

Alexandre Wallet

Docteur en informatique

☎ (+33) 637572324
✉ wallet.alexandre@gmail.com
🌐 <http://awallet.github.io>

Situation actuelle

Post-doctorant, NTT Secure Platform Laboratories, Tokyo.
Cryptographie post-quantique, réseaux euclidiens, théorie algébrique des nombres

Intérêts scientifiques

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

Formation

- 2013–2016 **Doctorat d’informatique**, 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”*.

Encadrements d’étudiants

- Avril 2018, 4 mois Thanh Huyen Nguyen, stage de recherche, ENS de Lyon.
Co-encadrée avec E. Kirshanova et D. Stehlé.

Articles de journaux

- À paraître 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)*.
- Publié 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

- Publié An LLL algorithm for module lattices, avec A. Pellet-Mary, C. Lee et D. Stehlé, *International Conference on Cryptology and Information Security, ASIACRYPT 2019*.
Sélectionné pour une version étendue dans le Journal of Cryptology.
- Publié One Bit is All It Takes: A Devastating Timing Attack on BLISS’s Non-Constant Time Sign Flips, avec M. Tibouchi, *International Workshop on Mathematical Cryptology, MATH-CRYPT 2019*.
- Publié On the Ring-LWE and Polynomial-LWE problems, avec M. Roşca et D. Stehlé, *International Conference on Cryptology and Information Security, EUROCRYPT 2018*.
- Publié Improved Sieving on Algebraic Curves, avec V. Vitse, *International Conference on Cryptology and Information Security in Latin America, LATINCRYPT 2015*.

Sélection de présentations

Side-channel sur BLISS

18 Août 2019 MATHCRYPT, Santa Barbara, USA.

Aspects algébriques de “Learning with errors”

11 Septembre 2018 Séminaire de cryptologie et sécurité, NTT Tokyo, Japon.

15 Juin 2018 Séminaire CCA, Centre INRIA de Paris, France.

20 Octobre 2017 Lattice Meetings, ENS Lyon, LIP, France.

Logarithme discret sur courbes algébriques

17 Mai 2017 Séminaire ECO/ESCAPE, LIRMM, Montpellier.

24 Avril 2017 Journées Codage et Cryptographie, La Bresse.

14 Mars 2017 Journées du GDR-IM, LIRMM, Montpellier. Poster.

25 Août 2015 LATINCRYPT 2015, Guadalajara, Mexique.

Expériences professionnelles et scientifiques

2017 – 2019 **Post-doctorant**, *ENS de Lyon*, supervisé par D. Stehlé.

Thèmes: réseaux euclidiens, cryptographie post-quantique, théorie algébrique des nombres

2012 – 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.

Activités d'enseignement

2e semestre 2018 **Enseignant en informatique**, École Normale Supérieure de Lyon, 69.

- Travaux dirigés de Calcul Formel, M1

- Évaluateur des stages de L3

2013 – 2016 **Moniteur en licence d'informatique**, Université Pierre et Marie Curie, Paris 6.

La charge d'enseignement comprend l'élaboration et la correction des examens.

- L3: Introduction à la Cryptologie (TD/TP)

- L2: Calcul Scientifique (TP), Types et Structures de données en C (TP), Architecture Machine et Représentation (TP), Environnement de Développement (TP), Structures discrètes (TP)

- L1: Initiation à la programmation avec Python (TP)

Autres activités Master SFPN de l'Université Pierre et Marie Curie, LIP6, mention Sécurité-Cryptologie.

- Elaboration d'examens

- TP “Attaque par canaux cachés sur une implémentation AES”

2012 – 2013 **Enseignant de mathématiques**, *Lycée Parc Chabrières*, Oullins, 69.

Classes de seconde.

Compétences

Langages C, C++, Assembleur (8051, x86, MIPS), Python, Shell

Calcul Formel Magma, Maple, Sage

Environnements Windows, Linux

Autres Bases de reverse-engineering et exploitation de failles de sécurité (buffer overflow, injection shellcode,...).

Langues

- Français: natif
- Anglais: professionnel
- Allemand: scolaire (B1)
- Japonais: scolaire (B1)
- Russe: scolaire (A2)