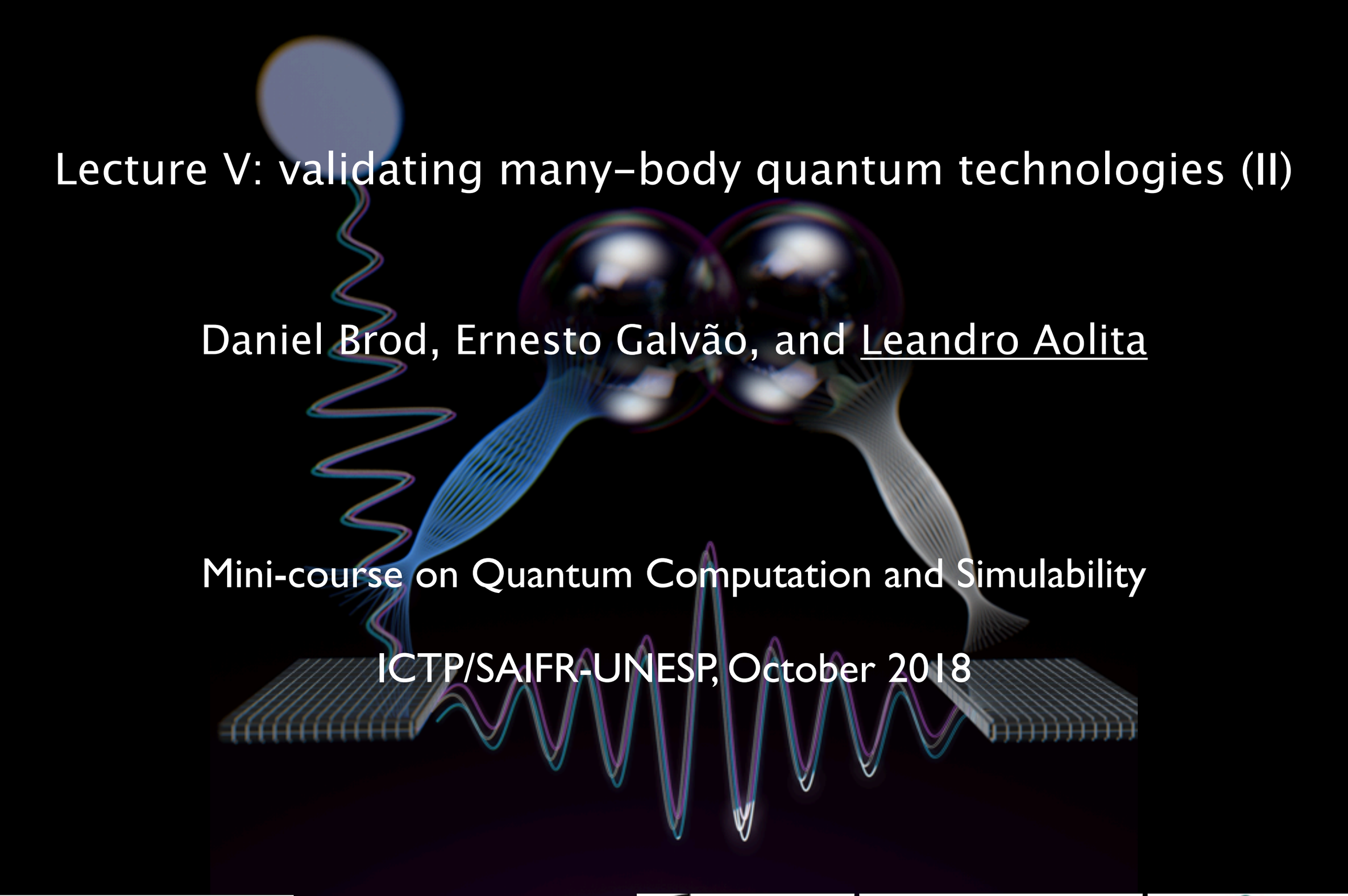
Lecture V: validating many-body quantum technologies (II)

