論　文

井草不変量を用いた超楕円曲線暗号の構成について

松尾　和人[†]　芳賀　智之[††]　趙　晋輝[†††]　辻井　重男[††]

On Construction of Secure Hyperelliptic Curve Cryptosystems Using Igusa Invariants

Kazuto MATSUO[†], Tomoyuki HAGA[††], Jinhui CHAO[†††], and 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，これを求めることは困難な研究課題である．そこで，本論文では超楕円曲線の種数を 2 に限定し，有限体上で与えられた不変量をもつ曲線の定義方程式を求めるアルゴリズムを提案している．また，実装によりアルゴリズムの実用性を確認した．提案アルゴリズムにより，暗号系により多くの超楕円曲線を用いることが可能になると期待される．

キーワード　超楕円曲線暗号，超楕円曲線，井草不変量，虚数乗法，種数 2

1. まえがき

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りつつある．特に楕円曲線暗号は既に多くの実用化がなされているが，これは効果的な安全な楕円曲線の構成法が多く提案されていることも一つの要因である．しかしながら，暗号系の運用にあたっては特定の暗号方式だけを用いることは安全管理上好ましくない．したがって，より一般な曲線である超楕円曲線を用いた暗号系が望まれ，この構成について多くの研究がなされている．

超楕円曲線の Jacobi 多様体上の離散対数問題に基づく暗号系を構成するためには，大別して二つの研究課題がある．その一つは因子の高速算法であり，一つは安全な曲線の構成である．因子の高速算法は近年多くの研究成果 [4], [7], [19], [21] があげられており，奇数次数の曲線を用いた場合には実用上十分な暗号化速度が得られるようになった．安全な曲線の構成は多くの研究 [5], [8], [10], [15], [22], [24]〜[27] がなされているが困難な問題であり暗号研究における一つの課題としてあげることができる．

安全な曲線の構成方法として，その Jacobi 多様体が虚数乗法をもつ代数体上の超楕円曲線（以降 CM 超楕円曲線と呼ぶ）を用いて，暗号系を構成する方法が提案されている [2], [3], [14], [23]．この方法を用いることで 1 本の CM 超楕円曲線から高速かつ豊富に暗号系を構成可能であるが，この方法は代数体上の CM 超楕円曲線を必要とする．代数体上の CM 超楕円曲線を得ることは困難であり現状ではいくつかの例 [13], [22], [24] が知られているに過ぎない．

代数体上の CM 超楕円曲線の構成において曲線の種数を 2 に限定して考えると，楕円曲線の j-不変量に対応する井草不変量 [9] が知られているので，これを用いることで曲線構成を容易に行える可能性がある．しかし，井草不変量を用いた CM 超楕円曲線を構成を行うとき，1. 類多項式の構成法，2. 井草不変量から曲線の定義方程式を求める方法，の二つのアルゴリズムが必要であり，これらのアルゴリズム構成は各々が困難な課題である．井草不変量から曲線の定義方程式を求める方法はいくつか提案されている [5], [16], [22], [26].

† 東洋通信機株式会社，神奈川県
Toyo Communication Equipment Co., Ltd., 1-1, Koyato 2, Samukawa-machi, Koza-gun, Kanagawa-pref., 253–0192 Japan
†† 中央大学理工学部情報工学科，東京都
Dept. of Information and System Engineering, Faculty of Science and Engineering, Chuo University, 1–13–27 Kasuga, Bunkyo-ku, Tokyo, 112–8551 Japan
††† 中央大学理工学部電気電子情報通信工学科，東京都
Dept. of Electrical, Electronic, and Communication Engineering, Faculty of Science and Engineering, Chuo University, 1–13–27 Kasuga, Bunkyo-ku, Tokyo, 112–8551 Japan

しかし，これらはいずれも代数体上の不定代数方程式系を解く必要が有り実用的な方法とは言えず，CM 超楕円曲線の構成ひいては超楕円曲線を用いた暗号系の構成を困難にしている要因の一つとなっている．これらの方法はいずれも代数体上の曲線の定義方程式を求めるものであるが，安全な楕円曲線の構成では不変量を有限体上に reduction した後に有限体上の曲線の定義方程式を求める効果的な方法が存在し [17], [18]，超楕円曲線の場合にも有限体上で曲線の定義方程式を求めることで，この問題が解決することが期待できる．

そこで，本論文では超楕円曲線の種数を 2 に限定し，有限体上で与えられた不変量をもつ曲線の定義方程式を求めるアルゴリズムを提案する．曲線の定義方程式を求めるアルゴリズムは，因子の高速算法が奇数次数の曲線に限定されていることを考慮し，定義方程式の次数を奇数に限定することで実現した．定義方程式の次数を奇数に限定することで，不定代数方程式系を解くこと無く曲線の定義方程式を求めることが可能となり，十分な実用性をもったアルゴリズムが得られた．

提案アルゴリズムを用いて CM 体法 [18] として知られている楕円曲線暗号の構成法を超楕円曲線に一般化することで，暗号系にこれまでより多くの超楕円曲線を用いることが可能になると期待される．

本論文の構成はまず **2.** で後に必要になる知識の導入を行い，**3.** で井草不変量から超楕円曲線の定義方程式を求めるために必要となる曲線の同型類を与える．これによって定義方程式のパラメータ空間を限定し，曲線の定義方程式の求解をアルゴリズム化可能にしている．次に，**4.** で実際のアルゴリズムを与え，**5.** で提案アルゴリズムの計算量評価を実装結果とともに与える．

2. 準　　備

本章では種数 2 の超楕円曲線とその井草不変量の定義を与え，後に必要になる性質について述べる．

2.1 超楕円曲線

［定義 2.1］**（種数 2 の超楕円曲線の標準形）**
k を体とする．genus 2 の超楕円曲線 H は，$\mathrm{char}\, k \neq 2$ のとき

$$H : Y^2 = F(X) \tag{1}$$

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

と定義される．ただし，$F(X)$ は重根をもたないものとする．また，$a_6 \neq 0$ または $a_5 \neq 0$ とする．

本論文では超楕円曲線と言った場合必ず種数 2 の超楕円曲線を意味するものとする．

$\deg F = 6$ のとき，F が k 上で根 α をも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 の曲線に同型変換することができる [1].

