Curriculum Vitae détaillé

Jérémy Marrez
Enseignant universitaire
en Informatique et Mathématiques

Docteur en Informatique

Table des matières

1. Curriculum Vitæ

Jérémy MARREZ

Enseignant universitaire
en Informatique et Mathématiques

Docteur en Informatique

Né le 3 Juin 1993 à Aubergenville (78), France
Nationalité française

Site web : jeremy-marrez.science
Mail : jeremy.marrez@hotmail.fr

Situation actuelle

2023- **Professeur d'Informatique et de Mathématiques (PRCE) à l'Université Paris-Saclay (Orsay)**

Département d'Informatique, UFR des Sciences

Diplômes et formation

2020-2022 **Diplôme d'Université Formation Professeurs des lycées et collèges, Mathématiques** à l'Université Paris-Saclay (Orsay)
Stage suivant l'admission au concours externe du Capes de Mathématiques en 2021
Sujet du travail scientifique de nature réflexive : « Modalités du travail de groupe en seconde et impact sur l'engagement des élèves »
Encadrement : Line ORRÉ

2016-2019 **Doctorat en Informatique** de Sorbonne Université (Paris)

Titre : « Représentations adaptées à l'arithmétique modulaire et à la résolution de systèmes flous »
Date de soutenance : 6 décembre 2019
Laboratoire d'Informatique de Paris 6 (LIP6), UMR 7606, Équipe Algorithmes pour la sécurité des communications

Jury :	Louis GOUBIN	Pr.	UVSQ	Président
	Marine MINIER	Pr.	Université de Lorraine	Rapporteure
	Clément PERNET	MCF HDR	Université Grenoble Alpes	Rapporteur
	Annick VALIBOUZE	Pr.	Sorbonne Université	Examinatrice
	Jean-Claude BAJARD	Pr.	Sorbonne Université	Directeur
	Lokmane ABBAS-TURKI	MCF	Sorbonne Université	Encadrant

2015-2016 **Master Mention Mathématiques et Applications parcours Algèbre Appliquée** à l'UFR des sciences de l'Université de Versailles Saint-Quentin-en-Yvelines (Versailles) - Mention Bien

Sujet : « Étude et implantation d'une méthode algébrique pour résoudre des systèmes à coefficients flous »
Encadrement : Annick Valibouze (directrice) et Philippe Aubry (encadrant)
Laboratoire d'Informatique de Paris 6 (LIP6), UMR 7606, Équipe Algorithmes, Programmes et Résolution
• Bourse Master du programme Excellence de la Fondation Mathématique Jacques Hadamard

2014-2015 **Maîtrise Mention Mathématiques** à l'UFR des sciences de l'Université de Versailles Saint-Quentin-en-Yvelines (Versailles) - Mention Très Bien

• Bourse Master du programme Excellence de la Fondation Mathématique Jacques Hadamard

2011-2014 **Licence Sciences et Technologies, Santé, Mention Informatique** à l'UFR des sciences de l'Université de Versailles Saint-Quentin-en-Yvelines (Versailles) - Mention Bien

2011-2014 **Licence Sciences et Technologies, Santé, Mention Mathématiques** à l'UFR des sciences - Université de Versailles Saint-Quentin-en-Yvelines (Versailles) - Mention Bien

2008-2011 **Baccalauréat Scientifique option Sciences de la Vie et de la Terre** au Lycée Sonia Delaunay (Villepreux) - Mention Bien

Activités d'enseignement

2019-2020 **Attaché Temporaire d'Enseignement et de Recherche**

Filière Informatique, UFR d'Ingénierie à Sorbonne Université (Paris)
Total de 201.5 heures équivalent TD en Licence (L1, L2, L3) et Master (M1, M2)

Rattaché au Laboratoire d'Informatique de Paris 6 (LIP6), UMR 7606, Équipe Algorithmes pour la sécurité des communications

2016-2019 **Doctorant contractuel** (moniteur)

Filières Informatique et Mathématique, UFR d'Ingénierie et de Mathématiques à Sorbonne Université (Paris)
Total de 241.5 heures équivalent TD en Licence (L1, L2) et Master (M2)

Compétences générales

Langues

Français	Langue maternelle
Anglais	Courant
Espagnol	Intermédiaire

Transversales

Propriété intellectuelle	Dépôt de logiciel
Gestion de projet	Planification de tâches, Rédaction de rapport
Communication	Présentations orales, Articles, Posters, Rapports techniques, Schémas et dessins
Enseignement, formation	Rédaction de contrôle et de devoir de TD et TP Élaboration collective de sujets d'examen, de TD et TP Encadrement de projets Corrections et gestion de notes Documentations techniques Manuels utilisateurs
Savoir être	Écoute, Adaptabilité, Autonomie, Gestion des conflits, Esprit de synthèse et d'analyse, Travail en équipe, Gestion des priorités

Compétences informatiques

Langages	C, C++, C#, CUDA, Java, Python, Lisp Javascript, PHP, XML, SQL, Assembleur, Fortran
IDE	Eclipse, Matlab / Scilab, GNUplot, Magma, Geany, Spyder, MARS
Web	XHTML, CSS, Apache
Bases de données	Oracle, SQL Server, Access, MySQL
Systèmes d'exploitation	Windows, Unix / Linux, Mac OS
Bureautique	Microsoft Office, OpenOffice, Latex / TikZ

Autres activités et intérêts

Cinéma	Tous les genres, réalisation de petits films indépendants
Réalisation, montage	Réalisation d'un documentaire au parc des Loups du Gévaudan en Lozère
Lecture, écriture	Romans historiques, fantastiques, naturalistes, essais, poésie, philosophie, psychologie, art et architecture
Musique	Piano, Chant
Sport	Sport en salle
Programmation	Création de jeux de réflexion et de divertissement 2D

2. Activités d'enseignement dans le supérieur

Synthèse des enseignements

Mon statut de doctorant moniteur m'a permis d'effectuer **241.5 heures équivalent TD** au sein des filières Informatique et Mathématiques de Sorbonne Université, en Licence et en Master.

J'ai poursuivi mes activités d'enseignements en tant qu'ATER au sein de la filière Informatique de Sorbonne Université, en Licence et en Master, pour un total de **201.5 heures équivalent TD**.

