

量子スプレマシー、セキュアクラウド 量子計算、量子計算の検証

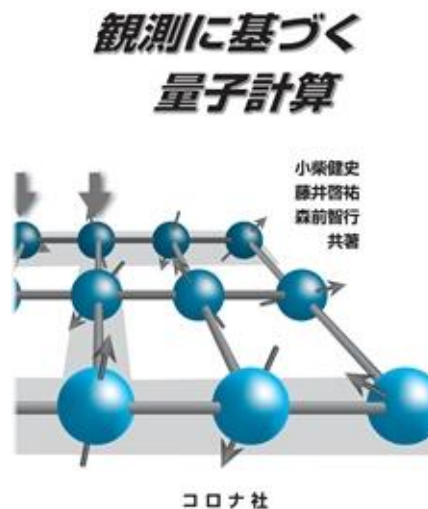
森前智行
(京都大学基礎物理学研究所)

大阪市立大コロキウム



内容

- 量子スプレマシー
- セキュアクラウド量子計算
- 量子計算の検証



小柴、藤井、森前
コロナ社



森前
森北出版

量子スーパーマシーン (量子超越性)

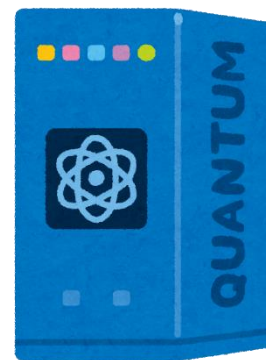
弱い量子計算機が古典より強いことを強い基盤に基づいて証明する

量子計算の歴史は約 36 年



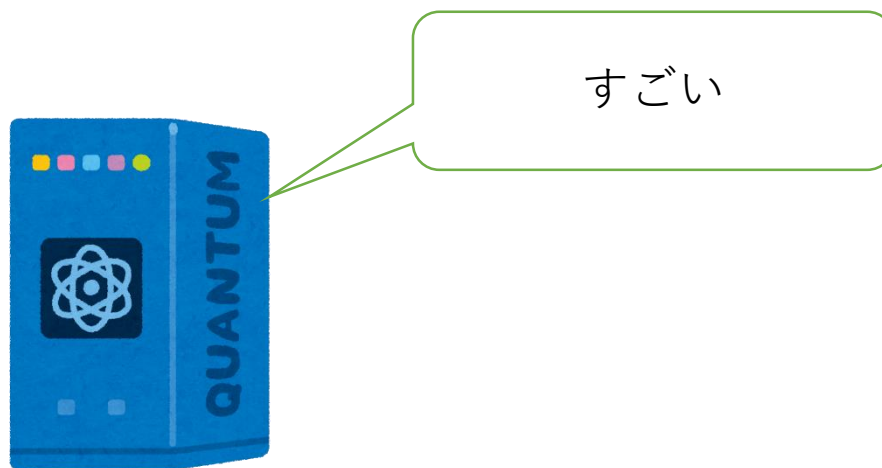
1982年

おもいついた



36年間の間に非常に多くの理論的・実験的結果が得られてきている

→現在では量子計算は古典計算よりすごいと信じられている



実際、様々な場面で量子優位性が証明されている

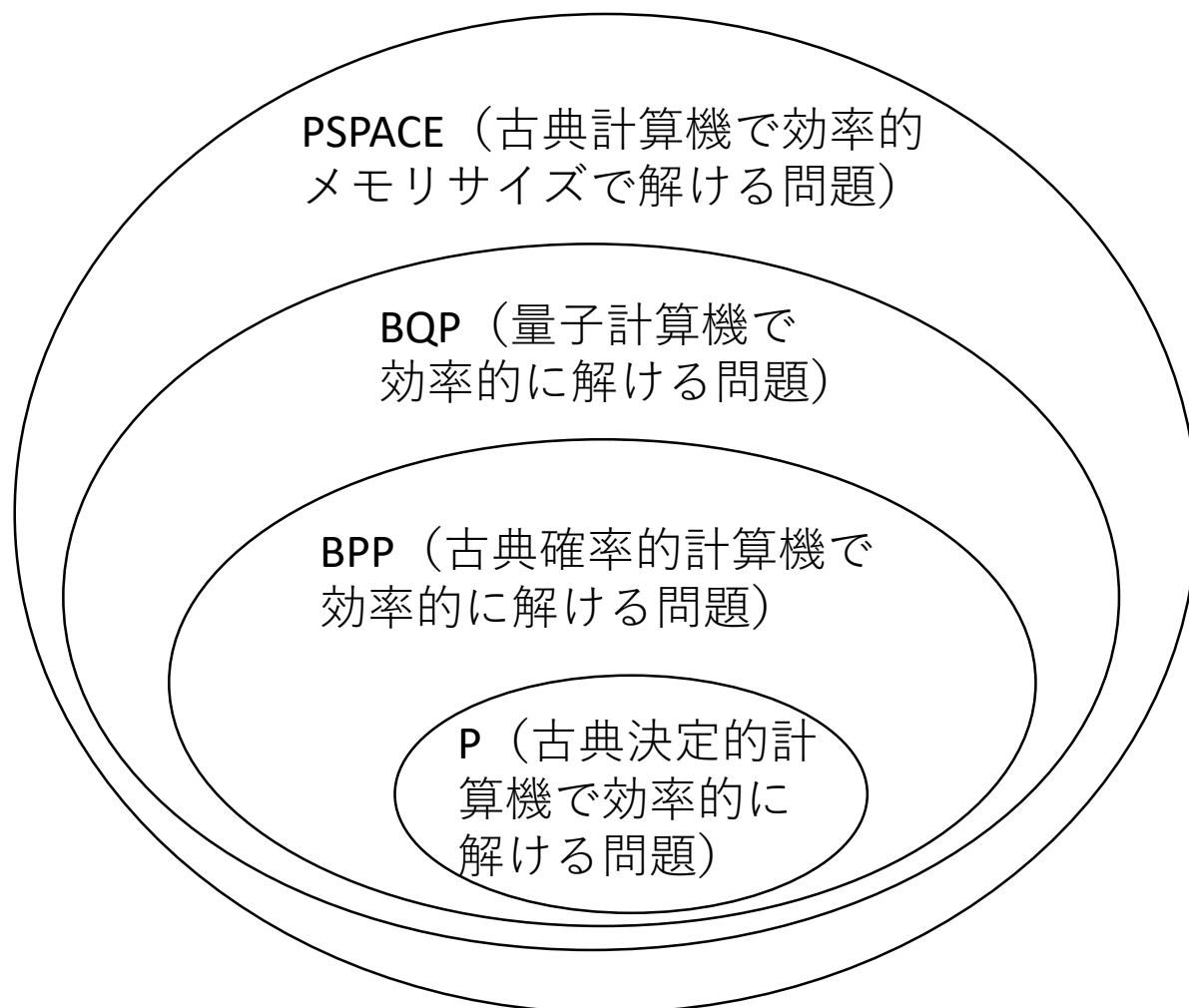
→通信量複雑性、ゲーム、定数深さ回路等

しかし、計算時間については、計算量理論の意味ではまだ未解決

計算量理論

計算機科学の一分野

計算にどのくらいのリソース（時間、メモリ）が必要かを調べる学問



$PSPACE \neq P$ は
大未解決問題！



$BQP \neq BPP$ を示すのは
恐ろしく難しいだろう

量子高速性証明のこれまでのアプローチ

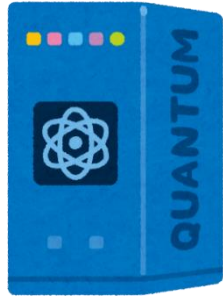
しかしながら、量子 > 古典であることを示唆する結果は大量にある
(quantum algorithm zoo)

二つのタイプに分類される

1. グローバータイプ (Grover、Simon、Bernstein-Vazirani)
2. ショアタイプ (素因数分解、Jones多項式、量子シミュレーション)

グローバertype

私の勝ち



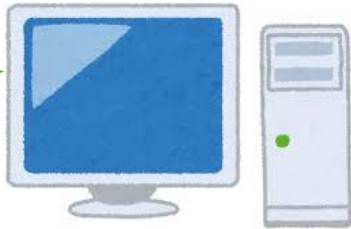
量子計算機

回数少ない



サブルーチン

くやしい



古典計算機

回数多い



サブルーチン

サブルーチンを呼ぶ回数だけ見ている。

→計算量理論におけるスタンダードなアプローチ（oracle query complexity）

→古典の限界の証明がしやすい。（多くの結果が得られている。）

→実時間でどうなるか不明。

ショアタイプ

こちらは実時間を見る(time complexity)

