CM construction of genus 2 curves with p-rank 1

Laura Hitt O'Connor[1⋆], Gary McGuire[1⋆⋆], Michael Naehrig[2], and Marco Streng[3]

[1] School of Mathematical Sciences,
University College Dublin, Ireland,
{laura.hitt, gary.mcguire}@ucd.ie

[2] Department of Mathematics and Computer Science,
Technical University Eindhoven, the Netherlands,
m.naehrig@tue.nl

[3] Mathematisch Instituut,
Universiteit Leiden, the Netherlands,
streng@math.leidenuniv.nl

Abstract. We present an algorithm for constructing cryptographic hyperelliptic curves of genus 2 and p-rank 1, using the CM method. We also present an algorithm for constructing such curves that, in addition, have a prescribed small embedding degree. We describe the algorithms in detail, and discuss other aspects of p-rank 1 curves too, including the reduction of the class polynomials modulo p.

1 Introduction

An important class of problems in computational number theory is to find techniques for constructing explicit algebraic curves with certain specified properties. Solutions to such problems have applications in cryptography and primality proving. Elliptic curves with specified properties can be constructed using the complex multiplication (CM) method, first outlined by Atkin and Morain [1]. The CM method has been extended to ordinary hyperelliptic curves of genus 2, by Spallek [19] and others. Using the CM method, we present here the first construction of genus 2 curves with p-rank 1. In particular, we construct curves whose Jacobian group order is of cryptographic size.

The layout of this paper is as follows. In Section 2 we give the background for the paper. This section includes a review of endomorphism rings, and discusses genus 2 curves, and those having p-rank 1, in particular. Section 2 also discusses cryptographic applications. Section 3 presents our algorithms for constructing p-rank 1 curves with the property that the Jacobian has prime order. That section also gives an algorithm (based on the algorithm proposed by Freeman, Stevenhagen and Streng in [5]) that constructs p-rank 1 curves with a prescribed

⋆ Research supported by Science Foundation Ireland Post-Doctoral Grant 07/RFP/ENM123

⋆⋆ Research supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006

embedding degree. Section 4 provides an overview of the CM method, which occurs as the final step of our algorithms. In Section 5 we apply basic class field theory to explain the behaviour of the class polynomials modulo p, which is relevant to a particular speedup of the CM method. With precomputed class polynomials, we computed examples using Magma in less than 10 seconds on an Intel Core 2 Duo. The details are given in an appendix.

2 Background

In this section we present a summary of the background needed for this paper. Throughout, p will denote a prime in $\mathbb{Z}$ and q will be a power of p. We use k to denote the finite field $\mathbb{F}_q$ with q elements, and we fix an algebraic closure $\overline{k}$ of k.

Whenever we talk about curves, we mean smooth projective geometrically irreducible curves over a field. Any curve C has an associated abelian variety, called the *Jacobian of* C and denoted J_C. The dimension of the Jacobian is the genus of the curve. The abelian varieties in this paper will be Jacobians of genus 2 curves, but for the moment we state some known results for arbitrary abelian varieties. Every principally polarized 2-dimensional abelian variety over a perfect field is either the Jacobian of some genus 2 curve or becomes isomorphic to a product of two elliptic curves with the product polarization over a field extension of degree at most 2.

Given an abelian variety A defined over k, the *p-rank* of A is defined by

$$r_p(A) = \dim_{\mathbb{F}_p} A(\overline{k})[p],$$

where $A(\overline{k})[p]$ is the subgroup of p-torsion points over the algebraic closure. We have $0 \leq r_p(A) \leq \dim(A)$. The number $r_p(A)$ is invariant under isogenies over $\overline{k}$, and satisfies $r_p(A \times A') = r_p(A) + r_p(A')$. An abelian variety defined over k is called *k-simple* if it is not k-isogenous to a product of abelian varieties of smaller dimensions. The term *absolutely simple* means $\overline{k}$-simple.

An elliptic curve over k is called ordinary if its p-rank is 1, and is called supersingular if its p-rank is 0. An abelian variety A of dimension g over k is called *ordinary* if its p-rank is g and *supersingular* if it is $\overline{k}$-isogenous to a power of a supersingular elliptic curve.

A supersingular abelian variety has p-rank 0. If $g \leq 2$, then the converse also holds [16]. For genus $g > 2$, there are several intermediate types, but for $g = 2$, the only intermediate type between supersingular and ordinary is the case where the p-rank is equal to 1. This intermediate case is the topic of this paper.

2.1 Zeta functions, Weil q-numbers

The *zeta function* $Z_C(T)$ of a smooth projective curve C over $k = \mathbb{F}_q$ is defined by

$$Z_C(T) = \exp\left(\sum_{m \geq 1} N_m \frac{T^m}{m}\right),$$

where N_m is the number of $\mathbb{F}_{q^m}$-rational points on C. The zeta function was first defined by E. Artin and F. K. Schmidt, who proved that the zeta function (of a curve) is a rational function in T of the form

$$\frac{P(T)}{(1-T)(1-qT)}$$

where $P(T)$ is a polynomial of degree $2g$ with rational coefficients, and g is the genus of the curve. Schmidt also proved a functional equation for the zeta function, from which it follows that if α is a root of $P(T)$, so is α/q. The Riemann Hypothesis for curves over finite fields (proven by Weil) states that the roots of the numerator have absolute value $q^{-1/2}$.

For genus 2 curves, these facts imply that $P(T)$ has the form

$$P(T) = 1 + a_1T + a_2T^2 + qa_1T^3 + q^2T^4$$

for some integers a_1, a_2. These integers are related to N_1, N_2 by $N_1 = q+1+a_1$, $N_2 = q^2 + 1 - a_1^2 + 2a_2$.

For any abelian variety A, the characteristic polynomial of the Frobenius endomorphism (acting on the ℓ-adic Tate module of A), will be denoted $f_A(t)$. It is independent of ℓ and has coefficients in $\mathbb{Z}$. If $A = J_C$ for a curve C, then it was shown by Weil that $f_A(t)$ is the reciprocal polynomial of the numerator $P(T)$ of the zeta function of C. For genus 2 curves, then,

$$f_{J_C}(t) = t^4 + a_1t^3 + a_2t^2 + qa_1t + q^2.$$

An algebraic integer π is called a *Weil q-number* if its image under every complex embedding of $\mathbb{Q}(\pi)$ has absolute value $\sqrt{q}$. The minimal polynomial over $\mathbb{Q}$ of a Weil q-number is thus a candidate for being f_A for some A. We say that a polynomial f is a *Weil q-polynomial* if $f = f_A$ for some abelian variety A defined over $\mathbb{F}_q$. Honda showed that every Weil q-number is a root of some Weil q-polynomial, see [22]. Tate showed that two abelian varieties are $\mathbb{F}_q$-isogenous if and only if their associated Weil q-polynomials (characteristic polynomials of Frobenius) are equal.

The following theorem summarizes the results of Rück [17] and Maisner and Nart [13], which gives conditions on a_1, a_2 for a hyperelliptic genus 2 curve C to have p-rank 1.

