Lecture 17: Pseudorandom Functions

Random Functions

- Let $\mathcal{F}_{m,n}$ be the set of all function from the domain $\{0,1\}^m$ to the range $\{0,1\}^n$
- Each function $f \in \mathcal{F}_{m,n}$ can be uniquely represented by a list of length $\{0,1\}^m$ where the i-th entry in the list is the entry $f(i)$, for $i \in \{0,1\}^m$
- So, each entry in the list has 2^n options. And, there are a total of 2^m such entries. So, the total number of distinct functions from the set $\{0,1\}^m \to \{0,1\}^n$ is

$$\overbrace{(2^n) \times \cdots \times (2^n)}^{2^m\text{-times}} = 2^{n2^m}$$

- So, we can conclude that each function $f \in \mathcal{F}_{m,n}$ can be described using $n2^m$ bits

Crucial Property of Random Functions

Intuition.

- Suppose we pick a random $f \xleftarrow{\$} \mathcal{F}_{m,n}$
- Then the evaluation of f at any input x_1 is uniformly random over $\{0,1\}^n$.
- Further, the evaluation of f at any other input x_2 given $f(x_1)$ is again uniformly random over $\{0,1\}^n$.
- In particular, the evaluation of f at an input x_t given $f(x_1), \ldots, f(x_{t-1})$ is uniformly random
- Intuitively, the evaluation of a random f is completely unpredictable at any <u>new</u> input

Formally. For any distinct inputs $x_1, \ldots, x_t \in \{0,1\}^m$ and any outputs $y_1, \ldots, y_t \in \{0,1\}^n$, the following holds

$$\mathbb{P}_{f \xleftarrow{\$} \mathcal{F}_{m,n}} \left[f(x_t) = y_t | f(x_1) = y_1, \ldots, f(x_{t-1}) = y_{t-1} \right] = \frac{1}{2^n}$$

Secret-key Encryption using Random Functions

Consider the following private-key encryption scheme

1. Gen(): Return $\mathsf{sk} = f \overset{\$}{\leftarrow} \mathcal{F}_{m,n}$
2. $\mathrm{Enc}_f(m)$: Pick a random $r \overset{\$}{\leftarrow} \{0,1\}^m$. Return $(m \oplus f(r), r)$, where $m \in \{0,1\}^n$.
3. $\mathrm{Dec}_f(\widetilde{c}, \widetilde{r})$: Return $\widetilde{c} \oplus f(\widetilde{r})$.

Features. Suppose the messages $m_1, \dots, m_u$ are encrypted as the cipher-texts $(c_1, r_1), \dots, (c_u, r_u)$.

- As long as the $r_1, \dots, r_u$ are all distinct, each one-time pad $f(r_1), \dots, f(r_u)$ are uniform and independent of others. So, this encryption scheme is perfectly secure!
- The probability that any two of the randomness in $r_1, \dots, r_u$ are not distinct is very small (We shall prove this later as "Birthday Paradox")
- This scheme is a "state-less" encryption scheme. Alice and Bob do not need to remember any private state (except the secret-key sk)!

Bottleneck of using Random Functions

- The secret-key sk needs $n2^m$ bits to represent it, which is exponentially large.
- We shall replace "random functions" using "pseudorandom functions" to construct an encryption scheme that has short keys and remains secure against computationally bounded adversaries!

Pseudo-random Functions (PRF)

- Let $\mathcal{G}_{m,n,k} = \{g_1, g_2, \ldots, g_{2^k}\}$ be a set of functions such that each $g_i \colon \{0,1\}^m \to \{0,1\}^n$
- This set of functions $\mathcal{G}_{m,n,k}$ is called a pseudo-random function if the following holds.

  Suppose we pick $g \xleftarrow{\$} \mathcal{G}_{m,n,k}$. Let $x_1, \ldots, x_t \in \{0,1\}^m$ be distinct inputs. Given $(x_1, g(x_1)), \ldots, (x_{t-1}, g(x_{t-1}))$ for any computationally bounded party the value $g(x_t)$ appears to be uniformly random over $\{0,1\}^n$

Secret-key Encryption using Pseudo-Random Functions

Before we construct a PRF, let us consider the following secret-key encryption scheme.

1. Gen(): Return $\mathsf{sk} = \mathsf{id} \xleftarrow{\$} \{1, \dots, 2^k\}$
2. $\mathsf{Enc}_{\mathsf{id}}(m)$: Pick a random $r \xleftarrow{\$} \{0,1\}^m$. Return $(m \oplus g_{\mathsf{id}}(r), r)$, where $m \in \{0,1\}^n$.
3. $\mathsf{Dec}_{\mathsf{id}}(\widetilde{c}, \widetilde{r})$: Return $\widetilde{c} \oplus g_{\mathsf{id}}(\widetilde{r})$.

