

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, Game Theory, Random Processes, Combinatorics, Graph Theory

University of Vermont, PhD student

2019-present

Computer Science PhD student, minor in Pure Mathematics

Selected (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.

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:

- ❖ Mathematical Cryptography: Work on Compositional Isogeny Schemes (ongoing) 2022-present (Mentor: C. Vincent)
- ❖ Combinatorics: Work on Computational Combinatorial Graph Theory research 2022-present (Mentor: M. Rombach) (ongoing)

Selected Preprints:

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

Selected Workshop Conference Posters:

- ❖ "Compositional Isogeny Schemes"- presented as poster at **ACM Richard Tapia** 2022 Conference (Maughan, K)

Whitepapers:

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

Collaboration on Other Research Projects in Progress:

- ❖ **Women in Number Theory 6 at BIRS** (Banff, Canada) (selected participant) 2023
Research on "Machine Learning and Arithmetic Geometry / Statistics"
(Number Theory research led by mentors K. Lauter, R. Newton and co-authors)

Collaboration on Other Research Projects in Progress:

- ❖ **Summer of Bitcoin** (Virtual) “Price of Anarchy in Selfish Routing on the Lightning Network” (R. Pickhardt, S. Alscher, **K. Maughan**) 2022

Graduate Teacher’s Assistant, Fall/Spring 2019-2020 (Vermont)**2019-2020**

Compiler Construction with Haskell, Programming with Matlab, Data Privacy, 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
- ❖ 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), 2022

UVM CS Research Day for “Price of Anarchy in Selfish Routing on the Lightning Network”

Best Poster, Brilliant Idea Category, Mediterranean Machine Learning Summer School 2021**MERIT-BASED MENTORSHIPS / RESEARCH MENTORSHIPS (SELECTED)**

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. Finocchiario, 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), etc.

RESEARCH PhD INVITATIONS (ABRIDGED)

Participant, WIN6, "Machine Learning and Arithmetic" (mentors: K. Lauter, R. Newton)	2023
- Research in Arithmetic Statistics and Machine Learning at BIRS (Banff, Canada)	
- Received award for lodging, travel (~1 of 42)	
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, Arizona Winter School, "Unlikely Intersections: Model Theory", (Tucson, AZ)	2023
Virtual Participant, "Algebraic Cycles, L-Values, and Euler Systems": MSRI	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; also	
Invited to proceeding AWM Research Symposium at University of Minnesota (UMN))	
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	2022
- Automorphic Forms beyond GL ₂ : Unitary Groups Study Group (mentor E. Eischen)	
Virtual Participant, West Coast Number Theory (WCNT): Problems in Number Theory	2021
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	
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)	

MERIT-BASED GRANTS / FELLOWSHIPS / SCHOLARSHIPS (ABRIDGED)

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

OTHER GRANTS/ FELLOWSHIPS (ABRIDGED)

<i>TechX Social Impact / Harvard Franklin Fellowship (1 of 12)</i>	2020
<i>USENIX Enigma Grant</i>	2021
<i>NCAS Workshop participant (NASA Community College Aerospace Scholars)</i>	2016
<i>Who's Who/ Peggy Williams Memorial Scholarship/ Best BFA Award (Best of Major)</i>	2008
<i>Northeast Combinatorics, Discrete Maths Day (lodging)</i>	2022
<i>Upstate Number Theory Conference 2021 (lodging provided)</i>	2021
<i>IEEE Symposium on Security and Privacy (student travel grant, complimentary ticket)</i>	2021
<i>4th Annual ZK-Proof Workshop (complimentary ticket)</i>	2021
<i>WISP Privacy+Security Conference</i>	2021
- <i>EU Data Law / De-Identification Workshop (Scholarship via WISP)</i>	
<i>ICERM (Brown University) Variable Precision in Mathematical & Scientific Thinking</i>	2020
<i>RWC2020 (Real World Crypto: registration, flight, lodging) Grant via IACR</i>	2020
<i>Sage-Days-104 : To work on SageMath Software: Arithmetic Dynamics</i>	2019
<i>Simons Institute (Berkeley) Error-Correcting Codes and High-Dimensional Expansion Boot Camp (attendee)</i>	2019
<i>ICERM (Brown University) Encrypted Search Workshop Grant (Lodging provided)</i>	2019
<i>Cornell Number Theory Conference Grant (Lodging provided)</i>	2019
<i>MSRI (Mathematical Sciences Research Institute) Grants to attend:</i>	
<i>Optimal Transport and applications to machine learning and statistics</i>	2020
<i>Connections for Women:</i>	2019
- <i>Derived Algebraic Geometry, Birational Geometry and Moduli Spaces workshop</i>	
- <i>Introductory Workshop: Derived Algebraic Geometry and Birational Geometry And Moduli Spaces</i>	
<i>Racket Summer School (National Science Foundation Grant)</i>	2018-2019
<i>PLMW (Programming Languages Mentorship Workshop)</i>	2018
<i>ICFP (International Conference Functional Programming)</i>	
<i>PLMW(Programming Languages Mentorship Workshop)</i>	2018
<i>PLDI (Programming Languages Design and Implementation)</i>	
<i>OPLSS (Oregon Programming Languages Summer School Grant) - declined offer</i>	2018

