被覆攻撃の対象となる奇標数素数次拡大体上種数 3 超楕円曲線の完全分類

A Classification of Genus Three Hyperelliptic Curves Subjected to the Cover Attack over Prime Degree Extensions of Odd Characteristic

情報工学専攻　18N8100020K　山岸 純一
Information and System Engineering Yamagishi Junichi

要約　GHS 攻撃は, 初め偶標数拡大体上の楕円曲線に適用され, その後, 奇標数を含む拡大体上のより一般的な代数曲線に拡張され, 更に被覆攻撃としても一般化されている. 被覆攻撃とは, 有限体 $k := \mathbb{F}_q$ の d 次拡大体 $k_d := \mathbb{F}_{q^d}$ 上定義される代数曲線 C_0 の離散対数問題を k 上被覆曲線 C に変換して攻撃する手法である. 現在, 奇標数拡大体 k_d 上の楕円曲線および種数 2 超楕円曲線について被覆攻撃の対象となる曲線 C_0 の分類が完了している. 本論文では奇標数素数次拡大体 k_d 上種数 3 超楕円曲線 C_0 について完全分類を行う.

キーワード　楕円曲線 · 超楕円曲線, GHS 攻撃, 被覆攻撃

1　はじめに

楕円 · 超楕円曲線暗号は, 短い鍵長で高い安全性を持ちハードウェア実装との相性が良いため, 計算資源が限られる IoT 機器への応用が期待されている. 最近種数 2 超楕円曲線暗号に関して, 楕円曲線暗号より効率の良い実装手法が提案されている. その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の検証も非常に重要となっている.

GHS 攻撃は, Gaudry, Hess, Smart らによって偶標数拡大体上楕円曲線に対して提案された [**?**]. その後, 奇標数を含む拡大体上の代数曲線に拡張され被覆攻撃として一般化されている [**?**]. この攻撃手法は $k := \mathbb{F}_q$ の d 次拡大体 $k_d := \mathbb{F}_{q^d}$ 上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, これを解く手法である. このとき, 被覆曲線 C の種数は大きくなる一方で, 定義体は k_d から k へと位数が小さくなる. これらの影響を総合して計算量が小さくなるような被覆曲線を構成できたとき被覆攻撃は成功となる. したがって被覆攻撃が適用可能となるためにはそのような被覆曲線 C を持つような C_0 の解析が重要である.

近年, 百瀬らによって isogeny 条件 $(g(C) = d \cdot g(C_0))$ の下で $(2, \cdots, 2)$ 型被覆曲線 C/k を持つような C_0 として楕円曲線, 種数 $2 \cdot 3$ 超楕円曲線の完全分類が示された. 加えて, 橋詰らにより被覆曲線 C/k の具体的な構成も行われ, 160bit の安全性を持つ楕円曲線暗号が 107bit 程度になるなど, 被覆攻撃が非常に強力な攻撃となる場合を示した [**?**]. Isogeny 条件を課さない一般の場合 (i.e. $g(C) \geq d \cdot g(C_0)$) に, 飯島らによって奇標数について系統的な分類手法が提案された [**?**]. その後, この分類手法を用いて奇標数について $(2, \cdots, 2)$ 型被覆曲線を持つ素数次及び, 合成次拡大体 k_d 上楕円曲線, 種数 2 超楕円曲線 C_0 の完全分類が行われた [**?**, **?**, **?**, **?**]. 本論文では, 被覆攻撃の対象となる奇標数素数次拡大体 k_d 上定義される種数 3 の超楕円曲線 C_0 の分類を行った.

2　被覆攻撃と $(2, \cdots, 2)$ 型被覆

k_d/k 上の Frobenius 自己同型写像 $\sigma_{k_d/k}$ を $k_d(x)$ の分離閉包において位数 d を持つように拡張し, これを σ と書く. 本論文で扱う奇標数拡大体上楕円 · 超楕円曲線 C_0/k_d において, このような σ の存在条件は既に示されている [**?**]. このとき, σ による $k_d(C_0)/k(x)$ の Galois 閉包は $K := k_d(C_0) \cdot k_d({}^{\sigma}C_0) \cdot k_d({}^{\sigma^2}C_0) \cdot \cdots \cdot k_d({}^{\sigma^{d-1}}C_0) \simeq k_d(C)$ であり, σ の固定体は $K' := \{\zeta \in K |\ \sigma(\zeta) = \zeta\} \simeq k(C)$ である. 初め, Gaudry, Hess, Smart により偶標数拡大体上の楕円曲線に対し, conorm 写像 $Con_{K/k_d(C_0)} : Cl^0(k_d(C_0)) \to Cl^0(k_d(C))$ と norm 写像 $N_{K/K'} : Cl^0(k_d(C)) \to Cl^0(k(C))$ の合成写像 $N_{K/K'} \circ Con_{K/k_d(C_0)} : Cl^0(k_d(C_0)) \to Cl^0(k(C))$ を用いて $Cl^0(k_d(C_0))$ の離散対数問題を $Cl^0(k(C)) \simeq J(C_0)(k)$ 上の離散対数問題に移す攻撃手法が提案された [**?**]. その後さまざまな曲線に拡張され, さらに, Frey, Diem により被覆攻撃として一般化された [**?**]. 本論文では奇標数 d 次拡大体 k_d 上の種数 3 超楕円曲線

