Construction of almost-prime Jacobian varieties using CM curves in polynomial time (extended abstract)

Jinhui Chao,
Chuo University
Kazuto Matsuo
Toyo Communication Equipment Co.Ltd.
and
Shigeo Tsujii
Chuo University

Introduction

Jacobian varieties of hyperelliptic curves have been recently used in cryptosystems. However, lacking of efficient point-counting algorithms for such varieties over finite fields makes the design of secure cryptosystems very difficult. In this paper, we presents how to construct secure hyperelliptic curves of small genera over large prime fields $\mathbf{F}_p$ in polynomial time of $\log p$.

Preliminary

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

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

where $\deg f = 2g + 1$, for $\mathrm{char} F \neq 2$.
A F-rational point is defined by both $P = (x, y) \in C \ \ x, y \in F$ such that $y^2 = f(x)$ or the point at infinity.
A (Weil) divisor D on C is defined as a finite formal sum of form $\sum_i m_i P_i, m_i \in \mathbf{Z}, P_i \in C(\bar{F})$,where $\bar{F}$ is a separable algebraic closure of 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.
All the divisors of functions over C have degree zero and are 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 $\mathcal{J}(F) = \mathcal{D}^0(C)/\mathcal{D}^l(C)$.
Let F be a number field or a finite extension of $\mathbf{Q}$, 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 $\mathbf{Q}$ with an involution $x \mapsto x'$ such that if $x \neq 0$, $\mathrm{Tr}_{F/\mathbf{Q}}(xx') > 0$. Define $K = \mathrm{End}^\circ A := \mathrm{End}_F A \otimes_{\mathbf{Z}} \mathbf{Q}$. When K is isomorphic to a totally imaginary quadratic extension of a totally real extension of $\mathbf{Q}$ of degree $2g$, A is called with complex multiplication or CM and K is called a CM field of A.

Computation of CM type of Abelian varieties

Let K be a CM field of a g-dimensional Abelian variety A with $[K : \mathbf{Q}] = 2g$ and $\{\varphi_1, \cdots, \varphi_g\}$ be g embeddings of K into $\mathbf{C}$ such that none of

them are pairwisely complex conjugate. Then $(K;\{\varphi_i\})$ is called the CM-type of A. (Using notation $\Phi := \oplus_i \varphi_i$, a CM type is also denoted as $(K;\Phi)$.)

Following above notations , one can define for $x \in K$ the type trace $T_\Phi(x) := tr\Phi(x) = \sum_i \varphi_i(x)$ and the type norm $N_\Phi(x) := det\Phi(x) = \prod_i \varphi_i(x)$. The reflex of a CM field K is defined as $K' := \mathbf{Q}(T_\Phi(x)|x \in K)$.

Theorem 1. *Let L be a finite Galois extension of $\mathbf{Q}$ s.t. $L \supset K$ and $G =$Gal$(L/\mathbf{Q})$. Extend φ_i to $\tilde{\varphi}_i$ over L, let $H = Gal(L/K) \subset G$ and $S_L = \cup_{i=1}^{g} \tilde{\varphi}_i H$.*

Define $S'_L := \{\sigma^{-1}|\sigma \in S_L\}$ and $H' = \{\gamma \in G \mid S'_L\gamma = S'_L\}$ then, $H' = Gal(L/K') \subset G$.

Let $\{\psi_j\}$ be the embeddings of $K' \longrightarrow \mathbf{C}$ induced from S'_L, $\tilde{\psi}_j$ the lifts of ψ_j to over L and $[K' : \mathbf{Q}] = 2g'$, then $S'_L = \cup_{j=1}^{g'} \tilde{\psi}_j H'$.

Let $\Phi' := \oplus_j \psi_j$, (K', Φ') is always a primitive CM type, called the reflex CM type of (K, Φ). When K is Galois, $\psi_i = \varphi_i^{-1}, \Phi' = \oplus \varphi_i^{-1}$.

For a CM type (K, Φ), and $L \supset K'$, one can define the reflex type norm over L as follows. For $x \in L$,

$$N_{\Phi'_L}(x) = \prod_{i=1}^{n/2} \theta_i(x)$$

$$N_{\Phi'_L}(x) = N_{\Phi'}(N_{L/K'}(x)) = \prod_{j=1}^{g'} N_{L/K'}(x)^{\psi_j},$$

where $\{\theta_i\}$ denote the embeddings of $L \to \mathbf{C}$ induced from $\{\psi_i\}$ and $[L : \mathbf{Q}] = n$. For $L \supset F \supset K'$, $N_{\Phi'_F} = N_{\Phi'} \circ N_{F/K'}$.

Bellow, we show an algorithm to determine the embedding $\{\psi_i\}$ of the reflex CM type which will be used in the following chapter.

[Algorithm 1]

Input : A curve C/F of genus g, K the CM field of its Jacobian variety $\mathcal{J}$, L the normal closure of F and $G := Gal(L/\mathbf{Q}), [L : \mathbf{Q}] = n$.

