MIT 6.5620/6.875/18.425: Cryptography and Cryptanalysis **Due: Oct. 4, 2023**

Problem Set 2

Total Number of Points: 60.

Collaboration Policy: Collaboration is allowed and encouraged in small groups of at most three students. You are free to collaborate in discussing answers, but you must write up solutions on your own and must specify in your submission the names of any collaborators. Do not copy any text from your collaborators; the writeup must be entirely your work. Do not write down solutions on a board and copy them verbatim into LaTeX; again, the writeup must be entirely your own words and your own work and should demonstrate a clear understanding of the solution. Additionally, you may make use of published material, provided that you acknowledge all sources used. Of course, scavenging for solutions from prior years is forbidden.

Problem 1. Input Length Extension for PRFs. (16 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 is not.

(a) (1 point) $f'_k(x,y) = f_k(x \oplus y)$.

(b) (5 points) $f'_k(x,y) = f_{k\oplus x}(y)$.

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

Problem 2. Swapping the Input and the Key. (10 points) Recall the Goldreich-Goldwasser-Micali (GGM) construction of a pseudo-random function (PRFs) family from any pseudo-random generator (PRGs): let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG and let G_0 (resp. G_1) be the function that outputs 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

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

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.

(a) (5 points) Tim the Tinkerer, a first-year taking 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

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

Help Tim 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.

(b) (5 points) Callista the Cryptographer, a graduate student in 6.5620, decides to modify the construction further and comes up with the following variant of GGM. She defines the function family $\{\mathcal{F}''_n\}$ where each

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

and

$$f''_{k,r}(x) = G_{k_n}(G_{k_{n-1}}(\cdots G_{k_2}(G_{k_1}(x \oplus r))\cdots)).$$

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

Problem 3. One-way ... or another. (20 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) $f_2(x) := f(x)_{[1:|x|-1]}$.

(d) (5 points) $f_3(x) := f(x) \oplus x$.

Problem 4. A Hardcore Problem. (14 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 there exists a negligible function v such that for every PPT adversary A and for every n:

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

(a) (2 points) 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.

(b) (12 points) Could there be a one-way function f for which *none* of the individual bits of the input are hardcore? It turns out that there are such beasts. Construct a one-way function $f : \{0,1\}^n \to \{0,1\}^m$ for which none of the predicates $b_i(x_1, \ldots, x_n) = x_i$ are hardcore.