Chapter 4 One-Way Function 单向函数

4.1 One-Way Function (OWF)

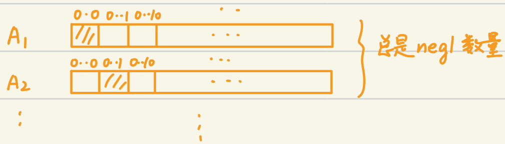
1. One-Way Function (OWF)

$f: \{0,1\}^* \to \{0,1\}^*$

① Easy to compute, $\exists$ poly-time algorithm

② Hard to invert, $\forall$ p.p.t A, $\Pr_{x \leftarrow \{0,1\}^n}[A(1^n, f(x)) \in f^{-1}(f(x))] \le negl(n)$ 给 A 一定时间运行

注：比PRG的 Uniform Distribution 弱



2. One-Way Permutation (OWP)

$f: \{0,1\}^* \to \{0,1\}^*$

① f is a OWF

② f is bijection (长度不变)

eg. $f: \mathbb{Z}_p \to \mathbb{Z}_p$, $f(x) = g^x \bmod p$

3. Weak OWF

Weak OWF:

① Easy to compute

② Hard to invert with $\frac{1}{poly(n)}$

$\forall$ sufficient large n, $\Pr_{x \leftarrow \{0,1\}^n}[A(f(x)) \in \{0,1\}^n \cap f^{-1}(f(x))] \le 1 - \frac{1}{poly(n)}$

eg. $f(x, y) = xy$, x, y 为 n bit

由于素数密度为 $\frac{1}{n}$，故 $\frac{1}{n^2}$ 为两个素数，但极大可能好分解（假设大素数分解很难）

$\exists$ Weak OWF $w \Rightarrow \exists$ OWF

Proof: $f(x_1, x_2 \cdots x_n) = w(x_1) w(x_2) \cdots w(x_n)$

则至少有一个落在很难 invert 的区域

$\exists$ OWF $\Rightarrow$ Construct Weak OWF (Universal OWF)

Proof: $x = \underbrace{0000\cdots0}_{i个}1x'$, $f(x) = (i, TM_i(x', \text{time limit} = |x|^2))$

由于每种 TM 以常数概率 chosen. ($\mathbb{P}[TM_0 = \frac{1}{2}]$, $\mathbb{P}[TM_1 = \frac{1}{4}]$ $\cdots$)

而又存在一个 OWF. (某一个 TM_i)

故至少以常数概率为 OWF. 即 Weak OWF

Proof: $x = \boxed{x_1 \mid x_2 \mid x_3 \mid \cdots}$

$f(x) = (TM_1(x_1), TM_2(x_2) \cdots)$

4.2 Hardcore Bit

For OWF f with hardcore bit $h: \{0,1\}^* \to \{0,1\}$:

If $\forall$ p.p.t A,

$$\mathbb{P}_{x \sim \{0,1\}^n}\left[A(1^n, f(x)) = h(x)\right] \leq \frac{1}{2} + negl(n)$$

注：很难猜出的某一位

eg. $f'(x \| y) = f(y)$，没有 x 的信息.

$\exists$ OWP with hardcore bit $\Rightarrow$ $\exists$ PRG

Proof: 令 OWP f, hardcore bit h, $g(x) = f(x) \| h(x)$

若 g 不是 PRG, $\exists$ p.p.t D, $\exists$ inf n,

$$\left|\mathbb{P}_{x \sim \{0,1\}^n}\left[D(f(x) \| h(x)) \to 1\right] - \mathbb{P}_{\substack{y \sim \{0,1\}^n \\ b \sim \{0,1\}}}\left[D(y \| b) \to 1\right]\right| \geq \frac{1}{poly(n)}$$

又由 f 定义

$$\left|\mathbb{P}_{\substack{x \sim \{0,1\}^n \\ b \sim \{0,1\}}}\left[D(f(x) \| b) \to 1\right] - \mathbb{P}_{\substack{y \sim \{0,1\}^n \\ b \sim \{0,1\}}}\left[D(y \| b) \to 1\right]\right| \leq negl(n)$$

