生成适用于双线性对的椭圆曲线中的多项式构造*

苏志图，李 晖，马建峰
（西安电子科技大学计算机网络与信息安全教育部重点实验室，陕西 西安 710071）

摘 要：在构造适用于双线性对的椭圆曲线的方法中，通常将椭圆曲线的参数表示成有理多项式，为有效地生成椭圆曲线，要求复乘方程的次数应小于3。通过将椭圆曲线参数看作数域元素，提出了一种构造合适的有理多项式的方法，使得复乘方程的次数小于3。给出一些例子，特别给出了嵌入次数为8的例子，一般认为嵌入次数为8时，次数小于3的复乘方程不存在。

关键词：双线性对；多项式；椭圆曲线；数域
中图分类号：TN918.1 **文献标志码**：A **文章编号**：0529-6579（2010）04-0030-04

Constructing Polynomials for Generating Pairing-friendly Elliptic Curves

SU Zhitu, *LI Hui*, *MA Jianfeng*
(Key Lab of Computer Networks and Information Security of Ministry of Education,
Xidian University, Xi'an 710071, China)

Abstract: In constructing pairing-friendly ellitpic curves, the curve parameters are often represented by polynomials with rational coefficients. For efficiently generating the curves parameters, the degree of the complex multipliction polynomial must be less than 3. A method is proposed to constructed suitable polynomials which will make the degree of the complex multipliction polynomial less than 3. Some examples are given, especially when embedding degree is 8. It is generally believed that when embedding degree is 8 the complex multipliction polynomial whose degree is less than 3 does not exist.

Key words: pairing; polynomial; ellitpic curve; number field

基于双线性对的密码体制是目前公钥密码学的一个热点研究方向，许多协议已经提出，例如：单轮三方密钥交换协议[1]，基于身份的加密体制[2]，短签名方案[3-5]。但是这些基于双线性对的密码方案不能在随机选取的椭圆曲线上实现，因为实现双线性对的椭圆曲线需要一般的椭圆曲线所不具备的一些特殊性质[2]。

设 E 是一条定义于有限域 F_q 上的椭圆曲线，它的点群的阶 $\#E(F_q)$ 有一个大的素因子 r。如果 k 是满足 $r \mid q^k - 1$ 的最小的正整数，则称 E 对于 r 的嵌入次数为 k。满足这种条件的椭圆曲线称为适用于双线性对的椭圆曲线。在实际应用中，要求嵌入次数 k 大小应适当。Menezes 等[6]指出超奇异椭圆曲线的嵌入次数小于6，它适合实现基于双线性对的密码体制。由于基于双线性对的密码体制的安全性与嵌入次数密切相关，为了达到更高的安全级别，必须转向一般的椭圆曲线。但 Balasubramanian 等[7]的研究结果表明具有小嵌入次数的椭圆曲线非常稀少。因此，很难通过随机选取椭圆曲线的方法来得到适用于双线性对的椭圆曲线，必须通过一些方法来精确构造出嵌入次数较小的适用于双线性对的椭圆曲线。

Miyaji 等[8]首先提出了构造嵌入次数为3，4和6并具有素数点群阶的一般椭圆曲线的方法。在他们方法的基础上 Scott 等[9]构造了接近素数阶的一般椭圆曲线。之后许多构造具有任意嵌入次数的

* 收稿日期：2009-04-10
基金项目：国家自然科学基金资助项目（60772136，60702059）
作者简介：苏志图（1983 年生），男，博士生；E-mail：ztsu@mail.xidian.edu.cn

一般椭圆曲线的方法被提出[10-11]。但这些方法都有各自的不足，为了解决这些不足，Freeman[11]将构造适用于双线性对的椭圆曲线的构造方法进行总结，并阐明了解决这些不足的所需要做的工作。本文提出的方法就是完成文献［11］提出的要做的工作之一，即构造适宜的有理多项式使得复乘方程的次数小于3。

