Factoring Polynomials for Constructing Pairing-friendly Elliptic Curves

Zhitu su,[*] Hui Li,[†] and JianFeng Ma[‡]

Key lab of Computer Networks and Information Security(Xidian University)
of Ministry of Education, Xidian University
Xi'an, China

January 7, 2008

Abstract

In this paper we present a new method to construct a polynomial $u(x) \in \mathbb{Z}[x]$ which will make $\Phi_k(u(x))$ reducible. We construct a finite separable extension of $\mathbb{Q}(\zeta_k)$, denoted as $\mathbb{E}$. By primitive element theorem, there exists a primitive element $\theta \in \mathbb{E}$ such that $\mathbb{E} = \mathbb{Q}(\theta)$. We represent the primitive k-th root of unity ζ_k by θ and get a polynomial $u(x) \in \mathbb{Q}[x]$ from the representation. The resulting $u(x)$ will make $\Phi_k(u(x))$ factorable.

1 Introduction

In recent years, there has been much interest in pairing-based cryptography. Many protocols have been proposed such as [5, 15, 6]. In these protocols the following problem is of great interest: given a small positive integer k, constructing an elliptic curve over finite field $\mathbb{F}_q$, denoted by $E(\mathbb{F}_q)$, such that $\#E(\mathbb{F}_q)$, its group order, has a large enough prime factor r and r divides $q^k - 1$, but does not divide $q^i - 1$, $0 < i < k$. k is called *embedding degree* of $E(\mathbb{F}_q)$ and $E(\mathbb{F}_q)$ *pairing-friendly curve*.

In practical application, the embedding degree of $E(\mathbb{F}_q)$ should be small enough. Menezes, Okamoto and Vanstone [19] have pointed out that supersingular elliptic curves have embedding degree $k \leq 6$, thus they are suitable for paring-based cryptography. However, the security of the cryptosystem is directly related to embedding degree, but the embedding degree of supersingular elliptic curves is limited to 6. In order to achieve higher security level, we turn to ordinary elliptic curves. However Balasubramanian and Koblitz [2] have shown that ordinary elliptic curves

---

[*]ztsu@mail.xidian.edu.cn

[†]lihui@mail.xidian.edu.cn

[‡]jfma@mail.xidian.edu.cn

which have small embedding degree are very rare. Hence we can not expect to find elliptic curves with prescribed embedding degree by random selection.

Miyaji, Nakabayashi and Takano [20] first proposed a method to construct ordinary curves of prime order with embedding degree $k = 3, 4, 6$. Scott, Barreto [25] extended Miyaji et al's method and obtained curves of near prime order. A lot of methods have been proposed to construct curves with arbitrary embedding degree, such as Barreto, Lynn and Scott [6], Dupont, Enge and Morain [9] and Brezing, Weng [7].

The factorization of $\Phi_k(u(x))$ plays a important role in many methods such as [20, 7, 4, 10], where $\Phi_k(u(x))$ is the k-th cyclotomic polynomial [16] and $u(x) \in \mathbb{Z}[x]$. Generally believe that $u(x) \in \mathbb{Z}[x]$ such that makes $\Phi_k(u(x))$ factorable is rare. The results of Galbraith, McKee and Valença [12] are often used when $k = 5, 8, 10, 12$ [4, 10]. In other cases, $u(x)$ is found by computer search.

In this paper we describe a new method to explicitly construct $u(x) \in \mathbb{Q}[x]$ such that $\Phi_k(u(x))$ splits. By this method, we can find all most all suitable $u(x)$. The resulting $u(x)$ can be used to search paring-friendly elliptic curves with good property.

This paper is organized as follows. In Section 2, we describe some prerequisites for our method and our previous work on selecting suitable $u(x)$. In Section 3, we present our method and give some examples. In section 4, some applications are presented.

2 Prerequisites and Previous Work

If $\mathbb{E}$ is an extension of field $\mathbb{F}$, an element α of $\mathbb{E}$ is said to be *algebraic* over $\mathbb{F}$ if there is nonconstant polynomial $f \in \mathbb{F}[x]$ such that $f(\alpha) = 0$. $\mathbb{E}$ is said to be *algebraic* if every element of $\mathbb{E}$ is algebraic over $\mathbb{F}$.

