

Tutorial 1

Instructor: Sruthi Sekar

Date: 4th Sep 2026

Problem 1 (Hybrid Argument). Let $F^{(1)} := \{f_k^{(1)} : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ and $F^{(2)} := \{f_k^{(2)} : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ be pseudorandom functions. Is the following $F := \{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}\}_{k \in \{0, 1\}^{2n}}$ a PRF:

$$f_{k_1 || k_2}(x) := f_{k_1}^{(1)}(x) || f_{k_2}^{(2)}(x)$$

for independent keys k_1 and k_2 .

Problem 2 (Weak PRFs). Consider the following definition of a weak pseudorandom function (weakPRF), which intuitively is like a PRF but has a weaker oracle access: it only allows you to get the PRF output on a uniform random input (similar to how you see the PRG output only on a random input). $\mathcal{F} := \{f_k : \{0, 1\}^{\ell_{in}(n)} \rightarrow \{0, 1\}^{\ell_{out}(n)}\}_{k \in \{0, 1\}^{\ell_{key}(n)}}$ is a *weak* PRF if for every PPT adversary **Eve**, there exists a negligible negl such that $\forall n$:

$$\left| \Pr_{k \in_R \{0, 1\}^{\ell_{key}}} [\text{Eve}^{f_k(\$)}(1^n) = 1] - \Pr_{R \in_R \mathcal{F}[\ell_{in}, \ell_{out}]} [\text{Eve}^{R(\$)}(1^n) = 1] \right| \leq \text{negl}(n),$$

where $\mathcal{F}[\ell_{in}, \ell_{out}] := \{g : \{0, 1\}^{\ell_{in}(n)} \rightarrow \{0, 1\}^{\ell_{out}(n)}\}$, and $f_k(\$)$ and $R(\$)$ are the modified oracles that give the function outputs on randomly chosen input points, i.e., $f_k(\$)$ and $R(\$)$ output $(r, f_k(r))$ and $(r, R(r))$, respectively, for $r \in_R \{0, 1\}^{\ell_{in}}$.

- Prove that if $\mathcal{F}$ is a PRF then $\mathcal{F}$ is a weak-PRF.
- Let $\mathcal{F}' = \{f'_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ be a PRF. Define $\mathcal{F} = \{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ as: For all $k \in \{0, 1\}^n$,

$$f_k(x) := \begin{cases} 0^n, & \text{if } x = 0^n \\ f'_k(x), & \text{otherwise} \end{cases}$$

Is $\mathcal{F}$ a PRF? If not, is it a weak-PRF? Prove or dispute formally.

- Prove that the construction we saw in class is CPA-secure even if $\mathcal{F}$ is just a weak-PRF. Recall the construction $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$:
 - $\text{Gen}(1^n)$: output random $k \in_R \{0, 1\}^n$.
 - $\text{Enc}(k, m)$: pick random $r \in_R \{0, 1\}^n$ and output $c := (r, f_k(r) \oplus m)$.
 - $\text{Dec}(k, c = (r, s))$: output $m := f_k(r) \oplus s$.

Problem 3. Let $F := \{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ be a pseudorandom function. In each part below, is $(\text{Gen}, \text{Mac}, \text{Vrfy})$ EU-CMA secure? If yes, give proof of security via reduction; if not, show an attack. Each of them is a fixed-length MAC with canonical verification.

- Gen** outputs a uniform $k \in \{0, 1\}^n$. To authenticate a message $m_1 || m_2$ with $|m_1| = |m_2| = n - 1$, **Mac** _{k} computes the tag $t = f_k(0 || m_1) \oplus f_k(1 || m_2)$.
- Gen** outputs a uniform $k \in \{0, 1\}^n$. To authenticate a message m , **Mac** _{k} computes the tag $t = (f_k(m), f_k(m))$.