「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

H28 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 28 年度は，参加研究者を集めた CREST 暗号数理の全体会議を 4 月 27 日と 12 月 22 日に実施し，合計 9 件のチュートリアル講演（代数的組み合わせ論，漸近安定性や分数拡散方程式，整数計画法と最短ベクトル問題，量子ラビ模型の数理など）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，9 月 28 日に東京大学において CREST 暗号数理ミニワークショップ「格子・光子と暗号」を開催し，量子ラビ模型のスペクトルゼータ関数や量子光学モデルのスペクトルなどに関して議論を行なった．更に，平成 29 年 2 月 9 日には九州大学にて CREST 暗号数理ミニワークショップ「計算数論と暗号」を実施し，参加学生の 5 名により RSA 秘密鍵復元攻撃や同種写像暗号に関する成果発表があった．また，平成 29 年 3 月 22-23 日に東工大で CREST 主催により 3rd Asian Post-Quantum Cryptography Forum を開催した．オープニングでは CREST 数理モデリングの坪井総括から挨拶を頂き，国内外からポスト量子暗号に関する招待講演10件があり，米国標準技術研究所 NIST からは今後のポスト量子暗号の標準化計画が報告された．

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： ドイツ・ダルムシュタット工科大が主催する格子暗号の解読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，暗号分野のトップレベルの国際会議 Eurocrypt 2016 で発表した[1]．また，格子暗号において(Learning with Errors) LWE 問題を基にした暗号方式に対して，法 q が比較的大きな場合の鍵復元攻撃に対する安全性評価や JavaScript により IoT ディバス上での暗号演算の性能評価を実施した．一方，多変数多項式暗号に関して，多変数多項式暗号の中で最も効率的な SRP 暗号化方式を考察し，公開鍵に巡回構造を導入することによりサイズを 55%圧縮する方法を提案し，国際会議 ACISP2016 で発表した．更に，Cubic 型 UOV 署名を高速化するアルゴリズムと ZHFE 暗号化方式で用いる効率的な鍵生成アルゴリズムを提案した．最後に，代数曲面の求セクション問題の困難性を基にした公開鍵暗号の安全性を，グレブナ基底アルゴリズムにより評価し，国際会議 CANDAR 2016 において Outstanding Paper を受賞した．

○若山グループ： 平成 28 年度の研究は以下の通りである．(1)非対称ラビ模型のスペクトル退化問題をリー環 sl2 の表現を通じて記述する論文が出版された（Wakayama, Journal of Physics A: Mathematical and Theoretical 50 (2017)）．スペクトル退化を記述する多項式と組合せ論的な量とを結びつける公式を得た（若山・Reyes-Bustos）．(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を与える論文が出版された[2]．

(3)有限群とその部分群のペアに対して定義されるケイリー型グラフのスペクトルの群指標を用い

た明示公式を，部分群がアーベル群の場合に与えた（木本）．(4)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，対称群上の球関数，プレシズムとの関係をまとめて投稿した（木本, Wreath determinants, spherical functions on symmetric groups and the Alon-Tarsi conjecture）．(5)二面体群の一般化であるフロベニウス群の場合に，ケーリーグラフが必ずラマヌジャングラフとなるような次数の限界を決定し，それが自明な限界とならない条件が素数に関するハーディ・リトルウッド予想と関係することを明らかにした（Hirano-Katata-Yamasaki, Bull. Aust. Math. Soc. 94 (2016), 373-383）．(6)数体 K のデデキントゼータ関数に対する深リーマン予想を仮定した場合の，ガロア拡大 L/K に付随するチェボタレフ型密度定理の誤差項のオーダー評価を行った（Reyes-Bustos）．

○田中グループ： 平成 28 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，そこに求められる機能要件として暗号理論分野で議論が進んでいる，構造保存署名と呼ばれる強力な機能について主に着目した．具体的には，構造保存署名に対して，通常の機能を満たすものから非常に強力な機能を満たすものへの変換可能性について考察し，機能要件の一部整理に成功している．これを含む暗号学的側面からの考察に加え，数学オブジェクトを暗号要素として用いる可能性を検討するために，ファイバー束に対する特徴量クラス等の数学要素に関する様々な基礎的考察を行なった．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，特定の安全性を満たす秘密鍵暗号における秘密鍵長の下界を得るため解析手法の改良等を行なうとともに，帰着マッピング要素の可能性を探るために，流体の境界層等に関する様々な基礎的考察を行った．

○國廣グループ： 平成 28 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 3 つの課題に関して研究を行った．(1)秘密鍵に依存するアナログ値が得られた時の 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．従来の研究では，理想的な観測モデルのみしか議論を行っていなかったが，近似的な分布が得られた時，および，分散が得られた時に有効なアルゴリズムの提案を行った．(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．共通の RSA 法 N に対して，複数の鍵ペアが与えられた時の安全性評価を行った．その結果，従来知られている解読の条件の改善に成功した[3]．本論文は国際会議 ACISP 2016 において Best student award を受賞した．複数の素数の積からなり RSA 暗号の変形方式の安全性評価を行った．(3)ポスト量子暗号，その中でも，有望な同種写像を用いた暗号方式の提案を行った．n 者間鍵共有方式を経由することにより，同種写像に関連する問題を安全性の根拠とした擬似ランダム関数の構成に成功した．以上の成果により，査読付き論文誌 1 件，難解な査読付き国際会議に 7 件採録され，4 つの論文賞を受賞している．

代表的な発表論文

[1] Yoshinori Aono, Yuntao Wang, Takuya Hayashi, and Tsuyoshi Takagi, “Improved Progressive BKZ Algorithms and Their Precise Cost Estimation by Sharp Simulator”, EUROCRYPT 2016, LNCS 9665, pp.789-819, 2016.
(DOI:10.1007/978-3-662-49890-3_30)

[2] Singo Sugiyama, “Spectral zeta functions for the quantum Rabi models”, Nagoya Mathematical Journal, pp.1-47, 2016. (DOI: 10.1017/nmj.2016.62)
[3] Atsushi Takayasu and Noboru Kunihiro, “Partial Key Exposure Attacks on RSA with Multiple Exponent Pairs”, ACISP2016, LNCS 9723, pp. 243-257, 2016. (DOI: 10.1007/978-3-319-40367-0_15)