More constructing pairing-friendly elliptic curves for cryptography

Tanaka Satoru and Nakamula Ken

Department of Mathematics and Information Sciences, Tokyo Metropolitan University,
1-1 Minami Osawa, Hachioji-shi, Tokyo, 192-0397 Japan
satoru@tnt.math.metro-u.ac.jp, nakamula@tnt.math.metro-u.ac.jp

Abstract. The problem of constructing elliptic curves suitable for pairing applications has received a lot of attention. To solve this, we propose a variant algorithm of a known method by Brezing and Weng. We produce new families of parameters using our algorithm for pairing-friendly elliptic curves of embedding degree 8, and we actually compute some explicit curves as numerical examples.

1 Introduction

Researches on pairing-based cryptographic schemes have received interest over the past few years. Recently many new and novel protocols have been proposed as in [13, 4, 5, 10]. A randomly chosen elliptic curve, however, rarely has a subgroup of large prime order, therefore construction of "pairing-friendly" elliptic curves is one of the important problems for cryptography [2].

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, and r be the largest prime dividing $\#E(\mathbb{F}_q) = q + 1 - t$, the order of the group of $\mathbb{F}_q$-rational points of E with the Frobenius trace t. We define the *embedding degree* by the smallest positive integer k such that r divides $q^k - 1$. The parameters required to determine pairing-friendly elliptic curves are t, r, q, k and the CM discriminant D for the CM method introduced in [1] to construct elliptic curves.

In this paper, we study the problem of computing suitable parameters t, r, q from given parameters k, D. We employ the method proposed in [7, 6] which generates a family of pairing-friendly curves by considering t, r, q as polynomial $t(x), r(x), q(x)$ of a new parameter x. We restrict the embedding degree to $k = 8$ and the CM discriminant to $D = 1$. The key point is how to choose a good $r(x)$. Instead of taking $r(x)$ to be the ℓth cyclotomic polynomial $\Phi_\ell(x)$ with a multiple ℓ of k, we modified the original method by starting from a finite subset of the k-th cyclotomic field $\mathbb{Q}(\zeta_k)$ with a primitive kth root ζ_k of unity so that $r(x)$ can be systematically computable. As a result, we came up with new families of pairing-friendly curves which are given explicitly in Table 1 and Theorem 5 of Section 3. We also give, for the first time in this case so far as we know, explicit numerical results as in Examples 1–3.

This paper is organized as follows. Section 2 gives a brief mathematical definition of curves suitable for pairing-based cryptography and the method of construction we used to generate our curves. In Section 3 we give our algorithm to construct curves. Section 4 gives numerical examples of curves that we generate using our parameters. Finally, we will discuss the conclusions that we will draw from our approach in Section 5.

2 Our framework of pairing-friendly curves

A survey on the construction of pairing-friendly elliptic curves is given by Freeman et al. [7]. We introduce several essential definitions from that paper to explain our algorithm. We will use the same notation there without notice. Let lg mean the base 2 logarithm in the following.

2.1 Families of curves for pairing

At first, we give the definition of pairing-friendly elliptic curves used in cryptography.

Definition 1 ([7, Definition 2.3]). Suppose E is an elliptic curve defined over $\mathbb{F}_q$. We say that E is *pairing-friendly* if E satisfies the following conditions:

(1) there is a prime $r \geq \sqrt{q}$ such that $r \mid \#E(\mathbb{F}_q)$.
(2) the embedding degree of E with respect to r is less than $(\lg r)/8$.

For cryptographic applications of pairings, basically we desire enough security depending on the *elliptic curve discrete logarithm problem* (*ECDLP*). In fact, by this definition, suitable sizes of r, q^k seem to avoid any known attack for the ECDLP today [7].

Next, we explain how to construct pairing-friendly curves. The parameter q has to be a prime power. If a family of pairing-friendly curves represented by $t(x), r(x)$ and $q(x)$ is given, we anticipate that $q(x)$ is a prime power for infinitely many x. Freeman et al. gave a definition with a familiar conjecture as follows [7, Section 2].

