楕円・超楕円曲線暗号の安全性と効率性を高める取組み

Security and Efficiency Evaluation of Elliptic/Hyperelliptic Curves Cryptography

奥村祐太・暗号認証分科会・中央大学大学院

研究背景

公開鍵暗号の一つに楕円・超楕円曲線暗号が存在する．楕円・超楕円曲線暗号は従来の RSA 暗号などと比べて，短い鍵長で同等の安全性を確保できる．その長所を活かして近年 IoT 機器などに採用されている．

研究目的

拡大体上に定義された一部の楕円・超楕円曲線暗号に対して被覆攻撃という攻撃が存在する．曲線を分類することで被覆攻撃の対象にならない楕円・超楕円曲線を用いることができる．

研究計画

今年度は被覆攻撃及び分類に必要な知識を身に着けた．来年度は楕円・超楕円曲線暗号の安全性だけでなく効率性にも着目して研究を行う．