Gustavo Zambonin rev. 20201101

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 Laboratório de Segurança em Computação (LabSEC), INE 218,
Universidade Federal de Santa Catarina (UFSC), Florianópolis, 88040-900, Brasil

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

Education

M.Sc. in Computer Science (UFSC) Aug/2018–Sep/2020

- G. Zambonin. On the randomness of Rainbow signatures. Master's thesis, Universidade Federal de Santa Catarina, Sept. 2020

B.Sc. in Computer Science (UFSC) Mar/2013–Jul/2018

- G. Zambonin. Otimização de desempenho do esquema de assinatura digital Winternitz. Bachelor's thesis, Universidade Federal de Santa Catarina, June 2018

Academic activities

Visiting researcher at Carleton University (Ottawa, Canada) Mar/2020–Jun/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. Bachelor's thesis, Universidade Federal de Santa Catarina, Nov. 2019

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

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

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

Professional experience

Software project manager at LabSEC

Jan/2020–Today

- In partnership with the Brazilian National Institute of Information Technology (ITI). Coordinates the development of desktop, web and mobile tools used in the Brazilian Public-Key Infrastructure (ICP-Brasil) to generate and validate digital signatures.

Security ceremony agent at LabSEC

Oct/2018–Apr/2019

- In partnership with several public institutions. Secure servers are provisioned to run online elections through the end-to-end verifiable voting system Helios, with reduced need for human-computer interaction.

Senior software developer and systems administrator at LabSEC

Jan/2018–Dec/2019

- In partnership with ITI. Major development effort towards the official digital signature verification tool of ICP-Brasil, that resulted in a responsive new web interface, an API that enables headless/batch signature verification, enforced automated unit testing and continuous deployment practices.

Researcher 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.

Junior software developer at LabSEC

Nov/2016–Dec/2017

- In partnership with a Brazilian digital security company. Developed a proof-of-concept signature verification module for PDF.js and a customizable library to create artifacts in a public-key infrastructure.

Junior software developer at LabSEC

May/2016–Oct/2016

- In partnership with ITI. Implemented support for CMS signatures (standalone or embedded in PDFs) in the official digital signature verification tool of ICP-Brasil.

Qualifications

Programming languages and frameworks

- Worked with several Python frameworks: Flask, gspread, Helios, IPython, Matplotlib, NumPy, PyQt, Requests, robobrowser, Scrapy. For 5+ years routinely used AWK, Bash, C, C++, gnuplot, Java (JSE, JEE), LaTeX, 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.