

Finding More Non-Supersingular Elliptic Curves for Pairing-Based Cryptosystems

Pu Duan, Shi Cui, and Choong Wah Chan

Abstract—Finding suitable non-supersingular elliptic curves for pairing-based cryptosystems becomes an important issue for the modern public-key cryptography after the proposition of id-based encryption scheme and short signature scheme. In previous work different algorithms have been proposed for finding such elliptic curves when embedding degree $k \in \{3, 4, 6\}$ and cofactor $h \in \{1, 2, 3, 4, 5\}$. In this paper a new method is presented to find more non-supersingular elliptic curves for pairing-based cryptosystems with general embedding degree k and large values of cofactor h . In addition, some effective parameters of these non-supersingular elliptic curves are provided in this paper.

Keywords—Family of group order, k th root of unity, non-supersingular elliptic curves polynomial field.

I. INTRODUCTION

AFTER the proposition of identity-based encryption scheme [1] and short signature scheme [2], selecting suitable elliptic curves for pairing-based cryptosystems becomes one of the most important issues in public-key cryptography. Elliptic Curve Discrete Logarithm Problem (ECDLP) on such elliptic curves can be reduced to Discrete Logarithm Problem (DLP) over an extension field by Tate Pairing or Weil Pairing [10]. Thus supersingular elliptic curves appear as the nature choice [12]. However, because of the weakness of supersingular elliptic curves [3], [6], there is a need to find non-supersingular elliptic curves with the same features suitable for pairing-based cryptosystems.

In 2001, Miyaji *et al.* [4] first proposed a method to find suitable non-supersingular elliptic curves for pairing-based cryptosystems. Later Scott and Barreto [3] extended their work and found more suitable elliptic curves. Gallbraith *et al.* [7] summarized the method proposed by the early researchers and presented some families of group orders of non-supersingular elliptic curves suitable for pairing-based cryptosystems. Brezing and Weng [5] also proposed an alternative method to find such elliptic curves.

May 2, 2005.

Pu Duan is with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore (phone: +65(90702346); e-mail: pg03460751@ntu.edu.sg).

Shi Cui is with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore (e-mail: pg04063705@ntu.edu.sg).

Choong Wah Chan is with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore (e-mail: ecwchan@ntu.edu.sg).

In this paper we propose a new method for finding more 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 the proposed method some effective parameters are found and thus elliptic curves can be generated by Complex Multiplication (CM) method [8].

This paper is organized as the follows. In sections 2 we give an analysis of previous work on finding suitable non-supersingular elliptic curves for pairing-based cryptosystems. In section 3 we describe the new method and discuss certain important features. In section 4 some effective parameters of non-supersingular elliptic curves are provided with different values of embedding degree k [4] and cofactor h [3]. Finally, we draw the conclusion in section 5.

II. ANALYSIS OF PREVIOUS WORK

To find suitable elliptic curves for pairing-based cryptosystems, certain equations are to be solved. Assume the cofactor h is an integer, r is the order of a point as a big prime and t is the trace of an elliptic curve, we want to find the elliptic curve over 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 F_q^k , where k is the embedding degree [12]. Certain conditions determine whether such an elliptic curve exists or not. They are described as the follows.

$$dr = \Phi_k(q) \quad (1)$$

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

$$hr = q + 1 - t \quad (2)$$

where h is an integer. By combining the above two equations together, we have

$$sr = \Phi_k(t - 1) \quad (3)$$

where s is also an integer [3]. Besides these equations we still need

$$|t| \leq 2\sqrt{q} \quad (4)$$

as the Hasse bound. With all the above equations we compute the elliptic curve by solving

$$DV^2 = 4q - t^2 \quad (5)$$

where D is chosen by certain conditions as outlined in [11].

When solving (5), it is desired to find quadratic relations between q and t , as the proposed families of group orders [7]. Then (5) can be transformed into a well known Pell equation

[9] as

$$y^2 - uDV^2 = m \quad (6)$$

where D should be a square free number.