Output : The embeddings $\{\psi_i\}$ in the reflex CM type of $\mathcal{J}$ over F.

1 : Choose an algebraic integer $\omega \in \mathcal{O}_L$ such that its absolute norm $N(\omega) = p$ equals a prime number p splitting completely in $\mathcal{O}_L$.

2 : Calculate $\sharp C(\mathbf{F}_{p^k})$ and $M_F = \sharp C(\mathbf{F}_{p^k}) - p^k - 1 \quad (k = 1, \cdots, g)$.

3 : Choose $n/2$ embedding $\{\theta_i\}$ s.t. $G \ni \theta_i : L \longrightarrow \mathbf{C}$ such that none of them are pairwisely complex conjugate, calculate the type norm $\gamma = N_{\Theta}(\omega) = \prod_i \omega^{\theta_i}$ for $\Theta = \oplus\theta_i$.

4 : If $\gamma \notin K$ or $\exists M_k \neq -Tr_{K/\mathbf{Q}}\gamma^k$, then go to Step 3 to choose another set of embeddings.

5 : Output the embedding of $\{\psi_i : F \longrightarrow \mathbf{C}\}$ which induce $\{\theta_i\}$ such that (F, Θ) as the reflex CM type lifted from the CM type (K', Φ') and terminate.

The Algorithm 1 calculates the reflex CM type with complexity of $O\left(n^{n+3}\log^3 n + n^{n+1}\log^4 n\right)$ bit-operations.

Design of secure CM Jacobian varieties using Weil number of type (A_0)

It was proved by Shimura and Taniyama the existence of the Grössen or Hecke character and the associated CM character in CM fields, which can be used to determine the Frobenius endomorphisms of the Jacobian varieties over finite fields, therefore their orders.

Theorem 2. *Let $(A, \iota, \mathcal{C})$ denotes an Abelian variety A, $\iota : K \longrightarrow End^0 A$, and $\mathcal{C}$ a polarization. Assume this triple is defined over F, a number field and with CM type (K, Φ) and reflex (K', Φ').*

Then there is a unique (CM) character defined on the idele group $\mathbf{A}_F^*$ of F

$$\exists! \alpha : \mathbf{A}_F^* \longrightarrow K^*$$

such that for $s \in \mathbf{A}_F^*$

$$\alpha(s)\overline{\alpha}(s) = N(s).$$

Let $\mathfrak{P} \subset \mathcal{O}_F$ be a prime ideal, $U_{\mathfrak{P}}$ the group of local units, then α is unramified at $\mathfrak{P}$ or

$$\alpha(U_{\mathfrak{P}}) = 1 \Longleftrightarrow A \bmod \mathfrak{P} \text{ is a good reduction.}$$

In this case, the character determines the so-called Frobenius element by

$$\iota(\alpha(\mathfrak{P})) \equiv Fr_{\mathfrak{P}} \bmod \mathfrak{P}$$

where $Fr_{\mathfrak{P}}$ is the Frobenius endomorphism of the Jacobian variety over the finite field $\mathcal{O}_F/\mathfrak{P}$. For such $\mathfrak{P}$ if $\mathcal{O}_K \subset EndA$ and $\iota(\mathcal{O}_K) = EndA \cap \iota(K)$ one has factorization $(\alpha(\mathfrak{P})) = N_{\Phi'_F}(\mathfrak{P})$. Further, $|\alpha(\mathfrak{P})| = \sqrt{N(\mathfrak{P})}$.

It was Honda and Tate proved the following theorem.

Definition 1. *Let K be a CM field. $\pi_0 \in K$ is called a Weil number of type (A_0) of order m, if it satisfies the following condition.*

$$\pi_0^{\sigma}\overline{\pi}_0^{\sigma} = p^m$$

for all embeddings σ of K into $\mathbf{C}$, where $\overline{(\ )}$ denotes complex conjugate.

Theorem 3. *The type norm of prime ideals in Theorem 2 are principal generated by the Weil numbers of type (A_0). Furthermore, there is a bijective correspondence between the isogeny classes of $\mathbf{F}_{p^m}$-simple Abelian varieties and the conjugate classes of the Weil numbers of type (A_0).*

Bellow, we show a fast algorithm to calculate the principal ideal factorization by use of the so-called Weil numbers of type (A_0).

[Algorithm 2]

Input : Definition field F of C, a reflex CM type (F, Φ'_F), and bit-length c for prime numbers.

Output : π_0: Weil number of type (A_0) of order 1 such that $N(\pi_0) = p^g$, where p is a prime number of bit-length c.

1 : Choose an algebraic integer $\omega \in \mathcal{O}_F$ such that $N(\omega) = p$ for a prime number p of bit-length c. Thus one derives primal ideal $\mathfrak{P}$'s in $\mathcal{O}_F$ lying over p such that $(p) = N\mathfrak{P} = N(\omega)$.
2 : Calculate the Weil number $\pi_0 \in \mathcal{O}_K$ of type (A_0) of order 1 such that $\pi_0 = N_{\Phi'_F}(\omega)$.
3 : Output π_0 as the Weil number of type (A_0) of order 1 associated with p.

