



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 发布
国家标准化管理委员会

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、安萱、封维端、张立圆。

引 言

A. Shamir 在 1984 年提出了标识密码 (Identity-based cryptography) 的概念, 在标识密码系统中, 用户的私钥由密钥生成中心 (KGC) 根据主密钥和用户标识计算得出, 用户的公钥由用户标识唯一确定, 由标识管理者保证标识的真实性。与基于证书的公钥密码系统相比, 标识密码系统中的密钥管理环节可以得到适当简化。

1999 年, K. Ohgishi、R. Sakai 和 M. Kasahara 在日本提出了用椭圆曲线对 (pairing) 构造基于标识的密钥共享方案; 2001 年, D. Boneh 和 M. Franklin, 以及 R. Sakai、K. Ohgishi 和 M. Kasahara 等人独立提出了用椭圆曲线对构造标识公钥加密算法。这些工作引发了标识密码的新发展, 出现了一批用椭圆曲线对实现的标识密码算法, 其中包括数字签名算法、密钥交换协议、密钥封装机制和公钥加密算法等。

椭圆曲线对具有双线性的性质, 它在椭圆曲线的循环子群与扩域的乘法循环子群之间建立联系, 构成了双线性 DH、双线性逆 DH、判定性双线性逆 DH、 τ -双线性逆 DH 和 τ -Gap-双线性逆 DH 等难题, 当椭圆曲线离散对数问题和扩域离散对数问题的求解难度相当时, 可用椭圆曲线对构造出安全性和实现效率兼顾的标识密码。

信息安全技术 SM9 标识密码算法

第 2 部分:算法

1 范围

GB/T 38635 的本部分规定了 SM9 标识密码算法中数字签名算法、密钥交换协议、密钥封装机制和加密算法。

本部分适用于 SM9 标识密码算法工程化的实现,指导 SM9 标识密码算法相关产品的研制和检测。

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。

GB/T 17964 信息安全技术 分组密码算法的工作模式

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32915 信息安全技术 二元序列随机性检测规范

GB/T 38635.1—2020 信息安全技术 SM9 标识密码算法 第 1 部分:总则

3 术语和定义

GB/T 38635.1—2020 界定的以及下列术语和定义适用于本文件。为了便于使用,以下重复列出了 GB/T 38635.1—2020 中的一些术语和定义。

3.1

加密主密钥 encryption master key

处于标识密码密钥分层结构最顶层的密钥,内容为加密主私钥和加密主公钥,其中加密主公钥公开,加密主私钥由密钥生成中心(KGC)秘密保存。KGC 用加密主私钥和用户的标识生成用户的加密私钥。在标识密码中,加密主私钥一般由 KGC 通过随机数发生器产生,加密主公钥由加密主私钥结合系统参数产生。

3.2

标识 identity

由实体无法否认的信息组成,如实体的可识别名称、电子邮箱、身份证号、电话号码、街道地址等,可唯一确定一个实体的身份。

[GB/T 38635.1—2020,定义 3.1]

3.3

发起方 initiator

在一个协议的操作过程中发送首轮交换信息的用户。

3.4

初始向量/值 initialization vector/initialization value; IV

在密码变换中,为增加安全性或使密码设备同步而引入的用于数据变换的起始数据。