A Note on the Advanced Use of the Tate Pairing

Krijn Reijnders*

COSIC, KU Leuven, Belgium
crypto.krijn@gmail.com

Abstract. This short note explains how the Tate pairing can be used to efficiently sample torsion points with precise requirements, and other applications. These applications are most clearly explained on Montgomery curves, using the Tate pairing of degree 2, but hold more generally for any degree or abelian variety, or even generalized Tate pairings, as long as we have non-degeneracy. This note is explanatory in nature; it does not contain new results, but aims to provide a clear and concise explanation of results in the literature that are somewhat hidden, yet are extremely useful in practical isogeny-based cryptography.

This note explains the use of *profiles* of Tate pairings, generalizing some results in the literature. In short, the Tate pairing allow us to study the fibers $\varphi^{-1}(P)$ of an isogeny φ. For scalar multiplication $[n]$, this allows us to study divisibility of points and therefore to find rational points of order ℓ^k. Many applications in isogeny-based cryptography use such results, especially for $\ell = 2$.

However, the general derivation of these divisibility results is hidden in the literature, and not easy to find. We go over several results, both for elliptic curves and Jacobians of hyperelliptic curves, and reframe them using (profiles of) Tate pairings. The core theoretical framework is by Robert [16], which explains the study of fibers $\varphi^{-1}(P)$ in detail.[1] Work by Bruin [2] explains the generalization of the Tate pairing, and work by Corte-Real Santos and me [7] develops more tools that fit into this framework, and applies profiles to 2-dimensional Jacobians.

We first look at classical results on divisibility by the [2]-map, described in elementary terms. We then introduce the concept of profiles to unify these results. After that, we look at some other applications of divisibility using Tate pairings in genus 1 and 2, and the study of fibers of generalized Tate pairings for specific cases. To simplify exposition, we restrict ourselves to non-degenerate Tate pairings for elliptic curves over finite fields, and sometimes principally polarized abelian surfaces or varieties. We hope that this note inspires others to think in terms of profiles of generalized Tate pairings whenever results require certain divisibility properties, or simply more extravagant use of the Tate pairing.

[1] Sections 3 and 4 of [16] are heavy in algebraic geometry, however, many of the useful applications in its Section 5 can be understood in the traditional interpretation!

*This work was supported in part by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement ISOCRYPT - No. 101020788), by the Research Council KU Leuven grant C14/24/099 and by CyberSecurity Research Flanders with reference number VR20192203. Date of this document: 2025-03-13.

1 Divisibility results

Many results on the divisibility of points are Tate pairings in disguise [16, Sec. 5.2]. An easy, yet surprisingly useful result is the following classical theorem.

Theorem 1. *[12] Let E be an elliptic curve over a finite field $\mathbb{F}_q$ with $\mathbb{F}_q$-rational 2-torsion, given in short Weierstrass form as*

$$E : y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3), \quad \lambda_i \in \mathbb{F}_q.$$

Then $P \in [2]E$ if and only if $x_P - \lambda_i$ is a square in $\mathbb{F}_q$ for $i = 1, 2, 3$.

As the quadratic character of $(x_P - \lambda_i)$ is precisely the 2-Tate pairing

$$t_2 : E[2](\mathbb{F}_{p^2}) \times E(\mathbb{F}_{p^2})/[2]E(\mathbb{F}_{p^2}) \to \{1, -1\} \tag{1}$$

of $(\lambda_i, 0)$ with P, this result is equivalent to the non-degeneracy of the 2-Tate pairing: a point $P \in E$ has trivial 2-Tate pairings with all points in $E[2]$ must be in the trivial equivalence class of $E(\mathbb{F}_{p^2})/[2]E(\mathbb{F}_{p^2})$, hence $P \in [2]E(\mathbb{F}_{p^2})$.

This theorem finds immediate applications in isogeny-based cryptography using Montgomery curves of the form $E_A : y^2 = x^3 + Ax^2 + x$, where we take $\lambda_1 = 0$. In this case, whenever x_P is non-square for some $P \in E(\mathbb{F}_q)$, we must have $P \in E \setminus [2]E$. When E_A is maximal supersingular and $2^f \mid p + 1$, any $P \in E \setminus [2]E$ has order divisible by 2^f. We can therefore efficiently sample a point P of order 2^f by sampling a non-square $x_P \in \mathbb{F}_q$ and checking if it is a point on E_A, then setting $P \leftarrow [\frac{p+1}{2^f}]P$.

Two results generalize this approach to easily obtain a basis (P, Q) for $E[2^f]$ instead of only a point $P \in E[2^f]$. First, Zanon, Simplicio, Pereira, Doliskani, and Barreto [18] show that by choosing x_P carefully, we can immediately obtain a suitable x_Q to complete the torsion basis.

