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 had been proposed when embedding degree k and cofactor h were 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 perfect pairing-friendly elliptic curves over extension fields, e.g. F_{q^2}.

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], selecting suitable elliptic curves for pairing-based cryptosystems is one of the most important issues 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, for pairing-based cryptosystems. 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 for producing 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, extended versions of Pell equations are found 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 method 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 the new method. 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. Some parameters of several 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 elliptic curves suitable for pairing-based cryptosystems [10], we need

$$r^2 \mid \#E(F_q) \tag{1}$$

$$r \mid q^k - 1 \tag{2}$$

However, under a mild condition [6], we can just consider q as kth roots of unity modulo r, like what had been done in [7]. Meanwhile since k should be the smallest integer satisfying the conditions, equation (2) 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

$$dr = \Phi_k(q) \tag{3}$$

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

$$d'r \neq \Phi_i(q),\ 0 < i < k \tag{4}$$

Besides these conditions we still need

$$hr = q + 1 - t \quad (5)$$

where h is an integer. By combining equation (3) and (5) together, we can get

$$sr = \Phi_k(t - 1) \quad (6)$$

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

$$s'r \neq \Phi_i(t - 1),\ 0 < i < k \quad (7)$$

By Hasse's bound we also need

$$|t| \leq 2q^{1/2} \quad (8)$$

Then we can compute the elliptic curve by solving

$$DV^2 = 4q - t^2 \quad (9)$$

where D is chosen by certain conditions [2]. For solving equation (9), 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 (9) may be transformed into a well known Pell equation [4] as

$$y^2 - uDV^2 = m \quad (10)$$

where D should 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 follows we give a Lemma which proves that in polynomial field, equation (4) and (7) are already both efficient and necessary conditions. In polynomial field equation (5) and (8) 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 (3, 5, 6, 8, 9) are required and they can be rewritten as:

$$d(x)r(x) = \Phi_k(q(x)) \quad (11)$$

$$h(x)r(x) = q(x) + 1 - t(x) \quad (12)$$

$$s(x)r(x) = \Phi_k(t(x) - 1) \quad (13)$$

$$|t(x)| < 2q(x)^{1/2} \quad (14)$$

$$D(x)V(x)^2 = 4q(x) - t^2(x) \tag{15}$$

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

In the following section the math evidence for our new method is first provided. As proposed in [8], from equation (5) and (9) we can get the difference between $4q$ and t^2 after knowing t and r:

$$DV^2 = 4q - t^2 = 4(hr + t - 1) - t^2 \equiv -(t-2)^2 \bmod r \tag{16}$$

Represented in polynomial field, we have

$$D(x)V^2(x) = 4q(x) - t^2(x) = -(t(x) - 2)^2 \bmod r(x) \tag{17}$$

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

$$q(x) = [D(x)V^2(x) + t^2(x)]/4 \tag{18}$$

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. Thus in the follows 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 also satisfy that $\Phi_k(q(x)) \equiv 0 \bmod r(x)$. If the obtained $q(x)$ is according to all the conditions, then 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 when D is a “small” integer ($D \le 10^{10}$) [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 $D(x)V^2(x) = 4q(x) - t^2(x)$ in polynomial field. Since when $D(x)V^2(x)$ is an arbitrary polynomial, to find valid values of D is very difficult when q and r are secure parameters. In the following parts we will discuss different forms of $D(x)V^2(x)$ that can be used to produce parameters of pairing-friendly elliptic curves efficiently.

Before the discussion we need to mention a observation that when $q(x)$, $t(x)$ and $r(x)$ are suitable polynomial families that can be used to generate pairing-based cryptosystems, then $q(-x)$, $t(-x)$ and $r(-x)$ are such polynomial families too. This observation comes from the fact that in the operation x can be taken as either positive or negative values.

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 the parameter D will always equal the constant integer. It is rather easy to find such x. The beauty for finding such polynomial families is that in the paring-based cryptosystems based on these polynomial families we have better possibilities to find certain x satisfying certain conditions which makes the computation of the systems more efficient, such as the compressed pairing [18].

