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,

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 focuses on the security evaluation of post-quantum digital signature schemes selected in the latest NIST call, with a particular emphasis on side-channel analysis (SCA). As cryptographic algorithms transition towards quantum resistance, their resilience to physical attacks remains a critical challenge. The primary objectives of this research are:

- **Evaluation of Side-Channel Attacks**: Analyzing vulnerabilities in selected signature schemes by applying both passive and active side-channel techniques, such as power analysis, fault injection, and electromagnetic analysis.

- **Design of Countermeasures**: Developing robust mitigation strategies tailored to each scheme, including masking, blinding, and fault detection mechanisms.

- **Benchmarking & Validation**: Assessing the effectiveness of the proposed countermeasures by measuring their security, computational overhead, and feasibility for real-world deployment.

This work aligns with the strategic research priorities of the School, particularly in cybersecurity, cryptographic engineering, and embedded system security. It contributes to strengthening expertise in hardware security and advanced cryptographic implementations, reinforcing the School's position as a leader in post-quantum cryptography research.

Impacts, Outcomes, and Ambitions

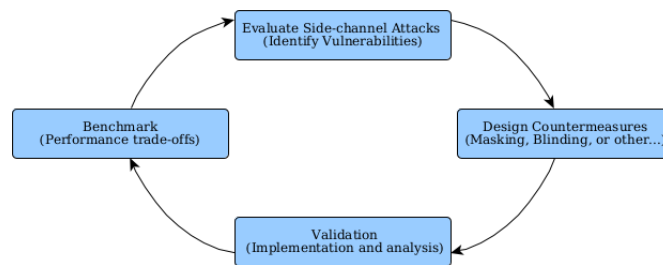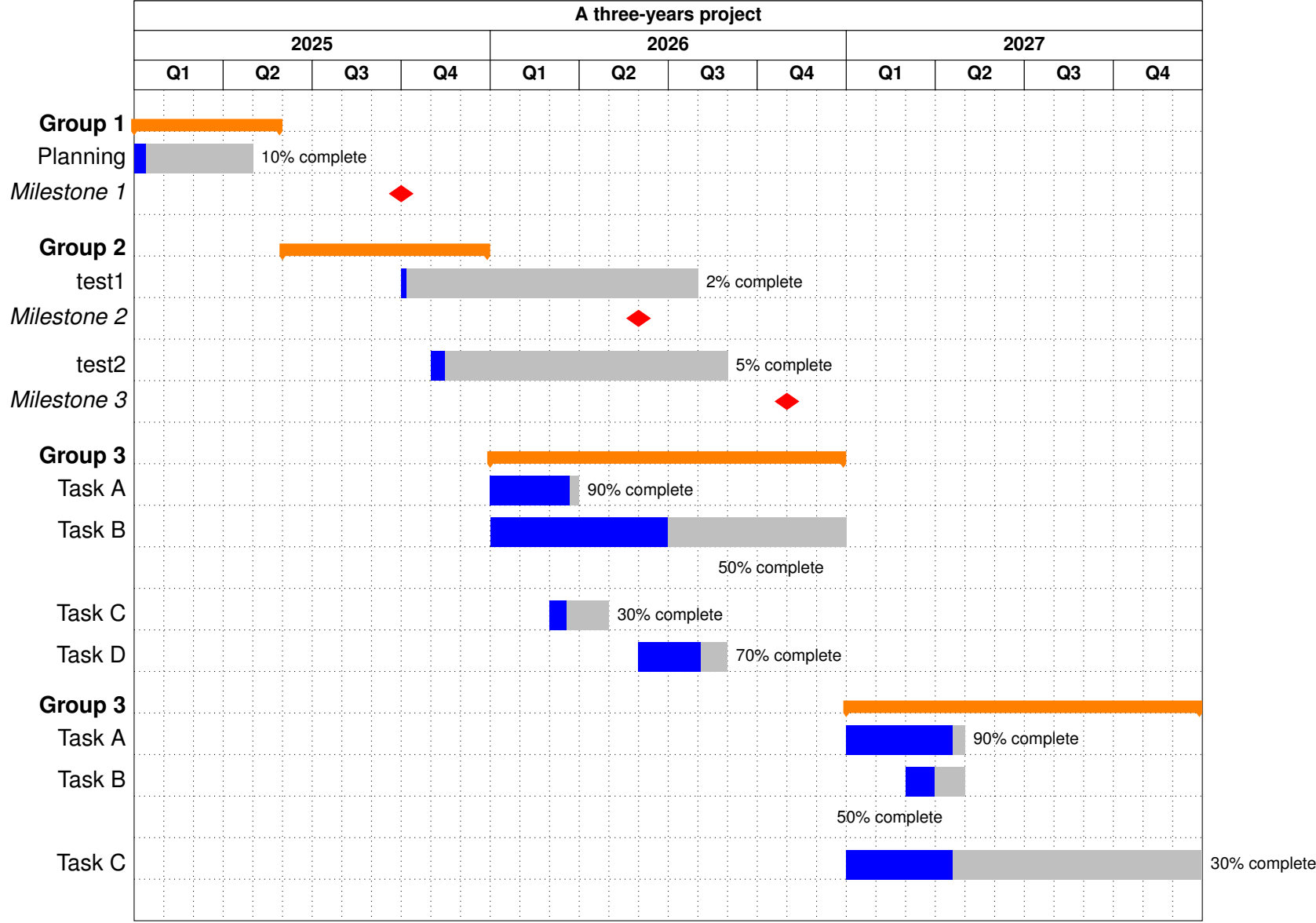The results of this research will contribute to the broader scientific community by:

Figure 1: Overview of the methdology for the project.

- **Publications**: Targeting top-tier cryptography and security conferences/journals such as CHES, EUROCRYPT, CRYPTO, and IEEE Transactions on Information Forensics and Security.

- **Conferences & Collaborations**: Engaging with academic and industrial partners to disseminate findings, participate in research workshops, and enhance interdisciplinary knowledge exchange.

- **Industrial Impact**: Establishing connections with industry stakeholders, particularly in embedded security and hardware-based cryptographic implementations, to assess the practical adoption of countermeasures.

- **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.

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

	A three-years project											
	2025				**2026**				**2027**			
	Q1	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

Group 1

Planning — 10% complete

Milestone 1

Group 2

test1 — 2% complete

Milestone 2

test2 — 5% complete

Milestone 3

Group 3

Task A — 90% complete

Task B — 50% complete

Task C — 30% complete

Task D — 70% complete

Group 3

Task A — 90% complete

Task B — 50% complete

Task C — 30% complete

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. *LATIN-CRYPT 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