Delegating quantum computations
1. Problem formulation
2. Overview of existing approaches
3. An open question
Problem formulation
Problem formulation

- Verifier has quantum computation $C$
- Multiple rounds of interaction with quantum device
- Verifier returns $(\text{flag}, b)$ s.t. $\text{flag} \in \{\text{acc}, \text{rej}\}$ and $b \in \{0, 1\}$
- Goal: Whenever $\Pr(\text{flag} = \text{acc})$ is non-negligible,

$$\Pr( b = 1 | \text{flag} = \text{acc}) \approx \Pr( C \text{ returns } 1 \text{ on input } |0^n\rangle)$$
An example

\[ |0\rangle \xrightarrow{\text{H}} b = 0 \text{ w.p. } 50\% \]
\[ b = 1 \text{ w.p. } 50\% \]

“description of circuit $C$”

“I got $b = 0$”

Really??
Join the IBM Q Experience Community

The IBM Q Experience Community brings together researchers and quantum enthusiasts to share, connect and collaborate.

If you want to interact within the community, you need a username.

Set your username

IBM Q Awards Contest Program

Submit a contribution to the IBM Q Awards! The IBM Q Awards are a series of prizes for professors, lecturers and students who use the IBM Q Experience and QISKit...

21 comments
4.9k views
15 likes

IBM Q Awards | IBM QE | QISKit | quantum software | compiling

Posted 10 months ago | Last comment by yy387 10 days ago

Results in hex format?

Does anyone else find the sudden change of presenting results in hex and not binary counterintuitive? I'm sure everyone in the field of Q1 is more familiar with...

1 comment
9 views

XA | xavierlin | Posted a day ago | Last comment by constantine 3 hours ago

Software

Quick links
FAQ
Beginner's Guide
Full User Guide

Tags

Top Users (Last week)

Courses
Experiment #20181220105605

Device: ibmqx4

Quantum State: Computation Basis

Quantum Circuit

OPENQASM 2.0

1. include "qelib1.inc"
2. qreg q[5];
3. crreg c[5];
4. h q[2];
5. measure q[2] -> c[2];
An example

\[ |0\rangle \xrightarrow{\text{H}} b = 0 \text{ w.p. } 50\% \]
\[ b = 1 \text{ w.p. } 50\% \]

“description of circuit C”

Really??
Repeat and collect statistics?
Run some tests?

© IBM
Aside: benchmarking

Sequentially test gate by injecting well-characterized states and collecting output statistics

- Requires access to inner workings of device
- Trusted state preparation and/or measurement
- Gates are not allowed to be “malicious”, e.g. i.i.d. behavior is generally assumed
- Ineffective at large scales

\[ |0\rangle, |1\rangle, |+\rangle, |-\rangle \]
Testing quantum mechanics at scale

- Quantum mechanics untested at large scales
- Is there a limit to the exponential scaling of quantum devices?
Some other reasons to care

- Near-term demonstration of quantum advantage
  - Can verifiability be baked in current proposals?
- Cryptographic techniques
  - What modes of encryption allow transversal (homomorphic) computation?
  - Can they be combined with authentication?
- Models of computation & fault-tolerance
  - Do small nodes in a quantum network create fault-tolerance bottlenecks?
- Complexity theory
  - What is the expressive power of bounded-prover interactive proofs?
- Foundations
  - Are there analogues of the Bell inequalities without locality assumptions?
Prelude: Definitions
Semi-formal definition

A delegation protocol for quantum computations is:

A description of a (classical or quantum) polynomial-time verifier, that takes as input a quantum circuit $C$ of size $|C| \leq n$, interacts with a quantum prover, and returns a pair $(flag, b)$ such that:

- **(Completeness)** There exists a (quantum, poly-time) prover $P$ such that
  \[
  \Pr(flag = acc) \approx 1 \quad \text{AND} \quad \Pr(b = 1) \approx \Pr(C \text{ returns } 1 \text{ on input } |0^n\rangle)
  \]

- **(Soundness)** For any prover $P^*$ such that $\Pr(flag = acc)$ is non-negligible,
  \[
  \Pr(b = 1 |flag = acc) \approx \Pr(C \text{ returns } 1 \text{ on input } |0^n\rangle)
  \]

