ICS 35.040
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 32907-2016

Information security technology - SM4 block cipher algorithm

信息安全技术 SM4 分组密码算法

Issued on: August 29, 2016 **Implemented on: March 1, 2017**

Issued by: General Administration of Quality Supervision, Inspection and Quarantine;
Standardization Administration of PRC..

Table of Contents

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

Please note that certain contents of this document may involve patents. The issuing agency of this document is not responsible for identifying these patents.

This standard was proposed by the State Cryptography Administration.

This standard shall be under the jurisdiction of the National Information Security Standardization Technical Committee (SAC/TC 260).

Drafting organizations of this standard: Data and Communication Protection Research and Education Center of Chinese Academy of Sciences, Commercial Cryptographic Testing Center of National Cryptography Administration, Beijing Institute of Information Science and Technology.

The main drafters of this standard: Lv Shuwang, Li Dawei, Deng Kaiyong, Zhang Chao, Luo Peng, Zhang Zhong, Dong Fang, Mao Yingying, Liu Zhenhua.

1 Scope

This standard specifies the algorithm structure and algorithm description of the SM4 block cipher algorithm; gives examples of operations.

This standard applies to the realization, testing, application of block cipher algorithms in commercial cipher products.

2 Terms and definitions

The following terms and definitions apply to this document.

The number of bits in an information packet.

The number of bits in the key.

The arithmetic unit that transforms the key into a round key.

The number of iterations of the round function.

Also known as sub-key, which is the key used in each round of iterative block cipher and derived from the input key using a key arrangement algorithm.

A group (string) with a length of 32 bits.

The S box is a fixed 8-bit input and 8-bit output replacement, denoted as Sbox(.).

3 Symbols and abbreviations

4 Algorithm structure

The SM4 cipher algorithm is a block algorithm. The block length of this algorithm is 128 bits; the key length is 128 bits. Both the encryption algorithm and the key expansion algorithm adopt a nonlinear iterative structure; the number of operation rounds is 32 rounds. The algorithm structure of data decryption and data encryption is the same, but the use order of the round key is reversed. The decryption round key is the reverse order of the encryption round key.

5 Key and key parameters

FK = (FK0, FK1, FK2, FK3) is the system parameter, CK = (CK0, CK1, ..., CK31) is the fixed parameter, which is used for the key expansion algorithm, where FKi (i = 0, ..., 3), CKi (i = 0, ..., 31) is a word.

6 Round function F

6.1 Round function structure

Suppose the input is (X0, X1, X2, X3) □ ( )4, meanwhile the round key is rk □ , then the round function F is as shown in formula (1):

6.2 Synthetic replacement T

T: → is a reversible transformation, which is a composite of nonlinear transformation τ and linear transformation L, that is, T(.) = L(τ(.)). τ consists of 4 parallel S boxes. Where, Sbox data are as shown in Table 1.

7 Algorithm description

7.1 Encryption algorithm

This encryption algorithm consists of 32 iterations and 1 reverse transformation R.

Suppose the plaintext input is (X0, X1, X2, X3) □ ( )4, the cipher text output is (Y0, Y1, Y2, Y3) □ ( )4, the round key is rki □ , i = 0, 1, 2, …, 31.

The operation process of the encryption algorithm is as follows:

a) For 32 iterations, see formula (4):

See Appendix A for an example of the encryption operation process.

7.2 Decryption algorithm

The decryption transformation of this algorithm has the same structure as the encryption transformation, the only difference is the use order of the round keys. When decrypting, use the round key sequence (rk31, rk30, ..., rk0).