Construction of Hyperelliptic Curves with CM and Its Application to Cryptosystems

Jinhui Chao[1], Kazuto Matsuo[2], Hiroto Kawashiro[3], and Shigeo Tsujii[3]

[1] Dept. of Electrical, Electronic, and Communication Engineering,
Faculty of Science and Engineering, Chuo University,
1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8851 Japan
jchao@elect.chuo-u.ac.jp
[2] Toyo Communication Equipment Co., Ltd.,
1-1, Koyato 2, Samukawa-machi, Koza-gun,
Kanagawa-pref., 253-0192 Japan
matuo@toyocom.co.jp
[3] Dept. of Information and System Engineering,
Faculty of Science and Engineering, Chuo University,
1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8851 Japan
tsujii@ise.chuo-u.ac.jp

Abstract. Construction of secure hyperelliptic curves is of most important yet most difficult problem in design of cryptosystems based on the discrete logarithm problems on hyperelliptic curves. Presently the only accessible approach is to use CM curves. However, to find models of the CM curves is nontrivial. The popular approach uses theta functions to derive a projective embedding of the Jacobian varieties, which needs to calculate the theta functions to very high precision. As we show in this paper, it costs computation time of an exponential function in the discriminant of the CM field. This paper presents new algorithms to find explicit models of hyperelliptic curves with CM. Algorithms for CM test of Jacobian varieties of algebraic curves and to lift from small finite fields both the models and the invariants of CM curves are presented. We also show that the proposed algorithm for invariants lifting has complexity of a polynomial time in the discriminant of the CM field.

1 Introduction

Hyperelliptic curves and more general Jacobian varieties over finite fields have been used to build cryptosystems in recent years e.g. [20]. The cryptosystems based on these curves are recently under intensive investigation on their integrity. The generic square-root attacks works for arbitrary Abelian groups but cost exponential time in general. Various "reduction" attack initiated by the MOV attacks[23] intended to transform the discrete logarithm problem on the Jacobian varieties to some simpler and easier problems, e.g. the discrete logarithm problems on the multiplicative or the additive group of the ground field. Such attacks are effective to certain curves with special properties[30]. Another generic attack, the "smooth divisor attack" [2],[24] solves the discrete logarithm

T. Okamoto (Ed.): ASIACRYPT 2000, LNCS 1976, pp. 259–273, 2000.

problem on curves of large genera in subexponential time. In particular, an attack on hyperelliptic curves of genus six is reported recently [14][11]. In spite of these researches, the discrete logarithm problems on generic curves with small genera and almost-prime orders still seemed to be at least as intractable as on the elliptic curves.

Besides, cryptosystems based on Abelian varieties of genus $g > 1$ will have also shorter word-length for the same key size than the systems on elliptic curves, which means advantages in processing, transmission and implementation. Moreover, since there is much richer isogenous classes of such curves than elliptic curves, more secure and flexible application of the cryptosystems can be expected. However, construction of secure hyperelliptic curves seems far more nontrivial than elliptic curves.

The order-counting algorithms or Schoof's algorithm for elliptic curves is extended to hyperelliptic curves. e.g. [1] shown an algorithm to calculate orders of Jacobians for curves of genus 2 in random polynomial time. [29] presented a deterministic polynomial time order-counting algorithm of $O(\log p)^{\Delta}$. However, it is observed that the $\Delta > \exp(\exp(2g+1))$ where g is the genus of the curve [17]. [17] also extended Schoof's algorithm to plane curves over algebraic number fields with arbitrary singularity, with cost of random polynomial time $O((\log p)^{\delta})$, where the $\delta = (2g+1)^{O(1)}$. The present record of these kind of algorithms is by [3] which gave a deterministic algorithm improving [29] and cost $O((\log q)^{O(g^6)})$. All these general order counting algorithms are still too costly to be used in practical calculation and seems difficult to implement. Besides, they have to repeat the whole order counting calculations many times until an almost prime Jacobian is found. In [20], the order of a Jacobian variety at small finite fields is counted then lift the curve by the Weil conjecture This method is very fast although the number of secure curves can be found seems limited. Besides, these curves are also subjected to attacks using large automorphism groups [11].

Another approach which has been pursued in recent years is to use the simple factors of the Jacobian varieties of a special kind of curves called modular curves [13][38][39] using analytical embedding by theta functions [25][26]. Besides the computation cost for high precision expansion of these modular functions, since their method to count the order by the Eichler-Shimura formula is of exponential time, it seems that Jacobian varieties can be built over finite fields with characteristic no more than ten digits. Considering that presently used curves are with genera less than or equal to four, one can only count Jacobian varieties with order of forty digits, still quite insufficient for cryptographic applications. A recent report shown a straightforward implementation of Schoof-like algorithm on hyperelliptic curves using Cantor's analogue of the division polynomials of elliptic curves, but it can only count the Jacobian varieties with orders less than, again, forty digits[15].

A hopeful direction is to use CM curves, or the algebraic curves defined over algebraic number fields whose Jacobian varieties with complex multiplications. In fact, fast algorithms which design secure Jacobian varieties over finite field using CM curves have been shown in [7][8]. These algorithms have complexity as

a polynomial in the characteristic of the finite ground fields[8]. The CM curves have nice properties to make order-counting easy and enough randomness for security as well. Furthermore, they have a potential advantage in implementation of cryptosystems. In particular, once one has an arbitrary CM curve over an algebraic number field, he will be able to design different secure curves or their Jacobian varieties over finite fields based on the same CM curve very quickly by changing the definition finite fields. It is then convenient in practice since when one wishes to update the system periodically by changing the curves he needs not to transmit a new curve over an insecure channel.

