APP

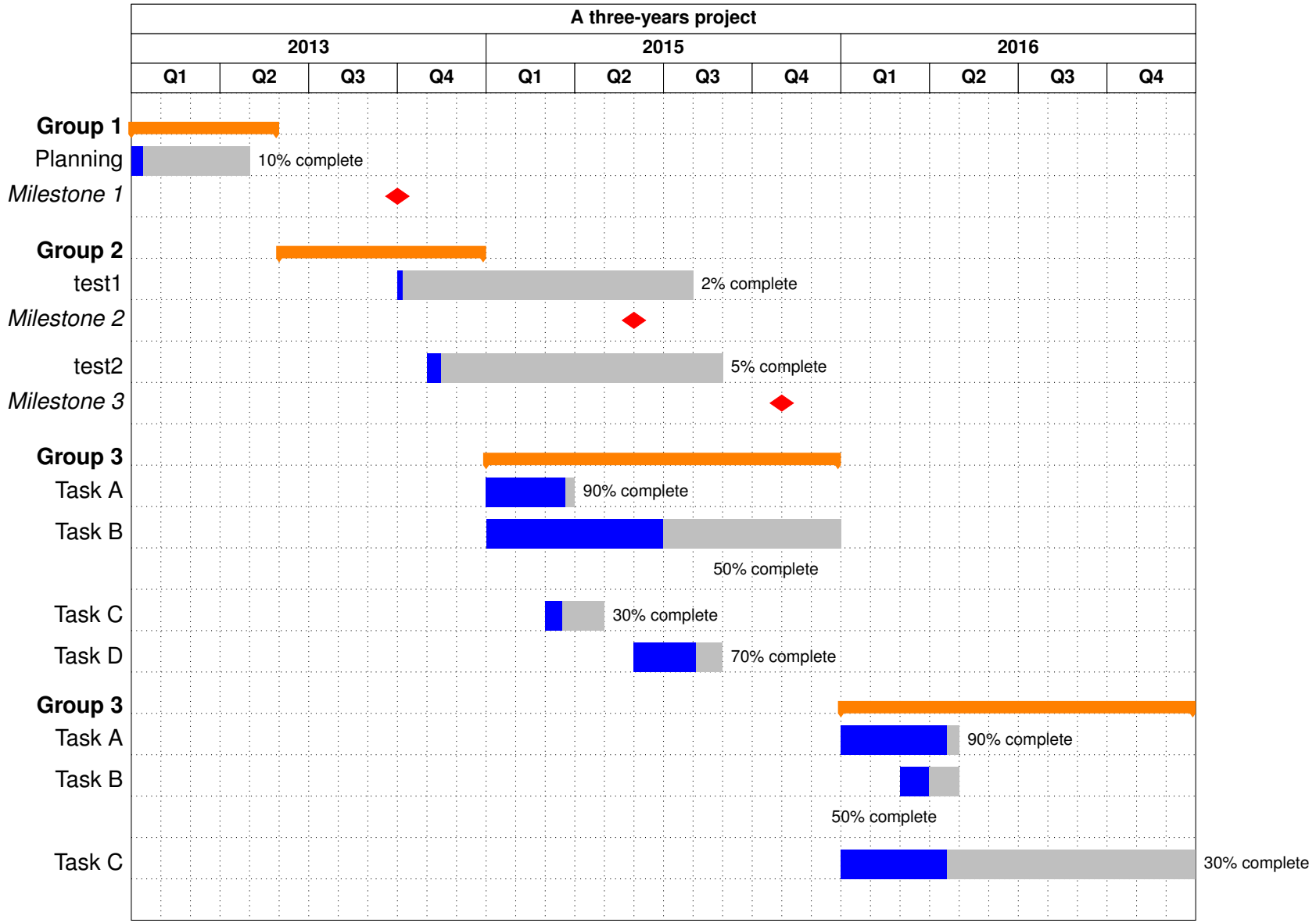
Gustavo Banegas

1 Résumé du Scientifique

1. **Le résumé du scientifique** (3 pages max.) mettant en avant les rubriques suivantes, en lien avec les critères d'évaluation :

    - **Présentation** : positionnement, enjeux, objectifs, méthodes, liens avec la stratégie de l'École.
    - **Impacts, retombées et ambitions** : publications, colloques, collaborations, contrat industriel, obtention de financement (ERC, ANR, . . .).

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).

