五、实践构造PRP（分组密码）

哈尔滨工业大学

张宇

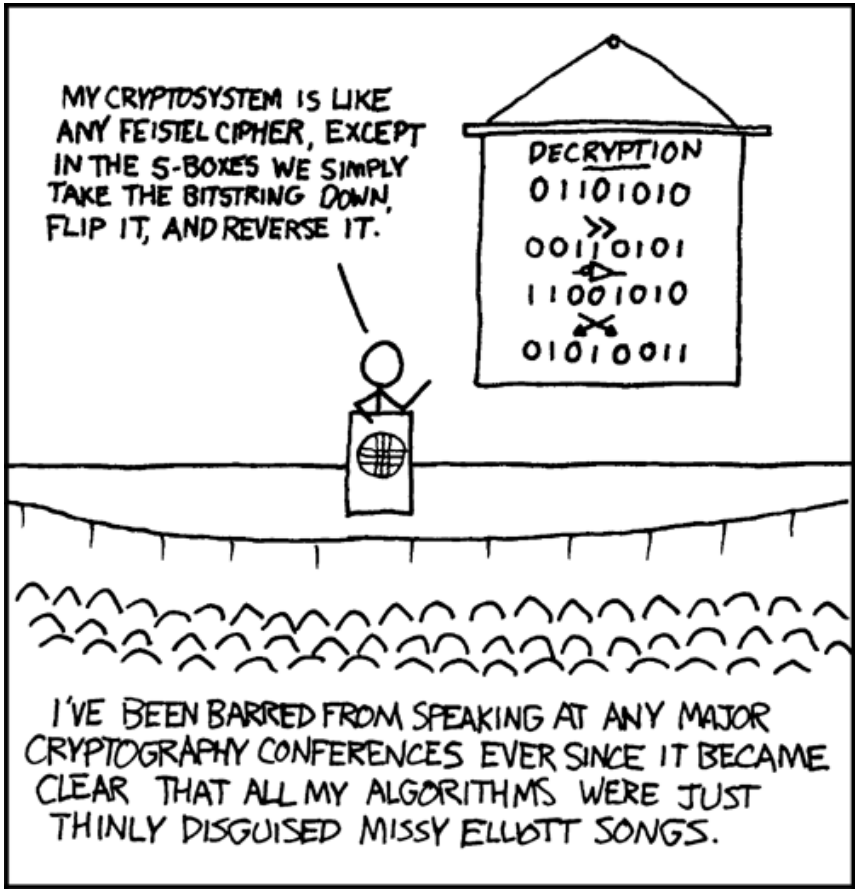
2024春

概览

1. 替换-置换网络（Substitution-Permutation Networks）
2. Feistel网络
3. DES——数据加密标准
4. 增加分组密码密钥长度
5. AES——高级加密标准

分组密码漫画

- My cryptosystem is like any Feistel cipher, except in the S-Boxes we simply take the bitstring down, flip it, and reverse it.



分组密码/块密码（Block cipher）

- 块密码 $F:\{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^\ell$. 是一个带密钥的函数。

  $F_k:\{0,1\}^\ell \to \{0,1\}^\ell, F_k(x) \stackrel{\text{def}}{=} F(k,x).$

  n 是密钥长度, ℓ 是块长度.
- 构造是启发式的，而非被证明了的；
- 注意：虽然有“密码”二字，但在实践中，块密码被当作是一个PRP，而非加密方案；在之前AES的提案召集中要求，算法输出的范围应该与输入块的随机排列是不可区分的；
- 方案被认为是“优秀的”，如果已知的最佳攻击具有的时间复杂性与蛮力搜索密钥大致相当
  - 一个$n = 112$的加密方案，可以在2^{56}时间内被破解是不安全的；
  - 在渐进设定中，尽管$2^{\frac{n}{2}}$是指数，但与上面的例子一样，实际可能不安全；

