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.

The Purpose of this Note

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

*An extended version of this note is published in combination with another note of mine, *Optimized Cubical Pairings of Degree 2 for Subgroup Membership Testing in Genus 2*, (available here) in the proceedings of LATINCRYPT 2025 as

> Krijn Reijnders. "The Tate Profile". In: *Progress in Cryptology - LATINCRYPT 2025 - 9th International Conference on Cryptology and Information Security in Latin America, LATINCRYPT 2025, Medellin, Colombia, October 1-3, 2025, Proceedings*. Springer. 2025.

In my opinion, the notes are self-contained and have a better reading experience than the paper. For citation purposes, however, I recommend citing the paper above instead of the notes. 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: 2026-03-19.

elliptic curves and Jacobians of hyperelliptic curves, and reframe them using (profiles of) Tate pairings. The core theoretical framework is by Robert [Rob23], which explains the study of fibers $\varphi^{-1}(P)$ in detail.[1] Work by Bruin [Bru11] explains the generalization of the Tate pairing, and work by Corte-Real Santos and me [CR24] 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.

Examples & Code. As this note is mostly educational, I'm building a repository of examples to showcase most of the use cases given in this note. This is available at

`https://github.com/Krijn-math/squared_kummer_surfaces`.

Acknowledgements. We thank Lorenz Panny for noticing a mistake in the, admittedly sparse, description of the algorithm to compute ℓ-Sylow torsion in Section 5.5

1 Divisibility results

Many results on the divisibility of points are Tate pairings in disguise [Rob23, Sec. 5.2]. An easy, yet surprisingly useful result is the following classical theorem.

Theorem 1 [Hus04]**.** *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 $i = 1, 2, 3$.

[1] Sections 3 and 4 of [Rob23] are heavy in algebraic geometry, however, many of the useful applications in its Section 5 can be understood in the traditional interpretation!

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: if a point $P \in E$ has trivial 2-Tate pairings with all points in $E[2]$ then it 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 $T_2((\lambda_1, 0), P) = (x_P - \lambda_1) = x_P$ 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 [ZSPD+18] show that by choosing x_P carefully, we can immediately obtain a suitable x_Q to complete the torsion basis.

Lemma 1 [ZSPD+18]**.** *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 [CEMR24] shows that the quadratic characters of $(x - \lambda_i)$ contain precise information on points $P \in E[2^f]$.

Lemma 2 [CEMR24]**.** *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 [Bru11]

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

As Robert [Rob23] 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 $K_i \in E[n](\mathbb{F}_q)$. Let m be the rank of $E[n](\mathbb{F}_q)$, then of course $m \leq 2$. However, we write this for general m as this will similarly generalize to abelian varieties A of dimension g, where $A[n](\mathbb{F}_q)$ can go up to rank $2g$. Hence, let $\langle K_1, \ldots, K_m \rangle$ denote a basis of the rational ℓ-torsion. Then we get the n-Tate profile as the map:

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

We call the image $t_{[n]}(P)$ the *n-profile* of P under the Tate pairing, which we define more precisely and generally in Definition 2 later. 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 [Rob23, Cor. 5.2].

2.1 Profiles of the [2]-Tate pairing

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] If we then rephrase the lemma in terms of profiles, we get:

Lemma 3. *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 $A \neq 0$. Choose a non-square $t \in \mathbb{F}_{p^2}$, such that $x_P = -A/(1+t^2)$ is also non-square, and x_P defines a point $P \in E(\mathbb{F}_{p^2})$. Then $t_{[2]}(P)$ is non-trivial.*

Furthermore, taking $x_Q = -x_P - A$ defines a point $Q \in E(\mathbb{F}_{p^2})$ with $t_{[2]}(Q) \neq t_{[2]}(P)$ and both non-trivial.

2.2 Profiles assuming 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' 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 [CR24, Lem. 6],

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

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 $E(\mathbb{F}_q)$.

2.3 Profiles on abelian varieties

As we discovered in the previous subsections, we should think of the Tate profile with respect to a basis, as this ensures a natural identification with μ_n^2. This turns out to be the correct interpretation for higher dimensions too, although we will need to be a bit more precise by what we mean by basis, and we need to introduce the exponent and rank too.

