PhD Thesis

- **Title:** Cryptographic approaches based on fast elliptic algorithmics
- **Research unit:** IRMAR, UMR-6625
- **Theme:** Effective geometry and algebra.
- **Keywords:** Algebraic curves, cryptography.
- **PhD supervisors:**

_ *Jean-Marc Couveignes*, IMB, Univ. Bordeaux.
email: `jean-marc.couveignes@math.u-bordeaux.fr`
webpage: https://www.math.u-bordeaux.fr/~jcouveig/

_ *Reynald Lercier*, IRMAR, Univ. Rennes.
email: `reynald.lercier@univ-rennes.fr`
webpage: https://lercier.pages.math.cnrs.fr/

The Fast Fourier Transform (FFT) is a fundamental tool in signal processing over the field of complex numbers. Its adaptation to discrete settings, such as coding theory or cryptography, nevertheless runs into several structural constraints. In particular, its reliance on the existence of primitive roots of unity requires working over finite rings of suitable order and mastering their arithmetic peculiarities.

This thesis aims to tackle these problems by building on recent work that reformulates them within the more geometric framework of elliptic curves [CL26]. In the particular case of a curve admitting a rational point t of order d, where d is a power of two, this work exhibits the existence of natural analogues of the butterfly structures characteristic of the FFT. In this approach, the roots of unity are replaced by the multiples of the point t, while the classical involution $x \mapsto -x$ corresponds to translation by a point of order two. This generalization yields optimal complexity bounds of $\mathcal{O}(d \log d)$, thereby opening up new perspectives.

This thesis work will seek to generalize and improve this approach in order to offer greater flexibility of use in applications. The main challenge is to maintain quasi-linear complexity despite the increased arithmetic constraints. The expected outcomes concern in particular geometric codes based on elliptic curves, where new FFT structures could speed up encoding and error detection.

The thesis could also explore the cryptographic applications of these constructions. The post-quantum schemes selected by NIST often rely on fast polynomial multiplication. By transposing these computations to the setting of elliptic curves, one can envisage the possibility of designing new cryptographic schemes or new so-called "elliptic" lattices. These could provide an alternative to classical cyclotomic lattices, combining algorithmic efficiency with increased robustness, in particular thanks to arithmetic properties that are difficult to achieve in characteristic zero.

References

[CL26] J.-M. Couveignes and R. Lercier. "Elliptic butterflies". In: *Journal of Complexity* 95 (2026). DOI: https://doi.org/10.1016/j.jco.2026.102046.