替换置换网络（Substitution-Permutation Network）

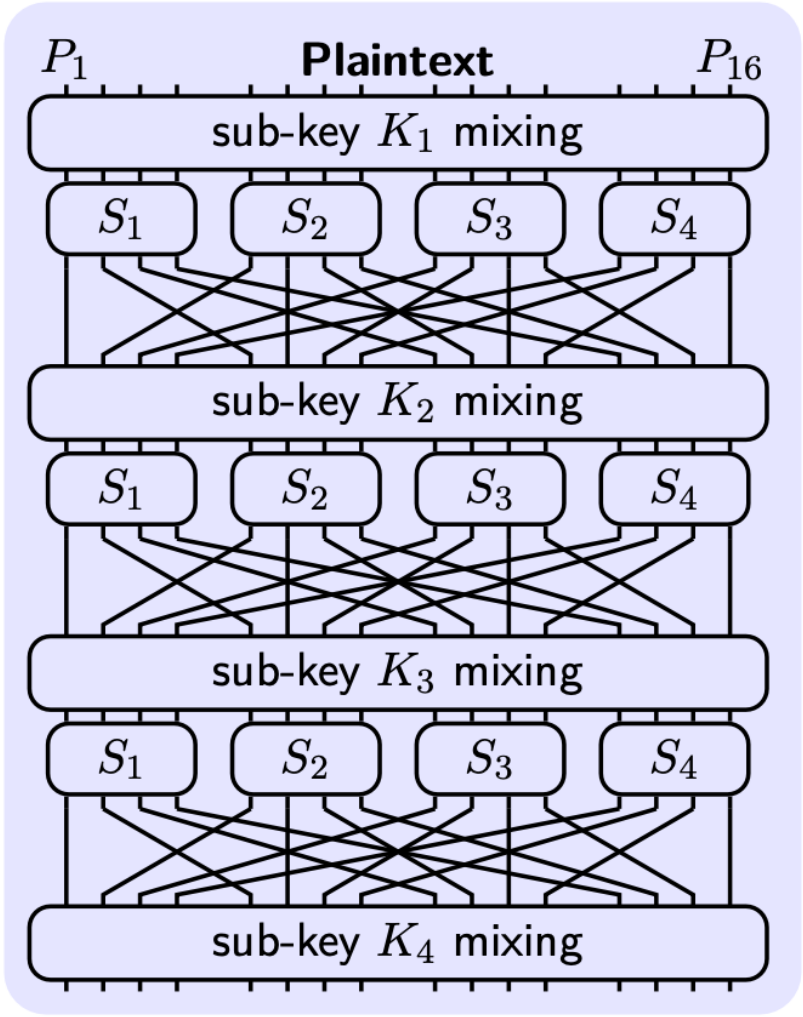
- 目标：构造“简洁的”但看起来随机的排列
- 思路：混乱（密钥与密文关系复杂）-扩散（明文统计冗余在密文中消散）

