六、理论构造PRP

哈尔滨工业大学

张宇

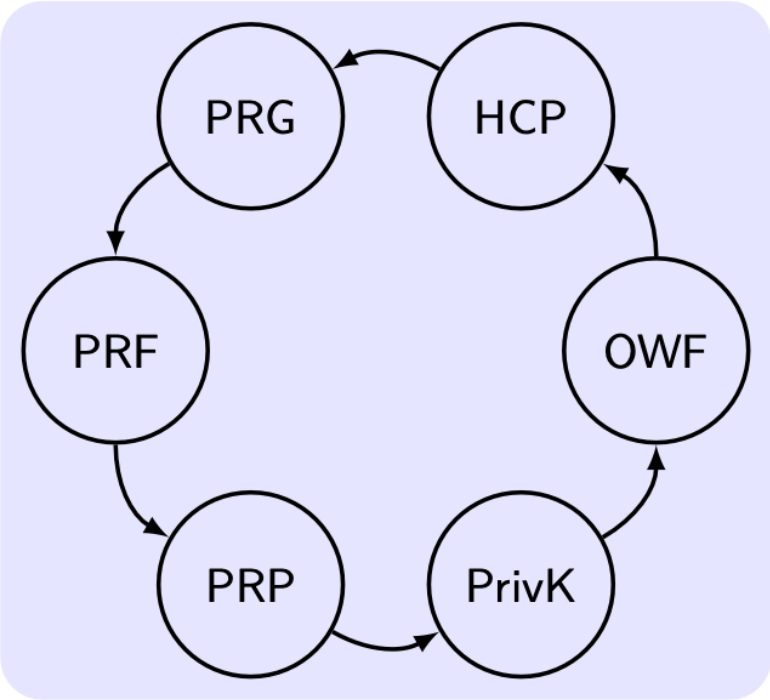
2024春

概览

1. 单向函数（One-Way Function）
2. 从单向函数构造PRP

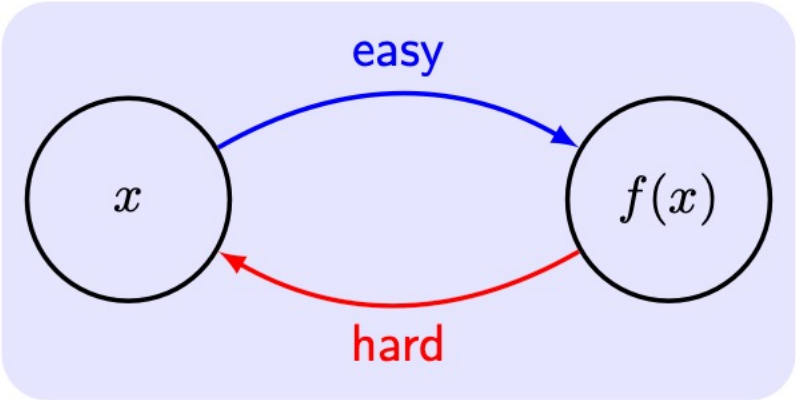
概览

- 现代密码学的贡献之一是，单向函数的存在等价于所有（有意义的）私钥加密的存在
- 密码学对象的构造过程：从OWF构造核心断言（HCP），构造RPG，构造PRF，构造PRP，构造安全私钥加密，而安全私钥加密就是一个OWF，从而形成一个闭环



单向函数（One-Way Functions）

- 单向函数是一个易于计算（多项式时间），而逆向难以计算（无多项式时间算法）



The inverting experiment $\mathsf{Invert}_{\mathcal{A},f}(n)$:

1. Choose input $x \leftarrow \{0,1\}^n$. Compute $y := f(x)$.
2. $\mathcal{A}$ is given 1^n and y as input, and outputs x'.
3. $\mathsf{Invert}_{\mathcal{A},f}(n) = 1$ if $f(x') = y$, otherwise 0.

OWF定义

Definitions of OWF/OWP [Yao]

For polynomial-time algorithm M_f and $\mathcal{A}$.