Definition 1. [1] *An irreducible polynomial $f \in \mathbb{F}[x]$ is separable if f has no multiple roots.*

Definition 2. [1] *Let $\mathbb{E}$ be an extension of $\mathbb{F}$ and $\alpha \in \mathbb{E}$, α is separable over $\mathbb{F}$, if α is algebraic over $\mathbb{F}$ and the minimal polynomial of α over $\mathbb{F}$ is a separable polynomial. If every element of $\mathbb{E}$ is separable over $\mathbb{F}$, then we say that $\mathbb{E}$ is a separable extension of $\mathbb{F}$.*

It is well-known that every algebraic extension of a field of characteristic zero is separable[1].

In this paper we are interested in *number field*. A number field is a subfield L of $\mathbb{C}$ which is a finite extension of $\mathbb{Q}$. Since every finite extension of a field is an algebraic extension [1, 16], then every element of L is algebraic over $\mathbb{Q}$. Because the characteristic of L is zero, L is a separable extension of $\mathbb{Q}$.

In the remaining part of this section, we describe our previous work on factoring $\Phi_k(u(x))$ [26].

Theorem 1. *Let $u(x)$ be a polynomial with rational coefficients. Suppose ζ_k is a primitive k-th root of unity, if equation $u(x) = \zeta_k$ has a solution in $\mathbb{Q}(\zeta_k)$, then $\Phi_k(u(x))$ has an irreducible factor of degree $\varphi(k)$.*

Proof. Suppose $\theta \in \mathbb{Q}(\zeta_k)$ and $u(\theta) = \zeta_k$, then $\Phi_k(u(\theta)) = 0$. Let $r(x)$ be the minimal polynomial of θ over $\mathbb{Q}$, so $r(x)|\Phi_k(u(x))$. By the hypothesis, $\mathbb{Q}(\zeta_k) \subseteq \mathbb{Q}(\theta)$. Since $\theta \in \mathbb{Q}(\zeta_k)$, we have $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\zeta_k)$. Hence $\mathbb{Q}(\zeta_k) = \mathbb{Q}(\theta)$ and $\deg r(x) = \varphi(k)$. $\qquad\square$

Theorem 1 extends the results of Galbraith, McKee and Valença [12]. From the theorem we see that if an element $\theta \in \mathbb{Q}(\zeta_k)$ can be found such that $\zeta_k = u(\theta)$, $u(x) \in \mathbb{Q}[x]$, then $\Phi_k(u(x))$ is factorable.

Definition 3. [23] *Let K be a number field and $\mathcal{O}_K$ is its ring of integers, then $\mathcal{O}_K$ is said to have a power integral basis if there exists an element α of $\mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.*

If $K = \mathbb{Q}(\zeta_k)$, then $\mathcal{O}_K = \mathbb{Z}[\zeta_k]$ [17].

Definition 4. *Suppose α, $\tilde{\alpha} \in \mathcal{O}_K$, α and $\tilde{\alpha}$ are said to be equivalent if $\alpha = n \pm \delta(\tilde{\alpha})$, $\delta \in \mathrm{Gal}(K/\mathbb{Q})$.*

According to Györy [14], up to equivalent, there are only finitely many elements which generate a power integral basis for any number field.

As $\mathbb{Q}(\zeta_k)$ is concerned, if $\theta \neq \zeta_k$ generates a power integral basis(i.e. $\mathcal{O}_K = \mathbb{Z}[\theta]$), then $\zeta_k = u(\theta)$, $u(x) \in \mathbb{Z}[x]$, since $\zeta_k \in \mathcal{O}_K$. By Theorem 1, $\Phi_k(u(x))$ splits. In [26], we used the results of [23, 24, 13] to find elements that generate a power integral basis for $\mathbb{Q}(\zeta_k)$. If $k = p$ or p^m, where p is a prime, we choose $\theta = n \pm \delta(\zeta_k)$ or $\theta = n \pm \delta(\eta)$, $\eta = \frac{1}{1+\zeta_k}$, $\delta \in \mathrm{Gal}(K/\mathbb{Q})$. Otherwise, we select $\theta = n \pm \delta(\zeta_k)$ where $\delta \in \mathrm{Gal}(K/\mathbb{Q})$. The advantage of above method is that the polynomial $u(x)$ has small integer coefficients.

