On Efficient Pairings on Elliptic Curves over Extension Fields

Xusheng Zhang[1,2], Kunpeng Wang[3], and Dongdai Lin[3]

[1] Institute of Software, Chinese Academy of Sciences, Beijing, 100190, China.
[2] Graduate University of Chinese Academy of Sciences, Beijing, 100049, China.
xszhang.is@gmail.com
[3] SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences,
Beijing, 100195, China.
kunpengwang@263.net, ddlin@iie.ac.cn

Abstract. In implementation of elliptic curve cryptography, three kinds of finite fields have been widely studied, i.e. prime field, binary field and optimal extension field. In pairing-based cryptography, however, pairing-friendly curves are usually chosen among ordinary curves over prime fields and supersingular curves over extension fields with small characteristics. In this paper, we study pairings on elliptic curves over extension fields from the point of view of accelerating the Miller's algorithm to present further advantage of pairing-friendly curves over extension fields, not relying on the much faster field arithmetic. We propose new pairings on elliptic curves over extension fields can make better use of the multi-pairing technique for the efficient implementation. By using some implementation skills, our new pairings could be implemented much more efficiently than the optimal ate pairing and the optimal twisted ate pairing on elliptic curves over extension fields. At last, we use the similar method to give more efficient pairings on Estibals's supersingular curves over composite extension fields in parallel implementation.

Keywords: pairing, elliptic curve over extension field, multi-pairing technique

1 Introduction

Elliptic curve cryptography (ECC) has the shorter key length requirement in comparison with other public-key cryptosystems such as RSA. This means faster implementation as well as more efficient use of power, bandwidth and storage. In particular, much research has been conducted on fast algorithms and implementation techniques of elliptic curve arithmetic over various finite fields. Up to now, three kinds of finite fields are widely used for ECC, i.e. prime field, binary field and optimal extension field. Binary fields $\mathbb{F}(2^m)$ are especially attractive for hardware circuit design, but does not offer the same computational advantages in a software implementation. Similarly, prime fields $\mathbb{F}(p)$ also have computational difficulties on standard computers. Optimal extension fields $\mathbb{F}(p^m)$ introduced in [1, 2], offer considerable computational advantages in software by selecting p and m specifically to match the underlying hardware used to perform the arithmetic. Besides, efficient methods have been devised in [27, 3] for speeding up field arithmetic for elliptic curves over general extension fields.

In recent years, there has been much interest in cryptographic schemes based on bilinear pairings on elliptic curves. So efficient implementation of pairings is of great importance. Miller [29] proposed the first effective algorithm named Miller's algorithm to compute Weil pairing and Tate pairing. As the important breakthroughs, there are many optimizations and adaptations of these pairings which offer implementation improvements, such as speeding up each Miller's iteration and the final exponentiation of the Tate pairing, and developing many truncated loop variant pairings: Eta pairing [5], ate pairing and twisted ate pairing [22], R-ate pairing [26], and optimal pairing [33]. Recently, pairing lattices [21] were proposed as the generalization contained all former pairings.

On the other side, there is much research on the generation of suitable elliptic curves for pairings, namely pairing-friendly curves, which contain the large prime subgroup and the small embedding degree. Please refer to the in-depth overview [12] for details. Whereas strong elliptic curves used in ECC can be generated randomly, the pairing-friendly curves are rare and require specific constructions. All the time, pairing-friendly curves are chosen among ordinary curves over prime fields and supersingular curves over extension fields with the characteristic 2 and 3. In the latter case, pairings are suitable for hardware implementation in lightweight cryptosystems. For higher security, pairings on ordinary pairing-friendly curves are preferred in practice.

In implementation, there are always some strong requests to use curves defined over certain extension fields, such as the extension fields with small characteristics, and the optimal extension fields which possess the fast field multiplication and inversion. So there are theoretical advantages to using pairing-friendly elliptic curves over carefully chosen finite fields. Recently, Hitt [23] and Benger *et al.* [6] outlined possible security concerns for using pairing-friendly elliptic curves defined over extension fields, and Benger *et al.* [6] gave a method for selecting curves with the highest possible security against ECDLP and DLP solving attacks, given currently known methods. To the best of our knowledge, there is still no known example of an ordinary pairing-friendly curve defined over the extension field $\mathbb{F}_{p^m}$ or $\mathbb{F}_{2^m}$. Hence, we present results which may motivate further research into the generation of pairing-friendly elliptic curves defined over extension fields.

In this paper, our main aim is to present further evidence of an advantage of using pairing-friendly elliptic curves defined over extension fields by introducing a pairing which can be computed using an accelerated version of Miller's algorithm, using the multi-pairing technique. We develop new pairings on an elliptic curve over an extension field which could be computed more efficiently not relying on the fast field arithmetic of the extension field. Concretely, for an ordinary curve E over an extension field $\mathbb{F}_{p^m}$, we modify the ate pairing and the twisted ate pairing to define new pairings as the products of several rational functions with the same

Miller loop on the curves $\{E^{(p^i)}\}_{0\le i<m}$ defined by raising the coefficients of the equations for E to the p^i-power. These new pairings can be implemented with the multi-pairing technique which was proposed in [31, 19] and first applied to a single pairing computation by Sakemi *et al.* [30]. Then we give the optimal versions of our new pairings according to the theory of pairing lattice [21], which can make better use of the multi-pairing technique for efficient implementation. Specially, our method can explain Sakemi's acceleration [30] of the twisted ate pairing on the BN curves and extend it further. Given a theoretical comparison with some implementation skills, our new optimal pairings could have more efficient performance than the optimal ate pairing and the optimal twisted ate pairing. Specially in many protocols, with the fixed argument optimization, the performance of our new optimal pairing could offer a speed up of between 30% and 43% faster than the performance of the optimal ate pairing when m is greater than 6. Finally, we develop similar pairings having much faster parallel implementation on supersingular curves over composite extension fields, and then construct concrete pairings on Estibals's supersingular curves $E_1(\mathbb{F}_{3^{5\times 97}})$ and $E_2(\mathbb{F}_{3^{17\times 67}})$ respectively.

The organization is given as: Section 2 recalls basics of pairing on elliptic curve and multi-pairing technique, and lists known conditions on suitably chosen extension fields for pairing-based cryptography; in Section 3 we propose new faster pairings on ordinary curves over extension fields; then in Section 4 we analyze the theoretical performance of our new optimal pairings compared to the optimal ate pairing and optimal twisted ate pairing; in Section 5 we extend the similar method to supersingular curves over composite extension fields.

2 Background

2.1 Bilinear Pairing

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ where q is a prime power, and the neutral element of which is denoted by $\mathcal{O}$. Let $r \geq 5$ be a prime factor of $|E(\mathbb{F}_q)|$ and let $k > 1$ be the smallest integer such that $r|q^k - 1$ which is named the embedding degree with respect to r. Here we define $G_1 = E[r] \cap \mathrm{Ker}(\pi_q - 1)$ and $G_2 = E[r] \cap \mathrm{Ker}(\pi_q - q)$ as the two eigenspaces of the q-power Frobenius endomorphism π_q on E. Let $\mu_r \subset \mathbb{F}_{q^k}^*$ denote the group of r-th roots of unity. For $s \in \mathbb{Z}$ and $R \in E[r]$, let $f_{s,R}$ be a $\mathbb{F}_{q^k}$-rational function with divisor $\mathrm{div}(f_{s,R}) = s(R) - ([s]R) - (s-1)(\mathcal{O})$.

Tate pairing and its variants. The reduced Tate pairing [4] is given by

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

Let s be an integer such that $s \equiv q \pmod r$. When $r \nmid c \equiv \sum_{j=0}^{k-1} s^{k-1-j} q^j \pmod r$, the modified ate pairing [22] is given by

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

Assume that $E/\mathbb{F}_q$ admits a degree-d twist. Let $e = k/\gcd(k,d)$ and $s' \in \mathbb{Z}$ satisfy that $s' \equiv q^e \pmod r$. The modified twisted ate pairing [22] is given by

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

Then a_s and $a_{s'}^{twist}$ are non-degenerate if and only if $r \nmid L = (s^k - 1)/r$.

