◎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]
MA Zi-tang[1],DUAN Bin[1],LIU Yun-fei[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
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
E-mail:330564332@qq.com

MA Zi-tang,DUAN Bin,LIU Yun-fei.Fast parallelable multiplier architecture over $GF(2^m)$.Computer Engineering and Applications,2009,45(35):59-61.

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

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
DOI:10.3778/j.issn.1002-8331.2009.35.019 **文章编号**:1002-8331(2009)35-0059-03 **文献标识码**:A **中图分类号**:TN918;TN47

1 引言

有限域在密码学领域有着广泛的应用。在公钥密码RSA和ECC等算法设计中,有限域乘法运算是最重要的一种运算。乘法运算的速度会对算法整体速度有很大影响,因此,设计复杂性低、速度快的乘法运算算法和乘法器结构对提高加解密运算速度非常重要。

乘法器按实现结构的不同可分为三类,一是反复式乘法器(Iterative Structure Multiplier)即移位累加乘法器,二是阵列式乘法器(Array Structure Multiplier),三是树状结构乘法器(Tree Structure Multiplier)。反复式面积最小,但所耗时钟数最多;阵列式乘法器速度快些,结构规则,但关键路径时延和面积都随乘数被乘数的比特位同比递增;现多采用树状结构乘法器,即部分积+压缩树+最终加法器结构,如Booth编码器+Wallace树+CLA加法器。进一步对于有限域$GF(2^m)$来说,其乘法器还可以按串并行方式的不同一般分为三类:比特串行乘法器、并行乘法器和混合乘法器。若乘法器在每个时钟周期产生出乘积的一个位,则称它为位串行的。若乘法器在每个时钟周期产生出乘积的多个位,则称它为数字串行的。若乘法器在一个时钟周期产生出乘积的所有位,则称为并行的。从理论上来说,串行乘法器的时间和面积复杂度一般为$O(m)$,并行乘法器的时间和面积复杂度极限情况下为常数和$O(m^2)$。混合乘法器通常用来在硬件资源受限时均衡性能和面积。例如,串行乘法器中的高位优先乘法器(MSB)能用2个m比特移位寄存器和2个寄存器在进行m次移位后完成一次$GF(2^m)$上的乘法运算。而当硬件资源允许时,并行乘法器可以用组合电路将乘法运算的m位乘积一次并计算出来,但这是以更多的电路复杂度为代价的。混合乘法器如数字串行乘法器能一次同时计算出乘积的多位。如果乘法运算以k倍的速度加速完成,但电路复杂度也会增加k倍。

在高位优先乘法器的基础上,提出了一种在$GF(2^m)$上可

作者简介:马自堂(1962-),男,教授,硕士生导师,主要研究领域为信息系统安全,嵌入式系统设计,EDA技术;段斌(1981-),男,硕士研究生,主要研究领域为信息系统安全,嵌入式系统设计;刘云飞(1979-),女,讲师,主要研究领域为嵌入式系统设计,制导与仿真。

收稿日期:2009-07-07 **修回日期**:2009-08-26

控制的快速乘法器结构。通过增加控制信号和多路选择器,乘法器在域宽小于最大域宽的一半时能将速度提高一倍。它不占用额外的存储空间,并能扩展应用于串并混合结构中。

2 可重构的高位优先乘法器

在多项式基$\{1,x,\cdots,x^{m-1}\}$表示下,$a(x)=\sum_{i=0}^{m-1}a_i x^i$,$b(x)=\sum_{i=0}^{m-1}b_i x^i\in GF(2^m)$,$f(x)=x^m+r(x)=x^m+\sum_{i=0}^{m-1}r_i x^i$为$GF(2^m)$的约减多项式,则

$$c(x)=a(x)b(x)\bmod f(x)=$$
$$a(x)(b_0+b_1x+\cdots+b_{m-1}x^{m-1})\bmod f(x)=$$
$$(b_0a(x)+b_1a(x)\cdot x+\cdots+b_{m-2}a(x)\cdot x^{m-2}+b_{m-1}a(x)\cdot x^{m-1})\bmod f(x)=$$
$$b_0a(x)\bmod f(x)+b_1a(x)\cdot x\bmod f(x)+\cdots+b_{m-1}a(x)\cdot x^{m-1}\bmod f(x)$$

按照对b各位处理顺序的不同,可以将串行乘法器分为高位优先(MSB)和低位优先(LSB)两种。

算法 1 $GF(2^m)$上的高位优先乘法器[1]

输入:$a=(a_{m-1},\cdots,a_1,a_0)$,$b=(b_{m-1},\cdots,b_1,b_0)\in GF(2^m)$,$f(x)=x^m+r(x)$

