ICS 35.040

L 80

GB

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 01, 2017**

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

Standardization Administration of PRC.

Table of Contents

Foreword 3
1 Scope 4
2 Terms and definitions 4
3 Symbols and abbreviations 5
4 Algorithm structure 5
5 Key and key parameters 5
6 Round function F 6
6.1 Round function structure 6
6.2 Synthetic replacement T 6
7 Algorithm description 7
7.1 Encryption algorithm 7
7.2 Decryption algorithm 8
7.3 Key expansion algorithm 8
Appendix A (Informative) Calculation example 10
A.1 Example 1 10
A.2 Example 2 12

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.

Information security technology -

SM4 block cipher algorithm

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.

2.1

Block length

The number of bits in an information packet.

2.2

Key length

The number of bits in the key.

2.3

Key expansion algorithm

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

2.4

Rounds

The number of iterations of the round function.

2.5

Round key