Harjasleen Malvai

harjasleenmalvai@gmail.com

Education

University of Illinois, Urbana-Champaign — **Urbana-Champaign, IL**
PhD Student, Computer Science — Aug 2021 - Present

Cornell University — **Ithaca, NY**
Master of Science, Computer Science — Aug 2018 - Aug 2021

Brown University — **Providence, RI**
Sc.B. Mathematics & A.B. Computer Science, Davis and Brown University Scholar. — Aug 2013 - Dec 2017
Recipient of the Senior Prize in the Department of Computer Science.

Publications

Practical Proofs of Parsing for Context-free Grammars
Malvai, H., Neven, G., Miller, A., Hussain, S. — 2024
(In preparation)

SoK: Transparency Systems for Key-Value Stores
Malvai, H., Zitek, A., Meiklejohn, S., Bonneau, J. — 2024
(In preparation)

SGXonerate: Finding (and Partially Fixing) Privacy Flaws in TEE-based Smart Contract Platforms Without Breaking the TEE
Jean-Louis, N., Li, Y., Ji, Y., Malvai, H., Yurek, T., Bellemare, S., Miller, A. — 2024
Proceedings on Privacy Enhancing Technologies — Bristol, UK

Parakeet: Practical Key Transparency for End-to-End Encrypted Messaging
Malvai, H., Kokoris-Kogias, L., Sonnino, A., Ghosh, E., Oztürk, E., Lewi, K., Lawlor, S. — 2023
Proceedings of the 2023 Network and Distributed System Security (NDSS) Symposium — San Diego, CA

Aggregating and thresholdizing hash-based signatures using STARKs
Malvai, H., Khaburzaniya, I., Chalkias, K., Lewi, K. — 2022
Proceedings of the 2020 ACM ASIA SIGSAC Conference on Computer and Communications Security — Nagasaki, JP

CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability
Maram, D., Malvai, H., Zhang, F., Jean-Louis, N., Frolov, A., Kell, T., Lobban, T., Moy, C., Juels, A., Miller, A. — 2021
Proceedings of the 42nd IEEE Symposium on Security and Privacy — San Francisco, CA

DECO: Liberating Web Data Using Decentralized Oracles for TLS.
Zhang, F., Maram, S. K. D., Malvai, H., Goldfeder, S., Juels, A. — 2020
Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. — Orlando, FL

SEEMless: Secure End-to-End Encrypted Messaging with less trust
Chase, M., Deshpande, A., Ghosh, E., Malvai, H. — 2019
Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. — London, UK

Consensus and clustering in opinion formation on small-world networks.
Bujalski, J., Dwyer, G., Kapitula, T., Le, Q., Malvai, H., Rosenthal-Kay, J., and Ruiter, J. — 2018
Philosophical Transactions of the Royal Society A.

Taming Information Leaks in Machine Learning.
Mejia Domenzain, L., Dibbern, N. and Malvai, H. — Jan 2018
Presented paper at the Joint Mathematics Meetings special session — San Diego, CA
Research in Mathematics by Undergraduates and Students in Post-Baccalaureate Programs, I.

Awards and Honours

Applied Networking Research Prize, Winner. — 2024
Secret Network Bug Bounty for SGXonerate — 2024
Berkeley RDI ZKP Hackathon, Benchmarking Category, 1st Place — 2023
IC3 Hackathon, 2nd Place — 2023
, 1st Place
Facebook PhD Fellowship, Finalist.
Initiative of CryptoCurrencies and Contracts Fellowship, Awarded fellowship (including tuition and stipend) for 2019-2020 academic year.
Brown University Department of Computer Science, Awarded department senior prize for academic work as well as service to Brown CS.
Brown University Department of Mathematics, Third place in the Hypatia Math Exam for Freshman.

(Continued on next page)

Graduate Research Experience

University of Illinois, Urbana-Champaign, Department of Computer Science
Graduate Researcher **Urbana-Champaign, IL**
- Advised by Prof. Andrew Miller. August 2021-Present

Chainlink Labs
Research Intern **Remote, USA**
- Advised by Prof. Dahlia Malkhi. June 2023 - Sept. 2023

Facebook, Novi Cryptography Research
Research Intern **Menlo Park, CA**
- Collaborated with Dr. Kevin Lewi to implement SEEMless and Parakeet. June 2021 - Dec 2022

Cornell University, Department of Computer Science
Graduate Researcher **Ithaca, NY**
- Advised by Profs. Ari Juels and Andrew Miller. Oct 2018 - August 2021
- Collaborated with Prof. Elaine Shi.

Facebook, Novi Cryptography Research
Research Intern **Menlo Park, CA**
- Collaborated with Dr. Kevin Lewi to study biometric authentication without trusted hardware. May 2020-August 2020
- Reviewed literature on light client solutions.
- Implemented various cryptographic primitives in secure computation tools such as emp-toolkit, MP-SPDZ and jsnark.