For the convenience of the construction of new pairings, we use the variants $a(Q,P) = f_{q,Q}(P)^{(q^k-1)/r}$ and $a^{twist}(P,Q) = f_{q^e,P}(Q)^{(q^k-1)/r}$ instead of the above ate pairing and twisted ate pairing in the rest of this paper.

Miller's algorithm. Let $f_{i,P}$ be the rational function with divisor $\mathrm{div}(f_{i,P}) = i(P) - ([i]P) - (i-1)(\mathcal{O})$, and $l_{R,S}$ is the line passing through points R, S and v_{R+S} is the vertical line passing through point $R+S$ with divisor $\mathrm{div}(l_{R,S}) = (R) + (S) + (-(R+S)) - 3(\mathcal{O})$ and $\mathrm{div}(v_{R+S}) = (R+S) + (-(R+S)) - 2(\mathcal{O})$. Using the fact that $f_{i_1+i_2,P} = f_{i_1,P} f_{i_2,P} l_{[i_1]P,[i_2]P}/v_{[i_1+i_2]P}$, Miller's algorithm [29] calculates the evaluation of $f_{i,P}(Q)$ recursively. In §2.2 Algorithm 1 is just the classical Miller's algorithm when assuming $N = 1$.

Optimal pairing. In [33], Vercauteren proposed an important conception of a pairing having the "optimal" loop length. Let $e : G_1 \times G_2 \to \mu_r$ be a non-degenerate pairing with $|G_1| = |G_2| = r$, then e is called an optimal pairing if it can be computed in $\frac{1}{\varphi(k)} \log_2 r + \epsilon(k)$ basic Miller iterations, with $\epsilon(k) \leq \log_2 k$. Furthermore, Vercauteren conjectured that any non-degenerate pairing on an elliptic curve without efficiently computable endomorphisms different from powers of Frobenius, requires at least $O(\log_2(r)/\varphi(k))$ basic Miller iterations, where the O-constant only depends on k.

Pairing lattices. Hess [21] generalized the conception of the optimal pairing to provide pairing lattices as a convenient mathematical framework to create pairings with optimal degrees of the divisors of pairing functions. Let $r \in \mathbb{Z}$ be an integer, and let s be a primitive n-th root of unity modulo r^i for $n \geq 2$ and $i \geq 1$. Define the $\mathbb{Z}$-module $I^{(i)} = \{h(t) + (t^n - 1)\mathbb{Z}[t] | h(s) \equiv 0 \pmod{r^i}\}$, and $||h||_1 = \sum_{i=0}^{m} |h_i|$. For $h(t) = \sum_{i=0}^{m} h_i t^i \in I^{(1)}$ and $R \in E(\mathbb{F}_{q^k})[r]$, let $f_{s,h,R}$ be the $\mathbb{F}_{q^k}$-rational function with divisor $\mathrm{div}(f_{s,h,R}) = \sum_{i=0}^{m} h_i\big(([s^i]R) - (\mathcal{O})\big)$. It is easy to deduce that $\mathrm{div}(f_{s,ht,R}) = \mathrm{div}(f_{s,h,[s]R})$ and $\mathrm{div}(f_{s,h+g,R}) = \mathrm{div}(f_{s,h,R} f_{s,g,R})$ for $g(t) \in I^{(1)}$.

The evaluation of $f_{s,h,R}(P)$ can be calculated analogously to the method for the optimal ate pairing in [33] (also cf. [34]). Following this analysis, we may assume that the length of the Miller loop for calculating $f_{s,h,R}$ is approximated by $\log_2 ||h||_1 + \epsilon$, where $\epsilon \leq \log_2 n$.

Theorem 1. *([21], Theorem 6) Assume that r is a prime, and s is a primitive n-th root of unity modulo r^2. Let W denote the multiplicative group of functions $G_1 \times G_2 \to \mu_r$, and W^{bilin} denote the subgroup of bilinear functions. Let $a_s : I^{(1)} \to W, h \mapsto a_{s,h}$ be a map with the following properties:*

1. *$a_{s,g+h} = a_{s,g} a_{s,h}$ for all $g, h \in I^{(1)}$,*

2. *$a_{s,hx} = a_{s,h}^{s}$ for all $h \in I^{(1)}$ with $a_{s,h} \in W^{bilin}$,*
3. *$a_{s,r} \in W^{bilin} \setminus \{1\}$ and $a_{s,x-s} = 1$.*

Then $\mathrm{Im}(a_s) = W^{bilin}$, $\ker(a_s) = I^{(2)}$. *More precisely, $a_{s,h} = a_{s,r}^{h(s)/r}$ for all $h \in I^{(1)}$. There exists an efficiently computable $h \in I^{(1)}$ with $\|h\|_1 = O(r^{1/\varphi(n)})$. Any $h \in I^{(1)}$ with $a_{s,h} \neq 1$ satisfies $\|h\|_1 \geq r^{1/\varphi(n)}$.*

Especially, the optimal ate pairing and the optimal twisted ate pairing are well-defined and probably constructed in the ate pairing lattice and the twisted ate pairing lattice in [21] with the optimal loop length $\log_2(r)/\varphi(k) + \epsilon_1$ and $\log_2(r)/\varphi(d) + \epsilon_2$.

2.2 Multi-Pairing Technique

In many protocols the evaluation of the products of the form $\prod_{i=1}^{N} t_r(P_i, Q_i)$ is required. A naive way to calculate it is to evaluate each $t_r(P_i, Q_i)$ independently, and then multiply the results. Since all $t_r(P_i, Q_i)$ share some same Miller operations, Scott [31] and Granger and Smart [19] showed the products can be calculated in a single Miller algorithm rather than the naive way. The multi-Miller algorithm only needs a single squaring in the extension field per doubling, instead of N squarings in the naive method, and also combines the final powerings required in each pairing evaluation. As far as we know, this method is usually named multi-pairing algorithm given in Algorithm 1.

Algorithm 1 Miller's Algorithm for Multi-pairing

```
Input: $s = \sum_{j=0}^{L} s_j 2^j \in \mathbb{N}$ (2-adic), $N \in \mathbb{N}$, $\{P_1, P_2, \cdots, P_N\}$, $\{Q_1, Q_2, \cdots, Q_N\}$
Output: $\prod_{i=1}^{N} f_{s,P_i}(Q_i)$, $\{[s]P_1, [s]P_2, \cdots, [s]P_N\}$
f ← 1
for $i$ from $N$ downto 1 do
    $T_i \leftarrow P_i$
for $j$ from $L-1$ downto 0 do
    $f \leftarrow f^2$
    for $i$ from $N$ downto 1 do
        $f \leftarrow f \cdot l_{T_i,T_i}(Q)/v_{[2]T_i}(Q_i)$;   $T_i \leftarrow [2]T_i$
    if $s_j = 1$ then
        for $i$ from $N$ downto 1 do
            $f \leftarrow f \cdot l_{T_i,P_i}(Q_i)/v_{T_i+P_i}(Q_i)$;   $T_i \leftarrow T_i + P_i$
return f.
```

However, not only can the multi-pairing technique be used to calculate the products of pairings, but it also can be applied to calculate a single pairing defined as the products of several rational functions with the same Miller loop. In [30], Sakemi *et al.* utilized the multi-pairing technique to calculate the improved twisted ate pairing on the BN curves with the sophisticated reduction. We extend this idea to the implementation of pairings considered in this paper.

2.3 Suitable Extension Field for Pairing-Based Cryptography

In the rest of this paper we always assume that there is a pairing-friendly curve E defined over an extension field $\mathbb{F}_q$ with $q = p^m$. Let r divide $|E(\mathbb{F}_q)|$ but do not divide any other $|E(\mathbb{F}_{p^i})|$ for $1 \leq i < m$. We list some well-known results of the security extension fields for ECC and Pairing-Based Cryptography, and show our suitable choice of the extension fields for the comparison in Section 4.

