Non-interactive classical verification of quantum computation

Gorjan Alagic

Andrew M. Childs

Alex B. Grilo

Shih-Han Hung

Joint Center for Quantum Information and Computer Science

University of Maryland

NIST

CWI Centrum Wiskunde & Informatica

QuSoft

QCrypt 2020 arXiv:1911.08101

Verifiable quantum advantage

nature

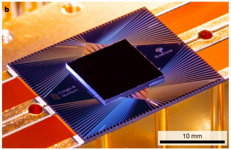
Article | Published: 23 October 2019

Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, […] John M. Martinis

Nature **574**, 505–510(2019) | Cite this article

742k Accesses | **246** Citations | **6011** Altmetric | Metrics



Verifiable quantum advantage

nature

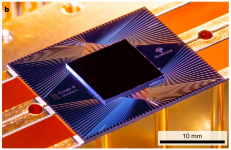
Article | Published: 23 October 2019

Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, […] John M. Martinis

Nature **574**, 505–510(2019) | Cite this article

742k Accesses | **246** Citations | **6011** Altmetric | Metrics



When a quantum cloud is available for remote access...

Verifiable quantum advantage

nature

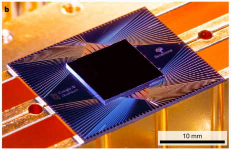
Article | Published: 23 October 2019

Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, […] John M. Martinis

Nature **574**, 505–510(2019) | Cite this article

742k Accesses | **246** Citations | **6011** Altmetric | Metrics



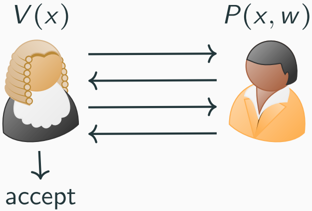
When a quantum cloud is available for remote access...

How do you know if you can trust it via classical communication (e.g., email messages)?

Interactive proofs/arguments

An interactive proof (or argument) system for language L is a protocol which is both complete and sound.

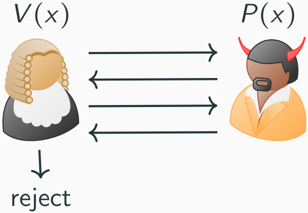
Completeness: for $x \in L_{yes}$,



Interactive proofs/arguments

An interactive proof (or argument) system for language L is a protocol which is both complete and sound.

Soundness: for $x \in L_{no}$,



Interactive proofs/arguments

An interactive proof (or argument) system for language L is a protocol which is both complete and sound.

It is sometimes desirable that the interaction conveys no information about the witness.

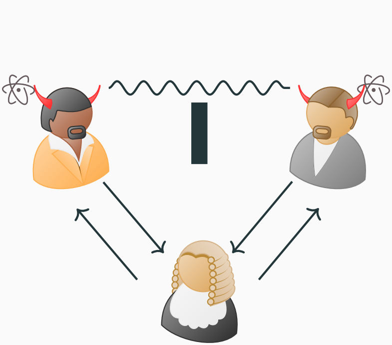
Zero knowledge: there exists a simulator $\mathcal{S}$ who outputs an indistinguishable view.

$V(x)$ $\qquad\qquad$ $P(x, w)$

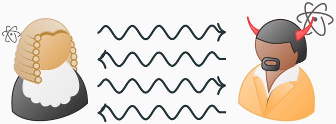
$$\approx \qquad \mathcal{S}(V, x)$$

Testing quantum computers

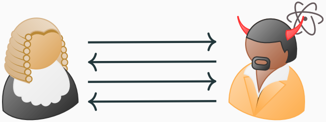
How do we classically verify quantum computers when classical simulation is impossible?



Multiprover interactive proofs with pre-shared entanglements. [RUV13, M16, GKW15, HPDF15, FH15, NV17, CGJV19, G19]



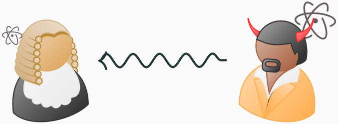
Interactive proof systems with a limited quantum verifier. [B18, ABEM17, MHF18]



$\leq$ LWE

Interactive arguments with a bounded quantum prover. [M18]

An XZ verification protocol for BQP/QMA



Verifier(H):

- measures ρ in X or Z bases, and checks the parity of 2 qubits.

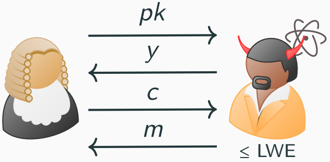
Prover(H):

- prepares the ground state ρ and sends it.

