代数曲線暗号

松尾 和人 * 有田 正剛 ** 趙 晋輝 ***
* 中央大学研究開発機構 ** 日本電気
*** 中央大学理工学部電気電子情報通信工学科

A Survey on Algebraic Curve Cryptosystems

Kazuto Matsuo* Seigo Arita** Jinhui Chao***
*, *** Chuo University ** NEC

Abstract. This paper is a survey on the state-of-the-art of cryptosystems based on the discrete logarithm over algebraic curves on finite fields. The issue on security of these systems against various attacks are firstly considered. Then fast addition algorithms and efficient point counting algorithms for Jacobian varieties of algebraic curves are discussed. These algorithms, although are necessary for construction of algebraic curve cryptosystems, had not been available until very recently. This paper also surveys the known results and the recent advances of related number theoretic algorithms and new developments in construction of algebraic curve cryptosystems.

1 緒言

有限体 K 上の (平面) 代数曲線 C の Jacobi 多様体 J_C の K-有理点のなす集合 $J_C(K)$ は有限 Abel 群を成し，その上で離散対数問題を定義可能である．(以降では $J_C(K)$ を K 上の Jacobi 群と呼ぶ．) 注意深く選択された C 上の離散対数問題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と比較しより解読が困難であり，この離散対数問題を安全性の根拠におくことで，より安全性の高い公開鍵暗号系を構成可能である．それ故，C として楕円曲線を採った楕円曲線暗号は，最近では公開鍵暗号の主流となり多くの実用化がなされてきた．一方，楕円曲線と比較しより一般的な代数曲線を用いた暗号系についても多くの研究が行なわれてきたがごく最近まで実用には供されてこなかった．

代数曲線上の離散対数問題に基づく暗号系の構成には，大別して 2 種類のアルゴリズム，即ち:

- Jacobi 群における高速加算アルゴリズム
- 安全な曲線の構成アルゴリズム

が必要である．楕円曲線に対しては，これらに関し多くの実用的なアルゴリズムが得られている．しかし，超楕円曲線や C_{ab} 曲線等，より一般的な代数曲線に対しては有効なアルゴリズムが知られていなかった．しかし，最近のめざましい研究の結果，高速加算，安全な曲線の構成共に幾つかの効率的なアルゴリズムが提案され，これらにより超楕円曲線や C_{ab} 曲線を用いた暗号系が実用に供されつつある．そこで本論文では，超楕円曲線や C_{ab} 曲線等の暗号応用に必要なアルゴリズムの最近の研究成果，研究動向を紹介する．

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．

本論文では，まず 2 章で代数曲線上の離散対数を定義すると共にその攻撃法をまとめる．そして 3 章で超楕円曲線，4 章でより一般的な代数曲線に対する，高速加算アルゴリズム，安全な曲線の構成アルゴリズムのこれまでの研究成果と研究動向を紹介する．

2　代数曲線上の離散対数問題とその攻撃法

本章では，代数曲線上の離散対数問題を与え，その攻撃方法をまとめる．

$K = \mathbb{F}_q$ を標数 p，位数 q の有限体とする．C を K 上の代数曲線で，Jacobi 群 $J_C(K)$ の位数 N の元 P および，P が生成する巡回群の要素 Q が与えられているとする．

代数曲線上の離散対数問題 与えられた K, C, P, N および Q に対して，$Q = nP$ となる整数 $n \in [0, N-1]$ を求めよ．

$J_C(K)$ における効率的な加算アルゴリズムが与えられているとき，代数曲線上の離散対数問題を用いて離散対数型暗号を構成可能である．

代数曲線上の離散対数問題に対しても，Pohlig-Hellman 法，baby step giant step 法，Pollard rho 法等の一般的な攻撃法が成立することはいうまでもない．したがって，N はほぼ素数であること (大きな素数と小さな整数 (1,2,4 等) の積) が必要であり，また代数曲線上の離散対数問題は高々$O(N^{1/2})$ の計算量で解かれる．

代数曲線上の離散対数問題固有の攻撃方法としては，楕円曲線暗号に対する MOV 攻撃の一般化である Tate pairing 法，楕円曲線暗号に対する SSSA 法の一般化である Rück 法および Adleman-DeMarrais-Huang 法とその Gaudry variant が知られている．

Tate pairing 法 [13]

標数 p と素な整数 m に対し，Jacobi 群の m-torsion element のなす群 $J_C[m](K)$ は，Tate-Lichtenbaum pairing を用いて，K に 1 の m 乗恨を添加した体の乗法群に埋め込まれ，有限体の乗法群における離散対数問題に帰着する．したがって，代数曲線上の離散対数問題が安全であるには，楕円曲線暗号の場合と同様に，体 K の小さな拡大体 (拡大次数が数十程度) には 1 の N 乗根が含まれないことが必要である．

Rück 法 [49]

