

密码学

第五讲 中国商用分组密码SMS4

张焕国

武汉大学计算机学院

空天信息安全与可信计算教育部重点实验室





内容简介

- 第一讲 信息安全概论
- 第二讲 密码学的基本概念
- 第三讲 数据加密标准 (DES)
- 第四讲 高级数据加密标准 (AES)
- 第五讲 中国商用分组密码 (SMS4)**
- 第六讲 分组密码的应用技术
- 第七讲 序列密码
- 第八讲 复习
- 第九讲 公钥密码 (1)





内容简介

第十讲 公钥密码 (2)

第十一讲 数字签名 (1)

第十二讲 数字签名 (2)

第十三讲 **HASH**函数

第十四讲 认证

第十五讲 密码协议

第十六讲 密钥管理 (1)

第十七讲 密钥管理 (2)

第十八讲 复习

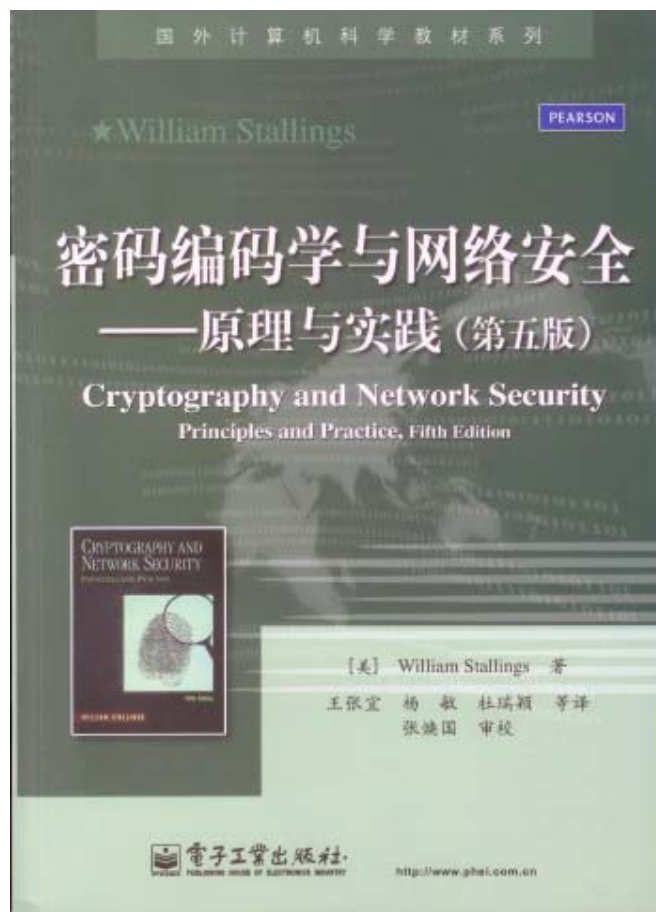


教材与主要参考书

教材



参考书



武汉大学



一、我国商用密码的概况

(1) 坚持密码的公开设计原则

- 密码的安全应仅依赖于密钥的保密，不依赖于算法的保密

(2) 公开设计原则并不要求使用时公开所有的密码算法

- 核心密码不能公开算法
- 核心密码的设计也要遵循公开设计原则

(3) 商用密码应当公开算法

- 美国DES开创了公开商用密码算法的先例
- 美国经历了DES（公开）→EES（保密）→AES（公开）的曲折过程，实践证明公开征集、公布算法的路线是正确的
- 欧洲也公布商用密码算法





