

安全技术

基于ECC的无线传感器网络密钥管理协议

蹇波, 郭永辉, 罗长远, 李伟

(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** 针对无线传感器网络在电量、计算能力和内存容量等方面的局限性, 基于椭圆曲线密码体制, 提出一种适用于无线传感器网络的密钥管理协议, 给出通信密钥建立、新节点加入以及节点密钥更新与回收的实现过程。从协议的安全性、抗毁性和效能方面进行性能分析, 实验结果表明该协议具有较强的可扩展性与抵抗攻击能力。

**关键词** [无线传感器网络](#); [密钥管理](#); [椭圆曲线密码体制](#); [密钥回收](#)

分类号 [TP393](#)

**DOI:**

通讯作者:

作者个人主页: [蹇波](#); [郭永辉](#); [罗长远](#); [李伟](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(335KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [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“无线传感器网络; 密钥管理; 椭圆曲线密码体制; 密钥回收”的相关文章](#)
- ▶ [本文作者相关文章](#)