令和元年度 共同利用研究報告書

令和 元 年 12 月 13 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	20190004		
1.研究計画題目	量子計算, ポスト量子暗号, 量子符号の融合と深化			
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	令和 元 年 11 月 5 日(火 曜日)～令和 元 年 11 月 7 日(木 曜日)			
6.キーワード (複数可)	量子計算, 量子アニーリング, ポスト量子暗号, 量子鍵配送, 量子プロトコル			
7.参加者数	37 人 ＊1			

＊1 短期研究員は九大の共同研究者も含める.
研究集会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)

量子計算機の実現に向けた研究開発が世界中で加速すると共に, 量子計算機による解読に対しても耐性を持つ「ポスト量子暗号」(「耐量子計算機暗号」とも呼ばれる)の研究開発も活発化している. 本研究集会では, 研究開発が急速に加速している量子計算機の現状・進展とポスト量子暗号を含む量子関連の数理暗号・符号などの異なる分野の融合と深化を目的とする. 本研究集会では全 10 件の講演があり, 次の 3 つのテーマに大きく分かれる:

A) 量子計算機の研究開発に関する講演: 超電導回路を利用した量子計算, 量子誤り訂正のためのソフトウェア開発など
B) 量子計算の応用に関する講演:共同学習向け量子デバイスによる分散平均計算, 量子鍵配送の安全性証明, 安全な委任量子計算の公開検証性, 一般確率論における相関の基礎研究と量子情報理論への応用など
C) ポスト量子暗号に対する講演:楕円曲線上の同種写像グラフと種数が高い曲線への一般化, 多変数公開鍵暗号への代数攻撃, デジタルアニーリング計算機を利用した数理暗号解読の報告など

本研究集会の各講演において, 異なる研究分野における研究スタンスや認識の違いに関する議論が活発にできた. 例えば量子計算の応用において, 実際の量子計算機では誤り訂正があるため, 提案通りの暗号プロトコルが実現できない可能性があることや, 量子誤り訂正が必要となる処理が存在するなど, 異なる分野間における議論からこれまで見えなかった研究課題を抽出することができた. さらに, 本研究集会では, 産官学における計算機開発エンジニア・暗号研究者・数学者など多種多様な方々に参加して頂くと共に, 研究内容以外にも他機関・他分野での研究の進め方・研究開発規模などの意見交換ができ, 非常に有意義な研究交流ができた.

成果報告書

【研究背景】 近年，米 Google の研究チームが量子計算機の優位性を示す「量子超越性」の実証実験の成功について報道されるなど，量子計算機の実用化に向けた開発競争が世界中で加速している．一方，RSA 暗号や楕円曲線暗号などの現在普及している暗号技術の（大規模な）量子計算機の解読による危殆化に備え，2016 年から米国標準技術研究所 NIST は量子計算機に耐性のある「ポスト量子暗号」（「耐量子計算機暗号」とも呼ばれる）の標準化計画を進めている．このように，現代の情報社会において，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，暗号を利用した社会システムに対する影響も同時に存在する．

【本研究集会の目的】本研究集会では，研究開発が急速に加速している量子計算機の現状・進展とポスト量子暗号を含む量子関連の数理暗号・符号などの異なる分野の融合と深化を目的とする．具体的には，量子プロトコル・量子鍵配送・量子アニーリングによる暗号解読などの量子計算と数理暗号がより密接に関係する研究分野において，産学官にまたがる数学者・暗号研究者・量子計算機開発エンジニアなど多種多様な研究者間の積極的な交流を図ることを目指す．

【本研究集会の成果】本研究集会では全 10 件の講演があり，次の 3 つのテーマに大きく分かれる：

A) **量子計算機の研究開発に関する講演**：超電導回路を利用した量子計算，量子誤り訂正のためのソフトウェア開発

B) **量子計算の応用に関する講演**：共同学習向け量子デバイスによる分散平均計算，量子鍵配送の安全性証明，安全な委任量子計算の公開検証性，一般確率論における相関と量子情報理論への応用など

C) **ポスト量子暗号に対する講演**：楕円曲線上の同種写像グラフと種数が高い曲線への一般化，多変数公開鍵暗号への代数攻撃，デジタルアニーリング計算機を利用した数理暗号解読の報告など

本研究集会の各講演において，異なる研究分野における研究スタンスや認識の違いに関する議論が活発にできた．例えば量子計算の応用において，実際の量子計算機では誤り訂正があるため，提案通りの暗号プロトコルが実現できない可能性があることや，量子誤り訂正が必要となる処理が存在するなど，異なる分野間における議論からこれまで見えなかった研究課題を抽出することができた．さらに，本研究集会では，産官学における計算機開発エンジニア・暗号研究者・数学者など多種多様な方々に参加して頂くと共に，研究内容以外にも他機関・他分野での研究の進め方・研究開発規模などの意見交換ができ，非常に有意義な研究交流ができた．