Attack on ECDLP over extension field. Weil descent proposed by Frey [13] aims at transferring the DLP from $E(\mathbb{F}_{q^m})$ to the Jacobian of a curve C over $\mathbb{F}_q$ and then computes the logarithm on this Jacobian by using index calculus. Many researches [15, 17, 14, 20, 28] have studied on the scope of this technique on the vulnerable curves over binary fields. Diem [9] extended this attack in odd characteristic.

Later, Gaudry [16] developed decomposition-based index calculus, which applies to all (hyper-)elliptic curves defined over small degree extension field with the running time $O(q^{2-2/m})$ for $m \geq 3$. Diem [10] proved that Gaudry's algorithm has subexponential running time when the field order p^m increases in such a way that m^2 is of order $\log_2 p$. Later, Joux and Vitse [24] improved this index calculus, when $m > 5$ and $\log_2 p \leq O(m^3)$.

But, both Weil descent and decomposition-based index calculus are often just a little more efficient than generic attacks, and ineffective for solving the ECDLP in practice.

The static Diffie-Hellman problem The Static Diffie-Hellman problem (Static DHP) on an elliptic curve consists of: for a secret integer d, given two points $P, [d]P \in E(\mathbb{F}_q)$ and an oracle $Q \mapsto [d]Q$, compute $[d]R$ where R is randomly chosen point. Recently Granger [18] discovered the best known algorithm that solves the Static DHP problem on elliptic curves defined over a finite field of composite extension degree $\mathbb{F}_{q^n}$ by making $O(q^{1-\frac{1}{n+1}})$ Static DHP oracle queries and in *heuristic* time $O(q^{1-\frac{1}{n+1}})$. Estibals [11] showed that a simple but efficient protection against this attack is revoking a key after a certain amount of use.

Minimal embedding field. The embedding degree k should be small enough that the pairing is efficiently computable, but large enough that the DLP in $\mathbb{F}_{q^k}^*$ is hard. However, Hitt [23] showed that the minimal finite field ensures the ECDLP of $E(\mathbb{F}_q)[r]$ secure is not necessarily $\mathbb{F}_{q^k}$, but rather is $\mathbb{F}_{p^{\mathrm{ord}_r(p)}} = \mathbb{F}_{q^{\mathrm{ord}_r(p)/m}}$. Then $\mathbb{F}_{q^{\mathrm{ord}_r(p)/m}}$ is named the minimal embedding field and coincides with the traditional assumptions when $m = 1$. Later, Benger *et al.* [6] gave explicit conditions on q, k, and r, which (when satisfied) imply that the minimal embedding field of E with respect to r is $\mathbb{F}_{q^k}$.

Theorem 2. *([6], Corollary 2.10) Let A be an abelian variety over F_q, where $q = p^m$ with p prime. Let $r \neq p$ be a prime dividing $|A(F_q)|$, and suppose A has embedding degree k with respect to r. Assume that $r \nmid km$. Write $m = \alpha\beta$, where every prime dividing α also divides k and* $\gcd(k, \beta) = 1$. *(This factorization is* *unique.) Denote by e the smallest prime factor of β. If q, k, and r satisfy any of the following conditions:*

1. *$m = \alpha$ (and $\beta = 1$);*
2. *β is prime and $r > \Phi_{k\alpha}(p)$;*
3. *$r > p^{km/e}$;*
4. *$4|m$ or $2|k$ and $r > p^{km/2e} + 1$.*

Then the minimal embedding field of A with respect to r is $\mathbb{F}_{p^{km}}$.

Hence, in this paper we prefer to choose a large prime p and an integer $m \geq 5$ to prevent the known attacks in practice. If there exist algorithms to generate pairing-friendly curves over $\mathbb{F}_{p^m}$ defined in [12], we may restrict m, p, k and r to satisfy one of the conditions in Theorem 2. For the comparison in Section 4, we use even embedding degrees of the form $k = 2^i 3^j$ and examine examples using: $m = 7, 11$ ($m > \phi(k)$), such that condition (2) of Theorem 2 is satisfied; and, $m = 8, 9$, such that condition (1) of Theorem 2 is satisfied.

3 New Pairings on Elliptic Curve over Extension Field

In this section we propose new pairings on an elliptic curve E over an extension field $\mathbb{F}_q$ which make better use of the multi-pairing technique to speed up their implementation. We first transform the ate pairing $a(Q,P) = f_{q,Q}(P)^{(q^k-1)/r}$ and the twisted ate pairing $a^{twist}(P,Q) = f_{q^e,P}(Q)^{(q^k-1)/r}$ as follows.

Theorem 3. *Let E be an ordinary elliptic curve defined over $\mathbb{F}_q$ with $q = p^m$. Let r be a prime such that r divides $|E(\mathbb{F}_q)|$ and $\gcd(r,p) = 1$. Let k be the minimal embedding degree with respect to r. Let $E^{(p^i)}$ be denoted the curve defined by raising the coefficients of the equation for E to the p^i-power for $0 \leq i < m$. Let π_{p^i} and $\widehat{\pi}_{p^i}$ be the p^i-power Frobenius isogeny and its dual isogeny from every $E^{(p^j)}$ to $E^{(p^{j+i})}$. For $P \in G_1$ and $Q \in G_2$, then*

$$\bar{a}(Q,P) = \left(\prod_{i=0}^{m-1} f_{p,\widehat{\pi}_{p^i}(Q)}\big(\pi_{p^{m-i}}(P)\big) \right)^{(p^{mk}-1)/r}$$

defines a pairing.

Assume that $E/\mathbb{F}_q$ admits a degree-d twist $E'/\mathbb{F}_{q^e}$ with $e = k/\gcd(k,d)$ and $d \geq 2$. Let ψ be the associated twist isomorphism $\psi : E \to E'$. Then

$$\hat{a}(Q,P) = \left(\prod_{i=0}^{m-1} f_{p,\widehat{\pi}_{p^i}\circ\psi(Q)}\big(\pi_{p^{mk-i}} \circ \psi(P)\big) \right)^{(p^{mk}-1)/r}$$

and

$$\bar{a}^{twist}(P,Q) = \left(\prod_{i=0}^{m-1} \prod_{j=0}^{e-1} f_{p,\widehat{\pi}_{p^i}([p^{mj}]P)}\big(\pi_{p^{mk-i}}(Q_{e-j-1})\big) \right)^{(p^{mk}-1)/r}$$

define pairings, where $Q_j = \pi_{p^{mj}}(Q)$ for $0 \leq j \leq e-1$.

Proof. Since $[p^i] = \pi_{p^i} \circ \widehat{\pi}_{p^i}$ with $\pi_{p^i} : E^{(p^{m-i})} \to E$ for some i, it follows that for $R \in E(\mathbb{F}_{p^k})[r]$, $\pi^*_{p^i}\mathrm{div}(f_{p,[p^i]R}) = \pi^*_{p^i}\big(p([p^i]R) - ([p^{i+1}]R) - (p-1)(\mathcal{O})\big) = p^i\big(p(\widehat{\pi}_{p^i}(R)) - (\widehat{\pi}_{p^i}([p]R)) - (p-1)(\mathcal{O})\big) = \mathrm{div}(f^{p^i}_{p,\widehat{\pi}_{p^i}(R)})$, where $\pi^*_{p^i}$ is the pullback of π_{p^i}. Thus $f_{p,[p^i]R} \circ \pi_{p^i} = f^{p^i}_{p,\widehat{\pi}_{p^i}(R)} \in \mathbb{F}_{q^k}(E^{(p^{m-i})})$. If $R = Q$, then $f_{p,[p^i]Q}(P) = f_{p,\widehat{\pi}_{p^i}(Q)}(\pi_{p^{m-i}}(P))^{p^i}$; if $R = P$, then $f_{p,[p^i]P}(Q) = f_{p,\widehat{\pi}_{p^i}(P)}(\pi_{p^{mk-i}}(Q))^{p^i}$. When E admits a twist of degree d, if $R = Q' = \psi(Q) \in E'(\mathbb{F}_{q^e})[r]$ and $P' = \psi(P) \in E'(\mathbb{F}_{q^k})[r]$, then $f_{p,[p^i]Q'}(P') = f_{p,\widehat{\pi}_{p^i}(Q')}(\pi_{p^{mk-i}}(P'))^{p^i}$.

