種数 2 の超楕円曲線の 2 冪ねじれ点計算の改良

小崎 俊二 *　松尾 和人 *
* 情報セキュリティ大学院大学

概要.　Gaudry と Harley により提案された種数 2 の超楕円曲線の Schoof アルゴリズムは 2 冪ねじれ点を利用する．Gaudry と Schost は 2 ねじれ群の作用を利用しこの 2 冪ねじれ点計算の改良を行なった．本論文では，2 冪ねじれ点の 2 等分点の性質と 2 ねじれ群のそれらへの作用の性質を明らかにし，これらの性質を用いて 2 冪ねじれ点計算の改良を行なった．また，実装実験により改良の効果を確認した．

An improvement on the computation of 2-power torsion points on genus 2 hyperelliptic curves

Shunji Kozaki*　Kazuto Matsuo*
*Institute of Information Security

Abstract.　Gaudry and Harley proposed a Schoof-like algorithm for genus 2 hyperelliptic curves which uses the 2-power torsion points on the Jacobians. Using actions of the 2 torsion subgroups on the 2-power torsion points, Gaudry and Schost improved the 2-power torsion point computation. This paper shows properties of the halved points of the 2-power torsion points and the actions of the 2 torsion subgroups. By using these properties, this paper improves the computation of the 2-power torsion points. Moreover, an implementation of the improved algorithm is shown in this paper. The implementation results show that the improvement is efficient.

1. はじめに

超楕円曲線暗号 [11] は有限体上の超楕円曲線の Jacobian の有理点のなす有限アーベル群を利用し構成される公開鍵暗号である．この超楕円曲線暗号の実用化には安全かつ効率的な暗号系を実現する超楕円曲線を豊富に構成することが必要である．超楕円曲線暗号が安全であるためには利用する曲線の Jacobian の位数が 160bit 以上の素数を因子に持つ必要があるが，この条件を満足する超楕円曲線の構成法の 1 つとしてランダムに選択した曲線の中から Jacobian の位数が 160bit 以上の素数を因子に持つ曲線を探索する方法がある．しかし，この構成法は多くの曲線に対し Jacobian の位数の計算を行なう必要があるため，高速な位数計算アルゴリズムを必要とする．

小標数の有限体上の超楕円曲線に対しては，暗号利用可能なサイズの Jacobian の位数を高速に計算可能なアルゴリズムが存在する [2, 10, 15, 21]．一方大標数の有限体上の超楕円曲線を用いて高速な暗号系を構成可能である [16, 17] が，この場合に関しては楕円曲線

に対する高速位数計算アルゴリズムとして知られる Schoof アルゴリズム [14, 18, 19] の種数 2 の超楕円曲線に対する拡張アルゴリズム [5, 6, 13] が知られている．しかし，この拡張アルゴリズムは与えられた曲線に対し約 1 週間の計算時間を必要とするため，暗号利用可能な曲線を豊富に構成するには至っていない．したがってこのアルゴリズムの高速化は重要な課題である．

Schoof アルゴリズムとその超楕円曲線への拡張は，十分な数の小さな素数に対し各々の素数を法とした位数の剰余を計算し，各々の素数に対し得られた位数の剰余から中国の剰余定理によって Jacobian の位数を計算するものである．これらのアルゴリズムにおいて，各々の小さな素数 ℓ に対する計算では Jacobian の ℓ ねじれ点が利用される．標数 2 の有限体上の楕円曲線に対する Schoof アルゴリズムにおいては素数のみならず 2 冪を法とした位数の剰余も用いることでより高速な計算が可能であることが知られている [8,14]．同様に超楕円曲線に対するアルゴリズムにおいても 2 冪を法とした位数の剰余を用いることでアルゴリズムの効率化が計られている．超楕円曲線に対するアルゴリズムにおいてはこの計算のために 2 冪ねじれ点を得る必要が有る．Gaudry と Harley [5] は 2 冪ねじれ点の必要十分条件を表す多変数方程式系を与え，Gröbner 基底計算によって得られた 1 変数多項式の求根により 2 冪ねじれ点を求めた．この方法においては 1 変数多項式の求根に最も時間を必要とした．Gaudry と Schost [6] は，Hanrot と Morain [7] により得られた知見を応用し 2 ねじれ群（とその部分群）の 2 冪ねじれ点への自然な作用を利用することでこの 1 変数多項式の求根を高速化した．

本論文では，まず 2 冪ねじれ点の 2 等分点の性質を詳細に検討し，次に [6] で利用された 2 ねじれ点の 2 冪ねじれ点への自然な作用の性質を詳細に見る．そして以上によって得られた知見に基づき，Gaudry と Schost [6] の提案した種数 2 の超楕円曲線の 2 冪ねじれ点計算アルゴリズムの改良を行う．さらに実装実験により提案アルゴリズムの効果を確認する．

本論文の構成を以下に示す．まず，第 2 節において以降で必要な記号の定義と仮定を行う．次に，第 3 節において Gaudry と Harley [5] 及び Gaudry と Schost [6] の提案した 2 冪ねじれ点の計算アルゴリズムについて概説する．そして，第 4 節において 2 冪ねじれ点の 2 等分点の性質と 2 ねじれ点の 2 冪ねじれ点への作用の性質について議論し，この議論の下で [6] によって提案された 2 冪ねじれ点計算アルゴリズムの改良を行う．さらに，第 5 節において提案アルゴリズムの実装実験を行いその効果を確認する．最後に，第 6 節において本論文をまとめる．

尚，本論文では有限素体上の曲線を対象とするがこれは簡明な議論のためであり本論文の結果は拡大体上の曲線に対しても直接利用可能である．

2. 準備

p を奇素数とする．有限体 $\mathbb{F}_p$ 上定義された種数 2 の超楕円曲線 C を，

$$C : Y^2 = F,\ F \in \mathbb{F}_p[X] : \text{monic},\ \deg F = 5 \tag{2.1}$$

と定義する．ここで，F は重根を持たないものとする．この C の Jacobian を $\mathbb{J}_C$ と書く．

$d \in \mathbb{N}$ に対し $q = p^d$ とする．このとき，$\mathbb{J}_C$ の q 乗 Frobenius 写像を ϕ_q で表し，$\mathbb{J}_C$ の点 $\mathcal{D}$ の ϕ_q による像を $\mathcal{D}^q$ と書く．$\mathcal{D}^q = \mathcal{D}$ を満足するとき $\mathcal{D}$ は $\mathbb{F}_q$ 上定義されるとする．また，$\mathbb{F}_q$ 上定義される $\mathcal{D}$ を $\mathbb{F}_q$-有理点という．$\mathbb{F}_q$-有理点全体の集合を $\mathbb{J}_C(\mathbb{F}_q)$ と書く．この $\mathbb{J}_C(\mathbb{F}_q)$ は有限アーベル群をなす．

$\mathbb{J}_C(\mathbb{F}_q)$ の点は，以下の条件を満足する多項式 $U, V \in \mathbb{F}_q[X]$ の組 (U, V) により一意に表現される [1, Th.14.5].

$$\begin{aligned} &U : \text{monic},\ \deg V < \deg U \le 2, \\ &F - V^2 \equiv 0 \bmod U \end{aligned} \tag{2.2}$$

この (U, V) を $\mathbb{J}_C(\mathbb{F}_q)$ の点の Mumford 表現と呼ぶ．本論文では $\mathbb{J}_C(\mathbb{F}_q)$ の点は Mumford 表現を用いて表現されているとする．

