量子計算のポストホック検証とは

平成 30 年 2 月 28 日

ここでは、[Fitzsimons, Hajdusek, and Morimae, Phys. Rev. Lett. 120, 040501 (2018)] で最近提案された、「量子計算のポストホック検証」という新しい量子暗号プロトコルについて解説します。

昔々あるところにアリスがいました。アリスはある難しい問題を量子計算で解きたいのですが、残念ながら量子計算機を持っていません。そこで、アリスは○△社のクラウド量子計算サービスを利用することにしました。

アリスは電話で○△社に、解きたい問題の内容を伝えました。すると、○△社は自社の量子計算機を走らせて瞬時に問題を解き、アリスに答えを教えてくれました。アリスは量子ビットコインで料金 10 万円を○△社に支払うと、どうもありがとう、といって電話を切りました。

ところが、数か月後、アリスは○△社についての悪い噂を耳にしました。彼女はもはや○△社を信用できなくなりました。数か月前に電話で教えてくれた量子計算の結果も実は嘘かもしれない、と疑い始めるようになってしまいました。そこで、アリスは安心するために、○△社にもう一度電話をかけて、数か月前の量子計算の結果が正しいものであることを証明するように要求しました。アリスは、数か月前の量子計算の結果が正しいものであるか確認できるでしょうか？

一方で、○△社としても、実はその悪い噂は根も葉も無いものであり、困っていたところでした。○△社としても是非、アリスに、数か月前の結果の正しさを証明したいところです。しかし、ある問題があります。アリスが実は悪人だったらどうしましょう？○△社が数か月前に行った量子計算は本当に正しいものなのに、アリスが、意図的に「それは間違っていた！」と騒ぎ立てて、以前支払った料金を返却しろとごねてくるかもしれません。○△社は中立的な第三者に、数か月前の量子計算の結果の正しさを証明できるでしょうか？

ポストホック検証プロトコルを使えばそれらが可能になります。プロトコルは次のような流れです。

1. ○△社はある量子状態を作ってアリスに送る。

2. アリスは、○△社から届いた量子状態を測定し、その測定結果を入力としてある (古典）アルゴリズムを走らせる。

3. アルゴリズムが「受理」を出力したら、数か月前の量子計算の結果はほぼ確率 1 で正しい。

(注 : ステップ 1 におけるある量子状態というのは、あるハミルトニアンの基底状態であり、量子計算機を使えば多項式時間で生成できるものです。ステップ 2 におけるアルゴリズムは古典計算機で多項式時間で実行できるものです。これらの詳細については論文を参照してください。また、ステップ 3 における、ほぼ確率 1、というのは、指数関数的に 1 に近づくという意味です。)

このように、ポストホック検証プロトコルを使えば、アリスは、数か月前の結果が正しいものであることが確認できます。また、このプロトコルにおいてアリスを中立な第三者に変えれば、○△社は、中立な第三者も納得させることができます。