ICS 35.040
L 80
备案号：55618—2016

GM

中华人民共和国密码行业标准

GM/T 0044.1—2016

SM9 标识密码算法 第 1 部分：总则

Identity-based cryptographic algorithms SM9—Part 1：General

2016-03-28 发布　　2016-03-28 实施

国家密码管理局　　发 布

目　　次

前　言

GM/T 0044《SM9 标识密码算法》分为 5 个部分：

——第 1 部分：总则；

——第 2 部分：数字签名算法；

——第 3 部分：密钥交换协议；

——第 4 部分：密钥封装机制和公钥加密算法；

——第 5 部分：参数定义。

本部分为 GM/T 0044 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。

本部分由密码行业标准化技术委员会提出并归口。

本部分起草单位：国家信息安全工程技术研究中心、深圳奥联信息安全技术有限公司、武汉大学、上海交通大学、中科院信息工程研究所、北方信息技术研究所。

本部分主要起草人：陈晓、程朝辉、叶顶峰、胡磊、陈建华、路贝可、季庆光、曹珍富、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。

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,从而用户不需要通过第三方保证其公钥的真实性。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。

本部分描述必要的数学基础知识与相关密码技术,以帮助实现本标准其他各部分所规定的密码机制。

SM9 标识密码算法
第 1 部分:总则

1 范围

GM/T 0044 的本部分描述了必要的数学基础知识与相关密码技术,以帮助实现 GM/T 0044 的其他各部分所规定的密码机制。

本部分适用于商用密码算法中标识密码的实现、应用和检测。

本部分规定使用 F_p(素数 $p>2^{191}$)上椭圆曲线。

2 术语和定义

下列术语和定义适用于本文件。

2.1

标识 identity

可唯一确定一个实体身份的信息。标识应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、电话号码等。

2.2

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。

本部分中,签名系统的主密钥与加密系统的主密钥不同。数字签名算法属于签名系统,其主密钥为签名主密钥,密钥交换协议、密钥封装机制和公钥加密算法属于加密系统,其主密钥为加密主密钥。

2.3

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 符号和缩略语

下列符号和缩略语适用于本文件。

cf:椭圆曲线阶相对于 N 的余因子。

cid:用一个字节表示的曲线识别符,用以区分所用曲线的类型。

DLP:有限域上离散对数问题。

$deg(f)$:多项式 $f(x)$的次数。

d_1、d_2:k 的两个因子。

E:定义在有限域上的椭圆曲线。

$ECDLP$:椭圆曲线离散对数问题。

$E(F_q)$:有限域 F_q 上椭圆曲线 E 的所有有理点(包括无穷远点 O)组成的集合。

$E(F_q)[r]$:$E(F_q)$上 r-扭点的集合(即曲线 $E(F_q)$上的 r 阶扭子群)。