数理・情報のフロンティア
2020 年度採択研究代表者

2020 年度
年次報告書

相川　勇輔

三菱電機(株)　開発本部　情報技術総合研究所
研究員

楕円曲線を用いた耐量子計算機暗号の安全性解析と高効率化

§1. 研究成果の概要

量子コンピュータによる解読に耐性を持つとされる公開鍵暗号は総称して耐量子計算機暗号とよばれる。その有力な候補の一つに、同種写像暗号がある。この暗号は、楕円曲線が 2 つ与えられたときにそれらの間の同種写像を計算せよという問題（同種写像問題とよぶ）の計算量的困難性に安全性の根拠を置いている。この暗号は耐量子計算機暗号の候補の中でも最もコンパクトな暗号を達成できる。しかし、その研究の歴史は浅く、そのため安全性の解析が未だ不十分であるといった課題を抱えている。

その重要な方式の一つに SIDH 方式があり、2020 年度はその安全性解析へ向けて研究を開始した。本研究では、Deuring 対応を利用し、四元数代数の観点から同種写像問題の困難性に関する知見を得ることを目的とする。その際に重要となる数論アルゴリズムに、同種写像問題の四元数代数類似を解く KLPT アルゴリズムがある。しかし、このアルゴリズムは一般にアウトプットのサイズが大きいことや、一般的な性能評価がされていないことなどの問題点がある。

今回、我々は出力サイズの削減を目標にアルゴリズムに改良を施し、その性能の評価を sage での実装により行った。さらに、この改良によってアルゴリズムの実行時間の高速化にも貢献した。より具体的には、今回の研究で動作確認ができた最大の有限体サイズである 45 ビットにおいて、出力サイズを 16%削減、さらに実行時間（実時間での比較）を 63%削減することに成功した。本結果は論文にまとめ国際会議 ICMC に投稿し、採択された。