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

現在，公開鍵暗号は RSA 暗号が主流で有りつつも，その安全性の問題から楕円曲線暗号が実用化され，重要度の高い情報は楕円曲線暗号利用が主流となるであろう。しかし，コンピューターの進歩は激しく，既に楕円曲線暗号の次世代暗号形式が模索され，その一つとして考えられているのが代数曲線の Jscobi 多様体を用いる暗号である。

本研究では，数学関係と情報関係合同の勉強会・研究会を主体に行い，そうした成果を基に，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行ってきた。本文では，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 多様体を用いる手法について報告する。尚，一般化された Jacobi 多様体とは，特異曲線の Jacobi 多様体であり，こうした一般化された Jacobi 多様体を暗号設計の対象とする考えは，本研究が多分最初であり，代数曲線型公開鍵暗号設計に関しての可能性が広がることを期待するものである。

2　特異曲線を考える根拠

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，その書き表し方も，出来るだけ単純化する必要がある。楕円曲線は種数 1 の非特異代数曲線であり，平面非特異 3 次曲線として書き表され，そしてその最大の特徴の一つが射影平面において一つの方程式で与えられることであり，それが演算アルゴリズムを効率的に行える最大の根拠となっている。一般種数の非特異代数曲線の場合，その具体的表現に関して，次の結果がある。

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。楕円曲線のように，射影平面の中に埋め込もうとすると，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 は 2 本の枝が異なる方向から交わる特異点をいう。

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。

こうした曲線の種数は次の式で与えられる。

定理３ $\mathbb{P}^2_k \supset C$ 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，種数は

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

である。

次に，特異曲線の Jacobi 多様体（**一般化された Jacobi 多様体**という）の記述について説明を行う。

3　特異曲線の Jacobi 多様体

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 U 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 4 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 $C\subset\mathbb{P}_k^2$ 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。

例 1 $\mathbb{P}_k^2\supset C:\ Y^2Z=X^3$ で定義される 3 次 cuspidal curve とする。このとき $g(C)=0$ となり $\widetilde{C}=\mathbb{P}_k^1$ であり，上記完全系列より

$$0\longrightarrow k\longrightarrow\mathrm{Pic}_k(C)\longrightarrow\mathbb{Z}\longrightarrow 0$$

を得る。

例 2 $\mathbb{P}_k^2\supset C:\ XYZ=X^3$ で定義される 3 次 nodal curve とする。このとき $g(C)=0$ となり $\widetilde{C}=\mathbb{P}_k^1$ であり，上記完全系列より

$$0\longrightarrow k^*\longrightarrow\mathrm{Pic}_k(C)\longrightarrow\mathbb{Z}\longrightarrow 0$$

を得る。

4 Cartier Divisor の表現

以下，$\mathbb{P}_k^2\supset C$ を, 特異点として r 個の node $P_1,P_2,\dots,P_r$ 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 $(i=1,\dots,r)$ 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。

各特異点 $P_i\in C$ の十分小さい affine 近傍 U_i と，$C\setminus\{P_1,P_2,\dots,P_r\}\supset U_0$ となる affine open subset をとり，C の affine 開被覆 $C=\cup_{i=0}^r U_i$ をとる。このとき，C 上の Cartier divisor D は

$$D=\{(U_i,f_i)_{i=1,\dots,r}\mid f_j/f_i\in\mathcal{O}_C(U_i\cap U_j)\}$$

と表される。Cartier divisor class $[D]\in\mathrm{CaCl}_k(C)$ を考えるとき，この class の代表元として

$$f_i(P_i)\neq 0,\infty\quad(i=1,\dots,r)$$

となるように出来る。このとき，D に対応する Weil divisor $\overline{D}$ を考えることが出来，support を非特異点にもつ：

$$\overline{D}=\sum_{P\in C\setminus\{P_1,\dots,P_r\}}v_P(f_{i_P})P,$$

但し，i_P は P を含む一つの affine open set U_i の i を表す。こうした操作は，逆に与えられた非特異点を support にもつ divisor

$$\overline{D}=\sum_{j=1}^{g(C)}m_jQ_j-g(C)P_\infty$$

から出発して，各 Q_j の座標を具体的に与えて D の記述を得ることが出来る。

一方，Cartier divisor $D = \{(U_i, f_i)_{i=1,\ldots,r} \mid f_j/f_i \in \mathcal{O}_C^*(U_i \cap U_j)\}$ に対応する invertible sheaf $\mathcal{O}_C(D)$ は

$$\mathcal{O}_{U_i}(D) = \mathcal{O}_{U_i} \cdot \frac{1}{f_i} \quad (i = 0, \ldots, r)$$

で与えられ，もう一つの Cartier divisor

$$D' = \{(U_i, f_i')_{i=1,\ldots,r} \mid f_j'/f_i' \in \mathcal{O}_C(U_i \cap U_j)\}$$

に対して，その加法は

$$D + D' = \{(U_i, f_i f_i')_{i=1,\ldots,r}\}$$

あるいは

$$\mathcal{O}_{U_i}(D + D') = \mathcal{O}_{U_i} \cdot \frac{1}{f_i f_i'} \quad (i = 0, \ldots, r)$$

で与えられ, また，べき乗は

$$\mathcal{O}_{U_i}(mD) = \mathcal{O}_{U_i} \cdot \frac{1}{f_i^m} \quad (i = 0, \ldots, r)$$

で与えられる。

尚，この研究は開発途上であり，課題として次のことを克服していかなければならない。

1) normalization $\pi : \widetilde{C} \to C$ を介した $\mathrm{Pic}_k(C) \to \mathrm{Pic}_k(\widetilde{C})$ の差 $(k^*)^r$ の標準化。
2) Cartier divisor $D = \{(U_i, f_i)_{i=1,\ldots,r} \mid f_j/f_i \in \mathcal{O}_C^*(U_i \cap U_j)\}$ の，非特異点に support をもつ Weil divisor との関連で，正規化された表現（例えば，hyperelliptic curve における divisor の Mumford 表現）の模索。
3) 上記 divisor の正規化の実用的なアルゴリズムの開発（例えば，hyperelliptic curve における Mumford 表現では，中国人剰余定理を用いた具体的アルゴイズムがある）。
4) 具体的な曲線を用いた，実装実験。

参 考 文 献

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

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

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

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

[5] 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