Haut Conseil de l'Évaluation de la Recherche et de l'Enseignement Supérieur

DOCUMENT D'AUTOÉVALUATION

Équipe PolSys

Campagne d'évaluation 2023-2024 — Vague D

Table des matières

1 INFORMATIONS GÉNÉRALES SUR L'ÉQUIPE PolSys

Nom de l'équipe : Systemes Polynomiaux (PolSys)

Responsable de l'équipe Mohab Safey El Din

	2017	2018	2019	2020	2021	2022
PR	1	1	1	1	1	1
MCF HDR	1	1	0	0	0	1
MCF	1	1	1	1	1	2
DR	1	1	0	0	0	0
CR HDR	0	0	0	0	0	0
CR	1	1	1	0	0	0
Total permanents	5	5	3	2	2	4
Émérites	1	1	1	1	1	0
Doctorants	5	7	6	8	6	6
Ingénieurs CDD ou hors tutelles	1	0	0	0	0	0
Post-doc, ATER, etc.	0	3	1	0	0	1
Stagiaires	3	5	1	2	1	3
Total non permanents	9	15	8	10	7	10
Total avec émérites	**15**	**21**	**12**	**13**	**10**	**14**
Equivalent temps plein recherche	3.5	3.5	2.0	1.0	1.0	2.0

TABLE 1 – Personnels PolSys sur la période 2017-2022 (au 1er juillet de chaque année)

1.1 Les thématiques scientifiques et leurs enjeux

Positionnement scientifique

L'équipe PolSys se concentre sur la conception d'*algorithmes du calcul formel*, relevant souvent de méthodes algébriques, pour la résolution de problèmes effectifs en mathématiques, et tout particulièrement la *résolution de systèmes polynomiaux*. L'équipe a une activité de développement logiciel qui vient compléter et amplifier ses productions de nature plus algorithmique/théorique. L'enjeu pour l'équipe est non seulement d'*impacter directement sur des domaines d'applications cibles* mais aussi de transférer à diverses communautés scientifiques les avancées permises par les techniques pointues du calcul formel.

La résolution des systèmes polynomiaux est en effet un problème fondamental qui apparaît dans un grand nombre de domaines comme la cryptologie, la géométrie algorithmique ou la vérification de programmes dans les sciences du numérique, des conjectures de nature géométrique ou combinatoire en mathématiques ou bien dans des sciences de l'ingénieur comme la robotique, la biologie et la chimie.

La nature *non linéaire* de ces problèmes, le caractère *exact, ou exhaustif, ou global,* des solutions calculées, requis par certaines applications, rendent délicat l'usage de méthodes purement numériques ou d'approximation. Les défis algorithmiques posés par la résolution de systèmes polynomiaux sont donc considérables et ce, d'autant que ce problème est $\mathcal{NP}$-dur, même lorsque les coefficients vivent dans un corps fini [3, Appendix A7.2]. En s'appuyant sur des méthodes de calcul formel, notamment le calcul de bases de Gröbner, l'équipe PolSys conçoit une grande *variété d'algorithmes* qui permettent de répondre à un *nombre de spécifications algorithmiques variées*, notamment :

(A) énumérer l'ensemble des solutions (dans une clôture algébrique [1]) lorsque celui-ci est fini ; ceci trouve des applications en cryptologie ou théorie des codes correcteurs (les coefficients vivent dans un corps fini) ou en sciences de l'ingénieur (les coefficients sont des nombres rationnels) ;

(B) la résolution sur les nombres réels de systèmes dépendant de paramètres (pour des applications de nature géométrique ou provenant de la robotique) ;

(C) la résolution de problèmes d'élimination des quantificateurs, et les problèmes d'optimisation polynomiale (applications en vérification de programmes ou en sciences de l'ingénieur) ;

(D) la détermination de propriétés topologiques d'ensembles de solutions réelles de systèmes polynomiaux (notamment la détermination du nombre de composantes connexes avec des applications en robotique).

La résolution de cette *large gamme de problèmes et d'applications qui leur sont associées* nécessite le développement de plusieurs logiciels par l'équipe ainsi que leur diffusion la plus large possible. Notamment, la bibliothèque

1. Ceci correspond au corps des nombres complexes lorsque les coefficients sont rationnels ; la construction est similaire pour d'autres types de coefficients

`msolve` est, depuis peu, intégrée à des systèmes de calcul formel généralistes comme SAGEMATH (voir ici et là) et OSCAR (voir ici) ce qui lui assure une diffusion large.

Enfin, l'équipe développe une activité régulière dans plusieurs domaines d'applications qu'elle a ciblées prioritairement, en particulier, la cryptologie et la robotique.

Ainsi, l'équipe PolSys se positionne naturellement dans les axes du LIP6 :

- *Théorie et outils mathématiques pour l'informatique* en apportant des méthodes pour la résolution automatisée de problèmes mathématiques, qui trouvent de nombreuses applications ;
- *Sécurité, sûreté et fiabilité* en apportant des méthodologies, algorithmes et logiciels conçus pour fiabiliser et rendre robustes les systèmes de calcul scientifique d'une part et en contribuant à la conception et l'analyse de schémas de cryptographie post-quantique.

L'équipe a des publications communes avec les équipes ALMASTY [Kushilevitz et al., 2021], MOVE [Bérard et al., 2021], PEQUAN [Lairez et al., 2019] et QI [Faugère et al., 2017]. L'équipe co-encadre deux thèses avec les équipes PEQUAN et ALMASTY respectivement. Elle collabore avec QI au travers d'un projet Européen.

Contexte international

Nous identifions trois mouvements de fond au niveau international.

Algorithmique du calcul formel au niveau international

Du point de vue algorithmique, on a assisté, d'une part, à un renouveau des opérations algorithmiques dites "de base" (multiplication d'entiers [4], calculs de polynômes caractéristiques [5] et résultants bivariés [6–8], entre autres) où la communauté française excelle et, d'autre part, le développement d'une algorithmique dédiée pour exploiter des propriétés structurelles de systèmes polynomiaux et la résolution de problèmes de nature plus topologique (détermination du nombre de composantes connexes, exploitation de symétries, etc.). À l'avant-garde internationale de cette mouvance, dont l'objectif est centré sur l'amélioration des complexités théoriques, on trouve, entre autres, l'équipe de calcul formel de l'Université de Waterloo (G. Labahn, É. Schost) avec laquelle nous collaborons régulièrement, Purdue University aux USA (S. Basu) avec laquelle nous collaborons un peu moins ces dernières années et l'équipe de calcul formel de l'université de Buenos Aires en Argentine (G. Jeronimo, T. Krick) avec laquelle nous avons des contacts réguliers – notamment pour l'accueil d'étudiants. Plus récemment, de nouveaux acteurs ont émergé notamment en Norvège (C. Riener) avec lequel nous collaborons régulièrement et à Berlin (P. Bürgisser) avec lequel nous avons des échanges réguliers.

Ces acteurs sont une des composantes d'une communauté encore plus dense (regroupant souvent plus de 800 chercheurs à la conférence bi-annuelle SIAM Conference on Applied Algebra and Geometry) qui intègre les méthodes numériques pour la résolution des systèmes polynomiaux, l'étude de leurs propriétés mathématiques et leurs applications. Les groupes de recherche les plus en vue se trouvent au MIT (P. Parillo/C. Uhler), à l'université de Berkeley et au MPI Leipzig (B. Sturmfels), au CWI (M. Laurent), à l'Université de Copenhague (E. Feliu) et l'académie des sciences en Chine (L. Zhi). Ils contribuent souvent moins aux aspects purement algorithmiques mais sont très présents sur le développement des mathématiques du calcul formel et sur le front des applications. Nous avons collaboré et/ou participé à divers projets européens avec le MIT et le CWI. Nous avons des échanges réguliers avec Berkeley/MPI et des échanges plus récents avec l'université de Copenhague au Danemark.

Des logiciels internationaux et le virage open source

Jusqu'au milieu des années 2000, les logiciels de calcul formel se distinguaient par la présence quasi exclusive d'éditeurs développant et distribuant des systèmes de calcul formel (les plus connus étant MATHEMATICA et MAPLE) et une nébuleuse de bibliothèques académiques plus spécialisées, souvent open source, mais pas toujours.

Cette situation a radicalement changé. La mise à disposition de logiciels open source et sous licence libre est devenue une nécessité pour le développement du calcul scientifique, notamment au niveau académique. Ainsi, le système de calcul formel SAGEMATH a émergé en agglomérant les efforts de plusieurs groupes académiques, aux États-Unis dans un premier temps, puis en Europe. SAGEMATH fait aujourd'hui partie des logiciels recommandés pour l'agrégation de mathématiques en France. Ce changement radical s'est observé par l'octroi d'un financement européen de type "Research Infrastructure" pour le projet OpenDreamKit (H2020, 2015–2019, 7.6M€) visant justement à développer et harmoniser le développement de logiciels scientifiques open-source ; SAGEMATH est

l'un des principaux composants de ce projet. Plus récemment encore, le système OSCAR a émergé avec l'idée d'exploiter les potentialités offertes par le langage de programmation `Julia`.

Le virage open source s'est amplifié et, pour les bibliothèques spécialisées, on a constaté également une convergence entre calcul formel et calcul haute-performance.

L'équipe PolSys a une activité de développement logiciel qui s'inscrit pleinement dans ces évolutions. Le fait majeur est assurément le développement de la bibliothèque `msolve` dont on peut mesurer le succès à son intégration en cours dans des systèmes comme SAGEMATH et OSCAR.

La révolution post-quantique en cryptographie

En quelques années, le statut de la cryptographie post-quantique a connu une véritable révolution. Le domaine est passé d'une thématique essentiellement académique à un domaine industriel stratégique à part entière. L'élément déclencheur est le processus de normalisation post-quantique du NIST (organisme de standardisation américain) qui préfigure un déploiement massif et à grande échelle de cette cryptographie de nouvelle génération. Les deux grands défis du post-quantique sont liés, d'une part, à l'intégration de cette nouvelle cryptographie dans des environnements contraints et protocoles de sécurité (`https`, `IPSEC`, etc) et, d'autre part, à la nécessité d'analyser la sécurité des nouvelles primitives pour maintenir la confiance des utilisateurs.

Le calcul formel est au cœur des défis du post-quantique. La cryptanalyse algébrique qui réduit la sécurité d'un cryptosystème au calcul de complexité d'une base de Gröbner constitue une approche privilégiée pour analyser la sécurité des primitives post-quantiques. Aussi, les outils du calcul formel apparaissent naturellement dans la conception et l'implantation efficace des primitives post-quantiques (multiplication rapide des entiers, des polynômes, des matrices, etc).

La cryptographie post-quantique est un domaine d'application historique de PolSys qui a développé un positionnement original combinant la valorisation de son savoir-faire à travers la société CRYPTONEXT SECURITY (leader français du post-quantique) et le développement d'outils algorithmiques et logiciels, notamment `msolve`, pour l'analyse de la sécurité des primitives post-quantiques.

Avancées scientifiques majeures

Nous les classifions en trois catégories :

1. une première série de résultats qui revisitent et réinventent les fondements algorithmiques du domaine pour améliorer la complexité de résolution sur des systèmes généraux ou génériques ;
2. une deuxième série, complémentaire à la première, de résultats qui améliorent les résultats de complexité dans le cas de systèmes dits structurés, spécifiques à certaines applications ;
3. enfin, des développements logiciels marquants, qui sont novateurs, "changent la donne" dans le domaine et à la base de résultats scientifiques importants dans nos domaines d'applications.

Des fondements méthodologiques renouvelés et des résultats de complexité

Comme on l'a expliqué plus haut, "résoudre" un système de contraintes polynomiales a un sens algorithmique qui peut varier fortement, voir les problèmes (A), (B), (C) et (D) listés ci-dessus. Sur ces problèmes, nous avons apporté de *nouvelles approches qui permettent d'obtenir des complexités améliorant sensiblement l'état de l'art*.

Pour le problème (A), la stratégie classique consiste à calculer une *paramétrisation* des coordonnées des solutions (à l'instar de la triangularisation de Gauss dans le cas linéaire). Une telle représentation est une base de Gröbner associée à un ordre monomial dit lexicographique. Le calcul direct d'une telle base est souvent prohibitif et on passe classiquement par un calcul de base de Gröbner pour un ordre monomial dit *gradué* (qui filtre les monômes, d'abord, par leur degré). Puis on applique un algorithme de changement d'ordre qui revient à faire des opérations d'algèbre linéaire dans un anneau quotient qui a le bon goût d'avoir aussi une structure d'espace vectoriel de *dimension finie*. Ces opérations reviennent à calculer le polynôme caractéristique d'une matrice associée à un endomorphisme de multiplication dans cet anneau. Elles ont jusqu'à présent été pensées en lien avec la parcimonie de cette matrice.

Dans [Berthomieu et al., 2022b], nous opérons le *changement de paradigme* suivant : au lieu d'être aveuglé par la parcimonie de ces matrices, nous exhibons une structure spécifique à ces endomorphismes de multiplication. Nous corrélons cette structure à la théorie des modules en algèbre commutative d'une part, et aux progrès récemment effectués sur l'algorithmique des matrices polynomiales d'autre part. Cela nous permet d'obtenir une

complexité $\log$-linéaire en $t^{\omega-1}D$ où ω est l'exposant de la multiplication matricielle, D est le nombre de solutions et $t \ll D$ est le nombre de polynômes utiles pour définir l'endomorphisme de multiplication étudié. Ceci permet d'obtenir un facteur d'accélération signaficatif en pratique car, dans le cas générique, ce facteur est exponentiel en le nombre de variables. Ce résultat fait l'objet d'une fiche du portfolio.

