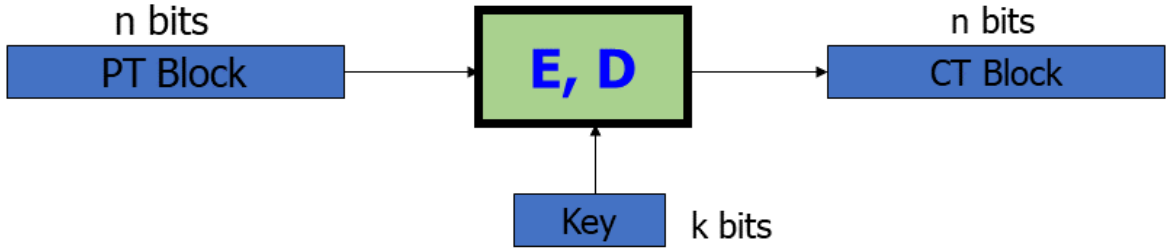
块密码的使用

- 伪随机置换(PRPs)与伪随机函数(PRFs)
- 一次性密钥在分组密码中的使用

块密码

块密码工作流程：



实例：

1. 3DES: n= 64 bits, k = 168 bits
2. AES: n=128 bits, k = 128, 192, 256 bits

块密码

- 伪随机函数(PRF)

$$F: K \times X \rightarrow Y$$

- ◆ 取一个密钥和某个集合X的元素作为输入，输出某个集合Y里的元素
- ◆ 存在评估F(k , x)的高校方法

- 伪随机置换(PRP)

$$E: K \times X \rightarrow X$$

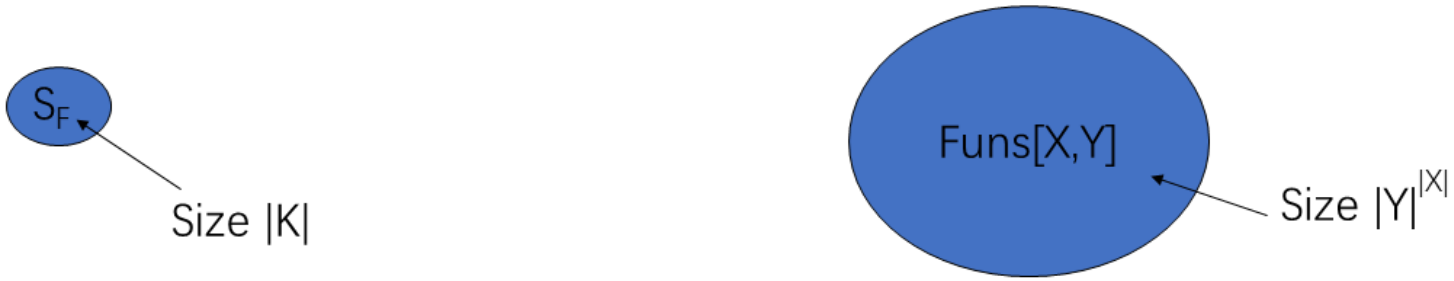
- ◆ 存在用于评估E(k , x)的有效确定性算法
- ◆ 函数对所有密钥一一映射
- ◆ 存在一个算法D可以计算函数E的逆

