Optimal pairing revisited*

Mingqiang Wang[1], Puwen Wei[1], Haifeng Zhang[1], Yuliang Zheng[2]
1. Key Laboratory of Cryptologic Technology and Information Security,
Ministry of Education, Shandong University, 250100 Jinan, China
2. Department of Software and Information Systems,
University of North Carolina at Charlotte
9201 University City Blvd Charlotte, NC 28223

Abstract

Vercauteren [27] introduced a notion of optimal pairings. Up to know the only known optimal pairing is the optimal Ate pairing. In this paper, we give some properties of optimal pairing and provide an algorithm for finding an optimal pairing if there exists one which is defined on the given elliptic curve. Applying the cyclotomic polynomial, we construct some new optimal pairings and provide a construction method of pairing-friendly elliptic curves on which the optimal pairing can be defined. Our algorithm is explicit and works for arbitrary embedding degree k and large prime subgroup orders r.

Keywords: Pairing-friendly; Optimal pairing; Cyclotomic polynomial; Pairing lattice

1 Introduction

Pairing based cryptography is a major area of research in public key cryptography. There has been a huge interest in developing fast algorithms to compute bilinear pairing. A bilinear pairing is a map of form

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$$

where $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ are cyclic groups of prime order r.

So far as we known, all the fast algorithms of computing Weil and Tate pairings are based on Miller's algorithm [23] on (hyper)elliptic curves. One line of research focuses on shortening the loop in Millers algorithm, which was

*This work is supported by national 973. Grant No.2007CB807903 and nature science of Shandong province Grant No Y2008G23.

initiated by Duursma-Lee [9] and extended by Barreto et al. [3] to supersingular abelian varieties. The ate pairing introduced in [17] for elliptic curves and in [15] for hyperelliptic curves generalize these pairings to all ordinary curves. Recently, variants of the ate pairing were introduced thereby reducing the loop length in Miller's algorithm, such as the optimized ate pairing [22], and finally the R-ate pairing [20]. All variants of the ate pairing have a Miller loop of length at least $\frac{\log_2 r}{\varphi(k)}$, with the embedding degree k. Vercauteren [27] introduced the notion of optimal pairings, which by definition attains this lower bound and conjectured that any non-degenerate pairing on an elliptic curve without extra efficiently computable endomorphisms different from Frobenius requires at least $\frac{\log_2 r}{\varphi(k)}$ basic Miller operations. Hess [16] proved this conjecture and thereby justifying the term "optimal pairing" in [27].

One calls an elliptic curve with a small embedding degree and a large prime-order subgroup pairing-friendly which is introduced by Freeman, Scott and Teske [11] and defined as follows.

Definition 1 *Suppose E is an elliptic curve defined over a finite field $\mathbb{F}_q$. We say that E is pairing-friendly if the following two conditions hold:*

1. *there is a prime $r \geq \sqrt{q}$ dividing $\sharp E(\mathbb{F}_q)$, and*
2. *the embedding degree of E with respect to r is less than $\log_2(r)/8$.*

In this paper, a pairing-friendly elliptic curve is called a **pairing-friendly elliptic curve with optimal pairing** if there exists an optimal pairing defined on such elliptic curve. By the Hess's result in [16], we notice that pairing-friendly curves with optimal pairing are quite scarce.

Our main contributions in this paper are as follows:

- An upper bound of the number of Miller iterations that are required to evaluate a function is obtained and if the pairing defined by the function is an optimal pairing, an algorithm is proposed to get the coefficients of the principal divisor of the function.
- Many new optimal pairings are constructed by using cyclotomic polynomial.
- A method for constructing pairing friendly curves is provided. The resulting elliptic curves of the method have optimal paring defined on them.

This paper is organized as follows: Section 2 recalls the necessary background knowledge, including all variants of the ate pairing, pairing lattice and Miller algorithm. Section 3 describes the properties of the coefficients of a principal divisor of which the function define a pairing and gives an algorithm to find such optimal pairings for a given pairing-friendly elliptic curve. Section 4

construct some new optimal pairings. Section 5 provides an efficient method for constructing pairing-friendly curves with optimal pairing. Finally, Section 6, concludes the paper.

2 Preliminaries

2.1 Bilinear pairing

In this paper, we will only consider the ordinary elliptic curve, and the method can be generalized to supersingular elliptic curve or hyperelliptic curve. Let us recall the definitions of standard notation and pairing on elliptic curve.