Pour le problème (B), nous considérons les systèmes d'équations polynomiales à coefficients rationnels et dépendant de paramètres qui ont un nombre fini de solutions complexes pour des spécialisations génériques de ces paramètres. D'après un théorème de Tarski, on peut classifier le nombre de solutions réelles de ces systèmes par des formules polynomiales. Dans [Le and Safey El Din, 2022], *nous refondons l'algorithmique de ce problème en proposant de nouvelles structures de données en sortie*. L'idée est d'encoder les sorties de ces algorithmes non plus par des formules écrites classiquement dans une base monomiale mais comme des mineurs de matrices polynomiales. Ces sorties sont plus pertinentes pour le contexte applicatif de ces algorithmes. Nous obtenons les *premiers résultats de complexité simplement exponentielle* pour ce problème qui soient cubiques en $n\delta^{nk}$ où δ est le degré des équations polynomiales données en entrée, n est le nombre de variables et k le nombre de paramètres. Une première implantation de cet algorithme permet de résoudre des problèmes hors d'atteinte par l'état de l'art, notamment une application en physique (synchronisation d'oscillateurs couplés).

Cet algorithme est un des ingrédients du nouvel algorithme proposé dans [Le and Safey El Din, 2021] pour le problème (C), c'est-à-dire, l'élimination d'un bloc de quantificateurs sur les réels (géométriquement, cela consiste à calculer une formule qui définit la projection de l'ensemble des solutions réelles d'un systèmes d'équations polynomiales à coefficients réels). Nous obtenons une complexité cubique en $n2^k\delta^{pk}(\delta-1)^{(n-p-1)k}$ où p est le nombre d'équations données en entrée. Il s'agit du *premier résultat de complexité où les constantes en exposant* sont explicitées pour ce problème (il était connu qu'on pouvait le résoudre en $\delta^{O(kn)}$). Notons aussi que cet algorithme devient polynomial en n quand p et k sont fixés. Ici aussi, *les performances obtenues en pratique sont spectaculaires* et permettent de résoudre des problèmes qui étaient hors de portée jusqu'à présent.

Pour le problème (D), nous avons poursuivi nos travaux sur le comptage de composantes connexes des solutions réelles de systèmes d'équations polynomiales initiés dans [Safey El Din and Schost, 2011, Basu et al., 2014]. Ces travaux culminent avec l'algorithme décrit dans [Safey El Din and Schost, 2017], dont la complexité est essentiellement en $O\left((n\delta)^{6n\log_2(d)}\right)$, sous des hypothèses de régularité classiques, (d est la dimension de l'ensemble étudié). Il s'agit du *premier algorithme de complexité asymptotiquement optimal* au sens où dans le pire cas, le nombre de composantes connexes est en $O\left(\delta^n\right)$ et où la complexité de cet algorithme, qui fait l'objet d'un élément de notre portfolio, est *sous-quadratique en la taille de sa sortie*. L'existence d'un tel algorithme était un problème ouvert depuis la thèse de J. Canny [2].

Tous les systèmes polynomiaux ne sont pas durs à résoudre

On l'a dit plus haut, la résolution de systèmes polynomiaux est un problème prouvé difficile dans le pire cas, en tout cas exponentiel en le nombre de variables (alors que dans le cas linéaire ce problème est résoluble en temps polynomial). *Comprendre finement et classifier les classes de problèmes résolubles en temps polynomial, sous-exponentiel ou exponentiel* est un *enjeu majeur* pour les applications.

Cela implique d'exploiter toute propriété mathématiquement structurante qui pourrait impacter sur les tailles de sortie qu'il convient alors d'identifier précisément et d'exploiter algorithmiquement. C'est ce que nous avons fait pour trois grandes classes de structures : *(1)* les structures déterminantielles, fréquentes dans les applications cryptographiques et robotiques qui encodent des chutes de rang dans des matrices polynomiales ; *(2)* les structures multi-homogènes, fréquentes pour encoder des phénomènes physiques et enfin *(3)* les systèmes polynomiaux invariants par actions de groupes.

Nos travaux concernant le cas déterminantiel relèvent du problème (A). Dans [Berthomieu et al., 2022a], nous décrivons la *structure d'une base de Gröbner* dans le cas déterminantiel. Ce résultat permet de *prévoir asymptotiquement le paramètre* t évoqué plus haut et donc des résultats de complexité particulièrement fins. Il peut permettre à plus long terme de déboucher sur des algorithmes de calcul de bases de Gröbner dédiés. Aussi, l'équipe étend sa panoplie algorithmique au-delà des bases de Gröbner : dans [Hauenstein et al., 2021], nous développons des algorithmes pour le problème (A) basés sur des *méthodes d'homotopie symbolique* dans le cas déterminantiel. Ceux-ci s'appuient sur des bornes sur le nombre de solutions, spécifiques au cas déterminantiel et issues de la théorie de l'intersection en géométrie algébrique. Il en résulte les *premiers algorithmes de complexité quadratique en la taille de la sortie* pour cette classe de systèmes.

Le cas multi-homogène est important (les degrés par "paquets de variables" ne coïncident pas avec le degré total des polynômes) : ces systèmes encodent naturellement des situations physiques (les équations de la physique étant naturellement homogènes globalement) ou arithmétiques. Dans le cas où les coefficients des systèmes

considérés vivent dans un corps assez grands, nous obtenons dans [Safey El Din and Schost, 2018], un algorithme de *complexité quadratique en la taille de la sortie* qui est déterminée par des bornes sur le nombre de solutions, spécifiques au cas multi-homogène (là encore, celles-ci proviennent de la théorie de l'intersection en géométrie algébrique).

Pour le problème (B), nous avons considéré le cas des systèmes polynomiaux dits équivariants par action du groupe symétrique. Dans [Riener and Safey El Din, 2018], nous exhibons un *premier algorithme dont la complexité est polynomiale* sur les classes de problèmes où le degré δ est fixé et le nombre de variables croît. Un ingrédient clé de ce travail est de s'appuyer sur la *théorie de la représentation* des familles de polynômes équivariantes par action du groupe symétrique et la théorie des modules associés pour obtenir des gains de complexité de l'ordre de la complexité combinatoire du groupe symétrique.

Des logiciels à fort impact et des applications spectaculaires en robotique

Le développement et la publication de la bibliothèque open source `msolve` (voir [Berthomieu et al., 2021]), écrite en C (plus de 40 000 lignes de code) assure la pérennité du savoir-faire de l'équipe et ses performances permettent des calculs de bases de Gröbner et la résolution de systèmes polynomiaux, au sens de (A), qui étaient hors de portée il y a 5 ans. Son intégration dans des systèmes de calcul formel généralistes comme SAGEMATH et OSCAR atteste du succès qu'elle rencontre. Une fiche du portfolio lui est consacrée.

Ces développements logiciels sont essentiels pour que l'équipe puisse *augmenter son impact scientifique* par la résolution d'applications. Ces dernières années ont vu *une série de succès importants dans différents domaines de la robotique*. Notre savoir-faire calculatoire [García Fontán et al., 2022] a permis de faire l'analyse complète des singularités liées à l'observation de $N > 3$ droites/points par des systèmes mécaniques sous asservissement visuel, *étendant ainsi significativement l'état de l'art dans ce domaine* et donnant les outils pour fiabiliser les estimations de pose de caméra. Toujours en robotique, dans [Trutman et al., 2022], *nous fiabilisons la résolution de problèmes de cinématique inverses* en les réduisant à des problèmes d'optimisation dans lesquels le calcul de base de Gröbner est utilisé comme un pré-conditionneur au calcul numérique. Enfin, les progrès effectués sur le problème (D) nous ont permis de fournir le premier algorithme décidant le problème de cuspidalité en robotique dans [Chablat et al., 2022]. Cet algorithme est de complexité simplement exponentielle en le nombre de variables (on ne peut espérer guère mieux) et qu'une première implantation prototype a montré son potentiel. Toujours sur la thématique des singularités cinématiques, nous donnons dans [Capco et al., 2020] un algorithme (toujours basé sur la résolution du problème (D)) permettant d'effectuer automatiquement une telle analyse sur toute une famille de problèmes. Le potentiel de cet algorithme est illustré sur son application à la famille des robots *UR* commercialisés par Universal Robots et dont les paramètres de conception sont publics.

Enfin, l'équipe a renoué avec une tradition de résolution de problèmes en mathématiques dites expérimentales. Nous avons contribué à la conception et l'analyse de complexité d'algorithmes calculant des témoins d'algébricité de solutions d'équations fonctionnelles associées à des séries génératrices à variables catalytiques [Bostan et al., 2022]. Ces algorithmes dont la génèse remonte aux travaux de Bousquet-Mélou et Jehanne [1] trouvent des applications naturelles et importantes en combinatoire. En géométrie algébrique rélle, nous calculons dans [Le et al., 2022], à l'aide de l'algorithme développé dans [Le and Safey El Din, 2022], des contre-exemples à une conjecture de Huismann sur le nombre de points réels à l'intersection d'une hypersurface et d'une courbe algébrique.

Enfin, sur la période d'évaluation, les travaux en cryptologie post-quantique ont principalement porté sur un *transfert technologique d'ampleur*, notamment via la création de la startup CRYPTONEXT SECURITY et la participation à la normalisation de cette cryptographie. Il ne s'agit pas d'avancées scientifiques majeures ; aussi les éléments saillants de cette activité sont décrits dans la section 3.

Animation scientifique de l'équipe

L'équipe organise un *séminaire mensuel conjoint avec l'équipe* MATHEXP (Centre Inria de Saclay). Ce séminaire réunit entre 20 et 50 participants et se déroule d'une fois sur l'autre soit à Saclay soit à Paris. Ceci permet de renforcer nos liens nombreux avec cette équipe. Ce séminaire commun concourt également à structurer la communauté dans la région parisienne et a été le point de départ de l'organisation du trimestre thématique Recent Trends in Computer Algebra (RTCA) que nous co-organisons à l'IHP en 2023.

À cela s'ajoutent des *groupes de travail/lecture* en comités plus restreints et qui réunissent les permanents et des doctorants ou post-doctorants. L'objectif est de compléter leur formation de base (notamment en début de thèse) pour leur permettre d'appréhender plus rapidement l'état de l'art et, dans un second temps, de susciter des collaborations entre doctorants/post-doctorants.

L'organisation de ces groupes de travail est rendue aisée par une *politique de co-encadrement assumée* dans l'équipe, soit en interne dans l'équipe, soit avec d'autres équipes de recherche (deux doctorants sont ainsi co-encadrés au LIP6), soit avec d'autres groupes de recherche en France, ou des co-tutelles internationales (3 étudiants sont concernés sur la période d'évaluation par des co-tutelles). Il n'y a qu'un seul doctorant dans l'équipe qui n'ait qu'un seul encadrant.

À cela, s'ajoute depuis un an, une *réunion hebdomadaire* qui vise à coordonner les *développements logiciels* par les permanents de l'équipe, notamment autour de la bibliothèque `msolve`.

2 INTRODUCTION DU PORTFOLIO

Cette section identifie les éléments de portfolio présentés par l'équipe PolSys. Chaque élément disposant de sa propre fiche explicative, nous nous contentons ici d'en donner une liste simple :

- *Élément 1 (création d'entreprise) :* CRYPTONEXT SECURITY est une startup issue des laboratoires de Sorbonne Université, du CNRS et de l'INRIA, créée par deux membres de l'équipe. La société valorise le savoir-faire de l'équipe en cryptographie post-quantique. CRYPTONEXT SECURITY commercialise des solutions logicielles qui permettent aux entreprises et gouvernements d'effectuer la transition de leurs infrastructures vers la cryptographie de nouvelle génération, post-quantique. La startup a déjà travaillé avec le gouvernement français ainsi qu'avec des clients nationaux et internationaux dans les domaines de la finance et la défense.
- *Élément 2 (logiciel ou bibliothèque logicielle) :* `msolve` est la bibliothèque open source de calcul de bases de Gröbner et de résolution de systèmes polynomiaux [Berthomieu et al., 2021], écrite en C, dont le développement est transverse dans l'équipe et conjoint avec TU Kaiserslautern, et qui est en cours d'intégration dans les systèmes de calcul formel généralistes SAGEMATH et OSCAR. Ses performances pratiques sont supérieures de plusieurs ordres de grandeur aux performances des logiciels de l'état de l'art. Elle a été utilisée pour résoudre une large gamme de problèmes, provenant d'applications, complètement inaccessibles par l'état de l'art.
- *Élément 3 (article) :* [Safey El Din and Schost, 2017] *A Nearly Optimal Algorithm for Deciding Connectivity Queries in Smooth and Bounded Real Algebraic Sets*, publié au *Journal of the ACM*, la revue "flagship" de l'ACM qui indique sur sont site web : "To be accepted, a paper must be judged to be truly outstanding in its field". Dans cet article, nous atteignons, pour la première fois depuis 1988 [2], des bornes de complexité quasi optimales pour le comptage de composantes connexes d'ensembles de solutions réelles de systèmes polynomiaux à coefficients réels (sous des hypothèses non restrictives).
- *Élément 4 (article) :* [Berthomieu et al., 2022b] *Faster change of order algorithm for Gröbner bases under shape and stability assumptions*, publié dans les actes de la *conférence ACM ISSAC* (International Symposium on Symbolic and Algebraic Computation), qui est la conférence de référence pour le calcul formel. Nous considérons cet article comme précurseur des innovations à venir sur l'algorithmique du calcul de bases de Gröbner car il met en œuvre, pour la première fois, le changement de paradigme qui consiste à mieux exploiter la théorie des modules du point de vue purement algébrique et les structures apparaissant dans les réductions aux problèmes d'algèbre linéaire du point de vue calculatoire. Dans les situations génériques, cet algorithme permet d'obtenir des facteurs d'accélération qui sont exponentiels en le nombre de variables.

3 AUTOÉVALUATION DU BILAN

3.1 Autoévaluation de l'équipe

Domaine 2. Attractivité

Référence 1. L'unité est attractive par son rayonnement scientifique et s'insère dans l'espace européen de la recherche.

