João Miguel Lourenço Ribeiro

Address 9129 Gates & Hillman Centers
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213, USA

Website sites.google.com/site/joaorib94/

Email jlourenc@cs.cmu.edu

Updated July 2022

Current Position

Aug 2021 - Carnegie Mellon University, Pittsburgh, PA, USA
Post Doctoral Fellow (Computer Science Department)

Working with Vipul Goyal and Venkatesan Guruswami.

Education

2017-2021 **Imperial College London, UK**

Ph.D. in Computing
Thesis: Coding against synchronisation and related errors
Advisor: Mahdi Cheraghchi

2015-2017 **ETH Zurich, Switzerland**

M.Sc. in Computer Science *(with distinction)*
Track: Theoretical Computer Science
Thesis: Challenges in information-theoretic secret-key agreement
(awarded the ETH Medal for outstanding M.Sc. theses)
Advisor: Ueli Maurer
Final grade: 5.89/6.00

2012-2015 **Instituto Superior Técnico, University of Lisbon, Portugal**

B.Sc. in Applied Mathematics and Computation *(excellent)*
Final grade: 19/20

Previous Positions

Feb 2020 - Mar 2020 University of Michigan, Ann Arbor, MI, USA
Visiting Scholar

Hosted by Mahdi Cheraghchi at the Computer Science and Engineering Department. Topics: information theory and theoretical computer science. Originally planned until May 2020, cut short due to the Covid-19 pandemic.

July 2019 - Aug 2019 University of Illinois at Urbana-Champaign, IL, USA
Visiting Scholar

Hosted by Olgica Milenkovic at the Coordinated Science Laboratory. Topic: coding theory for DNA-based data storage.

Feb 2019 - Apr 2019 Centre for Quantum Technologies, National University of Singapore, Singapore
Research Intern

Hosted by Divesh Aggarwal. Topics: pseudorandomness and information-theoretic cryptography.

July 2018 - Aug 2018 Centre for Quantum Technologies, National University of Singapore, Singapore
Research Intern

Hosted by Divesh Aggarwal. Topics: pseudorandomness and information-theoretic cryptography.

Selected Awards

2018 *ETH Medal*
Awarded by ETH Zurich for an outstanding M.Sc. thesis.

2015 *Excellence Scholarship & Opportunity Award*
Awarded by ETH Zurich to high potential M.Sc. students.

2015 *Professor Jaime Campos Ferreira Prize*
Awarded by the Department of Mathematics of Instituto Superior Técnico for outstanding performance in Mathematics.

2015 *Diploma of Academic Excellence*
Awarded by Instituto Superior Técnico.

2013-2015 *"New Talents in Mathematics" Scholarship*
Awarded by the Calouste Gulbenkian Foundations to 20 outstanding undergraduate students in mathematical subjects in Portugal.

Patents

1. Olgica Milenkovic, Ryan Gabrys, João Ribeiro, Mahdi Cheraghchi. *Coded Trace Reconstruction*. United States Patent Application 17/069,247, filed on October 13, 2020 (Provisional application No. 62/925,332, filed on October 24, 2019), published on April 29, 2021.

Research Papers

All papers are available online at sites.google.com/site/joaorib94, and DOIs or links to preprint versions are also listed below. Author ordering is almost always alphabetical (as usual in theoretical computer science). Works where author ordering has been chosen uniformly at random are signaled by ⓡ. Works with other non-alphabetical author ordering are signaled by ⓞ.

Journal papers

[J1] Gianluca Brian, Antonio Faonio, Maciej Obremski, João Ribeiro, Mark Simkin, Maciej Skórski, and Daniele Venturi. The mother of all leakages: How to simulate noisy leakages via bounded leakage (almost) for free. *IEEE Transactions on Information Theory*, 2022. To appear. Extended version of [C5]. 10.1109/TIT.2022.3193848.