Definition 2. Let $f(x)$ be a polynomial with rational coefficients. We say f *represents primes* if the following conditions are satisfied.

(1) $f(x)$ is non-constant and irreducible.
(2) $f(x)$ has positive leading coefficient.
(3) $f(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$.
(4) $\gcd(\{f(x) \mid x, f(x) \in \mathbb{Z}\}) = 1$.

We use this definition to define families of pairing-friendly curves.

Definition 3 ([7, Definition 2.6]). For a given positive integer k and positive square-free integer D, the triple (t, r, q) *represents a family of elliptic curves with embedding degree k and discriminant D* if the following conditions are satisfied:

(1) $q(x) = p(x)^d$ $(d \geq 1)$ and $p(x)$ that represents primes.
(2) $r(x) = c \cdot \tilde{r}(x)$ $(c \in \mathbb{Z}_{\geq 1})$ and $\tilde{r}(x)$ that represents primes.
(3) $r(x) \mid q(x) + 1 - t(x)$.
(4) $r(x) \mid \Phi_k(t(x) - 1)$, where Φ_k is the kth cyclotomic polynomial.
(5) The CM equation $4q(x) - t(x)^2 = Dy^2$ $(D \in \mathbb{Z}_{>0})$ has infinitely many integer solutions (x, y).

For a family $(t(x), r(x), q(x))$, if the CM equation in (5) has a suitable set of integer solutions (x_0, y_0) with both of $p(x_0)$ and $\tilde{r}(x_0)$ are primes, then we are able to construct curves E over $\mathbb{F}_{q(x_0)}$ where $E(\mathbb{F}_{q(x_0)})$ has a subgroup of order $\tilde{r}(x_0)$ and embedding degree k with respect to $\tilde{r}(x_0)$ by using the CM method in [1].

We therefore define a parameter ρ that represent how close to the ideal curve that is $\#E(\mathbb{F}_q)$ is prime as follows.

Definition 4 ([7, Definition 2.7]).

(1) Let $E/\mathbb{F}_q$ be an elliptic curve, and suppose E has a subgroup of order r. The *ρ-value of E (with respect to r)* is

$$\rho(E) = \frac{\log q}{\log r}.$$

(2) Let $t(x), r(x), q(x) \in \mathbb{Q}[x]$, and suppose (t, r, q) represents a family of elliptic curves with embedding degree k. The *ρ-value of the family represented by (t, r, q)* is

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

By Definition 1, a pairing-friendly curve E has $\rho(E) \leq 2$. The smaller the ρ-value, the faster the computation of points on elliptic curve (See [7, Section 1.1]). On the other hand, the Hasse bound implies that $\rho(t, r, q)$ is always at least 1. Finding parameters efficiently with the same bit size of r and q, hence $\rho(E)$ is close to 1, is one of the important problems for cryptography.

2.2 Original method

In this section, we briefly explain the construction of curves satisfying the condition of Definition 3 proposed by Brezing and Weng [6][7, Section 6.1].

Theorem 1. *Fix a positive integer k and a positive square-free integer D. Execute the following steps:*

Step 1. *Choose a number field K containing a primitive kth root of unity ζ_k and $\sqrt{-D}$.*
Step 2. *Find an irreducible polynomial $r(x) \in \mathbb{Z}[x]$ such that $\mathbb{Q}[x]/(r(x)) \cong K$.*
Step 3. *Let $t(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $\zeta_k + 1 \in K$.*

Step 4. *Let* $y(x) \in \mathbb{Q}[x]$ *be a polynomial mapping to* $(\zeta_k - 1)/\sqrt{-D} \in K$. *(So, if we discover a polynomial* $s(x) \in \mathbb{Q}[x]$ *mapping to* $\sqrt{-D} \in K$, *then* $y(x) \equiv (2 - t(x))s(x)/D \pmod{r(x)}$.*)*

Step 5. *Let* $q(x) = (t(x)^2 + Dy(x)^2)/4$.