Theorem 1. *Let $q = p^n$ for a prime p and positive integer n. Let $f(t) = t^4 + a_1t^3 + a_2t^2 + qa_1t + q^2 \in \mathbb{Z}[t]$ and let $\Delta = a_1^2 - 4a_2 + 8q$, $\delta = (a_2 + 2q)^2 - 4qa_1^2$. Then, $f(t)$ is the characteristic polynomial of a simple p-rank 1 Jacobian of a projective smooth curve of genus 2 defined over $\mathbb{F}_q$ if and only if*

i) $|a_1| < 4\sqrt{q}$,
ii) $2|a_1|\sqrt{q} - 2q < a_2 < a_1^2/4 + 2q$,
iii) *Δ is not a square in $\mathbb{Z}$,*
iv) $v_p(a_1) = 0$,
v) $v_p(a_2) \geq n/2$,

vi) δ is not a square in the p-adic integers.

Proof. The first three conditions are equivalent to $f(t)$ being an irreducible Weil q-polynomial, see [13, Lemma 2.1, Lemma 2.4] and [17, Lemma 3.1]. This implies that A is simple. Conversely, note that for a simple abelian variety, by Theorem 2 below we have $f_A(t) = m_A(t)^e$ for some monic irreducible polynomial $m_A(t)$. The number e must divide the p-rank of A [8, Prop. 3.2]. Thus for a simple abelian variety with p-rank 1 the characteristic polynomial of Frobenius f_A is always irreducible. The last three conditions are then equivalent to having p-rank 1, see [13, Theorem 2.9] □

2.2 Endomorphisms

For any field $l \supset k$, let $\mathrm{End}_l(A)$ denote the *ring of endomorphisms* of A that are defined over l. Let

$$\mathrm{End}_l^0(A) := \mathbb{Q} \otimes \mathrm{End}_l(A).$$

If A is $\overline{k}$-isogenous to $\prod A_i^{n_i}$, where the A_i are pairwise non-isogenous, then $\mathrm{End}_{\overline{k}}^0(A) \cong \oplus M_{n_i}(\mathrm{End}_{\overline{k}}^0(A_i))$. Here is an important result on the endomorphism ring $\mathrm{End}_k^0(A)$.

Theorem 2 ([24]). *Let A be a simple abelian variety over the field k with q elements. Then there exists an integer e such that*

1. *$f_A(t) = m(t)^e$ for some irreducible monic polynomial $m(t) \in \mathbb{Z}[t]$,*
2. *$\mathrm{End}_k^0(A)$ is a division algebra with center $K = \mathbb{Q}(\pi)$,*
3. *$[\mathrm{End}_k^0(A) : \mathbb{Q}] = e^2[K : \mathbb{Q}]$, and $2\ \dim A = e[K : \mathbb{Q}]$.*

In Section 2.4 we detail the implications of this result for genus 2 curves.

2.3 Complex multiplication

A *CM field* is a totally imaginary quadratic extension of a totally real algebraic number field of finite degree. In particular, a field K is a *quartic CM field* if K is an imaginary quadratic extension of a totally real field K_0 of degree 2 over $\mathbb{Q}$.

Definition 3. *Let C be a curve of genus 2 defined over $k = \mathbb{F}_q$, and let K be a quartic CM field. For any order $\mathcal{O}$ of K, we say that C has* complex multiplication (CM) by $\mathcal{O}$ *if $\mathrm{End}_{\overline{k}}(J_C) \cong \mathcal{O}$. We say that C has* CM by K *if C has CM by an order in K.*

The moduli space of 2-dimensional principally polarized abelian varieties over $\mathbb{C}$ is 3-dimensional. Its function field is generated by three invariants (j_1, j_2, j_3) called the (absolute) Igusa invariants of C [12]. We define three *Igusa class polynomials* of an order $\mathcal{O}$ of a quartic CM field K by

$$H_{\mathcal{O},\ell}(x) = \prod_{i=1}^{s}(x - j_\ell^{(i)})$$

for $\ell = 1, 2, 3$. Here s is the number of isomorphism classes of 2-dimensional principally polarized abelian varieties over $\mathbb{C}$ with CM by $\mathcal{O}$, and the product is over the invariants $j_\ell^{(i)}$ from the s classes. For the sake of simplicity of both theory and computations, we will restrict our attention to $\mathcal{O} = \mathcal{O}_K$.

2.4 Endomorphisms in genus 2

We summarise some facts for endomorphism algebras of 2-dimensional abelian varieties with p-rank 1 here.

For elliptic curves E, we can read off the p-rank from the $\mathbb{Q}$-rank of the algebra $\mathrm{End}_{\overline{k}}^0(E)$. Indeed, there are two cases: an ordinary curve, with p-rank 1, where $\mathrm{End}_{\overline{k}}^0(E)$ is a CM field of degree 2; and a supersingular curve, with p-rank 0, where $\mathrm{End}_{\overline{k}}^0(E)$ is a quaternion algebra. Now let A be an absolutely simple abelian surface defined over a finite field k. By Theorem 2 we have three possibilities: $[\mathrm{End}_{\overline{k}}^0(A) : \mathbb{Q}] = 4$, 8 or 16. In line with the genus 1 results, one might intuitively guess that these correspond to the p-rank 2, 1, 0, cases respectively. However, this is not correct, as we will explain below. We note that Mumford in [15, Chapter IV, pg. 201] states the classification due to Albert of the four types that $\mathrm{End}_{\overline{k}}^0(A)$ can be, though there he does not give an association of these types with the p-rank of the abelian variety.

Lemma 4. *Let A be a simple abelian surface defined over a finite field k. If A has p-rank 1 then A is absolutely simple and $\mathrm{End}_{\overline{k}}^0(A)$ is a CM field of degree 4.*

Proof. We note that Maisner-Nart [13, Corollary 2.17] show that a simple abelian surface of p-rank 1 is absolutely simple. By going to an extension field of k, we can therefore assume without loss of generality that all endomorphisms of A over $\overline{k}$ are already defined over k.

By Theorem 2, the characteristic polynomial of Frobenius is $f_A(t) = m(t)^e$ for some irreducible monic polynomial $m(t) \in \mathbb{Z}[t]$. Also, $\mathrm{End}_{\overline{k}}^0(A)$ is a field if and only if $e = 1$. In this $e = 1$ case, the field $\mathrm{End}_{\overline{k}}^0(A) = K$ is a totally imaginary quadratic extension of K_0, a totally real quadratic algebraic number field. In other words, K is a quartic CM field. To complete the proof, it only remains to show that $e = 1$. But for simple abelian surfaces of p-rank 1, $f_A(t)$ must be irreducible by the remarks after Theorem 1, so indeed $e = 1$. □

Note that if A is not simple, and has p-rank 1, then A is isogenous to the product of an ordinary elliptic curve and a supersingular elliptic curve. Both of these are well understood.

