LIP, É.N.S. de Lyon,
46 allée d'Italie,
69364 Lyon Cedex 07
☎ *+33 (0)4 72 72 83 52*
+33 (0)6 38 61 92 22
✉ *fabrice.mouhartem@ens-lyon.org*
perso.ens-lyon.fr/fabrice.mouhartem/

Fabrice Mouhartem

Curriculum Vitæ

Études

2015–... **Doctorat**, *LIP, É.N.S. de Lyon*, Sous la direction de Benoît Libert et Damien Stehlé, Informatique Fondamentale/Cryptologie.
Cryptographie pour protéger la vie privée débloquant des fonctionnalités avancées.

2015 **Master**, *É.N.S. de Lyon*, Informatique Fondamentale.
Mention Bien

2013 **Licence**, *É.N.S. de Lyon*, Informatique Fondamentale.
Mention Bien

2010–2012 **CPGE**, *Lycée Charlemagne*, Paris, MPSI/MP*.

2010 **Baccalauréat Scientifique**.
Mention Bien

Expériences

Recherche et Enseignement

2016–... **Activité Complémentaire d'Enseignement**, *É.N.S. de Lyon*, Lyon, France.
Chargé de TD en *Architecture, Système et Réseaux* (L3), en *Complexité Algorithmique* (M1), et en *Cryptographie et Sécurité* (M1)

2015–2016 **Activité Complémentaire d'Enseignement**, *É.N.S. de Lyon*, Lyon, France.
Chargé de TD en *Théorie de la Programmation* (L3) et en *Complexité Algorithmique* (M1)

Mars 2016 **Accueil d'un stagiaire de troisième**, *É.N.S. de Lyon*, Lyon, France.
Accueil d'Aloys Delobel, élève au collège Notre-Dame-des-Minimes, pendant une semaine

Février-Juin 2015 **Stage de Recherche**, *É.N.S. de Lyon*, Lyon, France.
Construction d'un schéma de signature de groupe dynamique à l'aide de réseaux euclidiens

2014–2015 & 2013–2014 **Interrogations orales en CPGE**, *Lycée du Parc*, Lyon.
Colleur en 832 (MPSI)

Mai-Août 2014 **Stage de recherche**, *Katholieke Universiteit Leuven*, Louvain, Belgique.
Survol des algorithmes quasi-polynomiaux pour le logarithme discret sur des corps de petite caractéristique

Juin-Juillet 2013 **Stage de recherche**, *Inria/Irisa*, Rennes.
Améliorer l'efficacité énergétique des GPU par localité de valeurs entre threads

Concours de programmation

Novembre 2015 **Participation aux ACM ICPC SWERC**, *Université de Porto*, Portugal.
Novembre 2014 Concours d'algorithmique et de programmation en équipe, participation en C++

Novembre 2013 **Participation aux ACM ICPC SWERC**, *Université de Valence*, Espagne.

2013 **Finaliste prologin**, *EPITA, Paris*, France.
Concours d'algorithmique, participation en C++

Vulgarisation Scientifique

Avril 2017 **Origami mathématiques et informatique**, *É.N.S. de Lyon/MMI*, Lyon.
Après-midi d'ateliers de pliage avec des explications sur les mathématiques et l'algorithmique sous-jacentes.

2017 **Origami mathématiques et informatique**, *É.N.S. de Lyon/MMI*, Lyon.
Organisation bimensuelle de rencontres de pliage.

Octobre 2015 & Octobre 2016 **Animateur à la fête de la science**, *É.N.S. de Lyon*, Lyon.
Animateur d'un atelier sur les pliages mathématiques

Publications

Conférences

[1] B. Libert, S. Ling, F. Mouhartem, K. Nguyen, and H. Wang. Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions. In *Asiacrypt'16*, pages 373–403, 2016. `http://ia.cr/2016/101`.

[2] B. Libert, S. Ling, F. Mouhartem, K. Nguyen, and H. Wang. Zero-Knowledge Arguments for Matrix-Vector Relations and Lattice-Based Group Encryption. In *Asiacrypt'16*, pages 101–131, 2016. `http://ia.cr/2016/879`.

[3] B. Libert, F. Mouhartem, and K. Nguyen. A Lattice-Based Group Signature Scheme with Message-Dependent Opening. In *ACNS'16*, pages 137–155. Springer, 2016. `https://hal.inria.fr/hal-01302790`.

