基于预计算和周期性的 ECC 标量乘法算法

张晓强 朱贵良 王卫苹 王蒙蒙

(北京航空航天大学 软件开发环境国家重点实验室, 北京 100191) (华北水利水电学院 信息工程学院, 郑州 450011)

摘 要: 在研究二进制、带符号的二进制(NAF, Non-Adjacent Form)等常见标量乘法算法的基础上,结合椭圆曲线基点的周期特性和预计算倍点序列方式,提出了一种新的标量乘法算法,并给出了新算法的详细步骤. 点的周期性和系数决定了直接进行标量乘法运算还是转化为求其逆元,预计算倍点序列方式避免了椭圆曲线密码体制(ECC, Elliptic Curve Cryptosystem)加解密过程中大量的重复运算. 为验证算法的正确性,采用密钥长度为 192 bit 椭圆曲线,给出了一个具体实例. 实例结果和算法分析表明:与二进制和 NAF 算法相比,新算法虽占用了一些存储空间,但省去了倍点运算的时间开销,同时减少了点加的运算次数,极大地提高了标量乘法运算的效率. 该算法的提出对完善 ECC 理论和加快 ECC 在实际中的应用具有重要意义.

关 键 词: 椭圆曲线密码体制; 二进制算法; 带符号的二进制算法; 标量乘法; 预计算; 周期性

中图分类号: TN 918.4

文献标识码: A **文 章 编 号**: 1001-5965(2011)11-1451-05

Scalar multiplication algorithm of ECC based on precomputation and periodicity

Zhang Xiaoqiang

(State Key Lab of Software Development Environment, Beijing University of Aeronautics and Astronautics, Beijing 100191, China)

Zhu Guiliang Wang Weiping Wang Mengmeng

(Department of Information Engineering, North China University of Water Conservancy and Electric Power, Zhengzhou 450011, China)

Abstract: Based on the binary method, non-adjacent form (NAF) method, etc., a new scalar multiplication algorithm was proposed, which uses the periodicity of based point and the precomputation mean. Meanwhile, the steps of new algorithm were given. The periodicity of based point and the coefficient of scalar multiplication determine performing the operation of scalar multiplication directly or computing its inverse element. The precomputation mean can void a quantity of repeat computation during the encryption and decryption processes of elliptic curve cryptosystem (ECC). To verify the correctness of new algorithm, a concrete experiment was offered with an elliptic curve, whose key length is 192 bit. The experimental results and algorithm analyses show that comparing with binary and NAF methods, although the new algorithm requires a little extra space to store precomputed points, it does not need the operation of point doublings and reduces the operation times of point addition. Therefore, the new algorithm can improve the efficiency of scalar multiplication sharply. The research achievement is significant for completing the theory of ECC and accelerating its application in practice.

Key words: elliptic curve cryptosystem(ECC); binary method; non-adjacent form(NAF) method; scalar multiplication; precomputation; periodicity

收稿日期: 2010-07-02; **网络出版时间**: 2011-11-14 17:20; **DOI**: CNKI:11-2625/V.20111114.1720.016

网络出版地址: www.cnki.net/kcms/detail/11.2625.V.20111114.1720.016.html

作者简介: 张晓强(1983 -),男,河南内黄人,博士生,grayqiang@163.com.

目前,网络信息的安全问题倍受关注. 密码学是信息安全的核心基础[1]. 密码体制分为对称和非对称密码体制. 椭圆曲线密码体制(ECC,Elliptic Curve Cryptosystem)具有安全性高、计算量小和密钥短等优势,是目前有着广泛应用前景的非对称密码体制. 近年,人们对 ECC 研究的兴趣不断提升[2],理论逐渐成熟和加密产品不断涌现. 人们普遍认为,它将取代公钥密码体制 RSA,成为通用的密码体制[3].

