有限拡大体上定義された楕円曲線とその被覆曲線の離散対数問題に対する安全性評価

Security evaluation of elliptic curve discrete logarithm problem over extensions of finite field under cover attack

西垣佳亮・暗号認証分科会・中央大学大学院

研究背景

楕円曲線暗号には被覆攻撃と呼ばれる攻撃があり，特定の曲線に於いては安全性が下がることがある．被覆攻撃の対象となる楕円曲線の分類と被覆曲線の構成は研究されているものの，被覆攻撃の下で安全性を評価する研究は少ない．

研究目的

本研究では，実際の計算機実験によって被覆攻撃が楕円曲線暗号の安全性に及ぼす脅威を明らかにする．

研究計画

今年度は数学的な対象を扱うプログラムの実装を行った．
来年度は，大きな規模の離散対数問題を解くために，分散コンピューティングのためのシステムとプログラムを構築し，計算機実験を行う．