Let $\mathbb{F}_q$ be a finite field with q elements and E be a non-singular elliptic curve over $\mathbb{F}_q$. Let r be a positive divisor of $\sharp E(\mathbb{F}_q)$ and $k > 1$ be the embedding degree i.e. k is the smallest integer such that $r \mid q^k - 1$. Then $E(\mathbb{F}_{q^k})[r] \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ and there exists a basis P, Q of $E(\mathbb{F}_{q^k})[r]$ satisfying $\pi(P) = P$ and $\pi(Q) = qQ$, where π is the q-power Frobenius endomorphism on E. The subgroup of r-th roots of unity of $\mathbb{F}_{q^k}$ is denoted by μ_r, i.e. $\mu_r = \{z \in \mathbb{F}_{q^k}^* : z^r = 1\}$. We define $G_1 =< P >$ and $G_2 =< Q >$. Note that $G_1 \bigcap G_2 = \{\mathcal{O}\}$.

For $s \in \mathbb{Z}$ and $R \in E(\mathbb{F}_{q^k})$, let $f_{s,R} \in \mathbb{F}_{q^k}(E)$ be the uniquely determined monic function with divisor $(f_{s,R}) = ((sR) - (\mathcal{O})) - s((R) - (\mathcal{O}))$, where (R) is the divisor corresponding to the point R. The reduced Tate pairing is

$$t : G_2 \times G_1 \to \mu_r, \qquad (Q, P) \mapsto f_{r,Q}(P)^{q^k - 1/r}.$$

It is in fact defined on all $E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})[r]$ and is always non-degenerate.

Let s be an integer with $s \equiv q \bmod r$. Define $N = \gcd(s^k - 1, q^k - 1)$, $L = s^k - 1/N$ and $c = \sum_{j=0}^{k-1} s^{k-1-j} q^j \bmod N$. The ate pairing with respect to s is given by

$$a_s : G_2 \times G_1 \to \mu_r, \qquad (Q, P) \mapsto f_{s,Q}(P)^{c(q^k - 1)/N}.$$

The relation with the Tate pairing is $a_s(Q, P) = t(Q, P)^L$. It is non-degenerate if and only if $r \nmid L$ (see [22]).

Consider the following modified ate pairing

$$a_s : G_2 \times G_1 \to \mu_r, \qquad (Q, P) \mapsto f_{s,Q}(P)^{(q^k - 1)/r}.$$

Since $r|N$ and $r \nmid c$, a_s is always bilinear, and using the relation with the Tate pairing it is not difficult to show that a_s is non-degenerate if and only if $s^k \neq 1 \bmod r^2$ (see also [16] Corollary 14 and its proof).

2.2 Pairing lattice

Let s be an integer, for $h = \sum_{i=0}^{d} h_i x^i \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod r$, define $||h||_1 = \sum_{i=0}^{d} |h_i|$, and let $f_{s,h,R} \in \mathbb{F}_{q^k}(E)$ for $R \in E(\mathbb{F}_{q^k})[r]$ be the uniquely

defined monic polynomial satisfying

$$(f_{s,h,R}) = \sum_{i=0}^{d} h_i((s^i R) - (\mathcal{O})).$$

Fact 1 [16] *Assume that s is a primitive k-th root of unity modulo r^2. Let $h \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod r$. Then*

$$a_{s,h} : G_2 \times G_1 \to \mu_r, \qquad (Q, P) \mapsto f_{s,h,Q}(P)^{(q^k-1)/r}$$

is a bilinear pairing that is non-degenerate if and only if $h(s) \neq 0 \bmod r^2$. The relation with the Tate pairing is $a_{s,h}(Q, P) = t(Q, P)^{h(s)/r}$.

There exists an efficiently computable $h \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod r, deg(h) \leq \varphi(k) - 1$ and $||h||_1 = O(r^{1/\varphi(k)})$ such that $a_{s,h}$ is non-degenerate. The O-constant depends only on k.

Any $h \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod r$ such that $a_{s,h}$ is a non-degenerate bilinear pairing satisfies $||h||_1 \geq r^{1/\varphi(k)}$.

2.3 Miller algorithm

To compute the function $f_{s,P}$ for $s > 0$, one can use Miller's algorithm [23], which is a double-and-add approach based on the following observation

$$f_{m+n,P} = f_{m,P} f_{n,P} \frac{l_{mP,nP}}{v_{(m+n)P}},$$

where $l_{mP,nP}$ is the equation of the line through mP and nP (or the tangent line when $mP = nP$) and $v_{(m+n)P}$ the equation of the vertical line through $(m + n)P$.

