João Miguel Lourenço Ribeiro

Address   Instituto Superior Técnico
Departamento de Matemática
Gabinete 5.16   **Email**   jribeiro@tecnico.ulisboa.pt
Av. Rovisco Pais 1   **Updated**   August 2024
1049-001 Lisboa, Portugal
Website   sites.google.com/site/joaorib94/

Current Positions

Aug 2024 -   Instituto Superior Técnico – Universidade de Lisboa, Portugal
Professor Auxiliar (U.S. equivalent: Assistant Professor), Department of Mathematics

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)
Advisors: Ueli Maurer and Daniel Jost
Final grade: 5.89/6.00

2012-2015   **Instituto Superior Técnico – Universidade de Lisboa, Portugal**

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

Previous Positions

Feb 2023 -   NOVA School of Science and Technology, Universidade Nova de Lisboa, Portugal
July 2023   *Professor Auxiliar (U.S. equivalent: Assistant Professor), Computer Science Department*

Feb 2023 -   NOVA Laboratory for Computer Science and Informatics (NOVA LINCS)
July 2023   *Integrated Researcher*

Aug 2021 -   Carnegie Mellon University, Pittsburgh, PA, USA
Jan 2023   *Post Doctoral Fellow, Computer Science Department*

Hosted jointly by Vipul Goyal and Venkatesan Guruswami. Part of the Cryptography and Theory groups.

Visiting Positions

30 Jan 2024- Simons Institute for the Theory of Computing, University of California, Berkeley, CA, USA
29 Feb 2024 *Visiting Scientist*

    Invited long-term participant in the Error-Correcting Codes: Theory and Practice semester research program.

Feb 2020 - University of Michigan, Ann Arbor, MI, USA
Mar 2020 *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 - University of Illinois at Urbana-Champaign, IL, USA
Aug 2019 *Visiting Scholar*

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

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

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

July 2018 - Centre for Quantum Technologies, National University of Singapore, Singapore
Aug 2018 *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.

2014-2015 *"New Talents in Mathematics" Scholarship*
Awarded by the Calouste Gulbenkian Foundations to 20 outstanding undergraduate students in mathematical subjects in Portugal.

2013-2014 *"New Talents in Mathematics" Scholarship*
Awarded by the Calouste Gulbenkian Foundations to 20 outstanding undergraduate students in mathematical subjects in Portugal.

Grants

1. Protocol Labs Cryptonet Network Grant: "Stateless Distributed Randomness Generation" (USD 35,000). Co-PI with Chen-Da Liu Zhang (HSLU & Web3 Foundation), Elisaweta Masserova (CMU), Mark Simkin (Ethereum Foundation), Pratik Soni (U Utah), and Sri AravindaKrishnan Thyagarajan (U Sydney).

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. Current status: Pending.

Research Papers

All papers are available online at sites.google.com/site/joaorib94. 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] Huck Bennett, Mahdi Cheraghchi, Venkatesan Guruswami, and João Ribeiro. Parameterized inapproximability of the minimum distance problem over all fields and the shortest vector problem in all ℓ_p norms. *SIAM Journal on Computing*, 2024. To appear. Extended version of [C4]. https://eccc.weizmann.ac.il/report/2022/156/.

[J2] ⓞ Ananthan Nambiar, Chao Pan, Vishal Rana, Mahdi Cheraghchi, João Ribeiro, Sergei Maslov, and Olgica Milenkovic. Semi-quantitative group testing for efficient and accurate qPCR screening of pathogens with a wide range of loads. *BMC bioinformatics*, 25(1):195, 2024. 10.1186/s12859-024-05798-3.

[J3] Mahdi Cheraghchi and João Ribeiro. Simple codes and sparse recovery with fast decoding. *SIAM Journal on Discrete Mathematics*, 37(2):612–631, 2023. Extended version of [C17]. 10.1137/21M1465354.

[J4] Ryan Gabrys, Venkatesan Guruswami, João Ribeiro, and Ke Wu. Beyond single-deletion correcting codes: Substitutions and transpositions. *IEEE Transactions on Information Theory*, 69(1):169–186, 2023. Extended version of [C7]. 10.1109/TIT.2022.3202856.

[J5] Gianluca Brian, Antonio Faonio, João Ribeiro, and Daniele Venturi. Short non-malleable codes from related-key secure block ciphers, revisited. *IACR Transactions on Symmetric Cryptology*, 2022(3):1–19, Sep. 2022. This work has also been presented at the 2023 Fast Software Encryption (FSE) Workshop. 10.46586/tosc.v2022.i3.1-19.

