint: it is instructive to first think about constructing such schemes against eavesdroppers.

Problem 4 (Custom Counter Mode). Let F be a pseudorandom permutation [Slide 17, Lec 8]. Consider the mode of operation (variant of CTR mode) in which a uniform value $IV \in_R \{0, 1\}^n$ is chosen, and the i^{th} ciphertext block c_i is computed as $c_i := F_k(IV + i + m_i)$, where addition is modulo 2^n . The ciphertext is $IV, c_1, c_2, \dots$. Show that this scheme is not COA-secure.

Problem 5 (CPA from PRP). Let $F = \{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ be a PRP [Slide 17, Lec 8], define a fixed-length encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ as:

- $\text{Gen}(1^n)$: Pick and output $k \in_R \{0, 1\}^n$.
- $\text{Enc}(k, m)$: Pick $r \in_R \{0, 1\}^{n/2}$. For $m \in \{0, 1\}^{n/2}$, compute and output $c := f_k(r || m)$.

Show how to decrypt, and prove that this scheme is CPA-secure for messages of length $n/2$.