ZJU ACEE

Assignment 1

for Cryptography

zzw4257

2024

Question 1.A broken one time pad

description

Consider a variant of the one-time pad with message space $\{0,1\}^n$, where n is an odd integer and the secret key space is restricted to all n-bits strings with an even number of 1’ s. Construct an efficient adversary that breaks the perfect privacy.

Solution:

0.0.1 answer

设密钥集合为 K :$|K| = \sum_{i=0}^{n-1} \binom{n}{i} \cdot [2 \mid i] = 2^{n-1}$
对于 1 的个数为奇数的任意 m_1 和 1 的个数为偶数的任意 m_2，由于 n 为奇数
则

$$\Pr_{sk}[m_1 \oplus sk = c] = \begin{cases} \frac{1}{2^{n-1}} & 2 \nmid \text{pop}_{\text{count}}(\text{c}) \\ 0 & 2 \mid \text{pop}_{\text{count}}(\text{c}) \end{cases}$$

同时

$$\Pr_{sk}[m_2 \oplus sk = c] = \begin{cases} \frac{1}{2^{n-1}} & 2 \mid \text{pop}_{\text{count}}(\text{c}) \\ 0 & 2 \nmid \text{pop}_{\text{count}}(\text{c}) \end{cases}$$

有

故攻击者可以通过获取一次加密结果的 c，若 c 中的 1 的个数是奇数，则消息中 1 的个数是奇数; 若 c 中的 1 的个数是偶数，则消息中 1 的个数是偶数。

这使得攻击者获取了额外信息，破坏了完美安全原则。

0.0.2 idea

The original One-Time Pad encryption and decryption processes are defined as follows:

$$M = \{0,1\}^n = K$$
$$\text{Gen}(\cdot) \to sk, sk \xleftarrow{\$} K$$
$$\text{Enc}(sk, m) = sk \oplus m$$
$$\text{Dec}(sk, c) = sk \oplus c$$

Under the condition that sk is uniformly random, the probability of encrypting m_1 and m_2 to the same ciphertext c is equal, i.e.,

$$\Pr_{sk}[m_1 \oplus sk = c] = \Pr_{sk}[m_2 \oplus sk = c]$$

实际上修改 K 定义后出现的问题是

$$\Pr_{sk}[m_1 \oplus sk = c] \neq \Pr_{sk}[m_2 \oplus sk = c](\mathrm{pop_{count}}(\mathrm{m_1}) \not\equiv \mathrm{pop_{count}}(\mathrm{m_2})) \mod 2$$

Question 2. One Way Functions vs Pseudo-random Generators

0.0.3 2.1

description

Let G be a PRG that maps n bits to $2n$ bits, prove that G is a (strong) one way function.

Solution:

The definition of a PRG is that for any algorithm A, the probability that $\mathcal{A}$ can distinguish between the output of $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ (本题中 $l(n) = 2n$) on a random input and a truly random string is negligible. Formally,

$$|\Pr_{s \leftarrow \{0,1\}^n, r \leftarrow G(s)}[\mathcal{A}(r) = 1] - \Pr_{r \xleftarrow{\mathbb{R}} \{0,1\}^{l(n)}}[\mathcal{A}(r) = 1]| \leq \mathtt{negl}(n)$$

If G is not a one-way function, there exists an efficient algorithm $\mathcal{A}$ that can invert G.

具体而言这里采取强 One-way function 的定义

$$f \text{ is (strong) one way function iff}, \forall \mathcal{A}, \Pr_{x \xleftarrow[\mathbb{R}]{} \{0,1\}^*}[f(\mathcal{A}(f(x))) = f(x)] \leqslant \mathtt{negl}(n)$$

或采取教科书中的定义方法

$$\forall \mathcal{A} \in \mathrm{PPT}[\{0,1\}^{\mathrm{l(n)}} \to \{0,1\}], \Pr_{\mathrm{x} \leftarrow \{0,1\}^*}[\mathcal{A}(1^{\mathrm{n}}, \mathrm{f(x)}) \in \mathrm{f}^{-1}(\mathrm{f(x)})] \leq \mathtt{negl}(\mathrm{n})$$

其中

$$\forall k \in \mathbb{R}^*, \mathrm{poly}(n), \mathtt{negl}(n) < \frac{k}{\mathrm{poly}(n)}$$

对本题，反证，假设 $G \in \mathrm{PRG}[\{0,1\}^n \to \{0,1\}^{2n}]$ 不是 One way function ，则存在 $\mathcal{A}_0, \mathrm{poly}(n)$ 使得 $\Pr_x[f(\mathcal{A}_0(G(x)) = G(x)] \geqslant \frac{1}{\mathrm{poly}(n)}$(注意，我们下面叙述的 G 实质上是定义中的 f)