Algorithm 1 Miller's algorithm for elliptic curves

Input: $s \in \mathbb{N}$ and $P, Q \in E[r]$ with $P \neq Q$
Output: $f_{s,P}(Q)$
  Write $s = \sum_{j=0}^{L} s_j 2^j$, with $s_j \in \{0, 1\}$ and $s_L = 1$.
  $T \leftarrow P, f \leftarrow 1$.
  for $j = L - 1$ down to 0 do
    $f \leftarrow c^2 l_{T,T}(Q)/v_{2T}(Q)$
    $T \leftarrow 2T$
    if $s_j = 1$ **then**
      $f \leftarrow f l_{T,P}(Q)/v_{T+P}(Q)$
      $T = T + P$
    end if
  end for
  Return f

For $s < 0$ it suffices to remark that $(f_{s,P}) = -(f_{-s,P}) - (v_{sP})$. One execution of the main loop in algorithm 1 will be called *a basic Miller iteration*, during which one doubling and at most one addition is computed.

3 Properties of optimal pairing

At first, we recall the definition of optimal pairing in [27].

Definition 2 *Let $e : G_1 \times G_2 \to G_T$ be a non-degenerate, bilinear pairing with $|G_1| = |G_2| = |G_T| = r$, where the field of definition of G_T is $\mathbb{F}_{q^k}$. $e(\cdot, \cdot)$ is called an optimal pairing if it can be evaluated with about at most $(\log_2 r)/\varphi(k) + \varepsilon(k)$ Miller iterations, where $\varepsilon(k)$ is less than $\log_2 k$.*

From Fact 1 and the definition of optimal pairing, we get the following proposition which gives a simple criterion for determining whether a pairing $a_{s,h}$ is an optimal pairing.

Theorem 1 *Assume that s is a primitive k-th root of unity modulo r^2. Let $h(x) = \sum_{i=0}^{\varphi(k)-1} h_i x^i$ be a polynomial in $\mathbb{Z}[x]$ of degree less than $\varphi(k) - 1$ with $h(s) \equiv 0 \bmod r$ and $h(s) \neq 0 \bmod r^2$ and let $\omega(h)$ be the Hamming weight of $(h_0, \cdots, h_{\varphi(k)-1})$. If*

$$\prod_{\substack{0 \le i \le \varphi(k)-1 \\ h_i \neq 0}} |h_i| \le 2^{-\omega(h)} k r^{1/\varphi(k)},$$

then $a_{s,h}$ is an optimal pairing.

Proof The assumption of the proposition and Fact 1 implies that $a_{s,h}$ is a non-degenerate pairing. From Fact 1, $a_{s,h}(Q, P) = f_{s,h,Q}(P)^{q^k-1/r}$, where

$$(f_{s,h,Q}) = \sum_{0 \le i \le \varphi(k)-1} h_i((s^i Q) - (\mathcal{O}))$$

and $P, Q \in E(\mathbb{F}_{q^k})[r]$. By the Proposition 3.4 in Silverman [26], one have $h_i((s^i Q) - (\mathcal{O})) \sim (h_i s^i Q) - (\mathcal{O})$ i.e. there exists a function $f_i \in \mathbb{F}_{q^k}(E)$ such that

$$h_i((s^i Q) - (\mathcal{O})) - ((h_i s^i Q) - (\mathcal{O})) = (f_i).$$

The number of the basic Miller iterations to build f_i is at most $\log_2 |h_i|$. By the above discussion, one can find that there is function $g \in \mathbb{F}_{q^k}(E)$ such that

$$(g) = \sum_{0 \le i \le \varphi(k)-1} ((h_i s^i Q) - (\mathcal{O})).$$

To compute g, one can only use the add approach in Miller iteration loop, and the number of the basic Miller iterations g is at most $\omega(h)-1$. It is not difficult to see that

$$f_{a,s,h} = cg \prod_{0\le i\le \varphi(k)-1} f_i,$$

where c is a nonzero constant. Therefore the number of the basic Miller iterations to compute $f_{a,s,h}$ is at most $\sum_{\substack{0\le i\le \varphi(k)-1\\ h_i\neq 0}} \log_2 |h_i| + \omega(h) - 1$. If

$$(\prod_{\substack{0\le i\le \varphi(k)-1\\ h_i\neq 0}} |h_i|) \le 2^{-\omega(h)} k r^{1/\varphi(k)},$$

then

$$\log_2(\prod_{\substack{0\le i\le \varphi(k)-1\\ h_i\neq 0}} |h_i|) + \omega(h) - 1 \le (\log_2 r)/\varphi(k) + \log_2 k.$$

This implies $a_{s,h}$ is an optimal pairing.

