LMS J. Comput. Math. 17 (Special issue A) (2014) 157–180
doi:10.1112/S1461157014000370

Constructing abelian surfaces for cryptography via Rosenhain invariants

Craig Costello, Alyson Deines-Schartz, Kristin Lauter and Tonghai Yang

Abstract

This paper presents an algorithm to construct cryptographically strong genus 2 curves and their Kummer surfaces via Rosenhain invariants and related Kummer parameters. The most common version of the complex multiplication (CM) algorithm for constructing cryptographic curves in genus 2 relies on the well-studied Igusa invariants and Mestre's algorithm for reconstructing the curve. On the other hand, the Rosenhain invariants typically have much smaller height, so computing them requires less precision, and in addition, the Rosenhain model for the curve can be written down directly given the Rosenhain invariants. Similarly, the parameters for a Kummer surface can be expressed directly in terms of rational functions of theta constants. CM-values of these functions are algebraic numbers, and when computed to high enough precision, LLL can recognize their minimal polynomials. Motivated by fast cryptography on Kummer surfaces, we investigate a variant of the CM method for computing cryptographically strong Rosenhain models of curves (as well as their associated Kummer surfaces) and use it to generate several example curves at different security levels that are suitable for use in cryptography.

1. *Introduction*

The extension of the Atkin–Morain complex multiplication (CM) algorithm [**1**] from elliptic curves to abelian surfaces began with the work of Spallek in 1994 [**31**]. In the two decades since then, the CM method in genus 2 has undergone a vast range of improvements, both theoretical and computational, which were motivated in large part by its application to generating abelian surfaces for use in cryptography. For a long time, the CM method was the only practical way to find abelian surfaces suitable for deployment; while Schoof's classical point counting algorithm [**28**] was more than efficient enough to find cryptographic curves in genus 1, the genus 2 analogue [**27**] was originally too slow to count points on abelian surfaces with cardinalities large enough to match their elliptic curve counterparts. Nowadays, genus 2 point counting has become more efficient, such that (with enough computing power) one can find cryptographically strong Jacobians of size up to 256 bits [**17**] suitable for the 128-bit security level. When targeting higher security levels, however, counting points still appears too slow to find suitable genus 2 curves, and it is likely that the 192- and 256-bit security levels will remain out of reach of the Schoof–Pila algorithm for some time. On the other hand, the CM method can be used to efficiently construct cryptographically strong abelian surfaces at any foreseeable security level. Moreover, a state-of-the-art implementation [**14**] computes class polynomials for CM fields of class number well beyond 10^4, which essentially guarantees that the CM method can be used to find secure curves over any specific prime field: a larger search pool of CM fields means that implementers can fix their favorite prime characteristic p in advance, and can then expect to find such a CM field K where the splitting of p in $\mathcal{O}_K$ gives rise to almost prime group order(s) and thus strong cryptographic curves.

Received 27 February 2014; revised 23 May 2014.

2010 Mathematics Subject Classification 11G10, 11R37, 11G15, 11G20, 11T71, 11Y16 (primary).

Contributed to the Algorithmic Number Theory Symposium XI, GyeongJu, Korea, 6–11 August 2014.

In this paper we present a variant of the CM method in genus 2. Our primary motivation is the advent of 'Kummer cryptography': based on observations by Chudnovsky and Chudnovsky [10], Gaudry showed that working on the Kummer surface associated to a genus 2 Jacobian, rather than the Jacobian itself, results in large performance gains in the realm of public-key cryptography [15]. Just like the Jacobian variety, the Kummer surface, denoted by $\mathcal{K}$, can be embedded into projective space via the use of theta constants with half integer characteristics. For hyperelliptic curves of the form $C\colon y^2 = f(x)$, this embedding is linked to the roots of $f(x)$ (cf. [34]), and hence is also related to the *Rosenhain invariants* of C: for a genus 2 curve with $f(x) = \prod_{i=1}^{6}(x - u_i)$, over the algebraic closure, any three of the u_i can be mapped to 0, 1 and ∞ using linear fractional transformations to write C in Rosenhain form as

$$C_\lambda\colon y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3), \tag{1.1}$$

where λ_1, λ_2 and λ_3 are called 'the' Rosenhain invariants of C. Gaudry gives explicit relations between the constants defining the Kummer surface $\mathcal{K}$ and the Rosenhain invariants [15, § 4], which can be used to write down C_λ given the coefficients of $\mathcal{K}$, and vice versa.

We propose an algorithm to construct cryptographically strong genus 2 curves and their Kummer surfaces via Rosenhain invariants and the related Kummer parameters. The main benefits of the proposed approach include the following:

- The Rosenhain invariants satisfy minimal polynomials whose coefficients are much smaller than the coefficients of the Igusa class polynomials, which means that less precision is required in the computations.
- The equation of the curve $C = C_\lambda$ (1.1) is immediate once the Rosenhain invariants are found, in contrast to Igusa invariants, where the Mestre–Cardona–Quer algorithm [9, 24] is required in order to find the equation for C.
- Minimal polynomials for Kummer parameters can be computed in the same way as those of the Rosenhain invariants. These provide a direct way of determining the Kummer surfaces over a finite field $\mathbb{F}_p$, by taking a compatible system of roots. This avoids square root extractions required when computing $\mathcal{K}$ from C (cf. [6, § 5.2]), which can give rise to Kummer surface parameters not defined over the ground field $\mathbb{F}_p$.

To understand the trade-offs involved in this approach, we must consider the following issues:

- While the coefficients of the Rosenhain class polynomials are much smaller than their Igusa counterparts, the degrees of the Rosenhain polynomials are generally (though not always) larger[†].
- The method does not lend itself to finding cryptographic curves with Jacobian of prime order, since the entire 2-torsion is rational (that is, defined over $\mathbb{F}_p$) when the Rosenhain model is defined over $\mathbb{F}_p$, and thus 16 divides the group order.

To address the first point, we study the relationship between the degrees of the Igusa and Rosenhain invariants, and show that the degree increases by a small factor which depends on how the prime 2 splits in the CM field. In practice we can use our formulas to predict the degree of the Rosenhain invariants (or a small multiple of the degree) before computing them, which can help with recognizing their minimal polynomials when using algorithms based on LLL. We also give an algorithm for computing the Galois conjugates of the invariants, which can be used to compute minimal polynomials directly without LLL.

The second point above turns out to be a benefit, rather than a drawback. While prime order groups provide the best ratio of security to bit-length, the last decade of research has shown several benefits of using curves with a small amount of rational torsion. For elliptic curves, allowing rational 2- and 4-torsion points can facilitate much more efficient cryptography via the Montgomery model [26] or variants of the Edwards model [5, 12], while in genus 2 the

[†]Intuitively, the Igusa polynomials split in the field where the abelian surface C is defined, but the Rosenhain polynomials only split where the 2-torsion of the Jacobian, $\mathrm{Jac}(C)$, is also defined.

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

benefits are even more extreme: operation counts for Gaudry's formulas [15] estimate that allowing rational 2-torsion in order to use the Kummer surface can give rise to cryptographic operations which are more than twice as fast as working on a prime-order Jacobian [3], and this was confirmed both by recent performance results in [6] (which compared the two) and in [4] (which pushed the relative Kummer performance even further ahead). Furthermore, recent work by Lubicz and Robert [23] shows that it can be advantageous to allow at least one more rational small-torsion point in addition to the full 2-torsion, in order to facilitate 'compatible' additions on the Kummer surface (D. Robert, private communication, December 2013). The conclusion is that abelian surfaces constructed for state-of-the-art cryptography will have rational 2-torsion anyway. In addition, the Rosenhain polynomials can sometimes be used to deduce, for a specific CM field, congruence conditions on the primes p where all the 2-torsion is rational (Example 2 was chosen to illustrate this).

We give several tables with experimental data reflecting the degrees of the invariants and the size of the coefficients. Tables 2 and 3 show the degree of the Rosenhain invariants as it relates to the decomposition of the prime 2 in the CM field K. Table 4 summarizes the coefficient size for a number of examples which were used to find cryptographically strong curves at different security levels.

2. *Theta functions, Rosenhain invariants, and Kummer surfaces*

We give the basic theory of theta functions in § 2.1, set our choice of Rosenhain invariants in § 2.2, and recall the Kummer surface parameters in terms of theta functions in § 2.3. In this section we describe everything over the complex numbers. Let $\mathbb{H}_n = \{\Omega \in M_n(\mathbb{C}) : \Omega^t = \Omega, \operatorname{Im} \Omega \text{ is positive definite}\}$ denote the n-dimensional Siegel upper half-space parameterizing n-dimensional principally polarized abelian varieties.

2.1. *Theta functions*

Theta functions are modular forms, and we can take quotients to form modular functions whose values at points in $\mathbb{H}_2$ are the invariants of genus 2 curves. We adopt Gaudry's notation from [15] for the most part. Let $\tau \in \mathbb{H}_2$. For $z \in \mathbb{C}^2$, the Riemann theta function with characteristics $c_1, c_2 \in \mathbb{Q}^2$ is defined as

$$\theta[c_1, c_2](z, \tau) = \sum_{m \in \mathbb{Z}^2} \exp(\pi i (m + c_1)^t \tau (m + c_1) + 2\pi i (m + c_1)^t (z + c_2)).$$

We focus on the case where c_1 and c_2 are vectors with entries either 0 or $\frac{1}{2}$, so there are 16 possibilities for $[c_1, c_2]$. By evaluating at $z = (0, 0)$, this gives rise to 16 *theta constants*, which we number consistent with the numberings from [15, § 7.1], using the abbreviation $\theta[c_1, c_2] = \theta[c_1, c_2]((0, 0), \tau)$. The first ten theta constants are values of *even* theta functions, the last six are *odd*.

$$\begin{array}{llll}
\theta_1 = \theta[(0,0),(0,0)]; & \theta_2 = \theta[(0,0),(\frac{1}{2},\frac{1}{2})]; & \theta_3 = \theta[(0,0),(\frac{1}{2},0)]; & \theta_4 = \theta[(0,0),(0,\frac{1}{2})]; \\
\theta_5 = \theta[(\frac{1}{2},0),(0,0)]; & \theta_6 = \theta[(\frac{1}{2},0),(0,\frac{1}{2})]; & \theta_7 = \theta[(0,\frac{1}{2}),(0,0)]; & \theta_8 = \theta[(\frac{1}{2},\frac{1}{2}),(0,0)]; \\
\theta_9 = \theta[(0,\frac{1}{2}),(\frac{1}{2},0)]; & \theta_{10} = \theta[(\frac{1}{2},\frac{1}{2}),(\frac{1}{2},\frac{1}{2})]; & \theta_{11} = \theta[(0,\frac{1}{2}),(0,\frac{1}{2})]; & \theta_{12} = \theta[(0,\frac{1}{2}),(\frac{1}{2},\frac{1}{2})]; \\
\theta_{13} = \theta[(\frac{1}{2},0),(\frac{1}{2},0)]; & \theta_{14} = \theta[(\frac{1}{2},\frac{1}{2}),(\frac{1}{2},0)]; & \theta_{15} = \theta[(\frac{1}{2},0),(\frac{1}{2},\frac{1}{2})]; & \theta_{16} = \theta[(\frac{1}{2},\frac{1}{2}),(0,\frac{1}{2})].
\end{array}$$

2.2. *Rosenhain invariants*

For generating genus 2 curves for use in cryptography, there are many different possible combinations of six even theta constants which yield a Rosenhain model for the curve C_λ

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

as in (1.1), with

$$\lambda_1 = \frac{\theta_{i_1}^2 \theta_{i_3}^2}{\theta_{i_2}^2 \theta_{i_4}^2}, \quad \lambda_2 = \frac{\theta_{i_3}^2 \theta_{i_5}^2}{\theta_{i_4}^2 \theta_{i_6}^2}, \quad \lambda_3 = \frac{\theta_{i_1}^2 \theta_{i_5}^2}{\theta_{i_2}^2 \theta_{i_6}^2}.$$

Several different choices for this combination have appeared in the literature: Igusa [20] and Goren–Lauter [18] use $(i_1, \ldots, i_6) = (5, 1, 8, 7, 6, 4)$ while van Wamelen [35] takes $(i_1, \ldots, i_6) = (3, 5, 9, 8, 2, 6)$. In this work we find it convenient to adopt the choices of Gaudry [15], Cosset [11] and Grunewald [19], who all use $(i_1, \ldots, i_6) = (1, 2, 3, 4, 8, 10)$, to write

$$\lambda_1 = \frac{\theta_1^2 \theta_3^2}{\theta_2^2 \theta_4^2}, \quad \lambda_2 = \frac{\theta_3^2 \theta_8^2}{\theta_4^2 \theta_{10}^2}, \quad \lambda_3 = \frac{\theta_1^2 \theta_8^2}{\theta_2^2 \theta_{10}^2}. \tag{2.1}$$

2.3. *Kummer surfaces*

Kummer surfaces for use in cryptography can also be described directly in terms of their parameters, written as rational functions of the theta constants. We employ Cosset's reformulation [11] of Gaudry's Kummer surface description [15]. The first four theta constants

$$a = \theta_1, \quad b = \theta_2, \quad c = \theta_3, \quad d = \theta_4,$$

can be used to define a model for the level 2 Kummer variety $\mathcal{K}$ associated to the abelian surface corresponding to τ. Further defining

$$A = a + b + c + d, \quad B = a + b - c - d, \quad C = a - b + c - d, \quad D = a - b - c + d;$$
$$F = \frac{a^2 - b^2 - c^2 + d^2}{ad - bc}, \quad G = \frac{a^2 - b^2 + c^2 - d^2}{ac - bd}, \quad H = \frac{a^2 + b^2 - c^2 - d^2}{ab - cd};$$
$$E = \frac{ABCD}{(ad - bc)(ac - bd)(ab - cd)}, \quad E' = 4E^2 abcd,$$

then the projective surface $\mathcal{K} = \mathcal{K}(x, y, z, t)$ is defined by

$$E' \cdot xyzt = ((x^2 + y^2 + z^2 + t^2) - F \cdot (xt + yz) - G \cdot (xz + yt) - H \cdot (xy + zt))^2. \tag{2.2}$$

In addition to the four constants E', F, G, H that define the surface, routines for cryptographic *scalar multiplications* on $\mathcal{K}$ require six additional constants that appear in the (pseudo-)group law formulas:

$$y_0 = \frac{a}{b}, \quad z_0 = \frac{a}{c}, \quad t_0 = \frac{a}{d}, \quad y_0' = \frac{A}{B}, \quad z_0' = \frac{A}{C}, \quad t_0' = \frac{A}{D}.$$

Together with the four constants in (2.2), the above six constants are all that is needed to instantiate cryptographic scalar multiplications on $\mathcal{K}$; see [15] and [11] for the associated algorithms. The constant point (a, b, c, d) is the zero element for the (pseudo-)group law on $\mathcal{K}$.

