ICS 35.040
CCS L 80

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 1, 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.

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

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.

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.

FFj: boolean function; take different expressions as j changes GGj: boolean function; take different expressions as j changes IV: initial value; it is used to determine the initial state of the compression function register P0: permutation function in compression function P1: permutation function in message expansion Tj: 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 232 bit arithmetic addition operation <<<k: 32-bit cyclic left shift k-bit operation ←: left assignment operator

4 Constants and functions

4.1 Initial value

4.2 Constant

4.3 Boolean function

Where X, Y, Z are words

4.4 Permutation function

5 Algorithm description

5.1 Overview

The input of SM3 cryptographic hash algorithm is a message m whose length is l (l<264) bits. After filling and iterative compression, a hash value is generated. The output length of the hash value is 256 bits. See Appendix A for calculation examples.

5.2 Filling

Assuming that the length of the message m is l bits, first add the bit “l” to the end of the message; then, add k “0”s. K is the smallest non-negative integer that satisfies l+1+k≡448 (mod 512). Then, add a 64-bit bit string, which is a binary representation of length l. The bit length of the filled message m’ is a multiple of 512.

5.3 Iterative compression

5.3.1 Iterative process

5.3.2 Message extension

Extend the message group B(i) by the following method to generate 132 message words W0, W1, … W67, W'0, W'1, … W'63, which are used for the compression function CF:

5.3.3 Compression function

5.4 Output hash value

The output 256-bit hash value y = ABCDEFGH.