$\therefore \exists$ p.p.t D, $\exists$ inf n,

$$\left| \mathbb{P}_{x \sim \{0,1\}^n}[D(f(x) \| h(x)) \to 1] - \mathbb{P}_{\substack{x \sim \{0,1\}^n \\ b \sim \{0,1\}}}[D(f(x) \| b) \to 1] \right| \geq \frac{1}{poly(n)}$$

$$\boxed{\begin{array}{l} \text{构造 } A(1^n, y)\text{，先随机 } b \in \{0,1\}\text{，运行 } D(y, b) \text{ 得到 } s, \\ \quad \text{输出} \begin{cases} b, & s = 1 \\ 1-b, & s = 0 \end{cases} \end{array}}$$

$\therefore \mathbb{P}[A(1^n, f(x)) = h(x)]$

$= \frac{1}{2} \mathbb{P}_{x \leftarrow \{0,1\}^n}[D(f(x) \| h(x)) \to 1] + \frac{1}{2} \mathbb{P}_{x \leftarrow \{0,1\}^n}[D(f(x) \| 1-h(x)) \to 0]$

$= \frac{1}{2} + \frac{1}{2}\left(\mathbb{P}_{x \leftarrow \{0,1\}^n}[D(f(x) \| h(x)) \to 1] - \mathbb{P}_{x \leftarrow \{0,1\}^n}[D(f(x) \| 1-h(x)) \to 1]\right)$

$= \frac{1}{2} + \mathbb{P}_{x \sim \{0,1\}^n}[D(f(x) \| h(x)) \to 1] - \mathbb{P}_{\substack{x \sim \{0,1\}^n \\ b \sim \{0,1\}}}[D(f(x) \| b) \to 1]$

$\geq \frac{1}{2} + negl(n)$

$\exists$ OWP f $\Rightarrow$ $\exists$ OWP with hardcore bit

Proof: 令 OWP f，$f'(x \| y) = x \| f(y)$ 也是 OWP

令 $h(x, y) = \langle x, y \rangle = \bigoplus_i x_i y_i$，下证 h 为 hardcore bit

① 先假设 $\exists A$，$\exists$ inf n，$\mathbb{P}_{x, y \leftarrow \{0,1\}^n}[A(x, f(y)) = \langle x, y \rangle] = 1$，

构造 A'：$\boxed{\text{对 } \forall i,\ y_i = A(x, f(y)) \oplus A(x \oplus e_i, f(y))}$

由于 $\langle e_i, y \rangle = \langle x, f(y) \rangle \oplus \langle x \oplus e_i, y \rangle$

则可得到 y 的每一位，即 $\mathbb{P}_{x, y \leftarrow \{0,1\}^n}[A'(f(y)) \in f^{-1}(f(y))] = 1$，矛盾

② 若 $\exists A$, $\exists$ inf n. $\underset{x,y\leftarrow\{0,1\}^n}{\mathbb{P}}\left[A(x,f(y))=\langle x,y\rangle\right] \geq \frac{3}{4}+\frac{1}{p(n)}$

引理1: $\underset{y\sim\{0,1\}^n}{\mathbb{P}}\left[\underset{x\sim\{0,1\}^n}{\mathbb{P}}\left[A(x,f(y))=\langle x,y\rangle\right] \geq \frac{3}{4}+\frac{1}{2p(n)}\right] \geq \frac{1}{2p(n)}$

Proof: 令 $S_n = \left\{ y \,\middle|\, \underset{x\sim\{0,1\}^n}{\mathbb{P}}\left[A(x,f(y))=\langle x,y\rangle\right] \geq \frac{3}{4}+\frac{1}{2p(n)} \right\}$

$$\underset{x,y}{\mathbb{P}}\left[A(x,f(y))=\langle x,y\rangle\right]$$

$$= \underset{x,y}{\mathbb{P}}\left[A(x,f(y))=\langle x,y\rangle \mid y\in S_n\right] \underset{y}{\mathbb{P}}\left[y\in S_n\right]$$

$$+ \underset{x,y}{\mathbb{P}}\left[A(x,f(y))=\langle x,y\rangle \mid y\notin S_n\right] \underset{y}{\mathbb{P}}\left[y\notin S_n\right]$$

$$\leq \underset{y}{\mathbb{P}}\left[y\in S_n\right] + \underset{x,y}{\mathbb{P}}\left[A(x,f(y))=\langle x,y\rangle \mid y\notin S_n\right]$$

$$\therefore \underset{y}{\mathbb{P}}\left[y\in S_n\right] \geq \underset{x,y}{\mathbb{P}}\left[A(x,f(y))=\langle x,y\rangle\right] - \underset{x,y}{\mathbb{P}}\left[A(x,f(y))=\langle x,y\rangle \mid y\notin S_n\right]$$

