Indistinguishability and Pseudorandomness

2021年3月10日 19:39

Pseudorandomness

Def. (Next-bit unpredictability)

$x \in \{0,1\}^n$, $x \leftarrow D$ is next-bit unpredictable

if $\forall$ nuppt. M $\exists$ neglible $\varepsilon(\cdot)$, s.t.

$$\forall i \in \{0,\cdots,n-1\},\ \Pr_{x \in D}\left[M(x_1,\cdots,x_i,1^n) \rightarrow x_{i+1}\right] \le \frac{1}{2} + \varepsilon(n).$$

non-uniform

Def. (Pseudorandom, Yao).

$x \leftarrow D$ is pseudorandom if $\forall$ nuppt. Adv., $\exists$ neglible $\varepsilon()$. s.t.

some literals write "1" in place of "random"

Also. def of Indistinguishability

$$\left|\Pr[x \leftarrow D,\ Adv(1^n,x) \rightarrow \text{"random"}] - \Pr[x \leftarrow U_n,\ Adv(1^n,x) \rightarrow \text{"random"}]\right| < \varepsilon(n)$$

uniform from $\{0,1\}^n$

PseudoRandomness $= D \approx U_n$

- namely, hard to distinguish distribution from unif. given sampled strings.

(Yao 82)

Theorem: Def Next bit Indistinguishability = Def. Pseudorandomness (Yao)

Def. (PR Generator) boost the randomness!

A poly-time computable function $G_n: \{0,1\}^n \rightarrow \{0,1\}^m$, $m > n$ is PRG ($m = poly(n)$)

if $s \leftarrow U(\{0,1\}^n)$, $G(s) = x \sim D$ and

$$D \approx_c U(\{0,1\}^m)$$

indistinguishable

c: short for computational.

Claim: If G is a PRG, then G is a one-way function.

Proof $2 \Rightarrow 1$ is easy. (Def of NBU is a specialization of Def 2[nd])

$1 \Rightarrow 2$. By contradiction. Suppose $\exists$ unppt Adv. and non-negliable function $\delta()$

$$\text{s.t. } \left|\Pr_{x \leftarrow D}[Adv(1^n,x) \rightarrow 1] - \Pr_{u \leftarrow U_n}[Adv(1^n,u) \rightarrow 1]\right| > \delta(n)$$

$$\text{Define } H^i = \{x \leftarrow D,\ u \leftarrow U_n \mid x_1 \cdots x_i u_{i+1} \cdots u_n\}$$

Define $H^i = \{x \leftarrow D,\ u \leftarrow U_n \mid x_1 \cdots x_i u_{i+1} \cdots u_n\}$

$$U = H^0 \approx_c H^1 \approx_c \cdots \approx_c H^n = D$$

by assumption. $\exists i.\ H^i \not\approx_c H^{i+1}$ ($\frac{\delta(n)}{n}$ still non-negligable)

$$\bar{H}^i = \{x \leftarrow D,\ u \leftarrow U_n \mid x_1 x_2 \cdots \bar{x}_i u_{i+1} \cdots u_n\}$$

Then, $H^i = \dfrac{H^{i+1} + \bar{H}^{i+1}}{2}$.

$$\left| \frac{1}{2} \Pr_{x \leftarrow H^{i+1}}[Adv(1^n, x) \to 1] + \frac{1}{2} \Pr_{x \leftarrow \bar{H}^{i+1}}[Adv(1^n, x) \to 1] - \Pr_{x \leftarrow H^{i+1}}[Adv(1^n, x) \to 1] \right| > \delta'(n)$$

Not Next-bit unpredictable by Def 1st.