Antonio Carlos Guimarães Junior

Personal Data

email: antonio.guimaraes@ic.unicamp.br
website: antonioguimaraes.org

Education

2019 - present | Ph.D. in Computer Science,
University of Campinas
Advisor: Prof. Edson Borin
Co-advisor: Prof. Diego de Freitas Aranha
GPA: 4.0/4.0

2017 - 2019 | Master in Computer Science,
University of Campinas
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

2012 - 2017 | Bachelor of Computer engineering,
University of Campinas
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

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

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

Publications

2021 | Antonio Guimarães, Edson Borin, Diego F. Aranha
Revisiting the functional bootstrap in TFHE
IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES 2021).

Antonio Guimarães, Luis Lacalle, Charles B. Rodamilans, Edson Borin
High-performance IO for seismic processing on the cloud
Concurrency and Computation: Practice and Experience, 2021;e6250

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

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
Concurrency and Computation: Practice and Experience, 31(18), 2019.

2017 | Antonio Guimarães, Diego F. Aranha, Edson Borin
Optimizing the Decoding Process of a Post-Quantum Cryptographic Algorithm
19th Brazilian Symposium on High-Performance Computing Systems (WSCAD 2017)

2016 | Antonio Guimarães, Edson Borin, Diego F. Aranha
Instruction set extension for the secure implementation of X25519
Undergraduate Research Workshop - In portuguese
16th Brazilian Symposium on Information and Computational Systems Security (SBSeg 2016)

Experience

03/2017 - 12/2019 | Teaching Assistant
Institute of Computing - University of Campinas
1 semester in `MC102: Algorithms and Computer Programming`
2 semesters in `MC404: Computer Organization and Assembly Language`
1 month in `INF617: Big Data` (extension course)
1 month in `INF744: Security and Privacy for IoT` (extension course)
Supervisors: Prof. Ricardo Anido, Prof. Edson Borin, Prof. Diego F. Aranha, and Prof. Islene C. Garcia

02/2016 - 12/2016 | Undergraduate Research
Institute of Computing - University of Campinas
Theme: Prototying of instruction set extensions for side-channel attack mitigation.
Supervisor: Prof. Diego de Freitas Aranha
Funding: Intel Labs and the São Paulo Research Foundation (Grant 14/50704-7).

02/2015 - 02/2016 | iOS app development training
Apple Developer Academy
Eldorado Research Institute, Campinas, Brazil

02/2013 - 12/2015 | Undergraduate Teaching Assistant
Institute of Computing - University of Campinas
3 semesters in `MC102: Algorithms and Computer Programming`
2 semesters in `MC404: Computer Organization and Assembly Language`
Supervisors: Prof. Maria B. F. de Toledo (1s2013), Prof. Eduardo C. Xavier (2s2013), and Prof. Diego F. Aranha (1s2014, 1s2015, and 2s2015)

Languages

Portuguese: Native
English: Advanced

Technical Skills

Proficient: C, Python, JavaScript, and Assembly (RISC-V, ARM 32, and Intel x86) languages.
Familiar: C++, Objective C, HTML, CSS, Verilog, and JAVA languages.