論　文

有限体上の超楕円曲線の Jacobi 多様体の自己準同型環の決定法

松尾　和人[†*]　　趙　　晋輝[††]　　辻井　重男[†††]

Determination of Endomorphism Type of Jacobian Varieties of Hyperelliptic Curves over Finite Fields

Kazuto MATSUO[†*], 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暗号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．しかし，これを求めることは困難な課題である．一方，代数体上の CM 楕円曲線の構成法として知られる lifting による方法は CM 体の判別式の多項式時間計算量アルゴリズムであり，これの一般化により豊富な CM 超楕円曲線が得られると期待できる．lifting には有限体上の Jacobi 多様体の自己準同型環を決定する必要があるが，これまで超楕円曲線の Jacobi 多様体に対してこの決定方法は知られていなかった．そこで本論文では有限体上の ordinary 超楕円曲線の Jacobi 多様体の自己準同型環決定アルゴリズムを提案し，その計算量を評価した．更に実装実験を行いその有効性を確認した．

キーワード　超楕円曲線暗号，超楕円曲線，Jacobi 多様体，自己準同型環，Frobenius 写像

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（超楕円曲線暗号）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 divisor の高速算法であり，一つは安全な曲線の構成である．Divisor の高速算法は近年多くの研究成果 [1]〜[5] が挙げられており，実用上十分な暗号化速度が得られるようになった．一方，安全な曲線の構成は多くの研究 [6]〜[20] 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挙げることができる．

安全な曲線の構成法として知られている CM 体法は

（1） 代数体上の CM 超楕円曲線の構成
（2） 曲線の定義方程式の決定
（3） 安全な位数をもつ曲線の決定

の 3 種類のアルゴリズムを必要とする．このうち (2) については効率的なアルゴリズムの提案が有り [18], [20], [21]，種数 2 の曲線については解決されている．また，(3) については高速かつ豊富に暗号系を構成可能な方法が提案されている [8], [14], [17], [18].

(1) については theta 関数のゼロ値を近似計算によって求める方法が知られている [6], [7], [9], [10], [12], [13], [18], [19]．この方法は実際的に効率的に計算が行われいくつかの計算例 [6], [12], [18], [19] も知られている．しかし，近似計算を用いるため誤差伝搬を考慮する必要があり，CM 体の判別式の指数関数時間計算量を必要とする．したがって，より豊富な曲線構成を考えた

† 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-ken, 253–0192 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, 112–8851 Japan
††† 中央大学理工学部情報工学科，東京都
Dept. of Information and System Engineerring, Faculty of Science and Engineering, Chuo University, 1–13–27 Kasuga, Bunkyo-ku, Tokyo, 112–8851 Japan
* 現在，中央大学研究開発機構

とき，この特性により構成可能な曲線が限定されると予想される．

一方，この方法とは別の CM 曲線構成法として，楕円曲線について lifting による方法 [22], [23] が提案されている．この構成法は CM 体の判別式の多項式時間計算量アルゴリズムであり，これを超楕円曲線に一般化することで theta 関数を用いた構成法に比べより多くの CM 超楕円曲線が得られる可能性がある．この一般化について筆者らはこれまでにいくつかの報告 [11], [15], [16] を行ってきたが，いずれも有限体上の超楕円曲線の Jacobi 多様体の自己準同型環の決定が可能であるという前提のもとでの報告であった．

有限体上の超楕円曲線の Jacobi 多様体の自己準同型環決定は，それ自体興味深い研究課題であるが，これまでは楕円曲線に対し Kohel [24] によって提案されたアルゴリズムが存在するのみで，一般の超楕円曲線に対しては Jacobi 多様体の自己準同型環の決定アルゴリズムは知られていなかった．

そこで本論文では CM 超楕円曲線の lifting による構成に必要な，有限体上の超楕円曲線の Jacobi 多様体の自己準同型環の決定アルゴリズムを提案する．また，種数 2 の曲線に対し実装実験を行い，提案アルゴリズムの有効性を確認する．

2. 準　　備

本章では有限体上の超楕円曲線の定義を与え，その Jacobi 多様体の自己準同型環の性質を述べる．更に，以降の章で必要となる CM 体の order の基底について述べる．

標数 $p \neq 2$ の有限体 $\mathbb{F}_q$ 上の種数 g の超楕円曲線 C を下式で定義する．

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

$$F(X) = X^{2g+1} + a_{2g}X^{2g} + \cdots + a_0 \in \mathbb{F}_q[X] \tag{2}$$

ただし，$F(X)$ は重根をもたないものとする．$\mathcal{J}_C$ で C の Jacobi 多様体を表すと，$\mathcal{J}_C$ はアーベル群となり，この $\mathbb{F}_q$-divisor の集合 $\mathcal{J}_C(\mathbb{F}_q)$ は有限アーベル群をなす．

種数 g の超楕円曲線 $C/\mathbb{F}_q$ に対し，その Jacobi 多様体の位数 $\#\mathcal{J}_C(\mathbb{F}_q)$ は下式に示す Hasse-Weil Range に入ることが知られている．

$$(\sqrt{q}-1)^{2g} \leq \#\mathcal{J}_C(\mathbb{F}_q) \leq (\sqrt{q}+1)^{2g} \tag{3}$$

$\mathcal{J}_C(\mathbb{F}_q)$ 上で定義した離散対数問題を用いて，安全な暗号系を構成可能なことは広く知られている．

$\mathcal{J}_C[n]$ で $\mathcal{J}_C$ の n-torsion group を表す．このとき

$$\mathcal{J}_C[p^a] \cong (\mathbb{Z}/p^a\mathbb{Z})^r,\ 0 \leq r \leq g \tag{4}$$

であることが知られている．特に $r = g$ のとき $\mathcal{J}_C$ は ordinary であるといい，このとき本論文では $\mathcal{J}_C$ を ordinary Jacobi 多様体，C を ordinary 超楕円曲線と呼ぶ．

以下では，C は常に ordinary 超楕円曲線であるとする．また，$\mathcal{J}_C$ は simple であるとする．

$\mathcal{J}_C$ の自己準同型環を $\mathrm{End}(\mathcal{J}_C)$ で表す．また，

$$K = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(\mathcal{J}_C) \tag{5}$$

を $\mathcal{J}_C$ の CM 体といい，

$$[K : \mathbb{Q}] = 2g$$

であることが知られている．また，$\mathrm{End}(\mathcal{J}_C)$ は K のある order $\mathcal{O}$ と同型となる．

$\mathrm{End}(\mathcal{J}_C)$ の決定法は lifting による CM 超楕円曲線の構成 [11], [15], [16] に欠かせないが，これまでは C が楕円曲線の場合の決定法 [24] が示されているに過ぎず，一般の場合については検討されていなかった．

今，π_q を $\mathcal{J}_C$ の q 乗 Frobenius 写像，$\chi_q(X) \in \mathbb{Z}[X]$ をその特性多項式とすると，

$$K = \mathbb{Q}(\pi_q) \tag{6}$$

であり，また

$$\chi_q(X) = X^{2g} - s_1X^{2g-1} + s_2X^{2g-2} - \cdots - s_1q^{g-1}X + q^g,\ s_i \in \mathbb{Z} \tag{7}$$

が成立する [25]．このとき，K の maximal order $\mathcal{O}_K$ の $\mathbb{Z}$-basis（rank $2g$ の $\mathbb{Z}$-module としての基底）が以下の補題で与えられる．

補題 1. K を $2g$ 次の CM 体，$\mathcal{O}_K$ を K の maximal order とする．このとき，以下に示す $\mathcal{O}_K$ の $\mathbb{Z}$-basis $\mathbf{B}_K$ が存在する．

$$\mathbf{B}_K = (\omega_1 \quad \omega_2 \quad \cdots \quad \omega_{2g}) \tag{8}$$

ただし $\omega_i = f_i(\pi_q)/d_i, f_i(X) \in \mathbb{Z}[X]$,

$\deg f_i = i-1$, $d_i \in \mathbb{Z}$, $d_{i-1} | d_i$, $f_1 = 1$, $d_1 = 1$.

Proof. [26, V Lemma1.1] を参照. □

$\mathbf{B}_K$ は $\chi_q(X)$ から効率的に計算可能である [26]〜[28].

