MIT 6.5620/6.875/18.425: Foundations of Cryptography **Due: Oct. 7, 2026**

Problem Set 2

Your name **Your Collaborators**

Total Number of Points: 50.
Instructions: Solutions should be typeset in LaTeX and submitted as PDF by 11:59:59 PM ET on the due date. You can collaborate on the psets in small groups (of up to three), but must write your solutions separately, in your own words. This means not copying from a board nor from your collaborator's computer.

We strongly recommend ***not*** using AI tools to solve your problem sets. You are responsible for understanding everything you submit and you must be able to explain and justify every part of your solution. In particular, the oral problem set review (10% of the course grade) will evaluate your understanding of the solutions you submit. In all cases, you must list your collaborators, human or machine.

Problem 1. One-way... or another. (15 points) Let f be a length-preserving one-way function. For each of the following parts, either prove that f_i is necessarily a one-way function or show a counterexample (namely, a length-preserving one-way function f for which f_i is *not* one-way). Your counterexamples must rely only on the *existence* of one-way functions.

- **(a)** (5 points) $f_0(x) := f(f(x))$
- **(b)** (5 points) $f_1(x, y) := f(x) \| f(x \oplus y)$, where the length of x and y is the same, i.e., $|x| = |y|$.
- **(c)** (5 points) $f_2(x) := f(x) \oplus x$.

Problem 2. (10 points) Assume that one-way functions exist. $b : \{0,1\}^* \to \{0,1\}$ is a hard-core predicate of a one-way function $f(\cdot)$ if $b(x)$ is efficiently computable given x and for every PPT adversary A there exists a negligible function v such that for every n:

$$\Pr[x \leftarrow \{0,1\}^n : A(f(x)) = b(x)] \leq \frac{1}{2} + v(n).$$

A polynomial time-computable predicate $b : \{0,1\}^n \to \{0,1\}$ is called a *universal* hardcore predicate if for *every* one-way function $f : \{0,1\}^n \to \{0,1\}^m$, b is hardcore. Prove that there is no universal hardcore predicate.

Problem 3. Input Length Extension for PRFs. (15 points) Let $\{\mathcal{F}_n\}_{n\in\mathbb{N}}$ where

$$\mathcal{F}_n = \{f_k : \{0,1\}^\ell \to \{0,1\}^\ell\}_{k\in\{0,1\}^\ell}$$

is a pseudo-random function (PRF) family. For each of the following parts, either prove that the function family $\{\mathcal{F}'_n\}_{n\in\mathbb{N}}$ where

$$\mathcal{F}'_n = \{f'_k : \{0,1\}^{2\ell} \to \{0,1\}^\ell\}_{k\in\{0,1\}^\ell}$$

is a pseudorandom function family or provide a polynomial-time attack showing that it isn't.

(a) (5 points) $f'_k(x, y) = f_k(x \oplus y)$

(b) (10 points) $f'_k(x, y) = f_{f_k(x)}(y)$.

Problem 4. Swapping the Input and the Key. (10 points) Recall the Goldreich-Goldwasser-Micali (GGM) construction of a pseudo-random function (PRF) family from any pseudo-random generator (PRG): let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG and let G_0 (resp., G_1) be the function that output the first (resp., second) half of the bits of G. That is, $G(k) = G_0(k)\|G_1(k)$, the concatenation of $G_0(k)$ and $G_1(k)$. For any key $k \in \{0,1\}^n$, the GGM construction defines $f_k : \{0,1\}^n \to \{0,1\}^n$ as

$$f_k(x_1, \cdots, x_n) = G_{x_n}(G_{x_{n-1}}(\cdots G_{x_2}(G_{x_1}(k)))).$$

where $x_i \in \{0,1\}$ are the bits of the input x.

We saw in class that if G is a PRG, the collection of functions $\{\mathcal{F}_n\}_{n\in\mathbb{N}}$ where

$$\mathcal{F}_n = \{f_k : \{0,1\}^n \to \{0,1\}^n\}_{k\in\{0,1\}^n}$$

is a pseudorandom function family.

Quack the Duck, the best student in 6.5620, wants to poke around GGM a bit. In particular, he wants to see what happens if you swap the roles of the input and the key in the GGM construction. That is, he defines the function family $\{\mathcal{F}'_n\}$ where each

$$\mathcal{F}'_n = \{f'_k : \{0,1\}^n \to \{0,1\}^n\}_{k\in\{0,1\}^n}$$

and

$$f'_k(x) = G_{k_n}(G_{k_{n-1}}(\cdots G_{k_2}(G_{k_1}(x)))).$$

Help Quack by proving or disproving the following statement: For every PRG $G : \{0,1\}^n \to \{0,1\}^{2n}$, $\mathcal{F}'_n$ is a pseudo-random function family.