# 楕円暗号と認証システムに関する研究

研究代表者　趙　晋輝　研究員

The GHS attack maps the discrete logarithm problem (DLP) in the Jacobian of a curve C_0 defined over the d degree extension of a finite field k to the DLP in the Jacobian of a new curve C over k which is a covering curve of C_0 . This attack is very powerful. e.g., in the case of d=3, security of ECC with 160-bit key length is reduced to security of 107-bits. In this research, we show a complete classification of all genus two hyperelliptic curves subjected to the GHS attack over prime degree extensions of finite fields with odd characteristic. This result provides an explicit approach to select secure genus two curves in hyperelliptic cryptosystems.

## 1.　はじめに:

拡大体上定義された楕円・超楕円曲線暗号は、高性能実装のために注目されており、特に種数が大きい超楕円曲線は、短い語長で高速実装可能等の利点があるため、IoT　環境における軽量化、省エネ、コンパクトな次世代暗号系として期待されている。

一方、GHS攻撃は、拡大体上の曲線Coの, より小さな定義体上に定義される種数の大きな被覆曲線Cを構築し, Co上の離散対数問題を被覆曲線Cのヤコビ多様体に移して解く攻撃手法である.

本研究では、GHS攻撃の対象となる奇標数素数拡大次数$d$ = 2, 3, 5, 7 の拡大体上定義される種数2超楕円曲線の分類を行い、それらの曲線のすべてを列挙した.これらの情報は、安全な超楕円曲線暗号系を設計する際必要不可欠なものである。

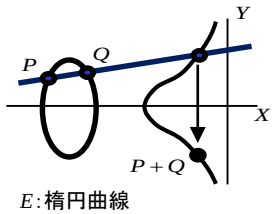
## 2. 超楕円曲線:

超楕円曲線Hは, 次のように定義される代数曲線である.

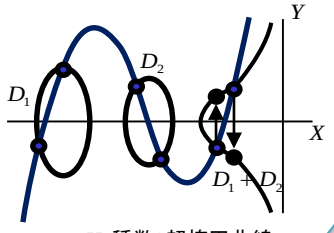
$$H/\mathbf{F}_q : y^2 = f(x),\ \deg f(x) = 2g_0+1 \quad or \quad 2g_0+2$$

f(x); 重解を持たない

超楕円曲線のヤコビアンJ(H)は, 楕円曲線Eの有理点群の一般化であり、E上有理点PとQの和と同様に、J(H)の因子演算、以下の例では、因子D1とD2との足し算の定義が知られている。



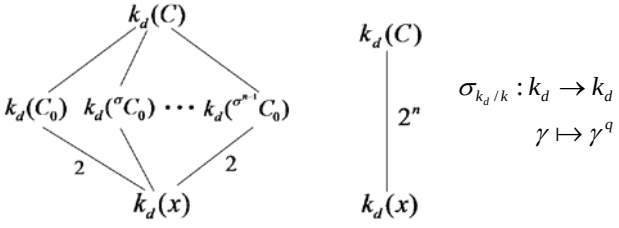

$E$:楕円曲線




$H$:種数2超楕円曲線

## 3. GHS攻撃とその解析

有限体kのd次拡大体kd上に定義された楕円・超楕円曲線Co/kdは、P^1の2次被覆を定義するため、そのガロワ閉包により、以下のP^1上の(2,..,,2)-被覆が定義される.

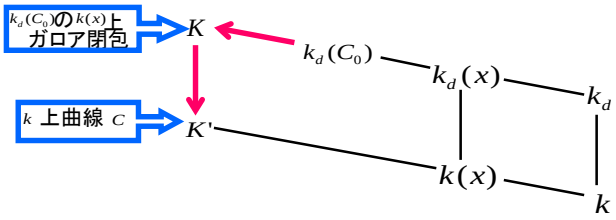



$$\sigma_{k_d/k} : k_d \to k_d,\quad \gamma \mapsto \gamma^q$$

ここでは、ガロワ作用は以下のものとする。

$$Gal(k_d/k)\times \mathrm{cov}(C/\mathbf{P}^1) \to \mathrm{cov}(C/\mathbf{P}^1)$$
$$(\sigma^i_{k_d/k}, \phi) \mapsto {}^{\sigma^i}\phi := \sigma^i \phi \sigma^{-i}$$