以後 K の標準基底を

$$\mathbf{B}_{\pi_q} = (1 \quad \pi_q \quad \cdots \quad \pi_q^{2g-1}) \tag{9}$$

と書く．$\mathbf{B}_{\pi_q}$ は $\mathbb{Z}[\pi_q]$ の $\mathbb{Z}$-basis であるが，明らかに

$$\mathbf{B}_{\mathbb{Z}[\pi_q]} = (f_1(\pi_q) \quad f_2(\pi_q) \quad \cdots \quad f_{2g}(\pi_q)) \tag{10}$$

もまた $\mathbb{Z}[\pi_q]$ の $\mathbb{Z}$-basis である．

3. 有限体上の楕円曲線の自己準同型環の決定 [24]

本章では Kohel [24] によって提案された有限体上の ordinary 楕円曲線の自己準同型環の計算アルゴリズムを概説する．

$\mathbb{F}_q$ 上の ordinary 楕円曲線を E と書く．$\mathrm{End}(E)$ で E の $\bar{\mathbb{F}}_q$ 上の自己準同型環を表し c でその conductor を表す．π_q で E の q 乗 Frobenius 写像を表し K で E の CM 体を表す．

ここで自己準同型環の計算とは conductor c の計算を指す．

Kohel は $\mathcal{O}_K$ の $\mathbb{Z}$-basis がある $a, m \in \mathbb{Z}$ に対し

$$\mathbf{B} = \begin{pmatrix} 1 & \frac{\pi_q + a}{m} \end{pmatrix}$$

で与えられることを利用し，c の計算に以下の補題を用いた．

補題 2 (Kohel). 任意の整数 $n \mid m$ に対し

$$\ker(\pi_q + a) \supseteq E[n] \Leftrightarrow \mathrm{End}(E) \supseteq \mathbb{Z} + \mathbb{Z}\frac{\pi_q + a}{n}$$

が成立する．

上記補題により直ちに E の自己準同型環計算アルゴリズムが導かれる．

すなわち m の素因数分解が

$$m = \prod p_i^{e_i}$$

と与えられているとき任意の素因数 p_i に対し

$$E\left[p_i^{j_i}\right] \subseteq \ker(\pi_q + a)$$

かつ

$$E\left[p_i^{j_i+1}\right] \not\subset \ker(\pi_q + a)$$

である j_i が計算されれば c は

$$c = \frac{m}{\prod p_i^{j_i}}$$

で与えられる．Kohel は j_i の計算を E の division polynomial を用いた有限体上の多項式演算で実現した．

4. 自己準同型環の決定

本章では超楕円曲線の Jacobi 多様体の自己準同型環の決定法を提案する．

Division polynomial は超楕円曲線に対し効率的に計算されず，Kohel のアルゴリズムの自然な一般化では超楕円曲線に対し有効なアルゴリズムが構成されない．そこで Baby step giant step algorithm を用いてアルゴリズムの効率化を図る．

4.1 メインアルゴリズム

本節では，まず有限体上の ordinary 超楕円曲線の Jacobi 多様体の自己準同型環計算問題の定式化を行い，次に自己準同型環計算アルゴリズムを提案する．

Jacobi 多様体 $\mathcal{J}_C/\mathbb{F}_q$ の自己準同型環 $\mathrm{End}(\mathcal{J}_C)$ は $\mathcal{J}_C$ の CM 体 K のある order であるので，K の order で

$$\mathrm{End}(\mathcal{J}_C) \cong \mathcal{O}_E \subseteq \mathcal{O}_K \tag{11}$$

を満足する $\mathcal{O}_E$ を求めることが本論文の目的となる．実際には $\mathcal{O}_E$ の $\mathbb{Z}$-basis を求めることで目的は達成される．

π_q を $\mathcal{J}_C$ の q 乗 Frobenius 写像とすると

$$\pi_q \in \mathrm{End}(\mathcal{J}_C) \tag{12}$$

である．よって $\mathcal{O}_E$ は

$$\mathbb{Z}[\pi_q] \subseteq \mathcal{O}_E \subseteq \mathcal{O}_K \tag{13}$$

を満足する．

ここで，補題 1 に現れる f_i を用いて

$$\mathbf{B}_0 = (f_1(\pi_q) \quad \cdots \quad f_{2g-1}(\pi_q) \quad \tfrac{f_{2g}(\pi_q)}{q^{g-1}}) \tag{14}$$

とすると，$\mathbf{B}_0$ は K のある order $\mathcal{O}_0$ の $\mathbb{Z}$-basis であり，この $\mathcal{O}_0$ は

$$\mathbb{Z}[\pi_q] \subseteq \mathcal{O}_0 \subseteq \mathcal{O}_K \tag{15}$$

を満足する．更に，この $\mathcal{O}_0$ に対し以下の補題が成立する．

補題 3.

$$\mathcal{O}_0 \subseteq \mathcal{O}_E \tag{16}$$

Proof. π_q^{-1} を $\mathbf{B}_{\pi_q}$ を用いて

$$\pi_q^{-1} = \mathbf{B}_{\pi_q} \begin{pmatrix} b_1 \\ \vdots \\ b_{2g} \end{pmatrix}, b_i \in \mathbb{Q} \tag{17}$$

と書くと，式 (7) より

$$\begin{aligned} \pi_q \pi_q^{-1} &= \mathbf{B}_{\pi_q} \begin{pmatrix} -q^g b_{2g} \\ \vdots \\ b_{2g-1} + s_1 b_{2g} \end{pmatrix} \\ &= 1 \end{aligned} \tag{18}$$

が成立する．したがって $b_{2g} = -1/q^g$ であり，

$$q\pi_q^{-1} = \mathbf{B}_{\pi_q} \begin{pmatrix} qb_1 \\ \vdots \\ -\frac{1}{q^{g-1}} \end{pmatrix} \tag{19}$$

を得る．これと

$$q\pi_q^{-1} \in \mathcal{O}_E \tag{20}$$

[29, Theorem 7.4] 及び補題 1 の f_i の条件から式 (16) を得る． □

そこで

$$\mathcal{O}_0 \subseteq \mathcal{O} \subseteq \mathcal{O}_K \tag{21}$$

を満足する K の任意の order $\mathcal{O}$ に対し $\mathrm{End}(\mathcal{J}_C) \supseteq \mathcal{O}$ をテストしその包含関係を見ることで $\mathcal{O}_E$ を得る．

Algorithm 1 に有限体 $\mathbb{F}_q$ 上の ordinary 超楕円曲線 C の Jacobi 多様体 $\mathcal{J}_C$ の自己準同型環計算のメインアルゴリズムを示す．

Algorithm 1 中 step 1 の $\mathcal{J}_C$ の q 乗 Frobenius 写像 π_q の特性多項式 $\chi_q(X)$ の計算アルゴリズム，step 8 の $\mathcal{O}_0 \subset \mathcal{O} \subseteq \mathcal{O}_K$ なる K の order の $\mathbb{Z}$-basis $\mathbf{B}_{\mathcal{O}}$ の計算アルゴリズム，step 10 の $\omega \in \mathcal{O}$ に対する $\omega \in \mathrm{End}(\mathcal{J}_C)$ のテストアルゴリズムが得られれば $\mathcal{J}_C/\mathbb{F}_q$ の自己準同型環の計算が可能となる．そこで以下ではこれらのアルゴリズムについて検討する．

Algorithm 1 $\mathcal{J}_C/\mathbb{F}_q$ の自己準同型環

Input: 超楕円曲線 $C/\mathbb{F}_q$
Output: $\mathcal{O}_E \cong \mathrm{End}(\mathcal{J}_C)$ である $\mathcal{J}_C$ の CM 体 K の order $\mathcal{O}_E$
1: $\mathcal{J}_C$ の q 乗 Frobenius 写像 π_q の特性多項式 $\chi_q(X)$ を計算する
2: π_q の多項式を要素とする $\mathcal{O}_K$ の $\mathbb{Z}$-basis $\mathbf{B}_K$ を計算する
3: $\mathcal{O}_E \leftarrow \mathcal{O}_0$
4: **for all** $\mathcal{O}_0 \subset \mathcal{O} \subseteq \mathcal{O}_K$ **do**
5: **if** $\mathcal{O} \not\supset \mathcal{O}_E$ **then**
6: **goto** step 4
7: **end if**
8: π_q の $\mathbb{Q}$ 係数多項式を要素とする $\mathcal{O}$ の $\mathbb{Z}$-basis $\mathbf{B}_{\mathcal{O}}$ を計算する
9: **for all** $\omega \in \mathcal{O}$ **do**
10: **if** $\omega \notin \mathrm{End}(\mathcal{J}_C)$ **then**
11: **goto** step 4
12: **end if**
13: **end for**
14: $\mathcal{O}_E \leftarrow \mathcal{O}$
15: **end for**
16: **return** $\mathcal{O}_E$

4.2 χ_q の計算

有限体 $\mathbb{F}_q$ 上定義された超楕円曲線 C の Jacobi 多様体 $\mathcal{J}_C$ の q 乗 Frobenius 写像 π_q の特性多項式に対し，

$$\chi_q(X) \in \mathbb{Z}[X] \tag{22}$$

が成り立つ．

C の zeta 関数 $Z(X, C)$ は

$$\frac{d}{dX} \log Z(X, C) = \sum_{i=1}^{\infty} N_i X^{i-1} \tag{23}$$

で定義される．ここで N_i は C の $\mathbb{F}_{q^i}$-有理点数を表す．$Z(X, C)$ と $\chi_q(X)$ の間に

$$Z(X, C) = \frac{X^{2g} \chi_q(\frac{1}{X})}{(1 - X)(1 - qX)} \tag{24}$$

が成立することが知られている．これらから

$$N_i = q^i + 1 - \sum_{j=1}^{2g} \pi_q^{i\varphi_j} \tag{25}$$

が成立する．ここで $\pi_q^{i\varphi_j}, j = 1 \ldots 2g$ は π_q^i の $2g$ 個の共役を表す．

したがって χ_q は C の $\mathbb{F}_{q^i}$-有理点数を $i = 1 \ldots g$ に対して数え上げることで得られる．

以上より Algorithm 2 を得る．

Algorithm 2 $\mathcal{J}_C/\mathbb{F}_q$ の q 乗 Frobenius 写像の特性多項式

Input: 種数 g の超楕円曲線 $C/\mathbb{F}_q$
Output: $\mathcal{J}_C$ の q 乗 Frobenius 写像 π_q の特性多項式 $\chi_q(X)$
1: **for** i=1 ... g **do**
2: $N_i \leftarrow \#C(\mathbb{F}_{q^i})$
3: **end for**
4: 等式

$$\sum_{j=1}^{2g} \pi_q^{i\varphi_j} = N_i - q^i - 1$$

から Newton 公式を用いて，$\pi_q^{\varphi_j}$ の基本対称式 $s_i = \binom{i}{2g}$ $\sum \prod^{i} \pi_q^{\varphi_j}$ を計算する．
5: $\chi_q \leftarrow X^{2g} - s_1 X^{2g-1} + s_2 X^{2g-2} - \cdots - s_1 q^{g-1} X + q^g$
6: **return** χ_q