Daniel Brod, Ernesto Galvão, and Leandro Aolita



Mini-course on Quantum Computation and Simulability

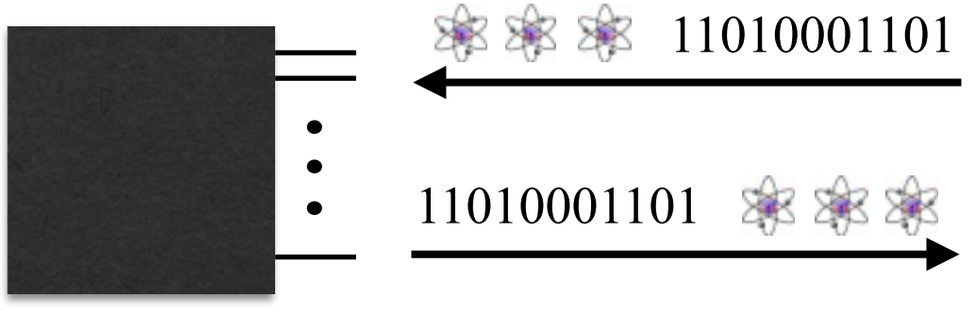
ICTP/SAIFR-UNESP, October 2018

CNPq Conselho Nacional de Desenvolvimento Científico e Tecnológico
CAPES
FAPESP SÃO PAULO RESEARCH FOUNDATION
serrapilheira
FAPERJ
INCT-IQ

Certification of universal quantum computations

General quantum certification mindset

Untrusted prover Merlin



Skeptic certifier Arthur

- **Interactive tests:** prover and certifier exchange quantum messages until the certifier gets convinced.

Interactive proof (IPs): **(unbounded prover/classical certifier)** S. Goldwasser, S. Micali, and C. Rackoff, In Proceedings of the seventeenth annual ACM symposium on Theory of computing, pages 291–304. ACM New York, NY, USA, 1985.

Quantum interactive proofs (QIP): **(unbounded quantum prover/ BQP certifier)** A. Kitaev, J. Watrous, STOC '00: Proceedings of the thirty-second annual ACM symposium on Theory of computing, ACM, pp. 608 (2000); J. Watrous, Theor. Comput. Sci. 292 (3): 575 (2003).

Quantum-prover interactive proofs (QPIP): **(BQP quantum prover/ almost-classical certifier)** A. M. Childs, D. W. Leung, and M. A. Nielsen, Phys. Rev. A **71**, 032318 (2005)**;** D. Aharonov, M. Ben-Or, and E. Eban, arXiv: 0810.5375; A. Broadbent, J. Fitzsimons, and E. Kashefi, Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009), 517 (2009); J. Fitzsimons and E. Kashefi, arXiv: 1203.5217.

- **Non-interactive tests:** certifier sends a classical input and prover returns an output that convinces him.

Quantum-prover interactive proofs with a single classical message (QPIP(1)): (BQP quantum prover/ classical* certifier): M. Cramer et al., Nat. Commun. **1**, 149 (2010); G. Toth et al., Phys. Rev. Lett. **105**, 250403 (2010); S. S. T. Flammia and Y.-K. Liu, Phys. Rev. Lett., **106,** 230501 (2011); M. P. da Silva, O. Landon-Cardinal, and D. Poulin, Phys. Rev. Lett., **107**, 210404 (2011); T. Moroder et al., New J. Phys. **14**, 105001 (2012); T. Baumgratz, D. Gross, M. Cramer, and M. B. Plenio, Phys. Rev. Lett. **111**, 020401 (2013); L. Aolita, C. Gogolin, M. Kliesch, and J. Eisert, Nat. Comms. **6**, 8498 (2015); M. Hayashi and T. Morimae, Phys. Rev. Lett., **115,** 220502 (2016).

↓

More practical

Interactive tests

Quantum-prover IPs

- A BQP prover can efficiently convince an almost-classical certifier :-)
- Require fully fledged fault-tolerant universal quantum computers :-(

Two main flavours:

Measurement-based quantum computing

- The certifier sends single-qubit states which include **traps** to test the prover.
- The prover stores the cluster state **blindly** and implements measurements instructed by the certifier.