Microsoft Research, Cryptography Research Group
Collaborator **Redmond, WA**
- Collaborating with Dr. Melissa Chase and Dr. Esha Ghosh to study public key infrastructure for secure messaging. Oct 2018 - Sept 2019
- Wrote code to experiment with performance, achieving a $>$ 20x speedup over existing research systems on backend updates while providing better privacy guarantees.
- Designed algorithms for compressed, persistent Patricia trees which provide a basis for other applications such as tamper evident logging.

Undergraduate Research Experience

Encrypted Systems Lab at Brown Computer Science Dept.
Undergraduate Research Assistant **Providence, RI**
- Collaborated with Prof. Seny Kamara to study Differentially private machine learning using secure multi-party computation. Sept 2017 - May 2018
- Reviewed literature and designed several components of the system.
- Wrote proofs of correctness and ϵ-differential privacy.

Cryptography, Anonymity, Privacy and Security Lab at Brown Computer Science Dept.
Undergraduate Research Assistant **Providence, RI**
- Collaborated with Prof. Roberto Tamassia and Esha Ghosh to study Zero-knowlege queries to a graph stored on the cloud. Sept 2017 - Aug 2018
- Prototyped graph data structure computations.
- Used Python's Charm Crypto Library to implement number theoretic computations.
- Designed and implemented algorithms to compute zero-knowledge accumulators and proofs.
- Used Python's multi-processing libraries and designed algorithms to optimize large computations.

Institute for Pure and Applied Mathematics - UCLA
Research in Industrial Projects for Students: Google Project, Researcher and Project Manager **Los Angeles, CA**
- Researched and prototyped problems on Preserving privacy in machine learning. June 2017 - Aug 2017
- Completed detailed statement of work, mid-term progress report and final report with team.
- Organized tasks, coordinated with team members and communicated with mentors.
- Made original models, reviewed literature, identified and solved relevant problems.
- Presented research to general as well as technical audiences.

University of Michigan, Department of Mathematics
NSF-Research Experience for Undergraduates: Researcher, Brown LINK Award Recipient **Ann Arbor, MI**
- Collaborated with Dr. Patrick Boland to study a Generalization of Dedekind Sums. May 2016 - Sept 2016
- Presented research at the Young Mathematicians Conference at OSU (Columbus, OH).
- Implemented algorithms for number theory computations (C++), made conjectures, proved original results.

Institute for Computational and Experimental Research in Mathematics
Summer@ICERM: Applied Math Researcher **Providence, RI**
- Worked in a team on Applied Math research modeling the spread of ideas using graph theory and differential equations. June 2016 - Aug 2016
- Made original models, reviewed literature, identified and studied interesting special cases.
- Ran MATLAB simulations to study the models.
- Presented a poster at the UTRA Research Symposium and at Nebraska Conference for Undergraduate Women in Mathematics.
- Academic paper accepted to Philosophical Transactions of the Royal Society A.

Division of Applied Mathematics at Brown University
Researcher in Generalizations of Chip-Firing Games **Providence, RI**
- Received the Katherin T. Romer Undergraduate Teaching and Research Award May 2015 - Aug 2015

to work with Prof. Caroline J Klivans.
- Studied the generalizations of Chip-Firing Games – a discrete dynamical system.
- Ran simulations, proved lemmas and read papers.

Undergraduate Conference Posters and Presentations

Women's Intellectual Network Research Symposium March 2017
- Accepted to present a poster on Providence, RI
  Consensus and clustering in opinion formation on small-world networks
  at the Women's Intellectual Network Research Symposium.
- Attended the various other mathematics talks and poster sessions at the conference.

Nebraska Conference for Undergraduate Women in Mathematics Feb 2017
- Accepted to present a poster on Lincoln, NE
  Consensus and clustering in opinion formation on small-world networks
  at the Nebraska Conference for Undergraduate Women in Mathematics.
- Funded by the Institute for Computational and Experimental Research in Mathematics and the Deparment of Mathematics at the University of Nebraska, Lincoln.
- Attended the various other talks and poster sessions at the conference.

Young Mathematicians Conference Aug 2016
- Accepted to present Generalized Dedekind Sums at the Young Mathematicians Conference. Columbus, OH
- Joint presentation with Samual Freedman of University of Michigan.
- Funded by the Department of Mathematics at Ohio State University.
- Attended various other mathematics talks and poster sessions at the conference.

Math Slam event hosted by Association for Women in Mathematics Brown Chapter Nov 2015
- Invited to present talk on Generalizations of Chip-Firing Games. Providence, RI

Workshops and Conferences Attended

Zero-Knowledge Week May 2023
- Attended talks and led unconference session on identity applications for zkp. Chicago, IL

NDSS Symposium April 2023
- Presented Parakeet. San Diego, CA

Zero-Knowledge Summit March 2022
- Presented WIP talk on comparing arithmetizations. Amsterdam, NL

IC3 Blockchain Camp June 2019, 2020, 2023, 2024
- Worked on a privacy-preserving auction using HoneyBadgerMPC (2019). Ithaca, NY

ACM SIGSAC Conference on Computer and Communications Security Nov 2019
- Presented conference talk on SEEMless. London, UK
- Received conference student scholarship.

