构造小嵌入次数的椭圆曲线参数化族

张 猛[①] 徐茂智*[①] 胡 志[②] 侯 英[③]
[①](北京大学数学科学学院 北京 100871)
[②](中南大学数学与统计学院 长沙 410083)
[③](清华大学计算机科学与技术系 北京 100084)

摘 要：配对友好椭圆曲线在基于配对的密码系统中起关键作用。这类曲线的构造不仅极大影响实现效率，更关系到系统安全。虽然目前已提出很多构造方法，但几乎都依赖穷尽搜索。该文提出一种构造该类曲线的系统方法，将寻找配对友好曲线问题转化到解方程，从而避免了穷尽搜索，并设计出具体算法。最后，将该算法应用到寻找嵌入次数为 5,8,10 和 12 的配对友好曲线中，发现所有类型的椭圆曲线族都可由该方法统一得到，包括完全族、可变判别式的完全族和稀疏族。特别地，还找到了新的椭圆曲线族。

关键词：基于配对的密码；椭圆曲线；配对友好曲线；参数化族
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2018)01-0035-07
DOI: 10.11999/JEIT170261

On Parameterized Families of Elliptic Curves with Low Embedding Degrees

Zhang Meng[①] Xu Maozhi[①] Hu Zhi[②] Hou Ying[③]
[①](*School of Mathematical Sciences*, *Peking University*, *Beijing* 100871, *China*)
[②](*School of Mathematics and Statistics*, *Central South University*, *Changsha* 410083, *China*)
[③](*Department of Compute Science and Technology*, *Tsinghua University*, *Beijing* 100084, *China*)

Abstract: Pairing-friendly elliptic curves play a vital role in pairing-based cryptography. The constructionof such curves not only influences the implementation efficiency, but concerns the security of system. Though many methods for constructing such curves are introduced, most of which rely on exhaustive search. In this paper, a new systematic method is proposed for constructing such curves which converts the problem to solving equation systems, instead of exhaustive searching. The utility of the method is demonstrated by surveying such elliptic curves with embedding degree 5, 8, 10 and 12, and all kinds of families can be explained via the proposed method including complete families, complete families with variable discriminant and sparse families. Specifically, a new family of elliptic curves is found.

Key words: Pairing-based cryptography; Elliptic curves; Pairing-friendly curves; Parameterized families

1 引言

近二十来，椭圆曲线上的双线性对一直在密码学研究受到广泛关注。一方面，它是攻击椭圆曲线离散对数问题的重要工具。众所周知，椭圆曲线密码学的强度正是建立在椭圆曲线离散对数的难解性上。而利用双线性对，可将椭圆曲线离散对数问题转化为有限域扩域乘法群的离散对数问题，因为有限域上离散对数问题存在亚指数时间算法，所以有可能降低椭圆曲线离散对数的计算复杂度。这类攻击方法的代表是 Menezes-Okamoto-Vanstone 攻击[1]；另一方面，基于双线性映射的良好性质，大量新颖的密码方案被设计出来，例如 Joux[2]的三方一轮密钥交换协议、Boneh 等人[3]的基于身份的加密体制、基于身份的签名[4,5]等。所有这类基于配对的密码方案都将双线性映射作核心工具，其安全级别由双线性对所在基域和扩域的离散对数求解的复杂度决定。虽然理论上可使用任何群上的非退化双线性映射，但到目前前为止，唯一满足条件的双线性映射只有有限域上阿贝尔簇的 Weil 对和 Tate 对，以及它们的各种变种。而在实际应用中，通常使用有限域上椭圆曲线的双线性对。

但是，并不是任意椭圆曲线都能构造实用的双线性对，基于配对的密码方案需要满足特殊性质的

收稿日期：2017-03-29；改回日期：2017-10-20；网络出版：2017-11-08
*通信作者：徐茂智 mzxu@pku.edu.cn
基金项目：国家自然科学基金(61272499, 61472016, 61672059, 61602526)，国家重点研发计划资助(2017YFB0802000)
Foundation Items: The National Natural Science Foundation of China (61272499, 61472016, 61672059, 61602526), The National Key R&D Program of China (2017YFB0802000)

曲线。设 E 是定义在有限域 $\mathbb{F}_q$ 上的椭圆曲线，P 是 E 上阶数为素数 r 的点，则 $r \mid \#E\left(\mathbb{F}_q\right)$。令 k 表示嵌入次数，即满足 $r \mid q^k - 1$ 最小的整数，则双线性对可将椭圆曲线群 $\langle P\rangle \subset E\left(\mathbb{F}_q\right)$ 上的离散对数问题规约到有限域乘法群 $\mathbb{F}_{q^k}^*$ 中。为保证安全性，需要选择合适的参数 (q,k,r)，使得 $\langle P\rangle$ 和 $\mathbb{F}_{q^k}^*$ 上的离散对数问题都是计算难解的。同时考虑到计算效率，群 $\langle P\rangle$ 的阶数 r 尽量接近 $\#E\left(\mathbb{F}_q\right)$，一般用参数 $\rho = \dfrac{\lg q}{\lg r}$ 来衡量这种接近程度。配对密码中使用的这类特殊曲线称为配对友好椭圆曲线。

