Effective Polynomial Families for Generating More Pairing-Friendly Elliptic Curves

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

Finding suitable non-supersingular elliptic curves becomes an important issue for the growing area of pairing-based cryptosystems. For this purpose, many methods have been proposed when embedding degree k and cofactor h are taken different values. In this paper we propose a new method to find pairing-friendly elliptic curves without restrictions on embedding degree k and cofactor h. We propose the idea of effective polynomial families for finding the curves through different kinds of Pell equations or special forms of $D(x)V^2(x)$. In addition, we discover some efficient families which can be used to build pairing-friendly elliptic curves over extension fields, e.g. F_p^2 and F_p^4.

Keywords: *elliptic curves over extension field, effective polynomial family, non-supersingular elliptic curves, pairing-friendly elliptic curves, Pell equation*

1. Introduction

Apart from identity-based encryption scheme [12] and short signature scheme [13], paring-based cryptography has attracted more attention in modern public-key cryptography. In 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]. However, because of the weakness of supersingular elliptic curves [11], researchers have explored other form of curves, such as the 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. Gallbraith, Mckee and Valenca [3] summarized the method proposed by early researchers and presented some appropriate families of group orders of such elliptic curves. Brezing and Weng also proposed an alternative method to find these curves [7]. They used $t - 1$ as a kth root of unity modulo prime r. Dupont, Enge and Morain [16] also proposed another method for finding the suitable non-supersingular elliptic curves. In their method, tract t was chosen large enough to make $4q - t^2$ small as to

produce effective values of D. In the most recent work, Barreto and Naehrig [17] generated non-supersingular elliptic curves with $lg(q)/lg(r) = 1$ and embedding degree $k = 12$. They presented the best curves known so far and these curves were 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 this paper we propose a new method for finding suitable non-supersingular elliptic curves for pairing-based cryptosystems. Compared to the previous work, the new method ignores the restrictions imposed on the embedding degree k and cofactor h. By using the new method, different kinds of Pell equations are built and solved to produce the elliptic curves by Complex Multiplication **(**CM**)** method [5]. Also when Pell equation can not be found, the idea of effective polynomial families of elliptic curves is proposed as another possible approach for finding the suitable elliptic curves.

This paper is organized as follows. In sections 2 we give a description of the mathematics background. In Section 3 we present the theoretical analysis and many useful polynomial families of pairing-friendly elliptic curves. In addition, the idea of effective polynomial families of elliptic curves is proposed in this section. In Section 4 we propose some special polynomial families which can be used to generate pairing-friendly elliptic curves over extension field and 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 and Appendix B.

2. Mathematics Background

To find suitable elliptic curves for pairing-based cryptosystems, certain equations are required to be solved. Actually all the previous work used different approaches to solve the relative equations and set up the elliptic curves.

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 field 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 can just consider q as a kth root of unity modulo r, like what had been done in [7]. Meanwhile since k should be 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 $0 < i < k$. Thus from [14] we can get

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

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 still need

$$hr = q + 1 - t \quad (4)$$

where h is an integer. By combining equation (2) and (4) together, we can get

$$sr = \Phi_k(t - 1) \quad (5)$$

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

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

By Hasse's bound we also need

$$|t| \leq 2q^{1/2} \quad (7)$$

Then we can compute the elliptic curve by solving

$$DV^2 = 4q - t^2 \quad (8)$$

where D is chosen by certain conditions [2]. For solving equation (8), it is desired to find the relations between q and t, as the family of group order [3]. When q and t belong to quadratic families, equation (8) may be transformed into a well known Pell equation [4] as

$$y^2 - uDV^2 = m \quad (9)$$

where D should be a square free number. After finding effective values of D, q and t, the elliptic curve can be obtained by implementing the Complex Multiplication (CM) method [5].

All the above contents are about how to find suitable elliptic curves for pairing-based cryptosystems in integer field. But it is impossible to search the whole integer field to obtain the suitable solutions. Thus we should transfer the problem into polynomial field. When analyzing in polynomial field, 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 $V(x)$. In the following paragraph we will propose a Lemma which proves that in polynomial field, equation (2) and (5) are already both efficient and necessary conditions. In polynomial field equation (3) and (6) are not needed to ensure that k is the smallest integer.

Lemma 1

Finding the smallest integer k with that ECDLP over $E(F_q)$ can be reduced to DLP over F_q^k, in polynomial field, we only need the conditions as $r(x) | \Phi_k(q(x))$ and $r(x) | \Phi_k(t(x) - 1)$. In the proof of Lemma 1, $q(x)$, $t(x)$, $r(x)$ and Φ_k are defined as different polynomials.

Proof: In polynomial field, by common knowledge we know that from $r(x) \mid q(x)^k - 1$, we can get $r(x) \mid \Phi_1(q(x))\Phi_i(q(x))\Phi_j(q(x))\ldots\Phi_k(q(x))$, where $i, j \ldots k$ are all the factors of k. Then since in polynomial field $\Phi_i(q(x))$ is relative irreducible to $\Phi_j(q(x))$ where $i \neq j$, if we get $r(x) | \Phi_k(q(x))$, $\Phi_i(q(x))$ will not be divisible by $r(x)$, when $i < k$. Thus to get the smallest integer with $r(x) \mid q(x)^k - 1$, we only need to have $r(x) | \Phi_k(q(x))$. For the same reason when finding the smallest integer with $r(x) \mid (t(x) - 1)^k - 1$, we only require $r(x) | \Phi_k(t(x) - 1)$. □

Thus for finding suitable elliptic curves for pairing-based cryptosystems in polynomial field, the equations (2, 4, 5, 7, 8) are required and they can be rewritten as:

$$d(x)r(x) = \Phi_k(q(x)) \quad (10)$$

$$h(x)r(x) = q(x) + 1 - t(x) \quad (11)$$

$$s(x)r(x) = \Phi_k(t(x) - 1) \quad (12)$$

$$|t(x)| < 2q(x)^{1/2} \quad (13)$$

$$D(x)V(x)^2 = 4q(x) - t^2(x) \quad (14)$$

3. Effective Polynomial Families for Producing More Pairing - Friendly Elliptic Curves

In the following section the math evidence for our new method is provided. As proposed in [8], from equation (4) and (8) we can get the difference between $4q$ and t^2 after knowing t and r:

$$DV^2 = 4q - t^2 = 4(hr + t - 1) - t^2 \equiv -(t-2)^2 \bmod r \quad (15)$$

Represented in polynomial field, we have

$$D(x)V^2(x) = 4q(x) - t^2(x) = -(t(x) - 2)^2 \bmod r(x) \quad (16)$$

Then after getting $r(x)$ and $t(x)$, the form of $D(x)V^2(x)$ can be obtained. But whether

$$q(x) = [D(x)V^2(x) + t^2(x)]/4 \quad (17)$$

satisfies equation (11) should be tested. After finding the effective $q(x)$, we can directly solve

$$DV^2 = 4q(x) - t^2(x)$$

as a Pell equation if $D(x)V^2(x) = 4q(x) - t^2(x)$ is quadratic. Otherwise all possible values of x should be tested to satisfy that $q(x)$ and $r(x)$ are prime numbers and at the same time small values of D exist. In the next paragraph we will give a rough description of our new method.

When finding the suitable elliptic curves for pairing-based cryptosystems in polynomial field, we assume q, t, r as $q(x)$, $t(x)$ and $r(x)$ respectively; meanwhile h, d, s, D and V should be considered as $h(x)$, $d(x)$, $s(x)$, $D(x)$ and $V(x)$. At first we use an arbitrary irreducible polynomial $r(x)$ to represent prime r. Then by $\Phi_k(t(x) - 1) \equiv 0 \bmod r(x)$ we can find effective trace polynomials $t(x)$. As proposed in [8], $D(x)V^2(x) = 4q(x) - t^2(x) \equiv -(t(x) - 2)^2 \bmod r(x)$. Thus we can compute $D(x)V^2(x)$ by the above equation after knowing $t(x)$ and $r(x)$. Then the irreducible polynomial $q(x)$ can be obtained by $4q(x) = D(x)V^2(x) + t^2(x)$. $q(x)$ should satisfy that $\Phi_k(q(x)) \equiv 0 \bmod r(x)$. If the obtained $q(x)$ is according to all the conditions, the $D(x)V^2(x)$ found above is effective.

