Razvan Barbulescu

Curriculum Vitae

Institut de mathématiques de Bordeaux
351, cour de la Libération, 33400, Talence, France
(+33) 05400006103
razvan.barbulescu@u-bordeaux.fr
My Webpage

Education

2010–2013 **Master internship and PhD thesis**, *University of Lorraine, Laboratoire LORIA, Nancy.*.

2008–2010 **Agregation of Mathematics and Master of Informatics**, *ENS de Lyon).*

2005-2008 **Classes préparatoires and Bachelor of Mathematics**, *Lycée Louis-le-Grand, Paris, and ENS de Lyon.*.

Research positions

2019–present **Chargé de recherche (permanent researcher)**, *Institut de mathématiques de Bordeaux, CNRS, the LFANT/Canari Inria team.*.

2014–2019 **Chargé de recherche (permanent researcher)**, *Institut de mathématiques de Jussieu – Paris rive gauche, CNRS.*.

2014(Jan-Sept) **Post-doc**, *Laboratoire d'informatique de l'École polytechnique, Palaiseau, the GRACE Inria team.*.

Awards

2024 **Bitdefender fellowship at IMAR Bucharest**.

2014 **Best paper award–Eurocrypt 2014**.

2014 **PhD thesis award of Le Monde**, *awarded to 5 scientific theses in France.*

Summer school lectures

2016 **10 lectures on the number field sieve**, *Indian Statistics Institute, New Delhi, India.*.

2016 **ECC summer school**, *Izmir, Turkey.*.

PhD supervision

2022-2025 **Nicolas Sarkis**, *Arithmetic of Kummer lines*, co-supervised with Damien Robert..

2016-2020 **Sudarshan Shinde**, *Cryptographic applications of modular curves, available online, co-supervised with Pierre-Vincent Koseleff.*

Internship supervision

2014-present **one or more supervision per year.**.

Post-doc responsible

2025 **Xia Wenwen, hybrid-quantum initiative project, co-responsible with Alice Pellet-Mary**.

Responsability positions

2023-present **dissemination correspondent of the math institute in Bordeaux.**.

2022-present **member of the laboratory council of the IMB.**.

2015-present **member of the administration council of Animath.**.

2017-2019 **dissemination correspondent of the IMJ-PRG**.

2013 **representative of the PhD students in the IAEM doctoral school of the Université de Lorraine.**.

Selection comitee

2020 **Maître de conférence position at the University of Paris.**.

Member of the jury for oral contests

2024-2025 **Oral exam of the mathematics agregation (recruitment contest for teachers of high school and the first 2 years of higher education).**.

2019-2023 **Oral exam of the admission contest of ENS de Lyon.**.

Member of the jury for prizes

2024-2025 **member of the jury of the Gilles Kahn prize of Société d'informatique de France.**.

Teaching

2024-2025 **New quantum technologies, L2, University of Bordeaux.**.

2014-2019 **Cryptography lectures at Parisian master of research in informatics, M2, Ecole polytechnique-ENS Paris-ENS Saclay and other institutions.**.

2014-2019 **preparation for the agregation exam, options C and D computer algebra and computer science, M2, Sorbonne université.**.

2014-2019 **preparation for the agregation contest, options C and D computer algebra and computer science, M2, Sorbonne université.**.

2011-2013 **exercise sessions, L3, M1 Télécom Nancy.**.

2012-2018 **olympiad exercises in the Animath association, middle-and-high school level.**.

Scientific dissemination

2020-present **Organiser of the $TFJM^2$ tournament in Bordeaux and member of the jury.**.

2018,2019 **Organiser of a common internship of the French and Romanian team for olympiads in Romania (2018), then of the Romanian, Bulgarian and French teams (2019).**.

2015-2023 **Organiser of the Alkindi contest of cryptanalysis,**, *middle-and-high school students,*, approx. 50000 participants per year..

2015 **One chapter in "5 chercheurs d'avenir",**, *edited by "Le Pommier",*, ISBN 13 : 9782746509375..

2015 **One chapter in "5 chercheurs d'avenir",**, *edited by "Le Pommier",*, ISBN 13 : 9782746509375..

2014-present **Articles in the journals and magazines as Le monde (2014), The Conversation (2021), Le Sud-Ouest (2022).**.

2003 **One of the authors of a book of mathematics for high-school students**, *dited by Repograph Craiova, Romania,*, ISBN 973-8419-50-6..

Razvan Barbulescu

List of publications (see also the HTML version

Institut de mathématiques de Bordeaux
351, cour de la Libération, 33400, Talence, France
(+33) 05400006103
razvan.barbulescu@u-bordeaux.fr
My Webpage

Refereed journal articles

2024 **ECM and the Elliott-Halberstam conjecture for quadratic fields.**, *Razvan Barbulescu and Florent Jouve.*, **Acta Arithmetica**., Instytut Matematyczny PAN..

2022 **A classification of ECM-friendly families using modular curves.**, *Razvan Barbulescu and Sudarshan Shinde.*, **Mathematics of Computation**,, pages 1405–1436. American Mathematical Society..

2020 **Numerical verification of the Cohen-Lenstra-Martinet heuristics and of Greenberg's p-rationality conjecture.**, *Razvan Barbulescu and Jishnu Ray.*, **Journal de Théorie des Nombres de Bordeaux**,, volume 32, pages 159–177. Société Arithmétique de Bordeaux..

2019 **Updating key size estimations for pairings.**, *Razvan Barbulescu and Sylvain Duquesne.*, **Journal of Cryptology**,, volume 32, pages 1298–1336. IACR, Springer Verlag..