Symposium on the Theory of Computing June 2019
- Attended various mentoring lunches, talks and workshops. Phoenix, AZ
- Funded by Prof. Elaine Shi and TCS Women.

Grace Hopper Convention Oct 2018
- Selected to attend the conference to help recruit women for Cornell's PhD program. Houston, TX
- Attended various technical and non-technical lectures, and workshops.
- Funded by Cornell University, Department of Computer Science.

DIMACS/Northeast Big Data Hub Workshop on
Overcoming Barriers to Data Sharing including Privacy and Fairness Oct 2017
- Attended two day workshop on private data sharing and differential privacy. Piscataway, NJ
- Funded by the workshop.

Graduate Research Opportunities for Women Oct 2017
- Selected to attend the two day conference to encourage women in Chicago, IL
  mathematics to consider future opportunities.
- The conference featured lectures, research talks and panels from faculty at various univerisities.
- Funded by Northwestern University, Department of Mathematics.

Research Visits

Microsoft Research November 2018
- Made a week long research visit to collaborate on SEEMless. Redmond, WA

Teaching

Cornell University, Department of Computer Science
Graduate Teaching Assistant **Ithaca, NY**
- Systems Security Aug 2020 - Present
  Held guest lectures, wrote assignments and rubrics, graded and helped with logistics.
- Blockchains, Cryptocurrencies, and Smart Contracts Jan 2019 - May 2019
  Worked on stencil code, assignments, rubrics and grading, held office hours, managed logistics.
- Security and Privacy Concepts in the Wild Aug 2018 - Dec 2018
  Wrote assignments and rubrics, held office hours, managed logistics, graded exams.

Brown University, School of Professional Studies
Executive Masters in Cybersecurity, Teaching Assistant **Providence, RI**

- Applied Cryptography and Data Privacy — March 2018 - Aug 2018

  Created lecture content, wrote assignments, conducted in-class discussions, graded assignments.
- Advanced Topics in Computer Security — March 2018 - Aug 2018

  Created lecture content, wrote assignments, conducted in-class discussions, graded assignments, created a web portal to access a Windows VM using Google Cloud Compute and Windows Server 2016.

Brown University, Dept. of Mathematics and Dept. of Computer Science

Undergraduate Teaching Assistant **Providence, RI**

- Computer Systems Security — March 2018 - May 2018

  Graded, held office hours, made assignments and in-class demos.
- Abstract Algebra — Sept 2015 - Dec 2015

  Graded for algebra course covering groups, rings and fields.
- Discrete Structures and Probability — Jan 2015 - May 2015

  Graded, wrote up solutions and held office hours.
- "How Big is Infinity? And other questions" and "Fundamentals for Calculus" — July 2014

  Graded, wrote up solutions, held office hours and lectured.

Brown University, Science Center

LaTeXWorkshop Leader **Providence, RI**

- Designed curriculum, created lesson plans and led workshops on LaTeX. — Jan 2014 - Dec 2019

Selected Coursework

Graduate **Ithaca, NY**

Computer Science: *Advanced Systems, Cryptography, Designing Secure Cryptography, Blockchains, Programming Languages.*

Undergraduate **Providence, RI**

Computer Science: *Discrete Structures and Probability, Logic for Systems, Computer Systems, Computer Systems Security (with Lab), Artificial Intelligence, Programming Languages, Theory of Computation.*

Mathematics: *Abstract Algebra (including Galois Theory, Representation Theory), Analysis (including measure theory), Cryptography, Topology, Probability, Graph Theory, Geometry, (graduate:) Manifolds, Number Theory.*

Selected Projects

Python: Implemented a blockchain, a SAT solver, Chip-Firing algorithms, binary decision diagrams, Neural Network, α-β Pruning.

C: Implemented a shell and malloc, designed a random maze generator and solver.

Julia: Implemented percolation, Random Cluster Model and Metropolis Algorithm to break the Shift Cipher.

Java: Implemented clients and a server to simulate and test a public key infrastructure.

Others: Designed and implemented a "secure" Dropbox in Go and various riddle solving models in Alloy.

Number Theory Textbook: Collaborated with Prof. Jeffrey Hoffstein on an undergraduate textbook.

Programming Languages and Technologies

Experience With: git, NTL, pandas, Linux/Unix, shell, Charm Crypto Library, Google Cloud Compute, Microsoft Azure, Bitmain, Antminer S1 and S9, TCP, Windows Server, Multiprocessing in Python.

Languages Used: Rust, various zkp DSLs, Python, C, Julia, MATLAB, C++, LISP, Ruby, Go, Java, model checkers (e.g. Idris and Alloy).

Leadership and Community Engagement

Girls' Adventures in Math, Volunteer

Helped organize food and logistics for math outreach event for middle-school girls.

Women in Science and Engineering, Mentor

One-on-one mentoring with freshman women interested in math or CS.

Algebra in Motion Mathematics Tutoring Program, Volunteer

In class and after school tutor at Hope High School.

Activities and Interests

Guitar, Philosophy, Literary Fiction, Teaching, Member Association for Women in Math chapter at Brown, Fitness, (Bowed and Plucked) String Instruments, Craft Chocolate.