The work of Barreto and Naehrig [17] gave us a perfect example of such polynomial families when $k = 12$. For finding such polynomials they claimed to use the condition that $\Phi_k(t(x) - 1) = r(x)r(-x)$. When $k = 12$, they got from [3] that $t(x) - 1$ only could be $2x^2$ or $6x^2$ when $\Phi_k(t(x) - 1)$ is the multiple of two quadratic polynomials as $r(x)$ and $r(-x)$. But as the lemma proposed in [19], $-2x^2$ and $-6x^2$ also can be used as the possible polynomial with the feature of splitting. This generates the results tabulated in Table 1.

t(x)	**r(x)**	**q(x)**	**4q(x) – t²(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. Actually $\Phi_k(t(x) - 1) = r(x)r(-x)$ may not be a necessary condition to find such polynomial families. When $k = 6$, in Table 2 we list some polynomials of $r(x)$, $q(x)$ and $t(x)$, where $4q(x) - t^2(x) = DV^2(x)$ but $\Phi_k(t(x) - 1) \neq r(x)r(-x)$. 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) – t²(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 best form of $4q(x) - t^2(x) = DV(x)$ will always lead to a small D. This gives us better possibilities to search suitable x with other efficient conditions such as [18]. For finding such results, in the following we will propose a Lemma which can be used to find the same polynomial family in Table 1 easily.

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 $q(x) = q_nx^n + q_{n-1}x^{n-1} + ... + q_1x + q_0$, $t(x) = t_nx^n + t_{n-1}x^{n-1} + ... + t_1x + t_0$, then $4q_n - t_n^2$ and $4q_0 - t_0^2$ can be factorized as one constant number multiplying with one square number.

Proof: Assuming $q(x) = q_nx^n + q_{n-1}x^{n-1} + ... + q_1x + q_0$, $t(x) = t_nx^n + t_{n-1}x^{n-1} + ... + t_1x + t_0$, $V(x) = v_nx^n + v_{n-1}x^{n-1} + ... + v_1x + v_0$, when $4q(x) - t^2(x) = DV(x)$, since $4q_n - t_n^2 = Dv_n^2$ and $4q_0 - t_0^2 = Dv_0^2$, we can have the above conclusion. □

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 $q_n = a^2$, $t_{n/2} = a$ and $q_0 = b^2$, $t_0 = b$, where a, b are integers. In such case, $4q_n - t_{n/2} = 3a^2$ and $4q_0 - t_0^2 = 3b^2$ and m/n just equals a/b. In these situations 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 more such polynomial families when $k = 3$ and 4. Table 3 and Table 4 tabulate the results.

q(x)	t(x)	r(x)	4q(x) – t²(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) – t²(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 as the conditions proposed by [17] for finding the special forms of polynomial $t(x)$ with $\Phi_k(t(x) - 1) = r(x)r(-x)$, the value of k can not be 3, 4 or 6. If we want $\rho = lg(q)/lg(r) \approx 1$, the degree of $q(x)$ must equal with that of $r(x)$. Then since equation (8) 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 of $r(x)r(-x)$. 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 previous work had been proposed in [1, 3, 8]. In this section, we will propose the ideas of effective Pell equations and extended versions of Pell equations. The first idea gives the definition of certain Pell equations which have a better chance to generate pairing-friendly non-supersingular elliptic curves and the second idea 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 $r(x)$ is a polynomial family of a non-supersingular elliptic curves with embedding degree $k = 6$. Then use $2 - t(x)$ as another trace polynomial $t'(x)$, with same $r(x)$ we can find a families 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 $\Phi_6(t(x) - 1) = (t(x) - 1)^2 - (t(x) - 1) + 1 = t^2(x) - 3t(x) + 3 \equiv 0 \bmod r(x)$. Then use $2 - t(x)$ 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, $2 - t(x)$ and $r(x)$ can set up a valid polynomial family of a non-supersingular elliptic curve 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. But due to the security reason, special forms of families should be considered.

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 (5) 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 $q(x)$ and $r(x)$. 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 $DV^2 = ax^2 + bx + c = (a_1x + c_1)(a_2x + c_2)$, 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. In such situations we just need to find the suitable values of D and V where $c - DV^2$ can be factorized as d_1d_2 and $a_1d_2 + a_2d_1 = b$, $a_1 \mid d_1$ and $a_2 \mid d_2$. This is actually the other "lucky" family mentioned in [3].

