The 2-adic CM method for genus 2 curves with application to cryptography

P. Gaudry[1,2], T. Houtmann[2], D. Kohel[3], C. Ritzenthaler[4], and A. Weng[2]

[1] LORIA - Projet SPACES
Campus Scientifique - BP 239, 54506 Vandoeuvre-lès-Nancy Cedex France
[2] Laboratoire d'Informatique (LIX)
École polytechnique, 91128 Palaiseau Cedex France
[3] School of Mathematics and Statistics
The University of Sydney, NSW 2006 Australia
[4] Institut de Mathématiques de Luminy
163 Avenue de Luminy, Case 907, 13288 Marseille Cedex 9 France

Abstract. The complex multiplication (CM) method for genus 2 is currently the most efficient way of generating genus 2 hyperelliptic curves defined over large prime fields and suitable for cryptography. Since low class number might be seen as a potential threat, it is of interest to push the method as far as possible. We have thus designed a new algorithm for the construction of CM invariants of genus 2 curves, using 2-adic lifting of an input curve over a small finite field. This provides a numerically stable alternative to the complex analytic method in the first phase of the CM method for genus 2. As an example we compute an irreducible factor of the Igusa class polynomial system for the quartic CM field $\mathbb{Q}(i\sqrt{75+12\sqrt{17}})$, whose class number is 50. We also introduce a new representation to describe the CM curves: a set of polynomials in (j_1, j_2, j_3) which vanish on the precise set of triples which are the Igusa invariants of curves whose Jacobians have CM by a prescribed field. The new representation provides a speedup in the second phase, which uses Mestre's algorithm to construct a genus 2 Jacobian of prime order over a large prime field for use in cryptography.

1 Introduction

In the late 1980's, Koblitz proposed the use of hyperelliptic curves in cryptography. Since then, significant progress has been made in turning this idea into practice, and currently genus two cryptosystems present the same security benefits as elliptic curves, together with potential benefits in terms of performance and new protocols [31, 2, 17, 22].

The efficient generation of genus two groups of prime or nearly prime order over finite fields of large characteristic, however, remains an important issue. Random curve generation in characteristic 2 is amenable to efficient versions of Kedlaya's algorithm or Mestre's AGM algorithm. In contrast, over large prime fields the latest records for point counting (see [18]) still require about a week's computation time for each curve. In this case, the complex multiplication method currently provides the only efficient approach to cryptographic curve construction. For genus one, several authors have introduced improvements to the CM method using p-adic lifting [13, 7, 6, 24]. Our article generalizes such work to the case of genus two. Furthermore, in the past few years, the elliptic CM method has gained new interest as the key tool for building curves with a special structure, in particular curves with a computable bilinear map [29]. Similar constructions in genus two will also require explicit CM methods.

The first phase of the CM method constructs the *Igusa class polynomials* for CM genus two curves, which determine the triples (j_1, j_2, j_3) of invariants of curves whose Jacobians have prescribed endomorphism ring. These polynomials are determined by complex analytic techniques, or, in this work, by p-adic analytic construction. After solving for the roots of these polynomials over a chosen finite field of large characteristic, the algorithm of Mestre [28] allows one to construct a model of the curve for which the group order of its Jacobian has been previously determined to be prime or nearly prime. In this article, we extend the computational limit for Igusa class polynomials in genus two, addressing concerns that a CM field of low class number might give rise to weak curves in a cryptographic protocol.

Our first contribution is to use a 2-adic lifting method in place of the classical floating point complex approach. We start with a binary curve over a field small enough so that point counting is possible using naive methods. We determine not only the number of points but also the endomorphism ring of the Jacobian and therefore the CM field K associated to it. By computing the canonical 2-adic lift with sufficiently high precision we are able to get the class polynomials which we recognize as polynomials over the rationals. This bypasses the costly step of evaluating theta functions. We also introduce a simple representation of the ideal of CM invariants in terms of univariate polynomials. Prior authors focused on finding the degree h_K^* minimal polynomials $H_1(X)$, $H_2(X)$, and $H_3(X)$ of the invariants j_1, j_2, and j_3. However in the second phase of the CM method, this requires a combinatorial match of ${h_K^*}^3$ roots to find one of h_K^* valid triples, when constructing a CM curve. For those small values of h_K^* previously attainable, this was not particularly onerous, but with our 2-adic method, our largest examples computed have reached $h_K^* = 100$, for which this combinatorial matching problem is undesirable.

Our `Magma` and `C` implementation of the 2-adic CM method allow us to compute a degree 50 irreducible factor of Igusa class polynomials for the quartic CM field $K = \mathbb{Q}(i\sqrt{75 + 12\sqrt{17}})$. The class number of K is 50 and the Igusa class polynomials for K have degree $h_K^* = 100$.

The paper is organized as follows. In section 2 we introduce the mathematical objects we need to explain the 2-adic CM method and the generation of hyperelliptic curves suitable for cryptography. In section 3 we deal with Igusa class polynomials, our new representation of the ideal of invariants. In section 4 we give details about the 2-adic CM method. In section 5 we analyze its complexity and compare it with previous methods [35, 40, 9, 16].

2 Mathematical background

In this section, we briefly present the mathematical tools that we need. The first part deals with complex multiplication theory. We give theoretical results applied to our genus two case. Then we recall Lubin-Serre-Tate theorem for genus two and finally we deal with the reduction of the variety of j-invariants.

2.1 Complex multiplication theory

We begin with some definitions and results from the theory of complex multiplication (see [33] for further details). The central notion is that of a *CM field*, defined to be a totally imaginary quadratic extension K of a totally real number field K_0.

For the study of genus two curves we will be interested in quartic CM fields K. We define a *type* of such a field as a pair of non-conjugate embeddings $\Phi = (\phi_1, \phi_2)$ of K in $\mathbb{C}$. If I is an ideal in the ring of integers $\mathcal{O}_K$ of K, we consider $\Phi(I) = \{(\phi_1(\alpha), \phi_2(\alpha)) \subset \mathbb{C}^2, \alpha \in I\}$. The set $\Phi(I)$ is a lattice in $\mathbb{C}^2$ and $\mathbb{C}^2/\Phi(I)$ is an abelian variety A such that $K \subset \mathrm{End}(A) \otimes \mathbb{Q}$. We furthermore make the following restrictions:

1. We assume that K is cyclic or non-Galois. The abelian variety A (for which $\mathrm{End}(A) \otimes \mathbb{Q} = K$) is then absolutely simple. This is a good condition for cryptographic applications since we want $\#A(\mathbb{F}_q)$ to be almost prime.
2. We assume that $h_{K_0} = 1$, which implies that the abelian surface A has a principal polarization. As A is absolutely simple, it follows there exists a genus two curve $\mathcal{C}$ such that $A = \mathrm{Jac}(\mathcal{C})$.
3. We assume moreover that $\mathrm{End}(\mathrm{Jac}(\mathcal{C})) = \mathcal{O}_K$. The above conditions imply $\mathrm{End}(\mathrm{Jac}(\mathcal{C})) \subseteq \mathcal{O}_K$, but for sake of simplicity of both theory and computations, we restrict to the case where this inclusion is an equality. This requires us to address the issue of testing effectively this hypothesis for a given curve $\mathcal{C}$, but we will not treat these algorithms in this article (see however [16]).

