SCIS2000 The 2000 Symposium on Cryptography and Information Security
Okinawa, Japan, January 26-28, 2000

Ordinary lifting を用いたCM超楕円曲線の生成
Construction of CM hyperelliptic curve using ordinary liftings (extended abstract)

芳賀 智之* 松尾 和人† 趙 晋輝‡ 辻井 重男*
Tomoyuki HAGA Kazuto MATSUO Jinhui CHAO Shigeo TSUJII

あらまし 安全な暗号系を豊富に提供することが可能な超楕円曲線を用いた暗号系の構成法において, 現在最も実用的である CM 体法では, 代数体上の CM 超楕円曲線を必要とするが, これまでに提案されている CM 超楕円曲線の構成手法は近似計算を必要とするものであった. しかし, CM 楕円曲線の構成法としては, ordinary lifting を用いた近似計算を必要としない方法が知られている. 本論文では, この方法を拡張し, ordinary lifting によって代数的演算のみを用いて CM 超楕円曲線を構成する方法を提案する.

キーワード 超楕円暗号, 超楕円曲線, Jacobi 多様体, 虚数乗法, CM 体, ordinary lifting

1 まえがき

楕円暗号系はもとより, 平面代数曲線の Jacobi 多様体上の離散対数問題に基づく暗号系は, これまで知られていた素因数分解や有限体上の離散対数問題に基づく暗号系と比べ攻撃が困難なことから, 最近では公開鍵暗号の主流となっている. 特に超楕円曲線を用いた暗号系は, Cantor[5] によって提案された, 高速な加算アルゴリズムによって実用的な暗号系を構築可能なため多くの提案がなされてきた.

代数曲線を用いた暗号系ではその Jacobi 多様体が安全な位数を持つ曲線が必要である. 楕円暗号系では安全な曲線の実用的な構成法が幾つか知られているが, 一般の代数曲線に対しては今のところ効果的な構成法は知られていない. しかし, 超楕円曲線を始め幾つかの曲線の class について, 安全な曲線の構成法が近年盛んに研究されている.

超楕円暗号系の構成法では, 大きく 2 通りの方法が知られている. Order Counting による構成法 [1][37] は, 非常に高次な多項式時間アルゴリズムであり, 実行困難であるうえに, 安全な位数を持つまで繰り返し実行しなければならない. これとは別に Jacobi 多様体が CM(Complex multiplication) を持つ超楕円曲線 (CM 超楕円曲線) を用いた構成法が提案されている [54].

CM 超楕円曲線を用いた構成法は, Weil number を計算することにより, 数体上の CM 曲線を有限体に reduction することによって安全な超楕円曲線を高速に設計できる. また, 1 本の数体上の CM 曲線から多数の暗号系を構築することが可能であり, 実用上非常に効果的な方法である. そこで, この構成法に必要な CM 超楕円曲線の生成法の検討が必要となる.

現在まで知られている CM 超楕円曲線の生成法として Spallek[49] によって提案された方法がある. この方法は, Siegel modular form を用いて Igusa invariant[15] を計算し, genus 2 の CM 曲線の model を求めるものであるが, Wang[58], Weber[59], Walemen[55][56] 等によって様々な拡張, 改良がなされている. 特に, Spallek では invariant から model への変換法が示されていなかったが, Walemen は, ここに Mestre[30] の方法を用いることで, $\boldsymbol{Q}$ 上の genus 2 の CM 超楕円曲線 の model を全て導出することに成功した. しかし, これらの構成法は何れも近似計算を必要とするものであった.

これらとは別に, CM 楕円曲線の生成法として lifting による方法が提案されている [48]. 簡単な代数演算のみを用いるこの生成法を超楕円に拡張した場合, Spallek 等の方法に比べより多くの曲線が得られると期待できる. そこで本論文では, この生成法を基とした, genus 2 の CM 超楕円曲線の生成法を提案する.

