量子スプレマシー

量子計算の検証、fine-graind量子スプレマシー

森前智行
(京都大学基礎物理学研究所)

量子計算機は古典計算機より速い？

計算量理論の「標準的な」意味ではまだ証明されていない

→しかも証明するのは恐ろしく難しいだろうと思われている

理由：

BQP≠BPP

P≠PSPACE
（未解決の大問題）

注：簡単、省メモリ、という単語は誇張しすぎ。正確には「多項式時間」、「多項式メモリ」

そうはいっても、皆量子計算は速いと信じている。。。

理由：現在のベスト古典アルゴリズムより速い例がある。

素因数分解、量子多体系のシミレーション、等

→しかし、将来古典の高速アルゴリズムが見つかるかもしれない！

例：recommendation system

18歳の学部生が卒研（？）で古典高速アルゴリズムを見つけてしまう [Tang, STOC2019]

古典のベストは将来アップデートされる恐れがある

量子スプレマシーの目的

BQP≠BPPを示すのは恐ろしく難しい。

「条件付き」証明ならできるかも。

つまり、

〇〇と仮定したら、量子計算機は古典計算機より高速

というものを証明しよう！

〇〇は量子と関係なく、しかも皆信じているものでないといけない。例：P≠NP

多項式階層が第二レベルで崩壊しないと仮定したら、

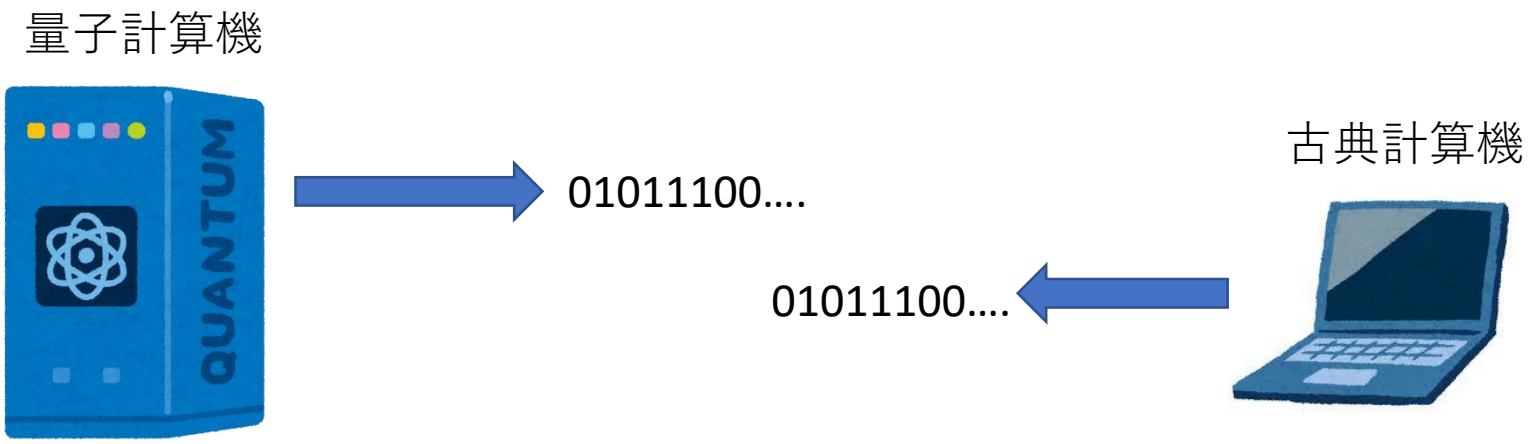
量子計算機は古典計算機より高速

多項式階層が第二レベルで崩壊しない：P≠NPのようなもの　（注：超大雑把）

サンプリング問題

量子計算機がある確率分布でランダムなビット列を吐き出す

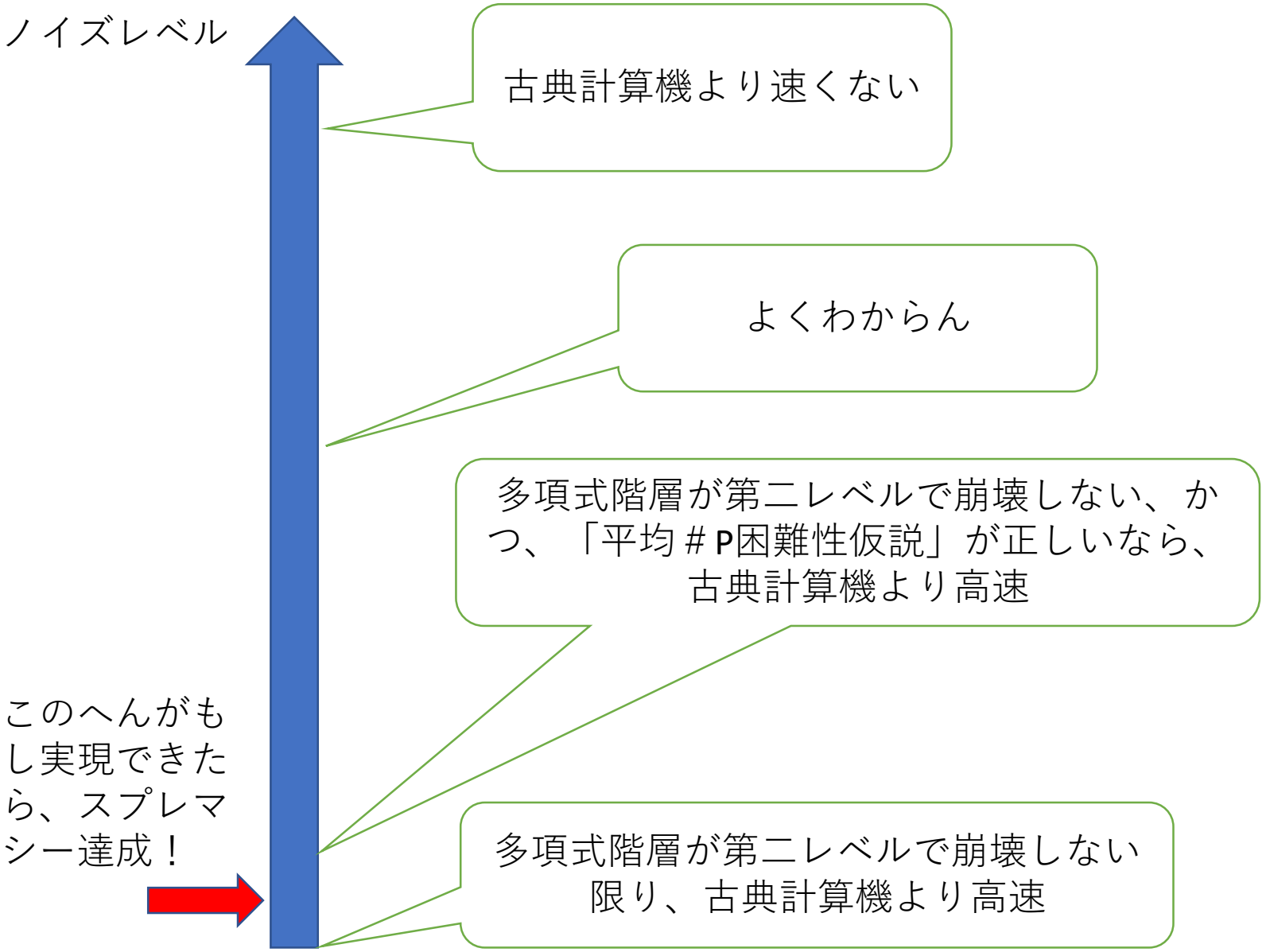
それと同じ確率分布でビット列を出せ　（なんの役に立つかは不明）



多項式階層が第二レベルで崩壊しないと仮定したら、

量子計算機は古典計算機より高速にサンプルできる

もっと正確には、ノイズレベルに応じて状況が変わる（実際のマシンにはノイズがある）



「弱い」マシンでもOK！

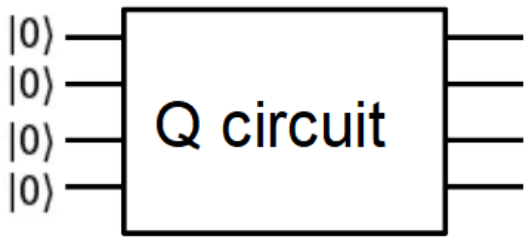
深さが４しかない量子回路
Terhal and DiVincenzo 2004

相互作用無し光子を使った量子計算機(Boson Sampling)
Aaronson and Arkhipov 2011

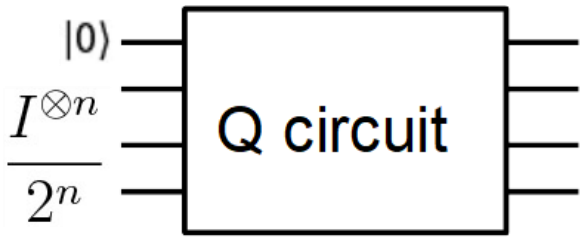
交換するゲートのみ(IQP)
Bremner, Montanaro, and Shepherd 2016

