Special Polynomial Families for Generating More Suitable Elliptic Curves for Pairing-Based Cryptosystems

Pu Duan, Shi Cui and Choong Wah Chan

School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore
dp@pmail.ntu.edu.sg
cuishi@pmail.ntu.edu.sg
ecwchan@ntu.edu.sg

Abstract

Constructing non-supersingular elliptic curves for pairing-based cryptosystems have attracted much attention in recent years. The best previous technique builds curves with $\rho = lg(q)/lg(r) \approx 1$ ($k = 12$) and $\rho = lg(q)/lg(r) \approx 1.25$ ($k = 24$). When $k > 12$, most of the previous works address the question by representing $r(x)$ as a cyclotomic polynomial. In this paper, we propose a new method to find more pairing-friendly elliptic curves with arbitrary embedding degree k by certain special polynomial families. The new method generates curves with $lg(q)/lg(r) \approx 1$ ($k \geq 48$) by random forms of $r(x)$. Different representations of $r(x)$ allow us to obtain many new families of pairing-friendly elliptic curves. In addition, we propose a equation to illustrate how to obtain small values of ρ by choosing appropriate forms of discriminant D and trace t. Numerous parameters of certain pairing-friendly elliptic curves are presented with support for the theoretical conclusions.

Keywords: *pairing-friendly elliptic curves, special polynomial families, cyclotomic polynomials*

1. Introduction

After the propositions of identity-based encryption scheme [12] and short signature scheme [13], paring-based cryptography has attracted significant attention in modern public-key cryptography. Over pairing-based cryptosystems, Elliptic Curve Discrete Logarithm Problem (ECDLP) on supersingular elliptic curves can be reduced to Discrete Logarithm Problem (DLP) over an extension field by Weil Pairing [10] or Tate Paring [15]. Although supersingular elliptic curves provides high efficiency for pairing-based cryptosystems [19, 20], since these curves only can be built when

embedding degree k ≤ 6 [11], researchers have explored other form of curves, e.g. non-supersingular elliptic curves.

In 2001, Miyaji, Nakabayashi and Takano [8] first proposed a method to find suitable non-supersingular elliptic curves for pairing-based cryptosystems. They discussed the problem from the point of view of tract t. Scott and Barreto [1] extended the method of Miyaji *et al.* and found more suitable non-supersingular elliptic curves when $k \in [3, 4, 6]$. Gallbraith, Mckee and Valenca [3] summarized the method proposed by early researchers and presented some appropriate families of group orders of such elliptic curves when embedding degree $k \leq 6$. Duan, Cui and Chan [5] extended the work of Gallbraith *et al*. by proposing the idea of effective polynomial families of pairing-friendly elliptic curves.

For larger values of k, Brezing and Weng proposed an alternative method to find these curves [7]. They used $t - 1$ as a kth root of unity modulo prime r. They generated the curves with best performance so far as $lg(q)/lg(r) = 1.25$ ($k = 24$). Dupont, Enge and Morain [16] proposed another method for finding the suitable non-supersingular elliptic curves. Most of the curves they found had $lg(q)/lg(r) \approx 2$. In their method, tract t was chosen large enough to make $4q - t^2$ small as to produce effective values of D. Barreto and Naehrig [17] generated non-supersingular elliptic curves with $lg(q)/lg(r) = 1$ when embedding degree $k = 12$. They presented the best curves with prime group order known so far. Their work was actually generated by a special polynomial family of $q(x)$, $t(x)$ and $r(x)$, where $4q(x) - t^2(x)$ can be factorized as one square polynomial multiplying with one constant number. In the most recent work, Murphy and Fitzpatrick [4] extended the work of Brezing *et al*. and generated pairing-friendly elliptic curves over prime fields with discriminant $D > 4$ for arbitrary values of k.

In this paper we propose a new method for finding more pairing-friendly elliptic curves. Compared to the previous works, we explicitly present the special polynomial families for generating elliptic curves suitable for pairing-based cryptosystmes with arbitrary values of embedding degree k. We also illustrate the relation to obtain small values of ρ by choosing appropriate forms of discriminant D, trace t and embedding degree k. Our method allows to find more pairing-friendly elliptic curves with higher security ($k \geq 48$) and more efficiency ($\rho \leq 1.2$) by various representations of $r(x)$. In fact, the work of Brezing *et al*. [17] and Murphy *et al*. [4] can be represented as a special case of our new method, since they implement $r(x)$ only as cyclotomic polynomials in their work.

This paper is organized as the follows. In Sections 2 we give a description of the mathematics background. In Section 3 we present the new method and discuss the difference compared with previous works. In Section 4 certain special polynomial families of pairing-friendly elliptic curves with random forms of $r(x)$ and arbitrary embedding degree k are presented. In addition, we propose the idea to construct

curves with $\rho = lg(q)/lg(r) \approx 1$ for large values of $k \geq 48$. We draw the conclusion in Section 5. The parameters of some pairing-friendly elliptic curves, based on the proposed polynomial families, are presented in Appendix (a), (b), (c) and (d) over prime fields.

2. Mathematics Background

To find suitable elliptic curves for pairing-based cryptosystems, we need to solve certain equations. Assume the cofactor h is an integer, r is the order of a point as a big prime number and t is the trace of an elliptic curve, we want to find an elliptic curve over $\boldsymbol{F}_q$, where $q = p$ is a prime number (we only consider the prime fields in this paper). ECDLP on such elliptic curves can be reduced to DLP over $\boldsymbol{F}_q^k$, where k is the smallest integer satisfying certain conditions, defined as the embedding degree [1]. The following equations determine whether such an elliptic curve exists or not.