因子 D と線形同値な Jacobi 群の p-torsion element $j = [D]$ に対して，pD は主因子 (f) となり，df/f は C 上の正則微分形式となる．この対応 $j \mapsto df/f$ によって，$J_C[p](K)$ は C 上の正則微分形式の空間 $\Omega^1(C)$ に埋め込まれる．正則微分形式 df/f はその局所パラメータによる展開 $\sum_{i=0}^{\infty} a_i t^i$ の最初の $2g-1$ 個の項 $(a_0, a_1, \cdots, a_{2g-2})$ で決まるので (g は種数)，結局，$J_C[p](K)$ は K^{2g-1} に埋め込まれ，p-torsion element に関する離散対数問題は，有限体の加法群における離散対数問題に帰着し，trivial となる．

Adleman-DeMarrais-Huang 法

K 上の，種数 g の超楕円曲線 $Y^2 = F(X)$ に対して，$a(X) + b(X)Y$ という形の関数の主因子に表れる因子を factor base として指数計算法を用いれば，$\log q \leq (2g+1)^{.98}$ という制約のもとで，g を無限大にとばすと，その離散対数問題が subexponential なアルゴリズムで解かれる [1]．同様な結果は superellitpic 曲線に対しても予想されている [15].

Gaudry variant

Gaudry variant[17] は，指数計算法における factor base の発想を rho 法に取り入れたもので，種数 g の超楕円曲線上の離散対数問題を $O(g^2 g! q \log^2 q + g^3 q^2 \log^2 q)$ の計算量で解く．これにより，種数が 4 以上の超楕円曲線を暗号に用いることは原則としてできない (ただし，もちろん，有限体のサイズを十分な大きさにとれば用いることはできる).

Gaudry variant では，factor base として曲線上の有理点の集合 (要素数は $O(q)$) が用いられる．rho 法では群上の random walk が過去の軌跡に衝突するのをまつが，Gaudry variant では，過去の軌跡との「ニアミス」をまつ．ニアミスとは差が smooth な元であることである．このようなニアミスが factor base の要素数以上発生すると，離散対数問題は $O(q)$ 元のスパースな連立一次方程式を解く問題に帰着される．

Gaudry variant を，C_{ab} 曲線など，Jacobi 群 $J_C(K)$ における効率的な加算アルゴリズムが与えれている曲線に一般化することは容易である [4].

また，Gaudry variant は Frey[14] によって提唱された Weil descent attack を実現可能にした．すなわち，与えられた代数曲線 C に対して，Weil descent を用いて，定義体のサイズを落し，種数を大きくした代数曲線 C' を構成し，C 上の離散対数問題を C' 上のそれに帰着させ，Gaudry variant を適用するものである．Weil descent attack は楕円曲線のみならず [21], 超楕円曲線に対しても適用されている [16].

ここで紹介した攻撃法に対し耐性があり且つ N が 160bit 以上の素数を因子としてもつ代数曲線上の離散対数問題に基づく暗号系は現在のところ安全であると考えられている．

3　超楕円曲線を用いた離散対数型暗号

本章では，超楕円曲線を用いた離散対数型暗号に関するアルゴリズムについて紹介する．

議論の簡略化のため，本章では有限体 $K = \mathbb{F}_q$ の標数 $p \neq 2$ とする．

K 上の種数 g の超楕円曲線 C は，$\deg F = 2g+1, \mathrm{disc}\,(F) \neq 0$ である $F \in K[X]$ により

$$C : Y^2 = F(X) \tag{3.1}$$

と定義される．$y^2 = F(x)$ を満足する $P = (x, y) \in \bar{K}^2$ と，唯一の無限遠点 P_∞ を併せて C 上の点と呼ぶ．点 $P = (x, y)$ に対して $\bar{P} = (x, -y)$，また $\bar{P}_\infty = P_\infty$ と定義する．C の因子 D を C 上の点 P_i の有限形式和

$$D = \sum_{P_i \in C} \mathrm{ord}_{P_i}(D) P_i, \mathrm{ord}_{P_i}(D) \in \mathbb{Z} \tag{3.2}$$

で定義する．(3.2)で与えられた因子 D の次数を $\deg D = \sum_i \mathrm{ord}_{P_i}(D)$ で定義する．次数 0 の因子の集合を $\mathfrak{D}^0$ と書く．また，主因子の集合を $\mathfrak{D}^l$ と書く．C の Jacobi 多様体 J_C は

$$(3.3)\ J_C = \mathfrak{D}^0/\mathfrak{D}^l$$

と定義される．

C の点の間の写像 $(x, y) \mapsto (x^{q^k}, y^{q^k})$ の J_C への延長 π_{q^k} は J_C の自己準同型になる．π_{q^k} を J_C の q^k 乗 Frobenius 写像と呼ぶ．$\mathbb{F}_{q^k}$ 上の Jacobi 群 $J_C(\mathbb{F}_{q^k})$ は π_{q^k} で固定される J_C の元全体である．