Example 5. When $q = 2$, $k = \mathbb{F}_2$, the curve $y^2 + y = x^3 + 1/x$ has p-rank 1 (see [14] for example, or use Theorem 1). It is easy to calculate that $N_1 = N_2 = 4$, and the formulas in section 2.1 give $a_1 = 1$, $a_2 = 0$. Then the characteristic polynomial of Frobenius is $f_A(t) = t^4 + t^3 + 2t + 4$, which is irreducible over $\mathbb{Q}$ and so J_C is simple. Thus $\mathrm{End}_{\overline{k}}^0(J_C)$ is a CM field for this curve.

2.5 The reflex field, and splitting of primes

Given a CM field K and a *CM-type* Φ of K, i.e. a set of embeddings of K into its normal closure such that Φ and $\overline{\Phi}$ are disjoint and their union is the complete set of embeddings of K. The *reflex field* K^* of K with respect to Φ is the field generated by elements $\sum_{\phi\in\Phi}\phi(x)$ for $x \in K$. We call the CM type *primitive* if there is no subfield $K' \subset K$ such that the set of restrictions of elements of Φ to K' is a CM type of K'. If Φ is primitive and K is Galois over $\mathbb{Q}$, then $K = K^*$. In this paper we will consider non-Galois extensions, and K^* will be different from K, although both fields will be degree 4 extensions of $\mathbb{Q}$. The Galois closure L of K (and K^*) is a degree 2 extension of K, with Galois group D_4 over $\mathbb{Q}$.

Given a CM field K, an abelian variety A defined over $\mathbb{C}$ which has CM by K, and a prime p, the splitting behavior of primes above p in K determines the p-rank of the reduction $\overline{A}$ over $\mathbb{F}_p$ modulo a prime above p. Whenever A has dimension 1 (an elliptic curve), a criterion of Deuring states that $\overline{A}$ is supersingular if p is either ramified or inert in K and $\overline{A}$ is ordinary if p splits completely in K. However, whenever A has dimension 2, then there are more possibilities that occur.

For dimension 2, Goren distinguishes the cases in [9] assuming p is unramified in K and Gaudry, Houtmann, Kohel, Ritzenthaler and Weng in [6] extend this result to the ramified case. They show that whenever K is cyclic, then the reduction of A is either ordinary or supersingular, but whenever K is non-Galois, then it is possible for $\overline{A}$ to be in the "intermediate" case, and have p-rank 1. If K is Galois non-cyclic, then $\overline{A}$ will not be absolutely simple. As simple p-rank 1 varieties are absolutely simple, we will restrict to the case that K is non-Galois. The result of [9] and [6] is as follows.

Lemma 6. *Let K be a quartic CM field and C a curve of genus 2 over a number field $L \supseteq K$ with endomorphism ring $\mathcal{O}_K$. Let p be a prime number and $\mathfrak{p}$ a prime of $\mathcal{O}_L$, lying over p. The reduction of C modulo $\mathfrak{p}$ is a genus 2 curve with p-rank 1 if and only if (p) factors in $\mathcal{O}_K$ as $(p) = P_1P_2P_3$ or $(p) = P_1P_2P_3^2$. If that is the case, then the reduction $(C \bmod \mathfrak{p})$ is absolutely simple.*

Given any triple of invariants (j_1, j_2, j_3), the main theorem of complex multiplication implies that the field $K^*(j_1, j_2, j_3)$ is an unramified abelian extension of the reflex field K^*, and is therefore contained in the Hilbert class field H^* of K^*. On the other hand, $\mathbb{Q}(j_1, j_2, j_3)$ contains K_0^* by [18].

2.6 Cryptography

Elliptic and hyperelliptic curves with certain special properties are used in elliptic curve cryptography and hyperelliptic curve cryptography. One common requirement is that the Jacobian should be a group of prime (or nearly prime) order. The CM method provides a means of finding such curves quickly.

An alternative method for constructing curves with a certain number of points is to randomly choose a curve and count the number of points. The speed of this method clearly depends on the speed of the point-counting algorithm.

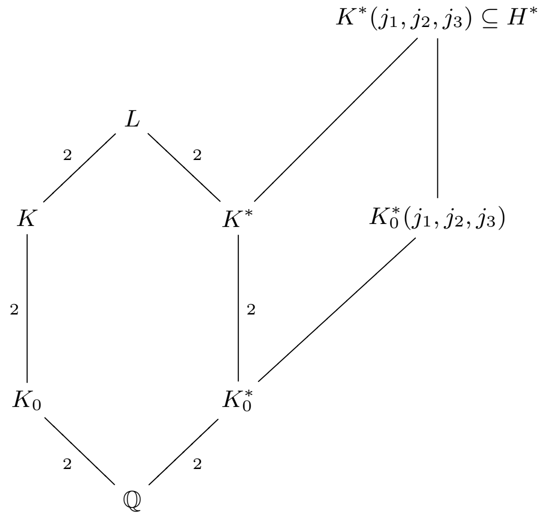

Fig. 1. Relations between CM field K, reflex field K^* and Hilbert class field H^*.

At present, point-counting algorithms are fast enough to compete with the CM method for elliptic curves, but not for hyperelliptic curves.

An important example for an application of the CM method in cryptography is the construction of pairing-friendly curves. An algebraic curve C over a finite field $\mathbb{F}_q$ is called *pairing-friendly* if the number $\#J_C(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on its Jacobian J_C is divisible by a large prime r and the embedding degree of $J_C(\mathbb{F}_q)$ with respect to r is small. The number κ is called the *embedding degree of J_C with respect to r*, if κ is the smallest integer such that $r \mid q^\kappa - 1$. In general, for random curves the embedding degree grows linearly with r and thus tends to be very large.

Pairing-friendliness means that the Jacobian group order must fulfill a very special condition that will never be satisfied by chance. For constructing such curves one thus seeks Weil numbers that fulfill this condition and afterwards constructs a corresponding curve by using the CM method. To measure the quality of a pairing-friendly curve one introduces the ρ-value

$$\rho(J_C) = \frac{g \log(q)}{\log(r)}.$$

This ratio shows how far the size of the group we can actually use for cryptographic applications differs from the size of $J_C(\mathbb{F}_q)$. Optimally the ρ-value is 1, meaning that we have a prime order group of $\mathbb{F}_q$-rational points. This optimal value currently is only achieved for elliptic curves, for an overview see [4].

3 Algorithms

We present three algorithms here. Algorithm 1 constructs curves of genus 2 and p-rank 1 with a Jacobian of prime order. Algorithm 2 is an alternative to Algorithm 1. Algorithm 3 constructs curves of p-rank 1 with a prescribed embedding degree.

Before we begin, we would like to point out that the final step in all our algorithms is always the same, to invoke the CM method and construct a curve from a given CM field $\mathbb{Q}(\pi)$. We present the details of the CM method later in Section 4. There are different ways to implement the CM method, but the specific implementation is not relevant for our paper so we leave this unspecified. Here is our first algorithm.