Lemma 1. *Let E_A be a maximal supersingular Montgomery curve over $\mathbb{F}_{p^2}$ with $p = 2^f \cdot h - 1$ for $f \in \mathbb{N}$ and some cofactor h, and $A \neq 0$. Let $x_P = -A/(1 + t^2)$ be the x-coordinate of a point $P \in E(\mathbb{F}_{p^2})$, where $t \in \mathbb{F}_{p^2}$ is a non-square chosen so that x_P is also non-square.*

Then $x_Q = -x_P - A$ is the x-coordinate of a point $Q \in E(\mathbb{F}_{p^2})$, and $([h]P, [h]Q)$ is a basis for $E[2^f]$.

Second, Theorem 2 of AprèsSQI [6] shows that the quadratic characters of $(x - \lambda_i)$ contain precise information on points $P \in E[2^f]$.

Lemma 2. *Let E_A be a maximal supersingular Montgomery curve over $\mathbb{F}_{p^2}$ with $p = 2^f \cdot h - 1$, written as $E_A : y^2 = x(x - \alpha)(x - 1/\alpha)$. Let $T_0 = (0, 0)$, $T_1 = (\alpha, 0)$, and $T_2 = (1/\alpha, 0)$ be the 2-torsion points of E_A. Let $P \in E[2^f]$, then*

$$[2^{f-1}]P = T_i \quad \Leftrightarrow \quad t_2(T_i, P) = 1 \text{ and } t_2(T_j, P) = -1 \text{ for } j \neq i.$$

This implies that we can determine the 2-torsion point that P is above by computing only three Tate pairings!

All these results have one thing in common, which will be key to understanding the usefulness of the Tate pairing: they require us to compute multiple Tate pairings for the same point! In the next section, we give a natural interpretation, which unifies these results and allows us to expand our Tate toolkit.

2 Profiles of Tate pairings

Assuming $\mu_n \subset \mathbb{F}_q^*$, the (reduced) Tate pairing t_n of degree n over $\mathbb{F}_q$ for an elliptic curve E is a non-degenerate pairing [2]

$$t_n : E[n](\mathbb{F}_q) \times E(\mathbb{F}_q)/[n]E(\mathbb{F}_q) \to \mu_n.$$

As Robert [16] notes, it also makes sense to view the Tate pairing of a point $P \in E(\mathbb{F}_q)$ when evaluated in all of $E[n]$. This gives a map which we denote $t_{[n]}$, which we describe in terms of the kernel points $K_i \in E[n]$:

$$t_{[n]} : E(\mathbb{F}_q) \to \mu_n^m, \quad P \mapsto (t_n(K_1, P), \ldots, t_n(K_m, P))$$

We call the image $t_{[n]}(P)$ the *n-profile* of P under the Tate pairing. Non-degeneracy now implies that $t_{[n]}$ is trivial precisely when $P \in [n]E(\mathbb{F}_q)$. In other words, when viewing the codomain as $E(\mathbb{F}_q)/[n]E(\mathbb{F}_q)$, the map $t_{[n]}$ is injective [16, Cor. 5.2]. This gives a neat explanation of Theorem 1: for degree $n = 2$, the quadratic characters of the three values $(x - \lambda_i)$ become the 2-profile $t_{[2]}(P)$, and the trivial profile $(1, 1, 1)$ indicates $P \in [2]E$. The two generalizations Lemmas 1 and 2 have similar interpretations using profiles. For clarity, we begin with Lemma 2, and use this understanding for Lemma 1.

Example 1. Lemma 2 essentially shows that the profile of P determines the coset of $E(\mathbb{F}_q)/[2]E(\mathbb{F}_q)$ in which P lies! This allows for an even broader implementation: Any basis (P, Q) for $E[2^f]$ must have P and Q in different, non-trivial, cosets of $E(\mathbb{F}_q)/[2]E(\mathbb{F}_q)$. In simpler terms, if we want a basis P, Q for $E(\mathbb{F}_q)[2^f]$, we need two points P and Q with different non-trivial profiles $t_{[2]}(P)$ and $t_{[2]}Q$.

Example 2. From this point of view, Lemma 1 becomes remarkable: by the choice of x_P as a non-square, we get that P has a non-trivial profile. Hence, $t_{[2]}(P)$ is either $(-1, 1, -1)$ or $(-1, -1, 1)$. And the clever choice of x_Q as $-x_P - A$ ensures two things: First, x_Q is non-square and defines a point $Q \in E$. Second, this choice determines the quadratic character of $x_Q - \alpha$ and $x_Q - 1/\alpha$, by

$$x_Q - \alpha = -x_P - A - \alpha = -x_P + \alpha + 1/\alpha - \alpha = -(x_P - 1/\alpha),$$

where we use that $A = -\alpha - 1/\alpha$. Thus, this choice of x_Q ensure that the profile of Q is either $(-1, -1, 1)$ or $(-1, 1, -1)$ and different from the profile of P, hence ensuring a basis for $E[2]$.[2]

