Chinese Journal of Electronics
Vol.27, No.4, July 2018

Efficient Pairing Computation on Twisted Weierstrass Curves*

WANG Bei[1], OUYANG Yi[1] and HU Honggang[2]

(1. *School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, China*)

(2. *School of Information Science and Technology, University of Science and Technology of China, Hefei 230027, China*)

Abstract — In this paper, we construct the twists of twisted Edwards curves in Weierstrass form. Then we define a new twisted Ate pairing on twisted Weierstrass curves named the Tx-Ate pairing. Following Miller's algorithm, we give a computation of the Tx-Ate pairing on high degree twisted Weierstrass curves, where the point operations are over Edwards form, and the computation of Miller function is over Weierstrass form. Although, in one doubling loop, our method to compute the Tx-Ate pairing is a litter slower than the previously fastest method. By twists, the Tx-Ate pairing can be calculated on more twisted Weierstrass curves with short loop length. The Tx-Ate pairing is even competitive with optimal Ate pairing when they have the same short loop length.

Key words — Weierstrass curves, Twisted Ate pairing, Twisted Edwards curves, Miller function.

I. Introduction

Pairings on Elliptic curves have many applications in cryptographic protocols. They have been used to give one-round three-party key exchange[1], identity-based encryption[2], pairing-based cryptography[3], short signature[4] and many other schemes. Research on implementing efficient pairings has focussed on reducing the loop length[5−7], and on using high degree twists[8,9].

Edwards elliptic curve is a quartic form introduced by Edwards[10] in 2007, then it was generalized to twisted Edwards curves by Bernstein *et al.*[11]. The point addition formula of twisted Edwards curves is unified. In comparison to Weierstrass curves, twisted Edwards curves possess a faster addition law. However, pairing computation over Edwards curves is more complicated than that over Weierstrass ones. The important problem is to compute the Miller function. For Weierstrass curves, the function is easy to obtain due to the chord-and-tangent rule for addition. However, the Edwards equation is of degree 4, *i.e.*, any line has 4 intersections with the curves instead of 3 as in the case of Weierstrass curves. So far, Arène *et al.*[12] and Le *et al.*[13] gave a geometric method to calculate it over twisted Edwards curves, but the formulas of the function are quite complicated. Arène *et al.*[12] also gave an open problem whether optimal ate pairings can be computed and whether the high degree twists can be used as well for suitable pairing-friendly curves in Edwards form. Since the twisted Edwards curve and its twists can not both be in Edwards forms for twists of degree larger than 2, if we want to compute the optimal Ate pairing on Edwards forms using the high degree twists, points addition and Miller functions should be computed separately.

The best known algorithm for computing pairings is Miller's algorithm[14]. Each loop of this algorithm contains two steps, updating points and updating Miller functions. We want to combine the faster addition law of Edwards form and the Miller function of Weierstrass form to compute the two steps. Based on this idea, we construct isomorphisms between twisted Edwards curves and twisted Weierstrass curves. Furthermore, on twisted Weierstrass curves, we construct a new twisted Ate pairing called the Tx-Ate pairing. By the isomorphisms and Miller's algorithm, we give an efficient computation of the new pairing, in which the point operations are over twisted Edwards curves and the computation of the Miller function is over twisted Weierstrass curves. The Tx-Ate pairing provides an implementation of the twisted Ate pairing on high-degree twisted Weierstrass curves. We also give a comparison about various pairings. In one doubling loop, the operation costs by our formulas are a little higher than that by all previous fastest formulas for pairings. But, the Tx-Ate pairing can be calculated on more twisted Weierstrass curves with short loop length. We can get that the

*Manuscript Received May 12, 2016; Accepted Sept. 21, 2017. This work is supported by the National Key Basic Research Program of China (No.2013CB834202) and the National Natural Science Foundation of China (No.11571328, No.61522210).

 DOI:10.1049/cje.2018.05.004

Tx-Ate pairing is even competitive with optimal Ate pairing.

This paper is organized as follows. In Section II, we give some notations and background. Section III contains the main work of this paper, which is constructing the twists of twisted Edwards curves and constructing the Tx-Ate pairing. In Section IV, we compute the Tx-Ate pairing on twisted Weierstrass curves with high degree twists. Finally, Section V gives an explicit comparison about various pairings.

II. Preliminaries

1. Forms and twists of elliptic curves

In this paper, let $p > 3$ be a prime number, $q = p^n$, and $\mathbb{F}_q$ be the finite field of order q. Let $W_{b,c}$ be a Weierstrass curve over $\mathbb{F}_q$ defined as

$$W_{b,c} : v^2 = u^3 + bu + c \tag{1}$$

A twisted Edwards curve is a quartic curve over $\mathbb{F}_q$ defined by

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2, \quad a, d \in \mathbb{F}_q^* \tag{2}$$

The addition law of twisted Edwards curves is given by the following formula

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right) \tag{3}$$

The unit is $(0, 1)$, the point $(0, -1)$ has order 2, and the inverse of a point (x, y) on $E_{a,d}$ is $(-x, y)$. As a special case, the doubling formula is

$$2(x, y) = \left(\frac{2xy}{y^2 + ax^2}, \frac{y^2 - ax^2}{2 - y^2 - ax^2} \right) \tag{4}$$

The elliptic curve $E'/\mathbb{F}_q$ is called a twist of degree g of $E/\mathbb{F}_q$ if there exists an isomorphism $\psi : E' \to E$ over $\mathbb{F}_{q^g}$ such that g is minimal with this property. Then the condition $g \mid \#\mathrm{Aut}(E)$ holds if and only if E admits a twist of degree g. Pairing-friendly curves with twists of degree higher than 2 arise from elliptic curves with j-invariants $j(E) = 0$ or 1728, see Ref.[15].

For the Weierstrass form, a twist of $W_{b,c}$ is given by

$$W_{b,c,\omega} : v^2 = u^3 + b\omega^4u + c\omega^6, \omega \in \mathbb{F}_{q^k} \tag{5}$$

The isomorphism between $W_{b,c}$ and $W_{b,c,\omega}$ is

$$\psi : W_{b,c} \to W_{b,c,\omega}, (u, v) \mapsto (\omega^2u, \omega^3v) \tag{6}$$

For the Edwards form, the twisted Edwards curve has j-invariant $j(E_{a,d}) = 16(a^2 + 14ad + d^2)^3/ad(a - d)^4$, see Ref.[16]. For twists of degree larger than 2, the twisted Edwards curve and its twists can not both be in Edwards forms, so the high degree twists of the twisted Edwards curves should be in different forms.