The double-cover $\mathcal{J}_{C_\lambda} \to \mathcal{K}$ maps inverse divisors on the Jacobian of C_λ to the same element on $\mathcal{K}$; it also identically maps inverse points on $\mathcal{J}_{C'_\lambda}$ to $\mathcal{K}$, where C'_λ is the non-trivial quadratic twist of C_λ, which means that a random point on $\mathcal{K}$ can be pulled back (via the formulas in [11, 15]) to either $\mathcal{J}_{C_\lambda}$ or $\mathcal{J}_{C'_\lambda}$. Therefore, following an observation made in [2], in state-of-the-art Kummer cryptography it is essential that C_λ is chosen to be *twist-secure*, that is, that both $\mathcal{J}_{C_\lambda}$ and $\mathcal{J}_{C'_\lambda}$ have almost prime group orders.

The relation between the Kummer surface parameters and the Rosenhain invariants is given explicitly in [15] as

$$\lambda_1 = \frac{ac}{bd}, \qquad \lambda_2 = \frac{c}{d} \cdot \frac{1 + \sqrt{CD/AB}}{1 - \sqrt{CD/AB}}, \qquad \lambda_3 = \frac{a}{b} \cdot \frac{1 + \sqrt{CD/AB}}{1 - \sqrt{CD/AB}}. \tag{2.3}$$

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

3. *The CM method for abelian surfaces*

The goal of using the CM method in cryptography is to generate (smooth, projective, irreducible) curves over a finite field with a given number of points on the Jacobian. The complex analytic version of the CM method for genus 2 has been proposed, implemented and improved in [**14**, **31**–**33**, **35**, **36**]. We do not discuss the p-adic [**16**] or CRT [**13**] versions of the method here. The method works by relating the number of points on the Jacobian of the curve over a finite field $\mathbb{F}_p$ to the endomorphism ring of the Jacobian of the curve. In the ordinary case, the endomorphism ring determines a CM field K, and then the problem becomes constructing abelian varieties with CM by the field K. This is accomplished by computing the CM points on $\mathbb{H}_2$ and evaluating certain modular functions at those points. These values are algebraic numbers lying in some large number field. In order to recognize the invariants of the curve or variety over a finite field, we first compute the minimal polynomial over $\mathbb{Q}$ (or some extension field of $\mathbb{Q}$), and then reduce modulo the prime p to find its roots. The rest of this section will explain these steps in detail and give the algorithm we use for evaluating Rosenhain invariants.

3.1. *Determining the number of points*

A (smooth, projective, irreducible) curve over a finite field $\mathbb{F}_p$ has a Frobenius endomorphism, and in genus 2 this endomorphism has a quartic characteristic polynomial $f(t) = t^4 - s_1t^3 + s_2t^2 - ps_1t + p^2$. If the curve is ordinary and f is irreducible, let K be the quartic CM field defined by the polynomial f and fix an embedding of K into the complex numbers. Let π be a complex root of the polynomial $f(t)$. The roots of f consist of conjugate pairs $(\pi, \overline{\pi})$ and $(\pi', \overline{\pi}')$, with the property $\pi'\overline{\pi}' = \pi\overline{\pi} = p$, and these are called 'Weil p-numbers'.

If a solution to $\pi\overline{\pi} = p$ exists in the field K, then the ideal $\mathfrak{p} = (\pi)$ in $\mathcal{O}_K$ has relative norm $\mathfrak{p}\overline{\mathfrak{p}} = p$. So to determine the possible group orders of abelian surfaces over $\mathbb{F}_p$ with CM by K, it suffices to factor the ideal $p\mathcal{O}_K$ and look for principal generators of the factors.

Thus, given a CM field K and a prime p, the ordinary genus 2 curves over $\mathbb{F}_p$ with CM by K (that is, with $\mathrm{End}(\mathcal{J}_C) \cong \mathcal{O}_K$) correspond to generators of principal ideals with relative norm p such that $|\pi| = \sqrt{p}$. Note that a generator may have to be scaled by a unit in K to ensure that $|\pi| = \sqrt{p}$. Since $\#\mathcal{J}_C(\mathbb{F}_p) = (1-\pi)(1-\overline{\pi})(1-\pi')(1-\overline{\pi}')$, in order to know the possible group orders for genus 2 curves with CM by K, it suffices to find the prime ideal decomposition of p in $\mathcal{O}_K$ (which determines all possible πs). For primes which split completely into principal ideals in the reflex field of K, there are always two possible group orders when $K \neq \mathbb{Q}(\zeta_5)$ is Galois cyclic and four possible group orders when K is non-Galois (see [**13**, Proposition 4] for the possibilities).

In our application, we generate many CM fields K for which we can compute the minimal polynomials of the Rosenhain invariants, and then we sieve through primes p (of a special form which are advantageous for implementation) until the pair (p, K) gives rise to group orders suitable for cryptography.

3.2. *Computing CM points on the moduli space*

An abelian variety of dimension n over $\mathbb{C}$ is analytically isomorphic to $\mathbb{C}^n/\Lambda$ for some lattice Λ with a non-degenerate Riemann form; this form induces a polarization on the abelian variety. As above, let $\mathbb{H}_n$ be the Siegel upper half plane parameterizing polarized abelian varieties of dimension n. By constructing a symplectic basis for the lattice with respect to the Riemann form, we can write Λ as $\Lambda = \mathbb{Z}^n + \tau\mathbb{Z}^n$ where $\tau \in \mathbb{H}_n$. Any Jacobian variety of a curve has a principal polarization induced by the curve. In particular, we focus on two-dimensional abelian varieties that are Jacobians of genus 2 curves. Our first goal will be to compute at least one τ given the endomorphism ring.

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

An abelian variety of dimension n over $\mathbb{C}$ is called a *CM abelian variety* if its endomorphism ring is isomorphic to an order in the ring of integers of a CM number field of degree $2n$. We will focus here on the case where the endomorphism ring is isomorphic to the maximal order $\mathcal{O}_K$. A CM number field K is an imaginary quadratic extension of a totally real field K_0 of degree n.

A CM type (K, Φ) is a pair where K is a CM field and Φ is a set of n complex embeddings of K, $\Phi = \{\phi_1, \ldots, \phi_n\}$ such that $\phi_i \neq \phi_j, \rho\phi_j$ for $i \neq j$ where ρ is complex conjugation. A CM type is called simple if it is not lifted from a CM type strictly contained in K. Let $\mathfrak{a}$ be an ideal of K and let $\mathcal{O}_K$ be the ring of integers of K. Then

$$\Phi(\alpha) = (\phi_1(\alpha), \ldots, \phi_n(\alpha))^t, \quad \alpha \in \mathfrak{a},$$

forms a lattice in $\mathbb{C}^n$ with CM by $\mathcal{O}_K$. The corresponding abelian variety is said to have CM of type (K, Φ). We only study simple CM types of dimension 2. Thus we restrict to quartic CM number fields K where $K/\mathbb{Q}$ is either Galois cyclic or non-Galois, avoiding the biquadratic case where the Galois group is the Klein 4-group because (K, Φ) is not simple [**30**, pp. 63–65].

To compute τ, we must also specify the Riemann form on $\Phi(\mathfrak{a})$. To do so, we use the following theorems of Shimura and Taniyama [**30**, Chapter 2, Theorem 4]: if K_0 is the real quadratic subfield and ξ is such that

(1) $K = K_0(\xi)$, $\xi^2 \in K_0$ and $\mathrm{Im}(\phi_i(\xi)) > 0$ for all $\phi_i \in \Phi$, and
(2) $\mathfrak{D}_{K/\mathbb{Q}}\mathfrak{a}\overline{\mathfrak{a}} = (\xi^{-1})$ for some fractional ideal $\mathfrak{a}$ of K, where $\mathfrak{D}_{K/\mathbb{Q}}$ is the different,

then $E(z, w) = \sum_{j=1}^{n} \phi_j(\xi)(\overline{z_j}w_j - z_j\overline{w_j})$ defines a principal polarization of type (K, Φ) on $\mathbb{C}^n/\Phi(\mathfrak{a})$. Furthermore, if (K, Φ) is a simple type, then all principal polarizations of type (K, Φ) on $\mathbb{C}^n/\Phi(\mathfrak{a})$ are given by such ξ. Shimura and Taniyama also prove that two principally polarized simple abelian varieties $(\mathbb{C}^n/\Phi(\mathfrak{a}), \xi_1)$ and $(\mathbb{C}^n/\Phi(\mathfrak{b}), \xi_2)$ of the same type are isomorphic if and only if there exists $\gamma \in K$ such that $\gamma\mathfrak{a} = \mathfrak{b}$ and $\xi_1 = \gamma\overline{\gamma}\xi_2$ [**30**, Chapter 2, Proposition 14, and p. 107]. Together, these theorems give an algorithm to compute the principally polarized CM abelian varieties with CM by K up to isomorphism. This algorithm was first proposed by Spallek [**31**] and then implemented robustly by van Wamelen [**35**] and Weng [**36**] for the Jacobian of a genus 2 curve. In particular, when K_0 has class number 1, Weng and Spallek gave a closed form for the entries of the period matrices for all isomorphism classes of principally polarized abelian varieties with CM by K. For our results, we implemented the following algorithm which is an extension of [**35**, Algorithm 1], and essentially the same as [**32**, Algorithm 3.1] and [**14**, Algorithm 1].

ALGORITHM 1. Input: a primitive quartic CM field K.
Output: period matrices for all principally polarized abelian surfaces with CM by $\mathcal{O}_K$.

(i) Compute the class group of K. Each ideal class gives an isomorphism class of complex tori with CM by $\mathcal{O}_K$ as above.
(ii) Find all ideal classes $[\mathfrak{a}]$ such that $[\mathfrak{a}\overline{\mathfrak{a}}] = [\mathfrak{D}_{K/\mathbb{Q}}^{-1}]$. Pick an ideal $\mathfrak{a}$ from each of these ideal classes and compute a generator b of the ideal $\mathfrak{D}_{K/\mathbb{Q}}\mathfrak{a}\overline{\mathfrak{a}}$.
(iii) If the ideal class gives an abelian variety with a principal polarization, we can find a unit $u \in \mathcal{O}_K$ so that $ub = -\overline{ub}$. Then set $\xi_0 = (ub)^{-1}$.
(iv) Iterate over the units in $\mathcal{O}_{K_0}$ modulo norms of units in $\mathcal{O}_K$ to find all possible principal polarizations for each ideal class: for each unit u^+ in this set, choose a type Φ so that if $\xi = u^+\xi_0$, then $\mathrm{Im}(\phi_i(\xi)) > 0$ for each $\phi_i \in \Phi$.
(v) Each ξ defines a principal polarization E of type (K, Φ) on $\mathbb{C}^n/\Phi(\mathfrak{a})$.
(vi) Compute a symplectic basis of $\mathcal{B} = \{e_1, e_2, f_1, f_2\}$ of $\Phi(\mathfrak{a})$ with respect to the symplectic form $\langle z, w\rangle = \mathrm{tr}(\xi z w)$. Then

$$\omega_1 = \begin{pmatrix} \sigma_1(e_1) & \sigma_2(e_1) \\ \sigma_1(e_2) & \sigma_2(e_2) \end{pmatrix}, \quad \omega_2 = \begin{pmatrix} \sigma_1(f_1) & \sigma_2(f_1) \\ \sigma_1(f_2) & \sigma_2(f_2) \end{pmatrix}, \quad \text{and} \quad \tau = \omega_1\omega_2^{-1}.$$

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

3.3. *Igusa class polynomials*

Let $\{\tau_i\} \in \mathbb{H}_2$ be the period matrices as output by Algorithm 1. The three *Igusa invariants*, $j_{1,i}$, $j_{2,i}$, $j_{3,i}$, are computed (via the evaluation of the theta functions) as functions of τ_i, from which the *Igusa class polynomials*, $H_1(x), H_2(x), H_3(x)$, are constructed:

$$H_1(x) = \prod_i (x - j_{1,i}), \quad H_2(x) = \prod_i (x - j_{2,i}), \quad H_3(x) = \prod_i (x - j_{3,i}). \tag{3.1}$$

The purpose of this paper is to replace the Igusa class polynomials (in the CM method) by analogous polynomials obtained from the Rosenhain invariants, $\lambda_1, \lambda_2, \lambda_3$. In both cases, there is a precise representation of the ideal defining the invariants (proposed for Igusa invariants in [**16**, § 3]) which is more convenient than (3.1); we illustrate this modification for the Rosenhain polynomials in Examples 4 and 5.