2.1 Rational torsion.

The Tate pairing $t_{[n]}$ is especially intuitive when $E[n] \subset E(\mathbb{F}_q)$: given a basis P, Q, we first note that the profile of a point R is determined by $(t_n(P, R), t_n(Q, R))$ already. And in fact, viewing $t_{[n]}(R)$ as determined by a basis P, Q is the 'correct'

[2] We thank Damien Robert for explaining entangled basis generation in this way.

interpretation, as the map $t_{[n]} : E(\mathbb{F}_q)/[n]E(\mathbb{F}_q) \to \mu_n^2$ becomes an isomorphism! We find a genus-1 example of [7, Lem. 6],

$$E[n] \xrightarrow{\sim} E(\mathbb{F}_q)/[n]E(\mathbb{F}_q) \xrightarrow{\sim} \mu_n^2.$$

One should be careful not to misunderstand the depth of the above isomorphisms: They show us that (profiles of) the Tate pairing determines cosets in $E/[n]E$, and this is *everything* the Tate pairing does, as it has no more information to give. In other words, the Tate pairing allows us to decompose $E(\mathbb{F}_q)$ in cosets, where the size of $E[n](\mathbb{F}_q)$ determines the number of cosets and hence the precision of our decomposition of $E(\mathbb{F}_q)$.

3 Sampling generators for the $\ell^\bullet$-torsion

So far, we have restricted ourselves to curves E with 'nice' $2^\bullet$-torsion $E[2^\infty](\mathbb{F}_q) \cong \mathbb{Z}_{2^f} \times \mathbb{Z}_{2^f}$. But the Tate pairing has a useful connection with the more general $\ell^\bullet$-torsion, more aptly named the Sylow-ℓ subgroup $E[\ell^\infty](\mathbb{F}_q)$, where $\ell \neq p$ prime.[3] We will denote the Sylow-ℓ subgroup by $\mathcal{S}_{\ell,\mathbb{F}_q}(E)$ and we may think of $\mathcal{S}_{\ell,\mathbb{F}_q}(E)$ as a group isomorphic to $\mathbb{Z}_{\ell^f} \times \mathbb{Z}_{\ell^g}$ for $f, g \in \mathbb{N}$, with $f \geq g \geq 0$.

For $\ell = 2$, we can easily find generators for $\mathcal{S}_{2,\mathbb{F}_q}(E)$, as long as we know $E[2]$, using a genus-1 interpretation of [7, Sec. 3], which is close to the techniques described before: We look for two points $P, Q \in E(\mathbb{F}_q)$ with different non-trivial profiles, clearing the cofactor if necessary. None of this relies particularly on $n = 2$, and we could do the same for any other prime ℓ to find generators of $\mathcal{S}_{\ell,\mathbb{F}_q}(E)$ for $\ell \neq p$. In fact, this even generalizes to higher-dimensional abelian varieties as demonstrated in [7, Sec. 3] for $n = 2$ on two-dimensional Jacobians. Profiles therefore allow us to determine precise cosets in $E(\mathbb{F}_q)/[n]E(\mathbb{F}_q)$, and this can be used to determine points with certain 'nice' properties, such as an order divisible by ℓ^k.

In more precise terms, for primes ℓ, the Sylow-ℓ subgroup on a principally polarized abelian variety A of dimension g for $\ell \neq p$ is a subgroup of $A(\mathbb{F}_q)$ of the form

$$\mathbb{Z}_{\ell^{f_1}} \times \mathbb{Z}_{\ell^{f_2}} \times \ldots \times \mathbb{Z}_{\ell^{f_d}}$$

with $f_i \in \mathbb{N}$ such that $f_1 \geq f_2 \geq \ldots \geq f_d > 0$ and $d \leq 2g$. Given a basis $K_1, \ldots, K_d$ for $A[\ell]$, we can find generators for $\mathcal{S}_{\ell,\mathbb{F}_q}(A)$ by finding points $B_i \in A(\mathbb{F}_q)$ whose ℓ-Tate profiles are independent, and then clearing the cofactor $\#A(\mathbb{F}_q)/\ell^{\sum f_i}$. This ensures linear combinations of the Tate profiles, corresponding to linear combinations of the B_i, span all possible profiles and hence give representatives of every coset in $A(\mathbb{F}_q)/[\ell]A(\mathbb{F}_q)$. By a counting argument, we find that the B_i generate $\mathcal{S}_{\ell,\mathbb{F}_q}(A)$.

[3] One could also say that this is the $\mathbb{F}_q$-rational part of the ℓ-Tate module, i.e., those $\mathbb{F}_q$-rational points on E whose order is ℓ^f for some integer f.

