计算机工程 2010 36 (8): 158-160 ISSN: 1000-3428 CN: 31-1289/TP 首页 当期目录 上一期 下一期

安全技术

可伸缩双有限域模加减器的研究与实现

张 军1，戴紫彬1，孟 强2，秦 帆1

(1. 解放军信息工程大学电子技术学院，郑州 450004；2. 郑州大学体育学院，郑州 450044)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 在改进通用模加减算法的基础上，实现一种结构优化的模加减器。采用基于字的模加减法统一硬件架构，使该设计具有良好的可扩展性，可以完成素数有限域GF(p)和二进制有限域GF(2m)上任意长度操作数的模加减法运算。该设计引入流水线结构，使其工作效率提高50%~80%，可以应用于各种高性能的椭圆曲线密码协处理器设计中。

关键词 可伸缩；模加减器；双有限域

分类号 TP309

DOI:

通讯作者:

作者个人主页: 张 军1;戴紫彬1;孟 强2;秦 帆1