これまでに提案されている Jacobi 多様体上の高速算法 [4], [7], [19], [21] はすべて奇数次の曲線に対するものである．したがって，超楕円曲線を暗号に利用する場合，奇数次の曲線を用いることになる．そこで，以下では $\deg F = 5$ とし，(1) において $a_6 = 0, a_5 \neq 0$ とする．

［Remark 2.1］ 実際には，有限体上定義された 6 次の超楕円曲線は約 60%が 5 次曲線に同型変換可能である．

H, H' が代数的閉体上同型であるときその Jacobi 多様体 $\mathcal{J}_H$ と $\mathcal{J}'_H$ は代数的閉体上同型であることが知られている．

2.2 井草不変量

［定義 2.2］**（Integral invariant）** [9]
超楕円曲線 H が (1) で定義されるものとする．このとき，$F(X)$ の根を $x_1, \cdots, x_6$ とし，$(x_i - x_j)$ を (ij) と表記すると，integral invariant [9] は，以下で定義される．

$$I_2 = {a_6}^2 \sum_{15} (15)^2(34)^2(56)^2 \tag{3}$$

$$I_4 = {a_6}^4 \sum_{10} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2 \tag{4}$$

$$I_6 = {a_6}^6 \sum_{60} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2 \cdot (14)^2(25)^2(36)^2 \tag{5}$$

$$I_{10} = {a_6}^{10} \prod_{(i<j)} (ij)^2 = \mathrm{disc}\,(F) \tag{6}$$

［Remark 2.2］ $a_6 = 0$ のときは x_i の一つを無限遠点とする．この場合，実際には $a_6 \neq 0$ として I_i を評価した後に $a_6 = 0$ と置くことで I_i の explicit な形式を得る．

［定義 2.3］**（Absolute invariant）** [9]
同次数の二つの integral invariant の商は，absolute invariant と呼ばれ

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

$$i_4 = \frac{I_4 I_6}{I_{10}}, i_5 = \frac{I_4^5}{I_{10}^2}, i_6 = \frac{I_6^5}{I_{10}^3} \tag{7}$$

と定義される．

Absolute invariant について，以下の重要な補題が成り立つ．

［補題 2.1］ [9] 種数 2 の超楕円曲線 H/k，H'/k に対して，各々の integral invariant を I_j, I_j'，absolute invariant を i_j, i_j' としたとき，$I_2 \neq 0$，$I_2{}' \neq 0$ ならば，H と H' が k の代数的閉体 $\bar{k}$ 上同型のときかつそのときに限って

$$i_1 = i_1', i_2 = i_2', i_3 = i_3' \tag{8}$$

となる．

$I_2 = 0$ のときは，

$$i_4 = i_4', i_5 = i_5', i_6 = i_6' \tag{9}$$

が同型の必要十分条件になり，以下の議論も同様に成り立つ．そこで，以下では $I_2 \neq 0$ として議論を進める．

［Remark 2.3］ 実際には $I_2 = 0$ となる曲線は非常に少ない．

3. 曲線の同型類

本章では有限体上の超楕円曲線を代数閉体上の同型で分類し，与えられた absolute invariant をもつ曲線の定義方程式を求めるときのパラメータ空間を小さくし問題を簡単化する．

代数的閉体上の同型変換により以下に示す定理が成り立つ．

［定理 3.1］ $\mathrm{char}\,\mathbb{F}_q \neq 2, 5$ のとき，(1) で与えられる $H/\mathbb{F}_q$ と代数的閉体 $\bar{\mathbb{F}}_q$ 上同型の曲線が必ず

$$Y^2 = X^5 + \{1, \gamma_2\}X^3 + a_2X^2 + a_1X + a_0 \tag{10}$$

$$Y^2 = X^5 + \{1, \gamma_3, \gamma_3^2\}X^2 + a_1X + a_0 \tag{11}$$

$$Y^2 = X^5 + \{0, 1, \gamma_4, \gamma_4^2, \gamma_4^3\}X + a_0 \tag{12}$$

の中に存在する．ここで，$a_2, a_1, a_0 \in \mathbb{F}_q$ $\gamma_2 \in \mathbb{F}_q$ は平方非剰余，$\gamma_3 \in \mathbb{F}_q$ は 3 乗非剰余，$\gamma_4 \in \mathbb{F}_q$ は平方非剰余かつ 4 乗非剰余である任意の数である．

証明： 変換 $(X, Y) \mapsto (a_5^{-1}X, a_5^{-3}Y)$ によって $a_5 = 1$ を得る．また，$(X, Y) \mapsto (X + a_4/5, Y)$ によって $a_4 = 0$ とできる．

a_3 が $\mathbb{F}_q$ 上で平方剰余のとき $(X, Y) \mapsto (a_3^{-1/2}X, a_3^{-5/4}Y)$ と双有理変換すると，$a_3 = 1$，また，a_3 が $\mathbb{F}_q$ 上で平方非剰余のとき，平方非剰余数 $\gamma_2 \in \mathbb{F}_q$ に対して，$(\gamma_2/a_3)^{1/2} \in \mathbb{F}_q$ であるので，変換 $(X, Y) \mapsto ((\gamma_2/a_3)^{1/2}X, (\gamma_2/a_3)^{5/4}Y)$ によって，$a_3 = \gamma_2$ と変換できる．$a_3 = 0, a_2 \neq 0$ のときも同様に，$a_2, a_2/\gamma_3, a_2/\gamma_3^2$ の中の 1 個は 3 乗剰余であるから，これらの中 3 乗剰余のものを γ とすれば，$(X, Y) \mapsto ((1/\gamma)^{1/3}X, (1/\gamma)^{5/6}Y)$ によって，$a_2 = a_2/\gamma$ を得る．明らかに，$a_3 = a_2 = 0$ の場合も同様の変換によって (12) を得る． □

