

安全技术

基于分簇的Ad Hoc网络密钥协商协议

张小彬, 韩继红, 王亚弟, 刘敏

(解放军信息工程大学电子技术学院, 郑州 450004)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 以节点的公钥证书为基础, 基于椭圆曲线密码体制提出一种分簇结构的Ad Hoc网络会话密钥协商协议, 对协议的安全性和效率进行分析。该协议满足普遍认可的密钥协商安全要求, 可抵抗中间人攻击、重放攻击、消息伪造攻击等多种攻击, 有效地降低终端的计算、存储能力需求, 减少了协商过程的通信开销。

关键词 [Ad Hoc网络](#); [椭圆曲线密码体制](#); [分簇](#); [密钥协商](#)

分类号 [TP393](#)

DOI:

通讯作者:

作者个人主页: [张小彬](#); [韩继红](#); [王亚弟](#); [刘敏](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(366KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [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“Ad Hoc网络; 椭圆曲线密码体制; 分簇; 密钥协商”的相关文章](#)
- ▶ [本文作者相关文章](#)