实际中，人们更希望同时构造一批相同比特规模的配对友好曲线，这就产生了“族”的概念：即把曲线参数 (q,k,r) 替换成关于 x 的多项式组 $(q(x), r(x), t(x))$。根据复乘多项式的形式，配对友好椭圆曲线族可分为 3 类：完全族、可变判别式的完全族及稀疏族。目前，针对各类曲线族已有了很多构造方法，其中绝大多数方法都依赖于穷尽搜索，具体可参考文献[6−16]。

本文提出一种高效的构造配对友好曲线的新方法。通过引入一个更广义的概念“参数化族”，将寻找配对友好曲线问题转化为解方程，从而避免了穷尽搜索，使得寻找曲线的过程更加高效，并设计了具体算法。作为应用，本文利用新算法构造嵌入次数为 5,8,10 和 12 的椭圆曲线族，并进一步将问题转化为寻找指定椭圆曲线上的有理点。实验结果表明，该算法可统一得到所有类型的椭圆曲线族。

论文结构如下：第 2 节简要介绍配对友好曲线的基本概念，第 3 节描述构造曲线的新策略，并给出具体算法，第 4 节将算法应用到构造嵌入次数为 5,8,10 和 12 的椭圆曲线族中，最后在第 5 节总结全文。

2 配对友好椭圆曲线

本节简要介绍配对友好椭圆曲线的基本知识。按照文献[8]中定义，对于 $\mathbb{F}_q$ 上的椭圆曲线 E，如果存在素数 r，满足 $r \mid E\left(\mathbb{F}_q\right)$ 且 $\rho \le 2$，同时嵌入次数 k 满足 $k \le \dfrac{\lg r}{8}$，则称 E 为配对友好椭圆曲线。本文称不可约多项式 $f(x) \in \mathbb{Q}(x)$ 可表示素数当且仅当 $f(x)$ 的首项系数为正，且集合 $S(f) = \{f(x) \in \mathbb{Z} : x \in \mathbb{Z}\}$ 满足 $|S(f)| > 1, \gcd(S(f)) = 1$。

基于构造椭圆曲线的复乘方法[17]，可给出配对友好椭圆曲线族的定义。

定义 1 令三元组 $(q(x),t(x),r(x))$ 为非零的有理系数多项式，若满足条件：

(1) $q(x) = p(x)^d (d \ge 1)$，其中 $q(x)$ 可表示素数；

(2) $r(x) = c \cdot r'(x)$，其中 $c \in Z, c \ge 1, r'(x)$ 可表示素数；

(3) $q(x) + 1 - t(x) = h(x)r(x)$，其中 $t(x)$ 为 Frobenius 迹函数，$h(x) \in \mathbb{Q}(x)$；

(4) $r(x) \mid \phi_k(t(x)-1)$，其中 ϕ_k 为第 k 个分圆多项式；

(5) 复乘方程 $Dy^2 = 4q(x) - t(x)^2$ 有无限组整数解 (x,y)，其中 $D > 0$。

则称 $(q(x),t(x),r(x))$ 为嵌入次数 k、复乘判别式 D 的配对友好椭圆曲线族。

对于椭圆曲线族 $(q(x),t(x),r(x))$，仍可定义 ρ 值为

$$\rho(q(x),t(x),r(x)) = \lim_{x\to\infty} \frac{\lg q}{\lg r} = \frac{\deg q(x)}{\deg r(x)}$$

称复乘方程 $Dy^2 = 4q(x) - t(x)^2$ 的右端为复乘多项式，记为 $f(x) = 4q(x) - t(x)^2$。如果复乘方程存在整数解 (x_0, y_0)，满足 $q(x_0)$ 和 $r'(x_0)$ 为素数，则可利用复乘方法构造 $\mathbb{F}_{q(x_0)}$ 上的椭圆曲线 E，其中 $E\left(\mathbb{F}_{q(x_0)}\right)$ 存在阶数为 $r'(x_0)$ 的子群，且嵌入次数为 k。

根据 Freeman 等人在文献[8]中的结论，如果 $f(x) = 4q(x) - t(x)^2$ 中无平方部分的次数大于 2，则 $Dy^2 = f(x)$ 只有有限个整数解。因此，合适的复乘多项式必然具有形式 $f(x) = g(x)s^2(x)$，其中 $g(x), s(x) \in \mathbb{Q}[x]$，且 $\deg g \le 2$。

由 $g(x)$ 的次数，配对友好椭圆曲线族可分为 3 类：

(1) $\deg g = 0$ 时，则 $f(x) = D \cdot s^2(x)$，其中复乘判别式 $D > 0$，为完全曲线族；

(2) $\deg g = 1$ 时，则 $f(x) = (ax + b) \cdot s^2(x)$，为可变判别式的完全曲线族；

(3) $\deg g = 2$ 时，则 $f(x) = (ax^2 + bx + c) \cdot s^2(x)$，其中 $a > 0$，为稀疏曲线族。

3 构造配对友好曲线族的新方法

为满足定义 1 的条件(4)，需寻找特殊形式的分圆多项式分解，但此类分解十分稀少。Galbraith 等人[18]提供了一种方法来寻找合适的二次多项式 $u(x)$，后来 Tanaka 等人[11]将 $u(x)$ 扩展到任意次数。