这个情况下，我们考虑设

$$\mathcal{A}' : \{0,1\}^{2n} \to \{0,1\} | \mathcal{A}'(r) = [G(\mathcal{A}_0(r)) = r]$$

则有

$$\Pr_{s\leftarrow\{0,1\}^n, r\leftarrow G(s)}[\mathcal{A}'(r)=1]=\Pr_{s\leftarrow\{0,1\}^n}[G(\mathcal{A}_0(G(s)))=G(s)]\geqslant\frac{1}{\text{poly}(n)}$$

而

$$\Pr_{r\xleftarrow{\mathbb{R}}\{0,1\}^{2n}}[\mathcal{A}'(r)=1]\leqslant\Pr_{r\xleftarrow{\mathbb{R}}\{0,1\}^{2n}}[\exists s\in\{0,1\}^n, G(s)=r]=\frac{2^n}{2^{2n}}=\frac{1}{2^n}$$

因此

$$\left|\Pr_{s\leftarrow\{0,1\}^n, r\leftarrow G(s)}[\mathcal{A}'(r)=1]-\Pr_{r\xleftarrow{\mathbb{R}}\{0,1\}^{n+1}}[\mathcal{A}'(r)=1]\right|\geqslant\left|\frac{1}{\text{poly}(n)}-\frac{1}{2^n}\right|\geqslant\frac{1}{\text{poly}'(n)}$$

由于 $\frac{1}{\text{poly}'(n)}\neq\texttt{negl}(n)$

与前设条件矛盾，故 G 是 One - Way -function

0.0.4 2.2

description

Given that F is a one-way function, construct a function G such that:

- G is a one-way function.
- G is not a pseudorandom generator (PRG).

Solution:

直接给出构造设 $F:\{0,1\}^n\to\{0,1\}^{l(n)}$

构造

$$G:\{0,1\}^n\to\{0,1\}^{l(n)+1}\ \mid\ G(r)=\text{concat}(F(r),\{\mathtt{1}\})$$

其中

concat 表示对两个 01 序列的顺序拼接换句话说 G 就是对 F 对应像的末尾添加 1

下面考虑对两个任务进行证明

对于 G 是 OWF 我们直接根据定义证明

由于 F 满足

$$\forall\mathcal{A}:\{0,1\}^{l(n)}\to\{0,1\}^n,\Pr_{x\xleftarrow[\mathbb{R}]{}\{0,1\}^n}[F(\mathcal{A}(F(x)))=F(x)]\leqslant\texttt{negl}(x)$$

若 G 不是 OWF 则存在 $\mathcal{A}_0:\{0,1\}^{l(n)+1}\to\{0,1\}^n,\text{poly}(\cdot)$ 使得 $\Pr_{x\xleftarrow[\mathbb{R}]{}\{0,1\}^n}[G(\mathcal{A}_0(G(x_0))=G(x_0)]\geqslant\frac{1}{\text{poly}(n)}$

则我们构造 $\mathcal{A}_0':\{0,1\}^{l(n)}\to\{0,1\}^n\ \mid\ \mathcal{A}_0'(r)=\mathcal{A}_0(\text{concat}(r,\{\mathtt{1}\}))$

则 $\mathcal{A}_0'(F(x_0))=\mathcal{A}_0(G(x_0))$

$\mathcal{A}_0'$ 满足

$$\Pr_{x \xleftarrow[\mathbb{R}]{} \{0,1\}^n}[F(\mathcal{A}_0'(F(x_0)) = F(x_0)] \geqslant \frac{1}{\text{poly}(n)}$$

其与 F 是 OWF 矛盾, 故 G 为 one-way function

接下来我们考虑证明 G 不是 PRG

构造

$$\mathcal{A}'' : \{0,1\}^{l(n)+1} \to \{0,1\} \ \mid \ \mathcal{A}''(r) = \begin{cases} 1 & r_{l(n)+1} = 1 \\ 0 & r_{l(n)+1} = 0 \end{cases}$$

则

$$|\Pr_{s \leftarrow \{0,1\}^n, r \leftarrow G(s)}[\mathcal{A}''(r) = 1] - \Pr_{r \xleftarrow{\mathbb{R}} \{0,1\}^{l(n)+1}}[\mathcal{A}''(r) = 1]| = 1 - \frac{1}{2} = \frac{1}{2}$$

显然与 PRG 定义需要可忽略矛盾

综上，我们构造出来的 G 是 One-Way-Function 但不是 PRG