Christelle Vincent

The University of Vermont
Department of Mathematics and Statistics
christelle.vincent@uvm.edu
`http://www.uvm.edu/~cvincen1`

Appointments

Associate Professor, University of Vermont	September 2023 onward
Assistant Professor, University of Vermont	January 2016 - August 2023
Visiting Scholar, Télécom ParisTech	June 2016
Visiting Scholar, ICERM	Fall 2015
Lecturer, Stanford University	2012–2015

Grants and other funding

Travel Support for Mathematicians Simons Foundation	2023-2028
Mathematical Endeavors Revitalization Program Association for Women in Mathematics	2023-2024
Rethinking Number Theory Research Community American Institute of Mathematics	2022 onwards
NSF individual grant DMS-1802323 (PI) *Applications to cryptography of the construction of curves from modular invariants*	2018–2022
Thomas Jefferson Fund of the FACE Foundation (Co-PI) *Effective constructions of genus 3 CM curves and applications to cryptography*	2018–2022
Collaborate@ICERM, *Solving the S-unit equation*	2022
NSF conference grant, Connecticut Summer School in Number Theory (Co-PI)	2020–2023
NSA conference grant, Connecticut Summer School in Number Theory (Co-PI)	2020–2023
NSF conference grant, Canadian Number Theory Association meeting (Co-PI)	2018
Collaborate@ICERM, *Solving the S-unit equation*	2017

Graduate students

Annie Zhang, MSc 2023, *An Analysis of a Linear Algebra Based Group Key Exchange Protocol*
Marcus Elia, PhD 2021, *Loss of Precision in Implementations of the Toom-Cook Algorithm*
Garvin Gaston, MSc 2017, *Hilbert Class Fields of Imaginary Quadratic Fields and Reflex Fields of Certain Sextic CM Fields*

Honors theses advised

Alec Critten, BS 2021, *Characterizing Insecure Error Distributions for Various RLWE Problems*
Grace Brill, BS 2019, *Maximal Artin-Schreier Curves for Coding Theory*
Rosie Steinberg, BA 2018, *Enumerating Curves of Genus 2 over Finite Fields*

Unusual teaching experience

Lecturer at the Undergraduate Summer School of the PCMI Mini-course on Introduction to mathematical cryptography	July-August 2022
Organizer and lecturer at the Connecticut Summer School in Number Theory Mini-course on Local Fields	June 2022
Organizer and lecturer at the Summer Program for Inclusive Excellence in Mathematics Mini-course entitled Topology Done Quick	June 2021
Lecturer at the Governor's Institute of Vermont	June 2018
Invited lecturer at the Connecticut Summer School in Number Theory Mini-course on Function Field Arithmetic	May 2018

Publications

S. Ionica, P. Kılıçer, K. Lauter, E. Lorenzo García, A. Mânzăţeanu, C. Vincent, Determining the primes of bad reduction of CM curves of genus 3, submitted for publication.

J. Booher, R. Bowden, J. Doliskani, T. B. Fouotsa, S. D. Galbraith, S. Kunzweiler, S.-P. Merz, C. Petit, B. Smith, K. E. Stange, Y. B. Ti, C. Vincent, J. F. Voloch, C. Weitkämper, L. Zobernig, Failing to hash into supersingular isogeny graphs, extended abstract has appeared in *CFAIL 2022*, full article submitted for publication.

T. Dupuy, K. Kedlaya, D. Roe, C. Vincent, Counterexamples to a conjecture of Ahmadi and Shparlinski, *Experimental Mathematics*, vol. 32 (3), 2023, pp. 540-544

T. Stevens, C. Skalka, C. Vincent, J. Ring, S. Clark, J. Near, Efficient differentially private secure aggregation for federated learning via hardness of Learning With Errors, 31st USENIX Security Symposium (USENIX Security 22), 2022, pp. 1379–1395.

T. Dupuy, K. Kedlaya, D. Roe, C. Vincent, Isogeny classes of abelian varieties over finite fields in the LMFDB, *Arithmetic geometry, number theory, and computation*, Simons Symposia, Springer, 2021, pp. 375-448.

A. Alvarado, A. Koutsianas, B. Malmskog, C. Rasmussen, C. Vincent, M. West, A robust implementation for solving the S-unit equation and several applications, *Arithmetic geometry, number theory, and computation*, Simons Symposia, Springer, 2021, pp. 1-41.

Appendix for J.-C. Lario and A. Somoza, An inverse Jacobian algorithm for Picard curves, *Research in Number Theory*, Vol. 7 (2), 2021, 23 pp.