Work Experience

- **Researcher**, INRIA, Palaiseau, France (Oct/2024 – Current)
    - Conduct cryptography research in the following areas, among others:
        * Secure implementation of post-quantum cryptography.
        * Design and development of specialized hardware for post-quantum cryptography.
        * Creation of countermeasures to mitigate side-channel vulnerabilities.
- **Senior Cryptographer**, QUALCOMM, Sophia Antipolis, France (Jul/2022 – Sept/2024)
    - Development of post-quantum cryptography on Snapdragon processors, including but not limited to:
        * Design and develop specific hardware for post-quantum cryptography.
        * Development of new attacks on post-quantum cryptography (side-channel attacks).
        * Development of countermeasures against side-channel attacks.
        * Speed-up implementations on Cortex-M3 and M4.
        * Development of post-quantum cryptography for RISC-V.

- **Post-doc**, INRIA AND ÉCOLE POLYTECHNIQUE, Paris, France (Dec/2020 – Jul/2022)
  - Development of post-quantum cryptography in embedded devices:
    * Development of new attacks on post-quantum cryptography (side-channel attacks).
    * Development of countermeasures against side-channel attacks.
    * Speed-up implementations of cryptographic signatures for RIOT-OS.
- **Post-doc**, CHALMERS UNIVERSITY OF TECHNOLOGY, Gothenburg, Sweden (Nov/2019 – Nov/2020)
  - Development of the WASP Project:
    * Development of new attacks on post-quantum cryptography.
    * Development of post-quantum cryptography.
    * Development of verifiable functions.
- **Research Assistant**, CHALMERS UNIVERSITY OF TECHNOLOGY, Gothenburg, Sweden (Sep/2019 – Nov/2019)
  - Development of the WASP Project:
    * Development of new attacks on post-quantum cryptography.
    * Development of post-quantum cryptography.
    * Development of verifiable functions.
- **Intern**, CRYPTOEXPERTS, Paris, France (Sep/2018 – Nov/2018)
  - Side-channel attacks on post-quantum cryptography implementations.
    * Detected leakage of timing in operations to develop timing attacks.
- **Intern**, RISCURE, Delft, Netherlands (Feb/2017 – Apr/2017)
  - Side-channel attacks on ECC implementations.
    * Investigated attacks on implementations of ECC in FPGAs using power analysis.
- **System Analyst**, BRY TECNOLOGIA, Florianópolis, Brazil (Oct/2014 – Sep/2015)
  - Software development for Public Key Infrastructure (PKI).

        * Developed software in Java and C++.
        * Integrated HSM in Java applications.
        * Managed a team using Scrum.

- **Researcher, Project Manager, and Developer**, LABSEC - LABORATORY FOR COMPUTER SECURITY, Florianópolis, Brazil (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 defining attribute certification in Brazil.
        * Developed software in C/C++, Java, and Python.

Program Committee Member

- CBCrypto: 2020, 2021
- CHES: 2022, 2023, 2024
- Eurocrypt: 2022
- LatinCrypt: 2023
- Asiacrypt: 2023
- ACNS: 2024

External Reviewer

- CRYPTO: 2022
- Asiacrypt: 2018, 2019, 2020, 2021
- FSE: 2021
- LatinCrypt: 2021
- SPACE: 2020
- PQCrypto: 2018

Software

- **WAVE**: `https://github.com/wavesign/wave`
- **Wavelet**: `https://github.com/wavelet/`
- **CTIDH**: `http://ctidh.isogeny.org/software.html`
- **DAGS Key encapsulation**: `https://github.com/gbanegas/dags_v2`
- **HSS/LMS hash-based signatures**: `https://github.com/gbanegas/sphss`
- **More code**: `https://github.com/gbanegas/`

Supervision: Master Theses

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

Supervision: Bachelor Theses

- **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.

References

[1] Gustavo Banegas and Ricardo Villanueva-Polanco. A fault analysis on SNOVA. Cryptology ePrint Archive, Paper 2024/1883, 2024.

[2] Estuardo Alpirez Bock, Gustavo Banegas, Chris Brzuska, Lukasz Chmielewski, Kirthivaasan Puniamurthy, and Milan Sorf. Breaking dpa-protected kyber via the pair-pointwise multiplication. In Christina Pöpper and Lejla Batina, editors, *Applied Cryptography and Network Security - 22nd International Conference, ACNS 2024, Abu Dhabi, United Arab Emirates, March 5-8, 2024, Proceedings, Part II*, volume 14584 of *Lecture Notes in Computer Science*, pages 101–130. Springer, 2024.

