一种 Montgomery 型椭圆曲线的高效标量乘算法

庞世春[1,2],刘淑芬[1],从福仲[2],姚志林[1]
(1.吉林大学计算机科学与技术学院,吉林长春 130022; 2.空军航空大学基础部,吉林长春 130012)

摘 要: 椭圆曲线标量乘法是椭圆曲线密码系统的基本运算,安全高效的标量乘法将直接提高椭圆曲线密码系统的效率和安全性.本文将 Fibonacci 数列的概念进行了扩展,提出了 Fibonacci 型数列的概念,并用 Fibonacci 型数列将 Montgomery 型曲线上点的加法运算公式进行了简化,得到了新的点加公式 fibAdd.利用黄金比率加法链方法计算任意整数 k 的 Fibonacci 型数列.将二种方法结合,构造了 Montgomery 型曲线上任意整数 k 的标量乘算法.本文提出的算法比 GRAC-258 快 23%,在最优情况下比 EAC-320 快 39%,同时,由于本算法只需要进行点的加法运算,不需要进行倍点运算,因而本算法天然地具有对抗边信道攻击的特性.

关键词: 标量乘法; Montgomery 曲线; 黄金比率加法链
中图分类号: TP301.6 **文献标识码:** A **文章编号:** 0372-2112 (2011) 04-0865-04

An Efficient Scalar Multiplication Algorithm on Montgomery-Form Elliptic Curve

PANG Shi-chun[1,2], LIU Shu-fen[1], CONG Fu-zhong[2], YAO Zhi-lin[1]
(1. *College of Computer Science and Technology, JiLin University, , Changchun, Jilin* 130022, *China*;
2. *Fundamental Department, Aviation University of Air Force, Changchun, Jilin* 130012, *China*)

Abstract: Elliptic curve scalar multiplication is a basic operation of elliptic curve cryptosystem. Secure and efficient scalar multiplication algorithm will directly promote efficiency and security of elliptic curve cryptosystem. In this paper, the concept of Fibonacci series is extended and proposed, which is used to simplify point addition formula on Montgomery-Form elliptic curve and to get a new point addition formula fibAdd. The Fibonacci-type series of any positive integer k is computed by using Golden Ratio Addition Chain method. By combing of both methods, the paper constructs an efficient and secure scalar multiplication algorithm for any given integer k on Montgomery-Form elliptic curve is constructed. This new algorithm is 23% faster than GRAC-258 and is 39% faster than EAC-320 in the best case. Also, because the algorithm performs only point addition operation, and there is no need for doubling operation, it possesses naturally the ability to resist side channel attack.

Key words: scalar multiplication; montgomery-form elliptic curve; golden ratio addition chain

1 引言

椭圆曲线密码是由 Miller(1986)和 Koblitz(1987)共同提出的,目前已经成为公钥密码的主要标准之一(IEEE P1363, ANSI X9.62, ANSI X9.63).同 RSA 公钥密码及 ElGamal 公钥密码相比,椭圆曲线密码提供了更高的单位比特安全强度,160 位密钥长度的椭圆曲线密码提供的安全强度相当于 1024 位密钥长度的 RSA 密码提供的安全强度.因而,椭圆曲线密码特别适合那些存储资源或计算资源受限的应用环境,如:智能卡、PDA 等.

椭圆曲线密码中主要的运算是标量乘运算$[k]P = P + \cdots + P$,此处,P 是给定椭圆曲线 E 上的一点,k 为给定整数.标准的计算方法是利用 k 的二进制表示 $k = d_{n-1}2^{n-1} + d_{n-2}2^{n-2} + \cdots + d_1 2 + d_0$,其中 $d_{n-1} = 1$, $d_i = -1, 0, 1 (i = 0, 1, \cdots, n-2)$, $n = \lceil \log_2^k \rceil$,该方法称为加减链方法,非临接标准型(NAF, Non-adjacent Form)提供了一种构建加减链的方法.加减链方法常和窗口方法结合使用.在 IEEE P1363 标准中,标量乘法运算是采用 Jacobean 坐标系上的加减链方法实现的.由于一次标量乘法常常需要进行一系列的点的加法和倍点运算,而每个点的加法或倍点运算又需要很多次有限域上的乘法、平方、求逆运算,因而,优化标量乘法的运算具有重要意义.

