Optimized Cubical Pairings of Degree 2 for Subgroup Membership Testing in Genus 2

Krijn Reijnders*

COSIC, KU Leuven
crypto.krijn@gmail.com

Abstract

In this short paper, we combine two new techniques in pairings to do subgroup membership testing for the Gaudry–Schost Kummer surface: showing that a point P is in the subgroup G of large prime order. First, we generalize Koshelev's method for subgroup membership testing using Tate pairings to higher dimensions. Second, using Robert's cubical arithmetic, we optimize degree-2 Tate pairings on Kummer surfaces. We verify $P \in G$ using only 6 additions, 10 multiplications, and 4 Legendre symbols.

1 Introduction

Subgroup membership testing, in the context of elliptic-curve cryptography, 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 [Kos22] performs subgroup membership testing using the non-degeneracy of the Tate pairing. For certain curves,

*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.

this may outperform previous methods for subgroup membership testing, in particular when the Tate pairing computation is fast, and the parameters of the elliptic curve are suitable.

Contributions.

In this work, we study the abstract problem of solving subgroup membership testing on Kummer surfaces as efficiently as possible, focusing specifically on the Kummer surface described by Gaudry and Schost [GS12]. For this surface $\mathcal{K}$, we want to verify that points $P \in \mathcal{K}(\mathbb{F}_p)$ are in a specific subgroup $G = \mathcal{K}(\mathbb{F}_p)[r]$, where r is a large (125-bit) prime. This brings along some challenges: we need to adapt Koshelev's method [Kos22] to higher dimensions, and optimize the computation of Tate pairings of degree 2 on Kummer surfaces. Our results are incremental; we rephrase Koshelev's method in dimension 2, rather than dimension 1, and significantly optimize the cubical arithmetic on Kummer surfaces for pairings of degree 2.

Our main result is summarized by Theorem 1, which shows that we can easily compute subgroup membership $P \in G$ using a few operations in $\mathbb{F}_p$ and four Legendre symbols, which dominate the cost.

Theorem 1. *Let $P = (P_1, P_2, P_3, P_4) \in \mathcal{K}(\mathbb{F}_p)$, originating from $\mathcal{J}(\mathbb{F}_p)$. Let $G = \mathcal{K}[r]$. 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 $m_4 := P_1 \cdot P_3$ given precomputed constants $M_{i,j} \in \mathbb{F}_p$. Denote by ζ_i the Legendre symbol of m_i. Then*

$$P \in G \quad \Leftrightarrow \quad (\zeta_1, \zeta_2, \zeta_3, \zeta_4) = (1, 1, 1, 1).$$

Theorem 1 is a combination of two lemmas: Lemma 2, which applies Koshelev's subgroup membership testing [Kos22; DHK+24] in higher-dimensions, and Lemma 3 which shows that the values ζ_i actually compute the reduced Tate pairing of degree 2, following Robert's cubical arithmetic [Rob24].

Lemma 2. *Let $P \in \mathcal{K}(\mathbb{F}_p)$, originating from $\mathcal{J}(\mathbb{F}_p)$. Then $P \in G$ if and only if all 2-Tate pairings are trivial, i.e., $t_2(L, P) = 1$ for all $L \in \mathcal{J}[2]$.*

Lemma 3. *Let $P \in \mathcal{K}(\mathbb{F}_p)$. If $\zeta_i = 1$ for $1 \leq i \leq 4$, then all 2-Tate pairings are trivial, i.e., $t_2(L, P) = 1$ for all $L \in \mathcal{J}[2]$.*

We prove Lemma 2 in Section 3 using the language of Tate profiles [CR24], and then optimize the computation of such profiles in Sections 4 and 5, both for general Kummer surfaces and specifically the Gaudry–Schost Kummer surface. We discuss possible generalizations in Section 6.

Altogether, the subgroup membership test takes only 6 additions, 10 multiplications, and 4 Legendre symbols. The non-reduced cubical pairings, when optimized for this specific surface, are more than 10 times faster to compute the 2-Tate profile of a point, compared to previous (generic) approaches to compute 2-Tate profiles on Kummer surfaces [CR24]. Our approach to subgroup membership testing is more than fourteen times faster than the naïve approach of computing $[r]P$ via a Montgomery ladder.

2 Preliminaries

Notation. We work mostly over $\mathbb{F}_p$. An extension is denoted $\mathbb{F}_q$ for $q = p^m$. 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 $W_{i,j}$.

On Kummer surfaces, we denote a point $Q \in \mathcal{K}$ as $(Q_1 : Q_2 : Q_3 : Q_4) \in \mathbb{P}^3(\mathbb{F}_p)$, which is defined up to scalars. An *affine lift* for Q is denoted $\widetilde{Q}$, 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 **M** for multiplication, **S** for squaring, **A** for addition, and **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].

