



GM/T 0002

SM4 Block Cipher Algorithm

Cryptography Standardization
Technical Committee of China

Issued on 2012-03-21

Translated on 2024-10-30

Contents

1 Scope	1
2 Terms and Definitions	1
2.1 block length	1
2.2 key length	1
2.3 key expansion algorithm	1
2.4 rounds	1
2.5 word	1
2.6 S-box	1
3 Symbols and Acronyms	1
4 Algorithm Structure	1
5 Key and Key Parameters	2
6 Round Function F	2
6.1 Round Function Structure	2
6.2 Permutation T	2
7 Algorithm Description	3
7.1 Encryption	3
7.2 Decryption	3
7.3 Key Expansion	3
Annex A	5
(informative)	5
SM4 Numerical Examples	5
A.1 SM4 encryption	5
A.2 SM4 encryption 1 000 000 times	6

1 Scope

This document specifies the SM4 block cipher algorithm, including its structure and description, and also the corresponding numerical examples. This document applies to cryptographic applications using block cipher algorithms.

2 Terms and Definitions

The following terms and definitions are applied to this document.

2.1 block length

bit size of one block plaintext

2.2 key length

bit size of the key

2.3 key expansion algorithm

an algorithm that transforms the key into round keys

2.4 rounds

the number of round function iterations

2.5 word

a bit string of length 32

2.6 S-box

a permutation with 8-bit input and 8-bit output, represented as $Sbox(\cdot)$

3 Symbols and Acronyms

The following symbols and acronyms are applied to this document.

\oplus logical exclusive-or of 32-bit words

$\lll i$ left circular rotation by i bits

Z_2^n a set of n -bit strings

4 Algorithm Structure

SM4 is a block cipher algorithm. Its block length and key length are both of 128 bits. SM4 adopts an unbalanced Feistel structure and iterates its round functions for 32 times in both encryption and key expansion algorithm. The structure of decryption is the same as the encryption. But the round keys for decryption are in the reverse order of the round keys for encryption.

5 Key and Key Parameters

The 128-bit key is represented as $MK = (MK_0, MK_1, MK_2, MK_3)$, where MK_i ($i = 0, 1, 2, 3$) are 32-bit words.

The round keys are represented as $(rk_0, rk_1, \dots, rk_{31})$, where rk_i ($i = 0, \dots, 31$) are 32-bit words. The round keys are generated from the key via key expansion algorithm.

The system parameter is $FK = (FK_0, FK_1, FK_2, FK_3)$, and the fixed parameter is $CK = (CK_0, CK_1, \dots, CK_{31})$, where FK_i ($i = 0, 1, 2, 3$) and CK_i ($i = 0, \dots, 31$) are 32-bit words used in the key expansion algorithm.

6 Round Function F

6.1 Round Function Structure

Suppose the input to round function is $(X_0, X_1, X_2, X_3) \in (Z_2^{32})^4$ and the round key is $rk \in Z_2^{32}$, then F can be represented as:

$$F(X_0, X_1, X_2, X_3, rk) = X_0 \oplus T(X_1 \oplus X_2 \oplus X_3 \oplus rk).$$

6.2 Permutation T

$T: Z_2^{32} \rightarrow Z_2^{32}$ is an invertible transformation, composed of a nonlinear transformation τ and a linear transformation L . That is, $T(\cdot) = L(\tau(\cdot))$.

(1) Nonlinear transformation τ

τ is composed of 4 S-boxes in parallel. Suppose $A = (a_0, a_1, a_2, a_3) \in (Z_2^8)^4$ is input to τ , and $B = (b_0, b_1, b_2, b_3) \in (Z_2^8)^4$ is the corresponding output, then

$$(b_0, b_1, b_2, b_3) = \tau(A) = (Sbox(a_0), Sbox(a_1), Sbox(a_2), Sbox(a_3)).$$

The S-box is as follows:

		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

Note: substitution values for the byte xy (in hexadecimal format), e.g. when the input is 'EF', then the output is the value in row E and column F, i.e. $Sbox(EF) = 84$.

(2) Linear transformation L

The output from the nonlinear transformation τ is the input to the linear transformation L . Suppose the input to L is $B \in Z_2^{32}$, and the corresponding output is $C \in Z_2^{32}$, then

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

7 Algorithm Description

7.1 Encryption

The encryption algorithm first iterates the round function F for 32 times, and then applies the reverse transformation R in the end.

Suppose its input plaintext is $(X_0, X_1, X_2, X_3) \in (Z_2^{32})^4$, the corresponding output ciphertext is $(Y_0, Y_1, Y_2, Y_3) \in (Z_2^{32})^4$, and the round keys are $rk_i \in Z_2^{32}, i = 0, 1, \dots, 31$, then the process of the encryption algorithm is as follows:

(1) 32-round iterated operation: $X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i), i = 0, 1, \dots, 31$.

