被覆攻撃の対象となる偶標数有限体上の楕円・超楕円曲線の分類に関する研究

A Classification of Elliptic and Hyperelliptic Curves over Finite Fields of Even Characteristic Subjected to the Cover Attack

情報工学専攻　20N8100018H　村井 公輔

要約　GHS 攻撃の一般化である被覆攻撃とは, 有限体 $k := \mathbb{F}_q$ の d 次拡大体 $k_d := \mathbb{F}_{q^d}$ 上定義される楕円・超楕円曲線 C_0 の離散対数問題を, k 上定義される被覆曲線 C の離散対数問題に変換する攻撃手法である. 現在, 百瀬らにより同種条件 $(g(C) = d \cdot g(C_0))$ の下で, 被覆攻撃の対象となる偶標数超楕円曲線の分類が発表されている [1]. 本論文では, 百瀬らの分類結果の検証を行い詳細な証明を与えることによって, 偶標数拡大体 k_d 上の種数 $g(C_0) = 1, 2, 3$ 楕円・超楕円曲線 C_0 に対する同種条件下での曲線の完全分類を行った. つまり存在しうる攻撃の対象となる曲線のすべてを列挙した. また, 分類表の曲線の導出方法を初めて示した.

キーワード　楕円・超楕円曲線暗号, 被覆攻撃

1　はじめに

楕円・超楕円曲線を用いた暗号は, 短い鍵長で高い安全性を持ち, さらに拡大体を用いることで効率的な実装も可能である. これらの特徴から, IoT 機器などメモリの限られた装置への実装に有効である. 一方で, この暗号技術の安全性の検証も重要となっている.

拡大体上定義される楕円・超楕円曲線が持つ, 拡大体の性質を利用した攻撃手法として GHS 攻撃がある. この攻撃は, Weil descent の手法を偶標数拡大体上の楕円曲線に適用したものである [2]. GHS 攻撃は, 奇標数拡大体上の曲線を含めて, より一般的な曲線にも適用され, 被覆攻撃として一般化されている [3]. この攻撃手法は, 有限体 $k := \mathbb{F}_q$ (q : 素数のベキ乗) の d 次拡大体 $k_d := \mathbb{F}_{q^d}$ 上定義される楕円・超楕円曲線 C_0 の離散対数問題を,k 上定義される被覆曲線 C の離散対数問題に変換するものである. 変換先の離散対数問題の計算量が, 元の計算量より小さくなった場合, 攻撃が成功となる. 実際, 被覆攻撃の手法を用いることで, 鍵長 160bit の安全性を持つ楕円曲線暗号が 107bit 程度の安全性に低下したという結果も発表されている. 被覆攻撃の対象となる範囲は未だ明らかになっておらず, 攻撃の対象となる曲線の解析と分類が重要課題となっている.

現在, 被覆攻撃の対象となる楕円・超楕円曲線の分類が進められている. 奇標数の場合, 奇標数拡大体上の種数 1,2,3 超楕円曲線の完全分類が行われた. 偶標数の場合, 奇標数とは異なる扱いが必要となり完全な分類が困難であるが, 百瀬らにより偶標数拡大体上の種数 1,2,3 楕円・超楕円曲線に対して, 同種条件下での曲線の分類が行われている [1].

本論文では, 百瀬らの分類結果の検証と証明を行い, 偶標数拡大体 k_d 上の種数 1,2,3 楕円・超楕円曲線 C_0 に対する同種条件下での曲線の分類を行う. また分類表の曲線の導出方法を示す.

2　被覆攻撃の概要

k_d/k 上のフロベニウス自己同型写像を $\sigma_{k_d/k}$ とし, $\sigma_{k_d/k}$ の位数 d の拡張 σ を考える. そのとき, $k_d(C_0)/k_d(x)$ のガロア閉包 $K := k_d(C_0) \cdot k_d({}^{\sigma}C_0) \cdots k_d({}^{\sigma^{d-1}}C_0) \simeq k_d(C)$ であり, σ の固定体 $K' := \{\xi \in K \mid \sigma(\xi) = \xi\} \simeq k(C)$ となる. GHS 攻撃 [2] では, 標数 2 の楕円曲線 C_0/k_d に対して, conorm-norm 写像 $N_{K/K'} \circ Con_{K/k_d(C_0)} : Cl^0(k_d(C_0)) \to Cl^0(K')$ を用いて, $Cl^0(k_d(C_0)) \simeq J(C_0)(k_d)$ 上の離散対数問題を $Cl^0(k(C)) \simeq J(C)(k)$ 上の離散対数問題に変換して攻撃を行う. 現在, この攻撃は一般的な曲線にも適用され, 被覆攻撃として一般化されている. 本論文では, 偶標数の楕円・超楕円曲線 C_0 を用いる.

