计算机工程 2010 36 (06): 140-141 ISSN: 1000-3428 CN: 31-1289/TP 首页 当期目录 上一期

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