但 ECC 仍存在一些问题有待解决或进一步优化,如安全椭圆曲线的选取、基点的选取、快速算法、明文嵌入等. 标量乘法是 ECC 的核心运算,也是最耗时的运算,其运算效率直接决定着 ECC 的性能[4]. 文献[3]描述了计算标量乘法的二进制、带符号的二进制(NAF,Non-Adjacent Form)和滑动窗口等算法. 二进制算法将系数用二进制表示,再进行倍点和点加的运算,是计算标量乘法的经典算法. NAF 算法减少了二进制编码中非"0"元个数,在一定程度上提高了运算效率. 滑动窗口算法实质也是二进制算法的改进,其运算效率明显优于二进制算法[5]. 文献[6]对滑动窗口算法又做了改进,提出了一种自适应的滑动窗口标量乘法算法. 但同时指出,当系数的二进制表示中"1"和"0"相间隔出现时,如"101010",该算法的执行效率退化为二进制算法. 另外,文献[7]定义了一种系数补元,设计了一种基于系统补元的标量乘法算法;文献[8]提出了一种基于系数分割和命题逻辑理论的标量乘法算法;文献[4]设计了一种具有弹性的滑动窗口标量乘法算法.

上述算法在一定程度上提高了标量乘法运算的效率,但因算法复杂或难以实现,未能令人满意. 为提高 ECC 的性能,本文在研究常见标量乘法算法的基础上,提出了一种新的标量乘法算法.

1 ECC

文献[9-10]根据椭圆曲线点群上离散对数问题的难解性,提出了 ECC. 常用的椭圆曲线为基于有限域 $F_p=\{0,1,2,\cdots,p-1\}$ 上的同余方程:$y^2=x^3+ax+b(\mathrm{mod}\,p)$. 其中,$p>3$ 且为素数,$a,b\in F_p$ 且满足 $4a^3+27b^2\neq 0(\mathrm{mod}\,p)$. 方程的所有解$(x,y)\in F_p\times F_p$,连同无穷远点 O,共同构成 F_p 上椭圆曲线的点群,记作:$E_p(a,b)$[11].

ECC 的主要运算包括点的加法和标量乘法运算,其运算法则如下:

1) 点的加法运算法则[11]:令椭圆曲线为 $E_p(a,b)$, $\forall P(x_1,y_1),Q(x_2,y_2)\in E_p(a,b)$,定义:$P+Q=R(x_3,y_3)$. 其中,$x_3=(\lambda^2-x_1-x_2)\,\mathrm{mod}\,p$,$y_3=[\lambda(x_1-x_3)-y_1]\,\mathrm{mod}\,p$. 当 $P\neq Q$ 时,$\lambda=(y_2-y_1)/(x_2-x_1)$,此时点的加法又称点加运算;当 $P=Q$ 时,$\lambda=(3x_1^2+a)/2y_1$,此时点的加法又称倍点运算.

2) 标量乘法运算法则[11]:$\forall k\in\mathbf{Z}$,定义:$kP=P+P+\cdots+P$, 即 k 个 P 进行点的加法运算,此运算称为点的标量乘法运算.

2 常见标量乘法算法

2.1 二进制算法

二进制算法是目前模指数运算最简单、最快的方法[12],也是标量乘法最经典的算法. 该算法的思想源于中国宋朝的秦九韶算法[13].

设椭圆曲线为 $E_p(a,b)$,选取基点为 P,P 的周期为 T,$k\in\{1,2,\cdots,T-1\}$,采用二进制算法计算 kP 的步骤如下:

1) 二进制编码 $k=k_{l-1}k_{l-2}\cdots k_0$,$k_i\in\{0,1\}$;

2) 计算 $2^1P,2^2P,\cdots,2^{l-1}P$;

3) 利用上述步骤结果,计算 k_i2^iP,$i=0,1,2,\cdots,l-1$,若 $k_i=0$,则 $k_iP=0\times P=O$;若 $k_i=1$,则 $k_iP=1\times P=P$;

4) 将 k_i2^iP,$i=0,1,2,\cdots,l-1$ 的值相加,即 $k_02^0P+k_12^1P+\cdots+k_{l-1}2^{l-1}P=(k_02^0+k_12^1+\cdots+k_{l-1}2^{l-1})P=kP$.

2.2 NAF 算法

椭圆曲线 Abel 群上点的加法和点的减法的计算量相等[11]. NAF 编码的思想是将 k 的二进制编码中若干连续的"1"用一个"1"和一个"-1"表示,从而减小了二进制编码中非"0"元的个数,即减少了点加的运算次数. 任何非负整数均有唯一的 NAF 编码[3].