Actually in the strict sense (1) can also be presented as $r \mid q^k - 1$ and $q^i - 1$ is not divisible by r when $i < k$. It is same for (3). However, under a mild condition [14], we can just consider q and $t - 1$ as kth roots of unity modulo r, like what had been done in [5]. The k should be the smallest integer satisfying the condition. This generates the equations as

$$q^k \equiv 1 \pmod{r} \quad (7)$$

and

$$(t - 1)^k \equiv 1 \pmod{r} \quad (8)$$

Miyaji *et al.* [4] first proposed the method to find non-supersingular elliptic curves suitable for pairing-based cryptosystems. As the reason pointed by [3], their method only could find the curves when embedding degree k was 3, 4, 6 and cofactor h was 1. Scott and Barreto [3] extended the work of Miyaji *et al.* In their paper more suitable elliptic curves were found when the embedding degree $k \in \{3, 4, 6\}$ and $h \in \{1, 2, 3, 4, 5\}$. They combined (1) and (3) into (5) and transformed (5) into a Pell equation. But because of the limitations for solving Pell equations, h was only taken from 1 to 5. Meanwhile since the Pell equation [3] could only be set up when $sr = \Phi_k(t - 1)$ is a quadratic equation, the embedding degree k needed to be in the range of $\{3, 4, 6\}$. Galbraith *et al.* [7] proposed the idea of suitable families of group orders of non-supersingular elliptic curves for pairing-based cryptosystems when $k \in \{3, 4, 6\}$. They found that when q and t were satisfying certain quadratic relations, as the families of group orders, numerous suitable elliptic curves could be produced by CM method. But there were same limitations in their work as embedding degree $k \in \{3, 4, 6\}$ and cofactor $h \in \{1, 2, 3, 4, 5\}$. Brezing and Weng [5] proposed an alternative way to find such non-supersingular elliptic curves. They used the equation $t = \zeta_{(t-1)_k} + 1$, where $\zeta_{(t-1)_k}$ was a kth root of unity modulo r. When r is presented by a cyclotomic polynomial, polynomial forms of t could be easily found. However since they only represented r as a cyclotomic polynomial, not all suitable non-supersingular elliptic curves were found by their method (e.g. the suitable examples proposed in [3]).

III. NEW METHOD FOR FINDING MORE NON-SUPERSINGULAR ELLIPTIC CURVES FOR PAIRING-BASED CRYPTOSYSTEMS

In this section we propose a new method for finding suitable non-suitable elliptic curves for pairing-based cryptosystems. First we deduce some useful equations. As proposed in [5], from (2) and (5) we can get the difference between $4q$ and t^2 after knowing t and r. It can be described as

$$DV^2 = 4q - t^2 \equiv -(t - 2)^2 \pmod{r} \quad (9)$$

where t should satisfy (8). Represented in polynomial field, we have

$$D(x)V^2(x) \equiv -(t(x) - 2)^2 \pmod{r(x)} \quad (10)$$

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

$$q(x) = [D(x)V^2(x) + t^2(x)]/4 \quad (11)$$

satisfies (7) should be tested. In polynomial field (7) can be written as

$$q^k(x) \equiv 1 \pmod{r(x)} \quad (12)$$

After finding the effective $q(x)$, we can directly solve

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

as a possible Pell equation if $D(x)V^2(x) = 4q(x) - t^2(x)$ is quadratic. Otherwise all values of x should be tested to satisfy that $q(x)$, $r(x)$ are prime numbers and meanwhile small values of D exist.

The main idea of our new method can be described as the follows. For finding suitable non-supersingular elliptic curves for pairing-based cryptosystems, 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 $V(x)$. At first we use an arbitrary irreducible polynomial $r(x)$ to represent prime r. Then by $(t(x) - 1)^k \equiv 1 \pmod{r(x)}$ we can find trace polynomials $t(x)$, where k should be the smallest integer with this condition. From $D(x)V^2(x) = 4q(x) - t^2(x) \equiv -(t(x) - 2)^2 \pmod{r(x)}$ we can compute $D(x)V^2(x)$ after knowing $t(x)$ and $r(x)$. Then the irreducible polynomial $q(x)$ can be obtained by $q(x) = [D(x)V^2(x) + t^2(x)]/4$. After that we test whether $q(x)$ satisfies $q(x)^k \equiv 1 \pmod{r(x)}$. If the $q(x)$ is effective, the $D(x)V^2(x)$ found above is valid. Now if $D(x)V^2(x) = 4q(x) - t^2(x)$ is a quadratic polynomial, a Pell equation as $DV^2 = 4q(x) - t^2(x)$ may be set up and suitable values of D can be found by solving this Pell equation; otherwise we must test all possible values of x to satisfy that $q(x)$ and $r(x)$ are prime numbers and small values of D exist in the same time. After finding all the parameters, the desired elliptic curve can be established by CM method [8].