引理 1 令 $u(x) \in \mathbb{Q}[x]$，则 $\Phi_k(u(x))$ 任何不可约因子的次数均为 $\phi(k)$ 的倍数。而且，多项式 $\Phi_k(u(x))$ 有次数为 $\phi(k)$ 的不可约因子当且仅当方程

$$u(z) = \zeta_k \tag{1}$$

在 $\mathbb{Q}(\zeta_k)$ 内有解。

如果找到满足式(1)的 $u(x)\in\mathbb{Q}[x]$，则分圆多项式 $\Phi_k(u(x))$ 可约。令多项式 $r(x)$ 为 $\Phi_k(u(x))$ 的 $\phi(k)$ 次不可约因子，并令 Frobenius 迹函数为 $t(x)=u(x)+1$，则有 $r(x)\,|\,\phi_k(t(x)-1)$，说明已找到满足定义 1 中条件(4)的 $r(x)$ 和 $t(x)$。

称定义 1 的条件(5)为复乘条件，在构造曲线过程中，它是最难满足的。接下来分析如何满足复乘条件。

设 deg $f(x)$<deg $r(x)$，这是实际中最常见的情形。令 $f(x)=4q(x)-t(x)^2=4r(x)h(x)-(t(x)-2)^2$，则有

$$f(x)=(-(t(x)-2)^2 \bmod r(x)) \tag{2}$$

若式(2)中 $f(x)$ 可以分解为 $f(x)=g(x)s(x)^2$，其中 $\deg g(x)<2$ 或者 $\deg g(x)=2$ 且首项系数为正，则令 $q(x)$ 为 $q(x)=(t(x)^2+f(x))/4$。如果 $q(x)$ 可表示素数，则 $(q(x),r(x),t(x))$ 为嵌入次数为 k 的椭圆曲线族。

为充分利用引理 1，将 $q(x),r(x)$ 和 $t(x)$ 的系数也考虑在内，引入参数化椭圆曲线族[19]。

定义2 (参数化椭圆曲线族)　符号和条件同定义1，配对友好椭圆曲线的参数化族由如下三元组组成

$$\left(q\left(x,a_0,a_1,\cdots,a_n\right),r\left(x,a_0,a_1,\cdots,a_n\right),t\left(x,a_0,a_1,\cdots,a_n\right)\right)$$

其中，$a_0,a_1,\cdots,a_n\in\mathbb{Q}$。

注意到当 $a_0,a_1,\cdots,a_n$ 被赋予一组具体的有理数时，有可能得到一个椭圆曲线族。

参数化椭圆曲线族是对定义 1 的进一步推广，在此基础上，可给出构造配对友好曲线的新策略。

对于某嵌入次数 k，若能找到满足引理 1 的参数化多项式 $u\left(x,a_0,a_1,\cdots,a_n\right)=\sum_{i=0}^{\phi(k)-1}u_i\left(a_0,a_1,\cdots,a_n\right)x^i$，则令 $r\left(x,a_0,a_1,\cdots,a_n\right)$ 为 $\Phi_k\left(u\left(x,a_0,a_1,\cdots,a_n\right)\right)$ 的 $\phi(k)$ 次不可约因子(后文若无特殊说明，所有参数化多项式仍看做关于 x 的一元多项式，对它的各种运算都将 x 视为未知元，将 $a_0,a_1,\cdots,a_n$ 视为待定系数)。

由此得到 Frobenius 迹函数的参数化多项式 $t\left(x,a_0,a_1,\cdots,a_n\right)=u\left(x,a_0,a_1,\cdots,a_n\right)+1$，接着根据式(2)计算复乘多项式

$$\begin{aligned}f\left(x,a_0,a_1,\cdots,a_n\right)&=-\left(t\left(x,a_0,a_1,\cdots,a_n\right)-2\right)^2\\&\quad\cdot\bmod r\left(x,a_0,a_1,\cdots,a_n\right)\\&=\sum_{i=0}^{\phi(k)-1}f_i\left(a_0,a_1,\cdots,a_n\right)x^i\end{aligned}\tag{3}$$

最后得到

$$\begin{aligned}&q\left(x,a_0,a_1,\cdots,a_n\right)\\&=\frac{t\left(x,a_0,a_1,\cdots,a_n\right)^2+f\left(x,a_0,a_1,\cdots,a_n\right)}{4}\end{aligned}\tag{4}$$

为满足复乘条件，式(3)中的 $f\left(x,a_0,a_1,\cdots,a_n\right)$ 的高次项系数必须消掉，由此列出关于 $a_0,a_1,\cdots,a_n$ 的方程组

$$\left.\begin{aligned}f_3\left(a_0,a_1,\cdots,a_n\right)&=0\\&\vdots\\f_{\phi(k)-1}\left(a_0,a_1,\cdots,a_n\right)&=0\end{aligned}\right\}\tag{5}$$

将方程组式(5)中 $\mathbb{Q}$ 内的任意解代入 $q\left(x,a_0,a_1,\cdots,a_n\right)$，$t\left(x,a_0,a_1,\cdots,a_n\right)$ 和 $r\left(x,a_0,a_1,\cdots,a_n\right)$，可得到 $\rho\le\dfrac{2\phi(k)-2}{\phi(k)}$ 的参数化族。

以上步骤的关键是构造满足条件的 $u\left(x,a_0,a_1,\cdots,a_n\right)$。借鉴 Tanaka 等人[11]提出的方法，利用同构，构造 $\mathbb{Q}(\zeta_k)=\mathbb{Q}[x]/\Phi_k(x)$，则 $\zeta_k=x$。因此引理 1 的式(1)可以等价表示为：存在 $a(x)\in\mathbb{Q}[x]$，满足 $u(a(x))\equiv x \bmod \Phi_k(x)$。

