计算机工程与应用 2009 45 (35): 59-61 ISSN: 1002-8331 CN: 11-2127/TP

研发、设计、测试

GF（2^m）上的一种可并行快速乘法器结构

马自堂[1]，段 斌[2]，刘云飞[2]

1.解放军信息工程大学 电子技术学院，郑州 450004
2.防空兵指挥学院 防空导弹系，郑州 450052

收稿日期 2009-7-7 修回日期 2009-8-26 网络版发布日期 2009-12-16 接受日期

摘要 在可重构的高位优先串行乘法器基础上，提出了一种GF（2^m）上可控制的快速乘法器结构。该乘法器增加了1个控制信号和7个两路选择器，在域宽小于最大域宽的一半时能利用现有硬件资源并行计算两个乘法。该乘法器结构电路复杂度低，能利用现有存储空间并行计算，并能扩展应用于串并混合结构中。这种乘法器适合存储空间小、低硬件复杂度的可重构密码系统VLSI设计。

关键词 超大规模集成电路（VLSI） 乘法器 可重构 椭圆曲线密码

分类号 TN918 TN47]

Fast parallelable multiplier architecture over *GF*（2^m）

MA Zi-tang[1]，DUAN Bin[1]，LIU Yun-fei[2]

1.Institute of Electronic Technology，PLA Information Engineering University，Zhengzhou 450004，China
2.Department of Antiaircraft，PLA Aerial Defense Force Command Academy，Zhengzhou 450002，China

Abstract

A fast parallelable multiplier architecture over *GF*（2^m） is presented based on the reconfigurable most significant bit serial multiplier.One control signal and six two-way muxes are added in the multiplier，and it can use the fixed hardware resource to compute two multiplication parallelly，when the field length is less than half of the maximum.The proposed multiplier architecture has low circuit complexity and low power cost.It can use limited registers to accelerate computing，and also can be applied to the serial-parallel architecture.It suits the VLSI design of reconfigurable cryptographic applications with limited storage and low hardware complexity.

Key words Very Large Scale Integrated Circuits（VLSI） multiplier reconfigurable elliptic curve cryptogaphy

DOI: 10.3778/j.issn.1002-8331.2009.35.019

通讯作者 马自堂 330564332@qq.com