Krystal Maughan

krystal.maughan@gmail.com
Github: https://github.com/kammitama5
Tel: 607.342. 6970
Blog: https://kammitama5.github.io/

Research Interests: Isogeny-Based Cryptography, Mathematical Cryptography, Elliptic Curves, Random Processes, Computational Number Theory (Arithmetic Geometry), Algebraic Graph Theory

---

University of Vermont, PhD student ***2019-present***
Computer Science PhD student, minor in Pure Mathematics

(PhD) classes: *Mathematical (Post-Quantum) Cryptography, Elliptic Curves and Modular Forms, Combinatorial Graph Theory, Spectral Graph Theory, Category Theory, Random Probabilistic Graphs, Secure and Distributed Computation, Abstract Algebra I (Groups), III (Rings/Fields/Galois Theory), IV (Category Theory, Lie Algebra), Privacy Law and Policy, Machine Learning, Data Privacy, Software Verification, Computer Human Interaction.*

Oral Qualification Exams in: *(1) Quantum Computing, Quantum Algorithms and Classical Mathematical Cryptanalysis, (2) Elliptic Curves (3) Graph Theory*

RESEARCH EXPERIENCE:

Research Assistant (Vermont) ***2021-present***
PhD Supervisors: C. Vincent, J. Near: Research on Isogeny-Based Cryptography
- *Mathematical Cryptography Research*

Research Assistant: P. Rombach: Research on Computational Combinatorics ***2022-present***
- *Algebraic Combinatorial Graph Theory Research*

Supervisor: Joe Near: Research on Provable Fairness and (Differential) Privacy ***2019-2021***
Using Machine Learning. Funded via Amazon Research Award (2020-2022 PI: J. Near, D. Darais).

Working Preprints (Cryptanalysis / Computational Number Theory):
- ❖ *Mathematical Cryptography: Work on Compositional Isogeny Schemes (ongoing)* *2022-present*
  *(PI: C. Vincent, **Maughan, K.**)*
- ❖ *Computational Number Theory research* 2023-present
  to be published in proceedings **Women in Numbers :**
  Research Directions in Number Theory : Women in Numbers VI (2024)
  (PIs: Lauter K. PhD, Newton R. PhD, with Li C., **Maughan K.**, Srivastava M.)

Preprints (Data Privacy and Security):
- ❖ *"Improving Utility for Analysis of Correlated Columns using Pufferfish Privacy"* *2022*
  *(**Maughan, K.** and Near, J.)*

Workshop Conference Posters (Cryptanalysis / Computational Number Theory):
- ❖ *"Compositional Isogeny Schemes"- poster presented, **CrossFyre at Eurocrypt*** *2023*
  *Poster for workshop on Provably Robust Schemes (**Maughan, K**)*
- ❖ *"Compositional Isogeny Schemes"- presented as poster at **ACM Richard Tapia*** *2022*
  *Poster Competition at Conference (**Maughan, K**)*

Collaboration on Other Research Projects in Progress:

- ***Research Project*** 2023-present
  Rethinking Number Theory
  (*PIs and project: TBD*)
- ***Research Project*** 2023-present
  Independent research project
  (*PI: Lees A., PhD,* ***K. Maughan***)
- ***Research Project*** 2023-present
  Independent research project
  (*PI: Rombach, P., PhD,* ***K. Maughan***)
- ***Summer of Bitcoin*** *(Virtual) "Price of Anarchy in Selfish Routing on the Lightning Network" (R. Pickhardt, S. Alscher,* ***K. Maughan****)* *2022*

Preprints (Machine Learning):

- *Prediction Sensitivity: Continual Audit of Counterfactual Fairness in Deployed Classifiers (**Maughan, K.**, Ngong, I., Near, J.)* *2022*
  *(presented as poster at **EAAMO Doctoral Consortium**)*
- *"Towards a Measure of Individual Fairness for Deep Learning"* *2020*
  *(**Maughan, K.** and Near, J.) - presented as poster for **MD4SG***
- *"Towards Auditability for Fairness in Deep Learning"* *2020*
  *(Ngong, I., **Maughan, K.** and Near, J.)- presented as poster for **AFCI at NeurIPS***

