Computing Bilinear Pairings on Elliptic Curves with Automorphisms

Chang-An Zhao[1], Dongqing Xie[1], Fangguo Zhang[2],
Jingwei Zhang[2] and Bing-Long Chen[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] Department of Mathematics, Sun Yat-Sen University, Guangzhou 510275, P.R.China.

changanzhao@gmail.com

dqxie@hnu.cn

isszhfg@mail.sysu.edu.cn

zhangjw3@mail2.sysu.edu.cn

mcscbl@mail.sysu.edu.cn

Abstract. In this paper, we present a novel method for constructing a super-optimal pairing with great efficiency, which we call the omega pairing. The computation of the omega pairing requires the simple final exponentiation and short loop length in Miller's algorithm which leads to a significant improvement over the previously known techniques on certain pairing-friendly curves. Experimental results show that the omega pairing is about 22% faster and 19% faster than the super-optimal pairing proposed by Scott at security level of AES 80 bits on certain pairing-friendly curves in affine coordinate systems and projective coordinate systems, respectively.

Keywords: Elliptic curves, Automorphism, Pairing based cryptography, Weil pairing

1 Introduction

Bilinear pairings play an important role in cryptographic protocols [22]. This leads to the development of efficient pairing computations since the implemen-

tation of pairing based cryptosystems involves pairing evaluation. In practice, many methods have been designed for optimizing Miller's algorithm [20]. Some extensive surveys of pairing computations can be found in [1, 9]. Recently, many results focus on shortening the loop length in Miller's algorithm, e.g., Duursma-Lee methods [8], the eta pairing [3], the ate pairing and its variants [14, 19, 30], as well as the R-ate pairing [17]. In [31], it is proved that all pairings are in a group from an abstract point of view which provides a new explanation for the R-ate pairing. Vercauteren gives an efficient method to construct the optimal Ate pairing [29]. Hess presents an integral framework that covers all known fast pairing functions [13].

Computing the classical Tate and Weil pairings requires $\log_2 r$ Miller iteration loops where r is the order of the points. If the number of the Miller iteration loops is less than $\log_2 r/\varphi(k)$ where k is the embedding degree of elliptic curves, the corresponding pairing is called super-optimal [29]. Motivated by GLV methods [11], Scott indeed constructs a super-optimal pairing on pairing-friendly curves with embedding degree $k = 2$ [24], which is the fastest pairing at security level of AES 80 bits till now. Using pairing-friendly curves with embedding degree $k = 2$ has competitive advantages, which is described clearly in [25]. Moreover, pairing compression techniques can be applied efficiently to reduce the bandwidth in this case [10]. Therefore, the focus of our presentation is primarily on pairing computations over pairing-friendly curves with embedding degree $k = 2$.

In this paper, we present a novel variant of the Weil pairing on ordinary elliptic curves with nontrivial automorphisms, which we call the omega pairing. The computation of the omega pairing requires the simple final exponentiation and short loop length in Miller's algorithm which leads to a significant improvement over the previous techniques. This new pairing is super-optimal and more efficient than the previously known pairings on certain pairing-friendly curves. Experimental results show that the omega pairing is about 22% faster and 19% faster than the super-optimal pairing proposed by Scott in affine coordinate systems and projective coordinate systems, respectively.

The rest of this paper is organized as follows. Section 2 introduces the basic pairings and a family of ordinary elliptic curves with nontrivial automorphisms. In Section 3, we propose the omega pairing whose structure is similar to that of the Weil pairing. Section 4 compares the new pairing with the previous fastest

pairing at security level of AES 80 bits on certain pairing-friendly curves and presents the experimental results.

2 Preliminaries

In this section, we briefly recall the definitions of the Tate and Weil pairings. Then we introduce a family of elliptic curves with nontrivial automorphisms.

2.1 Tate Pairing

Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements where p is a prime, and E an elliptic curve defined over $\mathbb{F}_q$. Consider a large prime r such that $r \mid \#E(\mathbb{F}_q)$, where $\#E(\mathbb{F}_q)$ denotes the order of $E(\mathbb{F}_q)$. Assume that r^2 does not divide $q^k - 1$ and k is greater than 1, where k is the embedding degree. We denote by $E[r]$ the r-torsion group of E.