- **(Blindness)** For any prover $P^*$, $\text{View}_P(V_n(C) \leftrightarrow P^*)$ does not depend on $C$
“Stand-alone” definitions can fail! Example:

**Protocol for testing if formula $\varphi = (x_1 \lor \overline{x_3} \lor x_5) \land (\cdots)$ is satisfiable**

1. Prover sends assignment $x = (x_1, \ldots, x_n)$
2. Verifier checks that $x$ satisfies $\varphi$

This protocol is blind (prover learns nothing about $\varphi$) & verifiable

“Attack”: Prover sends a uniformly random assignment

- Learns information about $\varphi$ from verifier’s accept/reject decision
- Protocol is not composable

Composable security: ideal-world/real-world paradigm
Parameters

Completeness: Probability of accepting honest prover. This will always be $\approx 1$

Soundness: Max. distinguishing ability between real-world/ideal-world.

Ideally, exponentially small in $n$.

Verifier complexity: Ideally, classical polynomial-time.

Limited quantum capability may be acceptable.

Prover complexity: Quantum polynomial-time. Ideally $\approx \text{runtime}(C)$.

Interaction: Minimize number of rounds + total communication

Input size: $n = \text{number of qubits of circuit } C$

$|C| = \text{number of gates}$
Overview of existing approaches
Models of computation

**Circuit model**
- **Input:** circuit = sequence of gates acting on \( n \) qubits
- **Goal:** determine value of output qubit, on input \( |0\rangle \)

**Measurement-based**
- **Input:** adaptive sequence of single-qubit measurements on resource state (e.g. “cluster state”)
- **Goal:** determine value of output qubit

**Hamiltonian model**
- **Input:** local Hamiltonian w. efficiently preparable ground state
- **Goal:** estimate ground state energy

\[
H = H_{in} + H_{clock} + H_{prop} + H_{out}
\]
Models for black-box verification

Challenge: Use minimal resources to verify complex quantum computation
Models for black-box verification

[Childs’05] Blind delegation
- Verifier has constant-size quantum computer and can only perform single-qubit Pauli gates
- Many-round quantum interaction
- Blind but not verifiable

Where are the qubits? Honest-but-curious model
Models for black-box verification

“Prepare-and-send” protocols:
- Verifier has ability to prepare & send $O(1)$ qubits at a time
- Many-round classical interaction
  - [ABOE] *Circuit model*, uses authentication codes
  - [BFK] *Measurement-based model*, uses traps
- Both protocols are blind + verifiable

Where are the qubits? The verifier authenticates them
Models for black-box verification

[Reichardt-Unger-Vazirani’12]

Two-prover protocols:

• Verifier is classical
• Many-round classical interaction with two isolated provers
• Verifier uses Bell tests to do state & process tomography
• Protocol is blind + verifiable

Where are the qubits? Bell tests $\rightarrow$ EPR pairs $\rightarrow$ qubits
Models for black-box verification

[Morimae-Fuji’13, Morimae-Fitzsimons’16]
“Receive & measure” protocols:
• Verifier has ability to receive & measure constant qubits
• [MNS’16] Measurement-based model, protocol is blind & verifiable
• [MF’16] Hamiltonian model, protocol is verifiable but not blind

Where are the qubits? The verifier measures them
Models for black-box verification

[Mahadev’18] “Commit & Reveal” protocols:

- Verifier is classical
- *Hamiltonian model*: protocol is not blind
- Verifiability assumes prover does not break post-quantum crypto

*Where are the qubits?*  
*Encoded using the crypto*
Building up

authentication + transversal gates

Self-testing

Self-testing

qubit commitment protocol

use crypto

run Bell tests
Some experiments


[Huang et al. 2017] Thousands of Bell tests certify factorization of number 15.
An open question
An open question

- Verifier is classical polynomial-time
- Communication channel is classical
- Verifier wants to determine $\Pr(C|0) = 1$
An open question

- Problems with efficient classical verification?
- MA = class of problems with efficient (probabilistic) verification
- Any problem in MA \( \cap \) BQP has an efficiently verifiable solution
- Factoring, Graph Isomorphism

