计算机工程 2010 36 (4): 150-151 ISSN: 1000-3428 CN: 31-1289/TP 首页 当期目录 上一期

安全技术

6阶W-广义割圆序列的线性复杂度

李淑清1，闫统江2

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

收稿日期 修回日期 网络版发布日期 接受日期

摘要 在所有周期为pq的2k阶W-广义割圆序列的线性复杂度都已经得到准确计算的基础上，考虑周期为pq的6阶W-广义割圆序列的线性复杂度。结果表明这类序列的线性复杂度的下界是 。从密码学的角度看，多数的二元W-广义割圆序列具有良好的线性复杂度性质，以它们做密钥流序列的密码系统具有很强的抵抗B-M算法攻击的能力。

关键词 流密码；割圆类；割圆序列；线性复杂度

分类号 TN918.4

DOI:

通讯作者:

作者个人主页: 李淑清1;闫统江2