

安全技术

模2n加的异或差分概率的快速计算方法

张庆贵

(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 分析模2n加变换的异或差分概率计算算法的计算复杂性, 利用以空间换时间的思想, 将该算法中的矩阵乘积运算预先计算并予以存储, 从而以查表运算替代多个矩阵乘积运算等方法对模2n加变换的异或差分概率计算算法进行改进, 改进后算法的计算复杂性小于现有方法计算复杂性的7.7%。

关键词 [模2n加; 异或差分概率; 快速计算](#)

分类号 [TN918.1](#)

DOI:

通讯作者:

作者个人主页: 张庆贵

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(73KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [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“模2n加; 异或差分概率; 快速计算”的 相关文章](#)
- ▶ [本文作者相关文章](#)