素数域 $GF(P)$ 上椭圆曲线快速标量乘算法的研究

赖忠喜,林君焕,张占军
LAI Zhongxi, LIN Junhuan, ZHANG Zhanjun

台州职业技术学院 机电工程学院,浙江 台州 318000
College of Mechanical and Electrical Engineering, Taizhou Vocational Technical, Taizhou, Zhejiang 318000, China

LAI Zhongxi, LIN Junhuan, ZHANG Zhanjun. Study on fast method of scalar multiplication on elliptic curves over Prime field $GF(P)$. Computer Engineering and Applications, 2015, 51(4):100-104.

Abstract: Based on the idea of trading inversions for multiplications, an efficient algorithm is proposed to compute $7P$ directly over prime field F_P in terms of affine coordinates, its computational complexity is I+23M+10S, saving one inversion compared with traditional method. Moreover, a new method is given to compute 7^kP directly, which is more efficient than k repeated $7P$. Finally, apply these new algorithms to scalar multiplication combined with MBNS. The experimental results show that on the elliptic curves recommended by NIST, the efficiency of new algorithm is superior to algorithm given by Xu kai-ping and other traditional algorithms, such as ternary-binary, 3-NAF, Dimitro algorithms, and the ration I/M of break-even point can be reduced to 2.4.

Key words: elliptic curve cryptosystem; scalar multiplication; Multi Base Number System(MBNS); field operation; affine coordinate

摘 要: 基于求逆转换为乘法的思想,利用仿射坐标提出了直接计算椭圆曲线上 $7P$ 的算法,该算法运算量为 I+23M+10S,比现有的算法节省了一次求逆运算,同时也给出了直接计算 7^kP 的快速算法,该算法比重复计算 k 次 $7P$ 更有效。结合多基数系统将这些新算法应用到标量乘法中,实验结果表明,在NIST推荐的椭圆曲线上,新算法的效率优于徐凯平等人所提的算法及传统的ternary-binary、3-NAF、Dimitro算法,相交处I/M可降至2.4。

关键词: 椭圆曲线密码体制;标量乘法;多基数系统;底层域运算;仿射坐标
文献标志码: A **中图分类号:** TP309.7 doi:10.3778/j.issn.1002-8331.1303-0370

1 引言

自Koblitz和Miller在1985年分别提出椭圆曲线密码体制(Elliptic Curve Cryptography,ECC)以来,由于其安全性高,实现性能优等独特的优势被广泛地应用于信息安全领域,并逐步成为国内外学者研究的重点。实现椭圆曲线密码体制最耗时的运算是椭圆曲线标量乘法,即 kP 的计算,其运算速度从整体上决定了ECC的实现效率[1-3]。研究标量乘法通常可从两个方面来考虑,一方面是研究标量 k 的有效表示,尽量减少上层运算,如 k 的三元表示、NAF及w-NAF等表示形式,Dimitrov[4]等人提出将双基数系统[5]应用到椭圆曲线标量乘中,取得了显著的效果。Mishra[6]等人改进了双基的思想,将其扩展到多基,在素数域上提出了以2,3,和5为底的多基链来计算标量乘的快速算法,取得了更好的效果。另一方面是对底层域快速算法进行研究,以减少底层域运算量。在这一方面,Sakai[7]等人利用求逆转化为乘法的思想推导出了 F_P 上计算 2^kP 的公式,极大提高了效率。Ciet[8]等人利用分母的最小公倍数思想,对 $2P+Q$、$3P$、$3P+Q$、$4P$、$4P+Q$ 等底层域运算进行优化。刘连浩[9]等人对 $3P+Q$ 算法进行了改进,并同时给出了 F_P 上仿射坐标系下的 3^kP 递推公式,大量减少了求逆运算。Mishra[6]等人利用除法多项式提出了计算 $5P$ 的快速算法。之后徐凯平[10]等人给出了在仿射坐标系下直接计算 5^kP 的快速算法,进一步提高了效率。邓维勇[11]又进一步改进了计算 3^kP 的算法。此外,周梦[12]等人也对 F_P 上计算 2^kP 和 3^kP 的算法进行了一些改进。所有的这

