《现代密码学》第四讲

分组密码（四）

《现代密码学》第四讲

中国无线局域网标准（SMS4）算法介绍

上讲内容回顾

- AES 算法的整体结构
- AES 算法的轮函数
- AES 算法的密钥编排算法
- AES 的解密变换

本节主要内容

- SMS4 加 / 解密算法
- SMS4 密钥编排算法
- 分组密码算法的运行模式

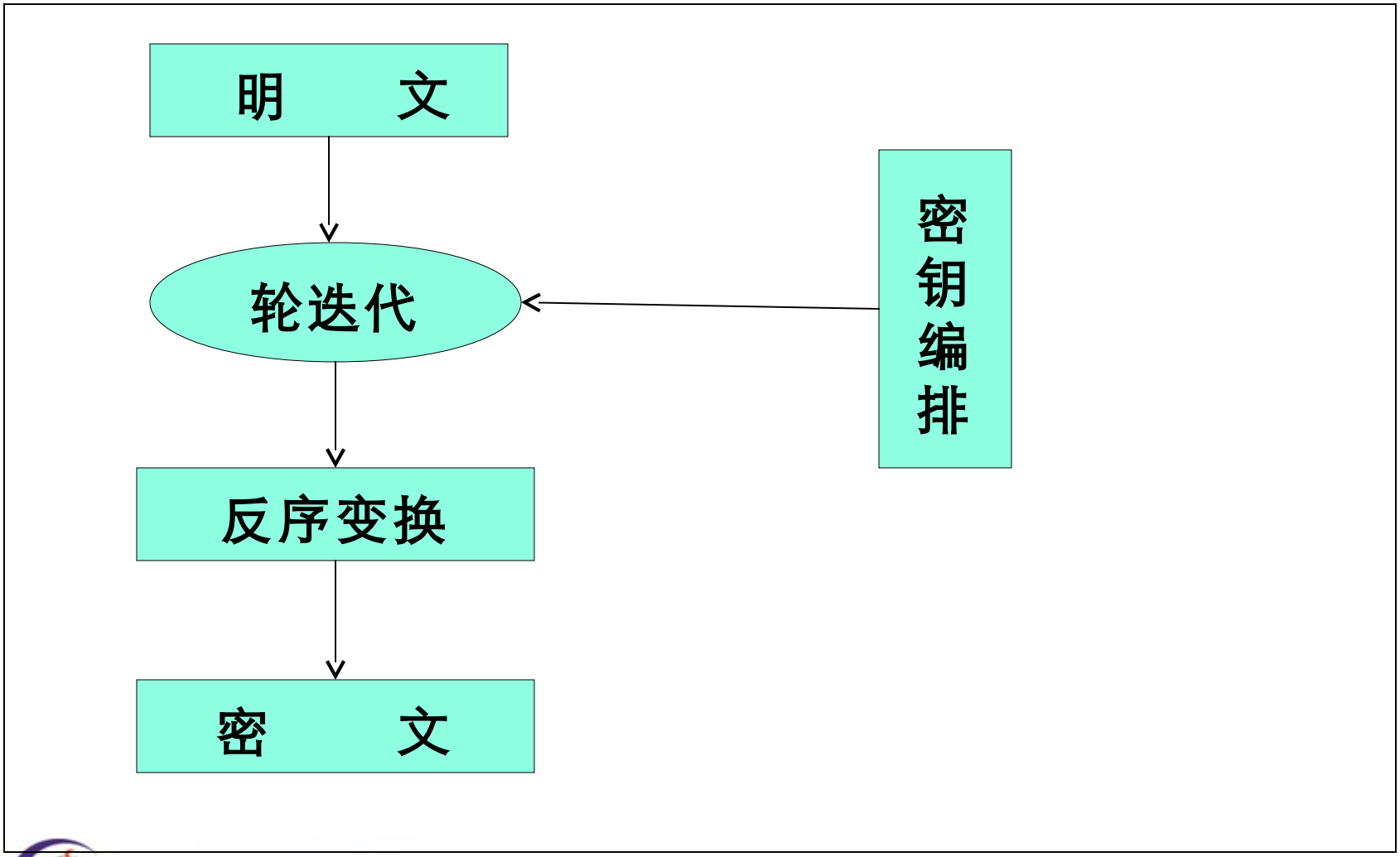
本节主要内容

- SMS4 加 / 解密算法
- SMS4 密钥编排算法
- 分组密码算法的运行模式

SMS4 加密算法

- 2006 年 1 月，国家密码管理局公布了无线局域网产品中适用的建议密码算法，其中包括分组密码 SMS4 .