设 $u(x)=\sum_{i=0}^{\phi(k)-1}u_i'x^i$, $a(x)=\sum_{i=0}^{\phi(k)-1}a_ix^i$，令 $v(x)$ 表示次数小于 $\phi(k)$ 的多项式，且满足 $v(x)\equiv u\left(a(x)\right)\cdot\left(\bmod\ \Phi_k(x)\right)$，则 $v(x)$ 可写成 $\sum_{i=0}^{\phi(k)-1}\sum_{j=0}^{\phi(k)}u_j'v_{ij}x^i$，其中 v_{ij} 是 $a_0,a_1,\cdots,a_{\phi(k)-1}$ 的线性组合。

置 $a_0,a_1,\cdots,a_{\phi(k)-1}$ 为待定系数，得到线性方程组

$$\boldsymbol{V}\begin{pmatrix}u_0'\\u_1'\\u_2'\\\vdots\\u_{\phi(k)-1}'\end{pmatrix}=\begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix}\tag{6}$$

其中，$\boldsymbol{V}$ 是 $\phi(k)\times\phi(k)$ 阶矩阵。

若 $\mathrm{Det}(\boldsymbol{V})\ne0$，说明式(6)在 $\mathbb{Q}\left(a_0,a_1,\cdots,a_{\phi(k)-1}\right)$ 中有唯一解，则 $u(x)$ 的系数可表为多元多项式 $u_i'=u_i\left(a_0,a_1,\cdots,a_{\phi(k)-1}\right)$，其中 $i=0,1,\cdots,(\phi(k)-1)$。于是得到满足条件的参数化多项式 $u\left(x,a_0,a_1,\cdots,a_{\phi(k)-1}\right)=\sum_{i=0}^{\phi(k)-1}u_i\left(a_0,a_1,\cdots,a_{\phi(k)-1}\right)x^i$。

表 1 的算法 1 总结了产生参数化椭圆曲线族的方法。

需要指出的是，并不是任意有理数组 $\left(a_0,a_1,\cdots,a_{\phi(k)-1}\right)$ 代入参数化曲线族后，都能产生合适的曲线族，转化过程可能因如下任一原因失败：

表 1 产生参数化椭圆曲线族

算法 1 产生参数化椭圆曲线族

输入：嵌入次数 k

输出：参数化椭圆曲线族

(1)令 $u(x)=\sum_{i=0}^{\phi(k)-1}u_i'x^i$；

(2)构造关于 $u_0',u_1',\cdots,u_{\phi(k)-1}'$ 的式(6)；

(3)若 $\mathrm{Det}(\boldsymbol{V})\neq 0$，求解方程组(6)，得到唯一解为 $u_i'=u_i\left(a_0,a_1,\cdots,a_{\phi(k)-1}\right)$，其中 $i=0,1,\cdots,(\phi(k)-1)$，则 $u(x)$ 可重新表为 $u\left(x,a_0,a_1,\cdots,a_{\phi(k)-1}\right)=\sum_{i=0}^{\phi(k)-1}u_i\left(a_0,a_1,\cdots,a_{\phi(k)-1}\right)x^i$；

(4)分解多项式 $\Phi_k\left(u\left(x,a_0,a_1,\cdots,a_{\phi(k)-1}\right)\right)$ 得到次数为 $\phi(k)$ 的不可约多项式，置为 $r\left(x,a_0,a_1,\cdots,a_{\phi(k)-1}\right)$

(5)令Frobenius迹函数的参数化多项式为 $t\left(x,a_0,a_1,\cdots,a_{\phi(k)-1}\right)=u\left(x,a_0,a_1,\cdots,a_{\phi(k)-1}\right)+1$；

(6)计算参数化复乘方程 $f\left(x,a_0,a_1,\cdots,a_{\phi(k)-1}\right)$：

$$f\left(x,a_0,a_1,\cdots,a_{\phi(k)-1}\right)=-\left(t\left(x,a_0,a_1,\cdots,a_{\phi(k)-1}\right)-2\right)^2\cdot\mathrm{mod}\,r\left(x,a_0,a_1,\cdots,a_{\phi(k)-1}\right)$$

(7)在有理数域 $\mathbb{Q}$ 内求解式(5)：

对每个解 $\left\{a_0,a_1,\cdots,a_{\phi(k)-1}\right\}=\left\{b_0,\cdots,b_{\phi(k)-1}\right\}$，计算

$$q\left(x,b_0,\cdots,b_{\phi(k)-1}\right)=\frac{t\left(x,b_0,\cdots,b_{\phi(k)-1}\right)^2+f\left(x,b_0,\cdots,b_{\phi(k)-1}\right)}{4}$$

输出参数化椭圆曲线族 $\left(q\left(x,b_0,\cdots,b_{\phi(k)-1}\right),r\left(x,b_0,\cdots,b_{\phi(k)-1}\right),t\left(x,b_0,\cdots,b_{\phi(k)-1}\right)\right)$。

(1)不存在有理数 x，使得 $q(x)$ 表示素数；

(2)复乘多项式 $f(x)$ 是二次的，但首项系数为负。

4 产生 $\phi(k)=4$ 的椭圆曲线族

本节构造若干 $\phi(k)=4$ 的参数化椭圆曲线族。此种情况下，算法 1 中的多项式 $u\left(x,a_0,a_1,a_2,a_3\right)$ 确保 $\Phi_k(u)$ 存在 4 次不可约因子 $r\left(x,a_0,a_1,a_2,a_3\right)$，因此可得到次数为 3 的复乘多项式 $f\left(x,a_0,a_1,a_2,a_3\right)$。故列出的式(5)只有一个方程，即 $f_3\left(a_0,a_1,a_2,a_3\right)=0$。

