Antonio Guimarães

Personal Data

Full name:	Antonio Carlos Guimarães Junior
Nationality:	Brazilian
email:	antonio.guimaraes@imdea.org
website:	https://antonioguimaraes.org/
Google Scholar:	https://scholar.google.com/citations?hl=en&user=UZzoYYgAAAAJ

Work

Present | Post-doctoral Researcher
IMDEA Software Institute, Madrid, Spain
Supervisor: Prof. Ignacio Cascudo

Selected Publications

2025

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 (to appear)

Antonio Guimarães and Hilder V. L. Pereira
Fast amortized bootstrapping with small keys and polynomial noise overhead
ACM SIGSAC Conference on Computer and Communications Security
CCS 2025 (to appear)

Diego F. Aranha, Antonio Guimarães, Clément Hoffmann, Pierrick Méaux
Secure and efficient transciphering for FHE-based MPC
Implementation (C): https://github.com/antoniocgj/MARGRETHE
IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025(3), 745-780.
CHES 2025

Leonardo Neumann, Antonio Guimarães, Diego F. Aranha, Edson Borin
Homomorphic WiSARDs: Efficient Weightless Neural Network training over encrypted data
Implementation (C/Rust): https://github.com/antoniocgj/homomorphic-wisards
23rd International Conference on Applied Cryptography and Network Security
ACNS 2025

2024

Diego F. Aranha, Anamaria Costache, Antonio Guimarães, Eduardo Soria-Vazquez
HELIOPOLIS: Verifiable Computation over Homomorphically Encrypted Data from Interactive Oracle Proofs is Practical
Implementation (C/C++/Python): https://github.com/antoniocgj/HELIOPOLIS
30th International Conference on the Theory and Application of Cryptology and Information Security
ASIACRYPT 2024

Antonio Guimarães, Edson Borin, Diego F. Aranha
MOSFHET: Optimized Software for FHE over the Torus
Implementation (Assembly/C): https://github.com/antoniocgj/MOSFHET
Journal of Cryptographic Engineering 14, 577–593, 2024.

2023 | Antonio Guimarães, Hilder V. L. Pereira, Barry van Leeuwen
Amortized Bootstrapping Revisited: Simpler, Asymptotically-faster, Implemented
Implementation (C/C++): https://github.com/antoniocgj/Amortized-Bootstrapping
29th International Conference on the Theory and Application of Cryptology and Information Security
ASIACRYPT 2023

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 (WCC 2022), Bordeaux, France, 2022

2021 | Antonio Guimarães, Edson Borin, Diego F. Aranha
Revisiting the functional bootstrap in TFHE
Implementation (C/C++): https://github.com/antoniocgj/FBT-TFHE
IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021(2), 229-253
CHES 2021

2020 | Rafael Junio, Antonio Guimarães, Diego F. Aranha
Efficient and secure software implementations of Fantomas
Journal of Cryptographic Engineering 10, 211-228, 2020.

2019 | Antonio Guimarães, Edson Borin, Diego F. Aranha
Introducing Arithmetic Failures to Accelerate QC-MDPC Code-Based Cryptography
Implementation (C):
https://github.com/antoniocgj/Optimized-implementation-of-QC-MDPC-code-based-cryptography
7th Code-Based Cryptography Workshop (CBC 2019), Springer, 44-68, Darmstadt, Germany, 2019.

Antonio Guimarães, Diego F. Aranha, Edson Borin
Optimized implementation of QC-MDPC code-based cryptography
Implementation (C):
https://github.com/antoniocgj/Optimized-implementation-of-QC-MDPC-code-based-cryptography
Concurrency and Computation: Practice and Experience, 31(18), 2019.

Education

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

Jan 2023 – Feb 2022 | Visiting Ph.D. student
Aarhus University, Aarhus, Denmark
Project: Efficient multi-key homomorphic evaluation for applications in genomics
Advisor (host): Prof. Diego de Freitas Aranha

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

Dec 2016 – Mar 2012 | Bachelor of Computer engineering
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 de Freitas Aranha
GPA: 84.3/100

Honors and Awards

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

2020 | **Best Master's dissertation award**
20th Brazilian Symposium on Information and Computational Systems Security

2019 | **Best Master's dissertation award**
21st Brazilian Symposium on High-Performance Computing Systems

Activities

PC member: CHES 2026, SBSEG 2025, WAHC 2024
External Reviewer / Sub-reviewer: Crypto, Eurocrypt, Asiacrypt, TCHES, PKC, ACNS, FC, ICICS, SBAC-PAD, SoftwareX, ISC, and others
Teaching: Teaching Assistant for undergraduate and extension courses (Algorithms, Assembly Programming, Big Data, and Security and Privacy for IoT, 2017-2019, University of Campinas), Teaching Internship (Algorithms and Computer Programming, 2019, University of Campinas)

Technical Skills

Programming languages:
Daily use: C, C++, and Python
Proficient: JavaScript, HTML, CSS, Assembly (RISC-V, ARM32, Intel x86)
Familiar: Objective C, Verilog, JAVA, AutoIT, Shell Script.

Programming skills: profiling and micro-optimization (Intel VTune, Valgrind, Gprof, Perf), vectorization (Intrinsics, inline ASM), multithreading/parallel programming (Pthreads, OpenMP), networking (Sockets, WebSockets, TLS)

Languages

Portuguese: Native
English: Advanced