ISO/IEC JTC 1/SC 27/WG 2 N1460

REPLACES:

ISO/IEC JTC 1/SC 27/WG 2

Cryptography and security mechanisms

Convenorship: JISC (Japan)

Document type:	Working Draft Amendment Text
Title:	**First Working Draft 18033-3/AMD2 – Encryption algorithms – Part 3: Block ciphers – Amendment 2**
Status:	In accordance with Recommendations 3 and 10 (contained in SC 27/WG 2 N1500) of the 54th SC 27/WG 2 meeting at Hamilton, New Zealand on 18th – 22nd April, 2017, this document is being circulated to experts of National Bodies and liaison organizations as a call for contributions closing on **2017-09-15**. **PLEASE submit your contribution to the hereby attached document by the following operations:** **Open http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg2 then find the project, to which you want to input your contribution, in the "Consultation" window and click it. If log-in screen appears, log in using your ID and PW. If log-in is successful, project file opens. Click "Cast Vote" button at the top right corner, then you can input your contribution. After input, click "Cast vote" button at the bottom of the screen.**
Date of document:	2017-06-13
Source:	Project Editor (Limin Liu)
Expected action:	**COMM**
Action due date:	**2017-09-15**
No. of pages:	1 + 10
Email of secretary:	sc27wg2-secretary@ipa.go.jp
Committee URL:	http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg2

© ISO/IEC 2017 – All rights reserved

ISO/IEC JTC 1/SC 27 N 1460

Date: 2017-06-13

N/A

ISO/IEC JTC 1/SC 27/WG 2

Secretariat: DIN

Information technology - Security techniques — Encryption algorithms — Part 3: Block Ciphers

Technologies de l'information — Techniques de sécurité — Algorithmes de chiffrement — Partie 3: Chiffrement par blocs— Amendment 2

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

— Amendment 2: SM4

Document type: International Standard
Document subtype: Amendment
Document stage: (20) Preparatory
Document language: E

C:\Users\PZ46184\Desktop\ISO-IEC_18033-3_A2_(E)_1stWD_20170613.docx STD Version 2.8f

Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

[Indicate the full address, telephone number, fax number, telex number, and electronic mail address, as appropriate, of the Copyright Manager of the ISO member body responsible for the secretariat of the TC or SC within the framework of which the working document has been prepared.]

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

© ISO/IEC 2017 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC XXX

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

ISO XXXX consists of the following parts. [Add information as necessary.]

© ISO/IEC 2017 – All rights reserved

Information technology - Security techniques — Encryption algorithms — Part 3: Block Ciphers

— Amendment 2: SM4

AA: Page 1, 1:

Change the following sentence of paragraph 1:

A total of seven different block ciphers are defined.

to:

A total of eight different block ciphers are defined.

BB: Page 1, 1, Table 1:

Replace Table 1 with the following:

Block length	Algorithm name (see #)	Key length
64 bits	TDEA (4.2)	128 or 192 bits
	MISTY (4.3)	128 bits
	CAST-128 (4.4)	
	HIGHT (4.5)	
128 bits	AES (5.2)	128, 192 or 256 bits
	Camelia (5.3)	
	SEED (5.4)	128 bits
	SM4 (5.5)	

CC: Page 24, 5.1:

Change the following sentence of paragraph 1:

In this clause, three 128-bit block ciphers are specified; AES in 5.2, Camellia in 5.3, and SEED in 5.4.

to:

© ISO/IEC 2017 – All rights reserved

In this clause, four 128-bit block ciphers are specified; AES in 5.2, Camellia in 5.3, SEED in 5.4, and SM4 in 5.5.

DD: Page 51, After 5.4.5:

Add the following new 5.5 thru 5.4.5 to the end of 5.4.5:

5.5 SM4

5.5.1 The SM4 algorithm

The SM4 block cipher is a symmetric block cipher that can process data blocks of 128 bits, using a cipher key with length of 128 bits under 32 rounds.