GHS攻撃は、拡大体kd上の曲線Coから, k上種数の大きな被覆曲線Cを構築し, 以下のようにNorm-Conorm写像により、Coの離散対数問題をJ(C)に移して解く攻撃.




$$K := k_d(C_0)\sigma(k_d(C_0))\cdots\sigma^{n-1}(k_d(C_0)).$$
$$K' := \{\varsigma \in K \mid \sigma(\varsigma) = \varsigma\}.$$

## 4 :種数2超楕円曲線の分類

本研究は、種数2(2,…,2)被覆Cを持つCo/kdについて、ガロワ表現

$$Gal(k_d/k) \to Aut(\mathrm{cov}(C/\mathbf{P}^1)) \cong GL_n(\mathbf{F}_2)$$

を分類し、リーマン_ホルビツ種数公式による被覆の分岐点集合の解析を行った。上記被覆曲線を持つすべてのCoを割り出し、さらにその方程式を明示的に求めた。以下、$d$ = 2, 3場合のCoの分類を示す。

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

| case | $d$ | $n$ | $e$ | $g(C)$ | $c$ | $h_d(x)$ | $\deg h_1(x)$ | 備考 1 | 備考 2 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 2 | 0 | 4 | $\eta$ | $(x-\alpha)$ | 4, 5 | | |
| 2 | 2 | 2 | 1 | 5 | $\eta$ | $(x-\alpha_1)(x-\alpha_2)$ | 3, 4 | * | |
| 3 | 2 | 2 | 2 | 6 | $\eta$ | $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ | 2, 3 | * | |
| 4 | 2 | 2 | 3 | 7 | $\eta$ | $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$ | 1, 2 | * | |
| 5 | 2 | 2 | 4 | 8 | $\eta$ | $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)$ | 0, 1 | * | |
| 6 | 2 | 2 | 5 | 9 | $\eta$ | $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)(x-\alpha_6)$ | 0 | * | |
| 7 | 3 | 2 | 0 | 6 | 1 | $(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)(x-\alpha_3)(x-\alpha_3^q)$ | 0 | * | |
| 8 | 3 | 3 | 1 | 7 | $\eta$ | $(x-\alpha)(x-\alpha^q)$ | 3, 4 | | |
| 9 | 3 | 3 | 3 | 9 | $\eta$ | $(x-\alpha)$ | 4, 5 | | |
| | | | | | $\eta$ | $(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)$ | 1, 2 | * | |
| 10 | 3 | 3 | 5 | 11 | $\eta$ | $(x-\alpha_1)(x-\alpha_2)(x-\alpha_2^q)$ | 2, 3 | | |
| 11 | 3 | 3 | 7 | 13 | $\eta$ | $(x-\alpha_1)(x-\alpha_2)$ | 3, 4 | * | † |
| | | | | | $\eta$ | $(x-\alpha_1)(x-\alpha_2)(x-\alpha_2^q)(x-\alpha_3)(x-\alpha_3^q)$ | 0, 1 | * | |
| 12 | 3 | 3 | 9 | 15 | $\eta$ | $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_3^q)$ | 1, 2 | * | † |
| 13 | 3 | 3 | 11 | 17 | $\eta$ | $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ | 2, 3 | * | † |
| | | | | | $\eta$ | $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_3^q)(x-\alpha_4)(x-\alpha_4^q)$ | 0 | * | † |
| 14 | 3 | 3 | 13 | 19 | $\eta$ | $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_4^q)$ | 0, 1 | * | † |
| 15 | 3 | 3 | 15 | 21 | $\eta$ | $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$ | 1, 2 | * | † |
| 16 | 3 | 3 | 17 | 23 | $\eta$ | $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)(x-\alpha_5^q)$ | 0 | * | † |
| 17 | 3 | 3 | 19 | 25 | $\eta$ | $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)$ | 0, 1 | * | † |
| 18 | 3 | 3 | 23 | 29 | $\eta$ | $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)(x-\alpha_6)$ | 0 | * | † |