* 中央大学理工学部情報工学科, 〒 112-8551 東京都文京区春日 1-13-27, Department of Information and System Engineering, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan
† 東洋通信機株式会社, 〒 253-0192 神奈川県高座郡寒川町小谷 2-1-1, Toyo Communication Equipment Co., LTD., 2-1-1 Koyato, Samukawa-machi, Koza-gun, Kanagawa 253-0192 Japan
‡ 中央大学理工学部電気・電子工学科〒 112-8551 東京都文京区春日 1-13-27, Department of Electrical and Electronic Engineering, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan

2 準備

定義 2.1 (genus 2 の超楕円曲線の標準型)
k を体とする．*genus 2* の超楕円曲線 H は，*char(k)≠2* のとき

$$H : Y^2 = F(X) \tag{2.1}$$
$$F(X) = a_6X^6 + a_5X^5 + \cdots + a_0 \in k[X] \tag{2.2}$$

と定義される．但し，$F(X)$ は重根を持たないものとする．また，$a_6 \neq 0$ または $a_5 \neq 0$ とする．□

$\deg F = 6$ のとき，F が k 上で根 α を持つならばそのときに限り双有理変換

$$(X, Y) \mapsto \left(\frac{1}{X-\alpha}, \frac{Y}{(X-\alpha)^3}\right)$$

によって次数 5 の双有理同値な曲線に同型変換することができる．[3]

H 上の因子 D は，有限形式和 $\sum_i m_iP_i, m_i \in \mathbf{Z}, P_i \in H$ と定義される．また，D の次数は，$deg(D) = \sum_i m_i$ と定義される．特に，次数 0 の因子は，因子群の部分群 $\mathcal{D}^0(H)$ を形成する．

H の有理関数体 $k(H)$ は，

$$k(H) = \{p/q\}, p, q \in k[X, Y], q \not\equiv 0 \bmod Y^2 - F(X)$$

で定義される．$k(H)$ の元 p/q の因子 (p/q) は，$P_i, Q_j \in H$ をそれぞれ，F での零点，極とし，重複度を m_i, n_j とすると，$\sum_i m_iP_i - \sum_j n_jQ_j$ と定義される．このとき，(p/q) を主因子と呼ぶ．

定義 2.2 (Jacobi 多様体)
$D(H)$ を因子の集合，次数 0 の因子の集合を $\mathcal{D}^0(H)$，主因子の集合を $\mathcal{D}^l(H)$ とする．H の *Jacobi* 多様体を

$$\mathbf{J}(H) = \mathcal{D}^0(H)/\mathcal{D}^l(H) \tag{2.3}$$

と定義する．□

H, H' が双有理同値のとき $\mathbf{J}(H)$ と $\mathbf{J}(H')$ はアーベル多様体として同型であることが知られている．

定義 2.3 (超楕円曲線の離散対数問題)
$\mathbf{F}_q$ 上の超楕円曲線を $H/\mathbf{F}_q$，$\mathbf{J}$ を H の *Jacobi* 多様体とする．因子 $D_1, D_2 \in \mathbf{J}(\mathbf{F}_q)$ が与えられたとき，

$$D_2 = mD_1$$

となるような $m \in \mathbf{Z}$ を求める問題を超楕円曲線上の離散対数問題と呼ぶ．□

定義 2.4 (integral invariant)[15]
超楕円曲線 H を (2.1) で定義されるものとする．このとき，$F(X)$ の根を $x_1, \cdots, x_6$ とする．$(x_i - x_j)$ を (ij) と表記すると，Igusa[15] は，4 つ integral invariant を定義している．
$I_2 = {a_6}^2 \sum_{15}(15)^2(34)^2(56)^2$
$I_4 = {a_6}^4 \sum_{10}(12)^2(23)^2(31)^2(45)^2(56)^2(64)^2$
$I_6 = {a_6}^6 \sum_{60}(12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2$
$(25)^2(36)^2$
$I_{10} = {a_6}^{10} \prod_{(i<j)}(ij)^2 = disc(F)$ □

定義 2.5 (absolute invariant) [15]
同次数の 2 つの integral invariant の商は，absolute invariant と呼ばれ

$$i_1 = \frac{{I_2}^5}{I_{10}}, i_2 = \frac{{I_2}^3 I_4}{I_{10}}, i_3 = \frac{{I_2}^2 I_6}{I_{10}} \tag{2.4}$$

と定義される．□

absolute invariant は，以下の重要な補題が成り立つ．

補題 2.1 [15] *genus 2* の超楕円曲線 H, H' に対して，もし，$I_2 \neq 0, {I_2}' \neq 0$ ならば，H と H' が $\mathbf{C}$ 上で双有理同値のときかつそのときに限って

$$i_1 = i_1', i_2 = i_2', i_3 = i_3' \tag{2.5}$$

となる．

3 Ordinary lifting による CM 超楕円曲線の生成

Algorithm 3.1 に ordinary lifting による Jacobi 多様体が CM を持つ超楕円曲線 (CM 超楕円曲線) の生成アルゴリズムを示す．このアルゴリズムは $End(\mathbf{J})$ が CM 体 K の maximal order と同型な曲線を構成するものである．