L'équipe participe aux évènements internationaux structurant la communauté et organise fréquemment des conférences ou workshops pour participer à l'effort d'animation de la communauté scientifique. La conférence ISSAC constitue le centre névralgique de la communauté ; nous y participons ainsi qu'à des évènements soit plus ancrés dans les mathématiques (comme les conférences MEGA et SIAM AG) soit dans des domaines d'application.

Organisation de conférences ou workshops internationaux. ISSAC 2019 (General co-chair), workshop final POEMA, Eurocrypt 2017, Quantum-Safe Cryptography for Industry 2017.

Participation à des comités de programmes.. ISSAC (PC chair en 2017, puis 2018, 2020–2022, membre du steering committee depuis 2021), Poster committee chair d'ISSAC 2019, PASCO (co-chair en 2017), MACIS (2017), PKC (2017), CASC (2017, 2018), CHES (2017–2019), CARDIS (2018, 2019), COSADE (2018).

Invitations pour exposés pleiniers dans des conférences ou workshops internationaux (non exhaustives). Workshops Real Algebraic Geometry and Optimization du trimestre Non-linear algebra à l'ICERM, Solving polynomial equations au CWI, les workshops Conic linear optimization and computer-assisted proofs, Real Algebraic Geometry with a View Toward Hyperbolic Programming and Free Probability, Real Algebraic Geometry with a View Toward Moment Problems and Optimization à Oberwolfach, Geometry of Real Polynomials à Banff International Research Station, AMUSEC, Conférence MEGA 2021, ou encore au niveau national, les Structured Matrix Days.

Invitations pour séjours de recherches dans des institutions académiques. les membres de l'équipe ont été régulièrement invités à l'université de Waterloo, Czech Tech. Univ. de Prague, City Univ. of New-York, l'université J. Kepler, l'ICERM aux USA, pour ne citer que les invitations les plus importantes.

Comités éditoriaux. Journal of Symbolic Computation (et éditeur invité pour un numéro spécial), Journal of Algebra (computational section), Journal of Cryptographic Engineering, Designs, Codes and Cryptography, The Computer Journal, Mathematics in Computer Science (editor-in-chief), SN Computer Science, Texts and Monographs in Symbolic Computation.

Prix et distinctions. Des membres de l'équipe ont reçu le prix Atos – Joseph Fourier 2018 dans la catégorie "calcul quantique", le distinguished student author award à la conférence ISSAC 2017, le distinguished software demonstration award à ISSAC 2018, le troisième prix de la compétition chinoise post-quantique en 2020 et le best paper award du Journal of Complexity en 2021. Des membres de l'équipe sont nommés dans le Top 100 des inventeurs français par le magazine Le Point en 2022, nominé pour la médaille de bronze du CNRS en section 6 à deux reprises et membre junior de l'IUF depuis 2012. Enfin, des membres de l'équipe ont participé à la soumission du schéma de signature post-quantique GeMSS, un schéma de signature post-quantique qui a atteint le troisième tour du processus de normalisation post-quantique du NIST de 2020.

Responsabilités dans les instances académiques. Vice présidence de la commission recherche de l'UFR d'ingéniérie, Chargé de mission "informatique" auprès du Vice-Doyen Recherche de la FSI de SU, membre élu au conseil des doctorants du LIP6, membre élu au collège D (docteurs) pour le conseil de la FSI de SU, et enfin membre élu au collège étudiants à la Commission de la Formation et de la Vie Universitaire.

Référence 2. L'unité est attractive par la qualité de sa politique d'accompagnement des personnels.

Les doctorants et post-doctorants bénéficient d'un encadrement pro-actif qui vise à les former le plus efficacement possible, non seulement pour leur thèse mais en prévision aussi de leur insertion professionnelle (qu'elle soit académique ou non). Il leur est proposé de *(a)* suivre des cours, notamment au MPRI ou dans le parcours de master SFPN pour compléter leur formation de base et *(b)* participer à des groupes de travail soit organisés autour de sujets assez théoriques, soit autour de problèmes de programmation spécifiques au calcul formel. Un groupe de travail interne est dédié à *(c)* des séances de répétitions pour les exposés que les doctorants et post-doctorants vont faire dans des conférences (par défaut, ce sont eux qui présentent les travaux communs). Aussi, *(d)* le séminaire permet d'exposer nos doctorants et post-doctorants à des sujets qui ne sont pas développés dans

notre équipe. Enfin, pour ceux qui ont le plus d'expérience, il leur est proposé *(e)* une visite dans un laboratoire à l'étranger (auprès de nos collaborateurs) pour qu'ils commencent à développer leur réseau indépendamment de leur direction de thèse. Finalement, *(f)* des groupes de relecture sont organisés pour les post-doctorants et doctorants en fin de thèse pour les aider à constituer leurs dossiers de candidature. Cette politique pro-active a conduit à de bons résultats sur le dernier quinquennat : 1 CR Inria, 1 CR au CEA, 1 post-doctorant classé 2^e sur un concours MCF 6 mois après l'obtention de sa thèse.

Pour ce qui est de l'accueil des plus jeunes permanents, l'équipe met en œuvre tous les moyens à sa disposition pour leur développement scientifique. Ils sont très fortement incités à se rendre en conférences, ils sont très tôt associés à des co-encadrements de thèse (tous les MCF de l'équipe ont un ou plusieurs co-encadrements en cours), eux aussi sont fortement incités à soit inviter des chercheurs exerçant à l'étranger, soit à leur rendre visite. Lorsqu'ils deviennent un peu plus âgés, ils sont stimulés et aidés sur le montage de projet.

Dans l'équipe, toute personne participant à l'élaboration des résultats d'un article est co-signataire. L'ordre alphabétique est pratiqué dans les revues et actes de conférences où nous publions.

Référence 3. L'unité est attractive par la reconnaissance de ses succès à des appels à projets compétitifs.

Notre stratégie de participation et de développement de projets collaboratifs se décline sur plusieurs niveaux. Certains projets portent directement sur notre cœur de métier et d'autres sont plus orientés vers des applications, comme par exemple la cryptographie, la robotique ou la combinatoire. Nous mentionnons ci-dessous les projets les plus emblématiques de la période d'évaluation, la liste complète étant fournie par ailleurs.

Projets internationaux.

- **POEMA** (Polynomial Optimization, Efficiency through Moments and Algebra, 2018–2023) : un projet Marie Skłodowska Curie H2020-MSCA-ITN (Innovative Training Network), qui se trouve être un réseau doctoral européen regroupant des nœuds en France, aux Pays-Bas, en Allemagne, en Italie, au Royaume-Uni et en Norvège. Ce projet a permis le financement de deux thèses. L'équipe a participé à la conception d'algorithmes exacts pour l'optimisation polynomiale, leur analyse et leur implantation. C'est un projet *cœur de métier*.
- **NonNegativeRank** (2017–2018) : projet H2020 Marie Skłodowska Curie de bourse postdoctorale, attribué à K. Kubjas et mis en place dans PolSys en partenariat avec C. Uhler (MIT). K. Kubjas est actuellement maîtresse de conférences en Finlande.
- **ECARP** (Efficient Certified Algorithms for Robot motion Planning, 2019–2024) : un PRCI ANR–FWF entre la France et l'Autriche qui a permis le financement d'une thèse. Les résultats principaux qui en découlent sont de nouveaux algorithmes pour le calcul de cartes routières, permettant de résoudre des problèmes de connexité, et un algorithme permettant de déterminer si un robot est *cuspidal*, après avoir mis ses caractéristiques sous forme d'équations polynomiales. Si nos contributions sont fondamentales, c'est un *projet orienté vers des applications en robotique* dont le consortium est pluri-disciplinaire.
- **AFOSR** : un projet financé par l'US Air Force (Air Force Office for Scientific Research) pour le guidage automatique, 2021–2024, que nous portons avec E. Trélat du LJLL (laboratoire de mathématiques appliquées, SU). Il a permis de financer un post-doc (Georgy Scholten) pour la résolution de problèmes de contrôle optimal par réductions à des systèmes algébriques en vue d'applications au guidage automatique. Il s'agit d'un projet *cœur de métier*.
  Mentionnons également les participations à deux programmes européens COST (European Cooperation in Science & Technology) : **CryptoAction** et **CRYPTACUS**.

PIA. RISQ (Regroupement de l'Industrie française pour la Sécurité Post-Quantique, 2017–2020) : Il a financé deux thèses. L'équipe a pu proposer plusieurs schémas au processus de normalisation post-quantique du NIST, (GeMSS et CFPKM). Il s'agit d'un *projet orienté sur les applications en cryptologie*.

Projets nationaux.

- **SESAME** (Singularités et Stabilité des Asservissements référencés Capteurs, 2019–2020) : SESAME, un PRC de l'ANR, a financé une thèse. Parmi les résultats obtenus, on peut noter une analyse des singularités de systèmes d'asservissement visuel, ce qui permettra de les fiabiliser en vue d'une meilleure intégration industrielle. Il s'agit d'un *projet orienté vers les applications en robotique*.
- **De Rerum Natura** (Deciding irrationality and transcendence, 2020–2024) : Le but de De Rerum Natura, un PRC de l'ANR, est de concevoir des algorithmes pour la classification en théorie des nombres et en combinatoire. Il s'agit d'un projet *cœur de métier* dont le consortium est à cheval entre mathématiques et

informatique. L'équipe contribue à ce projet en concevant des algorithmes pour la résolution d'équations fonctionnelles (étroitement reliées à la résolution de systèmes polynomiaux).

Projets régionaux et locaux. Nous avons bénéficié du support de plusieurs projets d'envergure plus locale, notamment via le PGMO, l'appel Tremplin de Sorbonne Université et le dispositif de projets LIP6. Ci-dessous, nous mentionnons plus particulièrement un projet structurant financé par la région IdF.

Citons aussi **Hmm** (Symbolic-numerical algorithms for Holonomic Method of Moments, 2021–2024) : Un projet financé par le DIM-RFSI de la région Île-de-France. Ce projet a permis le financement d'un post-doc pour le calcul des moments de grand ordre d'une mesure en exploitant les relations de récurrence linéaires satisfaites par ces moments. Il s'agit d'une collaboration avec l'équipe MATHEXP.

Ces contrats sont aussi utilisés pour l'achat de serveurs de calculs spécifiques (voir ci-dessous).

Référence 4. L'unité est attractive par la qualité de ses équipements et de ses compétences techniques.

Nous avons des besoins en ressources de calculs qui sont relativement spécifiques (grosse consommation mémoire, temps de calcul difficiles à prédire, etc.) et pas toujours comblés par les plateformes. Aussi, une partie significative du budget de l'équipe (sur ressources propres) va dans l'achat et la jouvance d'un nombre modéré de serveurs de calculs dédiés. Cet outil de travail quotidien (et complémentaire des ressources de calculs du LIP6) est précieux pour pleinement exploiter la puissance de nos algorithmes et logiciels. Ces serveurs ont été décisifs pour des applications en robotique, dans le cadre des projets ANR SESAME [García Fontán, 2023], et ECARP [Capco et al., 2020] ainsi que pour le calcul de contre-exemples [Le et al., 2022] à une conjecture en géométrie algébrique réelle.

Un des serveurs de calculs a constitué la base des discussions sur l'identification des architectures considérées pour le cluser de calculs CONVERGENCES du LIP6. L'équipe contribue aussi financièrement à ce cluster (financement de 15 000 euros en 2022).

Domaine 3. Production scientifique

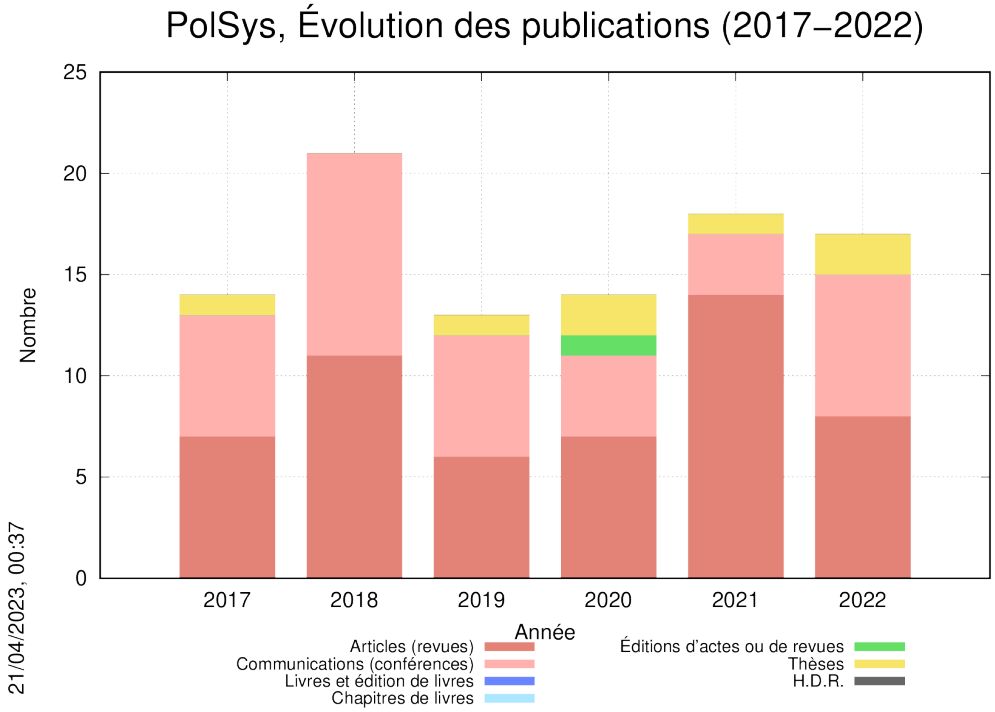

FIGURE 1 – Évolution des publications entre 2017 et 2022

	2017	2018	2019	2020	2021	2022
Articles (revues)	2.00	3.14	3.00	7.00	14.00	4.00
Communications (conférences)	1.71	2.85	3.00	4.00	3.00	3.50

TABLE 2 – Publications par ETPR par an entre 2017 et 2022

Référence 1. La production scientifique de l'unité satisfait à des critères de qualité.