If both of $r(x)$ *and* $q(x)$ *represent primes, then the triple* (t, r, q) *represents a family of curves with embedding degree* k *and CM discriminant* D.

The ρ-value for this family is

$$\rho(t, r, q) = \frac{2\max\{\deg t(x), \deg y(x)\}}{\deg r(x)} < 2.$$

For more details, refer to [7, Section 6.1]. To find a family of pairing-friendly elliptic curves efficiently, we have to choose a good $r(x)$ satisfying $\zeta_k, \sqrt{-D} \in K$. The idea by Brezing, Weng and also Freeman et al. is as follows. Choose an integer multiple ℓ of k so that $\sqrt{-D} \in K = \mathbb{Q}(\zeta_\ell)$. Then let $r(x) = \Phi_\ell(x)$. They further give some sporadic families [7, Section 6.2]. Our idea given explicitly below is to construct such sporadic curves systematically.

3 Proposed algorithm

3.1 Factorization of cyclotomic polynomial

When we use the original method to construct families, the problem is how to choose polynomials at Step 2 and 3 in Theorem 1. If $\Phi_k(u(x))$ has a factorization over $\mathbb{Q}$ for some $u(x) \in \mathbb{Q}[x]$, we let $r(x)$ be one of the irreducible factors. Set $K = \mathbb{Q}[x]/(r(x))$ and we will get $u(x) \mapsto \zeta_k$. But these factorizations are rare, so this technique to construct families is called "Sporadic" families by Freeman [7, §6.2].

One of the technique to find such $u(x)$ was discussed in Galbraith, Mckee and Valença by proving an important lemma below [8, Lemma 1]. Baretto and Naehrig [3] found a family of embedding degree 12 and $u(x)$ is a quadratic polynomial with $\rho(t, r, q) = 1$ using this lemma. It was restricted to quadratic polynomials $u(x)$. In fact, it is effective for general case as is easily seem from the proof there:

Lemma 1. *Let* $u(x) \in \mathbb{Q}[x]$ *and* φ *be Euler function. Then, the polynomial* $\Phi_k(u(x))$ *has an irreducible factor of degree* $\varphi(k)$ *if and only if the equation*

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

has a solution in $\mathbb{Q}(\zeta_k)$.

We rediscover families of elliptic curves by Freeman[7, Example 6.18] using Lemma 1 and we try to construct new families of curves. We propose an algorithm for the construction of a family of curves using Lemma 1 and Theorem 1. The algorithm is as follows.

Algorithm 2.

Input Positive integers D, k such that $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$ and a finite subset $S \subset \mathbb{Q}(\zeta_k)$.
Output Families of elliptic curves with parameters $t(x), r(x), q(x)$.

Step 1. For each $\omega \in S$, compute $u(x) \in \mathbb{Q}[x]$ such that the equation (1) has a root $x = \omega$. If $u(x)$ does not exist for all ω, then the algorithm fails.
Step 2. For each $u(x)$ at Step 1, compute all irreducible factors $r(x)$ of the polynomial $\Phi_k(u(x))$.
Step 3. For each pair of $u(x), r(x)$ at Step 2, compute all polynomials $t(x) \in \mathbb{Q}[x]$ such that $\deg t(x) < \deg r(x)$ and $t(x) \equiv u(x)^m + 1 \pmod{r(x)}$ for all m with $1 \leq m < k, \gcd(m, k) = 1$.
Step 4. For each pair of $r(x), t(x)$ at Step 3, execute Step 4 and Step 5 of Theorem 1 to compute $q(x)$.
Step 5. For each triple $r(x), t(x), q(x)$ at Step 4, check whether $q(x), r(x)$ represent primes. If $q(x), r(x)$ represent primes, output a family $t(x), r(x), q(x)$.