一、我国商用密码的概况

(4)我国的商用密码概况

- 我国在密码技术方面具有优势

- 密码理论

- 密码分析

- 长期以来不公开密码算法，只提供密码芯片

- 少数专家设计，难免有疏漏

- 难于标准化，应用成本高，不利于推广应用

- 近年来我国陆续公布了商用密码算法

- 2006年2月公布了分组密码SMS4

- 2011年2月公布了椭圆曲线密码SM2和杂凑算法SM3

- 商用密码管理更加科学化、与国际接轨

- 这将促进我国商用密码的发展





二、商用分组密码SMS4的概况

● 分组密码

- 数据分组（明文，密文）长度=128位、密钥长度=128位
- 数据处理单位：字节（8位），字（32位）

● 密码算法特点

- 对合运算：解密算法与加密算法相同
- 子密钥生成算法与加密算法结构类似

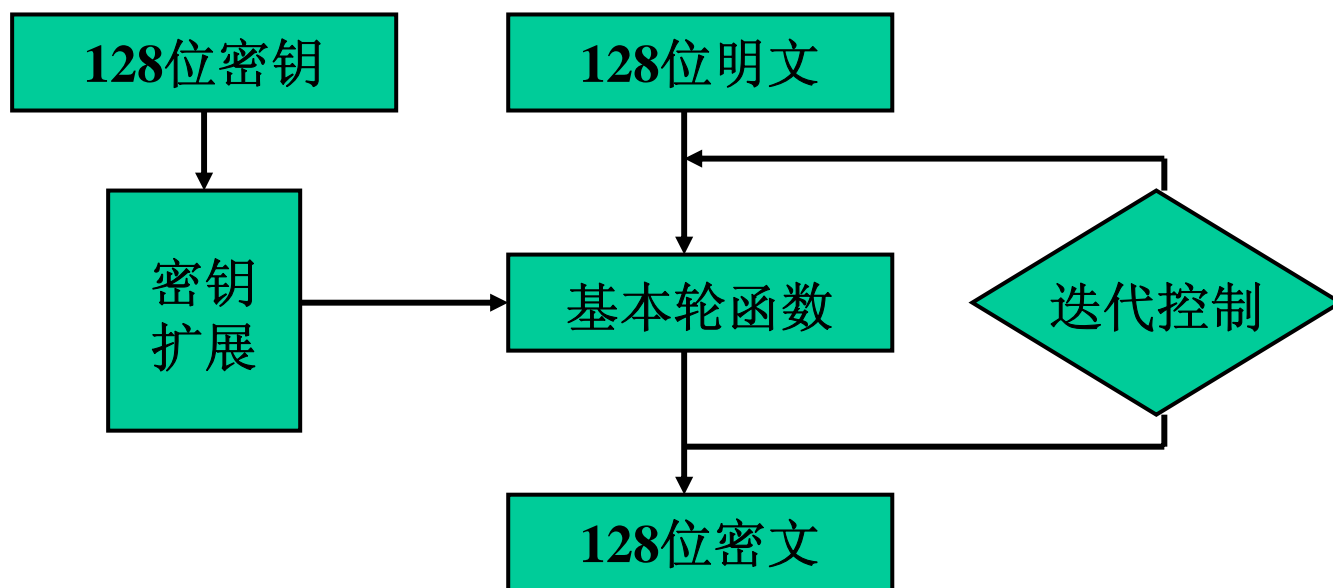
● 密码结构

- 不是SP结构，也不是Feistel结构
- 是一种新的结构：滑动窗口结构



三、SMS4密码算法

1、SMS4 密码算法结构



三、SMS4密码算法

2、SMS4 密码算法

(1)基本运算:

① 模2加: \oplus , 32 比特异或运算

② 循环移位: $\lll i$, 把32位字循环左移*i* 位

(2)基本密码部件:

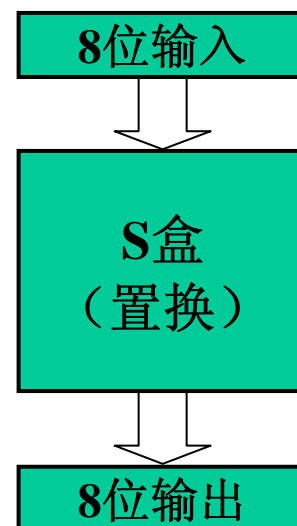
① 非线性字节变换部件S盒:

■ 8位输入, 8位输出。

■ 本质上是 8位的非线性置换。

■ 设输入为a, 输出为b, S盒运算可表示为:

$$b = S_Box(a)$$




三、SMS4密码算法

S盒数据表:

S 盒中数据均采用 16 进制表示。

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	d6	90	e9	fe	cc	e1	3d	b7	16	b6	14	c2	28	fb	2c	05
1	2b	67	9a	76	2a	be	04	c3	aa	44	13	26	49	86	06	99
2	9c	42	50	f4	91	ef	98	7a	33	54	0b	43	ed	cf	ac	62
3	e4	b3	1c	a9	c9	08	e8	95	80	df	94	fa	75	8f	3f	a6
4	47	07	a7	fc	f3	73	17	ba	83	59	3c	19	e6	85	4f	a8
5	68	6b	81	b2	71	64	da	8b	f8	eb	0f	4b	70	56	9d	35
6	1e	24	0e	5e	63	58	d1	a2	25	22	7c	3b	01	21	78	87
7	d4	00	46	57	9f	d3	27	52	4c	36	02	e7	a0	c4	c8	9e
8	ea	bf	8a	d2	40	c7	38	b5	a3	f7	f2	ce	f9	61	15	a1
9	e0	ae	5d	a4	9b	34	1a	55	ad	93	32	30	f5	8c	b1	e3
a	1d	f6	e2	2e	82	66	ca	60	c0	29	23	ab	0d	53	4e	6f
b	d5	db	37	45	de	fd	8e	2f	03	ff	6a	72	6d	6c	5b	51
c	8d	1b	af	92	bb	dd	bc	7f	11	d9	5c	41	1f	10	5a	d8
d	0a	c1	31	88	a5	cd	7b	bd	2d	74	d0	12	b8	e5	b4	b0
e	89	69	97	4a	0c	96	77	7e	65	b9	f1	09	c5	6e	c6	84
f	18	f0	7d	ec	3a	dc	4d	20	79	ee	5f	3e	d7	cb	39	48





三、SMS4密码算法

● S盒的置换规则:

■ 以输入的前半字节为行号，后半字节为列号，行列交叉点处的数据即为输出。

■ 举例：设输入为“ef”，则行号为e，列号为f，于是S盒的输出值为表中第e行和第f列交叉点的值，即

$$Sbox('ef') = '84'$$

■ 说明：在主要密码学指标上达到最佳，与AES的S盒相当

② 非线性字变换 τ ：32位字的非线性变换

■ 4个S盒并行置换

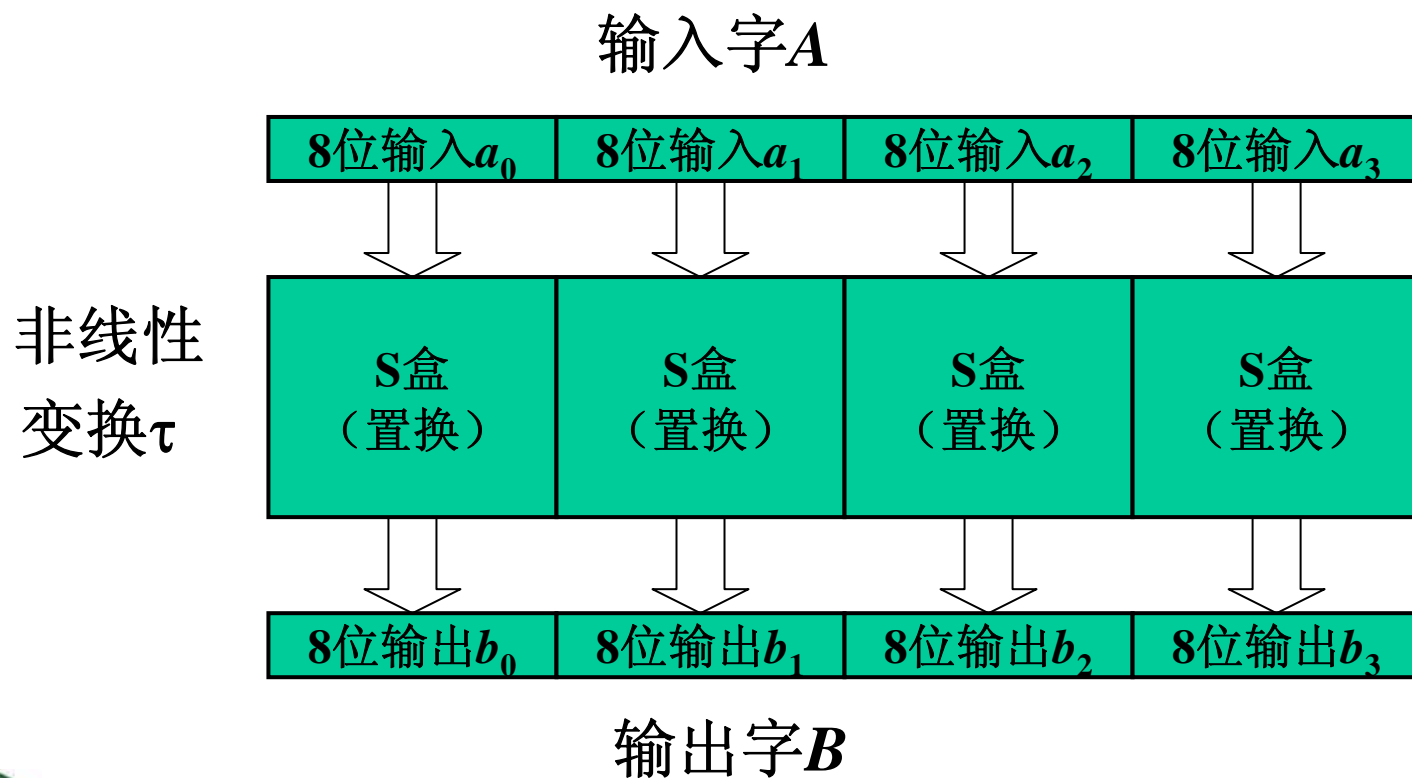
■ 设输入字 $A=(a_0, a_1, a_2, a_3)$ ，输出字 $B=(b_0, b_1, b_2, b_3)$ ，

$$B = \tau(A) = (S_box(a_0), S_box(a_1), S_box(a_2), S_box(a_3))$$



三、SMS4密码算法

②非线性变换 τ : 32位字的非线性变换





三、SMS4密码算法

③字线性部件 L 变换:

- 32位输入, 32位输出。
- 设输入为 B , 输出为 C , 表为:

$$C=L(B)$$

- 运算规则:

$$C=L(B)$$

$$=B \oplus (B \lll 2) \oplus (B \lll 10) \oplus (B \lll 18) \oplus (B \lll 24)$$

④字合成变换 T :


- 由非线性变换 τ 和线性变换 L 复合而成;

$$T(X)=L(\tau(X))。$$

先S盒变换, 后 L 变换。

武汉大学





三、SMS4密码算法

(3)轮函数 F :

