The Tate Profile

Krijn Reijnders*

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

Abstract. This work explores the Tate profile and its applications. We show that, framed using Tate profiles, several well-known results on divisibility and basis sampling become natural. Then, having rewritten these results in this more natural setting, we generalize and optimize several use cases: First, we use Tate profiles to generalize entangled basis generation to any Weierstrass curve. Second, we optimize the computation of degree-2 Tate pairings on Kummer surfaces using cubical arithmetic, which allows us to compute the 2-Tate profile in only 6 additions, 10 multiplications, and 4 Legendre symbols. Third, we apply the optimized 2-Tate profile computation to perform subgroup membership testing on the Gaudry–Schost Kummer Surface, smoothly combining these ideas.

Keywords: pairings · isogenies · Kummer surfaces

[*] This paper is a merge of two notes:

- *The Advanced Use of the Tate Pairing*, available at 2025/477, in which I discuss the Tate pairing and Tate profile, its role in isogeny-based cryptography, and its applications with respect to divisibility. In this note, I also generalize entangled basis generation, which is Lemma 5 in this work. The note captures most of the content of Section 3 and Section 4 of this paper.
- *Optimized Cubical Pairings of Degree 2 for Subgroup Membership Testing in Genus 2*, available at my website, in which I try to optimize the computation of degree-2 Tate pairings on Kummer surfaces, both for a general and specific Kummer surfaces. As an application, I show that this can be used to perform subgroup membership testing. The note captures most of the content of Section 5 and Section 6 of this paper.

In my opinion, the notes are self-contained and have a better reading experience than this paper. For citation purposes, however, I recommend citing this paper instead of the notes, as it is published in the proceedings of LATINCRYPT 2025:

> 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.

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: 2025-07-22.

1 Introduction

Pairings have been ubiquitous in curve-based cryptography, both as an adversarial and constructive tool in elliptic curve cryptography [MVO91; FR94; HSSI99; Jou04], as the main points of interest in pairing-based cryptography [BLS01; BF01; BKLS02; GHS02; Jou02; BGLS03; BLS04; Gal05; Ver09], and again as an adversarial and constructive tool in isogeny-based cryptography [CJL+17; KT18; Reij23; CHM+23; LWXZ24; MS24]. This work specifically looks at the Tate pairing. Often, we look at a single pairing value $t_n(P,Q)$ to learn something about the relation between P and Q, or we use several pairing values and the properties of the Tate pairing to derive a result.

The easiest example of the usability of the Tate pairing is given on Montgomery curves $E_A : y^2 = x^3 + Ax^2 + x$, with $A \in \mathbb{F}_q$, where any point P with non-square x-coordinate x_P must be in the set $E_A \setminus [2]E_A$. It is no coincidence that the quadratic character of x_P is also exactly the value of the degree-2 reduced Tate pairing $t_2(L_0, P)$ where $L_0 = (0,0) \in E_A[2]$. In this example, the Tate pairing allows us to transform something we know about $E_A[2]$ into something we know about $[2]E_A$. In fact, this correspondence between $E_A[2]$ and $[2]E_A$, or in other words, between the kernel and the image of the endomorphism $[2] : E_A \to E_A$ is one of the core properties of the Tate pairing, and highlights its connection to divisibility.

This study of divisibility by $[\ell]$ quickly leads to useful building blocks in modern isogeny-based cryptography [CJL+17; ZSP+18; CEMR24], which highly impact the practical performance of schemes: When computing isogenies of large smooth degree, for example 2^n, we often rely on Vélu's formulas [Vél71; BDLS20] to compute these isogenies, which often takes a generator K of the kernel as input. To describe K, we may take a basis P, Q of $E[2^n]$ and express K as a linear combination $[a]P + [b]Q$, for some $a, b \in \mathbb{Z}_{2^n}$. Finding such a basis is linked to divisibility, as we must look for these points P and Q in the set $E \setminus [2]E$, i.e., those points that are *not* divisible by [2].

Another example is subgroup membership testing, in the context of elliptic-curve cryptography. Subgroup membership testing asks if a point $P \in E(\mathbb{F}_q)$ is a member of a particular subgroup $G \subset E(\mathbb{F}_q)$. Usually, G is a subgroup of large prime order r of $E(\mathbb{F}_q)$, and we assume the hardness of the discrete logarithm in G to build cryptographic primitives. 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 [BCM+15; Bow19; Sco21]. A recent innovation by Koshelev [Kos23] applies the non-degeneracy of the Tate pairing to subgroup membership testing. For certain curves, this may outperform previous methods when the Tate pairing computation is fast, and the parameters of the elliptic curve are suitable.

In recent years, the Tate pairing has been put into a wider context: Bruin [Bru11] highlights the connection of the Tate pairing to isogenies, and shows that we may define a (generalized) Tate pairing t_ϕ for any isogeny $\phi : E \to E'$,

$$t_\phi : (\ker \phi)(k) \times (\operatorname{coker} \widehat{\phi})(k) \to \mu_n$$

instead of the classical Tate pairing t_n defined with respect to the endomorphism $[n] : E \to E$. Similarly to our initial example, such a generalized Tate pairing is able to transform knowledge of the kernel of ϕ into knowledge of the image of the dual $\widehat{\phi}$, and vice versa. Expanding on this, Robert [Rob23] rephrases the Tate pairing as a map that allows us to study the fibers $\phi^{-1}(P)$ of an isogeny ϕ, as a single abstraction that covers many of the examples given above, and many other results can similarly be phrased in this context [IJ13; Dol18; CDV20].

When placed in this broader context, we find that it is easier to see several individual Tate pairing as a single object instead, which we denote the Tate profile [Rob23; CR24]. Starting with the Tate profile as our essential tool, we study core properties of $\phi^{-1}(P)$, following the theoretical framework of [Rob23].

Contributions.

In this work we explore the Tate profile and its applications. First, in Section 3, we derive a result that shows how the Tate profile allows us to transform knowledge of the rational ℓ-torsion into knowledge of the Sylow ℓ-subgroup, that is, the largest rational $\ell^\bullet$-torsion. This result, Theorem 1, lies at the heart of many of the later results, as it shows that thinking in terms of the Tate profile helps us to understand most results that rely on Tate pairings.

Second, in Section 4, we rephrase smart torsion basis sampling [CEMR24], entangled basis generation [ZSP+18], and subgroup membership [Kos23] in terms of Tate profiles, which gives us a deeper understanding of these results and their connection to the Tate pairing. This allows us to generalize these results to different curves or higher dimensions.

Third, in Section 5, to achieve an efficient computation of the 2-Tate pairing on Kummer surfaces, we study cubical arithmetic [Rob24] to compute such pairings, and highly optimize the computation of the 2-Tate profile. We are able to compute the 2-Tate profile in only 6 additions, 10 multiplications, and 4 Legendre symbols.

Lastly, in Section 6, we look at a concrete example in which most of the above comes together: subgroup membership testing on the Gaudry–Schost Kummer surface [GS12]. As a challenge, we try to perform subgroup membership testing on this surface as efficiently as possible, by combining a higher-dimensional application of Koshelev's method [Kos23] with the optimized cubical arithmetic from Robert [Rob24]. Although this approach to subgroup membership testing is significantly faster than other approaches, our main goals are to **a.)** highlight the usefulness of the Tate profile, and **b.)** showcase the effectiveness of cubical arithmetic to compute Tate profiles.

2 Preliminaries

Notation. We work mostly over $\mathbb{F}_p$. An extension is denoted by $\mathbb{F}_q$ for $q = p^m$. Whenever we write $\mathbb{Z}_n$, we mean $\mathbb{Z}/n\mathbb{Z}$, the integers modulo n. We denote exact divisibility by $a \parallel b$. When working with Jacobians $\mathcal{J}/\mathbb{F}_p$, we describe the 2-torsion by $D_{i,j} \in \mathcal{J}[2]$, which refers to element of $\mathcal{J}$ associated to the divisor $(w_i, 0) + (w_j, 0)$, where w_i, w_j are Weierstrass points of the hyperelliptic curve. We assume this curve is in Rosenhain form, and so $w_1 = \infty$, $w_2 = 0$, $w_3 = 1$, $w_4 = \lambda$, $w_5 = \mu$, and $w_6 = \nu$. More details can be found in, for example, [CR24, §2].

On their Kummer surfaces, we denote by $L_{i,j} \in \mathcal{K}[2]$ the point associated to $D_{i,j} \in \mathcal{J}[2]$. The map $Q \mapsto Q + L_{i,j}$ is well-defined for 2-torsion points $L_{i,j}$, and can be given as a (4×4)-matrix, which we denote by $W_{i,j}$.

On Kummer surfaces, we denote a point $Q \in \mathcal{K}$ by $(Q_1 : Q_2 : Q_3 : Q_4) \in \mathbb{P}^3(\mathbb{F}_p)$, which is defined up to scalars. An *affine lift* for Q is denoted by $\widetilde{Q}$, and in this work specifically refers to any choice $(Q_1, Q_2, Q_3, Q_4) \in \mathbb{F}_p^4$ that represents Q. We may normalize such a lift $\widetilde{Q}$ in index k by $Q_i \mapsto Q_i/Q_k$, as long as $Q_k \neq 0$.

Operations in $\mathbb{F}_p$ are denoted by $\mathbf{M}$ for multiplication, $\mathbf{S}$ for squaring, $\mathbf{A}$ for addition, and $\mathbf{L}$ for the Legendre symbol. Whenever we refer to $\mathbb{F}_p$-operations, we use the model $\mathbf{S} = 0.8\mathbf{M}$ and $\mathbf{A} = 0.05\mathbf{M}$. We estimate $1\mathbf{L}$ at $125\mathbf{S} + 9\mathbf{M}$ using an addition chain [McL21].

