高速可伸缩 Montgomery 模除器设计技术研究

赵宗国[1]，李　伟[1,2]，戴紫彬[1]

（1 解放军信息工程大学，河南 郑州 450000）

（2 复旦大学 专用集成电路与系统国家重点实验室，上海 201203）

摘　要：为解决传统方式计算模除周期数过长、灵活性太差的问题，提出了一种基于原始 Montgomery 模逆算法的高效 Montgomery 模除算法. 该算法相比于模逆-模乘方式计算模除可减少34％的循环次数. 基于该算法设计了同时支持素数域 GF(p)和二进制域 GF(2^n)的模除器硬件结构. 在 CMOS 0.18 μm typical 工艺库下综合，时钟频率可以达到270 MHz. 与原始 Montgomery 模除运算相比，本设计可支持576 bit 以内任意长度、单次模除运算需要的时钟周期数可减少15％；与模逆-模乘方式相比，模除速度提高了45％.

关键词：椭圆曲线加密算法；模除器；双域；高速

中图分类号：TP309.7　　**文献标识码**：A　　**文章编号**：1000－7180(2015)12－0026－05

The Design Technologyof High-speed Scalable Montgomery Modular Division Device

ZHAO Zong-guo[1]，LI Wei[1,2]，DAI Zi-bin[1]

（1 PLA Information Engineering University，Zhengzhou 450000，China；
2 State Key Laboratory of Special Integrated Circuit and System，Fudan University，Shanghai 201203，China）

Abstract：To solve the problem of long cycle of calculation modular division with traditional way，in this paper，an improved Montgomery modular division algorithm is proposed based on the original Montgomery modular inversion algorithm. The algorithm compared calculation with modular inversion-division way can reduce 34％ cycle. A modular division device is designed to operate in both finite fields GF(p) and GF(2^n) based on the proposed algorithm. We synthesize the modular division device under 0.18 μm CMOS technology and the clock frequency can reach 270 MHz. Compared with original Montgomery division，the design can support the calculation below 576 bits and can reduce 15％ cycle calculating modular division. Comparing with modular inversion-division way，45％ speed of modular division faster can be accelerated.

Key words：elliptic curve cryptography；montgomery modular division device；dual field；high speed

作者简介：

赵宗国　男，(1990-)，硕士研究生. 研究方向为安全专用芯片设计. E-mail：zhaozongguo9302@163.com.

李　伟　男，(1983-)，博士研究生，讲师. 研究方向为专用集成电路设计.

戴紫彬　男，(1966-)，博士，教授. 研究方向为专用集成电路设计、芯片可重构设计.

收稿日期：2015－02－08；**修回日期**：2015－04－01

基金项目：国家自然科学基金(61404175)