$$C_0/k_d \ : \ y^2 + g(x)y = f(x)$$

このとき C_0 は 2 次の被覆を持つ.

$$C_0 \xrightarrow{2} \mathbb{P}^1(x)/k, \quad (x, y) \mapsto x$$

C_0 の共役な楕円・超楕円曲線 ${}^{\sigma^i}C_0$ は,

$$\sigma_{k_d/k} \ : \ k_d \to k_d, \ \alpha \mapsto \alpha^q, \ x \mapsto x, \ y \mapsto {}^{\sigma}y$$

$${}^{\sigma^i}C_0 : {}^{\sigma^i}y^2 + {}^{\sigma^i}g(x){}^{\sigma^i}y = {}^{\sigma^i}f(x) \quad (0 \le i \le n-1)$$

と表せ, ${}^{\sigma^i}C_0$ の関数体 $k_d({}^{\sigma^i}C_0) = k_d(x, {}^{\sigma^i}y)$ となる. また, $k_d({}^{\sigma^i}C_0)$ が線形無関連である最大の n $(\le d)$ を選ぶと, $k_d(C) \simeq k_d(x, y, {}^{\sigma}y, \cdots, {}^{\sigma^{n-1}}y)$ となる.
被覆 $\pi/k_d : C \longrightarrow \mathbb{P}^1(x)$ は,

$$cov(C/\mathbb{P}^1(x)) := \mathrm{Gal}(k_d(C)/k_d(x)) \simeq \mathbb{F}_2^n$$

となっており, これを $\overbrace{(2, \ldots, 2)}^{n}$ 型被覆と呼ぶ.

以降, 指数 2 の $cov(C/\mathbb{P}^1(x))$ の部分群 I を $I \underset{2}{\le} cov(C/\mathbb{P}^1(x))$ と表記する.

3　ガロア表現の分類と同種条件

3.1　ガロア表現の分類

$\overbrace{(2, \ldots, 2)}^{n}$ 型被覆曲線 C を持つ楕円・超楕円曲線 C_0 の分類を考える.

$$\overbrace{C \to \underbrace{C_0 \to \mathbb{P}^1(x)}_{2}}^{\overbrace{(2, \ldots, 2)}^{n}}$$

$cov(C/\mathbb{P}^1(x))$ へのガロア群 $\mathrm{Gal}(k_d/k)$ の作用を,

$$\begin{aligned}\mathrm{Gal}(k_d/k)\times cov(C/\mathbb{P}^1(x)) &\to cov(C/\mathbb{P}^1(x))\\ (\sigma^i_{k_d/k},\ \phi) &\mapsto {}^{\sigma^i}\phi := \sigma^i\phi\sigma^{-i}\end{aligned}$$

とすると, $\mathrm{Gal}(k_d/k)$ から $\mathrm{Aut}(cov(C/\mathbb{P}^1(x)))$ への埋め込みが得られる.

$$\mathrm{Gal}(k_d/k)\hookrightarrow \mathrm{Aut}(cov(C/\mathbb{P}^1(x)))\simeq GL_n(\mathbb{F}_2)$$

以降, $\sigma_{k_d/k}$ とその表現を σ を用いて表記する.

