「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

H29 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　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 29 年度は，4 月 27 日と 12 月 14 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，合計 9 件のチュートリアル講演（多変数多項式暗号，深リーマン予想，ラマヌジャングラフなど）により，暗号分野と数学分野の研究課題を議論した．また，9 月 6 日に湘南国際村センターにおいて 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，量子ランダムウォーク，同種写像問題などに関して議論を行なった．更に，平成 29 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「量子と暗号」を実施し，Braak 教授のラビ模型に関する招待講演や量子アルゴリズムに関する成果発表があった．また，本課題の研究成果と未解決問題をまとめた査読付論文集（15 編：計 365 ページ）を，平成 29 年 7 月に Springer 社の Mathematics for Industry シリーズから出版した．最後に，本課題の研究活動は，平成 29 年 8 月 3 日放送の NHK クローズアップ現代において，安全な次世代暗号として取り上げられ大きな注目を集めた．

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： 格子暗号の安全性解析として，NTRU 暗号の法を大きくした場合の攻撃方法を考察した．円分体を用いた部分体格子攻撃において，部分体の幅の選択方法を改良しより小さな法に対して攻撃が可能な領域を示した[1]．また，多変数多項式を用いた暗号化方式を考察し， SRP 暗号化方式に対する公開鍵サイズの圧縮方法，ZHFE 暗号化方式に対する選択暗号文攻撃および効率的な鍵生成アルゴリズムに関する論文を発表した．更に，ラマヌジャングラフを利用したハッシュ関数に関して，3-正則な Cui グラフから構成した LPS ハッシュ関数に対する安全性を考察した．同種写像暗号に関しては，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．最後に，研究代表者の高木はポスト量子暗号の研究動向に関するサーベイ論文を電子情報通信学会英文誌で発表した．

○若山グループ： 平成 29 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記述する多項式と組合せ論的な量とを結びつける論文が出版された．(2)一般のパラメタに対する非対称ラビ模型のスペクトル退化予想が解決した．sl2 の最低ウェイト表現による非 Juddi 固有値の記述を得た（論文投稿中）．(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論文が出版された．(4)ケイリーグラフによるラマヌジャングラフ構成の古典例である LPS グラフの拡張を考察した．

○田中グループ： 平成 29 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，エラー訂正符号に着目した．特に，符号ベース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強い匿名性を満たす最初の方式の提案に成功した[2]. また, 数学オブジェクトの可能性を検討するために, 低次元トポロジーでのジョンソン準同型の概念を用いる非アーベル岩澤理論への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変換手法について着目した. 特に, 任意のラウンド数をもつ合理的な秘密分散方式を, 定数ラウンドをもつプロトコルに Nash 均衡性を保ちながら変換する変換手法の構成に成功した. また, 帰着マッピング要素の可能性を探るために, 一般的な双曲型-放物型非線形偏微分方程式系の半空間上での定常解の存在と漸近安定性を示すなど基礎的考察を行った.

○國廣グループ: 平成 29 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. 従来の研究では, 系列が誤りなく観測できる理想的なモデルのみでしか議論を行っていなかったが, 本年度は, 小さいノイズがあっても秘密鍵を復元できるアルゴリズムの提案に成功している. (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. CRT-RSA 暗号に対して, 秘密鍵 d_p, d_q が小さい時には解読できることが知られているが, この限界を大幅に更新することに成功している. 具体的には, d_p, d_q が $N^{0.091}$ よりも小さい時に攻撃が成功している[3]. さらに, いくつかの RSA 暗号に対する格子理論を用いた安全性評価を継続的に行っている. また, 楕円曲線暗号に対する格子理論による安全性評価を開始し, Edwards 曲線へも適用範囲を拡張している. (3) ポスト量子暗号の中でも, Information Set Decoding Problem はその困難性として注目されているが, この問題の困難性に関しても着手している. さらに, (4) ポスト量子暗号実現の研究自身も主開始している. 特に, 格子理論を用いた高機能暗号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, 2 つの論文賞を受賞している.

代表的な発表論文

[1] Dung Hoang Duong, Masaya Yasuda, and Tsuyoshi Takagi, “Choosing Parameters for the Subfield Lattice Attack Against Overstretched NTRU", ISC 2017, LNCS 10599, pp.79-91, 2017. (DOI: 10.1007/978-3-319-69659-1_5)

[2] Yusuke Yoshida, Kirill Morozov, Keisuke Tanaka, “CCA2 Key-Privacy for Code-Based Encryption in the Standard Model”, PQCrypto 2017, LNCS 10346, pp.35-50, 2017. (DOI:10.1007/978-3-319-59879-6_3)

[3] Atsushi Takayasu, Yao Lu, and Liquiang Peng, “Small CRT-Exponent RSA Revisited”, Eurocrypt 2017, LNCS 10211, pp.130-159, 2017. (DOI: 10.1007/978-3-319-56614-6_5)