PRP & PRF (Pseudo Random Function & permutation)

Tips

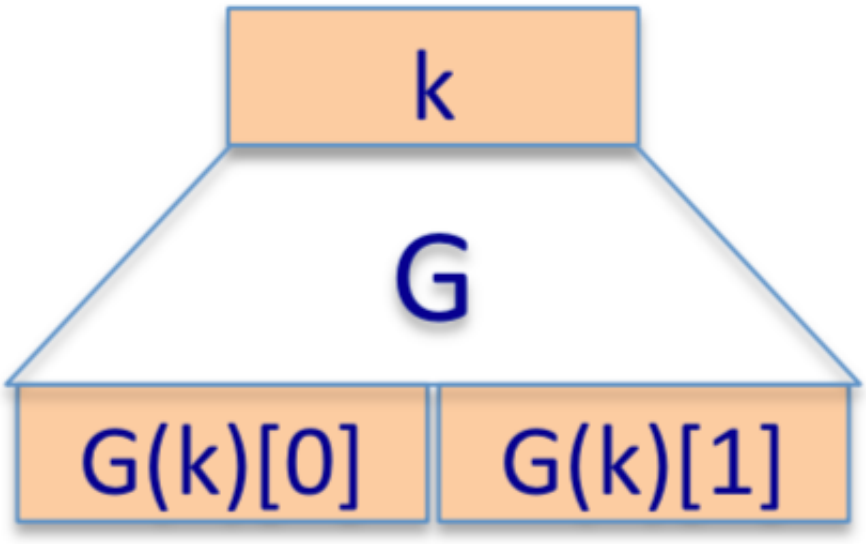
- PRP 在某种程度上就是一个 block cipher

特性:

PRP :

- K x X -> X
- e.g.
  - AES => K = X = $\{0,1\}^{128}$
  - X = $\{0,1\}^{64}$, K = $\{0,1\}^{168}$

PRF:

- K x X -> Y , 当Y = X , 且提供了有效的可逆函数的时候, PRF 就是一个PFP
- Application : **build secure PRG from secure PRF**
  - G(k) = F(k, 0) || F(k, 1) || ... || F(k, t-1)
- Application :**build sercure PRF from secure PRG**
  - 

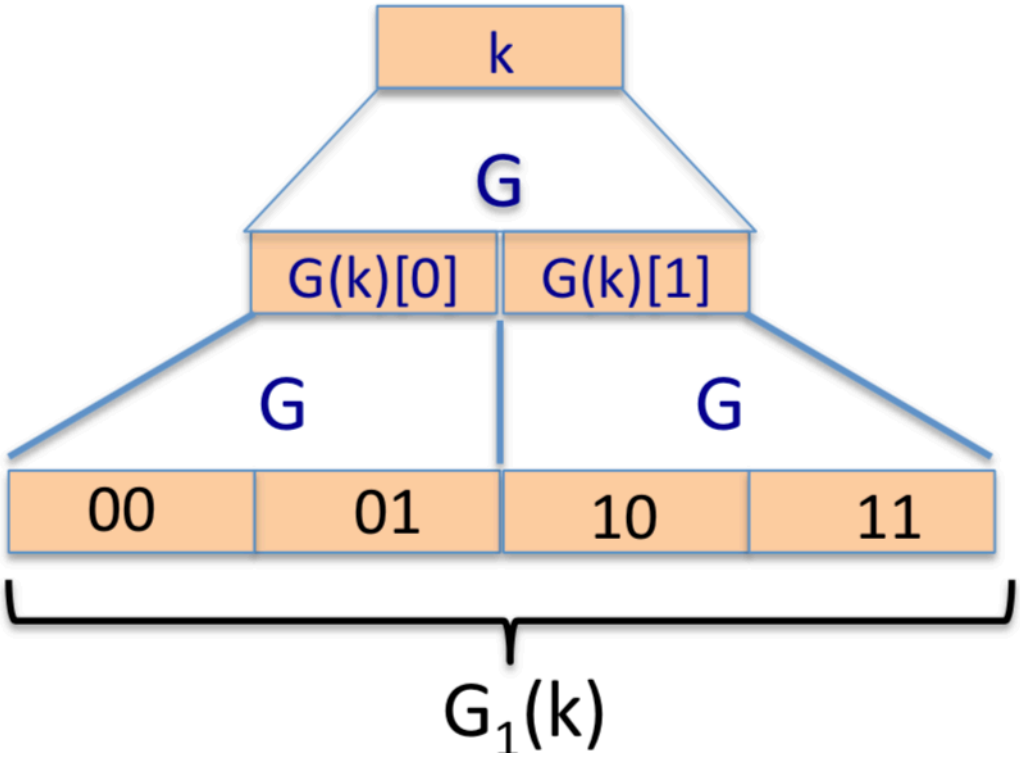
    先从1个bit的PRF定义开始 : 假设定义一个G 为 G(k) -> k^2

    那么可以定义一个 PRF F(k, x 属于 {0, 1}) = G[k][x]

    - 同样的, 可以扩充到多个bit :

Let $G: K \longrightarrow K^2$.

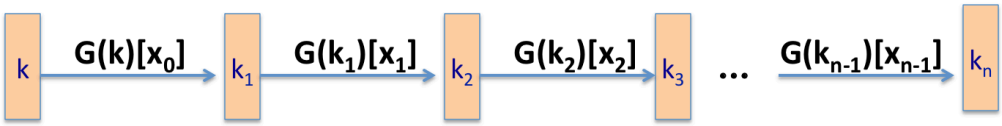
define $G_1: K \longrightarrow K^4$ as $G_1(k) = G(G(k)[0]) \,||\, G(G(k)[1])$



- 最后实现无限的扩充:

Let $G: K \longrightarrow K^2$. define PRF $F: K \times \{0,1\}^n \longrightarrow K$ as

For input $x = x_0\, x_1 \ldots x_{n-1} \in \{0,1\}^n$ do:



异同点:

1. Same

- 都是伪随机的
- 都是给定一个 function F(k, x) 两个输入, 输出一个关于k, x 的映射
- Any secure PRP is also a secure PRF, if $|X|$ is sufficiently large.

Then for any q-query adversary A:

$$\left| Adv_{PRF}[A,E] - Adv_{PRP}[A,E] \right| < q^2 / 2|X|$$

neg

neg.

2. Differ

- PRF 可以是对多对一的映射, PRP 必须是一对一的映射 (one-to-one) , 即PRP 是 PRF 的一种
- PRP 必须提供有效的加密和解密函数 E , D . 因为一对一, 所以解密函数一定是需要可以复原的. PRF 就不一定可以复原, 因为可能存在多对一的情况

3. Security

- 对于PRF来说, 一个安全的PRF , 就是给定一个PRF形成的Y 和, 这个位数的**完全随机**形成的 Y 是无法区分的
- 对于PRP来说, 一个安全的PRP, 就是给定一个PRP映射的Y 和, 这个位数的**所有的one - to - one** 是无法区分的