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

Definition 1. *Let A be an abelian variety of dimension g over a finite field k. Let G be a subgroup of $A(k)$. By the structure theorem, there are unique integers $d_1, \ldots, d_r \geq 1$ such that G decomposes into cyclic groups as*

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z},$$

where $d_1 \mid d_2 \mid \cdots \mid d_r$, with $d_1 \geq 1$ and $d_r = n$. We say that n is the exponent *of G and r is the* rank *of G. We say that a set of points $(P_1, \ldots, P_r)$ with $P_i \in A(k)$ is a* basis *for G if there exists an isomorphism*

$$\varphi : G \to \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z},$$

where $\varphi(P_i) = (0, \ldots, 0, 1, 0, \ldots, 0)$, with the 1 in the i-th position.

The notation $G = \langle P_1, \ldots, P_r \rangle$ is used to denote that $(P_1, \ldots, P_r)$ is a basis for G. In this text, we usually consider abelian varieties A of dimension g with $A[n](k) = A[n]$. Then for $G = A[n]$, we get $d_i = n$ for all $1 \leq i \leq r$, and the rank of G is $r = 2g$. Another example that we see often in isogeny-based cryptography is given by $(n, n, \ldots, n)$-isogenies $f : (A, \lambda_A) \to (B, \lambda_B)$ of principally polarized abelian varieties, where for $G = \ker f$, we get $d_1 = \cdots = d_r = n$, and $r = g$. Lastly, note that when n is prime, we must similarly have $d_i = n$ for all i. This definition generalizes the usual notions of a basis (P, Q) for the rational n-torsion of an elliptic curve, or a generator K for a cyclic isogeny $E \to E/\langle K \rangle$. We can then properly define the profile with respect to such a basis as follows.

Definition 2. *Let A be an abelian variety over a finite field k and let $n \in \mathbb{N}$ be a positive integer. Let r be the rank of $A[n](k)$, whose exponents is n, and let $(P_1, \ldots, P_r)$ be a basis for $A[n](k)$. The* Tate profile $t_{[n]}$ *with respect to this basis is the map*

$$\begin{aligned} t_{[n]} : A(k) &\to \mu_n^r \\ Q &\mapsto (t_n(P_1, Q), \ldots, t_n(P_r, Q)) \end{aligned}$$

We refer to $t_{[n]}(Q)$ for $Q \in A(k)$ as the n-Tate profile of Q. We say that the profile $t_{[n]}(Q)$ is trivial*, when $t_n(P_i, Q) = 1$ for all $1 \leq i \leq r$.*

Similar to before, if the n-Tate pairing is non-degenerate, this induces an isomorphism

$$t_{[n]} : A(k)/[n]A(k) \xrightarrow{\sim} \mu_n^r. \tag{2}$$

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 [CR24, 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 [CR24, 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.

3.1 In higher dimensions

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

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

with $f_i \in \mathbb{N}$ such that $f_1 \geq f_2 \geq \ldots \geq f_r > 0$ and of rank $r \leq 2g$. Given a basis $\mathcal{B} = K_1, \ldots, K_r$ for $A[\ell]$, we can find generators for $\mathcal{S}_{\ell,\mathbb{F}_q}(A)$ by finding points $P_i \in A(\mathbb{F}_q)$ 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 P_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 P_i generate $\mathcal{S}_{\ell,\mathbb{F}_q}(A)$. More formally, we state the following theorem.

Theorem 2. *Let r denote the rank of $A[\ell](\mathbb{F}_q)$, assume the ℓ-Tate pairing is non-degenerate, and define the Tate profile $t_{[\ell]}$ with respect to a basis $\mathcal{B}$ of $A[\ell](\mathbb{F}_q)$. Then, for points $P_1, \ldots, P_r \in A(\mathbb{F}_q)$, we get*

$$A(\mathbb{F}_q)/A[\ell](\mathbb{F}_q) = \langle P_1, \ldots, P_r \rangle \quad \textit{if and only if} \quad \mu_\ell^r = \langle t_{[\ell]}(P_1), \ldots, t_{[\ell]}(P_r) \rangle.$$

[3] One could also look at this subgroup as the largest subgroup of $\mathbb{F}_q$-rational points on E whose order is ℓ^f for some integer f.