5.5.2 SM4 encryption

The transformation of a 128-bit block P into a 128-bit block C is defined as follows (X_i (i = 0,1,2,3) are variables with 32-bit length, rk_i (i = 0,1,···,31) are subkeys with 32-bit length):

(1) $P = X_0 \,||\, X_1 \,||\, X_2 \,||\, X_3$

(2) for i = 0 to 31:

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

(3) $C = X_{35} \,||\, X_{34} \,||\, X_{33} \,||\, X_{32}$

5.5.3 SM4 decryption

The decryption operation is identical in operation to encryption, except that the rounds (and therefore the subkeys) are used in reverse order.

5.5.4 SM4 functions

5.5.4.1 Function F

The function F is used for both encryption and decryption. The function F is defined as follows:

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

where X_i (i = 0,1,2,3) and rk are 32 bits wide, T is a permutation defined in 5.5.4.2.

5.5.4.2 Permutation T and T'

The permutation T is used both for encryption and decryption. T is a composition of a nonlinear transformation τ and a linear transformation L, that is $\mathrm{T}(\cdot) = \mathrm{L}(\tau(\cdot))$.

The permutation T' is used for key schedule. T' is a composition of a nonlinear transformation τ and a linear transformation L', that is $\mathrm{T}'(\cdot) = \mathrm{L}'(\tau(\cdot))$.

5.5.4.2.1 Nonlinear transformation τ

The nonlinear transformation τ is defined as follows (a_i (i = 0,1,2,3) are bytes and S is a S-box defined in 5.5.4.2.3):

© ISO/IEC 2017 – All rights reserved

$$\tau(a_0 \parallel a_1 \parallel a_2 \parallel a_3) = \mathrm{S}(a_0) \parallel \mathrm{S}(a_1) \parallel \mathrm{S}(a_2) \parallel \mathrm{S}(a_3).$$

5.5.4.2.2 Linear transformation L and L’

The linear transformation L is defined as follows (B is a variable with 32-bit length):

$$\mathrm{L}(B) = B \oplus (B{<}{<}{<}2) \oplus (B{<}{<}{<}10) \oplus (B{<}{<}{<}18) \oplus (B{<}{<}{<}24).$$

The linear transformation L’ is defined as follows (B is a variable with 32-bit length):

$$\mathrm{L}'(B) = B \oplus (B{<}{<}{<}13) \oplus (B{<}{<}{<}23).$$

5.5.4.2.3 S-box S

The S-box S used in the transformation τ is presented in hexadecimal form in Table 17.

Table 17 – SM4 S-box

	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	0a	44	13	26	49	86	06	99
2	9c	42	50	f4	91	ef	98	7a	33	54	0b	43	0e	cf	ac	62
3	e4	b3	1c	a9	c9	08	e8	95	80	df	94	0f	75	8f	3f	a6
4	47	07	a7	fc	f3	73	17	ba	83	59	3c	19	f6	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	0e	bf	8a	d2	40	c7	38	b5	a3	f7	f2	ce	f9	61	15	a1
9	e0	ae	5d	a4	9b	34	1a	55	0a	93	32	30	f5	8c	b1	e3
a	1d	f6	e2	2e	82	66	ca	60	c0	29	23	ab	00	53	4e	6f
b	d5	db	37	45	de	fd	8e	2f	03	ff	6a	72	06	6c	5b	51
c	8d	1b	0a	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	0d	cb	39	48

5.5.5 SM4 key schedule

The key scheduling part accepts a 128-bit master key $MK = MK_0 \parallel MK_1 \parallel MK_2 \parallel MK_3$, and yields 32 subkeys, as shown below.

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

(2) for i = 0 to 31:

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

The constants FK_i (i = 0,1,2,3) are as follows (in hexadecimal form):

FK_0 = a3b1bac6, FK_1 = 56aa3350, FK_2 = 677d9197, FK_3 = b27022dc.

© ISO/IEC 2017 – All rights reserved

The constants CK_i (i = 0,1,···,31) are defined as follows. Suppose $CK_i = ck_{i,0} \| ck_{i,1} \| ck_{i,2} \| ck_{i,3}$, where $ck_{i,j}$ are bytes, and $ck_{i,j} = (4i+j) \times 7 \pmod{256}$ (i = 0,1,···,31, j = 0,1,2,3).

