Gaetan Bisson

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

Mathematical aspects of computer science, particularly applications of number theory to cryptography.

MAIN RESPONSIBILITIES

CURRENTLY AT THE UNIVERSITY OF FRENCH POLYNESIA

2025–2029	*Vice-Chairman*	University Board
2021–2026	*Principal Investigator*	MELODIA Project (ANR Grant)
2017–now	*Coordinator*	CUPGE-MP elite curriculum
2024–now	*Managing Editor*	Polynesian Journal of Mathematics

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

2023	*Habilitation*	University of French Polynesia
2011	*Doctor 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

RESEARCH PUBLICATIONS

Samuele Anni, Gaetan Bisson, Annamaria Iezzi, Elisa Lorenzo García, and Benjamin Wesolowski. *On the computation of endomorphism rings of abelian surfaces over finite fields.* 2025. URL: http://arxiv.org/abs/2503.08925

Yaiza Bermudez, Gaetan Bisson, Iñaki Esnaola, and Samir M. Perlaza. *Proofs for Folklore Theorems on the Radon-Nikodym Derivative.* 2025. URL: https://www.arxiv.org/abs/2501.18374

Samir M. Perlaza and Gaetan Bisson. *Variations on the Expectation Due to Changes in the Probability Measure.* 2025. URL: https://arxiv.org/abs/2502.02887

Razvan Barbulescu and Gaetan Bisson. *Regev's attack on hyperelliptic cryptosystems.* 2024. URL: https://eprint.iacr.org/2024/2004

Samir Perlaza, Gaetan Bisson, Iñaki Esnaola, Alain Jean-Marie, and Stefano Rini. *Empirical Risk Minimization with Relative Entropy Regularization.* IEEE Transactions on Information Theory, volume 70.7, pages 5122–5161. 2024. DOI: 10.1109/TIT.2024.3365728

Alp Bassa, Gaetan Bisson, and Roger Oyono. *Iterative constructions of irreducible polynomials from isogenies.* Finite Fields and their Applications, volume 97, reference 102429. 2024. DOI: 10.1016/j.ffa.2024.102429

Samir Perlaza, Iñaki Esnaola, Gaetan Bisson, and H. Vincent Poor. *On the Validation of Gibbs Algorithms: Training Datasets, Test Datasets and their Aggregation.* IEEE International Symposium on Information Theory — ISIT 2023, pages 328 – 333. 2023. DOI: 10.1109/ISIT54713.2023.10206506

Gaetan Bisson and Roger Oyono. *On the vaccination threshold for Covid-19 in French Polynesia.* Pacific Health, volume 5. 2022. DOI: 10.24135/pacifichealth.v5i.59

Samir Perlaza, Gaetan Bisson, Iñaki Esnaola, Alain Jean-Marie, and Stefano Rini. *Empirical Risk Minimization with Relative Entropy Regularization: Optimality and Sensitivity Analysis.* IEEE International Symposium on Information Theory — ISIT 2022, pages 684–689. 2022. DOI: 10.1109/ISIT50566.2022.9834273

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

Gaetan Bisson and Mehdi Tibouchi. 同種写像を用いた置換有理関数の生成手法. IEICE Symposium on Cryptography and Information Security — SCIS 2017, reference 3B2-3. 2017.

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

Gaetan Bisson. *Computing endomorphism rings of abelian varieties of dimension two.* Mathematics of Computation, volume 84.294, pages 1977–1989. 2015. DOI: 10.1090/S0025-5718-2015-02938-X

Gaetan Bisson. *Computing endomorphism rings of elliptic curves under the GRH.* Journal of Mathematical Cryptology, volume 5.2, pages 101–114. 2012. DOI: 10.1515/jmc.2011.008

Gaetan Bisson and Andrew V. Sutherland. *A low-memory algorithm for finding short product representations in finite groups.* Designs, Codes and Cryptography, volume 63, pages 1–13. 2012. DOI: 10.1007/s10623-011-9527-8

Gaetan Bisson and Andrew V. Sutherland. *Computing the endomorphism ring of an ordinary elliptic curve over a finite field.* Journal of Number Theory, volume 131.5, pages 815–831. 2011. DOI: 10.1016/j.jnt.2009.11.003

Gaetan Bisson and Takakazu Satoh. *More discriminants with the Brezing-Weng method.* Progress in Cryptology — INDOCRYPT 2008, Springer LNCS, volume 5365, pages 389–399. 2008. DOI: 10.1007/978-3-540-89754-5_30

COMPUTER SOFTWARE

Gaetan Bisson, Romain Cosset, and Damien Robert. *AVIsogenies, a library for computing isogenies between abelian varieties.* 2010. URL: https://gitlab.inria.fr/roberdam/avisogenies/

ACADEMIC MANUSCRIPTS

Gaetan Bisson. *Contributions aux aspects effectifs des variétés abéliennes et à leurs applications.* Habilitation thesis, University of French Polynesia. 2023.