优化标量乘法的方法一是优化点的加法或倍点公式,二是减少每次标量乘法运算所需的点的加法或倍

收稿日期:2010-03-03;修回日期:2010-07-05
基金项目:吉林省重大项目(No.20060328);国家科技攻关项目(No.2004BA907A20)

点运算次数.使用混合坐标系策略可以提高点的加法或倍点运算效率.由于求逆运算同乘法和平方运算相比计算费时的多,文献[1]通过将求逆运算转化为除法运算提高了求逆运算的效率.基于最优扩域(OEF,optimal extension field)概念,文献[2]研究了 p 元扩域上的快速乘法算法.欧几里德加法链(Euclidean Addition Chain)方法提供了一种仅通过加法计算椭圆曲线标量乘法的方法,文献[3]提出了一种求最短加法链的黄金比率加法链方法,从而减少了加法运算的次数.文献[4]提出了在 Montgomery 型曲线和 Koblitz 曲线上进行的高效标量乘算法.文献[5]利用一些特殊点上点乘计算公式效率较高的特点,基于双基数表示方法,构造了椭圆曲线多标量乘法的算法,文献[6]提出了一种超椭圆上的高效标量乘算法.文献[7]对椭圆曲线密码系统整体算法优化进行了研究.

边信道攻击(SCA,Side Channel Attack)是一种通过分析密码设备泄露的边信道信息来推测秘钥的密码分析方法.具体方法包括简单边信道分析和差分边信道分析.可用的边信道信息包括:设备运行时泄漏的时间信息、能量消耗信息、电磁辐射信息、出错信息等.标量乘法中的乘数 k 通常是一个秘密的参数.Weierstras 型曲线上点的加法和二倍点计算公式是不同的,因而在点乘算法中通过能量消耗信息分析可能推导出 k 的值.文献[8]给出了使用边信道分析攻击目前计算标量乘法的二进制方法如:Double-and-Add 算法,double-Add-and-Subtract 算法,Double-and-Add-Always 算法的例子.

对抗边信道攻击主要有三种基本的方法:(1)统一加法公式或者考虑可选的参数;(2)插入伪指令或伪操作;(3)使用比较"平滑"的算法.所有这些方法都会在增加安全性的同时损失计算效率.设计合理的椭圆曲线标量乘法算法需要综合运用多种方法,才能在保证安全性的同时,提高密码系统实现的效率.

2 相关工作

2.1 Euclid 加法链方法

Euclid 加法链方法和椭圆曲线相结合可以构造高效安全的椭圆曲线标量乘法[3].事实上,由于椭圆曲线加法链方法只涉及点的加法运算而不需要进行点的倍点运算,因而保证了边信道信息的"平滑"性,能够对抗边信道攻击[9].

定义 1 加法链

计算整数 k 的加法链是一个序列,$v=v(v_1,\cdots,v_l)$,其中 $v_1=1, v_l=k, v_i=v_{i-1}+v_{i-2}(1\leqslant i\leqslant l)$. l 是加法链的长度.

定义 2 Euclid 加法链

Euclid 加法链是满足如下条件的加法链:$v_1=1, v_2=2, v_3=v_1+v_2$,对所有的 $3\leqslant i\leqslant l-1$,如果 $v_i=v_{i-1}+v_j(j<i-1)$,则 $v_{i+1}=v_i+v_{i-1}$或 $v_{i+1}=v_i+v_j$.

通过辗转相减可以求得计算任意整数 k 的加法链[9],但该加法链的长度取决于选取的减数 g.求最短加法链问题是一个 NP 完全问题,已知的上限为

$$l(n)\leqslant \log n+\log/\log\log n+o(\log n/\log\log n)$$

注意到,若整数 k 是 Fibonacci 数,则求 k 的加法链序列 $v=v(v_0,\cdots,v_l)$恰好就是整数 k 对应的 Fibonacci 数列,l 就是整数 k 的最短加法链长度.

