# GF($2^n$)域上的一种Ⅱ型优化正规基乘法器及其 FPGA 实现

方 冰,樊海宁,戴一奇
(清华大学计算机科学与技术系网络所,北京 100084)

**摘 要:** 有限域 GF($2^n$)上的椭圆曲线密码体制以其密钥短,安全强度高的优点正在获得广泛的重视和应用.该密码体制最主要的运算是有限域上的乘法运算.本文提出了一种基于Ⅱ型优化正规基的乘法器,该乘法器具有 Massey-Omura 乘法器的优点,又避免了其不足,易于编程,适合 FPGA 实现.实验表明,该算法简单,快速.

**关键词:** 有限域; 正规基; 乘法
**中图分类号:** TN47 **文献标识码:** A **文章编号:** 0372-2112 (2002) 12A-2045-04

# An Optimal Normal Basis Type Ⅱ Multiplier over GF($2^n$) for FPGAs

FANG Bing, FAN Hai-ning, DAI Yi-qi
(*Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China*)

**Abstract:** The elliptic curve cryptosystems over the finite field GF($2^n$) receive considerable attention and are widely used because of their small key size and high security. Multiplication operation over the finite field GF($2^n$) is the crucial arithmetic operation. This paper presents a multiplication algorithm for the optimal normal basis type Ⅱ. The algorithm has the advantage of Massey-Omura multiplication algorithm and eliminate its deficiency. The test shows that this algorithm is simple, fast and is easy to be implemented by FPGA.

**Key words:** finite field; normal basis; multiplication

## 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、无舍入误差的特点,在纠错码、加密和数字信号处理等领域有着广泛的用途.

随着网络技术的不断发展,网络的安全问题日益暴露出来.密码技术作为最根本的有效解决手段,在各种安全解决方案中都得到了越来越广泛的应用.许多加密算法都需要基于 GF($2^n$)的运算,例如:基于有限域离散对数难题的 DSA 算法,基于椭圆曲线上离散对数难题的 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,而 GF($2^n$)域的乘法往往是关系这些算法实现性能的最重要的因素.

1985 年 Koblitz 和 Miller 提出了一种新的公钥体制——椭圆曲线密码体制,该体制以其短密钥,高强度等优点引起了人们的重视,其中基于 GF($2^n$)上的椭圆曲线密码体制是一种比较重要的密码体制.但是由于 GF($2^n$)上运算的复杂性,使得该体制的加解密速度较低,因此人们越来越多地利用硬件来实现该密码体制.近年来,FPGA(Field Programable Gate Array)以其编程方便、集成度高、速度快等特点获得了广泛的应用,人们开始研究其在椭圆曲线密码体制中的应用.在椭圆曲线密码体制中,有限域上的乘法运算是最基本的运算,也是制约其速度的一个重要因素,因此设计一个快速的乘法器显得非常重要.

关于 GF($2^n$)域的乘法器的研究由来已久,按照参加运算的数的形式来分有正规基[1]、标准基和双基.由于以正规基表示元素的一个优点就是元素的平方运算仅相当于元素的一次循环移位,本文主要研究正规基上的运算.正规基中有两类比较重要的正规基,一种是Ⅰ型优化正规基,另一种是Ⅱ型优化正规基.在 ANSI X.962[2]和 ANSI X.963[3]中强制规定了有限域中元素以正规基表示时,特征为 2 的有限域选取步骤为:优先选取存在Ⅱ型优化正规基的有限域,其次选取存在Ⅰ型优化正规基的有限域,否则选取存在其它低复杂性正规基的有限域,因此设计基于Ⅱ型优化正规基的乘法器显得非常必要.本文提出了一个 GF($2^n$)上基于Ⅱ型优化正规基的乘法器,该乘法器具有 Massey-Omura 乘法器[4]的优点,又避免了其不足,简单,快速,易于 FPGA 实现.