3.2 同種条件

同種条件とは, [1] の Condition(C) を指す. この条件は $g(C)=dg(C_0)$ と同値である. $H \underset{2}{<} cov(C/\mathbb{P}^1(x))$ を $C/H=C_0$ とすると, ${}^{\sigma^i}C_0 = C/{}^{\sigma^i}H$ となる. $I \underset{2}{<} cov(C/\mathbb{P}^1(x))$ に対して, 次は同種条件と同値である.

$$g(C/I)=\begin{cases}0 \ \cdots (I\neq {}^{\sigma^i}H)\\ g(C_0)\ \cdots (I={}^{\sigma^i}H)\end{cases}$$

つまり, ${}^\forall I \underset{2}{<} cov(C/\mathbb{P}^1(x))$ に対して, C/I は楕円・超楕円曲線 ${}^{\sigma^i}C_0$ または $\mathbb{P}^1$ となる.

以降, 本論文では, 同種条件を仮定する.

偶標数上楕円・超楕円曲線を分類する際, 下記の条件により被覆構造が異なるため, それぞれ分類を行う.

- σ が indecomposable or decomposable
- 拡大次数 d が $2\mid d$ or $2\nmid d$
- C_0 が ordinary or non-ordinary

4 Indecomposable case

4.1 $2\mid d$ and ordinary case

C_0 が ordinary の場合について, $(2,\dots,2)$ 型被覆曲線 C/k が存在するような d と n を定める. ここで, 無限遠点で分岐しない 種数 $g(C_0)$ の ordinary な楕円・超楕円曲線 C_0 は, 次の形になる.

$$\begin{aligned}&C_0: y^2+g(x)y=f(x)\\ &(\deg g(x)=g(C_0)+1,\ \deg f(x)=2g(C_0)+2)\end{aligned}\quad(1)$$

$2|d$ の条件より, d の可能性として, 2 ベキかそれ以外の偶数が考えられる. [1] より, d が 2 ベキでない場合は被覆構造が存在しない. したがって, 本論文では $d=2^r$ $(r\in\mathbb{N})$ のみを考える. このとき, indecomposable な表現行列 σ は, 既約な Jordan 行列となる.

$$\sigma=\begin{pmatrix}1 & 1 & 0 & \cdots & 0\\ 0 & 1 & 1 & \ddots & \vdots\\ 0 & 0 & \ddots & \ddots & 0\\ \vdots & \vdots & \ddots & 1 & 1\\ 0 & \cdots & \cdots & 0 & 1\end{pmatrix}\in GL_n(\mathbb{F}_2)$$

σ が上記の形より, $(\sigma+I)^n=0$ である. 他方で, $\mathrm{ord}(\sigma)=d=2^r$ より, d は $\sigma^{2^r}=I$ となる最小の整数であるので, $(\sigma+I)^{2^r}=\sigma^{2^r}+I=2I=0$ となる. また, $(\sigma+I)^{2^{r-1}}\neq 0$ であることから, $2^{r-1}<n\leq 2^r=d$ が得られる. $\phi\in cov(C/\mathbb{P}^1(x))$ $s.t.$ $\phi/k=(1\ 0\ \cdots\ 0)^T$, ${}^\sigma\phi=\phi$ に対して, k 上 2 次の被覆 $(C\xrightarrow{2}C/\phi)$ を考えると, 同種条件より $C/\phi=\mathbb{P}^1/k$ となる. 被覆曲線 C から $\mathbb{P}^1/k$ への 2 次の被覆が存在することから, C は hyperelliptic とわかる. Riemann-Hurwitz より $d=2^{n-1}$ となる. $2^{r-1}<n\leq 2^r=d$ より, $2^{n-2}<n\leq 2^{n-1}$ となるので $(d,n)=(2,2),\ (4,3)$ が得られる.

4.2 $2\mid d$ and non-ordinary case

C_0 が non-ordinary の場合について, $(2,\dots,2)$ 型被覆曲線 C/k が存在するような d と n を定める.

C_0 が non-ordinary のとき, 分岐構造から $d=2^{n-1}$ となるので $(d,n)=(2,2),(4,3)$ が得られる.

4.3 $2\nmid d$ and ordinary case

$2\nmid d$ の場合, 4.2 節の結果から ordinary case しか存在しない. さらに [1] より, d が 2^n-1 の真の約数である場合は被覆構造が存在しないことがわかっている. したがって, 本論文では $d=2^n-1$ かつ ordinary の場合のみを考える. 以下では, $(2,\dots,2)$ 型被覆曲線 C/k を持つ楕円・超楕円曲線 C_0 の構成方法について示す.

