Krystal Maughan

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

Research Interests: Mathematical Cryptography, Elliptic Curves, Random Processes, Computational Number Theory (Arithmetic Geometry), Coding Theory (Error-Correcting Codes), Algebraic Graph Theory, Quantum Algorithms, Quantum Resource Estimation

---

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, Algebraic Graph Theory and Quantum Computing, Abstract Algebra I (Groups), III (Rings/Fields/Galois Theory), IV (Category Theory, Lie Algebra), Privacy Law and Policy, Machine Learning, Data Privacy, Software Verification (Agda), Computer Human Interaction.*

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

RESEARCH EXPERIENCE:

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

- *Mathematical Cryptography Research*

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

Publications

- *"Foldable, Recursive Proofs of Isogeny Computation with Reduced Time Complexity"- accepted to* ***IEEE Quantum Computation and Engineering (QCE)*** *(**Maughan K.**, Near J., Vincent C.)* — *2024*
- *"Machine Learning for Modular Multiplication"* — 2024
  Women in Numbers VI (2024) : Research Directions in Number Theory
  (Lauter K.,Li C., **Maughan K.**,PhD, Newton R., Srivastava M.)

Pre-prints:

- *"Improving Utility for Analysis of Correlated Columns using Pufferfish Privacy" (**Maughan, K.** and Near, J.)* — *2022*
- *"Continual Audit of Individual and Group Fairness in Deployed Classifiers via" "Prediction Sensitivity" (**Maughan, K.**, Ngong I., Near J.)* — *2022*

Accepted Workshop Conference Posters:

- *Foldable Proofs of Isogeny Knowledge* — *2024*
  *presented at **11th Heidelberg Laureate Forum (HLF)**, Flash Poster Session (1 of 30)*

Accepted Workshop Conference Posters:

- *Post-Quantum Secure Recursive Proofs of Isogeny Knowledge with Reduced Time Complexity (Maughan, K. and Vincent C., and Near, J.) at **CQIQC-X*** *2024*
- *Post-Quantum Secure Recursive Proofs of Isogeny Knowledge with Reduced Time Complexity (Maughan, K. and Vincent C., and Near, J.) at **USTARS 2024*** *2024*
- *Post-Quantum Secure Recursive Proofs of Isogeny Knowledge with Reduced Time Complexity (**Maughan, K.**, and Vincent C., PhD) accepted at **QIP 2024** Poster for Quantum Information Processing conference, Taipei, Taiwan* *2024*
- *"Compositional Isogeny Schemes"- poster presented, **CrossFyre at Eurocrypt** Poster for workshop on Provably Robust Schemes, Lyon, France (***Maughan, K**) *2023*
- *"Compositional Isogeny Schemes"- presented as poster at **ACM Richard Tapia** Poster Competition at Conference, Washington, D.C. (***Maughan, K**) *2022*
- *Prediction Sensitivity: Continual Audit of Counterfactual Fairness in Deployed Classifiers (**Maughan, K.**, Ngong, I., Near, J.) (presented as poster at "Equity and Access in Algorithms, Mechanisms and Optimization **(EAAMO) Doctoral Consortium**"* *2022*
- *"Towards a Measure of Individual Fairness for Deep Learning" (**Maughan, K.** and Near, J.) - presented as poster for **MD4SG** (presented at "Mechanism Design for Social Good" conference)* *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 as a poster for Resistance AI (**RAIS) at NeurIPS*** *2020*

Collaboration on Other Research Projects in Progress:

- *Mathematical Cryptography: Work on Compositional Isogeny Schemes (ongoing) (PI: C. Vincent, Near J. PhD, **Maughan, K.**)* *2022-present*
- *Number Theory paper (**Maughan, K.**)* *2024-present*
- *Error-correcting codes / LDPC using group algebras* *2023-present*
  (PI: Chimal-Dzul, H., Hoffer W., **Maughan, K.**, Maya N.A., W., Morris K.)
- *Expander properties of Isogenies* *2023-present*
  *(Arpin, S., Bowen R., Clements J., Codogni G., Eisenträger K., Ghantous W., Bo Lau J., LeGrow J., Macula J., Mahaney W., **Maughan. K**., Morrison T., Orvis E., Rickards J., Sabitova M., Scullard G., Zobernig L.)*
- *"Experimental Investigation of Lehmer's Conjecture for Elliptic Curves", (Clark J. M., Dombrowsky C., Iranzo M. C., Katz S., **Maughan K.**, Orvis E., Supervised by: Looper N., PhD and Chidambaram S., PhD, Silverman J., PhD)* *2024-present*
- Graphs research, Pure Maths (***Maughan K.,** PI: Rombach, P.*) 2023-present
- *Summer Research Project, Advanced Cryptography Group* *2024-present*
  *(Alamati N., Chakraborty S., **Maughan K.,** Raghuraman S., Rindal P.)*
- *Post-Quantum Cryptography project* *2024-present*
  *(**Maughan K.,** and other co-authors, PI: Cherkaoui, I.)*
- *Quantum Backtracking for Constraint Satisfaction Problems (CSP)* *2023-2024*
  *(Jhunjhunwala V., **Maughan K.** PI: Schirman E.)*

