Curriculum Vitae

Alexandra Veliche Hostetler

aveliche@umich.edu – https://web.eecs.umich.edu/~aveliche/index.html

Education

University of Michigan, Ann Arbor, MI *Expected Graduation Date:* May 2025
PhD Candidate in Computer Science and Engineering
Advisor: Mahdi Cheraghchi

Northeastern University, Boston, MA *Graduation Date:* May 2020
Bachelor of Science in Mathematics, Minor in Computer Science Summa Cum Laude

Publications

[ALV,2024] – Divesh Aggarwal, Leong Jin Ming, Alexandra V., *Worst-case to Average-case Hardness of LWE: An Alternative Perspective.* To appear in TCC 2024 Proceedings, Part II, 15365, 2024.

[CDRV,2022] – Mahdi Cheraghchi, Joseph Downs, João Ribeiro, Alexandra V., *Mean-Based Trace Reconstruction over Oblivious Synchronization Channels.* IEEE Transactions on Information Theory, 68(7):4272-4281, 2022.

Research

Research Interests: I am broadly interested in theoretical computer science and its mathematical foundations. I am especially interested in the computational complexity of problems that lie at the foundation of post-quantum cryptography, particularly those problems related to error-correcting codes and geometric lattices.

Worst-Case to Average-Case Hardness of LWE: An Alternative Perspective National University of Singapore
Computational Complexity Theory 2023 – 2024

- *Collaborators:* Divesh Aggarwal, Leong Jin Ming.
- Introduced alternative framework for measuring hardness of problems relevant to cryptography, and proved a near-optimal bound on the maximum success probability of solving the Learning with Errors (LWE) problem under a reasonable hardness assumption about that of solving the Bounded Distance Decoding (BDD) problem.
- Presented results at TCC 2024.

Mean-Based Worst-Case Trace Reconstruction University of Michigan
Coding Theory 2020 – 2021

- *Collaborators:* João Ribeiro, Mahdi Cheraghchi, Joseph Downs.
- Generalized all best known upper bounds on the number of traces needed for mean-based trace reconstruction to a more general model called the oblivious synchronization channel.
- Presented results at ISIT 2021 and published paper in IEEE Transactions on Information Theory.

Randomness Extractors Northeastern University
Cryptography Spring 2020

- *Advisor:* Daniel Wichs.
- Worked on proving that any good seeded extractor is a good two-source extractor.

Nonlocality in Quantum Shallow Circuits (Honors Thesis) Northeastern University
Quantum Computing Fall 2019

- *Advisor:* Christopher King.
- Proved results in "Quantum Advantage of Shallow Circuits" by Bravyi, Gosset, and König, for small examples and illustrated the role of nonlocality and graph states in solving the Hidden Linear Function Problem to separate the classes NC^0 and QNC^0. Presented at Honors Thesis Seminar.

Shor's Algorithm and Its Impact on Present-Day Cryptography (Research Capstone) Northeastern University
Quantum Computing Fall 2018

- *Advisor:* Christopher King.
- Wrote exposition of Shor's algorithm for factoring, with a focus on the role of roots of unity in the quantum Fourier transform. Presented at the research capstone seminar.

Invited Talks

Theory of Cryptography Conference (TCC) December 2024
Milan, Italy

- Presented "Worst-case to Average-case Hardness of LWE: An Alternative Perspective" paper.

Theory of Computer Science Seminar, Purdue University September 2024
West Lafayette, IN

- Presented "Worst-case to Average-case Hardness of LWE: An Alternative Perspective" paper.

Crypto Reading Group, Northeastern University May 2024
Boston, MA

- Presented "Worst-case to Average-case Hardness of LWE: An Alternative Perspective" paper.

Computing Theory Seminar, National University of Singapore May 2023
Singapore

- Presented "Mean-Based Trace Reconstruction over Oblivious Synchronisation Channels" paper.

IEEE International Symposium on Information Theory (ISIT) July 2021
Online

- 4-minute highlight talk on "Mean-Based Trace Reconstruction over Oblivious Synchronisation Channels" paper.

