Gaetan Bisson, Ph.D.

Associate Professor of Mathematics
University of French Polynesia
BP 6570 — 98702 Faaa
French Polynesia

+689 40 866 473
bisson@gaati.org
https://gaati.org/bisson/

RESEARCH INTERESTS

Computational algebra, theoretical computer science, number theory, cryptography.

PROFESSIONAL EXPERIENCE

2013–now	*Associate Professor*	University of French Polynesia
2011–2013	*Research Fellow*	Macquarie University
2011	*Research Intern*	Microsoft Corporation
2008–2011	*Teaching Fellow*	École des mines de Nancy
2007	*Research Intern*	Tokyo Institute of Technology

ACADEMIC EDUCATION

2011	*Doctorate of Philosophy*	Technische Universiteit Eindhoven Institut national polytechnique de Lorraine
2007	*Master of Science*	Université Paris XI
2006	*Agrégation externe*	Ministère de l'éducation nationale
2004–2008	*Élève normalien*	École normale supérieure de la rue d'Ulm

RECREATIONAL INVOLVEMENTS

2013–now	*Divemaster*	CMAS, FFESSM & PADI
2010–now	*Developer*	Arch Linux Distribution
2006–now	*Skipper*	Private sailing cruises

RESEARCH PUBLICATIONS

Gaetan Bisson and Mehdi Tibouchi. "Constructing Permutation Rational Functions From Isogenies."
In: *SIAM Journal on Discrete Mathematics* 32.3 (2018), pp. 1741–1749. DOI: 10.1137/17M1135736.

Gaetan Bisson and Marco Streng. "On polarised class groups of orders in quartic CM-fields."
In: *Mathematical Research Letters* 24.2 (2017), pp. 247–270. DOI: 10.4310/MRL.2017.v24.n2.a1.

Gaetan Bisson. "Computing endomorphism rings of abelian varieties of dimension two."
In: *Mathematics of Computation* 84.294 (July 2015), pp. 1977–1989.
DOI: 10.1090/S0025-5718-2015-02938-X.

Gaetan Bisson. "Computing endomorphism rings of elliptic curves under the GRH."
In: *Journal of Mathematical Cryptology* 5.2 (Apr. 2012), pp. 101–113. DOI: 10.1515/jmc.2011.008.

Gaetan Bisson and Andrew V. Sutherland.
"A low-memory algorithm for finding short product representations in finite groups."
In: *Designs, Codes and Cryptography* 63.1 (Apr. 2012), pp. 1–13. DOI: 10.1007/s10623-011-9527-8.

Gaetan Bisson. "Endomorphism Rings in Cryptography." PhD Thesis. Eindhoven University of Technology, Netherlands & Institut National Polytechnique de Lorraine, France, July 2011. ISBN: 90-386-2519-7.
DOI: 10.6100/IR714676.

Gaetan Bisson, Romain Cosset, and Damien Robert.
AVIsogenies. A library for computing isogenies between abelian varieties.
Registered software IDDN.FR.001.440011.000.R.P.2010.000.10000. Dec. 2010.
URL: http://avisogenies.gforge.inria.fr/.

Gaetan Bisson and Andrew V. Sutherland.
"Computing the endomorphism ring of an ordinary elliptic curve over a finite field." In: *Journal of Number Theory* 131.5 (May 2011): *Elliptic Curve Cryptography*. Ed. by Neal Koblitz and Victor S. Miller, pp. 815–831.
DOI: 10.1016/j.jnt.2009.11.003.

Gaetan Bisson and Takakazu Satoh. "More discriminants with the Brezing-Weng method."
In: *Progress in Cryptology — INDOCRYPT 2008*.
Ed. by Dipanwita R. Chowdhury, Vincent Rijmen, and Abhijit Das. Vol. 5365.
Lecture Notes in Computer Science. Springer, Dec. 2008, pp. 389–399.
DOI: 10.1007/978-3-540-89754-5_30.