Consequently, for $h = \frac{|A(\mathbb{F}_q)|}{|\mathcal{S}_{\ell,q}(E)(A)|}$ *so that* $[h]P \in \mathcal{S}_{\ell,q}(E)(A)$ *for all* $P \in A(\mathbb{F}_q)$*, we get*

$$\mathcal{S}_{\ell,q}(E)(A) = \langle [h]P_1, \ldots, [h]P_r \rangle.$$

4 Generalized Tate pairings

Bruin [Bru11] 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 [Rob23] refers as the Tate-Cartier pairing, and [CR24] as the φ-Tate pairing t_φ. When reduced, this pairing becomes a map

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

where n is the exponent of $(\ker \varphi)(\mathbb{F}_q)$, with $\widehat{\varphi}$ the dual $E' \to E$, 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. For general isogenies between abelian varieties, the kernel can be rather complicated. However, in isogeny-based cryptography, we often work with separable $(n, \ldots, n)$-isogenies φ between principally polarized abelian varieties with rational kernel, so that we get $(\ker \varphi)(\mathbb{F}_q) = \ker \varphi \cong (\mathbb{Z}_n)^r$ of exponent n and rank $r = g$. Another example is scalar multiplication $\varphi = [n]$, with kernel $A[n](\mathbb{F}_q)$ of some rank $r \leq 2g$ isomorphic to $\mathbb{Z}_n^r$. In both cases, whenever the generalized Tate pairing t_φ is non-degenerate, the induced profile $t_{\ker \varphi}$ with respect to some basis of $(\ker \varphi)(\mathbb{F}_q)$ gives an isomorphism

$$t_{\ker \varphi} : (\operatorname{coker} \widehat{\varphi})(\mathbb{F}_q) \xrightarrow{\sim} \mu_n^r,$$

where r is the rank. In essence, the choice of a basis for $(\ker f)(k)$ fixes an isomorphism to this product of roots of unities, which gives us a coordinate system to work with on the cokernel.

Remark 1. This improves our understanding of the situation in Section 2.2: when $E[n]$ is not rational, say $E[n](\mathbb{F}_q)$ is cyclic and generated by K, we get

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

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

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 is the exponent of $(\ker \varphi)(\mathbb{F}_q)$. 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 $E(\mathbb{F}_q)/[n](E(\mathbb{F}_q))$. In other words, the generalized Tate pairing gives us coarser information! That is, 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 which give us less information on the position of points within $E(\mathbb{F}_q)/[n]E(\mathbb{F}_q)$.

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 4. *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,*

$$t_{\ker \varphi_i}(P) \neq 1 \quad \Leftrightarrow \quad 2^f \mid \mathrm{Order}(P) \text{ and } [2^{f-1}]P \neq T_i.$$

Proof. We have $t_{\ker \varphi_i}(P) \neq 1$ only if $P \in E \setminus \widehat{\varphi}_i(E'(\mathbb{F}_q))$. By writing out the action of φ_i and $\widehat{\varphi}_i$ on $E[2^f]$, we find that $P \in E \setminus \widehat{\varphi}_i(E'(\mathbb{F}_q))$ only if $2^f \mid \mathrm{Order}(P)$ and P is above T_i, i.e., $[2^{f-1}]P \neq T_i$. □

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 $\varphi : E \to E/\langle (0,0) \rangle$.

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 [Rob23, Sec. 5] gives an interpretation of 'Pairing the Volcano' [IJ13]. We will showcase how this fits our understanding using the easiest example: the 2-volcano used in CSURF [CD20].

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 if' already, whereas the second 'if and only if' is the analogue of [IJ13, 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

[5] We thank Thomas Decru for the picture.

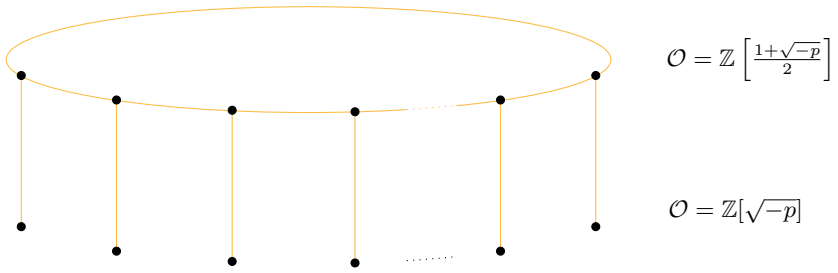

Fig. 1. Volcano structure using 2-isogenies for $p \equiv 7 \bmod 8$.

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 [IJ13] and Section 5 of [Rob23].