3.4. *Computing λ-invariants and Kummer surfaces*

Similar to the Igusa invariants case, we compute the Rosenhain invariants as algebraic numbers by evaluating theta functions to high precision on the period matrices that are output by Algorithm 1. Recall that we are computing the following choice of Rosenhain invariants: $\lambda_1(\tau) = \theta_1^2\theta_3^2/\theta_2^2\theta_4^2, \lambda_2(\tau) = \theta_3^2\theta_8^2/\theta_4^2\theta_{10}^2, \lambda_3(\tau) = \theta_1^2\theta_8^2/\theta_2^2\theta_{10}^2$ at $z = (0,0)$. Computer algebra systems such as Magma and Sage have theta function implementations which can be used to compute the Rosenhain invariants as complex numbers with given precision. The bottleneck occurs when trying to recognize the Rosenhain invariants as algebraic numbers. For τ output by Algorithm 1, if we compute $\lambda_1(\tau), \lambda_2(\tau), \lambda_3(\tau)$ to enough precision, we can use the LLL algorithm [**22**] to recognize the minimal polynomials of the Rosenhain invariants.

In § 5 below, we compute a bound on (actually a multiple of) the degree of the minimal polynomials of the Rosenhain invariants which helps with the speed and accuracy of the LLL step. The parameters defining the Kummer surface are also written as rational functions in the theta constants, and the precise relationship with the Rosenhains was given in (2.3). In practice, we have recognized the Rosenhain invariants and Kummer invariants for many CM fields K with this approach, and used them to generate suitable curves and Kummer surfaces for cryptography; see § 6. However, the above algorithm does not produce all the Galois conjugates of the CM values of the Rosenhain functions. In the next section, we describe how to compute them.

4. *Galois conjugates of a CM point*

In this section we will explain how to compute the Galois conjugates of a CM value of the λ functions and their minimal polynomials. The algorithm we give here follows from the theory of complex multiplication and does not use Shimura's reciprocity law (see [**38**] for further explanation). We describe the algorithm in concrete terms. A self-contained and readable account of Shimura's explicit reciprocity law and its applications to computing the Galois conjugates of CM values of a modular function is given by Streng [**33**]. While Streng's work deals with a much more general case, we focus on the application to the Rosenhain invariants and give an algorithm for explicitly computing the Galois conjugates of a CM point and the minimal polynomials of Rosenhain invariants.

4.1. *Preliminaries*

Let (K, Φ) be a non-biquadratic quartic CM number field with CM type $\Phi = \{\sigma_1, \sigma_2\}$ and real quadratic subfield K_0. Let (K^r, Φ^r) be its reflex field and reflex CM type with real quadratic

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

subfield K_0^r. Let $M = KK^r$ be the Galois closure of K and K^r over $\mathbb{Q}$; then $\mathrm{Gal}(M/\mathbb{Q})$ is either the dihedral group of order 8 or the cyclic group of order 4. Let

$$\Phi_M = \{\sigma \in \mathrm{Gal}(M/\mathbb{Q}) : \sigma|_K = \sigma_1 \text{ or } \sigma_2\}$$

which is a CM type of M. Similarly, one defines the reflex CM type extension Φ_M^r of Φ^r to M. Then $\Phi_M^r = \{\sigma^{-1} : \sigma \in \Phi_M\}$. The type norm N_{Φ^r} is defined as follows. For an element $x \in K^r$, one has $\mathrm{N}_{\Phi^r}(x) = \sigma_1^r(x)\sigma_2^r(x)$. For a fractional ideal $\mathfrak{b}$ of K^r, one has

$$\mathrm{N}_{\Phi^r}(\mathfrak{b}) = \sigma_1^r(\mathfrak{b})\sigma_2^r(\mathfrak{b})\mathcal{O}_M \cap K. \tag{4.1}$$

Let us identify $\{\pm 1\} \cong \mathbb{Z}/2$. For a principally polarized abelian surface (A, λ), the Weil pairing on the 2-torsion $A[2]$ becomes a non-degenerate symplectic form:

$$\langle\,,\rangle \quad A[2] \times A[2] \to \mathbb{Z}/2.$$

Recall that $X(2) = \Gamma(2)\backslash\mathbb{H}_2$ is the coarse moduli space of the isomorphism classes of triples (A, λ, B), where (A, λ) is a principally polarized abelian surface and $B = \{e_1, e_2, f_1, f_2\}$ is an ordered symplectic basic of $A[2]$. A CM point of CM type (K, Φ) in $X(2)$ is then indexed by a tuple $(\mathfrak{a}, \xi, B)$, where:

(1) $\mathfrak{a}$ is a fractional ideal of K, $\xi \in K^\times$ with $\bar{\xi} = -\xi$ such that $\mathfrak{a}$ is self-dual with respect to the symplectic form

$$\langle x, y\rangle = \mathrm{tr}_{K/\mathbb{Q}}\, \xi x \bar{y} \tag{4.2}$$

on K, which is equivalent to

$$\xi \mathfrak{D}_{K/\mathbb{Q}} \mathfrak{a}\bar{\mathfrak{a}} = \mathcal{O}_K. \tag{4.3}$$

(2) $B = \{e_1, e_2, f_1, f_2\}$ is an ordered symplectic $\mathbb{Z}$-basis with the following property. Let

$$\omega_1 = \begin{pmatrix} \sigma_1(e_1) & \sigma_2(e_1) \\ \sigma_1(e_2) & \sigma_2(e_2) \end{pmatrix}, \quad \omega_2 = \begin{pmatrix} \sigma_1(f_1) & \sigma_2(f_1) \\ \sigma_1(f_2) & \sigma_2(f_2) \end{pmatrix}, \quad \text{and} \quad \tau = \omega_1\omega_2^{-1}.$$

We require $\mathrm{Im}\,\tau > 0$.

In this case, $\tau \in X(2)$ gives the CM point, and the associated triple is $(A_{\mathfrak{a}}, \lambda, \Phi(B))$, where $A = \mathbb{C}^2/\Phi(\mathfrak{a})$, λ is given by the symplectic form, $\Phi(B) = \{\Phi(e_1), \Phi(e_2), \Phi(f_1), \Phi(f_2)\}$, and $\Phi(a) = (\sigma_1(a), \sigma_2(a)) \in \mathbb{C}^2$ for $a \in \mathfrak{a}$. Furthermore, $A[2] \cong \frac{1}{2}\mathfrak{a}/\mathfrak{a}$, and the Weil pairing is given by

$$\tfrac{1}{2}\mathfrak{a} \times \tfrac{1}{2}\mathfrak{a} \to \mathbb{Z}/2, \quad \langle \tfrac{1}{2}x, \tfrac{1}{2}y\rangle = \langle x, y\rangle \pmod 2,$$

where the left-hand side is the Weil pairing and the right-hand side is the symplectic pairing given by (4.2).

4.2. *The action*

Let $\mathrm{CL}(K^r, \Phi^r, 2)$ be the quotient group of fractional ideals of K^r which are prime to 2, modulo fractional ideals $\mathfrak{b}$, with the property

$$\mathrm{N}_{\Phi^r}(\mathfrak{b}) = \alpha\mathcal{O}_K, \quad \alpha \equiv 1 \pmod 2, \quad \alpha\bar{\alpha} = \mathrm{N}(\mathfrak{b}).$$

We call this group the *CM class group of K^r of type Φ^r and level* 2. Let $H(2)$ be the associated class field of K^r with the canonical isomorphism

$$\mathrm{CL}(K^r, \Phi^r, 2) \cong \mathrm{Gal}(H(2)/K^r), \quad [\mathfrak{b}] \mapsto \sigma_{\mathfrak{b}}.$$

By the theory of complex multiplication, a CM point $\tau = (\mathfrak{a}, \xi, B)$ of CM type (K, Φ) is defined over $H(2)$. We now describe the image of τ under the action of $\sigma_{\mathfrak{b}^{-1}}$.

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

Step 1: Since $\mathrm{N}_{\Phi^r}(\mathfrak{b})\overline{\mathrm{N}_{\Phi^r}(\mathfrak{b})} = \mathrm{N}(\mathfrak{b}) \in \mathbb{Q}_{>0}$, $\mathfrak{a}\,\mathrm{N}_{\Phi^r}(\mathfrak{b})$ is *self-dual* with respect to the new symplectic form

$$\langle x, y\rangle_{\mathfrak{b}} = \frac{1}{\mathrm{N}(\mathfrak{b})}\langle x, y\rangle.$$

Choose a symplectic basis $B' = \{e_1', e_2', f_1', f_2'\}$ of $\mathfrak{a}\,\mathrm{N}_{\Phi^r}(\mathfrak{b})$ with respect to this new symplectic form, such that $\tau' = \omega_1'(\omega_2')^{-1} \in \mathbb{H}_2$, where ω_i' is defined the same way as ω_i in this new context. Then $\tau' = (\mathfrak{a}\,\mathrm{N}_{\Phi^r}(\mathfrak{b}), (\xi/\,\mathrm{N}(\mathfrak{b})), B') \in X(2)$ is a CM point of CM type (K, Φ). Note that a symplectic basis can be computed using the `FrobeniusFormAlternating` command in Magma, or the `symplecticform` command in Sage.

Step 2: To get $\sigma_{\mathfrak{b}^{-1}}\tau$, we need to modify the symplectic basis B'. Choose an $\alpha \in \mathrm{N}_{\Phi^r}(\mathfrak{b})$ such that $\alpha \equiv 1 \pmod 2$, that is, $\mathrm{ord}_v(\alpha - 1) \geqslant 0$ for $v|2$ if 2 is unramified, and that $\alpha\bar{\alpha} \in \mathbb{Q}_{>0}$. One choice is to take $\alpha = \mathrm{N}_{\Phi^r}(b)$ with $b \in \mathfrak{b}$ and $b \equiv 1 \pmod 2$.

Step 3: Notice that $(\alpha e_i/2), (\alpha f_j/2) \in A_{\mathfrak{a}\,\mathrm{N}_{\Phi^r}(\mathfrak{b})}[2]$, and that

$$\left\langle \frac{\alpha e_i}{2}, \frac{\alpha f_j}{2} \right\rangle_{\mathfrak{b}} = \frac{\alpha\bar{\alpha}}{\mathrm{N}(\mathfrak{b})}\delta_{ij} = \delta_{ij} \in \mathbb{Z}/2,$$
$$\left\langle \frac{\alpha e_i}{2}, \frac{\alpha e_j}{2} \right\rangle_{\mathfrak{b}} = \left\langle \frac{\alpha f_i}{2}, \frac{\alpha f_j}{2} \right\rangle_{\mathfrak{b}} = 0,$$

where δ_{ij} is the Dirac symbol. Now we find a $\gamma \in \mathrm{Sp}_4(\mathbb{Z})$ such that

$$\gamma\left(\frac{e_1'}{2}, \frac{e_2'}{2}, \frac{f_1'}{2}, \frac{f_2'}{2}\right)^t = \left(\frac{\alpha e_1}{2}, \frac{\alpha e_2}{2}, \frac{\alpha f_1}{2}, \frac{\alpha f_2}{2}\right)^t \mod (\mathfrak{a}\,\mathrm{N}_{\Phi^r}(\mathfrak{b})).$$

Then, by the main theorem of complex multiplication [29], we have:

$$\sigma_{\mathfrak{b}^{-1}}(\mathfrak{a}, \xi, B) = \left(\mathfrak{a}\,\mathrm{N}_{\Phi^r}(\mathfrak{b}), \frac{\xi}{\mathrm{N}(\mathfrak{b})}, \gamma(B')\right), \quad \text{or, more concretely,} \quad \sigma_{\mathfrak{b}^{-1}}(\tau) = \gamma(\tau'). \tag{4.4}$$

Before the next subsection, we give a brief justification of the above steps (see [38, § 3] for a proof and generalization). Clearly the above definition depends only on the class of $[\mathfrak{b}]$. Let s be a finite idele of K^r such that $s_v = 1$ for a prime $v|2$ of K^r, and that the ideal of s is $(s) = \mathfrak{b}^{-1}$. Then [29, Theorem 5.15] asserts that $\sigma_s(A_{\mathfrak{a}}) = A_{\mathfrak{a}\,\mathrm{N}_{\Phi^r}(\mathfrak{b})}$ and it moves a 2-torsion point $x/2 \in \frac{1}{2}\mathfrak{a}/\mathfrak{a}$ in $A_{\mathfrak{a}}$ to the 2-torsion point $y/2 \in \frac{1}{2}(\mathfrak{a}\,\mathrm{N}_{\Phi^r}(\mathfrak{b}))/(\mathfrak{a}\,\mathrm{N}_{\Phi^r}(\mathfrak{b}))$ in $A_{\mathfrak{a}\,\mathrm{N}_{\Phi^r}(\mathfrak{b})}$, where $y \in \mathfrak{a}\,\mathrm{N}_{\Phi^r}(\mathfrak{b})$ satisfies

$$\frac{y}{2} = \frac{s^{-1}x}{2} = \left(\frac{s_v^{-1}x_v}{2}\right) \in K/\mathfrak{a}\,\mathrm{N}_{\Phi^r}(\mathfrak{b}) = \oplus K_v/(\mathfrak{a}\,\mathrm{N}_{\Phi^r}(\mathfrak{b}))_v.$$

Our construction gives

$$\sigma_s\left(\frac{e_i}{2}\right) = \frac{\alpha e_i}{2}, \quad \sigma_s\left(\frac{f_i}{2}\right) = \frac{\alpha f_i}{2}, \quad i = 1, 2.$$

So

$$\sigma_{\mathfrak{b}^{-1}}(\mathfrak{a}, \xi, B) = \sigma_s\left(A_{\mathfrak{a}}, \frac{e_i}{2}, \frac{f_i}{2}\right) = \left(A_{\mathfrak{a}\,\mathrm{N}_{\Phi^r}(\mathfrak{b})}, \frac{\alpha e_i}{2}, \frac{\alpha f_i}{2}\right).$$

Notice that $\{\alpha e_i, \alpha f_i, i = 1, 2\}$ does not in general give a $\mathbb{Z}$-basis of $\mathfrak{a}\,\mathrm{N}_{\Phi^r}(\mathfrak{b})$. However, our modification $\gamma(B')$ is a symplectic $\mathbb{Z}$-basis of $\mathfrak{a}\,\mathrm{N}_{\Phi^r}(\mathfrak{b})$ which satisfies

$$\frac{\gamma(B')}{2} = \{\alpha e_i, \alpha f_i, i = 1, 2\} \mod (\mathfrak{a}\,\mathrm{N}_{\Phi^r}(\mathfrak{b})).$$

This justifies our construction.