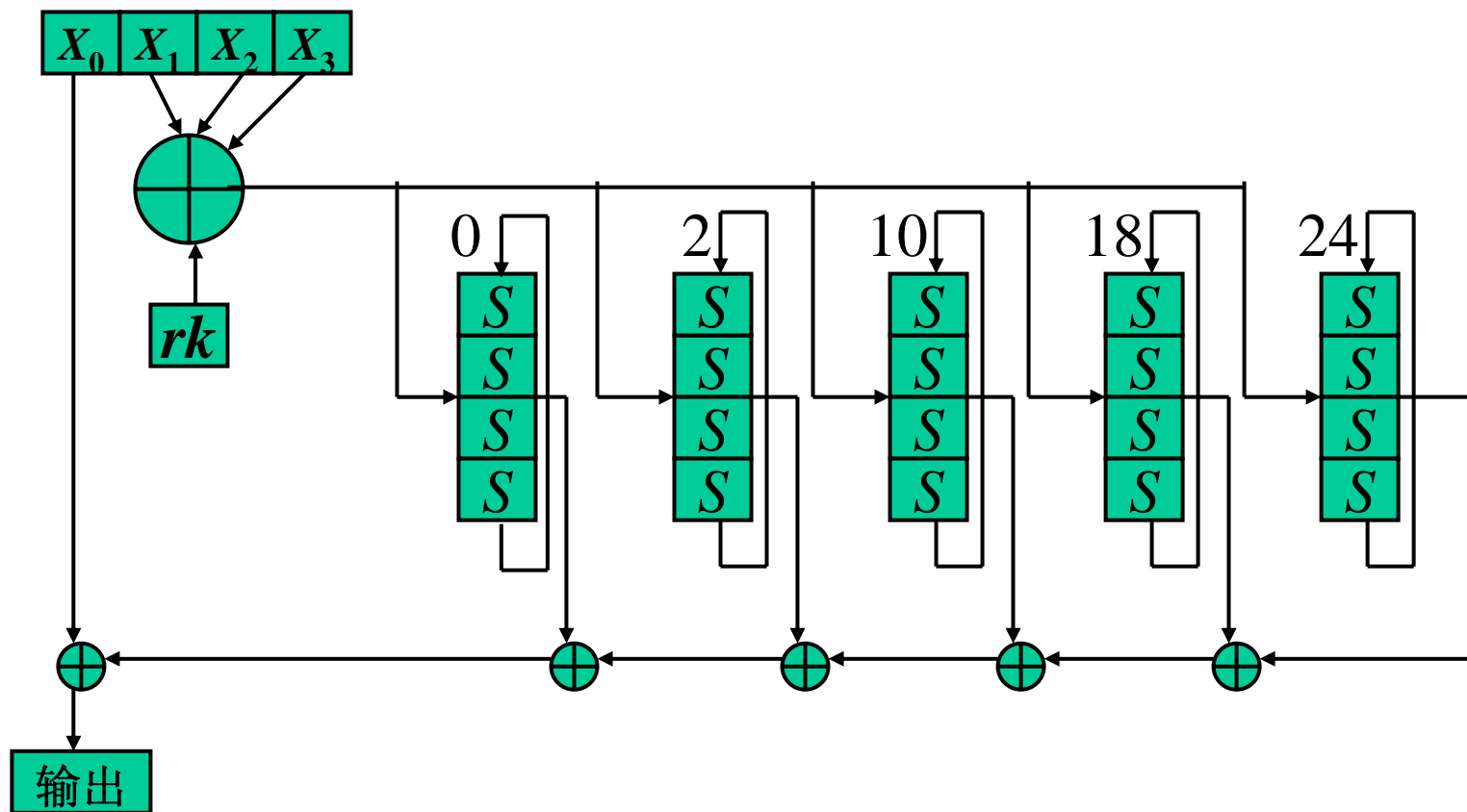
- 输入数据: (X_0, X_1, X_2, X_3) , 128位, 四个32位字。
- 输入轮密钥: rk , 32位字。
- 输出数据: 32位字。
- 轮函数 F :


$$\begin{aligned} &F(X_0, X_1, X_2, X_3, rk) \\ &= X_0 \oplus T(X_1 \oplus X_2 \oplus X_3 \oplus rk) \end{aligned}$$



三、SMS4密码算法

(3)轮函数 F :





三、SMS4密码算法

(4)加密算法:

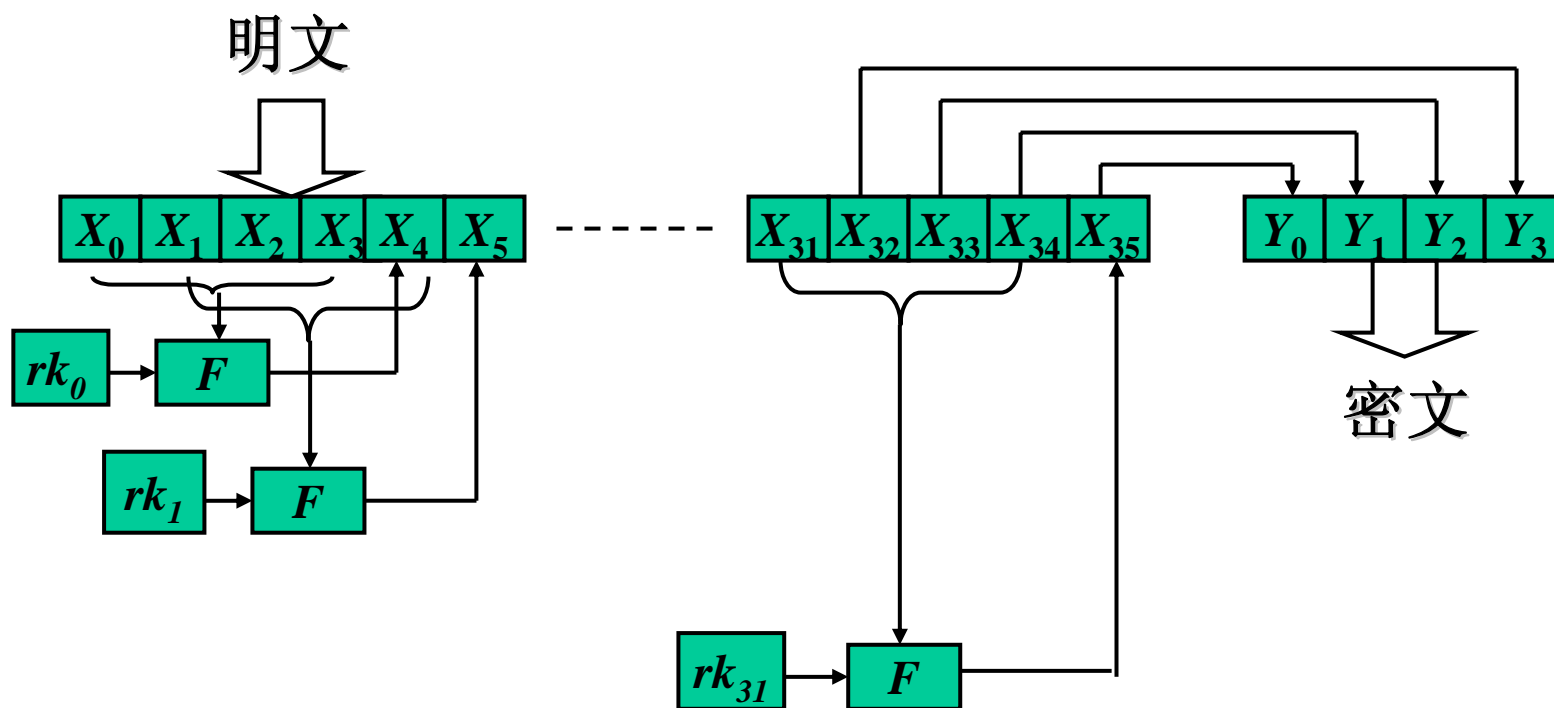
- 输入明文: (X_0, X_1, X_2, X_3) , 128位, 四个字。
- 输入轮密钥: rk_i , $i=0,1,...,31$, 共32个轮密钥。
- 输出密文: (Y_0, Y_1, Y_2, Y_3) , 128位, 四个字。
- 算法结构: 轮函数32轮迭代, 每轮使用一个轮密钥。
- 加密算法:


$$\begin{cases} X_{i+4}=F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) \\ \quad = X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i), \quad i = 0,1...31 \\ (Y_0, Y_1, Y_2, Y_3) = (X_{35}, X_{34}, X_{33}, X_{32}) \end{cases}$$



三、SMS4密码算法

(4)加密算法:






三、SMS4密码算法

(5)解密算法:

- SMS4密码算法是对合的, 因此解密与加密算法相同, 只是轮密钥的使用顺序相反。
- 输入密文: (Y_0, Y_1, Y_2, Y_3)
- 输入轮密钥: $rk_i, i=31,30, \dots,1, 0$
- 输出明文: (X_0, X_1, X_2, X_3)
- 算法: 轮函数的32轮迭代, 每轮使用一个轮密钥。
- 解密算法:

$$\left\{ \begin{array}{l} Y_{i+4}=F(Y_i, Y_{i+1}, Y_{i+2}, Y_{i+3}, rk_i) \\ \quad = Y_i \oplus T(Y_{i+1} \oplus Y_{i+2} \oplus Y_{i+3} \oplus rk_i), i=31, \dots, 1, 0 \\ (X_0, X_1, X_2, X_3) = (Y_{35}, Y_{34}, Y_{33}, Y_{32}) \end{array} \right.$$





三、SMS4密码算法

(6)密钥扩展算法:

①常数FK

● 在密钥扩展中使用一些常数


$FK_0=(A3B1BAC6)$

$FK_1=(56AA3350)$

$FK_2=(677D9197)$

$FK_3=(B27022DC)$





三、SMS4密码算法

(6)密钥扩展算法:


②固定参数CK

● 32 个固定参数 Ck_i , $i=0,1,2,...,31$

00070e15, 1c232a31, 383f464d, 545b6269,
70777e85, 8c939aa1, a8afb6bd, c4cbd2d9,
e0e7eef5, fc030a11, 181f262d, 343b4249,
50575e65, 6c737a81, 888f969d, a4abb2b9,
c0c7ced5, dce3eaf1, f8ff060d, 141b2229,
30373e45, 4c535a61, 686f767d, 848b9299,
a0a7aeb5, bcc3cad1, d8dfe6ed, f4fb0209,
10171e25, 2c333a41, 484f565d, 646b7279

产生规则: $Ck_{ij} = (4i+j) \times 7 \pmod{256}$, $i=0,1,2,...,31, j=0,1,...,3$ 。





三、SMS4密码算法

(6)密钥扩展算法:

- 输入加密密钥: $MK = (MK_0, MK_1, MK_2, MK_3)$

- 输出轮密钥: $rk_i, i=0, 1, \dots, 30, 31$

- 中间数据: $K_i, i=0, 1, \dots, 34, 35$

- 密钥扩展算法:

① $(K_0, K_1, K_2, K_3) = (MK_0 \oplus FK_0, MK_1 \oplus FK_1, MK_2 \oplus FK_2, MK_3 \oplus FK_3)$

② For $i=0, 1, \dots, 30, 31$ Do

$$ik_i = K_{i+4} = K_i \oplus T'(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i)$$

- 说明: T' 变换与加密算法轮函数中的 T 基本相同, 只将其中的线性变换 L 修改为以下: L'

$$L'(B) = B \oplus (B \lll 13) \oplus (B \lll 23)$$





三、SMS4密码算法

3、实例：

- 明文: 01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10
- 密钥: 01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10
- 密文: 68 1e df 34 d2 06 96 5e 86 b3 e9 4f 53 6e 42 46

