超楕円曲線暗号と位数計算

松尾 和人 †

概 要

本論文では超楕円曲線暗号の概説を行う．まず，超楕円曲線暗号に必要な数学的な知見を導入した後に，超楕円曲線の Jacobian 上で離散対数問題に基づく公開鍵暗号を構成できることを説明する．そして，安全な超楕円曲線暗号を構成するためには，その位数を知る必要があることを説明し，これまでに知られている位数計算法を紹介する．その中で，実用に近づきつつある ℓ 進位数計算法を取り上げ，そのアウトラインを述べた後に，Gaudry-Harley, Gaudry-Schost の研究結果を紹介する．最後に ℓ 進位数計算法を用いた $\mathbb{F}_p$ 上の超楕円曲線の位数計算結果をまとめるとともに，最近の話題に触れる．

1 はじめに

超楕円曲線暗号は，楕円曲線暗号 [57, 42] の自然な一般化として，Koblitz [43] により提案された．RSA 暗号の安全性の根拠となる素因数分解や DSA 署名等の安全性の根拠となる有限体上の離散対数問題と比較し，超楕円曲線暗号が安全性の根拠とする超楕円曲線上の離散対数問題は，より難しい問題であり，超楕円曲線暗号によってより安全性の高い公開鍵暗号系を実現可能である．それ故,（超楕円曲線の特殊ケースである）楕円曲線を利用した楕円曲線暗号は，最近では公開鍵暗号標準化の主流となり，AV 機器の著作権保護機構，電子マネー，ETC，SSL 等に利用されるようになった．一方，より一般的な超楕円曲線を用いた超楕円曲線暗号に対しても多くの研究が行なわれてきたが，未だ実用に至っていない．

超楕円曲線暗号の実現には安全な曲線の構成法が必要である．楕円曲線に対しては既に安全な曲線の実用的な構成法が得られており，これが楕円曲線暗号実用化の大きな要因となった．一方，一般の超楕円曲線に対しては，安全な曲線の実用的な構成法が長い間知られてこなかった．しかし，最近の研究の結果，超楕円曲線に対しても安全な曲線の実用的な構成法が実現しつつあり，これによって，超楕円曲線暗号が実用に近づいている．

そこで本論文では，超楕円曲線暗号と安全な超楕円曲線の構成法を，最近の研究成果を含めて紹介する．

2 超楕円曲線とその Jacobian

本節では，超楕円曲線とその Jacobian について，以降で必要となる最小限の知識をまとめる．

†情報セキュリティ大学院大学情報セキュリティ研究科 教授

奇標数 p の有限素体 $\mathbb{F}_p$ 上の種数 g の超楕円曲線 C は，重根を持たないモニック多項式

$$F := X^{2g+1} + f_{2g}X^{2g} + \cdots + f_1X + f_0 \in \mathbb{F}_p[X] \tag{1}$$

により

$$C : Y^2 = F \tag{2}$$

と定義される[1]．$g = 1$ のとき，C を楕円曲線という．本論文では，特に断らない限り $g \geq 2$（節以降は $g = 2$）を仮定する．

$y^2 = F(x)$ を満足する $P = (x, y) \in \overline{\mathbb{F}}_p^2$ と，唯一の無限遠点 P_∞ を併せて C 上の点と呼ぶ．ここで，$\overline{\mathbb{F}}_p$ は $\mathbb{F}_p$ の代数閉包を表す．P が C 上の点のとき，$P \in C$ と書く．点 $P = (x, y)$ に対して $\tilde{P} = (x, -y)$ とし，また $\tilde{P}_\infty = P_\infty$ と定義する．

C 上の有限個の点 P_i の型式和 $\mathcal{D}$ を下式で定義する．

$$\begin{aligned} &\mathcal{D} := \sum_i m_i P_i - \left(\sum_i m_i\right) P_\infty, \\ &P_i = (x_i, y_i) \in C \setminus \{P_\infty\},\ m_i > 0,\ \sum_i m_i \leq g. \end{aligned} \tag{3}$$

但し，$i \neq j$ に対し $P_i \neq \tilde{P}_j$，$F(x_i) = 0$ となる P_i に対し $m_i = 1$ とする．式 (3) の形で与えられる $\mathcal{D}$ を C の被約因子という．例えば，種数 2 の超楕円曲線 C の被約因子 $\mathcal{D}$ は以下の 4 タイプに分類される．

$$\mathcal{D} = \begin{cases} 0 & \\ P_1 - P_\infty & \text{(Type I)} \\ 2P_1 - 2P_\infty,\ y_1 \neq 0 & \text{(Type II)} \\ P_1 + P_2 - 2P_\infty,\ x_1 \neq x_2 & \text{(Type III)} \end{cases} \tag{4}$$

ここで，$P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in C$ である．

被約因子の集合を $\mathcal{J}_C$ と書き，C の Jacobian と呼ぶ．$\mathcal{J}_C$ は無限位数の（可換）加法群となる[2]．

式 (3) で与えた $\mathcal{J}_C$ の元 $\mathcal{D}$ に対し Frobenius 写像 ϕ を以下で定義する．

$$\begin{aligned} \phi : \mathcal{J}_C &\to \mathcal{J}_C \\ \mathcal{D} &\mapsto \mathcal{D}^p \end{aligned} \tag{5}$$

ここで，$\mathcal{D}^p := \sum_i m_i P_i^p - \left(\sum_i m_i\right) P_\infty \in \mathcal{J}_C$, $P_i^p := (x_i^p, y_i^p) \in C \setminus \{P_\infty\}$ とする．Frobenius 写像 ϕ で固定される $\mathcal{J}_C$ の元の集合を $\mathcal{J}_C(\mathbb{F}_p)$ と書く．すなわち，

$$\mathcal{J}_C(\mathbb{F}_p) := \{\mathcal{D} \in \mathcal{J}_C \mid \mathcal{D} = \phi(\mathcal{D})\} \tag{6}$$

である．$\mathcal{J}_C(\mathbb{F}_p)$ は有限可換群となる．

[1] 通常はより一般の有限体上の曲線を考えるが，本論文では議論を簡単にするために有限素体上の曲線のみを扱う．

[2] 例えば [86, 4 章] を参照されたい．

$\mathcal{J}_C(\mathbb{F}_p)$ の位数[3] $\#\mathcal{J}_C(\mathbb{F}_p)$ は式 (1) で与えた多項式 F によって変化するが，変化は，Hasse-Weil バウンド

$$(\sqrt{p}-1)^{2g} \leq \#\mathcal{J}_C(\mathbb{F}_p) \leq (\sqrt{p}+1)^{2g} \tag{7}$$

の範囲に限られる [44, Exercise 5.1]．したがって，$\#\mathcal{J}_C(\mathbb{F}_p) \approx p^g$ である．超楕円曲線暗号は $\mathcal{J}_C(\mathbb{F}_p)$ 上で実現されるが，3.3 項で述べるように位数 $\#\mathcal{J}_C(\mathbb{F}_p)$ が超楕円曲線暗号の主要な安全性指標となる．

超楕円曲線暗号に必須な $\mathcal{J}_C(\mathbb{F}_p)$ 上の効率的な加算アルゴリズムは Cantor [8] によって示され，その後，Harley [26, 34] によって $g=2$ に限定したより効率的なアルゴリズムが示された．Harley の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暗号化速度を実現可能であることが知られている [53]．その後，Harley アルゴリズムの研究 [91, 85, 72, 48, 49, 46, 62, 32, 39] が活発に行われ，現在では，楕円曲線暗号よりも高速な超楕円曲線暗号を実現できる実装環境もある．また，暗号化速度を律速する整数倍算に特化した高速演算法 [24] も提案されている．ここで，整数倍算とは，$\mathcal{D} \in \mathcal{J}_C$ と正整数 n に対する

$$[n]\mathcal{D} := \overbrace{\mathcal{D}+\mathcal{D}+\cdots+\mathcal{D}}^{n\text{ 個}} \in \mathcal{J}_C$$

の計算であり，これは繰り返し 2 倍法により $O(\log n)$ 回の $\mathcal{J}_C$ 上の加算によって実現される [4, Section IV.2].

