Pseudorandom Function

2021年3月17日 19:22

Pseudorandom Function = Pseudorandom Generator = One-way function

Def. PRF.

A collection of functions $F = \{F_k : \{0,1\}^n \to \{0,1\}\}_{k \leftarrow K_n}$ is a PRF family if:

1. $\exists$ efficient algorithm $k \leftarrow K_n$
2. $\exists$ poly time $Eval(k, x) \to F_k(x)$.

. $\forall$ nuppt Adv. $\exists$ negl. ε. s.t. $\forall n \in N$

$$\left| Pr[k \leftarrow K_n, Adv^{F_k(\cdot)}(1^n) = 1] - Pr[Adv^{TR(\cdot)}(1^n) = 1] \right| < \varepsilon(n)$$

Difference from PRG:

- PRG does not choose a key. but PRF get a $k \xleftarrow{\$} K_n$
- PRG assumes given its description (the key) $G_k(x)$ but x is secret and random; while PRF keeps key random & secret but x can be chosen by Adversaries.

We can design a PRG that is not a PRF

$\{ G'_k(x) = \begin{cases} 0 & \text{if } x = 0 \\ G_k(x) & \text{otherwise} \end{cases} \}$.

(still indistinguishable since $Pr(x=0)$ is negl. but the adversary of PRF can query 0 and reach prob. difference of $\frac{1}{2}$)

Example.

$F: \{k = a, b \leftarrow \mathbb{Z}_p, F_k(x) = ax + b \mod p\}$

Adv: query $x_1 = 1, x_2 = 2, x_3 = 3 \Rightarrow$ if $f(x_1) - f(x_2) \equiv f(x_2) - f(x_3) \mod p$.

Guess: 0 (not Truly Random)

Hence, F is not a PRF.

PRG $\Rightarrow$ PRF. Goldreich, Goldwasser, Micali 84). GGM

$G: \{0,1\}^n \to \{0,1\}^{2n}$ PRG.

G_0, G_1 / G / s

$G(s) = G_0(s) \mid G_1(s)$.

key $K_n = \{0,1\}^n$, $k \xleftarrow{\$} K_n$, Domain $D = \{0,1\}^\ell$, $R = \{0,1\}^n$

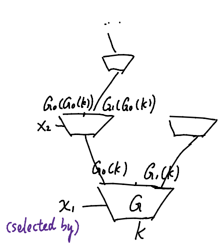
Let $F_k(\underline{x}) = G_{x_\ell}(\cdots G_{x_2}(G_{x_1}(k)) \cdots)$

$x = x_1 x_2 \cdots x_\ell$.

use input bits to determine right/left.

$\downarrow$

Binary Tree



"exponentially stretch PRG"

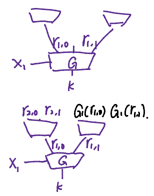
$F_k(x) = G_{x^{th}\ bit}(x)$.

Proof. Hybrid Argument.

$$\text{Assume Adv. queries} \quad \begin{array}{ccc} \text{“}L\text{”} & & \text{“}R\text{”} \\ x^{(1)} \to F_k(x^{(1)}) & \text{(Goal)} & x^{(1)} \to r^{(1)} \\ x^{(2)} \to F_k(x^{(2)}). & \approx_c & \cdots \\ \cdots & & \cdots \end{array}$$

Hybrid:

$L \to$



$\to$

at least one non-negl. $\geq \dfrac{\delta}{\ell \cdot \text{poly}(n)}$.

↑ H queries

$\to \cdots \to R$

PRF $\to$ PRG (easier).

$$F = \{F_k : D \to \{0,1\}\}_{k \in K_n}$$

$$G(k) = F_k(0) | \cdots | F_k(|D|-1)$$

$$\Rightarrow \text{Construct } G : \{0,1\}^n \to \{0,1\}^{|D|}$$

Recall Diffie-Hellman Problem.

$$g \in \mathbb{Z}_p. \quad DH: g, g^a, g^b \to g^{ab}.$$

Decisional Diffie Hellman. (DDH).

public parameters: G. $|G|$, g.

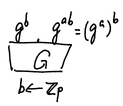
$$\{g^a \cdot g^b \cdot g^{ab}\} \approx_c \{g^a \cdot g^b \cdot g^c\}. \quad a,b,c \leftarrow \mathbb{Z}_p.$$

Remark: Solve Computational DH $\to$ Decisional DH.

Construct PRG from DDH:

$$G : \mathbb{Z}_p \to G \times G.$$

G_{g^a} ↖ key $\Rightarrow$



$$\underset{k}{\underline{\underline{g^a}}}, \underset{G_k(b)}{\underline{\underline{g^b \cdot g^{ab}}}} \approx_c g^a \cdot \underset{G}{g^b} \cdot \underset{G.}{g^c}$$

Construct PRF from DDH

$$K_n = \left\{ \begin{array}{ccc} \multicolumn{3}{c}{2\ell \text{ elems from } \mathbb{Z}_p.} \\ a_{1,0} & \cdots & a_{\ell,0} \\ a_{1,1} & & a_{\ell,1} \end{array} \right\}$$

$$F_k(x) = g^{a_{1,x_1} \cdot a_{2,x_2} \cdots a_{\ell,x_\ell}}$$

$x_1 | x_2 | \cdots | x_\ell$

(Naor-Reingold '97)