[3] Gustavo Banegas and Florian Caullery. Multi-armed sphincs$^+$. In Jianying Zhou, Lejla Batina, Zengpeng Li, Jingqiang Lin, Eleonora Losiouk, Suryadipta Majumdar, Daisuke Mashima, Weizhi Meng, Stjepan Picek, Mohammad Ashiqur Rahman, Jun Shao, Masaki Shimaoka, Ezekiel O. Soremekun, Chunhua Su, Je Sen Teh, Aleksei Udovenko, Cong Wang, Leo Yu Zhang, and Yury Zhauniarovich, editors, *Applied Cryptography and Network Security Workshops - ACNS 2023 Satellite Workshops, ADSC, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, SiMLA, Kyoto, Japan, June 19-22, 2023, Proceedings*, volume 13907 of *Lecture Notes in Computer Science*, pages 500–514. Springer, 2023.

[4] Gustavo Banegas, Valerie Gilchrist, Anaëlle Le Dévéhat, and Benjamin Smith. Fast and frobenius: Rational isogeny evaluation over finite fields. In Abdelrahaman Aly and Mehdi Tibouchi, editors, *Progress in Cryptology - LATINCRYPT 2023 - 8th International Conference on Cryptology and Information Security in Latin America, LATINCRYPT 2023, Quito, Ecuador, October 3-6, 2023, Proceedings*, volume 14168 of *Lecture Notes in Computer Science*, pages 129–148. Springer, 2023.

[5] Gustavo Banegas, Juliane Krämer, Tanja Lange, Michael Meyer, Lorenz Panny, Krijn Reijnders, Jana Sotáková, and Monika Trimoska. Disorientation faults in CSIDH. In *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*, pages 310–342. Springer, 2023.

[6] Gustavo Banegas and Ricardo Villanueva-Polanco. On recovering block cipher secret keys in the cold boot attack setting. *Cryptography and Communications*, pages 1–25, 2023.

[7] Gustavo Banegas, Valerie Gilchrist, and Benjamin Smith. Efficient supersingularity testing over GF(p) and CSIDH key validation. *Mathematical Cryptology*, 2(1):21–35, Oct. 2022.

[8] Gustavo Banegas, Koen Zandberg, Emmanuel Baccelli, Adrian Herrmann, and Benjamin Smith. Quantum-resistant software update security on low-power networked embedded devices. In Giuseppe Ateniese and Daniele Venturi, editors, *Applied Cryptography and Network Security - 20th International Conference, ACNS 2022, Rome, Italy, June 20-23, 2022, Proceedings*, volume 13269 of *Lecture Notes in Computer Science*, pages 872–891. Springer, 2022.

[9] 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.

[10] 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`.

[11] 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.

[12] Georgia Tsaloli, Bei Liang, Carlo Brunetta, Gustavo Banegas, and Aikaterini Mitrokotsa. DEVA: Decentralized, Verifiable Secure Aggregation for Privacy-Preserving Learning. In Joseph K. Liu, Sokratis Katsikas, Weizhi Meng, Willy Susilo, and Rolly Intan, editors, *Information Security*, pages 296–319, Cham, 2021. Springer International Publishing.

[13] 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.

[14] Gustavo Banegas, Paulo S. L. M. Barreto, Edoardo Persichetti, and Paolo Santini. Designing efficient dyadic operations for cryptographic applications. *J. Math. Cryptol.*, 14(1):95–109, 2020.

[15] Bei Liang, Gustavo Banegas, and Aikaterini Mitrokotsa. Statically aggregate verifiable random functions and application to e-lottery. *Cryptography*, 4(4), 2020.

[16] Georgia Tsaloli, Gustavo Banegas, and Aikaterini Mitrokotsa. Practical and provably secure distributed aggregation: Verifiable additive homomorphic secret sharing. *Cryptography*, 4(3):25, 2020.

[17] 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.

[18] Douglas Marcelino Beppler Martins, Gustavo Banegas, and Ricardo Felipe Custódio. Don't forget your roots: Constant-time root finding over 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.

[19] 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.

[20] 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.

[21] Gustavo Banegas, Paulo SLM Barreto, Edoardo Persichetti, and Paolo Santini. Designing efficient dyadic operations for cryptographic applications. *IACR Cryptology ePrint Archive*, 2018(650), 2018.

[22] 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.

[23] 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.

[24] Gustavo Banegas. Attacks in stream ciphers: A survey. Cryptology ePrint Archive, Report 2014/677, 2014. `https://eprint.iacr.org/2014/677`.