Alex Bredariol Grilo

✉ abgrilo@gmail.com • 🌐 abgrilo.org

Employment

LIP6, CNRS/Sorbonne Université
CNRS junior researcher (CR) *October 2020 – present*

CWI and QuSoft
Postdoc *June 2018 – September 2020*
Supervisors: Ronald de Wolf and Stacey Jeffery

Simons Institute, UC Berkeley
Research fellow *January 2020 – May 2020*

Université Paris Diderot
Lecturer (ATER) *September 2017 – May 2018*

Education

IRIF, CNRS/Université Paris Diderot, France
PhD, Computer Science *September 2014 – April 2018*
Title: Quantum proofs, the Local Hamiltonian problem and applications
Advisor: Iordanis Kerenidis

Institute of Computing, University of Campinas, Brazil
MSc., Computer Science *February 2012 – April 2014*
Title: Quantum Computing and Theoretical Computer Science
Advisor: Arnaldo Vieira Moura
GPA: 4.0/4.0

Institute of Computing, University of Campinas, Brazil
B.S., Computer Science *February 2007 – August 2011*
GPA: 0.9528/1.0

Awards

Simons Fellowship
Simons institute for the Theory of Computing *January 2020 – May 2020*
Research fellow in the program "The Quantum Wave in Computing"

Publications

Peer-reviewed conferences

Dorit Aharonov and Alex B. Grilo. Two combinatorial MA-complete problems. *Accepted at 12th Innovations in Theoretical Computer Science, ITCS 2021*, 2021, arXiv:2003.13065.

Anne Broadbent and Alex B. Grilo. QMA-hardness of Consistency of Local Density Matrices with Applications to Quantum Zero-Knowledge. *Accepted at 60th IEEE Annual Symposium on*

Foundations of Computer Science, FOCS 2019, 2020, arXiv:1911.07782. Invited talk at QCrypt 2020.

Gorjan Alagic, Andrew M. Childs, Alex B. Grilo, and Shih-Han Hung. Non-interactive classical verification of quantum computation . *Accepted at Theory of Cryptography - 18th International Conference, TCC 2020*, 2020, arXiv:1911.08101. Contributed talk at QCrypt 2020.

Yfke Dulek, Alex B. Grilo, Stacey Jeffery, Christian Majenz, and Christian Schaffner. Quantum multiparty computation against dishonest majority. In *EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 729–758, 2020, arXiv:1909.13770. Contributed talk at QCrypt 2020.

Alex B. Grilo, William Slofstra, and Henry Yuen. Perfect zero knowledge for quantum multiprover interactive proofs. In *60th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2019*, pages 611–635, 2019, arXiv:1905.11280. Contributed talk at QCrypt 2019 and QIP 2020 (single-track).

Dorit Aharonov and Alex B. Grilo. Stoquastic PCP vs. Randomness. In *60th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2019*, pages 1000–1023, 2019, arXiv:1901.05270. Contributed talk at QIP 2020 (single-track).

Alex B. Grilo. A simple protocol for verifiable delegation of quantum computation in one round. In *46th International Colloquium on Automata, Languages, and Programming, ICALP 2019*, pages 28:1–28:13, 2019, arXiv:1711.09585. Contributed talk at TQC 2019 and QCrypt 2019.

Andrea Coladangelo, Alex B. Grilo, Stacey Jeffery, and Thomas Vidick. Verifier-on-a-leash: New schemes for verifiable delegated quantum computation, with quasilinear resources. In *EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 247–277, 2019, arXiv:1708.07359. Contributed talk at QIP 2018.

Alex B. Grilo, Iordanis Kerenidis, and Attila Pereszlényi. Pointer Quantum PCPs and Multi-Prover Games. In *41st International Symposium on Mathematical Foundations of Computer Science, MFCS 2016*, pages 21:1–21:14, 2016, arXiv:1603.00903.

Alex B. Grilo, Iordanis Kerenidis, and Jamie Sikora. QMA with subset state witnesses. In *40th International Symposium on Mathematical Foundations of Computer Science 2015, MFCS 2015*, pages 163–174, 2015, arXiv:1410.2882.

Sergio Ordine, Alex B. Grilo, André Atanásio Almeida, and Zanoni Dias. ALGAe: A Test-bench Environment for a Genetic Algorithm-based Multiple Sequence Aligner. In *VI Brazilian Symposium on Bioinformatics, BSB 2011*, pages 57–60, 2011.

Peer-reviewed journals

Alex B. Grilo, Iordanis Kerenidis, and Timo Zijlstra. Learning with Errors is easy with quantum samples. *Phys. Rev. A*, 99:032314, 2019, arXiv:1702.08255.

Alex B. Grilo, Iordanis Kerenidis, and Jamie Sikora. QMA with subset state witnesses. *Chicago Journal of Theoretical Computer Science*, 2016(4), March 2016, arXiv:1410.2882.