采用 NAF 算法计算 kP 的步骤如下:

1) 二进制编码 $k=k_{l-1}k_{l-2}\cdots k_0$,$k_i\in\{0,1\}$;

2) 对 $k_{l-1}k_{l-2}\cdots k_0$ 进行 NAF 编码,令对应 NAF 编码为 $k'_{l'-1}k'_{l'-2}\cdots k'_0$,$k'_i\in\{-1,0,1\}$;

3) 计算 $2^1P,2^2P,\cdots,2^{l'-1}P$;

4) 利用上述步骤结果,计算 k'_i2^iP,$i=0,1,2,\cdots,l'-1$. 若 $k'_i=-1$,则 $k'_iP=(-1)\times P=-P$, $-P$ 为 P 的逆元;若 $k'_i=0$,则 $k'_iP=0\times P=O$;若 $k'_i=1$,则 $k'_iP=1\times P=P$;

5) 将 k'_i2^iP,$i=0,1,2\cdots,l'-1$ 的值相加,即 $k'_02^0P+k'_12^1P+\cdots+k'_{l'-1}2^{l'-1}P=(k'_02^0+k'_12^1+\cdots+k'_{l'-1}2^{l'-1})P=kP$.

3　标量乘法新算法

基点的周期性:设 ECC 的基点为 P,则 P 构成有限循环群 $G_P=\{O,P,2P,\cdots,(T-1)P\}$. 其中,$O$ 为无穷远点,T 为 P 周期. 因为 $TP=(T+k-k)P=kP+(T-k)P=O$,所以 $(T-k)P$ 为 kP 的逆元. 计算 kP 可转化为求其逆元 $(T-k)P$. 因此,当 $k\leqslant T-k$ 时,计算 kP 的运算量要比 $O-(T-k)P$ 小;否则,计算 $O-(T-k)P$ 的运算量要比 kP 小.

预计算倍点序列:设 ECC 密钥长度为 L,在进行标量乘法运算前,先利用二进制算法计算出 $2^i\times P$, $i=0,1,2,\cdots,L$. 在 ECC 加解密过程中,基点 P 不变,这些点反复用到. 采用预计算方式,虽然占用一些额外的存储空间,但是避免了大量重复的运算,可有效提高运算效率.

结合点的周期性和预计算倍点序列,设计了一种新的标量乘法算法. 预计算并保存倍点序列 $2^iP,i=1,2,\cdots,L$,采用新算法计算 kP 步骤如下:

1) 利用基点的周期性,确定标量乘法的系数 k',当 $k\leqslant T-k$ 时,则取 $k'=k$;否则,取 $k'=T-k$;

2) 二进制编码 k' 为 $k'_{l'-1}k'_{l'-2}\cdots k'_0$,$k'_i\in\{0,1\}$;

3) NAF 编码 $k'_{l'-1}k'_{l'-2}\cdots k'_0$ 为 $k''_{l'-1}k''_{l'-2}\cdots k''_0$,$k''_i\in\{-1,0,1\}$;

4) 利用预计算的倍点序列,计算 $k''_i2^iP,i=0,1,2,\cdots,l''$;

5) 将 $k''_i2^iP,i=0,1,2,\cdots,l''$ 的值相加,即 $k''_02^0P+k''_12^1P+\cdots+k''_{l''}2^{l''}P=(k''_02^0+k''_12^1+\cdots+k''_{l''}2^{l''})P=k'P$;

6) 若 $k'=k$,则 $k'P$ 即为所求;若 $k'=T-k$,则计算 $O-k'P$.

