暗号理論とそれを支える代数曲線に関する研究

研究代表者　研究員　**關口　　力**（中央大学理工学部数学科）
共同研究者　研究員　**今井　桂子**（中央大学理工学部情報工学科）
共同研究者　研究員　**諏訪　紀幸**（中央大学理工学部数学科）
共同研究者　研究員　**趙　　晋輝**（中央大学理工学部電気電子情報通信工学科）
共同研究者　研究員　**辻井　重男**（中央大学理工学部情報工学科）
共同研究者　研究員　**百瀬　文之**（中央大学理工学部数学科）
共同研究者　研究員　**山本　　慎**（中央大学理工学部数学科）

1　はじめに

本研究は，2000 年より暗号理論を中心に，数学関係と情報関係合同の勉強会・研究会を主体に，研究を始めたものである。昨年 20002 年をもって 3 年目を迎え，このプロジェクト研究の一応の区切りとし，この研究活動は 21COE セキュリティプログラムの一部として発展解消するものである。

この研究活動において，研究員全員による研究活動は，RA，大学院生も含めて，毎年夏に研究開発機構「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」との共催，FACT，FAIT の協賛を得て開催したワークショップ「暗号理論とそれを支える代数曲線理論」である。このワークショップでは，数学，情報工学，企業の現場，教育とのお互いの交流を得ることを計ったものであり，実際に，多数の企業の方々，大学の数学及び暗号の研究者，各大学の学生，と幅広く出席を得て，当初の目的の何分の一かは達成できたのではないかと，密かに自負しているものである。

研究内容についてであるが，現在の公開鍵暗号は RSA 暗号が主流であり，その安全性の問題から楕円曲線暗号が実用化され，更に次世代の暗号として，超楕円曲線あるいは一般の代数曲線の Jacobi 多様体の有理点を用いた暗号の実用化も模索され，一部は実際に実装されている。本研究では，上記研究集会の成果を基に，一般代数曲線を用いた公開鍵暗号システムを念頭に，代数曲線の Jacobi 多様体における群演算の効率的なアルゴリズムの研究，暗号学的に安全な代数曲線の探求，代数曲線暗号に対する攻撃法の可能性についての研究を目指して来た。

また，RSA 暗号は素因数分解の難しさに依存するものであるが，その難しさは素因数分解，素数判定のアルゴリズムに依存する。素数判定のアルゴリズムは色々存在し，実際に使われているが，確定的かつ実用的なアルゴリズムは未だ存在せず，現在の実用的アルゴリズムは全て確率的である。ここでは，こうした一連のアルゴリズムを体系化し，その実験的確率的評価を行い，アルゴリズムの効率化についても研究している。

2000，2001 年度の研究発表では，代数曲線の Jacobi 多様体における群演算アルゴリズムの効率化として，一般化された Jacobi 多様体と呼ばれる，特異代数曲線の Jacobi 多様体を用いる手法を提案し，その原理的な理論に関する基本研究を紹介し，その基本研究に基付き，そのアルゴリズムについて，代数曲線の三浦モデルである C_A モデルの有効な利用方法を提案したものであった。今回は，こうした研究の一応の集大成として，三浦晋示氏，有田正剛氏との共同研究の下，代数曲線を特異点を許し，平面三浦モデルである $C_{a,b}$ モデルを用い，方程式を単純化し，有田アルゴリズムの効率的計算方法を提案し，そのシュミレーションを与えたものである。

2000，2001，2003 年度の 3 年間に渡り，理工学研究所よりプロジェクト研究の援助を戴き，情報工学，数学の両分野の，ささやかではあるが交流を図ることが出来，こうした多くの方々との交流が中央大学を中心とした 21COE セキュリティプログラムの一部の流れとしていささかでもお役に立てたのではないかと自負するものであり，またこうした機会を与えて下さった理工学研究所に多大の感謝を捧げるものである。

2　一般化された Jacobi 多様体

代数曲線を用いた暗号を構成する際，その代数曲線を具体的に表示する必要がある。具体的表示とは座標空間（射影空間）の中で方程式で書き表すことであり，その書き表し方がその暗号アルゴリズムの全てを決定する。出来るものであれば，その書き表し方は，単純であれば単純である程良い。