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

を考える. ここで $c \in k_d^{\times}$, $f(x) \in k_d[x]$ は monic 多項式である. このとき, C_0 は次のような 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, 被覆 $\pi/k_d : C \to \mathbb{P}^1$ が存在し, $\mathbb{P}^1$ 上の $\overbrace{(2, \cdots, 2)}^{n}$ 型被覆となる C_0 の被覆曲線 C を考える. $\mathbb{P}^1$ 上の $\overbrace{(2, \cdots, 2)}^{n}$ 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. 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 Galois 表現の分類と $(2,\cdots,2)$ 型被覆を持つ超楕円曲線 C_0/k_d の分類

3.1 Galois 表現の分類

次に $(2,\cdots,2)$ 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.

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

まず, $cov(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n$ に作用する Galois 群 $Gal(k_d/k)$ の表現を分類して, σ の振る舞いを明らかにする.

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

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

このとき, 以下のように $Gal(k_d/k)$ 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, $\sigma_{k_d/k}$ とその行列表現に対しても, 同じ表記 σ を用いる. 一般に, d と $n(\leq d)$ に対する表現 σ は以下のように表せる.

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

ここで $\mathcal{O}$ は零行列を表しており,

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

は直既約 (indecomposable) な部分表現で $l_i \times l_i$ 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 Ω_i は $n_i/l_i \times n_i/l_i$ 行列で, $\hat{\mathcal{O}}$ は同じサイズの零行列である. また, Ω_i の特性多項式を $f_i(x)$ とし, Δ_i の特性多項式を $F_i(x) := f_i(x)^{l_i}$ とする. このとき, σ の最小多項式は $F(x) := LCM\{F_i(x)\}$ となる. また, Δ_i の位数を d_i としたとき, $d = LCM\{d_i\}$ となる.
一般に σ の表現は 2 つのタイプに分けられる.

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

d が素数次数の場合は, Type A の σ しか現れない. 具体的な表現は 4 節で示す. σ の最小多項式 $F(x)$ を $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{F}_2[x]$ と表すと, $\sigma^n = a_{n-1}\sigma^{n-1} + \cdots a_1\sigma + a_0$ である. このとき, Galois 群 $Gal(k_d/k)$ の y に対する作用は

$${}^{\sigma^n}y \equiv \prod_{j=0}^{n-1} ({}^{\sigma^j}y)^{a_j} \bmod k_d(x)^{\times} \tag{10}$$

となる. ここから,

$${}^{\sigma^n}y^2 \equiv \prod_{j=0}^{n-1} ({}^{\sigma^j}y^2)^{a_j} \bmod (k_d(x)^{\times})^2 \tag{11}$$

を導く. この等式から, 与えられた d, n, σ に対して, 以下のように 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.

$$\begin{aligned} &{}^{\forall}G(x)|F(x), G(x) \neq F(x) \text{ に対して,} \\ &{}^{F(\sigma)}y^2 \equiv 1 \bmod (k_d(x)^{\times})^2 \text{ かつ} \\ &{}^{G(\sigma)}y^2 \not\equiv 1 \bmod (k_d(x)^{\times})^2 \end{aligned} \tag{12}$$

これ以降, (**??**) の下で, 被覆曲線 C が k_d 上の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, 多項式 $\hat{F}(x) \in \mathbb{F}_2[x]$ を以下のように定義する.

$$x^d + 1 = F(x)\hat{F}(x) \in \mathbb{F}_2[x] \tag{13}$$

${}^{F(\sigma)}f(x) \equiv 1 \bmod (k_d(x)^{\times})^2$ が満たされているとき, 以下の条件が成立するならば被覆曲線 C は k 上のモデルとなる (i.e. 位数が d となる σ を構成できる) ことが知られている [**?**].