One-clean qubit model
TM, 2017

ゲートがランダムに作用する量子回路
Fefferman et al. 2018



通常の量子計算

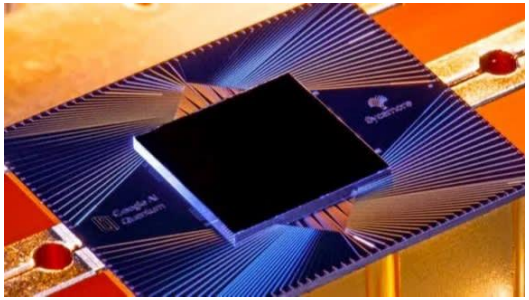


One clean qubit model

Googleの実験

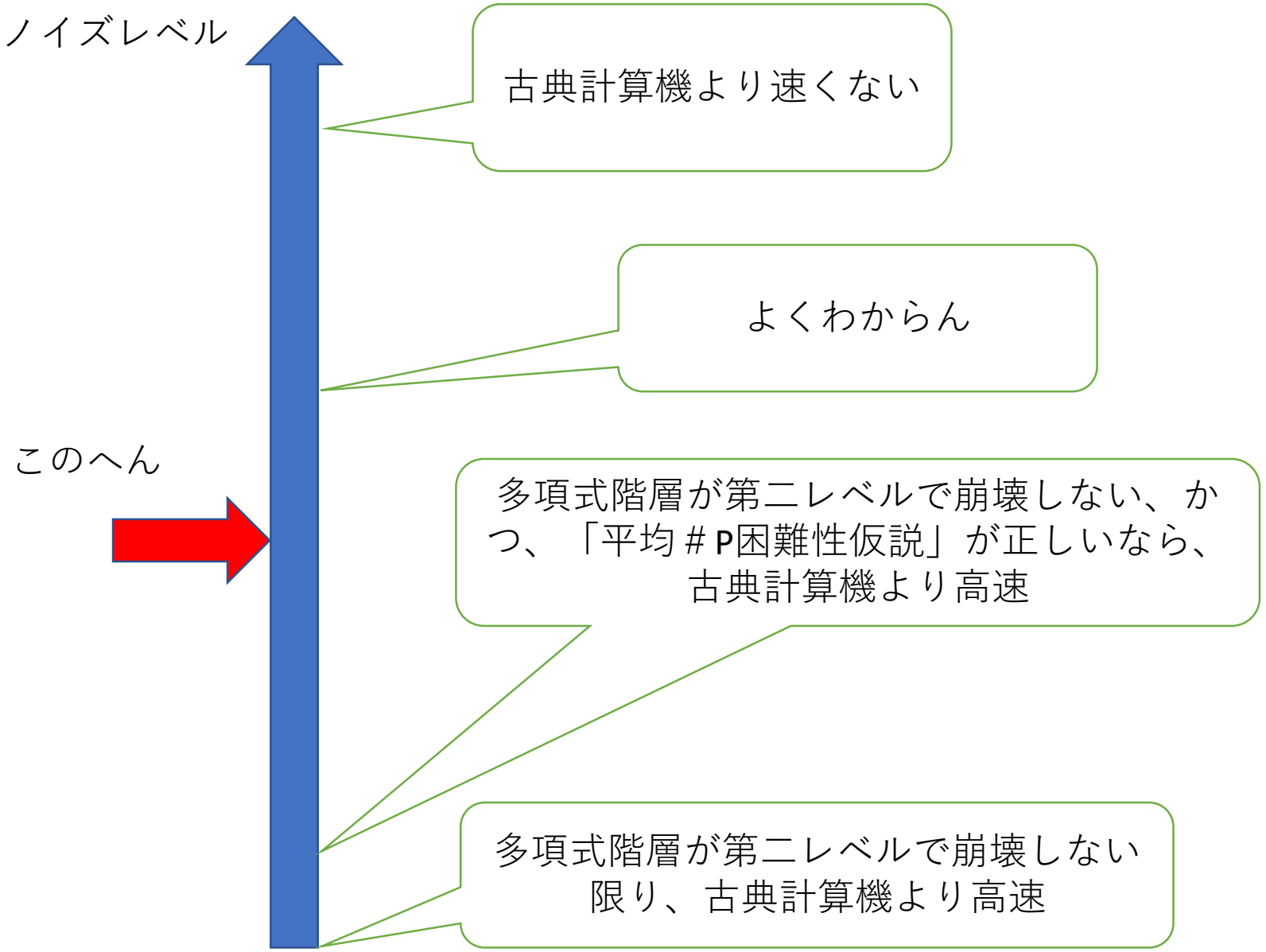
読売新聞　２０１９年１０月２４日

１万年かかる計算、３分２０秒で…量子計算機がスパコン超え



５０量子ビット

残念ながら、Googleマシンはノイズが大きすぎて、量子超越性理論は使えない。。。



えっじゃあ「古典計算機では１万年かかる」の根拠は？

→彼らが考えた「ベスト」の古典アルゴリズムで、１万年かかるというだけ。

→量子スプレマシー理論のように、「多項式階層が崩壊しない」とかで保証されたものではない。

実際、直後に

IBM：実際はもっとメモリ使えるから2.5日でできるよ。

アリババ：テンソルネットワーク使うと20日でできるよ。

Barak：もっと直接的な高速アルゴリズムあるよ。（確率分布完全に計算しなくても、クロスエントロピーベンチマークを破れるような古典シミレーションを直接的につくれるよ。）

