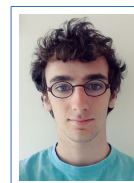


Simon Masson

Doctorant en cryptologie

31 allées Léon Gambetta
92110 Clichy
☎ (+33)6 03 86 27 13
✉ simon.masson@loria.fr
24 ans



Cursus universitaire

2018 **Doctorat en cryptographie**, *INRIA de Nancy - Grand Est*, première année.
Sous la direction de Emmanuel Thomé et Aurore Guillevic.

ALGORITHMIQUE DES COURBES DESTINÉES AUX CONTEXTES DE LA CRYPTOGRAPHIE
BILINÉAIRE ET POST-QUANTIQUE.

2017 **M2 Recherche Algèbre Appliquée**, *Université de Paris Saclay*.

Cours suivis : Algèbre effective, Courbes algébriques, Courbes elliptiques, Cryptographie, Complexité algébrique, Algorithmie et langage C.
Mention TRÈS BIEN (16.7/20). Rang : 1^{er}/12.

2016 **Agrégation externe de Mathématiques**, *Université de Rennes 1*.

Option C (algèbre et calcul formel). Rang : 92/305.

2016 **M2 Métiers de l'enseignement**, *Université de Rennes 1*.

2015 **M1 Mathématiques fondamentales**, *Université de Rennes 1*.

2014 **Licence de Mathématiques**, *Université de Rennes 1*.

Expériences professionnelles

2018 – **CDD CIFRE**, *Thales Communications & Security*.
aujourd'hui Doctorat encadré par Olivier Bernard.

Mars – **Stage de M2**, *Méthode GLV en dimension 4 sur les \mathbb{Q} -courbes*, Thales Communica-
Septembre tions & Security.

2017 Sous la direction de Olivier BERNARD, Renaud DUBOIS et Olivier ORCIÈRE.

Au sein d'un laboratoire Recherche & Développement de 10 cryptologues, l'objectif est de comprendre, reproduire et trouver de nouvelles courbes avec une arithmétique efficace. Je développe en **Sage** un outil de recherche de courbes, et j'implémente dans une librairie propriétaire la multiplication de point accélérée par des techniques de décomposition du scalaire, grâce à des endomorphismes de la courbe.

Janvier – Mars **Projet de C**, *Implémentation de la méthode GLV*, Université de Versailles.

2017 Sous la direction de Michaël QUISQUATER.

Développement à partir de la bibliothèque **GMP** de l'arithmétique des courbes elliptiques sous forme de Weierstrass. Implémentation de la méthode GLV avec une exponentiation efficace.

Juin – Juillet **Stage de M1**, *Introduction aux algèbres de Lie*, Università di Padova, Italie.

2015 Sous la direction de Giovanna CARNOVALE

Introduction aux notions d'algèbres de Lie et de leurs représentations. Théorème de Weyl sur la réduction complète des représentations.

Janvier – Mai **Travail encadré de recherche**, Université de Rennes 1.

2015 Sous la direction de Christophe MOUROUGANE, avec Jordan TRÉMOUREUX.

Introduction à la géométrie hyperbolique avec trois modèles : le disque et le demi-plan de Poincaré, ainsi que l'hyperboloïde. Etude des droites et des polygones sur différents modèles.

Avril – Mai **Stage de L3**, Université de Nantes.

2014 Sous la direction de Gilles CARRON.

Groupes de type fini à croissance linéaire, théorème de Gromov.

Compétences informatiques

Linux, C, Sage, L^AT_EX, HTML, CSS, PHP, jQuery

Expériences personnelles

- 2013–2016 Webmaster de plusieurs sites web de volley-ball
- 2015–2016 Colleur en MP au lycée Chateaubriand, Rennes (remplacement)
- 2013 Vice-champion de France universitaire en volley-ball, avec l'Université de Rennes 1
- 2011–12–13 Emploi saisonnier, Piscine municipale de Coutances (50), sauveteur
- Depuis 2001 Pratique du volley-ball en Nationale 2.