Recently, [11] presents an attack on curves with large automorphism groups and applied it to a genus six curve with CM fields as cyclotomic fields. In fact, these kind of fields contain the roots of unity of order $2g + 1$ where g is the genus. However, generic CM curves has only trivial automorphism groups so these curves are among very special CM curves. These CM fields were used simply because the order calculation of the Jacobian varieties could be easy by using the Jacobi sums in the cyclotomic fields[20][27][4]. Since the polynomial time algorithm to calculate the order of Jacobian varieties for general CM field is available already [7][8], one can readily avoid such non-generic curves.

Thus, the remain problem is how to find CM curves as fast and as many as possible. More concretely, to find CM curves with small genera and large discriminants of their CM fields. Until now, the main approach to build CM curves is to use theta function theory to build a projective embedding of the Jacobian varieties[25][26]. [33] built two CM hyperelliptic curves of genus two. This approach is then improved by [38][39][36]. In fact, the nineteen CM hyperelliptic curves defined over $\boldsymbol{Q}$ are built recently in [36]. This approach however needs exponentially high precision computation in the theta series expansion in order to cope with potential approximate errors. As we shown in this paper, this algorithm costs exponential time in the discriminant of the CM field.

In this paper, we present new algorithms to find explicit models of hyperelliptic curves with CM. We avoid the numerical difficulty of the analytical embedding by using only algebraic manipulations on small finite fields. Both models and invariants of the CM curves are lifted with CRT from these finite fields. The algorithm 2 which lifts models of CM curves has no restriction on genera and shapes of definition equations of curves. In the algorithm 3, 4 which lifts invariants of CM curves, we restrict ourselves to a subfamily so that one can always obtain the model of the curve from their invariants. Besides, these algorithms can also be used to other curves of genera larger than two if an explicit definition of their moduli invariants is available. Being probabilistic algorithms, the CM tests proved to be very simple and sharp. The lifting algorithms are of deterministic, and a complexity analysis shows that the invariant lifting algorithm has complexity of a polynomial in the discriminant of the CM field.

This paper is organized as follows. In the chapter two, we give some notations and definitions. In the chapter three, we show algorithms for CM test of Jacobian varieties of algebraic curves. In the chapter four, an algorithm to lift from finite fields the models of algebraic curves with CM is presented. In the chapter five,

an algorithm is presented to lift the invariants of CM hyperelliptic curves. In the chapter six, we show a complexity analysis for both the analytical embedding algorithm and the invariant lifting algorithm. Finally, we show an examples to compare the proposed algorithm with the analytical embedding algorithm and also application to design a secure hyperelliptic cryptosystems. In the appendix we show an algorithm to find the model of a curve from its moduli invariants using a subfamily of curves.

2 Preliminary

A hyperelliptic curve over a field F of genus g is defined by

$$C : Y^2 + Yh(X) = f(X)$$

with the point at infinity, where $\deg h \leq g, \deg f = 2g + 1$. For char$F \neq 2$, one can use the definition as

$$C : Y^2 = f(X).$$

A F-rational point $P \in C(F)$ is defined by both $P = (x, y)$ such that $x, y \in F$ and $y^2 + yh(x) = f(x)$ or the point at infinity. A (Weil) divisor D on C is defined as a finite formal sum of form $\sum_i m_i P_i, m_i \in \boldsymbol{Z}, P_i \in C(\bar{F})$. The degree of D is defined as $\deg(D) = \sum_i m_i$. In particular, the divisors with degree zero form a subgroup $\mathcal{D}^0(C)$ of the divisor group whose elements are algebraically equivalent to zero. The function field of C is consisted of $\{p/q\}, p, q \in \bar{F}[u, v], q \neq 0 \bmod v^2 + vh(u) - f(u)$. The divisor of a function p/q on C is defined as $\sum_i m_i P_i - \sum_j n_j Q_j$, here $P_i, Q_j \in C(\bar{F})$ are zeros and poles of the function and m_i, n_j are the multiplicity of the zeros and the poles. It can be shown that all the divisors of functions over C have degree zero and will be called as principal divisors, or linearly equivalent to zero. Obviously the principal divisors form a subgroup $\mathcal{D}^l(C)$ of $\mathcal{D}^0(C)$. The Jacobian variety of C is then defined as follows.

$$\mathcal{J} = \mathcal{D}^0(C)/\mathcal{D}^l(C)$$

For $F = \boldsymbol{F}_q$, a $\boldsymbol{F}_q$-rational divisor is defined as a divisor which is fixed under the Galois action on $\boldsymbol{F}_q$ and the group of $\boldsymbol{F}_q$-rational points $\mathcal{J}(\boldsymbol{F}_q)$ is generated by $\boldsymbol{F}_q$-rational divisors.

It is known that a Jacobian variety is an Abelian variety or a complete and nonsingular variety with the commutative addition law as an algebraic group. As proved by A. Weil for curves of genus g, the orders of their Jacobian varieties over finite fields fall in the following range.

$$(q^{1/2} - 1)^{2g} \leq \#\mathcal{J}(\boldsymbol{F}_q) \leq (q^{1/2} + 1)^{2g}$$

The Jacobian varieties of hyperelliptic curves can then be used to defined discrete logarithm problem as to find $m \in \boldsymbol{Z}$ given two divisors $D_1, D_2 \in \mathcal{J}(\boldsymbol{F}_q)$ such that $D_1 = mD_2$.