输出:$c=a\cdot b$

1.$c\leftarrow 0$

2.对于i从$m-1$降序到0,重复执行

2.1 $c\leftarrow$左移$(c)+c_{m-1}\cdot r$

2.2 $c\leftarrow c+b_i\cdot a$

3.返回c

算法1所示的高位优先乘法器可扩展为大小可变的域$GF(2^m)$上的乘法器,其中$m\in\{m_1,m_2,\cdots,m_t\}$,$m_1\leqslant m_2\leqslant\cdots\leqslant m_t$每个寄存器的长度为$m$。图1描述了在任意域$GF(2^m)$上,$m\in\{m_1,m_2,\cdots,m_t\}$和任意约减多项式中实现乘法的MSB。控制器按从高到低的顺序载入a,b和r的比特位,并将无用位置0。虽然无用位也被时钟所驱动,但由于无用位的内容未发生变化,所以其功耗几乎为零。这种乘法器能用一个计数器、两个m位存储器和两个m位移位寄存器在m个时钟周期内执行一次乘法运算。

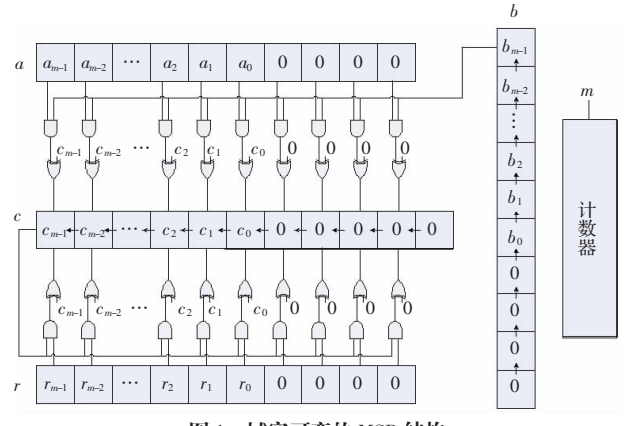

图1 域宽可变的MSB结构

3 一种改进的可重构高位优先乘法器

虽然这种乘法器能实现域宽在一定范围内任意的乘法运算,但是当域宽较小时会有很多的无用位,这无疑是对硬件资源很大的浪费。在这种情况下,可以让乘法器利用空闲硬件资源一次完成两个乘法的计算。通过引入1个选择控制信号和7个两路选择器,实现一个MSB串行计算与两个MSB并行计算的控制。图2和算法2给出改进后的算法和硬件结构。串并行模式通过一个控制信号sel来改变,如表1所示。其中,控制信号sel根据配置参数m产生,M和N是设计参数,$N=M/2$,M为乘法器在串行模式下的最大域宽,N为乘法器在并行模式下的最大域宽。

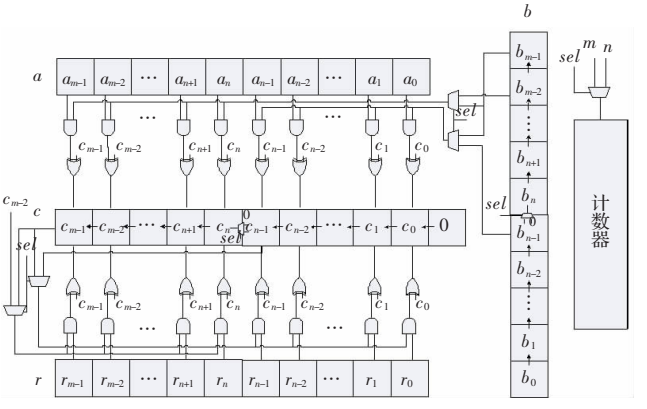

图2 改进后的MSB结构

表1 串并行模式控制说明

条 件	sel	模式	功能
$N<m\leqslant M$	0	串行	在m个时钟周期内计算一个m位乘法
$0<m\leqslant N$	1	并行	在m个时钟周期内计算两个m位乘法

算法 2 改进后的可重构高位优先(MSB)乘法器

输入:$a=(a_{m-1},\cdots,a_n,a_{n-1},\cdots,a_1,a_0)$,$b=(b_{m-1},\cdots,b_n,b_{n-1},\cdots,b_1,b_0)$,$r=(r_{m-1},\cdots,r_n,r_{n-1},\cdots,r_1,r_0)\in GF(2^m)$