作者简介: 赖忠喜(1984—),男,讲师,研究领域为加密技术,智能控制;林君焕(1982—),男,讲师,研究领域为加密技术,智能控制;张占军(1979—),男,讲师,研究领域为加密技术,智能控制。E-mail:laizhongxi@163.com

收稿日期: 2013-03-24 **修回日期:** 2013-06-13 **文章编号:** 1002-8331(2015)04-0100-05
CNKI **网络优先出版:** 2013-07-03, http://www.cnki.net/kcms/detail/11.2127.TP.20130703.1144.019.html

些算法减少了底层域的运算量，加快了椭圆曲线标量乘的运算速度。

本文延续将求逆转化为乘法运算的思想，提出了在素数域 F_P 上用仿射坐标直接计算 $7P$ 的算法，其运算量为I+23M+10S，比现有的算法节省了一次求逆运算，其中I、S、M分别表示求逆、平方、乘法运算。同时本文在文献[5]的基础上给出了利用除法多项式直接计算 7^kP 的快速算法，其运算量为I+(23k+1)M+(12k-1)S，与重复计算 k 次 $7P$ 的运算量 k(I+23M+10S)相比，该方法节省了 $k-1$ 次求逆运算，相交处（运算量相等时）I/M = $(1.6k+0.2)/(k-1)$。最后结合多基链将这些算法应用到计算椭圆曲线标量乘的算法中。

2　背景知识

在素数域 F_P 上设表示域 $K=F_P$，特征值 $P>3$，则 K 上的Weierstrass方程可简化为[2]：

$$y^2=x^3+ax^2+b;(a,b\in K且\Delta=4a^3+27b^3 \bmod p\neq 0)$$

$E(K)$ 表示定义在域 K 上的椭圆曲线 E 的所有点的集合，它是一个Abel群。椭圆曲线 E 的群运算是按照椭圆曲线群运算法则完成的，其中所涉及的运算有加、减、乘、求逆和平方五种基本运算[10]。分别用I、S、M表示域 F_P 上求逆，平方和乘法运算，用I/M表示求逆和乘法运算的复杂度比。五种基本运算中，加法和减法相对于其他运算来说，所用时间可忽略不计[9]。求逆运算最耗时，在素数域 F_P 上，一般认为I/M > 30，且I/M随着 P 的增大而增大；而对于平方和乘法运算，可设定S=0.8M[6]。

设 $P=(x_1,y_1)$ 和 $Q=(x_2,y_2)$ 椭圆曲线 $E(F_P)$ 上的任意两个非零点，且满足 $P\neq\pm Q$，则在仿射坐标下，点加运算 $P+Q=(x_3,y_3)$ 可由式(1)计算：

$$\lambda=(y_2-y_1)/(x_2-x_1)$$
$$x_3=\lambda^2-x_1-x_2,\ y_3=\lambda(x_1-x_3)-y_1 \tag{1}$$

当 $P=Q$，且 $P\neq O$（O 表示曲线E的无穷远点）时，则在仿射坐标下，倍点运算 $2P=(x_3,y_3)$ 可由式(2)计算：

$$\lambda=(3x_1^2+a)/(2y_1)$$
$$x_3=\lambda^2-2x_1,\ \ y_3=\lambda(x_1-x_3)-y_1 \tag{2}$$

由式(1)和式(2)可知，素数域 F_P 上完成点加运算和倍点运算的运算量分别为I+2M+S和I+2M+2S。

3　直接计算 $7P$ 的算法

利用将求逆转化为适量乘法的思想，在文献[6]的基础上提出一种在仿射坐标系下利用除法多项式来计算 $7P$ 的算法。

对于素数域 F_P 上的椭圆曲线 E 有如下除法多项式：

$$\psi_1=1$$
$$\psi_2=2y$$
$$\psi_3=3x^4+6ax2+12bx-a^2$$
$$\psi_4=4y(x^6+5ax^4+20bx^3-5a^2x^2-4abx-8b^2-a^3) \tag{3}$$