4 Generalized Tate pairings

Bruin [2] explains how we can generalize the Tate pairing to any separable isogeny

$$\varphi : E \to E', \qquad \ker \widehat{\varphi} \subseteq E'[q-1]$$

to which Robert [16] refers as the Tate-Cartier pairing, and [7] as the φ-Tate pairing t_φ. When reduced, this pairing becomes a map

$$t_\varphi : \ker \varphi\ (\mathbb{F}_q) \times \operatorname{coker} \widehat{\varphi}\ (\mathbb{F}_q) \to \mu_n,$$

with $n = \deg \varphi$, the dual $\widehat{\varphi} : E' \to E$, and $\operatorname{coker} \widehat{\varphi}\ (\mathbb{F}_q) = E(\mathbb{F}_q)/\widehat{\varphi}(E'(\mathbb{F}_q))$ the $\mathbb{F}_q$-rational part of the cokernel.[4] In general, when working on any abelian variety, and assuming an $\mathbb{F}_q$-rational basis $K_1, \ldots, K_m$ for $\ker \varphi$, we can define the profile $t_{\ker \varphi}(P)$ as the evaluation of $t_\varphi(K_i, P)$ for every kernel generator K_i, and we can again go ahead and decompose the cokernel $E(\mathbb{F}_q)/\widehat{\varphi}(E'(\mathbb{F}_q))$ into cosets, which again is isomorphic to μ_n^m as a group [7, Lem. 6], for prime n and φ an n-isogeny.

Remark 1. This improves our understanding of the situation in Section 2.1: when $E[n]$ is not rational, say $E[n](\mathbb{F}_q)$ is cyclic and generated by K, we get

$$t_{\ker \varphi} : E(\mathbb{F}_q)/\widehat{\varphi}(E'(\mathbb{F}_q)) \xrightarrow{\sim} \mu_n, \qquad P \mapsto t_\varphi(K, P),$$

derived from the generalized Tate pairing for the isogeny $\varphi : E \to E/\langle K \rangle$, instead of the $[n]$-Tate pairing.

Computing this Tate pairing t_φ is not hard: it can be computed as the Tate pairing t_n where $n = \deg \varphi$. This gives us a counter-intuitive result: the 'generalization' of the Tate pairing to any isogeny φ is actually already captured by the information from t_n, and the profile $t_{\ker \varphi}(P)$ is a subprofile of $t_{[n]}(P)$. Hence, we determine the position of P only up to larger cosets in $E(\mathbb{F}_q)/\widehat{\varphi}(E'(\mathbb{F}_q))$ compared to $E(\mathbb{F}_q)/[n](E(\mathbb{F}_q))$ The generalized Tate pairing gives us coarser information! In other words, if the curve E does not have enough rational n-torsion, or if we only compute a subset of pairings $t_n(K_i, P)$, then we can only divide $E(\mathbb{F}_q)$ into larger cosets.

Nevertheless, this generalized Tate pairing allows us to understand previous results in framework of profiles. We rephrase Lemma 2 in terms of generalized Tate pairings.

Lemma 3. *Let E_A be a maximal supersingular Montgomery curve over $\mathbb{F}_{p^2}$ with $p = 2^f \cdot h - 1$, written as $E_A : y^2 = x(x-\alpha)(x-1/\alpha)$. Let $T_0 = (0,0)$, $T_1 = (\alpha, 0)$, and $T_2 = (1/\alpha, 0)$ be the 2-torsion points of E_A. Let $\varphi_i : E \to E/\langle T_i \rangle$. Then,*

$$t_{\ker \varphi_i}(P) \neq 1 \quad \Leftrightarrow \quad P \in E \backslash \widehat{\varphi}_i(E'(\mathbb{F}_q)) \quad \Leftrightarrow \quad 2^f \mid \operatorname{Order}(P) \text{ and } [2^{f-1}]P \neq T_i.$$

This explains the trick to sample points P with order divisible by 2^f by sampling points with non-square x-coordinate x_P: we are sampling points in $E \setminus \widehat{\varphi}\ (\mathbb{F}_q)$, for the isogeny $\varphi : E \to E\langle(0,0)\rangle$.

[4] We recover the Tate pairing of degree n by $\varphi = [n]$, with $\varphi = \widehat{\varphi}$.

5 Examples of applications

We show that a broad range of applications find an concise interpretation as profiles of Tate pairings.

