计算机应用研究
Application Research Of Computers





# 基于双线性对的秘密分享方案*

## Secret sharing scheme based on bilinear pairings



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 parings. 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.