Secure PRFs

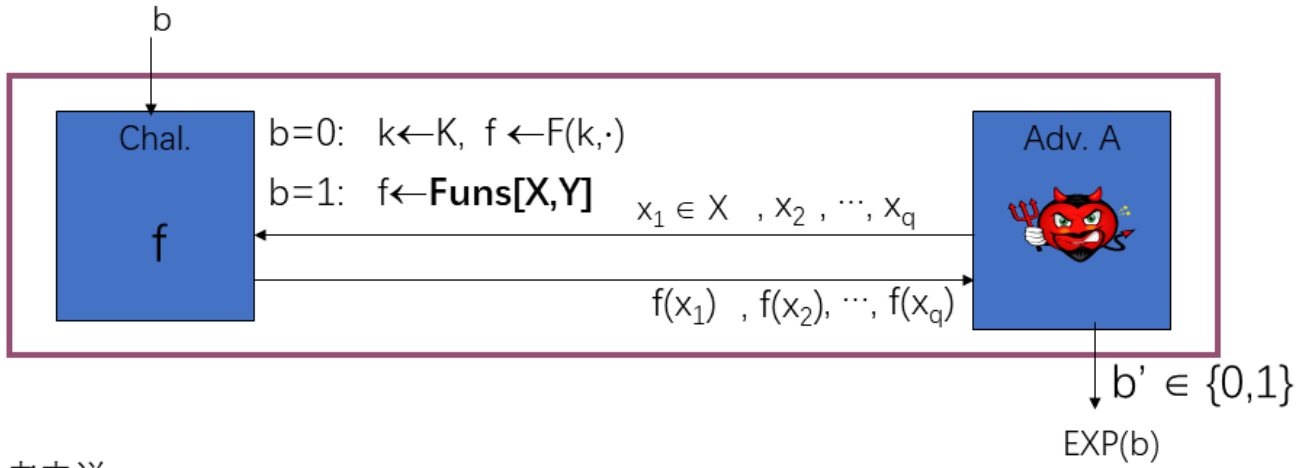
◆ Let $F: K \times X \rightarrow Y$ be a PRF

- Funs[X,Y]: 从X到Y的全部映射
- $S_F = \{ F(k,\cdot) \text{ s.t. } k \in K \} \subseteq$ Funs[X,Y]

