Antonio Guimarães

Personal Data

Full name:	Antonio Carlos Guimarães Junior
Nationality:	Brazilian
Email:	antonio.guimaraes@imdea.org
Website:	antonioguimaraes.org
Google Scholar:	scholar.google.com/citations?user=UZzoYYgAAAAJ
GitHub:	github.com/antoniocgj
ORCID:	0000-0001-5110-6639
DBLP:	dblp.org/pid/245/2520

Research

I am an applied cryptographer working on fully homomorphic encryption. I design and implement FHE schemes and protocols that combine conservative assumptions, security against malicious parties and efficiency, with privacy-preserving machine learning as the target application.

Positions

Present | Postdoctoral Researcher
2023 | **IMDEA Software Institute**, Madrid, Spain
Supervisor: Prof. Ignacio Cascudo. Juan de la Cierva fellow (2026–2027).

Education

2023 | Ph.D. in Computer Science
2019 | **University of Campinas**, Campinas, Brazil
Thesis: *Accelerating FHE for arbitrary computation*
Advisor: Prof. Edson Borin – Co-advisor: Prof. Diego F. Aranha – GPA: 4.0/4.0

2023 | Visiting Ph.D. student
2022 | **Aarhus University**, Aarhus, Denmark
Project: *Efficient multi-key homomorphic evaluation for applications in genomics*
Host: Prof. Diego F. Aranha

2019 | M.Sc. in Computer Science
2017 | **University of Campinas**, Campinas, Brazil
Dissertation: *Secure and efficient software implementation of QC-MDPC code-based cryptography*
Advisor: Prof. Diego F. Aranha – Co-advisor: Prof. Edson Borin – GPA: 4.0/4.0

2016 | B.Sc. in Computer Engineering
2012 | **University of Campinas**, Campinas, Brazil
Graduated with **distinction** for high academic performance.
Project: *Instruction set extensions for the secure implementation of cryptographic algorithms*
Advisor: Prof. Diego F. Aranha

Honors, Awards, and Scholarships

2025 | **Juan de la Cierva Postdoctoral Fellowship**
Spanish Ministry of Science, 2024 call, held 2026–2027 (76 600 EUR)

2024 | **Best Ph.D. thesis award**
25th Brazilian Symposium on High-Performance Computing Systems (WSCAD)

2020 | **Best Master's dissertation awards**
20th Brazilian Symposium on Information and Computational Systems Security (SBSeg)
21st Brazilian Symposium on High-Performance Computing Systems (WSCAD)

2019 | **Ph.D. Scholarship**
São Paulo Research Foundation (FAPESP) (∼70 000 USD)

Publications

2027 | Valerio Cini, Antonio Guimarães, Russell W. F. Lai, Michał Osadnik, Ivy K. Y. Woo
Tulva: Practical Asynchronous Threshold FHE
IEEE Symposium on Security and Privacy
IEEE S&P 2027
ePrint 2026/2485 · code

2026 | Ignacio Cascudo, Anamaria Costache, Daniele Cozzo, Dario Fiore, Antonio Guimarães, Eduardo Soria-Vazquez
Batch, Pack, and Prove: More Efficient Verifiable Computation for CKKS
32nd International Conference on the Theory and Application of Cryptology and Information Security
ASIACRYPT 2026
PDF

Antonio Guimarães, Gabriela M. Jacob, Hilder V. L. Pereira
PETCHA: Post-quantum Efficient Transciphering with ChaCha
International Conference on Post-Quantum Cryptography
PQCrypto 2026
ePrint 2026/112 · code

2025 | Nabil Chacal, Antonio Guimarães, Ange Martinelli, Pierrick Méaux, Romain Poussier
Nostalgia Cipher: Can Filtered LFSRs Be Secure Again? An Application to Hybrid Homomorphic Encryption with Sub-50 ms Latency
IACR Transactions on Symmetric Cryptology, 2025(4), 1–30
ToSC 2025
ePrint 2025/2140 · code

Antonio Guimarães, Hilder V. L. Pereira
Fast amortized bootstrapping with small keys and polynomial noise overhead
ACM SIGSAC Conference on Computer and Communications Security
CCS 2025
doi:10.1145/3719027.3765181 · ePrint 2025/686 · code

Ignacio Cascudo, Anamaria Costache, Daniele Cozzo, Dario Fiore, Antonio Guimarães, Eduardo Soria-Vazquez
Verifiable Computation for Approximate Homomorphic Encryption Schemes
45th Annual International Cryptology Conference
CRYPTO 2025
doi:10.1007/978-3-032-01907-3_21 · ePrint 2025/286

Diego F. Aranha, Antonio Guimarães, Clément Hoffmann, Pierrick Méaux
Secure and efficient transciphering for FHE-based MPC
IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025(3), 745–780
TCHES 2025
doi:10.46586/tches.v2025.i3.745-780 · ePrint 2024/1702 · code

Leonardo Neumann, Antonio Guimarães, Diego F. Aranha, Edson Borin
Homomorphic WiSARDs: Efficient Weightless Neural Network training over encrypted data
23rd International Conference on Applied Cryptography and Network Security
ACNS 2025
doi:10.1007/978-3-031-95767-3_12 · code

João Seródio, Antonio Guimarães, Edson Borin
RISC-V Assembly Learning Environment: An extensible web-based platform
Workshop on Computer Architecture Education, Tokyo, Japan
WCAE 2025
doi:10.1145/3743646.3750016 · code