S. Ionica, P. Kılıçer, K. Lauter, E. Lorenzo García, M. Massierer, A. Mânzăţeanu, C. Vincent, Modular invariants for genus 3 hyperelliptic curves. *Research in Number Theory*, Vol. 5 (1), 2019, 22 pp.

C. Vincent, A characterization of the $U(\Omega, m)$ sets of a hyperelliptic curve as Ω and m vary. *Advances in the Mathematical Sciences*, pp. 79–95, Association for Women in Mathematics Series, Vol. 15, Springer, 2018.

J. S. Balakrishnan, S. Ionica, K. Lauter, C. Vincent, Constructing genus 3 hyperelliptic Jacobians with complex multiplication. *LMS Journal of Computation and Mathematics*, Vol. 19 (A), 2016, pp. 283–300.

I. Bouw, W. Ho, B. Malmskog, R. Scheidler, P. Srinivasan, C. Vincent, Zeta functions of a class of Artin-Schreier curves with many automorphisms. *Directions in Number Theory*, pp. 87–124, Association for Women in Mathematics Series, Vol. 3, Springer, 2016.

C. Vincent, Weierstrass points on the Drinfeld modular curve $X_0(\mathfrak{p})$, *Research in the Mathematical Sciences*, Vol. 2 (10), 2015.

Appendix B for Z. Yun, Galois representations attached to moments of Kloosterman sums and conjectures of Evans. *Compositio Mathematica*, Vol. 151, 2015, pp. 68–120.

C. Vincent, On the trace and norm maps from $\Gamma_0(\mathfrak{p})$ to $\mathrm{GL}_2(A)$. *Journal of Number Theory*, Vol. 142, 2014, pp. 18-43.

C. Vincent, Drinfeld modular forms modulo $\mathfrak{p}$. *Proceedings of the American Mathematical Society*, Vol. 138 (12), 2010, pp. 4217–4229.

M. Desgroseilliers, B. Larose, C. Malvenuto, C. Vincent, Some results on two conjectures of Schützenberger. *Canadian Mathematical Bulletin*, Vol. 53 (3), 2010, pp. 453–465.

Service and outreach

Organizer and lecturer, Connecticut Summer School in Number Theory	February–June 2024
Member of the program committee, Algorithmic Number Theory Symposium	February–July 2024
Planned the *Thinking session: A better math community* Special session on Rethinking Number Theory Joint Mathematics Meetings	January 2023
Merit review panelist for the National Science Foundation	2022
Organizer and lecturer, Connecticut Summer School in Number Theory	February–June 2022
Organizer, AMS Special Session on Rethinking Number Theory	June 2021–April 2022
Panelist on inclusion, École d'été JCCA in Paris	August 2021
Organizer, Summer Program for Inclusive Excellence	February–June 2021
Organizer, Rethinking Number Theory Workshop	July–October 2020
Member of the program committee, Algorithmic Number Theory Symposium	February–July 2020
Organizer, Connecticut Summer School in Number Theory	February–June 2020
Project leader, Women in Sage	August 2019
Visiting advisor, Mathematical Research Communities Explicit Methods in Arithmetic Geometry in Characteristic p	June 2019
Member of the program committee, Algorithmic Number Theory Symposium	February–July 2018
Member of the scientific committee, Canadian Number Theory Association	February–July 2018
Organizer, Witt Vectors, Deformations, and Absolute Geometry Conference	January–July 2018
Faculty advisor to UVM's Math Club	September 2016–May 2018
Organizer, Sage Days 87 workshop	January–July 2017
Organizer, Kummer Classes and Anabelian Geometry Conference	January–September 2016
Organizer, AMS Special Session on Number Theory and Cryptography	June 2015–January 2016

Invited Presentations

What can theta functions tell us about abelian threefolds?

Special Session on Cryptography and Related Fields Joint Mathematics Meetings	January 2024
Special Session on Computational Number Theory Applied Mathematics, Modelling and Computational Science Conference Series	August 2023

The cryptography of the future: lattice-based cryptography

Five Colleges Number Theory Seminar	November 2023

Post-quantum cryptography: What is it and why?

