

Alexandre GÉLIN

Curriculum vitae

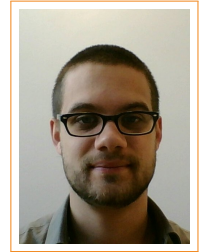
7 rue Leriche

75015 PARIS

+33 622 762 839

✉ alexandre.gelin@uvsq.fr

📄 <https://alexgelin.github.io/>



Education

- 2017 – 2019 **Postdoctoral Researcher**, Laboratoire de Mathématiques de Versailles, UVSQ.
- 2014 – 2017 **PhD**, *Computer science*, Université Pierre et Marie Curie, Paris.
Title: Class Group Computations in Number Fields and Applications to Cryptology.
- 2013 – 2014 **Master**, *Mathematics for cryptography*, École Normale Supérieure de Rennes.
Thesis: On genus 2 curves over \mathbb{C} with special split jacobian.
- 2012 – 2013 **Agrégation**, *Mathematics*, École Normale Supérieure de Rennes, *Rank 92*.
French civil service competitive examination
- 2010 – 2012 **Bachelor**, *Mathematics*, Université Rennes 1.
- 2008 – 2010 **French Preparatory classes**, *Mathematics*, Le Mans.
- 2008 **French Baccalauréat**, Le Mans.

Teaching

- 2017 – 2018 **Teaching assistant**, *Université de Versailles-Saint-Quentin-en-Yvelines*.
Tutorials and practical works for undergraduate students
○ Cryptology (*Fall 2017*)
- 2017 – 2018 **Oral examiner**, *ENC Bessières*, Paris.
Weekly Mathematics oral examination in Preparatory classes
- 2014 – 2017 **Teaching assistant**, *Université Pierre et Marie Curie*, Paris.
Tutorials and practical works for undergraduate students
○ Introduction to cryptology (*Spring 2016 & 2017*)
○ Integrated development environment (*Spring 2016*)
○ Discrete structures (*Fall 2015 & 2014*)
○ Introduction to programming language C (*Spring 2015*)
- 2013 – 2014 **Oral examiner**, *Lycée Joliot Curie*, Rennes.
Weekly Mathematics oral examination in Preparatory classes
- 2013 – 2014 **Teaching assistant**, *INSA*, Rennes.

Languages

- French Native
- English Advanced
- Spanish Intermediate

TOEIC 825 in 2011

Computer skills

OS	Windows, MacOS, Linux
Office suite	Office, OpenOffice, LibreOffice, LaTeX
Software	Magma, Pari-gp, Maple, Sage
Languages	C, C++, bash, Python

Publications

- [1] J.-F. Biasse, T. Espitau, P.-A. Fouque, A. G lin, and P. Kirchner. Computing generator in cyclotomic integer rings. In *Advances in Cryptology - EUROCRYPT 2017, Proceedings*, pages 60–88, 2017.
- [2] A. G lin. *Class Group Computations in Number Fields and Applications to Cryptology*. PhD thesis, Universit  Pierre et Marie Curie Paris, 2017.
- [3] A. G lin and A. Joux. Reducing number field defining polynomials: an application to class group computation. In *LMS Journal of Computation and Mathematics*, volume 19, pages 315–331, 2016.
- [4] A. G lin and A. Joux. On the complexity of class group computations for large-degree number fields. *To appear*, 2017.
- [5] A. G lin and A. Joux. Reducing the complexity for class group computations using small defining polynomials. *To appear*, 2017.
- [6] A. G lin, T. Kleinjung, and A. K. Lenstra. Parametrizations for families of ECM-friendly curves. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2017*, pages 165–171, 2017.
- [7] A. G lin and B. Wesolowski. Loop-abort faults on supersingular isogeny cryptosystems. In *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017, Proceedings*, pages 93–106, 2017.

REVIEWS for CRYPTO 2017

Talks

- Sept. 2017 PhD Defense in Paris
Class Group Computations in Number Fields and Applications to Cryptology
- July 2017 ISSAC in Kaiserslautern
Parametrizations for Families of ECM-Friendly Curves
- July 2017 Journ es Arithm tiques in Caen
Class Group Computations in Number Fields and Applications to Cryptology
- June 2017 PQCrypto in Utrecht
Loop-Abort Faults on Supersingular Isogeny Cryptosystems
- June 2017 Cryptology and Security Seminar in Caen
Param trisations de familles de courbes adapt es   ECM
- May 2017 EuroCrypt in Paris
Computing Generator in Cyclotomic Integer Rings
- April 2017 Journ es Codage et Cryptographie in La Bresse
Calcul du groupe de classes et applications   la cryptologie

- Nov. 2016 Seminar Butte aux Cailles in Paris
Un algorithme de réduction du polynôme de définition d'un corps de nombres et applications au calcul du groupe de classes
- Sept. 2016 ANTS XII in Kaiserslautern
Reducing Number Field Defining Polynomials: An Application to Class Group Computations
- April 2016 LACAL Team Seminar in Lausanne
Class Group Computations in Number Fields
- Feb. 2016 Mid-Term Defense in Paris
Class Group Computations in Number Fields
- May 2015 Workshop VACHES (Abelian varieties, hyperelliptic and Shimura curves) in Paris
Jacobiennes isomorphes à un produit de courbes elliptiques
- May 2015 Workshop VACHES (Abelian varieties, hyperelliptic and Shimura curves) in Paris
Espaces de modules des courbes de genre 2

Interests

- Sport Judo for 20 years (3rd Dan - interregional referee)
- Lecture Thriller and Science-fiction