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.

(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 give two families with the feature of factorization when $k = 3$, $\rho = lg(q)/lg(r) \approx 1$. Both of them should have a better chance for generating pairing-friendly elliptic curves.

h	**q(x)**	**t(x)**	**r(x)**	**4q(x) – t²(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 a non-supersingular elliptic curve in Appendix A.

h	**q(x)**	**t(x)**	**r(x)**	**4q(x) – t²(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 $k = 6, h > 5 \text{ and } \rho \approx 1$

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) – t²(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	**$279x^2 + 130x + 15$**	**$31x + 7$**	**$31x^2 + 11x + 1$**	**$(5x + 1)(31x + 11)$**
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 certain Pell equation. 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 may be found when k > 6. Here we should mention one useful observation. 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:

$$4q(x) - t^2(x) = ax^{2i} + bx^i + c \tag{19}$$

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

$$DV^2 = ay^2 + by + c \tag{20}$$

Actually when $4q(x) - t^2(x)$ can be viewed as $y(x)^2 - c$, where $y(x)^2$ is any square polynomials and c is a constant number, the effective Pell equations may be established. 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 $k > 6$.

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

When $k = 12$, it is unlikely to find 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 obtained. Table 9 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 9: effective polynomial families when $k = 12$, $\rho \approx 1.5$

(e) 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 10 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 10: effective polynomial families when $k = 12$, $\rho \approx 2$

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 (8) 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 polynomial families with small degree $D(x)V^2(x)$.

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 non-supersingular elliptic curves in implementations.

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

Algorithm 2

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

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 certain 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 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 as $h \times m$.

Another issue we should point out is that when finding the effective polynomial families, testing different values of x, we could obtain different non-supersingular elliptic curves. 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 non-supersingular elliptic curves based on a same polynomial family. In their work the proposed results are special and unique; people can not get other results by their method.

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

In [17] the authors have proposed an open problem to find pairing-friendly elliptic curves over extension fields. In their work the authors used the condition as $\Phi_k(t(x) - 1) = r(x)r(-x)$ and found some square $q(x)$ as q^2 when $k = 5$. But since in their example $4q(x) - t^2(x)$ did not belong to any effective forms proposed above; finding valid values of D became a hard problem. In the follows we will propose the effective polynomial families, which can be used to find the pairing-friendly elliptic curves over extension field when $k = 3$.

To find the elliptic curves over extension fields, $q(x)$ is not an irreducible polynomial but a polynomial with integer degree. Assuming to find $q(x)$ as a square polynomial, then we can get pairing-friendly elliptic curves over $F_q{}^2$. For this purpose, we modify our algorithm as:

Algorithm 3
Input: embedding degree k, $q^k > 2^{1024}$ and $r > 2^{160}$
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 $D(x)V^2(x) = 4q(x) - t^2(x) \equiv -(t^2(x) - 2)^2 \bmod r(x)$. 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 $q(x)$ is a square polynomial.
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 certain 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 x_0 and parameters, set up different elliptic curves.
8. If no elliptic curves are found, repeat from step 1

As a result, we find some effective polynomial families for pairing-friendly elliptic curves over F_{q^2}, where $q(x)$ is a square polynomial and $D(x)V^2(x)$ can be factorized as one constant number multiplying with a square polynomial. This means the values for D are always valid. Also the families we found have near-prime orders or prime orders. In Table 11 we list some of these effective polynomial families:

q(x)	r(x)	h	t(x)	DV²(x)
$(3x + 1)^2$	$3x^2 + 3x + 1$	3	$-3x - 1$	$3(3x + 1)^2$
$(4x - 1)^2$	$16x^2 - 4x + 1$	1	$-4x + 1$	$3(4x - 1)^2$
$(3x - 1)^2$	$9x^2 - 3x + 1$	1	$-3x + 1$	$3(3x - 1)^2$
$(2x - 1)^2$	4x^2 – 2x + 1	1	$-2x + 1$	$3(2x - 1)^2$

Table 11: effective polynomial families of elliptic curves over extension field

In Appendix B we will present some parameters of certain pairing-friendly elliptic curves over extension fields based on the families proposed above.