定义 3 Fibonacci 数列

Fibonacci 数列$\{F_n\}$定义为 $F_0=0, F_1=1, F_n=F_{n-1}+F_{n-2}(n\geqslant 2)$.

定理 1 $\{F_n\}$是 Fibonacci 数列,则

$$\lim_{n\to\infty}\frac{F_n}{F_{n-1}}=\phi$$

其中,$\phi=\dfrac{1+\sqrt{5}}{2}$称为黄金比率或黄金分割点.

2.2 Montgomery 型曲线

定义 4 Montgomery 型曲线[10]

设 $p(\geqslant 3)$是一个素数,F_{p^n}是特征为 p 的有限域,F_{p^n}上的 Montgomery 型椭圆曲线定义为

$$E: By^2=x^3+Ax^2+x$$

此处,$A, B\in F_{p^n}$并且 $B(A^2-4)\neq 0$.

设(x_n, y_n, z_n)表示 Montgomery 型曲线 E_K 上的点 $[n]P$,则投影坐标系下点的加法运算公式为:

$$x_{n+m}=z_{m-n}((x_m-z_m)(x_n+z_n)+(x_m+z_m)(x_n-z_n))^2 \quad (1)$$

$$z_{n+m}=x_{m-n}((x_m-z_m)(x_n+z_n)-(x_m+z_m)(x_n-z_n))^2 \quad (2)$$

注意到,该加法的计算时间为 $4M+2S$,此处 M 表示 F_{p^n}上的乘法操作,S 表示 F_{p^n}上的平方操作,倍点公式的计算时间为 $3M+2S$[10].同时,为了计算点$[m+n]P=[m]P+[n]P$,需要知道点$[m]P$,$[n]P$,$[m-n]P$的 x 坐标和 z 坐标,而点的 y 坐标可以在标量乘法结束后通过一次运算进行恢复,恢复操作的时间为 $12M+S$.同 Weierstrass 型曲线在单一坐标系及混合坐标系下的点的加法进行效率比较,发现 Montgomery 型曲线上点的加法效率是最高的,应用时的主要困难在于要计算$[m]P$ 和$[n]P$ 的和需要预先知道$[m-n]P$,而这一般是做不到的.

3 高效安全的椭圆曲线标量乘法

3.1 整数 k 的 Fibonacci 型数列

定义 5 设数列$\{F_i \mid i=0,\cdots,n\}$满足 Fibonacci 数列的条件 $F_i=F_{i-1}+F_{i-2}(i\geqslant 2)$,称该数列为 Fibonacci

型数列.

由定义知 Fibonacci 数列一定是 Fibonacci 型数列,反之则不成立,如数列{1,3,4,7,11}是 Fibonacci 型数列但不是 Fibonacci 数列.

定义 6　若存在 Fibonacci 型数列$\{F_i \mid i=0,\cdots,n\}$,使正整数 $k=F_n$,则称该 Fibonacci 型数列$\{F_i \mid i=0,\cdots,n\}$为整数 k 的 Fibonacci 型数列.

定理 2　任意整数 k,都存在自己的 Fibonacci 型数列.

由上述定义和定理知标量乘法$[k]P$可以通过 k 的 Fibonacci 型数列迭代求得.事实上,若整数 k 的 Fibonacci 型数列为$\{F_i \mid i=0,\cdots,n\}$,则$[F_i]P=[F_{i-1}+F_{i-2}]P=[F_{i-1}]P+[F_{i-2}]P$,而$[F_{i-1}-F_{i-2}]P=[F_{i-3}]P$,式(1)、(2)变为:

$$x_{F_i}=z_{F_{i-3}}((x_{F_{i-1}}-z_{F_{i-1}})(x_{F_{i-2}}+z_{F_{i-2}})+(x_{F_{i-1}}+z_{F_{i-1}})(x_{F_{i-2}}-z_{F_{i-2}}))^2 \quad (3)$$

$$z_{F_i}=x_{F_{i-3}}((x_{F_{i-1}}-z_{F_{i-1}})(x_{F_{i-2}}+z_{F_{i-2}})-(x_{F_{i-1}}+z_{F_{i-1}})(x_{F_{i-2}}-z_{F_{i-2}}))^2 \quad (4)$$

用助记符 fibAdd()表示该加法,则上式简记为$[F_i]P=\text{fibAdd}([F_{i-1}]P,[F_{i-2}]P,[F_{i-3}]P)$.