Since $\gcd(p, r) = 1$, there exits an integer M such that $Mp^{m-1} \equiv 1 \pmod{r}$. Note that a power of a nondegenerate pairing is also a nondegenerate pairing when the power and the pairing order are coprime. Thus we can do the following reduction for a fixed power M of the ate pairing $a(Q, P)$.

$$a(Q,P)^M = f_{q,Q}(P)^{M(q^k-1)/r} = \prod_{i=0}^{m-1} f_{p,[p^i]Q}(P)^{p^{m-i-1}M(q^k-1)/r}$$
$$= \prod_{i=0}^{m-1} f_{p,\widehat{\pi}_{p^i}(Q)}(\pi_{p^{m-i}}(P))^{Mp^{m-1}(q^k-1)/r} = \prod_{i=0}^{m-1} f_{p,\widehat{\pi}_{p^i}(Q)}(\pi_{p^{m-i}}(P))^{(q^k-1)/r}.$$

When E admits a twist of degree d, then $a(Q', P') = f_{q,Q'}(P')^{(q^k-1)/r}$ also defines a pairing from Theorem 1 in [7], where $P' = \psi(P) \in E'(\mathbb{F}_{q^k})[r]$ and $Q' = \psi(Q) \in E'(\mathbb{F}_{q^e})[r]$. So a similar reduction can be done for $a(Q', P')^M$ as

$$a(Q',P')^M = f_{q,Q'}(P')^{M(q^k-1)/r} = \prod_{i=0}^{m-1} f_{p,[p^i]Q'}(P')^{p^{m-i-1}M(q^k-1)/r}$$
$$= \prod_{i=0}^{m-1} f_{p,\widehat{\pi}_{p^i}(Q')}(\pi_{p^{mk-i}}(P'))^{Mp^{m-1}(q^k-1)/r} = \prod_{i=0}^{m-1} f_{p,\widehat{\pi}_{p^i}(Q')}(\pi_{p^{mk-i}}(P'))^{(q^k-1)/r}.$$

For the twisted ate pairing, since $f_{p,\widehat{\pi}_{p^i}(P)} \in \mathbb{F}_q(E^{(p^{m-i})})$, let $Q_j = \pi_{q^j}(Q)$ for $0 \le j \le e-1$, it follows that $f_{p,\widehat{\pi}_{p^i}(P)}(\pi_{p^{mk-i}}(Q))^{q^j} = f_{p,\widehat{\pi}_{p^i}(P)}(\pi_{p^{mk-i}}(Q_j))$. Thus we have that

$$\begin{aligned} a^{twist}(P,Q)^M &= f_{q^e,P}(Q)^{M(q^k-1)/r} = \prod_{j=0}^{e-1} f_{q,[q^i]P}(Q)^{q^{e-i-1}M(q^k-1)/r} \\ &= \prod_{j=0}^{e-1}\prod_{i=0}^{m-1} f_{p,[p^{mj+i}]P}(Q)^{q^{e-i-1}p^{m-i-1}M(q^k-1)/r} \\ &= \prod_{j=0}^{e-1}\prod_{i=0}^{m-1} f_{p,[p^{mj+i}]P}(Q_{e-j-1})^{p^{m-i-1}M(q^k-1)/r} \\ &= \prod_{j=0}^{e-1}\prod_{i=0}^{m-1} f_{p,\widehat{\pi}_{p^i}([p^{mj}]P)}(\pi_{p^{mk-i}}(Q_{e-j-1}))^{(q^k-1)/r}. \end{aligned}$$

Write $\bar{a}(Q,P) = a(Q,P)^M$, $\hat{a}(Q,P) = a(Q',P')^M = a(\psi(Q),\psi(P))^M$ and $\bar{a}^{twist}(P,Q) = a^{twist}(P,Q)^M$. Thus they define new pairings. □

Theorem 3 shows that the ate pairing and the twisted ate pairing on the curve E over $\mathbb{F}_{p^m}$ can be modified as the products of several rational functions with the same Miller loop on the curves $\{E^{(p^i)}\}_{0\leq i<m}$. Next we give the optimal versions of the new pairings in Theorem 3 according to the theory of pairing lattices.

Theorem 4. *Use the notations in Theorem 3. Let s be a primitive (mk)-th root of unity modulo r^2 such that $s \equiv q \pmod{r}$. Let $h \in \mathbb{Z}[t]$ satisfy $h(s) \equiv 0 \pmod{r}$. For $P \in G_1$ and $Q \in G_2$, following the respective assumptions for $\bar{a}, \hat{a}, \bar{a}^{twist}$ of Theorem 3, then*

$$\bar{a}_{s,h}(Q,P) = \Big(\prod_{i=0}^{m-1} f_{s,h,\widehat{\pi}_{p^i}(Q)}\big(\pi_{p^{m-i}}(P)\big)\Big)^{(p^{mk}-1)/r},$$

$$\hat{a}_{s,h}(Q,P) = \Big(\prod_{i=0}^{m-1} f_{s,h,\widehat{\pi}_{p^i}\circ\psi(Q)}\big(\pi_{p^{mk-i}}\circ\psi(P)\big)\Big)^{(p^{mk}-1)/r},$$

$$\bar{a}^{twist}_{s,h}(P,Q) = \Big(\prod_{i=0}^{m-1}\prod_{j=0}^{e-1} f_{s,h,\widehat{\pi}_{p^i}([p^{mj}]P)}\big(\pi_{p^{mk-i}}(Q_{e-j-1})\big)\Big)^{(p^{mk}-1)/r}$$

define pairings, which are nondegenerate if and only if $h(s) \not\equiv 0 \pmod{r^2}$.

There exists an efficiently computable $h \in I^{(1)}$ with $\|h\|_1 = O(r^{1/\varphi(mk)})$. Any $h \in I^{(1)}$ with $a_{s,h} \neq 1$ satisfies $\|h\|_1 \geq r^{1/\varphi(mk)}$.

Proof. Since $f_{s,g+h,R} = f_{s,g,R}f_{s,h,R}$ and $f_{s,hx,R} = f_{s,h,[s]R}$ for $h, g \in I^{(1)}$, it follows that $\bar{a}_{s,g+h} = \bar{a}_{s,g}\bar{a}_{s,h}$, $\hat{a}_{s,g+h} = \hat{a}_{s,g}\hat{a}_{s,h}$, $\bar{a}^{twist}_{s,g+h} = \bar{a}^{twist}_{s,g}\bar{a}^{twist}_{s,h}$, and $\bar{a}_{s,hx} = (\bar{a}_{s,h})^s$, $\hat{a}_{s,hx} = (\hat{a}_{s,h})^s$, $\bar{a}^{twist}_{s,hx} = (\bar{a}^{twist}_{s,h})^s$ for the pairings $\bar{a}_{s,h}$, $\hat{a}_{s,h}$ and $\bar{a}^{twist}_{s,h}$. Let $t^{(i)}_r$ denote the Tate pairing on $E^{(p^i)}[r]$. Since $f_{r,R} = f_{s,r,R}$, we have

$$\bar{a}_{s,r}(Q,P) = \Big(\prod_{i=0}^{m-1} f_{r,\widehat{\pi}_{p^i}(Q)}(\pi_{p^{m-i}}(P))\Big)^{(p^{mk}-1)/r} = \prod_{i=0}^{m-1} t^{(i)}_r(\widehat{\pi}_{p^i}(Q), \pi_{p^{m-i}}(P)).$$

Write $t_i(Q,P) = t^{(i)}_r(\widehat{\pi}_{p^i}(Q), \pi_{p^{m-i}}(P))$, then each $t_i(Q,P)$ is a pairing on $E[r]$. As with the proof of Theorem 3, we have $f_{r,[p^i]Q}(P) = f_{r,\widehat{\pi}_{p^i}(Q)}(\pi_{p^{m-i}}(P))^{p^i}$, and furthermore $t([p^i]Q,P) = t_i(Q,P)^{p^i}$. Thus $\bar{a}_{s,r}(Q,P) = t_r(Q,P)^m$ is a pairing on $E[r]$.

