研究課題別　事後評価結果

1．研究課題名：量子情報システムアーキテクチャ

2．研 究 総 括：今井　浩　（東京大学　情報理工学系研究科　教授）

3．研究内容および成果：

本研究課題（SORST）の主な目的は、ERATO今井量子計算機構プロジェクト（2000年10月から2005年9月まで）での成果を基盤として、現実の社会にインパクトを与えうる量子情報システムのアーキテクチャを創出することである。そこでは、理論と実験の双方を有機的に結合させるERATOでの研究スタイルを継続させ量子計算及び量子計算プロトコル・システムに重点を置いた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、量子情報理論及び量子統計推測についても研究を行った。

SORSTでは、2つの理論グループと一つの実験グループから構成され、東京オフィス（量子コンピューティング理論グループと量子情報理論グループ）及び筑波分室（量子情報実験グループ：NECグリーンイノベーション研究所内）が設置された。以下、グループごとの研究内容と主立った成果についてまとめる。

（1）量子コンピューティング理論グループ

・ERATOで取り組んだ「リーダ選挙問題」の発展を目指し、量子リーダ選挙を行うアルゴリズムを光量子システムにおいて実現した。また、応用上重要な特殊なトポロジーに対して効率的な量子アルゴリズムを考案した。

・代数的な問題を解く量子アルゴリズムに対しては、群判定問題や群同型問題などを解く効率的な量子アルゴリズムを提案した。

・“量子の計算能力“に関して多証明者量子対話型証明系や量子ネットワークコーディングといった観点から解析を行い、複数の証明者が相関を事前に共有する場合において、量子計算の優位性とその特性を明らかにした。

（2）量子情報理論グループ

・ERATOでの成果である「BB84型秘密鍵配付量子暗号における有限の符号長での安全性証明」について、新しいデコイ状態法の量子鍵配布プロトコルを開発し、量子情報実験グループと協力して実装した。

・BB84型秘密鍵配付量子暗号を超えたより広義の量子セキュリティ理論を追究し、古典理論・量子通信・エンタングルメント操作などが同時に関わる、複雑な種々のプロトコルの統一的理論を構築した。さらに量子エンタングルメントそのものについても理論的研究を進め、束縛エンタングルメント問題とヒルベルト第17問題というある種の数学的な問題との密接な関係があることを明らかにした。

（3）量子情報実験グループ

・量子コンピューティンググループと協力して、2者間の量子リーダ選挙アルゴリズムを実装するための光量子回路の構成法を研究し、システム実証を行った。その結果、不完全な量子システムでも古典的なリーダ選挙アルゴリズムを凌駕することを示した。

・量子情報理論グループとは、量子暗号鍵配付システムの実証実験を協力して行い、定量的な安全性を永久に保証できるシステムを開発した（128bitの暗号文を読み取る際に盗聴できる確率が10^{-33}で、事実上盗聴が不可能であることを示唆する）。

・APD光子検出器の開発においては、超低雑音電荷積分アンプを利用することで、光電子検出効率約90%に向上することに成功し、光子検出効率を80%以上にまで高めることが可能となった。

4．事後評価結果

4－1．外部発表（論文、口頭発表等）、特許、研究を通じての新たな知見の取得等の研究成果の状況

期間中の外部発表、特許等の実績を示す。

発表論文：（邦文）　3件／（英文）　64件

口頭発表：（国内）116件／（国際）　84件　（うち招待講演は、国内26件／国際29件）

特許出願：（国内）　6件／（外国）　1件

まず論文及び口頭発表の観点においては、質及び量ともに適切なものであったと評価できる。国際会議での招待講演も多数であり、国際的にも高いビジビリティを保持したと認められる。ERATO の成果に基づいた発展研究という SORST の位置づけを踏まえて、研究課題の開始当初から応用技術に資する研究に意図的に取り組んだ様子がうかがえる。

その中では、3つのグループが互いに連携し、量子アルゴリズムの実装実験（リーダ選挙問題）や量子暗号鍵配付システムの実装実験で成果を上げ、今後さらなる発展の期待が膨らむものとして捉えることができる。実験グループとしては、国内外の他研究チームと比べ担当する分野は限定的ではあるが、理論グループと協調して重要な成果を上げている点での研究の水準は高いといえる。またSORSTでは、新たな量子理論の構築及び提案を通じたシーズの創出にも努め、他証明版の量子対話型証明系の優位性や束縛エンタングルメント問題などの成果を上げた。これらは当初の研究構想に沿ったものであり、今後の応用に向けた重要な基礎的知見を与える上で高く評価される。中間評価において盗聴攻撃に対する耐性の検討についてコメントされ取り組みを進めたが、技術的困難さがあることは予想された通りで、成果としては未だ無いが今後とも取り組みを進めて貰いたい。

特許出願に関して言えば、量子鍵配送については特許の出願がなされてはいるが、その一方で量子情報の新規アルゴリズムに関しては、それが見受けられない。外部発表とともに特許出願についてもより積極的な対応が望まれる。

４－２．　成果の科学技術への貢献

量子暗号鍵配付システムについては、SORST 開始当初から実用化が期待されていた技術ではあったが、その当時はまだ理論及び原理実証実験の段階にあった。SORST を推進する過程で、実用化を念頭に置いたシステムを実際に作り上げるという重要かつ不可欠なステップを達成しており、そのインパクトは大きいものといえる。既に本研究課題で培われた知見や技術をもとに、2010 年秋の「Tokyo QKD Network」（NICT、NEC、三菱電機、NTT 他が参加）のデモンストレーションにおいて実際のシステムとして用いられ、実用化レベルを印象づけるところまで至っている。

一方、リーダ選挙問題の提案及び原理実証の成果については、量子情報技術の応用を量子鍵配送以外の多者間プロトコルへと拡大したことは、将来の進展に向けた鍵となる成果として注目される。同じく将来への期待という観点では、量子情報実験グループ独自の成果であるアバランシェフォトダイオードを用いた光子検出器の開発も上げておきたい。現在のところ最大で 90%以上の検出効率を上げており、今後多くの波及効果が期待できるものといえる。

４－３．　その他特記事項（受賞等）

上述の、研究成果以外の「成果」としては、まず「国際貢献」を挙げることができる。ERATO 時代から毎年開催してきた EQIS（ERATO conference on Quantum Information Science）を AQIS（Asian Conference on Quantum Information Science）へと発展させて、アジア地域を中心にグローバルなアジアの量子科学技術のフォーラムと交流の場を作り上げた功績は大きい。

その他特記事項として「人材育成」を挙げることができる。参加した多くのグループリーダや研究員が、その後国内外のアカデミックポジションを次々と獲得しており、この分野の次世代のリーダクラスがこの SORST から育っている。グループリーダとして参画していた林正人博士（現在は、東北大学准教授）が、2010 年 IBM 科学賞（コンピューターサイエンス部門）を受賞するなど、対外的にも高く評価されている。