2017 **Some mathematical remarks on the polynomial selection in NFS.**, *Razvan Barbulescu and Armand Lachand.*, **Mathematics of Computation**,, volume 86, pages 397–418. American Mathematical Society..

2015 **Selecting polynomials for the Function Field Sieve.**, *Razvan Barbulescu.*, **Mathematics of Computation**,, volume 84, pages 2987–3012. American Mathematical Society..

Refereed conference articles with proceedings

2023 **The special case of cyclotomic fields in quantum algorithms for unit groups.**, *Razvan Barbulescu and Adrien Poulalion.*, In Nadia El Mrabet, Luca de Feo, and Sylvain Duquesne, editors, volume 14064 of LNCS, Progress in Cryptology – **AFRICACRYPT 2023**, page 229, Sousse, Tunisia, July 2023. Ministry of Communication Technologies of Tunisia and in partnership with the IACR, Springer..

2016 **Extended Tower Number Field Sieve**, *Taechan Kim and Razvan Barbulescu.*, In Jonathan Katz Matthew Robshaw, editor, volume 9814 of LNCS, Advances in cryptology – **CRYPTO 2016**–Part I, pages 543–571, Santa Barbara, United States, IACR, Springer..

2015 **The Tower Number Field Sieve.**, *Razvan Barbulescu, Pierrick Gaudry, and Thorsten Kleinjung.*, In Tetsu Iwata and Jung Hee Cheon, editors, volume 9453 of LNCS, Advances in cryptology-**Asiacrypt 2015**, pages 31–58, Auckland, New Zealand. IACR, Springer.

2015 **Improving NFS for the Discrete Logarithm Problem in Non-prime Finite Fields.**, *Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic, and François Morain.*, In Elisabeth Oswald and Marc Fischlin, editors, volume 9056 of LNCS, Advances in cryptology–**EUROCRYPT 2015**, Part I, pages 129–155, Sofia, Bulgaria, IACR, Springer..

2014 **The Multiple Number Field Sieve for Medium and High Characteristic Finite Fields .**, *Razvan Barbulescu and Cécile Pierrot.*, In Algorithmic number theory – **ANTS XI**, Gyeongju, Korea, volume 17 of the LMS Journal of Computation and Mathematics, pages 230–246. London Mathematical Society..

2014 **A heuristic quasi- polynomial algorithm for discrete logarithm in finite fields of small characteristic.**, *Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé.*, In Phong Q. Nguyen and Elisabeth Oswald, editors, Advances in Cryptology – **EUROCRYPT 2014**, volume 8441 of LNCS, pages 1–16, Copenhagen, Denmark, IACR. Springer..

2014 **Discrete logarithm in GF(2^{809}) with FFS.**, *Razvan Barbulescu, Cyril Bouvier, Jérémie Detrey, Pierrick Gaudry, Hamza Jeljeli, Emmanuel Thomé, Marion Videau, and Paul Zimmermann.*, In Hugo Krawczyk, editor, Public-Key Cryptography – **PKC 2014**, volume 8383 of LNCS, Buenos Aires, Argentina, IACR, Springer..

2012 **Finding Optimal Formulae for Bilinear Maps.**, *Razvan Barbulescu, Jérémie Detrey, Nicolas Estibals, and Paul Zimmermann.*, In Ferruh Özbudak and Francisco Rodríguez-Henríquez, editors, International Workshop of the Arithmetics of Finite Fields–**WAIFI 2012**, volume 7369 of LNCS, Bochum, Germany. Ruhr Universitat Bochum..

2012 **Finding ECM-friendly curves through a study of Galois properties**, *Razvan Barbulescu, Joppe W. Bos, Cyril Bouvier, Thorsten Kleinjung, and Peter L. Montgomery.*, In 10th Algorithmic Number Theory Symposium - **ANTS X**, San Diego, United States, July 2012. University of California. volume 1 of the Open book series. 2013. Mathematical Science Publishers..

Invited speaker presentations in peer reviewed conferences

(generally one or several talks are invited)

2024 **Les courbes de Montgomery adaptées à la factorisation d'entiers,**, *Jornées de la fédération Normastic conference page*, **Normastic 2024**.

2018 **An overview on the discrete logarithm problem in finite fields,**, *conference page*, **CAEN 2018**.

2016 **Extended Tower Number Field Sieve: A New Complexity for Medium Prime Case,**, *conference page*, **ECC 2016**.

2016 **A brief history of pairings,**, *In International Workshop on the Arithmetic of Finite Fields,* ***WAIFI 2016****,Lecture notes in computer science, volume 10064. Springer.*.

2014 **A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic,**, *conference page*, **ECC 2014**.

Submitted or unpublished articles

2025 **Models of Kummer lines and Galois representations.**, *Razvan Barbulescu, Damien Robert, Nicolas Sarkis*, available online.

2024 **Regev's attack on hyperelliptic cryptosystems**, *Razvan Barbulescu and Gaëtan Bisson*, available online.

2024 **A comprehensive analysis of Regev's quantum algorithm.**, *Razvan Barbulescu, Mugurel Barcau, Vicentiu Pasol*, available online.

2021 **(Non)practicabilité de l'algorithme classique-quantique de factorisation des entiers,**, *Razvan Barbulescu*, available online.

2021 **A taxonomy of pairings, their security, their complexity**, *Razvan Barbulescu, Nadia El Mrabet and Loubna Ghammam,*, available online.

2015 **Improvements to the number field sieve for non-prime finite fields.**, *Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic and François Morain,*, available online.