$f(x)$为域的不可约多项式,$n=m/2$,$sel\in[0,1]$为控制信号

输出:$c=(c_{m-1},\cdots,c_n,c_{n-1},\cdots,c_1,c_0)=a\cdot b$

1.$c\leftarrow 0$

2.如果$sel=1$

2.1 令$(r_{n-1},\cdots r_1,r_0)=(r_{2n-1},\cdots r_{n+1},r_n)=f(x)+x^n$

2.2 对于i从$n-1$降序到0,重复执行

2.2.1 同时执行

$(c_{n-1},\cdots c_1,c_0)\leftarrow$左移$(c_{n-1},\cdots c_1,c_0)+c_{n-1}(r_{n-1},\cdots r_1,r_0)$

$(c_{2n-1},\cdots,c_{n+1},c_n)\leftarrow$左移$(c_{2n-1},\cdots c_{n+1},c_n)+c_{n-1}(r_{2n-1},\cdots r_{n+1},r_n)$

2.2.2 同时执行

$(c_{n-1},\cdots c_1,c_0)\leftarrow(c_{n-1},\cdots c_1,c_0)+b_i(a_{n-1},\cdots,a_1,a_0)$

$(c_{2n-1},\cdots c_{n+1},c_n)\leftarrow(c_{2n-1},\cdots c_{n+1},c_n)+b_{i+n}(a_{2n-1},\cdots,a_{n+1},a_n)$

否则

2.3 令r为$f(x)+x^m$的二进制表示

2.4 对于i从$m-1$降序到0,重复执行

2.4.1 $c\leftarrow$左移$(c)+c_{m-1}r$

2.4.2 $c\leftarrow c+b_ia$

3.返回c

乘法器的关键路径延迟主要由反馈路径的与门、异或门和两路选择器的延迟组成,因此乘法器路径延迟为$T=T_{AND}+T_{XOR}+T_{MUX}$。这里$T_{AND}$、$T_{XOR}$和$T_{MUX}$分别表示与门、异或门和两路选择器的延迟。与MSB相比,虽然加入了额外的两路选择器,但反

馈后的位由于都经过同样的延迟,所以能严格同步输出。

4　改进方法在串并混合模式中的应用

由于 MSB 在 m 个时钟周期内完成一次乘法运算,当 m 较大时采用 MSB 乘法器实现速度还是较慢,因此可以根据芯片的资源情况采用串并混合结构的乘法器。这种算法能通过对并行计算的位数-数字大小(digit-size)k 的选取在速度与面积之间进行平衡。若数字大小为 k,则完成一次模乘运算只需$\lceil(m+1)/k\rceil$个时钟周期。记 $s=\lceil m/k\rceil$,且

$$B_i(x)=\begin{cases}\sum_{j=0}^{k-1} b_{ik+j}x^j, & 0\leqslant i\leqslant s-2\\ \sum_{j=0}^{m\%k-1} b_{ik+j}x^j, & i=s-1\end{cases}$$

则

$$\begin{aligned}c(x)=&a(x)b(x)\bmod f(x)=\\ &a(x)(x^{(s-1)k}B_{s-1}(x)+x^{(s-2)k}B_{s-2}(x)+\cdots+\\ &x^kB_1(x)+B_0(x))\bmod f(x)=\\ &((\cdots((a(x)B_{s-1}(x))x^k+a(x)B_{s-2}(x))x^k+\cdots+\\ &a(x)B_1(x))x^k+a(x)B_0(x))\bmod f(x)\end{aligned}$$

算法 3　$GF(2^m)$上的串并混合乘法器[4]

输入:$a=(a_{m-1},\cdots,a_1,a_0)$,$b=(b_{m-1},\cdots,b_1,b_0)\in GF(2^m)$,$f(x)$,$k$

输出:$c=a\cdot b$

1.$c(x)\leftarrow a(x)B_{s-1}(x)\bmod f(x)$

2.对于 i 从 $s-2$ 降序到 0,重复执行

2.1　$u(x)\leftarrow x^k\sum_{j=0}^{m}c_jx^j\bmod f(x)$

2.2　$v(x)\leftarrow a(k)\sum_{j=0}^{k-1}b_{ik+j}x^j\bmod f(x)$

2.3　$c(x)=u(x)+v(x)$

3.返回 c

算法 4　可一次并行计算两个乘法的串并混合乘法器

输入:$a=(a_{m-1},\cdots,a_n,a_{n-1},\cdots,a_1,a_0)$,$b=(b_{m-1},\cdots,b_n,b_{n-1},\cdots,b_1,b_0)$,$r=(r_{m-1},\cdots,r_n,r_{n-1},\cdots,r_1,r_0)\in GF(2^m)$

