Andrea Lesavourey

Curriculum Vitae

andrea.lesavourey@inria.fr
https://andlesav.github.io/

Mes travaux de recherche portent essentiellement sur l'analyse de problèmes algorithmiques liés aux réseaux euclidiens dans un contexte cryptographique, ainsi que sur la théorie algorithmique des nombres. Je m'intéresse notamment à la possibilité de retrouver des éléments courts dans des réseaux algébriques (idéaux ou modules). J'ai d'abord travaillé sur le problème du Short Generator Principal Ideal Problem (SG-PIP) dans des extensions de Kummer durant mon doctorat. Durant mon post-doctorat au sein de l'équipe CAPSULE à Rennes, je me suis concentré sur des problématiques plus proches des considérations actuelles de la cryptographie fondée sur les réseaux euclidiens, notamment en travaillant sur l'étude de la complexité des problèmes Ideal-SVP et Module-SVP. Je suis maintenant membre de l'équipe STORM à Bordeaux, au sein de laquelle je travaille à incorporer les codes correcteurs d'erreurs utilisés en cryptographie post-quantique dans le logiciel AFF3CT.

Scolarité

Parcours

oct. 2017–juin 2021 **Doctorat**, *University of Wollongong*, Wollongong (Australie)
Responsables : Willy Susilo et Thomas Plantard
Usability of structured lattices for a post-quantum cryptography: practical computations, and a study of some real Kummer extensions.
Dans cette thèse je me suis intéressé à la possibilité d'utiliser les réseaux euclidiens afin de construire des cryptosystèmes post-quantiques, c'est-à-dire qui résistent à la puissance du calcul quantique. Je me suis concentré sur l'étude pratique de problèmes algorithmiques qui sous-tendent la sécurité de certaines constructions. J'ai notamment étudié la possibilité de retrouver en pratique des générateurs courts d'idéaux dans des extensions de Kummer réelles de grands degrés. Pour ce faire, j'ai développé et implanté des algorithmes efficaces pour résoudre certaines tâches classiques dans des corps de nombres, comme le calcul de racines polynomiales.

juin 2016 **Master 1 de Cryptologie**, *Université de Bordeaux*, Bordeaux

juin 2015 **Master 2 "Mathématiques fondamentales"**, *Université de Bordeaux*, Bordeaux
Mémoire encadré par Pierre Parent
Théorème de Chabauty et et version effective de Coleman

sept. 2012– juin 2014 **Agrégation de mathématiques, option Probabilités et statistiques**, *Université de Bordeaux*, Bordeaux

juin 2012 **Master 1 "Mathématiques fondamentales"**, *Université de Bordeaux*, Bordeaux

juin 2011 **Licence "Mathématiques fondamentales"**, *Université de Bordeaux*, Bordeaux

sept. 2008–juillet 2010 **CPGE (MPSI-MP)**, *Lycée Michel Montaigne*, Bordeaux

Projets notables

juin 2016 **Projet de Master 1 Cryptologie**
Encadré par Christophe Nègre et Thomas Plantard
Randomisation en RNS et Leak Resistant arithmetic
La "Leak Resistant Arithmetic" propose de randomiser une procédure d'exponentiation en représentation RNS via la multiplication de Montgomery. Nous avons étudié une approche différente où le masque n'est pas effacé durant l'exponentiation. Cela permet d'économiser deux multiplications par étape de boucle et d'améliorer le niveau de randomisation. Ce travail a mené à une publication dans une conférence internationale avec comité de relecture.

Expérience professionelle

octobre 2023–aujourd'hui **Ingénieur de recherche**, *Equipe STORM, INRIA*, Bordeaux (France)

juin 2021–août 2023 **Post-doctorant**, *Equipe CAPSULE, Univ Rennes, CNRS, IRISA*, Rennes (France)

2016–2017 **Professeur agrégé de Mathématiques**, *Lycée Malherbe*, Caen
Classes de Seconde générale et de Première scientifique.

Compétences

Langues Français (langue maternelle), Anglais (intermédiaire), Espagnol (débutant).

Programmation C (bases), Python, SageMath, Pari/Gp, Magma

Activités académiques et de recherche

Articles de revues internationales avec comité de relecture

2020 **Short Principal Ideal Problem in multicubic fields**, avec T. Plantard et W. Susilo, *Journal of Mathematical Cryptology* 14.1: 359-392. `https://doi.org/10.1515/jmc-2019-0028`
Version post-print de l'article accepté à NuTMiC 2019, publié après une seconde phase de relecture.

Articles de conférences internationales avec comité de relecture

2023 **Computing eth roots in number fields**, avec O. Bernard, P.-A. Fouque, SIAM Symposium on Algorithm Engineering and Experiments (ALENEX24)
`https://www.siam.org/conferences/cm/conference/alenex24`

2022 **Log-S-unit lattices using Explicit Stickelberger Generators to solve Approx Ideal-SVP**, avec O. Bernard, T. H. Nguyen, et A. Roux-Langlois, AsiaCrypt 2022
`https://asiacrypt.iacr.org/2022/`

2020 **On ideal lattices in multicubic fields**, avec T. Plantard et W. Susilo, Number-Theoretic Methods in Cryptology (NuTMiC) 2019
`http://nutmic2019.imj-prg.fr/`

2017 **Efficient Leak Resistant Modular Exponentiation in RNS**, avec C. Negre et T. Plantard, ARITH 2017: 156-163

Articles courts de conférences internationales avec comité de relecture

2016 **Efficient Randomized Regular Modular Exponentiation using Combined Montgomery and Barrett Multiplications**, avec C. Negre et T. Plantard, SECRYPT 2016: 368-375 ; DOI:10.5220/0005998503680375

Preprints

- A. Lesavourey, K. Fukushima, T. Plantard et A. Sipasseuth (2024). *Diagonally dominant matrices for cryptography.*

- A. Lesavourey, T. Plantard et W. Susilo (2022). *Computing roots of polynomials over number fields using complex embeddings.*
  Code en support `https://github.com/AndLesav/nf_polynomial_roots`.

