# Gustavo Zambonin rev. 20191218

zambonin.org · zambonin@pm.me

**About** Quantum-safe cryptography researcher focusing on digital signature schemes, backed by years of contributions to the Brazilian Public-Key Infrastructure standards and a diversified set of projects related to information security.

**Address** Computer Security Laboratory (LabSEC)
Department of Informatics and Statistics, 218
Federal University of Santa Catarina (UFSC)
Florianópolis, Santa Catarina, 88040-900, Brazil

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

## Education

**Aug/2018–Today** **M.Sc. in Computer Science** (PPGCC/UFSC)
- Thesis: Reduction of key sizes on Rainbow-like multivariate signature schemes (expected to finish Jul/2020)

**Mar/2013–Jul/2018** **B.Sc. in Computer Science** (UFSC)
- Thesis: Performance optimization for the Winternitz signature scheme (pt-BR)

## Publications

**Zambonin et al. [2019]** G. Zambonin, M. S. P. Bittencourt, and R. Custódio. Handling Vinegar Variables to Shorten Rainbow Private Keys. In J. Buchmann, A. Nitaj, and T. Rachidi, editors, *Progress in Cryptology – AFRICACRYPT 2019*, volume 11627 of *Lecture Notes in Computer Science*, July 2019. doi: 10.1007/978-3-030-23696-0_20

**Perin et al. [2018]** L. P. Perin, G. Zambonin, D. M. B. Martins, R. Custódio, and J. E. Martina. Tuning the Winternitz Hash-Based Digital Signature Scheme. In *2018 IEEE Symposium on Computers and Communications (ISCC)*, pages 537–542, June 2018. doi: 10.1109/ISCC.2018.8538642

## Academic activities

**Aug/2019–Nov/2019** **Teaching assistance** for INE410134 - Post Quantum Cryptography and Computation
- Guest lecture and consultancy on multivariate cryptography to graduate students

**Mar/2019–Dec/2019** **Co-supervision of B.Sc. thesis**
- M. S. P. Bittencourt. Reducing keys in Rainbow-like signature schemes, December 2019. URL https://repositorio.ufsc.br/handle/123456789/202514

**Aug/2018–Dec/2018** **Teaching assistance** for INE5601 - Mathematical Foundations of Informatics
- Classes on order, lattice and group theory to undergraduate students

**Mar/2015–Aug/2015** **Teaching assistance** for INE5201 - Introduction to Computer Science
- Consultancy on building blocks of programming languages and GNU/Linux

**Oct/2014** **Lecturer** of "Data analysis with SEstatNet" for the 13th SEPEX at UFSC
- Workshop on data analysis and processing with specialized tool

**Jul/2014–Aug/2015** **Teaching assistance** for INE5404 - Probability and Statistics
- Consultancy on exploratory data analysis, probability distributions and events

## Professional experience

**Jan/2018–Today** **Senior software developer** and systems administrator at LabSEC

- In partnership with the Brazilian National Institute of Information Technology (ITI). Major development effort towards the official digital signature validation tool for the Brazilian Public-Key Infrastructure, that resulted in (i) a responsive new web interface; (ii) a clean API that enables headless/batch signature validation; (iii) enforced automated unit testing and continuous deployment practices.

**Oct/2018–Apr/2019** **Security ceremony agent** at LabSEC

- In partnership with public prosecutor's offices. Secure servers were provisioned to run online elections through the end-to-end verifiable voting system Helios, with reduced need for human-computer interaction.

**Sep/2018–Mar/2019** **Researcher** of quantum-safe blockchain protocols at LabSEC

- In partnership with a novel blockchain platform. Co-developed a protocol to quantum-proof a blockchain, with secure substitution of wallets, replacement of cryptographic algorithms and zero downtime for the platform.

**Sep/2017–Apr/2018** **Computer forensic examiner** at LabSEC

- In partnership with an intelligent transportation systems company. A complex data set was processed with native GNU/Linux tools and statistical techniques in order to verify the accuracy of pictures taken by speed enforcement cameras.

**Nov/2016–Dec/2017** **Junior software developer** at LabSEC

- In partnership with a Brazilian digital security company. Developed a proof-of-concept signature validation module for PDF.js and a small library able to easily customize and instantiate most artifacts in a public-key infrastructure.

**May/2016–Oct/2016** **Junior software developer** at LabSEC

- In partnership with the Brazilian National Institute of Information Technology (ITI). Implemented verification modules for CMS and PDF signatures in the official digital signature validation tool for the Brazilian Public-Key Infrastructure.

## Qualifications

**Coding** AWK, Bash, C, C++, gnuplot, Java (JSE, JEE), LaTeX, SageMath, sed

- Python (Flask, gspread, Helios, IPython, Matplotlib, NumPy, PyQt, Requests, robobrowser, Scrapy)

**Environs** GNU/Linux, Vim, IntelliJ Idea, PyCharm, Visual Studio Code

- Management: Ant, Git, GitLab CI/CD, Make, Maven, Subversion

**Software** Clang Tools, Docker, GDB, QEMU, PostgreSQL, SQLite, Valgrind

- Middleware: Apache HTTP Server, Archiva, Tomcat, WildFly