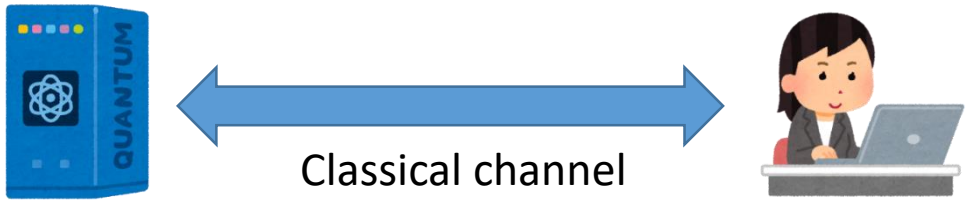
Rational proofs for quantum computing

Tomoyuki Morimae

(Yukawa Institute for Theoretical Physics, Kyoto University)

Classical verifiability of quantum computing



Quantum computer

Classical verifier

Can a classical verifier verify the correctness of quantum computing?

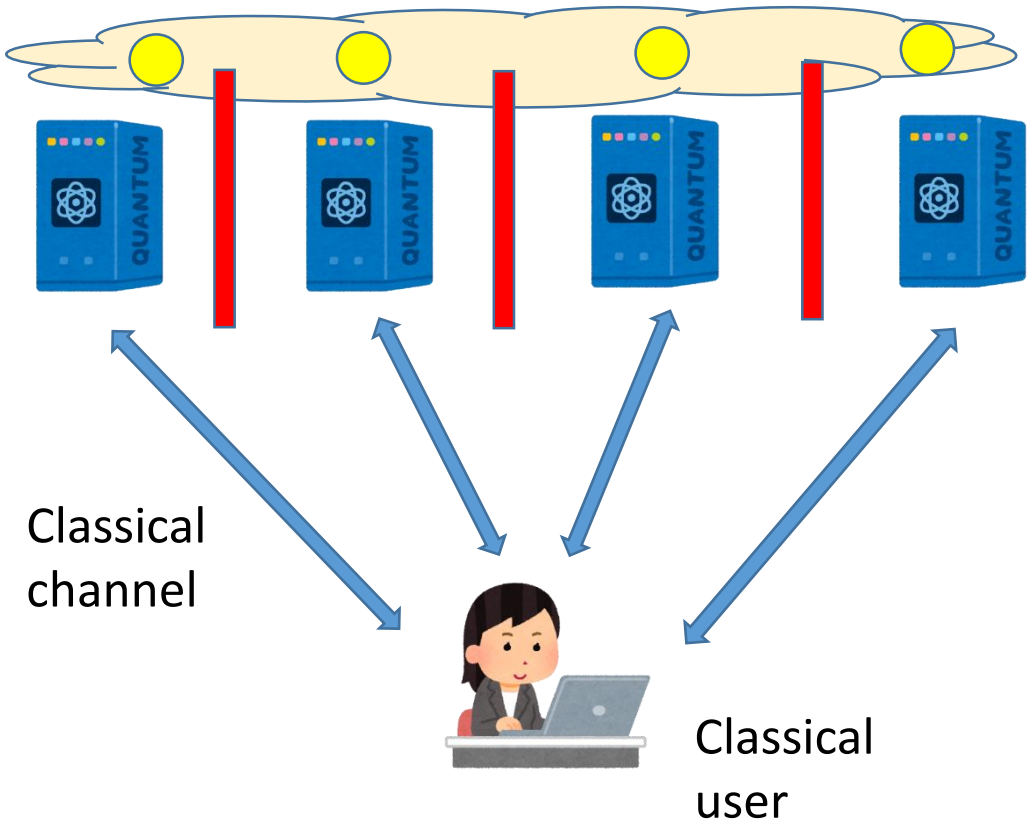
1. Correctness of cloud quantum computing
2. Verifying Google's quantum supremacy

QC is useful when classically not simulatable → ironical dilemma

6 partial solutions:

1. Multiple provers
2. Slightly quantum verifier
3. PSPACE=IP
4. Specific problems (recursive Fourier sampling, solvable group)
5. Computational security
6. Rational proof system ← today's main result

