Pierre-Jean Spaenlehauer

Research scientist at Inria

Inria Nancy Grand-Est
Équipe CARAMBA
Batiment A
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. 2016– **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 Quadratically Convergent Algorithm for Structured Low-Rank Approximation.
Éric Schost, Pierre-Jean Spaenlehauer. *Foundations of Computational Mathematics*, 1–36, 2015.

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

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.

Preprint

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

Invited talks in workshops and conferences

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

Aug. 6, 2015 SIAM Conference on Applied Algebraic Geometry – Mini-symposium "ML Degree and Critical Points". Daejeon, Korea.

Aug. 3, 2015 SIAM Conference on Applied Algebraic Geometry – Mini-symposium "Algorithms and Complexity in Polynomial System Solving". Daejeon, Korea.

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.
Aug. 2, 2013	SIAM Conference on Applied Algebraic Geometry – Mini-Symposium "Algorithms in Real Algebraic Geometry and its Applications". Fort Collins, Colorado, USA.
Oct. 6, 2011	SIAM Conference on Applied Algebraic Geometry – Mini-Symposium "Algebraic Complexity". Raleigh, North Carolina, USA.
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.

Professional service

Reviews for	INSCRYPT 2009, MEGA 2011, Journal of Symbolic Computation, Journal of Functional Analysis, ISSAC 2014, SNC 2014, ISSAC 2015, PKC 2015, ESAIM, DCC, CMUC, Asiacrypt 2015, ICJMS 2015.
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.

Teaching

2015–2016	M2: Introduction à la cryptographie. 10h CM, 12h TD, 8h TP.
2015–2016	M1: Introduction à la cryptographie. 12h CM.
2014–2015	M1: Introduction à la cryptographie. 12h CM.
2011–2012	L3: Bases de Données (Databases). 45h TD.
2010–2011	L3: Bases de Données (Databases). 45h TD.
2010–2011	L2: Programmation par objets (Object-Oriented Programming). 12h TD.
2009–2010	L2: Initiation à l'automatisation des tâches (Emacs, Shell, Make). 36h TD.
2009–2010	L2: Calcul Scientifique (Scientific Computing). 47h TP.

Languages

French	Native
English	Fluent
Japanese	Beginner, JLPT Level 4

Computer skills

OS	Linux, Unix	Programming	C, C++, Java

Scientific	Magma, Maple, Scilab	Typography	Latex
Web	XHTML, PHP, Javascript	Editor	Emacs, Vim