Let D_P be a degree zero divisor (see [27]) which is linearly equivalent to $(P) - (\mathcal{O})$, where $P \in E[r]$ and $\mathcal{O}$ is the point at infinity. For every integer i, let $f_{i,P}$ be a rational function on E with divisor $(f_{i,P}) = i(P) - (iP) - (i-1)(\mathcal{O})$. In particular, $(f_{r,P}) = rD_P$. Assume that μ_r is the r-th roots of unity in $\mathbb{F}_{q^k}$. Then the reduced Tate pairing [4] is defined as follows

$$e : E[r] \times E(\mathbb{F}_{q^k}) \to \mu_r,$$
$$e(P, R) = f_{r,P}(R)^{\frac{q^k-1}{r}}.$$

Note that $f_{r,P}(R)^{a(q^k-1)/r} = f_{ar,P}(R)^{(q^k-1)/r}$ for any integer a. The rational function $f_{r,P}$ can be computed in polynomial time by using Miller's algorithm [20, 21].

2.2 Weil Pairing

Using the same notation as before, one can 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 degree zero divisors which are linearly equivalent to $(P) - (\mathcal{O})$ and $(Q) - (\mathcal{O})$, respectively.

Suppose that $f_{r,P}$ and $f_{r,Q}$ are two rational functions on E with $(f_{r,P}) = rD_P$ and $(f_{r,Q}) = rD_Q$. Then the Weil pairing is a map [21]

$$e_r : E[r] \times E[r] \to \mu_r,$$
$$e_r(P,Q) = (-1)^r \frac{f_{r,P}(Q)}{f_{r,Q}(P)}.$$

If the embedding degree k is even, one can define the powered Weil pairing [16, 18] as

$$\hat{e}_r(P,Q) = e_r(P,Q)^{q^{k/2}-1}.$$

Note that the denominator elimination technique can be used when computing the powered Weil pairing.

2.3 A Family of Elliptic Curves with Nontrivial Automorphisms

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

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

Elliptic curves of this form have efficiently computable endomorphisms which are applied in fast point multiplication [11] and the computation of the Tate pairing [24]. In fact, these endomorphisms are also automorphisms which are used in speeding up the discrete log computation [7]. Note that some pairing-friendly curves like E_1 with low embedding degrees have been constructed in [24, 28] and thus can be applied in pairing based cryptosystems. In the following, we will focus on pairing computations on the elliptic curve like E_1. It is clear that the results can be generalized naturally to the pairing-friendly elliptic curve like E_2.

Suppose that β is an element of order three in $\mathbb{F}_p$. An automorphism of E_1 is given by

$$\phi : E_1 \to E_1,$$
$$(x,y) \to (\beta x, y).$$

Since this automorphism ϕ is also an isogeny, its dual isogeny is given by

$$\hat{\phi} : E_1 \to E_1,$$
$$(x,y) \to (\beta^2 x, y).$$

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 an automorphism of E_1.

We cite useful facts from [11] for interests. Let $P \in E_1(\mathbb{F}_p)$ be a point of prime order r, where r^2 does not divide $\#E_1(\mathbb{F}_p)$. Then ϕ and $\hat{\phi}$ act restrictively on the subgroup $\langle P \rangle$ as multiplication maps $[\lambda]$ and $[\hat{\lambda}]$ respectively, i.e., $\phi(P) = \lambda P$ and $\hat{\phi}(P) = \hat{\lambda} P$, 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 $\mathbb{F}_p$.

Assume that the embedding degree of E_1 is $k = 2$. 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 $\langle Q' \rangle$ of order r. Two automorphisms ϕ' and $\hat{\phi}'$ of $E_1^{'}$ can be given by

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

Suppose 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 $\langle Q' \rangle$ as multiplication maps. In practice, it can be checked that $\lambda Q' = \hat{\phi}'(Q')$ and $\hat{\lambda} Q' = \phi'(Q')$ using straightforward calculations. However, an explanation will be given in the following Lemma 2 of Section 3.

