Twisted Ate Pairing on Hyperelliptic Curves and Applications

Fangguo Zhang[1,2]

[1] School of Information Science and Technology,
Sun Yat-Sen University, Guangzhou 510275, P.R.China
isszhfg@mail.sysu.edu.cn
[2] Guangdong Key Laboratory of Information Security Technology
Guangzhou 510275, P.R.China

Abstract. In this paper we show that the twisted Ate pairing on elliptic curves can be generalized to hyperelliptic curves, we also give a series of variations of the hyperelliptic Ate and twisted Ate pairings. Using the hyperelliptic Ate pairing and twisted Ate pairing, we propose a new approach to speed up the Weil pairing computation, and obtain an interested result: For some hyperelliptic curves with high degree twist, using this approach to compute Weil pairing will be faster than Tate pairing, Ate pairing etc. all known pairings.

Keywords: Ate pairing, Weil pairing, Hyperelliptic curves, pairing-based cryptosystems, Twisting curves.

1 Introduction

In recent years, the bilinear pairings have been found to be very useful in various applications in cryptography and have allowed us to construct new cryptographic primitives. The pairing based cyptosystems became one of the most attractive areas of research in public key cryptography. Pairing computation is a key step in the implementation of pairing based cyptosystems. Much effort was put in developing fast algorithms to compute bilinear pairings.

Most fast algorithms are based on Miller's algorithm [18] to compute the Weil and Tate pairings on elliptic curves. Many efficient algorithms for implementing the pairings on elliptic curves have been proposed [10]. Duursma and Lee [5] firstly gave fast algorithms for implementing the pairings on curves of genus ≥ 2. This paper opened a new line to improve Miller's algorithm: Shortening the loop in Miller's algorithm. Barreto et.al. [1] extended Duursma and Lee's loop shortening idea to supersingular abelian varieties using the η_T approach. In [12], Hess et al. extended the η_T pairing over ordinary curves, and proposed the Ate pairing and twisted Ate pairing. The Miller loop in the two pairings can be reduced to T and T_e respectively, where $T = t-1$ and t is the Frobenius trace of the elliptic curve. More recently, several variants of the Ate pairing were introduced thereby further reducing the loop length in Millers algorithm, such as the optimized Ate pairing [17], the Ate_i pairings[21], the R-ate pairing [15] and finally optimal pairings [20]. Granger et al. [8] generalized the Ate pairing for elliptic curves to ordinary hyperelliptic curves. The hyperelliptic Ate pairing has two good properties: Firstly, the loop length in Millers algorithm for evaluating the pairing function is up to g times shorter than for the corresponding Tate pairing, where g is the genus of the underlying curve C. Secondly, the pairing is automatically reduced, that is, the final exponentiation required by the Tate pairing can be omitted. Even those, Galbraith et al. [11] showed that hyperelliptic curves usually less practical for pairings than elliptic curves.

There are many reasons such that hyperelliptic pairing (including Ate pairing) is not fast than elliptic pairing [11]. For Ate pairing on ordinary elliptic curves, Matsuda et al. [17] showed that the Ate pairing is always at least as fast as the Tate pairing by providing the optimized versions of the Ate and the twisted Ate pairing. However, currently, it seems to be more difficult to generate pairing-friendly non-supersingular genus g curves over $\mathbb{F}_q$. In [6], Freeman proposed the first explicit construction of pairing- friendly genus 2 hyperelliptic curves over prime fields with ordinary Jacobians by modeling on the Cocks-Pinch method for the elliptic curve case. Unfortunately, the parameters for these curves are not very attractive for fast pairing implementation (precisely, the size of r is too small compared with the size of q). In a recent paper [13], Kawazoe and Takahashi presented two different approaches for explicitly constructing pairing- friendly genus 2 curves of the type $y^2 = x^5 + ax$ over $\mathbb{F}_q$. Even Kawazoe et al.'s genus 2 curves satisfy $q \approx r^2$(some one can achieve to $q \approx r^{3/2}$), it is better than Freeman's construction, but the hyperelliptic Ate pairing on these curves is no any advantage than Tate pairing. Granger et al. [8] remained an open problem which whether high degree twists can be utilised for hyperelliptic Ate pairing, Galbraith et al. [11] also mentioned that if the twists of high degree can be exploited, the hyperelliptic pairing maybe have advantage than elliptic curve case.

Since the Tate pairing can be computed more efficiently than the Weil pairing, the researchers have mainly considered the Tate pairing computations. The Weil pairing computation does not need the final exponentiation while it involves two Miller iteration loops. Koblitz et al. [14] found that for very high security levels, such as 192 or 256 bits, the Weil pairing computation is sometimes faster than the Tate pairing. However, Granger et al. [9] showed that the Tate pairing over ordinary elliptic curves is more efficient than the Weil pairing for all security levels.

In this paper we will show that the twisted Ate pairing on elliptic curves can be generalized to hyperelliptic curves, we also give a series of variations of the hyperelliptic Ate and twisted Ate pairings. Using the twisted hyperelliptic curves, we propose a variant of Weil pairing, and obtain an interested result: For some hyperelliptic curves with high degree twist, to compute this variational Weil pairing maybe faster than Tate pairing and Ate or Ate_i pairing.

The rest of this paper is organized as follows. Section 2 introduces some mathematical preliminaries, including hyperelliptic Curves, Tate pairing and Ate pairing on hyperelliptic Curves. Section 3 introduces the theory of twisting hyperelliptic curves and gives some hyperelliptic Curves over prime field with high degree twist. Section 4 generalizes twisted Ate pairing on elliptic curves to hyperelliptic curves and analyzes the efficiency of the computation of them. Section 5 gives a variant of hyperelliptic Weil pairing based on twisted Ate pairings and analyzes its computation cost. Section 6 gives the conclusions.