Collaboration on Other Research Projects in Progress:

- ❖ Independent research project 2023-present
  (*PI: Lees A., PhD,* ***K. Maughan***)
- ❖ *Summer of Bitcoin (Virtual) "Price of Anarchy in Selfish Routing on the Lightning Network" (R. Pickhardt, S. AIscher,* ***K. Maughan****)* *2022*

Whitepapers (Data Privacy and Security):

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

INVITED VISITING PhD STUDENT RESEARCHER (UC Berkeley)

- ❖ *Simons Institute, "Quantum Algorithms, Complexity and Fault Tolerance" 2024*
  - *Invited as a visiting researcher for workshop and Error Correcting Codes*
  - *Participated in Bootcamp (Berkeley, California from Jan 22nd to Feb 16th)*
  - *Hosted by Irani, S., PhD (UC Irvine, Simons Associate Director)*
  - *Provided with Funding for Travel, Lodging and Per-Diem (1 of 8, $3,500 U.S.)*

SPECIAL HONOURS

- ❖ *Invited Student Participant, 11th Heidelberg Laureate Forum (HLF) 2024*
  - *Handpicked as 1 of 100 candidates in Maths (or Computer Science) to attend the Forum in Heidelberg. Chosen candidates represent promising young researchers who are given the opportunity to interact with the brightest minds in Mathematics and Computer Science (i.e. winners of the Turing award, The ACM Prize in Computing, Fields Medal, IMU Abacus Medal and Nevanlinna Prize).*
- ❖ *Chosen as 1 of 30 to present a poster at the Heidelberg Laureate Forum 2024*
  - *chosen participants receive a certificate*
- ❖ *Named on LDV Capital List as 1 of 120 Brilliant Women in Visual Tech and AI 2024*

TEACHING EXPERIENCE

- ❖ ***PhD Teaching Fellow****, iSchool Inclusion Institute (i3), "Computational Thinking" 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*
  Compiler Construction (with Haskell), Programming for Engineers (with Matlab), Data Privacy (Differential Privacy, K-anonymity, Machine Learning with Python),
- ❖ ***Graduate Teaching Assistant****, University of Vermont (Fall / Spring) 2019-2020*
  Advanced Web Design (Lead Teaching Assistant)

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*

GRANT WRITING / PROPOSALS (SELECTED)

- ❖ *Microsoft Research, Reinforcement Learning Open Source Festival Proposal 2021*
  (Awarded $10,000)
- ❖ *Google Summer of Code, Proposal to Haskell.org 2018*
  (Awarded $6,000)
- ❖ *Helium Grant, (for exploring questions on the edge of mainstream thinking) 2018*
  (1 of 11 chosen out of 700 applicants; Awarded $1,000)

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*

ACADEMIC REVIEWER (SELECTED)

AAAI-24 Workshop on Privacy-Preserving Artificial Intelligence (2024), Safe and Trustworthy AI (STAI) at International Conference on Logic Programming 2023 (ICLP),
Algorithmic Fairness through the Lens of Time at NeurIPS 2023 (AFT), 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, Black in AI Workshop @ NeurIPS (2020-present), Springer's AI Ethics Journal

REVIEWER (OTHER)

Effective Haskell, by R. Skinner: book on Haskell programming.

SUMMER SCHOOLS

(all summer schools were fully funded: lodging, flight, registration provided)

- *Participant, RSim (Quantum Simulation) Summer School 2024*
  - *(August 8th through 11th, Rhode Island)*
- *Participant, SLMath 1068, IBM Research Zurich, (Zurich, Switzerland) 2024*
  "Introduction to Quantum-Safe Cryptography" (June 24th to July 5th),
  - *Covers lattice, code-based, isogeny-based and multivariate cryptography*
  - *Organised by Bootle J., and De Feo L.*
- *Virtual Participant intern, Co-design Center for Quantum Advantage (C^2QA) 2024*
  - *QIS 102 Applied Quantum Computing Summer School at Brookhaven National Laboratory (June 10th-June 28) (provided $500 weekly stipend) (I Personally declined opportunity because of my internship offer)*
- *Hausdorff Research for Mathematics: Formalization of Mathematics (Bonn) 2024*
  - *Workshop focused on formalising Mathematics in proof assistant*
  - *In either Lean, sTEX, Naproche, Coq, Isabelle HOL, etc (May 13-17)*
- *Participant, IAS/ PCMI Graduate Research Summer School, (3 weeks) 2023*
  Topic of "Quantum Computing" covered algorithms, information theory, Cryptography and error-correcting codes.