尚，CM Type が与えられたとき，reflex CM Type を高速に求める方法が提案されている [51]．そこで，本アルゴリズムでは，与えられた CM 体に対してこのアルゴリズムを用いて，reflex CM 体を事前に計算しておく．

また，CM Type に対して，定義体 k の条件が，[46],[60] に示されている．特殊な CM Type に対してこれらの条件から k を求めることが可能であり，事前にこの k は計算済であるとする．

Algorithm 3.1 (Ordinary lifting による CM 超楕円曲線の生成)
Input : *CM* 体 K
Output: CM 超楕円曲線 H

step1 $p := 3$; テーブル $T_c := \{\}$;

step2 reflex CM 体 K' で完全分解する素数 p を選ぶ.

step3 テーブル $T_p := \{\}$;

step4 p の k での惰性次数 r に対し $q := p^r$ とし, $\mathbf{F}_q$ 上の全ての *genus* 2 の超楕円曲線に対しその曲線が *CM* 体 K を持つかどうかチェックする. *CM* 体 K を持つ曲線に対して *invariant* を計算し, かつて選んだ曲線と $\mathbf{F}_q$ 上双有理同値かどうかチェックする. 双有理同値でなければ, 曲線を T_p に入れる. *(Algorithm 3.2* 参照*)*

step5 T_p 内の曲線から $End(\mathbf{J}) \cong \mathcal{O}_K$ *(*K の *maximal order)* なる曲線を T_c に入れる.

step6 T_c 内の曲線から, *(Algorithm5.2)* を用いて, *absolute invariant* を *lift* し, H を構成する.

step7 *CRT* によって得られた H に対して *CM* テストを行い, *pass* すれば, H を出力し終了.

step8 *p:=nextprime(p)* とし *step*2 へ.

素イデアル分解を用いて Weil number の計算から Frobenius endomorphism π の特性多項式

$$Z(X) = X^4 - s_1X^3 + s_2X^2 - s_1qX + q^2 \qquad (3.1)$$

$$s.t. Z(\pi) = 0$$

を高速に求める方法が提案されている [51], [54].

そこで, 事前にこの方法を用いていくつかの q に対して (q, s_1, s_2) のテーブルを用意しておくことで高速化を計る.

Algorithm 3.2 (genus 2 の超楕円曲線が与えられた CM を持つか)

Input : $F(X)$ $s.t$ $H/\mathbf{F}_q$: $Y^2 = F(X)$, (3.1) の s_1, s_2

Output : F $s.t$ $H/\mathbf{F}_q : Y^2 = F(X)$

step1 $\deg F = 6$ のとき $\mathbf{F}_q$ 上で根を持つかチェックする. 根を持たなければ, *step5* へ.

step2 $C := q^2 + 1 + s_2 - s_1(1+q)$;
$C_t := q^2 + 1 + s_2 + s_1(1+q)$;

step3 $\mathbf{J}$ を H の *Jacobi* 多様体とし, $d \in \mathbf{J}(\mathbf{F}_q)$ をランダムに選ぶ. 幾つかの d に対して, Cd, C_td を計算することにより, $H/\mathbf{F}_q$ の *Frobenius endomorphism* の特性多項式が $Z(X)$ である可能性, または $H/\mathbf{F}_q$ の *Frobenius endomorphism* の特性多項式 $Z_t(X)$ である可能性をチェックする.

step4 もし, $Cd \neq 0$ *and* $C_td = 0$ ならば $F := F_t$*(H* の *quadratic twist);*

step5 $\#H(\mathbf{F}_q), \#H(\mathbf{F}_{q^2})$ を計算することにより, F に対応する *Frobenius endomorphism* の特性多項式が $Z(X)$ であるか, $Z_t(X)$ であるかをチェックする.

step6 もし, $H/\mathbf{F}_q$ の *Frobenius endomorphism* の特性多項式が $Z_t(X)$ であるならば $F := F_t$ *(H* の *quadratic twist); F* を出力し終了.

Algorithm 3.2 に於いて, step1 で入力された $\deg F = 6$ の曲線 H が $\mathbf{F}_q$ 上で根を持つ場合, H を $\deg F = 5$ の双有理同値な曲線に変換してチェックを行う.

