第 22 卷第 8 期　　半 导 体 学 报　　Vol. 22, No. 8
2001 年 8 月　　CHINESE JOURNAL OF SEMICONDUCTORS　　Aug., 2001

一种 GF(2^k) 域的高效乘法器及其 VLSI 实现

周浩华　沈　泊　章倩苓

(复旦大学专用集成电路与系统国家重点实验室，上海　200433)

摘要: 在分析全串行和全并行 GF(2^k) 域乘法的基本原理基础上提出了一种适合于任意 GF(2^k) 域的乘法器 UHGM (Unified Hybrid Galois Field Multiplier). 它为当前特别重要的 k 为素数的 GF(2^k) 域乘法, 提供了一种高效的实现方法. 该乘法器具有结构规整、模块化好的特点, 特别适合于 VLSI 实现, 同时这种结构具有粗粒度的面积和速度的可伸缩性, 方便了在大范围内进行实现面积和速度的权衡. 最后给出了 GF(2^{163}) 域上乘法器的 ASIC 综合的结果.

关键词: 有限域; 乘法; GF(2^{163}); 加密; 椭圆曲线; VLSI

EEACC: 2570D; 1265B; 6210

中图分类号: TN47　　**文献标识码**: A　　**文章编号**: 0253-4177(2001)08-1063-06

1 引言

有限域理论是一个古老的数学命题, 由于有限域的运算具有无进位、等比特、无舍入误差[1]的特点, 在纠错码(ECC)[2]、加密[3]、开关理论和数字信号处理[4]等领域有着广泛的应用.

公钥制加密算法是现代数字安全通讯中一种必不可少的技术, 它能提供信息加密、数字签名、身份认证等服务, 为现在的电子商务、网上银行等业务的实现提供了可能. 很多的加密算法都需要基于 GF(2^k) 域的运算, 例如, 基于有限域的离散对数难题的 DSA 算法[10], 基于椭圆曲线上的离散对数难题的 ECCDSA 算法和超级椭圆曲线加密算法等. 它们已成为国际标准如 IEEE 1363, IPsec 的重要组成部分[2], 而 GF(2^k) 域的乘法往往是关系这些加密算法实现性能的最重要因素.

现代的加密算法需要在比较大的有限域上的运算, 椭圆加密由于其短的密钥长度, 被认为是优于 RSA, DSA 的加密技术[5], 当前由于安全性的要求, 它仍需要 150—250bit 的密钥长度. 现代通讯的高带宽需求, 以及物理安全性的需要, 使 VLSI 实现 GF(2^k) 域的运算有着特别重要的意义. 由于安全性 VLSI 往往是嵌入系统中的, 人们需要对加密算法的实现作面积和速度上的权衡.

关于 GF(2^k) 域乘法器的研究开展已久, 按照参加运算的数的形式来分有正交基[6]、标准基和双基, 由于标准基是实现不同基间互操作的基础, 本文主要研究标准基上的运算. 按照结构来分又可分为基于比特的全串行的结构、全并行的结构以及串并结合的混合结构. 如文献[1]中提到的基于比特的串行结构, 它需要 k 个时钟节拍 $O(k)$ 个逻辑单元来完成一次 GF(2^k) 域的乘法. 又如文献[1]中提到的全并行结构, 它需要一个时钟节拍, $O(k^2)$ 个单元完成 GF(2^k) 域的乘法. 最近以来, Parr[7]等人研究提出一类特殊的 GF((2^n)^m) 复合域上的乘法器, 它可以在 m 个时钟内用 $O(mk)$ 个逻辑单元完成一次乘法.

当 k 为 150bit 以上时, 全串行结构的速度太慢, 而全并行则规模太大. 对于串并结合的结构, 目前有报道的都是基于 GF((2^n)^m) 复合域的, 由于 GF((2^n)^m) 复合域实际应用时往往需要与标准基之间进行转换[9]. 近几年的研究发现, 复合域上的椭圆加

周浩华　男, 1973 年出生, 博士研究生, 研究方向为专用集成电路和系统设计、VLSI 在信息安全中的应用等.

沈　泊　男, 1975 年出生, 博士研究生, 研究方向为 VLSI 系统集成等.

