# Gustavo Zambonin

**About** (rev. 20241218) — 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)

## 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.

## Publications

G. Zambonin, R. Custódio, L. Moura, and D. Panario. Faster combinatorial primitives for efficient hash-based signatures. In preparation.

J. P. C. Barbosa, G. Zambonin, T. B. Idalino, and R. Custódio. Practical Implementation of a Post-Quantum E-voting Protocol. In preparation.

A. B. Kamers, P. de Oliveira Abel, T. B. Idalino, G. Zambonin, and J. E. Martina. Practical algorithms and parameters for modification-tolerant signature scheme (extended version). Submitted to the Journal of the Brazilian Computer Society.

J. E. Martina, L. G. Rosa, and G. Zambonin. From Cat Videos to Catfish: The Case for a New Social Authentication Era. Submitted to SPW 2025 (Twenty-ninth International Workshop on Security Protocols).

W. Silvano, L. Mayr, G. Zambonin, and R. Custódio. Balancing Transparency, Immutability, and Secrecy in Blockchain: Extending Shannon's Secrecy. In preparation.

L. G. Rosa, G. Zambonin, and J. E. Martina. Enhanced SIM swap security practices via ceremony modeling. Submitted to AINA 2025 (39th International Conference on Advanced Information Networking and Applications).

L. Mayr, G. Zambonin, F. Schardong, and R. Custódio. One-Time Certificates for Reliable and Secure Document Signing, Aug. 2024. https://doi.org/10.48550/arXiv.2208.03951.

A. B. Kamers, P. de Oliveira Abel, T. B. Idalino, G. Zambonin, and J. E. Martina. Practical algorithms and parameters for modification-tolerant signature scheme. In A. Santin and R. Machado, editors, *Proceedings of the 24th Brazilian Symposium on Information and*

*Computational Systems Security (SBSeg 2024)*, pages 522–537, Sept. 2024. https://doi.org/10.5753/sbseg.2024.241677.

G. de Castro Biage, G. Zambonin, T. B. Idalino, D. Panario, and R. Custódio. A concrete LIP-based KEM with simple lattices. *IEEE Access*, 12:16408–16420, Jan. 2024. https://doi.org/10.1109/ACCESS.2024.3358670.

L. Mayr, L. Palma, G. Zambonin, W. Silvano, and R. Custódio. Monitoring key pair usage through distributed ledgers and one-time signatures. *Information*, 14(10):523–537, Sept. 2023. https://doi.org/10.3390/info14100523.

L. P. Perin, G. Zambonin, R. Custódio, L. Moura, and D. Panario. Improved constant-sum encodings for hash-based signatures. *Journal of Cryptographic Engineering*, 11(4):329–351, June 2021. https://doi.org/10.1007/s13389-021-00264-9.

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. https://doi.org/10.1007/978-3-030-23696-0_20.

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. https://doi.org/10.1109/ISCC.2018.8538642.

## 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.

## 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)