Computing the Bilinear Pairings on Elliptic Curves with Automorphisms

Chang-An Zhao[1,2,3] and Fangguo Zhang[2,3]

[1] School of Computer Science and Educational Software, Guangzhou University,
Guangzhou 510006, P.R.China

[2] School of Information Science and Technology, Sun Yat-Sen University,
Guangzhou, 510275, P.R.China

[3] Guangdong Key Laboratory of Information Security Technology,
Guangzhou 510275, P.R.China

changanzhao@gmail.com

isszhfg@mail.sysu.edu.cn

Abstract. In this paper, a super-optimal pairing based on the Weil pairing is proposed with great efficiency. It is the first approach to reduce the Miller iteration loop when computing the variants of the Weil pairing. The super-optimal pairing based on the Weil pairing is computed rather fast, while it is slightly slower than the previous fastest pairing on the corresponding elliptic curves.

Keywords: Weil pairing, super-optimal pairing, non-supersingular curves, automorphisms.

1 Introduction

In 1985, Victor Miller discovered a polynomial-time algorithm for computing the Weil pairing on elliptic curves in an unpublished (but widely distributed and cited) manuscript [19]. Since pairings on elliptic/hyperelliptic curves may find many interesting cryptographic applications [22], much attention has been paid to Miller's algorithm in recent years.

Many optimizations from different angles have been devised for practical implementations [7, 1]. One of the most efficient techniques is to reduce the iteration loops in Miller's algorithm. Inspired by the main idea, the researchers have proposed some variants of the Tate pairing with great efficiency, such as the eta pairing [3], the ate pairing and its variants [12, 18, 30], as well as the R-ate pairing [14].

Computing the traditional Tate/Weil pairings requires $\log_2 r$ Miller iteration loops with r the order of the corresponding groups. In [29], an optimal pairing is defined if it can be computed in $\log_2 r/\varphi(k)$ basic Miller iteration loops with k the embedding degree. If the number of the Miller iteration loops is smaller than $\log_2 r/\varphi(k)$, the corresponding pairing is called super-optimal. Motivated by GLV methods [9], Scott constructs a super-optimal pairing based on the Tate pairing in [23]. Hess presents an integral framework that covers all known fast pairing functions based on the Tate pairing [11].

However, there exist no references to shortening the Miller iteration loops in the Weil pairing computation for good efficiency. In this paper, we first investigate to speed up the computation of the Weil pairing with short Miller iteration loops under several certain conditions and then obtain some amazing results. Computing the pairings on elliptic curves with the embedding degree $k = 2$ has many conveniences, which was described clearly in [24]. Also, point compression techniques can be used [8]. Thus this paper is also devoted to computing the pairings in this case.

We present a novel derivation of the super-optimal pairing based on the Tate pairing in [23]. On the basis of the results, we construct some new variants of the Weil pairing which are also super-optimal. Using the super-optimal pairings based on the Weil pairing, the loop length in Miller's algorithm will be half the length of that required for the standard Tate/Weil pairing. It is the first approach to reduce the Miller iteration loops when computing the variants based on the Weil pairing, although computing the new pairings is slightly slower than computing the previous fastest pairings on the corresponding curves.

The rest of this paper is organized as follows. Section 2 introduces the basic pairing and a family of non-supersingular elliptic curves with non-trivial automorphisms. Section 3 gives the main results and Section 4 applies them into pairing computations. Section 5 analyzes the efficiency of the proposed algorithm and compares it with the previous other methods. Section 6 draws the conclusions.

2 Preliminaries

This section briefly recalls the definitions of the Tate pairing and the Weil pairing which were used to evaluate the elliptic curve discrete logarithm problem in [6, 17] and describes Miller's algorithm to compute the pairings. Then we introduce a family of elliptic curves with non-trivial automorphisms for interest.

2.1 Tate Pairing

Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements, where p is a prime. Let E be an elliptic curve defined over $\mathbb{F}_q$, and let $\mathcal{O}$ be the point at infinity. Let r be a prime such that $r|\#E(\mathbb{F}_q)$, where $\#E(\mathbb{F}_q)$ is denoted as the order of $E(\mathbb{F}_q)$. Let k be the embedding degree. Assume that r^2 does not divide $q^k - 1$ and k is greater than 1. $E[r]$ is denoted as the $r-$torsion group of E.

Let $P \in E[r]$ and $R \in E(\mathbb{F}_{q^k})$. Let D_P be the divisor which is linearly equivalent to $(P) - (\mathcal{O})$. For every integer i and point P, let $f_{i,P}$ be a function such that $(f_{i,P}) = i(P) - (iP) - (i-1)(\mathcal{O})$. In particular, $(f_{r,P}) = rD_P$. Let μ_r be the r-th roots of unity in $\mathbb{F}_{q^k}^*$. Then the reduced Tate pairing is defined as follows [4]

$$e : E[r] \times E(\mathbb{F}_{q^k}) \to \mu_r,$$

$$e(P,R) = f_{r,P}(R)^{\frac{q^k-1}{r}}.$$

Notice that $f_{r,P}(R)^{a(q^k-1)/r} = f_{ar,P}(R)^{(q^k-1)/r}$ for any integer a.