4　验证实例

采用美国国家标准和技术研究所(NIST,National Institute of Standards and Technology)推荐的素数域上密钥长度为 $L=192$ bit 椭圆曲线 $E_p(a,b)$[3]. 其中,$a=-3$,$b=2\,455\,155\,546\,008\,943\,817\,740\,293\,915\,197\,451\,784\,769\,108\,058\,161\,191\,238\,065$,$p=2^{192}-2^{64}-1=6\,277\,101\,735\,386\,680\,763\,835\,789\,423\,207\,666\,416\,083\,908\,700\,390\,324\,961\,279$,基点 $P(x,y)$:$x=602\,046\,282\,375\,688\,656\,758\,213\,480\,587\,526\,111\,916\,698\,976\,636\,884\,684\,818$,$y=174\,050\,332\,293\,622\,031\,404\,857\,552\,280\,219\,410\,364\,023\,488\,927\,386\,650\,641$,基点周期 $T=6\,277\,101\,735\,386\,680\,763\,835\,789\,423\,176\,059\,013\,767\,194\,773\,182\,842\,284\,081$.

令 $k=5\,094\,331\,665\,845\,340\,624\,984\,330\,319\,989\,351\,445\,359\,870\,854\,569\,012\,267\,555$,预计算并保存倍点序列 $2^iP,i=1,2,\cdots,192$,采用新算法计算 kP 的详细步骤如下:

1) 因为 $k>T-k$,则 $k'=T-k=1\,182\,770\,069\,541\,340\,138\,851\,459\,103\,186\,707\,568\,407\,323\,918\,613\,830\,016\,526$;

2) 二进制编码 $k'=k'_{189}k'_{188}\cdots k'_0=110000001\,111001011001000011010000111100011010001100010100011100001010000000010001101001010101101010110001100011001100001110101011110111111100000111000110010100101111110111010110011110000001110;

3) NAF 编码 $k'_{189}k'_{188}\cdots k'_0=k''_{190}k''_{189}\cdots k''_0=10-1000001000-1010-10-100100010-010001000-10010-1010010-100010100100-1000010100000000010010-101010-10-10-100-10-10-10-10010-10010-1010-10001000-10-10-10000-1000000-10000100-10010-100101010-100000-1000-10-10-101000-10000100-10;

4) 利用预计算的倍点序列,计算 $k''_i2^iP,i=0,1,2,\cdots,190$;

5) 将 $k''_i2^iP,i=0,1,2,\cdots,190$ 的值相加,计算 $k'P=(k''_02^0+k''_12^1+\cdots+k''_{190}2^{190})P=(3\,763\,518\,280\,863\,428\,479\,641\,794\,418\,782\,953\,997\,696\,461\,124\,259\,885\,273\,065,1\,190\,001\,601\,194\,143\,115\,067\,702\,913\,662\,457\,557\,438\,406\,239\,778\,202\,785\,329)$;

6) 因为 $k'=T-k$,则计算 $kP=O-k'P=(3\,763\,518\,280\,863\,428\,479\,641\,794\,418\,782\,953\,997\,696\,461\,124\,259\,885\,273\,065,5\,087\,100\,134\,192\,537\,648\,768\,086\,509\,545\,208\,858\,645\,502\,460\,612\,122\,175\,950)$.

5　算法分析

5.1　算法复杂度对比分析

设一次点加运算耗时为 A,一次倍点运算的耗时为 D,二进制编码 $k=k_{l-1}k_{l-2}\cdots k_0$,NAF 编码 $k=k'_{l'-1}k'_{l'-2}\cdots k'_0$,采用二进制、NAF 和新算法计算 kP,算法复杂度对比分析如下:

1) 二进制算法. $kP=(k_02^0+k_12^1+\cdots+k_{l-1}2^{l-1})P=(2^{l-1}k_{l-1}+\cdots+2^1k_1+2^0k_0)P=2(\cdots2(2k_{l-1}P+k_{l-2}P)+\cdots+k_1P)+k_0P$. 因此,采用二进制算法计算 kP 共需 l 次倍点运算和 $k_0+k_1+\cdots+k_{l-1}$ 次点加运算,总时间复杂度为

$lD + A(k_0 + k_1 + \cdots + k_{l-1})$. 平均一个长度为 l 的二进制数含有 $l/2$ 个“0”[11]. 因此,二进制算法的平均时间复杂度为 $l(D + A/2)$.