2 Mathematical Preliminaries

2.1 The Tate-Lichtenbaum Pairing on Hyperelliptic Curves

Let $\overline{\mathbb{F}}_q$ be the algebraic closure of the field $\mathbb{F}_q$. A hyperelliptic curve C of genus g over $\mathbb{F}_q$ with $g \geq 1$ is given by the following equation:

$$C : y^2 + h(x)y = f(x) \tag{1}$$

where $f(x)$ is a monic polynomial of degree $2g+1$, $h(x)$ is a polynomial of degree at most g, and there is no solutions $(x,y) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ simultaneously satisfying the equation $y^2 + h(x)y = f(x)$ and the partial derivative equations $2y + h(x) = 0$ and $h'(x)y - f'(x) = 0$. So, C is an imaginary nonsingular hyperelliptic curve and has only one point P_∞ at infinity.

For any algebraic extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$ consider the set

$$C(\mathbb{F}_{q^k}) := \{(x,y) \in \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} | y^2 + h(x)y = f(x)\} \cup \{P_\infty\},$$

called the set of $\mathbb{F}_{q^k}$-rational points on C.

Let $P = (x, y)$ be a finite point on hyperelliptic curve C, hyperelliptic involution ι of P defined by $\iota(P) = (x,\ -y - h(x))$, $\iota(P_\infty) = P_\infty$. The set $C(\mathbb{F}_{q^k})$ for $g \geq 2$ does not form a group, but we can embed C into an abelian variety of dimension g called the Jacobian of C and denoted by J_C which isomorphic to the divisor class group of degree zero Pic_C^0. The Jacobian of C defined over $\mathbb{F}_{q^k}$ is given by $J_C(\mathbb{F}_{q^k})$ that is isomorphic to the divisor class group of degree zero $Pic_C^0(\mathbb{F}_{q^k})$ od C over $\mathbb{F}_{q^k}$. Let $\mathcal{O}$ be the identity of J_C.

We fix a subgroup of $J_C(\mathbb{F}_q)$ of some order r. We say that this subgroup has embedding degree k if the order r divides $q^k - 1$, but does not divide $q^i - 1$ for any $0 < i < k$. This implies that the $r-$th roots of unity μ_r are contained in $\mathbb{F}_{q^k}$ and in no strictly smaller extension of $\mathbb{F}_q$. For cryptographic application, r should be a (large) prime with $r | \# J_C(\mathbb{F}_q)$ and $\gcd(r, q) = 1$. Let $J_C(\mathbb{F}_{q^k})[r]$ be the r-torsion group and $J_C(\mathbb{F}_{q^k})/rJ_C(\mathbb{F}_{q^k})$ be the quotient group. Then the Tate-Lichtenbaum pairing is a well defined, non-degenerate, bilinear pairing [7]

$$\langle \cdot, \cdot \rangle_r : \; J_C(\mathbb{F}_{q^k})[r] \times J_C(\mathbb{F}_{q^k})/rJ_C(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r,$$

defined as follows: let $\overline{D}_1 \in J_C(\mathbb{F}_{q^k})[r]$ and $\overline{D}_2 \in J_C(\mathbb{F}_{q^k})$ and let $\overline{D}_1$ be represented by a divisor D_1 and $\overline{D}_2$ by a divisor D_2 with $supp(D_1) \cap supp(D_2) = \emptyset$. There is a rational function $f_{r,D_1} \in \mathbb{F}_{q^k}(C)$ such that $div(f_{r,D_1}) = rD_1 - [r]D_1 = rD_1$. The Tate-Lichtenbaum pairing of two divisor classes $\overline{D}_1$ and $\overline{D}_2$ is then defined as

$$\langle \overline{D}_1, \overline{D}_2 \rangle_r = f_{r,D_1}(D_2) = \prod_{P \in C(\overline{\mathbb{F}}_q)} f_{r,D_1}(P)^{\mathrm{ord}_P(D_2)},$$

Note that the pairing as detailed above is only defined up to r-th powers. In practice, many pairing-based protocols require a unique pairing value instead of a whole coset. Hence one defines the reduced pairing as

$$e(\overline{D}_1, \overline{D}_2) = \langle \overline{D}_1, \overline{D}_2 \rangle_r^{(q^k-1)/r} \in \mu_r \subset \mathbb{F}_{q^k}^*$$

The reduced pairing has an important property: for any positive integer N with $r|N$ and $N|q^k - 1$, we have

$$e(\overline{D}_1, \overline{D}_2) = \langle \overline{D}_1, \overline{D}_2 \rangle_r^{(q^k-1)/r} = \langle \overline{D}_1, \overline{D}_2 \rangle_N^{(q^k-1)/N}$$

2.2 Miller's Algorithm

The main task in computation of $\langle \cdot, \cdot \rangle_r$ is constructing the rational function f_{r,D_1} and evaluating $f_{r,D_1}(D_2)$ with $div(f_{r,D_1}) = rD_1$ for divisors D_1 and D_2. Miller described a fast algorithm to compute evaluations of $f_{r,D_1}(D_2)$ for divisors on elliptic curves in [18]. The algorithm can be also adapted to compute the pairing on hyperelliptic curves.

Let G_{iD_1,jD_1} be a rational function with

$$div(G_{iD_1,jD_1}) = iD_1 + jD_1 - (iD_1 \oplus jD_1)$$

where $\oplus$ is the group law on J_C and $(iD_1 \oplus jD_1)$ is reduced. Miller's algorithm constructs the rational function f_{r,D_1} based on the following iterative formula:

$$f_{i+j,D_1} = f_{i,D_1} f_{j,D_1} G_{iD_1,jD_1}.$$

Miller's algorithm is described in Algorithm 1. For the detailed version of Miller's algorithm for hyperelliptic curves, please refer to [8].