3.2 Algorithm refinement with method of indeterminate coefficients

Let $\deg u(x) = 3$ as the case $\deg u(x) \leq 2$ is studied in [8]. Set the embedding degree to $k = 8$. In Step 1 of Algorithm 2, we employ the method of indeterminate coefficients to compute $u(x)$. This technique is also applicable for general k.

Write any rational cubic polynomial $u(x)$ with coefficients u_0, u_1, u_2, u_3 as follows:

$$u(x) = \sum_{i=0}^{3} u_i x^i = u_3 x^3 + u_2 x^2 + u_1 x + u_0 \quad (u_i \in \mathbb{Q}, u_3 \neq 0). \tag{2}$$

We represent a given value $\omega \in \mathbb{Q}(\zeta_8)$ as follows:

$$\omega = \sum_{i=0}^{3} a_i {\zeta_8}^i = a_0 + a_1\zeta_8 + a_2{\zeta_8}^2 + a_3{\zeta_8}^3 \quad (a_i \in \mathbb{Q}). \tag{3}$$

To avoid operation in $\mathbb{Q}(\zeta_8)$, we replace ζ_8 to x to get the following polynomial.

$$\omega(x) = \sum_{i=0}^{3} a_i x^i = a_3 x^3 + a_2 x^2 + a_1 x + a_0.$$

Next we look at polynomial $u(\omega(x))$. The equation (1) is equivalent to $u(\omega(x)) \equiv x \pmod{\Phi_8(x)}$. We take

$$v(x) \equiv u(\omega(x)) \pmod{\Phi_8(x)}$$

be the simplified polynomial of degree not exceeding three with coefficients expressed in terms of u_i, a_i. The equation (1) is transformed to the polynomial equation

$$v(x) = x. \tag{4}$$

We can easily show that the coefficients of the left hand side of the equation are all represented as linear combinations of u_i. More precisely, it is reduced to solve the following system of linear equations to obtain u_0, u_1, u_2, u_3.

$$A \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \tag{5}$$

where

$$A = \begin{pmatrix} 1 & a_0 & {a_0}^2 - {a_2}^2 - 2a_1a_3 & {a_0}^3 - 3a_2(a_0a_2 + {a_1}^2 - {a_3}^2) - 6a_0a_1a_3 \\ 0 & a_1 & 2a_0a_1 - 2a_2a_3 & {a_3}^3 - 3a_1(a_1a_3 + {a_2}^2 - {a_0}^2) - 6a_0a_2a_3 \\ 0 & a_2 & {a_1}^2 - {a_3}^2 + 2a_0a_2 & -{a_2}^3 + 3a_0(a_0a_2 + {a_1}^2 - {a_3}^2) - 6a_1a_2a_3 \\ 0 & a_3 & 2a_1a_2 + 2a_0a_3 & {a_1}^3 - 3a_3(a_1a_3 + {a_2}^2 - {a_0}^2) + 6a_0a_1a_2 \end{pmatrix}.$$

Let d and n_i be as follows:

$$\begin{aligned} d &:= ({a_1}^2 + {a_3}^2)((a_1 - a_3)^2 + 2{a_2}^2)((a_1 + a_3)^2 - 2{a_2}^2), \\ n_0 &:= -a_2(5{a_1}^4a_3 - 5{a_1}^3{a_2}^2 + 5a_1{a_2}^2{a_3}^2 - 2{a_2}^4a_3 + 3{a_3}^5), \\ n_1 &:= {a_1}^5 - 4{a_1}^3{a_3}^2 + 9{a_1}^2{a_2}^2a_3 + a_1(2{a_2}^4 + 3{a_3}^4) + 3{a_2}^2{a_3}^3, \\ n_2 &:= {a_1}^3a_2 + 3a_1a_2{a_3}^2 - 2{a_2}^3a_3, \\ n_3 &:= {a_3}^3 - {a_1}^2a_3 + 2a_1{a_2}^2. \end{aligned} \tag{6}$$