子密钥混合

（将密钥与中间结果异或）

P盒（置换）

变换位置



S盒（box）

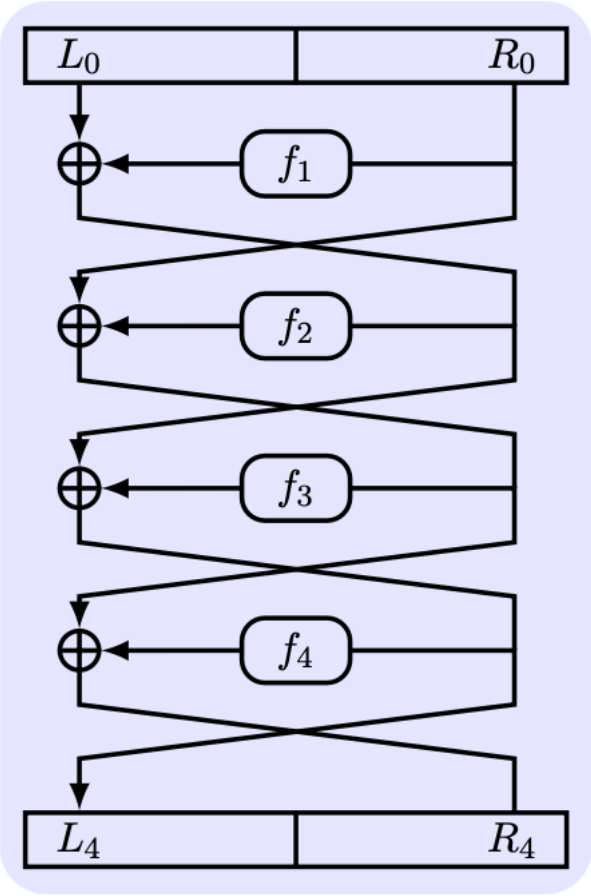
替换内容

结尾处需要子密钥混合，否则最后一轮S/P无效

SPN设计原则

- S盒可逆性（Invertibility）：S盒必须是可逆的，否则块密码不是排列；这可以从SPN构造中观察到，其中密钥混合（异或）和P盒（置换）都是排列操作，为了令SPN是排列，那剩下的S盒必须是可逆的；
- 雪崩效应（Avalanche Effect）：改变输入的一个比特影响输出的每个比特；
  - 严格雪崩条件：一个输入比特取补，每个输出比特都有50%的概率改变；
  - 比特独立条件：对于任意i, j, k，当改变一个输入比特i时，输出比特 j 和 k 应该独立改变；
  - S盒：改变1比特输入会改变至少2比特输出；
  - P盒：每个S盒的输出都被扩散到下一轮的不同S盒；
  - 例如，对于4比特的S盒，改变输入的1个比特，在经过R轮的SPN后，影响输出的2^R个比特；

Feistel Networks



- 为了构造排列，要求SPN网络中S盒是可逆的，这对S盒的设计提出了要求；那么，能不能放松对S盒设计需求，同时保留排列的？
- Feistel网络可以满足上面的需求：从若干非可逆组件构造一个可逆函数；

- $L_i := R_{i-1}$ and $R_i := L_{i-1} \oplus f_i(R_{i-1})$
- **Inverting**: $L_{i-1} := ?$
- **Decryption**: Operate with sub-keys in reverse order.

Proposition 2

Luby-Rackoff Theorem: *Regardless of the mangler functions* $\{\hat{f}_i\}$ *and the number of rounds,* F_k *is a permutation for any choice of* k.

课堂练习

What is the output of an r-round Feistel network when the input is (L_0, R_0) in each of the following two cases:

(a) Each round function F outputs all 0s, regardless of the input.
(b) Each round function F is the identity function.

DES（数据加密标准）编年史

DES经历了一个从成为加密标准到安全性不足、到安全性增强、到被彻底破解的历程；

- [1973] NBS (NIST) 发布标准召集公告；
- [1974] DES 在联邦政府公告发布；
- [1977] DES 被发布为 FIPS PUB 46；
- [1990] 2^{47} 个明文的CPA下差分分析；
- [1997] DESCHALL 项目公开破解DES；
- [1998] EFF（电子前沿基金会）的Deep Crack在56小时内花费\$250,000破解DES；
- [1999] 三重 DES
- [2001] AES 在 FIPS PUB 197 发布；
- [2004] DES标准 FIPS PUB 46-3 被撤销；
- [2006] COPACOBANA 在9天内花费1万美元破解DES；
- [2008] RIVYERA 在1天内破解 DES；
- [2016] Hashcat用8块GTX 1080Ti在2天内破解DES；
- [2017] 利用CPA攻击，针对一个特定明文在25秒内获得密钥；

DES设计

- 16轮的Feistel网络；64位块；56位密钥，48位子密钥 (64位密钥带有8个校验位)
- 密钥编排：$56 \text{ bits} \xrightarrow[\text{left rotation, PC}]{\text{divided into two halves}} 48 \text{ bits.}$
- 以初始排列开始 (IP) 以 IP^{-1} 结束；
- 轮函数 f 是一个 32位 I/O 的不可逆函数；
- f_i 由mangler函数 \hat{f}_i 和子密钥 k_i 来确定；
- S盒是 4 到1 函数，将6位映射为4位；