古典のベストより高速であることを示す

素因数分解：古典では遅いが量子では速い

→古典では遅いという数学的証明があるわけではない

将来古典の高速アルゴリズムが見つかるかも！

例：recommendation system

客の購買データからおすすめ商品を見つける量子機械学習アルゴリズム

→米国の18歳の学部生が高速古典アルゴリズムを見つけてしまった！

古典のベストと比較して速い、というのは危険！

さらなる問題点

複雑なアルゴリズムばかりで、実現が難しい

1 0 2 4 ビットの素因数分解をするのに

2 0 0 0 個の量子ビット、 10^{11} 個の量子ゲートが必要

[Roetteler et al., arXiv:1706.06752]



早く作って！

量子スーパーマシー

ショアータイプ、グローバータイプに次ぐ第三の新しいアプローチ！

2011頃から活発に。今ではGoogle等が実現を目指しており、一般向けのビジネス雑誌にも（用語だけは）出るように

これまでの問題を解決！

1. 基盤が弱い→計算量理論の強力な基盤で量子高速性を証明
2. 実現が大変→シンプルな量子計算機でもOK

注：デメリットもある
サンプリングなので応用がない
Additive errorの場合さらなる仮定が必要

強力な基盤

計算量理論の意味で量子 > 古典を完全に証明するのはほぼ不可能

量子 > 古典である確率を最大化する（メタ議論）

量子計算が古典計算でシミュレートできたら $P = NP$ になる

→ $P \neq NP$ なので、量子は古典ではシミュレートできない

Recommendation
Systemは
古典では遅い

素因数分解は
古典では遅い

$BQP \not\subseteq PH$

$P \neq NP$

PHの無限性

信頼度低

信頼度高

P、NPを一般化した多項式階層の無限性を使う！

シンプルでもOK

もう一つの重要なメリット：

量子スプレマシーは、ユニバーサルでなくて非常に弱い量子計算機でもOK!

1024ビットの素
因数分解

2000量子ビット
 10^{11} 個の量子ゲート

究極のゴール：
量子ビット使い放題
任意の量子アルゴリズム
量子誤り訂正完璧

近い将来に実現でき
そうな弱い量子計算
機でとにかく古典に
対する優位性を示す

弱い量子計算機でも量子優位性が強力な基盤で示せる！

量子スーパーマシンの歴史

深さ 4 の回路

Terhal and DiVincenzo, QIC 2004

相互作用無し光子(Boson Sampling)

Aaronson and Arkhipov, STOC 2011

交換するゲート(IQP)

Bremner, Jozsa, and Shepherd, Proc. Roy. Soc. A 2010

(古典イジング分配関数[Fujii and TM, NJP 2015])

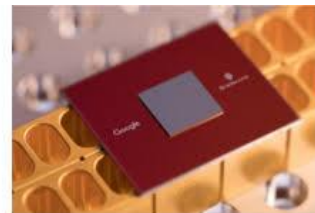
One-clean qubit model

TM, Fujii, and Fitzsimons, PRL 2014

ランダム回路

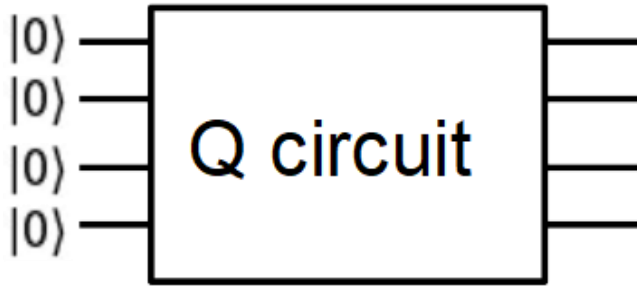
Fefferman et al. arXiv:1803.04402

Googleが実現！？

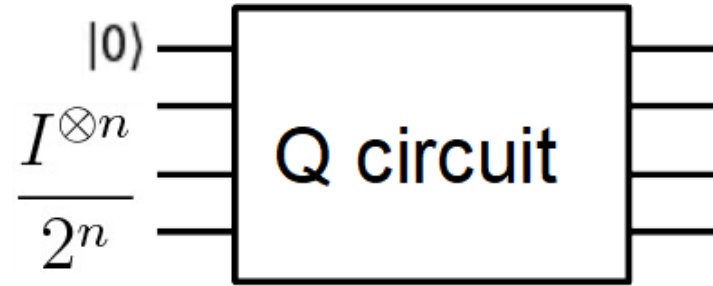


Googleマシン

One-clean qubit モデル



通常の量子計算



One clean qubit model
[Knill and Laflamme, PRL 1998]

古典よりはちょっと強いだろう

例：Jones多項式の計算
[Shor and Jordan 2007]

古典

ここじゃない
[Ambainis 2000]

ユニバーサル量子

明日誰かが古典の高速なアルゴリズムを発見するかも。。。

結果

One-clean qubitモデルがもし古典計算機で効率的にシミュレートできたら
多項式階層が崩壊する

$$P \subset NP \subset NP^{NP} \subset NP^{NP^{NP}} \subset \dots$$

$P=NP$ が信じられていないのと同様、多項式階層の崩壊は計算機科学では信じられていない

→ one-clean qubitモデルの古典シミュレート不可能性

TM, Fujii, and Fitzsimons, PRL 2014

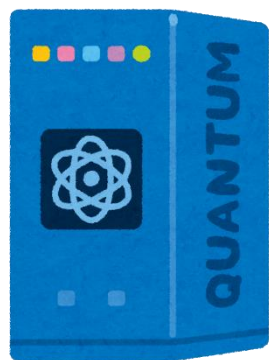
TM, PRA(R) 2017

Fujii, Kobayashi, TM, Nishimura, Tamate, and Tani, PRL 2018

長らく古典より速いだろうと信じられていたone-clean qubit modelの量子高速性を計算量理論の強固な基盤に基づいて初めて証明した！

セキュアクラウド量子計算

セキュアクラウド量子計算



量子計算機
(クラウド)



通信路 (古典)



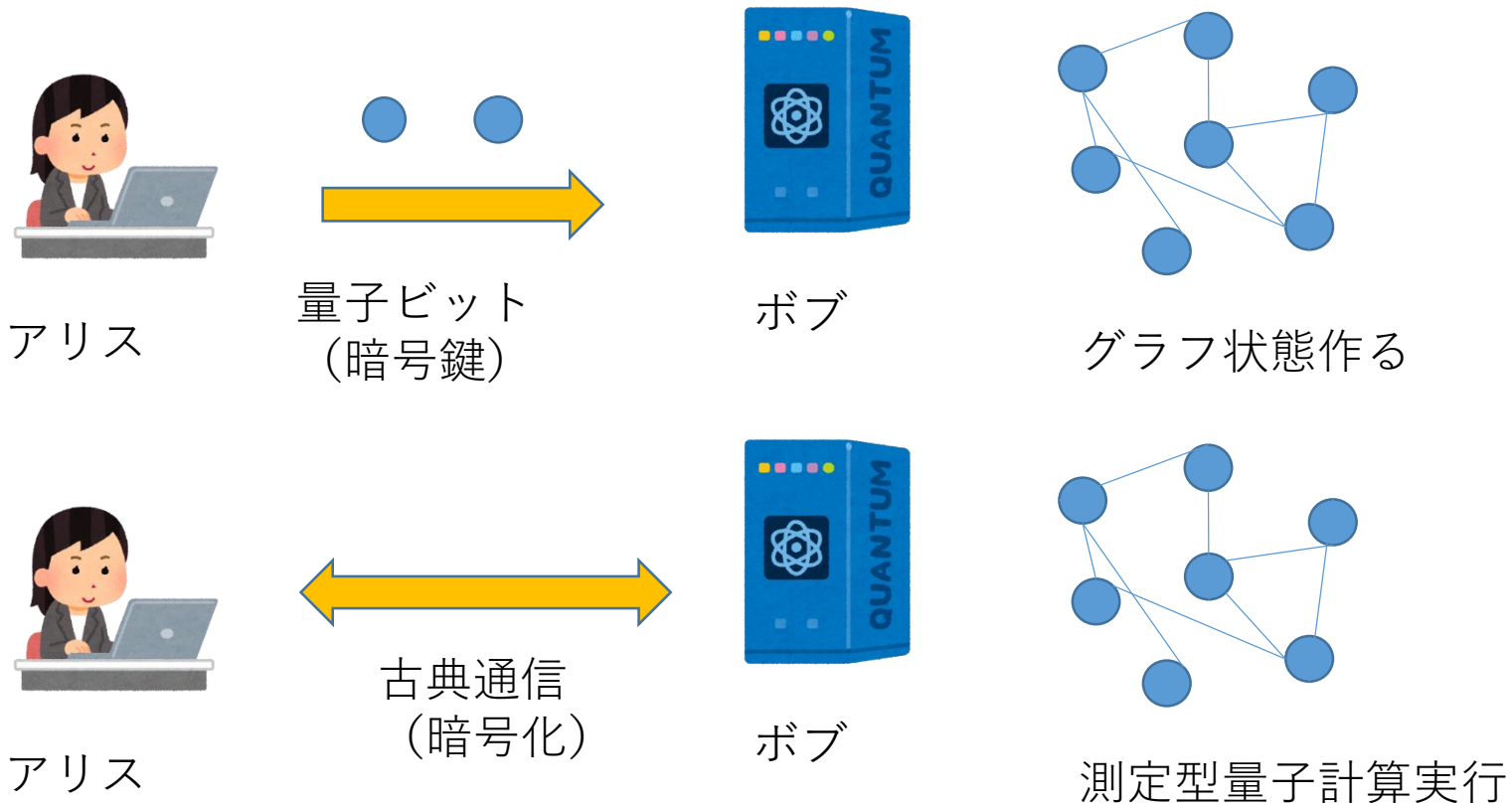
利用者 (古典計算のみ)