In the follows we discuss some important features before the proposition of the new method.

A. Polynomial Field

Instead of searching in the integer field, finding the suitable parameters of the elliptic curves in the polynomial field is much more efficient. The reason is that q and r must be taken as secure parameters. For the security reason, $q^k > 2^{1024}$ [3] is taken. Meanwhile to resist Pohlig-Hellman attack [13], the group order should contain a prime factor larger than 160 bits. This gives another security condition as $r > 2^{160}$. Thus it is hard to solve the above equations in the integer field.

B. Selecting $r(x)$

When dealing the issue in polynomial field, prime r is represented as $r(x)$. Here $r(x)$ must be an irreducible polynomial since r is prime. Then how to determine the degree of $r(x)$ affects the whole searching procedure. As analyzed above, if we want $D(x)V^2(x) = 4q(x) - t^2(x)$ to be a quadratic polynomial, as the necessary condition to set up a Pell equation, we should have $\text{degree}(r(x)) \leq 2$. Different with [5], we regard $r(x)$ as any arbitrary irreducible polynomials.

C. Selecting $t(x)$

After assuming the form of irreducible polynomial $r(x)$, the trace polynomial $t(x)$ should satisfy $(t(x) - 1)^k \equiv 1 \pmod{r(x)}$. Considering (4), we can get $\text{degree}(t(x)) < \text{degree}(q(x))/2$. For the reason of good performance, we also require $\lg(q)/\lg(r) \leq 2$ [3] and then $\text{degree}(q(x)) \geq \text{degree}(r(x)) \geq \text{degree}(q(x))/2$ can be obtained. As a result, we should use $\text{degree}(t(x)) \leq \text{degree}(r(x))$.

D. Choosing different forms of $D(x)V^2(x)$

As the analysis given above, polynomial $D(x)V^2(x)$ can be obtained by $D(x)V^2(x) = 4q(x) - t^2(x) \equiv -(t(x) - 2)^2 \pmod{r(x)}$ 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 of $4q(x) - t^2(x)$. 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 of x to satisfy that $q(x)$ and $r(x)$ are prime numbers and meanwhile small values of D exist. In the latter case, since it is impossible to search the whole integer field, $D(x)V^2(x)$ must contain a square polynomial factor as $V^2(x)$, which means $\text{degree}(V(x)) > 0$; or degree of $D(x)V^2(x)$ is much smaller than the degree of $q(x)$. Then it is possible to find small values of D without solving any Pell equations.

Compared to suitable q and t , the values for D must be a rather small integer (e.g. $D < 10^{10}$) [3]. This is actually a very strict condition since meanwhile we need q and t as secure parameters. When $k = 6$, we require that $q^6 > 2^{1024}$ [3] and $r > 2^{160}$ [13]. This gives that $q > 2^{171} \approx 10^{51}$. Since $|t| < 2q^{1/2}$, (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 [3] and [7]. The authors [7] 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 [3]. Actually for the suitable families as the quadratic polynomial relations between $q(x)$ and $t(x)$, it needs that $4q(x) - t^2(x)$ can be factorized. This ensures larger possibility of the existence of small values of D . In fact when $q(x) = 208x^2 + 30x + 1$ and $t(x) = -26x - 2$, $D(x)V^2(x)$ equals $4q(x) - t^2(x)$ as $4x(39x + 4)$. Compared to $D(x)V^2(x)$ as any irreducible quadratic polynomials, it is easier to find values of x to make $q(x)$, $r(x)$ as prime numbers and meanwhile x or $39x + 4$ has a large square factor. In other words, when transformed into Pell equations, these quadratic equations with the feature of factorization are more likely to produce suitable values of D . However, $4q(x) - t^2(x)$ is always an irreducible quadratic polynomial [7]. It is very difficult to find suitable x to satisfy that $q(x)$ and $r(x)$ are prime numbers and $4q(x) - t^2(x)$ has a large square factor in the same time. The other "lucky" family pointed out by [7] also has this feature. The above analysis illustrates the fact that most of the families proposed by [7] are hard for implementation.

