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。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。

現在の公開鍵暗号は RSA 暗号が主流であるが，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。ここでは，Rabin 素数判定を中心にそのアルゴリズムの効率化についても，研究している。

一方で共通鍵暗号では，一方向性関数あるいは擬似乱数が重要な要素であり，その安全性はその擬似乱数の質に依存している。従って，擬似乱数を評価することは重要な問題であるが，この評価についても既存の擬似乱数について実行することを目指している。

昨年の研究発表では，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た。今回，その基本研究に基付き，そのアルゴリズムについて，三浦晋二氏との共同研究の下，代数曲線の三浦モデルである C_{ab} モデルを用いたシュミレーションを行い，更に有田正剛氏の代数曲線を用いた暗号システムについて，そのアルゴリズムの効率化について考察するものである。

2　一般化された Jacobi 多様体

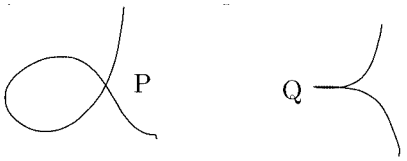
代数曲線を用いた暗号を構成する際，その代数曲線を具体的に表示する必要がある。具体的表示とは座標空間（射影空間）の中で方程式で書き表すことであり，その書き表し方がその暗号アルゴリズムの全てを決定する。出来るものであれば，その書き表し方は，単純であれば単純である程良い。代数曲線の書き表し方については，先ず次の事実がある。

定理１ 任意標数の代数的閉体 k 上の任意の完備非特異代数曲線 C は，3 次元射影空間 $\mathbb{P}^3_k$ に埋め込める。

この定理により，一般の代数曲線は全て非特異のまま 3 次元射影空間の中で具体的にかかれるのであるが，その際，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，一般には非特異性を犠牲にしなければならない。これに関して，次の事実が成り立つ。

定理２　任意標数の代数的閉体 k 上の任意の完備非特異代数曲線 C は，高々node のみの特異点を許すことにより，射影平面 $\mathbb{P}^2_k$ に埋め込める。ここで，node とは下記図の

点 P のように 2 本の枝が異なる方向から交わる特異点をいう。また，図の Q のような点を cusp という。



このように，射影平面に埋め込もうとすると非特異性を諦めないといけないが，その代り，曲線の単純表現を獲得することが出来る。

こうした曲線の genus は次の式で与えられる。

定理 3 $\mathbb{P}_k^2 \supset C$ は次数 d, r 個の node のみの特異点をもつ既約な曲線とする。このとき，genus は

$$g(C) = \frac{(d-1)(d-2)}{2} - r$$

である。

以下，既約平面曲線 $C \subset \mathbb{P}_k^2$ について，$\pi : \widetilde{C} \to C$ をその normalization, 即ち，C の非特異化とする。このとき，完全系列

$$0 \longrightarrow \pi_* \mathcal{O}_{\widetilde{C}}^* / \mathcal{O}_C^* \longrightarrow \mathcal{K}_C^* / \mathcal{O}_C^* \longrightarrow \mathcal{K}_C^* / \pi_* \mathcal{O}_{\widetilde{C}}^* \longrightarrow 0$$

から global section をとることより，完全系列

$$0 \longrightarrow \oplus_{P \in C} \widetilde{\mathcal{O}}_P^* / \mathcal{O}_p^* \longrightarrow \mathrm{Pic}_k(C) \xrightarrow{\pi^*} \mathrm{Pic}_k(\widetilde{C}) \longrightarrow 0$$

を得る。但し，$\widetilde{\mathcal{O}}_P$ は $\mathcal{O}_P$ の normalization である。

$\mathbb{P}_k^2 \supset C$ を, 特異点として r 個の node $P_1, P_2, \ldots, P_r$ をもつ d 次既約曲線, $\pi : \widetilde{C} \to C$ をその normalization とする。無限遠点 P_∞ とし，各 P_i $(i = 1, \ldots, r)$ は P_∞ と異なるものとする。このとき $g(\widetilde{C}) = (d-1)(d-2)/2 - r$ であり，$\pi^{-1}(P_i) = \{P_{i1}, P_{i2}\}$ とおくとき，$\mathcal{O}_{C,P_i} = k + \mathfrak{m}_{P_{i1}} \cap \mathfrak{m}_{P_{i2}}$ であり，この normalization は $\widetilde{\mathcal{O}}_{C,P_i} = \mathcal{O}_{\widetilde{C},P_{i1}} \cap \mathcal{O}_{\widetilde{C},P_{i2}}$ で与えられる。これらから上記完全系列より

$$0 \longrightarrow (k^*)^r \longrightarrow \mathrm{Pic}_k(C) \longrightarrow \mathrm{Pic}_k(\widetilde{C}) \longrightarrow 0$$