4、安全性

- 国家专业机构设计。算法简洁，以字和字节为处理单位，对合运算，符合当今分组密码主流。
- 专业机构进行了充分的密码分析，因此是安全的。
- 民间学者对21轮SMS4进行了差分密码分析。
- 尚需经过更进一步的应用实践检验。





四、分组密码的结构

● 商农的密码设计方法

- **扩散(diffusion)**: 将明文和密钥的每一位的影响散布到尽量多的密文位中。
- **混淆(confusion)**: 使明文、密钥和密文之间的关系复杂化。
- **迭代**: 轮函数迭代
- **乘积**: 多密码复合





四、分组密码的结构

分组密码的结构可以分为以下几种类型：

1、Feistel结构

■ Feistel于1973年提出这种结构，根据商农的思想来设计分组密码。

● 基本函数

■ 设要加密的明文数据 M 长 n 位(n 是偶数)，将 M 划分为两半： L_0 ， R_0 。

■ 定义一个函数：输入是 $\langle L_{i-1}, R_{i-1} \rangle$ ，输出是 $\langle L_i, R_i \rangle$ ，

$$L_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

$$R_i = R_{i-1}$$

其中 f 是任意函数， K_i 是子密钥。

武汉大学

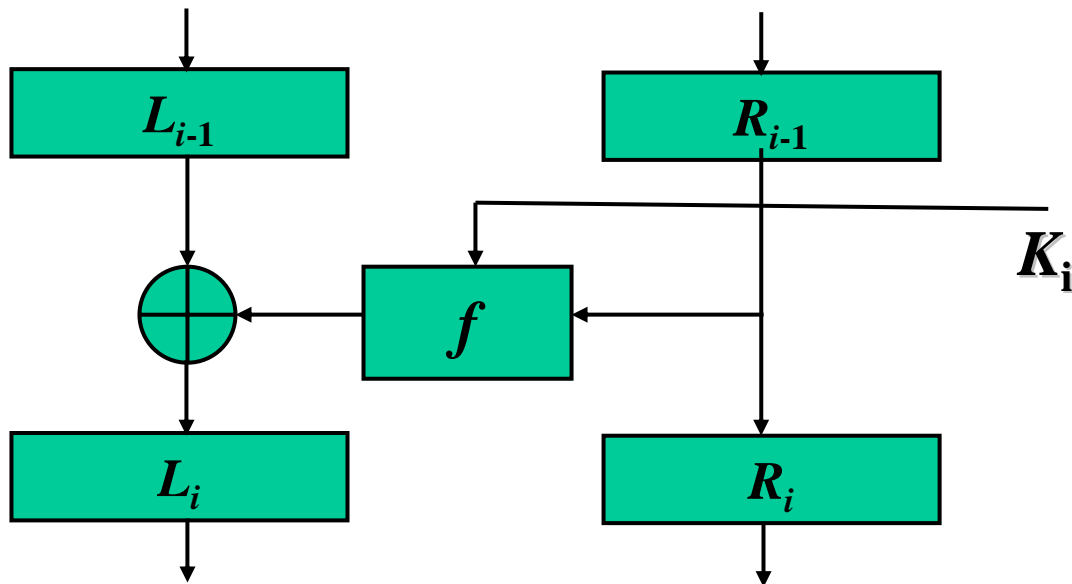




四、分组密码的结构

1、Feistel结构

- 基本函数





四、分组密码的结构

1、Feistel结构

■ **结论1：** 对于任意的函数 f ，上述函数都是可逆的。

证明：把 $\langle L_{i-1}, R_{i-1} \rangle$ 加到函数的输入端进行变换，可得 $\langle L_i, R_i \rangle = \langle L_{i-1} \oplus f(R_{i-1}, K_i), R_{i-1} \rangle$ 。现把 $\langle L_i, R_i \rangle$ 加到输入端再进行变换，可得

$$\langle (L_{i-1} \oplus f(R_{i-1}, K_i)) \oplus f(R_{i-1}, K_i), R_{i-1} \rangle = \langle L_{i-1}, R_{i-1} \rangle。$$

