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



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** **单位**

肖俊芳，曾贵华，廖 剑



**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