- IP = class of problems with efficient (probabilistic, interactive) verification
- IP Prover may not be efficient! Needs to compute exponentially large sums

IP = PSPACE

\[ \text{Recursive Fourier sampling} \]
Interactive proofs for BQP

• Feynman path integral: \( \Pr(C|0\rangle = 1) \) is (square of) summation over exponentially many paths

\[
\sum_{path=(x_1, \ldots, x_T)} \text{amplitude}(x_1, \ldots, x_T)
\]

\[
\left| 0 \right\rangle \quad H \quad Z \quad H \quad b = 1
\]

\[x_1 \quad x_2 \quad x_3 \quad x_4\]

• Amplitude of individual path is easy to compute

\[
\text{amplitude}(0,1,1,0) = 1 \cdot \frac{1}{\sqrt{2}} \cdot (-1) \cdot \frac{1}{\sqrt{2}} = -\frac{1}{2}
\]

• Amplitude is multilinear polynomial in \( x_1, \ldots, x_T \)
Interactive proofs for BQP

- Given $P \in \mathbb{F}_q[X_1, \ldots, X_T]$ multilinear, compute $\sum_{x_1, \ldots, x_T \in \{0,1\}} P(x_1, \ldots, x_T)$

\[
\begin{align*}
\sum_z p_T(z) &= S \quad ? \\
\tilde{z}_T &\leftarrow_R \mathbb{F}_q \\
\sum_z p_{T-1}(z) &= p_T(\tilde{z}_T) \quad ? \\
\tilde{z}_{T-1} &\leftarrow_R \mathbb{F}_q \\
p_0 &= P(\tilde{z}_1, \ldots, \tilde{z}_T) \quad ?
\end{align*}
\]
Receive & Measure
Protocols
Receive & Measure protocols

- **MBQC model:**
  - Prover prepares resource state (e.g. cluster state)
  - Verifier either (i) checks stabilizers of resource state
    (ii) implements computation
  - Only needs single-qubit measurements in small number of bases
- **Post-hoc model:**
  - Prover prepares history state of Kitaev Hamiltonian associated with circuit
  - Verifier measures randomly chosen term in Hamiltonian
  - Only needs single-qubit measurements in two bases, but protocol not blind
Circuit-to-Hamiltonian
[Kitaev’99]

- Hamiltonian can be expressed in “XX/ZZ form”:
  
  \[ H \text{ is weighted sum of local terms of the form } X_iX_j \text{ or } Z_iZ_j \]

- Gap \( \delta \) scales as \( 1/|C|^2 \)

- Complexity of preparing ground state of \( H \) scales as complexity of \( C \)
  
  (but may require higher depth)
Post-hoc verifiable delegation

\[ H = H_{\text{in}} + H_{\text{clock}} + H_{\text{prop}} + H_{\text{out}} \]

\[
\Pr(C|0) = 1 \geq \frac{2}{3} \implies \lambda_{\min}(H) \leq a
\]

\[
\Pr(C|0) = 1 \leq \frac{1}{3} \implies \lambda_{\min}(H) \geq a + \delta
\]

- Verifier computes \( H \) from \( C \), sends to prover
- Prover prepares ground state of \( H \)
- Sends to verifier one qubit at a time
- Verifier secretly selects random local term \( h_j = X_{j_1}X_{j_2} \) or \( h_j = Z_{j_1}Z_{j_2} \)
- Measures qubits \( j_1 \) and \( j_2 \) in required basis
- Repeat \( 1/\delta^2 \) times to estimate energy
Running example

\[ |0\rangle \xrightarrow{H} H \left(\frac{1}{2}(X \otimes X + Z \otimes Z)\right) \rightarrow b \]

flip coin \( W \in \{X, Z\} \)

Measure in basis \( W \)
\( \rightarrow b_1 \)

Measure in basis \( W \)
\( \rightarrow b_2 \)

Check: \( b_1 b_2 = +1 \)

\[ |\psi\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \]
Receive & Measure protocols: summary

- One-way quantum communication

- Hamiltonian model requires repetition for gap amplification
  MBQC model requires repetition for resource state testing
  Total communication at least $\sim |C|^3$

