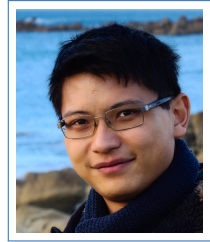


Fabrice Mouhartem

Docteur en Informatique

LIP, É.N.S. de Lyon,
46 allée d'Italie, 69364 Lyon Cedex 07
☎ +33 (0)6 38 61 92 22

✉ fabrice.mouhartem@ens-lyon.org
📄 perso.ens-lyon.fr/fabrice.mouhartem/



Formations

- 2018 **Doctorat**, LIP, É.N.S. de Lyon, Sous la direction de Benoît Libert, Informatique Fondamentale/Cryptologie.
Cryptographie protégeant la vie privée à base de couplages et de réseaux.
- 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

- 2015–2018 **Activité Complémentaire d'Enseignement**, É.N.S. de Lyon, Lyon, France.
Chargé de TD
 - 2017–2018
 - Architecture (TD/TP – L3). 32h
 - Projet (LIFProjet) à l'Université Claude Bernard Lyon 1. 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
- Janvier 2018 **Accueil d'un stagiaire de troisième**, É.N.S. de Lyon, Lyon, France.
Accueil de Jules Nogales, élève au collège du Val d'Ardières, pendant une semaine
- 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 **Interrogations orales en CPGE**, *Lycée du Parc*, Lyon.
& 2013–2014 Colleur en 832 (MPSI)

Scientifiques

Février–Juin **Stage de Recherche**, *É.N.S. de Lyon*, Lyon, France.

2015 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

Avril 2018 **Finaliste Google Hash Code**, *Google Dublin*, Irlande.

Concours d'optimisation en équipe, participation en C++

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

2017–2018 **Membre élu au Conseil de Laboratoire**, *É.N.S. de Lyon*.

Représentant doctorant au conseil de laboratoire du LIP

2017 **Participation à la labellisation HRS4R**, *Human Resources Strategie for Research*, *É.N.S. de Lyon*.

Comité de réflexion pour l'amélioration des conditions des personnels de l'É.N.S. de Lyon en vue d'une labellisation HRS4R

2015–2017 **Membre élu au Conseil Scientifique**, *É.N.S. de Lyon*.

Représentant étudiant au conseil scientifique de l'É.N.S. de Lyon

Médiation

2017–2018 **Origami mathématiques et informatique**, *É.N.S. de Lyon/MMI*, Lyon.

Organisation bimensuelle de rencontres de pliage.

Octobre 2015, **Animateur à la fête de la science**, *É.N.S. de Lyon*, Lyon.

2016 & 2017 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 scientifiques

Conférences internationales

- [1] Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong Wang. Adaptive oblivious transfer with access control from lattice assumptions. In *Asiacrypt'17*, pages 533–563. Springer, 2017.
<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.
<https://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.
<https://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 internationales

- 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 scientifiques

- Octobre 2018 **Journées du GT-C2**, *É.N.S. de Lyon*, Aussois, 30 min.
Zero-Knowledge Arguments for Matrix-Vector Relations and Lattice-Based Group Encryption.
- 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 Mathématique**, *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

- Septembre 2018 **Séminaire Cryptographie**, *Université Rennes 1 – Irmarr*, Rennes, 1 heure.
Zero-Knowledge Arguments for Matrix-Vector Relations and Lattice-Based Group Encryption.

- Août 2018 **Séminaire du Département d'Informatique, Indian Institute of Technology Madras, Chennai (Inde), 1h.**
Privacy-Preserving Cryptography from Pairings and Lattices
- Juillet 2018 **Séminaire de l'équipe complexité et cryptographie, Microsoft Research, Bangalore (Inde), 1h.**
Zero-Knowledge Arguments for Matrix-Vector Relations and Lattice-Based Group Encryption.
- Avril 2018 **AriC back from conferences, É.N.S. de Lyon, Lyon, 15 minutes.**
Post-quantum Fiat-Shamir from D. Unruh.
- 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 – Irmarr, 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 minutes.**
Lattice-Based Group Encryption.
- Septembre 2015 **Séminaire d'équipe AriC, É.N.S. de Lyon, Lyon, 1 heure.**
Un schéma de signature de groupe dynamique construit à l'aide de réseaux euclidiens.
- Médiation scientifique**
- Octobre 2018 **Fête de la Science, É.N.S. de Lyon, Lyon, Causeries mathématiques.**
Hôpitaux, banques et vie privée : en quoi la cryptographie peut-elle nous aider ?
- Mai 2018 **Journée des lauréats du concours Al-Kindi, É.N.S. de Lyon, Lyon.**
Présentation sur les preuves sans divulgation de connaissance
- Mars 2018 **Congrès MATH.en.JEANS, Université Lyon 1, Lyon.**
Exposé long invité au congrès MATH.en.JEANS de Lyon sur les mathématiques du pliage.
- Mai 2017 **Rencontres de Mai, Organisé par le M.F.P.P., Blois.**
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 **Journées Nationales de l'APMEP, Université Lyon 1, Lyon.**
Présentation sur les liens entre le pliage et la complexité algorithmique.
- Octobre 2016 **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 **Séminaire de la détente mathématique, É.N.S. de Lyon/MMI, Lyon.**
& Mars 2016 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 et ARM.

Contributions logicielles

2018 **Signatures de groupe**, *Signatures de groupe à base de couplages*, en C.

<https://gforge.inria.fr/projects/sigmasig-c>

2014 **Logarithme discret en petite caractéristique**, *Implantation de l'approche de Granger, Kleinjung et Zumbrägel*, en Magma.

2013 **Barra**, *Émulateur d'architecture de GPU (Tesla)*, en C++.

<https://raweb.inria.fr/rapportsactivite/RA2014/alf/uid43.html>

Langues

Français Langue maternelle Allemand Scolaire

Anglais Scientifique et courant. Malgache Notions

Certification : *CLES niveau B2* (2015)

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 de 2012 à 2018.

Wikipédia Rédaction d'articles portant sur la cryptologie. Tennis de table 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