

Gustavo Zambonin

About

(rev. 20261024)

I am an information security consultant with 10+ 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)

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.

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 (see thesis at [12])

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 (see thesis at [15])

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)

- [1] M. Tomaszewski, G. Zambonin, J. E. Martina, and R. Custódio. nth: Open-Source Generic Combinatorial (Un)ranking via the Symbolic Method. In B. Mourrain and I. Kotsireas, editors, *Mathematical Software – ICMS 2026*, volume 16677 of *Lecture Notes in Computer Science*, to appear, July 2026.
- [2] G. Zambonin, L. G. Rosa, R. Custódio, and D. Panario. Cryptographic applications of combinatorial ranking algorithms for integer compositions. In F. Foucaud and A. Parreau, editors, *Combinatorial Algorithms (IWOCOA 2026)*, volume 16587 of *Lecture Notes in Computer Science*, pages 515–530, June 2026. DOI: [10.1007/978-3-032-27731-2_36](https://doi.org/10.1007/978-3-032-27731-2_36).
- [3] G. Zambonin, T. Siqueira, L. G. Rosa, R. A. M. Stefanés, R. Custódio, and D. Panario. Combinatorial ranking algorithms for the general linear group. In C. Martínez and L. Moura, editors, *LATIN 2026: Theoretical Informatics*, *Lecture Notes in Computer Science*, to appear, Apr. 2026.
- [4] A. B. Kamers, G. Zambonin, T. B. Idalino, P. de Oliveira Abel, and J. E. Martina. Partial integrity, authenticity and belongingness using modification-tolerant signature schemes. *Journal of the Brazilian Computer Society*, 32(1):343–362, Mar. 2026. DOI: [10.5753/jbcs.2026.5565](https://doi.org/10.5753/jbcs.2026.5565).
- [5] J. P. C. Barbosa, G. Zambonin, T. B. Idalino, and R. Custódio. From ElGamal to Lattice-Based: Enhancing the Helios Voting System with Quantum-Safe Cryptography. In M. Fischlin and V. Moonsamy, editors, *Applied Cryptography and Network Security (ACNS 2025)*, volume 15287 of *Lecture Notes in Computer Science*, pages 29–49, June 2025. DOI: [10.1007/978-3-031-95767-3_2](https://doi.org/10.1007/978-3-031-95767-3_2).
- [6] L. G. Rosa, G. Zambonin, and J. E. Martina. Enhanced SIM Swap Security Practices via Ceremony Modeling. In L. Barolli, editor, *Advanced Information Networking and Applications (AINA 2025)*, volume 249 of *Lecture Notes on Data Engineering and Communications Technologies*, pages 201–211, Apr. 2025. DOI: [10.1007/978-3-031-87775-9_17](https://doi.org/10.1007/978-3-031-87775-9_17).
- [7] L. G. Rosa, G. Zambonin, and J. E. Martina. From Cat Videos to Catfish: The Case for a New Social Authentication Era. In F. Stajano, M. Lomas, V. Matyas, and J. Anderson, editors, *Security Protocols XXIX*, volume 16628 of *Lecture Notes in Computer Science*, to appear, Mar. 2025.
- [8] 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. DOI: [10.5753/sbseg.2024.241677](https://doi.org/10.5753/sbseg.2024.241677).
- [9] 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. DOI: [10.1109/ACCESS.2024.3358670](https://doi.org/10.1109/ACCESS.2024.3358670).
- [10] 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. DOI: [10.3390/info14100523](https://doi.org/10.3390/info14100523).
- [11] 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. DOI: [10.1007/s13389-021-00264-9](https://doi.org/10.1007/s13389-021-00264-9).
- [12] G. Zambonin. *On the randomness of Rainbow signatures*. Master’s thesis, Universidade Federal de Santa Catarina, Oct. 2020. URL: <https://repositorio.ufsc.br/handle/123456789/219497>.
- [13] 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](https://doi.org/10.1007/978-3-030-23696-0_20).
- [14] 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](https://doi.org/10.1109/ISCC.2018.8538642).
- [15] G. Zambonin. *Otimização de desempenho do esquema de assinatura digital Winternitz*. (Performance optimization of the Winternitz digital signature scheme). Bachelor’s thesis, Universidade Federal de Santa Catarina, June 2018. URL: <https://repositorio.ufsc.br/handle/123456789/187875>.