Launching Packages 2025
Protecting Hardware Impletations

Gustavo Banegas
Inria & LIX, École Polytechnique de Paris
gustavo.souza-banegas@polytechnique.edu

1 Résumé du Scientifique

Once a quantum computer capable of running Shor's algorithm [5] is built, currently deployed public-key cryptography **will be catastrophically and irreversibly broken**, exposing all past and future encrypted communications. In response, there is a global effort to develop cryptographic systems resistant to quantum attacks, known as Post-Quantum Cryptography (PQC). Research in PQC has intensified, particularly following the launch of the United States National Institute of Standards and Technology (NIST) PQC standardization project in 2016. However, participation in this project is global, and most countries follow its standards (including the Europe Union).

The development of cryptographic schemes follows a structured process: (1) It begins with the establishment of computational hardness assumptions through mathematical analysis, providing the theoretical foundation for security. (2) These foundations enable the design of cryptographic primitives that leverage secure trapdoor functions, forming the basis of new encryption and signature schemes. (3) Once the theoretical groundwork is laid, algorithms are formally specified and prototyped, leading to reference implementations. (4) The final stage involves integrating these solutions into real-world applications, ensuring their adoption through production-ready implementations.

While schemes like Kyber and Dilithium (two post-quantum schemes) have reached advanced stages, post-quantum cryptography remains an active research area with *critical challenges*. Following NIST's 2023 announcement of additional digital signature candidates, improving efficiency and **hardening implementations against side-channel attacks (SCA)** have become **crucial**. As cryptographic schemes transition from theory to practice, their security in real-world deployments depends not only on their mathematical foundations but also on their resilience to physical attacks. Strengthening implementations against SCA is mandatory to preventing adversaries from extracting secret information through power analysis, electromagnetic leakage, or fault injection. This aspect of PQC is essential for secure adoption in applications such as hardware security modules, IoT devices, and vehicular communication—where attackers have physical access and SCA defenses are not optional but necessary.

The goal of this project is to ensure cryptographic security beyond mathematical guarantees by evaluating and strengthening its resistance to physical attacks.

Security Analysis of Post-Quantum Schemes

Cryptosystems face vulnerabilities to SCA, wherein an adversary can deduce confidential information from physical observations, such as timing, electromagnetic emanation, or power consumption, made during the execution of computations using sensitive data [1–3]. These attacks can be classified as passive, where the a dversary simply observes leaked information without interfering, or active, where faults are intentionally injected to manipulate computations and extract secrets [4, 6]. Both types pose serious threats and have been successfully employed across various applications, often proving challenging to detect.

Exploring SCA requires specialized equipment and training, as the methodologies and countermeasures are highly dependent on the targeted cryptosystem. While techniques exist to mitigate these attacks, many are intrinsic to specific schemes and lack easy adaptability to others. Consequently, securing each implementation demands a unique approach, necessitating expertise in both cryptographic engineering and side-channel analysis. Unfortunately, the pool of individuals capable of combining these essential skills remains limited to a select group of professionals.

Methodology

The proposed methodology comprises three interdependent phases designed to bridge gaps in hardware security and achieve practical implementation robustness:

1. Systematic Vulnerability Analysis

- Investigation targets: NIST PQC candidates (Round 4, Additional Call), Korean PQC, and China PQC.
- Attack methodologies:
  - *Passive*: Time analysis, and Differential power analysis (DPA)
  - *Active*: Clock and voltage glitching

2. Adaptive Countermeasure Design

- Algorithm-aware protection strategies:
  - Masking: Implementing runtime techniques to obscure sensitive data and operations without compromising efficie;
  - Fault tolerant operations: : Designing systems capable of maintaining functionality and security in the presence of induced faults.