Definition 1

A function $f : \{0,1\}^* \to \{0,1\}^*$ is **one-way** if:

1. (Easy to compute): $\exists\ M_f$: $\forall x, M_f(x) = f(x)$.
2. (Hard to invert): $\forall\ \mathcal{A}$, $\exists$ negl such that

$$\Pr[\mathsf{Invert}_{\mathcal{A},f}(n) = 1] \leq \mathsf{negl}(n).$$

or

$$\Pr_{x \leftarrow \{0,1\}^n}[\mathcal{A}(f(x)) \in f^{-1}(f(x))] \leq \mathsf{negl}(n).$$

Definition 2

Let $f : \{0,1\}^* \to \{0,1\}^*$ be length-preserving, and f_n be the restriction of f to the domain $\{0,1\}^n$. A OWP f is a **one-way permutation** if $\forall n$, f_n is a bijection.

候选单向函数

- 乘法与分解（**Multiplication and factoring**）：$f_{\text{mult}}(x, y) = (xy, \|x\|, \|y\|)$, x 和 y 是相同长度的质数；*注：后面会学习RSA问题*
- 模平方和平方根（**Modular squaring and square roots**）：$f_{\text{square}}(x) = x^2 \bmod N$；*注：也被应用于公钥密码学*
- 离散指数与对数（**Discrete exponential and logarithm**）：$f_{g,p}(x) = g^x \bmod p$；*注：后面将学习DH密钥交换协议*
- 子集和问题（**Subset sum problem**）：$f(x_1, \ldots, x_n, J) = (x_1, \ldots, x_n, \sum_{j \in J} x_j)$；*注：子集和问题判定是否存在一个子集中元素之和为给定的值*
- 密码学安全哈希函数（**Cryptographically secure hash functions**）：稍后会学习；

课堂练习

$f: \{0,1\}^{128} \to \{0,1\}^{128}$ is a OWF. Is f' OWF?

- $f'(x) = f(x) \| x$
- $f'(x \| x') = f(x) \| x'$
- $f'(x) = f(x) \oplus f(x)$
- $f'(x) = \begin{cases} f(x) & \text{if } x[0,1,2,3] \neq 1010 \\ x & \text{otherwise} \end{cases}$
- $f'(x) = \begin{cases} f(x) & \text{if } x \neq 1010 \| 0^{124} \\ x & \text{otherwise} \end{cases}$
- more examples in homework

必要的假设

- 接下来学习OWP的存在是安全加密方案的充分条件，同时还可以证明OWP的存在也是安全加密方案的必要条件。
- 定理：假设存在OWP，那么存在PRG，PRF，PRP和CCA安全私钥加密方案。
  - 如何构造CCA安全的加密方案将在后面学习。
- 命题：如果存在窃听者不可区分私钥加密方案，那么存在一个OWF。

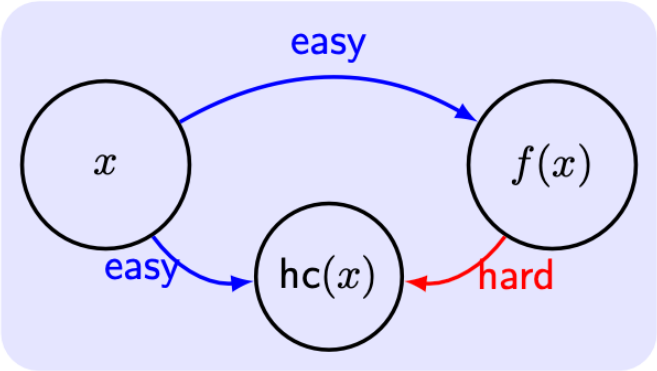
证明：$f(k,m,r) \stackrel{\text{def}}{=} (\mathsf{Enc}_k(m,r),m)$，其中 $|k|=n,|m|=2n,|r|=\ell(n)$。

- 从破解加密方案问题$\mathcal{A}'$规约到单向函数求逆问题$\mathcal{A}$。规约的关键之一在于将挑战密文和一个明文 $c||m_0$ 作为$\mathcal{A}$求逆的输入。当求拟成功时，$\mathcal{A}'$输出0；否则，输出1。当m_0被加密，则破解加密方案意味着可求逆；当m_1被加密，则破解加密方案意味着没有成功求逆，概率为$1-1/2^n$。

- 接下来证明从OWP可以构造出PRP。

核心断言（Hard-core predicate）

- 核心断言可以理解为根据函数的输出最难推断的关于输入的一个比特信息，任意敌手算法与随机猜测相比几乎没有差异。



Definition 3

A function $\mathsf{hc} : \{0,1\}^* \to \{0,1\}$ is a **hard-core predicate of a function** f if (1) hc can be computed in polynomial time, and (2) $\forall$ PPT $\mathcal{A}$, $\exists$ negl such that

$$\Pr_{x \leftarrow \{0,1\}^n}[\mathcal{A}(f(x)) = \mathsf{hc}(x)] \leq \frac{1}{2} + \mathsf{negl}(n).$$

