

MATHEUS DE OLIVEIRA SALDANHA

Computer Scientist | Software Engineer

+ (55) 48 99114 1020

matheus@saldanhash.xyz

zinho02

matheus-de-oliveira-saldanha

EDUCATION

- 2018-2022

B.Sc. in Computer Science, Federal University of Santa Catarina (UFSC), Florianópolis, *Grade 8.77*
Emphasis on Digital Certification and Post-Quantum Cryptography.
- 2024-2026

M.Sc. in Computer Science, Federal University of Santa Catarina (UFSC), Florianópolis, *Grade 9.00*
Emphasis on Isogeny-based Cryptography and IoT.
- 2026-2029

P.h.D. in Computer Science, Campinas State University (Unicamp), Campinas
Emphasis on Homomorphic Encryption.

WORK EXPERIENCE

- June 2025

Researcher, LABSEC, Internship
 - Brazilian Civil Registry : focused on solutions to improve information management in the Brazilian Civil Registry, using advanced security and AI techniques to ensure data protection, efficiency, and regulatory compliance.
- September 2024
September 2022

Software Developer , MOTOROLA SOLUTIONS, Full time
 - Emergency Call Handling Simulation : led the design and development of a minimum viable product (MVP) from the ground up, tailored to U.S. clients. The solution significantly improved the testability and reliability of emergency call handling environments.
 - U.S. Jail Management System : focused on the maintenance and enhancement of inmate management software utilized by multiple counties across the country.

JavaC#AngularMongoDBAzure DevOpsDocker
- September 2022
January 2022

Software Developer , CELK SISTEMAS, Full time
 - Health Management Project : aimed at enhancing the quality of Brazil's public healthcare system. Involved in the implementation of large-scale systems across multiple public health agencies nationwide. Contributed as part of a newly formed team that achieved, within the first quarter, the same revenue generated over the entire previous year.

JavaGoWicket FrameworkPostgreSQL
- January 2022
January 2021

Software Developer, LABSEC (UFSC COMPUTER SECURITY LABORATORY), Internship
 - Digital Document Validator : focused on the healthcare sector. Developed a system for validating digitally signed documents, including electronic medical prescriptions. Redesigned the system architecture, resulting in a 50% reduction in maintenance time for affected processes.

JavaBashPostgreSQLGitLab DevOpsDocker
- March 2020
November 2018

Software Developer, LABSEC (UFSC COMPUTER SECURITY LABORATORY), Internship
 - Hawa Certificate Management System : focused on developing software solutions for Certification Authorities. Expanded support for digital signature methods by integrating the system with a hardware cryptographic module, enabling a broader range of secure signature algorithms.

JavaBouncyCastlePostgreSQLGitLab DevOpsDocker

LANGUAGES

PortugueseNative

EnglishFluent

PROGRAMMING SKILLS

Core

Scripting

Others

Java, Go, C#, C, C++
Python, Sage, Bash, Octave/Matlab
Lua, Haskell, Prolog, Scheme, Perl

Assembly

Web

Databases

MIPS, ARM, x86
JavaScript, Angular, CSS, HTML
SQL, MongoDB

AWARDS

- 2018-2020 **National Institute of Information Technology (ITI) Scholarship**
Awarded for contributions to the Hawa Certificate Management System developed at LabSEC.
- 2021-2022 **National Institute of Information Technology (ITI) Scholarship**
Awarded for contributions to the Digital Signature Validator developed at LabSEC.
- 2024-2026 **CAPES Master's Scholarship**
Master's studies funded by the Coordination for the Improvement of Higher Education Personnel (CAPES).
- 2024-2026 **Foundation for Support of Research and University Extension (FAPEU) Scholarship**
Awarded for contributions to the Brazilian Civil Registry developed at LabSEC.

TALKS

- 2025 **Roundtable : Careers in Computing**, Jantar dos Filósofos, UFSC.
Presented insights on research careers in computing to primarily first-year undergrad students.
- 2025 **LabSECDay 25th Anniversary**, LabSEC, UFSC.
Presented the past and ongoing research on LabSEC.
- 2025 **Civil Registry Academic Workshop I**, LabSEC, UFSC.
Presented the latest projects of the Civil Registry in LabSEC.
- 2025 **Civil Registry Academic Workshop II**, LabSEC, UFSC.
Presented the latest projects of the Civil Registry in LabSEC.

TEACHING

- 2024 **Cryptography of Key Exchanges : A Brief Introduction**, Jantar dos Filósofos, UFSC.
Delivered an introductory presentation on DH and ECDH to undergraduate students.
- 2024 **Cryptography of Key Exchanges : From Classic To Post-Quantum**, SECCOM, UFSC.
Taught a mini-course on DH, ECDH, SIDH, and CSIDH key exchange protocols to undergraduate students.
- 2025 **Teaching Internship in Computer Security**, UFSC.
Assisted faculty with instructional activities in the undergraduate Computer Security course.

EVENTS

- 2019 **II Workshop on Quantum Computing**, UFSC.
Talks and Hackathon on Quantum Computing.
- 2019 **SECCOM**, UFSC.
Academic Week of Computing and Information Systems : Talks, Hackathon, and Mini-Courses.
- 2019 **The Developer's Conference**, Florianópolis.
Talks, Workshops, and Networking Events on Software Development and Technology Trends.
- 2024 **IEEE CASS Tour Santa Catarina**, UFSC.
Talks, Technical Sessions, and Networking Events on Circuit Design, Signal Processing, and Emerging Technologies.
- 2024 **SECCOM**, UFSC.
Academic Week of Computing and Information Systems : Talks, Hackathon, and Mini-Courses.
- 2025 **Fq16**, USP São Carlos.
International Conference on Finite Fields and Their Applications 2025 : Talks and Networking Events.
- 2025 **XXV Simpósio Brasileiro de Cibersegurança**, Foz do Iguaçu, PR.
Presentation of the paper *Enhancing LoRaWAN Security: Addressing Static Root Keys with Post-Quantum Cryptography*.
- 2025 **Indocrypt 2025**, IIIT Bhubaneswar, Odisha, India.
Presentation of the paper *Hardened CTIDH : Dummy-Free and Deterministic CTIDH*.

PUBLICATIONS

- 2025 **Matheus Saldanha**, Alexandre Giron, Ricardo Custódio, and Thaís Idalino. 2025. Enhancing LoRaWAN Security : Addressing Static Root Keys with Post-Quantum Cryptography. In Anais do XXV Simpósio Brasileiro de Cibersegurança, setembro 01, 2025, Foz do Iguaçu/PR, Brasil. SBC, Porto Alegre, Brasil, 367-383. DOI : <https://doi.org/10.5753/sbseg.2025.11371>.
- 2025 Banegas, G., Hellenbrand, A., and **Saldanha, M.** (2026). Hardened CTIDH : Dummy-Free and Deterministic CTIDH. In : Dutta, R., De Feo, L., Gangopadhyay, S. (eds) Progress in Cryptology – INDOCRYPT 2025. INDOCRYPT 2025. Lecture Notes in Computer Science, vol 16372. Springer, Cham. https://doi.org/10.1007/978-3-032-13301-4_9