Terminology. In this work, we will often refer to a *basis* $(P_1, \ldots, P_r)$ for some subgroup $G \subseteq A(k)$ of an abelian variety A, for example, $G = (\ker f)(k)$ for an isogeny $f : A \to B$, or $G = A(k)[n]$ is the rational n-torsion. In the elliptic curve case, we usually do not define what is meant by a basis, as it is understood from the context, but for higher dimensions we need to be a bit more careful.

Definition 1. *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*

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

where $\phi(P_i) = (0, \ldots, 0, 1, 0, \ldots, 0)$, 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. Often in this article, we 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 $E \to E/\langle K \rangle$,

2.1 The Generalized Tate Pairing

This work requires a generalized notion of the original Tate-Lichtenbaum pairing [Tat62; Lic69] on abelian varieties, which was introduced in a cryptographic context by Frey and Rück [FR94]. Over a finite field k, Bruin [Bru11] shows how to generalize the Tate pairing to any isogeny $f : A \to B$ between principally polarized abelian varieties A and B to obtain the generalized Tate pairing

$$T_f : (\ker f)(k) \times (\operatorname{coker} \hat{f})(k) \to k^*/k^{*,n},$$

where $(\operatorname{coker} \hat{f})(k) = A(k)/\hat{f}(B(k))$ and n is the exponent of $\ker f$. This pairing is also referred to as the Tate-Cartier pairing, and is explored by Robert [Rob23]. We slightly abuse notation here, by swapping the roles of f and its dual $\hat{f}$, which allows us to present some results more cleanly. In this work, we will often take for A and B the (Jacobians of) elliptic or hyperelliptic curves. If we take the endomorphism $f = [n]$ of degree n^2 and exponent n on a Jacobian $\mathcal{J}$, we obtain the original Tate pairing

$$T_n : \mathcal{J}[n](k) \times \mathcal{J}(k)/[n]\mathcal{J}(k) \to k^*/k^{*,n}.$$

Over a finite field $k = \mathbb{F}_q$ where n divides $q - 1$, we get a unique representative of the class $T_n(P, Q) \in k^*/k^{*,n}$ by raising any representative to the power $\frac{q-1}{n}$, giving us an n-th root of unity $\zeta \in \mu_n$. This combination is the *reduced* Tate pairing of degree n

$$t_n : \mathcal{J}[n](k) \times \mathcal{J}(k)/[n]\mathcal{J}(k) \to \mu_n.$$

Computation. Miller's algorithm [Mil04] enables efficient computation on the Jacobian. Methods to compute the Tate pairing are developed in [Sta07; LR10; LR15; LR16; Rob24]. Computing pairings on the Kummer variety of an abelian variety is more difficult. We discuss this for Kummer surfaces in Section 2.3, more generally see [Rob24].

2.2 Kummer Surfaces

Only a few years after the birth of elliptic-curve cryptography [Mil85; Kob87], Koblitz [Kob89] showed that one may just as well use curves of larger genus. In particular, genus-2 hyperelliptic curves, and their Jacobians, seem well-suited for cryptography based on the discrete-logarithm problem.

To improve the efficiency, one may choose to work on the *Kummer surface* of a Jacobian,[1] the higher-dimensional analogue to x-only arithmetic of elliptic curves. Already in 1986, Chudnovsky and Chudnovsky [CC86] realized the efficiency of Kummer surfaces, with the idea to apply this to factorization tests. Gaudry [Gau07] shows that working on the Kummer surface similarly improves cryptography in genus 2 as the Kummer surface has enough structure to allow us to compute $P \mapsto [n]P$. A good introduction to arithmetic in genus 2 can be found in Cassels and Flynn [CF96].

In genus 2, however, it is much harder to find secure curves, compared to genus 1. We want to find a curve such that the Jacobian has a large enough prime-order subgroup, and such that its *twist* has a similarly large prime-order subgroup. Furthermore, several other technical details are important to achieve fast arithmetic on their related Kummer surfaces. Through a large computational search, Gaudry and Schost [GS12] found a nearly perfect Jacobian over the prime $p = 2^{127} - 1$. We briefly describe the Jacobian, and its associated Kummer surface, as given in [BCHL16, §5.5.1]. A more detailed description of Kummer surfaces is given in [CR24, §2].

Example 1 (The Gaudry–Schost Kummer Surface). The fundamental constants $(a^2, b^2, c^2, d^2) = (11, -22, -19, -3) \in \mathbb{F}_p^4$, where $p = 2^{127} - 1$, give us a Kummer surface $\mathcal{K}/\mathbb{F}_p$ which we call the *Gaudry–Schost Kummer surface*. It is the Kummer surface associated to the Jacobian $\mathcal{J}/\mathbb{F}_p$ defined by the Rosenhain invariants

$$\begin{aligned}\lambda &= 28356863910078205288614550619314017618,\\ \mu &= 154040945529144206406682019582013187910,\\ \nu &= 113206060534360680770189432771018826227.\end{aligned}$$

The Jacobian $\mathcal{J}$ has $2^4 \cdot r$ rational points, and its twist $\mathcal{J}^T$ has $2^4 \cdot r'$ rational points, where r and r' are the primes

$$\begin{aligned}r &= 1809251394333065553414675955050290598923508843635941313077767297801179626051,\\ r' &= 1809251394333065553571917326471206521441306174399683558571672623546356726339.\end{aligned}$$

The zero point is $\mathbf{0}_{\mathcal{K}} = (a^2, b^2, c^2, d^2)$. To do arithmetic on the Kummer surface, we use the usual building blocks: the Hadamard transform, the 4-way squaring, and the 4-way multiply.

Remark 1. A similar Kummer surface over $p = 2^{128} - 34827$ is given in [BCHL16, §5.5.2]. As the group structure is similar, the techniques in this work apply directly to this Kummer surface too.

The origin of points on the Kummer surface. Points $P \in \mathcal{K}(\mathbb{F}_p)$ are either associated to a point $\bar{P} \in \mathcal{J}(\mathbb{F}_p)$ on the Jacobian, or to a point $\bar{P}' \in J^T(\mathbb{F}_p)$ on

[1] We choose to use the language of Kummer surfaces, although our work can be interpreted in the language of theta structures of level 2 for abelian surfaces as well.

its twist. In the former case, we say that a point $P \in \mathcal{K}(\mathbb{F}_p)$ *originates from* the Jacobian, whereas in the latter case, P originates from the twist. An algorithm to compute the origin of a point is given in [CR24, §4.1]. For the Gaudry–Schost Kummer surface, checking the origin of a point using this algorithm takes $22\mathbf{M} + 1\mathbf{S} + 13\mathbf{A} + 1\mathbf{L}$.

2.3 Pairings on Kummer Surfaces

For this work, we require level-2 pairings on Kummer surfaces. We quickly discuss two methods in details: first, using a partial map back to the Jacobian [CR24], and second, the more natural approach using cubical arithmetic [Rob24].

Pairings using a partial map to the Jacobian. Intuitively, computing pairings on Jacobians is simpler to understand than on Kummer surfaces, as we can perform Miller's algorithm [Mil04] on the Jacobian. Hence, if we can find an associated $P \in \mathcal{J}(\mathbb{F}_p)$ such that $Q = \rho(P)$ for the map $\rho : \mathcal{J}(\mathbb{F}_p) \to \mathcal{K}(\mathbb{F}_p)$, we can compute the required pairings on $\mathcal{J}(\mathbb{F}_p)$ using P. In particular, for the Tate pairing of degree 2, given $D_{i,j} \in \mathcal{J}[2]$ and $P \in \mathcal{J}(\mathbb{F}_p)$ in Mumford representation

$$D_{i,j} = \langle (x - w_i)(x - w_j), 0 \rangle, \quad P = \langle a(x), b(x) \rangle,$$

with $a(x) \in \mathbb{F}_p[x]$, we can compute the (non-reduced) Tate pairing as the resultant of $(x - w_i)(x - w_j)$ and $a(x)$. Hence, given $Q \in \mathcal{K}(\mathbb{F}_p)$, we only need to recover $a(x)$ from Q to compute the pairings.

Such a map $\mathcal{K}(\mathbb{F}_p) \to \mathbb{F}_p[x]$, with $Q \mapsto a(x)$ is given in [CR24, §2.7], as a partial inverse to the map $\mathcal{J}(\mathbb{F}_p) \to \mathcal{K}(\mathbb{F}_p)$. Given $a(x)$, we may then compute the 2-Tate pairing with respect to $D_{i,j} \in \mathcal{J}[2]$.

Cubical pairings of degree 2. In [Rob24], Robert introduces *cubical arithmetic* to compute pairings, specializing to Kummer varieties in §4.7. With this, we compute Tate pairings on Kummer surfaces naturally, without moving to the Jacobian.

The Tate pairing of degree $n = 2$ is special, as it requires almost none of the machinery of cubical arithmetic, beyond *translations*: Given a point $L_{i,j} \in \mathcal{K}[2]$, and any point $Q \in \mathcal{K}(\mathbb{F}_p)$, the point $L_{i,j} + Q$ is well-defined. The map $Q \mapsto L_{i,j} + Q$ is given by a (4×4)-matrix which we denote $W_{i,j}$. These matrices $W_{i,j}$ are given in [CR24, App. A] in terms of the coefficients of $\mathbf{0}_{\mathcal{K}}$ and the Rosenhain invariants of the associated Jacobian.

