



中华人民共和国国家标准

GB/T 41389—2022

信息安全技术 SM9 密码算法使用规范

Information security technology—
SM9 cryptographic algorithm application specification

2022-04-15 发布

2022-11-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

| | |
|-----------------------------|----|
| 前言 | I |
| 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 | 2 |
| 5 SM9 的密钥对 | 2 |
| 5.1 生成元 | 2 |
| 5.2 SM9 主私钥 | 2 |
| 5.3 SM9 主公钥 | 2 |
| 5.4 SM9 用户私钥 | 3 |
| 5.5 SM9 用户公钥 | 3 |
| 6 技术要求 | 3 |
| 6.1 数据格式 | 3 |
| 6.2 预处理 | 5 |
| 6.3 计算过程 | 7 |
| 7 证实方法 | 11 |
| 7.1 数据格式 | 11 |
| 7.2 预处理 | 11 |
| 7.3 计算过程 | 12 |
| 附录 A (规范性) 数据格式编码测试用例 | 14 |

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。

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。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：北京国脉信安科技有限公司、上海信息安全工程技术研究中心、深圳奥联信息安全技术有限公司、无锡华正天网信息安全系统有限公司、国网区块链科技(北京)有限公司。

本文件主要起草人：袁峰、王晓春、封维端、张立圆、王学进、药乐、蒋楠、程朝辉、蔡先勇、王一曲、王栋。