Non-local games and verifiable delegation of quantum computation

Alex Bredariol Grilo

joint work with Andrea Coladangelo, Stacey Jeffery and Thomas Vidick
Why verifiably delegate quantum computation?
Why verifiably delegate quantum computation?

- *Superiorita* 😊
Why verifiably delegate quantum computation?

- Superiorita 😊
- But they are expensive 😞
Why verifiably delegate quantum computation?

- *Superiorita 😊*
- But they are expensive 😞
- Online service 😊
Why verifiably delegate quantum computation?

- Superiorita 😊
- But they are expensive 😞
- Online service 😊
- Can a client be sure that she is experiencing a quantum speedup? 😊
Goal: Interactive proof system for BQP where

- the verifier runs poly-time probabilistic computation
- an honest prover runs poly-time quantum computation
- the protocol is sound against any malicious prover
- additional property: the prover does not learn the input
Ideal world

- Goal: Interactive proof system for BQP where
  - the verifier runs poly-time prob. computation

\[ V \]
\[ x \]
Goal: Interactive proof system for BQP where
- the verifier runs poly-time prob. computation
- an honest prover runs poly-time quantum computation
Ideal world

Goal: Interacrive proof system for BQP where

- the verifier runs poly-time prob. computation
- an honest prover runs poly-time quantum computation
- the protocol is sound against any malicious prover

Non-local games and verifiable delegation of quantum computation
• Ideal world

Goal: Interactive proof system for BQP where
- the verifier runs poly-time prob. computation
- an honest prover runs poly-time quantum computation
- the protocol is sound against any malicious prover
- additional property: the prover does not learn the input
Relaxed models

Exponential-size provers

Almost-classical clients

Comput. soundness
Multiple provers

\[ V \]

\[ \Psi_{EPR} \]

Multiple entangled non-communicating provers sound against any malicious strategy. Servers have to keep entangled.”

Non-local games and verifiable delegation of quantum computation
Multiple provers

- Multiple entangled non-communicating $P$
Multiple provers

- Multiple entangled non-communicating P
- Sound against any malicious strategy
Multiple provers

- Multiple entangled non-communicating P
- Sound against any malicious strategy
- Servers have to keep entangled 😊
Multiple provers

- Multiple entangled non-communicating P
- Sound against any malicious strategy
- Servers have to keep entangled 😊
- “Plug-and-play” 😊
## Previous works

<table>
<thead>
<tr>
<th></th>
<th>Provers</th>
<th>Rounds</th>
<th>Total Resources</th>
<th>Blind</th>
</tr>
</thead>
<tbody>
<tr>
<td>RUV 2012</td>
<td>2</td>
<td>poly($n$)</td>
<td>poly($n$)</td>
<td>yes</td>
</tr>
</tbody>
</table>
## Previous works

<table>
<thead>
<tr>
<th></th>
<th>Provers</th>
<th>Rounds</th>
<th>Total Resources</th>
<th>Blind</th>
</tr>
</thead>
<tbody>
<tr>
<td>RUV 2012</td>
<td>2</td>
<td>poly($n$)</td>
<td>$\geq g^{8192}$</td>
<td>yes</td>
</tr>
</tbody>
</table>
## Previous works

<table>
<thead>
<tr>
<th></th>
<th>Provers</th>
<th>Rounds</th>
<th>Total Resources</th>
<th>Blind</th>
</tr>
</thead>
<tbody>
<tr>
<td>RUV 2012</td>
<td>2</td>
<td>poly(n)</td>
<td>$g^{8192}$</td>
<td>yes</td>
</tr>
<tr>
<td>McKague 2013</td>
<td>poly(n)</td>
<td>poly(n)</td>
<td>$2^{153}g^{22}$</td>
<td>yes</td>
</tr>
<tr>
<td>GKW 2015</td>
<td>2</td>
<td>poly(n)</td>
<td>$g^{2048}$</td>
<td>yes</td>
</tr>
<tr>
<td>HDF 2015</td>
<td>poly(n)</td>
<td>poly(n)</td>
<td>$\Theta(g^4 \log g)$</td>
<td>yes</td>
</tr>
<tr>
<td>FH 2015</td>
<td>5</td>
<td>poly(n)</td>
<td>$&gt; g^3$</td>
<td>no</td>
</tr>
<tr>
<td>NV 2017</td>
<td>7</td>
<td>2</td>
<td>$&gt; g^3$</td>
<td>no</td>
</tr>
</tbody>
</table>
The results

Delegate circuit $Q$ on $n$ qubits, with $g$ gates and depth $d$, 2 provers:
The results