Algorithm 1 Miller's Algorithm for Hyperelliptic Curves

Input: $r = \sum_{i=0}^{n} l_i 2^i$, where $l_i \in \{0,1\}$. $\overline{D}_1 \in J_C(\mathbb{F}_{q^k})[r]$, $\overline{D}_2 \in J_C(\mathbb{F}_{q^k})$ represented by D_1 and D_2 with $supp(D_1) \cap supp(D_2) = \emptyset$.
Output: $f_{r,D_1}(D_2)$
1. $T \leftarrow D_1$, $f \leftarrow 1$
2. for $i = n-1, n-2, ..., 1, 0$ do
2.1 Compute T' and $G_{T,T}(x,y)$ such that $T' = 2T - div(G_{T,T})$
2.2 $f \leftarrow f^2 \cdot G_{T,T}(D_2)$, $\overline{T} \leftarrow [2]\overline{T}$
2.3 if $l_i = 1$ then
2.4 Compute T' and $G_{T,D_1}(x,y)$ such that $T' = T + D_1 - div(G_{T,D_1})$
2.4 $f \leftarrow f \cdot G_{T,D_1}(D_2)$, $\overline{T} \leftarrow \overline{T} \oplus \overline{D}_1$
3. return f

2.3 Ate Pairing on Hyperelliptic Curves

An important improving technique in pairing computation is reducing the iteration loops in Miller's algorithm. The Ate pairing on ordinary elliptic curves by Hess et al. [12], which is a generalization of Eta pairing, can be computed using only $\log_2 r/\varphi(k)$ basic Miller iterations. Granger et al. [8] generalized the Ate pairing for elliptic curves to ordinary hyperelliptic curves.

Let π be the q-power Frobenius map on C and Frobenius endomorphism on J_C and define $\rho(\overline{D})$ the unique reduced divisor in $\overline{D}$. We have the following theorem:

Theorem 1 ([8]). *Let C be a hyperelliptic curve over $\mathbb{F}_q$ and $r|\#J_C(\mathbb{F}_q)$ a large prime. Let $\mathbb{G}_1 = J_C[r] \cap Ker(\pi - [1])$ and $\mathbb{G}_2 = J_C[r] \cap Ker(\pi - [q])$, then*

$$a(\cdot,\cdot) : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r : (\overline{D}_2, \overline{D}_1) \to f_{q,D_2}(D_1)$$

with $D_2 = \rho(\overline{D}_2)$ and $D_1 \in \overline{D}_1$ such that $supp(D_1) \cap supp(D_2) = \emptyset$, defines a non-degenerate, bilinear pairing called the hyperelliptic Ate pairing. Furthermore, the relation with the reduced Tate-Lichtenbaum pairing is as follows:

$$e(\overline{D}_2, \overline{D}_1) = a(\overline{D}_2, \overline{D}_1)^{kq^{k-1}}.$$

The most important property of the Ate pairings is that no final exponentiation is necessary.

3 Twisting Hyperelliptic Curves

Let C be a curve with genus g defined over a field K. A curve C' over K that is isomorphic to C, is called a twist of C. Furthermore, we call C' is a twist of degree

d of C if there exists an isomorphism $\phi : C' \to C$ defined over K_d, here K_d is a d-th algebraic extension of K and d is minimal. For every curve C defined over a field K, the set of its twists $\mathrm{Twist}(C/K)$ is the set of K-isomorphism classes of curves C'/K that are K-isomorphic to C. As discussed in Theorem 2.2 of [19], there is a bijection between $\mathrm{Twist}(C/K)$ and the cohomology set $H^1(G_K, Aut(C))$. In other words, the twists of C/K (up to K-ismorphism) are in one-to-one correspondence with the elements of the cohomology set $H^1(G_K, Aut(C))$. Here G_K is the Galois group of an algebraic closure $\overline{K}/K$.

This bijection give us a way to construct the twist curve of given curve C: Consider the map

$$\xi : G_K \to Aut(C) \text{ defined by } \xi(\sigma) = \phi^\sigma \phi^{-1}.$$

It turns out that $\xi(\sigma)$ is a 1-cocycle, that is, it satisfies the equality $\xi_{\sigma\tau} = (\xi_\sigma)^\tau \xi_\tau$ (here $\sigma, \tau \in G_K$). Then the cohomology class of ξ is uniquely determined by the K-isomorphism class of C. For more detail, see [19, Theorem X.2.2]

To construct the twist curve of given curve C over a field K, we should compute the automorphisms group $Aut(C)$ of C. For the hyperelliptic curve C, and any finite field, the $Aut(C)$ and $H^1(G_K, Aut(C))$ can be computed using Magma [16]. For curves C/K of genus 2 given by hyperelliptic equations, the possible reduced groups of automorphisms were determined by Bolza in terms of their invariants [2, pag. 70], and the structure of the corresponding groups can be found in [3]. The picture, outside from characteristics 2, 3 and 5, is the following: the group $Aut(C)$ is isomorphic to one of the groups

$$C_2, V_4, D_8, D_{12}, 2D_{12}, \widetilde{S}_4, C_{10}.$$

Here C_n denotes the cyclic group of order n, V_4 is the Klein 4-group, D_n is the dihedral group of order n, and $2D_{12}, \widetilde{S}_4$ are certain 2-coverings of the dihedral and symmetric groups D_{12} and S_4, respectively. These groups can be identified with a subgroup of $GL_2(K)$ which is closed by the Galois action of the group G_K. Based on this, Cardona [3] computed the number of curves of genus 2 defined over a finite field K of odd characteristic up to isomorphisms defined over K.

