MARIE SKŁODOWSKA-CURIE POSTDOCTORAL FELLOWSHIPS 2023

EXPRESSION OF INTEREST FOR HOSTING MARIE CURIE FELLOWS

HOST INSTITUTION

NOVA LINCS and NOVA School of Science and Technology — NOVA University Lisbon

RESEARCH GROUP AND URL

SUPERVISOR (NAME AND E-MAIL)

João Ribeiro (joao.ribeiro@fct.unl.pt)

SHORT CV OF THE SUPERVISOR

João Ribeiro is an Assistant Professor in the Department of Computer Science of the NOVA School of Science and Technology and an integrated researcher at NOVA LINCS. Previously, he was a Post Doctoral Fellow in the Computer Science Department of Carnegie Mellon University, hosted jointly by Vipul Goyal and Venkatesan Guruswami. João received his PhD from the Department of Computing of Imperial College London, where he was advised by Mahdi Cheraghchi. Before that, he received an MSc in Computer Science from ETH Zurich and a BSc in Applied Mathematics and Computation from Instituto Superior Técnico.

He has broad interests within theoretical computer science, with special emphasis on pseudorandomness, coding theory, and cryptography.

More details can be found at https://sites.google.com/site/joaorib94/.

5 SELECTED PUBLICATIONS

1. Huck Bennett, Mahdi Cheraghchi, Venkatesan Guruswami, and João Ribeiro. 2023. Parameterized inapproximability of the minimum distance problem over all fields and the shortest vector problem in all ℓp norms. In 55th Annual ACM Symposium on Theory of Computing (STOC 2023). https://doi.org/10.1145/3564246.3585214. Also available at https://arxiv.org/abs/2211.07900.
2. Omar Alrabiah, Eshan Chattopadhyay, Jesse Goodman, Xin Li, and João Ribeiro. 2022. Low-degree polynomials extract from local sources. In 49th International Colloquium on Automata, Languages, and Programming (ICALP 2022). https://doi.org/10.4230/LIPIcs.ICALP.2022.10. Also available at https://eccc.weizmann.ac.il/report/2022/082/.
3. Gianluca Brian, Antonio Faonio, Maciej Obremski, João Ribeiro, Mark Simkin, Maciej Skórski, and Daniele Venturi. 2021. The mother of all leakages: How to simulate noisy leakages via bounded leakage (almost) for free. In Advances in Cryptology—EUROCRYPT 2021. https://doi.org/10.1007/978-3-030-77886-6_14. Also available at https://eprint.iacr.org/2020/1246.
4. Divesh Aggarwal, Maciej Obremski, João Ribeiro, Luisa Siniscalchi, and Ivan Visconti. 2020. How to extract useful randomness from unreliable sources. In Advances in Cryptology—EUROCRYPT 2020. https://doi.org/10.1007/978-3-030-45721-1_13. Also available at https://eprint.iacr.org/2019/1156.
5. Divesh Aggarwal, Ivan Damgård, Jesper Buus Nielsen, Maciej Obremski, Erick Purwanto, João Ribeiro, and Mark Simkin. 2019. Stronger leakage-resilient and non-malleable secret sharing schemes for general access structures. In Advances in Cryptology–CRYPTO 2019. https://doi.org/10.1007/978-3-030-26951-7_18. Also available at https://eprint.iacr.org/2018/1147.

PROJECT TITLE AND SHORT DESCRIPTION

Super-fast pseudorandomness and applications in cryptography

Pseudorandom objects, such as seeded, two-source, and non-malleable extractors, feature deep connections to several topics in combinatorics and graph theory, and have also found many important applications to cryptography, most notably to leakage-resilient and non-malleable cryptographic schemes. However, known constructions of such objects either have poor parameters, or are highly inefficient in practice. The goals of this project would be to:

1. Study "super-fast" randomness extractors (and possibly other pseudorandom objects) that can be computed by practical algorithms and which work for very weak sources of randomness. This includes both efficient deterministic constructions of such constructions as well as potentially randomized constructions (and the computational complexity of certifying these properties).
2. Investigate both old and new applications of such practically efficient objects in cryptography.

SCIENTIFIC AREA WHERE THE PROJECT FITS BEST*

Mathematics (MAT)

***Scientific Area where the project fits best** – Please select/indicate the scientific area according to the panel evaluation areas: Chemistry (CHE) • Social Sciences and Humanities (SOC) • Economic Sciences (ECO) •

Information Science and Engineering (ENG) • Environment and Geosciences (ENV) • Life Sciences (LIF) • Mathematics (MAT) • Physics (PHY)