2.2 Weil Pairing

Using the same notation as previous, one may make a few slight modifications and then define the Weil pairing. Let k be the minimal positive integer such that $E[r] \subset E(\mathbb{F}_{q^k})$. According to the results in [2], if $r \nmid q-1$ and $(r,q) = 1$, then $E[r] \subset E(\mathbb{F}_{q^k})$ if and only if $r|q^k - 1$, i.e., the embedding degree for the Weil pairing is equal to the embedding degree for the Tate pairing in this case.

Suppose that $P,\ Q \in E[r]$ and $P \neq Q$. Let D_P and D_Q be two divisors which are linearly equivalent to $(P) - (\mathcal{O})$ and $(Q) - (\mathcal{O})$, respectively. Let $f_{r,P}$ and $f_{r,Q}$ be two rational functions on E with $(f_{r,P}) = rD_P$ and $(f_{r,Q}) = rD_Q$. Then the Weil pairing is a map [20]

$$e_r : E[r] \times E[r] \to \mu_r,$$

$$e_r(P,Q) = (-1)^r \frac{f_{r,P}(Q)}{f_{r,Q}(P)}.$$

For fast pairing computations, one can define the powered Weil pairing [16, 15] as

$$\hat{e}_r(P,Q) = e_r(P,Q)^{(q^d-1)},$$

where d is a divisor of k. Notice that the denominator elimination technique can be used when computing the powered Weil pairing. Particularly, one may define the powered Weil pairing as $\hat{e}_r(P,Q) = e_r(P,Q)^{(q-1)}$ in the case of $k=2$.

2.3 Miller's Algorithm

In this subsection, we briefly recall how the Tate pairing can be computed in polynomial time using Miller's algorithm [19].

Let $P \in E[r]$ and $R \in E(\mathbb{F}_{q^k})$. Let $l_{S,T}$ be the equation of the line through points S and T, and let v_T be the equation of the vertical line through point T. Then for $i,j \in \mathbb{Z}$, we have

$$f_{i+j,P}(Q) = f_{i,P}(Q) f_{j,P}(Q) \frac{l_{iP,jP}(Q)}{v_{(i+j)P}(Q)}.$$

Miller's algorithm is described in Algorithm 1.

Algorithm 1: Miller's algorithm

```
Input: $r = \sum_{i=0}^{n} l_i 2^i$, where $l_i \in \{0,1\}$. $P \in E[r]$
and $R \in E(F_{q^k}),\ R \neq P$.
Output: $e(P,R)$
1. $T \leftarrow P,\ f \leftarrow 1$
2. for $i = n-1, n-2, \cdots, 1, 0$ do
   2.1 $f \leftarrow f^2 \cdot \frac{l_{T,T}(R)}{v_{2T}(R)},\ T \leftarrow 2T$
   2.2 if $l_i = 1$ then
   2.3 $f \leftarrow f \cdot \frac{l_{T,P}(R)}{v_{T+P}(R)},\ T \leftarrow T + P$
3. return $f^{(q^k-1)/r}$
```

2.4 A Family of Elliptic Curves with Non-trivial Automorphisms

Let p be a large prime. Consider the underlying non-supersingular elliptic curves over $\mathbb{F}_p$

$$\begin{aligned} E_1: \ y^2 =& x^3 + B, \text{where } p \ \equiv 1 \bmod 3, \\ E_2: \ y^2 =& x^3 + Ax, \text{where } p \ \equiv 1 \bmod 4. \end{aligned}$$

Both them have efficiently-computable endomorphisms which were applied in fast point multiplication [9] and the computation of the Tate pairing [23]. In fact, these endomorphisms are also non-trivial automorphisms which were used in speeding up the discrete log computation [5]. It is worth remarking that only the two non-supersingular elliptic curves with j-invariant $j = 0$ or 1728 have non-trivial automorphisms (see Silverman [27] page 103).

The conveniences of using pairing-friendly curves with $k = 2$ in pairing computations are discussed clearly in [24]. Therefore, we will mainly consider the first curve E_1 with $k = 2$ for speeding up the computation of the pairings in this paper. It should be clear that the results generalize easily to the second curve E_2. Notice that some suitable curves like E_1 with low embedding degrees have been constructed in [23, 28] and can be applied in pairing based cryptography.