安全的PRF：一个Funs中的随机函数无法和一个S_F中的函数区分开来



安全PRF



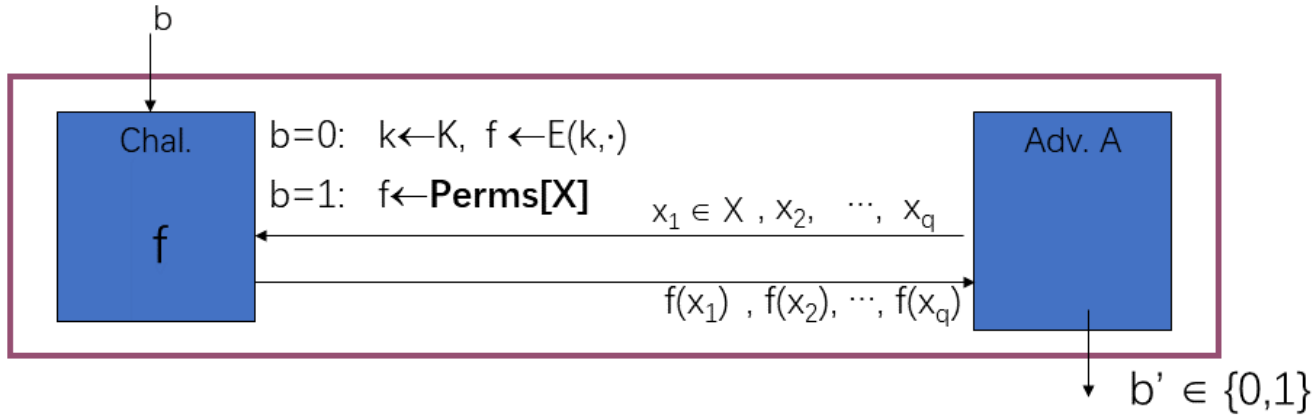
如果对于攻击者来说，

$$Adv_{PRP}[A,F] = |Pr[EXP(0)=1] - Pr[EXP(1)=1]|$$

的结果是可忽略的，那么这个F就是一个安全的PRF

攻击者无法区分一个伪随机函数和一个真随机函数

安全PRP



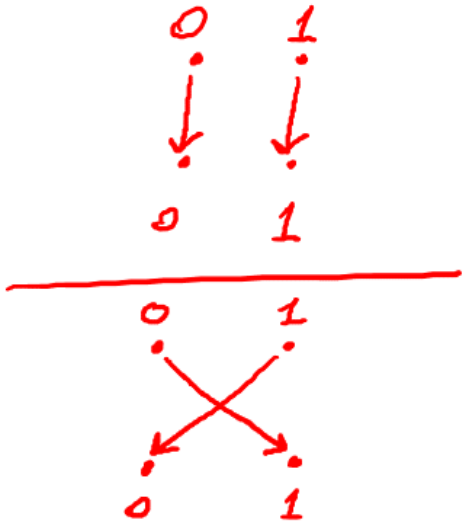
如果对于攻击者来说，

$$Adv_{PRP}[A,E] = |Pr[EXP(0)=1] - Pr[EXP(1)=1]|$$

的结果是可忽略的，那么这个E就是一个安全的PRP

块密码

X = {0,1}上只有两个可逆函数，一个是恒等函数，另一个是交叉映射函数。



密钥空间：K={0,1}，　输入空间：X = {0,1}

PRP：　　$E(k, x) = x \oplus k$

这是一个安全的PRP

块密码

安全PRP实例：3DES，AES …

AES-128：$K \times X \rightarrow X$　　$K = X = \{0,1\}^{128}$

一个关于AES的假设：

所有算法可以在2^80时间内运行完成. 那么攻击者对AES有最大优势：

$Adv_{PRP}[A, \mathbf{AES}] < 2^{-40}$

块密码

PRF 交换引理：当|X|足够大时，一个安全的PRP也是一个安全的PRF

引理：如果E是一个安全的PRP，那么对于任何q个查询：

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

当|X|足够大时，$q^2 / 2|X|$的值可以忽略不计。

因为$Adv_{PRP}\ [A,E]$可忽略不计，因此$Adv_{PRF}[A,E]$也可忽略不计

块密码

建议：

- 不要考虑AES和3DES的内部工作原理
- 假定它们都是安全的PRP，学习怎样去使用它们

块密码

➢ PRP与PRF的使用

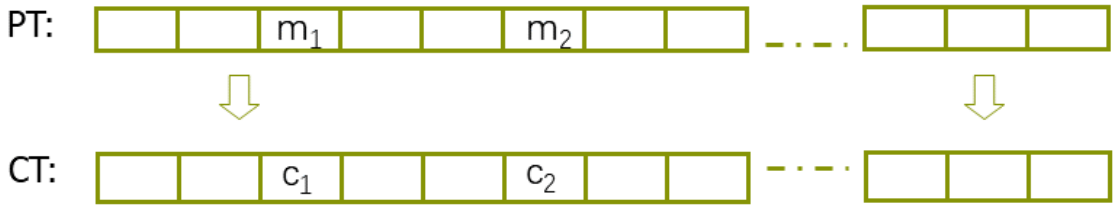
◆ 目标：从一个安全的PRP构造一个安全的加密

对于一次性密钥(**one-time keys**):

