Construct pseudorandom generators

2021年3月15日 13:38

Secure Encryption from PRG.

- Recall Perfect Secrecy:
  $\Pr_k[Enc(m_1)=c] = \Pr_k[Enc(m_2)=c]$. $\forall m_1, m_2, c$.

$\downarrow$

Relax the definition: $\{Enc_k(m_1)\} \approx_c \{Enc_k(m_2)\}$

Namely, $\forall$ p.p.t. Adv. $\exists \varepsilon$. $\forall n \in N$

$$\left|\Pr[Adv(Enc_k(m_1)) \to 1] - \Pr[Adv(Enc_k(m_2)) \to 1]\right| < \varepsilon(n).$$

Consider:

$K = \{0,1\}^n$. $M = \{0,1\}^m$, $m > n$.

Gen : $s \leftarrow \{0,1\}^n$

$Enc(m, s) = m \oplus PRG(s)$.

$Dec(c, s) = c \oplus PRG(s)$.

Prove this satisfies def above.

Hybrid Proof: $H_0 = Enc_k(m_0) = m_0 \oplus PRG(\overset{U_n}{\downarrow}{s})$

$H_1 = m_0 \oplus Y \leftarrow U_m$

$H_2 = m_1 \oplus Y$

$H_3 = Enc_k(m_1) = m_1 \oplus PRG(s)$

PR Generator

$G: D \to R$ such that

$G(s) \approx_c U(R)$ and $|D| < |R|$

PRG $\Leftarrow$ One-way

Hardcore bit

A poly. computable function $h: \{0,1\}^n \to \{0,1\}$ is hardcore bit for a OWF f. if: $\forall$ p.p.t Adv. & negl. $\varepsilon(n)$

$$\Pr_{x, Adv}[Adv(1^n, f(x)) \to h(x)] < \frac{1}{2} + \varepsilon(n)$$

$$\Pr_{x,\mathrm{Adv}}[\mathrm{Adv}(1^n, f(x)) \to h(x)] < \frac{1}{2} + \varepsilon(n)$$

Example: $x \to g^x \bmod q$. $(q = 2p+1)$.

$$\underset{\text{most significant bit}}{\mathrm{MSB}}(x) = \begin{cases} 1 & \text{if } x > p/2 \\ 0 & \text{if } x < p/2. \end{cases} \Rightarrow \text{Hardcore bit}$$

Example 2: $\mathrm{RSA}(x) = x^e \bmod N$.

$\mathrm{LSB}(x) = x_n \quad (x = x_1 \dots x_n)$.

Suppose f is a OWP (permutation) $\{0,1\}^n \to \{0,1\}^n$. and h is f's hardcore bit.

then we can construct PRG: $\{0,1\}^n \to \{0,1\}^{n+1}$ as

$$x \xleftarrow{\$} \{0,1\}^n \mapsto \underset{\text{(concatenate)}}{f(x) \circ h(x)}$$

<u>Theorem</u> (GL) (hardcore bit always exists)

If f is a OWF

Then $g(\underbrace{x, r}_{\{0,1\}^n}) = f(x) \mid r$ concatenate

Define $h: \{0,1\}^{2n} \to \{0,1\}$

$x, r \mapsto \langle x, r \rangle \bmod 2$.

$\boxed{h \text{ is a hardcore bit}}$

<u>Prove</u>.

If $\Pr_{x,r}[\mathrm{Adv}(f(x), r) \to \langle x, r\rangle] > \frac{1}{2} + \delta$

1. If Adv. wins w.p.= 1.

$f(x)$. $r = 00 \dots 1 \to x_n$
$r = 00 \dots 10 \to x_{n-1}$
$\dots$
$\Rightarrow f$ not OWF

2. Adv wins w.p. $3/4 + \delta$

Def. $S_{good} = \{x \in \{0,1\}^n \mid \Pr_{r,\mathrm{Adv}}[\mathrm{Adv}(f(x), r) \to \langle x, r\rangle] > \frac{3}{4} + \delta/2\}$

– Claim: $|S_{good}| > \frac{\delta}{2} \cdot 2^n$ (non-negl.)

- Claim: $|S_{good}| > \frac{\delta}{2} \cdot 2^n$ (non-negl.)

Suppose $\Pr_{x \in \{0,1\}} [x \in S_{good}] < \delta/2$.

then. $\Pr_{x,r}[\, Adv(f(x),r) \to \langle x,r\rangle]$

$\leq \Pr[x \in S_{good}] \cdot 1 + (1 - \Pr[x \in S_{good}]) \cdot (3/4 + \delta)$

$\leq \frac{\delta}{2} + 3/4 + \delta/2 = \frac{3}{4} + \delta$. contradiction!

Then suppose x falls in this set.

$\begin{cases} r_1 = r & \text{fail} \leq \frac{1}{4} \\ r_2 = r + 000\cdots01 & \leq \frac{1}{4} \end{cases}$ } succeed in both w.p. $\geq \frac{1}{2} + \delta$

Then $\langle x, r_1\rangle - \langle x, r_2\rangle$ $\Rightarrow$ Get x.

$= \langle x, 000\cdots01\rangle = x_n$