CS 276: Homework 2

Due Date: Sept. 13th, 2024 at 8:59pm via Gradescope

1 One-Way Functions

The security of a PRF is only guaranteed if the key is kept secret. However, [GGM86]'s PRF construction still retains some form of security (namely weak one-wayness) even if the key is leaked.

Definition 1.1 ([GGM86] Function Ensemble) *Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG, where $G_0(s)$ outputs the first n bits of $G(s)$ and $G_1(s)$ outputs the last n bits of $G(s)$.*

For any seed $s \in \{0,1\}^n$, and any input $x = (x_1, \ldots, x_n) \in \{0,1\}^n$, let the function $f_s^G : \{0,1\}^n \to \{0,1\}^n$ be defined as follows:

$$f_s^G(x_1, \ldots, x_n) = G_{x_n}\Big(\ldots G_{x_2}\big(G_{x_1}(s)\big) \ldots \Big)$$

We sometimes write f_s^G as f_s.

Finally let us define the function ensemble $\mathcal{F}_G = \{f_s^G\}_{s \in \{0,1\}^n}$.

Definition 1.2 (One-Way Function Ensemble) *Let $\mathcal{F} = \{f_s\}_{s \in \{0,1\}^n}$ be a function ensemble where for every $s \in \{0,1\}^n$, f_s maps $\{0,1\}^n \to \{0,1\}^n$ and is efficiently computable.*

*$\mathcal{F}$ is **one-way** if for any efficient adversary $\mathcal{A}$,*

$$\Pr_{\substack{s \xleftarrow{\$} \{0,1\}^n \\ x \xleftarrow{\$} \{0,1\}^n}} \left[\mathcal{A}(s, f_s(x)) \in f_s^{-1}(f_s(x))\right] \leq \mathsf{negl}(n)$$

Question: Prove that $\mathcal{F}_G$ is one-way, assuming conjecture 1.3 below.

Conjecture 1.3

$$\mathbb{E}_{s \xleftarrow{\$} \{0,1\}^n} \left[\frac{|\mathsf{Img}\,(f_s)\,|}{2^n}\right] \geq 1 - \mathsf{negl}(n)$$

Note: We do not know if this conjecture is true, but it is still possible to prove that $\mathcal{F}_G$ is *weakly* one-way without the conjecture.

If you're unsure how to get started, try assuming that f_s is one-to-one. This is a useful setting in which to build intuition.

References

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *J. ACM*, 33(4):792807, aug 1986.