

## Problem Set 2: Solutions

Your name

Your Collaborators

**Total Number of Points:** 50.

**Instructions:** Solutions should be typeset in  $\text{\LaTeX}$  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)  $f_0(x) := f(f(x))$

**Solution**

$f_0$  is not a one-way function (OWF). Let  $g : \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$  be an OWF. Consider the following function  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ :

$$f(x) = \begin{cases} 0^n & \text{if } x \text{ starts with } 0^{n/2} \\ 0^{n/2} \| g(x_{[1:n/2]}) & \text{else} \end{cases}$$

We firstly prove that  $f$  is a one-way function. Suppose there were a PPT adversary  $A$  which, on input  $f(x)$  for uniformly chosen  $x$ , outputs  $x'$  such that  $f(x') = f(x)$  with non-negl probability. Then consider the following adversary  $B$  for  $g$ :  $B$  gets a challenge  $g(y)$  for uniformly chosen  $y$ , gives  $A$   $0^{n/2} \| g(y)$ , receives  $x'$ , and outputs  $x'_{[1:n/2]}$ . The challenge that  $B$  gives  $A$  is drawn from a distribution which is negligibly close in total variation distance to the distribution  $A$  expects, since  $x \leftarrow_R \{0, 1\}^n$  starts with  $0^{n/2}$  with probability only  $2^{-n/2}$ . Therefore,  $A$ 's success probability remains non-negligible when  $B$  produces  $A$ 's challenge instead of the standard challenger.

Moreover,  $\Pr_y[g(y) = 0^{n/2}]$  must be negligible; otherwise, on input  $g(y)$ , an inverter could simply output a uniformly random  $y'$  whenever  $g(y) = 0^{n/2}$ , succeeding with non-negligible probability. Thus, except with negligible probability, a successful  $x'$  produced by  $A$  cannot start with  $0^{n/2}$ . Hence

$$g(x'_{[1:n/2]}) = g(y),$$

so  $x'_{[1:n/2]}$  is a valid preimage to the challenge received by  $B$ .

It is easy to see that  $f \circ f$  here is not a one-way function, since  $f \circ f$  maps everything to  $0^n$ .

- (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.,  $|x| = |y|$ .

**Solution**

$f_1$  is a one-way function. Suppose there were a PPT adversary  $A$  which, on input  $f_1(x, y)$  for  $(x, y) \leftarrow_R \{0, 1\}^{2n}$ , outputs  $(x', y')$  such that  $f_1(x', y') = f_1(x, y)$  with non-negligible probability. Then consider an adversary for  $f$  which receives  $f(x)$  for uniformly chosen  $x$ , chooses  $r \leftarrow_R \{0, 1\}^n$ , gives  $A(f(x) \| f(r))$ , and returns  $x'$  in the  $(x', y')$  pair which  $A$  outputs.  $x \oplus y$  is uniform and i.i.d. from  $x$  if  $y$  is uniform and i.i.d. from  $x$ , so the input which the reduction provides to  $A$  is of the correct form. Then, if  $A$  returns  $(x', y')$  such that  $f(x) \| f(r) = f(x') \| f(x' \oplus y')$ ,  $f(x) = f(x')$ , so  $x'$  is a valid preimage to  $f(x)$ .

- (c) (5 points)  $f_2(x) := f(x) \oplus x$ .

**Solution**

$f_2$  is not necessarily a one-way function. Let  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$  be any one-way function, and define

$$f'(x_1, x_2) = 0^n \| f(x_1),$$

where  $x_1, x_2 \in \{0, 1\}^n$ .

First,  $f'$  is a one-way function. Indeed, if there were an efficient inverter for  $f'$ , then given  $f(x_1)$  we could feed it  $0^n \| f(x_1)$  and obtain some  $(x'_1, x'_2)$  such that  $f'(x'_1, x'_2) = 0^n \| f(x_1)$ . This implies  $f(x'_1) = f(x_1)$ , contradicting the one-wayness of  $f$ .

Now consider the function obtained by XORing the input with the output ( $f_2$ ) instantiated with this  $f'$ :

$$f'_2(x_1, x_2) = f'(x_1, x_2) \oplus (x_1 \| x_2) = x_1 \| (f(x_1) \oplus x_2).$$

This function is efficiently invertible. Given an output  $y_1 \| y_2 = x_1 \| (f(x_1) \oplus x_2)$ , we immediately recover  $x_1 = y_1$ , and then compute  $x_2 = y_2 \oplus f(y_1)$ . Thus,  $f'_2$  is not a one-way function.

**Problem 2.** (10 points) Assume that one-way functions exist.  $b : \{0, 1\}^* \rightarrow \{0, 1\}$  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  $b : \{0, 1\}^n \rightarrow \{0, 1\}$  is called a *universal* hardcore predicate if for *every* one-way function  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ ,  $b$  is hardcore. Prove that there is no universal hardcore predicate.

**Solution**

Suppose otherwise, and that  $b$  is a universal hard-core predicate. Consider a one-way function  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ , and let  $h(x) = (f(x), b(x))$ . We claim that  $h$  is a one-way function.