出力の F は対応する Jacobi 多様体の Frobenius endomorphism の特性多項式が (3.1) になっている.

4 探索曲線の削減

Algorithm 3.1 の step4 において $\mathbf{F}_q$ 上の全ての曲線に対して CM を持つかどうかチェックしなければならない. 本アルゴリズムに於いてこの部分が計算量の dominant である. したがって, 探索する曲線を出来る限り削減することが望ましい.

定義 4.1 (quadratic twist)
超楕円曲線 $H/\mathbf{F}_q$ を (2.1) で定義されたものとする. このとき, 平方非剰余数 $c \in \mathbf{F}_q$ に対し, H の *quadratic twist* Ht を,

- $\deg F = 6$ のとき

$$(X, Y) \mapsto (cX, c^{7/2}Y)$$

$$Ht : Y^2 = ca_6X^6 + c^2a_5X^5 + \cdots + c^7a_0 \quad (4.1)$$

- $\deg F = 5$ のとき

$$(X, Y) \mapsto (cX, c^{5/2}Y)$$

$$Ht : Y^2 = a_5X^5 + ca_4X^4 + \cdots + c^5a_0 \quad (4.2)$$

と定義する. □

命題 4.1 $\mathbf{F}_{q^2}$ 上で H, Ht が双有理同値であるとする. このとき, $H/\mathbf{F}_q$ の *Jacobi* 多様体の *Frobenius endomorphism* の特性多項式を

$$Z(X) = X^4 - s_1X^3 + s_2X^2 - s_1qX + q^2 \qquad (4.3)$$

とすると, Ht の *Jacobi* 多様体の *Frobenius endomorphism* の特性多項式は

$$Z_t(X) = X^4 + s_1X^3 + s_2X^2 + s_1qX + q^2$$

である.

したがって, Jacobi 多様体の Frobenius endomorphism の特性多項式が $Z_t(X)$ である曲線を利用可能であり, Algorithm 3.2 では, 命題 4.1 を用いて効率良く CM を持つ曲線を探索することが可能となる.

次に, 命題 4.1 を用いて (2.1) で定義される曲線 H を 2 次拡大体上双有理同値な曲線に分類する.

補題 4.1 $k=\mathbf{F}_q, char(k)\neq 2,3$ とする. $\deg F=6$ のとき, (2.1) で与えられる H に対し,

$$H: Y^2=X^6+a_4X^4+\cdots+a_0$$

なる形式の $\mathbf{F}_{q^2}$ 上双有理同値な曲線が存在する.

proof
$char(k)\neq 2,3$ のとき, 双有理変換 $(X,Y)\mapsto(X+a_5/(6a_6), Y)$ によって 5 次の項を消去できる. さらに $a_6\neq 1$ のとき, $(X,Y)\mapsto(a_6^{-1}X, a_6^{-7/2}Y)$ によって $a_6=1$ を得る.
□

補題 4.2 $k=\mathbf{F}_q, char(k)\neq 5$ とする. $\deg F=5$ のとき, (2.1) で与えられる H に対し,

$$Y^2=X^5+\{0,1,\gamma\}X^3+a_2X^2+a_1X+a_0,$$

$$\gamma\in\mathbf{F}_q: \text{平方非剰余}$$

なる形式の $\mathbf{F}_{q^2}$ 上双有理同値な曲線が存在する.

proof
$char(k)\neq 5$ ならば, 双有理変換 $(X,Y)\mapsto(X+a_4/5, Y)$ によって 4 次の項を消去できる.

さらに $a_5\neq 1$ のとき, 変換 $(X,Y)\mapsto(a_5^{-1}X, a_5^{-3}Y)$ によって $a_5=1$ を得る.

a_3 が $\mathbf{F}_q$ 上で平方剰余のとき $(X,Y)\mapsto(a_3^{-1}X, a_3^{-5/2}Y)$ と双有理変換すると, $a_3=1$, また, a_3 が $\mathbf{F}_q$ 上で平方非剰余のとき, 平方非剰余数 $\gamma\in\mathbf{F}_q$ に対して, $(\gamma/a_3)^{1/2}\in\mathbf{F}_q$ であるので, 変換 $(X,Y)\mapsto((\gamma/a_3)^{1/2}X, (\gamma/a_3)^{5/4}Y)$ によって, $a_3=\gamma$ と変換できる.□

これらの変換によって, Algorithm 3.1 の step4 の探索回数は $O(q^7)$ から $O(q^5)$ に削減される.