Année et statut	Enseignement	Formation	TD	TP (HETD)	Total (HETD)
2019	Conception pratique d'algorithmes	M1 Informatique	6h		6h
2020	Programmation Objet avancée	L3 Informatique	38.5h	(+2h G)	40.5h
ATER	Algorithmique I	L2 Informatique	38.5h		38.5h
	Atelier de Recherche Encadrée	L1	30h		30h
	Algorithmique avancée	M1 Informatique	40h		40h
	Analyse d'algorithmes et génération aléatoire	M2 Informatique	6h		6h
	Mathématiques discrètes	L2 Informatique	38.5	(+2h G)	40.5h
2018	Introduction à l'architecture	L2 Informatique		19.3h	19.3h
2019	Structures discrètes	L2 Informatique		21h	21h
Moniteur	Crédit d'heures Moniteur	Excédent 2018-2019	36.6h		36.6h
2017	Programmation CUDA	M2 Maths	14h		14h
2018	Calcul haute performance : programmation et algorithmique avancée	M2 Informatique		14h	14h
Moniteur	Introduction à l'architecture, rep. des données et programmes	L2 Informatique		36.8h	36.8h
	Éléments de programmation 1	L1 Informatique		40.3h	40.3h
2016	Introduction aux bases de données	L2 Informatique		38.5h	38.5h
2017	relationnelles				
Moniteur	Représentations et méthodes numériques	L2 Informatique		21h	21h
		TOTAL	*252,1h*	*190,9h*	*443h*

Détail des enseignements dispensés

ATER

2019-2020

Programmation Objet avancée

40.5 HETD de TD en L3 informatique, UFR d'Ingénierie, effectif : 40

- Structuration en classes, relations entre classes, Cycle de vie des objets
- Héritage et Polymorphisme, liaison tardive, Abstraction et modularisation : interface et paquetage, Conception par contrat, exceptions et tests unitaires
- Classes génériques et collections, Design patterns

Algorithmique 1

38.5 HETD de TD en L2 informatique, UFR d'Ingénierie, effectif : 35

- Bases mathématiques (techniques de preuve), Validité, terminaison et complexité d'un algorithme itératif et récursif, application aux listes
- Tris, Arbres binaires : notions de base, induction structurelle, équilibrage, tas, arbres binaires de recherche
- Graphes : terminologie, propriétés élémentaires sur les graphes, premiers algorithmes sur les graphes (parcours, fermeture transitive, ordre topologique)

Conception pratique d'algorithmes

6 HETD de TD en M1 informatique parcours Science et Technologie du Logiciel, UFR d'Ingénierie, effectif : 30

- Arbre couvrant, Plus courts chemins et arbre de Steiner
- Introduction à l'algorithmique des graphes de terrain, Communautés dans les graphes
- PageRank, k-core décomposition et sous-graphes denses, Compression de graphes

Atelier de recherche encadrée CALRAIS (Calcul et Raisonnement)

30 HETD de TD en L1, SGFI, effectif : 30

- L'objectif est de fournir les éléments méthodologiques permettant d'acquérir de manière autonome des connaissances en mathématiques et en informatique. Une attention particulière est portée sur la démarche et la rigueur dans l'acquisition et la restitution de ces connaissances.
- En mathématiques, les thèmes abordés portent sur les notions de base sur les ensembles, les relations et les fonctions. Il s'agit via une plateforme logicielle pédagogique de (re)découvrir ces notions et de les expérimenter au travers de petits raisonnements mathématiques. Écriture de programmes informatiques sur les aspects calculatoires des concepts abordés.
- En informatique, un ensemble de textes – souvent sur les liens entre mathématiques et informatique – est proposé. Les textes choisis font l'objet d'une étude et donnent lieu à la rédaction d'un rapport (incluant une bibliographie) et à un exposé oral.

Algorithmique avancée

40 HETD de TD en M1 informatique parcours Science et Technologie du Logiciel, UFR d'Ingénierie, effectif : 30

- Étude des files de priorité : notations asymptotiques, coût amorti, files binomiales
- Recherche arborescente : arbres bicolores, arbres de recherche versus tries
- Hachage dynamique, application des familles de fonctions de hachage universelles, hachage k-universel, filtres de Bloom

Analyse d'algorithmes et génération aléatoire

6 HETD de TD en M2 informatique parcours Science et Technologie du Logiciel, UFR d'Ingénierie, effectif : 20

- Génération d'entiers : nombres aléatoires, générateurs linéaires congruentiels, twister de Mersenne
- Générateur d'arbres à la Rémy, arbres binaires de recherche
- Analyse en moyenne de Quicksort, génération de structures arborescentes

Mathématiques discrètes

40.5 HETD de TD en L2 informatique, UFR d'Ingénierie, effectif : 40

- Notions en lien avec le problème de la terminaison de programmes, récursion, compilation et recherche de motifs
- Étude des automates et de leur manipulation (intersection, déterminisation, minimisation...), des langages reconnaissables ou non, et des preuves par induction structurelle
- Introduction à la logique

Moniteur

2018-2019

Introduction à l'architecture, représentation des données et programmes

19.3 HETD de TP en L2 informatique, UFR d'Ingénierie, effectif : 30

- Étude de l'architecture générale d'un ordinateur, des fonctions booléennes et de la représentation des entiers naturels, relatifs, et des caractères alphanumériques
- Notions d'opérande registre et mémoire, d'instructions et de jeu d'instruction MIPS, et étude des circuits représentant le chemin de données du MIPS avec Logisim
- Introduction à la programmation assembleur avec le logiciel MARS

Structures discrètes (Mathématiques discrètes)

21 HETD de TP en L2 informatique, UFR d'Ingénierie, effectif : 40

2017-2018

Programmation CUDA

14 HETD de TD en M2 Mathématiques et Applications parcours Ingénierie Financière et Modèles Aléatoires, UFR de Mathématiques, effectif : 15

Calcul haute performance : programmation et algorithmique avancées
14 HETD de TP en M2 en Master informatique parcours Sécurité, Fiabilité et Performance du Numérique, UFR d'Ingénierie, effectif : 15

- Algorithmes et techniques de programmation parallèles avancés pour concevoir, implémenter et optimiser des programmes parallèles sur des architectures hétérogènes et massivement parallèles
- Calcul haute performance sur architectures hétérogènes (GPU ...), introduction aux langages standards pour le calcul haute performance avec CUDA/C (extensions de langage et directives de compilation), optimisation de code dans un contexte hétérogène
- Programmation GPU avec des équations différentielles partielles pour des applications financières