2000-09-02 收到, 2001-01-02 定稿

密等公钥制算法有安全性问题[8],因而复合域的运算越来越被人们认为不适合应用于加密场合,k 为素数的 GF(2^k) 域上的运算引起了人们的重视.例如在最近的 IPsec 加密国际标准中增加的关于椭圆曲线加密方案的有限域,是 k 为 163 和 283 上的 GF(2^k) 域[2,10].由于 k 为素数的 GF(2^k) 域无法分解为 GF((2^n)^m) 形式,因而研究适合于任意的 GF(2^k) 域,特别是 k 为素数的 GF(2^k) 域上的乘法就显得特别有意义.

本文在分析传统的全并行和全串行基本乘法结构的基础上,提出了一种适合于任意 k 的具有混合结构的 GF(2^k) 域乘法器,称为 UHGM (Unified Hybrid Galois Field Multiplier).

2 基本原理

为方便讨论,下文中考虑在 GF(2^k) 域上的运算,其中 $k=mn+r$,这里 k、m、n、r 为整数.定义乘数 $A(x)=\sum_{i=0}^{k-1}a_ix^i$,被乘数 $B(x)=\sum_{i=0}^{k-1}b_ix^i$,生成多项式为 $P(x)=x^k+\sum_{i=0}^{k-1}p_ix^i$,最后的乘积为 $C(x)=\sum_{i=0}^{k-1}c_ix^i$,其中 a_i、b_i、c_i、$p_i\in$GF(2).设 T_{xor}、T_{and}、T_{reg} 分别表示两输入的与门、异或门的延时和寄存器的建立时间,T_{cp} 为关键路径上的时延,# And、# Xor 表示两输入的异或门、与门的个数,# Reg 表示寄存器的个数.

本文提出的 UHGM 是结合全串行的 GF(2^k) 上乘法和 GF(2) 上的多项式的乘法的原理基础上提出的一种适合于任何 GF(2^k) 域的乘法结构.

2.1 基于比特的全串行的 GF(2^k) 域上的乘法

GF(2^k) 域上的乘法,可以通过模乘和模剩余交替进行来实现,它有两种实现方法,一种是文献[11]所描述的 SSR(Standard Shift Register) 结构,它是从最高位开始的 GF(2^k) 域乘法,另一种是文献[1]中提到的 MSR(Modified Shift Register) 算法,它是从最低位开始的 GF(2^k) 域乘法.

SSR 结构是通过下面过程的迭代来实现 GF(2^k) 域上的乘法的:

$$C'^{(i)}=xC'^{(i-1)}\bmod P(x)+b_{i-1}A(x)$$
$$i=1,2,\cdots,k;\ C'^{0}=0;\ C(x)=C'^{(k)} \quad (1)$$

上式中 $xC'^{(i-1)}$ 是一个最高项次数为 k 的多项式,再根据生成多项式 $x^k\bmod P(x)=\sum_{i=0}^{k-1}p_ix^i$ 进行化简,即得 $xC'^{(i-1)}\bmod P(x)$.

分析表明 MSR 的实现面积和关键路径的时延均比 SSR 小[1],结构也是比 SSR 优越.MSR 和 SSR 结构的实现复杂度和关键路径的时延如表 1 所示.

表 1 SSR 和 MSR 的实现复杂度和关键路径的时延

Table 1 Comparison of Area and Critical Path Delay Between SSR and MSR

	单元数			时延
结构	# And	# Xor	# Reg	T_{cp}
SSR	$2k$	$2k-1$	$4k$	$2T_{xor}+T_{reg}+T_{and}$
MSR	$2k$	$2k-1$	$4k$	$T_{xor}+T_{reg}+T_{and}$

从表中可以看出全串行结构的特点是:速度与 k 无关,面积与 k 成线性增长,完成一次模乘运算要 $k+1$ 个时钟.