For this approach to work [MHF18],

- the ground state energy of Hamiltonian $H = \sum_i p_i \Pi_i$ is either $\leq a$ or $\geq b$ with $(b - a) > n^{-c}$;
- for every problem L in BQP there is a corresponding Hamiltonian for every instance;
- for QMA, the prover is given access to a quantum witness.

The Mahadev protocol



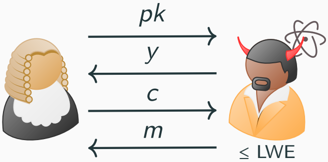
Assuming LWE is hard against quantum adversaries, there is a 4-message protocol for BQP. [M18]

- Verifier publicizes the key pk, and keeps sk secret;
- tosses a random coin c;
- checks $m = (b, x)$,
  - if $c = 0$, $f_{pk}(b, x) = y$;
  - if $c = 1$, the decryption of b or y is accepted to the XZ verification protocol.

- Prover prepares state $|\Psi\rangle = \sum_b \alpha_b |b\rangle|x\rangle|f_{pk}(b, x)\rangle$ and performs partial measurement;
- measures $|\psi_y\rangle$
  - if $c = 0$, in Z basis;
  - if $c = 1$, in X basis;

to get m.

The Mahadev protocol



Assuming LWE is hard against quantum adversaries, there is a 4-message protocol for BQP. [M18]

For this protocol to work,

- The key pairs (pk, sk) encode the bases.
- The function f_{pk} is either 2-to-1 or 1-to-1.
- Hard to prepare the preimage superposition for a fixed y without sk.

There exists an instantiation based on plain LWE. [M18]

The soundness error is constant.

Overview of our protocols

Overview of our protocols

Question

Can quantum computation be certified with a single message, up to instance-independent preprocessing?

Overview of our protocols

Question

Can quantum computation be certified with a single message, up to instance-independent preprocessing?

Question

Can certified quantum computation be performed in zero knowledge?

Overview of our protocols

Question

Can quantum computation be certified with a single message, up to instance-independent preprocessing?

Question

Can certified quantum computation be performed in zero knowledge?

Our contributions:

Overview of our protocols

Question

Can quantum computation be certified with a single message, up to instance-independent preprocessing?

Question

Can certified quantum computation be performed in zero knowledge?

Our contributions:

Overview of our protocols

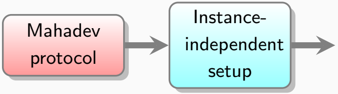
Question

Can quantum computation be certified with a single message, up to instance-independent preprocessing?

Question

Can certified quantum computation be performed in zero knowledge?

Our contributions:



Overview of our protocols

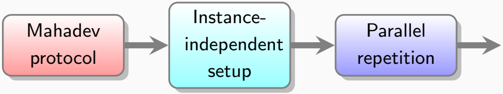
Question

Can quantum computation be certified with a single message, up to instance-independent preprocessing?

Question

Can certified quantum computation be performed in zero knowledge?

Our contributions:



Overview of our protocols

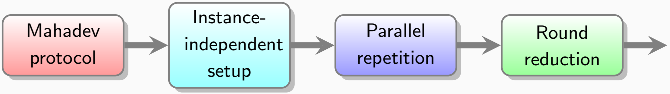
Question

Can quantum computation be certified with a single message, up to instance-independent preprocessing?

Question

Can certified quantum computation be performed in zero knowledge?

Our contributions:



Overview of our protocols

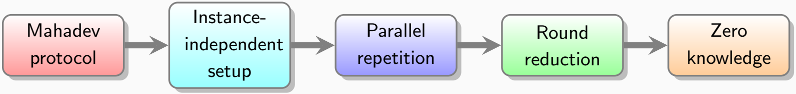
Question

Can quantum computation be certified with a single message, up to instance-independent preprocessing?

Question

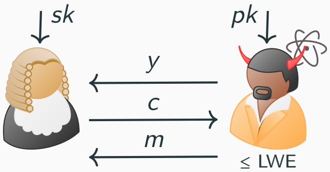
Can certified quantum computation be performed in zero knowledge?

Our contributions:



Instance independent setup

Instance independent setup

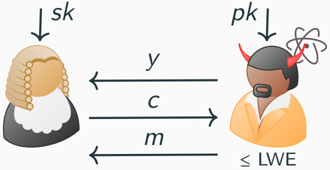


Theorem

The key sampling can be preprocessed prior to verification.