5 Invariant の lifting

CRT を用いて absolute invariant を lifting する必要があるが (2.4) で見られるように商の型であるために単に CRT だけでは, lifting することができない. そのため, 整数から有理数への変換アルゴリズムを用いる.

5.1 整数剰余から有理数の復元

$u\in\mathbf{Z}$ が与えられたとき, $u\equiv a/b \pmod m, 1\leq b<\sqrt{m/2}, |a|<\sqrt{m/2}$ を満たすような $a/b\in\mathbf{Q}, \gcd(a,b)=1, b\geq 1$ が高々1 つ存在する. 以下に示すアルゴリズムは, u,m が与えられたときに, 上記のような a,b を求めるものである. このアルゴリズムは拡張ユークリッドの互助法を拡張したもので P. S. Wang[57] よって提案されている.

Algorithm 5.1 (整数剰余から有理数の復元)
一般性を失うことなく $|u|\leq m/2$ とする.
Input : u,m
Output : (a,b) *s.t* $u\equiv a/b \pmod m$

step1 $i:=1; a_0:=m; a_1:=u;$
$b_0:=0; b_1:=1; n:=\sqrt{m/2};$

step2 もし, $|a_i|<n$ ならば (a,b) として $(sign(b_i)\times a_i, |b_i|)$ を出力し終了.
$i:=i+1; q:=quo(a_{i-2}, a_{i-1});$
$a_i:=a_{i-2}-q\cdot a_{i-1}, b_i:=b_{i-2}-q\cdot b_{i-1};$
もし, $|b_i|\geq n$ ならば $a_i:=u; b_i:=1$ とし (a_i,b_i) を出力し終了.
そうでなければ *step2* へ.

したがって, CRT を用いて u を lift した後に, u をこのアルゴリズムを用いて変換することで, 有理数 a/b の lifting を行うことが出来る.

5.2 absolute invariant の lifting

ここでは, いくつかの小さな有限体から CRT と Algorithm 5.1 を用いて absolute invariant の lifting について述べる. このアルゴリズムでは abusolute invariant が一定の値になるまで法を上げていく. I_j は, $\mathbf{F}_{q_j}$ 上での absolute invariant とする.

Algorithm 5.2 (absolute invariant の lifting)
Input : $q_j \quad s.t \quad \mathbf{F}_{q_j}, \quad I_j:=(i_{j1}, i_{j2}, i_{j3})$
Output : $I:=(i_1,i_2,i_3)$

step1 $I_0:=();j:=1;$

step2 $I_j, j=1,\cdots,j$ を用いて, *absolute invariant* $i_k, k=1,\cdots,3$ を $mod \prod_{l=1}^{j} q_l$ で各々 *CRT* する.

step3 各 *absolute invariant* i_k に対し $u:=i_k, m:=\prod_{l=1}^{j} q_l$ とし *Algorithm 5.1* を実行.

step4 $I:=(i_1,i_2,i_3); I=I_0$ ならば I を出力し終了.
そうでなければ $I_0:=I, j:=j+1$ とし, *step2* へ.

例 5.1 *H:* $Y^2=-8X^6+52X^5-250X^3+321X+131$ は *CM* 体 $K:=\mathbf{Q}(\sqrt{-5+\sqrt{5}})$ を持つ [55]. H の *absolute invariant* I は,

$$I=\left\{\frac{2\cdot 3^{10}5^5719^5}{11^{12}}, \frac{2\cdot 3^8 5^5 719^3}{11^8}, \frac{2\cdot 3^7 5^5 719^3}{11^8}\right\} \quad (5.1)$$

である.

reflex CM 体 K' で完全分解する素数 p を選び,

p: $\{19, 29, 31, 41, 59, 71, 109, 139, 149, 151, 179, 191, 229, 241, 269, 271, 281, 311, 349, 379, 389, 401, 419\}$ に対して $H/\mathbf{F}_p$ の absolute invariant を Algorithm 5.2 を用いて lifting すると確かに (5.1) に復元することができる.

参考文献

[1] L. M. Adleman, M. D. 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] J. W. S. Cassels, E. V. Flynn: "Proglegomena to a middlebrow arithmetic of curves of genus 2", London Math. Soc. LNS230, Cambridge, (1996).

