

# Bruno Pasqualotto Cavalar

bruno.cavalar@cs.ox.ac.uk  
<http://brunopc.github.io>

## RESEARCH INTERESTS

---

Computational and circuit complexity theory and their connections to combinatorics, algorithms, learning theory, quantum cryptography and quantum advantage.

## EMPLOYMENT

---

**Research Associate** *July 2024 - now*  
University of Oxford  
Department of Computer Science  
Host: Dr. Ján Pich

## EDUCATION

---

**Ph.D. in Computer Science** *2020 - 2024*  
University of Warwick  
Department of Computer Science  
Advisor: Igor Carboni Oliveira  
Thesis: *Complexity Theory of Classical and Quantum Computational Devices*

**M.Sc. in Computer Science** *2018 - 2020*  
University of Sao Paulo  
Institute of Mathematics and Statistics (IME-USP)  
Advisor: Yoshiharu Kohayakawa  
Thesis: *Sunflower theorems in monotone circuit complexity*

**B.Sc. in Computer Science (with honours)** *2014 - 2017*  
University of Sao Paulo (IME-USP) *Average: 9.1/10*  
Ranked 1st among 37 Computer Science students  
Advisor: Yoshiharu Kohayakawa  
Thesis: *Ramsey-type problems in orientations of graphs*

## FUNDING, DISTINCTIONS AND AWARDS

---

**Best Master Thesis Award:** Winner of the Latin American Master Thesis Contest (CLTM - XXVII) at the Latin American Computing Conference (CLEI 2021). *2021*

**Best Master Thesis Award:** Winner of the Contest of Theses and Dissertations (CTD - XXXIV) at the Congress of the Brazilian Computer Society (CSBC 2021). *2021*

**Alejandro López-Ortiz Best Paper Award:** For the paper *Monotone Circuit Lower Bounds from Robust Sunflowers* at the LATIN 2020 conference, joint work with Benjamin Rossman and Mrinal Kumar. *2021*

**Chancellor's International Scholarship:** Awarded to the 30 most outstanding international PhD applicants to the University of Warwick. *2020*

**Computational Complexity and extremal combinatorics** *September 2018 - August 2020*  
FAPESP Grant for M.Sc. research

**Computational Complexity and extremal combinatorics** *January 2019 - July 2019*  
FAPESP Grant for research internship abroad (University of Toronto)

**Best student award of IME-USP:** Awarded to the best student among all students graduating at IME-USP in a given year, including all majors in Mathematics, Applied Mathematics, Statistics and Computer Science. 2017

**Bridges in Mathematics and Computing**  
FAPESP Grant for undergraduate research

April 2016 - December 2017

**Second place**, in the admission exam of the University of Sao Paulo for undergraduate studies in Computer Science (over 3,500 applicants). 2014

## PUBLICATIONS

---

9. **A Meta-Complexity Characterisation of Quantum Cryptography** 2024  
Bruno P. Cavalar, Eli Goldin, Matthew Gray, Peter Hall  
Proc. **EUROCRYPT**, 2025  
Available at <https://arxiv.org/abs/2410.04984>  
*Brief description:* Obtains the first complexity-theoretic characterisation of a quantum cryptographic task, pioneering connections between quantum cryptography and Kolmogorov complexity.
8. **Boolean Circuit Complexity and Two-Dimensional Cover Problems** 2024  
Bruno P. Cavalar, Igor C. Oliveira  
ACM Transactions on Computation Theory (ACM **ToCT**) 2025  
Available at <https://dl.acm.org/doi/10.1145/3718746>  
*Brief description:* Reduces the problem of showing circuit lower bounds to a cleaner combinatorial problem, offering a new approach to a problem that has seen very little progress in decades.
7. **On the Computational Hardness of Quantum One-wayness** 2023  
Bruno P. Cavalar, Eli Goldin, Matthew Gray, Peter Hall, Yanyi Liu, Angelos Pelecanos  
**Quantum** 9, 1679 (2025).  
Available at <https://arxiv.org/abs/2312.08363>  
*Brief description:* Shows that complexity-theoretic separations are necessary for quantum one-wayness (an important cryptographic task) to be possible. Also proves that pseudorandom states imply one-way state generators in nearly all parameter regimes.
6. **Constant-Depth Circuits vs. Monotone Circuits** 2023  
Bruno P. Cavalar, Igor Carboni Oliveira  
Proc. 38th Computational Complexity Conference (**CCC**), LIPIcs, Vol. 264, 29:1–29:37  
Available at <https://arxiv.org/abs/2305.06821>  
*Brief description:* Proves the first separation between constant-depth circuit classes and monotone circuits, nearly solving an important open problem of 1990. Shows a dichotomy for the monotone complexity of CSPs, implying limitations for communication complexity methods.
5. **Algorithms and Lower Bounds for Comparator Circuits from Shrinkage** 2022  
Bruno P. Cavalar, Zhenjian Lu  
Proc. 13th Innovations in Theoretical Computer Science Conference (**ITCS**), LIPIcs, Vol. 215, 34:1–34:21  
**Algorithmica**, 85(7):2131–2155, 2023  
Available at <https://arxiv.org/abs/2111.14974>  
*Brief description:* Obtains superlinear average-case lower bounds for the strongest circuit classes ever studied, and derives the first algorithms analysing comparator circuits, such as satisfiability algorithms.
4. **Directed graphs with lower orientation Ramsey thresholds** 2021  
Gabriel Ferreira Barros, Bruno P. Cavalar, Yoshiharu Kohayakawa,  
Guilherme Oliveira Mota, Tássio Naia  
Extended Abstracts **EuroComb**, Trends in Mathematics, Vol. 14, 799–804  
**RAIRO-Oper. Res.** 58 (2024) 3607–3619

Available at <https://arxiv.org/abs/2211.07033>

*Brief description:* Constructs graphs for which the probability threshold of their directed Ramsey property is lower than the generic upper bound. Contains part of my undergraduate thesis.