1　理论背景

设 E 是一条定义于有限域 F_q 上的椭圆曲线，则它的点群的阶 $\#E(F_q)=q+1-t$，$|t|\leqslant 2\sqrt{q}$[12]。因为要构造适用于双线性对的椭圆曲线，故要求

$$hr=q+1-t \tag{1}$$

$$q^k\equiv 1(\bmod r) \tag{2}$$

从（1）和（2）式可得 $(t-1)^k\equiv 1(\bmod r)$，也就是说 $t-1$ 是模 r 的 k 次单位根。如果 $t-1$ 是模 r 的一个 k 次本元单位根，则有 q 模 r 的次数为 k。从而可得 $E(F_q)$ 的嵌入次数为 k。称方程 $t^2-4q=-Dv^2$ 为复乘方程，其中 D 是一个无平方因子的正整数。我们称 D 为复乘判别式。

定理 1　设 p 是一个素数，k 是一个小的正整数。如果 p 不能整除 k 且 $u\in\mathbb{Z}$，则 u 模 p 的次数为 k（即 $u^k\equiv 1(\bmod p)$，k 是满足着这一条件的最小正整数）当且仅当 $p\mid\Phi_k(u)$ 其中 $\Phi_k(x)$ 是 k 次本原多项式。

证明　见文献［13］。

在方程（1）中，如果 $r\mid\Phi_k(t-1)$，从定理1可知 $E(F_q)$ 的嵌入次数为 k。

构造适用于双线性对的椭圆曲线时，通常将椭圆曲线的参数 t,r,q 表示为有理多项式 $t(x)$，$r(x)$ 和 $q(x)$。于是椭圆曲线表示为 $E(F_{q(x)})$ 而它的点群的阶表示为 $E(F_{q(x)})=q(x)+1-t(x)=h(x)r(x)$。假设 $r(x)\mid\Phi_k(t(x)-1)$ 并且存在某个 $x_0\in\mathbb{Z}$ 使得 $r(x_0)$ 和 $q(x_0)$ 为素数，则可知 $r(x_0)\mid\Phi_k(t(x_0)-1)$。如果 $t(x_0)$ 为整数且 $|t(x_0)|\leqslant 2\sqrt{q(x_0)}$，那么就存在一条定义于有限域 $F_{q(x_0)}$ 上的椭圆曲线 $E(F_q)$，它的点群的阶为 $q(x_0)+1-t(x_0)$[14]。从定理1可知，$E(F_{q(x_0)})$ 相对于 $r(x_0)$ 的嵌入次数为 k。根据定理1，通常会令 $r(x)$ 为 $\Phi_k(u(x))$ 的一个不可约分因子并令 $t(x)=u(x)+1$。由于此时椭圆曲线的点群阶 $E(F_{q(x_0)})$ 已经固定，我们面临一个问题就是必须生成具有固定点群阶的椭圆曲线。通常采用复乘算法来解决这一问题[14]。但是复乘算法只有在复乘判别式不是太大的情况下效率才比较高。因此必须保证复乘判别式不能太大[14]。

在以上论述的基础上，可将适用于双线性对的椭圆曲线在参数表示成有理多项式后应满足的条件归结为[11]：

对于某个无平方因子的正整数 D

① $q(x)$ 和 $r(x)$ 均是不可约分的有理多项式，对于某些 $x_0\in\mathbb{Z}$，$q(x_0)$ 和 $r(x_0)$ 均为素数。

② $r(x)\mid q(x)+1-t(x)$。

③ $r(x)\mid\Phi_k(t(x)-1)$。

④ $Dy^2=4q(x)-t(x)^2$ 存在有无限多的整数解。

上述中的①，②，③和④保证存在适用于双线性对的椭圆曲线，并且保证这条椭圆曲线能有效生成，因为我们可以令 D 比较小。同时能比较容易找到 $x_0\in\mathbb{Z}$，使得 $q(x_0)$ 和 $r(x_0)$ 均为素数而 $t(x_0)$ 为整数。之所以要求存在无限多的整数解，是因为只有这样才有可能找到同时满足 $q(x_0)$ 和 $r(x_0)$ 均为素数而 $t(x_0)$ 为整数的 x_0。

