APP

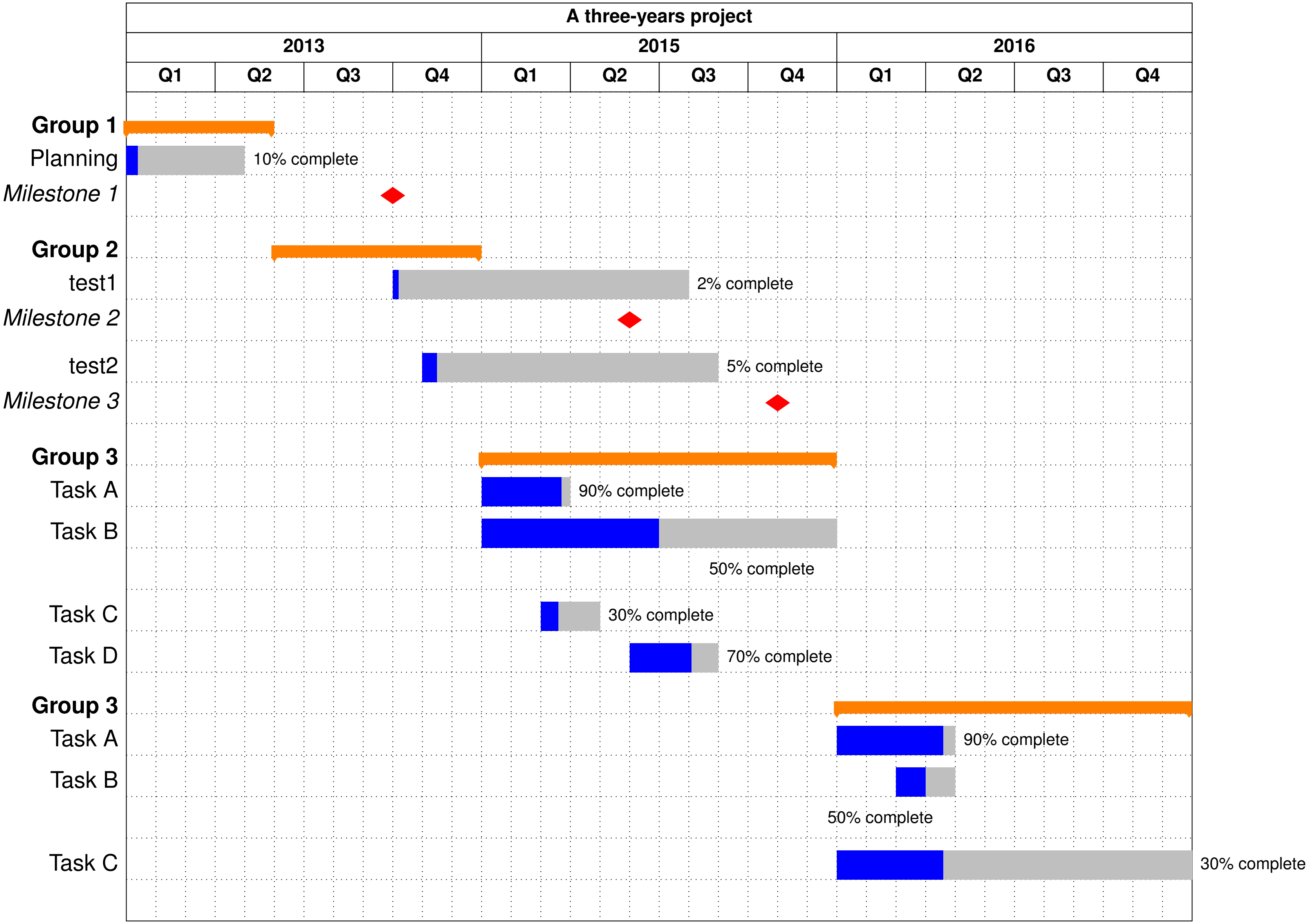
Gustavo Banegas

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

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/`