2. Background on pairings

Let E be a nonsingular elliptic curve over $\mathbb{F}_q$. Let r be a prime number and $r \mid \sharp E(\mathbb{F}_q)$. Let k be the embedding degree with respect to r, *i.e.*, k is the minimal integer such that $r \mid (q^k - 1)$. For the r-tortion subgroup, we have $E[r] \subseteq E(\mathbb{F}_{q^k})$. Let $P \in E[r]$ and let $f_{r,P} \in \mathbb{F}_q(E)$ be such that $div(f_{r,P}) = r(P) - r(\mathcal{O})$. Let $\mu_r \subseteq \mathbb{F}_{q^k}^*$ be the group of r-th roots of unity. The reduced Tate pairing is given by

$$\begin{gathered} \tau_r : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mu_r, \\ (P, Q) \mapsto f_{r,P}(Q)^{\frac{q^k-1}{r}} \end{gathered} \tag{7}$$

Let ϕ_q be the q-th power Frobenius endomorphism on E and t be the trace of ϕ_q. The groups G_1 and G_2 are the eigenspaces of ϕ_q on $E[r]$, defined as follows

$$G_1 = E[r] \cap ker(\phi_q - [1]) = E(\mathbb{F}_q)[r] \tag{8}$$

$$G_2 = E[r] \cap ker(\phi_q - [q]) \subseteq E(\mathbb{F}_{q^k})[r] \tag{9}$$

Let $T = t - 1$, then we have the reduced Ate pairing

$$\alpha : G_2 \times G_1 \to \mu_r, \ (Q, P) \mapsto f_{T,Q}(P)^{\frac{q^k-1}{r}} \tag{10}$$

The Ate pairing was first introduced by Hess *et al.*[17] in 2006. They simplified and extended the Eta pairing[18] to the case of ordinary curves. Assume that E has a twist of degree g with $g \mid k$. Let $e = k/g$, and $T_e \equiv T^e \bmod r$. The reduced twisted Ate pairing is defined as

$$\alpha^{\text{twist}} : G_1 \times G_2 \to \mu_r, \ (P, Q) \mapsto f_{T_e,P}(Q)^{\frac{q^k-1}{r}} \tag{11}$$

There are a series of variations of the Ate pairing, such as R-Ate pairing[19], optimal Ate pairing[6] and so on.

3. Miller's algorithm

The pairings over elliptic curves can be computed using the algorithm proposed by Miller[14]. For example, if we calculate the Ate pairing, one needs to compute the function $f_{T,Q}$, which is a double-and-add approach based on the following observation

$$f_{m+n,Q} = f_{m,Q}f_{n,Q}\frac{l_{[m]Q,[n]Q}}{\upsilon_{[m+n]Q}} \tag{12}$$

Let $g_{[m]Q,[n]Q} = \dfrac{l_{[m]Q,[n]Q}}{\upsilon_{[m+n]Q}}$ be the Miller function, where $l_{[m]Q,[n]Q}$ is the equation of the line through $[m]Q$ and $[n]Q$ and $\upsilon_{[m+n]Q}$ is the equation of the vertical line through $[m + n]Q$.

Let $\varphi : E' \to E, Q' \mapsto Q$ be an isomorphism, where E' is a g-th twist of E. When implementing the Ate pairing, instead of inputing the point Q on the curve $G_2 \subseteq E(\mathbb{F}_{q^k})[r]$, one can take $Q' \in G_2' \subseteq E'(\mathbb{F}_{q^e})[r]$ $(e = k/g)$. Points on the twisted curve are defined over a smaller field, so the point operations are much faster. The computation of $\alpha(\varphi(Q'), P)$ (shown in Algorithm 1) consists of two parts: evaluation of the function $f_{T,Q}$ at P and final exponentiation.

Algorithm 1 Miller's algorithm for the Ate pairing

Input: $T \in N$, $Q' \in G_2'$ not a multiple of $P \in G_1$

Output: $\alpha(Q,P) = f_{T,\varphi(Q')}(P)^{\frac{q^k-1}{r}}$

$T = \sum_{j=0}^{l} t_j 2^j$, with $t_j \in \{0,1\}$ and $t_l = 1$.

$R' \leftarrow Q'$, $f \leftarrow 1$

for $j = l-1$ down to 0 do

$f \leftarrow f^2 g_{\varphi(R'),\varphi(R')}(P)$, $R' \leftarrow [2]R'$

if $t_j = 1$ then

$f \leftarrow f g_{\varphi(R'),\varphi(Q')}(P)$, $R' \leftarrow R' + Q'$

end if

end for

$f \leftarrow f^{(q^k-1)/r}$

Return f

III. Computing the Twists and Constructing a New Pairing

In the following, let

$$b = \frac{3-A^2}{3B^2},\ c = \frac{2A^3-9A}{27B^3} \tag{13}$$

with $A = \frac{2(a+d)}{a-d}$, $B = \frac{4}{a-d}$. Suppose that the pairing-friendly Weierstrass curve $W_{b,c}$ has a g-th twisted curve $W_{b,c,\omega}$, we consider the isomorphisms between $W_{b,c,\omega}$ and $E_{a,d}$. In the following, $e = k/g$ with $g = 2, 3, 4, 6$.

1. Twists on twisted Edwards curves

Lemma 1 Assume that $g \mid k$, ω is a generator of $\mathbb{F}_{q^k}$ over $\mathbb{F}_{q^e}$ and $\omega^g \in \mathbb{F}_{q^e}$, and the twisted Edwards curve $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ is defined over $\mathbb{F}_q$. Then the Weierstrass curve $W_{b,c,\omega} : v^2 = u^3 + b\omega^4 u + c\omega^6$ over $\mathbb{F}_{q^e}$ is a twist of degree g of $E_{a,d}$. The isomorphism can be given as

$$\begin{aligned} \Psi\colon E_{a,d} &\longrightarrow W_{b,c,\omega}, \\ (x,y) &\mapsto \left(\frac{(1+y)\omega^2}{B(1-y)} + \frac{A\omega^2}{3B}, \frac{\omega^3(1+y)}{Bx(1-y)}\right) \end{aligned} \tag{14}$$

The inverse transformation is

$$\begin{aligned} \Phi\colon W_{b,c,\omega} &\longrightarrow E_{a,d}, \\ (u,v) &\mapsto \left(\frac{3B\omega u - A\omega^3}{3Bv}, \frac{3Bu - A\omega^2 - 3\omega^2}{3Bu - A\omega^2 + 3\omega^2}\right) \end{aligned} \tag{15}$$

Proof Firstly, it is easy to know that Ψ is well defined, *i.e.* $\Psi(x,y) \in W_{b,c,\omega}$.