[4] B. Libert, F. Mouhartem, T. Peters, and M. Yung. Practical "Signatures with Efficient Protocols" from Simple Assumptions. In *AsiaCCS'16*, pages 511–522. ACM, 2016.
`https://hal.inria.fr/hal-01303696`.

Présentations

Conférences

Décembre 2016 **Asiacrypt**, *Hanoi*, 25 min.
Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions.

Juin 2016 **ACNS**, *University of Surrey*, Royaume Uni, 25 min.
A Lattice-Based Group Signature Scheme with Message-Dependent Opening.

Juin 2016 **AsiaCCS**, *Xi'an*, Chine, 25 min.
Practical "Signatures with Efficient Protocols" from Simple Assumptions.

Séminaires

Juin 2017 **Séminaire Cryptographie**, *Rennes*, France, 1 hour.
Adaptive Oblivious Transfer with Access Control for NC1 from LWE.

Avril 2017 **Journées du GT-C2**, *Inria Nancy – Grand Est*, La Bresse, 30 min.
Adaptive Oblivious Transfer with Access Control for Branching Programs.

Avril 2017 **Lattice Meetings**, *É.N.S. de Lyon*, Lyon, 1h.
Adaptive Oblivious Transfer from LWE.

Novembre 2016 **Séminaire Cryptographie**, *Université de Caen*, Caen, 1 h.
Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions.

Juin 2016 **Rencontres Arithmétique de l'Informatique Mathematique**, *Banyuls*, 30 min.
Signature de Groupe et Réseaux Euclidiens.

Juin 2016 **AriC Crypto Fair**, *É.N.S. de Lyon*, Lyon, 10 min.
Lattice-Based Group Encryption

Octobre 2015 **Journées du GT-C2**, *Université de Toulon*, La Londe-les-Maures, 25 min.
A Dynamic Group Signature Scheme based on Lattices.

Octobre 2015 **Lattice Meetings**, *É.N.S. de Lyon*, Lyon, 1h30.
Lattice-based group signatures for dynamic groups.

Septembre 2015 **Séminaire d'équipe AriC**, *É.N.S. de Lyon*, Lyon, 1h.
Un schéma de signature de groupe dynamique construit à l'aide de réseaux euclidiens.

Vulgarisation Scientifique

Mai 2017 **Origami et Complexité Algorithmique**, *Rencontres de Mai*, Blois, M.F.P.P.
Présentation des liens entre le pliage et la complexité algorithmique.

Février 2017 **Rencontres du troisième cycle**, *É.N.S. de Lyon*, Lyon, Avec Simon Castellan.
Présentation de 10 minutes du doctorat en informatique fondamentale

Octobre 2016 **Origami et Complexité Algorithmique**, *Journées Nationales de l'APMEP*, Lyon.
Présentation sur les liens entre le pliage et la complexité algorithmique.

Octobre 2016 **Présentation à la Fête de la Science**, *É.N.S. de Lyon*, Lyon.
Présentation de vulgarisation sur les preuves sans divulgation de connaissances.

Juin 2016 **Journée des lauréats du concours Al-Kindi**, *É.N.S. de Lyon*, Lyon.
Aperçu de la Cryptographie Moderne : Le Vote Électronique.

Octobre 2014 & Mars 2016 **Séminaire de la détente mathématique**, *É.N.S. de Lyon/MMI*, Lyon.
Orateur pour deux exposés de vulgarisation pour public averti sur les preuves *zero-knowledge* et le pliage en mathématiques et en informatique.

Informatique

OS Linux (quotidien), Windows.

Compétences Maîtrisé : Utilisation de `git`/`svn`. Programmation en C/C++, OCaml, LaTeX.
Familier : Utilisation de `make`. Programmation en Python/Sage, Bash, Magma, Maple.
Connaissances en assembleur x86.

Centres d'intérêts La *cryptologie*, mais aussi le *calcul formel* et la *théorie algorithmique des nombres*.

Langues

Français Langue maternelle.

Anglais Scientifique et courant. Certification : *CLES niveau B2*

Allemand Scolaire.

Malgache Notions.

Loisirs

Origami Gestion de *Club Origami* à la M.M.I. et à l'É.N.S. de Lyon.

Danses de salon En particulier le rock.

Wikipédia Rédaction de quelques articles portant sur la cryptologie.

Tennis de table Loisir.

Tricot Loisir.

Pliage de papier

[1] F. Mouhartem Canard en vol. Dans *Origami du vivant. Pliages du monde qui bouge, nage ou vole*. Vol. 2. Pages 13–14. Ed. M. Lucas. ISBN : 978-2-9556489-1-9