Pierre-Jean Spaenlehauer

Research scientist at Inria

Inria Nancy Grand-Est
Équipe CARAMBA
Batiment B
615, rue du jardin botanique
F-54600 Villers-lès-Nancy Cedex
FRANCE
pierre-jean.spaenlehauer@inria.fr
Born on October 26, 1984

Current position

Jan. 2018– **Research scientist (CRCN)**, *Inria Nancy – Grand Est, Team CARAMBA*

Jan. 2016–Dec. 2017 **Research scientist (CR1)**, *Inria Nancy – Grand Est, Team CARAMBA*

Jan. 2014–Dec. 2015 **Young research scientist (CR2)**, *Inria Nancy – Grand Est, Team CARAMEL*

Previous positions

Jul. 2013–Dec. 2013 **Postdoctoral fellow**, *Max Planck Institute for Mathematics, Bonn, Germany*, Mentor: Bernd Sturmfels

Oct. 2012–Jun. 2013 **Postdoctoral fellow**, *University of Western Ontario, London, Canada*, Mentor: Éric Schost

Education

2009–2012 **Ph.D. Thesis**, *UPMC/LIP6/INRIA, SALSA/POLSYS project-team*, Paris,
Subject: Gröbner Bases of Multi-Homogeneous and Determinantal Systems, Applications to Cryptology and Geometry.
Supervisors: Jean-Charles Faugère, Mohab Safey El Din
Dissertation available at
`https://members.loria.fr/PJSpaenlehauer/data/these_spaenlehauer.pdf`

2008–2009 **Master of Computer Science**, *Master Parisien de Recherche en Informatique*, Paris

2005–2008 **Ingénieur Polytechnicien Program**, *École Polytechique*, Palaiseau

2002–2005 **Bachelor of Mathematics**, *University of Strasbourg*

Publications

Journals

Computing a Group Action from the Class Field Theory of Imaginary Hyperelliptic Function Fields.
Antoine Leudière, Pierre-Jean Spaenlehauer. To appear in *Journal of Symbolic Computation*.

Dimension results for extremal-generic polynomial systems over complete toric varieties.
Matías Bender, Pierre-Jean Spaenlehauer. *Journal of Algebra*, 646:156-182, 2024.

Refined Analysis of the Asymptotic Complexity of the Number Field Sieve.
Aude Le Gluher, Pierre-Jean Spaenlehauer, Emmanuel Thomé. *Mathematical Cryptology*, 1(1):71-88, 2021.

A Fast Randomized Geometric Algorithm for Computing Riemann-Roch Spaces.
Aude Le Gluher, Pierre-Jean Spaenlehauer. *Mathematics of Computation*, 89:2399-2433, 2020.

Improved Complexity Bounds for Counting Points on Hyperelliptic Curves.
Simon Abelard, Pierrick Gaudry, Pierre-Jean Spaenlehauer. *Foundations of Computational Mathematics*, 19(3):591-621, 2019.

A Polyhedral Method for Sparse Systems with many Positive Solutions.
Frédéric Bihan, Francisco Santos, Pierre-Jean Spaenlehauer. *SIAM Journal on Applied Algebra and Geometry*, 2(4):620-645, 2018.

A Quadratically Convergent Algorithm for Structured Low-Rank Approximation.
Éric Schost, Pierre-Jean Spaenlehauer. *Foundations of Computational Mathematics*, 16(2):457–492, 2016.

Exact Solutions in Structured Low-Rank Approximation.
Giorgio Ottaviani, Bernd Sturmfels, Pierre-Jean Spaenlehauer. *SIAM Journal on Matrix Analysis and Applications*, 35(4):1521–1542, 2014.

On the Complexity of Computing Critical Points with Gröbner Bases.
Pierre-Jean Spaenlehauer. *SIAM Journal on Optimization*, 24(3):1382–1401, 2014.

On the Complexity of the Generalized MinRank Problem.
Jean-Charles Faugère, Mohab Safey El Din, Pierre-Jean Spaenlehauer. *Journal of Symbolic Computation*, 55:30–58, Elsevier, 2013.

On the Complexity of Solving Quadratic Boolean Systems.
Magali Bardet, Jean-Charles Faugère, Bruno Salvy, Pierre-Jean Spaenlehauer. *Journal of Complexity*, 29:53–73, Elsevier, 2013.

Gröbner Bases of Bihomogeneous Ideals generated by Polynomials of Bidegree (1,1): Algorithms and Complexity.
Jean-Charles Faugère, Mohab Safey El Din, Pierre-Jean Spaenlehauer. *Journal of Symbolic Computation*, 46(4):406–437, Elsevier, 2011.