3 超楕円曲線暗号とその安全性

本節では，超楕円曲線暗号とその安全性について概説する．そのために，まず離散対数問題に基づく公開鍵暗号について復習した後に，離散対数問題に基づく公開鍵暗号を一般化することで超楕円曲線暗号が得られることを示す．そして，超楕円曲線暗号の安全性を議論する．

3.1 離散対数問題に基づく公開鍵暗号

Diffie と Hellman [17] によって提案された初めての公開鍵暗号は鍵共有プロトコルであった．この Diffie-Hellman 鍵共有プロトコルを Algorithm 1 に示す．

Algorithm 1 Diffie-Hellman 鍵共有プロトコル

1: A は素数 p, $g \in \mathbb{F}_p^*$, $n_a \in \{0,\ldots,p-2\}$ を選択する
2: A は $h_a = g^{n_a} \in \mathbb{F}_p^*$ を計算し，(p,g,h_a) を B に送る
3: B は (p,g,h_a) を受信し，$n_b \in \{0,\ldots,p-2\}$ を選択する
4: B は $h_b = g^{n_b} \in \mathbb{F}_p^*$ を計算し，h_b を A に送る
5: B は $k_b = h_a^{n_b} \in \mathbb{F}_p^*$ を暗号鍵とする
6: A は h_b を受信し，$k_a = h_b^{n_a} \in \mathbb{F}_p^*$ を暗号鍵とする

Algorithm 1 において $k_a = k_b$ が成立するので，A と B は暗号鍵を共有できたことになる．しかし，通信を傍受した第 3 者が (p,g,h_a) から $h_a = g^{n_a}$ を満足する n_a を求めるこ

[3] 集合の要素数を位数という．

とができると，$k_a = h_b^{n_a}$ が計算できてしまうので，このプロトコルでは安全な鍵共有ができないことになる．(p, g, h_a) から n_a を求める問題を離散対数問題 (DLP) という．DLP を以下で定義する．

離散対数問題 (DLP) 与えられた $\mathbb{F}_p$，h，$g \in \mathbb{F}_p^*$ に対して，$h = g^n$ となる整数 $n \in \{0, \ldots, p-2\}$ を求めよ．

Diffie-Hellman 鍵共有プロトコルは DLP が難しいことを安全性の根拠とする暗号プロトコルである．このように DLP の計算困難性を安全性の根拠とする公開鍵暗号を DLP に基づく暗号と呼ぶ[4]．

DLP を難しくするには p を（例えば，1024 ビットや 2048 ビット等の）十分な大きさにとる必要がある．さらに，$p-1$ が大きな素数で割り切れなければならない等の安全性条件があるが，このような p の選択は，試し割り算と確率的素数判定 [16, Chapter 3] を用いて容易に実現できる．安全性条件を満足した状態の DLP を解く計算量は

$$O\left(e^{(3^{2/3}+o(1))(\log p)^{1/3}(\log\log p)^{2/3}}\right) \tag{8}$$

となる [33].

Diffie と Hellman による公開暗号の提案後，RSA 暗号 [66] をはじめとする多くの公開鍵暗号が提案されている．

RSA 暗号は DLP に基づく暗号ではないが，DLP に基づく暗号も，ElGamal 暗号，ElGamal 署名 [18]，DSA 署名等，実用プロトコルに実装されているものを含め，数多く提案されている．DLP に基づく暗号の利点の一つは，DLP を一般化できることにある．DLP は有限体の乗法群 $\mathbb{F}_p^*$ 上で定義されているので，$\mathbb{F}_p^*$ を別の有限可換群に置き換えることで，その群上の DLP を定義可能であり，もし $\mathbb{F}_p^*$ よりも難しい DLP を定義可能な群が存在すれば，その群上で DLP に基づく，より安全な暗号を構成できる．

3.2 超楕円曲線暗号

前項で述べたように，有限可換群が存在すればその上で DLP に基づく公開鍵暗号を構成可能であり，$\mathcal{J}_C(\mathbb{F}_p)$ は有限可換群であるので，$\mathcal{J}_C(\mathbb{F}_p)$ 上で DLP に基づく公開鍵暗号を構成可能である．この様にして得られた公開鍵暗号を超楕円曲線暗号と呼ぶ.

Algorithm 2 に超楕円曲線上の Diffie-Hellman 鍵共有プロトコルを示す．Algorithm 2 は，Algorithm 1 の $\mathbb{F}_p^*$ を $\mathcal{J}_C(\mathbb{F}_p)$ に置き換え，この置き換えに従い適切な修正を施すことで容易に得られる．

Algorithm 2 超楕円曲線上の Diffie-Hellman 鍵共有プロトコル

1: A は素数 p, $\mathbb{F}_p$ 上の超楕円曲線 C, $\mathcal{D}_g \in \mathcal{J}_C(Fp)$, $n_a \in \{0, \ldots, \#\mathcal{J}_C(\mathbb{F}_p) - 1\}$ を選択する
2: A は $\mathcal{D}_a = [n_a]\mathcal{D}_g \in \mathcal{J}_C(\mathbb{F}_p)$ を計算し，$(p, C, \mathcal{D}_g, \mathcal{D}_a)$ を B に送る
3: B は $(p, C, \mathcal{D}_g, \mathcal{D}_a)$ を受信し，$n_b \in \{0, \ldots, \#\mathcal{J}_C(\mathbb{F}_p) - 1\}$ を選択する
4: B は $\mathcal{D}_b = [n_b]\mathcal{D}_g \in \mathcal{J}_C(\mathbb{F}_p)$ を計算し，$\mathcal{D}_b$ を A に送る
5: B は $k_b = [n_b]\mathcal{D}_a \in \mathcal{J}_C(\mathbb{F}_p)$ を暗号鍵とする
6: A は $\mathcal{D}_b$ を受信し，$k_a = [n_a]\mathcal{D}_b \in \mathcal{J}_C(\mathbb{F}_p)$ を暗号鍵とする

[4] DLP が難しいこととそれを用いたプロトコルが安全であることは必ずしも一致しないことに注意されたい.

超楕円曲線上の Diffie-Hellman 鍵共有プロトコルと同様な置き換えによって，ElGamal 暗号，ElGamal 署名，DSA 署名等の DLP に基づく公開鍵暗号を超楕円曲線上で構成可能である．これらの超楕円曲線暗号は以下で定義する超楕円曲線上の DLP の計算困難性を安全性の根拠とする．

超楕円曲線上の DLP 与えられた $\mathbb{F}_p$, C および $\mathcal{D}_1, \mathcal{D}_2 \in \mathcal{J}_C(\mathbb{F}_p)$ に対して，$\mathcal{D}_2 = [n]\mathcal{D}_1$ となる整数 $n \in \{0, \ldots, \#\mathcal{J}_C(\mathbb{F}_p) - 1\}$ を求めよ．

もし，超楕円曲線上の DLP が $\mathbb{F}_p^*$ 上の DLP よりも難しければ，$\mathbb{F}_p^*$ 上の DLP に基づく公開鍵暗号より高い安全性を超楕円曲線暗号によって得られることとなる．

3.3 超楕円曲線上の DLP の解法と安全な超楕円曲線

超楕円曲線暗号の安全性は，超楕円曲線上の DLP の解法（暗号学では,「解読法」「攻撃法」）の計算量に依存する．超楕円曲線上の DLP の解法は，これに特化したものや DLP 一般に適用可能なもの等数多く提案されている．以下にこれらを紹介する．

Baby-step giant-step 法 [70, 41]，Pollard の方法 [65] 等の，square-root 法と呼ばれる方法[5]は，DLP 一般に適用可能な解法である．Square-root 法を中国式剰余定理の応用である Pohlig-Hellman 法 [64] とともに用いることで，N を $\#\mathcal{J}_C(\mathbb{F}_p)$ の最大素因子としたとき，計算量

$$O\left(\sqrt{N}\right) \tag{9}$$

で DLP を解くことができる．したがって，たとえ $\#\mathcal{J}_C(\mathbb{F}_p)$ を十分な大きさにとったとしても，N が小さければ超楕円曲線上の DLP を容易に解くことができる．Square-root 法に対して耐性を持つためには N が十分な大きさを持つ必要があり，一方，超楕円曲線暗号の速度・サイズ等の効率を考慮すると p はできるだけ小さい方がよい．これらの要請を満足するためには

$$\#\mathcal{J}_C(\mathbb{F}_p) \approx N \tag{10}$$

かつ $\#\mathcal{J}_C(\mathbb{F}_p)$ が十分な大きさを持つ必要がある．式 (10) を満足する $\#\mathcal{J}_C(\mathbb{F}_p)$ を almost prime 位数，C を almost prime 曲線と呼ぶ．

また，種数 $g > 2$ のときに square-root 法より（漸近的に）効率的な，指数計算法と呼ばれる解法が知られている [1, 23, 20, 74, 60, 30]．したがって，暗号速度等の効率を考慮すると $g = 2$ が望ましい[6]．

超楕円曲線上の DLP の解法は他にも数多く提案されている [21, 68, 22, 3, 25, 61]．しかし，これらの多くは特殊な曲線にのみ適用可能な解法であり，また，適用の可否が $\#\mathcal{J}_C(\mathbb{F}_p)$ から容易に判断できるか，$\mathbb{F}_p$ 上の曲線に対しては適用できないかのどちらかである．

ここまでに述べた解法が十分に大きな計算量となる超楕円曲線上の DLP を構成できれば，それを用いた暗号系は安全であるといえる．本論文では，超楕円曲線 C 上の DLP が既知の解法に対して十分な耐性を持つとき C を「安全な超楕円曲線」と呼ぶ．また，$g \geq 3$