SMS4 加密算法



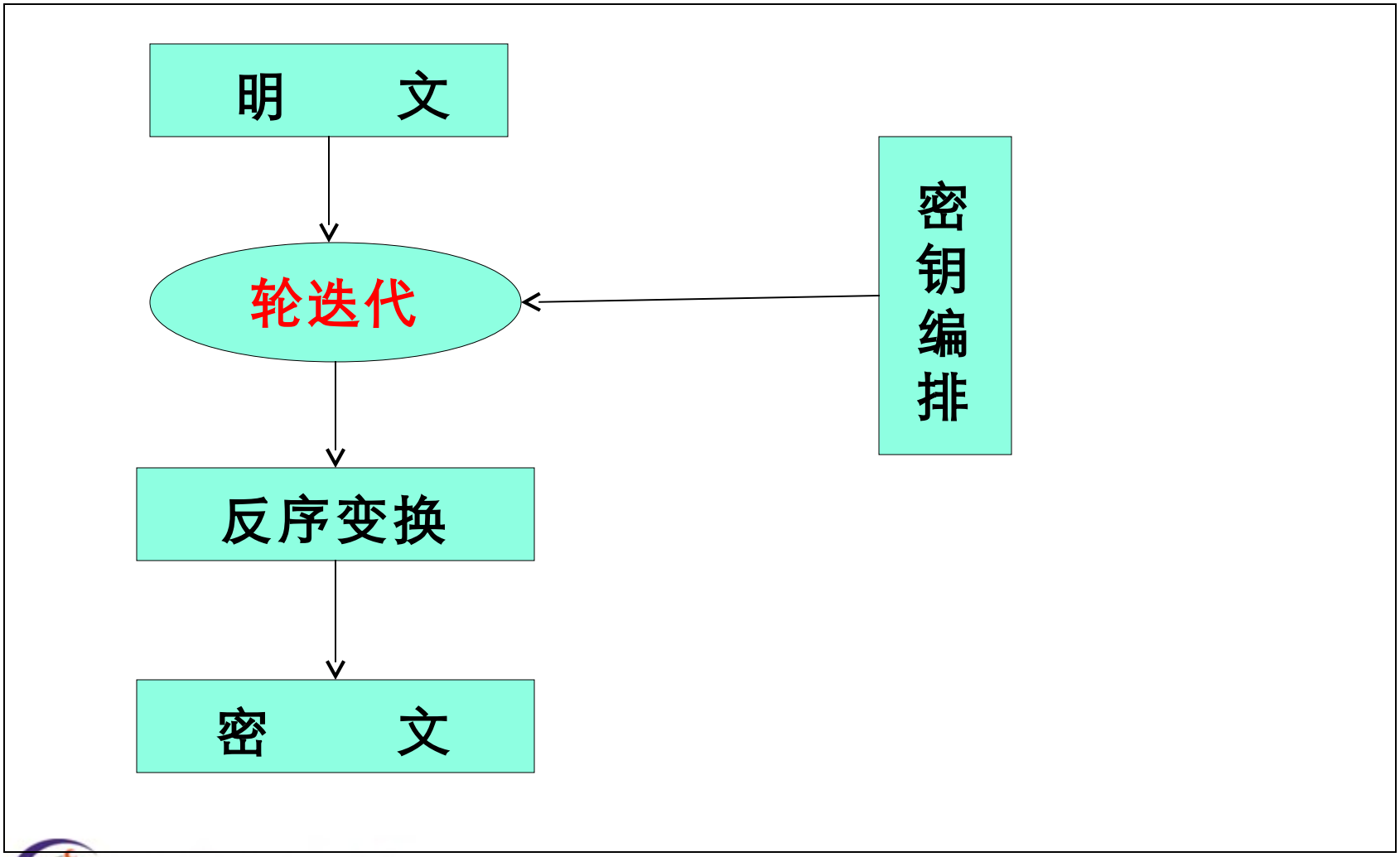
SMS4 加密算法

- 128 比特明文分为 4 个 32 比特字（ 中元素），分别赋值给四个寄存器 A、B，C，D（D 为最高）.
- 进行 32 轮 F 运算，设每轮输入 为寄存器当前状态值 ，则轮函数 F 为：

将寄存器最右边字 A 的值移出，高三个字顺次右移 32 位，F 函数的输出赋值给最左边的寄存器字 D.

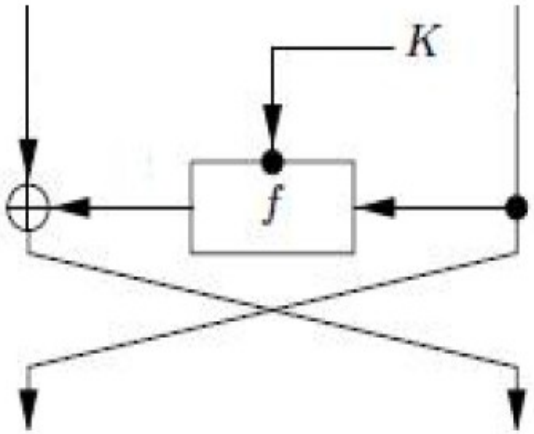
- 32 轮的输出 进行反序变换 R，

SMS4 加密算法

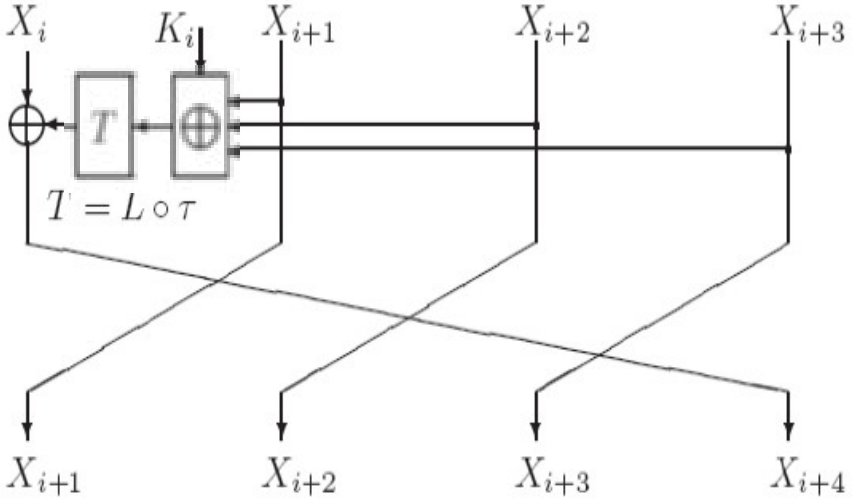


SMS4 加密算法

- 广义 Feistel 结构



1轮Feistel



1轮SMS4

SMS4 加密算法

- 轮函数 F
- 输入寄存器值$(X_{i+3}, X_{i+2}, X_{i+1}, X_i)$ rk_i 和轮密钥：

$$X_{i+4} = F(X_{i+3}, X_{i+2}, X_{i+1}, X_i; rk_i) = X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i)$$

$Z_2^{32} \times Z_2^{32} \to Z_2^{32}$ $i = 0,1,\ldots,31$

- 合成置换 T

T：是一个可逆变换，由非线性变换 τ 和线性变换 L 复合而成，即 T(.)=L(τ(.))