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

Algorithm 1

Input: embedding degree k

Output: $q(x)$, $t(x)$, $r(x)$, $D(x)V^2(x)$

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. Compute polynomial $D(x)V^2(x)$ by $D(x)V^2(x) = 4q(x) - t^2(x) \equiv -(t(x) - 2)^2 \bmod r(x)$.
4. After obtaining $D(x)V^2(x)$, compute $q(x)$ by $4q(x) = D(x)V^2(x) + t^2(x)$. Test whether the irreducible polynomial $q(x)$ satisfy $\Phi_k(q(x)) \equiv 0 \bmod r(x)$.
5. If the obtained $q(x)$ is effective, output all results as $q(x)$, $t(x)$, $r(x)$, $D(x)V^2(x)$; otherwise repeat from step 1.

By our new method more polynomial families for building the pairing-friendly elliptic curves can be easily found. But for finding the parameters of such curves often

needs special forms of $q(x)$, $t(x)$ and $r(x)$. In integer field, it means that when D is a "small" integer ($D \leq 10^{10}$) [1] and q, r are large prime numbers ($q^k > 2^{1024}$ and $r > 2^{160}$) [1, 9], $DV^2 = 4q - t^2$ must have a solution. This is actually to require special forms of $q(x)$, $r(x)$ and $D(x)V^2(x)$ in polynomial field. When $D(x)V^2(x)$ is an arbitrary polynomial, to find valid values of D is very difficult as q and r must be large secure parameters. In the following parts we will discuss different forms of $D(x)V^2(x)$ that can be used to produce the pairing-friendly elliptic curves efficiently.

Before the discussion we need to mention an observation. When $q(x)$, $t(x)$ and $r(x)$ are suitable polynomials that can be used to generate pairing-friendly elliptic curves, $q(-x)$, $t(-x)$ and $r(-x)$ are also such polynomials. This observation comes from the fact that in the operation x can be taken as either positive or negative integers.

3.1 Polynomial Families with Square Polynomial and Constant Number Factors

Considering polynomial family $D(x)V^2(x) = 4q(x) - t^2(x)$, when we require q, r as large prime numbers and D as an "small" integer, the simplest situation happens when $4q(x) - t^2(x)$ can be expressed as one square polynomial multiplying with one constant positive number. This means that $D(x)V^2(x) = DV^2(x)$, where the degree of $V(x)$ is not zero. Then we only need to seek the suitable x when $q(x)$ and $r(x)$ are prime numbers since D will always equal the constant integer. It is rather easy to find such x. With these polynomial families we have better possibilities to find certain x satisfying other conditions, which makes the computation of paring-based cryptosystems more efficient.

The work of Barreto and Naehrig [17] provided us a perfect example of such a polynomial family when $k = 12$. The polynomial family they found had a special property as $\Phi_k(t(x) - 1) = r(x)r(-x)$. When $k = 12$, they got from [3] that $t(x) - 1$ only could be $2x^2$ or $6x^2$ when $\Phi_k(t(x) - 1)$ was the multiple of two quartic polynomials as $n_1(x)$ and $n_2(x)$. They used $t(x) - 1$ as $6x^2$ and found a perfect polynomial family, in which $4q^2(x) - t^2(x)$ was a multiple of a square polynomial and a constant integer. Thus the value of D would be always valid as the constant integer and $\rho = lg(q)/lg(r) \approx 1$. But as the lemma proposed in [19], $-2x^2$ and $-6x^2$ also can be used as the possible polynomials with the feature of splitting. This generates the results tabulated in Table 1.

t(x)	r(x)	q(x)	$4q(x) - t^2(x)$
$2x^2 + 1$	$4x^4 + 4x^3 + 2x^2 + 2x + 1$	$4x^4 + 4x^3 + 4x^2 + 2x + 1$	$(2x^2 + 1)(6x^2 + 8x + 3)$
$-2x^2 + 1$	$4x^4 + 4x^3 + 2x^2 + 2x + 1$	$4x^4 + 4x^3 + 2x + 1$	$12x^4 + 16x^3 + 4x^2 + 8x + 3$
$6x^2 + 1$	$36x^4 + 36x^3 + 18x^2 + 6x + 1$	$36x^4 + 36x^3 + 24x^2 + 6x + 1$	$3(6x^2 + 4x + 1)^2$
$-6x^2 + 1$	$36x^4 + 36x^3 + 18x^2 + 6x + 1$	$36x^4 + 36x^3 + 12x^2 + 6x + 1$	$3(36x^4 + 48x^3 + 20x^2 + 8x + 1)$

Table 1: more splitting polynomial families when $k = 12$

In Table 1 when $t(x) - 1 = \pm 2x^2$ and $-6x^2$, $4q(x) - t^2(x)$ can not be factorized as one square polynomial multiplying with one constant number. When $t(x) - 1 = 2x^2$, $q(x) = 4x^4 + 4x^3 + 4x^2 + 2x + 1 = (2x^2 + 1)(2x^2 + 2x + 1)$ is not even an irreducible polynomial, which can not be used to produce a prime number q. Thus $t(x) - 1 = 6x^2$ may be the only family with the desired property. When $k = 6$, in Table 2 we list some

polynomials of $r(x)$, $q(x)$ and $t(x)$, where $4q(x) - t^2(x) = DV^2(x)$ also is the multiple of a square polynomial and a constant integer. These polynomial can be used to generate pairing-friendly elliptic curves efficiently when $k = 6$ and $\rho = lg(q)/lg(r) \approx 2$. The first family is used to generate the parameters of an elliptic curve in Appendix A.

q(x)	t(x)	r(x)	$4q(x) - t^2(x)$
$9x^4 - 9x^3 + 9x^2 - 3x + 1$	$3x^2 + 1$	$3x^2 - 3x + 1$	$3(3x^2 - 2x + 1)^2$
$27x^4 - 9x^3 + 3x^2 - 3x + 1$	$-9x^2 + 1$	$9x^2 - 3x + 1$	$3(3x^2 - 2x + 1)^2$
$36x^4 + 9x^2 - 3x + 1$	$-6x^2 - 3x + 1$	$12x^2 + 1$	$3(6x^2 - x + 1)^2$

Table 2: effective polynomial families when $k = 6$, $\rho \approx 2$

Although the curves produced from the above table may not be the ones with best performance since $\rho = lg(q)/lg(r) \approx 2$ [1], the special form of $4q(x) - t^2(x) = DV^2(x)$ will always lead to a small D. This gives us better possibilities to search suitable x with other efficient conditions, e.g. q and r are primes with low-hamming weight [20] or the technique for saving the bandwidth described in [18]. For finding such results, in the following paragraph we will propose a Lemma which can be used to find these polynomial families.

Lemma 2
When finding $q(x)$ and $t(x)$ with $4q(x) - t^2(x) = DV^2(x)$ and $degree(q(x)) = degree(t(x))/2$, if assuming $q(x) = q_n x^n + q_{n-1}x^{n-1} + ... + q_1 x + q_0$, $t^2(x) = t_n x^n + t_{n-1}x^{n-1} + ... + t_1 x + t_0$, $4q_n - t_n^2$ and $4q_0 - t_0^2$ should be factorized as one constant number multiplying with one square number.

