ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0009—2023
代替 GM/T 0009—2012

SM2 密码算法使用规范

SM2 cryptography algorithm application specification

2023-12-04 发布　　2024-06-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GM/T 0009—2012《SM2密码算法使用规范》，与GM/T 0009—2012相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改了SM2私钥（见5.1，2012年版的5.1）；

b) 更改了SM2公钥（见5.2，2012年版的5.2）；

c) 更改了SM2公钥格式（见7.1，2012年版的7.1）；

d) 更改了密钥对保护数据格式（见7.4，2012年版的7.4）；

e) 更改了预处理1（见8.1，2012年版的8.1）。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：北京海泰方圆科技股份有限公司、北京信安世纪科技股份有限公司、北京小雷科技有限公司、中电科网络安全科技股份有限公司、北京国脉信安科技有限公司、无锡江南信息安全工程技术中心、兴唐通信科技有限公司、山东得安信息技术有限公司、格尔软件股份有限公司、山东大学。

本文件主要起草人：刘平、蒋红宇、柳增寿、曾宇波、袁峰、李元正、徐强、谭武征、孔凡玉、王妮娜、汪宗斌、安晓江、罗俊、徐明翼、郑强、马洪富。

本文件及其所代替文件的历次版本发布情况为：

——2012年首次发布为GM/T 0009—2012；

——本次为第一次修订。

SM2 密码算法使用规范

1 范围

本文件定义了 SM2 密码算法的使用方法，也定义了相关的数据格式。

本文件适用于 SM2 密码算法的使用，也适用于支持 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

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 32905—2016 信息安全技术 SM3 密码杂凑算法

GB/T 32918.1—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 1 部分：总则

GB/T 32918.2—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 2 部分：数字签名算法

GB/T 32918.3—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 3 部分：密钥交换协议

GB/T 32918.4—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 4 部分：共钥加密算法

GB/T 32918.5—2017 信息安全技术 SM2 椭圆曲线公钥密码算法 第 5 部分：参数定义

GM/T 0006 密码应用标识规范

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001 界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件。

ECB 电码本模式(Electronic Codebook)

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

ID 用户身份标识(Identity)

5 SM2 密钥对

5.1 SM2 私钥

SM2 私钥是大于或等于 1 且小于 $n-1$ 的整数(n 为 SM2 算法的阶，其值见 GB/T 32918.5—2017)，简记为 d。

5.2 SM2 公钥

SM2 公钥是 SM2 曲线上的一个点，由横坐标和纵坐标两个分量来表示，记为(x，y)，简记为 Q。公