In a strict sense, to find the suitable elliptic curves for pairing-based cryptosystems [10], we need

$$r \mid q^k - 1 \tag{1}$$

However, under a mild condition [6], we just consider q as a kth root of unity modulo r [7]. Meanwhile, since k is the smallest integer satisfying $r \mid q^k - 1$, equation (1) should be presented as $r \mid q^k - 1$ and $q^i - 1$ is not divisible by r when $0 < i < k$. From [14] we have

$$dr = \Phi_k(q) \tag{2}$$

where d is an integer and $\Phi_k(q)$ is the cyclotomic polynomial of q with embedding degree k and

$$d'r \neq \Phi_i(q),\ 0 < i < k \tag{3}$$

Besides these conditions we need

$$hr = q + 1 - t \tag{4}$$

where h is an integer. Combining equation (2) and (4) together, we obtain

$$sr = \Phi_k(t - 1) \tag{5}$$

where s is also an integer [1]. Since k is the smallest integer, we have

$$s'r \neq \Phi_i(t - 1),\ 0 < i < k \tag{6}$$

By Hasse's bound we need

$$|t| \leq 2q^{1/2} \tag{7}$$

With all the above equations, we compute the elliptic curve by solving

$$DV^2 = 4q - t^2 \tag{8}$$

where D is chosen by certain conditions [2].

All the above equations aim for finding suitable elliptic curves for pairing-based cryptosystems in integer fields. But it is impossible to search the whole integer fields to obtain the suitable solutions. We should transfer the problem into polynomial fields. When analyzing in polynomial fields, we assume q, t, r as $q(x)$, $t(x)$ and $r(x)$;

meanwhile h, d, s, D and V should be considered as $h(x)$, $d(x)$, $s(x)$, $D(x)$ and $V(x)$. Duan *et al*. [5] have proposed a lemma which illustrates the fact that in polynomial fields, equation (2) and (5) are already both sufficient and necessary conditions. Thus for finding suitable elliptic curves for pairing-based cryptosystems in polynomial fields, the equations (2, 4, 5, 7, 8) are required and rewritten as:

$$d(x)r(x) = \Phi_k(q(x)) \quad (9)$$

$$h(x)r(x) = q(x) + 1 - t(x) \quad (10)$$

$$s(x)r(x) = \Phi_k(t(x) - 1) \quad (11)$$

$$|t(x)| < 2q(x)^{1/2} \quad (12)$$

$$D(x)V(x)^2 = 4q(x) - t^2(x) \quad (13)$$

How to build pairing-friendly elliptic curves by finding the polynomial families satisfying equation (9) to (13) were presented in [1, 3, 5, 8, 17]. Most of the work concentrated on embedding degree $k \leq 6$. Only one special polynomial family whe $k = 12$ was found by Barreto *et al*. [17], which built the best curves with prime group order known so far.

For larger values of k, the polynomial families of $q(x)$, $t(x)$ and $r(x)$ will not satisy all the conditions from equation (9) to (13). Only some of the parameters will maintain the polynomial relations and the other ones will only be valid for certain x as x_0. Brezing and Weng [7] proposed a method to find these curves. In their method, in polynomial fields, $t(x)$ and $r(x)$ will satisfy equation (11) by representing $t(x) - 1$ as a kth root of unity modulo $r(x)$. The irreducible polynomial $r(x)$ is always set as a cyclotomic polynomial. q and DV^2 will not have the polynomial relations. They can not be represented as polynomials in cyclotomic fields. But all the parameters are satisfying equations (9) - (13) for a specific x_0. In the next section, we will present a new method for finding more pairing-friendly elliptic curves with arbitrary embeddin degree k by some special polynomial families. The new method allows $r(x)$ to be an irreducible polynomial with different forms.

3. A New Method for Producing More Pairing - Friendly Elliptic Curves with Special Polynomial Families

In this section the math evidence for the new method is provided. As proposed in [7], from equation (4) and (8), difference between $4q$ and t^2 can be obtained after finding t and r:

$$DV^2 = 4q - t^2 = 4(hr + t - 1) - t^2 \quad (14)$$

Represented in polynomial fields, equation (16) can be rewritten as

$$DV^2(x) = 4h(x)r(x) - (t(x) - 2)^2 \quad (15)$$

where D is a square-free integer. This is a standard polynomial family of pairing-friendly elliptic curves proposed in [1, 3, 5, 8, 17] with the satisfaction to equation (9) - (13). In polynomial fields, choose $r(x)$ and $t(x)$ as

$$s(x)r(x) = \Phi_k(t(x) - 1)$$

This can be viewed as

$$r(x) \mid \Phi_k(t(x) - 1) \quad (16)$$

We should mention that polynomial families are hard to find for large values of k (e.g. $k > 12$) when equation (15) is satisfied. To find more curves, we choose suitable $r(x)$ and $t(x)$ satisfying equation (16). Then for a specific x_0, assuming equation (15) is satisfied, this can be presented as

$$DV^2(x_0) = 4h(x_0)r(x_0) - (t(x_0) - 2)^2 \quad (17)$$

Dividing D from both sides of equation (17), we have

$$V^2(x_0) = [4h(x_0)r(x_0) / D] - [t(x_0) - 2]^2 / D \quad (18)$$

where $4h(x_0)r(x_0)$ and $[t(x_0) - 2]^2$ divides D. Assuming $[t(x_0) - 2]^2 \mid 4Dh(x_0)$, equation (18) can be rewritten as

$$V^2(x_0) = \{[t(x_0) - 2]^2 / D^2\}\{[4Dh(x_0)r(x_0) / (t(x_0) - 2)^2] - D\} \quad (19)$$

