一类有限域的高效部分并行乘法器

陈华锋
CHEN Hua-feng

浙江传媒学院,杭州 310018
Zhejiang University of Media and Communications,Hangzhou 310018,China
E-mail:chenhf@vlsi.zju.edu.cn

CHEN Hua-feng.Efficient partial parallel multiplier for a kind of finite fields.Computer Engineering and Applications, 2009,45(19):66-67.

Abstract: A new high regular structure of partial parallel multiplier for irreducible trinomial generated finite field is proposed. Through the analysis of multiplication over finite field $GF(2^m)$,generated by irreducible trinomial,the basic computation format is deduced.The novel multiplier structure is designed based on the basic computation format.According to the complexity analysis, the multiplier has the same complexity with the optimal designs up to date.Meanwhile,it can be configured according to specific demands of all kinds of applications.

Key words: finite field;irreducible trinomial;partial parallel multiplier

摘 要:提出了一类新的具有高度规则性的部分并行三项式有限域乘法器架构。通过对由不可约三项式生成的有限域 $GF(2^m)$上的乘法分析,推导出基本的运算形式。基于该运算形式,设计出新颖的乘法器架构。复杂度分析结果表明,该乘法器具有同当前最优设计相同的复杂度。而且,可视具体的应用情境需求对乘法器电路进行灵活配置。

关键词:有限域;不可约三项式;部分并行乘法器
DOI:10.3778/j.issn.1002-8331.2009.19.019 **文章编号**:1002-8331(2009)19-0066-02 **文献标识码**:A **中图分类号**:TN402;TN918.4

有限域运算在密码学、编码理论等领域有着广泛的应用[1]。在密码算法中,有限域乘法是使用得最频繁也最为耗时的运算。根据加速经常性设计的原则,优化有限域乘法器的结构,对提高密码芯片的性能至关重要。

在基于有限域 $GF(2^m)$的椭圆曲线密码运算中,有限域的生成除取决于 m 值的选择外,还取决于不可约多项式的选取,包括不可约三项式、不可约五项式、系数全一多项式等[2]。其中,使用最广泛的是不可约三项式[3]。

由于椭圆曲线公钥密码算法的计算量比较大,在实时性要求较高的场合,需要进行高速的运算。因此,对有限域乘法器的研究主要地集中在并行乘法器上。针对由不可约三项式生成的有限域的并行乘法器的研究也比较多,并取得了不少的成果[4-7]。但是,密码运算的应用场合是多种多样的,如何在面积与速度性能上取得平衡同样是一个不应被忽视的课题。

鉴此,针对由不可约三项式生成的有限域提出了一种新的部分并行乘法器。该乘法器实现 $A(x)B(x)\bmod f(x)$的运算,其中 $A(x)$、$f(x)$作为整体输入,而对于 $B(x)$则采取分段输入、多周期迭代运算的方法。段长 r 的选值可根据系统对密码算法的性能需求进行调整,具有很大的灵活性。特别的,当 $r=1$ 时,则为串行乘法器;当 $r=m$ 时,则为并行乘法器。作为并行乘法器时,具有同其他最优并行乘法器架构同等的复杂度。

1 三项式有限域乘法分析

令 $GF(2^m)$是不可约三项式 $f(x)$产生的有限域,则定义三项式有限域乘法器为由多项式输入 $A(x)$,$B(x)$和不可约三项式 $f(x)$直接求解出 $A(x)B(x)\bmod f(x)$的乘法器,其中 $A(x)=a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_1x+a_0$,可表示成为二进制形式$[a_{m-1}a_{m-2}\cdots a_1a_0]_2$,$B(x)=b_{m-1}x^{m-1}+b_{m-2}x^{m-2}+\cdots+b_1x+b_0$,可表示成为二进制形式$[b_{m-1}b_{m-2}\cdots b_1b_0]_2$,$f(x)=x^m+x^k+1$,$k$ 的取值范围为 $1\leqslant k<m$。

令 $B(x)$可表示为$[B_{t-1}B_{t-2}\cdots B_1B_0]_{2^r}$,$t=\lceil m/r\rceil$,其中,$r$ 为 B_i 的位数,即每一段的长度,t 为分段的段数,$0\leqslant i\leqslant t-1$。则有:

$$A(x)B(x)\bmod f(x)=((((A(x)B_{t-1}x^r+A(x)B_{t-2})x^r+\cdots)x^r+A(x)B_1)x^r+A(x)B_0)\bmod f(x) \quad (1)$$