今後の方向性

（１）実験家が頑張ってノイズをもっとさげる（量子誤り訂正も？）

（２）理論家が頑張ってもっと大きいノイズでも良い理論を作れ（無茶なことをいいおる）

（３）応用があるといいね！

（４）検証可能だといいね！

（５）もっとFine-grainedだといいね！

量子計算の検証

量子サーバー

通信路（古典）

利用者（古典計算のみ）

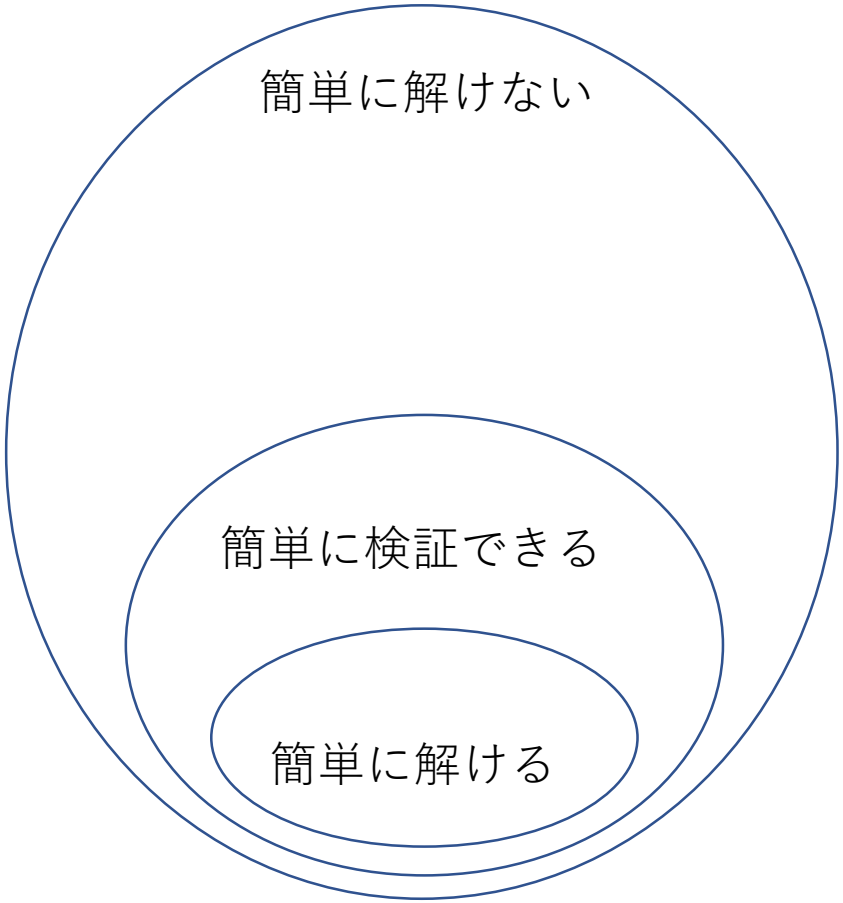
クラウドが正しい量子計算をしているのかチェックできるか？

Googleが超越性を出したことを確認できるか？

→かなり非自明な問題：量子計算は古典計算機でシミレートできないからこそ意味があるのに、そのせいで古典計算機で検算できなくなってしまうという皮肉なジレンマ！

基礎としても重要

検証というのは、「クラウドの検証」という応用だけでなく、そもそも計算機科学における重要な概念



まず気になるのは簡単に解けるか否か。

→簡単に解けないものが無数にある

その中で、「検証可能」という性質を持つサブクラスを考えるのは非常に有用

アルゴリズム、暗号、等。。。

注：要するにNPとか対話型証明は重用ですよといっているだけ。また、簡単に解けない、は正確には簡単に解く方法が知られていない

量子計算の検証の歴史

２００４年　Gottesmanが問題提起。Aaronsonがブログで紹介

２０１２年　Aharonov and Vazirani, arXiv:1206.3686 量子論の基礎とも関係することを指摘

1サーバー

２００８年　最初のプロトコル[Aharonov, BenOr, Eban, Mahadev, arXiv:1704.04487]

２０１２年　FKプロトコル[Fitzsimons and Kashefi, PRA 2017]

２０１８年　ポストフォックプロトコル[Fitzsimons, Hajdusek, TM, PRL 2018]

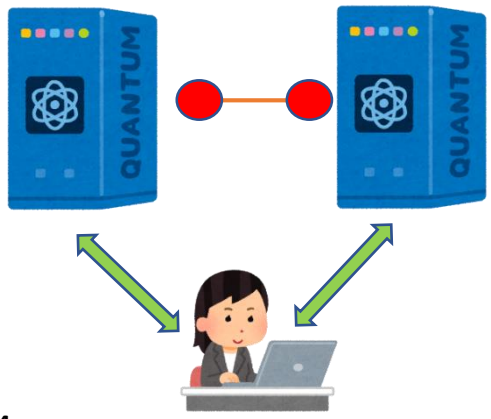
２０１８年　マハデフ [Mahadev FOCS2018]

