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

令和　３ 年　 ６ 月 ２４ 日現在

機関番号：１４３０１
研究種目：若手研究(B)
研究期間：2017～2020
課題番号：１７Ｋ１２６３７

研究課題名（和文）量子対話型証明とハミルトニアンに基づく検証つきセキュアクラウド量子計算

研究課題名（英文）secure cloud quantum computing based on local Hamiltonian

研究代表者
森前　智行（Tomoyuki, Morimae）

京都大学・基礎物理学研究所・准教授

研究者番号：５０７０８３０２

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：量子計算が正しく動作しているかを確認するための暗号プロトコルを構築した。検証者は量子計算を持つ必要はなく、完全に古典の能力のみで可能である。また、悪意のある検証者に対してサーバー側の秘密がもれないような安全性、ゼロ知識証明、についても構築した。局所ハミルトニアンの方法と、最近提案されたBroadbent-Griloによるゼロ知識証明のアイデアをベースとしている。

研究成果の学術的意義や社会的意義
量子計算が将来普及した際に、クラウド量子計算が正しい計算を行っているかどうかを簡単に確認することができる。また、悪意のある利用者がクラウドの秘密を盗み見ようとする場合でも、それを防ぐような暗号プロトコルが実現できる。これらの安全性は量子の性質を使うことにより、情報理論的安全なものになっており、非常に強力な安全性が達成されている。

研究成果の概要（英文）：We constructed non-interactive proof for QMA and non-interactive zero-knowledge proof (with information theoretical zero-knolwdge) based on the local Hamiltonian technique and the recent construction of zero-knolwedge for QMA by Broadbent and Grilo.

研究分野：量子計算

キーワード：量子暗号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

量子計算の実験的研究はかなり進んでおり、小規模のものなら実験室で普通に実現されている。しかし大きなサイズの量子計算機を作成し維持するには高い技術や費用がかかるため、一家に一台というのはまだだいぶ先のことで、当面は、現在のスパコンのように「クラウド」的に運用されるだろうと考えられる。つまり、利用者は自宅の端末から量子サーバーにアクセスし、量子サーバー上で量子計算を実行するのである。量子計算の場合にセキュアクラウド計算が可能かどうか、というのは長い間の未解決問題であったが、2009 年に可能であることが理論的に証明された[Broadbent et al. FOCS 2009]。面白いことに、古典暗号のこれまでの結果を単純に量子に応用した、というものではなく、量子ビットの状態を破壊することなく情報を読み出すことができないという、本質的に量子的な性質を使った新しい証明に基づいている。そのため、この量子クラウドのプロトコルは盗聴者の計算能力に仮定を設けない安全性（情報理論的安全性）が達成できている。

２．研究の目的

このように利用者は、セキュアにクラウド量子計算を行うことができ、かつ計算の正しさも検証できるのである。しかし、最後に残された不満な点がある。それは、利用者は何らかの量子的な技術を必要とする点である。最初に提案されたプロトコルでは、利用者は量子ビットを生成して、サーバーに送らなければならない。また、改良されたプロトコルでは、サーバーから送られた量子ビットを測定しなければならない。量子ビットの生成や測定は、現在の技術ではそれほど難しいものではなく、デバイスも普通に市販されている。しかしながら、より「ユーザーフレンドリー」なセキュアクラウド量子計算を目指すには、これらの要請を取り除きたい。本研究においては、この障害を取り除き、完全に古典の利用者（つまりラップトップ PC とインターネットアクセスのみを持つ利用者）でも実行できるセキュアクラウド量子計算プロトコルの構築を目指す。