Open: protocol with linear communication complexity

- Blind protocols only in MBQC model

- Protocols vulnerable to noise at the verifier

  [GHK’18] give fault-tolerant protocol in Hamiltonian model; not blind

Open: receive & measure fault-tolerant blind delegation
Part II(c): Commit & Reveal
Models for black-box verification

- Verifier “delegates” X and Z measurements to server
- Hurdle: Certify that reported measurement outcomes are obtained from a single underlying \( n \)-qubit state
- Idea: Use cryptography to “commit” prover to fixed \( n \)-qubit state
Committing to a bit

- **Hiding:** $c$ reveals no information about $b$  
  \[ c|_{b=0} \approx c|_{b=1} \]

- **Binding:** For any efficient Bob, and any $c$ such that $\Pr(flag = acc) \geq 0.01$, there is a $b$ such that $\Pr(b^* = b| flag = acc) \geq 0.95$
Claw-free functions

\( f_0, f_1 : \{0,1\}^n \to \{0,1\}^n \) a claw-free pair:

- Both \( f_0 \) and \( f_1 \) are bijections
- For every \( c \) in the range, there is a unique claw: a pair \((r_0, r_1)\) such that \( f_0(r_0) = f_1(r_1) = c \)
- Claws are hard to find: no efficient procedure returns \((r_0, r_1, c)\)
- Can construct based on “Learning with Errors” (LWE) problem
- \( f_0, f_1 \) are noisy multiplication by matrix \( A \):

\[
\begin{align*}
    f_0(x) &\approx A x + e, \\
    f_1(x) &\approx A(x - s) + e' \\
\end{align*}
\]

\( r_1 \approx r_0 - s \)
Committing to a bit

\((f_0, f_1): \{0,1\}^n \rightarrow \{0,1\}^n\) a claw-free pair

\[c = f_b(r)\]

\[d = (b, r)\]

Check \(f_b(r) = c\)

Return \(b\)

- **Perfectly hiding:** Any \(c\) has exactly one preimage under each function
- **Computationally binding:**
  
  If \(\Pr(b^* = 0|flag = acc) > 0.05\) and \(\Pr(b^* = 1|flag = acc) > 0.05\)
  
  then run Bob 100 times on \(c\) to find a claw
Committing to a qubit

- **Hiding:** \( c \) reveals no information about \( |\psi\rangle \)

- **Binding:** For any efficient Bob and \( c \) such that \( \Pr(flag = acc) \geq 0.01 \), there is a \( \rho \) such that \( a_Z \approx \Tr(Z\rho) \) and \( a_X \approx \Tr(X\rho) \)

\[
|\psi\rangle = \alpha |0\rangle + \beta |1\rangle
\]

\[
|R\rangle = \frac{1}{\sqrt{2^n}} \sum_{r \in \{0,1\}^n} |r\rangle
\]
Committing to a qubit

\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \]

\[ c = \text{com}(|\psi\rangle, |R\rangle) \]

\[ |R\rangle = \frac{1}{\sqrt{2^n}} \sum_{r \in \{0,1\}^n} |r\rangle \]

\[ |\psi\rangle \otimes |R\rangle \otimes |0^n\rangle = (\alpha |0\rangle + \beta |1\rangle) \otimes \frac{1}{\sqrt{2^n}} \sum_{r \in \{0,1\}^n} |r\rangle \otimes |0^n\rangle \]

\[ \text{CTL-}f \]

\[ \rightarrow \frac{\alpha}{\sqrt{2^n}} \sum_{r \in \{0,1\}^n} |0\rangle|r\rangle|f_0(r)\rangle + \frac{\beta}{\sqrt{2^n}} \sum_{r \in \{0,1\}^n} |1\rangle|r\rangle|f_1(r)\rangle \]

meas. last register

\[ \rightarrow (\alpha |0\rangle|r_0\rangle + \beta |1\rangle|r_1\rangle) \otimes |c\rangle \]
Committing to a qubit

\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \]

\[ c = \text{com}(|\psi\rangle, |R\rangle) \]

\[ |R\rangle = \frac{1}{\sqrt{2^n}} \sum_{r \in \{0,1\}^n} |r\rangle \]