4.1 $k=5$

根据算法1，本文分别构造 $u\left(x,a_0,a_1,a_2,a_3\right)$，$r\left(x,a_0,a_1,a_2,a_3\right)$ 和 $t\left(x,a_0,a_1,a_2,a_3\right)$，计算参数化复乘多项式 $f\left(x,a_0,a_1,a_2,a_3\right)$，并将式(5)列成式(7)：

$$f_3\left(a_0,a_1,a_2,a_3\right)=2a_1^2a_2-4a_3a_1^2-4a_2a_1a_3+3a_2^2a_1+6a_3^2a_1-a_3^3+3a_3a_2^2-2a_2^3=0\quad(7)$$

式(7)实际上定义了一条有理数域 Q 上的射影椭圆曲线，因此求解它等价于寻找该曲线的有理点。而该曲线秩为 1，说明存在无穷个有理点。利用 Sage 软件，列出了分子、分母界在 20 内的所有点：

$$(-2:1:0),(0:-1/2:1),(0:1:1),(1/20:-2/5:1),(1/6:1/3:1),(1/2:1:0),(1/2:2:1),(1:0:0),(4/3:1/3:1),(7/4:-1/2:1),(5/2:1:1)$$

族 1： 考虑点 $(-2:1:0)$。该点说明 a_1,a_2 和 a_3 存在关系 $\{a_1=-2a_2,a_3=0\}$，代入参数化多项式 u 和 f，得到

$$\begin{aligned}t=&\frac{1}{55a_2^3}\left[-x^3+\left(4a_2+3a_0\right)x^2\right.\\&+\left(-3a_0^2-8a_0a_2-24a_2^2\right)x\\&\left.+\left(24a_2^2a_0+4a_2a_0^2+41a_2^3+a_0^3\right)\right]\\r=&x^4+\left(-a_2-4a_0\right)x^3+\left(a_2^2+3a_0a_2+6a_0^2\right)x^2\\&+\left(9a_2^3-2a_2^2a_0-3a_2a_0^2-4a_0^3\right)x\\&+\left(a_0^4+31a_2^4+a_2^2a_0^2+a_0^3a_2-9a_0a_2^3\right)\\f=&-\frac{x}{a_2}+\frac{a_0-a_2}{a_2}\end{aligned}$$

这是一个复乘多项式次数为 1 的参数化曲线族。

置 $a_0=1,a_2=1$，得到具体曲线族：

$$\begin{aligned}q(x)=&\frac{1}{12100}\left(x^6-14x^5+119x^4-630x^3\right.\\&\left.+2205x^2-7925x+4900\right)\\r(x)=&x^4-5x^3+10x^2+25\\t(x)=&\frac{1}{55}\left(-x^3+7x^2-35x+70\right)\\f(x)=&-x\end{aligned}$$

当 $x\equiv 5,20,37,\cdots,192\,\mathrm{mod}\,220$，$q(x)$ 可表示素数。该曲线族的复乘多项式形为 $-x$，故为可变判别式的曲线族。事实上，任选判别式 D，可做变量替换 $-x=Dy^2$，则复乘多项式为 $f(x)=Dy^2$。若验证 $q\left(-Dy^2\right)$ 表示素数，则得到复乘判别式为 D 的完全族。

族 2： 接着考查点$(1/6:1/3:1)$，说明 a_1,a_2 和 a_3 间存在关系 $\{a_3=6a_1,a_2=2a_1\}$。代入 u 和 f，得到

$$\begin{aligned}t=&\frac{1}{1331a_1^3}\left[-6x^3+\left(18a_0+22a_1\right)x^2\right.\\&+\left(-44a_1a_0+39a_1^2-18a_0^2\right)x\\&\left.+\left(6a_0^3+22a_1a_0^2-39a_1^2a_0+3a_1^3\right)\right]\\r=&x^4+\left(9a_1-4a_0\right)x^3+\left(21a_1^2-27a_1a_0+6a_0^2\right)x^2\\&+\left(139a_1^3-42a_1^2a_0+27a_1a_0^2-4a_0^3\right)x\\&+\left(881a_1^4+a_0^4+21a_1^2a_0^2-139a_1^3a_0-9a_1a_0^3\right)\\f=&\frac{1}{11a_1^2}\left[x^2+\left(-2a_0+2a_1\right)x-\left(2a_1a_0-19a_1^2+a_0^2\right)\right]\end{aligned}$$

