



# 中华人民共和国国家标准

GB/T 38635.2—2020

---

## 信息安全技术 SM9 标识密码算法 第 2 部分：算法

Information security technology—Identity-based cryptographic algorithms SM9—  
Part 2: Algorithms

2020-04-28 发布

2020-11-01 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 .....	III
引言 .....	IV
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 符号 .....	2
5 算法参数与辅助函数 .....	3
5.1 概述 .....	3
5.2 系统参数组 .....	4
5.3 辅助函数 .....	4
6 数字签名生成和验证算法及流程 .....	6
6.1 系统签名主密钥和用户签名密钥的产生 .....	6
6.2 数字签名生成算法 .....	6
6.3 数字签名生成算法流程 .....	7
6.4 数字签名验证算法 .....	7
6.5 数字签名验证算法流程 .....	8
7 密钥交换协议及流程 .....	9
7.1 系统加密主密钥和用户加密密钥的产生 .....	9
7.2 密钥交换协议 .....	9
7.3 密钥交换协议流程 .....	10
8 密钥封装机制及流程 .....	11
8.1 系统加密主密钥和用户加密密钥的产生 .....	11
8.2 密钥封装算法 .....	11
8.3 密钥封装算法流程 .....	11
8.4 解封装算法 .....	12
8.5 解封装算法流程 .....	12
9 加密算法及流程 .....	13
9.1 系统加密主密钥和用户加密密钥的产生 .....	13
9.2 加密算法 .....	13
9.3 加密算法流程 .....	14
9.4 解密算法 .....	15
9.5 解密算法流程 .....	16
附录 A (资料性附录) 算法示例 .....	17

## 前 言

GB/T 38635《信息安全技术 SM9 标识密码算法》分为两个部分：

——第 1 部分：总则；

——第 2 部分：算法。

本部分为 GB/T 38635 的第 2 部分。

本部分按照 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。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：国家信息安全工程技术研究中心、北京国脉信安科技有限公司、深圳奥联信息安全技术有限公司、中国科学院软件研究所、武汉大学、中科院信息工程研究所。

本部分主要起草人：陈晓、程朝辉、张振峰、叶顶峰、胡磊、陈建华、季庆光、袁文恭、刘平、马宁、袁峰、李增欣、王学进、杨恒亮、张青坡、马艳丽、浦雨三、唐英、孙移盛、安莹、封维端、张立圆。