Fondements théoriques et méthodologiques. Nos articles publiés relèvent très majoritairement de la conception d'algorithmes opérant sur des objets mathématiques (polynômes, matrices, suites récurrentes, etc.). Du point de vue méthodologique, nous nous appuyons sur des *résultats quantitatifs de la géométrie algébrique et de l'algèbre commutative* (degré et hauteur de variétés algébriques, indices de régularité d'idéaux polynomiaux, etc.) pour identifier des *bornes inférieures* sur les tailles des objets calculés qui sont représentés algébriquement par le calcul formel. Notre démarche consiste ensuite à obtenir des algorithmes qui soient dans le pire cas polynomiaux en ces bornes inférieures (et ultimement quasi optimaux). Cette démarche est parfaitement illustrée par [Berthomieu et al., 2022b] et [Safey El Din and Schost, 2017] (articles choisis pour le portfolio) où les algorithmes obtenus sont de complexité sous-quadratique en le maximum des tailles des entrées/sorties dans le pire cas.

Dès qu'on comprend les limites des modèles utilisés, cette démarche, guidée par la théorie de la complexité, ne fait plus débat : elle a permis à la communauté de calcul formel d'effectuer des progrès spectaculaires, d'identifier et valider de nouveaux paradigmes algorithmiques qui ont le potentiel de *rendre calculable demain ce qui est hors de portée aujourd'hui*, ou bien d'obtenir des performances pratiques spectaculaires dès maintenant.

L'outillage mathématique mis en œuvre dans ces activités relève de l'algèbre commutative et de la géométrie algébrique. La solidité de ces domaines des mathématiques, qui ont traversé plusieurs siècles, est plus qu'avérée. Ceci nous conduit à publier régulièrement dans des revues de mathématiques ([Berthomieu et al., 2022a] au Journal of Algebra, [Fawzi and Safey El Din, 2018] au SIAM Journal on Applied Algebra and Geometry et [Magron et al., 2022] au SIAM Journal on Optimization).

Le troisième aspect méthodologique que nous développons consiste à dépasser les limites des modèles de complexité théorique en implantant nos algorithmes, à bas niveau si nécessaire, et à les confronter à des applications réputées difficiles et qui s'avéraient hors de portée de l'état de l'art. Le choix de la bibliothèque logicielle `msolve` [Berthomieu et al., 2021] dans notre portfolio illustre cette démarche. Elle a déjà été utilisée pour résoudre des applications en mathématiques (étude de conjectures en géométrie algébrique réelle [Le et al., 2022]), en physique [Le and Safey El Din, 2022], en combinatoire [Bostan et al., 2023b] ou en robotique [García Fontán, 2023].

Choix des supports de publications. Nous mettons en œuvre une stratégie de diffusion équilibrée du point de vue thématique. Notre recherche ayant un contenu mathématique fort, nous publions parfois dans des revues de mathématiques reconnues pour leur qualité comme celles indiquées ci-dessus en plus des revues de calcul formel classiques, notamment la revue de référence Journal of Symbolic Computation. Parmi les revues plus généralistes, nous privilégions régulièrement le Journal of Complexity pour des résultats de complexité qui ont le potentiel d'intéresser des communautés plus larges que celle de calcul formel et pour les résultats exceptionnels le Journal of the ACM. Dans tous les cas, il s'agit de revues reconnues pour leur qualité et le sérieux des procédures d'évaluation des soumissions.

De plus, notre stratégie de diffusion s'appuie sur une présence régulière dans les conférences du domaine. En premier lieu, la conférence de référence pour le calcul formel est la conférence ACM ISSAC (International Symposium on Symbolic and Algebraic Algorithms). Nous y publions régulièrement. Il existe d'autres conférences de calcul formel mais celles-ci sont moins exigeantes qu'ISSAC. Enfin, sur le versant plus mathématique du calcul formel, on trouve notamment les conférences :

- SIAM AAG (Applied Algebra and Geometry) qui est construite sur un modèle SIAM classique (regroupement de plusieurs mini-symposia) et qui regroupe approximativement 800 chercheurs sur tout ce qui touche les méthodes effectives en algèbre et géométrie algébrique ; nous y participons régulièrement, tant via l'organisation de mini-symposia que via des exposés ;
- MEGA (Effective Methods on Algebraic Geometry) dont l'audience est plus réduite et certainement plus mathématique, cette conférence ayant plus évolué vers l'étude des propriétés des objets mathématiques de la géométrie algébrique effective ; nous sommes moins fréquemment présents dans cette conférence ;
- ACA (Applications of Computer Algebra) rassemble entre 100 et 200 participants et propose des exposés pléniers ainsi que 3 à 5 sessions parallèles chacune sur une thématique ciblée. La spécificité d'ACA est de se focaliser sur des domaines d'applications, recoupant les intérêts de SIAM AAG et MEGA mais ouvrant également par exemple vers les sciences de la vie, éducation, les systèmes dynamiques. Comme pour

MEGA, nous y sommes moins fréquemment présents.

Enfin, pour valider nos contributions dans des domaines applicatifs, nous publions régulièrement (mais à une fréquence moindre) dans des revues ou conférences des domaines concernés comme International Journal of Computer Vision ; IEEE Robotics and Automation Letters ; Information and Computation ; IEEE Transactions on Information Theory ; Designs, Codes and Cryptography ; Journal of Mathematical Biology. La stratégie de publication en cryptographie s'est adaptée aux évolutions de l'équipe pendant la période d'évaluation. Les publications de l'équipe dans le domaine ciblent des conférences plus appliquées, comme CHES [Faugère et al., 2019], ou la rédaction de documents pour les agences de normalisations (ETSI [Perret, 2021], NIST [Casanova et al., 2017]).

Positionnement national et international. Le continuum que nous assurons entre développements mathématiques théoriques pour maîtriser et comprendre les tailles d'entrée et de sortie de nos algorithmes, conception et implantation de ces algorithmes pour la résolution de systèmes algébriques non-linéaires et enfin la confrontation de ces productions à des applications difficiles constitue l'ADN de PolSys qui est commun à assez peu d'équipes de calcul formel en France et ailleurs à l'international.

Ce positionnement nous amène à collaborer et échanger avec des équipes de pointe sur le territoire national comme au niveau international. Dans la région parisienne, citons notamment l'équipe MAX du LIX (École polytechnique) : M. Mezzarobba (CR CNRS) contribue à l'intégration de `msolve` dans SAGEMATH et G. Pogudin (Assistant Professor, École polytechnique) en est un utilisateur régulier. Nous avons déjà mentionné notre partenaire privilégié MATHEXP dont l'expertise sur les équations fonctionnelles, aux récurrences et différentielles est très complémentaire à la nôtre. Plusieurs séries d'articles et encadrements communs illustrent le potentiel de notre rapprochement.

Au niveau national, nous avons une proximité avec G. Villard et B. Salvy [Neiger et al., 2021] de l'équipe ARIC (ENS Lyon, CNRS, Inria) autour des questions liées aux algorithmes de calcul formel sur les matrices polynomiales. Nous co-organisons le trimestre IHP RTCA. Notre positionnement sur les méthodes algébriques nous rend complémentaires de l'équipe INRIA AROMATH qui est plus concentrée sur les méthodes semi-numériques. Nous avons collaboré au sein du réseau doctoral POEMA.

Nous collaborons avec les membres de l'équipe POP du LAAS-CNRS, eux aussi membres du réseau POEMA, depuis plus d'une dizaine d'années sur l'utilisation du calcul formel en optimisation polynomiale.

Notre investissement applicatif se concrétise par un réseau de collaborations avec des équipes de robotique, notamment au LS2N, sur différents problèmes calculatoires intervenant dans l'analyse géométrique de manipulateurs sériels ou parallèles [García Fontán et al., 2022, Chablat et al., 2022]. Ce champ applicatif a donné lieu à de nombreuses collaborations internationales, en particulier en Autriche avec l'Université J. Kepler, un haut lieu du calcul formel européen, et l'Université d'Innsbruck avec laquelle nous portons le projet ANR PRCI ECARP [Capco et al., 2020, Capco et al., 2023] ainsi que la Czech Technical University (CTU) de Prague [Trutman et al., 2022]. Enfin, pour des applications qui relèvent de la planification et du contrôle de trajectoires, nous travaillons avec le Laboratoire Jacques Louis Lions (E. Trélat, SU) dans le cadre d'un projet financé par l'AFOSR. Nous mettons en œuvre notre expertise sur la résolution de systèmes polynomiaux et les capacités de `msolve` pour les combiner à des méthodes directes de résolution de problèmes de contrôle optimal (méthodes de tirs) via des approximants polynomiaux. Plusieurs applications ont aussi été résolues en biologie.

Suite au montage de la startup CRYPTONEXT SECURITY, l'essentiel des activités sur ce domaine applicatif a relevé du transfert de technologies. Des collaborations ont pu être maintenues au niveau international, principalement avec la Chinese Academy of Sciences (Laboratoire de Cybersecurité, Chine, Pékin) dans le cadre d'une compétition Chinoise sur le post-quantique [Beullens et al.,] et une collaboration avec la City University of New York (USA) [Battarbee et al., 2022]. Au niveau national, l'équipe a pris le temps de construire une collaboration avec le laboratoire de cryptologie de Thalès en apportant son expertise sur la résolution de systèmes polynomiaux structurés, sur l'analyse de la complexité du calcul de bases de Gröbner et en exploitant là encore les capacités de `msolve`. *Un financement de Google ($150k$\$) soutiendra également l'équipe dans le développement de `msolve` et dans le cadre de l'activité de cryptanalyse des primitives post-quantiques*.

En plus des collaborations internationales mentionnées plus haut, nos partenaires internationaux privilégiés sont :

- l'équipe de calcul formel du département d'informatique de l'Université de Waterloo (G. Labahn et É. Schost), avec qui nous avons deux thèses en co-tutelle et des résultats de complexité théorique marquants (voir par exemple [Safey El Din and Schost, 2017] et le portfolio). Dans le cadre de ces collaborations, nous apportons notre expertise sur la géométrie et l'algèbre des systèmes polynomiaux, ainsi que sur l'algorithmique des matrices polynomiales.
- l'équipe d'algèbre du département de mathématiques de TU Kaiserslautern (C. Eder) avec qui nous avons une thèse en co-tutelle, développons une algorithmique nouvelle génération pour le calcul de bases de Gröbner, ainsi que la bibliothèque logicielle `msolve` qui fait l'objet d'une fiche de notre portfolio.

Référence 2. La production scientifique de l'unité est proportionnée à son potentiel de recherche et correctement répartie entre ses personnels.

Du fait du contenu mathématique des recherches menées dans l'équipe, la plupart des doctorants proviennent de master de Mathématiques avec une spécialisation en algèbre et géométrie. Pour favoriser leur mue vers l'informatique, ils sont encouragés et encadrés pour implanter les algorithmes qu'ils développent en cours de thèse, le plus souvent dans des systèmes de calcul formel généralistes. *Sauf exception, les personnels non permanents ne participent pas au développement de logiciels à bas niveau*, comme `msolve`, pour ne pas diluer leurs efforts. Ils sont encouragés à publier leurs résultats et l'encadrement est conduit de manière telle que les plus autonomes d'entre eux sont en capacité de publier seuls (ou, à tout le moins, sans leur équipe de direction de thèse) avant leur soutenance de thèse. Tout résultat impliquant des doctorants ou post-doctorants est présenté en conférence par un des doctorants ou post-doctorants concerné de manière à maximiser leur visibilité.

Notre politique d'invitations de chercheurs est aussi pensée pour maximiser les interactions entre les collègues invités et les membres de l'équipe (permanents comme non permanents).

Les différents groupes de travail organisés dans l'équipe permettent de faire participer jeunes et moins jeunes sur une variété de travaux théoriques qui peuvent toucher tous les aspects de la résolution de systèmes polynomiaux : calcul de bases de Gröbner, systèmes à paramètres, résolution sur les réels, applications, etc. Cela permet de maintenir un niveau d'activités de recherche relativement élevé sur l'ensemble de l'équipe.

Référence 3. La production scientifique de l'unité respecte les principes de l'intégrité scientifique, de l'éthique et de la science ouverte. Elle est conforme aux directives applicables dans ce domaine.

En plus des dispositifs mis en place par le LIP6, nous avons une politique active de mise à disposition des codes sources de nos implantations qui accompagnent nos articles sur des supports pérennes comme `github`. Cela permet à toute personne de pouvoir reproduire les résultats expérimentaux obtenus. Le reste de nos résultats est de nature théorique. Ils sont systématiquement mis à disposition sur des plateformes comme `arXiv` et `hal`. Les collègues les plus jeunes, notamment les doctorants, bénéficient de relectures internes systématiques avant de soumettre leurs articles, bien évidemment, même si leur équipe de direction de thèse ne co-signe pas l'article en question.

Domaine 4. Inscription des activités de recherche dans la société

Référence 1. L'unité se distingue par la qualité et la quantité de ses interactions avec le monde non-académique.

La création de valeurs par le biais de la recherche académique et la souveraineté technologique sont deux enjeux économiques et technologiques sur lesquels PolSys se positionne. D'une part, l'équipe partage son expérience de l'innovation afin d'aider d'autres chercheurs dans la maturation de leurs projets d'entreprises. Cela se traduit par la participation à des tables rondes (au Campus Cyber avec le CNRS Innovation ou avec des SATT dans des laboratoires de recherche) ou par le mentorat dans un programme à destination des startups innovantes de Sorbonne Université (MyStartupProgram).