Let $c \in \mathbb{Z}$ satisfy $s = p + cr$ and let $c_0 \in \mathbb{Z}$ satisfy $p^{mk} \equiv 1 + c_0 r \pmod{r^2}$, then $s^{mk} = (p+cr)^{mk} \equiv 1 + c_0 r + mkp^{mk-1}cr \equiv 1 \pmod{r^2}$. Thus $c_0 \equiv -mkp^{mk-1}c \pmod{r}$. We know that $a(Q,P)^{kp^{m(k-1)}} = t_r(Q,P)^{c_0}$ in [22]. From the proof Theorem 3, we have $\bar{a}(Q,P)^{p^{m-1}} = a(Q,P) = t_r(Q,P)^{-mp^{m-1}c}$. We conclude that $\bar{a}_{s,x-s}(Q,P)^{-1} = \bar{a}_{s,s-x}(Q,P) = \bar{a}(Q,P)\bar{a}_{s,r}(Q,P)^c = 1$.

Similarly, it can be demonstrated that $\hat{a}_{s,x-s}(P,Q) = 1$, $\bar{a}^{twist}_{s,x-s}(P,Q) = 1$, and $\hat{a}_{s,r}(Q,P) = t(Q',P')^m$, $\bar{a}^{twist}_{s,r}(P,Q) = t(P,Q)^{me}$ are pairings.

From Theorem 1, we conclude that for every h satisfying the conditions, $\bar{a}_{s,h}$, $\hat{a}_{s,r}$, and $\bar{a}^{twist}_{s,h}$ are nondegenerate if and only if $h(s) \not\equiv 0 \pmod{r^2}$. □

From Theorem 4, we may construct an optimal h satisfying the conditions of Theorem 4 and $\|h\|_1 = O(r^{1/\varphi(mk)})$ so that each pairing $\bar{a}_{s,h}$, $\hat{a}_{s,h}$ and $\bar{a}^{twist}_{s,h}$ has the optimal multi-Miller loop length $\log_2(r)/\varphi(mk) + \epsilon$, which is smaller than the traditional optimal loop length. We name these pairings the optimal $\bar{a}_{s,h}$, $\hat{a}_{s,h}$ and $\bar{a}^{twist}_{s,h}$. However, the implementations of these pairings involve the calculations of $\widehat{\pi}_{p^i}(R)$ and $\pi_{p^j}(R')$ for some R and R'. In practice, the implementation of the Frobenius power costs little, but the implementation of the dual Frobenius isogeny (also called Verschiebung) might be costly. We introduce skills to perform this costly calculation in Section 4.

Explanation and extension of Sakemi's method. In [30], Sakemi *et al.* proposed a variant of the twisted ate pairing on the BN curves with $e = 2$ (and $m = 1$ in the setting of this paper), whose pairing function is given as

$$\begin{aligned}\hat{f}_{\chi,P}(Q) = \big(f_{2\chi,P}(\pi_p(Q))f_{2\chi,[p]P}(Q)\big)^{p^{10}+1}\big(l_{[2\chi]P,-P}(\pi_p(Q))l_{[2\chi p]P,[-p]P}(Q)\big)^{p^{10}}\\ \cdot l_{[(2\chi-1)p^{10}]P,[2\chi]P}(\pi_p(Q))l_{[(2\chi-1)p^{11}]P,[2\chi p]P}(Q).\end{aligned}$$

Using the method of this paper and the property of the twisted ate pairing [22], we conclude that $f_{T,[p^{je}]P}(Q) = f_{T,P}(Q)^{p^{je}}$ for any $T \in \mathbb{Z}$ and $j \geq 1$, and then choose $\hat{h}(t) = (2\chi-1)t^{10} - t + 2\chi$ to transform the pairing function of $\bar{a}^{twist}_{s,\hat{h}}$ in Theorem 4 under the final exponentiation (using subfield elimination) as follows.

$$\begin{aligned}&f_{s,\hat{h},P}(\pi_p(Q))f_{s,\hat{h},[p]P}(Q)\\ \equiv &\prod_{i=0,1} f_{2\chi-1,[p^{10+i}]P}(\pi_{p^{1-i}}(Q))f_{2\chi,[p^i]P}(\pi_{p^{1-i}}(Q))l_{[(2\chi-1)p^{10+i}]P,[2\chi p^i]P}(\pi_{p^{1-i}}(Q))\\ \equiv &\prod_{i=0,1} \big(f_{2\chi,[p^i]P}(\pi_{p^{1-i}}(Q))f_{[2\chi]P,-P}(\pi_{p^{1-i}}(Q))\big)^{p^{10}} \cdot f_{2\chi,[p^i]P}(\pi_{p^{1-i}}(Q))\\ &\cdot l_{[(2\chi-1)p^{10+i}]P,[2\chi p^i]P}(\pi_{p^{1-i}}(Q))\\ = &\hat{f}_{\chi,P}(Q).\end{aligned}$$

As a further extension, we utilize $h(t) = t^3 - t^2 + t + 6\chi + 2$, originally used for the optimal ate pairing on the BN curves in [33], to obtain another variant as

$$\begin{aligned}&f_{s,h,P}(\pi_p(Q))f_{s,h,[p]P}(Q)\\ \equiv &\prod_{i=0,1} f_{6\chi+2,[p^i]P}(\pi_{p^{1-i}}(Q))\big(l_{[p^{3+i}]P,[-p^{2+i}]P}l_{[p^{3+i}-p^{2+i}]P,[p^{1+i}]P}\big)(\pi_{p^{1-i}}(Q)).\end{aligned}$$

The linear part of the above pairing function of $\bar{a}^{twist}_{s,h}(P,Q)$ is calculated efficiently by using the skew Frobenius map $\tilde{\pi}_{p^2}$ as in [30] and the new congruence $(1-2\chi)p^2-p+4\chi-1 \equiv 0$, and the hard part can be carried out by $[p^2]P = \tilde{\pi}_{p^2}(P)$, $[p^4]P = \tilde{\pi}^2_{p^2}(P)$, $[p]P = [4\chi-1]P - \tilde{\pi}_{p^2}([(2\chi-1)]P)$, $[p^3]P = \tilde{\pi}_{p^2}([p]P)$.

4 Comparison

In this section we make a theoretical comparison between the optimal pairings in the pairing lattices in Theorem 4 and the optimal ate pairing and optimal twisted ate pairing, which depends on the assumptions of the existence of the optimal pairings for all pairing lattices and the existence of the pairing-friendly curves over extension fields.

Following the analysis in [19], we assume that $\mathbb{F}_{p^{mk}}$ is a pairing-friendly field with $p^m \equiv 1 \pmod{12}$ and $k = 2^i 3^j$, and quantify the cost of a multiplication in $\mathbb{F}_{p^{mk}}$ as $3^i 5^j$ multiplications in $\mathbb{F}_{p^m}$ (cf. [25]). In implementation, the loop parameter usually has a negligible Hamming weight so that few addition steps are encountered throughout the loop. Thus we only compare the operation counts for the doubling steps in Miller's algorithm. We list the up-to-date known results [7] of operation counts for the doubling step in Table 1.

Let $\mathbf{m}_1$, $\mathbf{m}_e$, $\mathbf{m}_k$ denote multiplication in $\mathbb{F}_q$, $\mathbb{F}_{q^e}$, $\mathbb{F}_{q^k}$; let $\mathbf{s}_1$, $\mathbf{s}_e$, $\mathbf{s}_k$ denote squaring in $\mathbb{F}_q$, $\mathbb{F}_{q^e}$, $\mathbb{F}_{q^k}$. The cost part 1 is taken to update the point used for constructing the new rational function; the cost part 2 is taken to evaluate the new rational function at the right argument; then the cost part 3 is taken to update the final rational function.

