

计算机应用研究

Application Research Of Computers

- >> 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Merkle身份树的动态对等群组密钥协商*

Key agreement scheme for dynamic peer groups based on Merkle identity tree

摘要点击: 20 全文下载: 10

[查看全文](#) [查看/发表评论](#) [下载PDF阅读器](#)

中文关键词: [动态对等群组](#) [密钥协商](#) [身份树](#) [双线性对](#)

英文关键词: [dynamic peer groups](#) [key agreement](#) [identity tree](#) [bilinear pairing](#)

基金项目: 国家自然科学基金资助项目(60673070); 江苏省自然科学基金资助项目(BK2006217); 淮阴工学院青年教师科研基金项目(HGC0916)

作者	单位
陈礼青	(淮阴工学院 计算机工程学院, 江苏 淮安 223003)

中文摘要:

针对设计高效的分布式密钥协商方案是动态对等群组播通信的难点, 提出了一个新的基于Merkle身份树的密钥协商方案, 并具体地分析了子组之间的通信用程, 以及组成员动态变化时密钥的更新过程。结果表明该方案在降低计算和通信代价方面取得了较好的效果。

英文摘要:

Abstract: Designing efficient distributive key agreement scheme was a difficult problem in multicast communication of dynamic peer groups. This paper proposed a new key agreement scheme for multicast groups based on Merkle identity tree. Then analyzed the procedures of secret communications between subgroups and updating of group keys with the dynamic change of group members in detail. The analysis shows that the new scheme is efficient in computation and communication.

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

