Gustavo Banegas | Curriculum Vitae

✉ gustavo@cryptme.in • www.cryptme.in

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

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

- Development of Post-quantum cryptography in Embbeded Devices:
  - Development of new attacks to post-quantum cryptography (side-channel attacks).
  - Development of counter measurements against side-channel attacks.
  - Speed-up implementations and add 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 **Gothenburg, Sweden**
Research Assistant *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 **Paris, France**
Intern *Sep/2018 – Nov/2018*

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

Riscure **Delft, Netherlands**
Intern *Feb/2017 – Apr/2017*

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

BRy Tecnologia **Florianópolis, Brazil**
System Analyst *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 **Florianópolis, Brazil**
Researcher, Project Manager and Developer *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 **Florianópolis, Brazil**
Intern *Feb/2009 – Nov/2009*

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

Publications

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`.

Gustavo Banegas, Koen Zandberg, Adrian Herrmann, Emmanuel Baccelli, and Benjamin Smith. Quantum-resistant security for software updates on low-power networked embedded devices. Cryptology ePrint Archive, Report 2021/781, 2021. `https://eprint.iacr.org/2021/781`.

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. 2021. To Appear ISC 2021. https://isc2021.petra.ac.id/papers.

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.

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 Ndollane 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 Ndollane 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

Eurocrypt: 2022

External Reviewer

Asiacrypt: 2018, 2019, 2020, 2021

LatinCrypt: 2021

SPACE: 2020

FSE: 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

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

Program Languages

Basic: Perl, VHDL, Ruby, Haskell, Rust

Intermediate: GO

Advanced: Python, C, C++, Java

Projects

ECRYPT-NET Project **Fellow**
Marie Skłodowska-Curie ITN (Integrated Training Network) *https://www.ecrypt.eu.org/net/*

- Fellow PhD from 2015 to 2019.

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

- Fellow researcher from 2019 to 2020.

Teaching Experience

Universidade Federal de Santa Catarina (Online) **Florianópolis, Brazil**
Special Class *2021–2021*

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

Chalmers University of Technology **Gothenburg, Sweden**
Special Class *2020–2020*

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

Chalmers University of Technology **Gothenburg, Sweden**
Special Class *2020–2020*

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

Chalmers University of Technology **Gothenburg, Sweden**
Special Class *2020–2020*

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

Chalmers University of Technology **Gothenburg, Sweden**
Special Class *2020–2020*

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

Technische Universiteit Eindhoven **Eindhoven, Netherlands**
Tutor *2018–2019*

- Tutor of "Introduction to cryptology".

Technische Universiteit Eindhoven **Eindhoven, Netherlands**
Tutor *2017–2018*

- Tutor of "Introduction to cryptology".

Technische Universiteit Eindhoven **Eindhoven, Netherlands**
Tutor *2017–2018*

- Tutor of "Basic Mathematics".

Technische Universiteit Eindhoven **Eindhoven, Netherlands**
Tutor *2017–2018*

- Tutor of "cryptology".

Technische Universiteit Eindhoven **Eindhoven, Netherlands**
Tutor *2016–2017*

- Tutor of "Algebra and discrete mathematics".

Technische Universiteit Eindhoven **Eindhoven, Netherlands**
Tutor *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 — *Fluent (Speaking, Reading, Writing)*

Spanish: Nivel medio — *Nivel medio (Conversación, Lectura), Nivel bajo (Escritura)*

French: Niveau Basique — *Bon (Parle, Lis, Écrire)*

Extra-curricular Activities

AIESEC — **Budapest, Hungary**
Global Internship Program — *Dec/2014–Feb/2015*

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