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.

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}.

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

$x = 1079923412538715944704951959492080432089925874271352026133091 74$

$r = 48997129536858750551395254026363028117846034094749262407208574650078481 5$
$2145335260669092529850214195676660317018095683 1$ (395 bits)

$q = 699740746169559399899618985516537258938269852875978851245571527727256402$
$474354961742878884336406267751566744918826465419195 31$ (415 bits)

$t = -107992341253871594470495195949208043208992587427135202613309174$

$h = 6 \times 238021$

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

$1603682 \times 4089759288100256320226671910577333030102135009017528905691422^2$

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

$x = -78032692251618506636243630792697996030634522113185 3$

$r = 182673031801074087690113503172100516465178233671103794446691490860201196$
$627982189458637082256357024526 9$ (340 bits)

$q = 109603819080644452614068101903260309879106940202662300077822570001672708$
$849878551484581058544170848671 71$ (343 bits)

$t = 234098076754855519908730892378093988091903566339555 8$

$h = 6$

$DV^2 = 4q - t^2 = 745530 \times 717322252742877719871576051449166628968645197856 2^2$

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

$x = 261235601389009868084333940395287456087452353857107 87$

$r = 121530481182193083390377656544009605858732914274130896231861404619587954$
$815025809027931941484407717891059$ (346 bits)

$q = 532303507578005705249854135662762073661250164520693322099490134176666956$
$993471818403604974564825204220436 07$ (355 bits)

$t = -3396062818057128285096341225138736929136880600142402 34$

$h = 6 \times 73$

$DV^2 = 4q - t^2 = 519518 \times 4334111518135076339455165196214806199113970377471 98^2$

$r(x) = 19x^2 + 15x + 3$, $q(x) = 114x^2 + 71x + 10$, $t(x) = -19x - 7$, $D(x)V^2(x) = 95x^2 + 18x - 9$, $h = 6$, $2^{1024} < q^3$ and $r > 2^{160}$

$x = 320801126861880981730330815936000497674821272405342133526098295 7$

$r = 101313673415606241241596308947228535188074366040695735312539291029539770$
$080839729143944273820944294589645676851892527778217387 3$ (419 bits)

$q = 117321233815272027357768525760890643747790115875125661491920499006111832$
$343236667695811183581869483678988089618790046630179866874 3$ (429 bits)

$t = –60952214103757386528762855027840094558216041757015005369958676190$
$h = 6 \times 193$
$DV^2 = 4q – t^2 =$
$282662 \times 58811732609437157991535985807313203072529072377399909301517634^2$

$r(x) = 21x^2 + 9x + 1$, $q(x) = 126x^2 + 33x + 1$, $t(x) = –21x – 4$, $D(x)V^2(x) = 3(21x^2 – 12x – 4)$, $h = 6$, $2^{1024} < q^3$ and $r > 2^{160}$
$x = -113997343431526234288179224027552262202892207632485046758$
$r = 272903280498352086943725678029261579493673666731859088319897861938294465$
$988333500738467919384568218005166007101023$ (377 bits)
$q = 163741968299011252166235406817556947696204200039115452992178111584182884$
$6850052768135386113813670044391278228588051$ (380 bits)
$t = 2393944212062050920051763704578597506260736360282185981914$
$h = 6$
$DV^2 = 4q – t^2 =$
$909258 \times 948902170567142950844442058755521395000319865489846926^2$

(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)
$q = 458699723198014302322175075445042923367697888751204409021889707530902678$
$2460449640647092701307254113663007$ (352 bits)
$t = – 67727374317775992040088323004116844558866480061868004$
$h = 67727374317775992040088322483627173891807066841059004$
$DV^2 = 4q – t^2 = 3 \times 67727374317775992040088322483627173891807066841059002^2$

$x = 260244835333529706610427910$
$r = 67727374317775992040100506886572654419140859917396011$ (176 bits)
$q = 458699723198014302322340115443728482390883378426585298016395281587250254$
$0631060767770513165271906668613211$ (352 bits)
$t = –67727374317775992040100507146817489752670566527823921$
$h = 67727374317775992040100506626327819085611153306968103$
$DV^2 = 4q – t^2 = 3 \times 67727374317775992040100506626327819085611153306968101^2$

(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.