1. Multiple servers

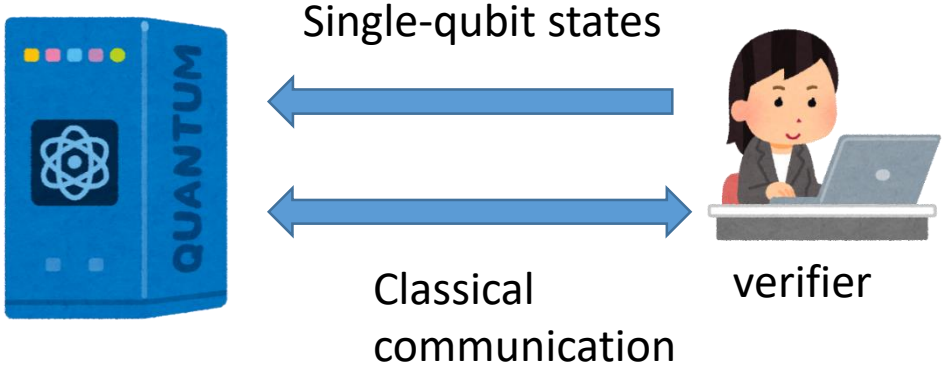


Many servers sharing entanglement, but no communication

Reichardt, Unger, Vazirani, Nature 2013
McKague Theory of Computing 2016
Zi, STOC16