The Algorithm 2 calculates Weil numbers with absolute norm of $O(p^g)$ has complexity of $O\left(d^d(n^2 \log^3 p + \log^4 p)\right)$ bit-operations, where n and d denote $[L : \mathbf{Q}]$ and $[F : \mathbf{Q}]$ respectively.

Below we present an algorithm for construction of a secure hyperelliptic curves over $\mathbf{F}_p$ which has a simple Jacobian variety.

[Algorithm 3]

Input : C/F an algebraic curve of genus g with CM, K its CM field and the reflex CM type, (F, Φ'_F).

Output : p and $C/\mathbf{F}_p$ such that $\#\mathcal{J}(\mathbf{F}_p)$ is almost prime.

1 : Choose a prime p large enough, and find a Weil number $\pi_0 \in \mathcal{O}_K$ associated with p^g of order 1 by Algorithm 2.

2 : For all roots of unity $\{\zeta \in K\}$, calculate the order $\#\mathcal{J}(\mathbf{F}_p) = N(1 - \zeta\pi_0)$.

3 : If $\{\#\mathcal{J}(\mathbf{F}_p)\}$ contains no almost prime order then go to Step 1.

4 : Output p and $C/\mathbf{F}_p$.

The Algorithm 3 outputs a secure Jacobian variety of order $O(p^g)$ in $O\left(d^d(n^2 \log^5 p + \log^5 p)\right)$ bit-operations.

Example

We show an example using the curve obtained by Wamelen as follows,

$$C/\mathbf{Q}: Y^2 = -103615X^6 - 41271X^5 + 17574X^4 + 197944X^3 + 67608X^2 - 103680X - 40824.$$

It is shown that C has its CM field $K = \mathbf{Q}(\alpha)$ with $Gal(K/\mathbf{Q}) \cong \mathbf{Z}/4\mathbf{Z}$, where $\alpha = \sqrt{-61 + 6\sqrt{61}}$. An integral basis of K as follows is used.

$$\mathbf{B} = \begin{pmatrix} 1 & \frac{\alpha+1}{2} & \frac{\alpha^2+7}{12} & \frac{\alpha^3+5\alpha^2+7\alpha+35}{120} \end{pmatrix}.$$

A simple CM type of C can be defined by $Gal(K/\mathbf{Q})$ which turns out to be $(K, \{\varphi_1, \varphi_2\})$, with

$$\psi_i = \varphi_i^{-1}: \omega \mapsto \omega_i$$

$$\omega = \mathbf{B}\mathbf{w}, \omega_i = \mathbf{B}\mathbf{M}_i\mathbf{w}$$

where $\mathbf{w} \in \mathbf{Q}^4$ and

$$\mathbf{M}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \mathbf{M}_2 = \begin{pmatrix} 1 & 2 & -9 & -7 \\ 0 & -3 & 0 & 5 \\ 0 & 1 & -1 & -2 \\ 0 & -2 & 0 & 3 \end{pmatrix}.$$

Then using the proposed algorithms, we found a principal prime ideal of K

$$(\omega) = \mathbf{B} \begin{pmatrix} -438577 \\ -3748 \\ 284050 \\ 124962 \end{pmatrix} \mathcal{O}_K$$

such that

$$N_{K/\mathbf{Q}}(\omega) = p$$

where the prime

$$p = 523126243402421378838738 7.$$

A Weil number of type-(A_0) is derived as

$$\begin{aligned} \pi_0 &= \omega^{\psi_1}\omega^{\psi_2} \\ &= \mathbf{B} \begin{pmatrix} 2390869554285 \\ -356014636334 \\ 163684973280 \\ -307468989412 \end{pmatrix}. \end{aligned}$$

Then we obtained

$$\#\mathcal{J}\left(\mathbf{F}_p\right) = N_{K/\mathbf{Q}}\left(1+\pi_0\right) = 2^4 \times p_{max}$$

where p_{max} is a $160bits$ prime
$p_{max} = 1710381665854894312958517262601197350921820022483$.
Finally we obtained a secure curve over $\mathbf{F}_p$ as follows,

$$\begin{aligned} C/\mathbf{F}_p : Y^2 = X^5 \; & +3812868605211523197610847X^3 \\ & +2045648471343061156816729X^2 \\ & +3859251142818901555051787X \\ & +619671438562334592260461 \end{aligned}$$

of which the Jacobian variety has the designed order .
Timing of the above construction by using Maple V on Pentium 166MHz are described in Table 1.

Table1

	iterations	time (sec.)
$\mathbf{B}$	1	3.4
φ_i	1	2.4
ω	1245	14.6
π_0	63	0.1
$\#\mathcal{J}(\mathbf{F}_p)$	63	1.7
Total		22.2