$r(x) = 17x^2 + 8x + 1$, $q(x) = 136x^2 + 81x + 12$, $t(x) = 17x + 5$, $h = 16$ $D(x)V^2(x) = (3x + 1)(85x + 23)$, $2^{1024} \leq q^4$ and $r \geq 2^{160}$

$x = –67312880206476020926828959804706092102631$
$r = 59251850237502809068157081127233412342791886154989998464801203851695647 7569955813$ (269 bits)
$q = 61621924247002921430883364372322748836503447169293247394157676396531805 6669188300797$ (279 bits)
$t = –1144318963510092355756092316680003565744722$
$h = 8 \times 130$
$DV^2 = 4q – t^2 = 266731 \times 2081284823077010880035398773129727940828^2$

$x = –940563495777424369885619271601566291 86135$
$r = 75196073615069164190797473423101418950553030681968316762089259463010128 529531280373$ (276 bits)
$q = 12031371778411066270527595747696227032088468919535502465719993458554003 33809804321677$ (280 bits)
$t = –15989579428216214288055527617226626961 64290$
$h = 8 \times 2$
$DV^2 = 4q – t^2 = 119787 \times 43396366202032564048181299670622281 68172^2$

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

$x = –1191231690501534684074243649437898746390327246677964774589 85$
$r = 16522986292970856178486958561861401696655500389635098483412626981954860 442924939858614293999309712603126705347140633 01$ (390 bits)
$q = 19298847990189960016472767600254117181693624455093795028625928063984538 47124670049271945494691505568488879832005909132827$ (400 bits)
$t = –2025093873852608962926214204044427868863556319352540116802740$
$h = 8 \times 292$
$DV^2 = 4q – t^2 =$
$270127 \times 3660010497455978271270174887773629620660623705237144384598^2$

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

$x = –4117985507219224624463967678092656335927903512156327$
$r = 10315704531609130821180192258032679337312254895425510930881907050573495 6853729618573873412897760597 93$ (333 bits)
$q = 23062614307227901594296132227438500540842262024604905577896525727557966 6750001180895721540669829442914 3869$ (352 bits)
$t = –70005753622726818615887450527575157710774359706657554$
$h = 8 \times 27946$
$DV^2 = 4q – t^2 = 119715 \times 1900555774530993472704021773230992625075594147385 72^2$

(iii) *K* = 6

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

$r(x) = 52x^2 + 14x + 1$, $q(x) = \zeta_{q\_k}(x) = 208x^2 + 30x + 1$, $t(x) = \zeta_{(t-1)\_k}(x) + 1 = –26x – 2$, $D(x)V^2(x) = 4x(39x + 4)$, $2^{1024} < q^6$ and $r > 2^{160}$
$x = –766788288673674457440 45$
$r = 305741425416493202361689487439975889605713608671$ (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.

$r(x) = 4x^2 + 2x + 1$, $q(x) = 24x^2 + 14x + 7$, $t(x) = 2x + 2$, $D(x)V^2(x) = 4(23x^2 + 12x + 6)$, $h = 6$, $2^{1024} \leq q^6$ and $r \geq 2^{160}$
$x = -1669173702985326133573653158446 3$
$r = 371485446765032766010643980506496987418584908560604945382941517$ *(208 bits)*
$q = 6686738041770589788191591649116912390060468647568217543829778381$
(213 bits)
$t = -3338347405970652267147306316892 4$
$h = 6 \times 3$
$DV^2 = 4q - t^2 = 889673 \times 1697384540279973006240061233 26^2$

$r(x) = 4x^2 + 2x + 1$, $q(x) = 32x^2 + 18x + 9$, $t(x) = 2x + 2$, $D(x)V^2(x) = 4(31x^2 + 16x + 8)$, $h = 8$, $2^{1024} \leq q^6$ and $r \geq 2^{160}$
$x = 667006492228484628797618935$
$r = 1779590642699790102050596774018164008195602559477374771$ *(181 bits)*
$q = 14236725141598320816404774193479325050021789733414236039$ *(184 bits)*
$t = 1334012984456969257595237872$
$h = 8$
$DV^2 = 4q - t^2 = 457543 \times 1098057154461991050928230 2^2$

(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.

