

安全技术

GF(2m)上的快速模约减算法

段 斌, 马自堂

(解放军信息工程大学电子技术学院, 郑州 450004)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 针对GF(2m)上的模约减运算问题, 在基于固定三(或五)项式(FTOP)算法的基础上提出一种改进的快速算法。该算法采用动态计算分组字序号和偏移量的方法, 克服FTOP只适用于特定约减多项式的不足。实验结果表明, 当约减多项式项数小于123($m < 719$)时, 该算法速度比一次一位的算法有较大提高, 最大为89%, 平均为30%左右, 当约减多项式为任意三(或五)项式时, 能达到与FTOP相同的速度。

关键词 [有限域; 模约减; 约减多项式; 快速算法](#)

分类号 [TP309](#)

DOI:

通讯作者:

作者个人主页: [段 斌; 马自堂](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(78KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [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“有限域; 模约减; 约减多项式; 快速算法”的 相关文章](#)
- ▶ [本文作者相关文章](#)