Here we use a technique to consider $4Dh(x_0)/ (t(x_0) - 2)^2$ as a polynomial $h'(x)$ for certain x_0. This means for a specific x_0, $4Dh(x_0)$ divides $[t(x_0) - 2]^2$ and it can be represented in polynomial fields as a polynomial $h'(x)$. Then equation (19) can be represented as

$$V^2(x_0) = \{[t(x_0) - 2]^2 / D^2\}\{h'(x)r(x) - D\} \quad (20)$$

Thus if $h'(x)r(x) - D$ can be viewed as a square polynomial $S^2(x)$, in equation (20) all parameters have square forms. If $h'(x)r(x) - D = S^2(x)$, for any suitable x_0, equation (20) is satisfied and can be written as

$$V^2(x_0) = \{[t(x_0) - 2]^2 / D^2\}S^2(x) \quad (21)$$

This equation represents a modified polynomial family. For the specific x_0, we have

$$DV^2(x_0) = \{[t(x_0) - 2]^2 / D\}S^2(x_0) \quad (22)$$

Representing equation (14) into equation (22), we obtain

$$q = [t^2(x_0) + DV^2(x_0)] / 4 \quad (23)$$

We choose x_0 as to satisfy that $r(x_0)$ is a prime integer. Then for the specific x_0, if $q = [t^2(x_0) + DV^2(x_0)] / 4$ is a prime integer, we find all the suitable parameters with satisfaction to a pairing-friendly elliptic curve.

The main idea can be presented as the following procedures. First we choose a specific $r(x)$ and trace polynomial $t(x)$ with $r(x) \mid \Phi_k(t(x) - 1)$. Then after choosing a suitable discriminant D, we find polynomial families $h'(x)$ satisfying that $h'(x)r(x) - D = S^2(x)$ as a square polynomial. In the following steps, we choose a suitable x_0 with $r(x_0)$ is a prime integer and test whether $q = \{t^2(x_0) + [(t(x_0) - 2)^2 / D]S(x_0)\} / 4$ is also a prime integer. Is q is according to the conditions, we have found the suitable parameters of a pairing-friendly elliptic curves. In the procedure, $4Dh(x_0) / (t(x_0) - 2)^2 = h'(x)$, $D \mid 4h(x_0)$ and $D \mid [t(x_0) - 2]^2$ are three hidden conditions since we represent $h'(x)$ as a polynomial.

The main step in the new method is to find a suitable discriminant D and special polynomial families $h'(x)$, $r(x)$, $S(x)$ with $h'(x)r(x) - D = S^2(x)$. The other work to test prime $r(x_0)$ and $q(x_0)$ is trivial. When $r(x)$ is taken as a standard cyclotomic polynomial, finding suitable $S(x)$ is equal to find the polynomial representations of $(-D)^{1/2}$ in cyclotomic fields. This is because

$$S^2(x) + D \equiv 0 \bmod r(x) \tag{24}$$

In such circumstances, our method is same with the methods proposed by Brezing and Weng [7] since equation (24) can be rewritten as

$$DV^2(x) = \{[t(x) - 2]^2 / D\}S^2(x) \tag{25}$$

where $S(x)$ is the representation of $(-D)^{1/2}$ in cyclotomic fields. This equation is same as the main relation proposed in [7]. Thus the work of Brezing *et al*. is a special case of our new method since in their method $r(x)$ is only taken as a standard cyclotomic polynomial. Our proposed method ignores the restrictions imposed on the form of $r(x)$. By our method more pairing-friendly elliptic curves are found by various forms of $r(x)$.

Based on the above analysis, we propose a new algorithm for finding the suitable pairing-friendly elliptic curves.

Algorithm 1

Input: embedding degree k, $q^k \geq 2^{1024}$ and $r \geq 2^{160}$

Output: x_0, $q(x_0)$, $t(x_0)$, $r(x_0)$, $DV^2(x_0)$

1. Choose an irreducible polynomial $r(x)$.
2. Compute trace polynomial $t(x)$ by $\Phi_k(t(x) - 1) \equiv 0 \bmod r(x)$.
3. Choose a polynomial family $h'(x)$ and a suitable discriminant D with $h'(x)r(x) - D = S^2(x)$, where $S^2(x)$ is a square polynomial.
4. Find a specific x_0 with $r(x_0)$ is a prime integer and $q(x_0) = \{t^2(x_0) + S^2(x_0)\ [(t(x_0) - 2)^2 / D]\ \} / 4$ is also a prime integer.
5. Output x_0, $q(x_0)$, $t(x_0)$, $r(x_0)$, $DV^2(x_0)$
6. Establish the elliptic curve by CM method with the above parameters.
7. If no suitable parameters are found, repeat from step 1

Because the key procedure of the new method is to find special polynomial families $h'(x)$, $r(x)$ and $S^2(x)$, in the next section we will list some polynomial families with different embedding degree k, $\rho = lg(q)/lg(r)$ and $r(x)$.

4. Special Polynomial Families for Producing More Pairing - Friendly Elliptic Curves

In this section we will present some special polynomial families obtained by the new method. These families can be used to generate more pairing-friendly elliptic curves

with different forms of $r(x)$, small values of ρ and arbitrary values of embedding degree k.

