Curriculum Vitae

Alexandre Wallet

Table des matières

1 Renseignements généraux

Date de naissance : 3 Février 1986
Nationalité : Française

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

Intérêts scientifiques

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

Situation actuelle

Depuis 11/2020 : **Chargé de recherche**, Inria, Centre de Rennes Bretagne-Atlantique, équipe CAPSULE. Cryptographie appliquée, attaque par canaux auxiliaires, réseaux euclidiens (algébriques).

2 Expériences scientifiques et professionnelles

02/2019 – 10/2020 : **Post-doctorant**, NTT Secure Platform Laboratories, Tokyo, Japon.
Cryptographie sur les réseaux euclidiens, aspects side-channel, cryptographie appliquée.

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 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

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

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

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

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

2021 : *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.

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).

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

2021 : Mitaka: A Simpler, Parallelizable, Maskable Variant of Falcon, T. Espitau, A. Takahashi, M. Tibouchi, A. Wallet. Third NIST PQC Standardization Conference.

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

5 Diffusions scientifiques et autres activités

Communications internationales

Exposés invités :

21-25 Avril 2022 : *Do not overstretch NTRU-like problems*, atelier Post-Quantum Cryptography Workshop Université de Birmingham, Angleterre. (Présentation)

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)

Communications nationales

7 Octobre 2022 : *Mitaka : a simpler, parallelizable, maskable variant of Falcon*, Séminaire C2. Inria, Paris.

15 Juillet 2018 : *On variants of Ring-LWE and Polynomial-LWE problems*, atelier Séminaire C2. Inria, Paris.

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.

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 programme

- Automne 2022 : membre des comités de programme pour les conférences INDOCRYPT 2022 et ACNS2023.
- 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.

6 Collaborations, implications dans des projets

Projet ANR-ASTRID : je suis partenaire sur le projet AMIRAL (impliqué à 30%).
Le projet a pour objectif principal l'amélioration des signatures numériques fondées sur les réseaux Euclidiens, dans leurs aspects de déploiement concret ou dans leur utilisation pour instancier des primitives avancées (signatures à seuil, signatures aveugles, ...).

Projet AAP-BPi France : je suis collaborateur sur le projet HYPERFORM.
Ce projet porté par l'entreprise Idemia se concentre sur la mise en oeuvre et le développement industriel des solutions post-quantiques retenues par le NIST dans divers supports de communications : stockage de données, implémentations logicielles, architectures contraintes et embarquées, ...

7 Encadrements scientifiques, enseignements

Encadrement de doctorants :

— Depuis Novembre 2022 : *Léo Ackermann*, Université de Rennes 1 et ENS. Co-encadrée avec Adeline Roux-Langlois (Université de Caen).

— Depuis Novembre 2021 : *Thi Thu Quyen Nguyen*, CIFRE entre Université de Rennes 1 et Idemia. Co-encadrée avec Adeline Roux-Langlois.

Encadrement d'un stage de recherche :

— Avril-Août 2018 : *Huyen Nguyen*, étudiante du M2 informatique de l'ENS de Lyon, promotion 2018. Co-encadrée avec Elena Kirshanova et Damien Stehlé (ENS Lyon).

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, en cotutelle avec BitDefender (Bucarest, Roumanie).

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

Activités d'enseignement

Depuis Septembre 2020, je suis chargé d'enseignement à temps partiel (64 heures) à l'Ecole Polytechnique. J'interviens aussi (15 heures) dans le master de mathématiques de l'Université de Rennes 1 (parcours mathématiques de l'information et cryptographie) et le master 2 SIF de l'ISTIC (cours de cryptanalyse).