# GHS 攻撃の対象となる奇標数合成数次拡大体上種数 2 超楕円曲線の分類に関する研究

# A Classification of Genus Two Hyperelliptic Curves Subjected to the GHS Attack over Composite Degree Extensions of Finite Fields of Odd Characteristic

情報工学専攻　相賀 陸
Riku Aiga

**要約**　楕円・超楕円曲線暗号はその暗号の持つ特徴から IoT 機器等への実装が期待されている. GHS 攻撃はこの暗号方式への攻撃手法であり, $k := \mathbb{F}_q$ の $d$ 次拡大体 $k_d := \mathbb{F}_{q^d}$ 上定義された曲線 $C_0$ の離散対数問題を, $C_0$ の $k$ 上被覆曲線 $C$ の離散対数問題に変換する攻撃手法である. 本論文では, 未だ攻撃を受ける曲線の分類が行われていない奇標数合成数次拡大体 $k_d$ 上種数 2 超楕円曲線 $C_0$ において分類を行った.

**キーワード**　楕円・超楕円曲線暗号, GHS 攻撃

## 1　はじめに

楕円・超楕円曲線暗号は, 安全性とハードウェアなどに対する実装性が優れているため, IoT 機器のための暗号として期待されている. 最近, 種数 2 超楕円曲線暗号に関して, 楕円曲線暗号より高効率な実装手法が報告されている. 一方で, ハードウェア攻撃を含む楕円・超楕円曲線暗号の安全性検証の重要性も増している.

GHS 攻撃は, Gaudry, Hess, Smart ら [1] によって偶標数の拡大体上の楕円曲線に適用され, その後, より一般的な曲線に拡張され, さらに被覆攻撃として一般化されている. この攻撃手法は, 有限体 $k := \mathbb{F}_q(q$ : 素数のべき) の $d$ 次拡大体 $k_d := \mathbb{F}_{q^d}$ 上に定義された代数曲線 $C_0$ の離散対数問題を, $C_0$ の $k$ 上被覆曲線 $C$ の離散対数問題に変換し, それを解く攻撃手法である. GHS 攻撃が提案された当初は, 極一部の曲線しか対象とならないと考えられていたが, 後の研究で, 奇標数 3 次拡大体上の楕円曲線の Legendre 標準形の半分以上, 偶標数の場合は 4 分の 3 以上が鍵長 160 ビットの安全性が 107 ビットの安全性に減少させられるなど, 多くの曲線に対し脅威となり得る事が分かった. しかし GHS 攻撃の解析は数学的に難解であるため, その対象範囲は未だ完全に明らかにされたわけではない.

近年, isogeny 条件 $(g(C) = d \cdot g(C_0))$ の下で, $(2, \ldots, 2)$ 型被覆曲線 $C/k$ を持つような種数 $1, 2, 3$ の楕円・超楕円曲線 $C_0/k_d$ の完全分類が示され, 様々な性質が明らかになった. また一般の場合 $(g(C) \geq d \cdot g(C_0))$ に, 奇標数においては系統的な分類手法が示され, それを用いた楕円・超楕円曲線 $C_0/k_d$ のある分類が与えられた. 更に最近, 奇標数における $k$ の素数次拡大体 $k_d$ に関して $(2, \ldots, 2)$ 型被覆曲線 $C/k$ を持つような楕円曲線 $C_0/k_d$ の完全分類 [4], 種数 2 超楕円曲線 $C_0/k_d$ の完全分類が行われ, その後に合成数次拡大体 $k_d (d \leq 10)$ に関しても $(2, \ldots, 2)$ 型被覆曲線 $C/k$ を持つような楕円曲線 $C_0/k_d$ の完全分類が行われた [6].

本論文では, GHS 攻撃の対象となる曲線の解明を目的とし, 奇標数合成数次拡大体上種数 2 超楕円曲線の分類を行った. なお, 紙数の関係上, 拡大次数 $d = 4$ の分類結果の一部のみをここでは記す.