Algorithm 1 ***Input:*** *A non-Galois CM field K of degree 4 and a positive integer n*
Output: *A prime p of n bits and a curve of genus 2 over $\mathbb{F}_{p^2}$ that has p-rank 1 and a Jacobian with a prime number of rational points.*

1. *Take a random prime p of n bits.*
2. *If $p\mathcal{O}_K$ factors as $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, where $\mathfrak{p}_3$ has degree 2, continue. Otherwise, go to step 1.*
3. *If $\mathfrak{p}_1$ is principal and generated by α, let $\pi = \alpha\overline{\alpha}^{-1}p$. Otherwise, go to step 1.*
4. *If $N(u\pi - 1)$ is prime for some root of unity $u \in K$, then replace π by $u\pi$. Otherwise, go to step 1.*
5. *Compute the curve corresponding to π using the CM method and return this curve.*

Here is our second algorithm, which has the same input and output.

Algorithm 2 ***Input:*** *A non-Galois CM field K of degree 4 and a positive integer n*
Output: *A prime p of n bits and a curve of genus 2 over $\mathbb{F}_{p^2}$ that has p-rank 1 and a Jacobian with a prime number of rational points.*

1. *Take a random element α of $\mathcal{O}_K \setminus \mathcal{O}_{K_0}$ of which the norm has n bits.*
2. *If $p = N(\alpha)$ is prime in $\mathbb{Z}$, continue. Otherwise, go to step 1.*
3. *If the prime $\beta = p\alpha^{-1}\overline{\alpha}^{-1}$ of $\mathcal{O}_{K_0}$ remains prime in $\mathcal{O}_K$, then let $\pi = \alpha^2\beta$ and $p = N(\alpha)$. Otherwise, go to step 1.*
4. *If $N(u\pi - 1)$ is prime for some root of unity $u \in K$, then replace π by $u\pi$. Otherwise, go to step 1.*
5. *Compute the curve corresponding to π using the CM method and return this curve.*

Theorem 7. *For both Algorithms 1 and 2, the following holds. If the algorithm terminates, then the output is correct. The heuristic expected runtime of the algorithm is polynomial in n for fixed K.*

Proof. In both algorithms, we have $\pi\overline{\pi} = p^2$, so π is a Weil p^2-number. Let $\beta = p\alpha^{-1}\overline{\alpha}^{-1}$. Then p factors in K as a product of three primes $\alpha\overline{\alpha}\beta$, so the output has p-rank 1 by Lemma 6. By the CM method of Section 4, the curve has a Jacobian of prime order $N(u\pi - 1)$.

For the runtime of Algorithm 1, note that, by the prime number theorem and fast primality checking, it takes time polynomial in n to find a prime p of n bits. By Chebotarev's density theorem, a prime factors into principal primes as $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ with a positive probability, depending only on the class group of K, which is fixed. We view the number $N(\pi - 1)$ as random and it has about $2n$ bits, so by the prime number theorem, it is prime with probability $1/(2n\log(2))$. In particular, we expect the number of iterations to be quadratic in n.

In Algorithm 2, we view $N(\alpha)$ as a random number of n bits. By the prime number theorem, we expect it to be prime with probability $1/(n\log(2))$. We expect the prime β of $\mathcal{O}_{K_0}$ to be inert in K/K_0 with positive probability depending only on K. Again, we view $N(\pi - 1)$ as random and use the prime number theorem to get an expected number of iterations which is quadratic in n. $\square$

We have implemented Algorithm 1 in Magma [2]. We give some examples of cryptographic relevant bitsizes in Appendix A. Using precomputed class polynomials the curves can be found very quickly. All our examples were computed in less than 10 seconds on an Intel Core 2 Duo.

The following algorithm constructs p-rank 1 curves with prescribed embedding degree. It is modeled after the method by Freeman, Stevenhagen and Streng [5].

Algorithm 3 ***Input:*** *A non-Galois CM field K of degree 4, a positive integer κ and a prime number $r \equiv 1 \pmod{2\kappa}$ which splits completely in K.*
Output: *A prime p and a curve of genus 2 over $\mathbb{F}_{p^2}$ that has p-rank 1 and embedding degree κ with respect to r.*

1. *Let $\mathfrak{r}$ be a prime of K dividing r and let $\mathfrak{s} = r\mathfrak{r}^{-1}\overline{\mathfrak{r}}^{-1}$.*
2. *Take a random element x of $\mathbb{F}_r^*$ and a primitive 2κ-th root of unity ζ.*
3. *Take $\alpha \in \mathcal{O}_K \setminus \mathcal{O}_{K_0}$ such that $\alpha \bmod \mathfrak{r} = x$, $\alpha \bmod \overline{\mathfrak{r}} = x\zeta$ and $\alpha \bmod \mathfrak{s} = x^{-1}$.*
4. *If $p = N(\alpha)$ is prime in $\mathbb{Z}$ and different from r, continue. Otherwise, go to step 2.*
5. *If the prime $\beta = N(\alpha)\alpha^{-1}\overline{\alpha}^{-1}$ of $\mathcal{O}_{K_0}$ remains prime in $\mathcal{O}_K$, let $\pi = \alpha^2\beta$ and $p = N(\alpha)$. Otherwise, go to step 2.*
6. *Compute the curve corresponding to π using the CM method and return this curve.*

Theorem 8. *If the algorithm terminates, then the output has p-rank 1 and embedding degree κ with respect to a subgroup of order r. The heuristic expected runtime of the algorithm is polynomial in r for fixed K.*

Proof. The number π is defined in step 4 by $\pi = \alpha^2\beta$, where p factors into primes of $\mathcal{O}_K$ as $\alpha\overline{\alpha}\beta$, just as in Algorithm 2. In particular, the facts that the output has p-rank 1 and a Jacobian of prime order $N(\pi - 1)$ is proven as in the proof of Theorem 7

We find $\pi \bmod \mathfrak{r} = (\alpha \bmod \mathfrak{r})^2(\phi(\alpha\overline{\alpha}) \bmod \mathfrak{r})$, where ϕ is the non-trivial automorphism of K_0. Inside $\mathbb{F}_r$, the right hand side is equal to $(\alpha \bmod \mathfrak{r})^2(\alpha \bmod \mathfrak{s})^2 = 1$, so $r|N(\pi - 1)$. On the other hand,

$$\begin{aligned} p^2 \bmod \mathfrak{r} &= (\alpha \bmod \mathfrak{r})^2(\overline{\alpha} \bmod \mathfrak{r})^2(\phi(\alpha\overline{\alpha}) \bmod \mathfrak{r})^2 \\ &= (\alpha \bmod \mathfrak{r})^2(\alpha \bmod \overline{\mathfrak{r}})^2(\alpha\overline{\alpha} \bmod \mathfrak{s})^2. \end{aligned}$$

As $\mathfrak{s} = \overline{\mathfrak{s}}$, we have $(\overline{\alpha} \bmod \mathfrak{s}) = (\alpha \bmod \overline{\mathfrak{s}}) = (\alpha \bmod \mathfrak{s})$, so $p^2 \bmod r = (\alpha \bmod \mathfrak{r})^2(\alpha \bmod \overline{\mathfrak{r}})^2(\alpha \bmod \mathfrak{s})^4 = \zeta^2$ is a primitive κ-th root of unity. By [5, Proposition 2.1], the facts that $p^2 \bmod r$ is a primitive κ-th root of unity and that $r|N(\pi-1)$ imply that J_C has embedding degree κ with respect to r.