Introduction à l'architecture, représentation des données et programmes

36.8 HETD de TP en L2 informatique, UFR d'Ingénierie, effectif : 30

Éléments de programmation 1

40.3 HETD de TP en L1 informatique, UFR d'Ingénierie, effectif : 30

- Étude et résolution de problèmes simples (numériques, informatiques, de données) par des outils informatiques
- Introduction des concepts fondamentaux de la programmation et première approche des notions élémentaires d'algorithmique ; programmation impérative avec sémantique semi-formelle, techniques générales de bonne programmation, concepts d'algorithmique, manipulation de constructions spécifiques
- Pour un public très large, sans aucun prérequis en programmation. Utilisation d'un langage de haut-niveau largement répandu, à la fois dans les mondes du développement et de la pédagogie : Python

2016-2017

Introduction aux bases de données relationnelles

38.5 HETD de TP en L2 informatique, UFR d'Ingénierie, effectif : 40

- Introduction aux bases de données relationnelles
- Utilisation pratique d'un système de gestion de base de données
- Fondements théoriques du modèle de données relationnel à travers le langage SQL

Représentations et méthodes numériques

21 HETD de TP en L2 informatique, UFR d'Ingénierie, effectif : 30

- Manipulation des nombres entiers, flottants et algorithmes associés
- Algorithmes de résolution de systèmes linéaires
- Méthodes d'interpolation polynomiale, et recherche des zéros

3. Publications

Revues internationales avec comité de lecture

[1] *On Polynomial Modular Number Systems over $\mathbb{Z}/p\mathbb{Z}$*
J. Marrez, J.C. Bajard, T. Plantard et P. Véron
Advances in Mathematics of Communications (AIMS), 2022

Contributions :
▷ *introduction de méthodes pour construire des bases d'un sous-réseau du réseau euclidien associé au système PMNS, assurant de faibles bornes sur les chiffres des représentations*
▷ *introduction des classes de polynômes de réduction externe adaptés à l'arithmétique sur les PMNS, garantissant une arithmétique efficace sur les représentations*
▷ *introduction de méthodes pour compter le nombre de systèmes obtenus à partir de ces classes (cas cyclotomique, binomial et général)*
▷ *tests et exemples*

[2] *Computing real solutions of fuzzy polynomial systems*
P. Aubry, J. Marrez et A. Valibouze (par ordre alphabétique)
Fuzzy Sets and Systems (Q1), 2020

Contributions :
▷ *introduction d'un système tranché général, applicable pour tous les systèmes polynomiaux avec des coefficients flous de type L-R, avec L et R bijectives*
▷ *introduction de la transformation réelle pour calculer les solutions positives d'un système flou*
▷ *introduction d'une méthode pour calculer les solutions réelles d'un système à coefficients flous symétriques à partir des solutions positives de systèmes induits, et optimisation de la méthode de résolution en réduisant le nombre de systèmes à résoudre*
▷ *implantation de l'algorithme optimisé et tests*

Conférences internationales avec comité de sélection et actes

[3] *Randomization of arithmetic over Polynomial Modular Number System*
L.S. Didier, F. Y. Dosso, N. El Mrabet, J. Marrez et P. Véron
(par ordre alphabétique)
26th IEEE International Symposium on Computer Arithmetic (ARITH-26), 2019, 199 - 206

Contributions :
▷ *utilisation d'un algorithme de type Babaï pour la réduction des coefficients au sein du système PMNS*
▷ *introduction d'une borne sur le produit de deux représentations du PMNS*
▷ *randomisation de la procédure de conversion du binaire vers le PMNS et de la multiplication au sein du PMNS avec la méthode de type Babaï, garantissant une protection face aux attaques SCA et aux attaques spécifiques de points (Goubin)*
▷ *estimation de la complexité, implantation et tests des algorithmes de type Babaï*

[4] *HyPoRes : An Hybrid Representation System for ECC*
P. Martins, J. Marrez, J.C. Bajard et L. Sousa
26th IEEE International Symposium on Computer Arithmetic (ARITH-26), 2019, 207 - 214

Contributions :
▷ *introduction des critères assurant l'existence du polynôme de réduction externe du système HyPoRes*
▷ *introduction des critères sur la base RNS utilisée par le système pour garantir une représentation de 0 compatible avec l'algorithme de multiplication proposé*
▷ *introduction d'une méthode de conversion du binaire vers HyPoRes et d'une conversion inter-HyPoRes pour assurer une protection face aux attaques DPA*
▷ *estimation de la complexité, implantation et tests des algorithmes*

[5] *The Real Transform : Computing Positive Solutions of Fuzzy Polynomial Systems*
P. Aubry, J. Marrez et A. Valibouze (par ordre alphabétique)
11th International Joint Conference on Computational Intelligence (IJCCI), 2019, Oral, Position Paper, 351-359

Contributions :
▷ *introduction d'un système tranché général, applicable pour tous les systèmes polynomiaux avec des coefficients flous de type L-R, avec L et R bijectives*
▷ *introduction de la transformation réelle pour calculer les solutions positives des systèmes flous*
▷ *extension de la méthode proposée au cas des nombres flous trapézoïdaux*
▷ *comparaison avec les méthodes précédentes dans le cas triangulaire*

Actes de conférences, colloques, séminaires

[6] *Efficient and secure modular operations using the Polynomial Modular Number System*
L.S. Didier, F. Y. Dosso, N. El Mrabet, J. Marrez et P. Véron
(par ordre alphabétique)
Workshop on Randomness and Arithmetics for Cryptography on Hardware, Avril 2019, Oral, Station Biologique de Roscoff - CNRS - Sorbonne Université

[7] *Les systèmes de représentation adaptés polynomiaux (PMNS) et les racines de leur polynôme de réduction dans le corps* $\mathbb{Z}/p\mathbb{Z}$
J. Marrez
Séminaire du laboratoire IMATH, Équipe d'Informatique et Algèbre Appliquée, Janvier 2019, Oral, Université de Toulon, France

[8] *Étude et implantation d'une méthode algébrique pour résoudre des systèmes à coefficients flous*
P. Aubry, J. Marrez et A. Valibouze (par ordre alphabétique)
Journées Nationales de Calcul Formel, 2018, Oral, Centre international de rencontres mathématiques, Luminy, Marseille

Logiciel et documentation

[9] *Bibliothèque Fuzzy en SageMath : Modélisation des nombres flous dans leurs différentes représentations, et résolution des systèmes de polynômes à coefficients flous ou réels* (www.github.com/JeremyMarrez/Fuzzy)
J. Marrez
au sein de l'équipe APR du LIP6, 2017, Paris, France

Mémoire

[10] *Étude et implantation d'une méthode algébrique pour résoudre des systèmes à coefficients flous*
J. Marrez, sous la direction d'Annick Valibouze
au sein de l'équipe APR du LIP6, 2016, Paris, France

