Fabrice Mouhartem

PQShield SAS,
8 rue des Pirogues de Bercy
75012, Paris 12
+33 (0)6 38 61 92 22
fmouhart@epheme.re
fmouhart.epheme.re
Nationality: French

Research

Interests: Cryptology, privacy, algorithmic number theory, computational complexity.

Positions

Post-Doctoral Researcher, *PQShield*, France. **July 2022–Now**

Post-Doctoral Researcher, *ENS de Lyon*, France. **August 2021–June 2022**

Young International Faculty, *I.I.T. Madras*, Chennai, India. **July 2019–June 2020**

Visiting Researcher, *Microsoft Research India*, Bangalore. **January–May 2019**

PhD Student, *É.N.S. de Lyon*, France. **2015–2018**

Program committees

Conferences: IWSEC 2019

Education

PhD, *L.I.P., É.N.S. de Lyon*, France. **October 2018**

Title: Privacy-Preserving Cryptography from Pairings and Lattices

Advisor: Benoît Libert

Reviewers
- Dario Catalano
- David Pointcheval

Committee members
- Shweta Agrawal
- Pierre-Alain Fouque
- Philippe Gaborit
- Carla Ràfols

Master d'Informatique Fondamentale, *É.N.S. de Lyon*. **September 2015**

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. *Cum laude*
Internships:
- M1 – 3 month research internship under the supervision of Fréderik Vercauteren at KU Leuven (Belgium): Implementation in Magma of the state of the art *discrete logarithm* solving algorithm in small characteristic with improvements
- M2 – 5 month research internship under the supervision of Benoît Libert at ENS de Lyon: Design a lattice-based dynamic group signature scheme

Licence d'Informatique Fondamentale, *É.N.S. de Lyon*. **September 2013**

Equivalent to a Bachelor of Science Degree in Computer Science. *Cum laude*.
Internship:
- L3 – 6 weeks research internship with Sylvain Collange at Irisa, Rennes (France): Works on the Barra simulator to implement techniques to improve energy efficiency of GPUs using data redundancy

Teaching

Teaching Assistant, *Univ. Grenoble-Alpes*, France. **2021–2022**

Co-teaching the Advanced Cryptography Course in M2 CySec. 21h

Teaching Assistant, *ÉPITA Lyon*, France. **2021**

Teaching assistant in regular language theory. 18h

Young International Faculty, *I.I.T. Madras*, Chennai, India. **2019–2020**

Teaching **CS6190:** *Recent Developments in Theoretical Computer Science*.
Subject: recent uses of (non-interactive) zero-knowledge proof in cryptography.

Teaching Assistant, *É.N.S. de Lyon*, France. **2015–2018**

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

- Project (LIFProjet) in *Université Claude Bernard Lyon 1*. 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

Publications

Journals

Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong Wang. Adaptive Oblivious Transfer with Access Control from Lattice Assumptions. *Theoretical Computer Science*, 2021.
`https://doi.org/10.1016/j.tcs.2021.09.001`.

Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong Wang. Zero-Knowledge Arguments for Matrix-Vector Relations and Lattice-Based Group Encryption. *Theoretical Computer Science*, 2019.
`https://doi.org/10.1016/j.tcs.2019.01.003`.

Conferences

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`.

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`.

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`.

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`.

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`.

Workshops

Benoît Libert, Marc Joye, Moti Yung, and Fabrice Mouhartem. Fully Distributed Non-Interactive Adaptively-Secure Threshold Signature Scheme with Short Shares: Efficiency Considerations and Implementation. In *NIST Threshold Cryptography Workshop 2019*, 2019.
`https://csrc.nist.gov/CSRC/media/Events/NTCW19/papers/paper-LJYM.pdf`.

Technical Reports

Benoît Libert and Fabrice Mouhartem. Survey of existing building blocks for practical advanced protocols. Technical report, h2020 Prometheus, May 2019. Available at https://www.h2020prometheus.eu/.

Benoît Libert and Fabrice Mouhartem. Méthodes appropriées - partie 1 - « preuves zero- knowledge ». Technical report, RISQ, April 2018.

Experience

Administrative Responsibilities

Laboratory Council, *LIP, É.N.S. de Lyon*, France. **2017–2018**

PhD representative at the laboratory council of the LIP.

HRS4R committee, *É.N.S. de Lyon*, France. **2017**

Employees representative to help É.N.S. de Lyon get the european label *Human Resources Strategy for Research*.

Scientific Council, *É.N.S. de Lyon*, France. **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*, France. **April 2017**

Open access origami workshop about mathematical origamis.

Origami in Math and C.S., *É.N.S. de Lyon/MMI*, France. **2017**

Organisation of a bimonthly origami's workshops.

Animator at Fête de la Science, *É.N.S. de Lyon*, France. **October 2015, 2016 & 2017**

Organisation of a workshop about mathematical origamis.

Programming Constests

Finalist for Google Hash Code, *Google Dublin*, Dublin, Ireland. **March 2017**

Team algorithmic/optimization contest, participation in C++.