Now, we need to prove that Ψ is an isomorphism. It suffices to prove that the map is one to one at the singularity (exceptional points for the birational equivalence). The map Ψ from $E_{a,d}$ to $W_{b,c,\omega}$ is undefined at the points $x = 0$ or $y = 1$ of $E_{a,d}$. The inverse map Φ is undefined at the point $v = 0$ and $u = \frac{A\omega^2 - 3\omega^2}{3B}$.

1) If $x = 0$, the point $(0,-1)$ on $E_{a,d}$ of order 2 corresponds to the affine point of order 2 on $W_{b,c,\omega}$, namely $(\frac{A\omega^2}{3B}, 0)$; the point $(0,1)$ is the unit on $E_{a,d}$, and it maps to the point at infinity of $W_{b,c,\omega}$.

2) If $v = 0$ and $(A-2)(A+2)$ is a square (*i.e.* ad is a square), then there are two more points $(\frac{-A\omega^2 \pm 3\omega^2\sqrt{(A-2)(A+2)}}{6B}, 0)$ on $W_{b,c,\omega}$. These two points of order 2 correspond to the two points of order 2 at infinity on the desingularization of $E_{a,d}$.

3) If $u = \frac{A\omega^2 - 3\omega^2}{3B}$, then $v^2 = \frac{(A-2)\omega^6}{B^3}$. If $\frac{A-2}{B}$ is a square (*i.e.* d is a square), then there are two points $(\frac{A-3}{3B}, \frac{\pm\omega^3}{B}\sqrt{\frac{A-2}{B}})$ of order 4 on $W_{b,c,\omega}$. These two points correspond to the two points of order 4 at infinity on the desingularization of $E_{a,d}$.

In conclusion, if a is a square and d is not a square in $\mathbb{F}_q$, Ψ is an isomorphism. We choose a, d and ω to satisfy the conditions, then the field of definition of Ψ is $\mathbb{F}_{q^k}$ which is of degree g over $\mathbb{F}_{q^e}$. Hence, the twist degree is g.

2. The Tx-Ate pairing on the twisted Weierstrass curve

We now define a new twisted Ate pairing on the twisted Weierstrass curves, which we call the Tx-Ate pairing. We take the twisted points P' and Q' as inputs instead of P and Q. The pairing is defined as follows:

$$\alpha^{\mathrm{Tx}} : G_1' \times G_2' \to \mu_r,\ (P', Q') \mapsto f_{T_e,P'}(Q')^{\frac{q^k-1}{r}} \tag{16}$$

Here, P' is a point of $G_1' = \psi(G_1) \subseteq W_{b,c,\omega}(\mathbb{F}_{q^k})[r]$ and Q' is a point of $G_2' = \psi(G_2) = W_{b,c,\omega}(\mathbb{F}_{q^e})[r]$, where ψ is defined as Eq.(6). We call our new pairing the Tx-Ate pairing for two reasons. Firstly it is like the twisted Ate pairing (hence the Capital "T"); the main feature of the Tx-Ate pairing is the isomorphism map ψ, in other words, $P \in W_{b,c}(\mathbb{F}_q)[r]$ is extended to $P' \in W_{b,c,\omega}(\mathbb{F}_{q^k})[r]$ and $Q \in W_{b,c}(\mathbb{F}_{q^k})[r]$ is compressed to $Q' \in W_{b,c,\omega}(\mathbb{F}_{q^e})[r]$ (hence like the cross-twist, using the small "x").

Theorem 1 The Tx-Ate pairing $\alpha^{Tx}(P', Q')$ is bilinear and non-degenerate.

Proof Let $R', P' \in W_{b,c,\omega}(\mathbb{F}_{q^k})[r]$ such that $R = \psi^{-1}(R')$ and $P = \psi^{-1}(P')$. The slope $\lambda_{R',R'}$ and $\lambda_{R',P'}$ are

$$\lambda_{R',R'} = \frac{3u_{R'}^2 + b\omega^4}{2v_{R'}} = \omega\frac{3u_R^2 + b}{2v_R} = \omega\lambda_{R,R} \tag{17}$$

$$\lambda_{R',P'} = \frac{v_{R'} - v_{P'}}{u_{R'} - u_{P'}} = \omega\frac{v_R - v_P}{u_R - u_P} = \omega\lambda_{R,P} \tag{18}$$

Thus, regardless of whether or not $R' = P'$, we have $\lambda_{R',P'} = \omega\lambda_{R,P}$. By $(u_{Q'}, v_{Q'}) = (u_Q\omega^2, v_Q\omega^3)$ and $(u_{R'}, v_{R'}) = (u_R\omega^2, v_R\omega^3)$, we get

$$\begin{aligned} l_{R',P'}(Q') &= (u_{Q'} - u_{R'})\lambda_{R',P'} - (v_{Q'} - v_{R'}) \\ &= l_{R,P}(Q)\omega^3 \end{aligned}$$

and

$$\nu_{R'+P',\mathcal{O}}(Q') = u_{Q'} - u_{R'+P'} = \nu_{R+P,\mathcal{O}}(Q)\omega^2$$

We have the Miller function

$$g_{ADD(R',P')}(Q') = \frac{l_{R',P'}(Q')}{\nu_{R'+P',\mathcal{O}}(Q')} = g_{ADD(R,P)}(Q)\omega$$

and also $g_{DOU(R',R')}(Q') = g_{DOU(R,R)}(Q)\omega$.

For twists of degree $g = 2, 4$, $\omega^2 = \omega^{\gcd(g,6)}$ is in a subfield of $\mathbb{F}_{q^k}$ and thus vanishes in the final exponentiation. Similarly, for $g = 3, 6$, ω^3 and ω^6 are both in subfields of $\mathbb{F}_{q^k}$ and vanish in the final exponentiation, too. So, $\alpha^{\mathrm{Tx}}(P', Q')^{\gcd(g,6)} = \alpha^{\mathrm{twist}}(P, Q)^{\gcd(g,6)}$. Let $\xi = \dfrac{\alpha^{\mathrm{Tx}}(P', Q')}{\alpha^{\mathrm{twist}}(P, Q)}$ and $m = \gcd(g, 6)$, then $\xi^m = 1$. Since $\xi \in \mu_r$ and $\gcd(m, r) = 1$ (r is a prime number), we get $\xi = 1$, *i.e.* $\alpha^{\mathrm{Tx}}(P', Q') = \alpha^{\mathrm{twist}}(P, Q)$. If $\alpha^{\mathrm{twist}}(P, Q)$ is bilinear and non-degenerate, so is $\alpha^{\mathrm{Tx}}(P', Q')$.