$2\nmid d$ より, d を以下とする.

$$d\mid 2^n-1,\ d\nmid 2^l-1\quad(1\leq {}^\forall l\leq n-1)$$

ここで, $\mathbb{F}_2$ の代数閉包 $\overline{\mathbb{F}}_2$ 上, 1 の原始 d 乗根を $\zeta=\zeta_d\in\overline{\mathbb{F}}_2$ とする. $\mathbb{F}_2$ 上の ζ の最小多項式を,

$$f(x)=x^n+\sum_{i=0}^{n-1}a_ix^i,\quad a_0=1,\ a_i\in\mathbb{F}_2 \qquad (2)$$

とする. そのとき ζ は, $\zeta^n=\sum_{i=0}^{n-1}a_i\zeta^i$ を満たし, ガロア群 $\mathrm{Gal}(k_d/k)$ の $cov(C/\mathbb{P}^1(x))\simeq\mathbb{F}_2^n$ への作用は, ${}^\forall v\in cov(C/\mathbb{P}^1(x))$ に対して, ${}^\sigma v=\sum_{i=0}^{n-1}a_i\ {}^{\sigma^i}v$ で表される. この既約表現の数は $\frac{\varphi(d)}{n}$ と等しい.

$m:=2^n-1, d=m$ のとき, $k_m(C)$ の k 線形写像 L を次のように定義する.

$$\begin{aligned}&L\ :\ k_m(C)\longrightarrow k_m(C)\\ &{}^\forall h\in k_m(C)\mapsto L(h):={}^{\sigma^n}h+\sum_{i=0}^{n-1}a_i\ {}^{\sigma^i}h\end{aligned}\qquad(3)$$

さらに, 数列 $\{b_i\in\mathbb{F}_2\mid i=0,1,\cdots,m-1\}$ を次のように定義する.

$$\begin{aligned}&b_0=b_1=\cdots=b_{n-1}=1,\ a_n=1,\\ &b_{n+l}=\sum_{i=0}^{n-1}a_{n-i}\ b_{l+i}\quad(l=0,1,\cdots,m-1-n)\end{aligned}\qquad(4)$$

4.3.1 楕円・超楕円曲線 C_0 の構成条件

楕円・超楕円曲線 C_0 を次のように定義する.

$$\begin{aligned}&C_0: y^2+g(x)y=f(x)\\ &(\deg g(x)=g(C_0)+1,\quad \deg f(x)=2g(C_0)+2)\end{aligned}$$

$d=2^n-1$ のとき, ${}^\forall H\underset{2}{<}cov(C/\mathbb{P}^1(x))$ は, $g(C/H)=g(C_0)$ である. さらに, $\hat{g}(x),\ Z,\ h(x)$ を次で定める.

$$\begin{aligned}&\hat{g}(x):=LCM\{{}^{\sigma^i}g(x)\}\in k[x]\\ &Z:=\frac{\hat{g}(x)}{g(x)}y,\quad h(x):=\left(\frac{\hat{g}(x)}{g(x)}\right)^2 f(x)\end{aligned}\qquad(5)$$

式 (5) を用いて C_0 および ${}^{\sigma^i}C_0$ を書き換えると,

$$C_0 : Z^2 + \hat{g}(x)Z = h(x)$$
$${}^{\sigma^i}C_0 : {}^{\sigma^i}Z^2 + \hat{g}(x)\ {}^{\sigma^i}Z = {}^{\sigma^i}h(x)$$

となる. そのとき,

$${}^{\sigma^l}Z \equiv \sum_{i=0}^{n-1} c_i\ {}^{\sigma^i}Z \pmod{k_m[x]}, \quad {}^{\exists}c_i \in \mathbb{F}_2$$
$${}^{\sigma^n}Z = \sum_{i=0}^{n-1} a_i\ {}^{\sigma^i}Z + l(x), \quad l(x) \in k_m[x]$$
$$l(x)^2 + \hat{g}(x)l(x) = L(h(x)) \in k_m[x]$$

となる. $l(x) = L(\ell(x))$ として, $L(h(x) + \ell(x)^2 + \hat{g}(x)\ell(x)) = 0$ のとき, $(2, \ldots, 2)$ 型被覆曲線 C/k を持つ C_0 を構成できる. そのため, $L(h(x)) \equiv 0 \pmod{L(\ell(x)^2 + \hat{g}(x)\ell(x))}$ が分類の条件となる.

