

博士论文

周期为 $p \equiv 7 \pmod{8}$ 的一类新六次剩余序列的迹表示

杜小妮<sup>1,2</sup>, 肖国镇<sup>1</sup>

(1. 西安电子科技大学ISN国家重点实验室, 西安 710071; 2. 西北师范大学数学与信息科学学院, 兰州 730070)

收稿日期 修回日期 网络版发布日期 2007-3-28 接受日期

摘要 构造了一类新的周期为素数  $p$  的六次剩余序列, 利用有限域和差集理论给出了该序列在周期为素数  $p$  情形下的迹函数表示。新序列的线性复杂度为  $\frac{p-1}{2}$ , 优于Hall六次剩余序列在相同条件下的线性复杂度。

关键词 [流密码](#) [迹函数](#) [六次剩余序列](#)

分类号

DOI:

通讯作者:

作者个人主页: [杜小妮<sup>1,2</sup>;肖国镇<sup>1</sup>](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(173KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [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“流密码”的 相关文章](#)
- ▶ 本文作者相关文章
- [杜小妮<sup>1,2</sup>, 肖国镇<sup>1</sup>](#)