Suppose that β is an element of order three in $\mathbb{F}_p$. A non-trivial automorphism of the above curve E_1 is defined as

$$\phi : E_1 \to E_1,$$

$$(x, y) \to (\beta x, y).$$

Since this automorphism ϕ is also an isogeny, its dual isogeny is defined as

$$\hat{\phi} : E_1 \to E_1,$$

$$(x, y) \to (\beta^2 x, y).$$

It is easily seen that $\hat{\phi} \circ \phi = [1]$, $\phi^2 = \hat{\phi}$ and $\# ker\phi = 1$ (see Silverman [27] pages 84-86). Note that $\hat{\phi}$ is also a non-trivial automorphism on the first curve E_1.

We cite some useful facts from [9]. Let $P \in E_1(\mathbb{F}_p)$ be a point of prime order r, where r^2 does not divide the order of $E_1(\mathbb{F}_p)$. Then ϕ and $\hat{\phi}$ act restrictively on the subgroup $<P>$ as multiplication maps $[\lambda]$ and $[\hat{\lambda}]$ respectively, i.e., $\phi(P) = \lambda P$, where λ and $\hat{\lambda}$ are the two roots of the equation: $x^2 + x + 1 = 0 \pmod r$. Note that $\lambda P = \phi(P)$ can be computed using one multiplication in $\mathbb{F}_p$.

Let $E_1^{'}$ be the twisted elliptic curve of E_1 with the equation $E_1^{'}: \ y^2 = x^3 + B/D^3$, where D is a quadratic non-residue in $\mathbb{F}_p^*$. Then $E_1^{'}(\mathbb{F}_p)$ has a subgroup $< Q' >$ of order r since the embedding degree k is 2. Two non-trivial automorphisms ϕ' and $\hat{\phi}'$ of $E_1^{'}$ can be defined as

$$\begin{array}{ll} \phi' : E_1^{'} \rightarrow E_1^{'}, & \hat{\phi}' : E_1^{'} \rightarrow E_1^{'}, \\ (x, y) \rightarrow (\beta x, y), & (x, y) \rightarrow (\beta^2 x, y). \end{array}$$

Assume that r^2 does not divide $\#E_1'(\mathbb{F}_p)$. By using the same argument as above, ϕ' and $\hat{\phi}'$ act restrictively on the subgroup $<Q'>$ as multiplication maps $[\hat{\lambda}]$ and $[\lambda]$ respectively, where $\hat{\lambda}$ and λ are defined same as above. In practice, it can be checked that $\lambda Q' = \hat{\phi}'(Q')$ and $\hat{\lambda} Q' = \phi'(Q')$ using straightforward calculations. However, we can give an explicit explanation in the following (see Lemma 4).

There exists an isomorphism

$$\psi : E_1^{'} \rightarrow E_1,$$

$$(x, y) \rightarrow (Dx, yD^{\frac{3}{2}})$$

defined over $\mathbb{F}_{p^2}$. Put Q=$\psi(Q')$. Then Q is a point in $E_1(\mathbb{F}_{p^2})[r]$. Since $< Q >$ is isomorphic to $< Q' >$, it leads to $\lambda Q = \hat{\phi}(Q)$ if $\lambda Q' = \hat{\phi}'(Q')$. This observation is the key to construct the super-optimal pairing based on the Weil pairing.

3 Main Results

In this section, we present some novel pairings which are super-optimal. The main results of this paper are summarized in the following theorems.

Theorem 1. *Let p be a large prime such that $p \equiv 1 \pmod 3$. Let E_1 be a non-supersingular curve over $\mathbb{F}_p$ with the equation: $y^2 = x^3 + B, \ B \in \mathbb{F}_p^*$. Let $k = 2$ be the embedding degree. Two non-trivial automorphisms of E_1 are defined as $\phi : E_1 \rightarrow E_1, (x, y) \rightarrow (\beta x, y)$ and $\hat{\phi} : E_1 \rightarrow E_1, (x, y) \rightarrow (\beta^2 x, y)$ respectively. Let $P \in E_1(\mathbb{F}_p)[r]$ be a point satisfying $\phi(P) = \lambda P$, where λ is a root of the equation: $x^2 + x + 1 = 0 \pmod r$. Let a be an integer such that $ar = \lambda^2 + \lambda + 1$. $l_{\phi(P), \hat{\phi}(P)}$ is denoted as the equation of the line through points $\phi(P)$ and $\hat{\phi}(P)$. Then for $R \in E_1(\mathbb{F}_{p^k})$, we have*

$$e(P, R)^a = (f_{\lambda,P}(R)^{\lambda+1} \cdot f_{\lambda,P}(\hat{\phi}(R)) \cdot l_{\phi(P),\hat{\phi}(P)}(R))^{\frac{p^2-1}{r}}.$$

Note that there does exist such an integer a since $\lambda^2 + \lambda + 1 = 0 \pmod r$. We also remark that $e(P,R)^a$ is equal to a fixed power of the reduced Tate pairing and keeps non-degeneracy provided that r does not divide a. The proof of Theorem 1 is based on three short lemmas as follows.

