photo.png

Andrea Lesavourey

Academic cursus

Post-doctoral fellow

Septembre 2021 - present, Univ Rennes, CNRS, IRISA.

PhD Student

October 2017 - June 2021, University of Wollongong, Australia.

- *Lattices for a post-quantum cryptography*, supervised by Pr Willy Susilo and Dr Thomas Plantard

Master 1 in Cryptology

2015 - 2016, University of Bordeaux, France

- Master Research thesis supervised by Christophe Negre and Thomas Plantard : *Randomization in RNS and Leak Resistant Arithmetic*
  Abstract : The Leak Resistant Arithmetic proposed to randomize an exponentiation procedure in RNS via Montgomery's multiplication. We study a modification of this approach by not clearing the mask during the procedure in order to save two Montgomery's multiplications at each loop and improve the level of randomization.

- Teaching followed : Programming (C), Arithmetic, Complexity Theory, Information Theory, Elliptic Curves (use of Pari/GP), Cryptology, Algorithmic Calculus (use of SageMaths), Introduction to Diophantine Approximations

Master Degree in Pure Mathematics

2015, University of Bordeaux, France

- Master Thesis supervised by Pierre Parent : *Théorème de Chabauty et version effective de Coleman*
  Abstract : Faltings proved in 1983 that every curve of genus strictly greater than 1 has only a finite number of rational points. Sadly, his proof cannot be made efficient. But Coleman improved the intermediate result of Chabauty (40's), which use some p-adic argument, to obtain a good bound for the number of rational points in special cases.

- Teaching followed : Algebraic Geometry, Introduction to p-adic numbers, Computational Number Theory (use of Pari/GP), Group cohomology, Geometry

2012, University of Bordeaux, France

- Master Thesis supervised by Valentin Féray : *Formalisation de la jonglerie et concepts mathématiques liés*
  Abstract : We study siteswaps, which can be defined as one way to juggle and can be described mathematically. In particular, we use different representations of these objects and study them from a combinatorial point of view.

Master Degree in Teaching of Mathematics

2012 - 2014, University of Bordeaux, France

- Agrégation de Mathématiques, option Probabilités et Statistiques

Bachelor Degree in Pure Mathematics

2008 - 2011, University of Bordeaux, France

Research and academic activities

Journal papers

- Andrea Lesavourey, Thomas Plantard, and Willy Susilo. "Short Principal Ideal Problem in multicubic fields". *Journal of Mathematical Cryptology* 14.1 (2020): 359-392. `https://doi.org/10.1515/jmc-2019-0028`

Conference papers

- Andrea Lesavourey, Thomas Plantard, Willy Susilo: *On ideal lattices in multicubic fields*, Accepted to Number-Theoretic Methods in Cryptology (NutMic) 2019, `http://nutmic2019.imj-prg.fr/`.
- Andrea Lesavourey, Christophe Negre, Thomas Plantard: *Efficient Leak Resistant Modular Exponentiation in RNS*. ARITH 2017: 156-163.
- Andrea Lesavourey, Christophe Negre, Thomas Plantard: *Efficient Randomized Regular Modular Exponentiation using Combined Montgomery and Barrett Multiplications*. SECRYPT 2016: 368-375.

Current activities

- Andrea Lesavourey, Thomas Plantard, Arnaud Sipasseuth, *Lattices defined by diagonally dominant matrices*, Submitted.
- Andrea Lesavourey, Thomas Plantard, Willy Susilo, *On the Short Principal Ideal Problem over some real Kummer fields*, Submitted to the journal *Mathematical Cryptology*.

- Andrea Lesavourey, Thomas Plantard, Willy Susilo, *Roots of polynomials in number fields: computation through complex embeddings*, To be submitted.

Collaboration visits

June/July 2019, Sorbonne University, LIP6
Guest of Jean-Claude Bajard within the MACAO program, `https://ssl.informatics.uow.edu.au/MACAO/`.
Discussions with Antoine Joux and Fabrice Rouiller on the computation of cube roots in multicubic fields.

Organisations

November 2019, MACAO workshop in Wollongong
`https://ssl.informatics.uow.edu.au/MACAO/workshop_2019.html`.

Reviews

ACISP 2020

Teaching

Tutoring in Computer Science

Autumn Session 2020, University of Wollongong
Knowledge and Information Engineering (ISIT219)

Tutoring in Computer Science

Autumn Session 2019, University of Wollongong
Problem Solving (CSIT113)

Highschool Mathematics Teacher

Septembre 2016 - June 2017, Lycée Malherbe of Caen, France
Year 10 and Year 11 with specialisation in science

Tutoring in Mathematics

2015-2016, University of Bordeaux
General Mathematics for Bachelor students (50 hours)

Tutoring in Mathematics

2014-2015, University of Bordeaux
General Mathematics for Bachelor students (35 hours)

Preparatory School Examiner

2014-2015, Camille Jullian Highschool, Bordeaux
Oral Examiner for students training to enter Engineering Schools
Linear Algebra, Real Analysis (60 hours)

Private tutoring

From secondary school to bachelor students

References

University of Wollongong, Australia

Dr Thomas Plantard
Senior Research Fellow
Institute of Cybersecurity and Cryptology
School of Computing and Information Technology
thomaspl@uow.edu.au

Pr Willy Susilo
Professor and Head of School
Institute of Cybersecurity and Cryptology
School of Computing and Information Technology
wsusilol@uow.edu.au

University of Perpignan, France

Dr Christophe Negre
Associate Professor
Digits Architectures Logiciels Informatique
christophe.negre@univ-perp.fr