科学技術振興機構（ＪＳＴ）
京　　都　　大　　学

量子計算の正しさを事後チェックする方法の提案
～安心安全な量子インターネットの実現に向けて～

ポイント

- 量子コンピューターはノイズに弱いため、量子計算結果の正しさを効率的にチェックする方法が必要不可欠である。
- 量子計算の正しさを計算終了後に事後チェックできる効率的な方法を世界で初めて開発した。
- 遠隔にある量子クラウドの計算の正しさもチェックできるため、今後、安心安全な量子インターネットを実現するうえで基盤となる技術である。

ＪＳＴ 戦略的創造研究推進事業において、京都大学 基礎物理学研究所の森前 智行　講師らは、量子計算の結果の正しさを効率的に事後チェックできる方法を開発しました。

コンピューターの計算結果の正しさのチェックは、我々が普段使っているコンピューターにおいても内部で自動的に行われている、必要不可欠なプロセスです。量子コンピューターの場合、ノイズに弱いという弱点があるため、計算の正しさのチェックはいっそう重要となりますが、これまで提案されていた方法では、計算本体と計算チェックのプロセスが分離不可能な形になっていたため、計算時間が増大してしまうという問題がありました。

今回、森前　講師らは、量子計算の計算本体と計算の正しさのチェックを分離して、チェックを事後に行える効率的な方法を新たに提案しました。量子コンピューターは近い将来、現在の通常のコンピューターではシミュレートできないようなサイズの領域に達するだろうと予想されていますが、そのような場合でも、本研究で得られた新しい方法を適用することにより、通常のコンピューターでも効率的なチェックが可能となると期待されます。また、さらなる将来、クラウドでの量子計算サービスがより一般化していくと、セキュリティーの観点からも、クラウドの量子計算の正しさを利用者が簡単にチェックできるスキームが必要となってきます。この成果は、そのような未来において、安心安全な量子インターネット[注1)]を実現する上で重要な基盤技術となるものです。

本研究は、National University of Singapore および Singapore University of Technology and Design の Joseph Fitzsimons 博士、Michal Hajdusek 博士と共同で行いました。

本研究成果は、２０１８年１月２２日（米国東部時間）に米国科学誌「Ｐｈｙｓｉｃａｌ Ｒｅｖｉｅｗ　Ｌｅｔｔｅｒｓ」のオンライン版で公開されました。

本成果は、以下の事業・研究領域・研究課題によって得られました。
戦略的創造研究推進事業（ＡＣＴ－Ｉ）
研 究 領 域：「情報と未来」※
（研究総括：後藤 真孝　産業技術総合研究所 情報技術研究部門　首席研究員）
研究課題名：古典検証者によるセキュアクラウド量子コンピューティング（課題番号：JPMJPR16UP）
研　究　者：森前 智行（京都大学 基礎物理学研究所　講師）
研 究 期 間：平成２８年１０月～平成３０年３月
※文部科学省の人工知能／ビッグデータ／ＩｏＴ／サイバーセキュリティ統合プロジェクト（ＡＩＰプロジェクト）の一環として運営

＜研究の背景と経緯＞

原子や光などのミクロな世界は量子力学という物理理論に従っています。量子力学の性質を制御することにより、これまでのコンピューターではできないような超高速な計算を実現する未来のコンピューターが量子コンピューターであり、現在、世界中の大学や企業等で多くの理論的、実験的研究が活発に行われています。

一方、量子コンピューターには、外場等のノイズに非常に弱いという弱点があります。そのため、量子コンピューターで実行した計算の正しさをチェックする必要があります。計算結果の正しさのチェックは、量子コンピューターに限らず、我々が現在使っているコンピューターの内部でも自動的に行われている重要なプロセスです。ノイズに弱い量子コンピューターの場合は、計算結果の正しさのチェックがより重要なものであり、また通常のコンピューターでもチェックできることが望まれます。

しかし、これまで提案されていた方法では、計算本体と計算チェックのプロセスが分離不可能な形で組み合わさっているため、常に同時に実行されます。量子コンピューターの信頼度はそれぞれで異なるにも関わらず、従来の手法では、信頼度の高い量子コンピューターに対しても低い量子コンピューターに対しても、全く一様に同じチェックをすることになり、非効率でした。

＜研究の内容＞

本研究では、世界で初めて、量子計算本体と計算チェックのプロセスを分離できる理論プロトコルを提案しました。これにより、量子コンピューターの信頼度の高さに応じて量子計算の正しさを事後チェックすることが可能となります。

利用者が量子コンピューターを信頼している場合は、不要な計算チェックプロセスを行わず、量子計算本体のみを実行すれば結果が得られるため、非常に効率的です。

一方、量子コンピューターの信頼性が低い場合は、利用者は量子計算の結果を受け取った後に、計算の正しさの証明を量子コンピューターに要求することで、当該計算結果が正しいものであるという証明がエンコードされた量子ビット[注2)]を受け取ることができます。

このエンコードされた量子ビットは、量子計算の各時間ステップの状態を量子的に重ね合わせたような状態になっており、クラウドが各ステップできちんと正しい量子計算を行っていることを示すものとなります。今回提案する理論プロトコルでは、利用者は送られてきた各量子ビットを測定用のデバイスを通して測定し、その測定結果を通常のコンピューターで処理します。測定結果がある条件を満たしている場合、非常に高い確率で、当該計算結果は正しいものであることが理論的に保証されることを示しました（間違う確率は指数関数的に小さいものとなります）。

また、提案手法では量子コンピューターからは量子ビットが１つずつ順に送られるため、利用者はその量子ビットを１つずつ順番に測定していけばよいので、測定用デバイスに量子メモリー[注3)]を必要としないという大きなメリットもあります。