SMS4 加密算法

- 非线性变换 τ 由 4 个并行的 S 盒构成，

  设输入 $Y=(y_3,y_2,y_1,y_0)\in\left(Z_2^8\right)^4$ ，输出 $(z_3,z_2,z_1,z_0)\in\left(Z_2^8\right)^4$

  则

$$(z_3,z_2,z_1,z_0)=\tau(Y)=(Sbox(y_3),Sbox(y_2),Sbox(y_1),Sbox(y_0))$$

- 线性变换 L

  设输入为 $Y\in Z_2^{32}$，输出为 $W\in Z_2^{32}$ ，则

$$W=L(Y)=Y\oplus(Y<<<2)\oplus(Y<<<10)\oplus(Y<<<18)\oplus(Y<<<24)$$

SMS4 加密算法

	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

例：输入‘ef’，则经 S 盒后的值为表中第 e 行和第 f 列的值，*Sbox*(‘ef’)= ‘84’

本节主要内容

- SMS4 加 / 解密算法
- **SMS4 密钥编排算法**
- 分组密码算法的运行模式

SMS4 密钥编排算法

- **输入：**

1）加密密钥长度为 128 比特 $MK=(MK_0,MK_1,MK_2,MK_3)$，其中 $MK_i(i=0,1,2,3)$ 为字；

2）$FK=(FK_0,FK_1,FK_2,FK_3)$ 为系统参数，$CK=(CK_0,CK_1,\ldots,CK_{31})$ 为固定参数，用于密钥扩展算法，其中 $FK_i(i=0,\ldots,3)$，$CK_i(i=0,\ldots,31)$ 均为字．

- **输出：**

轮密钥表示为 $(rk_0,rk_1,\ldots,rk_{31})$，其中 $rk_i(i=0,\ldots,31)$ 均为字

SMS4 密钥编排算法

说明：

- 系统参数 FK 的取值，采用 16 进制表示为：

$$FK_0=(\text{A3B1BAC6}), FK_1=(\text{56AA3350}), FK_2=(\text{677D9197}), FK_3=(\text{B27022DC}).$$