$r(x) = 3x^2 - 3x + 1$, $q(x) = 9x^4 - 9x^3 + 9x^2 - 3x + 1$, $t(x) = 3x^2 + 1$, $h(x) = 3x^2 +1$, $D(x)V^2(x) = 3(3x^2 - 2x + 1)^2$, $2^{1024} \leq q^6$ and $r \geq 2^{160}$.
$x = 604462909807314587356303$
$r = 1096126227998177188664421900678665941188259414519$ *(160 bits)*
$q = 1201492707705511921372759581927106464070100774026580820758565106026612079367476683682217162574559$ *(320 bits)*
$t = 1096126227998177188664423714067395363132021483428$
$h = 1096126227998177188664423714067395363132021483428$
$DV^2 = 4q - t^2 = = 3 \times 1096126227998177188664422505141575748502846770822^2$

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 8 and Table 9, 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 8.

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

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 9, the same procedure can be taken. The follows is an example of setting up a Pell equation based on the first family in Table 9. 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 square field F_q^2 when $k = 3$. The parameters are obtained based on the second and third families in Table 11. Many other non-supersingular elliptic curves over extension field can also be found by our proposed families. In the following results, we require that q is a multiple of 32 bits for the efficiency of computation of elliptic curve operations.

$q(x)^2 = 9x^2 - 6x + 1 = (3x - 1)^2$, $t(x) = -3x + 1$, $r(x) = 9x^2 - 3x + 1$, $h = 1$, $DV^2 = 3(3x - 1)^2$, $2^{1024} \leq q^3$ and $r \geq 2^{160}$
$x = 1569275433846670190958947355801916604025588861116008640328$

$q = 4707826301540010572876842067405749812076766583348025920983$ (192 bits)
$r = 2216362848547189455690696005633078276535735333963681409261738453662840633050208243012829337082378463043741338560 7273$ (384 bits)
$t = -4707826301540010572876842067405749812076766583348025920983$
$h = 1$
$DV^2 = 3 \times 4707826301540010572876842067405749812076766583348025920983^2$

$x = 1569275433846670190958947355801916604025588861116008647110$
$q = 4707826301540010572876842067405749812076766583348025941329$ (192 bits)
$r = 22163628485471894556906960056330782765357353339636814284188252398894516562006539837003064723851570440035284576227571$ (384 bits)
$t = -4707826301540010572876842067405749812076766583348025941329$
$h = 1$
$DV^2 = 3 \times 4707826301540010572876842067405749812076766583348025941329^2$

$q(x)^2 = 16x^2 - 8x + 1 = (4x - 1)^2$, $t(x) = -4x + 1$, $r(x) = 16x^2 - 4x + 1$, $h = 1$, $DV^2(x) = 3(4x - 1)^2$, $2^{1024} \leq q^3$ and $r \geq 2^{160}$
$x = 784637716923335095479473677900958302012794430558004330460$
$q = 3138550867693340381917894711603833208051177722232017321839$ (192 bits)
$r = 985050154909861980306976002503590345126993481761636207745617148059956561124232672053768501227840495\ 6871574123663761$ (384 bits)
$t = -3138550867693340381917894711603833208051177722232017321839$
$h = 3$
$DV^2 = 3 \times 3138550867693340381917894711603833208051177722232017321839^2$

$x = 784637716923335095479473677900958302012794430558004345091$
$q = 3138550867693340381917894711603833208051177722232017380363$ (192 bits)
$r = 985050154909861980306976002503590345126993481761636244481727344236967063396806692434315434825265498\ 8684741035392133$ (384 bits)
$t = -\ 3138550867693340381917894711603833208051177722232017380363$
$h = 3$
$DV^2 = 3 \times 3138550867693340381917894711603833208051177722232017380363^2$