www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Translated English of Chinese Standard: GM/T 0002-2012

www.ChineseStandard.net → Buy True-PDF → Auto-delivery.

Sales@ChineseStandard.net

GM

CRYPTOGRAPHIC INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80
Record no.: 36825-2012

GM/T 0002-2012

SM4 block cipher algorithm

SM4 分组密码算法

Issued on: March 21, 2012 **Implemented on: March 21, 2012**

Issued by: State Cryptography Administration of the People's Republic of China

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Table of Contents

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

SM4 block cipher algorithm

1 Scope

This Standard specifies the algorithm structure and algorithm description of SM4 block cipher algorithm and gives examples for computation.

This Standard applies to the requirements for the use of block cipher algorithm in cryptographic applications.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1

block length

Number of bits of an information block.

2.2

key length

Number of bits of key.

2.3

key expansion algorithm

Arithmetic unit in which a key is converted into a round key.

2.4

rounds

Number of iterations of round function.

2.5

word

Block (string) of 32-bit length.

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

2.6

S-box

S-box is the fixed replacement of 8-bit input with 8-bit output, expressed as Sbox(.).

3 Symbols and abbreviations

$\oplus$ 32-bit exclusive-OR operation

$<<<i$ Left shift of 32-bit words by *i* bits

4 Algorithm structure

SM4 cipher algorithm is a block algorithm. The block length of the algorithm is 128 bits; the key length is 128 bits. Both encryption algorithm and key expansion algorithm are of a 32-round nonlinear iteration structure. Data decryption and data encryption are of the same algorithm structure, but the use orders of round keys are opposite. A decryption round key is the reverse order of an encryption round key.

5 Key and key parameters

The length of an encryption key is 128 bits, expressed as $MK = (MK_0, MK_1, MK_2, MK_3)$, where MK_i (i = 0, 1, 2, 3) is a word.

Round keys are expressed as (rk_0, Fk_1, FK_2, FK_3), where rk_i (i = 0, …, 31) is a 32-bit word. Round keys are generated by encryption keys.

$FK = (FK_0, FK_1, FK_2, FK_3)$, a system parameter, and $CK = (CK_0, CK_1, \ldots, CK_{31})$, a fixed parameter, are used for key expansion algorithm, where FK_i (i =0, …, 3) and CK_i (i = 0, …, 31) are words.

6 Round function

6.1 Structure of round function

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

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

This is an excerpt of the PDF (Some pages are marked off intentionally)

Full-copy PDF can be purchased from 1 of 2 websites:

1. https://www.ChineseStandard.us

- SEARCH the standard ID, such as GB 4943.1-2022.
- Select your country (currency), for example: USA (USD); Germany (Euro).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Tax invoice can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with download links).

2. https://www.ChineseStandard.net

- SEARCH the standard ID, such as GB 4943.1-2022.
- Add to cart. Only accept USD (other currencies - https://www.ChineseStandard.us).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with PDFs attached, invoice and download links).

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

About Us (Goodwill, Policies, Fair Trading…): https://www.chinesestandard.net/AboutUs.aspx

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: https://www.linkedin.com/in/waynezhengwenrui/

------ The End ------