The degree d of the twist of a curve C depends on the order of the element of $Aut(C)$, i.e., if C' is a degree d twist of C, then $Aut(C)$ must contain an element of order d. However, if $Char(K) > 5$, $Aut(C)$ always is a subgroup of one of $C_2, V_4, D_8, D_{12}, 2D_{12}, \widetilde{S}_4, C_{10}$. So for $Char(K) > 5$, only $d = 1, 2, 3, 4, 5, 6, 8, 10$ are possible. Therefor, for the curves of genus 2, the highest degree of twist is 10, and then is 8.

For the cryptographic application, we only concern the high degree twist. So, we can consider the curves of genus 2 with group of automorphisms isomorphic to $\widetilde{S}_4$ and C_{10}. For a finite field $\mathbb{F}_q$, here q is a large prime and $q = 1 \mod 8$, the curve of form

$$C_1 : \; y^2 = x^5 + ax$$

has automorphisms group $C_8 \subset \widetilde{S}_4$. We can construct a degree 8 twist of C_1.

$$d = 8: \ C_1' : y^2 = x^5 + a\lambda x, \ (x, y) \to (\lambda^{\frac{1}{4}} x, \lambda^{\frac{5}{8}} y)$$

Here $\lambda \in \mathbb{F}_q$ is not l-th power residue in $\mathbb{F}_q$, for $l \in \{1, 2, 4, 8\}$.

For a finite field $\mathbb{F}_q$, here $q = 1 \mod 5$, the curve of form

$$C_2: \ y^2 = x^5 + a$$

has automorphisms group C_{10}. We can construct a degree 10 twist of C_2.

$$d = 10: \ C_2' : y^2 = x^5 + a\lambda, \ (x, y) \to (\lambda^{\frac{1}{5}} x, \lambda^{\frac{1}{2}} y)$$

Here $\lambda \in \mathbb{F}_q$ is not l-th power residue in $\mathbb{F}_q$, for $l \in \{1, 2, 5, 10\}$.

If we want to get higher than 10 degree twist, we should use larger g. For example, when $g = 3$, for the type hyperelliptic curve:

$$y^2 = x^7 + a$$

we can get a twist with degree 14 over $\mathbb{F}_q$ (here $q = 1 \mod 7$):

$$y^2 = x^7 + a\lambda, \ (x, y) \to (\lambda^{\frac{1}{7}} x, \lambda^{\frac{1}{2}} y)$$

When $g = 4$, for the type hyperelliptic curve:

$$y^2 = x^9 + ax$$

we can get a twist with degree 16 over $\mathbb{F}_q$ (here $q = 1 \mod 16$):

$$y^2 = x^9 + a\lambda x, \ (x, y) \to (\lambda^{\frac{1}{8}} x, \lambda^{\frac{9}{16}} y)$$

4 Twisted Hyperelliptic Ate Pairing

The hyperelliptic Ate pairing is defined on $\mathbb{G}_2 \times \mathbb{G}_1$, here $\mathbb{G}_2$ was defined as $\mathbb{G}_2 = J_C[r] \cap \mathrm{Ker}(\pi - [q])$, i.e., the q-eigenspace of Frobenius on $J_C[r]$. The operations in $\mathbb{G}_2$ are performed over $\mathbb{F}_{q^k}$. As elliptic curve case, we want to investigate if we can admit the twist curve to define the hyperelliptic Ate pairing on $\mathbb{G}_1 \times \mathbb{G}_2$.

Firstly, for $\overline{D}_1 \in \mathbb{G}_1 = J_C[r] \cap \mathrm{Ker}(\pi - [1])$ and $\overline{D}_2 \in \mathbb{G}_2 = J_C[r] \cap \mathrm{Ker}(\pi - [q])$, from the reduced Tate-Lichtenbaum Pairing, we have

$$e(\overline{D}_1, \overline{D}_2) = f_{q^k, D_1}(D_2) \tag{2}$$

and

$$f_{q^k, D_1} = \prod_{i=0}^{k-1} (f_{q, [q^i] D_1})^{q^{k-i-1}} \tag{3}$$

The proofs are same as Lemma 3 and 4 in [8].

From the Lemma 5 in [8], we also have the following lemma:

Lemma 1. *Let D be a reduced divisor and ψ a purely inseparable map on C with $\psi(P_\infty) = P_\infty$. Then $\psi(D)$ is also reduced and we can take*

$$f_{n,\psi(D)} \circ \psi = f_{n,D}^{deg(\psi)}.$$

So, the important step to define the hyperelliptic Ate pairing on $\mathbb{G}_1 \times \mathbb{G}_2$ is to construct the purely inseparable map ψ, such that: (1). $\psi(D) = [q^i]D$, $D \in \mathbb{G}_1$. (2). $\mathbb{G}_2$ is fixed under ψ. To give such map ψ, we will use twist curve and reconsider the representation of the group $\mathbb{G}_2$.

Let C be a hyperelliptic curve over $\mathbb{F}_q$ and $r|\#J_C(\mathbb{F}_q)$ be a large prime. k is the embedding degree. C' is the degree d twist of C. There is an isomorphism

$$[\cdot] : \mu_d \to Aut(C) : \xi \to [\xi].$$

The action of $[\xi]$ on C and J_C will be presented later on the concrete curve. Set $m = \gcd(k, d), e = k/m$. Since k is the minimal value such that r divides $q^k - 1$, then the group $J_C(\mathbb{F}_{q^e})$ has order divisible by r, but not r^2. C has a degree d twist, so, there is a unique degree m twist C_0 of C over $\mathbb{F}_{q^e}$ such that $r|\#J_{C_0}(\mathbb{F}_{q^e})$ (Actually, when $k = d$, C_0 is also the degree $me = d$ twist of C over $\mathbb{F}_q$, i.e., $C_0 = C'$). $[\xi_m]$ defines an automorphism on C_0, so on $J_{C_0}(\mathbb{F}_{q^e})$. Therefor, we have