Definition 1 *Let $\mathcal{C}$ be a hyperelliptic curve of genus two and K a quartic CM field. We say that $\mathcal{C}$ has* complex multiplication by $\mathcal{O}_K$ *if the endomorphism ring of the Jacobian of the curve is isomorphic to the ring of integers $\mathcal{O}_K$ of K.*

Example 1. As an example we consider $K = \mathbb{Q}(i\sqrt{2+\sqrt{2}})$. The real subfield of K is $\mathbb{Q}(\sqrt{2})$ since $(i\sqrt{2+\sqrt{2}})^2 + 2 = -\sqrt{2}$. Then there exists a curve defined over $\mathbb{Q}$ with model $y^2 = -x^5 + 3x^4 + 2x^3 - 6x^2 - 3x + 1$, whose Jacobian has endomorphism ring $\mathcal{O}_K$. Further details on this example can be found in [38] or [35].

We first recall basic notions of CM theory in genus one, for which we refer to [3]. We begin with a positive squarefree integer D, and compute the class group of $K = \mathbb{Q}(i\sqrt{D})$, which we denote by Cl_K. For complex numbers $(\tau_i)_{i \in [1, h_K]}$, representing the classes in Cl_K, we associate an elliptic curve with period lattice $\mathbb{Z} + \tau_i\mathbb{Z}$. Finally we compute the j-invariant $j_i = j(\tau_i)$ using η-functions and recover the classical Hilbert class polynomial from the definition $H(X) = \prod_{i=1}^{h_K}(X - j_i) \in \mathbb{Z}[X]$, as a monic polynomial over the integers.

The analogous theory for genus two presents several additional technical challenges. The first question is to determine how many isomorphism classes of CM curves are associated to a CM order $\mathcal{O}_K$. We denote this number by h_K^*. In genus one, this number equals the class number h_K, but in higher genus there is no longer a one-to-one correspondence between the ideal classes and the principally polarized abelian surfaces with endomorphism ring $\mathcal{O}_K$, each of which gives rise to an isomorphism class of CM curves. However, for a quartic CM field K with real subfield of class number one, we can make the following statement.

Theorem 1 *Let K be a quartic CM field with real quadratic subfield K_0 of class number 1. If K is cyclic over $\mathbb{Q}$ then there are h_K isomorphism classes and if K is not normal over $\mathbb{Q}$ then there are $2h_K$ isomorphism classes with h_K classes associated to each CM type.*

Remark 1. The Cohen-Lenstra heuristics [11] predict that the class number of the real quadratic field K_0 has class number 1 with density greater than 3/4 so this is expected to apply to this proportion of all quartic CM fields.

The above theorem establishes the degree of the Igusa class polynomials, which vanish on the triples of the CM Igusa invariants (j_1, j_2, j_3). Once their degree is known, we can apply a construction as in the genus 1 CM method for the classical complex CM method. Beginning from a quartic CM field K, we compute the class group of K over $\mathbb{Q}$, and find a representative of each class. Here the representatives are 2×2 matrices called *period matrices* which can be computed from a set of representatives of the class group of K and a fundamental unit of K_0. We refer to [40] for the exact construction of these period matrices $(\Omega_i)_{1 \le i \le h_K^*}$.

Evaluating theta functions at the Ω_i allows to recover the j-invariants $(j_1^{(i)}, j_2^{(i)}, j_3^{(i)})_i$ of the CM curves and joining the j-invariants together gives us the Igusa class polynomials described in [35] or in [40] as

$$H_1 = \prod_{i=1}^{h_K^*}(X - j_1^{(i)}),\ H_2 = \prod_{i=1}^{h_K^*}(X - j_2^{(i)}),\ H_3 = \prod_{i=1}^{h_K^*}(X - j_3^{(i)}).$$

For the purposes of 2-adic lifting we may use normalized invariants j_1, j_2, and j_3, defined in terms of the Igusa-Clebsch invariants A, B, C, D (denoted A', B', C', D' in Mestre [28]), by $j_1 = A^5/8D, j_2 = 2A^3B/D, j_3 = 8A^2C/D$.

2.2 The Lubin-Serre-Tate theorem for genus two

In 1964, Lubin, Serre and Tate [25] proved the existence of the canonical lift of an ordinary abelian variety and gave a way of computing this lift for elliptic curves, extending a result of Deuring [14]. Denote by $\mathbb{Q}_p$ the field of p-adic numbers, and by $\mathbb{Q}_{p^d}$ the unique unramified extension of degree d, and by $\mathbb{Z}_p$ or $\mathbb{Z}_{p^d}$ their respective rings of integers (see e.g. [4] or [21] for background). The fundamental property of the canonical lift $A^{\uparrow}/\mathbb{Z}_{p^d}$ of an ordinary abelian variety $A/\mathbb{F}_{p^d}$ is that $\mathrm{End}(A^{\uparrow}) \cong \mathrm{End}(A)$. Moreover, $A^{\uparrow}$ is actually defined over $\overline{\mathbb{Q}}$. Thus if we can find a curve over $\mathbb{F}_{p^d}$ whose Jacobian is ordinary and has complex multiplication by the ring of integers of a quartic CM field K, we theoretically obtain a curve over $\overline{\mathbb{Q}}$ with complex multiplication by $\mathcal{O}_K$. In the article, p is fixed to 2 and the CM-curves over $\mathbb{F}_{2^d}$ whose Jacobian is ordinary are not rare and can be found easily.

To perform this method explicitly, we require a constructive formulation of the existence theorem for the canonical lift. In genus 1, this is the following theorem (see [39]).

Theorem 2 *Let p be a prime number and d an integer greater than 2. Let $\bar{E}$ be an ordinary elliptic curve over $\mathbb{F}_{p^d}$ with j-invariant $j(\bar{E}) \in \mathbb{F}_{p^d} \backslash \mathbb{F}_{p^2}$. Denote by σ the Frobenius automorphism of $\mathbb{Z}_{p^d}$ and by $\Phi_p(X, Y)$ the p-th modular polynomial. Then the system of equations*

$$\Phi_p(X, X^{\sigma}) = 0 \text{ and } X \equiv j(\bar{E}) \bmod p,$$

has a unique solution $J \in \mathbb{Z}_{p^d}$, which is the j-invariant of the canonical lift E of $\bar{E}$ (defined up to isomorphism).

