現代の数理科学と連携するモデリング手法の構築
2014 年度採択研究代表者

2020 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

次世代暗号に向けたセキュリティ危殆化回避数理モデリング

§1. 研究成果の概要

本研究課題では，拡大している情報セキュリティの脅威に対して，想定される最強の攻撃者をモデル化して，予想困難な未来のセキュリティ危殆化回避モデルを確立することを目標としている．特に，暗号理論で不可欠な安全性の数理モデリングを行い，想定される最強の攻撃者をモデル化し，その攻撃に対する防御方法の確立を目指している．

2020 年度は，量子計算機に対して耐性のあるポスト量子暗号に関する研究を推進し，合計で 61 編の原著論文を発表した．特に，国際暗号学会 IACR が主催するトップレベルの国際会議となる ASIACRYPT 2020 において同種写像問題の困難性を安全性の根拠としてハッシュ関数を必要としない世界初の公開鍵暗号，金融セキュリティ分野のトップカンファレンスとなる Financial Cryptography 2021 においてスマートコントラクトを必要としないブロックチェーンを用いた高速な決済システムを発表した．また，量子計算機の基本素子で用いられる量子ラビ模型の数学解析を目指して，トロッター・加藤の積公式に基づいて量子ラビ模型の熱核（プロパゲータ）を逐次積分の級数（離散経路積分）として表す解析的公式を与えた．

JST の国際強化支援の助成を受けて 2019 年に開催した国際シンポジウム Mathematics, Quantum Theory, and Cryptography の予稿集を Springer 社から出版した．更に，主たる共同研究者の若山は，「数学通信」（日本数学会）から光とゼータ関数の特殊値に関する解説論文を発表した．最後に，博士課程 1 年の江利口らの論文が国際会議 ISITA 2020 において Best student paper award を受賞し，修士課程 2 年の樋渡らの論文が情報処理学会主催の国内シンポジウム CSS 2020 で学生論文賞を受賞した．

§2. 研究実施体制

(1)「高木」グループ

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

・次世代高機能暗号の構成と安全性評価

(2)「若山」グループ

① 主たる共同研究者：若山　正人　（東京理科大学理学部第一部、教授）

② 研究項目

・量子相互作用の数理と L-関数からの次世代暗号研究

(3)「田中」グループ

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

・数学オブジェクトと帰着マッピングの数理モデル

(4)「國廣」グループ

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

・攻撃者のモデル化と実社会環境下での安全性評価

【代表的な原著論文情報】

1) Tomoki Moriya, Hiroshi Onuki, Tsuyoshi Takagi, “SiGamal: A supersingular isogeny-based PKE and its application to a PRF”, ASIACRYPT 2020, LNCS 12492, pp.551-580, 2020.
2) Maxim Jourenko, Mario Larangeira, Keisuke Tanaka, “Payment Trees: Low Collateral Payments for Payment Channel Networks”, Financial Cryptography (FC 2021), 2021.
3) Hiroki Furue, Koha Kinjo, Yasuhiko Ikematsu, Yacheng Wang, Tsuyoshi Takagi, “A Structural Attack on Block-Anti-Circulant UOV at SAC 2019”, PQCrypto 2020, LNCS 12100, pp.323-339, 2020.
4) Cid Reyes-Bustos and Masato Wakayama, “Heat kernel for the quantum Rabi model: II. Propagators and spectral determinants”, Journal of Physics A: Mathematical and Theoretical, Vol. 54, 115202, 2021.
5) Reo Eriguchi, Noboru Kunihiro, “Strong Security of Linear Ramp Secret Sharing Schemes with General Access Structures”, Information Processing Letters, Vol. 164, 106018, 2020.