Harjasleen (Jasleen) Malvai

harjasleenmalvai@gmail.com

Education

University of Illinois, Urbana-Champaign — **Urbana-Champaign, IL**
PhD Candidate, 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.

Peer-reviewed Publications

∗ ***equal contribution*** † ***authors listed alphabetically***

SoK: Transparency Systems for Key-Value Stores
Malvai, H., Falzon, F., Zitek, A., Meiklejohn, S., Bonneau, J. 2026
(to appear, NDSS 2026)

Constraint-Friendly Map-to-Elliptic-Curve-Group Relations and Their Applications
Groth, J., **Malvai, H.**, Miller, A., Zhang, Y.† 2025
(to appear, Asiacrypt 2025)

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

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

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

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

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.

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.

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.

Under Preparation Publications

Black-box Approaches to Authenticated Dictionaries: New Constructions and Lower Bounds
Falzon, F., **Malvai, H.**, Opel, E.† 2025
(In submission)

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

Awards and Honours

IRTF 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/ 3rd Place 2023/2025
Facebook PhD Fellowship, Finalist. 2021, 2022
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.

Graduate Research Experience

Yale University, Department of Computer Science
Visiting Research Assistant **New Haven, CT**
- Collaborating with Prof. Babis Papamanthou. Feb. 2025-Present

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.

Academic Service

Usenix Security, Program Committee 2026
Workshop on Cryptography Applied to Transparency Systems at ACM CCS, PC 2023
CRYPTO, Financial Crypto, IEEE S & P, Euro S&P, Eurocrypt, Sub-reviewer 2020-Present
Reviewed several papers each year, starting in 2020.
UIUC CSL Student Conference, Program Chair 2023
Chaired the Networking and Security session, reviewing talk proposals and invited and hosted speakers from NYU and Cornell.

Research Visits

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

Teaching

Cornell University/UIUC
Proof systems seminar curator and organiser — **Remote**
- Compiled resources, led discussions and provided some tutorials. — Aug. 2020 - Dec 2020

Cornell University, Department of Computer Science
Graduate Teaching Assistant — **Ithaca, NY**
- Systems Security — Aug 2020 - Dec 2020
  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
LaTeX Workshop Leader — **Providence, RI**
- Designed curriculum, created lesson plans and led workshops on LaTeX. — Jan 2014 - Dec 2019

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.

(Continued on next page)

Selected Coursework

Graduate

Computer Science: *Universal Composability, Information Theory, Secure Computation, Advanced Systems, Cryptography, Designing Secure Cryptography, Blockchains, Programming Languages.*

Undergraduate

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.*

Activities and Interests

Guitar, Literary Fiction, Teaching, Fitness, (Bowed and Plucked) String Instruments, Craft Chocolate.

Spoken Languages

English, Hindi, Urdu, Punjabi (all native), German (intermediate).

References

- Andrew Miller, Associate Professor of ECE, Affiliate CS, UIUC, soc1024@illinois.edu
- Charalampos Papamanthou, Associate Professor of Computer Science, Yale University, charalampos.papamanthou@yale.edu
- Fan Zhang, Assistant Professor of Computer Science, Yale University, f.zhang@yale.edu
- Esha Ghosh, Principal Researcher, Cryptography group at Microsoft Research Redmond, esha.Ghosh@microsoft.com
- Donald R. Beaver, Independent Researcher, Fierce Logic, don.beaver@gmail.com