DES概览

Algorithm 1: DES

input : key k, message m

output: ciphertext c

1 $(k_1, \ldots, k_{16}) \leftarrow KeySchedule(k)$

2 $m \leftarrow IP(m)$

3 Parse m as $L_0 \| R_0$

4 **for** $r = 1$ **to** *16* **do**

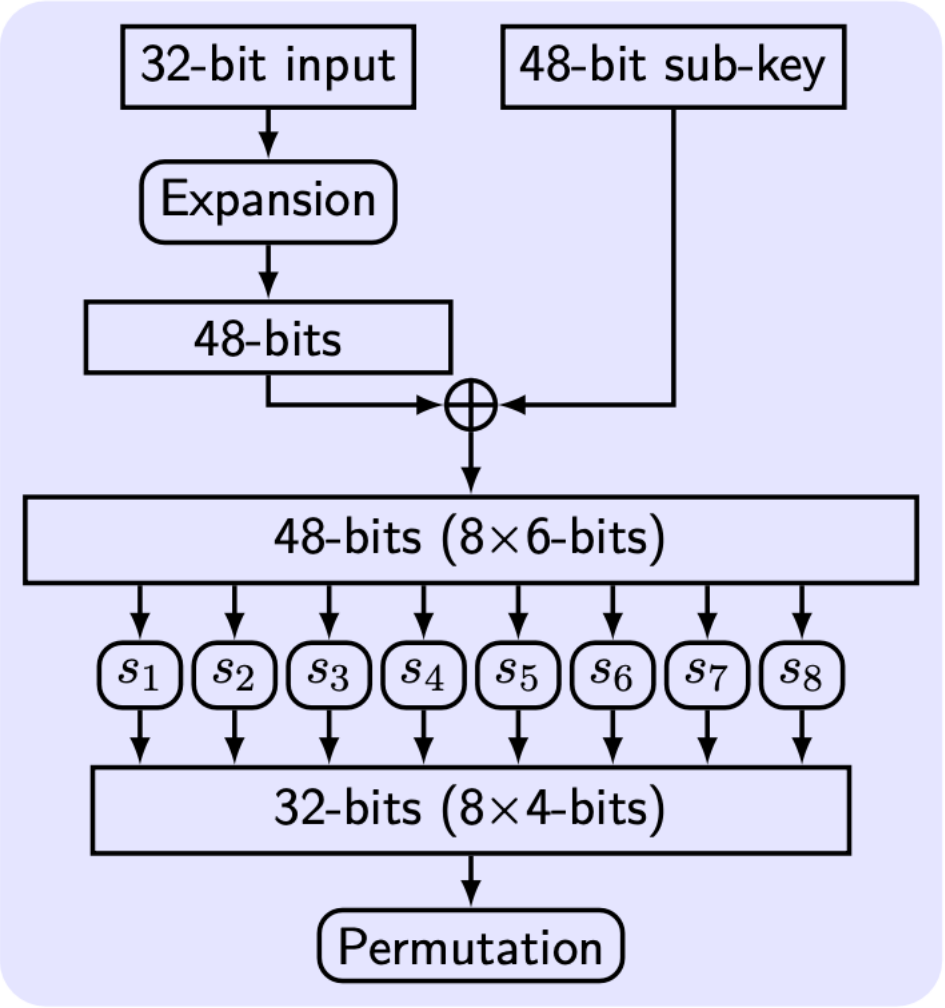
5 $\quad L_r \leftarrow R_{r-1}$

6 $\quad R_r \leftarrow f(k_r, R_{r-1}) \oplus L_{r-1}$

7 $c \leftarrow IP^{-1}(L_{16} \| R_{16})$

8 **return** c

DES Mangler 函数



DES中的一个S盒

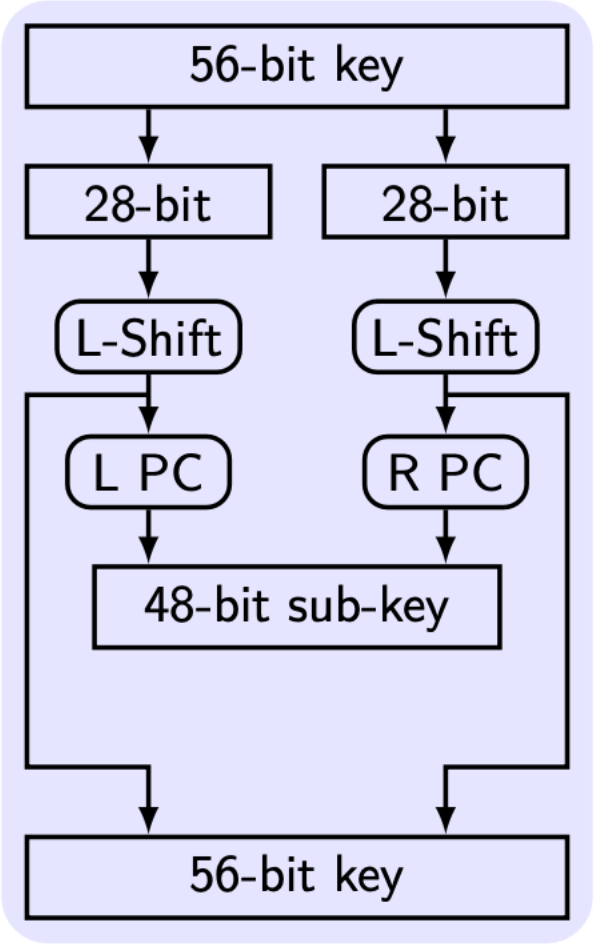
An S-box

Input: $b_{0,1,\ldots,5} = 011001$

Output: $S[b_{0,5}][b_{1,2,3,4}] = S[01][1100] = S[1][12] = 9 = 1001$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

子密钥生成



Bits of shift is 1 or 2 in different rounds.

弱密钥

- **Weak keys**: makes the cipher behave in some undesirable way–producing *identical* sub-keys.

