高機能暗号の理論的安全性評価

研究代表者　高島　克幸
（教育学部 数学科 教授）

１．研究課題

現在、インターネットが広く普及すると共に、その利用形態は高度化しており、インターネットの根幹を支える暗号技術も IoT 機器やクラウド環境での利用など幅広い場面での利活用が想定されている。これにより、安全性と共に利便性も追求することが可能な高機能暗号を研究開発することの重要性が高まっている。

本研究課題では、さまざまなアプローチにより高機能暗号の理論的な安全性評価を行っていく。とりわけ、耐量子計算機暗号技術は、理論的のみならず実際的にも大変重要であり、本研究で、理論的な安全性評価を進めて、安全な耐量子計算機暗号技術の確立に寄与することを目指す。そのため、特に、本研究課題では数理的技法を駆使した安全性評価に取り組む。例えば、格子・符号暗号に関連する計算問題の困難性を評価することで格子・符号暗号の安全性評価を進めていく。また、素因数分解や離散対数問題の正確な量子計算時間評価も、既存の RSA 暗号や離散対数型暗号から次世代耐量子暗号への移行を考える際に重要であるので本研究で取り上げる課題である。そして、格子暗号などの耐量子計算機暗号の安全性証明では量子計算モデルを用いる必要があるなど、従来の安全性証明技法の新たな見直しも重要な研究テーマである。

２．主な研究成果

2024 年 10 月から始まった本研究プロジェクトにおいて、2025 年度に、現在投稿中・投稿予定の論文も含めて、以下の研究成果を上げることができた。

2.1 耐量子計算機暗号安全性に関係する量子計算の改良

素因数分解・離散対数問題に対する量子計算量を削減して正確に評価することは次世代耐量子計算機暗号への移行を考える上で重要な研究テーマである。2023 年に発表された Regev 素因数分解法に基づいた Ragavan-Vaikuntanathan の方法では、フィボナッチ数列をべき乗算の加算鎖に用いることで量子メモリの削減に成功している。佐々木-高島は、文献［1］で、フィボナッチ数列の代わりにトリボナッチ数列を用いたときの量子メモリと回路サイズを見積もることで、パラメータに関するさまざまなバリエーションが得られることを示した。また、谷らは、文献［2］で、暗号安全性とも関係する量子探索問題に対する新たなアルゴリズムを提案している。

2.2 Naor 変換により得られる署名の BUFF 安全性

近年、署名の標準的な偽造困難性である EUF-CMA 安全性とは別に BUFF 安全性と呼ばれる安全性が研究されている。中野-楽-高島は、文献［3］で、ID ベース暗号(IBE)から Naor 変換で得られる署名方式の BUFF 安全性について調べた。特に、基となる IBE が IBK 安全性を満たすなら、Naor^D-then-PS-3 変換で得られた署名方式が、署名サイズは変えずに BUFF 安全性を達成できるこ

とを示した。

2.3 サイドチャネル攻撃に対するプロービング安全性の形式検証

格子暗号では、確率的なパラメータ生成が行われるため、より一層サイドチャネル攻撃に対する安全性の確保が重要である。そのための安全性モデルとしてプロービング安全性が提案されている。一方、形式検証分野では、近年、暗号応用も視野に入れて、確率的分離論理(PSL)の研究が進んでおり、条件付独立性を扱うのに優れたPSLであるLilacが2023年に提案されている。内藏-高島は、文献［4］で、プロービング安全性を示すのに必要なLilacの意味論を展開するとともに、実際の格子署名方式Raccoonに即して、証明規則の拡充を行い安全性の検証を行った。

2.4 離散数理アプローチによる格子暗号・符号暗号の安全性解析

格子暗号では、従来型のSIS・LWE問題困難性に加えて、近年、格子同型問題（LIP: Lattice Isomorphism Problem）に基づく格子暗号構成が注目されている。これまで有限体上の符号から得られるLIPに対してHull攻撃という安全性評価手法が知られていたが、我々(西村-高島-三枝崎)は、そのLIP安全性評価を、有限環上のLCD符号から得られるLIPに対するものに拡張することに成功した。電子情報通信学会英文論文誌に2026年3月に掲載された論文［5］においては、符号・格子・グラフ上の各計算問題間の関係について詳しく調べている。また、最近、文献［6］において、符号暗号安全性を評価する際に重要な平滑化パラメータの評価不等式をグラフ理論的アプローチにより導出することに成功した。

３． 共同研究者

谷　誠一郎（教育学部・数学科・教授）　　三枝崎　剛（基幹理工学部・応用数学科・教授）
内藏　理史（教育学部・数学科・講師）
Ng Iu-Iong（理工総研・研究助手、2025年9月まで）

