

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 Technology of High-speed Scalable Montgomery Modular Division Device

ZHAO Zong-guo¹, LI Wei^{1,2}, DAI Zi-bin¹

(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

1 引言

ECC 公钥密码体现的高计算安全性、低存储空间及带宽需求等特点^[1-2], 使其具有良好的应用前景, 目前已广泛应用于可穿戴设备及智能卡等计算资源受限的实际应用中, 逐渐成为新一代公钥密码标准. 点乘是 ECC 算法的核心运算, 但是, 在做点乘运算时往往需要对坐标进行变换. 例如: 二元域 GF

(2^n) 下的点乘算法通常是变换到 LD 坐标系下进行运算的; 素数域 $GF(P)$ 下点乘中的倍点运算通常是在雅克比坐标下运算的, 点加通常是在雅克比-仿射混合坐标系下进行运算的. 这些运算的共同特点就是在运算完成后需要转换到普通坐标系下, 并且在转换时都需要用到模除运算. 例如: 素数域 $GF(P)$ 雅克比坐标系下投影点 $(X : Y : Z)$ 对应仿射点 $(X/Z^2, Y/Z^3)$, 二元域 $GF(2^n)$ 在 LD 坐标系下投

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)

影点($X : Y : Z$)对应仿射点($X/Z, Y/Z^2$). 目前, 模除运算的实现方式有模逆-模乘方式和原始 Montgomery 模除^[3]方式. 模逆-模乘方式实现模除运算时的优势是不需要独立的模除单元, 但是模除周期太长, 不利于 ECC 算法的实现. 原始 Montgomery 模除方式实现模除运算时的优势是电路面积消耗小, 但电路延迟大. 以上电路共同的缺点是灵活性和可扩展性差.

针对以上面临的问题, 结合原始的 Montgomery 模除算法特点, 本文提出了一种改进的 Montgomery 模除算法, 基于该算法设计的模除器, 扩展性高、灵活性强、实现模除周期数少. 支持二元域 $GF(2^n)$ 、素数域 $GF(P)$ 下的模除运算, 且运算长度可配置, 相比较于模逆-模乘方式实现模除, 运算周期数可减少 45%. 与原始 Montgomery 模除方式相比, 运算周期数可减少 15%.

2 改进的 Montgomery 模除算法

2.1 传统的 Montgomery 模逆算法

对于一个给定的 n -bit 素数 p , 和一个 Montgomery 常量 $r=2^n \pmod{p}$, 则整数 a 对应于蒙域下的 $A=a \cdot r \pmod{p}$. 对应的两个蒙域下的整数 A 和 B 的 Montgomery 乘法运算如算法 1 所示.

算法 1: Montgomery 模乘算法^[4]

Input: $A \equiv ar \pmod{p}, B \equiv br \pmod{p}, p, n$;
Output: $C = \text{MonMul}(A, B)$
 $\equiv ABr^{-1} \pmod{p} \equiv abr \pmod{p}$;
1. Let $A = (A_{n-1}, A_{n-2}, \dots, A_1, A_0)_2, C = 0$
2. For i from 0 to $n-1$ do
 $\{T = (C + A_i B), C = \frac{T + T_0 P}{2}\}$
3. If $C \geq p$, then $C = C - p$
4. Return C

为了实现 Montgomery 模逆运算, Kaliski 提出了一种循环式的模逆算法, 具体算法如算法 2 所示.

算法 2: 原始 Montgomery 模逆算法^[5]

Input: b, p ;
Output: $R, k, R = b^{-1} 2^n \text{Mod } p, n \leq k \leq 2n$;
1. $u = p, v = b, R = 0$, and $s = 1$,
2. $k = 0$,
3. while ($v > 0$)
4. if u is even then
 $u = u/2, s = 2s$;
5. else if v is even then
 $v = v/2, R = 2R$;
6. else if $u > v$ then

$u = (u - v)/2, R = R + s, s = 2s$;
7. else then
 $v = (v - u)/2, s = s + R, R = 2R$;
8. $k = k + 1$;
9. if $R \geq p$ then $R = R - p$;
10. else then $R = p - R$;
11. for $i = 1$ to $k - n$ do
12. if $R_0 = 0$ then $R = R/2$ else
13. $R = (R + p)/2$
14. return R