RESEARCH PhD INVITATIONS (ABRIDGED)

- *Participant, Twelfth Summer School on Formal Techniques + FMiTF Bootcamp 2023*
    - *Two-week workshop in Atherton, California covering Alloy, PVS, Vampire And interactive proof checkers for applied formal methods domains*

Virtual Participant, Physics of Quantum Information, Perimeter Institute (Canada) 2024

Participant, 10th International Conference on Quantum Information and Quantum Control (CQIQC-X) at the Fields Institute (Toronto, Canada) 2024

Participant, Underrepresented Students in Topology and Algebra Research Symposium 2024

- *USTARS: granted lodging, travel, meals (University of Iowa)*

Virtual Participant, Summer of Quantum, Laboratory for Physical Sciences (LPS) (2 wks) 2023

- *Qubit fundamentals, hardware, Quantum Algorithms, error-correcting codes*

Participant, QSim Summer School (Rhode Island) (Rhode Island, United States) 2024

Mentee, Supervised Program for Alignment Research (SPAR) 2024

- *Chosen to work on research for Satisfia research project by PI Heitzig J.*

Virtual Participant, "Connecting Heavy Tails and Differential Privacy in Machine Learning"2024

- *Hosted by the Alan Turing Institute and the Newton Gateway for Mathematics*

Participant, WIN6, (mentors: Lauter K., Newton R.) 2023

- *Research project at BIRS, to be published in 10th WIN proceedings 2024 (Banff, Canada)*
- *Received award for lodging, travel (~1 of 42) (March 26th to March 31st)*

Participant, American Institute of Mathematics (AIM) workshop on 2024
"Post-Quantum Group-Based Cryptography" (Pasadena, California) ($750 funding)

Participant, Hausdorff Research Institute for Mathematics, "Formal Mathematics" (Lean) 2024

- *Given housing, funding for flight (1100 Euro)*

Participant, BIRS, Isogeny-based cryptography Banff research workshop 2023

- *Co-organized by de Quehen, Petit C. and Martindale C.*

Participant, SQuInT Chemistry Fellowship (to attend Southwest Quantum Information 2023

Invited Participant, 2023 Fields Medal Student Symposium, Birkar C., (Virtual) 2023

Participant, Quantum Workshop at North Carolina State (Nov 18-19) 2023

Participant, High Assurance Cryptographic Software (HACS) (Toronto, Canada) 2024

- *Received funding for flight, lodging, and granted free registration ($1200 funding)*

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 (1 of 50),"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 (4th edition) 2023

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

RESEARCH PhD INVITATIONS (ABRIDGED)

Participant, Twelfth Summer School on Formal Techniques + FMiTF Bootcamp 2023
- *Received admission, housing and funding for flight*
- *Labs using Vampire Theorem Prover, Alloy, TPTP, PVS, Easycrypt*
- *Guest lecture on Paxos by L. Lamport (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, "Abelian Varieties" 2024
- *Abelian Varieties (Tucson, AZ)*

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

Selected Participant, GREPSEC VI (1 of 42) 2023

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)

Fellow, SQuInT Chemistry Fellowship (to attend Southwest Quantum Information And Technology (SQuInT) (flight, housing and registration covered) (1 of 5) *2023*

Fellow, Institute for Logic and Data Science (ILDS) Coq and Lean Autumn School *2023*

- *Part of the Working Formal Methods Symposium (Bucharest, Romania)*

SOUPS 2023 Grant for Black Computer Science Students (USENIX 2023) *2023*

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 4 teams in hackathon*

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)

Quantum Information Processing (QIP) Student Stipend *2024*

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*

PL+HCI Swimmer Summer School (on Programming Languages and Usability) *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*
- *Invited Participant, Rochester Institute of Technology: Pathways to RIT Computing edition 2023*

INDUSTRY PhD INVITATIONS (ABRIDGED)

Participant, Goldman Sachs' Women's Possibilities Summit (~10% of 11,000 applicants) 2024
Participant, Adobe's Experience Day for Research 2023
Participant, Goldman Sachs HackerRank Prep 2023
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

Visa Research, *Staff Research Scientist Intern, Advanced Cryptography Group 2024*
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 (ACADEMIC) TALKS (ABRIDGED)

"Experimental Investigation of Lehmer's Conjecture for Elliptic Curves", (20 minutes) *2024*
- *Talk at the Arizona Winter School, on the topic of Abelian Varieties.*
- *Joint with Clark J. M., Dombrowsky C., Iranzo M. C., Katz S., Orvis E., (SW-AWS)*