## 2　GHS 攻撃と $(2, \ldots, 2)$ 型被覆

$k_d/k$ 上のフロベニウス自己同型写像 $\sigma_{k_d/k}$ と, 位数 $d$ の $\sigma_{k_d/k}$ の拡張 $\sigma$ を考える. 本研究で扱う奇標数拡大体上楕円・超楕円曲線 $C_0/k_d$ の場合にその様な $\sigma$ の存在条件は, 既に示されている. このような $\sigma$ の下で, $k_d(C_0)/k_d(x)$ のガロア閉包は $K := k_d(C_0) \cdot k_d({}^{\sigma}C_0) \cdot \cdots \cdot k_d({}^{\sigma^{d-1}}C_0)$ であり, $\sigma$ の固定体は $K' := \{\zeta \in K | \sigma(\zeta) = \zeta\} \simeq k(C)$ である. 最初に提案された GHS 攻撃は標数 2 の楕円曲線に対し, 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, $Cl^0(k_d(C_0)) \simeq J(C_0)(k_d)$ 上の DLP を $Cl^0(K') \simeq J(C)(k)$ 上の DLP へと移す攻撃手法だった. またその後, Frey, Diem によって被覆攻撃へと一般化されている. 本論文では奇標数拡大体 $k_d$ 上の種数 2 超楕円曲線

$$C_0/k_d : y^2 = c \cdot f(x) \tag{1}$$

について考える. ここで, $c \in k_d^{\times}$ かつ $f(x) \in k_d[x]$ はモニック多項式である. このとき $C_0$ は次の様な 2 次の被覆を持っている.

$$C_0 \to \mathbb{P}^1,\ (x, y) \mapsto x \tag{2}$$

ここでは, 被覆 $\pi/k_d : C \to \mathbb{P}^1$ が存在し, $\mathbb{P}^1$ 上の $\overbrace{(2, \ldots, 2)}^{n}$ 型被覆となる $C_0$ の被覆曲線 $C$ を考える. ここで $\mathbb{P}^1$ 上の $\overbrace{(2, \ldots, 2)}^{n}$ 型被覆であるとは,

$$cov(C/\mathbb{P}^1) := Gal(k_d(C)/k_d(x)) \simeq \mathbb{F}_2^n \tag{3}$$

となるような被覆である. これ以降, このような被覆 $\pi/k_d : C \to \mathbb{P}^1$ が存在する場合の分類を行う.

## 3　ガロア表現の分類と $(2, ..., 2)$ 型被覆を持つ超楕円曲線 $C_0/k_d$ の分類

### 3.1　ガロア表現の分類

次に $(2, \ldots, 2)$ 型被覆 $C/\mathbb{P}^1$ を伴うような次数 2 の部分被覆 $C_0/\mathbb{P}^1$ の分類について述べる.

$$\overbrace{C \to \underbrace{C_0 \to \mathbb{P}^1(x)}_{2}}^{\overbrace{(2, \ldots, 2)}^{n}} \tag{4}$$

そのために, $cov(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n$ 上作用するガロア群 $Gal(k_d/k)$ の表現を分類して, $\sigma$ の振る舞いを明らかにする.

$$Gal(k_d/k) \times cov(C/\mathbb{P}^1) \to cov(C/\mathbb{P}^1) \tag{5}$$

$$(\sigma^i_{k_d/k}\ ,\ \phi) \qquad \mapsto {}^{\sigma^i}\phi := \sigma^i \phi \sigma^{-i} \tag{6}$$

この時, 以下のような $Gal(k_d/k)$ から $Aut(cov(C/\mathbb{P}^1))$ への埋め込みを得る.

$$Gal(k_d/k) \hookrightarrow Aut(cov(C/\mathbb{P}^1)) \simeq GL_n(\mathbb{F}_2) \tag{7}$$

以降, 簡単のため $\sigma_{k_d/k}$ とその表現に対しても同じ表記 $\sigma$ を用いる. 一般に $n$ と $d$ に対する表現 $\sigma$ の形は以下のようになっている.

$$\sigma = \begin{pmatrix} \Delta_1 & O & \cdots & O \\ O & \Delta_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & O \\ O & \cdots & O & \Delta_s \end{pmatrix} \begin{matrix} \}n_1 \\ \}n_2 \\ \vdots \\ \}n_s \end{matrix}, n = \sum_{i=1}^{s} n_i \tag{8}$$