We now introduce an important property of the endomorphism rings of Abelian varieties. Let F be an algebraic number field, A/F a g-dimensional Abelian variety, $\mathrm{End}_F A$ its endomorphism ring. It is known that for a simple Abelian variety A, $\mathrm{End}_F A$ is a division algebra of finite rank over $\boldsymbol{Q}$ with an involution $x \mapsto x'$ such that if $x \neq 0$, $\mathrm{Tr}_{F/\boldsymbol{Q}}(xx') > 0$. Define $K = \mathrm{End}^\circ A := \mathrm{End}_F A \bigotimes_{\boldsymbol{Z}} \boldsymbol{Q}$. When K is isomorphic to a totally imaginary quadratic extension of a totally real extension of $\boldsymbol{Q}$ of degree $2g$, A is called with complex multiplications or CM. K is called the CM field of A. It is known that ordinary Abelian varieties over finite fields are all CM, and any CM Abelian variety is isogenous to an Abelian variety over finite fields. Further details of notations are referred to e.g. [21], [32].

3 CM Tests of Jacobian Varieties

In this section, we show an efficient algorithm to test whether the Jacobian variety of an algebraic curve has CM, which proves very useful in later chapters. This probabilistic algorithm is based on certain interesting relation between the reduction of an Abelian variety over an algebraic number field to a finite field modulo a prime ideal in the integral ring of the number field, lying over a prime number, and the decomposition of the principal ideal generated by the prime number in the integral ring of the definition field [32][21].

Definition 1. *A pseudo-CM algebraic curve is defined as one whose Jacobian variety passed one of the following CM tests.*

Consider a curve C/F, F an algebraic number field, we denote the residue field of a prime p of F as $\boldsymbol{F}_q$, $Z(X)$ the characteristic polynomial of the Frobenius endomorphism on $\mathbf{F}_q$-rational divisors of the Jacobian variety $\mathcal{J}/\mathbf{F}_q$ of $C/\mathbf{F}_q$. To simplify treatment involved with the reflex CM field and reflex CM type, we will hereafter assume that all the CM fields are abelian and the $Z(X)$'s are irreducible.

Below, we will use the algorithms in e.g. [8][28] to calculate CM field and CM type of a Jacobian variety with CM.

Algorithm 1
Procedure 1 (Ordinary reduction test)

Input A random curve C/F of genus g, $N \in \boldsymbol{N}$;
Output If C/F is a pseudo-CM curve, and when it is, the CM field K;
Step 1 Find the CM field and the discriminant d_1 of $Z_1(X)$ of $C/\boldsymbol{F}_{q_1}$ with ordinary reduction for a small prime p_1;
Step 2 Choose small primes $p_i, i = 2, \cdots, N$ such that $Z_1(X) \bmod p_i$ splits. For $\mathcal{J}/\boldsymbol{F}_{q_i}$ find the discriminant d_i of $Z_i(X)$, if the square-free part of d_1 equals not that of d_i for some i, output that C/F has no CM;
Step 3 Output C as a pseudo-CM curve whose CM field K has a minimal polynomial $Z_1(X)$;

Procedure 2 (Supersingular/bad reduction tests)

Input A random curve C/F of genus g, $N \in \boldsymbol{N}$;
Output If C/F is a pseudo-CM curve, its CM field K;
Step 1 Find the CM field and the characteristic polynomial $Z_1(X)$ of $\mathcal{J}/\boldsymbol{F}_{q_1}$ with ordinary reduction for a small prime p_1;
Step 2 Choose small primes $p_i, i = 2, \cdots, N$ such that $Z_1(X) \bmod p_i$ is irreducible or $p_i | d_1$, if neither $\mathcal{J}/\boldsymbol{F}_{q_i}$ is supersingular nor $C/\boldsymbol{F}_{q_i}$ is singular for any i, output that C/F has no CM;
Step 3 Output C as a pseudo-CM curve whose CM field has a minimal polynomial $Z_1(X)$;

4 Lifting Models of Curves with CM

It is known that every CM Abelian variety A has a projective model over $\bar{\boldsymbol{Q}}$. The definition field F of equations is contained in the definition field of the model $(A, \iota, \mathcal{C})$, where $\iota : K \hookrightarrow \mathrm{End}_F^o A$ an embedding and $\mathcal{C}$ a polarization, which is however not easy to find. One may then use the latter for F instead and also denote it as F. Furthermore, one may choose that the definition fields of the models are coincide with the so-called fields of moduli under certain conditions[40], which can be built from the class field of K. In particular, when A is simple which is the case we are dealing with, and A is principal e.g. $\mathrm{End}(A)$ equals the maximal order of $\mathcal{O}_K$, the definition field of the model can derived under minor conditions from the Hilbert class field, which we denote as K_{ab}. [32][40].

In this section, we show how to lift from small finite fields the models of curves with CM defined e.g. over the class field of K.

Algorithm 2

Input : A model of equations of a curve family $\{C/\bar{\boldsymbol{Q}}\}$ with genus g;
Output : Curves in the family with CM over K_{ab} and their CM fields K;
Step 1 For small prime p_1, choose models of all non-isomorphic curves $C_1/\boldsymbol{F}_{q_1}$ among the family over $\boldsymbol{F}_{q_1}$, e.g. in the case of hyperelliptic curves, one may use

