

ICS 35.040
L 80
备案号：38307—2013



中华人民共和国密码行业标准

GM/T 0009—2012

SM2 密码算法使用规范

SM2 cryptography algorithm application specification

2012-11-22 发布

2012-11-22 实施

国家密码管理局 发布

目 次

前言	I
引言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 符号和缩略语	1
5 SM2 的密钥对	1
5.1 SM2 私钥	1
5.2 SM2 公钥	2
6 数据转换	2
6.1 位串到 8 位字节串的转换	2
6.2 8 位字节串到位串的转换	2
6.3 整数到 8 位字节串的转换	2
6.4 8 位字节串到整数的转换	2
7 数据格式	3
7.1 密钥数据格式	3
7.2 加密数据格式	3
7.3 签名数据格式	3
7.4 密钥对保护数据格式	3
8 预处理	4
8.1 预处理 1	4
8.2 预处理 2	4
9 计算过程	4
9.1 生成密钥	4
9.2 加密	5
9.3 解密	5
9.4 数字签名	5
9.5 签名验证	5
9.6 密钥协商	6
10 用户身份标识 ID 的默认值	7

前 言

本标准按照 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。

本标准由国家密码管理局提出并归口。

本标准起草单位：北京海泰方圆科技有限公司、卫士通信息产业股份有限公司、无锡江南信息安全工程技术中心、兴唐通信科技股份有限公司、山东得安信息技术有限公司、上海格尔软件股份有限公司。

本标准主要起草人：刘平、蒋红宇、柳增寿、曾宇波、李元正、徐强、谭武征、孔凡玉、王妮娜。

引 言

SM2 椭圆曲线密码算法(以下简称 SM2)是国家密码管理局批准的一组算法,其中包括 SM2-1 椭圆曲线数字签名算法、SM2-2 椭圆曲线密钥协商协议、SM2-3 椭圆曲线加密算法。

本标准的目标是保证 SM2 使用的正确性,为 SM2 密码算法的使用制定统一的数据格式和使用方法。

本标准中涉及的 SM3 算法是指国家密码管理局批准的 SM3 密码杂凑算法。

本标准仅从算法应用的角度给出 SM2 密码算法的使用说明,不涉及 SM2 密码算法的具体编制细节。

SM2 密码算法使用规范

1 范围

本标准定义了 SM2 密码算法的使用方法,以及密钥、加密与签名等的数据格式。

本标准适用于 SM2 密码算法的使用,以及支持 SM2 密码算法的设备和系统的研发和检测。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GM/T 0003(所有部分) SM2 椭圆曲线公钥密码算法

GM/T 0004 SM3 密码杂凑算法

3 术语和定义

下列术语和定义适用于本文件。

3.1

算法标识 algorithm identifier

用于标明算法机制的数字化信息。

3.2

SM2 密码算法 SM2 algorithm

一种椭圆曲线密码算法,密钥长度为 256 比特。

3.3

SM3 算法 SM3 algorithm

一种杂凑算法,输出长度为 256 比特。

4 符号和缩略语

下列缩略语适用于本文件:

ECB 电码本模式

ECC 椭圆曲线密码算法(Elliptic Curve Cryptography)

ID 用户身份标识(Identity)

5 SM2 的密钥对

5.1 SM2 私钥

SM2 私钥是一个大于或等于 1 且小于 $n-1$ 的整数(n 为 SM2 算法的阶,其值参见 GM/T 0003),简记为 k ,长度为 256 位。