Nebraska Conference for Undergraduate Women in Mathematics (NCUWM) January 2020
University of Nebraska, Lincoln, NE

- Presented poster on "Nonlocality in Shallow Quantum Circuits" project.

Hudson River Undergraduate Math Conference (HRUMC) March 2019
Smith College, Northampton, MA

- Gave a talk about "Shor's Algorithm and Its Impact on Modern Cryptography".

Nebraska Conference for Undergraduate Women in Mathematics (NCUWM) January 2019
University of Nebraska, Lincoln, NE

- Presented poster on "Shor's Algorithm and Its Impact on Modern Cryptography".

Teaching

CSE Department of University of Michigan — Ann Arbor, MI
Graduate Student Instructor for Introduction to Cryptography (EECS 475) — August – December 2023

CSE Department of University of Michigan — Ann Arbor, MI
Graduate Student Instructor for Advanced Cryptography (EECS 575) — August – December 2022

CSE Department of University of Michigan — Ann Arbor, MI
Graduate Student Instructor for Introduction to Algorithms (EECS 477) — August – December 2021

New Horizons Summer School — Online
Volunteer Teaching Assistant for Cryptography — June 2021

Computer Science Department of Northeastern University — Boston, MA
Teaching Assistant for Cryptography (CS 4770) — January – April 2020

St. Herman of Alaska Christian School — Allston, MA
Volunteer Teacher's Assistant for Middle School Geometry Class — Fall 2016 – Fall 2019

Employment

National University of Singapore, Centre for Quantum Technologies — Singapore
Research Visitor / Intern — Summer 2023

- Collaborated with Divesh Aggarwal and Jin Ming Leong on a research project about fine-grained hardness of the Learning with Errors problem.

Center for Communications Research, Princeton — Princeton, NJ
Researcher — Summer 2022

- Worked on various topics in mathematical cryptology including practical applications and implementations of homomorphic encryption, secure multi-party computation, zero-knowledge proofs, and design and vulnerability analysis of novel cryptographic protocols.

Mathematics Department of Northeastern University — Boston, MA
Mathematics Tutor — May 2017 – April 2019

- Instructed over 10 students per week in various mathematics courses to facilitate comprehension of class material.

Cengage Learning — Boston, MA
Cybersecurity Co-op — January – July 2018

- Collaborated with cybersecurity team on projects for antivirus software installation and endpoint upgrades.
- Learned basics of ethical hacking and web application security, using OWASP Zap and Metasploit in Kali Linux.
- Compiled endpoint status reports in Microsoft Excel and monitored activity within the company environment.

Honors & Awards

Rackham Conference Travel Grant September 2024

Awarded to support travel expenses for conference presentation at TCC.

Honorable Mention Award for Teaching May 2022

Recognized for commitment as a Graduate Student Instructor to the academic mission of the University of Michigan's CSE Department.

ISIT 2021 Four Minutes, Two Techniques Student Challenge Winner July 2021

Awarded to each member of the top 3 teams for a collaborative 4-minute video explaining 2 techniques.

PEAK Shout-It-Out Award January 2020

Travel award to present a poster at the NCUWM in February 2020.

Churchill Scholarship Nominee November 2019

Nominated by Northeastern University for a fully-sponsored master's degree at Cambridge University.

National Merit Scholarship Fall 2016 – Spring 2020

Merit-based scholarship sponsored by Liberty Mutual, awarded per semester.

Service

CSE Department of University of Michigan Ann Arbor, MI

Theory Lab Retreat Fall 2024

- Collaborated with two other students to organize and lead the first weekend retreat for the graduate students in our theory group to promote interdisciplinary collaboration and improve the lab culture.

CSE Department of University of Michigan Ann Arbor, MI

Theory Lunch Seminar Organizer Fall 2021 – Spring 2022, Fall 2024

- Collaborated with other students to organize a joint faculty and graduate student lunch seminar as well as a student-only seminar for the theory group.