Lemma 2 $\Phi(G_1') \subseteq E_{a,d}(\mathbb{F}_q)[r]$.

Proof Let $P = (u, v) \in G_1 = W_{b,c}(\mathbb{F}_q)[r]$, then $P' = \psi(P) = (\omega^2 u, \omega^3 v) \in G_1'$. By the map Φ defined in Eq.(15),

$$\begin{aligned}\Phi(P') &= \left(\frac{3B\omega^3 u - A\omega^3}{3Bv\omega^3}, \frac{3Bu\omega^2 - A\omega^2 - 3\omega^2}{3Bu\omega^2 - A\omega^2 + 3\omega^2}\right)\\ &= \left(\frac{3Bu - A}{3Bv}, \frac{3Bu - A - 3}{3Bu - A + 3}\right)\end{aligned}$$

By $u, v, A, B \in \mathbb{F}_q$, we get $\Phi(P') \in E_{a,d}(\mathbb{F}_q)[r]$.

IV. Computing the Tx-Ate Pairing on Twisted Weierstrass Curves

Similar to the computation of the Ate pairing by Algorithm 1, we have $\alpha^{\mathrm{Tx}}(P', Q') = \alpha^{\mathrm{Tx}}(\Psi(P''), Q')$, where Ψ is given in Lemma 1 and $P'' \in \Phi(G_1') \subseteq E_{a,d}(\mathbb{F}_q)[r]$ by Lemma 2. In this section, we compute the Tx-Ate pairing on Twisted Curves by Algorithm 2.

Algorithm 2 Miller's algorithm for Tx-Ate pairing

Input: $T_e \in N$, P'' and Q'

Output: $\alpha^{\mathrm{Tx}}(P', Q') = f_{T_e,\Psi(P'')}(Q')^{\frac{q^k-1}{r}}$

$T_e = \sum_{j=0}^{l} s_j 2^j$, with $s_j \in \{0, 1\}$ and $s_l = 1$.
$R' \leftarrow P''$, $f \leftarrow 1$
for $j = l - 1$ down to 0 do
$f \leftarrow f^2 g_{\Psi(R'),\Psi(R')}(Q')$, $R' \leftarrow [2]R'$
  if $s_j = 1$ then
  $f \leftarrow f g_{\Psi(R'),\Psi(P'')}(Q')$, $R' \leftarrow R' + P''$
  end if
end for
$f \leftarrow f^{(q^k-1)/r}$
Return f

In the following, we use m and s to denote the cost of each multiplication and squaring in the field $\mathbb{F}_q$, m_c to denote the cost of multiplication by constant in the field $\mathbb{F}_q$. Let k be even and we just calculate the Tx-Ate pairing on twisted Weierstrass curves with high degree $g = 4, 6$. We will give explicit formulas for curves operations in projective coordinates.

1. The Tx-Ate pairing on $v^2 = u^3 + b\omega^4 u$

In this case, j-invariant is 1728 and $a = -d$, the curve $v^2 = u^3 + b\omega^4 u$ is a quartic twisted curve of $E_{a,-a}$. We can get $b = \dfrac{a^2}{4}$ by Eq.(13) and $\Psi : (x, y) \mapsto (u, v) = \left(\dfrac{a\omega^2(1+y)}{2(1-y)}, \dfrac{a\omega^3(1+y)}{2x(1-y)}\right)$, where $\omega^2 \in \mathbb{F}_{q^{k/2}}$ and $\omega^4 \in \mathbb{F}_{q^{k/4}}$.

Doubling loop Let $R' = (X_2 : Y_2 : Z_2)$ satisfy the homogeneous twisted Edwards curve equation. Let $R = \Psi(R') = \left(\dfrac{a\omega^2(Z_2+Y_2)}{2(Z_2-Y_2)}, \dfrac{a\omega^3 Z_2(Z_2+Y_2)}{2X_2(Z_2-Y_2)}\right) = (u_2, v_2)$. By the Eq.(4), $(X_3 : Y_3 : Z_3) = [2](X_2 : Y_2 : Z_2)$ has the formulas:

$$\begin{aligned}X_3 &= 2X_2Y_2(2Z_2^2 - aX_2^2 - Y_2^2)\\ Y_3 &= (Y_2^2 - aX_2^2)(Y_2^2 + aX_2^2)\\ Z_3 &= (Y_2^2 - aX_2^2)(2Z_2^2 - aX_2^2 - Y_2^2)\end{aligned}$$

Let $Q' = (u_{Q'}, v_{Q'}) \in W_{b,0,\omega}(\mathbb{F}_{q^{k/4}})[r]$, then we give the formulas for the computation of $g_{R,R}(Q')$

$$\begin{aligned}g_{R,R}(Q') &= \frac{v_{Q'} - v_2 - \dfrac{3u_2^2 + b\omega^4}{2v_2}(u_{Q'} - u_2)}{u_{Q'} - u_3} (b = \frac{a^2}{4})\\ &= \frac{a(\Delta_1 \cdot v_{Q'} - \omega \cdot \Delta_2 \cdot u_{Q'} - \omega^3 \cdot \Delta_3)}{8X_2^2(Z_2 - Y_2)^3 v_2'(u_{Q'} - u_3)}\\ &\in (\Delta_1 \cdot v_{Q'} - \omega \cdot \Delta_2 \cdot u_{Q'} - \omega^3 \cdot \Delta_3)\mathbb{F}_{q^{k/2}}^*\end{aligned}$$

where $v_2' = v_2/\omega^3$ and

$$\begin{aligned}\Delta_1 &= 4X_2Z_2(Z_2 - Y_2)^2(Z_2 + Y_2)\\ \Delta_2 &= 2aX_2^2(Z_2 - Y_2)[(Z_2 + Y_2)^2 + Z_2^2 + Y_2^2]\\ \Delta_3 &= a(Z_2 + Y_2)\\ &\quad \cdot\{2Z_2^2(Z_2^2 - Y_2^2) - aX_2^2[(Z_2 + Y_2)^2 + Z_2^2 + Y_2^2]\}\end{aligned}$$

Using the denominator elimination techniques, we just need to calculate the reduced function $g'_{R,R}(Q') = \Delta_1 \cdot v_{Q'} - \omega \cdot \Delta_2 \cdot u_{Q'} - \omega^3 \cdot \Delta_3$. While $\Delta_1, \Delta_2, \Delta_3 \in \mathbb{F}_q$ and $u_{Q'}, v_{Q'} \in \mathbb{F}_{q^{k/4}}$ is given, the evaluation at Q' can be computed in $\dfrac{k}{2}m$ (with $\dfrac{k}{4}m$ each for multiplications by $u_{Q'}$ and $v_{Q'}$).

