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

2021 年度
年次報告書

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

§1. 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。

2021 年度は、本課題の全体イベントとして 2021 年 12 月 23 日に Kickoff ミーティングを開催し、本プロジェクトに参加する研究者 25 名から自己紹介と研究内容に関する説明があった。また、研究課題が開始となる年度として、国内外の研究会などで 6 件の招待講演を含む合計 21 件の口頭発表を行った。更に、主たる共同研究者の國廣は、数学セミナーにおいて本研究課題の中心的研究テーマとなる耐量子計算機暗号に関する解説記事を発表した。

本年度の研究成果として、チーム全体で合計 9 編の原著論文を発表した。特に、主たる共同研究者の國廣らは、量子計算機による素因数分解で用いられる量子ゲート数の評価に関する論文を IEEE Transactions on Quantum Engineering において発表した [1)]。主たる共同研究者の田中らは、国際暗号学会が発行する権威あるジャーナル論文誌 Journal of Cryptology において、暗号方式の安全性モデルとなる鍵依存型平文の選択暗号文攻撃に関する論文を発表した [2)]。最後に、研究代表者の高木らは、多変数多項式求解問題の困難性を基にしたディジタル署名 QR-UOV に関して報道発表を行い、2022 年 1 月 1 日の産経新聞に掲載された。

§2. 研究実施体制

(1) 高木グループ(東京大学)

① 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)

② 研究項目

・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

(2) 若山グループ(日本電信電話株式会社)

① 主たる共同研究者:若山　正人 (日本電信電話株式会社　NTT 基礎数学研究センタ　数学研究プリンシパル)

② 研究項目

・量子相互作用模型と量子誤り訂正符号の研究

(3) 國廣グループ(筑波大学)

① 主たる共同研究者:國廣　昇 (筑波大学システム情報系　教授)

② 研究項目

・ポスト量子暗号に対する物理攻撃モデルの研究

(4) 田中グループ(東京工業大学)

① 主たる共同研究者:田中　圭介 (東京工業大学情報理工学院　教授)

② 研究項目

・大規模分散システムにおける高機能暗号の研究

【代表的な原著論文情報】

1) Kento Oonishi, Tomoki Tanaka, Shumpei Uno, Takahiko Satoh, Rodney Van Meter, and Noboru Kunihiro, "Efficient Construction of a Control Modular Adder on a Carry-Lookahead Adder Using Relative-phase Toffoli Gates", IEEE Transactions on Quantum Engineering, Vol. 3, 2021.

2) Keisuke Tanaka, Fuyuki Kitagawa, Takahiro Matsuda, "CCA Security and Trapdoor Functions via Key-Dependent-Message Security", Journal of Cryptology, Vol. 35, No. 2, 2022.