There exists an isomorphism

$$\begin{aligned} &\psi : E_1^{'} \to E_1, \\ &(x, y) \to (Dx, yD^{\frac{3}{2}}) \end{aligned}$$

defined over $\mathbb{F}_{p^k}$. Write $Q = \psi(Q')$. Then Q is a point in $E_1(\mathbb{F}_{p^k})[r]$. In practical implementations, Q is specified in this way when the curve only has a quadratic twist. Since $\langle Q \rangle$ is isomorphic to $\langle Q' \rangle$, it leads to $\lambda Q = \hat{\phi}(Q)$ provided that $\lambda Q' = \hat{\phi}'(Q')$ holds. This observation is instrumental in constructing the new variants of the Weil pairing.

3 New Variants of The Weil Pairing

In this section, we will construct the new variants of the Weil pairing. For interests, we will focus on pairing-friendly curves with the embedding degree $k = 2$ which has competitive merits in the implementations. It is not difficult to see

that our results can be generalized to pairing-friendly curve like E_1 and E_2 with even embedding degree.

Let p be a prime such that $p \equiv 1 \pmod 3$, and E_1 an ordinary elliptic curve over $\mathbb{F}_p$ with equation: $E_1 : y^2 = x^3 + B$. Consider a large prime r such that $r \mid \#E_1(\mathbb{F}_p)$. Assume that E_1 has the embedding degree $k = 2$ with respect to r. 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 $\mathbb{F}_p$. Suppose that $r^2 \nmid \#E_1(\mathbb{F}_p)$ 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 given by $\psi : E_1^{'} \to E_1, (x, y) \to (Dx, D^{\frac{3}{2}}y)$. Write $Q = \psi(Q')$. Let β be an element of order three in $\mathbb{F}_p$. Two automorphisms ϕ and $\hat{\phi}$ of E_1 are given by $\phi : E_1 \to E_1$, $(x, y) \to (\beta x, y)$ and $\hat{\phi} : E_1 \to E_1$, $(x, y) \to (\beta^2 x, y)$, respectively. Assume that λ is a 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 the integer such that $ar = \lambda^2 + \lambda + 1$. Then we have the following results.

Theorem 1. *For the points P and Q in $E_1[r]$ given in the above, the function $\omega(P, Q) = (\frac{f_{\lambda,P}(Q)}{f_{\lambda,Q}(P)})^{p-1}$ defines a bilinear pairing.*

We will show that $\omega(P, Q)$ equals a fixed power of the Weil pairing. This new pairing is named as the omega pairing. The non-degeneracy of $\omega(P, Q)$ holds if $\hat{e}_r(P, Q)$ is non-degenerate and r does not divide a. The proof of Theorem 1 is based on the following useful lemmas.

Lemma 1. *There does not exist an integer m such that $\phi(S) = mS$ for all $S \in E_1[r]$.*

Proof. It is known that $E_1[r] \cong \mathbb{Z}_r \times \mathbb{Z}_r$ can be viewed as a two-dimensional vector space. We remark that $\phi : E_1[r] \to E_1[r]$ is a linear map, whose characteristic polynomial is $g(x) = x^2 + x + 1$ [23]. It suffices to show that the characteristic polynomial $g(x)$ has no multiple roots. If not, assume that m is an integer such that $\phi(S) = mS$ for every point $S \in E_1[r]$, then m is a multiple root of $x^2 + x + 1 = 0 \pmod r$. It follows from $\phi(P) \neq P$ that $m \neq 1$. Note that the derivative of the characteristic polynomial $g(x)$ is $2x + 1$. So m must satisfy the following equation

$$\begin{cases} x^2 + x + 1 = 0 \pmod r \\ 2x + 1 = 0 \pmod r \end{cases}$$

It is obvious that there does not exist such an integer m satisfying the above equation if $r = 2$. Thus we may assume that $r \neq 2$. Then we conclude that only

$r = 3$ and $m = 1$ satisfy the conditions. However, m can not be equal to 1. So we can not find an integer m such that $\phi(S) = mS$ for all $S \in E_1[r]$. This completes the proof of Lemma 1. □

Lemma 2. *Using the notation defined as above, we have* $\lambda Q = \hat{\phi}(Q)$.