Now, we compute X_3, Y_3, Z_3 and $\Delta_i, i = 1, 2, 3$ using the following sequence of operations:

$$\begin{gathered}C = X_2 + Y_2, \quad D = X_2 + Z_2, \quad E = Z_2 + Y_2\\ F = X_2^2, \quad G = Y_2^2, \quad H = Z_2^2, \quad I = a \cdot F, \quad J = G - I\\ K = G + I, \quad L = 2H - K, \quad M = C^2, \quad N = D^2\\ O = E^2, \quad P = I \cdot (O + G + H), \quad Q = Z_2 - Y_2\\ X_3 = (M - F - G) \cdot L, \quad Y_3 = J \cdot K, \quad Z_3 = J \cdot L\end{gathered}$$

$$\Delta_1 = 2(N - F - H) \cdot (H - G) \cdot Q$$
$$\Delta_2 = 2Q \cdot P, \quad \Delta_3 = a \cdot E \cdot [2H \cdot (H - G) - P]$$

The total operation count for the above sequence of operations is $\frac{k}{2}m + 9m + 6s + 2m_c$.

Addition loop Let $P'' = (X_1 : Y_1 : Z_1)$ and $R' = (X_2 : Y_2 : Z_2)$, the addition $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$ has the formulas:

$$X_3 = Z_1Z_2(X_1Y_2 - X_2Y_1)[(Z_1Z_2)^2 + aX_1X_2Y_1Y_2]$$
$$Y_3 = Z_1Z_2(Y_1Y_2 - aX_1X_2)[(Z_1Z_2)^2 - aX_1X_2Y_1Y_2]$$
$$Z_3 = [(Z_1Z_2)^2 + aX_1X_2Y_1Y_2][(Z_1Z_2)^2 - aX_1X_2Y_1Y_2]$$

For two given points $P' = \Psi(P'') = (u_1, v_1) = \left(\frac{a\omega^2(Z_1 + Y_1)}{2(Z_1 - Y_1)}, \frac{a\omega^3 Z_1(Z_1 + Y_1)}{2X_1(Z_1 - Y_1)}\right)$ and $R = \Psi(R') = (u_2, v_2) = \left(\frac{a\omega^2(Z_2 + Y_2)}{2(Z_2 - Y_2)}, \frac{a\omega^3 Z_2(Z_2 + Y_2)}{2X_2(Z_2 - Y_2)}\right)$, we homogenize the Miller function:

$$\begin{aligned} g_{P',R}(Q') &= \frac{v_{Q'} - v_1 - \frac{v_1 - v_2}{u_1 - u_2}(u_{Q'} - u_1)}{u_{Q'} - u_3} \\ &= \frac{X_1(Z_1 - Y_1)^2}{\triangle_1 \cdot (u_{Q'} - u_3)} \\ &\quad \cdot \frac{\triangle_1 \cdot v_{Q'} - \omega \cdot \triangle_2 \cdot u_{Q'} + \omega^3 \cdot \triangle_3}{\triangle_1 \cdot (u_{Q'} - u_3)} \\ &\in \left(\triangle_1 \cdot v_{Q'} - \omega \cdot \triangle_2 \cdot u_{Q'} + \omega^3 \cdot \triangle_3\right) \mathbb{F}^*_{q^{k/2}} \end{aligned}$$

where

$$\triangle_1 = 2c_1 \cdot X_2 \cdot (Z_2 - Y_2) - 2X_2 \cdot (Z_2 + Y_2)$$
$$\triangle_2 = 2c_2 \cdot X_2 \cdot (Z_2 - Y_2) - 2Z_2 \cdot (Z_2 + Y_2)$$
$$\triangle_3 = ac_2 \cdot X_2(Z_2 + Y_2) - ac_1 \cdot Z_2 \cdot (Z_2 + Y_2)$$

with $c_1 = \frac{Z_1 + Y_1}{Z_1 - Y_1}, c_2 = \frac{Z_1(Z_1 + Y_1)}{X_1(Z_1 - Y_1)}$, the values c_1, c_2 do not change during the computation and can thus be precomputed. We just need to calculate the reduced function $g'_{P',R}(Q') = \triangle_1 \cdot v_{Q'} - \omega \cdot \triangle_2 \cdot u_{Q'} + \omega^3 \cdot \triangle_3$. While $\triangle_1, \triangle_2, \triangle_3 \in \mathbb{F}_q$ and $u_{Q'}, v_{Q'} \in \mathbb{F}_{q^{k/4}}$ is given, the evaluation at Q' can be computed in $\frac{k}{2}m$ (with $\frac{k}{4}m$ each for multiplications by $u_{Q'}$ and $v_{Q'}$).

Now, using the following sequence of operations to compute X_3, Y_3, Z_3 and $\Delta_i, i = 1, 2, 3$.

$$C = Z_1 \cdot Z_2, \quad D = X_1 \cdot X_2, \quad E = Y_1 \cdot Y_2$$
$$F = C^2, \quad G = a \cdot D, \quad H = G \cdot E, \quad I = F + H$$
$$J = F - H, \quad K = (Z_2 + Y_2), \quad L = X_2 \cdot K$$
$$M = X_2 \cdot (Z_2 - Y_2), \quad N = Z_2 \cdot K$$
$$X_3 = C \cdot I \cdot ((X_1 + Y_1) \cdot (X_2 + Y_2) - D - E)$$
$$Y_3 = C \cdot J \cdot (E - G), \quad Z_3 = I \cdot J, \quad \triangle_1 = 2c_1 \cdot M - 2L$$
$$\triangle_2 = 2c_2 \cdot M - 2N, \quad \triangle_3 = ac_2 \cdot L - ac_1 \cdot N$$

So, the total cost of the addition loop is $\frac{k}{2}m + 13m + 1s + 5m_c$. For mixed addition, *i.e.* $Z_1 = 1$, the total cost of the addition loop is $\frac{k}{2}m + 12m + 1s + 5m_c$.

