Generating Pairing-Friendly Curves with the CM Equation of Degree 1

Hyang-Sook Lee and Cheol-Min Park*

Department of Mathematics, Ewha Womans University,
Seoul 120-750, S. Korea
{hsl,mpcm}@ewha.ac.kr

Abstract. Refinements of the Brezing-Weng method have provided families of pairing-friendly curves with improved ρ-values by using non-cyclotomic polynomials that define cyclotomic fields. We revisit these methods via a change-of-basis matrix and completely classify a basis for a cyclotomic field to produce a family of pairing-friendly curves with a CM equation of degree 1. Using this classification, we propose a new algorithm to construct Brezing-Weng-like elliptic curves having the CM equation of degree 1, and we present new families of curves with larger discriminants.

1 Introduction

Research on pairing-based cryptography has been getting a great deal of attention over the past few years. Since 2000, a number of new protocols have been proposed based on the cryptographic pairings, such as identity-based key exchange [17], one-round tripartite key agreement [11], identity-based encryption [4], and short digital signature [5].

For the practical realization of these protocols, they must be implemented using some special curves, so called pairing-friendly curves with a large prime order subgroup whose embedding degree is small enough that computations in the finite field are feasible. One approach using pairing-friendly curves relies on supersingular elliptic curves. Over these curves, however, the embedding degrees are limited to $\{1, 2, 3, 4, 6\}$. Another approach is to use the ordinary elliptic curves with small embedding degree. However, since these curves are rare, according to the result of Balasubramania and Koblitz [2], it is necessary to develop algorithms to construct suitable pairing-friendly curves. Many algorithms have been proposed to construct pairing-friendly ordinary elliptic curves. One general method is the Brezing and Weng method [6], which generates polynomial families of curves by using a defining polynomial $r(x)$ of a cyclotomic field or its extension field. Usually, the defining polynomial of cyclotomic field $\mathbb{Q}(\zeta_k)$ for a primitive kth root of unity ζ_k is the kth cyclotomic polynomial $\Phi_k(x)$. But if

* This work was supported by the Korea Research Foundation Grant funded by the Korean Government(MOEHRD, Basic Research Promotion Fund)(KRF-2008-1645-1-1).

H. Shacham and B. Waters (Eds.): Pairing 2009, LNCS 5671, pp. 66–77, 2009.

we use an irreducible factor of $\Phi_k(u(x))$ for some $u(x) \in \mathbb{Q}[x]$, we can obtain a different defining polynomial of the cyclotomic field $\mathbb{Q}(\zeta_k)$ or its extension field. Using this idea, Galbraith, Mckee, and Valenca demonstrated the existence of ordinary abelian varieties of dimension 2 having small embedding degrees [10]. Building on this work, Barreto and Naehrig [3], and Freeman [8] constructed pairing-friendly elliptic curves of prime order. If we choose an irreducible factor $r(x)$ of $\Phi_k(u(x))$ such that the degree of $r(x)$ is $\varphi(k)$, $r(x)$ will define the same cyclotomic field $\mathbb{Q}(\zeta_k)$. But in some cyclotomic fields, a careful choice of $r(x)$ can produce a pairing-friendly curve with better ρ-values than curves constructed from $\Phi_k(x)$. Working from this idea, Kachisa, Schaefer and Scott [13] developed a method for constructing pairing-friendly elliptic curves with better ρ-values.

In a method that uses the factorization of $\Phi_k(u(x))$, the difficult part is how to choose a $u(x)$ that will produce an irreducible factor of $\Phi_k(u(x))$. Lemma 1 in Galbraith, Mckee and Valenca [10] offers one solution to this problem by providing the criterion for $u(x)$ to give a factorization of $\Phi_k(u(x))$. Another solution is provided by Tanaka and Nakamula [18]. They proposed a method of finding $u(x)$ such that $\Phi_k(u(x))$ has an irreducible factor of degree $\varphi(k)$, reducing the problem of finding an appropriate $u(x)$ to solving a system of multivariate polynomial equations for the coefficients of $u(x)$ using a matrix.

We observe that Tanaka and Nakamula's method can be also described via a change-of-basis matrix, because finding an irreducible factor of $\Phi_k(u(x))$ with degree $\varphi(k)$ is equivalent to finding a basis for $\mathbb{Q}(\zeta_k)$. Based on this idea, we completely classify a basis for $\mathbb{Q}(\zeta_k)$ which gives pairing-friendly elliptic curves with the CM equation of degree 1. From this classification, we can avoid the exhaustive search to find $u(x)$ such that $\Phi_k(u(x))$ has an irreducible factor of degree $\varphi(k)$ and the CM equation of curves constructed from $u(x)$ has degree 1. Using a change-of-basis matrix and this classification of a basis for $\mathbb{Q}(\zeta_k)$, we propose a new algorithm to construct Brezing-Weng-like elliptic curves with the CM equation of degree 1. Unlike the previous Brezing-Weng-like elliptic curves with small discriminants, we present new families of curves with larger discriminants which are less than 10^{10}.

The paper is organized as follows: Section 2 reviews the basic definitions related to pairing-friendly curves and methods involved in the construction of the curves. Section 3 reviews the method that uses the factorization of $\Phi_k(u(x))$ via a change-of-basis matrix. Section 4 presents the complete classification of a basis for $\mathbb{Q}(\zeta_k)$ which gives pairing-friendly elliptic curves with the CM equation of degree 1 and also gives an algorithm and examples. Section 5 discusses further works regarding our results and offers a conclusion.

2 Pairing-Friendly Elliptic Curves

In this section, we briefly review the definitions and methods involved in the construction of pairing-friendly curves. For a good survey, see [9].