Proof. The isomorphism

$$\begin{aligned} \psi : E_1^{'} &\to E_1, \\ (x, y) &\to (Dx, D^{\frac{3}{2}} y) \end{aligned}$$

maps $Q' \in E_1^{'}(\mathbb{F}_p)[r]$ into $E_1(F_{p^k})[r]$. It follows that $\langle Q \rangle$ is isomorphic to $\langle Q' \rangle$. Then we see that

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

Note that $\lambda Q'$ must equal $\hat{\phi}'(Q')$ or $\phi'(Q')$, where $\hat{\phi}'$ and ϕ' are denoted in the previous Section 2.3. In the following, we will show that $\lambda Q' = \hat{\phi}'(Q')$ which leads to $\lambda Q = \hat{\phi}(Q)$.

Write $Q' = (x_{Q'}, y_{Q'})$. Then $Q = \psi(Q') = (Dx_{Q'}, D^{\frac{3}{2}} y_{Q'})$. If $\lambda Q' = \phi'(Q')$, we deduce

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

Note that $E_1[r] = \{P \in E_1(\overline{\mathbb{F}_p}) | rP = \mathcal{O}\}$ can be viewed as a two-dimensional vector space. It is not 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 Lemma 1. Therefore, we have $\lambda Q' = \hat{\phi}'(Q')$. It follows that

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

This completes the proof of Lemma 2. □

Lemma 3. *For* $i \in \mathbb{Z}$, *the function* $F(P, Q) = \frac{f_{i,P}(iQ)}{f_{i,Q}(iP)}$ *satisfies*

$$(\frac{f_{i,P}(iQ)}{f_{i,Q}(iP)})^{p-1} = (\frac{f_{i,P}(Q)}{f_{i,Q}(P)})^{i(p-1)}.$$

Proof. To prove the assertion, it suffices to show that

$$(f_{i,P}(iQ) f_{i,P}(Q)^{-i})^{p-1} = (f_{i,Q}(iP) f_{i,Q}(P)^{-i})^{p-1}.$$

Let t be a $\mathbb{F}_p$-rational local parameter for $\mathcal{O}$. Assume that $(t) \cap P = \varnothing$. Thus the $\mathbb{F}_p$-rational divisor $(i-1)(\mathcal{O}) + (\frac{1}{t^{i-1}})$ satisfies $(i-1)(\mathcal{O}) + (\frac{1}{t^{i-1}}) \cap (f_{i,P}) = \varnothing$. Since $f_{i,P}$ is a $\mathbb{F}_p$-rational function, it follows that $f_{i,P}((i-1)(\mathcal{O})+(\frac{1}{t^{i-1}}))^{p-1} = 1$ by Fermat's Little Theorem (or Lemma 1 in [8]). Then

$$\begin{aligned}(f_{i,P}(iQ)f_{i,P}(Q)^{-i})^{p-1} =& (f_{i,P}(iQ)f_{i,P}(Q)^{-i}f_{i,P}((i-1)(\mathcal{O}) + (\frac{1}{t^{i-1}})))^{p-1} \\ =& f_{i,P}(-(i(Q) - (iQ) - (i-1)(\mathcal{O})) + (\frac{1}{t^{i-1}}))^{p-1} \\ =& f_{i,P}((\frac{1}{f_{i,Q}t^{i-1}}))^{p-1}.\end{aligned}$$

Note that $(f_{i,P}) \cap (\frac{1}{f_{i,Q}t^{i-1}}) = \varnothing$. Thanks to Weil reciprocity [9, 21], we have $f_{i,P}((\frac{1}{f_{i,Q}t^{i-1}})) = f_{i,Q}t^{i-1}((f_{i,P}))^{-1}$ and thus

$$\begin{aligned}(f_{i,P}(iQ)f_{i,P}(Q)^{-i})^{p-1} =& (f_{i,Q}t^{i-1}((f_{i,P}))^{-1})^{p-1} \\ =& (f_{i,Q}t^{i-1}(i(P) - (iP) - (i-1)(\mathcal{O}))^{-1})^{p-1}.\end{aligned}$$