[J2] Divesh Aggarwal, Maciej Obremski, João Ribeiro, Mark Simkin, and Luisa Siniscalchi. Privacy amplification with tamperable memory via non-malleable two-source extractors. *IEEE Transactions on Information Theory*, 68(8):5475–5495, 2022. 10.1109/TIT.2022.3167404.

[J3] Mahdi Cheraghchi, Joseph Downs, João Ribeiro, and Alexandra Veliche. Mean-based trace reconstruction over oblivious synchronization channels. *IEEE Transactions on Information Theory*, 68(7):4272–4281, 2022. Extended version of [C4]. 10.1109/TIT.2022.3157383.

[J4] Mahdi Cheraghchi and João Ribeiro. Non-asymptotic capacity upper bounds for the discrete-time Poisson channel with positive dark current. *IEEE Communications Letters*, 25(12):3829–3832, 2021. 10.1109/LCOMM.2021.3120706.

[J5] Mahdi Cheraghchi and João Ribeiro. An overview of capacity results for synchronization channels. *IEEE Transactions on Information Theory*, 67(6):3207–3232, 2021. 10.1109/TIT.2020.2997329.

[J6] Mahdi Cheraghchi, Ryan Gabrys, Olgica Milenkovic, and João Ribeiro. Coded trace reconstruction. *IEEE Transactions on Information Theory*, 66(10):6084–6103, 2020. Extended version of [C10]. 10.1109/TIT.2020.2996377.

[J7] Mahdi Cheraghchi and João Ribeiro. Sharp analytical capacity upper bounds for sticky and related channels. *IEEE Transactions on Information Theory*, 65(11):6950–6974, Nov 2019. Extended version of [C12]. 10.1109/TIT.2019.2920375.

[J8] Mahdi Cheraghchi and João Ribeiro. Improved upper bounds and structural results on the capacity of the discrete-time Poisson channel. *IEEE Transactions on Information Theory*, 65(7):4052–4068, July 2019. Extended version of [C13]. 10.1109/TIT.2019.2896931.

[J9] ⓞ João Ribeiro, André Souto, and Paulo Mateus. Quantum blind signature with an offline repository. *International Journal of Quantum Information*, 13(02):1550016, 2015. Undergraduate research. 10.1142/S0219749915500161.

Conference papers

[C1] Ryan Gabrys, Venkatesan Guruswami, João Ribeiro, and Ke Wu. Beyond single-deletion correcting codes: Substitutions and transpositions. In *RANDOM 2022*, 2022. To appear. https://arxiv.org/abs/2112.09971.

[C2] ⓡ Jesper Buus Nielsen, João Ribeiro, and Maciej Obremski. Public randomness extraction with ephemeral roles and worst-case corruptions. In *Advances in Cryptology – CRYPTO 2022*, 2022. To appear. https://eprint.iacr.org/2022/237.

[C3] Omar Alrabiah, Eshan Chattopadhyay, Jesse Goodman, Xin Li, and João Ribeiro. Low-degree polynomials extract from local sources. In *49th International Colloquium on Automata, Languages, and Programming (ICALP 2022)*, pages 10:1–10:20, 2022. 10.4230/LIPIcs.ICALP.2022.10.

[C4] Mahdi Cheraghchi, Joseph Downs, João Ribeiro, and Alexandra Veliche. Mean-based trace reconstruction over practically any replication-insertion channel. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 2459–2464, 2021. 10.1109/ISIT45174.2021.9518161.

[C5] Gianluca Brian, Antonio Faonio, Maciej Obremski, João Ribeiro, Mark Simkin, Maciej Skórski, and Daniele Venturi. The mother of all leakages: How to simulate noisy leakages via bounded leakage (almost) for free. In *Advances in Cryptology – Eurocrypt 2021*, pages 408–437, 2021. 10.1007/978-3-030-77886-6_14.

[C6] Divesh Aggarwal, Siyao Guo, Maciej Obremski, João Ribeiro, and Noah Stephens-Davidowitz. Extractor lower bounds, revisited. In *RANDOM 2020*, pages 1:1–1:20, 2020. 10.4230/LIPIcs.APPROX/RANDOM.2020.1.