Proof: Assuming $q(x) = q_n x^n + q_{n-1}x^{n-1} + ... + q_1 x + q_0$, $t^2(x) = t_n x^n + t_{n-1}x^{n-1} + ... + t_1 x + t_0$, $V(x) = v_n x^n + v_{n-1}x^{n-1} + ... + v_1 x + v_0$, when $4q(x) - t^2(x) = DV^2(x)$, we must have $4q_n - t_n = Dv_n^2$ *and* $4q_0 - t_0 = Dv_0^2$. □

In the above Lemma we just suggest the common form of $q(x)$ and $t(x)$ when $4q(x) - t^2(x)$ can be factorized as one constant number multiplying with one square polynomial. Actually the simplest case appears when $q_n = a^2$, $t_n = a^2$ and $q_0 = b^2$, $t_0 = b^2$, where a, b are integers. In such case, $4q_n - t_n = 3a^2$ and $4q_0 - t_0 = 3b^2$. In such cases D will equal 3. All the results in Table 2 are according to this condition. By the same technique, we also find the perfect polynomial family proposed by [17] and some other polynomial families when $k = 3$ and 4. Table 3 and Table 4 tabulate the results.

q(x)	t(x)	r(x)	$4q(x) - t^2(x)$
$3x^4 + 3x^3 + 4x^2 + 2x + 1$	$-3x^2 - 2x - 2$	$x^2 + x + 1$	$3x^4$
$x^4 + x^3 + 3x^2 + x + 1$	$-x^2 - 2x - 1$	$x^2 + x + 1$	$3(x^2 + 1)^2$

Table 3: effective polynomial families when $k = 3$, $\rho \approx 2$

q(x)	t(x)	r(x)	$4q(x) - t^2(x)$
$4x^4 - 4x^3 + 2x^2 - 2x + 1$	$-4x^2 + 2x$	$2x^2 - 2x + 1$	$4(x - 1)^2$
$8x^4 + 6x^2 + 2x + 1$	$4x^2 + 2x + 2$	$4x^2 + 1$	$4x^2(2x^2 - 1)^2$
$128x^4 + 24x^2 + 4x + 1$	$-16x^2 + 4x$	$16x^2 + 1$	$4(8x^2 + 2x + 1)^2$

Table 4: effective polynomial families when $k = 4$, $\rho \approx 2$

Actually for finding the special forms of polynomial $t(x)$ with $\Phi_k(t(x) - 1) = n_1(x)n_2(x)$ [3], the value of k can not be 3, 4 or 6 if we want $\rho = lg(q)/lg(r) \approx 1$. Because when $\rho = lg(q)/lg(r) \approx 1$, the degree of $q(x)$ must equal that of $r(x)$. Then since equation (7) must be satisfied as the Hasse's bound, the degree of $\Phi_k(t(x) - 1)$ has to be at least four times of the degree of $t(x)$ so that $\Phi_k(t(x) - 1)$ has the same degree as $n_1(x)n_2(x)$. Thus the values of k can not be 3, 4 or 6.

3.2 Polynomial Families for Building and Solving Pell Equations

When finding the suitable non-supersingular elliptic curves by setting up and solving certain Pell equations, different methods had been proposed in [1, 3, 8]. In this section, we will implement different kinds of Pell equations for finding the pairing-friendly elliptic curves. The first kind of Pell equations can be viewed as the effective Pell equations, which have a better chance to generate such elliptic curves. The second kind are the extended versions of Pell equations, which shows the possibility to find such elliptic curves when k is larger than 6. Before the proposition of our new definitions, first we will give a Lemma which discovers an intrinsic relation between the polynomial families of elliptic curves when $k = 3$ and $k = 6$.

Lemma 3

Suppose in polynomial field $t(x)$ and $r(x)$ compose a polynomial family with embedding degree $k = 6$. Then using $2 - t(x)$ as another trace polynomial $t'(x)$, with same $r(x)$ we can find a different polynomial family with embedding degree $k = 3$. The converse situation is also true.

Proof: when $t(x)$ and $r(x)$ satisfy the condition as a polynomial family with embedding degree $k = 6$, we have $\Phi_6(t(x) - 1) = (t(x) - 1)^2 - (t(x) - 1) + 1 = t^2(x) - 3t(x) + 3 \equiv 0 \bmod r(x)$. By using $2 - t(x)$ as $t'(x)$, with the same $r(x)$, we implement them into the relation of a family when $k = 3$ as $\Phi_3(2 - t(x) - 1) = (1 - t(x))^2 + (1 - t(x)) + 1 = t^2(x) - 3t(x) + 3$. It is same with the equation when $k = 6$. Thus we can have $\Phi_3(2 - t(x) - 1) \equiv 0 \bmod r(x)$. As a conclusion, if $t(x)$ and $r(x)$ compose a polynomial family when $k = 3$, $2 - t(x)$ and $r(x)$ can also set up another valid polynomial family with embedding degree $k = 6$. The proof of the converse situation is similar. □

By the above lemma we can easily find polynomial families with $k = 3$ from the polynomial families with $k = 6$ or do on the converse case. Actually in [3] all the listed families with $k = 3$ or $k = 6$ can be found by the above lemma. Now we discuss some important issues for our new method.

As analyzed above, polynomial $D(x)V^2(x)$ can be obtained by $D(x)V^2(x) = 4q(x) - t^2(x) \equiv -(t(x) - 2)^2 \bmod r(x)$ after knowing $t(x)$ and $r(x)$. In most cases $V^2(x)$ will equal 1 since it is hard to find square polynomial factors contained in $4q(x) - t^2(x)$. Here if we want to set up a Pell equation, $D(x)V^2(x)$ must be chosen as a quadratic polynomial as $ax^2 + bx + c$; otherwise we have to test all possible values for x to satisfy that $q(x)$ and $r(x)$ are prime numbers and meanwhile small values of D exist. Considering the quadratic form of $D(x)V^2(x)$ used to set up Pell equations, as analyzed in [3], the relation between $q(x)$ and $t(x)$ can be defined as the polynomial families of elliptic curves.

For suitable q and t, the value for D must be a small integer (e.g. $D < 10^{10}$) [1]. This is actually a very strict condition since meanwhile we need q and t as secure parameters. When $k = 6$, we at least require that $q^6 > 2^{1024}$ [1] and $r > 2^{160}$ [9]. This gives that $q > 2^{171} \approx 10^{51}$. Since $|t| < 2q^{1/2}$, equation (8) will always generate a very large number. It is very hard to find a value of D smaller than 10^{10} for implementation.

This idea can be proved by the examples proposed in [1] and [3]. The authors [3] noticed that compared to other families, $q(x) = 208x^2 + 30x + 1$ and $t(x) = -26x - 2$ is particularly "lucky" in generating suitable (q, t) pairs. But it seemed they did not give the reason why this family could generate most of the examples in [1]. Now we provide some mathematics analysis to illustrate this question. Assuming $4q(x) - t^2(x)$ is a quadratic polynomial as $ax^2 + bx + c$, then finding suitable values of D is actually to solve a quadratic equation as $DV^2 = ax^2 + bx + c$ for integer solutions with enough length, where D is taken as a square free number between 0 to 10^{10} [1] and V^2 is a square number. Meanwhile for the suitable x, $q(x)$ and $r(x)$ need to be prime numbers. Thus more suitable integer solutions found for $DV^2 = ax^2 + bx + c$, more possibilities we can test for prime q and r. Now we transform the equation into $ax^2 + bx + c - DV^2 = 0$ and try to factorize it since we only need the integer solutions. This means that $ax^2 + bx + c - DV^2 = 0$ must be factorized as $(a_1x + d_1)(a_2x + d_2) = 0$, where $a_1a_2 = a$, $d_1d_2 = c - DV^2$, $a_1d_2 + a_2d_1 = b$, $a_1 \mid d_1$ and $a_2 \mid d_2$. Now considering the situation that $a_1 = 1$, obviously this kind of equations will have a better chance to generate the suitable integer solutions since the condition $a_1 \mid c_1$ can be ignored. Actually this is the most "lucky" family mentioned in [3]. The proposed family is that $q(x) = 208x^2 + 30x + 1$, $t(x) = -26x - 2$, DV^2 equals $4q(x) - t^2(x)$ as $4x(39x + 4)$. Here $4x$ can be viewed as x since 4 is a square contained in V^2, which can be ignored in the computation. When $4q(x) - t^2(x)$ can be factorized, which means $ax^2 + bx + c - DV^2 = (a_1x + c_1)(a_2x + c_2)$, the final quadratic equation also has a better chance to generate suitable values of D because the condition $a_1a_2 = a$ can be ignored.