置 $a_1=1,a_0=0$，得到曲线族：

$$q(x)=\frac{1}{1771561}\left(9x^6-66x^5+4x^4+420x^3+40676x^2+80584x-764990\right)$$

$$r(x)=x^4+9x^3+21x^2+139x+881$$

$$t(x)=\frac{1}{1331}\left(-6x^3+22x^2+39x+3\right)$$

$$f(x)=\frac{1}{11}\left(x^2+2x-19\right)$$

当 $x\equiv 35,62,68 \bmod 121$ 时，$q(x)$ 可表示素数。因为 $\deg f(x)=2$，这是一个稀疏曲线族。

族 3： 若考查点 $(7/4:-1/2:1)$，则对应关系 $\left\{a_1=\frac{7}{4}a_3, a_2=-\frac{1}{2}a_3\right\}$，由此得到参数化曲线族

$$t=\frac{1}{3025a_3^3}\left[256x^3+\left(-768a_0+992a_3\right)x^2+\left(-1984a_0a_3+3548a_3^2+768a_0^2\right)x+\left(-256a_0^3-3548a_3^2a_0+4129a_3^3+992a_3a_0^2\right)\right]$$

$$r=256x^4+\left(576a_3-1024a_0\right)x^3+\left(1936a_3^2+1536a_0^2-1728a_0a_3\right)x^2+\left(-3872a_3^2a_0-1024a_0^3+1728a_3a_0^2-124a_3^3\right)x+\left(124a_3^3a_0+1231a_3^4+1936a_3^2a_0^2+256a_0^4-576a_3a_0^3\right)$$

$$f=\frac{1}{55}\left(4x+a_3-4a_0\right)\left(4x+21a_3-4a_0\right)$$

置 $a_3=1, a_0=1$，得到曲线族：

$$q(x)=\frac{1}{9150625}\left(16384x^6+28672x^5+311040x^4+429760x^3+2172560x^2+3864872x-1687659\right)$$

$$r(x)=256x^4-448x^3+1744x^2-3292x+2971$$

$$t(x)=\frac{1}{3025}\left(256x^3+224x^2+2332x+1317\right)$$

$$f(x)=\frac{1}{55}(4x+17)(4x-3)$$

当 $x\equiv 37 \bmod 55$ 时，$q(x)$ 可表示素数。这是一个具有可分解复乘多项式的稀疏类。按照文献[20]中分析，若 $f(x)$ 可分解，则利用复乘方法构造曲线时更容易产生出合适的参数，故此类曲线族非常实用。

4.2 $k=8$

首先构造 $u\left(x,a_0,a_1,a_2,a_3\right)$，$r\left(x,a_0,a_1,a_2,a_3\right)$ 和 $t\left(x,a_0,a_1,a_2,a_3\right)$，并计算参数化多项式 $f\left(x,a_0,a_1,a_2,a_3\right)$，则式(5)可列成式(8)形式：

$$f_3\left(a_0,a_1,a_2,a_3\right)=-a_3a_1^2+a_1^2a_2+2a_2^2a_1+a_3^2a_2+a_3^3=0 \tag{8}$$

该椭圆曲线的秩为 0，群结构为 8 阶扭点群，故只有 8 个有理点：

$$(-2:1:0),(-1:0:1),(-1:1:1),(0:-1:1),(0:1:0),(1:-1:1),(1:0:0),(1:0:1)$$

族 4： 选择点 $(0:-1:1)$，则对应关系 $\{a_2=-a_3, a_1=0\}$。将该关系代入 u 和 f，得到

$$t=-\frac{1}{3a_3^3}\left[x^3-\left(2a_3+3a_0\right)x^2-\left(-3a_0^2-3a_3^2-4a_0a_3\right)x-\left(3a_3^2a_0+2a_3a_0^2+2a_3^3+a_0^3\right)\right]$$

$$r=x^4-4a_0x^3+\left(2a_3^2+6a_0^2\right)x^2+\left(-4a_0^3-4a_3^2a_0+4a_3^3\right)x+\left(a_0^4+2a_3^2a_0^2-4a_0a_3^3+2a_3^4\right)$$

$$f=\left(\frac{x-a_0}{a_3}\right)^2$$

若令 $a_3=1/6, a_0=1/3$，则得到曲线族：

$$q(x)=1296x^6-3456x^5+3960x^4-2496x^3+922x^2-190x+17$$

$$t(x)=-72x^3+96x^2-46x+8$$

$$r(x)=72x^4-96x^3+52x^2-12x+1$$

$$f(x)=(6x-2)^2$$

这是一个复乘判别式为 1 的完全族。

4.3 $k=10$

计算 $u\left(x,a_0,a_1,a_2,a_3\right)$，$r\left(x,a_0,a_1,a_2,a_3\right)$ 和 $t\left(x,a_0,a_1,a_2,a_3\right)$，得到参数化复乘多项式 $f\left(x,a_0,a_1,a_2,a_3\right)$，则式(5)可列为

$$f_3\left(a_0,a_1,a_2,a_3\right)=2a_1^2a_2+5a_2^2a_1+2a_3^2a_1+4a_2a_1a_3+a_3a_2^2+a_3^3+2a_2^3=0 \tag{9}$$

该椭圆曲线的秩为 1，说明有无穷多个有理点。类似地，利用 Sage 软件列出射影平面上分子、分母界在 20 内的所有有理点：

$$(-2:1:0),\ (-1/2:0:1),\ (-1/2:1:0),\ (0:-1:1),\ (2/3:-3/2:1),(1:0:0),\ (3/2:-1:1),\ (7/4:-3/2:1),\ (11/6:-3:1),\ (4:-3:1)$$

