現代の数理科学と連携するモデリング手法の構築
平成 26 年度採択研究代表者

H27 年度
実績報告書

高木　剛

九州大学マス・フォア・インダストリ研究所
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. 研究実施体制

(1)「高木」グループ
① 研究代表者：高木　剛 （九州大学マス・フォア・インダストリ研究所，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）
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 （東京工業大学大学院情報理工学研究科，准教授）
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 （東京大学大学院新領域創成科学研究科，准教授）
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

§2. 研究実施の概要

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．

平成 27 年度は，参加研究者を集めた CREST 暗号数理全体会議を 5 月 8 日と 12 月 15 日に実施し，合計 8 件のチュートリアル講演（暗号理論の安全性証明技法，量子計算機の基礎数理，ラマヌジャングラフなど）により研究者間で暗号分野における数学問題の共有を行なった．また，CREST 暗号数理ミニワークショップ「幾何と暗号」及び「L-関数と暗号」を開催して，参加研究者の個別の専門研究テーマに関して議論を進めた．更に，本課題で研究を推進しているポスト量子暗号に関する有力な国際会議 PQCrypto2016 を，九州大学において 2016 年 2 月 24-26 日に CREST 共催として開催した．アメリカ国立標準技術研究所 NIST から次世代暗号の標準化プランの発表があり，次世代暗号の安全性評価や効率性に関して幅広い議論が行なわれた．また，アウトリーチ活動として，一般向け数学雑誌「数学セミナー」において本領域の研究内に関する解説記事を 3 件発表した．

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： 今年度は，ポスト量子暗号の候補である格子暗号に関して，LWE 問題を基にした代表的な方式（Regev05, LPR11 など）に対して，JavaScript によるソフトウェア実装を行い演算の性能評価を行なった．この成果は，国際会議 Third International Symposium on Computing and Networking（CANDAR'15）において発表し，Outstanding Paper を受賞した．また，ダルムシュタット工科大の主催する格子解読のチャレンジ問題において 625 次元の解読世界記録を達成し，ドイツの Dagstuhl Seminar において招待講演を行った．更に，國廣グループと共同で，超特異楕円曲線の 3-同種写像のラマヌジャングラフを用いた高速なハッシュ関数の構成を行なった．本成果は，暗号と情報セキュリティシンポジウム SCIS2016 および 2016 年日本応用数理学会研究部会連合発表会で発表し，三菱電機と九州大学と共同で特許出願を行った．他には，秘密分散と符号理論を用いたポスト量子暗号の安全性に関する論文を IEICE Transaction に 2 編掲載した．

○若山グループ： 平成 27 年度の研究は以下の通りである．(1)NcHO のスペクトル問題のホイン微分方程式による記述を，固有関数が偶関数である場合に与える論文が出版された（Wakayama, Int. Math. Res. Not. 03 (2016), 759-794). (2)ラビ模型のスペクトルにおける数論的構造の研究への第一歩として，そのスペクトルゼータ関数の解析接続が得られた（プレプリント: 杉山, Spectral Zeta Functions for the Quantum Rabi Models）. (3)有限群とその部分群のペアに対してケーリーグラフの拡張を与える論文が出版された[2]. グラフの彩色問題に由来する予想であるラテン方陣の Alon-Tarsi 予想とリース行列式や対称群上の球関数との関係について研究を進めた（プレプリント: 木本, Wreath determinants, spherical functions on symmetric groups and the Alon-Tarsi conjecture）. (4)高木グループとの共同研究として，

Garg-Gentry-Halevi によって提案されている格子暗号の安全性についての解析を行い，既存の結果の改良を得た（論文投稿中： Security Analysis of Cryptosystems Using Short Generators over Ideal Lattices）.

○田中グループ： 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，数学オブジェクトに求められる暗号学的な機能要件の抽出を試み，暗号分野で近年議論が進んでいる情報漏洩に着目した．具体的には，continual leakage モデルと呼ばれる強い漏洩モデルのもとでの署名の安全性に関する考察を行い，暗号学的な機能要件の抽出に一部成功している[3]．これに加え，暗号要素として用いることの可能性を検討するために，3 次元多様体・結び目/絡み目等の数学要素に関する様々な基礎的考察を行った．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，安全性証明の新たな手法を目指し，既存の高度な安全性証明手法を深く理解するためランダムオラクルモデルとスタンダードモデルの双方の手法に着目し，具体的な証明手法の調査とその拡張を行った．安全性証明の際に有用となる帰着マッピングの要素の可能性を探るために，流体方程式に関する様々な基礎的考察を行った．

○國廣グループ： 平成 27 年度は，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 3 つの課題に関して研究を行った．(1) 秘密鍵にノイズが生じた時の RSA 鍵回復アルゴリズムの，従来の研究よりも詳細な解析を行なった．従来の研究で未解決であった理論限界を達成するアルゴリズムを提案し，この攻撃に対する防御手法を提案した．さらに攻撃対象を，共通鍵暗号 AES にも広げた．(2)格子理論を用いた RSA 暗号およびその変形方式に関する安全性評価を行った．中国人の剰余定理に基づく RSA 暗号に対して，秘密鍵が部分的に漏洩した場合の安全性解析，法が未知である線形方程式の求解条件の改良，$p^r q$ というタイプの RSA 暗号の変形方式に対する安全性評価を包括的に行った[1]．いずれの研究においても，改良の結果得られた値は，従来知られている最良の値を上回っており，真に優れた評価となっている．(3)ポスト量子暗号，その中でも，特に有望な格子暗号の安全性に関する研究を行った．特に，安全性の根拠となっている LPN 問題，LWE 問題の困難さの解析を行った．この研究では，ノイズが小さい時に，従来知られている方式よりも，少ないサンプルで解を求めるアルゴリズムの提案に成功している．以上の成果により，難解な査読付き国際会議に 6 件採録され，3 つの論文賞を受賞している．

代表的な発表論文

[1] Atsushi Takayasu and Noboru Kunihiro, “How to Generalize RSA Cryptanalyses”, PKC 2016, LNCS 9615, pp. 67-97, 2016. (DOI: 10.1007/978-3-662-49387-8_4)

[2] Cid Reyes-Bustos, “Cayley-type graphs for group–subgroup pairs”, Linear Algebra and its Applications, Vol.488, pp.320-349, 2016. (DOI: 10.1016/j.laa.2015.09.049)

[3] Yuyu Wang and Keisuke Tanaka, “Generic transformation to strongly existentially unforgeable signature schemes with continuous leakage resiliency”, ACISP 2015, LNCS 9144, pp.213-229, 2015. (DOI: 10.1007/978-3-319-19962-7_13)