代数曲線を非特異モデルにより表そうとすると，一般には 3 次元空間が必要であり，曲線を具体的に表そうとする

と少なくとも二つの方程式が必要である。楕円曲線あるいは超楕円曲線（無限遠点を除いて）は，射影平面の中に非特異のまま埋め込めるが，一般には平面に埋め込む場合，非特異性を犠牲にしなければならない。ここでは，我々は非特異性を犠牲にし，曲線の単純表現を採用するのである。Jacobi 多様体の加法アルゴリズムを具体化するためには，更に代数曲線のモデルを旨く取らなければならない。この方法は三浦モデルと言われるもので，これ以上ない形で実現され，これについては次の節で説明を行う。ここでは，特異代数曲線の，所謂一般化された Jacobi 多様体について議論する。

C_0 を体 $k = \mathbb{F}_q$ 上の代数曲線とし，その関数体を $K = k(C_0)$ とする。以下，k-rational point $\mathrm{P}_0 \in C_0$ を高々 cusp singularity とし，C_1 の点 P_0 のみを非特異化した曲線とする。$\pi : C \to C_1 \to C_0$ を C_1 の，また C_0 の正規化，すなわち非特異化とし，$g = g(C)$ を C の種数とする。

$\mathcal{O} = \mathcal{O}_{C_1}$ を C_1 の構造層とし，$\mathcal{K}$ を関数体からなる C_1 上の定数層とする。このとき，$\mathrm{H}^0(C_1, \mathcal{K}^*/\mathcal{O}^*)$ の元は C_1 の Cartier divisor と呼ばれるものであり，Cartier divisor class group は次で与えられる。

$$\begin{aligned}\mathrm{CalCl}(C_1) &:= \mathrm{H}^0(C_1, \mathcal{K}^*/\mathcal{O}^*) \\ &\quad /\mathrm{Image}(K^* \to \mathrm{H}^0(C_1, \mathcal{K}^*/\mathcal{O}^*)).\end{aligned}$$

更に，Picard group は次で与えられる。

$$\begin{aligned}\mathrm{Pic}(C_1) &:= \mathrm{H}^1(C_1, \mathcal{O}^*) \\ &= \{\text{invertible sheaves on } C_1\}/\text{isomorphisms}.\end{aligned}$$

このとき，標準的同型写像

$$\mathrm{Pic}(C_1) \cong \mathrm{CalCl}(C_1)$$

を得る。

正規化写像 $\pi : C \to C_1$ は完全列 (cf. [3, Ch.II, Ex.6.9]):

$$\begin{aligned}0 &\longrightarrow \oplus_{\mathrm{P}\in C_1} \widetilde{\mathcal{O}}_{\mathrm{P}}^*/\mathcal{O}_{\mathrm{P}}^* \\ &\longrightarrow \mathrm{Pic}(C_1) \xrightarrow{\pi^*} \mathrm{Pic}(C) \longrightarrow 0 \qquad (1)\end{aligned}$$

を導く。但し，$\widetilde{\mathcal{O}}_{\mathrm{P}}$ は $\mathcal{O}_{\mathrm{P}}$ の K における整閉包を意味する。

非特異代数曲線 C に対して，群 $\mathrm{Pic}(C)$，$\mathrm{CalCl}(C)$ は divisor class group:

$$\mathrm{DivCl}(C) := \{k\text{-rational divisors on } C\}/\{(f) \mid f \in K\}$$

に同型である。以下，$[D]$ により因子 D により代表される因子類を表す。次数零の因子類群を

$$\mathrm{Pic}^0(C) \cong \mathrm{CalCl}^0(C) \cong \mathrm{DivCl}^0(C) \subset \mathrm{DivCl}(C)$$

で表し，

$$\mathrm{Pic}^0(C_1) := (\pi^*)^{-1}(\mathrm{Pic}^0(C)) \subset \mathrm{Pic}(C_1) \qquad (2)$$

とおく。このとき，完全系列 (1) は次の完全列

$$\begin{aligned}0 \longrightarrow \oplus_{\mathrm{P}\in C_1} \widetilde{\mathcal{O}}_{\mathrm{P}}^*/\mathcal{O}_{\mathrm{P}}^* &\longrightarrow \mathrm{Pic}^0(C_1) \\ &\xrightarrow{\pi^*} \mathrm{Pic}^0(C) \longrightarrow 0 \qquad (3)\end{aligned}$$

