安全技术

一类群组注册协议的设计及其BAN逻辑演绎

陆正福，刘吉庆

(云南大学数学系，昆明 650091)

收稿日期 修回日期 网络版发布日期 2007-1-29 接受日期

摘要 MIKEY是一种可应用于实时的、多媒体通信的群组注册协议的规范。该文分析了MIKEY规范中的密钥生成、分发机制，设计了一个符合MIKEY规范、基于公钥的群组注册协议，最后应用BAN逻辑分析了该协议的安全性。

关键词 MIKEY 密钥管理 注册协议 BAN逻辑

分类号

DOI:

通讯作者:

作者个人主页: 陆正福;刘吉庆