4. Charges collectives

Co-organisation d'atelier de recherche

2020 **Coorganisateur de l'Atelier de Recherche Encadrée Calcul et Raisonnement (ARE CALRAIS) en Licence 1ère année** à Sorbonne Université, Paris, France
Durée : 1 semestre

- Choix pédagogiques, recherches documentaires et sélection de textes sur les thématiques de l'ARE accessibles au niveau L1 et permettant d'approfondir certaines notions
- Encadrement des étudiants dans le processus de formalisation des preuves, dans la compréhension des textes, dans la rédaction d'un rapport et dans la préparation d'un exposé oral
- Présentation de parties du cours, évaluation, gestion

Valorisation de la recherche

Co-organisation de colloques

2019 **Coorganisateur et Webmaster pour la conférence Workshop on Randomness and Arithmetics for Cryptography on Hardware** (https ://wrach2019.lip6.fr/) à Sorbonne Université, Paris, France
Durée : 3 mois

- Création du site web et mise à jour continue
- Gestion de la présentation du programme et des slides
- Cogestion des inscriptions et du calendrier

2017 **Coorganisateur des journées Deep Learning & Accélération GPU en collaboration avec HPE, NVIDIA et ANEO** à Sorbonne Université, Paris, France
Durée : 3 journées

- Accueil des participants
- Cogestion des sessions de présentation
- Transmission d'information aux auditeurs, sur le programme et les intervenants

Présentations affichées

2018 **Animation du stand d'initiation à la Cryptographie de l'équipe Algorithmes pour la sécurité des communications à la Fête de la Science** à Sorbonne Université, Paris, France
Durée : 1 semaine

- Production d'affiches et de schémas sur le chiffrement homomorphique en cryptographie, via LATEX avec TikZ
- Présentation et vulgarisation scientifique devant des publics hétérogènes

5. Activités de recherche

Exposés dans des conférences nationales ou internationales

Sept. 2019	**11th International Joint Conference on Computational Intelligence** à Vienne, Autriche Titre : « The Real Transform : Computing Positive Solutions of Fuzzy Polynomial Systems »
Avr. 2019	**Workshop on Randomness and Arithmetics for Cryptography on Hardware** à la Station Biologique de Roscoff - CNRS / Sorbonne UniversitéVienne, Bretagne, France Titre : « Efficient and secure modular operations using the Polynomial Modular Number System »
Janv. 2018	**Journées Nationales de Calcul Formel** au Centre international de rencontres mathématiques, Luminy, Marseille, France Titre : « Étude et implantation d'une méthode algébrique pour résoudre des systèmes à coefficients flous »

Exposés à des séminaires

Janv. 2019	**Séminaire du laboratoire IMATH, Équipe d'Informatique et Algèbre Appliquée** à l'Université de Toulon, France Titre : « Les systèmes de représentation adaptés polynomiaux (PMNS) et les racines de leur polynôme de réduction dans le corps $\mathbb{Z}/p\mathbb{Z}$ »
Juin 2018	**Journée de l'équipe APR** à Sorbonne Université, Paris, France Titre : « La transformation réelle : calculer les solutions positives des systèmes à coefficients flous »

Participation régulière à des groupes de travail, avec exposé

2016-2020	**Groupe de travail de l' Équipe Algorithmes pour la sécurité des communications** à Sorbonne Université, Paris, France

Participation à des conférences, congrès, colloques, écoles d'été en tant qu'auditeur

Févr. 2020	**Demie-journée Théorie et Outils mathématiques pour l'informatique** à Sorbonne Université, Paris, France
Juin 2019	**Conférence Number-Theoretic Methods in Cryptology** à Sorbonne Université, Institut de Mathématiques de Jussieu, Paris, France

Mai 2018	**Conférence Numeration** à l'Université Paris Diderot - Paris 7, Paris, France
Avr. 2018	**Groupe de travail ISCD Institute of Computing and Data Sciences** à Sorbonne Université, Paris, France
Mars 2018	**École de printemps "Post-Scryptum" dédiée aux méthodes algorithmiques pour la cryptographie post-quantique** à la station des 7 Laux, Isère, France

Séjours de recherche à l'étranger

Déc. 2018	Séjour à l'Instituto Superior Técnico (Université de Lisbonne, Portugal), INESC-ID avec Paulo Martins – Programme Pessoa, Partenariat Hubert Curien (PHC) franco-portugais
Juin 2017	Séjour au Computer & Information Security Research Laboratory (Université de Wollongong, Australie), avec Thomas Plantard – CNRS, Projet International de Coopération Scientifique (PICS)

Collaborations nationales et internationales

2018- 2020...	Laboratoire de l'Institut de Mathématiques de Toulon (Université de Toulon, France), équipe d'Informatique et Algèbre Appliquée (IAA) avec Yssouf Dosso ▷ *Collaboration sur la randomisation de l'arithmétique sur les systèmes PMNS*
2018- 2019...	Instituto Superior Técnico (Université de Lisbonne, Portugal), INESC-ID avec Paulo Martins ▷ *Collaboration sur l'amélioration de l'arithmétique modulaire via le système hybride HyPoRes*
2017- 2020...	Computer & Information Security Research Laboratory (Université de Wollongong, Australie), avec Thomas Plantard ▷ *Collaboration sur la recherche de bases de systèmes PMNS*

6. Thèse

Encadrement et financement

Ma thèse de doctorat, intitulée "Représentations adaptées à l'arithmétique modulaire et à la résolution de systèmes flous", et financée par l'Agence nationale de la recherche dans le cadre du projet Arithmétiques Randomisées - ARRAND [1], a débuté en novembre 2016 et a été soutenue en décembre 2019. Mes recherches ont été dirigées à Sorbonne Université par le Professeur Jean-Claude Bajard et co-encadrées par Lokmane Abbas-Turki (MCF). Mes travaux ont été réalisés au sein du Laboratoire d'informatique de Paris 6 (LIP6) et ont donné lieu à plusieurs collaborations nationales et internationales. Le manuscrit de thèse, ainsi que la présentation de soutenance sont disponibles à cette adresse : jeremy-marrez.science/publications.

