



中华人民共和国国家标准

GB/T 32905—2016

信息安全技术 SM3 密码杂凑算法

Information security techniques—SM3 cryptographic hash algorithm

2016-08-29 发布

2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

目 次

前言	Ⅲ
1 范围	1
2 术语和定义	1
3 符号	1
4 常数与函数	2
4.1 初始值	2
4.2 常量	2
4.3 布尔函数	2
4.4 置换函数	2
5 算法描述	2
5.1 概述	2
5.2 填充	2
5.3 迭代压缩	3
5.4 输出杂凑值	4
附录 A (资料性附录) 运算示例	5

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由国家密码管理局提出。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)归口。

本标准起草单位:清华大学、国家密码管理局商用密码检测中心、解放军信息工程大学、中国科学院数据与通信保护研究教育中心。

本标准主要起草人:王小云、李峥、王永传、于红波、谢永泉、张超、罗鹏、吕述望。

信息安全技术 SM3 密码杂凑算法

1 范围

本标准规定了 SM3 密码杂凑算法的计算方法和计算步骤,并给出了运算示例。

本标准适用于商用密码应用中的数字签名和验证、消息认证码的生成与验证以及随机数的生成,可满足多种密码应用的安全需求。

2 术语和定义

下列术语和定义适用于本文件。

2.1

比特串 bit string

具有 0 或 1 值的二进制数字序列。

2.2

大端 big-endian

数据在内存中的一种表示格式,规定左边为高有效位,右边为低有效位。即数的高阶字节放在存储器的低地址,数的低阶字节放在存储器的高地址。

2.3

消息 message

任意有限长度的比特串,本标准中消息作为杂凑算法的输入数据。

2.4

杂凑值 hash value

杂凑算法作用于一条消息时输出的消息摘要(比特串)。

2.5

字 word

长度为 32 比特的组(串)。

3 符号

下列符号适用于本文件。

$ABCDEFGH$: 8 个字寄存器或它们的值的串连

$B^{(i)}$: 第 i 个消息分组

CF : 压缩函数

FF_j : 布尔函数,随 j 的变化取不同的表达式

GG_j : 布尔函数,随 j 的变化取不同的表达式

IV : 初始值,用于确定压缩函数寄存器的初态

P_0 : 压缩函数中的置换函数

P_1 : 消息扩展中的置换函数

T_j : 算法常量,随 j 的变化取不同的值