4.3.2 $g(x)$ の構成法

$2 \nmid d$ の場合について, 楕円・超楕円曲線 C_0 の $g(x)$ の構成法を示す. $g_1(x) := GCD\{{}^{\sigma^i}g(x)\} \in k[x]$, $g_2(x) := \frac{g(x)}{g_1(x)}$ とする. そのとき, 被覆構造の分岐点の関係より, 次が成り立つ.

$$g(C_0) + 1 = \deg g_1(x)$$
$$+ \sum_{i=1}^{n-1} \sum_{d|m,\, \frac{m}{d}|(2^{n-r}-1)} (2^n - 2^r)\frac{d}{m} \times b_{i,d},\ {}^{\exists}b_{i,d} \in \mathbb{Z}_{\geq 0}$$

α を $g_2(x)$ の 1 つの根として, $l' := \#\{i \mid 0 \leq i \leq m-1,\ g_2(\alpha^{q^i}) = 0\}$ とする. そのとき, α が $C/H \overset{2}{\to} \mathbb{P}^1(x)$ で分岐点となる $H \underset{2}{<} cov(C/\mathbb{P}^1(x))$ の数は, $(2^n - 1) - (2^r - 1),\ (1 \leq {}^{\exists}r \leq n-1)$ となり, $l' \times \frac{m}{d}$ と等しくなる. ここで, $d = m,\ r = n-1,\ l' = 2^{n-1}$ の場合について考える. α に対応する式を $g_\alpha(x)$ とすると,

$$R := \{i \mid 0 \leq i \leq m-1,\ s.t.\ b_i = 1\},\ \#R = 2^{n-1}$$
$${}^{\exists}j,\ g_\alpha(x) = \prod_{i \in \sigma^j R} (x + \alpha^{q^i}) \tag{6}$$

であり, α を分岐点に持つ楕円・超楕円曲線 C_0 の $g(x)$ は, $g(x) = g_\alpha(x)$ となる. 本論文では, 関数 L の条件を簡略化するため, $g(x) = {}^{\sigma}g_\alpha(x)$ とする.

5 Decomposable case

Decomposable な表現行列 σ は, 既約な Jordan 行列の直和の形となる. 例えば $(n_1, n_2) = (2, 1)$ のとき, $d = (2^{n_1} - 1)(2^{n_2} - 1) = 3$, $n = n_1 + n_2 = 3$ であり, 被覆曲線 C/k を持つ楕円曲線 C_0 は次の形になる [1].

$$C_0 \ :\ y^2 + xy = x^3 + ax^2 + bx$$
$$\mathrm{Tr}(b) = 0,\ a \in k,\ b \in k_3 \backslash k$$

6 分類

6.1 分類例 $g(C_0) = 1, d = 4, n = 3$

4.1 節の $(d, n) = (4, 3)$ の場合について, $(2, 2, 2)$ 型被覆曲線 C/k を持つ楕円曲線 C_0 の形を求める. また, 同種条件を満たし, 構成した全ての曲線が楕円曲線か $\mathbb{P}^1$ となることを確認する.

6.1.1 楕円曲線 C_0 の形

$g(C_0) = 1$ より, $\deg f(x) = 4$ である. 式 (1) は 1 次分数変換を用いることで, 無限遠点で分岐する monic な 3 次の楕円曲線に変形できる.

$$C_0 : y^2 + xy = x^3 + ax^2 + b'x + c' \quad (a, b', c' \in k_d) \tag{7}$$

有限体 k_d が完全体であること, また k_d の 2 次拡大体上の同型によって式 (7) から, 次のように変形できる.

$$C_0 : y^2 + xy = x^3 + bx \quad (b \in k_d) \tag{8}$$

6.1.2 同種条件を満たすことの確認

$(d, n) = (4, 3)$ の場合, 式 (8) は同種条件を満たし, 共役な 3 つの楕円曲線は, 次のようになる.