ここで $O$ は零行列を表しており,

$$\Delta_i = \begin{pmatrix} \Omega_i & \Omega_i & \hat{O} & \cdots \\ \hat{O} & \Omega_i & \ddots & \ddots \\ \vdots & \ddots & \ddots & \Omega_i \\ \hat{O} & \cdots & \hat{O} & \Omega_i \end{pmatrix} \begin{matrix} \}n_i/\ell_i \\ \}n_i/\ell_i \\ \vdots \\ \}n_i/\ell_i \end{matrix} \tag{9}$$

は直既約 (indecomposable) な部分表現で, $\ell_i \times \ell_i$ のブロックを持つような $n_i \times n_i$ 行列である. サブブロック $\Omega_i$ は $n_i/\ell_i \times n_i/\ell_i$ 行列で, $\hat{O}$ は同じサイズの零行列である. また $\Omega_i$ の特性多項式を $f_i(x)$ とし, $\Delta_i$ の特性多項式を $F_i(x) := f_i(x)^{\ell_i}$ とする. このとき $F(x) := LCM\{F_i(x)\}$ は $\sigma$ の最小多項式である. また $\Delta_i$ の位数を $d_i$ とした時, $d = LCM\{d_i\}$ となる.

例えば, $d = 2$ の表現 $\sigma$ の分類は

- $d = 2, n = 2$
  $\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_2), F(x) = x^2 + 1$

となる.
一般に $\sigma$ の表現は以下の 2 つのタイプに分けられる.

- Type A : ${}^{\exists}d_i\ s.t.\ d_i = d$
- Type B : $d_i \neq d$ for ${}^{\forall}d_i$

素数次数 $d$ の場合には, 先の $d = 2$ の例のように Type A の $\sigma$ しか現れない. 一方で, $d$ が合成数の場合は Type A と Type B の両方の表現が現れる場合がある.

合成数 $d = 4$ の表現 $\sigma$ は以下のように分類できる. $d = 4$ の場合は Type A のみである.

- $d = 4, n = 4$
  $\sigma = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in GL_4(\mathbb{F}_2),$
  $F(x) = x^4 + 1 = (x+1)^4$
- $d = 4, n = 3$
  $\sigma = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \in GL_3(\mathbb{F}_2),$
  $F(x) = (x+1)^3 = x^3 + x^2 + x + 1$

$\sigma$ の最小多項式 $F(x)$ を $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_2[x]$ と表すと, $\sigma^n = a_{n-1}\sigma^{n-1} + \cdots + a_1\sigma + a_0$ である. この時, ガロア群 $Gal(k_d/k)$ の $y$ に対する作用は,

$${}^{\sigma^n}y \equiv \prod_{j=0}^{n-1} ({}^{\sigma^j}y)^{a_j} \qquad \mod k_d(x)^\times$$

となり, ここから,

$${}^{\sigma^n}y^2 \equiv \prod_{j=0}^{n-1} ({}^{\sigma^j}y^2)^{a_j} \qquad \mod (k_d(x)^\times)^2$$

を導く. 結果として, 与えられた $d, n, \sigma$ に対して, $C$ が $k_d$ 上のモデルとなるための必要十分条件が得られる.

$$\begin{aligned} &{}^{\forall}G(x) | F(x), G(x) \neq F(x) \text{ に対して,} \\ &{}^{F(\sigma)}y^2 \equiv 1 \mod (k_d(x)^\times)^2 \text{ かつ} \\ &{}^{G(\sigma)}y^2 \not\equiv 1 \mod (k_d(x)^\times)^2 \end{aligned} \tag{10}$$

これを用いて, $C$ が $k_d$ 上モデルを持つ場合の分類を行う.

### 3.2 $C/k$ の存在条件

以降, $\hat{F}(x) \in \mathbb{F}_2[x]$ を以下の様な多項式として定義する.

$$x^d + 1 = F(x)\hat{F}(x) \in \mathbb{F}_2[x] \tag{11}$$

${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^\times)^2$ が満たされている時, 以下が成立するならば $C$ が $k$ 上のモデルとなる (i.e. 位数が $d$ となるよう $\sigma$ を取ることが出来る) ことが知られている.