$$\geq \left(\frac{3}{4}+\frac{1}{p(n)}\right) - \left(\frac{3}{4}+\frac{1}{2p(n)}\right)$$

$$= \frac{1}{2p(n)}$$

引理2: 随机采样 $X_1 \cdots X_n \overset{\text{i.i.d}}{\sim} \{0,1\}^l$, 则

$\forall y_1\neq y_2 \in \{0,1\cdots 2^l\}$, $\bigoplus\limits_{y_1\oplus e_i\neq 0} X_i$ 与 $\bigoplus\limits_{y_2\oplus e_i\neq 0} X_i$ 独立 ($\bigoplus\limits_{y\oplus e_i\neq 0} X_i$ 两两独立)

Proof: $\mathbb{P}\left[\bigoplus\limits_{y_1\oplus e_i\neq 0} X_i = a,\ \bigoplus\limits_{y_2\oplus e_i\neq 0} X_i = b\right]$

$$= \mathbb{P}\left[\bigoplus_{\substack{y_1\oplus e_i\neq 0\\ y_2\oplus e_i=0}} X_i = a\oplus c,\ \bigoplus_{\substack{y_2\oplus e_i\neq 0\\ y_1\oplus e_i=0}} X_i = b\oplus c\right]$$

$$= \mathbb{P}\left[\bigoplus_{\substack{y_1\oplus e_i\neq 0\\ y_2\oplus e_i=0}} X_i = a\oplus c\right] \mathbb{P}\left[\bigoplus_{\substack{y_2\oplus e_i\neq 0\\ y_1\oplus e_i=0}} X_i = b\oplus c\right]$$

$$= \mathbb{P}\left[\bigoplus_{y_1\oplus e_i\neq 0} X_i = a\right] \mathbb{P}\left[\bigoplus_{y_2\oplus e_i\neq 0} X_i = b\right]$$

引理 3 ：若 $X_1 \cdots X_m$ 两两独立，且 $\mathbb{E}[X_i] = \mu$， $D[X_i] = \sigma^2$.

则 $\forall \varepsilon > 0$，

$$\mathbb{P}\left[\left|\frac{\sum_{i=1}^{m} X_i}{m} - \mu\right| \geq \varepsilon\right] \leq \frac{\sigma^2}{\varepsilon^2 m}$$

Proof: 由 Chebyshev's Inequality:

$$\mathbb{P}\left[\left|\frac{\sum_{i=1}^{m} X_i}{m} - \mu\right| \geq \varepsilon\right] \leq \frac{Var\left(\sum_{i=1}^{m} \frac{X_i}{m}\right)}{\varepsilon^2}$$

$$= \frac{\frac{1}{m^2} Var\left(\sum_{i=1}^{m} X_i\right)}{\varepsilon^2}$$

$$= \frac{\frac{1}{m^2} \sum_{i=1}^{m} Var(X_i)}{\varepsilon^2}$$

$$= \frac{\sigma^2}{\varepsilon^2 m}$$

对于 $y \in S_n$，$\forall x$，$\mathbb{P}_{x \sim \{0,1\}^n}\left[A(x, f(y)) = \langle x, y\rangle,\ A(x \oplus e_i, f(y)) = \langle x \oplus e_i, f(y)\rangle\right]$

$$\geq 1 - \left(1 - \frac{3}{4} - \frac{1}{2p(n)}\right)^2$$

$$\geq \frac{1}{2} + \frac{1}{p(n)}$$

构造 A'：

$$\boxed{\begin{array}{l} \text{采样 } m = np^2(n) \text{ 个 } X_i \\ \text{猜测 } y_i = \text{Majority}_j \{A(X_j, f(y)) \oplus A(X_j \oplus e_i, f(y))\} \end{array}}$$

$\therefore \mathbb{P}_y[A'(f(y)) = y]$

$$\geq \mathbb{P}_{y \in S_n}[A'(f(y)) = y] \cdot \mathbb{P}_y[y \in S_n]$$

$$\geq \left(1 - \frac{\frac{1}{4}}{\frac{1}{p^2(n)} \cdot np^2(n)}\right) \cdot \frac{1}{2p(n)}$$

$$= \left(1 - \frac{1}{4n}\right)\frac{1}{2p(n)} \sim \frac{1}{poly(n)}$$，f 不是 OWP. 矛盾

③ 若∃A，∃ inf n，

$$\underset{x,y}{\mathbb{P}}\left[A(x,f(y))=\langle x,y\rangle\right]\geq\frac{1}{2}+\frac{1}{p(n)}$$

