戦略的創造研究推進事業　CREST
研究領域「現代の数理科学と連携するモデリング手法の構築」
研究課題「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」

研究終了報告書

研究期間　2014年10月～2022年3月

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）

§1 研究実施の概要

(1)実施概要

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 26 年 10 月から，参加研究者を集めた全体会議を 14 回および特定のテーマに関するミニワークショップを 11 回開催して定期的にミーティングを行い，量子計算機に対して耐性のあるポスト量子暗号に関する安全性評価などの研究を推進してきた．代表的な研究成果としては，高木グループでは，格子暗号で用いられる最短ベクトル問題の計算量評価を暗号分野のトップ国際会議 Eurocrypt 2016 で発表し，円分体のイデアル理論による格子暗号の安全性に関する論文を Japan Journal of Industrial and Applied Mathematics から発表した．また，若山グループでは，量子計算機の理論基盤である量子ラビ模型におけるスペクトル構造および数論的構造の研究に関する論文を International Mathematics Research Notices などから発表してきた．更には，田中グループは，暗号方式の秘密鍵や乱数の漏洩耐性を数学オブジェクトとして考察した論文を国際会議 Asiacrypt 2016, Eurocrypt 2018, CRYPTO 2019 などから発表し，國廣グループは，秘密鍵が部分的に漏洩した場合の安全性評価を包括的に行い国際会議 PKC 2016, EUROCRYPT 2017 やジャーナル論文誌 Journal of Cryptology などで発表した．最後に，高木グループでは，同種写像暗号の新しい効率的な方式を国際会議 Asiacrypt 2020 で発表し，効率的な多変数多項式暗号に対する安全性評価に関する論文が Journal of Information Processing において 2019 年の Outstanding Paper Award を受賞している．また，本課題の前半部分の研究成果と未解決問題をまとめた査読付論文集を，2017 年に Springer 社の Mathematics for Industry シリーズから出版した．本研究課題の総計として，原著論文 275 編，招待講演 180 件，受賞 49 件，特許申請 1 件などの研究成果を得た．

本研究課題に所属するメンバは国際的に高く評価されており，主要な国際会議（Post-Quantum Cryptography 2019, Elliptic Curve Cryptography 2018 など）や研究集会(Dagstuhl Seminar, DIMACS Workshop など)で招待講演を行ってきた．また，本研究課題の国際的な研究活動として，2016 年 2 月には，ポスト量子暗号を専門とする国際会議 PQCrypto 2016 を九州大学において CREST 共催で開催し，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が発表された．このアジア版となる Asia PQCrypto Forum 2017 を，2017 年 3 月に東京工業大学において CREST 共催として開催した．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，予稿集を Springer 社から出版した．これらの国際的な研究活動により，本研究プロジェクトが次世代暗号の研究における世界的拠点となることが期待できる．

最後に，本プロジェクトの研究成果に関するアウトリーチ活動として，数学セミナーなどへの寄稿やサーベイ論文集の編纂，国際フォーラムの主催，報道発表やテレビ取材なども積極的に進めている．2019 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．本課題の研究活動は，2017 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た．更に，2018 年 6 月には NHK 教育テレビ『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組まれ，代表者の高木が出演するなど大きな注目を集めている．

(2)顕著な成果

＜優れた基礎研究としての成果＞

1． 大規模解読実験による攻撃者モデル／次世代暗号の安全性解析
概要:ポスト量子暗号の有力な候補として，最短ベクトル問題の困難性を基にした格子暗号がある．最短ベクトル問題を高速に解くことが可能な Progressive BKZ を提案し，そのアルゴリズムの厳密な計算量評価を与えた．また，ダルムシュタット工科大学が主催する最短ベクトル問題のコンテストにおいて，提案アルゴリズムにより625次元の解読世界記録を達成した．この成果は，国際暗号学会が主催するトップカンファレンスとなる Eurocrypt 2016 やジャーナル論文誌 International Journal of Information Security などで発表を行った．

2． 想定される最強の攻撃者のモデル化／量子相互作用モデルの理解促進
概要:現在実用化されている暗号は，量子計算機により多項式時間で解読されることが知られている．よって量子計算機の理論基盤である量子相互作用モデルの(スペクトル構造、特に系のプロパゲータ等に対する)理解を深め明確にすることは，暗号の危殆化回避の議論において重要である．量子ラビ模型におけるスペクトル構造および代数的構造の研究として，そのフルヴィッツ型スペクトルゼータ関数の全平面への解析接続や，スペクトルの退化構造，プロパゲータの明示式を与える論文を Journal of Physics A, International Mathematics Research Notices, Nagoya Mathematical Journal などに発表した。

3． 数学問題による暗号構成・安全性評価／格子理論/多変数多項式
概要:多変数多項式の求解問題の困難性を基にしたディジタル署名の安全性を考察した．多変数多項式暗号の主要な方式として Rainbow, HFEv-, 5-pass 認証などが知られているが，Rainbow を改良した ELSA 署名に対して平文と署名の多項式関係から張られる空間の構造を調べることにより多項式時間の攻撃アルゴリズムを提案した．本成果は，国際会議 IWSEC 2018 において Best Paper Award を受賞し，ジャーナル論文誌 Journal of Information Processing において 2019 年の Outstanding Paper Award も受賞している．