By Theorem 1 in [4] and Theorem 2 in [8], we can discard the evaluation of the rational function at the infinity point. Thus

$$\begin{aligned}(f_{i,P}(iQ)f_{i,P}(Q)^{-i})^{p-1} =& (f_{i,Q}t^{i-1}((f_{i,P}))^{-1})^{p-1} \\ =& (f_{i,Q}t^{i-1}(i(P) - (iP))^{-1})^{p-1} \\ =& (f_{i,Q}t^{i-1}(iP)f_{i,Q}t^{i-1}(P)^{-i})^{p-1} \\ =& (f_{i,Q}(iP)f_{i,Q}(P)^{-i})^{p-1}.\end{aligned}$$

The last identity holds since $t^{i-1}(iP)^{p-1} = 1$ and $t^{i-1}(P)^{p-1} = 1$ using Fermat's Little Theorem. This completes the proof of Lemma 3. □

Corollary 1. *If $i = \lambda$ with λ defined as above, we have*

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

Note that Corollary 1 is instrumental in the construction of the omega pairing. In light of the above discussion, one arrives then at the following proof of Theorem 1.

Proof (of Theorem 1). According to the results in [29], we have

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

By using the same argument for $f_{ar,Q}(P)$, we obtain

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

It is not hard to see that $l_{\phi(Q),\hat{\phi}(Q)}(P) = -(l_{\phi(P),\hat{\phi}(P)}(Q))$. Altogether,

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

Since $\hat{\phi}(Q) = \lambda Q$ and $\phi(P) = \lambda P$, we obtain

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

By Corollary 1, we have

$$\hat{e_r}(P,Q)^a = (\frac{f_{\lambda,P}(Q)}{f_{\lambda,Q}(P)})^{(2\lambda+1)(p-1)}. \tag{1}$$

Following the argument of Theorem 2 in [13], we can ignore the exponent c from the final exponentiation. In fact, it is seen that

$$(\frac{f_{r^2,P}(Q)}{f_{r^2,Q}(P)})^{(p-1)} = e_r(P,Q)^{r(p-1)} = 1.$$

By the Chinese Remainder Theorem, we can find $\lambda' = \lambda + \tau r^2$ for some integer τ such that $\lambda' \equiv 0$ for all prime number $r' \neq r$ dividing p^2-1. Then $(2\lambda'+1, r) = 1$ and $(2\lambda'+1, r') = 1$. This implies that $(2\lambda'+1, p^2-1) = 1$. By replacing λ by λ' in Equation (1). we have

$$\hat{e_r}(P,Q)^a = (\frac{f_{\lambda',P}(Q)}{f_{\lambda',Q}(P)})^{(2\lambda'+1)(p-1)}. \tag{2}$$

Let $M \equiv (2\lambda'+1)^{-1} \pmod{p^2-1}$. Raising Equation 2 to the power M we get

$$\begin{aligned}\hat{e_r}(P,Q)^{aM} =& (\frac{f_{\lambda',P}(Q)}{f_{\lambda',Q}(P)})^{(2\lambda'+1)M(p-1)} \\ =& (\frac{f_{\lambda,P}(Q)}{f_{\lambda,Q}(P)})^{(p-1)} (\frac{f_{r^2,P}(Q)}{f_{r^2,Q}(P)})^{(p-1)} = \quad (\frac{f_{\lambda,P}(Q)}{f_{\lambda,Q}(P)})^{(p-1)}.\end{aligned}$$

This completes the proof of Theorem 1.

