Non-local games and verifiable delegation of quantum computation

Alex Bredariol Grilo

CWI QuSoft

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? 😐

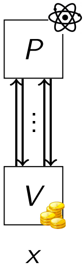
Ideal world

- Goal: Interacrive proof system for BQP where

Ideal world

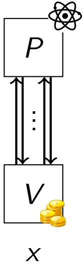
- Goal: Interacrive proof system for BQP where
  - the verifier runs poly-time prob. computation

Ideal world



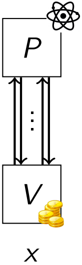
- Goal: Interacrive proof system for BQP where
  - the verifier runs poly-time prob. computation
  - an honest prover runs poly-time quantum computation

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

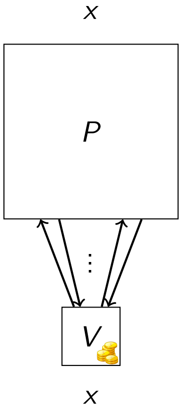
Ideal world



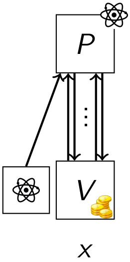
- Goal: Interacrive proof system for BQP where
  - the verifier runs poly-time prob. computation
  - an honest prover runs poly-time quantum computation
  - the protocol is sound against any malicious prover
  - additional property: the prover does not learn the input

Relaxed models

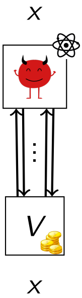
Exponential-size provers



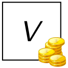
Almost-classical clients



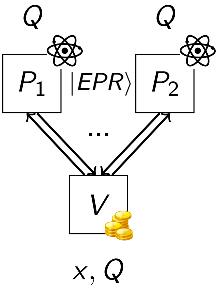
Comput. soundness



Multiple provers

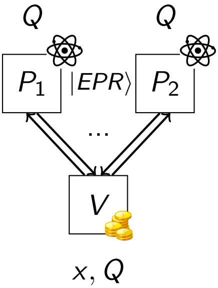


Multiple provers



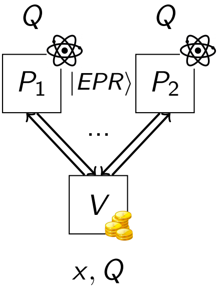
- Multiple entangled non-communicating P

Multiple provers



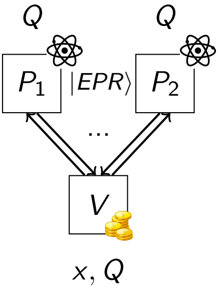
- Multiple entangled non-communicating P
- Sound against any malicious strategy

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

	Provers	Rounds	Total Resources	Blind
RUV 2012	2	poly(n)	poly(n)	yes

Previous works

	Provers	Rounds	Total Resources	Blind
RUV 2012	2	poly(n)	$\geq g^{8192}$	yes

Previous works

	Provers	Rounds	Total Resources	Blind
RUV 2012	2	poly(n)	$\geq g^{8192}$	yes
McKague 2013	$\mathrm{poly}(n)$	poly(n)	$\geq 2^{153} g^{22}$	yes
GKW 2015	2	poly(n)	$\geq g^{2048}$	yes
HDF 2015	poly(n)	poly(n)	$\Theta(g^4 \log g)$	yes
FH 2015	5	poly(n)	$> g^3$	no
NV 2017	7	2	$> g^3$	no

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

	Provers	Rounds	Total Resources	Blind
RUV 2012	2	poly(n)	$\geq g^{8192}$	yes
McKague 2013	poly(n)	poly(n)	$\geq 2^{153} g^{22}$	yes
GKW 2015	2	poly(n)	$\geq g^{2048}$	yes
HDF 2015	poly(n)	poly(n)	$\Theta(g^4 \log g)$	yes
FH 2015	5	poly(n)	$> g^3$	no
NV 2017	7	2	$> g^3$	no
VoL	2	O(depth)	$\Theta(g \log g)$	yes
DW	2	2	$\Theta(g \log g)$	no
Relativistic	2	1	g^3	no