Workshop Posters (Machine Learning):

- *"Archipelago Penseé"* *2020*
  *(**Maughan, K.**) - presented as a poster for Resistance AI (**RAIS) at NeurIPS***

Whitepapers (Data Privacy and Security):

- *Client Telemetry Aggregation, Microsoft internal (joint work with: P. Angulo, PhD)* *2021*

TEACHING EXPERIENCE

- *PhD Teaching Fellow, iSchool Inclusion Institute (i3), "Computational Tools"* *2023*
  - *1 of 2 PhD applicants chosen to design and teach curriculum for 10-day Summer course at the University of Texas at Austin (with S. Stueve, co-teaching fellow)*
  - *Provided salary and funded with accommodation, flight and stipend for supplies.*
- *Guest Lecturer, "Privacy Law and Policy", University of Vermont (UVM)* *2021*
  - *Presented research work on Impacts of Data Leakage and Data Privacy*
- *Graduate Teaching Assistant, University of Vermont (Fall / Spring)* *2019-2020*
  - *Teacher's Assistant for:*
    - *Compiler Construction (with Haskell)*
    - *Programming for Engineers (with Matlab)*
    - *Data Privacy (Differential Privacy, K-anonymity, Machine Learning with Python)*
    - *Advanced Web Design*

GRANT WRITING / PROPOSALS (SELECTED)

- *Summer of Bitcoin, "Price of Anarchy in Selfish Routing On the Lightning Network" (Research proposal with 0.4% acceptance rate, Awarded $3,000)* *2022*

GRANT WRITING / PROPOSALS (SELECTED)

- *COST Action Proposal OC-2021-1-25315 "Mathematics and Algorithmics of Group actions and Isogenies for Cryptography" (Secondary Proposer)* *2021*
- *Microsoft Research, Reinforcement Learning Open Source Festival Proposal (Awarded $10,000)* *2021*
- *Google Summer of Code, Proposal to Haskell.org (Awarded $6,000)* *2018*
- *Helium Grant, (for exploring questions on the edge of mainstream thinking) (1 of 11 chosen out of 700 applicants; Awarded $1,000)* *2018*

RESEARCH AWARDS (SELECTED)

***2nd Place Winner**, Best Research Project (tie with X. Zhang), UVM CS Research Day for "Price of Anarchy in Selfish Routing on the Lightning Network"* *2022*

***Best Poster**, Brilliant Idea Category, Mediterranean Machine Learning Summer School* *2021*

MERIT-BASED MENTORSHIPS / RESEARCH MENTORSHIPS (SELECTED)

Mentee, LXAI Computer Vision (LXCV) at CVPR (Computer Vision) workshop *2023*
- *Mentor: F. N. Paravecino, PhD (Research collaborations)*

Mentee, Algorithmic Game Theory Workshop (AGT), Economics and Computation *2022*
- *(mentor: H. Zhang, PhD), paper dissection and Ask me Anything session*

Mentee, MD4SG Mentorship Program, with J. Finocchiaro, PhD (1 of 3) *2022-2023*

Mentee, AiC Connectors Program with Facebook, with S. Lim, PhD *2022*

Mentee, BlackComputeHer Fellowship, with Y. Rankin, PhD, A. Robinson, M.Ed *2022*

Mentee, Microsoft's Tech Resilience (mentors: O. Kroshkina, M. Ward) *2022*

Mentee, Google's CS Research Mentorship Program (CSRMP) with A. Lees, PhD *2021*

Mentee, AiC Connectors Program with Facebook with O. Dalleleau, PhD *2021*

Mentee, She256 Blockchain Group with P. Mishra, PhD *2021*

Mentee, Women in Privacy and Security (WISP), D. Sharma, PhD *2021*

Mentee, Algorithmic Game Theory (AGT), Economics and Computation Conference *2020*
- *Global Outreach Mentorship with S. Gupta, PhD (EC 2020)*

Mentee, Mentored by A. Ahmed, PhD, *2020-present*
- *ICFP 2020, ACM SIGPLAN-Mentorship, organized by T. Ringer*

ACADEMIC REVIEWER (SELECTED)

AAAI 2023 Workshop on Privacy Preserving Artificial Intelligence (PPAI), PML4DC (Practical Machine Learning for Developing Countries), ICLR / NeurIPS: Algorithmic Fairness through the Lens of Causality and Privacy, ICLR Distributed and Private Machine Learning (DPML), Tiny Papers Workshop at ICLR 2023 (Co-Area Chair), etc.