Generalization to genus two is easier if one speaks about isogeny instead of modular equations:

Theorem 3 *Let $\bar{\mathcal{C}}$ be an ordinary hyperelliptic curve of genus two over $\mathbb{F}_{p^d}$. Then there exists a hyperelliptic curve $\mathcal{C}$ of genus two defined over $\mathbb{Q}_{p^d}$ that is a canonical lift of $\bar{\mathcal{C}}$ (in the sense that the endomorphism ring of the Jacobian is preserved) and furthermore there exists a (p, p)-isogeny between $\mathrm{Jac}(\mathcal{C})$ and $\mathrm{Jac}(\mathcal{C}^{\sigma})$ that reduces to the Frobenius map from $\mathrm{Jac}(\bar{\mathcal{C}})$ to its conjugate.*

In the case where $p = 2$, the Richelot isogeny [5] provides explicit formulae that allow us to translate this theorem into a set of equations that must be satisfied by the defining equation of the canonical lift. A Newton-like process due to Harley is then used to solve it (more details are given in Section 4.1).

General results on the convergence of the Newton process for the AGM is given by Carls [8] for abstract abelian varieties. In our case, we have explicit equations for the Richelot correspondences of curves, for which this theoretical machinery is not required and the convergence can be checked using classical criteria (valuation of the Jacobian matrix of the system of equations).

2.3 Reduction of the moduli subvariety

This section is based on the work of Goren [19] describing the reduction of an abelian surface.

Theorem 4 ([19]) *Let K be a cyclic quartic CM field and A an abelian variety having CM by $\mathcal{O}_K$ the ring of integers of K. Let $\bar{\mathfrak{p}}$ be a prime of $\bar{\mathbb{Q}}$, $\mathfrak{p}_1 = \bar{\mathfrak{p}} \cap \mathcal{O}_K$ and $(p) = \mathfrak{p}_1 \cap \mathbb{Z}$. Assume that p is unramified in K. Then the reduction $A_{\bar{\mathfrak{p}}}$ of $A \bmod \bar{\mathfrak{p}}$ is determined by the decomposition of p in $\mathcal{O}_K$ as follows:*

(i) if $p = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4$ then $A_{\bar{\mathfrak{p}}}$ is ordinary and simple;
(ii) if $p = \mathfrak{P}_1\mathfrak{P}_2$ then $A_{\bar{\mathfrak{p}}}$ is isomorphic to the product of two supersingular elliptic curves;
(iii) if $p = \mathfrak{P}_1$ then $A_{\bar{\mathfrak{p}}}$ is isogenous but not isomorphic to a product of two supersingular elliptic curves.

For a non-normal quartic CM field, which is the generic case, an analogous theorem holds: depending on group theoretic considerations in the Galois group of the normal closure of K, one can decide whether the reduction of the Jacobian of a CM curve is ordinary, intermediate, or supersingular, and whether or not it is simple. We omit the details here and refer instead to Goren [19] for a precise statement.

These results are used at two places. First, they are required in the final curve construction step, to determine a prime of ordinary reduction, a necessary condition for cryptographic use. From the primes of ordinary reduction, we choose a prime p such that a solution to the Igusa class polynomials over $\mathbb{F}_p$ gives a group order which is prime. Second, for the 2-adic method to work, the reduction modulo 2 must be ordinary, otherwise the canonical lift is not well-defined and the lifting algorithm does not apply. Given a CM field K, the theorem describes when there exists an ordinary curve defined over a finite field $\mathbb{F}_{2^d}$ with CM by $\mathcal{O}_K$. As the input to our algorithm is an ordinary curve, rather than the CM field K, this theorem describes the condition at 2 on those CM fields which can be treated by our algorithm.

3 New representation of the CM variety

Before presenting our 2-adic CM method, we explain our modification to the representation of the ideal describing the CM invariants. In the classical CM method, Spallek [35] chose to compute three polynomials H_1, H_2 and H_3, defined as

$$H_1 = \prod_{i=1}^{h_K^*}(X - j_1^{(i)}),\ H_2 = \prod_{i=1}^{h_K^*}(X - j_2^{(i)}) \text{ and } H_3 = \prod_{i=1}^{h_K^*}(X - j_3^{(i)}).$$

Subsequently Weng [40] formalized the classical CM method for genus two in terms of the same polynomials. However these polynomials determine an ideal $(H_1(j_1), H_2(j_2), H_2(j_3)) \subset \mathbb{Q}[j_1, j_2, j_3]$, of degree ${h_K^*}^3$, i.e. defining ${h_K^*}^3$ points $(j_1^{(i_1)}, j_2^{(i_2)}, j_3^{(i_3)})$, of which only the h_K^* solutions $(j_1^{(i)}, j_2^{(i)}, j_3^{(i)})$ determine valid CM curves.

In order to compute the equation of a CM curve, we need to test all ${h_K^*}^3$ candidate solutions to this system of equations to find one of the h_K^* which is known to have the correct endomorphism ring. For each solution we must apply

Mestre's algorithm [28] to find the corresponding curve, then to test a random point on the Jacobian to determine if the group of rational points has the correct order. This overhead is unnecessary since with a few additional relations among the (j_1, j_2, j_3), we determine a complete set of relations for the CM invariants of the desired CM order.

The solution is to find some compact representation for the full ideal of class invariants. Beginning with the minimal polynomial of j_1, $H_1(X) = \prod_{i=1}^{h_K^*}(X - j_1^{(i)}) \in \mathbb{Q}[X]$, we then use Lagrange interpolation to compute

$$G_k(X) = \sum_{i=1}^{h_K^*} j_k^{(i)} \prod_{\substack{\ell=1 \\ \ell \neq i}}^{h_K^*} \frac{X - j_1^{(\ell)}}{j_1^{(i)} - j_1^{(\ell)}} \in \mathbb{Q}[X], \text{ for } k = 2, 3.$$

This solves the problem of having an incomplete specification for the ideal of invariants, since $j_k = G_k(j_1)$ are uniquely determined by any root j_1 of $H_1(X)$. To determine a CM curve over $\mathbb{F}_p$, we solve for a root $\bar{\jmath}_1$ of $H_1(X)$ mod p which determines $\bar{\jmath}_2 = G_2(\bar{\jmath}_1)$ and $\bar{\jmath}_3 = G_3(\bar{\jmath}_1)$, and use Mestre's algorithm to determine a CM curve from the triple $(\bar{\jmath}_1, \bar{\jmath}_2, \bar{\jmath}_3)$.