を導く。以下，$\mathrm{Pic}^0(C_1)$ を C_1 を *Jacobian group* と呼ぶ。

スキーム $C_0 \setminus \{\mathrm{P}_0\} = C_1 \setminus \{\mathrm{P}_0\}$ の座標環を

$$R := \Gamma(C_0 \setminus \{\mathrm{P}_0\}, \mathcal{O})$$

で表す。

$\mathcal{I}(R)$ により R の可逆イデアルのなす群を表し，$H(R)$ によりイデアル類群:

$$\mathrm{H}(R) := \mathcal{I}(R)/\{(f) = fR \mid f \in K^*\}$$

を表す。このとき，自然に同型

$$\mathrm{H}(R) \cong \mathrm{Pic}(C_1 \setminus \{P_0\})$$

を得，結局次の同型を得る。

$$\begin{aligned}\mathrm{H}(R) \cong \mathrm{Pic}(C_1 \setminus \{P_0\}) &\cong \mathrm{CalCl}(C_1 \setminus \{P_0\}) \\ &\cong \mathrm{CalCl}^0(C_1) \cong \mathrm{Pic}^0(C_1) \quad (4)\end{aligned}$$

以上により，$\mathrm{Pic}^0(C)$ の加法アルゴリズムは座標環 $R = \Gamma(C_0 \setminus \{\mathrm{P}_0\}, \mathcal{O})$ のイデアル類群のアルゴリズムに帰着される。

次に，C_A 曲線と呼ばれる三浦モデルにより，曲線の我々の目的にそうモデルの取れることを示す。

1 三浦 C_A curves

この節の結果は三浦 [4, Appendix] のまとめである。

$\mathbb{N}$ により非負整数のなす半群を表す。$\mathbb{N}$ の部分半群 M は，有限生成，即ち，M の元 $a_1, a_2, \ldots, a_t \in M$ $(a_1 < a_2 < \cdots < a_t)$ が存在し

$$M = < a_1, a_2, \ldots, a_t > = \mathbb{N}a_1 + \mathbb{N}a_2 + \ldots + \mathbb{N}a_t$$

と表される。但し，$t \le a_1$ である。

M の生成系 $A = \{a_1, \ldots, a_t\}$ に対して，M の $\mathbb{N}$ における補集合が有限集合であるための必要十分条件は $(a_1, a_2, \ldots, a_t) = 1$ であり，このとき，実際に次を得る。

$$\#(\mathbb{N} \setminus M) = \sum_{i=1}^{a_1 - 1} \left[\frac{b_i}{a_1}\right],$$

但し，各 $i = 0, 1, \ldots, a_1 - 1$ に対して

$$b_i := \mathrm{M}in\{a \in M \mid a \equiv i \pmod{a_1}\} \tag{5}$$

である。この場合に M を *numerical semigroup* と言う。

以下，M を生成系 $A = \{a_1, a_2, \ldots, a_t\}$ を持つ numerical semigroup とする。

numerical semigroup M に対して，全射写像 $\Psi : \mathbb{N}^t \to M$ を $\Psi(n_1, n_2, \ldots, n_t) := \sum_{i=1}^{t} n_i a_i$ で定義する。この写像を用いて $\mathbb{N}^t$ 上の単項順序（これを C_A- 順序という）を次のように定義できる。

定義 1.1. $\mathbb{N}^t$ の二つの元 $\boldsymbol{m} = (m_1, m_2, \ldots, m_t)$，$\boldsymbol{n} = (n_1, n_2, \ldots, n_t)$ に対して，順序を

$$\boldsymbol{m} < \boldsymbol{n} \overset{\text{def}}{\Longleftrightarrow} \begin{cases} \Psi(\boldsymbol{m}) < \Psi(\boldsymbol{n}) \\ or \\ \Psi(\boldsymbol{m}) = \Psi(\boldsymbol{n}) \ and \\ m_1 = n_1, \ldots, m_i = n_i, m_{i+1} > n_{i+1} \end{cases}$$

で定義する。この順序を用いて $\mathbb{N}^t$ の二つの部分集合を次のように定義する。

定義 1.2.