$k \in \mathbb{N}$ に対し $\mathbb{J}_C$ の点 $\mathcal{D}$ を 2^k 倍した点を $[2^k]\mathcal{D}$ と書く．$[2^k]\mathcal{D} = 0$ を満足する点 $\mathcal{D}$ を 2^k ねじれ点と呼び，また 2^k ねじれ点の全体を $\mathbb{J}_C[2^k]$ と書く．このとき，

$$\mathbb{J}_C[2^k] \simeq (\mathbb{Z}/2^k\mathbb{Z})^4 \tag{2.3}$$

である [1, Th.14.11]．特に $\mathbb{J}_C[2]$ は F の根を X 座標とする C の点及びその和によって尽くされることが知られている．したがって F が $\mathbb{F}_p$ 上既約であれば Jacobian の位数 $\sharp\mathbb{J}_C(\mathbb{F}_p)$ は 2 で割れない．この性質は暗号利用を考慮した場合好ましい性質であり，また F の既約判定は位数計算と比較して無視可能な計算量である．そこで，本論文では F は $\mathbb{F}_p$ 上既約であると仮定する．さらに，F の（分解体上での）因子分解も高速に実行可能であり，$\mathbb{J}_C[2]$ の点が高速に得られることに注意されたい．

本論文では，$k \in \mathbb{N}$ に対し $\mathcal{D}_k \in \mathbb{J}_C[2^k] \setminus \mathbb{J}_C[2^{k-1}]$ とする．また，与えられた $\mathcal{D}_k$ に対し $\mathcal{D}_{k+1}$ は $\mathcal{D}_k$ の 2 等分点，すなわち $[2]\mathcal{D}_{k+1} = \mathcal{D}_k$ を満足する点であるとする．このとき明らかに $\mathcal{D}_{k+1} \in \mathbb{J}_C[2^{k+1}] \setminus \mathbb{J}_C[2^k]$ である．さらに，$\mathcal{D}_k$ の 2 等分点の集合を

$$H_{\mathcal{D}_k} := \left\{\mathcal{D} \in \mathbb{J}_C[2^{k+1}] \setminus \mathbb{J}_C[2^k] \mid [2]\mathcal{D} = \mathcal{D}_k\right\} \tag{2.4}$$

と書く．

3. $\mathbb{J}_C$ の 2 冪ねじれ点の計算

本節では，Gaudry と Harley [5] が提案し Gaudry と Schost [6] が改良を行った種数 2 の超楕円曲線 C に関する $\mathbb{J}_C$ の 2 冪ねじれ点計算アルゴリズムの概略を示す．アルゴリズムの詳細については [4–6] を参照されたい．

このアルゴリズムは，任意の $\mathcal{D}_1 \in \mathbb{J}_C[2] \setminus \{0\}$ を初期値としてその 2 等分点の 1 つ $\mathcal{D}_2 \in \mathbb{J}_C[4] \setminus \mathbb{J}_C[2]$ を求め，さらに得られた点に対し 2 等分計算を繰り返し冪指数の大きい 2 冪ねじれ点を順に求めていくものである．以下では [5, 6] に従って与えられた $\mathcal{D}_k \in \mathbb{J}_C[2^k] \setminus \mathbb{J}_C[2^{k-1}]$ に対する 2 等分点 $\mathcal{D}_{k+1} \in \mathbb{J}_C[2^{k+1}] \setminus \mathbb{J}_C[2^k]$ の計算について説明する．以下では自然数 k および $\mathcal{D}_k \in \mathbb{J}_C[2^k] \setminus \mathbb{J}_C[2^{k-1}]$ を固定し，$\mathbb{F}_q$ を $\mathcal{D}_k$ が定義される体とする．

まず，変数 U_0, U_1, V_0, V_1 を用いて C を $\mathbb{F}_p(U_0, U_1, V_0, V_1)$ 上の曲線とみなし，

$$\mathbf{D}_{k+1} = (X^2 + U_1X + U_0, V_1X + V_0) \in \mathbb{J}_C(\mathbb{F}_p(U_0, U_1, V_0, V_1)) \tag{3.1}$$

とおく．次に，$\mathbf{D}_{k+1}$ に対し $\mathbf{D}_k = [2]\mathbf{D}_{k+1}$ を計算し $\mathbf{D}_k = \mathcal{D}_k$ とすることで，変数 U_0, U_1, V_0, V_1 に関する方程式系を得る．また，$\mathbf{D}_{k+1}$ に対し条件 (2.2) を適用することで変数 U_0, U_1, V_0, V_1 に関する方程式系がさらに得られる．これらの方程式系を Gröbner 基底計算を用いて簡約化することで以下で与えられる形式の方程式系が得られる．

$$M_1(U_1) = 0, U_0 = M_0(U_1), V_1 = L_1(U_1), V_0 = L_0(U_1) \tag{3.2}$$

ここで M_1, M_0, L_1, $L_0 \in \mathbb{F}_q[U_1]$ である．また，多くの場合 $\deg M_0, \deg L_1, \deg L_0 < \deg M_1 = 16$ であり M_1 は重根を持たない．本論文ではこの条件が成立する場合を対象とし，M_1 は $\deg M_1 = 16$ かつ重根を持たないことを仮定する．

尚，現状の計算環境と Gröbner 基底計算アルゴリズムにより (3.2) の一般的な記述を得ることは困難であると考えられる．実際 [5, 6] では (3.2) の一般的な記述を与えておらず，(2.1) で与えられる曲線 C のパラメータを固定した上で (3.2) を得ている．

式 (3.2) に現れる多項式 M_1 の根を $\alpha \in \overline{\mathbb{F}}_q$ とすると，(3.1)，(3.2) より

$$\mathcal{D}_{k+1} = (X^2 + \alpha X + M_0(\alpha), L_1(\alpha) + L_0(\alpha)) \tag{3.3}$$

である．ここで，M_1 の 16 個の異なる根 α それぞれに対し異なる $\mathcal{D}_{k+1}$ が定まり，(2.3) よりこれらが $H_{\mathcal{D}_k}$ のすべてを尽くしていることに注意されたい．

以上の議論より，M_1 の根を求めれば $\mathcal{D}_k \in \mathbb{J}_C[2^k] \setminus \mathbb{J}_C[2^{k-1}]$ に対し $\mathcal{D}_{k+1} \in \mathbb{J}_C[2^{k+1}] \setminus \mathbb{J}_C[2^k]$ を求めたこととなる．

Gaudry と Harley [5] は一般的な多項式因子分解アルゴリズムを用いて M_1 の根を求めていた．しかし，一般に $\alpha \in \mathbb{F}_q$ とは限らず，k の増加に従って $\mathcal{D}_k$ の定義される体 $\mathbb{F}_q$ の拡大次数 d も増加する．その結果，冪指数 k の増加に従って M_1 の求根は困難となる．そ

こで，Gaudry と Schost [6] は，Hanrot と Morain [7] によって得られた知見を応用し 2 ねじれ群の 2 冪ねじれ点への自然な作用を利用することでこの M_1 の求根の高速化を行った．以下では，[6] が提案した M_1 の求根計算の概略を示す．

式 (3.2) より (3.1) を $R := \mathbb{F}_q[U_1]/(M_1)$ 上の多項式の組とみなすことが可能である．そこで C を R 上の曲線とみなし

$$\mathbf{D}_{k+1} = (X^2 + U_1 X + M_0, L_1 X + L_0) \in \mathbb{J}_C(R) \tag{3.4}$$

とおく．ここで，M_0, L_1, $L_0 \in \mathbb{F}_q[U_1]$ は (3.2) で定められた多項式である．このとき，任意の $g \in \mathbb{J}_C[2] \subset \mathbb{J}_C(R)$ に対し $\mathbf{D}_{k+1} + g$ を R 上で計算可能である．そこで $U_1^{(g)}$, $U_0^{(g)}$, $V_1^{(g)}$, $V_0^{(g)} \in R$ を

$$\mathbf{D}_{k+1} + g = (X^2 + U_1^{(g)} X + U_0^{(g)}, V_1^{(g)} X + V_0^{(g)}) \tag{3.5}$$

で定義すると，その構成から $U_1^{(g)} \in R$ の $\mathbb{F}_q$ 上の最小多項式は M_1 となる．さらに $\mathbb{J}_C[2]$ の部分群 G に対し，

$$s_G := \sum_{g \in G} U_1^{(g)} \in R \tag{3.6}$$

とすると，s_G の $\mathbb{F}_q$ 上の最小多項式 $\tilde{T}$ は M_1 の根の部分和を根とする多項式となり，$G \neq \{0\}$ ならば $\deg \tilde{T} < \deg M_1$ である．ここで，$s \in R$ の $\mathbb{F}_q$ 上の最小多項式は，代入写像

$$\begin{aligned} \psi_s : \mathbb{F}_q[X] &\to R \\ f &\mapsto f(s) \end{aligned}$$