2　新的多项式构造方法

由于前述的限制，我们对 $t(x)$，$r(x)$ 和 $q(x)$ 就有特殊的要求。满足上节①，②和③的 $t(x)$，$r(x)$ 和 $q(x)$ 能比较容易找到，可以采用文献［6，15］中的方法。而对于④最为理想的情况就是 $4q(x)-t(x)^2=Df(x)^2$，即 $4q(x)-t(x)^2$ 是一个无平方因子的正整数乘以一个有理多项式的平方。但这种情况极少，目前只发现在 $k=12$ 时存在这种结果[11]。令 $f(x)=4q(x)-t(x)^2$，则④可以表示为 $Dy^2=f(x)$，从而④的求整数解的问题，转变为求曲线 $Dy^2=f(x)$ 的整点问题。在文献［11］中作者指出只有当 $f(x)$ 的次数小于3时，$Dy^2=f(x)$ 才会存在有无限多的整数解。

可以将 $4q(x)-t(x)^2$ 用更为一般的形式来表示，令 $4q(x)-t(x)^2=D(x)V(x)^2$。因为 $V(x)^2$ 可以合并到 y^2 中去，故只要求 $D(x)$ 的次数小于3。目前通常采用的方法是使用计算机去搜索满足条件的多项式 $t(x)$，$r(x)$ 和 $q(x)$[11]。通常先选取满足关系式 $r(x)\mid\Phi_k(t(x)-1)$ 的有理多项式 $t(x)$ 和 $r(x)$，然后通过一些方法可以得到满足条件的 $q(x)$。令 $4q(x)-t(x)^2=D(x)V(x)^2$。根据前面的论述，要求有理多项式 $D(x)$ 的次数小于3。但在一般情况下 $V(x)$ 不存在，而只存在 $D(x)$ 并且它的次数大于3[11]。

为了寻找次数小于3的有理多项式 $D(x)$，我

们可以从另一个角度来看上述问题。假设 $r(x) \mid \Phi_k(t(x)-1)$，θ 是 $r(x)=0$ 的一个根，则有 $t(\theta)-1=\zeta_k$，$t(\theta)-1$ 是一个 k 次本原单位根[10]。如果 $K=Q[x]/(r(x))$ 是一个由 $r(x)$ 定义的数域，即 $K \cong Q(\theta)$，则 $D(x)V(x)^2 \equiv -(t(x)-2)^2 \bmod(r(x))$ 变为 $D(\theta)V(\theta)^2=-(\zeta_k-1)^2$，从而可得 $D(\theta)=\dfrac{-(\zeta_k-1)^2}{V(\theta)^2}$。将有理多项式 $t(x)-2$ 和 $V(x)$ 看作是数域 K 中的元素，则 $D(x)V(x)^2 \equiv -(t(x)-2)^2 \bmod(r(x))$ 可以变为数域 K 中的一个等式 $D(x) \equiv \dfrac{-(t(x)-2)^2}{V(x)^2}$，这样所有的计算都在数域 K 中进行。因为 $t(x)$ 和 $r(x)$ 之前已经选定，通过选取不同的 $V(x)$，寻找次数小于 3 的有理多项式 $D(x)$。

