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楕円・超楕円曲線の分類

A family of elliptic and hyperelliptic curves over extension fields of even characteristic subjected to the cover attack without the isogeny condition

鐘ヶ江柊子・法制・倫理文化会・中央大学大学院

研究背景・研究目的

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．本研究は，被覆攻撃の対象となる，偶標数拡大体上被覆曲線が同種条件を満たさないあるクラスの楕円曲線の完全分類を目的とする．

提案手法

偶標数拡大体上の同型変換によって得られるすべての共役曲線から構成される曲線が$\mathbb{P}^1$と同型かどうかの判定によって，同種条件の確認と分類をする．

今後の方針

偶標数拡大体上で，一般的な場合に対しての被覆攻撃対象曲線の存在判定と完全分類を行う．