

# Alexandre Wallet

Docteur en informatique, agrégé de mathématiques

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

## Situation actuelle

**Chargé de recherche**, Inria, Centre de Rennes Bretagne-Atlantique.  
Cryptographie post-quantique, 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

- À paraître 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

- 2020 MODFALCON: compact signatures based on module-NTRU lattices, avec C. Chuengsatiansup, T. Prest, D. Stehlé et K. Xagawa, *AsiaCCS 2020*.
- 2020 Uprooting the FALCON tree? How to recover secret keys from Gram-Schmidt norms, 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

**Exposé invité:** “Mod-NTRU trapdoors and applications”

29 avril 2020 Atelier “Lattices: From Theory to Practice”, Simons Institute for the Theory of Computing, Berkeley, USA.

**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

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

01/2017 – 12/2018 **Post-doctorant**, *ENS de Lyon*, supervisé par D. Stehlé.  
Thèmes: 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.

---

## Encadrements d'étudiants

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

---

## Activités d'enseignement

2e semestre 2018 **Enseignant en informatique**, École Normale Supérieure de Lyon.  
Chargé de TD en M1, évaluateur des stages de L3

2013 – 2016 **Moniteur en licence d'informatique**, Université Pierre et Marie Curie, Paris 6.  
Chargé de TD/TP de la L1 à la L3

Autres activités Master SFPN de l'Université Pierre et Marie Curie, LIP6, mention Sécurité-Cryptologie.  
Elaboration d'examens et de TP (attaques par canaux auxiliaires sur AES)

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

---

## 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)