更高次项的除法多项式可以使用下面的递推关系来求得：

$$\psi_{2n+1}=\psi_{n+2}\psi_n^3-\psi_{n-1}\psi_{n+1}^3$$
$$2y\psi_{2n}=\psi_n(\psi_{n+2}\psi_{n-1}^2-\psi_{n-2}\psi_{n+1}^2) \tag{4}$$

而对于任意在椭圆曲线 E 上的点 $P(x,y)$，它的 n 倍点的计算公式[6]如下：

$$[n]P=(x-\frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2},\frac{\psi_{n+2}\psi_{n-1}^2-\psi_{n-2}\psi_{n+1}^2}{4y\psi_n^3}) \tag{5}$$

令 $A=8y^4$；　$B=3x^2+a$；　$C=12xy^2-B^2$；$D=BC-A$；

$E=4yD$；$F=4AD-C^3$；$G=F-4D^2$；$H=2yGC$；

$M=FC^3-16AD^3$；$N=D(C^3G-F^2)$

利用式(6)和(7)可以得到以下等式：

$$\psi_1=1\quad \psi_2=2y\quad \psi_3=12xy^2-B^2=C\quad \psi_4=4yD=E$$
$$\psi_5=\psi_4\psi_2^3-\psi_3^3=4AD-C^3=F$$
$$\psi_6=(\psi_5\psi_3\psi_2^2-\psi_3\psi_4^2)/\psi_2=2yGC=H$$
$$\psi_7=\psi_5\psi_3^3-\psi_2\psi_4^3=FC^3-16AD^3=M$$
$$\psi_8=(\psi_6\psi_4\psi_3^2+\psi_2\psi_4\psi_5^2)/\psi_2=D(C^3G-F^2)=N$$

如果 $T=7P=(x_7,y_7)$，那么由式(5)可推导出：

$$x_7=x-\frac{\psi_8\psi_6}{\psi_7^2}=x-\frac{NH}{M^2}$$

$$y_7=\frac{\psi_9\psi_6^2-\psi_5\psi_8^2}{4y\psi_7^3}=$$

$$\frac{C^3G(2y^2G^2E^3-DNF)+F^3(DN-C^3yG^2)}{M^3}$$

具体的算法如下所示，算法的运算量见表1。

表1　算法1的运算量

步骤	运算量	已知项
A	2S	—
B	S	—
C	M+S	—
D	M	—
E	M	—
F	2M+S	—
G	S	—
H	2M	—
M	2M	C^3, AD, D^2
N	2M+S	—
x_7	I+2M+S	—
y_7	10M+2S	$1/M, 1/M^2, yG, F^2, C^3G$
总运算量	I+23M+10S	

算法1　利用除法多项式计算 $7P$ 的算法

input：$P=(x,y)\neq O$

output：$T=7P=(x_7,y_7)$

$A=8y^4$;

$B=3x^2+a$;

$C=12xy^2-B^2$;

$D=BC-A$;

$E=4yD$;

$F=4AD-C^3$;

$G=F-4D^2$;

$H=2yGC$;

$M=FC^3-16AD^3$;

$N=D(C^3G-F^2)$;

$x_7=x-\frac{HN}{M^2}$;

$y_7=\frac{C^3G(2y^2G^2E^3-DNF)+F^3(DN-C^3yG^2)}{M^3}$;

$return(x_7,y_7)$

经过分析,算法1的总运算量为I+23M+10S。$7P$还可以通过$(2P+5P)$、$(3P+4P)$、$(4P+3P)$和$(3(2P)+P)$等表示形式来进行计算。当用已有的算法来计算上述形式时,运算量分别为:(2I+24M+10S)(2I+25M+12S)、(3I+18M+8S)和(2I+18M+5S)。显然当$I/M\geqslant 9$时,算法1的效率最高。