Contestant for the ACM ICPC SWERC, *Porto/València*. **November 2013, 2014 & 2015**

Team algorithmic contest, participation in C++.

Finalist for Prologin, *EPITA*, Paris, France. **2013**

Individual algorithmic & A.I. contest, participation in C++.

Talks

International conference talks

Asiacrypt, *Hong Kong*, China, 25 min. **December 2017**

Adaptive Oblivious Transfer with Access Control from Lattice Assumptions.

Asiacrypt, *Hanoi*, Vietnam, 25 min. **December 2016**

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.

International Workshops

NIST Workshop on Threshold Cryptography, *U.S.A.*, 25 min. **March 2019**

Fully Distributed Non-Interactive Adaptively-Secure Threshold Signature Scheme with Short Shares: Efficiency Considerations and Implementation

Invited seminars

CAS^{3}C^3 seminar, *LJK, Université Grenoble Alpes*, France, 1 hour. **October 2019**

Lattice-Based Group Signatures in the Standard Model

Almasty crypto seminar, *LIP6, Paris*, France, 1 hour. **December 2018**
Privacy-Preserving Cryptography

Rennes Crypto Seminar, *Rennes*, France, 1 hour. **September 2018**
Zero-Knowledge Arguments for Matrix-Vector Relations and Lattice-Based Group Encryption.

Department Seminar, *Indian Institute of Technology Madras*, Chennai, India, 1 hour. **August 2018**
Privacy-Preserving Cryptography from Pairings and Lattices.

Talk at Microsoft Research, *Microsoft Research Bangalore*, India, 1 hour. **July 2018**
Zero-Knowledge Arguments for Matrix-Vector Relations and Lattice-Based Group Encryption.

AriC "back from conferences", *É.N.S. de Lyon*, France, 15 min. **May 2018**
Post-Quantum Fiat Shamir.

Oxford Crypto Seminar, *Oxford*, UK, 1 hour. **November 2017**
Adaptive Oblivious Transfer with Access Control from Lattice Assumptions.

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

Caen Crypto Seminar, *Caen*, France, 1 hour. **November 2016**
Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions.

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

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

Scientific Events

Journées du GT-C2, *É.N.S. de Lyon*, Aussois, 30 min. **October 2017**
Zero-Knowledge Arguments for Matrix-Vector Relations and Lattice-Based Group Encryption.

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

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

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

RAIM, *Banyuls-sur-Mer*, France, 30 min. **June 2016**
Group Signatures and Lattice-Based Cryptography.

Journées du GT-C2, *Université de Toulon*, France, 25 min. **October 2015**
A Dynamic Group Signature Scheme based on Lattices.

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

Popularisation

Fête de la Science, *É.N.S. de Lyon*, France. **October 2018**
Popularisation talk about privacy-preserving cryptography.

Al-Kindi cryptography contest, *É.N.S. de Lyon*, France. **May 2018**
Overview of zero-knowledge proofs for middle school students

MATh.en.JEANS' congress, *Univ. Lyon 1*, France. **March 2018**
Invited popularisation talk for middle school students about mathematical origamis

MFPP's National Days, *Origami and computational complexity*, 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.

APMEP's National Days, *Origami and computational complexity*, **October 2016** France.

Popularisation talk about the link between origami and computational complexity.

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

Popularisation talk about zero-knowledge proofs.

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

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

Recreational Mathematics Seminar, *É.N.S. de Lyon/MMI*. **October 2014 & March 2016**

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

Languages

French: Native

English: Fluent

German: Basic

Malagasy: Basic

Computer Skills

Everyday use of GNU/Linux on desktop computers and servers. Typesetting with LaTeX/TeX. Proficient in C/C++, Rust and OCaml. Familiar with Python/Sage, bash/sh scripting, gnuplot and magma CAS.

Software

Threshold signatures, *Implementation of a pairing-based threshold signature scheme*, in C++. **2019**

`https://gitlab.inria.fr/fmouhart/threshold-signature`

Group signatures, *Implementation of our dynamic group signature scheme from pairing assumptions*, in C. **2018**

`https://gitlab.inria.fr/fmouhart/sigmasig-c`

Discrete logarithm in small characteristic, *Implementation of Granger, Kleinjung and Zumbrägel's approach*, in Magma. **2014**

Barra, *GPU Tesla architecture emulator*, in C++. **2013**

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

Interests

Paper folder, table tennis player, and also popularisation on Wikipedia.

Origami

Président of the MFPP (French Origami Society)

Publications:

Fabrice Mouhartem. Flying duck. In *Origami du vivant. Pliages du monde qui bouge, nage ou vole*. Vol. 2. pp. 13–14. Ed. M. Lucas. ISBN: `978-2-9556489-1-9`

Fabrice Mouhartem, Constructions exactes et approchées dans le pliage de papier To appear in *Tangente Éducation* magazine. July 2021. Available at https://epheme.re/vulgarisation/tangente21.pdf (in French).