- 攻击者的能力：只能看到一个密文
- 攻击者的目标：破坏密文的语义安全

块密码

PRP的不正确使用：电子密码本



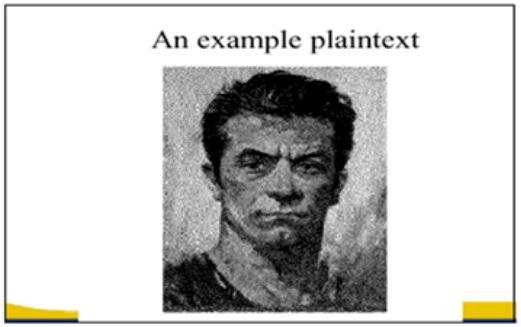
◆ 加密过程：

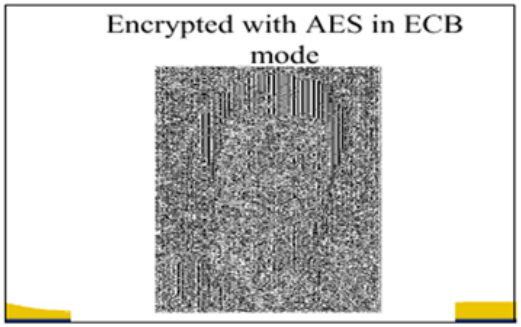
将需要加密的消息按照块密码的块大小被分为数个块，并对每个块进行独立加密

◆ 存在的问题：

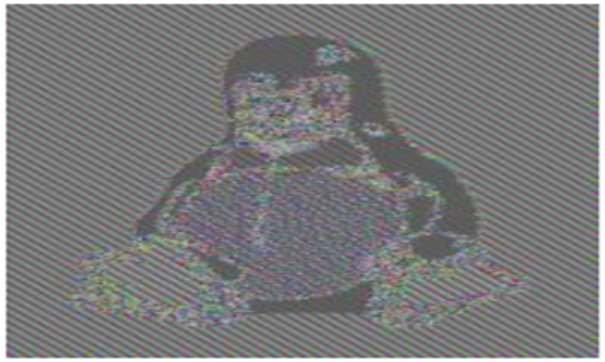
如果明文相同，那么得到的密文相同

块密码





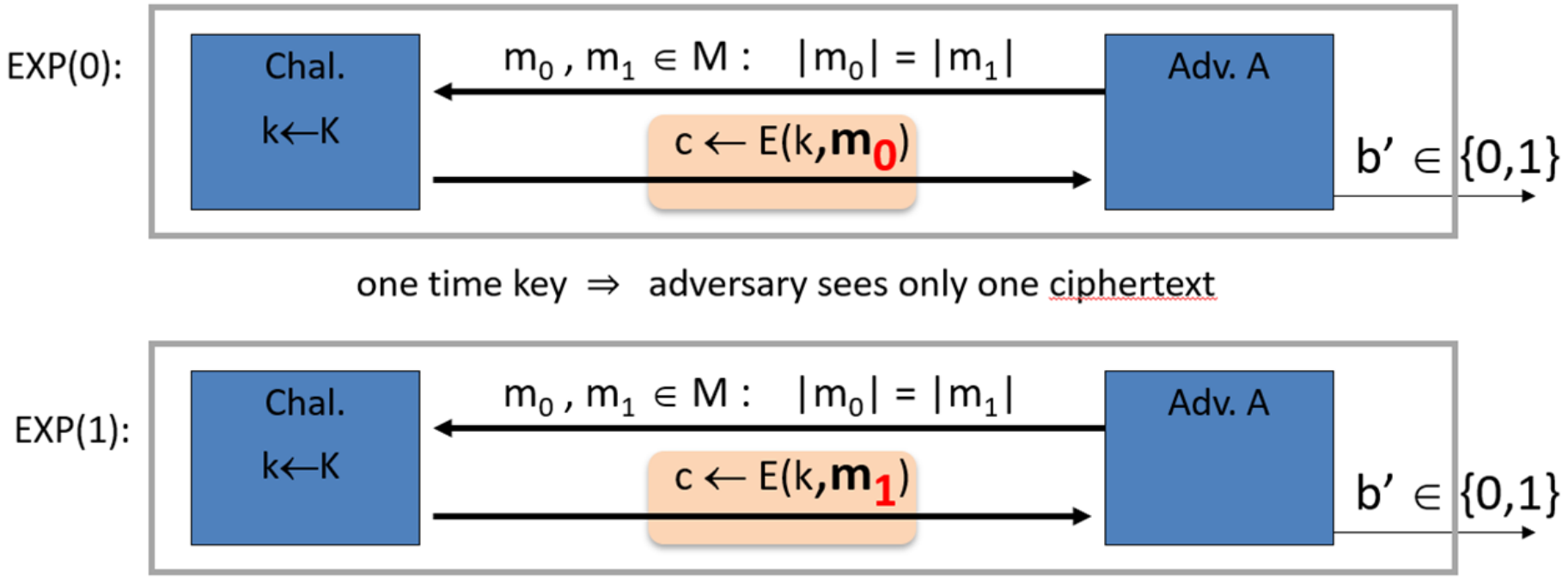
原图



使用ECB模式加密

块密码

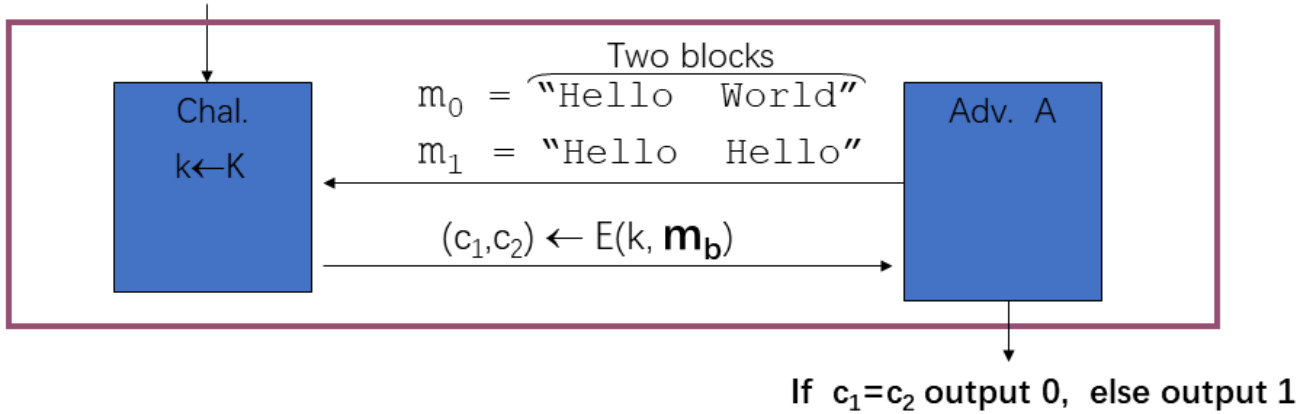