の核 $\ker \psi_s$ のモニック生成多項式である．したがって，この最小多項式が $\mathbb{F}_q$ 上既約であるとは限らないことに注意されたい．多項式の剰余環の元の最小多項式については [20, Section 17.5] 等を，その計算法については [20, Section 18.2] 等を参照されたい．

いま，$\mathbb{J}_C[2]$ の部分群の系列

$$\mathbb{J}_C[2] \supsetneq G_3 \simeq (\mathbb{Z}/2\mathbb{Z})^3 \supsetneq G_2 \simeq (\mathbb{Z}/2\mathbb{Z})^2 \supsetneq G_1 \simeq (\mathbb{Z}/2\mathbb{Z}) \supsetneq G_0 = \{0\} \tag{3.7}$$

を考え，それぞれの G_i, $0 \leq i \leq 3$ に対して s_{G_i} を計算すれば，それぞれの $\mathbb{F}_q$ 上の最小多項式 $\tilde{T}_i$ は $8 \deg \tilde{T}_3 = 4 \deg \tilde{T}_2 = 2 \deg \tilde{T}_1 = \deg \tilde{T}_0 = 16$ を満足する．そこでまず s_{G_3} の $\mathbb{F}_q$ 上の最小多項式 $T_3 = \tilde{T}_3 \in \mathbb{F}_q[X]$ とその根 $\alpha_3 \in \overline{\mathbb{F}}_q$ を求め，次に s_{G_2} に対し根の和が α_3 となる $\mathbb{F}_q(\alpha_3)$ 上の最小多項式 T_2 とその根 $\alpha_2 \in \overline{\mathbb{F}}_q$ を求めるという操作を順次繰り返すことで，M_1 のある根 α に関する M_1 の根の部分和 $s_{G_i}(\alpha) = \alpha_i$ を根にもつ多項式 T_i の列

$$T_3 \in \mathbb{F}_q[X],\ T_2 \in \mathbb{F}_q(\alpha_3)[X],\ T_1 \in \mathbb{F}_q(\alpha_3, \alpha_2)[X],\ T_0 \in \mathbb{F}_q(\alpha_3, \alpha_2, \alpha_1)[X] \tag{3.8}$$

が得られる．ここで $\deg T_i = 2$ である．また T_0 の根 α_0 に対し $M_1(\alpha_0) = 0$ である．したがって，T_0 の根を求めることで M_1 の根を求めることが可能である．実際には T_i を得るために α_{i+1} が必要であることから，M_1 の根を求めるために 2 次多項式の求根 4 回が必要である．なお，T_{i+1} が可約のとき，T_i はこの α_{i+1} の選択に依存することに注意されたい．

Gaudry と Schost [6] はこの計算によって，83bit の素体上の種数 2 の超楕円曲線の 2^{10} ねじれ点の計算を行った．また，この結果を用いてこの曲線の位数計算に成功した．著者らの知る限り，これは素体上の超楕円曲線の位数計算の現状の記録である．

しかし，この方法を用いても 2 冪ねじれ点計算において M_1 の求根が最も計算時間を必要とする部分である．また，この M_1 の求根計算においては T_3, T_2, T_1, T_0 の求根計算の時間が支配的である．特に，T_i, $0 \leq i \leq 2$ は一般に $\mathbb{F}_q$ の拡大体上の多項式となるため，一般に i の減少とともにその求根計算の計算量が増加する．

一方，Gaudry と Schost [6] は実験結果から 2^k ねじれ点が $\mathbb{F}_p$ の（$O(16^k)$ 次拡大ではなく）$O(2^k)$ 次拡大に存在すると推測している．これは，$M_1 \in \mathbb{F}_q[U_1]$ が 2 次以下の既約因子を持つことを意味する．したがって，この特性を利用することでアルゴリズムの高速化が計れると考えられる．しかし，[6] ではこの特性を利用していなかった．

4. 2 冪ねじれ点計算の改良

本節では，(2.4) で定義した $H_{\mathcal{D}_k}$ への $\mathbb{J}_C[2]$ の (3.5) で与えられた作用を解析し，その結果を用いて Gaudry と Schost [6] の示した 2 冪ねじれ点計算の改良を行う．

4.1 M_1 の既約因子の性質

[6] は (3.2) で与えられた $M_1 \in \mathbb{F}_q[U_1]$ が $\mathbb{F}_q$ 上 2 次以下の既約因子を持つことを推測した．本節ではこの結果をさらに拡張し M_1 の既約因子の分解パターンを正確に与える．また，この性質を用いた M_1 の求根計算の改良について議論する．そのために，まず (3.5) で与えられた $g \in \mathbb{J}_C[2]$ の作用に関する基本的な性質を以下の補題 4.1 で明示する．[6] においてもこの補題 4.1 を暗に仮定した議論がなされていることに注意されたい．

補題 4.1 $\mathcal{D}_k \in \mathbb{J}_C[2^k] \setminus \mathbb{J}_C[2^{k-1}]$ に対し $\mathcal{D}_{k+1} \in H_{\mathcal{D}_k}$ ならば，

$$H_{\mathcal{D}_k} = \{\mathcal{D}_{k+1} + g \mid g \in \mathbb{J}_C[2]\}$$

である．

証明 $S := \{\mathcal{D}_{k+1} + g \mid g \in \mathbb{J}_C[2]\}$ とする．すると任意の $g \in \mathbb{J}_C[2]$ に対し $[2](\mathcal{D}_{k+1} + g) = \mathcal{D}_k$ であるので $H_{\mathcal{D}_k} \supset S$ である．逆に任意の $\mathcal{D} \in H_{\mathcal{D}_k}$ に対し $[2](\mathcal{D}_{k+1} - \mathcal{D}) = 0$ であるから，$\mathcal{D}_{k+1} - \mathcal{D} \in \mathbb{J}_C[2]$ であり，したがって $H_{\mathcal{D}_i} \subset S$ である． □

次に，以下の補題により $\mathbb{J}_C[2^k]$ の生成系の一つを与える．

補題 4.2 $\mathcal{D}_k \in \mathbb{J}_C[2^k] \setminus \mathbb{J}_C[2^{k-1}]$ に対し $(\mathcal{D}_k, \mathcal{D}_k^p, \mathcal{D}_k^{p^2}, \mathcal{D}_k^{p^3})$ は $\mathbb{J}_C[2^k]$ を生成する．

証明 $\mathcal{D}_1 := [2^{k-1}]\mathcal{D}_k$ とおくと，$\mathcal{D}_1 \in \mathbb{J}_C[2] \setminus \{0\}$ である．したがって，$i \in \mathbb{N}$ に対し $\mathcal{D}_1^{p^i} \in \mathbb{J}_C[2] \setminus \{0\}$ である．また，F が $\mathbb{F}_p$ 上既約であるから，$0 \leq i, j \leq 3$ に対し $i \neq j$ ならば $\mathcal{D}_1^{p^i} \neq \mathcal{D}_1^{p^j}$ である．したがって，(2.3) より $(\mathcal{D}_1, \mathcal{D}_1^p, \mathcal{D}_1^{p^2}, \mathcal{D}_1^{p^3})$ は $\mathbb{J}_C[2]$ を生成する．

次に，$1 \leq i < k$ に対し $\mathcal{D}_i := [2^{k-i}]\mathcal{D}_k$ とおき，$(\mathcal{D}_i, \mathcal{D}_i^p, \mathcal{D}_i^{p^2}, \mathcal{D}_i^{p^3})$ が $\mathbb{J}_C[2^i]$ を生成すると仮定する．すると任意の $\mathcal{D} \in \mathbb{J}_C[2^{i+1}]$ に対し

$$[2]\mathcal{D} = \sum_{j=0}^{3} [a_j]\mathcal{D}_i^{p^j},\ a_j \in [0, 2^i - 1]$$