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

4.3. *The minimal polynomial of Rosenhain invariants*

Now it is easy to compute class and minimal polynomials of $\lambda_j(\tau)$, $j = 1, 2, 3$, over K^r.

Step 4: For each class $[\mathfrak{b}] \in \mathrm{CL}(K^r, \Phi^r, 2)$, choose a representative ideal $\mathfrak{b}$ and compute $\sigma_{\mathfrak{b}^{-1}}\tau = \tau_{\mathfrak{b}} \in \mathbb{H}_2$.

Step 5: Compute the class polynomial of $\lambda_j(\tau)$

$$\lambda_j(x) = \prod_{[\mathfrak{b}]\in \mathrm{CL}(K^r,\Phi^r,2)} (x - \lambda_j(\tau_{\mathfrak{b}})). \tag{4.5}$$

It is defined over K^r by construction. It is actually defined over the real quadratic field K_0^r of K^r if at least one of the values $\lambda_j(\tau_{\mathfrak{b}})$ is (recognizable as) real, as the Fourier coefficients of λ_j are defined over $\mathbb{Q}$. To get the minimal polynomial, we do the same, except that we use only one $\lambda_j(\tau_{\mathfrak{b}})$ value in the case where more than one are the same value. This minimal polynomial is also defined over K_0^r when $\lambda_j(x)$ is.

Although the coefficients of $\lambda_j(x)$ can have denominators, we can clear the denominators by multiplying by some integer, which is given by formulas proved independently by Yang [**37**] and then by Lauter and Viray [**21**] for more general CM fields. Actually using the result in [**8**], one can compute the norm of $\lambda_j(\tau) \in \mathbb{Q}$ with a precise factorization.

Remark 1. We get the other conjugates over $\mathbb{Q}$ by varying the CM type to obtain the minimal polynomial over $\mathbb{Q}$. Note, though, that when working over a finite field $\mathbb{F}_p$, we often work under the assumption that p splits completely in the reflex field. In that case we could directly use the minimal polynomial arising from one CM type modulo p. Also, an anonymous reviewer commented that once we have computed a polynomial over K_0^r, there is actually no need to compute a second polynomial for the other CM type, since we may simply apply the real conjugation map to the first polynomial.

In the remainder of the paper, we compute minimal polynomials for the λ_i by the method described in § 3.4 above, using LLL to recognize minimal polynomials over $\mathbb{Q}$, instead of the method just described which computes all conjugates. This often leads to polynomials which have different degree for λ_i and λ_j, and makes it difficult to find a nice representation for the ideal which represents the CM points precisely on the moduli space. In fact, the Lagrange interpolation method from [**16**, § 3] will work smoothly when using the same set of CM points, for example, the orbit set just described in this section where all three polynomials have the same degree (all over K_0^r) but might not be irreducible.

5. *Comparing the degree of Igusa and Rosenhain invariants*

5.1. *Degree of Igusa invariants*

In order to understand the potential advantage of computing genus 2 curves via their Rosenhain invariants, we need to compare the degrees of Igusa and Rosenhain invariants. Equations (3.1) define the *Igusa class polynomials*, but they are not necessarily irreducible over $\mathbb{Q}$, as can be seen already from the examples of genus 2 CM curves over $\mathbb{Q}$ given by van Wamelen [**35**]. Nonetheless, we will refer to the degree of the Igusa class polynomials as the *degree* of the invariants. In other words, it is the number of principally polarized abelian surfaces with CM by K, which is equal to the number of period matrices output by Algorithm 1 above. It follows from [**7**, Theorem 3.1 and Corollary 3.3] and equivalently from [**32**, Lemma 3.5] that the number of isomorphism classes of principally polarized abelian surfaces with CM by K is equal to $c_0 \cdot |\mathrm{Cl}(K)|/|\mathrm{Cl}(K_0)|$ if $K/\mathbb{Q}$ is Galois cyclic, and $2c_0 \cdot |\mathrm{Cl}(K)|/|\mathrm{Cl}(K_0)|$ if $K/\mathbb{Q}$ is non-Galois, where $c_0 = |\mathcal{O}_{K_0}^{\times}/(\mathcal{O}_{K_0}^{\times})^{+}|$, the order of the group of units in $\mathcal{O}_{K_0}$ modulo the

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

totally positive units, and so $c_0 = 1$ or 2. In what follows we denote the order of the class group $\mathrm{Cl}(K)$ of K, by $h = |\mathrm{Cl}(K)|$, and the order of the quotient $h^- = h^-(K) = |\mathrm{Cl}(K)|/|\mathrm{Cl}(K_0)|$.

5.2. *Degree of Rosenhain invariants*

Next we will relate the degree of the Rosenhain invariants to h^-. We define the *degree* of the Rosenhain invariants to be the degree of the polynomials $\lambda_i(x)$ defined in equation (4.5). In § 4.2 above, we used the fact that the CM values $\lambda_i(\tau)$ lie in the field $H(2)$, an extension of K^r of degree $h_2^{\Phi^r} = |\mathrm{CL}(K^r, \Phi^r, 2)|$. Thus the Rosenhain invariants lie in a field of degree at most $4h_2^{\Phi^r}$ over $\mathbb{Q}$. In what follows we will relate $h_2^{\Phi^r}$ to h^-.

In [**25**, Theorem 1.7, p. 146], an exact sequence is given which relates the *ray class group with modulus* $\mathfrak{m}$ of a number field K to the class group of K. To simplify, we will assume here that the modulus $\mathfrak{m}$ is a product of prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$, (*finite* primes), with some multiplicity $m(\mathfrak{p})$, and in particular in our application we will take $\mathfrak{m}$ to be the modulus $2\mathcal{O}_K$ (or sometimes $2\mathcal{O}_{K_0}$). This exact sequence can be used to understand the relationship between $h_2^{\Phi^r}$ and h^-:

$$0 \to U/U_{\mathfrak{m},1} \to K_{\mathfrak{m}}/K_{\mathfrak{m},1} \to C_{\mathfrak{m}} \to \mathrm{Cl}(K) \to 0,$$

where $C_{\mathfrak{m}} = C_{\mathfrak{m}}(K)$ is the group of fractional ideals of K prime to $\mathfrak{m}$, modulo principal ideals generated by elements of $K_{\mathfrak{m},1}$, where

$$\begin{aligned} K_{\mathfrak{m}} &= \{\alpha \in K^\times \mid \mathrm{ord}_{\mathfrak{p}}(\alpha) = 0, \forall \mathfrak{p} \mid \mathfrak{m}\}, \\ K_{\mathfrak{m},1} &= \{\alpha \in K^\times \mid \mathrm{ord}_{\mathfrak{p}}(\alpha - 1) \geqslant m(\mathfrak{p}), \forall \mathfrak{p} \mid \mathfrak{m}\}, \\ U &= U(K) = \mathcal{O}_K^\times, \quad U(K_0) = \mathcal{O}_{K_0}^\times, \\ U_{\mathfrak{m},1} &= U \cap K_{\mathfrak{m},1}, \quad U_{\mathfrak{m}_0,1}(K_0) = U(K_0) \cap K_{\mathfrak{m}_0,1}. \end{aligned}$$

Thus the order of $C_{\mathfrak{m}}$ is given by the formula

$$|C_{\mathfrak{m}}| = h \cdot \mathrm{N}(\mathfrak{m}) \cdot \prod_{\mathfrak{p}|\mathfrak{m}} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})}\right) \Big/ [U : U_{\mathfrak{m},1}].$$

Corollary 5.1. *Let* $\mathfrak{m}_0 = 2\mathcal{O}_{K_0}$ *and* $\mathfrak{m} = 2\mathcal{O}_K$. *Denote* $h_2^-(K) = |C_{\mathfrak{m}}(K)|/|C_{\mathfrak{m}_0}(K_0)|$. *Then*

$$h_2^-(K) = h^-(K)c(K) \tag{5.1}$$

where

$$c(K) = \frac{\mathrm{N}(\mathfrak{m}) \prod_{\mathfrak{p}|\mathfrak{m}} (1 - (\mathrm{N}(\mathfrak{p})^{-1}))}{\mathrm{N}(\mathfrak{m}_0) \prod_{\mathfrak{p}_0|\mathfrak{m}_0} (1 - \mathrm{N}(\mathfrak{p}_0)^{-1})} \frac{[U(K_0) : U_{\mathfrak{m}_0,1}(K_0)]}{[U(K) : U_{\mathfrak{m},1}(K)]}.$$

Proof. Apply the above exact sequence twice, for $C_{\mathfrak{m}}(K)$ and $C_{\mathfrak{m}_0}(K_0)$. □

Now in the case at hand, $\mathfrak{m}_0 = 2\mathcal{O}_{K_0}$ and $\mathfrak{m} = 2\mathcal{O}_K$, let $h_2 = |C_{\mathfrak{m}}|$. We can determine $c(K)$ fairly precisely because the following proposition shows that the contribution from the unit terms is 1, except when $K = \mathbb{Q}(\zeta_5)$, and in that case we have $c(\mathbb{Q}(\zeta_5)) = 1$.

Proposition 5.2. *Let* K *be a non-biquadratic quartic CM number field with real quadratic subfield* K_0.

(i) *Then* $U(K) = U(K_0)$ *unless* $K = \mathbb{Q}(\zeta_5)$, *in which case* $U(K) = U(K_0)\langle\zeta_5\rangle$.
(ii) *Assume* $K \neq \mathbb{Q}(\zeta_5)$. *Then* $[U(K_0) : U_{\mathfrak{m}_0,1}(K_0)] = [U(K) : U_{\mathfrak{m},1}(K)]$.

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

Proof. The case $K = \mathbb{Q}(\zeta_5)$ can be handled with a straightforward calculation. Assume now $K \neq \mathbb{Q}(\zeta_5)$ so that the only roots of unity in K are ± 1. Let u be a unit of K; then there is a positive integer n such that $u^n = a$ is a unit of K_0 by the Dirichlet unit theorem. So $(\bar{u})^n = a$ and $(u/\bar{u})^n = 1$. This implies $\bar{u} = \pm u$. If $\bar{u} = u$, $u \in U(K_0)$, we are done. If $\bar{u} = -u$, $u^2 = -\epsilon$ for a totally positive unit ϵ of K_0 and $K = K_0(u) = K_0(\sqrt{-\epsilon})$. Then $K_0^r = \mathbb{Q}(\sqrt{\epsilon\epsilon'}) = \mathbb{Q}(\sqrt{1})$, where ϵ' is the real conjugate of ϵ. This contradicts the assumption that K is non-biquadratic.
Part (ii) follows from part (i). □

It follows from Proposition 5.2 that the value of $c(K)$ is completely determined by the splitting behavior of the prime in K_0 and K. A case-by-case calculation for each possible decomposition yields the following proposition:

PROPOSITION 5.3. *Let $\mathfrak{m}_0 = 2\mathcal{O}_{K_0}$ and $\mathfrak{m} = 2\mathcal{O}_K$ and $c(K)$ as in Corollary 5.1. Then the value of $c(K)$ is given by Table 1 according to the splitting of 2 in K_0 and K.*

TABLE 1. *Values for $c(K)$, where $h_2^-(K) = h^-(K)c(K)$.*

	$\mathfrak{p}_0$ inert	$\mathfrak{p}_0$ ramified	$\mathfrak{p}_0$ split (in K)
$2\mathcal{O}_{K_0} = \mathfrak{p}_0$	5	4	3
$2\mathcal{O}_{K_0} = \mathfrak{p}_0^2$	6	4	2
$2\mathcal{O}_{K_0} = \mathfrak{p}_0\mathfrak{p}_0'$	Both inert	Both ramified	Both split (in K)
	9	4	1
	1 inert, 1 ramified	1 inert, 1 split	1 ramified, 1 split (in K)
	6	3	2

Although $h_2^{\Phi^r} = |\mathrm{Cl}(K^r, \Phi^r, 2)|$ is not equal to $h_2^-(K)$, it is typically a factor of $h_2^-(K)$. One can show the following claim (up to a small 2-power factor) via careful analysis on various class groups and type norms: if we write the degree of the Igusa class polynomials as $c \cdot h^-(K)$, then the Rosenhain polynomials have degree which is a factor of $c \cdot h_2^-(K)2^r$. In other words, $h_2^{\Phi^r} \mid h_2^-(K)2^r$ for some small non-negative integer r. Therefore, the quotient of the degree of the Rosenhain polynomials by the degree of the Igusa class polynomials is a factor of $c(K)$ (up to a small 2-power factor). In Tables 2 and 3 below we give examples of all of these cases.

5.3. *Data for degrees of Rosenhain invariants*

Here we present some data for h^- and h_2^-, and compare it with the degree of minimal polynomials for the λs. We list examples according to the class number h of K, the splitting of 2 in $\mathcal{O}_K$, and the discriminants of the number fields $\mathbb{Q}(\lambda_i)$ generated by the λ_i. Note that in all cases, the maximum degree of the λ_i actually divides $4h_2^-$ as explained in §§ 4.2 and 5.2 above, but also that it can be significantly smaller.

The notation in Tables 2 and 3 is as follows. The CM fields are given by $K = \mathbb{Q}[x]/(x^4 + Ax^2 + B) = \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$ where $d = A^2 - 4B = n^2D$, $a = A/2$, and $b = n/2$.