It follows from Theorem 1 that the method described in [26] can only generate $u(x) \in \mathbb{Z}[x]$ such that $\Phi_k(u(x))$ has an irreducible factor of degree $\varphi(k)$. So there are some suitable polynomials which can not be generated by [26].

Example 1. *Let $k = 3$, $u(x) = \frac{2}{9}x^5 - \frac{7}{9}x^4 + \frac{14}{9}x^3 - \frac{26}{9}x^2 + \frac{28}{9}x - \frac{2}{9}$, then $\Phi_3(u(x)) = \frac{1}{81}(4x^4 - 16x^3 + 33x^2 - 61x + 67)(x^6 - 3x^5 + 6x^4 - 11x^3 + 12x^2 + 3x + 1)$*

It is a problem whether there is a method which can construct all suitable polynomials. We will solve this problem in Section 3.

3 Primitive Element Theorem

The following theorem extends Theorem 1.

Theorem 2. *Let ζ_k be a primitive k-th root of unity and $\mathbb{Q}(\zeta_k)$ the k-th cyclotomic field. Then $\Phi_k(u(x))$ splits where $u(x) \in \mathbb{Q}[x]$ iff there exists an finite extension $\mathbb{E}$ of $\mathbb{Q}$ such that $\zeta_k \in \mathbb{E}$ and $u(x) = \zeta_k$ has a solution in $\mathbb{E}$.*

Proof. If there exists an extension $\mathbb{E}$ of $\mathbb{Q}$ which satisfies above conditions and $u(\theta) = \zeta_k$, then $\Phi_k(u(\theta)) = 0$. Let $r(x)$ be the minimal polynomial of θ over $\mathbb{Q}$, so $r(x)|\Phi_k(u(x))$. Conversely, if $\Phi_k(u(x))$ is factorable, let $r(x) \in \mathbb{Q}[x]$ be an irreducible factor of $\Phi_k(u(x))$ and θ be a solution of $r(x) = 0$, then $\Phi_k(u(\theta)) = 0$. Hence $u(\theta)$ is a primitive k-th root of unity, without loss of generality, we assume $u(\theta) = \zeta_k$. So $\zeta_k \in \mathbb{E} = \mathbb{Q}(\theta)$ and $\mathbb{E} = \mathbb{Q}(\theta)$ is an finite extension of $\mathbb{Q}$. $\square$

Without loss of generality, we assume $\mathbb{E} = \mathbb{Q}(\theta)$. If a simple extension $\mathbb{E} = \mathbb{Q}(\theta)$ of $\mathbb{Q}$ can be found such that $\mathbb{Q}(\zeta_k) \subseteq \mathbb{E}$, then there exists $u(x) \in \mathbb{Q}[x]$ such that $u(\theta) = \zeta_k$. According to Theorem 2, $\Phi_k(u(x))$ is factorable.

Here we face the problem of generating such $\mathbb{E}$. We use following theorems to solve this problem.

Theorem 3. *Suppose $\mathbb{E} = \mathbb{F}(\alpha_1, \cdots, \alpha_n)$, if α_i is separable over $\mathbb{F}$, then $\mathbb{E}$ is separable over $\mathbb{F}$.*

Proof. See Ash [1] or Lang [16]. $\square$

Theorem 4. *(Primitive Element Theorem) If $\mathbb{E}$ is a finite separable extension of $\mathbb{F}$, then $\mathbb{E} = \mathbb{F}(\alpha)$ for some $\alpha \in \mathbb{E}$.*

Proof. See Ash [1] or Lang [16]. $\square$

We say that α is a primitive element of $\mathbb{E}$ over $\mathbb{F}$.

Let $g(x)$ be an irreducible polynomial over $\mathbb{Q}$, then $g(x)$ is separable over $\mathbb{Q}$, since the characteristic of $\mathbb{Q}$ is zero. Suppose β is a root of $g(x) = 0$. Because $\Phi_k(x)$ is also separable, according to Theorem 3, $\mathbb{Q}(\zeta_k, \beta)$ is finite separable extension of $\mathbb{Q}$. By Theorem 4, there exists $\alpha \in \mathbb{Q}(\zeta_k, \beta)$ such that $\mathbb{Q}(\zeta_k, \beta) = \mathbb{Q}(\alpha)$. So $\zeta_k = u(\alpha)$ for some $u(x) \in \mathbb{Q}[x]$. According to Theorem 2, $\Phi_k(u(x))$ is reducible. Determining α for $\mathbb{Q}(\zeta_k, \beta)$ is known as the *primitive element problem* [8].

