ICS 35.040
L 80
备案号：55616—2016

GM

中华人民共和国密码行业标准

GM/T 0044.4—2016

SM9 标识密码算法
第 4 部分：密钥封装机制和公钥加密算法

Identity-based cryptographic algorithms SM9—
Part 4：Key encapsulation mechanism and public key encryption algorithm

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 4 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。

本部分描述了用椭圆曲线对实现的基于标识的密钥封装机制和公钥加密算法。

SM9 标识密码算法
第 4 部分:密钥封装机制和公钥加密算法

1 范围

GM/T 0044 的本部分规定了用椭圆曲线对实现的基于标识的密钥封装机制和公钥加密与解密算法,并提供相应的流程。利用密钥封装机制可以封装密钥给特定的实体。公钥加密与解密算法即基于标识的非对称密码算法,该算法使消息发送者可以利用接收者的标识对消息进行加密,唯有接收者可以用相应的私钥对该密文进行解密,从而获取消息。

本部分适用于密钥封装和对消息的加解密。

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。

GM/T 0004—2012 SM3 密码杂凑算法

GM/T 0002—2012 SM4 分组密码算法

GM/T 0044.1—2016 SM9 标识密码算法 第 1 部分:总则

GM/T 0044.2—2016 SM9 标识密码算法 第 2 部分:数字签名算法

GM/T 0044.3—2016 SM9 标识密码算法 第 3 部分:密钥交换协议

3 术语和定义

下列术语和定义适用于本文件。

3.1

秘密密钥 secret key

在密码体制中收发双方共同拥有的、而第三方不知道的一种密钥。

3.2

消息 message

任意有限长度的比特串。

3.3

明文 plaintext

未加密的信息。

3.4

密文 ciphertext

经过变换、信息内容被隐藏起来的数据。

3.5

加密 encipherment

为了产生密文,即隐藏数据的信息内容,由密码算法对数据进行(可逆)变换。