

Education

Technische Universiteit Eindhoven **Eindhoven, Netherlands**
PhD in Computer Science and Mathematics (Cryptography) *Oct/2015–Nov/2019*

- Title: *Constructive and Destructive Approaches to Post-Quantum Cryptography*
- Supervisors: Professor Tanja Lange & Professor Daniel J. Bernstein
- Summary: In my Ph.D. thesis, I studied the construction of code-based cryptosystems that are secure against quantum computers. First, I showed how to explore a side-channel attack against some current code-based cryptosystems. Second, I showed how to recover the key of a cryptosystem using a reaction attack. Third, I studied the application of quantum algorithms where I showed the constraints to build a quantum circuit. Furthermore, I gave a quantum algorithm for finding preimages of a hash function.

UFSC - Federal University of Santa Catarina **Florianópolis, Brazil**
Master in Computer Science *Sep/2012–Oct/2015*

- Title: *Irreducible Pentanomials over \mathbb{F}_{2^m} to improve the modular reduction*
- Supervisors: Professor Ricardo Custódio & Professor Daniel Panário
- Summary: In my master thesis I studied the impact of irreducible polynomials in the arithmetic of finite fields. Our primary focus was to speed up the lower operations in binary ECC. Lately, I found a new class of irreducible pentanomials that are able to reduce the number of gates. Also, I provide analysis of the complexity in pentanomials in the polynomial modular arithmetic over \mathbb{F}_{2^m} .

UFSC - Federal University of Santa Catarina **Florianópolis, Brazil**
Bachelor in Computer Science *Sep/2007–Sep/2012*

- Title: *Framework for Brazilian PKI*
- Supervisor: Professor Ricardo Custódio
- Summary: We developed a framework for the Brazilian PKI. In this work we used software engineering techniques creating first a high level description of the needs of the PKI and lately it was implemented in C++.

UDESC - State University of Santa Catarina **Florianópolis, Brazil**
Bachelor in Public Administration *2006–2008 (incomplete)*

Work Experience

Qualcomm **Sophia Antipolis, France**
Senior Cryptographer *Jul/2022 – Current*

- Development of post-quantum cryptography on Snapdragon processors, included but not limited to:
 - Design and develop specific hardware for post-quantum cryptography.
 - Development of new attacks to post-quantum cryptography (side-channel attacks).
 - Development of counter measurements against side-channel attacks.
 - Speed-up implementations on Cortex-M3 and M4.
 - Development of post-quantum cryptography to RISC-V.

INRIA and École polytechnique **Paris, France**
Post-doc *Dec/2020 – Jul/2022*

- Development of Post-quantum cryptography in Embedded Devices:
 - Development of new attacks to post-quantum cryptography (side-channel attacks).
 - Development of counter measurements against side-channel attacks.
 - Speed-up implementations of cryptography signatures to RIOT-OS.

Chalmers University of Technology **Gothenburg, Sweden**
Post-doc *Nov/2019 – Nov/2020*

- Development of WASP Project:
 - Development of new attacks to post-quantum cryptography.
 - Development of post-quantum cryptography.
 - Development of verifiable functions.

Chalmers University of Technology
Research Assistant

Gothenburg, Sweden
Sep/2019 – Nov/2019

- Development of WASP Project:
 - Development of new attacks to post-quantum cryptography.
 - Development of post-quantum cryptography.
 - Development of verifiable functions.

Cryptoexperts
Intern

Paris, France
Sep/2018 – Nov/2018

- Side channel attacks on Post-Quantum cryptography implementations.
 - Detected leakage of timing in operations to develop timing attacks.

Riscure
Intern

Delft, Netherlands
Feb/2017 – Apr/2017

- Side channel attacks on ECC implementations.
 - Investigated attacks in implementations of ECC in FPGAs using power analysis.

BRy Tecnologia
System Analyst

Florianópolis, Brazil
Oct/2014 – Sep/2015

- Software for Public Key Infrastructure (PKI).
 - Developed software in Java and C++.
 - Integrated HSM in Java applications.
 - Managed a team using Scrum.