$$y^2 \equiv x^{2g+1} + a_1 x^{2g} +, \cdots, + a_{2g} \bmod p_1$$

such that $\mathcal{J}_1/\boldsymbol{F}_{q_1}$ are ordinary, their CM fields K are abelian and $Z(X)$ irreducible. Calculate K, its discriminant d_K and the class number h of $\mathcal{O}_K$;
Step 2 For each of the pairs $(C_1/\boldsymbol{F}_{q_1}, K)$, choose small prime p_i such that $p_i | d_K$, then find the curves $C_i/\boldsymbol{F}_{q_i}$ such that either $C_i/\boldsymbol{F}_{q_i}$ is singular or $\mathcal{J}_i/\boldsymbol{F}_{q_i}$ is supersingular. The conjugates of the coefficients in each definition equation are collected to compose the reduction of the minimal polynomial of the same coefficients in the curve C/K_{ab} with CM field K, modulo the prime ideal over p_i;
Step 3 For each of the pairs $(C_1/\boldsymbol{F}_{q_1}, K)$, choose small prime $p_i, i = 2, \ldots M$ such that p_i is inert in K, then find the curves $C_i/\boldsymbol{F}_{q_i}$ such that either $C_i/\boldsymbol{F}_{q_i}$ is singular or $\mathcal{J}_i/\boldsymbol{F}_{q_i}$ is supersingular. The conjugate of coefficients in the

equation are collected to compose the reduction of the minimal polynomial of the same coefficients in the curve C/K_{ab} with CM field K;

Step 4 For each of the pair $(C_1/\boldsymbol{F}_{q_1}, K)$, choose small prime $p_i, i = 2, \ldots M$ such that p_i splits completely in K, then find the curves $C_i/\boldsymbol{F}_{q_i}$ such that $End^{\circ}_{\boldsymbol{F}_{q_i}} \mathcal{J}_i \cong K$. Again, the conjugate coefficients are collected to compose the minimal polynomial of the same coefficient in the curve $C/\boldsymbol{Q}$ with CM field K;

Step 5 Choose one candidate curve C_i for each i and apply the CRT to each coefficients to recover the equation C/K_{ab};

Step 6 If the C/K_{ab} passed the CM tests, then output it as a pseudo-CM curves, if not goto step 2-4 to try the other combinations or add one more prime;

Remark 1. The family of curves is not limited to hyperelliptic curves or genus two curves. A reasonable choice for such a family is the de Jong-Noot family [10], which is known to contain infinite number of CM curves.

Remark 2. For fast implementation, one-parameter family would be desirable. More efficient approach is to use to select candidate curves by determination of the isomorphic type of the endomorphism ring of $J/\boldsymbol{F}_q$, using the algorithm such as generalization of the Kohel's algorithm for ordinary reduction in [22].

Remark 3. It is also possible to use certain convenient properties in the supersingular reduction to raise the lift efficiency. Especially, choose p_i carefully the reduction of the Jacobian will be isomorphic to product of supersingular elliptic curves (supersingular Abelian varieties) then calculation over elliptic curves can be made use of [19].

5 Lifting of Invariants of Hyperelliptic Curves with CM Jacobians

It can be observed in the lifting of the models of curves that it is desirable if one can lift the invariants instead of the models in order to reduce the number of candidates. This is possible if an explicit definition of moduli invariants is known, such as in the genus two case.

Algorithm 3

Input A model of curve family $C/\bar{\boldsymbol{Q}}$ of which their invariants $\mathcal{I} = (I_1, \ldots, I_m)$ in their moduli space is explicitly defined;

Output : Invariants $\mathcal{I}$ of curves in the family with CM over K_{ab} and their CM fields K;

Step 1 For small prime p_1, choose among the family of all non-isomorphic curves $C_1/\boldsymbol{F}_{q_1}$ such that $\mathcal{J}_{1s}/\boldsymbol{F}_{q_1}$ are ordinary reductions, their CM fields K are abelian and $Z(X)$ irreducible. Calculate K and the discriminants d_K, the class number h of $\mathcal{O}_K$ and their invariants $\mathcal{I}_1/\boldsymbol{F}_{q_1}$;

Step 2 For each of the pairs $(C_1/\boldsymbol{F}_{q_1}, K)$, choose small prime p_i such that $p_i|d_K$, then find the curves among the family $C_i/\boldsymbol{F}_{q_i}$ such that either $C_i/\boldsymbol{F}_{q_i}$ is singular or $\mathcal{J}_i/\boldsymbol{F}_{q_i}$ is supersingular. Calculate all conjugates of their invariants $\mathcal{I}_i/\boldsymbol{F}_{q_i}$. These invariants are collected to compose the reduction of the minimal polynomial of the same invariant $\mathcal{I}$ of the curve C/K_{ab} with CM field K, modulo the prime ideal over p_i;

Step 3 For each of the pairs $(C_1/\boldsymbol{F}_{q_1}, K)$, choose small prime $p_i, i = 2, \ldots M$ such that p_i is inert in K, then find the curves among the family $C_i/\boldsymbol{F}_{q_i}$ such that either $C_i/\boldsymbol{F}_{q_i}$ is singular or $\mathcal{J}_i/\boldsymbol{F}_{q_i}$ is supersingular. Calculate all conjugates of their invariant $\mathcal{I}_i/\boldsymbol{F}_{q_i}$. Then compose the reduction of the minimal polynomial the same invariants $\mathcal{I}$ of the curve C/K_{ab} with CM field K;

Step 4 For each of the pair $(C_1/\boldsymbol{F}_{q_1}, K)$, choose small prime $p_i, i = 2, \ldots M$ such that p_i splits completely in K, then find the curves among the 1-parameter family $C_i/\boldsymbol{F}_{q_i}$ such that $End^{\circ}_{\boldsymbol{F}_{q_i}} \mathcal{J}_i \cong K$. Calculate all conjugates of their invariants $\mathcal{I}_i/\boldsymbol{F}_{q_i}$. Then compose the reduction of the minimal polynomial of the same invariants $\mathcal{I}$ of the curve C/K_{ab} with CM field K;