[4] J. Chao, N. Matsuda, S. Tsujii "Efficient construction of secure hyperelliptic discrete logarithm problems" Springer-Verlag LNCS1334, pp.292-301, ICICS'97,Beijing, China, Nov., (1997).

[5] D.Cantor: "Computing in the Jacobian of hyperelliptic curve", Math. Comp., vol. 48, (1987), page 95-101.

[6] D. Cox : "Primes of the forms x^2+ny^2", John Wiley and Sons. (1989).

[7] N. D. Elkies: "Elliptic and modular curves over finite fields and related computational issues" "Computational perspectives on number theory", Proceedings of a Conference in Honor of A.O.L. Atkin, AMS, D.A.Buell, and J.T. Teitelbaum ed. pp.21-76, Sept. (1995).

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

[9] E. Hecke : "Über die Konstruktion relativ Abelscher Zahlkörper durch Modulfunktionen von zwei Variabeln, Math. Ann. 74, (1913), pp. 465-510.

[10] M.D.Huang, D.Ierardi: "Efficient Algorithms for the Riemann-Roch Problem and for Addition in the Jacobian of a Curve", Proceedings of the Twenty-first ACM Symp. on the Foundations of Computer Science,pp. 678-687, May (1991).

[11] M. D. Huang, D. Ierardi: "Counting Rational Point on Curves over Finite Fields", manuscript.

[12] K. Hashimoto, N. Murabayashi: "Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two", Tohoku Math.J. 47, (1995), page 271-296.

[13] T. Honda: "Isogeny classes of abelian varieties over finite fields", J. Math. Soc. Japan , vol. 20, Nos. 1-2,pp. 83-95, (1968).

[14] T. Honda: "On The Jacobian Variety of The Algebraic Curve $y^2 = 1-x^l$ over A Field of Characteristic $p > 0$", Osaka J. Math., vol 3,pp. 189-194 (1968).

[15] J. Igusa: "Arithmetic variety of moduli for genus two", Ann. of Math., vol 72 No.3,pp. 612-649, (1960).

[16] H. Kawashiro, O. Nakamura, J. Chao, S.Tsujii: "Construction of CM hyperelliptic curves using RM families", Tech. Rep IEICE. ISEC97-72, pp. 43-50, March, (1998).

[17] N. Koblitz: "Hyperelliptic cryptosystems", J. Cryptography, 1, pp. 139-150, (1989).

[18] N. Koblitz: "A Family of Jacobians Suitable for Discrete Log Cryptosystems", manuscript.

[19] N. Koblitz: "Algebraic Aspects of Cryptography", ACM 3, Springer, (1998).

[20] D. Kohel "Endomorphism rings of ellitpic curves over finite fields" PhD thesis, UCB, (1996).

[21] H. Kuboyama, K. Kamio, K. Matsuo, J. Chao, S. Tsujii: "Construction of Superelliptic Curve Cryptosystem", IEICE, Japan, Proc. of SCIS2000, C52, (2000).

[22] K. Kurotani, J. Chao, S. Tsujii: "A Consideration on Security of Cryptosystems based on Discrete Logarithm Problems over Abelian Varieties", Proc. of SCIS'97, 12F, (1997).

[23] S. Lang: "Abelian Varieties", Intersciencs, New York, (1959).

[24] S. Lang: "Algebraic Number Theory", Springer-Verlag, (1994).

[25] S. Lang: "Complex Multiplication", Springer-Verlag, (1982).

[26] H. W. Lenstra Jr.: "Complex multiplication structure of elliptic curves", J. Num. Theory, 56, pp. 227-241, (1996).

[27] N. Matsuda, J. Chao, S. Tsujii: "Efficient construction algorithms of secure hyperelliptic discrete logarithm problems", Tech. Rep. IEICE, ISEC96-18, (1996).

[28] K. Matsuo, J. Chao, S.Tsujii : "Design of cryptosistems based on Abelian varieties over extension fields", Tec. Rep. IEICE, ISEC97-30, (1997).

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

[30] J. F. Mestre "Construction de curbes de genere 2 à partir de leurs modules", pp. 313-334 in *Effective methods in algebraic geometry* (Castiglioncello, 1990), edited by T. Mora and C. Traverso, Progr. Math. 94., Birkhäuser, Boston, (1991).

[31] V. S. Miller: "Use of Elliptic Curves in Cryptography", Proc. of Crypto'85, LNCS218 ,pp.417-426, Springer-Verlag, (1986).