2.2 改进的 Montgomery 模除算法

传统方式要实现模除运算, 需要先通过算法 2 计算模逆, 然后通过算法 1 进行一步模乘运算. 通过分析可知, 完成算法 2 运算需要大约 $n \sim 3n$ 个循环周期, 完成算法 1 运算大约需要 n 个循环周期, 即完成一次模除运算大约需要 $2n \sim 4n$ 个循环周期. 针对此种情况, 本文提出了一种改进的双域模除算法, 如算法 3 所示. 该算法对 Kaliski 的模逆算法进行了改进, 具体表现: (1) 将算法 1 和算法 2 进行了统一; (2) 通过判断最低位是否为“0”, 且以 3 位作为步长进行判断, 替代算法 2 的步骤 4、5 判断辅助参数 u 、 v 的奇偶, 从而减少算法循环迭代次数; (3) 在硬件映射上, 基于字的多精度减法运算代替算法中复杂的大数比较运算, 实现两个大数的比较. 通过以上三点改进之后, 算法整体循环迭代次数可降低近 45%, 非常有利于 ECC 算法的实现.

算法 3: 改进的 Montgomery 模除算法

Input: $A \equiv ar \pmod{p}, B \equiv br \pmod{p}, p, n$.
Output: $R \equiv ab^{-1} r \pmod{p}$.
1. $u = p; v = B; R = 0; s = A$;
 $x = 0; y = 0; z = 0; k = 0$.
2. while ($v > 0$) do {
If ($u_{2..0} = 000$), $\{u = u/8; s = 8s; k = k + 3\}$;
else if ($u_{2..0} = 100$), $\{u = u/4; s = 4s; k = k + 2\}$;
else if ($u_{2..0} = 110$), $\{u = u/2; s = 2s; k = k + 1\}$;
else if ($v_{2..0} = 000$), $\{v = v/8; R = 8R; k = k + 3\}$;
else if ($v_{2..0} = 100$), $\{v = v/4; R = 4R; k = k + 2\}$;
else if ($v_{2..0} = 110$), $\{v = v/2; R = 2R; k = k + 1\}$;
else $\{\epsilon_1 = 0, \epsilon_2 = 0, \epsilon_3 = 0$;
 $(\epsilon_1, x) = u - v - \epsilon_1$;
 $(\epsilon_2, y) = v - u - \epsilon_2$;
 $(\epsilon_3, z) = R + s + \epsilon_3$;
If ($\epsilon_1 = 0$) $\{u = x/2; R = z; s = 2s; k = k + 1\}$;
else $\{s = z; v = y/2; R = 2R; k = k + 1\}$;
 $\}$
If ($r \geq p$) $\{R = R - p\}$;
If ($r \geq p$) $\{s = s - p\}$;

```

}
3. for  $i = 1$  to  $k - n$  do{
  If( $R_0 = 0$ ) { $R = R/2$ }
  else { $R = (R + p)/2$ }
}
4.  $R = p - R$ 
5. return  $R$ 

```

该算法是基于素数域 $GF(p)$ 的,但是其也可以扩展到二元域 $GF(2^n)$ 中,只是在运算上二元域与素数域的区别体现是:二元域 $GF(2^n)$ 的加法运算为异或操作,不产生进位。

2.3 算法理论分析

考虑算法 2 中 u, s 或 v, R 的移位操作依赖于 u, v 寄存器的值的奇偶即其最低有效位 (u_0, v_0), 若其最低有效位为 0, 则对 u, s 或 v, R 进行移位一次。如果 u 的最低五位有效位为 0 的话, 那么连续执行 5 轮迭代才能完成对 u 的移位操作。

表 1 平均循环迭代次数 (i)

x	概率表达式	i
1	$(1 - p_0)k + p_0k$	$1.00k$
2	$(1 - p_0)k + p_0[(1 - p_0)k + p_0k/2]$	$0.88k$
3	$(1 - p_0)k + p_0[(1 - p_0)k + p_0((1 - p_0)k/2 + p_0k/3)]$	$0.85k$
4	$(1 - p_0)k + p_0[(1 - p_0)k + p_0((1 - p_0)k/2 + p_0[(1 - p_0)k/3 + p_0k/4])]$	$0.849k$
5	$(1 - p_0)k + p_0[(1 - p_0)k + p_0((1 - p_0)k/2 + p_0[(1 - p_0)k/3 + p_0((1 - p_0)k/4 + p_0k/5)])]$	$0.847k$