Above method can be summarized as:

Algorithm 1. *For a fixed small positive integer k:*
1. *Random select an irreducible polynomial $g(x)$ over $\mathbb{Q}$.*
2. *Find a primitive element α of $\mathbb{Q}(\zeta_k, \beta)$ where β is a root of equation $g(x) = 0$.*
3. *Represent ζ_k by α.*
4. *Get $u(x)$ from the representation.*

Using PARI [22], we have following examples.

Example 2. *Let $k = 3$, $g(x) = x^2 - 3$, suppose β is a root of the equation $x^2 - 3 = 0$ and α is a primitive element of $\mathbb{Q}(\zeta_3, \beta)$, the minimal polynomial of α over $\mathbb{Q}$ is $x^4 - 2x^3 - 3x^2 + 4x + 13$. We have $u(x) = -\frac{2}{15}x^3 + \frac{1}{5}x^2 - \frac{8}{15}$, $\Phi_3(u(x)) = \frac{1}{225}(4x^2 - 4x + 13)(x^4 - 2x^3 - 3x^2 + 4x + 13)$*

Example 3. *Suppose $k = 3$ and $g(x) = x^3 - 3x^2 + 1$, let β be the root of equation $x^3 - 3x^2 + 1 = 0$, we get a primitive element α of $\mathbb{Q}(\zeta_3, \beta)$ whose minimal polynomial over $\mathbb{Q}$ is $x^6 - 9x^5 + 30x^4 - 47x^3 + 45x^2 - 30x + 19$. Then $u(x) = -\frac{4}{57}x^5 + \frac{31}{57}x^4 - \frac{86}{57}x^3 + \frac{109}{57}x^2 - \frac{115}{57}x + \frac{2}{3}$, $\Phi_k(u(x)) = \frac{1}{3249}(16x^4 - 104x^3 + 233x^2 - 235x + 361)(x^6 - 9x^5 + 30x^4 - 47x^3 + 45x^2 - 30x + 19)$*

Example 4. *Assume $k = 4$, $g(x) = x^3 - 3$ and β is a root of equation $x^3 - 3 = 0$, then the primitive element α of $\mathbb{Q}(\zeta_4, \beta)$ found in this example is such that its minimal polynomial over $\mathbb{Q}$ is $x^6 + 3x^4 - 6x^3 + 3x^2 + 18x + 10$. Hence $u(x) = \frac{24}{179}x^5 - \frac{27}{179}x^4 + \frac{80}{179}x^3 - \frac{234}{179}x^2 + \frac{201}{179}x + \frac{273}{179}$, $\Phi_4(u(x)) = \frac{1}{32041}(x^6 + 3x^4 - 6x^3 + 3x^2 + 18x + 10)(576x^4 - 1296x^3 + 2841x^2 - 8208x - 10657)$*

In some cases, $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta_k)$.

Theorem 5. *Suppose d is a squarefree positive integer, then (1) if $2 \nmid d$, $4 \nmid k$ and $d|k$, then $\sqrt{d} \in \mathbb{Q}(\zeta_k)$ if $d \equiv 1 \pmod 4$, $\sqrt{-d} \in \mathbb{Q}(\zeta_k)$ if $d \equiv 3 \pmod 4$; (2) If $4|k$ and $d|k$ but $2 \nmid d$, then $\sqrt{d}, \sqrt{-d} \in \mathbb{Q}(\zeta_k)$; (3) if $8|k$ and $d|k$ then $\sqrt{d}, \sqrt{-d} \in \mathbb{Q}(\zeta_k)$.*

Proof. See Murphy, Fitzpatrick [21]. $\square$

If $g(x) = x^2 + d$ or $g(x) = x^2 - d$ and d satisfies above conditions, then $\beta = \sqrt{d}$ or $\sqrt{-d} \in \mathbb{Q}(\zeta_k)$. Hence $\mathrm{Q}(\zeta_k, \beta) = \mathrm{Q}(\zeta_k)$.