J_C の元を以下の形式の因子 D で表現可能である．

$$(3.4)\ D = \sum_i m_i P_i - \left(\sum_i m_i\right) P_\infty,\ P_i = (x_i, y_i),\ m_i \geq 0$$

但し，$i \neq j$ に対し $P_i \neq \bar{P}_j$ とする．式 (3.4) の形式の因子を semi-reduced divisor といい，$\sum_i m_i$ を D の weight と呼ぶ．Weight が種数以下の semi-reduced divisor を特に reduced divisor と呼ぶ．Reduced divisor により J_C の元は一意的に表現される．

式 (3.4) で与えられた semi-reduced divisor を多項式 $U, V \in \overline{\mathbb{F}}_q[X]$ を用いて $D = (U, V)$ と表現可能である．ここで，$U = \prod (X - x_i)^{m_i}$ であり，V は $F - V^2 \equiv 0 \bmod U, \deg V < \deg U$ を満足する唯一の多項式である．Semi-reduced divisor の，この表現を Mumford 表現と呼ぶ．$D = (U, V)$ に対し，$U, V \in \mathbb{F}_{q^k}[X]$ と $D \in J_C(\mathbb{F}_{q^k})$ は同値である．超楕円曲線の暗号応用では，Jacobi 群の元の表現に殆どの場合 reduced divisor の Mumford 表現が利用される．

3.1 Jacobi 群における加算

超楕円曲線を用いて効率的な暗号系を構成するために，$J_C(K)$ 上の高速加算アルゴリズムが必要不可欠である．幸い C が超楕円曲線のときは，Gauss の整係数虚 2 次形式に対する composition と reduction アルゴリズムを，Mumford 表現を利用した多項式の 2 次形式に自然に拡張し，加算アルゴリズムが得られる [6]．通常この種の加算アルゴリズムを Cantor アルゴリズムと呼ぶ．Algorithm 1 に Cantor アルゴリズムの概略を示す．

Algorithm 1 Cantor アルゴリズム

入力: Reduced divisors $D_1 = (U_1, V_1), D_2 = (U_2, V_2) \in J_C(K)$
出力: Reduced divisor $D_3 = (U_3, V_3) = D_1 + D_2$

1: $W \leftarrow \gcd(U_1, U_2, V_1 + V_2) = S_1 U_1 + S_2 U_2 + S_3(V_1 + V_2)$ `/*Composition*/`
2: $U_3 \leftarrow U_1 U_2 / W^2$
3: $V_3 \leftarrow (S_1 U_1 V_2 + S_2 U_2 V_1 + S_3(V_1 V_2 + F)) W^{-1} \bmod U_3$
4: **while** $\deg U_3 > g$ **do** `/*Reduction*/`
5: $\quad U_3 \leftarrow (F - V_3^2)/U_3$
6: $\quad V_3 \leftarrow -V_3 \bmod U_3$
7: **end while**

$J_C(K)$ 上の加算に Cantor アルゴリズムを用いることで，実用的な速度の暗号系を構成可能である．また，Cantor アルゴリズムに対し多くの改良 [47, 46, 27] が行なわれ，より高速

な暗号系が構成可能になった．しかし，Cantor アルゴリズムを用いた超楕円曲線暗号は安全性が同一の楕円曲線暗号と比較し数倍以上低速であり，より高速な加算アルゴリズムが望まれていた．

最近，$g = 2$ の超楕円曲線に対し，Harley によって Cantor アルゴリズムとは計算方針の異なるアルゴリズム (Harley アルゴリズム) が与えられた [18, 23]．Harley アルゴリズムでは種数を固定し，また入力因子を詳細に分類し各々に対して最適化された計算手順を用いることで，高速化が図られている．更に，これらの制限により多項式に対する中国人剰余定理，Newton 反復，Karatsuba 乗算をアルゴリズム中に陽に記述可能となり，定義体上の演算を用いた記述による高速アルゴリズムが得られた。Algorithm 2, 3 に最も良く起こる入力ケースに対する Harley アルゴリズムの概略を示す．

Algorithm 2 Harley 加算アルゴリズム

入力: Reduced divisors $D_1 = (U_1, V_1), D_2 = (U_2, V_2) \in J_C(K)$, $\deg U_i = 2, \gcd(U_1, U_2) = 1$
出力: Reduced divisor $D_3 = (U_3, V_3) = D_1 + D_2$

1: $U_3 \leftarrow U_1 U_2$ `/*Composition*/`
2: $S \leftarrow (V_2 - V_1) U_1^{-1} \bmod U_2$
3: $V_3 \leftarrow S U_1 + V_1$
4: $U_3 \leftarrow (F - V_3^2)/U_3$ `/*Reduction*/`
5: $V_3 \leftarrow -V_3 \bmod U_3$

Algorithm 3 Harley 2 倍算アルゴリズム

入力: Reduced divisor $D_1 = (U_1, V_1) \in J_C(K)$, $\deg U_1 = 2, \gcd(U_1, V_1) = 1$
出力: Reduced divisor $D_3 = (U_3, V_3) = 2D_1$