For the suitable families as the quadratic polynomial relations between $q(x)$ and $t(x)$, as analyzed above, we need that $4q(x) - t^2(x)$ can be factorized. This ensures a larger possibility of the existence of small values of D. In other words, when transformed into Pell equations, these quadratic equations with the feature of factorization between $4q(x)$ and $t^2(x)$ are more likely to have suitable solutions. However, in most cases $4q(x) - t^2(x)$ is an irreducible quadratic polynomial [3]. It is very difficult to find suitable x to satisfy that $q(x)$ and $r(x)$ are prime numbers and at the same time $4q(x) - t^2(x)$ has a factor as a large square. In the following paragraphs, we will present some effective polynomial families with larger values of cofactor h, when $k = 3$, 4, and 6. In [3] the authors only presented the complete polynomial families of $h \in [2, 5]$ when $k = 3, 4, 6$.

(a) New quadratic families of elliptic curves when $k = 3$, $h > 5$ and $\rho \approx 1$

By our new algorithm, we can easily find all polynomial families with arbitrary values of h. In Table 5 we tabulate some polynomial families when $k = 3$, $h = 6$ and $\rho \approx 1$. These families have not been proposed by any previous work and in Append A we generate the parameters of several elliptic curves for each of the family.

h	q(x)	t(x)	r(x)	$4q(x) - t^2(x)$

6	$6x^2 + 5x + 5$	$-x$	$x^2 + x + 1$	$23x^2 + 20x + 20$
6	$18x^2 + 15x + 4$	$-3x - 1$	$3x^2 + 3x + 1$	$3(21x^2 + 18x + 5)$
6	$78x^2 + 29x + 2$	$-13x - 3$	$13x^2 + 7x + 1$	$143x^2 + 38x - 1$
6	$114x^2 + 71 + 10$	$-19x - 7$	$19x^2 + 15x + 3$	$95x^2 + 18x - 9$
6	$126x^2 + 33x + 1$	$-21x - 4$	$21x^2 + 9x + 1$	$3(21x^2 - 12x - 4)$

Table 5: new quadratic polynomial families when $k = 3$, $h = 6$

Based on the idea of effective polynomial families of elliptic curves, for large values of cofactor h, in Table 6 we tabulate some quadratic polynomial families when $k = 3$ and $h = 7$ to 12. Among them we present two families with the feature of factorization. Both of them should have a better chance for generating pairing-friendly elliptic curves.

h	**q(x)**	**t(x)**	**r(x)**	**$4q(x) - t^2(x)$**
7	$364x^2 + 72x + 3$	$-26x - 3$	$52x^2 + 14x + 1$	$3(260x^2 + 44x + 1)$
8	$504x^2 + 141x + 10$	$21x + 3$	$63x^2 + 15x + 1$	$1575x^2 + 438x + 31$
9	$432x^2 + 96 + 7$	$-12x - 1$	$48x^2 + 12x + 1$	$9(176x^2 + 40x + 3)$
10	$310x^2 + 79x + 4$	$-31x - 5$	$31x^2 + 11x + 1$	$3(93x^2 + 2x - 3)$
11	$473x^2 + 100x + 4$	$-43x - 6$	$43x^2 + 13x + 1$	$43x^2 - 116x - 20$
12	$\mathbf{252x^2 + 87x + 7}$	$\mathbf{-21x - 4}$	$\mathbf{21x^2 + 9x + 1}$	$\mathbf{3(9x + 2)(21x + 2)}$
16	$\mathbf{688x^2 + 251x + 22}$	$\mathbf{43x + 7}$	$\mathbf{43x^2 + 13x + 1}$	$\mathbf{3(7x + 1)(43x + 13)}$

Table 6: new quadratic polynomial families when $k = 3$, $\rho \approx 1$

(b)New quadratic families of elliptic curves when $k = 4$, $h > 5$ and $\rho \approx 1$

In Table 7 we list some quadratic polynomial families when $k = 4$ and $h = 6$ to 12. The third and fourth families in the table are effective families with the feature of factorization. The second polynomial family of $h = 8$ is used to generate the parameters of some pairing-friendly elliptic curves in Appendix A.

h	**q(x)**	**t(x)**	**r(x)**	**$4q(x) - t^2(x)$**
6	$12x^2 + 10x + 5$	$-2x$	$2x^2 + 2x + 1$	$4(11x^2 + 10x + 5)$
7	$35x^2 + 23x + 5$	$-5x - 1$	$5x^2 + 4x + 1$	$115x^2 + 82x + 19$
8	$\mathbf{136x^2 + 47x + 4}$	$\mathbf{-17x - 3}$	$\mathbf{17x^2 + 8x + 1}$	$\mathbf{(5x + 1)(51x + 7)}$
8	$\mathbf{136x^2 + 81x + 12}$	$\mathbf{17x + 5}$	$\mathbf{17x^2 + 8x + 1}$	$\mathbf{(3x + 1)(85x + 23)}$
9	$45x^2 + 41x + 11$	$5x + 3$	$5x^2 + 4x + 1$	$155x^2 + 134x + 35$
10	$80x^2 + 36x + 9$	$-4x$	$8x^2 + 4x + 1$	$4(76x^2 + 36x + 9)$
11	$220x^2 + 98x + 13$	$10x + 3$	$20x^2 + 8x + 1$	$780x^2 + 332x + 43$
12	$384x^2 + 88x + 11$	$-8x$	$32x^2 + 8x + 1$	$4(368x^2 + 88x + 11)$

Table 7: new quadratic polynomial families when $k = 4$, $\rho \approx 1$

(c) New quadratic families of elliptic curves when $k = 6$, $h > 5$ *and* $\rho \approx 1$

Same as the results listed in Table 6, by our method we find more quadratic polynomial families of non-supersingular elliptic curves when $k = 6$, $h > 5$ and $\rho \approx 1$. When $h = 9$, one of the families we present in Table 8 is an effective polynomial family. Two of the families in Table 8 are used to generate the parameters of two non-supersingular elliptic curves in Appendix A.

h	**q(x)**	**t(x)**	**r(x)**	**$4q(x) - t^2(x)$**
6	$24x^2 + 14x + 7$	$2x + 2$	$4x^2 + 2x + 1$	$4(23x^2 + 12x + 6)$
6	$72x^2 + 30x + 5$	$-6x$	$12x^2 + 6x + 1$	$4(63x^2 + 30x + 5)$
7	$91x^2 + 36x + 4$	$-13x - 2$	$13x^2 + 7x + 1$	$195x^2 + 92x + 12$

7	$49x^2 + 28x + 5$	$-7x - 1$	$7x^2 + 5x + 1$	$147x^2 + 98x + 19$
8	$32x^2 + 18x + 9$	$2x + 2$	$4x^2 + 2x + 1$	$4(31x^2 + 16x + 8)$
8	$608x^2 + 202x + 17$	$-38x - 6$	$76x^2 + 30x + 3$	$4(247x^2 + 88x + 8)$
9	$\mathbf{279x^2 + 130x + 15}$	$\mathbf{31x + 7}$	$\mathbf{31x^2 + 11x + 1}$	$\mathbf{(5x + 1)(31x + 11)}$
9	$81x^2 + 30x + 10$	$3x + 2$	$9x^2 + 3x + 1$	$9(35x^2 + 12x + 4)$
10	$40x^2 + 22x + 11$	$2x + 2$	$4x^2 + 2x + 1$	$4(39x^2 + 20x + 10)$
10	$1750x^2 + 415x + 26$	$-35x - 3$	$175x^2 + 45x + 3$	$5(1155x^2 + 290x + 19)$

Table 8: new quadratic polynomial families when $k = 6$, $\rho \approx 1$

In the above contents, actually we present some effective polynomial families which can be used to set up the standard Pell equations. These Pell equations have better chances to obtain pairing-friendly elliptic curves in implementations. Then we should point out that when $q(x)$ has degree larger than 2, we can not get Pell equation from $4q(x) - t^2(x)$ since it will not be a quadratic polynomial. But if we factorize $4q(x) - t^2(x)$ as $D(x)V^2(x)$ and $D(x)$ is quadratic, we still can obtain Pell equations just by $D(x)$. The reason is that square polynomial $V^2(x)$ can be ignored in the computation. This can be viewed as to set up the extended versions of Pell equations. By this idea more Pell equation can be established and more elliptic curves can be found when $k > 6$. In addition, besides the situations when $q(x)$ and $t^2(x)$ are quadratic polynomials, sometimes extended versions of Pell equations can be produced when $4q(x) - t^2(x)$ are like the forms as:

$$4q(x) - t^2(x) = ax^{2i} + bx^i + c \quad (18)$$

where a, b, c and i are integers. For example, when $4q(x) - t^2(x) = ax^4 + bx^2 + c$, replacing x^2 by y, we still may get a Pell equation as

$$DV^2 = ay^2 + by + c \quad (19)$$

Thus in the implementations we will enlarge the searching for all kinds of Pell equations.