□

Using the similar analysis, the omega pairing can be generalized on the elliptic curve like E_2. Let p be a prime such that $p \equiv 1 \pmod 4$, and E_2 an ordinary elliptic curve over $\mathbb{F}_p$ with equation: $E_2 : y^2 = x^3 + Ax$. Consider a large prime r such that $r \mid \#E_2(\mathbb{F}_p)$. Assume that E_2 has the the embedding degree $k = 2$ with respect to r. The quadratic twist E_2' is given by the equation $E_2' : y^2 = x^3 + A/D^2 x$, where D is a quadratic non-residue in $\mathbb{F}_p$. Suppose that $r^2 \nmid \#E_2(\mathbb{F}_p)$ and $r^2 \nmid \#E_2'(\mathbb{F}_p)$. Let $P \in E_2(\mathbb{F}_p)[r]$ and $Q' \in E_2'(\mathbb{F}_p)[r]$. An isomorphism is given by $\psi : E_2' \to E_2, (x, y) \to (Dx, D^{\frac{3}{2}} y)$. Write $Q = \psi(Q')$. Assume that α be an element of order four in $\mathbb{F}_p$. Two automorphisms ϕ and $\hat{\phi}$ of E_2 are given by $\phi : E_2 \to E_2, (x, y) \to (-x, \alpha y)$ and $\hat{\phi} : E_2 \to E_2, (x, y) \to (-x, -\alpha y)$ respectively. Let λ be the root of the equation $x^2 + 1 = 0 \pmod r$ such that $\lambda P = \phi(P)$ and $\lambda Q = \hat{\phi}(Q)$. Then we have the following results.

Theorem 2. *For the points P and Q in $E_2[r]$ in the above, the function $\omega(P, Q) = (\frac{f_{\lambda,P}(Q)}{f_{\lambda,Q}(P)})^{p-1}$ defines a bilinear pairing.*

Proof. This follows immediately from the proof of Theorem 1. □

The number of the Miller iteration loops for computing the omega pairing is determined by the bit length of λ, which is possibly half that of r. Note that computing the omega pairing requires the simple final exponentiation. These lead to a significant improvement over the previous techniques. By Theorem 1 and 2, we establish a modified Miller's algorithm for computing the omega pairing in Algorithm 1.

We give some useful remarks which have been discussed in [12, 25] in the implementations. Write $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ with $i \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ and $i^2 \in \mathbb{F}_p$. Let $\nu = a + bi$ with $a,\ b \in \mathbb{F}_p$. Then the conjugate of ν can be given by $\overline{\nu} = \overline{a + bi} = a - bi$. Note that $\frac{1}{f_{\lambda,Q}(P)}$ can be replaced by its conjugate $\overline{f_{\lambda,Q}(P)}$ according to the observations in [26]. A second useful remark is that one can share the same Miller variable f when computing $\frac{f_{\lambda,P}(Q)}{f_{\lambda,Q}(P)}$. Finally, we can employ Montgomery's trick to compute scalar multiplications of P and Q' in affine coordinate systems.

4 Efficiency Comparison

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 computation cost of one multiplication

Algorithm 1 Computation of $\omega(P, Q)$

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: $\omega(P, Q)$

1. $T \leftarrow P$, $T' \leftarrow Q'$, $f \leftarrow 1$,
2. for $i = n-1, n-2, \cdots, 1, 0$ do
   2.1 $f \leftarrow f^2 \cdot l_{T,T}(Q) \cdot \overline{l_{\psi(T'),\psi(T')}(P)}$, $T \leftarrow 2T$, $T' \leftarrow 2T'$
   2.2 if $l_i = 1$ then
   2.3 $f \leftarrow f \cdot l_{T,P}(Q) \cdot \overline{l_{\psi(T'),\psi(Q')}(P)}$, $T \leftarrow T + P$, $T' \leftarrow T' + Q'$
3. return f^{p-1}

and one inverse in $\mathbb{F}_p$ can be denoted as M and I, respectively. We also count one square as one multiplication in $\mathbb{F}_p$. If $i^2 \in \mathbb{F}_p$ is very small, one square and one multiplication in $\mathbb{F}_{p^2}$ is equal to $2M$ and $3M$ respectively. We will implement pairing computations on the pairing-friendly curve with embedding degree $k = 2$ given by Scott in [24]. Note that we can choose the suitable λ which has low Hamming weight on this family of pairing-friendly curves [24, 28].