上述的方法可以归结为如下的过程：

给定一个嵌入次数 k：

1）选取有理多项式 $r(x)$ 和 $t(x)$，$r(x) \mid \Phi_k(t(x)-1)$。

2）构造数域 $K=Q[x]/(r(x))$。

3）选取合适的有理多项式 $V(x)$，在数域 K 中计算 $\dfrac{-(t(x)-2)^2}{V(x)^2}$。

4）判断 $D(x)$ 的次数是否小于 3，如果不是，返回 1）。

在选取好 $t(x)$，$r(x)$ 和 $V(x)$ 后，可得 $q(x)=\dfrac{1}{4}(t(x)^2+D(x)V(x)^2)$，并且得到的 $r(x)$，$t(x)$ 和 $q(x)$ 满足关系式 $r(x) \mid q(x)+1-t(x)$。对于给定一个无平方因子的正整数 D，令 $Dy^2=D(x)$，去求这个方程的整数解，如果 $q(x)$ 和 $r(x)$ 对于方程的某个整数解 $x_0 \in \mathbb{Z}$，$q(x_0)$ 和 $r(x_0)$ 均为素数且 $t(x_0)$ 为整数。则存在一条具有以上参数的椭圆曲线。可以运用复乘算法来生成具有这些参数的椭圆曲线。因为可以选取适宜的复乘判别式 D，故而复乘算法能很有效地生成这条曲线。

以下给出一些运用上述方法，得到的 $D(x)$ 的次数小于 3 的例子。

例子 1

假设 $k=6$，令 $u(x)=-x+1$，$r(x)=x^2-x+1$，可知 $r(x) \mid \Phi_k(t(x)-1)$。在数域 $K=Q[x]/(r(x))$ 中我们选取 $v(x)=x-1$，计算 $D(\theta)=\dfrac{-(\zeta_k-1)^2}{V(\theta)^2}$，得 $D(x)=x$。$D(x)$ 的次数小于 3。

例子 2

假设嵌入次数为 $k=8$，选取 $u(x)=x^3-3x^2+3x-1$ 和 $r(x)=x^4-4x^3+6x^2-4x+2$，计算可知 $r(x) \mid \Phi_k(t(x)-1)$。选取 $v(x)=x-1$，在数域 $K=Q[x]/(r(x))$ 中计算 $D(\theta)=\dfrac{-(\zeta_k-1)^2}{V(\theta)^2}$，我们得到 $D(x)=x^2$，$D(x)$ 次数为 2。

例子 3

假设 $k=8$，选取 $u(x)=x^3$ 和 $r(x)=x^4+1$，经过计算可知 $r(x) \mid \Phi_k(t(x)-1)$。令 $v(x)=x+1$，在数域 $K=Q[x]/(r(x))$ 中计算 $D(\theta)=\dfrac{-(\zeta_k-1)^2}{V(\theta)^2}$，可得到 $D(x)=x^2$，$D(x)$ 次数为 2。

在文献［11］中，作者认为当 $k=8$ 时，几乎不能得到 $4q(x)-t(x)^2$ 是次数小于 3 的多项式。而上面的例子则表明这是可能的，这就为 $k=8$ 时构造适用于双线性对的椭圆曲线提供了一种可能的途径。

3 结 论

将椭圆曲线的参数用多项式表示是构造适用于双线性对的椭圆曲线通常采用的方法。但要求 $q(x)-4t(x)^2$ 的次数不能大于 2，只有这样才有可能构造出适用于双线性对的椭圆曲线的参数。本文提出了一种新的构造次数低于 3 的多项式的方法，运用这个方法得到了一些例子，特别是在一般认为不存在当 $k=8$，找到了次数小于 3 的例子，这就为构造适用于双线性对的椭圆曲线提供了一种新的途径。

参考文献：

[1] JOUX A. A one round protocol for Tripartite Diffie-Hellman [J]. Journal of Cryptology, 2004, 17 (4): 263 - 276.

[2] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing [J]. SIAM Journal of Computing, 2003, 32 (3): 586 - 615.

[3] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing [C] // Advances in Cryptology-Asiacrypt'2001: Lecture Notes in Computer Science 2248. Berlin: Springer-verlag, 2002: 154 - 532.

[4] 张串绒，肖国镇. 利用身份和双线性对的多重签密 [J]. 西安电子科技大学学报，2007，34 (2)：270 - 273.

（下转第37页）

是 Lagrange 体系下的算法，而辛空间有限元 - 时间子域法是 Hamilton 体系下的算法。所有算例都明显看出，文中建立的新方法的计算精度和计算效率远高于国际上常用的 Wilson - θ 法和 Newmark - β 法。由于这种 Hamilton 力学体系下的新方法的稳定性、收敛性、计算精度和效率都高于 Lagrange 力学体系下的已有方法，因此这种辛算法具有广阔的应用前景。

参考文献：

[1] GOLDSTEIN H. Classical mechanics[M]. 2nd ed. Mass: Addison-Wesley Publishing Co,1980.