Algorithm 2 において，step 2 が計算量の dominant part である．step 2 では任意の $a \in \mathbb{F}_{q^g}$ に対し $a^{(q^g-1)/2}$ を計算する必要がある．したがって Algorithm 2 の計算量は

$$O(g^3 q^g (\log q)^3) \tag{26}$$

である．

Algorithm 2 とは別に，小種数の超楕円曲線に対し $\chi_q(X)$ をより効率的に計算するアルゴリズムが Elkies によって提案されている [30]．Elkies のアルゴリズムの計算量は

$$O\left(g^2 q^{\lfloor 8g/5 \rfloor/4} (\log q)^2\right) \tag{27}$$

である．提案アルゴリズムにおいても，Algorithm 2 の代わりに Elkies のアルゴリズムを用いることで，実際の計算速度を高速化可能である．しかし Algorithm 2 を用いた場合と Elkies のアルゴリズムを用いた場合で，提案アルゴリズムの計算量は変わらない．そこで以降の計算量評価は Algorithm 2 を用いたとして行う．

次に **4. 4** に示される Algorithm 6 に必要な $\mathcal{J}_C/\mathbb{F}_q$ の q^n 乗 Frobenius 写像 π_{q^n} の特性多項式 χ_{q^n} の計算について検討する．

χ_{q^n} は Algorithm 2 を $\mathbb{F}_{q^n}$ 上で用いることで直接計算することが可能であるが，多くの場合により高速なアルゴリズムが線形代数の知識から導かれる．

Algorithm 3 に χ_{q^n} の計算アルゴリズムを示す．

Algorithm 3 中 step 4 の $R_{i,j}$ は多項式 R_i の j 次の係数を表し，step 5 の $\mathbf{I}_{2g}$ は $2g \times 2g$ 単位行列を表す．

Algorithm 3 $\mathcal{J}_C/\mathbb{F}_q$ の q^n 乗 Frobenius 写像の特性多項式

Input: $\mathcal{J}_C$ の q 乗 Frobenius 写像 π_q の特性多項式 $\chi_q(X)$
Output: $\mathcal{J}_C$ の q^n 乗 Frobenius 写像 π_{q^n} の特性多項式 $\chi_{q^n}(X) \in \mathbb{Z}[X]$
1: **for** $i = 1 \ldots 2g$ **do**
2: $R_i(X) \leftarrow X^{n+i} \bmod \chi_q(X)$
3: **end for**
4:

$$\mathbf{A} \leftarrow \begin{pmatrix} R_{1,0} & R_{1,1} & \cdots & R_{1,2g-1} \\ R_{2,0} & R_{2,1} & \cdots & R_{2,2g-1} \\ \vdots & \vdots & \ddots & \vdots \\ R_{2g,0} & R_{2g,1} & \cdots & R_{2g,2g-1} \end{pmatrix}$$

5: $\chi_{q^n} \leftarrow |X\mathbf{I}_{2g} - \mathbf{A}|$
6: **return** χ_{q^n}

Algorithm 3 の計算量の g, n に対する dominant part は step 5 である．π_q に関し，

$$|\pi_q| = \sqrt{q} \tag{28}$$

が成り立つことが知られている．そこで

$$\chi_{q^n}(X) = X^{2g} - s_1 X^{2g-1} + s_2 X^{2g-2} - \cdots - s_1 q^{(g-1)n} X + q^{gn} \tag{29}$$

と書くと，$s_i \in \mathbb{Z}, i = 1 \ldots g$ であり，式 (28) から

$$|s_i| \leq \binom{2g}{i} q^{\frac{gi}{2}} < 2^{2g} q^{\frac{gn}{2}} \tag{30}$$

を得る．このバウンドにより，中国人剰余定理と Hessenberg の方法 [28] を用いて step 5 は，

$$O((2g)^3 (\log(2^{2g}\sqrt{q^{gn}}))^3) = O(g^6 n^3 (\log q)^3) \tag{31}$$

で計算可能である．以上より，式 (31) が Algorithm 3 の計算量を与える．

4. 3 $\mathcal{O}$ の計算

本節では，Algorithm 1 に必要な $\mathcal{O}_0 \subset \mathcal{O} \subseteq \mathcal{O}_K$ なる任意の $\mathcal{O}$ の $\mathbb{Z}$-basis の計算アルゴリズムを与える．

まず始めに $\mathbb{Z}[\pi_q] \subset \mathcal{O} \subseteq \mathcal{O}_K$ なる任意の $\mathcal{O}$ の $\mathbb{Z}$-basis の計算について検討する．

式 (8) で与えられる $\mathbf{B}_K$ と式 (10) で与えられる $\mathbf{B}_{\mathbb{Z}[\pi_q]}$ を用いて $\mathcal{O}$ の $\mathbb{Z}$-basis が以下の補題で与えられる．

補題 4. $\mathbb{Z}[\pi_q] \subseteq \mathcal{O}$ とする．$\mathbf{B}_{\mathbb{Z}[\pi_q]}$ に対して $\mathbf{B}_{\mathbb{Z}[\pi_q]} = \mathbf{B}_{\mathcal{O}}\mathbf{A}$ となる $\mathcal{O}$ の $\mathbb{Z}$-basis $\mathbf{B}_{\mathcal{O}}$ が存在する．ここで $\mathbf{A} = (a_{ij}) \in \mathbb{Z}^{2g\times 2g}$ は上三角行列で対角要素 a_{ii} は $a_{ii}|d_i$ を満足する．また要素 $a_{ij}(i < j)$ は $0 \le a_{ij} < a_{ii}$ を満足する．

証明. [27, 3 Lemma(2.9)(ii)] とその証明から上三角行列 $\mathbf{A} \in \mathbb{Z}^{2g\times 2g}$ が存在し要素 $a_{ij}(i < j)$ を $0 \le a_{ij} < a_{ii}$ とできる．また $\det \mathbf{A} \neq 0$ である．$\mathcal{O} \subseteq \mathcal{O}_K$ より $\mathbf{B}_{\mathcal{O}} = \mathbf{B}_K\mathbf{A}_1$ となる $\mathbf{A}_1 = (b_{ij}) \in \mathbb{Z}^{2g\times 2g}$ が存在する．また $\mathbf{B}_{\mathbb{Z}[\pi_q]} = \mathbf{B}_K\mathbf{A}_2$ とすれば，$\mathbf{A}_2 = (c_{ij}) \in \mathbb{Z}^{2g\times 2g}$ は対角要素 $c_{ii} = d_i$ の対角行列である．ここで $\mathbf{A}^{-1} \in \mathbb{Q}^{2g\times 2g}$ を用いて $\mathbf{A}_1 = \mathbf{A}_2\mathbf{A}^{-1}$ と書けるので，$\mathbf{A}_1$ は上三角行列である．また $\mathbf{A}_2 = \mathbf{A}_1\mathbf{A}$ であるので，$\mathbf{A}_1\mathbf{A}$ の対角要素 $a_{ii}b_{ii} = d_i$ である．ゆえに $a_{ii}|d_i$． □

補題 4 を満足する $\mathcal{O}$ が $\mathcal{O} \subseteq \mathcal{O}_K$ となるのは，

$$\mathbf{B}_{\mathcal{O}} = \mathbf{B}_K\bar{\mathbf{A}} \tag{32}$$

なる行列 $\bar{\mathbf{A}}$ が

$$\bar{\mathbf{A}} \in \mathbb{Z}^{2g\times 2g} \tag{33}$$

となるときである．

ここで行列 $\mathbf{A}_{\mathbb{Z}[\pi_q]} \in \mathbb{Z}^{2g\times 2g}, \mathbf{A}_K, \mathbf{A}_O \in \mathbb{Q}^{2g\times 2g}$ と $\mathbb{Q}(\pi_q)$ の標準基底 $\mathbf{B}_{\pi_q}$ を用いて各基底を

$$\mathbf{B}_{\mathbb{Z}[\pi_q]} = \mathbf{B}_{\pi_q}\mathbf{A}_{\mathbb{Z}[\pi_q]} \tag{34}$$

$$\mathbf{B}_K = \mathbf{B}_{\pi_q}\mathbf{A}_K \tag{35}$$

$$\mathbf{B}_{\mathcal{O}} = \mathbf{B}_{\pi_q}\mathbf{A}_{\mathcal{O}} \tag{36}$$