[J6] 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*, 68(12):8197–8227, 2022. Extended version of [C11]. 10.1109/TIT.2022.3193848.

[J7] 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.

[J8] 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 [C10]. 10.1109/TIT.2022.3157383.

[J9] 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.

[J10] 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.

[J11] 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 [C16]. 10.1109/TIT.2020.2996377.

[J12] 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 [C18]. 10.1109/TIT.2019.2920375.

[J13] 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 [C19]. 10.1109/TIT.2019.2896931.

[J14] Ⓞ 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] Maciej Obremski, João Ribeiro, Lawrence Roy, François-Xavier Standaert, and Daniele Venturi. Improved reductions from noisy to bounded and probing leakages via hockey-stick divergences. In *Advances in Cryptology – CRYPTO 2024*, 2024. To appear. https://eprint.iacr.org/2024/1009.

[C2] Chen-Da Liu Zhang, Elisaweta Masserova, João Ribeiro, Pratik Soni, and Sri AravindaKrishnan Thyagarajan. Improved YOSO randomness generation with worst-case corruptions. In *Financial Cryptography and Data Security (FC 2024)*, 2024. To appear.

[C3] Alper Çakan, Vipul Goyal, Chen-Da Liu Zhang, and João Ribeiro. Computational quantum secret sharing. In *18th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2023)*, pages 4:1–4:26, 2023. 10.4230/LIPIcs.TQC.2023.4.

[C4] Huck Bennett, Mahdi Cheraghchi, Venkatesan Guruswami, and João Ribeiro. Parameterized inapproximability of the minimum distance problem over all fields and the shortest vector problem in all ℓ_p norms. In *55th Annual ACM Symposium on Theory of Computing (STOC 2023)*, pages 553–566, 2023. 10.1145/3564246.3585214.

[C5] Vipul Goyal, Chen-Da Liu Zhang, Justin Raizes, and João Ribeiro. Asynchronous multi-party quantum computation. In *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*, pages 62:1–62:22, 2023. 10.4230/LIPIcs.ITCS.2023.62.

[C6] Divesh Aggarwal, Eldon Chung, Maciej Obremski, and João Ribeiro. On secret sharing, randomness, and random-less reductions for secret sharing. In *Theory of Cryptography Conference (TCC) 2022*, pages 327–354, 2022. 10.1007/978-3-031-22318-1_12.

[C7] Ryan Gabrys, Venkatesan Guruswami, João Ribeiro, and Ke Wu. Beyond single-deletion correcting codes: Substitutions and transpositions. In *RANDOM 2022*, pages 8:1–8:17, 2022. 10.4230/LIPIcs.APPROX/RANDOM.2022.8.

[C8] ⓡ Jesper Buus Nielsen, João Ribeiro, and Maciej Obremski. Public randomness extraction with ephemeral roles and worst-case corruptions. In *Advances in Cryptology – CRYPTO 2022*, pages 127–147, 2022. 10.1007/978-3-031-15802-5_5.

[C9] 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.

[C10] 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.

[C11] 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.

[C12] 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.

[C13] 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.

[C14] 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*, pages 343–372, 2020. 10.1007/978-3-030-45721-1_13.

[C15] 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.

[C16] ⓞ 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.

[C17] 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.

[C18] 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.

[C19] 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.

[C20] 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.

[C21] 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.

Preprints

[M1] Omar Alrabiah, Jesse Goodman, Jonathan Mosheiff, and João Ribeiro. Low-degree polynomials are good extractors. https://eccc.weizmann.ac.il/report/2024/093/.

[M2] Alper Çakan, Vipul Goyal, Chen-Da Liu Zhang, and João Ribeiro. Unbounded leakage-resilience and intrusion-detection in a quantum world. https://eprint.iacr.org/2023/410. Accepted as a contributed talk at TQC 2024.

[M3] Naresh Goud Boddu, Vipul Goyal, Rahul Jain, and João Ribeiro. Split-state non-malleable codes and secret sharing schemes for quantum messages. https://arxiv.org/abs/2308.06466. Accepted as a contributed talk at QCRYPT 2023.

Scientific Outreach

1. Scientific committee member for ToPAS 2024, a programming competition for high school students in Portugal.

2. COVID-19 group testing annotated bibliography, edited in collaboration with Laura Balzano, Kyle Gilman, Matthew Malloy, Ivo Stoepker, and Yutong Wang, 2020.

3. Como poupar testes de rastreio: A testagem em grupos como introdução ao método probabilístico (in Portuguese). Article to appear in the Gazeta de Matemática da SPM, 2024.

