INTERNATIONAL STANDARD

ISO/IEC 18033-3

Second edition
2010-12-15

AMENDMENT 1
2021-06

Information technology — Security techniques — Encryption algorithms —

Part 3: **Block ciphers**

AMENDMENT 1: SM4

Technologies de l'information — Techniques de sécurité — Algorithmes de chiffrement —

Partie 3: Chiffrement par blocs

AMENDEMENT 1: SM4

Reference number
ISO/IEC 18033-3:2010/Amd.1:2021(E)

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.

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) or the IEC list of patent declarations received (see patents.iec.ch).

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

For an explanation of the voluntary nature of standards, 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 www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Information technology — Security techniques — Encryption algorithms —

Part 3:
Block ciphers

AMENDMENT 1: SM4

Clause 1

In the first paragraph, replace "seven different block ciphers" with "eight different block ciphers".

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
	Camellia (5.3)	
	SEED (5.4)	128 bits
	SM4 (5.5)	

5.1

Replace the sentence with the following:

> 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.

5.5

Add new subclause 5.5 as follows:

5.5 SM4

5.5.1 The SM4 algorithm

The SM4 algorithm 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

A 128-bit block P is transformed into a 128-bit block C using the following procedure, where for $i = 0, 1, 2, 3$ the X_i are 32-bit variables, and for $i = 0, 1, \ldots, 31$ the rk_i are 32-bit subkeys:

(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 to the encryption operation, except that the rounds (and therefore the subkeys) are used in reverse order:

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

(2) for i = 31 to 0:

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

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

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 bit strings of length 32, T is a permutation defined in 5.5.4.2.

5.5.4.2 Permutation T and T'

5.5.4.2.1 General

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 T(·) = L(τ(·)). The permutation T' is used for the key schedule. T' is a composition of the nonlinear transformation τ and a linear transformation L', that is T'(·) = L'(τ(·)). T, T', L, L' and τ are all transformations on 32-bit strings.

5.5.4.2.2 Nonlinear transformation τ

The nonlinear transformation τ is defined as follows, where for i = 0, 1, 2, 3 the a_i are bytes and S is an S-box defined in 5.5.4.2.4:

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

5.5.4.2.3 Linear transformation L and L'

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

$$\mathrm{L}(B) = B \oplus (B{<}{<}{<}_2) \oplus (B{<}{<}{<}_{10}) \oplus (B{<}{<}{<}_{18}) \oplus (B{<}{<}{<}_{24}).$$

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

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

5.5.4.2.4 S-box S

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