Proof.

Instance independent setup



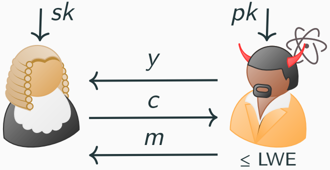
Theorem

The key sampling can be preprocessed prior to verification.

Proof.

- Sample bases S randomly and the keys according to the bases.

Instance independent setup



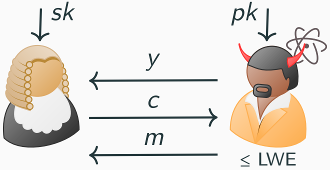
Theorem

The key sampling can be preprocessed prior to verification.

Proof.

- Sample bases S randomly and the keys according to the bases.
- V samples the real bases S' according to the Hamiltonian.

Instance independent setup



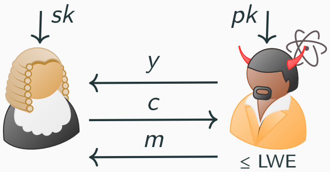
Theorem

The key sampling can be preprocessed prior to verification.

Proof.

- Sample bases S randomly and the keys according to the bases.
- V samples the real bases S' according to the Hamiltonian.
- If $S \neq S'$, the verifier accepts; otherwise run the same verification protocol as before.

Instance independent setup



Theorem

The key sampling can be preprocessed prior to verification.

Proof.

- Sample bases S randomly and the keys according to the bases.
- V samples the real bases S' according to the Hamiltonian.
- If $S \neq S'$, the verifier accepts; otherwise run the same verification protocol as before.
- Since the Hamiltonian is 2-local, with probability $1/4$ they match $\Rightarrow$ the gap decreases by a factor of $1/4$.

A parallel repetition theorem

Hardness amplification

Given a protocol Π with small completeness-soundness gap,
two possibilities to amplify the gap:

Hardness amplification

Given a protocol Π with small completeness-soundness gap, two possibilities to amplify the gap:

- Sequential repetition
  Run Π sequentially, accept if many rounds are accepted.
  ☺ Always amplifies the gap.
  ☹ Requires more interaction.

Hardness amplification

Given a protocol Π with small completeness-soundness gap, two possibilities to amplify the gap:

- Sequential repetition
  Run Π sequentially, accept if many rounds are accepted.
  ☺ Always amplifies the gap.
  ☹ Requires more interaction.

- Parallel repetition (PR)
  Run Π in parallel, accept if many copies are accepted.
  ☺ Additional interaction is not required.
  ☹ Not always reduce the soundness error.

Hardness amplification

Given a protocol Π with small completeness-soundness gap,
two possibilities to amplify the gap:

- Sequential repetition
  Run Π sequentially, accept if many rounds are accepted.
  ☺ Always amplifies the gap.
  ☹ Requires more interaction.

- Parallel repetition (PR)
  Run Π in parallel, accept if many copies are accepted.
  ☺ Additional interaction is not required.
  ☹ Not always reduce the soundness error.
  - There exists a protocol for which the soundness error stays the same using two-fold PR.

A parallel repetition theorem

Theorem

The soundness error of a k-fold protocol is $2^{-k} + \epsilon$ *for negligible* ϵ.

Proof.

[1] In the sense that $\mathcal{P}$ is quantum efficient and only knows the public keys.

A parallel repetition theorem

Theorem

The soundness error of a k-fold protocol is $2^{-k} + \epsilon$ *for negligible* ϵ.

Proof.

- $\mathcal{P}$ prepares a quantum state ρ_{pk}, fixed by $\mathcal{V}$ by requesting a partial measurement.

[1] In the sense that $\mathcal{P}$ is quantum efficient and only knows the public keys.

A parallel repetition theorem

Theorem

The soundness error of a k-fold protocol is $2^{-k} + \epsilon$ *for negligible* ϵ.

Proof.

- $\mathcal{P}$ prepares a quantum state ρ_{pk}, fixed by $\mathcal{V}$ by requesting a partial measurement.
- After the challenges $c = (c_1, \ldots, c_k)$ are sent, $(\mathcal{P}, \mathcal{V})$ effectively applies an arbitrary[1] binary measurement $\{M_{sk,s,c}, \mathbb{I} - M_{sk,s,c}\}$. These projectors are nearly orthogonal w.r.t. ρ_{pk}

$$\forall a \neq b, \underset{pk,sk,s}{\mathbb{E}}[\mathrm{tr}(\rho_{pk}\{M_{sk,s,a}, M_{sk,s,b}\})] \leq \mathrm{negl}(n).$$

Otherwise, there exists an adversary who wins the single-copy protocol w.p. close to 1.

