被覆攻撃の対象となる偶標数有限体上楕円・超楕円曲線の分類に関する研究

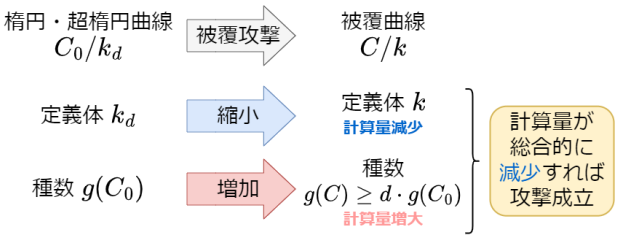
Classification of Elliptic and Hyperelliptic Curves over Finite Fields of Even Characteristics Subject to Cover Attack

上里優介・暗号認証分科会・中央大学

Abstract: The cover attack is known as an attack on cryptosystems based on elliptic/hyperelliptic curves over extensions of finite fields. A complete classification of elliptic curves and hyperelliptic curves over finite fields of even characteristics under the isogeny condition has been shown, while a classification of the curves without the isogeny condition has been obtained partially. In this study, we propose a more general and efficient classification method for the curves with even characteristics using systematic genus evaluation of curves under group ring action of Galois group.

被覆攻撃とは

- **拡大体**上の楕円・超楕円曲線の**離散対数問題**に対する攻撃.
- Weil descent attackやGHS attackを拡張した攻撃.
- 奇標数3次拡大体上のLegendre form楕円曲線の半分以上が攻撃の対象となる結果が知られている.



被覆曲線 C の種数 $g(C)$ を調べることで被覆攻撃の有効性を評価することが目的.

被覆曲線の種数をどのように調べるか？

1. 分岐点を調べる. (百瀬, 飯島らのアプローチ)
   Riemann-Hurwitzの定理を利用
   → 偶標数では分岐の構造が複雑.
2. 関数体を調べる. (鐘ケ江, 登丸らのアプローチ)
   $k_d(C)/k_d(x)$ の2次中間体の種数の総和
   → 考察対象が多く非効率.
   種数評価方法が不完全.

本研究は2.のアプローチで, 考察対象の種数評価を体系化することで従来の課題を解決する.

考察対象曲線の列挙方法

$k = \mathbb{F}_{2^r}$: 偶標数有限体　　k_d : k の d 次拡大体

$C_0 : y^2 + g(x)y = f(x),\ f \in k_d[x], g \in k[x]$ に対し,

$$ {}^F C_0 : y^2 + g(x)y = {}^F f(x) := {}^{F(\sigma)} f(x) = \sum_{i=0}^{m} c_i{}^{\sigma^i} f(x) $$

$$ F = \sum_{i=0}^{m} c_i t^i \in \mathbb{F}_2[t] $$

$k_d({}^F C_0)$ が $k_d(C)/k_d(x)$ の2次中間体を網羅する.

→ $g(C)$ を調べるには $g({}^F C_0)$ をすべて調べればよい.

種数判定法と分類手法

- $g({}^F C_0)$ はいくつかの特徴量 $\delta_1({}^F C_0), \ldots, \delta_m({}^F C_0)$ がそれぞれ0か非0かで決定される.

例:次数が落ちたら種数も落ちる
→ 最高次の係数が特徴量の一つ.

- 特徴量 $\delta_i({}^F C_0)$ が0か非0かは, F がある多項式 $\hat{F}_i$ ($\hat{F}_i \mid t^d + 1$)の倍数か否かで決定される.

$$ \delta_i({}^F C_0) = \mathbf{0} \iff \hat{F}_i \mid F $$

(※ $\mathrm{Ann}_{\mathbb{F}_2[t]/(t^d+1)}(\delta_i(C_0)) = (\hat{F}_i)$)

- 種数 $g(C)$ は多項式 $\hat{F}_i$ から簡単に計算できる.

$$ g(C) \geq d \cdot g(C_0) + e(\hat{F}_1, \ldots, \hat{F}_m) $$

例: $e(\hat{F}_1, \hat{F}_2, \hat{F}_3) = 2 \cdot (2^n - d - 1) - (2^{n - \deg \hat{F}_1} - 1)$
$- (2^{n - \deg \mathrm{lcm}(\hat{F}_1, \hat{F}_2)} - 1) - (2^{n - \deg \hat{F}_3} - 1)$

$g(C)$ が多項式の組で代表されることから, $t^d + 1$ の約数の組を探索することで分類が可能.

分類の達成状況

本研究にて, 以下の条件を満たす偶標数有限体上楕円・超楕円曲線の分類を達成した.

- $g(C_0) = 1$ or 2 .
- $g(x) \in k[x]$.
- $g(x)$ の分解体を k_τ として $\gcd(\tau, d) = 1$.

安全性への影響

- 本研究で新たに発見された楕円・超楕円曲線で, 被覆攻撃が脅威となりうる種類が存在する.
  - 有効鍵長が160ビットからおよそ90ビットに削減されうる種類の曲線が存在する.
- **奇標数素体**上の曲線(例: Ed25519)は攻撃の対象とならない.
- 偶標数で $[k_d : \mathbb{F}_2]$ が**素数**である場合(例:NIST SP 800-186)も, 被覆攻撃が有効でないとされている. ($g(C)$ が巨大なため)

対策は容易だが重要. 標準方式を採用すれば概ね十分.

結論と今後の課題

- 本研究では, 偶標数有限体上楕円・超楕円曲線の効率的な分類手法を提案し, 実際に分類を行った.
- 課題 : 上記の条件を満たさない種類の曲線の分類