$$J_{C_0}(\mathbb{F}_{q^e}) \simeq \mathrm{Ker}([\xi_m]\pi^e - 1).$$

Define $\psi = [\xi_m]\pi^e$ and

$$\mathbb{G}_2 = J_C[r] \cap \mathrm{Ker}([\xi_m]\pi^e - 1).$$

Since

$$\mathrm{Ker}(\pi - 1) \cap \mathrm{Ker}([\xi_m]\pi^e - 1) = \mathcal{O},$$

so, π acts as multiplication by q on $\mathbb{G}_2$. $\psi = [\xi_m]\pi^e$ acts as identity on $\mathbb{G}_2$, therefor, $[\xi_m]$ acts as multiplication by q^{-e} on $\mathbb{G}_2$. Since $J_C[r] = \mathbb{G}_1 \times \mathbb{G}_2$ and $[\xi_m]$ has degree 1, we conclude that $[\xi_m]$ acts as multiplication by q^e on $\mathbb{G}_1$, i.e., for $D_1 \in \mathbb{G}_1$, we have

$$[\xi_m]D_1 = [q^e]D_1.$$

Now, for $\overline{D}_1 \in \mathbb{G}_1 = J_C[r] \cap \mathrm{Ker}(\pi - [1])$ and $\overline{D}_2 \in \mathbb{G}_2 = J_C[r] \cap \mathrm{Ker}([\xi_m]\pi^e - 1)$, we can compute

$$e(\overline{D}_1, \overline{D}_2) = f_{q^k,D_1}(D_2)$$

as follows:

$$
\begin{aligned}
f_{q^k,D_1}(D_2) &= f_{q^{em},D_1}(D_2) \\
&= \prod_{i=0}^{m-1} (f_{q^e,[(q^e)^i]D_1})^{q^{e(m-i-1)}}(D_2) \\
&= \prod_{i=0}^{m-1} (f_{q^e,[[\xi_m]^i]D_1} \circ [\xi_m]^i \circ \pi^{ei})(D_2) \\
&= \prod_{i=0}^{m-1} f_{q^e,D_1}(D_2)^{q^{ei}q^{e(m-i-1)}} \\
&= f_{q^e,D_1}(D_2)^{\sum_{i=0}^{m-1} q^{ei}q^{e(m-i-1)}} \\
&= f_{q^e,D_1}(D_2)^{mq^{e(m-1)}}
\end{aligned}
$$

This means that $f_{q^e,D_1}(D_2)$ defines a non-degenerate, bilinear pairing, we called the hyperelliptic twisted Ate pairing. Note that, if q^e is not modular r, then the final exponentiation in the hyperelliptic twisted Ate pairing is not needed.

To sum up, we have the following theorem about hyperelliptic twisted Ate pairing.

Theorem 2. *Let C be a hyperelliptic curve over $\mathbb{F}_q$ which has a degree d twisted curve C' and $r|\#J_C(\mathbb{F}_q)$ be a large prime. Let k be the embedding degree and $m = \gcd(k,d), e = k/m$. Let $\mathbb{G}_1 = J_C[r] \cap Ker(\pi - [1])$ and $\mathbb{G}_2 = J_C[r] \cap Ker(\pi - [q]) = J_C[r] \cap Ker([\xi_m]\pi^e - 1)$, then*

$$t(\overline{D}_1, \overline{D}_2) = f_{q^e,D_1}(D_2)$$

with $D_1 \in \overline{D}_1$ and $D_2 = \rho(\overline{D}_2)$ such that $supp(D_1) \cap supp(D_2) = \emptyset$, defines a non-degenerate, bilinear pairing called the hyperelliptic twisted Ate pairing. Furthermore, the relation with the reduced Tate-Lichtenbaum pairing is as follows:

$$e(\overline{D}_1, \overline{D}_2) = t(\overline{D}_1, \overline{D}_2)^{\sum_{i=0}^{m-1} q^{ei}q^{e(m-i-1)}} = t(\overline{D}_1, \overline{D}_2)^{mq^{e(m-1)}}.$$

Like the case in elliptic curve [21], we can generalize hyperelliptic Ate and twisted Ate pairing to generalized Ate and twisted Ate pairing.

Theorem 3. *For $\mathbb{G}_1 = J_C[r] \cap Ker(\pi - [1])$ and $\mathbb{G}_2 = J_C[r] \cap Ker(\pi - [q])$, then*

$$f_{(q \mod r),D_2}(D_1)^{\frac{q^k-1}{r}}$$

$$f_{(q^e \mod r),D_1}(D_2)^{\frac{q^k-1}{r}}$$

are still pairings , called them Optimised hyperelliptic Ate and twisted Ate pairings.

Proof . Assume that $q = lr + w$, i.e., $w = q \mod r$, then we have

$$\begin{aligned} f_{q,D_2} &= f_{lr+w,D_2} \\ &= f_{lr,D_2} \cdot f_{w,D_2} \cdot G_{lrD_2,wD_2} \\ &= f^l_{r,D_2} \cdot f_{w,D_2} \cdot G_{\mathcal{O},wD_2} \end{aligned}$$

Note that

$$div(G_{\mathcal{O},wD_2}) = \mathcal{O} + wD_2 - (\mathcal{O} \oplus wD_2) = \mathcal{O} + wD_2 - wD_2 = \mathcal{O},$$

$G_{\mathcal{O},wD_2}(D_1) = c \in \mathbb{F}_q^*$, so,

$$f_{q,D_2}(D_1)^{\frac{q^k-1}{r}} = (f^l_{r,D_2}(D_1)f_{w,D_2}(D_1))^{\frac{q^k-1}{r}} = e(\overline{D}_2, \overline{D}_1)^l f_{w,D_2}(D_1)^{\frac{q^k-1}{r}}$$

Therefor,

$$f_{(q \mod r),D_2}(D_1)^{\frac{q^k-1}{r}}$$

is still a pairing.

