ICS 35.040
L 80

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

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。

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 1 部分:总则

1　范围

GB/T 38635 的本部分规定了 SM9 标识密码算法涉及的必要相关数学基础知识、密码技术和具体参数。

本部分适用于 SM9 标识密码的实现和应用。

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 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

3　术语和定义

下列术语和定义适用于本文件。

3.1

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。

3.2

主密钥　master key

处于标识密码密钥分层结构最顶层的密钥,包括主私钥和主公钥,其中主公钥公开,主私钥由 KGC 秘密保存。KGC 用主私钥和用户的标识生成用户的私钥。在标识密码中,主私钥一般由 KGC 通过随机数发生器产生,主公钥由主私钥结合系统参数产生。

3.3

密钥生成中心　key generation center;KGC

在 SM9 标识密码中,负责选择系统参数、生成主密钥并产生用户私钥的可信机构。

3.4

SM3 算法　SM3 algorithm

由 GB/T 32905 定义的一种杂凑算法。

3.5

SM4 算法　SM4 algorithm

由 GB/T 32907 定义的一种分组加密算法。

4　符号

下列符号适用于本文件。