2.2 GF(2^n) 域上的多项式乘法

全并行的 GF(2^n) 域上的乘法,一般可分为 GF(2^n) 域上的多项式乘法和 GF(2^n) 域上的模剩余两部分[1,7,9],这里主要讨论 GF(2^n) 域上的多项式乘法.设 $A(x)$ 和 $B(x)$ 是 GF(2^n) 域上的多项式,deg 表示多项式的次数.$\deg(A(x))\leqslant n-1$,$\deg(B(x))\leqslant n-1$,$C'(x)=A(x)B(x)$,则 $\deg(C'(x))\leqslant 2n-2$.由于 GF(2) 域上的加法是无进位的,因而 GF(2^n) 域上的多项式乘法有着和传统的乘法器不同的时延特性,对于 $A(x)$ 和 $B(x)$ 的乘法运算按多项式乘法定义展开,如图 1 所示,其关键路径为:

$$a_{n-1}b_0+a_{n-2}b_1+\cdots+a_0b_{n-1}$$

上式中的“+”为 GF(2) 域上的加法,用一个异或门即可实现,共有加法器 $n-1$ 个,由于被加的各项之间没有相互因果关联,可同时产生,因而上式运算可按如图 2 的层次化结构来组织,它的实现可看作为 2∶1 的压缩过程.

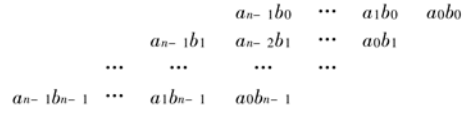

图 1 多项式乘法的展开

FIG. 1 Partial Product for Polynomial Multiplication

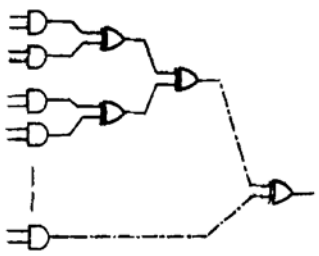

图 2　GF(2) 域加法的层次式结构

FIG. 2　Hierarchy Structure for GF(2) Addition

按照上面的结构可得其实现复杂度和时延特性为:

$$\#\ \mathrm{And} = n^2, \#\ \mathrm{Xor} = (n-1)^2,$$
$$T_{cp} = T_{and} + [\log_2 n] T_{xor}$$

2.3　UHGM 的基本原理

文献[7, 9]中提到的复合域乘法是将 k bit 和 k bit 的有限域乘法, 用 $n$bit 和 $n$bit 的串接结构的多次调用来实现, 复合域乘法得到的结果要经过一种变换才能变为标准基, 并且只适合于 $k = mn$ 的有限情形, 对 k 为素数的情况不能适用. UHGM 是将 $k$bit 和 $k$bit 的有限域乘法分解为多次 $n$bit 和 $k$bit 有限域乘法的迭代来实现. UHGM 实现原理如下:

假设 $a_i'(x)$, $b_i'(x)$ 是 GF(2^n) 域上的最高次为 $n-1$ 的多项式, 可将 $A(x)$、$B(x)$ 按照 $n$bit 的单位分别表示为下面的形式:

$$A(x) = \sum_{i=0}^{k-1} a_i x^i = \sum_{i=0}^{m} a_i'(x) x^{ni},$$
$$B(x) = \sum_{i=0}^{k-1} b_i x^i = \sum_{i=0}^{m} b_i'(x) x^{ni}$$

按照多项式乘法, 可将 $a_i'(x) \times b_j'(x)$ 结果表示如下式:

$$a_i'(x) \times b_j'(x) = q1_{i,j}(x) + x^n q2_{i,j}(x) \quad (3)$$

则 $\deg(q1_{i,j}(x)) \leqslant n-1, \deg(q2_{i,j}(x)) \leqslant n-2$

对于最高位 $b_m'(x)$, 由于 $k = mn + r$, 故最高位只有 r 个有效位, 可看作是 $b_m'(x)$ 高 $n-r$ 位为 0 的多项式乘法, 这样有:

$$\deg(q2_{i,m}(x)) \leqslant r - 1 \quad (4)$$

考虑 $a_i'(x)$ 和 $B(x)$ 的乘积:

$$a_i'(x) \times \sum_{j=0}^{m} b_j'(x) x^{nj} =$$
$$q1_{i,0}(x) + \sum_{j=1}^{m} (q1_{i,j}(x) + q2_{i,(j-1)}(x)) x^{nj}$$
$$+ q2_{i,m}(x) x^{n(m+1)} = L_i(x) + x^k H_i(x) \quad (5)$$

按多项式乘法和(4)式的关系, 可知等式(5)右边的次数不大于 $mn + (n-1) + (r-1) = k + n - 2$, $L_i(x)$ 是等式(5)右边的次数小于等于 k 的部分, 即 $\deg(L_i(x)) \leqslant k-1$, $x^k H_i(x)$ 是等式(5)右边次数大于 $k-1$ 的部分, 即 $\deg(H_i(x)) \leqslant n-2$.