SELECTED TALKS

Gaetan Bisson. "Isogeny Graphs and Endomorphism Rings of Ordinary Abelian Varieties."
Invited talk at the conference on L-functions and algebraic varieties.
Poncelet Scientific Center, Higher School of Economics, Russia, Feb. 6, 2018.

Gaetan Bisson. "On Polarized Class Groups of Orders in Quartic CM-Fields."
Invited talk at the conference on Effective moduli spaces and applications to cryptography.
IRMAR, University of Rennes, France, June 12, 2014.

Gaetan Bisson. "On Polarized Class Groups of Orders in Quartic CM-Fields." Invited talk at the conference on Theoretical and Practical Aspects of the Discrete Logarithm Problem — DLP 2014.
Centro Stefano Franscini, ETH Zürich, Switzerland, May 7, 2014.

Gaetan Bisson. "Computing Endomorphism Rings of Abelian Varieties."
Invited talk at the Workshop on Elliptic Curve Cryptography — ECC 2011.
LORIA, University of Nancy, France, Sept. 19, 2011.

EDITORIAL ACTIVITIES

Stéphane Ballet, Gaetan Bisson, Roger Oyono, Renate Scheidler, and Nicolas Thériault, eds.
Advances in Mathematics of Communications 8.4 (2014): *Special issue on GEOCRYPT 2013*.
American Institute of Mathematical Sciences.
URL: `http://www.aimsciences.org/journals/contentsListnew.jsp?pubID=728`.

AWARDED GRANTS

Project Co-Investigator. Constructing Cryptographically Secure Structures.
Supported by STIC AmSud Grant of 22,300 EUR.
CNRS, France, MEAE, France, CAPES, Brasil, CONICYT, Chile, 2019–2020.

Project Chief Investigator. Cryptographic hash functions of number theoretic origins.
Supported by Research Development Grant of 33,000 AUD. Macquarie University, Australia, 2012–2014.

PROFESSIONAL ACTIVITIES

Expert Witness on Cryptography. Court of Appeal of French Polynesia, 2018.

Research Advisor. Graduate internship of Garry Terii. University of French Polynesia, 2016.

Thesis Advisor. Master's dissertation in Education of Roger Doom. University of French Polynesia, 2015.

Thesis Reviewer. Honours dissertation of Alex Fowler. University of Auckland, 2014.

EVENT COORDINATION

Conference Organizer. Arithmetic, Geometry, Cryptography and Coding Theory (AGC2T'19).
CIRM, University of Marseille, France, 2019.

Conference Organizer. Non-Archimedean Analytic Geometry: Theory and Practice.
University of French Polynesia, 2015.

Conference Organizer. Geometry and Cryptography (GeoCrypt'13). University of French Polynesia, 2013.

Seminar Coordinator. ACAC Group. Macquarie University, Australia, 2012–2013.

Program Committee Member. Manifestation des Jeunes Chercheurs en Sciences et Technologies de l'Information et de la Communication (MajecSTIC'10). University of Bordeaux, France, 2010.

UNIVERSITY SERVICE

Director of Teaching. CUPGE-MP elite curriculum. University of French Polynesia, 2017–2019.

Deputy Director of Teaching. Semesters 5 & 6, undergraduate mathematics.
University of French Polynesia, 2015–2018.

Technical Committee Member. University of French Polynesia, 2014–2016.

Scientific Council Member. École Normale Supérieure, France, 2006–2007.

Student Body Representative. École Normale Supérieure, France, 2004–2006.

LECTURE NOTES

Gaetan Bisson. *Mathématiques générales*. Semester 1, undergraduate mathematics. Taught Aug.–Dec. 2013.
University of French Polynesia.

Gaetan Bisson. *Analyse*. Semester 2, undergraduate mathematics. Taught Jan.–May 2014–2016.
University of French Polynesia.