［Remark 3.1］ $Y^2 = X^5 + a_0$ のとき $I_2 = 0$ である．

［Remark 3.2］ 定理 3.1 は数学的な分類を与えるわけではない．実際，(10)，(11)，(12) には互いに同型な曲線が存在する．しかし，我々の構成ではこのことは問題にならない．

上記の曲線の integral invariant は 3 変数多項式，すなわち $k[a_2, a_1, a_0]$ の元と考えられ，

$$I_2 = 40a_1 + 6a_3^2 \tag{13}$$

$$I_4 = 36a_1a_3^2 - 12a_2^2a_3 + 300a_0a_2 - 80a_1^2 \tag{14}$$

$$\begin{aligned} I_6 = {} & 72a_1a_3^4 + 1600a_1a_0a_2 + 330a_0a_3^2a_2 \\ & + 26a_1a_3a_2^2 + 176a_1^2a_3^2 + 2250a_0^2a_3 \\ & - 24a_2^2a_3^3 - 320a_1^3 - 36a_2^4 \end{aligned} \tag{15}$$

$$\begin{aligned} I_{10} = {} & 108a_2^5a_0 - 128a_1^4a_3^2 + 108a_3^5a_0^2 \\ & + 16a_3^4a_1^3 - 27a_2^4a_1^2 + 256a_1^5 + 3125a_0^4 \\ & - 1600a_2a_1^3a_0 + 2250a_2^2a_1a_0^2 \\ & + 2000a_1^2a_3a_0^2 - 900a_1a_3^3a_0^2 - 3750a_2a_0^3a_3 \\ & + 825a_2^2a_3^2a_0^2 + 16a_3^3a_2^3a_0 - 4a_3^3a_2^2a_1^2 \\ & + 144a_2^2a_1^3a_3 - 630a_2^3a_1a_3a_0 \\ & - 72a_3^4a_2a_1a_0 + 560a_1^2a_3^2a_2a_0 \end{aligned} \tag{16}$$

で与えられる．ここで，a_3 は F の 3 次の項の係数を表す．すなわち $a_3 \in \{0, 1, \gamma_2\}$ である．

4. 井草不変量を用いた曲線の構成

本章では与えられた $i_1, i_2, i_3 \in \mathbb{F}_q$ に対応する $\mathbb{F}_q$ 上の曲線の定義方程式の計算アルゴリズムを提案する．提案アルゴリズムは，多項式の終結式を用いて，absolute invariant から integral invariant を経由し曲線の定義式のパラメータ $a_3, a_2, a_1, a_0 \in \mathbb{F}_q$ を求めるものである．(7) に a_3 の値を与えることで 3 変数方程式を 3 個作ることが可能であり，これを $a_2, a_1, a_0 \in \mathbb{F}_q$ について解くことで目的は達せられる．すなわち，

$$i_1 I_{10} - {I_2}^5 = 0 \tag{17}$$

$$i_2 I_{10} - {I_2}^3 I_4 = 0 \tag{18}$$

$$i_3 I_{10} - {I_2}^2 I_6 = 0 \tag{19}$$

を $a_3 = 1$ として $a_2, a_1, a_0 \in \mathbb{F}_q$ について解き，解をもたなかったときには，$a_3 = \gamma_2$ として同様の手順を繰り返せばよいことがわかる．$a_3 = \{1, \gamma_2\}$ に対して解が無かった場合には $a_3 = 0$ としてまた同様に a_2 を $\{1, \gamma_3, \gamma_3^2\}$ から選んで 2 変数方程式をとき，更に根をもたなければ，a_1 を $\{1, \gamma_4, \gamma_4^2, \gamma_4^3\}$ から選んで 1 変数方程式を解けばよいことになる．以上の計算で解が無ければ $i_1, i_2, i_3 \in \mathbb{F}_q$ に対応する曲線は $\mathbb{F}_q$ 上 5 次方程式として定義されない．以上をまとめたアルゴリズムを以下に示す．

［Algorithm 4.1］**（曲線の構成）**

入力：$i_1, i_2, i_3 \in \mathbb{F}_q$ ただし，$i_1 \neq 0$.
出力：i_1, i_2, i_3 を invariant とする曲線に対応する 5 次の $F \in \mathbb{F}_q[X]$.

1: $a_3 = 1$ とする．
2: (17)，(18)，(19) を解き，$a_2, a_1, a_0 \in \mathbb{F}_q$ を求める．
3: $a_2, a_1, a_0 \in \mathbb{F}_q$ が求まったならば，

$$F(X) = X^5 + a_3 X^3 + a_2 X^2 + a_1 X + a0$$

を出力し終了．
4: $a_3 = 1$ ならば $a_3 = \gamma_2$ として step2 へ．
5: $a_3 = 0, a_2 = 1$ とする．
6: (17)，(18)，(19) を解き，$a_1, a_0 \in \mathbb{F}_q$ を求める．
7: $a_1, a_0 \in \mathbb{F}_q$ が求まったならば，

$$F(X) = X^5 + a_2 X^2 + a_1 X + a0$$

を出力し終了．
8: $a_3 = 1$ ならば $a_3 = \gamma_3$，$a_3 = \gamma_3$ ならば $a_3 = \gamma_3^2$ として step6 へ．
9: $a_3 = 0, a_2 = 1$ とする．
10: (17)，(18)，(19) を解き，$a_1, a_0 \in \mathbb{F}_q$ を求める．
11: $a_1, a_0 \in \mathbb{F}_q$ が求まったならば，

$$F(X) = X^5 + a_2 X^2 + a_1 X + a0$$

を出力し終了．
12: $a_3 = 1$ ならば $a_3 = \gamma_3$，$a_3 = \gamma_3$ ならば $a_3 = \gamma_3^2$ として step6 へ．
13: $a_3 = a_2 = 0, a_1 = 1$ とする．
14: (17)，(18)，(19) を解き，$a_0 \in \mathbb{F}_q$ を求める．
15: $a_0 \in \mathbb{F}_q$ が求まったならば，

$$F(X) = X^5 + a_1 X + a0$$

を出力し終了．
16: $a_2 = 1$ ならば $a_2 = \gamma_4$，$a_2 = \gamma_4$ ならば $a_2 = \gamma_4^2$ $a_2 = \gamma_4^2$ ならば $a_2 = \gamma_4^3$ として step10 へ．
17: $\deg F = 5$ の $F \in \mathbb{F}_q[X]$ は存在しないとして，終了．