Corollary 1 *Let $s, h(x)$ be defined as Theorem 1 and let*

$$h_{max} = \max\{|h_0|, \cdots, |h_{\varphi(k)-1}|\}.$$

If $a_{s,h}$ is an optimal pairing, then

$$(\prod_{\substack{0\le i\le \varphi(k)-1\\ h_i\neq 0}} |h_i|)/h_{max} \le k^2.$$

Proof Since $a_{s,h}$ is a non-degenerate pairing, by Fact 1, one have $\| h \|_1 \ge r^{1/\varphi(k)}$, this implies $h_{max} \ge r^{1/\varphi(k)}/k$. By the proof of proposition 1, we have that the number of basic Miller iterations to compute an optimal pairing $a_{s,h}$ is at least

$$(\prod_{\substack{0\le i\le \varphi(k)-1\\ h_i\neq 0}} |h_i|) \le k r^{1/\varphi(k)}$$

which completes the proof of the proposition.

In order to describe the method of constructing elliptic curves clearly, we introduce the following definition.

Definition 3 *A polynomial is called an optimal polynomial with respect to $[k, s]$ modulus r if $a_{s,h}$ is a non-degenerate optimal pairing.*

Vercauteren [27] apply LLL-algorithm to find an optimal polynomial of family elliptic curves. However, the short vector h output by LLL-algorithm satisfying $\| h \|_1 \le r^{1/\varphi(k)}$ may not meet the condition of optimal pairing in proposition 1.

Applying Proposition 2, for a given elliptic curve, we provide the following algorithm which can output an optimal polynomial if there exists one. Let

$$A_{k,j} = \{(h_0, \cdots, h_{j-1}, h_{j+1}, \cdots, h_{\varphi(k)-1}) | h_i \in \mathbb{Z}, \ (\prod_{\substack{h_i \neq 0 \\ i \neq j}} |h_i|) \leq k^2\}.$$

Algorithm 2 Algorithm for finding an optimal polynomial

Input: $r, s, k \in \mathbb{N}$ satisfy that s is a primitive k-th root of unity modulo r^2

Output: an optimal polynomial h with respect to s modulus r

1. For $j = 0$ to $\varphi(k) - 1$
2. For $h' \in A_{k,j}$, $c \leftarrow -\sum_{\substack{i=0 \\ i \neq j}}^{\varphi(k)-1} h_i s^i \bmod r$
3. Find the absolute smallest integer h_j satisfying $s^j h_j \equiv c \bmod r$, $h \leftarrow (h_0, \cdots, h_{j-1}, h_j, h_{j+1}, \cdots, h_{\varphi(k)-1})$
4. Endif $(\prod_{\substack{i=0 \\ h_i \neq 0}}^{\varphi(k)-1} |h_i|) \leq k r^{1/\varphi(k)}$, and $\sum_{i=0}^{\varphi(k)-1} h_i s^i \neq 0 \bmod r^2$
5. $j \leftarrow j + 1$
6. Output $h(x) = \sum_{i=0}^{\varphi(k)-1} h_i x^i$

In practice, $\sharp A_{k,j}$ is a small number which is dependent on the embedding degree k, hence all the cases in step 2 can be exhausted search. Applying the Euclidean algorithm, one can solve the following equation in step 3

$$s^j x \equiv c \bmod r.$$

Therefore, algorithm 2 is an efficient way to determine whether there exists an optimal polynomial with respect to $[k, s]$ modulus r. However, the following proposition shows that such optimal polynomial is rare which shows that the optimal pairing is sparse.

Theorem 2 *Let r be a prime number and s be a primitive k-root of unity modulo r^2. Let $l = \varphi(k)$. Then the number of polynomials, which have a root s and its degree are less than l in $\mathbb{F}_r[x]$ is $r^{l-1} - 1$. The number of optimal polynomials of degree less than l in $\mathbb{F}_r[x]$ with respect to $[k, s]$ modulo r is at most k^{2l}.*

Proof It is easy to see that there are exactly $r^l - 1$ nonzero polynomials of degree less than l in $\mathbb{F}_r[x]$. By the step 2 and step 3 of algorithm 2, one can see that if a polynomial has a root s, then any $l - 1$ coefficients of the polynomial can take freely in $\mathbb{F}_r$ and the l-th coefficient of the polynomial can be determined

uniquely by the $l-1$ coefficients. Hence the number of polynomials, which have a root s and its degree are less than l in $\mathbb{F}_r[x]$ is $r^{l-1}-1$. By proposition 2, any coefficient of an optimal polynomials with respect to k, s modulo r is at most k^2. Therefore, the number of optimal polynomials of degree less than l in $\mathbb{F}_r[x]$ with respect to $[k, s]$ modulo r is at most k^{2l}.