3. Quantitative Security Benchmarking

Metric	Evaluation Methodology
Side-channel resistance	Practical approach and Test Vector Leakage Assessment (TVLA)
Computational overhead	Cycle count analysis vs. baseline specifications

More specifically, The methodology comprises the following steps: (1) *Attack surface enumeration* involves identifying targets, assessing potential side-channel vulnerabilities, and evaluating these targets using Husky and CW-Lite boards. (2) *Countermeasure prototyping* will be done by tailoring an algorithmic countermeasure to the attack and then it will be implemented in a software and hardware. (3) *Validation* will involve implementing and measure the software countermeasure on Cortex-M3 and M4 processors, and the hardware countermeasure on FPGAs, followed by testing on PolarFire and Xilinx platforms.

To achieve our objectives, we will need to acquire the materials listed in Table 1. Additionally, I plan to hire a PhD student to develop a framework for side-channel analysis and cryptographic hardware security.

Impacts and Outcomes

Impacts on École Polytechnique de Paris. Producing new knowledge in the hardware security domain aligns with the objectives of the cybersecurity program at *École Polytechnique de Paris*, which aims to equip students with advanced expertise in cryptographic security, hardware security, and side-channel analysis. By fostering research and innovation in these critical areas, the program contributes to the development of next-generation security professionals capable of addressing emerging threats in cryptography and beyond.

Table 1: Budget for hardware equipment.

Hardware	Usage	Qty	Total Price (€)	Link
Husk Board	Side-channel acquisition / fault attack	2	1,060	Mouser
Server	Run analysis and store the data acquired by the boards.	1	3,100	
Polarfire FPGA	Development of specific hardware for cryptography	1	150	Microchip
Arty S7: Spartan-7 FPGA	Development of specific hardware for cryptography	1	300	Digilent
CW-lite ARM	Small ARM board for side-channel attacks	2	700	NewAE
Nucleo ARM	Board with Cortex-M3/M4 (NUCLEO-F207ZG/NUCLEO-L4R5ZI)	4	400	Mouser
PicoScope 3000E	Oscilloscope	1	4,225	PicoTech
Wires / Cables / Others	Connection with oscilloscope, soldering kit, etc.	1	700	
——	——	——	10,635	——

Industrial Impact. Establishing connections with industry, particularly in embedded security and hardware-based cryptographic implementations, to evaluate the practical adoption of countermeasures. My experience at Qualcomm provides a strong foundation for building future collaborations. Additionally, I have connections with professionals such as Matthieu Rivain and Sonia Belaïd from CryptoExperts, as well as Christine Cloostermans at NXP, facilitating real-world feedback and further industrial partnerships.

Publications and scientific outcome. Targeting top-tier cryptography and security conferences and journals such as CHES, EUROCRYPT, ASIACRYPT, IEEE Transactions on Information Forensics and Security, and the Journal of Cryptographic Engineering. Moreover, other satellite conferences, such as CASCADE, also focus on related topics.

Scientific Collaborations. Engaging in academic collaborations with international early-career researchers, including Monika Trimoska (TU/e, Netherlands) and Fábio Campos(H-BRS, Germany), as well as continuing partnerships with other international researchers like Chris Brzuska (Aalto, Finland) and Łukasz Chmielewski (Masaryk University, Czech Republic). Additionally, initiating a project with local researcher Guénaël Renault. Participation in research workshops and summer schools, such as the Summer School on Real-World Cryptography and Privacy, is also planned.

Funding Prospects. The plan is to establish this project, set up the necessary equipment, consolidate the results, and then prepare an application for funding from the E uropean Research Council (ERC) and the French National Research Agency (ANR). This proposal will also support the formation of a new group, Éclair, which originates from the former GRACE team.

Budget. Table 1 details the essential equipment required for comprehensive security evaluation of post-quantum cryptographic implementations. The hardware selection addresses three critical operational needs: (1) precise side-channel measurement capabilities, (2) target device programmability for various cryptographic schemes, and (3) high-speed signal acquisition infrastructure.

The *PhD student position* is planned for a duration of three years, with a total salary of €75,000. Additionally, we have allocated €4,000 per year for the student to attend international conferences such as Eurocrypt and CHES, as well as summer schools. This brings the total estimated cost to €87,000.