This finishes the proof of the correctness of the output. To prove the runtime, as r splits completely, α is a lift of some element modulo r. We treat its norm $p = N(\alpha)$ as a random integer around r^4, which by the prime number theorem is prime with probability $1/(4\log r)$. Again, we expect the prime $\beta = p\alpha^{-1}\overline{\alpha}^{-1}$ of K_0 to be inert in K/K_0 with constant positive probability. $\square$

Algorithm 3 produces curves with prescribed embedding degree κ with respect to a prime number r that is chosen in advance. Our algorithm is an adaptation of the method proposed by Freeman, Stevenhagen and Streng in [5]. They give a heuristic analysis of their method. It is shown in [5, Thm. 3.4] that one expects the prime q to yield a ρ-value of about 8 for genus 2, which means that $\log(q) = 4\log(r)$. The same reasoning holds for our algorithm. The prime p computed as the norm of the element α in step 4 is therefore expected to give $\log(p) = 4\log(r)$. Since our p-rank 1 curve will be defined over $\mathbb{F}_{p^2}$, its ρ-value will be $\rho = 2\log(p^2)/\log(r) \approx 16$.

For cryptographic applications one requires that the prime r has at least 160 bits, since r is the order of the subgroup used in protocols. Then p already has 640 bits. This makes field and curve arithmetic very slow, compared to elliptic curve implementations of the same security level, where it is possible to have p of the same size as r. Thus the curves produced by algorithm 3 currently have no relevance for practical applications in cryptography. Still, our examples show, that in principle pairing-based cryptography is possible for p-rank 1.

4 The CM method

Roughly speaking, the basic principle of the complex multiplication (CM) method of constructing curves over finite fields with desired properties is to construct a complete list of all candidate abelian varieties in characteristic 0 whose reduction modulo Q could be the Jacobian of the curve we seek (where Q is a prime over q). Then each entry on the list of candidates is checked.

The Lubin-Serre-Tate lifting theorem states that any *ordinary* abelian variety over $\mathbb{F}_q$ is the reduction modulo Q of some characteristic 0 abelian variety, so we know that if the curve we seek exists it will be found by this method.

It seems to be standard to include the computation of Igusa class polynomials as part of the CM method, although this is the most costly step. We propose separating this step from the CM method. Reasons for doing this include

1. Computation of class polynomials has other applications in computational number theory.
2. In practice the class polynomials are pre-computed and stored, and a lookup table is used.
3. The method used after obtaining the class polynomials does not depend on the way the class polynomials are computed.

So we shall not present any particular method of computing the class polynomials. There are a few methods in the literature. The complex analytic approach, first described by Spallek [19] and van Wamelen [23] computes the CM abelian varieties as lattices in $\mathbb{C}^2$ and evaluates Igusa invariants in them via Siegel modular forms. Recently, a complete runtime analysis of the complex analytic method was given by Streng [21]. Eisenträger and Lauter [3] present an algorithm for constructing genus 2 curves over finite fields that differs from the classical approach in that their method computes the class polynomials using a Chinese Remainder Theorem method rather than complex analytic techniques. Gaudry, et al [6], [7] modify the classical CM method by using a 2-adic lifting method to construct the class polynomials.

In more detail the genus 2 CM method is as follows.

1. Fix a quartic CM field $K = \mathbb{Q}(\pi)$.
2. Somehow get the Igusa class polynomials $H_1(x)$, $H_2(x)$, $H_3(x)$ for K.
3. Choose a "suitable" (we will address this below) prime p and reduce $H_i(x)$ modulo p to get Igusa invariants in $\mathbb{F}_q$.
4. Then an algorithm such as that of Mestre can be used to generate a curve over $\mathbb{F}_p$ with the given invariants such that $J_C = A$.
5. Select correct twist.

Remark 9. The "suitable" prime needs to be one whose splitting behavior in K is as one desires. For example, if one wants an ordinary curve, then one could require that p splits completely in K. This case has been studied before in [3],[6],[7], for example. We shall be looking for curves of p-rank 1, and we will require that (p) splits as $P_1P_2P_3$ or $P_1P_2P_3^2$ as we explained in Section 2.5.

By a *twist* of a curve C/k in step 5, we mean a curve C'/k such that C and C' become isomorphic over $\overline{k}$. The number of such curves is small and depends only on the number of $\overline{k}$-automorphisms of C.

In step 3, we need to pick one root $j_1 \in \mathbb{F}_q$ of $h \bmod p$ for every irreducible factor h of $H_1(x)$, and for each, take all roots $j_2, j_3 \in \mathbb{F}_q$ of $H_2 \bmod p$ and $H_3 \bmod p$. If s is the degree of the class polynomials and n the number of irreducible factors of $H_1(x)$, then among the s^2n triples $(j_1, j_2, j_3) \in \mathbb{F}_q$ obtained, there are n that correspond to the reductions of CM curves. All the twists of those n curves are exactly all possible reductions of curves with CM by $\mathcal{O}_K$. The correct triples and twists, if they exist, can be selected by probabilistic checking of the order of the Jacobian of C, which is $N_{K/\mathbb{Q}}(\pi-1)$ for the correct curve C.

One refinement put forth in [7] is that we replace $H_2(x)$ and $H_3(x)$ by two other polynomials in such a way that we directly only have the correct n triples (j_1, j_2, j_3) instead of the ns^2 mentioned above. This refinement works only if $H_1(x)$ has no roots of multiplicity greater than 1 in characteristic 0, and the j_1 we are looking for has multiplicity 1 as a root modulo p. They define $G_2(x), G_3(x)$ by Lagrange interpolation and $\widehat{H}_2(x), \widehat{H}_3(x)$ by a modification thereof. More precisely, $G_k(x)$ and $\widehat{H}_k(x)$ are defined by saying that they have degree at most $n-1$ and that for all zeroes j_1 of $H_1(x)$ and for $\ell \in \{2,3\}$,

$$j_\ell = G_\ell(j_1) = \frac{\widehat{H}_\ell(j_1)}{H_1'(j_1)}.$$

We mention G because it is much more straightforward and $\widehat{H}$ because its height is smaller ([7]). So we first find a root of $H_1(x)$ modulo a prime p of mixed reduction, and this will be the potential j_1 Igusa invariant. Then the invariants j_2, j_3 that go with this j_1 are computed from these formulas. This refinement means we do not have to try all n triples, just one, which is a big speedup when the class number is large. Notice also that such a representation proves that $\mathbb{Q}(j_1, j_2, j_3) = \mathbb{Q}(j_1)$ if $H_1(x)$ has only simple roots.

We will prove in Section 5 that these G_i or $\widehat{H}_i$ do not work in the case $(p) = P_1P_2P_3^2$, and we will show how to adapt the formulas in that case. The formulas do work in the case $(p) = P_1P_2P_3$. The problem in the case where $(p) = P_1P_2P_3^2$ is that $H_1(x)$ has only roots of higher multiplicity modulo p, so that $G_i(j_1)$ and $\frac{\widehat{H}_i(j_1)}{H_1'(j_1)}$ have a zero in the denominator.