計算内容を秘密に保ったまま、量子クラウドに量子計算を委託できるか？

古典の場合でも、RSA暗号が提案されてから30年間未解決問題であった
→ 2009年にIBMのGentryがfully homomorphic encryptionを提案！

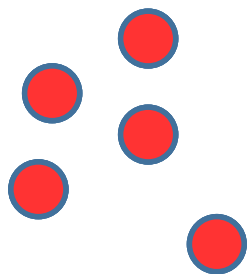
量子の場合も、可能であることが2009年にBroadbent-Fitzsimons-Kashefiにより証明された！

BFKプロトコル

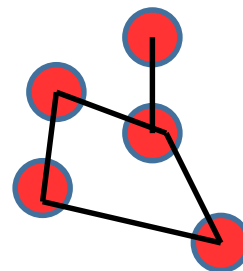


Broadbent, Fitzsimons, Kashefi, FOCS2009

量子論が正しいなら安全 (c.f. FHEは計算量的安全性)



ボブに送る



$$\{e^{iZ\theta_j}|+\rangle\}_j$$

$$CZ(\otimes_{j=1}^N e^{iZ\theta_j}|+\rangle) = (\otimes_{j=1}^N e^{iZ\theta_j})|G\rangle$$

測定角度の指示



$$e^{iZ\delta_j}|\pm\rangle \quad \text{基底で測定}$$

$$\delta_j = \phi_j - \theta_j$$

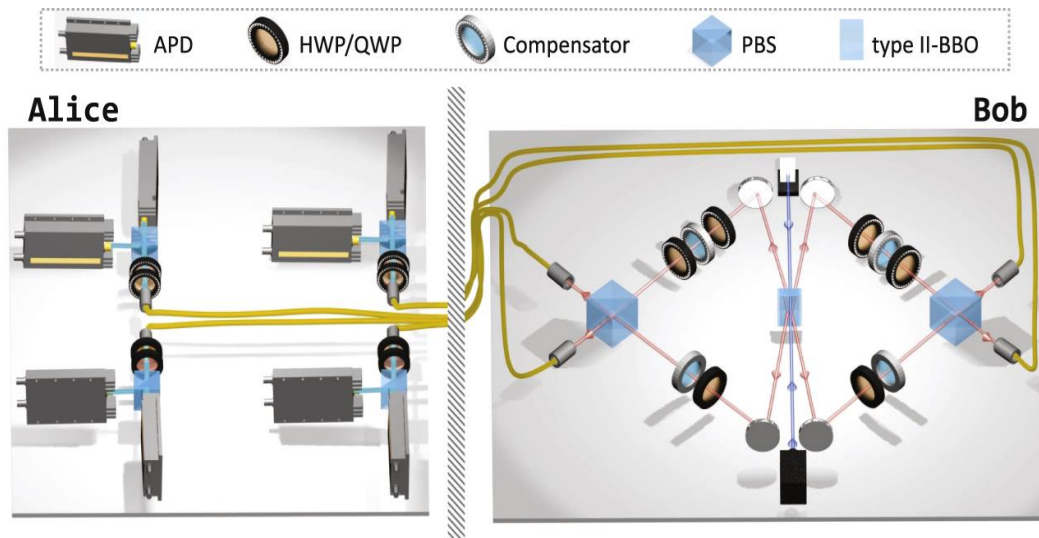


測定結果もらう

ボブは $\{\phi_j\}_j$ を知ることができない！！

もっとちゃんとした厳密な証明が知りたい方は[Dunjko et al. ASIACRYPTO2014]を参照。

実験



光キュービットによる実験(ウィーン大学)
Barz et al., Science 2012

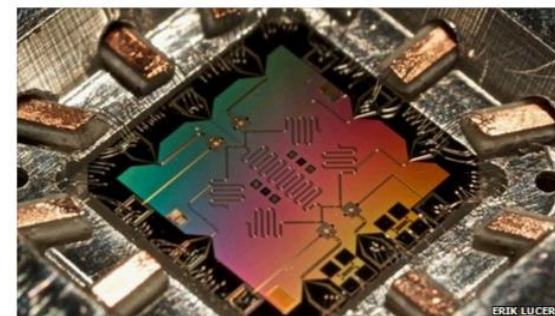


19 January 2012 Last updated at 19:17 GMT

732 Share f t e

Quantum computing could head to 'the cloud', study says

By Jason Palmer
Science and technology reporter, BBC News



Simple laboratory-based quantum computers may yet find a way to the desktop

A novel high-speed, high-security computing technology will be compatible with the "cloud computing" approach popular on the web, a study suggests.

Quantum computing will use the inherent uncertainties in quantum physics to carry out fast, complex computations.

A report in *Science* shows the trick can extend to "cloud" services such as Google Docs without loss of security.