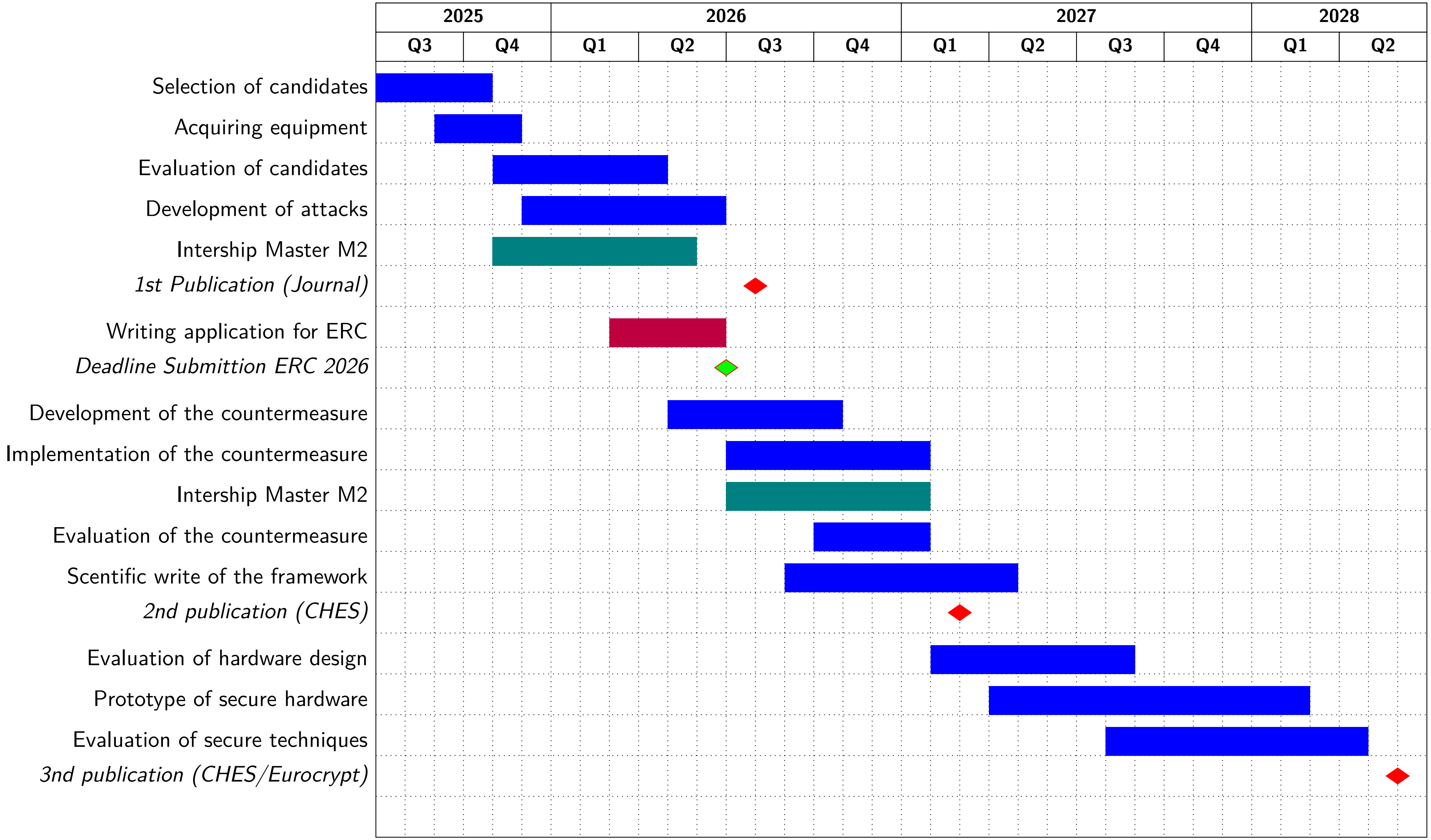
Regarding internship opportunities, we can host master's students for six-month projects. The main goal is to familiarize them with side-channel attacks through smaller projects, such as data acquisition and analysis or the implementation of countermeasures for cryptographic schemes. For such, X will be destinated to pay for the internship.