Le jury de thèse était composé comme suit :

Louis Goubin	Pr.	UVSQ	Président
Marine Minier	Pr.	Université de Lorraine	Rapporteure
Clément Pernet	MCF HDR	Université Grenoble Alpes	Rapporteur
Annick Valibouze	Pr.	Sorbonne Université	Examinatrice
Jean-Claude Bajard	Pr.	Sorbonne Université	Directeur
Lokmane Abbas-Turki	MCF	Sorbonne Université	Encadrant

Mots-clés

— **Calcul formel, Intelligence artificielle** : Modélisation et gestion de données incertaines, résolution de systèmes polynomiaux à coefficients flous, approche globale de résolution, méthodes algèbriques, parallélisme

— **Cryptographie et sécurité, Arithmétique des ordinateurs :**

  — Efficacité et sécurité des primitives en cryptographie asymétrique, amélioration et randomisation de l'arithmétique modulaire, protections arithmétiques contre les attaques par canaux cachés

  — Algorithmes de réduction, systèmes de représentation adaptés au calcul modulaire, corps fini, réseaux, familles de polynômes, génération de systèmes compacts et efficient, complexité

  — Contre-mesures aux attaques sur les courbes elliptiques, représentations redondantes, système hybride, applications basées sur de grands corps finis premiers, représentations de loi uniforme

— **Développement logiciel :** Implantation de bibliothèque, Algorithme de résolution optimisé, systèmes induits, gestion des signes, identification de systèmes identiques, programmation mathématique

1. anr.fr/Projet-ANR-15-CE39-0002

7. Résumé des travaux de recherche

Thème 1 - Arithmétiques améliorées et randomisées pour la Cryptographie

Contexte

Au cours de mes trois années de thèse, je me suis intéressé dans un premier temps aux **calculs modulaires** entrant en jeu dans **les applications en cryptographie asymétrique**, qui utilisent le plus souvent un modulo premier standardisé dont le choix n'est pas toujours libre en pratique. Je me suis attaché à proposer des solutions pour **l'amélioration et la randomisation des opérations modulaires**, centrales dans le double problème de **l'efficacité et de la sécurité des primitives en cryptographie asymétrique**.

L'objectif de ce travail de recherche consiste à **fournir une arithmétique modulaire efficace pour le plus grand nombre de premiers possible**, tout en **la prémunissant contre certains types d'attaques**, comme les attaques par canaux cachés. Nous souhaitons ainsi contribuer à lever une partie des restrictions qui limitent la performance des calculs modulaires lorsque le choix du modulo est imposé par le protocole cryptographique.

L'originalité de notre approche consiste à la fois en **la recherche de bases d'un système** assurant une arithmétique modulaire efficace pour un modulo donné, et **l'exploitation de la redondance intrinsèque** à ces systèmes **pour rendre imprévisible la représentation des données** à chaque exécution. Nous proposons également **un système hybride améliorant l'arithmétique modulaire** pour tout modulo premier.

Recherche des bases d'un système assurant une arithmétique modulaire efficace pour un modulo premier donné (2016-2020)

Travail en collaboration avec l'Université de Wollongong

L'objectif est la recherche de bases d'un système de représentation qui a fait ses preuves en cryptographie ; le système de représentation adapté polynomial, ou Polynomial Modular Number System (PMNS) [11], utilisé pour l'arithmétique modulaire, avec des algorithmes plus efficaces que les méthodes sans division connues telles que Montgomery et Barrett ([12],[13]).

En effet, de nombreuses applications en cryptographie sont basées sur de grands corps finis premiers, comme les protocoles Diffie-Hellmann, ElGamal et ECC [14]. Notre but est de proposer de nombreuses bases de ce système en assurant une arithmétique efficace pour un modulo premier donné, chacune avec leurs propres propriétés de calcul. Cette capacité à fournir plusieurs représentations équivalentes est également un point intéressant en termes de performance si l'on veut masquer les calculs pour protéger une implantation contre des observateurs malveillants.

Néanmoins, la construction de ces systèmes est limitée par les paramètres restrictifs du théorème d'existence et la recherche de bases viables n'est pas triviale, conduisant à peu de systèmes en pratique. La construction de tels systèmes est basée sur des polynômes creux, appelés polynômes de réduction, dont les racines sont utilisées comme bases de ce type de représentation positionnelle. L'intérêt de ces polynômes creux réside dans l'efficacité de l'arithmétique modulaire engendrée. Le nombre de systèmes PMNS que nous pouvons générer à partir d'un entier p et d'un polynôme de réduction $E(X)$ est égal au nombre de racines de $E(X)$ dans $\mathbb{Z}/p\mathbb{Z}$.

Nous apportons des solutions à ces limitations, d'abord via la proposition d'un théorème général d'existence, en garantissant une borne sur les chiffres, qui peut être calculée simplement à partir de la norme 1 du réseau euclidien associé au système. Pour cela, nous proposons trois stratégies pour calculer une base d'un sous-réseau du réseau associé. Ce théorème nous conduit à considérer les systèmes PMNS définis par un polynôme de réduction irréductible, pour lesquels définir une base du réseau associé est aisé.

Par la suite, nous présentons des classes de polynômes adaptés pour obtenir des systèmes avec une arithmétique efficace sur les représentations. Ces polynômes sont sélectionnés en adaptant et en combinant des critères d'irréducitibilité (Dumas, Mills, Finch et Jones, Perron) et des corollaires (Ljunggren, Bonciotat) en fonction de la forme souhaitée. Enfin pour un premier p, nous proposons plusieurs méthodes pour évaluer le nombre de racines de polynômes modulo p en fonction du polynôme, afin de décrire le nombre minimum de bases PMNS que nous pouvons atteindre. Ces théorèmes, propositions et corollaires nous permettent de produire des PMNS avec des polynômes de réduction spécifiques garantissant des réductions efficaces et dont les racines fournissent les bases de ces systèmes.

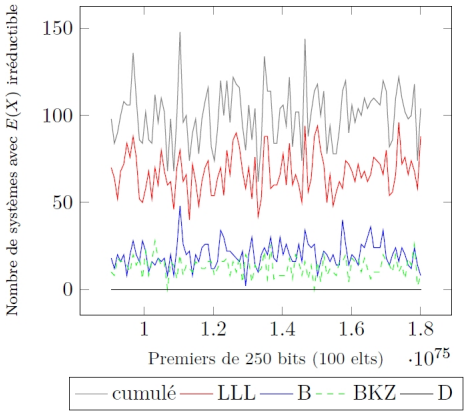


FIGURE 1 – Nombre de systèmes PMNS avec $n = 8$ chiffres, pour 100 premiers p de 250 bits tirés de façon uniforme, tels que $|\mathcal{B}|_1 < 4p^{1/n}$, où $\mathcal{B}$ est une base du réseau associé au système, calculée via LLL ou BKZ (stratégie 1), B (stratégie 2), ou D (stratégie 3), pour des polynômes de réduction irréductibles.