Remark. In practice, the embedding degree k is at most 50 and r is at least 2^{160}. Hence the optimal polynomials of degree less than l in $\mathbb{F}_r[x]$ with respect to $[k, s]$ modulo r is sparse.

4 New optimal pairings

In this section, we introduce some new optimal pairings. Given a positive integer k, let $r \in R = \{\Phi_k(x) | x \in \mathbb{Z}\}$ be a prime number i.e., there exists an integer s' such that $r = \Phi_k(s')$, where $\Phi_k(x)$ is the kth cyclotomic polynomial. In this section, we suppose that $s' \geq 3k$. Let

$$h_i(x) = x^i - s'x^{i-1}, 1 \leq i \leq k.$$

The main result in this section is the following theorem.

Theorem 3 *Let r, s' and $h_i(x), 1 \leq i \leq k$ be defined as above, and s be a k-th primitive root of unity modulus r^2 and $s \equiv s' \bmod r$. Then*

1. *for $1 \leq i \leq k$, a_{s,h_i} are optimal pairings;*
2. *a_{s,h_1} is the general optimal ate pairing.*

The main steps in the proof of Theorem 3 are the following results.

Lemma 1 *Let $\Phi_k(x)$ be the kth cyclotomic polynomial. Let r be a prime number and s' be an integer such that $r = \Phi_k(s')$. Then*

$$\frac{s'^l}{s'^l + l(s'+1)^{l-1}} r \leq s'^l \leq \frac{s'^l}{s'^l - l(s'+1)^{l-1}} r.$$

Proof It is well-known that the kth cyclotomic polynomial is as follows

$$\Phi_k(x) = \prod_{\substack{\omega \in \mathbb{C} \text{primitive} \\ nth \text{root of unity}}} (x - \omega) = \prod_{\substack{1 \leq a \leq k \\ (a,k)=1}} (x - e^{2\pi i a/k}) \in \mathbb{Z}[x],$$

hence it can be rewritten as

$$\Phi_k(x) = x^l + c_{l-1}x^{l-1} + \cdots + c_1 x + 1,$$

where $l = \varphi(k)$, and $|c_i| \leq \begin{pmatrix} l \\ i \end{pmatrix}$. Therefore

$$s'^l - \sum_{0 \leq i \leq l-1} \begin{pmatrix} l \\ i \end{pmatrix} s'^i \leq \Phi_k(s') \leq s'^l + \sum_{0 \leq i \leq l-1} \begin{pmatrix} l \\ i \end{pmatrix} s'^i.$$

Since $\begin{pmatrix} l \\ i \end{pmatrix} \leq l \begin{pmatrix} l-1 \\ i \end{pmatrix}$, we have

$$\sum_{0 \leq i \leq l-1} \begin{pmatrix} l \\ i \end{pmatrix} s'^i \leq \sum_{0 \leq i \leq l-1} l \begin{pmatrix} l-1 \\ i \end{pmatrix} s'^i = l(s'+1)^{l-1},$$

Which implies that

$$\frac{s'^l}{s'^l + l(s'+1)^{l-1}} \Phi_k(s') \leq s'^l \leq \frac{s'^l}{s'^l - l(s'+1)^{l-1}} \Phi_k(s').$$

Lemma 2 *Let r be a prime number and k be an integer satisfying that $k|r-1$. Then the number of solutions in the equation $x^k \equiv 1(\mathrm{mod} r)$ is k. If $s^k \equiv 1(\mathrm{mod} r^2)$, then s can be written as $s = x_0 + y_0 r \bmod r^2$, where*

$$x_0^k \equiv 1 \bmod r, \quad y_0 \equiv (kr)^{-1}(x_0^{1-k} - x_0) \bmod r.$$

Proof Since r is a prime number, there exists an generator element g in $\mathbb{Z}_r^*$, i.e., for any $\alpha \in \mathbb{Z}_r^*$ there is an unique integer $1 \leq a \leq r-1$ such that $\alpha \equiv g^a \bmod r$. By the assumption of $k|r-1$, it is easy to see that

$$\alpha^k \equiv 1 \bmod r \Longleftrightarrow \frac{r-1}{k} | a.$$

This proves the first part of the lemma.