Pre-prints

Alex B. Grilo, Kathrin Hövelmann, Andreas Hülsing, and Christian Majenz. Tight adaptive reprogramming in the QROM. *Under submission*, 2020, arXiv:2010.15103.

Dorit Aharonov, Alex B. Grilo, and Yupan Liu. StoqMA vs. MA: the power of error reduction. *Under submission*, 2020, arXiv:2010.02835.

Srinivasan Arunachalam, Alex B. Grilo, and Henry Yuen. Quantum statistical query learning. *Under submission*, 2020, arXiv:2002.08240.

Srinivasan Arunachalam, Alex B. Grilo, and Aarthi Sundaram. Quantum hardness of learning shallow classical circuits. *Under submission*, 2019, arXiv:1903.02840. Contributed talk at QIP 2020 (double-track).

Invited talks and courses

QICF 2020 **09/2020**
Hamiltonian complexity meets derandomization

QCrypt 2020 **08/2020**
Zero-Knowledge for QMA from Locally Simulatable Proofs

19th Bellairs's Quantum Crypto-Workshop 2020 **03/2020**
Recent advances in Zero-knowledge proofs in the quantum setting

3rd Quantum Software Consortium General Assembly, Amsterdam **12/2019**
Recent advances in Zero-knowledge proofs in the quantum setting

Workshop "Mathematics of QIT" - Lorentz Center, Leiden **05/2019**
Hamiltonian complexity meets derandomization

18th Bellairs's Quantum Crypto-Workshop 2019 **03/2019**
Quantum proof systems for iterated exponential time, and beyond (with Henry Yuen)

Workshop "Quantum innovators", IQC, University of Waterloo **10/2018**
New schemes for verifiable delegated quantum computation, with quasilinear resources.

Conference talks

QuAlg 2020
- Quantum statistical query learning

QIP 2020
- Stoquastic PCPs vs. Randomness
- Quantum hardness of learning shallow classical circuits

FOCS 2019
- Stoquastic PCPs vs. Randomness
- Perfect zero knowledge for quantum multiprover interactive proofs

ICALP 2019
- A Simple Protocol for Verifiable Delegation of Quantum Computation in One Round

QCrypt 2019
- Perfect zero knowledge for quantum multiprover interactive proofs
- A Simple Protocol for Verifiable Delegation of Quantum Computation in One Round

TQC 2019

- A Simple Protocol for Verifiable Delegation of Quantum Computation in One Round

Eurocrypt 2019

- Verifier-on-a-Leash: New Schemes for Verifiable Delegated Quantum Computation, with Quasilinear Resources

MFCS 2016

- QMA with subset state witnesses

Seminars

Recent advances in Zero-knowledge proofs in the quantum setting

- Quantum information theory seminar, UCL (online) - 07/2020
- Quantum information seminar, MIT (online) - 07/2020
- QuICS, University of Maryland - 11/2019
- QuSoft, CWI - 10/2019

Hamiltonian complexity meets derandomization

- IBM Thomas J. Watson Research Center - 11/2019
- QuantAlgo workshop, CWI - 09/2019
- Weizmann Institute of Science - 04/2019
- Tel-Aviv University - 04/2019
- QuSoft, CWI - 09/2018

Quantum hardness of learning classical shallow circuits

- University of Ottawa - 08/2019
- Hebrew University of Jerusalem - 04/2019

New schemes for verifiable delegated quantum computation.

- IRIF-IQC collaboration workshop - 12/2017
- Junior Seminar of Analysis in Quantum Information Theory, IHP - 11/2017
- Journées GT Informatique Quantique - 11/2017

Learning with Errors is easy with quantum samples.

- University of Hannover - 06/2017

Pointer Quantum PCPs and Multi-Prover Games.

- Hebrew University of Jerusalem - 08/2017
- QuSoft, CWI - 04/2017
- QALGO workshop, University of Cambridge - 04/2016
- Journées GT Informatique Quantique - 11/2015

QMA with subset state witnesses.

- Journées GT Informatique Quantique - 11/2014

Professional services

Editor:

- Quantum

Reviewer:

- Conferences: AQIS, AsiaCrypt, FOCS, QCrypt, QIP, SODA, STOC, TCC
- Journals: QIC, Quantum, SICOMP, TCS

Student representative:

- Departmental Council, IRIF, CNRS/Université Paris Diderot, 2016–2017

- Departmental Council, Institute of Computing, University of Campinas, 2012–2013
- Undergraduate Council, Institute of Computing, University of Campinas, 2010–2011

Teaching Experience

Université Paris Diderot, France
Lecturer

- Computer Science Projects
- Programming for computer networks

Université Paris Diderot, France
Teaching assistant

- Technologies for Internet

University of Campinas, Brazil
Teaching assistant

- Programming Paradigms
- Laboratory of Compilers
- Analysis of Algorithms