被覆攻撃の対象となる楕円・超楕円曲線とその被覆曲線に関する研究

Research on Elliptic and Hyperelliptic Curves Subject to Cover Attack and Their Covering Curves

吉田幸貴・暗号/認証分科会・中央大学大学院

研究目的

楕円・超楕円曲線暗号は，有限体の拡大体上で定義することでより効率的な計算が可能となる．しかし拡大体上楕円・超楕円曲線には，「被覆曲線」を用いるこ とで解読の計算量が低下するような場合が数多く存在することも明らかとなっている．本研究ではそのような曲線を分類・構成し，安全性を明らかにする．

一年次の活動

楕円・超楕円曲線暗号の安全性には、曲線の位数がalmost prime(素数または巨大な素因数を持つ)であることが不可欠である。被覆攻撃への耐性を評価するため、特定の曲線における位数の性質を調査した。
Imaginary, Non-ordinary楕円曲線では、ごく一部のケースを除き、almost primeとなる確率は極めて低いことが判明した。種数2超楕円曲線においては、ヤコビ群が楕円曲線の直積と同種になる場合、位数が分解され安全性が低下する。Zeta関数の既約性判定により、特定の条件において分解が生じやすい傾向を確認した。

研究計画

位数がalmost primeにならない係数条件についての研究を行う予定である．
また被覆攻撃の対象とならない曲線について，暗号利用を想定した「ホワイトリスト」の作成を行う予定である．