

## Mireille Fouquet

3 passage des entrepreneurs

75 015 PARIS

FRANCE

Tél : (+33) 06 21 05 28 77

Mèl : mireille.fouquet@u-paris.fr

Maîtresse de conférence

Docteure de l'école Polytechnique

Née le 22 Octobre 1975

Mariée, deux enfants

### Parcours académique

**Depuis octobre 2002** Maîtresse de conférences à l'UFR de Mathématiques d'Université Paris Cité, anciennement Université Paris Diderot - Paris 7

Membre de l'équipe de théorie des nombres de l'Institut de Mathématiques de Jussieu - Paris Rive Gauche

**1998 - 2001** Thèse sous la direction de François Morain

### Responsabilités

- Co-responsable avec Mathilde Herblot du programme MathC2+ porté par la SMF, Animath et le ministère de l'éducation nationale depuis septembre 2024
- Responsable du Master Professionnel Mathématiques, Informatique et applications à la Cryptologie depuis sa création
- Porteuse du projet de création de la spécialité Mathématiques, Informatique et applications à la cryptologie du master Mathématiques et applications en 2005
- Vice-présidente en charge de la vie étudiante d'Université Paris Cité de janvier 2020 à juillet 2023
- Membre élue du conseil d'administration de l'université Paris Diderot d'avril 2018 à décembre 2019
- Vice-présidente en charge de la vie étudiante de l'université Paris Diderot de mars 2017 à décembre 2019

### Co-encadrement

**Étudiant** Javier Valera

**Co-directeur** Josep M. Miret

**Université** Universitat de Lleida

**Titre** Algoritmos para obtener curvas elípticas e curvas hiperelípticas criptográficamente útiles

**Date de soutenance** 22 septembre 2017

### Publications

- *An extension of Satoh's algorithm and its implementation.* (avec P. Gaudry et R. Harley) J. Ramanujan Math. Soc. (2000)
- *Finding Secure Curves with the Satoh-FGH Algorithm and an Early-Abort Strategy.* avec P. Gaudry et R. Harley, Eurocrypt 2001.
- *Isogeny volcanoes and the SEA algorithm.* (avec F. Morain), ANTS V, 2002
- *Isogenies between elliptic curves defined over a finite field and binary quadratic forms,* avec J. Miret, D. Sadornil, J. Tena et M. Valls, Proceedings of the " Segundas jornadas de teoria de numeros ", 2008
- *Isogeny volcanoes of elliptic curves and Sylow subgroups* avec J. Miret et J. Valera, Latincrypt 2014
- *Distorting the volcano* (avec J. Miret Biosca et J. Valera) Finite Fields and their Applications, Elsevier (2017)