ICS 35.040
L 80
备案号:36831—2012

GM

中华人民共和国密码行业标准

GM/T 0004—2012

SM3 密码杂凑算法

SM3 cryptographic hash algorithm

2012-03-21 发布　　2012-03-21 实施

国家密码管理局　　发 布

目　　次

前　言

本标准依据 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准的附录 A 为资料性附录。

本标准由国家密码管理局提出并归口。

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、于红波、张超、罗鹏、吕述望。

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。同时，本标准还可为安全产品生产商提供产品和技术的标准定位以及标准化的参考，提高安全产品的可信性与互操作性。

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

下列符号适用于本标准。

$ABCDEFGH$：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