Example 5. *Let $k = 12$ and $d = 3$, suppose $f(x) = x^2 - 3$ and $f(\beta) = 0$, using PARI [22], the primitive element α of $\mathbb{Q}(\zeta_k, \beta)$ we find is such that its minimal polynomial over $\mathbb{Q}$ is $x^4 - 13x^2 + 49$. Using the modreverse function of PARI [22], we get that $\mathbb{Q}(\zeta_k, \beta) = \mathbb{Q}(\alpha) = \mathbb{Q}(\zeta_k)$.*

Theorem 6. *All $u(x) \in \mathbb{Q}[x]$ such that $\Phi_k(u(x))$ is reducible can be constructed by Algorithm 1.*

Proof. Suppose $u(x)$ is a suitable polynomial, by Theorem 2, there exists a simple extension $\mathbb{Q}(\theta)$ of $\mathbb{Q}$ such that $\zeta_k \in \mathbb{Q}(\theta)$ and $u(\theta) = \zeta_k$. Let $f(x)$ be the minimal polynomial of θ over $\mathbb{Q}$. Assume $g(x) = f(x)$ and $\beta = \theta$, since $\zeta_k \in \mathbb{Q}(\theta)$, we have $\mathrm{Q}(\zeta_k, \beta) = \mathrm{Q}(\beta)$(i.e. $\alpha = \beta$). If ζ_k is represented by θ, we get $u(x)$ from the representation. $\square$

4 Applications

Brezing-Weng's method [7] is often used in constructing pairing-friendly curves. It can be described as follow [11].

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

4. *Let $y(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $\frac{\zeta_k - 1}{\sqrt{-D}} \in K$.*

5. *Let $p(x) \in \mathbb{Q}[x]$ be given by $(t(x)^2 + Dy(x)^2)/4$. If $p(x)$ and $r(x)$ represent primes, then then the triple $(t(x), r(x), p(x))$ represents a family of curves with embedding degree k and discriminant D.*

We will search $x_0 \in \mathbb{Z}^+$ such that $r(x_0)$ and $p(x_0)$ are primes. If x_0 is found, then there exists an elliptic curves over the prime fields $\mathbb{F}_{p(x_0)}$ with embedding degree k [7].

Our method can be used in step 2 and 3. Let $t(x) = u(x) + 1$ and $r(x)$ be an irreducible factor of $\Phi_k(u(x))$.

Theorem 7. *Suppose p is a prime, $p \nmid k$ and $u \in \mathbb{Z}$, the multiplication order of $u \bmod p$ is k(i.e. $u^k \equiv 1 \pmod{p}$ and k is minimal) iff $p | \Phi_k(u)$.*

Proof. See Washington [27] or Menezes [18]. $\qquad\square$

Theorem 8. *Suppose $k = 4d$, $k \in \mathbb{Z}^+$ and r is a prime, if x is a primitive k-th root of unity modulo r, then $-x$ is also a primitive k-th root of unity modulo r.*

Proof. If $-x$ is not a primitive k-th root of unity modulo r, suppose $(-x)^{d_0} \equiv 1 \pmod{r}$, where d_0 is the smallest positive integer and $1 < d_0 < k$, then d_0 is odd. If d_0 is even, we have $(-x)^{d_0} = (x)^{d_0} \equiv 1 \pmod{r}$, a contradiction. It follows from the hypothesis that $d_0 | d$ and $(-x)^{2d} \equiv -1 \pmod{r}$. Since $(-x)^{d_0} \equiv 1 \pmod{r}$ and d_0 is odd, we have $(x)^{d_0} \equiv -1 \pmod{r}$. So $r | x^{2d} - x^{d_0} = x^{d_0}(x^{\frac{2d}{d_0}} - 1)$. Because $r \neq x$, we get $r | x^{\frac{2d}{d_0}} - 1$(i.e.$x^{\frac{2d}{d_0}} \equiv 1 \pmod{r}$), contradict to the hypothesis. $\qquad\square$

If $r(x)$ is an irreducible factor of $\Phi_k(u(x))$ where $4|k$ and $r(x_0)$ is a prime, by Theorem 7, $u(x_0)$ is a primitive k-th root of unity modulo $r(x_0)$. According to Theorem 8, $-u(x_0)$ is also a primitive k-th root of unity modulo $r(x_0)$. So in Algorithm 1, $t(x)$ can also be set to $-u(x) + 1$.

