



# 中华人民共和国国家标准

GB/T 38635.1—2020

---

## 信息安全技术 SM9 标识密码算法 第 1 部分：总则

Information security technology—Identity-based cryptographic algorithms SM9—  
Part 1: General

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 .....	1
5 有限域和椭圆曲线 .....	3
5.1 有限域 .....	3
5.2 有限域上的椭圆曲线 .....	4
5.3 椭圆曲线群 .....	4
5.4 椭圆曲线多倍点运算 .....	5
5.5 椭圆曲线子群上点的验证 .....	5
5.6 离散对数问题 .....	5
6 双线性对及安全曲线 .....	5
6.1 双线性对 .....	5
6.2 安全性 .....	6
6.3 嵌入次数及安全曲线 .....	6
7 数据类型及其转换 .....	6
7.1 数据类型 .....	6
7.2 数据类型转换 .....	7
8 系统参数及其验证 .....	10
8.1 系统参数 .....	10
8.2 系统参数的验证 .....	11
附录 A (规范性附录) 参数定义 .....	12
附录 B (资料性附录) 关于椭圆曲线的背景知识 .....	14
附录 C (资料性附录) 椭圆曲线上双线性对的计算 .....	21
附录 D (资料性附录) 数论算法 .....	28
参考文献 .....	33

## 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 1 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、安萱、封维端、张立圆。