If d is nonzero, then we can solve the system (5). The solution is

$$\begin{cases} u_0 = -\left(n_3{a_0}^3 + n_2{a_0}^2 + n_1a_0 - n_0\right)/d \\ u_1 = \left(3n_3{a_0}^2 + 2n_2a_0 + n_1\right)/d \\ u_2 = -\left(3n_3a_0 + n_2\right)/d \\ u_3 = -n_3/d \end{cases}. \tag{7}$$

We now have a concrete solution for $k = 8$ with $\deg u(x) = 3$. Although this method of indeterminate coefficients can be used for any embedding degree k, it is not sure wheter the obtained solution is as simple as the ones we discussed. We present the following theorem as a resut of the solutions we computed.

Theorem 3. *For $\omega \in \mathbb{Q}(\zeta_8)$ given by (3), let d, n_i be as in (6). Then, if and only if both d and n_3 are nonzero, the equation (1) has a solution $x = \omega$ for a cubic polynomial $u(x) \in \mathbb{Q}[x]$, which is uniquely determined by (7) and (2). For this $u(x)$, at least one irreducible quartic polynomial is a factor of $\Phi_8(u(x))$.*

For a cubic polynomial $u(x)$ given by Theorem 3, we take an irreducible quartic factor $r(x)$ from the factorization of $\Phi_8(u(x))$. If we let $t(x) \equiv u(x)^{2n+1} + 1 \pmod{r(x)}$ $(0 \leq n \leq 3)$, then Step 3 of Algorithm 2 are finished. We continue the computation under the assumption that $k = 8$ and $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$. We can choose the CM discriminant $D = 1$. Then we take $s(x) = (t(x) - 1)^2 \mapsto \sqrt{-1}$ and execute Steps 4, 5 in Algorithm 2 to get a family of curves.

We now state the refinement of Algorithm 2 with restricted to our special case:

Algorithm 4. Let $k = 8, D = 1, \deg u(x) = 3$.

Input A finite subset $S \subset \mathbb{Q}(\zeta_8)$.
Output Families of elliptic curves with parameters $t(x), r(x), q(x)$.

Step 1. For each $\omega \in S$, compute d, n_i by the equation (6), and let $S' = \{\omega \in S \mid d \neq 0, n_3 \neq 0\}$. If S' is an empty set, then the algorithm fails.
Step 2. For each $\omega \in S'$, compute $u(x)$ by the equations (7) and (2).
Step 3. For each $u(x)$ of Step 2, compute all irreducible factors $r(x)$ of the polynomial $\Phi_8(u(x))$.
Step 4. For each pair $u(x), r(x)$ of Step 3, compute all polynomials $t(x) \in \mathbb{Q}[x]$ such that $\deg t(x) < \deg r(x)$ and $t(x) \equiv u(x)^m + 1 \pmod{r(x)}$ for all $m = 1, 3, 5, 7$.
Step 5. Compute $y(x) \equiv (2 - t(x))(t(x) - 1)^2 \pmod{r(x)}$ $(\deg y(x) < \deg r(x))$.
Step 6. Let $q(x) = (t(x)^2 + y(x)^2)/4$.
Step 7. For each triple $r(x), t(x), q(x)$ at Step 6, check whether $q(x), r(x)$ represent primes. If $q(x), r(x)$ represent primes, output a family $t(x), r(x), q(x)$.