[1] In the sense that $\mathcal{P}$ is quantum efficient and only knows the public keys.

A parallel repetition theorem

Theorem

The soundness error of a k-fold protocol is $2^{-k} + \epsilon$ for negligible ϵ.

Proof.

- $\mathcal{P}$ prepares a quantum state ρ_{pk}, fixed by $\mathcal{V}$ by requesting a partial measurement.
- After the challenges $c = (c_1, \ldots, c_k)$ are sent, $(\mathcal{P}, \mathcal{V})$ effectively applies an arbitrary[1] binary measurement $\{M_{sk,s,c}, \mathbb{I} - M_{sk,s,c}\}$. These projectors are nearly orthogonal w.r.t. ρ_{pk}

  $$\forall a \neq b, \underset{pk,sk,s}{\mathbb{E}}[\mathrm{tr}(\rho_{pk}\{M_{sk,s,a}, M_{sk,s,b}\})] \leq \mathrm{negl}(n).$$

  Otherwise, there exists an adversary who wins the single-copy protocol w.p. close to 1.
- Thus any prover can win at most a single challenge (out of 2^k possibilities).

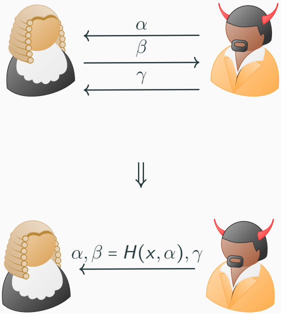
[1] In the sense that $\mathcal{P}$ is quantum efficient and only knows the public keys.

Round reduction

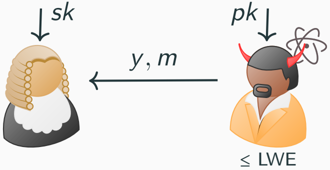
The Fiat-Shamir paradigm

The Fiat-Shamir transform turns a Σ-protocol (3-message, public-coin), into a non-interactive protocol.

In the QROM, FS is secure with an $O(q^2)$ loss against a q-query adversary to the random oracle.



Round reduction for BQP verification



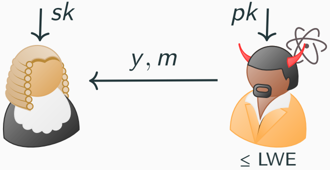
Theorem

The FS-transformed BQP verification has negligible soundness error.

Proof.

- Assuming the existence of an FS-breaking adversary $\mathcal{A}$, there must be a noticeable fraction of bad keys (pk^*, sk^*).

Round reduction for BQP verification



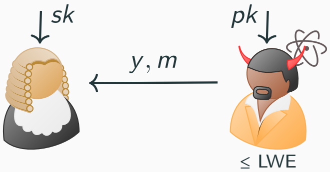
Theorem

The FS-transformed BQP verification has negligible soundness error.

Proof.

- Assuming the existence of an FS-breaking adversary $\mathcal{A}$, there must be a noticeable fraction of bad keys (pk^*, sk^*).
- Conditioned on these keys, $\mathcal{A}(pk^*)$ is a FS-breaking adversary to a transformed Σ-protocol.

Round reduction for BQP verification



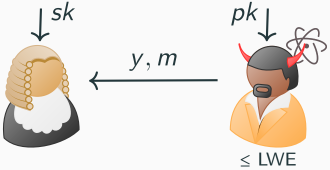
Theorem

The FS-transformed BQP verification has negligible soundness error.

Proof.

- Assuming the existence of an FS-breaking adversary $\mathcal{A}$, there must be a noticeable fraction of bad keys (pk^*, sk^*).
- Conditioned on these keys, $\mathcal{A}(pk^*)$ is a FS-breaking adversary to a transformed Σ-protocol.
- There exists an adversary $\mathcal{B}(pk^*)$ who wins the Σ-protocol w.p. arbitrarily close to 1, using the same reduction as [DFMS19].

Round reduction for BQP verification



Theorem

The FS-transformed BQP verification has negligible soundness error.

Proof.