一次性密钥的语义安全



$Adv_{SS}[A,OTP] = | Pr[\ \mathbf{EXP(0)}=1\ ] - Pr[\ \mathbf{EXP(1)}=1\ ] |$应该是可以忽略的

电子密码本不是语义安全的

- 当信息超过一个分组时，ECB就不是语义安全的



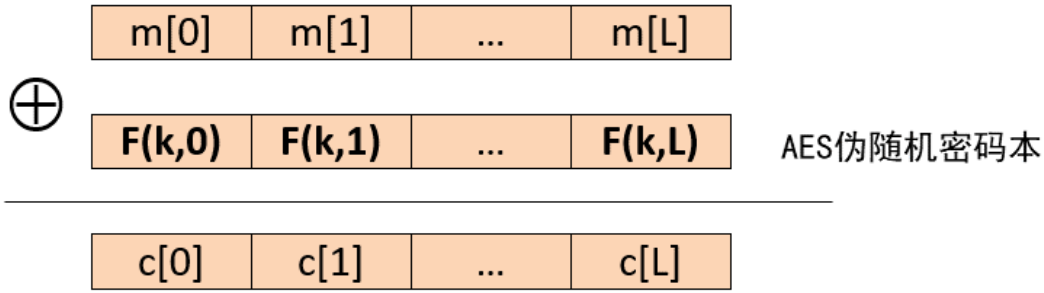
Then $Adv_{SS}[A, ECB] = 1$

块密码

一种安全的构建:

- 确定的计数器模式

- $E_{DETCTR}(k, m) =$



由分组密码构建一个流密码

块密码

理论: 对于任意的L满足 $L>0$,

如果F是一个安全的 PRF over (K, X, X)

E_{DETCTR} 是一个安全的加密 (K, X^L, X^L).

