APP

Gustavo Banegas

1 Résumé du Scientifique

Research in post-quantum cryptography (PQC) has been boosted since the National Institute of Standards and Technology (NIST) initiated its PQC standardization project in 2016. The development of PQC schemes typically progresses through four stages:

1. **Mathematical Foundations**: Assessing the computational hardness of underlying mathematical problems;
2. **Scheme Construction**: Designing cryptographic schemes by leveraging these mathematical problems to create secure trapdoors;
3. **Algorithm and Prototype Development**: Developing algorithms and coding prototypes, leading to the release of specifications for standard algorithms;
4. **Deployment and Adoption**: Implementing and widely disseminating the cryptographic schemes.

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 (SCAs) are ongoing priorities. It is also essential to adapt PQC to current applications, including communication protocols, hardware security modules (HSMs), 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,

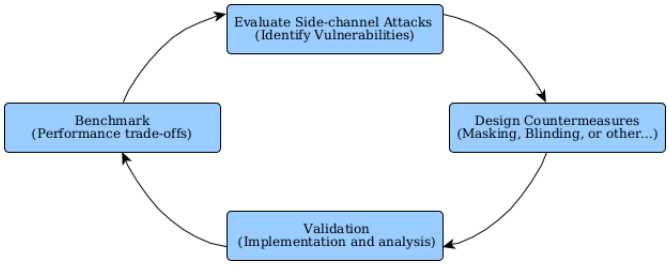


Figure 1: Overview of the methdology for the project.

electromagnetic emanation, or power consumption, made during the execution of sensitive computations. 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. 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.

This research proposal aims to achieve **three key objectives**: first, to evaluate side-channel attacks on digital signature schemes selected in the latest NIST call, identifying potential vulnerabilities and attack vectors; second, to design effective countermeasures that enhance the resilience of these schemes against such threats; and third, to benchmark the proposed solutions, assessing their efficiency, security, and practicality for real-world implementation.

Evaluating side-channel attacks

SCA evaluation encompasses two critical components: attack design and countermeasure design. I am deeply involved in advancing both facets of this process. My primary emphasis is on identifying vulnerabilities within PQC implementations and formulating countermeasures that can seamlessly integrate at the compilation (assembly language) level. This strategic approach not only fortifies the code securely but also upholds the integrity of the algorithm, ensuring a secure and resilient implementation.

Furthermore, I am exploring on an ongoing project the possibility of developing specialized hardware designed to be side-channel secure. For instance, this may involve creating a coprocessor that addresses the entire cryptographic scheme or designing a coprocessor tailored for specific functions, enhancing both the security and speed of the cryptographic system.

As previously mentioned, NIST introduced a new call for cryptographic signature proposals. It is typical for these new implementations to lack side-channel protection. To attack them, my approach involves initiating timing attacks on these implementations. Additionally, I am exploring fault attacks, another type of side-channel attack that exploits specific hardware to introduce faults in the code. I have addressed this concern in a specific cryptographic scheme in a published paper [1]. While the project provides a theoretical overview of fault attacks, the practical application requires specific hardware. Presently, there is a lack of such equipment at INRIA Saclay. However, we can fix this issue with two options; we can acquire the equipment or we can collaborate with other centers. For example, I maintain close contact with groups possessing this hardware, particularly at Fraunhofer AISEC Institut (Germany) and Masaryk University (Czech Republic).

In the **immediate and primary phase (short term)**, we can leverage the most recent NIST call to identify optimal candidates. By assessing metrics such as the ratio of public key to signature size, we aim to pinpoint the most efficient options, prioritizing those with smaller ratios. Additionally, our selection criteria will prioritize cryptographic schemes that have withstood potential vulnerabilities or attacks. Once this initial selection is made, our subsequent focus will shift towards initiating a comprehensive security evaluation process.

Side-channel attacks for post-quantum cryptosystems. Addressing the threat landscape of side-channel attacks, timing attacks pose a significant risk, exploiting the temporal variations in certain operations to uncover sensitive data, including secret keys. What makes them particularly formidable is their accessibility to attackers without the need for specialized hardware, as demonstrated in remote scenarios [3]. Both hardware and software implementations of cryptosystems may fall prey to these insidious attacks.

Another potent class of SCA is Differential Power Analysis [4] (DPA), recognized for its effectiveness and now considered an indispensable tool for attackers. I have employed DPA to successfully breach a protected version of Kyber [2].

Crafting such attacks demands proficiency not only in software but also in hardware, a dual expertise I possess. However, the challenge arises when extending these skills to other cryptographic schemes, necessitating collaborations for a broader understanding. Within the GRACE team, we

cover a spectrum of knowledge encompassing pre-quantum schemes and post-quantum schemes such as lattice-based, code-based, and isogeny-based schemes. Additionally, the COSMIC team contributes to a different type of expertise, that is, the knowledge of symmetric cryptography.