Modified Lagrange interpolation. The above construction provides an exact description of the CM invariants, but we observe empirically that the coefficient sizes of G_k, in comparison with those for H_k, are larger by a factor of three to four. However, in the formulae for G_k, we can pull out the factor $H_1'(j_1^{(i)})^{-1} = \prod_{k \neq i}(j_1^{(i)} - j_1^{(k)})^{-1}$. Therefore instead of using G_k we consider the polynomials

$$\widehat{H}_k(X) = \sum_{i=1}^{h_K^*} j_k^{(i)} \prod_{\substack{\ell=1 \\ \ell \neq i}}^{h_K^*} (X - j_1^{(\ell)}) \in \mathbb{Q}[X] \text{ for } k = 2, 3,$$

which recover the lost factor, and have coefficients of the same order of magnitude as H_k. The defining relations for our CM invariants can now be expressed as

$$H_1(j_1) = 0,\ H_1'(j_1)j_2 = \widehat{H}_2(j_1),\ H_1'(j_1)j_3 = \widehat{H}_3(j_1).$$

In order to explain the decrease in the size of the polynomial coefficients, we make some assumptions to deal with a notion of size for the j-invariants we are manipulating. Let L be a number field containing all Galois conjugates $j_k^{(i)}$ of the j-invariants. We assume that there exists a notion of a logarithmic height function $h : L \to \mathbb{R}_{>0}$, measuring the size of elements, which satisfies the properties: $h(ab) = h(a) + h(b)$, and $h(a+b) \leqslant \max(h(a), h(b))$, for general a and b. We extend h to a height function on $L[X]$ by: $h(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} h(a_n)$. We also assume that all the j-invariants are random elements of bounded height S. We can then estimate the relative heights of our polynomials H_k, G_k, and $\widehat{H}_k$. We evaluate the size of H_k to be

$$h(H_k) \leq \sum_{i=1}^{h_K^*} iS = \frac{h_K^*(h_K^*+1)}{2} S,$$

since the coefficients of H_k are symmetric polynomials in the $j_k^{(i)}$. A similar calculation for G_k and $\widehat{H}_k$ gives $h(G_k) \leq 2h_K^*(h_K^*-1)S,$ and $h(\widehat{H}_k) \leq h_K^*(h_K^*-1)S$. Under the assumption that the j-invariants behave as random elements, we expect equality to hold for each bound. This analysis, although heuristic, agrees with the empirical results of the algorithm.

Remark 2. We emphasize the fact that this new representation applies both to the classical CM construction and to our new p-adic method that we present in the next section.

4 The 2-adic CM method

In this section we describe our algorithm for computing the Igusa class polynomials H_1, $\widehat{H}_2$, $\widehat{H}_3$ corresponding to a CM order. In the classical approach one starts from a CM field and computes the Igusa class polynomials. In our approach, the input is a genus 2 curve defined over a small finite field $\mathbb{F}_{2^d}$, for some small d, and we reconstruct the class polynomials associated to its canonical lift. The input curves for this construction are defined over a tiny field of no cryptographic interest, but via their canonical lift we find their class invariants over $\mathbb{Q}$, which can then be reduced modulo p to produce curves of cryptographic application over some large prime field $\mathbb{F}_p$. We note that the class polynomials we find may determine a proper irreducible factor of the CM class invariants, in the case the invariants fall into distinct Galois orbits. However, for their application to cryptography this only aids in the rational reconstruction phase of our algorithm.

The algorithm proceeds as follows. Since d is small, one can easily compute all the data related to the input curve $\mathcal{C}$, in particular the endomorphism ring $\mathcal{O}$ of its Jacobian, which we assume to be the maximal order of a CM field K. The canonical lift of $\mathcal{C}$ is then computed to a high precision, so that we can get a good 2-adic approximation of its Igusa invariants. Theorem 1 gives a way to predict the degree h_K^* of the class polynomials. From this information, if the precision is sufficient, there is a unique possibility left for the polynomials H_1, $\widehat{H}_2$, $\widehat{H}_3$. These can be computed by running the LLL algorithm on a matrix built from powers of the invariants of the canonical lift. Algorithm 1 gives a summary of the algorithm, and in the next two subsections we discuss the details.

4.1 Computing the canonical lift

Canonical lifts were introduced in cryptography for the purpose of point counting by Satoh [32] for elliptic curves. After many improvements by several people, this ended up in a very fast method that runs in a time which is almost-linear in the required precision. A precise description and comparison of the various methods in the elliptic case can be found in [39] to which we refer for additional reading. Two genus 2 variants have been introduced by Mestre [27, 26], based on the Richelot isogeny or on the Borchardt mean. The latter variant has been developed in detail by Lercier and Lubicz [23].

Algorithm 1 The 2-adic CM method

Input : An ordinary genus 2 curve $\mathcal{C}$ defined over $\mathbb{F}_{2^d}$ having CM by an order $\mathcal{O}$;
Output : $(H_{1,\mathfrak{irr}}, \widehat{H}_{2,\mathfrak{irr}}, \widehat{H}_{3,\mathfrak{irr}})$ which determine an irreducible factor of the class invariants $(H_1, \widehat{H}_2, \widehat{H}_3)$ of $\mathcal{O}$.

1: Compute the j-invariants of $\mathcal{C}$ and choose an arbitrary lift to $\mathbb{Z}_{2^d}$;
2: Compute the canonical lifts $(j_1, j_2, j_3) \in (\mathbb{Z}_{2^d})^3$, i.e. the j-invariants of the canonical lift of $\mathcal{C}$;
3: Determine the degree h_K^* of $(H_1, \widehat{H}_2, \widehat{H}_3)$;
4: Apply the LLL algorithm with input h_K^* and powers of (j_1, j_2, j_3);
5: Retrieve the result of LLL, that is the polynomials $H_{1,\mathfrak{irr}}$, $\widehat{H}_{2,\mathfrak{irr}}$ and $\widehat{H}_{3,\mathfrak{irr}}$ verifying

$$H_{1,\mathfrak{irr}}(j_1) = 0, \quad H'_{1,\mathfrak{irr}}(j_1) \cdot j_2 = \widehat{H}_{2,\mathfrak{irr}}(j_1) \quad \text{and} \quad H'_{1,\mathfrak{irr}}(j_1) \cdot j_3 = \widehat{H}_{3,\mathfrak{irr}}(j_1);$$

6: Return the triple $\left(H_{1,\mathfrak{irr}}, \widehat{H}_{2,\mathfrak{irr}}, \widehat{H}_{3,\mathfrak{irr}}\right)$.

For the present work, we used the former approach, based on Richelot isogenies, together with the asymptotically fast lifting algorithm of Harley. Since this is not well described in the literature, we say a few words about it.

The main point is that Richelot isogeny as described in [5] gives relations between the defining equations of genus 2 curves whose Jacobian are $(2,2)$-isogenous. We take equations in the Rosenhain form: $y^2 = x(x-1)(x-\lambda_0)(x-\lambda_1)(x-\lambda_\infty)$. Putting $\Lambda = (\lambda_0, \lambda_1, \lambda_\infty)$, we can realize the relations coming from Richelot isogeny as a system of polynomial maps $\Phi = (\Phi_1, \Phi_2, \Phi_3)$ from $\mathbb{Q}_{2^d}^6 = \mathbb{Q}_{2^d}^3 \times \mathbb{Q}_{2^d}^3$ to $\mathbb{Q}_{2^d}^3$, such that two curves of Rosenhain invariants Λ and Λ' have Jacobians related by a $(2,2)$-isogeny if and only if $\Phi(\Lambda, \Lambda') = 0$. Hence, according to Theorem 3, the Rosenhain invariants Λ of the canonical lift of the curve $\mathcal{C}$ we are interested in must verify $\Phi(\Lambda, \Lambda^\sigma) = 0$. Before giving the explicit formulae for Φ, we sketch how Harley's algorithm can be adapted to the multivariate setting.