- $\hat{F}(1) = 0$ の時, $c \in (k_d^\times)^2$
  この場合, $c$ は平方元の時のみ $C$ は $k$ 上のモデルに落ちる.
- $\hat{F}(1) = 1$ の時, $c \in k_d^\times$
  この場合, $c$ は平方元と非平方元のどちらでも可能.

次に, ${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^\times)^2$ が満たされるように $f(x)$ を分類していく. まず, $d, n, \sigma$ を与えた時に, $C_0/\mathbb{P}^1$ の分岐点の候補の組を求める必要がある.

### 3.3 $C_0/\mathbb{P}^1$ の分岐点の求め方

$\Phi(x) := a(x)\hat{F}(x) := b_{d-1}x^{d-1} + \cdots + b_1 x + b_0$, $N := \#\{(\mathbb{F}_2[x]/F(x))^\times\}/d$ と定義する. ここで $a(x)$ は, 以下を満たす多項式である.

$$a(x) \in \mathbb{F}_2[x], \deg a(x) < \deg F(x), GCD(a(x), F(x)) = 1 \tag{12}$$

以下では与えられた $d, n, \sigma$ に対して, $C_0/\mathbb{P}^1$ の分岐点の候補の組を求める方法を示す.

**Algorithm 1**：$C_0/\mathbb{P}^1$ の分岐点を求める
**Step 1-1**：$a(x)=1$ とする．この時, $\Phi(x)=\hat{F}(x)$ となり, これは $C_0/\mathbb{P}^1$ の分岐点の候補の 1 組

$$\left\{(\alpha^{q^i},0)|i\in\{0,\dots,d-1\}\ s.t.\ b_i=1\right\}$$

を与えている．$\alpha\in k_d\backslash k_v$ $(v|_{\neq d})$ または, $\alpha\in k_{d\tau}\backslash k_v$ $(\mathbb{N}\ni{}^{\exists}\tau>1,\ v|_{\neq d\tau})$ である．ただし, 後者の場合は $f(x)$ が $k_d$ 上 $\alpha^{q^i}\in k_{d\tau}$ の全ての共役元を根として含む必要がある．ここで $N=1$ ならば Algorithm 1 は終了する．$N\geq 2$ ならば, 次の Step へ進む.
**Step 1-2**：(12) 式を満たすような新たな $a(x)$ を選び $\Phi(x):=a(x)\hat{F}(x)$ とする.
**Step 1-3**：ここまでに選ばれた全ての $\Phi(x)$ が互いに異なるかを確認する．ここで, $\Phi(x)$ が互いに異なっているとは, $\Phi(x)$ の係数が,

$$(b_0,b_1,\dots,b_{d-1})\sim(b_j,\dots,b_{d-1},b_0,\dots,b_{j-1})$$

の様な巡回置換の関係でない事を意味する．ここで選んだ $\Phi(x)$ が, 既に候補として選ばれたものと互いに異なっているならば, $\left\{(\alpha^{q^i},0)|b_i=1\right\}$ を新たな分岐点の候補の 1 組として加え, 次の Step へ進む. そうでないなら, ここで選んだ $\Phi(x)$ を破棄し, Step 1-2 へ戻る.
**Step 1-4**：$N$ 組の分岐点の候補が見つかったならば, Algorithm 1 は終了する．そうでないなら Step 1-2 へ戻る.

### 3.4 $C_0/k_d$ の構成法

$S$ を $C/\mathbb{P}^1$ の分岐点の数, $S_0$ を $C_0/\mathbb{P}^1$ の分岐点の数とし, $g(C)=d\cdot g(C_0)+e(0\leq e\in\mathbb{Z})$ とすると, Riemann-Hurwitz の種数公式より,

$$S=4+\frac{d\cdot g(C_0)+e-1}{2^{n-2}} \tag{13}$$

と書くことができ, Abhyankar's lemma により,

$$\text{Type A の時}: dS_0\geq S\geq\max\{d,2g_0+3\} \tag{14}$$
$$\text{Type B の時}: dS_0\geq S\geq\max\{q(d),2g_0+4\} \tag{15}$$
$$(q(d):=\sum p_i^{e_i}, d=\prod p_i^{e_i})$$