Gaetan Bisson. *Endomorphism Rings in Cryptography.* Doctoral thesis, Eindhoven University of Technology & Institut National Polytechnique de Lorraine. 2011. ISBN: 90-3862-519-7 DOI: 10.6100/IR714676

EDITORIAL ACTIVITIES

Gaetan Bisson, Philippe Lebacque, and Roger Oyono. *Actes du colloque international «Géométrie algébrique, Théorie des nombres et Applications» (GTA 2021).* Publications mathématiques de Besançon, volume 2024. ISBN: 2-38549-112-5

Stéphane Ballet, Gaetan Bisson, and Irene Bouw. *Arithmetic, Geometry, Cryptography and Coding Theory.* Contemporary Mathematics, volume 770. 2021. ISBN: 14-7045-426-2 DOI: 10.1090/conm/770

Stéphane Ballet, Gaetan Bisson, Roger Oyono, Renate Scheidler, and Nicolas Thériault. *Special issue on GEOCRYPT 2013.* Advances in Mathematics of Communications, volume 8.4. 2014. ISSN: 1930-5346

INVITED TALKS

Gaetan Bisson. *Constructing irreducible polynomials using isogenies.* Computations and their uses in number theory. CIRM, University of Marseille, France. 1 March 2023.

Gaetan Bisson. *Isogeny Graphs and Endomorphism Rings of Ordinary Abelian Varieties.* Conference on L-functions and algebraic varieties. Poncelet Scientific Center, Higher School of Economics, Russia. 6 February 2018.

Gaetan Bisson. *On Polarized Class Groups of Orders in Quartic CM-Fields.* Conference on Effective moduli spaces and applications to cryptography. IRMAR, University of Rennes, France. 12 June 2014.

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

Gaetan Bisson. *Computing Endomorphism Rings of Abelian Varieties.* Workshop on Elliptic Curve Cryptography — ECC 2011. LORIA, University of Nancy, France. 19 September 2011.

STUDENT SUPERVISION

Keva Djambaé, PhD Candidate, University of French Polynesia. 2024 – now. (With David Kohel.)

Stefano Marseglia, postdoctoral researcher, University of French Polynesia. 2024.

Emiliano Torti, postdoctoral researcher, University of French Polynesia. 2023–2025. (With Alexander Rahm.)

Marama Simoneau, L3 Candidate, ENSAE Paris. 2023.

Hugo Nartz, PhD Candidate, University of French Polynesia. 2022. (With Alexander Rahm.)

Nathan Chiche, M2 Candidate, Sorbonne University. 2022.

Garry Terii, M1 Candidate, University of Lyon. 2016.

AWARDED GRANTS

AS PRINCIPAL INVESTIGATOR

Methods for Low Dimensional Abelian Varieties — MELODIA. Supported by AAPG Grant of EUR 160,000. Agence Nationale de la Recherche, France. 2021–2026.

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

AS CO-INVESTIGATOR

Cryptography for everyone — Crypto4All. Supported by STIC AmSud Grant of EUR 19,600. CNRS & MEAE, France; ANID, Chile; ANII, Uruguay. 2019–2021.

Calculateur haute performance — AI'A. Supported by AESEP Grant of EUR 33,350. Gouvernement de la Polynésie française. 2022.

Constructing Cryptographically Secure Structures — C2S2. Supported by STIC AmSud Grant of EUR 25,125. CNRS & MEAE, France; CAPES, Brasil; CONICYT, Chile. 2019–2021.

Courbes Hyperelliptiques : Isogénies et Comptage — CHIC. Supported by BLAN Grant of EUR 380,000. Agence Nationale de la Recherche, France. 2010–2014.

EVENT COORDINATION

AS GENERAL CHAIR

René 25. A conference celebrating the research interests of René Schoof. University of French Polynesia. 2025.

Géométrie algébrique, Théorie des nombres et Applications — GTA. University of French Polynesia. 2021.

Arithmetic, Geometry, Cryptography and Coding Theory — AGC2T. CIRM Luminy, France. 2019.

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

Geometry and Cryptography — GeoCrypt. University of French Polynesia. 2013.

AS PROGRAM COMMITTEE MEMBER

Algèbre, géométrie algébrique et applications à la théorie de l'information — École CIMPA. University of Douala, Cameroon. 2024.

Manifestation des Jeunes Chercheurs en Sciences et Technologies de l'Information et de la Communication — MajecSTIC. University of Bordeaux, France. 2010.

SCIENTIFIC EXPERTISE

Expert witness on cryptography. Court of appeals of French Polynesia. 2018.

Scientific reviewer. 2008 – now.