D'autre part, la question de la maitrise des technologies innovantes est particulièrement stratégique dans le contexte actuel. La cryptographie post-quantique est naturellement un sujet de souveraineté et l'équipe participe au débat public, notamment avec une tribune dans le journal Le Monde ("*L'Europe doit se préparer à la révolution post-quantique*") ou une interview diffusée sur France 24, ("*Informatique quantique : l'Europe à la traîne face à une cybermenace grandissante*"). L'objectif de ces interventions est de sensibiliser le grand public, ainsi que les décideurs, aux risque quantique sur la sécurité et aux enjeux de la normalisation post-quantique à l'échelle européenne.

L'équipe a développé des liens forts avec ATOS qui a financé une thèse CIFRE (2018 – 2021, Nagarjun Dwarakanath) et participe au board stratégique de CRYPTONEXT SECURITY. Plus récemment, l'équipe collabore étroitement avec le laboratoire de cryptologie de Thalès, notamment avec une thèse CIFRE qui a démarré en novembre 2022.

Référence 2. L'unité développe des produits à destination du monde culturel, économique et social.

L'activité de l'équipe a un fort impact sur le monde économique : principalement au travers de la création d'une startup (CRYPTONEXT SECURITY, dont les fondateurs sont des membres de l'équipe) et la participation à plusieurs comités de normalisation de la cryptographie post-quantique (ETSI, IEEE et NIST). Ces activités découlent d'une approche globale de l'équipe consistant à faire progresser les aspects théoriques et algorithmiques du calcul formel, produire des implémentations efficaces, et les confronter à des applications pratiques. Le cas de la cryptographie est celui pour lequel la logique de maîtrise d'une chaine complète – des aspects les plus théoriques aux plus pratiques – est poussée à son paroxysme. CRYPTONEXT SECURITY est ainsi le produit de plus de 15 ans de recherche sur la cryptanalyse algébrique des cryptosystèmes post-quantiques (par exemple [Bettale et al., 2013, Faugère et al., 2010]) ainsi que des progrès constants dans l'implémentation efficace de briques fondamentales du calcul formel (multiplication de polynômes univariés, évaluation de polynômes multivariés, ... [Faugère et al., 2019]). CRYPTONEXT repose sur cette expertise ainsi que des briques de logiciels transférées après un projet de maturation financé par la SATT Lutech (un brevet [Perret and Faugère, 2017] et un dépôt logiciel relié à MQSOFT [Faugère et al., 2019]).

L'activité de standardisation a démarré avec le processus post-quantique du NIST. Ce processus a pris la forme d'un appel international à contributions de cryptosystèmes (échange de clé et signature) et une sélection sur une période de 5 ans découpée en plusieurs étapes de sélection. L'équipe a proposé plusieurs algorithmes dont GeMSS (algorithme de signature, [Casanova et al., 2017]) qui a été sélectionné au troisième (et avant-dernier) tour du processus NIST. L'équipe a également participé à un processus essentiellement similaire en Chine et proposé un autre algorithme de signature post-quantique (PKP-DSS, [Beullens et al.,]) qui a remporté un troisième prix.

L'activité de standardisation s'est ensuite développée avec une participation au groupe de standardisation post-quantique de l'ETSI (*"Quantum-Safe Cryptography Specification Group"*, [Perret, 2021]) et la création en 2022 de deux nouveaux groupes à l'IEEE ("*P3172 Working Group – Recommended Practice for Post-Quantum Cryptography Migration*", "*P1943 Working Group Post-Quantum Network Security*") dédiés à la transition post-quantique et dont l'équipe est co-responsable.

Par ailleurs, l'enseignement est une activité importante dans laquelle les membres de l'équipe s'impliquent fortement. L'équipe assure la responsabilité du parcours de master SFPN – centré sur le calcul haute-performance et la cryptologie –, la co-responsabilité de la déclinaison "Sorbonne" du master européen EUMaster4hpc – formation bi-disciplinaire entre mathématiques et informatique dédiée au calcul haute-performance –, la coordination pour l'informatique de la mobilité internationale des étudiants, la responsabilité de 5 unités d'enseignements à SU. Elle assure des cours au MPRI et, depuis 2022, la responsabilité d'un cours dans ce master.

Référence 3. L'unité partage ses connaissances avec le grand public et intervient dans des débats de société.

L'équipe participe à la sensibilisation du grand public et des industriels sur l'impact du quantique en cybersécurité. Cette action est composée d'interventions ponctuelles dans les médias nationaux (Le Monde, Le Point, France 24) et d'une action plus structurée via un think-tank industriel (et international) de la Cloud Security Alliance (*"Quantum-Safe Security Working Group"*). L'équipe a assuré la responsabilité de ce groupe de travail qui a publié une dizaine d'articles (dont la moitié par l'équipe) de vulgarisation autour du risque quantique. Le groupe maintient également une newsletter, ainsi qu'une horloge qui décompte le temps (approximatif) avant l'apparition d'un ordinateur quantique assez puissant pour casser la cryptographie actuelle (cette date reste incertaine encore aujourd'hui et l'objectif est uniquement la sensibilisation).

4 RÉFÉRENCES BIBLIOGRAPHIQUES EXTERNES

[1] Mireille Bousquet-Mélou and Arnaud Jehanne. Polynomial equations with one catalytic variable, algebraic series and map enumeration. *Journal of Combinatorial Theory, Series B*, 96(5) :623–672, 2006.

[2] John Canny. *The complexity of robot motion planning*. MIT press, 1988.

[3] Michael R. Garey and David S. Johnson. *Computers and Intractability ; A Guide to the Theory of NP-Completeness*. W. H. Freeman & Co., USA, 1990.

[4] David Harvey and Joris van der Hoeven. Integer multiplication in time $O(n\log n)$. *Annals of Mathematics*, 193(2) :563–617, 2021.

[5] Vincent Neiger and Clément Pernet. Deterministic computation of the characteristic polynomial in the time of matrix multiplication. *Journal of Complexity*, 67 :101572, 2021.

[6] Joris van der Hoeven and Grégoire Lecerf. Fast computation of generic bivariate resultants. *Journal of Complexity*, 62 :101499, 2021.

[7] Gilles Villard. On computing the resultant of generic bivariate polynomials. In *Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation*, ISSAC '18, page 391–398, New York, NY, USA, 2018. Association for Computing Machinery.

[8] Gilles Villard. Elimination ideal and bivariate resultant over finite fields. Working paper or preprint, 2023.

5 RÉFÉRENCES BIBLIOGRAPHIQUES SIGNIFICATIVES DE PolSys

[Basu et al., 2014] Basu, S., Roy, M.-F., Safey El Din, M., and Schost, É. (2014). A Baby Step–Giant Step Roadmap Algorithm for General Algebraic Sets. *Foundations of Computational Mathematics*, 14(6) :1117 – 1172.

[Battarbee et al., 2022] Battarbee, C., Kahrobaei, D., Perret, L., and Shahandashti, S. F. (2022). A Subexponential Quantum Algorithm for the Semidirect Discrete Logarithm Problem. In *NIST Fourth PQC Standardization Conference*, On-line conference, United States.

[Bérard et al., 2021] Bérard, B., Haddad, S., Picaronny, C., Safey El Din, M., and Sassolas, M. (2021). Polynomial interrupt timed automata : Verification and expressiveness. *Information and Computation*, 277 :104580.

[Berthomieu et al., 2022a] Berthomieu, J., Bostan, A., Ferguson, A., and Safey El Din, M. (2022a). Gröbner bases and critical values : The asymptotic combinatorics of determinantal systems. *Journal of Algebra*, 602 :154–180.

[Berthomieu et al., 2021] Berthomieu, J., Eder, C., and Safey El Din, M. (2021). msolve : A Library for Solving Polynomial Systems. In *2021 International Symposium on Symbolic and Algebraic Computation*, pages 51–58, Saint Petersburg, Russia.

[Berthomieu et al., 2022b] Berthomieu, J., Neiger, V., and Safey El Din, M. (2022b). Faster change of order algorithm for Gröbner bases under shape and stability assumptions. In *2022 International Symposium on Symbolic and Algebraic Computation*, Lille, France.

[Bettale et al., 2013] Bettale, L., Faugère, J.-C., and Perret, L. (2013). Cryptanalysis of HFE, Multi-HFE and Variants for Odd and Even Characteristic. *Designs, Codes and Cryptography*, 69(1) :1 – 52.

[Beullens et al.,] Beullens, W., Faugère, J.-C., Han, X., Lin, D., Koussa, E., Macario-Rat, G., Patarin, J., and Perret, L. PKPDSS : A submission to the Chinese post-quantum competition. Technical report.

[Bostan et al., 2022] Bostan, A., Chyzak, F., Notarantonio, H., and Safey El Din, M. (2022). Algorithms for discrete differential equations of order 1. In *ISSAC 2022 - 47th International Symposium on Symbolic and Algebraic Computation*, pages 101–110, Lille, France. To appear in ISSAC'22.

[Bostan et al., 2023b] Bostan, A., Notarantonio, H., and Safey El Din, M. (2023b). Fast Algorithms for Discrete Differential Equations. Working paper or preprint.

[Capco et al., 2020] Capco, J., Safey El Din, M., and Schicho, J. (2020). Robots, computer algebra and eight connected components. In *ISSAC '20 : International Symposium on Symbolic and Algebraic Computation*, ISSAC'20 : Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation, pages 62–69, Kalamata / Virtual, Greece. ACM.

[Capco et al., 2023] Capco, J., Schicho, J., and Mohab, S. E. D. (2023). Positive dimensional parametric polynomial systems, connectivity queries and applications in robotics. *Journal of Symbolic Computation*.

[Casanova et al., 2017] Casanova, A., Faugère, J.-C., Macario-Rat, G., Patarin, J., Perret, L., and Ryckeghem, J. (2017). GeMSS : A Great Multivariate Short Signature. Research report, UPMC - Paris 6 Sorbonne Universités ; INRIA Paris Research Centre, MAMBA Team, F-75012, Paris, France ; LIP6 - Laboratoire d'Informatique de Paris 6.

[Chablat et al., 2022] Chablat, D., Prébet, R., Safey El Din, M., Salunkhe, D., and Wenger, P. (2022). Deciding Cuspidality of Manipulators through Computer Algebra and Algorithms in Real Algebraic Geometry. In *2022 International Symposium on Symbolic and Algebraic Computation*, Lille, France.

[Faugère et al., 2017] Faugère, J., Horan, K., Kahrobaei, D., Kaplan, M., Kashefi, E., and Perret, L. (2017). Fast quantum algorithm for solving multivariate quadratic equations. *IACR Cryptol. ePrint Arch.*, page 1236.

[Faugère et al., 2010] Faugère, J.-C., Otmani, A., Perret, L., and Tillich, J.-P. (2010). Algebraic Cryptanalysis of McEliece Variants with Compact Keys. In Gilbert, H., editor, *Eurocrypt 2010 - 29th International Conference on Cryptology*, volume 6110 of *Lecture Notes in Computer Science*, pages 279–298, Monaco, Monaco. Springer Verlag.

[Faugère et al., 2019] Faugère, J.-C., Perret, L., and Ryckeghem, J. (2019). Software Toolkit for HFE-based Multivariate Schemes. In *CHES 2019 : International Conference on Cryptographic Hardware and Embedded Systems*, volume 2019 of *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 257–304, Atlanta, United States.

[Fawzi and Safey El Din, 2018] Fawzi, H. and Safey El Din, M. (2018). A lower bound on the positive semidefinite rank of convex bodies. *SIAM Journal on Applied Algebra and Geometry*, 2(1) :126–139.

[García Fontán, 2023] García Fontán, J. (2023). *Singularity and stability analysis of vision-based controllers*. Theses, Sorbonne Université.

[García Fontán et al., 2022] García Fontán, J., Nayak, A., Briot, S., and Safey El Din, M. (2022). Singularity Analysis for the Perspective-Four and Five-Line Problems. *International Journal of Computer Vision*, 130 :909–932.

[Hauenstein et al., 2021] Hauenstein, J. D., Safey El Din, M., Schost, É., and Vu, T. X. (2021). Solving determinantal systems using homotopy techniques. *Journal of Symbolic Computation*, 104 :754–804.

[Kushilevitz et al., 2021] Kushilevitz, E., Ostrovsky, R., Prouff, E., Rosén, A., Thillard, A., and Vergnaud, D. (2021). Lower and Upper Bounds on the Randomness Complexity of Private Computations of AND. *SIAM Journal on Discrete Mathematics*, 35(1) :465–484.

[Lairez et al., 2019] Lairez, P., Mezzarobba, M., and Safey El Din, M. (2019). Computing the volume of compact semi-algebraic sets. In *ISSAC 2019 - International Symposium on Symbolic and Algebraic Computation*, Beijing, China. ACM.

[Le et al., 2022] Le, H. P., Manevich, D., and Plaumann, D. (2022). Computing totally real hyperplane sections and linear series on algebraic curves. *Le Matematiche*, 77(1) :119–141.

[Le and Safey El Din, 2021] Le, H. P. and Safey El Din, M. (2021). Faster One Block Quantifier Elimination for Regular Polynomial Systems of Equations. In *International Symposium on Symbolic and Algebraic Computation 2021 (ISSAC '21)*, Proceedings of the 2021 on International Symposium on Symbolic and Algebraic Computation, pages 265–272, Saint Petersburg, Russia.

[Le and Safey El Din, 2022] Le, H. P. and Safey El Din, M. (2022). Solving parametric systems of polynomial equations over the reals through Hermite matrices. *Journal of Symbolic Computation*, 112 :25–61.

[Magron et al., 2022] Magron, V., Safey El Din, M., and Vu, T.-H. (2022). Sum of Squares Decompositions of Polynomials over their Gradient Ideals with Rational Coefficients. *SIAM Journal on Optimization*. 24 pages, 2 tables.

[Neiger et al., 2021] Neiger, V., Salvy, B., Schost, É., and Villard, G. (2021). Faster Modular Composition. Working paper or preprint.