REVIEWER (OTHER)

Effective Haskell, by R. Skinner, Springer's AI Ethics Journal, BAI workshops at NeurIPS

RESEARCH PhD INVITATIONS (ABRIDGED)

Participant, WIN6, (mentors: Lauter K., Newton R.) *2023*
- *Research project at BIRS, to be published in WIN proceedings 2024 (Banff, Canada)*
- *Received award for lodging, travel (~1 of 42) (March 26th to March 31st)*

RESEARCH PhD INVITATIONS (ABRIDGED)

Participant, IPAM "Machine Assisted Proofs" (Feb 13-17), (Los Angeles, California) 2023
- *Formal methods at the intersection of Pure Mathematics and Computer Science*
- *Received award for lodging, waived registration*

(organized by E. Abraham, J. Avigad, J. Ellenberg, M. Heule, T. Tao, K. Buzzard, T. Gowers)

Participant, PCMI Graduate Summer School, "Quantum Computation" (3 weeks) 2023
- *Awarded full funding (housing, registration, flight) (July 16-August 5th)*
- *Coursework on: Quantum and quantum-inspired linear algebra,*
- *Quantum fourier transforms and quantum information theory, LDPC codes*
- *Topological aspects of quantum codes, quantum hamiltonian complexity*
- *Quantum learning theory*

Participant, Rethinking Number Theory 2023
- *Collaborative research in Number Theory (June 12th to 23rd)*
- *Organized by A. Serrano López, M. West, H. Goodson)*

Participant, Twelfth Summer School on Formal Techniques + FMiTF Bootcamp 2023
- *Received admission, housing and funding for flight*
- *Learning Vampire Theorem Prover (May 23rd to June 2nd) (Menlo College, Atherton)*

Participant, ICERM's LMFDB, Computation and Number Theory (LuCaNT) workshop 2023
- *(Provided housing, registration)*

Invited Participant, Lorentz Center, "Machine-Checked Proofs", Leiden, the Netherlands 2023
- *Lean Workshop, Funding (provided housing, funding for travel)*

Invited Participant, High Assurance Crypto Software (HACS) (Tokyo, Japan) 2023
- *(Post-quantum) cryptographic verification workshop (conflicted with WIN6)*

Invited Participant, CrossFyre at Eurocrypt (Lyon, France) 2023
- *Cryptography, Robustness and Provably Secure Schemes for Female Young Researchers: presented research poster*
  (Received funding for accommodation, registration and flight courtesy of PQ-Shield)

Participant, Arizona Winter School, "Point Counting and Applications" (J. Pila) 2023
- *Applications of Point-counting for algebraic points of bounded degree (Tucson, AZ)*

Virtual Participant, "Algebraic Cycles, L-Values, and Euler Systems": MSRI 2023
- *Originally granted registration but opted for virtual attendance*

Virtual Participant, Research Institute for Mathematical Sciences (RIMS) 2023
- *Zeta functions and their representations*

Participant, 1st Roots of Unity reunion, American Institute of Mathematics, Pasadena CA 2023

Participant, Doctoral Consortium at ACM Richard Tapia Conference (Washington, D.C.) 2022

Participant,1st Roots of Unity Summer School: Arithmetic Geometry group (fully-funded) 2022
- *focus on Arithmetic Geometry and Arithmetic Statistics with six PhD students*

Invited to proceeding AWM Research Symposium at University of Minnesota (UMN)) 2022

Invited Participant, IAS/ Park City Mathematics Institute (PCMI) 2022
- *Graduate Summer School, Computational Number Theory (fully-funded: declined offer)*

