

# Harjasleen Malvai

harjasleenmalvai@gmail.com

## Education

### University of Illinois, Urbana-Champaign

PhD Student, Computer Science

Urbana-Champaign, IL

Aug 2021 - Present

### Cornell University

Master of Science, Computer Science

Ithaca, NY

Aug 2018 - Aug 2021

### Brown University

Sc.B. Mathematics & A.B. Computer Science, Davis and Brown University Scholar.

Providence, RI

Recipient of the Senior Prize in the Department of Computer Science.

Aug 2013 - Dec 2017

## Publications

### 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 Ruiters, 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.

## Research Experience

### University of Illinois, Urbana-Champaign, Department of Computer Science

*Graduate Researcher*

- Advised by Prof. Andrew Miller.

Urbana-Champaign, IL

August 2021-Present

### Facebook, Novi Cryptography Research

*Research Intern*

- Collaborated with Dr. Kevin Lewi to implement SEEMless.

Menlo Park, CA

June 2021 - Present

### Cornell University, Department of Computer Science

*Graduate Researcher*

- Advised by Profs. Ari Juels and Andrew Miller.

- Collaborated with Prof. Elaine Shi.

Ithaca, NY

Oct 2018 - August 2021

### Facebook, Novi Cryptography Research

*Research Intern*

- Collaborated with Dr. Kevin Lewi to study biometric authentication without trusted hardware.

- Reviewed literature on light client solutions.

- Implemented various cryptographic primitives in secure computation tools such as emp-toolkit, MP-SPDZ and jsnark.

Menlo Park, CA

May 2020-August 2020

### Microsoft Research, Cryptography Research Group

*Collaborator*

- Collaborating with Dr. Melissa Chase and Dr. Esha Ghosh to study public key infrastructure for secure messaging.

- 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.

Redmond, WA

Oct 2018 - Sept 2019

(Continued on next page)

## Encrypted Systems Lab at Brown Computer Science Dept.

*Undergraduate Research Assistant*

Providence, RI  
Sept 2017 - May 2018

- Collaborated with Prof. Seny Kamara to study Differentially private machine learning using secure multi-party computation.
- Reviewed literature and designed several components of the system.
- Wrote proofs of correctness and  $\epsilon$ -differential privacy.

## Cryptography, Anonymity, Privacy and Security Lab at Brown Computer Science Dept.

*Undergraduate Research Assistant*

Providence, RI  
Sept 2017 - Aug 2018

- Collaborated with Prof. Roberto Tamassia and Esha Ghosh to study Zero-knowledge queries to a graph stored on the cloud.
- 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  
June 2017 - Aug 2017

- Researched and prototyped problems on Preserving privacy in machine learning.
- 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  
May 2016 - Sept 2016

- Collaborated with Dr. Patrick Boland to study a Generalization of Dedekind Sums.
- 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  
June 2016 - Aug 2016

- Worked in a team on Applied Math research modeling the spread of ideas using graph theory and differential equations.
- 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  
May 2015 - Aug 2015

- Received the Katherin T. Romer Undergraduate Teaching and Research Award 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.

## Awards and Honours

---

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.

## Undergraduate Conference Posters and Presentations

---

### Women's Intellectual Network Research Symposium

March 2017  
Providence, RI

- Accepted to present a poster on *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  
Lincoln, NE

- Accepted to present a poster on *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 Department of Mathematics at the University of Nebraska, Lincoln.
- Attended the various other talks and poster sessions at the conference.

### Young Mathematicians Conference

Aug 2016  
Columbus, OH

- Accepted to present Generalized Dedekind Sums at the Young Mathematicians Conference.
- Joint presentation with Samuel 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

## Workshops and Conferences Attended

---

### Zero-Knowledge Summit

- Presented WIP talk on comparing arithmetizations.

March 2022

Amsterdam, NL

### IC3 Blockchain Camp

- Worked on a privacy-preserving auction using HoneyBadgerMPC (2019).

June 2019 and 2020

Ithaca, NY

### ACM SIGSAC Conference on Computer and Communications Security

- Presented conference talk on SEEMless.
- Received conference student scholarship.

Nov 2019

London, UK

### Symposium on the Theory of Computing

- Attended various mentoring lunches, talks and workshops.
- Funded by Prof. Elaine Shi and TCS Women.

June 2019

Phoenix, AZ

### Grace Hopper Convention

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

Oct 2018

Houston, TX

### DIMACS/Northeast Big Data Hub Workshop on

### Overcoming Barriers to Data Sharing including Privacy and Fairness

- Attended two day workshop on private data sharing and differential privacy.
- Funded by the workshop.

Oct 2017

Piscataway, NJ

### Graduate Research Opportunities for Women

- Selected to attend the two day conference to encourage women in mathematics to consider future opportunities.
- The conference featured lectures, research talks and panels from faculty at various universities.
- Funded by Northwestern University, Department of Mathematics.

Oct 2017

Chicago, IL

## Research Visits

---

### Microsoft Research

- Made a week long research visit to collaborate on SEEMless.

November 2018

Redmond, WA

## Teaching

---

### Cornell University, Department of Computer Science

#### Graduate Teaching Assistant

- Systems Security

Held guest lectures, wrote assignments and rubrics, graded and helped with logistics.

- Blockchains, Cryptocurrencies, and Smart Contracts

Worked on stencil code, assignments, rubrics and grading, held office hours, managed logistics.

- Security and Privacy Concepts in the Wild

Wrote assignments and rubrics, held office hours, managed logistics, graded exams.

**Ithaca, NY**

Aug 2020 - Present

Jan 2019 - May 2019

Aug 2018 - Dec 2018

### Brown University, School of Professional Studies

#### Executive Masters in Cybersecurity, Teaching Assistant

- Applied Cryptography and Data Privacy

Created lecture content, wrote assignments, conducted in-class discussions, graded assignments.

- Advanced Topics in Computer Security

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.

**Providence, RI**

March 2018 - Aug 2018

March 2018 - Aug 2018

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

#### Undergraduate Teaching Assistant

- Computer Systems Security

Graded, held office hours, made assignments and in-class demos.

- Abstract Algebra

Graded for algebra course covering groups, rings and fields.

- Discrete Structures and Probability

Graded, wrote up solutions and held office hours.

- "How Big is Infinity? And other questions" and "Fundamentals for Calculus"

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

**Providence, RI**

March 2018 - May 2018

Sept 2015 - Dec 2015

Jan 2015 - May 2015

July 2014

### Brown University, Science Center

#### L<sup>A</sup>T<sub>E</sub>X Workshop Leader

- Designed curriculum, created lesson plans and led workshops on L<sup>A</sup>T<sub>E</sub>X.

**Providence, RI**

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,  $\alpha$ - $\beta$  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:** 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

---

Running, Sitar, Philosophy, Teaching, Member Association for Women in Math chapter at Brown, HIIT, Guitar.