$f(x)$为域的不可约多项式,$n=m/2$,$sel\in[0,1]$为控制信号

输出:$c=(c_{m-1},\cdots,c_n,c_{n-1},\cdots,c_1,c_0)=a\cdot b$

1.$c(x)\leftarrow 0$

2.如果 sel=1

2.1　对于 i 从$\lceil n/k\rceil-2$ 降序到 0,重复执行

2.1.1　同时执行

$(u_{n-1},\cdots,u_1,u_0)\leftarrow x^k\sum_{j=0}^{n}c_jx^j\bmod f(x)$

$(u_{2n-1},\cdots,u_{n+1},u_n)\leftarrow x^k\sum_{j=n}^{2n-1}c_jx^j\bmod f(x)$

2.1.2　同时执行

$(v_{n-1},\cdots,v_1,v_0)\leftarrow(a_{n-1},\cdots,a_1,a_0)\sum_{j=0}^{k-1}b_{ik+j}x^j\bmod f(x)$

$(v_{2n-1},\cdots,v_{n+1},v_n)\leftarrow(a_{2n-1},\cdots,a_{n+1},a_n)\sum_{j=0}^{k-1}b_{n+ik+j}x^j\bmod f(x)$

2.1.3　$c(x)=u(x)+v(x)$

否则

2.2　对于 i 从$\lceil m/k\rceil-2$ 降序到 0,重复执行

2.2.1　$u(x)\leftarrow x^k\sum_{j=0}^{m}c_jx^j\bmod f(x)$

2.2.2　$v(x)\leftarrow a(x)\sum_{j=0}^{k-1}b_{ik+j}x^j\bmod f(x)$

2.2.3　$c(x)=u(x)+v(x)$

3.返回 c

5　性能分析与比较

表 2 是对几种乘法器的比较结果。其中文献[3]和[5]是可重构的乘法器。文献[2]中延迟周期较小为 $m/2+1$,但是以将奇偶部分展开为代价,需要的硬件资源比 MSB 多 50%,需要两路选择器 $m+w_i-2$ 个,其中 w_i 为多项式$f(x)=\sum_{i=0}^{m}f_ix^i$的汉明重量。文献[3]中的乘法器需要 $3m$ 个寄存器,且延迟周期为 m,但路径延迟较大。文献[5]延迟周期较小,但使用与门、或门太多。文献[6]迟时周期小,但需要与门 $mD(D+1)/2$,异或门$(Dm-D+2)(D-1)/2$,其中 D 为乘法器的并行度。

表 2　几种乘法器的比较

乘法器	文献[2]	文献[3]	文献[5]	文献[6]	本文
与门	$2m$	$2m$	$6m$	$mD(D+3)/2$	$2m$
异或门	$3m$	m	$3m$	$3D(m-1)/2+D-1$	$2m$
或门	0	m	$4m-2$	0	0
寄存器	$3m$	$3m$	$3m$	$3m$	$3m$
延迟周期	$m/2+1$	m	$m/2+1$	$[m/D]+1$	$m:m/2$
两路选择器	$m+w_i-2$	m	$8m-2$	0	7
路径延迟	(1)	(2)	(3)	(4)	(1)
可重构性	否	是	是	是	是
可并行性	否	否	否	否	是

实现了最大域宽为 359 位的乘法器,选用 Altera 公司的 Stratix EPIS10F780C5,使用 Synplify 6.9.1 综合,并通过 ModelSim Altera 6.4a 仿真验证。在综合考虑后选择并行度为 8,时钟频率为 105.2 MHz,占用资源为 7 350 个 LE。该乘法器完成一次 $GF(2^{359})$上模乘运算的时间为 0.63 μs,同时完成两次 $GF(2^{163})$上模乘运算的时间为 0.28 μs。

(1)$T_{and}+T_{mux}+T_{xor}$

(2)$2T_{and}+T_{xor}+T_{not}+(m+1)T_{or}$

(3)$mT_{or}+T_{xor}+2T_{mux}+T_{not}+T_{and}+T_{mux}$

(4)$2DT_{and}+(5D/2-1)T_{xor}$

6　结束语

在可重构高位优先乘法器(MSB)基础上,提出了一种串并模式可以控制的乘法器结构,在域宽小于最大域宽的一半时能有效利用硬件资源并行计算两个乘法。该乘法器结构电路复杂度低,具有可重构、可扩展、占用存储空间小的特点。这种乘法器适合变有限域 $GF(2^m)$、存储较小和低硬件复杂度等要求的可重构密码系统 VLSI 设计。

参考文献:

[1] Hankerson D,Menezes A,Vanstone S.Guide to elliptic curve cryptography[M].[S.l.]:Publishing House of Electronics Industry,2005.

(下转 90 页)