[Perret, 2021] Perret, L. (2021). Quantum-safe signatures. Research report – tr 103 616, ETSI.

[Perret and Faugère, 2017] Perret, L. and Faugère, J.-C. (2017). Mise en Oeuvre Optimisée du HFE.

[Riener and Safey El Din, 2018] Riener, C. and Safey El Din, M. (2018). Real root finding for equivariant semi-algebraic systems. In *ISSAC 20018 - 43rd International Symposium on Symbolic and Algebraic Computation*, New-York, United States.

[Safey El Din and Schost, 2011] Safey El Din, M. and Schost, É. (2011). A baby steps/giant steps Monte Carlo algorithm for computing roadmaps in smooth compact real hypersurfaces. *Discrete and Computational Geometry*, 45(1) :181–220.

[Safey El Din and Schost, 2017] Safey El Din, M. and Schost, É. (2017). A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *Journal of the ACM (JACM)*, 63(6) :48 :1–48 :37.

[Safey El Din and Schost, 2018] Safey El Din, M. and Schost, É. (2018). Bit complexity for multi-homogeneous polynomial system solving Application to polynomial minimization. *Journal of Symbolic Computation*, 87 :176–206.

[Trutman et al., 2022] Trutman, P., Safey El Din, M., Henrion, D., and Pajdla, T. (2022). Globally Optimal Solution to Inverse Kinematics of 7DOF Serial Manipulator. *IEEE Robotics and Automation Letters*, 7(3) :6012 – 6019.

A ANNEXE — MEMBRES PERMANENTS AU 31/12/2022

La table ci dessous liste les membres permanents de l'équipe PolSys.

NOM	Prénom	Corps	Employeur
BERTHOMIEU	Jérémy	MCF	Sorbonne Université
NEIGER	Vincent	MCF	Sorbonne Université
PERRET	Ludovic	MCF (HDR)	Sorbonne Université
SAFEY EL DIN	Mohab	PR	Sorbonne Université

ÉLÉMENT DE PORTFOLIO 01

Création d'entreprise

1 DÉFINITION DE CET ÉLÉMENT

Titre de l'élément : CryptoNext Security

URL de l'élément : `https://www.cryptonext-security.com/`

2 MOTIVATIONS DU CHOIX DE CET ÉLÉMENT

La création de CRYPTONEXT SECURITY atteste du leadership de PolSys sur la cryptographie post-quantique ainsi que sa capacité à valoriser les outils du calcul formel dans le monde économique. Elle montre aussi comment l'équipe a su se saisir des dispositifs de transfert technologique pour mettre en œuvre un cycle complet d'innovation technologique (de la recherche fondamentale jusqu'à l'entrepreneuriat).

3 PRÉSENTATION DE CET ÉLÉMENT

CRYPTONEXT SECURITY est une startup issue de PolSys et créée le 13 juin 2019. Les deux fondateurs sont liés à l'équipe : Jean-Charles Faugère (CTO, temps complet dans la société) en a été le responsable, et Ludovic Perret (CEO, en délégation à temps complet de 2019 à 2022) membre. La cryptographie post-quantique est une composante majeure des recherches de PolSys et la startup repose sur cette expertise (un brevet [2] et un dépôt logiciel relié à MQSOFT [1]).

En 2015, dans le cadre d'une visite organisée par le LIP6, le Ministère des Armées a demandé à PolSys de concevoir une application de messagerie instantanée post-quantique fonctionnant sur des téléphones portables du commerce. Le Ministère des Armées a testé l'application et mené une expérience en conditions réelles en installant l'application sur une centaine de téléphones utilisés sur le terrain par des militaires. Le succès de cette expérience a incité les fondateurs à entamer cette même année un projet de maturation porté par la SATT Lutech, dont CRYPTONEXT SECURITY est l'aboutissement. En 2016, l'institut de normalisation américain NIST a annoncé le lancement d'un processus de sélection de nouveaux standards de cryptographie post-quantique en vue d'une migration des administrations américaines à partir de 2024.

Constatant l'intérêt croissant suscité par la cryptographie post-quantique, les fondateurs de CRYPTONEXT SECURITY ont alors créé la société et ont finalisé une première levée de fonds avec Quantonation (fonds professionnel) en décembre 2019 ainsi qu'avec ses tutelles via la SATT Lutech. En 2021, l'équipe des deux fondateurs a été rejointe par Florent Grosmaitre comme nouveau CEO afin d'accompagner la croissance rapide CRYPTONEXT SECURITY et entraînant le retour de L. Perret dans PolSys en juin 2022.

CRYPTONEXT SECURITY est aujourd'hui présente au campus Cyber à la Défense. L'entreprise était, auparavant accélérée par la BNPP via le programme Plug & Play de Station F, par Wilco (promotion 2019), incubée par Agoranov (avril 2019) et sélectionnée dans le programme Cyber@StationF de Thales à (Cyber@StationF, juin 2019). Pendant le programme Cyber@StationF, CRYPTONEXT SECURITY a été sélectionnée parmi 1000 start-ups comme faisant partie des 40 plus prometteuses. En 2020, CRYPTONEXT SECURITY a été lauréate du prestigieux Concours d'innovation i-Lab et l'un des 10 Grands Prix récompensant des projets exceptionnels qui ont vocation à relever un défi sociétal majeur.

J.-C Faugère et L. Perret ont reçu le premier prix Atos-Fourier (2018) dans le domaine des technologies quantiques pour la création de CryptoNext Security et leurs contributions académiques au post-quantique et nommés, en 2022, par le Magazine Le Point dans les 100 inventeurs de demain.

3.1 Nature de l'activité

L'ordinateur quantique remettant en cause la sécurité des techniques cryptographiques actuelles, CryptoNext Security a pour mission de simplifier la transition des organisations publiques et privées vers de nouvelles normes cryptographiques post-quantiques. Le cœur technologique et le savoir-faire de CryptoNext Security sont une bibliothèque logicielle de cryptographie, qui implémente les deux fonctions fondamentales de la cryptographie à clé publique, l'échange de clés et la signature numérique, en utilisant une cryptographie post-quantique.

La bibliothèque logicielle est destinée à être intégrée dans tous les cas d'usage qui utilisent de la cryptographie à clé publique, en particulier HSM (Hardware Security Module), VPN (Virtual Private network), les solutions de signatures numériques, les solutions métiers (logiciel métier santé, embarqué automobile, ...), les solutions de bureautique (messagerie instantanée, visio-conférence, email, ...).

Le logiciel a déjà été testé par plusieurs clients : le gouvernement français avec la transmission du premier message diplomatique utilisant de la cryptographie post-quantique et des clients du monde de la défense ou de la finance (comme la Banque de France).

CRYPTONEXT SECURITY a collaboré avec l'équipe QI du LIP6 sur deux projets (Européen et régional) qui visent à intégrer la cryptographie post-quantique et la distribution de clé quantique (QKD) dans le cadre de la conception d'un futur réseau Européen de communication quantique.

4 RÉFÉRENCES BIBLIOGRAPHIQUES

[1] Jean-Charles Faugère, Ludovic Perret, and Jocelyn Ryckeghem. Software Toolkit for HFE-based Multivariate Schemes. In *CHES 2019 : International Conference on Cryptographic Hardware and Embedded Systems*, volume 2019 of *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 257–304, Atlanta, United States, August 2019.

[2] Ludovic Perret and Jean-Charles Faugère. Mise en Oeuvre Optimisée du HFE, January 2017.

ÉLÉMENT DE PORTFOLIO 02

Logiciel ou bibliothèque logicielle

1 DÉFINITION DE CET ÉLÉMENT

Titre de l'élément : `msolve`

URL de l'élément : `https://msolve.lip6.fr`

2 MOTIVATIONS DU CHOIX DE CET ÉLÉMENT

Le développement de la bibliothèque *open source*, sous licence GPLv2+, `msolve` pour la résolution de systèmes polynomiaux et le calcul de bases de Gröbner a été initié lors de la période d'évaluation en collaboration avec C. Eder (TU Kaiserslautern). Elle est capable de résoudre des systèmes hors d'atteinte par les logiciels de calcul formel de l'état de l'art. Son usage a été crucial dans la résoluion récente d'applications en robotique. Ce logiciel démontre l'impact et la visibilité des développements algorithmiques et logiciels de l'équipe pour la résolution des systèmes polynomiaux (en calcul formel et dans d'autres champs disciplinaires).

3 PRÉSENTATION DE CET ÉLÉMENT

La bibliothèque open source `msolve`, écrite en `C` et sous licence GPLv2+, est développée par l'équipe PolSys en collaboration avec C. Eder (TU Kaiserslautern) pour la résolution de systèmes polynomiaux. Elle a fait l'objet de la publication d'un article dans les actes de la conférence ISSAC 2021 (International Symposium on Symbolic and Algebraic Computation) [1].

Son développement a été pensé et initié en $2015-2016$ lorsque l'équipe s'est engagée vers des développements logiciels communs et open source pour le calcul de bases de Gröbner et la résolution de systèmes polynomiaux afin de garantir la pérennité de ces développements et renforcer son impact scientifique. Cet objectif était clairement identifié et énoncé dans le projet scientifique de l'équipe lors de la dernière évaluation.

L'équipe a entamé le développement de `msolve` dès l'année 2017 et la première version disponible date de 2021.

Actuellement, `msolve` permet le calcul de bases de Gröbner à coefficients dans des corps premiers de cardinalités inférieures à 2^{31} pour des ordres monomiaux admissibles, gradués ou d'élimination, incluant des algorithmes de changement d'ordres monomiaux dans le cas zéro-dimensionnel (nombre fini de solutions dans une clôture algébrique du corps de base) et, via une stratégie de calcul multi-modulaire exploitant les propriétés des algorithmes de calcul de bases de Gröbner, le calcul des paramétrisations des solutions de systèmes polynomiaux ayant un nombre fini de solutions complexes ainsi que l'isolation de leurs racines réelles. Son code source est librement accessible sur GitHub.

La mise à disposition de `msolve` enm 2021 a été assez retentissante. Une large composante de la communauté (en calcul formel, robotique et cryptographie) se l'est appropriée et, malgré sa jeunesse, elle est déjà intégrée à des systèmes de calcul formel généralistes comme SageMath (voir ici et là) et Oscar (voir ici) ce qui lui assure une diffusion large. En 2022, google a fait une donation de 150k$ pour le développement de `msolve` et ses applications.

3.1 Algorithmes implémentés

`msolve` fournit une implémentation efficace, fondée sur des structures de données et des routines d'algèbre linéaire dédiées, de l'algorithme F_4 [4] pour le calcul de base de Gröbner. Lorsque le nombre de solutions dans la clôture algébrique est fini, `msolve` fournit une implémentation efficace d'une variante de l'algorithme de changement d'ordre SPARSE-FGLM [5,6] pour retourner une paramétrisation des solutions. Cette paramétrisation permet d'isoler les solutions réelles du système donné en entrée.

En plus de de structures de données dédiées et l'usage de vectorisation, l'efficacité de `msolve` est en partie due à son *tracer* pour le calcul de bases de Gröbner en caractéristique 0. L'idée, introduite dans [8], est d'effectuer

un premier calcul modulo un premier p_1 et d'apprendre les sous-calculs qui sont nécessaires au calcul de la base de Gröbner finale et ceux qui lui sont inutiles. Ensuite, modulo d'autres premiers $p_2, p_3, \ldots$, seules les étapes nécessaires sont effectuées, rendant le calcul global bien plus rapide. Elle est aussi due au fait que la chaîne complète de calculs (base de Gröbner pour un ordre du degré puis calcul de paramétrisations) est effectuée modulo chacun des premiers avant de remonter les paramétrisations sur les rationnels via le théorème des restes chinois. En effet, les autres logiciels et bibliothèques de calcul formel font le choix de remonter sur les rationnels la base de Gröbner pour l'ordre du degré avant de calculer les paramétrisations modulo plusieurs premiers. Cette remontée intermédiaire a un coût non négligeable qu'`msolve` s'affranchit de calculer.

Plus récemment, nous avons commencé à doter `msolve` d'implantations moins mûres d'algorithmes plus récents comme F$_4$SATet SPARSE-FGLM-COLON qui sont des variantes respectives de F$_4$et de SPARSE-FGLM dédiées au calcul de bases de Gröbner pour des idéaux saturés [2] (géométriquement cela correspond à calculer des différences ensemblistes d'ensembles de solutions). Une implémentation du nouvel algorithme de changement d'ordre est en cours [3].

3.2 Efficacité

`msolve` s'appuie sur des instructions vectorielles pour accélérer les opérations d'algèbre linéaire. Elle s'appuie aussi sur la bibliothèque `C` et open source FLINT [7]. Dans la Table 1, on compare pour différents systèmes le temps pris par `msolve` pour calculer les paramétrisations avec le tracer ou non (independent) modulo plusieurs nombres premiers avec le temps pris par MAPLE et MAGMA.

En 2021, `msolve` (version v0.1.0) pouvait résoudre un système polynomial avec des milliers de solutions complexes, comme Katsura-14, qui en a $8\,192$ (la paramétrisation des solutions a des coefficients de taille binaire $\simeq 147\,623$), sequentiellement en 15 jours sur un Intel® Xeon® CPU E7-4820 v4 2.00 GHz, tandis que MAPLE et MAGMA ne pouvaient y arriver en l'espace de 6 mois, voir Table 1. Les améliorations apportées récemment ont permis d'accélérer ce calcul à 11 jours sur la même machine avec la version v0.2.9. Cette version de `msolve` a récemment permis de résoudre un système (à coefficients dans un corps premier) ayant jusque $120\,000$ solutions dans la clôture algébrique. C'est la première fois que de telles tailles sont atteintes par des méthodes algébriques.

