

# 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,  
Algorithmic Fairness & Game Theory, Interpretability, Random Processes

---

**University of Vermont, PhD candidate**

**2019-present**

Computer Science PhD student, minor in Pure Mathematics

---

## RESEARCH EXPERIENCE:

**Research Assistant (Vermont)**

**2021-present**

PhD Supervisors: C. Vincent, J. Near: Research on Isogeny-Based Cryptography

Research Assistant: P. Rombach: Computational Combinatorics research

**2022-present**

Research Assistant: Joe Near: Research on Provable Fairness and Privacy

**2019-2022**

- Using Machine Learning. Funded via Amazon Research Award
- (2020-2022 PI: J. Near, D. Darais).

## RESEARCH

### Preprints:

- ❖ "Price of Anarchy in Selfish Routing on the Lightning Network" (ongoing) 2022  
(R. Pickhardt, S. Alscher, **K. Maughan**)
- ❖ "Attribute Differential Privacy" (ongoing) 2022  
(**Maughan, K.** and Near, J.)
- ❖ "Continual Audit of Individual Fairness in Deployed Classifiers via Prediction Sensitivity" (**Maughan, K.**, I. Ngong and J. Near) 2021

### Workshop Publications:

- ❖ "JP Morgan AI Research department project" 2022  
(joint work with S. Mishra PhD, D. Ley, D. Magazzeni, PhD) (ongoing)
- ❖ "Towards a Measure of Individual Fairness for Deep Learning" 2020  
(**Maughan, K.** and Near, J.) - presented as poster for **MD4SG 2020**
- ❖ "Towards Auditability for Fairness in Deep Learning" 2020  
(Ngong, I., **Maughan, K.** and Near, J.)- presented as poster for **AFCI at NeurIPS**

### Workshop Conference Posters:

- ❖ "Compositional Isogeny Schemes"- presented as poster at **ACM Richard Tapia Conference** (**Maughan, K.**) 2022
- ❖ "Archipelago Pensée" (**Maughan, K.**) 2020  
Presented writing and artwork as poster for **RAIS (Resistance AI) at NeurIPS**

### Whitepapers:

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

### Other:

- ❖ OpenMined Federated Medical Learning Research Project 2022  
(ongoing participant with hundreds of researchers and health practitioners)

<b>Graduate Teacher's Assistant, Fall/Spring 2019-2020 (Vermont)</b>	<b>2019-2020</b>
Compiler Construction with Haskell (taught by Joe Near)	2020
Advanced Web Design (taught by B. Erickson)	
Programming with Matlab (taught by R. Dasari)	2019
Data Privacy with Jupyter, Python (taught by J. Near)	

---

## GRANT WRITING / PROPOSALS

- ❖ Summer of Bitcoin, "Price of Anarchy in Selfish Routing On the Lightning Network" (Research proposal with 0.4% acceptance rate, total award \$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
- ❖ CDS&E Computational and Data-Enabled Science and Engineering Database Grant Proposal for SageMaths (as Key Personnel) (PI B. Hutz, PhD) (not awarded) 2020
- ❖ 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

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

## MERIT-BASED MENTORSHIPS / RESEARCH MENTORSHIPS

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

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

Mentee, BlackComputeHer Fellowship, with Y. Rankin, PhD 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, LatinX in AI Research Workshop Mentorship, C. White, PhD (NeurIPS 2021) 2021

Mentee, LatinX in AI Research Workshop Mentorship with J. Barajas, PhD (ICML 2020) 2020

Mentee, Mentored by Amal Ahmed, PhD (ICFP 2020) 2020

Mentee, Lighthouse3 AI Ethics Mentoring Externship with F. McEvoy (1 of 20 chosen) 2020

Mentee, Code2040 Fellowship with Ben Waber, PhD 2020

## ACADEMIC REVIEWER

Reviewer, Springer AI and Ethics Journal 2020 - present

Reviewer, PML4DC (Practical Machine Learning for Developing Countries), ICLR 2021- 2022

