様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　１９　日現在

機関番号：　１２３０１
研究種目：　若手研究(B)
研究期間：　2014～2016
課題番号：　２６７３０００３

研究課題名（和文）より実現しやすいクラウド量子計算の研究

研究課題名（英文）More practical cloud quantum computing

研究代表者
森前　智行（Morimae, Tomoyuki）

群馬大学・先端科学研究指導者育成ユニット・助教

研究者番号：５０７０８３０２

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：より実現しやすいクラウド量子計算の実現を目指した。特に、１量子ビットしか測定できない検証者と、任意のユニバーサル量子計算ができる検証者との間で量子ビットをやりとりすることにより、任意の量子計算をサーバー上で行うことができる。計算内容はサーバーには秘密にされ、しかも、サーバが正しい計算をしているのかどうかを検証することができる。具体的には、スタビライザー状態を測定してチェックすることにより、サーバーが正しいグラフ状態を作ったかどうかを確認する。

研究成果の概要（英文）：The purpose of the present project was to realize more practical blind quantum computing. Blind quantum enables a client to delegate her quantum computing to a remote server in without leaking any privacy. The correctness of the quantum computing done by the server can also be verified. For that goal, the graph state that is generated by the server was tested by measuring stabilizer operators. If the test passes, the state is guaranteed to be close to the ideal graph state.

研究分野：　量子計算

キーワード：　量子計算

１．研究開始当初の背景

多くの粒子からなる量子系を制御することにより様々な量子状態を生成する技術は、量子計算機や量子シミレータ、高精度信号検出などの重要な応用につながるものであり、世界中で理論的・実験的研究が活発に行われている。例えば、光、半導体、トラップされたイオン、冷却原子などを用いて多くの実験が行われてきた[Buluta, Science(2009)]。

しかし、制御が正しく行われ、望みの量子状態が正しく生成されたかどうかを検証するにはどうしたらよいのであろうか？現在は、
（１）古典計算機でのシミレーション結果と比較する
（２）何度も測定し、測定結果から量子状態を構築する「量子トモグラフィ」を行う
の二つの方法しかない。しかし、これらを行うためには、粒子数の指数関数でスケールする計算時間、メモリ、測定回数が必要となるため、近い将来、実現不可能になってしまう。そのため、量子クラウドを利用する方法が考えられるが、量子計算機を持たない利用者が遠隔にある量子サーバー上で安全にクラウド量子計算を行う方法が提案されていたが、利用者は多量の量子テクノロジーを必要とするという問題があった。また、実際に量子サーバーが正しい量子計算を行っているかどうかをチェックする必要もあるが、それについても利用者の量子的負担が多少あった。

２．研究の目的

そこで本研究では利用者の負担を減らすことにより、より実現しやすいセキュアクラウド量子計算の実現を目指した。クラウド量子計算とは、利用者が小さな端末から量子クラウドにアクセスして、量子計算をクラウド上で実行するというものである。利用者はクラウドが正しい量子計算をしているか検証できるだろうか？2009 年に、それが可能であることが証明された[Broadbent, et.al. FOCS 2009]。その基本的なアイデアは、利用者が、計算に使うキュービットの中にトラップキュービットをこっそり仕込んでおくというものである。もし、トラップが変えられていなければ計算内容が改ざんされている確率は指数関数的に小さいということが厳密に証明された。彼らの方法を改良しより効率的にトラップを隠す方法を私が 2012 年に提案した[Morimae,arXiv:1208.1495]。この私の手法と Broadbent らの手法は、2013 年にウィーン大学のグループにより、光キュービットを用いた実験で実証された[Barz, et. al. Nature Physics (2013)]。（解説は[Morimae, Nature Physics (2013)]）。
本研究ではとくに、これまでは量子通信や量子ビット生成が必要であったが、それをできるだけ減らすことを目指した。また、ユニバーサル量子計算だけでなく、IQP や DQC1 といったような、ユニバーサルでないにも関わらず古典シミレートが難しいような Quantum supremacy モデルをセキュアかつ検証付きでクラウド上で行うためのプロトコルについても検討する。