收稿日期:2002-06-15;修回日期:2002-09-09
基金项目:国家 973 项目(No.G1998030409)

## 2 基本原理

$GF(2^n)$可以看作是 $GF(2)$上的 $n$ 维矢量空间，一旦选定 $GF(2^n)$在 $GF(2)$上的基，则 $GF(2^n)$上的元素就可以表示为长度为 $n$ 的 0，1 矢量．本文选取优化正规基来表示 $GF(2^n)$上的元素．

**定义 1** 如果域 $GF(2^n)$上在 $GF(2)$上的基 $N$ 形如 $\{\beta,\beta^2,\cdots\cdots\beta^{2^{n-2}},\beta^{2^{n-1}}\}$，则称 $N$ 为 $GF(2^n)$ 上的正规基．

设 $A,B\in GF(2^n)$，$A=\sum_{i=1}^{n}a_i\beta^{2^{i-1}}=(a_n,a_{n-1},\cdots\cdots,a_2,a_1)$；

$B=\sum_{i=1}^{n}b_i\cdot\beta^{2^{i-1}}=(b_n,b_{n-1},\cdots\cdots,b_2,b_1)$，$i=0,1,2,\cdots\cdots,n-1$

不难得到以下引理：

**引理 1**

$A^2=(a_n,a_{n-1},\cdots\cdots,a_2,a_1)^2=(a_{n-1},\cdots\cdots a_2,a_1,a_n)$

设 $D=A\cdot B=\sum_{i=1}^{n}\sum_{j=1}^{n}a_i\cdot b_j\cdot\beta^{2^{i-1}+2^{j-1}}=\sum_{k=1}^{n}d_k\cdot\beta^{2^{k-1}}$

如称 $a_i\cdot b_j$ 为一个项．那么，每一个 $d_k(k=1,2,\cdots\cdots,n$，下同）均等于若干个不同项之和．记 $C_N$ 为 $d_1$ 中项的个数．在文献[1]中，给出了优化正规基的定义．并指出存在两种类型的优化正规基．

**定义 2** $GF(2^n)$上的正规基 $N$ 称为优化正规基，如果 $C_N=2n-1$．

**引理 2** $GF(2^n)$上存在优化正规基，如果 $n+1$ 是素数，并且 2 是模 $n+1$ 的原根．这类优化正规基称为Ⅰ型优化正规基．

**引理 3** $GF(2^n)$上存在优化正规基，如果 $2n+1$ 是素数，并且满足以下两个条件之一：

(1)2 是模 $2n+1$ 的原根；

(2)$2n+1$ 是模 4 为 3 的一个素数，并且 2 是模 $2n+1$ 的二次剩余，

这类优化正规基称为Ⅱ型优化正规基，其正规元素如下构造：$\beta=\gamma+\gamma^{-1}$，其中 $\gamma^{2n+1}=1$ 并且 $\gamma^i\neq1(1\leqslant i\leqslant2n+1)$

由引理 1 可得出

$D=(d_n,d_{n-1},\cdots,d_2,d_1)=(a_n,a_{n-1},\cdots\cdots,a_2,a_1)\cdot(b_n,b_{n-1},\cdots\cdots,b_2,b_1)$

则 $d_1=f(a_n,a_{n-1},\cdots\cdots a_2,a_1;b_n,b_{n-1},\cdots\cdots b_2,b_1)$ (1)

由于在正规基下，平方运算仅相当于一位循环移位，可以得出：

$D^2=(d_{n-1},d_{n-2},\cdots\cdots,d_1,d_n)=A^2\cdot B^2=(a_{n-1},a_{n-2},\cdots\cdots,a_1,a_n)\cdot(b_{n-1},b_{n-2},\cdots\cdots,b_1,b_n)$

因此 $d_n$ 可以通过式(1)中相同的函数 $f$ 得到：

$d_n=f(a_{n-1},a_{n-2},\cdots\cdots,a_1,a_n;b_{n-1},b_n,\cdots\cdots,b_1,b_n)$

通过重复的平方，很容易有下面的结论：

$d_{n-1}=f(a_{n-2},\cdots\cdots,a_1,a_n,a_{n-1};b_{n-2},\cdots\cdots,b_1,b_n,b_{n-1})$

$d_{n-2}=f(a_{n-3},\cdots\cdots,a_1,a_n,a_{n-1},a_{n-2};b_{n-3},\cdots\cdots,b_1,b_n,b_{n-1},b_{n-2})$

……

$d_2=f(a_1,a_n,\cdots\cdots,a_3,a_2;b_1,b_n,\cdots\cdots,b_3,b_2)$

由上面的叙述可以构造 $GF(2^n)$上 Massey-Omura 乘法器的逻辑图(见图 1)：

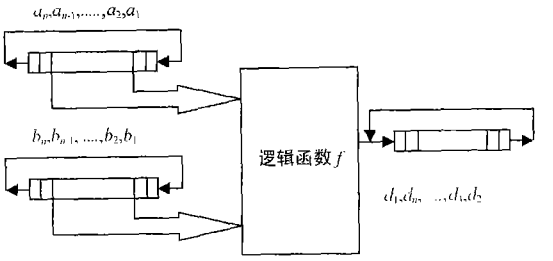



图 1

可以看出设计逻辑函数是 Massey-Omura 乘法器的关键，但是在一般情况下求逻辑函数是比较复杂的，非常不适合编程实现，因此一般选取存在优化正规基的有限域 $GF(2^n)$．针对Ⅰ型优化正规基，人们提出了许多改进的方法[5,6]，而针对基于Ⅱ型优化正规基的乘法算法的文献却很少．针对Ⅱ型优化正规基，本文提出了一种简单的，易于 FPGA 编程实现的方法．