Reviewer, BlackAIR Summer Research Grant Program 2021

## **ACADEMIC REVIEWER**

Reviewer, ICLR Distributed and Private Machine Learning workshop	2021
Committee Reviewer, HCI Track, GHC (Grace Hopper Conference)	2021
Reviewer for AFCR workshop at NeurIPS (Fairness, Accountability, Robustness)	2021
Reviewer for AFCI workshop at NeurIPS (Fairness and Accountability)	2020
Reviewer for Black in AI at NeurIPS workshop	2020-2021
Reviewer and Programme Committee Member, LXAI@ICML Workshop	2020
Committee Reviewer, HCI Track, GHC (Grace Hopper Conference)	2020
Chair Reviewer, PML4DC (Practical ML for Developing Countries) workshop, ICLR	2020
Reviewer, Tapia Conference (Panels and Workshops)	2020 - 2022
Reviewer, Travel Grant Applications, Black in AI for AAAI	2020

## **ACADEMIC JOURNALS (AI/Machine Learning)**

Board Member, AI and Ethics, Springer	2020
---------------------------------------	------

## **REVIEWER (NON-ACADEMIC PEDAGOGICAL)**

Published Book, "Effective Haskell" by R. Skinner	2022
Medium Post, "Pure Print Style Debugging in Haskell" by R. Skinner	2022

## **RESEARCH PhD INVITATIONS (ABRIDGED)**

Participant, Doctoral Consortium at ACM Richard Tapia Conference (Washington, D.C.)	2022
Participant, 1st Roots of Unity Summer School: Arithmetic Geometry group (fully-funded) (focus on Arithmetic Geometry and Arithmetic Statistics with six PhD students; also 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, 16th International Symposium on Orthogonal Polynomials, Special Functions and Applications	2022
Virtual Participant, Random : The Conference on Randomization and Computation	2022
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 Attendee, Recent Advances on Total Search Problems	2022
Virtual Participant, Arizona Winter School	2022
- Automorphic Forms beyond GL <sub>2</sub> : Unitary Groups Study Group (mentor E. Eischen)	
Virtual Participant, West Coast Number Theory (WCNT): Problems in Number Theory	2021
Participant, Community-Driven Cryptography Seminar (Brown / John Hopkins)	2021-present
Participant, <a href="#">GREPSEC V</a> :	2021
- (Graduate Students in Privacy and Security Early Career Workshop)	
Participant, Isogeny-Based Cryptography Winter School	2021
Participant, Post-Quantum Networks Workshop	2021
Participant, <a href="#">PRIMA</a> Summer School	2021
- Rational curves and moduli spaces in arithmetic geometry	

## **RESEARCH PhD INVITATIONS (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
  - One of top four winning teams chosen

The Alan Turing Institute:

- Invited Participant, "Threats and Opportunities for AI in Cybersecurity" 2021
  - Invited Participant, "Society-centric approaches to AI challenges in 2021
- Participant, Scottish Programming Languages and Verification School 2021
- Invited Participant, "Key themes for informing a Research Roadmap", 2021
- Alan Turing Institute, Invited Participant, "Environmental Enablers for AI challenges in" 2021
- Simons Institute, Average-Case Complexity: From Cryptography to Statistical Learning 2021
- Simons Institute, Optimization Under Symmetry 2021
- Simons Institute, Innovations in Theoretical Computer Science ([ITCS](#)) 2021
- Simons Institute, Geometric Methods in Optimization and Sampling Bootcamp 2021
- 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 8 ) 2022
- Scholarship winner (to attend Richard Tapia Celebration of Diversity in Computing) 2022
- (registration, flight, hotel costs, Washington D.C.)
- 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
- 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

## **OTHER GRANTS/ FELLOWSHIPS (ABRIDGED)**

- Northeast Combinatorics, Discrete Maths Day 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

**OTHER GRANTS/ FELLOWSHIPS (ABRIDGED)**

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
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