5 Multiplicity of roots of class polynomials modulo p

In this section we shall explain why the refinement of the CM method from [7] with polynomials $G_2(x), G_3(x)$, does not work directly for curves of p-rank 1 when $(p) = P_1P_2P_3^2$. We will explain how to get around the problem by modifying $G_2(x), G_3(x)$.

As stated in the previous section, the CM method for ordinary curves with its refinement of the $G_i(x)$ polynomials appears to require that the $H_i(x)$ have no repeated roots (or at least some roots of multiplicity 1) modulo p. Computer experiments indicated that, for the primes of mixed reduction with $(p) = P_1P_2P_3^2$, the reduction of $H_1(x)$ mod p always had all roots of multiplicity > 1. This turns out to be always true, and we will provide a proof below. This means that the modified CM method for ordinary curves will not work directly.

Note that the degree of $H_1(x)$ is twice the class number of the CM field K, as stated in [7, Theorem 1].

We will study the splitting behavior of relevant primes in the reflex field K^*. This turns out to be the key, along with the fact that $\mathbb{Q}(j_1)$ is an unramified abelian extension of K_0^*.

We will use the following theorem.

Theorem 10 (Kummer-Dedekind). *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial. Let α be a root of f, and let $K = \mathbb{Q}(\alpha)$. Let p be a prime in $\mathbb{Z}$ and write*

$$f = \prod_{i=1}^{m} g_i^{e_i} \pmod p, \quad g_i \in \mathbb{Z}[x],$$

where the $g_i \bmod p$ are distinct irreducible polynomials in $\mathbb{F}_p[x]$. The prime ideals of $A = \mathbb{Z}[x]/(f)$ that divide (p) are exactly the ideals $P_i = (p, g_i)$ for $i = 1, \ldots, m$. If P_i is not invertible as a fractional $\mathbb{Z}[x]$-ideal, then $e_i > 1$ and p divides the index of A in the maximal order of K. If P_i is invertible, then its ramification index over $\mathbb{Z}$ is e_i and the residue class field degree $\dim_{\mathbb{F}_p} A/P_i$ equals $\deg(g_i \bmod p)$.

Proof. This is part of Theorem 8.2 of [20]. □

5.1 Case $(p) = P_1P_2P_3^2$

We will use L to denote the Galois closure of K. Let G denote the Galois group of $L/\mathbb{Q}$, which is isomorphic to the dihedral group of order 8.

Lemma 11. *Let K be a quartic CM field and K^* its reflex field. Let p be a prime that splits in K as $(p) = P_1P_2P_3^2$, for some prime ideals P_i. Then $(p) = S^2$ in K_0^* (the real quadratic subfield of K^*) and S splits in K^*/K_0^*.*

Proof. Let P be a prime of L lying over P_1. As P splits in $K_0/\mathbb{Q}$, its decomposition group D_P contains $\mathrm{Gal}(L/K)$, but as P does not split completely in L, we find that D_P is equal to $\mathrm{Gal}(L/K)$. As there is ramification and the inertia group I_P is contained in D_P, it must also be equal to $\mathrm{Gal}(L/K)$. As K^* is one of the non-conjugate non-normal degree 4 fields in L, this implies that P ramifies in $K_0^*/\mathbb{Q}$ and splits in K^*/K_0^*. □

Next we prove a lemma relating the invariants and p. Assume that $H_1(x)$ has only roots of multiplicity 1. Recall that $\mathbb{Q}(j_1, j_2, j_3) = \mathbb{Q}(j_1)$ as we explained in Section 3.

Lemma 12. *Let K be a quartic CM field and K^* its reflex field. Let p be a prime that splits in K as $(p) = P_1P_2P_3^2$, for some prime ideals P_i. Let $E = \mathbb{Q}(j_1)$. Then any prime of E lying over p has ramification index 2.*

Proof. By Figure 1, we know that $K^*(j_1)$ is unramified over K^* and hence by Lemma 11 over K_0^*. In particular, the subfield E is also unramified over K_0^*. By Lemma 11, $(p) = S^2$ in K_0^*. □

We call a prime $p \in \mathbb{Z}$ *ok* for a monic irreducible polynomial $F \in \mathbb{Q}[x]$ if there exists a positive rational number a such that $\mathrm{ord}_p\, a = 0$, $G = F(ax)$ is in $\mathbb{Z}[x]$, and the index of $\mathbb{Z}[x]/(G)$ in its normal closure is coprime to p. We call a prime $p \in \mathbb{Z}$ *ok* for an arbitrary polynomial $F \in \mathbb{Q}[x]$ if p is ok for every monic irreducible factor of F and $\mathrm{ord}_p\, b = 0$ for the leading coefficient b of F.

Corollary 13. *Let K be a quartic CM field and K^* its reflex field. If a prime p splits in K as $(p) = P_1 P_2 P_3^2$, for some prime ideals P_i, and p is ok for H_1, then $H_1 \bmod p$ is a square.*

Proof. Let F be an irreducible factor of $H_1(x)$ in $\mathbb{Z}[x]$; we prove that G (as in the definition of 'ok') is a square modulo p. By Theorem 10, it suffices to prove that (p) factorizes into prime ideals with even powers in $E = \mathbb{Q}(j_1)$, where w.l.o.g. j_1 is a root of $F(x)$. This follows from Lemma 12. □

Corollary 14. *Let K be a quartic CM field and K^* its reflex field. If a prime p splits in K as $(p) = P_1 P_2 P_3^2$, for some prime ideals P_i, then all roots of $H_1(x) \bmod p$ in $\overline{\mathbb{F}_p}$ have multiplicity greater than 1.*

Proof. As the CM curves have good reduction, there exist positive integers d and a such that $dH_1(ax)$ is monic in $\mathbb{Z}[x]$ and $\mathrm{ord}_p\, d = \mathrm{ord}_p\, a = 0$. Let F be a monic irreducible factor of $dH_1(ax)$ in $\mathbb{Z}[x]$; we prove that $F \bmod p$ has only roots of multiplicity at least 2. By Theorem 10, it suffices to prove that (p) factorizes into ramified prime ideals in $E = \mathbb{Q}(j_1)$, where w.l.o.g. j_1 is a root of $F(x)$. This follows from Lemma 12. □

Remark 15. The above is not specific for the invariant j_1, it will hold for any rational function in j_1, j_2, j_3.

We now proceed to obtain even more information about the factorization of $H_1(x)$ modulo p.

Lemma 16. *If K as above contains a Weil p-number (recall p is prime), then any prime R of K_0^* lying over p splits completely in $E^* = EK^*$.*

Proof. The main theorem of complex multiplication states that E^* is an unramified abelian extension of K^*. Class field theory tells us that the decomposition group of a prime lying over R in E^*/K^* is the subgroup of the class group generated by the class of R. In particular, it suffices to prove that R is in H_0, where H_0 is the subgroup corresponding to the extension E^*/K^*. This will imply that the decomposition group is trivial.