2.1 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. Gaudry [Gau07] shows that in such cases, one may work on the *Kummer surface*[1] $\mathcal{K}$ associated to the Jacobian $\mathcal{J}$, which boasts much faster arithmetic and still

[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.

allows us to compute $P \mapsto [n]P$. This is similar to the situation for elliptic curves, where the *Kummer line* of an elliptic curve gives us fast x-only arithmetic. 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].

The Gaudry–Schost's 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 4. 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 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 $22\mathbf{M} + 1\mathbf{S} + 13\mathbf{A} + 1\mathbf{L}$.

2.2 The Tate Pairing

The Tate-Lichtenbaum pairing [Tat62; Lic69] on a Jacobian $\mathcal{J}/k$, often referred to as simply the Tate pairing, is a bilinear map

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

which is bilinear and Galois invariant. We will assume $k = \mathbb{F}_q$, where $q = p^m$ is a power of a prime p. Whenever $\mu_n \subseteq k^*$, the Tate pairing is non-degenerate. The *reduced* Tate pairing t_n is the Tate pairing T_n composed with the exponentiation by $(q-1)/n$, which maps $k^*/k^{*,n} \to \mu_n$.

The Tate pairing was introduced in a cryptographic context by Frey and Rück [FR94]. 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 4, more generally see [Rob24].

3 Koshelev's subgroup membership test

Koshelev's method for subgroup membership testing [Kos22; 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 5 ([Kos22, 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,*

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

We rephrase this latter test in the language of *Tate profiles* [CR24], i.e., the array of values of the Tate pairings with respect to (a basis of) the n-torsion $E[n]$.

Definition 6. The *Tate profile* of degree n of a point $Q \in E(\mathbb{F}_q)$ with respect to a basis $B = (B_1, B_2)$ of $E[n]$ is the image of the map

$$t_{[n]} : E(\mathbb{F}_q) \to \mu_n^2$$
$$Q \mapsto (t_n(B_1, Q), t_n(B_2, Q)),$$

where t_n is the Tate pairing of degree n. If $t_{[n]}(Q) = (1, 1)$, we say that the profile is *trivial.*

Using profiles, we rephrase Koshelev's subgroup membership test as follows: $Q \in G$ if and only if Q has trivial profile $t_{[e_2]}(Q)$. For more details on profiles and their applications, we refer the reader to [Rei25].

Subgroup Membership Testing for the Gaudry–Schost's surface. The above approach generalizes easily to higher-dimensions. In particular, 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 7. *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*

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

From this, we easily find the subgroup membership test, by proving Lemma 3, repeated here for convenience:

Lemma. *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 7 we know that $[2]\mathcal{J}(\mathbb{F}_p) = G$. □

For the remainder of this work, we assume a point $Q \in \mathcal{K}(\mathbb{F}_p)$, originating from $\mathcal{J}(\mathbb{F}_p)$, and try to compute its profile to determine that Q originates from 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 $G = \mathcal{J}[r](\mathbb{F}_p)$.

4 Pairings on Kummer Surfaces

In this section we describe the computation of level-2 pairings on Kummer surfaces. We 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].

4.1 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 covering $\rho : \mathcal{J}(\mathbb{F}_p) \to \mathcal{K}(\mathbb{F}_p)$, 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 covering $\mathcal{J}(\mathbb{F}_p) \to \mathcal{K}(\mathbb{F}_p)$. Given $a(x)$, we may then compute the four Tate pairings with respect to a basis of $\mathcal{J}[2]$ to compute the 2-profile $t_{[2]}(Q)$.

Altogether, this approach costs $76\mathbf{M} + 33\mathbf{S} + 53\mathbf{A} + 4\mathbf{L}$ for the computation of the 2-profile $t_{[2]}(Q)$ of a point Q on the Kummer surface $\mathcal{K}(\mathbb{F}_p)$.

4.2 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.

To compute the pairing $t_2(L_{i,j}, Q)$ using cubical arithmetic[2], we compute

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

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.

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 $L_{i,j}$
$\widetilde{2L_{i,j}+Q} \leftarrow W_{i,j} \cdot \widetilde{L_{i,j}+Q}$ ▷ 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 ζ

Remark 8. A naive implementation of Algorithm 1 does not outperform the previous method due to the many matrix multiplications, and we therefore do not assess its performance. Instead, we go straight to optimizing this computation in Section 5.

5 Optimizing Cubical Pairings

In this section we optimize the computation of level-2 cubical pairings on Gaudry–Schost's Kummer surface. 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.

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

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

k^*/k^{*n}, which allows us to remove inversions if n is small enough, using the following observation.