1: $U_3 \leftarrow U_1^2$ `/*Composition*/`
2: $S \leftarrow ((F - V_1^2)/U_1) V_1^{-1} \bmod U_1$
3: $V_3 \leftarrow S U_1 + V_1$
4: $U_3 \leftarrow (F - V_3^2)/U_3$ `/*Reduction*/`
5: $V_3 \leftarrow -V_3 \bmod U_3$

Harley アルゴリズムを用いた超楕円曲線暗号は，安全性が同一の楕円曲線暗号と同程度の速度であることが知られている [38]．更に，幾つかの改良 [38, 44, 54] の結果，現在では加算を K 上の逆元計算 1 回と乗算 25 回で，2 倍算を逆元計算 1 回と乗算 26 回で実現可能である [53]．

上記アルゴリズムはいずれも $p = 2$ の場合には対応していないが，この場合に対する Cantor アルゴリズムが [31] に，Harley アルゴリズムが [53] に示された．また，[34] は Harley アルゴリズムの $g = 3$ への拡張を示した．

3.2 安全な超楕円曲線の構成

2 章で紹介した攻撃に対し耐性があり，N が 160bit 以上の素数を因子としてもつ超楕円曲線を「安全な超楕円曲線」と呼ぶ．安全な超楕円曲線を構成する上で最も重要且つ困難な課題は，N が 160bit 以上の素数を因子としてもつ曲線の構成である．超楕円曲線は楕円曲線と

比較しより複雑な構造を持ち，得られている数学的知見が少ないこともあり，安全な超楕円曲線の実用的な構成アルゴリズムは知られてこなかった．しかし，ここ数年多くの研究が行なわれ実用的なアルゴリズムが幾つか提案されるようになった．

安全な超楕円曲線の構成アルゴリズムは，楕円曲線に対するアルゴリズムの拡張として大きく分けて 3 通りの方法が考えられる．即ち，

- ランダム曲線を用いる方法
- CM 曲線を用いる方法
- Koblitz の方法

である．これらはいずれも与えられた超楕円曲線C/Kに対し，K 上の Jacobi 群の位数 $\#J_C(K)$ または K の拡大 $\mathbb{F}_{q^k}$ 上の Jacobi 群の位数 $\#J_C(\mathbb{F}_{q^k})$ を計算するアルゴリズムである．

J_C の q^k 乗 Frobenius 写像の特性多項式は $2g$ 次の整係数多項式

$$\chi_{q^k}(X) = X^{2g} + \sum_{i=1}^{g} (-1)^i s_i X^{2g-i} + \sum_{i=1}^{g-1} (-1)^i s_i q^{k(g-i)} X^i + q^{kg} \tag{3.5}$$

として与えられるが，$\#J_C(\mathbb{F}_{q^k})$ は $\chi_{q^k}(X)$ を用いて

$$\#J_C(\mathbb{F}_{q^k}) = \chi_{q^k}(1) \tag{3.6}$$

と計算される．これまでに提案されたアルゴリズムは，いずれも $\chi_{q^k}(X)$ (またはその根) を計算するものである．

ランダム曲線を用いる方法

与えられた超楕円曲線 C/K に対し，$\#J_C(K)$ を計算するアルゴリズムが在れば，これをランダムに与えられた超楕円曲線に対し繰り返し用いることで安全な曲線を得ることが可能である．

与えられた曲線の Jacobi 群の位数を計算するアルゴリズムは，初めに楕円曲線に対し Schoof によって与えられ，その後，これの超楕円曲線に対する拡張が行なわれた [48, 28, 2, 25]．これらの拡張アルゴリズムはいずれも $\log q$ の多項式オーダーのアルゴリズムではあるものの，実用的なアルゴリズムとはいいがたく，その実装は行なわれて来なかった．

最近，Gaudry と Harley により種数 2 の超楕円曲線の Jacobi 群の位数計算アルゴリズム (Gaudry-Harley アルゴリズム) が実装された [18].

Gaudry-Harley アルゴリズムでは J_C の l-torsion element (l は p と異なる素数) を得るために Cantor の division polynomial [7] を用いる．Cantor の division polynomial は weight が 1 の因子に対するものだが，Gaudry-Harley アルゴリズムでは resultant 計算による変数消去を用いて，これから一般の l-torsion element に関する division polynomial を計算する．そして，多項式の因数分解アルゴリズムにより K の拡大体上の l-torsion element の Mumford 表現を実際に計算する．従って，l-torsion element の存在する拡大次数によってアルゴリズムの動作速度は大きく変動する．また，division polynomial の次数は $O(l^4)$ であり，現状の計算機環境では $l = 13$ 程度の計算が限界である．$D \in J_C[l]$ が求まった後には，(3.5) から $[\pi_q^4 - s_1\pi_q^3 + s_2\pi_q^2 - s_1 q\pi_q + q^2]D = 0$ を満足する $0 \le s_i < l$ を実際の群演算によって発見し，