Similar proof can be used to the twisted Ate pairing case. □

Theorem 4. *For* $\mathbb{G}_1 = J_C[r] \cap Ker(\pi - [1])$ *and* $\mathbb{G}_2 = J_C[r] \cap Ker(\pi - [q])$,

$$f_{(q^i \mod r),D_2}(D_1)^{\frac{q^k-1}{r}}$$

and

$$f_{(q^{ei} \mod r),D_1}(D_2)^{\frac{q^k-1}{r}}$$

are all still pairing, called the generalized hyperelliptic Ate pairing and generalized hyperelliptic twisted Ate pairing, respectively.

These generalized hyperelliptic Ate and twisted Ate pairing should need the final exponentiation to obtain the unique pairing value.

All of these variants have a common goal, namely to make the length of the loop in Miller's algorithm as small as possible.

In the practice, we will consider the evaluation of $f(P_\infty)$. Using the same approach in [8], let u_∞ be a fixed $\mathbb{F}_q$-rational uniformizer at P_∞, then for any function $f \in \overline{\mathbb{F}}_q(C)^*$ we define $\mathrm{lc}_\infty(f)$ to be the leading coefficient of f as a Laurent series in u_∞. So when f is defined at P_∞ we have $f(P_\infty) = \mathrm{lc}_\infty(f)$ independent of the uniformizer chosen. Using Magma[16], we can verify that these pairings are all bilinear.

The first example of pairing-friendly genus 2 curves with ordinary Jacobians was given by D. Freeman [6]. However, the parameters for these curves are not very attractive for fast pairing implementation, the size of r is too small compared with the size of q, it is $q \approx r^4$. Kawazoe and Takahashi [13] presented two different approaches for explicitly constructing pairing- friendly genus 2 curves of the type $y^2 = x^5 + ax$ over prime field. Even Kawazoe et al.'s genus 2 curves are much better than Freeman's construction, because $q \approx r^2$(some one can achieve to $q \approx r^{3/2}$), but the hyperelliptic Ate pairing on these curves is still no any advantage than Tate pairing although hyperelliptic Ate pairing is no final exponentiation. This is why we should consider Theorem 3 currently.

However, when we use the twist curve, the optimised hyperelliptic twisted Ate pairing will be comparable with Tate pairing. We use some curves presented in [13] to construct hyperelliptic twisted Ate pairing and generalized hyperelliptic twisted Ate pairing.

Consider the hyperelliptic curve

$$C : y^2 = x^5 + 13x$$

over $\mathbb{F}_q$, where

$q =$ 26699838029972102220848505267856400207807895259155218981981072088044088950777212163875545592 5409.

From [13], we know that $\#J_C(\mathbb{F}_q)$ has a prime factor

$$r = 730750819774027608217118960060276298985251336001,$$

and the embedding degree $k = 8$. As discussed in Section 3, this curve has a twist with degree 8:

$$C' : y^2 = x^5 + 13\lambda x, \ (x, y) \to (\lambda^{\frac{1}{4}} x, \lambda^{\frac{5}{8}} y)$$

Here $\lambda \in \mathbb{F}_q$ is not l-th power residue in $\mathbb{F}_q$, for $l \in \{1, 2, 4, 8\}$.

As presented in [4], $[\xi] : P = (x, y) \to [\xi](P) = (\zeta_8^2 x, \zeta_8 y)$ ($\zeta_8 \in \mathbb{F}_p$ is a primitive 8-th root of unity) is an automorphism of curve C, it induces an efficient automorphism of order 8 on J_C as follows:

$$[\xi] : [x^2 + u_1 x + u_0, v_1 x + v_0] \to [x^2 + \zeta_8^2 u_1 x + \zeta_8^4 u_0, \zeta_8^{-1} v_1 x + \zeta_8 v_0]$$

$$[x + u_0, v_0] \to [x + \zeta_8^2 u_0, \zeta_8 v_0]$$

$$[\mathcal{O}] \to [\mathcal{O}]$$

So, we have $k = 8, d = 8, m = \gcd(k, d) = 8, e = k/m = 1$, and the hyperelliptic twisted Ate pairing is defined as

$$t(\overline{D}_1, \overline{D}_2) = f_{q,D_1}(D_2),$$

here $\overline{D}_1 \in \mathbb{G}_1 = J_C[r] \cap \mathrm{Ker}(\pi - [1])$ and $\overline{D}_2 \in \mathbb{G}_2 = J_C[r] \cap \mathrm{Ker}(\pi - [q]) = J_C[r] \cap \mathrm{Ker}([\xi]\pi - 1)$. It is easy to compute that $q^3 \mod r = 1099511628193 \approx r^{1/\varphi(8)}$, so the generalized hyperelliptic twisted Ate pairing $tAte_3$ is defined as

$$tAte_3(\overline{D}_1, \overline{D}_2) = f_{q^3 \mod r, D_1}(D_2)^{\frac{q^k-1}{r}} = f_{1099511628193, D_1}(D_2)^{\frac{q^k-1}{r}}.$$

This generalized hyperelliptic twisted Ate pairing has a miller loop of length of $r^{1/\varphi(8)}$. We also consider another curve in [13],

$$C : y^2 = x^5 + 2x$$

over $\mathbb{F}_q$, where

$q = 444292483637841082598410015665493978083277385484222711267571600830352907$ and $r = 1467186828927128936514540199634172027208104690001$.

