同種条件を満たさない被覆攻撃の対象となる偶標数拡大体上の種数3 ordinary imaginary 超楕円曲線の分類

A Classification of Genus 3 Hyperelliptic Curves Over Finite Fields of Even Characteristic Without the Isogeny Condition Subject to the Cover Attack

佐藤 佑哉・暗号/認証分科会・中央大学大学院

研究背景/目的

拡大体上に定義された楕円・超楕円曲線に対して有効とされる被覆攻撃と呼ばれる攻撃手法が存在する.この攻撃は対象となる曲線の使用を避けることで回避できるため,被覆攻撃の対象となる曲線の分類は非常に重要な研究課題である.本研究では,タイトルが示す未解明の曲線の分類を目指す.

用いる分類手法

上里の手法[1]を用いる.この手法は,研究対象である曲線C_0の共役曲線から構成される曲線${}^{F}C_0$の種数$g({}^{F}C_0)$の総和を得るために必要となる.この手法を用いた結果, 被覆攻撃の対象となるタイトルが示す曲線の分類を実現し、さらに分類した曲線の存在証明に成功した.

研究計画

同種条件を満たさない偶標数拡大体上の種数3超楕円曲線のうち,未だ分類が行われていないrealやnon-ordinaryな曲線の分類を目標として研究活動を行う.

参考文献

[1] 上里優介ほか, “ガロア群の群作用下の曲線の体系的な種数評価を用いた被覆攻撃の対象となる偶標数有限体上楕円曲線および種数2超楕円曲線の分類”, Proc. of SCIS2025, IEICE Japan, 2025.