

一种高效的多基标量乘扩展算法

罗琴灵, 蒋朝惠

(贵州大学 计算机科学与技术学院, 贵州 贵阳 550025)

摘要: 为了提高椭圆曲线中最基本、最耗时的标量乘法的效率, 基于 Extended DBNS 以及半点运算的理论, 提出了一种新的二进制域上椭圆曲线 $GF(2^m)$ 标量 k 的多基表示方法, 并在此基础上给出了改进后的多基链标量乘法。在美国国家标准技术研究所 (NIST) 推荐的椭圆曲线上, 实验结果表明, 当预计算点的存储个数 $N = 2, N = 5$ 时, 新算法比 Purohit 等提出的算法效率分别至少提高了 29.1%、35.0%, 比洪银芳等提出的算法效率分别至少提高了 7.8%、6.4%。新算法通过增加少量的预计算存储空间, 有效降低了标量乘法的运算量, 使标量乘法的运算更高效。因此, 该算法可以较好地应用到无线传感器网络等计算资源受限的领域中。

关键词: 椭圆曲线密码学; 半点运算; 扩展多基表示; 标量乘法

中图分类号: TP309.7

文献标识码: A

文章编号: 1673-629X(2015)05-0095-04

doi: 10.3969/j.issn.1673-629X.2015.05.023

An Efficient Multi-base Scalar Multiplication Algorithm

LUO Qin-ling, JIANG Chao-hui

(College of Computer Science and Technology, Guizhou University, Guiyang 550025, China)

Abstract: In order to improve the efficiency of the most basic and time-consuming scalar multiplication on elliptic curve, based on the theory of extended DBNS and point halving, not only propose a new method of MBNS of the scalar k on binary domain elliptic curve $GF(2^m)$, but also show the improved scalar multiplication algorithm using multi-base chain. In the United States National Institute of Standards and Technology (NIST) recommended elliptic curve, the experimental results show that when the stored number of precalculated point $N = 2, N = 5$, efficiency of the new algorithm is increased by 29.1%, 35.0% at least than that proposed by Purohit, increased by 7.8% and 6.4% at least than that proposed by Hong Yinfang. By adding a small amount of calculation storage space, the new algorithm can effectively reduce the computational complexity of scalar multiplication, which leads the scalar multiplication operation more efficient. Therefore, the algorithm can be applied to the domain of wireless sensor network and other limited computing resources.

Key words: Elliptic Curve Cryptography (ECC); point halving; Multi-Base Number System (MBNS); scalar multiplication

0 引言

Miller^[1] 和 Koblitz^[2] 分别在 1986 年和 1987 年提出了 Elliptic Curve Cryptography (椭圆曲线密码体制), ECC 的安全性基于求解椭圆曲线离散对数难的问题, 即考虑方程 $Q = kP$, 其中 $Q, P \in E_p(a, b)$ 。当得到给定的 k 和 P 的值, 计算 Q 的值是比较容易的, 而当得到了 Q 和 P 的值要计算 k 的值则非常困难。

标量乘法即 $[k]P$ 的计算作为椭圆曲线加密中最核心、最基本的运算, 却也是最耗时的过程, 它的效率决定了整个椭圆曲线加密系统的性能^[3]。在标量 k 的表示上, 由于双基数系统 (DBNS)^[4] 的独特优势, 引起了人们更多的关注。Mishra^[5] 等将双基扩展到多基,

并且提出了相应的 5 倍点计算公式和对应的标量乘法, 计算速度得到了有效提高。文献[6]在半点运算 (point halving)^[7] 与多基表示的基础上, 结合扩展的双基数系统 (Extended Double Base Number System, Extended DBNS)^[8] 提出了一种新的多基表示标量乘扩展算法。该算法降低了标量乘法的计算复杂度及多基链的链长, 从而达到了效率上的提高。