[5] square-root 法は位数計算にも利用される．

[6] パラメータを注意深く選択することで $g \geq 3$ の場合にも安全かつ効率的な暗号系を構成できることがある．

に対しては漸近的に効率的な解法が知られているので，議論を簡単にするために，以降では $g = 2$ とする．

上で指摘したように，square-root 法以外の解法に対して耐性を持たせるのは容易なので，square-root 法に耐性を持つ C を考える．超楕円曲線 C が square-root 法に十分な耐性を持つには almost-prime 曲線であればよい．しかし，$\#\mathcal{J}_C(\mathbb{F}_p)$ の大きさは，要求される安全性によって変化する．例えば,「解法に $O(2^{80})$ 回の $\mathcal{J}_C(\mathbb{F}_p)$ の演算を必要とするならばよし」とするならば，式 (9), (10) から $\#\mathcal{J}_C(\mathbb{F}_p)$ を 160 ビット程度に採ればよい[7]．このとき，式 (7) より p は約 80 ビットとなる．同様の議論は通常の DLP に基づく暗号にも成立し，式 (8) より 1024 ビット程度の p が必要となる．すなわち，80 ビットの p を利用した超楕円曲線暗号と同一の安全性を得るために，通常の DLP に基づく暗号では 1024 ビットの p が必要であり，80 ビットの p に対する $\mathcal{J}_C(\mathbb{F}_p)$ 上の加算と 1024 ビットの $\mathbb{F}_p$ の乗算を比較すると，$\mathcal{J}_C(\mathbb{F}_p)$ 上の加算の方がより高速なため，超楕円曲線暗号は安全な暗号を通常の DLP に基づく暗号より高速に実現できる．

4 安全な超楕円曲線の構成

素数定理 [16, Theorem 1.1.4] と Hasse-Weil バウンド (7) より，ランダムに選択された曲線 C が almost prime 曲線となる確率は $1/(\log p)$ 程度と推測されるので，ランダムに選択した C を用いた超楕円曲線暗号は所望の安全性を満足しない可能性が高い．したがって，安全な超楕円曲線を構成する方法が必要となる．安全な超楕円曲線の実用的な構成法は長い間知られてこなかったが，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てきた．

安全な超楕円曲線の構成法には，大別して，Koblitz 法 [43]，CM 体法 [71, 10, 12, 11, 77, 59, 87, 81, 84]，p 進法 [78, 40, 56, 50, 76, 51]，ℓ 進法があり，CM 体法と ℓ 進法が $\mathbb{F}_p$ 上の曲線に適用可能な方法である．

CM 体法と ℓ 進法はともに楕円曲線に対する方法の拡張として得られるが，数学的知見が少ないこともあり，一般の超楕円曲線に対して楕円曲線と同程度に効率的な方法は知られていない．特に，CM 体法は，楕円曲線に対しても構成可能な曲線が限られているが，超楕円曲線に対しては構成可能な曲線がより限定的である．

ここまでの議論をまとめ，Algorithm3 に安全な超楕円曲線を得るために用いられる一般的な戦略を示す．

Algorithm 3 安全な超楕円曲線の構成

1: **repeat**
2: **repeat**
3: C をランダムに選択
4: $\#\mathcal{J}_C(\mathbb{F}_p)$ を計算/*位数計算*/
5: **until** $\#\mathcal{J}_C(\mathbb{F}_p)$: almost-prime /*$O(\log p)$ 回*/
6: **until** $\mathcal{J}_C(\mathbb{F}_p)$ 上の DLP は既知の解法で解けない/*$O(1)$ 回*/
7: **return** C

Algorithm3 は,「Step 4 で計算した $\#\mathcal{J}_C(\mathbb{F}_p)$ が almost-prime 位数になるまで $O(\log p)$ 回ランダムに C を選ぶ.」と要約される．ランダムに選んだ C 対して $\#\mathcal{J}_C(\mathbb{F}_p)$ を得る計算を位数計算という．位数計算には数え上げ的な方法も知られているが，そのような方法

[7]実際の利用では 160 ∼ 256 ビット程度の $\#\mathcal{J}_C(\mathbb{F}_p)$ が選択される．

は計算量が超楕円曲線上の DLP の解法より大きくなり，安全な超楕円曲線の構成に用いることはできない．ℓ 進法は，Algorithm3, Step 4 の位数計算に ℓ 進位数計算法を利用する方法である．以降ではこの ℓ 進位数計算法を紹介する．

5 ℓ 進位数計算法

1985 年に Schoof [69] は位数の多項式時間計算量である楕円曲線に対する ℓ 進位数計算法を提案した．その後，Schoof の方法に対して多くの改良が行われ，現在では ℓ 進位数計算法を用いて安全な楕円曲線を容易に得られるようになっている．一方，Schoof の方法の超楕円曲線に対する拡張 [63, 38, 2, 35] も行なわれてきたが，これらはいずれも現実的な方法ではなかった．しかし，この十年の間に実装結果を含めたいくつかの研究成果 [23, 54, 27, 29, 82] が挙がり，超楕円曲線に対しても位数計算が実用的な方法に近づきつつある．そこで，本節では超楕円曲線に対する ℓ 進位数計算法を概説する．

5.1 Frobenius 写像と位数 $\#\mathcal{J}_C(\mathbb{F}_p)$

式 (5) で与えた $\mathcal{J}_C$ の Frobenius 写像 ϕ の特性多項式は，C の種数が 2 のとき，4 次の整数係数多項式

$$\chi := X^4 - s_1X^3 + s_2X^2 - s_1pX + p^2 \in \mathbb{Z}[X] \tag{11}$$

となることが知られている [44, Theorem 5.1]．すなわち，任意の $\mathcal{D} \in \mathcal{J}_C$ に対して

$$\begin{aligned} \chi(\phi)\mathcal{D} &= (\phi^4 - s_1\phi^3 + s_2\phi^2 - s_1p\phi + p^2)\mathcal{D} \\ &= \phi^4(\mathcal{D}) - [s_1]\phi^3(\mathcal{D}) + [s_2]\phi^2(\mathcal{D}) - [s_1p]\phi(\mathcal{D}) + [p^2]\mathcal{D} = 0 \end{aligned} \tag{12}$$

を満足する $(s_1, s_2) \in \mathbb{Z}^2$ が C に対して一意に存在する．この (s_1, s_2) は

$$-\lfloor 4\sqrt{p} \rfloor \leq s_1 \leq \lfloor 4\sqrt{p} \rfloor, \tag{13}$$

$$\lceil 2\sqrt{p}|s_1| - 2p \rceil \leq s_2 \leq \left\lfloor \frac{1}{4}s_1^2 + 2p \right\rfloor \tag{14}$$

を満足する [67, 19, 54, 55].

Frobenius 写像の特性多項式 χ と位数 $\#\mathcal{J}_C(\mathbb{F}_p)$ とは式 (15) に示す強い関係を持つ [44, Theorem 5.1]：

$$\#\mathcal{J}_C(\mathbb{F}_p) = \chi(1) \tag{15}$$

したがって，$\#\mathcal{J}_C(\mathbb{F}_p)$ を直接求める必要はなく，χ を求めれば $\#\mathcal{J}_C(\mathbb{F}_p)$ が得られる．すなわち，式 (12) を満足する $(s_1, s_2) \in \mathbb{Z}^2$ を求めることで位数計算ができる．しかし，$\#\{(s_1, s_2)\} = O(p^{3/2})$ なので，暗号に利用される p に対して，式 (12) を満足する (s_1, s_2) を直接探索するのは難しい．

ℓ 進位数計算法は与えられた C に関する (s_1, s_2) を求める方法であり，上述の課題を解決するために $\mathcal{J}_C$ のねじれ群 $\mathcal{J}_C[\ell]$ と中国式剰余定理 [31, Theorem 5.7] を利用する．

5.2 ねじれ群 $\mathcal{J}_C[\ell]$ と Frobenius 写像の作用

素数 $\ell \neq p$ に対して，ℓ 倍すると 0 になる $\mathcal{D} \in \mathcal{J}_C$ を ℓ 等分点という．ℓ 等分点の集合を $\mathcal{J}_C[\ell]$ と書き，ℓ ねじれ群と呼ぶ．すなわち，

$$\mathcal{J}_C[\ell] := \{\mathcal{D} \in \mathcal{J}_C \mid [\ell]\mathcal{D} = 0\} \subset \mathcal{J}_C \tag{16}$$