Lemma 1. *Using the notation of Theorem 1, we have*

$$e(P,R)^a = (f_{\lambda^2+\lambda,P}(R) \cdot l_{-P,P}(R))^{\frac{p^k-1}{r}}.$$

Proof. It is obvious from the definition of the reduced Tate pairing that

$$e(P,R)^a = f_{r,P}(R)^{\frac{a(p^k-1)}{r}} = f_{ar,P}(R)^{\frac{p^k-1}{r}}.$$

Applying the identity $ar = \lambda^2 + \lambda + 1$ into the above equation, we obtain

$$e(P,R)^a = f_{ar,P}(R)^{\frac{p^k-1}{r}} = f_{\lambda^2+\lambda+1,P}(R)^{\frac{p^k-1}{r}}.$$

According to $(\lambda^2 + \lambda)P = -P$, we see that

$$(f_{\lambda^2+\lambda+1,P}) = (f_{\lambda^2+\lambda,P} \cdot f_{1,P} \cdot l_{-P,P}).$$

Since $f_{1,P} = 1$ up to a scalar multiple in $\mathbb{F}_p^*$, it follows that

$$e(P,R)^a = f_{\lambda^2+\lambda+1,P}(R)^{\frac{p^k-1}{r}} = (f_{\lambda^2+\lambda,P}(R) \cdot l_{-P,P}(R))^{\frac{p^k-1}{r}}$$

This completes the proof of Lemma 1.

Lemma 2. *Using the notation of Theorem 1, we can choose $f_{\lambda^2+\lambda,P} l_{-P,P}$ such that*

$$(f_{\lambda^2+\lambda,P} \cdot l_{-P,P}) = (f_{\lambda,P}^{\lambda+1} \cdot f_{\lambda,\lambda P} \cdot l_{\phi(P),\hat{\phi}(P)}).$$

Proof. Note that $(f_{i,P}) = i(P) - (iP) - (i-1)(\mathcal{O})$ and $(\lambda^2 + \lambda)P = -P$. Then

$$\begin{aligned}(f_{\lambda^2+\lambda,P} \cdot l_{-P,P}) =& (f_{\lambda^2,P} \cdot f_{\lambda,P} \cdot \frac{l_{\lambda^2 P,\lambda P}}{l_{(\lambda^2+\lambda)P,-(\lambda^2+\lambda)P}} \cdot l_{-P,P}) \\ =& (f_{\lambda^2,P} \cdot f_{\lambda,P} \cdot l_{\lambda^2 P,\lambda P}).\end{aligned}$$

Since $\lambda P = \phi(P)$ and $\lambda^2 P = \phi^2(P) = \hat{\phi}(P)$, we have

$$l_{\lambda^2 P,\lambda P} = l_{\lambda P,\lambda^2 P} = l_{\phi(P),\hat{\phi}(P)}.$$

Also, (see Lemma 2 in [3])

$$(f_{\lambda^2,P}) = (f_{\lambda,P}^{\lambda} \cdot f_{\lambda,\lambda P}).$$

Hence

$$(f_{\lambda^2+\lambda,P} \cdot l_{-P,P}) = (f_{\lambda^2,P} \cdot f_{\lambda,P} \cdot l_{\lambda^2 P,\lambda P}) = (f_{\lambda,P}^{\lambda+1} \cdot f_{\lambda,\lambda P} \cdot l_{\phi(P),\hat{\phi}(P)})$$

which completes the proof.

Lemma 3. *For $P \in E_1[r]$ and $R \in E_1(\mathbb{F}_{p^k})$, we have $f_{\lambda,\lambda P}(R) = f_{\lambda,P}(\hat{\phi}(R))$, with $\hat{\phi}$ defined as above.*

Proof. By definition, $(f_{\lambda,\lambda P}) = \lambda(\lambda P) - (\lambda^2 P) - (\lambda - 1)(\mathcal{O})$. Note that $\phi(P) = \lambda P$ and $\#ker\phi = deg[1] = 1$ (see [27] Chapter III pages 85-86). Since ϕ is an automorphism of the curve and thus separable of degree 1, we get

$$\begin{aligned} \phi^*(f_{\lambda,\lambda P}) =& \phi^*(\lambda(\lambda P) - (\lambda^2 P) - (\lambda - 1)(\mathcal{O})) \\ =& \lambda(P) - (\lambda P) - (\lambda - 1)(\mathcal{O}) \\ =& (f_{\lambda,P}). \end{aligned}$$

On the other hand, $\phi^*(f_{\lambda,\lambda P}) = (f_{\lambda,\lambda P} \circ \phi)$. Hence, we have (up to a scalar multiple in $\mathbb{F}_p^*$)

$$f_{\lambda,\lambda P} \circ \phi = f_{\lambda,P}.$$

Applying $\hat{\phi}$ to the above equality yields

$$f_{\lambda,\lambda P} \circ \phi \circ \hat{\phi} = f_{\lambda,P} \circ \hat{\phi}.$$

Since $\phi \circ \hat{\phi} = [1]$, we have

$$f_{\lambda,\lambda P} = f_{\lambda,P} \circ \hat{\phi}.$$

This completes the proof.