To compute the pairing $t_2(L_{i,j}, Q)$ using cubical arithmetic[2], we compute two values[3] λ_Q and $\lambda_{L_{i,j}}$ using the translation matrix $W_{i,j}$. The pairing $t_2(L_{i,j}, Q)$ is then given by the Legendre symbol of λ_Q/λ_P. We describe the cubical pairing computation of degree 2 on $\mathcal{K}(\mathbb{F}_p)$ in Algorithm 1, which is slightly adjusted from [Rob24] for easier implementation.

[2] For full details, see [Rob24, Alg. 5.2]. For a more friendly introduction, see [PRR+25].

[3] More properly speaking, monodromies [Sta07; Rob24].

Algorithm 1 Degree-2 cubical pairing computation on $\mathcal{K}(\mathbb{F}_p)$

```
Input: The point $Q$ as $(Q_1, Q_2, Q_3, Q_4)$, the normalization index $n_{ij}$, and the matrix $W_{i,j}$.
Output: The reduced Tate pairing $t_2(L_{i,j}, Q) \in \mu_2$.
$\widetilde{L_{i,j}} \leftarrow W_{i,j} \cdot \widetilde{\mathbf{0}_\mathcal{K}}$
$\widetilde{L_{i,j} + Q} \leftarrow W_{i,j} \cdot \widetilde{Q}$            ▷ Compute $L_{i,j} + Q$
$\widetilde{2L_{i,j}} \leftarrow W_{i,j} \cdot \widetilde{L_{i,j}}$            ▷ Translate $L_{i,j}$
$\left(\widetilde{2L_{i,j} + Q}\right) \leftarrow W_{i,j} \cdot \left(\widetilde{L_{i,j} + Q}\right)$            ▷ Translate $L_{i,j} + Q$
$\lambda_{L_{ij}} \leftarrow (\widetilde{2L_{i,j}})_{n_{i,j}} / (\widetilde{L_{i,j}})_{n_{i,j}}$
$\lambda_Q \leftarrow (\widetilde{2L_{i,j} + Q})_{n_{i,j}} / (\widetilde{L_{i,j} + Q})_{n_{i,j}}$
$\zeta \leftarrow \mathsf{Legendre}(\lambda_Q / \lambda_{L_{ij}})$
return $\zeta$
```

3 The Tate Profile

In this section we analyze the Tate profile and give a crucial connection between the Tate pairing of degree ℓ and the ℓ-Sylow subgroup of $E(\mathbb{F}_q)$ in Theorem 1, which captures the essence of many subsequent results in this work.

The description in terms of Tate profiles heavily relies on the results in [Rob23, Sec. 5]. We hope that rephrasing those results allows for a more concrete and practical understanding, suitable for applications. Although Sections 3.1 and 3.2 are written for general abelian varieties to prove Theorem 1, later sections only require such results for elliptic curves or Jacobians of hyperelliptic curves. All isogenies in this section are assumed to be separable, and we are working over a finite field $k = \mathbb{F}_q$ of characteristic p.

3.1 The Tate Profile

The Tate profile [CR24] of an isogeny $f : A \to B$ allows us to study the properties of the Tate pairing T_f in a single object, by evaluating a point $Q \in A(k)$ in a basis of $\ker f$, as defined in Definition 1. The profile rephrases several of the ideas explored in [Rob23; CR24].

Definition 2. *Let $f : A \to B$ be a separable isogeny between abelian varieties A and B over a finite field k, and let n be the exponent of $(\ker f)(k)$ and r its rank. Let $(P_1, \ldots, P_r)$ be a basis for $(\ker f)(k)$, so that P_i has order d_i for all i. The* Tate profile *$t_{\ker f}$ associated to the reduced generalized Tate pairing $t_f : (\ker f)(k) \times (\operatorname{coker} \hat{f})(k) \to \mu_n$ with respect to this basis is the map*

$$\begin{aligned} t_{\ker f} : A(k) &\to \mu_{d_1} \times \ldots \times \mu_{d_r} \\ Q &\mapsto (t_f(P_1, Q), \ldots, t_f(P_r, Q)) \end{aligned}$$

We refer to $t_{\ker f}(Q)$ for $Q \in A(k)$ as the Tate profile of Q. We say that the profile $t_{\ker f}(Q)$ is trivial*, when $t_{\ker f}(Q) = (1, \ldots, 1)$.*

From the bilinearity of the Tate pairing, the Tate profile inherits linearity. When the Tate pairing is non-degenerate, the Tate profile then induces an isomorphism

$$(\operatorname{coker} \hat{f})(k) \xrightarrow{\sim} \mu_{d_1} \times \ldots \times \mu_{d_r}.$$

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. In practice, we will mostly use the Tate profile either in the case where f is a separable $(n, \ldots, n)$-isogeny between principally polarized abelian varieties, so that we get a map $t_{\ker f} : A(k) \to \mu_n^r$ with $r = g$, or the case $f = [n]$ with $t_{\ker f} : A(k) \to \mu_n^r$ with $r = 2g$ if the $[n]$-torsion is rational. In both these cases, non-degeneracy of the Tate pairing t_f gives us an isomorphism

$$t_{\ker f} : (\operatorname{coker} \hat{f})(k) \xrightarrow{\sim} \mu_n^r, \tag{1}$$

which will be key to the results in this work. A trivial but useful corollary of this definition is the following.

Corollary 1 ([Rob23, Cor. 5.2]). *If the Tate pairing t_f is non-degenerate, then*

$$t_{\ker f}(Q) \textit{ is trivial} \quad \Leftrightarrow \quad Q \in \widehat{f}(B(k)).$$

In other words, $\ker t_{\ker f} = \hat{f}(B(k))$.

Many divisibility results require only this corollary, in particular for the Tate pairing t_n associated to scalar multiplication by $[n]$, as we get that $Q \in [n]A(k)$ if the profile $t_{\ker[n]}(Q)$ is trivial. A notable exception is in [CR24, §3], which requires the full isomorphism to identify points with certain properties in $\mathcal{J}[2^f]$ for a specific Jacobian $\mathcal{J}$.

3.2 Sylow ℓ-torsion of Abelian Varieties

The Tate profile of degree n is a useful tool to analyze divisibility by $[n]$, as its kernel describes precisely those points divisible by $[n]$ on an abelian variety A. Similarly, for ℓ prime, we know that divisibility by ℓ is observable in the subgroup $A[\ell^\infty](\mathbb{F}_q)$. This section describes the close connection between the divisibility by $[\ell]$ and the subgroup $A[\ell^\infty](\mathbb{F}_q)$. To avoid the annoying notation $A[\ell^\infty](\mathbb{F}_q)$, we introduce the following notation.

Definition 3. *Let A be an abelian variety over $\mathbb{F}_q$ and ℓ a prime, coprime to p. The* Sylow ℓ-torsion *of $A(\mathbb{F}_q)$, which we denote $\mathcal{S}_{\ell,q}(A)$, is the unique subgroup $A[\ell^\infty](\mathbb{F}_q)$. As a group, $\mathcal{S}_{\ell,q}(A)$ is isomorphic to*

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

with $f_i \in \mathbb{N}$ such that $f_1 \geq f_2 \geq \ldots \geq f_d > 0$ and $d \leq 2g$.

The rank d is equal to the rank of the rational ℓ-torsion, as $A[\ell](\mathbb{F}_q) \subseteq \mathcal{S}_{\ell,q}(A)$, and the exponent is ℓ^{f_1}. An isogeny $f : A \to B$ induces a group homomorphism $\mathcal{S}_{\ell,q}(A) \to \mathcal{S}_{\ell,q}(B)$, and, when $\deg f$ and ℓ are coprime, this induced map is an isomorphism.

Example 2. Many of the later results will study $\mathcal{S}_{2,p^2}(E)$ for supersingular Montgomery curves E. When $2^f \parallel p+1$, we have the 'nice' structure

$$\mathcal{S}_{2,p^2}(E) \cong \mathbb{Z}_{2^f} \times \mathbb{Z}_{2^f},$$

whereas more generally we may have $\mathcal{S}_{2,p^2}(E) \cong \mathbb{Z}_{2^f} \times \mathbb{Z}_{2^g}$ for some $g < f$. Examples of sampling of points in this structure using the 2-Tate profile are ample in isogeny-based cryptography, and we revisit some examples in Section 4.

Example 3. The Jacobian $\mathcal{J}(\mathbb{F}_p)$ derived from Scholten's construction [Sch03] for supersingular elliptic curves E over $\mathbb{F}_{p^2}$ with $\mathcal{S}_{2,p^2}(E) \cong \mathbb{Z}_{2^f} \times \mathbb{Z}_{2^f}$ has the peculiar structure

$$\mathcal{S}_{2,p}(\mathcal{J}) \cong \mathbb{Z}_{2^{f-1}} \times \mathbb{Z}_{2^{f-1}} \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Sampling of points in this structure using the 2-Tate profile is explored in [CR24].

3.3 The Tate Profile and the Sylow ℓ-torsion.

As a concretization of Definition 1, we define what a basis for $\mathcal{S}_{\ell,q}(A)$ means.