Pour bien mesurer l'impact scientifique de `msolve` il est aussi pertinent de la confronter à des applications qui constituent de véritables défis, non seulement pour le calcul formel mais aussi pour les méthodes numériques. Dans la Table 2, on compare le calcul de points critiques (qui réalisent des extrema locaux) d'une fonction mesurant l'erreur de servo-commandes visuelles (basées sur l'observation de 4 points). On constate que `msolve` est la seule bibliothèque de calcul formel capable de résoudre ce problème mais aussi, et surtout, que les méthodes numériques échouent à calculer tous les points critiques. Pour `msolve`, nous donnons les temps obtenus pour la modélisation originelle du problème, puis pour des modélisations tirant profit de la symétrie et de l'éventuelle co-planarité des points observés ce qui montre également que le logiciel ne suffit pas et que l'expertise dans le domaine est importante.

Examples	System data		`msolve` overall (v0.1.0)			Others overall	
	degree	radical	# primes	trace	independent	MAPLE	MAGMA
Katsura-9	256	yes	83	4.89	7.49	104	2,522
Katsura-10	512	yes	188	43.7	70.5	1,278	82,540
Katsura-11	1,024	yes	388	424	814	7,812	–
Katsura-12	2,048	yes	835	6,262	11,215	120,804	–
Katsura-13	4,096	yes	1,772	89,390	148,372	–	–
Katsura-14	8,192	yes	3,847	1,308,602	2,007,170	–	–
Eco-10	256	yes	161	12.5	21.2	26.3	6,520
Eco-11	512	yes	327	90.3	161	312	214,770
Eco-12	1,024	yes	530	877	1,619	4,287	–
Eco-13	2,048	yes	1,225	12,137	19,553	66,115	–
Eco-14	4,096	yes	2,670	167,798	254,389	–	–
Henrion-5	100	yes	83	0.71	0.83	2.7	93
Henrion-6	720	yes	612	138	157	1,470	–
Henrion-7	5,040	yes	4,243	117,803	127,456	–	–
Phuoc-1	1,102	no	753	4,467	5,056	–	–
CP$(3,5,2)$	288	yes	326	18.1	19.2	249	–
CP$(3,6,2)$	720	yes	1,042	390	450	23,440	–
CP$(3,7,2)$	1,728	yes	3,037	9,643	11,511	–	–
CP$(3,8,2)$	4,032	yes	8,211	269,766	323,838	–	–
CP$(4,4,3)$	576	yes	339	40.9	41.8	916	–
CP$(4,5,3)$	3,456	yes	2,747	21,528	23,559	–	–
CP$(3,6,6)$	729	yes	779	255	294	–	–
CP$(4,6,6)$	4,096	yes	3,476	71,472	77,941	–	–
CP$(3,7,7)$	2,187	yes	2,795	12,412	14,375	–	–

TABLE 1 – Temps donnés en secondes. $-$ signifie > 6 mois ou mémoire insuffisante

Systems	msolve (on $\times 12$ cores)						Julia (Homotopy Continuation)		
Description	$\#\text{sols}_{\mathbf{C}}$	$\#\text{sols}_{\mathbf{R}}$	Time				$\#\text{sols}_{\mathbf{C}}$	$\#\text{sols}_{\mathbf{R}}$	Time
			Orig.	Sym.	Coplan.	Both			
Ex.1 square - parallel	402	50	15 d	48.6 h	478 s	172 s	403	50	1 630 s
Ex.2 square - side	1016	44	24 d	44.1 h	29.4 h	9 308 s	1016	44	1 495 s
Ex.4 rectangle - side	1064	48	27 d	31.5 h	18.1 h	9 275 s	871	32	1 950 s
Ex.7 generic - parallel	3656	84	41 d	26 h	N/A	N/A	3537	95	2 280 s

TABLE 2 – Calcul de points critiques en robotique

4 RÉFÉRENCES BIBLIOGRAPHIQUES

[1] J. Berthomieu, Ch. Eder, and M. Safey El Din. msolve : A Library for Solving Polynomial Systems. In *2021 International Symposium on Symbolic and Algebraic Computation*, pages 51–58, Saint Petersburg, Russia, July 2021.

[2] J. Berthomieu, Ch. Eder, and M. Safey El Din. New efficient algorithms for computing Gröbner bases of saturation ideals (F4SAT) and colon ideals (Sparse-FGLM-colon). preprint, 2022.

[3] Jérémy Berthomieu, Vincent Neiger, and Mohab Safey El Din. Faster change of order algorithm for Gröbner bases under shape and stability assumptions. In *2022 International Symposium on Symbolic and Algebraic Computation*, Lille, France, July 2022.

[4] J.-Ch. Faugère. A New Efficient Algorithm for Computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1) :61–88, 1999.

[5] J.-Ch. Faugère and Ch. Mou. Fast algorithm for change of ordering of zero-dimensional gröbner bases with sparse multiplication matrices. In *Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation*, ISSAC '11, pages 115–122, New York, NY, USA, 2011. ACM.

[6] J.-Ch. Faugère and Ch. Mou. Sparse FGLM algorithms. *Journal of Symbolic Computation*, 80(3) :538–569, 2017.

[7] W. B. Hart. Fast library for number theory : An introduction. In *Proc. of the 3rd Int. Cong. on Math. Soft.*, ICMS'10, pages 88–91. Springer-Verlag, 2010. `http://flintlib.org`.

[8] Carlo Traverso. Gröbner trace algorithms. In *Symbolic and algebraic computation (Rome, 1988)*, volume 358 of *Lecture Notes in Comput. Sci.*, pages 125–138. Springer, Berlin, 1989.

ÉLÉMENT DE PORTFOLIO 03

Publication

1 DÉFINITION DE CET ÉLÉMENT

Titre de l'élément : A Nearly Optimal Algorithm for Deciding Connectivity Queries in Smooth and Bounded Real Algebraic Sets

URL de l'élément : `https://dl.acm.org/doi/10.1145/2996450`

2 MOTIVATIONS DU CHOIX DE CET ÉLÉMENT

Dans cette publication [15], nous décrivons un nouvel algorithme qui compte le nombre de composantes connexes (et résout des requêtes de connectivité) de variétés algébriques réelles lisses et compactes [1]. Il s'agit d'un problème calculatoire difficile qui trouve de fortes motivations applicatives, notamment en robotique pour la planification de trajectoires et l'analyse de singularités cinématiques [11].

En 1988, J. Canny [5] introduit la notion de carte routière pour résoudre ces problèmes. Il s'agit d'une courbe algébrique dont la trace réelle est contenue dans la variété étudiée et dont l'intersection avec chaque composante connexe de cette variété est connexe. Ainsi, les requêtes de connectivité en dimension arbitraire sont réduites à des requêtes de connectivité en dimension un. L'algorithme de Canny avait pour complexité $(n\delta)^{O(n^2)}$ où n est la dimension de l'espace ambiant et δ est le maximum des degrés des polynômes donnés en entrée.

Or, un résultat classique de géométrie dû à Petrovski, Oleinik [13], Milnor [12] et Thom [16] établit que le nombre de composantes connexes d'une variété algébrique réelle vit dans $\delta^{O(n)}$.

Malgré plusieurs tentatives d'amélioration, aucun algorithme n'avait été proposé pour le calcul de carte routière avec une complexité dont l'exposant est meilleur que $O(n^2)$ jusqu'à celui proposé dans [14] qui améliore l'exposant en $O\left(n^{1.5}\right)$ en introduisant un nouveau procédé géométrique de résolution. Dès lors, plusieurs algorithmes [3, 4] ont été proposés mais les seuls à avoir une complexité en exposant $\log$-linéaire en n sont tels que cette complexité n'est pas polynomiale en la taille de leur sortie.

Dans la publication qui fait l'objet de ce portfolio, nous obtenons un algorithme de complexité $(n\delta)^{O(n\log(n))}$ pour une taille de sortie en $(n\delta)^{O(n\log(n))}$. Ce résultat est publié au *Journal of the ACM*, la revue porte-drapeau de l'ACM. Il est à noter que la preuve complète de ce résultat de complexité fait plus de 100 pages.

Ce résultat illustre aussi comment nos méthodologies, combinant algèbre, géométrie, théorie de la complexité et exploitation des structures des systèmes polynomiaux sont mises en œuvre.

3 PRÉSENTATION DE CET ÉLÉMENT

3.1 Approche générale

L'approche mise en œuvre dans le calcul de cartes routières repose sur des ingrédients qui proviennent de la théorie de Morse en géométrie différentielle et qui sont utilisés ici, dans un contexte algébrique.

Comme illustré par la Figure 1, une carte routière est construite en :

(a) considérant l'ensemble des points critiques d'une projection sur un sous-espace de coordonnées bien choisi (ici la courbe rouge sur la figure) ; ce lieu a une intersection non vide mais non nécessairement connexe avec chaque composante connexe de la variété étudiée ;

(b) ajoutant à cet ensemble de points critiques des sections (en jaune sur la figure) de la variété étudiée pour réparer les défauts de connectivité.

Les résultats de [14] ont permis une plus grande flexibilité dans les choix de l'ensemble des points critiques (et donc de la projection associée). Notamment, alors que le schéma géométrique de résolution utilisé jusqu'alors imposait de choisir une projection sur un plan et donc, une courbe comme ensemble de points critiques, ce qui,

1. Une variété algébrique réelle est l'ensemble des solutions réelles de systèmes d'équations polynomiales à coefficients réels.

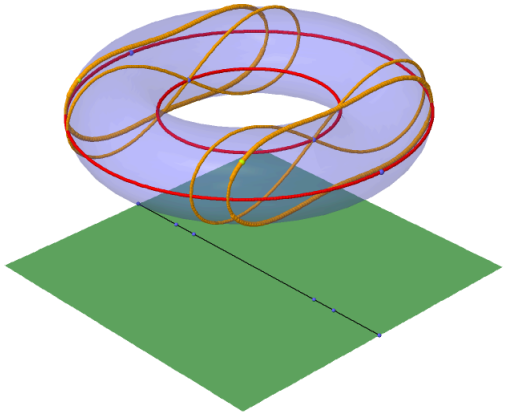

FIGURE 1 – Construction d'une carte routière sur un tore

pour des raisons intrinsèques conduisait à une complexité exponentielle en $O(n^2)$, il est devenu possible de choisir des lieux critiques de plus grande dimension.

3.2 Des systèmes structurés pour une meilleure complexité

Le choix fait dans cette publication, naturel au demeurant, a été d'équilibrer les dimensions des lieux critiques et sections considérés pour mettre en place une stratégie du type "diviser pour régner" : lieux critiques et sections sont alors de dimension approximativement $d/2$ où d est la dimension de la variété étudiée et l'algorithme est ensuite appelé récursivement sur chacun de ces lieux géométriques. Cette stratégie est aussi facile à décrire qu'elle est difficile à mettre en place et à prouver rigoureusement.

En effet, ne serait-ce qu'un encodage naïf des lieux critiques, considérés récursivement, conduirait à des complexités doublement exponentielles en n. Aussi, ces appels récursifs nécessitent de garantir un certain nombre de propriétés géométriques non triviales (lissité, équidimensionnalité notamment) aux objets considérés.

Pour contourner cette difficulté, nous combinons notre expertise géométrique du problème à celle qui concerne les systèmes polynomiaux structurés, notamment les polynômes multi-homogènes en montrant comment ces lieux critiques récursifs peuvent être encodés par des systèmes que nous avons appelé systèmes de Lagrange généralisés. Ceux-ci font intervenir un nombre de variables significativement supérieur à celui de la dimension de l'espace ambient, mais, la structure naturellement multi-homogène de ces systèmes fait que les degrés de leurs ensembles de solutions sont bien maîtrisés.

La virtuosité de la preuve complète du théorème de complexité consiste alors à montrer que les propriétés requises pour les appels récursifs sont satisfaits et surtout la conception d'algorithmes dédiés permettant de résoudre ces systèmes de Lagrange généralisés dans des complexités qui sont quadratiques en le degré de leurs ensembles de solutions.

Au final, nous obtenons un algorithme de calcul de cartes routière dont la complexité arithmétique est en

$$O^{\sim}\left(16^{9d}E(n\log_2(n))^{6(2d+12\log_2(d))(\log_2(d)+7)}\delta^{3(2n+1)(\log_2(d)+5)}\right)$$

où d est la dimension de la variété étudiée et E la complexité d'évaluation du système étudié. Cette complexité est en fait cubique en le degré de la carte routière et donc sous-quadratique en la taille de sa sortie.

3.3 Impact scientifique

L'impact de ce résultat et les perspectives qu'il ouvre pour les applications en robotique sont multiples et avérées par les publications [6–8].

De manière plus marquante, mentionnons également que la publication de cet article a engendré un intérêt du côté du calcul numérique pour ces méthodes (voir [9] et [10]).

Enfin, les méthodes de résolution de systèmes polynomiaux structurés développées dans cet article ont un impact qui va bien au-delà du cadre applicatif lié à la robotique puisque ces résultats ont déjà été utilisés par une partie de la communauté de cryptologie [1, 2].

4 RÉFÉRENCES BIBLIOGRAPHIQUES

[1] Simon Abelard. Counting points on hyperelliptic curves with explicit real multiplication in arbitrary genus. *Journal of Complexity*, 57 :101440, 2020.

[2] Simon Abelard, Pierrick Gaudry, and Pierre-Jean Spaenlehauer. Improved complexity bounds for counting points on hyperelliptic curves. *Foundations of Computational Mathematics*, 19 :591–621, 2019.

[3] Saugata Basu and Marie-Françoise Roy. Divide and conquer roadmap for algebraic sets. *Discrete & Computational Geometry*, 52 :278–343, 2014.

[4] Saugata Basu, Marie-Françoise Roy, Mohab Safey El Din, and Éric Schost. A baby step–giant step roadmap algorithm for general algebraic sets. *Foundations of Computational Mathematics*, 14 :1117–1172, 2014.

[5] John Canny. *The complexity of robot motion planning*. MIT press, 1988.