得られた s_i を (3.6) に代入することで $\#J_C(K) \bmod l$ を得る．この操作を十分な数の l に対して行なえば中国人剰余定理により $\#J_C(K)$ が得られる．

しかし，現状では十分な l が得られないため，更に Cartier-Manin operator [36] を用いて $\#J_C(K) \bmod p$ を計算し，中国人剰余定理により得られた $\#J_C(K) \bmod m$ (m は l 達と p の積) を用いて，最終的に Pollard lambda 法を用いて $\#J_C(K)$ を得る．Gaudry-Harley アルゴリズムにおける lambda 法の計算量は $O(q^{3/4}/\sqrt{m})$ である．Gaudry と Harley は，このアルゴリズムにより 128bit の位数計算を実現した．しかし，実際の計算は lambda 法によるところが大きかった．

その後，計算量が $O(q^{3/4}/m)$ の baby step giant step 法が提案され，lambda 法の代りにこのアルゴリズムを用いることで 160bit の位数計算が実現された [41]．しかし，これらは拡大体上の曲線に対する位数計算の結果であり，素体上の曲線に対しては今のところ暗号に利用可能なサイズの位数計算は実現されていない．また，種数 3 以上の超楕円曲線に対する実装も知られていない．特に，Gaudry-Harley アルゴリズムで用いられた一般の l-torsion element を得る手法の，種数 3 以上の曲線への拡張は困難な課題である．

以上では定義体 K の標数 p に係わらず有効なアルゴリズムを紹介した．これらとは別に，p が十分に小さいとき有効な位数計算アルゴリズムが知られている．この種のアルゴリズムは初めに楕円曲線に対し佐藤によって与えられた．超楕円曲線に対しては，canonical lifting を用いる AGM 法 [24, 19] と p 進コホモロジーを用いる Kedlaya アルゴリズム等 [30, 20, 35, 11] が知られており，いずれも暗号利用に十分なサイズの位数を高速に計算可能である．

CM 曲線を用いる方法

Jacobi 多様体が虚数乗法を持つ代数体上の超楕円曲線（以降 CM 超楕円曲線と呼ぶ.）を用いて安全な位数の有限体上の超楕円曲線を得る方法が知られている．この方法は Abel 多様体の虚数乗法理論 [50] を基礎とする方法であり，

- 代数体上の CM 超楕円曲線の構成
- CM 超楕円曲線の有限体上での位数計算

を必要とする．

代数体上の CM 超楕円曲線の構成は，テータ定数 [33] を近似計算により求め，これから曲線の不変量を求めることで行なわれる．種数 2 の超楕円曲線に対しては井草不変量 [26] が知られており，これを用いることで代数体上の CM 超楕円曲線を効率的に計算可能である [52, 56, 45, 58, 55]．特に [58, 55] では類数が 10 を超える曲線を効率的に計算可能な計算アルゴリズムを与えている．また，これらとは別に有限体上の超楕円曲線から CM 超楕円曲線を得る試みがなされている [9, 40]．しかし，現状ではいずれのアルゴリズムも，楕円曲線に対するアルゴリズムと比較すると計算可能な類数は小さい．上記は全て曲線の井草不変量を求めるアルゴリズムであり，実際の CM 超楕円曲線を求めるには井草不変量から曲線の定義式を導くアルゴリズムが必要となる．これに対する効率的なアルゴリズムは幾つか知られている [42, 58, 39].

種数 3 の超楕円曲線に対しては，塩田不変量 [51] を用いた構成の試み [59] がなされているが，CM 体 (の order) に対応する Abel 多様体が一般には超楕円曲線の Jacobi 多様体にならない等，多くの課題が残されている．

上記アルゴリズムによって得られた CM 超楕円曲線の有限体上への reduction の Jacobi 群の位数計算は高速アルゴリズム [8, 10, 58] が知られており，CM 超楕円曲線から効率的に安全な超楕円曲線を得ることが可能である．しかし，これらはいずれも素体上の曲線に対するアルゴリズムであり，また有限体のサイズを指定するものであって，与えられた有限体に対し位数計算を行なうものではない等，解決すべき課題は多い．

Koblitz の方法とその改良

Koblitz [31] は，χ_q から χ_{q^k} ひいては $\#J_C(\mathbb{F}_{q^k})$ が簡単に計算可能なことを利用し，$J_C(\mathbb{F}_{q^k})$ 上で暗号系を構成した．[31] に示されたアルゴリズムは χ_q を求めるために，C の $\mathbb{F}_{q^g}$-有理点数を数え挙げる必要が有り，この計算量は $O(q^g)$ であった．従って，小さな q に対してのみ有効であり，利用可能な曲線のクラスは小さかった．しかし，最近，χ_q を求めるために Elkies [12] の方法を利用した高速アルゴリズム [29] が提案され十分な数の曲線を利用可能になった．

