ICS 35.040

L 80

GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

GB/T 32905-2016

Information security techniques - SM3 cryptographic hash algorithm

信息安全技术 SM3 密码杂凑算法

Issued on: August 29, 2016 **Implemented on: March 01, 2017**

Issued by: General Administration of Quality Supervision, Inspection and Quarantine;
Standardization Administration of the People's Republic of China.

Table of Contents

Foreword

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

This Standard was proposed by State Cryptography Administration.

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

The drafting organizations of this Standard: Tsinghua University, Commercial Cryptography Testing Center of State Cryptography Administration, PLA Information Engineering University, Data Assurance & Communications Security Center, Chinese Academy of Sciences.

The drafters of this Standard: Wang Xiaoyun, Li Zheng, Wang Yongchuan, Yu Hongbo, Xie Yongquan, Zhang Chao, Luo Peng, Lv Shuwang.

Information security techniques - SM3 cryptographic hash algorithm

1 Scope

This Standard specifies the calculation method and calculation steps of SM3 cryptographic hash algorithm, and gives examples of calculations.

This Standard applies to digital signature and verification in commercial cryptographic applications, the generation and verification of message authentication codes, and the generation of random numbers. It can meet the security requirements of a variety of cryptographic applications.

2 Terms and definitions

The following terms and definitions are applicable to this document.

2.1 Bit string

A sequence of binary digits that has the value of 0 or 1.

2.2 Big-endian

A representation format of data in memory, which stipulates that the left side is the most significant bit and the right side is the least significant bit. That is, the high-order byte of the number is placed at the low address of the memory, and the low-order byte of the number is placed at the high address of the memory.

2.3 Message

Any bit string of finite length. In this Standard, message is used as the input data of the hash algorithm.

2.4 Hash value

The output message digest (bit string) when the hash algorithm is applied to a message.

2.5 Word

A group (string) whose length is 32 bits.

3 Symbols

The following symbols apply to this document.

ABCDEFGH: 8 word registers or concatenation of their values

$B^{(i)}$: the i^{th} message group

CF: compression function

FF_j: boolean function; take different expressions as j changes

GG_j: boolean function; take different expressions as j changes

IV: initial value; it is used to determine the initial state of the compression function register

P_0: permutation function in compression function

P_1: permutation function in message expansion

T_j: algorithm constant; take different values as j changes

m: message

m': filled message

mod: modular arithmetic

n: number of message groups

∧: 32-bit AND operation

∨: 32-bit OR operation

⊕: 32-bit exclusive OR operation

¬: 32-bit NOT operation

+: mod 2^{32} bit arithmetic addition operation

<<<k: 32-bit cyclic left shift k-bit operation

←: left assignment operator

4 Constants and functions

4.1 Initial value