Definition 4. *Let $\mathcal{S}_{\ell,q}(A) \cong \bigoplus_{i=1}^d \mathbb{Z}_{\ell^{f_i}}$. A* basis *$\mathcal{B}$ for $\mathcal{S}_{\ell,q}(A)$ is a minimal set of points $(P_1, \dots, P_d)$ that generates every point $Q \in \mathcal{S}_{\ell,q}(A)$ as a linear combination $\sum \lambda_i P_i$, with $\lambda_i \in \mathbb{Z}_{\ell^{f_i}}$. We write $\langle P_1, \dots, P_d \rangle = \mathcal{S}_{\ell,q}(A)$ to denote that $(P_1, \dots, P_d)$ is a basis for $\mathcal{S}_{\ell,q}(A)$.*

From any basis $\mathcal{B} = (P_i)_{i=1}^d$ of $\mathcal{S}_{\ell,q}(A)$, we easily find a description of $[\ell]A(\mathbb{F}_q)$, the points divisible by $[\ell]$, as the points

$$Q = \sum \lambda_i [\ell] P_i + R, \quad R \in [\ell^{f_1}]A(\mathbb{F}_q), \lambda_i \in \mathbb{Z}_{\ell^{f_i}}.$$

For principally polarized abelian varieties, the Tate profile of degree ℓ connects $A[\ell](\mathbb{F}_q)$ to $A(\mathbb{F}_q)/[\ell]A(\mathbb{F}_q)$. Given a basis $\mathcal{B} = (P_i)_{i=1}^d$ of $\mathcal{S}_{\ell,q}(A)$, we may represent the classes of $A(\mathbb{F}_q)/[\ell]A(\mathbb{F}_q)$, using the description above, by

$$\sum \lambda_i P_i + [\ell]A(\mathbb{F}_q), \quad \lambda_i \in \mathbb{Z}_\ell.$$

The following theorem captures the essence of the connection between the kernel $A[\ell]$ and divisibility by $[\ell]$, using the Tate profile. Recall that for $f = [\ell]$, the map $t_{\ker f}$ gives the isomorphism from (1), where r is the rank of $A[\ell](\mathbb{F}_q)$.

Theorem 1. *Let r denote the rank of $A[\ell](\mathbb{F}_q)$, assume the ℓ-Tate pairing is non-degenerate, and define the Tate profile $t_{\ker[\ell]}$ with respect to a basis of $A[\ell](\mathbb{F}_q)$. Then, for points $P_1, \dots, P_r \in A(\mathbb{F}_q)$, we get*

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

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

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

Proof. The map $[\ell] : A(\mathbb{F}_q) \to A(\mathbb{F}_q)$ has kernel $A[\ell](\mathbb{F}_q)$ by definition, whose size is ℓ^r by assumption. Thus, there are ℓ^r cosets which we may write as $P_i + [\ell]A(\mathbb{F}_q)$ for some $P_i \in A(\mathbb{F}_q)$. By the non-degeneracy of the ℓ-Tate pairing and Equation (1), we find that

$$Q \in \sum \lambda_i P_i + [\ell]A(\mathbb{F}_q) \quad \Leftrightarrow \quad t_{\ker[\ell]}(Q) = t_{\ker[\ell]}\left(\sum \lambda_i P_i\right).$$

By linearity, we find that $t_{\ker[\ell]}\left(\sum \lambda_i P_i\right) = \prod t_{\ker[\ell]}(P_i)^{\lambda_i}$. As a result, if the profiles $t_{\ker[\ell]}(P_i)$ span μ_ℓ^r, their combinations span every coset, and vice versa. Consequently, by killing any non-ℓ torsion using $[h]$, we obtain points $[h]P_i$ that are a basis for $\mathcal{S}_{\ell,q}(A)$. □

Concretely, this means that we can find such a basis for the Sylow ℓ-torsion if we have a basis for the kernel $A[\ell]$ and can efficiently compute the Tate profile (i.e., can efficiently compute the required Tate pairings): we sample random points of $A(\mathbb{F}_q)$ and compute their ℓ-Tate profiles until we find r points whose profiles span μ_ℓ^r, and then we clear the cofactor h.

Although Theorem 1 is written in a general setting, most of the results in this work follow from the general idea that we can derive as a consequence: if we know the ℓ-torsion, the ℓ-Tate profile helps us find a basis for the ℓ-Sylow torsion.

Remark 2. In the most practical case, we may apply the above mantra to the case $\ell = 2$, with E a supersingular elliptic curve and $2^f \parallel p + 1$. Then, if we know the rational 2-torsion $E[2](\mathbb{F}_{p^2})$ and we want to find points Q whose order is divisible by 2^f, the 2-Tate profile will be the essential tool that connects these Q to $E[2](\mathbb{F}_{p^2})$.

3.4 Single Tate Pairing Results As Profiles

One may wonder how we should handle the case of results that only use a single Tate pairing value $t_n(P, Q)$ for some $P \in E[n]$ and $Q \in E(\mathbb{F}_q)$, which do not seem to fit the above framework of Tate profiles. We argue that such results should be interpreted with respect to the cyclic isogeny $f : E \to E/\langle P \rangle$ and the generalized Tate pairing t_f, instead of the Tate pairing t_n associated to scalar multiplication by $[n]$.

With respect to this isogeny, the single Tate pairing value $t_n(P, Q)$ becomes the full Tate profile $t_{\ker f}(Q) = t_f(P, Q)$ as we have the basis $\ker f = \langle P \rangle$, instead of simply a partial profile with respect to $[n]$. We believe this more clearly demonstrates what the value $t_n(P, Q)$ illustrates: it signifies the position of $Q \in E(\mathbb{F}_q)$ with respect to the decomposition of $E(\mathbb{F}_q)$ into cosets $Q' + \widehat{f}(E'(\mathbb{F}_q))$, where $E' = E/\langle P \rangle$. We illustrate this with a few examples from the literature.

Example 4. Assume we are working with supersingular Montgomery curves over $\mathbb{F}_{p^2}$ with $2^f \mid p + 1$ so that $\mathcal{S}_{2,p^2} = \mathbb{Z}_{2^f} \times \mathbb{Z}_{2^f}$. A well-known trick to find points Q whose order is divisible by 2^f is to simply sample a non-square x_Q

until it defines a point $Q \in E(\mathbb{F}_{p^2})$ [CJL+17]. This should be interpreted as a non-trivial reduced Tate pairing of degree 2 with $P = (0,0)$, as we have that $t_2(P,Q) = x_Q^{\frac{q-1}{2}}$. Using the above interpretation, we can similarly say that Q has a non-trivial profile with respect to the degree-2 isogeny $f : E \to E'$ where $\ker f = \langle P \rangle$, and so, we find that Q is *not* in the image $\widehat{f}(E'(\mathbb{F}_{p^2}))$. This implies two things:

1. The order of Q is divisible by 2^f. Otherwise, there is an $R \in E(\mathbb{F}_q)$ such that $[2]R = \widehat{f}(f(R)) = Q$, which implies $Q \in \widehat{f}(E'(\mathbb{F}_{p^2}))$
2. The point Q is *not* above $(0,0)$. Namely, if Q is above $(0,0)$, then $f(Q)$ is of order 2^{f-1}, and there is an $R' \in E'(\mathbb{F}_{p^2})$ such that $[2]R' = f(Q)$. But then $\widehat{f}(R') = Q$.

This interpretation of the value $t_2(P,Q)$ gives us slightly more information: we learn something about the *position* of Q instead of only about the *order* of Q.

Example 5. The self-Tate pairing $t_\ell(P,P)$ for $P \in E(\mathbb{F}_q)$ gives us information about the ℓ-volcano structure [IJ13]. Indeed, Robert [Rob23] shows that, rephrased as the Tate profile, triviality of the value $t_\ell(P,P)$ implies that $P \in \widehat{f}(E'(\mathbb{F}_q))$ where $E' = E/\langle P \rangle$. Hence, $E'(\mathbb{F}_q)[\ell]$ must be rank 2: there is a point $P' \in E'[\ell]$ that generates the dual $\widehat{f}$, and some other point $Q' \in E'[\ell]$ that maps back to P under $\widehat{f}$.

4 Improving Known Results using Tate Profiles

In this section, we improve smart sampling [CEMR24], entangled basis generation [ZSP+18], and subgroup membership testing [Kos23] in terms of Tate profiles. We then generalize entangled basis generation to a wider set of elliptic curves.

Remark 3. This section focuses solely on elliptic curves. In the previous section we computed the profile with respect to a basis of $E[n]$. In this section, when $n = 2$, we will compute the profile with respect to all three points $E[2] \setminus \mathbf{0}_E$, which clarifies some results. For Montgomery curves $E_A : y^2 = x^3 + Ax^2 + x$, we use the notation $L_0 = (0,0)$, $L_1 = (\alpha, 0)$, and $L_2 = (1/\alpha, 0)$ to denote the three 2-torsion points, and we denote by $t_{[2]}(Q)$ the 2-Tate profile

$$t_{[2]}(Q) = (t_2(L_0,Q), t_2(L_1,Q), t_2(L_2,Q)) \in \mu_2^3$$

with respect to these three points. This is only meant to illustrate the results: the third value of the profile can be derived from the first two.

4.1 Smart Torsion Basis Sampling

Theorem 2 of AprèsSQI [CEMR24] shows that the quadratic characters of x, $x - \alpha$ and $x - 1/\alpha$ on Montgomery curves contain precise information on points $P \in E[2^f]$, namely, that they are above a certain 2-torsion point L_i.

Lemma 1 ([CEMR24, Thm. 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 $P \in E[2^f]$, then*

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

Lemma 1 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 interpretation: 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 $t_{[2]}(Q)$. The profile interpretation of Lemma 1 tells us that $t_{[2]}(P)$ indicates precisely the coset $P + [2]E(\mathbb{F}_q)$ that lies above a certain 2-torsion point.