を得る。

$\mathrm{Pic}_k^o(C) \subset \mathrm{Pic}_k(C)$ は前回の報告で与えられている通り，一般に C 上の degree 0 の Cartier divisors あるいは invertible sheves で記述されるもので，特異曲線の Jacobi 多様体**一般化された Jacobi 多様体**というものである。

更に，以下，$C_0 \subset \mathbb{P}_k^2$ を，特異点として無限遠点 $\mathrm{P}_\infty \in C_0$ で高々 cusp, 点 $Q \in C_0$ で node のみをもつ曲線とし，C を C_0 の点 P_∞ を非特異化したもの，$\pi : \widetilde{C} \to C$ をその normalization, $\pi^{-1}(Q) = \{Q_1, Q_2, \ldots, Q_r\} \subset \widetilde{C}$ とする。C_0 の次数を d とするとき，C の arithmetic genus g_a と genus g は

$$g_a(C_0) = \frac{(d-1)(d-2)}{2};$$
$$g(C) = g(\widetilde{C}) = g_a(C_0) - r + 1 - \epsilon$$

で与えられる。但し，$\epsilon = dim(\widetilde{\mathcal{O}}_{P_\infty}^* / \mathcal{O}_{P_\infty}^*$ である．$\widetilde{C}$ の divisor $\mathfrak{m} := \sum_{i=1}^r Q_i$ に対して，divisor E が $\mathfrak{m}$ と**互いに素**であるとは，互いに共通因子を持たないこと，即ち $|E| \cap |\mathfrak{m}| = \emptyset$ を意味し，$(E, \mathfrak{m}) = 1$ で表す。$\mathrm{Pic}_{\mathfrak{m}}^o(C)$ を

$$\mathrm{Pic}_{\mathfrak{m}}^o(C) := \left\{ D\colon \text{ divisor on } C \setminus \mathfrak{m} \;\middle|\; \begin{array}{c} \deg(D) = 0 \\ (D, \mathfrak{m}) = 1 \end{array} \right\} \Big/ \{(f) \mid f \in k(C), ((f), \mathfrak{m}) = 1\}$$

で定義するとき，

補題 4 任意の元 $[D] \in \mathrm{Pic}^o(\widetilde{C})$ に対して，$E \succeq 0$, $\ell = \deg(E) \leq g_a$, $E - \sum_1^\ell M_i \in [D]$, $(E - \sum M_i, m) = 1$ を満たすものが存在する。従って，

$$\mathrm{Pic}^o(\widetilde{C}) = \mathrm{Pic}_{\mathfrak{m}}^o(C)$$

を得る。

証明. [5, (V,n^o4, Lem. 4)] 参照。

C 上の関数 $f \in k(C)$ に対して，

$$f \overset{\mathfrak{m}}{\equiv} 1 \pmod{\mathfrak{m}} \overset{\text{def}}{\Longleftrightarrow} \nu_{\mathrm{Q_i}}(\mathfrak{f} - \mathfrak{1}) \geq \mathfrak{1} \quad (\mathfrak{i} = \mathfrak{1}, \ldots, \mathfrak{r})$$

で定義する。このとき

$$\mathrm{Pic}^o(C) = \{D \mid \deg(D) = 0, (D, \mathfrak{m}) = 1\} / \{(f) \mid f \overset{\mathfrak{m}}{\equiv} 1\}$$

と表される。従って，完全系列

$$0 \longrightarrow k(C)^* / \{f \in k(C)^* \mid f \overset{\mathfrak{m}}{\equiv} 1\} \longrightarrow \mathrm{Pic}^o(C) \xrightarrow{\pi^*} \mathrm{Pic}^0(\widetilde{C}) \longrightarrow 0$$

を得，$k(C)^* / \{f \in k(C)^* \mid f \overset{\mathfrak{m}}{\equiv} 1\} \cong \mathbb{G}_m^{r-1}$ を得る。

