现代密码学

第三十讲 SM4算法

信息与软件工程学院

第三十讲 SM4算法

- SM4术语说明
- SM4轮函数
- SM4密钥扩展

SM4概况

- **SM4**分组密码算法是国家密码管理局于**2006**年**1**月**6**日公布的无线局域网产品使用的密码算法，是国内官方公布的第一个商用密码算法。
- **SM4**是一个分组密码算法，分组长度和密钥长度均为**128**比特。加密算法与密钥扩展算法都采用**32**轮非线性迭代结构。
- 它的解密算法与加密算法的结构相同，只是轮密钥的使用顺序相反，解密轮密钥是加密轮密钥的逆序。

SM4算法的术语说明

- Z_2^e 表示**e-**比特的向量集，Z_2^8 中的元素称为字节，Z_2^{32}中的元素称为字
- **S**盒是一个固定的**8**比特输入**8**比特输出的置换，记为 *Sbox*(.)
- **SM4**中的采用了两个基本运算：⊕，**32**比特异或；$<<<i$，**32**比特循环左移 ***i*** 位。

SM4算法的术语说明（续）

- SM4算法的加密密钥长度为128比特，表示为，

$$MK = (MK_0, MK_1, MK_2, MK_3)$$

其中，$MK_i \ i = 0,1,2,3$ 为字。

- 轮密钥为，$(rk_0, rk_1, \cdots, rk_{31})$，$rk_i$为字。轮密钥由加密密钥通过密钥扩展算法生成。
- $FK = (FK_0, FK_1, FK_2, FK_3)$ 为系统参数，
- $CK = (CK_0, CK_1, \cdots, CK_{31})$ 为固定参数，用于密钥扩展算法。

