

# Jean Kieffer

## Position

---

**CNRS and Université de Lorraine**, Nancy, France:

**Junior researcher** (Chargé de recherche), from January 2024

Research team: Caramba, <https://caramba.loria.fr>

Address: LORIA, Campus Scientifique BP 239  
54506 Vandoeuvre-lès-Nancy, France

Email address: [jean.kieffer@loria.fr](mailto:jean.kieffer@loria.fr)

Home page: <https://members.loria.fr/JKieffer/>

## Education

---

**Université de Bordeaux**, France (2018–2021):

**PhD**, Pure Mathematics, 2021. Title: Higher-dimensional modular equations, applications to isogeny computations and point counting.

**École normale supérieure (ENS) – Sorbonne Université**, Paris, France (2014–2018):

**Master's degree** (M.Sc.), with honors, Fundamental Mathematics (Algebra, Geometry, Number theory), 2017

**Licence** (B.Sc.), with honors, Mathematics, 2015

**Nationwide rank 2** at ENS entrance examination and 1 at École Polytechnique, 2014

## Previous positions

---

**Harvard University**, Cambridge, MA, United States:

**Research Scientist** (Postdoc, Sep. 2021–Dec. 2023) in the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation (PI: Noam D. Elkies)

## Publications

---

- with R. van Bommel, S. Chidambaram and E. Costa: Computing isogeny classes of typical principally polarized abelian surfaces over the rationals. Proceedings of the conference *LMFDB, Computation and Number Theory* (LuCaNT), Contemporary Mathematics, 2023. [arxiv:2301.10118](https://arxiv.org/abs/2301.10118)
- with E. Assaf, A. Babei, B. Breen, E. Costa, J. Duque-Rosero, A. Horawa, A. Kulkarni, G. Molnar, S. Schiavone, and J. Voight. A database of basic numerical invariants of Hilbert modular surfaces. Proceedings of the LuCaNT conference, Contemporary Mathematics, 2023. [arXiv:2301.10302](https://arxiv.org/abs/2301.10302)
- Certified Newton schemes for the evaluation of low-genus theta functions. *Numerical algorithms*, 2022. [arXiv:2203.02000](https://arxiv.org/abs/2203.02000)
- Degree and height estimates for modular equations on PEL Shimura varieties. *Journal of the London Mathematical Society* 105:1314–1361, 2022. [arXiv:2010.10094](https://arxiv.org/abs/2010.10094)
- Upper bounds on the heights of polynomials and rational fractions from their values. *Acta Arithmetica* 203:49–68, 2022. [arXiv:2105.07670](https://arxiv.org/abs/2105.07670)

- Sign choices in the AGM for genus two theta constants. *Publications Mathématiques de Besançon, Algèbre et théorie des nombres*, 37–58, 2022. [arXiv:2010.07579](#)
- with L. De Feo and B. Smith: Towards practical key exchange from ordinary isogeny graphs. In T. Peyrin and S. Galbraith (ed.), *Advances in Cryptology: AsiaCrypt 2018*, Springer, 365–394, 2018. [arXiv:1809.07543](#)

## Preprints

---

- with Noam D. Elkies: a uniform quasi-linear algorithm for evaluating theta functions in any dimension, in preparation.
- Counting points on abelian surfaces over finite fields with Elkies’s method. [arXiv:2203.02009](#)
- Evaluating modular equations for abelian surfaces. [arXiv:2010.10094](#)
- with A. Page and D. Robert: Computing isogenies from modular equations in genus two. [arXiv:2001.04137](#)

## Software

---

- `acb_theta`: a FLINT module featuring quasi-linear time algorithms for evaluating Riemann theta functions in any dimension. [https://github.com/j-kieffer/flint2/tree/acb\\_theta](https://github.com/j-kieffer/flint2/tree/acb_theta)
- `hdme`: a C library for the evaluation of modular equations in dimension 2. <https://github.com/j-kieffer/hdme>.

*Produced January 9, 2024*