- Assuming the existence of an FS-breaking adversary $\mathcal{A}$, there must be a noticeable fraction of bad keys (pk^*, sk^*).
- Conditioned on these keys, $\mathcal{A}(pk^*)$ is a FS-breaking adversary to a transformed Σ-protocol.
- There exists an adversary $\mathcal{B}(pk^*)$ who wins the Σ-protocol w.p. arbitrarily close to 1, using the same reduction as [DFMS19].
- The adversary $\mathcal{B}$ breaks the original protocol.

Classical NIZK for BQP/QMA

Making the protocol zero-knowledge

Theorem

There exists a classical NIZK for QMA in the QROM, assuming the existence of a circularly secure FHE and a NIZK for NP.

Sketch of construction.

Making the protocol zero-knowledge

Theorem

There exists a classical NIZK for QMA in the QROM, assuming the existence of a circularly secure FHE and a NIZK for NP.

Sketch of construction.

- In the setup phase, the prover gets the encryption of sk, which is part of the instance to some NP relation.

Making the protocol zero-knowledge

Theorem

There exists a classical NIZK for QMA in the QROM, assuming the existence of a circularly secure FHE and a NIZK for NP.

Sketch of construction.

- In the setup phase, the prover gets the encryption of sk, which is part of the instance to some NP relation.
- ☹ The first message is obtained by querying f_{pk} on the witness.
  $\Rightarrow$ Prover encrypts the witness state with quantum one-time pad and commits to the keys.

Making the protocol zero-knowledge

Theorem

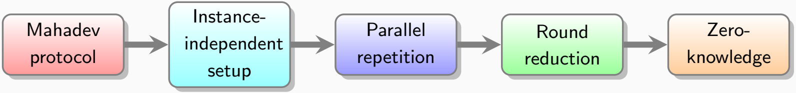
There exists a classical NIZK for QMA in the QROM, assuming the existence of a circularly secure FHE and a NIZK for NP.

Sketch of construction.

- In the setup phase, the prover gets the encryption of sk, which is part of the instance to some NP relation.
- ☹ The first message is obtained by querying f_{pk} on the witness.
  $\Rightarrow$ Prover encrypts the witness state with quantum one-time pad and commits to the keys.
- ☹ The prover gets accepted by sending the openings and the measurement outcomes.
  $\Rightarrow$ Viewing these as the witness to the NP relation.
  $\Rightarrow$ Sending a homomorphically evaluated NIZK proof.

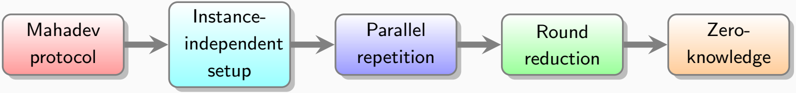
Summary

We showed classical verification of quantum computation can be performed non-interactively and in zero-knowledge.



Summary

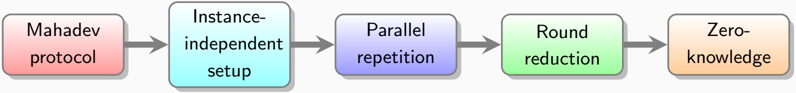
We showed classical verification of quantum computation can be performed non-interactively and in zero-knowledge.



Open questions:

Summary

We showed classical verification of quantum computation can be performed non-interactively and in zero-knowledge.

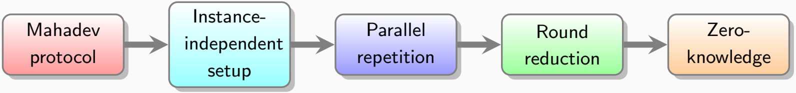


Open questions:

- Can we prove security when the oracle is instantiated with a concrete hash function?

Summary

We showed classical verification of quantum computation can be performed non-interactively and in zero-knowledge.

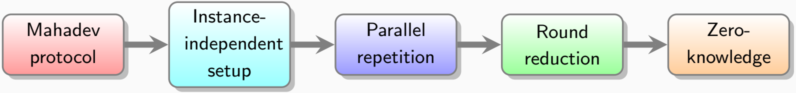


Open questions:

- Can we prove security when the oracle is instantiated with a concrete hash function?
- A parallel repetition theorem for any quantum prover interactive arguments?

Summary

We showed classical verification of quantum computation can be performed non-interactively and in zero-knowledge.



Open questions:

- Can we prove security when the oracle is instantiated with a concrete hash function?
- A parallel repetition theorem for any quantum prover interactive arguments?
- Simpler NIZK arguments for BQP/QMA?