Nous avons à présent la possibilité d'offrir pour un modulo premier donné une grande variété de PMNS qui peuvent être utilisés efficacement pour différentes applications basées sur de grands corps finis premiers. Nos implémentations permettent la génération et la sélection des systèmes les plus compacts et efficients. À chaque exécution, un système différent peut être choisi.

L'ensemble de ces activités de recherche a été valorisé par :

— **1 revue internationale** [1] : Advances in Mathematics of Communications (AIMS), 2022 ;

— 1 présentation au séminaire du laboratoire IMATH à l'Université de Toulon [7], 2019.

Randomisation de l'arithmétique modulaire (2018-2020)

Travail en collaboration avec l'équipe d'Informatique et Algèbre Appliquée de l'Institut de Mathématiques de Toulon de l'Université de Toulon

Dans [3], nous montrons comment utiliser la redondance intrinsèque du système de représentation PMNS pour construire des protections arithmétiques efficaces contre les attaques SCA et les attaques spécifiques de points ([15],[16]). En effet, le système PMNS peut devenir très redondant quand la taille des chiffres augmente, laissant suggérer une possible exploitation de cette redondance afin de changer aléatoirement de représentation au cours des calculs, au sein d'une même exécution, pour empêcher tout hypothèse de la part d'un attaquant sur les représentations utilisées.

Nous décrivons comment randomiser les données en entrée lors de la conversion vers le système PMNS via deux algorithmes de type Montgomery et Babaï. Nous introduisons également deux multiplications modulaires randomisées sur le PMNS. Nous démontrons la résistance de nos constructions, et décrivons la génération d'un PMNS en garantissant, pour tous les éléments de $\mathbb{Z}/p\mathbb{Z}$, le nombre minimum de représentations distinctes que nous voulons. Nous montrons aussi comment accéder à toutes ces représentations. À partir d'une fonction générant un polynôme (ou un vecteur) aléatoire, aux coefficients bornés par un entier z, nos algorithmes peuvent génèrer des représentations aléatoires distinctes du même élément modulo un premier p. Ces représentations suivent une loi uniforme sur l'ensemble fini composé des $(2z+1)^n$ représentations obtenues pour chaque sortie possible de la fonction.

Ces méthodes peuvent être utilisées pour appliquer des contre-mesures classiques sur la multiplication scalaire $k\mathcal{P}$ sur les courbes elliptiques [17]. Contrairement à certaines contre-mesures existantes nécessitant une ECSM supplémentaire $k\mathcal{R}$ pour un point aléatoire $\mathcal{R}$, nous montrons que la randomisation du processus de conversion suffit à elle seule à protéger les données contre l'attaque de Goubin [16]. Ces résultats constituent une première étape dans l'utilisation de la randomisation des opérations arithmétiques sur le système PMNS et ouvrent de nouvelles perspectives dans le domaine des contre-mesures aux attaques SCA.

L'ensemble de ces activités de recherche a été valorisé par des publications dans :

— **1 conférence internationale** [3] : 26th IEEE International Symposium on Computer Arithmetic, 2019 ;

— 1 présentation au Workshop on Randomness and Arithmetics for Cryptography on Hardware [6], 2019.

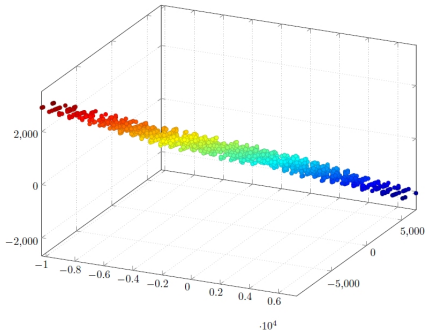


FIGURE 2 – Vecteurs retournés pour 1000 exécutions de la multiplication randomisée via Babaï pour le même système PMNS $\mathcal{B}$ et les mêmes représentations $A, B \in \mathcal{B}$ en entrée.

Introduction d'un système hybride pour améliorer l'arithmétique modulaire pour tout modulo premier (2018-2019)

Travail en collaboration avec deux membres de l'Instituto Superior Tecnico de l'Université de Lisbonne

Dans [4], nous proposons un nouveau système hybride pour le calcul modulaire. Le but est d'améliorer l'arithmétique modulaire pour tout modulo premier. L'état de l'art effectué dans ce domaine a mis en évidence que les systèmes proposant une arithmétique efficace sont souvent limités à des premiers spéciaux, avec de fortes contraintes. Bien qu'il soit possible d'implémenter l'addition et la multiplication de façon efficace via le système RNS [18], ce système se prête moins aux réductions modulaires. L'approche traditionnelle de Montgomery sur ces systèmes exige de revenir dans la représentation classique, une étape impliquant de grandes extensions de bases qui augmentent le coût de la réduction.

Le système hybride Hybrid Position-Residues Number System (HPR) [19], proposé par Bigou et Tisserand, rend les algorithmes de multiplication avec une complexité en temps sous-quadratique viables pour ECC, mais reste limité à des premiers d'une forme spéciale, empêchant d'étendre cette approche aux opérations de groupe sur des courbes elliptiques actuellement standardisées.

Pour répondre à ce besoin d'applicabilité pour les courbes elliptiques, nous proposons un nouveau système hybride, nommé HyPoRes, où les nombres sont représentés dans un système PMNS avec les coefficients représentés en RNS. Via un affaiblissement des hypothèses sous-jacentes, ce système atteint une complexité en temps sous-quadratique similaire, et supporte n'importe quelle valeur première, ce qui le rend compatible avec les courbes elliptiques standardisées.
Les résultats expérimentaux montrent que la réduction modulaire de HyPoRes est jusqu'à 1,4 fois plus rapide que les approches basées sur RNS pour les nombres premiers standardisés pour ECC. Ce système rend l'application de petites bases RNS de modules proches d'une puissance de deux, habituellement utilisées en traitement du signal, viable pour les applications cryptographiques. De plus, puisque ce système réduit la complexité des extensions de base par rapport à une approche purement RNS, il se prête mieux au parallélisme à une plus petite échelle. La possibilité de généraliser le polynôme de réduction permet également d'introduire des représentations redondantes, obtenues par des changements de systèmes, procurant une protection contre les attaques SCA.

Ce modèle a été appliqué dans des primitives de cryptographie. L'analyse des expérimentations menées lors de la thèse est très positive : nos méthodes fonctionnent quel que soit la forme du modulo utilisé, tout en permettant une arithmétique rapide et efficace [20]. L'ensemble de ces activités de recherche a été valorisé par une publication dans :

— **1 conférence internationale** [4] : 26th IEEE International Symposium on Computer Arithmetic, 2019.