と行列表現すれば，補題 4 と式 (32) の条件は

$$\mathbf{A}_{\mathbb{Z}[\pi_q]} = \mathbf{A}_{\mathcal{O}}\mathbf{A} \tag{37}$$

$$\mathbf{A}_{\mathcal{O}} = \mathbf{A}_K\bar{\mathbf{A}} \tag{38}$$

と書ける．したがって補題 4 の条件を満足する $\mathbf{A}$ に対して

$$\bar{\mathbf{A}} = \mathbf{A}_K^{-1}\mathbf{A}_{\mathbb{Z}[\pi_q]}\mathbf{A}^{-1} \in \mathbb{Q}^{2g\times 2g} \tag{39}$$

が $\mathbb{Z}$ 係数行列であれば，対応する $\mathcal{O}$ は $\mathbb{Z}[\pi_q] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$ を満足する．

以上の議論より $\mathbb{Z}[\pi_q] \subset \mathcal{O} \subseteq \mathcal{O}_K$ なるすべての $\mathcal{O}$ の $\mathbb{Z}$-basisを計算可能である．これらの $\mathcal{O}$ が $\mathcal{O} \supseteq \mathcal{O}_0$ を満足するのは，対応する A の $2g$ 行 $2g$ 列要素 $a_{2g,2g}$ が $q^{g-1} \mid a_{2g,2g}$ を満足するときに限る．

Algorithm 4 $\mathcal{O}_0 \subset \mathcal{O} \subseteq \mathcal{O}_K$

Input: π_q の特性多項式 $\chi_q(X)$
Output: $\mathbb{Z}[\pi_q] \subset \mathcal{O} \subseteq \mathcal{O}_K$ である CM 体 K の order $\mathcal{O}$ の $\mathbb{Z}$-basis の集合 $T = \{\mathbf{B}_{\mathcal{O}}\}$
1: 式 (8) の $\mathbf{B}_K$ を計算する
2: 式 (9)，式 (10) の $\mathbf{B}_{\pi_q}, \mathbf{B}_{\mathbb{Z}[\pi_q]}$ を計算する
3: $T \leftarrow \{\mathbf{B}_K\}$
4: 式 (34)，式 (35) の $\mathbf{A}_{\mathbb{Z}[\pi_q]}, \mathbf{A}_K$ を計算する
5: **for all** $\mathbf{A} = (a_{ij}) \in \mathbb{Z}^{2g\times 2g}$ s.t. $a_{ii}|d_i$，$q^{g-1} \mid a_{2g,2g}$，$0 \le a_{ij} < a_{ii}$ for $j > i$，$a_{ij} = 0$ for $j < i$ **do**
6: $\quad\bar{\mathbf{A}} \leftarrow \mathbf{A}_K^{-1}\mathbf{A}_{\mathbb{Z}[\pi_q]}\mathbf{A}^{-1}$
7: $\quad$**if** $\bar{\mathbf{A}} \in \mathbb{Z}^{2g\times 2g}$ **then**
8: $\quad\quad T \leftarrow T \cup \{\mathbf{B}_{\pi_q}\mathbf{A}_K\bar{\mathbf{A}}\}$
9: $\quad$**end if**
10: **end for**
11: **return** T

Algorithm 4 に $\mathcal{O}_0 \subset \mathcal{O} \subseteq \mathcal{O}_K$ を満足するすべての $\mathcal{O}$ の $\mathbb{Z}$-basis を求めるアルゴリズムを示す．

次に Algorithm 4 の計算量を評価する．

まず step 5 の $\mathbf{A}$ の個数を評価する．式 (8) の d_i の積を

$$c = \prod_{i=1}^{2g} d_i \tag{40}$$

と書く．各 d_i は $d_i \le c^{1/(2g+1-i)}$ を満足する．要素 $a_{2g,2g}$ は $O(q^{1-g}d_{2g})$ 個の値をとり，$i < 2g, j \le i$ に対し a_{ij} は $O(d_i)$ 個の値をとる．また，各 i に対して $2g+1-i$ 個の a_{ij} が存在するので，$\mathbf{A}$ のとり得る個数 $\#\{\mathbf{A}\} = O(q^{1-g}c^{2g})$ を得る．

各 $\mathbf{A}$ に対して $\bar{\mathbf{A}}$ を計算する必要があるが，これは線形方程式系

$$\bar{\mathbf{A}}\mathbf{A} = \mathbf{A}_K^{-1}\mathbf{A}_{\mathbb{Z}[\pi_q]} \tag{41}$$

を解くことによって得られる．$\mathbf{A}_K^{-1}\mathbf{A}_{\mathbb{Z}[\pi_q]}$ が対角要素が d_i の対角行列であることと $\mathbf{A}$ が上三角行列であり $a_{ij} \le c^{1/(2g+1-i)}$ であることを考慮すると，$\bar{\mathbf{A}}$ は $O(g(\log c)^2)$ の計算量で計算可能である．したがって Algorithm 4 全体の計算量は

$$O(gq^{1-g}c^{2g}(\log c)^2) \tag{42}$$

である．

$\chi_q(X)$ の discriminant の絶対値は $\chi_q(X)$ の各根の絶対値が $\sqrt{q}$ であることから

$$|\mathrm{disc}\,(\chi_q)| \le (4q)^{g(2g-1)} \tag{43}$$

を満足する．また $c \leq \sqrt{|\mathrm{disc}\,(\chi_q)|}$ である．

以上より Algorithm 4 の計算量は

$$O(2^{2g^2(2g-1)} g^5 q^{2g^3-g^2-g+1} (\log q)^2) \tag{44}$$

である．

4.4 $\omega \in \mathcal{O}$ に対する $\omega \in \mathrm{End}(\mathcal{J}_C)$ のテスト

本節では Algorithm 1 の step 10 の $\omega \in \mathcal{O} \subseteq \mathcal{O}_K$ に対する $\omega \in \mathrm{End}(\mathcal{J}_C)$ のテストについて論ずる．

4.3 の結果から $\mathcal{O} \supset \mathbb{Z}[\pi_q]$ の基底の各要素は $\mathcal{J}_C$ の q 乗 Frobenius 写像 π_q の有理数係数多項式として与えられる．よって $\omega \in \mathcal{O}$ もまた π_q を用いて

$$\omega = f(\pi_q)/d, d \in \mathbb{Z}, f(X) \in \mathbb{Z}[X] \tag{45}$$

と書ける．以下では ω は f, d とともに式 (45) で与えられているとする．

ここで以下に示す補題 5 が成り立つ．

補題 5. $\omega = f(\pi_q)/d \in \mathcal{O}$，$f(X) \in \mathbb{Z}[X], d \in \mathbb{Z}$ とする．このとき

$$\omega \in \mathrm{End}(\mathcal{J}_C) \Leftrightarrow \mathcal{J}_C[d] \subseteq \ker f(\pi_q) \tag{46}$$

が成立する．

証明． $\omega \in End(\mathcal{J}_C)$ とする．任意の $\mathcal{D} \in \mathcal{J}_C[d]$ に対して $d\mathcal{D} = 0$ より $\omega d\mathcal{D} = 0$ であり，したがって $f(\pi_q)\mathcal{D} = 0$ を得る．

次に，$\mathcal{J}_C[d] \subseteq \ker f(\pi_q)$ とし，

$$\sigma_1 : d\mathcal{J}_C \xrightarrow{\sim} \mathcal{J}_C/\mathcal{J}_C[d] \tag{47}$$

$$\sigma_2 : \mathcal{J}_C/\mathcal{J}_C[d] \xrightarrow{Can.} \mathcal{J}_C/\ker f(\pi_q) \tag{48}$$

$$\sigma_3 : \mathcal{J}_C/\ker f(\pi_q) \xrightarrow{\sim} f(\pi_q)\mathcal{J}_C \tag{49}$$

とする．ここで，σ_1 は $d\mathcal{J}_C = \mathcal{J}_C$ から $\mathcal{J}_C/\mathcal{J}_C[d]$ への同型写像，σ_2 は $\mathcal{J}_C/\mathcal{J}_C[d]$ から $\mathcal{J}_C/\ker f(\pi_q)$ への標準的全射準同型写像，σ_3 は $\mathcal{J}_C/\ker f(\pi_q)$ から $f(\pi_q)\mathcal{J}_C = \mathcal{J}_C$ への同型写像であり，仮定より σ_2 が存在する．これら σ_i を用いて，準同型写像

$$\omega : \mathcal{J}_C \longrightarrow \mathcal{J}_C \tag{50}$$

$$\mathcal{D} \longmapsto \sigma_3(\sigma_2(\sigma_1(\mathcal{D}))) \tag{51}$$

が定義可能であり，任意の $\mathcal{D} \in \mathcal{J}_C$ に対し，

$$d\omega(\mathcal{D}) = \omega(d\mathcal{D}) = f(\pi_q)\mathcal{D} \tag{52}$$

が成立する．よって，$\omega = f(\pi_q)/d$ である． □

補題 5 により $\omega \in \mathrm{End}(\mathcal{J}_C)$ のテストは，実際の divisor 演算によって行えることとなる．すなわち，任意の $\mathcal{D} \in \mathcal{J}_C[d]$ に対し

$$f(\pi_q)\mathcal{D} = 0 \tag{53}$$

が成立すれば，$\omega \in \mathrm{End}(\mathcal{J}_C)$ である．

また明らかに以下の補題が成り立つ．

補題 6. l_i を d の素因数 s_i を d の l_i べき part とする．すなわち

$$d = \prod_i s_i,\ s_i = l_i^{e_i} \tag{54}$$

とする．このとき

$$^{\forall} s_i, \mathcal{J}_C[s_i] \subseteq \ker f(\pi_q) \Leftrightarrow \mathcal{J}_C[d] \subseteq \ker f(\pi_q) \tag{55}$$

