Pairing with Supersingular Trace Zero Varieties Revisited

Emanuele Cesena

Università degli Studi RomaTre
Dip. di Matematica
Roma – Italy
cesena at mat.uniroma3.it

Abstract. A Trace Zero Variety is a specific subgroup of the group of the divisor classes on a hyperelliptic curve $C/\mathbb{F}_q$, which are rational over a small degree extension $\mathbb{F}_{q^r}$ of the definition field. Trace Zero Varieties (TZV) are interesting for cryptographic applications since they enjoy properties that can be exploited to achieve fast arithmetic and group construction. Furthermore, supersingular TZV allows to achieve higher MOV security per bit than supersingular elliptic curves, thus making them interesting for applications in pairing-based cryptography.
In this paper we survey algorithms in literature for computing bilinear pairings and we present a new algorithm for the Tate pairing over supersingular TZV, which exploits the action of the q-Frobenius. We give explicit examples and provide experimental results for supersingular TZV defined over fields of characteristic 2. Moreover, in the same settings, we propose a more efficient variant of the Silverberg's point compression algorithm.

1 Introduction

The development of pairing-based cryptography motivated the growth of interest in the efficient computation of bilinear pairings.

Originally supersingular elliptic curves were considered, as they enjoy a number of properties suitable for an efficient implementation. In [1], Rubin and Silverberg propose to use supersingular abelian varieties of dimension greater than one to improve the security of pairing-based cryptosystems. A part from Jacobian varieties of hyperelliptic curves, the other significant example is the class of trace zero varieties (also called primitive subgroups).

Trace zero varieties (TZV) were first proposed by Frey [2]: if C is a hyperelliptic curve of genus g defined over a finite field of q elements $\mathbb{F}_q$, the *trace zero (sub)variety of C over a field extension of degree r* is a subgroup G of the Jacobian variety $J(\mathbb{F}_{q^r})$ of C over $\mathbb{F}_{q^r}$, that is isomorphic to the quotient group $J(\mathbb{F}_{q^r})/J(\mathbb{F}_q)$; it is a codimension one subvariety of the Weil restriction of scalars of $J(\mathbb{F}_{q^r})$ on $\mathbb{F}_q$. Several authors addressed the study of TZV, and their results are summarised by Avanzi, Lange [3] for prime fields and by Avanzi, Cesena [4] for binary fields.

The work of Rubin and Silverberg and the more recent results available in [5] constitute the motivation of this paper. Notably, supersingular TZV allow to achieve higher MOV security per bit than supersingular elliptic curves: in characteristic 3 ($g = 1, r = 5$) TZV represent the first example of supersingular abelian varieties with security parameter greater than 6; in characteristic 2 ($g = 1, r = 3$), they provide a more efficient alternative (with equivalent security properties) to supersingular elliptic curves over $\mathbb{F}_{3^m}$.

The computation of pairings over TZV has already been taken into account by Barreto et al. [6], that define the Eta and Eta$_T$ pairings over supersingular abelian varieties. Other pairings, such as the (twisted) Ate pairing [7] and its extended versions [8,9,10] can be naturally defined on TZV. All these pairings exploit the q^r-Frobenius and can in fact be defined not only on the TZV, but on the whole $J(\mathbb{F}_{q^r})$.

Our main result is a new algorithm for computing the Tate pairing over supersingular TZV exploiting the action of the q-Frobenius.

Scott [11] describes a technique to speed up the computation of pairing using an efficient endomorphism and a class of ordinary curves, called NSS (not supersingular) curves, endowed with such an endomorphism. A similar technique can be applied to TZV, but the resulting algorithm is not efficient for supersingular varieties; we will come back to this point in the discussion after presenting our algorithm in Theorem 2.

The rest of the paper is organized as follows: in Sect. 2 we review the background on hyperelliptic curves and TZV; in Sect. 3 we introduce the Miller function and its properties; we survey the most efficient algorithms for computing bilinear pairings in Sect. 4, then we present our new algorithm in Sect. 5. Section 6 is devoted to explicit examples and experimental results: we focus to supersingular TZV defined over fields of characteristic 2; in the same settings, we review the Silverberg's point compression algorithm for TZV and we propose a more efficient variant. In Sect. 7 we draw our conclusions.

2 Background

In this section we introduce elliptic and hyperelliptic curves and define TZV, mentioning only a few facts.

We present TZV in a “naïf” form, following [3,4]. In [5], Rubin and Silverberg provide a more formal definition containing all the results we require.

There are several books on the subject of elliptic and hyperelliptic curves. For reference material within the perspective of cryptographic of applications we refer to [12].

2.1 Hyperelliptic Curves

In this paper $\mathbb{F}_q$ denotes the Galois field of order q. A *hyperelliptic curve* C of genus g over $\mathbb{F}_q$ having an $\mathbb{F}_q$-rational Weierstraß point is a non singular curve defined by the equation:

$$y^2 + h(x)y = f(x), \qquad f \text{ monic}, \ \deg f = 2g+1, \ \deg h \leq g \ .$$

A hyperelliptic curve of genus 1 is called an *elliptic curve.* An elliptic curve has Weierstraß equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ , \qquad \text{with} \quad a_i \in \mathbb{F}_q \ . \tag{1}$$

Let J denote the *Jacobian variety* of C.

Let $\sigma \in \mathrm{Gal}_{\overline{\mathbb{F}}_q/\mathbb{F}_q}$ be the $q-$Frobenius automorphism. It naturally extends to an endomorphism of J, that we call *Frobenius endomorphism* and we still denote with σ. It satisfies the characteristic polynomial:

$$\chi(T) = T^{2g} + a_1T^{2g-1} + \cdots + a_gT^g + \cdots + a_1q^{g-1}T + q^g \ , \tag{2}$$

where $a_i \in \mathbb{Z}$. The Hasse–Weil theorem states that from the complex roots τ_i of $\chi(T)$ we can obtain the group order over any extension:

$$|J(\mathbb{F}_{q^n})| = \prod_{i=1}^{2g}(1 - \tau_i^n) \ ,$$

in particular $|J(\mathbb{F}_q)| = \chi(1)$.

For an elliptic curve $E/\mathbb{F}_q$, we use to write $\chi(T) = T^2 - tT + q$, where $t = -a_1$ is the *trace* of the Frobenius; the previous statement can be made explicit as follows:

$$|E(\mathbb{F}_{q^n})| = q^n + 1 - t_n \tag{3}$$

where the sequence $(t_n)_{n\in\mathbb{N}}$ satisfies $t_0 = 2$, $t_1 = t$ and $t_{n+1} = tt_n - qt_{n-1}$, for $n \geq 1$.

2.2 Trace Zero Varieties

Let r be a (small) prime number; let $J(\mathbb{F}_{q^r})$ be the Jacobian variety over $\mathbb{F}_{q^r}$ of a hyperelliptic curve $C/\mathbb{F}_q$ and let $D \in J(\mathbb{F}_{q^r})$. Suppose $r \nmid |J(\mathbb{F}_{q^r})|$.

We can formally define the *trace* of D, as for fields:

$$\mathrm{Tr}(D) = D + \sigma(D) + \cdots + \sigma^{r-1}(D) \ .$$

It is clearly an endomorphism of $J(\mathbb{F}_{q^r})$. The *trace zero (sub)variety* (TZV) of $J(\mathbb{F}_{q^r})$ is the set:

$$J_r(\mathbb{F}_q) = \{D \in J(\mathbb{F}_{q^r}) \mid \mathrm{Tr}(D) = \mathcal{O}\} \ ,$$

where $\mathcal{O}$ is the neutral element in $J(\mathbb{F}_{q^r})$. Being the kernel of the trace endomorphism, $J_r(\mathbb{F}_q)$ is a group. It is a codimension 1 subvariety of the *Weil restriction of scalars* of $J(\mathbb{F}_{q^r})$ on $\mathbb{F}_q$.

From the cryptographic point of view, only the following cases are relevant: $g = 1, \ n = 3$; $g = 1, \ n = 5$; $g = 2, \ n = 3$. The next proposition (cf. [3,4]) gives us the group orders.