$C'^i(x)$ 的最高的 n 位组成的多项式为 $HC^i(x)$, $\deg(HC^i(x)) \leqslant n-1$, 剩下的 $k-n$ 位组成的多项式为 $LC^i(x)$, $\deg(LC^i(x)) \leqslant k-n-1$. $C'^i(x)$ 则可表示为:

$$\begin{aligned} C'^i(x) &= ((x^n C'^{(i-1)}(x) + a'_{(m-i+1)}(x) \times \sum_{j=0}^{m} (b_j'(x) x^{nj})) \bmod P(x) \\ &= ((x^n C'^{(i-1)}(x) + x^k H_{(m-i+1)}(x)) + L_{(m-i+1)}(x)) \bmod P(x) \\ &= (x^k [HC^{(i-1)}(x) + H_{(m-i+1)}(x)]) \bmod P(x) + L_{(m-i+1)}(x) + x^n LC^{(i-1)}(x) \\ &= \sum_{j=k}^{k+n-1} q_j x^j \bmod P(x) + L_{(m-i+1)}(x) + x^n LC^{(i-1)}(x) \\ &= Q(x) \bmod P(x) + L_{(m-i+1)}(x) + x^n LC^{(i-1)}(x) \end{aligned} \quad (6)$$

式中　$i = 1, 2, \cdots, m$; $C'^0 = 0$; $C(x) = C'^m(x)$.

等式(6)中的 $Q(x) \bmod P(x)$ 的运算过程可看作是 n 个 $Q(x)$ 系数到 k 个 $C'^i(x)$ 的线性映射, 因而可用矩阵表示为:

$$\begin{bmatrix} C_0'^i \\ C_1'^i \\ \cdots \\ C_{k-1}'^i \end{bmatrix} = \begin{bmatrix} r_{0,0} & \cdots & r_{0,n-1} \\ r_{1,0} & \cdots & r_{1,n-1} \\ \cdots & \cdots & \cdots \\ r_{k-1,0} & \cdots & r_{k-1,n-1} \end{bmatrix} \begin{bmatrix} q_k \\ q_{k+1} \\ \cdots \\ q_{k+n-1} \end{bmatrix} \quad (7)$$

$r_{i,j}$ 是仅与生成多项式 $P(x)$ 有关的函数,

$$r_{i,j} = \begin{cases} p_j & i = 0, \cdots, k-1;\ j = 0 \\ r_{i-1,j-1} + r_{k-1,j-1} r_{i,0} & \\ \qquad i = 0, \cdots, k-1;\ j = 1, \cdots, n-1 & \\ 0 \qquad i = -1 & \end{cases} \quad (8)$$

综上所述, UHGM 是用 $n$bit 和 $k$bit 有限域乘法的迭代来实现 $k$bit 和 $k$bit 的有限域乘法, 是一种串并结合的方法.

3 UHGM 结构的 VLSI 实现

根据第二部分对 UHGM 的原理分析, 可以得到它的一种 VLSI 实现结构, 如图 3 所示, 它实际上是一个高位优先的结构. 同理参照 UHGM 的原理分析, 可以得到类似 UHGM 的低位优先的乘法器结构, 如图 4 所示.