If $s^k \equiv 1(\mathrm{mod} r^2)$, then $s^k \equiv 1(\mathrm{mod} r)$ holds. Assume that $s^k \equiv 1(\mathrm{mod} r^2)$, then s can be written as $s \equiv x_0 + y_0 r \bmod r^2$, where $x_0^k \equiv 1 \bmod r$. Therefore we have

$$\begin{aligned} s^k &\equiv (x_0 + y_0 r)^k \bmod r^2 \\ &\equiv x_0^k + k x_0^{k-1} y_0 r \bmod r^2 \\ &\equiv 1 \bmod r^2, \end{aligned}$$

which completes the proof of the second part of the lemma.

Lemma 3 *Let r, s' be defined as above, and s be a k-th primitive root of unity modulus r^2 and $s \equiv s' \bmod r$. Then, for all $1 \leq i \leq k$, we have $h_i(s) \equiv 0 \bmod r$ and $h_i(s) \neq 0 \bmod r^2$.*

Proof By the assumption of the lemma, it is not difficult to see that $s' \neq s \bmod r^2$. Since $s \equiv s' \bmod r$, and by the definition of $h_i(x)$, we have

$$h_i(s) \equiv 0 \bmod r.$$

Suppose $h_i(s) \equiv 0 \bmod r^2$, then we have

$$s^i \equiv ss'^{i-1} \bmod r^2.$$

Since $\gcd(s, r) = 1$, this gives $s' \equiv s \bmod r^2$, which contradicts to $s' \neq s \bmod r^2$, and the proof is complete.

Proof of Theorem 3 By the assumption of Theorem 3 and from Lemmas 2 and 3, there exists s satisfying $s \equiv s' \bmod r$ and

$$h_i(s) \equiv 0 \bmod r, \quad h_i(s) \neq 0 \bmod r^2, \quad 1 \leq i \leq k.$$

Hence, by fact 1, for all $1 \leq i \leq k$, a_{s,h_i} are non-degenerate bilinear pairings.

Collected the results in Lemma 1 and Theorem 1 and by the definition of $h_i(x)$, it is easy to see that the number of basic Miller iterations to compute a_{s,h_i} is at most

$$\log s' + \omega(h_i) - 1 \leq (\log_2 \frac{s'^l}{s'^l - l(s'+1)^{l-1}} r)/\varphi(k) + 1 \leq (\log_2 r)/\varphi(k) + 2,$$

where we have used $s' \geq 3k$. By the definition of optimal pairing, one can see that a_{s,h_i} are optimal pairings.

Since $s' \equiv s \bmod r$ and $Q \in E(\mathbb{F}_q)[r]$, we can obtain

$$(f_{s,h_1,Q}) = (sQ) - s'(Q) + (s'-1)(\mathcal{O}) = (sQ) - s'(Q) + (s'-1)(\mathcal{O}),$$

so $a_{s,h_1}(Q, P) = f_{s,h_1,Q}(P)^{q^k-1/r}$ is an optimal ate pairing.

5 Constructing pairing-friendly elliptic curves with optimal pairing

In this section, we introduce an explicit algorithms to construct pairing-friendly elliptic curve on which the optimal pairings a_{s,h_i} can be defined.

5.1 Construction methods

The following well-known observation[11] is crucial for the construction of prime-order curves with embedding degree k.

Lemma 4 *Let k be a positive integer, $E/\mathbb{F}_q$ an elliptic curve with $\sharp E(Fq) = hr$ where r is prime, and let t be the trace of $E/\mathbb{F}_q$. Assume that $r \nmid k$. Then $E/\mathbb{F}_q$ has embedding degree k with respect to r if and only if $\Phi_k(q) \equiv 0(\mathrm{mod} r)$, or, equivalently, if and only if $\Phi_k(t-1) \equiv 0(\mathrm{mod} r)$.*

The following algorithm gives a procedure for constructing pairing-friendly curve with an optimal pairing. Modifying the Cocks-Pinch method, we get the following construction method in which the discriminant D can be chosen arbitrarily. The idea of the following algorithm can be found in some papers for constructing of family pairing friendly curve, as an example see [14]. Here, we apply this idea to construct a pairing friendly elliptic curve explicitly.

