Alexandre Wallet

Ph. D. in computer science

(+33) 637572324
alexandre.wallet@inria.fr
http://awallet.github.io

Current position

Researcher, Inria, Rennes Bretagne-Atlantique center.

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

2021 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

2022 Shorter Hash-and-Sign Lattice-Based Signatures, *with T. Espitau, M. Tibouchi and Y. Yu, CRYPTO 2022*.

2022 Mitaka: A Simpler, Parallelizable, Maskable Variant of Falcon, *with T. Espitau, P.A. Fouque, F. Gérard, M. Rossi, A. Takahashi, M. Tibouchi and Y. Yu, EUROCRYPT 2022*.

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

2020 Key Recovery from Gram-Schmidt Norm Leakage in Hash-and-Sign Signatures over NTRU Lattices, *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.*

Invited talks

7 October 2022 *Mitaka: a simpler, parallelizable, maskable variant of Falcon*, C2 seminar, Paris.

21-25 March 2022 *Do not overstretch NTRU-like problems*, workshop on Post-quantum cryptanalysis, Birmingham University.

29 April 2020 *Mod-NTRU trapdoors and applications*, workshop "Lattices: From Theory to Practice", Simons Institute for the Theory of Computing, Berkeley, USA.

Professional and scientific experiences

02/2019 – 11/2020 **Post-doctoral researcher**, *NTT Secure Platform Laboratories, Tokyo*, Japan, Supervisor: M. Tibouchi.
Topics: applied post-quantum cryptography, algorithmic number theory

01/2017 – 12/2018 **Post-doctoral researcher**, *ENS de Lyon*, France, Supervisor: D. Stehlé.
Topics: post-quantum cryptology, lattices, algebraic number theory

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

Since April 2022 Léo Ackermann, Ph.D. student at IRISA, Rennes.
Co-supervised with Adeline Roux-Langlois

Since October 2021 Thi Thu Quyen Nguyen, Ph.D. student at IRISA, Rennes.
Co-supervised with Adeline Roux-Langlois

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