Proposition 1. *Let $J_r/\mathbb{F}_q$ be a TZV.*

(i) For $g=1$ and $r=3$:

$$|J_r(\mathbb{F}_q)| = q^2 - q(1+a_1) + a_1^2 - a_1 + 1$$

(ii) For $g=1$ and $r=5$:

$$\begin{aligned}|J_r(\mathbb{F}_q)| = q^4 - (a_1+1)q^3 + (a_1+1)^2q^2 + \big(5a_1 - (a_1+1)^3\big)q+ \\ - \big(5a_1(a_1^2+a_1+1) - (a_1+1)^4\big)\end{aligned}$$

(iii) For $g=2$ and $r=3$:

$$\begin{aligned}|J_r(\mathbb{F}_q)| = q^4 - a_1q^3 + (a_1^2+2a_1-a_2-1)q^2 + (-a_1^2 - a_1a_2 + 2a_1)q+ \\ + a_1^2 + a_2^2 - a_1a_2 - a_1 - a_2 + 1\end{aligned}$$

Here, the integers a_1, a_2 are coefficients of the characteristic polynomial of the Frobenius endomophism (2).

Suppose $|J_r(\mathbb{F}_q)|$ is divisible by a large prime factor l; with the purpose of cryptographic applications we will restrict ourselves to work in the subgroup $\mathbb{G}_1 \leq J_r(\mathbb{F}_q)$ of order l.

On the points of $\mathbb{G}_1$, σ acts as a multiplication times an integer s; explicit values are given in the next proposition (cf. [3,4]).

Proposition 2. *Let $J_r/\mathbb{F}_q$ be a TZV. Let $D \in J_r(\mathbb{F}_q)$ a divisor of large prime order l. Then $\sigma(D) = [s]D$ for some integer s.*

(i) For $g=1$ and $r=3$: $s = \dfrac{q-1}{1-a_1} \bmod \ell$;

(ii) For $g=1$ and $r=5$: $s = \dfrac{q^2-q-a_1^2q+a_1q+1}{q-2a_1q+a_1^3-a_1^2+a_1-1} \bmod \ell$;

(iii) For $g=2$ and $r=3$: $s = -\dfrac{q^2-a_2+a_1}{a_1q-a_2+1} \bmod \ell$.

Let $k_{J,q}$ be the embedding degree, i.e. the multiplicative order of q modulo l. It is the smallest integer such that $J[l] \subset J(\mathbb{F}_{q^{k_{J,q}}})$. Rubin and Silverberg [5] define the cryptographic exponent and prove that it is a finer invariant than the embedding degree; however for the cases of our interest (see Lemmas 1, 2 and 3 below) the two measures coincide. To simplify the notation we set $k = k_{J_r,q}$ and $h = k_{J,q}$.

Theorem 9.2 of [5] proves that if J is supersingular and r is coprime with $2qk_{J,q}$, then $k_{J_r,q} = rk_{J,q}$, i.e. $k = rh$.

Suppose now $l^2 \nmid \big|J(\mathbb{F}_{q^k})\big|$. Frey and Rück [13] (see also [12, Prop. 6.12]) show that there exists a non-degenerate, bilinear Tate pairing:

$$t\colon J[l](\mathbb{F}_{q^r}) \times J[l](\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^l \ .$$

By restriction, we define a Tate pairing on J_r in the following way.
Set $\mathbb{G}_1 = J_r[l] \cap \mathrm{Ker}\,(\pi - [1])^1$ and $\mathbb{G}_2 = J_r[l] \cap \mathrm{Ker}\,(\pi - [q^r])$, where $\pi = \sigma^r$ is the q^r-Frobenius endomorphism; let μ_l be the set of l-th roots of unity. Then there is a non-degenerate, bilinear (reduced) Tate pairing:

$$t\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_l \subset \mathbb{F}_{q^k}^* \ .$$

Most of the results on the pairing computation rely on the action of π in the two groups $\mathbb{G}_1$ and $\mathbb{G}_2$, namely identity and multiplication times q^r. For TZV however another efficient endomorphism exists, σ, acting as multiplication times s in $\mathbb{G}_1$. The next proposition describe the action of σ in $\mathbb{G}_2$.

Proposition 3. *Let $J_r/\mathbb{F}_q$ be a TZV. Let $D \in J_r[l] \cap \mathrm{Ker}\,(\pi - [q^r])$. Then $\sigma(D) = [S]D$ for some integer S.*

(i) For $g = 1$ and $r = 3$: $S = \dfrac{q - q^2}{q - a_1} \bmod l$;

(ii) For $g = 1$ and $r = 5$: $S = -\dfrac{q^4 - q^3 + (1 - a_1)q^2 - a_1^2 q}{q^3 + (1 - a_1)q^2 + (2a_1 - a_1^2)q - a_1^3} \bmod l$;

(iii) For $g = 2$ and $r = 3$: $S = -\dfrac{q^3 - a_2 q + a_1}{2q^2 - (a_1 + 1)q + 2a_1 - a_2} \bmod l$.

Proof. The proof is essentially the same as for s in Prop. 2, that can be found in [3]. S satisfies modulo l both: $\chi(S) \equiv 0$ and $(S^r - q^r)/(S - q) \equiv 0$. The results follow by expliciting the three cases. □

In this paper we will only focus on TZV defined over supersingular elliptic curves. To simplify the notation, we present results in the setting of elliptic curves: we consider an elliptic curve $E/\mathbb{F}_q$ and work with its K-rational points, where $K/\mathbb{F}_q$ is a finite extension. The intent is to set $K = \mathbb{F}_q$ to retrieve results on E, and $K = \mathbb{F}_{q^r}$ to obtain results that, by restriction, apply to E_r.

Moreover, altough we are using supersingular curves where a distortion map allows to define a symmetric pairing, we prefer to keep the two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ distinct, in order to have a better understanding of the two components of the l-torsion group.

3 Miller Function

Let $K/\mathbb{F}_q$ be a finite field and $E/\mathbb{F}_q$ an elliptic curve. For $P \in E(K)$ and $n \in \mathbb{Z}$, the Miller function $f_{n,P}$ is a K-rational function with divisor:

$$(f_{n,P}) = n\,(P) - ([n]P) - (n-1)\mathcal{O} \ .$$

The Miller function is defined up to multiplication by elements of K^*.

[1] Note the definition of $\mathbb{G}_1$ is the same as before.

The following properties hold (for every $\lambda, \mu \in \mathbb{Z}, k \in \mathbb{N}$):

$$f_{\lambda+\mu,P} = f_{\lambda,P} \cdot f_{\mu,P} \cdot \frac{l_{[\lambda]P,[\mu]P}}{v_{[\lambda+\mu]P}} \tag{4}$$

$$f_{\lambda\mu,P} = f_{\lambda,P}^{\mu} \cdot f_{\mu,[\lambda]P} \quad , \tag{5}$$

where $l_{[\lambda]P,[\mu]P}$ and $v_{[\lambda+\mu]P}$ are resp. the line through $[\lambda]P$, $[\mu]P$ and the vertical line through $[\lambda+\mu]P$.

From (4) one can deduce the Miller's algorithm [14]; from (5) the following useful property derives (cf. [6,7, both in Lemma 2]):

$$f_{\lambda^k,P} = f_{\lambda,P}^{\lambda^{k-1}} \cdot f_{\lambda,[\lambda]P}^{\lambda^{k-2}} \cdots f_{\lambda,[\lambda^{k-1}]P} \quad . \tag{6}$$

The property stated by equation (5) is simple to understand if we refer to the Miller's algorithm: suppose we are calculating $f_{n,P}(Q)$ with $n = \lambda\mu$ and we already computed $f_{\lambda,P}(Q)$; then we still need to perform a loop on μ, starting from the point $[\lambda]P$, i.e. we still need $f_{\mu,[\lambda]P}(Q)$; moreover the quantity $f_{\lambda,P}(Q)$ will be iteratively accumulated during the loop, thus raising it to μ.

Hence a single loop on $n = \lambda\mu$ can be "reduced" onto two independent loops on λ and μ (plus one exponentiation to μ). However, this property alone does not allow to reduce the complexity of the Miller's algorithm, since the two loops require to work with distinct points, resp. P and $[\lambda]P$.

Let $\sigma \in \mathrm{Gal}_{\bar{K}/K}$. Then clearly $f_{n,P^\sigma} = f_{n,P}^{\sigma}$ and hence the Miller function is Galois invariant:

$$f_{n,P^\sigma}\left(Q^\sigma\right) = \left(f_{n,P}(Q)\right)^\sigma \quad . \tag{7}$$

The next proposition describes the relationship between endomorphisms and Miller function. Proofs are included for completeness.

