广义最优扩域上的快速运算

王庆先 孙世新
(电子科技大学 计算机科学与工程学院 成都 610054)

摘 要 在椭圆曲线密码体制(ECC)中，无论是最终性能或是存储需求，最优扩域都具有明显优势。但由于ECC要求有限域F_p是素域，而伪Mesernne素数却难以选取，且难以满足p恰好可由目标处理机的一个寄存器表示的要求。该文利用广义Mersenne数代替伪Mesernne数，提出了广义最优扩域的概念，研究了其上的快速乘法运算和模约简运算，为乘法运算给出了通用的计算量公式，为模约简运算给出了具体的运算公式。推广了Bailey, Mihăilescu和Woodbury等在最优扩域上的相应结果。

关键词 保密通信，椭圆曲线密码体制，广义最优扩域，乘法运算，模约简运算
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2006)03-0404-03

Fast Arithmetic in Generalized Optimal Extension Fields

Wang Qing-xian Sun Shi-xin
(*Department of Computer Science, UESTC, Chengdu* 610054, *China*)

Abstract In Elliptic Curves Cryptosystems (ECC), the optimal extension fields is preferable to others method, whether concerns performance or memory request. But, it is very difficult to choose pseudo-Mersenne prime numbers, and satisfy the condition that p just is presented by a register of processor. This paper replaces pseudo-Mersenne numbers by generalized Mersenne numbers, provides a new notation-Generalized Optimal Extension Fields(GOEFs), and studies the fast arithmetic about multiplication and modular reduction in GOEFs, finally, deduces common formulas for multiplication and some more general formulas for modular reduction in GOEFs. The results in this paper extend the corresponding work on arithmetic of Bailey, Mihăilescu, and Woodbury in OEFs.

Key words Private communication, Elliptic curves cryptosystems, Generalized optimal extension fields, Multiplication, Modular reduction

1 引言

最优扩域(Optimal Extension Fields, OEFs)分别由Bailey和Paar[1]以及Mihăilescu[2]在1998年和1997年独立提出的。OEFs是一簇具有特殊性质的有限域，在其上能够利用软件有效执行域运算，其主要动机在于使被选出的域参数与机器更匹配，从而使得域运算操作能够更有效执行。特别地，如果素数p恰好可由目标处理机的一个寄存器表示，则这种最优扩域GF(p^m)上的域运算尤其有效[3,4]。

Smart[5]分别对一般素域、广义Mersenne素域、特征为2的非素域和最优扩域等4种域上的域运算性能进行了实验分析和比较后认为：在ECC中，无论是最终性能，还是存储要求，最优扩域都具有明显优势。

但是，通常情况下，当c较小时，形如$p=2^n-c$的素数较少。例如，李[6]令机器字长是32位，$n=32\times d$, $5\le d\le 16$, $c=1,3,5,7$，经过搜索发现，不存在这种形式的素数。但由于ECC要求有限域F_p是素域，而伪Mesernne素数却难以选取，且难以满足p恰好可由目标处理机的一个寄存器表示的要求。

因此，本文使用广义Mersenne数代替伪Mesernne数，提出了广义最优扩域的概念，研究了其上的快速乘法运算和模约简运算，为乘法运算给出了通用的计算量公式，为模约简运算给出了具体的运算公式，得到了更一般的结果，推广了Bailey和Paar[1], Mihăilescu[2], Bailey[3]和Woodbury[4]等在最优扩域上的相应结果。

本文余下部分安排如下：第2节给出相关概念和定理；第3节研究广义最优扩域GF(P^m)上的乘法运算和模约简运算；第4节比较相关结果；第5节得出结论和进一步的工作。

2 定义和引理

设p是素数，m是一个正整数，GF(P)表示特征为p的有限域，GF(P^m)表示有限域GF(P)的m次扩域。

定义1[7] 令t是机器字长，如果$f(x)$是首一d次整系数多项式，且$f(x)$只有少数几个非零项，则称$f(2^t)$是广义Mersenne数。

注意：$f(x)$应满足下面的条件：

(1) $f(x)$的次数尽可能高，但不超过p的字长。通常$f(t)$的次数满足条件：

$$\text{word}(p)\approx lw,\quad \text{word}(t)\times\deg(f)\approx\text{word}(p) \tag{1}$$