Remark 4. In practice, Lemma 1 can be used to avoid certain edge cases: we may want to avoid cyclic 2^f-isogenies with $L_0 = (0, 0)$ in their kernel, and so, we can sample P above L_1 or L_2, and Q above L_0. Then, any combination $K = P + sQ$ for $s \in \mathbb{Z}_{2^f}$ gives us an isogeny $E \to E/\langle K \rangle$, whose kernel does not contain L_0.

We rephrase Lemma 1 in terms of the profile of the generalized Tate pairing with respect to the isogenies $E \to E/\langle L_i \rangle$, as described in Section 3.4, essentially generalizing Example 4.

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 $\phi_i : E \to E/\langle L_i \rangle$. Then,*

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

Proof. The proof is a repetition of Example 4: we have $t_{\ker \phi_i}(P) \neq 1$ only if $P \in E \setminus \widehat{\phi_i}(E'(\mathbb{F}_q))$. By writing out the action of ϕ_i and $\widehat{\phi_i}$ on $E[2^f]$, we find that $P \in E \setminus \widehat{\phi_i}(E'(\mathbb{F}_q))$ only if $2^f \mid \mathrm{Order}(P)$ and P is above L_i, i.e., $[2^{f-1}]P \neq L_i$. □

4.2 Entangled Basis Generation

Entangled basis generation [ZSP+18] allows us to sample a basis for $E[2^f]$ very efficiently, using a modification of the Elligator map [BHKL13]. Due to its efficiency, this approach is often used in practice. Examples are SIDH/SIKE [DJP14; JAC+17] and SQIsign [AAA+25].

Lemma 3 ([ZSP+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 $A \neq 0$. 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 $x_Q = -x_P - A$ defines a point $Q \in E(\mathbb{F}_{p^2})$, and $([h]P, [h]Q)$ is a basis for $E[2^f]$.

At first, this result feels somewhat magical: there is no good reason why this particular choice of x_Q would define a point on $E(\mathbb{F}_{p^2})$, nor why both points have order divisible by 2^f and together generate $E[2^f]$. Following the mantra, we must look at their 2-Tate profiles $t_{[2]}(P)$ and $t_{[2]}(Q)$.[4]

First, notice that the choice of x_P as a non-square implies that $t_{\ker\phi_i}(L_0, P) \neq 1$, hence from Example 4 P has order divisible by 2^f and is not above $(0,0)$. As $t_{\ker\phi_i}(L_0, P) \neq 1$, we furthermore get that $t_{[2]}(P)$ is non-trivial, so, either $(-1,1,-1)$ or $(-1,-1,1)$. Then, choosing x_Q as $-x_P - A$ ensures two things: First, $x_Q = -x_P - A = t^2 \cdot x_P$ is non-square too, and second, the quadratic character of $x_Q - \alpha$ and $x_Q - 1/\alpha$ can be computed as

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

where we use that $A = -\alpha - 1/\alpha$. Thus, this choice of x_Q ensure two things: x_Q determines a point $Q \in E(\mathbb{F}_{p^2})$ with a non-trivial profile, and this profile $t_{[2]}(Q)$ is the permutation of the profile $t_{[2]}(P)$, as it swaps the last two elements, i.e., mapping either $t_{[2]}(P) = (-1,-1,1) \mapsto t_{[2]}(Q) = (-1,1,-1)$, or vice versa. Although we know neither the profile of P, nor of Q, we know both profiles are different and non-trivial, hence some multiple of P and Q generate $E[2^f]$. Rephrased in Tate profiles, we get the following.

Lemma 4. *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.

We see that the magic is somewhat clarified: the choice of x_Q is determined by the permutation of the profile. This observation allows us to generalize this result in Section 4.3.

Remark 5. In contrast to Lemma 1, entangled basis generation does not give us the exact position of P and Q. However, we can still avoid $L_0 = (0,0)$ in the kernel of an isogeny: this only happens when $K = aP + bQ$, with $a, b, \in \mathbb{Z}_{2^f}$ is above $(0,0)$, which can only occur when either both a and b are even (but then K has order smaller than 2^f) or when both a and b are odd. Thus, we can still avoid $(0,0)$ by choosing only one of a or b odd.

4.3 Generalizing Entangled Basis Generation

We now also have enough understanding of profiles to generalize entangled basis generation (Lemma 3) to any Weierstrass curve over $\mathbb{F}_q$ with $q = p^{2k}$, so that -1 is a square, and

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

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

Remark 6. In practice, restricting to Weierstrass curves whose right-hand side factors is not an actual restriction: this implies that the 2-torsion is rational, and so that $\mathcal{S}_{2,q}(E)$ has rank 2. If the right-hand-side does not factor, the Sylow-2 torsion has rank 1, so we just need to find a single generator $P \in E[2^f]$.

In this case, we do not just find a basis for $E[2^f]$, but really for the Sylow 2-torsion, even if $\mathcal{S}_{2,q}(E) \ncong \mathbb{Z}_{2^f} \times \mathbb{Z}_{2^f}$. 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 do not change the quadratic character of the first (unreduced) 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, when x_P defines a point on E, the derived $x_Q = -x_P + \lambda_2 + \lambda_3$ defines a point $Q \in E$, 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 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 $x_P = \frac{\lambda_2+\lambda_3-2\cdot\lambda_1}{1+u^2}$ for some $u \in \mathbb{F}_q$. Then, $x_Q = -x_P + \lambda_2 + \lambda_3$ defines a second point Q on E such that $[h]P$ and $[h]Q$ generate the Sylow-2 subgroup $\mathcal{S}_{2,q} \cong \mathbb{Z}_{2^f} \times \mathbb{Z}_{2^g}$, with $f \geq g$, for $h = \frac{\#E(\mathbb{F}_q)}{2^{f+g}}$.*

If necessary, we may also permute the profiles in any other permutation. This approach similarly extends to other curve models if we can solve the following linear system, which is underneath the above result: Let $f_i(x)$ denote the unreduced 2-Tate pairing $T_2(L_i, -)$ on the given curve E. Crucially, in the above, we have that x defines a point on $E(\mathbb{F}_{p^2})$ whenever $\prod f_i(x) = 1$, as this is the right-hand side of the curve equation of E. Then, for entangled basis generation, we want a non-trivial profile, i.e., at least some $f_i(x_P)$ is a non-square, and furthermore

$$f_1(x_P) = t_1^2 \cdot f_1(x_Q)$$
$$f_2(x_P) = t_2^2 \cdot f_3(x_Q)$$
$$f_3(x_P) = t_3^2 \cdot f_2(x_Q)$$

where the $t_i \in \mathbb{F}_q^*$ are chosen so that we have slightly more freedom, as they do not affect the profiles. In the above example, if we choose $t_2^2 = -1$, we turn the second equation into $x_P - \alpha = -(x_Q - 1/\alpha)$, from which we find the choice $x_Q = -x_P - A$. The first equation then ensures our choice of x_P must satisfy $x_P = -A/(1+t_1^2)$, which recovers the original solution in Lemma 3. Note that the third equation is satisfied by these choices.

4.4 Subgroup Membership Testing

Koshelev's method for subgroup membership testing [Kos23; DHK+24] is based on the observation that the subgroup membership problem can, in some cases, be rephrased using the non-degeneracy of the Tate pairing. This is significantly different from other approaches [Sco21].

Theorem 2 ([Kos23, Lem. 1]). *Let $E/\mathbb{F}_p$ be an elliptic curve with $E(\mathbb{F}_p) \cong \mathbb{Z}_{e_1} \times \mathbb{Z}_{e_2} \times \mathbb{Z}_r$, with $e_1 \mid e_2$ and both coprime with r, and let G denote the subgroup of $E(\mathbb{F}_p)$ of order r. Let P_1 and P_2 generate $E[e_2](\mathbb{F}_p)$, of order e_1, resp. e_2. Assume $e_2 \mid p-1$, so that the Tate pairing is non-degenerate. Then,*

$$Q \in G \quad \Leftrightarrow \quad t_{e_1}(P_1, Q) = 1 \text{ and } t_{e_2}(P_2, Q) = 1.$$

Rephrased in Tate profiles, Koshelev's subgroup membership test simply says that $Q \in E[r](\mathbb{F}_p)$ if and only if Q has trivial profile $t_{[e_2]}(Q)$. This simple observation makes the generalization to higher dimensions clear: we need to verify the triviality of the n-profile of Q with respect to the cofactor n.

5 Optimized 2-Tate Profile using Cubical Pairings

In this section we optimize the computation of level-2 cubical pairings on Kummer surfaces. We first discuss generic improvements, which apply in general to improve cubical pairings of degree 2 on Kummer surfaces, before we describe specific improvements that are possible by precomputation given a specific Kummer surface. The starting point is Algorithm 1, which we try to optimize as much as possible to compute the full 2-Tate profile.

In this section, $\mathcal{K}$ denotes a Kummer surface associated to some Jacobian $\mathcal{J}$, and we want to compute the 2-Tate profile with respect to some basis $B_1, \dots, B_4$ of $\mathcal{K}[2]$. We assume this basis is k-rational, for some finite field k. Later, we want to specifically work with the Gaudry–Schost Kummer surface from Example 1, with $k = \mathbb{F}_p$. The result of this section is summarized in the following theorem.