Proposition 4. *Let $\phi \in \mathrm{End}_K(E)$ with $\mathrm{Ker}\,\phi = \{\mathcal{O}\}$. Then, up to multiplication by elements in K^*:*

$$f_{n,\phi(P)} \circ \phi = \left(f_{n,P}\right)^{\deg\phi} \quad , \tag{8}$$

In particular:

(i) If ϕ is purely inseparable of degree q, $f_{n,\phi(P)} \circ \phi = f_{n,P}^{q}$.
(ii) If ϕ is an automorphism, $f_{n,\phi(P)} = f_{n,P} \circ \phi^{-1}$.

Proof. The left part of (8) is the pullback $\phi^* f_{n,\phi(P)}$. The equality up to elements in K^* holds because $(\phi^* f) = \phi^*\left(f\right)$, for every $f \in K(E)$ [15, Prop 3.6(b)]. Since $\mathrm{Ker}\,\phi = \{\mathcal{O}\}$, $P = \phi^{-1}\left(\phi(P)\right)$ is unique and the pullback of $\big(f_{n,\phi(P)}\big)$ is:

$$\phi^*\big(n\left(\phi(P)\right) - \left([n]\phi(P)\right) - (n-1)\left(\mathcal{O}\right)\big) = \deg\phi\big(n\left(P\right) - \left([n]P\right) - (n-1)\left(\mathcal{O}\right)\big) \quad ,$$

($[n]$ permutes with ϕ). The first statement holds. If ϕ is an automorphism, the right-side composition of (8) with ϕ^{-1} gives the second statement. □

Remarks.

1. The terms endo/automorphism in Prop. 4 have a geometric meaning, i.e. in $E(\bar{K})$; in cryptography an endomorphism is sometimes referred to as an automorphism when thinking to its restriction onto the considered group.
2. With a sligthly misleading notation, 4.ii provides a way to compute $f_{n,\phi(P)}(Q)$ based on $f_{n,P}$, at the price of evaluating it in $\phi^{-1}(Q)$; the misleading notation is because if $\phi\colon E \to E$, then P is naturally taken from the "left" E, while the point Q from the right one.
3. If $\phi(Q) = Q$, then 4.i allows to reduce $f_{n,\phi(P)}$ to a power of $f_{n,P}$. This has been used to define the twisted Ate pairing (see [7] and Sect. 4.1).

4 A Survey of Pairings

Let $K = \mathbb{F}_q$ be a finite field and $E/\mathbb{F}_q$ an elliptic curve.

We recall the notation introduced in Sect. 2. Let l be a large prime factor of $|E(K)|$ and suppose $l^2 \nmid |E(K)|$. Let k be the embedding degree, i.e. the smallest integer such that $E[l] \subset E(\mathbb{F}_{q^k})$. Let π the Frobenius endomorphism fixing $E(K)$.

Set $\mathbb{G}_1 = E[l] \cap E(K)$ and $\mathbb{G}_2 = E[l] \setminus E(K)$; let μ_l be the set of l-th roots of unity. Then there is a non-degenerate, bilinear Tate pairing:

$$t\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_l \subset \mathbb{F}_{q^k}^* \ , \qquad t(P,Q) = f_{l,P}(Q)^{\frac{q^k-1}{l}} \ .$$

For every $l \mid n \mid q^k - 1$, we have:

$$t(P,Q) = f_{n,P}(Q)^{\frac{q^k-1}{n}} \ . \tag{9}$$

We begin by defining $\mathtt{t}_n$ as the algorithm that computes the Tate pairing as in (9); the key point is that we run a Miller loop on n.

In what follows we are going to survey other algorithms to compute bilinear pairings. All of them require to compute $f_{a,X}(Y)^b$ for some integer a, b and some points X, Y. For the purpose of comparing them, we will refer to a as the *loop size*. At least for moderate security levels, the exponentiation to b is negligible with respect to the computation of $f_{a,X}(Y)$.

We note that Hess [16] recently proposes a new framework which encompasses all known pairing functions based on the Tate and Weil pairings, including the ones mentioned here.

Example 1. Let $q = 2^m$ and $E/\mathbb{F}_q : y^2 + y = x^3 + x + b$, $b \in \mathbb{F}_2$. We consider $E_3 \leq E(\mathbb{F}_{2^{3m}})$ the TZV, whose order is

$$N = q^2 - q(1-t) + t^2 + t + 1 \ , \qquad \text{with } t = \pm\sqrt{2q} \ .$$

Let l be a large prime dividing N, i.e. $N = lc$, where c is a small cofactor. A real example is with $m = 103$ and $b = 1$, having l a 192-bit prime (cf. [5]).

Let σ the q-Frobenius endomorphism; we have $\pi = \sigma^3$. Given a point $\breve{P} \in E(\mathbb{F}_{2^{3m}})$, $P = c\left(\breve{P} - \sigma(\breve{P})\right)$ is either $\mathcal{O}$ or, as we assume, a generator of $\mathbb{G}_1$.

E has embedding degree $h = 4$ so, for E_r, $k = 12$. For every $\tilde{Q} \in \mathbb{G}_1$, $Q = \psi(\tilde{Q}) \in \mathbb{G}_2$ where ψ is a distortion map (an actual example is given in [6] or in Sect. 6.1).

We define two algorithms for computing the Tate pairing:

$$\mathsf{t}_N(P,Q) := f_{N,P}(Q)^{\frac{q^k-1}{N}} \qquad \mathsf{t}_l(P,Q) := f_{l,P}(Q)^{\frac{q^k-1}{l}} \quad .$$

The first looks promising, since N has a low Hamming weight[2]; for both, the loop size is $O(q^2)$.

4.1 Ate Pairing

The Ate pairing was defined in [7]; we introduce it in a similar fashion as in [10]. Here we need to explicit the size of the field K, so we let $K = \mathbb{F}_{q^r}$ ($r = 1$ is also accepted).

For every $L \in \mathbb{Z}$ such that $l \nmid L$,

$$f_{lL,P}(Q)^{\frac{q^k-1}{l}} = t(P,Q)^L \tag{10}$$

is a non-degenerate, bilinear pairing.

Let $\lambda \equiv q^r \bmod l$, e.g. $\lambda = t_r - 1$ with the notation of (3). Then $l \mid \lambda^k - 1$ since $l \mid q^k - 1$. Let L such that $lL = \lambda^k - 1$ and note $l \nmid L$:

$$t(P,Q)^L = f_{lL,P}(Q)^{\frac{q^k-1}{l}} = f_{\lambda^k-1,P}(Q)^{\frac{q^k-1}{l}} = f_{\lambda^k,P}(Q)^{\frac{q^k-1}{l}} \quad .$$

Using (6) and $[\lambda^i]P = [q^{ir}]P$:

$$f_{\lambda^k,P} = f_{\lambda,P}^{\lambda^{k-1}} \cdot f_{\lambda,[q^r]P}^{\lambda^{k-2}} \cdots f_{\lambda,[q^{(k-1)r}]P} \quad .$$

In order to achieve a better algorithm for computing a bilinear pairing, we would like to reduce the computation of $f_{\lambda,[q^{ir}]P}$ to the computation of $f_{\lambda,P}$. Unfortunately this is not possible for a general curve.

By exchanging the roles of P and Q, it is instead possible to exploit the Miller function Galois-invariance (7) against the Frobenius π:

$$f_{n,[q^{ir}]Q}(P) = f_{n,\pi^i(Q)}\left(\pi^i(P)\right) = f_{n,Q^{\pi^i}}\left(P^{\pi^i}\right) = \left(f_{n,Q}(P)\right)^{\pi^i} = \left(f_{n,Q}(P)\right)^{q^{ir}} \quad .$$

In conclusion we have:

$$t(Q,P)^L = f_{\lambda^k,Q}(P)^{\frac{q^k-1}{l}} = f_{\lambda,Q}(P)^{\frac{q^k-1}{l}\sum_{i=0}^{k-1}\lambda^{k-1-i}q^{ir}} \quad ,$$

and we define the algorithm:

$$\mathsf{a}_\lambda(Q,P) := f_{\lambda,Q}(P)^{\frac{q^k-1}{l}} \quad .$$

[2] At least in NAF representation.