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

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

3.3 $C_0/\mathbb{P}^1$ の分岐点の求め方

まず $\Phi(x) := a(x)\hat{F}(x) = b_0 + b_1x + \cdots + b_{d-1}x^{d-1}$, $N := \#\left(\mathbb{F}_2[x]/F(x)\right)^{\times}/d$ とする. ここで $a(x)$ は以下を満たす多項式である.

$$\begin{gathered} a(x) \in \mathbb{F}_2[x],\ \deg a(x) < \deg F(x), \\ \mathrm{GCD}(a(x), F(x)) = 1 \end{gathered} \tag{14}$$

以下の Algorithm 1 では与えられた d, n, σ から, $C_0/\mathbb{P}^1$ の分岐点の候補の組を求める方法を示す.
Algorithm 1 : $C_0/\mathbb{P}^1$ の分岐点の候補の組を求める
Step1-1 : $a(x) = 1$ とする. このとき, $\Phi(x) = \hat{F}(x)$ となる. これから $C_0/\mathbb{P}^1$ の分岐点の候補の 1 組

$$\{(\alpha^{q^i},\ 0) \mid i \in \{0, 1, \cdots, d-1\}\ s.t.\ b_i = 1\} \tag{15}$$

を与えられる. ここで $\alpha \in k_d \backslash k_v$ $(v|d,\ v \neq d)$ または $\alpha \in k_{d\tau} \backslash k_v$ $(\mathbb{N} \ni {}^{\exists}\tau > 1, v|d,\ v \neq d\tau)$ である. ただし, 後者の場合は $f(x)$ が k_d 上共役な元 $\alpha^{q^i} \in k_{d\tau}$ を全て根として含む必要がある.
ここで $N = 1$ なら Algorithm 1 は終了する. $N \geq 2$ ならば, 次の Step に進む.
Step1-2 : (**??**) 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.
Step1-3 : ここまでに選ばれた全ての $\Phi(x)$ が互いに

異なっているかを確認する．ここで, $\Phi(x)$ 同士が互いに異なっているとは, $\Phi(x)$ の係数が

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

のような巡回置換の関係でないことを意味する．ここで選んだ $\Phi(x)$ が既に候補として選ばれたもの全てと互いに異なっているならば, $\{(\alpha^{q^i},\ 0) \mid b_i = 1\}$ を新たな分岐点の候補の 1 組として加えて次の Step へ進む．そうでないならば, ここで選んだ $\Phi(x)$ を破棄して Step1-2 に戻る．

Step1-4 ： N 組の分岐点の候補が見つかったとき, Algorithm 1 は終了する．そうでないならば Step1-2 に戻る

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, $g(C) = d \cdot g(C_0) + e$ $(e \in \mathbb{Z},\ 0 \leq e)$ とする．Riemann-Hurwitz の種数公式より

$$S = 4 + \frac{d \cdot g(C_0) + e - 1}{2^{n-2}} \tag{16}$$

と表せる．また Abhyankar's lemma などにより,

$$dS_0 \geq S \geq \mathrm{max}\{d, 2g(C_0) + 3\} \tag{17}$$

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 を構成する方法を以下に示す．本論文では種数 3 超楕円曲線のみを扱うため $S_0 = 8$ である．

> **Algorithm 2** ： C_0/k_d の定義方程式 $f(x)$ を求める
> **Step2-1** ： $d, n, g(C_0), e$ を与え, (**??**), (**??**) 式から取りうる S の値を求める．
> **Step2-2** ： 1 のみからなる自明な表現を除いて, σ とそのすべての部分表現に対して, Algorithm 1 を用いて $C_0/\mathbb{P}^1$ の N 組の分岐点の候補を求める．
> **Step2-3** ： ${}^{F(\sigma)}f(x) \equiv 1 \bmod (k_d(x)^{\times})^2$ の下で, Step2-2 で求めた分岐点の候補の組を Step2-1 で求めた C, C_0 の分岐点数 S, S_0 の個数を満たすように $f(x)$ を求める．このとき, k_d の拡大体から α を取る (i.e. $\mathbb{N} \ni \tau > 1,\ \alpha \in k_{d\tau}\backslash k_\tau, v|d,\ v \neq d\tau$) 場合には, $f(x)$ が k_d 上の全ての共役元を根に持たなければならないことに注意する．
> **Step2-4** ： 第**??**節で示した方法により, c のとり得る範囲を決定する．