3. **Orientation Ramsey thresholds for cycles and cliques** 2021

Gabriel Ferreira Barros, Bruno P. Cavalar, Yoshiharu Kohayakawa, Tássio Naia

SIAM Journal on Discrete Mathematics (**SIDMA**), 35(4):2844–2857, 2021

Available at <https://arxiv.org/abs/2012.08632>

*Brief description:* Initiates the problem of determining the threshold function for the directed Ramsey property in random graphs. Determines the corresponding threshold for cycles and cliques.

2. **Monotone circuit lower bounds from robust sunflowers** 2020

Bruno P. Cavalar, Mrinal Kumar, Benjamin Rossman

Proc. 14th Latin American Theoretical Informatics Symposium (**LATIN**),

LNCS Vol. 12118, 311–322

Winner of the *Alejandro López-Ortiz Best Paper Award* at LATIN

**Algorithmica**, 84(12):3655–3685, 2022

Available at <https://arxiv.org/abs/2012.03883>

*Brief description:* Obtains the strongest monotone circuit lower bound to-date, improving a 30-year old record, and a tight monotone circuit lower bound for large cliques.

1. **Anti-Ramsey threshold of cycles** 2019

Gabriel Ferreira Barros, Bruno P. Cavalar, Guilherme Oliveira Mota, Olaf Parczyk

Proc. 10th Latin American Algorithms, Graphs and Optimization Symposium (**LAGOS**) 2019,

ENTCS Vol. 346, 89–98

Discrete Applied Mathematics (**DAM**), 323:228–235, 2022

Available at <https://arxiv.org/abs/2006.02079>

*Brief description:* Settles the problem of determining the threshold function for the anti-Ramsey property of cycles in random graphs, whereas previous works only addressed large cycles.

## ACADEMIC VISITS

---

**Lund University and University of Copenhagen**

*October 2023*

Visiting Graduate Student

*Host:* Susanna Rezende

**École Polytechnique Fédérale de Lausanne (EPFL)**

*May 2023 - June 2023*

Visiting Graduate Student

*Host:* Mika Göös

**Simons Institute for the Theory of Computing (UC Berkeley)**

*Jan 2023 - March 2023*

Visiting Graduate Student

*Program:* **Meta-Complexity**

**University of Toronto**

*Jan 2019 - Jul 2019*

International Visiting Graduate Student (IVGS)

*Host:* Benjamin Rossman

## TEACHING ACTIVITIES

---

**University of Warwick**

- *Discrete Mathematics and its Applications 1*

*2022*

Marking and teaching of seminars (~ 10 students).

1st year course for Discrete Mathematics undergraduates.

- *Quantum Computing* 2021, 2022  
Marking and teaching of seminars (~ 40 students).  
Undergraduate and graduate students of Computer Science.
- *Computational Learning Theory* 2021  
Marking and teaching of seminars (~ 20 students).  
Undergraduate and graduate students of Computer Science.
- *Algorithms* 2020  
Teaching of seminars (~ 40 students).  
2nd year course for Computer Science undergraduates.

## University of São Paulo

- *Introduction to Graph Theory* 2020  
Marking and teaching of seminars (~ 20 students).  
Undergraduate/graduate course.
- *Foundations of Data Science* 2019  
Marking and teaching of seminars (~ 20 students).  
Undergraduate/graduate course.
- *Combinatorial Optimization* 2018  
Marking and teaching of seminars (~ 20 students).  
Undergraduate course.
- *Languages, Automata and Computability* 2018  
Marking and teaching of seminars (~ 80 students).  
Graduate course.
- *Introduction to Computer Science* 2015  
Marking and teaching of seminars (~ 40 students).  
1st year undergraduate course.
- *Mathematical Foundations for Computer Science* 2015  
Marking and teaching of seminars (~ 60 students).  
1st year undergraduate course.

## SELECTED TALKS AND SEMINARS

---

### A Meta-Complexity Characterization of Quantum Cryptography

- Quantinuum (London Office)* 2025
- Complexity Network UK (Imperial College London)* 2024

### Constant-depth Circuits vs. Monotone Circuits

- MIAO Seminar (University of Copenhagen)* 2023
- EPFL Theory Coffee Seminar (EPFL)* 2023
- Computational Complexity Conference (CCC)* 2023
- 39th British Colloquium for Theoretical Computer Science (BCTCS)* 2023
- Simons Institute for the Theory of Computing* 2023
- Complexity Network UK (Imperial College London)* 2022

### Algorithms and Lower Bounds for Comparator Circuits from Shrinkage

*13th Innovations in Theoretical Computer Science (ITCS)* 2022

*Complexity Network UK* 2022

**Monotone circuit lower bounds from robust sunflowers**

*37th British Colloquium for Theoretical Computer Science (BCTCS)* 2021

*14th Latin American Theoretical Informatics Symposium (LATIN)* 2021

## LEADERSHIP AND SCIENTIFIC SERVICE

---

### Organisation of events:

- *Warwick-Imperial-Oxford Complexity Network*  
Online and Local Events. Running since December 2021
- Complexity Lunches at Warwick.

**Journal reviewing:** Journal of Graph Theory, Theory of Computing, Random Structures and Algorithms

**Conference reviewing:** Computational Complexity Conference (CCC), Innovations in Theoretical Computer Science (ITCS), Symposium on Theory of Computing (STOC)