＜科学技術イノベーションに大きく寄与する成果＞
1． 数学問題による暗号構成・安全性評価／数学オブジェクト
概要： 暗号システム設計の際にコアとなる数学オブジェクトに関する研究，安全性証明で想定される最強の攻撃者をモデル化する帰着マッピングに関する研究を田中グループにおいて幅広く実施した．双方に関連し，暗号分野で近年議論が進んでいる秘密鍵や乱数の漏洩耐性，鍵依存平文安全性など強力な機能について着目した．特に，構造保存署名と呼ばれる機能に対しては，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整理に成功した．本成果は，国際暗号学会 IACR 主催のトップカンファレンス Asiacrypt 2016, Eurocrypt 2018, CRYPTO 2019 などで発表した．

2. 社会環境下での安全性評価／公開鍵暗号の安全性モデル
概要:格子理論を用いた RSA 暗号に対する安全性評価の研究を，國廣グループにおいて幅広く実施した．具体的には，RSA 暗号に対する幾つかの高速化方式に注目し，秘密鍵が部分的に漏洩したときの安全性評価を包括的に行い，従来知られている最良の攻撃限界値の更新に成功している．これらの結果は，学会でも高く評価されており，国際会議 ACISP2016 Best Student Award などを受賞し，幾つかのトップカンファレンス PKC 2016, EUROCRYPT 2017 やジャーナル論文誌 Journal of Cryptology, Theoretical Computer Science などにおいて論文を発表した．

3. 実社会環境下での安全性評価／ポスト量子暗号の性能評価

概要：量子計算機の時代にも安全となる同種写像暗号 SiGamal 暗号を提案した．現在までに提案されている同種写像暗号は，鍵交換方式 SIDH/CISDH やハッシュ関数を利用した暗号化方式 SIKE などが提案されていた．本論文では，同種写像問題の困難性を安全性の根拠とする暗号方式において，ハッシュ関数を必要としない世界初の公開鍵暗号を提案した．特に，同種写像暗号 CISDH-512 からの計算量のオーバーヘッドが 2.62 倍と効率的な方式となる．また，同種写像暗号 CSIDH において，位数 3 の元に対する衝突が存在することを指摘し，それを回避することにより高速に暗号演算が可能となることを示し，更には，秘密鍵に依存する計算時間の差異を 2 点の保存により回避する高速実装方法を提案した．

＜代表的な論文＞

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.
概要：円分体のイデアルを利用した格子暗号の安全性に関して議論した．この格子暗号では，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ており，秘密鍵を復元することはディリクレの L 関数の s=1 における特殊値の近似値を求める問題となる．本論文では，既存研究の漸近的な評価ではなく，暗号で利用される固定したパラメータに対する安全性評価を考察した．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．

2．Kazufumi Kimoto, Cid Reyes-Bustos, Masato Wakayama, “Determinant Expressions of Constraint Polynomials and the Spectrum of the Asymmetric Quantum Rabi Model”, International Mathematics Research Notices, Volume 2021, Issue 12, pp.9458-9544, 2021.
概要：量子ラビ模型はハミルトニアンの形から Z/2Z-対称性をもつことがわかり，それによりスペクトルの縮退や積分可能性が明らかになっていた．本論文の非対称量子ラビ模型はこのような対称性をもたない．しかし，それを定義するパラメータが 1/2 のときに，数値計算において縮退が示唆されていた（Li-Batchelor 2015）．それは数学的に証明されパラメータが一般の半整数のときにも予想の形で提出されていたが（Wakayama 2017），これを一般の半整数に対して証明したのが本論文である．この論文に基づき，最近になって，物理学者が存在を信じていた「隠れた対称性」の発見にも至った．

3．Atsushi Takayasu, Yao Lu and Liqiang Peng, “Small CRT-Exponent RSA Revisited”, Journal of Cryptology 32, pp. 1337-1382, 2019.
概要：広く普及している CRT-RSA 暗号に対して，秘密鍵が小さいときの安全性評価を実施した．復号，署名の速度を考慮した場合，秘密鍵を小さくすることが望ましいが，どの程度小さくすると安全性が損なわれないかが明らかでなかった．これまでに，秘密鍵が N の 0.073 乗よりも小さいときには，破られることが知られていたが，この研究では，N の 0.122 乗まで拡張することに成功している．この成果は，暗号分野のトップカンファレンスである Eurocrypt 2017 で発表を行うとともに，改良アルゴリズムを暗号理論で権威のあるジャーナル論文誌 Journal of Cryptology において発表した．

§2 研究実施体制

（1）研究チームの体制について

① 「高木」グループ
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）
研究項目（次世代高機能暗号の構成と安全性評価）
・次世代暗号の安全性解析，格子理論/多変数多項式，ポスト量子暗号の性能評価

② 「若山」グループ
主たる共同研究者:若山　正人(東京理科大学データサイエンスセンター　客員教授)
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)
・深リーマン予想(DRH), 量子相互作用モデルの理解促進, ラマヌジャングラフ

③ 「田中」グループ
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)
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)
・帰着マッピング, 数学オブジェクト

④ 「國廣」グループ
主たる共同研究者:國廣　昇(筑波大学システム情報系　教授)
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)
・攻撃者のモデル化, 公開鍵暗号の安全性モデル

(2)国内外の研究者や産業界等との連携によるネットワーク形成の状況について
海外の研究者としては, ポスト量子暗号の第一人者となる Buchmann 教授(ドイツ・ダルムシュタット工科大), 多変数多項式暗号 Rainbow を提案した Ding 教授(中国・清華大), 実用的な格子暗号 NTRU を提案した Pipher 教授(米国・ブラウン大)と研究協力を進めている. また, 本研究課題は, 三菱電機および NTT 研究所が参画する形で研究チームが構成されており, 産業界からのニーズを踏まえた上で研究課題を推進している.