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

---

University of Vermont, PhD candidate	***2019-present***

Computer Science PhD student, minor in Pure Mathematics

RESEARCH EXPERIENCE:

Research Assistant (Vermont)	***2021-2024***

Supervisors: C. Vincent, J. Near: Research on Isogeny Graph Cryptography, Mathematical Cryptography

Research Assistant (Vermont)	***2019-2021***

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

Conference Publications:

- *"Continual Audit of Individual Fairness in Deployed Classifiers via Prediction Sensitivity"* (**Maughan, K**, I. Ngong and J. Near) (under review) — *2021*

Workshop Publications:

- *"Attribute Differential Privacy"* **(Pre-print available upon request)** (**Maughan, K.** and Near, J.) — *2021*
- *"Towards a Measure of Individual Fairness for Deep Learning"* (**Maughan, K.** and Near, J.) - presented as poster for **MD4SG 2020** — *2020*
- *"Towards Auditability for Fairness in Deep Learning"* (Ngong, I., **Maughan, K.** and Near, J.)- presented as poster for **AFCI at NeurIPS** — *2020*
- *"Archipelago Penseé"* (**Maughan, K**.) presented artwork and writing as a poster: **RAIS (Resistance AI) at NeurIPS** — *2020*

Graduate Teacher's Assistant, Fall/Spring 2019-2020 (Vermont)	***2019-2020***
Compiler Construction with Haskell (taught by Joe Near)	*2020*
Advanced Web Design (taught by Bob Erickson)	
Programming with Matlab (taught by Radhakrishna Dasari)	*2019*
Data Privacy with Jupyter, Python (taught by Joe Near)	

GRANT WRITING / PROPOSALS

- *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*

GRANT WRITING / PROPOSALS

- ❖ CDS&E Computational and Data-Enabled Science and Engineering   2020
  Database Grant Proposal for SageMaths (as Key Personnel)
  (PI B. Hutz, PhD) (not awarded)
- ❖ Google Summer of Code, Proposal to Haskell.org   2018
  (Awarded $6,000)
- ❖ Helium Grant, (for exploring questions on the edge of mainstream thinking)   2018
  (Awarded $1000)

MERIT-BASED MENTORSHIPS / RESEARCH MENTORSHIPS

Mentee, AiC Connectors Program, (TBD)	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, Global Outreach Mentorship with S. Gupta, PhD (EC 2020)	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
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

RESEARCH PhD INVITATIONS (ABRIDGED)

Virtual Participant, MSRI: Connections Workshop: 2023
- Algebraic Cycles, L-Values and Euler Systems
- Introductory Workshop: Algebraic Cycles, L-Values and Euler Systems
- Shimura Varieties and L-Functions

Participant, Community-Driven Cryptography Seminar (Brown / John Hopkins)   2021-present

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

Virtual Participant, Arizona Winter School   2022
- Automorphic Forms beyond GL2: 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
- One of top four winning teams chosen

Participant, Scottish Programming Languages and Verification School   2021

Invited Participant, "Key themes for informing a Research Roadmap",   2021
The Alan Turing Institute:
- Invited Participant, "Threats and Opportunities for AI in Cybersecurity"   2021
- Invited Participant, "Society-centric approaches to AI challenges in   2021
- Invited Participant, "Environmental Enables for AI challenges in   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)

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

MERIT-BASED GRANTS / FELLOWSHIPS / SCHOLARSHIPS (ABRIDGED)

Fellow, BlackComputeHER (2022-2023)   2022
Google Grace Hopper Conference (GHC) Scholarship   2021
NCWIT Collegiate Award Finalist (1 of 80)   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

MERIT-BASED GRANTS / FELLOWSHIPS / SCHOLARSHIPS (ABRIDGED)

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

OTHER GRANTS/ FELLOWSHIPS (ABRIDGED)

Northeast Combinatorics, Discrete Maths Day (TBD)	*2022*
Participant, Roots of Unity Summer School: Arithmetic Geometry group (fully-funded)	*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*
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)

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	*2018*
(Systems, Programming, Languages, and Applications) (declined offer)	

INDUSTRY PhD INVITATIONS (ABRIDGED)

Fellow, JP Morgan, Advancing Black Pathways in AI & Quantitative Modelling Program	*2022*
Virtual Participant, Jane Street's Preview Program, The Game Show / Trading Games	*2022*
Participant, JP Morgan, Advancing Black Pathways in AI & Quant Modeling Summit	*2021*
Participant, Facebook, Amplified: Above & Beyond Computer Science Program (PhDs)	*2021*

INDUSTRY PhD INVITATIONS (ABRIDGED)

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

JP Morgan, Quantitative AI Research, Summer 2022 (New York) (1 of 10)	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

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 (remote)	2018
Mozilla: 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)

Brown University, Fair February talk on Security, Privacy, Fairness	2022
Meetup "Math for Math's Sake", Virtual Lightning Talk (10-15 minutes) "Isogenies, Elliptic Curves and Random Walks on Random Graphs	2022
"Composable Forgetful Isogenies", Google CSRMP Research Alumni Talk	2022
"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 (PRE.CISE)	2021
University of Vermont, CIS196, Privacy Law Research Talk	2021
PLAID Lab speaker, "What Scientists can learn from Artists"	2020

OTHER (NON-INDUSTRY) TALKS (ABRIDGED)

PLAID Lab Speaker, "Information Theory: from Spacecraft to Blockchain"   *2021*
CS Crew Project talk : contributing to Maths software (CodeWorld, SageMaths)   *2019*

CLASSES (PhD)

Doctoral Research with advisors Joe Near and Christelle Vincent   *2021-present*
Random Probabilistic Graphs, taught by Puck Rombach (Spring)   *2022*
Abstract Algebra IV A: (Ring & Module Theory, Category Theory) taught by Taylor Dupuy   *2022*
Abstract Algebra IV C: (Elliptic Curves & Modular Forms), taught by Christelle Vincent   *2022*
Abstract Algebra I taught by Puck Rombach (Commutative Group theory) (Fall)   *2021*
Abstract Algebra III taught by Christelle Vincent : (Fields, Rings, Galois Theory) (Fall)   *2021*
(Post-quantum) Mathematical Cryptography, taught by Christelle Vincent (Spring)   *2021*
Privacy, Law and Policy, taught by Ryan Kriger (Spring)   *2021*
Secure Distributed Computation; taught by Joe Near using Python (Fall)   *2020*
Machine Learning; taught by Safwan Wshah using Python (Spring)   *2020*
Doctoral Research with advisors Joe Near and David Darais (Spring, Fall)   *2019-2020*
Data Privacy; taught by Joe Near using Python (Fall)   *2019*
Software Verification; taught by David Darais using Agda (Fall)   *2019*
Computer Human Interaction; taught by Josh Bongard (Fall)   *2019*

CLASSES (AUDIT)

UVM: Elementary Number Theory taught by Christelle Vincent (Spring)   *2022*
Stanford EE 374 : Internet-Scale Consensus in the Blockchain Era   *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*

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*

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

ACADEMIC ASSOCIATION FOR COMPUTING MACHINERY (ACM) MEMBERSHIPS

Student Member, International Association of Cryptologic Research (IACR)   *2020-present*
Student Member, IEEE Computer Society Technical Committee on Security and Privacy *2021-present*
SIGecom Special Interest Group on Economics and Computation   *2020-2021*

NON-ACADEMIC MEMBERSHIP

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*