Very quick introduction to quantum computation

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

Very quick introduction to quantum computation

- 1 qubit
  - Unit vector in $\mathbb{C}^2$
  - Basis: $|0\rangle = \binom{1}{0}$ and $|1\rangle = \binom{0}{1}$
  - $|\psi_1\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,\ \ \alpha, \beta \in \mathbb{C}$ 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: $|0\rangle = \binom{1}{0}$ and $|1\rangle = \binom{0}{1}$
  - $|\psi_1\rangle = \alpha |0\rangle + \beta |1\rangle$, $\alpha, \beta \in \mathbb{C}$ 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 orthonomal basis $\{|v\rangle, |v^\perp\rangle\}$, $|EPR\rangle = \frac{1}{\sqrt{2}}\left(|vv\rangle + |v^\perp v^\perp\rangle\right)$

Very quick introduction to quantum computation

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

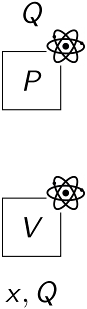
Very quick introduction to quantum computation

- 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 $\frac{P_i|\psi\rangle}{\| P_i|\psi\rangle \|}$

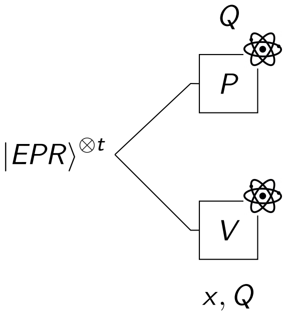
Very quick introduction to quantum computation

- 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

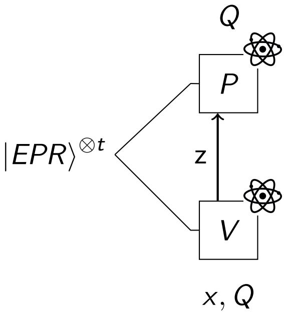


From quantum delegation to classical delegation



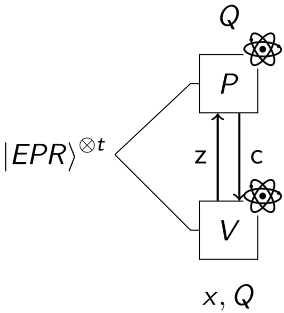
- V and P share EPR pairs

From quantum delegation to classical delegation



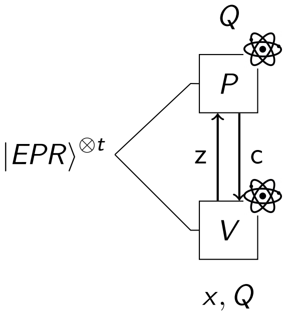
- V and P share EPR pairs
- V sends $z_i \in_R \{0, 1\}$

From quantum delegation to classical delegation



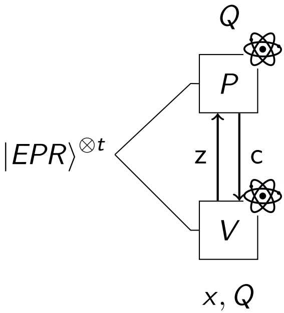
- V and P share EPR pairs
- V sends $z_i \in_R \{0, 1\}$
- P sends back $c_i \in \{0, 1\}$

From quantum delegation to classical delegation



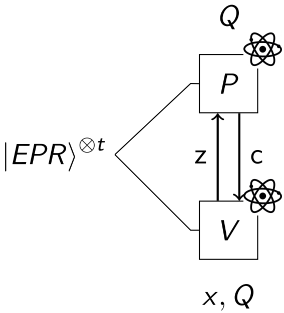
- V and P share EPR pairs
- V sends $z_i \in_R \{0, 1\}$
- P sends back $c_i \in \{0, 1\}$
- V measures half of EPR pairs with Clifford observables