**ACADEMIC SERVICE (ABRIDGED)**

Co-Organizer, Co-submitting Summer Workshop, ICLR (with R. Liu)	2022, 2023
ICLR Program Committee, ICLR DEI Committee (with R. Liu)	2022, 2023
Panelist, Google CSRMP (Computer Science Research Mentorship Program)	2022
Panelist, PhD recruiting event (included multiple schools, sponsored by CodePath)	2020
Student Volunteer, ICFP (International Conference Functional Programming)	2020
Student volunteer, ICFP (International Conference Functional Programming)	2018
Student volunteer, PLDI (Programming Languages Design and Implementation)	2018
Student volunteer, POPL (Principles of Programming Languages)	2018
Student volunteer, SPLASH (Systems, Programming, Languages, and Applications) (declined offer)	

**INDUSTRY PhD INVITATIONS (ABRIDGED)**

Virtual Participant, Jane Street's Preview Program, The Game Show / Trading Games	2022
Virtual Participant, JP Morgan Chase & Co. Advancing Hispanic & Latinos Summit	2022
Virtual Participant, Asana, AsanaLaunch Interview Prep Series (1 of 50)	2022
Participant, JP Morgan, Advancing Black Pathways in AI & Quant Modelling Summit	2021
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, JP Morgan, Advancing Black Pathways in Data Science	2021
Participant, TwoSigma Mock Interview Day for Early Career Women (Quant Research)	2021
Participant, Hudson River Trading (HRT) Systems Engineering Tech Talks (1 of 14)	2021
Participant, Adobe, "The Future of Creativity" (Virtual)	2020
Participant, Microsoft Research, Frontiers in Machine Learning (Redmond, remote)	2020
Participant, Discover Bloomberg: Women in Engineering event (New York, remote)	2020
Participant, Twitter PhD ML Flock Event (New York, Boston office)	2019



## GRADUATE SCHOOL INTERNSHIPS

<b>JP Morgan</b> , Quantitative AI Research, Summer Associate (New York) (1 of 10) (mentors: S. Mishra PhD, D. Ley, A. Anzagira, E. Albini, D. Magazzeni, PhD)	2022
<b>Summer of Bitcoin</b> , PhD Research intern (mentor: R. Pickhardt)	2022
- Modelling congestion games for Simulating Price of Anarchy Selfish Routing to show the Boundary of Channel Depletion in the Bitcoin Lightning Network	
<b>Microsoft Research</b> , Independent Contractor, Summer 2021 (New York: remote)	2021
- Reinforcement Learning Distributed pipeline project for Vowpal estimators library	
<b>Microsoft</b> , PhD Intern, Summer 2021 (Redmond: remote) (mentor: P. Angulo, PhD)	2021
- Whitepaper: Fair, private and storage-efficient Telemetry Client-side aggregation	
<b>Autodesk</b> , PhD Intern, Summer 2020 (Pier 9, San Francisco: remote)	2020
- Renyi-Differential Privacy prototyping project for Distributed Databases	

## RELEVANT WORK / INDUSTRY EXPERIENCE (Pre-Grad school)

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

## NON-ACADEMIC SERVICE (ABRIDGED)

Invited Finalist Judge, Technovation, AI for Good	2021
Participant, Git Contributors Inclusion Summit	2020
Reviewer, Code2040 Application Essays	2020
Reviewer, OpenMined Differential Privacy articles	2020
Judge, DataKind, Data.org, Inclusive Growth and Recovery Challenge	2020
Google Developer Student Club Lead (for University of Vermont)	2019
Reviewer, Travel Grant Applications, Clojure Conj (2 rounds)	2017

