电子与信息学报 2009 31 (12): 2897-2900 ISSN: 1009-5896 CN: 11-4494/TN

论文

本原σ-LFSR序列的线性复杂度研究

刘向辉,曾 光, 韩文报

解放军信息工程大学信息工程学院 郑州 450002

收稿日期 2008-12-15 修回日期 2009-4-27 网络版发布日期 2009-12-4 接受日期

摘要
线性复杂度是衡量密钥流序列安全性的重要参数。该文考察了有限域上*n*级本原σ–LFSR序列的线性复杂度性质。首先得到了它的上下界并证明了界是紧致的，然后利用序列的根表示给出了计算本原σ–LFSR序列线性复杂度的方法。

关键词 序列密码 σ-本原线性反馈移位寄存器 线性复杂度 根表示

分类号 TN918.1

Research on Linear Complexity of Primitive σ-LFSR Sequences

Liu Xiang-hui,Zeng Guang,Han Wen-bao

Information Engineering Institute, PLA Information Engineering University, Zhengzhou 450002, China

Abstract
Linear complexity is an important parameter of sequences' security. In this paper, the linear complexity properties of primitive σ-LFSR sequences are studied. Firstly, the bounds of the linear complexity for one n stages primitive σ-LFSR sequence is given and it is proved that the bounds are tight; then, with the tool of root representation, a method to get the linear complexity of one primitive LFSR sequence is obtained.

Key words Stream cipher Primitive σ-LFSR(Linear Feedback Shift Register) Linear complexity Root representation

DOI:

通讯作者

作者个人主页 刘向辉;曾 光; 韩文报