From quantum delegation to classical delegation



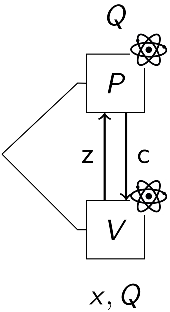
- V and P share EPR pairs
- V sends $z_i \in_R \{0,1\}$
- P sends back $c_i \in \{0,1\}$
- V measures half of EPR pairs with Clifford observables
- V performs checks

From quantum delegation to classical delegation

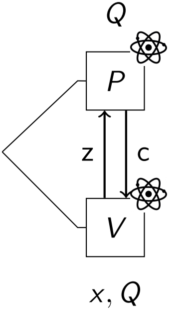


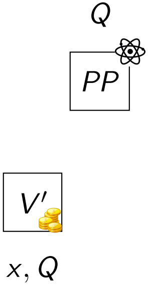
- V and P share EPR pairs
- V sends $z_i \in_R \{0,1\}$
- P sends back $c_i \in \{0,1\}$
- V measures half of EPR pairs with Clifford observables
- V performs checks
- If P passes tests, then no "harmful" errors

From quantum delegation to classical delegation

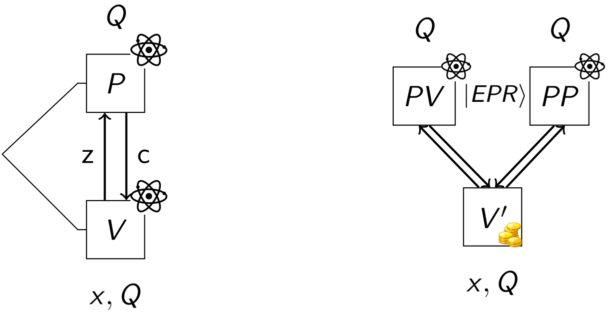


From quantum delegation to classical delegation



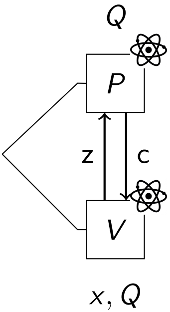


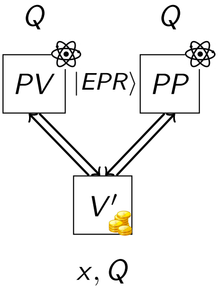
From quantum delegation to classical delegation



- Idea: Delegate V to a prover

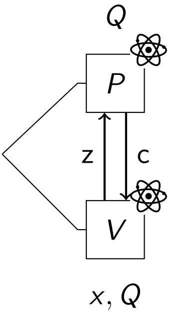
From quantum delegation to classical delegation

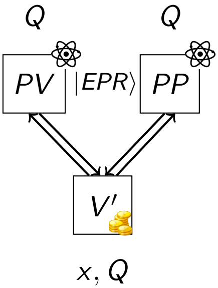




- Idea: Delegate V to a prover

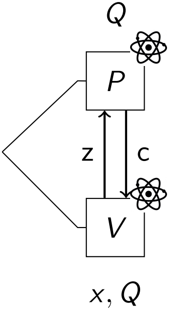
From quantum delegation to classical delegation

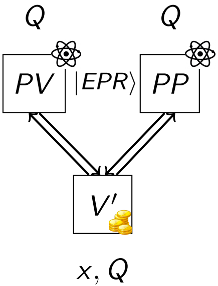




- Idea: Delegate V to a prover
- If PV is honest, we are done

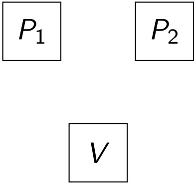
From quantum delegation to classical delegation



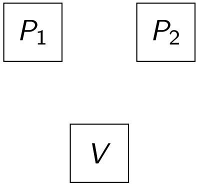


- Idea: Delegate V to a prover
- If PV is honest, we are done
- How to test PV?

