

安全技术

阶数为2的pq周期广义割圆序列的自相关值

白恩健^{1,2}, 刘晓娟³

(1. 东华大学信息科学与技术学院, 上海 201620; 2. 信息安全国家重点实验室, 中国科学院研究生院, 北京 100039; 3. 上海电力学院数理系, 上海 200090)

收稿日期 修回日期 网络版发布日期 2007-9-28 接受日期

摘要 给出了关于阶数为2的pq周期广义割圆序列自相关值的几个猜想, 这类序列是由Ding和Helleseth构造的, 大量的实验结果验证了猜想的正确性, 但没有找到理论证明的方法。结果表明这类序列的自相关值为5-, 4-或3-值, 序列具有“好”的自相关性质, 而且这类序列也具有大的线性复杂度, 可以作为流密码中的密钥流序列或作为随机数发生器。

关键词 [序列](#) [广义割圆类](#) [自相关值](#)

分类号 [TP309](#)

DOI:

通讯作者:

作者个人主页: 白恩健^{1,2}; 刘晓娟³

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(101KB\)](#)
- ▶ [\[HTML全文\] \(0KB\)](#)
- ▶ [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“序列”的 相关文章](#)
- ▶ 本文作者相关文章
- [白恩健^{1,2}, 刘晓娟³](#)