[C7] Abhishek Agarwal, Olgica Milenkovic, Srilakshmi Pattabiraman, and João Ribeiro. Group testing with runlength constraints for topological molecular storage. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 132–137, 2020. 10.1109/ISIT44484.2020.9174502.

[C8] Divesh Aggarwal, Maciej Obremski, João Ribeiro, Luisa Siniscalchi, and Ivan Visconti. How to extract useful randomness from unreliable sources. In *Advances in Cryptology – Eurocrypt 2020*. 10.1007/978-3-030-45721-1_13.

[C9] Divesh Aggarwal, Ivan Damgård, Jesper Buus Nielsen, Maciej Obremski, Erick Purwanto, João Ribeiro, and Mark Simkin. Stronger leakage-resilient and non-malleable secret sharing schemes for general access structures. In *Advances in Cryptology – CRYPTO 2019*, pages 510–539, 2019. 10.1007/978-3-030-26951-7_18.

[C10] ⓪ Mahdi Cheraghchi, João Ribeiro, Ryan Gabrys, and Olgica Milenkovic. Coded trace reconstruction. In *2019 IEEE Information Theory Workshop (ITW)*, pages 1–5, 2019. 10.1109/ITW44776.2019.8989261.

[C11] Mahdi Cheraghchi and João Ribeiro. Simple codes and sparse recovery with fast decoding. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 156–160, 2019. 10.1109/ISIT.2019.8849702.

[C12] Mahdi Cheraghchi and João Ribeiro. Sharp analytical capacity upper bounds for sticky and related channels. In *2018 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1104–1111, 2018. 10.1109/ALLERTON.2018.8636009.

[C13] Mahdi Cheraghchi and João Ribeiro. Improved capacity upper bounds for the discrete-time Poisson channel. In *2018 IEEE International Symposium on Information Theory (ISIT)*, pages 1769–1773, 2018. 10.1109/ISIT.2018.8437514.

[C14] Daniel Jost, Ueli Maurer, and João L. Ribeiro. Information-theoretic secret-key agreement: The asymptotically tight relation between the secret-key rate and the channel quality ratio. In *2018 Theory of Cryptography Conference (TCC)*, pages 345–369, 2018. 10.1007/978-3-030-03807-6_13.

[C15] Ueli Maurer and João Ribeiro. New perspectives on weak oblivious transfer. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 790–794, 2016. 10.1109/ISIT.2016.7541407.

Manuscripts

[M1] Divesh Aggarwal, Eldon Chung, Maciej Obremski, and João Ribeiro. On secret sharing, randomness, and random-less reductions for secret sharing. https://eprint.iacr.org/2021/802.

[M2] ⓪ Ryan Gabrys, Srilakshmi Pattabiraman, Vishal Rana, João Ribeiro, Mahdi Cheraghchi, Venkatesan Guruswami, and Olgica Milenkovic. AC-DC: Amplification curve diagnostics for Covid-19 group testing. https://arxiv.org/abs/2011.05223.

Talks

1. *Public randomness extraction with ephemeral roles and worst-case corruptions.*
   Indian Institute of Science – Microsoft Research Seminar, August 2022.

2. *Low-degree polynomials, local sources, and a curious log factor.*
   CMU Theory Lunch, March 2022.
   Recording at `https://www.youtube.com/watch?v=eviaYIt_S6M`

3. *The mother of all leakages: How to simulate noisy leakages via bounded leakage (almost) for free.*
   Logic and Computation Seminar, Instituto Superior Técnico, University of Lisbon, June 2022.
   Special in-person workshop at the 2021 Theory of Cryptography Conference, November 2021.

4. *Extractor lower bounds, revisited.*
   Random 2020, August 2020.
   Recording at `https://www.youtube.com/watch?v=JpHcqsqMFr0`

5. *How to extract useful randomness from unreliable sources.*
   Eurocrypt 2020, May 2020.
   Recording at `youtube.com/watch?v=15zsUxU9y2o`

6. *Coded and uncoded trace reconstruction.*
   Shannon Channel (hosted by Salim El Rouayheb), September 2019.
   Recording at `youtube.com/watch?v=mMEeGD6a0qI`

7. *Coded trace reconstruction.*
   2019 IEEE Information Theory Workshop, August 2019.

