CS178 Assignment 3

Jonas Chen

March 06, 2025

Problem 1

> Let $F : \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^\lambda$ be a pseudorandom function.
>
> Define $G : \{0,1\}^\lambda \times \{0,1\}^{2n} \to \{0,1\}^\lambda$ such that $G(k, x_1 \parallel x_2) = F(F(k, x_1), x_2)$ where $|x_1| = |x_2| = n$
>
> Show that G is also a pseudorandom function.

Solution

Since F is a pseudorandom function, then we know that $F(k,x) \underset{c}{\approx} u$ such that $x \in \{0,1\}^n, u \xleftarrow{\$} \{0,1\}^\lambda (\dagger)$

(this version of the definition for security of PRFs is both implied by the oracle definition and defined in class in the prf "game")

Fix a key $k = |\lambda|$ and let H be the set of all random functions from $\{0,1\}^\lambda \times \{0,1\}^{2n} \to \{0,1\}^\lambda$

Goal: show that queries to G_k are indistinguishable from queries to h_k

Consider the following distributions:

$H_1 \coloneqq \left\{G_k(x_1, x_2) : x_1, x_2 \xleftarrow{\$} \{0,1\}^n\right\}$

$H_2 \coloneqq \left\{G_k(x_1 \| x_2) : x_1, x_2 \xleftarrow{\$} \{0,1\}^n\right\}$

$H_3 \coloneqq \left\{F(F(k, x_1), x_2) : x_1, x_2 \xleftarrow{\$} \{0,1\}^n\right\}$

$H_4 \coloneqq \left\{F(z, x_2) : x_1, x_2 \xleftarrow{\$} \{0,1\}^n; z \coloneqq F(k, x_1) \in \{0,1\}^\lambda\right\}$

$H_5 \coloneqq \left\{u : u \xleftarrow{\$} \{0,1\}^\lambda\right\}$

$H_6 \coloneqq \left\{h_k(x_1, x_2) : x_1, x_2 \xleftarrow{\$} \{0,1\}^n\right\}$ where $h_k \xleftarrow{\$} H$

Note that $H_1 \underset{c}{\approx} H_2 \underset{c}{\approx} H_3$ by definition of G

Also $H_3 \approx H_4$ by definition of z

Also $H_4 \underset{c}{\approx} H_5$ by $(\dagger)$

Finally, $H_5 \underset{c}{\approx} H_6$ by definition of random function

By transitivity $H_1 \underset{c}{\approx} H_6$ and therefore any queries that some PPT A makes to an orcale that could be G_k or h_k is indisguishable from queries to the function that the oracle is not.

Since G makes 2 invocations of F, and F runs in polynomial time then G also runs in polynomial time

It follows that G is a pesudorandom function.

Problem 2

> Let $G : \{0,1\}^\lambda \to \{0,1\}^m$ be a secure pseudorandom generator, where $\lambda < m$. Given $x \in \{0,1\}^n$ and $k \in \{0,1\}^{2n\cdot\lambda}$, we split k into $2n$ substrings of length λ, where $k = (S_{1,0}, S_{1,1}, ..., S_{n,0}, S_{n,1})$ and $|S_{i,j}| = \lambda$ and define S_{i,x_i} as follows:
>
> $$S_{i,x_i} = \begin{cases} S_{i,0} \text{ if } x_i = 0 \\ X_{i,1} \text{ if } x_i = 1 \end{cases}$$
>
> Where x_i is the ith bit of $x_1, ..., x_n$. Let $F : \{0,1\}^{2n\lambda} \times \{0,1\}^n \to \{0,1\}^m$ be a pseudorandom function where
>
> $$F(k,x) = G(S_{1,x_1}) \oplus ... \oplus G(S_{n,x_n})$$
>
> Show that F is not a secure pseudorandom function

Solution

Let $\mathcal{G}_{n,m}$ be the set of random functions from $\{0,1\}^n \to \{0,1\}^m$ Consider the following 4 inputs into F :

$x_1 = (0000...)$; $x_2 = (1111...)$; $x_3 = (000, ..., 1, ..., 000)$; $x_4 = (111, ..., 0, ...111)$

i.e. the first input is all $0'$s, second input is all $1'$s, and the last two inputs are negations of eachother. We consider the specific example listed above where we have two strings of $0'$s and $1'$s expect at the mth position. Consider the following:

$F(k,x_1) = G(S_{1,0}) \oplus ... \oplus G(S_{n,0}) = G(S_{1,0}) \oplus ...G(S_{m,0}) \oplus ... \oplus G(S_{n,0})$

$F(k,x_2) = G(S_{1,1}) \oplus ... \oplus G(S_{n,1}) = G(S_{1,1}) = G(S_{m,1}) \oplus ... \oplus G(S_{n,1})$

$F(k,x_3) = G(S_{1,0}) \oplus ... \oplus G(S_{m,1}) \oplus ... \oplus G(S_{n,0})$