LabSEC - Laboratory for Computer Security
Researcher, Project Manager and Developer

Florianópolis, Brazil
Nov/2009 – Oct/2014

- Researcher in cryptography, project manager and developer of security software, using *Java*, *C/C++*, and *Python*.
 - Researched cryptography applied to PKI.
 - Managed the project reference for the Brazilian PKI.
 - Managed the project involving the definition of attribute certification in Brazil.
 - Developed software in C/C++, Java and Python.

Pixeon Medical Systems
Intern

Florianópolis, Brazil
Feb/2009 – Nov/2009

- Tester of medical imaging software.
 - Learned application of unit tests (JUnit).
 - Executed manual tests in the software.

Publications

Gustavo Banegas, Valerie Gilchrist, Anaëlle Le Dévéhat, and Benjamin Smith. Fast and frobenius: Rational isogeny evaluation over finite fields. *Cryptology ePrint Archive*, Paper 2023/995, 2023. <https://eprint.iacr.org/2023/995>.

Gustavo Banegas, Juliane Krämer, Tanja Lange, Michael Meyer, Lorenz Panny, Krijn Reijnders, Jana Sotáková, and Monika Trimoska. Disorientation faults in CSIDH. In *Advances in Cryptology–EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23–27, 2023, Proceedings, Part V*, pages 310–342. Springer, 2023.

Gustavo Banegas and Ricardo Villanueva-Polanco. On recovering block cipher secret keys in the cold boot attack setting. *Cryptography and Communications*, pages 1–25, 2023.

Estuardo Alpírez Bock, Gustavo Banegas, Chris Brzuska, Łukasz Chmielewski, Kirthivaasan Puniamurthy, and Milan Šorf. Breaking dpa-protected kyber via the pair-pointwise multiplication. *Cryptology ePrint Archive*, Paper 2023/551, 2023. <https://eprint.iacr.org/2023/551>.

Gustavo Banegas, Valerie Gilchrist, and Benjamin Smith. Efficient supersingularity testing over GF(p) and CSIDH key validation. *Mathematical Cryptology*, 2(1):21–35, Oct. 2022.

Gustavo Banegas, Koen Zandberg, Emmanuel Baccelli, Adrian Herrmann, and Benjamin Smith. Quantum-resistant software update security on low-power networked embedded devices. In Giuseppe Ateniese and Daniele Venturi, editors, *Applied Cryptography and Network Security - 20th International Conference, ACNS 2022, Rome, Italy, June 20-23, 2022, Proceedings*, volume 13269 of *Lecture Notes in Computer Science*, pages 872–891. Springer, 2022.

Gustavo Banegas, Daniel J. Bernstein, Fabio Campos, Tung Chou, Tanja Lange, Michael Meyer, Benjamin Smith, and Jana Sotáková. CTIDH: faster constant-time CSIDH. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021(4):351–387, Aug. 2021.

Gustavo Banegas, Thomas Debris-Alazard, Milena Nedeljković, and Benjamin Smith. Wavelet: Code-based postquantum signatures with fast verification on microcontrollers. Cryptology ePrint Archive, Report 2021/1432, 2021. <https://ia.cr/2021/1432>.

Carlo Brunetta, Georgia Tsaloli, Bei Liang, Gustavo Banegas, and Aikaterini Mitrokotsa. Non-interactive, secure verifiable aggregation for decentralized, privacy-preserving learning. In Joonsang Baek and Sushmita Ruj, editors, *Information Security and Privacy*, pages 510–528, Cham, 2021. Springer International Publishing.

Georgia Tsaloli, Bei Liang, Carlo Brunetta, Gustavo Banegas, and Aikaterini Mitrokotsa. DEVA: Decentralized, Verifiable Secure Aggregation for Privacy-Preserving Learning. In Joseph K. Liu, Sokratis Katsikas, Weizhi Meng, Willy Susilo, and Rolly Intan, editors, *Information Security*, pages 296–319, Cham, 2021. Springer International Publishing.