と書ける．さらに $0 \leq j \leq 3$ に対して $\mathcal{D}_i^{p^j} = [2]\mathcal{D}_{i+1}^{p^j}$ であるから，

$$[2]\mathcal{D} = [2]\sum_{j=0}^{3} [a_j]\mathcal{D}_{i+1}^{p^j},\ a_j \in [0, 2^i - 1]$$

である．したがって $\mathcal{D} - \sum_{j=0}^{3} [a_j]\mathcal{D}_{i+1}^{p^j} \in \mathbb{J}_C[2]$ であり，$(\mathcal{D}_1, \mathcal{D}_1^p, \mathcal{D}_1^{p^2}, \mathcal{D}_1^{p^3})$ を用いて，

$$\mathcal{D} - \sum_{j=0}^{3} [a_j]\mathcal{D}_{i+1}^{p^j} = \sum_{j=0}^{3} [b_j]\mathcal{D}_1^{p^j},\ b_j \in [0, 1]$$

と書ける．$0 \leq j \leq 3$ に対し $\mathcal{D}_1^{p^j} = [2^i]\mathcal{D}_{i+1}^{p^j}$ であるから，

$$\mathcal{D} = \sum_{j=0}^{3} [a_j]\mathcal{D}_{i+1}^{p^j} + \sum_{j=0}^{3} [b_j][2^i]\mathcal{D}_{i+1}^{p^j} = \sum_{j=0}^{3} [a_j + 2^i b_j]\mathcal{D}_{i+1}^{p^j}$$

と書ける．したがって，$(\mathcal{D}_{i+1}, \mathcal{D}_{i+1}^p, \mathcal{D}_{i+1}^{p^2}, \mathcal{D}_{i+1}^{p^3})$ は $\mathbb{J}_C[2^{i+1}]$ を生成する．以上から，帰納法により $(\mathcal{D}_k, \mathcal{D}_k^p, \mathcal{D}_k^{p^2}, \mathcal{D}_k^{p^3})$ は $\mathbb{J}_C[2^k]$ を生成する． □

以上で示した補題 4.1, 4.2 より，以下に示す補題 4.3 を得る．

補題 4.3 $\mathcal{D}_k \in \mathbb{J}_C[2^k](\mathbb{F}_q) \setminus \mathbb{J}_C[2^{k-1}]$ に対し (3.2) で与えられた $M_1 \in \mathbb{F}_q[U_1]$ は高々 2 次の既約因子を持つ．

証明 任意の $\mathcal{D}_{k+1} \in H_{\mathcal{D}_k}$ に対し $\mathcal{D}_{k+1}^q \in H_{\mathcal{D}_k}$ であるので，補題 4.1 より $\mathcal{D}_{k+1}^q = \mathcal{D}_{k+1} + g$ を満足する $g \in \mathbb{J}_C[2]$ が存在する．また, 補題 4.2 より $\mathbb{J}_C[2] \subset \mathbb{J}_C[2^k] \subset \mathbb{J}_C(\mathbb{F}_q)$ であるから，$g^q = g$ が成立する．したがって，

$$\mathcal{D}_{k+1}^{q^2} = (\mathcal{D}_{k+1} + g)^q = \mathcal{D}_{k+1}^q + g = (\mathcal{D}_{k+1} + g) + g = \mathcal{D}_{k+1} + [2]g = \mathcal{D}_{k+1}$$

より $\mathcal{D}_{k+1} \in \mathbb{J}_C(\mathbb{F}_{q^2})$ である．故に，(3.3) より M_1 の任意の根 α に対し $\alpha \in \mathbb{F}_{q^2}$ である． □

補題 4.3 より M_1 の既約因子は 1 次か 2 次であるので，M_1 の既約因子の分解パターンとして (i) すべて 1 次，(ii) すべて 2 次，(iii) 1 次因子と 2 次因子が混在の 3 パターンが考えられる．しかし，実際には以下に示す補題 4.4 によって (iii) は現れない．

補題 4.4 $\mathcal{D}_k \in \mathbb{J}_C[2^k](\mathbb{F}_q) \setminus \mathbb{J}_C[2^{k-1}]$ に対し (3.2) で与えられた $M_1 \in \mathbb{F}_q[U_1]$ の既約因子はすべて同次である．

証明 M_1 の根 $\alpha \in \mathbb{F}_q$ が存在すると仮定する．すると，(3.3) より α に対応する $\mathcal{D}_{k+1} \in \mathbb{J}_C(\mathbb{F}_q)$ が得られる．また，M_1 の根 $\beta \neq \alpha$ を (3.3) に代入して得られる $\mathcal{D}_k$ の 2 等分点を $\mathcal{D}$ とする．補題 4.1, 4.2 より，この $\mathcal{D}$ に対し $\mathcal{D} = \mathcal{D}_{k+1} + g$ を満足する $g \in \mathbb{J}_C[2] \subset \mathbb{J}_C(\mathbb{F}_q)$ が存在する．したがって，$\mathcal{D} \in \mathbb{J}_C(\mathbb{F}_q)$ である．よって M_1 が 1 次の既約因子を持つとき，他のすべての既約因子も 1 次である．一方，補題 4.3 より，M_1 が 1 次の既約因子を持たないとき M_1 の根はすべて $\mathbb{F}_{q^2}$ で定義され，M_1 のすべての既約因子は 2 次である． □

以上により，$\mathcal{D}_k \in \mathbb{J}_C[2^k](\mathbb{F}_q) \setminus \mathbb{J}_C[2^{k-1}]$ に対し (3.2) で与えられた $M_1 \in \mathbb{F}_q[U_1]$ は (i) 1 次の既約因子のみに分解，または (ii) 2 次の既約因子のみに分解することが示された．

(i) の場合，(3.8) で与えられた T_0 は $\mathbb{F}_q$ 上可約である．したがってこのとき $0 \leq i \leq 3$ に対し $T_i \in \mathbb{F}_q[X]$ であり，[6] の方法で十分な効果が得られる．また，後に述べるように一般には M_1 の分解パターンは (ii) となり (i) の場合は k が小さいときにのみ起こりうるので，この場合についての改良はその効果が期待できない．そこで，(i) の場合は [6] の方法により 2 冪ねじれ点を計算することとし，以下では (ii) の場合のみを考慮する．

(ii) の場合は T_i, $0 \leq i \leq 2$ の定義体に関し，

$$T_{i+1} \in \mathbb{F}_{q^2}[X] \setminus \mathbb{F}_q[X] \Rightarrow T_i \in \mathbb{F}_{q^2}[X] \setminus \mathbb{F}_q[X]$$

を満足する 4 通りの可能性がある．したがって，これらの可能性により 2 冪ねじれ点の計算時間が一定しない．例えば $T_3 \in \mathbb{F}_q[X]$, $T_2, T_1, T_0 \in \mathbb{F}_{q^2}[X] \setminus \mathbb{F}_q[X]$ の場合は $\mathbb{F}_q$ 上の 2 次多項式の求根 1 回と $\mathbb{F}_{q^2}$ 上の 2 次多項式の求根 3 回が必要であるのに対し，$T_3, T_2, T_1, T_0 \in \mathbb{F}_q[X]$, $0 \leq i \leq 3$ の場合は，$\mathbb{F}_q$ 上の 2 次多項式の求根 3 回で 2 冪ねじれ点が計算可能であり[*1]，計算量が少なくなる．一方，M_1 の計算過程に現れる (3.7) で与えられた G_i, $1 \leq i \leq 3$ はその取りかたに任意性がある．そこで，以下では G_i の選択により $T_3, T_2, T_1, T_0 \in \mathbb{F}_q[X]$ とする方法を検討する．

[*1] この場合には T_0 の根が $\mathbb{F}_q$ 上存在しないことが明らかなので，T_0 に対しては求根計算を行う代わりに $\mathbb{F}_{q^2} \cong \mathbb{F}_q[X]/T_0$ とする．