5.3 Sampling specific points of order 2^f

When using Scholten's construction [Sch03] 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 [Cos18]. In [CR24], 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 [CR24].

5.4 Isogeny compression

One of the main applications of basis sampling techniques is to compress isogenies. We will first focus on the most common example, where we have a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ with $p = 2^f \cdot h - 1$, and we want to compress an isogeny $\varphi : E \to E'$ of degree 2^f. This isogeny can be described by its kernel $\ker \varphi = \langle K \rangle$ for some $K \in E[2^f]$, and so we can communicate this isogeny by sending $x_K \in \mathbb{F}_{p^2}$, which takes $2 \log p$

bits. However, by *deterministically* sampling a basis (P, Q) for $E[2^f]$, using deterministic variants of Lemma 3 or Lemma 2, we may similarly express (some odd multiple of) K as $K = P + [a]Q$ for some $a \in \mathbb{Z}_{2^f}$. By only sending a, we have compressed the isogeny to f bits. Decompression requires the receiver of a and E to recompute the basis (P, Q) using the same deterministic method, so that they can recompute $K = P + [a]Q$.

Higher dimensions. We generalize this to higher-dimensional abelian varieties, where we want to compress an isogeny $f : A \to B$, with $\ker f = \langle K_1, \ldots, K_d \rangle$. Let n be the exponent of $\ker f$, then we may assume $K_i \in \mathcal{S}_{n,q}(A)$, the Sylow-$n$ torsion of $A(\mathbb{F}_q)$. We then agree on a deterministic method to sample a basis $(P_1, \ldots, P_r)$ for $\mathcal{S}_{n,q}(A)$, for example by sampling random points P_i until they have a certain predescribed profile t_i. This allows us to compress each K_i to the scalars $\lambda_j^{(i)} \in \mathbb{Z}/n\mathbb{Z}$ such that

$$K_i = \sum_{j=1}^{r} \lambda_j^{(i)} P_j, \quad \text{for } i = 1, \ldots, d,$$

and similarly, we can communicate the full isogeny f by the scalars $(\lambda_j^{(i)})$ where $1 \leq i \leq d$ and $1 \leq j \leq r$.

Example 4. In [CR24], we needed to compress $(2^n, 2^n)$-isogenies between Jacobians of genus-2 curves in a variant of SQIsign. Although the Jacobians were of a specific form, and we only needed to compress a single point $K \in \mathcal{J}[2^n]$ instead of a rank-2 subgroup, there is no fundamental difference with the method described above. There are some noteworthy differences: It is often possible to choose specific predescribed profiles t_i that are much easier to sample for. Such a profile prescribes certain properties of the point P_i, which makes sampling for such points much easier. For full details, see [CR24, Sec. 4.5].

All of the above is essentially also visible in isogeny compression for elliptic curves, as we sample basis points P, Q with respect to certain profiles. However, as is often the case, the elegance of elliptic curves hides a lot of the complexities and nuances behind these techniques.[6]

5.5 Computation of the ℓ-Sylow Torsion

The Tate profile is a crucial ingredient to compute the ℓ-Sylow torsion of an abelian variety A, especially when the general group $A(\mathbb{F}_q)$ is un-

[6] The most striking example is Lemma 1, whose initial description fully hides that this result has anything to do with Tate pairings and profiles.

known. This has been worked out for specific cases, such as the Sylow-2 torsion [MMRV05] and Sylow-ℓ torsion [MMRV09] on elliptic curves, and the Sylow-2torsion on hyperelliptic curves of genus 2 [MPR10]. Although, the Tate pairing is not yet used in these works, all three follow the same general approach to compute the ℓ-Sylow subgroup of an unknown group G. We may trace back a similar approach to computing the 2-Sylow subgroup of certain class groups, by Bosma and Stevenhagen [BS96]. The comparison is enlightening as it shows us how the Tate pairing naturally gives us *characters* on $A(\mathbb{F}_q)$, originating from points $P \in A[\ell]$. The approach requires three essential ingredients, and we focus on the case $G = E(\mathbb{F}_q)$, to compute a basis of $\mathcal{S}_{\ell,q}(E)$.