Gustavo Banegas, Daniel J. Bernstein, Iggy van Hoof, and Tanja Lange. Concrete quantum cryptanalysis of binary elliptic curves. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021(1):451–472, Dec. 2020.

Gustavo Banegas, Paulo S. L. M. Barreto, Edoardo Persichetti, and Paolo Santini. Designing efficient dyadic operations for cryptographic applications. *J. Math. Cryptol.*, 14(1):95–109, 2020.

Bei Liang, Gustavo Banegas, and Aikaterini Mitrokotsa. Statically aggregate verifiable random functions and application to e-lottery. *Cryptography*, 4(4), 2020.

Georgia Tsaloli, Gustavo Banegas, and Aikaterini Mitrokotsa. Practical and provably secure distributed aggregation: Verifiable additive homomorphic secret sharing. *Cryptography*, 4(3):25, 2020.

Gustavo Banegas, Paulo S. L. M. Barreto, Brice Odilon Boidje, Pierre-Louis Cayrel, Gilbert Ndolane Dione, Kris Gaj, Cheikh Thiécoumba Gueye, Richard Haeussler, Jean Belo Klamti, Ousmane Ndiaye, Duc Tri Nguyen, Edoardo Persichetti, and Jefferson E. Ricardini. DAGS: reloaded revisiting dyadic key encapsulation. In *Code-Based Cryptography - 7th International Workshop, CBC 2019, Darmstadt, Germany, May 18-19, 2019, Revised Selected Papers*, pages 69–85, 2019.

Douglas Marcelino Beppler Martins, Gustavo Banegas, and Ricardo Felipe Custódio. Don't forget your roots: Constant-time root finding over \mathbb{F}_{2^m} . In *Progress in Cryptology - LATINCRYPT 2019 - 6th International Conference on Cryptology and Information Security in Latin America, Santiago de Chile, Chile, October 2-4, 2019, Proceedings*, pages 109–129, 2019.

Simona Samardjiska, Paolo Santini, Edoardo Persichetti, and Gustavo Banegas. A reaction attack against cryptosystems based on LRPC codes. In *Progress in Cryptology - LATINCRYPT 2019 - 6th International Conference on Cryptology and Information Security in Latin America, Santiago de Chile, Chile, October 2-4, 2019, Proceedings*, pages 197–216, 2019.

Gustavo Banegas, Paulo SLM Barreto, Brice Odilon Boidje, Pierre-Louis Cayrel, Gilbert Ndolane Dione, Kris Gaj, Cheikh Thiécoumba Gueye, Richard Haeussler, Jean Belo Klamti, Ousmane N'diaye, Duc Tri Nguyen, Edoardo Persichetti, and Jefferson Ricardini. DAGS: key encapsulation using dyadic GS codes. *Journal of Mathematical Cryptology*, 12(4):221–239, 2018.

Gustavo Banegas, Paulo SLM Barreto, Edoardo Persichetti, and Paolo Santini. Designing efficient dyadic operations for cryptographic applications. *IACR Cryptology ePrint Archive*, 2018(650), 2018.

Gustavo Banegas, Ricardo Custódio, and Daniel Panario. A new class of irreducible pentanomials for polynomial-based multipliers in binary fields. *Journal of Cryptographic Engineering*, Online first:1–15, 2018.

Gustavo Banegas and Daniel J Bernstein. Low-communication parallel quantum multi-target preimage search. In *International Conference on Selected Areas in Cryptography*, volume 10719 of *LNCS*, pages 325–335. Springer, 2017.

Gustavo Banegas. Attacks in stream ciphers: A survey. Cryptology ePrint Archive, Report 2014/677, 2014. <https://eprint.iacr.org/2014/677>.