Step 5 Choose one candidate minimal polynomial of $\mathcal{I}_i$ for each i and use the CRT to lift each coefficient of the minimal polynomial to K_{ab};

Step 7 Test if the model C/K_{ab} with the invariant $\mathcal{I}$ passed the CM tests, then output it as a pseudo-CM curve, if not goto Steps 2-4 to try the other combinations or add one more prime;

Remark 4. Again efficient identification of the isomorphism type of the endomorphism ring of $J/\boldsymbol{F}_q$ could substantially accelerate the calculation. The only algorithm available presently is in [22] which generalizes Kohel's algorithm for determination of the isomorphic type of endomorphism ring of ordinary elliptic curves over finite fields, which uses the Cantor's analogue of division polynomials for elliptic curves.

Remark 5. One can lift either the integral (relative) or the absolute invariants. The absolute invariants is known as algebraic numbers but may not be algebraic integers. To lift such numbers, one may use the algorithm in [37] which needs the CRT of double size of the maximum between the numerator or the denominator.

Remark 6. It is known that usually to find the equation of a curve from its invariants is very difficult. In projective embedding using theta functions, this problem is solved by using Mestre's trick, which however does not apply here. We show an algorithm to overcome this problem using one-parameter family. It is shown as Algorithm 4 in Appendix. To find equations of curves one may apply its Steps 1-2 before the Step 1 of the algorithm 3 and its Step2 3-4 will be used after the Step 5 in the algorithm 3. The example to be shown bellow used a new approach to find curve equation from its invariant based on polynomial resultant, which will be reported in the near future.

Remark 7. Further approaches to reduce the number of candidates so as to accelerate the whole calculation are discussed in [22][16].

6 Complexity Analysis

We give analysis of both the analytical embedding of CM Jacobian varieties using the theta functions and the proposed algorithm for invariant lifting.

Below, we follow the notations and the algorithms in e.g. [36] and assume $g = 2$.

Theorem 1. *The analytical embedding using the theta functions costs exponential time of the discriminant of the CM field K: $O(|d_K|^{9/8} 2^{3/2\sqrt{|d_K|}})$.*

Proof. For simplicity we assume the CM type $(K, \{\phi_i\})$ is self-dual, the endomorphism ring is the maximal order of $\mathcal{O}_K$. The discriminant of K is denoted as d_K. Assume the principal polarization of the embedding is given by the Riemann form

$$E(z, w) = \sum_i \phi_i(\xi)(\bar{z}_i w_i - z_i \bar{w}_i), \quad \xi \in K, K = K^+(\xi),\ \phi_i(\xi^2) < 0.$$

The theta functions can be estimated by Minkowsky's lemma, using minimal the sum of abstract values to approximate the minimal type trace. In particular, for $\delta, \epsilon \in \boldsymbol{R}^2, \Omega = \mathrm{diag}[\phi_i(\xi)]$

$$\begin{aligned} |\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (\Omega)| &= |\sum_{m \in \boldsymbol{Z}^2} e^{\pi i (m+\delta)^t \Omega (m+\delta)} \times e^{2\pi i (m+\delta)^t \epsilon}| \\ &= O(\sum_{m \in \boldsymbol{Z}} e^{-\pi\ \mathrm{Im} T_\Phi(\xi) m^2}) \\ &= O(e^{-(96\pi^3)^{1/4} |d_K|^{1/8}}). \end{aligned}$$

Then in the Rosenhain normal form

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$$

the roots λ_i can be estimated from the theta constants or the values of theta functions on particular choices of δ, ϵ: $\lambda_i = O(e^{\ 4(96\pi^3)^{1/4} |d_K|^{1/8}})$. Thus, the integral Igusa Invariants which are defined by the Rosenhain normal form can be estimated as $I_i = O(e^{120(96\pi^3)^{1/4} |d_K|^{1/8}})$. Since the absolute invariants are homogeneous ratios of the integral invariants, the calculations in the embedding by the theta functions will be dominated by those for the integral invariants, we will use the estimate of integral invariants in analysis of the whole algorithm.

Next, assume that the Igusa invariant is defined over a ray class field, for simplicity a Hilbert class field. To calculate an algebraic integer with a minimal polynomial of degree h will generally cause precision of

$$\mathrm{Prec}(d_K) = O(120(96\pi^3)^{1/4} h \binom{h}{\lfloor \frac{h}{2} \rfloor} |d_K|^{1/8})$$

due to the error accumulation mainly in the middle term of the minimal polynomial (see also [5]). Using the Sterling formula and take a upper bound of the class number h as $\sqrt{|d_K|}$,

$$\mathrm{Prec}(d_K) = O(2^{\sqrt{|d_K|}}\ |d_K|^{\frac{3}{8}}).$$

Take the number of the terms in the theta series expansion as

$$\sqrt{\frac{\mathrm{Prec}(d_K)}{|d_K|^{1/8}}} = 2^{1/2\sqrt{|d_K|}}|d_K|^{1/4}$$

the complexity of the whole embedding is of $O(|d_K|^{9/8}2^{3/2\sqrt{|d_K|}})$. □

Theorem 2. *The invariant lifting algorithm find the model of a CM curve in cost of polynomial time of the discriminant of the CM field K: $O(|d_K|^{135/8})$.*

Proof. Consider the lifting of the Igusa invariants over the Hilbert class field of the CM field K. The largest coefficient, which is of the middle degree term, but its order can also be estimated as the highest degree coefficient. Since $I_i = O(e^{120(96\pi^3)^{1/4}|d_K|^{1/8}})$, the order of the largest coefficient is about $O(I_i^h)$. By the Chinese remainder theorem and the theorem of prime number, one knows that in order to lift such integers, it is enough to repeat calculations of its shadows or reductions on $L = O(|d_K|^{5/8})$ finite fields $\boldsymbol{F}_q$. The sizes of these finite fields are also of the same order $q = O(L)$. (Here lifting of a rational numbers requires CRT in twice size of denominators and numerators, but the order remains the same [37].)

