

**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** Laboratório de Segurança em Computação (LabSEC)  
Departamento de Informática e Estatística, 218  
Universidade Federal de Santa Catarina (UFSC)  
Florianópolis, Santa Catarina, 88040-900, Brasil

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

## Education

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

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

## Publications

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*, pages 391–408, July 2019. doi: 10.1007/978-3-030-23696-0\\_20 Zambonin et al. [2019]

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 Perin et al. [2018]

## Academic activities

*Visiting researcher* at Carleton University Mar/2020–  
May/2020  
► Recipient of a Mitacs-CALAREO Globalink Research Award to study the security of Rainbow-like signature schemes

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

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

*Teaching assistance* for INE5601 - Mathematical Foundations of Informatics Aug/2018–  
Dec/2018  
► Classes on order theory, lattice theory, algebraic structures and group theory

*Lecturer* of “Data analysis with SEstatNet” on the 13th SEPEX at UFSC Oct/2014  
► Workshop on data analysis and processing with specialized tool

*Teaching assistance* (undergraduate) for INE5405 - Probability and Statistics Aug/2014–  
Jul/2015  
► Consultancy on exploratory data analysis, probability distributions and events

## Professional experience

<i>Senior software developer</i> and systems administrator at LabSEC	Jan/2018– Today
► 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.	
<i>Security ceremony agent</i> at LabSEC	Oct/2018– Apr/2019
► 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.	
<i>Researcher</i> of quantum-safe blockchain protocols at LabSEC	Sep/2018– Mar/2019
► 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.	
<i>Computer forensic examiner</i> at LabSEC	Sep/2017– Apr/2018
► 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.	
<i>Junior software developer</i> at LabSEC	Nov/2016– Dec/2017
► 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.	
<i>Junior software developer</i> at LabSEC	May/2016– Oct/2016
► 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

### *Programming languages* and frameworks

- Worked with several Python frameworks: Flask, gspread, Helios, IPython, Matplotlib, NumPy, PyQt, Requests, robobrowser, Scrappy. For 5+ years routinely used AWK, Bash, C, C++, gnuplot, Java (JSE, JEE), L<sup>A</sup>T<sub>E</sub>X, Make, SageMath, sed.

### *Software* and environment tools

- GNU/Linux exclusive user for 4+ years, with the following skill set: (i) text editors and IDEs include Vim, IntelliJ Idea, PyCharm; (ii) management software includes Git, GitLab CI/CD, Maven, Subversion; (iii) middleware includes Apache HTTP Server, Archiva, Tomcat, WildFly; (iv) miscellaneous software includes Clang Tools, Docker, GDB, OpenSSL, QEMU, PostgreSQL, SQLite, Valgrind.

## Other interests

Enthusiastic about astronomy, the immersive sim game genre, IBM keyboards specifically older than the author and any song with a saxophone line.