- For book proposals: *CRC Press*.
- For grant proposals: *Université Côte d'Azur*.
- For honours dissertations: *University of Auckland*.
- For research journals: *Advances in Mathematics of Communications*, *Finite Fields and Their Applications*, *International Journal of Number Theory*, *Journal of Algebra*, *Journal of Cryptology*, *Journal of Mathematical Cryptology*, *Journal of Number Theory*, *Journal of Pure and Applied Algebra*, *LMS Journal of Computation and Mathematics*, *Mathematics of Computation*, *Research in Number Theory*.
- For research conferences: *Algorithmic Number Theory Symposium (ANTS)*, *Conference on Algebraic Informatics (CAI)*, *Cryptology and Information Security in Latin America (LATINCRYPT)*, *International Cryptology Conference (CRYPTO)*, *LMFDB, Computation, and Number Theory (LUCANT)*, *Post-Quantum Cryptography (PQCRYPTO)*, *Practice and Theory in Public Key Cryptography (PKC)*, *Selected Areas in Cryptography (SAC)*, *Theory and Application of Cryptology and Information Security (ASIACRYPT)*, *Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, *Theory and Applications of Cryptology (AFRICACRYPT)*, *Theory of Cryptography Conference (TCC)*, *Western European Workshop on Research in Cryptology (WEWORC)*.

PROFESSIONAL ACTIVITIES

Managing Editor. Polynesian Journal of Mathematics. 2024–now.

Correspondent for the Pacific region. Groupe de travail C2 (codage & cryptographie) des groupements de recherche n°673 (informatique mathématique) et n°2046 (sécurité informatique), CNRS. 2023–now.

Chairman of the board of examiners.

- Baccalauréat professionnel, spécialité sécurité, procédure VAE. 2025.
- Baccalauréat professionnel, spécialité logistique, procédure VAE. 2023.
- Baccalauréat professionnel, spécialité SPVL, procédure VAE. 2022.
- Baccalauréat technologique, séries ST2S, STD2A, STHR & STL. 2021.
- Baccalauréat général, série scientifique. 2020.

Member of hiring committees.

- For 1 associate professor (MCF).
- For 2 visiting associate professors (délégation MCF), once as chairman.
- For 2 postdoctoral researchers as chairman.
- For 10 teaching fellows (PRAG), including 7 as chairman.
- For 8 research associates (ATER), including 5 as chairman.
- For 4 teaching associates (CDD-E), including 2 as chairman.

UNIVERSITY SERVICE

AT THE UNIVERSITY OF FRENCH POLYNESIA

Vice-Chairman. University Board. 2025–2029.

Director. Department of Science. 2022–2025.

Deputy Director. GAATI Laboratory. 2019–2025.

Coordinator. CUPGE-MP elite curriculum. 2017–now.

Elected member. Research Council. 2021–2025.

Elected member. Technical Committee. 2014–2016.

AT MACQUARIE UNIVERSITY

Coordinator. ACAC Group Seminar. 2012–2013.

AT THE ÉCOLE NORMALE SUPÉRIEURE

Member of the Scientific Council. 2006–2007.

Student Body Representative (DG). 2004–2006.

LECTURE NOTES

AT THE UNIVERSITY OF FRENCH POLYNESIA

2017–now	CUPGE MP1&2	*Informatique*
2017–now	CUPGE MP1	*Logique et fondements*
2013–now	Math L3	*Calcul formel*
2013–2020	Math L3	*Équations différentielles*
2015–2017	Math L2	*Géométrie*
2015–2016	Math L2	*Arithmétique — Cryptographie*
2015	Math M2	*Préparation à l'agrégation interne*
2013–2015	Math L1	*Analyse*
2013–2014	CS L1	*Unix/Linux*
2014	Ed M1	*Initiation à la recherche*
2013–2014	Math L2	*Algèbre linéaire 2*
2013	Math L1	*Mathématiques générales*

AT THE ÉCOLE DES MINES DE NANCY

2009–2010	Eng L3	*Systèmes d'exploitation de type Unix*
2009–2010	Eng L3	*Composition de documents avec LaTeX*
2009	Eng L3	*Algorithmique des graphes*
2008	Eng L3	*Factorisation d'entiers*

MISCELLANEOUS WRITINGS

Colles de mathématiques en CUPGE-MP. University of French Polynesia. 2017–now.

Colles de mathématiques en classes de MPSI & MP.* Lycées Louis-le-Grand et Chaptal. 2005–2006.

Autour des nombres et des polynômes de Bernoulli. Based on a course by Don Zagier. École normale supérieure. 2005.

Langages formels, calculabilité et complexité. With François Garillot, Thierry Martinez and Sam Zoghaib. Based on a course by Olivier Carton. École normale supérieure. 2004.

OUTREACH EFFORTS

Interview for the "Le Journal" TV news program. TNTV. 26 Sep 2021.

Interview for the "La matinale" radio show. Polynésie La Première. 18 Feb 2021.

Delegate to the "Journée nationale des sciences de l'ingénieur au féminin." Lycée de Raiatea. 3 Dec 2020.

Speaker at the "Special conferences" conference series. French Polynesia IT security group — CLUSIR. 20 Oct 2020.

Speaker at the "Savoirs pour tous" conference series. University of French Polynesia. 14 Mar 2019.

Interview for the "La matinale" radio show. Polynésie La Première. 14 Mar 2019.

HONORS AND AWARDS

Promoted "hors classe" associate professor. 2023.

Recipient of the RIPEC C3 performance bonus. 2023–2026.