- A. Lesavourey, T. Plantard et W. Susilo (2021). *On the Short Principal Ideal Problem over some real Kummer fields.*
  Code en support `https://github.com/AndLesav/spip-on-kummer`
  Soumis à Mathematical Cryptology (en déc. 2021).

Notes et travaux en cours

- R. Cramer, A. Lesavourey, A. Pellet–Mary (2023). *On Module Lattices with Galois-Symmetries.*

- A. Lesavourey. *A note on the discriminant and prime ramification of some real Kummer extensions.*

.

Quelques présentations

mars 2023 **Computing roots in number fields**
Journées Nationales du Calcul Formel (JNCF 2023)

février 2023 **Calcul de racines de polynômes dans un corps de nombres**
Séminaire de l'équipe Lfant, Bordeaux

août 2022 **Covering radius and first minimum of diagonally dominant lattices for the max norm**
Number-Theoretic Methods in Cryptology (NutMic 2022)

mai 2022 **Vecteurs courts dans des réseaux idéaux ; études pratiques**
Séminaire Cryptologie & Sécurité, GREYC, Caen

novembre 2021 **Recovering short elements of ideal lattices**
EDUC research seminar

novembre 2020 **Retrouver des générateurs courts dans certaines extensions de Kummer réelles**
Journées Codages et Cryptographie (JC2)

avril 2020 **Générateurs courts dans certaines extensions de Kummer réelles**
Ecoles des Jeunes Chercheurs en Informatique Mathématique (EJCIM)

juin 2019 **On ideal lattices in multicubic fields**
Seconde conférence Number-Theoretic Methods in Cryptology (NutMic 2019)

juillet 2016 **Efficient Randomized Regular Modular Exponentiation using Combined Montgomery and Barrett Multiplications**
13ème conférence internationale Security and Cryptography (SECRYPT 2016)

Séjours et collaborations

juin–juillet 2019 **Invité de Jean-Claude Bajard**, *Sorbonne Université, LIP6*, Paris
Séjour dans le cadre du projet MACAO, `https://ssl.informatics.uow.edu.au/MACAO/`.
Discussions avec Antoine Joux and Fabrice Rouiller sur le calcul de racines dans des corps multicubiques.

Expérience pédagogique dans le supérieur

mars 2024 – mai 2024 **Equiv. M1, Cryptologie**, *Enseirb-Matmeca*, Bordeaux, (36h)
Chargé de TD, initiation à la cryptologie.

jan. 2024 – mars 2024 **Equiv. M1, Systèmes d'exploitation**, *Enseirb-Matmeca*, Bordeaux, (14h)
Chargé de TD/TP, implantation en C.

jan. 2023 – mai 2023 **M1, Cryptographie**, *Université Rennes 1*, Rennes, (16h)
Chargé de TP, implantation grâce au logiciel SageMath de notions vues en cours (constructions cryptographiques, attaques).

sept. 2022 – déc. 2023 **M2, Bases de cryptographie**, *Cyberschool, Université Rennes 1*, Rennes, (16h)
Chargé de TP, implantation en SageMath ou en C de schémas et attaques liées.

sept. 2022 – oct. 2022 **M2, Réseaux euclidiens et cryptographie**, *Université Rennes 1*, Rennes, (6h)
Chargé de TD/TP, notions algorithmiques des réseaux euclidiens.

jan. 2022 – mai 2022 **M1, Cryptographie**, *Université Rennes 1*, Rennes, (16h)
Chargé de TP, implantation grâce au logiciel SageMath de notions vues en cours (constructions cryptographiques, attaques).

sept. 2021– nov. 2021 **L1, Introduction à la programmation (Java)**, *Université Rennes 1*, Rennes, (20h)
Chargé de TD, Notions élémentaires de programmation impérative, et du langage Java.

sept. 2021– oct. 2021 **M1 Meef, Algorithmique**, *Université Rennes 1*, Rennes, (10h)
Chargé de TD/TP, Algorithmique pour des étudiants préparant le CAPES d'informatique.

mars – mai 2020 et 2021 **L2, Knowledge Based Engineering**, *University of Wollongong*, Wollongong, 2x(40h)
Chargé de TP, Introduction aux bases de données et à l'utilisation de procédures de traitement de données, comme les réseaux de neurones, les arbres de décision ou le minage de règles.

mars 2019 – mai 2019 **L1, Problem Solving**, *University of Wollongong*, Wollongong, (36h)
Chargé de TD, Initiation à la résolution algorithmique.

sept. 2015 – mars 2016 **CPGE, Khôlles (MPSI et PSI)**, *Lycée Camille Julian*, Bordeaux, (60h)
Préparation aux oraux de mathématiques.

Charges administratives et collectives

2019 **Séminaire MACAO à Wollongong**, Coorganisation avec Thomas Plantard, Dung Duong, Arnaud Sipasseuth et Quoc-Huy Le.
J'ai participé à l'organisation scientifique (discussions sur le contenu et la forme) et logistique (réservation de salles, nourriture, etc...) du séminaire.