Using the above lemmas, we will give a proof of Theorem 1 as follows.

Proof (of Theorem 1). Since $P \in E_1(\mathbb{F}_p)[r]$, Lemma 3 gives

$$f_{\lambda,\lambda P}(R) = f_{\lambda,P}(\hat{\phi}(R)).$$

Substituting the above equality into Lemma 2, we get

$$f_{\lambda^2+\lambda,P}(R) \cdot l_{-P,P}(R) = f_{\lambda,P}^{\lambda+1}(R) \cdot f_{\lambda,P}(\hat{\phi}(R)) \cdot l_{\phi(P),\hat{\phi}(P)}(R).$$

By applying the above equation to Lemma 1, we have

$$\begin{aligned} e(P,R)^a =& (f_{\lambda^2+\lambda,P}(R) \cdot l_{-P,P}(R))^{\frac{p^k-1}{r}} \\ =& (f_{\lambda,P}(R)^{\lambda+1} \cdot f_{\lambda,P}(\hat{\phi}(R)) \cdot l_{\phi(P),\hat{\phi}(P)}(R))^{\frac{p^k-1}{r}}. \end{aligned}$$

This completes the whole proof of Theorem 1.

By Theorem 1, we can define the super-optimal pairing based on the Tate pairing, which is similar to the main results in [23]. In connection with Theorem 1, we will construct some super-optimal pairings based on the Weil pairings in the following.

Theorem 2. *Let p be a prime such that $p \equiv 1 \pmod 3$. Let E_1 be a non-supersingular curve over $\mathbb{F}_p$ with the equation: $E_1 : y^2 = x^3 + B, B \in \mathbb{F}_p^*$. The quadratic twist E_1' is given by the equation $E_1' : y^2 = x^3 + B/D^3$, where D is a quadratic non-residue in $\mathbb{F}_p^*$. Assume that the embedding degree k of E is 2. Let r be a large prime which satisfies $r|\#E_1(\mathbb{F}_p)$, $r|\#E_1^{'}(\mathbb{F}_p)$, $r^2 \nmid \#E_1(\mathbb{F}_p)$ and $r^2 \nmid \#E_1^{'}(\mathbb{F}_p)$. Let $P \in E_1(\mathbb{F}_p)[r]$ and $Q' \in E_1'(\mathbb{F}_p)[r]$. An isomorphism is defined as $\psi : E_1^{'} \to E_1, (x, y) \to (Dx, D^{\frac{3}{2}}y)$. Put $Q = \psi(Q')$. Two non-trivial automorphisms ϕ and $\hat{\phi}$ of E_1 are defined as $(x, y) \to (\beta x, y)$ and $(x, y) \to (\beta^2 x, y)$, respectively. Let λ be the root of the equation $x^2+x+1 = 0 \pmod r$ such that $\lambda P = \phi(P)$ and $\lambda Q = \hat{\phi}(Q)$. Let a be an integer such that $ar = \lambda^2 + \lambda + 1$. Then for such P and Q, we have*

$$\hat{e_r}(P, Q)^a = ((\frac{f_{\lambda,P}(Q)}{f_{\lambda,Q}(P)})^{\lambda+1} \cdot \frac{f_{\lambda,P}(\hat{\phi}(Q))}{f_{\lambda,Q}(\phi(P))})^{p-1}.$$

On the same basis of the discussions for Theorem 1, one may show that there does exist such an integer a. Notice that $\hat{e}_r(P, Q)^a$ equals a fixed power of the Weil pairing. In addition, the non-degeneracy of $\hat{e}_r(P, Q)^a$ holds if $\hat{e}_r(P, Q)$ is non-degenerate and r does not divide a. In practical implementations, P and Q are often taken from the specific subgroups for fast pairing computations. Here we take $P \in E_1[r] \cap Ker(\phi - [\lambda])$ and $Q \in E_1[r] \cap Ker(\hat{\phi} - [\lambda])$.

The proof of Theorem 2 needs the following lemma.

Lemma 4. *Using the notation of Theorem 2, we have $\lambda(Q) = \hat{\phi}(Q)$.*

Proof. The isomorphism

$$\psi : E_1^{'} \to E_1,$$

$$(x, y) \to (Dx, D^{\frac{3}{2}}y)$$

maps $Q' \in E_1^{'}(\mathbb{F}_p)[r]$ to be in $E_1(F_{p^2})[r]$. Then we see that $< Q >$ is isomorphic to $< Q' >$. Let $Q' = (x_{Q'}, y_{Q'})$. Then $Q = (Dx_{Q'}, D^{\frac{3}{2}}y_{Q'})$. We have

$$\lambda Q = \lambda\psi(Q') = \psi(\lambda Q').$$

Since λ is a root of the equation $x^2 + x + 1 = 0 \pmod r$, $\lambda Q'$ must satisfy $\lambda Q' = \hat{\phi}'(Q')$ or $\lambda Q' = \phi'(Q')$, where $\hat{\phi}'$ and ϕ' are denoted in the previous Section 2.4. We will show that $\lambda Q' = \hat{\phi}'(Q')$ as follows.