Assume we have an approximation $\Lambda_0 \in \mathbb{Q}_{2^d}^3$ to the Rosenhain invariants Λ of the canonical lift, correct to precision 2^k. Let $\Lambda_1 \in \mathbb{Z}_{2^d}^3$ be such that $\Lambda = \Lambda_0 + 2^k \Lambda_1$. Then Λ satisfies the equation $\Phi(\Lambda, \Lambda^\sigma) = 0$, which rewrites as

$$0 = \Phi(\Lambda_0 + 2^k\Lambda_1, \Lambda_0^\sigma + 2^k\Lambda_1^\sigma) = \Phi(\Lambda_0, \Lambda_0^\sigma) + 2^k d\Phi(\Lambda_0, \Lambda_0^\sigma) \begin{bmatrix} \Lambda_1 \\ \Lambda_1^\sigma \end{bmatrix} \bmod 2^{2k},$$

from which Λ_1 can be deduced. Indeed, since $\Phi(\Lambda_0, \Lambda_0^\sigma) \equiv 0 \bmod 2^k$, the equation in Λ_1 can be restated as $\Lambda_1^\sigma + A\,\Lambda_1 + B = 0$, where A is a 3×3 matrix over $\mathbb{Z}_{2^d}$, and B and Λ_1 are vectors in $\mathbb{Z}_{2^d}^3$. Another level of recursive Newton-lifting is used for solving this so-called Artin-Schreier equation.

In this brief description, we have freely assumed that computing σ is a cheap operation, which is unfortunately not true if one takes an arbitrary defining polynomial $f(x)$ for the extension field $\mathbb{Q}_{2^d} = \mathbb{Q}_2[x]/(f(x))$. The trick is to choose the polynomial $f(x)$ such that f divides $x^{2^d} - x$, which in turn implies that $t^\sigma = t^2$, where t is the defining element of the extension field. The computation of such an f is done, again, by a Newton lifting algorithm based on the equation

$f(x^2) = f(x)f(-x)$, which is easily seen to be satisfied by the polynomial we are looking for. We refer to [39] for a more precise description.

Let us now describe the polynomial maps Φ given by the Richelot's isogeny. For clarity, we give them in an implicit form that introduces new intermediate variables. Let λ_0, λ_1 and λ_∞ be the starting Rosenhain invariants. The images λ_0^σ, λ_1^σ and λ_∞^σ of λ_0, λ_1 and λ_∞ by the second power Frobenius automorphism are given by the following formulae:

$$\lambda_0^\sigma = \frac{(u_1 - v_\infty)(w_0 - v_0)}{(u_1 - v_0)(w_0 - v_\infty)},\ \lambda_1^\sigma = \frac{(u_1 - u_\infty)(w_1 - v_0)}{(u_1 - v_0)(w_1 - v_\infty)} \text{ and } \lambda_\infty^\sigma = \frac{(u_1 - v_\infty)(u_\infty - v_0)}{(u_1 - v_0)(u_\infty - v_\infty)},$$

where (u_1, u_∞), (v_0, v_∞) and (w_0, w_1) are the respective roots of the polynomials

$$\begin{array}{l} U^2 - 2\lambda_\infty U + \lambda_\infty(1 + \lambda_1) - \lambda_1, \\ V^2 - 2\lambda_\infty V + \lambda_0\lambda_\infty, \text{ and} \\ (\lambda_0 - 1 - \lambda_1)W^2 + 2\lambda_1 W - \lambda_0\lambda_1. \end{array}$$

Remark 3. We need to pay attention to the valuations of our Rosenhain invariants. Assuming that we begin with $\lambda_0 \equiv 0 \bmod 4$, $\lambda_1 \equiv 1 \bmod 4$ and $\mathrm{val}(\lambda_\infty) = -2$, we choose the labeling of the roots of our quadratic polynomials such that $v_0,\ w_0 \equiv 0 \bmod 2,\ u_1,\ w_1 \equiv 1 \bmod 2$, and $\mathrm{val}(u_\infty),\ \mathrm{val}(v_\infty) < 0$, from which $\lambda_0^\sigma \equiv 0 \bmod 4$, $\lambda_1^\sigma \equiv 1 \bmod 4$ and $\mathrm{val}(\lambda_\infty^\sigma) = -2$ follows.

4.2 Recognizing class polynomials in $\mathbb{Q}[X]$

In this section we explain how we use the LLL algorithm to recover the minimal polynomials over $\mathbb{Z}$ of the canonical lifted j-invariants. Let $\Lambda = \langle b_1, \ldots, b_m \rangle$ be a lattice and let $\det(\Lambda)$ be its determinant. Minkowski's inequality gives the upper bound $\sqrt{m/2\pi e}\det(L)^{1/m}$, for the norm of the shortest lattice vector, and in a random lattice, one expects a minimal length vector to be close to this norm. The LLL algorithm outputs a basis of short vectors, and if we construct Λ to have a known vector $v \in \Lambda$ of norm much smaller than this bound, then, heuristically, it will be the shortest vector in Λ.

Let $\mathbb{Z}_{2^d}$ be an extension of $\mathbb{Z}_2$ of degree d with $\mathbb{Z}_2$-basis $1, w_1, \ldots, w_{d-1}$. Let $\alpha \in \mathbb{Z}_{2^d}$ generate $\mathbb{Z}_{2^d}$, and $\tilde{\alpha}$ be an approximation of α modulo a high power of 2, say $\alpha \equiv \tilde{\alpha} \bmod 2^N$. We assume that we know the degree s of its minimal polynomial $f(x) \in \mathbb{Z}[x]$, i.e. $f(x) = a_s x^s + \ldots + a_0$ where the $(a_i) \subseteq \mathbb{Z}$ are unknown. The degree s of the minimal polynomial is the degree of an irreducible factor of Igusa class polynomials, whose degree is h_K^*. In order to determine the (a_i), we determine a basis of the left kernel in $\mathbb{Z}^{s+d+1}$ of the matrix

$$\begin{pmatrix} A \\ 2^N I_d \end{pmatrix}, \text{ where } A \text{ is the } (s+1) \times d \text{ matrix: } \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \alpha_{1,0} & \alpha_{1,1} & \cdots & \alpha_{1,(d-1)} \\ \vdots & & & \vdots \\ \alpha_{s,0} & \alpha_{s,1} & \cdots & \alpha_{s,(d-1)} \end{pmatrix},$$

with $\alpha_{j,k}$ defined by $\alpha^j = \alpha_{j,0} + \alpha_{j,1} w_1 + \ldots + \alpha_{j,(d-1)} w_{d-1}$.