任意单向函数存在核心断言

9. 对于任意OWF的HCP [Goldreich and Levin]

- 定理：f是一个OWF。那么，存在一个OWF g 并与 g 伴随着一个HCP gl。
- 问题：$\mathrm{gl}(x) = \bigoplus_{i=1}^{n} x_i$ 是任意OWF的HCP吗? 答案是否定的，例如一个单向函数输出的最后一个比特就是输入按位异或的结果；
- 证明：$g(x,r) \overset{\text{def}}{=} (f(x),r)$, for $|x| = |r|$, 并定义 $\mathrm{gl}(x,r) \overset{\text{def}}{=} \bigoplus_{i=1}^{n} x_i \cdot r_i$。其中，$r$ 是一个随机串。
- *说明：gl就是从x中随机选择若干比特异或结果作为核心断言。即便敌手根据输出推断出x中若干比特的信息，但仍不能推断出（由r来）随机挑选的任意若干比特信息（核心断言），否则意味着敌手可以求出整个x。*

- gl就是从x中随机选择若干比特异或结果作为核心断言。即便敌手根据输出推断出x中若干比特的信息，但仍不能推断出（由r来）随机挑选的任意若干比特信息（核心断言），否则意味着敌手可以求出整个x。

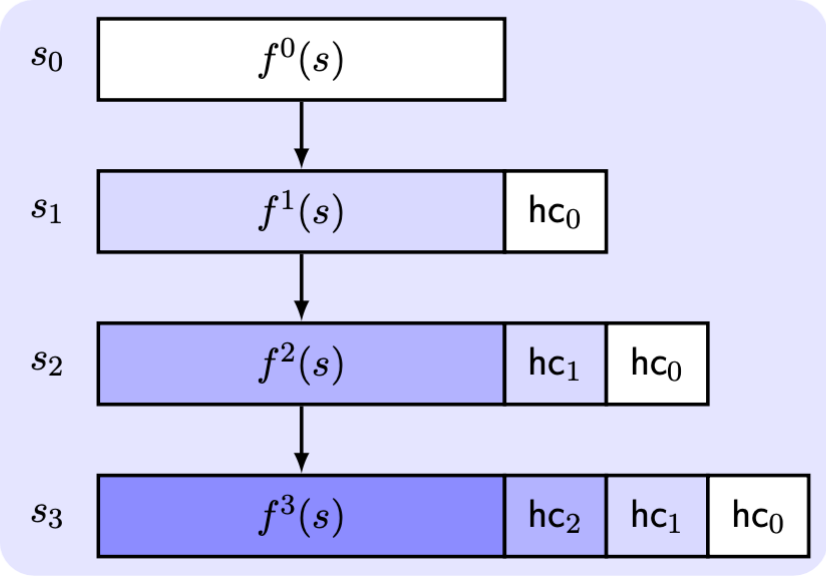
从OWP到PRG

- 因为f为排列（这很重要，不能是非排列的函数），那么当s随机生成时，f(s)也是均匀随机的，G(s)的头部也就是随机的；
- 根据f(s)难以推断核心断言hc(s)，这正是伪随机生成器的伪随机性的判断依据：下一比特不可预测性。

PRG from OWP: Blum-Micali Generator

Theorem 5

f is an OWP and hc *is an HCP of f. Then $G(s) \stackrel{def}{=} (f(s), \mathsf{hc}(s))$ constitutes a PRG with expansion factor $\ell(n) = n + 1$, then $\forall$ polynomial $p(n) > n$, $\exists$ a PRG with expansion factor $\ell(n) = p(n)$.*