Delegate circuit $Q$ on $n$ qubits, with $g$ gates and depth $d$, 2 provers:

- Verifier-on-a-leash protocol: $O(d)$ rounds, $O(g \log g)$ EPR pairs, blind
The results

Delegate circuit $Q$ on $n$ qubits, with $g$ gates and depth $d$, 2 provers:
- Verifier-on-a-leash protocol: $O(d)$ rounds, $O(g \log g)$ EPR pairs, blind
- Dogwalker protocol: 2 rounds, $O(g \log g)$ EPR pairs
## Comparing to previous works

<table>
<thead>
<tr>
<th></th>
<th>Provers</th>
<th>Rounds</th>
<th>Total Resources</th>
<th>Blind</th>
</tr>
</thead>
<tbody>
<tr>
<td>RUV 2012</td>
<td>2</td>
<td>poly($n$)</td>
<td>$\geq g^{8192}$</td>
<td>yes</td>
</tr>
<tr>
<td>McKague 2013</td>
<td>poly($n$)</td>
<td>poly($n$)</td>
<td>$\geq 2^{153}g^{22}$</td>
<td>yes</td>
</tr>
<tr>
<td>GKW 2015</td>
<td>2</td>
<td>poly($n$)</td>
<td>$\geq g^{2048}$</td>
<td>yes</td>
</tr>
<tr>
<td>HDF 2015</td>
<td>poly($n$)</td>
<td>poly($n$)</td>
<td>$\Theta(g^4 \log g)$</td>
<td>yes</td>
</tr>
<tr>
<td>FH 2015</td>
<td>5</td>
<td>poly($n$)</td>
<td>$&gt; g^3$</td>
<td>no</td>
</tr>
<tr>
<td>NV 2017</td>
<td>7</td>
<td>2</td>
<td>$&gt; g^3$</td>
<td>no</td>
</tr>
<tr>
<td>VoL</td>
<td>2</td>
<td>$O$(depth)</td>
<td>$\Theta(g \log g)$</td>
<td>yes</td>
</tr>
<tr>
<td>DW</td>
<td>2</td>
<td>2</td>
<td>$\Theta(g \log g)$</td>
<td>no</td>
</tr>
<tr>
<td>Relativistic</td>
<td>2</td>
<td>1</td>
<td>$g^3$</td>
<td>no</td>
</tr>
</tbody>
</table>
1. Basics on quantum computation

2. General idea

3. Our protocols

4. Open problems
Very quick introduction to quantum computation

- 1 qubit
  - Unit vector in $\mathbb{C}^2$
  - Basis: $|0\rangle = \left(\begin{array}{c} 1 \\ 0 \end{array}\right)$ and $|1\rangle = \left(\begin{array}{c} 0 \\ 1 \end{array}\right)$
  - $|\psi_1\rangle = \alpha |0\rangle + \beta |1\rangle$, $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$
1 qubit
- Unit vector in $\mathbb{C}^2$
- Basis: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- $|\psi_1\rangle = \alpha |0\rangle + \beta |1\rangle$, $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$

$n$ qubits
- Unit vector in $(\mathbb{C}^2)^\otimes n$
- Basis: $|i\rangle$, $i \in \{0, 1\}^n$
- $|\psi_2\rangle = \sum_{i\in\{0,1\}^n} \alpha_i |i\rangle$, $\alpha_i \in \mathbb{C}$ and $\sum |\alpha_i|^2 = 1$
Very quick introduction to quantum computation

- **1 qubit**
  - Unit vector in $\mathbb{C}^2$
  - Basis: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
  - $|\psi_1\rangle = \alpha |0\rangle + \beta |1\rangle$, $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$

- **$n$ qubits**
  - Unit vector in $(\mathbb{C}^2)^\otimes n$
  - Basis: $|i\rangle$, $i \in \{0, 1\}^n$
  - $|\psi_2\rangle = \sum_{i \in \{0,1\}^n} \alpha_i |i\rangle$, $\alpha_i \in \mathbb{C}$ and $\sum |\alpha_i|^2 = 1$

- $|EPR\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$
  - It cannot be written as a product state
  - Source of quantum “spooky actions”
  - For every orthonormal basis $\{|v\rangle, |v\perp\rangle\}$, $|EPR\rangle = \frac{1}{\sqrt{2}} (|vv\rangle + |v\perp v\perp\rangle)$
Very quick introduction to quantum computation

- Evolution of quantum states
  - Unitary operators
  - Composed by gates picked from a (universal) gate-set
Very quick introduction to quantum computation

- Evolution of quantum states
  - Unitary operators
  - Composed by gates picked from a (universal) gate-set