When the difference between $4q(x)$ and $t^2(x)$, as $D(x)V^2(x)$, is not a quadratic form, we must test all possible values of x to make $r(x)$ and $q(x)$ prime with the existence of small values of

D . Actually in such situation it is desired that $D(x)V^2(x) = 4q(x) - t^2(x)$ contains a factor as a square polynomial $V^2(x)$, which means $\text{degree}(V^2(x)) > 0$; otherwise $D(x)V^2(x)$ itself should only has terms with smaller degree compared to $q(x)$. Thus the degree of $D(x)$ will be small and effective values of D may exist. If the degree of $V(x)$ is large, small values of D can be obtained easily. This makes the computation of CM method more efficient.

With all of the analysis, now we give the whole algorithm for finding suitable non-supersingular elliptic curves for pairing-based cryptosystems.

Algorithm

Input: embedding degree k , $2^{1024} < q^k$ 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 $(t(x) - 1)^k \equiv 1 \pmod{r(x)}$, k is the embedding degree
- 3) Compute polynomial $D(x)V^2(x)$ by $D(x)V^2(x) = 4q(x) - t^2(x) \equiv -(t(x) - 2)^2 \pmod{r(x)}$. If $D(x)V^2(x)$ is taken as a quadratic polynomial, it should be represented as the $ax(bx + c)$ or $(ax + b)(cx + d)$; otherwise $\text{degree}(V(x)) > 0$ or $\text{degree}(D(x)V^2(x)) < 2\text{degree}(r(x))$ should be satisfied.
- 4) After obtaining $D(x)V^2(x)$, compute $q(x)$ by $q(x) = [D(x)V^2(x) + t^2(x)]/4$. Then test whether the irreducible polynomial $q(x)$ satisfy $q(x)^k \equiv 1 \pmod{r(x)}$
- 5) If the obtained effective $q(x)$ is a quadratic polynomial, set up and solve the possible Pell equation as $DV^2 = D(x)V^2(x) = 4q(x) - t^2(x)$; otherwise test all values of x to find x_0 satisfying that $q(x_0)$, $r(x_0)$ are prime numbers and meanwhile small values of D exist. The security conditions should be satisfied.
- 6) Output x_0 and $q(x)$, $t(x)$, $r(x)$, $D(x)V^2(x)$; otherwise repeat from step 1.

IV. EXPERIMENTAL RESULTS

In the implementation we run the above algorithm when $k = 6$ and $k = 12$. The following results are some effective parameters of non-supersingular elliptic curves. The programs are implemented on a PC with 1.7 GHz Pentium IV and 256Mb RAM.

$K = 6$

(1) $r(x) = 52x^2 + 14x + 1$, $q(x) = 208x^2 + 30x + 1$, $t(x) = -26x - 2$, $D(x)V^2(x) = 4x(39x + 4)$, $2^{1024} < q^6$ and $r > 2^{160}$

$x = -76678828867367445744045$

$r = 305741425416493202361689487439975889605713608671$

$q = 1222965701665972809446759943409454109976443779851$

$t = 1993649550551553589345168$

$h = 4$

$DV^2 = 4q - t^2 = 717595 \times 1130571591118871561262^2$

This example had been presented in [3]. The family of the group order had been proposed in [7]. 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 is enlarged.

$$(2) \quad r(x) = 13x^2 + 7x + 1, q(x) = 52x^2 + 41x + 8, t(x) = 13x + 5, \\ D(x)V^2(x) = (3x + 1)(13x + 7), 2^{1024} < q^6 \text{ and } r > 2^{160} \\ x = 156827708198894751651410401 \\ r = 1522543289361570673414220010509278243128375354583920 \\ 1 \\ q = 1278936363063719365667944810866553930813467069318828 \\ 101 \\ t = 2038760206585631771468335218 \\ h = 84 \\ DV^2 = 4q - t^2 = 5 \times 437995952560703356153167676^2$$

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, 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 .

