# Fabrice Mouhartem

*Curriculum Vitæ*

*LIP, É.N.S. de Lyon,*
*46 allée d'Italie,69364 Lyon Cedex 07*
☎ *+33 (0)4 72 72 87 60*
*+33 (0)6 38 61 92 22*
✉ *fabrice.mouhartem@ens-lyon.org*
*perso.ens-lyon.fr/fabrice.mouhartem/*

## Études

2015–... **Doctorat**, *LIP, É.N.S. de Lyon*, Sous la direction de Benoît Libert, 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

### Enseignements

2015–... **Activité Complémentaire d'Enseignement**, *É.N.S. de Lyon*, Lyon, France.
Chargé de TD en *Architecture* (L3)

2017–2018

- Architecture (TD/TP – L3). 32h

2016–2017

- Complexité Algorithmique (TD –M1). 20h
- Cryptographie et Sécurité (TD – M1). 20h
- Système et Réseaux (TD/TP – L3). 32h
- Jury de soutenances de stages en M1 (M1). 2h

2015–2016

- Théorie de la Programmation (TD/TP – L3). 32h
- Complexité Algorithmique (TD – M1). 20h
- Soutien en Probabilité (TD – L3). 2h

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

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

### Scientifique

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

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++

### Responsabilités administratives

2015 – 2017 **Membre élu au Conseil Scientifique**, *É.N.S. de Lyon*.
Représentant étudiant au conseil scientifique de l'É.N.S. de Lyon

### Vulgarisation Scientifique

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

Octobre 2015, 2016 & 2017 **Animateur à la fête de la science**, *É.N.S. de Lyon*, Lyon.
Animateur d'un atelier sur les pliages mathématiques

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.

## Publications

### Conférences


[1] Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong Wang. Adaptive Oblivious Transfer with Access Control from Lattice Assumptions. In *Asiacrypt'17*, 2017. To appear.
`https://hal.inria.fr/hal-01622197`.

[2] Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong 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`.

[3] Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong 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`.

[4] Benoît Libert, Fabrice Mouhartem, and Khoa 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`.

[5] Benoît Libert, Fabrice Mouhartem, Thomas Peters, and Moti 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 2017 **Asiacrypt**, *Hong Kong*, 25 min.
Adaptive Oblivious Transfer with Access Control from Lattice Assumptions

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.

### Rencontres

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.

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

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.

### Séminaires invités

Novembre 2017 **Séminaire Cryptographie**, *Université de Caen*, Caen, 1 heure.
Adaptive Oblivious Transfer with Access Control for $NC^1$ from LWE.

Novembre 2017 **Cryptography Seminar**, *Oxford*, Royaume-Uni, 1 heure.
Adaptive Oblivious Transfer with Access Control for $NC^1$ from LWE.

Juin 2017 **Séminaire Cryptographie**, *Université Rennes 1 – Irmar*, Rennes, 1 heure.
Adaptive Oblivious Transfer with Access Control for $NC^1$ from LWE.

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

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

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 Vice-président du MFPP (association francophone pour la promotion du pliage). Gestion des clubs de la M.M.I. et de l'É.N.S de Lyon.

Wikipédia Rédaction d'articles portant sur la cryptologie.

Danses de salon En particulier le rock.

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