が成立する．

補題 7. $d \in \mathbb{Z}$ とする．

$$G = (\mathcal{D}_1 \quad \mathcal{D}_2 \quad \cdots \quad \mathcal{D}_{2g}) \tag{56}$$

を $\mathcal{J}_C[d]$ の生成系，すなわち

$$\mathcal{J}_C[d] = \mathbb{Z}\mathcal{D}_1 + \mathbb{Z}\mathcal{D}_2 + \cdots + \mathbb{Z}\mathcal{D}_{2g} \tag{57}$$

であるような *divisor* の集合とする．このとき，

$$^{\forall}\mathcal{D} \in \mathcal{J}_C[d], f(\pi_q)\mathcal{D} = 0 \Leftrightarrow {}^{\forall}\mathcal{D} \in G, f(\pi_q)\mathcal{D} = 0 \tag{58}$$

が成立する．

補題 5，6，7 から d の各素数べき part s に対し，$\mathcal{J}_C[s]$ の生成系 G の divisor $\mathcal{D} \in G$ が式 (53) を満足することを確認することで $\omega \in End(\mathcal{J}_C)$ のテストが可能となる．

Algorithm 5 に $\omega \in \mathcal{O}$ に対する $\omega \in \mathrm{End}(\mathcal{J}_C)$ のテストアルゴリズムを示す．

Algorithm 5 には素数べき $s = l^e$ に対する $\mathcal{J}_C[s]$ の生成系 G が必要である．G の計算には Cantor [31] の division polynomial を利用可能であるが，これには多変数多項式の計算が必要であり，実用的な構成は困難である．そこで，ここではより実用的かつ効果的な方法を提案する．

今，$\mathcal{J}_C$ の q 乗 Frobenius 写像の特性多項式 $\chi_q(X)$

Algorithm 5 $\omega \in \mathcal{O}$ に対する $\omega \in \mathrm{End}(\mathcal{J}_C)$ のテスト

Input: ordinary 超楕円曲線 $C/\mathbb{F}_q$，$\mathcal{J}_C$ の q 乗 Frobenius 写像 π_q の特性多項式 $\chi_q(X)$，$\omega = f(\pi_q)/d$ ただし $d \in \mathbb{Z}, f(X) \in \mathbb{Z}[X]$
Output: $\omega \in \mathrm{End}(\mathcal{J}_C)$ のとき *true*，そうでないとき *false*

d に対し素因数分解

$$d = \prod l_i^{e_i} \tag{59}$$

を行い素数 l_i べき part $s_i = l_i^{e_i}$ を計算する
for all s_i **do**
  $\mathcal{J}_C[s_i]$ の生成系 G を計算する
  for all $\mathcal{D} \in G$ **do**
    if $f(\pi_q)\mathcal{D} \neq 0$ **then**
      return *false*
    end if
  end for
end for
return *true*

が既知であるので，π_q^n の特性多項式 $\chi_{q^n}(X)$ を Algorithm 3 により計算可能である．したがって $\#\mathcal{J}_C(\mathbb{F}_{q^n}) = \chi_{q^n}(1)$ を用いて $s \mid \#\mathcal{J}_C(\mathbb{F}_{q^n})$ を調べることで，$\mathcal{J}_C[s](\mathbb{F}_{q^n}) \neq \phi$ がテスト可能である．ここで $\mathcal{J}_C[s](\mathbb{F}_{q^n}) \neq \phi$ となる $\mathbb{F}_{q^n}$ 上で $l^{e_0} \parallel \#\mathcal{J}_C(\mathbb{F}_{q^n})$ である e_0 により $s_0 = l^{e_0}$ とすれば，$\mathcal{D} \in \mathcal{J}_C(\mathbb{F}_{q^n})$ に対し

$$\tilde{\mathcal{D}} = \frac{\#\mathcal{J}_C(\mathbb{F}_{q^n})}{s_0}\mathcal{D} \in \mathcal{J}_C[s_0] \tag{60}$$

となり，ランダムに選択した $\mathcal{D}$ に対し，$\tilde{\mathcal{D}}$ は $\mathcal{J}_C[s_0](\mathbb{F}_{q^n})$ のランダムな divisor となる．そこでこの $\tilde{\mathcal{D}}$ を用いて Baby step giant step algorithm [28], [32], [33] により $\mathcal{J}_C[s_0](\mathbb{F}_{q^n})$ の生成系 G_0 と群構造を得ることが可能である．

ここで

$$G_0 = (\bar{\mathcal{D}}_1 \quad \bar{\mathcal{D}}_2 \quad \cdots \quad \bar{\mathcal{D}}_{2g}) \tag{61}$$

とし，$\#\langle\bar{\mathcal{D}}_i\rangle = l^{\tilde{e}_i}$ を満足する整数を $\bar{e}_i$ とおく．$\hat{e}_i = \max\{0, \bar{e}_i - e\}$ とすると，

$$G = (l^{\hat{e}_1}\bar{\mathcal{D}}_1 \quad l^{\hat{e}_2}\bar{\mathcal{D}}_2 \quad \cdots \quad l^{\hat{e}_{2g}}\bar{\mathcal{D}}_{2g}) \tag{62}$$

は $\mathcal{J}_C[s](\mathbb{F}_{q^n})$ の生成系となる．

以上の議論より素数べき s に対する $\mathcal{J}_C[s]$ の生成系 G の計算アルゴリズム Algorithm 6 を得る．

次に Algorithm 6 の計算量を評価する．

Algorithm 6 中 step 3 に現れる Algorithm 3 の計算量は式 (31) より n に対し $O(g^6 n^3 (\log q)^3)$ である．$\gcd(q, s) = 1$ のとき $n = 1 \ldots O(s^{2g})$ に対し χ_{q^n} を計算する必要があるので，$\#\mathcal{J}_C(\mathbb{F}_{q^n})$ の計算に Algorithm 6 全体で

$$O(g^6 s^{8g} (\log q)^3) \tag{63}$$

の計算量が必要である．一方，$\gcd(q, s) \neq 1$ のときは $n = 1 \ldots O(s^g)$ に対し χ_{q^n} を計算すればよいので，

$$O(g^6 s^{4g} (\log q)^3) \tag{64}$$

で計算可能である．

次に n 次拡大での G_0 の計算量を検討する．

式 (3) より

$$\#\mathcal{J}_C(\mathbb{F}_{q^n}) = O(q^{gn}) \tag{65}$$

であるので Baby step giant step algorithm に必要な $\tilde{\mathcal{D}} \in \mathcal{J}_C[l^{e_0}](\mathbb{F}_{q^n})$ を得るために $O(gn \log q)$ 回の divisor の加算が必要であり，この $\mathcal{D}$ が $O(g)$ 個必要なので，十分な個数の $\tilde{\mathcal{D}}$ を得るために

$$O(g^4 (n \log q)^3) \tag{66}$$

の計算量が必要である．

Baby step giant step algorithm に必要な $O(\sqrt{l^{e_0}})$ 回の divisor の加算の計算量は

$$O(\sqrt{l^{e_0}} (gn \log q)^2) \tag{67}$$

Algorithm 6 素数べき s に対する $\mathcal{J}_C[s]$ の生成系 G

Input: ordinary 超楕円曲線 $C/\mathbb{F}_q$，$\mathcal{J}_C$ の q 乗 Frobenius 写像 π_q の特性多項式 $\chi_q(X)$，素数べき $s = l^e \in \mathbb{Z}$
Output: $G = \{\mathcal{D}_i \mid \mathcal{J}_C[s] = \sum_{i=1}^{2g} \mathbb{Z}\mathcal{D}_i\}$

1: $n \leftarrow 1, e_1 \leftarrow 0$
2: **loop**
3: Algorithm 3 を用いて $\#\mathcal{J}_C(\mathbb{F}_{q^n})$ を計算する
4: **if** $s \mid \#\mathcal{J}_C(\mathbb{F}_{q^n})$ **then**
5: $l^{e_0} \parallel \#\mathcal{J}_C(\mathbb{F}_{q^n})$ を満足する $e_0 \in \mathbb{Z}$ を計算する
6: **if** $e_0 > e_1$ **then**
7: $e_1 \leftarrow e_0$
8: $\mathcal{J}_C[l^{e_0}](\mathbb{F}_{q^n})$ の生成系 G_0 と群構造を Baby step giant step algorithm により計算する
9: G_0 から式 (62) により $\mathcal{J}_C[s](\mathbb{F}_{q^n})$ の生成系 G を計算する
10: **if** $\gcd(q, s) = 1$ and $\#G = 2g$ **then**
11: **return** G
12: **else if** $\gcd(q, s) \neq 1$ and $\#G = g$ **then**
13: **return** G
14: **end if**
15: **end if**
16: **end if**
17: $n \leftarrow n + 1$
18: **end loop**