2) NAF 算法. $kP = (k'_0 2^0 + k'_1 2^1 + \cdots + k'_{l'-1} 2^{l'-1})P = (2^{l'-1} k'_{l'-1} + \cdots + 2^1 k'_1 + 2^0 k'_0)P = 2(\cdots 2(2k'_{l-1}P + k'_{l-2}P) + \cdots + k'_1 P) + k'_0 P$. 因此,采用 NAF 算法计算 kP 共需要 l' 次倍点运算和 $|k'_0| + |k'_1| + \cdots + |k'_{l'-1}|$ 次点加运算,总时间复杂度为 $l'D + A(|k'_0| + |k'_1| + \cdots + |k'_{l'-1}|)$. NAF 编码具有最小的非零元个数,其长度至多比二进制表示多 1 bit[3],即 $l' = l$ 或 $l' = l + 1$. 平均一个 l 的二进制数对应的 NAF 编码中含有 $2l/3$ 个“0”[11]. 因此,NAF 算法的平均时间复杂度为 $l'(D + A/3) = l(D + A/3)$ 或 $(l + 1)(D + A/3)$.

3) 新算法. 因为 k' 取 k 和 $T - k$ 中较小者,则 $k' \leqslant k$ 且 $k' \leqslant T/2$. 令二进制编码 $k' = k'_{l'-1} k'_{l'-2} \cdots k'_0$, $l' \leqslant l$, NAF 编码 $k' = k''_{l''-1} k''_{l''-2} \cdots k''_0$. 计算 $k'P = (k''_0 2^0 + k''_1 2^1 + \cdots + k''_{l''-1} 2^{l''-1}) \times P = 2(\cdots 2(2k''_{l''-1}P + k''_{l''-2}P) + \cdots + k''_1 P) + k''_0 P$ 需要 $|k''_0| + |k''_1| + \cdots + |k''_{l''-1}|$ 次点加运算. 因为倍点 $2^i P, i = 1, 2, \cdots, L$ 已预先计算,所以省去了对其运算的时间开销. 因此,采用新算法计算 kP 的时间复杂度为 $A(|k''_0| + |k''_1| + \cdots + |k''_{l''-1}|)$,平均时间复杂度为 $Al'/3 \leqslant Al/3$.

针对验证实验中的椭圆曲线 $E_p(a, b)$、基点 P 和系数 k,分别采用二进制、NAF 和新算法计算 kP. 经计算得:k 的二进制码长 $l = 192$ bit,非“0”元个数为 104;对应 NAF 码长为 193 bit,非“0”元个数为 65;$k' = T - k$ 的 NAF 码长为 191 bit,非“0”元个数为 64. 实例中 ECC 密钥长度为 192 bit,采用新算法时,需要保存 192 个点. 因为椭圆曲线上的点 $(x, y) \in F_p \times F_p$,所以每个点需要占用 $192 \times 2 = 384$ bit. 因此,实例保存预计算的倍点序列共需要 $192 \times 2 \times 192 = 73728$ bit = 9 kB 的存储空间.

3 种算法的时间和空间复杂度对比见表 1.

表 1 算法复杂性对比

算法	时间复杂度	空间复杂度
二进制算法	$192D + 104A$	
NAF 算法	$193D + 65A$	
新算法	$64A$	9 kB

新算法采用预计算倍点序列的方式,在进行标量乘法运算时,省去了倍点运算的时间开销;同时与二进制和 NAF 算法相比,它的点加运算量也有所减少. 总之,新算法用较小的存储空间开销,极大地提高了标量乘法的效率.

5.2 耗时对比分析

利用 Intel (R) Core (TM)2 CPU 1.83 GHz 1.83 GHz, 2.50 GB 内存的 PC 机,采用 Java 语言在 Eclipse 3.2 开发平台下编程实现二进制、NAF 和新算法. 针对实例中的椭圆曲线 $E_p(a, b)$ 和基点 P,给定 $k_1 = 342\,022\,277\,916$, $k_2 = 658\,453\,406\,249\,843\,303\,199\,893$, $k_3 = 100\,007\,262\,728\,299\,865\,628\,764\,269\,050\,385\,423\,453\,895\,943\,703$, $k_4 = 1\,257\,665\,175\,181\,983\,932\,879\,442\,163\,337\,659\,926\,839\,196\,360\,431\,526\,691\,610$, $k_5 = 6\,277\,101\,735\,386\,680\,763\,835\,789\,400\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000$, $k_6 = 6\,277\,101\,735\,386\,680\,763\,835\,789\,423\,176\,059\,013\,767\,194\,773\,000\,000\,000\,000$. 其中,$k_1 < k_2 < k_3 < k_4 < T/2 < k_5 < k_6$. 分别采用二进制、NAF 和新算法计算 $i = 1, 2, \cdots, 6$. 3 种算法的实际耗时对比如表 2 所示.