が得られる．これらと Algorithm 1 で求めた分岐点の候補の組を用いて $C_0/k_d$ を構成する方法を示す.
**Algorithm 2**：$C_0/k_d$ の定義方程式 $f(x)$ を求める
**Step 2-1**：$d,n,g(C_0),e$ を与え, (14)(15) の範囲と (13) 式から $S$ を求める.
**Step 2-2**：1 のみから成る自明な表現を除いて, $\sigma$ の全ての部分表現に対して, Algorithm 1 を用いて, $C_0/\mathbb{P}^1$ の全ての分岐点の候補を $N$ 組リストアップする.
**Step 2-3**：${}^{F(\sigma)}f(x)\equiv 1 \mod (k_d(x)^\times)^2$ の下で, Step 2-1 で求めた $S$ と, Step 2-2 で作った分岐点の候補の組から, 全ての組み合わせを試し, $f(x)$ を求める．このとき, $k_d$ の拡大体から $\alpha$ を取る (つまり, $\mathbb{N}\ni{}^{\exists}\tau>1,\ \alpha\in k_{d\tau}\backslash k_v, v|_{\neq d\tau}$) 場合には, $f(x)$ が $k_d$ 上の全ての共役元を含まなければならないことに注意する.
**Step 2-4**：第 3.2 節 で示した方法により, $c$ のとり得る範囲を決定する.

## 4 $k$ の合成数次拡大 $k_d$ 上種数 2 超楕円曲線の分類

本章では実際に Algorithm1, 2 を用いて種数 2 超楕円曲線 $C_0/k_d: y^2=c\cdot f(x)$ の分類例を示す.

### 4.1 $d=4$

第 3.1 節で示したように表現の分類を行う事で, $\sigma$ とその最小多項式 $F(x)$ が定まる．$d=4$ の場合, $n=3,4$ となり得る事が分かる.
• $d=4,n=3$ の分類例

$$\sigma=\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}\in GL_3(\mathbb{F}_2), F(x)=(x+1)^3$$

まず Algorithm 1 を用いて分岐点の候補を求める．$N=1$ より分岐点の組の候補は 1 つのみである．$\hat{F}(x)=x+1$ のため, $a(x)=1$ とすると, $\Phi(x):=a(x)\hat{F}(x):=b_{d-1}x^{d-1}+\cdots+b_1x+b_0=x+1$ であり, $b_1=b_0=1$ である．これより分岐点の候補 $\{(\alpha,0),(\alpha^q,0)\}$ を得る．また, それに加え次の部分表現を持つ.

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\in GL_2(\mathbb{F}_2), F(x)=x^2+1$$

これは $d=2,n=2$ の時の $\sigma$ の表現であり, その分岐点の候補は $\{(\beta,0)\}$ であることが既存の研究より明らかにされている．以上より全分岐点の候補は $\{(\alpha,0),(\alpha^q,0)\},\{(\beta,0)\}$ である.

次に可能な $e$ の範囲を求める．種数 2 超楕円曲線 $C_0/k_d$ の分岐点の個数は $S_0=6$ であるため, $d,n,g(C_0),S_0$ を (13) 式に与え, (14) 式に代入し式を変形することで, $1\leq e\leq 33$ を得る.

次に Algorithm 2 を用いる．ここでは一例として $e=3$ の場合を取り上げる．この時, (13) 式より $S=9$ となる．この $S$ と, 求めた分岐点の候補に対して (10) 式の下で全ての組み合わせを試すことで,

$$f(x)=(x-\alpha)(x-\alpha^q)(x-\beta)h_1(x)$$
$$\alpha\in k_4\backslash k_2,\ \beta\in k_2\backslash k,$$
$$h_1(x)\in k[x],\ deg\ h_1(x)=2,3$$

を得る．最後に第 3.2 節より, $\hat{F}(1)=0$ であるため, $c\in(k_d(x)^\times)^2$ となり, $c$ は平方元に限る．以上より,
$C_0/k_d: y^2=c\cdot(x-\alpha)(x-\alpha^q)(x-\beta)h_1(x)$
を得る．これは付録の分類表における case 2 の分類である.

