Alice Pellet--Mary

ENS de Lyon, LIP
9 rue du Vercors, 69007 Lyon
✉ *alice.pellet-mary@ens-lyon.org*

Education

2016-2018 **First and second year of PhD, under the supervision of Damien Stehlé**, *LIP, ENS de Lyon*, Lyon, France.

2016 **Agrégée de mathématiques**, *8th*.

2015-2016 **Preparing the "agrégation externe" competitive exam in mathematics**, *ENS de Lyon*, Lyon, France.

February-June 2015 **Research internship**, *Multilinear maps in cryptography*, under the direction of Damien Stehlé, Laboratoire d'Informatique et du Parallélisme, ENS de Lyon, Lyon, France.

2014-2015 **Master degree in computer science**, *ENS de Lyon*, Lyon, France.

May-July 2014 **Research internship**, *Relative equilibria for the restricted four body problem*, under the direction of Warwick Tucker, Angstrom laboratoriet, Uppsala university, Sweden.

2013-2014 **First year of master degree in computer science**, *ENS de Lyon*, Lyon, France.

June-July 2013 **Research internship**, *Asymptotically fast algorithm for cubic reciprocity*, under the direction of Pierrick Gaudry, Loria, Nancy, France.

2012-2013 **Bachelor degree in computer science**, *ENS de Lyon*, Lyon, France.

2012-2016 **Student at the ENS of Lyon**.

2010-2012 **Two-years intensive course preparing for the competitive entrance examination to French "Grandes Ecoles"**, *Lycée Saint Louis*, Paris, France.

2010 **A-Levels in science with highest honours**, *Lycée Emmanuel Mounier*, Châtenay-Malabry, France.

Skills

Computers

Programming languages: C, C++, Python, SAGE

Other: LaTeX, Git

Languages

French: Mother tongue

English: Reasonable working knowledge

Spanish: Basic knowledge

Teaching

Spring 2018 Teaching assistant in Cryptography and Security, for master students, ENS de Lyon, Lyon, France.

Fall 2017 Teaching assistant in Computer Architecture, for undergraduate students, ENS de Lyon, Lyon, France.

April 2017 Supervision of a one week internship of a middle school student.

Spring 2017 Teaching assistant in Computer Algebra, for master students, ENS de Lyon, Lyon, France.

Fall 2016 Teaching assistant in Information Theory, for master students, ENS de Lyon, Lyon, France.

2015 Occasional tutoring for secondary school students.

2014-2016 Maths tutorial for a first year undergraduate student.

Publications

2018 *Quantum Attacks against Indistinguishablility Obfuscators Proved Secure in the Weak Multilinear Map Model.* In Crypto 2018.

Preprints

2017 *Notes On GGH13 Without The Presence Of Ideals*, with Martin R. Albrecht, Alex Davidson and Enrique Larraia. EPRINT 2017/906.

2017 *On the Statistical Leak of the GGH13 Multilinear Map and some Variants*, with Léo Ducas. EPRINT 2017/482.

2015 *Cryptanalysis of Gu's ideal multilinear map*, with Damien Stehlé. EPRINT 2015/759.

Talks

May 2018 **Popularization talk for high school students**, Lyon, France, 30 min.
Introduction à la cryptographie.

September 2017 **Monthly lattice and crypto meetings**, Lyon, France, 90 min.
Quantum Attacks against Indistinguishablility Obfuscators Proved Secure in the Weak Multilinear Map Model.

June 2017 **Popularization talk for high school students**, Lyon, France, 30 min.
Introduction à la cryptographie.

April 2017 **Journées C2**, La Bresse, France, 25 min.
On the Statistical Leak of the GGH13 Multilinear Map and some Variants

Miscellaneous

Hobbies Piano, ultimate frisbee, knitting.