A. Broadbent, J. Fitzsimons, and E. Kashefi, Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009), 517 (2009); J. Fitzsimons and E. Kashefi, Phys. Rev. A **96**, 012303 (2017); T. Kapourniotis, E. Kashefi, and A. Datta, arXiv: 1403.1438; M. Hayashi and T. Morimae, Phys. Rev. Lett., **115,** 220502 (2016).

Certifier with a constant-size quantum circuit

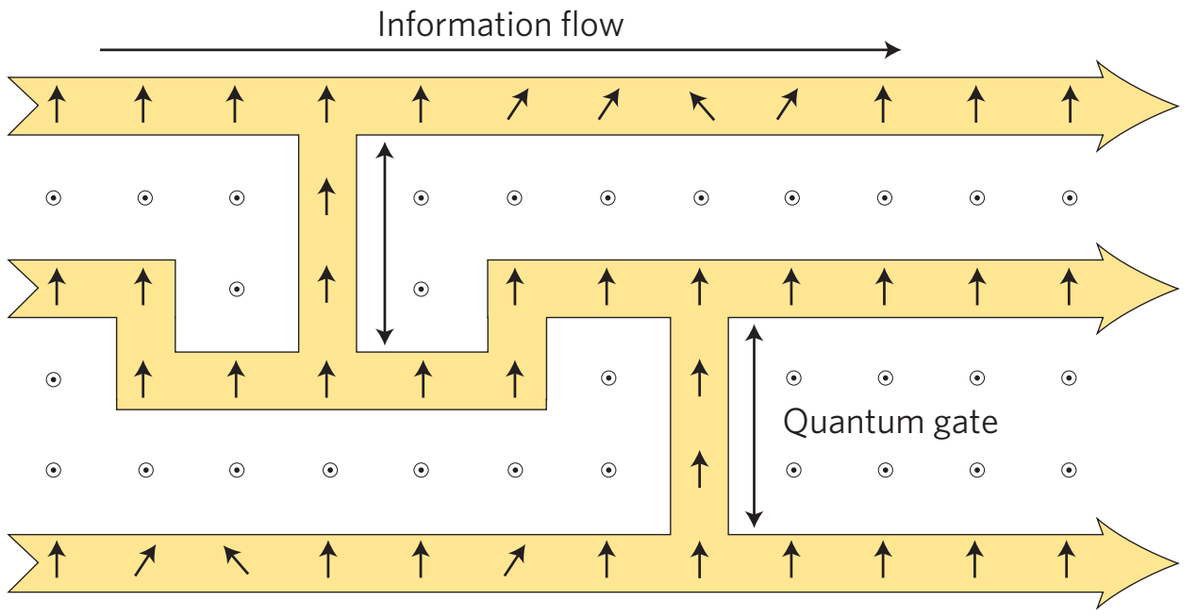
- The certifier sends **authenticated** qubits.
- The prover stores these qubits and either sends them back to the certifier, who **decodes and processes**, or processes himself instructed by the certifier.

D. Aharonov, M. Ben-Or, and E. Eban, arXiv: 0810.5375; D. Aharonov and U. Vazirani, arXiv: 1206.3686.

Measurement-based quantum-prover IPs

Conventional MBQC:

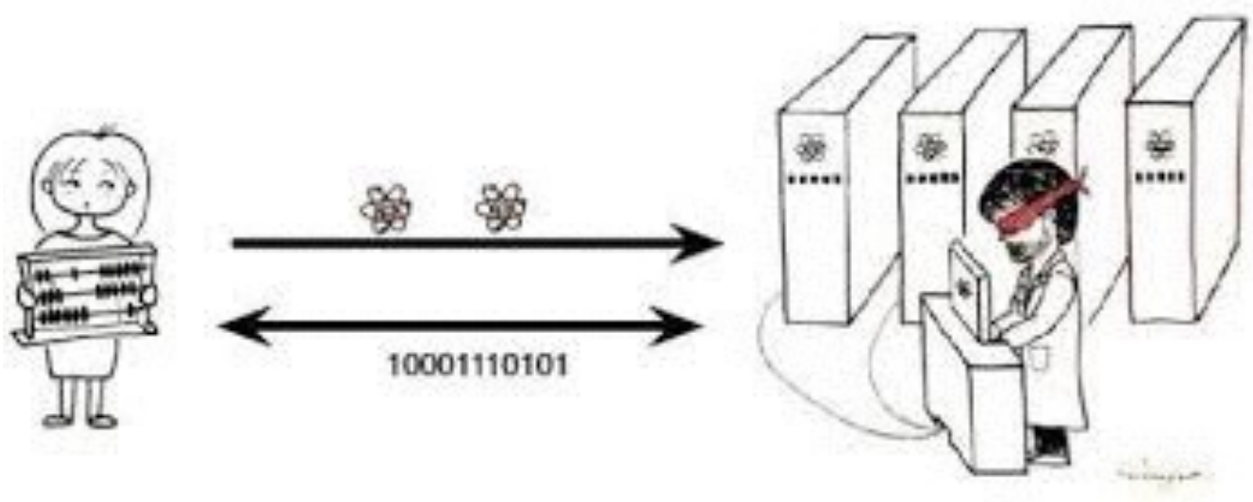
- Information processed by local measurements on a cluster state.
- Randomness compensated by adaptiveness.
- Measurement graph associated to an underlying circuit.



R. Rausendorf and H. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).

Blind MBQC:

- The **measurement graph** is **hidden** to Merlin.
- He performs measurements in directions given by Arthur but is **blind** to the **underlying circuit**.
- The hidden **graph contains traps** for him.



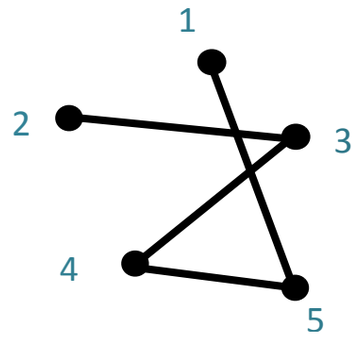
A. Broadbent, J. Fitzsimons, and E. Kashefi, Proceedings of the 50th Annual IEEE Symposium on FOCS (2009), 517 (2009); J. Fitzsimons and E. Kashefi, arXiv: 1203.5217.

Graph states (in a minute)

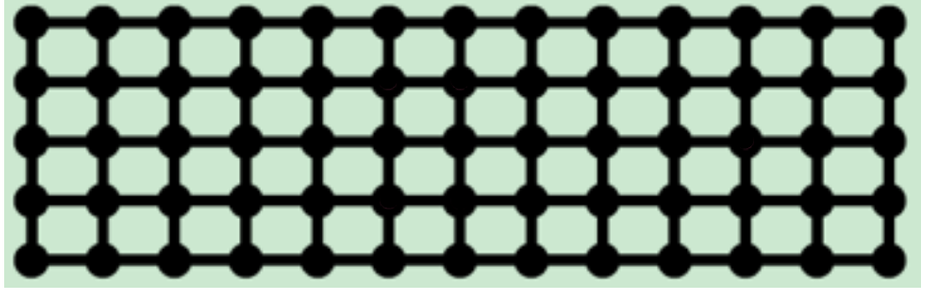
Definition:

Given a set of **vertices connected** by a pattern of **edges**, associate to **each vertex the state** $|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and apply a **controlled-*Z* gate** to each pair of **connected vertices**.

$$|G_5\rangle = CZ_{15}CZ_{23}CZ_{34}CZ_{45}|+\rangle_1 \otimes |+\rangle_2 \otimes |+\rangle_3 \otimes |+\rangle_4 \otimes |+\rangle_5$$



The cluster (state):



If a qubit is initialised in $|0\rangle$ *instead of* $|+\rangle$ *it does not get entangled to the graph*

M. Hein, J. Eisert, and H. J. Briegel, Phys. Rev. A **69,** 062311 (2004); M. Hein et al., In Proceedings of the International School of Physics "Enrico Fermi" on Quantum Computers, Algorithms and Chaos (2006).