4.1 Special Polynomial Families with Small Values of ρ

The new method indicates that the value of ρ is related to the choice of $r(x)$, $t(x)$ and $h'(x)$. It is because $\rho = lg(q)/lg(r) = degree(q(x)) / degree(r(x))$. Since $DV^2(x_0) = \{[t(x_0) - 2]^2 / D\}\{h'(x)r(x) - D\}$, we have $degree(q(x)) = degree(DV^2(x)) \approx 2degree(t(x)) + degree(h'(x)) + degree(r(x))$. Thus the value of $\rho = degree(q(x)) / degree(r(x)) = [2degree(t(x)) + degree(h'(x)) + degree(r(x))] / degree(r(x)) = 1 + [2degree(t(x)) + degree(h'(x))] / degree(r(x))$. It is to say that ρ will always be larger than 1. This can also be deduced from the conditions used in the new method. Since we assume $[t(x_0) - 2]^2 \mid 4Dh(x_0)$ in the algorithm, when $\rho = 1$, $h(x)$ will be a constant integer as h. Then $[t(x_0) - 2]^2 \mid 4Dh$ will not be satisfied since $|t^2(x_0)| > 4Dh$. When the degree of $h'(x)$ is 0 ($h'(x)$ is a constant number), ρ has the smallest values as $1 + 2degree(t(x)) / degree(r(x))$. Thus for finding ρ close to 1, $h'(x)$ should be chosen as a constant number and $t(x)$ should be chosen with smallest degrees.

Table 1 presents all the different special polynomial families when embedding degree $k \in [12, 14, 15, 16]$ over cyclotomic fields. All the results satisfy the nice representations of $(-D)^{1/2}$ in the work of Murphy and Fitzpatrick [4].

	h'(x)	r(x)	D	$S^2(x)$	t(x)	ρ
k = 12	$x^2 + 1$	$\Phi_{12}(x)$	1	x^6	x + 1	2
k = 12	4	$\Phi_{12}(x)$	3	$(2x^2 - 1)^2$	x + 1	1.5
k = 14	$4x^2 + 4x + 8$	$\Phi_{14}(x)$	7	$(2x^4 + 2x^2 - 2x + 1)^2$	x + 1	1.66
k = 15	$4x^2 + 4x + 4$	$\Phi_{15}(x)$	3	$(2x^5 + 1)^2$	x + 1	1.5
k = 15	$4x^6 + 4x^5 - 4x^4 + 8x^3 + 4x^2 + 24$	$\Phi_{15}(x)$	15	$(2x^7 - 2x^5 + 4x^4 - 2x^3 + 2x^2 + 4x - 3)$	x + 1	2

Table 1: Special polynomial families when $k = 12, 14, 15$

In Table 2 we tabulate all the possible special polynomial families when $k = 28$. When $r(x)$ is fixed as a cyclotomic polynomial with embedding degree k, $h'(x)$ and $t(x)$ should be chosen with smallest degrees. Thus $t(x)$ always should be taken as $x + 1$ if $r(x) = \Phi_k(x)$. Although in cyclotomic fields we can modulo $S^2(x_0)[t(x_0) - 2)]^2 / D$ by $\Phi_k(x_0)$ to a smaller integer; from the deductions of section 3 we can find that the best choice is still to set $t(x)$ as $x + 1$. Murphy *et al*. [4] implemented $t(x)$ as $x^3 + 1$ with standard cyclotomic polynomial $r(x)$ when $k = 28$. They found the elliptic curves with $\rho \approx 1.8$. We will present some pairing-friendly elliptic curves when $k = 15, 28$ in Appendix (a). These curves have smaller values of ρ compared to the work of Murphy *et al*. [4] when representing $t(x)$ as $x + 1$.

	h'(x)	r(x)	D	$S^2(x)$	t(x)	ρ
k = 28	$x^2 + 1$	$\Phi_{28}(x)$	1	x^{14}	x + 1	1.3

k = 28	$4x^4 + 4x^2 + 8$	$\Phi_{28}(x)$	7	$(-2x^8 - 2x^4 + 2x^2 - 1)^2$	x + 1	1.5

Table 2: Special polynomial families when $k = 12, 14, 15$

Brezing *et al*. [7] and Murphy *et al*. [4] have implemented $r(x)$ as $\Phi_{ik}(x)$ for a given embedding degree k, where i is an integer. In fact, such techniques can not obtain elliptic curves with smaller values of ρ. First we analyze the situation when k is an even number. When $r(x)$ is taken as $\Phi_{ik}(x)$, we have $degree(r(x)) = degree(\Phi_{ik}(x)) = i \times degree(\Phi_k(x))$; meanwhile, we have $i \times degree(t(x))$ and $i \times degree(h'(x))$. Thus the value of ρ is not related to the choice of cyclotomic polynomials since the degrees of $r(x)$, $t(x)$ and $h'(x)$ are increased with same multiples. When k is an odd number, the analysis is similar. Brezing *et al*. [7] have found the best curves with $\rho \approx 1.25$, $k = 24$. They took $r(x)$ as $\Phi_{48}(x)$ and $t(x)$ as $x^2 + 1$. In Table 3, we tabulate some polynomial families when $k = 24$ which illustrates that $\rho \approx 1.25$ is also obtained for $k = 24$ when $t(x) = x + 1$, $r(x) = \Phi_{24}(x)$. These polynomial families prove that the value of ρ has no relation with the choice of the degrees of $\Phi_k(x)$ and $t(x)$.