It computes a non-degenerate bilinear pairing, which is a fixed power of the Tate pairing. Such an algorithm, however, requires to perform a Miller loop on $Q \in E(\mathbb{F}_{q^k})$, which is fairly less efficient than working with $P \in E(K)$ (the latter is sometimes referred as Miller lite loop/algorithm).

By further generalization, we can take $\lambda \equiv q^{ir} \bmod l$, for any $1 \leq i < k$; we refer to [17] for more details.

4.2 Twisted Ate Pairing for Supersingular Curves: Eta and Eta$_T$ Pairings

As already noted, the Ate pairing requires to switch between P and Q, which is not a good choice from the implementation perspective.

The twisted Ate pairing [7] has been defined to overcome this problem for ordinary curves.

Supersingular curves allow to swap Q and P in a more natural way, and this in fact was described before the introduction of the Ate pairing, by defining the Eta and Eta$_T$ pairings (cf. [6]). We prefer to introduce them, however, from an a-posteriori point of view.

Let E be supersingular. Denote $\hat{\pi}$ the dual of the Frobenius π, also called Verschiebung. Since E is supersingular, $E[q^r] = \{\mathcal{O}\}$ and $\hat{\pi}$ is purely inseparable. Since $\pi \circ \hat{\pi} = [q^r]$, $\hat{\pi}$ acts on $\mathbb{G}_1$, resp. $\mathbb{G}_2$, as π acts on $\mathbb{G}_2$, resp. $\mathbb{G}_1$.

We fit into the hypothesis of Prop. 4.i (setting $\phi = \hat{\pi}$), so we have:

$$f_{n,[q^{ir}]P}(Q) = f_{n,\hat{\pi}^i(P)}\left(\hat{\pi}^i(Q)\right) = f_{n,\hat{\pi}^i(P)} \circ \hat{\pi}^i\,(Q) = (f_{n,P}(Q))^{q^{ir}} \quad ,$$

and repeating the arguments of the previous section, we can define the algorithm:

$$\mathsf{a}^{\mathsf{t}}_{\lambda}(P,Q) := f_{\lambda,P}(Q)^{\frac{q^k-1}{l}} \quad ,$$

which computes a non-degenerate, bilinear pairing.

The Eta and Eta$_T$ pairings were defined in [6]. The point of view is sligthly different, but the final result almost coincides with the one we just achieved. We repeat the original argument, since we are going to use a similar approach in the proof of Theorem 2.

The starting point is a supersingular elliptic curve E with even embedding degree k and a distortion map ψ that allows for denominator elimination [18]. Let T such that $T^a + 1 = lL$, for some positive integers a and L, and $T \equiv q^r \bmod l$. Suppose there exists an automorphism γ of E such that $\gamma(P) = [T]P$ and $\gamma \circ \psi^{\pi} = \psi$, or equivalently $\gamma^{-1} \circ \psi = \psi^{\pi}$. We have:

$$t(P,Q)^L = f_{lL,P}(Q)^{\frac{q^k-1}{l}} = f_{T^a+1,P}(Q)^{\frac{q^k-1}{l}} = f_{T^a,P}(Q)^{\frac{q^k-1}{l}} \quad .$$

Compare the last equality with the similar derivation done for the Ate pairing in Sect. 4.1: let $[n]P = \mathcal{O}$; for Ate we used $f_{n,P} = f_{n+1,P}$, which is always true; here $f_{n,P} = f_{n-1,P} \cdot v_P$ holds, where v_P is the vertical line through P, whose contribution cancels out using the hypothesys of “denominator” elimination.

Again using (6) we reduce the computation of $f_{T^a,P}$ to powers of $f_{T,[T^i]P}$ for $0 \leq i < a$. We have $[T^i]P = \gamma^i(P)$ and by using Prop. 4.ii and Galois invariance (7):

$$\begin{aligned} f_{T,\gamma^i(P)}(Q) &= f_{T,P} \circ \gamma^{-i}(Q) = \\ &= f_{T,P} \circ \gamma^{-i}\left(\psi(\tilde{Q})\right) = f_{T,P}\left(\psi^{\pi^i}(\tilde{Q})\right) = f_{T,P}\left(\psi(\tilde{Q})^{\pi^i}\right) = \\ &= f_{T,P^{\pi^i}}(Q^{\pi^i}) = (f_{T,P}(Q))^{\pi^i} = (f_{T,P}(Q))^{q^{ir}} \quad . \end{aligned}$$

Finally, $T \equiv q^r \bmod l$ allows to replace the last exponent with T^i when raising to the power of $\frac{q^k-1}{l}$. In conclusion we have:

$$t(P,Q)^L = f_{T^a,P}(Q)^{\frac{q^k-1}{l}} = f_{T,P}(Q)^{\frac{q^k-1}{l}aT^{a-1}} \quad ,$$

and we define the algorithms:

$$\eta_T(P,Q) := f_{T,P}(Q)^{\frac{q^k-1}{l}} \qquad \text{and} \qquad \eta(P,Q) := \eta_{q^r}(P,Q) \quad .$$

For $T = \lambda = t_r - 1$ (and $a = k/2$), the algorithms η_T and $\mathsf{a}^{\mathsf{t}}_{\lambda}$ coincide.

Example 2. Let E_3 be defined as in Example 1 and η, η_T as before. The loop size of η is 2^{3m}, which is worse than a direct computation from the definition of Tate pairing using t_N. The loop size of η_T is T, in particular for $T = t_3 - 1 = \mp 2^{(3m+1)/2} - 1$, we have an algorithm with a loop size $O(q^{3/2})$.

4.3 Optimal (Twisted) Ate Pairing

Vercauteren [10] defines the concept of *optimal pairing* and describes an algorithm to compute optimal Ate pairings. Hess [16] extends this framework by (i) allowing for more general pairing functions and (ii) applying it to the Weil pairing; however no better explicit algorithm is given than in [10].

The starting point is again (10). Let $\lambda = lL$ and write $\lambda = \sum_{i=0}^{a} c_i q^i$. Given the vector $[c_0, \ldots, c_a]$, define the following algorithm:

$$\mathsf{a}^{\mathsf{t}}_{[c_0,\ldots,c_a]}(P,Q) := \left(\prod_{i=0}^{a} f_{c_i,P}(Q)^{q^i} \cdot C(P,Q)\right)^{\frac{q^k-1}{l}} \quad ,$$

where $C(P,Q)$ plays the role of a “correction” term and is given by:

$$C(P,Q) = \prod_{i=0}^{a-1} \frac{l_{[s_{i+1}]P,[c_i q^i]P}(Q)}{v_{[s_i]P}(Q)}, \qquad \text{with } s_i = \sum_{j=i}^{a} c_j q^j \quad .$$

Theorem 1 in [10] shows that $\mathsf{a}^{\mathsf{t}}_{[c_0,\ldots,c_a]}(P,Q)$ computes a bilinear pairing and states a condition for non-degeneracy. Furthermore, an algorithm to explicitly derive useful vectors $[c_0, \dots, c_a]$ is given, based on finding short vectors in a proper lattice. Given such a small vector V, we define the algorithm[3]:

$$\mathsf{a}_{\mathrm{opt}}(P,Q) := \mathsf{a}^{\mathrm{t}}_V(P,Q) \ .$$

We illustrate it through an explicit example.

Example 3. This example is similar to the one presented in [10, Sect. 4], related to supersingular elliptic curves with $k = 6$ over $\mathbb{F}_{3^m}$.

Let E_3 be defined as in Example 1. The shortest vector is $V = [v_0, v_1] = [2^{(3m-1)/2}, 2^{(3m-1)/2} \mp 1]$, and "another nice choice" is $W = [2^{(3m+1)/2}, -1]$ that gives the η_T pairing.

We have $l \mid v_0 + v_1 q^3 = 2^{(3m-1)/2} \cdot \left|E(\mathbb{F}_{q^3})\right|$. We consider the algorithm:

$$\mathsf{a}_{\mathrm{opt}} := \mathsf{a}_V = f_{v_0,P}(Q) \cdot f_{v_1,P}(Q)^{q^3} \cdot l_{[v_0]P,[v_1 q^3]P}(Q) \ ;$$

we note that $[v_0]P = -[v_1 q^3]P$, so $l_{[v_0]P,[v_1 q^3]P}$ is actually the vertical line through $[v_0]P$ and we can ignore it because the distortion map allows for denominator elimination.