$$(3) \quad r(x) = 3x^2 - 3x + 1, q(x) = 9x^4 - 9x^3 + 9x^2 - 3x + 1, t(x) = 3x^2 + 1, \\ D(x)V^2(x) = 3(3x^2 - 2x + 1)^2, 2^{1024} < q^6 \text{ and } r > 2^{160} \\ x = 1208925819614629174707026 \\ r = 4384504911992708754617216393051424823871277172951 \\ t = 4384504911992708754617220019828883667758801294029 \\ q = 192238833232881907416092449740846045864506803420131 \\ 72953010162927246286125473585503144906437903607 \\ DV^2 = 4q - t^2 = \\ 3 \times 4384504911992708754617217601977244438500451879977^2$$

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

$K = 3$

When embedding degree $k = 3$, besides the quadratic relations between $q(x)$ and $t(x)$, we find other results in which the values of D is always effective.

$$(4) \quad r(x) = x^2 + x + 1, q(x) = 3x^4 + 3x^3 + 4x^2 + 2x + 1, t(x) = -3x^2 - 2x - 2, \\ h(x) = 3x^2 + 4, D(x)V^2(x) = 3x^4, 2^{1024} < q^3 \text{ and } r > 2^{160} \\ x = 1208925819614629174710702 \\ r = 1461501637330902918214629238161254257574568043507 \\ q = 6407961107762730247281031416832094288669969321336719 \\ 105533822464081583120486986614959472949665093 \\ t = -4384504911992708754643886505557943158094529419818 \\ DV^2 = 4q - t^2 = \\ 3 \times 1461501637330902918214628029235434642945393332804^2$$

$K = 12$

When $k = 12$, it is unlikely to find quadratic relations between $4q(x)$ and $t^2(x)$ to set up Pell equations. But it is still possible to find certain forms of $D(x)V^2(x) = 4q(x) - t(x)^2$ with certain square polynomial factors. Thus small values of D can be obtained. The following examples are two of the results found

by our method.

$$(5) \quad r(x) = x^4 - x^2 + 1, t(x) = -x + 1, q(x) = x^6 + 2x^5 - 2x^3 + x + 1 \\ D(x)V^2(x) = (x + 1)^2(4x^4 - 4x^2 + 3), \lg(q)/\lg(r) \approx 1.5$$

$$(6) \quad r(x) = x^4 - x^2 + 1, t(x) = -x + 1, q(x) = x^8 + 2x^7 + x^6 + x^2 + x + 1, \\ D(x)V^2(x) = (x + 1)^2(4x^6 + 3), \lg(q)/\lg(r) \approx 2$$

Since the square polynomials contained in $D(x)V^2(x)$ can be ignored in implementations, when replacing x^2 or x^3 as y , certain Pell equations will be set up from the two examples and thus small values of D should be obtained.

V. CONCLUSION

In this paper, we describe a new method to find more non-supersingular elliptic curves for pairing-based cryptosystems without limitations on embedding degree k and cofactor h . The curves found in this paper are important for the realization of pairing-based cryptosystems over ordinary elliptic curves with desired parameters.

REFERENCES

- [1] D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing," *SIAM J. of Computing*, vol. 32, no.3, pp. 586-615, 2003.
- [2] 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.
- [3] M. Scott and P. S. L. M. Barreto, "Generating more MNT elliptic curves," *Cryptology ePrint Archive*, Report 2004/058, 2004.
- [4] 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.
- [5] F. Brezing and A. Weng, "Elliptic curves suitable for pairing based cryptography," *Cryptology ePrint Archive*, Report 2003/143, 2003.
- [6] D. Page, N. P. Smart and F. Vercauteren, "A comparison of MNT curves and supersingular curves," *Cryptology ePrint Archive*, Report 2004/165, 2004.
- [7] Steven D. Galbraith, J. Mckee and P. Valenca, "Ordinary abelian varieties having small embedding degree," *Cryptology ePrint Archive*, Report 2004/365, 2004.
- [8] 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.
- [9] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, Landon Mathematical Society Student Text 41, Cambridge University Press, 1998.
- [10] A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publisher, 1993
- [11] IEEE Computer Society, New York, USA, *IEEE Standard Specifications for Public Key Cryptography- IEEE Std 1363-2000*, 2000.
- [12] 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.
- [13] A. M. Odlyzko, Discrete logarithms: the past and the future. *Design, Codes and Cryptography*, 19:129-145, 2000.
- [14] 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.