Algorithm 3 Algorithm for finding an elliptic curve with optimal pairings

Input: Fix a positive integer k and a positive square-free integer D

Output: q, r, t

1. Find a prime number $r = \Phi_k(s')$ in the sequence
   $$R = \{\Phi_k(x) | x \in \mathbb{Z}\}$$
   satisfying $(\frac{-D}{r}) = 1$
2. Let $t = s' + 1$, and $y_0 = (t-2)/\sqrt{-D} \bmod r$
3. Let y be the unique lift of y_0 to $(0, r]$ and $q = (t^2 + Dy^2)/4$
4. Output q, r, t

If q is an integer and prime, then there exists an elliptic curve E over $\mathbb{F}_q$ with a subgroup of order r and embedding degree k. If $D < 10^{10}$ then E can be constructed via the CM method.

We observe that there is no reason to believe that y is much smaller than r, and thus in general $q \approx r^2$. We conclude that the curves produced by this method tend to have ρ-value around 2. In this algorithm the CM discriminant D is chosen arbitrarily.

5.2 Analysis of the construction methods

In this section, we analyse the efficiency of our construction methods.

Step 1 of algorithm 3 is motivated by the fact: if $f(x) \in \mathbb{Z}[x]$, then a famous conjecture of Buniakowski and Schinzel (see [19], p. 323) says that a nonconstant $f(x)$ takes an infinite number of prime values if and only if f has positive leading coefficient, f is irreducible, and $\gcd(\{f(x) : x \in \mathbb{Z}\}) = 1$. Cyclotomic polynomial $\Phi_k(x)$ of which the leading coefficient is 1, is irreducible, and $\Phi_k(0) = 1$, i.e. $\Phi_k(x)$ satisfies the conditions of the conjecture. In practice, one can often find a prime number in the sequence $R = \{\Phi_k(x) | x \in \mathbb{Z}\}$.

There exists polynomial time algorithm to compute the square root of $-D \bmod r$, specially when $r \equiv 3 \bmod 4$, $\sqrt{-D} \equiv (-D)^{(r+1)/4} \bmod r$. Hence step 2 of algorithm 3 is efficient.

Collecting the above discussion, for a given integer k, we can apply algorithm 3 to construct an elliptic curve with embedding degree k on which the optimal pairings a_{s,h_i} can be defined.

5.3 Numberical examples

All of the following curves have an optimal pairing defined on it.

Example 1 Let $k = 5$ and $s = 57094839957$. We set

$$\begin{aligned} r &= 346402613132596898814774496698704450863800426740491114025940435 43 \\ t &= 57094839958 \\ q &= 399982567950305311559257648093755592145223213687850333294366871 91 \\ &\quad 123556666575762132392241523793359515942766370957652420975279912 4 \end{aligned}$$

Then the optimal pairing polynomial with respect to k, s modulo r are

$$x^i - 57094839957x^{i-1}, \quad 1 \leq i \leq 5.$$

Example 2 Let $k = 9$ and $s = 261570885$. We set

$$\begin{aligned} r &= 320284860597467165903904990581461251942458624919751 \\ t &= 261570886 \\ q &= 341941306426463241768623925118459711481212713770919 \\ &\quad 555568631159130511549535072242882251249646808130 76 \end{aligned}$$

Then the optimal pairing polynomial with respect to k, s modulo r are

$$x^i - 261570885x^{i-1}, \quad 1 \leq i \leq 9.$$

Example 3 Let $k = 23$ and $s = 1023$. We set

$$\begin{aligned} r = {} & 168874592200122720489359717298798075849920643510192970849797341919 2320 \\ t = {} & 1024 \\ q = {} & 165912523864570880015933398889413140089476443580742448460810467353231 9 \\ & 669194786771008601182809331447396172665876895208843254029702370960387 \end{aligned}$$

Then the optimal pairing polynomial with respect to k, s modulo r are

$$x^i - 1023x^{i-1}, \quad 1 \leq i \leq 23.$$

6 Conclusion

In this paper, we consider the optimal pairing which was introduced by Vercautern and give some properties of optimal pairing. Our result shows that the optimal pairing is rare. However, we can construct many optimal pairings by using cyclotomic polynomial and provide an explicit method to construct pairing friendly curves with optimal pairing. Our algorithm works for arbitrary embedding degree k and large prime subgroups order r. In this paper, we provide an algorithm for finding an optimal pairing if there exists one which is defined on the given elliptic curve.

References

[1] D. Boneh and M. Franklin, Identity-based Encryption from the Weil pairing, CRYPTO 2001, Lecture Notes on Computer Science, Vol. 2139, pp.213-229, 2001.