通过表格可以看出,在当 $x = 3$ 之后,平均循环迭代次数不再有明显的减小,此时可以将平均循环迭代次数降低 15% 左右,因此本文改进算法采用一次最多移位 3 比特。

本文提出的高效算法中还将原始的 Montgomery 模逆算法修改为 Montgomery 模除算法,但是其改进是依据算法 2 中步骤 3 中

$$\begin{cases} BR \equiv -u2^i \pmod{p} \\ Bs \equiv v2^i \pmod{p} \end{cases}$$

的运算进行的。在算法 3 中,通过设置 (u, v, R, s) 的初始值为 $(p, B, 0, A)$, 影响了步骤 2 中的

$$\begin{cases} A^{-1}BR \equiv -u2^i \pmod{p} \\ A^{-1}Bs \equiv v2^i \pmod{p} \end{cases}$$

因为初始的 (u, v) 的值是相关的素数,所以经过最后一次循环后, (u, v) 的值都变成了 1, 等完成算法 3 中整个步骤 2 的循环之后, (u, v, R, s) 变成了 $(1, 0, -AB^{-1}2^i \pmod{p}, 0)$ 。因此必须保证整个循环中 (R, s) 的值必须一直在 $\{0, 1, \dots, p-1\}$ 的范围内^[6], 所以在步骤 2 中相对于算法 2 增加了对 (R, s) 的约减操作。最后, 本文改进的 Montgomery

在硬件电路中,映射完成移位操作时,多比特联合移位完全可以一次完成。根据 u, v 寄存器中最低有效位 0 的个数,可以考虑一次移位 2 bit、3 bit 甚至更多。但是,由于在计算过程中 u, v 的值在不断地变化,所以需要对 u, v 值连续 0 的个数的期望进行判断,确定最合适的联合移位比特数目。

假设一次移位比特数目为 x , 那么总共循环移位次数概率表达式可以表示成如表 1 描述的形式。

其中, $(1 - p)k$ 项表示用于加 / 减运算的循环迭代次数,通过不同的 x 的值的变化的可以得知,最大移位数目 $(1 - p)k$ 项的的影响;多比特移位的影响由其他项考虑。总的循环迭代次数 k 主要受一次移位比特数目的影响;其他项则考虑了多比特移位的影响。总的迭代次数 k 应该受一次移位比特数目的影响,平均迭代次数 i 如表 1 所示。

算法仅需要 $n \sim 3n$ 个循环周期,不再需要算法 1 的模乘运算,相比于采用传统方式进行模除运算减少近 34% 的循环次数。通过以上两点对算法的改进,本文提出的模除算法能够提高大约 45% 的性能。

3 算法的硬件实现

3.1 模除器整体硬件实现

根据对算法 3 进行硬件结构分析,模除器硬件实现整体电路结构如图 1 所示。电路采用了 192 位数据路径,其最大运算长度在 576 位以内可配置。主要构成单元有模除运算电路、状态机控制电路、数据输入单元、数据输出单元及计数器电路。整个电路的输入接口模块由数据输入单元构成,其主要完成态机的控制下外部数据注入到内部模除运算中的寄存器;整个电路的核心控制器是状态机控制电路,其主要协调控制整个模除运算的操作。电路的核心运算模块是模除运算电路,其主要由运算电路和内部寄存器所构成,在状态机控制下完成模除运算。计数器电路完成 K 值的计数输出;最后数据输出单元是整个电路的输出接口,负责将运算结果输出。