1. A basis of *characters* of $E(\mathbb{F}_q)/[\ell]E(\mathbb{F}_q)$, such that we can identify $P \in [\ell]E(\mathbb{F}_q)$ using triviality of these characters
2. A basis of $E[\ell](\mathbb{F}_q)$, which serve as a starting point for the goal of computing the basis $\mathcal{S}_{\ell,q}(E)$.
3. A *division algorithm*, that takes as input $P \in E(\mathbb{F}_q)$ and computes $Q \in E(\mathbb{F}_q)$ such that $[\ell]Q = P$, if such a point exists.

Interestingly, the Tate pairing combines the first and second item precisely: given a basis $\mathcal{B} = \{P_1, \ldots, P_r\}$ of $E[\ell](\mathbb{F}_q)$, we get a starting point towards a basis of $\mathcal{S}_{\ell,q}(E)$, but we also get the basis of characters $t_\ell(P_i, -)$ that we need, naturally arising from the Tate pairing, which takes the role of the perfect pairing in [BS96, Eq. 3.2]. Consequently, the 'vanishing of all characters' on a point $Q \in E(\mathbb{F}_q)$ is the analogue of the trivial Tate profile $t_{[\ell]}(Q)$, indicating $Q \in [\ell]E(\mathbb{F}_q)$. As a result, the above Theorem 2 is the analogue on abelian varieties of [BS96, Lem. 3.5]. This use of the Tate profile simplifies the expositions in [MMRV05, MMRV09, MPR10] and shows the large degree of similarity with [BS96]. The resulting algorithm to compute Sylow-ℓ torsion on abelian varieties, assuming a concrete division algorithm, is simple.

1. Let $A[\ell](\mathbb{F}_q)$ be of rank r, and find a basis $\mathcal{B} = \{P_1, \ldots, P_r\}$ of $A[\ell](\mathbb{F}_q)$. This may be done by division of $\mathbf{o}_A$, but is not necessarily the fastest approach.
2. Set $Q_i = P_i$, and compute $Q_i \leftarrow [\frac{1}{\ell}]Q_i$ using the division algorithm until the profile $t_{[\ell]}(Q_i)$ with respect to $\mathcal{B}$ is non-trivial.
3. Compute the rank r' of the profiles $Q_1, \ldots, Q_r$. If $r' = r$, we are finished. If not, find a linear dependency $t_{[\ell]}(Q_j) = \sum \lambda_i t_{[\ell]}(Q_i)$, set $Q_j \leftarrow Q_j - [\lambda_i]Q_i$, and continue dividing.
4. This terminates when the rank of $t_{[\ell]}(Q_1), \ldots, t_{[\ell]}(Q_r)$ equals r, hence $\mathcal{B}' = \{Q_1, \ldots, Q_r\}$ is now a basis of the Sylow-ℓ torsion.

By Theorem 2, the resulting set $Q_1, \ldots, Q_r$ is a basis of the Sylow-ℓ torsion, and the full algorithm requires no knowledge of the full group structure to compute this basis. We stress two important notions: first, the above algorithm relies on the non-degeneracy of the ℓ-Tate pairing so that trivial profiles indicate the existence of pre-images, and second, the existence of a division algorithm with respect to the group operation can be highly non-trivial. Summarizing, the above algorithm is introduced for class groups in [BS96] for $\ell = 2$, and applied to elliptic curves and Jacobians by introducing clear and concrete division algorithms for general ℓ in genus 1 [MMRV05, MMRV09], and $\ell = 2$ in genus 2 [MPR10].

5.6 Generalized entangled basis generation

We now also have enough understanding to generalize entangled basis generation (Lemma 1) to any Weierstrass curve over $\mathbb{F}_q$ with rational 2-torsion, and with -1 a square in $\mathbb{F}_q$,

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

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

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

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 sample $x_P - \lambda_1$ 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 Lemma 5.

Lemma 5. *Let $E : y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$, with $\lambda_i \in \mathbb{F}_q$. Let $P \in E(\mathbb{F}_q)$ with non-square $x_P - \lambda_1 = \frac{\lambda_2 + \lambda_3 - 2 \cdot \lambda_1}{1+u^2}$ for some $u \in \mathbb{F}_q$. Then, $x_Q = -x_P + \lambda_2 + \lambda_3$ defines a $Q \in E(\mathbb{F}_q)$ such that $[h]P$ and $[h]Q$ generate the Sylow-2 torsion $\mathcal{S}_{2,\mathbb{F}_q}(E) \cong \mathbb{Z}_{2^f} \times \mathbb{Z}_{2^g}$, with $f \geq g$, where $h = \frac{\#E(\mathbb{F}_q)}{2^{f+g}}$.*