Related Stories

Quantum computing takes big leap

Quantum computer slips onto chips

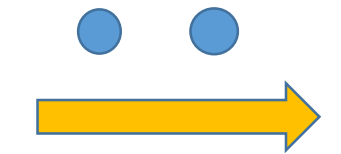
Limits of quantum world stretched

BFKプロトコルの問題点

1. Fault-tolerantなのか？
2. 証明が複雑
3. アリスが量子ビットを生成する必要がある



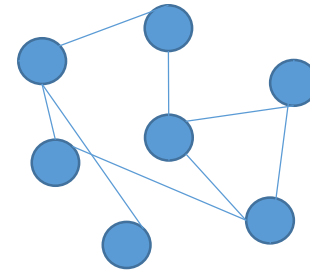
アリス



量子ビット送る

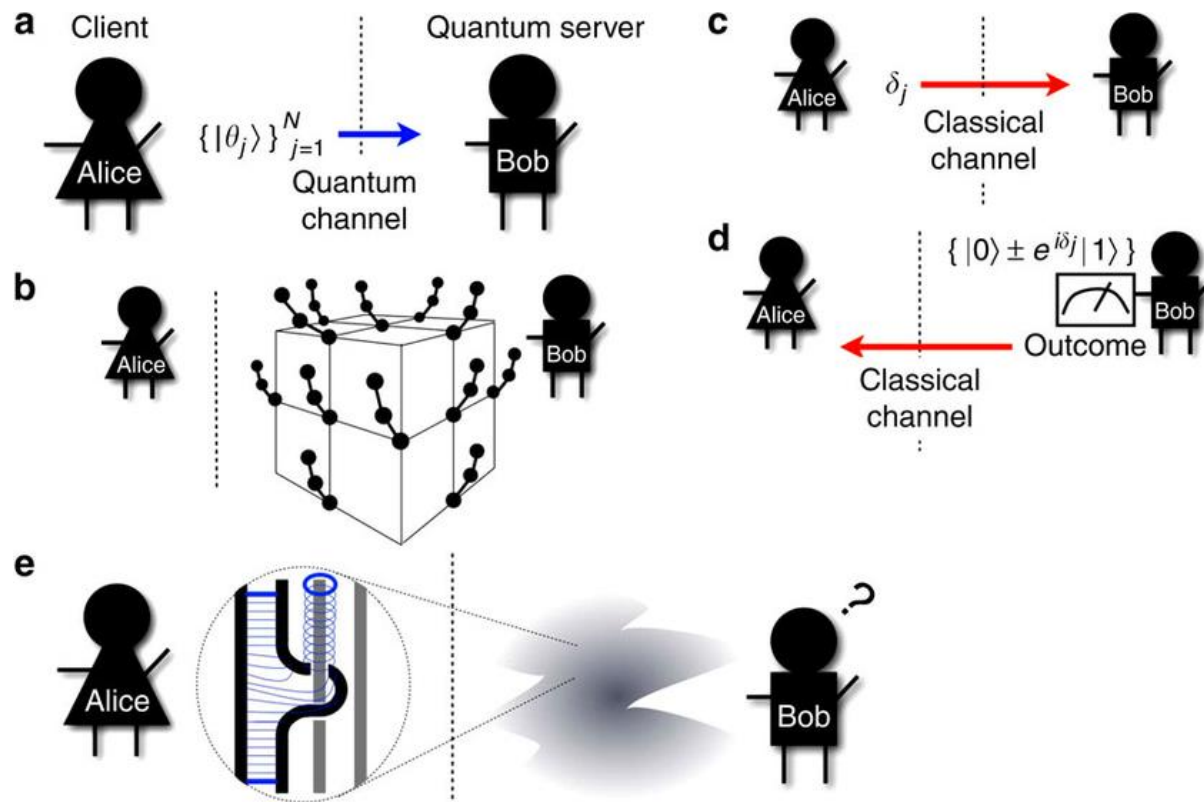


ボブ



グラフ状態作る

トポロジカルプロトコル

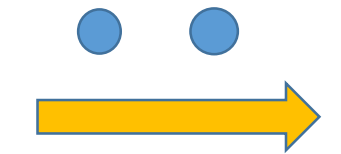


BFKプロトコルの問題点

1. Fault-tolerantなのか？
2. 証明が複雑
3. アリスが量子ビットを生成する必要がある



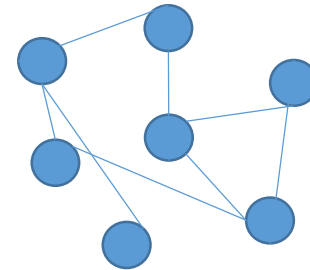
アリス



量子ビット送る



ボブ

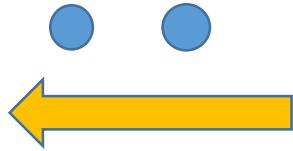


グラフ状態作る

Measurement-only プロトコル



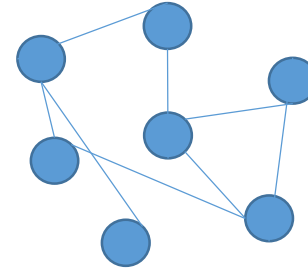
アリス
測定する



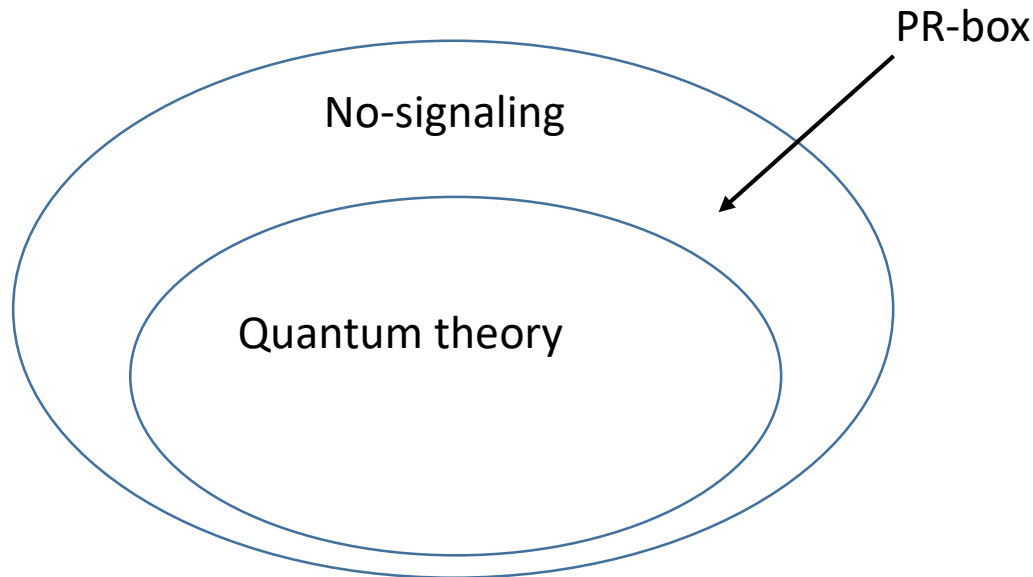
量子ビット送る



ボブ



グラフ状態作る



メリット：

測定は簡単な場合が多い
量子論より強い安全性
証明がシンプル（安全性を
無視できる）

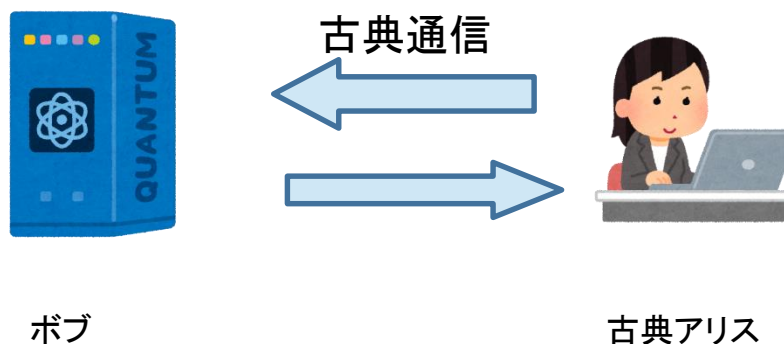
Device-independent

完全古典アリスは可能？

ある特別な場合は不可能

1ラウンド+Perfectly secureで可能ならBQPがNPに入る。

(BQPがNPに入るとは信じられていない。)



TM and Koshiha, arXiv:1407.1636

最近拡張された[Aaronson et al., arXiv:1704.08482]

→通信回数poly, インプットのサイズは漏れてもいい、
ボソンサンプリングできたらPH4崩壊、

その他の結果

通信量の効率化 [Giovanetti, Maccone, TM, and Rudolph, PRL 2013]

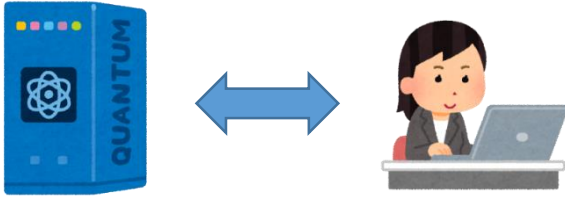
エンタングルメント蒸留 [TM and Fujii, PRL 2013]

アンシラ駆動型 [Sueki, Koshiba, and TM, PRA(R) 2013]

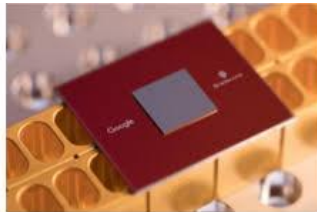
連続変数 [TM, PRL 2012]

