共同利用

量子情報社会に向けた数理的アプローチ

種別	一般研究_研究集会(II)
研究計画題目	量子情報社会に向けた数理的アプローチ
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・主席技師長）
研究実施期間	平成30年9月17日（月）～ 平成30年9月19日（水）
研究分野のキーワード	耐量子暗号、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、
目的と期待される成果	急速に高度化する現代の情報社会において、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、量子計算機の実現によりこれらの数学問題は効率的に解読可能なため、NIST（米国立標準技術研究所）により量子計算機による攻撃に耐性を持つ「耐量子暗号」の標準化が近年積極的に進められている。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。本研究集会では、耐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数理的アプローチに関する専門知識・最新情報を共有し、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が期待できる。
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） 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）
成果報告書	【Web公開】成果報告書_共20180006.pdf