Therefore, the total estimated cost for the PhD student is €87,000, the costs for internship is estimated in X, and the overall project cost, including equipment, is €97,635 + X. FIXME

Table 2: Budget Breakdown

Category	**Details**	**Amount**
Personnel	1 PhD	€XXX
	2 x 6-month M2 interns	€XXX
Equipment	Hardware	10,635
	Laptop for PhD	–
Travel	International conference (Overseas)	€3K/year
	International conference (Europe)	€2K/year
	National workshops & seminars	€1K/year
Total		€XXX

2 Calendar


2025
2026
2027
2028
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
Selection of candidates
Acquiring equipment
Evaluation of candidates
Development of attacks
Intership Master M2
1st Publication (Journal)
Writing application for ERC
Deadline Submittion ERC 2026
Development of the countermeasure
Implementation of the countermeasure
Intership Master M2
Evaluation of the countermeasure
Scentific write of the framework
2nd publication (CHES)
Evaluation of hardware design
Prototype of secure hardware
Evaluation of secure techniques
3nd publication (CHES/Eurocrypt)

CV - Gustavo Banegas

Current position: INRIA ISFP & Lecturer at École Polytechnique de Paris
Personal Webpage
gustavo.souza-banegas@polytechnique.edu

Education

PhD in Computer Science and Mathematics (Oct/2015–Nov/2019)
Technische Universiteit Eindhoven, Eindhoven, Netherlands
Title: Constructive and Destructive Approaches to Post-Quantum Cryptography
Supervisors: Professor Tanja Lange & Professor Daniel J. Bernstein

Master in Computer Science (Sep/2012–Oct/2015)
UFSC - Federal University of Santa Catarina, Florianópolis, Brazil
Title: Irreducible Pentanomials over $\mathbb{F}_{2^m}$ to improve the modular reduction
Supervisors: Professor Ricardo Custódio & Professor Daniel Panário

Bachelor in Computer Science (Sep/2007–Sep/2012)
UFSC - Federal University of Santa Catarina, Florianópolis, Brazil
Supervisor: Professor Ricardo Custódio

Professional Experience

Start	End	Institution	Position and status
01/10/2024	Current	INRIA	ISFP (Cryptography Researcher)
01/06/2022	30/09/2024	Qualcomm (France)	Senior Cryptographer
01/12/2020	30/05/2022	INRIA Saclay (France)	Post Doc
01/11/2019	30/11/2020	Chalmers University of Technology (Sweden)	Post Doc
01/11/2015	12/11/2019	Technische Universiteit Eindhoven (Netherlands)	Ph.D. Candidate
01/09/2018	01/12/2018	CryptoExperts (France)	Internship
01/02/2017	01/05/2017	Riscure (Netherlands)	Internship
01/10/2014	31/10/2015	Bry Tecnologia (Brazil)	Software Engineer

Supervision

Master Thesis

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

Bachelor Lab Project

Sigurjon Agustsson, *Montgomery Reduction in RSA*, École Polytechnique, 2021.

Bachelor Thesis

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

Intern at Qualcomm

Liana Koleva, *Vectorization of HQC on RISC-V architecture*, 2023.

Scientific Responsabilities

Table 3: Conference Involvement

Role	Conferences and Years
Program Committee Member	AsiaCCS: 2025 Communications in Cryptology: 2025 CBCrypto: 2020, 2021 CHES: 2022, 2023, 2024 Eurocrypt: 2022 LatinCrypt: 2023, 2025 Asiacrypt: 2023 ACNS: 2024 PQCrypto: 2025
External Reviewer	CRYPTO: 2022, Asiacrypt: 2018, 2019, 2020, 2021, FSE: 2021, LatinCrypt: 2021, SPACE: 2020, PQCrypto: 2018 Design, Codes and Cryptography Springer Nature Quantum Information Processing Springer Nature Scientific Reports IEEE Transactions on Quantum Engineering, IEEE Access, IEEE Transactions on Circuits and Systems I: Regular Papers, IEEE Communications Letters, IEEE Transactions on Information Forensics and Security, Springer Algorithmica

Table 4: Workshop Organization

Event	Year
Quantum Research Retreat	2018
Quantum Research Retreat	2016

Selected Publications

For a full list of publications see: Google Scholar, Personal Website or DBLP.