本アルゴリズムにおいて時間計算量は step2 が支配的であり，この step の繰返し回数は高々2 回である．したがって，本アルゴリズムの計算量は step2 の計算量で押えられる．

以下，step2 の計算に付いて詳細に記述する．

4.1 $a_3 = 1$ の場合の計算

本節では Algorithm 4.1 の step2 について計算の詳細を述べる．簡単のため $a_3 = 1$ として議論を進めるが，$a_3 = \gamma_2$ の場合も同様の議論が成り立つ．

(13)，(14)，(15)，(16) で与えられる integral invariant に $a_3 = 1$ を代入すると，各々を a_2, a_1, a_0 を変数とする $\mathbb{F}_q$ 上の 3 変数多項式と見ることができる．そこでこれらを (17)，(18)，(19) に代入して得られる 3 元 3 連立非線形方程式系を解くことで a_2, a_1, a_0 を求めることが可能である．この方程式系は多項式終結式を利用して解くことが可能である．そこで (17)，(18)，(19) の左辺を以下のように置く．

$$f_1 = i_1 I_{10} - {I_2}^5 \tag{20}$$

$$f_2 = i_2 I_{10} - {I_2}^3 I_4 \tag{21}$$

$$f_3 = i_3 I_{10} - {I_2}^2 I_6 \tag{22}$$

(20)，(21)，(22) の共通零点を求めることで曲線の定義方程式を決定できる．すなわち，

$$\begin{cases} f_1|_{a_0=A_0, a_1=A_1, a_2=A_2, a_3=1} = 0 \\ f_2|_{a_0=A_0, a_1=A_1, a_2=A_2, a_3=1} = 0 \\ f_3|_{a_0=A_0, a_1=A_1, a_2=A_2, a_3=1} = 0 \end{cases} \tag{23}$$

を満足する $A_0, A_1, A_2 \in \mathbb{F}_q$ が，

$$I_{10}|_{a_0=A_0, a_1=A_1, a_2=A_2, a_3=1} \neq 0 \tag{24}$$

を満足するとき，

$$Y^2 = X^5 + X^3 + A_2 X^2 + A_1 X + A_0 \tag{25}$$

は，与えられた absolute invariant (i_1, i_2, i_3) をもつ．ここで $|_{a=A}$ は変数 a への値 A の代入を表す．以降

でこの A_0, A_1, A_2 を求めていく．以降では f_1, f_2, f_3 には $a_3 = 1$ が代入されているとする．

まず，(23) に対して a_2 を変数として終結式を求めることにより，a_2 を消去する．a_2 を消去した独立な 2 式を (26)，(27) に示す．

$$r_1 = \mathrm{res}_{a_2}(f_1, f_2) \tag{26}$$

$$r_2 = \mathrm{res}_{a_2}(f_1, f_3) \tag{27}$$

これらに対して，

$$\begin{cases} r_1|_{a_0=A_0, a_1=A_1} = 0 \\ r_2|_{a_0=A_0, a_1=A_1} = 0 \end{cases} \tag{28}$$

を満足する A_0, A_1 の組は (23) を満足する．更に，これら r_1, r_2 に対して a_0 を変数として終結式を求めることによって，

$$r_3 = \mathrm{res}_{a_0}(r_1, r_2) \tag{29}$$

を得る．

$$r_3|_{a_1=A_1} = 0 \tag{30}$$

は A_1 が (23) を満足することの必要条件である．r_3 は有限体上の 1 変数多項式であるので，因数分解の高速アルゴリズム [6], [20] を用いて，高速に求めることが可能である．A_3 が $\mathbb{F}_q$ 上に解をもつ場合 r_1, r_2 を用いて対応する A_0 を求める．r_1, r_2 に対して $a_1 = A_1$ としたときに，それらの最大公約数

$$g_1 = \gcd(r_1|_{a_1=A_1}, r_2|_{a_1=A_1}) \tag{31}$$

は r_1, r_2 の共通零点の集合になる．そこで，1 変数多項式 g_1 の根，すなわち

$$g_1|_{a_0=A_0} = 0 \tag{32}$$

を満足する $A_0 \in \mathbb{F}_q$ を求めれば，以上で求めた A_1 と A_0 の組は (28) を満足する．更に，

$$g_2 = \gcd(f_1|_{a_0=A_0, a_1=A_1}, f_2|_{a_0=A_0, a_1=A_1}, f_3|_{a_0=A_0, a_1=A_1}) \tag{33}$$

を計算し，

$$g_2|_{a_2=A_2} = 0 \tag{34}$$

を満足する A_2 を求めれば，(30) で求めた A_1 と (32) で求めた A_0 と (34) で求めた A_2 の組は (23) を満足する．

そこで，(16) で与えられる absolute invariant I_{10} にこれらを代入し

$$I_{10}|_{a_0=A_0, a_1=A_1, a_2=A_2, a_3=1} \neq 0 \tag{35}$$

であれば，求めた係数に対応する曲線は与えられた absolute invariant をもつ．

［Remark 4.1］ 以上の議論では変数の消去順序を a_2, a_0, a_1 としていたが，一般にはこの消去順序で必ず解が求まる保証は無い．しかし，実験により，この消去順序以外に a_0, a_2, a_1 という順序で変数消去を行うことで解が存在する場合には必ず解が求まることを確認した．また，$a_3 = \gamma_2$ の場合にも同じ消去順序で解が求まる．更に，実験によりほとんどの場合 a_0, a_2, a_1 の消去順序で解が求まることを確認した．

［例 4.1］ 以上で述べた計算の例を示す．$q = 7, (i_1, i_2, i_3) = (5, 6, 0)$ とし，(i_1, i_2, i_3) に対応する曲線の定義方程式を求める．