The values of CK_i (i = 0,1,···,31) are (in hexadecimal form):

```
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.
```

EE: Page 60, Annex B:

Insert the following line after id-bc128-seed:

```
id-bc128-sm4 OID ::= {id-bc128 sm4(4)}
```

FF: Page 61, Annex B:

Change the following line of code:

```
 { OID id-bc128-seed  PARMS KeyLength },
```

to:

```
{ OID id-bc128-seed  PARMS KeyLength } |

{ OID id-bc128-sm4  PARMS KeyLength },
```

GG: Page 76, After D.8:

Add the following new D.9 thru D.8 to the end of D.8:

D.9 SM4 test vectors

D.9.1 SM4 encryption

Given inputs (plaintext and key), output (ciphertext and subkeys) and intermediate values are described.

 © ISO/IEC 2017 – All rights reserved

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 subkeys and the values of the output of each round:

rk[0] = `f12186f9` X[0] = `27fad345`

rk[1] = `41662b61` X[1] = `a18b4cb2`

rk[2] = `5a6ab19a` X[2] = `11c1e22a`

rk[3] = `7ba92077` X[3] = `cc13e2ee`

rk[4] = `367360f4` X[4] = `f87c5bd5`

rk[5] = `776a0c61` X[5] = `33220757`

rk[6] = `b6bb89b3` X[6] = `77f4c297`

rk[7] = `24763151` X[7] = `7a96f2eb`

rk[8] = `a520307c` X[8] = `27dac07f`

rk[9] = `b7584dbd` X[9] = `42dd0f19`

rk[10] = `c30753ed` X[10] = `b8a5da02`

rk[11] = `7ee55b57` X[11] = `907127fa`

rk[12] = `6988608c` X[12] = `8b952b83`

rk[13] = `30d895b7` X[13] = `d42b7c59`

rk[14] = `44ba14af` X[14] = `2ffc5831`

rk[15] = `104495a1` X[15] = `f69e6888`

rk[16] = `d120b428` X[16] = `af2432c4`

rk[17] = `73b55fa3` X[17] = `ed1ec85e`

rk[18] = `cc874966` X[18] = `55a3ba22`

rk[19] = `92244439` X[19] = `124b18aa`

rk[20] = `e89e641f` X[20] = `6ae7725f`

rk[21] = `98ca015a` X[21] = `f4cba1f9`

rk[22] = `c7159060` X[22] = `1dcdfa10`

rk[23] = `99e1fd2e` X[23] = `2ff60603`

rk[24] = `b79bd80c` X[24] = `eff24fdc`

rk[25] = `1d2115b0` X[25] = `6fe46b75`

© ISO/IEC 2017 – All rights reserved

rk[26] = `0e228aeb` X[26] = `893450ad`

rk[27] = `f1780c81` X[27] = `7b938f4c`

rk[28] = `428d3654` X[28] = `536e4246`

rk[29] = `62293496` X[29] = `86b3e94f`

rk[30] = `01cf72e5` X[30] = `d206965e`

rk[31] = `9124a012` X[31] = `681edf34`

The output ciphertext: `68 1e df 34 d2 06 96 5e 86 b3 e9 4f 53 6e 42 46`.

D.9.2 SM4 encryption 1000000 times

Given inputs (plaintext and key), output (ciphertext) after encryption iteratively 1000000 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`.

Output ciphertext: `59 52 98 c7 c6 fd 27 1f 04 02 f8 04 c3 3d 3f 66`.

HH: Page 77, Annex E, Feature table:

Insert the following item after Korean e-government algorithm:

8	SM4 [13]	● High speed encryption with compact hardware	● Chinese standard (GM/T 0002-2012)

II: Page 78, Bibliography:

Add the following to the end of Bibliography:

[13] GM/T 0002-2012, Block Cipher Algorithm SM4, 2012 (In Chinese).

------ End of Amendment ---

 © ISO/IEC 2017 – All rights reserved