- Projective measurements on $|\psi\rangle$
  - Set of projectors $\{P_i\}$, s.t. $\sum_i P_i = I$
  - Output $i$ with probability $\|P_i |\psi\rangle\|^2$
  - After the measurement, the states collapses to $\frac{P_i |\psi\rangle}{\|P_i |\psi\rangle\|}$
Very quick introduction to quantum computation

- Evolution of quantum states
  - Unitary operators
  - Composed by gates picked from a (universal) gate-set

- Projective measurements on $|\psi\rangle$
  - Set of projectors $\{P_i\}$, s.t. $\sum_i P_i = I$
  - Output $i$ with probability $\|P_i |\psi\rangle\|^2$
  - After the measurement, the states collapses to $\frac{P_i |\psi\rangle}{\|P_i |\psi\rangle\|}$

- $|EPR\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$
  - If measure the first half, the second half is completely defined (independent of the chosen basis)
From quantum delegation to classical delegation

$V$ and $P$ share EPR pairs

$V$ sends $z_i \in \{0, 1\}$

$P$ sends back $c_i \in \{0, 1\}$

$V$ measures half of EPR pairs with Clifford observables

$V$ performs checks

If $P$ passes tests, then no "harmful" errors
From quantum delegation to classical delegation

$|EPR\rangle^\otimes t$

- $V$ and $P$ share EPR pairs

$V$ and $P$ share EPR pairs

$V$ and $P$ share EPR pairs
From quantum delegation to classical delegation

V and P share EPR pairs

V sends $z_i \in \{0, 1\}$
From quantum delegation to classical delegation

- V and P share EPR pairs
- V sends $z_i \in \{0, 1\}$
- P sends back $c_i \in \{0, 1\}$
From quantum delegation to classical delegation

- V and P share EPR pairs
- V sends $z_i \in \{0, 1\}$
- P sends back $c_i \in \{0, 1\}$
- V measures half of EPR pairs with Clifford observables
From quantum delegation to classical delegation

- V and P share EPR pairs
- V sends $z_i \in \{0, 1\}$
- P sends back $c_i \in \{0, 1\}$
- V measures half of EPR pairs with Clifford observables
- V performs checks
From quantum delegation to classical delegation

\[ |EPR\rangle ^{\otimes t} \]

- V and P share EPR pairs
- V sends \( z_i \in R \{0, 1\} \)
- P sends back \( c_i \in \{0, 1\} \)
- V measures half of EPR pairs with Clifford observables
- V performs checks
- If P passes tests, then no “harmful” errors
From quantum delegation to classical delegation

Idea: Delegate $V$ to a prover $P$

If $PV$ is honest, we are done

How to test $PV$?
From quantum delegation to classical delegation

Idea: Delegate $V$ to a prover $PV$
If $PV$ is honest, we are done
How to test $PV$?
From quantum delegation to classical delegation

- Idea: Delegate $V$ to a prover

If $PV$ is honest, we are done

How to test $PV$?
From quantum delegation to classical delegation

Idea: Delegate V to a prover
From quantum delegation to classical delegation

- Idea: Delegate $V$ to a prover
- If $PV$ is honest, we are done
From quantum delegation to classical delegation

Idea: Delegate V to a prover
If PV is honest, we are done
How to test PV?
Non-local games

\[ V(x, y) \sim D \]

\[ V(a, b | x, y) \in \{0, 1\} \]

\[ P_1 \text{ and } P_2 \text{ share a strategy before the game start and then they do not communicate} \]

\[ V \text{ picks } x, y \text{ from distribution } D \]

\[ V \text{ sends } x \text{ to } P_1 \text{ and } y \text{ to } P_2 \]

\[ P_1 \text{ answers with } a \text{ and } P_2 \text{ answers with } b \]

\[ V \text{ accepts iff } V(a, b | x, y) = 1 \]

Classical value \( \omega(G) \) and quantum value \( \omega^*(G) \)

\[ \omega^*(G) > \omega(G) \]
Non-local games

$P_1$ and $P_2$ share a strategy before the game start and then they do not communicate.
Non-local games

- $P_1$ and $P_2$ share a strategy before the game start and then they do not communicate.
- $V$ picks $x, y$ from distribution $D$.

$x, y \sim D$
Non-local games

- $P_1$ and $P_2$ share a strategy before the game start and then they do not communicate
- $V$ picks $x, y$ from distribution $D$
- $V$ sends $x$ to $P_1$ and $y$ to $P_2$

$V(x, y) \in \{0, 1\}$

Classical value $\omega(G)$ and quantum value $\omega^*(G)$

$\omega^*(G) > \omega(G)$
Non-local games

- $P_1$ and $P_2$ share a strategy before the game start and then they do not communicate.
- $V$ picks $x, y$ from distribution $D$.
- $V$ sends $x$ to $P_1$ and $y$ to $P_2$.
- $P_1$ answers with $a$ and $P_2$ answers with $b$.