Determination of isomorphic types of the endomorphism ring over $\boldsymbol{F}_q$ using the generalized Kohel algorithm in [22] required $O(q^{20})$ computations. If this algorithm is applied to all q^6 curves over each finite fields, the calculations will be $L^{26} = O(|d_K|^{65/4})$. The overall cost is then $L^{27} = O(|d_K|^{135/8})$.

Lifting of the minimal polynomials of the absolute Igusa invariants for h coefficients from the L residues over finite fields of size L requires hL^3 computations . The whole calculation is $L = O(|d_K|^{19/8})$. Thus, the whole complexity is dominated by $L^{27} = O(|d_K|^{135/8})$. □

7 Example

We show an example of construction of a secure hyperelliptic curve using the CM field $K = \boldsymbol{Q}(\alpha)$, where $\alpha = \sqrt{-61 + 6\sqrt{61}}$. One can shown that $Gal(K/\boldsymbol{Q}) \cong \boldsymbol{Z}/4\boldsymbol{Z}$, its class number $h = 1$ and the minimal polynomial of α is $Z(X) = X^4 + 4X^2 + 2$.

Firstly, we construct by ordinary lifting the absolute Igusa invariants of a curve of which the endomorphism ring is isomorphic to the maximal order O_K of K. We chose some small primes l such that Z splits completely modulo l and we

can compute the absolute Igusa invariants of curves of which the endomorphism ring over $\boldsymbol{F}_l$ is isomorphic to O_K. Then they were lifted to $\boldsymbol{Q}$ by the CRT and Wang's algorithm in [37]. The following table shows the process in which the set of the primes l, used in residue collecting and lifting steps of the invariants by CRT, is enlarged one by one. The places marked by "−" denotes when no rational number is output by Wang's algorithm, which means one has to use more primes and the residues because Wang's algorithm requires the product of all the primes used in CRT greater than the square of the maximum between the numerator and the denominator.

l	(i_1, i_2, i_3)
13	$(-, \frac{1}{2}, 1)$
47	$(8, \frac{-4}{5}, -)$
73	$(\frac{-11}{75}, \frac{31}{114}, \frac{-139}{95})$
83	$(\frac{-782}{1277}, \frac{32}{7}, \frac{-960}{977})$
103	$(\frac{5212}{957}, \frac{909}{9098}, \frac{12548}{2655})$
131	$(\frac{45725}{81556}, -, -)$
137	$(-, \frac{179573}{119374}, -)$
179	$(-, -, \frac{-11412461}{1383790})$
199	$(\frac{-77531094}{109697555},, -, \frac{24918900}{5235127})$
239	$(\frac{2186985284}{3193941857}, -, \frac{-1640487534}{4170341347})$
241	$(\frac{23480370079}{7651764248}, -, \frac{-3798052317}{1459572997})$
257	$(\frac{245299012496}{677918816561}, -, -)$
269	$(-, \frac{-73355585483}{60532992290}, \frac{13309544621557}{7113235908976})$
317	$(-, \frac{-131053190222379}{52778584689371}, -)$
347	$(\frac{-21342583751735}{3808553318042}, \frac{4795562804619412}{416652904406961}, \frac{437038183335891}{1181681515448155})$
367	$(\frac{-95446913549733067}{13383094726804267 6}, \frac{57711532928870746}{49544577811039265}, -)$
379	$(\frac{481547553916414864}{556460739772033019}, \frac{793418475254355983}{2138941242118446}, \frac{-1724244246804899840}{957123916241973161})$
439	$(\frac{6401196155012958989}{3823830469612399046 3}, \frac{5088610823737322931 5}{3757404045194682888 4}, -)$
443	$(-, \frac{-61811314844862517342 1}{95297355789554914867 5}, \frac{1072978816049248202527}{842824205190253192560})$
449	$(-, \frac{-3510317073529145008681}{739273871370166606358}, \frac{-12388639766753383014443}{1718710450420739650187 0})$
461	$(\frac{-29927487013532718098126 7}{2493120362012596532825 11}, \frac{16384940590002328300 16}{751528652099393064921 1}, \frac{-363114988047137371773 1}{198125214271045606249 8})$
503	$(\frac{-977914909416525265184231 6}{614891742157678442199480 9}, -, -)$
569	$(-, -, -)$
571	$(-, -, \frac{-59635665577431549497960782 03}{153654705030022551635069516 3})$
607	$(-, \frac{-40404764693716413637740986368}{2210164921192340292187 5}, \frac{-6358570380638204937480139571 2}{663049476357702087656 25})$
619	$(\frac{-28863365619965901713439468220 01}{184005852797284144076142609559}, \cdot, \cdot)$
683	$(\frac{-82310585301850115990999586471322}{6883986318338374838069483160436 3}, \cdot, \cdot)$
691	$(-, \cdot, \cdot)$
727	$(\frac{900221825756843306292001070288067 9}{7319341342731625939019371833763483 9}, \cdot, \cdot)$
733	$(-, \cdot, \cdot)$
757	$(-, \cdot, \cdot)$
809	$(\frac{287937809605549912245372120696446280663}{1417662602226964645619988631257350586163}, \cdot, \cdot)$
827	$(\frac{-144980658532908976096752457420835962 24}{1078013978414987133575367742110738088 7}, \cdot, \cdot)$
863	$(\frac{45988698383572734726451530268687176195060 5}{10075139539033433299760423482165704367092 49}, \cdot, \cdot)$
911	$(\frac{64362934261601970395843388504956649599191 99}{31649835338309069933550235889538091910369641}, \cdot, \cdot)$
937	$(\frac{-116152266457850949605013807041682945649672192}{640250862723239113078565449877929687 5}, \cdot, \cdot)$
977	$(\frac{-116152266457850949605013807041682945649672192}{640250862723239113078565449877929687 5}, \cdot, \cdot)$