In the tables, h denotes the class number of K, $h^- = h^-(K) = |\mathrm{Cl}(K)|/|\mathrm{Cl}(K_0)|$, and $h_2^-(K) = |C_{\mathfrak{m}}(K)|/|C_{\mathfrak{m}_0}(K_0)|$. Let $D(K) =$ discriminant of K, $D(K^r) =$ discriminant of K^r. Galois cyclic quartic fields are listed under the heading C_4, and non-Galois quartic fields are listed under the heading D_4. In Tables 2 and 3, the *degree* of λ_i refers to the degree of the minimal polynomial of λ_i, not the degree of the polynomials defined in (4.5). Question marks indicate that either the factorization or the LLL computation did not terminate yet.

Tables 2 and 3 contain examples for all possible splittings of the prime 2 in $\mathcal{O}_K$, exhibiting all possible values for $c(K)$ given in Proposition 1. There are some blocks where the splitting

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

TABLE 2. *Degrees of Rosenhain invariants.*

CM field	h^-, h_2^-	$\mathrm{disc}(K)$	$\mathrm{disc}(K^r)$	λ_i degrees	$\mathrm{disc}(\mathbb{Q}(\lambda_i))$		
A, B, D					λ_1	λ_2	λ_3
C_4	$h=1$	$(2)=p$					
5, 5, 5	1, 1	5^3	5^3	4, 4, 4	5^3	5^3	5^3
13, 13,13	1, 5	13^3	13^3	20, 20, 20	$2^{16}13^{15}$	$2^{16}13^{15}$	$2^{16}13^{15}$
29, 29, 29	1, 5	29^3	29^3	10, 10, 20	$2^8 29^7$	$2^8 29^7$	$2^{16}29^{15}$
37, 333, 37	1, 5	37^3	37^3	10, 20, 10	$2^8 37^7$	$2^{16}37^{15}$	$2^8 37^7$
53, 53, 53	1, 5	53^3	53^3	20, 20, 20	$2^{16}53^{15}$	$2^{16}53^{15}$	$2^{16}53^{15}$
61, 549, 61	1, 5	61^3	61^3	20, 20, 20	$2^{16}61^{15}$	$2^{16}61^{15}$	$2^{16}61^{15}$
C_4	$h=2$	$(2)=p$					
65, 845, 5	2, 10	$5^3 13^2$	$5^3 13^2$	20, 20, 20	$2^{16}5^{15}13^{10}$	$2^{16}5^{15}13^{10}$	$2^{16}5^{15}13^{10}$
85, 1445, 5	2, 10	$5^3 17^2$	$5^3 17^2$	20, 20, 20	$2^{16}5^{15}17^{10}$	$2^{16}5^{15}17^{10}$	$2^{16}5^{15}17^{10}$
65, 325, 13	2, 10	$5^2 13^3$	$5^2 13^3$	10, 10, 20	$2^8 5^4 13^7$	$2^8 5^4 13^7$	$2^{16}5^{10}13^{15}$
D_4	$h=1$	$(2)=p$					
17, 61, 5	1, 5	$5^2 61$	$5\cdot 61^2$	20, 20, 20	$2^{16}5^5 61^{10}$	$2^{16}5^5 61^{10}$	$2^{16}5^5 61^{10}$
21, 109, 5	1, 5	$5^2 109$	$5\cdot 109^2$	20, 20, 20	$2^{16}5^5 109^{10}$	$2^{16}5^5 109^{10}$	$2^{16}5^5 109^{10}$
26, 149, 5	1, 5	$5^2 149$	$5\cdot 149^2$	20, 10, 10	$2^{16}5^5 149^{10}$	$2^8 5^2 149^5$	$2^8 5^2 149^5$
34, 269, 5	1, 5	$5^2 269$	$5\cdot 269^2$	20, 10, 10	$2^{16}5^5 269^{10}$	$2^8 5^2 269^5$	$2^8 5^2 269^5$
41, 389, 5	1, 5	$5^2 389$	$5\cdot 389^2$	20, 20, 20	$2^{16}5^5 389^{10}$	$2^{16}5^5 389^{10}$	$2^{16}5^5 389^{10}$
18, 29, 13	1, 5	$13^2 29$	$13\cdot 29^2$	10, 20, 10	$2^8 13^2 29^5$	$2^{16}13^5 29^{10}$	$2^8 13^2 29^5$
D_4	$h=2$	$(2)=p$					
33, 261, 5	2, 10	$3^2 5^2 29$	$3^2\cdot 5\cdot 29^2$	20, 10, 10	$2^{16}3^{10}5^5 29^{10}$	$2^8 3^4 5^2 29^5$	$2^8 3^4 5^2 29^5$
66, 909, 5	2, 10	$3^2 5^2 101$	$3^2\cdot 5\cdot 101^2$	10, 20, 10	$2^8 3^4 5^2 101^5$	$2^{16}3^{10}5^5 101^{10}$	$2^8 3^4 5^2 101^5$
C_4	$h=2$	$(2)=p_1p_2$					
119, 3332, 17	2, 18	$7^2 17^3$	$7^2 17^3$	18, 18, ?	$2^{12}7^8 17^{13}$	$2^{12}7^8 17^{13}$	?
D_4	$h=1$	$(2)=p_1p_2$					
9, 17, 13	1, 3	$13^2\cdot 17$	$13\cdot 17^2$	12, 12, 6	$2^4 13^3 17^6$	$2^4 13^3 17^6$	$2^2\cdot 13\cdot 17^3$
13, 41, 5	1, 3	$5^2\cdot 41$	$5\cdot 41^2$	12, 6, 12	$2^4 5^3 41^6$	$2^2 5\cdot 41^3$	$2^4 5^3 41^6$
47, 548, 17	1, 9	$16^2\cdot 137$	$17\cdot 137^2$	18, 18, ?	?	?	?
D_4	$h=2$	$(2)=p_1p_2$					
25, 145, 5	2, 6	$5^3 29$	$5^3 29^2$	24, 24, 12	$2^8 5^{18} 29^{12}$	$2^8 5^{18} 29^{12}$	$2^4 5^8 29^6$
29, 209, 5	2, 6	$5^2\cdot 11\cdot 19$	$5\cdot 11^2 19^2$	12, 24, 24	$2^4 5^3 11^6 19^6$	$2^8 5^6 11^{12} 19^{12}$	$2^8 5^6 11^{12} 19^{12}$
17, 65, 29	2, 6	$5\cdot 13\cdot 29^2$	$5^2 13^2\cdot 29$	12, 24, 24	$2^4 5^6 13^6 29^2$	?	?
13, 33, 37	2, 6	$3\cdot 11\cdot 37^2$	$3^2 11^2\cdot 37$	12, 24, 24	$2^4 3^6 11^6 37^3$	?	?
D_4	$h=1$	$(2)=p_1p_2p_3$					
15, 52, 17	1, 3	$13\cdot 17^2$	$13^2\cdot 17$	12, 12, ?	$2^8 13^6 17^3$	$2^8 13^6 17^3$	?
11, 20, 41	1, 3	$5\cdot 41^2$	$5^2\cdot 41$	12, 12, 12	$2^8 5^6 41^3$	$2^8 5^6 41^3$	$2^8 5^6 41^3$
D_4	$h=2$	$(2)=p_1p_2p_3$					
26, 37, 33	2, 6	$3^2 11^2\cdot 37$	$3\cdot 11\cdot 33^2$	24, 24, 24	?	?	?
D_4	$h=7$	$(2)=p_1p_2p_3p_4$					
19, 68, 89	7, 7	$17\cdot 89^2$	$17^2\cdot 89$	28, 28, 28	$17^{14}89^7$	?	?

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

TABLE 3. *Degrees of Rosenhain invariants.*

CM field	h^-, h_2^-	$\mathrm{disc}(K)$	$\mathrm{disc}(K^r)$	λ_i degrees	$\mathrm{disc}(\mathbb{Q}(\lambda_i))$		
A, B, D					λ_1	λ_2	λ_3
C_4	$h=2$	$(2)=p^2$					
10, 20, 5	2, 8	$2^6 5^3$	$2^6 5^3$	2, 4, 4	5	$2^6 5^3$	$2^6 5^3$
26, 52, 13	2, 8	$2^6 13^3$	$2^6 13^3$	4, 4, 4	$2^6 13^3$	$2^6 13^3$	$2^6 13^3$
C_4	$h=4$	$(2)=p^2$					
15, 45, 5	4, 16	$2^4 3^2 5^3$	$2^4 3^2 5^3$	8, 8, 8	$2^8 3^4 5^6$	$2^8 3^4 5^6$	$2^8 3^4 5^6$
D_4	$h=1$	$(2)=p^2$					
22, 89, 8	1, 6	$2^6 \cdot 89$	$2^3 \cdot 89$	6, 12, ?	$2^5 89^3$	$2^{14} 89^6$	?
34, 281, 8	1, 6	$2^6 \cdot 281$	$2^3 \cdot 281$	12, 12, ?	$2^{14} 281^6$	$2^{14} 281^6$	?
D_4	$h=2$	$(2)=p^2$					
11, 29, 5	2, 8	$2^4 5^2 \cdot 29$	$2^4 \cdot 5 \cdot 29^2$	8, 8, 8	$2^8 5^2 29^4$	$2^8 5^2 29^4$	$2^8 5^2 29^4$
7, 5, 29	2, 8	$2^4 \cdot 5 \cdot 29^2$	$2^4 5^2 \cdot 29$	8, 8, 8	$2^8 5^4 29^2$	$2^8 5^4 29^2$	$2^8 5^4 29^2$
14, 44, 5	2, 8	$2^6 5^2 \cdot 11$	$2^8 \cdot 5 \cdot 11^2$	4, 4, 4	$2^8 \cdot 5 \cdot 11^2$	$2^8 \cdot 5 \cdot 11^2$	$2^8 \cdot 5 \cdot 11^2$
30, 177, 12	2, 12	$2^4 3^3 \cdot 59$	$2^2 3^3 59^2$	12, 24, 48	$2^{10} 3^9 59^6$	?	?
38, 329, 8	2, 12	$2^6 \cdot 7 \cdot 47$	$2^3 7^2 47^2$	12, 24, 24	$2^{13} 7^6 47^6$	?	?
D_4	$h=8$	$(2)=p^2$					
26, 145, 24	2, 12	$2^6 3^2 \cdot 529$	$2^3 \cdot 3 \cdot 5^2 29^2$	12, 24, ?	$2^{10} 3^2 5^6 29^6$	?	?
C_4	$h=1$	$(2)=p^4$					
4, 2, 2	1, 4	2^{11}	2^{11}	4, 2, 2	2^{11}	2^3	2^3
C_4	$h=2$	$(2)=p^4$					
12, 18, 8	2, 8	$2^{11} 3^2$	$2^{11} 3^2$	4, 4, 4	$2^{11} 3^2$	$2^{11} 3^2$	$2^{11} 3^2$
20, 50, 8	2, 8	$2^{11} 5^2$	$2^{11} 5^2$	4, 4, 4	$2^{11} 5^2$	$2^{11} 5^2$	$2^{11} 5^2$
14, 41, 8	2, 8	$2^8 \cdot 41$	$2^5 41^2$	16, 32, 32	$2^{24} 41^8$	?	?
D_4	$h=2$	$(2)=p^4$					
8, 13, 12	2, 8	$2^8 3^2 \cdot 13$	$2^6 \cdot 3 \cdot 13^2$	4, 8, 8	$2^6 13^2$	$2^{12} 3^2 13^4$	$2^{12} 3^2 13^4$
6, 6, 12	2, 8	$2^9 3^3$	$2^{10} 3^3$	4, 8, 8	$2^{10} 3^3$	$2^{22} 3^6$	$2^{22} 3^6$
D_4	$h=1$	$(2)=p_1^2 p_2^2$					
10, 17, 2	1, 2	$2^6 \cdot 17$	$2^3 17^2$	8, 8, 4	$2^8 17^4$	$2^8 17^4$	$2^2 17^2$
D_4	$h=2$	$(2)=p_1^2 p_2^2$					
18, 33, 12	2, 4	$2^4 3^3 \cdot 11$	$2^2 3^3 11^2$	16, 8, 8	$2^{12} 3^{12} 11^8$	$2^4 3^6 11^4$	$2^6 3^6 11^4$
D_4	$h=1$	$(2)=p_1^2 p_2 p_3$					
5, 2,17	1, 2	$2^3 17^2$	$2^6 \cdot 17$	8, 8, 2	$2^{16} 17^2$	$2^{16} 17^2$	2^2
D_4	$h=2$	$(2)=p_1^2 p_2 p_3$					
9, 12, 33	2, 4	$2^2 3^3 \cdot 11$	$2^4 3^3 \cdot 11$	8, 16, 16	$2^{12} 3^6 11^2$	$2^{24} 3^{12} 11^4$	$2^{24} 3^{12} 11^4$

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

is ambiguous in the tables. In the D_4-case $h = 1$ and $(2) = p_1p_2$, for the first two lines, (2) is inert, then split, whereas for the third line (2) is split, then inert. In the D_4-case $h = 2$ and $(2) = p^2$, for the first three lines (2) is inert and then ramified, and in the last two lines (2) is ramified and then inert.

6. *Experimental results and examples*

Comparing the formulas for Rosenhain invariants (2.1) with the formulas for Igusa invariants, in terms of the products of even theta constants, we can see directly from comparing the weights of the modular forms which appear in the numerators and denominators (weight 2 for Rosenhains, weight 60 at worst for Igusas) that the height of the Rosenhain invariants is likely to be much less, therefore requiring less precision to compute. The same is true for the Kummer invariants, where the required precision is often much smaller. Indeed, quotients of theta constants examined in [**33**] also are quotients of modular forms of low weight and they too have much smaller height and smaller coefficients than the Igusa polynomials. By the same argument given there [**33**, § 6.1], because the coefficients of the minimal polynomial are so much smaller, we need much less precision in order to recognize the minimal polynomial via LLL. This is one of the advantages of our approach: decreasing the amount of precision needed in computation.