In order to compute the basis of the left kernel, we apply the LLL algorithm in the same way as described in [10]. This kernel is a lattice Λ, in which the coefficients of the minimal polynomial of α are part of a short vector. Indeed, if $a_0, \ldots, a_s$ are integers with $|a_i| \ll 2^N$ such that $a_s\alpha^s + \ldots + a_0 \equiv 0 \bmod 2^N$, then $(a_0, \ldots, a_s, \varepsilon_1, \ldots, \varepsilon_d)$ will be a short vector in Λ, for appropriate integers (ε_i). Any other solution that is not proportional to the (a_i) will differ by an element of $\Lambda_0 + 2^N\mathbb{Z}^{s+d+1}$, where Λ_0 is generated by the $c_d\alpha^{d+i} + \ldots + c_0\alpha^i \equiv 0 \bmod 2^N,\ 1 \leq i \leq s-d$, coming from the minimal polynomial $g(x) = c_dx^d + \cdots + c_0$ of α in $\mathbb{Z}_2[x]$ having arbitrary coefficients in $\mathbb{Z}_2$. If the precision N is sufficiently high, we expect the unique solution $(a_0, \ldots, a_s)$ to appear as the shortest vector in the LLL-reduced lattice basis.

We remark that we can easily compute the image of (j_1, j_2, j_3) by the Frobenius σ and therefore we have access to the powers of (j_1, j_2, j_3) and $(j_1^{\sigma^i}, j_2^{\sigma^i}, j_3^{\sigma^i})$ for $i \in [1, d]$. Therefore we can use this information as input of our LLL algorithm. It implies a more complicated recognition phase where we have to use the subresultant algorithm to recognize our minimal polynomials. Moreover an explosion of the coefficient size in the course of the algorithm leads us to use modular arithmetic and the Chinese remainder theorem for our computations.

5 Complexity and comparison with other methods

5.1 Complexity of the 2-adic CM method

The two costly steps of the 2-adic CM method are the computation of the canonical lift and the reconstruction of the polynomials using LLL. Those two steps highly depend on the precision k at which we have to compute the canonical lift in order to recover the full polynomials. This precision k depends itself on the sizes of the polynomial H_1, $\widehat{H}_2$, $\widehat{H}_3$, for which no bound (that would depend on the class number of K) is known. Hence we shall keep k in our formulae, although this is not a parameter under control.

By using advanced algorithms coming from point counting, the canonical lift computation takes a time which is essentially linear in the precision k. More precisely it has a complexity $O(M(dk)\log(k))$ where $M(dk)$ is the time for multiplying integers with dk bits, that is $O(dk)$ up to logarithmic factors.

The complexity of the LLL step involves the further parameter h_K^*, which is the degree of the polynomials we are trying to reconstruct. Using the classical LLL algorithm, we end up with a complexity of $O((h_K^*+d)^6k^3)$. The L^2 variant of Nguyễn and Stehlé [30] has a better general complexity of $O((h_K^*+d)^5(h_K^*+d+k)k)$, and in our case the structure of the lattice gives us an improved complexity of $O((h_K^*+d)^4(h_K^*+d+k)k)$.

Now we will analyze what we could expect from the PSLQ algorithm. In [1], given an input of h_K^*+d complex numbers whose integer relation is bounded by 2^k, the PSLQ algorithm is claimed to have a number of iterations in $O((h_K^*+d)^3 + (h_K^*+d)^2k)$. Each iteration consists of four steps. Both for the complexity in the dimension and in the precision the bottleneck step is the third step, Hermite's reduction and matrix multiplication. Therefore the complexity of one iteration is $O((h_K^*+d)^3k)$. The total complexity of PSLQ seems to be $O((h_K^*+d)^6k + (h_K^*+d)k^2)$ thus we do not expect any improvement from using a 2-adic version of PSLQ.

5.2 Comparison with other methods

The comparison with the classical CM method [35, 40] is only valid for inputs at which their outputs coincide, since the inputs to each algorithm is different. In the 2-adic method one treats only CM fields where the ideal (2) has a special structure, and moreover the input is not the field but a hyperelliptic curve over a small finite field. In the classical CM method one starts directly from a CM field, with the requirement that the class number of the real subfield is 1. The main advantage of the 2-adic method compared to the classical method is that the complex floating point evaluation of theta constants at the period matrices (which is the bottleneck in the classical method) is replaced by a p-adic canonical lifting procedure for which we have precise control over precision and precision loss (there is none). Furthermore, the time-complexity of the evaluation of theta constants is quadratic in the required precision, whereas the canonical lift is essentially linear in the precision. On the other hand, the drawback of the 2-adic CM method is that the reconstruction step is much more expensive than in the classical case, since the step of building a polynomial from its roots is replaced by a call to the LLL algorithm. In this later case, the complexity becomes again quadratic in the precision. In other words, by changing the method, we have moved the bottleneck of the approach from the first step to the second step.

We can also compare to the CRT approach [9, 16]. In that case, to be able to build a class polynomial whose coefficients have k bits, one needs to use $O(k)$ small finite fields $\mathbb{F}_{p_i}$, where p_i is $O(k)$. Finding the appropriate curves implies $O(p_i^3)$ steps for each p_i, since we essentially have to enumerate all isomorphism classes over the field $\mathbb{F}_{p_i}$. Hence the complexity is more than quadratic in the precision, so that the CRT method is not competitive with the other methods in terms of required precision. This ignores the endomorphism ring computation which is exponential in p_i in the worst case (but might be controlled by a more selective sieving for CRT primes).

5.3 Experiments

All of the experiments we carried out were written using `Magma` [12] and `C` routines. The 2-adic arithmetic is taken from an experimental `gmp`-style library called `Mploc` which was developed by E. Thomé [37]. It currently contains far more than the 2-adic arithmetic, including efficient arithmetic in $\mathbb{Q}_p$, $\mathbb{Q}_p[X]$, and extensions of $\mathbb{Q}_p$. We use `NTL` [34] library for the floating-point LLL routine, as at the time we developed our program, Stehlé's LLL `C` routines were not available [36]. All the experiments were conducted on a 2.4 GHz Athlon 64. On such a computer, computing irreducible factors of Igusa class polynomials of degree less than twenty is a question of minutes.

Example. Let $\mathcal{C}$ be the curve of equation $y^2 + h(x)y + f(x) = 0$ over $\mathbb{F}_{32} = \mathbb{F}_2[t]/(t^5 + t^2 + 1)$, with $f(x) = x^5 + t^{20}x^3 + t^{17}x^2 + t^{19}x$ and $h(x) = x^2 + t^9x$. The curve is ordinary and has CM by the maximal order of $K = \mathbb{Q}(i\sqrt{75 + 12\sqrt{17}})$. The field K is non-normal and its class number is 50; so we have $h_K^* = 100$ isomorphism classes of principally polarized abelian varieties.