Non-local games

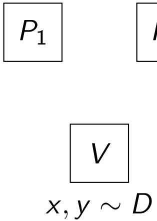


Non-local games



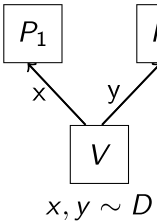
- P_1 and P_2 share a strategy before the game start and then they do not communicate

Non-local games



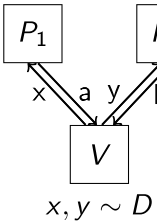
- P_1 and P_2 share a strategy before the game start and then they do not communicate
- V picks x, y from distribution D

Non-local games



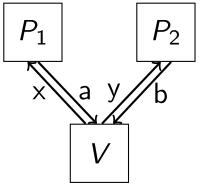
- P_1 and P_2 share a strategy before the game start and then they do not communicate
- V picks x, y from distribution D
- V sends x to P_1 and y to P_2

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

Non-local games

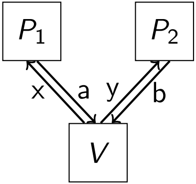


$x, y \sim D$

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

- 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 $V(a, b|x, y) = 1$

Non-local games

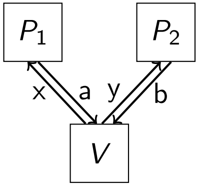


$x, y \sim D$

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

- 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



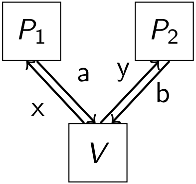
$x, y \sim D$

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

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

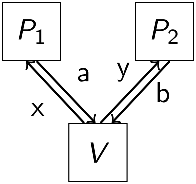
Bell inequalities and rigidity theorems - Example CHSH

Bell inequalities and rigidity theorems - Example CHSH



$$x, y \in_R \{0, 1\}$$
$$x \cdot y = a \oplus b$$

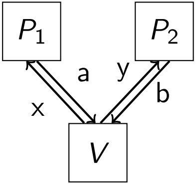
Bell inequalities and rigidity theorems - Example CHSH



$x, y \in_R \{0, 1\}$
$x \cdot y = a \oplus b$

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

Bell inequalities and rigidity theorems - Example CHSH

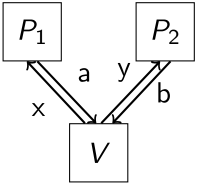


$x, y \in_R \{0,1\}$
$x \cdot y = a \oplus b$

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

	0	1
P_1	X	Z
P_2	$\frac{X+Z}{\sqrt{2}}$	$\frac{Z-X}{\sqrt{2}}$

Bell inequalities and rigidity theorems - Example CHSH



$x, y \in_R \{0,1\}$
$x \cdot y = a \oplus b$

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

	0	1
P_1	X	Z
P_2	$\frac{X+Z}{\sqrt{2}}$	$\frac{Z-X}{\sqrt{2}}$

- 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 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

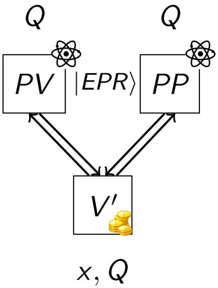
Theorem

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

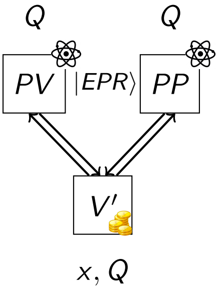
Theorem

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

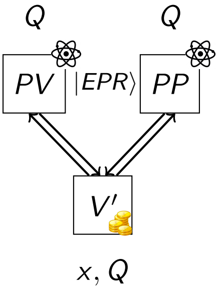


From quantum delegation to classical delegation



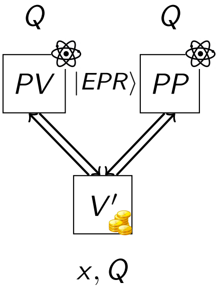
- Protocol

From quantum delegation to classical delegation



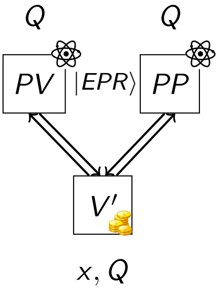
- Protocol
  - With prob. p, play non-local game

