Gustavo Zambonin rev. 20230215

About I supervise research and development of the Brazilian Digital Signature Standard, and act as a consultant to a breadth of projects related to information security. 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

Software project manager and researcher at the Computer Security Lab of the Universidade Federal de Santa Catarina (UFSC) — May/2016–Today

I lead 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, we enable any Brazilian citizen to generate and verify digitally signed files according to the latest standards.

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

I have also worked as a consultant on digital signature standards; a ceremony operator deploying Helios-based e-voting platforms; a quantum-safe blockchain researcher; and a computer forensic examiner measuring the accuracy of pictures from speed enforcement cameras.

Education

MSc in Computer Science from UFSC (thesis named 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 named 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)