Program Committee Member

CBCrypto: 2020, 2021

CHES: 2022, 2023, 2024

Eurocrypt: 2022

LatinCrypt: 2023

Asiacrypt: 2023

ACNS: 2024

External Reviewer

CRYPTO: 2022

Asiacrypt: 2018, 2019, 2020, 2021

FSE: 2021

LatinCrypt: 2021

SPACE: 2020

PQCrypto: 2018

Software

Wavelet: <https://github.com/wavelet/>

CTIDH: <http://ctidh.isogeny.org/software.html>

DAGS Key encapsulation: https://github.com/gbanegas/dags_v2

HSS/LMS hash-based signatures: <https://github.com/gbanegas/sphss>

More code: <https://github.com/gbanegas/>

Program Languages

Basic: PERL, VHDL, SYSTEMVERILOG,, HASKELL, RUST

Intermediate: GO

Advanced: PYTHON, C, C++, JAVA

Projects

ECRYPT-NET Project

Marie Skłodowska-Curie ITN (Integrated Training Network)

Fellow
<https://www.ecrypt.eu.org/net/>

- Fellow PhD from 2015 to 2019.

WASP expedition project Massive, Secure,
and Low-Latency Connectivity for IoT Applications
Wallenberg AI, Autonomous Systems and Software Program

Researcher

- Fellow researcher from 2019 to 2020.

Teaching Experience

Universidade Federal de Santa Catarina (Online)
Special Class

Florianópolis, Brazil
2021–2021

- Introduction to Quantum computation, Grover's Algorithm and Shor's Algorithm.

Chalmers University of Technology
Special Class

Gothenburg, Sweden
2020–2020

- Taught Textbook RSA (The Factoring Problem) and Primality test, replacing Prof. Katerina Mitrokotsa.

Chalmers University of Technology
Special Class

Gothenburg, Sweden
2020–2020

- Taught Attacks against Block Ciphers and Introduction to Public Key Cryptography (PKC), replacing Prof. Katerina Mitrokotsa.

Chalmers University of Technology
Special Class

Gothenburg, Sweden
2020–2020

- Taught Block Ciphers and Operation Modes, replacing Prof. Katerina Mitrokotsa.

Chalmers University of Technology
Special Class

Gothenburg, Sweden
2020–2020

- Taught the unit on Sigma protocols, replacing Prof. Katerina Mitrokotsa.

Technische Universiteit Eindhoven
Tutor

Eindhoven, Netherlands
2018–2019

- Tutor of "Introduction to cryptology".

Technische Universiteit Eindhoven
Tutor

Eindhoven, Netherlands
2017–2018

- Tutor of "Introduction to cryptology".

Technische Universiteit Eindhoven
Tutor

Eindhoven, Netherlands
2017–2018

- Tutor of "Basic Mathematics".

Technische Universiteit Eindhoven
Tutor

Eindhoven, Netherlands
2017–2018

- Tutor of "cryptology".

Technische Universiteit Eindhoven
Tutor

Eindhoven, Netherlands
2016–2017

- Tutor of "Algebra and discrete mathematics".

Technische Universiteit Eindhoven
Tutor

Eindhoven, Netherlands
2016–2017

- Tutor of "cryptology".

Supervision

Master Theses

Iggy van Hoof: Concrete quantum-cryptanalysis of binary elliptic curves,
Eindhoven University of Technology
2019

Bachelor Theses

David Brandberg, Lisa Fahlbeck, Henrik Hellström, Hampus Karlsson, John Kristoffersson, Lukas Sandman: End-to-end Encrypted Instant Messaging Application,
Chalmers University of Technology
2020

Languages

Portuguese: Native

English: Advanced

Spanish: Nivel medio

Fluent (Speaking, Reading, Writing)

Nivel medio (Conversación, Lectura), Nivel bajo (Escritura)

Extra-curricular Activities

AIESEC

Global Internship Program

Budapest, Hungary

Dec/2014–Feb/2015

- Volunteer work in the Global Internship Program with AIESEC, living two months working and helping in a daycare.