Curriculum Vitae

Alexandre Wallet

Table des matières

1 Renseignements généraux

Date de naissance : 3 Février 1986
Nationalité : Française

Adresse email : wallet.alexandre@gmail.com
Page personnelle : http://awallet.github.io/

Qualifications MCF : sections 25, 26, 27

Intérêts scientifiques

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

Situation actuelle

Depuis Février 2019 : **Post-doctorant**, NTT Secure Platform Laboratories, Tokyo.
Cryptographie post-quantique, attaque par canaux auxiliaires, réseaux euclidiens (algébriques).

2 Expériences scientifiques et professionnelles

01/2017 – 12/2018 : **Post-doctorant**, Laboratoire de l'Informatique du Parallélisme (LIP), équipe AriC, ENS Lyon
Cryptographie post-quantique, réseaux euclidiens, théorie algorithmique des nombres.

10/2013 – 12/2016 : **Doctorant**, Laboratoire d'Informatique de Paris 6 (LIP6), équipe PolSys, INRIA, UPMC.
Théorie algorithmique des nombres, cryptographie sur courbes elliptiques.

09/2012 – 08/2013 : **Enseignant en mathématiques**, Lycée du Parc Chabrière, Oullins (69).

2012 : **Stage de recherche**, Institut Camille Jordan (ICJ), UCBL, encadré par Denis Perrot.
Mémoire : *Éléments de K-théorie des C^*-algèbres.*
Algèbres d'opérateurs, géométrie non-commutative.

2010 : **Stage de recherche**, Institut Camille Jordan (ICJ), UCBL, encadré par Christophe Delaunay.
Mémoire : *Introduction au problème du logarithme discret.*
Logarithme discret et cryptographie.

3 Formation

Décembre 2016 : **Doctorat en informatique**, Université Pierre et Marie Curie, Paris 6.
Intitulé : *Le problème de décomposition de points dans les variétés Jacobiennes.*
Directeur : Jean-Charles Faugère.
Encadrante : Vanessa Vitse.
Rapporteurs : David Lubicz, François Morain.
Examinateurs : Stef Graillat, Mohab Safey-el-Din.

Septembre 2012 : **Master en mathématiques fondamentales**, École Normale Supérieure de Lyon.

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

Septembre 2010 : **Master de mathématiques appliquées**, Université Claude Bernard, Lyon 1.

4 Auditions, classements

En Mai 2019, j'ai été classé 3e au concours pour un poste de maître de conférence à l'Université de Versailles Saint-Quentin, rattaché à l'équipe de cryptographie du Laboratoire de Mathématiques de Versailles (LMV).

5 Publications

Dans mon domaine de recherche, les publications scientifiques sont majoritairement au format d'articles de conférence. En particulier, toutes les conférences imposent une étape de relecture par les pairs ; les plus sélectives sont EUROCRYPT, CRYPTO, ASIACRYPT et TCC. L'usage est de ranger les auteurs par ordre alphabétique.

Conférences internationales avec comité de sélection

2020 : *MODFALCON: compact signatures based on module-NTRU lattices*, C. Chuengsatiansup, T. Prest, D. Stehlé, A. Wallet, K. Xagawa, AsiaCCS 2020 **(à paraître)**.

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

2019 : *An LLL algorithm for module lattices*, C. Lee, A. Pellet--Mary, D. Stehlé, A. Wallet, ASIACRYPT 2019. Classé dans les trois meilleurs articles de la conférence, invité pour une version étendue dans le *Journal of Cryptology*.

2018 : *On the Ring-LWE and Polynomial-LWE problems*, M. Roșca, D. Stehlé, A. Wallet, EUROCRYPT 2018.

2015 : *Improved Sieving over Algebraic Curves*, V. Vitse, A. Wallet, LATINCRYPT 2015.

Journaux internationaux

2019 : *On the smoothing parameter and last minimum of random orthgonal lattices*, E. Kirshanova, H. T. Nguyen, D. Stehlé, A. Wallet. Designs, Codes and Cryptography (DCC).

2017 : *The Point Decomposition Problem in the divisor class group of hyperelliptic curves: toward efficient computations in even characteristic*, J-C. Faugère, A. Wallet. Designs, Codes and Cryptography (DCC).

