计算机工程 2009 35 (18): 154-155 ISSN: 1000-3428 CN: 31-1289/TP 首页 当期目录 上一期

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F2上次数小于n的互素多项式的对数解决F4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