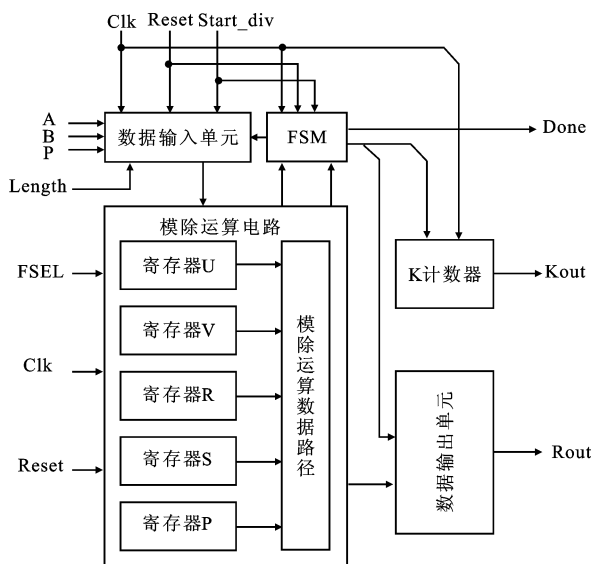


图 1 双域模除器的整体硬件结构

3.2 模除器内部电路实现

为提高模除运算的速度,电路内部的运算单元采用了并行处理机制,U、V、R、S等模除运算中间变量的值以及ROUT得值可以在同一时刻计算得到.图2给出了U/V值运算电路结构.

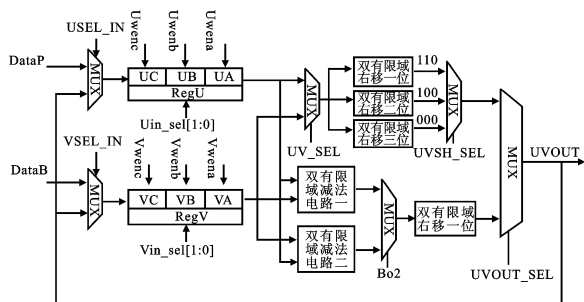


图 2 U/V 值运算电路硬件结构

图2中双有限域减法电路可以实现两个有限域上的减法运算和两个数的比较运算. 为了实现一次对192比特的数据进行计算, 本设计采用了6个32比特的字减法器串接. 且本设计采用了借位预计算的方式串接多个32比特字级减法器. 多级字减法器的计算结果可以在同一时刻得到, 并且每级字减法器针对两种借位情况预先分别计算两种结果. 第一级的字减法器计算产生结果时, 同时产生正确的借位信号, 第二级字减法器的两个计算结果的数据选择信号, 则由该借位选择信号充当; 同理, 在相同时刻, 第三级字减法器的两个计算结果的数据选择信号, 由第二级字减法器的正确借位值充当, 最后一级字减法器的两个计算结果的数据选择信号, 由倒数第二级字减法器的正确借位值充当. 以此方式最终

串接完成六级 32 比特字级减法器。如果计算数据的长度超过 192 比特,那么,第一级字减法器也需要预先计算两种结果,并且由第六级字减法器的借位选择信号选择第一级的正确结果,进行第二轮的计算。因此 192 比特减法器的延时就缩短至一级 32 比特字级减法器的延时与 6 级数据选择器的延时的总和,大大减小了数据路径的延时。图 3、图 4 分别表示双有限域减法模块和双有限域字减法器电路。

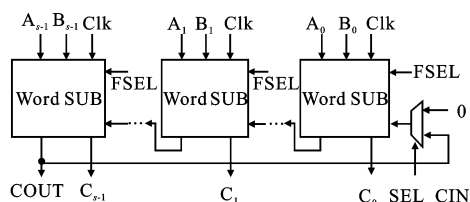


图 3 双有限域减法电路硬件结构

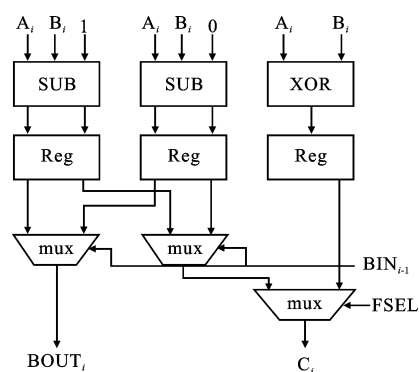


图 4 双有限域字减法器电路硬件结构

4 电路性能分析

4.1 结构性能分析

考虑到 NIST 推荐的有限域长度,并根据以上对模除算法结构的分析,在设计可配置模除电路时,本文设计的双有限域加减法电路中均设置了 6 个字级的加/减法子电路,且 U、V 寄存器分别由 3 个 192 比特长度寄存器组成.这样两种有限域的模除运算电路均支持 576 比特以内任意长度.将以上设计的模除器用 VerilogHDL 硬件语言进行代码描述.在功能仿真正确后,在 CMOS 0.18 μm 工艺库下进行综合.采用改进的算法结构模除单元实现结果如表 2 所示.