### 4.2 $d\geq 6$

Algorithm 1, 2 を用いることで同様に分類を行うことが出来る．しかし, $d\geq 8$ の場合, 被覆曲線 $C$ の種数 $g(C)$ が多くの場合に大きくなりすぎる．$d=8,n=5$ の時, $g(C)$ の下限は $g(C)\geq 33$ であるが, $n=6,7,8$ の場合はより大きくなり, 例えば $d=8,n=8$ の時 $g(C)\geq 257$ となる．10 以上の合成数の場合には, $g(C)$ がかなり大きくなる事が, 次数毎の計算から観察されており, 精々 9 次程度までの分類で実質的には十分と思われる.

## 5 $(2,\ldots,2)$ 型被覆曲線 $C/k$ を持つような種数 2 超楕円曲線 $C_0/k_d$ の分類表

第 3 節の手法を用いて種数 2 超楕円曲線 $C_0/k_d$ の分類を行い, $d=4,n=3$ 及び $d=4,n=4$ の分類結果の一部を下の表にまとめた. $d\geq 6$ の分類結果は紙数の関係で割愛する. 本論文では, isogeny 条件が一般の場合 $(g(C)\geq d\cdot g(C_0))$ を扱っているため $g(C)=d\cdot g(C_0)+e$ とする, $c$ が $\eta$ の時, 平方元, 非平方元どちらも取り得る事を意味する. 表において $\alpha,\beta$ 及び $\alpha_i,\beta_i$ が属する体は以下の通りになる.

備考 1 において, *印が付いてないケースは $\alpha\in k_4\backslash k_2,\ \beta\in k_2\backslash k$, もしくは $\alpha_i\in k_4\backslash k_2,\ \beta_i\in k_2\backslash k$ である. *印が付いているケースは, $\alpha_i\in k_4\backslash k_2,\ \beta_i\in k_2\backslash k$ と $\alpha_i\in k_{4\tau_j}\backslash k_{2v_l}, \beta_i\in k_{2\tau_j}\backslash k_{v_l}, (\mathbb{N}\ni {}^{\exists}\tau>1, v|_{\neq d\tau})$ が混在している事を示している. また, *印が付いている場合, $f(x)$ が $k_d$ 上の全ての共役元を含まなければならない事に注意する.

備考 2 において, † 印が付いているケースは, 他のケースと等しくなるような $h_d(x)$ を取らない事を意味する.

## 6 結論

奇標数合成数次拡大体において, GHS 攻撃の対象となる被覆曲線 $C/k$ を持つような種数 2 超楕円曲線 $C_0/k_d$ の分類を明らかにした. 分類表には GHS 攻撃により安全性が落ちる, 暗号として使用するべきでない曲線が列挙しているため暗号系設計時の活用が期待される. 今後の課題として, 今回分類された曲線において, 実際の被害範囲や計算量の評価, 分類間で移り合う同型攻撃に関する考察や, 偶標数体上の楕円・超楕円曲線の一般の場合で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 晋輝教授と, 共同で研究を行った株式会社 光電製作所飯島 努氏に, 深く感謝致します. 本研究に臨むにあたり, 東海大学理学部情報数理学科准教授 志村真帆呂先生に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

- 相賀陸, 飯島努, 志村真帆呂, 趙晋輝,"GHS 攻撃の対象となる奇標数合成数次拡大体上種数 2 超楕円曲線の分類", Proc. of SCIS2019, IEICE Japan, 2019.

## 参考文献


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

[2] C. Diem, "The GHS attack in odd characteristic", J. Ramanujan Math.Soc, 18 no.1, pp.1-32,2003.

[3] T. Iijima, F. Momose, and J. Chao, "Classification of elliptic/hyperelliptic curves with weak coverings against GHS attack without isogeny condition", preprint, 2009. Available from http://eprint.iacr.org/2009/613.