Secondly, we construct a secure Jacobian defined over a finite field by the fast algorithm of [8]. Specifically, using prime ideal factorization of the Frobenius endomorphism, we found a principal prime ideal of K

$$(\omega) = \begin{pmatrix} 1 & \frac{\alpha+1}{2} & \frac{\alpha^2+7}{12} & \frac{\alpha^3+5\alpha^2+7\alpha+35}{120} \end{pmatrix} \begin{pmatrix} -438577 \\ -3748 \\ 284050 \\ 124962 \end{pmatrix} \mathcal{O}_K$$

such that $N_{K/\boldsymbol{Q}}(\omega) = p$, where $p = 52312624340242137883873 87$. Then we obtained a secure Jacobian with order

$$\#\mathcal{J}\left(\boldsymbol{F}_p\right) = 2^4 \times p_{max}$$

where p_{max} is a $160bits$ prime number

$$p_{max} = 171038166585489431295851726260119735092182002248 3.$$

Finally, we construct a secure curve over $\boldsymbol{F}_p$, of which Jacobian has above order, from invariants calculated above:

$$i_1 = \frac{-116152266457850949605013807041682945649672192}{64025086272323911307856544987792968 75}$$
$$i_2 = \frac{-40404764693716413637740986368}{22101649211923402921875}$$
$$i_3 = \frac{-63585703806382049374801395712}{66304947635770208765625}.$$

The equation of curves is restricted here in form of

$$Y^2 = X^5 + X^3 + a_2X^2 + a_1X + a_0.$$

Notice that this restriction does not exclude any possible isomorphism classes of the curves.

By an algorithm mentioned before using polynomial resultant computation, we obtained coefficients of a curve with given invariants as

$$a_0 = 417929590974323696943368$$
$$a_1 = 22575619650324475964544 92$$
$$a_2 = 24184665785957054639461 19$$

over $\boldsymbol{F}_p$. The twisted curve of the above curve has equation as

$$C/\boldsymbol{F}_p : Y^2 = X^5 + c^2X^3 + c^3a_2X^2 + c^4a_1X + c^5a_0,$$

where $c = 2$. It has the same secure order constructed above.

Acknowledgment: The authors wish to thank Prof. Fumiyuki Momose for helpful discussions, Prof. Gerhard Frey for interesting comments on [33] and Dr. Michael Müller for sending us a copy of Dr. Spallek's thesis.

References

1. L.M.Adleman, M.D.A.Huang, "Primality Testing and Abelian Varieties Over Finite Fields," Springer-Verlag , (1992.)
2. L.M.Adleman , J.DeMarrais, M.D.Huang, "A Subexponential Algorithms for Discrete Logarithms over the Rational Subgroup of the Jacobians of Large Genus Hyperelliptic Curves over Finite Fields," Proc. of ANTS95, Springer, (1995)

3. L.M.Adleman, M.D.Huang, "Counting rational points on curves and Abelian varieties over finite fields" Henri Cohen (Ed)"Algorithmic number theory" Lecture Notes in Computer Science, 1122, Second International Symposium, ANTS-II, Proceedings, p.1-16. 1996
4. S.Arita, "Public key cryptosystems with C_{ab} curve (II)" IEICE, Symposium on Cryptography and Information Security, SCIS'98, 7.1-B, 1998-1.
5. A.O.L.Atkin, F.Morain, "Elliptic Curves and Primality Proving" , Research Report 1256, INRIA, (1990).
6. D.Cantor, "Computing in the jacobian of hyperelliptic curve," Math. Comp., vol.48, p.95-101, (1987)
7. J.Chao, N.Matsuda, S.Tsujii, "Efficient construction of secure hyperelliptic discrete logarithm problems" Springer-Verlag Lecture Notes on Computer Science, Vol.1334, pp.292-301, "Information and Communication Security" Y. Han, T. Okamoto, S. Qing (Eds.) Proceedings of First International Conference ICICS'97, Beijing, China, Nov. 1997.
8. J.Chao, K.Matsuo, S.Tsujii "Fast construction of secure discrete logarithm problems over Jacobian varieties," Information Security for Global Information Infrastructures: IFIP TC 11 16th Annual Working Conference on Information Security, S.Qing and J.Eloff(Eds.), Kluwer, July 2000.
9. H. Cohen "A course in computational algebraic number theory," Springer, GTM-138, 1995.
10. J.de Jong, R.Noot, "Jacobians with complex multiplication," Arithmetic Algebraic Geometry, Birkhäuser PM89, pp.177-192, 1991.
11. Duursma, Gaudry, Morain, "Speeding up the discrete log computation on curves with automorphism", Proceeding. Asiacrypt-99, 1999.
12. G. Frey, H.G. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves," Math. Comp., 62, 865-874, 1994.
13. G.Frey, M.Müller, "Arithmetic of modular curves and applications," Preprint, 1998.
14. P.Gaudry "A variant of the Adelman-DeMarrais-Huang algorithm and its application to small genera," Preliminary version, June 1999.
15. P.Gaudry, R.Harley, "Counting points on hyperelliptic curves over finite fields," Preprint, 2000.
16. T.Haga, K.Matsuo, J.Chao, S.Tsujii, "Construction of CM hyperelliptic curves using ordinary lifting," Proc. of SCIS'2000, IEICE Japan, 2000.
17. M.D.Huang, D.Ierardi,"Counting Rational Point on Curves over Finite Fields," Proc. 32nd IEEE Symp. on the Foundations of Computers Science, 1993.
18. J.Igusa, "Arithmetic variety of for genus two," Ann. of Math. , vol.72, No.3, p.612-649, (1960)
19. K. Kamio, H. Kawashiro, J. Chao, S. Tsujii, "A fast algorithm of model lifting for CM hyperelliptic curves," Proc. SCIS'99, IEICE, Japan, 1999.
20. N.Koblitz, "Hyperelliptic cryptosystems," J. of Cryptology, vol.1, p.139-150, (1989)
21. S.Lang, "Complex multiplication," Springer-Verlag, (1983)
22. K.Matsuo, J.Chao and S.Tsujii, "On lifting of CM hyperelliptic curves," Proc. of SCIS'99, W3-1.4, IEICE Japan (1999).
23. A.Menezes, S.Vanstone, T.Okamoto, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Fields," Proc. of STOC, p.80-89, (1991).
24. V. Müller, A. Stein, C. Thiel, "Computing discrete logarithms in real quadratic congruence function fields of large genus," Preprint, Nov. 13, (1997)
25. D.Mumford, "Tata Lectures on Theta I," Birkhäuser, Boston , (1983).