这说明函数是可逆的。

■ **结论2：** 上述函数是对合的。

证明：由于上述函数的逆就是其本身，说明其是对合的。



四、分组密码的结构

1、Feistel结构

● 轮函数

- 在基本函数基础上增加一个交换函数 T

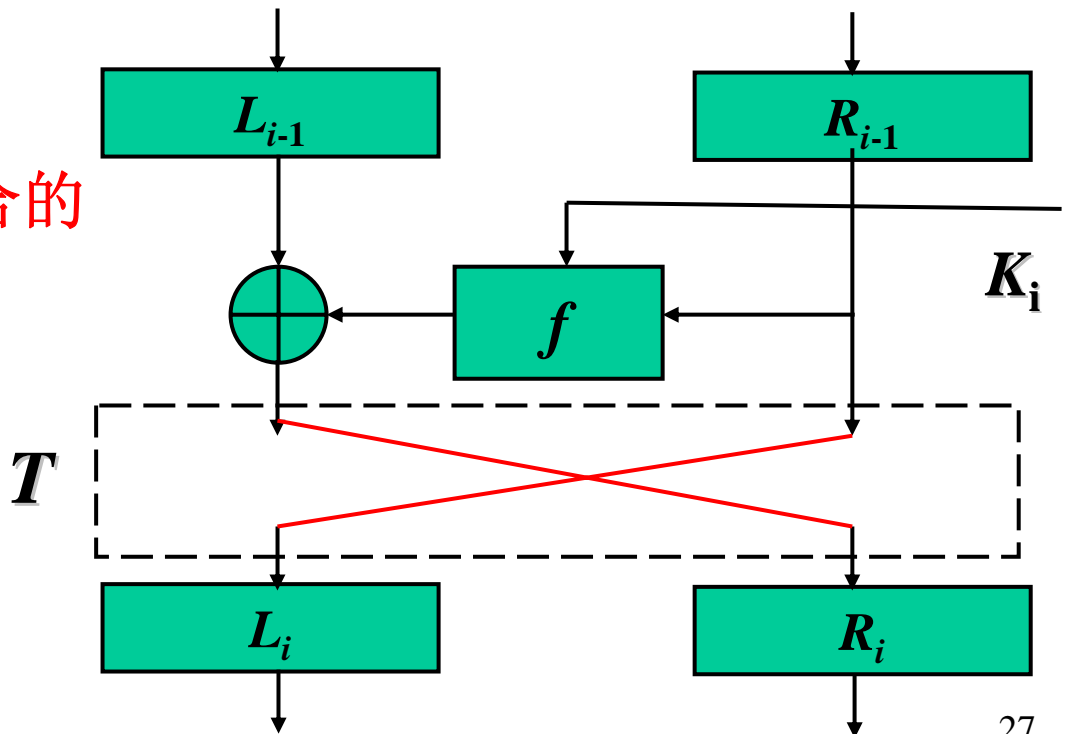
$$T(L,R)=(R,L)$$

- T 是对合的

- 因此轮函数是对合的

● 密码算法

- 对轮函数迭代





四、分组密码的结构

1、Feistel结构

● 优点

- 不管 f 是什么函数，基本函数都可逆，进而确保轮函数可逆以及整个密码算法可逆。
- 由于基本函数是对合的，进而确保轮函数是对合的以及整个密码算法是对合的。
- 这使得密码算法的设计变得比较容易。

● 缺点

- 扩散较慢，算法迭代2轮才能改变输入的每1位。

● 成功实例DES

- S盒实现混淆，P置换实现扩散，构成一个复杂的轮函数。
- 算法是对合的，工程实现节省一半。
- 密码是安全的。





四、分组密码的结构

1、Feistel结构

● Feistel结构得到广泛应用与发展

■ DES, FEAL, GOST, LOKI, E2, Blowfish, RC5等著名密码都采用Feistel结构。

■ 除了标准Feistel结构外，被推广到非平衡Feistel结构。

◆ 标准Feistel结构中，左右两半数据等长。而非平衡Feistel结构中左右两块数据长度不同。





四、分组密码的结构

2、SP结构

● S(Substitution)P(Permutation)结构

- 用非线性S盒实现混淆，称为混淆层。
- 用线性置换实现扩散，称为扩散层。
- 在混淆层之前设置一个受密钥控制的前置处理层。
- 或者在扩散层之后设置一个受密钥控制的后置处理层。