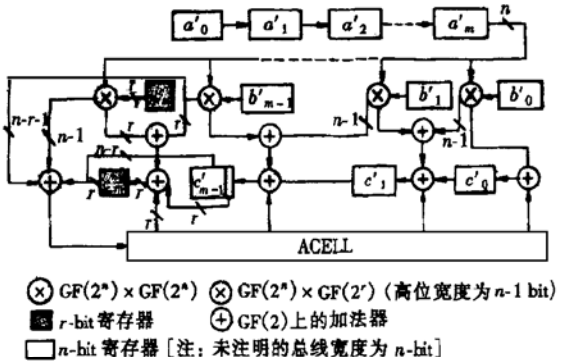

图 3 UHGM 的结构框图

FIG. 3 UHGM Structure

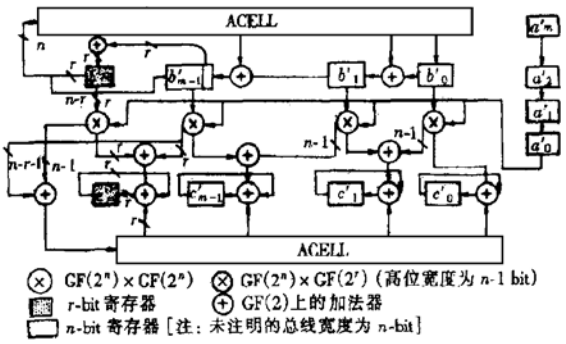

图 4 低位优先的混合结构的乘法器

FIG. 4 Multiplier with Low-Prior Hybrid Structure

为适应结构规整性的需要, 图中 a'_m 是一个只有低 r 位有效, 其余位填充 0 的 $n$bit 宽的寄存器. 图中的 ACELL 是实现 $n$bit 的系数到 $k$bit 的映射, 即公式(7)所示的矩阵的功能. 从图 3 和 4 中可以看出其结构是规整的块状结构, 仅相邻的块之间才有联系, 这种结构方便了布线, 因而这种结构特别适合于用 VLSI 实现. 图 3 的 UHGM 结构是最高位优先的类 SSR 结构, 图 4 为最低位优先的类 MSR 结构, 可以看出图 4 比图 3 的结构要复杂得多, 但关键路径是一样的, 这样图 3 结构具有图 4 的所有优点, 这一点与前面讨论的全串行的乘法器正好相反, 故 UHGM 采用的是图 3 的结构.

参照文献[1]和公式(8), 当 $P(x)$ 可变时, ACELL 的实现可看作是下面过程的迭代:

$$xP'(x)\bmod P(x) = P''(x) = (p'_{i-1}p_{i-1} + p'_{i-2})x^{i-1} + (p'_{i-1}p_{i-2} + p'_{i-3})x^{i-2} + \cdots(p'_{i-1}p_1 + p'_0)x + p'_{i-1}p_0$$

开始时 $P'(x)=P(x)$, 后面用 $P''(x)$ 代替 $P'(x)$ 进行迭代. 因而它的实现复杂度和时延特性为:

$$\#\,\mathrm{And} = 2nk - k,\ \#\,\mathrm{Xor} = 2nk - 2k - n + 1$$

$$T_{\mathrm{cp}} = n(T_{\mathrm{and}} + T_{\mathrm{xor}})$$

对于加密应用的场合中, $P(x)$ 往往事先是固定的, 并且它的结构多为三项式或五项式[7]. 设 s 为 $P(x)$ 中不为 0 的次高项次数, 一般地 $k-n>s$, 则迭代时 p'_{i-1} 始终为 0, 假设 $P(x)$ 汉明距离为 w_p+1, 则 ACELL 的实现复杂度和时延特性为:

$$\#\,\mathrm{And} = nw_p,\ \#\,\mathrm{Xor} \leqslant n(w_p - 1)$$

$$T_{\mathrm{cp}} \leqslant T_{\mathrm{and}} + \lceil \log_2 w_p \rceil T_{\mathrm{xor}}$$

参照图 3 和上面的讨论, 用 UHGM 实现的 GF(2^k) 域的乘法器, 其实现复杂度和性能如表 2 所示, 同理可算出图 4 所示的结构实现复杂度和性能, 结果也列在表 2 中.

表 2 图 3 和图 4 的结构实现复杂度和性能

Table 2 Comparison of Area and Performance Between Two Structures in Figs. 3 and 4

	实现复杂度			性能	
结构	# And	# Xor	# Reg	# Clock	T_{cp}
可变 $P(x)$, 图 3	$3nk-k-n+1$	$3nk-2k-n+1$	$4k$	$m+1$	$(n+1+\lceil\log_2 n\rceil)T_{\mathrm{xor}}+T_{\mathrm{reg}}+(n+1)T_{\mathrm{and}}$
固定 $P(x)$, 图 3	$nk+nw_p$	$nk+nw_p$	$3k$	$m+1$	$(2+\lceil\log_2 w_p\rceil+\lceil\log_2 n\rceil)T_{\mathrm{xor}}+T_{\mathrm{reg}}+2T_{\mathrm{and}}$
可变 $P(x)$, 图 4	$5nk-2k$	$5nk-2k-3n+2$	$4k$	$m+1$	$(n+1+\lceil\log_2 n\rceil)T_{\mathrm{xor}}+T_{\mathrm{reg}}+(n+1)T_{\mathrm{and}}$
固定 $P(x)$, 图 4	$nk+2nw_p$	$nk+2nw_p$	$3k$	$m+1$	$(2+\lceil\log_2 w_p\rceil+\lceil\log_2 n\rceil)T_{\mathrm{xor}}+T_{\mathrm{reg}}+2T_{\mathrm{and}}$

