ISS square 2025年度ISS Squareシンポジウム(2026/2/27) No.208

# 同種条件を満たさない被覆攻撃の対象となる偶標数有限体上の種数3超楕円曲線の分類に関する研究

# A Classification of Genus 3 Hyperelliptic Curves Over Finite Fields of Even Characteristic Subject to the Cover Attack Without the Isogeny Condition

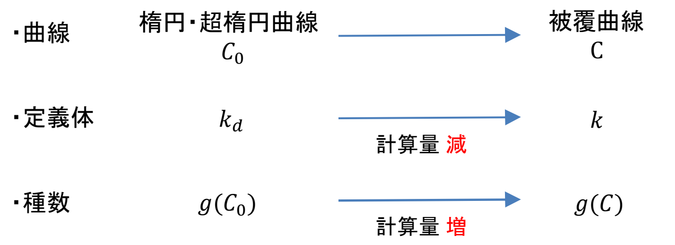
佐藤佑哉・暗号認証分科会・中央大学大学院

**Abstract**：Covering attacks are a method of solving the discrete logarithm problem on elliptic/hyperelliptic curves defined over finite field extensions. Although the classification for elliptic/hyperelliptic curves over finite fields of even characteristics under the isogeny condition has been completed, classifications for the curves without the isogeny condition has only been shown partially. Recently, Uesato proposed a more efficient classification method for curves over finite fields of even characteristic without the isogeny condition. In this study, we applied this method to genus 3 hyperelliptic curves over two types of finite fields of even characteristic which have never been classified before.

## 1. 被覆攻撃とは

○ 拡大体上の楕円・超楕円曲線における離散対数問題に対する攻撃.

○ 楕円・超楕円曲線暗号に被覆攻撃を行うと…



・曲線　楕円・超楕円曲線 $C_0$ → 被覆曲線 C

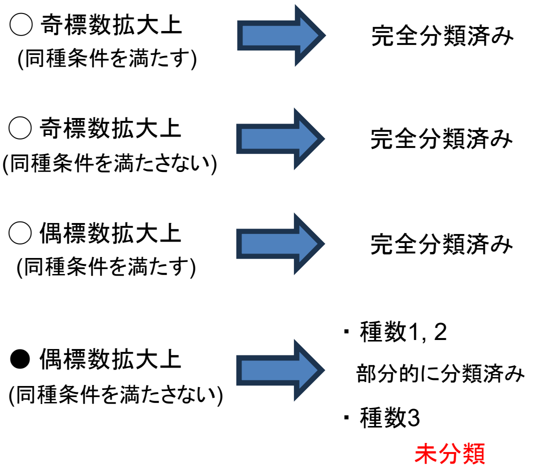
・定義体　$k_d$ → $k$　計算量 減

・種数　$g(C_0)$ → $g(C)$　計算量 増

○ 総合的に見て, 計算量が減少していれば被覆攻撃は成功.

○ 被覆曲線の種数$g(C)$を調べることが分類研究において重要.

## 2. 既存研究



○ 奇標数拡大上 (同種条件を満たす) → 完全分類済み

○ 奇標数拡大上 (同種条件を満たさない) → 完全分類済み

○ 偶標数拡大上 (同種条件を満たす) → 完全分類済み

● 偶標数拡大上 (同種条件を満たさない) →

・ 種数1, 2
部分的に分類済み

・ 種数3
未分類

## 3. 主結果 : 2タイプの偶標数有限体上種数3超楕円曲線の分類

○ Imaginary model ordinary (1)

$$C_0 :\ y^2 + c(x+\alpha)(x+\beta)(x+\gamma)y = \sum_{i=0}^{7} a_i x^i$$

$$(c \in k^{\times}, \alpha, \beta, \gamma \in k, a_i\ \in k_d, \alpha \neq \beta \neq \gamma)$$

1. $\delta_1\left({}^F C_0\right) = g'(\alpha)^2\, {}^F f(\alpha) + {}^F f'(\alpha)^2$

2. $\delta_2\left({}^F C_0\right) = g'(\beta)^2\, {}^F f(\beta) + {}^F f'(\beta)^2$

3. $\delta_3\left({}^F C_0\right) = g'(\gamma)^2\, {}^F f(\gamma) + {}^F f'(\gamma)^2$

4. $\delta_4\left({}^F C_0\right) = {}^F \alpha_7$

$$\Delta : \begin{cases} \begin{array}{lll} (0,0,0,0) \to 0, & (1,0,0,0) \to 0, & (0,1,0,0) \to 0, \\ (0,0,1,0) \to 0, & (0,0,0,1) \to 0, & (1,1,0,0) \to 1, \\ (1,0,1,0) \to 1, & (1,0,0,1) \to 1, & (0,1,1,0) \to 1, \\ (0,1,0,1) \to 1, & (0,0,1,1) \to 1, & (1,1,1,0) \to 2, \\ (1,1,0,1) \to 2, & (1,0,1,1) \to 2, & (0,1,1,1) \to 2, \\ & (1,1,1,1) \to 3, & \end{array} \end{cases}$$