である．$e_0 = O(g \log_l n)$ であるので Baby step giant step algorithm に必要な計算量は

$$O(g^2 l^g n^{5/2} (\log q)^2) \tag{68}$$

である．

ここで $\gcd(q,s) = 1$ のとき $1 \le n < O(s^{2g})$ に対して G_0 を計算する必要があるが，n は $O(\sqrt[g]{l})$ 倍ごとに step 6 の条件を満足すると考えられる．したがって Algorithm 6 全体で，G_0 の計算は $\tilde{\mathcal{D}} \in \mathcal{J}_C[l^{e_0}](\mathbb{F}_{q^n})$ の計算に

$$O(g^4 s^{6g} (\log q)^3) \tag{69}$$

Baby step giant step algorithm に

$$O(g^2 l^g s^{5g} (\log q)^2) \tag{70}$$

の計算量が必要であり，$l \le s$ より，全体では

$$O(g^4 s^{6g} (\log q)^3) \tag{71}$$

の計算量が必要である．

同様にして $\gcd(q,s) \neq 1$ のとき $1 \le n < O(s^g)$ に対して G_0 を計算する必要があり，全体の計算量は

$$O(g^4 s^{3g} (\log q)^3) \tag{72}$$

となる．

以上より Algorithm 6 の計算量は $\gcd(q,s) = 1$ のとき

$$O(g^6 s^{8g} (\log q)^3) \tag{73}$$

$\gcd(q,s) \neq 1$ のとき

$$O(g^6 s^{4g} (\log q)^3) \tag{74}$$

である．

次に Algorithm 5 の計算量を評価する．

Algorithm 5 では step 3 で $\mathcal{D} \in G$ に対し $f(\pi_q)\mathcal{D}$ を計算する．ここで $\pi_q^i D, i = 1 \ldots 2g$ の計算量は各 s_i に対し $\gcd(q,s) = 1$ のとき

$$O(g^2 s_i^{4g} (\log q)^3) \tag{75}$$

$\gcd(q,s) \neq 1$ のとき

$$O(g^2 s_i^{2g} (\log q)^3) \tag{76}$$

である．これら $\pi_q^i \mathcal{D}, i = 1 \ldots 2g$ に対し s_i 以下の整数による整数倍が必要であるが，これに必要な計算量は $\gcd(q,s) = 1$ のとき

$$O(g^3 s_i^{4g} (\log q)^2 \log s_i) \tag{77}$$

$\gcd(q,s) \neq 1$ のとき

$$O(g^3 s_i^{2g} (\log q)^2 \log s_i) \tag{78}$$

である．更に $2g$ 個の $\mathcal{D}$ に対しこれらの計算を行うので $f(\pi_q)\mathcal{D}$ の計算量は s_i に対し $\gcd(q,s) = 1$ のとき

$$O(g^3 s_i^{4g} (\log q)^2 (\log q + g \log s_i)) \tag{79}$$

$\gcd(q,s) \neq 1$ のとき

$$O(g^3 s_i^{2g} (\log q)^2 (\log q + g \log s_i)) \tag{80}$$

となる．これらと $s = s_i$ としたときの式 (73) と式 (74) を比較することで Algorithm 5 の計算量の dominant part が Algorithm 6 であることがわかる．

したがって Algorithm 5 の計算量は d の l_i べき part s_i を用いて $\gcd(q,s) = 1$ のとき

$$O(g^6 (\log q)^3 \sum_i s_i^{8g}) \tag{81}$$

$\gcd(q,s) \neq 1$ のとき

$$O(g^6 (\log q)^3 s_i^{4g}) \tag{82}$$

である．

5. 計算量評価

本章では，Algorithm 1 で提案した Jacobi 多様体の自己準同型環計算アルゴリズムの計算量を評価する．

前章で見たように Algorithm 5 の計算量の dominant part は Algorithm 6 であった．

Algorithm 6 が Algorithm 1 中で必要な素数べき torsion に対し一度実行すれば良いものであることを考慮すると，Algorithm 1 全体で Algorithm 6 の計算量が最悪値をとるのは式 (40) で定義した c を用いて

$$\begin{aligned} &d_1 = d_2 = \cdots = d_{2g-1} = 1, \\ &d_{2g} = c = O((4q)^{\frac{g(2g-1)}{2}}) \end{aligned} \tag{83}$$

のときである．そこでこの case について Algorithm 6

の計算量を見積もる．

$\mathcal{J}_C$ の q 乗 Frobenius 写像 π_q の特性多項式 $\chi_q(X)$ の discriminant は $q^{g(g-1)}$ を因数としてもつ．すなわち $\mathrm{disc}\,(\chi_q) = q^{g(g-1)}d'$ と表せる．したがって考察中の case においては

$$d_{2g} = O\left(\sqrt{|\mathrm{disc}\,(\chi_q)|}\right) = O\left(\sqrt{q^{g(g-1)}|d'|}\right) \tag{84}$$

である．

式 (81) と式 (82) の比較により，Algorithm 6 では q べき part に対する計算量がそれ以外の場合の計算量より小さくなることがわかる．これと式 (81) から計算量が最悪値をとるのは $q = p^n$ としたとき d_{2g} の p べき part の指数が $g(g-1)n/2$ でそれ以外の part，すなわち $O(\sqrt{|d'|})$ の part が素数べきの場合である．このときそれぞれの part の s は，$\gcd(q,s) = 1$ に対し

$$s = O(2^{g(2g-1)}q^{g^2/2}) \tag{85}$$

$\gcd(q,s) \neq 1$ に対しては，補題 3 を考慮して

$$s = O(q^{(g-1)(g-2)/2}) \tag{86}$$

である．これらを式 (73)，式 (74) と比較することで $\gcd(q,s) = 1$ の場合が dominant であることがわかり，この計算量は

$$O(2^{8g^2(2g-1)}g^6q^{4g^3}(\log q)^3) \tag{87}$$

となる．これと式 (44) との比較により式 (87) が Algorithm 1 の計算量を与える．

6. 実装実験と平均計算量の検討

前章の結果から提案アルゴリズムは q の多項式時間オーダアルゴリズムではあるものの，定数項，指数ともに大きく実際的なアルゴリズムではないように見える．しかし，前章の計算量評価は最悪の場合を想定したもので，現実的な曲線に対する計算の振舞いを表していると必ずしも言えるものではない．

そこで本章では，種数 2 の超楕円曲線に対し提案アルゴリズムの実装実験を行い，アルゴリズムの現実的な有効性を確認する．また，実験結果をもとに種数 2 の曲線に対する提案アルゴリズムの平均計算量を検討する．更に，実験中に得られた計算例を示す．

実装には Magma [34] を用いた．実装の際，χ_q の計算には Elkies のアルゴリズム [30] を，Algorithm 6 step 8 には [28, Algorithm 5.4.1] の Baby step giant step algorithm を適用した．また，実際的な計算効率化手法として，Algorithm 6 の step 10 で $\#G < 4$ の場合にも Algorithm 5 に G を返し，G の元に対し Algorithm 5，step 5 のテストを行った．

6.1 実　　験

実験環境として Pentium III 866 MHz，memory 500 MByte を使用し，

$$p \in \{7, 17, 31, 61, 127, 251, 509, 1031\}$$

に対応する $\mathbb{F}_p$ 上で，ランダムな種数 2 の超楕円曲線各 100 本に対し，提案アルゴリズムを用いて各曲線の Jacobi 多様体の自己準同型環の決定を行った．その際，計算時間，memory 使用量と，計算の難易度を示す指標として式 (40) で定義した c，Algorithm 6 に現れる n の最大値 N を測定した．

表 1 に各測定値の平均値と最大値を示す．表 1 中「$\#\{C^*\}$」の値は，memory 量が不十分で，今回の実験環境では計算を完了できなかった曲線の本数を示す．表 1 の各測定値はこれらの曲線を除いたものである．例えば，$p = 1031$ に対する測定値は 99 本の曲線についての値を示している．表 2 に今回の実験で自己準同型環を決定できなかった曲線とその c の値及び計算経過から推定した N の最悪値を示す．

実験結果から，位数が 1000 程度の有限体上の種数 2 の超楕円曲線の Jacobi 多様体の自己準同型環の多くは，現実的な環境下で十分な速度で計算可能であると結論付けられる．

6.2 平均計算量の見積り

本節では，実験結果をもとに提案アルゴリズムの平均計算量について考察する．

実験結果から，実際の計算時間が個々の曲線固有の性質に大きく依存し，平均計算量の正確な見積りが困難であることがわかる．しかし，表 1 と表 2 から c の平均値を $O(p^2)$，N の平均値を $O(p)$ とすることは妥当である．そこで，

$$c = O(q^2) \tag{88}$$

$$N = O(q) \tag{89}$$

として平均計算量を見積もる．

まず，式 (42) に $g = 2$ と式 (88) を代入し，Algorithm 4 の平均計算量

表 1　自己準同型環の計算
Table 1　Experimental results of computing endomorphism rings of hyperelliptic curves over $\mathbb{F}_p$.

p	$\#\{C^*\}$	計算時間（秒）		Memory 使用量 (MByte)		c		N	
		平均	最大	平均	最大	平均	最大	平均	最大
7	0	0.1	0.5	0.03	0.5	30.7	448	2.2	9
17	0	127	11673	3.2	280	265	4896	6.4	156
31	0	9.8	476	0.6	26	978	22599	6.8	110
61	0	4.6	233	0.4	4.8	1166	19520	5.6	78
127	1	962	86177	0.9	47	4614	92583	14.4	602
251	1	371	14005	6.9	278	14104	208832	11.0	156
509	3	131	9005	1.0	53	207320	16288000	12.3	253
1031	1	84	8052	0.8	36	232329	14846400	6.5	168