まず，(20)，(21)，(22) に $a_3 = 1, i_1 = 5, i_2 = 6, i_3 = 0$ を代入し，

$$\begin{aligned} f_1 &= a_0^4 + 3a_2a_0^3 \\ &\quad + (4a_1^2 + (a_2^2 + 1)a_1 + 2a_2^2 + 1)a_0^2 \\ &\quad + (a_2a_1^3 + 4a_2a_1 + a_2^5 + 3a_2^3)a_0 \\ &\quad + 3a_1^5 + (6a_2^2 + 6)a_1^3 + (5a_2^4 + a_2^2 + 5)a_1^2 \\ &\quad + 3a_1 + 1 \\ f_2 &= 4a_0^4 + 5a_2a_0^3 \\ &\quad + (2a_1^2 + (4a_2^2 + 4)a_1 + a_2^2 + 4)a_0^2 \\ &\quad + (3a_2a_1^3 + 2a_2a_1^2 + 3a_2a_1 + 4a_2^5 + 5a_2^3 \\ &\quad + 6a_2)a_0 \\ &\quad + 2a_1^4 + (5a_2^2 + 6)a_1^3 + (6a_2^4 + 3)a_1^2 \\ &\quad + (5a_2^2 + 1)a_1 + 2a_2^2 \\ f_3 &= (2a_1^2 + 2a_1 + 4)a_0^2 \\ &\quad + (5a_2a_1^3 + a_2a_1^2 + 6a_2a_1 + 6a_2)a_0 \\ &\quad + 6a_1^5 + 2a_1^4 + a_2^2a_1^3 + (4a_2^4 + 6a_2^2 + 5)a_1^2 \\ &\quad + (4a_2^4 + 5)a_1 + a_2^4 + 3a_2^2 \end{aligned}$$

を得る．次に，(26)，(27) を用いて f_1, f_2, f_3 から変数 a_2 を消去し，

$$\begin{aligned} r_1 &= (a_1^{15} + 4a_1^{14} + a_1^8 + 4a_1^7 + 2a_1 + 1)a_0^{13} \\ &\quad + (2a_1^{16} + 5a_1^{15} + 2a_1^{14} + 2a_1^9 + 5a_1^8 + 2a_1^7 \\ &\quad + 4a_1^2 + 3a_1 + 4)a_0^{11} \end{aligned}$$

$$
\begin{aligned}
&+(2a_1^{20}+2a_1^{19}+6a_1^{18}+6a_1^{17}+6a_1^{16}+5a_1^{15}\\
&+6a_1^{14}+2a_1^{13}+2a_1^{12}+6a_1^{11}+6a_1^{10}+6a_1^{9}\\
&+5a_1^{8}+6a_1^{7}+4a_1^{6}+4a_1^{5}+5a_1^{4}+5a_1^{3}+5a_1^{2}\\
&+3a_1+5)a_0^{9}\\
&+(2a_1^{22}+2a_1^{21}+4a_1^{20}+3a_1^{19}+a_1^{18}+3a_1^{17}\\
&+2a_1^{16}+3a_1^{15}+4a_1^{13}+3a_1^{12}+a_1^{11}+3a_1^{10}\\
&+2a_1^{9}+5a_1^{8}+2a_1^{7}+a_1^{6}+6a_1^{5}+2a_1^{4}+6a_1^{3}\\
&+4a_1^{2}+2a_1+3)a_0^{7}\\
&+(5a_1^{24}+a_1^{23}+3a_1^{22}+4a_1^{21}+5a_1^{20}+5a_1^{19}\\
&+6a_1^{18}+2a_1^{17}+5a_1^{14}+5a_1^{13}+5a_1^{12}+6a_1^{11}\\
&+a_1^{9}+3a_1^{8}+2a_1^{7}+3a_1^{6}+3a_1^{5}+5a_1^{4}+a_1^{3}\\
&+5a_1^{2}+a_1+2)a_0^{5}\\
&+(2a_1^{27}+3a_1^{26}+3a_1^{24}+2a_1^{23}+6a_1^{22}+3a_1^{21}\\
&+3a_1^{20}+5a_1^{18}+5a_1^{16}+a_1^{15}+5a_1^{14}+5a_1^{13}\\
&+3a_1^{12}+5a_1^{11}+3a_1^{10}+a_1^{7}+2a_1^{6}+a_1^{5}\\
&+3a_1^{4}+a_1^{3}+6a_1^{2}+4a_1+4)a_0^{3}\\
r_2=&(2a_1^{10}+3a_1^{9}+5a_1^{8}+2a_1^{7}+a_1^{3}+5a_1^{2}+6a_1\\
&+1)a_0^{16}\\
&+(3a_1^{12}+3a_1^{11}+a_1^{10}+6a_1^{9}+a_1^{8}+a_1^{7}+5a_1^{5}\\
&+5a_1^{4}+4a_1^{3}+3a_1^{2}+4a_1+4)a_0^{14}\\
&+(3a_1^{15}+4a_1^{14}+2a_1^{13}+3a_1^{12}+5a_1^{11}+5a_1^{10}\\
&+a_1^{9}+a_1^{6}+5a_1^{5}+6a_1^{4}+6a_1^{3}+4a_1^{2}+a_1\\
&+6)a_0^{12}\\
&+(2a_1^{17}+a_1^{16}+6a_1^{15}+5a_1^{14}+4a_1^{13}+4a_1^{12}\\
&+3a_1^{11}+2a_1^{10}+3a_1^{9}+2a_1^{8}+5a_1^{7}+2a_1^{6}\\
&+2a_1^{5}+5a_1^{4}+4a_1^{3}+3a_1^{2}+3a_1+3)a_0^{10}\\
&+(5a_1^{20}+2a_1^{19}+2a_1^{18}+6a_1^{17}+4a_1^{16}+2a_1^{15}\\
&+a_1^{13}+2a_1^{11}+2a_1^{10}+a_1^{9}+a_1^{8}+5a_1^{7}+a_1^{6}\\
&+3a_1^{5}+4a_1^{4}+3a_1^{3}+3a_1^{2}+6)a_0^{8}\\
&+(5a_1^{21}+5a_1^{20}+6a_1^{19}+2a_1^{17}+a_1^{16}+4a_1^{15}\\
&+6a_1^{14}+3a_1^{13}+2a_1^{12}+a_1^{11}+3a_1^{10}+4a_1^{9}\\
&+5a_1^{8}+2a_1^{6}+3a_1^{5}+4a_1^{4}+a_1^{3}+5a_1)a_0^{6}\\
&+(6a_1^{24}+2a_1^{23}+5a_1^{22}+6a_1^{21}+5a_1^{20}+5a_1^{19}\\
&+4a_1^{18}+3a_1^{17}+4a_1^{15}+a_1^{11}+4a_1^{10}+4a_1^{9}\\
&+6a_1^{8}+6a_1^{7}+4a_1^{6}+4a_1^{5}+3a_1^{4}+2a_1^{3}+4a_1^{2}\\
&+2)a_0^{4}\\
&+(5a_1^{26}+2a_1^{24}+6a_1^{23}+5a_1^{22}+4a_1^{21}+a_1^{20}\\
&+4a_1^{19}+4a_1^{18}+5a_1^{17}+4a_1^{16}+a_1^{15}+4a_1^{14}\\
&+a_1^{13}+a_1^{12}+4a_1^{11}+5a_1^{10}+4a_1^{9}+4a_1^{8}\\
&+a_1^{7}+2a_1^{6}+a_1^{5}+a_1^{4}+5a_1^{3}+5a_1)a_0^{2}\\
&+2a_1^{30}+6a_1^{29}+4a_1^{27}+4a_1^{26}+2a_1^{25}+5a_1^{23}\\
&+2a_1^{22}+6a_1^{21}+a_1^{20}+4a_1^{19}+6a_1^{17}+4a_1^{16}\\
&+5a_1^{15}+3a_1^{14}+3a_1^{13}+3a_1^{12}+a_1^{10}+2a_1^{9}\\
&+2a_1^{8}+2a_1^{7}+a_1^{5}+2a_1^{4}+6a_1^{3}\\
&+4a_1^{2}+4a_1+1
\end{aligned}
$$