第三十讲 SM4算法

- SM4术语说明
- SM4轮函数
- SM4密钥扩展

SM4加密算法整体结构

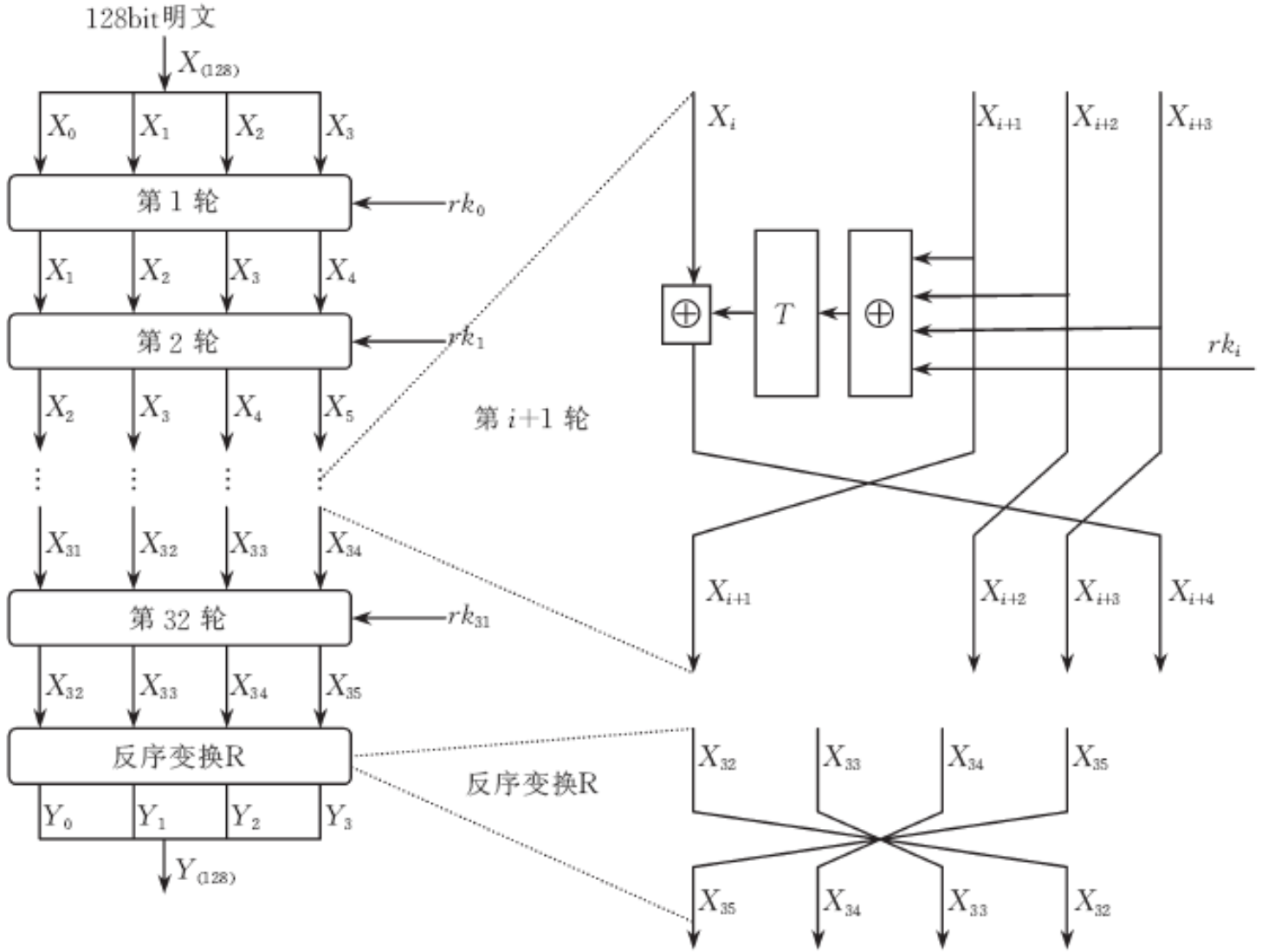


图 1　SMS4 加密算法整体结构

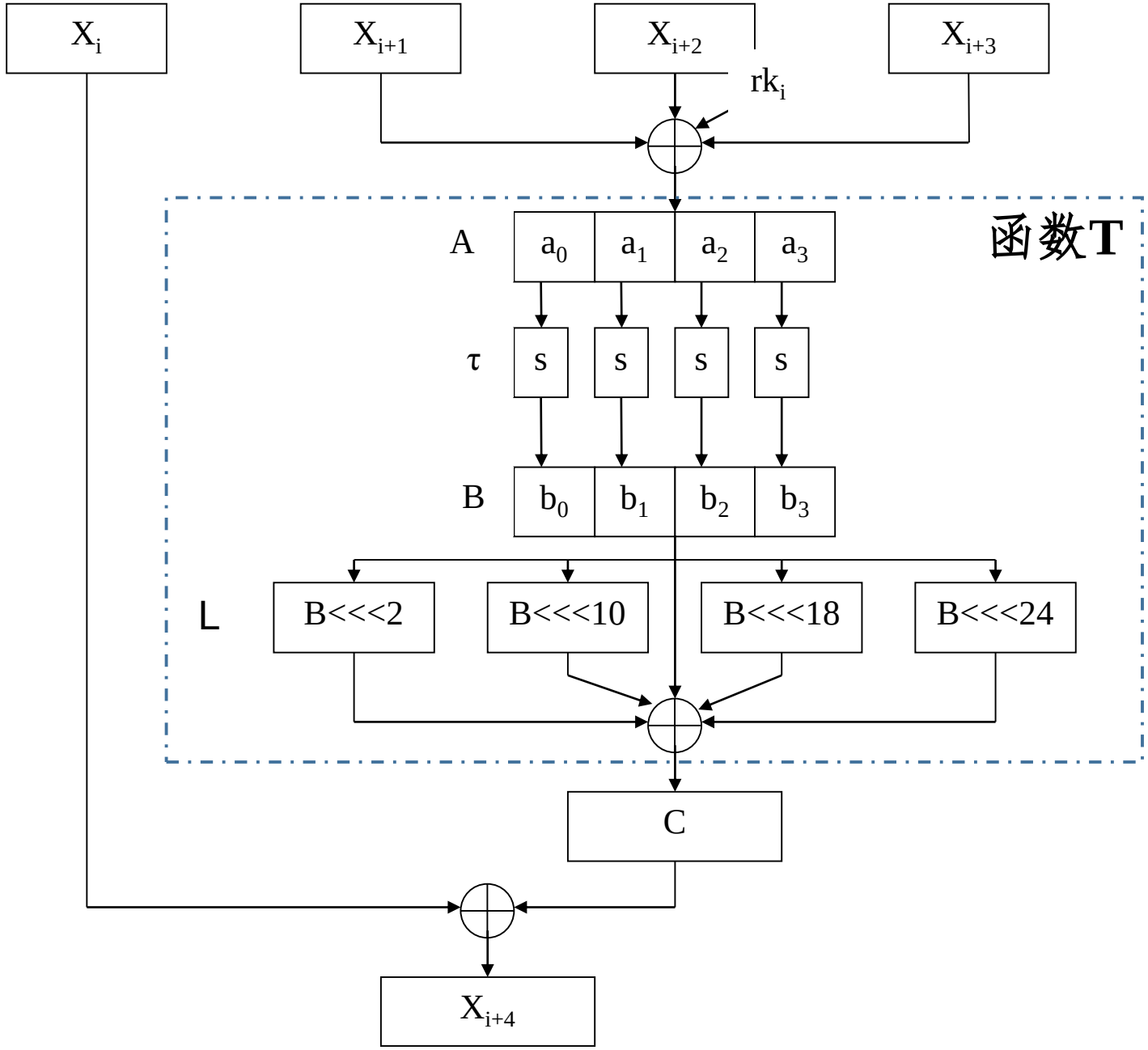
SM4 的轮函数

- 设输入为 $(X_i, X_{i+1}, X_{i+2}, X_{i+3}) \in (Z_2^{32})^4$ ，轮密钥为 $rk_i \in Z_2^{32}$，则轮函数为：

$$X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) = X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i), \quad i = 0,1,\cdots,31$$

- 其中 $T: Z_2^{32} \to Z_2^{32}$ 称为合成置换，是一个由非线性变换和一个线性变换复合而成的可逆变换，即

$$T(.) = L(\tau(.))$$


X_i
X_{i+1}
X_{i+2}
X_{i+3}
rk_i
函数T
A
a_0 a_1 a_2 a_3
τ
s s s s
B
b_0 b_1 b_2 b_3
L
B<<<2
B<<<10
B<<<18
B<<<24
C
X_{i+4}

SM4的S盒

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	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

SM4的S盒说明

- 非线性变换 τ 中所使用的S盒是一个具有很好密码学特性的、由8比特输入产生8比特输出的置换
- 在设计原理上，SMS4比AES的S盒设计多了一个仿射变换
- 即

$$y = A(Ax + B)^{-1} + B$$

- SMS4有很高的灵活性，所采用的S盒可以灵活地被替换，以应对突发性的安全威胁。算法的32轮迭代采用串行处理，这与AES中每轮使用代换和混淆并行地处理整个分组有很大不同。

SM4的加密算法和解密算法

- 设明文输入为 $(X_0, X_1, X_2, X_3) \in (Z_2^{32})^4$，密文为 $(Y_0, Y_1, Y_2, Y_3) \in (Z_2^{32})^4$，轮密钥为 $rk_i \in Z_2^{32}$。加密变换为：

$$X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) = X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i), \quad i = 0,1,\cdots,31$$

$$(Y_0, Y_1, Y_2, Y_3) = (X_{35}, X_{34}, X_{33}, X_{32})$$

- SM4算法的解密变换和加密变换结构相同，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 $(rk_{31}, rk_{30}, \cdots, rk_0)$ 。