ここでは，群 $\mathrm{Pic}_{\mathfrak{m}}^o(C)$ あるいは $\mathrm{Pic}^o(C)$ の表現について，議論する。

3 Picard 群の表現

以下, 考える多様体は integral なもの, 即ち, irreducible かつ reduced なもののみを扱う。k を標数 $p\,(\geq 0)$ の体, X を簡単のために k 上の integral scheme とする。$\mathcal{K}_X$ を X の各 open set に対して X の関数体 $k(X)$ を対応させる sheaf $\Gamma(U,\mathcal{K}_X)=k(X)$ を表し, $\mathcal{K}_X$ の subsheaf $\mathcal{K}_X^*$ を $\Gamma(U,\mathcal{K}_X^*)=k(X)\setminus\{0\}$ で定義する。同様に, 構造層 $\mathcal{O}_X$ の subsheaf $\mathcal{O}_X^*$ を $\Gamma(U,\mathcal{O}_x^*)=\Gamma(U,\mathcal{O}_x)^\times$ で定義する。このとき, 完全系列

$$0\longrightarrow\mathcal{O}_X^*\longrightarrow\mathcal{K}_X^*\longrightarrow\mathcal{K}_X^*/\mathcal{O}_X^*\longrightarrow 0$$

を得るが, $\Gamma(X,\mathcal{K}_X^*/\mathcal{O}_X^*)$ の元を X の Cartier divisor といい,

$$\mathrm{CaCl}_k(X):=\Gamma(X,\mathcal{K}_X^*/\mathcal{O}^*)/\Gamma(X,\mathcal{K}_X^*)$$

を X の Cartier divisor class group という。一方,

$$\mathrm{Pic}_k(X):=\mathrm{H}^1(X,\mathcal{O}_X^*)=\{\text{invertible sheaves over } X\}/\cong$$

を X の Picard group という。このとき, 上の完全系列より写像

$$\partial:\mathrm{CaCl}_k(X)\longrightarrow\mathrm{Pic}_k(X)$$

を得るが, これに関して次の結果を得る。

定理 5 X が integral scheme のとき, 写像 $\mathrm{CaCl}_k(X)\to\mathrm{Pic}_k(X)$ は同型写像である。

Cartier divisor は具体的に次のように表現される。

$D=[(U_i,f_i)_{i\in I}]\in\mathrm{CaCl}_k(X)$
$:=\Gamma(X,\mathcal{K}_X^*/\mathcal{O}^*)/\Gamma(X,\mathcal{K}_X^*)$, 但し, $X=\cup_{i\in I}U_i$: open covering, $f_i\in\Gamma(U_i,\mathcal{K}_X^*)=k(X)^*$ $(i\in I)$ であり, 各 $i,j\in I$ に対して, $f_i/f_j\in\Gamma(U_i\cap U_j,\mathcal{O}_X^*)$ を満たす。f_i を Cartier divisor D の **local equation** という。

Cartier divisor $D=[(U_i,f_i)_{i\in I}]\in\mathrm{CaCl}_k(X)$ に対応する invertible sheaf $\mathcal{O}_X(D)$ は, 各 $i\in I$ に対して $\Gamma(U_i,\mathcal{O}_X(D))=\Gamma(U_i,\mathcal{O}_X)f_i^{-1}\subset\Gamma(U_i,\mathcal{K}_X)$ で定義されるものである。

以下, 既約平面曲線 $C_0\subset\mathbb{P}_k^2$ について, $\pi:\widetilde{C}\to C\to C_0$ をその normalization, 即ち, C の非特異化とし, 前節の後半の設定とする。このとき, 前節の完全系列より

$$0\longrightarrow(k^*)^{r-1}\longrightarrow\mathrm{Pic}_k^o(C)\longrightarrow\mathrm{Pic}_k^o(\widetilde{C})\longrightarrow 0$$

を得る。

$\mathrm{Pic}_k^o(C)$ あるいは $\mathrm{Pic}_k^o(\tilde{C})$ における演算の記号であるが, Cartier divisor による表現の問題は, affine 開被覆の特定化である。

ここでは, 次の設定を設ける。$\mathrm{Pic}_k^o(\tilde{C})$ 有限部分群 G をとり, G の元を $E-\boldsymbol{\ell}\mathrm{P}_\infty$, $E\succeq 0$ と書いたとき, G の全ての元に対して $(E,\mathrm{m})=1$ となる divisor m を選ぶ。このとき, 我々は, 有田 [1] によるアルゴリズムを座標環 $A=\Gamma(C\setminus\{Q_1,\ldots,Q_r,P_\infty\},\mathcal{O}_C)$ 上で実行することが出来る。

Remark. $\mathrm{Pic}_{\mathrm{m}}^o(C)$ あるいは $\mathrm{Pic}^o(C)$ の元の表現として, Weil divisor として, あるいは Cartier divisor として, あるいは $H^1(C,\mathcal{O}_C^*)$ の元として cocycle で表す方法が考えられ, cohological な表現によるアルゴリズムの開発は, 今後の課題である。