Assume that $\lambda Q' = \phi'(Q')$. This implies that

$$\lambda Q = \lambda\psi(Q') = \psi(\lambda Q') = (\beta D x_{Q'}, y_{Q'} D^{\frac{3}{2}}) = \phi(Q).$$

Notice that $E_1[r]$ can be viewed as a 2-dimensional vector space and $\phi : E_1[r] \to E_1[r]$ be a linear map, whose characteristic polynomial is $g(x) = x^2 + x + 1$. It is not too hard to see that $\{P, Q\}$ is a basis for $E_1[r]$. According to $\phi(P) = \lambda(P)$ and $\phi(Q) = \lambda(Q)$, it is immediate that $\phi(S) = \lambda S$ for every point $S \in E_1[r]$, a contradiction to the characteristic polynomial $g(x) = x^2 + x + 1$ of ϕ [21]. Therefore, $\lambda Q = \hat{\phi}(Q)$. This completes the proof of Lemma 4.

It should be noted that, in general, $S \in E_1(\mathbb{F}_{p^2})[r]$ does not satisfy $\lambda(S) = \phi(S)$. In light of the above discussion, one arrives then at the following proof of Theorem 2.

Proof (of Theorem 2*).* By using the same argument for $f_{r,P}(Q)$ in Theorem 1, we obtain then

$$f_{r,Q}(P) = f_{\lambda,Q}(P)^{\lambda+1} \cdot f_{\lambda,Q}(\phi(P)) \cdot l_{\phi(Q),\hat{\phi}(Q)}(P).$$

According to Theorem 1, we have $f_{r,P}(Q) = f_{\lambda,P}(Q)^{\lambda+1} \cdot f_{\lambda,P}(\hat{\phi}(Q)) \cdot l_{\phi(Q),\hat{\phi}(P)}(Q)$. It is easy to see that $l_{\phi(Q),\hat{\phi}(Q)}(P)$ equals $-(l_{\phi(Q),\hat{\phi}(P)}(Q))$. Altogether,

$$\begin{aligned}\hat{e_r}(P,Q)^a =& (\frac{f_{\lambda,P}(Q)^{\lambda+1} \cdot f_{\lambda,P}(\hat{\phi}(Q)) \cdot l_{\phi(Q),\hat{\phi}(P)}(Q)}{f_{\lambda,Q}(P)^{\lambda+1} \cdot f_{\lambda,Q}(\phi(P)) \cdot l_{\phi(Q),\hat{\phi}(Q)}(P)})^{p-1} \\ =& ((\frac{f_{\lambda,P}(Q)}{f_{\lambda,Q}(P)})^{\lambda+1} \cdot \frac{f_{\lambda,P}(\hat{\phi}(Q))}{f_{\lambda,Q}(\phi(P))})^{p-1}.\end{aligned}$$

This completes the whole proof of Theorem 2.

Similar to the super-optimal pairing based on the Tate pairing, the new pairings in Theorem 2 can be named as the super-optimal pairing based on the Weil pairing. Notice that computing the new pairings only needs $\log_2 \lambda$ Miller iteration loops, which is generally a half of the number of the Miller loops for computing the standard Tate/Weil pairings.

4 Novel Algorithms for Computing the Pairings

On the basis of the information provided by Theorem 1, we can give an efficient algorithm for computing the super-optimal pairing based on the Tate pairing. Since it is totally similar to Algorithm 4 in [23], we do not repeat it for simplicity.

By Theorem 2, we establish an algorithm for computing the super-optimal pairing based on the Weil pairing in Algorithm 2. Let $\omega = a+bi \in \mathbb{F}_{p^2}$. Then the conjugate of ω can be defined as $\overline{a+bi} = a - bi$. Thus $\frac{1}{f_{\lambda,Q}(P)}$ can be replace by its conjugate $\overline{f_{\lambda,Q}(P)}$ according to the observations in [25]. Therefore one may share the same Miller variable f when computing $\frac{f_{\lambda,P}(Q)}{f_{\lambda,Q}(P)}$. By using the same techniques, we can compute $\frac{f_{\lambda,P}(\hat{\phi}(Q))}{f_{\lambda,Q}(\phi(P))}$. Finally, we employ Montgomery's trick to compute the scalar multiplications of P and Q' in affine coordinates. The above techniques are clearly discussed in [24, 10].