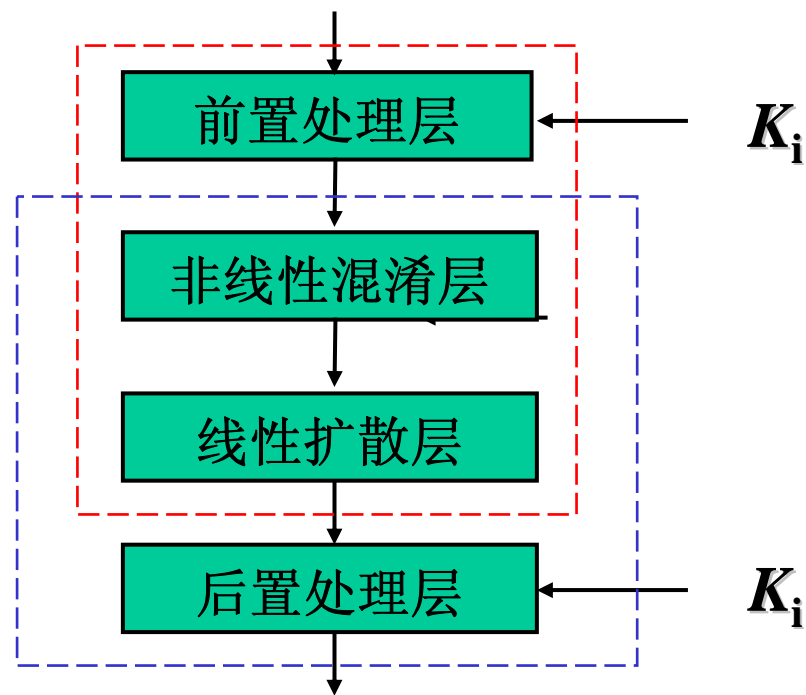




四、分组密码的结构

2、SP结构

- 轮函数





四、分组密码的结构

2、SP结构

● 优点

- 结构清晰，容易分析和把握每层的密码学指标，从而把握密码的安全性
- 扩散较Feistel结构快

● 缺点

- 不容易得到对合的密码算法
- 要注意密码算法迭代的开始和最后处理，应有密钥参与的密码变换。

● 应用实例

- AES，MARS，SAFER，SHARK 等密码都采用SP结构。

武汉大学





四、分组密码的结构

3、滑动窗口结构

- 代表密码SMS4

- 结构特点

- 仍然是轮函数迭代结构

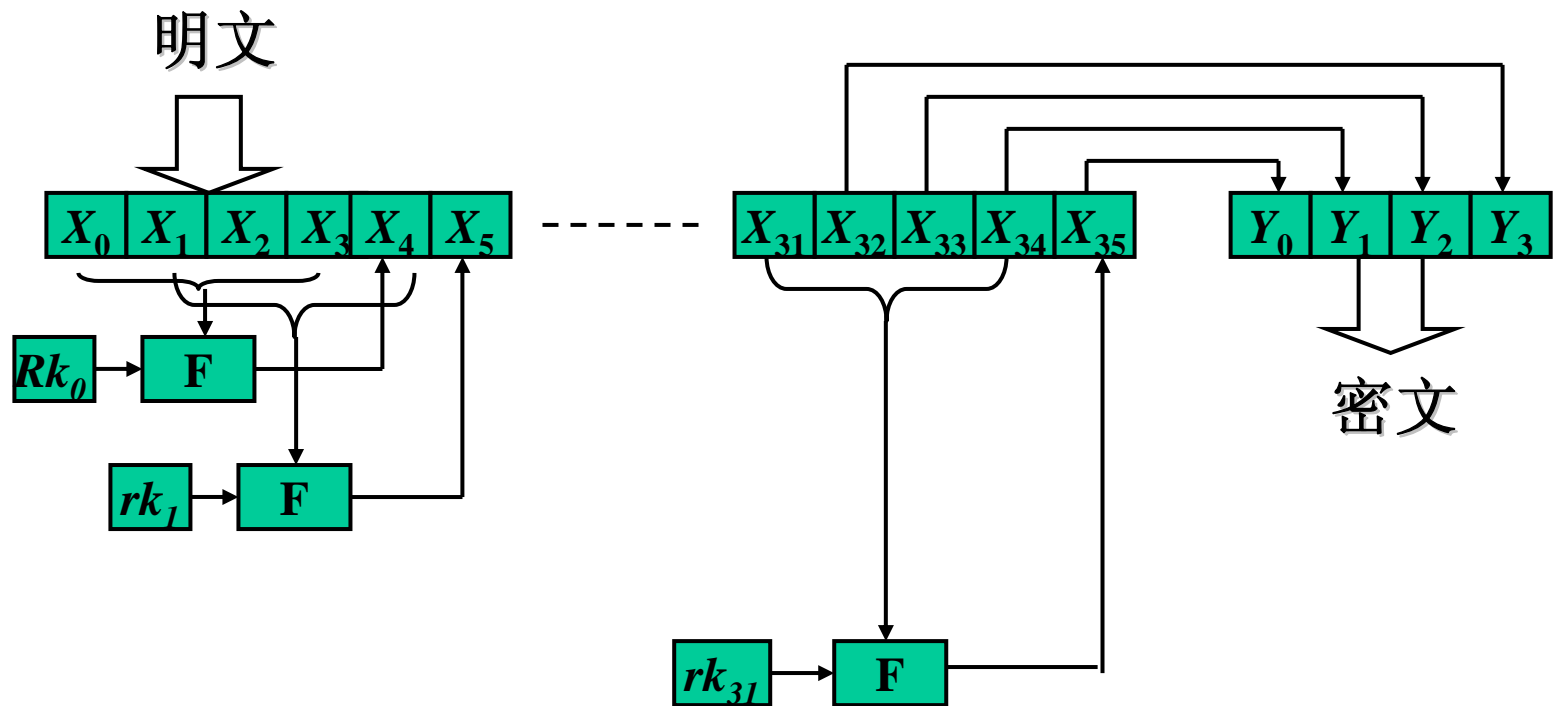
- 但是，具有密文链接的特点。每轮加密产生的最后一个密文字加入到下一轮的加密过程中，第一个密文字退出加密。相当于一个窗口在移动。

- 因此，形象地称为滑动窗口型



四、分组密码的结构

SMS4算法:





四、分组密码的结构

3、滑动窗口结构

- 优点

- 容易得到对合的密码算法

- 缺点

- 迭代轮数多

- 目前实例校少

- 应用实例

- SMS4采用这种结构





四、分组密码的结构

4、Lai-Massey结构

- 代表密码IDEA

- 结构特点

- 采用三个代数群（ \oplus 16位按位异或群， \odot 16位 $\text{mod } 2^{16} + 1$ 乘法群， \boxplus 16位 $\text{mod } 2^{16}$ 加法群）。
- 这三种运算中的任意两种都不满足分配律和结合律，不构成群。
- 混合运用这三种运算，获得了很好的非线性和混淆特性，确保密码的安全性。





四、分组密码的结构

4、Lai-Massey结构

- 优点

- 容易得到对合的密码算法

- 缺点

- 结构扩展不方便。因为 $2^{16}+1$ 是素数， $\text{mod } 2^{16} + 1$ 构成乘法群，所以可构成IDEA。

- 但 $2^{32}+1$ 不是素数， $\text{mod } 2^{32} + 1$ 不构成乘法群，所以不能构成32位的IDEA。

- 应用实例

- 目前只有IDEA采用这种结构





作业题

1、p114第30题。

自选实践题

1、p114第29题。





谢 谢！



武汉大学