4　直接计算7^kP的算法

如果将标量表示成7^k的形式,那么直接计算7^kP会大大提高计算效率。本章延续将求逆转化为乘法的思想,给出了在仿射坐标系下直接计算7^kP的快速算法,如算法2所示,具体运算量见表2。

表2　算法2的运算量

步骤	运算量	已知项
A_i	$2k$S	—
B_i	$(k-1)$M+$(3k-2)$S	—
C_i	kM+kS	H_i^2
D_i	kM	—
E_i	kM	—
F_i	$2k$M+kS	—
M_i	kS	—
N_i	$2k$M	—
R_i	$2k$M	C_i^3, A_iD_i, D_i^2
S_i	$2k$M+kS	—
T_i	$(k-1)$M	—
X_i	$2k$M+kS	—
Y_i	$8k$M+$2k$S	$C_i^3M_i, H_iM_i, F_i^2$
x_{7^k}	I+M+S	—
y_{7^k}	2M	$1/T_k, 1/T_k^2$
总运算量	I+$(23k+1)$M+$(12k-1)$S	

算法2　利用除法多项式计算7^kP的算法

input: $P=(x,y)\neq O$

output: $T=7^kP=(x_{7^k},\ y_{7^k})$

令$X_0=x$, $Y_0=y$, $T_0=1$;

For $i=1$ to k do

$G_i=X_{i-1}$, $H_i=Y_{i-1}$;

$A_i=8H_i^4$;

$B_i=3G_i^2+aT_{i-1}^4$;

$C_i=12G_iH_i^2-B_i^2$;

$D_i=B_iC_i-A_i$;

$E_i=4H_iD_i$;

$F_i=4A_iD_i-C_i^3$;

$M_i=F_i-4D_i^2$;

$N_i=2H_iM_iC_i$;

$R_i=F_iC_i^3-16A_iD_i^3$;

$S_i=E_i(C_i^3M_i-F_i^2)$;

$T_i=R_iT_{i-1}$;

$X_i=G_iR_i^2-N_iS_i$;

$Y_i=C_i^3M_i(2H_i^2M_i^2E_i^3-S_iD_iF_i)+F_i^3(S_iD_i-C_i^3H_iM_i^2)$;

$i=i+1$;

End for

$x_{7^k}=\frac{X_k}{T_k^2}, Y_{7^k}=\frac{Y_k}{T_k^3}$;

$return(x_{7^k},Y_{7^k})$

经过分析,算法2总的运算量为$\mathrm{I}+(23k+1)\mathrm{M}+(12k-1)\mathrm{S}$。显然,当计算$7P(k=1)$时,算法2的运算量为I+24M+11S,而算法1的运算量为I+23M+10S,算法2效率略低于算法1。但当计算$49P(k=2)$时,算法2的运算量为I+47M+23S,而算法1的运算量为2(I+23M+10S),当$I/M\geqslant 3.4$时,算法2效率高于算法1。若计算7^kP,算法2只需一次求逆运算,与用算法1重复k次计算7P的运算量$k(\mathrm{I}+23\mathrm{M}+10\mathrm{S})$相比,节省了$k-1$次求逆运算,相交处$\mathrm{I/M}=(1.6k+0.2)/(k-1)$。显然,随着$k$的增大,I/M在逐渐减小,算法2的计算效率也不断的提高,当k足够大时,算法2与算法1的I/M值可降到1.6。表3列出了素数域上在仿射坐标系下不同运算的开销。

表3　素数域中不同运算的开销(仿射坐标系)