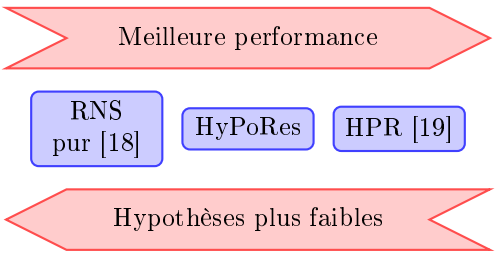


FIGURE 3 – Comparaison qualitative du système HyPoRes avec l'art associé [18, 19].

Thème 2 - Modélisation et résolution floue
(Calcul formel / Intelligence artificielle)

Contexte

En parallèle, dans **le champ de la modélisation incertaine**, je me suis intéressé à **la modélisation et la gestion des nombres flous** ainsi qu'à **la résolution réelle de systèmes flous**, enjeu majeur qui s'étend à un large spectre d'**applications en sciences, comme l'ingénierie, l'économie et les sciences sociales**.

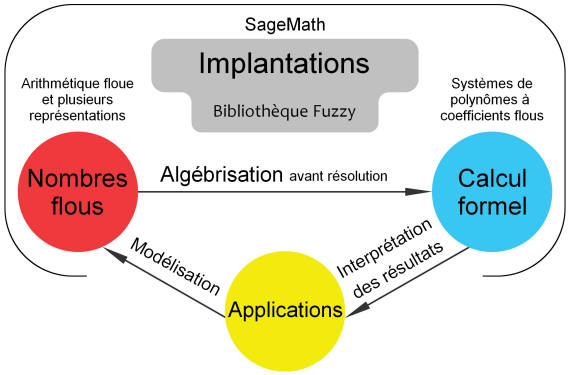
Introduction d'une méthode complète pour calculer les solutions réelles des systèmes flous (2016-2019)

Travail effectué au sein du LIP6 avec l'équipe Algorithmes, Programmes et Résolution

Dans ce travail, nous étudions la résolution réelle de systèmes à coefficients flous ; les coefficients sont des nombres flous, qui permettent de capturer l'incertitude autour d'une valeur donnée.

Certains problèmes sont modélisés par un système de fonctions continues à valeurs floues définies sur $\mathbb{R}^n$ [21] ; Liu propose une interpolation polynomiale fournissant une interface entre la résolution de ces problèmes et la résolution de systèmes polynomiaux à coefficients flous [22]. Les méthodes de résolution se sont d'abord appuyées sur des techniques locales ([23], [24], [25]). Puis ces dernières années s'est développée une approche globale faisant appel à des techniques algébriques classiques ([26, 27]). Ces nombres flous, issus des expériences, sont donnés sous une représentation appelée "tuple" qui, bien que formelle, ne peut être traitée par les méthodes algébriques habituelles (bases de Gröbner [28], décomposition triangulaire [29], représentation univariée rationnelle [30], ...).

Néanmoins, cette représentation en tuple est transformable en une autre représentation dite "paramétrique", où les coefficients ne sont plus flous mais réels, obtenue en inversant les fonctions de dispersions associées. Étant donné un système flou (S) de s équations et k indéterminées, les méthodes algébriques globales existantes effectuent des calculs avec la représentation paramétrique des coefficients, en se limitant au cas des nombres flous triangulaires.



Ce travail a débuté durant mon stage de Master, par la conception d'une bibliothèque pour modéliser et gérer des nombres flous. Le but était d'implanter la méthode algèbrique de Wu Wen Tsun pour calculer les solutions positives d'un système de polynômes à coefficients flous triangulaires [31]. Suite à ce stage, nous avons étendu et renforcé l'approche globale de résolution. Nous montrons que ces calculs sont superflus et présentons une formule, la transformation réelle, qui définit un système équivalent avec moins d'équations et possédant les mêmes solutions positives que le système de départ. Cette méthode peut s'appliquer à n'importe quelle famille de nombre flous, et ce, sans avoir à calculer l'inverse des fonctions de dispersions. Une adaptation de ces résultats aux nombres flous trapézoïdaux est donnée.

Pour résoudre des équations avec des coefficients flous symétriques, il faut également se poser la question du signe des solutions. Cette question est intrinsèque aux nombres flous et provient du fait que la multiplication d'un nombre flou par un scalaire réel s'exprime différemment selon le signe de ce scalaire. Notre stratégie consiste à nous concentrer sur les solutions positives en reportant a priori sur les coefficients flous ce problème de signes. Nous rendons possible cette stratégie en exprimant l'ensemble des solutions réelles de (S) à partir des solutions positives de systèmes réels induits, dont certains sont identiques. Pour identifier les systèmes induits identiques, nous proposons un algorithme optimisé implémenté dans la bibliothèque `Fuzzy` en `SageMath` [32], décrivons une parallélisation de l'algorithme et illustrons son fonctionnement.

L'ensemble de ces activités de recherche a été valorisé par des publications dans :

- **1 revue internationale** [2] : Fuzzy Sets and Systems (Q1), 2020 ;
- **1 conférence internationale** [5] : 11th International Conference on Fuzzy Computation Theory and Applications, part of the 11th International Joint Conference on Computational Intelligence, 2019 ;
- 1 présentation aux Journées Nationales de Calcul Formel au Centre international de rencontres mathématiques à Luminy, Marseille [8], 2018.

8. Bibliographie

[1] Jean-Claude Bajard, Jérémy Marrez, Thomas Plantard, and Pascal Véron. On Polynomial Modular Number Systems over $\mathbb{Z}/p\mathbb{Z}$. *Advances in Mathematics of Communications*, 2022. Available from : https://hal.science/hal-03611829.

[2] Philippe Aubry, Jérémy Marrez, and Annick Valibouze. Computing real solutions of fuzzy polynomial systems. *Fuzzy Sets and Systems*, January 2020. Author's version available from : http://jeremy-marrez.science/Computing%20real%20solutions%20of%20fuzzy%20polynomial%20systems%20Aubry,%20Marrez%20and%20Valibouze%20FSS.pdf.

[3] L.-S. Didier, F.-Y. Dosso, N. El Mrabet, J. Marrez, and P. Véron. Randomization of arithmetic over polynomial modular number system. June 2019. Available from : https://hal.archives-ouvertes.fr/hal-02099713.

[4] Paulo Martins, Jérémy Marrez, Jean-Claude Bajard, and Leonel Sousa. Hypores : An hybrid representation system for ecc. June 2019. Available from : https://hal.sorbonne-universite.fr/hal-02337787/.

