Finite Fields and Their Applications 28 (2014) 79–93

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Self-pairings on supersingular elliptic curves with embedding degree *three* ☆

BingLong Chen, Chang-An Zhao *

Department of Mathematics, Sun Yat-sen University, Guangzhou 510275, PR China

ARTICLE INFO

Article history:
Received 16 October 2013
Received in revised form 23 January 2014
Accepted 25 January 2014
Available online 25 February 2014
Communicated by Neal Koblitz

MSC:
14H52
11G20
14G15
14Q05
11T71

Keywords:
Elliptic curves
Tate pairing
Weil pairing
Self-pairing
Pairing based cryptography

ABSTRACT

Self-pairings are a special subclass of pairings and have interesting applications in cryptographic schemes and protocols. In this paper, we speed up the computation of the self-pairing by using a simple final exponentiation on supersingular elliptic curves with embedding degree $k = 3$. We also compare the efficiency of self-pairing computations on different curves over large characteristic. We indicate that supersingular elliptic curves with $k = 3$ may be more attractive for implementing the self-pairings.

☆ The work of Binglong Chen is supported by the National Natural Science Foundation of China under Grant No. 11025107. The work of Chang-An Zhao is supported by the National Natural Science Foundation of China under Grant No. 61003227.

* Corresponding author.
E-mail addresses: mcscbl@mail.sysu.edu.cn (B. Chen), zhaochan3@mail.sysu.edu.cn (C.-A. Zhao).

http://dx.doi.org/10.1016/j.ffa.2014.01.013
1071-5797/

1. Introduction

Pairing based cryptography has been one of the most active areas in cryptologic research in the past years [1,2]. This leads to the improvement of mathematical algorithmic foundations of pairings. For the general bilinear pairing $e(P, Q)$ on (hyper-)elliptic curves, many variants of the Tate pairing have been proposed in efficiency [3–9].

Self-pairings $e(P, P)$ are a special subclass of pairings, which are of vital use in several cryptographic applications, such as the on-line/off-line signature scheme of Zhang et al. [10] and the designated confirmer signature [11]. Since both input points are equal in the self-pairings, it is natural to ask whether self-pairings can be computed faster than the general case. By using the distortion maps on supersingular elliptic curves [12,13], the authors of [14] accelerate the computation of the self-pairing by using a simple final exponentiation. This idea has been also generalized to the hyperelliptic case [15].

It is known that self-pairings can be constructed on supersingular elliptic curves with distortion maps. Verheul first introduces the notion of distortion maps on a supersingular elliptic curve with $k = 3$ [12]. This curve is defined over a finite field $\mathbb{F}_{p^2}$ for p a prime $p \equiv 2 \pmod 3$, and has $p^2 - p + 1$ $\mathbb{F}_{p^2}$-rational points. The general bilinear pairings on this elliptic curve have been studied by Hu et al. in [16] and improved by Galbraith et al. in [17]. Recently, there are more works that improved the efficiency of the general pairings on this curve [18,19]. This curve has many merits in performance. Firstly, the Miller loop of the Eta/Ate pairings on this curve can be shortened to a half of that of the reduced Tate pairing. This is better than computing pairings on supersingular curves over large prime fields with $k = 2$. Secondly, the authors of [20] propose a modified Miller's iteration formula which makes the denominator elimination technique available for pairing friendly curves with odd embedding degrees. Finally, for supersingular elliptic curves with $k = 3$ we can generate the suitable parameters which allow the pairings to be computed quickly [17], i.e., the number of iterations of the Miller loop and the order of the prime field $\mathbb{F}_p$ can be chosen to have a low Hamming weight. Therefore, it is meaningful to consider the self-pairing computation on supersingular curves with $k = 3$.

The self-pairing computation has been investigated on supersingular elliptic curves with even embedding degrees [14]. Note that the distortion maps on curves with even embedding degrees [14] are also the non-trivial automorphisms of the curves. By this property, the main results of [14] can be presented. However, the distortion map on supersingular elliptic curves with $k = 3$ is not an automorphism of the curve. This leads to the ignorance of this family of curves in [14]. In this paper, we tackle this problem and speed up the computation of the self-pairing by using a simpler final exponentiation.

The recent prominent developments of solving the discrete logarithm problem in finite fields with small characteristic [21–25] possibly weaken the security of pairings derived from supersingular curves with embedding degree 6 and 4 defined, respectively, over finite fields with characteristic 3 and 2. Thus we only compare the efficiency of self-pairings on supersingular elliptic curves over large characteristic. The efficiency estimation and experimental results indicate that the self-pairing on curves with $k = 3$ can be more