8. *Simple codes and sparse recovery with fast decoding.*
   2019 IEEE International Symposium on Information Theory, July 2019.

9. *Information-theoretic secret-key agreement and classical bound entanglement.*
   Quantum Computation and Information Seminar, Instituto Superior Técnico, University of Lisbon, February 2019.

10. *Information-theoretic secret-key agreement: The asymptotically tight relation between the secret-key rate and the channel quality ratio.*
    2018 Theory of Cryptography Conference, November 2018.

11. *Sharp analytical capacity upper bounds for sticky and related channels.*
    56th Annual Allerton Conference on Communication, Control, and Computing, October 2018.

12. *Information-theoretic secret-key agreement: The satellite setting.*
    Cryptography Seminar, ETH Zurich, June 2017.

13. *New perspectives on weak oblivious transfer.* 2016 IEEE International Symposium on Information Theory, July 2016.

Teaching Experience

2020 Tutor for the Mathematics I course at Imperial College London. Duties include leading a weekly small-group tutorial and grading weekly assessed coursework.

2018 Graduate Teaching Assistant for the Information & Coding Theory and Algorithms II courses at Imperial College London. Duties included teaching weekly exercise classes, grading midterms, and designing coursework.

2017 Graduate Teaching Assistant for the Information & Coding Theory course at Imperial College London. Duties included teaching weekly exercise classes and grading midterms.

2015-2016 Teaching Assistant for the Discrete Mathematics course at ETH Zurich. Duties included leading a weekly small-group tutorial and grading weekly homework.

Student Mentoring and Supervision

1. Arda Aydın (BSc student, Boğaziçi University). Research project, Fall 2021. Topic: Capacity bounds for the multi-trace deletion channel.

   Next position: PhD student in the ECE Department of the University of Maryland, College Park, MD, USA.

Academic Service

- Co-organizer of the CMU CyLab Crypto Seminar (2021 – present).
- COVID-19 group testing annotated bibliography, edited in collaboration with Laura Balzano, Kyle Gilman, Matthew Malloy, Ivo Stoepker, and Yutong Wang.
- **External reviewer for the following conferences:** CRYPTO (2020, 2021), Eurocrypt (2019, 2020, 2021, 2022), FOCS (2019, 2020), ICALP (2022), ISIT (2017, 2018, 2019, 2020, 2021, 2022), Conference on Information-Theoretic Cryptography (ITC, 2020), ITCS (2019, 2021, 2022), ITW (2019, 2020, 2021, 2022), SODA (2020, 2021), STOC (2018, 2021, 2022), TCC (2018, 2019, 2021), Conference on Security and Cryptography for Networks (SCN, 2020).
- **Reviewer for the following journals:** IEEE Transactions on Information Theory, IEEE Transactions on Communications.

References (in alphabetical order)

1. Divesh Aggarwal, Principal Investigator, Centre for Quantum Technologies, and Associate Professor, School of Computing, National University of Singapore, Singapore.

   email: divesh@comp.nus.edu.sg

2. Mahdi Cheraghchi, Assistant Professor, Computer Science and Engineering Department, University of Michigan, Ann Arbor, MI, USA.

   email: mahdich@umich.edu

3. Vipul Goyal, Associate Professor, Computer Science Department, Carnegie Mellon University, Pittsburgh, PA, USA, and Senior Scientist, NTT Research, Sunnyvale, CA, USA.

   email: vipul@cmu.edu

4. Venkatesan Guruswami, Chancellor's Professor, Department of EECS, Senior Scientist, Simons Institute for the Theory of Computing, and Professor, Department of Mathematics, University of California, Berkeley, CA, USA.

   email: venkatg@berkeley.edu