Gaetan Bisson. *Unix/Linux*. Semester 2, undergraduate computer science. Taught Jan.–May 2014–2015.
University of French Polynesia.

Gaetan Bisson. *Arithmétique – Cryptographie*. Semester 3, undergraduate mathematics.
Taught Aug.–Dec. 2015–2016. University of French Polynesia.

Gaetan Bisson. *Algèbre linéaire 2*. Semester 3, undergraduate mathematics. Taught Aug.–Dec. 2013–2014.
University of French Polynesia.

Gaetan Bisson. *Géométrie*. Semester 4, undergraduate mathematics. Taught Jan.–May 2016–2018.
University of French Polynesia.

Gaetan Bisson. *Équations différentielles*. Semester 5, undergraduate mathematics. Taught Aug.–Dec. 2013–2018.
University of French Polynesia.

Gaetan Bisson. *Calcul formel*. Semester 6, undergraduate mathematics. Taught Jan.–May 2014–2019.
University of French Polynesia.

Gaetan Bisson. *Initiation à la recherche*. Semester 2, graduate mathematics. Taught Jan.–May 2015.
University of French Polynesia.

Gaetan Bisson. *Préparation à l'agrégation interne*. Semester 3, graduate mathematics. Taught Aug.–Dec. 2015.
University of French Polynesia.

Gaetan Bisson. *Logique et fondements*. Semester 1, CUPGE-MP elite curriculum. Taught Aug.–Dec 2017–2018. University of French Polynesia.

Gaetan Bisson. *Informatique*. Semester 1–4, CUPGE-MP elite curriculum. Taught 2017–2019. University of French Polynesia.

LESSON SERIES

Gaetan Bisson. *Pépites algorithmiques*. *Factorisation d'entiers*. Semester 1, graduate engineering. Taught May 2009. École des Mines de Nancy.

Gaetan Bisson. *Séminaire Informatique et Internet*. *Systèmes d'exploitation de type Unix*. Semester 5, undergraduate engineering. Taught Sept. 2009–2010. École des Mines de Nancy.

Gaetan Bisson. *Séminaire Informatique et Internet*. *Composition de documents avec LaTeX*. Semester 5, undergraduate engineering. Taught Sept. 2009–2010. École des Mines de Nancy.

Gaetan Bisson. *Pépites algorithmiques*. *Algorithmique des graphes*. Semester 1, graduate engineering. Taught Mar. 2010. École des Mines de Nancy.

MISCELLANEOUS WRITINGS

Gaetan Bisson, François Garillot, Thierry Martinez, and Sam Zoghaib. *Langages formels, calculabilité et complexité*. Ed. by Olivier Carton. Semester 5, undergraduate computer science. École Normale Supérieure, Apr. 2005.

Gaetan Bisson. *Cours aux carrés*. *Autour des nombres et des polynômes de Bernoulli*. Ed. by Don Zagier. Semester 1, graduate mathematics. École Normale Supérieure, May 2006.

Gaetan Bisson. *Colles de mathématiques en classes de MPSI & MP**. Semester 1–4, undergraduate mathematics. Lycées Louis-le-Grand and Chaptal, Jan. 2008.

Gaetan Bisson. *Colles de mathématiques en CUPGE-MP*. Semester 1–4, undergraduate mathematics. Taught 2017–2019. University of French Polynesia.

PUBLIC ENGAGEMENTS

Gaetan Bisson. "L'invité café." Interview for the "La matinale" radio show. La Première, Polynésie française, Mar. 14, 2019. URL: `https://la1ere.francetvinfo.fr/polynesie/emissions-radio/l-invite-cafe/invite-cafe-gaetan-bisson-14032019-689826.html`.

Gaetan Bisson. "Construire et attaquer des codes secrets." Contributed talk to the "Savoirs pour tous" talk series. University of French Polynesia, Mar. 14, 2019. URL: `http://www.upf.pf/node/6346`.