$$\begin{cases} C_0 : y^2 + xy = x^3 + bx \\ {}^{\sigma}C_0 : {}^{\sigma}y^2 + x^{\sigma}y = x^3 + b^q x \\ {}^{\sigma^2}C_0 : {}^{\sigma^2}y^2 + x^{\sigma^2}y = x^3 + b^{q^2}x \end{cases} \tag{9}$$

このとき, 以下で示すように, $C_0, \cdots, {}^{\sigma^{n-1}}C_0$ の組み合わせで全ての 2 次拡大と $\mathbb{P}^1$ を構成できる. $(d, n) = (4, 3)$ より, 部分群 $H \underset{2}{<} cov(C/\mathbb{P}^1(x))$ の数は 7 つ, その中で楕円曲線となる数は $(d =)4$ つ, $\mathbb{P}^1$ となる数は 3 つである. 同種条件より, それ以外の曲線は現れない. 標数 2 であることから, 共役な楕円曲線の組み合わせにより新たな曲線を構成でき, 式 (9) を組み合わせると,

$$(y + {}^{\sigma}y + {}^{\sigma^2}y)^2 + x(y + {}^{\sigma}y + {}^{\sigma^2}y) = x^3 + (b + b^q + b^{q^2})x \tag{10}$$

が得られる. $\mathrm{Tr}(b) = b + b^q + b^{q^2} + b^{q^3} = 0,\ b \in k_4 \backslash k_2$ のとき式 (10) は, ${}^{\sigma^3}y^2 + x^{\sigma^3}y = x^3 + b^{q^3}x$ と書き換えられる. これは, C_0, ${}^{\sigma}C_0$, ${}^{\sigma^2}C_0$ とは異なる 4 つ目の楕円曲線 ${}^{\sigma^3}C_0$ となる. 一方で, C_0 と ${}^{\sigma}C_0$ を組み合わせると, $(y + {}^{\sigma}y)^2 + x(y + {}^{\sigma}y) = (b + b^q)x$ となる. $\mathrm{Tr}(b) = 0$ より $(b + b^q) \neq 0$ なので, 構成した曲線は $\mathbb{P}^1$ となる. 同様に,C_0 と ${}^{\sigma^2}C_0$, ${}^{\sigma}C_0$ と ${}^{\sigma^2}C_0$ の組み合わせも $\mathbb{P}^1$ となり, 計 3 つの $\mathbb{P}^1$ が構成できる. 以上より, $(2, 2, 2)$ 型被覆曲線 C/k を持つ, $g(C_0) = 1$,$(d, n) = (4, 3)$ の楕円曲線 C_0 は下記となる.

$$C_0 : y^2 + xy = x^3 + bx, \quad b \in k_4 \backslash k_2$$
$$\mathrm{Tr}(b) = b + b^q + b^{q^2} + b^{q^3} = 0$$

6.2 分類例 $g(C_0) = 3, d = 7, n = 3$

4.3 節の $(d, n) = (7, 3)$ の場合について, $(2, 2, 2)$ 型被覆曲線 C/k を持つ種数 3 超楕円曲線の形を求める.

6.2.1 超楕円曲線 C_0 の形

式 (2) より, $d = 7$ のとき ζ の取り方により 2 通りの最小多項式が存在する. ここでは, $f(\zeta) = \zeta^3 + \zeta^2 + 1 = 0$ を用いる. 式 (4), (6) より,

$$b_0 = b_1 = b_2 = 1,\ b_3 = 0,\ b_4 = 0,\ b_5 = 1,\ b_6 = 0$$
$$R = \{i \mid 0 \leq i \leq 6\ s.t.\ b_i = 1\} = \{0, 1, 2, 5\}$$

である. 最小多項式として, $\zeta^3 + \zeta + 1 = 0$ を選択した場合は, b_4 と b_5 の値が入れ替わる. 上記の結果より,

$$g_\alpha(x) = (x+\alpha)(x+\alpha^q)(x+\alpha^{q^2})(x+\alpha^{q^5})$$

が得られる. $g(x) = {}^\sigma g_\alpha(x)$ とおくと,

$$g(x) = (x+\alpha^q)(x+\alpha^{q^2})(x+\alpha^{q^3})(x+\alpha^{q^6})$$

となり超楕円曲線 C_0 は次の形となる.