其中word(·)表示一个整数的字长，w是处理机的字长，$l>0$是一任意正整数。如果条件(1)不能满足，则提出的方法可能慢于经典算法。

(2) 避免使用大于1的系数；

2004-06-25 收到，2005-02-04 改回
国家自然科学基金(60373109)资助课题

(3) 多项式的项数尽可能少，设m次多项式$f(x)$的项数为l，则多项式转换步数为$2m-2$，必须的加法或者减法数目是$(l-1)(m-1)$；

(4) $f(x)$是不可约多项式，因为这样的$p=f(x)$才可能是素数。

定义2 有限域GF(p^m)是广义最优扩域，如果：

(1) p是广义Mersenne素数；

(2) 在GF(p)上存在不可约三项式$f(x)=x^m-x^k-w$。

例如：$p=2^{192}-2^{64}-1$是素数，$f(x)=x^{14}-x^7-1$是GF(p)上的不可约三项式，则GF($(2^{192}-2^{64}-1)^{14}$)就是广义最优扩域。

下面给出多项式在GF(p)上不可约的充要条件。

定理1[8] 令$p_1,p_2,\cdots,p_k$是m的所有素因数，$m_i=m/p_i(1\le i\le k)$。次数为m的多项式$f\in F_p[x]$是$F_p[x]$上的不可约多项式当且仅当$\gcd(f,x^{p^{m_i}}-x \bmod f)=1$，$(1\le i\le k)$，且$f\mid x^{p^m}-x$。

3 广义最优扩域(GOEFs)上的运算

利用标准基表示GOEFs的元素，即对任意$A\in \mathrm{GF}(p^m)$，

$$A=\sum_{i=0}^{m-1}a_ix^i=a_0+a_1x+\cdots+a_{m-1}x^{m-1},\quad a_i\in \mathrm{GF}(p) \tag{2}$$

3.1 加法/减法

任意$A,B\in \mathrm{GF}(p^m)$，设$A=\sum_{i=0}^{m-1}a_ix^i$，$B=\sum_{i=0}^{m-1}b_ix^i$，$a_i,b^i\in \mathrm{GF}(p)$，则

$$A\pm B=\sum_{i=0}^{m-1}a_ix^i\pm\sum_{i=0}^{m-1}b_ix^i=\sum_{i=0}^{m-1}c_ix^i,\quad c_i=(a_i\pm b_i)\bmod p \tag{3}$$

3.2 乘法

任意$A,B\in \mathrm{GF}(p^m)$，设$A=\sum_{i=0}^{m-1}a_ix^i$，$B=\sum_{i=0}^{m-1}b_ix^i$，$a_i,b_i\in \mathrm{GF}(p)$，则$C=AB$分以下两步进行。

3.3 多项式乘法

$$C'=A\times B=\sum_{i=0}^{2m-2}c'_ix^i \tag{4}$$

按照多项式乘法规则，需要m^2个乘法，$(m-1)^2$个加法。由于一个乘法操作时间远大于一个加法操作时间，因此利用增加加法数目的方式来减少乘法数目，可以有效减少运算时间。

定理2 设$D_i=a_ib_i$，$(0\le i\le m-1)$，$d_{ij}=D_i+D_j$，$(0\le i\le m-2,\ j=i+1)$，$D_{ij}=(a_i+a_j)(b_i+b_j)$，$(0\le i\le m-2,\ i+1\le j\le m-1)$，则$AB$所需乘法数为$m(m+1)/2$，加法数$n$至多为

$$n=\begin{cases}(3m^2+5m-12)/2, & m>3\\ (m-1)(5m-2)/2, & m=1,2,3\end{cases}.$$

证明 设按照多项式乘法规则所得x^i的系数为c'_i，则

$$c'_i=\begin{cases}\sum_{k=i-m+1}^{m-1}a_kb_{i-k}, & m\le i\le 2(m-1)\\ \sum_{k=0}^{i}a_kb_{i-k}, & 0\le i\le m-1\end{cases}$$

根据对称性，仅考虑$c'_i(0\le i\le m-1)$，用D_i，$D_{ij}(0\le i\le m-1)$的值代替a_kb_{i-k}，$(0\le k\le i)$，得

$$c'_i=\sum_{k=0}^{i}a_kb_{i-k}=\begin{cases}(D_{0i}-D_0-D_i)+\cdots+\left(D_{i/2-1,i/2+1}-D_{i/2-1}-D_{i/2+1}\right)\\ +D_{i/2,i/2}, & i\text{是偶数}\\ (D_{0i}-D_0-D_i)+\cdots+\left(D_{(i-1)/2,(i+1)/2}-D_{(i-1)/2}-D_{(i+1)/2}\right), & i\text{是奇数}\end{cases} \tag{5}$$

