CS178 Assignment 3

Jonas Chen

March 02, 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

Suppose for contradiction that G is not a pseudorandom function

Since F is a pseudorandom function, then we know that

(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 U be the set of all random functions from $\{0,1\}^{\lambda+2n} \to \{0,1\}^\lambda$

Goal: show that $\left\{G(\lambda, x_1, x_2) : x_1, x_2 \xleftarrow{\$} \{0,1\}^n\right\} \underset{c}{\approx} \{u : \{0,1\}^{\lambda+2n} \to \{0,1\}^\lambda\} = U$

Consider the following distributions:

$H_0 = \{G_k : k \in \{0,1\}^\lambda\}$ is the distribution of PRFs G with key k

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

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

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

$H_4 = \left\{F(z_1, x_2) : x_1 \xleftarrow{\$} \{0,1\}^n, z_1 := F(k, x_1) \in \{0,1\}^\lambda\right\}$

$H_5 = \left\{u : u \xleftarrow{\$} \{0,1\}^{\lambda+2n}\right\}$

$H_6 = \{\}$

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 $1 - \frac{1}{2^n}$ that the oracle is F if $F(k, x_1) \oplus F(k, x_2) \oplus F(k, x_3) \oplus F(k, x_4) = 0^m$, since g outputs $0, ..., 0 \in \{0,1\}^m$ with probability $\frac{1}{2^n}$

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

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

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

$$|1 - \Pr\left[z_1 = z_2 : z_1, z_2 \xleftarrow{\$} \{0,1\}^m\right]| = |1 - \frac{1}{2^m}| \nleq \text{negl}(\lambda)$$

Therefore F is not a secure pesudorandom function

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