Selected Talks

1. *Parameterized hardness of coding and lattice problems.*

   - Theory of Computing Seminar, Faculdade de Ciências, University of Lisbon, November 2023.
   - Talks@DCC Seminar, Faculdade de Ciências, University of Porto, May 2023.

2. *Public randomness extraction with ephemeral roles and worst-case corruptions.*

   - Cryptography Seminar, ETH Zurich, July 2023.
   - CRYPTO 2022, August 2022.
     Recording at https://www.youtube.com/watch?v=TGRUGoeRA1g
   - Indian Institute of Science – Microsoft Research Lecture Series, August 2022.
     Recording at https://www.youtube.com/watch?v=zob_q-ck8Qo

3. *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

4. *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.

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

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

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

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

Teaching Experience

As Lead/Co-Instructor

Spring 2024 Lead instructor (regente) for the Theory of Computation course at the NOVA School of Science and Technology, Universidade Nova de Lisboa (FCT-UNL). This course is taught to 2nd year Computer Science BSc students.

Fall 2023 Co-instructor for the Introduction to Programming course at the NOVA School of Science and Technology, Universidade Nova de Lisboa (FCT-UNL). This course is taught to 1st year Computer Science BSc students.

Spring 2023 Instructor for the "Codes and Lattices in Cryptography" informal 5-lecture mini-course at the NOVA School of Science and Technology, Universidade Nova de Lisboa (FCT-UNL). This mini-course was aimed mostly at Masters and PhD students and also faculty of the Department of Mathematics of FCT-UNL. The full set of lecture notes can be found at the course webpage.

Spring 2023 Co-instructor for the Theory of Computation course at the NOVA School of Science and Technology, Universidade Nova de Lisboa (FCT-UNL). This course is taught to 2nd year Computer Science BSc students.

As TA

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

Fall 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.

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

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

Fall 2015   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

Gulbenkian's New Talents in Mathematics Program

This section lists students mentored through the Calouste Gulbenkian Foundation's New Talents in Mathematics (*Novos Talentos em Matemática*) program. This program awards fellowships to outstanding undergraduate students studying mathematical subjects at Portuguese institutions. This fellowship includes undertaking a year-long research project.

1. Mariana Rio Costa (Math, IST-UL), 2023 – 2024. Topic: Complexity of computational problems on point lattices.

MSc theses

1. Gonçalo Cavaco (CS, FCT-UNL), 2024.

BSc research and final projects

1. Pedro Bezerra da Costa (Math BSc final project, IST-UL), 2024.
   Next steps: MFoCS MSc at the University of Oxford.

2. Rui Zhu Wang (Math BSc final project, IST-UL), 2024.
   Next steps: MFoCS MSc at the University of Oxford.

3. Tomás Oliveira (Math BSc final project, IST-UL), 2024.

4. Diogo Carvalho (CS BSc research project, FCT-UNL, co-advised with Alexander Davidson), 2024.

5. Arda Aydın (BSc student, Boğaziçi University), co-advised with Venkatesan Guruswami. Remote research project, 2021.
   Next steps: PhD student in the ECE Department of the University of Maryland, College Park, MD, USA.

Thesis committee membership

1. Thesis defense committee member for Bernardo Ramalho (FEUP). Thesis title: Secure Machine Learning via Homomorphic Encryption. Supervised by Manuel Barbosa and Alberto Pedrouzo. Defended July 17, 2023.

2. Thesis defense committee member for Henrique Navas (IST-UL). Thesis title: Weakly Non-Computable Processes Described by Evolving Recursive Functions. Supervised by José Félix Costa. Defended July 6, 2023.

Academic Service

- Co-organizer of the CMU Cryptography Seminar (08/2021 – 01/2023).

- **Member of the Conference Program Committee for:**

  1. The 28th International Conference on Randomization and Computation (RANDOM 2024).
  2. The 5th Conference on Information-Theoretic Cryptography (ITC 2024).
  3. The 21st IACR Theory of Cryptography Conference (TCC 2023).
  4. The 4th Conference on Information-Theoretic Cryptography (ITC 2023).

- **External reviewer for the following conferences:** CiE (Computability in Europe, 2023), CRYPTO (2020, 2021), Eurocrypt (2019, 2020, 2021, 2022), FOCS (2019, 2020, 2023, 2024), ICALP (2022), ISIT (2017, 2018, 2019, 2020, 2021, 2022, 2023), Conference on Information-Theoretic Cryptography (ITC, 2020), ITCS (2019, 2021, 2022, 2024), 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, Discrete Applied Mathematics.

- Reviewer for AMS Mathematical Reviews (10/2022 – present).

- Reviewer of funding proposals for the Israel Science Foundation (ISF).