

- >> 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

基于双线性对的秘密分享方案*

Secret sharing scheme based on bilinear pairings

摘要点击: 32 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: [秘密分享](#) [双线性对](#) [密钥更新](#)

英文关键词: [secret sharing](#) [bilinear pairings](#) [key updating](#)

基金项目: 国家自然科学基金资助项目(70771079); 鲁东大学人才基金资助项目(LY20062706); 鲁东大学科研基金资助项目(L20082702)

作者

单位

[柏钦玺¹](#), [黄崇超²](#), [刘锋¹](#)

(1. 鲁东大学 数学与信息学院, 山东 烟台 264025; 2. 武汉大学 数学与统计学院, 武汉 430072)

中文摘要:

提出了一种新的基于双线性对的门限秘密分享方案, 并对其正确性、安全性和性能进行了分析讨论; 该方案将分享者私钥计算和秘密分发过程分离, 秘密份额可以重新利用, 具有更好的性能, 更适合实际应用。

英文摘要:

This paper proposed a new secret sharing scheme based on the bilinear pairings. And discussed its correctness, security and performance. At the same time, the proposed scheme departs the private keys of participants computation from the secret distribution process, which made this scheme more secure and more efficient. Therefore, the proposed scheme is more applicable than the existing ones.

您是第2826912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