If K contains a Weil p-number π, then $(\pi) = P_1^a P_2^b P_3^c$ and as $\overline{P_1} = P_2$, $\overline{P_3} = P_3$ and $\pi\overline{\pi} = p$, we find $a + b = 1, c = 1$, so without loss of generality, $P_1 P_3$ and $P_2 P_3$ are principal and generated by π and $\overline{\pi}$.

By [7], H_0 consists of those ideals of K^* whose type norm for the reflex type is principal. The type norm of R is either $P_1 P_3$ or $P_2 P_3$, hence R is in H_0. □

Corollary 17. *Let K be a quartic CM field. Let the characteristic polynomial of Frobenius used to generate K be $f(t) = t^4 + a_1 t^3 + a_2 t^2 + a_1 p t + p^2$ for integers a_1, a_2 and a prime p that splits in $\mathcal{O}_K$ as $(p) = P_1 P_2 P_3^2$ for some prime ideals P_i in K. If p is ok for H_1, then $H_1(x) \bmod p$ has the form $\prod_{i=1}^{h} (x - \alpha_i)^2$ where the α_i are distinct elements of $\mathbb{F}_p$.*

Proof. We know that p ramifies as S^2 in $K_0^*/\mathbb{Q}$ and then S splits in K^*/K_0^* by Lemma 11. By Lemma 16, the resulting two primes lying over S split completely in E^*/K^*. In particular, any prime of E lying over p has residue field degree 1. By Theorem 10, this implies that every irreducible factor of $H_1(x)$ splits into linear factors when reduced mod p, and $H_1(x)$ has the form stated. □

Adapting G_i or $\widehat{H}_i$ to the case where p ramifies in K_0^* is not that hard. First of all, we can factor H_1 in $K_0^*[x]$ and get an irreducible factor $f \in K_0^*[x]$. As there is no more ramification of p in E/K_0^*, this polynomial modulo the unique prime S of K_0^* over p has no roots of higher multiplicity (assuming of course that p does not divide the index of $\mathbb{Z}[j_1]$ in the ring of integers of its field of fractions).

If one works with G_i, then simply replacing G_i by its remainder $R_i \in K_0^*[x]$ upon division by f solves the problem. Indeed, R_i is the Lagrange interpolation when only zeroes j_1 of f are considered, because for them we have $j_i = G_i(j_1) = R_i(j_1)$ in characteristic 0.

If one works with $\widehat{H}_i$, then a similar argument shows that it suffices to replace H_1 by a $K_0^*[x]$-irreducible factor f and $\widehat{H}_i$ by the unique polynomial S_i of degree at most $\deg(f) - 1$ which is equivalent modulo f to

$$\frac{\widehat{H}_i}{H_1/f}.$$

5.2 Case $(p) = P_1P_2P_3$

Unlike the previous section, this case presents no obstruction, and the CM method used in for ordinary curves can be applied directly. We proceed to prove this. Continue the notation from the previous section.

Lemma 18. *Let K be a quartic CM field and K^* its reflex field. Let p be a prime that splits in K as $(p) = P_1P_2P_3$, for some prime ideals P_i. Then (p) is inert in K_0^* and splits in K^*/K_0^*.*

Proof. Completely the same as the proof of Lemma 12, except that this time the inertia group is trivial and primes are inert where they ramified in the other case. See also the proof of Theorem 3.5 (3) in [6]. □

Corollary 19. *Let K be a quartic CM field and K^* its reflex field. If a prime p splits in K as $(p) = P_1P_2P_3$, for some prime ideals P_i, and p is ok for H_1, then all roots of $H_1(x)$* mod p *are distinct.*

Proof. By Figure 1, we know that $K^*(j_1)$ is unramified over K^*, and hence by Lemma 18 over $\mathbb{Q}$. In particular, the subfield $\mathbb{Q}(j_1)$ is also unramified over $\mathbb{Q}$.

Let $F(x)$ be an irreducible factor of $H_1(x)$ in $\mathbb{Z}[x]$; we prove that $F(x)$ is separable mod p. By Theorem 10, it suffices to prove that (p) does not ramify in $E = \mathbb{Q}(j_1)$, where w.l.o.g. j_1 is a root of $F(x)$. This follows from Lemma 12. □

Lemma 20. *If K as above contains a Weil p^2-number (recall p is prime) corresponding to a p-rank 1 abelian surface, then the unique prime R of K_0 lying over p splits completely in $E^* = EK^*$.*

Proof. We follow the proof of Lemma 16. This time, K contains a Weil p^2-number π, so $(\pi) = P_1^a P_2^b P_3^c$. As $\overline{P_1} = P_2$, $\overline{P_3} = P_3$ and $\pi\overline{\pi} = p$, we find $a + b = 2, c = 1$. If $a = b = 1$, then $\mathrm{End}_k(A_\pi)$ has order 2 in the Brauer group of $\mathbb{Q}(\pi)$ and we don't have p-rank 1, so without loss of generality, $P_1^2 P_3$ and $P_2^2 P_3$ are principal and generated by π and $\overline{\pi}$. The type norm of R is either $P_1^2 P_3$ or $P_2^2 P_3$, hence R is in H_0. □

Corollary 21. *Let K be a quartic CM field. Let the characteristic polynomial of Frobenius used to generate K be $f(t) = t^4 + a_1 t^3 + a_2 t^2 + a_1 p t + p^2$ for integers a_1, a_2 and a prime p that splits in $\mathcal{O}_K$ as $(p) = P_1 P_2 P_3$ for some prime ideals P_i in K. If p is ok for H_1, then $H_1(x) \bmod p$ has the form $\prod_{i=1}^{h} g_i$ where the g_i are distinct irreducible polynomials of degree 2 over $\mathbb{F}_p$.*

Proof. We know that p is inert in $K_0^*/\mathbb{Q}$. By Lemma 20, it then splits completely in $\mathbb{Q}(j_1)$. By Theorem 10, this implies that every irreducible factor of $H_1(x)$ splits into distinct irreducible quadratic factors when reduced mod p, and $H_1(x)$ has the form stated. □

Remark 22. The same argument works in the ordinary case since p is unramified everywhere, and shows that $H_1(x)$ has distinct roots modulo p.

6 Conclusion

In this paper we have presented algorithms to construct genus 2 curves of p-rank 1, using the complex multiplication (CM) method. We have demonstrated that it is possible to efficiently construct curves such that their Jacobian has a prime number of rational points over the ground field. These curves might be useful for cryptographic purposes, and we have given examples for certain bitsizes of the Jacobian group order, suitable for different security levels. Further, our method can be used to construct p-rank 1 curves with a prescribed small embedding degree. We have discussed the CM method and the modulo p reduction of class polynomials in the case of p-rank 1. Our algorithms show, that for genus 2, constructing p-rank 1 curves is as easy as constructing ordinary curves.