Weak keys (Key with check bits : key w/o check bits)

```
01010101 01010101  :  0000000 0000000
FEFEFEFE FEFEFEFE  :  FFFFFFF FFFFFFF
E0E0E0E0 F1F1F1F1  :  FFFFFFF 0000000
1F1F1F1F 0E0E0E0E  :  0000000 FFFFFFF
```

- **Semi-weak keys**: producing only two different sub-keys. A pair of semi-weak keys k_1, k_2: $F_{k_1}(F_{k_2}(M)) = M$.

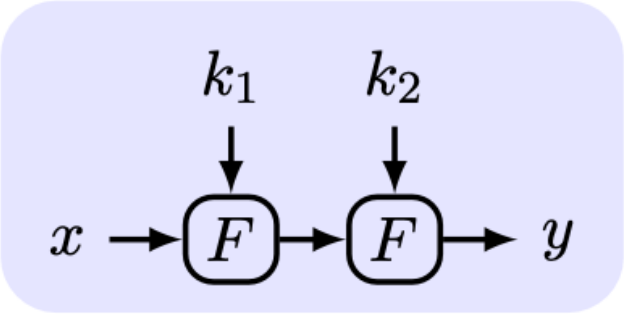
Semi-weak key pairs (2 of total 6 pairs)

```
011F011F 010E010E  &  1F011F01 0E010E01
01E001E0 01F101F1  &  E001E001 F101F101
```

双重加密

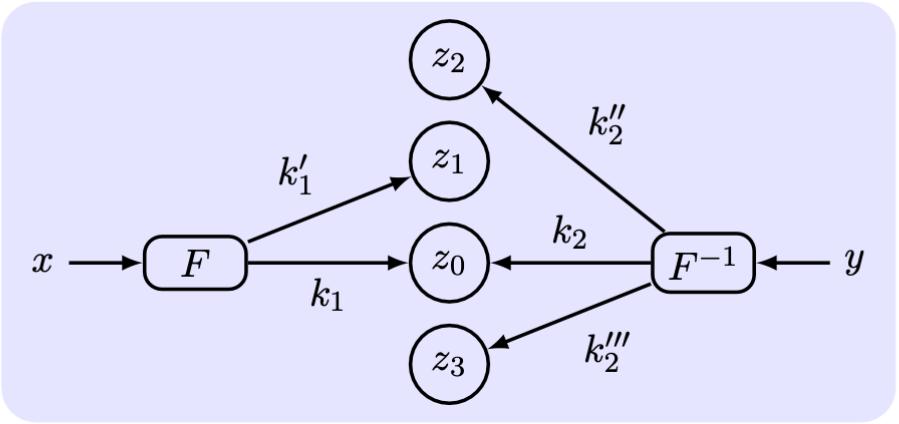
- 为了弥补DES密钥长度不足的缺点，增强加密安全性有两种思路：从内部修改 vs. 黑盒构造；
- 从内部修改不可行，因为即使以最小的方式修改DES，也将失去我们已经从DES获得的信心；

- **Double encryption**: $y = F'_{k_1,k_2}(x) \stackrel{\text{def}}{=} F_{k_2}(F_{k_1}(x))$.