Blind MBQC

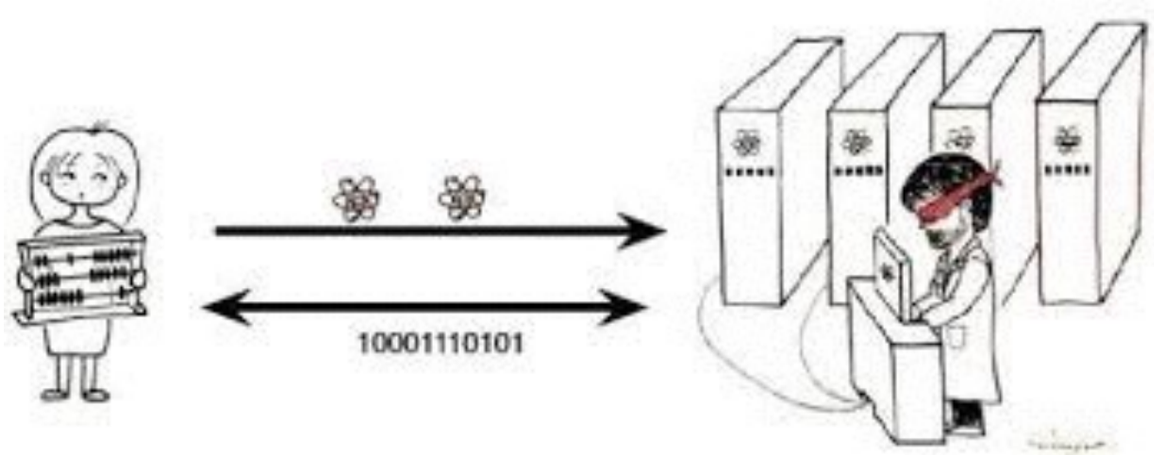
Preliminaries:

1. Depending on the computation, Arthur chooses a graph *G*.
2. For each vertex *v*, he prepares a qubit in:
   - an **input** state $|+_{\theta_v}\rangle$,
   - a **dummy** state $|z_v\rangle$, or
   - a **trap** state $|+_{\varphi_v}\rangle$,

(chosen randomly)

with $z_v \in \{0,1\}$, $|+_{\varphi_v}\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\,\varphi_v}|1\rangle\right)$ and $|+_{\theta_v}\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\,\theta_v}|1\rangle\right)$.

- The **inputs encode the computation**.
- The **dummies surround the traps**, isolating them.
- The **traps test Merlin**'s procedure. The **traps' positions** in *G* are **random**.



(Arthur) (Merlin)

Blind MBQC

Idea of the protocol:

1. Arthur sends G and the qubits to Merlin.
2. Merlin applies CZs according to G.
3. Merlin measures each qubit v in a basis B_ν given by Arthur and returns him the outcome. (with B_ν and $B_{\nu+1}$ correlated with z_ν, φ_ν, and θ_ν)
4. With the ν-th outcome, Arthur chooses $B_{\nu+1}$.
5. **If all trap** measurements yield the **correct** outcome, Arthur **accepts**. Otherwise, he rejects.

Then, if Arthur accepts,

$$\mathbb{P}_{\text{incorrect}} \leq \epsilon := \left(1 - \frac{N_{\text{T}}}{N}\right)^{\text{d}}.$$

d: constant (maximal weight of correctable Pauli error)

N_{T}: number of trap qubits

N: number of qubits

$(\Rightarrow F \geq 1 - \epsilon)$

- Universal quantum computations efficiently certifiable :-)
- Fault-tolerance and universality required :-(
- Dummy and trap qubits required :-(

***For the moment, way out of reach* :-(**

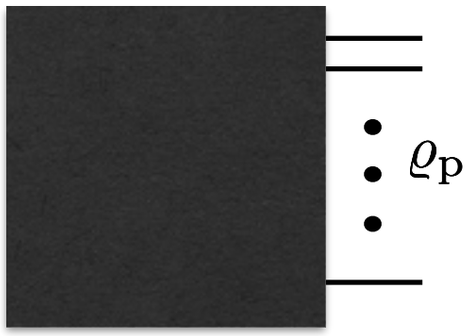
Non-interactive (measurement only!) tests