4.2 M_1 の共役根の置換を与える 2 ねじれ点の利用

本節では，(3.8) で与えられた T_i, $0 \leq i \leq 3$ が $T_i \in \mathbb{F}_q[X]$ を満足するための (3.7) で与えられた G_i, $1 \leq i \leq 3$ の選択方法を示す．さらに，冪指数 k を増加させて 2^k ねじれ点計算を行ったときに G_i を再選択する必要がないことを示す．これにより，大きな k に対し 2^k ねじれ点を計算する場合においても G_i, $1 \leq i \leq 3$ の選択は多くの場合より小さな k において一度行えばよいこととなり，実際の 2^k ねじれ点計算の効率化が可能である．

以上を示すために，まず (3.5) で与えられた $g \in \mathbb{J}_C[2]$ の作用に関する基本的な性質を以下の補題 4.5 で明示する．[6] では補題 4.1 と同様に補題 4.5 を部分的に仮定した議論がなされていることに注意されたい．

補題 4.5 $\mathcal{D}_k \in \mathbb{J}_C[2^k](\mathbb{F}_q) \setminus \mathbb{J}_C[2^{k-1}]$ に対し $\mathcal{D}_{k+1} \in H_{\mathcal{D}_k}$ とする．このとき $g = \mathcal{D}_{k+1}^q - \mathcal{D}_{k+1}$ を満足する $g \in \mathbb{J}_C[2]$ が $\mathcal{D}_{k+1}$ に依らずに定まる．

証明 $\mathcal{D} \in H_{\mathcal{D}_k}$ とする．$\mathcal{D}^q \in H_{\mathcal{D}_k}$ より，補題 4.1 から $g = \mathcal{D}^q - \mathcal{D}$ を満足する $g \in \mathbb{J}_C[2]$ が存在する．さらに，補題 4.1 より任意の $\mathcal{D}_{k+1} \in H_{\mathcal{D}_k}$ に対し $\mathcal{D} + \tilde{g}$ を満足する $\tilde{g} \in \mathbb{J}_C[2]$ が存在し，$\tilde{g}^q = \tilde{g}$ である．したがって，

$$\mathcal{D}_{k+1}^q - \mathcal{D}_{k+1} = (\mathcal{D} + \tilde{g})^q - (\mathcal{D} + \tilde{g}) = \mathcal{D}^q - \mathcal{D} + \tilde{g}^q - \tilde{g} = g$$

であり，g は $\mathcal{D}_{k+1}$ の取りかたに依らない． □

補題 4.5 で与えられた $g \in \mathbb{J}_C[2]$ は $H_{\mathcal{D}_k}$ に対し q 乗 Frobenius 写像として作用する．一方，T_0 の 2 根は M_1 の根に含まれるので (3.7) で与えられた G_1 を生成する 2 ねじれ点を M_1 の根の置換とみなすことが可能である．したがって，この 2 ねじれ点を q 乗 Frobenius 写像すなわち補題 4.5 で与えた $g \in \mathbb{J}_C[2] \setminus \{0\}$ とすれば，$T_0 \in \mathbb{F}_q[X]$ となる．さらにこの g を効率的に選択可能であれば M_1 の求根が高速に行えることとなる．

補題 4.5 で与えた $g \in \mathbb{J}_C[2] \setminus \{0\}$ の選択方法を与える前に，冪指数 k を増加させて 2^k ねじれ点計算を行ったときにも，この g がその性質を保持することを以下の補題 4.6 で示す．

補題 4.6 $k \geq 2$ に対し $\mathcal{D}_k \in \mathbb{J}_C[2^k](\mathbb{F}_q) \setminus \mathbb{J}_C[2^{k-1}]$ とする．また，$\mathcal{D}_{k+1} \in H_{\mathcal{D}_k}$, $\mathcal{D}_{k+2} \in H_{\mathcal{D}_{k+1}}$ とする．このとき，$\mathcal{D}_{k+1}^q - \mathcal{D}_{k+1} = \mathcal{D}_{k+2}^{q^2} - \mathcal{D}_{k+2}$ である．

証明 補題 4.5 より

$$[2](\mathcal{D}_{k+2}^q - \mathcal{D}_{k+2}) = ([2]\mathcal{D}_{k+2})^q - [2]\mathcal{D}_{k+2} = \mathcal{D}_{k+1}^q - \mathcal{D}_{k+1} \in \mathbb{J}_C[2]$$

が成立するから，補題 4.2 を用いると $\mathcal{D}_{k+2}^q - \mathcal{D}_{k+2} \in \mathbb{J}_C[4] \subset \mathbb{J}_C[2^k] \subset \mathbb{J}_C(\mathbb{F}_q)$ であり，

$\mathcal{D}_{k+2}^q - \mathcal{D}_{k+2} = (\mathcal{D}_{k+2}^q - \mathcal{D}_{k+2})^q$ である．したがって，

$$\begin{aligned}\mathcal{D}_{k+1}^q - \mathcal{D}_{k+1} &= [2](\mathcal{D}_{k+2}^q - \mathcal{D}_{k+2}) = (\mathcal{D}_{k+2}^q - \mathcal{D}_{k+2})^q + (\mathcal{D}_{k+2}^q - \mathcal{D}_{k+2}) \\ &= \mathcal{D}_{k+2}^{q^2} - \mathcal{D}_{k+2}^q + \mathcal{D}_{k+2}^q - \mathcal{D}_{k+2} = \mathcal{D}_{k+2}^{q^2} - \mathcal{D}_{k+2}\end{aligned}$$

である． □

補題 4.6 は $\mathbb{J}_C[2^k]$ の冪指数 k を増加させて 2 冪ねじれ点計算を行ったときにも補題 4.5 で与えた $g \in \mathbb{J}_C[2] \setminus \{0\}$ がその性質を保持することを示している．さらに，$\mathcal{D}_k \in \mathbb{J}_C[2^k](\mathbb{F}_q) \setminus \mathbb{J}_C[2^{k-1}]$ に対し $\mathcal{D}_{k+1} \in H_{\mathcal{D}_k}$ が $\mathcal{D}_{k+1} \in \mathbb{J}_C(\mathbb{F}_{q^2}) \setminus \mathbb{J}_C(\mathbb{F}_q)$ を満足するとき，$\mathcal{D}_{k+1}^q - \mathcal{D}_{k+1} = \mathcal{D}_{k+2}^{q^2} - \mathcal{D}_{k+2} \neq 0$ であり，したがってこのとき $\mathcal{D}_{k+2} \in \mathbb{J}_C(\mathbb{F}_{q^4}) \setminus \mathbb{J}_C(\mathbb{F}_{q^2})$ が成立する．すなわち，冪指数 k を増加させながら 2^k ねじれ点を計算して行く場合，ある k において (3.2) で与えられた M_1 の既約因子がすべて 2 次であったならば，以降の $k+1, k+2, \ldots$ に対しても M_1 の既約因子はすべて 2 次である．したがって，g の選択は M_1 の既約因子がすべて 2 次となった k において 1 回行えばよいことが判る．

以上の補題 4.5, 4.6 をまとめ，以下の定理 4.7 を得る．

定理 4.7 $k \geq 2$ とする．$\mathcal{D}_k \in \mathbb{J}_C[2^k](\mathbb{F}_q)$ に対し $\mathcal{D}_{k+1} \in H_{\mathcal{D}_k}$ とし，$\mathbf{D}_{k+1}$ を $\mathcal{D}_k$ に対し (3.4) で与えられた点とする．また $\mathcal{D}_{k+1}$ に対し (3.4) で与えられた点を $\mathbf{D}_{k+2}$ と書く．

$\mathcal{D}_{k+1} \in \mathbb{J}_C(\mathbb{F}_{q^2})$ のとき，

$$\mathbf{D}_{k+1} + g = \mathbf{D}_{k+1}^q \tag{4.1}$$

を満足する $g \in \mathbb{J}_C[2]$ が存在する．さらに g は

$$\mathbf{D}_{k+2} + g = \mathbf{D}_{k+2}^{q^2}$$

を満足する．ここで，$\mathbf{D}_{k+i}^q$, $i = 1, 2$ は $\mathbf{D}_{k+i}$ の X の各次数の係数を q 乗したものを表す．

