计算机工程与应用 2007 43-12 (12): 91-93 ISSN: 1002-8331 CN: 11-2127/TP

产品、研发、测试

GF(2^m)域上通用可配置乘法器的设计与实现

卫学陶 戴紫彬 陈韬

解放军信息工程大学电子技术学院301教研室 解放军信息工程大学电子技术学院 信息工程大学电子技术学院

收稿日期 2006-5-8 修回日期 网络版发布日期 2007-4-19 接受日期

摘要 摘 要：本文提出了一种应用于椭圆曲线密码体制中的有限域乘法器结构，基于已有的digit-serial结构乘法器，利用局部并行的bit-parallel结构，有效的省去了模约简电路，使得乘法器适用于任意不可约多项式；通过使用数据接口控制输入数据的格式并内嵌大尺寸乘法器，可以配置有限域乘法器的结构，用以实现基于多项式基的有限域乘法运算。该结构可以有效满足椭圆曲线密码体制的不同安全需求。

关键词 有限域,GF(2m) ,乘法器

分类号

A Design and Implementation of Versatile and Reconfigurable Multiplier over GF(2m)

Abstract

Abstract: A finite field multiplier architecture is proposed in this paper for ECC. Based on previous digit-serial multiplier architecture, we used bit-parallel architecture of local parallel to eliminate reduction modulo circuit effectively, and the multiplier architecture also be the same with arbitrary irreducible polynomials. We controlled data format of import by data interface and embedded multiplier of most size, that can configure architecture of finite field multiplier to carry out multiplication operation base on polynomial base. A multiplier is proposed in this paper able to satisfy different security demand of ECC.

Key words Galois field GF(2m) multiplier

DOI:

通讯作者 卫学陶 ahtoh2000@163.com