[4] T. Iijima, F. Momose, and J. Chao, "A classification of elliptic curves with respect to the GHS attack in odd characteristic", preprint, 2015. Available from http://eprint.iacr.org/2015/805.

[5] 小林龍平, 飯島努, 趙晋輝, "GHS 攻撃の対象となる奇標数素数次数拡大体上種数 2 の曲線の完全分類," Proc. of SCIS2016, IEICE Japan, 2016.

[6] 小林龍平, 飯島努, 趙晋輝 "GHS 攻撃の対象となる奇標数合成数次拡大体上の楕円曲線の分類", Proc. of SCIS2017, IEICE Japan, 2017


$C_0/k_d: y^2=c\cdot f(x):=c\cdot h_d(x)h_1(x),\ h_d(x)\in k_d[x]\backslash k[x],\ h_1(x)\in k[x],\ g(C)=d\cdot g(C_0)+e\ (\mathbb{Z}\ni e\geq 0)$

| case | $d$ | $n$ | $e$ | $g(C)$ | $c$ | $h_d(x)$ | deg $h_1(x)$ | 備考 1 | 備考 2 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 4 | 3 | 1 | 9 | 1 | $(x-\alpha)(x-\alpha^q)$ | 3, 4 | | |
| 2 | 4 | 3 | 3 | 11 | 1 | $(x-\alpha)(x-\alpha^q)(x-\beta)$ | 2, 3 | | |
| 3 | 4 | 3 | 5 | 13 | 1 | $(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)$ | 1, 2 | * | |
| | | | | | 1 | $(x-\alpha)(x-\alpha^q)(x-\beta_1)(x-\beta_2)$ | 1, 2 | * | |
| 4 | 4 | 3 | 7 | 15 | 1 | $(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)(x-\beta)$ | 0, 1 | * | |
| | | | | | 1 | $(x-\alpha)(x-\alpha^q)(x-\beta_1)(x-\beta_2)(x-\beta_3)$ | 0, 1 | * | |
| 5 | 4 | 3 | 9 | 17 | 1 | $(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)(x-\alpha_3)(x-\alpha_3^q)$ | 0 | * | |
| | | | | | 1 | $(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)(x-\beta_1)(x-\beta_2)$ | 0 | * | |
| | | | | | 1 | $(x-\alpha)(x-\alpha^q)(x-\beta_1)(x-\beta_2)(x-\beta_3)(x-\beta_4)$ | 0 | * | |
| 6 | 4 | 4 | 5 | 13 | $\eta$ | $(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})$ | 2, 3 | | |
| 7 | 4 | 4 | 9 | 17 | $\eta$ | $(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_1^{q^2})(x-\alpha_2)(x-\alpha_2^q)(x-\alpha_2^{q^2})$ | 0 | * | |
| | | | | | $\eta$ | $(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\beta)$ | 1, 2 | | |
| 8 | 4 | 4 | 13 | 21 | $\eta$ | $(x-\alpha)$ | 4, 5 | | |
| | | | | | $\eta$ | $(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_1^{q^2})(x-\alpha_2)(x-\alpha_2^q)$ | 0, 1 | | |
| | | | | | $\eta$ | $(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\beta_1)(x-\beta_2)$ | 0, 1 | * | |
| 9 | 4 | 4 | 17 | 25 | $\eta$ | $(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_1^{q^2})(x-\alpha_2)$ | 1, 2 | | |
| | | | | | $\eta$ | $(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha_2)(x-\alpha_2^q)(x-\beta)$ | 0 | | |
| | | | | | $\eta$ | $(x-\alpha)(x-\beta)$ | 3, 4 | | |
| | | | | | $\eta$ | $(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\beta_1)(x-\beta_2)(x-\beta_3)$ | 0 | * | |
| 10 | 4 | 4 | 21 | 29 | $\eta$ | $(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_1^{q^2})(x-\alpha_2)(x-\beta)$ | 0, 1 | | |
| | | | | | $\eta$ | $(x-\alpha_1)(x-\alpha_2)(x-\alpha_2^q)$ | 2, 3 | | † |
| | | | | | $\eta$ | $(x-\alpha)(x-\beta_1)(x-\beta_2)$ | 2, 3 | * | |