In the following paragraphs, we will present some polynomial families which can be used to set up the extended versions of Pell equations when $k = 8$ and $k = 12$.

(d) Effective polynomial families of elliptic curves when $k = 8$, $\rho \approx 1.5$

When $k = 8$, it is unlikely to obtain quadratic relations between $4q(x)$ and $t^2(x)$. But it is still possible to find certain forms of $4q(x) - t(x)^2$ with square polynomials factors and set up extended versions of Pell equations. Then small values of D can be solved. Table 9 lists some of the results when $k = 8$ and $\rho \approx 1.5$. For convenience, we just take $r(x)$ as the standard cyclotomic polynomial as $x^4 + 1$.

t(x)	**q(x)**	**$4q(x) - t^2(x)$**
$x + 1$	$x^6 - 2x^5 + x^4 + x^2 - x + 1$	$(x - 1)^2(4x^4 + 3)$
$x + 1$	$2x^6 - 4x^5 + 2x^4 + 2x^2 - 3x + 2$	$(x - 1)^2(8x^4 + 7)$
$x + 1$	$3x^6 - 6x^5 + 3x^4 + 3x^2 - 5x + 3$	$(x - 1)^2(12x^4 + 11)$
$x + 1$	$4x^6 - 8x^5 + 4x^4 + 4x^2 - 7x + 4$	$(x - 1)^2(16x^4 + 15)$

Table 9: effective polynomial families when $k = 8$, $\rho \approx 1.5$

(e) Effective polynomial families of elliptic curves when $k = 12$, $\rho \approx 1.5$

When $k = 12$, we also find some polynomial families, which can be used to set up the extended versions of Pell equations. Table 10 lists some of the results when $k = 12$ and $\rho \approx 1.5$. For convenience, we just take $r(x)$ as the standard cyclotomic polynomial as $x^4 - x^2 + 1$.

q(x)	t(x)	$4q(x) - t^2(x)$
$x^6 + 2x^5 - 2x^3 + x + 1$	$-x + 1$	$(x + 1)^2(4x^4 - 4x^2 + 3)$
$3x^6 + 6x^5 - 6x^3 + 5x + 3$	$-x + 1$	$(x + 1)^2(12x^4 - 12x^2 + 11)$
$5x^6 + 10x^5 - 10x^3 + 9x + 5$	$-x + 1$	$(x + 1)^2(20x^4 - 20x^2 + 19)$

Table 10: effective polynomial families when $k = 12$, $\rho \approx 1.5$

(f) More effective families of elliptic curves when $k = 12$, $\rho \approx 2$
When $k = 12$ and $\rho \approx 2$, we find some special forms of $D(x)V^2(x)$, which can also be used to set up extended versions of Pell equations. Table 11 presents the results. During the implementation we still use the simplest form of $r(x)$ as the cyclotomic polynomial as $x^4 - x^2 + 1$.

q(x)	t(x)	$4q(x) - t^2(x)$
$x^8 + 2x^7 + x^6 + x^2 + x + 1$	$-x + 1$	$(x + 1)^2(4x^6 + 3)$
$2x^8 + 4x^7 + 2x^6 + 2x^2 + 3x + 2$	$-x + 1$	$(x + 1)^2(8x^6 + 7)$

Table 11: effective polynomial families when $k = 12$, $\rho \approx 2$

When we can not directly obtain one Pell equation or its extended version from $4q(x) - t^2(x)$, some other forms of $D(x)V^2(x)$ may also be possible to generate valid values of D, e.g. $4q(x) - t^2(x)$ is a multiple of two quadratic equations [20]. In the following paragraph we will present some of such polynomial families when $k = 12$ and $\rho = lg(q)/lg(r) \approx 1$.

(g) Some other polynomial families of elliptic curves when $k = 12$, $\rho \approx 1$
When $k = 12$ and $\rho \approx 1$, besides the perfect polynomial family proposed in [17], we find some other useful forms of $D(x)V^2(x)$. They can be factorized as the multiple of two quadratic equations. Thus we can set up two separate Pell equations for obtaining small values of D. In [17] the authors also presented a polynomial family with the same property when $k = 5$. These polynomial families may generate best pairing-friendly elliptic curves with $\rho \approx 1$ if we can find certain techniques to solve the Pell-like equations. Table 12 tabulates the results.

h	q(x)	t(x)	r(x)	$4q(x) - t^2(x)$
25	$900x^4 + 900x^3 + 456x^2 + 150x + 25$	$6x^2 + 1$	$36x^4 + 36x^3 + 18x^2 + 6x + 1$	$3(18x^2 + 4x + 3)(66x^2 + 52x + 11)$
4705	$169380x^4 + 169380x^3 + 84696x^2 + 28230x + 4705$	$6x^2 + 1$	$36x^4 + 36x^3 + 18x^2 + 6x + 1$	$3(246x^2 + 52x + 41)(918x^2 + 724x + 153)$
113	$452x^4 + 452x^3 + 228x^2 + 226x + 113$	$2x^2 + 1$	$4x^4 + 4x^3 + 2x^2 + 2x + 1$	$(22x^2 - 8x + 11)(82x^2 + 112x + 41)$
21841	$87364x^4 + 87364x^3 + 43684x^2 + 43682x + 21841$	$2x^2 + 1$	$4x^4 + 4x^3 + 2x^2 + 2x + 1$	$(306x^2 - 112x + 153)(1142x^2 + 1560x + 571)$

Table 12: some other polynomial families when $k = 12$, $\rho \approx 1$

3.3 Polynomial Families with Small Degree

Actually when the degree of $D(x)V^2(x)$ is much smaller than that of $q(x)$, finding valid values of D may not be a hard problem. But unfortunately since equation (7) must be

satisfied, the degree of $D(x)V^2(x)$ is always same as that of $q(x)$. Thus it is hard to find $D(x)V^2(x)$ with small degree.

From the above analysis, we now define the effective polynomial families of suitable non-supersingular elliptic curves for pairing-based cryptosystems.

Definition: When finding the polynomial families of suitable non-supersingular elliptic curves for pairing-based cryptosystems in polynomial field, $r(x)$, $q(x)$ and $t(x)$ should satisfy that $4q(x) - t^2(x)$ can be factorized with one square polynomial; or $4q(x) - t^2(x)$ at least can be factorized; or $4q(x) - t^2(x)$ only contains terms with smaller degree compared to $q(x)$. These families as the relations between $q(x)$ and $t(x)$ are defined as the effective polynomial families. They have a better chance to generate pairing-friendly elliptic curves in implementations.

Now we propose the complete algorithm for finding suitable elliptic curves for pairing-based cryptosystems.