$F(k,x_4) = G(S_{1,1}) \oplus ... \oplus G(S_{m,0}) \oplus ... \oplus G(S_{n,1})$

We have $F(k,x_1) \oplus F(k,x_2) \oplus F(k,x_3) \oplus F(k,x_4) = \bigoplus_{i=1}^{n} \bigoplus_{j=0}^{1} [G(S_{i,j}) \oplus G(S_{i,j})] = \bigoplus_{i=1}^{n} 0^m = 0^m$ since $\oplus$ is commutative

Then, if some adversary A querys an oracle on inputs x_1, x_2, x_3, x_4 where the oracle could be F or $g \in \mathcal{G}_{n,m}$ then A will know with probability $1 - \frac{1}{2^m}$ that the oracle is F if $F(k,x_1) \oplus F(k,x_2) \oplus F(k,x_3) \oplus F(k,x_4) = 0^m$, and since g outputs $0, ..., 0 \in \{0,1\}^m$ with probability $\frac{1}{2^m}$

Specifically, applying the definition of pseudorandom functions, set $(\cdot) = (x_1, x_2, x_3, x_4)$ then we have

$$|\Pr\left[1 \leftarrow A^{F(k,\cdot)} : k \xleftarrow{\$} \{0,1\}^\lambda\right] - \Pr\left[1 \leftarrow A^{g(\cdot)} : g \xleftarrow{\$} \mathcal{G}_{n,m}\right]| =$$

$$|\ 1 - \Pr[g(x_1) \oplus g(x_2) \oplus g(x_3) \oplus g(x_4) = 0]\ | = |1 - \Pr[g(x_1) \oplus g(x_2) = g(x_3) \oplus g(x_4)]| =$$

$$|1 - \Pr\left[z_1 = z_2 : z_1, z_2 \xleftarrow{\$} \{0,1\}^m\right]| = |1 - \frac{1}{2^m}| \not\leq \mathrm{negl}(\lambda)$$

Therefore F is not a secure pesudorandom function

(note that an A exists which breaks the security of F and is defined as: 1. query the orcale on input $x_1, ..., x_4$ 2. check if the queries xor to 0 and if so, guess F and else guess g)

Problem 3

> Let $\mathcal{F} = \{f_k : \{0,1\}^n \to \{0,1\}^m : k \in \{0,1\}^\lambda\}$ be a class of functions such that for every $k \in \{0,1\}^\lambda$, f_k is one-way and moreoever, $m < n$. Using $\mathcal{F}$ design another function class $\mathcal{F}' = \{f'_k : \{0,1\}^n \to \{0,1\}^m : k \in \{0,1\}^\lambda\}$ such that
>
> a) for every $k \in \{0,1\}^\lambda$, f'_k is a one-way function
>
> b) $\mathcal{F}'$ is not collision resistant

Solution

For each $f'_k \in \mathcal{F}'$ we can define f'_k to be f_k but $f'_k\left(\underbrace{(0, ..., 0)}_{\text{n zeros}}\right) = f'_k\left(\underbrace{(1, ..., 1)}_{\text{n ones}}\right)$, i.e. introduce one collision and everything else the same

Clearly, $\mathcal{F}'$ is not collision resistant since for each $f'_k \in \mathcal{F}'$ the probability of finding a collision is 1 (The adversary knows the definition of f'_k)

Next, we show that each $f'_k \in \mathcal{F}'$ is one-way:

The goal is to show that f'_k is computable in polynomial time (this is clearly true) and crucially that

For all PPT A we have that (by total probability):

$$\Pr\left[A(1^n, f'(x)) \to x' : f'(x') = f'(x); x \xleftarrow{\$} \{0,1\}^n\right] =$$

$$\Pr\left[A(1^n, f'(x)) \to x' : f'(x') = f'(x); x \xleftarrow{\$} \{0,1\}^n \mid x = (0, ..., 0) \lor x = (1, ..., 1)\right] \cdot$$

$$\Pr[x = (0, ..., 0) \lor x = (1, ..., 1)]$$

$$+$$

$$\Pr\left[A(1^n, f'(x)) \to x' : f'(x') = f'(x); x \xleftarrow{\$} \{0,1\}^n \mid x \neq (0..., 0) \land x \neq (1, ..., 1)\right] \cdot$$

$$\Pr[x \neq (0, ..., 0) \land x \neq (1, ..., 1)] =$$

$$(1)\left(\frac{2}{2^n}\right) + \text{negl}(n)\left(1 - \frac{2}{2^n}\right) = \frac{2}{2^n} + \text{negl}(n) - \text{negl}(n)\left(\frac{2}{2^n}\right)$$

In class, we showed that the addition of two neglible functions is still neglible

In addition we showed that a neglible function multiplied by a polynomial function is neglible. Here we have two neglible functions multiplied with eachother, which is clearly neglible.

The conclusion is that each $f'_k \in \mathcal{F}'$ satisfies the definition of a one-way function.