$k = 24, d = 8, m = \gcd(k, d) = 8, e = k/m = 3$. It is easy to compute that $q^{11} \mod r = 1049085 \approx r^{1/\varphi(24)}$, so the generalized hyperelliptic Ate pairing Ate_3 is defined as

$$Ate_{11}(\overline{D}_2, \overline{D}_1) = f_{1049085, D_2}(D_1)^{\frac{q^k-1}{r}}.$$

For these known pairing-friendly hyperelliptic curves, the minimal value of $q^i \mod r$ is as small as $\approx r^{1/\varphi(k)}$. Therefore, the generalized hyperelliptic Ate pairing and twisted Ate pairing which have the minimal of $q^i \mod r$ can be computed more efficient than the original Ate pairing. When the embedding degree k of pairing-friendly hyperelliptic curve equals to the twist degree d, and the minimal value of $q^i \mod r$ is as small as $\approx r^{1/\varphi(k)}$, then the generalized hyperelliptic twisted Ate pairing $tAte_i$ will be most efficient in Tate pairing, Ate pairing and generalized hyperelliptic Ate and twisted Ate pairings.

5 Weil Pairing Computation using Twisted Ate Pairing

The Weil pairing is defined to be a non-degenerate bilinear map

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

which

$$e_w(\overline{D}_1, \overline{D}_2) = (-1)^r \frac{f_{r,D_1}(D_2)}{f_{r,D_2}(D_1)}.$$

The Weil pairing computation does not need the final exponentiation while it involves two Miller iteration loops. In this section, we investigate how to speed up the Weil pairing computations with twisted curve. Similar to the Ate pairing, the new variants based on the Weil pairing are proposed with short Miller iteration loops. Computing the new variants of the Weil pairing maybe the fastest than computing all the known pairings under some certain conditions.

For q^{ej}, let $q^{(ej)a}-1=Lr$, $r^2\nmid q^{(ej)a}-1$. Define $q_r^{ej}=q^{ej} \mod r$

Theorem 5.

$$\frac{f_{q_r^{ej},D_1}(D_2)}{f_{q_r^{ej},D_2}(D_1)}$$

is a fixed power of Weil pairing, called twisted Weil pairing.

Proof . From

$$e_w(\overline{D}_1,\overline{D}_2)=(-1)^r\frac{f_{r,D_1}(D_2)}{f_{r,D_2}(D_1)}$$

$\gcd(L,q^{(ej)a}-1)=1$, we have

$$\begin{aligned}
\frac{f_{r,D_1}(D_2)}{f_{r,D_2}(D_1)} &= (\frac{f_{r,D_1}(D_2)}{f_{r,D_2}(D_1)})^{L\cdot(L^{-1} \mod r)}\\
&= (\frac{f_{Lr,D_1}(D_2)}{f_{Lr,D_2}(D_1)})^{(L^{-1} \mod r)}\\
&= (\frac{f_{q^{(ej)a}-1,D_1}(D_2)}{f_{q^{(ej)a}-1,D_2}(D_1)})^{(L^{-1} \mod r)}\\
&= (\frac{f_{q^{(ej)a},D_1}(D_2)}{f_{q^{(ej)a},D_2}(D_1)})^{(L^{-1} \mod r)}\\
&= (\frac{f_{q^{ej},D_1}(D_2)}{f_{q^{ej},D_2}(D_1)})^{aq^{(ej)(a-1)}\cdot(L^{-1} \mod r)}\\
&= (\frac{f_{lr+q_r^{ej},D_1}(D_2)}{f_{lr+q_r^{ej},D_2}(D_1)})^{aq^{(ej)(a-1)}\cdot(L^{-1} \mod r)}\\
&= (\frac{f_{lr,D_1}(D_2)}{f_{lr,D_2}(D_1)}\frac{f_{q_r^{ej},D_1}(D_2)}{f_{q_r^{ej},D_2}(D_1)})^{aq^{(ej)(a-1)}\cdot(L^{-1} \mod r)}\\
&= (e_w(\overline{D}_1,\overline{D}_2)^l\cdot\frac{f_{q_r^{ej},D_1}(D_2)}{f_{q_r^{ej},D_2}(D_1)})^{aq^{(ej)(a-1)}\cdot(L^{-1} \mod r)}
\end{aligned}$$

So, we have

$$\frac{f_{q_r^{ej},D_1}(D_2)}{f_{q_r^{ej},D_2}(D_1)}=e_w(\overline{D}_1,\overline{D}_2)^c$$

Here $c=L\cdot(aq^{(ej)(a-1)})^{-1}-l \mod r$. □

For example, we consider the curve in Section 4, $C : y^2 = x^5+13x$ over $\mathbb{F}_q$, and $k = 8, d = 8, m = \gcd(k,d) = 8, e = k/m = 1$, when $j = 3$, $q^3 \mod r = 1099511628193 \approx r^{1/\varphi(8)}$, then the twisted Weil pairing can be defined as

$$tw(\overline{D}_1, \overline{D}_2) = \frac{f_{1099511628193,D_1}(D_2)}{f_{1099511628193,D_2}(D_1)}.$$

In [22], Zhao and Zhang discussed the twisted Weil pairing in elliptic curve case. Because the degree d of twists of ordinary elliptic curves over $\mathbb{F}_q$, $Char(\mathbb{F}_q) \geq 5$ only 2, 3, 4, 6 are possible [19], the minimal value of $(q^i \mod r)$ or $(q^{ei} \mod r)$ is only as small as $r^{1/2}$. In this case, the computation cost of $f_{q^{ei} \mod r,Q}(P)$ is lager than the computation of final exponentiation. So, the Miller loop of twisted Weil pairing is only half of that required for the Weil pairing and it is clear that the elliptic twisted Weil pairing is computed slower than other pairings, such as Tate pairing and Ate pairing, etc.

