Gustavo Zambonin

About (rev. 20240408)
I am an information security consultant with 7+ years of experience and a solid academic background. I was a former lead of technical research and development for the Brazilian Digital Signature Standard. I specialize in quantum-safe cryptography and public-key infrastructures.

Address zambonin.org · zambonin@pm.me

Languages Portuguese (native), English (fluent), French (beginner)

Professional experience

Information security specialist in partnership with several institutions — Sep/2017–Today

Some of my roles include acting as a consultant on digital signature standards; a ceremony operator deploying e-voting platforms; a quantum-safe blockchain researcher; and a computer forensic examiner measuring the accuracy of pictures from speed enforcement cameras. Maybe I can also help you, get in touch!

Technical lead and researcher at the Computer Security Lab of the Universidade Federal de Santa Catarina (UFSC) — May/2016–Feb/2024

From 2020 onwards, I led the team whose job is to improve, maintain and add features to the Brazilian Digital Signature Standard official implementation, all derived applications, and normative documents. As a result, any Brazilian citizen is able to generate and verify digitally signed files per the latest standards.

Until 2019, as a software developer at that same team, I implemented several large new features to the signature verification service, such as a new responsive web interface, a REST API, and support for verification of CMS signatures.

Education

PhD in Computer Science at UFSC — Mar/2024–Today

Currently researching novel combinatorial (un)ranking algorithms to generate random objects in quantum-safe cryptosystems.

MSc in Computer Science from UFSC (thesis: "On the randomness of Rainbow signatures") — Aug/2018–Sep/2020

I was a visiting researcher at Carleton University under a Mitacs-CALAREO Globalink Research Award, and a teaching assistant at UFSC that taught order theory, lattice theory and algebraic structures.

BSc in Computer Science from UFSC (thesis: "Performance optimization for the Winternitz signature scheme") — Mar/2013–Jul/2018

I was a teaching assistant for a probability and statistics class as a sophomore. Later, as a junior, I started working at the Computer Security Laboratory, developing features for the Brazilian Digital Signature Standard official implementation.

Personal values and interests

I strive to solve problems and deliver elegant solutions with great efficiency, attention to detail, and a minimal number of tools—most likely AWK, Bash, tmux and Vim.

I'm also committed to bring out the best of the people working alongside me, through frequent knowledge transfers and a constant feedback loop.

I'm enthusiastic about astronomy, immersive sim games, IBM keyboards specifically older than myself and most songs with a saxophone line. 8)