Observation 9. *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 $B_1, \ldots, B_4$ 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 10. *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 $(i, j) \notin \{(1, 2), (3, 4), (5, 6)\}$[4].

5.2 Specific improvements

We now describe improvements that are possible when working on a specific Kummer surface, in our case the Gaudry–Schost Kummer surface.

[4]The case $(i, j) \in \{(1, 2), (3, 4), (5, 6)\}$ is covered by Observation 10 to be even cheaper.

Removing the action of $W_{i,j}^2$. 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 11. *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 $k \in \{1, \dots 4\}$, we find that $W_{i,j} \cdot a_k \cdot \widetilde{L_{i,j}+Q} = a_k \cdot W_{i,j}^2 \widetilde{Q}$. For every possible (i,j), we have $W_{i,j}^2 = \gamma_{i,j} \cdot I_4$ for some $\gamma_{i,j} \in \mathbb{F}_p$. Hence,*

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

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

Now, we combine all these improvements. Let $\langle L_{2,3}, L_{3,5}, L_{3,4}, L_{5,6} \rangle = \mathcal{K}[2]$ be the basis, then we compute the profile $t_{[2]}(Q)$ of a point $Q \in \mathcal{K}(\mathbb{F}_p)$, originating from $\mathcal{J}(\mathbb{F}_p)$, in Algorithm 2. This is an algorithmic description of Theorem 1: computing the profile $t_{[2]}(Q)$ for $Q \in \mathcal{K}(\mathbb{F}_p)$ originating from $\mathcal{J}(\mathbb{F}_p)$, at a cost of $10\mathbf{M} + 6\mathbf{A} + 4\mathbf{L}$, is enough to determine $Q \in G$.

Remark 12. 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 $t_{[2]}(Q) \in \mu_2^4$.

1: $T_1 \leftarrow Q_1 \cdot (w_1 Q_1 + w_2 Q_2 + w_3 Q_3 + w_4 Q_4)$
2: $T_2 \leftarrow Q_3 \cdot (w'_1 Q_1 + w'_2 Q_2 + w'_3 Q_3 + w'_4 Q_4)$
3: $T_3 \leftarrow Q_1 \cdot Q_4$
4: $T_4 \leftarrow Q_1 \cdot Q_3$
5: For $i \in \{1, 2, 3, 4\}$ do $\zeta_i \leftarrow \mathsf{Legendre}(T_i)$,
6: **return** $(\zeta_1, \zeta_2, \zeta_3, \zeta_4)$

5.4 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 4.1 to compute the profile.

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[5] in $\mathbb{F}_p$.

b.) The overhead, i.e., everything beyond the Legendre symbols, of the approach of Section 4.1 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 $\mathbf{A} = 0.5\mathbf{M}$, 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.

[5] 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].

b.) For the pairings from Section 4.1, 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 more than three times less.

6 Future Work

One can 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.

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, initialize $Q = (X, Y, Z, T)$ and set $X = 1$ and Z to any non-square element in $\mathbb{F}_p$ to 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.

References

[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. 11).

[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. 4).

[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. 1).

[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. 1).

[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. 4).

[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. 2–5, 7).

[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 pp. 2, 5).

[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 p. 5).

[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. 3).

[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. 2, 4).

[Kob87] Neal Koblitz. "Elliptic curve cryptosystems". In: *Mathematics of computation* 48.177 (1987), pp. 203–209 (cit. on p. 3).

[Kob89] Neal Koblitz. "Hyperelliptic cryptosystems". In: *Journal of cryptology* 1 (1989), pp. 139–150 (cit. on p. 3).

[Kos22] Dmitrii Koshelev. *Subgroup membership testing on elliptic curves via the Tate pairing*. Cryptology ePrint Archive, Paper 2022/037. 2022. URL: https://eprint.iacr.org/2022/037 (cit. on pp. 1, 2, 5).

[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. 1).

[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. 1).

[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. 3).

[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. 3).

[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. 11).

[PRR+25] Giacomo Pope, Krijn Reijnders, Damien Robert, Alessandro Sferlazza, and Benjamin Smith. *Simpler and Faster Pairings from the Montgomery Ladder*. Cryptology ePrint Archive, Paper 2025/672. 2025. URL: https://eprint.iacr.org/2025/672 (cit. on p. 7).

[Rei25] Krijn Reijnders. *A Note on the Advanced Use of the Tate Pairing*. Cryptology ePrint Archive, Paper 2025/477. 2025. URL: https://eprint.iacr.org/2025/477 (cit. on p. 6).

[Rob24] Damien Robert. "Fast pairings via biextensions and cubical arithmetic". Apr. 2024. eprint: 2024/517, HAL: hal-04848028. (Cit. on pp. 2, 5, 7, 8).

[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. 1, 5).

[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, 8).

[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).