2. The Tx-Ate pairing on $v^2 = u^3 + c\omega^6$

In this case, the j-invariant is zero and $a = (-7 \pm 4\sqrt{3})d$. Assume that $6 \mid k$, ω is a generator of $\mathbb{F}_{q^k}$ over $\mathbb{F}_{q^{k/6}}$, $\omega^6 \in \mathbb{F}_{q^{k/6}}$, $\omega^3 \in \mathbb{F}_{q^{k/3}}$ and $\omega^2 \in \mathbb{F}_{q^{k/2}}$. If the curve $W_{0,c,\omega} : v^2 = u^3 + c\omega^6$ is a sextic twisted curve of $E_{a,d}$, we can calculate the Tx-Ate pairing using the map Ψ defined in Eq.(14).

Doubling loop Let $R' = (X_2 : Y_2 : Z_2)$ and $(X_3 : Y_3 : Z_3) = [2](X_2 : Y_2 : Z_2)$, $R = \Psi(R') = \left(\frac{(Z_2 + Y_2)\omega^2}{B(Z_2 - Y_2)} + \frac{A\omega^2}{3B}, \frac{Z_2(Z_2 + Y_2)\omega^3}{BX_2(Z_2 - Y_2)}\right) = (u_2, v_2)$ and $Q' = (u_{Q'}, v_{Q'}) \in W_{0,c,\omega}(\mathbb{F}_{q^{k/6}})[r]$, we homogenize the affine doubling line using the map Ψ and get

$$\begin{aligned} g_{R,R}(Q') &= \frac{v_{Q'} - v_2 - \frac{3u_2^2}{2v_2}(u_{Q'} - u_2)}{u_{Q'} - u_3} \\ &= \frac{\Delta_1 \cdot v_{Q'} - \omega \cdot \Delta_2 \cdot u_{Q'} - \omega^3 \cdot \Delta_3}{18B^3X_2^2(Z_2 - Y_2)^3(u_{Q'} - u_3)} \\ &\in (\Delta_1 \cdot v_{Q'} - \omega \cdot \Delta_2 \cdot u_{Q'} - \omega^3 \cdot \Delta_3)\mathbb{F}^*_{q^{k/2}} \end{aligned}$$

where

$$\Delta_1 = 18B^2X_2Z_2(Z_2 - Y_2)^2(Z_2 + Y_2)$$
$$\Delta_2 = 3BX_2^2(Z_2 - Y_2)[3(Z_2 + Y_2) + A(Z_2 - Y_2)]^2$$
$$\Delta_3 = 18BZ_2^2(Z_2 + Y_2)^2(Z_2 - Y_2) - X_2^2[3(Z_2 + Y_2) + A(Z_2 - Y_2)]^3$$

We need to calculate the reduced function $g'_{R,R}(Q') = \Delta_1 \cdot v_{Q'} - \omega \cdot \Delta_2 \cdot u_{Q'} - \omega^3 \cdot \Delta_3$. While $\Delta_1, \Delta_2, \Delta_3 \in \mathbb{F}_q$ and $u_{Q'}, v_{Q'} \in \mathbb{F}_{q^{k/6}}$ is given, the evaluation at Q' can be computed in $\frac{k}{3}m$ (with $\frac{k}{6}m$ each for multiplications by $u_{Q'}$ and $v_{Q'}$).

We compute X_3, Y_3, Z_3 and $\Delta_i, i = 1, 2, 3$ using the following operations:

$$C = X_2 + Y_2, \ D = X_2^2, \ E = Y_2^2, \ F = Z_2^2, \ G = a \cdot D$$
$$H = E - G, \ I = E + G, \ J = 2F - I, \ K = X_2 + Z_2$$
$$L = Z_2 + Y_2, \quad M = Z_2 - Y_2, \quad N = 3B \cdot (F - E)$$
$$O = 3L + A \cdot M, \quad P = D \cdot O^2, \quad Q = 3B \cdot M$$
$$S = C^2 - D - E, \quad T = K^2 - D - F, \quad X_3 = S \cdot J$$
$$Y_3 = H \cdot I, \quad Z_3 = I \cdot J, \quad \Delta_1 = T \cdot N \cdot Q$$
$$\Delta_2 = Q \cdot P, \quad \Delta_3 = 6F \cdot N \cdot L - P \cdot O$$

The total count for the operations in doubling loop is $\frac{k}{3}m + 10m + 6s + 4m_c$.

Addition loop Let $P'' = (X_1 : Y_1 : Z_1)$ and $R' = (X_2 : Y_2 : Z_2)$, $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$. For the points $P' = \Psi(P'') = (u_1, v_1)$, $R =$

$\Psi(R')=(u_2,v_2)$ and $Q'=(u_{Q'},v_{Q'})$, we can use the formula $(u,v)=\left(\dfrac{Z+Y}{B(Z-Y)}\omega^2+\dfrac{A}{3B}\omega^2,\dfrac{\omega^3}{B}\cdot\dfrac{Z(Z+Y)}{X(Z-Y)}\right)$ and get

$$g_{P',R}(Q')=\frac{v_{Q'}-v_1-\dfrac{v_1-v_2}{u_1-u_2}(u_{Q'}-u_1)}{u_{Q'}-u_3}\in(\triangle_1\cdot v_{Q'}-\omega\cdot\triangle_2\cdot u_{Q'}+\omega^3\cdot\triangle_3)\mathbb{F}^*_{q^{k/2}}$$

where

$$\begin{aligned}\triangle_1&=X_2[c_1(Z_2-Y_2)-(Z_2+Y_2)]\\\triangle_2&=c_2X_2(Z_2-Y_2)-Z_2(Z_2+Y_2)\\\triangle_3&=c_3X_2[c_1(Z_2-Y_2)-(Z_2+Y_2)]\\&\quad-c_4[c_2X_2(Z_2-Y_2)-Z_2(Z_2+Y_2)]\end{aligned}$$

with $c_1=\dfrac{Z_1+Y_1}{Z_1-Y_1},c_2=\dfrac{Z_1(Z_1+Y_1)}{X_1(Z_1-Y_1)},c_3=\dfrac{c_1}{B},c_4=\dfrac{3c_1+A}{3B}$, the values c_1,c_2,c_3,c_4 do not change during the computation and can thus be precomputed. Then we just to calculate the reduced function $g'_{P',R'}(Q')=\triangle_1\cdot v_{Q'}-\omega\cdot\triangle_2\cdot u_{Q'}+\omega^2\cdot\triangle_3$, the evaluation at Q' can be computed in $\dfrac{k}{3}m$ (with $\dfrac{k}{6}m$ each for multiplications by $u_{Q'}$ and $v_{Q'}$).