	h'(x)	r(x)	D	$S^2(x)$	t(x)	ρ
k = 24	4	$\Phi_{24}(x)$	3	$(2x^4 - 1)^2$	x + 1	1.25
k = 24	4	$\Phi_{48}(x)$	3	$(2x^8 - 1)^2$	$x^2 + 1$	1.25
k = 24	$x^2 + 2$	$\Phi_{24}(x)$	2	$(x^5 + x^3 - x)^2$	x + 1	1.5
k = 24	$x^4 + 2$	$\Phi_{48}(x)$	2	$(x^{10} + x^6 - x^2)^2$	$x^2 + 1$	1.5

Table 3: Special polynomial families when $k = 24$

4.2 Special Polynomial Families with Arbitrary Values of *k*

As finding the special polynomial families, we notice a fact which can be implemented to construct pairing-friendly elliptic curves with arbitrary embedding degree k. When k is an even integer, $\Phi_{sk}(x)$ will have the same form as $\Phi_k(x)$ where $s = 2^i$ (i is a positive integer). The only difference is that x in $\Phi_k(x)$ will be represented as x^s in $\Phi_{sk}(x)$. Meanwhile, $h'(x)$ will also have the same property. Thus if we find a special polynomial family for embedding degree k, we can easily obtain the families with the same forms for embedding degree sk ($s = 2^i$). The only work is to represent x as x^s, where s is a positive integer power of 2.

The beauty of this property is to find curves with larger embedding degree k with smaller ρ. It is because $\rho = 1 + [2degree(t(x)) + degree(h'(x))] / degree(r(x))$. When degree of $r(x)$ is increased with same multiples of $h'(x)$, if the degree of $t(x)$ is not changed, the value of ρ will be decreased. When $h'(x)$ is a constant integer, the situations are more easily to analyze. Since if we always choose $t(x)$ as $x + 1$, the values of ρ equals $1 + [2 / degree(r(x))]$. By choosing larger values of embedding degree k, the degree of $r(x)$ will increase, then the value of ρ will be decreased (but it can not reach 1 for ever).

Koblitz and Menezes [18] have suggested to find pairing-friendly elliptic curves

with $k = 2^i 3^j$ as large as possible. In Table 4, we tabulate the polynomial families when $k = 12, 24, 48, 96$. The value of ρ is decreased close to *1* when taking larger values of k. Since in these families the value of h is always *4*, the small values of ρ is obtained when $k = 96$. When $k = 48$, we construct the parameters of certain paring-friendly elliptic curves with $\rho \approx 1.125$. When $k = 96$, we construct the parameters of certain paring-friendly elliptic curves with $\rho \approx 1.06$. These curves have better performance compared to previous works, since they have smaller values of ρ for larger values of k. The results are presented in Appendix (b).

	h'(x)	r(x)	D	$S^2(x)$	t(x)	ρ
k = 12	4	$\Phi_{12}(x)$	3	$(2x^2 - 1)^2$	x + 1	1.5
k = 24	4	$\Phi_{24}(x)$	3	$(2x^4 - 1)^2$	x + 1	1.25
k = 48	4	$\Phi_{48}(x)$	3	$(2x^8 - 1)^2$	x + 1	1.12
k = 96	4	$\Phi_{96}(x)$	3	$(2x^{16} - 1)^2$	x + 1	1.06

Table 4: More special polynomial families when $k = 12, 24, 48, 96$

With this technique we could find any pairing-friendly elliptic curves with arbitrary embedding degree k, e.g. finding curves with larger k than *96* is not a hard task. But since the suitable values of x become sparse when k is increased, finding parameters of elliptic curves with the essential security level (r is a *160* bits prime) [9] is more difficult with large k. This is the reason we find the parameters of an elliptic curve with r as a *416* bits prime integer when $k = 96$. In addition, it is still not aware how large the embedding degree k should be for a pairing-friendly curve with best performance. (To find curves with prime r close to *160* bits integer for larger values of k, e.g. $k = 96$, we should use some other techniques. This question will be further discussed in section 4.4.)

4.3 Special Polynomial Families with Different Forms of *r(x)*

Brezing and Weng [7] had successfully found pairing-friendly elliptic curves with arbitrary embedding degree. But the limitation of their work was that *r(x)* was only represented as the standard cyclotomic polynomial. It was because their method was to derive kth roots of unity and polynomial representations of $(-D)^{1/2}$ in the cyclotomic fields. They did not provide any explanations to the circumstances when *r(x)* was taken as an arbitrary irreducible polynomial. The work of Murphy and Fitzpatrick [4] was also based on the standard representations of *r(x)* as $\Phi_k(x)$.

Our method ignores the limitation imposed on the forms of *r(x)* since we only need to find $h'(x)$ and D with $h'(x)r(x) - D = S^2(x)$. For this point, *r(x)* can be any irreducible polynomials satisfying $r(x) \mid \Phi_k(t(x) - 1)$. This allows us to find much more ellitpc curves by various representations of *r(x)*. In Table 5 we tabulate more special polynomial families with different *r(x)* when $k = 12, 14$ and *28*. The trace *t(x)* is taken

with degree as small as possible to obtain desired values of ρ. In Appendix (c) we generate certain parameters of pairing-friendly elliptic curves by the polynomial families listed in Table 5.

