Lecture 13: Pseudo-random Functions

Random Functions

- A function $f\colon \{0,1\}^n \rightarrow \{0,1\}^n$ is described by the list of values $(f(0), \ldots, f(2^n - 1))$
- So, f is described by a length $n \cdot 2^n$ long bit-string
- Note that any length $n \cdot 2^n$ long bit-string corresponds to a function, and no two different functions have an identical $n \cdot 2^n$ long bit-string description
- So, the set of all functions from $\{0,1\}^n \rightarrow \{0,1\}^n$ has a bijection to the set of all bit-strings of length $n \cdot 2^n$
- Let $\mathcal{F}_n$ be the set of all functions that map $\{0,1\}^n \rightarrow \{0,1\}^n$
- Then, due to the bijection, $|\mathcal{F}_n| = 2^{n \cdot 2^n}$

Definition (Random Function)

A function $f \xleftarrow{\$} \mathcal{F}_n$ is a *random function*

Pseudo-Random Functions

Let $\mathcal{H}_n \subseteq \mathcal{F}_n$ and consider the following experiment between an honest challenger $\mathcal{H}$ and an arbitrary efficient adversary $\mathcal{A}$

- The honest challenger $\mathcal{H}$ samples $b \xleftarrow{\$} \{0,1\}$. If $b = 0$, it draws $f \xleftarrow{\$} \mathcal{H}_n$, otherwise $f \xleftarrow{\$} \mathcal{F}_n$.
- For $i = 1$ to q, the adversary $\mathcal{A}$ provides $x^{(i)} \in \{0,1\}^n$ and the honest challenger $\mathcal{H}$ replies with $y^{(i)} = f(x^{(i)})$
- The adversary $\mathcal{A}$ provides a bit $\widetilde{b}$ to the honest challenger $\mathcal{H}$.
- The honest challenger outputs $z = 1$, if $b = \widetilde{b}$, otherwise outputs $z = 0$

Definition

Pseudo-random Function $\mathcal{H}_n$ is called a family of pseudorandom functions if the advantage of any computationally bounded adversary $\mathcal{A}$ is at most a negligible

Goldreich-Goldwasser-Micali Construction

- Let $G_n\colon \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG
- Define functions $G_n^{(0)}\colon \{0,1\}^n \to \{0,1\}^n$ and $G_n^{(1)}\colon \{0,1\}^n \to \{0,1\}^n$ as follows.
  - $G_n^{(0)}(s)$ is the first n-bits of $G_n(s)$
  - $G_n^{(1)}(s)$ is the last n-bits of $G_n(s)$
  - Note: We have $G_n(s) = (G_n^{(0)}(s), G_n^{(1)}(s))$
- For $s \in \{0,1\}^n$, define $f_s\colon \{0,1\}^n \to \{0,1\}^n$ as the function:

$$f_s(x) = G_n^{(x_n)}(\cdots G_n^{(x_2)}(G_n^{(x_1)}(s))\cdots),$$

  where $x = x_1 x_2 \ldots x_n$.
- Let $\mathcal{H}_n = \{f_s\colon s \in \{0,1\}^n\}$

Theorem (GGM is a PRF)

The set of function $\mathcal{H}_n$ defined above is a PRF family

Additional Notes

- We will not prove the theorem that GGM construction provides PRFs
- Interested students are referred to the following lecture notes: link 1 and link 2
- There is another construction of PRFs known as the Naor-Reingold Construction that is provided in the above mentioned lecture notes. The GGM construction is highly sequential in nature, but the evaluation of the Naor-Reingold function can be easily parallelized. Albeit, the security of the Naor-Reingold construction is based on significantly stronger computational assumptions than the existence of OWF, unlike the security of the GGM construction.