根据模运算的性质,可将式(1)转化为:

$$\begin{aligned}&A(x)B(x)\bmod f(x)=\\&(((((A(x)B_{t-1}\bmod f(x))x^r \bmod f(x)+\\&A(x)B_{t-2}\bmod f(x))x^r \bmod f(x)+\cdots)x^r \bmod f(x)+\\&A(x)B_1 \bmod f(x))x^r \bmod f(x)+A(x)B_0 \bmod f(x))\bmod f(x)\end{aligned} \quad (2)$$

由式(2)可知,有限域乘法主要由 $A(x)B_i \bmod f(x)$及 $C(x)x^r \bmod f(x)$两种形式组成。

其中:

$$A(x)B_i \bmod f(x)=(b_{i(r-1)}x^{r-1}+b_{i(r-2)}x^{r-2}+\cdots+b_0)A(x)\bmod f(x)=b_{i(r-1)}(A(x)x^{r-1}\bmod f(x))+b_{i(r-2)}(A(x)x^{r-2}\bmod f(x))+\cdots+b_0A(x) \quad (3)$$

作者简介:陈华锋(1979-),男,博士,教师,研究方向为应用密码学、集成电路设计。
收稿日期:2008-05-21 **修回日期**:2008-09-22

由式(3)可知,$A(x)B_i \bmod f(x)$的求解可由$A(x)x^i \bmod f(x)$的运算和加法运算完成,其中$1\leqslant i\leqslant r-1$。进而,有限域的乘法运算主要由形如$\alpha x^i \bmod f(x)$,$1\leqslant i\leqslant r$的运算组成,其中$\alpha$是有限域$GF(2^m)$的一个多项式。

实际上,若对于有限域$GF(2^m)$中的任一多项式α,通过某一运算单元可实现$\alpha x \bmod f(x)$的运算,则通过i个运算单元的串联,必可实现$\alpha x^i \bmod f(x)$的运算。下文将通过运算推导进而实现运算单元的架构设计。

2　架构设计

根据上章分析,引入$D(x)=d_{m-1}x^{m-1}+d_{m-2}x^{m-2}+\cdots+d_1x+d_0$,可表示成为二进制形式$[d_{m-1}d_{m-2}\cdots d_1d_0]_2$,且:

$$D(x)\equiv \alpha x \bmod f(x)=a_{m-2}x^{m-1}+a_{m-3}x^{m-2}+\cdots+a_kx^{k+1}+(a_{k-1}+a_{m-1})x^k+\cdots+a_0x+a_{m-1} \tag{4}$$

即:

$$\begin{cases} d_{m-i}=a_{m-i-1},\{1\leqslant i\leqslant m-k-1,m-k<i<m\} \\ d_k=a_{k-1}+a_{m-1} \\ d_0=a_{m-1} \end{cases} \tag{5}$$

式(5)可用图1所示电路实现,并将该模块命名为*x_MUL*模块,根据上章的分析结果,由该模块可得到$\alpha x^i \bmod f(x)$的运算电路,如图2所示。需要指出,在$\alpha x^i \bmod f(x)$的实现电路中,不管i的取值如何,其每一级x_MUL模块中的异或门都不会出现在同一条路径中,即$\alpha x^i \bmod f(x)$的实现电路其时延将保持为T_x。

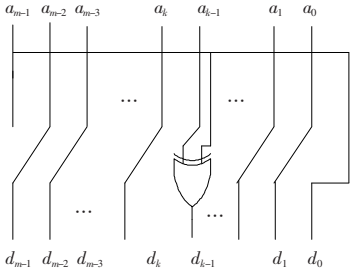

图1　$\alpha x \bmod f(x)$**运算实现电路**

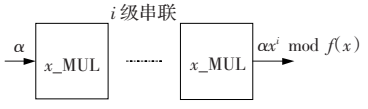

图2　$\alpha x^i \bmod f(x)$**运算实现电路**

由式(3)可得出$A(x)B_i \bmod f(x)$的运算电路如图3所示。其中数据线除标示的$b_{ij}(0\leqslant j<r)$外,其数据宽度皆为m位。