It remains to show how to efficiently compute the product of the two Miller functions: since $v_1 = v_0 - 1$, by (4) we have $f_{v_1,P}(Q)^{q^3} = f_{v_0,P}(Q)^{q^3} \cdot l_{[v_0]P,[v_0-1]P}$; here we can not avoid the final multiplication because $[v_0]P \neq \mathcal{O}$. In conclusion

$$\mathsf{a}_{\mathrm{opt}} = l_{[v_0]P,[v_0-1]P} \cdot f_{v_0,P}(Q)^{1+q^3} \ , \qquad \text{where } v_0 = 2^{(3m-1)/2} \ .$$

The loop size is $O(2^{(3m-1)/2})$, but a final correction term is required, thus this algorithm is essentially equivalent to η_T.

5 Pairing over Supersingular Trace Zero Varieties

We already presented through examples how to apply the current literature to a particular TZV. We stress the following facts:

1. The presented pairings make use of the q^r-Frobenius $\pi\colon \mathbb{F}_{q^k} \to \mathbb{F}_{q^k},\ x \mapsto x^{q^r}$. They apply not only to points of the TZV, but to the whole $E(\mathbb{F}_{q^r})$.
2. The supersingular curve in the examples is perfectly equivalent from a security perspective to the supersingular curve in characteristic 3 (security parameter 6, small characteristic field); furthermore, since $q = 2^m$ and $t = 2^{(m+1)/2}$, most of the algorithms come with a very efficient (i.e. low Hamming weight) Miller loop; the two pairings η_T and $\mathsf{a}_{\mathrm{opt}}$ achieve the shortest loops.

[3] Actually the property for V to be small is only a necessary condition for the related Ate pairing to be optimal; a detailed discussion is out of the scope of this paper and we refer to the original work for further details.

We now look at how to exploit the action of the Frobenius relative to the base field.

Let $\sigma\colon \mathbb{F}_{q^k} \to \mathbb{F}_{q^k},\ x \mapsto x^q$. From Sect. 2 we already know σ acts on $\mathbb{G}_1$, resp. $\mathbb{G}_2$, as multiplication times s, resp. S. The next lemmas show that, for particular curves, the action of σ can be better explicited and s, S are indeed powers of q (or close to).

Lemma 1 (Supersingular E_3 over $\mathbb{F}_{2^m}$). *Let $E/\mathbb{F}_{2^m}$ (m prime) be a supersingular elliptic curve defined by the Weierstraß equation:*

$$y^2 + y = x^3 + x + b \ , \qquad b \in \mathbb{F}_2 \ ,$$

with embedding degree $h = 4$. Let E_3 be the TZV built upon E and an extension of degree $r = 3$. Then:

$$\sigma(P) = -\left[q^{\frac{r+1}{2}}\right] P = -\left[q^2\right] P \ , \qquad \sigma(Q) = \left[q^{\frac{r^2+1}{2}}\right] Q = \left[q^5\right] Q \ .$$

Proof. We are going to show that $s \equiv -q^{\frac{r+1}{2}}$ and $S \equiv q^{\frac{r^2+1}{2}}$ satisfy their respective defining polynomials (all the equivalences are intended modulo l if not differently specified).

Note that $h = r + 1$. This allows to easily prove that $s^r \equiv 1$ and $S^r \equiv q^r$. For the first: $s^r \equiv -q^{rc/2} = -q^{k/2} \equiv 1$, the last equivalence occurring because k is the smallest integer such that $q^k \equiv 1$. The latter follows since $r \equiv -1 \bmod h$, $\frac{r^2+1}{2} \equiv 1 \bmod h$: $S^r \equiv q^{(1+tc)r} = q^{r+tk} \equiv q^r$, for some integer t.

We now prove that both s and S are roots of $\chi(T)$. Write

$$\chi(s) \equiv \left(q^r + tq^{\frac{r-1}{2}} + 1\right) q \ , \qquad \chi(S) \equiv \left(q^{r^2} - tq^{\frac{r^2-1}{2}} + 1\right) q \ ,$$

and, using (3), note the expressions between brackets are resp. $|E(\mathbb{F}_{q^r})|$ and $\left|E(\mathbb{F}_{q^{r^2}})\right|$, i.e. $t_r = -tq^{\frac{r-1}{2}}$ and $t_{r^2} = tq^{\frac{r^2-1}{2}}$ (this is true in this particular case where $t = \sqrt{2q}$ and $r = 3$). Since $l \mid |E(\mathbb{F}_{q^r})| \mid \left|E(\mathbb{F}_{q^{r^2}})\right|$, both the expressions vanish modulo l and the thesis follows. □

Lemma 2 (Supersingular E_5 over $\mathbb{F}_{3^m}$). *Let $E/\mathbb{F}_{3^m}$ (m prime) be a supersingular elliptic curve defined by the Weierstraß equation:*

$$y^2 = x^3 - x \pm 1 \ .$$

Let E_5 be the TZV built upon E and an extension of degree $r = 5$. Then:

$$\sigma(P) = -\left[q^{\frac{r+1}{2}}\right] P = -\left[q^3\right] P \ , \qquad \sigma(Q) = \left[q^{\frac{r^2+1}{2}}\right] Q = \left[q^{13}\right] Q \ .$$

Proof. The proof proceedes exactly as in Lemma 1. Here again $h = r + 1$, $\chi(s) \equiv q \cdot |E(\mathbb{F}_{q^r})|$ and $\chi(S) \equiv q \cdot \left|E(\mathbb{F}_{q^{r^2}})\right| \bmod l$. □

Lemma 3 (Supersingular E_3 over $\mathbb{F}_p$). *Let $E/\mathbb{F}_p$ ($p > 3$ prime) be a supersingular elliptic curve. Let E_3 be the TZV built upon E and an extension of degree $r = 3$. Then:*

$$\sigma(P) = \left[p^{\frac{r+1}{2}}\right] P = \left[p^2\right] P \ , \qquad \sigma(Q) = \left[p^{\frac{r^2+1}{2}}\right] Q = \left[p^5\right] Q \ .$$

Proof. Since $t = 0$ we proceed by direct computation:

$$\begin{aligned} s &\equiv p - 1 \equiv p^2 = \left[p^{\frac{r+1}{2}}\right] P \ , \\ S &\equiv (p - p^2)/p \equiv 1 - p \equiv p^5 = p^{\frac{r^2+1}{2}} \ . \end{aligned}$$

□

In what follows, we assume that E is one of the curves defined in Lemma 1, 2 or 3 and we adopt the following common notation:

$$\sigma(P) = \left[\pm q^{\frac{r+1}{2}}\right] P \ , \qquad \sigma(Q) = \left[q^{\Sigma}\right] Q \ .$$

The next lemma describes the action $\hat{\sigma}$, the dual of the Frobenius endomorphism σ. Our main theorem will then follow.

Lemma 4. *Let E_r be a TZV as in Lemma 1, 2 or 3. Let $\hat{\sigma}$ be the dual of the Frobenius endomorphism σ. Then:*

$$\hat{\sigma}^i(P) = \left[\left(qs^{-1}\right)^i\right] P \ , \qquad \hat{\sigma}^i(Q) = \left[q^{i(1-\Sigma)}\right] Q \ .$$

Moreover $\hat{\sigma}^{r+2}(P) = [q]P$.

Proof. Let $X \in E[l]$ and suppose $\sigma(X) = [z]X$ for some $z \in \mathbb{Z}_l^*$. Then:

$$\hat{\sigma} \colon X \mapsto (X) - (\mathcal{O}) \mapsto q\left(\sigma^{-1}(X)\right) - q\left(\mathcal{O}\right) = \left(\left[qz^{-1}\right] X\right) - (\mathcal{O}) \mapsto \left[qz^{-1}\right] X \ ,$$

and $\hat{\sigma}^i(X) = \left[\left(qz^{-1}\right)^i\right] X$. This proves the first result on $\hat{\sigma}^i(P)$, resp. $\hat{\sigma}^i(Q)$, setting $X = P,\ z = s$, resp. $X = Q,\ z = S = q^{\Sigma}$.