Algorithm 2

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

Output: x_0, $q(x)$, $t(x)$, $r(x)$, $D(x)V^2(x)$

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. Compute polynomial $D(x)V^2(x)$ by $D(x)V^2(x) = 4q(x) - t^2(x) \equiv -(t(x) - 2)^2 \bmod r(x)$. According to the definition of effective polynomial families, if $D(x)V^2(x)$ can be used to set up Pell equations, it should be represented as the $ax^i(bx^i + c)$ or $(ax^i + b)(cx^i + d)$ where a, b, c, d and i are all integers; otherwise $degree(V(x)) > 0$ or $degree(D(x)V^2(x)) < 2degree(r(x))$ should be satisfied.
4. After obtaining $D(x)V^2(x)$, compute $q(x)$ by $4q(x) = D(x)V^2(x) + t^2(x)$. Test whether the irreducible polynomial $q(x)$ satisfy $\Phi_k(q(x)) \equiv 0 \bmod r(x)$.
5. If $D(x)V^2(x) = 4q(x) - t^2(x)$ is as the form as $ax^{2i} + bx^i + c$, transfer $DV^2 = 4q(x) - t^2(x)$ into a Pell equation and solve it for effective values of D, q, r, t based on certain integer x_0 as $D(x_0)$, $q(x_0)$, $r(x_0)$ and $t(x_0)$; otherwise test all possible values of x to obtain an integer x_0 with $D(x_0)$, $q(x_0)$, $r(x_0)$ and $t(x_0)$ as the suitable parameters.
6. Establish the elliptic curve by CM method with the above parameters.
7. Find other effective values of x_0 and parameters, set up different elliptic curves
8. If no elliptic curves are found, repeat from step 1.

After finding all the suitable polynomials of $D(x)V^2(x)$, $q(x)$, $t(x)$ and $r(x)$, we can get effective values of D, q and r by solving certain Pell equations or testing all possible values of x in $D(x)V^2(x)$, where $V^2(x)$ is a square polynomial. Then CM method can be used to produce the desired non-supersingular elliptic curves for pairing-based cryptosystems. Here we should mention that prime r can also be regarded as $m \times n$, where m is a small composite number and n is a large prime. In such case the cofactor will be increased to $h \times m$.

Another issue we should point out is that by testing different values of x, we could obtain different pairing-friendly elliptic curves with a same polynomial family. This is an important advantage for using the idea of family in polynomial field. Since

compared to the work of [7, 18], we give the possibility to obtain different suitable elliptic curves based on a same polynomial family.

In the following section we will discuss the possibilities for building the pairing-friendly elliptic curves over extension fields.

4. Pairing-Friendly Elliptic Curves over Extension Fields

Since the work of [10], supersingular elliptic curves are viewed as the nature choice for pairing-based cryptography. Many efficient computations of pairing-based cryptosystems [21, 22] have been implemented over such curves. In [17] the authors have proposed an open problem to find pairing-friendly elliptic curves over extension fields. In their work they found some square $q(x)$ as $p(x)^2$ when $k = 5$. But since in their examples $4q(x) - t^2(x)$ was not an effective form, finding valid values of D became a hard problem. Actually Menezes *et al*. [10] had proposed the possible solution to set up supersingular elliptic curves over extension field when $k = 3$. By their work, when $k = 3$ we have $t^2 = q$. Thus it is possible to view q as p^{2i}, where i is an integer. Then we can set up the supersingular elliptic curves over extension fields as F_p^{2i}, where p is a large prime. In Table 13 we tabulate the simplest forms of polynomial families for pairing-friendly elliptic curves over F_p^2 when $k = 3$. In the results, $D(x)V^2(x)$ will be factorized as one constant number multiplying with a square polynomial since $4q(x) - t^2(x) = 3t^2(x)$. This means the values for D are always valid.

q(x)	r(x)	h	t(x)	$DV^2(x)$
x^2	$x^2 + x + 1$	1	$-x$	$3x^2$
x^2	$x^2 - x + 1$	1	x	$3x^2$

Table 13: effective families of supersingular elliptic curves over square field

In fact with the simplest forms, we can easily generate suitable supersingualr elliptic curves for pairing-based cryptosystems over quartic field as F_p^4. In Table 14 we tabulate the families.

q(x)	r(x)	h	t(x)	$DV^2(x)$
x^4	$x^4 + x^2 + 1$	1	$-x^2$	$3x^4$
x^4	$x^4 - x^2 + 1$	1	x^2	$3x^4$

Table 14: effective families of supersingular elliptic curves over quartic field

The deduction for such polynomial families is trivial. But the most important advantage is that we can set up such supersingular elliptic curves over certain special extension fields, e.g. Optimal Extension Field (OEF) [24]. Bailey and Paar [24] proposed to build elliptic curves over such extension field with many efficient arithmetic operations. The form of OEF can be described as $F_{(2^n \pm c)^m}$, where $2^n \pm c$ is a pseudo-Mersenne prime. Since when $k = 3$, we take F_q as the form of F_p^{2i} ($p = 2^n \pm c$, $m = 2i$); then we have the possibilities to set up the curves over certain OEFs. The tract t will equal p^i as the property of supersingular curves with $k = 3$. But we still need to ensure that $hr(x) = p^{2i} + 1 - p^i$ is a large prime ($h = 1$) or contains a large prime factor ($h > 1$). For example, from Table 14 we take x as a pseudo-Mersenne prime ($2^{57} - 195$) and m as 4, then we can set up the supersingular pairing-friendly elliptic curves over $F_{(2^{57} - 195)^4}$, where the embedding degree $k = 3$ and $t = (2^{57} - 195)^2$. Here r is a large prime factor of the curve order $(2^{57} - 195)^4 + 1 - (2^{57} - 195)^2$

with $\rho = lg(q)/lg(r) \approx 1.1$. In this example the values of x and m are chosen from the database presented in [24]. The other problem is that for this OEF, $q = (2^{57} - 195)^4$ is only a 228 bits number, which is not secure as we need $q^3 > 2^{1024}$. But since in [24] the authors only list part of the OEFs and the upper bound of the curve order is set on 2^{256}, we can easily build secure supersingular pairing-friendly elliptic curves when increasing the level of OEFs. Then all the favorable efficient arithmetic algorithms can be transformed into the computation of pairing-based cryptosystems. In Appendix B we list two possible OEFs for supersingular elliptic curves with $m = 4, 8$.

5. Conclusion

In this paper we present a new method for finding more pairing-friendly elliptic curves over prime field and extension field. We propose the idea of effective polynomial families to build such elliptic curves through different kinds of Pell equations and special forms of $D(x)V^2(x)$. By using these effective families, numerous pairing-friendly elliptic curves can be found without restrictions on embedding degree k and cofactor h.

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] N. P. Smart. The Algorithmic Resolution of Diophantine Equations. Landon Mathematical Society Student Text 41, Cambridge University Press, 1998.

[5] I. F. Blake, G. Seroussi and N. P. Smart. Elliptic Curves in Cryptography. Volume 265 of London Mathematical Society Lecture Note Series. Cambridge University Press, 1999.

[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] M. Scott and P. S. L. M. Barreto. Compressed pairings. In Advances in cryptology – Crypto'2004, volume 3152 of Lecture Notes in Computer Science, pages 140 – 156, Santa Barbara, USA, 2004. Springer – Verlag.

[19] S. Cui, P. Duan and C. W. Chan. A New Method for Building More Non-Supersingular Curves. International Workshop on Information Security & Hiding (ISH'05), Singapore. LNCS 3481, Springer-Verlag, pp. 657 – 664, May 2005.

[20] Neal Koblitz and Alfred Menezes. Pairing-based cryptography at high security levels. Cryptography ePrint Archive, Report 2005/076, 2005.

[21] 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.

[22] 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.

[23] P. S. L. M. Barreto, S. Galbraith, C. O. hEigeartaigh and M. Scott. Efficient pairing computation on supersingular abelian varieties. Cryptology ePrint Archive, Report 2004/375, 2004.

[24] D.V.Bailey and C.Paar. Efficient Arithmetic in Finite Field Extensions with Application in Elliptic Curve Cryptography. Journal of CRYPTOLOGY, 2001.

Appendix A: Pairing-friendly elliptic curves over prime fields

(i) $K = 3$

(a) Examples of elliptic curve parameters when $k = 3$, $\rho \approx 1$

Compared to the previous work, when $k = 3$ by our method more non-supersingular elliptic curves are found with larger values of cofactor h. In the follows we just list the parameters of some pairing-friendly elliptic curves based on each of the polynomial family in Table 5. For finding the parameters, we use the same technique as [4]. We allow r to contain a small factor m as $r = m \times s$ where s should be larger than 2^{160}.