k	r(x)	t(x)	D	ρ
12	$2197x^4 - 1352x^3 + 299x^2 - 28x + 1$	$13x - 1$	3	1.5
14	$20511149x^6 - 30413083x^5 + 18803919x^4 - 6205739x^3 + 1153069x^2 - 114381x + 4733$	$29x - 6$	7	1.67
14	$x^{12} + x^{11} - x^9 - x^8 + x^6 - x^4 - x^3 + x + 1$	$x^3 + 1$	3	1.67
28	$x^{24} + x^{22} - x^{18} - x^{16} + x^{12} - x^8 - x^6 + x^2 + 1$	$x^3 + 1$	3	1.4

Table 5: More special polynomial families with different *r(x)* when *k = 12*, *14*, *28*

Table 5 just tabulates some new polynomial families of different *r(x)* when *k = 12*, *14* and 28. When the irreducible polynomial *r(x)* is not limited as a cyclotomic polynomial, more values of the discriminant *D* will be suitable for generating pairing-friendly elliptic curves. Appendix (c) presents parameters of curves with *D = 3* when embedding degree *k = 14* and *28*. Such curves have not been proposed in any relative works before. By the new method, more polynomial families can be found for other values of *k*. It is no way to list all the special polynomial families with various values of embedding degree *k*. Table 6 presents such special polynomial families with different forms of *r(x)* when *k = 13*, *14* and *15*. These new polynomial families will be implemented for finding much more pairing-friendly elliptic curves.

k	r(x)	t(x)
13	$x^{22} - 11x^{20} + 56x^{18} - 173x^{16} + 359x^{14} - 524x^{12} + 548x^{10} - 410x^8 + 215x^6 - 75x^4 + 16x^2 - 1$	x^2
13	$x^{22} + 11x^{20} + 56x^{18} + 173x^{16} + 359x^{14} + 524x^{12} + 548x^{10} + 410x^8 + 215x^6 + 75x^4 + 16x^2 + 1$	$-x^2$
14	$343x^6 - 343x^5 + 147x^4 - 49x^3 + 21x^2 - 7x + 1$	$7x^2 + 1$
14	$343x^6 + 343x^5 + 147x^4 + 49x^3 + 21x^2 + 7x + 1$	$7x^2 + 1$
15	$81x^8 + 81x^7 + 54x^6 + 27x^5 + 9x^4 + 9x^3 + 6x^2 + 3x + 1$	$-3x^2 + 1$
15	$625x^8 + 625x^7 + 250x^6 + 125x^5 + 75x^4 + 25x^3 + 10x^2 + 5x + 1$	$5x^2 + 1$
15	$50625x^8 + 50625x^7 + 27000x^6 + 10125x^5 + 2925x^4 + 675x^3 + 120x^2 + 15x + 1$	$-15x^2 + 1$

Table 6: More special polynomial families with different *r(x)* when *k = 13*, *14*, *15*

4.4 More *r* with a small factor

In fact, when it is allowed that *r* contains a small factor *s* as *r = sn* (*n* is a prime larger than 2^{160}), much more suitable elliptic curves are found. The same technique has been used in [1]. When $r = s \times n$, *n* should be a large prime bigger than 2^{160} [9] and cofactor *h* will be multiplied with the small factor *s*. Brezing *et al*. [7] and Murphy *et al*. [4] only implemented *r* as a large prime in their methods. By our method it is easy to find that the condition of prime *r(x)* can be loosed to *r = sn* without effecting the values of ρ much. Thus more elliptic curves different with their work are found. The value of ρ will not increase much if *s* is carefully chosen. In Appendix (d), we

presented some examples with this technique when $k = 96$. By this technique, we effectively decrease the length of r.

5. Conclusion

In this paper, we propose a new method to find more pairing-friendly elliptic curves with arbitrary embedding degree k by certain special polynomial families. This method allows us to obtain new families of pairing-friendly elliptic curves by representing $r(x)$ with various forms. In addition, we propose a new technique to let prime r contain a small factor s. Numerous parameters of new pairing-friendly elliptic curves are found with the proposed method. These curves have higher security ($k \geq 48$) and more efficiency ($\rho \leq 1.2$) compared to the previous work for paring-based cryptosystems.

Reference

[1] M. Scott and P. S. L. M. Barreto. Generating more MNT elliptic curves. Cryptology ePrint Archive, Report 2004/058, 2004.

[2] IEEE Computer Society, New York, USA. IEEE Standard Specifications for Public Key Cryptography- IEEE Std 1363-2000, 2000.

[3] S. D. Galbraith, J. Mckee and P. Valenca. Ordinary abelian varieties having small embedding degree. Cryptology ePrint Archive, Report 2004/365, 2004.

[4] A. Murphy and N. Fitzpatrick. Elliptic curves for pairing applications. Cryptology ePrint Archive, Report 2005/302, 2005.

[5] P. Duan, S. Cui and C. W. Chan. Effective polynomial families for generating more pairing-friendly elliptic curves. Cryptology ePrint Archive, Report 2005/236, 2005.

[6] R. Balasubramanian and N. Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. Journal of Cryptology, vol. 11, pp. 141- 145, 1998.

[7] F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. Cryptology ePrint Archive, Report 2003/143, 2003.

[8] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. IEICE Transactions on Fundamentals, E84-A(5):1234-1243, 2001.

[9] A. M. Odlyzko. Discrete logarithms: the past and the future. Design, Codes and Cryptography, 19:129-145, 2000.

[10] A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. Proc.22nd Annual ACM Symposium on the Theory of Computing, pp. 80-89, 1991.

[11] D. Page, N. P. Smart and F. Vercauteren. A comparison of MNT curves and supersingular curves. Cryptology ePrint Archive, Report 2004/165, 2004.