以上のようにして, $(2, \cdots, 2)$ 型被覆曲線 C/k を持つような超楕円曲線 $C_0/k_d : y^2 = c \cdot f(x)$ の分類を行うことが出来る．

4 k の素数次拡大体 k_d 上種数 3 超楕円曲線の分類

本章では実際に Algorithm1, 2 を用いた種数 3 超楕円曲線 $C_0/k_d : y^2 = c \cdot f(x)$ の分類例を示す．

4.1 $d = 2$

まず σ の表現の分類を行うことで, σ とその最小多項式 $F(x)$ が定まる．$d = 2$ のとき n のとり得る値は $n = 2$ のみであることが分かる．まず Algorithm 1 を用いて分岐点の候補を求める．
$\#\left(\mathbb{F}_2[x]/(x^2+1)\right)^{\times} = 2$ より $N = 1$ なので候補は 1 つのみである．$\hat{F}(x) = 1,\ a(x) = 1$ より $\Phi(x) := \hat{F}(x)a(x) = 1$ であり $b_0 = 1$ である．これより分岐点の候補は $\{(\alpha, 0)\}$ の 1 つである．ここで, α は $k_2\backslash k$ かあるいは k_2 のある拡大体の元ともなり得る．
次に可能な e の範囲を求める．種数 3 超楕円曲線 C_0/k_d の分岐点の個数は $S_0 = 8$ であるため, $d,\ n,\ g(C_0),\ S_0$ を式 (**??**) と (**??**) に代入し式を変形することで $0 \leq e \leq 7$ を得る．
次に Algorithm 2 を用いる．ここでは $e = 2$ の場合を取り上げる．まず (**??**) 式より $S = 11$ となる．この S と Algorithm 1 で求めた分岐点の候補に対して (**??**) 式の下ですべての組み合わせを試すことで,

$$f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)h(x),$$
$$h(x) \in k[x],\ \deg h(x) = 4,\ 5$$

を得る．ここで, α_i の組み合わせは,

$$\alpha_1, \alpha_2, \alpha_3 \in k_2\backslash k$$
$$\alpha_1, \alpha_2 := \alpha_1^{q^2} \in k_4\backslash k_2,\ \alpha_3 \in k_2$$
$$\alpha_1, \alpha_2 := \alpha_1^{q^2}, \alpha_3 := \alpha_1^{q^4} \in k_6\backslash(k_2 \cup k_3)$$

の 3 通りである．最後に**??**節より, $\hat{F}(1) = 1$ であるため, $c \in k_2^{\times}$ となり, c は平方元でも非平方元でもよい．
以上より, $C_0/k_2 : y^2 = c\cdot(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)h(x)$ である．これは付録の表における Case 3 の例である．

4.2 $d = 3$

$d = 3$ においては $n = 2, 3$ となり得ることが分かる．
• $d = 3,\ n = 3$ の分類例

$$\sigma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \in GL_2(\mathbb{F}_3),\ F(x) = x^3 + 1$$

Algorithm 1 を用いると, $N = 1$ となり, また以下のような部分表現を持つ．

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

これらの表現に対して, Algorithm 1 を用いて分岐点の候補を求めると $d = 3$, $n = 2$ のとき $\{(\alpha,\ 0),\ (\alpha^q,\ 0)\}$, $d = 3,\ n = 3$ のとき $\{(\beta,\ 0)\}$ となる．
また e の範囲を求めると $2 \leq e \leq 32$ となる．
次に Algorithm 2 を用いる．ここで一例として $e = 4$ の例を述べる．まず, (**??**) 式から $S = 10$ となる．求めた S を考慮し, (**??**) 式の下で全ての分岐点の組み合わせを試すことで,

$$\begin{aligned} f(x) &= (x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q) \\ f(x) &= (x-\beta)h(x) \end{aligned} \tag{18}$$

となる．ここで, (**??**) 式での α_i の組み合わせは

$\alpha_1,\ \alpha_2 \in k_3\backslash k$
$\alpha_1,\ \alpha_2 := \alpha_1^{q^3} \in k_6\backslash(k_2 \cup k_3)$

の 2 通りである.
最後に**??**節より, $\hat{F}(1) = 1$ のため, c は平方元でも非平方元でもよい.
よって,

$$\begin{aligned} C_0/k_3 &: y^2 = c\cdot(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)h(x), \\ C_0/k_3 &: y^2 = c\cdot(x-\beta)h(x) \end{aligned}$$

である. これは付録の Case 11 の例である. 分岐点の候補の組が複数ある場合, 複数の曲線が現れる可能性があることに注意されたい.

