计算机工程 2010 36 (5): 137-139,142 ISSN: 1000-3428 CN: 31-1289/TP 首页 当期目录 上一期

安全技术

新的二元互素序列的迹表示和线性复杂度

闫统江1，李淑清2

(1. 中国石油大学数学与计算科学学院，东营 257061；2. 中国石油大学计算机与通信工程学院，东营 257061)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 利用周期分别为奇素数p 和q的Legendre序列构造大量新的周期为 的二元序列，根据这些序列与Legendre序列在结构上的联系，给出它们的迹表示，依据E.L. Key方法得到其线性复杂度。结果表明该类序列具有良好的符号平衡性和线性复杂度性质，作为密钥流序列可抵抗Berlekamp-Massey算法的攻击。

关键词 流密码；Legendre序列；Jacobi序列；迹表示；线性复杂度

分类号 TN918.1

DOI:

通讯作者:

作者个人主页: 闫统江1;李淑清2