[32] D. Mumford: "Abelian varieties", Tata Studies in Mathematics, Oxford, Bobay, (1970).

[33] D. Mumford: "Tata Lectures on Theta I", Birkhäuser, Boston , (1983).

[34] D. Mumford: "Tata Lectures on Theta II", Birkhäuser, Boston, (1984).

[35] O. Nakamura, N. Matsuda, J. Chao, S. Tsujii: "Cryptosystems Based on CM Abelian Variety", Tec. Rep. IEICE, ISEC97-81, (1997).

[36] T.Okamoto, K.Sakurai: "Efficient Algorithms for the Construction of Hyperelliptic Cryptosystems", Proc. of CRYPTO'91, LNCS 576, pp. 267-278, (1992).

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

[38] M.Pohst, H.Zassenhaus: "Algorithmic Algebraic Number Theory", Cambridge Univ. Press,(1989).

[39] M.Pohst: "Computational Algebraic Number Theory", Birkhäuser, (1993).

[40] T. Sasaki, M. Sasaki : "On Integer-to-rational Conversion" , SIGSAM Bulletin, ACM, 26, pp19-21, (1992).

[41] J. Sato, N. Matsuda, J. Chao, S. Tsujii: "Efficient construction of secure hyperelliptic discrete logarithm problems of large genera", Tec. Rep. IEICE, ISEC96-80, (1997).

[42] J. P. Serre, J. Tate: "Good reduction of abelian varieties", Ann. of Math. (2), 88 (1968), page 492-517.

[43] J. H. Silverman: "The Arithmetic of Elliptic Curves", Springer-Verlag, (1988).

[44] J. H. Silverman: "Advanced Topics in the Arithmetic of Elliptic Curves", Springer-Verlag, (1994).

[45] G. Shimura: "Introduction to the Arithmetic Theory of Automorphic Functions", Princeton Univ. Press, (1971).

[46] G. Shimura : "Abelian varieties with complex multiplication and modular functions", Princeton, (1997).

[47] G. Shimura, Y.Taniyama: "Complex multiplication of abelian varieties and its application to number theory", Pub. Math. Soc. Jap. no.6, (1961).

[48] K. Sobataka, O. Nakamura, J. Chao, S.Tsujii : "Construction of secure elliptic cryptosystems using CM tests and Lifting ", Tech. Rep. IEICE, ISEC97-71, pp. 35-42, March, (1998).

[49] A. M. Spallek: "Kurven vom Geshlcht 2 und ihre Anwendung in Public-Key-Kryptosystememem", Dr. thesis, Essen, (1994).

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

[51] T. Umeki, M. Hosoya, K. Matsuo, J. Chao, S. Tsujii: "Computation of CM Type of Jacobian Varieties", IEICE, Japan, Proc. of SCIS2000, C49, (2000).

[52] Emil J. Volcheck: "Computing in the Jacobian of a plane algebraic curve", manuscript.

[53] W. C. Waterhouse: "Abelian varieties over finite fields", Ann. scient. Ec. Norm. ,Sup. 4^o t. 2, pp.521-560, (1969).

[54] T. Wakabayashi, T. Nakamizo, K. Matsuo, J. Chao, S. Tsujii: "Computation of Weil Number of CM Varieties and Design of Jacobian Cryptosystems", IEICE, Japan, Proc. of SCIS2000, C50, (2000).

[55] P. V. Wamelen : "EXAMPLE OF TWO CM CURVES DEFINED OVER THE RATIONALS" , Math. Comp., vol 68, (1999) pp. 307-320.

[56] P. V. Wamelen : "PROVING THAT A GENUS 2 CURVE HAS COMPLEX MULTIPLICATION" , Math. Comp., vol 68, (1999) pp. 1663-1677.

[57] P. S. Wang : "A p-adic algorithm for univariate partial fractions" , Proc. of ACM SYMSAC'81, ACM, 1981, pp.212-217.

[58] X. Wang: "2-dimensional simple factors of $J_0(N)$", manuscripta math., 87, pp. 179-197, (1995).

[59] H. J. Weber : "Hyperelliptic Simple Factor of $J_0(N)$ with Dimension at Least 3", Experimental Math., vol 6, (1997)

[60] H. Yoshida : "Hecke characters and models of abelian varieties with complex multiplication", J. Fac. Sci. Univ. of Tokyo, Sec. 1A, 28, pp.633-649, (1981).