中间相遇攻击（Meet-In-the-Middle Attack）

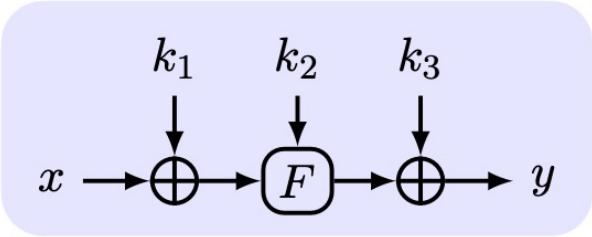
- 在已知明文攻击（KPA）下，从输入方向输入一个明文，通过一次DES加密，猜测不同密钥来得到一组中间值，保存这些密钥和中间值对；从输出方向反向输入一个密文，通过一个DES解密，猜测不同密钥来得到另一组中间值，也保存这些密钥和中间值对；这两组中间值中相同的为z_0，相应的两个密钥k_1和k_2就可能是实际密钥。



- $z_0 = F_{k_1}(x) = F_{k_2}^{-1}(y) \iff y = F'_{k_1,k_2}(x)$.
- Key pair (k_1, k_2) satisfies the equation with probability 2^{-n}.
- The number of such key pairs is $2^{2n}/2^n = 2^n$.
- With another two I/O pairs, the expected number of key pairs is $2^n/2^{2n} = 2^{-n}$. So that is it!
- $\mathcal{O}(2^n)$ time and $\mathcal{O}(2^n)$ space.

DESX

- 为了增强DES并对抗中间相遇攻击，DESX通过密钥白化来增加有效密钥长度；
- 白化（whitening）：一个xor-enc-xor（XEX）模式，用部分密钥来与输入和输出进行异或；



Whitening: XORing Input/Output with partial keys.
DESX:

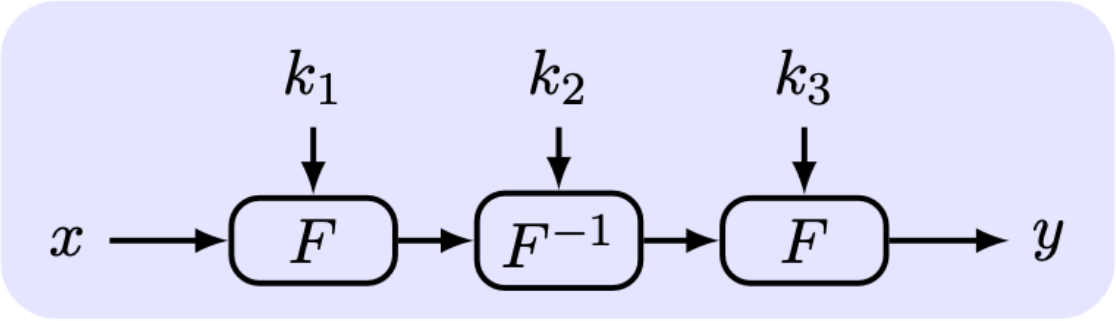
$$k = (k_1, k_2, k_3), |k_1| = |k_3| = 64, |k_2| = 56$$

$$y = k_3 \oplus F_{k_2}(x \oplus k_1)$$

$$x = k_1 \oplus F_{k_2}^{-1}(y \oplus k_3)$$

Security: $|k| = 184$, but break in time 2^{64+56}.

三重加密



- $k_1 = k_2 = k_3$: a single F with backward compatibility.
- $k_1 \neq k_2 \neq k_3$: time 2^{2n} under the meet-in-the-middle attack.
- $k_1 = k_3 \neq k_2$: time 2^{2n} with 1 I/O pair; time 2^n with 2^n pair.
- **Triple-DES** (3DES): strong, but small block length and slow.

