被覆攻撃の対象となる偶標数有限体上の楕円・超楕円曲線に関する研究

On elliptic and hyperelliptic curves over finite fields of even characteristic subjected to the cover attack

鐘ケ江柊子・法制・倫理分科会・中央大学

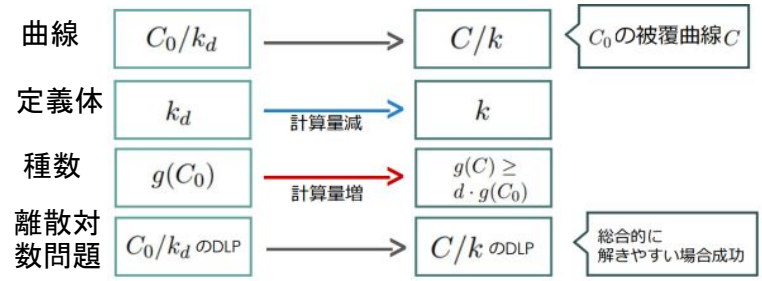
The covering attack is known to transform the discrete logarithm problem of an elliptic or a hyperelliptic curve C_0 defined over the d degree extension k_d := F_q^d of a finite field k := F_q (q: a power of a prime number), to the discrete logarithm problem of a covering curve C of C_0 defined over k. Analysis of the covering attack turned out mathematically difficult, hence curves subject to the attack are not yet completely understood. In this paper, we re-examine the known classifications and investigate with a detailed proof of existence of covering curves for cases which were missing in the classification table. And we classify elliptic and hyperelliptic curves over finite fields of even characteristic subjected to the cover attack without the isogeny condition.

研究背景・目的

拡大体上で定義された楕円・超楕円曲線暗号は高速化や効率的な実装に向いているが,特定の攻撃である被覆攻撃が存在する. これらの攻撃を受ける曲線のその対象範囲の全体は未だ完全に明らかになっていない.したがって, この攻撃の対象となるような被覆について調査することは重要な課題であるが,偶標数は奇標数よりも扱いが難しく分類が困難であった. しかし, 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, 同種条件下という条件のもと曲線分類が行われ, さらに村井らによって分類の再検討が行われた. 本論文では, 明らかになっていなかった曲線の存在判定と証明を与えた. また, 同種条件を満たさない一般の場合のあるクラスで,攻撃の対象となる曲線の分類を行った.

被覆攻撃

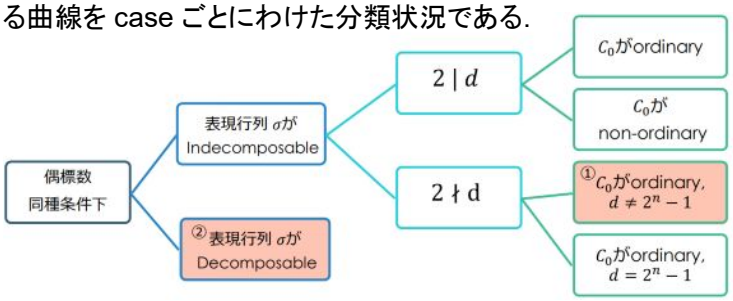
拡大体 k_d 上の楕円・超楕円曲線に対する攻撃を指す.



同種条件は, $g(C) = d \cdot g(C_0)$ という種数の条件を指す.
また,同種条件を満たさない一般の場合については,
$g(C) \geq d \cdot g(C_0) + e\ (e > 0)$ という種数の条件を指す.

同種条件下の攻撃対象曲線分類

$(2, \ldots, 2)$ 型被覆という構造を持つ楕円・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.以下は攻撃対象となる曲線を case ごとにわけた分類状況である.



分類されているが,曲線の存在判定と証明は完了していなかった

①→被覆曲線が存在しない→被覆攻撃に対して安全
②→条件を満たす被覆曲線が存在→被覆攻撃を受ける危険な曲線

Decomposable case

攻撃対象となる曲線の定義式は以下の定義式で与えられる.

$$C_0 : y^2 + xy = x^3 + \frac{b}{\rho_1^2}x^2 + \left(\frac{1}{\rho_1\rho_2}\right)^2 x$$

(n_1 or $n_2 = 1$ のとき C は hyperelliptic)

攻撃対象曲線例:

$g(C_0)$	d, n	C_0	isHyper(C)
1	$d = (2^{n_1} - 1)(2^{n_2} - 1) = 3$ $n = n_1 + n_2 = 3$ $(n_1, n_2) = (2, 1)$	$y^2 + xy = x^3 + ax^2 + bx$ $a \in k,\ \mathrm{Tr}(b) = 0,\ b \in k_3 \backslash k$	Hyper

※村井らの論文より引用かつ抜粋

同種条件を満たさない攻撃対象曲線分類

偶標数有限体上楕円曲線において同種条件を満たさない $g(C_0) = 1,\ d = 4,\ n = 3$ の下で存在する, 被覆攻撃の対象となる曲線の分類と構成を行った.共役曲線から構成される曲線が代数的閉体上既約であることを仮定し,標準形の係数を変更した場合に条件を満たすか判定した. 以下は分類した結果の抜粋である.

$(g(C_0), d, n, e, g(C))$	C_0	条件
$(1, 4, 3, 3, 7)$	$y^2 + xy = ax^3 + cx$	$a, c, ac \in k_4 \backslash k_2,$ $\mathrm{Tr}(a) = \mathrm{Tr}(c) = 0$
$(1, 4, 3, 2, 6)$	$y^2 + y = ax^3 + bx^2 + cx + d$	$a \in k_2 \backslash k,$ b or $c \in k_4 \backslash k_2,$ $\mathrm{Tr}(b) = \mathrm{Tr}(c) = \mathrm{Tr}(d) = 0$

結論

偶標数同種条件下での被覆攻撃に関して, 村井らが行った再検討では証明されていなかった曲線の存在判定と証明を与えた.また, 同種条件を満たさない一般の場合のあるクラスで攻撃対象曲線の分類を行った.