A paraître :

- *One Bit is All It Takes: a devastating timing attack agains BLISS non constant-time sign flips*, M. Tibouchi, A. Wallet. Journal of Mathematical Cryptology.

Atelier international, avec comité de sélection

2019 : *One Bit is All It Takes: a devastating attack against BLISS non constant-time sign flips*, M. Tibouchi, A. Wallet, MATHCRYPT 2019, affilié à la conférence CRYPTO 2019.

Prépublications, rapports, ou archives

2020 : *Lattice analysis of the MiNTRU problem*, C. Lee, A. Wallet, archive ePrint IACR.

6 Collaborations en cours

- *Avec Mehdi Tibouchi (NTT Corporation, Tokyo) :*
  Développement d'un utilitaire pour l'analyse du caractère "temps constant" des implémentations cryptographiques. Il sera à terme intégré à SUPERCOP, un outil libre permettant de tester le comportement d'algorithmes cryptographiques sous différentes architectures matérielles, options de compilation, optimisation, ... Nous espérons démontrer l'intérêt de notre utilitaire en identifiant, exploitant et corrigeant des fuites dans les implémentations proposées pour les candidats participant à l'appel à standardisation post-quantique du NIST.
- *Avec E. Kirshanova (Université de Kaliningrad) et A. Pellet--Mary (KU Leuven) :*
  Travaux généraux sur les réseaux construits à partir de modules sur des anneaux d'entiers algébriques : étude des aspects algorithmiques en présence d'un oracle pour un sous-problème, et cryptanalyse des problèmes de types Learning With Errors formulés pour ces réseaux. Article en cours de rédaction.

- *Avec Thomas Espitau (NTT Corporation, Tokyo) :*
  Thomas et moi tentons d'unifier les concepts de la théorie cryptographique des réseaux euclidiens à travers la théorie d'Arakelov des courbes arithmétiques telle que développée par Bost, Gillet et Soulé. Nous espérons obtenir une théorie plus uniforme et des outils mieux adaptés à l'analyse d'algorithmes récemment présentés pour les modules projectifs.

Projet CNRS-RFFI Je suis collaborateur externe sur un projet de recherche porté par Elena Kirshanova (Université de Kaliningrad) et proposé pour financement au partenariat entre le CNRS et le Fond Russe pour la Recherche Fondamentale (RFFI).

7 Diffusions scientifiques et autres activités

Communications internationales

Exposé invité :

24 Avril 2020 : *"Mod-NTRU trapdoors and applications"*, atelier "Lattices: From Theory to Practice" Simons Institute for the Theory of Computing, Berkeley, Etats-Unis. (Vidéo)

Exposés en conférence :

Mes contributions les plus récentes sont partagées avec des doctorants, à qui revient en général l'opportunité de présenter les résultats. J'ai exposé d'autres mes travaux lors des conférences où ils ont été publiés :

18 Août 2019 : *One Bit is All It Takes : a devastating attack against BLISS' non constant-time sign flips*, MATHCRYPT 2019, Santa Barbara, Etats-Unis.

25 Août 2015 : *Improved Sieving over Algebraic Curves*, LATINCRYPT 2015, Guadalajara, Mexique.

Communications nationales

J'ai présenté certains de mes résultats de thèse et de post-doctorat sous forme de **posters** lors de mes participations aux Journées Nationales du groupe de travail d'Informatique-Mathématique (GDR-IM). J'ai aussi donné **un court exposé** à l'édition 2017 des Journées Nationales du groupe de travail Codage et Cryptographie (C2).

Séminaires (sélections)

Nos résultats sur les variantes algébriques de Learning With Errors à EUROCRYPT ont suscité un vif intérêt de la communauté. J'ai eu l'occasion de le présenter dans **des exposés longs** à de nombreux séminaires en France et à l'étranger. La liste ci-dessous recense certains de ces exposés. D'autres exposés longs plus anciens concernent mes travaux de thèse.

Internationaux :

26 Août 2019 : INTEL, San Diego.

16 Janvier 2019 : Cryptography and security seminar, PQ Shield, Mathematical Institute of Oxford University.

11 Septembre 2018 : Cryptography seminar, NTT Secure Platform Laboratories, Tokyo.

Nationaux :

15 Juin 2018 :	Séminaire CCA de l'INRIA, Centre INRIA de Paris.
20 Octobre 2017 :	Lattice meetings, ENS Lyon.
17 Mai 2017 :	Séminaire de l'équipe ECO/ESCAPE, LIRMM, Montpellier.
8 Décembre 2016 :	Séminaire GTBAC, Télécom ParisTech.

