

2023 年度年次報告書

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

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。

2023年度は、本課題の参加研究者が集まる全体会議を5月12日と12月8日に開催し、合計7件のチュートリアル講演(多変数多項式問題、量子情報処理、リー群の表現論など)により、暗号分野と数学分野の研究課題を議論した。また、9月8日には、エクスパンダーハッシュ関数、ブロックチェーンなどに関するミニワークショップを開催した。更に、2024年2月14日には、若手成果発表会を実施し修了学生らの成果発表があった。

本年度の成果として、合計で32編の原著論文を発表した。特に、研究代表者の高木らは米国標準技術研究所が進めるポスト量子暗号の標準化プロジェクトに効率的な署名方式 QR-UOV を提案した。また、劣決定系の多変数多項式問題の困難性を考察し、署名方式 MAYO の安全性の計算量が25ビット低下することを示した¹⁾。主たる共同研究者の若山らは、非可換調和振動子のシフト版(η -NCHO)を導入し、それが非対称量子ラビ模型の被覆模型となることを示した²⁾。主たる共同研究者の國廣らは、署名方式 ECDSA に対するフーリエ解析ベース攻撃に対する安全性評価を行い³⁾、更には格子暗号 CRYSTALS-Kyber に対する相関電力解析を改良し200個のトレースを用いた解読に成功した⁴⁾。主たる共同研究者の田中らは、安全性証明手法に関わるメタ-メタ帰着について新たな知見を得ている。

また、アウトリーチ活動として暗号関係の解説記事(合計10編)を、電子情報通信学会誌や岩波書店『科学』において執筆した。最後に、国際会議 IWSEC 2023 において Best Student Paper Award⁵⁾などチーム全体で4件の受賞があった。

【代表的な原著論文情報】

- 1) Yasufumi Hashimoto, “An Improvement of Algorithms to Solve Under-defined Systems of Multivariate Quadratic Equations,” JSIAM Letters, Vol.15, pp.53-56, 2023.
- 2) Cid Reyes-Bustos and Masato Wakayama, “Covering Families of the Asymmetric Quantum Rabi Model: η -Shifted Non-commutative Harmonic Oscillators,” Communications in Mathematical Physics, Vol.403 pp.1429-1476, 2023.
- 3) Shunsuke Osaki and Noboru Kunihiro, “Extended Attacks on ECDSA with Noisy Multiple Bit Nonce Leakages,” ICISC 2023, LNCS 14561, pp. 163-184, 2023.
- 4) Yen-Ting Kuo and Atsushi Takayasu, “A Lattice Attack on CRYSTALS-Kyber with Correlation Power Analysis,” ICISC 2023, LNCS 14561, pp. 202-220, 2023.
- 5) Hiroki Furue, Yasuhiko Ikematsu, “A New Security Analysis Against MAYO and QR-UOV Using Rectangular MinRank Attack,” The 18th International Workshop on Security, IWSEC 2023, LNCS 14128, pp.101–116, 2023.