Algorithm 2: Computations of $\hat{e_r}(P,Q)^a$ using automorphisms

```
Input:$\lambda = \sum_{i=0}^{n} l_i 2^i$ , where $l_i \in \{0,1\}$. $P \in E_1(\mathbb{F}_p)[r]$ and $Q' \in E'_1(F_p)[r]$. $Q = \psi(Q')$.
Output: $\hat{e_r}(P,Q)^a$
1. $T \leftarrow P$, $T' \leftarrow Q'$, $f_1 \leftarrow 1$, $f_2 \leftarrow 1$,
2. for $i = n-1, n-2, \cdots, 1, 0$ do
  2.1 $f_1 \leftarrow f_1^2 \cdot l_{T,T}(Q) \cdot \overline{l_{\psi(T'),\psi(T')}(P)}$, $f_2 \leftarrow f_2^2 \cdot l_{T,T}(\hat{\phi}(Q)) \cdot \overline{l_{\psi(T'),\psi(T')}(\phi(P))}$,
        $T \leftarrow 2T$, $T' \leftarrow 2T'$
  2.2 if $l_i = 1$ then
  2.3 $f_1 \leftarrow f_1 \cdot l_{T,P}(Q) \cdot \overline{l_{\psi(T'),\psi(Q')}(P)}$, $f_2 \leftarrow f_2 \cdot l_{T,P}(\hat{\phi}(Q)) \cdot \overline{l_{\psi(T'),\psi(Q')}(\phi(P))}$,
        $T \leftarrow T + P$, $T' \leftarrow T' + Q'$
3. $f_1 \leftarrow f_1^{\lambda+1}$,
4. return $(f_1 \cdot f_2)^{(p-1)}$
```

5 Efficiency Consideration

Now the performance of the proposed algorithm is considered in this section. We neglect the cost of field additions and subtractions, as well as the cost of multiplication by small constants. The computational cost of one multiplication and one inverse in $\mathbb{F}_p^*$ is denoted as M and I, respectively. Assume that the computational cost of one inverse in $\mathbb{F}_p^*$ is $10M$. We also count one square as one multiplication in $\mathbb{F}_p^*$. One square and one multiplication in $\mathbb{F}_{p^2}$ is equal to $2M$ and $3M$, respectively. For convenient comparisons, we consider the pairing computation on the same curve in [23].

If affine coordinates are employed, one point doubling requires $1I + 4M$ and one point addition requires $1I+3M$ in $E(\mathbb{F}_p)$ respectively [13]. We first consider the cost of Line 2.1 in Algorithm 2. Computing directly $2T$ and $2T'$ requires $2I+8M$. However, due to Montgomery's trick, computing these two point doublings reduces to $1I + 11M$. Four line evaluations requires $4M$. The remained in Line 2.1 requires $16M$ for computing two squares and four multiplications in $\mathbb{F}_{p^2}$. Thus Line 2.1 in one iteration loop needs $41M$ if $1I = 10M$. It follows that the total cost for Line 2.1 is equal to $41 \cdot 80 = 3280M$.

It is not difficult to show that the total cost of Line 2.3 requires $35M$. The exponentiation in Line 3 requires $80{\cdot}2 = 160M$ using the Lucas laddering algorithm [26]. By now, we cost $3280 + 35 + 160 = 3475M$. There are one multiplication in $\mathbb{F}_{p^2}$ in Line 4 of Algorithm 2, which requires $3M$. The exponentiation $(p-1)$ requires five multiplications and one inverse in $\mathbb{F}_p^*$ since the Frobenius map can be used here. Thus the total contribution of Line 4 is $3 + 15 = 18M$. Therefore the total cost for Algorithm 2 is $3475 + 18 = 3493M$.

Finally, we compare the new algorithm with other methods at the same levels of security in Table 1. From the table, we conclude that the super-optimal pairing based on the Weil pairing can be computed rather fast, while it is slightly slower than the super-optimal pairing based on the Tate pairing.

Table 1. Cost comparisons of the proposed algorithms

Algorithm	Cost of Multiplications in $\mathbb{F}_p^*$
Algorithm 2	3493M
Algorithm 4 in [23]	3329M
Miller's algorithm in IBE Scheme [24]	4070M

6 Conclusion

In this paper, some efficient algorithms have been proposed for computing the variants of the Weil pairing on a family of non-supersingular curves with non-trivial automorphisms. It is the first step to speed up the variants based on the Weil pairing by using short Miller iteration loops. Our results show that the super-optimal pairing based on the Weil pairing is computed rather fast, while it is slightly slower than the previous fastest pairing. It is possible to further optimize the results and extend them into hyperelliptic curves. Finally, it should be remarked that there may exist other methods to reduce the Miller loop for the Weil pairing computation.