$$B(A) := \{\boldsymbol{m}(a) \mid a \in M\} \subset \mathbb{N}^t,$$

$$V(A) := \left\{ \boldsymbol{\ell} \in \mathbb{N}^t \setminus B(A) \;\middle|\; \begin{array}{l} if\ \boldsymbol{\ell} = \boldsymbol{m} + \boldsymbol{n} \\ with\ \boldsymbol{m} \in \mathbb{N}^t \setminus B(A) \\ and\ \boldsymbol{n} \in \mathbb{N}^t, \\ then\ \boldsymbol{n} = \boldsymbol{0} \end{array} \right\},$$

但し $a \in M$ に対して，$\boldsymbol{m}(a) := \mathrm{M}in\{\boldsymbol{n} \mid \boldsymbol{n} \in \Psi^{-1}(a)\}$，また b_i's は *(5)* で与えられた数である。

こうした記号の下に，多項式 $F_{\boldsymbol{m}} \in k[X] = k[X_1, X_2, \ldots, X_t]$ $(\boldsymbol{m} \in V(A))$ で次の性質を満たすものを考える。

(D1) 各 $\boldsymbol{m} \in V(A)$ に対して，

$$F_{\boldsymbol{m}} = X^{\boldsymbol{m}} + a_{\boldsymbol{\ell}} X^{\boldsymbol{\ell}} + \sum_{\boldsymbol{n}} a_{\boldsymbol{n}} X^{\boldsymbol{n}},$$

但し，$\boldsymbol{\ell} = \boldsymbol{m}(\Psi(\boldsymbol{m}))$，$a_{\boldsymbol{\ell}} \neq 0$ であり，和は $\boldsymbol{n} \in B(A)$ with $\boldsymbol{n} < \boldsymbol{m}$ の上を走らせる。ここで，$\boldsymbol{m} = (m_1, m_2, \ldots, m_t)$ に対して，$X^{\boldsymbol{m}} = \prod_{i=1}^{t} X_i^{m_i}$ である。

(D2) $\left(\sum_{\boldsymbol{n} \in B(A)} kX^{\boldsymbol{n}}\right) \cap (F_{\boldsymbol{m}} \mid \boldsymbol{m} \in V(A)) = (0)$

次に，関数体 K の非特異モデル C の k-有理点 P に対して

$$L(\infty \mathrm{P}) := \cup_{n \geq 0} L(n\mathrm{P}) \subset K,$$

and

$$M(\mathrm{P}) := \{-\mathrm{ord}_{\mathrm{P}}(f) \mid f \in L(\infty \mathrm{P}) \setminus \{0\}\} \subset \mathbb{N}$$

と定義する。このとき $M(\mathrm{P})$ は numerical semigroup である。

$L(\infty \mathrm{P})$ の部分代数 R で k を含むものをとり，半群を

$$M(R) := \{-\mathrm{ord}_{\mathrm{P}}(f) \mid f \in R \setminus \{0\}\} \subset \mathbb{N}$$

で定義し，$A = \{a_1, a_2, \ldots, a_t\}$ をその生成系とする。このとき次を得る。

Lemma 1.1. f.f.(R) が K と一致するための必要十分条件は $(a_1, a_2, \ldots, a_t) = 1$ である。

以下，f.f.$(R) = K$，すなわち，$M(R)$ が numerical semigroup とする。各 $i = 1, 2, \ldots, t$ に対して，関数 $f_i \in R$ を $\mathrm{ord}_{\mathrm{P}}(f_i) = -a_i$ を満たすものとする。ここで $\Theta(F) := F(f_1, f_2, \ldots, f_t)$ により定義される

$$\Theta : k[X] = k[X_1, X_2, \ldots, X_t] \to R$$

を考える。このとき，核 $I(R) := \mathrm{Ker}(\Theta)$ は条件 (D1) と (D2) を満たす多項式により生成され，K の C_A 曲線と呼ばれるアフィンモデル $\mathrm{Spec}(k[X]/I(R)$ が得られ，これが我々の望む曲線の具体的なもであるである。三浦は更にこの逆の成り立つことも示している。

