通信学报

Journal on Communications

主管单位:中国科学技术协会 主办单位:中国通信学会

首页 | 期刊简介 | 编委会 | 投稿须知 | 在线订阅 | 资料下载 | 编委论坛

肖俊芳, 曾贵华, 廖 剑. 应用于无线传感器网络的门限环签名方案[J]. 通信学报, 2012, (3):75~81

应用于无线传感器网络的门限环签名方案

DOI:

中文关键词:

英文关键词:

基金项目:

作者

肖俊芳,曾贵华,廖 剑

摘要点击次数:76

全文下载次数: 49

中文摘要:

近年研究完全意义上适应分布式自组织网络的安全机制成为热点。针对节点的能量损耗、通信带宽、存储空间等有严格限制的无线传感器网络环境,基于双线性配对,本文提出门限签名方案。在假设计算Diffie-Hellman问题困难的前提下,利用规约到矛盾的方法给出在随机预言机模型下的严格安全性证明。此外所提的方案具备群合作条件下应有的顽健性,可以进行多签,满足分布式并行计算等特点,非常适应于无线传感器网络。

英文摘要:

查看全文 查看/发表评论 下载PDF阅读器

关闭

版权所有:通信学报 地址:北京东城区广渠门内大街80号通正国际大厦6层602室 电话: 010-67110006-869/878/881 电子邮件: xuebao@ptpress.com.cn 技术支持:北京勤云科技发展有限公司