である．$\mathcal{J}_C[\ell]$ は $\mathbb{F}_\ell$ 上の 4 次元ベクトル空間となる [80]．したがって，$\#\mathcal{J}_C[\ell] = \ell^4$ である．また，式 (5) で定義した Frobenius 写像 ϕ は $\mathcal{J}_C[\ell]$ の $\mathbb{F}_\ell$-線型写像となる．また，Frobenius 写像の $\mathbb{F}_\ell$ 上の特性多項式 χ_ℓ は式 (11) で与えた χ の法 ℓ による簡約となる．したがって，任意の $\mathcal{D} \in \mathcal{J}_C[\ell]$ に対して式 (12) を満足する $(s_1, s_2) \in \mathbb{F}_\ell^2$ を求めれば，$\chi_\ell \equiv \chi \bmod \ell$ が得られたこととなる．ここで，$\#\{(s_1, s_2) \in \mathbb{F}_\ell^2\} = \ell^2$ なので，ℓ が十分に小さければ，全数探索によって $(s_1, s_2) \in \mathbb{F}_\ell^2$ を求められる[8]．

5.3 ℓ 進位数計算法のアウトライン

5.2 項において，$\mathcal{D} \in \mathcal{J}_C[\ell]$ によって $\chi_\ell \equiv \chi \bmod \ell$ が得られることを説明した．本項では，5.2 項で説明した方法と中国式剰余定理によって χ を得る方法を，以下に示す Algorithm 4 に従って説明する．

Algorithm 4 ℓ 進位数計算法

入力: 式 (2) で与えられた $\mathbb{F}_p$ 上の種数 2 の超楕円曲線 C
出力: $\mathcal{J}_C$ の Frobenius 写像 ϕ の特性多項式 $\chi \in \mathbb{Z}[X]$

1: 式 (17) を満足する素数 $\ell_{\max}$ と $m \in \mathbb{Z}$ を計算：

$$m := 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots \ell_{\max} > 4p \tag{17}$$

2: **for** 素数 $\ell \in \{2, 3, 5, \ldots, \ell_{\max}\}$ **do**
3: $\quad \chi_\ell \equiv \chi \bmod \ell$ を計算
4: **end for**
5: 中国式剰余定理により，$\{\chi_\ell\}$ から $\chi \bmod m$ を計算
6: $\chi \bmod m$ から $\chi \in \mathbb{Z}[X]$ を計算

中国式剰余定理は，互いに素な整数 $n_1, \ldots, n_{\max}$ と整数 $x_1, \ldots, x_{\max}$ に対して連立合同式 $x \equiv x_i \bmod n_i$ $(i = 1, \ldots, k)$ を満足する $x \bmod n_1 \cdot n_2 \cdots n_{\max}$ を計算する方法を与える．そこで，まず素数を 2 から順に乗じ，式 (17) を満足する整数 m と素数の集合 $\{2, 3, 5, \ldots, \ell_{\max}\}$ を求める．そして，各 $\ell \in \{2, 3, 5, \ldots, \ell_{\max}\}$ に対して，式 (12) を満足する $s_1 \bmod \ell$, $s_2 \bmod \ell$ を求め，その結果に中国式剰余定理を適用すれば，$s_1 \bmod m$, $s_2 \bmod m$ が求まる．これらの値から s_1, s_2 を（未知の）$q_1, q_2 \in \mathbb{Z}$ を用いて $s_1 = q_1 m + (s_1 \bmod m)$, $s_2 = q_2 m + (s_2 \bmod m)$ と書けるが，式 (13), (14) より

$$\begin{aligned} \#\{s_1\} &= 2\lfloor 4\sqrt{p} \rfloor + 1 \leq m \\ \#\{s_2\} &\leq 4p + 1 \leq m \end{aligned}$$

なので，s_1, s_2（と $\chi \in \mathbb{Z}[X]$）を一意に決定可能である[9]．

[8] 実際には square-root 法によって効率的に計算可能である．

[9] このように中国式剰余定理を援用した方法は「モジュラーアルゴリズム」と呼ばれ，モダンな代数計算アルゴリズムの基盤となっている．

残念ながら現在の一般のコンピュータの計算能力では，Algorithm 4 のみで χ を得るのは難しい．例えば，p が 80 ビットの場合 $\ell_{\max} = 67$ であるが，現状では $\ell = 31$ 程度が計算限界である．そこで，通常は他の方法を併用して χ を得る．たとえば，ごく小さな ℓ と k に対して $\chi \bmod \ell^k$ を計算する方法が知られている [26, 27, 83, 29]．また，Manin の定理 [52] と Chudonovski-Chudonovski アルゴリズム [13] によって，$\chi \bmod p$ を計算量 $O(\sqrt{p})$ で計算できることが知られている [6, 7, 45]．そこで，実際には，計算可能な場合には $\chi \bmod \ell^k$ や $\chi \bmod p$ も計算し，中国式剰余定理に利用するより大きな法 m と $s_1 \bmod m$, $s_2 \bmod m$ を得たうえで，最終的に square-root 法や，より効率的な多次元 square-root 法 [54, 37, 28] を用いて $\chi \in \mathbb{Z}[X]$ を得ている．

6 ℓ 等分点の計算

前節で概略を与えた ℓ 進位数計算法では，任意の $\mathcal{D} \in \mathcal{J}_C[\ell] \subset \mathcal{J}_C$ に対して式 (12) を満足する $(s_1, s_2) \in \mathbb{F}_\ell^2$ を求める必要があった．これには $\mathcal{D} \in \mathcal{J}_C[\ell]$ を実際に知る必要があり，そのため無限集合 $\mathcal{J}_C$ の中から $[\ell]\mathcal{D} = 0$ を満足する $\mathcal{D}$ を発見する方法が必要となる．

楕円曲線に対しては，$\mathcal{D} \in \mathcal{J}_C[\ell]$ の発見に利用可能な ℓ 等分多項式 [47, Chapter II] が知られている．楕円曲線 C の ℓ 等分多項式は，C に対して一意に定まる $\mathbb{F}_p$ 上の $(\ell^2-1)/2$ 次の 1 変数多項式である．楕円曲線の ℓ 等分多項式は，その根から全ての ℓ 等分点を定められる多項式であり，Schoof はこの ℓ 等分多項式を利用して楕円曲線の位数計算法を構成した．しかし，超楕円曲線に対しては完全な ℓ 等分多項式が知られておらず，位数計算の研究も ℓ 等分多項式利用せずに ℓ 等分点を得る方法の検討を主旨としていた [63, 38, 2, 35]．一方，超楕円曲線に対する完全な ℓ 等分多項式は知られていなかったものの，式 (4) の Type I に対する ℓ 等分多項式は Cantor [9] によって得られていた．しかし，残念ながら，$\mathcal{J}_C[\ell]$ の被約因子の殆どは Type III であり，Type I の被約因子は殆ど無いことが知られている．したがって，Cantor の ℓ 等分多項式を用いた位数計算は現実的ではない．

Gaudry と Harley [26] は Cantor の結果を利用して式 (4) の Type III の被約因子対する ℓ 等分多項式を得ることに成功し，これを用いて超楕円曲線の ℓ 進位数計算に初めて成功した．さらに，Gaudry と Schost [27] は Gaudry と Harley の結果を改良し，ℓ 進位数計算法による安全な超楕円曲線を構成に成功した．そこで，本節では，Cantor, Gaudry-Harley, Gaudry-Schost の ℓ 等分多項式とその導出法の概略を紹介する．

$\ell = 2$ に対しては，ℓ 等分点や，$s_1 \bmod \ell$, $s_2 \bmod \ell$ を，式 (1) に与えた F から容易に得られることが知られている [54]．そこで，以降では $\ell \neq 2$ を仮定する．

6.1 Cantor の等分多項式と n 倍公式

Cantor [9] は $\mathbb{F}_p$ 上の種数 2 の超楕円曲線 C と自然数 n に対して C の n 等分多項式 ψ_n

$\in \mathbb{F}_p[X]$ を下式で与えた[10].

$$
\begin{aligned}
\psi_1 &:= 0 \\
\psi_2 &:= 1 \\
\psi_3 &:= 4F \\
\psi_4 &:= 10X^{12} + (104f_1 - 80f_4)X^{11} + \cdots \\
\psi_5 &:= 20X^{21} + (-4416f_1 + 4500f_4)X^{20} + \cdots \\
\psi_6 &:= 35X^{32} + (-52416f_1 + 52640f_4)X^{31} + \cdots \\
\psi_7 &:= 56X^{45} + (179200f_1 - 178696f_4)X^{44} + \cdots \\
\psi_n &:= \frac{\begin{vmatrix} \psi_s\psi_{r-2} & \psi_{s+1}\psi_{r-1} & \psi_{s+2}\psi_r \\ \psi_{s-1}\psi_{r-1} & \psi_s\psi_r & \psi_{s+1}\psi_{r+1} \\ \psi_{s-2}\psi_r & \psi_{s-1}\psi_{r+1} & \psi_s\psi_{r+2} \end{vmatrix}}{\psi_s\psi_r\psi_{s-r}};\ n \geq 8
\end{aligned}
$$

ここで，s, r は $n = s + r$, $s > r$ を満足する自然数であり，F, f_i は式 (1) の定義通りとする．また，紙面の制約上各多項式の低次項を省略している．

