SM4分组密码算法

1 符号

$\oplus$：32位异或

<<< i：32位循环左移 i 位

$\mathbb{Z}_2^n$：比特长度为n的二进制序列集合

2 密钥及密钥参量

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。

轮密钥表示为$(rk_0,rk_1,\ldots,rk_{31})$，其中$rk_i(i=0,\ldots,31)$为32比特字。轮密钥由密钥生成。

$FK=(FK_0,FK_1,FK_2,FK_3)$为系统参数，$CK=(CK_0,CK_1,CK_2,CK_3)$为固定参数，用于密钥扩展算法，其中$FK_i(i=0,1,2,3)$、$CK_i(i=0,1,2,3)$为字。

3 轮函数 F

3.1 轮函数结构

设输入为$(X_0,X_1,X_2,X_3)\in(Z_2^{32})^4$,轮密钥为$rk\in Z_2^{32}$,则轮函数F见式(1):

$$F(X_0,X_1,X_2,X_3,rk)=X_0\oplus T(X_1\oplus X_2\oplus X_3\oplus rk) \tag{1}$$

3.2 合成置换 T

$T:Z_2^{32}\rightarrow Z_2^{32}$是一个可逆变换，由非线性变换$\tau$和线性变换L复合而成，即$T(.)=L(\tau(.))$。

(a)非线性变换τ

τ由4个并行的S盒构成。

设输入为$A=(a_0,a_1,a_2,a_3)\in(Z_2^8)^4$,输出为$B=(b_0,b_1,b_2,b_3)\in(Z_2^8)^4$,则见式(2):

$$(b_0,b_1,b_2,b_3)=\tau(A)=(Sbox(a_0),Sbox(a_1),Sbox(a_2),Sbox(a_3)) \tag{2}$$

Sbox数据见下表：

	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

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
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

(b)线性变换L

非线性变换τ的输出是线性变换L的输入。设输入为$B \in Z_2^{32}$，则见式(3):

$$C = L(B) = B \oplus (B <<< 2) \oplus (B <<< 10) \oplus (B <<< 18) \oplus (B <<< 24) \quad (3)$$

4 算法描述

4.1 加密算法

本加密算法由32次迭代运算和1次反序变换R组成。

设明文输入为$(X_0, X_1, X_2, X_3) \in (Z_2^{32})^4$，密文输出为$(Y_0, Y_1, Y_2, Y_3) \in (Z_2^{32})^4$，轮密钥为$rk_i \in Z_2^{32}, i = 0, 1, 2, \ldots, 31$。加密算法的运算过程如下：

(a)32次迭代运算见式(4):

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

(b)反序变换见式(5):

$$(Y_0, Y_1, Y_2, Y_3) = R(X_{32}, X_{33}, X_{34}, X_{35}) = (X_{35}, X_{34}, X_{33}, X_{32}) \quad (5)$$

4.2 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。解密时，使用轮密钥序$(rk_{31}, rk_{30}, \ldots, rk_0)$。

4.3 密钥扩展算法

加密过程使用的轮密钥由加密密钥生成，其中加密密钥$MK = (MK_0, MK_1, MK_2, MK_3) \in (Z_2^{32})^4$，加密过程中的轮密钥生成方式见式(6)和式(7):

$$(K_0, K_1, K_2, K_3) = (MK_0 \oplus FK_0, MK_1 \oplus FK_1, MK_2 \oplus FK_2, MK_3 \oplus FK_3) \quad (6)$$

$$rk_i = K_{i+4} = K_i \oplus T'(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i), i = 0, 1, \ldots, 31 \quad (7)$$

式中：

a)T'是将6.2中合成置换 T 的线性变换 L 替换为 L'，见式(8):

$$L'(B) = B \oplus (B <<< 13) \oplus (B <<< 23) \quad (8)$$

b)系统参数FK的取值为:

$$FK_0 = (A3B1BAC6), FK_1 = (56AA3350), FK_2 = (677D9197), FK_3 = (B27022DC)$$

c)固定参数CK取值方法为：

$ck_{i,j}$为CK_i的第j字节$(i = 0, 1, \ldots, 31; j = 0, 1, 2, 3)$，即$CK_i = (ck_{i,0}, ck_{i,1}, ck_{i,2}, ck_{i,3}) \in (Z_2^8)^4$，则$ck_{i,j} = (4i + j)x7(mod256)$

固定参数$CK_i(i = 0, 1, \ldots, 31)$具体值为:

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。

解密密钥同加密密钥，解密使用的轮密钥由解密密钥生成，其轮密钥生成方法同加密过程的轮密钥生成方法。