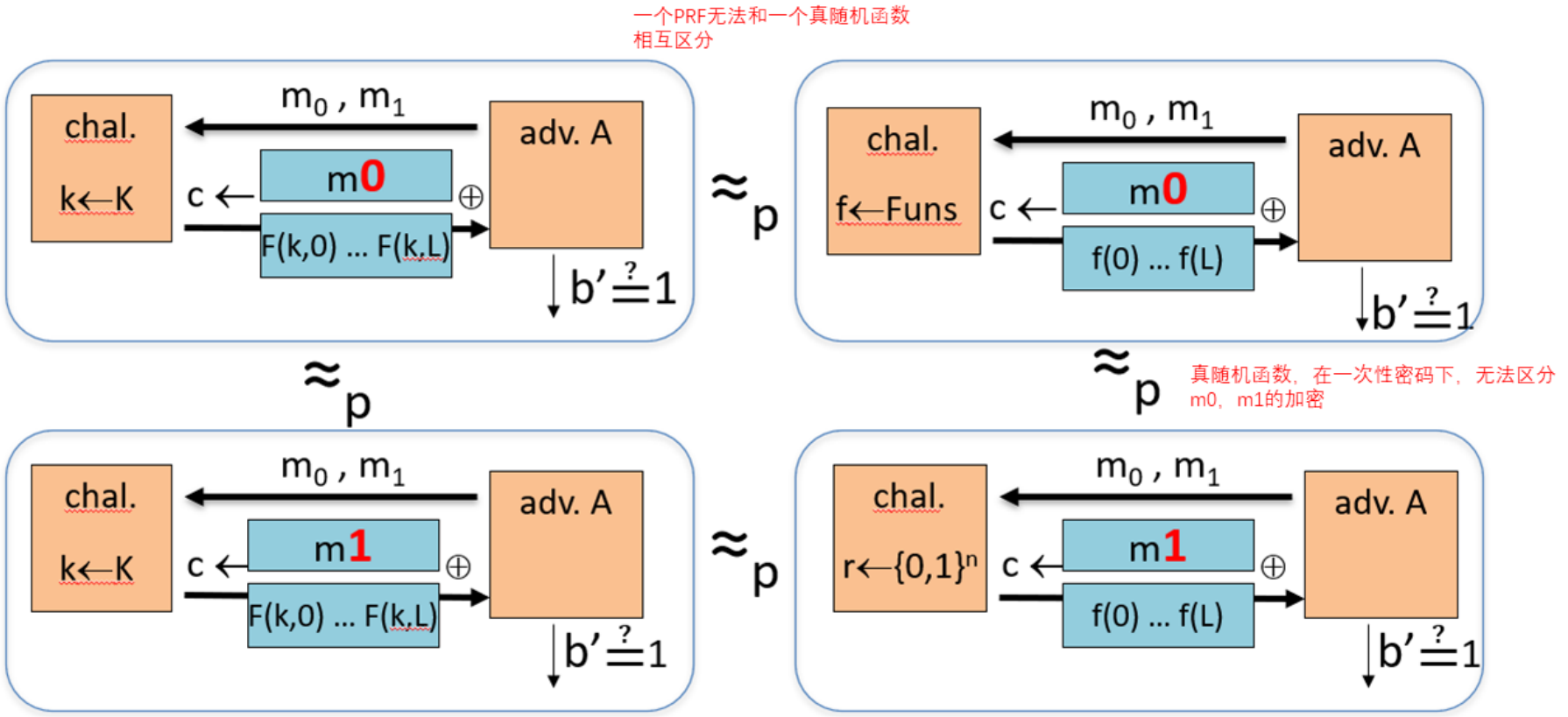
对于任何攻击E_{DETCTR}的攻击者A

这里存在另一个攻击PRF的攻击者B:

$$Adv_{SS}[A, E_{DETCTR}] = 2 \cdot Adv_{PRF}[B, F]$$

因为F是一个安全的PRF，所以$Adv_{PRF}[B, F]$是可忽略的，所以$Adv_{SS}[A, E_{DETCTR}]$也是可忽略的.

块密码



谢谢观看！