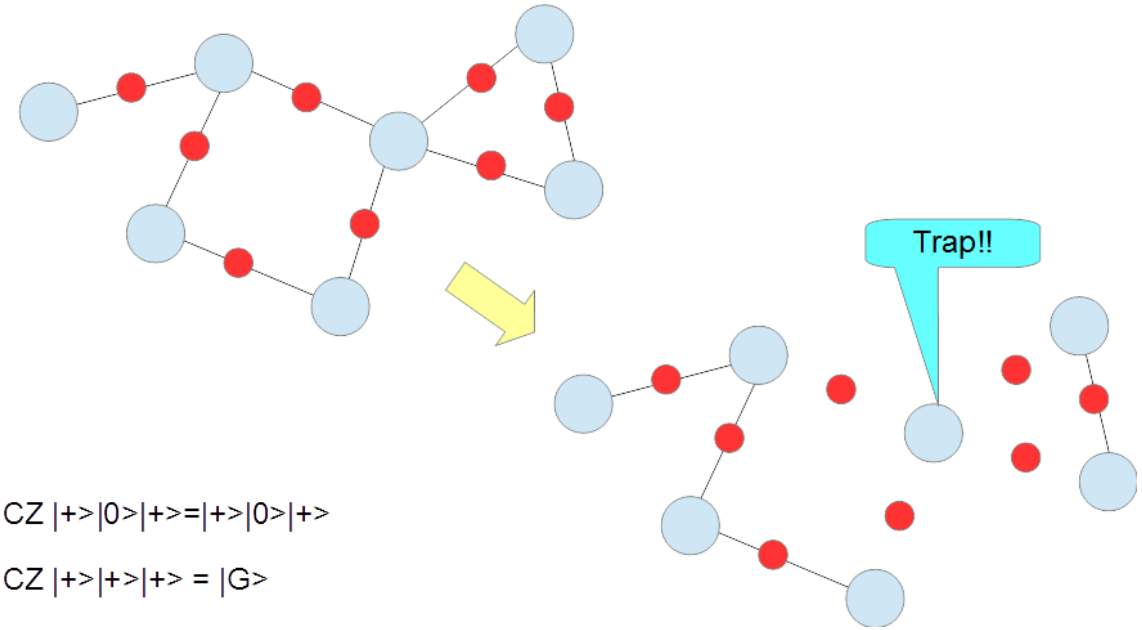
Experiment: Jian-Wei Pan, PRL2017

2. Slightly quantum user



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

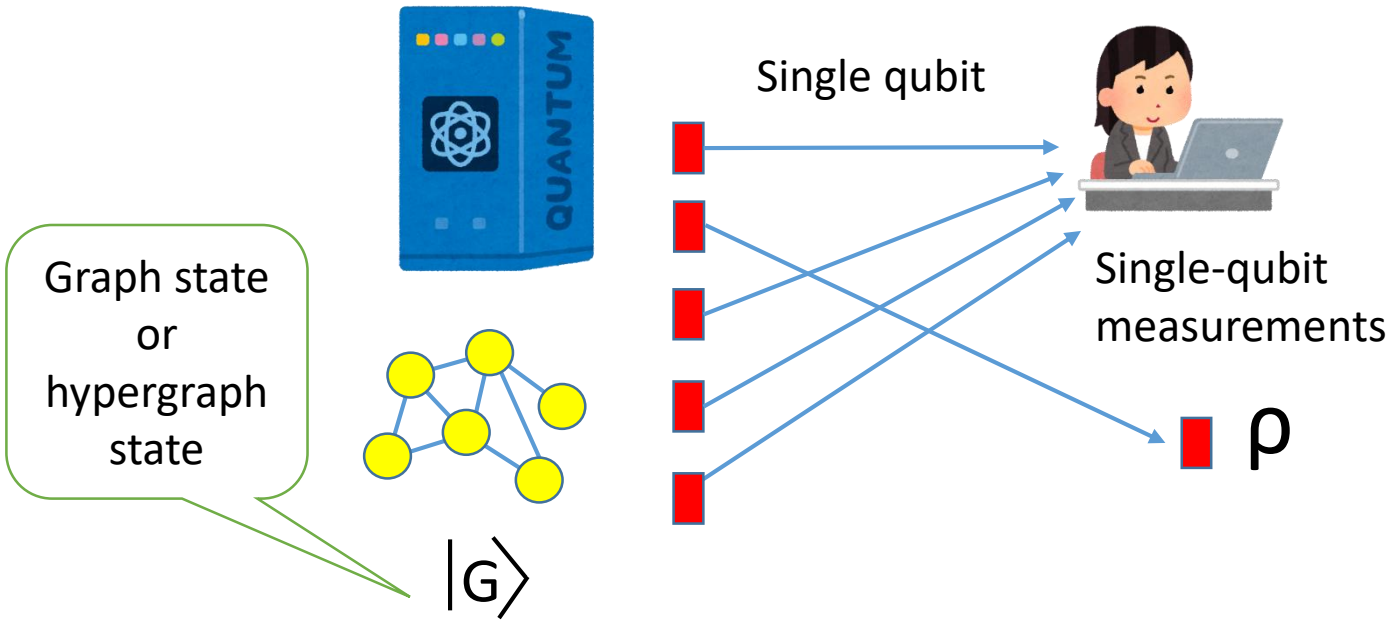
Experiment:
Barz et al. Nature Phys. 2013
TM, Nature Phys. N&V 2013



CZ CZ |+>|0>|+>=|+>|0>|+>

CZ CZ |+>|+>|+> = |G>

2. Slightly quantum user



If she passes the stabilizer test,

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

No i.i.d. assumption is required!
(quantum de Finetti, Serfling bound)

Theory:
Hayashi and TM, PRL 2015
Takeuchi and TM, PRX 2018

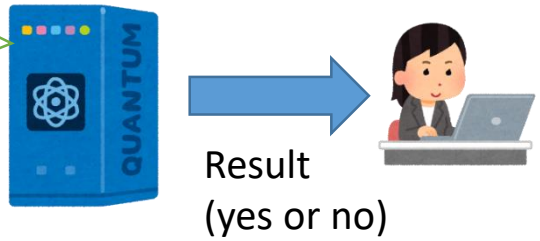
Experiment:
Greganti, Roehsner, Barz, TM, and Walther, NJP 2016

2. Post hoc verification

Fitzsimons, Hajdusek, and TM, PRL 2018

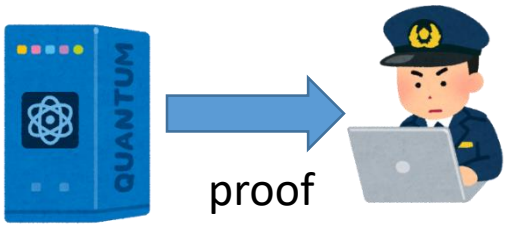
L in BQP

$x \in L$ or $x \notin L$



Result
(yes or no)

10 years later..



proof

Correctness of QC can be checked in the post hoc way!