Activités administratives et d'organisation

- Automne 2018 : pendant mon post-doctorat à l'ENS de Lyon, j'ai participé à l'organisation de l'édition 2018 des Journées C2.
- Juillet 2017 : j'ai fait partie du comité d'harmonisation pour l'obtention du label HRS4R (Human Ressource Strategies For Researchers) à l'ENS de Lyon, en tant que représentant des doctorants et post-doctorants.
- Septembre 2015 : j'ai été membre du comité d'organisation de la conférence internationale Cryptographic Hardware and Embedded Systems (CHES), à Saint-Malo.

Comités de relectures

- Printemps 2020 : membre du comité de programme de la conférence bi-annuelle de théorie algorithmique des nombres ANTS.

La communauté publiant essentiellement en conférence, une activité habituelle des chercheurs du domaine concerne l'évaluation des soumissions. Je suis régulièrement relecteur externe pour les conférences de l'IACR, particulièrement CRYPTO, EUROCRYPT, et ASIACRYPT. J'ai participé plus sporadiquement au processus pour d'autres conférences du domaine comme TCC, ainsi que pour la conférence bi-annuelle de théorie algorithmique des nombres ANTS.

8 Encadrements scientifiques, enseignements

Encadrement d'un stage de recherche : *Huyen Nguyen*, étudiante du M2 informatique de l'ENS de Lyon, promotion 2018. Co-encadrée avec Elena Kirshanova (ENS Lyon) et Damien Stehlé (ENS Lyon) :

Sujet du stage : Etude des quantités fondamentales (minima successifs, paramètre de lissage) de réseaux orthogonaux à des matrices dont les entrées ont été tirées selon une distribution Gaussienne discrète. Cet encadrement a conduit à l'écriture d'un article en publication au journal *Designs, Codes and Cryptography*. Huyen poursuit actuellement son travail en thèse.

Encadrement scientifique non officiel : Cet encart correspond à des activités et responsabilités qui n'ont pas été pas clairement établies par des documents administratifs, mais dépassant nettement le cadre de discussions scientifiques épisodiques.

— *Miruna Roșca*, doctorante sous la direction de Damien Stehlé (ENS Lyon), en cotutelle avec BitDefender (Bucarest, Roumanie).

— *Emily Clément*, étudiante de master à Rennes, encadrée par Adeline Roux-Langlois (IRISA).

Activités d'enseignement

J'ai six années d'activité en tant qu'enseignant, partagée entre le secondaire et le supérieur, et les mathématiques et l'informatique. En post-doctorat, j'ai effectué 12 heures d'enseignement en première année du master d'informatique, et participé à l'évaluation des stages des étudiants de licence à l'ENS de Lyon. Pendant mes trois années de thèse, j'ai effectué 192 heures d'enseignement d'informatique en licence à l'UPMC (campus Jussieu), sur des thèmes variés. Avant ma thèse, j'ai eu la responsabilité de deux classes de secondes à temps plein pendant une année, en tant qu'enseignant agrégé de mathématiques. Ceci correspond essentiellement à un volume de 12 heures hebdomadaires sur 36 semaines, soit 432 heures (sans inclure les heures de formation pour les enseignants stagiaires). La Table 1 résume ce paragraphe.

Table 1 – **Résumé des activités antérieures d'enseignement**

Type	Niveau	Fonction	Volume horaire (équivalent TD)	Effectif
Encadrement d'un stage	M2	-	-	1
Calcul Formel	M1	TD	12 heures	~ 15
Introduction à la cryptologie	L3	TD/TP	63 heures	~ 25
Calcul scientifique	L2	TP	20 heures	~ 20
Types et structures de données en C	L2	TP	18 heures	~ 20
Architecture machine et représentation	L2	TP	21 heures	~ 20
Environnement de développement et compilation	L2	TP	30 heures	~ 25
Structures discrètes	L2	TP	21 heures	~ 15
Initiation à la programmation avec Python	L1	TP	19 heures	~ 25
Enseignant de mathématiques	2nde	-	432 heures (1 an)	~ 35
Formation enseignant (IUFM)	-	-	$\sim$ 168 heures	-