

## Diplômes et Études

- 2016-2018 **Première et deuxième années de thèse**, *Obfuscation de programmes*, sous la direction de Damien STEHLÉ, LIP, ENS de Lyon, Lyon, France.
- 2016 **Agrégée de mathématiques**, 8ème.
- 2015-2016 **Préparation de l'agrégation externe de mathématiques**, ENS de Lyon, Lyon, France.
- Février-Juin 2015 **Stage de recherche**, *Fonctions multilinéaires en cryptographie*, sous la direction de Damien STEHLÉ, Laboratoire d'Informatique et du Parallélisme, ENS de Lyon, Lyon, France.
- 2014-2015 **Master d'informatique fondamentale mention très bien**, ENS de Lyon, Lyon, France.
- Mai-Juillet 2014 **Stage de recherche**, *Problème à 3+1 corps*, sous la direction de Warwick TUCKER, Angstrom laboriet, Université d'Uppsala, Suède.
- 2013-2014 **Première année de master d'informatique fondamentale**, ENS de Lyon, Lyon, France.
- Juin-Juillet 2013 **Stage d'initiation à la recherche**, *Algorithme rapide pour calculer le symbole de réciprocité cubique*, sous la direction de Pierrick GAUDRY, Loria, Nancy, France.
- 2012-2013 **Licence d'informatique fondamentale mention très bien**, ENS de Lyon, Lyon, France.
- 2012-2016 **Élève Normalienne à l'ENS de Lyon**.
- 2010-2012 **Classes préparatoires aux grandes écoles**, *Lycée Saint Louis*, Paris, France.
- 2010 **Baccalauréat S mention très bien**, *Lycée Emmanuel Mounier*, Châtenay-Malabry, France.

## Compétences

### Informatique

Langages de programmation	C, C++, Python, SAGE	Autre	LaTeX, Git
---------------------------	----------------------	-------	------------

### Langues

Anglais	écrit, parlé	Espagnol	notions
---------	--------------	----------	---------

## Enseignement

- Février 2017 Co-encadrement d'un stagiaire de 3ème en stage d'observation avec Fabrice MOUHARTEM.
- 2017-2018 Chargée de TDs en architecture, systèmes et réseaux (niveau L3) et en cryptographie et sécurité (niveau M1), ENS de Lyon, Lyon, France.
- Avril 2016 Encadrement d'un stagiaire de 3ème en stage d'observation.
- 2016-2017 Chargée de TDs en théorie de l'information (niveau M1) et calcul formel (niveau M1), ENS de Lyon, Lyon, France.
- Septembre 2016 Cours de mise à niveau en maths pour les étudiants de L3 n'ayant pas fait de prépa, ENS de Lyon, Lyon, France.

## Soutien scolaire

- 2015 Soutien scolaire ponctuel en mathématiques pour des lycéens, avec l'association ENSeigner de l'ENS de Lyon.
- 2014-2016 Soutien scolaire en mathématiques à un élève de CPES (classe préparatoire à l'enseignement supérieur) de l'ENS de Lyon.

---

## Production scientifique

- 2018 *Approx-SVP in Ideal Lattices with Pre-processing*, avec Damien STEHLÉ. Soumis à ASIACRYPT 2018.
- 2017 *Notes On GGH13 Without The Presence Of Ideals*, avec Martin R. ALBRECHT, Alex DAVIDSON et Enrique LARRAIA. EPRINT 2017/906.
- 2017 *Quantum Attacks against Indistinguishability Obfuscators Proved Secure in the Weak Multilinear Map Model*. Accepté à CRYPTO 2018.
- 2017 *On the Statistical Leak of the GGH13 Multilinear Map and some Variants*, avec Léo DUCAS. EPRINT 2017/482, soumis à ASIACRYPT 2018.
- 2015 *Cryptanalysis of Gu's ideal multilinear map*, avec Damien STEHLÉ. EPRINT 2015/759.

---

## Exposés

- Mai 2018 **Exposé de vulgarisation scientifique pour des collégiens et lycéens ayant participé au concours Alkindi**, Lyon, France, 30 min.  
Introduction à la cryptographie.
- Septembre 2017 **Monthly lattice and crypto meetings**, Lyon, France, 90 min.  
Quantum Attacks against Indistinguishability Obfuscators Proved Secure in the Weak Multilinear Map Model.
- Juin 2017 **Exposé de vulgarisation scientifique pour des collégiens et lycéens ayant participé au concours Alkindi**, Lyon, France, 30 min.  
Introduction à la cryptographie.
- Avril 2017 **Journées C2**, La Bresse, France, 25 min.  
On the Statistical Leak of the GGH13 Multilinear Map and some Variants.