Using this result, we have $\hat{\sigma}^{r+2}(P) = [q]P$ if and only if $\left(qs^{-1}\right)^{r+2} \equiv q \bmod l$ if and only if $q^{r+1} \equiv s^{r+2} \equiv s^2 \bmod l$, and this is true in force of Lemmas 1, 2 and 3. □

Theorem 1. *Let E_r be a TZV as in Lemma 1, 2 or 3. Then there exist a j, $0 \le j < k$, such that:*

$$\left(\hat{\sigma}^{r+2} \circ \sigma^j\right)(Q) = Q \qquad \text{for every } Q \in \mathbb{G}_2 \ ,$$

and:

$$f_{n,[s]P}(Q) = f_{n,P}\left(Q^{\sigma^{-1}}\right)^{\sigma} = f_{n,P}\left(\left[q^{k-\Sigma}\right] Q\right)^q \tag{11}$$

$$f_{n,[q]P}(Q) = f_{n,P}\left(Q^{\sigma^j}\right)^{q^{r+2}} = f_{n,P}\left(\left[q^{j\Sigma}\right] Q\right)^{q^{r+2}} \tag{12}$$

Proof. Equation (11) comes from $[s]P = P^{\sigma}$ and (7); the last equality gives an explicit result but is of no practical use.
For (12) we have:

$$f_{n,[q]P}(Q) = f_{n,\hat{\sigma}^{r+2}(P)}\left((\hat{\sigma}^{r+2} \circ \sigma^j)(Q)\right) = f_{n,\hat{\sigma}^{r+2}(P)} \circ \hat{\sigma}^{r+2}\left(Q^{\sigma^j}\right) =$$

$$= f_{n,P}\left(Q^{\sigma^j}\right)^{q^{r+2}} = f_{n,P}\left(\left[q^{j\Sigma}\right]Q\right)^{q^{r+2}} \quad ,$$

where the first equality follows by Lemma 4 and the third by Prop. 4.i by setting $\phi = \hat{\sigma}^{r+2}$.

It remains to show that such a j exists. Using the previous lemmas, we can rewrite $\left(\hat{\sigma}^{r+2} \circ \sigma^j\right)(Q) = Q$ as:

$$q^{(r+2)(1-\Sigma)} \cdot q^{j\Sigma} \equiv 1 \bmod l \quad ,$$

which holds if and only if

$$(r+2)(1-\Sigma) + j\Sigma \equiv 0 \bmod k \quad .$$

In our setting Σ is invertible modulo k and such a j can be found. Explicitly we get $j \equiv 4 \bmod k$, resp. $j \equiv 18$, for $r = 3$, resp. $r = 5$. □

We now use the results of Theorem 1 to derive a new algorithm for computing the Tate pairing.

Theorem 2. *Let E_r be a TZV as in Lemma 1, 2 or 3, so k is even; assume the distortion map allows for denominator elimination. Then the Tate pairing can be computed as:*

$$t(P,Q) = \left(\prod_{i=0}^{r-1} f_{q,P}\left(Q^{\sigma_i}\right)^{q^{i(r+1)}}\right)^{M\frac{a}{r}q^{a-1}} \quad , \tag{13}$$

where $\sigma_i = \sigma^{ij}$ (j given in Theorem 1), $a = k/2$ and $M = q^{k/2} - 1$.

Proof. Since k is even, we have $l \mid q^k - 1 = (q^{k/2}-1)(q^{k/2}+1)$ and, by minimality of k, $l \mid q^{k/2}+1$. Hence:

$$t(P,Q) = f_{l,P}(Q)^{(q^k-1)/l} = f_{q^{k/2}+1,P}(Q)^{q^{k/2}-1} = f_{q^{k/2},P}(Q)^{q^{k/2}-1} \quad ,$$

where for the last equality we use the hypotesys that the distortion map allows for denominator elimination (similarly as in Sect. 4.2). Set $a = k/2$, $M = q^{k/2}-1$. Exploiting (6) we reduce a single loop on q^a in a loops on q; moreover, the action of the r-th power of the Frobenius π allows to pack them into r distinct loops working resp. with $P, [q]P, \ldots, [q^{r-1}]P$:

$$f_{q^a,P}(Q)^M = \left(f_{q,P}(Q)^{q^{a-1}} \cdot f_{q,[q]P}(Q)^{q^{a-2}} \cdots f_{q,[q^{a-1}]P}(Q)\right)^M =$$

$$= \left(f_{q,P}(Q)^{\frac{a}{r}q^{(a-1)}} \cdot f_{q,[q]P}(Q)^{\frac{a}{r}q^{(a-2)}} \cdots f_{q,[q^{r-1}]P}(Q)^{\frac{a}{r}q^{(a-r)}}\right)^M =$$

$$= \left(f_{q,P}(Q) \cdot f_{q,[q]P}(Q)^{q^{-1}} \cdots f_{q,[q^{r-1}]P}(Q)^{q^{-(r-1)}}\right)^{M\frac{a}{r}q^{a-1}} \quad .$$

We have proved that:

$$t(P,Q) = \left(\prod_{i=0}^{r-1} f_{q,[q^i]P}\left(Q\right)^{q^{-i}} \right)^{M \frac{a}{r} q^{a-1}} \quad .$$

Using (12) from Theorem 1, we have:

$$f_{q,[q^i]P}\left(Q\right)^{q^{-i}} = f_{q,P}\left(Q^{\sigma^{ij}}\right)^{q^{-i+i(r+2)}} = f_{q,P}\left(Q^{\sigma_i}\right)^{q^{i(r+1)}} \quad ,$$

and the thesis follows. □

The previous theorem suggests a new algorithm to compute the Tate pairing over supersingular TZV: perform a single Miller loop on P and evaluate it at the r points Q^{σ_i} (raising each evaluation to the proper power $q^{i(r+1)}$). In the end compute the final exponentiation to $M\frac{a}{r}q^{a-1}$.

We first deal with the final exponentiation to $M\frac{a}{r}q^{a-1}$. Power to (i) M is computed as a power of the (r-th power of the) Frobenius and a division; (ii) q^{a-1} is again done exploiting the Frobenius; (iii) $\frac{a}{r}$ is as well efficient, being resp. 2, 3, 1 for the TZV of our interest. If we avoid the two last exponentiations, we still get a bilinear pairing.

Each iteration in the Miller loop requires a point doubling in $E(\mathbb{F}_{q^r})$ and r multiplications in $\mathbb{F}_{q^k}$ (we avoid from the count the exponentiations, obtained exploiting the Frobenius). A number of techniques have been described to carry out efficiently these operations, see for instance [6].

The algorithm results less efficient, for instance, than η_T or a_{opt}. However a parallel implementation would be straightforward, requiring r processors and achieving a loop of length q.

Moreover, both in a parallel and in a sequential model, an implementation with precomputation of the multiples of P requires the storage of only q points.

Remark. Equation (11) might also be exploited to derive an algorithm reducing a loop on $s^{r-1} + \cdots + s + 1$ in $r-1$ loops on s. The result is similar to the use of the endomorphism in NSS curves [11]. This approach does not seem interesting because s is generally too big. The best case is in characteristic 2 for $r = 3$: $s = O\left(q^{3/2}\right)$, and the resulting algorithm (even assuming the two loops can be "packed" in some way) can not be better than η_T or a_{opt}.

6 Supersingular Elliptic Curve in Characteristic 2

We conclude with an explicit example in characteristic 2 and we provide some experimental results. We take advantage of this section to fix an oversight in the Silverberg's point compression algorithm [19,5].

Through this section, `S`, `M`, `H` denote resp. square, multiplication and solution of quadratic equation (of the form $y^2 + y + C = 0$, i.e. half-trace computation) in $\mathbb{F}_{q^r}$; `s`, `m`, `h`, `r`, `i` denote resp. square, multiplication, solution of quadratic equation, square root and inversion in $\mathbb{F}_q$.

