# Simon Masson

*Docteur en informatique*

✉ *simon.masson@loria.fr*
*members.loria.fr/smasson/*
*Français, 27 ans*

## Cursus universitaire

2018–2020 **Doctorat en informatique**. *INRIA de Nancy - Grand Est.*
Sous la direction de Emmanuel Thomé et Aurore Guillevic.
Soutenue le 4 décembre 2020.

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 : 1er.

2016 **Agrégation externe de Mathématiques**. *Université de Rennes 1.*
Option C (algèbre et calcul formel). Rang : 92ème.

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

Janvier 2018 – Janvier 2021 **CDD CIFRE**. *Thales.*
Doctorat encadré par Olivier Bernard. Génération de courbes à couplages résistantes aux variantes d'attaques basées sur NFS. Construction d'une fonction à délai vérifiable basée sur la cryptographie à base d'isogénies et de couplages. Étude de la cryptanalyse des protocoles à base d'isogénies.

Janvier – Décembre 2019 **Enseignement en L1**. *Université Paris Diderot.*
Travaux pratiques et dirigés de Java (introduction à la programmation 2), 48 heures.
Travaux pratiques de Python (classe préparatoire universitaire aux grandes écoles), 24 heures.

Mars – Septembre 2017 **Stage de M2**. *Méthode GLV en dimension 4 sur les $\mathbb{Q}$–courbes*, Thales.
Sous la direction de Olivier Bernard, Renaud Dubois et Olivier Orcière.
Développement d'un outil de recherche de courbes avec une arithmétique efficace. Implémentation dans une librairie propriétaire de la multiplication de point accélérée par des techniques de décomposition du scalaire, grâce à des endomorphismes de la courbe.

## Publications scientifiques

Janvier 2020 **Cocks-Pinch curves of embedding degrees five to eight and optimal ate pairing computation**. *Aurore Guillevic,* Simon Masson *et Emmanuel Thomé.*
Publication dans la revue Designs, Codes and Cryptography.

Décembre 2019 **Verifiable delay functions from supersingular isogenies and pairings**. *Luca De Feo, Christophe Petit,* Simon Masson *et Antonio Sanso.*
Publication à la conférence Asiacrypt 2019.

## Autres

**Langages informatiques**. *LaTeX, Python, Magma, Java, Git, Bash.*

**Langues**. *Anglais (parlé, écrit), espagnol (débutant).*

**Loisirs**. *Volley-ball, guitare, piano, saxophone, cartomagie.*