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

2019 年度
実績報告書

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．

2019 年度は，4 月 25 日と 12 月 17 日に CREST 暗号数理の参加研究者を集めた全体会議を実施し，完全準同型暗号，同種写像暗号，非可換グレブナー基底，格子暗号，ラマヌジャングラフ，可積分系に関して，数学問題の暗号理論応用に関して議論した．また，JST の国際強化支援策から助成を受ける形で，2019 年 9 月 25-27 日に九州大学 IMI において International Symposium on Mathematics, Quantum Theory, and Cryptography (MQC 2019)を開催した．量子計算，量子相互作用，精度保証付き数値計算，最適化モデリング手法，グラフ理論，ポスト量子暗号などの幅広い分野に関する講演がなされ，国内外の大学，研究機関，企業から 66 名の参加があった．講演を論文形式でまとめた予稿集を Springer-Nature 社から出版する予定である．また，2019 年 3 月 27 日に予定していた CREST 暗号数理ミニワークショップ「若手研究者講演」は新型コロナウィルスのため中止となった．今年度は，参加メンバから本研究課題に関する 3 冊の書籍（木本一史著『レクチャー離散数学』サイエンス社，高木剛著『暗号と量子コンピュータ』オーム社，青野良範・安田雅哉著『格子暗号解読のための数学的基礎』近代科学社）を出版した．

特に今年度は，各研究グループは以下の項目に関して研究を進めた．

○高木グループ： 2019 年度は，ポスト量子暗号の安全性や効率性に関する考察を行った．多変数多項式の困難性に基づく署名 ELSA に対する多項式時間の攻撃法を提案した論文が，論文誌 Journal of Information Processing において 2019 年度の Outstanding Paper Award を受賞した．また，多変数多項式をベースとした署名 SOFIA に関して，安全性を低下させることなく公開

鍵のサイズを約 3 割削減する方法を提案した. 本成果は, 国際会議 CANDAR 2019 において Outstanding Paper Award を受賞した. 更には, 同種写像暗号 CSIDH のサイドチャネル攻撃に対して安全となる高速な定時間実装を考察し, Edwards 曲線を用いた高速化アルゴリズムも提案した. 後者は, 国際会議 IWSEC 2019 において Best Poster Award を受賞した. 格子暗号に関しても研究を進め, 格子簡約アルゴリズム LLL の低次元や deep insertion 版における改良を行い, LWE 問題をベースとした鍵交換方式や鍵漏洩に耐性がある階層型 ID ベース暗号を提案した.

○若山グループ： 2019 年度の研究は以下の通りである. (1) 非対称量子ラビ模型の固有値の退化を記述する論文を完成させ, 投稿した(2020年1月に受理された). (2) 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を逐次積分の級数として表す明示的公式を与えた. 非自明な量子相互作用モデルにおいて熱核の解析的明示式が得られた恐らく初めての例である. (3) 加藤クラスのポテンシャルを持つネルソン模型と呼ばれる量子場模型において, 束縛状態の指数関数的減衰性を示した. (4) 國廣グループとの協働として, Lubotzky-Phillips-Sarnak 型のグラフ族について, 特別な場合にそのラマヌジャン性を示した. (5) 群・部分群ペアグラフの一般化を導入し, ラマヌジャングラフの族を構成する問題を提起した. (6) 論文[1]において, プレシズムの特別な場合として, 一般線形群の標準表現に対し, その対称テンソル積の2階および3階対称テンソル積をある多項式代数の中に実現し, その最高ウェイトベクトルがなす極大一次独立系を具体的に与えた. ここでの手法は対称群とそのヤング型部分群との球関数の記述, 従って対応するペアグラフの固有値の記述への応用が期待される.

○田中グループ： 2019 年度は, 暗号システムの設計の際に有用となる数学オブジェクトに関する研究として, 計算リソースが極端に制限された状況においても動作するような要素, Fine-grained 暗号要素の考察を主に行った. Fine-grained 暗号要素とは, 計算リソースが制限された攻撃者に対して安全, かつ, 攻撃者より少ない計算リソースしか持たない正当な参加者が実行できる暗号技術である. 我々は基本的な暗号技術である一方向性置換, hash proof system (選択暗号文攻撃に耐性をもつ公開鍵暗号を実現する要素), 落とし戸付き一方向性関数に着目し, これらの具体的方式の提案を行った. さらに, 暗号システムの安全性証明の際に有用となる帰着マッピングに関する研究として、選択平文攻撃に対して安全な公開鍵暗号、選択暗号文攻撃に対して安全な公開鍵暗号, 落とし戸付き一方向性関数の関係性についての考察を行った[2].

○國廣グループ： 2019 年度も引き続き, 実社会でよく用いられている, もしくは, 用いられることが強く期待されている暗号に関する 5 つの課題に関して研究を行った. (1) 次世代暗号として期待されている格子暗号に対して, より精密な安全性評価を与えた. 具体的には, 格子簡約基底における短いベクトルを列挙する最悪ケースのコストが, 従来知られている評価よりも小さいこと, さらに, これまでのアプローチに従う限り, 与えた評価が最適であることを示した[3]. (2) RSA 暗号の秘密鍵にノイズが乗った系列が得られた時に秘密鍵を復元するアルゴリズムに関して研究を行った. Sliding Window 法を用いた実装において, 二乗算および乗算が, ノイズ付きで得られた時に秘密鍵を復元するアルゴリズムを提案した. (3) 量子アルゴリズムに対する現代暗号, 特に, 楕円曲線暗号に対する影響に関して解析を行った. 剰余逆元計算を効率的に行う量子回路の提案を行い, 提案した量子回路を用いて, 楕円離散対数問題を解く手法を提案し, 必要となるリソースの厳密な評価を行った. (4) ポスト量子暗号, 特に同種写像に基づく鍵共有方式の提案を

行った. 定数ラウンドで複数人での鍵共有方式を行う方式に関して, 研究を進め, 静的な仮定の下で安全性が証明された方式の提案に成功した. (5) 効率的な秘密分散法に関する研究を行った. 特定のアクセス構造を実現する理想的な秘密分散法を用いた最適な複数割り当て法, および, 多値アクセス構造を実現する秘密分散法を用いた最適な複数割り当て法を提案した.

【代表的な原著論文】

[1] Kazufumi Kimoto, Soo Teck Lee, “Highest weight vectors in plethysms,” Communications in Mathematical Physics, Available online 4 December, 2019. (DOI: 10.1007/s00220-019-03639-6)

[2] Fuyuki Kitagawa, Takahiro Matsuda, Keisuke Tanaka, “CCA Security and Trapdoor Functions via Key-Dependent-Message Security,” Annual International Cryptology Conference – Advances in Cryptology - CRYPTO 2019, pp. 33-64, 2019. (DOI: 10.1007/978-3-030-26954-8_2)

[3] Noboru Kunihiro, Atsushi Takayasu, “Worst case short lattice vector enumeration on block reduced bases of arbitrary blocksizes,” Discrete Applied Mathematics, Vol.277, pp.198-220, 2020. (DOI: 10.1016/j.dam.2019.09.017)

§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 （九州大学マス・フォア・インダストリ研究所　教授/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