[12] D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. SIAM Journal. of Computing, vol. 32, no.3, pp. 586-615, 2003.

[13] D. Boneh, B. Lynn and H. Shacham. Short signatures from the Weil pairing. Advances in Cryptology – Asiacrypt'2001, volume 2248 of Lecture Notes in Computer Science, page 514-532, Springer-Verlag, 2002.

[14] P. S. L. M. Barreto, B. Lynn, and M. Scott. Constructing elliptic curves with prescribed embedding degrees. In Security in Communication Networks – SCN'2002, volume 2576 of Lecture Notes in Computer Science, pages 263 – 273. Springer-Verlag, 2002.

[15] G. Frey, M. Muller and H. G Ruck. The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems. IEEE Transactions on Information Theory, Vol 45, 1999.

[16] R. Dupont, A. Enge, and F. Morain. Building curves with arbitrary small MOV degree over finite prime fields. Journal of Cryptology, 18(2): 79-89, 2005.

[17] P. S. L. M. Barreto and M. Naehrig. Pairing-Friendly Elliptic Curves of Prime Order. Cryptology ePrint Archive, Report 2005/133, 2005.

[18] N. Koblitz and A. Menezes. Pairing-based cryptography at high security levels. Cryptography ePrint Archive, Report 2005/076, 2005.

[19] S. Galbraith, K. Harrison and D. Soldera. Implementing the Tate pairing. In Algorithm Number Theory Symposium – ANTS V, volume 2369 of Lecture Notes in Computer Science, pages 324 – 337. Springer – Verlag, 2002.

[20] P. S. L. M. Barreto, H. Y. Kim, B. Lynn and M. Scott. Efficient algorithms for pairing-based cryptosystems. In Advances in Cryptology – Crypto' 2002, volume 2442 of Lecture Notes in Computer Science, pages 354-368. Springer-Verlag, 2002.

Appendix

(a) Special Polynomial Families with Small Values of ρ

(1) k = 15, $\rho \approx 1.5$
$S(x)^2 = 4x^{10} + 4x^5 + 1 = (2x^5 + 1)^2$, D = 3, $h'(x) = 4x^2 + 4x + 4$, $r(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$; $t = x + 1$

x = 962542
r = 736812625806875488411619464155914329720828004251 (160 bits)
t = 962543
q = 21082111624242378127392870715467849117003034307261239000753006319008248 1
$DV^2 = 3 \times 530183762158522770519556331457747855^2$

x = 963691
r = 743878444107727695162122767267461445685217722161 (160 bits)
t = 963692
q = 21386094473663184255325672790155329822344906504518272856132597084927479 1
$DV^2 = 3 \times 533992440316816773008967539136810690^2$

(2) k = 28, $\rho \approx 1.3$
$S(x)^2 = x^{14} = (x^7)^2$, D = 1, $h'(x) = x^2 + 1$, $r(x) = x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1$

x = 9803
r = 787604206770071823093201411395167729501255763497 (160 bits)
t = 9804
q = 181800654318120295847585099325624297268679864947052622552683437 3
$DV^2 = 1 \times 852761758800475986371318138157742$

x = 11137
r = 364098284272844368011618772721554259182887991833 7 (162 bits)
t = 11138
q = 140008218142045960128367315585381287185484743705881821082247688 97
$DV^2 = 1 \times 2366501368197753315031167615578882$

(3) k = 28, $\rho \approx 1.5$
$S(x)^2 = 4x^{16} + 8x^{12} - 8x^{10} + 8x^8 - 8x^6 + 8x^4 - 4x^2 + 1 = (-2x^8 - 2x^4 + 2x^2 - 1)^2$, D = 7,
$h'(x) = 4x^4 + 4x^2 + 8$, $r(x) = x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1$; t = x + 1

x = 41707
r = 277017639209941104676599724457301004412674528087667116 57 (160 bits)
t = 41708
q = 208277458642659286262143174064593219937166390246750999549996523200303792983
73672379
$DV^2 = 7 \times 109094312708292985321534452446978270635506^2$

(b) Special Polynomial Families with Arbitrary Values of *k*

(1) k = 24, $\rho \approx 1.25$
$S(x)^2 = 4x^8 - 4x^4 + 1 = (2x^4 - 1)^2$, D = 3, h'(x) = 4, $r(x) = x^8 - x^4 + 1$

x = 962833
r = 738597331833134695682651527040098006595721222721 (160 bits)
t = 962834
q = 228237767803155599843901956912501345675531789475531151146001
$DV^2 = 3 \times 551649366661052915408297885104^2$

x = 965365
r = 754279653484785063609361644146986474789548990001 (160 bits)
t = 965366
q = 234311355599190690060865477933001341274428958628739903196197
$DV^2 = 3 \times 558941088844719770688608313212^2$

(2) k = 48, $\rho \approx 1.125$
$S(x)^2 = 4x^{16} - 4x^8 + 1 = (2x^8 - 1)^2$, D = 3, h'(x) = 4, $r(x) = x^{16} - x^8 + 1$; t = x + 1

x = 2470
r = 191933707364169721870043501834499777475161174390000000 1 (181 bits)
t = 2471
q = 390006798225797140633544085162179699332420329265212930203 4457
$DV^2 = 3 \times 228037072490650706954059999917 7^2$

x = 5479
r = 659509122132996966757981555872075218495015674349333558784961 (199 bits)
t = 5480
q = 659695631312736178300180713056075841366806064782039550315385387 5187
$DV^2 = 3 \times 296579529820189754399141613017654 6^2$

