数理・情報のフロンティア
2020 年度採択研究者

2021 年度
年次報告書

相川 勇輔

三菱電機(株) 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データサイズの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、これは NIST による耐量子計算機暗号の標準化暗号候補の一となっている。SIDH 方式は 2011 年に提案された新しい暗号であるため、将来的な実用化に向けては、その安全性に関する知見を蓄えることが重要な研究課題である。

2021 年度は 2020 年度に引き続き、同種写像問題の安全性解析研究を進めた。本研究のアプローチは、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というものである。その際に重要となる数論アルゴリズムの一つに、構成的 Deuring 対応アルゴリズムがある。このアルゴリズムは四元数代数のイデアルが入力されたときに、Deuring 対応により対応する同種写像の情報を復元するアルゴリズムである。しかし、このアルゴリズム内の楕円曲線のねじれ点計算がボトルネックとなり、これまでの研究では 10 ビット程度の標数での実装例しか得られていなかった。今回、我々はねじれ点計算に核多項式の Symbolic formula の技術を応用することで大幅に計算量を削減、その結果 25 ビットの標数での実装例を構成することに成功した。この結果は数理暗号分野の主要な国際会議 MathCrypt に採択され、学術雑誌 Mathematical Cryptology より出版された。