If affine coordinates are employed, one point doubling requires $1I + 4M$ and one point addition requires $1I + 3M$ in $E(\mathbb{F}_p)$ respectively [15]. 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 the two point doublings reduces to $1I + 11M$. Two line evaluations require $2M$. The remainder of Line 2.1 requires $1S_2 + 2M_2 = 2M + 6M = 8M$ for computing one square and two multiplications in $\mathbb{F}_{p^2}$. Thus Line 2.1 in one iteration loop needs $21M + 1I$. Since $\lambda = 2^{80} + 2^{16}$ in [24], the total contribution from Line 2.1 is $(21M + 1I) \cdot 80 = 1680M + 80I$. It is not difficult to show that the total contribution from Line 2.3 is $1I + 17M$. By now, we cost $(1680M + 17M) + 81I = 1697M + 81I$. The exponentiation $(p - 1)$ requires $5M + 1I$ since the Frobenius map can be used here. Thus the total cost for Algorithm 1 in affine coordinate systems is $1702M + 82I$.

If Jacobian projective coordinates are employed, one point doubling requires $8M$ and one point addition requires $11M$ in $E(\mathbb{F}_p)$ respectively [15]. Computing $l_{T,T}(Q)$ requires $4M$ provided that the operation $T \leftarrow 2T$ has been computed [6]. We can see that the cost of computing $2T'$ and $\overline{l_{\psi(T'),\psi(T')}(P)})$ is 12M in a similar way. Also, computing $f^2 \cdot l_{T,T}(Q) \cdot \overline{l_{\psi(T'),\psi(T')}(P)}$ requires $8M$. Thus the cost

of Line 2.1 is $24M + 8M = 32M$. In the whole iteration, we need $80 \cdot 32M = 2560M$ for the part of point doubling and line evaluation. the total cost of point addition and line evaluation requires $34M$. Thus the total cost for Algorithm 1 in projective coordinate systems is $2560M + 34M + 5M + 1I = 2599M + 1I$.

Using the similar analysis, the cost for Algorithm 4 in [24] can be also given in different coordinate systems. The cost of computing the omega pairing and the proposed pairing in [24] is summarized in Table 1. We implement the computation of the omega pairing and the previous fastest pairing using Magma online demo [5]. Experimental results indicate that the omega pairing is about 22% faster and 19% faster than the previous fastest pairing in affine coordinate systems and projective coordinate systems, respectively.

Table 1. Efficiency Comparison of the Computations of the Different Pairings

	Pairings	**Operation**	**1I = 30M**	**1I = 10M**	**Time**
Affine	Proposed pairing in [24]	$2162M + 82I$	$4622M$	$2982M$	7.2ms
	$\omega(P, Q)$	$1702M + 82I$	$4162M$	$2522M$	5.9ms
Projective	Proposed pairing in [24]	$2817M + 1I$	$2847M$	$2827M$	7.9ms
	$\omega(P, Q)$	$2599M + 1I$	$2629M$	$2609M$	6.6ms

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, vol. 11, no. 2, pp. 141-145. (1998)
3. P.S.L.M. Barreto, S. Galbraith, C. ÓhÉigeartaigh, and M. Scott. Efficient pairing computation on supersingular Abelian varieties, Designs, Codes and Cryptography, vol. 42, no. 3, pp. 239-271. Springer-Netherlands (2007)
4. P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing-based cryptosystems, in Proc. Advances in Cryptology-Crypto 2002, Lecture Notes in Computer Science, vol. 2442, pp. 354-368, Springer-Verlag (2002)

