Lecture 11: Using and Constructing PRG

Encryption

Suppose $G_{n,\ell}\colon \{0,1\}^n \rightarrow \{0,1\}^\ell$ be a PRG. Consider the encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$

- $\mathsf{Gen}(1^n)$ outputs $\mathsf{sk} \sim U_{\{0,1\}^n}$
- $\mathsf{Enc}_{\mathsf{sk}}(m)$ outputs $m + G_{n,\ell}(\mathsf{sk})$, where $m \in \{0,1\}^\ell$
- $\mathsf{Dec}_{\mathsf{sk}}(c)$ outputs $c - G_{n,\ell}(\mathsf{sk})$

Computational Security

- The security game is defined between an honest challenger and any arbitrary efficient adversary $\mathcal{A}$
- The adversary $\mathcal{A}$ sends two messages $(m^{(0)}, m^{(1)})$ of same length to the honest challenger $\mathcal{H}$
- The honest challenge $\mathcal{H}$ samples $\mathsf{sk} = \mathsf{Gen}(1^n)$, picks $b \stackrel{\$}{\leftarrow} \{0,1\}$, and sends $c = \mathsf{Enc}_{\mathsf{sk}}(m^{(b)})$ to the adversary $\mathcal{A}$
- The adversary $\mathcal{A}$ replies back with a bit $\widetilde{b}$
- The honest challenger outputs $z = 1$ if and only if $b = \widetilde{b}$

An encryption scheme is computationally secure if there exists a negligible function ε such that $\frac{1}{2} - \varepsilon \leqslant \Pr[z = 1] \leqslant \frac{1}{2} + \varepsilon$

PRG $\implies$ Our Encryption Scheme is Secure

- We shall prove the contrapositive
- Suppose there exists an efficient adversary $\mathcal{A}^*$ that can ensure $\Pr[z = 1] > \frac{1}{2} + \frac{1}{n^c}$, for a constant $c > 0$
- Our task is to construct an efficient adversary $\widetilde{\mathcal{A}}$ that can distinguish the output of $G_{n,\ell}(U_{\{0,1\}^n})$ from $U_{\{0,1\}^\ell}$
- Following is the code for $\widetilde{\mathcal{A}}$ when it receives a sample $s \in \{0,1\}^\ell$:
    - Instead of using $G_{n,\ell}(\mathsf{sk})$ as the mask in the encryption algorithm, use s as the mask
- Prove that this adversary can distinguish the output of $G_{n,\ell}(U_{\{0,1\}^n})$ from $U_{\{0,1\}^\ell}$. Hint: Note that if $s \sim U_{\{0,1\}^\ell}$ then $\Pr[z = 1] = \frac{1}{2}$ (why?); and if $s \sim G(U_{\{0,1\}^n})$ then $\Pr[z = 1] > \frac{1}{2} + \frac{1}{n^c}$ (why?).

Background on PRG Construction

- It is known that one-way functions, i.e., functions that are easy to compute but hard to invert, are necessary to construct PRGs
- It has also been shown that one-way functions suffice to construct PRGs
- In this course, we will see a construction of PRG from one-way permutations (which is slightly more structured that one-way functions)

One-way Functions

Definition (One-way Function)

A function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ is a one-way function if for any arbitrary efficient adversary $\mathcal{A}$, there exists a negligible ε such that the following holds:

$$\Pr[x \sim U_{\{0,1\}^n}, y = f(x) \colon \mathcal{A}(y) \in f^{-1}(y)] \leqslant \varepsilon$$

Intuition: For a randomly sampled x, any efficient adversary $\mathcal{A}$ is unable to find a pre-image of y.

One-way Permutations

Definition (One-way Permutation)

A function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ is a one-way permutation if it is a permutation (i.e., a bijection) and a one-way function.

Comment: We prefer to have secure constructions based on OWFs, if possible, instead of OWPs

Example Reduction

Claim

Let $f_n\colon \{0,1\}^n \to \{0,1\}^n$ *be a one-way permutation. Prove that* $g_n\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n \times \{0,1\}^n$ *defined by* $g_n(x,r) = (f_n(x), r)$ *is also a one-way permutation.*

- Proof that g_n is a permutation: Suppose $g(x', r') = g(x'', r'') = (y, r)$ such that $(x', r') \neq (x'', r'')$. Then, note that $r' = r'' = r$. This implies that $f_n(x') = f_n(x'') = y$ such that $x' \neq x''$. This violates the assumption that f_n is a permutation.
- One-way-ness: Suppose $\mathcal{A}^*$ is able to invert g_n with probability $1/n^c$. Then, consider the adversary $\widetilde{\mathcal{A}}$ that on input $y \in \{0,1\}^n$ does the following. It samples $r \sim U_{\{0,1\}^n}$ and outputs $\mathcal{A}^*(y, r)$. Prove that this successfully inverts f_n with $1/\mathrm{poly}$ probability.

Hardcore Predicate

Definition (Hardcore Predicate)

Let $f_n\colon \{0,1\}^n \to \{0,1\}^n$ be a OWF. A function $h_n\colon \{0,1\}^n \to \{0,1\}$ is a hardcore predicate for f_n if for any arbitrary efficient adversary $\mathcal{A}$ there exists a negligible function ε such that the following holds.

$$\Pr[x \sim U_{\{0,1\}^n} \colon \mathcal{A}(f(x)) = h(x)] \leqslant \frac{1}{2} + \varepsilon$$

Intuition: Even given $f(x)$, for a randomly sampled x, any efficient adversary cannot predict the bit $h(x)$

PRG Construction

- Suppose $f_n\colon \{0,1\}^n \to \{0,1\}^n$ is a OWP
- Suppose $h_n\colon \{0,1\}^n \to \{0,1\}$ is a hardcore predicate for f_n
- Consider the function $G_n\colon \{0,1\}^n \to \{0,1\}^{n+1}$ defined as follows: $G_n(x) = (f_n(x), h_n(x))$

Claim

G_n is a PRG

- Note that $f_n(x)$ is uniformly random string when $x \sim U_{\{0,1\}^n}$, because f_n is a permutation. So, every bit of $f_n(x)$ is unpredictable.
- The last bit $h_n(x)$ is unpredictable given $f_n(x)$, because of the definition of hardcore-bit
- By the next-bit unpredictability definition of PRG, we have shown that G_n is a PRG