4 より一般的な代数曲線を用いた離散対数型暗号

ここでは，楕円，超楕円曲線以外のより一般的な代数曲線を用いた離散対数型暗号の試みについて紹介する．

3 章で述べたように，代数曲線の Jacobi 群を用いて離散対数型暗号を構成するには，Jacobi 群における加算を効率的に実行すること，および Jacobi 群の位数を効率的に計算することが必要である．楕円，超楕円曲線以外で，これらの問題に対して幾らかの結果が知られている曲線として，superelliptic 曲線 [15] および C_{ab} 曲線 [43, 37] がある．

Superelliptic 曲線とは以下の定義式をもつ非特異アフィン曲線である．

$$Y^n = a_\delta X^\delta + a_{\delta-1} X^{\delta-1} + \cdots + a_0.$$

ここで，n と δ は互いに素な自然数であり，n は定義体の標数とは素であるとする．C_{ab} 曲線とは以下の定義式をもつ非特異アフィン曲線である．

$$F(X,Y) = \sum_{0\le i\le b, 0\le j\le a, ai+bj\le ab} \alpha_{i,j} X^i Y^j = 0 \tag{4.1}$$

ここで，a と b は互いに素な自然数である．明らかに，superelliptic 曲線は C_{ab} 曲線のサブセットである．

4.1 Jacobi 群における加算

Superelliptic 曲線や C_{ab} 曲線においては，無限遠点が一点しかないことから，Jacobi 群と座標環のイデアル類群が自然に同型となる．そのため，Jacobi 群における加算をイデアル類群における乗算として実行できる．イデアル類の代表系としては，同じイデアル類に属するイデアルのうち，次数が最小のイデアルを取ることができ，Jacobi 群の加算は以下のようにして実行される [3].

Algorithm 4 イデアル表現による Jacobi 群加算アルゴリズム

入力: 座標環 A_K のイデアル I_1 と I_2

出力: イデアル積 $I_1 \cdot I_2$ に同値なイデアルで次数が最小のイデアル I_3

1: $I \leftarrow I_1 \cdot I_2$
2: $f \leftarrow$ 極位数が最小の $f(\neq 0) \in I$
3: $J \leftarrow (f) : I$
4: $g \leftarrow$ 極位数が最小の $g(\neq 0) \in J$
5: $I_3 \leftarrow (g) : J$

ここで，極位数とは唯一の無限遠点における極位数を指す．また，$(f) : I = \{r \in A_K \mid rI \subset (f)\}$ はイデアル商である．

上記のアルゴリズム (或はそのバリエーション) を実現するには，イデアルを何らかの方法で表現しなければならない．Superelliptic 曲線に対して，[15] では，数体におけるイデアル類群の演算方法を流用し，イデアルを $K[x]$-加群としての Hermite 標準形によって表現している．C_{ab} 曲線に対しては，[3] では，極位数から定まる位数つき単項式順序に関するグレブナ基底を用いている．また，[22] では，[15] の手法を C_{ab} 曲線に拡張している．

いずれの場合も効率上重要なのは，与えられたイデアルに対して，極位数が最小の多項式を求めることである．そのために，[15, 22] では LLL アルゴリズムを，[3] では Buchberger アルゴリズムを用いているが，これらはいずれも「万能」アルゴリズムに頼ったものであり，より効率的な手法が待たれるところである．

4.2 Jacobi 群の位数計算

任意の superelliptic 曲線や C_{ab} 曲線に対して，その Jacobi 群の位数計算を効率的に実行するアルゴリズムは知られていない．いくつかの特殊なケースについて効率的な計算方法があるという状態である．

Jacobi 和を用いる方法

超楕円曲線の場合と同様に [32]，異なる素数 a, b に対して

$$\alpha Y^a + \beta X^b + 1 = 0$$

という形の式で定義される C_{ab} (superelliptic) 曲線はその合同ゼータ関数 (の分子) が Jacobi 和によって表示される [57] ため，容易に Jacobi 群の位数を計算することができる [4].

モジュラー曲線を用いる方法

モジュラー曲線の商曲線として表れる C_{ab} 曲線に対しては，Eichler-Shimura relation を用いて，一般のケースよりは，効率的に Jacobi 群の位数を計算することができる [5].

Kedlya の方法の拡張

[30] は，標数 p が小さいとき，1 次の de Ram コホモロジー群への Frobenius 準同型の作用を計算することで，超楕円曲線にたいして Jacobi 群の位数計算が可能であることを示したが，この方法は [20] によって，superelliptic 曲線に，直接的な形で，拡張されている．

参考文献

[1] L. M. Adleman, J. DeMarrais, and M. D. Huang, A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobian of large genus hyperelliptic curves over finite fields, ANTS-I, Springer-Verlag LNCS 877, 1994, 28–40.

[2] L. M. Adleman and M. D. Huang, Counting rational points on curves and Abelian varieties over finite fields, ANTS-II, Springer-Verlag LNCS 1122, 1996, 1–16.