5. W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language," J. Symbolic Comput., vol. 24 no. 3,pp. 235-265, http://magma.maths.usyd.edu.au/ (1997)
6. S. Chatterjee, P. Sarkar, and R. Barua, Efficient Computation of Tate Pairingin Projective Coordinate over General Characteristic Fields, minus in ICISC 2004, Lecture Notes in Computer Science, vol. 3506, pp. 168C181, Springer-Verlag (2005)
7. I. Duursma, P. Gaudry, and F. Morain. Speeding up the discrete log computation on curves with automorphisms, in Proc. Advances in Cryptology-AsiaCrypt 99, Lecture Notes in Computer Science, vol. 1716, pp. 203-121, Springer-Verlag (1999)
8. I. Duursma, H.-S. Lee. Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$, in Advances in Cryptology-AsiaCrypt'2003, Lecture Notes in Computer Science, vol. 2894, pp. 111-123, Springer-Verlag (2003)
9. 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)
10. S. Galbraith and X. Lin. Computing pairings using x-coordinates only, Designs, Codes and Cryptography. vol. 50, no. 3, pp. 305-324. Springer-Netherlands (2009)
11. R.P. Gallant, R.J. Lambert and S.A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms, in Proc. Advances in Cryptology-Crypto 2001, Lecture Notes in Computer Science, vol. 2139, pp. 190-200, Springer-Verlag (2001)
12. R. Granger and N.P. Smart. On computing products of pairings. Technical Report CSTR-06-013, University of Bristol (2006)
13. F. Hess. Pairing lattices. in Pairing 2008, Lecture Notes in Computer Science, vol. 5209, pp. 18-38, Springer-Verlag (2008)
14. F. Hess, N.P. Smart and F. Vercauteren. The Eta pairing revisited, IEEE Trans. Inform. Theory, vol. 52, no. 10, pp. 4595-4602 (2006)
15. IEEE Std 1363-2000. Standard Specifications for Public-key Cryptography. IEEE P1363 Working Group (2000)
16. B. G. Kang and J. H. Park. On the relationship between squared pairings and plain pairings, Inf. Process. Lett. vol. 97, no. 6, pp. 219-224 (2006)
17. E. Lee, H.-S. Lee, and C.-M. Park. Efficient and generalized pairing computation on Abelian varieties, IEEE Trans. Inform. Theory, vol. 55, no.4, pp. 1793-1803 (2009)
18. A.J. Menezes and N. Koblitz. Pairing-based cryptography at high security levels, in Cryptography and Coding, Lecture Notes in Computer Science, vol. 3796, pp. 13-36, Springer-Verlag (2005)
19. S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto. Optimised versions of the Ate and twisted Ate pairings, in Cryptography and Coding, Lecture Notes in Computer Science, vol. 4887, pp. 302-312, Springer-Verlag (2007)

20. V.S. Miller. Short programs for functions on curves, [online]. Available from http://crypto.stanford.edu/miller/miller.pdf
21. V.S. Miller. The Weil pairing and its efficient calculation, J. Cryptology, vol. 17, no. 44, pp. 235-261 (2004)
22. K.G. Paterson. Cryptography from Pairing, Ch. X of I.F.Blake, G.Seroussi, and N.P.Smart, eds., Advances in Elliptic Curve Cryptography. Cambridge University Press (2005)
23. P. R. Schoof. Counting points on elliptic curves over finite fields. Journal de Théorie des Nombres de Bordeaux 7, pp. 219-254 (1995)
24. M. Scott. Faster pairings using an elliptic curve with an efficient endomorphism, in Progress in Cryptology - IndoCrypt 2005, Lecture Notes in Computer Science, vol. 3797, pp. 258-269, Springer-Verlag (2005)
25. M. Scott. Computing the Tate pairing, in CT-RSA'05, Lecture Notes in Computer Science, vol. 3376, pp. 293-304, Springer-Verlag. (2005)
26. M. Scott. Implementing cryptographic pairings, in Pairing 2007, Lecture Notes in Computer Science, vol. 4575, pp. 177-196, Springer-Verlag (2007)
27. J.H. Silverman. The Arithmetic of Elliptic Curves. New York, Springer-Verlag (1986)
28. K. Takashima. Scaling security of elliptic curves with fast pairing using efficient endomorphisms, IEICE Trans. Fundamentals, vol E90-A, no. 1, pp. 152-159, 2007.
29. F. Vercauteren. Optimal pairings,IEEE Trans. Inform. Theory, vol. 56, no.1, pp. 455-461 (2009)
30. C.-A. Zhao, F. Zhang and J. Huang. A note on the Ate pairing, Int. J. Inf. Security, vol. 7, no. 6, pp. 379-382, (2008)
31. C.-A. Zhao, F. Zhang and J. Huang. All pairings are in a group, IEICE Trans. Fundamentals, vol E91-A, no.10, pp. 3084-3087 (2008)