○ Imaginary model non-ordinary

$$C_0 :\ y^2 + c(x+\alpha)^3 y = \sum_{i=0}^{7} a_i (x+\alpha)^i$$

$$(c \in k^{\times}, \alpha \in k, a_i\ \in k_d)$$

1. $\delta_1\left({}^F C_0\right) = {}^F \alpha_7$

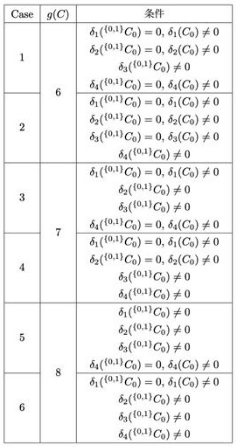
2. $\delta_2\left({}^F C_0\right) = {}^F \alpha_1$

3. $\delta_3\left({}^F C_0\right) = {}^F a_3^2 + c^2\, {}^F \alpha_0$

4. $\delta_4\left({}^F C_0\right) = c^3 \sqrt{{}^F \alpha_2} + c^2\, {}^F \alpha_4 + {}^F a_5^2$

$$\Delta : \begin{cases} \begin{array}{lll} (0,0,0,0) \to 0, & (1,0,0,0) \to 0, & (0,1,0,0) \to 2, \\ (0,0,1,0) \to 1, & (0,0,0,1) \to 0, & (1,1,0,0) \to 3, \\ (1,0,1,0) \to 2, & (1,0,0,1) \to 1, & (0,1,1,0) \to 2, \\ (0,1,0,1) \to 2, & (0,0,1,1) \to 1, & (1,1,1,0) \to 3, \\ (1,1,0,1) \to 3, & (1,0,1,1) \to 2, & (0,1,1,1) \to 2, \\ & (1,1,1,1) \to 3, & \end{array} \end{cases}$$

曲線(1) の分類表の一部



| Case | $g(C)$ | 条件 |
|---|---|---|
| 1 | 6 | $\delta_1({}^{\{0,1\}}C_0) = 0,\ \delta_1(C_0) \neq 0$<br>$\delta_2({}^{\{0,1\}}C_0) = 0,\ \delta_2(C_0) \neq 0$<br>$\delta_3({}^{\{0,1\}}C_0) \neq 0$<br>$\delta_4({}^{\{0,1\}}C_0) = 0,\ \delta_4(C_0) \neq 0$ |
| 2 |  | $\delta_1({}^{\{0,1\}}C_0) = 0,\ \delta_1(C_0) \neq 0$<br>$\delta_2({}^{\{0,1\}}C_0) = 0,\ \delta_2(C_0) \neq 0$<br>$\delta_3({}^{\{0,1\}}C_0) = 0,\ \delta_3(C_0) \neq 0$<br>$\delta_4({}^{\{0,1\}}C_0) \neq 0$ |
| 3 | 7 | $\delta_1({}^{\{0,1\}}C_0) = 0,\ \delta_1(C_0) \neq 0$<br>$\delta_2({}^{\{0,1\}}C_0) \neq 0$<br>$\delta_3({}^{\{0,1\}}C_0) \neq 0$<br>$\delta_4({}^{\{0,1\}}C_0) = 0,\ \delta_4(C_0) \neq 0$ |
| 4 |  | $\delta_1({}^{\{0,1\}}C_0) = 0,\ \delta_1(C_0) \neq 0$<br>$\delta_2({}^{\{0,1\}}C_0) = 0,\ \delta_2(C_0) \neq 0$<br>$\delta_3({}^{\{0,1\}}C_0) \neq 0$<br>$\delta_4({}^{\{0,1\}}C_0) \neq 0$ |
| 5 | 8 | $\delta_1({}^{\{0,1\}}C_0) \neq 0$<br>$\delta_2({}^{\{0,1\}}C_0) \neq 0$<br>$\delta_3({}^{\{0,1\}}C_0) \neq 0$<br>$\delta_4({}^{\{0,1\}}C_0) = 0,\ \delta_4(C_0) \neq 0$ |
| 6 |  | $\delta_1({}^{\{0,1\}}C_0) = 0,\ \delta_1(C_0) \neq 0$<br>$\delta_2({}^{\{0,1\}}C_0) \neq 0$<br>$\delta_3({}^{\{0,1\}}C_0) \neq 0$<br>$\delta_4({}^{\{0,1\}}C_0) \neq 0$ |