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

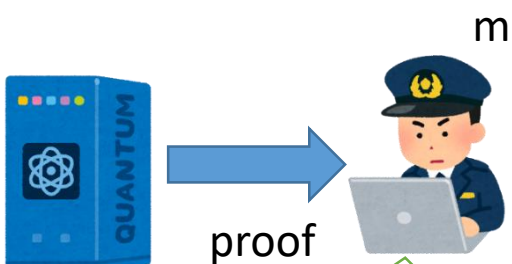
If x is in L
There exists |H> such that <H|H|H> < a
For any |psi>, <psi|H'|psi> >b

If x is not in L
There exists |H'> such that <H'|H'|H'> < a
For any |psi>, <psi|H|psi> >b

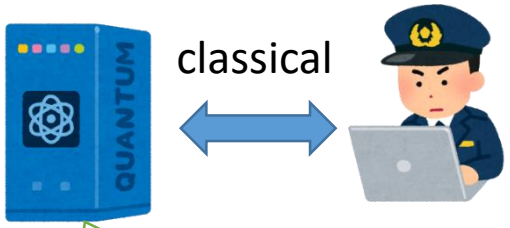
Measurement of energy can be done with single-qubit measurements!
[TM, Nagaj, Schuch, PRA2016]

3. Computational security

If LWE is hard for QC, quantum computing is classically verifiable
[arXiv:1804.01082 Mahadev]



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



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

4. IP=PSPACE

BQP $\subseteq$ PSPACE =IP

Quantum computing is classically verifiable if the server is #P

If we can make #P server to BQP server, the open problem is solved!

It does not seem to be easy to modify the sum check protocol so that the prover is BQP

At least, postBQP prover is possible [Aharonov and Green, arXiv:1710.09078]

5. Specific problems

1. Simon, Shor: trivially classically verifiable

2. Recursive Fourier sampling [McKague, Chicago J. 2012]

3. Order of solvable groups [Le Gall, TM, Nishimura, and Takeuchi, arXiv:1805.03385]

4. Second level of Fourier hierarchy [TM, Takeuchi, and Nishimura, arXiv:1711.10605]

Several problems in BQP are known to be classically verifiable

6. Rational proof system

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

If $x \in L$ then b=1

If $x \notin L$ then b=0

BQP server

b

$ (b)

BPP verifier

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

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!

TM and Nishimura, arXiv:1804.08868

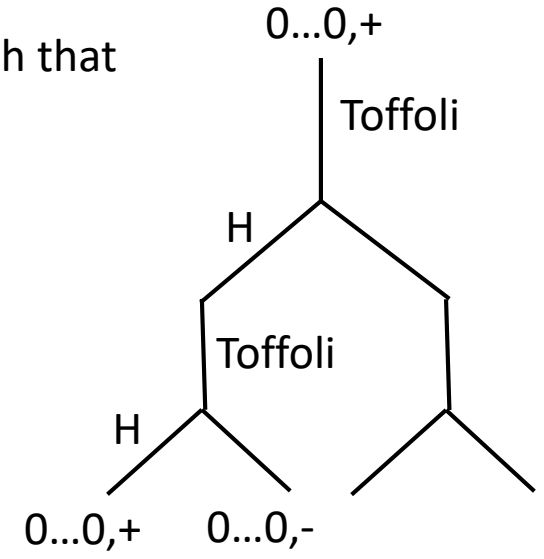
Assume L is in BQP. Then there exists poly-time quantum circuits W such that