を得る．更に，(29) を用いて r_1, r_2 から変数 a_0 を消去し，a_1 を変数とする 630 次多項式 r_3 を得る．$r_3=0$ の解の一つ $a_1=4$ を r_1, r_2 に代入し，それらの最大公約数を取ることで，

$$g_1 = a_0^2$$

を得る．$g_1=0$ の解は $a_0=0$ であるので，これを先程求めた a_1 とともに f_1, f_2, f_3 に代入し，最大公約数を求めると

$$g_2 = 3a_2^2+1$$

となる．そして，$g_2=0$ を解き $a_2=3$ を得る．以上で求めた $a_0=0, a_1=4, a_2=3$ と $a_3=1$ を (16) に代入すると

$$I_{10}=2$$

となる．したがって，

$$Y^2 = X^5+X^3+3X^2+4X$$

は，与えられた absolute invariant $(5,6,0)$ をもつはずであり，確かに与えられた absolute invariant をもつことが確認される．

以上をまとめたアルゴリズムを以下に示す．

［Algorithm 4.2］**（$a_3=1$ の場合の曲線の係数計算）**

入力：$i_1, i_2, i_3 \in \mathbb{F}_q$ ただし，$i_1 \neq 0$.
出力：$a_0, a_1, a_2 \in \mathbb{F}_q$.

1: 変数 $b_1=a_2, b_2=a_0$ とする．
2: (20)，(21)，(22) に i_1, i_2, i_3 と $a_3=1$ を代入した結果をまた f_1, f_2, f_3 とする．
3: $r_1=\mathrm{res}_{b_1}(f_1,f_2), r_2=\mathrm{res}_{b_1}(f_1,f_3)$ を求める．
4: $r_3=\mathrm{res}_{b_2}(r_1,r_2)$ を求める．

5: $r_3 = 0$ の $\mathbb{F}_q$ 上の解を A_1 とする．解が無い場合 step11 へ．
6: $g_1 = \gcd(r_1|_{a_1=A1}, r_2|_{a_1=A1})$ を求める．
7: $g_1 = 0$ の $\mathbb{F}_q$ 上の解を B_2 とする．解が無い場合 step11 へ．
8: $g_2 = \gcd(f_1|_{b2=B2,a_1=A1}, f_2|_{b2=B2,a_1=A1}, f_3|_{b2=B2,a_1=A1})$ を求める．
9: $g_2 = 0$ の $\mathbb{F}_q$ 上の解を B_1 とする．解が無い場合 step11 へ．
10: b_1 に対応する変数値を B_1，b_2 に対応する変数値を B_2，$a_1 = A_1$ として出力し終了
11: $b_1 = a_2$ ならば $b_1 = a_0, b_2 = a_2$ として，step2 へ．そうでなければ終了．

$a_3 = \gamma_2$ の場合は Algorithm 4.2 の step2 において $a_3 = 0$ を $a_3 = \gamma_2$ で置き換えることで，同一アルゴリズムによって，曲線の定義方程式の係数を求めることができる．

4.2 $a_3 = 0$ の場合の計算

本節では Algorithm 4.1 において $a_3 = 1, \gamma_2$ としたときに根をもたなかった場合の計算，すなわち $a_3 = 0$ としたときの計算について述べる．Algorithm 4.1 では step5 以降に当たる．計算は $a \neq 0$ のときと同様の手順で行われる．$a_2 = 1$ として議論を進めるが，$a_3 = \gamma_3, \gamma_3^2$ の場合も同様の議論が成り立つ．

(13), (14), (15), (16)で与えられる integral invariant に $a_3 = 0, a_2 = 1$ を代入すると，各々を a_1, a_0 を変数とする $\mathbb{F}_q$ 上の 2 変数多項式と見ることができる．そこでこれらを (17), (18), (19) に代入し得られる 2 元 3 連立非線形方程式系を解くことで a_1, a_0 を求めることが可能である．この方程式系は $a_3 \neq 0$ の場合と同様に多項式終結式を利用して解くことが可能である．