量子計算の検証

量子計算の検証



量子クラウドが正しい量子計算をしているのかどうか、量子計算機を持たない利用者は検証できるか？



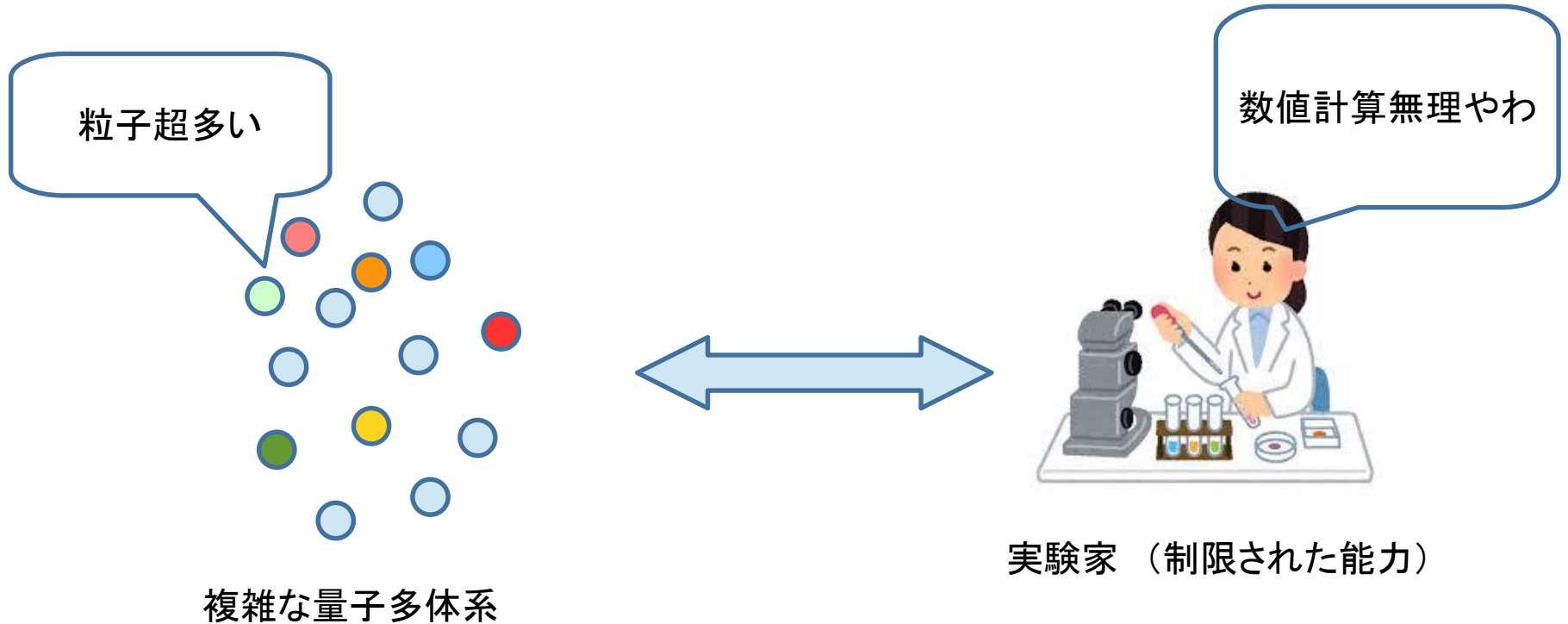
Google等は量子スプレマシーの領域に達する→どうやって検証するのか？

量子計算機は古典計算機ではシミュレートできない

→ 古典計算機では検証ができないという皮肉なジレンマ

→非常に重要な問題であり、世界中で研究がなされている

量子論基礎への応用



実験家は、量子多体物理理論が本当に正しいのか検証できるのか！？

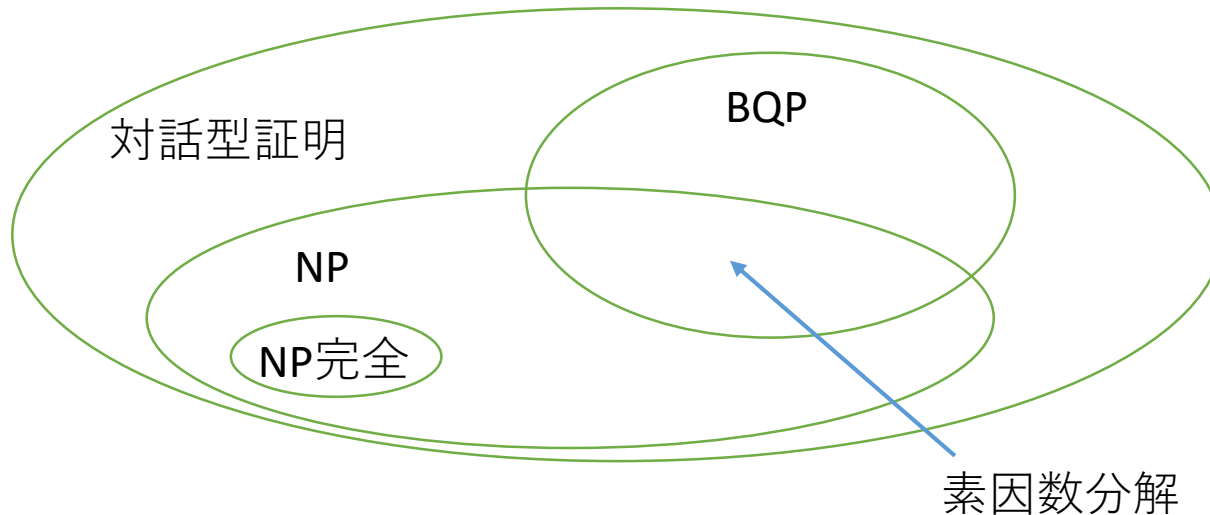
少数粒子系は、解析、数値計算と実験が一致することが検証されている。
量子多体系は解析、数値計算が無理！

NPなら検証可能

NP = 答えをもらえば、チェックは簡単にできる問題
素因数分解、巡回セールスマン等



しかし、NPは量子計算と相性が悪い！



対話型証明を考える必要がある！

対話型証明系



Merlin (なんでも解ける)



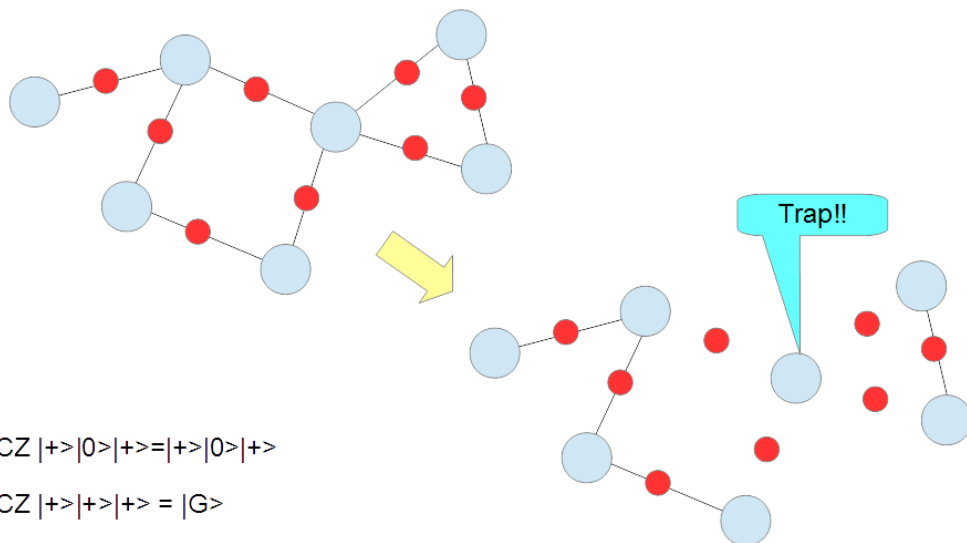
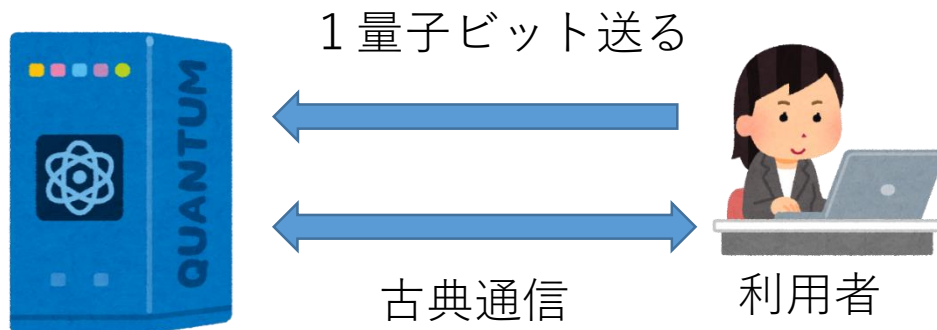
通信路 (古典)



Arthur (古典計算のみ)

NPの拡張。計算量理論におけるもっとも重要な概念の一つであり、暗号や近似アルゴリズム等においても重要！

利用者が少し量子なら可能



$CZ CZ |+\rangle|0\rangle|+\rangle=|+\rangle|0\rangle|+\rangle$

$CZ CZ |+\rangle|+\rangle|+\rangle = |G\rangle$

理論:

Fitzsimons and Kashefi, PRA 2017
TM, Phys. Rev. A (R) 2014

news & views

QUANTUM COMPUTATION

Honesty test

Alice does not have a quantum computer so she delegates a computation to Bob, who does own one. But how can Alice check whether the computation that Bob performs for her is correct? An experiment with photonic qubits demonstrates such a verification protocol.

Tomoyuki Morimae

Access to first-generation quantum computers will most probably come as a cloud service because only few organizations, such as governments or big companies, will own such expensive and high-maintenance machines. How can client's privacy be protected in cloud quantum computing? How can clients test the correctness of the results output by the quantum server even though they do not have a quantum computer of their own? Writing in *Nature Physics*, Stefanie Barz and colleagues answer these questions with a photonic qubit experiment.

