FAST CONSTRUCTION OF SECURE DISCRETE LOGARITHM PROBLEMS OVER JACOBIAN VARIETIES

Jinhui Chao *,
Kazuto Matsuo †
and Shigeo Tsujii ‡

Abstract 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. This paper presents efficient algorithms to calculate the CM type and ideal factorization of Frobenius endomorphisms of Jacobian varieties over finite fields $\mathbf{F}_p$ in polynomial time of $\log p$. Then we show how to construct secure hyperelliptic curves of small genera over large prime fields $\mathbf{F}_p$ in polynomial time of $\log p$.

1. INTRODUCTION

In recent years, elliptic curves are used to define a novel kind of discrete logarithm, which is expected to resist all known subexponential attacks [11][17]. Furthermore, Jacobian varieties of hyperelliptic curves or general algebraic curves over finite fields have also been used to build cryptosystems[12]. It is known that if one chooses a generic curve with small genus and the Jacobian variety with an almostprime order, or has a large prime factor in its order, the discrete logarithm seems at least as intractable as the elliptic curves[2][18][7][23]. Besides, cryptosystems based on Abelian varieties of genus $g > 1$ have shorter bit-length for the same key size, which means possible use of cheaper processors, or higher processing and transmission efficiency.

However, construction of secure Jacobian varieties seems far more nontrivial than elliptic curves. The generalized Schoof's algorithms ,

*Dept. of Electrical and Electronic Eng.,Chuo University. jchao@elect.chuo-u.ac.jp
†Toyo Communication Equipment Co.Ltd.. matuo@toyocom.co.jp
‡Dept. of Information Systems Eng.,Chuo University. tsujii@ise.chuo-u.ac.jp

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35515-3_53

S. Qing et al. (eds.), *Information Security for Global Information Infrastructures*

either following [21] such as [1], or using Cantor's analogue of division polynomials of elliptic curves [8] are still not practical for cryptosystem design. Using Jacobian factors of modular curves [6] seems have difficulty to determine orders of Jacobians of low genera curves. Besides, they have to repeat the whole order-counting calculations $O(\log^2 q)$ times over $\mathbf{F}_q$ until an almost prime Jacobian variety to be found.

A hopeful direction is to use CM curves or curves whose Jacobian varieties are with complex multiplication. Since the Frobenius endomorphisms of their reductions to finite fields are completely determined by their endomorphism rings, it is easier to calculate the orders of these Jacobian varieties over finite fields and design secure discrete logarithms. It is known that for small genera, e.g. less than five or equal to six, there are infinitely many CM curves[5]. Moreover, methods are proposed to construct CM hyperelliptic curves using theta function theory [25][27] or using lifting from small finite fields [10][16]. However, calculation of the order of a Jacobian variety of CM curves, as in [25] with genus two, by solving norm equation costs exponential time [22]. Other methods in [13][19] [3] use the Jacobi sums when the CM fields are cyclotomic fields. [20] extended the Cornacchia algorithm assuming the maximal total real subfields of the CM fields have the integral rings to be Euclidean domains.

In this paper we show a fast algorithm to calculate the order of Jacobian varieties over $\mathbf{F}_p$ with general CM fields and in cost of polynomial time in $\log p$. In particular, we show an algorithm to compute the CM types of CM Jacobian varieties. Then an algorithm to calculate the ideal factorization of the Frobenius endomorphism using Weil numbers is presented. In particular, we use the principal primal ideal factorization of the Frobenius endomorphism in the definition field to obtain the fast algorithm. These algorithms are applied to design secure Jacobian varieties of small genus over large finite fields. Finally, performance of the proposed algorithms are shown by simulation results.

2. PRELIMINARY

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

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

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 is defined by both $P = (x, y) \in C\ x, y \in F$ such that $y^2 + yh(x) = f(x)$ or the point at infinity. A (Weil) divisor D on

C is defined as a finite formal sum of form $\sum_i m_i P_i, m_i \in \mathbf{Z}, P_i \in C(\bar{\mathbf{F}}_q)$,where $\bar{\mathbf{F}}_q$ is a separable algebraic closure of $\mathbf{F}$. 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 $\{p/q\}, p, q \in F[u, v], q \neq 0 \bmod v^2 + vh(u) - f(u)$. 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 $P_i, Q_j \in C$ 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 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 $\mathcal{J}(F) = \mathcal{D}^0(C)/\mathcal{D}^l(C)$.