式(5)表明，利用D_i,D_{ij}，计算c'_i不再需要乘法，从而乘法数目为$m(m+1)/2$。

又由D_i,D_{ij}的假设和式(5)知，当i是偶数时，计算c'_i所需加法数为$5i/2$；当i是奇数时，计算c'_i需加法数为$(5i+3)/2$。另外，当m是偶数时，偶数项比奇数项多一项，即偶数项有$(m-1)/2$项，奇数项有$(m-3)/2$项；当m是奇数时，偶数项和奇数项一样多，都为$(m-1)/2$项。

于是计算所有$c'_i(0\le i\le 2m-1)$所需加法数目n_1为

$$n_1=\begin{cases}2\sum_{i=0}^{(m-3)/2}[5i+(5(2i+1)+3)/2]+5(m-1)/2\\ \quad=(m-1)(5m-2)/2, & m\text{是奇数}\\ 2\sum_{i=0}^{(m-2)/2}[5i+(5(2i+1)+3)/2]-(5m-2)/2\\ \quad=(m-1)(5m-2)/2, & m\text{是偶数}\end{cases}$$

(1) $m>3$时，利用d_{ij}的假设，为了简单，仅考虑d_{ij}被使用一次的情形，可以再减少的加法数目n_2为

$$n_2=2[m(m-1)/2-(2m-3)]-(m-1)=m^2-6m+7$$

(2) $m=1,2,3$时，不会使用d_{ij}，因此加法数与n_2无关，从而其加法数为$(m-1)(5m-2)/2$。　　证毕

3.4 模化简

设
$$C=C' \bmod f(x)=\sum_{i=0}^{2m-2}c'_ix^i \bmod(x^m-x^k-a)=\sum_{i=0}^{m-1}c_ix^i,\quad c_i\in \mathrm{GF}(p)$$

则

$$(1)\ m<2k,\begin{cases}c_i=c'_i+a(c'_{m+i}+c'_{2m-k+i}),\\ \quad i=0,1,\cdots,k-1\\ c_{k+i}=c'_{k+i}+c'_{m+i}+c'_{2m-k+i}+ac'_{m+k+i},\\ \quad i=0,1,\cdots,k-2\\ c'_{2m-1}=0\end{cases} \tag{6}$$

$$(2)\ m=2k,\begin{cases}c_i=c'_i+a(c'_{m+i}+c'_{2m-k+i})\\ c_{k+i}=c'_{k+i}+c'_{2k+i}+(a+1)c'_{3k+i},\\ \quad i=0,1,\cdots,k-1\\ c'_{2m-1}=0\end{cases} \tag{7}$$

$$(3)\ m>2k,\begin{cases}c_i=c'_i+a(c'_{m+i}+c'_{2m-k+i}),\\ \quad i=0,1,\cdots,k-1\\ c_{k+i}=c'_{k+i}+c'_{m+i}+c'_{2m-k+i}+ac'_{m+k+i},\\ \quad i=0,1,\cdots,k-2\\ c_{2k-1+i}=c'_{2k-1+i}+c'_{m+k-1+i}+ac'_{m+2k-1+i},\\ \quad i=0,1,\cdots,m-2k\\ c'_{2m-1}=0\end{cases} \tag{8}$$

由式(6) – 式(8)可以看出，在模约简运算中，除法完全被加法和乘法代替。其所需的加法和乘法数目如表1所示。

表 1 模约简所需运算数目

	加法数	乘法数
$m<2k$	$5k-4$	$5k-4$
$m=2k$	$4k-2$	$m-1$
$m>2k$	$2m+k-3$	$m-1$

4 性能比较

4.1 与多项式乘法规则结果比较

按照多项式乘法规则，所需乘法和加法数目分别为m^2和$(m-1)^2$，而采用定理2的假设方式，所需乘法数目为$m(m+1)/2$，加法数目至多为$(3m^2+5m-12)/2$个。假设一个乘法所需时间是一个加法所需时间的t倍，令$tm^2+(m-1)^2=tm(m+1)/2+(3m^2+5m-12)/2$，则

$$t=(m^2+9m-14)/(m^2-m)$$
$$=(1-9/m-14/m^2)/(1-1/m)\to 1,\ (m\to\infty) \qquad (9)$$

图1给出了m的取值从2到1000000时，t的取值情况。由图1可以看出，对不同的m，当t取对应曲线上方的值时，本文方法优于传统方法。而事实上乘法运行时间远大于加法运行时间，因此，本文方法所需运算时间远小于一般多项式乘法法则所需时间。