$V$ accepts iff $V(a, b | x, y) = 1$.

Classical value $\omega(G)$ and quantum value $\omega^*(G)$.

$\omega^*(G) > \omega(G)$. 

Non-local games and verifiable delegation of quantum computation
Non-local games

- $P_1$ and $P_2$ share a strategy before the game start and then they do not communicate
- $V$ picks $x, y$ from distribution $D$
- $V$ sends $x$ to $P_1$ and $y$ to $P_2$
- $P_1$ answers with $a$ and $P_2$ answers with $b$
- $V$ accepts iff $V(a, b|x, y) = 1$

$V(a, b|x, y) \in \{0, 1\}$

Classical value $\omega(G)$ and quantum value $\omega^*(G)$

$\omega^*(G) > \omega(G)$
Non-local games

- $P_1$ and $P_2$ share a strategy before the game start and then they do not communicate.
- $V$ picks $x, y$ from distribution $D$.
- $V$ sends $x$ to $P_1$ and $y$ to $P_2$.
- $P_1$ answers with $a$ and $P_2$ answers with $b$.
- $V$ accepts iff $V(a, b|x, y) = 1$.
- Classical value $\omega(G)$ and quantum value $\omega^*(G)$.
Non-local games

$P_1$ and $P_2$ share a strategy before the game start and then they do not communicate.

V picks $x, y$ from distribution $D$.

V sends $x$ to $P_1$ and $y$ to $P_2$.

$P_1$ answers with $a$ and $P_2$ answers with $b$.

V accepts iff $V(a, b|x, y) = 1$.

Classical value $\omega(G)$ and quantum value $\omega^*(G)$.

$\omega^*(G) > \omega(G)$.
Bell inequalities and rigidity theorems - Example CHSH

\[ x \cdot y = a \oplus b \]

Classical value \( \omega(CHSH) = \frac{3}{4} \)

Quantum value \( \omega^*(CHSH) = \cos^2(\frac{\pi}{8}) \)

Provers share \( |EPR\rangle \) and measure

__Rigidity:__ if acceptance prob. is \( \omega^*(CHSH) - \varepsilon \), then strategy is \( O(\sqrt{\varepsilon}) \) close to the previous one
Bell inequalities and rigidity theorems - Example CHSH

\[ x, y \in \mathbb{R} \{0, 1\} \]
\[ x \cdot y = a \oplus b \]
Bell inequalities and rigidity theorems - Example CHSH

- Classical value $\omega(CHSH) = \frac{3}{4}$
- Quantum value $\omega^*(CHSH) = \cos^2\left(\frac{\pi}{8}\right)$

$x, y \in \mathbb{R}\{0, 1\}$
$x \cdot y = a \oplus b$
Bell inequalities and rigidity theorems - Example CHSH

- Classical value $\omega(CHSH) = \frac{3}{4}$
- Quantum value $\omega^*(CHSH) = \cos^2\left(\frac{\pi}{8}\right)$
- Provers share $|EPR\rangle$ and measure

\[
\begin{array}{c|cc}
 & 0 & 1 \\
\hline
P_1 & X & Z \\
\hline
P_2 & \frac{X+Z}{\sqrt{2}} & \frac{Z-X}{\sqrt{2}} \\
\end{array}
\]

$x, y \in \mathbb{R} \{0, 1\}$

$x \cdot y = a \oplus b$
Bell inequalities and rigidity theorems - Example CHSH

- Classical value $\omega(CHSH) = \frac{3}{4}$
- Quantum value $\omega^*(CHSH) = \cos^2\left(\frac{\pi}{8}\right)$
- Provers share $|EPR\rangle$ and measure

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_1$</td>
<td>$X$</td>
<td>$Z$</td>
</tr>
<tr>
<td>$P_2$</td>
<td>$\frac{X+Z}{\sqrt{2}}$</td>
<td>$\frac{Z-X}{\sqrt{2}}$</td>
</tr>
</tbody>
</table>

- Rigidity: if acceptance prob. is $\omega^*(CHSH) - \varepsilon$, then strategy is $O(\sqrt{\varepsilon})$ close to the previous one
Our rigidity results

Our game

Our game is a set of one-qubit Clifford observables Game where a constant fraction of the questions are in a random $G_m$. Based on the Pauli Braiding Test Honest strategy Share $m$ EPR pairs and on question of the form $W \in G_m$ the prover measures the "correct" observable $W$. 
Our rigidity results