[5] Philippe Aubry, Jérémy Marrez, and Annick Valibouze. The Real Transform : Computing Positive Solutions of Fuzzy Polynomial Systems. In *11th International Conference on Fuzzy Computation Theory and Applications*, volume 1 : FCTA of *Proceedings of the 11th International Joint Conference on Computational Intelligence*, pages 351–359, Vienna, Austria, September 2019. SciTePress - Science and Technology Publications. Available from : https://hal.archives-ouvertes.fr/hal-02457335.

[6] Jérémy Marrez. Efficient and secure modular operations using the polynomial modular number system. [Online]. Presentation available from : https://wrach2019.lip6.fr/slides/Efficient%20and%20secure%20modular%20operations%20using%20PMNS%20-%20J%C3%A9r%C3%A9my%20Marrez.pdf, english, 2019. Workshop on Randomness and Arithmetics for Cryptography on Hardware.

[7] Jérémy Marrez. Les systèmes de représentation adaptés polynomiaux (pmns) et les racines de leur polynôme de réduction dans le corps $\mathbb{Z}/p\mathbb{Z}$. [Online]. Presentation available from : http://jeremy-marrez.science/Slides%20S%C3%A9minaire%20IMATH.pdf, english, 2019. Séminaire du laboratoire IMATH, Équipe d'Informatique et Algèbre Appliquée, Université de Toulon, France.

[8] Jérémy Marrez. Étude et implantation d'une méthode algébrique pour résoudre des systèmes à coefficients flous. [Online]. Presentation available from : http://jeremy-marrez.science/Pr%C3%A9sentation%20JNCF%202018%20en.pdf, english. Resume available from : https://jncf2018.lip6.fr/program/abs-marrez.pdf, french, 2018. Journées Nationales de Calcul Formel (JNCF), Centre international de rencontres mathématiques, Luminy, Marseille, France.

[9] Jérémy Marrez. Bibliothèque Fuzzy en SageMath, Documentation. Technical report, December 2017. Available from : https://hal.sorbonne-universite.fr/hal-01663476.

[10] Jérémy Marrez. Étude et implantation d'une méthode algébrique pour résoudre des systèmes à coefficients flous. Mémoire de stage, UFR des Sciences de l'Université de Versailles Saint-Quentin-en-Yvelines, September 2016. Available from : http://jeremy-marrez.science/M%C3%A9moire%20de%20stage%20-%20J%C3%A9r%C3%A9my%20Marrez.pdf, french.

[11] T. Plantard. *Arithmétique modulaire pour la cryptographie*. Theses, Université Montpellier II - Sciences et Techniques du Languedoc, 2005.

[12] P.D. Barrett. Implementing the rivest shamir and adleman public key encryption algorithm on a standard digital signal processor. In Springer-Verlag, editor, *Advances in Cryptology, Proc. Crypto'86*, volume 263 of *LNCS*, pages 311–323, 1987.

[13] P.L. Montgomery. Modular multiplication without trial division. *Mathematics of Computation*, 44 :519–521, 1985.

[14] Jonathan Katz, Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 1996.

[15] P. Kocher. Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems. In *CRYPTO*, LNCS, pages 104–113. Springer, 1996.

[16] L. Goubin. A refined power-analysis attack on elliptic curve cryptosystems. In *Public Key Cryptography*, volume 2567 of *LNCS*, pages 199–210. Springer, 2003.

[17] J. Fan and I. Verbauwhede. An updated survey on secure ECC implementations : Attacks, countermeasures and cost. In *Cryptography and Security : From Theory to Applications*, pages 265–282. Springer, 2012.

[18] Samuel Antao, Jean Claude Bajard, and Leonel Sousa. RNS-based elliptic curve point multiplication for massive parallel architectures. *The Computer Journal*, 55 :629–647, 05 2012.

[19] K. Bigou and A. Tisserand. Hybrid position-residues number system. In *IEEE 23nd Symposium on Computer Arithmetic (ARITH)*, pages 126–133, July 2016.

[20] Paulo Martins and Jérémy Marrez. HyPoRes Multiplication C++. [Online]. Code available from : https://github.com/JeremyMarrez/HyPoRes, 2019. GitHub repository.

[21] Weldon A. Lodwick and Jorge Santos. Constructing consistent fuzzy surfaces from fuzzy data. *Fuzzy Sets and Systems*, 135(2) :259 – 277, 2003.

[22] Puyin Liu. Analysis of approximation of continuous fuzzy functions by multivariate fuzzy polynomials. *Fuzzy Sets and Systems*, 127(3) :299–313, 2002.

[23] Saeid Abbasbandy and Mahmood Otadi. Numerical solution of fuzzy polynomials by fuzzy neural network. *Applied Mathematics and Computation*, 181(2) :1084–1089, 2006.

[24] H. Rouhparvar. Solving fuzzy polynomial equation by ranking method. First Joint Congress on Fuzzy and Intelligent Systems, Ferdowsi University of Mashhad, Iran, 2007.

[25] S. Abbasbandy, M. Otadi, and M. Mosleh. Numerical solution of a system of fuzzy polynomials by fuzzy neural network. *Information Sciences*, 178(8) :1948 – 1960, 2008.

[26] Ali Abbasi Molai, Abdolali Basiri, and Sajjad Rahmany. Resolution of a system of fuzzy polynomial equations using the gröbner basis. *Information Sciences*, 220 :541–558, 2013.

[27] Marziyeh Boroujeni, Abdolali Basiri, Sajjad Rahmany, and Annick Valibouze. Finding solutions of fuzzy polynomial equations systems by an algebraic method. *Journal of Intelligent & Fuzzy Systems*, 30(2) :791–800, 2016.

[28] Becker and Weispfenning. *Grobner bases*, volume 141 of *Graduate texts in math*. Springer-Verlag, 1993.

[29] Philippe Aubry and Marc Moreno Maza. Triangular sets for solving polynomial systems : a comparative implementation of four methods. *Journal of Symbolic Computation*, 28 :125–154, 07 1999.

[30] Fabrice Rouillier. Solving Zero-Dimensional Systems through the Rational Univariate Representation. *Applicable Algebra in Engineering, Communication and Computing*, 9(5) :433–461, May 1999. Article dans revue scientifique avec comité de lecture.

[31] Wen-tsun Wu. A zero structure theorem for polynomial-equations-solving and its applications. In *EUROCAL*, page 44, 1987.

[32] Jérémy Marrez. Fuzzy package SageMath. [Online]. Code available from : https://github.com/JeremyMarrez/Fuzzy, 2019. GitHub repository.