5.1 Decompostion of R as $aP + bQ$

Let $E/\mathbb{F}_{p^2}$ be a maximal supersingular elliptic curve, with $2^f \mid p+1$, and let P, Q be a basis for $E[2^f]$, then we may want to decompose a third point R as $aP + bQ$. First, we find the profiles $t_{[2^f]}(P) = (t_{2^f}(P,P), t_{2^f}(Q,P))$ and $t_{[2^f]}(Q) = (t_{2^f}(P,Q), t_{2^f}(Q,Q))$. Then, the decomposition $R = aP + bQ$ is equivalent to the decomposition as profiles

$$t_{[2^f]}(R) = t_{[2^f]}(P)^a \cdot t_{[2^f]}(Q)^b, \quad \text{where } t_{[2^f]}(R) = (t_{2^f}(P,R), t_{2^f}(Q,R)).$$

Of course, the easier approach uses bilinearity of the Tate pairing to compute a and b by discrete logarithms of $t_{2^f}(P,R)$ and $t_{2^f}(Q,R)$ in base $\zeta = t_{2^f}(P,Q)$. Nevertheless, these discrete logarithms generalize when interpreted as profiles in terms of their structure $\mu_{2^f}^n$.

5.2 Pairing the volcano

Robert [16, Sec. 5] gives an interpretation of 'Pairing the Volcano' [13]. We will showcase how this fits our understanding using the easiest example: the 2-volcano used in CSURF [3].

Let p be a prime $p \equiv 7 \mod 8$. We will work over $\mathbb{F}_p$ with supersingular Montgomery curves $E_A : y^2 = x^3 + Ax^2 + x$. These curves come in two categories: those whose $\mathbb{F}_p$-rational endomorphisms $\mathrm{End}_p(E)$ forms a ring isomorphic to $\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ and those with $\mathrm{End}_p(E) \cong \mathcal{O}' = \mathbb{Z}[\sqrt{-p}]$. The 2-volcano structure in this case is rather nice: the surface is given by those E with $\mathrm{End}_p(E) \cong \mathcal{O}$, and the floor is given by E with $\mathrm{End}_p(E) \cong \mathcal{O}'$. On the surface, we have $E(\mathbb{F}_p)[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, whereas on the floor $E(\mathbb{F}_p)[2] \cong \mathbb{Z}_2$. This implies we have three 2-isogenies on the surface, out of which two are horizontal. The last isogeny is vertical, and connects us to the floor. The dual of this isogeny is the single $\mathbb{F}_p$-rational 2-isogeny on the floor, connecting us back to the surface. See Figure 1 for an illustrative picture.[5]

For E_A with $x^3 + Ax^2 + x = x(x-\alpha)(x-1/\alpha)$, we once again denote the three torsion points by $T_0 = (0,0)$, $T_\alpha = (\alpha, 0)$ and $T_{\overline{\alpha}} = (1/\alpha, 0)$. On the surface, $\alpha \in \mathbb{F}_p$, whereas on the floor $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. Denote by $\varphi_0, \varphi_\alpha, \varphi_{\overline{\alpha}}$ the three isogenies with kernel $T_0, T_\alpha, T_{\overline{\alpha}}$ respectively, then the generalized φ-Tate pairing should be able to tell us which isogeny is vertical, and which ones are horizontal. That is, the self-Tate pairing $t_\varphi(P,P)$ is non-trivial if and only if $P \notin \widehat{\varphi}(E'(\mathbb{F}_p))$ if and only if φ is vertical. We have seen the first 'if and only

[5] We thank Thomas Decru for the picture.

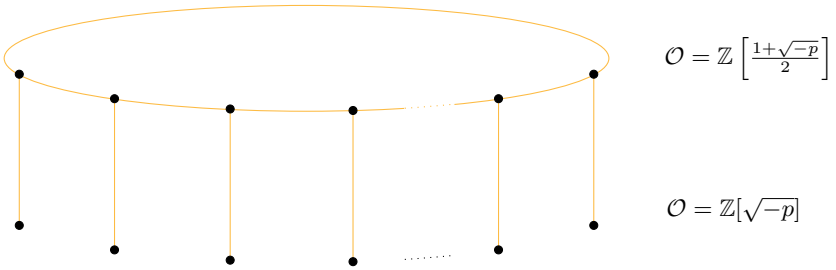

Fig. 1. Volcano structure using 2-isogenies for $p \equiv 7 \bmod 8$.

if' already, whereas the second 'if and only if' is the analogue of [13, Prop. 4.8], which we illustrate for this specific example as follows.

Let $\varphi : E \to E'$ be a horizontal isogeny, and let P, Q denote a basis for $E[2]$ such that P generates the kernel of φ, then the dual $\widehat{\varphi}$ is generated by $\varphi(Q)$. We still have E' on the surface, so $E'[2] \subset E'(\mathbb{F}_p)$. Hence, there is some point P' such that $E'[2] = \langle \varphi(Q), P' \rangle$. We then must have $\widehat{\varphi}(P') = R$ for some 2-torsion point $R \in E(\mathbb{F}_p)$ with $\varphi(R) = \infty_{E'}$, as $\varphi(\widehat{\varphi})(P') = [2]P' = \infty_{E'}$. So $R = P$, and we find that $P \in \widehat{\varphi}(E'(\mathbb{F}_p))$, as required.

