研究課題別　中間評価結果

１．　研究課題名：　量子情報システムアーキテクチャ

２．　総括責任者：　今井　浩　（東京大学　大学院情報理学研究科　教授）

３．　研究概要

本研究は、ERATO　研究を継続・発展させ、理論と実験の双方のアプローチを有機的に結合させることにより、量子情報システムのためのアーキテクチャ創出を目指すものである。本研究では、特に量子計算および量子暗号プロトコル・システムに重点を置いて研究を進めるとともに、これらを支える基礎的テーマとして量子情報理論および量子統計推測について研究を行っている。

量子暗号におけるこれまでの安全性証明は、計算機資源を制約しないことや単一光子を発生する光源を使用すること等、実際の装置に用いた場合には適用出来ない理想的な条件を仮定しているため、実システムにおける鍵暗号の安全性保証が課題となっていた。本研究は、ERATO　研究において発展させた符号化やデコイ法の着想を発展させることで、理想条件が整わない場合でも盗聴者に漏洩する情報量を推定出来る理論を構築し、実証可能なアルゴリズムを確立した。また、これを基にした安全性を保証する鍵蒸留ソフトウェアやデコイ法を実行するハードウェアの開発を行うとともに、20km　の光ファイバー伝送後における漏洩情報量の割合が　2^{-9} 以下と、事実上盗聴が不可能であることが保証された最終鍵を実際に生成した。

本研究では、半導体レーザ等の通常の光通信デバイスを用いた現実の装置・システムにおいて、安全性が定量的に保証された暗号鍵を生成可能であることが実証されたことから、盗聴に対して高度な安全性を有する量子暗号ネットワークシステムの実現に貢献するものと考えられる。また、量子計算に関して群論的構造等を用いる量子アルゴリズムおよび量子分散計算・量子プロトコル等で研究を進展させている。

４．　中間評価結果

４－１．研究の進捗状況と今後の見込み

量子計算と量子暗号の両研究分野において、2 年間に多くの成果を出しているとともに、論文、国際会議等においてレベルの高い内容が発表されている。特に、有限符号長という条件下で量子鍵配送の定量的な安全性の証明や、量子分散アルゴリズムおよび他者間プロトコルの研究において、世界に先駆けて独自の問題設定を行い貴重な成果を上げている。また、ノイズ、盗聴、単一光源の不完全性、データ処理の有限性等の現実的状況を計算に入れ、数十キロの量子通信について安全性を保証した量子暗号システムの構築を世界で初めて成功している。この成果は、

量子暗号システムが現実に稼動し得ることを示した最初の例であり、社会的なインパクトは大きいと考えられる。また、情報理論の側面から量子計算、量子通信の現実性を追求しており、そこで得られたオリジナルな研究成果については他の追随を許していない。本研究の成果は、量子情報理論が単に学術的な体系の範囲で自己完結してしまうものではなく、量子暗号あるいは量子計算における現実の問題の理解とその解決に対して有用なツール足り得ることを示した点で、量子情報理論研究の出口のあり方を示唆している。

4－2. 研究成果の現状と今後の見込み

ERATO の成果に基づいた発展研究という位置づけを踏まえて、本研究では応用技術の方向へと意図的に舵を切っていることが伺える。量子暗号システムに関しては、個々の構成要素についての原理的な理解は既知であったものの、それらを統合したシステムの動作可否について検証が困難であり、その解決が期待されていた。本研究では、理論を構築する際には無視する現実に生じる様々な不都合を計算に入れた上で、全体として動作するシステムを組み上げ、秘密鍵の生成に成功した。また、システムとしての構成の検討やソフトウェアの開発等により、定量的な安全性を理論的に保証した上で、ある程度のレートで動作する量子暗号システムを組み上げたことは、技術的に高く評価出来る。なお、有限長のデータ処理における鍵生成については、各国の研究者の間で 2007 年前半頃から重要性が意識されつつあることも付記する。

ERATO 研究で生まれた量子リーダー選挙プロトコルの実証実験は成功し、この量子リーダー選挙プロトコルの実証実験は、実際に古典的プロトコルの計算限界を破るデモンストレーションとして目的を達成した。量子プロトコルの実質的な優位性を実験的に示した点で高く評価出来る。

また、ハードウェア、ソフトウェアの技術者と理論研究者を実質的に協同させることによって、通常得られないような学際的な成果を多く得ている点は、他の量子情報の研究グループやプロジェクトにない特色を出せたと評価する。基礎から応用開発までの人材を組み合わせることにより個性の強い研究者を動機付けて視野を広げさせ、幅広い成果の創出へとつなげさせる研究代表者の研究者育成手腕およびマネージメント能力は高く評価すべきである。そして、あえて独自の問題設定を行い、安易に国外の先行研究の後追いに走らない研究姿勢も評価出来る。

一方で、量子計算、量子情報の基礎理論に関する研究は、基礎科学への貢献という観点で捉えた場合には、研究分野の本質的難しさもあり、当初計画に対してごく標準的な進捗状況である。また、研究グループ全体としてのアウトプットは比較的多く評価が高いが、特定の研究者・研究テーマに集中しているとともに実用化への明確なブレイクスルーが出ておらず、必ずしも全体が活性化されているわけではないという印象がある。

今後、本研究で開発した暗号システムの安全性を確かめるため、各種盗聴攻撃への耐性を具体的に示すことが必要であろう。主要な研究者のうち 1 名が転出して人材の補充に関する議論も生じたが、基本的には他の主要メンバーによってカバーし得るものである。研究グループ間での問題意識の共有や境界領域での新テーマの立ち上げをこれまで以上に積極的に進め、次世代の量子情報研究の方向性を提示するために成果を取りまとめることが望まれる。

４－３．総合的評価

本研究の成果は、標準以上の質でコンスタントに創出され、その中のいくつかは高い独自性を持ち新しい研究の流れを生み出す可能性を秘めている。特にハードウェアに関しては、現状の実験技術レベルで可能なテーマを設定し、量子情報の理論研究者と技術者が共同でシステム開発を行っている点は高く評価出来る。このような研究を通して、理論研究者の研究への取り組みに幅が増したことは、今後の本研究分野の展開に良い効果をもたらすと期待する。そのためにも、主催する AQIS（Asian conference on Quantum Information Science）の国際会議等を発展させ、本研究が機軸となって国内の情報系の研究者と物理系の研究者の間における交流促進に寄与することを期待したい。

本研究が、ERATO で得られた知的、人的、物的資産を有効に生かして新しい課題に果敢に挑戦し、実用化に向けての重要なステップを 2 年で成し遂げていることは、高く評価すべきと考える。長く蓄積してきた膨大なノウハウや発表まで至らなかった多くの知見が、今後融合されて学術的に集大成するためには、情報理論の観点から量子計算や量子暗号を研究する特徴を活かして研究を推進する努力が不可欠である。そのためには、本研究の特徴である計算機科学・情報科学の個性を引き出し、軸足を実用化に置きつつ本質的な部分へと進むことを視野に入れる必要がある。