	Curve & twist degree	Cost part 1	Cost part 2	Cost part 3
ate	$y^2 = x^3 + ax,\ d = 2, 4$	$2\mathbf{m}_e + 8\mathbf{s}_e + 1\mathbf{d}_a$	$2(\frac{k}{d})\mathbf{m}_1$	$1\mathbf{m}_k + 1\mathbf{s}_k$
$a(Q', P')$	$y^2 = x^3 + b,\ d = 2, 6$	$2\mathbf{m}_e + 7\mathbf{s}_e + 1\mathbf{d}_b$		
twisted ate	$y^2 = x^3 + ax,\ d = 2, 4$	$2\mathbf{m}_1 + 8\mathbf{s}_1 + 1\mathbf{d}_a$	$2(\frac{k}{d})\mathbf{m}_1$	$1\mathbf{m}_k + 1\mathbf{s}_k$
$a^{twist}(P, Q)$	$y^2 = x^3 + b,\ d = 2, 6$	$2\mathbf{m}_1 + 7\mathbf{s}_1 + 1\mathbf{d}_b$		

Table 1. Operation counts for single doubling step for the ate pairing and the twisted ate pairing.

Since the multi-pairing technique can save $m - 1$ squarings (using 2-basis) in each iteration when computing the products of m pairings (or functions with the same Miller loop), it follows that it is less efficient for the ate-like pairing computation compared with the twisted ate-like case. However, when the high-degree twist technique in [7] is available, the ate-like pairing computation can be still more efficient with the multi-pairing technique. Thus we assume that E admits a high-degree twist, and both the optimal ate pairing and twisted ate pairing have the loop length $\lceil \log_2(r)/\varphi(k) \rceil$, and both the optimal $\hat{a}_{s,h}$ and $\bar{a}_{s,h}^{twist}$ have the loop length $\lceil \log_2(r)/\varphi(mk) \rceil$. We show that the optimal $\hat{a}_{s,h}$ and $\bar{a}_{s,h}^{twist}$ could be implemented more efficient than the optimal ate pairing and the optimal twisted ate pairing when choosing suitable values of m and k in §2.3.

Precomputation vs. storage. The calculation of pairings in Theorem 4 involves the calculation of $\widehat{\pi}_{p^i}(R)$ for $R \in E(\mathbb{F}_{p^{mk}})$ and $1 \leq i < m$. As far as we know, there is no efficient method to calculate the dual Frobenius isogeny on the general curves. Here we rewrite $\widehat{\pi}_{p^i}(R) = \pi_{p^{mk-i}}([p^i]R)$ by using $\widehat{\pi}_{p^i} \circ \pi_{p^i} = [p^i]$ and $\pi_{p^{mk}}(R) = R$. Thus the costly part of this calculation is the multiplication by p^i. We introduce two skills to deal with it. One named the precomputation skill

(P) utilizes the fixed argument optimization first pointed out by Scott [31] and recently analyzed in more detail (cf. [8, 32]); the other named the storage skill (S) is proposed in this paper for computing our new pairings.

The first skill can be applied to many protocols in which the fixed argument optimization is feasible. With the fixed argument optimization, we can precompute all calculations depending solely on the lift argument R including the calculations of all $\{\widehat{\pi}_{p^i}(R)\}_{1\leq i<m}$. Hence, in each Miller iteration, the operations for the doubling step only involve the cost part 2 and the cost part 3 in Table 1. Besides, in this situation, there is no advantage of using a pairing-friendly curve with the maximal twist, and calculating a pairing in the twisted ate pairing family.

When the fixed argument optimization is infeasible, the precomputation is useless. But we could still store these calculations depending solely on the lift argument in each pairing computation, which are useful for the calculations of $\widehat{\pi}_{p^i}(R)$, and then we do the other calculations depending on the right argument. Taking the pairing $\bar{a}(Q,P)$ in Theorem 3 for example, we assume that $\widehat{\pi}_{p^i}(Q)$ is given for some $i\in[1,m-2]$. Then the calculation of the coefficients of $f_{p,\widehat{\pi}_{p^i}(Q)}$ involves $[p]\widehat{\pi}_{p^i}(Q) = \pi_{p^{mk-i}}([p^{i+1}]Q) = \pi_p(\widehat{\pi}_{p^{i+1}}(Q))$. Thus we can compute $\widehat{\pi}_{p^{i+1}}(Q)$ easily by using $\pi_{p^{mk-1}}([p]\widehat{\pi}_{p^i}(Q)) = \widehat{\pi}_{p^{i+1}}(Q)$, which is essential to the construction of $f_{p,\widehat{\pi}_{p^{i+1}}(Q)}$. This process only increases a few costs for implementing the Frobenius power, and needs the same additional memory compared with the precomputation skill which may be feasible in modern devices. Hence, we may omit the calculations of $\widehat{\pi}_{p^i}(R)$ when using our storage skill, and then give the comparisons below.

Optimal ate pairing vs. optimal $\hat{a}_{s,h}$. In Table 2 we make a theoretical implementation comparison between the optimal ate pairing and the optimal $\hat{a}_{s,h}$ for some suitable embedding degrees and extension degrees, when ignoring the final exponentiation and using the precomputation skill or the storage skill. Table 2 shows that the implementation of the optimal $\hat{a}_{s,h}$ improves the runtime cost of the Miller iterations by between 30% and 43% when using the precomputation skill, and between 14% and 34% when using the storage skill.

	Skill	$k=8$	$k=12$	$k=16$	$k=18$	$k=24$	$k=32$	$k=36$
		$d=4$	$d=6$	$d=4$	$d=6$	$d=6$	$d=4$	$d=6$
$m=7$	S	$1:0.860$	$1:0.795$	—	$1:0.794$	—	—	—
	P	$1:0.701$	$1:0.688$	—	$1:0.686$	—	—	—
$m=8$	S	$1:0.732$	$1:0.675$	$1:0.727$	$1:0.673$	$1:0.671$	$1:0.725$	$1:0.670$
	P	$1:0.593$	$1:0.581$	$1:0.583$	$1:0.579$	$1:0.575$	$1:0.576$	$1:0.574$
$m=9$	S	—	$1:0.669$	—	$1:0.668$	$1:0.666$	—	$1:0.665$
	P	—	$1:0.574$	—	$1:0.573$	$1:0.568$	—	$1:0.567$
$m=11$	S	$1:0.793$	$1:0.728$	$1:0.789$	$1:0.727$	$1:0.724$	—	—
	P	$1:0.669$	$1:0.621$	$1:0.623$	$1:0.619$	$1:0.614$	—	—

Table 2. The proportion of the runtime cost of the Miller loop of the optimal ate pairing to the optimal $\hat{a}_{s,h}$.

Optimal twisted ate pairing vs. optimal $\bar{a}^{twist}_{s,h}$*.* Since the fixed argument technique is mainly used for pairings of the ate family in practice, we only compare the theoretical implementation of the optimal twisted ate pairing with the optimal $\hat{a}^{twist}_{s,h}$ for some suitable embedding degrees and extension degrees, by using the storage skill and ignoring the final exponentiation. Table 3 shows that the implementation of the optimal $\bar{a}^{twist}_{s,h}$ improves the runtime cost of the Miller iterations by between 26% and 47%.

	Skill	$k = 8$	$k = 12$	$k = 16$	$k = 18$	$k = 24$	$k = 32$	$k = 36$
		$d = 4$	$d = 6$	$d = 4$	$d = 6$	$d = 6$	$d = 4$	$d = 6$
$m = 7$	S	$1 : 0.736$	$1 : 0.693$	—	$1 : 0.662$	—	—	—
$m = 8$	S	$1 : 0.628$	$1 : 0.590$	$1 : 0.564$	$1 : 0.564$	$1 : 0.544$	$1 : 0.533$	$1 : 0.532$
$m = 9$	S	—	$1 : 0.587$	—	$1 : 0.562$	$1 : 0.543$	—	$1 : 0.531$
$m = 11$	S	$1 : 0.683$	$1 : 0.641$	$1 : 0.616$	$1 : 0.615$	$1 : 0.594$	—	—

Table 3. The proportion of the runtime cost of the Miller loop of the optimal twisted ate pairing to the optimal $\bar{a}^{twist}_{s,h}$.