Features. Suppose the messages $m_1, \dots, m_u$ are encrypted as the cipher-texts $(c_1, r_1), \dots, (c_u, r_u)$.

- As long as the $r_1, \dots, r_u$ are all distinct, each one-time pad $g_{\mathsf{id}}(r_1), \dots, g_{\mathsf{id}}(r_u)$ appear uniform and independent of others to computationally bounded adversaries. So, this encryption scheme is secure against computationally bounded adversaries!
- The probability that any two of the randomness in $r_1, \dots, r_u$ are not distinct is very small (We shall prove this later as "Birthday Paradox")
- This scheme is a "state-less" encryption scheme. Alice and Bob do not need to remember any private state (except the secret-key sk)!

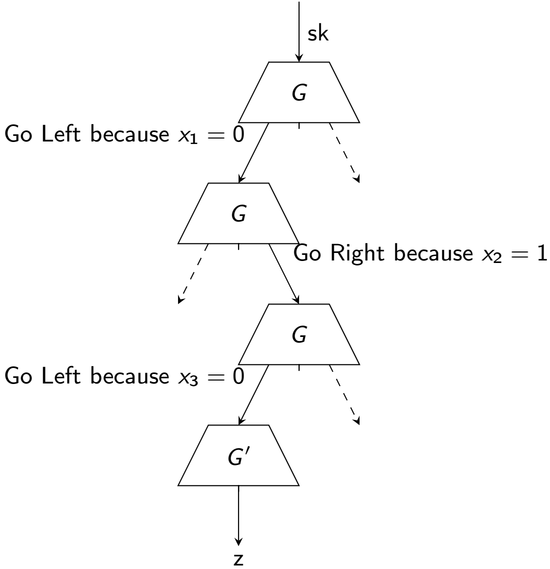
Construction of PRF I

- We shall consider the construction of Goldreich-Goldwasser-Micali (GGM) construction.
- Let $G\colon \{0,1\}^k \to \{0,1\}^{2k}$ be a PRG. We define $G(x) = (G_0(x), G_1(x))$, where $G_0, G_1\colon \{0,1\}^k \to \{0,1\}^k$
- Let $G'\colon \{0,1\}^k \to \{0,1\}^n$ be a PRG
- We define $g_{\text{id}}(x_1 x_2 \dots x_m)$ as follows

$$G'\left(G_{x_m}(\cdots G_{x_2}(G_{x_1}(\text{id}))\cdots)\right)$$

Construction of PRF II

Consider the execution for $x = x_1x_2x_3 = 010$. Output z is computed as follows.


sk
G
Go Left because $x_1 = 0$
G
Go Right because $x_2 = 1$
G
Go Left because $x_3 = 0$
G'
z

Pseudocodes

We give the pseudocode of algorithms to construct PRG and PRF using a OWP $f\colon \{0,1\}^{k/2} \to \{0,1\}^{k/2}$

- Suppose $f\colon \{0,1\}^{k/2} \to \{0,1\}^{k/2}$ is a OWP
- We provide the pseudocode of a PRG $G\colon \{0,1\}^k \to \{0,1\}^t$, for any integer t, using the one-bit extension PRG construction of Goldreich-Levin hardcore predicate construction. Given input $s \in \{0,1\}^k$, it outputs $G(s)$.

```
G(k, t, s):
1. Interpret $s = (r, x)$, where $r, x \in \{0,1\}^{k/2}$
2. Initialize bits = [ ] (i.e., an empty list)
3. Initialize $z = x$
4. For $i = 1$ to $t$:
    1. bits.append($\langle r, z\rangle$), here $\langle \cdot, \cdot \rangle$ is the inner-product
    2. $z = f(z)$
5. Return bits
```

Pseudocodes II

- We provide the pseudocode of the PRF $g_{\mathrm{id}}\colon \{0,1\}^m \to \{0,1\}^n$, where $\mathrm{id} \in \{0,1\}^k$, using the GGM construction. Given input $x \in \{0,1\}^m$, it outputs $g_{\mathrm{id}}(x)$.

```
$g(m, n, k, \mathrm{id}, x)$:
  1. Interpret $x = x_1 x_2 \ldots x_m$, where $x_1, \ldots, x_m \in \{0,1\}$
  2. Initialize $\mathrm{inp} = \mathrm{id}$
  3. For $i = 1$ to $m$:
       1. Let $y = G(k, 2k, \mathrm{inp})$
       2. If $x_i = 0$, then inp is the first $k$ bits of $y$. Otherwise (if
          $x_i = 1$), inp is the last $k$ bits of $y$.
  4. Return $G(k, n, \mathrm{inp})$
```