Bowdoin College Number Theory and Cryptography class Invited lecturer	November 2023
Upstate Number Theory Conference Plenary speaker	October 2021

Cryptography, a hack, and a backdoor

Math Majors Seminar, Bowdoin College	November 2023
Debate Club talk on cryptography, University of Vermont	October 2018

Exploring angle rank using the LMFDB

VaNTAGe Math Seminar	March 2022

On the equidistribution of joint shapes of fields and their resolvents

Special Session on Analytic Methods in Arithmetic Statistics Spring Eastern Sectional Meeting of the AMS	February 2022

Computing hyperelliptic modular invariants from period matrices

Session on Algebra and Number Theory XXIII International Symposium of Mathematical Methods Applied to Sciences	February 2022
Session on Computational Number Theory MAA MathFest	August 2021
Special Session on Coding Theory, Cryptography, and Number Theory Fall Southeastern Sectional Meeting of the AMS	October 2020
Special Session on Algorithms, Experimentation, and Applications in Number Theory Joint Mathematics Meetings	January 2020
Arithmetic, Geometry, Cryptography and Coding Theory	June 2019
Invited Session on Women in Numbers AWM Research Symposium	April 2019
Special Session on Special Values of L-functions and Arithmetic Invariants in Families Spring Eastern Sectional Meeting of the AMS	April 2019
Special Session on Number Theory, Arithmetic Geometry, and Computation Joint Mathematics Meetings	January 2019

Une banque de données sur les classes d'isogénie des variétés abéliennes sur les corps finis

CMS Summer Meeting Special session Amicale de théorie des nombres en hommage à Robert Langlands	June 2021

On the distribution of joint shapes of number fields

Quebec-Vermont Number Theory Seminar	September 2020
Number Theory Seminar, University of Oregon	June 2020
Number Theory Seminar, University of Illinois–Urbana-Champaign Note: This talk was canceled due to COVID.	April 2020
Number Theory Seminar, Arizona State University	November 2018
Number Theory Seminar, CU Boulder	November 2018

Constructing curves of genus 3 with CM Jacobians

Front Range Number Theory Day Plenary speaker	September 2020
Modular Forms, Arithmetic, and Women in Mathematics Plenary speaker	November 2019

Sage and the L-functions and modular forms database

AMS MRC on Explicit Methods in Arithmetic Geometry in Characteristic p Plenary speaker	June 2019

A lightning-fast survey of post-quantum cryptography

CTNT Research Conference	May 2018

The number theory behind cryptography

UVM Math Club	April 2018
Undergraduate Seminar, Norwich University	October 2017
Vermont Math Day	April 2017
Spuyten Duyvil Undergraduate Mathematics Conference Keynote address	April 2016

Constructing hyperelliptic curves of genus 3 whose Jacobian has CM

Number Theory Seminar, University of Virgina	October 2017
Special Session on Computational Number Theory Applied Mathematics, Modeling and Computational Science Conference	August 2017

Invited Conference and Seminar Talks (continued)

Constructing hyperelliptic curves of genus 3 whose Jacobian has CM (continued)

Number Theory Seminar, University of Georgia	April 2017
Number Theory Seminar, Tufts University	April 2017
Number Theory Seminar, University of Rochester	March 2017
Number Theory Seminar, University of Pennsylvania	March 2017

Computing equations of hyperelliptic curves whose Jacobian has CM

Number Theory Seminar, Boston University	October 2017
Special Session on Algebraic Curves and their Applications Fall Southeastern Sectional Meeting of the AMS	September 2017
Special Session on Women in Sage AWM Research Symposium	April 2017
Five College Number Theory Seminar, Amherst	April 2017
Number Theory Seminar, University of Michigan	December 2016
Number Theory Seminar, MIT	October 2016
Séminaire du Laboratoire MIS Université de Picardie Jules Verne	May 2016
Séminaire de la Butte-aux-Cailles Télécom ParisTech	May 2016
Number Theory Seminar, Copenhagen University	May 2016
Number Theory Seminar, Bristol University	March 2016
Quebec-Vermont Number Theory Seminar	March 2016

Towards computing the structure of algebras of Drinfeld modular forms

Groups, Geometry, and Actions University of Münster	June 2017

Abel-Jacobi maps and Riemann points on hyperelliptic Riemann surfaces

Special Session on Discrete Structures in Number Theory Joint Mathematics Meetings	January 2017

Curves with many automorphisms

AWM Workshop: Special Session on Number Theory Joint Mathematics Meetings	January 2017

Weierstrass points on Drinfeld modular curves

Colloquium, American University	September 2016

References

Ken Ono, Marvin Rosenblum Prof. of Mathematics, University of Virginia (ko5wk@virginia.edu)

Jennifer S. Balakrishnan, Clare Boothe Luce Professor, Boston University (jbala@bu.edu)

Kristin Lauter, West Coast Head of Research Science, Facebook (klauter@meta.com)

Andrew Sutherland, Principal Research Scientist, MIT (drew@math.mit.edu)

Álvaro Lozano-Robledo, Professor, University of Connecticut (alvaro.lozano-robledo@uconn.edu)

Rafe Mazzeo, Professor, Stanford University (mazzeo@math.stanford.edu)