３．研究の方法

量子計算量理論において重要な概念である量子対話型証明を利用することにより、利用者の量子的負担を軽減する。また、IQP や DQC1 回路といったような、Quantum supremacy をデモンストレートできるような量子計算をサーバー上でセキュアに行うプロトコルも考案する。測定型量子計算（Measurement-based 量子計算)[Raussendorf and Briegel, Phys. Rev. Lett.(2001)]という
新しい手法を利用する。これは 2001 年にドイツの研究者により提案された新しい量子計算の方法であり、クラスター状態と呼ばれる、エンタングルした特殊な多キュービット状態を用意し、あとはその各キュービットを１キュービット測定するだけで任意の量子計算が実現できる（すなわち任意の量子状態が生成できる）というものである。次頁で詳しく述べるように、この測定型量子計算を利用すれば、制御する粒子数の多項式でスケールする個数のキュービットをそれぞれ１キュービット測定するだけで、量子多体系の制御の検証が実現できる。制御する粒子数の指数関数スケールを扱う必要のある量子トモグラフィや古典シミレーションよりもはるかに効率的である。また、多数のキュービットを一度に測定する必要はなく、１キュービットづつ順番に測定すればよいため、実験的にも容易である。

４．研究成果

DQC1 モデルにおいては、古典シミレート不可能性を示すとともに、ノイズのある場合等にも拡張できた。これらの成果は、PostBQP=PP という関係を使うことにより、DQC1 モデルの出力確率分布が古典計算機で効率的にシミレートできたら多項式階層が崩壊する、というものである。ノイズがある場合には、多項式階層の崩壊ではなく、BQP が多項式階層にはいる、という帰結になる。この帰結は多項式階層の崩壊に比べると弱いが、オラクルセパレーションなどもあり、起こらないだろうと強く信じられている。

また、量子対話型証明についても、検証者の必要な能力を弱めても検証能力が変化しないことが証明できた。例えば、クリフォード量子回路のみからなる検証者を考えても、それが実現できる。証明者は通常の Witness に加えて、Magic state を送ればよい。実際に正しい Magic state を送ってきているかどうかの検証は、検証者がクリフォードゲートのみでできることを示した。さらに、測定型量子計算の手法を応用することにより、検証者は1量子ビットの測定のみでも QMA を解けることが示された。この方法は、ハミルトニアンの基底エネルギーを求める問題が QMA 完全であることをつかっても証明できる。これはさらに QMA だけでなく、QAM などの、他の量子対話型証明系のクラスにも拡張された。

また、AWPP の量子的解釈を与えた。AWPP は BQP のベストな上界として知られているが、定義は複雑かつ人工的であり、あまり使い勝手が良くなかった。しかし、ポストセレクション確率が FP 関数であるような PostBQP のクラスとして解釈できることをはじめて示した。この、その応用として、group nonmembership 問題という、QMA にはいる有名な問題を修正したものは AWPP にはいることを証明できた。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　１０　件）全て査読有り

(1) T. Morimae, K. Fujii, and H. Nishimura, Power of one non-clean qubit, Phys. Rev. A 95, 042336 (2017).
(2) T. Morimae, Measurement-only verifiable blind quantum computing with quantum input verification, Phys. Rev. A 94, 042301 (2016).
(3) T. Morimae, Quantum Merlin-Arthur with single-qubit measurements, Phys. Rev. A 93, 062333 (2016)
(4) T. Morimae, H. Nishimura, and F. LeGall, Modified group non-membership is in AWPP, Quant. Inf. Comput. 17, 0242 (2017)
(5) C. Greganti, M. Roehsner, S. Barz, T. Morimae, and P. Walther, Demonstration of measurement-only blind quantum computing, New J. Phys. 18, 013020 (2016)
(6) T. Morimae, D. Nagaj, and N. Schuch, Quantum proofs can be verified using only single qubit measurements. Phys. Rev. A 93, 022326 (2016)
(7) T. Morimae, M. Hayashi, H. Nishimura, and K. Fujii, Quantum Merlin-Arthur with Clifford Arthur, Quant. Inf. Comput. 15, 1420 (2015)
(8) M. Hayashi and T. Morimae, Verifiable measurement-only blind quantum computing with stabilizer testing, Phys. Rev. Lett. 115, 220502 (2015)
(9) T. Morimae and H. Nishimura, Quantum interpretations of AWPP and APP, Quant. Inf. Comput. 16, 0498 (2016)
(10) T. Morimae, Acousal measurement-based quantum computing, Phys. Rev. A 90, 010101® (2014)

〔学会発表〕（計　０　件）

〔図書〕（計　１　件）

小柴健史、藤井啓佑、森前智行、観測に基づく量子計算、コロナ社、2016 年 2 月、196 ページ

〔産業財産権〕

○出願状況（計　０　件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　　件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
森前　智行（Morimae,Tomoyuki）
群馬大学・大学院理工学府・准教授
研究者番号：50708302

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：

(4)研究協力者

（　　）