电子与信息学报 2006 28 (4): 717-720 ISSN: 1009-5896 CN: 11-4494/TN

论文

一种可重构的快速有限域乘法结构

袁丹寿,戎蒙恬

上海交通大学电子工程系 上海 200030

收稿日期 2004-6-3 修回日期 2004-9-9 网络版发布日期 2007-12-5 接受日期

摘要

在一种改进的串行乘法器的基础上，提出了一种可重构的快速有限域GF（2^m）($1<m\leq M$)乘法器结构。利用一组配置信号和逻辑电路来改变有限域的度m，使得乘法器可以重构和编程。同时采用“门控时钟”减小电路功耗。该乘法器结构具有可重构性、高灵活性和低电路复杂性等特点。与传统的移位乘法器相比，它将乘法器速度提高一倍。这种乘法器适合于变有限域，低硬件复杂度的高性能加密算法的VLSI设计。

关键词 VLSI 有限域 乘法器 可重构 椭圆曲线密码

分类号 TN918 TN47

Reconfigurable and Fast Finite Field Multiplier Architecture

Yuan Dan-shou, Rong Meng-tian

Dept of Electronic Engineering, Shanghai Jiaotong Univ., Shanghai 200030, China

Abstract

A reconfigurable and fast architecture over Galois field GF (2^m)($1<m\leq M$) is presented based on the improved serial multiplier. The value m, of the irreducible polynomial degree, can changed by adding a set of configuring signals and logic circuits, which results in that the multiplier architecture is reconfigurable and programmable without changing the hardware. The proposed multiplier architecture has high order of flexibility and low hardware complexity. Compared with the traditional serial multiplier, it can obtain twice speed-up. It suits high-security cryptographic applications with variable finite fields and low complexity requirements.

Key words VLSI Finite field Multiplier Reconfigurable Elliptic curve cryptosystems

DOI:

通讯作者

作者个人主页 袁丹寿;戎蒙恬