电子与信息学报 2008 30 (6): 1457-1461 ISSN: 1009-5896 CN: 11-4494/TN

论文

基于离散对数问题的两层分散式组密钥管理方案

杨 军[1,2], 周贤伟[2]

[1]西南民族大学计算机科学与技术学院 成都 610041; [2]北京科技大学信息工程学院 北京 100083

收稿日期 2006-11-20 修回日期 2007-5-28 网络版发布日期 2008-8-28 接受日期

摘要
该文基于"多个解密密钥映射到同一加密密钥"的公钥加密算法提出一个组密钥更新协议，结合LKH算法为特定源多播模型设计一个两层分散式组密钥管理方案。证明它具有后向保密性、高概率的前向保密性和抗串谋性。通过上层私钥的长寿性和密钥转换的方法来缓解子组管理者的性能瓶颈及共享组密钥方法中普遍存在的"1影响*n*"问题。分析表明，采用混合密码体制的新方案在一定程度上兼备了两类不同组密钥管理方法的优势。

关键词 安全多播 组密钥管理 “1影响*n*”问题 后向/前向保密性 抗串谋性

分类号 TP309

A Two-level Decentralized Group Key Management Scheme Based on the Discrete Logarithm Problem

Yang Jun[1,2], Zhou Xian-wei[2]

[1]College of Computer Science and Technology, Southwest University for Nationalities, Chengdu 610041, China; [2]School of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China

Abstract
Based on a public-key encryption algorithm with “multiple decryption keys mapping to one encryption key”, a group re-keying protocol is proposed and then combining the protocol with the LKH algorithm a two-level decentralized group key management scheme is designed for Source Specific Multicast(SSM). Its backward secrecy, forward secrecy and non-collusion with high probability are demonstrated. The performance bottleneck of sub-group managers and the “1-affects-*n*” problem existing universally in the common group key approach are miti-gated through the long-livedness of private keys in the upper level and the method of key translation. The analysis shows that adopting a hybrid cryptosystem the novel scheme possesses some advantages of two distinct classes of approaches to group key management.

Key words Secure multicasting Group Key Management（GKM） n"problem')">"1-affects-*n*"problem Backward Secrecy（BS）/Forward Secrecy（FS） Non-Collusion（NC）

DOI:

通讯作者

作者个人主页 杨 军[1,2]; 周贤伟[2]

扩展功能

本文信息

- Supporting info
- PDF(269KB)
- [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
- 复制索引
- Email Alert
- 文章反馈
- 浏览反馈信息

相关信息

- 本刊中 包含“安全多播”的 相关文章
- 本文作者相关文章
- 杨 军
- 周贤伟