様 式 Ｃ－７－１　　該当する研究種目 … 「特別推進研究(COE)」を除く全ての研究種目

平成　　年度科学研究費補助金実績報告書（研究実績報告書）

1. 機 関 番 号　1 4 6 0 3　　2. 研究機関名　奈良先端科学技術大学院大学

3. 研 究 種 目 名　若手研究（B）　　4. 研究期間　平 成 15 年 度 ～ 平 成 17 年 度

5. 課 題 番 号　1 5 7 0 0 0 1 4

6. 研 究 課 題 名　実現可能性を考慮した量子計算モデルの解析に関する研究

7. 研 究 代 表 者

研 究 者 番 号	研 究 代 表 者 名	所 属 部 局 名	職 名
4 0 3 2 4 9 6 7	ﾌﾘｶﾞﾅ ナカニシ マサキ 中西 正樹	情報科学研究科	助手

8.研究分担者(所属研究機関名については、研究代表者の所属研究機関と異なる場合のみ記入すること。)

研 究 者 番 号	研 究 分 担 者 名	所属研究機関名・部局名	職 名
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		

9. 研究実績の概要(国立情報学研究所でﾃﾞｰﾀﾍﾞｰｽ化するため、600 字～800 字で記入。図､ｸﾞﾗﾌ等は記載しないこと。)

本年度の研究実績としては主に次の３点が挙げられる．１つ目は，量子オートマトンに関する結果であり，量子プッシュダウンオートマトンに関して，対応する古典モデルとの比較を行い，量子モデルの優位性を示した．具体的には，片側誤りの条件の下で，古典スタック付き量子プッシュダウンオートマトンが古典プッシュダウンオートマトンよりも真に能力が高いこと，及び，エラーなし計算の条件の下で，量子プッシュダウンオートマトンで計算可能であるが，古典プッシュダウンオートマトンでは計算不可能な部分関数が存在することを示した．

２つ目は，分散計算において，量子プロトコルが古典プロトコルと比べて通信量を減らすことができることを示した．具体的には，分散計算のためのネットワークにトポロジを取り入れ，リング上のn人でDistinctnessと呼ばれる関数を計算する効率的なプロトコルを提案した．また，そのプロトコルが条件によっては最適であることを示した．

３つ目の結果として，効率的に盗聴者の存在を検出できる量子秘密通信プロトコルを開発した．送信者と受信者の間で，秘密情報および囮情報を複数回やりとりすることにより，安全に量子情報を送信することができる．量子情報を送信できる秘密通信プロトコルの提案は，筆者の知る限り初めてであり，重要な結果であるといえる．

その他にも，エラーを含むオラクルを用いた場合の量子質問量に関する結果として，オラクルがエラーを含む場合でも効率的に問題を解くためのアルゴリズムを提案した．また，量子封印プロトコルについても，成果を挙げている．

これらの結果は，いずれも量子デバイスだけでなく古典デバイスとの協調計算を行ったり，問題設定として現実的な状況を考えており，結果として現実的な状況を考慮した場合に置ける量子計算機の優位性を示している．

※　成果の公表を見合わせる必要がある場合は、その理由及び差し控え期間等を記入した調書(A4 判縦長横書 1 枚)を添付すること。

10. キーワード

(1) 量子計算　(2) 量子オートマトン　(3) 量子分散計算
(4) 量子秘密通信プロトコル　(5) 量子質問量　(6) 量子計算モデル
(7)　(8)

(裏面に続く)

11.研究発表(平成１７年度の研究成果)

〔雑誌論文〕 計（ 8 ）件

著者名	論文標題
M. Nakanishi	Expressive power of quantum pushdown automata with classical stack operations under the perfect-soundness conditions

雑誌名	巻・号	発行年	ページ
IEICE Transactions on Information and Systems	Vol. E89-D, no. 3	2006	1120-1127

著者名	論文標題
Y. Murakami	Quantum versus classical pushdown automata in exact computation

雑誌名	巻・号	発行年	ページ
IPSJ Journal	Vol. 46, no. 10	2005	2471-2480

著者名	論文標題
M. Nakanishi	Automata with quantum and classical resources

雑誌名	巻・号	発行年	ページ
IPSJ Journal	Vol. 46, no. 10	2005	2384-2391

著者名	論文標題
S. Tani	Quantum communication complexity for the distinctness function on a ring

雑誌名	巻・号	発行年	ページ
Proc. of Workshop on Theory of Quantum Computation, Communication, and Cryptography (TQC2006)		2006	10-11

著者名	論文標題
Y. Murakami	No preshared key quantum secret communication protocol

雑誌名	巻・号	発行年	ページ
電子情報通信学会２００６年総合大会講演論文集		2006	DS-1-12

著者名	論文標題
T. Suzuki	Upper bounds for quantum biased oracles with explicit bias rate

雑誌名	巻・号	発行年	ページ
LA Symposium		2006	

〔図 書〕 計（ ）件

著者名	出版社

書名	発行年	総ページ数

12．研究成果による工業所有権の出願・取得状況

計（ 1 ）件

工業所有権の名称	発明者	権利者	工業所有権の種類、番号	出願年月日	取得年月日
特許権	村上ユミコ；中西正樹；山下茂	奈良先端科学技術大学院大学	特願2006-58933	H.18.3.6	

11.研究発表(平成１７年度の研究成果)

〔雑誌論文〕 計（ 8 ）件

著者名	論文標題		
T. Katsumata	Quantum sealing schemes against collective measurement attacks		
雑誌名	巻・号	発行年	ページ
IEICE Technical Report, QIT2005-90		2005	229-232

著者名	論文標題		
Y. Murakami	Cheater identifiable quantum secret sharing schemes		
雑誌名	巻・号	発行年	ページ
IEICE Technical Report, ISEC2005-55		2005	89-92

著者名	論文標題		
雑誌名	巻・号	発行年	ページ

著者名	論文標題		
雑誌名	巻・号	発行年	ページ

著者名	論文標題		
雑誌名	巻・号	発行年	ページ

著者名	論文標題		
雑誌名	巻・号	発行年	ページ

〔図 書〕 計（ ）件

著者名	出版社	
書名	発行年	総ページ数

12. 研究成果による工業所有権の出願・取得状況

計（ ）件

工業所有権の名称	発明者	権利者	工業所有権の種類、番号	出願年月日	取得年月日