On the other hand, the cost of our approach is that the Rosenhain and Kummer invariants lie in a potentially larger extension field, so they may have larger degree. As explained in § 4.2 above, the CM values of the λ functions lie in the extension $H(2)/K^r$ of the reflex field. Thus the degree of their minimal polynomials over $\mathbb{Q}$ is potentially as large as $4 \cdot \#\,\mathrm{Gal}(H(2)/K^r) = 4 \cdot h_2^{\Phi^r}$ or degree $h_2^{\Phi^r}$ over K^r. We find though, surprisingly, that often the CM λ-values satisfy minimal polynomials over $\mathbb{Q}$ with much smaller degree. We found cases, for example, where the Rosenhain and Igusa invariants satisfy minimal polynomials over $\mathbb{Q}$ of the same degree, as in the following example.

Example 1. The quartic CM field $K = \mathbb{Q}[x]/(x^4 + 14x^2 + 44)$ is non-Galois, with class number $h_K = 2$ and $K_0 = \mathbb{Q}(\sqrt{5})$. The Igusa class polynomials have degree 4 and coefficients with size up to 164 bits[†]. The Rosenhain invariants are found as roots of the polynomials

$$\begin{aligned}\lambda_1(x) &= 49x^4 + 1464x^3 - 1280x^2 + 64x + 64,\\ \lambda_2(x) &= 30625x^4 - 16400x^3 - 21736x^2 + 7616x + 16,\\ \lambda_3(x) &= 625x^4 + 183600x^3 - 173824x^2 + 32256x + 1024,\end{aligned} \tag{6.1}$$

where the coefficients are at most 18 bits. Both the Rosenhain and the Igusa invariants have degree 4 over $\mathbb{Q}$ in this case, but the Rosenhain invariants require less precision to recognize.

6.1. *Finding genus 2 curves and Kummer surfaces for cryptography*

To generate the examples we present in this work, we computed minimal polynomials over $\mathbb{Q}$ of both Rosenhain and Kummer CM-values for many different CM fields K with small class number. We then searched over many primes of a special form $p = 2^s - c$ or $p = 2^{s-1} - c$, pseudo-Mersenne primes for $s = 128, 192, 256$, which are advantageous for efficient implementations of curve-based cryptography. For each prime p, we checked all the CM fields K in our list, using the method described in § 3.1, to see if the number of points over $\mathbb{F}_p$ on the Jacobian of a curve with CM by K could be suitable for use in cryptography.

[†]See http://echidna.maths.usyd.edu.au/cgi-bin/dbs/igusa_cm_invariants.py?D=5&A=14&B=44&raw=0.

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

Our search was designed to return only those CM fields K and primes p where (i) $2^4 = 16$ divides the two matching curve-twist group orders[†], and (ii) when all small powers of 2 were removed from each such group order, the remaining factor was a large prime.

To continue with Example 1 above, the prime $p = 2^{127} - 28719$ splits into four principal ideals in $\mathcal{O}_K$. Two of the four possible group orders for $\mathcal{J}_{C_\lambda}(\mathbb{F}_p)$ are $N = 2^6 \cdot r$ and $N' = 2^4 \cdot r'$, where $r = 2^{248} + \hat{r}$ and $r' = 2^{250} - \hat{r}'$ are 249-and 250-bit primes, with

$$\hat{r} = 354366672761901834696101037004854409766246697073126749 45,$$
$$\hat{r}' = 141746669104761955446228299558628861917994511630039822125.$$

The minimal polynomials for the λ-invariants (6.1) all split completely in $\mathbb{F}_p[x]$. In this case there are two roots of $\lambda_1(x)$ that match up with roots of $\lambda_2(x)$ and $\lambda_3(x)$ to give rise to curves C_λ such that $\#\mathcal{J}_{C_\lambda}(\mathbb{F}_p) = N$ and $\#\mathcal{J}_{C'_\lambda}(\mathbb{F}_p) = N'$.

Another advantage of this approach is that the curve is given directly by the Rosenhain invariants in the form $C_\lambda \colon y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$. Note that when the Rosenhain model is defined over $\mathbb{F}_p$, with $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_p$, then all of the 2-torsion on the Jacobian of the curve is defined over $\mathbb{F}_p$, that is, $\#\mathcal{J}_{C_\lambda}(\mathbb{F}_p)[2] = 16$, because it is generated by the Weierstrass points on the curve.

6.2. *Splitting of Rosenhain polynomials modulo primes*

We can give a condition on primes which ensures that the Rosenhain polynomials split completely modulo those primes. It follows from class field theory that if a rational prime, p, splits completely in K^r into principal prime ideals with generators which are congruent to $1 \mod 2$, then the prime p will split completely in the ray class field of K^r modulo 2.

For example, for the field $K = \mathbb{Q}[x]/(x^4 + 13x^2 + 13)$, where $h_2(K) = 5$, the λ-polynomials have degree 20. There is only one prime less than 1000 for which that condition holds, $p = 757$, and the lambda polynomials split completely modulo 757:

$$\begin{aligned}
\lambda_1(x) &= x^{20} - 10x^{19} + 124x^{18} - 831x^{17} + 4509x^{16} - 18528x^{15} + 65066x^{14} - 190688x^{13} \\
&\quad + 368386x^{12} - 354722x^{11} + 20742x^{10} + 207694x^9 + 44631x^8 - 413118x^7 + 441258x^6 \\
&\quad - 234907x^5 + 72682x^4 - 13880x^3 + 1662x^2 - 71x + 1, \\
\lambda_2(x) &= x^{20} - 71x^{19} + 1662x^{18} - 13880x^{17} + 72682x^{16} - 234907x^{15} + 441258x^{14} \\
&\quad - 413118x^{13} + 44631x^{12} + 207694x^{11} + 20742x^{10} - 354722x^9 + 368386x^8 \\
&\quad - 190688x^7 + 65066x^6 - 18528x^5 + 4509x^4 - 831x^3 + 124x^2 - 10x + 1, \\
\lambda_3(x) &= x^{20} + 51x^{19} + 503x^{18} - 5035x^{17} + 27054x^{16} - 136825x^{15} + 499985x^{14} \\
&\quad - 1157943x^{13} + 1739480x^{12} - 1879141x^{11} + 1823741x^{10} - 1879141x^9 + 1739480x^8 \\
&\quad - 1157943x^7 + 499985x^6 - 136825x^5 + 27054x^4 - 5035x^3 + 503x^2 + 51x + 1.
\end{aligned}$$

6.3. *Existence of a Kummer surface over* $\mathbb{F}_p$

Another potential advantage of the Rosenhain approach is that, for a fixed CM field K, we can sometimes determine congruence conditions on the prime p which must hold in order to find a Kummer surface over $\mathbb{F}_p$ (arising as the quotient of a Jacobian variety with CM by K). When the minimal polynomials $\lambda_i(x)$ split completely in $\mathbb{F}_p$, then as just remarked, all of the

[†]Two-torsion is shared by a curve and its quadratic twist, so this is necessary, but not sufficient (cf. Example 2), to find a rational Kummer surface over $\mathbb{F}_p$.

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

2-torsion on the Jacobian of the curve is defined over $\mathbb{F}_p$. This is a necessary condition for the Kummer surface to be defined over $\mathbb{F}_p$. The following example illustrates this point.

EXAMPLE 2. The non-Galois quartic CM field $K = \mathbb{Q}[x]/(x^4 + 5x^2 + 2)$ has class number 1 with $K_0 = \mathbb{Q}(\sqrt{17})$. The prime $p = 2^{256} - 1204385$ splits into four principal ideals in $\mathcal{O}_K$, and there are two possible suitable group orders, $N = 2^6 \cdot r$ and $N' = 2^6 \cdot r'$, where $r = 2^{506} + \hat{r}$ and $r' = 2^{506} - \hat{r}'$ are the 507- and 506-bit primes given by

$$\hat{r} = 1042069017142527808074607196449149476090722442842106883749718550538937655101283257400133472983552933838816961141335,$$
$$\hat{r}' = 1042069017142527808074607196449161749125921965770655297925581003982254064511088864103924137074740555751503901721761.$$

In this example, the Igusa class polynomials have degree 2 and coefficients with size up to 28 bits[†]. Running Mestre's algorithm on triples of Igusa invariants (j_1, j_2, j_3) produces the curves with group orders N and N'. In both cases we soon find that the 2-torsion is not entirely defined over $\mathbb{F}_p$. While we cannot predict this from the Igusa class polynomials, it is readily apparent from the Rosenhain minimal polynomials:

$$\begin{aligned}\lambda_1(x) &= 1024x^8 - 4608x^7 + 10368x^6 - 15984x^5 + 18401x^4 - 15984x^3 + 10368x^2 \\ &\quad - 4608x + 1024,\\ \lambda_2(x) &= 4x^8 - 8x^7 + 8x^6 - 4x^5 + x^4 - 4x^3 + 8x^2 - 8x + 4,\\ \lambda_3(x) &= x^2 + 1.\end{aligned}$$

The third polynomial $\lambda_3(x)$ has roots in $\mathbb{F}_p[x]$ if and only if $p \equiv 1 \bmod 4$. Furthermore, we see (experimentally) that $\lambda_1(x)$ and $\lambda_2(x)$ only have roots in $\mathbb{F}_p[x]$ when $p \equiv 1 \bmod 8$. In some cases, the Rosenhain polynomials associated to certain CM fields can be used to derive analogous congruence conditions to rule out primes p where the entire 2-torsion is not defined over $\mathbb{F}_p$. This was mentioned in the specific case of $K = \mathbb{Q}(\zeta_5)$ in [6].

6.4. *Kummer surfaces for cryptography*

In both [6] and [4], record timings for scalar multiplications on Kummer surfaces were announced, competitive with Diffie–Hellman groups arising from elliptic curves. In [6, Tables 4 and 6], minimal polynomials for Kummer invariants were given for two CM fields (computed in a different way than in the present paper). In Table 4, the minimal polynomials for the parameters had very small roots in some cases, for example $y_0 = t_0 = 1$, which helps to speed up scalar multiplication on these surfaces. But the group orders for those CM fields were not suitable for cryptography over primes fields where the minimal polynomials split. Unfortunately we have not yet found other examples where the parameters for the Kummer surface and its arithmetic are as nice, but here are some examples where we computed the minimal polynomials for the Kummer surface parameters, and produced pairs (p, K) suitable for cryptography.

EXAMPLE 3. The quartic CM field $K = \mathbb{Q}[x]/(x^4 + 11x^2 + 29)$ is non-Galois, class number $h_K = 2$ and $K_0 = \mathbb{Q}(\sqrt{5})$. The minimal polynomials for the four Kummer surface constants in (2.2) are:

$$E'(x) = 625x^2 - 2169836x + 219395344, \quad F(x) = 625x^4 + 78016x^2 - 313600,$$
$$G(x) = x^4 + 7232x^2 - 20480, \quad H(x) = x^4 - 83x^2 + 845.$$

[†]See http://echidna.maths.usyd.edu.au/cgi-bin/dbs/igusa_cm_invariants.py?D=17&A=5&B=2&raw=0.

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

In this case, the Kummer polynomials have degree 2 or 4, while the Igusa class polynomials have degree 2 and coefficients of size up to 61 bits[†]. This time the Rosenhain polynomials have degree 8, and have coefficients whose size are at most 27 bits:

$$\begin{aligned}\lambda_1(x) &= 49x^8 - 3544x^7 - 315732x^6 + 4407944x^5 - 12245178x^4 + 16201976x^3 \\ &\quad - 11265364x^2 + 3379800x + 49, \\ \lambda_2(x) &= 256x^8 + 12032x^7 - 156096x^6 + 2945536x^5 - 7106976x^4 + 44710832x^3 \\ &\quad - 74749184x^2 + 34343600x + 30625, \\ \lambda_3(x) &= 49x^8 + 2918x^7 - 27147x^6 - 50376x^5 + 51502x^4 + 187134x^3 \\ &\quad - 236856x^2 + 72200x + 625. \end{aligned} \tag{6.2}$$

The prime $p = 2^{128} - 26567$ splits into four principal ideals in $\mathcal{O}_K$. Two possible group orders for $\mathcal{J}_{C_\lambda}(\mathbb{F}_p)$ are $N = 2^8 \cdot r$ and $N' = 2^4 \cdot r'$, where $r = 2^{248} + \hat{r}$ and $r' = 2^{252} - \hat{r}'$ are the 249- and 252-bit primes given by

$$\begin{aligned}\hat{r} &= 183775597520433761422100216220468044206485137281150339 93, \\ \hat{r}' &= 294040956032696278365589529217522617502604803983008251707.\end{aligned}$$

The polynomials in (6.2) all split completely in $\mathbb{F}_p[x]$. In this case we find four triples of roots which give rise to C_λ such that $\#\mathcal{J}_{C_\lambda}(\mathbb{F}_p) = N$ and $\#\mathcal{J}_{C'_\lambda}(\mathbb{F}_p) = N'$.

An associated Kummer surface is defined by the four roots

$$\begin{aligned}E' &= 191454713862007738160316578206844341556, \\ F &= 277186088880174207254108642006536815063, \\ G &= 851706630119819832144394062262280969 56, \\ H &= 144009629596880962160390585763815059845.\end{aligned}$$

Example 4. The quartic CM field $K = \mathbb{Q}[x]/(x^4 + 12x^2 + 18)$ is Galois cyclic, with class number $h_K = 2$ and $K_0 = \mathbb{Q}(\sqrt{2})$.