Looking for a minimal polynomial of the lifted value of j_1, the LLL algorithm produced a plausible answer of degree 50. A more subtle analysis of the Galois theory in fact predicts that the class polynomial of degree 100 is reducible over the rationals, splitting in two factors of degree 50. Using our method, we produce one of these two factors $H_1(X)$, with the corresponding polynomials $\widehat{H}_2(X)$ and $\widehat{H}_3(X)$. The leading coefficient of H_1 is $3^{50}11^{156}17^{60}23^{72}41^{24}73^{12}83^{12}181^{48}691^{12}$, consistent with the theory of Goren-Lauter [20], and reduction at a large prime gave rise to a Jacobian whose group of rational points agreed with the expected order for this CM field.

For this example, we used a 2-adic precision of 65000 bits, and the running time to lift the curve and compute the invariants was 20 seconds. The subsequent lattice reductions took about one day. This confirms that the bottleneck is in the second step, as predicted by the complexity estimates, and suggests that an improved strategy would be to lift additional j-invariants to reduce the size of the lattice in the reduction phase.

6 Conclusion and perspectives

This work presents a new p-adic method for building Igusa class polynomials for genus two curves, that can be used to efficiently produce CM curves suitable for cryptography. Our method makes use of p-adic lifting techniques borrowed from point counting algorithms. The algorithm performs well in practice and has allowed us to treat much larger class numbers than previously reported in the literature.

In order to deal with such large degree class polynomials, we were led to introduce a new representation for the ideal of CM points, so that the final step of the CM method — namely reducing the polynomials modulo an appropriate prime p and constructing the corresponding curve equation — no longer requires a combinatorial search for one valid tuple of invariants for each ${h_K^*}^3$ tuple when using class polynomials of degree h_K^*.

Our work is based on curves of characteristic 2, which places a restriction on which CM fields we can treat. This is analogous to the condition on discriminants treatable by the CM construction in genus 1 using reduced class polynomials in terms of Weber functions. Extending this algorithm to other small characteristics p would impose an independent condition so that more CM fields could be treated. Such algorithms are the subject of ongoing investigation, motivated by this research.

As the discussion of complexity issues indicates, the different methods for building Igusa class polynomials (complex analytic, p-adic analytic, CRT) all have advantages and limitations. Combining them in order to take advantage of the best of each method is something that should be explored. For example, an algebraic formula for the exact leading coefficient of the Igusa class polynomials (see [20]) would have benefit to a greater or lesser extent in each of these methods. We note that the bottleneck of the classical CM method is the evaluation of theta constants. Recently, Dupont [15] developed new algorithms for this task, yielding a huge performance improvement for the classical CM method. Further investigation of the limiting steps for the classical and p-adic methods will determine in the end which algorithm applies most effectively to a given problem.

References

1. S. Arno, D. H. Bailey, and H. R. P. Ferguson. Analysis of PSLQ, an integer relation finding algorithm. *Math. Comp.*, 68(225):351–369, January 1999.
2. R. Avanzi. Aspects of hyperelliptic curves over large prime fields in software implementations, 2003. Preprint (available at `http://eprint.iacr.org/2003/253`).
3. A. Borel, S. Chowla, C. S. Herz, K. Iwasawa, and J.-P. Serre. *Seminar on complex multiplication.* Number 21 in Lecture Notes in Math. Springer, 1966.
4. Z. I. Borevitch and I. R. Shafarevich. *Number theory*, volume 20 of *Pure and Applied Mathematics.* Academic Press Inc., New-York, 1966.
5. J.-B. Bost and J.-F. Mestre. Moyenne arithmético-géométrique et périodes de courbes de genre 1 et 2. *Gaz. Math. Soc. France*, 38:36–64, 1988.
6. R. Bröker and P. Stevenhagen. Elliptic curves with a given number of points. In D. Buell, editor, *ANTS-VI*, vol. 3076 of LNCS, pages 117–131. Springer-Verlag, 2004.

7. R. M. Bröker. *Constructing elliptic curves of prescribed order.* PhD thesis, Thomas Stieltjes Institute for Mathematics, 2006.
8. R. Carls. *A generalized arithmetic geometric mean*. PhD thesis, Rijksuniversiteit Groningen, 2004.
9. J. Chao, K. Matsuo, H. Kawashiro, and S. Tsujii. Construction of hyperelliptic curves with CM and its application to cryptosystems. In T. Okamoto, editor, *ASIACRYPT 2000*, vol. 1976 of LNCS, pages 259–273. Springer-Verlag, 2000.
10. H. Cohen. *A course in algorithmic algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer–Verlag, 1993. Second corrected printing, 1995.
11. H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.
12. The University of Sydney Computational Algebra Group. Magma online handbook, 2006. `http://magma.maths.usyd.edu.au/magma/htmlhelp/MAGMA.htm`.
13. J.-M. Couveignes and T. Henocq. Action of modular correspondences around CM points. In C. Fieker and D. R. Kohel, editors, *ANTS-V*, vol. 2369 of LNCS, pages 234–243. Springer-Verlag, 2002.
14. M. Deuring. Die Typen der Multiplikatoringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen*, 14:197–272, 1941.
15. R. Dupont. *Moyenne arithmético-géométrique, suites de Borchardt et applications.* PhD thesis, École polytechnique, 2006.
16. K. Eisentrager and K. Lauter. Computing Igusa class polynomials via Chinese Remainder Theorem. Preprint (available at `http://arxiv.org/abs/math.NT/0405305`), 2004.
17. P. Gaudry. Fast genus 2 arithmetic based on Theta functions, 2005. Preprint (available at `http://eprint.iacr.org/2005/314`).
18. P. Gaudry and É. Schost. Construction of secure random curves of genus 2 over prime fields. In C. Cachin and J. Camenisch, editors, *Eurocrypt 2004*, vol. 3027 of LNCS, pages 239–256. Springer–Verlag, 2004.
19. E. Z. Goren. On certain reduction problems concerning abelian surfaces. *Manuscripta math.*, 94:33–43, 1997.
20. E. Z. Goren and K. Lauter. Class invariants for quartic CM fields. Preprint (available at `http://arxiv.org/abs/math.NT/0404378`), 2004.
21. N. Koblitz. *p-adic Numbers, p-adic Analysis and Zeta-Functions*, volume 58 of *Graduate Texts in Mathematics*. Springer–Verlag, 1984.
22. T. Lange and M. Stevens. Efficient doubling on genus two curves over binary fields. vol. 3357 of LNCS, pages 170–181. Springer-Verlag, 2005. In H. Handschuhand M.A. Hasan, editors, *SAC 2004*.
23. R. Lercier and D. Lubicz. A quasi quadratic time algorithm for hyperelliptic curve point counting. To appear in J. Ramanujan Math. Soc.
24. R. Lercier and E. Riboulet-Deyris. Elliptic curves with complex multiplication. Posting to the Number Theory List, available at `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0401&L=nmbrthry&P=R305`, 2004.
25. J. Lubin, J.-P. Serre, and J. Tate. Elliptic curves and formal groups. In *Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry, Whitney Estate, Woods Hole, Massachusetts, July 6-July 31, 1964*, 1964. Scanned copies available at `http://www.ma.utexas.edu/users/voloch/lst.html`.
26. J.-F. Mestre. Algorithmes pour compter des points de courbes en petite caractéristique et en petit genre. Talk given in Rennes in March 2002. Notes written by D. Lubicz.