6.1 A Worked out Example

Let E be the curve defined in Example 1.
As in [4], we set $\mathbb{F}_{q^3} = \mathbb{F}_q[T]/(T^3 + T + 1)$. We use the same distortion map as in [6], but we prefer the more efficient representation for $\mathbb{F}_{q^{12}}$ as $\mathbb{F}_{q^3}[T]/(T^4 + T + 1) = \mathbb{F}_{q^3}(\alpha)$. Let $P = (x_P, y_P), \tilde{Q} = (x_{\tilde{Q}}, y_{\tilde{Q}}) \in E(\mathbb{F}_{q^3})$ be points of order l. Let $\phi\colon \mathbb{F}_{q^3} \to \mathbb{F}_{q^{12}},\ \tilde{Q} \mapsto Q = (x_Q, y_Q)$ be a distortion map, with:

$$\begin{aligned} x_Q &= x_{\tilde{Q}} + \alpha + \alpha^2 \\ y_Q &= y_{\tilde{Q}} + x_{\tilde{Q}} + x_{\tilde{Q}}\alpha + (x_{\tilde{Q}} + 1)\alpha^2 \ . \end{aligned}$$

Then $Q \in E[l] \setminus E(\mathbb{F}_{q^3})$.

Recall that $\pi = \sigma^3$ acts in the usual way, i.e. fixes P and sends Q in $[q^3]Q$. We have, for σ:

$$P^\sigma = (x_P^q, y_P^q) = [s]P \qquad\qquad \begin{aligned} Q^\sigma &= (x_Q^q, y_Q^q) = [q^5]Q \\ &\big(= \psi(x_{\tilde{Q}}^q + 1, y_{\tilde{Q}}^q + x_{\tilde{Q}}^q + 1)\big) \ . \end{aligned}$$

Remember from Theorem 1 (cf. end of the proof) that we will need to compute $Q_i = Q^{\sigma^{4i}}$, for $i = 0, 1, 2$. It is easy to check that $Q_i = \psi\left(\tilde{Q}^{\sigma^i}\right)$.

Now we turn the attention to the computation within the Miller loop: since we perform a loop on $q = 2^m$, we only consider doublings. Let $T = (x_T, y_T) \in E(\mathbb{F}_{q^3})$ denote the point which is accumulated during the loop. Let λ the slope of the line l_{2T} (for the curve of interest, $\lambda = x_T^2 + 1$). At each iteration we have to compute $l_{2T}(Q_i) = \lambda(x_T + x_i) + y_T + y_i$, where $(x_i, y_i) = \psi\left(\tilde{Q}^{\sigma^i}\right)$. Due to the special choice of the distortion map, $l_{2T}(Q_i) = a_i + b_i\alpha + (b_i + 1)\alpha^2$ for some $a_i, b_i \in \mathbb{F}_{q^3}$.

Recall in our algorithm (cf. Theorem 2) we have to compute three independent contributions, namely:

$$f_{q,P}(Q), \qquad f_{q,P}\left(Q^{\sigma^4}\right)^{q^4}, \qquad f_{q,P}\left(Q^{\sigma^8}\right)^{q^8} \ .$$

Note that if $x \in \mathbb{F}_{q^{12}}$, $x = \sum_{i=0}^{3} x_i\alpha^i$ with $x_i \in \mathbb{F}_{q^3}$, then $x^{q^4} = \sum_{i=0}^{3} x_i^q\alpha^i$. We finally explicit the computation at each iteration of the Miller loop:

$$l_{2T}(Q_i)^{q^{4i}} = a_i^{q^i} + b_i^{q^i}\alpha + \left(b_i^{q^i} + 1\right)\alpha^2 \ .$$

The computation of each a_i requires 1M and doubling the point T is for free since $[2]T = (x_T^4 + 1, y_T^4 + x_{2T})$. Accumulating each contribution costs 6M: we have to compute products of the form:

$$\left(f_0 + f_1\alpha + f_2\alpha^2 + f_3\alpha^3\right)\left(x_0 + x_1\alpha + (x_1 + 1)\alpha^2\right) \ .$$

Let $t = \sum_{i=0}^{5} t_i \alpha^i$ be such a product (as polynomial). Then:

$$\begin{aligned} t_0 &= M_0 & t_3 &= M_3 + M_5 + f_1 \\ t_1 &= M_0 + M_1 + M_2 + M_3 & t_4 &= M_1 + f_2 \\ t_2 &= M_0 + M_2 + M_3 + M_4 + M_5 + f_0 & t_5 &= M_4 + f_3 \ , \end{aligned}$$

where:

$$\begin{aligned} M_0 &= f_0 x_0 & M_3 &= (f_1 + f_2 + f_3) x_0 \\ M_1 &= (f_2 + f_3) x_1 & M_4 &= f_3 x_1 \\ M_2 &= (f_0 + f_2 + f_3)(x_0 + x_1) & M_5 &= (f_1 + f_2)(x_0 + x_1) \ . \end{aligned}$$

Finally the reduction modulo $\alpha^4 + \alpha + 1$ can be done with a few additions. Note this is the approach proposed in [6], up to our isomorphic representation of $\mathbb{F}_{q^{12}}$.

A Tate pairing can thus be computed in roughly $3 \times 7m\mathtt{M}$. A point halving based approach as in [6] might also be used.

6.2 Experimental Results

We have implemented the algorithms presented in Sect. 4 and the one described in the previous section in C language: the arithmetic over the ground field $\mathbb{F}_q$ is described in [20] and over the extension field $\mathbb{F}_{q^r}$ in [4]. We perform experiments on an Intel Core2 2GHz with the Intel C Compiler 10.1; all the implementations run on a single core (i.e. no parallel implemetations have been done).

Table 1 shows our experimental results for the curve defined in Example 1 for $m = 103$, compared with their theoretical complexity. We recall the notation introduced in Sect. 4: t_l, resp. t_N, computes the Tate pairing using the definition with a loop on l, resp. N; η and η_T are the Eta and Eta$_T$ pairings defined in [6]; a_{opt} is the optimized Ate pairing [10]. We also include t_σ that computes the Tate pairing exploiting the $q-$Frobenius σ as in [11]; finally t_{TZV} refers to our new algorithm as detailed in Sect. 6.1.

Table 1. Timing of different pairings algorithms (§§ 4, 6.1) for the TZV $E_3/\mathbb{F}_{2^{103}} : y^2 + y = x^3 + x + 1$ (time in ms).

Pairing	Loop Size	Core2
t_l	$l = O(q^2)$	3.318
t_N	$N = O(q^2)$	2.234
η	q^3	2.659
η (Halving)	q^3	2.557
η_T	$2^{(3m+1)/2} - 1$	1.436
η_T (Halving)	$2^{(3m+1)/2} - 1$	1.371
a_{opt}	$2^{(3m-1)/2}$	1.408
t_σ	$2 \times s$	3.281
t_{TZV}	$3 \times q$	2.517

For each of the η and η_T we provide two implementations: the former uses essentially the same Miller loop as the other algorithms, the latter (Halving) exploits all the tricks described in [6], including a point halving based iteration within the Miller loop. The tricks make the implementation harder (for η_T much more than for η), but the gain is limited, less than 4% in our experiments.

As expected, our new algorithm $\mathtt{t}_{\mathrm{TZV}}$ performs almost like η (3 loops on q against a single loop on q^3). As already noted, it has indeed better properties for parallelization and/or storage requirements.

The best algorithms are η_T and $\mathsf{a}_{\mathrm{opt}}$.

6.3 Point Compression on TZV

In [19], Silverberg presents an algorithm for point compression over TZV.

Classical point compression over elliptic curves allows to compress a point $P = (x, y)$ by dropping the y-coordinate and to recover, or decompress, it by solving a quadratic equation (up to a sign ambiguity). For supersingular curves in characteristic 2 (cf. Lemma 1), this requires to compute $C = x^3 + x + b$ and solve $y^2 + y + C$. The total cost is $1\mathtt{S} + 1\mathtt{M} + 1\mathtt{H}$.

For a TZV, $P \in E_r \subset E(\mathbb{F}_{q^r})$. So $x \in \mathbb{F}_{q^r}$ can be seen as a vector in $\mathbb{F}_q^r$, whose coordinates are not independent; it is possible to exploit such a dependency to compress x to a vector in $\mathbb{F}_q^{r-1}$.

In this section we briefly introduce Silverberg's algorithm and we present a more detailed analysis in characteristic 2 which results in a improved algorithm. We refer to [19,5] for more details.

