数学・数理科学と情報科学の連携・融合による情報活用基盤の創出と社会課題解決に向けた展開　2022 年度 年次報告書

2021 年度採択研究代表者

高木 剛

東京大学 大学院情報理工学系研究科
教授

ポスト量子社会が求める高機能暗号の数理基盤創出と展開

主たる共同研究者：

國廣 昇（筑波大学 システム情報系 教授）
田中 圭介（東京工業大学 情報理工学院 教授）
若山 正人（日本電信電話(株) NTT コミュニケーション科学基礎研究所 数学研究プリンシパル）

研究成果の概要

本研究課題では、暗号の危殆化を回避するために、量子計算機を用いた攻撃や電力解析によるサイドチャネル攻撃など想定される多様な攻撃者を考察し、それらの攻撃に対しても耐性を有する暗号技術の実現を目指した数理の基盤的研究を推進する。更には、大規模分散システム向けに、ブロックチェーンを利用した非中央集権セキュリティ機能を有する暗号システムを構築する。

2022 年度は、本課題の参加研究者が集まる全体会議を 2022 年 5 月 13 日と 12 月 16 日に開催し、合計 6 件のチュートリアル講演（量子公開鍵暗号、量子制御代数、同種写像暗号、Farey Fractal など）により、暗号分野と数学分野の研究課題を議論した。また、2022 年 9 月 12 日にはドワンゴ・セミナールームにおいてミニワークショップ「量子計算と暗号」開催し、量子ウォークとゼータ関数、数論と量子計算に関して議論を行なった。更に、2023 年 2 月 20 日に東京大学本郷キャンパスにおいてミニワークショップ「若手成果発表会」を実施し、修士・博士課程を修了する学生やポスドクから最新研究の成果発表があった。

本年度の成果として、合計で 31 編の原著論文を発表した。特に、研究代表者の高木らは、同種写像暗号で用いる一般的なスカラー倍算および同種写像計算の公式に関する論文を Mathematical Cryptology において発表した [1)]。主たる共同研究者の若山らは、量子相互作用の物理学と代数曲面の幾何及び数論・表現論をつなぐ非対称ラビ模型の論文を Communications in Number Theory and Physics において発表した [2)]。國廣グループの篠原らは、実際の量子計算機(IBM Quantum)により、7 量子ビットを用いて 2 ビットの離散対数問題の求解に成功している [3)]。主たる共同研究者の田中らは、符号ベースで構成された効率的な耐量子ディジタル署名 SURF に関する安全性評価を行った [4)]。最後に、研究代表者の高木らは、多変数多項式暗号の効率的な構成に関して第7回「辻井重男セキュリティ論文賞」特別賞を受賞するなど、チーム全体で7件の受賞があった。

【代表的な原著論文情報】

1) “The Generalized Montgomery Coordinate: A New Computational Tool for Isogeny-based Cryptography,” Mathematical Cryptology, Vol.2, pp.36-59, 2022.
2) “Degeneracy and Hidden Symmetry for the Asymmetric Quantum Rabi Model with Integral Bias,” Communications in Number Theory and Physics, Vol. 17, pp.615-672, 2022.
3) “The Present and Future of Discrete Logarithm Problems on Noisy Quantum Computers,” IEEE Transactions on Quantum Engineering, Vol.3, pp.1-21, 2022.
4) “Analysis of (U, U+V)-code Problem with Gramian over Binary and Ternary Fields,” The 25th International Conference on Information Security and Cryptology (ICISC 2022), LNCS 13849, pp.435-449, 2022.