[2] 冯康,秦孟兆. Hamilton 体系的辛计算格式[M]. 杭州：浙江科技出版社,2004.

[3] 钟万勰. 应用力学的辛数学方法[M]. 北京：高等教育出版社,2006.

[4] 林家浩,钟万勰. 辛数学精细积分随机振动及应用[M]. 合肥：中国科学技术大学出版社,2008.

[5] 高强,彭海军,吴志刚,钟万勰. 非线性动力学系统最优控制问题的保辛求解方法[J]. 动力学与控制学报,2010,8(1):1 - 7.

[6] 钟万勰. 分析结构力学与有限元[J]. 动力学与控制学报,2004,2(4):1 - 8.

[7] 黄伟江,罗恩,章学军. 辛数值流形时间子域法[J]. 中国科学,2010,39(10):1487 - 1494.

[8] 章学军,黄伟江,罗恩. 夹层梁动力响应分析的一种辛算法[J]. 建筑科学,2010,26(1):56 - 59.

[9] 龚克. 单广义位移的深梁理论和中厚板理论[J]. 应用数学和力学,2000,21(9):984 - 990.

[10] LUO En,CHEUNG Y K. On the variational principles in linear elastodynamics [J]. Acta Mechanica Sinica, 1988, 4(4):377 - 349.

[11] 罗恩. 几何非线性弹性动力学中广义 Hamilton 型拟变分原理[J]. 中山大学学报：自然科学版, 1990,29(2):15 - 19.

[12] FINLAYSON B A. The method of weighted residuals and variational principles[M]. New York: Acad Press,1972.

[13] 王勖成,邵敏. 有限单元法基本原理和数值方法[M]. 2 版. 北京：清华大学出版社,1997.

(上接第 32 页)

[5] 辛向军, 李发根, 肖国镇. 一种基于短签名和离线半可信第三方的公平交换协议 [J]. 西安电子科技大学学报, 2007, 34 (1): 92 - 95.

[6] MENEZES A, OKAMOTO T, VANSTONE S. Reducing elliptic curve logarithms to logarithms in a finite field [J]. IEEE Transactions on Information Theory, 1993, 39 (5): 1639 - 1646.

[7] BALASUBRAMANIAN R, KOBLITZ N. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm [J]. Journal of Cryptology, 1998, 11 (2): 141 - 145.

[8] MIYAJI A, NAKABAYASHI M, TAKANO S. New explicit conditions of elliptic curve traces for FR-reduction [J]. IEICE Transactions on Fundamentals, 2001, E84 - A (5): 1234 - 1243.

[9] SCOTT M, BARRETO P. Generating more MNT elliptic curves [J]. Designs, Codes and Cryptography, 2006, 38 (2): 209 - 217.

[10] BREZING F, WENG A. Elliptic curves suitable for pairing based cryptography [J]. Designs, Codes and Cryptography, 2005, 37 (1): 133 - 141.

[11] FREEMAN D. Constructing pairing-friendly elliptic curves with embedding degree 10 [C] // Algorithmic Number Theory Symposium ANTS-VII: Lecture Notes in Computer Science 4076. Berlin: Springer-verlag, 2006: 452 - 465.

[12] SILVERMAN J. The arithmetic of elliptic curves [M]. New York: Springer-verlag, 1986: 131.

[13] WASHINGTON L. Introduction to cyclotomic fields [M]. New York: Springer-verlag, 1997: 13.

[14] ATKIN A, MORAIN F. Elliptic curves and primality proving [J]. Mathematics of Computation, 1993, 61 (203): 29 - 68.

[15] GALBRAITH S, MCKEE J, VALENCA P. Ordinary abelian varieties having small embedding degree [J]. Finite Fields and Their Applications, 2007, 13 (4): 800 - 814.