Virtual Participant, BIRS, Algebraic Methods in Coding Theory and Communication 2022

Virtual Participant, COGENT: Cohomology, Geometry and Explicit Number Theory 2022

Virtual Participant, Stinson66: New Advances in Designs, Codes and Cryptography 2022

Virtual Participant, Arizona Winter School, Southwest Arithmetic Geometry Center 2022
- *Automorphic Forms beyond GL2: Unitary Groups Study Group (mentor E. Eischen)*

Virtual Participant, West Coast Number Theory (WCNT): Problems in Number Theory 2021

RESEARCH PhD INVITATIONS (ABRIDGED)

Participant, GREPSEC V: *2021*
- *(Graduate Students in Privacy and Security Early Career Workshop)*

Participant, Isogeny-Based Cryptography Winter School *2021*

Participant, Post-Quantum Networks Workshop *2021*

Participant, PRIMA Summer School *2021*
- *Rational curves and moduli spaces in arithmetic geometry*

MERIT-BASED GRANTS / FELLOWSHIPS / SCHOLARSHIPS (ABRIDGED)

Initiative for Cryptocurrencies and Contracts (IC3) Blockchain Bootcamp *2021*
- *Worked on group project : Fairness consensus for Miner Extractable Value (MEVs)*
- *Implemented Aequitas protocol from paper with authors for fairness simulation*

Participant, Self Organizing Conference on Machine Learning (SOCML) *2021*
- *Machine Learning, and Privacy session, Moderated by U. Erlingsson* *2021*
- *organized by I. Goodfellow (1 of 9 chosen)*

(Privacy Engineering Practice and Respect) PEPR Grant, S&P Oakland *2022*

Fellow, BlackComputeHER (2022-2023) (1 of 11) *2022*

Scholarship winner (to attend Richard Tapia Celebration of Diversity in Computing) *2022*
- *(registration, flight, hotel costs, Washington D.C. courtesy BNY Mellon)*

Google Grace Hopper Conference (GHC) Scholarship *2021*

WISP & Black Hat USA Briefings Scholarship (1 of 25) *2021*

Kernel Fellowship Block III via Gitcoin (Security: Zero Knowledge Proofs project) *2021*

Gitcoin Scholarship for Women (for Kernel Fellowship Block III) *2021*

She256 Mentorship focused on ZK Snarks (6 months) *2021*

OTHER GRANTS/ FELLOWSHIPS (ABRIDGED)

USENIX Security Conference 2021 (via USENIX Diversity Grant via GREPSEC V) *2021*

TechX Social Impact / Harvard Franklin Fellowship (1 of 12) *2020*

USENIX Enigma Grant *2021*

NCAS Workshop participant (NASA Community College Aerospace Scholars) *2016*

Who's Who/ Peggy Williams Memorial Scholarship/ Best BFA Award (Best of Major) *2008*

Northeast Combinatorics, Discrete Maths Day (lodging) *2022*

Upstate Number Theory Conference 2021 (lodging provided) *2021*

IEEE Symposium on Security and Privacy (student travel grant, complimentary ticket) *2021*

4th Annual ZK-Proof Workshop (complimentary ticket) *2021*

WISP Privacy+Security Conference *2021*
- *EU Data Law / De-Identification Workshop (Scholarship via WISP)*

ICERM (Brown University) Variable Precision in Mathematical & Scientific Thinking *2020*

RWC2020 (Real World Crypto: registration, flight, lodging) Grant via IACR *2020*

Sage-Days-104 : To work on SageMath Software: Arithmetic Dynamics *2019*

Simons Institute (Berkeley) Error-Correcting Codes and High-Dimensional Expansion Boot Camp (attendee) *2019*

ICERM (Brown University) Encrypted Search Workshop Grant (Lodging provided) *2019*

Cornell Number Theory Conference Grant (Lodging provided) *2019*

OTHER GRANTS/ FELLOWSHIPS (ABRIDGED)