Since $P + \sigma(P) + \cdots + \sigma^{r-1}(P) = \mathcal{O}$, there exists a function $F(X, Y)$ with zeros of order 1 in $P, \sigma(P), \ldots, \sigma^{r-1}(P)$ and a pole of order r at $\mathcal{O}$. Let $\tilde{F}(X, Y) = -F(-P)$. The function $\prod_{i=0}^{r-1} X - \sigma^i(s)$ vanishes at $\pm P, \pm\sigma(P), \ldots, \pm\sigma^{r-1}(P)$, hence we have:

$$\gamma F(X,Y)\tilde{F}(X,Y) = \prod_{i=0}^{r-1} X - \sigma^i(s) \ , \qquad \gamma \in \mathbb{F}_q^* \ . \tag{14}$$

Expliciting (14) in the case of an elliptic curve given by (1) and $r = 3$ (and assuming $\mathbb{F}_{q^3} = \mathbb{F}_q[T]/(T^3 + T + 1)$), we get the following system of 3 equations:

$$\begin{aligned} \alpha_1^2 + a_1\alpha_1 + a_2 &= s_0 \\ a_1\alpha_0 + a_3\alpha_1 + a_4 &= s_0^2 + s_1^2 + s_1 s_2 + s_2^2 \\ \alpha_0^2 + a_3\alpha_0 + a_6 &= s_0^3 + \left(s_1^2 + s_1 s_2 + s_2^2\right) s_0 + s_1^3 + s_1 s_2^2 + s_2^3 \ . \end{aligned} \tag{15}$$

With proper reductions and for supersingular curves, i.e. $a_1 = a_2 = 0$, (15) becomes:

$$s_0^4 + s_0 a_3^2 + s_1^4 + s_1^2 s_2^2 + s_2^4 + a_4^2 = 0 \ ,$$

which is a bi-quadratic equation in s_1 (or s_2).

In [19], Silverberg proposes to set s_1 as indeterminate and therefore to solve:

$$s_1^2 + s_2 s_1 + K \ , \qquad K = (s_0 + s_2)^2 + a_3\sqrt{s_0} + a_4 \ .$$

Unfortunately the equation is not in the "canonical" form $y^2+y+C=0$, and this requires extra work when computing the solutions. In fact the cost is $1\mathtt{s}+1\mathtt{r}+1\mathtt{m}$ to compute the constant term K, $1\mathtt{s}+1\mathtt{m}+1\mathtt{i}$ to transform to an equation of the form y^2+y+C, $1\mathtt{h}$ to solve the equation and finally $1\mathtt{m}$ to recover the solution s_1.

We can improve the algorithm, in particular avoid the inversion, by taking s_0 as indeterminate (denoted x), under the assumption that $a_3 = 1$[4]. This leads to the equation:

$$x^4+x+C \quad , \qquad C = \left(s_1^2+s_1s_2+s_2^2+a_4\right)^2 \quad , \tag{16}$$

that can be reduced to a system of two quadratic equations: $x^2+x=y$ and $y^2+y+C=0$, since $x^4+x+C = \left(x^2+x\right)^2+(x^2+x)+C$. Note that in $\mathbb{F}_q$, with $q=2^k$ and k odd, equation (16) only admits two solutions.

The compression of the point $P=(s,t)$ is done by 1) dropping the coordinate s_0 and 2) computing the extra bit needed to distinguish s_0 by the other solution of (16). If s_0 is a solution x^2+x+y for some y, then s_0+1 is the other one. Hence the extra bit can be the LSB in the binary representation of s_0. The compression algorithm is for free.

Decompressing a pair $(s_1,s_2) \in \mathbb{F}_q^2$ can be done by solving equation (16): first compute a solution $\bar{y}$ of y^2+y+C; if $\operatorname{Tr}(\bar{y})=0$ then solve $x^2+x+\bar{y}$, otherwise solve $x^2+x+\bar{y}+1$ ($\bar{y}+1$ is the other solution); in both cases we come with two candidates for s_0 and we have to select the one having the LSB equal to the extra bit received. The total cost is $2\mathtt{s}+1\mathtt{m}$ to compute the constant term C and $2\mathtt{h}$ to solve the quartic equation (reduced as two quadratic equations).

7 Conclusion

We revisit the work of Rubin and Silverberg [5] on pairing computation over supersingular trace zero varieties defined over elliptic curves: we survey the available algorithms in literature and we derive a new algorithm for computing the Tate pairing $t(P,Q)$ exploiting the action of the q-Frobenius endomorphism (other works only considered the q^r-Frobenius).

Despite the new algorithm is less efficient than the best available algorithms, it is suitable for a parallel implementation, requiring r processors and achieving a Miller loop of length q for $E_r/\mathbb{F}_q$. Moreover, both in a parallel and in a sequential computational model, an implementation with precomputation of the multiples of P requires the storage of only q points.

We also propose a variant of the Silverberg's point compression algorithm in characteristic 2 which is more efficient and requires no inversion.

[4] the assumption is satisfied for the supersingular elliptic curves with Weierstraß equation $y^2+y=x^3+x+b$, $b \in \mathbb{F}_q$.

References

1. Rubin, K., Silverberg, A.: Supersingular abelian varieties in cryptology. In: CRYPTO '02: Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology, London, UK, Springer-Verlag (2002) 336–353
2. Frey, G.: How to disguise an elliptic curve. Talk at Waterloo workshop on the ECDLP (1998) `http://www.cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html`.
3. Avanzi, R.M., Lange, T.: Cryptographic Applications of Trace Zero Varieties. (2004) Submitted.
4. Avanzi, R., Cesena, E.: Trace Zero Varieties over Fields of Characteristic 2 for Cryptographic Applications. In Hirschfeld, J., Chaumine, J., Rolland, R., eds.: Algebraic geometry and its applications. Volume 5 of Number Theory and Its Applications., World Scientific (2008) 188–215 Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.
5. Rubin, K., Silverberg, A.: Using abelian varieties to improve pairing-based cryptography. To appear in Journal of Cryptology (2008)
6. Barreto, P.S., Galbraith, S.D., Héigeartaigh, C.O., Scott, M.: Efficient pairing computation on supersingular Abelian varieties. Designs, Codes and Cryptography **42**(3) (2007) 239–271
7. Hess, F., Smart, N.P., Vercauteren, F.: The Eta Pairing Revisited. IEEE Transactions on Information Theory **52** (2006) 4595–4602
8. Matsuda, S., Kanayama, N., Hess, F., Okamoto, E.: Optimised versions of the Ate and Twisted Ate Pairings. In: The 11th IMA International Conference on Cryptography and Coding. Volume 4887 of Lecture Notes in Computer Science., Springer-Verlag (2007) 302–312
9. Lee, E., Lee, H.S., Park, C.M.: Efficient and Generalized Pairing Computation on Abelian Varieties. Cryptology ePrint Archive, Report 2008/040 (2008)
10. Vercauteren, F.: Optimal Pairings. Cryptology ePrint Archive, Report 2008/096 (2008)
11. Scott, M.: Faster Pairings Using an Elliptic Curve with an Efficient Endomorphism. In: INDOCRYPT 2005. Volume 3797 of Lecture Notes in Computer Sciences., Springer-Verlag (2005) 258–269
12. Avanzi, R.M., Cohen, H., Doche, C., Frey, G., Lange, T., Nguyen, K., Vercauteren, F.: Handbook of Elliptic and Hyperelliptic Curve Cryptography. CRC Press (2005)
13. Frey, G., Rück, H.G.: A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Mathematics of Computation **62**(206) (1994) 865–874
14. Miller, V.: Short programs for functions on curves. (1986)
15. Silverman, J.H.: The arithmetic of elliptic curves. Volume 106 of Graduate texts in mathematics. Springer (1986)
16. Hess, F.: Pairing Lattices. In Galbraith, S.D., Paterson, K.G., eds.: Pairing 2008. Volume 5209 of Lecture Notes in Computer Science., Springer-Verlag (2008) 211–224
17. Zhao, C.A., Zhang, F., Huang, J.: A Note on the Ate Pairing. Cryptology ePrint Archive, Report 2007/247 (2007)
18. Scott, M.: Faster identity based encryption. Electronics Letters **40**(14) (July 2004)
19. Silverberg, A.: Compression for Trace Zero Subgroups of Elliptic Curves. In: Trends in Mathematics. Volume 8. (2005) 93–100 Proceedings of the Daewoo Workshop on Cryptography.

20. Avanzi, R.M., Thériault, N.: Effects of Optimizations for Software Implementations of Small Binary Field Arithmetic. In: WAIFI 2007. LNCS volume 4547, Springer (2007) 69–84