Cantor は，$n \geq 3$ に対して

$$\Psi_n := \frac{\gcd(\psi_{n-1}, \psi_n, \psi_{n+1})}{\gcd(\psi_{n-2}, \psi_{n-1}, \psi_n, \psi_{n+1})} \in \mathbb{F}_p[X]$$

と定義すれば，Ψ_n の根 $x \in \overline{\mathbb{F}}_p$ を X 座標とする点 $P = (x, y) \in C \setminus \{P_\infty\}$ に対して，$\mathcal{D} = P - P_\infty \in \mathcal{J}_C$ が $\mathcal{D} \in \mathcal{J}_C[n]$ を満足することを示した．すなわち，Ψ_ℓ の根から Type I の ℓ 等分点を求められる．同様に，$\Psi_{2\ell}$ の根から Type I の 2ℓ 等分点を求め，それを 2 倍することで Type II の ℓ 等分点が得られる．こうして，$\mathcal{D} \in \mathcal{J}_C[\ell]$ が得られた場合には，式 (12) から χ_ℓ を決定できる可能性がある．しかし，上述のように，この方法で $\mathcal{D} \in \mathcal{J}_C[\ell]$ を得ることは殆どできない．

Cantor [9] は ψ_n を求めるに留まらず，Type I の被約因子に対する n 倍公式も与えた．そのために，ψ_n 以外に等分多項式として $\alpha_n, \gamma_n, \delta_n, \in \mathbb{F}_p[X, Z]$ と $\epsilon_n \in \mathbb{F}_p(X)[Y, Z]$ を用いた．以下にこれらを示す．ただし，α_n と γ_n については Z の 1 次項以外は利用しないの

[10] Cantor [9] は一般種数の超楕円曲線を扱っているが，ここでは種数 2 に限定して述べる．

で，各々の 1 次項 $\alpha_{1,n}$, $\gamma_{1,n}$ のみを示す.

$$\begin{aligned}
\alpha_{1,1} &:= -2 \\
\alpha_{1,2} &:= 0 \\
\alpha_{1,3} &:= 10X^4 + 8f_1X^3 + 6f_2X^2 + 4f_3X + 2f_4 \\
\alpha_{1,4} &:= 40X^9 + (32f_1 + 40f_4)X^8 + \cdots \\
\alpha_{1,5} &:= 105X^{16} + (1696f_1 - 1360f_4)X^{15} + \cdots \\
\alpha_{1,n} &:= \frac{\psi_{n-1}\alpha_{1,n-1} + \psi_n\psi_{n-3}}{\psi_{n-2}};\ n \geq 6 \\
\gamma_{1,1} &:= 1 \\
\gamma_{1,2} &:= 4F \\
\gamma_{1,3} &:= 5X^{16} + (576f_1 - 560f_4)X^{15} + \cdots \\
\gamma_{1,4} &:= 24X^{25} + (12000f_1 - 11880f_4)X^{24} + \cdots \\
\gamma_{1,n} &:= \frac{\psi_{n+1}\gamma_{1,n-1} + \psi_{n-1}\psi_{n+2}}{\psi_n};\ n \geq 5
\end{aligned}$$

$$\begin{aligned}
\delta_n &:= (-16F^2\psi_n^2)Z^2 + (-\psi_{n-1}\gamma_{1,n} + \psi_{n+1}\alpha_{1,n})Z - \psi_{n-1}\psi_{n+1} \\
\epsilon_n &:= \frac{YZ(\psi_{n-1}^2\delta_{n+1} - \psi_{n+1}^2\delta_{n-1})}{\psi_{n-1}\psi_n^2\psi_{n-1}} \bmod \delta_n
\end{aligned}$$

ここで，modδ_n は Z の多項式としての δ_n による剰余を表す.

Cantor は C の Type I の被約因子に対して δ_n と ϵ_n を用いて定理 1 に示す n 倍公式を求めた.

定理 1 (Cantor) $\mathbb{F}_p$ 上の種数 2 の超楕円曲線 C 上の点 $P = (x, y)$ に対し，$\mathcal{D} = P - P_\infty \in \mathcal{J}_C$ とすれば,

$$[n]\mathcal{D} = \left\langle \delta_n\left(x, \frac{x - Z}{4y^2}\right), \epsilon_n\left(x, y, \frac{x - Z}{4y^2}\right)\right\rangle \in \mathcal{J}_C \tag{18}$$

が成立する.

式 (18) の左辺の多項式の組を被約因子の Mumford 表現という[11]．左辺の Mumford 表現の各項に対し，下式を満足する d_i, $e_i \in \mathbb{F}_p[X]$ が存在する.

$$\delta_n\left(x, \frac{x - Z}{4y^2}\right) = d_2(x)Z^2 + d_1(x)Z + d_0(x) \tag{19}$$

$$\epsilon_n\left(x, y, \frac{x - Z}{4y^2}\right) = y\left(\frac{e_1(x)Z + e_0(x)}{e_2(x)}\right) \tag{20}$$

ここで，$e_2(x) \neq 0$ である．また，この表現が Type III の被約因子を表すならば，$d_2(x) \neq 0$ である.

一般に，被約因子 $\mathcal{D}_1, \mathcal{D}_2 \in \mathcal{J}_C$ が Mumford 表現によって，$\mathcal{D}_1 = \langle U_1, V_1\rangle$, $\mathcal{D}_2 = \langle U_2, V_2\rangle \in (\overline{\mathbb{F}}_p[Z])^2$ と与えられたとき，$U_1 = cU_2$ を満足する $c \in \overline{\mathbb{F}}_p^*$ が存在し，かつ $V_1 = V_2$ であることと，$\mathcal{D}_1 = \mathcal{D}_2$ とは同値である．さらに，$\mathcal{D} = \langle U, V\rangle \in \mathcal{J}_C$ に対して，$-\mathcal{D} = \langle U, -V\rangle$ である.

[11] 超楕円曲線暗号の実装には Mumford 表現が利用される．Mumford 表現の詳細については，[58, 8, 86] 等を参照されたい.

6.2 Gaudry-Harley の等分多項式

Gaudry と Harley [26] は定理 1 を利用して式 (4) の Type III の被約因子対する ℓ 等分多項式を得た．ここでは，Gaudry と Harley の等分多項式の構成とその課題について述べる．

以下では，求める ℓ 等分点 $\mathcal{D} \in \mathcal{J}_C[\ell]$ が Type III の被約因子

$$\mathcal{D} = P_1 + P_2 - 2P_\infty \in \mathcal{J}_C[\ell],\ P_i = (x_i, y_i) \tag{21}$$

である場合を考える．この場合，$[\ell]\mathcal{D} = 0$ より

$$[\ell](P_1 + P_2 - 2P_\infty) = [\ell](P_1 - P_\infty) + [\ell](P_2 - P_\infty) = 0$$

を得る．したがって，

$$[\ell](P_1 - P_\infty) = -[\ell](P_2 - P_\infty) \tag{22}$$

である．式 (22) の両辺は Type I の被約因子の ℓ 倍なので，定理 1 を適用可能である．式 (19), (20) で与えた d_i, e_i 及び Mumford 表現の一般性質とともに定理 1 を式 (22) に適用し以下を得る：

$$\begin{aligned}&\left\langle Z^2 + \frac{d_1(x_1)}{d_2(x_1)}Z + \frac{d_0(x_1)}{d_2(x_1)}, y_1\left(\frac{e_1(x_1)}{e_2(x_1)}Z + \frac{e_0(x_1)}{e_2(x_1)}\right)\right\rangle \\ &= \left\langle Z^2 + \frac{d_1(x_2)}{d_2(x_2)}Z + \frac{d_0(x_2)}{d_2(x_2)}, -\left(y_2\left(\frac{e_1(x_2)}{e_2(x_2)}Z + \frac{e_0(x_2)}{e_2(x_2)}\right)\right)\right\rangle\end{aligned}$$

ここで，$d_2(x_1) \neq 0$, $d_2(x_2) \neq 0$, $e_2(x_1) \neq 0$, $e_2(x_2) \neq 0$ である．

これを Z の各係数に関して解き以下を得る．

$$\begin{aligned} d_1(x_1)d_2(x_2) - d_1(x_2)d_2(x_1) &= 0 &(23)\\ d_0(x_1)d_2(x_2) - d_0(x_2)d_2(x_1) &= 0 &(24)\\ e_0(x_1)e_2(x_2)y_1 + e_0(x_2)e_2(x_1)y_2 &= 0 &(25)\\ e_1(x_1)e_2(x_2)y_1 + e_1(x_2)e_2(x_1)y_2 &= 0 &(26)\end{aligned}$$

ここで，ℓ が奇数であることより $y_1 \neq 0$ または $y_2 \neq 0$ なので，式 (25), (26) より

$$\begin{vmatrix} e_0(x_1)e_2(x_2) & e_0(x_2)e_2(x_1) \\ e_1(x_1)e_2(x_2) & e_1(x_2)e_2(x_1) \end{vmatrix} = 0$$

