共同利用

量子計算、ポスト量子暗号、量子符号の融合と深化

種別	一般研究_研究集会(II)
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
研究代表者	高島克幸 （三菱電機　情報技術総合研究所　松井暗号プロジェクトG・主管技師長）
研究実施期間	令和元年11月5日（火）～ 令和元年11月7日（木）
研究分野のキーワード	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
目的と期待される成果	【研究背景】 高度に進化し続ける現代情報社会において、量子計算機の実現によって利便性の向上が期待できる一方、現行の社会システムに対する影響が同時に存在する。具体的には、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、量子計算機の実現によりこれらの数学問題は効率的に解読可能であることが知られているため、米国立標準技術研究所NISTにより量子計算機による攻撃に耐性を持つ「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月末に投稿された耐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に基づいている。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、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。 【本研究集会の目的と期待する成果】 本研究集会では、近年開発が急速に加速している量子計算機の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指す。より具体的には、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交流を図る。本研究集会を通して、量子計算・数理暗号・量子符号という異なる分野における継続的な協力関係を築くことが強く期待できる。
組織委員(研究集会) 参加者(短期共同利用)	縫田光司 （東京大学大学院　情報理工学系研究科・准教授） 鹿野豊（慶應義塾大学　理工学研究科・特任准教授） 阿部拓郎（九州大学マス・フォア・インダストリ研究所・准教授） 安田雅哉（九州大学マス・フォア・インダストリ研究所・准教授） 池松泰彦（九州大学マス・フォア・インダストリ研究所・助教）
成果報告書	【Web公開】成果報告書_共20190004.pdf