近年来, 许多专家学者对椭圆曲线标量乘算法的实现效率问题进行了深入研究, 虽然在一定程度上提高了其效率, 但效果并不十分理想。因此, 文中以整数 k 的多基表示、Extended DBNS^[9] 以及半点运算的理论为基础, 提出了二进制域上椭圆曲线标量 k 的 d

收稿日期: 2014-06-24

修回日期: 2014-09-25

网络出版时间: 2015-04-22

基金项目: 贵州省科学技术基金项目 (黔科合 J 字 [2012] 2128 号)

作者简介: 罗琴灵 (1988-), 女 (苗族), 硕士研究生, CCF 会员, 研究方向为信息安全; 蒋朝惠, 教授, 研究方向为信息安全。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20150422.0950.004.html>

(1/2)^{"3"7^w} 多基表示形式,同时给出了一个更为高效的标量乘扩展算法。

1 背景知识

1.1 整数 k 的多基表示

多基链是双基链的扩展,具有较高的冗余性,与其他的标量表示相比,其链长更短、非零比的数目也更少,能有效地减少标量乘法的运算量^[10]。若整数 k 表示成小整数集 $B = \{b_1, b_2, \dots, b_l\}$ 元素的和形式: $k = B(\sum_{j=1}^m s_j b_1^{e_j}, b_2^{e_2}, \dots, b_l^{e_l},)$, 其中 s_j 是符号位,整数 m 是表达式的长度,则称 k 为使用基集 B 表示的多基表示。

Mishra 等使用 $\{2, 3, 5\}$ 为基集,并使用贪婪算法将整数 k 转换为多基表示,相应整数 k 的多基表示形式如下:

$$k = \sum_{i=1}^m s_i 2^{u_i} 3^{v_i} 5^{w_i}$$

其中, $\{u_i\}, \{v_i\}, \{w_i\}$ 为单调递减序列。

1.2 Extended DBNS 方法

扩展的 DBNS 比原来的双基数系统更加稀疏,Extended DBNS 会牺牲一些存储空间来保存预计算点。和双基链相比,在 200 ~ 500 bits 范围中,当预计算点为 1 时,扩展双基链中整数的平均长度将近减少了 20%,当预计算点为 2 时,减少了近 30%,当预计算点为 4 时,减少了近 38%。在双基数系统中,任意一个正整数 k 能表示成如下形式:

$$k = \sum_{i=1}^m d_i 2^{u_i} 3^{v_i}$$

其中, $|d_i| \in S; u_1 \geq u_2 \geq \dots \geq u_m \geq 0; v_1 \geq v_2 \geq \dots \geq v_m \geq 0$ 。

在上述表达式中,与 3 和 5 互素的奇数组成的集合构成了系数集 S ,并且每个系数集 S_j 由该集合的前 $j + 1$ 个元素组成,例如 $S_2 = \{1, 7, 11\}$, $S_3 = \{1, 7, 11, 13, 17, 19\}$ 。

1.3 半点运算

Knudsen 提出的半点运算是倍点运算的逆运算^[11]。令 $P = (x_p, y_p)$ 为二进制域椭圆曲线上的一点,并且满足 $P \neq -P$,当在仿射坐标下时,点 P 的倍点 $R = 2P = (x_R, y_R)$ 可以通过下式计算得到:

$$x_R = \lambda^2 + \lambda + a \tag{1}$$

$$y_R = x_p^2 + (\lambda + 1)x_R \tag{2}$$

$$\lambda = x_p + y_p/x_p \tag{3}$$

半点运算即是对于给定点 $R = (x_R, y_R)$ 求点 $P = (x_p, y_p)$ 的过程,求解需满足 $R = 2P$ 。具体计算方法为:

第一步:由式(1)得 $\lambda^2 + \lambda = x_R - a$,解出 λ ;

第二步:将第一步求出的 λ 代入式(2),得 $x_p^2 = y_R - (\lambda + 1)x_R$,解出 x_p ;