26. D.Mumford, "Tata Lectures on Theta II," Birkhäuser, Boston , (1984).
27. K.Nagao, "Construction of the Jacobians of Curves $Y^2 = X^5 + k$ /$\boldsymbol{F}_p$ with Prime Order," Manuscript, 1998.
28. O. Nakamura, N. Matsuda, J. Chao, S. Tsujii, "On cryptosystems based on abeian varieties with CM," IEICE, Symposium on Cryptography and Information Security, SCIS'97, 12-E, 1997-1. IEICE, Tech. rep. ISEC-96-81, 1997-3.
29. J.Pila, "Frobenius maps of abelian varieties and finding roots of unity in finite fields," Math. Comp., vol.55 , p. 745-763, (1990)
30. H.G. Rück, "on the discrete logarithm problem in the divisor class group of curves," Preprint, 1997.
31. J.P.Serre, J.Tate, "Good reduction of abelian varieties," Ann. of Math. (2), 88 (1968), page 492-517.
32. G.Shimura : "Abelian Varieties with Complex Multiplication and Modular Functions", Princeton Univ. Press, 1998.
33. A-M.Spallek, "Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen," Dissertation, preprint, No. 18, 1994.
34. J.Tate, "Endomorphisms of Abelian varieties over finite fields," Invent. Math. 2, p.134-144, (1966)
35. E.J.Volcheck, "Computing in the Jacobian of a plane algebraic curve," Proc. of ANT-1, p.221-233, LNCS-877, (1994).
36. P.V.Wamelen, "Examples of genus two CM curves defined over the rationals," Math. Comp., 68(225), pp. 308-320, 1999.
37. P.S.Wang, "A p-adic algorithm for univariate partial fractions," Proc. of ACM SYMSAC'81, ACM, 212-217, 1981.
38. X. Wang, "2-dimensional simple factors of $J_0(N)$," Manuscripta Mathematica, 87:179-197, 1995.
39. H.J. Weber, "Hyperellptic simple factors of $J_0(N)$ with dimension at least 3," Experimental Math. vol. 6, No.4, 273-287, 1997.
40. H. Yoshida, "Hecke characters and models of abelian varieties with complex multiplication," J. Fac. Sci. Univ. of Tokyo, Sec. IA, 28 , 633-649(1982).

Appendix: Subfamilies Whose Models Can Be Determined from Their Invariants

Since it is generally difficult to find an explicit model of a curve with given invariants, we will use the following algorithm to find the models of curves from a point in their moduli space.

Algorithm 4

Input : A model of a family $\mathcal{C}/K$ with r parameter $\alpha_1, \cdots, \alpha_r$, $\{f(x, y, \alpha_1, \cdots, \alpha_r) = 0\}$, and a point $\mathcal{I} = (I_1, \ldots, I_m)$ in their moduli space;

Output : Definition field F and a model of $C/F : h(x, y, \alpha) = 0$ corresponding to $\mathcal{I}$, where $\alpha \in F$;

Step 1 Choose $r - 1$ constraints $c_i(\alpha_1, \cdots, \alpha_r) = 0, i = 1, \ldots, r - 1$ in the parameter space to obtain a subfamily $h(x, y, \alpha)$ with 1-parameter α;

Step 2 Reduce the definition equations of the invariants $I_i := g_i(\alpha_1, \cdots, \alpha_r)$ to $J_i(\alpha) = 0, i = 1, \ldots, m$;

Step 3 Calculate $\gcd(J_1, \ldots, J_m) =: J(x) \in K[I_1, \ldots, I_m][x]$;
Step 4 If $J(x) \neq const$, output $h(x, y, \alpha)$ as the model over definition field $F := K(\alpha)$ with a minimal polynomial as $J(x)$;

We can then apply this algorithm to obtain models of hyperelliptic curves of genus two from their Igusa invariants.