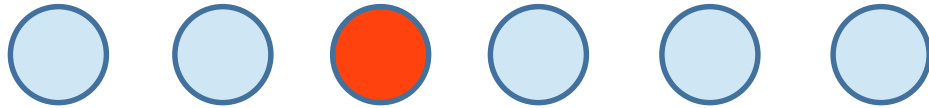
When you shop online, you do not want to reveal to a third party your private information, such as what you bought, your credit card number, your home address and so on. Alternatively, imagine that a pharmaceutical company uses a time-sharing service of a super-computer to run their molecular dynamics simulations. The pharmaceutical company wants to make sure that the data and the program — which are top secret in the industry — cannot be read by others. In short, securing



実験:

Barz et al. Nature Phys. 2013
TM, Nature Phys. N&V 2013

量子誤り訂正符号を使う



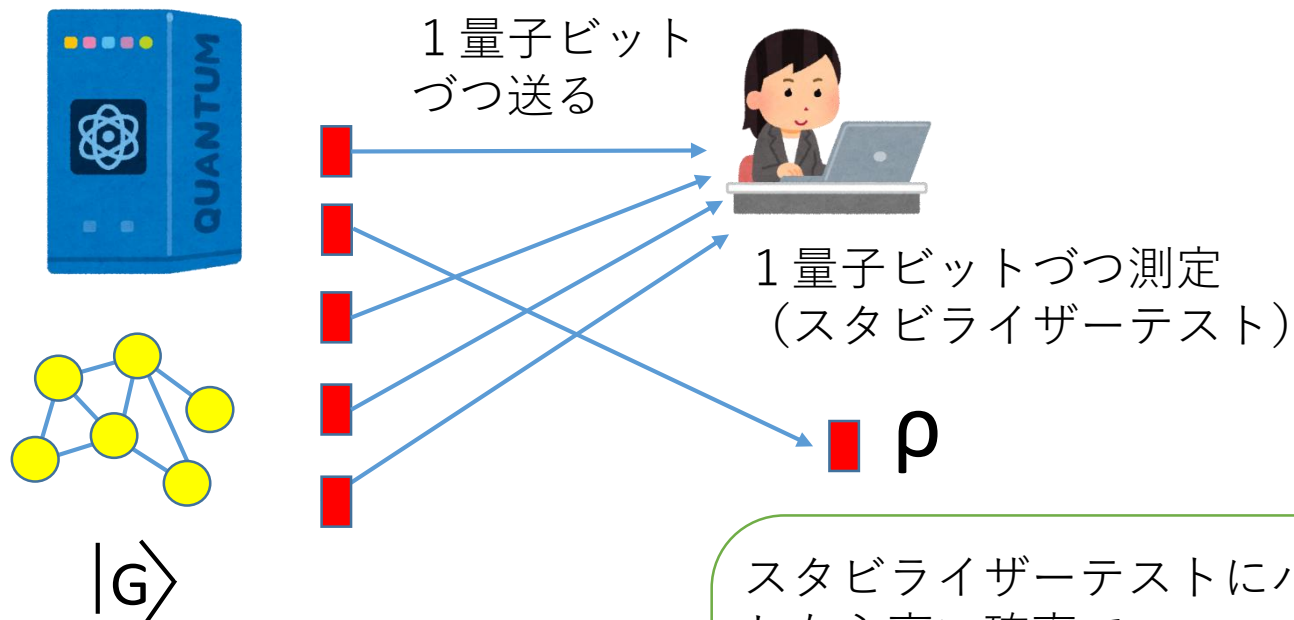
トラップに触れる確率 $=1/N$

量子誤り訂正符号をかませる

少数キュービットだけ触ってもただのエラーとして訂正(無視)される

内容を変えるには d 個以上のキュービットに触れる必要がある

→ トラップに触れないでロジカルビットを変えられる確率 $=2^{-d}$



スタビライザーテストにパス
したら高い確率で

$$\langle G | \rho | G \rangle \simeq 1$$

(i.i.d.でなくてもquantum de
Finetti定理使えばよい)

$$g_i |G\rangle = |G\rangle$$

$$|G\rangle\langle G| = \prod_i \frac{I + g_i}{2}$$

$$= \frac{1}{2^n} \sum_k s_k$$

理論:

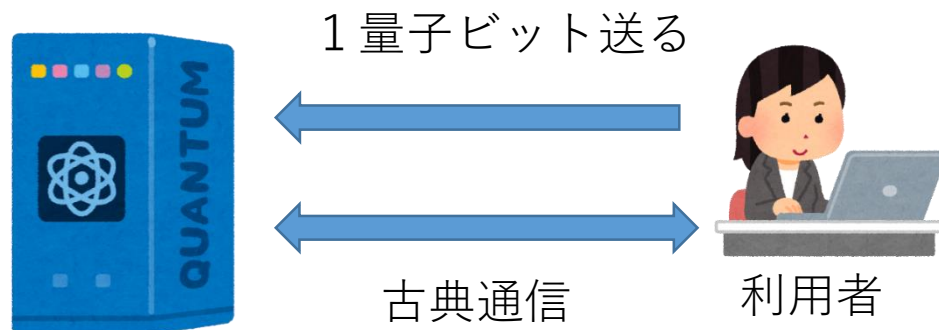
Hayashi and TM, PRL 2015

Takeuchi and TM, PRX 2018

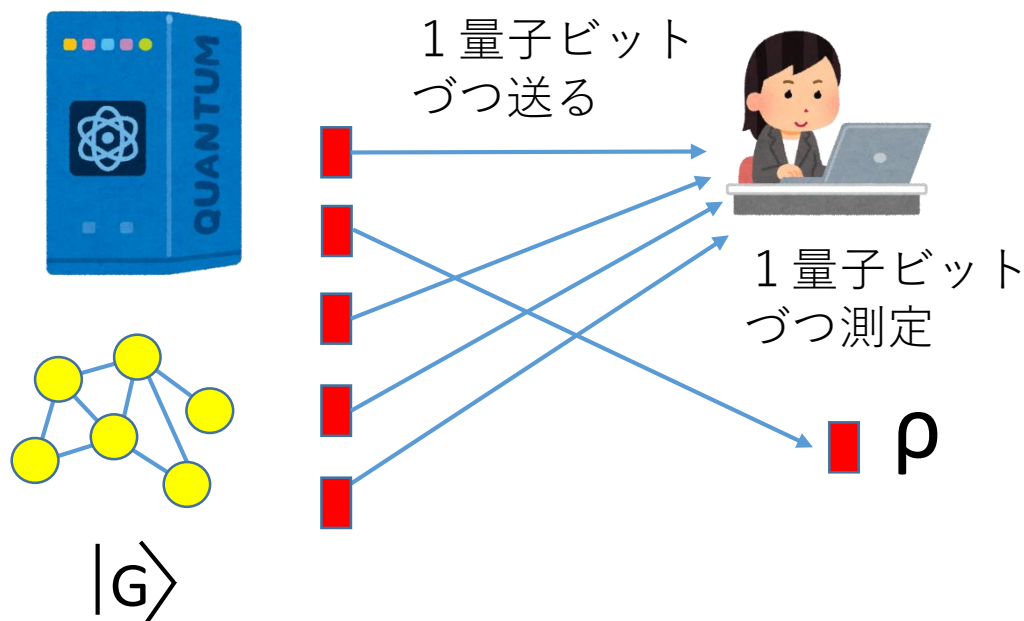
実験:

Greganti, Roehsner, Barz, TM, and Walther,
NJP 2016

計算と検証を分離できるか？

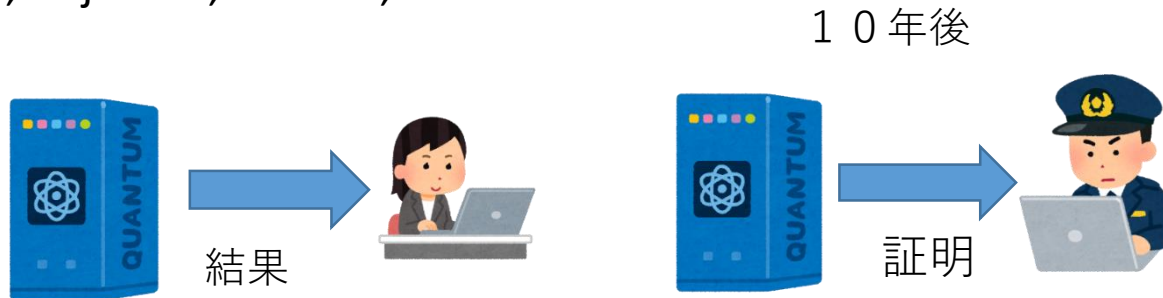


検証は検証で、計算は計算で切り離してできるのか？



Post hoc 検証

Fitzsimons, Hajdusek, and TM, PRL 2018

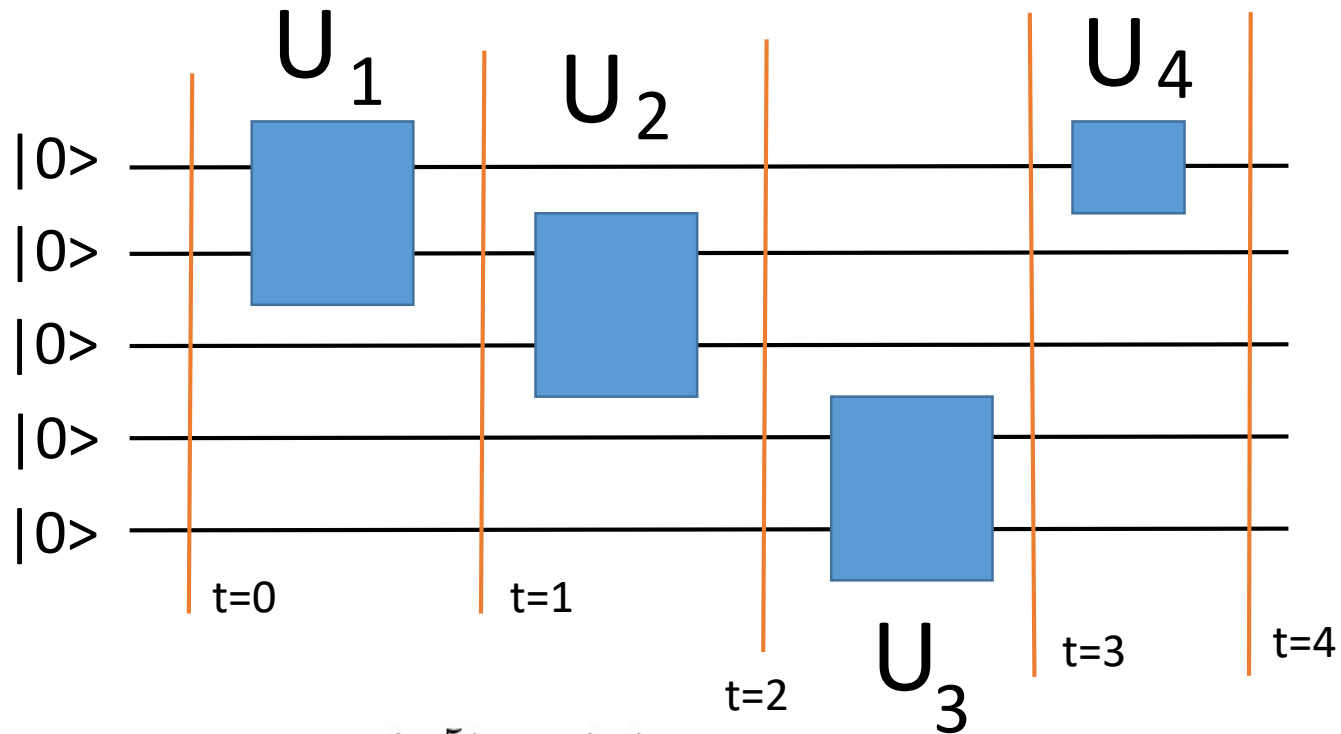


量子計算の正しさが事後的にチェックできる！

計算本体と検証を分離できる！

→量子計算そのものにはオーバーヘッドがない！

量子計算を状態にマップ



$$\begin{aligned}
 |\Psi\rangle = & U_4 U_3 U_2 U_1 |0^5\rangle \otimes |4\rangle \\
 & + U_3 U_2 U_1 |0^5\rangle \otimes |3\rangle \\
 & + U_2 U_1 |0^5\rangle \otimes |2\rangle \\
 & + U_1 |0^5\rangle \otimes |1\rangle \\
 & + |0^5\rangle \otimes |0\rangle
 \end{aligned}$$

history state と呼ばれている
[Feynmann and Kitaev]

History stateは基底状態！

$$\begin{aligned} |\Psi\rangle = & U_4 U_3 U_2 U_1 |0^5\rangle \otimes |4\rangle \\ & + U_3 U_2 U_1 |0^5\rangle \otimes |3\rangle \\ & + U_2 U_1 |0^5\rangle \otimes |2\rangle \\ & + U_1 |0^5\rangle \otimes |1\rangle \\ & + |0^5\rangle \otimes |0\rangle \end{aligned}$$

$$H_0 = (I - |0^5\rangle\langle 0^5|) \otimes |0\rangle\langle 0|$$

$$H_0 |\Psi\rangle = 0$$

初期状態の正しさをチェック

$$H_{prop}^1 = I \otimes |1\rangle\langle 1| + I \otimes |2\rangle\langle 2| - U_2 \otimes |2\rangle\langle 1| - U_2^\dagger \otimes |1\rangle\langle 2|$$

$$H_{prop}^1 |\Psi\rangle = 0 \quad \text{プロパゲーションのチェック}$$

$$H = H_0 + \sum_{t=0}^4 H_{prop}^t$$

$$H = H_0 + H_{prop}$$

$$H_0 = |0^n\rangle\langle 0^n| \otimes |t=0\rangle\langle t=0| \quad H_{prop} = \sum_{t=0}^{T-1} H_{prop}^t$$

時間をエンコード
するのに $\log T$
量子ビット必要

摂動法により、最終的に 2 体の XZ ハミルトニアンにできる！

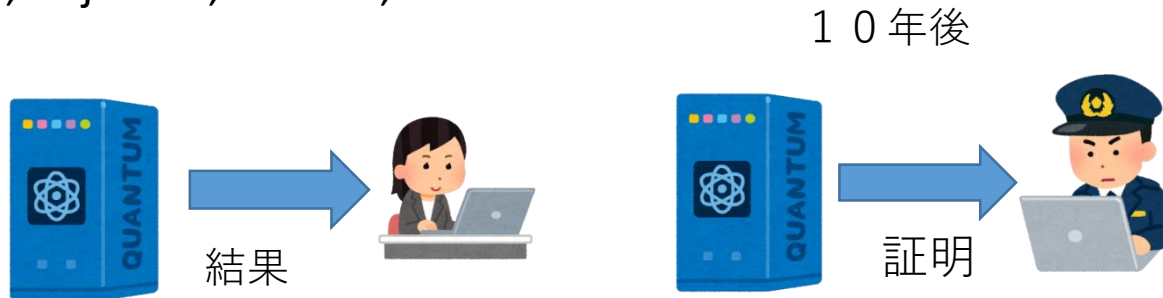
$$H = \sum_i (\alpha X_i X_{i+1} + \beta Z_i Z_{i+1} + \gamma X_i + \delta Z_i)$$

つまり、2 体 XZ ハミルトニアンの基底状態は、量子計算をエンコードしている！

(例：断熱量子計算)

Post hoc 検証

Fitzsimons, Hajdusek, and TM, PRL 2018



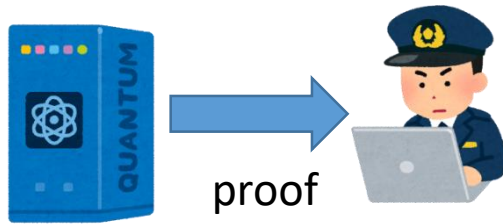
History stateを送ればよい

$$|\Psi\rangle = \sum_{t=0}^T U_t \dots U_1 |0^n\rangle \otimes |t\rangle$$

エネルギーの測定は1量子ビットでできる！

[TM, Nagaj, Schuch, PRA2016]

Fault-toleranceが簡単



CSSコードはXとZのロジカル測定が簡単！
(transversalにできる。)

$$|\Psi\rangle = \sum_{t=0}^T U_t \dots U_1 |0^n\rangle \otimes |t\rangle$$

$$H = \sum_i (\alpha X_i X_{i+1} + \beta Z_i Z_{i+1} + \gamma X_i + \delta Z_i)$$

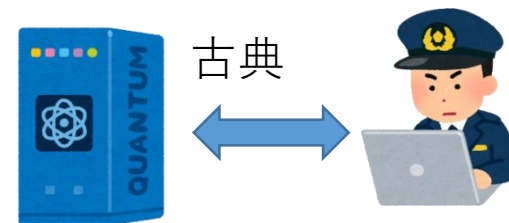
Post hocプロトコルが利用された

耐量子暗号が量子計算では難しいと仮定するなら、量子計算の検証は可能！
[Mahadev, arXiv:1804.01082]

→post hocプロトコルを利用！



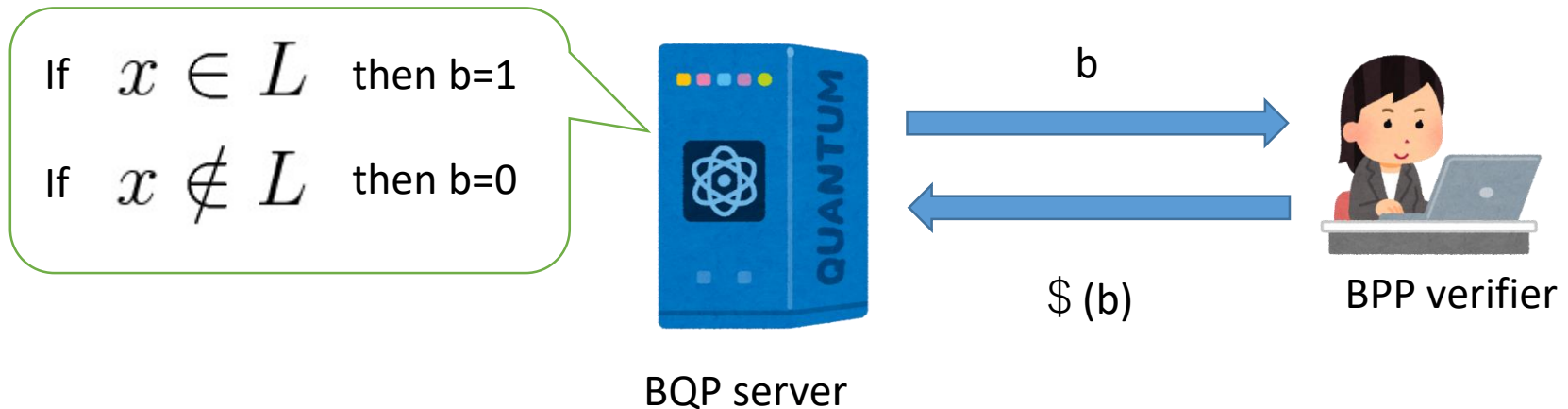
$$|\Psi\rangle = \sum_{t=0}^T U_t \dots U_1 |0^n\rangle \otimes |t\rangle$$



$$|\Psi\rangle = \sum_{t=0}^T U_t \dots U_1 |0^n\rangle \otimes |t\rangle$$

6. Rational proof system

Server is not malicious, but rational (economically motivated) [Azar and Micali, STOC 2012]



$$\langle \$ \rangle_b = bp_{acc} + (1 - b)(1 - p_{acc})$$

If $x \in L$ then $p_{acc} > 2/3$

If $x \notin L$ then $p_{acc} < 1/3$

To maximize the profit, the server has to send the correct b !