构造如下 $A'(f(y))$：

令 $l=\lceil\log(2np^2(n))\rceil$

采样 $S_1\cdots S_l$，

$\forall i\in\{1,\cdots l\}$，猜测 $\langle S_i,y\rangle=A(S_i,f(y))$

$\forall T\subseteq\{1,2\cdots l\}$，$X_T=\bigoplus_{i\in T}S_i$

猜测 $\langle X_T,y\rangle=\bigoplus_{i\in T}A(S_i,f(y))$

猜测 $\langle X_T\oplus e_j,y\rangle=A(X_T\oplus e_j,f(y))$

对 $\forall i\in\{1,2\cdots n\}$，

猜测 $y_i=\underset{T}{\text{Majority}}\left\{\bigoplus_{i\in T}A(x_i,f(y))\oplus\bigoplus_{i\in T}A(x_i\oplus e_j,f(y))\right\}$

令 $S_n'=\left\{y\mid\underset{x\sim\{0,1\}^n}{\mathbb{P}}\left[A(x,f(y))=\langle x,y\rangle\right]\geq\frac{3}{4}+\frac{1}{2p(n)}\right\}$

$$\therefore\ \underset{y}{\mathbb{P}}\left[A'(f(y))=y\right]\geq\underset{y}{\mathbb{P}}\left[y\in S_n'\right]\cdot\underset{y\in S_n'}{\mathbb{P}}\left[A'(f(y))=y\right]$$

而 $\underset{y\in S_n'}{\mathbb{P}}\left[A'(f(y))=y\right]$

$$=\underset{y\in S_n'}{\mathbb{P}}\left[\underset{T}{\text{Majority}}\left\{\bigoplus_{i\in T}A(x_i,f(y))\oplus A(x_T\oplus e_j,f(y))\right\}=y_i\right]$$

$$=\underset{y\in S_n'}{\mathbb{P}}\left[\underset{\substack{T\\ j\in\{1\cdots n\}}}{\mathbb{P}}\left[\bigoplus_{i\in T}A(x_i,f(y))\oplus A(x_T\oplus e_j,f(y))=y_i\right]\geq\frac{1}{2}\right]$$

$$=\underset{y\in S_n'}{\mathbb{P}}\left[\underset{\substack{T\\ j\in\{1\cdots n\}}}{\mathbb{P}}\left[\bigoplus_{i\in T}A(x_i,f(y))=\langle x_i,y\rangle,\ A(x_T\oplus e_j,f(y))=\langle x_T\oplus e_j,f(y)\rangle\right]\geq\frac{1}{2}\right]$$

而 $\mathbb{P}[A(x_i, f(y)) = \langle x_i, y\rangle] = 1$

$= \mathbb{P}[A(s_i, f(y)) = \langle s_i, y\rangle] = 1$

$= (\frac{1}{2})^l = \frac{1}{2np^2(n)}$

$\therefore$ 式 $= \frac{1}{n} \mathbb{P}_{y\in S_n'}\left[\mathbb{P}_{\substack{T\\ j\in\{1\cdots n\}}}[A(x_T\oplus e_j, f(y)) = \langle x_T\oplus e_j, f(y)\rangle] \geq \frac{1}{2}\right]$

$= \frac{1}{n} \mathbb{P}_{y\in S_n'}\left[\mathbb{P}_{\substack{T\\ j\in\{1\cdots n\}}}[A(x_T\oplus e_j, f(y)) = \langle x_T\oplus e_j, f(y)\rangle] \geq \frac{1}{2}\right]$

$= \frac{1}{n}\left(1 - \mathbb{P}_{y\in S_n'}\left[\mathbb{P}_{\substack{T\\ j\in\{1\cdots n\}}}[A(x_T\oplus e_j, f(y)) = \langle x_T\oplus e_j, f(y)\rangle] \leq \frac{1}{2}\right]\right)$

$\geq \frac{1}{n}\left(1 - \frac{\frac{1}{4}}{(\frac{1}{p(n)})^2 2np^2(n)} \cdot \frac{1}{2}\right)$

$= \frac{1}{n}(1 - \frac{1}{16n})$

$\therefore \mathbb{P}_y[A'(f(y)) = y] \geq \frac{1}{n}(1-\frac{1}{16n})\frac{1}{2p(n)} \sim \frac{1}{poly(n)}$, f 不是 OWP. 矛盾

$\therefore$ h 为 hardcore bit