Remark 2. One may wonder about the practicality of Lemma 5: 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 5 is efficient when a 2-torsion point is known *a priori* on the curve model. On the Montgomery model, Lemma 5 slightly generalizes Lemma 1, as we can now choose more freely which torsion point we take for λ_1, instead of the fixed choice $\lambda_1 = 0$.[7]

5.7 Subgroup Membership Testing

The problem of subgroup membership testing can be phrased as follows: Let E be an elliptic curve over $\mathbb{F}_p$, with a large prime order subgroup $G = E[r](\mathbb{F}_p)$. Verify that a given point $P \in E(\mathbb{F}_p)$ is in G. Optimizing subgroup membership testing is a non-trivial task, but essential to prevent certain *subgroup attacks* [LL97]. For example, a major bug in the Monero cryptocurrency allows for double-spending of coins, and requires a subgroup membership test to prevent this [lS17]. Similarly, pairing-based protocols require subgroup membership testing to ensure that we are working with points in the correct subgroups [BCMN+15, Bow19, Sco21]. A recent innovation by Koshelev [Kos23] applies the non-degeneracy of the Tate pairing to subgroup membership testing, and we may essentially phrase this in terms of profiles.

Lemma 6. *Let E be an elliptic curve over $\mathbb{F}_p$ with a large prime order subgroup $G = E[r](\mathbb{F}_p)$, and group structure $E(\mathbb{F}_p) \cong \mathbb{Z}_e^2 \times \mathbb{Z}_r$ for some $e \in \mathbb{N}$. Let $P \in E(\mathbb{F}_p)$. Then*

$$P \in G \quad \textit{if and only if} \quad t_{[e]}(P) \textit{ is trivial.}$$

Proof. By now, this is clear: the Tate profile $t_{[e]}(P)$ is trivial if and only if $P \in [e]E(\mathbb{F}_p)$, which in this case is precisely the subgroup $G = E[r](\mathbb{F}_p)$.

Elliptic curves that are used in practice often do not have precisely the group structure as above, so we require slight changes to the profiles that we need, as explained in [DHKP+24, Kos23]. However the main idea is the same: we may check for triviality with respect to a *cofactor*, to ensure a point must be in the prime-order subgroup. Of course, we may even

[7] 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.

apply the same idea in higher dimensions: as a fun exercise in optimizing 2-Tate pairing computations on Kummer surfaces, I explored subgroup membership testing for the Gaudry-Schost Kummer surface [GS12] in a note on my website. This surface is associated to the Jacobian $\mathcal{J}$ of a genus-2 curve with group structure

$$\mathcal{J}(\mathbb{F}_p) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_r,$$

where r is a 250-bit prime. And so, to verify that $P \in \mathcal{J}[r](\mathbb{F}_p)$, we may simply compute the 2-Tate profile $t_{[2]}(P)$ with respect to a basis of $\mathcal{J}[2](\mathbb{F}_p) = \mathcal{J}[2]$, which requires four Tate pairings of degree 2. Optimizing this computation is a fun challenge in cubical arithmetic and Kummer arithmetic, with the full details in the note.

Remark 3. A curious case is the Four$\mathbb{Q}$-curve [CL15] E over $\mathbb{F}_{p^2}$, of order $\#E(\mathbb{F}_{p^2}) = 2^3 \cdot 7^2 \cdot r$ where r is a 246-bit prime. One works in the subgroup $G = E[r](\mathbb{F}_{p^2})$. To verify membership of $P \in G$, we may either compute $[r]P = \mathbf{o}_E$, or, as $E[7]$ is rational, perform a combination of Koshelev's subgroup membership testing using the triviality of $t_{[7]}(P)$ together with halving formulas [Por22]. It is unclear to me which of these two approaches is faster, although the latter approach has the advantage that most of the pairing computation can be precomputed.