$r(x) = x^2 + x + 1$, $q(x) = 6x^2 + 5x + 5$, $t(x) = -x$, $D(x)V^2(x) = 23x^2 + 20x + 20$, $h = 6$, $2^{1024} \le q^3$ and $r \ge 2^{160}$

$x = 1079923412538715944704951959492080432089925874271352026133091 74$

$r = 4899712953685875055139525402636302811784603409474926240720857465007848152145335260669092529850214195676660317018095683 1$ (395 bits)

$q = 6997407461695593998996189855165372589382698528759788512455715277272564024743549617428788843364062677515667449188264654191953 1$ (415 bits)

$t = -1079923412538715944704951959492080432089925874271352026133091 74$

$h = 6 \times 238021$

$DV^2 = 4q - t^2 =$

$1603682 \times 40897592881002563202266719105773330301021350090175289056914 2^2$

$r(x) = 3x^2 + 3x + 1$, $q(x) = 18x^2 + 15x + 4$, $t(x) = -3x - 1$, $D(x)V^2(x) = 3(21x^2 + 18x + 5)$, $h = 6$, $2^{1024} \le q^3$ and $r \ge 2^{160}$

$x = -7803269225161850663624363079269799603063452211318 53$

$r = 1826730318010740876901135031721005164651782336711037944466914908602011966279821894586370822563570245269$ (340 bits)

$q = 1096038190806444526140681019032603098791069402026623000778225700016727088498785514845810585441708486717 1$ (343 bits)

$t = 2340980767548555199087308923780939880919035663395558$

$h = 6$

$DV^2 = 4q - t^2 = 745530 \times 71732225274287771987157605144916662896864519785 62^2$

$r(x) = 13x^2 + 7x + 1$, $q(x) = 78x^2 + 29x + 2$, $t(x) = -13x - 3$, $D(x)V^2(x) = 143x^2 + 38x - 1$, $h = 6$, $2^{1024} \le q^3$ and $r \ge 2^{160}$

$x = 2612356013890098680843339403952874560874523538571078 7$

$r = 1215304811821930833903776565440096058587329142741308962318614046195879548150258090279319414844077178910 59$ (346 bits)

$q = 532303507578005705249854135662762073661250164520693322099490134176666956$
$99347181840360497456482520422043607$ (355 bits)
$t = -339606281805712828509634122513873692913688060014240234$
$h = 6 \times 73$
$DV^2 = 4q - t^2 = 519518 \times 433411151813507633945516519621480619911397037747198^2$

$r(x) = 19x^2 + 15x + 3$, $q(x) = 114x^2 + 71x + 10$, $t(x) = -19x - 7$, $D(x)V^2(x) = 95x^2 + 18x - 9$,
$h = 6$, $2^{1024} \le q^3$ and $r \ge 2^{160}$
$x = 32080112686188098173033081593600049767482127240534213352609829 57$
$r = 10131367341560624124159630894722853518807436604069573531253929102953977 0$
$08083972914394427382094429458964567685189252777821738 73$ (419 bits)
$q = 11732123381527202735776852576089064374779011587512566149192049900611183 2$
$34323666769581118358186948367898808961879004663017986687 43$ (429 bits)
$t = -60952214103757386528762855027840094558216041757015005369958676190$
$h = 6 \times 193$
$DV^2 = 4q - t^2 =$
$282662 \times 588117326094371579915359858073132030725290723773999093015176342$

$r(x) = 21x^2 + 9x + 1$, $q(x) = 126x^2 + 33x + 1$, $t(x) = -21x - 4$, $D(x)V^2(x) = 3(21x^2 - 12x - 4)$,
$h = 6$, $2^{1024} \le q^3$ and $r \ge 2^{160}$
$x = -113997343431526234288179224027552262202892207632485046758$
$r = 27290328049835208694372567802926157949367366673185908831989786193829446 5$
$98833350073846791938456821800516600710102 3$ (377 bits)
$q = 16374196829901125216623540681755694769620420003911545299217811158418288 4$
$68500527681353861138136700443912782285880 51$ (380 bits)
$t = 23939442120620509200517637045785975062607363602821859819 14$
$h = 6$
$DV^2 = 4q - t^2 =$
$909258 \times 948902170567142950844442058755521395000319865489846926^2$

(b) Examples of elliptic curve parameters when $k = 3$, $\rho \approx 2$

When embedding degree $k = 3$, besides the quadratic relations between $q(x)$ and $t(x)$, we can easily find the following parameters from the families in Table 3. Here the value of D will always be effective as a constant number. In the following results we require that q is a multiple of 32 bits.

$r(x) = x^2 + x + 1$, $q(x) = x^4 + x^3 + 3x^2 + x + 1$, $t(x) = -x^2 - 2x - 1$, $D(x)V^2(x) = 3(x^2 + 1)^2$,
$h(x) = x^2 + 3$, $2^{1024} \le q^3$ and $r \ge 2^{160}$.
$x = 260244835333529706610404501$
$r = 67727374317775992040088322743872009225336773451463503$ (176 bits)
$q = 45869972319801430232217507544504292336769788875120440902188970753090267 8$
$24604496406470927013072541136630 07$ (352 bits)
$t = -67727374317775992040088323004116844558866480061868004$
$h = 67727374317775992040088322483627173891807066841059004$
$DV^2 = 4q - t^2 = 3 \times 677273743177759920400883224836271738918070668410590 02^2$

$x = 260244835333529706610427910$
$r = 67727374317775992040100506886572654419140859917396011$ (176 bits)
$q = 45869972319801430232234011544372848239088337842658529801639528158725025 4$
$06310607677705131652719066686132 11$ (352 bits)
$t = -67727374317775992040100507146817489752670566527823921$

$h = 677273743177759920401005066263278190856111533069681 03$
$DV^2 = 4q - t^2 = 3 \times 677273743177759920401005066263278190856111533069681 01^2$

(ii) $K = 4$

Example of elliptic curve parameters when $k = 4$, $\rho \approx 1$

When $k = 4$, we present two polynomial families with the feature of factorization in Table 7, which are not mentioned in any previous work. Many suitable elliptic curves can be built by implementing the two effective polynomial families. Here we still allow r to contain a small factor m as $r = m \times s$ and s > 2^{160}. In the last example q is a multiple of 32 bits and the curve built on such parameters should be has more efficiency.

$r(x) = 17x^2 + 8x + 1$, $q(x) = 136x^2 + 81x + 12$, $t(x) = 17x + 5$, $h = 8$, $D(x)V^2(x) = (3x + 1)(85x + 23)$, $2^{1024} \le q^4$ *and* $r \ge 2^{160}$

$x = -6731288020647602092682895980 4706092102631$
$r = 5925185023750280906815708112723341234279188615498999846480120385169564 77569955813$ *(269 bits)*
$q = 6162192424700292143088336437232274883650344716929324739415767639653180 56669188300797$ *(279 bits)*
$t = -1144318963510092355756092316680003565744722$
$h = 8 \times 130$
$DV^2 = 4q - t^2 = 266731 \times 208128482307701088003539877312972794082 8^2$

$x = -9405634957774243698856192716015662918613 5$
$r = 7519607361506916419079747342310141895055303068196831676208925946301012 8529531280373$ *(276 bits)*
$q = 1203137177841106627052759574769622703208846891953550246571999345855400 333809804321677$ *(280 bits)*
$t = -1598957942821621428805552761722662696164290$
$h = 8 \times 2$
$DV^2 = 4q - t^2 = 119787 \times 433963662020325640481812996706222816817 2^2$

For having higher security level, we present the parameters as:

$x = -1191231690501534684074243649437898746390327246677964774589 85$
$r = 1652298629297085617848695856186140169665550038963509848341262698195486 0442924939858614293999309712603126705347140633 01$ *(390 bits)*
$q = 1929884799018996001647276760025411718169362445509379502862592806398453 8471246700492719454946915055684888798320059091328 27$ *(400 bits)*
$t = -2025093873852608962926214204044427868863556319352540116802740$
$h = 8 \times 292$
$DV^2 = 4q - t^2 =$
$270127 \times 366001049745597827127017488777362962066062370523714438459 8^2$

For finding q as a multiple of 32 bits, we present the parameter as:

$x = -4117985507219224624463967678092656335927903512156327$
$r = 1031570453160913082118019225803267933731225489542551093088190705057349 5685372961857387341289776059793$ *(333 bits)*

$q = 230626143072279015942961322274385005408422620246049055778965257275579666$
$75000118089572154066982944291438 69$ (352 bits)
$t = -70005753622726818615887450527575157710774359706657554$
$h = 8 \times 27946$
$DV^2 = 4q - t^2 = 119715 \times 190055577453099347270402177323099262507559414738572^2$

(iii) $K = 6$

(a) Examples of elliptic curve parameters when $k = 6$, $\rho \approx 1$

$r(x) = 52x^2 + 14x + 1$, $q(x) = \zeta_{q\_k}(x) = 208x^2 + 30x + 1$, $t(x) = \zeta_{(t-1)\_k}(x) + 1 = -26x - 2$,
$D(x)V^2(x) = 4x(39x + 4)$, $2^{1024} \le q^6$ and $r \ge 2^{160}$
$x = -76678828867367445744045$
$r = 3057414254164932023616894874399758896057136086 71$ (158 bits)
$q = 1222965701665972809446759943409454109976443779851$ (160 bits)
$t = 1993649550551553589345168$
$h = 4$
$DV^2 = 4q - t^2 = 717595 \times 1130571591118871561262^2$

This example had been presented in [1]. The family had been proposed in [3]. By using our method, the same results are also found. After finding more quadratic relations between $q(x)$ and $t^2(x)$ with the feature of factorization, more suitable parameters of non-supersingular elliptic curves are obtained as the follows. Here r is allowed to contain a small factor and thus the cofactor h has increased.

$r(x) = 4x^2 + 2x + 1$, $q(x) = 24x^2 + 14x + 7$, $t(x) = 2x + 2$, $D(x)V^2(x) = 4(23x^2 + 12x + 6)$, $h = 6$, $2^{1024} \le q^6$ and $r \ge 2^{160}$
$x = -16691737029853261335736531584463$
$r = 3714854467650327660106439805064969874185849085606049453829415 17$ (208 bits)
$q = 6686738041770589788191591649116912390060468647568217543829778381$
(213 bits)
$t = -33383474059706522671473063168924$
$h = 6 \times 3$
$DV^2 = 4q - t^2 = 889673 \times 169738454027997300624006123326^2$

$r(x) = 4x^2 + 2x + 1$, $q(x) = 32x^2 + 18x + 9$, $t(x) = 2x + 2$, $D(x)V^2(x) = 4(31x^2 + 16x + 8)$, $h = 8$, $2^{1024} \le q^6$ and $r \ge 2^{160}$
$x = 667006492228484628797618935$
$r = 1779590642699790102050596774018164008195602559477374771$ (181 bits)
$q = 1423672514159832081640477419347932505002178973341423 6039$ (184 bits)
$t = 133401298445696925759523 7872$
$h = 8$
$DV^2 = 4q - t^2 = 457543 \times 109805715446199105092823 02^2$

(b) Examples of elliptic curve parameters when $k = 6$, $\rho \approx 2$

To find simpler examples, we start from more restrict condition. We require that $D(x)V^2(x) = 4q(x) - t(x)^2$ can be factorized as one square polynomial multiplying with one constant number. This is such a restrict condition and we loose the value of $lg(q)/lg(r)$ to about 2. In the following example, we used the families in Table 2 and the value of x only needs to satisfy that $q(x)$ and $r(x)$ are prime numbers since $4q(x) - t^2(x)$ is always effective for generating small values of D. In such situations we can

easily find the suitable x, which is satisfied with other efficient conditions, e.g. q is a multiple of 32 bits.

$r(x) = 3x^2 - 3x + 1$, $q(x) = 9x^4 - 9x^3 + 9x^2 - 3x + 1$, $t(x) = 3x^2 + 1$, $h(x) = 3x^2 + 1$, $D(x)V^2(x) = 3(3x^2 - 2x + 1)^2$, $2^{1024} \le q^6$ and $r \ge 2^{160}$.
$x = 60446290980731458735 6303$
$r = 109612622799817718866442190067866594118825941 4519$ (160 bits)
$q = 120149270770551192137275958192710646407010077402658082075856510602661207$
$93674766836822171625745 59$ (320 bits)
$t = 109612622799817718866442371406739536313202148 3428$
$h = 109612622799817718866442371406739536313202148 3428$
$DV^2 = 4q - t^2 = = 3 \times 109612622799817718866442250514157574850284677082 2^2$

With the above results, certain non-supersingular ellitptic curves suitable for pairing-based cryptosystems can be easily obtained by using CM method. More importantly, when changing the values of x, these polynomial families can produce different elliptic curves.

(iv) *K = 12*

(a) Examples of elliptic curve parameters when *k = 12*, $\rho \approx 1$

By our new method, we also find the perfect polynomial family [17] when $k = 12$ and $\rho \approx 1$ as $q(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$, $r(x) = 4x^4 + 4x^3 + 2x^2 + 2x + 1$, $t(x) = 6x^2 + 1$ and $D(x)V^2(x) = 3(6x^2 + 4x + 1)^2$. But since in [17] the authors already have implemented the family nicely to obtain many efficient non-supersingular elliptic curves, we will not list any examples for this special family.

(b) Examples of elliptic curve parameters when *k = 12*, $\rho > 1$

When $k = 12$, it is unlikely to find quadratic relations between $q(x)$ and $t(x)$. Then as the families presented in Table 10 and Table 11, we must set up extended versions of Pell equation. When $k = 12$ and $\rho \approx 1.5$, when $4q(x) - t^2(x)$ only contains the terms with even degree, we still can get Pell equations. The follows is an example based on the first family in Table 10.

$r(x) = x^4 - x^2 + 1$
$q(x) = x^6 + 2x^5 - 2x^3 + x + 1$
$t(x) = -x + 1$
$4q(x) - t^2(x) = (x + 1)^2(4x^4 - 4x^2 + 3)$

Since the square polynomial $(x + 1)^2$ does not need to be considered in the computation, we can easily get the Pell equation by replacing x^2 with y as $(2y - 1)^2 - DV^2 = -2$. Then after solving the above Pell equation for small values of D and prime q and r, we can obtain the desired parameters.

When $k = 12$ and $\rho \approx 2$, for the families presented in Table 11, the same procedure can be taken. The follows is an example of setting up a Pell equation based on the first family in Table 11. Here we replace x^3 with y.

$r(x) = x^4 - x^2 + 1$
$q(x) = x^8 + 2x^7 + x^6 + x^2 + x + 1$
$t(x) = -x + 1$
$4q(x) - t^2(x) = (x + 1)^2(4x^6 + 3)$

$(2y)^2 - DV^2 = -3$

Appendix B: Pairing-friendly elliptic curves over extension fields

In the follows we list some parameters of pairing-friendly elliptic curves over certain Optimal Extension Fields (OEFs) when $k = 3$. The parameters are obtained based on the database presented in [24].

(i) $q = p^4$

$p = 2^{57} - 195 = 144115188075855677$

$q = p^4 = 43135914667440790205349670351949492559699401588091475073897678233224 1$ (228 bits)

$t = p^2 = 207691874341392543091986357331283 29$

$r = 122874125597163357821467314214711541991863453844944657435437$

(ii) $q = p^8$

$p = 2^{31} - 19 = 2147483629$

$q = p^8 = 45231281656833071252167719388766558384942564306920621502449032930401115216 1$ (248 bits)

$t = p^4 = 212676471798911200698615628211789488 81$

$r = 154736708972129134182485557066869220547055437858402651666572 9$