[6] Jose Capco, Mohab Safey El Din, and Josef Schicho. Robots, computer algebra and eight connected components. In *ISSAC '20 : International Symposium on Symbolic and Algebraic Computation*, ISSAC'20 : Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation, pages 62–69, Kalamata / Virtual, Greece, 2020. ACM.

[7] Jose Capco, Mohab Safey El Din, and Josef Schicho. Positive dimensional parametric polynomial systems, connectivity queries and applications in robotics. *Journal of Symbolic Computation*, 2023.

[8] Damien Chablat, Rémi Prébet, Mohab Safey El Din, Durgesh Salunkhe, and Philippe Wenger. Deciding Cuspidality of Manipulators through Computer Algebra and Algorithms in Real Algebraic Geometry. In *2022 International Symposium on Symbolic and Algebraic Computation*, Lille, France, 2022.

[9] Changbo Chen, Wenyuan Wu, and Yong Feng. Numerical roadmap of smooth bounded real algebraic surface. *Computer Aided Geometric Design*, 79 :101858, 2020.

[10] Reza Iraji and Hamidreza Chitsaz. Nuroa : A numerical roadmap algorithm. In *53rd IEEE Conference on Decision and Control*, pages 5359–5366. IEEE, 2014.

[11] Lydia E Kavraki and Steven M LaValle. Motion planning. In *Springer handbook of robotics*, pages 139–162. Springer, 2016.

[12] John Milnor. On the Betti numbers of real varieties. *Proceedings of the American Mathematical Society*, 15(2) :275–280, 1964.

[13] I. G. Petrovskiĭ and O. A. Oleĭnik. On the topology of real algebraic surfaces. *Doklady Akad. Nauk SSSR (N.S.)*, 67 :31–32, 1949.

[14] Mohab Safey El Din and Éric Schost. A baby steps/giant steps probabilistic algorithm for computing roadmaps in smooth bounded real hypersurface. *Discrete & Computational Geometry*, 45(1) :181–220, 2011.

[15] Mohab Safey El Din and Éric Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *Journal of the ACM (JACM)*, 63(6) :48 :1–48 :37, 2017. Major revision, accepted for publication to Journal of the ACM.

[16] René Thom. Sur l'homologie des variétés algébriques réelles. *Differential and combinatorial topology*, pages 255–265, 1965.

ÉLÉMENT DE PORTFOLIO 04

Publication

1 DÉFINITION DE CET ÉLÉMENT

Titre de l'élément : Faster Change of Order Algorithm for Gröbner Bases under Shape and Stability Assumptions

URL de l'élément : `https://dl.acm.org/doi/10.1145/3476446.3535484`

2 MOTIVATIONS DU CHOIX DE CET ÉLÉMENT

Cet article [2], publié à la conférence ISSAC 2022 (International Symposium on Symbolic and Algebraic Computation), qui est la conférence de référence pour le calcul formel, propose un changement de paradigme pour le changement d'ordre monomial pour les bases de Gröbner, sous certaines hypothèses de *généricité*. La stratégie est d'utiliser la structure de module sur l'anneau des polynômes en une variable au lieu de la simple structure d'espace vectoriel sur le corps des coefficients. L'entrée est une matrice de taille $D \times D$ et de densité $t/D \leq 1$. Nous obtenons une complexité de l'ordre de $t^{\omega-1}D$, où ω est un exposant pour le produit de matrices. Ceci améliore la complexité de l'état de l'art d'un facteur qui est le minimum entre $(\frac{D}{t})^{\omega-1}$ et $\frac{D}{t}t^{3-\omega}$, tous deux ≥ 1 et exponentiels en le nombre de variables dans les situations génériques. Les gains de performance observés via une implémentation prototype sont significatifs sur des cas classiques.

3 PRÉSENTATION DE CET ÉLÉMENT

La résolution de systèmes polynomiaux zéro-dimensionnels (avec un nombre fini de solutions dans une clôture algébrique du corps engendré par les coefficients), par calcul de bases de Gröbner se décompose classiquement en deux étapes. Un premier calcul de base de Gröbner, pour un ordre du dégré, est tout d'abord effectué en utilisant l'algorithme de Buchberger [3] ou les algorithmes F_4 et F_5 de Faugère [4,5]. Ensuite, un algorithme de conversion, dit de changement d'ordre, est appliqué à la base de Gröbner donnée en entrée pour obtenir une base de Gröbner pour l'ordre lexicographique. Pour des systèmes génériques, cette seconde étape devient prépondérante sur la première lorsque la taille des problèmes grossit.

Or, à l'instar de l'élimination de Gauß pour les systèmes linéaires, les bases de Gröbner pour l'ordre lexicographique permettent aisément de calculer les coordonnées des solutions. Une telle base contient un polynôme non nul purement en la dernière variable, ce qui permet de calculer la dernière coordonnée de chaque solution. Puis, elle contient des polynômes en les deux dernières variables, ce qui permet de déterminer l'avant-dernière coordonnée en fonction de la dernière, et ainsi de suite. On peut citer pour cette étape, les algorithmes FGLM [6], de Neiger et Schost [12] ou SPARSE-FGLM de Faugère et Mou [7,8]. Dans le cas *générique*, l'entrée est une matrice de taille D et de densité t/D. Dans ce cas, d'une part, l'algorithme de [12] a une complexité quasi-linéaire en D^ω, où $2 \leq \omega \leq 3$ est un exposant pour la multiplication de matrice et d'autre part, celui de [8] a une complexité linéaire en tD^2. Ainsi, suivant le ratio t/D et la valeur prise pour ω, l'un ou l'autre algorithme est asymptotiquement plus rapide. Notre article [2] présente un nouvel algorithme pour cette seconde étape dont la complexité est quasi-linéaire en $t^{\omega-1}D$. Ainsi, quel que soient t/D et ω, il est asymptotiquement le plus rapide.

3.1 Idée générale

Cette étape de changement d'ordre s'appuie, classiquement, sur l'utilisation de matrices de multiplication. Il s'agit de matrices de taille $D \times D$ ayant deux types de lignes : des lignes denses et des lignes issues de la matrice identité (des 0 partout sauf un coefficient qui est 1). En particulier, dans la situation générique mentionnée précédemment, seule une matrice est nécessaire, celle dite de la dernière variable. Elle possède de plus exactement t lignes denses.

L'idée principale est de remplacer cette matrice par une matrice de taille $t \times t$ mais dont les coefficients sont des polynômes en une variable, de degrés moyens D/t. Cette matrice peut être vue comme une compression de la

matrice originelle et nécessite le même espace mémoire pour la stocker. Nous illustrons ci-dessous la matrice scalaire originelle M et la matrice polynomiale compressée P dans le cas de trois variables x, y et z :

$$M = \left(\begin{array}{cccc|cc|cc} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 7 & 26 & 26 & 3 & 6 & 0 & 14 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 12 & 0 & 26 & 0 & 14 & 1 & 10 & 24 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 26 & 20 & 10 & 11 & 0 & 2 & 27 & 5 \end{array}\right), \quad P = \begin{pmatrix} z^4 - 26z^3 - 26z^2 - 7z & -6z - 3 & -14z \\ -26z^2 - 12 & z^2 - z - 14 & -24z - 10 \\ -11z^3 - 10z^2 - 20z - 26 & -2z & z^2 - 5z - 27 \end{pmatrix}.$$

En s'appuyant sur les algorithmes rapides sur les matrices polynomiales [11], nous pouvons calculer la forme normale de Hermite de cette matrice en temps quasi-linéaire en $t^{\omega-1}D$. Sous les hypothèses de généricité données plus haut, cette forme nous permet de lire la base de Gröbner lexicographique du système donné en entrée et même une paramétrisation des solutions.

$$H = \begin{pmatrix} z^8 + 26z^7 + 8z^6 + 17z^5 + 19z^4 + z^3 + 28z^2 + 20z + 18 & 0 & 0 \\ 28z^7 + 23z^6 + 17z^5 + 25z^4 + 24z^3 + 17z^2 + 14z + 4 & 1 & 0 \\ 6z^7 + 13z^6 + 22z^5 + 12z^4 + 28z^3 + 24z^2 + 26z + 14 & 0 & 1 \end{pmatrix}.$$

Ainsi, on peut lire que les solutions (x_i, y_i, z_i) sont exactement telles que z_i annule le premier polynôme en z, de degré 8. De plus, la seconde ligne nous permet de paramétriser y_i en fonction de z_i, via le polynôme de la première colonne. De manière similaire, la dernière ligne nous informe que x_i se paramétrise en fonction de z_i, encore une fois via le polynôme de la première colonne.

3.2 Expérimentations

Nous avons étudié le comportement de cet algorithme en combinant l'implantation optimisée du calcul de forme normale de Hermite disponible dans POLYNOMIAL MATRIX LIBRARY (PML) [10] et des routines de `msolve` et comparé à l'implémentation actuelle de SPARSE-FGLM dans `msolve` [1].

Dans la Table 1, nous donnons les temps pour la première étape du calcul de bases de Gröbner par F_4 (et son *tracer*, voir le portfolio concernant `msolve`) avec les temps des différents algorithmes pour le changement d'ordre. Pour cette seconde étape, les points de comparaisons sont l'algorithme SPARSE-FGLM dans sa version originelle [8] (Wied.) ou par blocs [9, 13] (bl-Wied.) et notre nouvel algorithme (HNF).

TABLE 1 – Temps (en s) pour un système carré en n variables et degré d sur un corps fini premier avec un premier de 30 bits.

			Step 1 : P		Step 2 : H		
			`msolve`		`msolve`	NTL	PML
n, d	D	t	F_4	F_4-tr	Wied.	bl-Wied.	HNF
$11, 2$	2048	462	11.6	1.1	1.2	1.7	0.8
$12, 2$	4096	924	115.9	8.3	6.5	14.5	5.3
$13, 2$	8192	1716	970	62	103.6	110	34.8
$14, 2$	16384	3432	7921	460	1011	880	240
$15, 2$	32768	6435	61381	3193	7844	6691	1665
$16, 2$	65536	12870	482515	24523	58744	52709	11359
$8, 3$	6561	1107	122.6	12.8	23.6	44.7	15.1
$9, 3$	19683	3139	3552.7	361	1302	1163	314
$10, 3$	59049	8953	95052	8664	34844	29974	6709
$6, 4$	4096	580	9.9	2.2	4	8.8	3.5
$7, 4$	16384	2128	876	128	575	545	157
$8, 4$	65536	8092	57237	6977	36454	33452	7231

3.3 Impact scientifique

Cet algorithme ouvre la voie à un changement de paradigme dans le calcul de bases de Gröbner. Jusqu'à présent, le calcul de bases de Gröbner était appréhendé sous le prisme de l'algèbre linéaire creuse à coefficients scalaires. Nous remplaçons ici cette algèbre linéaire "scalaire" par de l'algèbre linéaire sur des polynômes à une variable. Ce

nouvel algorithme rend le changement d'ordre plus rapide que le calcul de la première base de Gröbner via F_4 [4], voir Table 1. Puisque ce premier calcul est dorénavant le facteur limitant, une prochaine étape sera d'étudier et modifier F_4 afin d'utiliser de l'algèbre linéaire polynomiale de sorte à en accélérer le calcul.

4 RÉFÉRENCES BIBLIOGRAPHIQUES

[1] J. Berthomieu, Ch. Eder, and M. Safey El Din. msolve : A Library for Solving Polynomial Systems. In *2021 International Symposium on Symbolic and Algebraic Computation*, pages 51–58, Saint Petersburg, Russia, July 2021.

[2] J. Berthomieu, V. Neiger, and M. Safey El Din. Faster Change of Order Algorithm for Gröbner Bases under Shape and Stability Assumptions. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation*, ISSAC '22, pages 409–418, New York, NY, USA, 2022. Association for Computing Machinery.

[3] B. Buchberger. A theoretical basis for the reduction of polynomials to canonical forms. *SIGSAM Bull.*, 10(3) :19–29, 1976.

[4] J.-Ch. Faugère. A New Efficient Algorithm for Computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1) :61–88, 1999.

[5] J.-Ch. Faugère. A New Efficient Algorithm for Computing Gröbner Bases Without Reduction to Zero (F5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, ISSAC '02, pages 75–83, New York, NY, USA, 2002. ACM.

[6] J.-Ch. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. *J. Symbolic Comput.*, 16(4) :329–344, 1993.

[7] J.-Ch. Faugère and Ch. Mou. Fast algorithm for change of ordering of zero-dimensional gröbner bases with sparse multiplication matrices. In *Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation*, ISSAC '11, pages 115–122, New York, NY, USA, 2011. ACM.

[8] J.-Ch. Faugère and Ch. Mou. Sparse FGLM algorithms. *Journal of Symbolic Computation*, 80(3) :538–569, 2017.

[9] S. G. Hyun, V. Neiger, H. Rahkooy, and É. Schost. Block-Krylov techniques in the context of sparse-FGLM algorithms. *J. Symb. Comput.*, 98 :163–191, 2020. Special Issue on Symbolic and Algebraic Computation : ISSAC 2017.

[10] S. G. Hyun, V. Neiger, and É. Schost. Implementations of efficient univariate polynomial matrix algorithms and application to bivariate resultants. In *Proceedings ISSAC 2019*, pages 235–242. ACM, 2019. `https://github.com/vneiger/pml`.

[11] G. Labahn, V. Neiger, and W. Zhou. Fast, deterministic computation of the Hermite normal form and determinant of a polynomial matrix. *J. Symb. Comput.*, 42 :44–71, 2017.

[12] V. Neiger and É. Schost. Computing syzygies in finite dimension using fast linear algebra. *Journal of Complexity*, 60 :101502, 2020.

[13] A. Steel. Direct Solution of the (11,9,8)-MinRank Problem by the Block Wiedemann Algorithm in Magma with a Tesla GPU. In *Proceedings PASCO 2015*, page 2–6. ACM, 2015.