3.2　黄金比率加法链

寻找最短加法链的问题是加法链方法的核心问题,文献[4]提出了一种基于黄金比率的计算最短加法链的方法.其思想是既然 Fibonacci 数的最短加法链可求,则可以通过黄金比率加法链方法构造任意整数 k 的 Fibonacci 型数列$\{F_i \mid i=0,\cdots,n\}$.方法是设

$u_0=k, u_1=[u_0\times\phi^{-1}], u_i=u_{i-2}-u_{i-1}(i=2,3,\cdots)$.

具体算法如下:

算法 1　GoldenAdditionChain(k, MG, LB)

$\phi^{-1}\leftarrow(-1+\sqrt{5})/2, u_0\leftarrow k, u_1\leftarrow[u_0\times\phi^{-1}]$,
$u_2\leftarrow u_0-u_1, S=\{1,2,3\}, i=2, j=1$
while　$u_i > LB$ do
if　$|u_i-u_{i-1}\times\phi^{-1}| > MG$ or $u_i\leqslant u_{i-1}/2$
then
　　$u_{i+1}\leftarrow[u_{i-1}\times\phi^{-1}]$
　　$g_i\leftarrow u_i-u_{i+1}$
　　$S\leftarrow S\cup\{g_i\}$
　　$j\leftarrow j+1$
　　$u_{i+2}\leftarrow u_{i-1}-u_{i+1}$
　　$i\leftarrow i+1$;
Else
　　$i\leftarrow i+1$
　　$u_i\leftarrow u_{i-2}-u_{i-1}$
　　$S\leftarrow S\cup\{u_i, u_{i-1}u_{i-2}\}$
Return S

令 $F_{n-i}=u_i$,则数列$\{F_i \mid i=0,\cdots,n\}$即为整数 k 的 Fibonacci 型数列$\{F_i \mid i=0,\cdots,n\}$.

3.3　Montgomery 型曲线的标量乘法

算法 2　MontScalarMultipilication
输入:整数 $k, P\in E$,整数 LB, MG
输出:$[k]P$
$\{F_i \mid i=0,\cdots,n\}\leftarrow$ GoldenAdditionChain(k, LB, MG)
//$u_i=F_{n-i}$
$a\leftarrow[F_0]P, b\leftarrow[F_1]P, c\leftarrow[F_2]P, temp\leftarrow 0$
$i\leftarrow 3$
while $i\leqslant n$ do
　　$temp\leftarrow$fibAdd(a, b, c)
　　$a\leftarrow b, b\leftarrow c, c\leftarrow temp$
　　$i\leftarrow i+1$
Return $temp$

4　结论

文献[11]中的实验表明一个 160 位的整数对应的黄金比率加法链长度最好可以达到 $n=258$.按照本文的算法 1 次标量乘需要进行$(n-1)$次点的加法,1 次倍点运算及 1 次 y 坐标恢复操作.1 个 160 位的整数标量乘总的计算时间为:

$$(4M+2S)(n-1)+(3M+2S)+(12M+4S)=1043M+520S$$

比率 S/M 独立于定义的有限域,也独立于具体的密码实现,可以近似看做 0.8.按该比率进行折算后的计算时间

$$\#[m]=1043M+520\times 0.8M=1459M$$

将本文的结果同文献[12]提出的新的点加公式(NewAdd)及文献[3]提出的混合坐标系下黄金比率加法链算法的结果列在表 1 中进行比较:

表 1　160 位标量乘法平均计算时间

算法	公式	折算计算时间 #[m]
Fibonacci-and-add	NewAdd[12]	2311
Signed Fib-and-add	NewAdd[12]	2088
Window Fib-and-add	NewAdd[12]	1960
EAC-320	NewAdd[12]	2112
GRAC-258	Mixed Coordinate[3]	1907
MontScarlarMultiplication-258	fibAdd	1459

从上表可知,本文提出的算法比 GRAC-258 快 23%,在最优情况下比 EAC-320 快 39%.