Theorem 3. *Let $P = (P_1 : P_2 : P_3 : P_4) \in \mathcal{K}(\mathbb{F}_p)$, originating from $\mathcal{J}(\mathbb{F}_p)$. Let $m_1 := P_1 \cdot \left(\sum_{j=1}^4 M_{1,j} P_i\right)$, $m_2 := P_3 \cdot \left(\sum_{j=1}^4 M_{2,j} P_i\right)$, $m_3 := P_1 \cdot P_4$, and $m_4 := P_1 \cdot P_3$ where the $M_{i,j} \in \mathbb{F}_p$ are precomputed constants. Denote by ζ_i the Legendre symbol of m_i. Then the 2-Tate profile*

$$t_{[2]}(P) = (\zeta_1, \zeta_2, \zeta_3, \zeta_4),$$

is computed in 6 additions, 10 multiplications, and 4 Legendre symbols over $\mathbb{F}_p$.

Remark 7. We should be careful that this profile computation assumes P originates from $\mathcal{J}$, and not $\mathcal{J}^T$, as this could affect some sign differences in the profile computation. Although these are easy and essentially free to correct, they are unnecessary if we simply care if a profile is trivial or not.

5.1 Generic Improvements

Replace inversions by multiplications. As inversions are rather costly in finite fields, we prefer to avoid them as much as possible in our computations. Luckily, in Tate pairing computations, our results live in the quotient k^*/k^{*n}, which allows us to remove inversions if n is small enough, using the following observation.

Observation 1. In k^*/k^{*n}, for $\lambda_Q, \lambda_P \in k^*$, we have $\lambda_P^n \in k^*$, hence,

$$\frac{\lambda_Q}{\lambda_P} \equiv \frac{\lambda_Q}{\lambda_P} \cdot \lambda_P^n \equiv \lambda_Q \cdot \lambda_P^{n-1}.$$

In particular, for $n = 2$, we have $\lambda_Q/\lambda_P \equiv \lambda_Q \cdot \lambda_P$.

As we focus only on the degree-2 Tate pairing, we are essentially able to remove most inversions in our cubical arithmetic. For the *reduced* Tate pairing, one can rephrase the above observation: the Legendre symbol of $1/\alpha$ is the same as the Legendre symbol of α.

An easy basis of $\mathcal{K}[2]$. We are free to choose our basis $B_1, \dots, B_4$ of $\mathcal{K}[2]$ with respect to which we compute the profile $t_{[2]}(Q) = (t_2(B_i, Q))_{i=1}^4$. We make the following observation.

Observation 2. The matrices $W_{1,2}$, $W_{3,4}$, and $W_{5,6}$ are permutation matrices, hence, their action on $Q = (Q_1 : Q_2 : Q_3 : Q_4) \in \mathcal{K}(\mathbb{F}_p)$ is essentially free. In particular, the computation of $t_2(L_{i,j}, Q)$ is significantly cheaper for $(i, j) \in \{(1, 2), (3, 4), (5, 6)\}$.

Therefore, choosing (arbitrarily) a basis with $B_3 = L_{3,4}$ and $B_4 = L_{5,6}$ saves a significant amount of multiplications in the computation of $t_2(B_3, Q)$ and $t_2(B_4, Q)$, and therefore in the profile $t_{[2]}(Q)$.

Partial matrix multiplication. In the computation of λ_Q, we require the action of $W_{i,j}$ on $\widetilde{L_{i,j} + Q} = (l_1, l_2, l_3, l_4)$ to compute the translation. However, in line 6 and later, we only need the k-th index of the result, for some predetermined $1 \leq k \leq 4$. Hence, if $W_{i,j}^{(k)} = (w_1, w_2, w_3, w_4)$ denotes the k-th row of $W_{i,j}$, we only need to compute the k-th index of $W_{i,j} \cdot \widetilde{L_{i,j} + Q}$ as $m_1 l_1 + m_2 l_2 + m_3 l_3 + m_4 l_4$. This saves a significant number of multiplications in the computation of $t_2(L_{i,j}, Q)$ for $(i, j) \notin \{(1, 2), (3, 4), (5, 6)\}$[5].

[5] The case $(i, j) \in \{(1, 2), (3, 4), (5, 6)\}$ is covered more efficiently by Observation 2.

5.2 Specific Improvements

We now describe improvements that are possible when working on a specific Kummer surface. An explicit example is given in Section 6, where we apply these optimizations to the Gaudry–Schost Kummer surface.

Removing the action of $\boldsymbol{W^2_{i,j}}$. To compute the λ_Q required for $t_2(L_{i,j}, Q)$, we compute $\widetilde{L_{i,j}+Q}$ using the action of $W_{i,j}$ on $\widetilde{Q}$, and translate the result again by $W_{i,j}$. This can be simplified by the following observation.

Observation 3. Let $\widetilde{Q} = (Q_1, Q_2, Q_3, Q_4) \in \mathcal{K}(\mathbb{F}_p)$. Then $\widetilde{L_{i,j}+Q} = W_{i,j} \cdot \widetilde{Q} = (a_1, a_2, a_3, a_4)$ for some $a_i \in \mathcal{K}(\mathbb{F}_p)$. After normalizing $\widetilde{L_{i,j}+Q}$ to a given index $k \in \{1, \ldots 4\}$, we find that $W_{i,j} \cdot a_k \cdot \widetilde{L_{i,j}+Q} = a_k \cdot W^2_{i,j}\widetilde{Q}$. For every possible (i, j), we have $W^2_{i,j} = \gamma_{i,j} \cdot I_4$ for some $\gamma_{i,j} \in \mathbb{F}_p$. Hence,

$$\lambda_Q \equiv \left(W_{i,j} \cdot a_k \cdot \widetilde{L_{i,j}+Q}\right)_k \equiv a_k \cdot \left(W^2_{i,j}\widetilde{Q}\right)_k \equiv a_k \cdot \gamma_{i,j} \cdot Q_k$$

As we can precompute the Legendre symbol of $\gamma_{i,j}$ on a specific Kummer surface, we can significantly simplify the computation of λ_Q: we only need to compute a_k as the k-th index of $W_{i,j} \cdot \widetilde{Q}$, which we can do using the partial matrix multiplication. Combined, these improvements replace two full matrix computations, at 16 multiplications each, by a single row multiplication at 4 multiplications, per pairing $t_2(L_{i,j}, Q)$ for $(i, j) \notin \{(1, 2), (3, 4), (5, 6)\}$.

For pairings with $(i, j) \in \{(1, 2), (3, 4), (5, 6)\}$, we find that we only need to know the permutation given by $W_{i,j}$. For example, as $W_{3,4}$ maps $(a, b, c, d) \mapsto (d, c, b, a)$, a similar derivation shows that we can compute λ_Q as $Q_1 \cdot Q_4$.

Precompute the Legendre symbol of $\lambda_{L_{i,j}}$. It is clear that $\lambda_{L_{i,j}}$ does not depend on the point Q we are pairing with. Hence, on a given Kummer surface, we may precompute the Legendre symbol of $\lambda_{L_{i,j}}$ for each index pair (i, j). To compute $t_2(L_{i,j}, Q)$, we then simply compute the Legendre symbol of λ_Q and adjust by -1 if $\lambda_{L_{i,j}}$ is non-square.

5.3 Optimized Profiles of Degree 2

We combine all these improvements: We choose the basis $\langle L_{2,3}, L_{3,5}, L_{3,4}, L_{5,6}\rangle$ for $\mathcal{K}[2]$, and, together with the other improvements, we obtain Algorithm 2. This is an algorithmic description of Theorem 3: we can compute the 2-profile $t_{[2]}(Q)$ for $Q \in \mathcal{K}(\mathbb{F}_p)$ in $10\mathbf{M} + 6\mathbf{A} + 4\mathbf{L}$ operations over $\mathbb{F}_p$.

Remark 8. Heuristically, it seems infeasible to compute a profile with fewer than 4 Legendre symbols, as the profile requires 4 bits of information. As the overhead, $10\mathbf{M} + 6\mathbf{A}$, is negligible compared to the cost of the Legendre symbols, we did not pursue further optimizations. If one assumes $\widetilde{Q}$ obtained as a normalized point $(1, Q_2, Q_3, Q_4)$, we save an extra $4\mathbf{M} + 1\mathbf{A}$.

Algorithm 2 Optimized pairing computation on $\mathcal{K}(\mathbb{F}_p)$

```
Input: The point $\widetilde{Q} = (Q_1, Q_2, Q_3, Q_4)$, row 1 of $W_{2,3}$ as $(w_1, w_2, w_3, w_4)$ with $w_1 = 1$,
    and row 3 of $W_{3,5}$ as $(w'_1, w'_2, w'_3, w'_4)$ with $w'_3 = -1$.
Output: The profile $t_{[2]}(Q) \in \mu_2^4$.
$T_1 \leftarrow Q_1 \cdot (w_1 Q_1 + w_2 Q_2 + w_3 Q_3 + w_4 Q_4)$
$T_2 \leftarrow Q_3 \cdot (w'_1 Q_1 + w'_2 Q_2 + w'_3 Q_3 + w'_4 Q_4)$
$T_3 \leftarrow Q_1 \cdot Q_4$
$T_4 \leftarrow Q_1 \cdot Q_3$
For $i \in \{1, 2, 3, 4\}$ do $\zeta_i \leftarrow \mathsf{Legendre}(T_i)$,
return $(\zeta_1, \zeta_2, \zeta_3, \zeta_4)$
```

6 Subgroup Membership Testing for Gaudry–Schost's $\mathcal{K}$

This section combines the ideas from Sections 4.4 and 5 and applies them to highly optimize a specific situation. First, we apply the generalization of subgroup membership testing to Kummer surfaces using Tate profiles to the Gaudry–Schost Kummer surface. Then, we use the optimized 2-Tate profile computation from Section 5 to perform this subgroup membership testing.