２０２０年　ポストマハデフ（Fiat-Shamir, proof of quantumness, ゼロ知識等）

2サーバー

２０１３年　２サーバープロトコル [Reichardt, Unger, Vazirani Nature 2013]

２０２０年　MIP＊＝RE [Ji, Natarajan, Vidick, Wright, Yuen]



量子計算の検証に関するレビュー：Gheorghiu et al. arXiv:1709.06984

量子計算の正しさを事後チェックする新手法、JSTと京大が開発　Fitzsimons, Hadjusek, TM, Physical Review Letters

2018年01月23日 10時56分 公開　[ITmedia]

科学技術振興機構（JST）と京都大学は1月22日、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たと発表した。計算本体と計算チェックのプロセスを、世界で初めて分離。量子コンピュータの信頼度が高い場合はチェックを省き、低い場合は計算結果を受け取った後に事後チェックする仕組みで効率化した。

量子コンピュータはノイズに弱く、実行した計算は、正しさをチェックする必要がある。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り、常に同時に実行される仕組み。量子コンピュータの信頼度の高低に関わらず一様に同じチェックをすることになり、非効率だった。

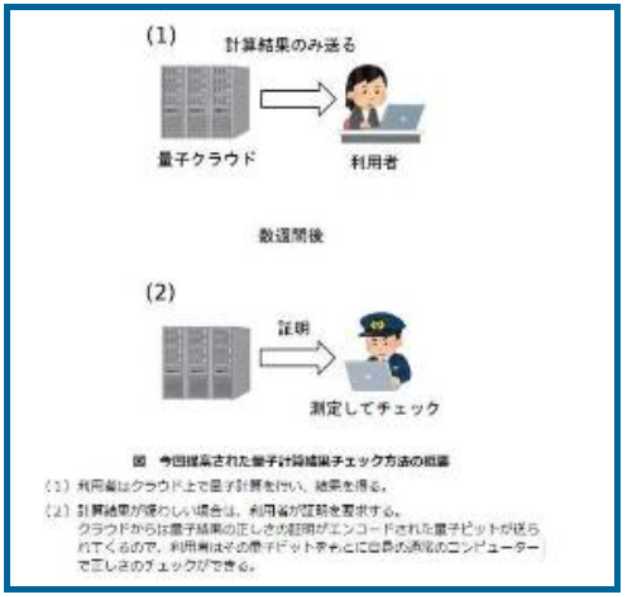


図　今回提案された量子計算結果チェック方法の概要
(1) 利用者はクラウド上で量子計算を行い、結果を得る。
(2) 計算結果が疑わしい場合は、利用者が証明を要求する。クラウドからは量子結果の正しさの証明がエンコードされた量子ビットが送られてくるので、利用者はその量子ビットそれぞれに自身の通常のコンピューターで正しさのチェックができる。

今回の研究では、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。量子コンピュータの信頼度の高さに応じて、計算の正しさを事後チェックできるようにした。