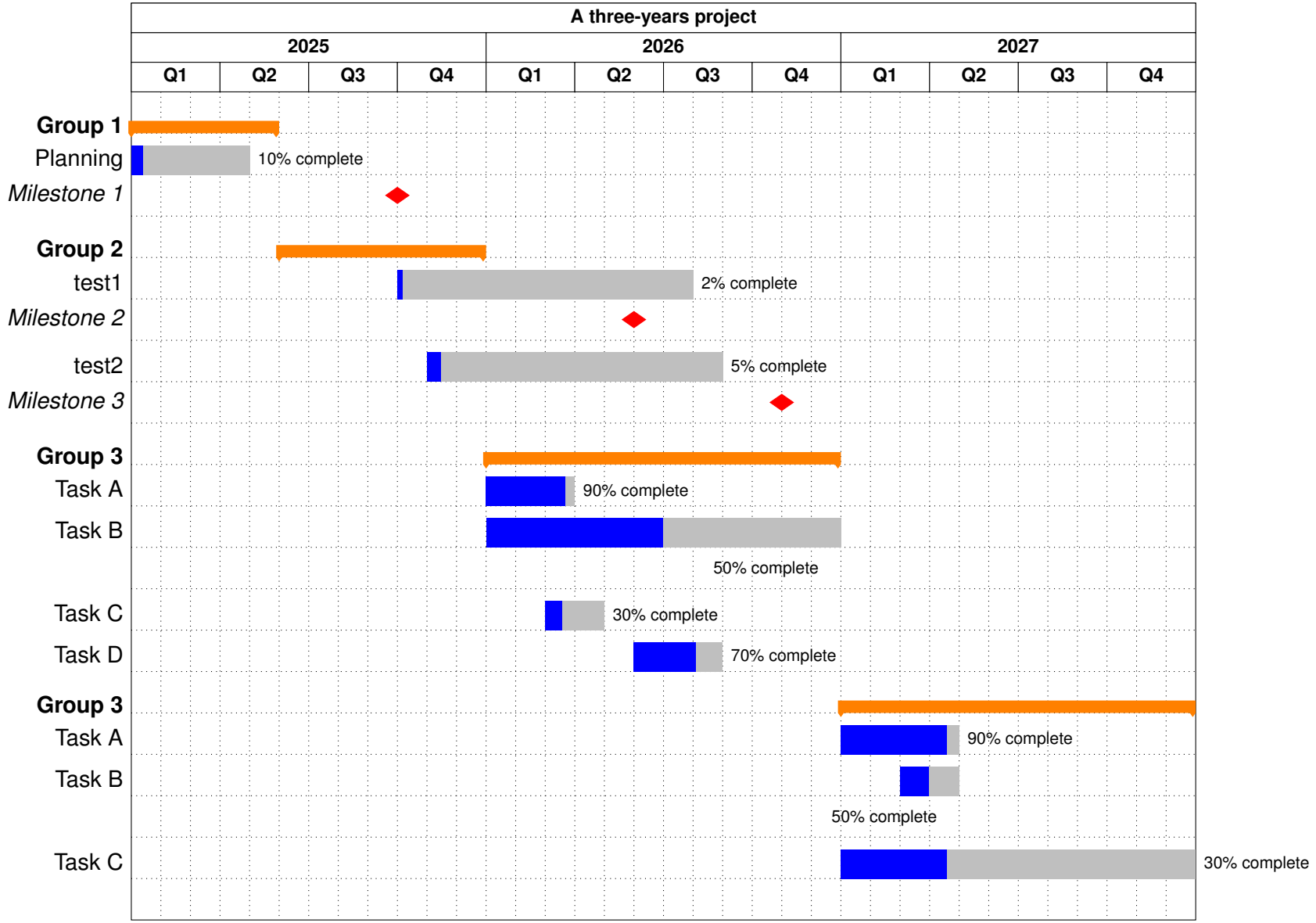
As a **mid-term objective**, we aim to cultivate a profound understanding of the post-quantum signature schemes, meticulously scrutinizing potential leakages encompassing both temporal and power-related vulnerabilities. Furthermore, the emergence of a novel class known as “MPC-in-the-head” provides a unique opportunity to delve deeper into this concept. This exploration not only entails comprehending the intricacies of MPC-in-the-head but also involves devising innovative strategies for potential attacks. The overarching goal of these efforts is to fortify the security of implementations, a perspective that will be explored in greater detail in the following section.

Side-channel protection for post-quantum cryptosystems. Transitioning from the previous section, we now explore countermeasures against such side-channel attacks. Initially, a crucial step involves implementing cryptosystems to operate in a ”constant-time” manner. It is important to note that constant time does not imply determinism or a fixed number of algorithmic steps. Instead, it ensures that the algorithm does not inadvertently disclose any secret data through timing variations across different inputs. This becomes a challenging endeavor, requiring not only a deep comprehension of the scheme and its functions but also the coding expertise to implement it effectively.

Addressing another layer of complexity involves mitigating the countermeasure’s impact on speed, code size, or hardware requirements. As part of my **mid-term goals** and in response to the NIST call for signatures, my ongoing efforts aim to propose efficient countermeasures against these attacks. This represents a vital step in advancing implementation security while maintaining a balance with practical considerations like speed and resource requirements. Fortunately, my background accelerates the comprehension of this process.

Producing new knowledge in this domain aligns with the objectives of the new cybersecurity master’s 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.

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.

Table 1: 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

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, 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] Gustavo Banegas, Juliane Krämer, Tanja Lange, Michael Meyer, Lorenz Panny, Krijn Reijnders, Jana Sotáková, and Monika Trimoska. Disorientation faults in CSIDH. In Carmit Hazay and Martijn Stam, editors, *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*, volume 14008 of *Lecture Notes in Computer Science*, pages 310–342. Springer, 2023.

[2] Estuardo Alpirez Bock, Gustavo Banegas, Chris Brzuska, Lukasz Chmielewski, Kirthivaasan Puniamurthy, and Milan Sorf. Breaking dpa-protected kyber via the pair-pointwise multiplication. *IACR Cryptol. ePrint Arch.*, page 551, 2023.

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

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