SM4解密的合理性

$$X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) = X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i), \quad i = 0,1,\cdots,31$$

$$(Y_0, Y_1, Y_2, Y_3) = (X_{35}, X_{34}, X_{33}, X_{32})$$

$$X_{35} = X_{31} \oplus T(X_{34} \oplus X_{33} \oplus X_{32} \oplus rk_{31})$$

$$\begin{aligned} Y_4 &= F(Y_0, Y_1, Y_2, Y_3, rk_{31}) \\ &= Y_0 \oplus T(Y_1 \oplus Y_2 \oplus Y_3 \oplus rk_{31}) \\ &= X_{35} \oplus T(X_{34} \oplus X_{33} \oplus X_{32} \oplus rk_{31}) \\ &= X_{31} \oplus T(X_{34} \oplus X_{33} \oplus X_{32} \oplus rk_{31}) \oplus T(X_{34} \oplus X_{33} \oplus X_{32} \oplus rk_{31}) \\ &= X_{31} \end{aligned}$$

第三十讲 SM4算法

- SM4术语说明
- SM4轮函数
- SM4密钥扩展

SM4的密钥扩展算法

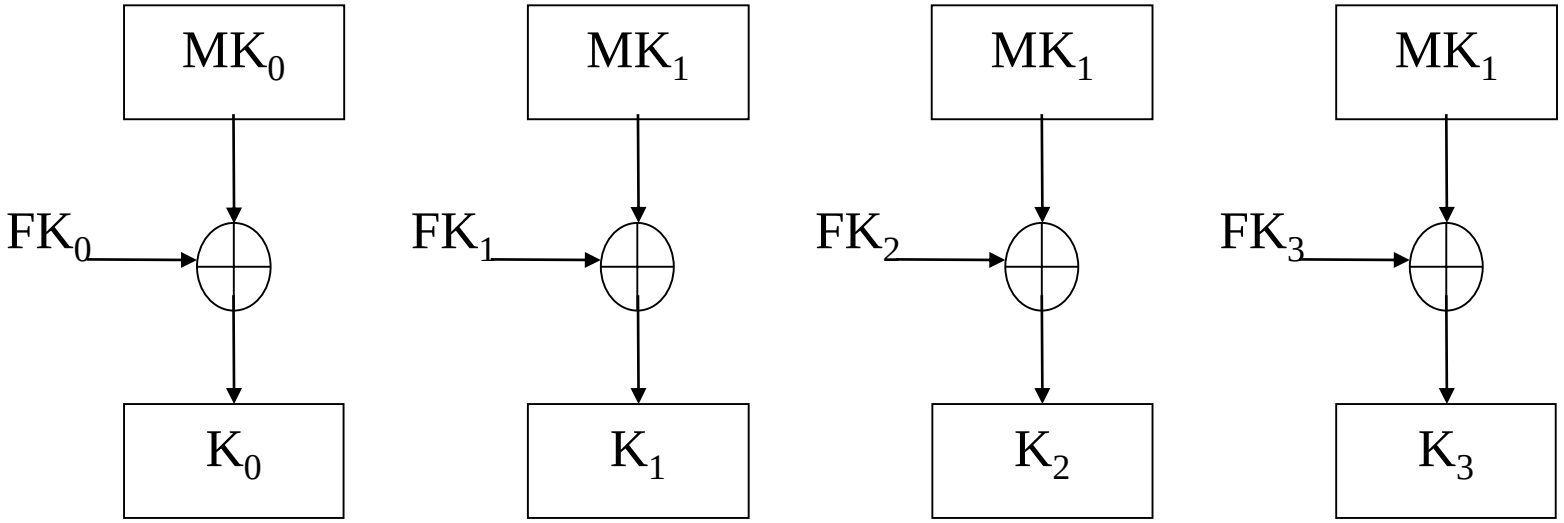
- 设加密密钥 $MK=(MK_0,MK_1,MK_2,MK_3)$，其中 MK_i 为字。
- 轮密钥为 $(rk_0,rk_1,\cdots,rk_{31})$ 。
- 轮密钥的生成方法具体为：