第三步:将前两步得到的 λ 和 x_p 代入式(3),得 $y_p = \lambda x_p + x_p^2$,解出 y_p ,求解完成^[12]。

若将传统点加操作中所需的倍点操作都用半点操作代替,那么计算速度将会有 39% 的提高。二进制域上 F_2 所涉及的运算有加、减、乘、求逆和平方 5 种^[13]。文中用 I, S, M 分别表示域 F_2 上的求逆、平方和乘法运算,则不同的运算在二进制域中的开销如表 1 所示。

表 1 二进制域中相关运算开销

运算	运算开销
$P/2$	$2M$
$P/2 \pm Q$	$I + 5M$
$P \pm Q$	$I + S + 2M$
$3P$	$I + 4S + 7M$
$3^k P^{[14]}$	$I + (14k + 12)M$
$7P^{[15]}$	$I + 6S + 20M$
$7^k P^{[15]}$	$I + (5k + 1)S + (21k + 3)M$

2 新的多基表示方法及标量乘扩展算法

2.1 新的多基表示方法

文中以整数 k 的多基表示、Extended DBNS 以及半点运算的理论为基础,在洪银芳等以 2、3、5 为底的多基表示思想的基础上,提出标量 k 的新多基表示如下:

$$k = \sum_{i=1}^m d_i \left(\frac{1}{2}\right)^{u_i} 3^{v_i} 7^{w_i}$$

其中, $|d_i| \in S; u_1 \geq u_2 \geq \dots \geq u_m \geq 0; v_1 \geq v_2 \geq \dots \geq v_m \geq 0; w_1 \geq w_2 \geq \dots \geq w_m \geq 0$ 。

可以由相应的贪婪算法很容易地生成此表达式。其中, m 表示多基链的链长, $\{u_i\}, \{v_i\}, \{w_i\}$ 为 3 个单调递减序列,与 3 和 7 互素的奇数组成的集合构成了系数集 S ,并且每个系数集 S_i 由该集合的前 $i + 1$ 个元素组成,例如 $S_1 = \{1, 5\}$ 、 $S_2 = \{1, 5, 11\}$ 、 $S_3 = \{1, 5, 11, 13, 17, 19\}$ 。

2.2 改进的结合半点运算并以 2、3、7 为基的标量乘扩展算法

输入:整数 $k = \sum_{i=1}^m d_i \left(\frac{1}{2}\right)^{u_i} 3^{v_i} 7^{w_i}$, 其中 $|d_i| \in S; u_1 \geq u_2 \geq \dots \geq u_m \geq 0; v_1 \geq v_2 \geq \dots \geq v_m \geq 0; w_1 \geq w_2 \geq \dots \geq w_m \geq 0$; 点 $P \in E(F_{2^n})$ 。

输出:二进制域椭圆曲线 E 上的点 $[k]P \in E(F_{2^n})$ 。

(1) $Z = d_i P$;

(2) for $i = 1$ to $m - 1$; do

(3) $a = u_i - u_{i+1}$;

(4) $b = v_i - v_{i+1}$;
(5) $c = w_i - w_{i+1}$;
(6) if $c = 1, Z = 7Z$; // $7P$ 运算
(7) else $Z = 7^c Z$; // $7^k P$ 运算
(8) if $b = 1, Z = 3Z$; // $3P$ 运算
(9) else $Z = 3^b Z$; // $3^k P$ 运算
(10) $Z = (1/2)^a Z$;
(11) $Z = Z + d_{i+1} P$;
(12) $i = i + 1$;
(13) end for ;
(14) $Z = (1/2)^{u_n} Z$;
(15) if $v_m = 1, Z = 3Z$; // $3P$ 运算
(16) else $Z = 3^b Z$; // $3^k P$ 运算
(17) if $w_m = 1, Z = 7Z$; // $7P$ 运算
(18) else $Z = 7^c Z$; // $7^k P$ 运算
(19) return Z

