Alexandre Wallet

Ph. D. in computer science

(+33) 637572324
wallet.alexandre@gmail.com
http://awallet.github.io

Current position

Post-doctoral researcher, NTT Secure Platform Laboratories, Tokyo.
Post-quantum cryptology, lattices, algebraic number theory

Scientific interests

- Cryptology
- Computer algebra
- Algebraic geometry
- Computer security
- Algorithmic
- Number theory

Education

2013 – 2016 **Ph. D. in computer science**, Université Pierre et Marie Curie, Sorbonne, Paris.
Thesis: *"Le problème de décomposition de points dans les variétés Jacobiennes"*
Advisor: J-C. Faugère, Supervisor: V. Vitse

September 2012 **Master degree in fundamental mathematics**, École Normale Supérieure de Lyon.
Memoir: *"Éléments de K-théorie des C*-algèbres"*.

July 2011 **"Agrégation" in mathematics**, prepared at Université Claude Bernard, Lyon 1.
Highly selective nation-wide qualification in mathematics at post-graduate level

September 2010 **Master degree in applied mathematics**, Université Claude Bernard, Lyon 1.
Memoir: *"Introduction au problème du logarithme discret"*.

Supervision of students

April 2018, 4 months — Thanh Huyen Nguyen, research internship at ENS de Lyon.
In collaboration with E. Kirshanova and D. Stehlé

Journal articles

Submitted (Revisions) — On the smoothing parameter and last minimum of random orthogonal lattices, *with E. Kirshanova, T. H. Nguyen and D. Stehlé, Design, Codes and Cryptography (DCC)*.

Published — The Point Decomposition Problem in the divisor class group of hyperelliptic curves: toward efficient computations in even characteristic, *with J-C. Faugère, Design, Codes and Cryptography (DCC)*.

Peer-reviewed conferences

Accepted — One Bit is All It Takes: A Devastating Timing Attack on BLISS's Non-Constant Time Sign Flips, *with M. Tibouchi, International Workshop on Mathematical Cryptology, MATHCRYPT 2019*.

Published — On the Ring-LWE and Polynomial-LWE problems, *with M. Rosca and D. Stehlé, International Conference on Cryptology and Information Security, EUROCRYPT 2018*.

Published — Improved Sieving on Algebraic Curves, *with V. Vitse, International Conference on Cryptology and Information Security in Latin America, LATINCRYPT 2015*.

Selected presentations

Algebraic aspects of "Learning with errors"

11 September 2018	Cryptology and security seminar NTT, Tokyo, Japan.
15 June 2018	CCA Seminar, INRIA Center, Paris, France.
20 October 2017	Lattice Meetings, ENS Lyon, LIP, France.

Discrete logarithm over algebraic curves

17 May 2017	ECO/ESCAPE Seminar, LIRMM, Montpellier, France.
24 April 2017	National days of Coding et Cryptograpy, La Bresse, France.
14 March 2017	National days of the Mathematical Computer Science society, LIRMM, Montpellier, France.
25 August 2015	LATINCRYPT 2015, *Guadalajara, Mexico.*

Professional and scientific experiences

2017 – 2019 **Post-doctoral researcher**, *ENS de Lyon*, France, Supervisor: D. Stehlé.
Topics: post-quantum cryptology, lattices, algebraic number theory

2012 – 2013 **Maths teacher**, *Parc Chabrières Highschool*, Oullins, France.

May 2012, 4 months **Research internship**, *Camille Jordan Institute*, Lyon, France.
Topic: K-theory for C^*-algebras and non-commutative index theory. Supervisor: D. Perrot

May 2010, 4 months **Research internship**, *Camille Jordan Institute*, Lyon, France.
Topic: Introduction to the discrete logarithm problem. Supervisor: C. Delaunay

Teachings

2018 2nd semester **Teacher assistant in Computer Science**, École Normale Supérieure de Lyon, 69.
- Tutorials in Computer Algebra in master degree
- Evaluation of undergraduate interns

2013 – 2016 **Teacher assistant in bachelor of computer science**, Université Pierre et Marie Curie, Sorbonne, Paris.
- 3rd year: Introduction to Cryptology
- 2nd year: Scientific computations , Types and Data structures in C, Machine Architecture and Representation , Development and compilation environment , Discrete structures
- 1st year: Introduction to programming with Python

Other Master SFPN of Université Pierre et Marie Curie, LIP6, specialization in Computer security and Cryptology.
- Elaboration of exams
- Realization of a Side-Channel Attack (SCA) on a faulty AES implementation

2012 – 2013 **Maths Teacher**, *Parc Chabrières Highschool*, Oullins, 69.
- Full responsibility of two classes for an entire year: lectures and exercises, homeworks, exams.
- Trimestrial meetings with the team of teachers and the hierarchy.
- Relationships with parents, orientation of students.

Skills

Programming	Basic skills in C, C++, Assembler (8051, x86, MIPS), Python, Shell
Computer algebra	Magma, Maple, Sage
Environments	Windows, Linux
Other	Basic skills in reverse-engineering, web-security fault exploitations and injections.

Languages

- French: native
- English: full professionnal proficiency
- German: school level (B1)
- Japanese: school level (B1)
- Russian: school level (A2)