高级加密标准 AES（The Advanced Encryption Standard）

- 1997年，NIST召集高级加密标准 AES提案；
- 2001年，J. Daemen 和 V. Rijmen设计的Rijndael成为AES；
- AES是第一个用于绝密信息的公开可用密码；
- 设计目标不仅包括安全，还包括有效性和灵活性等；
- 128位块长度，128，192，或256位密钥；
- 并非一个Feistel结构，而是一个SPN；
- 对于减少轮次的变体只有非简单的攻击：
- 对于 6/10轮的128位密钥，2^{27} 时间；
- 对于 8/12轮的192位密钥，2^{188} 时间；
- 对于 8/14轮的 256位密钥，2^{204} 时间；

AES加密过程演示（动画）

Algorithm 2: AES

input : key k, message m

output: ciphertext c

1 $(k_1, \ldots, k_{10}) \leftarrow Expand(k)$

2 $s \leftarrow m \oplus k_0$

3 **for** $r = 1$ **to** *10* **do**

4 $\quad s \leftarrow SubBytes(s)$

5 $\quad s \leftarrow ShiftRows(s)$

6 $\quad$ **if** $r \leq 9$ **then** $s \leftarrow MixColumns(s)$

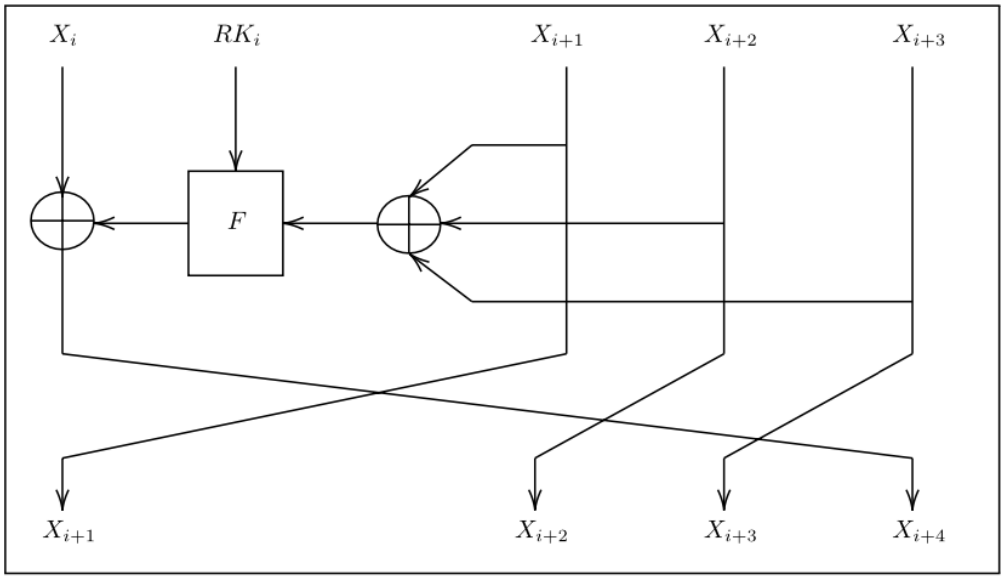
7 $\quad s \leftarrow s \oplus k_R$

8 **return** $c \leftarrow s$

See ▸ an animation of Rijndael !

我国商用分组密码SM4

- 我国商用密码标准SM4（ShangMi4）是分组密码的国家标准，用于无线局域网和TLS。
- SM4由吕述望老师主要开发，2006年解密，2012年由国家密码局发布，并在2016年成为国家标准（GB/T 32907-2016）。
- SM1以芯片实现，和SM7用于轻量级场景，也都是对称加密方案，都保密，未公开。
- 问题：为什么这些国密标准不公开，或者很晚才公开?



本节小结

- 实践中通过混乱扩散模式构造PRP
- SPN网络实现雪崩效应，Feistel网络实现不可逆为可逆
- DES是一个Feistel网络，其中加密使用SPN
- 扩展DES密钥长度面临中间相遇攻击
- 当前采用AES或者SM4