

- >> 首页
- >> 被收录信息
- >> 投稿须知
- >> 模板下载
- >> 信息发布
- >> 常见问题及解答
- >> 合作单位
- >> 产品介绍
- >> 编委会/董事会
- >> 关于我们
- >> 网上订阅
- >> 友情链接

友情链接

- >> 中国期刊网
- >> 万方数据资源库
- >> 台湾中文电子期刊
- >> 四川省计算应用研究中心
- >> 维普资讯网

基于身份的强指定验证人签名方案*

Identity-based strong designated verifier signature schemes

摘要点击: 33 全文下载: 17

[查看全文](#) [查看/发表评论](#) [下载PDF阅读器](#)

中文关键词: [基于身份的签名](#) [指定验证人签名](#) [代理签名](#) [双线性对](#)

英文关键词: [identity-based signature](#) [designated verifier signature](#) [proxy signature](#) [bilinear pairings](#)

基金项目: 国家自然科学基金资助项目(60873119); 陕西省自然科学基金基础研究计划资助项目(2007A06)

作者

单位

[毛卫霞, 李志慧, 薛婷](#)

[\(陕西师范大学 数学与信息科学学院, 西安 710062\)](#)

中文摘要:

在有些情况下, 需要将验证者限定为某一个人。利用基于身份的密码体制, 提出了一种强指定验证人签名和一种强指定验证人多重代理签名, 并对其安全性进行了分析。在签名代价和验证代价上, 提出的强指定验证人签名比Kang等人的方案要低。提出的强指定验证人多重代理签名可以同时授权给n个代理人, 可以有效防止代理签名人对签名权的滥用。

英文摘要:

We should specify a verifier in some circumstances. Using identity-based cryptography, this paper proposed a strong designated verifier signature and a strong designated verifier multi-proxy signature. It also analyzed the proposed schemes. The proposed strong designated verifier signature scheme was lower than Kang et al.'s scheme in the signing cost and verifying cost. The proposed strong designated verifier multi-proxy signature scheme could delegate n proxy signers. Thus it could prevent proxy signers abusing signing authority.

您是第2827010位访问者

主办单位: 四川省计算机研究院 单位地址: 成都市武侯区成科西路3号

服务热线: 028-85249567 传真: 028-85210177 邮编: 610041 Email: arocmag@163.com

蜀ICP备05005319号 本系统由北京勤云科技发展有限公司设计