运算	运算开销	运算	运算开销
$P\pm Q$	I+2M+S	$3P\pm Q$[5]	I+16M+3S
$2P$	I+2M+2S	$4P$[5]	I+9M+9S
2^kP	$\mathrm{I}+(4k+1)\mathrm{M}+(4k+1)\mathrm{S}$	$4P\pm Q$	2I+11M+4S
$2P\pm Q$	I+9M+2S	$5P$	I+15M+8S
$3P$	I+7M+4S	$7P$	I+23M+10S
3^kP[4]	$\mathrm{I}+(9k+2)\mathrm{M}+(5k+1)\mathrm{S}$	7^kP	$\mathrm{I}+(23k+1)\mathrm{M}+(12k-1)\mathrm{S}$

5　一种新的多基标量乘算法

上两章提出了在素数域仿射坐标系下直接计算$7P$和7^kP的算法,本章将这些算法应用到以2,5和7为基

的多基链来计算椭圆曲线标量乘法。

2007年，Mirshra和Dimitrov[6]提出将任意整数 k 表示成多基链的形式来计算椭圆曲线标量乘的算法，其表达形式为：$k=\sum_{i=1}^{m}s_i2^{b_i}3^{t_i}5^{h_i}$，本文在此基础上提出将 k 表示成 $\sum_{i=1}^{m}s_i2^{b_i}3^{t_i}7^{h_i}$ 其中 m 为多基链的长度，其中 $s_i\in\{1,-1\}$，$\{b_i\}$、$\{t_i\}$、$\{h_i\}$ 为3个单调递减序列。生成该表达形式的算法具体见文献[6]，下面给出基于该表达形式的多基链标量乘算法。

算法3 以2、3、7为基的标量乘算法

输入：整数 $k=\sum_{i=1}^{m}S_i2^{b_i}3^{t_i}7^{h_i}$，$s_i\in\{-1,1\}$；$b_1\geqslant b_2\geqslant\cdots\geqslant b_m\geqslant 0$；$t_1\geqslant t_2\geqslant\cdots\geqslant t_m\geqslant 0$；$h_1\geqslant h_2\geqslant\cdots\geqslant h_m\geqslant 0$；点 $P\in E(F_p)$

输出：曲线E上的点 $[k]P\in E(F_p)$

1）$Z=s_1P$；
2）for $i=1,2,\cdots,m-1$；do
3）　$u=b_i-b_{i+1}$；
4）　$v=t_i-t_{i+1}$；
5）　$w=h_i-h_{i+1}$；
6）　if $w=1$ then
7）　$Z=7Z$；//SP运算
8）　else
9）　$Z=7^wZ$；// k-SP运算
10）　if $u=0$ then
11）　　if $v=0$ then
12）　　$Z=Z+s_{i+1}P$；
13）　　else if $v=1$ then
14）　　$Z=3Z+s_{i+1}P$；
15）　　else if $v=2$ then
16）　　$Z=3(3Z)+s_{i+1}P$；//TA运算
17）　　else
18）　　$Z=3^vZ+s_{i+1}P$；//k-T运算
19）　else
20）　　if $v=1$ then
21）　　$Z=3Z$；
22）　　else
23）　　$Z=3^vZ$；//k-T运算
24）　　if $u=1$ then
25）　　$Z=2Z+s_{i+1}P$；//DA运算
26）　　else if $u=2$ then
27）　　$Z=2(2Z)+s_{i+1}P$；
28）　　else
29）　　$Z=2^uZ+s_{i+1}P$；//k-D运算
30）　return Z

在上述的算法中，将运算 $P\pm Q$、$2P$、$2P\pm Q$、2^kP、$3P$、$3P\pm Q$、3^kP、$7P$、7^kP 分别记为A、D、DA、k-D、T、TA、k-T、SP、k-SP，这些运算都可以通过计算公式快速计算得到，具体运算量见表3。