---

## OTHER (NON-INDUSTRY) TALKS (ABRIDGED)

"A Journey through Unboundedness of ranks of Elliptic Curves", (15 minute talk)	2022
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
ICLR, Main Conference, Opening Remarks by DEI Chairs	2022
- "Broadening Participation in Research Initiative" (with R. Liu) (5-10 minutes)	
"Composable Forgetful Isogeny Graph Cryptography", Google CSRMP Research	2021
"Isogeny Graph Cryptography", School for Poetic Computation, Re-learning to love Maths	2021
"Isogeny Graph Cryptography", School for Poetic Computation, "Learning to Love Maths"	2021
Invited Panelist, Peer-connected Undergraduate Research Exploration in Computer and Information Science and Engineering ( <a href="#">PRE.CISE</a> )	2021
University of Vermont, CIS196, Privacy Law Research Talk	2021
PLAID Lab speaker, "What Scientists can learn from Artists"	2020
PLAID Lab Speaker, "Information Theory: from Spacecraft to Blockchain"	2021

## **OTHER (NON-INDUSTRY) TALKS (ABRIDGED)**

CS Crew Project talk : contributing to Maths software (CodeWorld, SageMaths) 2019

## **INDUSTRY TALKS (ABRIDGED)**

“Isogeny-Based Cryptography”, JP Morgan AI Research Cryptography Group (30 min) 2022

“Prediction Sensitivity for Fairness in AI”, Jane Street Symposium (15 minutes) 2021

“Renyi-Differential Privacy”, Autodesk UX Group (20 minutes) 2020

## **CLASSES (PhD)**

Doctoral Research with advisors C. Vincent and J. Near 2021-present

Complex Analysis taught by C. Vincent (Fall 2022) 2022

Graduate Combinatorics (Spectral Graph Theory) taught by P. Rombach (Fall)

Independent Study: Category Theory taught by A. Patania (Fall)

Random Probabilistic Graphs, taught by P. Rombach (Spring 2022) 2022

Abstract Algebra IV A: (Ring & Module Theory, Category Theory) taught by T. Dupuy (Fall)

Abstract Algebra IV C: (Elliptic Curves & Modular Forms), taught by C. Vincent (Spring)

Abstract Algebra I taught by P. Rombach (Commutative Group theory) (Fall 2021) 2021

Abstract Algebra III taught by C. Vincent : (Fields, Rings, Galois Theory) (Fall)

(Post-quantum) Mathematical Cryptography, taught by C. Vincent (Spring 2021) 2021

Privacy, Law and Policy, taught by R. Kriger (Spring)

Secure Distributed Computation; taught by J. Near using Python (Fall) 2020

Machine Learning; taught by S. Wshah using Python (Spring) 2020

Doctoral Research with advisors J. Near and D. Darais (Spring, Fall) 2019-2020

Data Privacy; taught by J. Near using Python (Fall) 2019

Software Verification; taught by D. Darais using Agda (Fall) 2019

Computer Human Interaction; taught by J. Bongard (Fall) 2019

## **CLASSES (AUDIT)**

UVM: Topology (Point-Set Topology) taught by C. Vincent (Fall) 2022

Graph Theory taught by P. Rombach (Fall)

Theory of Algebraic Differential Equations taught by T. Dupuy (Fall)

Elementary Number Theory taught by C. Vincent (Spring)

Fundamentals of Mathematics taught by T. Dupuy : (writing proofs) (Spring)

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

## **CLASSES (RELATED)**

Rewriting the Code (RTC) Blockchain Basics + Developer Workshop 2021

## **HACKATHONS**

R Data Hackathon 2021, First Place, “Cast and Gender Roles in Movie Data” 2021

- Our group won First place at the R Data Hackathon 2021 for Best Visualization

## HACKATHONS

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
- One of [top four winning teams](#) chosen

**Competitive / Hobby Puzzle-Solving:** Top ~0.30% CodeWars (3 kyu, peak rank: 0.1%)

**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,  
Career Girls, Dataiku, Scott Hanselman's Podcast, NASA Tech Briefs (40th anniversary),  
Variety, the Los Angeles Times, Black Girls Code colouring book on Women Scientists, etc.

## GUEST WRITER (SELECTED)

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

Blog posts, **Harvard Tech X Social Impact Fellowship** (3 articles) 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