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

We assume that W consists of only Hadamard and Toffoli

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

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



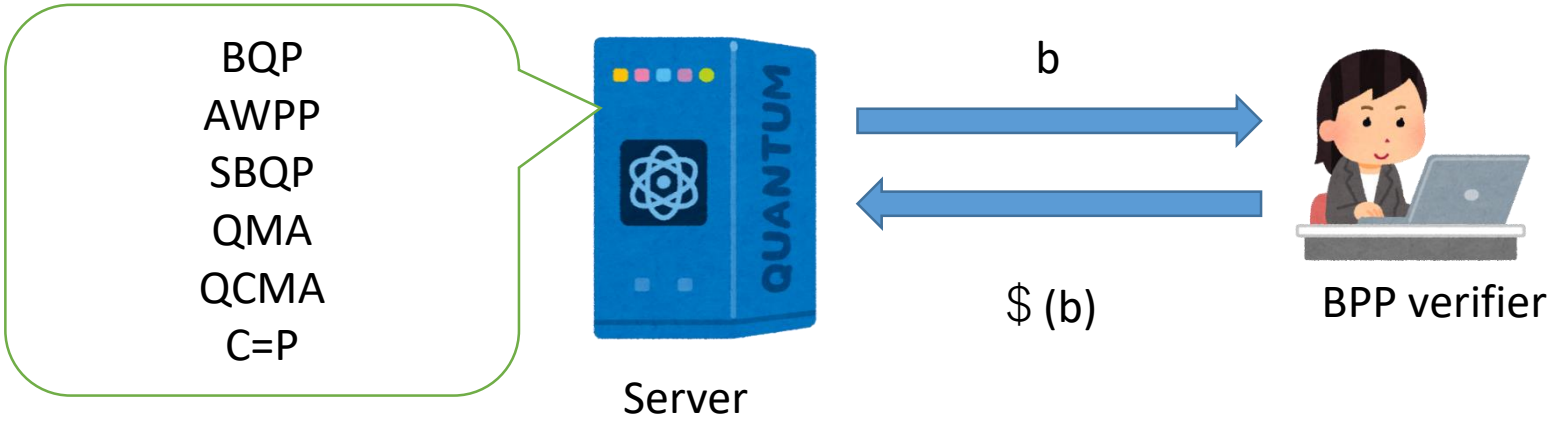
A: number of accepting paths
R: number of rejecting paths
h: number of Hadamard gates in W

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



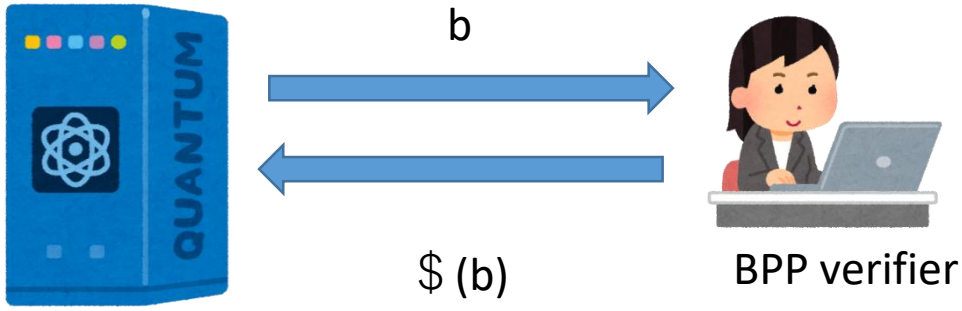
Simulate NDTM of GapP function probabilistically

Extra factors are renormalized into the reward.

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

TM and Nishimura, arXiv:1804.08868

Reward must be exponentially large



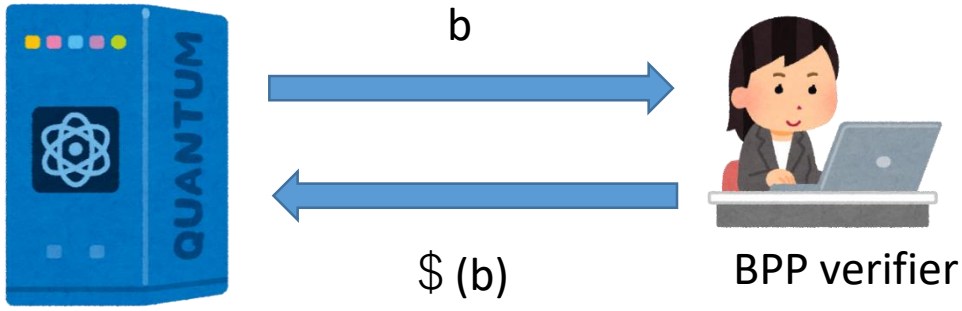
$$\$ = O(\sqrt{2^h})$$

Unfortunately, it is unavoidable unless BQP=BPP

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

If |$(b,w)|<poly, the BPP verifier can estimate <$>_b by herself
→BQP is in BPP!

Open problem



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

Can we make |$|<const?

One possible approarch: consider multiple rounds

END