[2] J.Bernstein, J. W. Lenstre, AND J. Pila Detecting perfect powers by factoring into coprimes, Math. Comp, Vol 76, no.257, pp.385-388, 2007.

[3] P. S. L. M. Barreto, S. Galbraith, C. Ó hÉigeartaigh, and M. Scott, Efficient pairing computation on supersingular abelian varieties, *Designs, Codes and Cryptography*, **42**(2007) 239-271.

[4] P. S. L. M. Barreto, H. Y. Kim, B. Lynn and M. Scott, Efficient algorithms for pairing-based cryptosystems, in *Advances in Cryptology-CRYPTO '2002*, LNCS 2442, 2002, pp.354-368.

[5] Ian Blake, Gadiel Seroussi & Nigel Smart, Elliptic Curves in Cryptography, Cambridge University Press, 1999.

[6] Ian Blake, Gadiel Seroussi & Nigel Smart, (ed.) Advances in Elliptic Curve Cryptography, Cambridge University Press, 2004.

[7] D. Boneh, B. Lynn and H. Shacham, Short Signatures from Weil pairing, ASIACRYPT 2001, Lecture Notes on Computer Science, Vol. 2248, pp.514-532, 2001.

[8] F. Brezing and A. Weng. Elliptic Curves Suitable for Pairing Based Cryptography. In Designs, Codes and Cryptography,vol 37(1), pages 133-141, 2005.

[9] I. Duursma and H. -S Lee, Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$, in *Advances in Cryptology–Asiacrypt'2003*, LNCS 2894, pp. 111-123.

[10] P.S.L.M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. In SAC 2005 - Selected Areas in Cryptography, volume 3897 of Lecture Notes in Computer Science, pages 319-331. Springer, 2006.

[11] D. Freeman, M. Scott, E. Teske, A taxonomy of pairing-friendly elliptic curves, To appear in Journal of Cryptology 2009.

[12] D. Freeman. Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10. In Algorithmic Number Theory Symposium ANTS-VII, volume 4076 of Lecture Notes in Computer Science, pages 452-465. Springer-Verlag, 2006.

[13] S. Galbraith, K. Harrison and D. Soldera, Implementing the Tate pairing, in *Algorithm Number Theory, ANTS-V*, LNCS 2369, 2002, pp.324-337.

[14] S. Galbraith, F. Hess, and F. Vercauteren, Aspects of Pairing Iversion, IEEE Transactions on Information Theory, 54(12):5719-5728, 2008.

[15] R. Granger, F. Hess, R. Oyono, N. Theriault and F. Vercauteren. Ate Pairing on Hyperelliptic Curves. In EUROCRYPT 2007, volume 4515 of Lecture Notes in Computer Science, pages 430-447. Springer-Verlag, 2007.

[16] Florian Hess, Pairing Lattices, In Pairing 2008, volume 5209 of Lecture Notes in Computer Science, pages 18-38. Springer-Verlag, 2008.

[17] F. Hess, N. Smart, and F. Vercauteren. The Eta-pairing revisited. IEEE Transactions on Information Theory, 52(10):4595-4602, 2006.

[18] E.J. Kachisa, E.F. Schaefer and M. Scott. Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field. In Pairing 2008, volume 5209 of Lecture Notes in Computer Science, pages 126-135. Springer-Verlag, 2008.

[19] S. Lang. Algebra, revised 3rd edition. Springer, 2002.

[20] E. Lee, H.-S. Lee, and C.-M. Park. Efficient and Generalized Pairing Computation on Abelian Varieties. Preprint, 2008. Available from http://eprint.iacr.org/2008/040.

[21] R. Lidl, and H. Niederreiter, Finite Fields. Cambridge University Press, 1997.

[22] S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto. Optimised versions of the Ate and twisted Ate pairings. In The 11th IMA International Conference on Cryptography and Coding, volume 4887 of Lecture Notes in Computer Science, pages 302-312. Springer-Verlag, 2007.

[23] V. S. Miller. The Weil pairing, and its efficient calculation. J. Cryptology, 17(4):235-261, 2004.

[24] 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.

[25] R. Sakai, K. Ohgishi and M. Kasahara, Cryptosystems based on pairing, SCIS 2000, 2000.

[26] J.H. Silverman, The Arithmetic of Elliptic Curves, Springer, Berlin, 1986.

[27] F. Vercauteren, Optimal Pairings, To appear in IEEE Transactions on Information Theory, 2009.