Suppose otherwise and there exists an inverter  $\mathcal{A}$  for  $h$  that succeeds with non-negligible probability  $p(n)$ . We now construct an inverter  $\mathcal{B}$  for  $f$  as follows.

- Given  $z$ , query  $x_b \leftarrow \mathcal{A}(z || b)$  for  $b \in \{0, 1\}$ .
- If either  $x_b$  satisfy  $f(x_b) = z$ , output  $x_b$ . Otherwise, output  $\perp$ .

Clearly,  $\mathcal{B}$  runs in polynomial time since it only invokes  $\mathcal{A}$  twice. Since  $z = f(x')$  for some  $x'$ , at least one choice of  $b$  corresponds to  $b(x')$ . Therefore, at least one of the queries to  $\mathcal{A}$  corresponds to the value of  $h$  on some uniformly chosen  $x$ . Therefore,  $\mathcal{B}$  also inverts  $f$  with probability at least  $p(n)$ . This contradicts the one-wayness of  $f$ .

Finally,  $b(x)$  is trivially predictable from  $h(x)$ : simply output the last bit of  $h(x)$ . Thus  $b$  is not a hard-core predicate of the one-way function  $h$ , contradicting the assumption that  $b$  is universal.

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

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

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

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

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

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

**Solution**

Not a PRF. Consider the following strategy where the adversary asks for  $T(\geq 2)$  queries  $(x = x_1, y = x_1), \dots, (x = x_T, y = x_T)$ , where the  $x_i$ 's are distinct. Since  $x_i \oplus x_i = 0^\ell$ , we have

$$f'_k(x_i, x_i) = f_k(0^\ell)$$

for every  $i$ . Thus, all  $T$  answers are always identical. On the other hand, if it is a truly random function, the adversary observes  $T$  independent random strings  $z_{[1:T]}$  (i.e.,  $z_1, \dots, z_T$ ). Thus, we construct a distinguisher  $D$  as follows: if all the returned answers of the above-described queries are identical, it votes for 1, representing a generation from  $f'_k$ ; otherwise, it votes for a true random function. Thus, the adversary has a constant distinguishing advantage, where, for  $z_i$  i.i.d. uniformly selected from  $\{0, 1\}^\ell$ ,

$$\left| \Pr_{k, x_{[1:T]}} [D(f'_k(x_i, x_i), i = 1, 2, \dots, T) = 1] - \Pr_{z_{[1:T]}} [D(z_i, i = 1, 2, \dots, T) = 1] \right| = 1 - \frac{1}{2^{\ell(T-1)}}.$$

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

**Solution**

This is a PRF. Let  $A$  be a PPT adversary making at most  $q(\ell)$  queries. We consider two hybrid steps.

First, replace the inner PRF  $f_k$  by a truly random function  $R : \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ . The resulting oracle is

$$(x, y) \mapsto f_{R(x)}(y).$$

If  $A$  could distinguish this hybrid from the real construction

$$(x, y) \mapsto f_{f_k(x)}(y),$$

then we could distinguish  $f_k$  from a random function: given oracle access to  $O$ , answer each query  $(x, y)$  with  $f_{O(x)}(y)$ . Thus, the two experiments are computationally indistinguishable.

Now consider the hybrid  $(x, y) \mapsto f_{R(x)}(y)$ . For every distinct value of  $x$ , the value  $K_x := R(x)$  is an independently uniform key. Although two distinct values  $x \neq x'$  may happen to satisfy  $K_x = K_{x'}$ , among at most  $q(\ell)$  queried values this occurs with probability at most  $\binom{q(\ell)}{2} 2^{-\ell}$ , which is negligible. We may therefore ignore this event. Thus, the oracle consists of polynomially many independently keyed copies of the PRF, one for each distinct  $x$  queried by  $A$ . By a standard hybrid argument over these distinct  $x$ 's, PRF security allows us to replace each function  $y \mapsto f_{K_x}(y)$  by an independent truly random function  $R_x(y)$ .

The resulting oracle is  $(x, y) \mapsto R_x(y)$ , where the  $R_x$ 's are independent random functions. This is exactly a truly random function on  $\{0, 1\}^{2\ell}$ . Hence  $F'_n$  is a pseudo-random function family.

**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  $G : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$  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  $f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n$  as

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

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

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

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

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

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  $G : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$ ,  $\mathcal{F}'_n$  is a pseudo-random function family.

**Solution**

Not necessarily a PRF. We consider the following construction. Suppose  $G' : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$  is some PRG, we consider  $G = G'$  except that we set  $G(0^n) = 0^{2n}$ . Clearly,  $G$  is still a secure PRG, since it differs from  $G'$  only on the seed  $0^n$ , which occurs with probability  $2^{-n}$ . Now, the adversary can select  $x = 0^n$  and it is clear that  $f'_k(0^n)$  becomes a constant  $0^{2n}$  independent of the selection of the key  $k$ , and thus the adversary can distinguish between  $f'_k(0^n)$  and  $z$  uniformly selected from  $\{0, 1\}^{2n}$ .