上述算法是在文献[15]算法的基础上进行改进,运算中的 $P/2$ 、 $P/2 \pm Q$ 、 $P \pm Q$ 、 $3P$ 、 $3^k P$ 、 $7P$ 、 $7^k P$ 都可以通过计算公式快速计算得到,其中 $3^k P$ 通过文献[14]计算、 $7P$ 和 $7^k P$ 通过文献[15]计算。

表2 当 $N = 2$ 时,相应算法的运算量比较

算法	N	NIST B-163($k = 160$ bit)			NIST B-233($k = 233$ bit)			NIST B-283($k = 283$ bit)		
		I	M	总运算量/ M	I	M	总运算量/ M	I	M	总运算量/ M
文献[6]算法	2	51.53	626.34	1 038.58	74.71	901.26	1 498.94	90.42	1 101.34	1 824.70
文献[7]算法	0	79.04	718.23	1 350.55	113.18	1 028.51	1 933.95	138.01	1 241.77	2 345.85
文中算法	2	42.16	620.78	958.06	58.33	852.54	1 319.18	71.17	1 040.11	1 615.47

表3 当 $N = 5$ 时,相应算法的运算量比较

算法	N	NIST B-163($k = 160$ bit)			NIST B-233($k = 233$ bit)			NIST B-283($k = 283$ bit)		
		I	M	总运算量/ M	I	M	总运算量/ M	I	M	总运算量/ M
文献[6]算法	5	44.65	580.30	937.5	64.75	842.07	1 360.07	78.55	1 028.38	1 656.78
文献[7]算法	0	79.04	718.23	1 350.55	113.18	1 028.51	1 933.95	138.01	1 241.77	2 345.85
文中算法	5	37.41	578.46	877.74	51.50	826.14	1 238.14	64.08	1 003.49	1 516.13

从表2可以看出,算法在 NIST B-163、NIST B-233、NIST B-283 椭圆曲线上,文中算法比文献[6]至少提高7.8%,比文献[7]至少提高29.1%,优势明显。

从表3可以看出,算法在 NIST B-163、NIST B-233、NIST B-283 椭圆曲线上,文中算法比文献[6]至少提高6.4%,比文献[7]至少提高35%,效率明显提高。

为了更直观地比较三种算法的效率,以表2和表3中的数据绘制各算法的复杂性曲线,如图1所示。文中假设标量乘法的复杂性与 k 的长度成正比。

从图1中可见,当 $N = 2$ 和 $N = 5$ 时,且 k 长度位于区间160~283 bit,文中算法比文献[6]效率提高

算法复杂度分析:该算法需迭代 $m - 1$ 次,第 i 轮所需的运算量为:

$$C_i = [\delta_{c,i} 7P + (1 - \delta_{c,i}) c_i - 7P] + [\delta_{b,i} 3P + (1 - \delta_{b,i}) - 3P] + [a_i H + A], \begin{cases} i = j \text{ 时}, \delta_{i,j} = 1 \\ i \neq j \text{ 时}, \delta_{i,j} = 0 \end{cases}$$

算法总的运算量为:

$$C = \sum_{i=1}^{m-1} C_i + C_m = \sum_{i=1}^{m-1} C_i + u_m H + [\delta_{w,m} 7P + (1 - \delta_{w,m}) w_m - 7P] + [\delta_{v,m} 3P + (1 - \delta_{v,m}) v_m - 3P]$$