INDUSTRY PhD INVITATIONS (ABRIDGED)

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

GRADUATE SCHOOL INTERNSHIPS

JP Morgan , Quantitative AI Research, Summer Associate (New York) (1 of 10)	2022
Summer of Bitcoin , PhD Research intern	2022

GRADUATE SCHOOL INTERNSHIPS

<i>Microsoft Research, Independent Contractor, Summer 2021 (New York: remote)</i>	2021
<i>Microsoft, PhD Intern, Summer 2021 (Redmond: remote)</i>	2021
<i>Autodesk, PhD Intern, Summer 2020 (Pier 9, San Francisco: remote)</i>	2020

RELEVANT WORK / INDUSTRY EXPERIENCE (Pre-Grad school)

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

OTHER (NON-INDUSTRY) TALKS (ABRIDGED)

<i>"Compositional Isogeny Schemes", Tapia Doctoral Consortium (45 minutes)</i>	2022
<i>"A Journey through Unboundedness of ranks of Elliptic Curves", (15 minute talk)</i>	2022
<i>Roots of Unity Workshop (joint talk with O. Del Guercio and M. Bustos Gonzalez)</i>	
<i>Brown University, Fair February talk on Security, Privacy, Fairness (30 minutes)</i>	2022
<i>Meetup "Math for Math's Sake", Virtual Lightning Talk (10-15 minutes)</i>	2022
<i>"Isogenies, Elliptic Curves and Random Walks on Random Graphs"</i>	
<i>"Composable Forgetful Isogenies", Google CSRMP Research Alumni Talk (30 minutes)</i>	2022
<i>"Price of Anarchy in Selfish Routing", Graph Theory and Spectral Graph Theory (15 min)</i>	2022
<i>"Price of Anarchy in Selfish Routing", Google CSRMP Research Alumni Talk (30 minutes)</i>	2022
<i>CS Research Day, "Price of Anarchy in Selfish Routing", UVM (16 min)</i>	2022
<i>"Composable Forgetful Isogeny Graph Cryptography", Google CSRMP Research</i>	2021
<i>"Isogeny Cryptography", School for Poetic Computation, Re-learning to love Maths</i>	2021
<i>PLAID Lab Speaker, "Information Theory: from Spacecraft to Blockchain"</i>	2021

INDUSTRY TALKS (ABRIDGED)

<i>"Isogeny-Based Cryptography", JP Morgan AI Research Cryptography Group (1 hour)</i>	2022
<i>JP Morgan AI Research Weekly Technical Meeting, (New York) (20 min)</i>	2022
<i>JP Morgan AI Research Reading Group Meeting (30 min)</i>	2022
<i>JP Morgan Summer Symposium (10 min)</i>	2022
<i>Women Who Code: SageMath: "Computational (Pure) Mathematics/Graph Theory"</i>	2022
- <i>Lightning Talk (2-4 min)</i>	
<i>"Prediction Sensitivity for Fairness in AI", Jane Street Symposium (15 minutes)</i>	2021
<i>"Renyi-Differential Privacy", Autodesk UX Group (20 minutes)</i>	2020

CLASSES (AUDIT)

<i>Preliminary Arizona Winter School, Model Theory and Applications, taught by R. Nagloo</i>	2022-2023
<i>Stanford: EE 374 : Internet-Scale Consensus in the Blockchain Era (Spring)</i>	2021
- <i>Information Theory class focused on scalability and protocols in Blockchain</i>	
- <i>Taught by D. Tse, PhD through Stanford University</i>	
- <i>Audited class, scribed for Lecture 11, Spring 2021</i>	
<i>IBM Qiskit Global Summer School (Quantum Computation using Qiskit)</i>	2020
<i>Matroids and Polytopes, Topology (Point-Set), Theory of Algebraic Differential Equations, Elementary Number Theory, Fundamentals of Mathematics, Extremal Graph Theory.</i>	

Book Clubs:

Quantum Computing (2022), *Quantum Computing and Quantum Information* (2022-2023), *HDX Expander Graphs* (2022-2023)

Skills: Python, Sage, Haskell, LaTeX, Matlab, (learning Rust and R), Jupyter, SQL, AWS, PySpark, Sparklyr, Maplesoft, Tensorflow, Git, writing proofs.

PRESS (SELECTED)

Publication Featured in Montreal AI Ethics Institute (MAIEI) newsletter 2022
 Publication work Featured in BitMEX Research blog 2022
 Also 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, 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

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