表 2　自己準同型環の計算を完了できなかった曲線（C^* と記す）
Table 2　List of curves that endomorphism rings of their Jacobian varieties could not be determined in the experiment (Denote as C^*).

p	C^*	c	N
127	$Y^2 = X^5 + 98X^4 + 75X^3 + 97X^2 + 32X + 25$	26289	506
251	$Y^2 = X^5 + 111X^4 + 105X^3 + 58X^2 + 99X + 146$	14809	3422
509	$Y^2 = X^5 + 478X^4 + 331X^3 + 220X^2 + 181X + 37$	11707	11638
	$Y^2 = X^5 + 505X^4 + 207X^3 + 10X^2 + 242X + 77$	105363	506
	$Y^2 = X^5 + 144X^4 + 55X^3 + 496X^2 + 147X + 129$	61589	7260
1031	$Y^2 = X^5 + 882X^4 + 650X^3 + 490X^2 + 707X + 307$	990791	153760

$$O(q^7(\log q)^2) \tag{90}$$

を得る．

次に式 (89) を考慮して Algorithm 5 の平均計算量を見積もる．

Algorithm 6 中 step 3 に現れる Algorithm 3 の平均計算量は式 (31) と $n = 1 \ldots N$ に対し χ_{q^n} を計算する必要から，

$$O(q^4(\log q)^3) \tag{91}$$

である．また，十分な個数の $\tilde{\mathcal{D}}$ を得るために，式 (66) より

$$O((q \log q)^3) \tag{92}$$

の平均計算量が必要である．更に，Baby step giant step algorithm の平均計算量は式 (68) において $l = q$ として，

$$O(q^{9/2}(\log q)^2) \tag{93}$$

である．

以上より，式 (90) が種数 2 の超楕円曲線に対する提案アルゴリズムの平均計算量を与える．

6.3 計　算　例

本節では，計算例として $p = 1031$ の実験で計算に最も時間を要した自己準同型環決定の過程を示す．

$\mathbb{F}_{1031}$ 上の種数 2 の超楕円曲線 C を下式で定義する．

$$C : Y^2 = X^5 + 860X^4 + 47X^3 + 685X^2 + 664X + 919 \tag{94}$$

C の Jacobi 多様体 $\mathcal{J}_C$ の p 乗 Frobenius 写像 π_p の特性多項式は，

$$\chi_p(X) = X^4 + 45X^3 + 1870X^2 + 46395X + 1062961 \tag{95}$$

と計算される．また，$\mathcal{J}_C$ の CM 体

$$K = \mathbb{Q}(\pi_p) \tag{96}$$

の maximal order $\mathcal{O}_K$ の $\mathbb{Z}$-basis が

$$\mathbf{B}_K = (\omega_1 \quad \omega_2 \quad \omega_3 \quad \omega_4), \tag{97}$$

$$\omega_1 = 1,$$

$$\omega_2 = \pi_q,$$

$$\omega_3 = \frac{\pi_q^2 + 5\pi_q + 2}{7},$$

$$\omega_4 = \frac{\pi_q^3 + 1076\pi_q^2 + 5994\pi_q + 7217}{2 \cdot 7 \cdot 1031}$$

と計算される．したがって，$\mathcal{O}_0$ の $\mathbb{Z}$-basis が

$$\mathbf{B}_0 = (\omega_1 \quad \omega_2 \quad 7\omega_3 \quad 14\omega_4) \tag{98}$$

で与えられる．

$\mathcal{O}_0 \subseteq \mathcal{O} \subseteq \mathcal{O}_K$ を満足する K の order $\mathcal{O}$ は 8 個存在する．これら $\mathcal{O}$ に対する $\mathcal{O} \subseteq \mathcal{O}_E$ のテストは

$$\mathcal{J}_C[2] \subseteq \ker f_1(\pi_p) \tag{99}$$
$$\mathcal{J}_C[7] \subseteq \ker f_2(\pi_p) \tag{100}$$
$$\mathcal{J}_C[7] \subseteq \ker f_3(\pi_p) \tag{101}$$

で十分である．ここで

$$f_1(X) = X^3 + 1 \tag{102}$$
$$f_2(X) = X^3 + 5X^2 + 2X \tag{103}$$
$$f_3(X) = X^2 + 5X + 2 \tag{104}$$

である．

まず，$\mathcal{J}_C[2]$ に対するテストを示す．

$\#\mathcal{J}_C(\mathbb{F}_{1031^n})$ を $n = 1, 2, \ldots$ に対して計算すると，$n = 1$ のとき

$$\#\mathcal{J}_C(\mathbb{F}_{1031}) = 2^3 \cdot 138909 \tag{105}$$

であり $\mathcal{J}_C[2] \cap \mathcal{J}_C(\mathbb{F}_{1031}) \neq \phi$ である．そこで $\mathcal{J}_C[2](\mathbb{F}_{1031})$ の群構造を計算し，

$$\mathcal{J}_C[2](\mathbb{F}_{1031}) \cong \mathbb{Z}/2\mathbb{Z} \tag{106}$$

を得る．この生成元 $\mathcal{D}$ に対し

$$f_1(\pi_p)\mathcal{D} = 0 \tag{107}$$

である．更に，続けて $\#\mathcal{J}_C(\mathbb{F}_{1031^n})$ を計算すると，$n = 2$ のとき

$$\#\mathcal{J}_C(\mathbb{F}_{1031^2}) = 2^6 \cdot 17682976791 \tag{108}$$

であり $\mathcal{J}_C[2] \cap \mathcal{J}_C(\mathbb{F}_{1031^2}) \neq \phi$ である．そこで $\mathcal{J}_C[2](\mathbb{F}_{1031^2})$ の群構造を計算し，

$$\mathcal{J}_C[2](\mathbb{F}_{1031^2}) \cong (\mathbb{Z}/2\mathbb{Z})^2 \tag{109}$$

を得る．この生成系に

$$f_1(\pi_p)\mathcal{D} \neq 0 \tag{110}$$

である $\mathcal{D}$ が存在する．したがって，$\mathcal{J}_C$ は式 (99) を満足せず，

$$\frac{f_1(\pi_q)}{2} \notin \mathrm{End}(\mathcal{J}_C) \tag{111}$$

である．

次に，$\mathcal{J}_C[7]$ に対するテストを示す．

$\#\mathcal{J}_C(\mathbb{F}_{1031^n})$ を計算すると，$n = 24$ のとき

$$\#\mathcal{J}_C(\mathbb{F}_{1031^{24}}) = 7^8 \cdot N_{24} \tag{112}$$

であり $\mathcal{J}_C[7] \cap \mathcal{J}_C(\mathbb{F}_{1031^{24}}) \neq \phi$ である．ここで，N_{24} は $7 \nmid N_{24}$ を満足する 470 bit の整数である．そこで $\mathcal{J}_C[7](\mathbb{F}_{1031^{24}})$ の群構造を計算し，

$$\mathcal{J}_C[7](\mathbb{F}_{1031^{24}}) \cong (\mathbb{Z}/7\mathbb{Z})^2 \tag{113}$$

を得る．ここで 2 個の生成元 $\mathcal{D}$ はともに

$$f_2(\pi_p)\mathcal{D} = 0 \tag{114}$$
$$f_3(\pi_p)\mathcal{D} = 0 \tag{115}$$

を満足する．更に，続けて $\#\mathcal{J}_C(\mathbb{F}_{1031^n})$ を計算すると，$n = 168$ のとき

$$\#\mathcal{J}_C(\mathbb{F}_{1031^{168}}) = 7^8 \cdot N_{168} \tag{116}$$

であり $\mathcal{J}_C[7] \cap \mathcal{J}_C(\mathbb{F}_{1031^{168}}) \neq \phi$ である．ここで，N_{168} は $7 \nmid N_{168}$ を満足する 3341 bit の整数である．そこで $\mathcal{J}_C[7](\mathbb{F}_{1031^{168}})$ の群構造を計算し，

$$\mathcal{J}_C[7](\mathbb{F}_{1031^{168}}) \cong (\mathbb{Z}/7\mathbb{Z})^4 \tag{117}$$

を得る．この生成系に

$$f_2(\pi_p)\mathcal{D}_1 \neq 0 \tag{118}$$
$$f_3(\pi_p)\mathcal{D}_2 \neq 0 \tag{119}$$

である $\mathcal{D}_1, \mathcal{D}_2$ が存在する．したがって，$\mathcal{J}_C$ は式 (100)，式 (101) を満足せず，

$$\frac{f_2(\pi_q)}{7} \notin \mathrm{End}(\mathcal{J}_C) \tag{120}$$
$$\frac{f_3(\pi_q)}{7} \notin \mathrm{End}(\mathcal{J}_C) \tag{121}$$

である．

以上より，

$$\mathrm{End}(\mathcal{J}_C) \cong \mathcal{O}_0 \tag{122}$$

を得る．

本計算例に要した計算時間を表 3 に示す．なお，本計算例は約 36 MByte の memory を必要とした．また，そのほとんどは $\mathcal{J}_C[7](\mathbb{F}_{1031^{168}})$ の群構造の計算に費された．

表 3　計算例に要した計算時間
Table 3　Timing of determining the endomorphism ring of the hyperelliptic curve (94).

