APP

Gustavo Banegas

1 Résumé du Scientifique

Research in post-quantum cryptography (PQC) has intensified significantly since the launch of the National Institute of Standards and Technology (NIST) PQC standardization project in 2016. The development lifecycle of cryptographic schemes can be categorized into four key phases:

1. **Mathematical Foundations**: Establishing the computational hardness of underlying mathematical problems through rigorous theoretical analysis;
2. **Scheme Construction**: Designing cryptographic primitives that utilize these mathematical foundations to create secure trapdoors functions;
3. **Algorithm Specification & Prototyping**: Developing formal algorithm descriptions and reference implementations, culminating in standardized specifications;
4. **Deployment & Integration**: Implementing production-ready solutions and fostering ecosystem adoption through standardization efforts.

While many schemes, such as Kyber and Dilithium, have reached stages three or four, PQC research remains an active field. There are still numerous open problems and challenges, particularly following NIST's announcement of new candidates for post-quantum signatures in 2023. Additionally, enhancing efficiency and strengthening implementations against side-channel attacks (SCA) are ongoing priorities. It is also essential to adapt PQC to current applications, including communication protocols, hardware security modules (HSM), and various scenarios such as the Internet of Things (IoT) and vehicular communication.

In this research project, I will delineate the challenges that PQC confronts in terms of its security evaluation regarding its physical aspects. While presenting these challenges, I will put forth a proposal outlining strategies to address the evaluation of security and measurement of the countermeasures against side-channel 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, 2]. 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 [3, 4]. 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	Test Vector Leakage Assessment (TVLA) with $t > 4.5$ threshold
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 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, Outcomes, and Ambitions

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.

The results of this research will contribute to the broader scientific community by:

Publications. 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.

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	4	400	
PicoScope 3000E	Oscilloscope	1	4,225	PicoTech
Wires / Cables / Others	Connection with oscilloscope, soldering kit, etc.	1	700	
––	––	––	10,635	––

Conferences & Collaborations. Engaging in academic collaborations with international early-career researchers, including Monika Trimoska and Fábio Campos, as well as continuing partnerships with other international researchers like Chris Brzuska and Łukasz Chmielewski. 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.

Industrial Impact. Establishing connections with industry stakeholders, particularly in embedded security and hardware-based cryptographic implementations, to assess the practical adoption of countermeasures. My background with Qualcomm facilitates establishing connections for future collaborations. Moreover, I have connections with professionals like Matthieu Rivain and Sonia Belaïd from CryptoExperts, and with Christine Cloostermans at NXP, opening avenues for further industrial partnerships.

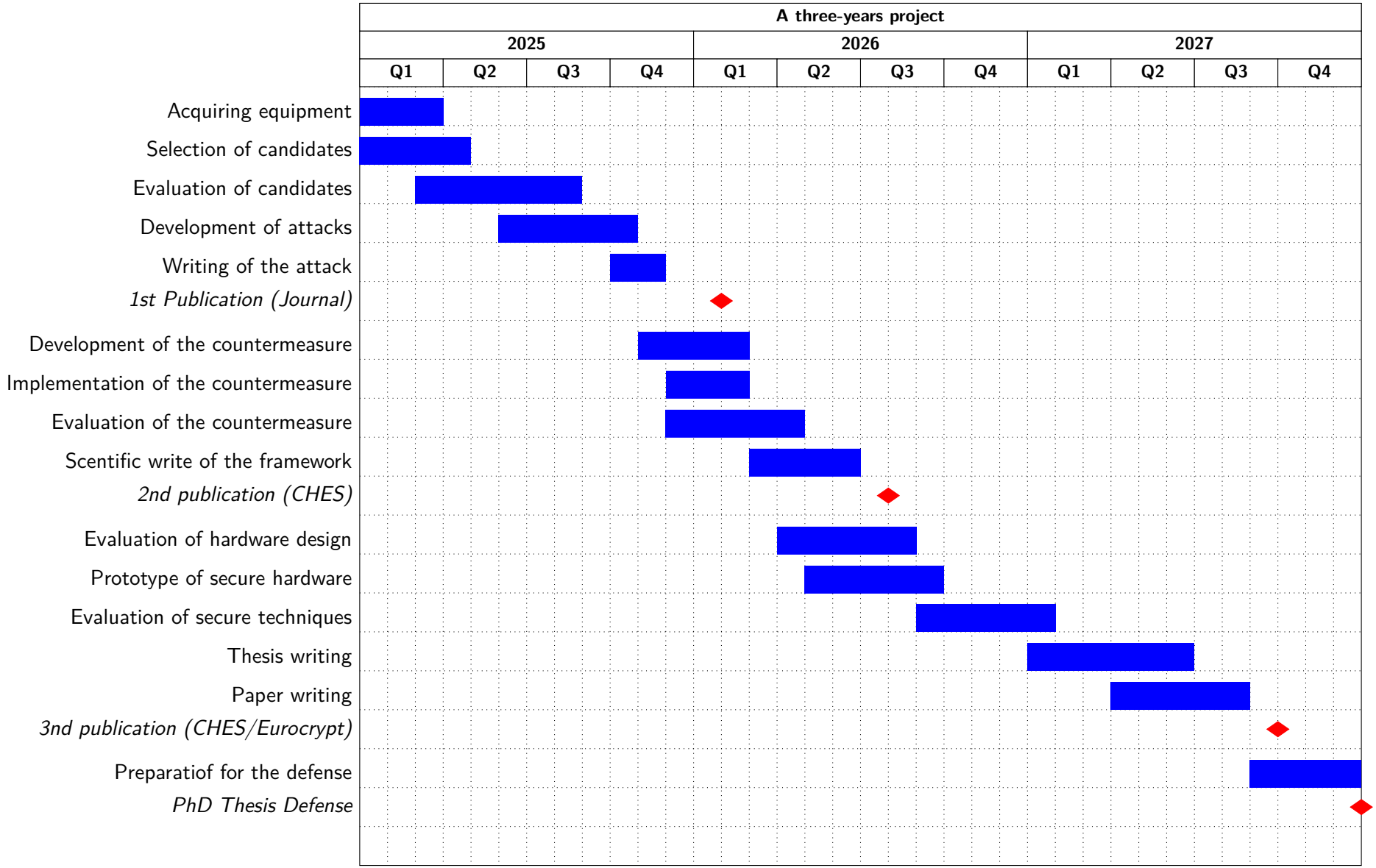
Funding Prospects. This work is positioned to support funding applications through agencies such as the European Research Council (ERC), the French National Research Agency (ANR), and cybersecurity-focused industrial partnerships.

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.

Therefore, the total estimated cost for the PhD student is €87,000, and the overall project cost, including equipment, is €97,635.

2 Calendrier



3 CV

1. The scientific summary (maximum 3 pages) highlighting the following sections, in connection with the evaluation criteria:
   - **Presentation:** positioning, challenges, objectives, methods, links with the School's strategy.
   - **Impacts, outcomes, and ambitions:** publications, conferences, collaborations, industrial contracts, funding acquisition (ERC, ANR, ...).
2. The timeline detailing the work plan over 3 years (maximum 1 page).
3. The projected budget over 3 years (maximum 1 page). This budget must be realistic, and the Foundation reserves the right to suspend or even terminate the project's funding, particularly in the event of an unjustified failure to comply with the budget.
4. The candidate's CV (maximum 3 pages).

CV

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

Supervision

Master Thesis

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

Bachelor Thesis

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

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.

Table 2: 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

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, 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, 2021.

4. 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, 2020.

5. 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.

6. 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.

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] 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.

[4] 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.