Non-interactive certification mindset

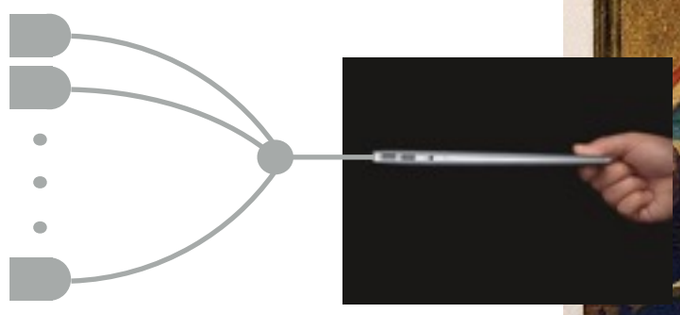
Untrusted quantum prover Merlin

Skeptic almost-classical certifier Arthur

$F(\varrho_{\mathrm{t}}, \varrho_{\mathrm{p}})$?



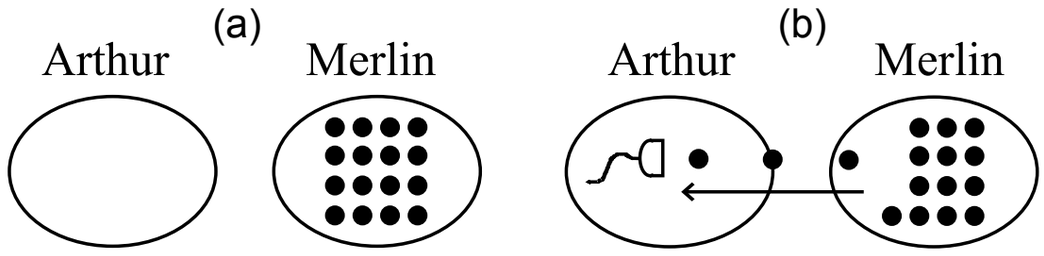
ϱ_{t} and C



- Similar mindset to QPIPs but with a single quantum interaction.
- No restriction on type of quantum noise, preparation totally unknown.
- ~~Only assumption: i.i.d. preparations~~ $\varrho_{\mathrm{p}}^{\otimes C}$.

Verifiable measurement-only blind quantum computing with stabilizer testing

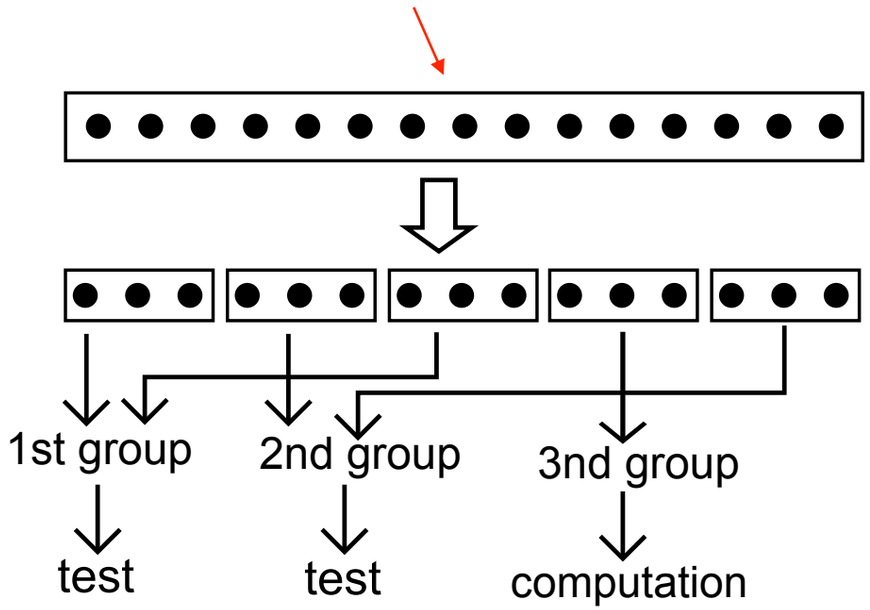
Non-interactive certification mindset:



Idea of the protocol:

1. Merlin prepares ***2k* + 1 copies of the *N*-qubit graph state** $|G\rangle$ and sends them one by one to Arthur.
2. Arthur randomly groups the $2k+1$ copies intro **3 groups**: **2 test groups** (of k N-qubit blocks each) and **1 computation group** (of one N-qubit block).
3. On each **test block**, Arthur runs one of **2 certification tests**. On the **computation block**, he runs the **MBQC**.
4. If **all *2k* tests** are **passed**, Arthur **accepts the outcomes** of the computation block.

$|G\rangle^{\otimes 2k+1}$ (if Merlin is honest)



M. Hayashi and T. Morimae, Phys. Rev. Lett., **115,** 220502 (2016).

The certification test: stabilizer testing (ground-state witnessing!)

Stabilizer operators:

$$X_i|+\rangle^{\otimes N} = |+\rangle^{\otimes N},\ \forall\ 1 \leq i \leq N$$

$$\Rightarrow \bigotimes_{e\in G} CZ_e\, X_i \bigotimes_{e\in G} CZ_e \bigotimes_{e\in G} CZ_e|+\rangle^{\otimes N} = \bigotimes_{e\in G} CZ_e|+\rangle^{\otimes N}$$

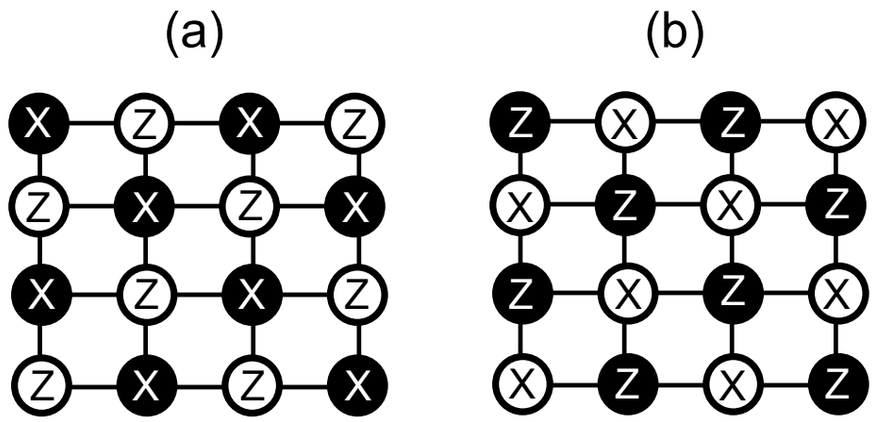
$$X_i \bigotimes_{j\in\mathcal{N}_i} Z_j |G\rangle = |G\rangle$$

(*i*-th generator of the Stabilizer group)

$|G\rangle$ is the unique state stabilized by all N generators of the stabilizer!!!

Stabilizer tests:

- Test 1: On each **black** qubit measure *X*. On each **white** quit measure *Z*. Accept if all outcomes coincide with stabilizer predictions.
- Test 2: On each **white** qubit measure *X*. On each **black** quit measure *Z*. Accept if all outcomes coincide with stabilizer predictions.



Theorem 1 *Assume that* $\alpha > \frac{1}{2k+1}$. *If the test is passed, with significance level* α, *we can guarantee that the resultant state* σ *of the third group satisfies*

$$(F = 1 - \mathbb{P}_{\text{incorrect}}) \longleftarrow \langle G|\sigma|G\rangle \geq 1 - \frac{1}{\alpha(2k+1)}. \quad)$$

Significance level: Maximum passing probability for an incorrect $(2k+1)N$ - qubit preparation

State of the computation block conditioned on all other $2k$ blocks having passed the test

- Universal quantum computations efficiently certifiable :-)
- No dummy or trap qubits required :-)
- Does not assume i.i.d. :-)
- Fault-tolerance and universality required :-(
- Only linear overhead in terms of copies of the state :-)

M. Hayashi and T. Morimae, Phys. Rev. Lett., **115,** 220502 (2016).

Classical verification of universal quantum computers!!! (???)