Birthday Bound

- Suppose we have a set $S = \{s_1, s_2, \ldots, s_n\}$
- Suppose we sample an element x_1 uniformly at random from the set S.
- Replace this element back in the set S and sample an element x_2 uniformly at random from the set S
- This process of sampling is referred to as "sampling with replacement"
- Suppose we sampled elements $\{x_1, x_2, \ldots, x_k\}$
- We are interested in understanding how likely is it that there are two elements $x_i = x_j$, such that $i \neq j$. Intuitively, we are interested in finding the probability that k elements when sampled uniformly at random from S (with replacement) encounters a collision

Birthday Bound

- Why are we studying this probability? Recall that earlier in this lecture we noted that if all the random r's chosen in the encryption algorithm are distinct, then the encryption scheme remains secure against computationally bounded eavesdroppers. So, the probability that we are computing shall help us determine the length of the randomness so that it is highly unlikely to encounter collisions.
- Okay, let us start by studying the complementary event. We are interested in the event that all the samples $\{x_1, x_2, \dots, x_k\}$ are distinct
- Note that the probability that x_1 is distinct from all previous samples is 1
- Conditioned on the fact that $\{x_1\}$ is distinct, the probability that x_2 is distinct from all previous samples is $\left(1 - \frac{1}{n}\right)$

Birthday Bound

- Conditioned on the fact that $\{x_1, x_2\}$ are distinct, the probability that x_3 is distinct from all previous samples is $\left(1 - \frac{2}{n}\right)$
- Extrapolating these observations, we can conclude the following. Conditioned on the fact that $\{x_1, x_2, \dots, x_{i-1}\}$ are distinct, the probability that x_i is distinct from all previous samples is $\left(1 - \frac{i-1}{n}\right)$
- So, using the chain rule, we can conclude the following. The probability that $\{x_1, \dots, x_k\}$ are all distinct is the following product.

$$1 \cdot \left(1 - \frac{1}{n}\right) \cdot \left(1 - \frac{2}{n}\right) \cdots \left(1 - \frac{k-1}{n}\right)$$

Birthday Bound

- This expression is the product that we saw in the midterm. We shall use the fact that $\exp(-x) \approx 1 - x$ when $0 \leqslant x \ll 1$. This fact can be made more mathematically precise using Taylor's Remainder Theorem, which is beyond the scope of this course. So, in this course, we shall proceed by using $\exp(-x) \approx 1 - x$
- So, let us begin the manipulation of the expression above

$$
\begin{aligned}
& 1 \cdot \left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right)\cdots\left(1 - \frac{k-1}{n}\right) \\
\approx & \exp(-0)\exp(-1/n)\exp(-2/n)\cdots\exp(-(k-1)/n) \\
= & \exp\left(-0 - \frac{1}{n} - \frac{2}{n} - \cdots - \frac{k-1}{n}\right) \\
= & \exp\left(-\frac{k(k-1)}{2n}\right) \approx \exp(-k^2/2n) = \exp(-k^2/2|S|)
\end{aligned}
$$

Birthday Bound

- Suppose we set $k = \sqrt{|S|}/100$. Substituting this value of k in the formula above, note that the probability that all the samples are distinct is $\approx \exp(-1/20000)$, which is very close to 1!
- Suppose we set $k = 100\sqrt{|S|}$. Substituting this value of k in the formula above, note that the probability that all the sample are distinct is $\approx \exp(-5000)$, which is very close to 0!
- Intuitively, it says that if $k \leqslant \sqrt{|S|}/100$, all samples are very likely to be distinct. On the other hand, if $k \geqslant 100\sqrt{|S|}$, it is highly unlikely that all samples are distinct (that is, there exists two identical samples; or collision occurs)

A Numerical Example of the Birthday Bound

- Suppose we are picking uniform random strings from the set $\{0,1\}^n$
- Our objective is that 2^{1000} random samples have a collision with probability at most 2^{-80}
- What value of n should we use?

- So, we have $S = \{0,1\}^n$. The size of the set S is 2^n.
- The probability that k samples are all distinct is $\exp(-k^2/2|S|) = \exp(-k^2/2^{n+1})$. The problem states that we shall pick $k = 2^{1000}$ samples.
- Our objective is to have collision probability $\leqslant 2^{-80}$. That is, the probability of all samples being distinct is $\geqslant 1 - 2^{-80}$.
- So, we have the following equation and we need to solve for n

$$\exp(-k^2/2^{n+1}) = \exp(-2^{2000}/2^{n+1}) \geqslant 1 - 2^{-80} \approx \exp(-2^{-80})$$

- Solving this equation is left as an exercise