

博士论文

基于层次超立方体模型的对偶密钥预置算法

王 雷^{1,2}, 陈治平^{1,2}

(1. 福建工程学院计算机与信息科学系, 福州 350014; 2. 清华大学计算机科学与技术系, 北京 100084)

收稿日期 修回日期 网络版发布日期 2007-5-15 接受日期

摘要 通过所建立对偶密钥, 传感器网络节点之间可使用加密技术进行通信, 从而保障了通信的安全性。在KDC和基于多项式池的密钥预置模型基础上, 提出了一种用于密钥预置的层次超立方体模型及其密钥预置算法。理论与实验分析表明, 与基于多项式和基于多项式池的对偶密钥预置算法相比, 该算法具有更好的安全性能与更高的对偶密钥建立概率。

关键词 [对偶密钥](#) [传感器网络](#) [密钥池](#) [密钥预置](#) [H2模型](#)

分类号 [TP393](#)

DOI:

对应的英文版文章: [071001](#)

通讯作者:

作者个人主页: 王 雷^{1,2};陈治平^{1,2}

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(187KB\)](#)
- ▶ [\[HTML全文\] \(0KB\)](#)
- ▶ [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“对偶密钥”的 相关文章](#)
- ▶ 本文作者相关文章
 - [王 雷](#)
 - [陈治平](#)
 -