Our game

- $\mathcal{G}$ is a set of one-qubit Clifford observables
- Game where a constant fraction of the questions are in a random $\mathcal{G}^m$
- Based on the Pauli Braiding Test
Our rigidity results

Our game

- $\mathcal{G}$ is a set of one-qubit Clifford observables
- Game where a constant fraction of the questions are in a random $\mathcal{G}^m$
- Based on the Pauli Braiding Test

Honest strategy

Share $m$ EPR pairs and on question of the form $W \in \mathcal{G}^m$ the prover measures the “correct” observable $W$. 
Our rigidity results

Theorem

The honest strategy succeeds with prob. \(1 - e^{-\Omega(m)}\) in the game.
Our rigidity results

**Theorem**

The honest strategy succeeds with prob. $1 - e^{-\Omega(m)}$ in the game.

**Theorem**

For any $\varepsilon > 0$, any strategy for the provers that succeeds with prob. $1 - \varepsilon$ must be $O(\sqrt{\varepsilon})$-close to the honest strategy.
From quantum delegation to classical delegation

With prob. $p$, play non-local game
With prob. $1 - p$, execute original protocol

Two tests are indistinguishable for $PV$
$PP$ is tested in the original protocol
$x, Q$
From quantum delegation to classical delegation

\[ \langle EPR \rangle \]

\[ PV \] \[ PP \]

\[ x, Q \]

\[ V' \]

Protocol

With prob. \( p \), play non-local game

With prob. \( 1 - p \), execute original protocol

Two tests are indistinguishable for \( PV \)

\( PV \) is tested with the game

\( PP \) is tested in the original protocol

If both pass the tests, they perform the computation
From quantum delegation to classical delegation

\[ |EPR \rangle \]

\[ PV \]

\[ PP \]

\[ V' \]

\[ x, Q \]

- Protocol
  - With prob. \( p \), play non-local game

Two tests are indistinguishable for PV

PV is tested with the game

PP is tested in the original protocol

If both pass the tests, they perform the computation
From quantum delegation to classical delegation

$Q'x, Q$

- Protocol
  - With prob. $p$, play non-local game
  - With prob. $1 - p$, execute original protocol
From quantum delegation to classical delegation

Protocol
- With prob. $p$, play non-local game
- With prob. $1 - p$, execute original protocol

Two tests are indistinguishable for PV
From quantum delegation to classical delegation

- Protocol
  - With prob. \( p \), play non-local game
  - With prob. \( 1 - p \), execute original protocol
- Two tests are indistinguishable for PV
- PV is tested with the game
From quantum delegation to classical delegation

- Protocol
  - With prob. $p$, play non-local game
  - With prob. $1 - p$, execute original protocol

- Two tests are indistinguishable for PV
- PV is tested with the game
- PP is tested in the original protocol
From quantum delegation to classical delegation

- Protocol
  - With prob. \( p \), play non-local game
  - With prob. \( 1 - p \), execute original protocol

- Two tests are indistinguishable for PV
- PV is tested with the game
- PP is tested in the original protocol
- If both pass the tests, they perform the computation
Verifier-on-a-leash protocol

Rigidity Test

Original protocol

Rigidity-Clifford

Test rounds

Computation rounds
DogWalker protocol

- In Verifier-on-a-leash protocol
DogWalker protocol

- In Verifier-on-a-leash protocol
  - Rounds of communication for blindness
DogWalker protocol

- In Verifier-on-a-leash protocol
  - Rounds of communication for blindness
- In DogWalker protocol
DogWalker protocol

- In Verifier-on-a-leash protocol
  - Rounds of communication for blindness
- In DogWalker protocol
  - Reveal $x$ to PV
DogWalker protocol

- In Verifier-on-a-leash protocol
  - Rounds of communication for blindness
- In DogWalker protocol
  - Reveal $x$ to PV
  - Extra tests to check if PV is honest
DogWalker protocol

PV

1

Rigidity Test

2

Original protocol

3

Uniformity of \{c_i\}_i

4

Tomography Test

PP

1

Rigidity-Clifford

2

Test rounds

3

Computation round

4

Rigidity-Tomography

Non-local games and verifiable delegation of quantum computation
Open problems

- More efficient 1-round schemes ($\tilde{O}(g)$ resources)
Open problems

- More efficient 1-round schemes ($\tilde{O}(g)$ resources)
- Blind $O(1)$-round protocols
Open problems

- More efficient 1-round schemes ($\tilde{O}(g)$ resources)
- Blind $O(1)$-round protocols
- Delegation protocol with non-entangled provers
Thank you for your attention!