2024

Diego F. Aranha, Anamaria Costache, Antonio Guimarães, Eduardo Soria-Vazquez
HELIOPOLIS: Verifiable Computation over Homomorphically Encrypted Data from Interactive Oracle Proofs is Practical
30th International Conference on the Theory and Application of Cryptology and Information Security
ASIACRYPT 2024
doi:10.1007/978-981-96-0935-2_10 · ePrint 2023/1949 · code

Antonio Guimarães, Edson Borin, Diego F. Aranha
MOSFHET: Optimized Software for FHE over the Torus
Journal of Cryptographic Engineering 14, 577–593
JCEN 2024
doi:10.1007/s13389-024-00359-z · ePrint 2022/515 · code

2023

Antonio Guimarães, Hilder V. L. Pereira, Barry van Leeuwen
Amortized Bootstrapping Revisited: Simpler, Asymptotically-faster, Implemented
29th International Conference on the Theory and Application of Cryptology and Information Security
ASIACRYPT 2023
doi:10.1007/978-981-99-8736-8_1 · ePrint 2023/014 · code

2022

Antonio Guimarães, Leonardo Neumann, Fernanda A. Andaló, Diego F. Aranha, Edson Borin
Homomorphic evaluation of large look-up tables for inference on human genome data in the cloud
2nd Workshop on Cloud Computing, at SBAC-PAD 2022, Bordeaux, France
WCC 2022
doi:10.1109/SBAC-PADW56527.2022.00015

2021

Antonio Guimarães, Edson Borin, Diego F. Aranha
Revisiting the functional bootstrap in TFHE
IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021(2), 229–253
TCHES 2021
doi:10.46586/tches.v2021.i2.229-253 · code

Antonio Guimarães, Luis Lacalle, Charles B. Rodamilans, Edson Borin
High-performance IO for seismic processing on the cloud
Concurrency and Computation: Practice and Experience
CCPE 2021
doi:10.1002/cpe.6250

2020

Rafael J. Cruz, Antonio Guimarães, Diego F. Aranha
Efficient and secure software implementations of Fantomas
Journal of Cryptographic Engineering 10, 211–228
JCEN 2020
doi:10.1007/s13389-019-00218-2 · ePrint 2019/906

2019 | Antonio Guimarães, Edson Borin, Diego F. Aranha
Introducing Arithmetic Failures to Accelerate QC-MDPC Code-Based Cryptography
7th Code-Based Cryptography Workshop, Darmstadt, Germany, Springer LNCS, 44–68
CBC 2019
doi:10.1007/978-3-030-25922-8_3

Antonio Guimarães, Diego F. Aranha, Edson Borin
Optimized implementation of QC-MDPC code-based cryptography
Concurrency and Computation: Practice and Experience, 31(18)
CCPE 2019
doi:10.1002/cpe.5089 · code

2017 | Antonio Guimarães, Diego F. Aranha, Edson Borin
Optimizing the Decoding Process of a Post-Quantum Cryptographic Algorithm
XVIII Simpósio em Sistemas Computacionais de Alto Desempenho
WSCAD 2017
doi:10.5753/wscad.2017.247

Standardization

2026 | **Kryptallage**: thresholdized FHE scheme switching, a unified multi-scheme FHE system with a threshold key-generation and decryption layer (categories S4 and S5), team of 16. First-round submission to the NIST Multi-Party Threshold Cryptography call. [spec]

Tulva: practical asynchronous threshold FHE (category S5), team of 6. First-round submission to the same call. [spec]

Software

MOSFHET: Optimized C library for TFHE: functional, programmable and multi-value bootstrapping, AVX-512 FFT. `github.com/antoniocgj/MOSFHET`
The `vfhe` library: The first open-source library dedicated to verifiable FHE: zero-knowledge proofs, fully homomorphic encryption and related techniques (co-author). `vfhe.ai`
RISC-V ALE: Browser-based RISC-V simulator with virtual devices, built for teaching assembly programming. `github.com/antoniocgj/RISC-V-ALE`
Artifacts: Open-source implementations for most papers above (HELIOPOLIS, amortized bootstrapping, MARGRETHE, Nostalgia, FBT-TFHE, QC-MDPC, …): `github.com/antoniocgj`

Teaching

2019 | Lecturer, teaching internship (PED B)
University of Campinas
Algorithms and Computer Programming (MC102), second semester: main lecturer of a class of 54 students. [course page]

2019
2017 | Teaching Assistant
University of Campinas
Computer Organization and Assembly Language (MC404, 2 semesters); extension courses Big Data (INF617) and Security and Privacy for IoT (INF744), one month each.

2015
2013 | Undergraduate Teaching Assistant
University of Campinas
Algorithms and Computer Programming (MC102, 3 semesters); Computer Organization and Assembly Language (MC404, 2 semesters).

Service

PC member: CHES 2027, FHE.org 2027, ASIACRYPT 2026, CHES 2026, CCS 2026, SAC 2026, WAHC 2026, FHE.org 2026, SBSeg 2025, WAHC 2024
Reviewer: External reviewer or sub-reviewer for CRYPTO, EUROCRYPT, ASIACRYPT, TCHES, PKC, ACNS, FC, ICICS, SBAC-PAD, SoftwareX, ISC, and others

Technical Skills

Programming languages: C, C++, Python, JavaScript, HTML/CSS, Assembly (x86, ARM32, RISC-V)

Programming skills: Profiling and micro-optimization (Intel VTune, perf, Valgrind, gprof); vectorization (intrinsics, inline assembly); multithreading and parallel programming (pthreads, OpenMP); networking (sockets, WebSockets, TLS)

Languages

Portuguese: Native
English: Advanced
Spanish: Intermediate