MSRI (Mathematical Sciences Research Institute) Grants to attend:
Optimal Transport and applications to machine learning and statistics 2020
Connections for Women: 2019
- *Derived Algebraic Geometry, Birational Geometry and Moduli Spaces workshop*
- *Introductory Workshop: Derived Algebraic Geometry and Birational Geometry And Moduli Spaces*

Racket Summer School (National Science Foundation Grant) 2018-2019
PLMW (Programming Languages Mentorship Workshop) 2018
ICFP (International Conference Functional Programming)
PLMW(Programming Languages Mentorship Workshop) 2018
PLDI (Programming Languages Design and Implementation)
OPLSS (Oregon Programming Languages Summer School Grant) - declined offer 2018

INSTITUTIONAL PROSPECTIVE FACULTY PhD INVITATIONS

- *Invited Participant, Rochester Institute of Technology: RIT Pathways to RIT (Pathways from PhD to Faculty programme) 2023*

INDUSTRY PhD INVITATIONS (ABRIDGED)

Participant, Meta's Uniting Scholars in Research (Menlo Park, Palo Alto) (1 of 35) 2022
Virtual Participant, Jane Street's Preview Program, The Game Show / Trading Games 2022
Virtual Participant, Adobe's Experience Day:Research Track (Emerging Devices)(1 of 35) 2022
Participant, Facebook, Amplified: Above & Beyond Computer Science Program (PhDs) 2021
Participant, Facebook's Amplified: Virtual Vivid in Research (1 of 30) 2021
Participant, Galois 1st Summer School on Trustworthy Machine Learning (1 of 35) 2021
Participant (via CSRMP), Google PhD Fellowship Summit 2021
Participant, Jane Street PhD Symposium (New York, remote) (Quant Research) 2021
Participant, TwoSigma Mock Interview Day for Early Career Women (Quant Research) 2021
Participant, Twitter PhD ML Flock Event (New York, Boston office) 2019

GRADUATE SCHOOL INTERNSHIPS

JP Morgan, *Quantitative AI Research, Summer Associate (New York) (1 of 10) 2022*
Summer of Bitcoin*, Blockchain (Lightning Network) PhD Research intern (remote) 2022*
Microsoft Research*, Independent Contractor, Summer 2021 (New York: remote) 2021*
Microsoft, *PhD Intern, Summer 2021 (Redmond: remote) 2021*
Autodesk, *PhD Intern, Summer 2020 (Pier 9, San Francisco: remote) 2020*

RELEVANT WORK / INDUSTRY EXPERIENCE (Pre-Grad school)

Mercury Banking (Haskell fintech) : *Software Engineering Intern (San Francisco) 2019*
Apple, Inc.: *Software Engineering Intern (Sunnyvale) 2019*
Google Summer of Code: *Developer for Haskell.org 2018*
Mozilla: *Increasing Rust's Reach Developer 2018*

OTHER (NON-INDUSTRY) TALKS (ABRIDGED)

"Compositional Isogeny Schemes", Tapia Doctoral Consortium (45 minutes) 2022
"A Journey through Unboundedness of ranks of Elliptic Curves", (15 minute talk) 2022

OTHER (NON-INDUSTRY) TALKS (ABRIDGED)

Roots of Unity Workshop (joint talk with O. Del Guercio and M. Bustos Gonzalez)
Brown University, Fair February talk on Security, Privacy, Fairness (30 minutes) 2022
Meetup "Math for Math's Sake", Virtual Lightning Talk (10-15 minutes) 2022
"Isogenies, Elliptic Curves and Random Walks on Random Graphs
"Composable Forgetful Isogenies", Google CSRMP Research Alumni Talk (30 minutes) 2022
"Price of Anarchy in Selfish Routing", Graph Theory and Spectral Graph Theory (15 min) 2022
"Price of Anarchy in Selfish Routing", Google CSRMP Research Alumni Talk (30 minutes)2022
CS Research Day, "Price of Anarchy in Selfish Routing", UVM (16 min) 2022
"Composable Forgetful Isogeny Graph Cryptography", Google CSRMP Research 2021
"Isogeny Cryptography",School for Poetic Computation, Re-learning to love Maths 2021
PLAID Lab Speaker, "Information Theory: from Spacecraft to Blockchain" 2021