从表 2 可以看出, 图 3 结构无论是面积和性能都比图 4 结构优越, 两种结构的实现复杂度随 n 线性增长, 所需的 Clock 数按 n 的比例减少, 因而这种结构具有粗粒度的面积和速度的可伸缩性, 方便

了在大范围内进行实现面积和速度的权衡. 同时也使权衡变得比较简单, 把问题简化为如何将 k 分解为 $mn+r$ 形式的问题.

4　实例分析

椭圆加密算法是 GF(2^k) 域的一个典型应用. 近几年椭圆加密算法由于其高的单比特安全性逐渐成为 IEEE 1363、ANSI X9.62、IPSec 等国际标准的重要组成部分[2,10], 并且已有产品问世, 如 Certicom 公司的 SC-400 智能卡[12] 等. 在 IPSec 的密钥交换方案中[13], Group 6, 7 都是基于 GF(2^{163}) 域的, 它们的生成多项式都为: $P(x)=x^{163}+x^7+x^6+x^3+1$. 当 $n=8$ 时, 其 ACELL 可看作是下面的矩阵的加法:

```
                1 1 0 0 1 0 0 1
              1 1 0 0 1 0 0 1
            1 1 0 0 1 0 0 1
          1 1 0 0 1 0 0 1
        1 1 0 0 1 0 0 1
      1 1 0 0 1 0 0 1
    1 1 0 0 1 0 0 1
  1 1 0 0 1 0 0 1
```

图 5　GF(2^{163}) 上的 ACELL 的产生示意图

FIG. 5　ACELL Generation for GF(2^{163})

其中每一行要和 ACELL 对应的输入相与, 再进行纵向的异或操作, 这里纵向异或按图 2 层次式结构组织, 从图中可看出 ACELL 实现复杂度和时延特性为:

And= $4\times8=32$, # Xor= 17, $T_{cp}=2T_{xor}+T_{and}$

按前面的分析可得 GF(2^{163}) 的实现复杂度和时延特性为:

$$\#\ \text{And}=1336,\ \#\ \text{Xor}=1336,$$

$$T_{cp}=2T_{and}+8T_{xor}+T_{reg}$$

最后我们用 Verilog 对全串行的 MSR 和 UHGM 分别进行了描述和仿真, 最后用新加坡 Chartered 的 0.6μm CMOS csmhd 库进行了综合, 在 Synopsys 工具中都用工作时钟为 200MHz 的约束, 综合后得到如表 3 的结果. 为便于参照和比较, 表中同时也列出了库基本单元的信息(表中标注有 * 者), And 和 Xor 为两输入单输出的与门和异或门.

表 3　ASIC 实现的结果

Table 3　Results of Synthesis

	单元数	T_{cp}/ns	时钟数
MSR, 固定 $P(x)$	11672	4.98	163
MSR, 可变 $P(x)$	14168	5.0	163
UHGM, 固定 $P(x)$	23586	5.0	21
UHGM, 可变 $P(x)$	51655	9.62	21
And*	4	0.15	
Xor*	7	0.26	
Register*	12	0.31	

从上面的综合和验证的结果可以看出, 相同结构时, $P(x)$ 固定比 $P(x)$ 可变的情况下有限域乘法器的实现面积和性能都得到很大的优化, 同全串行的结构相比, UHGM 结构能在适当增大面积情况下, 成比例的提高乘法器的速度. 由于 UHGM 的关键路径时间不是很大, 因而实际应用时系统时钟不会由它决定, 从而保证 UHGM 和全串行的结构能在相同的系统时钟下工作, 获得全串行结构 n 倍的速度.

5　结论

本文提出了一种适用于任意 k 的 GF(2^k) 域的乘法器结构, 它具有粗粒度的面积和速度的可伸缩性, 方便了在大范围内进行实现面积和速度的权衡, 同时它又具有规整性, 模块化的特点, 因而特别适合 VLSI 实现.