(2) The reverse transformation:

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

7.2 Decryption

The structure of the decryption transformation is the same as the encryption transformation. The only difference is the order of the round keys. In decryption, the round keys are used in the order of $(rk_{31}, rk_{30}, \dots, rk_0)$.

7.3 Key Expansion

The round keys in this algorithm are generated from the key via the key expansion algorithm.

Suppose the key is $MK = (MK_0, MK_1, MK_2, MK_3) \in (Z_2^{32})^4$, then the round keys are generated as follows:

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

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

where

(1) T' replaces the linear transformation L in permutation T by L' : $L'(B) = B \oplus (B \lll 13) \oplus (B \lll 23)$.

(2) The system parameter FK is:

$$FK_0 = A3B1BAC6, FK_1 = 56AA3350,$$

$$FK_2 = 677D9197, FK_3 = B27022DC.$$

(3) The fixed parameter CK is used in the key expansion algorithm. Suppose $ck_{i,j}$ is the j -th byte of $CK_i (i = 0, 1, \dots, 31, j = 0, 1, 2, 3)$, i.e. $CK_i = (ck_{i,0}, ck_{i,1}, ck_{i,2}, ck_{i,3}) \in (Z_2^8)^4$, then $ck_{i,j} = (4i + j) \times 7 \pmod{256}$. To be specific, the values of the fixed parameters $CK_i (i = 0, 1, \dots, 31)$ are:

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.

Annex A

(informative)

SM4 Numerical Examples

A.1 SM4 encryption

This part is an example of encrypting a plaintext using the SM4 block cipher algorithm.

Input plaintext: 01 23 45 67 89 AB CD EF FE DC BA 98 76 54 32 10.

Input key: 01 23 45 67 89 AB CD EF FE DC BA 98 76 54 32 10.

The round keys and the values of the output of each round:

rk_0 =F12186F9	X_4 =27FAD345
rk_1 =41662B61	X_5 =A18B4CB2
rk_2 =5A6AB19A	X_6 =11C1E22A
rk_3 =7BA92077	X_7 =CC13E2EE
rk_4 =367360F4	X_8 =F87C5BD5
rk_5 =776A0C61	X_9 =33220757
rk_6 =B6BB89B3	X_{10} =77F4C297
rk_7 =24763151	X_{11} =7A96F2EB
rk_8 =A520307C	X_{12} =27DAC07F
rk_9 =B7584DBD	X_{13} =42DD0F19
rk_{10} =C30753ED	X_{14} =B8A5DA02
rk_{11} =7EE55B57	X_{15} =907127FA
rk_{12} =6988608C	X_{16} =8B952B83
rk_{13} =30D895B7	X_{17} =D42B7C59
rk_{14} =44BA14AF	X_{18} =2FFC5831
rk_{15} =104495A1	X_{19} =F69E6888
rk_{16} =D120B428	X_{20} =AF2432C4
rk_{17} =73B55FA3	X_{21} =ED1EC85E
rk_{18} =CC874966	X_{22} =55A3BA22
rk_{19} =92244439	X_{23} =124B18AA
rk_{20} =E89E641F	X_{24} =6AE7725F
rk_{21} =98CA015A	X_{25} =F4CBA1F9

$rk_{22}=C7159060$	$X_{26}=1DCDFA10$
$rk_{23}=99E1FD2E$	$X_{27}=2FF60603$
$rk_{24}=B79BD80C$	$X_{28}=EFF24FDC$
$rk_{25}=1D2115B0$	$X_{29}=6FE46B75$
$rk_{26}=0E228AEB$	$X_{30}=893450AD$
$rk_{27}=F1780C81$	$X_{31}=7B938F4C$
$rk_{28}=428D3654$	$X_{32}=536E4246$
$rk_{29}=62293496$	$X_{33}=86B3E94F$
$rk_{30}=01CF72E5$	$X_{34}=D206965E$
$rk_{31}=9124A012$	$X_{35}=681EDF34$

The output ciphertext: 68 1E DF 34 D2 06 96 5E 86 B3 E9 4F 53 6E 42 46.

A.2 SM4 encryption 1 000 000 times

Given inputs (plaintext and key), output (ciphertext) after encryption iteratively 1 000 000 times is described.

Input plaintext: 01 23 45 67 89 AB CD EF FE DC BA 98 76 54 32 10.

Input key: 01 23 45 67 89 AB CD EF FE DC BA 98 76 54 32 10.

The output ciphertext: 59 52 98 C7 C6 FD 27 1F 04 02 F8 04 C3 3D 3F 66.