INDUSTRY TALKS (ABRIDGED)

"Isogeny-Based Cryptography", JP Morgan AI Research Cryptography Group (1 hour) 2022
JP Morgan AI Research Weekly Technical Meeting, (New York) (20 min) 2022
JP Morgan AI Research Reading Group Meeting (30 min) 2022
JP Morgan Summer Symposium (10 min) 2022
Women Who Code: SageMath: "Computational (Pure) Mathematics/Graph Theory" 2022
- *Lightning Talk (2-4 min)*

"Prediction Sensitivity for Fairness in AI", Jane Street Symposium (15 minutes) 2021
"Renyi-Differential Privacy", Autodesk UX Group (20 minutes) 2020

CLASSES (OTHER)

Zaiku Group, Software Verification Course (online) 2023
- *Class focused on Quantum Formalism, functional programming and Software verification for Homotopic Minds taught by B. Ahrens using Lean*

CLASSES (AUDIT)

Preliminary Arizona Winter School, Model Theory and Applications, taught by R. Nagloo 2022-2023
Stanford: EE 374 : Internet-Scale Consensus in the Blockchain Era (Spring) 2021
- *Information Theory class focused on scalability and protocols in Blockchain*
- *Taught by D. Tse, PhD through Stanford University*
- *Audited class, scribed for Lecture 11, Spring 2021*

IBM Qiskit Global Summer School (Quantum Computation using Qiskit) 2020

Audit / Other: *Internet Scale Consensus in the Blockchain Era (Information Theory class at Stanford), Matroids & Polytopes, Theory of Algebraic Differential Equations, Elementary Number Theory, Fundamentals of Mathematics, Extremal Graph Theory, Model Theory and Applications.*

Book Clubs:

Quantum Computing (2022), Quantum Computing and Quantum Information (2022-2023: study group with Mathematicians, Physicists and Computer Scientists), HDX Expander Graphs (2022-2023)

Skills: Python, SageMaths, Haskell, LaTeX, Matlab, Jupyter, Pytorch, SQL, AWS, PySpark, Sparklyr, Tensorflow, Git, Lean, writing proofs.

PRESS (SELECTED)

Publication Featured in Montreal AI Ethics Institute (MAIEI) newsletter 2022
Publication work Featured in BitMEX Research blog 2022
Featured / interviewed in articles / media by Coursera, NASA-JPL, Google, Udacity, 2016-present
The MacArthur Foundation, Venture Beat, The Data Standard, Corecursive Podcast,
OpenMined,Career Girls, Dataiku, Scott Hanselman's Podcast, BlackComputeHer,
NASA Tech Briefs (40th anniversary), Variety, ACM SPLASH 2022 PLMW Perspectives,
the Los Angeles Times, Black Girls Code colouring book on Women Scientists,
Women of Silicon Valley, CareerGirls, The Summer of Bitcoin experience (SBOE), Technovation,
Rewriting the Code, Montreal AI Ethics Institute, etc.

GUEST WRITER (SELECTED)

Blogpost, ***Summer of Bitcoin*** (joint with S. Alscher) (Lightning Network routing) 2022

ACADEMIC ASSOCIATION FOR COMPUTING MACHINERY (ACM) MEMBERSHIPS

Student Member, International Association of Cryptologic Research (IACR) *2020-present*
SIGecom Special Interest Group on Economics and Computation *2020-present*

NON-ACADEMIC MEMBERSHIP

Member, Isogeny Research Club *2023-present*
Member, Women in Cryptography *2023-present*
Student Member, IEEE Computer Society Technical Committee on Security and Privacy *2021-present*
Member, Women in Number Theory *2018-present*
Member, QVNTS (Quebec-Vermont Number Theory Seminar) *2021-present*
Member, Women in Combinatorics *2021-present*
Member, Association for Women in Mathematics *2021-present*
Member, She256 *2021-present*
Member, Women in Security and Privacy (WISP) *2020-present*
Member, IEEE Information Theory Society, Santa Clara Valley Chapter *2016-present*