[3] 有田正剛, C_{ab} 曲線のヤコビアン群加算アルゴリズムとその離散対数型暗号への応用, 電子情報通信学会論文誌 A, J82-A (1999),1291–1299.

[4] S. Arita, Gaudry's variant against C_{ab} curves, IEICE TRANS. FOUND., E83-A (2000), 1809-1814.

[5] S. Arita, Construction of Secure C_{ab} Curves Using Modular Curves , IEICE TRANS. FOUND., E84-A (2001), 2930-2938.

[6] D. G. Cantor, Computing in the Jacobian of hyperelliptic curve, Math. Comp., 48 (1987), 95–101.

[7] D. G. Cantor, On the analogue of the division polynomials for hyperelliptic curves, Journal für die reine und angewandte Mathematik, 447 (1994), 91–145.

[8] J. Chao, N. Matsuda, and S. Tsujii, Efficient construction of secure hyperelliptic discrete logarithm problems, ICICS'97, Springer-Verlag LNCS 1334, 1997, 292–301.

[9] J. Chao, K. Matsuo, H. Kawashiro, and S. Tsujii, Construction of hyperelliptic curves with CM and its application to cryptosystems, ASIACRYPT2000, Springer-Verlag LNCS 1976, 2000, 259–273.

[10] J. Chao, K. Matsuo, and S. Tsujii, Fast construction of secure discrete logarithm problems over Jacobian varieties, Information Security for Global Information Infrastructures, Kluwer Academic Pub., 2000, 241–250.

[11] J. Denef and F. Vercauteren, An extension of Kedlaya's algorithm to Artin–Schreier curves in characteristic 2, ANTS-V, Springer-Verlag LNCS 2369, 2002, 308–323.

[12] N. D. Elkies, Elliptic and modular curves over finite fields and related computational issues, Computational perspectives on number theory, AMS, 1995, 21–76.

[13] G.Frey and H.-G.Rück, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves, Math. Comp., 62 (1994), 865-874.

[14] G.Frey, How to disguise an elliptic curve, Talk at Waterloo workshop on the ECDLP, `http://cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html`, 1998.

[15] S.D.Galbraith, S.Paulus, and N.P.Smart, Arithmetic on Superelliptic Curves, J. Cryptology, 12 (1999), 193-196.

[16] S.D.Galbraith, Weil Descent of Jacobians, preprint at the University of Bristol, 2000.

[17] P.Gaudry, An algorithm for solving the discrete logarithm problem on hyperelliptic curves, EUROCRYPT 2000, Springer-Verlag LNCS 1807, 2000, 19-34.

[18] P. Gaudry and R. Harley, Counting points on hyperelliptic curves over finite fields, ANTS-IV, Springer-Verlag LNCS 1838, 2000, 297–312.

[19] P. Gaudry, Algorithms for counting points on curves, Talk at ECC 2001 Waterloo, `http://www.cacr.math.uwaterloo.ca/conferences/2001/ecc/gaudry.ps`, 2001.

[20] P. Gaudry and N. Gürel, An extension of Kedlaya's point–counting algorithm to superelliptic curves, ASIACRYPT2001, Springer-Verlag LNCS 2248, 2001, 480–494.

[21] P.Gaudry, F.Hess, and N.P.Smart, Constructive and destructive facets of Weil descent on elliptic curves, to apper in J. Cryptology.

[22] R. Harasawa, J. Suzuki, A Fast Jacobian Group Arithmetic Scheme for Algebraic Curve Cryptography, IEICE TRANS. FOUND., E84-A (2001), 130-139.

[23] R. Harley, adding.text, `http://cristal.inria.fr/~harley/hyper/`, 2000.

[24] R. Harley, Counting points with the arithmetic–geometric mean, Rump talk at EUROCRYPT 2001, 2001, (joint work with J.-F. Mestre and P. Gaudry)

[25] M. D. Huang and D. Ierardi, Counting rational point on curves over finite fields, J. Symbolic Computation, 25 (1998), 1–21.

[26] J. Igusa, Arithmetic variety of moduli for genus two, Ann. of Math., 72 (1960), 612–649.

[27] M.J. Jacobson, Jr. and A.J. van der Poorten, Computational aspects of NUCOMP, ANTS-V, Springer-Verlag LNCS 2369, 2002, 120–133.

[28] W. Kampkötter, Explizite Gleichungen für Jacobische Varietäten hyperelliptischer Kurven, PhD thesis, GH Essen, 1991.

[29] N. Kanayama, K. Nagao, and S. Uchiyama, Generating hyperelliptic curves of genus 2 suitable for cryptography, Proc. of SCI 2002, 2002.

[30] K. S. Kedlaya, Counting points on hyperelliptic curves using Monsky–Washinitzer cohomology, to appear in the Journal of the Ramanujan Mathematical Society, 2001.

[31] N. Koblitz, Hyperelliptic curve cryptosystems, J. Cryptology, 1 (1989), 139–150.

