# Alex Bredariol Grilo

Alex.Bredariol-Grilo@lip6.fr • abgrilo.github.io/

## 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

## Grants and fellowships

*ANR JCJC - TCS-NISQ* — *October 2022 – September 2026*
Coordinator

*Quantera - QOPT* — *September 2022 – August 2025*
Participant

*ANR PRCE - SecNISQ* — *January 2022 – December 2025*
Participant

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

## Publications

Selected publications are marked with ★

### Peer-reviewed conferences

[C1] ★ Srinivasan Arunachalam, Alex B. Grilo, Tom Gur, Igor C. Oliveira, and Aarthi Sundaram. "Quantum learning algorithms imply circuit lower bounds". In: *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021*. Vol. 12697. Contributed talk at QIP 2021. 2021, pp. 531–561. DOI: 10.1109/FOCS52979.2021.00062. arXiv: 2012.01920.

[C2] Alex B. Grilo, Kathrin Hövelmann, Andreas Hülsing, and Christian Majenz. "Tight adaptive reprogramming in the QROM". In: *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security*. Vol. 13090. Contributed talk at QIP 2021. 2021, pp. 637–667. DOI: 10.1007/978-3-030-92062-3_22. arXiv: 2010.15103.

[C3] ★ Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. "Oblivious Transfer Is in MiniQCrypt". In: *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Vol. 12697. Plenary talk at QIP 2021. 2021, pp. 531–561. DOI: 10.1007/978-3-030-77886-6_18. arXiv: 2011.14980.

[C4] Dorit Aharonov and Alex B. Grilo. "Two Combinatorial MA-Complete Problems". In: *12th Innovations in Theoretical Computer Science Conference, ITCS 2021*. Vol. 185. LIPIcs. 2021, 36:1–36:20. DOI: 10.4230/LIPIcs.ITCS.2021.36. arXiv: 2003.13065.

[C5] ★ Anne Broadbent and Alex B. Grilo. "QMA-hardness of Consistency of Local Density Matrices with Applications to Quantum Zero-Knowledge". In: *61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020*. Invited talk at QCrypt 2020 and Plenary talk at QIP 2021. IEEE, 2020, pp. 196–205. DOI: 10.1109/FOCS46700.2020.00027. arXiv: 1911.07782.

[C6] Gorjan Alagic, Andrew M. Childs, Alex B. Grilo, and Shih-Han Hung. "Non-interactive Classical Verification of Quantum Computation". In: *Theory of Cryptography - 18th International Conference, TCC 2020*. Vol. 12552. Contributed talk at QCrypt 2020 and QIP 2021. 2020, pp. 153–180. DOI: 10.1007/978-3-030-64381-2_6. arXiv: 1911.08101.

[C7] Yfke Dulek, Alex B. Grilo, Stacey Jeffery, Christian Majenz, and Christian Schaffner. "Secure Multi-party Quantum Computation with a Dishonest Majority". In: *EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Contributed talk at QCrypt 2020. 2020, pp. 729–758. DOI: 10.1007/978-3-030-45727-3_25. arXiv: 1909.13770.

[C8] 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*. Contributed talk at QCrypt 2019 and short plenary talk at QIP 2020. 2019, pp. 611–635. DOI: 10.1109/FOCS.2019.00044. arXiv: 1905.11280.

[C9] ★ Dorit Aharonov and Alex B. Grilo. "Stoquastic PCP vs. Randomness". In: *60th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2019*. Short plenary talk at QIP 2020. 2019, pp. 1000–1023. DOI: 10.1109/FOCS.2019.00065. arXiv: 1901.05270.

[C10] 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*. Contributed talk at TQC 2019 and QCrypt 2019. 2019, 28:1–28:13. DOI: 10.4230/LIPIcs.ICALP.2019.28. arXiv: 1711.09585.

[C11] ⋆ 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*. Contributed talk at QIP 2018. 2019, pp. 247–277. DOI: 10.1007/978-3-030-17659-4_9. arXiv: 1708.07359.

[C12] 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*. 2016, 21:1–21:14. DOI: 10.4230/LIPIcs.MFCS.2016.21. arXiv: 1603.00903.

[C13] 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*. 2015, pp. 163–174. DOI: 10.1007/978-3-662-48054-0_14. arXiv: 1410.2882.

[C14] 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*. 2011, pp. 57–60.

### Peer-reviewed journals

[J1] Anne Broadbent and Alex Bredariol Grilo. "QMA-Hardness of Consistency of Local Density Matrices with Applications to Quantum Zero-Knowledge". In: *SIAM Journal on Computing* 51.4 (2022), pp. 1400–1450. DOI: 10.1137/21M140729X. arXiv: 1911.07782.

[J2] Srinivasan Arunachalam, Alex B. Grilo, and Aarthi Sundaram. "Quantum hardness of learning shallow classical circuits". In: *SIAM Journal on Computing* 50.3 (2021). Contributed talk at QIP 2020, pp. 972–1013. DOI: 10.1137/20M1344202. arXiv: 1903.02840.

[J3] Alex B. Grilo, Iordanis Kerenidis, and Timo Zijlstra. "Learning with Errors is easy with quantum samples". In: *Phys. Rev. A* 99 (3 2019), p. 032314. DOI: 10.1103/PhysRevA.99.032314. arXiv: 1702.08255.

[J4] Alex B. Grilo, Iordanis Kerenidis, and Jamie Sikora. "QMA with subset state witnesses". In: *Chicago Journal of Theoretical Computer Science* 2016.4 (Mar. 2016). DOI: 10.4086/cjtcs.2016.004. arXiv: 1410.2882.

