计算机工程 2007 33 (07): 21-22 ISSN: 1000-3428 CN: 31-1289/TP

博士论文

周期为p 7(mod 8)的一类新六次剩余序列的迹表示

杜小妮1,2，肖国镇1

(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 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 情形下的迹函数表示。新序列的线性复杂度为 ，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1;2;肖国镇1