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

H26 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．

H26 年度のチーム内のミーティングとして，H26 年 11 月 7 日に研究代表者と主たる研究者 3 名による打合せ，H27 年 1 月 19-20 日に参加研究者を集めた CREST 暗号数理キックオフミーティング，H27 年 3 月 27 日にラマヌジャングラフと暗号に関する研究集会を実施した．更には，相互量子作用と数理物理，ポスト量子暗号の最新動向などに関するワークショップを開催した．

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： 2 次方程式の求解問題（MQ 問題）を利用した公開鍵暗号方式 Quaternion Rainbow に対して Rank 攻撃が効率的に適応できることを証明し，IEICE Transaction で原著論文として発表した．また多変数多項式を利用した楕円曲線暗号に対する攻撃方法(FPPR 法)の計算量と使用メモリ量が削減可能となる手法を考察した．拡大次数 29 次の標数 2 の有限体上で定義される楕円曲線暗号を，計算機代数ソフトウェア Magma を用いて AMD Opteron 6276 において約 34 日で解読することに成功した．この結果は，Pacific Journal of Mathematics for Industry に掲載された．更に，最短ベクトル問題(SVP)に対しては，BKZ アルゴリズムで利用される列挙法のブロックサイズの改良による高速化を行い，ダルムシュタット工科大が開催する SVP 解読チャレンジで 500 次元の解読記録を達成した．本成果は，暗号と情報セキュリティシンポジウム SCIS2015 で発表した．

○若山グループ： 今年度は，NcHO に関するこれまでの研究（数論・表現論・解析的微分方程式）を，方法論を含めグループで再検討しさらに押し進めるとともに，NcHO 及び一般ラビ模型やその回転波近似（RWA）模型のスペクトルの研究を表現論から迫る明確な糸口を発見した．また，群行列式の一般化である，有限群とその部分群のペアに対して定義される「群リース行列式」という不変量について，群として有限アーベル群を取った場合，適当な（群の元の）順序づけと変数の特殊化の下で，それが二項多項式の積に分解することを証明した．この結果は，Journal of Combinatorial Theory, Series A として出版した．群として有限アーベル群を取った場合，適当な（群の元の）順序づけと変数の特殊化の下で，それが二項多項式の積に分解することを証明した．

○田中グループ： 今年度は，数学オブジェクトの暗号学的な機能要件の数理モデル化を試みた．そのために，暗号分野で用いられている多くの具体的方式の調査を，そこで用いられている数学オブジェクトに注目し行った．この調査研究により，現在用いられている数学オブジェクトに要求される機能要件や，数学オブジェクトに要求される性質について，徐々に明らかになりつつある．また，数学オブジェクトのいくつかの重要な具体的な機能に関しては，その機能を用いた具体的暗号プロトコルを構成し，その安全性や効率に関して考察を行った．これにより，対象となった数学オブジェクトの機能に関する深い理解が得られた．これらの深い理解を調査研究と合わせて来年

度の研究につなげる.

○國廣グループ： 今年度は，従来よりも複雑なノイズモデルからの RSA 鍵回復アルゴリズムの研究を行なった. 非対称なアナログ情報が得られるノイズモデルに対して，分散値を陽に用いるアルゴリズムの提案を行なった. さらに，このアルゴリズムの前処理として，EM アルゴリズムを用いて分散値を推定するフェーズを入れることにより，観測値以外の情報を用いることなく，より大きいノイズからの鍵回復に成功している. ついで，公開鍵暗号だけでなく，攻撃対象を共通鍵暗号 AES に広げた. また，代表的な格子問題の一つである LPN 問題に対しても，効率的なアルゴリズムの提案を行なった. これらの成果は，暗号と情報セキュリティシンポジウム SCIS2015 で発表した. さらに，実社会への応用として，LPN 問題の困難さに安全性の根拠をおいた軽量認証方式の安全性評価を与えた. また，small inverse problem に対する効率的なアルゴリズムを提案し，このアルゴリズムを適用することにより，複数素数 RSA 暗号に対するより，精密な安全性評価を与えた.

代表的な発表論文

[1] Yun-Ju Huang, Christophe Petit, Naoyuki Shinohara, and Tsuyoshi Takagi, “Improvement of FPPR method to solve ECDLP”, Pacific Journal of Mathematics for Industry, Vol.7-1, Springer, 2015. (DOI: 10.1186/s40736-015-0012-6)

[2] Kei Hamamoto, Kazufumi Kimoto, Kazutoshi Tachibana, and Masato Wakayama, “Wreath determinants for group-subgroup pairs”, Journal of Combinatorial Theory, Series A, Vol.133, pp.76-96, 2015. (DOI:10.1016/j.jcta.2015.02.002)

[3] Atsushi Takayasu, and Noboru Kunihiro, “General Bounds for Small Inverse Problems and Its Applications to Multi-Prime RSA,” 18th Annual International Conference on Information Security and Cryptology, ICISC2014, LNCS 8949, pp. 3-17, 2015. (DOI:10.1007/978-3-319-15943-0_1)