証明 $\mathcal{D}_k$，$\mathcal{D}_{k+1}$ に対し (3.2) で与えられた M_1 をそれぞれ $M_1^{(k+1)}$, $M_1^{(k+2)}$ と書く．(3.3) より $M_1^{(k+1)}$ の各根 α_i, $1 \leq i \leq 16$ に対し $\mathbf{D}_{k+1}(\alpha_i) \in H_{\mathcal{D}_k}$ が得られる．また，補題 4.5 より

$$g = \mathbf{D}_{k+1}^q(\alpha_i) - \mathbf{D}_{k+1}(\alpha_i),\ 1 \leq i \leq 16$$

を満足する $g \in \mathbb{J}_C[2]$ が存在する．したがって，中国の剰余定理より，$g = \mathbf{D}_{k+1}^q - \mathbf{D}_{k+1}$ を得る．さらに $M_1^{(k+2)}$ の根を β_i とすると，補題 4.5, 4.6 より $\mathbf{D}_{k+2}(\beta_i) \in H_{\mathcal{D}_{k+1}}$ は

$$g = \mathbf{D}_{k+2}^{q^2}(\beta_i) - \mathbf{D}_{k+2}(\beta_i),\ 1 \leq i \leq 16$$

を満足する．したがって，中国の剰余定理より，$g = \mathbf{D}_{k+2}^{q^2} - \mathbf{D}_{k+2}$ を得る． □

以下では，この定理 4.7 から，補題 4.5 で与えた $g \in \mathbb{J}_C[2] \setminus \{0\}$ の選択方法を導く．

式 (4.1) と (3.5) を比較し (3.5) の第 1 成分の X の 1 次係数から

$$U_1^{(g)} \equiv U_1^q \bmod M_1 \tag{4.2}$$

を得る．したがって，ランダムに選択した $g \in \mathbb{J}_C[2] \setminus \{0\}$ に対し $U_1^{(g)}$ を計算し $U_1^q \bmod M_1$ と比較することで補題 4.5 を満足する g を得ることが可能である．

以上より，$k \geq 2$ のとき，式 (4.2) を満足する $g \in \mathbb{J}_C[2] \setminus \{0\}$ を選択し，この g を用いて補題 4.2 により $G_1 := \langle g \rangle, G_2 := \langle g, g^p \rangle, G_3 := \langle g, g^p, g^{p^2} \rangle$ とする．このとき，(3.6) から得られる s_{G_1}, s_{G_2}, s_{G_3} は M_1 の任意の根 α に対し $s_{G_1}(\alpha), s_{G_2}(\alpha), s_{G_3}(\alpha) \in \mathbb{F}_q$ を満足し，したがって (3.8) で与えられた T_1, T_2, T_3 は $T_1, T_2, T_3 \in \mathbb{F}_q[X]$ を満足する．

式 (4.2) を満足する $g \in \mathbb{J}_C[2] \setminus \{0\}$ の計算において，$M_1 \in \mathbb{F}_q[U_1]$ に対する $U_1^q \bmod M_1$ の計算時間が支配的である．しかし，これは一般に小さな冪指数 k において一度行えばよく，またこのとき定理 4.7 より $\mathbb{F}_q$ は 2^2 ねじれ点の定義される体である．いま，(2.1) の F を $\mathbb{F}_p$ 上既約と仮定していることから 2 ねじれ点は $\mathbb{F}_{p^5}$ 上定義されるため，補題 4.3 より $q \in \{p^5, p^{10}\}$ であることが判る．よって，大きな k に対する 2^k ねじれ点計算においてこの計算の計算時間への影響は小さい．

4.3 アルゴリズム

4.1, 4.2 節をまとめ (2.1) で定義された $\mathbb{F}_p$ 上の種数 2 の超楕円曲線 C の Jacobian の $1 \leq k \leq m$ に対する 2^k ねじれ点計算の改良アルゴリズムを Algorithm 1 に示す．

Algorithm 1 は，まずステップ 1 で $g \in \mathbb{J}_C[2] \setminus \{0\}$ を計算し，(3.7) で与えた G_i, $0 \leq i \leq 3$ をステップ 2 で構成した後に，ステップ 3 で [6] に従い $\mathcal{D}_2 \in \mathbb{J}_C[4] \setminus \mathbb{J}_C[2]$ を計算する．その後も $\mathcal{D}_k \in \mathbb{J}_C[2^k] \setminus \mathbb{J}_C[2^{k-1}]$ に対し $\mathcal{D}_{k+1} \in \mathbb{J}_C[2^{k+1}] \setminus \mathbb{J}_C[2^k]$ を [6] に従い計算し，$\mathcal{D}_k \in \mathbb{J}_C(\mathbb{F}_q)$ に対し $\mathcal{D}_{k+1} \in \mathbb{J}_C(\mathbb{F}_{q^2})$ となった時点でステップ 11, 12 において 4.2 節に従い G_i の再構成を行う．以降も，基本的に [6] に従い，ステップ 6, 14-16 で $\mathcal{D}_{k+1} \in \mathbb{J}_C[2^{k+1}] \setminus \mathbb{J}_C[2^k]$ を計算して行くものであるが，4.1, 4.2 節で示したようにこの場合 $\mathcal{D}_k \in \mathbb{J}_C(\mathbb{F}_q)$ に対し $T_i \in \mathbb{F}_q[X]$, $0 \leq i \leq 3$ であるので，T_i の求根計算の計算量は自然に削減される．T_i の求根計算に [6] は Cantor-Zassenhaus アルゴリズムの改良 [3,9] を用いている．一般に Cantor-Zassenhaus アルゴリズムでは与えられた多項式を “Distinct Degree Factorization” と呼ばれるパートで同次数の既約因子をもつ多項式に分解し，さらに得られた多項式をそれぞれ “Equal Degree Factorization” と呼ばれるパートで因子分解する．Cantor-Zassenhaus アルゴリズムの Distinct Degree Factorization は $X^q \bmod T_i$ の計算を必要とする．しかし，いま扱っている問題において Distinct Degree Factorization は T_i が 1 次因子を持つことの判定を行っているに過ぎない．一方，ステップ 14 においては求根を必要とする T_i, $1 \leq i \leq 3$ が必ず 1 次因子を持つように T_i を構成している．そこで，ステップ 14 では T_i の求根計算において Distinct Degree

Algorithm 1 種数 2 の超楕円曲線の Jacobian の 2 冪ねじれ点の計算

Input: $m \geq 2$, 種数 2 の超楕円曲線 $C : Y^2 = F(X)$, F: monic, $\mathbb{F}_p$ 上既約, $\deg F = 5$
Output: $(\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_m) \in \mathbb{J}_C[2] \setminus \{0\} \times \mathbb{J}_C[4] \setminus \mathbb{J}_C[2] \times \cdots \times \mathbb{J}_C[2^m] \setminus \mathbb{J}_C[2^{m-1}]$ s.t. $[2]\mathcal{D}_k = \mathcal{D}_{k-1}$, $2 \leq k \leq m$

