计算机工程与应用　2009 45 (30): 6-9　ISSN: 1002-8331　CN: 11-2127/TP

博士论坛

适用于3G网络的无证书的短签密方案

罗　铭，何光宇，闻英友，赵　宏

东北大学，沈阳　110004

收稿日期　2009-4-20　修回日期　2009-8-31　网络版发布日期　2009-11-6　接受日期

摘要　短签密方案实现了在一个逻辑步骤内同时完成了加密和数字签名二者的功能，并且所花费的代价，包括计算时间和消息扩展率两方面，要远远低于传统的先签名后加密的方法。然而目前大部分的短签密方案都不具有可信公钥以及签名验证阶段发生在解签密阶段之后，降低了签密消息的可靠性与伪造签密消息的处理效率。一种新型的基于无证书密码系统的短签密方案被提了出来，相应的安全模型也被定义。该方案计算量小，仅需一次对运算，而且还具有可信公钥以及临时密钥安全性。经过分析及实现验证，该方案可以在消息保密性的基础上实现3G网络信息在传播路径上的认证，从而防范垃圾信息的传播。

关键词　无证书密码系统　短签密　临时密钥安全性

分类号　TP393

Certificateless short signcryption scheme for 3G network

LUO Ming，HE Guang-yu，WEN Ying-you，ZHAO Hong

Northeastern University，Shenyang 110004，China

Abstract

Short signcryption is a technique which implements message encryption and digital signature in a logical single step，at lower computational times and message extension rates than the traditional signature-then-encryption approach.However，almost all short signcryption schemes that have been proposed until now have no creditable public key and signature verification is behind ciphertext decryption，which reduces the credibility of signcryption message and efficiency in dealing with fake message.A new certificateless-based short signcryption scheme is proposed and corresponding security models is defined，and the whole operation only requires one pairing operation.Moreover，the scheme has creditable public key and known session-specific temporary information security.Through analysis and validation，the scheme has defended network spam，since it carries out the confidentiality and authentication as the message transmission.

Key words　certificateless cryptography　short signcryption　known session-specific temporary information security

DOI:　10.3778/j.issn.1002-8331.2009.30.003

扩展功能

本文信息

- Supporting info
- PDF(907KB)
- [HTML全文](0KB)
- 参考文献

服务与反馈

- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- 复制索引
- Email Alert
- 文章反馈
- 浏览反馈信息

相关信息

- 本刊中 包含“无证书密码系统”的相关文章
- 本文作者相关文章
  - 罗　铭
  - 何光宇
  - 闻英友
  - 赵　宏

通讯作者　罗　铭 luom@neusoft.com