U. Mahadev, arXiv:1804.01082

QUANTUM COMPUTING

Graduate Student Solves Quantum Verification Problem

56 |

Urmila Mahadev spent eight years in graduate school solving one of the most basic questions in quantum computation: How do you know whether a quantum computer has done anything quantum at all?

Key assumption:

Quantum computers cannot break LWE
(leading candidate for post-quantum cryptography)

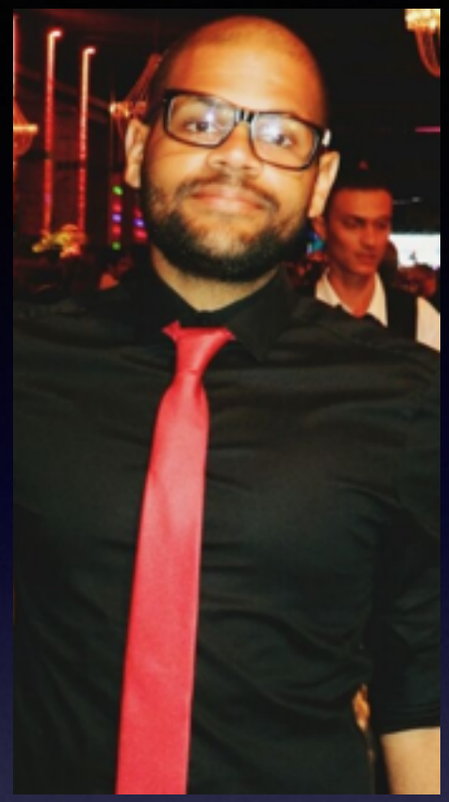
Conclusions of Lecture V:

- Interactive proofs
- Measurement only verification
- Classical verification of quantum computers?

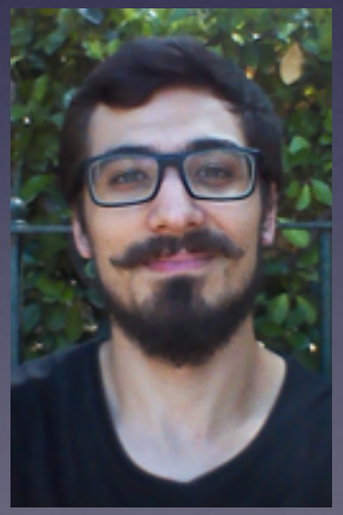
Close family at Rio & São Paulo:

Leonardo Guerini
Postdoc

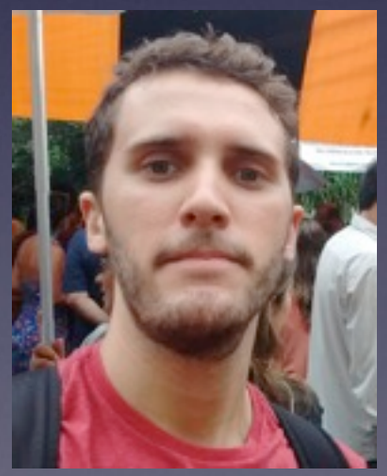
Carolina Gigliotti
PhD student



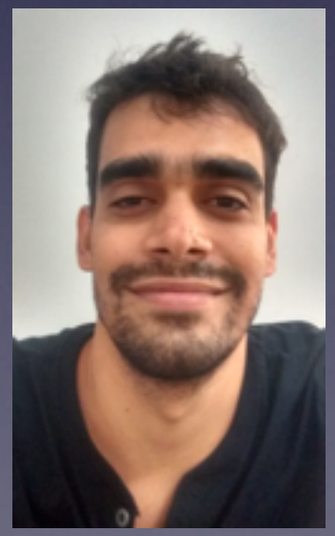
Renato M. S. Farias
PhD student



Ranieri V. Neri
Postdoc



Marcio M. Taddei
Postdoc



Eric G. A. Cavalcanti
PhD student

Thank you for your attention!