３．研究の方法

量子計算の各ステップごとに得られる状態を全て同じ重みで重ね合わせた状態は、ファインマン状態(history state)と呼ばれ、量子計算の情報を完全にエンコードしているため、それを測定すれば、量子計算の結果がわかるだけでなく、各ステップで正しい量子計算を行っているかどうかのチェックができる。（これは、チューリングマシンの各ステップの状態が SAT にエンコードされるという有名な事実の量子版である。）面白いことに、そのファインマン状態は、実際の物理系のハミルトニアンの最小エネルギー状態になっていることが最近判明した[Cubitt and Montanaro, SIAM J. Comput. 2013]。(物理系のエネルギーはハミルトニアンと呼ばれるエルミート演算子で記述される。固有値がエネルギーに対応し、固有ベクトルはそのエネルギーの量子状態に対応する。）したがって、サーバーはハミルトニアンを用意し、最小エネルギー状態まで冷やすことにより状態を準備する。(実際は十分低温でもよいことが我々により証明されている[Fujii and TM, Phys. Rev. A Rapid Comm. 2012])。利用者は、測定方法を暗号化して指示することにより、完全に古典の利用者が古典通信のみでサーバに任意の量子計算をさせることが可能となる。　サーバが正しい計算を行っているのかどうかの確認が最も難しいところであるが、ここで、計算機科学における対話型証明系のアイデアを利用する。対話型証明系というのは、前頁でも述べたように、計算能力の劣った「検証者」が、計算能力に制限のない「証明者」と対話することにより、その計算の正しさを確かめる方法であり、例えば、数個のランダムなサンプルをチェックするだけで、正しさが検証できることが知られている(確率的検査可能証明(PCP))。「量子版の PCP」も最近研究されてきており、それらの手法を使うことにより、セキュアクラウド量子計算の検証を実現する。例えば、[Hayashi and TM, Phys. Rev. Lett. 2015]においては、スタビライザーの手法を使うことにより、証明者が正しい状態を作っているかどうかをチェックしている。スタビライザーというのは交換するエルミート演算子のいくつかの組であり、量子状態をその同時固有ベクトルとして一意に指定することができる。スタビライザーの同時固有状態として指定された状態は、ある測定パターンに対し、常に固定した値を確率１で返すため、スタビライザーを測定することにより、正しい状態ができているのかどうかのチェックができる。そこで、検証者は、上記のプロトコルにおいて、実際の計算のための測定の指示の中に、スタビライザーの測定もランダムにこっそり混ぜる。証明者は、計算を行っているのかスタビライザーのチェックを行っているのか区別できないため、もし、指示された通りに測定を行わないと、スタビライザーの測定結果につじつまが合わなくなるため、悪意のある行動を検証者に検出されてしまう。

４．研究成果

量子計算が正しく動作しているかを確認するための暗号プロトコルを構築した。まずは局所ハミルトニアンの方法により、検証するプロトコルを構築した。これは計算をエンコードしたヒストリー状態を証明者が検証者に送るというものであり、これにより検証者はＢＱＰ問題の解を検証できる。局所ハミルトニアン問題はQMA完全であるが、ＢＱＰの場合はトリビアルなＷｉｔｎｅｓｓで実現できるため、ヒストリー状態の生成は多項式時間で可能である。さらに、ＢＱＰはＣｏｍｐｌｅｍｅｎｔについて閉じているため、最終結果をフリップするような量子回路を考えれば、ＹＥＳ，ＮＯの両方のインスタンスについて検証をすることが可能である。ハミルトニアンのエネルギーはパウリの測定で測定できるため、検証者はランダムにえらんだいくつかの量子ビットに対し、パウリ測定を行うだけで検証が可能である。

さらにこの方法を拡張し、検証者は量子計算を持つ必要はなく、完全に古典の能力のみで可能である。また、悪意のある検証者に対してサーバー側の秘密がもれないような安全性、ゼロ知識証明、についても構築した。局所ハミルトニアンの方法と、最近提案されたBroadbent-Grilo によるゼロ知識証明のアイデアをベースとしている。具体的には、Trusted center がランダムBB84状態を証明者に送り、その古典的記述を検証者に送る。証明者はその状態と量子証明を量子テレポーテーションすることにより、その結果の古典情報を検証者に送る。