本算法的复杂度分析如下：上述算法共迭代 $m-1$ 次，将第 i 轮所需的运算量记为 W_i，则有

$$\begin{aligned}W_i=&[\delta_{w_i,1}SP+(1-\delta_{w_i,1})w_i-SP]+\\&[\delta_{u_i,0}(\delta_{v_i,0}A+\delta_{v_i,1}TA+\delta_{v_i,2}(TA+T)+\\&(1-\delta_{v_i,0}-\delta_{v_i,1}-\delta_{v_i,2})(v_i-T+A))]+\\&[(1-\delta_{u_i,0})(\delta_{v_i,1}T+(1-\delta_{v_i,1})v_i-T+\delta_{u_i,1}DA+\\&\delta_{u_i,2}(D+DA)]+(1-\delta_{u_i,1}-\delta_{u_i,2})(u_i-D+A)\end{aligned}$$

其中 $i=j$ 时 $\delta_{i,j}=1$，$i\neq j$ 时 $\delta_{i,j}=0$。因此该算法总的运算量为 $W=\sum_{i=1}^{m-1}W_i$。

6　效率分析

用VC++6.0软件和MIRACL大数运算库实现了上述算法。在美国国家技术标准研究所NIST推荐的椭圆曲线上分别随机选取1 000组大整数标量 k，用算法3进行标量乘法运算，计算它们所需底层运算量的平均值，并将该算法与ternary-binary、3-NAF、Dimitrov算法和文献[10]中徐凯平等人提出的多基链算法的运算量进行比较。表4为在NIST P-160、NIST P-192、NIST P-224和NIST P-256曲线上当 k 分别为160 bit、192 bit、224 bit和256 bit时本文算法3与上述四种算法的运算量比较，其中设定S=0.8M。

从表4不难看出这五种算法中求逆运算最少的是本文算法，而最多则是ternary-binary方法。为了更详细地比较它们各自的性能，表5给出了本文算法与其他方法相交处的I/M值。

表4　不同方法不同长度的平均运算量比较

算法	NIST P-160 k=160 bit	NIST P-192 k=192 bit	NIST P-224 k=224 bit	NIST P-256 k=256 bit
ternary-binar算法	127I+1 074M	153I+1 296M	179I+1 505M	204I+1 725M
Dimitrov算法	117I+1 185M	133I+1 443M	153I+1 693M	178I+1 926M
3-NAF算法	101I+1 362M	122I+1 645M	142I+1 915M	162I+2 184M
文献[10]算法	80I+1 391M	95I+1 675M	111I+1 954M	127I+2 223M
本文算法	75I+1 431M	89I+1 724M	104I+2 012M	119I+2 291M

表5 本文算法与其他方法I/M值的比较

I/M	ternary-binary算法	Dimitrov算法	3-NAF算法	文献[10]算法
160 bit	6.9	5.9	2.7	8
192 bit	6.7	6.4	2.4	8.2
224 bit	6.8	6.5	2.6	8.3
256 bit	6.7	6.2	2.5	8.5

从表5可知,192 bit时本文算法与3-NAF算法的相交处I/M值最低,达到了2.4。同时还可以明显看出,各列的I/M值变化不大,即本文算法与ternary-binary、Dimitrov算法、3-NAF和文献[10]中算法相交处的I/M值并不随着k长度的变化而变化,当标量长度k为160 bit及I/M=30时,本文算法比ternary-binary算法提高了24.6%,比Dimitrov算法提高了21.6%,比3-NAF算法提高了16.2%,比文献[10]算法提高了2.9%,当I/M=10时,本文算法比3-NAF算法提高了8.1%,比Dimitrov算法提高了7.4%,比ternary-binary算法提高了7.0%,比文献[10]算法提高了0.5%。同时随着标量k长度的增加提高量的变化也不明显。