To calculate $P''+R'$ and the function $g_{P',R}(Q')$, one needs $\dfrac{k}{2}m+13m+1s+5m_c$ using the following sequence of operations.

$$\begin{gathered}C=Z_1\cdot Z_2,\quad D=X_1\cdot X_2,\quad E=Y_1\cdot Y_2,\quad F=C^2\\G=a\cdot D,\quad H=G\cdot E,\quad I=F+H,\quad J=F-H\\K=c_1\cdot(Z_2-Y_2)-(Z_2+Y_2)\\L=c_2\cdot X_2\cdot(Z_2-Y_2),\quad M=Z_2\cdot(Z_2+Y_2)\\X_3=C\cdot I\cdot((X_1+Y_1)\cdot(X_2+Y_2)-D-E)\\Y_3=C\cdot J\cdot(E+G),\quad Z_3=I\cdot J\\\triangle_1=X_2\cdot K,\quad\triangle_2=L-M,\quad\triangle_3=c_3\cdot\triangle_1-c_4\cdot\triangle_2\end{gathered}$$

For mixed addition, *i.e.* $Z_1=1$, the total cost of the addition loop is $\dfrac{k}{3}m+12m+1s+5m_c$.

We can calculate the Tx-Ate pairing on twisted Weierstrass curves with $g=2$ using the method above. The following Table 1 shows the total costs of the operations about the calculation of the Tx-Ate pairing with $g=2,4,6$, for simplicity, Dbl represents doubling loop, Add (mAdd) represents (mixed) addition loop.

V. Comparison and Conclusions

This part shows the efficiency of the Tx-Ate pairing. Table 2 shows the comparison of the input parameters of Miller's algorithm between various pairings. Now, we consider the function $f_{s,C}(D)$ with s,C and D in Miller's algorithm. The number of calculation loops of Miller's algorithm is given by $\lfloor\log_2 s\rfloor$, the point C is used for a lot of computations such as the point operations and computing Miller functions, and the point D makes effect on the denominator of Miller functions. As we all know, the Ate pairing and the twisted Ate pairing are more efficient than the Tate pairing. Furthermore, Costello *et al.*[9] compared the efficiency of optimal Ate pairing and the twisted Ate paring, from Table 4 of Ref.[9], we can get that the loop length of optimal Ate pairing is smaller than that of the twisted Ate pairing in many cases, but in each loop, the operation costs of optimal Ate pairing are always more than that of the twisted Ate pairing. When $k=4,6,8$ with twist degree $g=4,6,4$, the twisted Ate paring is more efficient than optimal Ate pairing.

Table 1. The costs of the Tx-Ate pairing

	Dbl	mAdd	Add
$W_{b\omega^4,c\omega^6}$ ($g=2$)	$km+10m$ $+6s+4m_c$	$km+12m$ $+1s+5m_c$	$km+13m$ $+1s+5m_c$
$W_{b\omega^4,0}$ ($g=4$)	$\frac{k}{2}m+9m$ $+6s+2m_c$	$\frac{k}{2}m+12m$ $+1s+5m_c$	$\frac{k}{2}m+13m$ $+1s+5m_c$
$W_{0,c\omega^6}$ ($g=6$)	$\frac{k}{3}m+10m$ $+6s+4m_c$	$\frac{k}{3}m+12m$ $+1s+5m_c$	$\frac{k}{3}m+13m$ $+1s+5m_c$

Table 2. Input parameters of Miller function $f_{s,C}(D)$

Pairing	s	C	D
Tate	r	$W_{b,c}(\mathbb{F}_q)$	$W_{b,c}(\mathbb{F}_{q^k})$
Ate	$t-1$	$W_{b,c}(\mathbb{F}_{q^k})$	$W_{b,c}(\mathbb{F}_q)$
Twisted Ate	$(t-1)^e \bmod r$	$W_{b,c}(\mathbb{F}_q)$	$W_{b,c}(\mathbb{F}_{q^k})$
Tx-Ate	$(t-1)^e \bmod r$	$E_{a,d}(\mathbb{F}_q)$	$W_{b,c,\omega}(\mathbb{F}_{q^e})$

In this paper, we define a special twisted Ate pairing—Tx-Ate pairing, which is defined on twisted Weierstrass curves. From Table 2, the input parameters of Tx-Ate pairing are computed in different forms of elliptic curves. Now, we compare the Tx-Ate pairing with the twisted Ate pairing computed total on Weierstrass curves and the Tate pairing computed total on Edwards curves, in Table 3, we give comparisons of our pairing formulas with the previous fastest formulas. Because the cost for the evaluation at Q' ($\dfrac{2k}{e}m$) does not change during the computation of pairings, we do not comment on the cost in Table 3. To compare across operations, we assume that $1s\approx 0.8m, 1m_c\approx 0.5m$ in Table 4. We also give detailed analyses of superior and inferior in the following.

1) In one Addition loop, the operation cost in this paper is almost the same as those of the other two forms.

2) In one doubling loop, the operation costs of our formulas are about $5m$ costs slower than that of computing the Tate pairing over twisted Edwards curves. But, the loop length of the Tate pairing is larger than the loop length of the Tx-Ate pairing. The Tx-Ate pairing can not be defined on twisted Edwards curves, because $E_{a,d}$ and

its twists can not both be in Edwards forms for high twist degree.

3) In one doubling loop, the operation costs of our formulas are about $6m$ costs slower than that of previous fastest formulas to compute the twisted Ate pairing in short Weierstrass curves. From above discussion, in the cases $k = 4, 6, 8$ with $g = 4, 6, 4$, the loop length $(t-1)^e \bmod r$ can achieve the loop length of optimal Ate pairing, the twisted Ate paring is more efficient than optimal Ate pairing. Although our pairing is slower than the twisted Ate pairing in one doubling loop. By twists, we can get more twisted Weierstrass curves with short loop length and can compute the Tx-Ate pairing on such pairing-friendly curves. So, the Tx-Ate pairing calculated by our method is also competitive with optimal Ate pairing when they have the same short loop length.