$a_3 \neq 0$ と同様に (20), (21), (22) に $a_2 = 1$ を代入し，a_0 を変数とみて終結式を求めることにより，(36), (37) を得る．

$$r_1 = \mathrm{res}_{a_0}(f_1, f_2) \tag{36}$$

$$r_2 = \mathrm{res}_{a_0}(f_1, f_3) \tag{37}$$

次に r_1, r_2 の最大公約数

$$g_1 = \gcd(r_1, r_2) \tag{38}$$

を求め，

$$g_1(A_1) = 0 \tag{39}$$

を満足する $A_1 \in \mathbb{F}_q$ を求めれば，A_1 は

$$\begin{cases} r_1|_{a_1=A_1} = 0 \\ r_2|_{a_1=A_1} = 0 \end{cases} \tag{40}$$

を満足する．

同様に，

$$g_2 = \gcd(f_1|_{a_1=A_1}, f_2|_{a_1=A_1}, f_3|_{a_1=A_1}) \tag{41}$$

を計算し，

$$g_2(A_0) = 0 \tag{42}$$

を満足する A_0 を求めれば，この A_0 と (39) で求めた A_1 の組は

$$\begin{cases} f_1|_{a_0=A_0,a_1=A_1,a_2=1,a_3=0} = 0 \\ f_2|_{a_0=A_0,a_1=A_1,a_2=1,a_3=0} = 0 \\ f_3|_{a_0=A_0,a_1=A_1,a_2=1,a_3=0} = 0 \end{cases} \tag{43}$$

を満足する．更に，これらが

$$I_{10}|_{a_0=A_0,a_1=A_1,a_2=1,a_3=0} \neq 0 \tag{44}$$

を満足すれば，求めた係数に対応する曲線は与えられた absolute invariant をもつ．

$a_3 = 1$ のときと同様に変数の消去順序を a_1, a_0 とも取り得るが，実験により消去順序を a_0, a_1 とすれば，解が存在するときには必ず解が求まることを確認した．

明らかに，$a_3 = 0, a_2 = 0$ のときも同様の計算手順で，定義方程式が求まる．

5. 計算量評価

本章では Algorithm 4.1 の計算量について考察する．Algorithm 4.1 において計算量は Algorithm 4.2 が支配的である．表 1 に Algorithm 4.2 で計算される多項式 f_i, r_1, r_2, r_3 の次数を示す．次数は a_0, a_1, a_2 の各々の変数に対する次数を表す．表には示さなかったが，変数の消去順序を a_0, a_2, a_1 としたときには，

表 1　Algorithm 4.2 で計算される多項式の次数
Table 1　Degrees of polynomials computing in Algorithm 4.2.

	a_0	a_1	a_2
f_i	4	5	5
r_1	13	27	0
r_2	17	30	0
r_3	0	630	0

表 2　Algorithm 4.1 の計算時間
Table 2　Computing time of Algorithm 4.1.

$\log_2 q$	全体（秒）	$a_3 \neq 0$（秒）	$a_3 = 0$（秒）
60	20.92	20.88	0.04
80	34.54	34.49	0.05
120	67.88	67.80	0.08
160	115.89	115.76	0.13

表 3　Algorithm 4.2 主要部の計算時間
Table 3　Computing time of dominant parts in Algorithm 4.2.

$\log_2 q$	終結式（秒）	因数分解（秒）
60	0.5	8.3
80	0.5	14.8
120	0.7	30.8
160	0.8	54.6

r_2 の次数は 400 次になる．

表 1 から明らかに，Algorithm 4.2 の計算時間において，r_2 を求める終結式の計算及び r_2 の因数分解が支配的であると考えられる．しかし，Algorithm 4.1 で計算される多項式はすべてその次数が q と独立であり，暗号系に用いる有限体のサイズに対しては終結式が $\mathcal{O}(\log^2 q)$，因数分解は $\mathcal{O}(\log^3 q)$ の時間計算量である．実際の暗号系構成では非常に大きな q を用いるので，計算時間の多項式の次数に対する依存は少なくなり，Algorithm 4.1 は高速に動作すると期待される．そこで，次節で Algorithm 4.1 を暗号系構成に用いるときの実際の計算時間について評価する．

5.1 実装評価

本節では実際に Algorithm 4.1 を実装し，q に対する計算時間の依存性を評価する．実装には PARI/GP を用いた．また，終結式，多項式の因数分解等は PARI の組込み関数を利用した．

計算時間は AMD K6-III 450 MHz 上で測定した．表 2 に Algorithm 4.1 の計算時間の計測結果を示す．実験は，すべての step を計算することになり最も計算に時間がかかるケースとして，5 次の定義方程式をもたない absolute invariant を用いて行った．60 bit，80 bit，120 bit，160 bit の固定した素体上で上記条件を満足する absolute invariannt を各々1000 個ランダムに発生し，各体について Algorithm 4.1 の計算時間の全体，$a_3 \neq 0$ に対する計算時間，$a_3 = 0$ に対する計算時間の absolute invariant 1000 個に対する平均値を測定した．表には示さなかったが計算時間の最悪値と平均値の差は 1%以内に収まっている．

測定結果から提案アルゴリズムが十分な実用性をもつことがわかる．

測定結果から Algorithm 4.1 において $a_3 \neq 0$ すなわち Algorithm 4.2 の計算にほとんどの時間が費されることがわかる．そこで更に，Algorithm 4.2 の r_3 における終結式と因数分解の計算時間を各定義体上で 1000 回測定した．

測定結果の平均値を表 3 に示す．測定結果から実際にはほとんどの計算時間が r_3 の因数分解に費されていることがわかる．終結式と因数分解の計算量の多項式次数の項を比較すると終結式の方が次数に対する計算量の依存度が高いが，この結果は提案アルゴリズムの計算時間の多項式の次数からの影響が少ないことを意味する．

文　献

[1] J.W.S. Cassels and E.V. Flynn, “Proglegomena to a middlebrow arithmetic of curves of genus 2,” London Math. Soc. LNS230, Cambridge U.P., London, 1996.