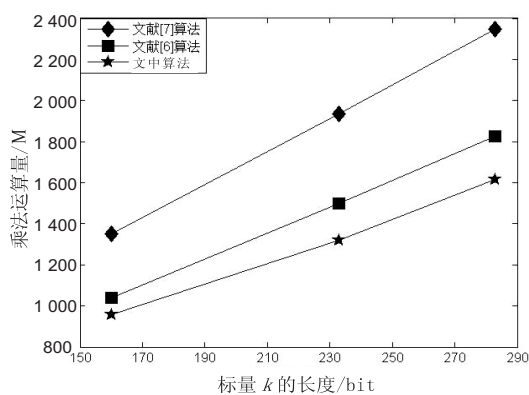
3 效率分析

文献[6-7]是目前运算效率较高的算法,文中在 NIST 推荐的椭圆曲线 NIST B-163、NIST B-233 和 NIST B-283 上分别随机选取1 000组大整数标量 k ,分别使用文献[6-7]及文中算法进行标量乘法运算,再分别计算它们所需底层运算量的平均值。当 $N = 2$ 和 $N = 5$ 时,结果分别如表2和表3所示。其中, N 表示预计算点的存储个数。对于二进制域 F_2 上的椭圆曲线,通常选取 $S = 0.8M, I = 8M$ 。

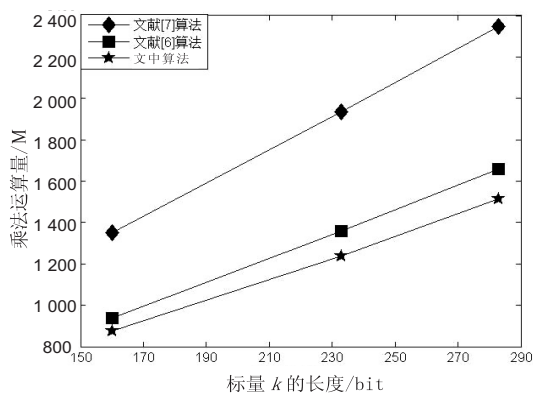
6.4%~12.0%,比文献[7]提高29.1%~36%。随着 k 值的增大,算法运算效率的提高程度有增大的趋势。

4 结束语

文中以整数 k 的多基表示、Extended DBNS 以及半点运算为基础,提出二进制域上椭圆曲线标量 k 的 $d(1/2)^u 3^v 7^w$ 多基表示形式,给出了一种改进的标量乘扩展算法。数值实验结果表明,在美国国家标准技术研究(NIST)推荐的椭圆曲线上,当预计算点的存储个数 $N = 2$ 、 $N = 5$ 时,文中算法比文献[6-7]效率有了不同程度的提高。因而,新算法能推广椭圆曲线密码体制在无线传感器网络等计算资源受限领域中的应用。



N=2 时的运算量曲线



N=5 时的运算量曲线

图 1 相应算法运算量比较

参考文献:


- [1] Miller V S. Use of elliptic curves in cryptography[C]//Proc of CRYPTO'85. [s. l.]: Springer-Verlag, 1986:417-426.
- [2] Koblitz N. Elliptic curve cryptosystems[J]. Mathematics of Computation, 1987, 48(177):203-209.
- [3] 陈厚友, 马传贵. 椭圆曲线密码中一种多标量乘算法[J]. 软件学报, 2011, 22(4):782-788.
- [4] Dimitrov V, Imbert L, Mishra P K. Efficient and secure elliptic curve point multiplication using double base chain[C]//Proc of Cryptology - ASIACRYPT' 05. [s. l.]: Springer-Verlag, 2005.
- [5] Mishra P K, Dimitrov V S. Efficient quintuple formulas for elliptic curves and efficient scalar multiplication using multibase number representation [C]//Proc of ISC ' 07. Valparaiso: Springer-Verlag, 2007.
- [6] 洪银芳, 桂 丰, 丁 勇. 基于半点和多基表示的标量乘法扩展算法[J]. 计算机工程, 2011, 37(4):163-164.
- [7] Purohit G N, Rawat S A, Kumar M. Elliptic curve point multiplication using MBNR and point halving [J]. International Journal of Advanced Networking and Applications, 2012, 3(5):1329-1337.
- [8] Doche C, Imbert L. Extended double-base number system with applications to elliptic curve cryptography[C]//Proceedings of the 7th international conference on cryptology. Berlin: Springer-Verlag, 2006:335-348.
- [9] 蒲 冰, 牛荣健. 扩展的 DBNS 椭圆曲线标量乘算法[J]. 计算机工程与应用, 2011, 47(26):98-102.
- [10] Knudsen E W. Elliptic scalar multiplication using point halving [C]//Proc of ASIACRYPT' 99. [s. l.]: Springer-Verlag, 1999.
- [11] 郝艳华, 李 磊, 王育民. 利用多基链计算椭圆曲线标量乘的高效算法[J]. 电子科技大学学报, 2008, 37(6):868-871.
- [12] 陈 辉, 鲍皖苏. 基于半点运算与多基表示的椭圆曲线标量乘法[J]. 计算机工程, 2008, 34(15):153-155.
- [13] Liu D G, Ning P. Establishing pairwise keys in distributed sensor networks[C]//Proceedings of the 10th ACM conference on computer and communication security. New York: ACM Press, 2003:52-61.
- [14] 殷新春, 赵 荣, 侯红祥, 等. 基于折半运算的快速双基数标量乘算法[J]. 计算机应用, 2009, 29(5):1285-1288.
- [15] 赖忠喜, 张占军, 陶东娅. 椭圆曲线中直接计算 7P 的方法及其应用[J]. 计算机应用, 2013, 33(7):1870-1874.

(上接第 94 页)

- [5] Ding Liya. Design and development of knowwares system [C]//Proc of the 2nd international conference on innovative computing, information and control. Kumamoto, Japan: [s. n.], 2007:152-158.
- [6] Ding Liya, Lo Sio-Long. Inference in knowware system[C]//Proc of international conference on machine learning and cybernetics. Baoding: IEEE, 2009.
- [7] Ding Liya. A model of hierarchical knowledge representation toward knowware for intelligent systems[J]. Journal of Advanced Computational Intelligence and Intelligent Informatics, 2007, 11(10):1232-1237.
- [8] 廖瑞华. 基于 CORBA 的智能信息家电的可插拔的模型研究[D]. 长沙: 湖南师范大学, 2004.

- [9] 阳俐君. 信息家电接口描述语言及其编译器的研究与设计[D]. 长沙: 湖南师范大学, 2007.
- [10] 黄慧华. 基于信息家电接口定义语言的远程监控系统的设计与实现[D]. 长沙: 湖南师范大学, 2005.
- [11] 王鹏杰. CORBA 核心服务的研究与实现[D]. 长春: 吉林大学, 2003.
- [12] 朱其亮, 郑 斌. CORBA 原理及应用[M]. 北京: 北京邮电大学出版社, 2001.
- [13] 潘慧芳, 周兴社, 於志文. CORBA 构件模型综述[J]. 计算机应用研究, 2005, 22(5):14-15.
- [14] 周丽娟, 姚丽娜. Java RMI 技术的研究与应用[J]. 株洲工学院学报, 2006, 20(2):42-44.
- [15] 熊志斌. 基于 CORBA 的智能小区网络模型的研究与实现[D]. 长沙: 湖南师范大学, 2005.

一种高效的多基标量乘扩展算法

作者：[罗琴灵](#)，[蒋朝惠](#)，[LUO Qin-ling](#)，[JIANG Chao-hui](#)
作者单位：[贵州大学 计算机科学与技术学院, 贵州 贵阳, 550025](#)
刊名：[计算机技术与发展](#)
英文刊名：[Computer Technology and Development](#)
年，卷(期)：2015(5)

引用本文格式：[罗琴灵](#).[蒋朝惠](#).[LUO Qin-ling](#).[JIANG Chao-hui](#) [一种高效的多基标量乘扩展算法](#)[期刊论文]-[计算机技术与发展](#) 2015(5)