This section only focuses on this particular Kummer surface, as described in Section 2.2. We denote it by $\mathcal{K}$, and the associated Jacobian by $\mathcal{J}$. Furthermore, $G = \mathcal{K}[r](\mathbb{F}_p)$ denotes the subgroup of large prime order r, and so subgroup membership testing asks us to verify $Q \in G$ for $Q = (Q_1 : Q_2 : Q_3 : Q_4) \in \mathcal{K}(\mathbb{F}_p)$.

6.1 The Sylow 2-Torsion Structure of $\mathcal{J}$

For the Gaudry–Schost surface, we know that the order of the associated Jacobian $\mathcal{J}(\mathbb{F}_p)$ is $16 \cdot r$, and of its twist $\mathcal{J}^T(\mathbb{F}_p)$ is $16 \cdot r'$. By construction, $\mathcal{J}$ has rational 2-torsion, which is the perfect set-up for Koshelev's approach to subgroup membership testing using Tate pairings:

Observation 4. Let G be the subgroup of order r of $\mathcal{J}(\mathbb{F}_p)$, and similarly, let G' be the subgroup of order r' of $\mathcal{J}^T(\mathbb{F}_p)$. We have that

$$J(\mathbb{F}_p) = \mathcal{J}[2] \times G, \quad \mathcal{J}^T(\mathbb{F}_p) = \mathcal{J}^T[2] \times G'.$$

In other words, we know that $\mathcal{S}_{2,p}(\mathcal{J}) = \mathcal{J}[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. From this, we easily find the subgroup membership test, by an application of Corollary 1:

Lemma 6. *For $Q \in \mathcal{J}(\mathbb{F}_p)$, we have*

$$Q \in G \quad \Leftrightarrow \quad t_{[2]}(Q) \text{ is trivial.}$$

Proof. By non-degeneracy of the 2-Tate pairing, we have that a trivial profile $t_{[2]}(Q)$ implies $Q \in [2]\mathcal{J}(\mathbb{F}_p)$, and, from Observation 4 we know that $[2]\mathcal{J}(\mathbb{F}_p) = G$. □

We will abuse notation and write $Q \in G$, when we mean that Q is a point on the Kummer surface $\mathcal{K}$ associated to a point in the subgroup $G = \mathcal{J}[r](\mathbb{F}_p)$.

6.2 Results

To the best of our knowledge, there are no previous attempts in the literature to perform subgroup membership testing on Kummer surfaces. We therefore compare our results against **a.)** the naive approach using a ladder, and **b.)** the approach of Section 2.3 to compute the profile. The results are summarized in Table 1.

a.) Verifying $[r]Q = \mathbf{0}_{\mathcal{K}}$ using a ladder takes almost 7000 operations in $\mathbb{F}_p$, whereas the optimized cubical profile takes only 478 operations[6] in $\mathbb{F}_p$.

b.) The dominating cost in both approaches is the overhead of the Legendre symbols, which takes more than 98% in the optimized approach. A more useful metric here is the reduction in overhead, i.e., everything beyond the Legendre symbols. The overhead of the approach of Section 2.3 is $76\mathbf{M} + 33\mathbf{S} + 53\mathbf{A}$, whereas Algorithm 2 computes the profile with an overhead of $10\mathbf{M} + 6\mathbf{A}$ operations in $\mathbb{F}_p$. Assuming $\mathbf{S} = 0.8\mathbf{M}$ and $\mathbf{A} = 0.05\mathbf{M}$, the latter takes roughly 10 times fewer operations.

Including origin check. Depending on the application, one may need to verify that $Q \in \mathcal{K}(\mathbb{F}_p)$ originates from $\mathcal{J}$ or its twist.

a.) The naive approach verifies the origin from the fact that only a point originating from the Jacobian could have order r, and so, we verify the origin at no extra cost. Including the origin check to the cubical approach adds 140 $\mathbb{F}_p$ operations, bringing the total to 618 operations in $\mathbb{F}_p$. The cubical approach is therefore still more than ten times faster than the naive approach, even including the origin check.

b.) For the pairings from Section 2.3, this only requires an extra Legendre symbol, whereas for the cubical pairings, this adds an extra $22\mathbf{M} + 1\mathbf{S} + 13\mathbf{A}$, beyond the extra Legendre symbol, to the overhead. The resulting overhead is however still three times less.

7 Future Work

In this work we have shown that the language of Tate profiles gives a natural description of many results in the literature, and, by placing these results in this language, we are able to generalize several of them. As a consequence, one may similarly rephrase other results in this language in the hope to generalize them.

[6] We estimate a Legendre symbol computation at $125\mathbf{S}+9\mathbf{M}$ using an optimal addition chain. In practice, this can be done much faster [Por20; AHST23].

Table 1. Operation counts for different approaches to subgroup membership testing on the Gaudry–Schost Kummer surface, with and without origin check. Cost model: $\mathbf{M} = 1$, $\mathbf{S} = 0.8$, $\mathbf{A} = 0.05$, Legendre $\mathbf{L} = 125\mathbf{S} + 9\mathbf{M}$.

	M	**S**	**A**	**L**	**Overhead**	**Total**
Ladder by $[r]$	4 514	2 008	8 016	0	–	**6992**
On Jacobian (Sec. 2.3)	76	33	53	4	105	**573**
Opt. Cubical (Sec. 5)	10	0	6	4	10	**478**
On Jacobian w/ Origin	76	33	53	5	105	**682**
Opt. Cubical w/ Origin	32	1	19	5	34	**579**

For example, one may apply the generalization of Koshelev's membership test to other Kummer surfaces, or essentially any (Kummer variety of an) abelian variety, and optimize the required cubical arithmetic.

Furthermore, the optimized cubical profile computation may be used more widely to sample points of order 2^f on Kummer surfaces: by forcing a non-trivial profile during sampling, we force $Q \in \mathcal{K} \setminus [2]\mathcal{K}$. For example, if we initialize Q as $(1, Y, Z, T)$ where Z is any non-square element in $\mathbb{F}_p$, we force $t_2(L_{5,6}, Q) = -1$, which ensures a non-trivial profile. We then look for suitable Y and T to ensure $Q \in \mathcal{K}(\mathbb{F}_p)$. In practice, Tate pairings are often used for basis generation, and so, simpler 2-pairings should apply more broadly to generate a basis of 2^f-torsion, with 2^f maximal.

Lastly, we may hope to generalize entangled basis generation to higher dimensions, using both the techniques from Section 4.3 and Section 5.

References

[AAA+25] Marius A. Aardal, Gora Adj, Diego F. Aranha, Andrea Basso, Isaac Andrés Canales Martínez, Jorge Chávez-Saab, Maria Corte-Real Santos, Pierrick Dartois, Luca De Feo, Max Duparc, Jonathan Komada Eriksen, Tako Boris Fouotsa, Décio Luiz Gazzoni Filho, Basil Hess, David Kohel, Antonin Leroux, Patrick Longa, Luciano Maino, Michael Meyer, Kohei Nakagawa, Hiroshi Onuki, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Giacomo Pope, Krijn Reijnders, Damien Robert, Francisco Rodríguez Henríquez, Sina Schaeffler, and Benjamin Wesolowski. *SQIsign 2.0: Algorithm specifications and supporting documentation.* Tech. rep. 2025 (cit. on p. 13).

[AHST23] Diego F Aranha, Benjamin Salling Hvass, Bas Spitters, and Mehdi Tibouchi. "Faster constant-time evaluation of the Kronecker symbol with application to elliptic curve hashing". In: *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security.* 2023, pp. 3228–3238 (cit. on p. 20).

[BCHL16] Joppe W Bos, Craig Costello, Huseyin Hisil, and Kristin Lauter. “Fast cryptography in genus 2”. In: *Journal of Cryptology* 29 (2016), pp. 28–60 (cit. on p. 6).

[BCM+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. 2).

[BDLS20] Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. “Faster computation of isogenies of large prime degree”. In: *ANTS-XIV-14th Algorithmic Number Theory Symposium*. Vol. 4. Mathematical Sciences Publishers. 2020, pp. 39–55 (cit. on p. 2).

[BF01] Dan Boneh and Matt Franklin. “Identity-based encryption from the Weil pairing”. In: *Annual international cryptology conference*. Springer. 2001, pp. 213–229 (cit. on p. 2).

[BGLS03] Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. “Aggregate and verifiably encrypted signatures from bilinear maps”. In: *Advances in Cryptology—EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4–8, 2003 Proceedings 22*. Springer. 2003, pp. 416–432 (cit. on p. 2).

[BHKL13] Daniel J. Bernstein, Mike Hamburg, Anna Krasnova, and Tanja Lange. “Elligator: elliptic-curve points indistinguishable from uniform random strings”. In: *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 2013, pp. 967–980 (cit. on p. 13).

[BKLS02] Paulo S. L. M. Barreto, Hae Y. Kim, Ben Lynn, and Michael Scott. “Efficient algorithms for pairing-based cryptosystems”. In: *Advances in Cryptology—CRYPTO 2002: 22nd Annual International Cryptology Conference Santa Barbara, California, USA, August 18–22, 2002 Proceedings 22*. Springer. 2002, pp. 354–369 (cit. on p. 2).