References

1. A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Mathematics of Computation*, 61(203), July 1993.
2. W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

3. K. Eisentraeger and K. Lauter. A CRT algorithm for constructing genus 2 curves over finite fields, 2004. To appear in Arithmetic, Geometry and Coding Theory - AGCT-10 (Marseille), 2005.
4. D. Freeman, M. Scott, and E. Teske. A taxonomy of pairing-friendly elliptic curves. Cryptology ePrint Archive, Report 2006/372, 2006. Available from `http://eprint.iacr.org/2006/372`.
5. D. Freeman, P. Stevenhagen, and M. Streng. Abelian varieties with prescribed embedding degree. In A. J. van der Poorten and A. Stein, editors, *ANTS*, volume 5011 of *Lecture Notes in Computer Science*, pages 60–73. Springer, 2008.
6. P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The p-adic CM-method for genus 2, 2005. Available at http://arxiv.org/abs/math.NT/0503148.
7. P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The 2-adic CM method for genus 2 curves with application to cryptography. In *Advances in Cryptology - ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 114–129. Springer-Verlag, Berlin, 2006.
8. J. Gonzalez. On the p-rank of an abelian variety and its endomorphism algebra. *Pub. Math.*, 42(1):119–130, 1998.
9. E. Z. Goren. On certain reduction problems concerning abelian surfaces. *Manuscripta Math.*, 94(1):33–43, 1997.
10. L. Hitt. Families of genus 2 curves with small embedding degree. Cryptology ePrint Archive, Report 2007/001, 2007. to appear in the Journal of Mathematical Cryptology.
11. E. W. Howe, E. Nart, and C. Ritzenthaler. Jacobians in isogeny classes of abelian surfaces over finite fields, 2006.
12. J.-I. Igusa. Arithmetic variety of moduli for genus 2. *The Annals of Mathematics*, 72(3):612–649, 1960.
13. D. Maisner and E. Nart. Abelian surfaces over finite fields as Jacobians. *Experiment. Math.*, 11(3):321–337, 2002. With an appendix by Everett W. Howe.
14. G. McGuire and J. F. Voloch. Weights in codes and genus 2 curves. *Proc. Amer. Math. Soc.*, 133(8):2429–2437 (electronic), 2005.
15. D. Mumford. *Abelian Varieties*. Tata Institute of Fundamental Research Studies in Mathematics. Oxford University Press, Bombay, 1970.
16. F. Oort. Subvarieties of moduli spaces. *Invent. Math.*, 24:95–119, 1974.
17. H.-G. Rück. Abelian surfaces and Jacobian varieties over finite fields. *Compositio Math.*, 76(3):351–366, 1990.
18. G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, 1994.
19. A. Spallek. *Kurven vom Geschlecht* 2 *und ihre Anwendung in Public-Key-Kryptosystemen*. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994.
20. P. Stevenhagen. The arithmetic of number rings. In J. Buhler and P. Stevenhagen, editors, *Surveys in Algorithmic Number Theory*. Cambridge University Press, 2008.
21. M. Streng. Computing Igusa class polynomials. preprint on http://www.math.leidenuniv.nl/~streng/icp.pdf, 2008.
22. J. Tate. Classes d'isogénie des variétés abéliennes sur un corps fini (d'après Z. Honda). *Sémin. Bourbaki 1968/69, No.352*, pages 95–110, 1971.
23. P. van Wamelen. Examples of genus two CM curves defined over the rationals. *Mathematics of Computation*, 68(225):307–320, 1999.
24. W. C. Waterhouse and J. S. Milne. Abelian varieties over finite fields. In *1969 Number Theory Institute (Proceedings of Symposia in Pure Math., Vol. XX)*, pages 53–64. Amer. Math. Soc., Providence, R.I., 1971.

A Examples

We provide examples of p-rank 1 curves C defined over a quadratic field $\mathbb{F}_{p^2}$ whose Jacobian $J_C(\mathbb{F}_{p^2})$ has prime order. The CM field for all examples is $K = \mathbb{Q}(\alpha)$, where α is a root of $X^4 + 34X + 217 \in \mathbb{Q}[X]$. We give the prime p, the coefficients a_1 and a_2 of the characteristic polynomial of Frobenius and the coefficients $c_i \in \mathbb{F}_{p^2}$ of the curve equation

$$C : y^2 = c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0.$$

The group order of the Jacobian can be computed as

$$\#J_C(\mathbb{F}_{p^2}) = p^4 + 1 + a_1(p^2 + 1) + a_2.$$

The field $\mathbb{F}_q = \mathbb{F}_{p^2}$ is given as $\mathbb{F}_p(\sigma)$, where σ has the minimal polynomial $f_\sigma = X^2 + 27X + 128 \in \mathbb{F}_p[X]$. Section headings describe the size of the group $J_C(\mathbb{F}_{p^2})$ in bits. The three example bit sizes are suitable for the 80-, 96- and 128-bit security levels.

A.1 160 Bits

$$\begin{aligned}
p &= 924575392409\\
a_1 &= -3396725192754\\
a_2 &= 4585861472127472591045899\\
c_6 &= 743799951755 \cdot \sigma + 324411853696\\
c_5 &= 883721851762 \cdot \sigma + 326341693855\\
c_4 &= 52647632309 \cdot \sigma + 594134629477\\
c_3 &= 237357033335 \cdot \sigma + 399172288834\\
c_2 &= 260092427705 \cdot \sigma + 863345808041\\
c_1 &= 383181044930 \cdot \sigma + 205909996395\\
c_0 &= 77193628324 \cdot \sigma + 227797496783
\end{aligned}$$

A.2 192 Bits

$$
\begin{aligned}
p &= 236691298903769\\
a_1 &= 9692493559086\\
a_2 &= 53053369677708708650361238059\\
c_6 &= 97034787970005 \cdot \sigma + 108070185883897\\
c_5 &= 177590039969265 \cdot \sigma + 71180325836815\\
c_4 &= 136325719779266 \cdot \sigma + 128119595448837\\
c_3 &= 113311153672510 \cdot \sigma + 118353899161689\\
c_2 &= 61497433468379 \cdot \sigma + 9079089070164\\
c_1 &= 61748720271204 \cdot \sigma + 92041395614564\\
c_0 &= 114758796702185 \cdot \sigma + 45168163359627
\end{aligned}
$$

A.3 256 Bits

$$
\begin{aligned}
p &= 15511800964685067143\\
a_1 &= -2183138494024250742\\
a_2 &= -3901714528939658445128584170758642995559\\
c_6 &= 12621432058784055423 \cdot \sigma + 4951229583301315115\\
c_5 &= 10615462210692139258 \cdot \sigma + 2491309670771144544\\
c_4 &= 302040341019595016 \cdot \sigma + 3121515878473940580\\
c_3 &= 1310375005142538356 \cdot \sigma + 5402372758879029239\\
c_2 &= 6984026189189411646 \cdot \sigma + 9715874427790652648\\
c_1 &= 2687728988296128478 \cdot \sigma + 12158404312714991145\\
c_0 &= 2543583512728983447 \cdot \sigma + 8504741143337818180
\end{aligned}
$$