5 Our Method for Supersingular Curve over Extension Field

As the earliest pairing-friendly curves utilized in pairing-based cryptography, supersingular curves have embedding degree $k = 2, 3, 4$ and 6. However, for the recommended supersingular pairing-friendly curves with $k = 4$ and 6, there are two obstacles to applying our method: (1) their defining fields $\mathbb{F}_{2^n}$ and $\mathbb{F}_{3^n}$ usually have large prime extension degrees; (2) the main advantage of applying multi-pairing technique, namely saving squarings (using 2-basis) or cubings (using 3-basis) in each iteration, might be worthless for these supersingular curves, since squaring or cubing can be implemented very fast.

But recently, Estibals [11] first considered the Tate pairing computation for supersingular curves over moderately-composite extension fields taking advantage of a much easier tower field arithmetic. Our method can be applied to Estibals's curves over composite extension fields to define new pairings $\bar{\eta}_{s,h}$, which can be implemented in an efficient and parallel way.

Theorem 5. *Let E be a supersingular curve over a composite extension field $\mathbb{F}_{q^m}$ with the embedding degree k. Let r be a large integer dividing $|E(\mathbb{F}_{q^m})|$ and let ψ be the distortion map. Let s be a primitive (mk)-th root of unity modulo r^2 such that $s \equiv q \pmod{r}$. Let $h(t) \in \mathbb{Z}[t]$ such that $h(s) \equiv 0 \pmod{r}$. For $P, Q \in E(\mathbb{F}_{q^m})[r]$, then*

$$\bar{\eta}_{s,h}(P, Q) = \left(\prod_{i=0}^{m-1} f_{s,h,P}\Big(\psi([q^{-i}]Q)\Big)^{q^i} \right)^{(q^{mk}-1)/r}.$$

defines a pairing, which is non-degenerate if and only if $h(s) \not\equiv 0 \pmod{r^2}$.

Proof. Given in Appendix A. □

Write $f_i(P,Q) = f_{s,h,P}\big(\psi([q^{-i}]Q)\big)^{p^i}$, then $\bar{\eta}_{s,h}(P,Q) = \prod_{i=0}^{m-1} f_i(P,Q)^{(q^{mk}-1)/r}$. When precomputing all $[q^{-i}]Q$ for $1 \leq i \leq m-1$, we could compute these $f_i(P,Q)$ in a natural parallel and efficient way, since they share the common pairing function $f_{s,h,P}$ whose coefficients could be computed and stored first.

5.1 Estibals's Supersingular Curve over Composite Extension Field

There are several supersingular curves of characteristic 2 and 3 on fields with composite extension degree large enough for the 128-bit or 192-bit security level given in [11]. Here, we take two most important curves $E_1(\mathbb{F}_{3^{5\times97}})$ (128-bit security level) and $E_2(\mathbb{F}_{3^{17\times67}})$ (192-bit security level) for example to construct the corresponding $\bar{\eta}_{s,h}$.

- $E_1(\mathbb{F}_{3^{5\times97}}) : y^2 = x^3 - x - 1, \quad (q_1 = 3^{97}, m_1 = 5, k = 6)$
  $r_1 = 434A97AFECDEB84F16624099C436CA9DE0CE4526690A8F0B24$
  $09B61DACB97A4411F3ED1CD3F39A6647D45$ (338 *bits*)
- $E_2(\mathbb{F}_{3^{17\times67}}) : y^2 = x^3 - x + 1, \quad (q_2 = 3^{67}, m_2 = 17, k = 6)$
  $r_2 = 4A40FE5A48A1956BEEEC98D0147445A190711D0FCA4FCD5A65$
  $598194911D4D9F5D32156CAB3B4C9D53D02B3793E8AA2B1BAD8383$
  $2815DABA55EE9A2CD28A38027D2EB2FD0B6E4BEFD03DA273CD$
  $DDC19A1507E36281BC212F28F78EA379AEE4A3353C8348E13F5890D$
  $AA8367040520FC04B2E073193BE13922CEA13F106C9D8A8FE546D2F$
  $27FE2FBEE373F79B198FC7F1A3FB5594FE97B2D6EE6ADA84E6D$
  $726A709370D86FEEFAFD20300BFBD72B4F162A26C70F9F1927AB6$
  $6111B1FD5E7C1197AAEDD81776BFE079449A11A1AC849$ (1650 *bits*)

Using the method of [21] (or [33]) to construct the $\varphi(mk)$ dimensional lattice $L = I^{(1)} = \{h(t)|h(s) \equiv 0 \pmod{r}\}$, we find a approximative "short vector" of the polynomial form $h_1(t) = t^5 + c_1t^2 + 1$ with $c_1 = 3^{49}$ for $E_1(\mathbb{F}_{3^{5\times97}})$; and, $h_2(t) = t^{17} + c_2t^8 + 1$ with $c_2 = 3^{34}$ for $E_2(\mathbb{F}_{3^{17\times67}})$. Form the theory of pairing lattice, it follows that

$$f_{s_1,h_1,P_1} = f_{c_1,P_1}\frac{l_{[q_1^{m_1}]P_1,[-q_1^{m_1}-1]P_1}l_{-P_1,P_1}}{v_{-P_1}},$$
$$f_{s_2,h_2,P_2} = f_{c_2,P_2}\frac{l_{[q_2^{m_2}]P_2,[-q_2^{m_2}-1]P_2}l_{-P_2,P_2}}{v_{-P_2}},$$

where $P_i \in E_i(\mathbb{F}_{q_i^{m_i}})[r_i]$ and $s_i \equiv q_i \pmod{r_i}$ for $i = 0, 1$. We note that the calculations of $[q_i^{m_i}]P_i$ and $[-q_i^{m_i} - 1]P_i$ are very fast by using Frobenius map $\pi_{q_i^{m_i}}$ and the trace equation. Thus, assuming that m_i multiprocessors ($i = 1, 2$) perform in parallel, the Miller's loop length of $\bar{\eta}_{s_i,h_i}$ for $E_i[r_i]$ can reach an small value $\log_3(c_i)$, although which is still a little worse than the theoretical minimal length $\log_3(r)/\varphi(mk)$, when using 3-basis in Miller algorithm. Further, with Estibals's compact hardware implementation of these fields arithmetic, we believe that our pairing $\bar{\eta}_{s,h}$ would be implemented at much higher speed in parallel way.

6 Conclusion

We have shown that pairing-friendly curves over extension fields could be more suitable for the pairing implementation not relying on a fast field arithmetic of certain extension field. When assuming there exists a pairing-friendly curve defined over an extension field, we have proposed new pairings and pairing lattices on this curve making better use of the multi-pairing technique to obtain a fast implementation. By the theoretical analysis in an ideal model, the performance of the optimal ones of our pairings could offer a speed up of between 30% and 43% with the fixed argument optimization, or by up to 47% with our new storage skill, compared to the performance of the optimal ate pairing and the optimal twisted ate pairing, when m is greater than 6. In addition, we have extended the similar method to supersingular curves over composite extension fields to construct more efficient pairings in parallel implementation. To sum up, our work has presented further important evidence of the advantage of pairing-friendly curves over extension fields.

In future, there are needs for careful study of the generation of pairing-friendly curves over suitably chosen extension fields, and further study of the parallel implementation of $\bar{\eta}_{s,h}$ on Estibals's supersingular curves $E_1(\mathbb{F}_{3^{5\times 97}})$ and $E_2(\mathbb{F}_{3^{17\times 67}})$.

Acknowledgments

This work is supported by the National 973 Program of China under Grant 2011CB302400, the National Natural Science Foundation of China under Grant 60970152 and 60970153, the Grand Project of Institute of Software under Grant YOCX285056. We are heartily grateful to the anonymous reviewers for their helpful and insightful comments and suggestions.