The Miller loop length of hyperelliptic Ate pairing only can be up to g times shorter than for the Tate pairing. For some big genus curves with very high degree twists , we can have $\varphi(d) > 2g$(Note that many of the computational assumptions in pairing based cryptography can be solved in subexponential time, hence it may not be necessary to restrict to very small genus g), then the twisted Weil pairing has more shorter Miller loop length, and therefor faster than hyperelliptic Ate pairing. For a very special case that $t = q^j \mod r \approx r^{1/\varphi(k)}{=}r^{1/\varphi(d)}$ is very small, then computing $f_{t,D_2}(D_1)$ maybe faster than the computation of the final exponentiation, in this case, computing the twisted Weil pairing maybe faster than computing Tate pairing and Ate pairing etc. all the known pairings.

6 Conclusion

In this paper we show that the twisted Ate pairing on elliptic curves can be generalized to hyperelliptic curves, we also give a series of variations of the hyperelliptic Ate and twisted Ate pairings. Using the hyperelliptic Ate pairing and twisted Ate pairing, we propose a new approach to speed up the Weil pairing computation, and obtain an interested result: For some hyperelliptic curves with high degree twist, computing the Weil pairing using this approach maybe the fastest in computing all the known pairings.

Acknowledgements

I am grateful to Xibin Lin for helpful discussions and his implementation.

References

1. P.S.L.M. Barreto, S. Galbraith, C. ÓhÉigeartaigh, and M. Scott. Efficient Pairing Computation on Supersingular Abelian Varieties. *In Designs, Codes and Cryptography*, vol 42(3), pp.239-271, 2007. Also availabe from http://eprint.iacr.org/2004/375.
2. O. Bolza, On binary sextics with linear transformations between themselves, *Amer. J. Math.* 10, pp.47-70, 1888.
3. G. Cardona, On the number of curves of genus 2 over a finite field, *Finite Fields Appl.* 9 (4), pp.505-526, 2003.
4. I.M. Duursma, P. Gaudry, and F. Morain. Speeding up the Discrete Log Computation on Curves with Automorphisms, *AsiaCrypt'99*, LNCS 1716, pp. 203-121. Springer-Verlag, 1999.
5. I.M. Duursma and H.-S. Lee. Tate Pairing Implementation for Hyperelliptic Curves $y^2 = x^p - x + d$. *ASIACRYPT 2003*, LNCS 2894, pp. 111-123. Springer, 2003.
6. D. Freeman, Constructing Pairing-Friendly Genus 2 Curves over Prime Fields with Ordinary Jacobians, Pairing-Based Cryptography - Pairing 2007, LNCS 4575, Springer-Verlag, pp. 152-176, 2007.
7. G. Frey, and H.-G. Rück, A Remark Concerning m-Divisibility and the Discrete Logarithm Problem in the Divisor Class Group of Curves, *Mathematics of Computation*, 62(206), pp.865-874, 1994.
8. R. Granger, F. Hess, R. Oyono, N. Thériault, and F. Vercauteren, Ate Pairing on Hyperelliptic Curves, *Advance in Cryptology - EUROCRYPT'2007*, LNCS 4515, Springer-Verlag, pp. 430-447, 2007.
9. R. Granger, D. Page and N.P. Smart, High Security Pairing-based Cryptography Revisited, Cryptology ePrint Archive, Report 2006/059, 2006, http://eprint.iacr.org/2006/059.
10. S.D. Galbraith. Pairings, *Ch. IX of I.F.Blake, G.Seroussi, and N.P.Smart, eds., Advances in Elliptic Curve Cryptography*. Cambridge University Press, 2005.
11. S.D. Galbraith, F. Hess and F. Vercauteren. Hyperelliptic Pairings, Pairing 2007, LNCS 4575, pp. 108-131. Springer-Verlag, 2007.
12. F. Hess, N.P. Smart and F. Vercauteren. The Eta Pairing Revisited. *IEEE Transactions on Information Theory*, vol 52, pp. 4595-4602, Oct. 2006. Also available from http://eprint.iacr.org/2006/110.
13. M. Kawazoe, and T. Takahashi, Pairing-friendly Hyperelliptic Curves of Type $y^2 = x^5 + ax$, Cryptology ePrint Archive, Report 2008/026, 2008, http://eprint.iacr.org/2008/026.
14. N. Koblitz and A. Menezes. Pairing-based Cryptography at High Security Levels. In Cryptography and Coding, LNCS 3796, pp. 235-249. Springer-Verlag, 2005.
15. E. Lee, H.-S. Lee, and C.-M. Park. Efficient and Generalized Pairing Computation on Abelian Varieties. Preprint, 2008. Available at http://eprint.iacr.org/2008/040.
16. MAGMA Computational Algebra System, http://magma.maths.usyd.edu.au/magma/
17. S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto. Optimised versions of the Ate and twisted Ate pairings. The 11th IMA International Conference on Cryptography and Coding, LNCS 4887, pp. 302-312. Springer-Verlag, 2007.
18. V.S. Miller. Short Programs for Functions on Curves. Unpublished manuscript, 1986.
19. J.H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York, 1986.
20. F. Vercauteren. Optimal Pairings. Preprint, 2008. Available at http://eprint.iacr.org/2008/096.
21. C.-A. Zhao, F. Zhang and J. Huang. A Note on the Ate Pairing. Preprint 2007, to appear in Internationl Journal of Information Security. Also available at http://eprint.iacr.org/2007/247.
22. C.-A. Zhao and F. Zhang. Reducing the Complexity of the Weil Pairing Computation. Preprint, 2008. Available at http://eprint.iacr.org/2008/212.