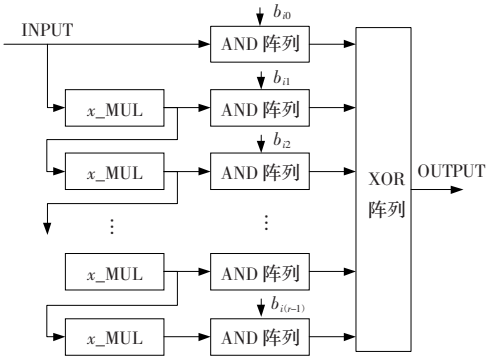

图3　$\alpha B_i \bmod f(x)$**运算实现电路**

由上述实现电路可完成有限域乘法器的设计,如图4。图4中,M1模块为图3所示电路,其输出结果为$A(x)B_i \bmod f(x)$,$0\leqslant i\leqslant t-1$。M2模块为图2所示电路,且其中的$i$取值为$r$。特别的,当$r=m$时,所示有限域乘法器为并行乘法器,图中M2和异或门电路皆可以去除。

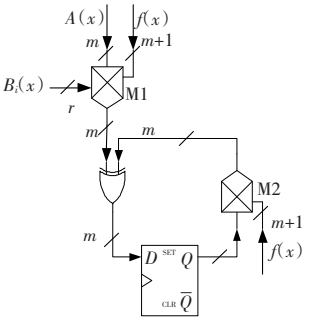

图4　$A(x)B(x) \bmod f(x)$**运算实现电路**

3　乘法器复杂度分析

在硬件的实现方面,用于衡量硬件实现效率的指标为电路的门数(包括与门、或门、异或门等)和用门延时来表达的电路的总延时。通常,将前者称为空间复杂度,将后者称为时间复杂度。对于乘法器的复杂度分析将从这两个角度予以说明。

对于图4中的M1模块,根据图3所示的电路架构,x_MUL模块中包含1个异或门,每一个AND阵列包含m个与门,而XOR阵列则包含$(r-1)\times m$个异或门。综上,M1的空间复杂度为与门数$r\times m$,异或门数$(r-1)\times(m+1)$,其时间复杂度为$T_a+(1+\lceil \mathrm{lb}\, r\rceil)T_x$。其中,$T_a$表示一个与门的延时,$T_x$表示一个异或门的延时。对于图4中的M2模块,可知其包括r个异或门,时延为T_x。

综上,所提出的乘法器电路完成$A(x)\cdot B(x) \bmod f(x)$的运算需通过$t$次迭代。其空间复杂度为与门数$r\times m$,$1\leqslant r\leqslant m$,异或门数:

$$\begin{cases} r\times(m+2)-1, 1\leqslant r<m \\ m^2-1, r=m \end{cases}$$

其时间复杂度为$\begin{cases} T_a+(2+\lceil \mathrm{lb}\, r\rceil)T_x, 1\leqslant r<m \\ T_a+(1+\lceil \mathrm{lb}\, m\rceil)T_x, r=m \end{cases}$

4　性能比较

对于三项式有限域乘法器的研究较多,以往提出了多种适用于三项式乘法的低复杂度高性能乘法器。为了使各类架构具备可比较性,取参数时的复杂度分析结果进行比较,如表1所示,从与门、异或门的数目和乘法器延时三个方面给出了各设计的指标。

表1　典型三项式有限域乘法器复杂度比较

方法	与门数	异或门数	时延
Koc[4]	m^2	m^2-1	$T_A+(2+\lceil \mathrm{lb}\ m\rceil)T_X$
Wu[5]	m^2	m^2-1	$\leqslant T_A+(2+\lceil \mathrm{lb}\ m\rceil)T_X$
Fan[6]	m^2	m^2-1	$T_A+(1+\lceil \mathrm{lb}\ m\rceil)T_X$
金[7]	m^2	m^2-1	$T_A+(1+\lceil \mathrm{lb}\ m\rceil)T_X$
本文设计	m^2	m^2-1	$T_A+(1+\lceil \mathrm{lb}\ m\rceil)T_X$

比较结果表明,所提出的三项式有限域乘法器具有和表1所示的最优架构同等的时间和空间复杂度。

(下转74页)