- 固定参数 CK_i 的取值方法：

设 $ck_{i,j}$ 为 CK_i 的第 j 字节（i=0, 1, …, 31；j=0, 1, 2, 3），即

$$ck_i=(ck_{i,0},ck_{i,1},ck_{i,2},ck_{i,3})\in\left(Z_2^8\right)^4$$

则 $$ck_{i,j}=(4i+7j)(\mathrm{mod}\,256).$$

SMS4 密钥编排算法

32 个固定参数CK_i ，其 16 进制表示为：

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

SMS4 密钥编排算法

密钥扩展方法

加密密钥 $MK=(MK_0,MK_1,MK_2,MK_3)$ $MK_i \in Z_2^{32}, i=0,1,2,3$

轮密钥为 $rk_i \in Z_2^{32}, i=0,1,...,31$ ，其生成方法为：

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）对 i=0,1,2,...,31

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

SMS4 密钥编排算法

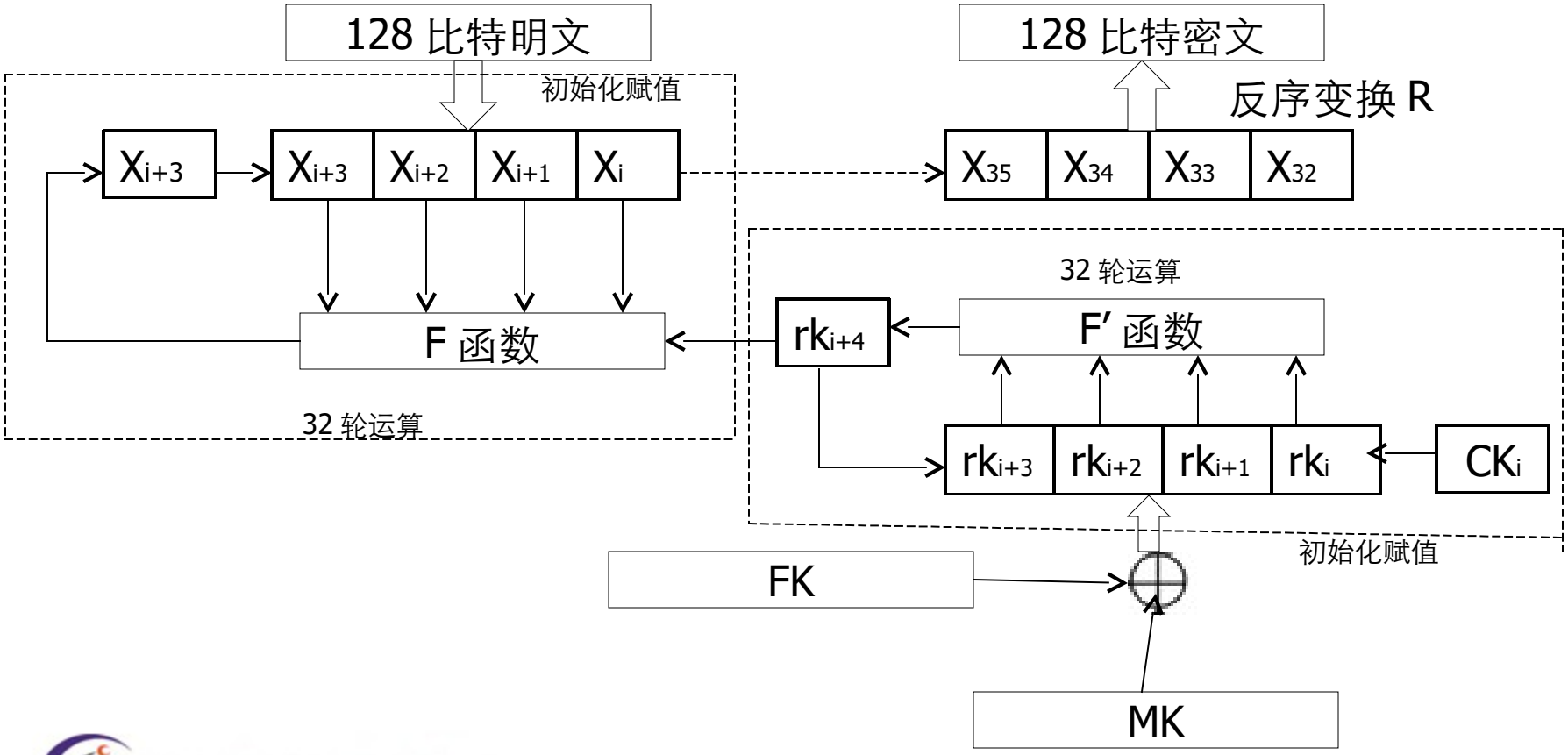
说明：

- *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：

$$L'(Y) = Y \oplus (Y <<< 13) \oplus (Y <<< 23)$$

SMS4 加密算法

SMS4 加密算法结构图



SMS4 解密算法

本算法的解密变换与加密变换结构相同，不同的仅是轮密钥的使用顺序。

加密时轮密钥的使用顺序为：

$$(rk_0, rk_1, \cdots, rk_{31})$$

解密时轮密钥的使用顺序为：

$$(rk_{31}, rk_{30}, \cdots, rk_0)$$

SMS4 解密算法

- 课堂练习：

  证明 SMS4 的迭代结构是加解密相似的

THE END !