We now consider the endomorphism rings of Abelian varieties. 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 $K = \mathrm{End}^\circ A := \mathrm{End}_F A \bigotimes_{\mathbf{Z}} \mathbf{Q}$. 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. 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 (Grothendieck). Further details of notations are referred to e.g. [15], [24].

3. CALCULATION 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, $\psi_i = \varphi_i^{-1}, \Phi' = \oplus \varphi_i^{-1}$.

Proof. This is basically from [15], [24]. □

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 $(F, \Theta)$ as the reflex CM type lifted from the CM type $(K', \Phi')$
    and terminate.
```

4. 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, ι, C) denotes an Abelian variety A, $\iota : K \longrightarrow End^0 A$, and 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

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

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, $|\alpha(\mathfrak{P})| = \sqrt{N(\mathfrak{P})}$.

Proof. This is basically from the so-called the second main theorem of complex multiplication. [24] chapter 13 Theorem 1 and [15] chapter 4 Theorem 1.1, 1.2. □

Basically, one needs to calculate ideal factorization of the Frobenius endomorphism given in type norm in the definition field, which generally costs exponential time[22].

It was Honda and Tate proved the following theorem.

Definition 1. *[9] 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).*

Proof. See Theorem 1 , 2 and 3 in [9]. See also [26]. □

Thus one may wish to use only principal ideal factorization of a prime number, but the solution of the so-called norm equation will be still exponentially hard.

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 $(F, \Phi'_F)$, and bit-length $c$ for prime numbers.
Output : $\pi_0$: 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 $\pi_0$ as the Weil number of type $(A_0)$ of order 1 associated with $p$.
```