### Pre-prints

[P1] Samuel Bouaziz–Ermann, Alex B. Grilo, and Damien Vergnaud. *Quantum security of subset cover problems*. 2022. arXiv: 2210.15396.

[P2] Prabhanjan Ananth and Alex B. Grilo. *Post-Quantum Zero-Knowledge with Space-Bounded Simulation*. 2022. arXiv: 2210.06093.

[P3] Jan Czajkowski and Alex B. Grilo. *On-State Commutativity of Measurements and Joint Distributions of Their Outcomes*. 2021. arXiv: 2210.06093.

[P4] Dorit Aharonov, Alex B. Grilo, and Yupan Liu. *StoqMA vs. MA: the power of error reduction*. 2020. arXiv: 2010.02835.

[P5] Srinivasan Arunachalam, Alex B. Grilo, and Henry Yuen. *Quantum statistical query learning*. 2020. arXiv: 2002.08240.

## Mentoring

**PhD students**:
- Slimane Thabet [2022-] (co-supervised with Elham Kashefi)
- Samuel Bouaziz-Ermann [2021-](co-supervised with Damien Vergnaud)
- Constantin Dalyac [2020-](co-supervised with Elham Kashefi)

**Master/undergrad students**:
- Alan Pulval-Dady [2022] (L3, Sorbonne University)
- Léo Monbroussou [2022] (Telecom ParisTech - co-supervised with Elham Kashefi)
- Dimitrios Tsintsilidas [2021-2022] (Major+MSc in CS, Aristotle University of Thessaloniki)
- Samuel Bouaziz-Ermann [2021] (MPRI, ENS Rennes - co-supervised with Damien Vergnaud)
- Bastien Mignoty [2021] (M1, ENS Lyon)

## Professional services

**Steering comitee**:
- DIM QuanTiP

**Editor**:
- Quantum

**Program commitee**:
- Asiacrypt 2021, ITCS 2022, QIP 2022, QIP 2023, CCC 2023

**Organizer**:
- Quantum in Paris workshop (QuPa) (06/2021)
- Journées Informatique Quantique, Paris (11/2021)

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

## Invited talks and courses

**INTRIQ Spring meeting, Bromont, Canada** **05/2022**
*Quantum learning algorithms imply circuit lower bounds*

**Escola de Tecnologias Quânticas, Campinas, Brazil** **10/2021**
*Introdução à computação quântica*

**Cargese School of Quantum Information and Quantum Technology 2021** **06/2021**
*Introduction to quantum complexity theory*

**11th BIU Winter School on Cryptography** **02/2021**
*Cryptography in a Quantum World: Quantum ZK + MPC*

**Charles River Crypto Day** **02/2021**
*Secure computation is in MiniQCrypt*

**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.*

## Workshop participation

**Extended Reunion: The Quantum Wave in Computing** **06/2022**
*Simons Insitute, UC Berkeley, USA*

**Towards Classically Intractable Quantum Simulations of Physics and Chemistry** **02/2022**
*KITP, UC Santa Barbara, USA*

**Quantum Wave in Computing Reunion** **07/2021**
*Simons Insitute, UC Berkeley, USA (online)*

**Quantum Complexity: Theory and Application** **06/2021**
*Dagstuhl, Germany (online)*

**The Quantum Wave in Computing** **01/2020-05/2020**
*Simons Insitute, UC Berkeley, USA*

**Mathematics of Quantum Information Theory** **05/2019**
*Lorenz Institute, Leiden University, The Netherlands*

**Workshop on QMA(2) and the Complexity of Entanglement** **07/2016**
*QuICS, University of Maryland, USA*

## Conference talks

I list here all the conference talks delivered by me in conferences. For the full list of accepted papers at conferences, see "Publications".

**Eurocrypt 2021**
- Oblivious Transfer is in MiniQCrypt

**QIP 2021**
- Secure Computation is in MiniQCrypt (long plenary talk)
- QMA-hardness of consistency of local density matrices with applications to quantum zero-knowledge (short plenary talk)

**ITCS 2020**
- Two combinatorial MA-complete problems.

**FOCS 2020**
- QMA-hardness of Consistency of Local Density Matrices with Applications to Quantum Zero-Knowledge

**QCrypt 2020**
- Secure Multi-party Quantum Computation with a Dishonest Majority

**QuAlg 2020**
- Quantum statistical query learning

**QIP 2020**
- Stoquastic PCPs vs. Randomness (short plenary talk)
- 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

**Secure Multi-party Quantum Computation with a Dishonest Majority**
- CS seminar at McGill University, Montreal, Canada - 05/2022

**Introduction à l'informatique quantique**
- Seminar for undergraduate students at ENS Lyon - 05/2021

**Secure multi-party computation in MiniQCrypt**
- Colloquium of the CS department at McGill University (online) - 04/2021

**Quantum learning algorithms imply circuit lower bounds.**
- Quantum information theory seminar, UC Berkeley (online) - 12/2020

**StoqMA vs. MA: the power of error reduction**

- Quantum information theory seminar, University of Bristol (online) - 11/2020

**Recent advances in Zero-knowledge proofs in the quantum setting**
- CS Seminar, CQT, Singapore (online) - 05/2022
- 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**
- Quantum PCPs reading group - 04/2021
- 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

## Teaching

**Sorbonne Université, France**

*Lecturer*
- Advanced quantum algorithms (Master of Computer Science, shared with Simon Apers) (Fall 2022)
- Computational complexity (Master of Physics) (Fall 2021)

**Télécom Paristech, France**

*Lecturer (shared with Romain Alléaume)*
- Introduction to quantum computing (Spring 2021)

**Université Paris Diderot, France**

*Lecturer*
- Computer Science Projects (Fall 2017/Spring 2018)
- Programming for computer networks (Spring 2018)