计算机工程与应用 2009 45 (13): 90-92 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

GMW-序列的三项生成多项式

祁传达[1], 李 刚[2]
1.信阳师范学院 数学与信息科学学院，河南 信阳 464000
2.信阳师范学院 计算机与信息技术学院，河南 信阳 464000

收稿日期 2008-10-6 修回日期 2008-11-14 网络版发布日期 2009-4-27 接受日期

摘要 研究了GMW-序列的三项生成多项式问题，给出了其三项生成多项式的结构和计数，证明了其三项生成多项式个数远远少于同周期的*m*-序列，这说明GMW-序列在抵抗快速相关攻击的能力方面要强于同周期的*m*-序列。

关键词 GMW-序列 *m*-序列 自相关函数 迹函数
分类号

Generation trinomials of GMW-sequences

QI Chuan-da[1],LI Gang[2]

1.College of Mathematics and Information Science，Xinyang Normal University，Xinyang，Henan 464000，China
2.College of Computer and Information Technology，Xinyang Normal University，Xinyang，Henan 464000，China

Abstract
The problem of generation trinomials for GMW-sequences is studied.The structure and count of generation trinomials for GMW-sequences is presented.It is proved that the amount of generation trinomials for GMW-sequences is less than *m*-sequences with the same period.It is explained that intensity of GMW-sequences resist the fast correlation attacks is greater than *m*-sequences with the same period.

Key words GMW sequences m-sequences auto-correlate function trace function

DOI: 10.3778/j.issn.1002-8331.2009.13.027

通讯作者 祁传达