References

1. R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography.* Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.
2. R. Balasubramanian and N. Koblitz. The Improbability That an Elliptic Curve Has Sub-exponential Discrete Log Problem Under the Menezes-Okamoto-Vanstone Algorithm. J. Cryptology, 11, 141-145, 1998.
3. P.S.L.M. Barreto, S. Galbraith, C. ÓhÉigeartaigh, and M. Scott. Efficient Pairing Computation on Supersingular Abelian Varieties. *In Designs, Codes and Cryptography.* Springer-Verlag, 2005.
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*, volume 2442 of *Lecture Notes in Computer Science*, pages. 354-368. Springer-Verlag, 2002.
5. I. Duursma, P. Gaudry, and F. Morain. Speeding up the Discrete Log Computation on Curves with Automorphisms, *AsiaCrypt'99*, volume 1716 of *Lecture Notes in Computer Science*, pages. 203-121. Springer-Verlag, 1999.
6. G. Frey, M. Müller and H.-G. Rück. The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems, *IEEE Trans. Inform. Theory*, vol. 45, pp. 1717-1719, 1999.
7. S. Galbraith. Pairings, *Ch. IX of I.F.Blake, G.Seroussi, and N.P.Smart, eds., Advances in Elliptic Curve Cryptography.* Cambridge University Press, 2005.
8. S. Galbraith and X. Lin. Computing Pairings Using x-Coordinates Only. Preprint, 2008. Available from http://eprint.iacr.org/2008/019.
9. R.P. Gallant, R.J. Lambert and S.A. Vanstone. Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms, *In Advances in Cryptology - Crypto 2001*, volume 2139 of *Lecture Notes in Computer Science.* Springer- Verlag, 2001.
10. R. Granger and N.P. Smart. On Computing Products of Pairings. Technical Report CSTR-06-013, University of Bristol, May, 2006.

11. F. Hess. Pairing Lattices. Preprint, 2008. Available at http://eprint.iacr.org/2008/125.
12. F. Hess, N.P. Smart and F. Vercauteren. The Eta Pairing Revisited. *IEEE Transactions on Information Theory*, vol 52, Pages. 4595-4602, Oct. 2006. Also available from http://eprint.iacr.org/2006/110.
13. IEEE Std 1363-2000. Standard Specifications for Public-key Cryptography. IEEE P1363 Working Group, 2000.
14. E. Lee, H.-S. Lee, and C.-M. Park. Efficient and Generalized Pairing Computation on Abelian Varieties. Preprint, 2008. Available at http://eprint.iacr.org/2008/040.
15. B. G. Kang, J. H. Park. On the relationship between squared pairings and plain pairings. Inf. Process. Lett. 97(6): 219-224, 2006.
16. A.J. Menezes and N. Koblitz. Pairing-based cryptography at high security levels. Cryptography and Coding, Lecture Notes in Computer Science 3796, 13-36, Springer-Verlag, 2005.
17. A.J. Menezes, T. Okamoto and S.A. Vanstone. Reducing elliptic curve logarithms to a finite field, *IEEE Trans. Inform. Theory,* vol. 39, pp. 1639-1646, 1993.
18. S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto. Optimised versions of the Ate and twisted Ate pairings. *The 11th IMA International Conference on Cryptography and Coding*, volume 4887 of *Lecture Notes in Computer Science*, pages 302-312. Springer-Verlag, 2007.
19. V.S. Miller. Short Programs for Functions on Curves. Unpublished manuscript, 1986.
20. V.S. Miller. The Weil pairing and its Efficient Calculation, J. Cryptology, 17 (2004), 235-261.
21. V.S. Miller. Private Communications. 2008.
22. K.G. Paterson. Cryptography from Pairing - Advances in Elliptic Curve Cryptography. Cambridge University Press, 2005.
23. M. Scott. Faster Pairings Using an Elliptic Curve with an Efficient Endomorphism. *Progress in Cryptology - INDOCRYPT 2005*, volume 3797 of *Lecture Notes in Computer Science*, pages. 258-269. Springer-Verlag, 2005.
24. M. Scott. Computing the Tate Pairing. *In CT-RSA05*, volume 3376 of *Lecture Notes in Computer Science*, pages. 293-304. Springer-Verlag, 2005.
25. M. Scott. Implementing cryptographic pairings. The 10th Workshop on Elliptic Curve Cryptography, 2006.
26. M. Scott and P.S.L.M. Barreto. Compressed Pairings. *In Advances in Cryptology-Crypto'2004*, volume 3152 of *Lecture Notes in Computer Science*, pages. 140-156. Springer-Verlag, 2004.
27. J.H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York, 1986.

28. K. Takashima. Scaling Security of Elliptic Curves with Fast Pairing Using Efficient Endomorphisms. *IEICE Trans. Fundamentals*, vol E90-A, no.1, pages. 152-159. Jan. 2007.
29. F. Vercauteren. Optimal Pairings. Preprint, 2008. Available at http://eprint.iacr.org/2008/096.
30. C.-A. Zhao, F. Zhang and J. Huang. A Note on the Ate Pairing. Preprint 2007, to appear in Internationl Journal of Information Security. Also available at http://eprint.iacr.org/2007/247.