# 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

## A classification of genus two hyperelliptic curves subjected to the GHS attack over composite degree extensions of finite fields of odd characteristic

相賀 陸・暗号認証分科会・中央大学

The GHS attack to elliptic/hyperelliptic curves cryptosystem is an attack to solve discrete logarithm problems(DLP) in an algebra curve $C_0$ defined over the $d$ degree extension field $k_d$ of $k := F_q$ by mapping it to the DLP a covering curve $C$ of $C_0$ over $k$. Recently, classifications for all elliptic/hyperelliptic curves subjected to the GHS attack over prime degree extensions of finite fields of odd characteristic were completed. In addition, classifications for elliptic curves subjected to the GHS attack over compose degree extension of finite fields of odd characteristic have been reported. This paper shows a classification of genus two hyperelliptic curves subjected to the GHS attack over composite degree extensions of finite fields of odd characteristic.

## 1 楕円・超楕円曲線暗号

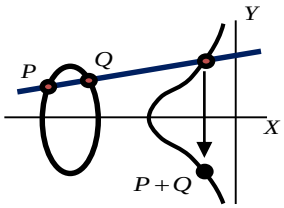
奇標数有限体上定義される楕円・超楕円曲線$C_0$は以下のような代数曲線である.

$$C_0/k_d : y^2 = f(x) \quad (\deg f(x) = 2g(C_0)+1 \ or \ 2g(C_0)+2)$$

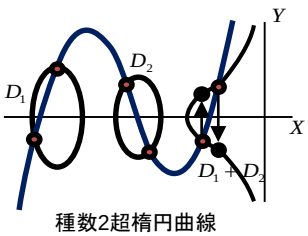
$g(C_0)$: 種数, $g(C_0) \in \mathbb{N}$

$g(C_0) = 1 \rightarrow$ 楕円曲線
$g(C_0) \geq 2 \rightarrow$ 超楕円曲線

楕円・超楕円曲線上の有理点集合は点同士の関係より群構造を成す. その群上の離散対数問題の求解困難性が楕円・超楕円曲線暗号の安全性の根拠である.




楕円曲線




種数2超楕円曲線

## 2 GHS攻撃

$d$次拡大体$k_d := \mathbb{F}_{q^d}$上定義された楕円・超楕円曲線$C_0$の離散対数問題を$k$上定義された被覆曲線$C$の離散対数問題に変換する攻撃手法

| $k_d$上定義された曲線$C_0$の離散対数問題 | → | $k$上定義された被覆曲線$C$の離散対数問題 |
|---|---|---|

| 定義体： | $k_d$ | → | $k$ |
|---|---|---|---|
| 種数： | $g(C_0)$ | → | $g(C) \geq dg(C_0)$ |

変換後の離散対数問題が変換前より簡単になっていた時, GHS攻撃が有効である. GHS攻撃は, 160bitの鍵長の安全性が107bitの鍵長の安全性にまで減少させられるケースがあるなど, 楕円・超楕円曲線暗号に対して大きな脅威となる事が分かっているが, この攻撃の解析は数学的に難解であるため, その攻撃の対象範囲はまだ完全には明らかになっていない. 本研究では未だ分類されていない「奇標数合成数次拡大体上種数2超楕円曲線」に関する分類を行った.

| | 素数次拡大 | | 合成数次拡大 | |
|---|---|---|---|---|
| 種数 | 条件付 | 一般 | 条件付 | 一般 |
| 1 | ○ | ○ | ○ | ○ |
| 2 | ○ | ○ | ○ | **本研究** |
| 3 | ○ | ○ | ○ | - |

同種条件
・条件付：$g(C) = dg(C_0)$
・一般：$g(C) = dg(C_0) + e$

○：済
-　：未

奇標数に関する分類状況

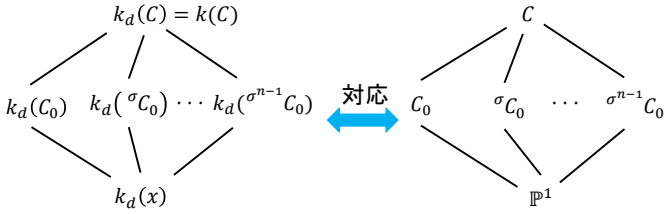
未解明である範囲の曲線の調査を行い, GHS攻撃の対象となる曲線を明らかにすることによって, 楕円・超楕円曲線暗号の安全性を高める事が本研究の目的である.

## 3 (2, … , 2)型被覆曲線

$C_0/k_d : y^2 = f(x)$　　${}^{\sigma^j}C_0 : {}^{\sigma^j}y^2 = {}^{\sigma^j}f(x)$

$k_d(C) := k_d(C_0) \cdot k_d({}^{\sigma}C_0) \cdots k_d({}^{\sigma^{n-1}}C_0)$

$k(C) := \{ \mu \in k_d(C) \mid \sigma(\mu) = \mu \}$

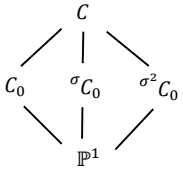



$C$が$\overbrace{(2,\dots,2)}^{n\geq 2}$型被覆 $\overset{\text{def}}{\Longleftrightarrow}$ 被覆 $C \longrightarrow \mathbb{P}^1$
s.t. $cov(C/\mathbb{P}^1) := Gal(k_d(C)/k_d(x)) \cong \mathbb{F}_2^n$

**$C_0$が$(2,\dots,2)$型被覆を持つ時, GHS攻撃の対象となる.**

## 4 曲線の分類手法

例) $d = 4, n = 3$




$$\sigma = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

分岐点の候補

$d = 4, n = 3$
$\{(\alpha, 0), (\alpha^q, 0)\} \ \alpha \in k_4 \setminus k_2$

$d = 3, n = 2$
$\{(\beta, 0)\} \quad \beta \in k_2 \setminus k$

$$F(x) = (x+1)^3 = x^3 + x^2 + x + 1$$

(1) $C_0$上, $C$上での分岐点の数を求める.

$d = 4, n = 3$
$\{(\alpha, 0), (\alpha^q, 0)\} \ \alpha \in k_4 \setminus k_2$
$\Rightarrow$ $C$上の分岐点: 4個
　　$C_0$上の分岐点: 2個

$C_0$ $(\alpha, 0), (\alpha^q, 0)$
${}^{\sigma}C_0$ $(\alpha^q, 0), (\alpha^{q^2}, 0)$
${}^{\sigma^2}C_0$ $(\alpha^{q^2}, 0), (\alpha^{q^3}, 0)$

$C$上の分岐点
$(\alpha, 0), (\alpha^q, 0) (\alpha^{q^2}, 0) (\alpha^{q^3}, 0)$

(2) 分岐点の組み合わせ考える.
$e = 9$とすると$C$の分岐点の数$S$は
Riemann-Hurwitzの種数公式より$S = 12$

Riemann-Hurwitzの種数公式より
$$S = 4 + \frac{dg(C_0) + e - 1}{2^{n-2}}$$

$S = 12$になるような分岐点の組み合わせは $d = 4n = 3$の分岐点:4個 ×3

よって, (2,2,2)型被覆を持つ種数2超楕円曲線$C_0$は

$$C_0/k_d : y^2 = (x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)(x-\alpha_3)(x-\alpha_3^q)$$

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

| 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 | $(x-\alpha_1)(x-\alpha_1^q)(x-\beta_1)(x-\beta_2)$ | 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 | | |