4 三浦モデルによる表現

曲線を表現する上で, 種々のアルゴリズムに馴染みの良い表現が三浦氏によって与えられている。それは C_{ab} 曲線と呼ばれるものであるが, これについて, 有田 [1] より引用する。k 上定義された, k 有理点 P をもつ非特異代数曲線とする。

$L(\infty\mathrm{P})$ に対応する半群を $M_{\mathrm{P}}:=\{-v_P(f)\mid f\in L(\infty P)\}\subset\mathbb{N}_0$ とするとき, その生成元を小さい順に $M_{\mathrm{P}}=\mathbb{N}_0a_1+\mathbb{N}_0a_2+\ldots+\mathbb{N}_0a_t$ とし, $a=(a_1,a_2,\ldots,a_t)$ とおく。

$\mathbb{N}_0^t\ni\boldsymbol{n}=(n_1,n_2,\ldots,n_t)$ に対して,

$$\Psi(\boldsymbol{n}):=\sum_{i=1}^t n_ia_i$$

とし, $\mathbb{N}_0^t$ の順序を

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

で定義するとき, これは項順序を定義し, $C_{\boldsymbol{a}}$ **順序** と呼ばれる。

$$B(\boldsymbol{a}):=\{\boldsymbol{n}\in\mathbb{N}^t\mid\boldsymbol{n}=\min\{\boldsymbol{m}\mid\Psi(\boldsymbol{m})=a\in N(\mathrm{P}_\infty)\}\}$$

更に

$$V(\boldsymbol{a}):=\left\{\boldsymbol{\ell}\in\mathbb{N}_0^t\setminus B(\boldsymbol{a})\;\middle|\;\begin{array}{c}\boldsymbol{\ell}=\boldsymbol{m}+\boldsymbol{n},,\boldsymbol{m}\in\mathbb{N}_0^t\setminus B(\boldsymbol{a})\\ \boldsymbol{n}\in\mathbb{N}_0^t\end{array}\right.$$
$$\left.\Longrightarrow\;\boldsymbol{n}=\boldsymbol{0}\right\}$$

即ち，$\mathbb{N}_0^t \setminus B(\boldsymbol{a})$ の元 $\boldsymbol{\ell}$ で極小のものの集合を $V(\boldsymbol{a})$ とおく。このとき，次が三浦の結果である。

定理 6 曲線 C は t 次元 affine 空間に非特異モデルをもち，定義方程式を

$$F_m = X^m + a_{\boldsymbol{\ell}} X^{\boldsymbol{\ell}} + \sum_{\boldsymbol{n} \in B(\boldsymbol{a}), \Psi(\boldsymbol{n}) < \Psi(\boldsymbol{m})} \alpha_n X^m \qquad (\boldsymbol{m} \in V(\boldsymbol{a}))$$

で与えられる。ここで，$\boldsymbol{\ell}$ は $\Psi(\boldsymbol{m}) = \Psi(\boldsymbol{\ell})$ となる唯一の $\boldsymbol{\ell} \in B(\boldsymbol{a})$ である。更に，この affine モデルは唯一の無限遠点 $\mathrm{P}_\infty = P$ をもつ。

例 C_{35} 曲線は，平面曲線として

$$y^3 + x(x-y) + x^5 = 0$$

で表され，arithmetic genus $g_a = 4$, geometric genus $g = 3$ であり，P_∞ で cusp, 原点で node である。

課題

この研究による，特異代数曲線を用いた Jacobi 多様体上のアルゴリズムは，現在三浦氏の力を借りて研究推進中であるが，よりよい divisor の表現法の開発，それによるそのアルゴリズムの実装シュミレーション，既存のアルゴリズムとの比較評価は今後の課題である。

参 考 文 献

[1] 有田正剛, 高次代数曲線を用いた離散対数型暗号，中央大学理工学研究科情報工学専攻博士論文　2000 年 1 月 25 日

[2] W. Fulton, *Algebraic curves*, W.A. Benjamin, Inc., 1969

[3] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, GTM 52, New York 1977

[4] D. Mumford, *Lectures on curves on an algebraic surface*, Annals of Math. Studies 59, Princeton University Press, Prenceton 1966

[5] J.-P. Serre, *Groupes algébriques et corps de classes*, Hermann Paris, 1959

[6] 松尾和人，趙　晋輝, 種数 2 の超楕円曲線を用いた高速暗号系について，preprint, 2001