1. Estuardo Alpirez Bock, Gustavo Banegas, Chris Brzuska, Łukasz Chmielewski, Kirthivaasan Puniamurthy, and Milan Šorf. Breaking DPA-protected Kyber via the pair-pointwise multiplication. *ACNS 2024. Lecture Notes in Computer Science*, vol 14584.

2. Gustavo Banegas, Valerie Gilchrist, Anaëlle Le Dévéhat, and Benjamin Smith. Fast and Frobenius: Rational isogeny evaluation over finite fields. *LATINCRYPT 2023. Lecture Notes in Computer Science*, vol 14168.

3. Gustavo Banegas, Juliane Krämer, Tanja Lange, Michael Meyer, Lorenz Panny, Krijn Reijnders, Jana Sotáková, and Monika Trimoska. Disorientation faults in CSIDH. *International Conference on the Theory and Applications of Cryptographic Techniques* - EUROCRYPT. Springer. 2023.

4. 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* - CHES, 2021(4):351–387, 2021.

5. 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* - CHES, 2021(1):451–472, 2020.

6. 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 Ricardini. DAGS: Key encapsulation using dyadic GS codes. *Journal of Mathematical Cryptology*, 12(4):221–239, 2018.

7. 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.

8. Gustavo Banegas and Daniel J. Bernstein. Low-communication parallel quantum multi-target preimage search. *SAC 2017. Lecture Notes in Computer Science*, vol 10719, pp. 325–335.

In cryptography, it is common to author list in alphabetical order. We usually follow the cultural statement of American Mathematical Society.

Teaching

Special Class (2021) — Universidade Federal de Santa Catarina (Online), Florianópolis, Brazil
Taught Quantum Computation, Grover's Algorithm, and Shor's Algorithm.

Special Classes (2020) — Chalmers University of Technology, Gothenburg, Sweden
Taught various cryptography topics, replacing Prof. Katerina Mitrokotsa:

- RSA and Primality Testing
- Attacks on Block Ciphers and Intro to PKC
- Block Ciphers and Operation Modes
- Sigma Protocols

Tutor (2016–2019) — Technische Universiteit Eindhoven, Netherlands
Tutor for courses including:

- Introduction to Cryptology
- Basic Mathematics
- Algebra and Discrete Mathematics

Software

- **WAVE**: `github.com/wavesign/wave`
- **Wavelet**: `github.com/wavelet/`
- **CTIDH**: `ctidh.isogeny.org/software.html`
- **DAGS Key Encapsulation**: `github.com/gbanegas/dags_v2`
- **HSS/LMS Hash-Based Signatures**: `github.com/gbanegas/sphss`
- **More Code**: `github.com/gbanegas/`

References

[1] David Brumley and Dan Boneh. Remote timing attacks are practical. *Computer Networks*, 48(5):701–716, 2005.

[2] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael Wiener, editor, *Advances in Cryptology — CRYPTO' 99*, pages 388–397, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

[3] Paul C. Kocher, Joshua Jaffe, Benjamin Jun, and Pankaj Rohatgi. Introduction to differential power analysis. *J. Cryptogr. Eng.*, 1(1):5–27, 2011.

[4] Jörn-Marc Schmidt and Christoph Herbst. A practical fault attack on square and multiply. In *2008 5th Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 53–58, 2008.

[5] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[6] Ingrid Verbauwhede, Dusko Karaklajic, and Jorn-Marc Schmidt. The fault attack jungle - a classification model to guide you. In *2011 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 3–8, 2011.