族 5： 选择点 $(-1/2:1:0)$，计算参数化曲线族为

$$t=\frac{1}{5a_1^2}\left[2x^2+\left(-3a_1-4a_0\right)x+13a_1^2+2a_0^2+3a_1a_0\right]$$

$$r=\left[x^4+\left(-3a_1-4a_0\right)x^3+\left(6a_0^2+9a_1a_0+9a_1^2\right)x^2+\left(-7a_1^3-9a_1a_0^2-4a_0^3-18a_1^2a_0\right)x+\left(a_0^4+9a_1^2a_0^2+7a_1^3a_0+3a_1a_0^3+11a_1^4\right)\right]$$

$$f=\frac{1}{5a_1^2}\left[3x^2+\left(-6a_0-2a_1\right)x+\left(2a_1a_0+7a_1^2+3a_0^2\right)\right]$$

注意到该参数化族的 ρ 值为 1，已达到最优值。事实上，它完全等价于 Freeman 曲线[8]。

取 $a_0=-2/5, a_1=1/5$，可得到和 Freeman 曲线完全相同的形式：

$$q(x)=25x^4+25x^3+25x^2+10x+3$$
$$r(x)=25x^4+25x^3+15x^2+5x+1$$
$$t(x)=10x^2+5x+3$$
$$f(x)=15x^2+10x+3$$

族 6： 选择点 $(2/3:-3/2:1)$，得到参数化曲线族：

$$\begin{aligned}t=&\frac{1}{605a_3^3}\big[-648x^3+\big(2592a_3+1944a_0\big)x^2\\&+\big(-5184a_0a_3-2940a_3^2-1944a_0^2\big)x\\&+\big(2592a_3a_0^2+2940a_3^2a_0+648a_0^3+281a_3^3\big)\big]\\r=&\big[1296x^4+\big(-4104a_3-5184a_0\big)x^3\\&+\big(3276a_3^2+12312a_0a_3+7776a_0^2\big)x^2\\&+\big(2226a_3^3-6552a_3^2a_0-12312a_3a_0^2-5184a_0^3\big)x\\&+\big(331a_3^4-2226a_0a_3^3+3276a_3^2a_0^2\\&+4104a_0^3a_3+1296a_0^4\big)\big]\\f=&\frac{1}{55a_3^2}\big[72x^2+\big(-144a_0-114a_3\big)x\\&-13a_3^2+72a_0^2+114a_0a_3\big]\end{aligned}$$

令 $a_3=1, a_0=0$，得到曲线族：

$$\begin{aligned}q(x)=&\frac{1}{732050}\big(209952x^6-1679616x^5+5264352x^4\\&-7802568x^3+5289732x^2-1205475x-3777\big)\\r(x)=&1296x^4-4104x^3+3276x^2+2226x+331\\t(x)=&\frac{1}{605}\big(-648x^3+2592x^2-2940x+281\big)\\f(x)=&\frac{1}{55}\big(72x^2-114x-13\big)\end{aligned}$$

当 $x\equiv 51 \mod 110$ 时，$q(x)$ 可表示素数。这是一个稀疏族。

4.4 $k=12$

计算参数化多项式 $u\big(x,a_0,a_1,a_2,a_3\big)$，$r\big(x,a_0,a_1,a_2,a_3\big), t\big(x,a_0,a_1,a_2,a_3\big)$，得到参数化多项式 $f\big(x,a_0,a_1,a_2,a_3\big)$，则式(5)可表示成

$$\begin{aligned}f_3\big(a_0,a_1,a_2,a_3\big)=&-a_3a_1^2+a_2a_1^2+a_1a_2a_3+2a_2^2a_1\\&-2a_3^2a_1+a_2a_3^2+a_3a_2^2=0\end{aligned}\tag{10}$$

该椭圆曲线的秩为 0，只有 8 个有理点：

$$(-2:0:1),(-2:1:0),(-2:1:1),(-1/2:-1:1),$$
$$(0:-1:1),(0:0:1),(0:1:0)-(1:0:0)$$

族 7： 选择点 $(-1/2:-1:1)$，得到参数化族：

$$\begin{aligned}t=&\frac{1}{15a_1^3}\big[2x^3-\big(6a_0+2a_1\big)x^2+\big(4a_1a_0+6a_0^2+19a_1^2\big)x\\&-\big(2a_0^2a_1+2a_0^3+19a_1^2a_0+13a_1^3\big)\big]\\r=&x^4+\big(-4a_0-4a_1\big)x^3+\big(15a_1^2+6a_0^2+12a_1a_0\big)x^2\\&+\big(-30a_1^2a_0-40a_1^3-4a_0^3-12a_0^2a_1\big)x\\&+\big(37a_1^4+40a_1^3a_0+4a_1a_0^3+a_0^4+15a_1^2a_0^2\big)\\f=&\frac{1}{3a_1^2}\big(x-a_1-a_0\big)^2\end{aligned}$$

令 $a_1=1, a_0=0$，得到曲线族：

$$\begin{aligned}q(x)=&\frac{1}{225}\big(x^6-2x^5+20x^4-32x^3\\&+122x^2-161x+61\big)\\r(x)=&x^4-4x^3+15x^2-40x+37\\t(x)=&\frac{1}{15}\big(2x^3-2x^2+19x-13\big)\\f(x)=&3\left(\frac{x-1}{3}\right)^2\end{aligned}$$

