同種条件を満たさない被覆攻撃の対象となる偶標数有限体上の楕円・超楕円曲線の分類

A classification of elliptic/hyperelliptic curves over finite fields of even characteristic without isogeny condition subject to cover attack

上里優介・暗号・認証分科会・中央大学大学院

研究背景・研究目的

被覆攻撃と呼ばれる攻撃手法により，拡大体上に定義される一部の楕円・超楕円曲線暗号の安全性が低下する恐れがある．しかし，攻撃の対象となる楕円・超楕円曲線の構造は完全には解明されていない．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．

提案手法

偶標数有限体上楕円曲線について，以下の2手法を計算機上に実装して分類を行う．

1. 楕円曲線とその共役曲線から構成される曲線をすべて列挙し，各曲線が$\mathbb{P}^1$か否かという仮定から分類を行う．本手法は実装および一部の曲線の分類に成功した．
2. 分類表の各caseは$x^d + 1 \in \mathbb{F}_2[x]$ (dは定義体の拡大次数)の真の約数(あるいは約数を2つ並べた組)によってラベル付けされることから，すべての約数を列挙して対応する係数条件を調べる．本手法は手法1より効率的であり，現在実装中である．

今後の方針

手法2の実装を完了させ，楕円曲線の完全分類を目指す．また種数2以上の超楕円曲線の分類およびその手法の確立を目指す．