If $\varphi : E \to E'$ was instead vertical, then E' has only a single 2-torsion point P', and this point generates the dual. Then, if $P \in \widehat{\varphi}(E'(\mathbb{F}_p))$ and so $P = \widehat{\varphi}(Q)$ then Q is either another rational 2-torsion point, which does not exist on E', or a 4-torsion point. But all 4-torsion points Q on E' are mapped to P' under $[2] = \varphi \circ \widehat{\varphi}$, and so $\widehat{\varphi}(Q) \notin \ker \varphi = \langle P \rangle$. We find that $P \notin \widehat{\varphi}(E'(\mathbb{F}_p))$, as required.

Example 3. Let $p = 23$ and $A = 10$ then $E_A : y^2 = x^3 + Ax^2 + x$ has 2-torsion points $T_0 = (0, 0)$, $T_{17} = (17, 0)$ and $T_{19} = (19, 0)$. We then compute the self-pairing as

$$t_2(T_i, T_i) = t_2(T_i, T_i + T_j)/t_2(T_i, T_j),$$

so that we can use the simple expression $t_2(T_i, T_j) = (x_{T_j} - x_{T_i})^{\frac{p-1}{2}}$. We get

$$\begin{aligned} t_2(T_0, T_0) &= t_2(T_0, T_{17})/t_2(T_0, T_{19}) = (17/19))^{\frac{p-1}{2}} = 1, \\ t_2(T_{17}, T_{17}) &= t_2(T_{17}, T_0)/t_2(T_{17}, T_{19}) = (-17/2)^{\frac{p-1}{2}} = 1, \\ t_2(T_{19}, T_{19}) &= t_2(T_{19}, T_0)/t_2(T_{19}, T_{17}) = (-19/-2)^{\frac{p-1}{2}} = -1. \end{aligned}$$

Hence, the vertical isogeny is given by T_{19}, whereas the other two points generate horizontal isogenies. Indeed, the corresponding isogenies are given by

$$\begin{aligned} \varphi_0 &: E_{10} \to E_{13}, && \text{with } E_{13}[2] = \{(0,0), (4,0), (6,0), \infty\}, \\ \varphi_{17} &: E_{10} \to E_{-4}, && \text{with } E_{-4}[2] = \{(0,0), (9,0), (18,0), \infty\}, \\ \varphi_{19} &: E_{10} \to E_7, && \text{with } E_7[2] = \{(0,0), \infty\}. \end{aligned}$$

In general, we find that $E[2^\infty](\mathbb{F}_p) \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ on the surface, and as T_0 is the double of the point $(1, -) \in E_A(\mathbb{F}_p)$ of order 4, its profile must be trivial. The two other points $T_\alpha, T_{\overline{\alpha}}$ have non-trivial profiles, but their profiles must be equal, as $t_{[2]}(T_{\overline{\alpha}}) = t_{[2]}(T_\alpha) \cdot t_{[2]}(T_0)$, giving a more general proof that one of these points must have a trivial self-pairing, and the other a non-trivial self-pairing. For more information, see [13] and Section 5 of [16].

5.3 Sampling specific points of order 2^f

When using Scholten's construction [17] on supersingular elliptic curves over $\mathbb{F}_{p^2}$, the resulting Jacobians one works with have $\mathbb{F}_p$-torsion structure

$$\mathcal{J}(\mathbb{F}_p) \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

as used by Costello [8]. In [7], we needed to sample points with order divisible by 2^f in the rather precise subgroup of $\mathcal{J}$ isomorphic to $\mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}}$. This is precisely an application where we need the full profile information of the 2-Tate pairing: there are three profiles, out of the sixteen in total, that are 'good', i.e., points P with such a profile $t_{[2]}(P)$ have precisely the property we need. Nine other profiles are 'ok', as they require us only to add the correct one of three 2-torsion points D_{ij} to P to obtain a point $P' = P + D_{ij}$ with a 'good' profile. The last four profiles are 'bad', the three profiles indicate points in the subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, and the last profile is the trivial profile indicating points in $[2]\mathcal{J}$. For more information, see Section 3 of [7].

5.4 Generalized entangled basis generation

We now also have enough understanding to generalize entangled basis generation (Lemma 1) to any Weierstrass curve over $\mathbb{F}_q$

$$E : y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3), \quad \lambda_i \in \mathbb{F}_q.$$

We need to find a transformation $x_P \mapsto x_Q$ that ensures we get two different non-trivial profiles $t_{[2]}(P) \neq t_{[2]}(Q)$. Thus, we need to sample x_P in such a way that we keep the value of the first Tate pairing $x_P - \lambda_1 = u^2(x_Q - \lambda_1)$ for some $u \in \mathbb{F}_q$, and permute the second and third Tate pairing using $x_Q = -x_P + \lambda_2 + \lambda_3$, as this ensures

$$(x_Q - \lambda_2) = -(x_P - \lambda_3), \quad (x_Q - \lambda_3) = -(x_P - \lambda_2).$$

