GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80
RECORD NO.: 36831-2012

GM/T 0004-2012

SM3 cryptography hash algorithm

SM3 密码杂凑算法

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

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

Table of Contents

Foreword

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The issuer of this document shall not be held responsible for identifying any or all such patent rights.

Annex A to this Standard is informative.

This Standard was proposed by and shall be under the jurisdiction of the State Cryptography Administration.

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

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

SM3 cryptography hash algorithm

1 Scope

This Standard specifies the calculation method and calculation procedures of SM3 cryptography hash algorithm; and gives operational examples.

This Standard applies to the digital signature-verification in commercial cryptography applications, the generation-verification of message authentication codes, and the generation of random numbers, which can satisfy the security requirements for multiple cryptography applications. Meanwhile, this Standard can also provide security product manufacturers with standard positioning for products and technologies as well as references for standardization, so as to improve the creditability and interoperability of security products.

2 Terms and conventions

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

2.1

bit string

Digital sequence of binary number 0 or 1.

2.2

big-endian

A representation format of data in memory, whose significant bits are specified to be on the left and less significant bits on the right. The high-order bytes of numbers are placed at lower addresses of memory while the low-order bytes of numbers are placed at high addresses of memory.

2.3

message

Bit string of random finite length. Message in this Standard is deemed as the input data of hash algorithm.

2.4

hash value

Message digest (bit string) output when hash algorithm acts on a message.

2.5

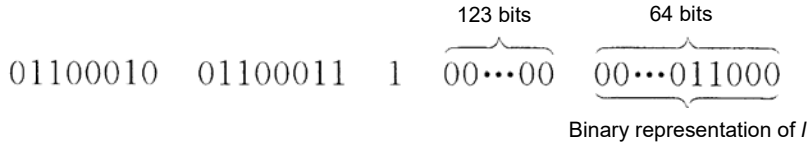
word

Group (string) which is 32 bits long.

3 Symbols

For the purposes of this Standard, the following symbols apply.

ABCDEFGH:	8-word register or series of their values
$B^{(i)}$:	the *i*-th message group
CF:	compression function
FF_j:	boolean function, which is expressed according to the change of *j*
GG_j:	boolean function, which is expressed according to the change of *j*
IV:	Initial value, which is used to determine the initial state of compression function register
P_0:	permutation function in compression function
P_1:	permutation function in message extension
T_j:	algorithmic constant
m:	message
m':	populated message
mod:	modulo operation
n:	number of message groups
$\wedge$:	32-bit AND operation
$\vee$:	32-bit OR operation
$\oplus$:	32-bit exclusive-OR operation
$\neg$:	32-bit NOT operation
$+$:	mod-2^{32}-bit arithmetic additive operation
$<<<_k$:	32-bit ring shift left operation by k bits
$\leftarrow$:	Left assignment operator



5.3 Iterative compression

5.3.1 Iteration process

Divide the populated message *m'* into groups by 512 bits:

$$m' = B^{(0)} B^{(1)} \cdots B^{(n-1)}$$

where $n = (l + k + 65)/512$.

Iterate *m'* as follows:

FOR $i = 0$ **TO** $n - 1$
$V^{(i+1)} = CF(V^{(i)}, B^{(i)})$
ENDFOR

where *CF* is compression function, $V^{(0)}$ is 256-bit initial value *IV*, $B^{(i)}$ is populated message group and the result of iterative compression is $V^{(n)}$.

5.3.2 Message extension

Extent the message group $B^{(i)}$ to generate 132 message words as follows, i.e. $W_0, W_1, \ldots, W_{67}, W'_0, W'_1, \ldots W'_{63}$, for compression function *CF*:

a) divide the message group $B^{(i)}$ into 16 words, i.e. $W_0, W_1, \ldots, W_{15}$.

b) **FOR** $j = 16$ **TO** 67
$W_j \leftarrow P_1(W_{j-16} \oplus W_{j-9} \oplus (W_{j-3} <<< 15)) \oplus (W_{j-13} <<< 7) \oplus W_{j-6}$
ENDFOR

c) **FOR** $j = 0$ **TO** 63
$W'_j = W_j \oplus W_{j+4}$
ENDFOR

5.3.3 Compression function

Let *A, B, C, D, E, F, G* and *H* be word registers, *SS1, SS2, TT1* and TT2 intermediate variables, and compression function $V^{(i+1)} = CF(V^{(i)}, B^{(i)})$ $(0 \le i \le n-1)$. The calculation process is described as follows:

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

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