$$C_0 : y^2+(x+\alpha^q)(x+\alpha^{q^2})(x+\alpha^{q^3})(x+\alpha^{q^6})y = f(x) \tag{11}$$

6.2.2 同種条件を満たすことの確認

$(d,n) = (7,3)$ の場合, 式 (11) は同種条件を満たし, 3 つの共役な超楕円曲線を用いて残り 4 つの曲線が構成できる. 式 (5) より C_0 は,

$$C_0 : Z^2 + \hat{g}(x)Z = h(x)$$

と書き換えられる. ${}^\sigma C_0$, ${}^{\sigma^2} C_0$ を C_0 と同様の方法で構成すると,

$$\begin{cases} {}^\sigma C_0 : {}^\sigma Z^2 + \hat{g}(x)\ {}^\sigma Z = {}^\sigma h(x) \\ {}^{\sigma^2} C_0 : {}^{\sigma^2} Z^2 + \hat{g}(x)\ {}^{\sigma^2} Z = {}^{\sigma^2} h(x) \end{cases}$$

となる. $L(h(x)) \equiv 0 \pmod{L(\ell(x)^2 + \hat{g}(x)\ell(x))}$ の条件より, ${}^{\sigma^3} h(x)$ が構成できる.

$$\begin{aligned} &L(h(x)) = h(x) + {}^{\sigma^2} h(x) + {}^{\sigma^3} h(x) \equiv 0 \\ &{}^{\sigma^3} h(x) \equiv h(x) + {}^{\sigma^2} h(x) \end{aligned} \tag{12}$$

したがって, C_0 と ${}^{\sigma^2} C_0$ を組み合わせることで,

$$(Z + {}^{\sigma^2} Z)^2 + \hat{g}(x)(Z + {}^{\sigma^2} Z) = h(x) + {}^{\sigma^2} h(x)$$

となり ${}^{\sigma^3} C_0$ が得られる. 式 (12) の両辺に σ を作用させることで, ${}^{\sigma^4} C_0$, ${}^{\sigma^5} C_0$, ${}^{\sigma^6} C_0$ も構成できる.

$$\begin{cases} {}^{\sigma^4} h(x) \equiv h(x) + {}^\sigma h(x) + {}^{\sigma^2} h(x) \\ {}^{\sigma^5} h(x) \equiv h(x) + {}^\sigma h(x) \\ {}^{\sigma^6} h(x) \equiv {}^\sigma h(x) + {}^{\sigma^2} h(x) \end{cases} \tag{13}$$

なお ${}^{\sigma^7} h(x) \equiv h(x)$ であるので, 式 (12),(13) 以外の曲線は新たに現れない. よって, 3 つの共役な超楕円曲線を用いて, 7 つの超楕円曲線を構成することができた.

以上より, $(2,2,2)$ 型被覆曲線 C/k を持つ $g(C_0) = 3, (d,n) = (7,3)$ の超楕円曲線 C_0 は下記となる.

$$C_0 : y^2+(x+\alpha^q)(x+\alpha^{q^2})(x+\alpha^{q^3})(x+\alpha^{q^6})y = f(x)$$
$$L((x+\alpha)^2(x+\alpha^{q^4})^2(x+\alpha^{q^5})^2 f(x)) \equiv 0 \quad (^*2)$$

本節の手法を用いて種数 1,2,3 偶標数曲線の分類を行った. 紙面の都合により種数 3 の分類結果の一部を下表にまとめた. 関数 L の詳細は表の (*2) を参照されたい.

7 結論

本論文では, 百瀬らの分類結果の検証を行い詳細な証明を与えることによって, 被覆攻撃の対象となる偶標数拡大体 k_d 上の種数 1,2,3 楕円・超楕円曲線 C_0 に対する同種条件下での曲線の完全分類を行った. さらに分類表の曲線の導出方法を初めて示した. 今後の課題として, 分類表の曲線の同型類に関する考察, 同種条件を外した一般の場合での曲線の分類などが挙げられる.