The Kummer surface constants that are needed for an implementation are: the four constants that define the surface in (2.2), which can be found as roots of the polynomials

$$\begin{aligned}E'(x) = 2401x^2 + 20915712x - 2341011456, \quad H(x) = x^2 + 28x - 92, \\ F(x) = G(x) = 2401x^8 + 1921232x^6 - 4039392x^4 - 87033088x^2 + 289272064,\end{aligned}$$

and the six Kummer constants from § 2.3 that are required in scalar multiplication routines, which can be found as roots of the six polynomials

$$\begin{aligned}y_0(x) &= 49x^4 + 2276x^3 - 4794x^2 + 2276x + 49, \\ z_0(x) &= 16x^8 + 7520x^6 - 18024x^4 + 8024x^2 + 2401, \\ t_0(x) &= 104976x^8 + 769824x^6 - 1511784x^4 + 621000x^2 + 2401, \\ y'_0(x) &= 9x^4 - 2508x^3 + 4214x^2 - 2508x + 9, \\ z'_0(x) &= 4x^8 - 608x^7 - 6240x^6 - 4688x^5 + 5092x^4 + 912x^3 - 5760x^2 - 2376x + 81, \\ t'_0(x) &= z'_0(-x).\end{aligned} \tag{6.3}$$

[†]See http://echidna.maths.usyd.edu.au/cgi-bin/dbs/igusa_cm_invariants.py?D=5&A=11&B=29&raw=0.

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

The defining polynomials have degree either 2, 4, or 8, whereas the Igusa class polynomials have degree 2 and coefficients with size up to 71 bits[†]. On the other hand, the Rosenhain polynomials are all of degree 4 and have coefficients whose size are at most 13 bits:

$$\begin{aligned}\lambda_1(x) &= 81x^4 + 216x^3 - 252x^2 - 240x + 196,\\ \lambda_2(x) &= x^4 - 44x^3 - 78x^2 + 268x + 49,\\ \lambda_3(x) &= 324x^4 + 3024x^3 + 180x^2 - 5880x + 2401.\end{aligned} \tag{6.4}$$

The prime $p = 2^{191} - 657687$ splits into four principal ideals in $\mathcal{O}_K$; two possible matching curve-twist group orders for $\mathcal{J}_{C_\lambda}(\mathbb{F}_p)$ are $N = 2^8 \cdot r$ and $N' = 2^4 \cdot r'$, where $r = 2^{374} - \hat{r}$ and $r' = 2^{378} + \hat{r}'$ are 374- and 379-bit primes with

$$\hat{r} = 16424313972654618704534890613377522188812216723938633865977034995495436135258091624 81.$$
$$\hat{r}' = 26278902356247389927255308936632476538381347724730421570962499591332201354672913898705.$$

Let $\tilde{\lambda}_1$ be any root of $\lambda_1(x)$. Here we can use the modified Lagrange interpolation [**16**, § 3] to rewrite the matching roots of $\lambda_2(x)$ and $\lambda_3(x)$ as functions of $\tilde{\lambda}_1$, given as

$$\tilde{\lambda}_2 = \frac{891\tilde{\lambda}_1^3 + 1620\tilde{\lambda}_1^2 - 4410\tilde{\lambda}_1 + 1896}{81\tilde{\lambda}_1^3 + 162\tilde{\lambda}_1^2 - 126\tilde{\lambda}_1 - 60}, \quad \tilde{\lambda}_3 = \frac{-189\tilde{\lambda}_1^3 + 63\tilde{\lambda}_1^2 + 126\tilde{\lambda}_1 - 98}{81\tilde{\lambda}_1^3 + 162\tilde{\lambda}_1^2 - 126\tilde{\lambda}_1 - 60}. \tag{6.5}$$

Using this representation, we only need to solve for roots $\tilde{\lambda}_1$ of $\lambda_1(x)$, from which we compute the matching $(\tilde{\lambda}_2, \tilde{\lambda}_3)$ pair directly from (6.5).

Over $\mathbb{F}_p$, a consistent set of the ten Kummer parameters are the following roots of the polynomials in (6.3):

$$\begin{aligned}E' &= 56702874506842682495927187055563543834564274774294839 9604,\\ F &= 23595635121758637236943942151462772976231221812484488 3233,\\ G &= 78438933438613125880991548664790570721563557962191063173,\\ H &= 25531411277075974978351938015083762845614170952681079457 56,\\ y_0 &= 45365629571161489877386664379507500802568387061984419563,\\ z_0 &= 29415381779346416821101637701203858739659508722025423112 27,\\ t_0 &= 99493243309726204151179128251660943449851851098188563364 9,\\ y_0' &= 27211237252939315475566507688526634059232514294802598093 80,\\ z_0' &= 73289427610812469881086822644635573981262730535806921748 8,\\ t_0' &= 18968417124325948743979232886128885735340728963532393452 04.\end{aligned}$$

6.5. *Table of examples*

In Table 4, we summarize the Rosenhain polynomials corresponding to eight different example CM fields; four are Galois and four are non-Galois. Four of the examples we have already explained and the details of the remaining four examples are provided in a more condensed form in the Appendix. These examples provide a list of cryptographic curves that are suitable for implementation at a range of security levels.

[†]See http://echidna.maths.usyd.edu.au/cgi-bin/dbs/igusa_cm_invariants.py?D=8&A=12&B=18&raw=0.

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

The notation in Table 4 is as follows. For each CM field $K = \mathbb{Q}[x]/(x^4 + Ax^2 + B)$ of class number h_K, we give the degree over $\mathbb{Q}$ (deg) and maximum bitlength over all coefficients (coeff) of the first Igusa class polynomial, $H_1(x)$, and over all coefficients of the three Rosenhain polynomials $\lambda_1(x)$, $\lambda_2(x)$ and $\lambda_3(x)$ corresponding to K. We only give the bitlength of $H_1(x)$ because $H_2(x)$ and $H_3(x)$ are not needed when using the representation proposed in [**16**, § 3]).

TABLE 4. *Summary of the Rosenhain polynomials for eight CM fields.*

Example	CM field					Igusa		Rosenhain		p		r, r'
#	A	B	D	h_K	Gal	deg	coeff	deg	coeff	(bits)	h, h'	(bits)
1	14	44	5	2	D_4	4	164	4	18	127	2^6, 2^4	249, 250
2	5	2	17	1	D_4	2	28	8	15	256	2^6, 2^6	507, 506
3	11	29	5	2	D_4	2	61	8	27	128	2^8, 2^4	249, 252
										191	2^8, 2^4	374, 379
4	12	18	2	2	C_4	2	71	4	13	191	2^4, 2^5	378, 378
										255	2^4, 2^5	507, 505
5	28	98	2	4	C_4	4	233	8	50	127	2^4, 2^5	251, 249
6	10	20	5	2	C_4	1	30	4	12	256	2^4, 2^4	509, 508
7	35	245	5	4	C_4	2	120	8	45	128	2^4, 2^4	253, 252
8	15	52	17	1	D_4	2	28	12	21	191	2^5, 2^5	378, 377

For each K, we also give a cryptographically strong, twist-secure curve C, whose Jacobian has CM by $\mathcal{O}_K$; the table reports the bitlengths of the underlying field characteristic p and the large prime factors r and r', as well as the curve-and-twist cofactors h and h', such that $\#\mathcal{J}_{C_\lambda}(\mathbb{F}_p) = hr$ and $\#\mathcal{J}_{C'_\lambda}(\mathbb{F}_p) = h'r'$.

Table 1 highlights the trend observed in the majority of examples we computed; namely, that the Rosenhain polynomials have coefficients which are much smaller than the coefficients of the Igusa class polynomials in most cases.

6.6. *Additional torsion*

For a curve C_λ with λ-invariants in $\mathbb{F}_p$, $\#\mathcal{J}_{C_\lambda}(\mathbb{F}_p)[2] = 2^4$, so if a higher power of 2 divides the group order $\#\mathcal{J}_{C_\lambda}(\mathbb{F}_p)$, then there must be some additional 2-power torsion. In Table 4 where all curves have $\mathbb{F}_p$-rational λ-invariants, only the curves in Examples 6 and 7 have no higher 2-power torsion.

When there is at least one additional small-torsion point on $\mathcal{J}_{C_\lambda}$ or $\mathcal{J}_{C'_\lambda}$, then the technique from [**23**] (see also D. Robert, private communication, December 2013) allows for 'compatible' additions on the Kummer surface $\mathcal{K}$. So in some cases, it may be worthwhile to allow an extra factor of 2 in the cofactor in order to take advantage of this technique.

Here we give an additional example with this feature which could be useful in cryptography. Continuing with the CM field from Example 4 above, the quartic CM field $K = \mathbb{Q}[x]/(x^4 + 12x^2 + 18)$ has class number $h_K = 2$ and $K_0 = \mathbb{Q}(\sqrt{2})$. We can give another example over this CM field with only one extra 2 in the cofactor. The prime $p = 2^{191} - 830439$ splits into 4 principal ideals in $\mathcal{O}_K$. Two possible group orders for Jacobians of curves C with CM by K are $N = 2^4 \cdot r$ and $N' = 2^5 \cdot r'$, where $r = 2^{378} - \hat{r}$ and $r' = 2^{377} + \hat{r}'$ are 378-bit primes with

$$\hat{r} = 27145707237528389726742606066121237906741397221275189669901645158791934103076877051777,$$

$$\hat{r}' = 13572853618764194863370977236789991112677548782757889556987587506326996397536581679559.$$

The first Rosenhain polynomial, $\lambda_1(x)$ in (6.4), splits completely in $\mathbb{F}_p[x]$. Substituting any one of its roots, $\tilde{\lambda}_1$, into (6.5) gives a triple $(\tilde{\lambda}_1, \tilde{\lambda}_2, \tilde{\lambda}_3)$ with $\#\mathcal{J}_{C_\lambda}(\mathbb{F}_p) = N$ and $\#\mathcal{J}_{C'_\lambda}(\mathbb{F}_p) = N'$.

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

Appendix. *More examples*

Here we provide, in condensed form, the other examples constituting Table 4. We only include the Rosenhain polynomials corresponding to each field K, and the strong curve-twist group orders N and N' corresponding to the specific prime p. If required, a correct combination of roots of the Rosenhain polynomials giving a model for C_λ can readily be found by testing each such combination against N and N', until a random divisor on $\mathcal{J}_{C_\lambda}$ or $\mathcal{J}_{C'_\lambda}$ is annihilated by N or N'. However, just as we did in Example 4, in the first example below we use the modified Lagrange interpolation [**16**, § 3] to avoid the need for any such testing.

Example 5. The quartic CM field $K = \mathbb{Q}[x]/(x^4 + 28x^2 + 98)$ has class number $h_K = 4$ and $K_0 = \mathbb{Q}(\sqrt{2})$. The Igusa class polynomials have degree 4 with coefficients of size up to 233 bits[†]. The Rosenhain invariants are found as roots of polynomials of degree 8 with coefficients of at most 50 bits. The first one, $\lambda_1(x)$, is

$$\begin{aligned}\lambda_1(x) = {} & 5096960449x^8 - 59943031251208x^7 + 370565801837364x^6 - 829064790892296x^5 \\ & + 864603976223110x^4 - 431439809757432x^3 + 92337255217908x^2 \\ & - 7241766843640x + 177302471329.\end{aligned}$$

Using the method in [**16**, § 3], we compute *the* corresponding Rosenhain invariants as $\tilde{\lambda}_i = (8/2122849)\tilde{\lambda}_i(\tilde{\lambda}_1)/\lambda'_1(\tilde{\lambda}_1)$ for $i = 2, 3$, where $\lambda'_1(x)$ is the derivative of $\lambda_1(x)$ above, and where

$$\begin{aligned}\tilde{\lambda}_2(\tilde{\lambda}_1) = {} & 6966080649859723\tilde{\lambda}_1^7 - 666561929379227076 16\tilde{\lambda}_1^6 + 321114020620982081059\tilde{\lambda}_1^5 \\ & - 523984877182732532190\tilde{\lambda}_1^4 + 356618367465929440173\tilde{\lambda}_1^3 \\ & - 955136558889475943 64\tilde{\lambda}_1^2 + 867056405060585306 1\tilde{\lambda}_1 - 244711480729669774, \\ \tilde{\lambda}_3(\tilde{\lambda}_1) = {} & 5381839762415508\tilde{\lambda}_1^7 - 608998888037314522 58\tilde{\lambda}_1^6 + 290876333336198374072\tilde{\lambda}_1^5 \\ & - 471585316360537736770\tilde{\lambda}_1^4 + 318626409958501535956\tilde{\lambda}_1^3 \\ & - 841042020560445268 62\tilde{\lambda}_1^2 + 728163671114465467 2\tilde{\lambda}_1 - 189571447740024142.\end{aligned}$$

The prime $p = 2^{127} - 373359$ splits into four principal ideals in $\mathcal{O}_K$. Two of the possible group orders for $\#\mathcal{J}_{C_\lambda}(\mathbb{F}_p)$ for curves C_λ with CM by K are $N = 2^4 \cdot r$ and $N' = 2^5 \cdot r'$, where $r = 2^{250} + \hat{r}$ and $r' = 2^{249} - \hat{r}'$ are 251- and 249-bit primes with

$$\begin{aligned}\hat{r} &= 526579428781408080357551267616694433684827725164791989679, \\ \hat{r}' &= 263289714390711980587065256830062076214183259931934080913.\end{aligned}$$

The polynomial $\lambda_1(x)$ (given above) splits completely in $\mathbb{F}_p[x]$: substituting any one of its roots into the computation of $\tilde{\lambda}_2$ and $\tilde{\lambda}_3$ defined above gives rise to a Rosenhain triple such that $\#\mathcal{J}_{C_\lambda}(\mathbb{F}_p) = N$. For such a C_λ, it follows that the Jacobian of the twist, $\mathcal{J}_{C'_\lambda}(\mathbb{F}_p)$, has points of exact order 4, in addition to all 2-torsion rational.

