Fabrice **Mouhartem**

fabrice@epheme.re | fmouhart.epheme.re | chouhartem |
Paris Region | PhD in Cryptology

Cryptography expert in post-quantum design and privacy-preserving provable security

Education

École Normale Supérieure de Lyon — *Lyon, France*
PhD in Cryptology — *2018*

- Thesis: Privacy-preserving cryptography from pairings and lattices
- Keywords: advanced cryptography | provable security | post-quantum | ZK proofs | public-key cryptography

École Normale Supérieure de Lyon — *Lyon, France*
Master in theoretical computer science — *2015*

- Thesis: Lattice-based dynamic group-signature from lattices

Experience

R&D

XWiki SAS — *Paris, France*
Senior R&D Engineer in Security and Cryptography — *2023–Now*

- CryptPad project, open-source end-to-end encrypted office suite
- Lead on the post-quantum and crypto-agility experiments in CryptPad
- Backend and day-to-day development of the software
- Talks at several FOSS conferences (FOSDEM, Pass the Salt, Capitole du Libre...) and technical blogpost writing
- Senior since 2026

Teaching and Research

PQShield SAS — *Paris, France*
Cryptography Researcher — *2022–2023*

- Design and proofs for post-quantum maskable threshold signatures
- NIST candidate submission for the new call on NIST post-quantum standards

ENS de Lyon — *Lyon, France*
Post-doctoral researcher — *2018, 2021–2022*

- H2020 Prometheus: European project on new post-quantum schemes for data privacy (Prize “Étoile de l’Europe”)
- Pairing-based threshold signature with a PoC implementation (Accepted at NIST 1st threshold cryptography workshop)
- Teaching: introduction to rational languages (EPITA Lyon), Advanced Cryptography (Grenoble university)

Indian Institute of Technology, Madras — *Chennai, India*
Young International Faculty — *2019–2020*

- Define and formalise multiparty functional encryption
- Design of a 50h course on Advanced Cryptography
- Program committee member of IWSEC 2020 and ProvSec 2020

Microsoft Research India — *Bangalore, India*
Invited Reseacher — *2019–2020*

- Works on large-scale anonymous credentials
- Program committee member of IWSEC 2019

ENS de Lyon — *Lyon, France*
PhD Student — *2015–2018*

- Work on different schemes based on several different security assumptions: group signatures, group encryption, oblivious transfer, anonymous credentials
- Design of more expressive zero-knowledge proofs than state of the art from lattice assumptions
- Teaching: Cryptography and Security, architecture, system and networks, theory of programming, algorithmic complexity, projects (bachelor degree)

Selected Papers

PhD Manuscript

- **FM**. Privacy-preserving cryptography from pairings and lattices. *Thèse de doctorat de l'Université de Lyon*. 2018. https://theses.hal.science/tel-01913872/

Journals

- Benoît Libert, San Ling, **FM**, Khoa Nguyen, and Huaxiong Wang. Adaptive Oblivious Transfer with Access Control from Lattice Assumptions. *Theoretical Computer Science*, 2021. "publications", doi:10.1016/j.tcs.2021.09.001.
- Benoît Libert, San Ling, **FM**, Khoa Nguyen, and Huaxiong Wang. Zero-Knowledge Arguments for Matrix-Vector Relations and Lattice-Based Group Encryption. *Theoretical Computer Science*, 2019. doi:10.1016/j.tcs.2019.01.003.

International Conferences

- Rafaël del Pino, Shuichi Katsumata, Mary Maller, **FM**, Thomas Prest, and Markku-Juhani Saarinen. Threshold Raccoon: Practical Threshold Signatures from Standard Lattice Assumptions. *Eurocrypt*, 2024. doi:10.1007/978-3-031-58723-8_8.
- Benoît Libert, San Ling, **FM**, Khoa Nguyen, and Huaxiong Wang. Adaptive oblivious transfer with access control from lattice assumptions. *Asiacrypt*, 2017. doi:10.1007/978-3-319-70694-8_19. https://hal.inria.fr/hal-01622197.
- Benoît Libert, San Ling, **FM**, Khoa Nguyen, and Huaxiong Wang. Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions. *Asiacrypt* 2016. doi:10.1007/978-3-662-53890-6_13. https://ia.cr/2016/101.
- Benoît Libert, San Ling, **FM**, Khoa Nguyen, and Huaxiong Wang. Zero- Knowledge Arguments for Matrix-Vector Relations and Lattice-Based Group Encryption. *Asiacrypt* 2016. doi:10.1007/978-3-662-53890-6_4. https://ia.cr/2016/879.

Workshops

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

Technical Reports

- Rafaël del Pino, Thomas Espitau, Shuichi Katsumata, Mary Maller, **FM**, Thomas Prest, Mélissa Rossi and Markku-Juhani Saarinen. Raccoon: A Side-Channel Secure Signature Scheme. *Specification Document for NIST*, 2023. https://raccoonfamily.org/wp-content/uploads/2023/07/raccoon.pdf
- Benoît Libert and **FM**. Survey of existing building blocks for practical advanced protocols. *h2020 Prometheus*, 2019. https://www.h2020prometheus.eu/.
- Benoît Libert and **FM**. Méthodes appropriées – partie 1 – « preuves zero-knowledge ». *RISQ* (projet BPI), 2018.

Technology

Open-Source

CryptPad
DEVELOPMENT TEAM MEMBER
2023–Now

- Daily tasks on the software (fixes and features)
- Refactor of the server for a horizontally scalable architecture
- User supports on CryptPad.fr

Associations

Mouvement Français des Plieurs de Papier
ADMINISTRATIVE COUNCIL
Paris, France
2015–Now

- Association for the promotion and diffusion of Origami in France
- Former president of the association (2019–2020)
- Administrative council member

Ergodis
COLLEGE MEMBER
Paris, France
2019–2026

- Association to promote and sensibilise about workspace ergonomy
- Standardisation of the "bépo" keyboard layout with AFNOR
- Participation in the design of the french-english keyboard layout "ergo-L"

Competences

Languages French (native) | English (fluent)
Hobbies Origami | Social dancing | Table tennis