Fabrice Mouhartem

CV

LIP, É.N.S. de Lyon, 46 allée d’Italie, 69364 Lyon Cedex 07
T +33 (0)4 72 72 87 60
M +33 (0)6 38 61 92 22
E fabrice.mouhartem@ens-lyon.org
Nationality: French

Education

PhD student, L.I.P., É.N.S. de Lyon, France, Privacy-Enhancing Cryptography with Advanced Functionalities. Advisor: Benoît Libert

Master d’Informatique Fondamentale, É.N.S. de Lyon, France, (university-level institution training teachers and researchers, entrance to which is based on a competitive exam. Equivalent to a Master of Science Degree in Computer Science).

Licence d’Informatique Fondamentale, É.N.S. de Lyon, France, (equivalent to a Bachelor of Science Degree in Computer Science).

Experience

Research

Supervision of a one week internship, É.N.S. de Lyon, Lyon, France. May 2016
Make a ninth grade student intern discover fundamental research laboratories

5 Month Research Internship, É.N.S. de Lyon, Lyon, France, Design a lattice-based dynamic group signature scheme. Spring 2015

3 Month Research Internship, Katholieke Universiteit Leuven, Leuven, Belgium, Implementation in M/A/C/G/SC/M/SC/A/SC of the state of the art discrete logarithm solving algorithm in small characteristic with improvements on them. Summer 2014

6 Week Research Internship, Inria, Rennes, France, Works on the BARRA simulator to implement techniques to improve energy efficiency of GPUs using data redundancy. Introduction to research. Summer 2013

Teaching

Teaching Assistant, É.N.S. de Lyon, Lyon, France. 2015–now

2017–2018
• Computer Architecture (L3). 32h

2016–2017
• Computational Complexity (M1). 20h
• Cryptography and Security (M1). 20h
• Operating Systems and Networks (L3). 32h
• Jury for M1 thesis. 2h

2015–2016
• Programming Language Theory (L3). 32h
• Computational Complexity (M1). 20h
• Remedial courses in Probability (L3). 2h

Administrative Responsibilities
Scientific Council, É.N.S. de Lyon, Lyon. 2015–2017
Student representative at the scientific council of É.N.S. de Lyon.

Popularisation
Origami in Math and C.S., É.N.S. de Lyon/MMI, Lyon. April 2017
Open access origami workshop about mathematical origamis.

Origami in Math and C.S., É.N.S. de Lyon/MMI, Lyon. 2017
Organisation of a bimonthly origami’s workshops.

Animator at Fête de la Science, É.N.S. de Lyon, Lyon. October 2015, 2016 & 2017
Organisation of a workshop about mathematical origamis.

Programming Contests
Contestant for the ACM ICPC SWERC, Universidad do Porto, November 2014 & 2015
Porto, Portugal.
Team algorithmic competition, participation in C++

Contestant for the ACM ICPC SWERC, Universitat de València, Valen-
cia, Spain. November 2013

Contestant for Prologin, EPITA, Paris, France. 2013
Individual algorithmic & A.I. competition, participation in C++

Publications
Conferences


Talks
Conference talks
Asiacrypt, Hong Kong, China, 25 min. December 2017
Adaptive Oblivious Transfer with Access Control from Lattice Assumptions

Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions.

ACNS, University of Surrey, United Kingdom, 25 min. June 2016
A Lattice-Based Group Signature Scheme with Message-Dependent Opening.

AsiaCCS, Xi’an, China, 25 min. June 2016
Practical “Signatures with Efficient Protocols” from Simple Assumptions.
Seminars

**Caen Crypto Seminar**, Caen, France, 1 hour. Adaptive Oblivious Transfer with Access Control for NC$^1$ from LWE. November 2017


**Rennes Crypto Seminar**, Rennes, France, 1 hour. Adaptive Oblivious Transfer with Access Control for NC$^1$ from LWE. June 2017


**Lattice meeting**, É.N.S. de Lyon, France, 1h30. Adaptive Oblivious Transfer from LWE. April 2017


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


**Lattice meeting**, É.N.S. de Lyon, France, 1h30. Lattice-based group signature for dynamic groups. October 2015

**Séminaire AriC**, É.N.S. de Lyon, France, 1h. Lattice-based dynamic group signature. September 2015

Popularisation

**Origami and computational complexity**, MFPP’s National Days, Blois. May 2017

Popularisation talk about the link between origami and computational complexity.

**Rencontres du troisième cycle**, É.N.S. de Lyon, With Simon Castellan. February 2017

10 minutes presentation of what is a PhD in Computer Science.


Popularisation talk about the link between origami and computational complexity.

**Fête de la Science**, É.N.S. de Lyon, Lyon. October 2016

Popularisation talk about zero-knowledge proofs.

**Al-Kindi cryptography contest**, É.N.S. de Lyon, Lyon. June 2016

Overview of modern cryptography: the case of e-voting.


Two popularisation talks: on zero-knowledge proofs and mathematical origamis.

Languages

French: Native

English: Fluent

German: Basic

Malagasy: Basic

Computer Skills

Use of Linux and Windows. Knowledge in Microsoft Office & \LaTeX{} usage. Proficient in C/C++ and OCaml. Familiar with Python/Sage, Bash scripting, gnuplot and magma CAS.

Interests

Paper folder, dancer (rock’n’roll, waltz, chachacha ...), table tennis player, and also popularisation on Wikipedia.

Last updated: 18th December 2017