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

2018 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．

2018 年度は，CREST 暗号数理の参加研究者を集めた全体会議を 2018 年 5 月 24 日と 12 月 11 日に実施し，合計 9 件のチュートリアル講演（多変数多項式暗号，量子計算，ラマヌジャングラフ，量子ラビ模型など）により，暗号分野と数学分野を横断した研究課題に関して議論した．また，2018 年 9 月 7 日に奈良春日野国際フォーラムにおいて CREST 暗号数理「未解決問題ワークショップ」を開催し，格子暗号，同種写像問題，情報理論的安全性などに関する未解決問題に関して議論を行なった．更に，2019 年 3 月 16 日には九州大学にて CREST 暗号数理ミニワークショップ「若手研究者講演」を実施し，修士・博士課程を修了する学生やポスドクから最新研究の成果発表があった．また，NHK の番組「サイエンス ZERO」において，本研究課題のポスト量子暗号に関する特集が取り上げられるなど，社会からも大きな注目を集めている．
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：** 格子暗号に関して議論を進め，円分体の小さな元で生成されるイデアルを秘密鍵として利用した暗号の安全性を，ディリクレの L 関数の s=1 における特殊値の近似値を求める問題として考察した．2 冪の次数が 10 以上となる円分体においては，秘密鍵として用いる小さな生成元が高い確率で復元可能となる理論的証明および実験的な検証を行なった[1]．また，多変数多項式を用いた署名方式を考察し，Rainbow 署名を高速化した方式 ELSA に対して選択平文攻撃が適応可能であることを示した．本成果は国際会議 IWSEC2018 において Best Paper Award を受賞した．更には，多変数多項式を用いた暗号方式となる EFCp$^-$の安全性を

考察して，既存のパラメータに対するグレブナ基底を用いたハイブリット攻撃を提案した．本論文は，情報処理学会主催のコンピュータセキュリティシンポジウム CSS 2018 において学生論文賞を受賞した．

**○若山グループ：** 2018 年度の研究は以下の通りである．(1) 量子ラビ模型の固有値の間隔分布について，計算機による数値計算を利用して観察を行った．(2) 量子ラビ模型の熱核の明示的公式を導くためのプロジェクトを開始して，ある程度の見通しが得られた．(3) Lubotzky-Phillips-Sarnak によるラマヌジャンクラフの構成の一般化について議論し，それに基づくハッシュ関数の提案およびその安全性評価を行った（國廣グループとの協働）．(4) 完全グラフおよび完全二部グラフの無限族に対するラプラシアン行列のアルファ行列式の（サイズが発散するときの）極限挙動について調べ，明示的な結果を与えた．(5) 円分体のイデアルを利用した格子暗号の安全性について議論を行った（高木グループとの協働）．

**○田中グループ：** 2018 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，一旦，基礎的な要素に立ち戻り，従来の数論に関する計算問題に着目した．特に，公開鍵暗号システムがランダムオラクルといった強い仮定を用いることなくシミュレーションベース受信者選択的開示攻撃という強い安全性をもつことを示した．また，数学オブジェクトの可能性を検討するために，二重グラフ複体とファイブレーションの特性類や，3次元時空の極大曲面に関する考察など，新しいアプローチを提示するなど基礎的考察を行った．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，帰着に密接に関わるプロトコルの一般的構成手法について着目した．特に，関数型秘密鍵暗号方式から識別不可能性をもつ難読化方式を一般的に構成できることを示すことに成功した．本成果は，暗号分野のトップカンファレンスとなる国際会議 EUROCRYPT 2018 において発表した[2]．また，帰着マッピング要素の可能性を探るために，対称な双曲型-放物型非線形偏微分方程式系の半空間上での収束速度に関する考察を与えるなど基礎的考察を行った．

**○國廣グループ：** 2018 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 4 つの課題に関して研究を行った．(1) 秘密鍵に依存する計算系列，特に，Sliding Window 法によるべき乗計算時において，二乗算と乗算の系列が得られた時の RSA 鍵回復アルゴリズムの改良を行った．従来の研究よりも，高い確率で秘密鍵全体の復元に成功している．(2)格子理論を用いた RSA 暗号およびその変形方式，楕円曲線暗号に関する安全性評価を行った[3]．CRT-RSA 暗号に対して，秘密鍵 d の上位部分および下位部分が漏洩した状況を考え，従来よりも少ない漏洩ビットから秘密鍵全体の復元できることを示している．(3) 量子計算機に対する現代暗号の安全性評価に関して研究を進めた．Shor の素因数分解アルゴリズムにより，量子計算機ができれば理論的には簡単に RSA 暗号は解読されることが知られている．これまでに行われている実際の量子計算機を用いた実験を統一的に理解し，素因数分解実験としては不適当であることを指摘している．さらに，(4) ポスト量子暗号実現の研究自身も行っている．特に，同種写像に基づく複数人鍵交換プロトコルや 1 ラウンド認証グルー

プ鍵共有の提案に成功している. さらに, ラマヌジャングラフに基づくハッシュ関数の提案, 安全性評価を行っている. 以上の成果により, 難解な査読付き国際会議に 5 件採録され, 1 つの論文賞を受賞している.

**代表的な発表論文**

[1] Shinya Okumura, Shingo Sugiyama, Masaya Yasuda, Tsuyoshi Takagi, "Security analysis of cryptosystems using short generators over ideal lattices", Japan Journal of Industrial and Applied Mathematics, Volume 35, Issue 2, pp.739‐771, 2018. (DOI: 10.1007/s13160-018-0306-z)

[2] Fuyuki Kitagawa, Ryo Nishimaki, Keisuke Tanaka, "Obfustopia Built on Secret-Key Functional Encryption", EUROCRYPT 2018, LNCS 10821, pp.603-648, 2018. (DOI: 10.1007/978-3-319-78375-8_20)

[3] Atsushi Takayasu, Noboru Kunihiro, "Partial Key Exposure Attacks on RSA: Achieving the Boneh-Durfee Bound", Theoretical Computer Science, Vol.761, pp.51-77, 2019. (DOI: 10.1016/j.tcs.2018.08.021)

## §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)

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 (東京大学大学院情報理工学系研究科 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