[BLS01] Dan Boneh, Ben Lynn, and Hovav Shacham. “Short signatures from the Weil pairing”. In: *International conference on the theory and application of cryptology and information security*. Springer. 2001, pp. 514–532 (cit. on p. 2).

[BLS04] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. “Efficient implementation of pairing-based cryptosystems”. In: *Journal of Cryptology* 17 (2004), pp. 321–334 (cit. on p. 2).

[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. 2).

[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, 5).

[CC86] David V Chudnovsky and Gregory V Chudnovsky. "Sequences of numbers generated by addition in formal groups and new primality and factorization tests". In: *Advances in Applied Mathematics* 7.4 (1986), pp. 385–434 (cit. on p. 6).

[CDV20] Wouter Castryck, Thomas Decru, and Frederik Vercauteren. "Radical Isogenies". In: *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part II*. Ed. by Shiho Moriai and Huaxiong Wang. Vol. 12492. Lecture Notes in Computer Science. Springer, 2020, pp. 493–519. DOI: 10.1007/978-3-030-64834-3_17. URL: https://doi.org/10.1007/978-3-030-64834-3%5C_17 (cit. on p. 3).

[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 pp. 2, 3, 12, 13).

[CF96] John William Scott Cassels and E Victor Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*. Vol. 230. Cambridge University Press, 1996 (cit. on p. 6).

[CHM+23] Wouter Castryck, Marc Houben, Simon-Philipp Merz, Marzio Mula, Sam van Buuren, and Frederik Vercauteren. "Weak instances of class group action based cryptography via self-pairings". In: *Annual International Cryptology Conference*. Springer. 2023, pp. 762–792 (cit. on p. 2).

[CJL+17] Craig Costello, David Jao, Patrick Longa, Michael Naehrig, Joost Renes, and David Urbanik. "Efficient compression of SIDH public keys". In: *Advances in Cryptology–EUROCRYPT 2017: 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30–May 4, 2017, Proceedings, Part I 36*. Springer. 2017, pp. 679–706 (cit. on pp. 2, 12).

[CR24] Maria Corte-Real Santos and Krijn Reijnders. *Return of the Kummer: a Toolbox for Genus-2 Cryptography*. Cryptology ePrint Archive, Paper 2024/948. 2024. URL: https://eprint.iacr.org/2024/948 (cit. on pp. 3, 4, 6–10).

[DHK+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).

[DJP14] Luca De Feo, David Jao, and Jérôme Plût. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". In: *Journal of Mathematical Cryptology* 8.3 (2014), pp. 209–247 (cit. on p. 13).

[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. 3).

[FR94] Gerhard Frey and Hans-Georg Rück. "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves". In: *Mathematics of computation* 62.206 (1994), pp. 865–874 (cit. on pp. 2, 5).

[Gal05] SD Galbraith. *Pairings. London Mathematics Society Lecture Note Series, vol. 317*. 2005 (cit. on p. 2).

[Gau07] Pierrick Gaudry. "Fast genus 2 arithmetic based on Theta functions". In: *Journal of Mathematical Cryptology* 1.3 (2007), pp. 243–265 (cit. on p. 6).

[GHS02] Steven D Galbraith, Keith Harrison, and David Soldera. "Implementing the Tate pairing". In: *International Algorithmic Number Theory Symposium*. Springer. 2002, pp. 324–337 (cit. on p. 2).

[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 pp. 3, 6).

[HSSI99] Ryuichi Harasawa, Junji Shikata, Joe Suzuki, and Hideki Imai. "Comparing the MOV and FR reductions in elliptic curve cryptography". In: *Advances in Cryptology—EUROCRYPT'99: International Conference on the Theory and Application of Cryptographic Techniques Prague, Czech Republic, May 2–6, 1999 Proceedings 18*. Springer. 1999, pp. 190–205 (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. 3, 12).

[JAC+17] David Jao, Reza Azarderakhsh, Matt Campagna, Craig Costello, Luca de Feo, Basil Hess, Amir Jalili, Brian Koziel, Brian Lamacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, and David Urbanik. *SIKE: Supersingular Isogeny Key Encapsulation*. Tech. rep. 2017 (cit. on p. 13).

[Jou02] Antoine Joux. "The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems: Survey". In: *International Algorithmic Number Theory Symposium*. Springer. 2002, pp. 20–32 (cit. on p. 2).

[Jou04] Antoine Joux. "A one round protocol for tripartite Diffie–Hellman". In: *Journal of cryptology* 17.4 (2004), pp. 263–276 (cit. on p. 2).

[Kob87] Neal Koblitz. "Elliptic curve cryptosystems". In: *Mathematics of computation* 48.177 (1987), pp. 203–209 (cit. on p. 5).

[Kob89] Neal Koblitz. "Hyperelliptic cryptosystems". In: *Journal of cryptology* 1 (1989), pp. 139–150 (cit. on p. 5).

[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 pp. 2, 3, 12, 16).

[KT18] Takeshi Koshiba and Katsuyuki Takashima. "New assumptions on isogenous pairing groups with applications to attribute-based encryption". In: *International Conference on Information Security and Cryptology*. Springer. 2018, pp. 3–19 (cit. on p. 2).

[Lic69] Stephen Lichtenbaum. "Duality theorems for curves over p-adic fields". In: *Inventiones mathematicae* 7.2 (1969), pp. 120–136 (cit. on p. 5).

[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. 2).

[LR10] David Lubicz and Damien Robert. "Efficient pairing computation with theta functions". In: *International Algorithmic Number Theory Symposium*. Springer. 2010, pp. 251–269 (cit. on p. 5).

[LR15] David Lubicz and Damien Robert. "A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties". In: *Journal of Symbolic Computation* 67 (2015), pp. 68–92 (cit. on p. 5).

[LR16] David Lubicz and Damien Robert. "Arithmetic on Abelian and Kummer Varieties". In: *Finite Fields and Their Applications* 39 (May 2016), pp. 130–158. DOI: 10.1016/j.ffa.2016.01.009. eprint: 2014/493, HAL: hal-01057467. (Cit. on p. 5).

[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. 2).

[LWXZ24] Kaizhan Lin, Weize Wang, Zheng Xu, and Chang-An Zhao. "A faster software implementation of SQISign". In: *IEEE Transactions on Information Theory* (2024) (cit. on p. 2).

[McL21] Michael B. McLoughlin. *addchain: Cryptographic Addition Chain Generation in Go*. Repository https://github.com/mmcloughlin/addchain. Version 0.4.0. Oct. 2021. DOI: 10.5281/zenodo.5622943. URL: https://doi.org/10.5281/zenodo.5622943 (cit. on p. 4).

[Mil04] Victor S Miller. "The Weil pairing, and its efficient calculation". In: *Journal of cryptology* 17.4 (2004), pp. 235–261 (cit. on pp. 5, 7).

[Mil85] Victor S Miller. "Use of elliptic curves in cryptography". In: *Conference on the theory and application of cryptographic techniques*. Springer. 1985, pp. 417–426 (cit. on p. 5).

[MS24] Joseph Macula and Katherine E Stange. “Extending class group action attacks via sesquilinear pairings”. In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2024, pp. 371–395 (cit. on p. 2).

[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. 2).

[Por20] Thomas Pornin. *Faster modular inversion and Legendre symbol, and an X25519 speed record*. 2020. URL: https://www.nccgroup.com/us/research-blog/faster-modular-inversion-and-legendre-symbol-and-an-x25519-speed-record0/ (cit. on p. 20).

[PRR+25] Giacomo Pope, Krijn Reijnders, Damien Robert, Alessandro Sferlazza, and Benjamin Smith. “Simpler and Faster Pairings from the Montgomery Ladder”. In: *IACR Commun. Cryptol.* 2.2 (2025), p. 29. DOI: 10.62056/AH2I893Y6. URL: https://doi.org/10.62056/ah2i893y6 (cit. on p. 7).

[Reij23] Krijn Reijnders. “Effective Pairings in Isogeny-based Cryptography”. In: *International Conference on Cryptology and Information Security in Latin America*. Springer. 2023, pp. 109–128 (cit. on p. 2).

[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. 3, 5, 8, 9, 12).

[Rob24] Damien Robert. *Fast pairings via biextensions and cubical arithmetic*. Cryptology ePrint Archive, Paper 2024/517. 2024. URL: https://eprint.iacr.org/2024/517 (cit. on pp. 3, 5, 7).

[Sch03] Jasper Scholten. *Weil restriction of an elliptic curve over a quadratic extension*. 2003 (cit. on p. 10).

[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 pp. 2, 16).

[Sta07] Katherine E Stange. “The Tate pairing via elliptic nets”. In: *Pairing-Based Cryptography–Pairing 2007: First International Conference, Tokyo, Japan, July 2-4, 2007. Proceedings 1*. Springer. 2007, pp. 329–348 (cit. on pp. 5, 7).

[Tat62] John Tate. “Duality theorems in Galois cohomology over number fields”. In: *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*. 1962, pp. 288–295 (cit. on p. 5).

[Vél71] Jacques Vélu. “Isogénies entre courbes elliptiques”. In: *Comptes-Rendus de l’Académie des Sciences* 273 (1971). https://gallica.bnf.fr/ark:/12148/cb34416987n/date, pp. 238–241. URL: https://gallica.bnf.fr/ark:/12148/cb34416987n/date (cit. on p. 2).

[Ver09] Frederik Vercauteren. “Optimal pairings”. In: *IEEE transactions on information theory* 56.1 (2009), pp. 455–461 (cit. on p. 2).

[ZSP+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 pp. 2, 3, 12, 13).