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

Education

Ph.D. Mathematics, University of Wisconsin–Madison Advisor: Ken Ono	2006-2012
B.Sc. Mathematics (Honours), McGill University	2003-2006

Grants and other funding

Travel Support for Mathematicians Simons Foundation	2023-2028
NSF conference grant, Connecticut Summer School in Number Theory (Co-PI)	2024–2025
NSA conference grant, Connecticut Summer School in Number Theory (Co-PI)	2024–2025
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

Sarah Days-Merill, PhD 2024, *Ring Learning with Errors*
Jesse Franklin, PhD 2024, *Computing the Canonical Ring of Certain Stacks*
co-advised with Taylor Dupuy
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*

Publications

K. Maughan, J. Near, C. Vincent, Foldable recursive proofs of isogeny computation with reduced time complexity, accepted for publication in the program of the *IEEE International Conference on Quantum Computing and Engineering – QCE24*

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, *The Computer Journal*, vol. 67 (8), August 2024, pages 2702–2719.

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, *The Quaterly Journal of Mathematics*, vol. 75 (1), 2024, pp. 239–276.

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

Member of the steering committee, CODE4math organization	December 2023-December 2024
Member of the Committee of Visitors, National Science Foundations	August–September 2024
Member of the program committee, Algorithmic Number Theory Symposium	February–July 2024
Organizer and lecturer, Connecticut Summer School in Number Theory	February–June 2024
Planned the *Thinking session: A better math community* Special session on Rethinking Number Theory at the 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

Shapes of endomorphism rings of supersingular elliptic curves

Special Session on Explicit Methods in Arithmetic Geometry Fall Eastern Sectional Meeting of the AMS	October 2024

The mathematics of electronic voting

Undergraduate colloquium, Fairfield University	September 2024

A short introduction to post-quantum cryptography

Mathematical Association of America Spring 2024 Northeastern meeting Invited address	June 2024

Generating a secure random supersingular elliptic curve

Combinatorics and optimization colloquium, University of Waterloo	January 2024

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

It is surprisingly hard to generate a (secure) random supersingular elliptic curve

Mathematics colloquium, University of Georgia	December 2023

Invited Conference and Seminar Talks (continued)

Post-quantum cryptography: What is it and why?

Bowdoin College Number Theory and Cryptography class — November 2023
Invited lecturer

Upstate Number Theory Conference — October 2021
Plenary speaker

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 — February 2022
Spring Eastern Sectional Meeting of the AMS

Computing hyperelliptic modular invariants from period matrices

Session on Algebra and Number Theory — February 2022
XXIII International Symposium of Mathematical Methods Applied to Sciences

Session on Computational Number Theory — August 2021
MAA MathFest

Special Session on Coding Theory, Cryptography, and Number Theory — October 2020
Fall Southeastern Sectional Meeting of the AMS

Special Session on Algorithms, Experimentation, and Applications in Number Theory — January 2020
Joint Mathematics Meetings

Arithmetic, Geometry, Cryptography and Coding Theory — June 2019

Invited Session on Women in Numbers — April 2019
AWM Research Symposium

Special Session on Special Values of L-functions and Arithmetic Invariants in Families — April 2019
Spring Eastern Sectional Meeting of the AMS

Special Session on Number Theory, Arithmetic Geometry, and Computation — January 2019
Joint Mathematics Meetings

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

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

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, 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 — September 2020
Plenary speaker

Modular Forms, Arithmetic, and Women in Mathematics — November 2019
Plenary speaker

Sage and the L-functions and modular forms database

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

Invited Conference and Seminar Talks (continued)

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 — April 2016
Keynote address

Constructing hyperelliptic curves of genus 3 whose Jacobian has CM
Number Theory Seminar, University of Virgina — October 2017
Special Session on Computational Number Theory — August 2017
Applied Mathematics, Modeling and Computational Science Conference

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 — September 2017
Fall Southeastern Sectional Meeting of the AMS
Special Session on Women in Sage — April 2017
AWM Research Symposium
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 — May 2016
Université de Picardie Jules Verne
Séminaire de la Butte-aux-Cailles — May 2016
Télécom ParisTech
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 — June 2017
University of Münster

Abel-Jacobi maps and Riemann points on hyperelliptic Riemann surfaces
Special Session on Discrete Structures in Number Theory — January 2017
Joint Mathematics Meetings

Curves with many automorphisms
AWM Workshop: Special Session on Number Theory — January 2017
Joint Mathematics Meetings

Weierstrass points on Drinfeld modular curves
Colloquium, American University — September 2016