[32] N.Koblitz, A Very Easy Way to Generate Curves over Prime Fields for Hyperelliptic Cryptosytems, Rump Talk at Crypto '97, 1997.

[33] 小泉正二, テータ函数, 紀伊國屋書店, 1982.

[34] J. Kuroki, M. Gonda, K. Matsuo, J. Chao, and S. Tsujii, Fast genus three hyperelliptic curve cryptosystems, Proc. of SCIS2002, 2002, 503–507.

[35] A. Lauder and D. Wan, Computing zeta functions of Artin-Schreier curves over finite fields, LMS J. Comput. Math., 5 (2002), 33–55.

[36] J. I. Manin, The theory of commutative formal groups over fields of finite characteristic, Russian Mathematical Surveys, 18 (1963), 1–83.

[37] R. Matsumoto, The Cab Curve — a generalization of the Weierstrass form to arbitrary plane curves, `http://www.rmatsumoto.org/cab.html`.

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

[39] 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, 電子情報通信学会論文誌 A, J84-A (2001), 1045–1053.

[40] 松尾和人・趙晋輝・辻井重男, 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, 電子情報通信学会論文誌 A, J85-A (2001), 677–690.

[41] K. Matsuo, J. Chao, and S. Tsujii, An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields, ANTS-V, Springer-Verlag LNCS 2369, 2002, 461–474.

[42] J. F. Mestre, Construction de curbes de genere 2 à partir de leurs modules, Effective methods in algebraic geometry, Birkhäuser PM94, 1991, 313–334.

[43] 三浦晋示, アフィン代数曲線上の線形符号, 電子情報通信学会論文誌 A, J81-A (1998), 1398–1421.

[44] 宮本洋輔・土井洋・松尾和人・趙晋輝・辻井重男, 種数 2 の超楕円曲線上の因子類群の高速演算法に関する考察, Proc. of SCIS2002, 2002, 497–502.

[45] N. Murabayashi and A. Umegaki, Determination of all $\mathbf{Q}$–rational CM–points in the moduli space of principally polarized abelian surfaces, J. of Algebra, 235 (2001), 267–274.

[46] K. Nagao, Improving group law algorithms for Jacobians of hyperelliptic curves, ANTS-IV, Springer-Verlag LNCS 1838, 2000, 439–448.

[47] S. Paulus and A. Stein, Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves, ANTS-III, Springer-Verlag LNCS 1423, 1998 ,576–591.

[48] J. Pila, Frobenius maps of Abelian varieties and finding roots of unity in finite fields, Math. Comp., 55 (1990), 1990, 745–763.

[49] H.-G.Rück, On the discrete logarithm in the divisor class group of curves, Math. Comp., 68 (1999), 805-806.

[50] G. Shimura, Abelian varieties with complex multiplication and modular functions, Princeton U. P., 1998.

[51] T. Shioda, On the graded ring of invariants of binary octavics, Amer. J. Math., 89 (1967), 1022–1046.

[52] A. M. Spallek, Kurven vom Geshlcht 2 und ihre Anwendung in Public-Key-Kryptosystememem, PhD thesis, GH Essen, 1994.

[53] H. Sugizaki, K. Matsuo, J. Chao, and S. Tsujii, An extension of Harley addition algorithm for hyperelliptic curves over finite fields of characteristic two, IEICE Technical Report ISEC2002-9, 2002.

[54] 高橋昌史, 種数 2 の超楕円曲線における Harley アルゴリズムの改良について, Proc. of SCIS2002, 2002, 155–160.

[55] 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, 2001, 749–754.

[56] P. V. Wamelen, Example of genus two CM curves defined over the rationals, Math. Comp., 68 (1999), 307–320.

[57] A.Weil, Numbers of solutions of equations in finite fields, Bull. Amer. Math. Soc., 55 (1949), 497-508.

[58] A. Weng, Constructing hyperelliptic curves of genus 2 suitable for cryptography, to apper in Math. Comp..

[59] A. Weng, Hyperelliptic CM–curves of genus 3, Journal of the Ramanujan Mathematical Society, 16 (2001), 2001, 339–372.

松尾 和人 (非会員) 〒 112-8851 東京都文京区春日 1-13-27

1988 年中大大学院博士前期課程了．同年東洋通信機（株）入社．2001 年中大大学院博士後期課程了．工博．2002 年中大・研究開発機構助教授．電子情報通信学会会員．

有田 正剛 (非会員) 〒 216-8555 川崎市宮前区宮崎四丁目１－１

1990 年 NEC 入社．現在，インターネットシステム研究所主任．2000 年中大大学院博士後期課程了．工博．電子情報通信学会，日本数学会会員．

趙 晋輝 (非会員) 〒 112-8851 東京都文京区春日 1-13-27

1982 年中国西安電子科技大・電子卒．1988 年東工大大学院博士課程了．工博．1989 年東工大助手．1992 年中大助教授．1996 年同大教授．電子情報通信学会論文賞受賞（昭 63，平 2）．電子情報通信学会会員．