表 2 算法耗时对比 ms

算法	系数					
	k_6	k_1	k_2	k_3	k_4	k_5
二进制算法	10	21	42	49	57	59
NAF 算法	8	19	38	46	40	40
新算法	2	5	10	12	6	2

表 2 说明:①一般来说,NAF 优于二进制算法;②二进制算法的耗时均最长;③一般来说,随着 k_i 的增大,二进制和 NAF 算法的耗时呈现递增趋势,但由于不同 k_i 对应的二进制或 NAF 编码中非“0”元个数的差异,会出现了 k_5, k_6 对应的 NAF 算法的耗时反而小于 k_4;④新算法的耗时最少,一般来说,当 $k_i < T/2$ 时,随着 k_i 的增大,新算法的耗时呈现递增趋势;否则,随着 k_i 的增大,耗时呈现递减趋势.

6 结 论

为提高 ECC 标量乘法运算的效率,提出了一种基于预计算和周期性的标量乘法算法. 由点的周期性易知 $kP = O - (T - k)P$,故选择 k 和 $T - k$ 中较小者作为系数进行标量乘法运算,可减少点加和倍点的运算次数. 采用二进制算法预计算并保存倍点序列,用较小的存储空间(实例仅需 9 kB),却节省了大量倍点运算的时间开销. 验证实例结果表明:在多次标量乘法运算中,新算法的耗时均为最少,特别是当 k 较小或接近周期 T 时,效果更加明显,实例耗时仅需 2 ms. 因此,与二进制和 NAF 算法相比,新算法的计算复杂度明显降低,运算效率得到了有效地提高.

参考文献（References）

[1] Yang Feng, Zhong Cheng, Yin Mengxiao, et al. Teaching cryptology course based on theory-algorithm-practice-application mode [C]//Proceedings of the 1st International Workshop on Education Technology and Computer Science. Shanghai: Inst. of Elec and Elec Eng Computer Society, 2009: 468 – 470

[2] Koray K, Berkant U. Invalid-curve attacks on (hyper) elliptic curve cryptosystems[J]. Advances in Mathematics of Communications, 2010, 4(3): 307 – 321

[3] 祝跃飞,张亚娟. 椭圆曲线公钥密码导引[M]. 北京:科学出版社,2006:129,219 – 223
Zhu Yuefei, Zhang Yajuan. Introduction of elliptic curve cyptosystem[M]. Beijing: Science Press, 2006: 129, 219 – 223 (in Chinese)

[4] Shah P G, Huang Xu, Sharma D. Sliding window method with flexible window size for scalar multiplication on wireless sensor network nodes[C]//Proceedings of the 1st International Conference on Wireless Communication and Sensor Computing. New York: IEEE Computer Society, 2010: 1 – 6

[5] Katja S S, Olivier S, Tsuyoshi T. Analysis of fractional window recoding methods and their application to elliptic curve cryptosystems[J]. IEEE Transactions on Computers, 2006, 55(1): 48 – 57

[6] 赵佳,韩臻. 自适应的椭圆曲线滑动窗口标量乘法[J]. 北京交通大学学报,2007,31(2):6 – 9
Zhao Jia, Han Zhen. Adaptive elliptic curve sliding window scalar multiplication algorithm[J]. Journal of Beijing Jiaotong University, 2007, 31(2): 6 – 9 (in Chinese)

[7] Shah P G, Huang Xu, Sharma D. lgorithm based on one's complement for fast scalar multiplication in ECC for wireless sensor network [C]//Proceedings of the 24th International Conference on Advanced Information Networking and Applications Workshops. New York: IEEE Computer Society, 2010: 571 – 576