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, $(F, \Phi'_F)$.
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 $C/\mathbf{F}_p$.
```

Remark 1. *The Weil number of type (A_0) is unique up to scaling by the roots of unity. These scaled Weil numbers then represent the so-called twists of the Abelian varieties. In fact, it is known not all of twists can be always found as curves. However, almost all twist are found as curves in our experiments. Therefore, the twist problem seems not a serious problem in practice.*

5. EXAMPLE

We show an example using the curve

$$C/\mathbf{Q} : Y^2 = X^5 + 3X^4 - 2X^3 - 6X^2 + 3X + 1 \tag{1}$$

described in [27][25], where 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 $\alpha = \sqrt{-2+\sqrt{2}}$.

An integral basis $\mathbf{B} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \end{pmatrix}$ of K is used. 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 $\psi_i = \varphi_i^{-1} : \alpha \mapsto \alpha_i$ where $\alpha_1 = \alpha$ and $\alpha_2 = 3\alpha + \alpha^3$. Then using the proposed algorithms, we found a principal prime ideal of K

$$(\omega) = \mathbf{B} \begin{pmatrix} 146241 \\ -241873 \\ 887081 \\ -526503 \end{pmatrix} \mathcal{O}_K$$

such that $p = N_{K/\mathbf{Q}}(\omega) = 2353539104668601065177079$. A Weil number of type-$(A_0)$ is derived as

$$\pi_0 = \omega^{\psi_1}\omega^{\psi_2} = \mathbf{B} \begin{pmatrix} 869249529777 \\ -1820564551008 \\ -103525925671 \\ -386358829007 \end{pmatrix} .$$

Then we obtained $\#\mathcal{J}(\mathbf{F}_p) = N_{K/\mathbf{Q}}(1-\pi_0) = 4 \times p_{max}$ where p_{max} is a $160 bits$ prime $1384786579298536962658040825319326195404691870759$. Finally we obtained a secure curve over $\mathbf{F}_p$ as follows,

$$\begin{aligned} C/\mathbf{F}_p : Y^2 =& X^5 + 3X^4 + 2353539104668601065177077X^3 \\ &+ 2353539104668601065177073X^2 + 3X + 1 \end{aligned}$$

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 Timing to construct secure Jacobians

	iterations	time (sec.)
φ_i	1	1.6
ω	2490	16.9
π_0	58	0.2
$\#\mathcal{J}(\mathbf{F}_p)$	58	1.2
Total		19.9

6. COMPLEXITY ANALYSIS

We will denoted $[L : \mathbf{Q}]$ and $[F : \mathbf{Q}]$ as n and d respectively.

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

Proof. The algorithm is based on the relation between the congruence zeta function of the curve over a finite field and the characteristic polynomial of the Frobenius endomorphism of its Jacobian varieties over the same finite field (See [14]). This relation is used to check the CM type and reflex CM type.

The computation cost can be analyzed as follows. One can choose in Step 1 a prime number splitting completely in L, thus we can take $p = O(n^n)$. Thus to derive an ordinary reduction needs $O\left(n^{n+3}\log^3 n + n^{n+1}\log^4 n\right)$ bit-operations (see also the proof of Theorem 5). The Step 2 needs $O(gn\log^3 n)$ for counting points of C over a field of cardinality $O(n^n)$. The cost in Step 3 and 4 is that of type norm of ω, to calculate it takes $O(gn^4\log^2 n)$bit-operations. The number of combinations for ψ_i is 2^n. □

Remark 2. *It can be noticed that, unlike the Algorithm 2 and 3 which have to use very large prime numbers for calculation the Weil numbers and design the Jacobian varieties, the prime p used in the Algorithm 1 to calculate CM type could be choosed as small as possible. Thus its cost will depend mainly on the extension degree of the definition field of the curve. Therefore, we will use only the curves which are defined over number fields with reasonable degrees, thus bounded discriminants. (This is consistent with the fact that all curves which have used until now are over the rational number field* $\mathbf{Q}$*)*

Theorem 5. *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.*

Proof. Correctness of the algorithm is based on Theorem 2 and 3.

We have to consider the costs of following computations: 1. Construction of an integral basis for $\mathcal{O}_L$; 2. Computation of Galois action on L; 3. Search algebraic integer $\omega \in \mathcal{O}_F$ such that $N_{F/\mathbf{Q}}\omega$ is a prime; 4. Computation of type norm of ω in $\mathcal{O}_F$;

The integral basis of $\mathcal{O}_L$ will cost $O\left(n^4\right)$ when $disc(L)$ is factorizable [22]. The Galois actions on L can be realized by computations of n $n \times n$ matrices, whose entries are bounded by the discriminant of L. Thus, these mappings can be calculated in $O\left(n^4\right)$.

The absolute norm is computed by matrix computations and multiplications on $\mathcal{O}_F$. It needs d multiplications of $n \times n$ matrices and