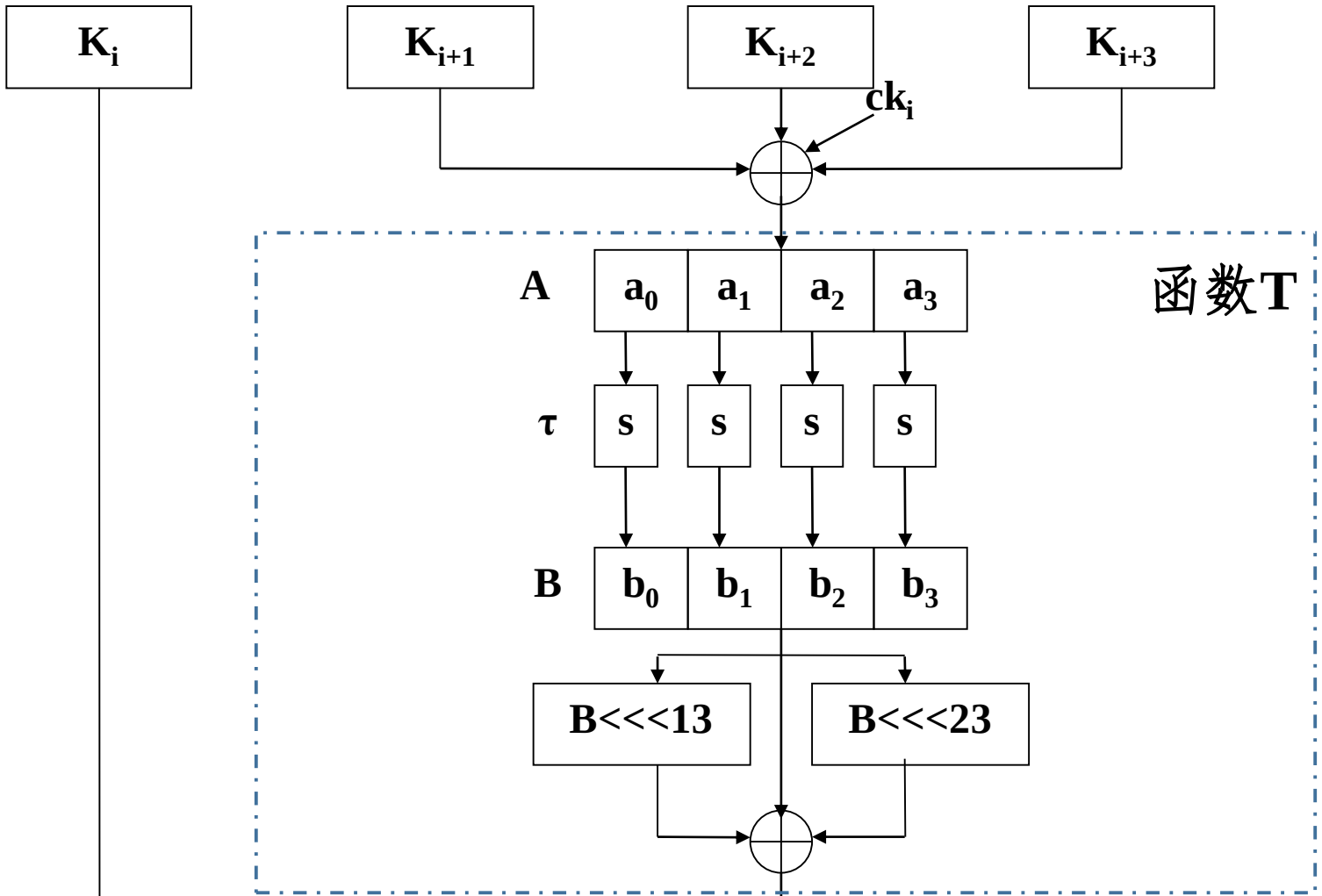
$$(K_0,K_1,K_2,K_3)=(MK_0\oplus FK_0,MK_1\oplus FK_1,MK_2\oplus FK_2,MK_3\oplus FK_3)$$

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

SM4的密钥扩展算法（续）

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





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

感 谢 聆 听!

xynie@uestc.edu.cn