计算机工程与应用 2007 43 (36): 153-156 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

基于ElGamal体制的指定验证人多重数字签名

段昌敏[1], 粟 栗[2]

1.湖北民族学院 信息工程学院，湖北 恩施 445000
2.华中科技大学 计算机学院，武汉 430074

收稿日期 修回日期 网络版发布日期 2007-12-10 接受日期

摘要 通过分析指出公开可验证的多重签名会产生信息泄漏，危机信息安全，指出指定验证人多重签名能保护信息的安全性，并设计了两个基于ElGamal体制的方案：一种是可验证的按序多重签名，另一种是可抵制合谋攻击的广播多重签名。两种方案都具有指定验证人的特性，避免了签名者和接收者的信息泄漏，同时签名长度都不随签名者的人数增加而增长，并能抵制伪造和勾结攻击，能保障签名者和签名接收者的安全性。

关键词 指定验证人多重数字签名 按序多重签名 广播多重签名

分类号

扩展功能

本文信息

- Supporting info
- PDF(678KB)
- [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“指定验证人多重数字签名”的相关文章
- 本文作者相关文章
  - 段昌敏
  - 粟 栗

Designated verifier multisignature schemes based on ElGamal scheme

DUAN Chang-min[1],SU Li[2]

1.School of Information Engineering，Hubei Institute for Nationalities，Enshi，Hubei 445000，China
2.College of Computer Science and Technology，Huazhong University of Science and Technology，Wuhan 430074，China

Abstract

Publicly verifiable multisignature makes the leakage of information，which is harmful to information security.Designated verifier multisignatures are privacy-oriented signatures that provide message authenticity only to specific receiver，which is suitable for some specific conditions.The paper proposes two designated verifier multisignature schemes based on ElGamal algorithm and designated verifier signature.One is a verifiably sequential multisignature，the other is a broadcasting multisignature.These multisignature schemes have the attribute of specified receiver，can avoid the leakage of information of both receiver and signatures，and resist forgery and coalition.The size of signature does not increase with signer number.These two schemes ensure the security of receiver and signatures.

Key words disignated receiver multisignature sequential multisignature broadcasting multisignature

DOI:

通讯作者 段昌敏 bydht@163.com