また、量子状態の検証プロトコルを構築した。とくに、グラフ状態やハイパーグラフ状態といったような測定型量子計算のユニバーサルリソースであるような状態が正しく作られているかを検証するプロトコルを考えた。それらの状態はスタビライザー状態、あるいは拡張スタビライザー状態になっているため、スタビライザーをランダムに選びその同時固有状態になっているかを検証することによりチェックできる。グラフ状態の場合はスタビライザーはパウリ演算子であるので、分解して１量子ビットごとに測定できるが、ハイパーグラフ状態の場合、一般にはＣＺなども含むため、それをパウリ演算子に分解し、Ａｄａｐｔｉｖｅに測定を変えることにより検証できることを示した。さらに、従来のＤｅＦｉｎｅｔｔｉの方法よりもより効率的なＳｅｒｆｌｉｎｇの方法を使うことにより、サンプル数に対しより効率的な検証方法を提案した。このように状態を検証する方法の場合、情報理論的健全性がＳｉｎｇｌｅ－ｒｏｕｎｄで成り立ち、しかも検証者は１量子ビットをそれぞれ測定するだけでよいとうメリットを持つ。

この成果により、量子計算が将来普及した際に、クラウド量子計算が正しい計算を行っているかどうかを簡単に確認することができる。また、悪意のある利用者がクラウドの秘密を盗み見ようとする場合でも、それを防ぐような暗号プロトコルが実現できる。これらの安全性は量子の性質を使うことにより、情報理論的安全なものになっており、非常に強力な安全性が達成されている。

５．主な発表論文等

〔雑誌論文〕　計8件（うち査読付論文　8件／うち国際共著　0件／うちオープンアクセス　4件）

１．著者名 Tomoyuki Morimae,Yuki Takeuchi, Masahito Hayashi	４．巻 96
２．論文標題 Verification of hypergraph states	５．発行年 2017年
３．雑誌名 PHYSICAL REVIEW A	６．最初と最後の頁 62321
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 YukiTakeuchi, Tomoyuki Morimae, Masahito Hayashi	４．巻 9
２．論文標題 Quantum computational universality of hypergraph states with Pauli-X and Z basis measurements	５．発行年 2019年
３．雑誌名 Sci. Rep.	６．最初と最後の頁 13585
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Tomoyuki Morimae, Yuki Takeuchi, Harumichi Nishimura	４．巻 2
２．論文標題 Merlin-Arthur with efficient quantum Merlin and quantum supremacy for the second level of the Fourier hierarchy	５．発行年 2018年
３．雑誌名 Quantum	６．最初と最後の頁 106
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Tomoyuki Morimae, Tamaki Suguru	４．巻 4
２．論文標題 Additive-error fine-grained quantum supremacy	５．発行年 2020年
３．雑誌名 Quantum	６．最初と最後の頁 329
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Tomoyuki Morimae	4．巻 96
2．論文標題 Hardness of classically sampling the one-clean-qubit model with constant total variation distance error	5．発行年 2017年
3．雑誌名 Phys. Rev. A	6．最初と最後の頁 40302
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 J. F. Fitzsimons, M. Hadjusek, Tomoyuki Morimae	4．巻 120
2．論文標題 Post hoc Verification of Quantum Computation	5．発行年 2018年
3．雑誌名 Phys. Rev. Lett.	6．最初と最後の頁 40501
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Keisuke Fujii, Hirotada Kobayashi,Tomoyuki Morimae,Harumichi Nishimura,Shuhei Tamate,Seiichiro Tani	4．巻 120
2．論文標題 Impossibility of Classically Simulating One-Clean-Qubit Model with Multiplicative Error	5．発行年 2018年
3．雑誌名 Phys. Rev. Lett.	6．最初と最後の頁 200502
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Yuki Takeuchi, Tomoyuki Morimae	4．巻 8
2．論文標題 Verification of Many-Qubit States	5．発行年 2018年
3．雑誌名 Phys. Rev. X	6．最初と最後の頁 21060
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計0件

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関