被覆攻撃の対象となる偶標数有限体上の楕円・超楕円曲線に対する同種条件下の分類

A classification of elliptic and hyperelliptic curves over finite fields of even characteristic subjected to the cover attack under the isogeny condition

村井公輔・ネットワーク分科会・中央大学

The cover attack to elliptic and hyperelliptic curves cryptosystem is an attack to solve discrete logarithm problems in an algebraic curve defined over the extension field by mapping it to the discrete logarithm problems a covering curve over the base field. Recently, a classification of elliptic and hyperelliptic curves over finite fields of odd characteristic subjected to the cover attack were completed. In addition, a classification of elliptic and hyperelliptic curves over finite fields of even characteristic subjected to the cover attack under the isogeny condition were reported by Momose. In this paper, we validate Momose's classification result and show a way to construct the curves of the classification table.

研究背景・目的

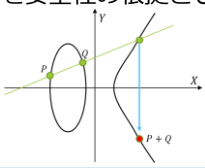
有限体の拡大体上定義される楕円・超楕円曲線を用いた暗号は, 短い鍵長で高い安全性を持ち, その特徴からメモリ容量の小さいデバイスへの実装に有効である. 一方で, 被覆攻撃という拡大体の性質を利用した攻撃手法により, 一部の曲線は安全性が低下してしまう恐れがある. 近年, 攻撃の対象となる種数1,2,3の奇標数楕円・超楕円曲線の完全な分類が行われた. 偶標数曲線に関しては, 分岐構造が複雑なため分類が困難であるが, 百瀬らにより, 偶標数拡大体上の楕円・超楕円曲線に対して, 同種条件という条件の下での分類が行われた. 本研究では, 百瀬らの結果を再検討し分類表の検証を行う. また, 分類した攻撃の対象となる楕円・超楕円曲線の具体的な構成方法について示す.

楕円・超楕円曲線暗号

偶標数有限体 $k := \mathbb{F}_q$ $(q = 2^r)$の d次拡大体 $k_d := \mathbb{F}_{q^d}$上定義される種数 $g(C_0)$の楕円・超楕円曲線C_0とは,

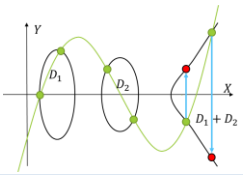
$$C_0/k_d : y^2 + g(x)y = f(x)$$
$$\left(\deg f(x) = 2g(C_0) + 1 \text{ or } 2g(C_0) + 2, \deg g(x) \leq \left\lfloor \frac{\deg f(x)}{2} \right\rfloor\right)$$

$g(C_0) = 1$のとき楕円曲線, $g(C_0) \geq 2$のとき超楕円曲線という. 楕円・超楕円曲線の有理点集合は群構造を持ち, 楕円・超楕円曲線暗号は, その群上の離散対数問題の求解が困難なことを安全性の根拠としている.



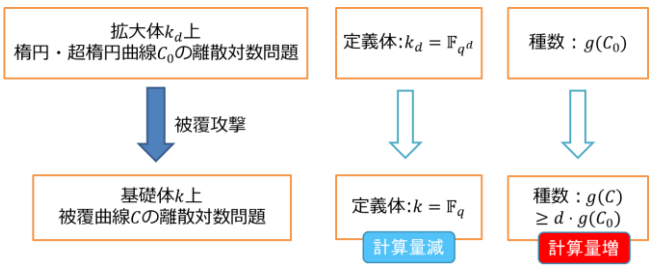
⇐楕円曲線

種数2の
超楕円曲線⇒



被覆攻撃

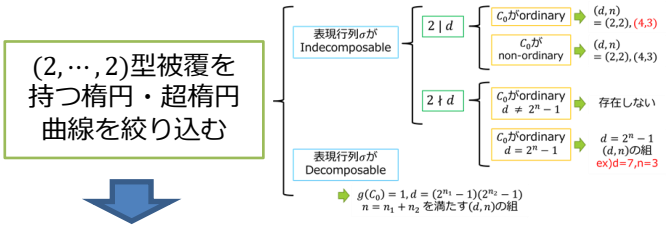
拡大体k_d上の楕円・超楕円曲線に対する攻撃手法である.



基礎体k上の曲線に移すことにより離散対数問題の計算量が小さくなれば攻撃成功となる. 実際, 160bitの鍵長の安全性を持つ曲線が最大107bit程度まで低下したという結果もある. 同種条件とは, $g(C) = d \cdot g(C_0)$ のことをいう.

被覆攻撃の対象となる曲線の分類

(2,…,2)型被覆と呼ばれる構造を持つ楕円・超楕円曲線は, 被覆攻撃の対象となることがわかっている.



同種条件を満たす楕円・超楕円曲線を構成する

以下は被覆攻撃の対象となる曲線の分類結果の抜粋である.

$C_0/k_d : y^2 + g(x)y = f(x) \quad (\deg g(x) = g(C_0) + 1, \deg f(x) = 2g(C_0) + 2)$
$(I)\ {}^{\sigma}g(x) = g(x), (II)\ {}^{\sigma}g(x) \neq g(x)$

	ex) $g(C_0) = 3,\ d = 3,\ n = 2$
(I)	$L(f(x)) = f(x) + {}^{\sigma}f(x) + {}^{\sigma^2}f(x) = 0$
(II)	$g(x) = g_1(x)(x + \alpha^q)(x + \alpha^{q^2}),\ \alpha \in k_3 \backslash k$ $g_1(x) \in k[x],\ \deg g_1(x) \leq 2,\ L((x + \alpha)^2 f(x)) = 0 \quad (*1)$
(II)	$g(x) = (x + \alpha^q)^2(x + \alpha^{q^2})^2,\ \alpha \in k_3 \backslash k,\ L((x + \alpha)^4 f(x)) = 0 \quad (*2)$

$(*1)\ L((x + \alpha)^2 f(x)) = (x + \alpha)^2\ f(x) + (x + \alpha^q)^2\ {}^{\sigma}f(x) + (x + \alpha^{q^2})^2\ {}^{\sigma^2}f(x) = 0$
$(*2)\ L((x + \alpha)^4 f(x)) = (x + \alpha)^4\ f(x) + (x + \alpha^q)^4\ {}^{\sigma}f(x) + (x + \alpha^{q^2})^4\ {}^{\sigma^2}f(x) = 0$

結論

百瀬らが発表した偶標数楕円・超楕円曲線の同種条件下での分類結果を再検討した. 分類手法に証明を与え, 情報を整理追加することで, より使いやすい分類表を作成した また分類表の曲線について, 初めて具体的な構成方法を示した.