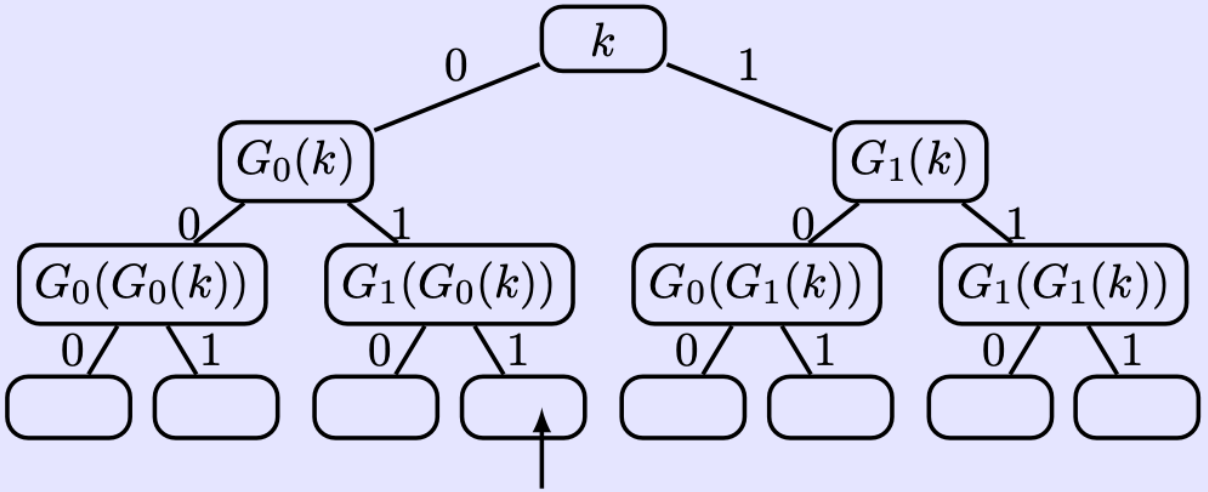
从PRG到PRF

- PRF随机性来自于PRG的随机性

Theorem 6

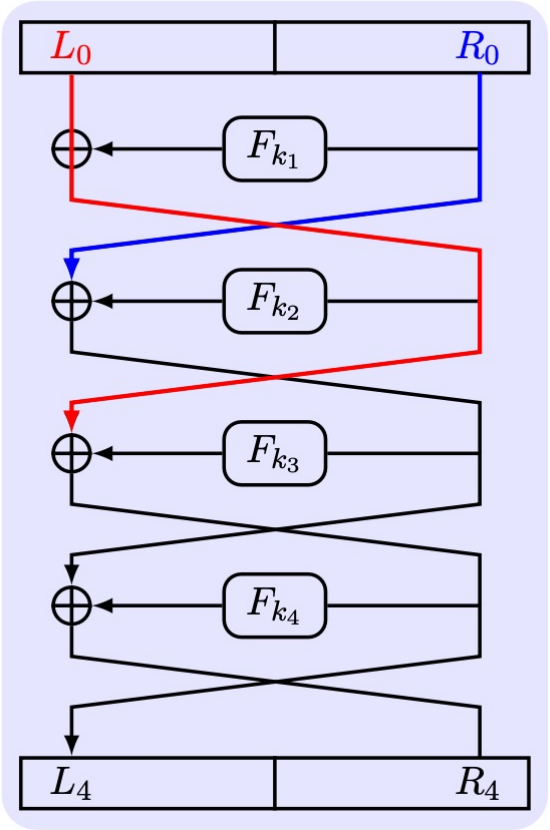
If ∃ a PRG with expansion factor $\ell(n) = 2n$, then ∃ a PRF.

$$G(k) = G_0(k) \| G_1(k)$$



$$F_k(x_1 x_2 \cdots x_n) = G_{x_n}(\cdots(G_{x_2}(G_{x_1}(k)))\cdots), G(s) = (G_0(s), G_1(s)).$$

从PRF到PRP



$F^{(r)}$ is an r-round Feistel network with the mangler function F.

Theorem 7

If F is a length-preserving PRF, then $F^{(3)}$ is a PRP, and $F^{(4)}$ is a strong PRP, that maps $2n$-bit strings to $2n$-bit strings (and uses a key of length $3n$ and $4n$).

Show that 1- or 2-round Feistel network is not a PRF.

- 首先，Feistel网络本身特性是排列，因此证明上述定理成立的关键在于，证明伪随机性；伪随机性来自与每轮的mangler函数是PRF，其输出是一个独立的随机值。
- 对于为什么至少需要3轮？首先可以观察到如果只有1轮，则不是伪随机的，因为R_0被直接输出为L_1；如果只有2轮，也不是随机的，因为只改变L_0来翻转1个比特，那么R_2也只翻转1个比特。当3轮时，上述两个情况不会发生，并且输出结果L_3, R_3都是经过了PRF结果得到的。

本节小结

- OWF意味着安全私钥加密方案，安全私钥加密方案意味着OWF。