平成３０年度 共同利用研究報告書

平成 30 年 11 月 26 日

九州大学 マス・フォア・インダストリ研究所長 殿

所属・職名　九州大学マス・フォア・インダストリ研究所・准教授
提案者 氏名　安田雅哉

下記の通り共同研究の報告をいたします.　　記

	※整理番号		20180006	
1.研究計画題目	量子情報社会に向けた数理的アプローチ			
2.種目（○で囲む）	a. プロジェクト研究　b. 若手研究　c. 一般研究			
3.種別（○で囲む）	a. 研究集会Ⅰ　b. 研究集会Ⅱ　c. 短期共同研究　d. 短期研究員			
4.研究代表者	氏 名	高島克幸		
	所 属 部局名	三菱電機　情報技術総合研究所 松井暗号プロジェクト G	職名	主管技師長
	連絡先			
	e-mail		TEL	
5.研究実施期間	平成 30 年 9 月 17 日（月曜日）～平成 30 年 9 月 19 日（水曜日）			
6.キーワード （複数可）	ポスト量子暗号、格子暗号、多変数公開鍵暗号、楕円曲線上の同種写像、 量子符号、代数的組み合わせ			
7.参加者数	47　人　＊1			

＊1　短期研究員は九大の共同研究者も含める.
　　Ⅰ，Ⅱ，短期共同研究は事務局から送った参加者データを元に記入.

8.本研究で得られた成果の概要（**成果報告書を別途要添付**　枚数は次頁参照）

本研究集会では、量子計算機に基づく新しい情報社会の実現に向けて、これまで独立に進展してきたポスト量子暗号や量子符号などの異なる数理的アプローチに関する最新情報を共有すると共に、新しい共同研究の芽や方向性の探索を目的とする。量子計算機による攻撃でも耐性を持つポスト量子暗号の研究開発において、量子アルゴリズムの理論解析しかこれまで行っていなかった。本研究集会では、量子計算機の開発進展とクラウド型量子計算機に関する講演があり、ポスト量子暗号における量子計算機による実機の解析研究の共同研究の方向性が見つかった。また、量子誤り訂正符号の理論が古典の情報理論の証明でも利用できることが分かった。さらに、量子状態の測定で用いられる SIC-POVM の構成は代数的組み合わせ論として非常に難しい数学問題であり、量子情報理論における重要課題であることが分かった。これらのように、量子情報と数学の接点となる問題をいくつか共有でき、異なる分野間での共同研究の芽を見つけることができた。一方、本研究集会では産学官から数学者・暗号研究者・量子計算機開発のエンジニアなど多種多様な方々に参加して頂き、研究以外にも他機関・他分野での研究の進め方・開発規模に関する意見交換ができ、非常に有意義な研究交流ができた。現在、量子計算・量子情報に関する研究は世界中で急速に発展している分野であり、本研究集会を通して継続的かつ積極的な研究交流の必要性を強く感じた。

2018 年 11 月 26 日

成果報告書

【研究背景】

急速に高度化する現代情報社会において、将来の実用化が期待される量子計算機によって利便性の向上が期待される一方、現行社会システムに対する影響も同時に存在する。例えば、現在広く普及している公開鍵暗号として RSA 暗号と楕円曲線暗号があり、それらの安全性は素因数分解問題と楕円曲線離散対数問題の解読計算量困難性に基づいている。しかし、量子計算機によりこれらの数学問題は効率的に解読可能なため、米国立標準技術研究所 NIST により量子計算機による攻撃でも耐性を持つ「ポスト量子暗号」の標準化が近年積極的に進められている。実際 2017 年 11 月末に投稿されたポスト量子暗号の候補方式は格子・符号・多変数多項式・楕円曲線上の同種写像などの暗号数学から構成されている。また一方、量子力学の情報理論への応用である量子符号の研究においても多くの数学理論が利用されている。例えば、量子状態の測定に関連した SIC-POVM や MUB は代数的組み合わせ論の球面デザインと深く関係している。

【本研究集会の目的】

上記の研究背景で述べたように、量子計算に基づく情報社会の実現に向けて、ポスト量子暗号で利用される暗号数学や代数的組み合わせ論に基づく量子符号など多様な数学理論の研究がこれまで独立に進展している。本研究集会では、ポスト量子暗号や量子符号などの量子情報理論で活用されている異なる数理的アプローチに関する専門知識・最新情報を共有すると共に、他分野間の研究アプローチによるシナジーからこれまでの既存研究では得られない新しい研究の芽や方向性の探索を目的とする。

【本研究集会の成果】

本研究集会では、大きく分けて下記 3 つの分野からの講演があった：

A) <u>ポスト量子暗号の構成と安全性解析</u>

NIST のポスト量子暗号の標準化プロジェクトに投稿された公開鍵暗号方式の構成に関する講演が 2 件あった。具体的には、非線形な不定方程式に基づく暗号方式 Giophantus と格子に基づく暗号方式 LOTUS の紹介があった。また、ポスト量子暗号の安全性解析に関して、多変数公開鍵暗号方式 HFERP の数学的解析や共通鍵暗号に対する量子計算攻撃の安全性評価に関する最新の講演があった。さらに、格子暗号の安全性を支える数学問題である最短ベクトル問題の最新の求解法に関するサーベイや高次元格子上のランダムサンプリングによる最先端アルゴリズムの技術解説があった。

B) <u>量子計算機の研究進展状況と情報社会への影響評価</u>

量子計算の歴史から量子計算センターIBM-Q に関する最新情報までの話題と量子誤り訂正能力に関する現状課題に関する講演があった。また、RSA 暗号の安全性を支える素因数分解問題を解くために必要な量子計算資源の見積もりに関する講演があった。

C) <u>量子誤り訂正符号における数学研究</u>

暗号を含む情報理論で不可欠な leftover hash lemma に対して量子誤り訂正理論による新しい証明アプローチの講演があった。また、量子状態の測定に関連した SIC-POVM の一般化とその構成に関する講演や、代数的組み合わせ論からみた SIC-POVM の数学研究とその代数的構成の講演があった。

本研究集会の各講演において異なる分野からの質疑が多くあり非常に活発な議論ができた。例えば、量子計算機の研究進展に関して、ポスト量子暗号の研究者と実際の量子計算機を開発する研究者が持っているイメージの間には大きな隔たりがあることが分かった。また、量子誤り訂正符号の理論が古典の情報理論の証明でも利用できることが分かった。さらには、量子状態の測定で用いられる SIC-POVM の構成は代数的組み合わせ論として非常に難しい数学問題であると共に、量子情報理論における重要な課題であることが分かった。これらのように、量子情報と数学の接点となる問題をいくつか共有でき、今後の異なる分野間での共同研究の芽を見つけることができた。一方、本研究集会では産学官における数学者・暗号を主に含む情報セキュリティ研究者・量子計算機開発のエンジニアなど多種多様な方々に参加して頂き、研究内容以外にも他機関・他分野での研究の進め方・開発規模に関する意見交換ができ、非常に有意義な研究交流ができた。現在、量子計算・量子情報に関する研究は世界中で急速に発展している分野であり、本研究集会を通して継続的かつ積極的な研究交流の必要性を強く感じた。