Table 3. Comparing with the previous fastest formulas

g		This paper	Total on $E_{a,d}$[12]	Total on $W_{b,c}$[9]
$g=2$	Dbl	$10m+6s+4m_c$	$6m+5s+2m_c$	$7m+6s+1m_c$
	mAdd	$12m+1s+5m_c$	$12m+1m_c$	$12m+2s$
	Add	$13m+1s+5m_c$	$14m+1m_c$	$14m+2s+1m_c$
$g=4$	Dbl	$9m+6s+2m_c$	$6m+5s+2m_c$	$2m+8s+1m_c$
	mAdd	$12m+1s+5m_c$	$12m+1m_c$	$9m+5s$
	Add	$13m+1s+5m_c$	$14m+1m_c$	$12m+7s$
$g=6$	Dbl	$10m+6s+4m_c$	$6m+5s+3m_c$	$2m+7s+1m_c$
	mAdd	$12m+1s+5m_c$	$12m+2m_c$	$10m+2s+1m_c$
	Add	$13m+1s+5m_c$	$14m+2m_c$	$13m+2s+1m_c$

Table 4. Comparing across operations in Table 3

g		This paper	Total on $E_{a,d}$[12]	Total on $W_{b,c}$[9]
$g=2$	Dbl	$16.8m$	$11m$	$12.3m$
	mAdd	$15.3m$	$12.8m$	$13.6m$
	Add	$16.3m$	$14.8m$	$16.1m$
$g=4$	Dbl	$14.8m$	$11m$	$8.9m$
	mAdd	$15.3m$	$12.8m$	$13m$
	Add	$16.3m$	$14.8m$	$17.6m$
$g=6$	Dbl	$16.8m$	$11.5m$	$8.1m$
	mAdd	$15.3m$	$13m$	$12.1m$
	Add	$16.3m$	$15m$	$15.1m$

References

[1] Joux Antoine, "A one round protocol for tripartite Diffie-Hellman", *International Algorithmic Number Theory Symposium*, Springer, Berlin, Heidelberg, Vol.17, No.4, pp.385–393, 2000.

[2] Boneh Dan and Matt Franklin, "Identity-based encryption from the Weil pairing", *Advances in Cryptology-CRYPTO 2001*, Springer, Berlin, Heidelberg, pp.213–229, 2001.

[3] Koblitz Neal and Alfred Menezes, "Pairing-based cryptography at high security levels", *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, Vol.3796, pp.13–36, 2005.

[4] Boneh Dan, Ben Lynn and Hovav Shacham, "Short signatures from the Weil pairing", *Advances in Cryptology ASIACRYPT*, pp.514–532, 2001.

[5] Hess Florian, "Pairing lattices", *Pairing-Based Cryptography-Pairing 2008*, Springer, Berlin, Heidelberg, pp.18–38, 2008.

[6] Vercauteren Frederik, "Optimal pairings", *IEEE Transactions on Information Theory*, Vol.56, No.1, pp.455–461, 2010.

[7] Boxall John, El Mrabet Nadia, Laguillaumie Fabien, *et al.*, "A variant of millers formula and algorithm", *International Conference on Pairing-Based Cryptography*, Springer, Berlin, Heidelberg, pp.417–434, 2010.

[8] Yasuyuki Nogami, Masataka Akane, Yumi Sakemi, *et al.*, "Efficient pairings on twisted Elliptic curve", *Third International Conference on Convergence and Hybrid Information Technology* (*ICCIT'08*), Vol.2, pp.430–439, 2008.

[9] Costello Craig, Lange Tanja and Naehrig Michael, "Faster pairing computations on curves with high-degree twists", *International Workshop on Public Key Cryptography*, Springer, Berlin, Heidelberg, pp.224–242, 2010.

[10] Edwards Harold, "A normal form for elliptic curves", *Bulletin of the American Mathematical Society*, Vol.44, No.3, pp.393–422, 2007.

[11] Bernstein Daniel J, Birkner Peter, Joye Marc, *et al.*, "Twisted Edwards curves", *International Conference on Cryptology in Africa*, Springer, Berlin, Heidelberg, pp.389–405, 2008.

[12] Arene Christophe, Lange Tanja, Naehrig, *et al.*, "Faster computation of the Tate pairing", *Journal of Number Theory*, Vol.131, No.5, pp.842–857, 2011.

[13] Le Duc-Phong and Tan Chik How, "Improved Millers algorithm for computing pairings on Edwards curves", *IEEE Transactions on Computers*, Vol.63, No.10, pp.2626–2632, 2014.

[14] Miller Victor S, "The Weil pairing, and its efficient calculation", *Journal of Cryptology*, Vol.17, No.4, pp.235–261, 2004.

[15] Silverman Joseph H and Artin M, *Arithmetic Geometry*, Springer, 1986.

[16] Morain François, "Edwards curves and CM curves", *arXiv preprint arXiv:0904 2243*, 2009.

[17] Hess Florian, Smart Nigel P and Vercauteren Frederik, "The eta pairing revisited", *IEEE Transactions on Information Theory*, Vol.52, No.10, pp.4595–4602, 2006.

[18] Barreto Paulo SLM, Galbraith Steven D, ÓhÉigeartaigh Colm, *et al*, "Efficient pairing computation on supersingular abelian varieties", *Designs, Codes and Cryptography*, Vol.42, No.3, pp.239–271, 2007.

[19] Lee Eunjeong, Lee Hyang-Sook and Park Cheol-Min, "Efficient and generalized pairing computation on abelian varieties", *IEEE Transactions on Information Theory*, Vol.55, No.4, pp.1793–1803, 2009.

WANG Bei is currently working toward the Ph.D. degree at University of Science and Technology of China. Her research interest focuses on fast computation of elliptic curve cryptography. (Email: wangbei@mail.ustc.edu.cn)

OUYANG Yi is currently a professor in School of Mathematical Sciences at University of Science and Technology of China. His research interests mainly include number theory and arithmetic algebraic geometry. (Email: yiouyang@ustc.edu.cn)

HU Honggang is currently a professor in School of Information Science and Technology at University of Science and Technology of China. His research interests mainly include coding, cryptography and network security. (Email: hghu2005@ustc.edu.cn)