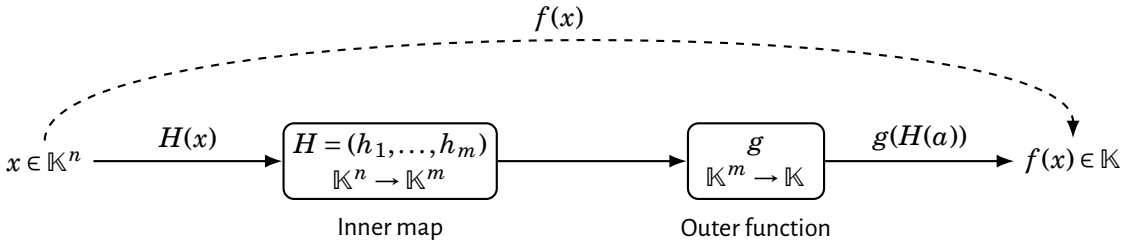
Toward Faster Algorithms for Decomposable Polynomial Systems



Supervision.

- Thi Xuan Vu (Maître de Conférences, Université de Lille, CRIStAL - CFHP team) thi-xuan.vu@univ-lille.fr
- Florent Bréhard (CNRS Researcher, CRIStAL, Lille - CFHP team) florent.brehard@univ-lille.fr
- Josué Tonelli-Cueto (Associate Professor, CUNEF Universidad) josue.tonelli.cueto@bizkaia.eu

Context and motivation. Decomposable polynomials, those that can be expressed as compositions of lower-degree polynomials, form a classical and fundamental topic in computer algebra, with numerous applications. These include cryptography (see, e.g., [12, 6, 5, 3, 10]), control theory and system identification [4], as well as the analysis and reduction of differential equations (cf. [11] and references therein). For instance, Multivariate Public-Key Cryptosystems (MPKCs) rely on the hardness of solving systems of multivariate polynomial equations over finite fields. A typical public map is of the form

$$F = S \circ C \circ T,$$

where S, T are secret affine transformations and C is a central map of special algebraic form.

This internship aims to develop theoretical and algorithmic foundations for exploiting decomposable structures in multivariate polynomial systems, combining symbolic and numerical techniques.

State of the art. Let f be a polynomial in $\mathbb{K}[x_1, \ldots, x_n]$ for a field $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. The *Polynomial Decomposition Problem* (PDP), known to be NP-hard [2, 14], asks whether there exist polynomials g and h_i such that

$$f(x_1, \ldots, x_n) = g\big(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n)\big),$$

and, if so, how to compute such a decomposition. The univariate case is completely solved: polynomial-time algorithms based on factorization in composition algebras are known [8, 1] and implemented in major computer algebra systems (e.g., `compoly` in Maple). In contrast, multivariate algorithms are only known for homogeneous polynomials of the same degree [6], leaving the general case open. These algorithms typically rely on Gröbner basis computations over various fields. Another common approach is to divide the problem into two steps: (1) computing candidate inner polynomials $h_1, \ldots, h_m$, and (2) reconstructing the outer polynomial g. Recent work by T. X. Vu [15] provides a solution to the second step, while the first remains open in the general setting.

Another central problem in computational algebraic geometry and computer algebra is *Polynomial System Solving* (PSS). Such systems arise in many areas, including computer algebra, robotics, geometric modeling, signal processing, cryptology, and molecular biology, and are generally NP-hard [7]. A key bottleneck in symbolic computation is the *intermediate expression swell*, where algebraic data grow combinatorially. A promising way

to mitigate this is by exploiting hidden algebraic structures, such as decomposability, to reduce computational complexity. However, only a few works have systematically explored this direction.

An alternative is to use *numerical computation*. While symbolic methods guarantee exactness, numerical approaches are approximate but often more scalable and parallelizable. Combining the two yields *symbolic-numeric hybrid algorithms*, which aim to balance precision and efficiency. For example, certified numerical algebraic geometry methods [13, 9] can provide correctness guarantees for numerically computed solutions. Surprisingly, despite this potential, the symbolic-numeric interface remains largely unexplored in the context of PSS, precisely the gap this project aims to bridge.

Objectives of the internship. The goal is to design faster algorithms for problems involving decomposable polynomials and to demonstrate their effectiveness on key applications. The intern will contribute to developing the **theoretical and algorithmic foundations** for **detecting, computing, and exploiting** decompositions of multivariate polynomial maps, with a particular focus on **hybrid symbolic-numeric** methods.

Required skills. A background in algebra, algorithms, and/or numerical analysis, as well as basic programming skills (in Maple, SageMath, Julia, or Python), would be useful but not mandatory. An interest in symbolic-numeric computation and computer algebra is expected.

Practical information.

- Duration: 4-6 months (Spring 2025)
- Location: Université de Lille, CRIStAL (CFHP team)
- Possible continuation: PhD opportunity in computer algebra

I. References

[1] D. Barton and R. Zippel. Polynomial decomposition algorithms. *Journal of Symbolic Computation*, 1(2):159–168, 1985.

[2] M. T. Dickerson. General polynomial decomposition and the $(s-1)$-decomposition are NP-hard. *International Journal of Foundations of Computer Science*, 4(2):147–156, 1993.

[3] J. Ding and D. Schmidt. Rainbow, a new multivariable polynomial signature scheme. In *ACNS 2005*, volume 3531 of *LNCS*, pages 164–175. Springer, 2005.

[4] C. Ebenbauer, T. Faulwasser, and F. Allgöwer. Analysis and design of polynomial control systems. *Automatica*, 42(10):1717–1727, 2006.

[5] J.-C. Faugère and A. Joux. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In *CRYPTO 2003*, volume 2729 of *LNCS*, pages 44–60. Springer, 2003.

[6] J.-C. Faugère and L. Perret. An efficient algorithm for decomposing multivariate polynomials and its applications to cryptography. *Journal of Symbolic Computation*, 44(12):1676–1689, 2009.

[7] M. R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*, volume 29 of *Series of Books in the Mathematical Sciences*. W. H. Freeman and Company, New York, 2002.

[8] D. Kozen and S. Landau. Polynomial decomposition algorithms. *Journal of Symbolic Computation*, 7(5):445–456, 1989.

[9] T. Y. Li. *Numerical Solution of Polynomial Systems by Homotopy Continuation Methods*, volume XI of *Handbook of Numerical Analysis*. Springer, 2003.

[10] J. Liu, H. Zhang, and J. Jia. Cryptanalysis of schemes based on polynomial symmetrical decomposition. *Chinese Journal of Electronics*, 26(5):1000–1006, 2017.

[11] A. Ovchinnikov, I. Pérez Verona, G. Pogudin, and M. Tribastone. Clue: exact maximal reduction of kinetic models by constrained lumping of differential equations. *Bioinformatics*, 37(12):1732–1738, 2021.

[12] J. Patarin. Hidden field equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In *EUROCRYPT 1996*, volume 1070 of *LNCS*, pages 33–48. Springer, 1996.

[13] J. Verschelde. Algorithm 795: Phcpack: A general-purpose solver for polynomial systems by homotopy continuation. *ACM Transactions on Mathematical Software*, 25(2):251–276, 1999.

[14] J. von zur Gathen, J. Gutierrez, and R. Rubio. Multivariate polynomial decomposition. *Applicable Algebra in Engineering, Communication and Computing*, 14(1):11–31, 2003.

[15] T. X. Vu. Computing polynomial representation in subrings of multivariate polynomial rings. *In Proceedings of the International Symposium on Symbolic and Algebraic Computation*, 2025.