Isotropic Membership Testing. There is an interesting specialized case of subgroup membership testing which arises only in dimension $g > 1$: Let $P, Q \in A[\ell]$ where ℓ is prime, one may wonder whether Q is a multiple of P or not, that is $Q \in \langle P \rangle$. Whereas in dimension 1, this is easily resolved by $e_\ell(P, Q) \neq 1$, in higher dimensions P and Q may be isotropic. To resolve this issue, we find a third point $R \in A[\ell]$ which is non-isotropic to P, and set $\zeta_0 = e_\ell(R, P)$ and $\zeta_1 = e_\ell(R, Q)$. If $Q \in \langle P \rangle$, then $Q = [a]P$ for some unknown $a \in \mathbb{Z}/\ell\mathbb{Z}$, and using R we get $a = \log_{\zeta_0}(\zeta_1)$ and can verify $Q = [a]P$. If $Q \notin \langle P \rangle$, then we can still compute $a = \log_{\zeta_0}(\zeta_1)$ and $[a]P$, but we will find that $Q \neq [a]P$. Hence, in the first case we find that the subgroup $\langle P, Q \rangle = \langle P \rangle \cong \mathbb{Z}/\ell\mathbb{Z}$ is rank 1, whereas in the second case we find that the *isotropic* subgroup $\langle P, Q \rangle \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ is rank 2.[8]

5.8 And many more[9]

The recent work PEGASIS [DEFM+25] 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 $2^f \mid p + 1$.

[8] The use of an additional point $R \in A[\ell]$ to resolve the discrete logarithm problem in P and Q is a natural generalization of the MOV-attack [MVO91] on elliptic curves.

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

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, [DEFM+25, 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 [Rob23] to prove conjectures regarding (multi-)radical isogenies [CD21, CDV20]. 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 [BGS22, Dol18] can be understood as studying such fibers.[10]

Lastly, several of the algorithms in [Reij23] 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 $E(\mathbb{F}_p)$.

[10] In fact, this note is mostly an exposition of examples in [Rob23].

References

[BCMN+15] Paulo SLM Barreto, Craig Costello, Rafael Misoczki, Michael Naehrig, Geovandro CCF Pereira, and Gustavo Zanon. "Subgroup security in pairing-based cryptography". In: *Progress in Cryptology–LATINCRYPT 2015: 4th International Conference on Cryptology and Information Security in Latin America, Guadalajara, Mexico, August 23-26, 2015, Proceedings 4*. Springer. 2015, pp. 245–265 (cit. on p. 16).

[BGS22] 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. 18).

[Bow19] Sean Bowe. *Faster Subgroup Checks for BLS12-381*. Cryptology ePrint Archive, Paper 2019/814. 2019. URL: https://eprint.iacr.org/2019/814 (cit. on p. 16).

[Bru11] 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. 2, 4, 8).

[BS96] Wieb Bosma and Peter Stevenhagen. "On the computation of quadratic 2-class groups". In: *Journal de théorie des nombres de Bordeaux* 8.2 (1996), pp. 283–313 (cit. on pp. 14, 15).

[CD20] Wouter Castryck and Thomas Decru. "CSIDH on the surface". In: *International Conference on Post-Quantum Cryptography*. Springer. 2020, pp. 111–129 (cit. on p. 10).

[CD21] Wouter Castryck and Thomas Decru. "Multiradical isogenies". In: *Arithmetic, Geometry, Cryptography, and Coding Theory* 779 (2021), pp. 57–89 (cit. on p. 18).

[CDV20] 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. 18).

[CEMR24] 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. 3).

[CL15] Craig Costello and Patrick Longa. "Four$\mathbb{Q}$: Four-Dimensional Decompositions on a $\mathbb{Q}$-curve over the Mersenne Prime". In: *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I*. 2015, pp. 214–235. DOI: 10.1007/978-3-662-48797-6_10. URL: https://doi.org/10.1007/978-3-662-48797-6%5C_10 (cit. on p. 17).

[Cos18] 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. 12).

[CR24] 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. 2, 5, 7, 8, 12, 13).

[DEFM+25] 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 pp. 17, 18).

[DHKP+24] Yu Dai, Debiao He, Dmitri 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. 16).

[Dol18] 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. 18).

[GS12] Pierrick Gaudry and Éric Schost. "Genus 2 point counting over prime fields". In: *Journal of Symbolic Computation* 47.4 (2012), pp. 368–400 (cit. on p. 17).

[Hus04] Dale Husemöller. *Elliptic Curves, 2nd edition*. Springer, 2004 (cit. on p. 2).

[IJ13] Sorina Ionica and Antoine Joux. "Pairing the volcano". In: *Mathematics of Computation* 82.281 (2013), pp. 581–603 (cit. on pp. 10, 12).

