信息安全研究 第2卷 第11期 2016年11月
Journal of Information Security Research Vol.2 No.11 Nov. 2016

SM9 标识密码算法综述

袁 峰[1] 程朝辉[2]
[1](国家信息安全工程技术研究中心 北京 100091)
[2](深圳市奥联信息安全技术有限公司 广东深圳 518052)
(yuanfengmail@163.com)

Overview on SM9 Identity-Based Cryptographic Algorithm

Yuan Feng[1] and Cheng Zhaohui[2]
[1](National Information Security Engineering and Technic Reseach Center, Beijing 100091)
[2](*Shenzhen OLYM Science Technology Ltd*, *Shenzhen*, *Guangdong* 518052)

Abstract SM9 identity-based cryptographic algorithm is an identity-based cryptosystem with bilinear pairings. In such a system the user s private key and public key may be extracted from user s identity and key generation center's parameters. The most common cryptographic uses of SM9 are with digital signature, data encryption, key exchange protocol and key encapsulation mechanism etc. The application and management of SM9 will not require digital certificate, certificate base, and key base. The key length of the SM9 cipher algorithm is 256 b. SM9 cryptographic algorithm was issued as the cryptography standard in 2015. This paper will summarize the design, algorithm, software and hardware implementation and cryptanalysis of SM9 cryptographic algorithm. We also give some concrete examples in appendix.

Key words SM9 algorithm; identity-based cryptographic algorithm; bilinear pairings; digital signature; data encryption

摘 要 SM9 标识密码算法是一种基于双线性对的标识密码算法,它可以把用户的身份标识用以生成用户的公、私密钥对,主要用于数字签名、数据加密、密钥交换以及身份认证等. SM9 密码算法的密钥长度为 256b. SM9 密码算法的应用与管理不需要数字证书、证书库或密钥库. 该算法于 2015 年发布为国家密码行业标准(GM/T 0044—2016). 总结了 SM9 密码算法的设计原理、算法描述、软硬件实现和安全性分析.

关键词 SM9 算法;基于标识的密码算法;双线性对;数字签名;数据加密

中图法分类号 TP309

SM9 标识密码算法是一种基于双线性对的标识密码体制(identity-based cryptography, IBC),是我国商用密码行业公钥密码算法的一种标准算法. SM9 算法的主要内容包括: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,简称 SM9 签名算法;SM9 密钥交换算法;SM9 加密算法. SM9 密码算法的理论基础和数学工具是有限域群上椭圆曲线的点群运算的性质及双线性对运算特性.

收稿日期:2016-10-20