理论分析和实现的结果表明, 本文的结构可以在适当增加面积的基础上, 成倍的提高 GF(2^k) 域的乘法器的速度. 它给已知生成多项式 $P(x)$ 的 GF(2^k) 域, 特别是 k 为素数时的乘法提供了一种高效的实现方法.

参考文献

[1] E. D. Mastrovito, VLSI Architectures for Computation in Galois Fields, PhD Thesis, Linkoping University, Department of Electronic Engineering, Linkoping, Sweden, 1991.

[2] Wang Yumin *et al.*, Security, Theory and Technology of Communication Network, Publishing House of Xi'an University of Electron Secience and Technology, 1999[王育民, 等, 通信网的安全理论和技术, 西安电子科技大学出版社, 1999].

[3] LU Kaicheng, Computer Cryptography. Publishing House of

Tsinghua University, 1998[卢开澄, 计算机密码学, 清华大学出版社, 1998].

[4] B. Benjauthrit and I. S. Reed, Galois Switching Functions and Their Applications, IEEE Trans. Comput., 1976, **C-25**: 78—86.

[5] G. Harper, A. Menezes and S. Vanstone, Public-key Cryptosystems with Very Small Key Lengths, Advances in Cryptology-EUROCRYPT '92, 1992, 163—173.

[6] C. Paar and N. Lange, A Comparative VLSI Synthesis of Finite Field Multipliers, 3rd International Symposium on Communication Theory and its Applications, Lake District, UK, 1995.

[7] C. Paar, Fast Arithmetic for Public-Key Algorithm in Galois Fields with Composite Exponents, IEEE Trans. Computers, 1999, **48**(10): 1025—1034.

[8] P. Gaudry, F. Hess and N. P. Smart, Constructive and Destructive Facets of Weil Descent on Elliptic Curves, http: // www. hpl. hp. com/techreports/2000/HPL-2000-10. html, 2000.

[9] C. Paar, Efficient VLSI Architectures for Bit-Parallel Computation in Galois Fields, PhD Thesis, (Engl. Transl.), Institute for Experimental Mathematics, University of Essen, Essen, Germany, 1994.

[10] Certicom Company, ECC Standards, http: // www. certicom. ca/research. html, 2000.

[11] P. A. Scott, S. E. Tavares and L. E. Peppard, A Fast VLSI Multiplier for GF(2^m), IEEE J. Sel. Areas Commun., 1986, **SAC-4**(1): 62—66.

[12] Certicom Whitepaper, The Elliptic Curve Cryptosystem for Smart Cards, http: // www. certicom. ca/products. html, 1998.

[13] P. Panjwani and Y. Poeluev, Additional ECC Groups For IKE, IPSec Working Group, http: // www. ietf. org/shadaw. html, 1999.

[14] Zhou Hao-hua, Li Zhi-yong *et al.*, A Regular Time-Efficient VLSI Architecture for Multiplication Modulo 2^n+1, Chinese Journal of Semiconductors, 2000, **21**(10): 1032—1037.

An Efficient Multiplier for GF(2^k) and the VLSI Implementation

ZHOU Hao-hua, SHEN Bo and ZHANG Qian-ling

(*ASIC & System State Key Laboratory, Fudan University, Shanghai* 200433, *China*)

Abstract: Public-Key Cryptography as the base of modern identification, authentication, secure communications technology, depends on Galois Field multiplication that is based on discrete logarithm problem. By analyzing the bit serial multiplier and bit parellel multiplier, a Unified Hybrid Galois field Multiplier, namely UHGM, is introduced. An Efficient implementation is carried out for the multiplication on GF (2^k), especially when k is a prime number. UHGM is suitable for the VLSI implemenation due to its regularity and modularity, whose structure can t rade off the area against the performance conveniently. Finally a sample GF(2^{163}) multiplier is presented, as well as the result of verification and sysnthesis on FPGA and ASIC.

Key words: galois field; multiplication; GF(2^{163}); cryptography; elliptic curves; VLSI

EEACC: 2570D; 1265B; 6210

Article ID: 0253-4177(2001)08-1063-06

ZHOU Hao-hua male, was born in 1973, PhD candidate. His research interests include ASIC & System, VLSI in information Security.

SHEN Bo male, was born in 1975, PhD candidate. His research interestes mainly focus on the VLSI integration of electronic systems.

Received 2 September 2000, revised manuscript received 2 January 2000