謝辞

本研究を進めるにあたり，適切な御指導, 御助言, 御検討を頂いた中央大学理工学部 趙晋輝教授，共同で研究を行った東海大学理学部情報数理学科准教授 志村真帆呂先生に深く感謝いたします．本研究に臨むにあたり, 株式会社光電製作所 飯島努氏より数多くの御助言を頂きました．ここに深謝の意を表します.

関連発表

- 村井公輔, 志村真帆呂, 飯島努, 趙晋輝, “被覆攻撃の対象となる偶標数有限体上の楕円・超楕円曲線に対する同種条件下の完全分類”, Proc. of SCIS2022, IEICE Japan, 2022.

参考文献

[1] F. Momose and J. Chao, “Classification of Weil restrictions obtained by $(2,\ldots,2)$ coverings of $\mathbb{P}^1$”, preprint, 2006. Available from http://eprint.iacr.org/2006/347.

[2] P. Gaudry, F. Hess and N. Smart, “Constructive and destructive facets of Weil descent on elliptic curves”, J. Cryptol, 15, pp.19-46, 2002.

[3] C. Diem, J. Scholten, “Cover attacks, a report for the AREHCC project”, preprint Oct. 2003.

$C_0/k_d : y^2 + g(x)y = f(x) \quad (\deg g(x) = g(C_0)+1, \deg f(x) = 2g(C_0)+2,\ g(C_0) = 3)$ $(I)\ {}^\sigma g(x) = g(x)$, $(II)\ {}^\sigma g(x) \neq g(x)$, 表の $\equiv$ は $\equiv 0\ (mod\ L(\ell(x)^2 + \hat{g}(x)\ell(x)))$ を意味する.		
$d = 2^n - 1, n \geq 2$	(I)	$L(f(x)) = 0$
$d = 3$ $n = 2$	(II)	$g(x) = g_1(x)(x+\alpha^q)(x+\alpha^{q^2}),\ \alpha \in k_3 \backslash k,\ g_1(x) \in k[x], \deg g_1(x) \leq 2$ $L((x+\alpha)^2 f(x)) = (x+\alpha)^2\ f(x) + (x+\alpha^q)^2\ {}^\sigma f(x) + (x+\alpha^{q^2})^2\ {}^{\sigma^2} f(x) = 0$
	(II)	$g(x) = (x+\alpha^q)^2(x+\alpha^{q^2})^2,\ \alpha \in k_3 \backslash k$ $L((x+\alpha)^4 f(x)) = (x+\alpha)^4\ f(x) + (x+\alpha^q)^4\ {}^\sigma f(x) + (x+\alpha^{q^2})^4\ {}^{\sigma^2} f(x) = 0$
$d = 7$ $n = 3$	(II)	$g(x) = (x+\alpha^q)(x+\alpha^{q^2})(x+\alpha^{q^3})(x+\alpha^{q^5}),\ \alpha \in k_7 \backslash k$ $L((x+\alpha)^2(x+\alpha^{q^4})^2(x+\alpha^{q^6})^2 f(x)) \equiv 0 \quad (^*1)$
	(II)	$g(x) = (x+\alpha^q)(x+\alpha^{q^2})(x+\alpha^{q^3})(x+\alpha^{q^6}),\ \alpha \in k_7 \backslash k$ $L((x+\alpha)^2(x+\alpha^{q^4})^2(x+\alpha^{q^5})^2 f(x)) \equiv 0 \quad (^*2)$
$(^*1)\ (x+\alpha)^2(x+\alpha^{q^4})^2(x+\alpha^{q^6})^2\ f(x)+(x+\alpha^q)^2(x+\alpha^{q^5})^2(x+\alpha)^2\ {}^\sigma f(x)+(x+\alpha^{q^3})^2(x+\alpha)^2(x+\alpha^{q^2})^2\ {}^{\sigma^3} f(x) \equiv 0$ $(^*2)\ (x+\alpha)^2(x+\alpha^{q^4})^2(x+\alpha^{q^5})^2\ f(x)+(x+\alpha^{q^2})^2(x+\alpha^{q^6})^2(x+\alpha)^2\ {}^{\sigma^2} f(x)+(x+\alpha^{q^3})^2(x+\alpha)^2(x+\alpha^q)^2\ {}^{\sigma^3} f(x) \equiv 0$		