This gives us two equations in terms of x_P and x_Q and solving these gives us

$$x_P = \frac{\lambda_2 + \lambda_3 - 2 \cdot \lambda_1}{1 + u^2}, \quad u \in \mathbb{F}_q.$$

Thus, if we precompute two lists with values $\frac{1}{1+u^2}$ either squares or non-squares, then by the quadratic character of $\lambda_2 + \lambda_3 - 2 \cdot \lambda_1$, we can ensure we sample

x_P as a non-square. By the above equations, any such x_P defining a point on E similarly defines a point $Q \in E$ by $x_Q = -x_P + \lambda_2 + \lambda_3$, such that P and Q have different non-trivial 2-profiles, and hence generate the Sylow-2 subgroup for E. Summarizing, we get the following.

Lemma 4. *Let $E : y^2 = (x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$, with $\lambda_i \in \mathbb{F}_q$. Let $P \in E(\mathbb{F}_{p^2})$ with non-square $x_P = \frac{\lambda_2+\lambda_3-2\cdot\lambda_1}{1+u^2}$ for some $u \in \mathbb{F}_{p^2}$. Then, $x_Q = -x_P + \lambda_2 + \lambda_3$ defines a second point Q on E such that $[h]P$ and $[h]Q$ generate the Sylow-2 subgroup $\mathcal{S}_{2,\mathbb{F}_q}(E) \cong \mathbb{Z}_{2^f} \times \mathbb{Z}_{2^g}$, with $f \geq g$, for $h = \frac{\#E(\mathbb{F}_q)}{2^{f+g}}$.*

Remark 2. One may wonder about the practicality of Lemma 4: given only the curve equation, we know $-(\lambda_1 + \lambda_2 + \lambda_3)$ from the coefficient of x^2. Hence, we need to know at least one point of order 2 to compute the value $\lambda_2+\lambda_3-2\cdot\lambda_1$ to apply the basis generation method. The elegance of Lemma 1 is that Montgomery curves have such a point of order 2 always at $(0,0)$, and so, Lemma 4 is efficient when a 2-torsion point is known *a priori* on the curve model. On the Montgomery model, Lemma 4 slightly generalizes Lemma 1, as we can now choose more freely which torsion point we take for λ_1, instead of the fixed choice $\lambda_1 = 0$.[6]

5.5 And many more[7]

The recent work PEGASIS [10] works with supersingular curves over $\mathbb{F}_p$ with Sylow-2 subgroup $\mathcal{S}_{2,\mathbb{F}_p}(E) \cong \mathbb{Z}_{2^{f-1}} \times \mathbb{Z}_2$, where $2^f \mid p+1$. By a clever use generalized Tate pairings, PEGASIS uses only a single pairing computation per point to find a basis $\langle P, Q\rangle = E(\mathbb{F}_{p^2})[2^f]$ with $P \in E(\mathbb{F}_p)$ and $Q \in E^t(\mathbb{F}_p)$. This combines several of the previous ideas, such as pairing the volcano and sampling points with specific profiles, into an optimized and fast sampling of such bases. Furthermore, [10, Alg. 1] cleverly uses the decomposition of points $T \in E[n]$ in terms of bases of $E[n]$ to evaluate endomorphisms without division points!

The geometric interpretation of the Tate pairing allows Robert [16] to prove conjectures regarding (multi-)radical isogenies [4, 5]. Such conjectures also have an interpretation as studying the fiber $f^{-1}(P)$ for isogenies f, hence shows why the Tate pairing appears. Similarly, Robert shows that testing supersingularity using Doliskani's test [1, 11] can be understood as studying such fibers.[8]

Furthermore, work on subgroup membership testing for elliptic curves can performed using Tate pairings [9, 14], cleverly combining several subprofiles to efficiently test membership of $[n]E(\mathbb{F}_q)$ for points $Q \in E(\mathbb{F}_q)$.

Lastly, several of the algorithms in [15] to verify supersingularity and to verify the orders of certain points on supersingular elliptic curves use a Tate pairing between $E(\mathbb{F}_p)$ and its twist over $\mathbb{F}_p$. This can be understood as a generalized Tate pairing for the endomorphism $\pi - 1$ for the curve over $\mathbb{F}_{p^2}$, which has kernel precisely $E(\mathbb{F}_p)$.

[6] One can also permute the profiles in any other permutation of S_3, beyond this involution $(1,2,3) \mapsto (1,3,2)$, using the same techniques.

[7] I intend to keep this document up to date with innovative use of the Tate pairing.

[8] In fact, this note is mostly an exposition of examples in [16].