Example 6. The quartic CM field $K = \mathbb{Q}/(x^4 + 10x^2 + 20)$ has class number $h_K = 2$ and $K_0 = \mathbb{Q}(\sqrt{5})$. This is one of van Wamelen's examples [**35**] of a CM field where the Igusa invariants[‡] are defined over $\mathbb{Q}$. The Rosenhain invariants are found as roots of the polynomials

$$\begin{aligned}\lambda_1(x) &= x^2 + 16x - 16, \\ \lambda_2(x) &= x^4 + 204x^3 + 2996x^2 - 3216x + 16, \\ \lambda_3(x) &= x^4 + 28x^3 + 4x^2 - 48x + 16. \end{aligned} \tag{A.1}$$

[†]See http://echidna.maths.usyd.edu.au/cgi-bin/dbs/igusa_cm_invariants.py?D=8&A=28&B=98&raw=0.

[‡]See http://echidna.maths.usyd.edu.au/cgi-bin/dbs/igusa_cm_invariants.py?D=5&A=10&B=20&raw=0.

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

The prime $p = 2^{256} - 1405067$ splits into 4 principal ideals in $\mathcal{O}_K$. There are two possible group orders for $\#\mathcal{J}_{C_\lambda}(\mathbb{F}_p)$ for curves C_λ with CM by K, given by are $N = 2^4 \cdot r$ and $N' = 2^4 \cdot r'$, where $r = 2^{508} + \hat{r}$ and $r' = 2^{508} - \hat{r}'$ are 509- and 508-bit primes, with $(\hat{r}, \hat{r}') =$

(3266146279590289616697288326643692977601759703506301403850455649701823577098001741197488639944233682641571217767825,
3266146279590289616697288326643733651499461058469703245103446399072893914517667448420904219450927907469641194338455).

The three Rosenhain polynomials in (A.1) split completely in $\mathbb{F}_p[x]$. For each of the two roots of $\lambda_1(x)$, precisely one root of $\lambda_2(x)$ and one root of $\lambda_3(x)$ gives rise to $\#\mathcal{J}_{C_\lambda}(\mathbb{F}_p) = N$ and $\#\mathcal{J}_{C'_\lambda}(\mathbb{F}_p) = N'$. This time, only the 2-torsion is $\mathbb{F}_p$-rational on both $\mathcal{J}_{C_\lambda}$ and $\mathcal{J}_{C'_\lambda}$.

Example 7. The quartic CM field $K = \mathbb{Q}/(x^4 + 35x^2 + 245)$ has class number $h_K = 4$ and $K_0 = \mathbb{Q}(\sqrt{5})$. The Igusa class polynomials have degree 2 with coefficients of size up to 120 bits[†]. The Rosenhain invariants are roots of the polynomials

$$\begin{aligned}
\lambda_1(x) &= 1698181681x^8 - 2332899512272x^7 + 5239365733308x^6 - 6861052011534x^5 \\
&\quad + 8127472357390x^4 - 13335162018684x^3 + 11133611696793x^2 \\
&\quad - 1973034426682x + 73805281, \\
\lambda_2(x) &= 1698181681x^8 + 2319314058824x^7 - 11043381765528x^6 + 24320649195262x^5 \\
&\quad - 29119911912510x^4 + 26204862793688x^3 - 19070415001283x^2 \\
&\quad + 6387184449866x + 73805281, \\
\lambda_3(x) &= 38416x^4 - 76832x^3 + 73304x^2 - 34888x + 5041,
\end{aligned} \tag{A.2}$$

where the coefficients are at most 45 bits.

The prime $p = 2^{128} - 1141887$ splits into four principal ideals in $\mathcal{O}_K$. Two possible curve-twist group orders for Jacobians with CM by K are $N = 2^4 \cdot r$ and $N' = 2^4 \cdot r'$, where $r = 2^{252} + \hat{r}$ and $r' = 2^{252} - \hat{r}'$ are 253- and 252-bit primes with

$$\begin{aligned}
\hat{r} &= 1126141268554063392138629773840371490317149533762468204 45, \\
\hat{r}' &= 1126141268555034802437172545174476916989535737441379985 35.
\end{aligned}$$

The Rosenhain polynomials in (A.2) all completely split in $\mathbb{F}_p[x]$, and there are four triples (found as roots) that give rise to $\#\mathcal{J}_{C_\lambda}(\mathbb{F}_p) = N$ and $\#\mathcal{J}_{C'_\lambda}(\mathbb{F}_p) = N'$.

Example 8. The quartic CM field $K = \mathbb{Q}[x]/(x^4 + 15x^2 + 52)$ has class number $h_K = 1$ and $K_0 = \mathbb{Q}(\sqrt{17})$. The Igusa class polynomials have degree 2 and coefficients of size up to 28 bits[‡]. The Rosenhain invariants are roots of the polynomials

$$\begin{aligned}
\lambda_1(x) &= 81x^{12} - 90x^{11} - 263x^{10} - 798x^9 + 6958x^8 - 15118x^7 \\
&\quad + 16985x^6 - 14710x^5 + 13186x^4 - 9442x^3 + 4093x^2 - 882x + 81, \\
\lambda_2(x) &= 81x^{12} - 2205x^{11} + 55216x^{10} - 199545x^9 + 359972x^8 - 662901x^7 \\
&\quad + 1163639x^6 - 1123328x^5 + 373568x^4 - 1280x^3 + 200704x^2 - 229376x + 65536, \\
\lambda_3(x) &= x^6 + 3x^5 - 9x^3 + 4x^2 + 11x - 9
\end{aligned} \tag{A.3}$$

where the coefficients are at most 21 bits.

The prime $p = 2^{191} - 4657$ is inert in $\mathcal{O}_{K_0}$ but splits into two principal ideals in $\mathcal{O}_K$. The two possible group orders for $\mathcal{J}_{C_\lambda}(\mathbb{F}_p)$ are $N = 2^5 \cdot r$ and $N' = 2^5 \cdot r'$, where $r = 2^{377} + \hat{r}$

[†]See http://echidna.maths.usyd.edu.au/cgi-bin/dbs/igusa_cm_invariants.py?D=5&A=35&B=245&raw=0.

[‡]See http://echidna.maths.usyd.edu.au/cgi-bin/dbs/igusa_cm_invariants.py?D=17&A=15&B=52&raw=0.

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press

and $r' = 2^{377} - \hat{r}'$ are 378- and 377-bit primes given by

$$\hat{r} = 138149640078182969295626581723827868171125113021541948407388890148863393900731383774 57,$$
$$\hat{r}' = 138149640078182969295626599987291907995203231833401962649049505220766923150017495685 95.$$

The polynomials $\lambda_1(x)$ and $\lambda_2(x)$ in (A.3) both have six roots in $\mathbb{F}_p$, while $\lambda_3(x)$ has four. There are three triples (of these roots) such that $\#\mathcal{J}_{C_\lambda}(\mathbb{F}_p) = N$ and $\#\mathcal{J}_{C'_\lambda}(\mathbb{F}_p) = N'$.

References

1. A. O. L. Atkin and F. Morain, 'Elliptic curves and primality proving', *Math. Comp.* 61 (1993) no. 203, 29–68.
2. D. J. Bernstein, 'A software implementation of NIST P-224', *Talk at ECC*, October 2001.
3. D. J. Bernstein, 'Elliptic vs. hyperelliptic, part I', *Talk at ECC*, September 2006.
4. D. J. Bernstein, C. Chuengsatiansup, T. Lange and P. Schwabe, 'Kummer strikes back: new DH speed records', http://cr.yp.to/papers.html#kummer.
5. D. J. Bernstein and T. Lange, 'Faster addition and doubling on elliptic curves', *Advances in cryptology – ASIACRYPT 2007*, Lecture Notes in Computer Science 4833 (ed. K. Kurosawa; Springer, 2007) 29–50.
6. J. W. Bos, C. Costello, H. Hisil and K. Lauter, 'Fast cryptography in genus 2', *Advances in cryptology – EUROCRYPT 2013*, Lecture Notes in Computer Science 7881 (eds T. Johansson and P. Q. Nguyen; Springer, 2013) 194–210. Full version: http://eprint.iacr.org/2012/670.
7. R. Broker, D. Gruenewald and K. Lauter, 'Explicit CM-theory for level 2-structures on abelian surfaces', *Algebra Number Theory* 5 (2011) no. 4, 495–528.
8. J. H. Bruinier, S. S. Kudla and T. Yang, 'Special values of Green functions at big CM points', *Int. Math. Res. Not. IMRN* 2012 (2012) no. 9, 1917–1967.
9. G. Cardona and J. Quer, 'Field of moduli and field of definition for curves of genus 2', *Computational aspects of algebraic curves*, Lecture Notes Series on Computing 13 (World Scientific, Hackensack, NJ, 2005) 71–83.
10. D. Chudnovsky and G. V. Chudnovsky, 'Sequences of numbers generated by addition in formal groups and new primality and factorization tests', *Adv. Appl. Math.* 7 (1986) no. 4, 385–434.
11. R. Cosset, 'Factorization with genus 2 curves', *Math. Comp.* 79 (2010) no. 270, 1191–1208.
12. H. Edwards, 'A normal form for elliptic curves', *Bull. Amer. Math. Soc.* 44 (2007) no. 3, 393–422.
13. K. Eisentraeger and K. Lauter, 'A CRT algorithm for constructing genus 2 curves over finite fields', *Arithmetic, geometry, and coding theory (AGCT 2005)*, Séminaires et Congrès 21 (eds F. Rodier and S. Vladut; Societe Mathematique de France, 2011) 161–176.
14. A. Enge and E. Thomé, 'Computing class polynomials for abelian surfaces', *Experiment. Math.*, to appear, http://eprint.iacr.org/2013/299.
15. P. Gaudry, 'Fast genus 2 arithmetic based on theta functions', *J. Math. Cryptology* 1 (2007) no. 3, 243–265.
16. P. Gaudry, T. Houtmann, D. R. Kohel, C. Ritzenthaler and A. Weng, 'The 2-adic CM method for genus 2 curves with application to cryptography', *Advances in cryptology – ASIACRYPT 2006*, Lecture Notes in Computer Science 4284 (eds X. Lai and K. Chen; Springer, 2006) 114–129.
17. P. Gaudry and E. Schost, 'Genus 2 point counting over prime fields', *J. Symbolic Comput.* 47 (2012) no. 4, 368–400.
18. E. Z. Goren and K. E. Lauter, 'Genus 2 curves with complex multiplication', *Int. Math. Res. Not. IMRN* 2012 (2012) no. 5, 1068–1142.
19. D. Gruenewald, 'Computing Humbert surfaces and applications', *Arithmetic, geometry, cryptography and coding theory 2009* (American Mathematical Society, Providence, RI, 2010) 59–69.
20. J. Igusa, 'On Siegel modular forms of genus two', *Amer. J. Math.* (1962) 175–200.
21. K. Lauter and B. Viray, 'An arithmetic intersection formula for denominators of Igusa class polynomials', Preprint, 2012, arXiv:1210.7841.
22. A. K. Lenstra, H. W. Lenstra and L. Lovász, 'Factoring polynomials with rational coefficients', *Math. Ann.* 261 (1982) no. 4, 515–534.
23. D. Lubicz and D. Robert, 'A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties', Cryptology ePrint Archive, Report 2013/192, 2013, http://eprint.iacr.org/.
24. J. Mestre, 'Construction de courbes de genre 2 à partir de leurs modules', *Effective methods in algebraic geometry*, Progress in Mathematics 94 (Birkhäuser, Boston, MA, 1991) 313–334.
25. J. S. Milne, 'Class field theory (v4.02)', 2013, available at www.jmilne.org/math/.
26. P. L. Montgomery, 'Speeding the Pollard and elliptic curve methods of factorization', *Math. Comp.* 48 (1987) no. 177, 243–264.

27. J. Pila, 'Frobenius maps of abelian varieties and finding roots of unity in finite fields', *Math. Comp.* 55 (1990) no. 192, 745–763.
28. R. Schoof, 'Elliptic curves over finite fields and the computation of square roots mod p', *Math. Comp.* 44 (1985) no. 170, 483–494.
29. G. Shimura, *Introduction to the arithmetic theory of automorphic functions,* vol. 1 (Princeton University Press, Princeton, NJ, 1971).
30. G. Shimura, *Abelian varieties with complex multiplication and modular functions,* vol. 46 (Princeton University Press, Princeton, NJ, 1998).
31. A. Spallek, 'Kurven vom Geschlecht 2 und ihre Anwendung in public-key-Kryptosystemen', PhD Thesis, Inst. für Experimentelle Mathematik, 1994.
32. M. Streng, 'Complex multiplication of abelian surfaces', PhD Thesis, Leiden University, June 2010, https://openaccess.leidenuniv.nl/handle/1887/15572.
33. M. Streng, 'An explicit version of Shimura's reciprocity law for Siegel modular functions', *CoRR*, 2012, arXiv:abs/1201.0020.
34. P. van Wamelen, 'Equations for the Jacobian of a hyperelliptic curve', *Trans. Amer. Math. Soc.* 350 (1998) no. 8, 3083–3106.
35. P. van Wamelen, 'Examples of genus two CM curves defined over the rationals', *Math. Comp.* 68 (1999) no. 225, 307–320.
36. A. Weng, 'Constructing hyperelliptic curves of genus 2 suitable for cryptography', *Math. Comp.* 72 (2003) no. 241, 435–458.
37. T. Yang, 'Arithmetic intersection on a Hilbert modular surface and the Faltings height', *Asian J. Math.* 17 (2013) no. 2, 335–382.
38. T. Yang, 'Rational structure of $X(N)$ over $\mathbb{Q}$ and explicit Galois action on CM points', Preprint, 2014.

Craig Costello
Microsoft Research
One Microsoft Way
Redmond, WA 98052
USA
craigco@microsoft.com

Alyson Deines-Schartz
Department of Mathematics
University of Washington
Seattle, WA 98195
USA
aly.deines@gmail.com

Kristin Lauter
Microsoft Research
One Microsoft Way
Redmond, WA 98052
USA
klauter@microsoft.com

Tonghai Yang
Department of Mathematics
University of Wisconsin
Madison, WI 53706
USA
thyang@math.wisc.edu

https://doi.org/10.1112/S1461157014000370 Published online by Cambridge University Press