2 特異 C_A 曲線の一般 Jacobi 多用体における有田アルゴリズ

以下，前節の記号の下に話を進める。R の可逆イデアル $\mathfrak{a}$ に対して，$h \in 1 :_K \mathfrak{a} = \mathfrak{a}^{-1}$ を零でない最小の minus order $-\mathrm{ord}_{\mathrm{P}}(h)$ を持つものとする。ここでイデアル $\mathfrak{a}^*$ を $\mathfrak{a}^* := h \cdot \mathfrak{a}$ で定義する。イデアル類 $[\mathfrak{a}]$ の特別な代表元として $\mathfrak{a}^*$ を採用するのである。実際，容易に次を得る。

Lemma 2.1. イデアル $\mathfrak{a}^*$ は，イデアル類 $[\mathfrak{a}]$ によって一意的に定まる。

我々は $\mathfrak{a}^* = h \cdot \mathfrak{a}$ (あるいは $\mathfrak{A}^* := \Theta^{-1}(\mathfrak{a}^*) \subset k[X] = k[X_1, X_2, \ldots, X_t]$) を $\mathfrak{a}$ の *reduced ideal* と呼ぶ。重要な点は，与えられたイデアル類の reduced ideal $\mathfrak{a}^*$ を如何に計算するかである。実際，零でない元 $f \in \mathfrak{a}$ をとり，

$$g \in (f) :_K \mathfrak{a} = (f) :_R \mathfrak{a} = f \cdot \mathfrak{a}^{-1}$$

を零でない最小の minus order $-\mathrm{ord}_{\mathrm{P}}(g)$ を持つものとする。このとき $h = g/f$ である。

以上により，特異曲線の一般化された Jacobi 群における加法アルゴリズムが次のように与えられる。

Algorithm 1 (C_A 曲線の加法アルゴリズム). *Inputs: R* の可逆イデアル $\mathfrak{a}_1$, $\mathfrak{a}_2$ の生成系

Output: reduced ideal $(\mathfrak{a}_1\mathfrak{a}_1)^*$ *の Gröbner basis*

1. 生成系 $(f_1, f_2, \ldots, f_\ell)+I = \mathfrak{A}_1$, $(g_1, g_2, \ldots, g_m)+I = \mathfrak{A}_2$ をとる
2. 零でない元 $f \in \mathfrak{A}_1\mathfrak{A}_2 \setminus I$ をとる
3. $g \in \left((fk[X] + I) :_{k[X]} \mathfrak{A}_1\mathfrak{A}_2\right)$ を最小の C_A-*order* をもつものをとる
4. $(\mathfrak{A}_1\mathfrak{A}_2)^* = h \cdot (\mathfrak{A}_1\mathfrak{A}_2)$ の *Gröbner basis*, 但し $h = g/f$

3 An example

$k := \mathbb{F}_{83}$ とし，特異 C_{35} 曲線 C を次で与える。

$$-30 - 11X - 6Y - 6X^2 - 31XY - 80X^3 - 59Y^2$$
$$-35X^2Y - 41X^4 - 7XY^2 - 78X^3Y - 10X^5 + Y^3.$$

$(70, 65)$ が C の唯一の特異点である。R の可逆イデアル $G := (X - 2, Y - 33)$ をとる。G は C の非特異モデルの Jacobi 群において位数 $n = 2^3 \cdot 3 \cdot 7 \cdot 11$ の点を与える。従って，$n \cdot G$ は 82 倍により零となる。実際 $H := n \cdot G = (Y^2+14Y+34X+38, XY+13Y+18X+68, X^2+26X+3)$ となり，$82 \cdot H = (1)$ を得る。

参 考 文 献

[1] S. Arita, *Algorithms for computations in Jacobian group of C_{ab} curve and their application to discrete-log-based public key cryptosystems*, Conference on The Mathematics of Public Key Cryptography, Toronto, 1999

[2] S. Arita, *The discretes-log-based public key cryptosystems using algebraic curves of heigher degree*, in Japanese, Doctor Thethis (Chuo University), 2000

[3] R. Hartshorne, *Aalgebraic geometry*, Springer-Verlag, 197

[4] S. Miura, *The linear code on affine algebraic curves*, in Japanese, Shingakuron(A), vol. J81-A, No. 10, 1398–1421(1998)

[5] J.-P. Serre, *Groupes algébriquees et corps de classes*, Hermann, Paris(1961)