４． 研究業績

4.1 学術論文

[1] T. Sasaki, K. Takashima, “Regev’s Quantum Factoring Algorithm with Tribonacci Sequence”, submitted, (2026), preliminary Japanese version, “トリボナッチ数列を用いたRegev素因数分解量子アルゴリズム”, was presented at SCIS 2026

[2] K. Tani, S. Tsuchiya, S. Tani and Y. Takeuchi. “Quantum algorithm for unstructured search of ranked targets”, Physica Scripta, 100(7), 075114, (2025),
URL: https://iopscience.iop.org/article/10.1088/1402-4896/ade377/meta

[3] S. Nakano, T. Raku, K. Takashima, “BUFF Security of Naor-Transformed Signatures from ElGamal-Type IBE”, to be submitted, (2026), preliminary Japanese version, “エルガマル型IBEに基づくNaor変換署名のBUFF安全性”, was presented at IEICE ISEC, in March 2026

[4] S. Kura, K. Takashima, “Formal Verification of Probing Security via Conditional Independence”, to appear at CSF 2026, (2026), preliminary Japanese version, “条件付き独立性によるプロービング安全性の形式検証に向けて”, was presented at IEICE ISEC, in July 2025

[5] Y. Nishimura, K. Takashima, T. Miezaki, “On Lattice Isomorphism Problems for Lattices from LCD Codes over Finite Rings”, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 109-A(3), 167-175 (2026), URL: https://www.jstage.jst.go.jp/article/transfun/E109.A/3/E109.A_2025CIP0017/_article/-char/ja

[6] T. Miezaki, Y. Nishimura, K. Takashima, “A New Approach to Code Smoothing Bounds”, submitted, (2026), preliminary Japanese version, “組織的準巡回符号の平滑化限界について”, was presented at SCIS 2026, URL: https://arxiv.org/abs/2603.18077

4.2 総説・著書

以下の CRYPTREC 調査報告書・ガイドラインは、これまで 2018 年度、2022 年度、2024 年度と継続して、最新技術情報を公開してきた。現在、2026 年度版への改訂に向けて準備中である。その準備状況に関しては、2026 年 4 月に CRYPTREC ホームページにて公開された「CRYPTREC 暗号技術検討会 2025 年度 報告書」を参照。

- CRYPTREC 暗号技術調査ワーキンググループ（耐量子計算機暗号）、“CRYPTREC 耐量子計算機暗号の研究動向調査報告書 2024 年度版”、2025 年 3 月、
  URL: https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2024.pdf
- CRYPTREC 暗号技術調査ワーキンググループ（耐量子計算機暗号）、“暗号技術ガイドライン（耐量子計算機暗号）2024 年度版”、2025 年 3 月、
  URL: https://www.cryptrec.go.jp/report/cryptrec-gl-2007-2024.pdf

4.3 招待講演

- 高島克幸、“耐量子計算機暗号”、神奈川県立産業技術総合研究所（KISTEC）講座「量子時代のセキュリティを理解する」、2025 年 9 月

4.4 学会および社会的活動

- 暗号技術評価委員会（CRYPTREC）暗号技術調査 WG(暗号解析評価) 委員
- 電子情報通信学会 ISEC（情報セキュリティ）研究専門委員会 副委員長
- 電子情報通信学会 英文論文誌 暗号と情報セキュリティ特集号 編集委員
- 国際会議 IWSEC 2026 実行委員長
- Japan Journal of Industrial and Applied Mathematics 編集委員
- 日本数学会 MSJ メモアール編集委員会 編集委員

５． 研究活動の課題と展望

2026 年度も引き続き、高機能暗号の安全性評価に数理的アプローチで取り組む。まずは、耐量子計算機暗号と関連する量子アルゴリズムについて、さらに研究を進めることが課題である。また、署名の BUFF 安全性も含む従来よりも広い安全性の枠組みが、近年検討されており、そのような多様な安全性要件の間の関係性を調べることも重要な課題であり、今後も、継続して研究に取り組んでいく。そして、プロービング安全性に限らない暗号の安全性を形式検証するために必要な基礎理論を確立することも今後の課題の一つである。さらに、格子暗号の基礎とされている格子問題は符号問題との関連性が深く、それらの問題の

計算困難性評価を格子暗号・符号暗号の両面から捉えて進めていくことも興味深い課題と考えられる。これらの取り組みを遂行することにより、量子計算機の脅威に耐えうる耐量子暗号基盤構築の促進に寄与していく。