References

[1] Gustavo Banegas, Valerie Gilchrist, and Benjamin Smith. "Efficient supersingularity testing over $\mathbb{F}_p$ and CSIDH key validation". In: *Mathematical Cryptology* 2.1 (2022), pp. 21–35 (cit. on p. 9).

[2] Peter Bruin. "The Tate pairing for abelian varieties over finite fields". In: *Journal de theorie des nombres de Bordeaux* 23.2 (2011), pp. 323–328 (cit. on pp. 1, 3, 5).

[3] Wouter Castryck and Thomas Decru. "CSIDH on the surface". In: *International Conference on Post-Quantum Cryptography*. Springer. 2020, pp. 111–129 (cit. on p. 6).

[4] Wouter Castryck and Thomas Decru. "Multiradical isogenies". In: *Arithmetic, Geometry, Cryptography, and Coding Theory* 779 (2021), pp. 57–89 (cit. on p. 9).

[5] Wouter Castryck, Thomas Decru, and Frederik Vercauteren. "Radical isogenies". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2020, pp. 493–519 (cit. on p. 9).

[6] Maria Corte-Real Santos, Jonathan Komada Eriksen, Michael Meyer, and Krijn Reijnders. "AprèsSQI: Extra Fast Verification for SQIsign Using Extension-Field Signing". In: *Advances in Cryptology - EUROCRYPT 2024 - 43nd Annual International Conference on the Theory and Applications of Cryptographic Techniques*. 2024 (cit. on p. 2).

[7] Maria Corte-Real Santos and Krijn Reijnders. "Return of the Kummer: a toolbox for genus 2 cryptography". In: *Cryptology ePrint Archive* (2024) (cit. on pp. 1, 4, 5, 8).

[8] Craig Costello. "Computing Supersingular Isogenies on Kummer Surfaces". In: *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III*. Ed. by Thomas Peyrin and Steven D. Galbraith. Vol. 11274. Lecture Notes in Computer Science. Springer, 2018, pp. 428–456. DOI: 10.1007/978-3-030-03332-3_16 (cit. on p. 8).

[9] Yu Dai, Debiao He, Dmitrii Koshelev, Cong Peng, and Zhijian Yang. *Revisiting subgroup membership testing on pairing-friendly curves via the Tate pairing*. Cryptology ePrint Archive, Paper 2024/1790. 2024. URL: https://eprint.iacr.org/2024/1790 (cit. on p. 9).

[10] Pierrick Dartois, Jonathan Komada Eriksen, Tako Boris Fouotsa, Arthur Herlédan Le Merdy, Riccardo Invernizzi, Damien Robert, Ryan Rueger, Frederik Vercauteren, and Benjamin Wesolowski. *PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies*. Cryptology ePrint Archive, Paper 2025/401. 2025. URL: https://eprint.iacr.org/2025/401 (cit. on p. 9).

[11] Javad Doliskani. "On division polynomial PIT and supersingularity". In: *Applicable Algebra in Engineering, Communication and Computing* 29.5 (2018), pp. 393–407 (cit. on p. 9).

[12] Dale Husemöller. *Elliptic Curves, 2nd edition*. Springer, 2004 (cit. on p. 2).
[13] Sorina Ionica and Antoine Joux. "Pairing the volcano". In: *Mathematics of Computation* 82.281 (2013), pp. 581–603 (cit. on pp. 6–8).
[14] Dmitrii Koshelev. "Subgroup membership testing on elliptic curves via the Tate pairing". In: *Journal of Cryptographic Engineering* 13.1 (2023), pp. 125–128 (cit. on p. 9).
[15] Krijn Reijnders. "Effective Pairings in Isogeny-Based Cryptography". In: *Progress in Cryptology - LATINCRYPT 2023 - 8th International Conference on Cryptology and Information Security in Latin America, LATINCRYPT 2023, Quito, Ecuador, October 3-6, 2023, Proceedings*. Ed. by Abdelrahaman Aly and Mehdi Tibouchi. Vol. 14168. Lecture Notes in Computer Science. Springer, 2023, pp. 109–128. DOI: 10.1007/978-3-031-44469-2_6. URL: https://doi.org/10.1007/978-3-031-44469-2_6 (cit. on p. 9).
[16] Damien Robert. *The geometric interpretation of the Tate pairing and its applications*. Cryptology ePrint Archive, Paper 2023/177. 2023. URL: https://eprint.iacr.org/2023/177 (cit. on pp. 1–3, 5, 6, 8, 9).
[17] Jasper Scholten. "Weil restriction of an elliptic curve over a quadratic extension". In: *Preprint* (2003) (cit. on p. 8).
[18] Gustavo HM Zanon, Marcos A Simplicio, Geovandro CCF Pereira, Javad Doliskani, and Paulo SLM Barreto. "Faster key compression for isogeny-based cryptosystems". In: *IEEE Transactions on Computers* 68.5 (2018), pp. 688–701 (cit. on p. 2).