Conference Proceedings

Counting points on genus-3 hyperelliptic curves with explicit real multiplication.
Simon Abelard, Pierrick Gaudry, Pierre-Jean Spaenlehauer. Proceedings of the Thirteenth Algorithmic Number Theory Symposium, Open Book Series 2, pp. 1–19, 2019.

Critical points computations on smooth varieties: degree and complexity bounds.
Mohab Safey El Din, Pierre-Jean Spaenlehauer. *Proceedings of the International Symposium on Symbolic and Algebraic Computation 2016 (ISSAC 2016)*, p. 183–190.

Computing small certificates of inconsistency of quadratic fewnomial systems.
Jean-Charles Faugère, Pierre-Jean Spaenlehauer, Jules Svartz. *Proceedings of the International Symposium on Symbolic and Algebraic Computation 2016 (ISSAC 2016)*, p. 223–230.

Sparse Gröbner Bases: the Unmixed Case.
Jean-Charles Faugère, Pierre-Jean Spaenlehauer, Jules Svartz. *Proceedings of the International Symposium on Symbolic and Algebraic Computation 2014 (ISSAC 2014)*, p. 178–185.

Critical Points and Gröbner Bases: the Unmixed Case.
Jean-Charles Faugère, Mohab Safey El Din, Pierre-Jean Spaenlehauer. *Proceedings of the International Symposium on Symbolic and Algebraic Computation 2012 (ISSAC 2012)*, p. 162–169.

Computing Loci of Rank Defects of Linear Matrices using Gröbner Bases and Applications to Cryptology.
Jean-Charles Faugère, Mohab Safey El Din, Pierre-Jean Spaenlehauer. *Proceedings of the International Symposium on Symbolic and Algebraic Computation 2010 (ISSAC 2010)*, p. 257–264.
ACM SIGSAM's ISSAC 2010 Distinguished Student Author Award.

Algebraic Cryptanalysis of the PKC'09 Algebraic Surface Cryptosystem.
Jean-Charles Faugère, Pierre-Jean Spaenlehauer. *Proceedings of the 13th International Conference on Practice and Theory in Public Key Cryptography (PKC 2010)*, p. 35–52.

Preprints

Unpublished work

Sparse Polynomial Systems with many Positive Solutions from Bipartite Simplicial Complexes.
Frédéric Bihan, Pierre-Jean Spaenlehauer. arXiv:1510.05622.

Computing the rho constant.
Jérémie Detrey, Pierre-Jean Spaenlehauer, Paul Zimmermann. Pdf available on my webpage.

Invited talks in workshops and conferences

Oct. 16, 2023 — Workshop: Geometry of Polynomial System Solving, Optimization and Topology. Institut Henri Poincaré, Paris, France.

Dec. 8, 2015 — Workshop on Algebra, Geometry and Proofs in Symbolic Computation. Fields Institute, Toronto, Canada.

Aug. 10, 2015 — ICIAM 2015, 3rd Workshop on Hybrid Symbolic-Numeric Methodologies. Beijing, China.

June 1, 2015	SLRA2015: Workshop on Structured Low-Rank Approximation. Grenoble, France.
June 12, 2014	Conference on Effective Moduli Spaces and Applications to Cryptology. Rennes, France.
Mar. 26, 2014	Journées C2. Grenoble, France.
Nov. 28, 2013	Rencontres "Arithmétique de l'Informatique Mathématique" (RAIM). Paris, France.
Jul. 28, 2011	ECRYPT MAYA Workshop 2011. Bochum, Germany.

Posters

ISSAC 2013 **Newton-like Iteration for Determinantal Systems and Structured Low-Rank Approximation.**
Éric Schost, Pierre-Jean Spaenlehauer.

Supervision

Ph.D. students

Oct. 2023–	Cosupervision with Pierrick Gaudry of the Ph.D. of Julien Soumier
Oct. 2021–	Cosupervision with Emmanuel Thomé of the Ph.D. of Antoine Leudière
Sep. 2018–Dec. 2021	Cosupervision with Emmanuel Thomé of the Ph.D. of Aude Le Gluher
Sep. 2015–Sep. 2018	Cosupervision with Pierrick Gaudry of the Ph.D. of Simon Abelard

Internships

Mar.-Sep. 2023	Master's thesis of Julien Soumier
Apr.-Sep. 2021	Master's thesis of Antoine Leudière
Feb-Jun. 2018	Master's thesis of Aude Le Gluher
Mars-Aug. 2017	Cosupervision with Marine Minier of the Master's thesis of Léo Barré
June-Jul. 2017	Internship of Joël Felderhoff (L3, ENS Lyon)
June-Jul. 2016	Internship of Nicolas Levy (L3, ENS Lyon)

Software

rrspace: a software for computing bases of Riemann-Roch spaces and for computing the group law in the Jacobian of curves defined over a finite field. Available at `https://gitlab.inria.fr/pspaenle/rrspace`.

tinyGB: a software implementing Gröbner basis algorithms. Distributed under license LGPLv3. Available at `https://gitlab.inria.fr/pspaenle/tinygb`

NewtonSLRA: a maple package implementing a variant of Newton iteration for Structured Low-Rank Approximation problems. Available on my webpage.