## 3 基于Ⅱ型优化正规基的乘法算法

如果 $p=2n+1$ 是素数，而且满足引理 3 的条件，则 $GF(2^n)$中存在Ⅱ型优化正规基，正规元素如下构造：$\beta=\gamma+\gamma^{-1}$，其中 $\gamma^{2n+1}=1$ 并且 $\gamma^i\neq1(1\leqslant i<2n+1)$．正规基为：

$$M=\{\beta,\beta^2,\beta^{2^{n-2}},\beta^{2^{n-1}}\}=\{\gamma+\gamma^{-1},\gamma^2+\gamma^{-2},\cdots\cdots,\gamma^{2^{n-2}}+\gamma^{-2^{n-2}},\gamma^{2^{n-1}}+\gamma^{-2^{n-1}}\}$$

下面我们对 $M$ 中的基元素进行一种简单的变换而得到另外一个基 $N$：

(1)如果 2 是模 $2n+1$ 的原根．，那么 2 的幂次模 $2n+1$ 的集合为：

$P_1=\{\langle2\rangle_{2n+1},\langle2^2\rangle_{2n+1},\langle2^3\rangle_{2n+1},\cdots\cdots,\langle2^{2n}\rangle_{2n+1}\}$

与 $Q_1=\{1,2,3,4\cdots,2n\}$相等

因此，形式为 $\gamma^{2^i}+\gamma^{-2^i}$的基元素可以改写为 $\gamma^j+\gamma^{-j}$，$j\in[1,2m]$．而且，因为 $\gamma^j+\gamma^{-j}=\gamma^{(2n+1)-j}+\gamma^{-(2n+1)+j}$，如果 $j\geqslant n+1$，可以把 $\gamma$ 的幂次限制在$[1,n]$．

(2)如果 $2n+1$ 是模 4 为 3 的一个素数，并且 2 是模 $2n+1$ 的二次剩余，那么 2 的幂次模 $2n+1$ 的集合为：

$P_2=\{\langle2\rangle_{2n+1},\langle2^2\rangle_{2n+1},\langle2^3\rangle_{2n+1},\cdots\cdots,\langle2^{n-1}\rangle_{2n+1},\langle2^n\rangle_{2n+1}\}$

是由在区间$[1,2n]$中 $n$ 个不同的整数组成．将其这样变换：假如 $<2^i>_{2n+1}$在区间$[1,n]$，则保持原值，而若$\langle2^i\rangle_{2n+1}$在区间$[n+1,2n]$，将其转变成$(2n+1)-\langle2^i\rangle_{2n+1}$，显然$(2n+1)-\langle2^i\rangle_{2n+1}$在区间$[1,n]$，可知这样变换后得到的集合与集合 $Q_2=\{1,2,3,4,\cdots\cdots,n\}$相等．

因此有这样的结论，形式为 $\gamma^{2^i}+\gamma^{-2^i}$的基元素可以改写为 $\gamma^j+\gamma^{-j}$，$j\in[1,n]$基 $M$ 和基 $N$ 可以表示如下：

$$M=\{\gamma+\gamma^{-1},\gamma^2+\gamma^{-2},\cdots\cdots,\gamma^{-2^{n-2}}+\gamma^{2^{n-2}},\gamma^{2^{n-1}}+\gamma^{-2^{n-1}}\}$$

$$N=\{\gamma+\gamma^{-1},\gamma^2+\gamma^{-2},\cdots\cdots,\gamma^{2^{n-1}}+\gamma^{-(n-1)},\gamma^{2^n}+\gamma^{-n}\}$$

假设在基 $M$ 下，域中元素 $A=(a_n,a_{n-1},\cdots\cdots,a_2,a_1)$ 表示如下：

$$A=a_1\beta+a_2\beta^2+a_3\beta^{2^2}+\cdots\cdots+a_n\beta^{2^{n-1}}\quad \beta=\gamma+\gamma^{-1}$$

在基 $N$ 下 $A$ 可以表示如下：

$$A=a'_1\beta_1+a'_2\beta_2+a'_3\beta_3+\cdots\cdots+a'_n\beta_n,\quad \beta_i=\gamma^i+\gamma^{-i}$$

由基 $M$ 和基 $N$ 之间的关系，很容易得出 $a'_j=a_i$，$i,j$ 的关系如下：

$$j=\begin{cases}k, & k\in[1,m]\\(2n+1)-k, & k\in[1+m,2m]\end{cases}\qquad(2)$$

这里 $k=2^{i-1}(\mathrm{mod}\ 2n+1)$，$i=1,2,\ldots,n$.