3.3 Examples

Table 1. Sporadic families generate from cubic $u(x)$ with embedding degree 8

lc (u)	$u(x)$	$t(x)$	$\deg r(x)$	$\deg q(x)$	$\rho(t, r, q)$
2	$\mathbf{2x^3 + 4x^2 + 6x + 3}$	$\mathbf{u(x)^3 + 1}$	**4**	**6**	**3/2**
9	$9x^3 + 3x^2 + 2x + 1$	$u(x)^5 + 1$	4	6	3/2
17	$17x^3 + 32x^2 + 24x + 6$	$u(x)^3 + 1$	4	6	3/2
18	$18x^3 + 39x^2 + 31x + 7$	$u(x)^3 + 1$	4	6	3/2
64	$64x^3 + 112x^2 + 75x + 18$	$u(x)^5 + 1$	8	14	7/4
68	$68x^3 + 110x^2 + 65x + 15$	$u(x)^5 + 1$	4	6	3/2
82	$\mathbf{82x^3 + 108x^2 + 54x + 9}$	$\mathbf{u(x)^5 + 1}$	**4**	**6**	**3/2**
144	$144x^3 + 480x^2 + 539x + 202$	$u(x)^5 + 1$	8	14	7/4
144	$144x^3 + 96x^2 + 29x + 2$	$u(x)^5 + 1$	8	14	7/4
216	$216x^3 + 372x^2 + 263x + 69$	—	—	(†)	—
225	$225x^3 + 2x$	—	—	(†)	—
257	$257x^3 + 256x^2 + 96x + 12$	$u(x)^3 + 1$	4	6	3/2
388	$388x^3 + 798x^2 + 561x + 134$	$u(x)^5 + 1$	4	6	3/2
392	$392x^3 + 980x^2 + 821x + 231$	$u(x)^5 + 1$	8	14	7/4
450	$450x^3 + 11x$	—	—	(†)	—
626	$\mathbf{626x^3 + 500x^2 + 150x + 15}$	$\mathbf{u(x)^5 + 1}$	**4**	**6**	**3/2**
738	$\mathbf{738x^3 + 1488x^2 + 1006x + 229}$	$\mathbf{u(x)^5 + 1}$	**4**	**6**	**3/2**
800	$800x^3 + 9x$	$u(x)^5 + 1$	8	14	7/4
873	$873x^3 + 969x^2 + 379x + 53$	$u(x)^7 + 1$	4	6	3/2

In Table 1 We give a result of computations of the polynomial $u(x)$ by MAGMA [11] using Algorithm 4. The heading $\mathrm{lc}\,(u)$ denotes the leading coefficient of $u(x)$. We choose the input $S = \{\omega \in \mathbb{Q}(\zeta_8) \mid \omega = \sum_{i=0}^{3} a_i x^i,\ a_i \in \mathbb{Z},\ 0 \leq a_i \leq 300\}$. In the actual computation to make polynomial coefficients small, we further transform $u(x)$ obtained by Step 2 of Algorithm 4 to $u(ax+b) \in \mathbb{Z}[x]$ with suitable $a, b \in \mathbb{Q}, a \neq 0$. After computation by MAGMA, we tried to construct families for $\lg \mathrm{lc}\,(u) < 10$. We explain the symbols in Table 1. For the column $\deg q(x)$, the symbol (†) denotes that $q(x)$ does not *represent primes* for all pair $t(x)$, $r(x)$. For rows, the **bold notation** means that there exists a family of curves such that both $q(x)$ and $r(x)$ are primes for many integers x.

We discovered many pairing-friendly families of curves with $\rho = 3/2$ and also rediscovered a family which has $\mathrm{lc}\,(u) = 9$ by Freeman et al. [7, Example 6.18]. It is interesting to note that for $\mathrm{lc}\,(u) = 2$, 82, 626, 738, both $q(x)$ and $r(x)$ are primes for (infinitely) many integers x. We describe the case where $\mathrm{lc}\,(u) = 82$ in detail as follows.

