

安全技术

本原s-LFSR的计数研究

刘向辉, 张 猛, 韩文报, 曾 光

(解放军信息工程大学信息研究系, 郑州 450002)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 针对s-LFSR能够充分利用现代通用CPU且具有结构简单、适合软件快速实现的特点, 利用本原s-LFSR的距离向量和基判别定理, 将本原s-LFSR的计数问题转化为线性空间上基的问题, 以此为基础, 利用 F_2 上次数小于 n 的互素多项式的对数解决 F_4 上本原s-LFSR的计数问题。

关键词 [序列密码](#); [本原s-LFSR](#); [基判别定理](#); [计数](#)

分类号 [TN918.1](#)

DOI:

通讯作者:

作者个人主页: [刘向辉](#); [张 猛](#); [韩文报](#); [曾 光](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(85KB\)](#)
- ▶ [\[HTML全文\] \(0KB\)](#)
- ▶ [参考文献 \[PDF\]](#)
- ▶ [参考文献](#)

服务与反馈

- ▶ [把本文推荐给朋友](#)
- ▶ [加入我的书架](#)
- ▶ [加入引用管理器](#)
- ▶ [引用本文](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

相关信息

- ▶ [本刊中 包含“序列密码; 本原s-LFSR; 基判别定理; 计数”的相关文章](#)
- ▶ [本文作者相关文章](#)