であり，さらに，$e_2(x_2)e_2(x_1) \neq 0$ なので，

$$e_0(x_1)e_1(x_2) - e_0(x_2)e_1(x_1) = 0 \tag{27}$$

が成立する．そこで，式 (23), (24), (27) から E_1, E_2, $E_3 \in \mathbb{F}_p[X_1, X_2]$ を

$$\begin{aligned} E_1 &:= d_1(X_1)d_2(X_2) - d_1(X_2)d_2(X_1)\\ E_2 &:= d_0(X_1)d_2(X_2) - d_0(X_2)d_2(X_1)\\ E_3 &:= e_0(X_1)e_1(X_2) - e_0(X_2)e_1(X_1)\end{aligned}$$

と定め,

$$E_1(X_1, X_2) = E_2(X_1, X_2) = E_3(X_1, X_2) = 0 \tag{28}$$

の解を $(X_1, X_2) = (x_1, x_2)$ とする．そして，x_1, x_2 に対して，$y_1^2 = F(x_1)$, $y_2^2 = F(x_2)$ を満足する y_1, y_2 を定め，$P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in C$ とすれば，$\mathcal{D} = P_1 + P_2 - 2P_\infty$ か $\mathcal{D} = P_1 + \tilde{P}_2 - 2P_\infty$ のどちらか一方は ℓ 等分点になる．どちらが ℓ 等分点になるのかは実際に ℓ 倍演算を行うことで容易に確認できる．

Gaudry と Harley [26] は式 (28) を解くために，終結式による変数消去を用いた標準的な代数方程式系の解法 [31, Algorithm 9.3] を利用した．実際には X_1 の多項式である ℓ 等分多項式 R_{GH} を，X_2 に関する終結式 Res_{X_2} によって，以下のように得ている．

$$\begin{aligned} &R_1 = \mathrm{Res}_{X_2}(E_1, E_2),\ R_2 = \mathrm{Res}_{X_2}(E_1, E_3) \in \mathbb{F}_p[X_1] \\ &R_{GH} = \gcd(R_1, R_2) \in \mathbb{F}_p[X_1] \end{aligned} \tag{29}$$

そして，R_{GH} の既約因子分解によって x_1 を求め，この x_1 を式 (28) に代入して得られる X_2 の多項式を既約因子分解することで，対応する x_2 を求めている．

任意の $\mathcal{D} \in \mathcal{J}_C[\ell]$ が Type III であれば，本来 $\deg R_{GH} = \ell^4 - 1$ となるが，実際には

$$\deg R_{GH} > \ell^4 - 1 \tag{30}$$

となる．これは変数消去に終結式を利用しているためであり，R_{GH} の根に d_2 の根の一部が含まれてしまうことによる．R_{GH} の根のうち d_2 の根に対しては対応する x_2 が求まらないので，Gaudry と Harley の方法の解は必ず ℓ 等分点になる．しかし，この方法による ℓ 進位数計算法の計算量において，R_{GH} の既約因子分解の計算量が支配的であり，既約因子分解の計算量は $\deg R_{GH}$ に大きく影響される．したがって，Gaudry-Harley の等分多項式には，式 (30) で与えた性質によって位数計算の速度が，本来の $\deg R_{GH} = \ell^4 - 1$ の場合と比較して，遅くなるという課題が残る．

6.3 Gaudry-Schost の等分多項式

Gaudry と Schost [27] は式 (29) で与えた Gaudry-Harley の等分多項式 R_{GH} の改良を行った．

改良の一つは，R_{GH} の根集合から d_2 の根を除去し R_{GH} の次数を下げることにある．Gaudry と Schost [27] は R_{GH} の性質を詳細に解析し，d_2 の根を除去する効率的な方法を提案している．

Gaudry と Schost [27] は多項式次数を更に小さくする改良をも行っている．以下ではこの改良を紹介する．

式 (21) で与えた Type III の $\mathcal{D} \in \mathcal{J}_C[\ell]$ に対して，x_1, x_2 は，その対称性から,

$$E_1(x_1, x_2) = E_2(x_1, x_2) = E_3(x_1, x_2) = 0$$

を満足するとともに

$$E_1(x_2, x_1) = E_2(x_2, x_1) = E_3(x_2, x_1) = 0$$

をも満足する．すなわち，x_1, x_2 はともに R_{GH} の根となる．一方，R_{GH} から x_1 が求まった後には，式 (28) から x_2 は容易に求まる．したがって，x_1, x_2 のどちらか一方が R_{GH}

の根であれば十分であり，もしそのような構成が可能であれば，根の個数を半分にできるので，次数を $(\ell^4-1)/2$ とすることができる．Gaudry と Schost は基本対称式変換 [15, 7. §1] を用いてこれを実現した[12].

まず，x_1, x_2 に対してその基本対称式

$$t_1 := x_1 + x_2,\ t_2 := x_1 x_2 \tag{31}$$

を考える．そして，これら t_1, t_2 を解とする方程式系を構成する．具体的には $E_1(X_1, X_2)$, $E_2(X_1, X_2)$, $E_3(X_1, X_2)$ を対称式簡約を用いて変数変換し，$E_{s1}(T_1, T_2)$, $E_{s2}(T_1, T_2)$, $E_{s3}(T_1, T_2) \in \mathbb{F}_p[T_1, T_2]$ を得る．ここで，

$$T_1 := X_1 + X_2,\ T_2 := X_1 X_2 \tag{32}$$

である．これらの多項式から，

$$E_{s1}(t_1, t_2) = E_{s2}(t_1, t_2) = E_{s3}(t_1, t_2) = 0 \tag{33}$$

を満足する t_1, t_2 を求めれば，式 (31) から

$$X^2 - t_1 X + t_2 \tag{34}$$

の根が x_1 となる．

具体的には，Gaudry-Harley と同様に，

$$\begin{aligned} &R_{s1} = \mathrm{Res}_{T_2}(E_{s1}, E_{s2}),\ R_{s2} = \mathrm{Res}_{T_2}(E_{s1}, E_{s3}) \in \mathbb{F}_p[T_1] \\ &R_{GS} = \gcd(R_{s1}, R_{s2}) \in \mathbb{F}_p[T_1] \end{aligned} \tag{35}$$

として，T_1 の多項式である ℓ 等分多項式 R_{GS} を求め，この根を t_1 とする．この方法を第一の改良とともに計算することで

$$\deg R_{GS} = \frac{\ell^4 - 1}{2} \tag{36}$$

が得られる．この $\deg R_{GS}$ は理論上の下限になっており，R_{GS} の利用によって高速な ℓ 進位数計算を実現できる．

7 既知の位数計算結果と最近の話題

表 1 に $\mathbb{F}_p$ 上の種数 2 の超楕円曲線の位数計算結果を示す．表中の “$\log_2 \#\mathcal{J}_C(\mathbb{F}_p)$” は計算された位数 $\#\mathcal{J}_C(\mathbb{F}_p)$ のビット数を表す．また，“ℓ” には Algorithm 4 に利用された法 ℓ を，併用した方法とともに示す.

2000 年に Gaudry と Harley は，6.2 項で紹介した等分多項式 R_{GH} を用いた ℓ 進位数計算を行い，さらに 2 冪の法を用いた後に，最終的に square-root 法の並列計算によって 126 ビットの位数計算に成功した．また，Gaudry と Schost は，6.3 項で紹介した等分多項式 R_{GS} を用いた ℓ 進位数計算，2 冪の法の利用と多次元 square-root 法によって 160 ビット位数の計算を行い，2004 年に安全な超楕円曲線の構成に成功している．しかし，この計算で

[12] 通常の基本対称式変換の適用は計算量的に困難であるが，Gaudry と Schost は終結式と基本対称式変換を同時計算する方法により計算量の増加を防いでいる．

表 1: 有限素体 $\mathbb{F}_p$ 上の種数 2 の超楕円曲線 C の位数計算結果

文献	年	$\log_2 \#\mathcal{J}_C(\mathbb{F}_p)$	ℓ	特殊性
[26]	2000	126	$2^7 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ + パラレル square-root 法	
[27]	2004	160	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ + 多次元 square-root 法	$\mathbb{F}_p$
[73]	2007	188	改良 square-root 法	C
[29]	2008	254	$2^{17} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$ + square-root 法	C
[82]	2010	160	$2^{10} \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ + 多次元 square-root 法	

は R_{GS} の既約因子分解が高速になる特殊な $\mathbb{F}_p$ が利用されていた．Gaudry と Schost は，2008 年には 254 ビットの安全な超楕円曲線の構成に成功している [29]．この計算には，3 冪等分点等の $\ell > 2$ に対する ℓ^k 等分点の計算が可能である特殊な曲線が利用されている．さらに，R_{GS} の既約因子分解を省略する新たな方法が利用されている．しかし，この方法は曲線によらずに利用できる方法ではなく，その一般性は今のところ明らかでない．石黒等 [36] は，R_{GS} の性質を解析して，Gaudry と Schost の方法の改良を行った．この改良は $\mathbb{F}_p$ の性質によらずに位数計算を高速化するものである．石黒等は，この改良を用いて，160 ビット位数の一般性の高い安全な超楕円曲線の構成に成功している [82].