[8] Wu Keke, Li Dawei, Li Huiyun, et al. Partitioned computation to accelerate scalar multiplication for elliptic curve cryptosystems [C]//Proceedings of the 15th International Conference on Parallel and Distributed Systems. New York: IEEE Computer Society, 2009: 551 – 555

[9] Miller V. Uses of elliptic curves in cryptography[C]//Advances in Cryptology-Crypto85. Berlin: Springer-Verlag, 1985: 417 – 426

[10] Koblitz N. Elliptic curve cryptosystems[J]. Mathematics of Computation, 1987, 48(17): 203 – 209

[11] Stinson D R. Cryptography theory and practice[M]. 3rd ed. London: Chapman & Hall/CRC Press Taylor & Francis Group, 2006: 257 – 258

[12] Diffie W, Hellman M E. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644 – 654

[13] 董付国,厉玉蓉. 秦九韶算法思想在 RSA 密码算法中的应用研究[J]. 计算机工程与应用,2008,44(28):65 – 66
Dong Fuguo, Li Yurong. Study on Qin Jiushao algorithm and its application in RSA[J]. Computer Engineering and Applications, 2008, 44(28): 65 – 66 (in Chinese)

(编　辑:文丽芳)

(上接第 1450 页)

[3] 孙小松,杨涤,耿云海,等. 中继卫星天线指向制策略研究[J]. 航空学报,2004,25(4):376 – 380
Sun Xiaosong, Yang Di, Geng Yunhai, et al. The antenna pointing control strategy study of tracking and data relay satellite [J]. Acta Aeronautica et Astronautica Sinica, 2004, 25(4): 376 – 380 (in Chinese)

[4] 佘海鹰,曲广吉. 中继卫星正常模式星体和天线两级控制耦合动力学初步仿真[J]. 航天器工程,1998,7(4):5 – 10
She Haiying, Qu Guangji. The tracking and data relay satellite's main body and antenna coupling dynamic elementary simulation [J]. Space Craft Engineering 1998, 7(4): 5 – 10 (in Chinese)

[5] 刘锦阳. 刚柔耦合动力学系统的建模理论研究[D]. 上海:上海交通大学船舶与建筑工程学院,2000
Liu Jinyang. Study on dynamic modeling theory of rigid-flexible coupling system[D]. Shanghai: School of Naval Architectye, Ocean and Civil Engineering, Shanghai Jiaotong University, 2000 (in Chinese)

[6] 李长江,廖瑛,廖超伟,等. 卫星天线双轴定位系统虚拟样机动力学仿真[J]. 中国空间科学技术,2005(5):52 – 55
Li Changjiang, Liao Ying, Liao Chaowei, et al. The dynamic simulation of the virtual prototype of the two-axes position mechanism for satellite antennas[J]. Chinese Space Science and Technology, 2005(5): 52 – 55 (in Chinese)

[7] Melkote H, Khorrami F. Robust nonlinear control and torque ripple reduction for permanent magnet stepper motors[J]. Control Theory and Applications, IEEE Proceedings, 1999, 146(2): 186 – 196

[8] 林瑞,孙兴进. 步进电机的细分电流波形及其实现[J]. 上海大学学报,1999,12(5):501 – 502
Lin Rui, Sun Xingjin. Subdivision current wave of stepping motor and its implementation [J]. Journal of Shanghai University, 1999, 12(5): 501 – 502 (in Chinese)

[9] 诸德超,邢誉峰,程伟,等. 工程振动基础[M]. 北京:北京航空航天大学出版社,2004
Zhu Dechao, Xing Yufeng, Cheng Wei, et al. The base of engineering vibration[M]. Beijing: Beihang University Press, 2004 (in Chinese)

[10] 张鹏飞,程伟,王和,等. 航天器反作用轮扰动建模及参数辨识[J]. 北京航空航天大学学报,2010,36(7):879 – 882
Zhang Pengfei, Cheng Wei, Wang He, et al. Disturbance modeling and parameters identification of reaction wheel assembly on spacecraft [J]. Journal of Beijing University of Aeronautics and Astronautics, 2010, 36(7): 879 – 882 (in Chinese)

(编　辑:李　晶)