戦略的国際科学技術協力推進事業
日本－仏国　　研究交流
研究課題「量子コンピュータ：理論と実現性」

研究終了報告書

研究交流期間　平成20年2月～平成23年3月

研究代表者：根本　香絵　（印）
（大学共同利用機関法人　情報・システム研究機構　国立情報学研究所　情報学プリンシプル研究系、教授）

１．研究・交流の目的

量子情報処理は革新的な技術発展の可能性からこの 10 年間に膨大な研究努力が払われてきた。その結果現在、量子鍵配送や単一光子源などが研究開発されるようになり、スケーラブルな量子情報処理システムが今後の最も重要かつ緊急な課題として大きな注目を集めている。しかしながら、量子情報処理システム研究では、単一光子源などと異なり複合的な量子操作が本質的で、それだけに困難も大きい。本研究交流は、スケーラブルな量子情報処理の優位性とその実現可能性を日仏共同で探求することを主目的とし、日仏双方からコンピュータサイエンスから物理学まで学際的な研究者が参加することで、その優れた専門性を結集しこの学際的な先進的研究を推し進める。

２．研究・交流の方法

本研究の主目的を実行するための４つの柱として、互いに深く関連を持ちながら、それぞれ特徴をもつサブプロジェクト（SB）に分けることができる。
SB１量子暗号と通信：　量子暗号は安全な通信に欠かせない要素であり、量子計算の登場によって従来の古典的な暗号が破られるといった状況下にあっても、安全性を確保できることが期待されている。量子One-way関数や、ゼロ知識証明などの量子暗号、通信における本質的な要素を取り扱い、また量子力学が可能とする革新的な通信の方法を探究する。
SB2 量子アルゴリズム：　量子アルゴリズムは量子情報処理の優位性の中でも最も注目されているもののひとつであり、オラクルを用いた量子アルゴリズムに焦点をおく。このタイプのアルゴリズムの重要性は、データ検索の有名な量子アルゴリズムであるGroverのアルゴリズムなどからも明らかで、グラフの問題や、量子ウォークなどを重要な課題として取り扱う。
SB3 量子計算と測定：　量子計算の優位性の根源となっている本質的な性質は未解決な部分が多い。そこで量子系に特徴的な測定の働きに着目し、測定ベースの量子計算を中心に、量子情報処理に優位性をもたらす物理的・情報的な本質的性質を解析する。
SB4 量子計算の実現可能性：　この研究交流で取り扱うような量子通信系において、量子的性質がもたらす優位性の安定性を議論する。また、誤り耐性のある量子計算のパフォーマンスについても解析し、量子情報処理の優位性を評価する。
これらの課題は、量子情報処理に絡む様々な分野の知識・スキルを必要とする。量子情報システムの研究には、学際的な研究が本質的であり、これらの分野の融合的な貢献が必須である。本研究課題は、このことも踏まえて、コンピュータ科学と物理学の量子情報分野での融合を研究協力を通して行い、共通の目的をもって研究を行うことで学際的研究を推進する。18 ヶ月ごとのジョイント・ワークショップ、研究訪問・滞在、PhD 学生の交換などを軸に、効果的かつ継続的な研究交流を目指した。PhD 学生の派遣については JST の制度上の制約から思うように行えなかったため、2 年度に参加研究者を若干広げることで十分な交流を図った。

３．研究・交流実施体制

３．１　日本側

氏名	所属	役職	学位	役割
（リーダー） 根本香絵	国立情報学研究所（NII）、情報学プリンシプル研究系	教授	博士	理論・数理物理
（研究者） 村尾美緒	東京大学大学院、理学研究科（NII客員准教授）	准教授	博士	理論物理・量子情報理論

