# 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、格子暗号に関連する計算問題の漸近計算量を見積もることで格子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ことから、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、半年間ではあるが、現在投稿中の論文も含めて、以下の研究成果を上げることができた。

### 2.1 格子同型問題の安全性解析

格子ベースの暗号方式はこれからの高機能暗号において重要な役割を果たすが、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。例えば、NIST 耐量子署名コンペティションに追加応募された Hawk 署名は Module LIP と呼ばれる LIP の変種に基づいて構成されている。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。そこでは符号理論・格子理論の知見が活かされた。

### 2.2 構造化された格子に対する格子問題の安全性解析

上記の Module LIP は、「構造化された格子問題(structured lattice problem)」と呼ばれる問題のクラスに属しており、暗号方式の安全性を高めるために、代数的整数論を背景とする格子問題が使われている。Ng の QIP に採録された論文では、構造化格子に対する暗号解析に必要な「イデアル類群計算」と「主イデアル計算」の量子計算量評価を進めて、より精密な

計算量上界の見積もりに成功した。これは、構造化格子に基づく格子暗号の安全性評価において重要な成果である。

2.3 素因数分解・離散対数 量子計算の応用・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。佐々木-高島は、2023 年に発表された Regev、Ragavan-Vaikuntanathan の素因数分解法、Ekera-Gartner の離散対数計算法を Markoff グラフ CGL ハッシュ関数の安全性評価と関連づけて研究を行った。

2.4 巻き戻しを許す量子計算の計算量クラス

ゼロ知識証明や署名の安全性証明において、巻き戻し（rewinding）は重要な技法である。よって、巻き戻しを許す場合の計算量クラスを調べることは、量子暗号にとって興味深い研究テーマである。谷らは、Theory of Computing Systems に発表した論文において、そのような巻き戻しを許す量子計算がいくつかの量子計算量クラスと等価であることに示すのに成功した。これにより、量子暗号の安全性証明を設計する際に重要な指標が得られた。

## 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)
内蔵　理史（教育学部・数学科・講師）　　Ng Iu-Iong（理工総研・研究助手）

## ４． 研究業績

4.1 学術論文

I.-I. Ng, “Upper bounding the quantum space complexity for computing class group and principal ideal problem”, Quantum Information and Computation (QIP), Vol. 24, No. 15&16 (2024) 1313–1324, https://doi.org/10.26421/QIC24.15-16-3

Y. Nishimura, K. Takashima, T. Miezaki, “On Lattice Isomorphism Problems for Lattices from LCD Codes over Finite Rings”, submitted, (2025)

T. Sasaki, K. Takashima, “Improvement of Silverman’s Path-Finding Quantum Algorithm”, submitted, (2025)

R. Hiromasa, A. Mizutani, Y. Takeuchi, S. Tani, “Rewindable Quantum Computation and Its Equivalence to Cloning and Adaptive Postselection”, Theory of Computing Systems 69, 6 (2025) 1-37, https://doi.org/10.1007/s00224-024-10208-5

4.2 総説・著書

相川勇輔、神戸祐太、工藤桃成、高島克幸、安田雅哉、“代数曲線の計算理論と暗号への応用”、日本数学会 数学メモアール 第 10 巻、2024 年 10 月

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、
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、
https://www.cryptrec.go.jp/report/cryptrec-gl-2007-2024.pdf

4.3 招待講演
高島克幸、“耐量子計算機暗号の構成法と安全性評価”、信州大学 数理科学談話会、2024 年 10 月

4.4 学会および社会的活動
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
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
Japan Journal of Industrial and Applied Mathematics 編集委員
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
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

2025 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。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符号理論の知見も活用して進めていくことが今後の展望として考えられる。また、格子問題に対する量子アルゴリズムの必要量子ビット数の評価を更に進めることも課題である。また、従来用いられてきた安全性証明を形式的に検証する際に使われる数理論理学的基盤を明らかにすることにも取り組む予定であり、例えば非干渉性に基づく形式検証に関した研究に取り組んでいきたい。