Diagram:
- Initial state: \( |0\rangle \rightarrow |\psi\rangle \)
- Commit: \( |\psi\rangle \rightarrow |1\rangle \otimes |r_1\rangle \)
- Commit: \( |0\rangle \otimes |r_0\rangle \)
Committing to a qubit

\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \]

\[ |R\rangle = \frac{1}{\sqrt{2^n}} \sum_{r \in \{0,1\}^n} |r\rangle \]

\[ c = \text{com}(|\psi\rangle, |R\rangle) \]

\[ d_Z = \text{Z-reveal}(b, |R\rangle) \]

\[ |\psi\rangle \otimes |R\rangle \otimes |0^n\rangle = (\alpha |0\rangle + \beta |1\rangle) \otimes \frac{1}{\sqrt{2^n}} \sum_{r \in \{0,1\}^n} |r\rangle \otimes |0^n\rangle \]

\[ \text{CTL-f} \rightarrow \frac{\alpha}{\sqrt{2^n}} \sum_{r \in \{0,1\}^n} |0\rangle |r\rangle |f_0(r)\rangle + \frac{\beta}{\sqrt{2^n}} \sum_{r \in \{0,1\}^n} |1\rangle |r\rangle |f_1(r)\rangle \]

meas. last register

\[ \rightarrow (\alpha |0\rangle |r_0\rangle + \beta |1\rangle |r_1\rangle) \otimes |c\rangle \]

- **Hiding**: \( c \) reveals no information about \( |\psi\rangle \)
- **Z-reveal**: Bob measures in computational basis and returns \( d_Z = (b, r_b) \)
  
  Alice checks \( f_b(r_b) = c \) and returns “decoded bit” \( a_Z = b \)
Committing to a qubit

\[ |\psi\rangle = \alpha|0\rangle + \beta|1\rangle \]

\[ |R\rangle = \frac{1}{\sqrt{2^n}} \sum_{r \in \{0,1\}^n} |r\rangle \]

\[ c = com(|\psi\rangle, |R\rangle) \]

\[ d_X = X\text{-}reveal(b, |R\rangle) \]

\[
\begin{align*}
(a|0\rangle|r_0\rangle + \beta|1\rangle|r_1\rangle) &\quad \xrightarrow{I \otimes H^\otimes n} \quad \frac{1}{\sqrt{2^n}} \sum_{t \in \{0,1\}^n} (\alpha(-1)^{t \cdot r_0}|0\rangle + \beta(-1)^{t \cdot r_1}|1\rangle) \otimes |t\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{t \in \{0,1\}^n} (-1)^{t \cdot r_0} Z^{t \cdot r_0 \oplus t \cdot r_1} |\psi\rangle \otimes |t\rangle
\end{align*}
\]

- \textit{X-reveal}: Bob measures in Hadamard basis and returns \( d_X = (u, t) \)
  Alice returns “decoded bit” \( a_X = u \oplus (t \cdot r_0 \oplus t \cdot r_1) \)
Commit & Reveal protocol

[Mahadev’18]

\[ H = \sum_{(j_1,j_2)} \alpha_{j_1j_2} (X_{j_1}X_{j_2} + Z_{j_1}Z_{j_2}) \]

\[ \Pr(C|0) = 1 \geq 2/3 \implies \lambda_{\text{min}}(H) \leq a \]

\[ \Pr(C|0) = 1 \leq 1/3 \implies \lambda_{\text{min}}(H) \geq a + \delta \]

- Verifier computes \( H \) from \( C \), sends to prover
- Prover prepares ground state of \( H \)
- Prover individually commits to each qubit by sending \( c_1, \ldots, c_n \)
- Verifier secretly selects random local term \( h_j = X_{j_1}X_{j_2} (Z_{j_1}Z_{j_2}) \)
- Executes \( X(Z) \)-reveal phase with prover
- Records decoded outcomes \( a_{X_{j_1}X_{j_2}} (a_{Z_{j_1}Z_{j_2}}) \)
- Repeat \( 1/\delta^2 \) times to estimate energy
Running example

\[ H = -\frac{1}{2} (X \otimes X + Z \otimes Z) \]

flip coin \( W \in \{X, Z\} \)

prepare \( \left| \psi \right> = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \)

commitments \( c, c' \)

run commitment procedure:
\[ \frac{1}{\sqrt{2}} (|0, r_0\rangle |0, r_0'\rangle + |1, r_1\rangle |1, r_1'\rangle) \]