Theorem 5. *The polynomials $t(x)$, $r(x)$, $q(x) \in \mathbb{Z}[x]$ given as follows represent a family of elliptic curves with embedding degree $k = 8$ and the CM discriminant $D = 1$. This family indeed generates pairing-friendly elliptic curves.*

$$\begin{aligned} t(x) &= -82x^3 - 108x^2 - 54x - 8 \\ r(x) &= 82x^4 + 108x^3 + 54x^2 + 12x + 1 \\ q(x) &= 379906x^6 + 799008x^5 + 705346x^4 \\ &\quad +333614x^3 + 88945x^2 + 12636x + 745 \end{aligned}$$

Proof. The former half is already proved by Algorithm 4, so we only need to prove the latter half. We may verify both $q(x_0)$ and $r(x_0)$ are primes with some integer x_0. We take $x_0 = 104$, then we get $q(x_0) = 490506332802458249$ and $r(x_0) = 9714910817$. Both of these are primes, so we can generate pairing-friendly curves by them. □

From a family of curves, we can actually construct pairing-friendly curves. Find an integer x such that $q(x)$ is a prime and check whether $r(x)$ is a prime. To find such an integer x, we can reduce the number of the candidate by the chinese remainder theorem.

Lemma 2. *If an integer $q(x)$ in Theorem 5 is a prime, then $x \equiv 14, 24 \pmod{30}$.*

Proof. We can easily check that all $q(x)$ is even if x is odd. We see that

$$q(x) \equiv x^6 + 3x^5 + x^4 + 4x^3 + x \pmod 5.$$

So $q(x) \equiv 0 \pmod 5$ if $x \not\equiv 4 \pmod 5$. In the same way we see that

$$q(x) \equiv x^6 + x^4 + 2x^3 + x^2 + 1 \pmod 3.$$

So $q(x) \equiv 0 \pmod 5$ if $x \not\equiv 1 \pmod 3$. Then by the Chinese remainder theorem, $q(x)$ has no prime factor $2, 3$ and 5 only if $x \equiv 14, 24 \pmod{30}$. □

4 Examples of pairing-friendly curves

By Theorem 5, we can generate pairing-friendly curves using [12, Theorems 3,4]. The elliptic curve $E/\mathbb{F}_q$ with the CM discriminant $D = 1$ is represented as

$$E : Y^2 \equiv X^3 + aX \pmod{q} \quad (a \neq 0)$$

where a is parameter. Since t is always divided by 4 from the form of $t(x)$ in Theorem 5, we can easily compute a by the method described in [12]. Using this, we give some numerical examples.

Example 1. For $x = 24000000000010394$ ($\lg x \approx 54.4$), we get

$$\begin{aligned}
q &= 726011672004446604951703464791789328991217313776602768811\\
&\quad 505320697581567547878422987036476401963225900 69,\\
r &= 272056320000471307161600306182614014808404525177076771934\\
&\quad 82845476817 \quad (224\text{-bit}),\\
t &= -113356800000147285043200063789391713609209096429 1460,\\
\#E(\mathbb{F}_q) &= 726011672004446604951703464791789328991217313776602780147\\
&\quad 185320712310071867884801926207837322872868815 30,\\
a &= 363005836002223302475851732395894664495608656888301384405\\
&\quad 752660348790783773939211493518238200981612950 35.
\end{aligned}$$

Then $\lg r \approx 224.0$, $\lg q \approx 345.0$ and $\rho(E) \approx 1.54$.

Example 2. For $x = 6130400000000029634$ ($\lg x \approx 62.4$), we get

$$\begin{aligned}
q &= 201655015390974685980897990123384483374976 85\\
&\quad 268073419312994695960148519299615127959281 95\\
&\quad 249643154463102416170215935678 9,\\
r &= 115816144321490890478327891899665854763905 03\\
&\quad 326918594658592037634937230763121 7 \quad (256\text{-bit}),\\
t &= -188921023622423219740582163008443944151642 9\\
&\quad 1734047019380020,\\
\#E(\mathbb{F}_q) &= 201655015390974685980897990123384483374976 85\\
&\quad 268073419312994714852250881541937102017498 25\\
&\quad 334082595979531589574917873681 0,\\
a &= 100827507695487342990448995061692241687488 42\\
&\quad 634036709656497347980074259649807563979640 97\\
&\quad 624821577231551208085107967839 52.
\end{aligned}$$

Then $\lg r \approx 256.0$, $\lg q \approx 393.0$ and $\rho(E) \approx 1.54$.

