Alexandre Wallet

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

Situation actuelle

Chargé de recherche, Inria, Centre de Rennes Bretagne-Atlantique.
Cryptographie post-quantique appliquée, théorie algorithmique des nombres, réseaux euclidiens

Intérêts scientifiques

- Cryptologie
- Calcul formel
- Géométrie algébrique
- Sécurité informatique
- Algorithmique
- Théorie des nombres

Formation

2013 – 2016 **Doctorat d'informatique**, Sorbonne, Université Pierre et Marie Curie (Paris 6).
Thèse: *Le problème de décomposition de points dans les variétés Jacobiennes"*
Directeur: J-C. Faugère, Encadrante: V. Vitse.

Septembre 2012 **Master de mathématiques fondamentales**, École Normale Supérieure de Lyon.
Encadré par D. Perrot. Mémoire: *"Éléments de K-théorie des C*-algèbres"*.

Juillet 2011 **Agrégation de mathématiques**, préparée à l'Université Claude Bernard, Lyon 1.

Septembre 2010 **Master de mathématiques appliquées**, Université Claude Bernard, Lyon 1.
Encadré par C. Delaunay. Mémoire: *"Introduction au problème du logarithme discret"*.

Articles de journaux

2021 One Bit is All It Takes: A Devastating Timing Attack on BLISS Non-Constant Time Sign Flips, *avec Mehdi Tibouchi, Journal of Mathematical Cryptology*.

2019 On the smoothing parameter and last minimum of random orthogonal lattices, *avec E. Kirshanova, T. H. Nguyen, et 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, *avec J-C. Faugère, Design, Codes and Cryptography (DCC)*.

Articles de conférences

2023 On Gaussian sampling, smoothing parameter and application to signatures, *avec T. Espitau, et Y. Yu, ASIACRYPT 2023*.

2023 Antrag: Annular NTRU Trapdoor Generation, *avec S. Chao, T. Espitau, Q. Nguyen et M. Tibouchi, ASIACRYPT 2023*.

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

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

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

2020 Key Recovery from Gram-Schmidt Norm Leakage in Hash-and-Sign Signatures over NTRU Lattices, *avec P. A. Fouque, P. Kirchner, M. Tibouchi et Y. Yu, EUROCRYPT 2020*.

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

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

2018 On the Ring-LWE and Polynomial-LWE problems, *avec M. Roşca et D. Stehlé, EUROCRYPT 2018* .

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

Sélection de présentations

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.

Expériences professionnelles et scientifiques

02/2019 – 11/2020 **Post-doctorant**, *NTT Secure Platform Laboratories, Tokyo*, supervisé par M. Tibouchi.
Cryptographie post-quantique appliquée, théorie algorithmique des nombres, réseaux euclidiens

01/2017 – 12/2018 **Post-doctorant**, *ENS de Lyon*, supervisé par D. Stehlé.
Réseaux euclidiens, cryptographie post-quantique, théorie algébrique des nombres

09/2012 – 08/2013 **Enseignant de mathématiques**, *Lycée Parc Chabrières*, Oullins.

Mai 2012, 4 mois **Stage de recherche**, *Institut Camille Jordan*, Lyon, encadré par D. Perrot.
Sujet: K-théorie des C^*-algèbres, Géométrie non commutative.

Mai 2010, 4 mois **Stage de recherche**, *Institut Camille Jordan*, Lyon, encadré par C. Delaunay.
Sujet: Problème du logarithme discret.

Supervision of students

Depuis Avril 2022 Léo Ackermann, doctorant, IRISA, Rennes.
co-encadrée with Adeline Roux-Langlois

Depuis Octobre 2021 Thi Thu Quyen Nguyen, doctorante, IRISA, Rennes.
co-encadrée avec Adeline Roux-Langlois

April 2018, 4 months Thanh Huyen Nguyen, stage de recherche à l'ENS de Lyon.
co-encadrée avec E. Kirshanova and D. Stehlé

- Allemand: scolaire (B1)