Invited Talk, Carnegie Mellon University Graduate Computer Science Seminar (20 mins) *2024*
- *"Post-Quantum Secure Recursive Proofs of Isogeny Knowledge with Reduced Time Complexity; a case for Formal Methods", SSSG seminar*

Simons Institute, Quantum Fault Tolerance workshop Lightning Talk (10 mins) *2024*
Presenter, Google CSRMP, "Quantum backtracking and implications to cryptography" *2023*
Number Theory in Quantum, American Institute of Mathematics (AIM), *2023*
Roots of Unity Workshop, Caltech (Pasadena, Los Angeles)
"Compositional Isogeny Schemes", Tapia Doctoral Consortium (45 minutes) *2022*
"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*
"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)

IBM Research "Foldable Schemes for Isogeny-Based Cryptography" (10 minutes) *2024*
- *Talk given at SL Math's "Quantum Safe Cryptography" workshop in Zurich*

"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*

MERIT-BASED MENTORSHIPS / RESEARCH MENTORSHIPS (SELECTED)

Mentee, Goldman Sachs Possibilities Mentorship, Noonan, H. *2024*

Mentee, Black Scholars Doctoral Mentorship *2023*

- *Mentor: K. Clark, PhD.*

Mentee, Institute for African-American Mentoring in Computing Sciences (IAAMCS) *2023*

- *Mentor: J. Gilbert, PhD*

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*

CLASSES (AUDIT)

Preliminary Arizona Winter School, "Abelian Varieties over Finite Fields", by L. Dembele *2023*

Preliminary Arizona Winter School, Model Theory and Applications, taught by R. Nagloo *2022-2023*

QWorld QClass 551: Quantum Software Development with Classiq *2023*

- *Quantum Algorithm Research Project under mentorship of a Principal Investigator*
- *Requires project written manuscript (1 out of 80 accepted from ~400 applicants)*
- *Received Classiq Bootcamp certificate (10/13/23)*

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*

Matroids & Polytopes, Theory of Algebraic Differential Equations, Elementary Number Theory, Fundamentals of Mathematics, Extremal Graph Theory, Model Theory and Applications

- *IBM Qiskit Global Summer School (Quantum Computation using Qiskit)* *2024, 2020*

HACKATHON (Quantum Computing) *2023-2024*

- *Project: "Quantum project using noisy intermediate-scale quantum (NISQ) Devices"*
  - *Project on homomorphic encryption for federated quantum models using Genomic DNA data (team of 3).*
  - *Used Qiskit, Pennylane, Flwr, Tenseal, implemented Differential Privacy And Homomorphic encryption to win First place ($10,000 team award)*

Skills: Python, LaTeX, SageMaths, Qiskit, Classiq, Haskell, Matlab, Jupyter, Pytorch, SQL, AWS, Azure, PySpark, Git, Lean (3; not 4…yet!), Z3, writing proofs.

PRESS (SELECTED)

Blogpost for the Mathematical Association of America (MAA) Grad Student Blog (April) 2024
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, Code 2040 Alumni event (2024) QC-AI Meetup, etc.

LEADERSHIP and SERVICE (SELECTED)

Student Volunteer, IEEE International Conference on Quantum Computing 2023, 2024
And Engineering (QCE)
Co-Workshop Organizer, Tiny Papers Track at ICLR (Vienna, Austria) 2024
(Junior) Program Committee, Safe and Trustworthy AI (STAI) at the International 2023
Conference on Logic Programming (ICLP)
Co-Committee / Area Chair, Broadening Participation and Tiny Papers Workshop at 2023
International Conference of Learning Representation (ICLR)
Co-Committee, Broadening Participation and Co-Submitting Summer School at 2022
International Conference of Learning Representation (ICLR)
Program Committee, BlackAIR Programme 2021
Virtual Co-Organizer, Women in Machine Learning, Black In AI at NeurIPS (NeurIPS) 2020
Virtual Volunteer Chair, Empirical Methods in Natural Language Processing (EMNLP) 2020
Virtual Student Volunteer, International Conference of Machine Learning (ICML) 2020
Virtual Student Volunteer, International Conference of Functional Programming (ICFP) 2020
Student Volunteer, Programming Languages and Design Conference (PLDI) 2018
Student Volunteer, International Conference of Functional Programming (ICFP) 2018
Invited Student Volunteer, SIGPLAN conference on Systems, Programming, 2018
Languages and Applications (SPLASH) (declined offer)
Student Volunteer, Principles of Programming Languages (POPL) 2017

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, Quantum Resource Estimation Group *2023-present*
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*

NON-ACADEMIC MEMBERSHIP

Member, She256 *2021-present*

Member, Women in Security and Privacy (WISP) *2020-present*

Member, IEEE Information Theory Society, Santa Clara Valley Chapter *2016-present*