

安全技术

基于广播加密的会话密钥分配新方案

赖霞, 何明星

(西华大学数学与计算机学院, 成都 610039)

收稿日期 修回日期 网络版发布日期 2008-2-29 接受日期

摘要 广播加密方案是一种应用广泛的群组安全通信方案, 在付费电视、视频会议和无线传感网络等场合具有良好的应用前景。该文针对许多基于二叉树结构的方案在中心控制密钥量上作了一些改进, 提出了一个安全的基于广播加密的会话密钥分配方案。新方案在中心密钥存储量上有明显的优势, 同时能安全有效地完成密钥的分发、用户添加以及加密密钥更新等功能。

关键词 [广播加密; 密钥分配; 伪随机函数; 预留节点](#)

分类号 [TP309](#)

DOI:

对应的英文版文章: [05-61C](#)

通讯作者:

作者个人主页: [赖霞; 何明星](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(156KB\)](#)
- ▶ [\[HTML全文\] \(0KB\)](#)
- ▶ [参考文献 \[PDF\]](#)
- ▶ [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](#)
- ▶ [引用本文](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

相关信息

- ▶ [本刊中 包含“广播加密; 密钥分配; 伪随机函数; 预留节点”的 相关文章](#)
- ▶ [本文作者相关文章](#)
- [赖霞](#)
- [何明星](#)