表 2 基于改进算法的模除器实现结果

实现功能	资源消耗/m ²	电路延迟/ns
双域模除	528 743	3.7

4.2 结构性能扩展

分别对不同数据位宽二元域/素数域周期在 CMOS 0.18 μm 工艺下进行期望统计,得到本架构在不同数据位宽下的性能扩展趋势,如图 5 所示:

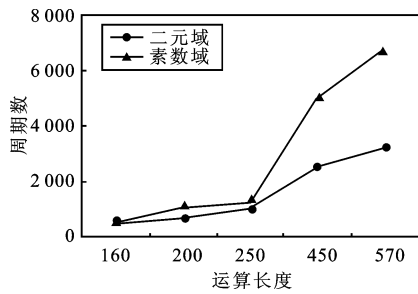


图 5 模除周期数走势

4.3 结构性能对比

表 3 中列出了本设计与其他文献的一些比较结果. 文献[7]中可完成 480 bit 以内双域下的任意模除运算,通过表 3 可以看出在 192 bit 长度下完成模除周期数本设计比文献[7]减少 51.7%;在 224 bit 长度下完成模除周期数本设计比文献[7]减少 52.9%;在 256 bit 长度下完成模除周期数本设计比文献[7]减少 58.5%;在 480 bit 长度下完成模除周期数本设计比文献[7]减少 46.1%,并且电路时钟频率提高 27.4%;虽然本设计面积消耗比文献[7]大,但是这是由于本设计扩展宽度造成的,通过估算,若本设计位宽缩减到 480 bit,面积基本能够与文献[7]持平. 文献[8]中仅能完成 160~512 bit 以内的任意模逆运算. 但是通过表 3 中的对比,可看出在 256 bit 数据长度下,本文比文献[8]减少 130 个循环周期,并且本文的时钟频率比文献[8]提高了 20 MHz,面积减少了 37%.

表 3 模除运算单元性能比较

设计	数据长度/ bit	工艺库/ μm	周期数	时钟频率/ MHz	门/ kgate
本文	192(GF(p))	0.18	781	270	52
	224(GF(p))		1 008		52
	256(GF(p))		1 150		52
	480(GF(p))		4 978		52
	576(GF(p))		6 716		52
文献 [7]	192(GF(p))	0.18	1 614	212	37
	224(GF(p))		2 140		37
	256(GF(p))		2 767		37
	480(GF(p))		9 220		37
	576(GF(p))				
文献 [8]	192(GF(p))	0.18	576	250	82
	224(GF(p))		1 120		82
	256(GF(p))		1 280		82

5 结束语

本文在提出了一种高效 Montgomery 模除算法的基础上,设计并实现完成了双域模除运算单元. 本文设计的模除运算单元不仅具有运算长度可配置功能,而且在时钟周期数和运算速度方面各有优势. 同时,能较好支持椭圆曲线密码算法中 576 位长度以内的有限域模除运算,具有较高的灵活性,为各种流行的可穿戴设备及各种无线终端设备用户高性能的信息安全加密服务提供了便利.

参考文献:

- [1] Miller V S. Use of elliptic curves in cryptography [C]//Proc. of CRYPTO'85. Berlin: Springer-Verlag, 1986: 417-426.
- [2] Koblitz N. Elliptic curve cryptosystems [J]. Mathematics of computation, 1987, 48(4): 203-209.
- [3] Bajard J C, Kaihara M, Plantard T. Selected RNS bases for modular multiplication[C]// IEEE computer society. Portland, 2009(20): 25-32.
- [4] Yang Xiaohui. Design and implementation of dual-field modular inversion algorithm[J]. Journal of Electronics, 2010,27(4):531-537.
- [5] Lee Jenwei. A 521-bit dual-field elliptic curve cryptographic processor with power analysis resistance[C]// 2010 ESSCIRC. Seville, IEEE, 2010:206-209.
- [6] Montgomery P L. Modular multiplication without trial division [J]. Mathematics of Computation, 1985, 170 (44): 519-521.
- [7] 曹丹,韩军,陈媛,等.可扩展的低成本双域模乘模除器算法及其 VLSI 实现[J]. 小型微型计算机系统, 2009, 30(5):1008-1012.
- [8] Yang Xiaohui, Yang Tongjie, Dai Zibin, et al. Design and implementation of dual-field modular inversion algorithm[J]. Journal of Electronics, 2010, 27(4): 532-537.

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.