岩間一雄	京都大学大学院、情報学研究科	教授	博士	計算理論
小柴健史	埼玉大学大学院、理工学研究科	准教授	博士	量子暗号
山下茂	立命館大学、情報理工学部情報システム学科	教授	博士	量子情報、計算理論
河内亮周	東京工業大学大学院、情報理工学研究科	助教	博士	量子暗号
田中篤司	首都大学東京、理工学研究科	助教	博士	理論物理、半古典理論
西村治道	大阪府立大学、理学系研究科	講師	博士	量子情報、計算理論
大島利雄	富士通研究所・東京大学　生産技術研究所	研究員	博士	理論物理
Simon Devitt	NII、情報学プリンシプル研究系	研究員	博士	理論物理
唐澤時代	NII、情報学プリンシプル研究系	研究員	博士	量子情報

３．２　相手国側

氏名	所属	役職	学位	役割
(リーダー) Iordanis Kerenidis	LRI,UMR8623	CNRS常勤研究員	PhD	量子情報・暗号
(研究者) Miklos Santha	LRI,UMR8623	CNRS研究ディレクター	PhD	量子情報・アルゴリズム
Sophie Laplante	LRI,UMR8623	教授	PhD	量子情報・計算量理論
Frederic Magniez	LRI,UMR8623	CNRS常勤研究員	PhD	量子情報・アルゴリズム
Elham Kashefi	LIG,UMR5217	CNRS常勤研究員	PhD	量子情報・理論物理
Mehdi Malha	LIG,UMR5217	CNRS常勤研究員	PhD	量子計算
Damian Markham	ENST, TELECOM ParisTech	CNRS常勤研究員	PhD	量子情報

４．研究成果

４．１　研究成果の自己評価

□　計画以上の成果がでた　　■　計画通りの成果がでた

□　計画とは異なるが有益な成果がでた　□　計画ほどの成果はでなかった

□　いずれでもない

４．２　研究成果の自己評価の根拠

量子計算量理論の観点からの量子暗号の研究で，CNRS 側リーダーの Kerenidis との研究交流から、特に量子一方向性関数に基づく紛失通信方式やマルチパーティ計算の可能性について研究のストーリーについて合意を形成することができた．最終年度における Univ.　Paris へ の研究訪問で,その初期段階についての成果を得ることができた。 今後はこれをもとに研究を共同で発展することを予定している。

量子情報処理の新たな可能性の発見としての量子暗号は重要なテーマに取り組み、フランス側の研究者 I. Kerenidis や A. Chailloux との議論を通じて， 量子ハードコア関数等の安全性の証明技法についての広い知見が得られ， 新たな計算量的な量子暗号の設計指針とその安全性証明のための技法を見つけることができた。

量子ネットワーク符号という新分野を開拓し，国内外への分野の拡大を行った． この分野はネットワーク上での多対多量子通信において，ネットワークの中継点での符号化を用いることで通信量を削減するという理論である．この分野に関する研究成果は，ICALP，QIP といった計算機科学および量子情報科学の主要な国際会議において発表されている．当該研究は，主に計算機科学の立場からなされたものであったが，今後は測定ベース量子計算など物理的見地からの展開が期待される．

測定ベース量子計算における グラフ状態の構造的解析に関する研究において、CNRS のフランス 側研究者 （Mehdi Mhalla，Simon Perdrix）との協力によって、入力と出力の量子ビットを 特定しないグラフ状態が量子計算に有効かどうかの判断基準を与えることに成功した。また、この研究は国際会議等で発表されており、論文は準備中である。これまでは、入力都出力の量子ビットを特定しないグラフ状態の量子計算的な性質のほとんどが未知であったが、この研究結果により新しい研究の道が開けた。

全のアンホロノミー(新奇な量子ホロノミー)の研究の進展として、任意の キュービット数での量子回路の例を系統的に構築できるようになった。このことから、理論的な立場からは、断熱量子計算の経路構築の素材としての全のアンホロノミー新しい価値を示した。

光を用いた大規模量子情報処理のモデルを拡張し、トポロジカルな連続量の量子情報処理の方法を検討した。CNRS 研究者 (Damian Markham) らとの共同研究により、連続量を用いた量子情報処理がもつ特殊性を明らかにし、連続量トポロジカル符号化の通信への応用についての可能性を示した。この研究成果の一部は QCMC 等の国際会議で発表済みで、現在成果をまとめて論文として準備中である。