Example 3. For $x = -72057594037930756$ ($\lg x \approx 56.0$), we get

$$\begin{aligned}
q &= 53180779126375041342927679012516474003955785403827730100050941212371435046023372666628598916049952969199369,\\
r &= 2210715626706698491377041180063927762099958931722603805474805907424817 \quad (230\text{-bit}),\\
t &= 306798423708539154983403942081629850761644294779940640,\\
\#E(\mathbb{F}_q) &= 53180779126375041342927679012516474003955785403827730069371098841517519547682978458465613839885523491204730,\\
a &= 17726926375458347114309226337505491334651928467942576700016980404123811682007790888876199638683317656399790.
\end{aligned}$$

Then $\lg r \approx 230.4$, $\lg q \approx 354.5$ and $\rho(E) \approx 1.54$. For the Ate pairing [9], it is important that t has a low hamming weight for computation. We tried to find a curve with r between 224 bit and 256 bit, we found that r has a Hamming weight 72 and t has a Hamming weight 45 in this example.

5 Conclusion

We proposed a new algorithm for systematically constructing families of elliptic curves with given embedding degree and the CM discriminant. It was shown to be efficient by producing actual families of curves and explicit numerical examples for the case of embedding degree 8. The key point is employing the method of indeterminate coefficients to choose polynomials. Obviously our method of indeterminate coefficients are also applicable to the general case.

References

[1] Atkin, A.O.L., Morain, F.: Elliptic curve and primarity proving. Math. Comp. **61**(203) (1993) 29–68.

[2] Balasubramanian, R., Koblitz, N.: The improbability that an elliptic curve has subexponential discrete log problem under the menezes-okamoto-vanstone algorithm. Journal of Cryptology **11**(2) (1998) 141–145.

[3] Barreto, P.S.L.M., Naehrig, M.: Pairing-friendly elliptic curves of prime order. In: SAC2005 - Workshop on Selected Areas in Cryptography. Volume 3897 of Lecture Notes in Computer Science., Springer (2006) 319–331.

[4] Boneh, D., Franklin, M.: Identity based encryption from the weil pairing. SIAM Journal of Computing **32**(3) (2003) 586–615.

[5] Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. In: Advances in Cryptology - AsiaCRYPT 2001. Volume 2248 of Lecture Notes in Computer Science., Springer (2001) 514–532.

[6] Brezing, F., Weng, A.: Elliptic curves suitable for pairing based cryptography. Designs, Code and Cryptography **37**(1) (2005) 133–141.

[7] Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. preprint (2006). http://math.berkeley.edu/ dfreeman/papers/taxonomy.pdf.
[8] Galbraith, S., Mckee, J., Valença, P.: Ordinary abelian varieties having small embedding degree. In: Workshop on Mathematical Problems and Techniques in Cryptology, Barcelona, CRM (2005) 29–45.
[9] Hess, F., Smart, N., Vercauteren, F.: The eta pairing revisited. Cryptology ePrint Archive, Report 2006/110 (2006). http://eprint.iacr.org/2006/110/.
[10] Joux, A.: A one round protocol for tripartite diffie-hellman. Journal of Cryptology **17**(4) (2004) 263–276.
[11] MAGMA Group: Magma computational algebra system. http://magma.maths.usyd.edu.au.
[12] Morain, F.: Primality proving using elliptic curves: An update. In: ANTS 1998 - 3rd Algorithmic Number Theory Symposium. Volume 1423 of Lecture Notes in Computer Science., Springer (1998) 111–127.
[13] Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairing. In: 2000 Symposium on Cryptography and Information Security (SCIS2000). (2000).