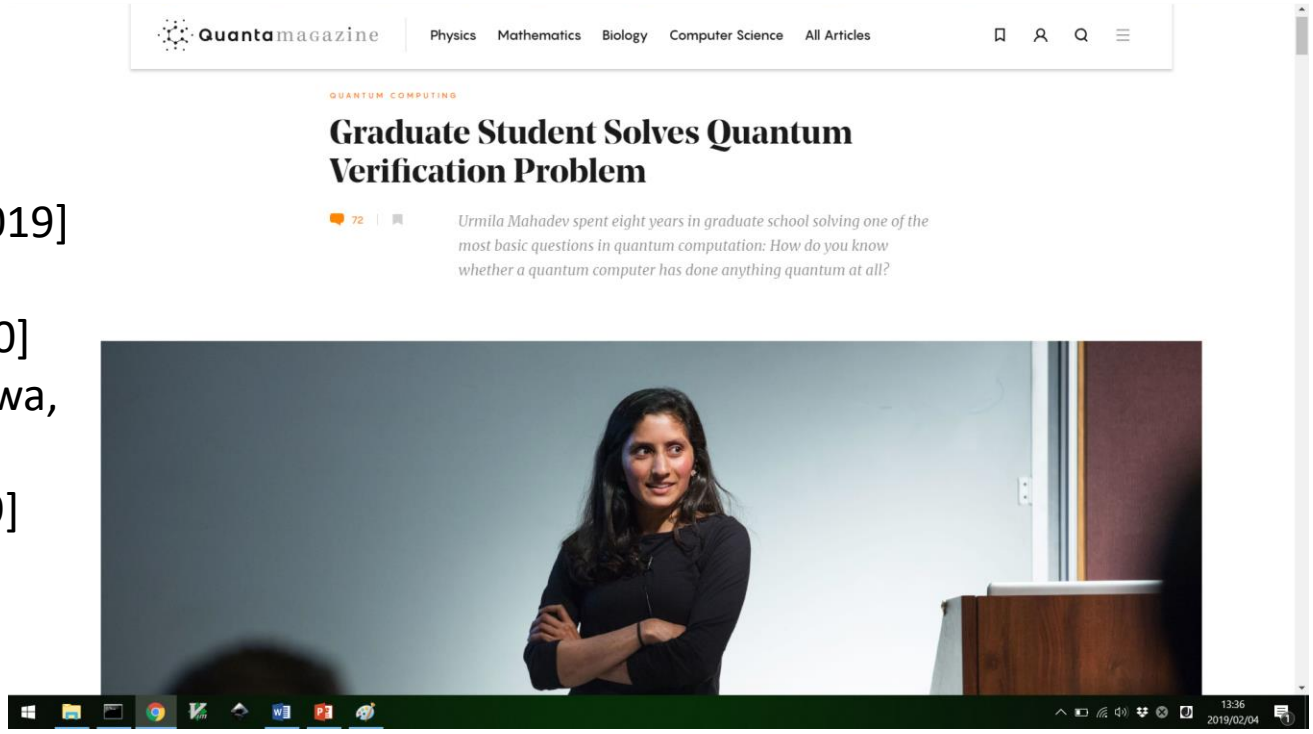
その後の発展

Mahadev FOCS 2018

Morimae-FitzsimonsプロトコルとLWEを組み合わせて、完全古典検証者による量子計算の検証を達成！！

ほかにも

[Andru and Vidick, FOCS2019]
[Alagic et al. 2020]
[Broadbent and Grilo, 2020]
[Chia, Chung, and Yamakawa, 2020]
[Cojocaru, ASIACRYPT2019]



Fine-grained 量子スプレマシー

Dalzell et al. Quantum 2020
TM and Tamaki, QIC 2019

従来の量子スプレマシー

多項式階層が崩壊しない限り量子計算機は古典計算機では多項式時間でシミレートできない

超多項式時間ならシミレートできるかも。５０量子ビット程度であれば頑張ってスパコンでできてしまうかも。。。
→Fine-grained complexity theoryを使う！

Fing-grained量子スプレマシー

SETHが破れない限り、量子計算は古典計算機ではある指数時間でシミレートできない

P≠NP：ある種の難しい問題は多項式時間で解けません
SETH：ある指数時間でも解けません

注：サンプリングの場合は厳密にはSETHでなくてcoC=P is not in NPのFine-grained版

Proof of quantumness

通信路（古典）

利用者（古典計算のみ）

ある量子証明者が存在して、利用者は高い確率で受理

どんな古典証明者に対しても、利用者は低い確率で受理

例：素因数分解（2000量子ビット、10^11個の量子ゲート）
Berkerski et al. FOCS 2018, TQC2020 (古典でできたらrewindしてLWE破れる）

END