电子与信息学报
JOURNAL OF ELECTRONICS & INFORMATION TECHNOLOGY

电子与信息学报 » 2014, Vol. 36 » Issue (3) :650-654 DOI: 10.3724/SP.J.1146.2013.00751

一类新的周期为2*pq*的二元广义分圆序列的线性复杂度

李瑞芳 柯品惠*

福建师范大学网络安全与密码技术福建省重点实验室 福州 350007

The Linear Complexity of a New Class of Generalized Cyclotomic Sequence with Period

Li Rui-fang Ke Pin-hui*

Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China

摘要 该文提出一类新的周期为2*pq*, *p*和*q*为不同奇素数的广义分圆序列，并给出了该序列线性复杂度的计算公式。在已知序列支撑集的情况下，利用该公式可以得到该序列线性复杂度的精确值。

关键词： 密码学 有限域 广义分圆序列 线性复杂度

Abstract： A new class of generalized cyclotomic sequence with period 2*pq* is proposed in this paper, where *p* and *q* are distinct primes. A formula for computing the linear complexity of the proposed sequence is also given. With the knowledge of the support set of the generalized cyclotomic sequence, its linear complexity can be easily determined using the formula.

Keywords： Crpytography Finite fields Generalized cyclotomic sequence Linear complexity

Received 2013-05-27;

本文基金:

国家自然科学基金(61102093)资助课题

通讯作者: 柯品惠： 男，1978年生，副教授，主要研究方向包括序列设计、现代密码学中的布尔函数. Email: keph@fjnu.edu.cn

引用本文:

李瑞芳, 柯品惠.一类新的周期为2*pq*的二元广义分圆序列的线性复杂度[J] 电子与信息学报, 2014,V36(3): 650-654

Li Rui-Fang, Ke Pin-Hui.The Linear Complexity of a New Class of Generalized Cyclotomic Sequence with Period[J] , 2014,V36(3): 650-654

链接本文:

http://jeit.ie.ac.cn/CN/10.3724/SP.J.1146.2013.00751 或 http://jeit.ie.ac.cn/CN/Y2014/V36/I3/650