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**, Sorbonne, Université Pierre et Marie Curie (Paris 6).
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"*.

Journal articles

To appear One Bit is All It Takes: A Devastating Timing Attack on BLISS's Non-Constant Time Sign Flips, *with M. Tibouchi, Journal of Mathematical Cryptology*.

2019 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)*.

2017 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

2020 MODFALCON: compact signatures based on module-NTRU lattices, *with C. Chuengsatiansup, T. Prest, D. Stehlé and K. Xagawa, AsiaCCS 2020*.

2020 Uprooting the FALCON tree? How to recover secret keys from Gram-Schmidt norms, *with P. A. Fouque, P. Kirchner, M. Tibouchi and Y. Yu, EUROCRYPT 2020*.

2019 An LLL algorithm for module lattices, *with C. Lee, A. Pellet--Mary, and D. Stehlé, ASIACRYPT 2019*.

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

2018 On the Ring-LWE and Polynomial-LWE problems, *with M. Rosca and D. Stehlé, EUROCRYPT 2018*.

2015 Improved Sieving on Algebraic Curves, *with V. Vitse, LATINCRYPT 2015*.

Selected presentations

Invited talk: "Mod-NTRU trapdoors and applications"

29 April 2020 Workshop "Lattices: From Theory to Practice", Simons Institute for the Theory of Computing, Berkeley, USA.

Side-channel against BLISS

18 August 2019 MATHCRYPT, Santa Barbara, USA.

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

Supervision of students

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

Teachings

2018 2nd semester **Teacher assistant in Computer Science**, École Normale Supérieure de Lyon.
Tutorials in master's degree (with exams), evaluation of undergraduate interns

2013 – 2016 **Teacher assistant in bachelor of computer science**, Sorbonne UPMC Paris 6.
Tutorials from first to third year, elaboration and correction of exams

Other Master SFPN at UPMC Paris 6, specialization in Computer security and Cryptology.
Elaboration of exams, tutorial on side-channel attacks against AES

2012 – 2013 **Maths Teacher**, *Parc Chabrières Highschool*, Oullins.
Full responsibility of two classes for a year

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)