Professional service

Member of the Program Committee of WCC 2024

Member of the Software Presentations Committee of ISSAC 2021

Member of the Program Committee of ISSAC 2019

Member of the Program Committee of ISSAC 2017

Reviews for journals — J. of Algebra, Applicable Algebra in Engineering Communication and Computing, J. of Symbolic Computation, J. of Complexity, J. of Functional Analysis, Mathematical Cryptology ESAIM Mathematical Modelling and Numerical Analysis, Designs Codes and Cryptography, Commentationes Mathematicae Universitatis Carolinae, SIAM J. on Applied Algebra and Geometry, IACR ToSC.

Reviews for conferences — INSCRYPT, MEGA, ICJMS, ISSAC, Asiacrypt, Eurocrypt, SNC, PKC.

2023 – now — Member of the Scientific Committee of the "Journées Nationales de Calcul Formel" (JNCF)

2024 – now — Head of the "Commission des Développements Technologiques du Centre Inria Nancy – Grand Est"

2015 – 2023 — Member of the "Commission des Développements Technologiques du Centre Inria Nancy – Grand Est"

Organization of scientific events

Member of the Organization Committee of the "Rencontres Arithmétiques du GDR Informatique Mathématique" (RAIM 2023), Nov. 6-8, 2023, Nancy, France.

Member of the Organization Committee of the "Journées Nationales de Calcul Formel" (JNCF) in 2022 and 2023 at CIRM, Marseille, France.

Organization with Anne-Lise Charbonnier and Jérémie Detrey of the "Journées Codage et Cryptographie" of the GT-C2 of the GDR-IM, La Bresse, France, 2017.

Organization with Alessio Caminata and Maike Massierer of the minisymposium "Applications of Polynomial System Solving in Cryptology" within the SIAM conference on Applied Algebraic Geometry, Atlanta, US, 2017.

Organization with Maike Massierer of the minisymposium "Applications of Polynomial System Solving in Cryptology" within the SIAM conference on Applied Algebraic Geometry, Daejeon, Corea, 2015.

Service in Ph.D. thesis committee

2024 — External reviewer for Joseph Musleh's Ph.D. thesis, University of Waterloo, Canada.

2022 — Examiner in Maxime Bros' Ph.D. thesis committee, Université de Limoges, France.

2020 — Examiner in Thi Xuan Vu's Ph.D. thesis committee, Sorbonne Université (France) and University of Waterloo (Canada).

2014 — Examiner in Jules Svartz' Ph.D. thesis committee, Université Pierre et Marie Curie, Paris 6, France.

Projects

2015 — Member of PEPS JCJC INSII RiCoRé on polynomial systems for error-correcting codes and robotics.

2016 — Member of PEPS JCJC INSII SPICE on polynomial systems for the discrete logarithm problem on elliptic curves over fields of small characteristic.

2022-2026 Local scientific coordinator for the project PQ-TLS of the PEPR on quantum technologies

Dissemination

2021–2022 Participation to the Math En Jeans program with Cécile Pierrot and Paul Zimmermann, for a group of students (6e/5e) at Collège Vauban (Luxembourg)

2022–2023 Participation to the Math En Jeans program with Paul Zimmermann, for a group of students (6e/5e) at Collège Vauban (Luxembourg)

Teaching

2021–2022 Université de Lorraine, M2: Théorie des nombres, géométrie algébrique et applications à la cryptographie. 12h CM + 6h TD.

2016–2017 Université de Lorraine, M2: Théorie des nombres et applications à la cryptographie. 10h CM.

2015–2016 Université de Lorraine, M2: Introduction à la cryptographie. 10h CM, 12h TD, 8h TP.

2015–2016 Université de Lorraine, M1: Introduction à la cryptographie. 12h CM.

2014–2015 Université de Lorraine, M1: Introduction à la cryptographie. 12h CM.

2011–2012 Université Paris 6, L3: Bases de Données (Databases). 45h TD.

2010–2011 Université Paris 6, L3: Bases de Données (Databases). 45h TD.

2010–2011 Université Paris 6, L2: Programmation par objets (Object-Oriented Programming). 12h TD.

2009–2010 Université Paris 6, L2: Initiation à l'automatisation des tâches (Emacs, Shell, Make). 36h TD.

2009–2010 Université Paris 6, L2: Calcul Scientifique (Scientific Computing). 47h TP.

Languages

French Native

English Fluent

Japanese Beginner, JLPT Level 4