(3) k = 96, $\rho \approx 1.06$

$S(x)^2 = 4x^{32} - 4x^{16} + 1 = (2x^{16} - 1)^2$, D = 3, h'(x) = 4, $r(x) = x^{32} - x^{16} + 1$; t = x + 1

x = 8053
r = 97869274957462648053823048369599967807487149089726854198173277268671530882746626642467570423271029692259277387159136085590721 (416 bits)
t = 8054
q = 21151084908539011258752644698068988370693194316787700109299072574747490593365787484542995859973106406242804468834519963349976870685 81
$DV^2 = 3 \times 167932863206457245463957419081399664848868883804481417725696594444 4^2$

(c) Special Polynomial Families with Different Forms of *r(x)*

(1) k = 12
$r(x) = 2197x^4 - 1352x^3 + 299x^2 - 28x + 1$, $t(x) = 13x - 1$

x = 137438953782
r = 78391580228787373878476928139585318511908631691 7 (160 bits)
t = 1786706399165
q = 10844209581049657402029453962827548199750866489317427585866728276041510847
$DV^2 = 3 \times 380249209178220512303502913837721631 1^2$
$\rho \approx 1.5$

(2) k = 14
$r(x) = 20511149x^6 - 30413083x^5 + 18803919x^4 - 6205739x^3 + 1153069x^2 - 114381x + 4733$, $t(x) = 29x - 6$

x = 5936652
r = 89792369440772206486670918839834935303559659236 9 (160 bits)
t = 172162902
q = 32681175972083556471473277579750323644791311126785365791791678052242118868836829 01
$DV^2 = 7 \times 432145319288933879814785107185576180841 00^2$
$\rho \approx 1.7$

(3) k = 14
$r(x) = x^{12} + x^{11} - x^9 - x^8 + x^6 - x^4 - x^3 + x + 1$, $t(x) = x^3 + 1$

x = 15232
r = 15599536102136296498661731398171694840382631813004 9 (167 bits)
t = 3534034567169
q = 15066673119306046585731807946325287909715901982949014978264985935985096510344650205 9
$DV^2 = 3 \times 448206397683121677619022856321082709420715^2$
$\rho \approx 1. 63$

x = 20407
r = 52164044279145037908767873210225494187626967955408 49 (172 bits)
t = 8498406359144
q = 5229522487982433102048732636329608562584662779967507108663259799850928791207 1180641259
$DV^2 = 3 \times 835026745119175457423399591345946218513529 0^2$
$\rho \approx 1.64$

(4) k = 28
$r(x) = x^{24} + x^{22} - x^{18} - x^{16} + x^{12} - x^8 - x^6 + x^2 + 1$, $t(x) = x^3 + 1$

x = 4771
r = 1934755172897947994728410192480110834394779405134439011249404032388632622350 0566190371441 (294 bits)
t = 108599606012
q = 3940931700644351676999778967026027611768493458697157224906246478662523751222508742907233737715393478235512636680743001834871 1
$DV^2 = 3 \times 229228610798458916310214822643061578056488974455156650579939870^2$
$\rho \approx 1.4$

x = 11482
r = 2756900067682603914910428454190159455946018000396363226508589807671190772572 0348452657645369203301 (324 bits)
t = 1513744672169
q = 3659950328540288301811127332474106827007430717348285891432678605275796284172287926707158623016718002672965826838633938310257662001513407 07
$DV^2 = 3 \times 6985652275476536392271825766370207017600309452882150334904590408712 83^2$
$\rho \approx 1.4$

(d) More *r* with a small factor

(1) k = 96

x = 790
r = 1043472095160358238056258121812220210087784049578745785235 3 (193 bits)
t = 791
$DV^2 = 3 \times 12106516682165495677419277453752459999999999999737^2$
q = 1099258096316635811122336014177943098887778245198159688444869289939580950444946545300000000000208297
$\rho \approx 1.67$

x = 1075
r = 960244477302499018655886830888768384605031972092397401372 9 (193 bits)
h = 193 × 189697 × 5 548897 × 44511 743233 × 116 517189 305089
t = 1076
$DV^2 = 3 \times 22774478984574661338473130929283797740936279296871422$
q = 389007669764124673056208123236933160496464959539104119574614994745358704230
57258129119873046875003855 67
ρ ≈ 1.75

x = 1462
r = 799856510600656312372792979921553204080181543003124919258645718098290466279 71851073 (276 bits)
h = 97 × 24464261226891361
t = 1463
$DV^2 = 3 \times 424342879248671780299130728442658508419523779578691097^2$
q = 135050159376789629563661162494941702923787864008293359224562874946890295339
32947961034755883180588381083264 9
ρ ≈ 1.3

x = 1990
r = 499530549187789116902899835715635587618608075220280202334114331084455419325231117458511731692993 (315 bits)
h = 769 × 95237953
t = 1991
$DV^2 = 3 \times 80203393950668375604161093376178805581259999999999999337^2$
q = 482443830090458143970598719142978471444730710196094627023340791823785775650
91833373901778494369300000000013206 97
ρ ≈ 1.17

(5)
x = 2344
r = 326534413608038975611706136294834613641018560287747216494888701221085147635724563907689293877005048825 61 (344 bits)
h = 21121
t = 2345
$DV^2 = 3 \times 1297187476163217640262247450446080231619521501549215874291^2$
q = 126202151123602375023567112106696114961035327131602564074987641333594437147
71697426952406770284100036164206374392 67
ρ ≈ 1.1