４．３　研究成果の補足

５．交流成果

５．１　交流成果の自己評価

■　計画以上の交流成果がでた　　□　計画通りの交流成果がでた
□　計画ほどの交流が行われなかったが成果はでた

□　計画ほど交流成果がでなかった
□　いずれでもない

５．２　交流成果の自己評価の根拠

研究者派遣では、日本側から、また仏国側から定期的な交流があり、共同研究で成果がすでに出ており、今後も研究計画が検討されている。例えば、量子一方向性関数に基づく紛失通信方式やマルチパーティ計算の可能性の研究、グラフ状態の研究等で、本プロジェクトで立ち上がった長期的な共同研究テーマがあり、今後も持続的発展させる予定で，相互訪問も検討している。今後も若手研究者を中心に日仏相互に研究者を受け入れることで合意している。

共同ワークショップは仏国で一回、日本で一回行ない、メンバーおよび両国の他の研究者との研究交流の増加に大きく寄与した。これとは別に仏国の CNRS 研究者が中心となって開かれた国際会議 PQSM2010 は古典暗号と量子暗号の研究者が一堂に会するという野心的なプログラムで、学際性を本質とする本プロジェクトも多大な支援を行い、会議を成功へ導いたことは、学際的な研究協力の土壌が育っていることを表す例として挙げられる。

ワークショップと併せて講演やセミナーは、新しい研究協力のきっかけとなった例が多い。量子質問計算量や量子ネットワーク符号の成果は，　仏国側からのフィードバックによってよりよい方向に進展したもので、特に量子質問計算量は，仏国側の主要成果である量子ウォークアルゴリズムなど今後の研究交流によって新たな展開を期待できるものもある．

本プロジェクトを通しての若手の研究交流は国際的な人材育成の観点から重要で、量子暗号，量子計算量理論分野の若手で 目覚ましい活躍をしている CNRS 研究者や大学院生との交流は日本の若手研究者に有形無形の利益があったと考える。実際に、若手メンバーや大学院生の染谷氏は CNRS 研究者との交流を通して、研究を大幅に発展させており、国際会議で報告へつなげるなど、目に見える人材育成効果があった。

５．３　交流成果の補足

本プログラムを中心に、直接的また間接的に国際的な研究交流が活発化できた。カナダ国ウォータルー大学のリチャード・クリーブ教授が２０１０年９月から２　０１１年３月までの６ヶ月間京都大学情報学研究科に滞在した．クリーブ教授は 量子質問計算量，量子ゲーム，量子ウォーク等々様々な分野で著明な研究成果 を上げており，今回の訪問中にもこれらの分野での関連研究者との共同研究を 通して本プロジェクトに多くの利益をもたらした．　シンガポールにある仏国 CNRS 研究所との共同研究のきっかけともなった。

６．主な論文発表・特許出願

論文 or 特許	・論文の場合：　著者名、タイトル、掲載誌名、巻、号、ページ、発行年 ・特許の場合：　知的財産権の種類、発明等の名称、出願国、出願日、 出願番号、出願人、発明者等	特記 事項
論文	M. Aulbach, D. Markham, and M. Murao, The maximally entangled symmetric state in terms of the geometric measure, New J. Phys. 12, 073025 (2010)	
論文	Kazuo Iwama (Kyoto U.), Harumichi Nishimura (Osaka Pref. U.), Rudy Raymond (IBM Research – Tokyo), Junichi Teruyama (Kyoto U.), Quantum counterfeit coin problems, Proceedings of 21st International Symposium on Algorithms and Computation (ISAAC2010), Lecture Notes in Computer Science 6506, pp.73–84, 2010	
論文	S.J. Devitt, A.G. Fowler, A.M. Stephens, A.D. Greentree, L.C.L. Hollenberg, W.J. Munro and K. Nemoto Architectural design for a topological cluster state quantum computer.　New J. Phys, 11, 083032 (2009).	