7 结束语

本文延续将求逆转化为乘法的思想,利用除法多项式在仿射坐标系中直接推导出直接计算$7P$和7^kP的快速算法,再结合直接计算$2P\pm Q$、$3P\pm Q$、2^kP和3^kP的快速算法,将这些底层域快速运算与多基数系统融合,给出了新的以2,3,7为基的多基数标量乘算法,实验结果表明,新算法的效率比ternary-binary、Dimitrov算法、3-NAF和文献[10]中的标量乘算法的效率都要高,相交处I/M甚至可降至2.4。此外新算法不需要任何预计算和预存储空间,不仅提高了椭圆曲线密码体制实现的运算速度,也节约了存储空间,适用于计算能力、存储资源都十分有限的单片机,更适用于设计高速的椭圆曲线密码的专用芯片。下一步工作考虑将新算法扩展应用到超椭圆曲线上。

参考文献:

[1] 赖忠喜,陶东娅.一种基于半点运算与双基表示的双标量乘算法[J].计算机应用与软件,2012,29(9):293-295.

[2] Hankerso D,Menezes A,Vanstone S.Guide to elliptic curve cryptography[M].New York:Springer-Verlag,2004:76-81.

[3] 殷新春,侯洪祥,谢立.基于双基数的快速标量乘算法[J].计算机科学,2008,35(6):186-195.

[4] Dimitrov V S,Imbert L,Mishra P K.Fast elliptic curve point multiplication using double-base chains[EB/OL].[2007-04-10].http//eprint.iacr.org/2005/069.

[5] Dimitrov V S,Jullien G A.A new number representation with applications[J].IEEE Circuits and Systems Magazine,2003(2):6-23.

[6] Mishra P K,Dimitrov V.Efficient quintuple formulas for elliptic curves and efficient scalar multiplication using multi-base number representation[C]//Proceedings of the 10th Information Security Conference.Berlin:Springer-Verlag,2007:390-406.

[7] Sakuraik S.Efficient scalar multiplications on elliptic curves with direct computations of several doublings[J].IEICE Transactions on Fundamentals,2001,E842A(1):120-129.

[8] Ciet M,Joye M,Lauter K,et al.Trading inversions for multiplications in elliptic curve cryptography[J].Designs Codes and Cryptography,2006,39(2):189-206.

[9] 刘连浩,申勇.椭圆曲线密码体制中标量乘法的快速算法[J].计算机应用研究,2009,26(3):1104-1107.

[10] 徐凯平,郑洪源,刘锦峰,等.椭圆曲线密码体制中快速标量乘方法研究[J].计算机工程与应用,2011,47(15):112-115.

[11] 邓维勇.椭圆曲线密码体制中标量乘法研究[D].昆明:昆明理工大学,2012.

[12] 周梦,周海波.椭圆曲线快速点乘算法优化[J].计算机应用研究,2012,29(8):3056-3058.

(上接16页)

[11] 杨晓梅,曾建潮.基于主动调度的编码方法及其在JSP中的应用[J].系统工程理论与实践,2004(6):55-60.

[12] 张超勇,饶运清,李培根,等.柔性作业车间调度问题的两级遗传算法[J].机械工程学报,2007,43(4):119-124.

[13] 刘琼,张超勇,饶运清,等.改进遗传算法解决柔性作业车间调度问题[J].工业工程与管理,2009,14(2):59-66.

[14] Deb K,Pratap A,Agarwal S,et al.A fast and elitist multi-objective genetic algorithm:NSGA-II[J].IEEE Trans on Evolutionary Computation,2002,6(2):184-197.

[15] 刘文程,高家全.解并行机模糊调度问题的自适应遗传算法[J].计算机工程与应用,2013,49(7):60-63.

[16] 胡喜玲,李洪波,胡俊.基于自适应混沌遗传算法的路径规划[J].计算机工程与应用,2013,49(9):68-73.

[17] 曹道友,程家兴.基于改进的选择算子和交叉算子的遗传算法[J].计算机技术与发展,2010,20(2):44-51.

[18] 张义长,杨加明,鲁宇明.结合保优策略和移民策略的自适应遗传算法[J].计算机工程与应用,2010,46(31):36-38.

[19] 王万良,周明,徐新黎,等.基于改进粒子群算法的离子膜车间调度问题研究[J].控制与决策,2010,25(7):1021-1025.