References

[1] R. Ash Abstract Algebra: The Basic Graduate Year, Available at: http://www.math.uiuc.edu/~r-ash/Algebra.html.

[2] 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*, 11, 141-145(1998).

[3] P. S. L. M. Barreto, B. Lynn and M. Scott, Constructing Elliptic Curves with Prescribed Embedding Degrees, *Security in Communication Networks–SCN'2002*, LNCS 2576, 263-273(2002).

[4] P. S. L. M. Barreto and M. Naehrig, Pairing-Friendly Elliptic Curves of Prime Order, *Selected Areas in Cryptography–SAC'2005*, LNCS 3897, 319-331(2006).

[5] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, *SIAM Journal of Computing*, 32, 586-615(2003).

[6] D. Boneh, B. Lynn, and H. Shacham, Short signatures from the Weil pairing, *Advances in Cryptology-Asiacrypt'2001*, LNCS 2248, 154-532(2002).

[7] F. Brezing and A. Weng, Elliptic curves suitable for pairing based cryptography, *Designs, Codes and Cryptography*, 37, 133-141(2005).

[8] H. Cohen, A Course In Computational Algebraic Number Theory, 3ed, Springer, New York(1996).

[9] R. Dupont, A. Enge and F. Morain, Building Curves with Arbitrary Small MOV Degree over Finite Prime Fields, *Journal of Cryptology*, 18, 79-89(2005).

[10] D. Freeman, Constructing pairing-friendly elliptic curves with embedding degree 10, *Algorithmic Number Theory Symposium ANTS-VII*, LNCS 4076, 452-465(2006).

[11] D. Freeman, M. Scott, E. Teske, A taxonomy of pairing-friendly elliptic curves, Cryptology ePrint Archive Report 2006/372, Available at: http://eprint.iacr.org/2006/372/.

[12] S. Galbraith, J. McKee, and P. Valença, Ordinary abelian varieties having small embedding degree, Finite Fields and Their Applications, 13, 800-814(2007).

[13] I. Gaál and L. Robertson, Power integral bases in prime-power cyclotomic fields, *Journal of Number Theory*, 120, 372-384(2006).

[14] K. Györy, Sur les polynômes à coefficients entiers et de discriminant donné, III, Publ. Math. Debrecen, 23, 141-165(1976).

[15] A. Joux, A One Round Protocol for Tripartite Diffie-Hellman, *Journal of Cryptology*, 17, 263-276(2004).

[16] S. Lang, Algebra, Revised 3ed, Springer, New York(2002).

[17] D. A. Marcus, Number Fields, Springer, New York(1977).

[18] A. Menezes, An introduction to pairing-based cryptography, Available at http://www.cacr.math.uwaterloo.ca/~ajmeneze/publications/pairings.pdf.

[19] A. Menezes, T. Okamoto, and S. Vanstone, Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field, *IEEE Transactions on Information Theory*, 39, 1639-1646(1993).

[20] 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).

[21] A. Murphy, N. Fitzpatrick, Elliptic Curves for Pairing Applications, Cryptology ePrint Archive Report 2005/302, Available at: http://eprint.iacr.org/2005/302.pdf.

[22] PARI/GP, Computer Algebra System, Available at: http://pari.math.u-bordeaux.fr.

[23] L. Robertson, Power Bases for Cyclotomic Integer Rings, *Journal of Number Theory*, 69, 98-118(1998).

[24] L. Robertson, Power Bases for 2-Power Cyclotomic Fields, *Journal of Num-*

ber Theory, 88, 196-209(2001).

[25] M. Scott and P. S. L. M. Barreto, Generating More MNT Elliptic Curves, *Designs, Codes and Cryptography*, 38, 209-217(2006).

[26] Zhitu Su, Hui Li and Jianfen Ma, Factoring of $\Phi_k(u(x))$ For Constructing Pairing-Friendly Elliptic Curves, Submitted to *Designs, Codes and Cryptography*.

[27] L. Washington, Introduction to Cyclotomic Fields, Springer, New York(1997).