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
`http://www.pjspaenlehauer.net/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

A Polyhedral Method for Sparse Systems with many Positive Solutions.
Frédéric Bihan, Francisco Santos, Pierre-Jean Spaenlehauer. To appear in the *SIAM Journal on Applied Algebra and Geometry*, 2018.

Improved Complexity Bounds for Counting Points on Hyperelliptic Curves.
Simon Abelard, Pierrick Gaudry, Pierre-Jean Spaenlehauer. To appear in *Foundations of Computational Mathematics*, 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. To appear in the *Proceedings of the Thirteenth Algorithmic Number Theory Symposium ANTS-XIII*, 2018.

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

A Fast Randomized Geometric Algorithm for Computing Riemann-Roch Spaces.
Aude Le Gluher, Pierre-Jean Spaenlehauer. arXiv:1811.08237.

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

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

Sep. 2018 –	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
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://gforge.inria.fr/projects/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 program committee	ISSAC 2017, ISSAC 2019
Reviews for journals	Applicable Algebra in Engineering Communication and Computing, J. of Symbolic Computation, J. of Complexity, J. of Functional Analysis, ESAIM Mathematical Modelling and Numerical Analysis, Designs Codes and Cryptography, Commentationes Mathematicae Universitatis Carolinae, SIAM J. on Applied Algebra and Geometry.
Reviews for conferences	INSCRYPT, MEGA, ICJMS, ISSAC, Asiacrypt, SNC, PKC, ICJMS

Organization of scientific events

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

2014	Examiner in Jules Svartz' Ph.D. thesis committee

Teaching

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