Check:
\[ f_b(r) = f'_b'(r') \]
\[ a_X = f_b(r) \oplus t \cdot r_1 \]
\[ a'_X = f'_b'(r') \oplus t' \cdot r'_1 \]

Measure \( X \)

Set \( a_X, a'_X \)

Record \( b_b a'_X \)

Repeat \( 1/\delta^2 \) times to estimate energy
Commit & Reveal protocol: summary

- Hamiltonian model: protocol is not blind, but can be made blind by combining with quantum FHE
  Open: blind protocol in circuit or MBQC models?

- Complexity: cubic overhead due to Hamiltonian model
  Crypto overhead linear in security parameter

- Soundness guarantee: there exists a state that gives computationally indistinguishable measurement outcomes
  Open: computational assumption, information-theoretic guarantee?

- Claw-free function instantiated from learning with errors assumption (LWE)
  Open: more generic construction (e.g. quantum-secure OWF)?
Interactive proofs for BQP

- Any language in BQP has a classical-verifier interactive proof
- Prover needs to compute unphysical quantities
- Cannot be implemented using quantum computer
- [AG’17] give “quantum-inspired” variant of protocol
- Open: protocol with prover less powerful than PostBQP
- Challenge: allow prover to make statistical estimation errors while restricting capacity to cheat
Problem formulation

Ideal functionality for verifiable & blind delegation

\[ b = \begin{cases} C(|0\rangle) & \text{if } e \in \{0,1\} \\ err & \text{if } e = 2 \end{cases} \]

A protocol is verifiable & blind if no malicious party interacting with the honest party can distinguish from an interaction with the ideal functionality.
Models of computation

Circuit model

\[ |0\rangle \rightarrow H \rightarrow b \]

|0\rangle \rightarrow H \rightarrow X \rightarrow Z

Measurement-based model

Hamiltonian model

\[ H = H_{in} + H_{clock} + H_{prop} + H_{out} \]
Protocols for verifiable delegation

- Prepare
- Measure
- Authentication + transversal gates
- Prepare
- Self-testing
- Run Bell tests
- Self-testing
- Self-testing
- Use crypto
- Qubit commitment protocol
- (bounded)
- (local)
Complexity considerations

Input: Circuit $C$, $T$ gates, $n$ qubits. $\epsilon$: distance from ideal functionality

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Computation model</th>
<th>Verifier</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Childs’05</td>
<td>Circuit</td>
<td>$O(1)$</td>
<td>$O(T)$</td>
</tr>
<tr>
<td>ABOE’08</td>
<td>Circuit</td>
<td>$O(\log 1/\epsilon)$</td>
<td>$O(T \log(1/\epsilon))$</td>
</tr>
<tr>
<td>BFK’09</td>
<td>MBQC</td>
<td>$O(1)$</td>
<td>$O(T \log(1/\epsilon))$</td>
</tr>
<tr>
<td>MF’13</td>
<td>MBQC</td>
<td>$O(1)$</td>
<td>$O(T/\epsilon^2)$</td>
</tr>
<tr>
<td>MF’16</td>
<td>Hamiltonian</td>
<td>$O(1)$</td>
<td>$O(T^3 \log(1/\epsilon))$</td>
</tr>
<tr>
<td>CGJV’18</td>
<td>Circuit</td>
<td>classical</td>
<td>$O(T/\epsilon^c)$</td>
</tr>
<tr>
<td>Mahadev’18</td>
<td>Hamiltonian</td>
<td>classical</td>
<td>$O(T^3 \log(1/\epsilon) \log(1/\lambda))$</td>
</tr>
</tbody>
</table>
Thank you

SLIDES:
HTTP://USERS.CMS.CALTECH.EDU/~VIDICK/VERIFICATION.{PPSX,PDF}


[MF’16] Morimae, Nagaj and Schuch. "Quantum proofs can be verified using only single-qubit measurements." arXiv:1510.06789