References

1. D. Bailey and C. Paar. Optimal extension fields for fast arithmetic in public-key algorithms. In *CRYPTO'98, LNCS 1462*, pages 472–485. Springer, 1998.
2. D.V. Bailey and C. Paar. Efficient arithmetic in finite field extensions with application in elliptic curve cryptography. *Journal of cryptology*, 14(3):153–176, 2001.
3. J.C. Bajard, L. Imbert, C. Negre, and T. Plantard. Efficient multiplication in $GF(p^k)$ for elliptic curve cryptography. In *Proceedings. 16th IEEE Symposium on Computer Arithmetic 2003*, pages 181–187. IEEE, 2003.
4. P. Barreto, H. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing-based cryptosystems. In *CRYPTO 2002, LNCS 2442*, pages 354–369. Springer, 2002.
5. P.S.L.M. Barreto, S.D. Galbraith, C.Ó. hÉigeartaigh, and M. Scott. Efficient pairing computation on supersingular abelian varieties. *Designs, Codes and Cryptography*, 42(3):239–271, 2007.
6. N. Benger, M. Charlemagne, and D. Freeman. On the security of pairing-friendly abelian varieties over non-prime fields. In *Pairing 2009, LNCS 5671*, pages 52–65. Springer, 2009.

7. C. Costello, T. Lange, and M. Naehrig. Faster pairing computations on curves with high-degree twists. In *PKC 2010, LNCS 6056*, pages 224–242. Springer, 2010.
8. C. Costello and D. Stebila. Fixed argument pairings. In *LATINCRYPT 2010, LNCS 6212*, pages 92–108. Springer, 2010.
9. C. Diem. The GHS attack in odd characteristic. *J. Ramanujan Math. Soc.*, 18(1):1–32, 2003.
10. C. Diem. On the discrete logarithm problem in elliptic curves. *Compositio Mathematica*, 147(01):75–104, 2011.
11. N. Estibals. Compact Hardware for Computing the Tate Pairing over 128-Bit-Security Supersingular Curves. In *Pairing 2010, LNCS 6487*, pages 397–416. Springer, 2010.
12. D. Freeman, M. Scott, and E. Teske. A Taxonomy of Pairing-Friendly Elliptic Curves. *Journal of Cryptology*, 23(2):224–280, 2010.
13. G. Frey and H. Gangl. How to disguise an elliptic curve (Weil descent). In *Talk at ECC'98*, volume 98, 1998.
14. S. Galbraith, F. Hess, and N. Smart. Extending the GHS Weil descent attack. In *EUROCRYPT 2002, LNCS 2332*, pages 29–44. Springer, 2002.
15. S. Galbraith and N. Smart. A cryptographic application of Weil descent. In *Cryptography and coding 1999, LNCS 1746*, pages 799–799. Springer, 1999.
16. P. Gaudry. Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. *Journal of Symbolic Computation*, 44(12):1690–1702, 2009.
17. P. Gaudry, F. Hess, and N.P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *Journal of Cryptology*, 15(1):19–46, 2002.
18. R. Granger. On the Static Diffie-Hellman Problem on Elliptic Curves over Extension Fields. In *ASIACRYPT 2010, LNCS 6477*, pages 283–302. Springer, 2010.
19. R. Granger and N.P. Smart. On computing products of pairings. Cryptology ePrint Archive Report 2006/172. Preprint available at http://eprint.iacr.org/2006/172, 2006.
20. F. Hess. Generalising the GHS attack on the elliptic curve discrete logarithm problem. *LMS Journal of Computation and Mathematics*, 7(1):167–192, 2004.
21. F. Hess. Pairing Lattices. In *Pairing 2008, LNCS 5209*, pages 18–38. Springer, 2008.
22. F. Hess, N.P. Smart, and F. Vercauteren. The Eta Pairing Revisited. *IEEE Trans. on Information Theory*, 52(10):4595–4602, 2006.
23. L. Hitt. On the minimal embedding field. In *Pairing 2007, LNCS 4575*, pages 294–301. Springer, 2007.
24. A. Joux and V. Vitse. Elliptic Curve Discrete Logarithm Problem over Small Degree Extension Fields. Application to the static Diffie-Hellman problem on $E(\mathbb{F}_{q^5})$. Cryptology ePrint Archive, Report 2010/157. Preprint available at http://eprint.iacr.org/2010/157, 2010.
25. N. Koblitz and A. Menezes. Pairing-Based Cryptography at High Security Levels. In *Cryptography and Coding 2005, LNCS 3796*, pages 13–36. Springer, 2005.
26. E. Lee, H.S. Lee, and C.M. Park. Efficient and generalized pairing computation on abelian varieties. *IEEE Trans. on Information Theory*, 55(4):1793–1803, 2009.
27. C. Lim and H. Hwang. Fast implementation of elliptic curve arithmetic in $GF(p^n)$. In *PKC 2000, LNCS 1751*, pages 405–421. Springer, 2000.
28. A. Menezes and E. Teske. Cryptographic implications of Hess' generalized GHS attack. *Applicable Algebra in Engineering, Communication and Computing*, 16(6):439–460, 2006.

29. V. Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology*, 17(4):235–261, 2004.
30. Y. Sakemi, S. Takeuchi, Y. Nogami, and Y. Morikawa. Accelerating twisted Ate pairing with Frobenius map, small scalar multiplication, and multi-pairing. In *ICISC 2009, LNCS 5984*, pages 47–64. Springer, 2010.
31. M. Scott. Computing the Tate pairing. In *CT-RSA 2005, LNCS 3376*, pages 293–304. Springer, 2005.
32. M. Scott. On the Efficient Implementation of Pairing-Based Protocols. In *Cryptography and Coding 2011, LNCS 7089*, pages 296–308. Springer, 2011.
33. F. Vercauteren. Optimal Pairings. *IEEE Trans. on Information Theory*, 56(1):455–461, 2010.
34. X. Zhang and D. Lin. Efficient Pairing Computation on Ordinary Elliptic Curves of Embedding Degree 1 and 2. In *Cryptography and Coding 2011, LNCS 7089*, pages 309–326. Springer, 2011.

A Proof of Theorem 5

We do the similar reduction as Theorem 3 for the modified Eta pairing to obtain that

$$\eta(P,Q) = f_{q^m,P}\big(\psi(Q)\big)^{(q^{mk}-1)/r} = \left(\prod_{i=0}^{m-1} f_{q,[q^i]P}\big(\psi(Q)\big)^{q^{m-i-1}}\right)^{(q^{mk}-1)/r}.$$

Since the multiplication by q^i on the supersingular curve is inseparable, it follows that $[q^i]^*\mathrm{div}(f_{q,[q^i]P}) = \mathrm{div}(f_{q,P}^{q^{2i}})$ and then $f_{q,[q^i]P}(\psi(Q)) = f_{q,P}(\psi([q^{-i}]Q))^{q^{2i}}$. Thus we have

$$\eta(P,Q) = \left(\prod_{i=0}^{m-1} f_{q,P}\Big(\psi([q^{-i}]Q)\Big)^{q^i}\right)^{q^{m-1}(q^{mk}-1)/r}.$$

Since $\gcd(q,r) = 1$, we can omit the power q^{m-1} to obtain the new pairing

$$\bar{\eta}(P,Q) = \left(\prod_{i=0}^{m-1} f_{q,P}\Big(\psi([q^{-i}]Q)\Big)^{q^i}\right)^{(q^{mk}-1)/r}.$$

Then, as with the proof of Theorem 4, we can construct $\bar{\eta}_{s,h}$ as

$$\bar{\eta}_{s,h}(P,Q) = \left(\prod_{i=0}^{m-1} f_{s,h,P}\Big(\psi([q^{-i}]Q)\Big)^{q^i}\right)^{(q^{mk}-1)/r}.$$

and demonstrate it defines a pairing using Theorem 1 similarly (omitted here).