1: F の因子から $g \in \mathbb{J}_C[2] \setminus \{0\}$ を計算する.
2: $G_0 \leftarrow \{0\}$, $G_1 \leftarrow \langle g \rangle$, $G_2 \leftarrow \langle g, g^p \rangle$, $G_3 \leftarrow \langle g, g^p, g^{p^2} \rangle$
3: [6] に従い $\mathcal{D}_2 \in H_g$ を計算し, $\mathcal{D}_2$ が定義される最小の体を $\mathbb{F}_q$ とする.
4: $e \leftarrow 1$
5: **for** $k = 2$ to $m - 1$ **do**
6: [6] に従い $\mathcal{D}_k$ に対し (3.2) で与えられた $M_1, M_0, L_1, L_0 \in \mathbb{F}_q[U_1]$ を計算する.
7: **if** $e = 1$ **then**
8: [6] に従い $M_1, M_0, L_1, L_0, G_i, 0 \leq i \leq 3$ より M_1 の根 α を計算する.
9: **if** $\alpha \notin \mathbb{F}_q$ **then**
10: $e \leftarrow 2$, $\mathbb{F}_q \leftarrow \mathbb{F}_{q^2}$
11: 式 (4.2) を満足する $g \in \mathbb{J}_C[2] \setminus \{0\}$ を探索する.
12: $G_1 \leftarrow \langle g \rangle$, $G_2 \leftarrow \langle g, g^p \rangle$, $G_3 \leftarrow \langle g, g^p, g^{p^2} \rangle$
13: **else**
14: 4.1, 4.2 節に従い $M_1, M_0, L_1, L_0, G_i, 0 \leq i \leq 3$ より M_1 の根 $\alpha \in \mathbb{F}_{q^2}$ を計算する.
15: $\mathbb{F}_q \leftarrow \mathbb{F}_{q^2}$
16: $\mathcal{D}_{k+1} \leftarrow (X^2 + \alpha X + M_0(\alpha), L_1(\alpha)X + L_0(\alpha))$
17: **return** $(g, \mathcal{D}_2, \ldots, \mathcal{D}_m)$

Factorization を省略し計算量をさらに削減しているものとする. Cantor-Zassenhaus アルゴリズムについては [20, Section 21.3] 等を参照されたい.

5. 改良アルゴリズムの実装

本節では, 前節で示した 2 冪ねじれ点計算の改良アルゴリズム Algorithm 1 の実装結果を示し改良の効果を確認する. 実装は代数計算システム Magma [12] で行った. 実装において Algorithm 1 のステップ 6 ではシステムの制約上 [6] で利用された方法と異なり (3.2) を求めるために各 k に対し Gröbner 基底計算を行った. また, 改良の効果を見るために, Algorithm 1 からステップ 4, 7, 9-15 を削除したアルゴリズムの実装も行った. これは本論文で示した改良を行っていないものに相当する. 以降, Algorithm 1 を "Proposed", 上記ステップを削除したアルゴリズムを "Reference" と略記する.

Algorithm 1 への入力値 $m = 10$ として Proposed, Reference のそれぞれを用いて, ランダムに選択した種数 2 の超楕円曲線 $C/\mathbb{F}_p$ の $\mathbb{J}_C$ の 2^k ねじれ点 $\mathcal{D}_k$ を $k = 2, \ldots, 10$ に対し求めた. 実験には Athlon64 2.4GHz を用いた.

$p = 10^5 + 3$ に対する結果を Table 1 に示す. Table 1 ではランダムに選択した 100 本の曲線に対する Reference, Proposed それぞれの平均計算時間を秒を単位として示した. $\mathcal{D}_k$ 列は $\mathcal{D}_{k-1}$ から $\mathcal{D}_k$ を求めるために必要とした時間を表す. また "Total" にその総

Table 1. Timing of computing a 2^k torsion point $\mathcal{D}_k$ from $\mathcal{D}_{k-1}$ for $p = 10^5 + 3$ on Athlon64 2.4GHz (sec.).

	$\mathcal{D}_3$	$\mathcal{D}_4$	$\mathcal{D}_5$	$\mathcal{D}_6$	$\mathcal{D}_7$	$\mathcal{D}_8$	$\mathcal{D}_9$	$\mathcal{D}_{10}$	Total
Reference	16	11	23	56	179	693	1560	6731	9269
Proposed	17	10	20	41	98	255	782	1876	3100

Table 2. Timing of computing a 2^k torsion point $\mathcal{D}_k$ from $\mathcal{D}_{k-1}$ for $p = 10^5 + 3$ on Athlon64 2.4GHz (sec.) (without Gröbner basis computation).

	$\mathcal{D}_3$	$\mathcal{D}_4$	$\mathcal{D}_5$	$\mathcal{D}_6$	$\mathcal{D}_7$	$\mathcal{D}_8$	$\mathcal{D}_9$	$\mathcal{D}_{10}$	Total
Reference	0.6	1.1	4	18	94	503	1119	5627	7366
Proposed	1.2	0.4	1	3	13	65	341	771	1197

和を示す．すなわち，Total は実際に $\mathcal{D}_{10}$ を求めるために必要とした時間を表している．尚，$\mathcal{D}_2$ を求めるために必要な時間は誤差の範囲に収まるので Table 1 には示していない．

Proposed を用いることで Reference と比較し約 1/3 の時間で $\mathcal{D}_{10}$ を得られることが Table 1 から判る．

改良の効果を詳細に見るため，Table 1 に示した値から Algorithm 1 のステップ 6 に必要とした時間，すなわち Gröbner 基底計算に必要とした時間を除いた値を Table 2 に示す．

Table 2 から $\mathcal{D}_{10}$ を求めるために必要な M_1 の求根に関し，本論文で示した改良により約 6 倍の高速化がなされたことが判る．また，Table 1 と Table 2 とを比較することで，k の増加に従って $\mathcal{D}_k$ の計算において M_1 の求根計算時間が支配的となることが判る．したがって，より大きな k に対しては改良はより大きな効果を示すことが予想される．

尚, 本実験においては, 取り扱ったすべての曲線において $\mathcal{D}_3$ の計算時に Algorithm 1 のステップ 10-12 が実行された．これにより，$\mathcal{D}_3$ の計算においては Proposed が Reference より計算時間を必要としていることが Tables 1, 2 から見て取れる．また，この計算がより大きな k に対し殆ど影響を与えないことが判る．

次に，$p = 2^{80} + 13$ に対する結果を Table 3 に示す．また，Table 2 と同様に Table 3 に示した値から Gröbner 基底計算時間を除いた値を Table 4 に示す．Tables 3, 4 ではランダムに選択した 30 本の曲線に対する Reference, Proposed それぞれの平均計算時間を秒を単位として示した．テーブルの記法は Table 1 に従う．

本実験においては Table 3 から $\mathcal{D}_{10}$ の計算に関し Proposed が Reference と比較し約 2.4 倍の高速化を実現していることが判る．また，Table 4 から $\mathcal{D}_{10}$ を求めるために必要な M_1 の求根に関しては Proposed が Reference と比較し約 2.8 倍の高速化を実現していることが判る．

$p = 10^5 + 3$ に対する結果と $p = 2^{80} + 13$ に対する結果を比較すると，本論文に示した改良は $p = 10^5 + 3$ に対してより効果が大きいことが判る．これは p の大きさに依存した性質ではなく，与えられた $\mathbb{J}_C$ の 2 ねじれ点群の 2 冪ねじれ点への作用の個別の性

Table 3. Timing of computing a 2^k torsion point $\mathcal{D}_k$ from $\mathcal{D}_{k-1}$ for $p = 2^{80} + 13$ on Athlon64 2.4GHz (sec.).

	$\mathcal{D}_3$	$\mathcal{D}_4$	$\mathcal{D}_5$	$\mathcal{D}_6$	$\mathcal{D}_7$	$\mathcal{D}_8$	$\mathcal{D}_9$	$\mathcal{D}_{10}$	Total
Reference	30	45	180	336	714	3673	15810	68923	89712
Proposed	34	46	152	271	482	1798	7165	27377	37323

Table 4. Timing of computing a 2^k torsion point $\mathcal{D}_k$ from $\mathcal{D}_{k-1}$ for $p = 2^{80} + 13$ on Athlon64 2.4GHz (sec.) (without Gröbner basis computation).

	$\mathcal{D}_3$	$\mathcal{D}_4$	$\mathcal{D}_5$	$\mathcal{D}_6$	$\mathcal{D}_7$	$\mathcal{D}_8$	$\mathcal{D}_9$	$\mathcal{D}_{10}$	Total
Reference	2	5	47	94	368	2888	13954	64450	81807
Proposed	5	4	17	43	135	1022	5349	23086	29661

Table 5. The extension degrees of the definition fields of $\mathcal{D}_k$ over $\mathbb{F}_p$.