当 $x\equiv 13 \mod 15$ 时，$q(x)$ 可表示素数。这是一个复乘判别式为 3 的完全族。

5 结束语

在设计基于配对的密码方案时，考虑到安全性、效率、应用背景等因素，需要使用各种类型的配对友好椭圆曲线族。虽然目前已有多种构造方法，但绝大多数都依赖于穷尽搜索，且只能构造特定类型的族。本文提出一种构造配对友好椭圆曲线族的新方法，通过把“族”的定义扩展到“参数化族”，将寻找曲线问题转化为解方程，避免了穷尽搜索，从而使寻找过程更加高效。据此设计出具体算法，给出了寻找曲线族的新框架。作为应用，使用该算法寻找 $\phi(k)=4$ 的椭圆曲线族，找出 7 组实用的族，囊括了曲线族的所有类型，包括完全族、可变判别式的完全族和稀疏族。且据我们所知，族 7 之前从未被发现过。我们希望这种构造曲线的思想可作为启发，用于寻找更多的新的配对友好椭圆曲线族。

参 考 文 献

[1] MENEZES A J, OKAMOTO T, and VANSTONE S A. Reducing elliptic curve logarithms to logarithms in a finite field[J]. *IEEE Transactions on Information Theory*, 1993, 39(5): 1639–1646. doi: 10.1109/18.259647.

[2] JOUX A. A one round protocol for tripartite Diffie-Hellman[J]. *Journal of Cryptology*, 2004, 17(4): 385–393. doi: 10.1007/s00145-004-0312-y.

[3] BONEH D and FRANKLIN M K. Identity-based encryption

from the Weil pairing[C]. International Cryptology Conference on Advances in Cryptology, Springer-Verlag, 2001: 213–229.

[4] PATERSON K G. ID-based signatures from pairings on elliptic curves[J]. *Electronics Letters*, 2002, 38(18): 1025–1026.

[5] GOPAL P V S S N and Reddy P V. Efficient ID-based key-insulated signature scheme with batch verifications using bilinear pairings over elliptic curves[J]. *Journal of Discrete Mathematical Sciences & Cryptography*, 2015, 18(4): 385–402. doi: 10.1080/09720529.2014.1001586.

[6] ROBERT O. On Constructing families of pairing-friendly elliptic curves with variable discriminant[C]. Progress in Cryptology-Indocrypt 2011, International Conference on Cryptology in India, Chennai, India, 2011: 310–319.

[7] FOTIADIS G and KONSTANTINOU E. More sparse families of pairing-friendly elliptic curves[C]. Cryptology and Network Security, Springer International Publishing, 2014: 384–399.

[8] FREEMAN D, SCOTT M, and TESKE E. A taxonomy of pairing-friendly elliptic curves[J]. *Journal of Cryptology*, 2010, 23(2): 224–280. doi: 10.1007/s00145-009-9048-z.

[9] LE D P, MRABET N E, and TAN C H. On near prime-order elliptic curves with small embedding degrees[C]. Algebraic Informatics. Springer International Publishing, 2015: 140–151.

[10] LEE H S and PARK C M. Constructing pairing-friendly curves with variable CM discriminant[J]. *Bulletin of the Korean Mathematical Society*, 2012, 49(1): 75–88. doi: 10.4134/BKMS.2012.49.1.075.

[11] TANAKA S and NAKAMULA K. Constructing pairing-friendly elliptic curves using factorization of cyclotomic polynomials[C]. Pairing-Based Cryptography-Pairing 2008, Second International Conference, Egham, UK, 2008: 136–145.

[12] YOON K. A new method of choosing primitive elements for Brezing-Weng families of pairing- friendly elliptic curves[J]. *Journal of Mathematical Cryptology*, 2015, 9(1):1–9.

[13] LEE H S and LEE P R. Families of pairing-friendly elliptic curves from a polynomial modification of the Dupont-Enge-Morain method[J]. *Applied Mathematics & Information Sciences*, 2016, 10(2): 571–580. doi: 10.18576/amis/100218.

[14] YASUDA T, TAKAGI T, and SAKURAI K. Constructing pairing-friendly elliptic curves using global number fields[C]. Third International Symposium on Computing and Networking, 2015: 477–483.

[15] OKANO K. Note on families of pairing-friendly elliptic curves with small embedding degree[J]. *JSIAM Letters*, 2016: 61–64. doi: 10.14495/jsiaml.8.61.

[16] LI L. Generating pairing-friendly elliptic curves with fixed embedding degrees[J]. *Science China Information Sciences*, 2017, 60(11): 119101. doi: 10.1007/s11432-016-0412-0.

[17] ATKIN A O L and MORAIN F. Elliptic curves and primality proving[J]. *Mathematics of Computation*, 1997, 61(203): 29–68. doi: 10.1090/S0025-5718-1993-1199989-X.

[18] GALBRAITH S D, MCKEE J F, and VALENCA P C. Ordinary abelian varieties having small embedding degree[J]. *Finite Fields & Their Applications*, 2007, 13(4): 800–814. doi: 10.1016/j.ffa.2007.02.003.

[19] ZHANG M, HU Z, and XU M. On constructing parameterized families of pairing-friendly elliptic curves with\rho=1[C]. International Conference on Information Security and Cryptology, Springer, Cham, 2016: 403–415.

[20] FOTIADIS G and KONSTANTINOU E. On the efficient generation of generalized MNT elliptic curves[C]. Algebraic Informatics, Springer Berlin Heidelberg, 2013: 147–159.

张　猛：　男，1982 年生，博士，研究方向为密码和信息安全.

徐茂智：　男，1962 年生，教授，研究方向为密码和信息安全.

胡　志：　男，1985 年生，博士，研究方向为密码和信息安全.

侯　英：　女，1971 年生，高级工程师，研究方向为高性能计算和信息安全.