n-D vectors. Assuming the entries of the matrix are bounded by the discriminant of L, they cost $O\left(dn^2 \log^2 p\right)$bit-operations. Since $d-1$ multiplications on $\mathcal{O}_L$ need $O\left(dn^2 \log^2 p\right)$bit-operations, the total cost will be $O\left(dn^2 \log^2 p\right)$bit-operations.

To search an $\omega \in \mathcal{O}_F$ with a prime absolute norm, we use random combinations of the integral basis $\{b_i \in \mathcal{O}_F | i = 1 \ldots d\}$ to generate $\omega = \sum_{i=1}^{d} \omega_i b_i | \omega_i \in \mathbf{Z}$, then calculate its absolute norm and check if it is a pseudo prime. The search will be carried out for ω in $0 \leq |\omega_i| < p^{\frac{1}{d}}$. The probability that the absolute norm of an algebraic number is prime p equals $1/\left(d^d h \log p\right)$. In fact, assuming that the probability of absolute norm of an ideal of $\mathcal{O}_F$ to be prime equals $1/\log p$, then the probability for such an ideal to be principal is $1/h$, where h is the class number of F which is of $O(disc(F)^{1/2})$, and the probability of such an ideal splits completely in $\mathcal{O}_F$ is $1/d^d$. Thus $d^d h \log p$ searches will be needed.

Including also the cost for probabilistic prime tests, an ω with prime absolute norm can be found in $O\left(d^d(n^2 \log^3 p + \log^4 p)\right)$bit-operations.

Computation of the type norm of ω on $\mathcal{O}_F$ will cost the same order as of absolute norm.

In conclusion, Algorithm 2 has complexity of $O\left(d^d(n^2 \log^3 p + \log^4 p)\right)$ bit-operations. □

Theorem 6. *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.*

Proof. This follows immediately from the above theorem. □

References

[1] L.M.Adleman, M.D.A.Huang, "Counting rational points on curves and abelian varieties over finite fields," Proc. of ANTS-2, Springer-Verlag, (1996).

[2] L.M.Adleman, J.D.Marrais, 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] S.Arita, "Public key cryptosystems with C_{ab} curve (2)," IEICE Japan, Proc. of SCIS'98, 7.1-B, (1998).

[4] 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.

[5] J.De Jong, R.Noot, "Jacobians with complex multiplication," Arithmetic Algebraic Geometry, Birkhäuser ,PM89, pp.177-192, (1991).

[6] G. Frey, M. Müller, "Arithmetic of modular curves and applications," pre-print.

[7] 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).

[8] P.Gaudry, R.Harley, "Counting Points on Hyperelliptic Curves over Finite Fields," pre-print.

[9] T.Honda, "Isogeny classes of abelian varieties over finite fields," J.Math.Soc.Japan, vol.20, No.1-2, p.83-95, (1968).

[10] H. Kawashiro, O. Nakamura, J. Chao, S. Tsujii, "Construction of CM hyperelliptic curves using RM family," IEICE Japan ISEC97-72, pp.43-49, (1998).

[11] N.Koblitz, "Elliptic Curve Cryptosystems," Math. Comp.,vol.48, p.203-209, (1987).

[12] N.Koblitz, "Hyperelliptic cryptosystems," J. of Cryptology, vol.1, p.139-150, (1989).

[13] N. Koblitz, "A very easy way to generate curves over prime field for hyperelliptic cryptosystems," CRYPTO'97, Ramp session, (1997).

[14] S.Lang, "Abelian Varieties", Interscience, New York (1959).

[15] S.Lang, "Complex multiplication" Springer-Verlag, (1983).

[16] K.Matsuo, J.Chao, S.Tsujii, "On lifting of CM hyperelliptic curves," IEICE Japan Proc. SCIS'99, (1999).

[17] V.S.Miller, "Use of Elliptic Curves in Cryptography," Proceedings of Crypto'85 , LNCS218, Springer-Verlag, p.417-426, (1986).

[18] V. Müller, A. Stein, C. Thiel, "Computing discrete logarithms in real quadratic congruence function fields of large genus," Preprint, Nov. 13, (1997).

[19] K.Nagao, "Construction of the Jacobians of Curves $Y^2 = X^5 + k/\mathbf{F}_p$ with Prime Order," Manuscript, (1998).

[20] S. Paulus, "Ein Algorithmus zur Berechunung der Klassengruppe quadratischer Ordnungen über Hauptidealringen," GH Essen, Dr. Thesis, (1996).

[21] J.Pila, "Frobenius maps of abelian varieties and finding roots of unity in finite fields," Math. Comp., vol.55 , p. 745-763, (1990).

[22] M.Pohst, "Computational Algebraic Number Theory," DMV21, Birkhäuser, (1993).

[23] H.G. Rück, "On the discrete logarithm problem in the divisor class group of curves," Preprint, 1997.

[24] G. Shimura, "Abelian Varieties with Complex Multiplication and Modular Functions," Princeton Univ. Press, (1998).

[25] A-M. Spallek, "Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen," Dissertation, preprint, No. 18, (1994).

[26] J.Tate, "Endomorphisms of Abelian varieties over finite fields," Invent. Math. 2, p.134-144, (1966).

[27] P. V. Wamelen, "Examples of genus two CM curves defined over the rationals," Math. Comp., 68(225), pp. 308-320, (1999).