27. J.-F. Mestre. Utilisation de l'AGM pour le calcul de $E(F_{2^n})$. Lettre adressée à Gaudry et Harley, Décembre 2000.
28. J.-F. Mestre. Construction de courbes de genre 2 à partir de leurs modules. In T. Mora and C. Traverso, editors, *Effective methods in algebraic geometry*, vol. 94 of *Progr. Math.*, pages 313–334. Birkhäuser, 1991.
29. A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Trans. Fundamentals*, E84-A(5), May 2001.
30. P. Nguyễn and D. Stehlé. Floating-point LLL revisited. In *Eurocrypt 2005*, vol. 3494 of LNCS, pages 215–233. Springer–Verlag, 2005.
31. J. Pelzl, T. Wollinger, J. Guajardo, and C. Paar. Hyperelliptic curve cryptosystems: Closing the performance gap to elliptic curves. Preprint, 2003.
32. Takakazu Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000.
33. G. Shimura. *Abelian Varieties with complex multiplication and modular functions*. Princeton University Press, revised edition, 1998.
34. V. Shoup. NTL: A library for doing number theory. `http://www.shoup.net/ntl/`.
35. A.-M. Spallek. *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*. PhD thesis, Universität Gesamthochschule Essen, July 1994.
36. D. Stehlé. `fplll-1.2` a lattice LLL-reduction program, 2006. available at `http://www.loria.fr/~stehle`.
37. E. Thomé. Multi-Precision for LOCal-fields library, 2006. still under development, see `http://www.loria.fr/~thome`.
38. P. van Wamelen. Examples of genus two CM curves defined over the rationals. *Math. Comp.*, 68(225):307–320, January 1999.
39. F. Vercauteren. *Computing zeta functions of curves over finite fields*. PhD thesis, Katholieke Universiteit Leuven, 2003.
40. A. Weng. *Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation*. PhD thesis, Universität GH Essen, 2001.

A Cryptographic CM curve generation on one example

We start with the curve $\mathcal{C}$ of equation $y^2+h(x)y+f(x)=0$ over $\mathbb{F}_8=\mathbb{F}_2[t]/(t^3+t+1)$, with $f(x)=x^5+t^6x^3+t^5x^2+t^3x$ and $h(x)=x^2+x$. The curve is ordinary and has complex multiplication by the maximal order of $K=\mathbb{Q}(i\sqrt{23+4\sqrt{5}})$. The field K is non-normal and its class number is 3; so we have 6 isomorphism classes of principally polarized abelian varieties. We apply our algorithm and compute the canonical lift of $\mathcal{C}$ to high precision (in fact, a posteriori, we see that 1200 bits are enough) and get its invariants. From this we reconstruct the minimal polynomial H_1 and the corresponding $\widehat{H}_2$ and $\widehat{H}_3$. As expected, the degree of H_1 is 6.

$$
\begin{aligned}
H_1 = {} & 2^{18}5^{36}7^{24}\ T^6 \\
& - 1118773039927368977400974047014016967290290543651580810546875000\,0\ T^5 \\
& + 50151252769059167950442083276747142151268450140383454764466298826367187500\,0\ T^4 \\
& - 1011240924278739178667628463373057504761454313557202566746822143270426385780826292\,3\ T^3 \\
& + 1182870002505886675645407447394061543981359784477927719285355412407973869920918282135218\,75\ T^2 \\
& - 2^1 3^{50} 5^{10} 11^1 13^1 53^1 701^1 16319^1\, 6993879349494895356919887000403213192686857808489931\,7\ T \\
& + 3^{60} 5^{15} 23^5 409^5 179364113^5 \\
\widehat{H}_2 = {} & 2^{-3}(2734249284974589542086559782016563911333032280921936035156250000\ T^5 \\
& + 57554607277149797568849387967258354564256002479144001401149377453125000000\ T^4 \\
& + 240213781608540858296636148041292340997729704037676050101454338233818948386188792\,3\ T^3 \\
& - 75691166837057576824962404339816428897154828109931810138346946500235981947587900092046875\ T^2 \\
& + 2^1 3^{48} 5^{10}\, 35828519670812312117443096939126403484719666514876459782054400437\ T \\
& - 3^{58} 5^{15} 11^1\, 13^2 23^3 409^3 23879^1 179364113^3\, 370974539856105277) \\
\widehat{H}_3 = {} & 2^{-4}(20062002297726501938753962499493388123426921176910400390625000\,0\ T^5 \\
& - 230064674317649756972825458821889005149084689925547595360431355781250000\,00\ T^4 \\
& + 615017294619678068611319414718144161545088218260214211563850151291136646894987547\ T^3 \\
& - 14310698742415340178789612716269299249317950024503557714370659520249839645781463819312875\ T^2 \\
& - 2^1 3^{46} 5^8 13^1 61^1 18373951326869^1\, 2571328858726120821210798572446805865150973416090\,7\ T \\
& + 3^{55} 5^{13} 23^2 409^2 23561^1 440131^1 179364113^2\, 451986402352017881724712641689)
\end{aligned}
$$

From the Newton polygon of H_1 for the 2-adic valuation, we see that there are three roots that have valuation 0, and the others have negative valuation. Hence only three of the curves have good reduction modulo 2. However, since H_1 is irreducible over $\mathbb{Q}$, the 2-adic lifted invariants of any of the three conjugate curves yields the whole H_1.

Choosing the 120-bit prime $p = 954090659715830612807582649452910809$, and solving a norm equation in the endomorphism ring $\mathcal{O}_K$, we know that a solution (j_1,j_2,j_3) to the Igusa class polynomials gives the invariants of a genus 2 curve whose Jacobian has prime order

$$910288986956988885753118558284481029311411128276048027584310525408884449$$

of 240-bits. We find a corresponding curve:

$$
\begin{aligned}
\mathcal{C}: y^2 = x^6 & + 827864728926129278937584622188769650\,x^4 \\
& + 102877610579816483342116736180407060\,x^3 \\
& + 335099510136640078379392471445640199\,x^2 \\
& + 351831044709132324687022261714141411\,x \\
& + 274535330436225557527308493450553085
\end{aligned}
$$

and a test of a random point on the Jacobian verifies the group order.