[Kos23] Dmitrii I. Koshelev. "Subgroup membership testing on elliptic curves via the Tate pairing". In: *J. Cryptogr. Eng.* 13.1 (2023), pp. 125–128. DOI: 10.1007/S13389-022-00296-9. URL: https://doi.org/10.1007/s13389-022-00296-9 (cit. on p. 16).

[LL97] Chae Hoon Lim and Pil Joong Lee. "A key recovery attack on discrete log-based schemes using a prime order subgroup". In: *Advances in Cryptology—CRYPTO'97: 17th Annual International Cryptology Conference Santa Barbara, California, USA August 17–21, 1997 Proceedings 17*. Springer. 1997, pp. 249–263 (cit. on p. 16).

[lS17] luigi1111 and Riccardo "fluffypony" Spagni. *Disclosure of a Major Bug in CryptoNote-Based Currencies*. Accessed: 2025-04-23. May 2017. URL: https://www.getmonero.org/2017/05/17/disclosure-of-a-major-bug-in-cryptonote-based-currencies.html (cit. on p. 16).

[MMRV05] Josep M. Miret, Ramiro Moreno, Anna Rio, and Magda Valls. "Determining the 2-Sylow subgroup of an elliptic curve over a finite field". In: *Math. Comput.* 74.249 (2005), pp. 411–427. DOI: 10.1090/S0025-5718-04-01640-0. URL: https://doi.org/10.1090/S0025-5718-04-01640-0 (cit. on pp. 14, 15).

[MMRV09] Josep M. Miret, Ramiro Moreno, Anna Rio, and Magda Valls. "Computing the -power torsion of an elliptic curve over a finite field". In: *Math. Comput.* 78.267 (2009), pp. 1767–1786. DOI: 10.1090/S0025-5718-08-02201-1. URL: https://doi.org/10.1090/S0025-5718-08-02201-1 (cit. on pp. 14, 15).

[MPR10] Josep M. Miret, Jordi Pujolàs, and Anna Rio. "Explicit 2-power torsion of genus 2 curves over finite fields". In: *Adv. Math. Commun.* 4.2 (2010), pp. 155–168. DOI: 10.3934/

AMC.2010.4.155. URL: https://doi.org/10.3934/amc.2010.4.155 (cit. on pp. 14, 15).

[MVO91] Alfred Menezes, Scott Vanstone, and Tatsuaki Okamoto. "Reducing elliptic curve logarithms to logarithms in a finite field". In: *Proceedings of the twenty-third annual ACM symposium on Theory of computing*. 1991, pp. 80–89 (cit. on p. 17).

[Por22] Thomas Pornin. *Point-Halving and Subgroup Membership in Twisted Edwards Curves*. Cryptology ePrint Archive, Paper 2022/1164. 2022. URL: https://eprint.iacr.org/2022/1164 (cit. on p. 17).

[Reij23] 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. 18).

[Reij25] Krijn Reijnders. "The Tate Profile". In: *Progress in Cryptology - LATINCRYPT 2025 - 9th International Conference on Cryptology and Information Security in Latin America, LATINCRYPT 2025, Medellin, Colombia, October 1-3, 2025, Proceedings*. Springer. 2025 (cit. on p. 1).

[Rob23] 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. 2, 4, 8, 10, 12, 18).

[Sch03] Jasper Scholten. "Weil restriction of an elliptic curve over a quadratic extension". In: *Preprint* (2003) (cit. on p. 12).

[Sco21] Michael Scott. "A note on group membership tests for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ on BLS pairing-friendly curves". In: (2021). URL: https://eprint.iacr.org/2021/1130 (cit. on p. 16).

[ZSPD+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. 3).

A Updates

2025-03-13. Initial version.
2025-07-28. Added details on higher-dimensional Tate profiles, expanded the section on subgroup membership testing, and added footnote to reader on how to cite (page 1).
2025-07-29. Added a section on deterministic bases and their use in isogeny compression, and improved citation style.
2025-08-26. Added a section on computing the Sylow-ℓ torsion even when the group structure of $A(\mathbb{F}_q)$ is unknown.
2026-02-09. Fixed a mistake noticed by Lorenz Panny in the algorithmic description in Section 5.5.
2026-03-19. Fixed a typo in Lemma 5, added the repository with example code, and added isotropic membership testing.