Type	$\mathcal{D}_2$	$\mathcal{D}_3$	$\mathcal{D}_4$	$\mathcal{D}_5$	$\mathcal{D}_6$	$\mathcal{D}_7$	$\mathcal{D}_8$	$\mathcal{D}_9$	$\mathcal{D}_{10}$
I	10	20	40	80	160	320	640	1280	2560
II	10	10	20	40	80	160	320	640	1280
III	5	10	20	40	80	160	320	640	1280

Table 6. Timing of computing a 2^k torsion point $\mathcal{D}_k$ from $\mathcal{D}_{k-1}$ for $p = 2^{80} + 13$ on Athlon64 2.4GHz (sec.) (without Gröbner basis computation).

Type		$\mathcal{D}_3$	$\mathcal{D}_4$	$\mathcal{D}_5$	$\mathcal{D}_6$	$\mathcal{D}_7$	$\mathcal{D}_8$	$\mathcal{D}_9$	$\mathcal{D}_{10}$	Total
I	Reference	2	6	61	105	456	3567	16848	79211	100255
	Proposed	7	4	33	53	228	1906	9232	39360	50824
II	Reference	2	4	39	89	302	2481	12863	54665	70445
	Proposed	2	9	4	35	51	250	1955	9342	11648
III	Reference	1	4	32	82	285	2180	10557	49657	62797
	Proposed	2	2	4	33	54	247	1950	8549	10841

質に依存するものである．この説明のために，まず本実験において得られた $\mathcal{D}_k$ の最小定義体の拡大次数を示す．Algorithm 1 を実行し $(\mathcal{D}_2, \ldots, \mathcal{D}_{10})$ 求めた結果，これらの定義体の $\mathbb{F}_p$ 上の拡大次数は Table 5 に示す Type I–III の 3 種類に分類された．より詳細には，$p = 10^5 + 3$ に対しては，100 本の曲線全てに対し $\mathcal{D}_k$ の拡大次数は Type I であった．一方 $p = 2^{80} + 13$ については，30 本のうち Type I が 14 本，II が 6 本，III が 10 本であった．それぞれのタイプにより $\mathcal{D}_k$ の計算時間が異なることは明らかであるので，$p = 2^{80} + 13$ に対し Gröbner 基底計算時間を除いた計算時間の各タイプ毎の平均を Table 6 に示す．Table 6 から $p = 2^{80} + 13$ のとき Type I の場合のみ改良の効果が小さいことが判る．本実装においては効率化のため Algorithm 1 のステップ 1 で F の根 γ に対し $g = (X - \gamma, 0)$ としている．$p = 2^{80} + 13$ の場合の Type I の曲線に対し，このように選択した g を用いて計算された (3.8) の T_0 は全て $\mathbb{F}_q$ 上既約であった．すなわち，本論文で述べた改良の一つである Algorithm 1 のステップ 12 における g の変更が不要であっ

た．しかし，この場合においても Reference では本論文で示した性質を用いていないため $T_i, i = 0, \ldots, 3$ の求根計算において Distinct Degree Factorization を必要とする．実際，これを必要としない Proposed と比較し約 2 倍の計算時間を必要としていることが Table 6 からわかる．したがって，$p = 2^{80} + 13$ の場合の Type I の曲線のような特殊ケースにおいても，本論文で示した改良は明らかな効果を持つものと考えられる．

6. 終わりに

本論文では，安全な超楕円曲線暗号の構成を目的とし，種数 2 の超楕円曲線に対する Schoof アルゴリズムに必要となる 2 冪ねじれ点計算の改良を行った．本論文では，まず 2 冪ねじれ点の 2 等分点の性質と 2 ねじれ群のそれらへの作用の性質を明らかにした．そしてこれらの性質を用いた 2 冪ねじれ点計算の改良アルゴリズムを示した．また，実装実験により実用サイズの計算において提案アルゴリズムを用いることで 2 冪ねじれ点計算の効率が 2 から 6 倍程度向上することを確認した．

謝辞 貴重なご助言を頂いた編集委員と匿名査読者の方々に感謝いたします．

参考文献

[1] H. Cohen, G. Frey, and C. Doche (eds.), Handbook of elliptic and hyperelliptic curve cryptography, Chapman & Hall/CRC, Boca Raton, 2005.

[2] J. Denef and F. Vercauteren, An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2, J. Cryptology, Vol. 19 No. 1 (2006), 1–25.

[3] J. von zur Gathen and V. Shoup, Computing Frobenius maps and factoring polynomials, Proc. of the twenty-fourth annual ACM symposium on the theory of computing, 1992, 97–105.

[4] P. Gaudry and É. Schost, Point counting on curves of genus 2 defined over a large prime field, 2003 International symposium on next generation cryptography and related mathematics in Chuo University, `http://www.loria.fr/~gaudry/publis/Japon.ps.gz`, 2003.

[5] P. Gaudry and R. Harley, Counting points on hyperelliptic curves over finite fields, ANTS-IV, Springer-Verlag LNCS 1838, 2000, 313–332.

[6] P. Gaudry and É. Schost, Construction of secure random curves of genus 2 over prime fields, EUROCRYPT 2004, Springer-Verlag LNCS 3027, 2004, 239–256.

[7] G. Hanrot and F. Morain, Solvability by radicals from an algorithmic point of view, Proc. of ISSAC 2001, 2001, 175–182.

[8] 伊豆 哲也, 小暮 淳, 野呂 正行, 横山 和弘, 標数 2 有限体上楕円曲線の位数計算, 電子情報通信学会論文誌 A, J82-A No. 8 (1999), 1253–1260.

[9] E. Kaltofen and V. Shoup, Fast polynomial factorization over high algebraic extensions of finite fields, Proc. of ISSAC 1997, 1997, 184–188.

[10] K. S. Kedlaya, Counting points on hyperelliptic curves using Monsky-Washinitzer cohomology, J. Ramanujan Math. Soc., Vol. 16 No. 4 (2001), 323–338.

[11] N. Koblitz, Hyperelliptic curve cryptosystems, J. Cryptology, Vol. 1 No. 3 (1989), 139–150.

[12] The Magma computational algebra system, `http://magma.maths.usyd.edu.au/magma/`.

[13] K. Matsuo, J. Chao, and S. Tsujii, Baby step giant step algorithms in point counting of hyperelliptic curves, IEICE Trans. EA, E86-A No. 5 (2003), 1127–1134.

[14] A. Menezes, S. Vanstone, and R. Zuccherato, Counting points on elliptic curves over $\mathbb{F}_{2^m}$, Math. Comp., Vol. 60 (1993), 407–420.

[15] 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.

[16] 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, Proceedings of SCIS2002, 2002, 497–502.

[17] 入海 淳, 松尾 和人, 趙 晋輝, 辻井 重男, 超楕円曲線上の Harley アルゴリズムにおける resultant 計算について, 信学技研 ISEC, Vol. 16 No. 51 (2006), 29–35.

[18] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, Math. Comp., Vol. 44 (1985), 483–494.

[19] R. Schoof, Counting points on elliptic curves over finite fields, J. Théorie des Nombers de Bordeaux, Vol. 7 (1995), 219–254.

[20] V. Shoup, A computational introduction to number theory and algebra, Cambridge University Press, Cambridge, 2005.

[21] F. Vercauteren, Computing zeta functions of hyperelliptic curves over finite fields of characteristic 2, CRYPTO 2002, Springer-Verlag LNCS 2442, 2002, 369–384.

小崎 俊二 (正会員)　〒221-0835　神奈川県横浜市神奈川区鶴屋町 2-14-1
　1992 年早稲田大学大学院理工学研究科修士課程修了．2007 年情報セキュリティ大学院大学情報セキュリティ研究科修士課程修了．現在，同博士後期課程在学.

松尾 和人 (正会員)　〒221-0835　神奈川県横浜市神奈川区鶴屋町 2-14-1
　1988 年中央大理工学研究科博士前期電気工修了．同年東洋通信機（株）入社．2001 年中央大理工学研究科博士後期情報工修了．博士（工学）．2002 年中央大研究開発機構機構助教授．2003 年同機構教授．2004 年情報セキュリティ大学院大教授.