5 $(2,\cdots,2)$ 型被覆曲線 C/k を持つような種数 3 超楕円曲線 C_0/k_d の分類

第**??**節の手法を用いて, 種数 3 超楕円曲線 C_0/k_d の分類を行い, $d = 2, 3$ の結果を以下の表にまとめた.
本論文では isogeny 条件が一般の場合 (i.e. $g(C) \geq d\cdot g(C_0)$) を扱っているため, $g(C) = d\cdot g(C_0) + e$ とする. c が η のとき, c は平方元, 非平方元のどちらもとり得ることを意味する.
付録の表において備考に $*$ がついているケースは各 $\alpha_i,\ \beta_i,\ \gamma_i$ が k_d あるいは k_d の拡大体 $k_{d\tau}$ の元になりうることを示す. また後者の場合, $h_d(x)$ は 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. 備考に † がついている曲線ケースは, 他のケースをサブセットとして含まないことを意味する.

6 結論

本論文では, $d \leq 7$ について $(2,\cdots,2)$ 型被覆曲線 C を持つ奇標数素数次拡大体 k_d 上種数 3 超楕円曲線 C_0 の分類を明らかにした. 11 次以上の場合は $g(C)$ がかなり大きくなることが予想されるため, 7 次程度の分類で実質的には十分と思われる. 今後の課題として奇標数合成数次拡大体上種数 3 超楕円曲線の完全分類, 分類間で移りあう同型類に関する考察, 偶標数拡大体上の楕円曲線 · 超楕円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

1. 山岸 純一, 飯島 努, 志村 真帆呂, 趙 晋輝, “被覆攻撃の対象となる奇標数素数次拡大体上種数 3 超楕円曲線の完全分類”, Proc. of SCIS2020, IEICE Japan, 2020.

参考文献

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

[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] 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] N. Hashizume, F. Momose, J. Chao, “On implementation of GHS attack against elliptic curve cryptosystems over cubic extension fields of odd characteristics”, Number Theory Related to Modular Curves (Contemporary Mathematics 701), AMS, 2018

[6] 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.

[7] 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.

[8] 相賀陸, 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種数 2 超楕円曲線の分類”, Proc.of SCIS2019, IEICE Japan, 2019.

Case	d	n	e	$g(C)$	c	$f(x)$	deg $h(x)$	備考
1	2	2	0	6	η	$(x-\alpha_1)h(x)$	6,7	
2	2	2	1	7	η	$(x-\alpha_1)(x-\alpha_2)h(x)$	5,6	$*$
3	2	2	2	8	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)h(x)$	4,5	$*$
4	2	2	3	9	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)h(x)$	3,4	$*$
5	2	2	4	10	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)h(x)$	2,3	$*$
6	2	2	5	11	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)(x-\alpha_6)h(x)$	1,2	$*$
7	2	2	6	12	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)(x-\alpha_6)(x-\alpha_7)h(x)$	0,1	$*$
8	2	2	7	13	η	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)(x-\alpha_6)(x-\alpha_7)(x-\alpha_8)$	0	$*$
9	3	2	0	9	1	$(x-\alpha_1)(x-\alpha_1{}^q)(x-\alpha_2)(x-\alpha_2{}^q)(x-\alpha_3)(x-\alpha_3{}^q)(x-\alpha_4)(x-\alpha_4{}^q)$	0	$*$
10	3	3	2	11	η	$(x-\alpha_1)(x-\alpha_1{}^q)h(x)$	5,6	
11	3	3	4	13	η	$(x-\alpha_1)(x-\alpha_1{}^q)(x-\alpha_2)(x-\alpha_2{}^q)h(x)$	3,4	$*$
					η	$(x-\beta_1)h(x)$	6,7	
12	3	3	6	15	η	$(x-\alpha_1)(x-\alpha_1{}^q)(x-\alpha_2)(x-\alpha_2{}^q)(x-\alpha_3)(x-\alpha_3{}^q)h(x)$	1,2	$*$
					η	$(x-\alpha_1)(x-\alpha_1{}^q)(x-\beta_1)h(x)$	4,5	
13	3	3	8	17	η	$(x-\alpha_1)(x-\alpha_1{}^q)(x-\alpha_2)(x-\alpha_2{}^q)(x-\beta_1)h(x)$	2,3	$*$
					η	$(x-\beta_1)(x-\beta_2)h(x)$	5,6	$*$ †

$d = 2,\ 3$ での分類表