From quantum delegation to classical delegation



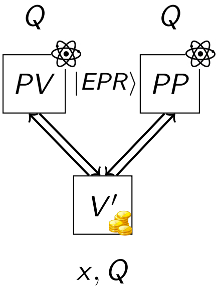
- Protocol
  - With prob. p, play non-local game
  - With prob. $1 - p$, execute original protocol

From quantum delegation to classical delegation



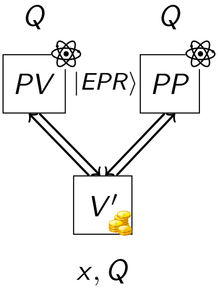
- Protocol
  - With prob. p, play non-local game
  - With prob. $1 - p$, execute original protocol
- Two tests are indistinguishable for PV

From quantum delegation to classical delegation



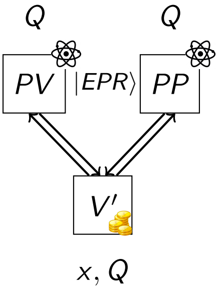
- Protocol
  - With prob. p, play non-local game
  - With prob. $1 - p$, execute original protocol
- Two tests are indistinguishable for PV
- PV is tested with the game

From quantum delegation to classical delegation



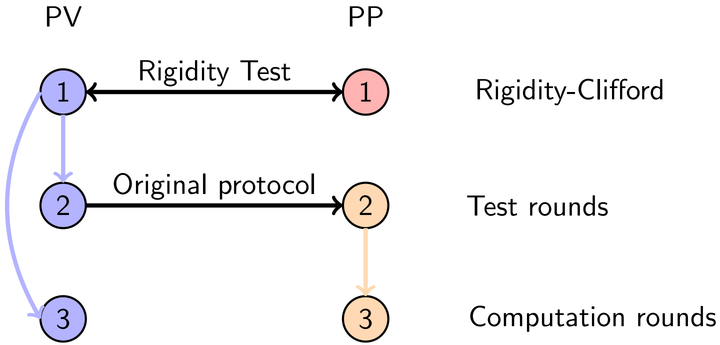
- Protocol
  - With prob. p, play non-local game
  - With prob. $1-p$, execute original protocol
- Two tests are indistinguishable for PV
- PV is tested with the game
- PP is tested in the original protocol

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



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

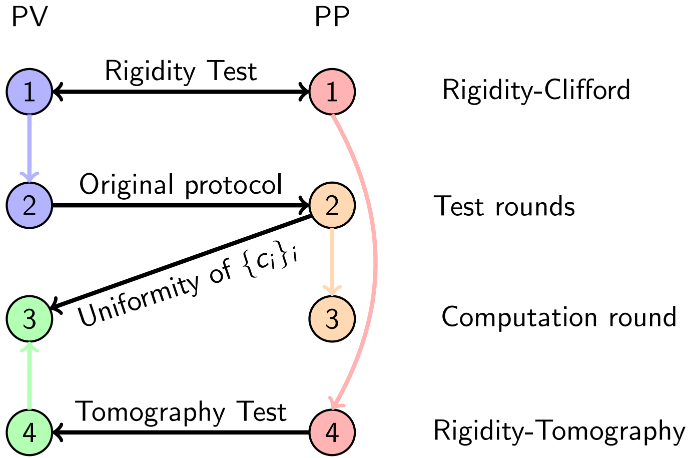
DogWalker protocol

- 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



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!