最近，Sutherland [73] によって（ℓ 進位数計算法を用いずに）square-root 法のみを用いる安全な曲線の構成法が提案された．この方法は，素因数分解に対する $p-1$ 法 [16, Section 5.4] を応用した方法であり，これまでに知られた位数計算法と発想が異なる興味深い方法である．Sutherland の方法では，位数計算可能な曲線が極めて限定されるが，計算可能な曲線の存在確率の解析や，より一層の高速化等，今後の研究の進展が期待されている．

さらに，2010 年に入り，内田 [75] によって一般種数の超楕円曲線の（完全な）ℓ 等分多項式が得られた．この等分多項式を利用することで効率的な位数計算法が得られる可能性があり，今後の研究が待たれている．

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. In L. M. Adleman and M. D. Huang, editors, *Algorithmic Number Theory - ANTS-I*, No. 877 in Lecture Notes in Computer Science, pp. 28–40. Springer, 1994.

[2] L. M. Adleman and M. D. Huang. Counting rational points on curves and Abelian varieties over finite fields. In H. Cohen, editor, *Algorithmic Number Theory - ANTS-II*, No. 1122 in Lecture Notes in Computer Science, pp. 1–16. Springer, 1996.

[3] S. Arita, K. Matsuo, K. Nagao, and M. Shimura. A Weil descent attack against elliptic curve cryptosystems over quartic extension fields. *IEICE Trans.*, Vol. E89-A, No. 5, pp. 1246–1254, May 2006.

[4] I. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography.* No. 265 in London Mathematical Society Lecture Note Series. Cambridge U. P., 1999.

[5] I. Blake, G. Seroussi, and N. Smart, editors. *Advances in Elliptic Curves Cryptography.* No. 317 in London Mathematical Society Lecture Note Series. Cambridge U. P., 2005.

[6] A. Bostan, P. Gaudry, and É. Schost. Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves. In G. L. Mullen, A. Poli, and H. Stichtenoth, editors, *Finite Fields and Applications, 7th International Conference, Fq7, Toulouse, France, May 5-9, 2003, Revised Papers*, Vol. 2948 of *Lecture Notes in Computer Science*, pp. 40–58. Springer, 2004.

[7] A. Bostan, P. Gaudry, and É. Schost. Linear recurrences with polynomial coefficients and

application to integer factorization and Cartier-Manin operator. *SIAM J. Comput.*, Vol. 36, No. 6, pp. 1777–1806, 2007.
[8] D. G. Cantor. Computing in the Jacobian of hyperelliptic curve. *Math. Comp.*, Vol. 48, No. 177, pp. 95–101, 1987.
[9] D. G. Cantor. On the analogue of the division polynomials for hyperelliptic curves. *J. für die reine und angewandte Mathematik*, Vol. 447, pp. 91–145, 1994.
[10] J. Chao, N. Matsuda, and S. Tsujii. Efficient construction of secure hyperelliptic discrete logarithm problems. In Y. Han, T. Okamoto, and S. Quing, editors, *ICICS'97*, No. 1334 in Lecture Notes in Computer Science, pp. 292–301. Springer, 1997.
[11] J. Chao, K. Matsuo, H. Kawashiro, and S. Tsujii. Construction of hyperelliptic curves with CM and its application to cryptosystems. In T. Okamoto, editor, *Advances in Cryptology - ASIACRYPT 2000*, No. 1976 in Lecture Notes in Computer Science, pp. 259–273. Springer, December 2000.
[12] J. Chao, K. Matsuo, and S. Tsujii. Fast construction of secure discrete logarithm problems over Jacobian varieties. In S. Qing and J.Eloff, editors, *Information Security for Global Information Infrastructures: IFIP TC 11 16th Annual Working Conference on Information Security*, pp. 241–250. Kluwer Academic Pub., August 2000.
[13] D. V. Chudnovsky and G. V. Chudonovsky. Approximations and complex multiplication according to Ramanujan. In *Ramanujan revisited (Urbana-Chmpaign, Ill., 1987)*, pp. 375–472. Academic Press, 1988.
[14] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of elliptic and hyperelliptic curve cryptography*. Chapman & Hall/CRC, 2005.
[15] D. Cox, J. Little, and D. O'Shea. *Ideals, vrieties, and algorithms*. Springer, 3rd edition, 2007.
[16] R. Crandall and C. Pomerance. *Prime Numbers*. Springer, 2nd edition, 2005.
[17] W. Diffie and M. Hellman. New direction in cryptography. *IEEE Trans. on Info. Theory*, Vol. IT-23, No. 6, pp. 644–654, 1976.
[18] T. ElGamal. A public key cryptosystem and sigunature scheme based on discrete logarithms. *IEEE Trans. on Info. Theory*, Vol. IT-31, No. 4, pp. 469–472, 1985.
[19] N. D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In D. A. Buell and J. T. Teitlbaum, editors, *Computational perspectives on number theory*, pp. 21–76. AMS, 1995.
[20] A. Enge and P. Gaudry. A general framework for subexponential discrete logarithm algorithms. *Acta Arith.*, Vol. 102, pp. 83–103, 2002.
[21] G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, Vol. 62, pp. 865–874, 1994.
[22] S. D. Galbraith. Weil descent of Jacobians. In Daniel Augot and Claude Carlet, editors, *Electronic Notes in Discrete Mathematics*, Vol. 6. Elsevier Science Publishers, 2001.
[23] P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In B. Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000*, No. 1807 in Lecture Notes in Computer Science, pp. 19–34. Springer, 2000.
[24] P. Gaudry. Fast genus 2 arithmetic based on Theta functions. *J. Mathematical Cryptology*, Vol. 1, pp. 243–265, 2007.
[25] P. Gaudry. Index calculus for abelian varieties and the elliptic curve discrete logarithm problem. *J. Symbolic Comput.*, Vol. 44, pp. 1690–1702, 2009.
[26] P. Gaudry and R. Harley. Counting points on hyperelliptic curves over finite fields. In W. Bosma, editor, *Algorithmic Number Theory - ANTS-IV*, No. 1838 in Lecture Notes in Computer Science, pp. 313–332. Springer, 2000.
[27] P. Gaudry and É. Schost. Construction of secure random curves of genus 2 over prime fields. In *Advances in Cryptology - EUROCRYPT 2004*, No. 3027 in Lecture Notes in Computer Science, pp. 239–256. Springer, 2004.
[28] P. Gaudry and É. Schost. A low-memory parallel version of Matsuo, Chao and Tsujii's algorithm. In D. Buell, editor, *Algorithmic Number Theory - ANTS-VI*, No. 3076 in Lecture Notes in Computer Science, pp. 208–222. Springer, 2004.