参考文献

[1] K Fong, D Hankerson, et al. Field inversion and point halving revisited[J]. IEEE Transactions on Computers, 2004, 53(8): 1047 – 1059.

[2] 李银,陈恭亮,李建华.P 元扩域上的快速乘法[J].通信学报,2009,30(11):101 – 105.

Li Yin, Chen Gongliang, Li Jianhua. Efficient multiplication for finite fields of p characteristic[J]. Journal on Communications, 2009, 31(11): 107 – 111. (in Chinese)

[3] Raveen R Goundar, Kenichi Shiota, Masahiko Toyonaga. SPA resistent scalar multiplication using golden ratio addition chain method[J]. International Journal of Applied Mathematics, 2008, 38(2): 110 – 119.

[4] Katsuyuki Okeya, Kouichi Sakurai. Efficient elliptic curve cryptosystems from a scalar multiplication algorithm with recovery of the y-coordinate on a montgomery-form elliptic curve[A]. Proceedings of CHES2001[C]. Berlin, Springer-Verlag, 2001. 126 – 134.

[5] 鲍皖苏,陈辉.基于双基表示的并列点乘算法[J].电子学报,2009,37(4):873 – 876.
Bao Wanshu, Chen Hui. A new simultaneous scalar multiplication based on double-base number system[J]. Acta Electrionica sinica, 2009, 37(4): 873 – 876. (in Chinese)

[6] 游林.一类超椭圆曲线上的快速除子标量乘[J].电子学报,2008,36(10):2049 – 2054.
You Lin. Fast divisor scalar multiplications on a class of hyperelliptic curves[J]. Acta Electrionica sinica, 2008, 36(10): 2049 – 2054. (in Chinese)

[7] 侯整风,李岚.椭圆曲线密码系统整体算法设计及优化研究[J].电子学报,2004,32(11):1904 – 1906.
Hou Zhengfeng, Li Lan. The research on designing and optimizing of the algorithm for elliptic curve cryptography[J]. Acta Electrionica sinica, 2004, 32(11): 1904 – 1906. (in Chinese)

[8] Ian F Blake, Gadeil Seroussi, Nigel P Smart. Advances in Elliptic Curve Cryptography[M]. London Mathematical Society Lecture Note Series 317. London. Cambridge University Press, 2005. 69 – 100.

[9] Andrew Bryne, Nicolas Meloni, Emanuel, et al. SPA resistant elliptic curve cyptosystem using addition chains[J]. International Journal of High Performance Systems Architecture, 2007, 1(2): 133 – 142.

[10] Katsuyuki Okeya, Kouichi Miyazaki, Kouichi Sakurai. A fast scalar multiplication method with randomized projective coordinates on a montgomery-form elliptic curve secure against side channel attacks[A]. Proceedings of ICICS2001, LNCS 2288[C]. Xian: Springer-Verlag, 2002. 428 – 439.

[11] Goundar R R, Shiota K, Toyonaga M. New strategy for doubling-free short additon-subtraction chain[J]. International Journal of Applied Mathematics, 2007, 2(3): 438 – 445.

[12] Nicolas Meloni. New point addition formulae for ECC application[A]. Proceedings of WAIF2007, LNCS 4547[C]. Berlin: Springer-Verlag, 2007. 189 – 201.

作者简介

庞世春 男,1975 年出生,吉林长春人,博士生,讲师.研究方向:计算机网络与安全,椭圆曲线密码.
E-mail: psc1975@126.com

刘淑芬 女,1950 年出生,教授,博士生导师,研究方向:计算机支持协同工作、软件体系结构、基于模型驱动的软件编程方法、网络管理技术.
E-mail: liusf@mail.jlu.edu.cn

从福仲 男,1967 年出生,教授,博士生导师.研究方向:微分方程与动力系统.
E-mail: congfz67@126.com

姚志林 男,1973 年出生,博士,讲师.研究方向:计算机支持协同工作、基于模型驱动的软件开发方法.
E-mail: yaozl@jlu.edu.cn