	計算時間（秒）
χ_P	0.1
$\mathcal{O}$ s.t $\mathcal{O}_0 \subseteq \mathcal{O} \subseteq \mathcal{O}_K$	0.05
$\#\mathcal{J}_C(\mathbb{F}_{1031^n})$	4.0
$\mathcal{J}_C[2](\mathbb{F}_{1031})$ の群構造	0.01
$\mathcal{J}_C[2](\mathbb{F}_{1031^2})$ の群構造	0.04
$\mathcal{J}_C[7](\mathbb{F}_{1031^{24}})$ の群構造	7.0
$\mathcal{J}_C[7](\mathbb{F}_{1031^{168}})$ の群構造	8036.7
式 (99) のテスト	0.00
式 (100) のテスト	2.2
式 (101) のテスト	2.2
合計	8052

7. むすび

本論文では，lifting による CM 超楕円曲線の構成に必要となる，有限体上の ordinary 超楕円曲線の Jacobi 多様体の自己準同型環決定アルゴリズムを提案した．また，提案アルゴリズムの計算量を評価し，計算量を式 (87) に得た．しかし，提案アルゴリズムの計算量の指数部は大きく，現実的な計算環境のもと，提案アルゴリズムを適用した lifting によりどの程度の CM 曲線が構成できるかは未知数であり，今後の検討課題である．

更に，本論文では提案アルゴリズムの実装実験を行い，提案アルゴリズムが $q \approx 1000$ 程度の有限体 $\mathbb{F}_q$ 上の種数 2 の多くの曲線に対して現実的な計算時間で自己準同型環を決定可能であることを確認した．しかし，個々の曲線固有の性質により自己準同型環決定困難な曲線も存在する．そこで，より一般的な曲線の自己準同型環を決定するために，提案アルゴリズムの高速化，memory 使用量削減について研究を続ける必要がある．特に Kohel は **3.** で紹介したアルゴリズムより高速なアルゴリズムを提案しており [24]，これの超楕円曲線への一般化は今後の重要な課題の一つである．

また，**6. 2** では実験結果をもとに平均計算量を見積もったが，より厳密な平均計算量の導出も今後の課題である．更に，種数 3 以上の超楕円曲線に対する提案アルゴリズムの実装も今後の課題として残る．

謝辞　本研究を進めるにあたり多くの有益な御助言を頂いた，中央大学百瀬文之教授に深謝致します．また，本研究に関し貴重な御意見，御指摘を頂いた査読委員に感謝致します．

本研究の一部は，通信・放送機構「情報セキュリティ高度化のための第 3 世代暗号技術の研究開発」プロジェクトの一環として行われたものである．

文　献

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

[2] S. Paulus and A. Stein, “Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves,” ANTS-III, no.1423 in Lecture Notes in Computer Science, pp.576–591, Springer-Verlag, 1998.

[3] P. Gaudry and R. Harley, “Counting points on hyperelliptic curves over finite fields,” ANTS-IV, ed. W. Bosma, no.1838 in Lecture Notes in Computer Science, pp.297–312, Springer-Verlag, 2000.

[4] K. Nagao, “Improving group law algorithms for Jacobians of hyperelliptic curves,” ANTS-IV, ed. W. Bosma, no.1838 in Lecture Notes in Computer Science, pp.439–448, Springer-Verlag, 2000.

[5] K. Matsuo, J. Chao, and S. Tsujii, “Fast genus two hyperelliptic curve cryptosystems,” IEICE Technical Report, ISEC2001-31, 2001.

[6] A.M. Spallek, “Kurven vom Geshlcht 2 und ihre Anwendung in Public-Key-Kryptosystemem,” PhD thesis, GH Essen, 1994.

[7] X. Wang, “2-dimensional simple factors of $J_0(N)$,” Manuscripta Math., vol.87, no.2, pp.179–197, 1995.

[8] K. Matsuo, J. Chao, and S. Tsujii, “Design of cryptosistems based on Abelian varieties over extension fields,” IEICE Technical Report, ISEC97-30, 1997.

[9] H.J. Weber, “Hyperelliptic simple factor of $J_0(N)$ with dimension at least 3,” Experimental Math., vol.6, no.4, 1997.

[10] G. Frey and M. Müller, “Arithmetic of modular curves and applications,” in Algorithmic algebra and number theory, ed. B. Matzat, G. Greuel, and G. Hiss, pp.11–48, Springer-Verlag, 1998.

[11] K. Matsuo, J. Chao, and S. Tsujii, “On lifting of CM hyperelliptic curves,” Proc. of SCIS’99, pp.173–178, 1999.

[12] P.V. Wamelen, “Example of genus two CM curves defined over the rationals,” Math. Comp., vol.68, no.225, pp.307–320, 1999.

[13] P.V. Wamelen, “Proving that a genus 2 curve has complex multiplication,” Math. Comp., vol.68, no.228, pp.1663–1677, 1999.

[14] J. Chao, K. Matsuo, and 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, ed. S. Qing and J.Eloff, pp.241–250, Kluwer Academic Pub., 2000.

[15] J. Chao, K. Matsuo, H. Kawashiro, and S. Tsujii, “Construction of hyperelliptic curves with CM and its application to cryptosystems,” Advances in Cryp-

tology - ASIACRYPT2000, ed. T. Okamoto, no.1976 in Lecture Notes in Computer Science, pp.259–273, Springer-Verlag, 2000.
[16] 芳賀智之, 松尾和人, 趙　晋輝, 辻井重男, “Ordinary lifting を用いた CM 超楕円曲線の生成,” Proc. of SCIS2000, no.C51, 2000.
[17] 若林岳秋, 中溝隆則, 松尾和人, 趙　晋輝, 辻井重男, “CM 多様体の Weil number の計算と安全な暗号系の設計,” Proc. of SCIS2000, no.C50, 2000.
[18] A. Weng, “Constructing hyperelliptic curves of genus 2 suitable for cryptography,” preprint, 2000.
[19] 高島克幸, “虚数乗法論を用いた種数 2 超楕円曲線の効率的な構成法について,” Proc. of SCIS2001, pp.749–754, 2001.
[20] 松尾和人, 芳賀智之, 趙　晋輝, 辻井重男, “井草不変量を用いた超楕円曲線暗号の構成について,” 信学論（A）, vol.J84-A, no.8, pp.1045–1053, Aug. 2001.
[21] J.F. Mestre, “Construction de curbes de genere 2 à partir de leurs modules,” in Effective methods in algebraic geometry, ed. C. T. T. Mora, no.94 in Progress in Mathematics, pp.313–334, Birkhäuser, 1991.
[22] J. Chao, O. Nakamura, K. Sobataka, and S. Tsujii, “Construction of secure elliptic cryptosystems,” Advances in Cryptology - ASIACRYPT’98, ed. K. Ohta and D. Pei, no.1514 in Lecture Notes in Computer Science, pp.95–109, Springer-Verlag, 1998.
[23] 趙　晋輝, 側高幸治, 中村　理, 辻井重男, “CM テストとリフティングによる安全な楕円暗号系の構成法,” 信学論（A）, vol.J82-A, no.8, pp.1261–1268, Aug. 1999.
[24] D. Kohel, “Endomorphism rings of elliptic curves over finite fields,” PhD thesis, UCB, 1996.
[25] H. Stichtenoth, “Algebraic function fields and codes,” Universitext, Springer-Verlag, 1993.
[26] M. Pohst, “Computational Algebraic Number Theory,” no.21 in DMV Seminer, Birkhäuser, 1993.
[27] M. Pohst and H. Zassenhaus, “Algorithmic Algebraic Number Theory,” no.30 in Encyclopedia of mathematics and its applications, Cambridge U.P., 1989.
[28] H. Cohen, “A Course in Computational Algebraic Number Theory,” no.138 in Graduate Text in Mathematics, Springer-Verlag, 1993.
[29] W.C. Waterhouse, “Abelian varieties over finite fields,” Ann. scient. Ec. Norm. Sup., 4^o **t. 2**, pp.521–560, 1969.
[30] N.D. Elkies, “Elliptic and modular curves over finite fields and related computational issues,” in Computational perspectives on number theory, ed. D.A. Buell and J.T. Teitlbaum, pp.21–76, AMS, 1995.
[31] D.G. Cantor, “On the analogue of the division polynomials for hyperelliptic curves,” Journal für die reine und angewandte Mathematik, vol.447, pp.91–145, 1994.
[32] H. Cohen, “Advanced Topics in Computational Number Theory,” no.193 in Graduate Text in Mathematics, Springer-Verlag, 1999.
[33] E. Teske, “A space efficient algorithm for group structure computation,” Math. Comp., vol.67, pp.1637–1663, 1998.
[34] `http://www.maths.usyd.edu.au:8000/u/magma/`.

（平成 13 年 7 月 9 日受付, 10 月 19 日再受付,
14 年 2 月 12 日最終原稿受付）

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．平 13 中大・理工・情報工博士後期課程了．工博．平 14 中大・研究開発機構助教授．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　（名誉員）

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．本会会長，米国電気電子学会（IEEE）東京支部長等歴任．中央大学研究開発機構長．総務省電波管理審議会会長．著書「暗号—ポストモダンの情報セキュリティ」（講談社メチエ選書),「暗号と情報社会」（文藝春秋社），他多数．