CS 276: Homework 1

Due Date: Fri. Sept. 6th, 2024 at 8:59pm via Gradescope

One-Way Functions

Let $f : \{0,1\}^* \to \{0,1\}^*$ be a one-way function, and let g be defined as follows:

$$g(x) = \begin{cases} f(x), & |x| \text{ is even} \\ x, & |x| \text{ is odd} \end{cases}$$

In our notation, $|x|$ is the bitlength of x. Note that g is not one-way because when $|x|$ is odd, g is easy to invert.

Question: Using g as a black box, construct a one-way function h and prove that h is one-way. This means that h can make calls to g, but it cannot call f directly.

Solution

1. $$\text{Let } h(x) = \begin{cases} g(x), & |x| \text{ is even} \\ g(x_{1,\ldots,|x|-1}), & |x| \text{ is odd}, |x| \geq 3 \\ 0 & |x| = 1 \end{cases}$$

   where $x_{1,\ldots,|x|-1}$ is x without the final bit.

2. Note that h always calls g on an input of even length, so

   $$h(x) = \begin{cases} f(x), & |x| \text{ is even} \\ f(x_{1,\ldots,|x|-1}), & |x| \text{ is odd}, |x| \geq 3 \\ 0 & |x| = 1 \end{cases}$$

   Next, we will prove that $h(x)$ is one-way.

3. Let us assume toward contradiction that h is not a one-way function. Then there exists a PPT adversary $\mathcal{A}_h$ that can break the one-wayness of h.

   $$\text{Let } \mu_{\mathcal{A}_h,h}(n) = \Pr_{x \xleftarrow{\$} \{0,1\}^n} \left[\mathcal{A}_h(1^n, h(x)) \in h^{-1}(h(x))\right]$$

   Then $\mu_{\mathcal{A}_h,h}(n)$ is non-negligible.

   Next, we will use $\mathcal{A}_h$ to construct an adversary $\mathcal{A}_f$ that breaks the one-wayness of f:

   Construction of $\mathcal{A}_f$:

   (a) $\mathcal{A}_f$ receives $(1^n, f(x))$ from the challenger, where $x \xleftarrow{\$} \{0,1\}^n$.

   (b) If n is odd, $\mathcal{A}_f$ outputs $\perp$ and halts.

   (c) If n is even, then $\mathcal{A}$ samples $b \xleftarrow{\$} \{0,1\}$.

i. If $b = 0$, then $\mathcal{A}$ computes $x' \leftarrow \mathcal{A}_h(1^n, f(x))$ and outputs x'.
ii. If $b = 1$, then $\mathcal{A}$ computes $x' \leftarrow \mathcal{A}_h(1^{n+1}, f(x))$. If $|x'| = n+1$, then $\mathcal{A}_f$ computes $x'' = x'_{1,\ldots,n}$ and outputs x''. If not, $\mathcal{A}_f$ outputs $\perp$.

4. **Analysis:**

(a) When n is odd, $\mathcal{A}_f$ fails to invert f.

(b) When n is even and $b = 0$, $\mathcal{A}_f$ simulates the one-way function security game for h with input length n. The probability that $\mathcal{A}_f$ succeeds in inverting f is $\mu_{\mathcal{A}_h,h}(n)$.

(c) When n is even and $b = 1$, $\mathcal{A}_f$ simulates the one-way function security game for h with input length $n+1$.

$$\begin{aligned} \mathcal{A}_h \text{ inverts } h \text{ on input length } n+1 &\iff |x'| = n+1 \text{ and } h(x') = f(x) \\ &\iff |x''| = n \text{ and } f(x'') = f(x) \\ &\iff \mathcal{A}_f \text{ inverts } f \text{ on input length } n \end{aligned}$$

Then the probability that $\mathcal{A}_f$ succeeds is $\mu_{\mathcal{A}_h,h}(n+1)$.

In summary:

$$\mu_{\mathcal{A}_f,f}(n) = \Pr_{x \xleftarrow{\$} \{0,1\}^n}\left[\mathcal{A}_f(1^n, f(x)) \in f^{-1}(f(x))\right] = \begin{cases} 0, & n \text{ is odd} \\ \frac{1}{2} \cdot \left(\mu_{\mathcal{A}_h,h}(n) + \mu_{\mathcal{A}_h,h}(n+1)\right), & n \text{ is even} \end{cases}$$

5. **Lemma 0.1** *If $\mu_{\mathcal{A}_h,h}(n)$ is non-negligible, then $\mu_{\mathcal{A}_f,f}(n)$ is also non-negligible.*

Proof.

Since $\mu_{\mathcal{A}_h,h}(n)$ is non-negligible, then there is some $c \in \mathbb{Z}^+$ such that for any $n_0 \in \mathbb{Z}^+$, there exists a sufficiently large $n \in \mathbb{Z}^+$ such that $\mu_{\mathcal{A}_h,h}(n) \geq n^{-c}$.

If n is even, then:

$$\mu_{\mathcal{A}_f,f}(n) = \frac{1}{2} \cdot \left(\mu_{\mathcal{A}_h,h}(n) + \mu_{\mathcal{A}_h,h}(n+1)\right) \geq \frac{n^{-c}}{2} \geq \frac{n^{-c}}{n} = n^{-(c+1)} \geq n^{-2c}$$

We used the fact that $n \geq 2$.

If n is odd and sufficiently large, then

$$\mu_{\mathcal{A}_f,f}(n-1) = \frac{1}{2} \cdot \left(\mu_{\mathcal{A}_h,h}(n-1) + \mu_{\mathcal{A}_h,h}(n)\right) \geq \frac{n^{-c}}{2} \geq (n-1)^{-2c}$$

Let $c' = 2c$ and $n' = \begin{cases} n, & n \text{ is even} \\ n-1, & n \text{ is odd} \end{cases}$. Note that $n' \geq n-1 \geq 2n_0 - 1 \geq n_0$.

Then for this $c' \in \mathbb{Z}^+$, and for any $n_0 \in \mathbb{Z}^+$, there is a value $n' \geq n_0$ such that $\mu_{\mathcal{A}_f,f}(n') \geq n'^{-c'}$. Therefore, $\mu_{\mathcal{A}_f,f}$ is non-negligible. ■

6. We've reached a contradiction because $\mu_{\mathcal{A}_f,f}$ must be negligible for any PPT $\mathcal{A}_f$. Therefore, the initial assumption was false, and in fact, h is a one-way function.

■