由上面的关系，显然有　　$a_1=a'_1$　　(3)

根据式(2)和(3)，我们提出了一种域 $GF(2^n)$ 中元素基于 $M$ 的乘法算法，步骤如下：

(1)将基 $M$ 下的元素转换为基 $N$ 下的元素；

(2)基 $N$ 下的元素相乘，得到基 $N$ 下的结果的 $d_1$(也就是在基 $M$ 下的 $d_1$)；

(3)将 $M$ 下的元素一位循环移位，重复 1,2；

(4)由 2 中得到的结果进行移位可以得到最终的乘法结果.

算法的具体实现如下：

在基 $M$ 下：　$D=A\cdot B=\sum_{i=1}^{n}a_i\beta^{2^{i-1}}\cdot\sum_{j=1}^{n}b_j\beta^{2^{j-1}}$

根据式(2)将上式转换为基 $N$ 下的乘法，有：

$$\begin{aligned}D=A\cdot B&=\sum_{i=1}^{n}a_i\beta^{2^{i-1}}\cdot\sum_{j=1}^{n}b_j\beta^{2^{j-1}}\\&=\sum_{i=1}^{n}a'_i\beta_i\cdot\sum_{j=1}^{n}b'_j\beta_j\\&=\sum_{i=1}^{n}a'_i(\gamma^i+\gamma^{-i})\sum_{j=0}^{n}b'_j(\gamma^j+\gamma^{-j})\\&=\sum_{i=1}^{n}\sum_{j=1}^{n}a_ib_j(\gamma^{i-j}+\gamma^{-(i-j)})\\&\quad+\sum_{i=1}^{n}\sum_{j=1}^{n}a'_ib'_j(\gamma^{i+j}+\gamma^{-(i+j)})\\&=C_1+C_2\end{aligned}$$

根据算法步骤 2，我们只关心 $d_1$，即 $\beta_1$ 的系数.

在 $C_1$ 中 $\beta_1$ 的系数为：

$$\sum_{\substack{1\le i,j\le n\\|i-j|=1}}a'_ib'_j=(a'_1b'_2+a'_2b'_1)+(a'_2b'_3+a'_3b'_2)+\cdots\cdots(a'_{n-1}b'_n+a'_nb'_{n-1})$$

在 $C_2$ 中：

$$\begin{aligned}C_2&=\sum_{i=1}^{n}\sum_{j=1}^{n}a'_ib'_j(\gamma^{i+j}+\gamma^{-(i+j)})\\&=\sum_{i=1}^{n}\sum_{j=1}^{n-i}a'_ib'_j(\gamma^{i+j}+\gamma^{-(i+j)})\\&\quad+\sum_{i=1}^{n}\sum_{j=n-i+1}^{n}a'_ib'_j(\gamma^{i+j}+\gamma^{-(i+j)})\\&=D_1+D_2\end{aligned}$$

易知，在 $D_1$ 中 $\beta_1$ 的系数为 0；

而　$D_2=\sum_{i=1}^{n}\sum_{j=n-i+1}^{n}a'_ib'_j(\gamma^{i+j}+\gamma^{-(i+j)})$

$$=\sum_{i=1}^{n}\sum_{j=n-i+1}^{n}a'_ib'_j(\gamma^{2n+1-(i+j)}+\gamma^{-(2n+1-(i+j))})$$

可以得出 $D_2$ 中 $\beta_1$ 的系数为 $a'_nb'_n$

因此 $\beta_1$ 的系数即 $d_1$ 为：

$$(a'_1b'_2+a'_2b'_1)+(a'_2b'_3+a'_3b'_2)+\cdots\cdots+(a'_{n-1}b'_n+a'_nb'_{n-1})+a'_nb'_n\qquad(4)$$

由于算法的步骤 1 只是乘法元素各位上的值的交换，不需要任何 AND 门或 XOR 门，而步骤 2 中计算 $d_1$ 所需要的 AND 门个数为 $n$，所需的 XOR 门个数为 $n-1$，因此该算法所需要的硬件资源很少.该算法计算所需时间为 $n$ 个时钟周期.