[2] J. Chao, N. Matsuda, and S. Tsujii, “Efficient construction of secure hyperelliptic discrete logarithm problems,” ICICS ’97, LNCS1334, pp.292–301, Beijing, China, Nov., 1997.

[3] J. Chao, K. Matsuo, and S. Tsujii, “Fast construction of secure discrete logarithm problems over Jacobian varieties,” Proc. of WCC2000, Kluwer Academic,2000.

[4] D. Cantor, “Computing in the Jacobian of hyperelliptic curve,” Math. Comput., vol.48, no.177, pp.95–101, 1987.

[5] G. Frey and M. Müller, “Arithmetic of modular curves and applications,” pre-print.

[6] K.O. Geddes, S.R. Czapor, and G. Labhan, Algorithms for computer algebra, Kluwer Academic, Boston, 1992.

[7] P. Gaudry and R. Harley, “Counting points on hyperelliptic curves over finite fields,” Proc. of ANTS IV, LNCS1838, pp.297–312, Springer-Verlag, 2000.

[8] T. Haga, K. Matsuo, J. Chao, and S. Tsujii, “Construction of CM hyperelliptic curve using ordinary liftings,” IEICE Japan Proc. of SCIS2000, no.C51, 2000.

[9] J. Igusa, “Arithmetic variety of moduli for genus two,” Ann. of Math., vol.72, no.3, pp.612–649, 1960.

[10] H. Kawashiro, O. Nakamura, J. Chao, and S. Tsujii, “Construction of CM hyperelliptic curves using RM families,” Tech. Rep. IEICE Japan ISEC97-72, pp.43–50, 1998.

[11] N. Koblitz, “Hyperelliptic cryptosystems,” J. Cryptography, vol.1, no.3, pp.139–150, 1989.

[12] N. Koblitz, Algebraic aspects of cryptography, ACM 3, Springer-Verlag, Berlin, 1998.

[13] S. Lang, Complex multiplication, Springer-Verlag, Berlin, 1982.

[14] K. Matsuo, J. Chao, and S. Tsujii, “Design of cryptosistems based on Abelian varieties over extension fields,” Tec. Rep. IEICE Japan ISEC97-30, 1997.
[15] K. Matsuo, J. Chao, and S. Tsujii, “On lifting of CM hyperelliptic curves,” IEICE Japan Proc. of SCIS’99, 1999.
[16] J.F. Mestre, “Construction de curbes de genere 2 à partir de leurs modules,” Effective methods in algebraic geometry, Progr. Math. 94, Birkhäuser, pp.313–334, 1991.
[17] A. Miyaji, “Elliptic curve cryptosystems immune to any reduction into the discrete logarithm problem,” IEICE Japan Trans. Fundamentals, E76-A, no.1, pp.50–54, 1993.
[18] F. Morain, “Building cyclic elliptic curves modulo large primes,” Proc. of EUROCRYPT ’91, LNCS547, Springer-Verlag, pp.328–336, 1991.
[19] K. Nagao, “Improving group law algorithms for Jacobians of hyperelliptic curves,” Proc. of ANTS IV, LNCS1838, pp.439–448, Springer-Verlag, 2000.
[20] M.O. Rabin, “Probabilistic algorithms in finite fields,” SIAM J. Comput., vol.9, no.2, pp.128–138, 1980.
[21] N. Smart, “On the performance of hyperelliptic cryptosystems,” Proc. of EUROCRYPTO ’99, LNCS1592, Springer-Verlag, pp.165–175, 1999.
[22] A.M. Spallek, “Kurven vom geshlcht 2 und ihre anwendung in public-key-kryptosystememem,” Dr. thesis, Essen, 1994.
[23] T. Wakabayashi, T. Nakamizo, K. Matsuo, J. Chao, and S. Tsujii, “Computation of Weil number of CM varieties and design of Jacobian cryptosystems,” IEICE Japan Proc. of SCIS2000, no.C50, 2000.
[24] P.V. Wamelen, “Example of genus two CM curves defined over the Rationals,” Math. Comput., vol.68, no.225, pp.307–320, 1999.
[25] P.V. Wamelen, “Proving that a genus 2 curve has complex multiplication,” Math. Comput., vol.68, no.228, pp.1663–1677, 1999.
[26] X. Wang, “2-dimensional simple factors of $J_0(N)$,” Manuscripta Math., vol.87, no.2, pp.179–197, 1995.
[27] H.J. Weber, “Hyperelliptic simple factor of $J_0(N)$ with dimension at least 3,” Experimental Math., vol.6, no.4, 1997.

（平成 12 年 8 月 9 日受付，13 年 2 月 2 日再受付）

松尾　和人　（正員）

昭 61 中大・理工・電気卒．昭 63 同大大学院博士前期課程了．同年東洋通信機入社，現在に至る．暗号理論などの情報セキュリティの研究に従事．

芳賀　智之　（学生員）

平 11 中大・理工・情報卒．現在，同大大学院博士前期課程在学中．暗号理論などの情報セキュリティの研究に従事．

趙　　晋輝　（正員）

昭 57 中国西安電子科技大・電子卒．昭 63 東工大大学院博士課程了．工博．平 1 東工大助手．平 4 中大助教授．平 8 同大教授．暗号理論などの情報セキュリティ，適応信号処理，3D 画像，ヒューマン情報処理などの研究に従事．本会論文賞受賞（昭 63，平 2）．

辻井　重男　（正員）

昭 33 東工大・工・電気卒．同年，日本電気入社．昭 40 山梨大助教授．昭 46 東工大助教授．昭 53 同教授．平 4 中大教授．東工大名誉教授．工博．本会論文賞・業績賞・功績賞．郵政大臣表彰．発明賞．大川出版賞．平 11 日本記念賞．本会会長等歴任．本会名誉員．郵政省電波管理審議会委員．平 11 IEEE 東京支部長．中央大学研究開発機構長．著書「暗号—ポストモダンの情報セキュリティ」（講談社メチエ),「暗号と情報社会」（文藝春秋社），他多数．