Finite Fields and Their Applications 34 (2015) 45–74

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Explicit formula for optimal ate pairing over cyclotomic family of elliptic curves

Hoon Hong [a], Eunjeong Lee [b], Hyang-Sook Lee [c,*]

[a] *Dept. of Mathematics, North Carolina State University, Raleigh, NC 27695-8205, USA*
[b] *Institute of Mathematical Sciences, Ewha Womans University, Seoul, 120-750, Republic of Korea*
[c] *Dept. of Mathematics, Ewha Womans University, Seoul, 120-750, Republic of Korea*

ARTICLE INFO

Article history:
Received 31 July 2014
Received in revised form 7 December 2014
Accepted 27 December 2014
Available online 30 January 2015
Communicated by Neal Koblitz

MSC:
11T71

Keywords:
Pairing-based cryptosystem
Elliptic curve
Cyclotomic polynomial

ABSTRACT

Pairings on elliptic curves play an important role in cryptography. We provide an *explicit* formula for vectors of polynomials describing optimal ate pairings over cyclotomic family of elliptic curves. The explicit formula is *simple* in that it only involves partitioning a certain cyclotomic polynomial. The simplicity of the formula allows us to analyze the sparsity of the vector.

1. Introduction

Pairings on elliptic curves play an important role in cryptography [2–4,6,7,13,17,19,21,22,24,26]. Thus there has been intensive research on finding *good* pairings over a given

* Corresponding author.
E-mail addresses: hong@ncsu.edu (H. Hong), ejlee127@ewha.ac.kr (E. Lee), hsl@ehwa.ac.kr (H.-S. Lee).

http://dx.doi.org/10.1016/j.ffa.2014.12.007
1071-5797/

curve, i.e., "allowing efficient execution", yielding pairings such as Eta, Eta$_T$, ate, ate$_i$, or R-ate [8,1,11,27,15]. Vercauteren [23] combined the previous pairings into a uniform framework, defining a *generalized ate pairing*, which is described by a vector of integers. He also provided an algorithm for finding a vector of integers describing an *optimal* ate pairing. The algorithm essentially searches for a short vector in a certain integer lattice.

The framework of generalized ate pairing can be naturally extended to a *family* of curves [10,9,5]. A family of curves is described by certain polynomials. Likewise, the family of corresponding generalized ate pairings is described by a vector of polynomials. A natural problem is to find a vector of polynomials describing optimal ate pairings over a given family of curves.

Hess [10] extended the idea of Vercauteren to a function field lattice and suggested to use the function field LLL [20], which would return a vector of polynomials with minimal degree describing optimal ate pairings. Zhang–Lin [25] suggested solving a certain linear system to find a vector of polynomials describing optimal ate pairings over KSS curves [14].

The main contribution of this paper is in providing an *explicit* formula for a vector of polynomials describing optimal ate pairings over a *cyclotomic* family of elliptic curves (see Formula 1). The explicit formula is *simple* in that it only involves partitioning a certain cyclotomic polynomial. The simplicity of the formula allows us to analyze the properties/structures of the resulting vector of polynomials, such as degree and sparsity, which are crucial information in gauging the execution efficiency of the pairings described by the vector.

In a sense, the main result of this paper (simple explicit formula) can be viewed as a certain compromise between *generality* and *analyzability*. The algorithms due to Hess [10] and Zhang–Lin [25] can handle almost arbitrary (pairing friendly) families of curves. Thus the methods are high in generality. On the other hand, the methods involve long series of computational steps, making the structural analysis difficult. Thus the methods are not so high in analyzability. The explicit formula presented in this paper can handle only cyclotomic families of curves. Thus it is not so high in generality. On the other hand, it is explicit and simple, making the structural analysis easy. Thus it is high in analyzability. Therefore, one might view our contribution as trading generality for analyzability.

Of course, one should not lose generality too much. In this regard, we observe that the cyclotomic families have been heavily discussed in [9] since they can produce pairing friendly curves efficiently and also have the chance to provide good performance. As an example, [18] observed the advantage for pairing computation of the optimal ate pairing over the cyclotomic family with embedding degree 15.

The paper is structured as follows. In Section 2, we briefly review elliptic curves, cyclotomic families of curves, and the generalized ate pairings of Vercauteren. We end with a description of the generalized ate pairings defined over cyclotomic families of pairing friendly curves. In Section 3, we state the problem and the main result precisely.