→ If the server is rational, classical verifier can guarantee the correctness of the result!

Assume L is in BQP. Then there exists poly-time quantum circuits W such that

$$p_{acc} = \langle 0^n | W | 0^n \rangle$$

We assume that W consists of only Hadamard and Toffoli

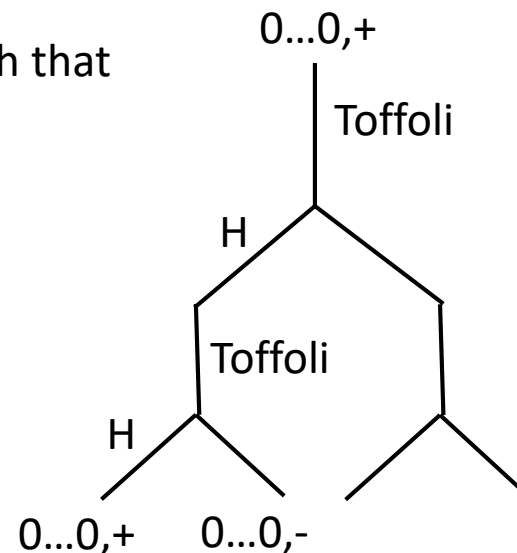
From W , we construct a non-deterministic algorithm such that

$$\langle 0^n | W | 0^n \rangle = \frac{A - R}{\sqrt{2^h}}$$

A : number of accepting paths

R : number of rejecting paths

h : number of Hadamard gates in W

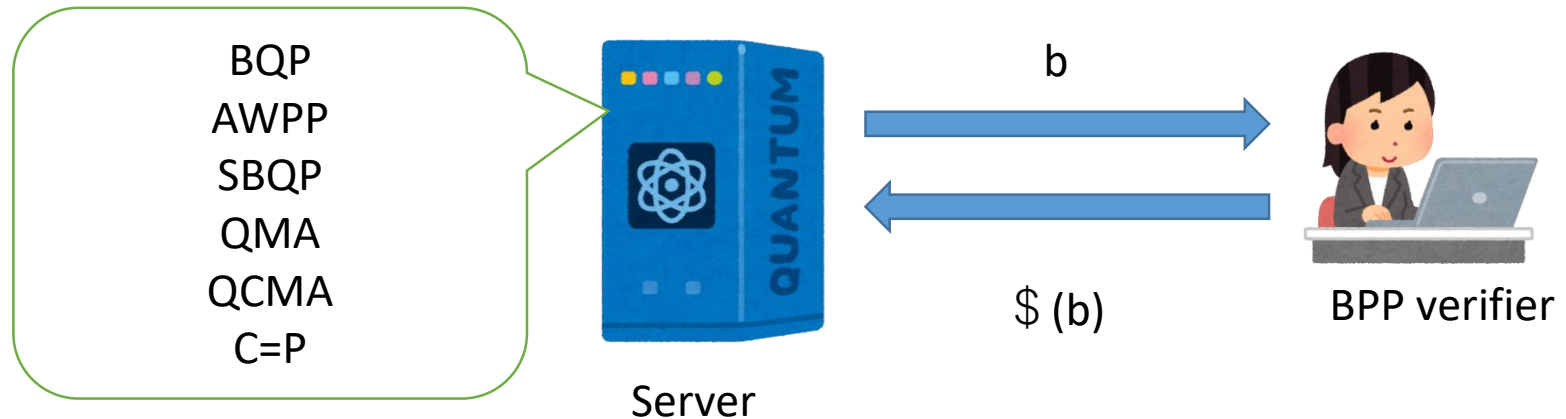


Probabilistically simulate the non-deterministic machine

$$q_A = \frac{A}{2^h}, \quad q_R = \frac{R}{2^h}$$

$$\langle 0^n | W | 0^n \rangle = \frac{A - R}{\sqrt{2^h}} = \sqrt{2^h} (q_A - q_R)$$

Generalization to other classes

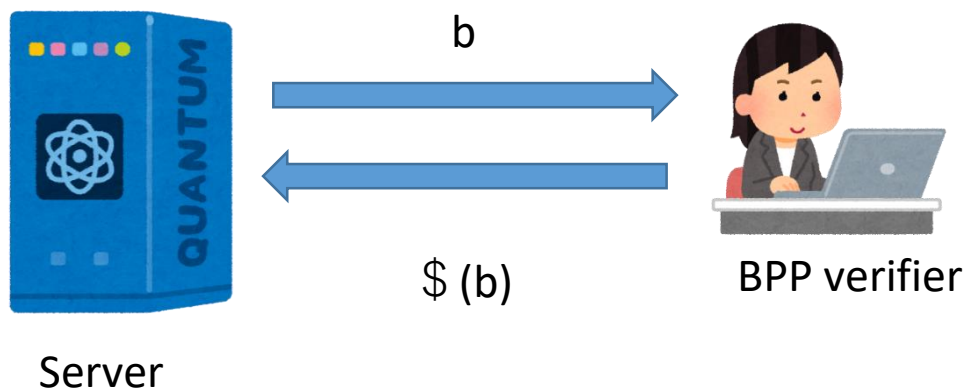


Simulate NDTM of GapP function probabilistically

Extra factors are renormalized into the reward.

To maximize the profit, the server has to send the correct b !

Reward must be exponentially large



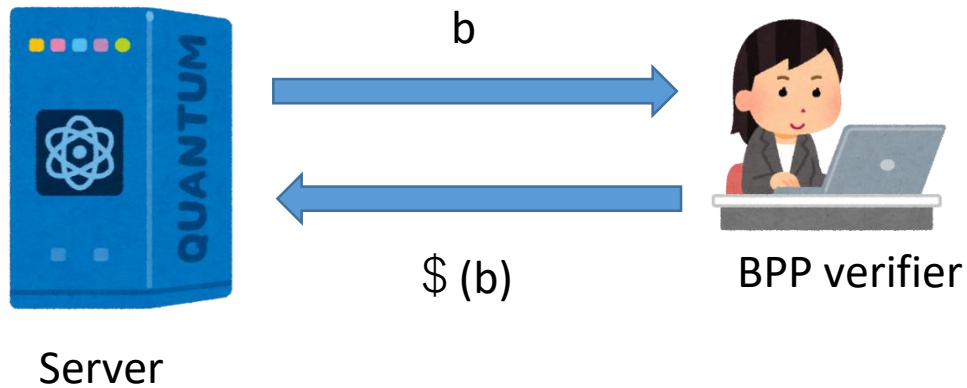
$$\$ = O(\sqrt{2^h})$$

Unfortunately, it is unavoidable unless $BQP=BPP$

$$\langle \$ \rangle_b = \sum_w p(b, w) \$(b, w)$$

If $|\$(b, w)| < \text{poly}$, the BPP verifier can estimate $\langle \$ \rangle_b$ by herself
→ BQP is in BPP!

Open problem



$$\$ = O(\sqrt{2^h})$$

Can we make $|\$| < \text{const}$?

One possible approach: consider multiple rounds

まとめ

1. 量子スプレマシー

弱い量子計算機であっても古典より強いことを計算量理論の強力な基盤に基づいて示す研究

→Google等が実現！？

量子と古典の境界を計算の視点から探るという
ファンダメンタルな研究でもある！

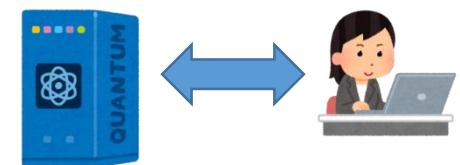


2. セキュアクラウド量子計算、量子計算の検証

ほぼ古典の利用者であっても、量子クラウドを安全に利用できる

→IBMがクラウドサービスを開始

対話型証明という基礎的な重要性もある！



END