＜今後の展開＞

現在、数十量子ビットの量子コンピューターは既に実験室で実現されており、近い将来、現在の通常のコンピューターではシミュレートできないようなサイズの領域（量子スプレマシー）に達するだろうと予想されています。そのような場合には、もはや通常のコンピューターによるシミュレーションで量子計算の動作チェックをすることは不可能と言われていました。

本研究で得られた新しい方法を使うことにより、通常のコンピューターでも効率的なチェックが可能となると期待され、本成果は今後の量子コンピューターの発展において非常に重要な基盤的技術となると考えられます。

また、量子コンピューターは高価で大規模なシステムであるため、当初はクラウド的に運用されるだろうと考えられています。つまり、利用者は自宅の端末から、センターに設置された量子コンピューターにアクセスして、量子計算を実行するという形式で利用されることが予想されます。実際に、ＩＢＭが量子計算をクラウド上で実行できるサービスをすでに開始しており[1]、現在すでに世界中で大学や企業の研究者が利用しています。

将来、クラウド量子計算がさらに一般に普及して、誰でも日常的に利用するようになってくると、量子計算結果の不安定性の観点からだけではなく、セキュリティーの観点からも、クラウドの量子計算の信頼性を利用者が簡単にチェックできるスキームが必要となってきます。なぜなら、例えば将来、量子コンピューターの利用者に意図的に間違った結果を送るような悪意のあるクラウドも現れてくるかもしれないからです。

将来一般的となるであろうクラウド量子計算においても、今回提案した事後チェック方法は有効です。図に示すように、利用者はクラウド上で量子計算本体を実行し、結果を受け取った後、利用者は計算の正しさの証明をクラウド量子コンピューターに要求することで、計算結果の正しさの証明がエンコードされた量子ビットを受け取ることができるので、自分のコンピューターで確認することができます。

利用者がクラウドを信頼している場合は、利用者はクラウド量子計算結果をそのまま受け入れ、完了とすることができます。しかし、疑わしい場合は、事後に（たとえ数週間後であったとしても）、利用者はクラウド量子コンピューターに証明を要求し、計算結果の正しさを事後チェックすることができます。このように利用者にとって、クラウド量子計算の正しさのチェックが非常に効率的かつ簡単に行えることが期待できます。

さらに将来的には量子コンピューターを量子ネットワークでつないだ量子インターネットの実現が世界規模で目指されていますが、この量子ネットワークにおいても、利用者のセキュリティーの確保は重要です。本研究成果は、そのような量子インターネットを安心安全に誰でも利用できるような社会をつくるうえで、セキュリティーの基盤となる技術です。

＜参考図＞

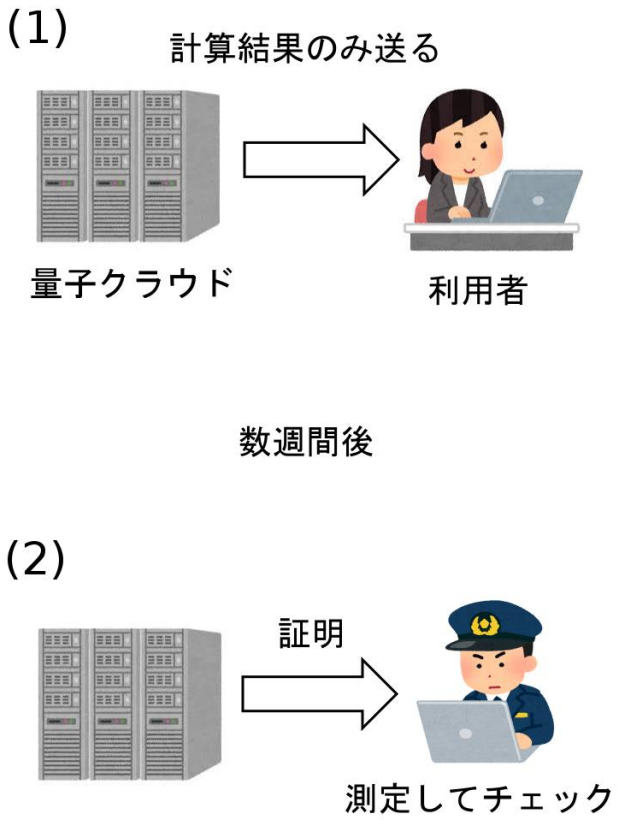

図　今回提案された量子計算結果チェック方法の概要

（１）利用者はクラウド上で量子計算を行い、結果を得る。

（２）計算結果が疑わしい場合は、利用者が証明を要求する。
クラウドからは量子結果の正しさの証明がエンコードされた量子ビットが送られてくるので、利用者はその量子ビットをもとに自身の通常のコンピューターで正しさのチェックができる。

＜用語解説＞

注１）量子インターネット

量子コンピューターが量子ネットワークにつながってできた大規模なシステムのこと。

注２）量子ビット

通常の計算機では０と１の値（ビット）を使って計算を行うが、量子コンピューターでは０と１の量子的重ね合わせというものも実現できる。このような量子的重ね合わせもできるビットのことを量子ビットと呼ぶ。

注３）量子メモリー

量子的なデータを蓄えておくためのメモリー。大きな量子データを長時間保持できるような量子メモリーの実現は非常に難しいため、量子メモリーを使わないような方法のほうが望ましいとされている。

＜論文情報＞

タイトル：“Post hoc verification of quantum computation”
著者名　：Joseph F. Fitzsimons, Michal Hajdusek, and Tomoyuki Morimae
掲載誌　：Physical Review Letters
ｄｏｉ　：10.1103/PhysRevLett.120.040501

＜出典＞

［１］ https://www.research.ibm.com/ibm-q/