## 4　乘法器的 FPGA 实现

FPGA 是高密度现场可编程逻辑芯片，能够将大量的逻辑功能集成于一个单片集成电路中，其集成度已发展到现在的几百万门.现场可编程门阵列(FPGA)是由掩膜可编程门阵列(MPGA)和可编程逻辑器件二者演变而来的，并将它们的特性结合在一起，因此 FPGA 既有门阵列的高逻辑密度和通用性，又有可编程逻辑器件的用户可编程特性.

对 FPGA 器件编程一般都是通过 VHDL(Very High Speed Integrated Circuit Hardware Description Language)语言来实现的.VHDL 主要用于描述数字系统的结构、行为、功能和接口，非常适用于可编程逻辑芯片的应用设计.与其它的 HDL 相比，VHDL 具有更强的行为描述能力，从而决定了它成为系统设计领域最佳的硬件描述语言.我们用 VHDL 来实现该乘法器.

算法步骤 2 中求 $d_1$ 可以用 VHDL 语言简单实现如下：

```
A: STD_LOGIC_VECTOR(n downto 1)
B: STD_LOGIC_VECTOR(n downto 1)
FUNCTION GetD1(A: std_logic_vector(n downto 1); B:
std_logic_vector(n downto 1)) return std_logic is
variable d1: std_logic;
variable Temp: std_logic_vector(n-1 downto 1);
BEGIN
Temp: = A(n-1 downto 1) and B(n downto 2);
d1: = '0';
for i in n-1 downto 1 loop
d1: = d1 xor Temp(i);
end loop;
Temp: = A(n downto 2) and B(n-1 downto 1);
for i in n-1 downto 1 loop
d1: = d1 xor Temp(i);
end loop;
d1: = d1 xor (A(n) and B(n));
return d1;
END GetD1;
```

其中 $A=(a'_n,a'_{n-1},\cdots\cdots,a'_1)$，$B=(b'_n,b'_{n-1},\cdots\cdots,b'_1)$

可以看出求 $d_1$ 非常简单，从而避免了 Massey-Omura 乘法器的函数 $f$ 的复杂性，而且此函数对任何存在Ⅱ型优化正规

基的 $n$ 都是适合的,因此避免了 Massey-Omura 乘法器的函数 $f$ 对不同的域均不相同的缺点.

## 5 结束语

本文提出了 $GF(2^n)$域上的一种Ⅱ型优化正规基乘法器,该乘法器具有 Massey-Omura 乘法器的优点,又避免了其不足,易于编程,适合 FPGA 实现.

在椭圆曲线密码体制中,有限域上的乘法运算是占了整个运算的很大比例,所以有限域上的乘法运算的效率关系到整个体制的执行效率.本文提出的适合 FPGA 实现的乘法器,为最终用 FPGA 实现椭圆曲线密码体制提供了有效的方法.

**参考文献:**


[1] R M Wilson. Optimal normal bases in GF($p^n$)[J]. Discrete Applied Mathematics, 1988/89, 22: 149 - 161.

[2] ANSI X.962, Public Key Cryptography for the Financial Services Industry-the Elliptic Curve Digital Signature Algorithm (ECDSA)[S]. 1999.

[3] ANSI X.962, Public Key Cryptography for the Financial Services Industry-Elliptic Curve Key Agreement and Transposition Standards[S]. 2000.

[4] J Omura, J Massey. Computational Method and Apparatus for Finite Field Arithmetic[P]. U S Patent Number 4,587,627, May 1986.

[5] C K Koc, B Sunar. Low-complexity bit-parallel canonical and normal basis multipliers for a class of finite fields [J]. IEEE Transactions on Computers, 1998, 3, 47(3): 353 - 356.

[6] M A Hasan, M Z Wang, V K Bhargava. A modified Massey-Omura parallel multiplier for a class of finite fields [J]. IEEE Transactions on Computers, 1993, 11, 42(10): 1278 - 1280.


**作者简介:**




**方 冰** 男,1978 年生于武汉,现就读于清华大学计算机系,硕士研究生,主要研究方向为信息安全.

**樊海宁** 男,1971 年生于宝鸡,现就读于清华大学计算机系,博士研究生,主要研究方向为信息安全,数据加密算法.

**戴一奇** 男,1946 年生于北京,清华大学教授,博士生导师,研究方向为网络信息安全.