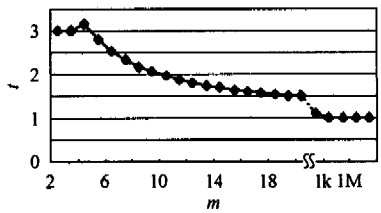

图1 t和m的关系图

Fig.1 The graph of the relation between t and m

4.2 与 Bailey 结果的比较

Bailey在文献[3]提出了一种快速乘法方式，但该方法只对m是偶数，且$E_0(x),E_1(x),E_2(x)$已有最少乘法数目和加法数目的情形才有效。例如，$m=6$时，

$$A(x)=a_5x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0,$$
$$B(x)=b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x+b_0 \text{ 则}$$
$$A(x)B(x)=E_2(x)x^6+(E_1(x)-E_2(x)-E_0(x))x^3+E_0(x)$$

其中

$$A_l(x)=a_5x^2+a_4x+a_3,\quad A_h(x)=a_2x^2+a_1x+a_0;$$
$$B_l(x)=b_5x^2+b_4x+b_3,\quad B_h(x)=b_2x^2+b_1x+b_0;$$
$$E_2(x)=A_l(x)B_l(x),\ E_1(x)=(A_l(x)+A_h(x))(B_l(x)+B_h(x)),$$
$$E_0(x)=A_h(x)B_h(x)。$$

Bailey 指出乘法数目＝6×3＝18，加法数目＝3×13＋(3＋3)+(5+5)+4=59，但按照本文的方法，当 m=6 时，乘法数目＝21，加法数目＝63。

然而，当 m=5 时，该方法失效。因为，此时，

$$A(x)B(x)=E_2(x)x^4+(E_1(x)-E_2(x)-E_0(x))x^2+E_0(x)$$

其中

$$A_l(x)=a_4x^2+a_3x+a_2,\quad A_h(x)=a_1x+a_0;$$
$$B_l(x)=b_4x^2+b_3x+b_2,\quad B_h(x)=b_1x+b_0;$$
$$E_2(x)=A_l(x)B_l(x),\ E_1(x)=(A_l(x)+A_h(x))(B_l(x)+B_h(x)),$$
$$E_0(x)=A_h(x)B_h(x)。$$

此时，乘法数目＝6×3＝18，加法数目＝13×3＋(2+2)＋(5+5)+6=59，但本文方法却得出乘法数目＝15，加法数目＝44，优于文献[3]的方法。

由此，我们得出结论：文献[3]的方法仅适合m是偶数，且$E_0(x),E_1(x),E_2(x)$已有最少乘法数目和加法数目的情形，而本文方法对所有m值都适用，因此比文献[3]的方法更有效，更适用。

5 结束语

本文推广了 Bailey 和 Paar, Măilescu, Bailey 和 Woodbury 等在最优扩域上所做工作：提出了广义最优扩域概念，并在广义最优扩域上研究了快速乘法运算和模约简运算，给出了具体的运算量公式，得到了更一般的结果，并作出相关比较。我们将进一步研究广义最优扩域上的求逆技术和广义最优扩域的构造，为广义最优扩域上的运算建立完整的体系。

参 考 文 献

[1] Bailey D V, Paar C. Optimal extension fields for fast arithmetic in public-key algorithms. In H. Krawczyk, editor, Advances in Cryptology-CRYPTO'98, Berlin, Germany, Springer- Verlag, 1998, volume LNCS 1462: 472-485.

[2] Mihăilescu P. Cyclotomy of rings & primality testing. [PhD thesis], Swiss Federal Institute of Technology, Zurich, 1997.

[3] Bailey D V, Paar C. Efficient arithmetic in finite field extensions with application in Elliptic curve cryptography. *Journal of Cryptology*, 2001, 14(3): 153-176.

[4] Woodbury A D. Efficient algorithms for elliptic curve cryptosystems on embedded systems, [Master Thesis], Department of Electrical & Computer Engineering, Worcester Polytechnic Institute, 2001，9.

[5] Smart N P A comparison of different finite fields for use in elliptic curve cryptosystems. Technical Report CSTR-00-007, University of Bristol, June 2000.

[6] 李俊全. 椭圆曲线公钥密码体制的设计与分析, [博士论文],中国科学院数学与系统科学研究院, 2001, 5.

[7] Chung J, Hasan A. More generalized mersenne numbers, Technical Report CORR99-39, Centre for Applied Cryptographic Research, University of Waterloo, http://cacr.uwaterloo.ca/techreports/1999/corr99-39.ps.

[8] Michael O R. Probabilistic algorithms in finite fields. SIAM JournalonComputing,1980,9:273-280. http://citeseer.ist.psu.edu/rabin79probabilistic.html

王庆先： 女，1970 年生,讲师. 研究方向为椭圆曲线密码体制与并行算法.

孙世新： 男,1940 年生，教授. 研究方向为组合数学与并行算法.