[29] P. Gaudry and É. Schost. Hyperelliptic curve point counting record: 254 bit Jacobian. http://www.loria.fr/~gaudry/record127/, 2008.
[30] P. Gaudry, E. Thomé, N. Thériault, and C. Diem. A double large prime variation for small genus hyperelliptic index calculus. *Math. Comp.*, Vol. 76, No. 257, pp. 475–492, 2007.
[31] K. O. Geddes, S. R. Czapor, and G. Labahn. *Algorithms for Computer Algebra*. Kluwer Academic Pub., 1992.
[32] M. Gonda, K. Matsuo, K. Aoki, J. Chao, and S. Tsujii. Improvements of addition algorithm on genus 3 hyperelliptic curves and their implementation. *IEICE Trans.*, Vol. E88-A, No. 1, January 2005. 89-96.
[33] D. M. Gordon. Discrete logarithms in $GF(p)$ using the number field sieve. *SIAM J. Discrete Math.*, Vol. 6, pp. 124–138, 1993.
[34] R. Harley. A short description of an efficient algorithm for computing the group law in the Jacobian of a genus-2 curve, 2000. preprint.
[35] M. D. Huang and D. Ierardi. Counting rational point on curves over finite fields. *J. Symbolic Computation*, Vol. 25, pp. 1–21, 1998.
[36] T. Ishiguro and K. Matsuo. Fields of definition of torsion points on the Jacobians of genus 2 hyperelliptic curves over finite fields. In *Proc. of SCIS2010*, No. 2D4-6, January 2010.
[37] F. A. Izadi and V. K. Murty. Counting points on an Abelian variety over a finite field. In *Progress in Cryptology - INDOCRYPT 2003*, No. 2904 in Lecture Notes in Computer Science, pp. 323–333. Springer, 2003.
[38] W. Kampkötter. *Explizite Gleichungen für Jacobische Varietäten hyperelliptischer Kurven*. PhD thesis, GH Essen, 1991.
[39] M. Katagi, T. Akishita, I. Kitamura, and T. Takagi. Efficient hyperelliptic curve cryptosystems using Theta divisors. *IEICE Trans.*, Vol. E89-A, No. 1, pp. 151–160, 2006.
[40] K. S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washinitzer cohomology. *J. Ramanujan Math. Soc.*, Vol. 16, No. 4, pp. 323–338, 2001.
[41] D. E. Knuth. *The art of computer programming*, Vol. 3 Sorting and Searching. Addison Wesley, 2nd edition, 1998.
[42] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, Vol. 48, pp. 203–209, 1987.
[43] N. Koblitz. Hyperelliptic curve cryptosystems. *J. Cryptology*, Vol. 1, No. 3, pp. 139–150, 1989.
[44] N. Koblitz. *Algebraic Aspects of Cryptography*, Vol. 3 of *Algorithms and Computation in Mathematics*. Springer, 1998.
[45] H. Komoto, S. Kozaki, and K. Matsuo. Improvements in the computation of the Hasse-Witt matrix. *JSIAM Letters*, Vol. 2, pp. 17–20, 2010.
[46] J. Kuroki, M. Gonda, K. Matsuo, J. Chao, and S. Tsujii. Fast genus three hyperelliptic curve cryptosystems. In *Proc. of SCIS2002*, pp. 503–507, January 2002.
[47] S. Lang. *Elliptic Curves Diophantine Analysis*. Springer, 1978.
[48] T. Lange. Efficient arithmetic on genus 2 hyperelliptic curves over finite fields via explicit formulae. Cryptology ePrint Archive, Report 2002/121, 2002. http://eprint.iacr.org/.
[49] T. Lange. Weighted coordinates on genus 2 hyperelliptic curves. Cryptology ePrint Archive, Report 2002/153, 2002. http://eprint.iacr.org/.
[50] A. Lauder and D. Wan. Computing zeta functions of Artin-Schreier curves over finite fields. *LMS J. Comput. Math.*, Vol. 5, pp. 33–55, 2002.
[51] R. Lercier and D. Lubicz. A quasi quadratic time algorithm for hyperelliptic curve point counting. *The Ramanujan J.*, Vol. 12, No. 3, pp. 399–423, 2006.
[52] J. I. Manin. The Hasse-Witt matrix of an algebraic curve. *Trans. AMS*, Vol. 45, pp. 245–264, 1965.
[53] K. Matsuo, J. Chao, and S. Tsujii. Fast genus two hyperelliptic curve cryptosystems. Technical Report ISEC2001-31, IEICE, July 2001.
[54] K. Matsuo, J. Chao, and S. Tsujii. An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields. In C. Fieker and D. R. Kohel, editors, *Algorithmic Number Theory - ANTS-V*, No. 2369 in Lecture Notes in Computer Science,

pp. 461–474. Springer, July 2002.
[55] K. Matsuo, J. Chao, and S. Tsujii. Baby step giant step algorithms in point counting of hyperelliptic curves. *IEICE Trans.*, Vol. E86-A, No. 5, pp. 1127–1134, May 2003.
[56] J.-F. Mestre. Algorithms pour compter des points en petite carctéristique en genre 1 and 2. `http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps`, 2002.
[57] V. S. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology - CRYPTO '85*, No. 218 in Lecture Notes in Computer Science, pp. 417–426. Springer, 1986.
[58] D. Mumford. *Tata Lectures on Theta II.* No. 43 in Progress in Mathematics. Birkhäuser, 1984.
[59] N. Murabayashi and A. Umegaki. Determination of all **Q**-rational CM-points in the moduli space of principally polarized abelian surfaces. *J. of Algebra*, Vol. 235, No. 1, pp. 267–274, 2001.
[60] K. Nagao. Index calculus attack for Jacobian of hyperelliptic curves of small genus using two large primes. *Japan J. Industrial and Applied Mathematics*, Vol. 24, No. 3, 2007.
[61] K. Nagao. Decomposition attack for the Jacobian of a hyperelliptic curve over an extension field, 2010.
[62] J. Pelzl, T. Wollinger, J. Guajardo, and C. Paar. Hyperelliptic curve cryptosystems: Closing the performance gap to elliptic curves. In *Cryptographic Hardware and Embedded Systems - CHES 2003*, No. 2779 in Lecture Notes in Computer Science, pp. 351–365. Springer, 2003.
[63] J. Pila. Frobenius maps of Abelian varieties and finding roots of unity in finite fields. *Math. Comp.*, Vol. 55, pp. 745–763, 1990.
[64] G. C. Pohlig and M. E. Hellman. An improved algorithm for comuting logarithms over GF(p) and its cryptographic significance. *IEEE Trans. on Info. Theory*, Vol. IT-24, pp. 106–110, 1978.
[65] J. M. Pollard. Monte Carlo methods for index computation (mod p). *Math. Comp.*, Vol. 32, pp. 918–924, 1978.
[66] R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Com. of the ACM*, Vol. 21, No. 2, pp. 120–126, 1978.
[67] H.-G. Rück. Abelian surfaces and Jacobian varieties over finite fields. *Compositio Math.*, Vol. 76, pp. 351–366, 1990.
[68] H.-G. Rück. On the discrete logarithm problem in the divisor class group of curves. *Math. Comp.*, Vol. 68, pp. 805–806, 1997.
[69] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, Vol. 44, pp. 483–494, 1985.
[70] D. Shanks. Class number, a theory of factorization, and genera. In *Proc. of Symp. Math. Soc. 20*, pp. 415–440, 1971.
[71] A. M. Spallek. *Kurven vom Geshlcht 2 und ihre Anwendung in Public-Key-Kryptosystemem.* PhD thesis, GH Essen, 1994.
[72] H. Sugizaki, K. Matsuo, J. Chao, and S. Tsujii. An extension of Harley addition algorithm for hyperelliptic curves over finite fields of characteristic two. Technical Report ISEC2002-9, IEICE, May 2002.
[73] A. V. Sutherland. A generic approach to searching for Jacobians. *Math. Comp.*, Vol. 78, pp. 485–507, 2009.
[74] N. Thériault. Index calculus attack for hyperelliptic curves of small genus. In C. S. Laih, editor, *Advances in Cryptology - ASIACRYPT 2003*, No. 2894 in Lecture Notes in Computer Science, pp. 75–92. Springer, 2003.
[75] Y. Uchida. Division polynomials and canonical local heights on hyperelliptic Jacobians, March 2010. preprint.
[76] F. Vercauteren. Computing zeta functions of hyperelliptic curves over finite fields of characteristic 2. In M. Yung, editor, *Advances in Cryptology - CRYPTO 2002*, No. 2442 in Lecture Notes in Computer Science, pp. 369–384. Springer, 2002.
[77] P. V. Wamelen. Example of genus two CM curves defined over the rationals. *Math. Comp.*, Vol. 68, No. 225, pp. 307–320, 1999.
[78] D. Wan. Computing zeta functions over finite fields. *Contemporary Mathematics*, Vol. 245,

pp. 131–141, 1999.
[79] L. Washington. *Elliptic curves: number theory and cryptography*. Chapman & Hall/CRC, 2nd edition, 2008.
[80] W. C. Waterhouse. Abelian varieties over finite fields. *Ann. scient. É.N.S.*, Vol. 4^o t. 2, pp. 521–560, 1969.
[81] A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp.*, Vol. 72, No. 241, pp. 435–458, 2003.
[82] 石黒司, 松尾和人. 種数 2 の超楕円曲線の位数計算の高速実装. 2010 年日本応用数理学会研究部会連合発表会 JANT セッション, 3 月 2010.
[83] 小崎俊二, 松尾和人. 種数 2 の超楕円曲線の 2 冪ねじれ点計算の改良. 日本応用数理学会論文誌, Vol. 17, No. 4, pp. 577–593, 12 月 2007.
[84] 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. 日本応用数理学会論文誌, Vol. 12, pp. 269–279, 2002.
[85] 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. In *Proc. of SCIS2002*, pp. 155–160, 2002.
[86] 辻井重男, 笠原正雄, 有田正剛, 境隆一, 只木孝太郎, 趙晋輝, 松尾和人. 暗号理論と楕円曲線. 森北出版, 2008.
[87] 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, Vol. J84-A, No. 8, pp. 1045–1053, 8 月 2001.
[88] 松尾和人, 有田正剛, 趙晋輝. 代数曲線暗号. 日本応用数理学会論文誌, Vol. 13, No. 2, pp. 231–243, 6 月 2003.
[89] 松尾和人, 有田正剛, 趙晋輝. 代数曲線上の公開鍵暗号. 情報処理, Vol. 45, No. 11, pp. 1114–1116, 11 月 2004.
[90] 松尾和人. 代数曲線暗号とその安全性. 第 15 回 整数論サマースクール — 種数の高い代数曲線と Abel 多様体 — 報告書, pp. 223–238, 1 月 2008.
[91] 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. In *Proc. of SCIS2002*, pp. 497–502, 2002.