Neekon Vafa

Personal Homepage: neekonvafa.com

Education

Massachusetts Institute of Technology September 2020 - present

– Ph.D. Candidate in Mathematics. Advised by Vinod Vaikuntanathan.

– Cumulative GPA: 5.000/5.

Harvard University September 2015 - September 2019

– B.A. (honors) in Mathematics with a secondary in Computer Science.

– Cumulative GPA: 4.000/4.

Publications (authors listed in alphabetical order)

1. Andrej Bogdanov, Alon Rosen, and Neekon Vafa. Statistically undetectable backdoors in deep neural networks.
   [In preparation]

2. Andrej Bogdanov, Alon Rosen, Neekon Vafa, and Vinod Vaikuntanathan. Adaptive robustness of hypergrid johnson-lindenstrauss. *IACR Cryptol. ePrint Arch.*, page 666, 2025.
   [Links: arXiv, ePrint]

3. Neekon Vafa and Vinod Vaikuntanathan. Symmetric perceptrons, number partitioning and lattices. In Michal Koucký and Nikhil Bansal, editors, *Proceedings of the 57th Annual ACM Symposium on Theory of Computing, STOC 2025, Prague, Czechia, June 23-27, 2025*, pages 2191–2202. ACM, 2025.
   [Links: arXiv, ePrint, ECCC, **STOC 2025**]
   Invited to the SIAM Journal of Computing Special Issue.

4. Shafi Goldwasser, Jonathan Shafer, Neekon Vafa, and Vinod Vaikuntanathan. Oblivious defense in ML models: Backdoor removal without detection. In Michal Koucký and Nikhil Bansal, editors, *Proceedings of the 57th Annual ACM Symposium on Theory of Computing, STOC 2025, Prague, Czechia, June 23-27, 2025*, pages 1785–1794. ACM, 2025.
   [Links: arXiv, **STOC 2025**]

5. Riddhi Ghosal, Aayush Jain, Paul Lou, Amit Sahai, and Neekon Vafa. Post-quantum PKE from unstructured noisy linear algebraic assumptions: Beyond LWE and alekhnovich's LPN. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part II*, volume 15602 of *Lecture Notes in Computer Science*, pages 64–93. Springer, 2025.
   [Links: ePrint, **Eurocrypt 2025**]

6. Elette Boyle, Ilan Komargodski, and Neekon Vafa. The complexity of memory checking with covert security. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications*

of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part V, volume 15605 of *Lecture Notes in Computer Science*, pages 301–330. Springer, 2025.
[Links: ePrint, **Eurocrypt 2025**]

7. Seyoon Ragavan, Neekon Vafa, and Vinod Vaikuntanathan. Indistinguishability obfuscation from bilinear maps and LPN variants. In Elette Boyle and Mohammad Mahmoody, editors, *Theory of Cryptography - 22nd International Conference, TCC 2024, Milan, Italy, December 2-6, 2024, Proceedings, Part IV*, volume 15367 of *Lecture Notes in Computer Science*, pages 3–36. Springer, 2024.
[Links: ePrint, **TCC 2024**]

8. Aparna Gupte, Neekon Vafa, and Vinod Vaikuntanathan. Sparse linear regression and lattice problems. In Elette Boyle and Mohammad Mahmoody, editors, *Theory of Cryptography - 22nd International Conference, TCC 2024, Milan, Italy, December 2-6, 2024, Proceedings, Part II*, volume 15365 of *Lecture Notes in Computer Science*, pages 276–307. Springer, 2024.
[Links: arXiv, **TCC 2024**]

9. Elette Boyle, Ilan Komargodski, and Neekon Vafa. Memory checking requires logarithmic overhead. *J. ACM*, 72(2):13:1–13:43, 2025.
[Links: ePrint, ECCC, **STOC 2024**, Journal of the ACM]

10. Surya Mathialagan and Neekon Vafa. Macorama: Optimal oblivious RAM with integrity. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part IV*, volume 14084 of *Lecture Notes in Computer Science*, pages 95–127. Springer, 2023.
[Links: ePrint, **Crypto 2023**]

11. Aparna Gupte, Neekon Vafa, and Vinod Vaikuntanathan. Continuous LWE is as hard as LWE & applications to learning gaussian mixtures. In *63rd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2022, Denver, CO, USA, October 31 - November 3, 2022*, pages 1162–1173. IEEE, 2022.
[Links: arXiv, ePrint, **FOCS 2022**]

12. Lijie Chen, Shuichi Hirahara, and Neekon Vafa. Average-case hardness of NP and PH from worst-case fine-grained assumptions. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference, ITCS 2022, January 31 - February 3, 2022, Berkeley, CA, USA*, volume 215 of *LIPIcs*, pages 45:1–45:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.
[Links: ECCC, **ITCS 2022**]

13. Eric Allender, Rahul Ilango, and Neekon Vafa. The non-hardness of approximating circuit size. *Theory Comput. Syst.*, 65(3):559–578, 2021.
[Links: ECCC, **CSR 2019**, Special Issue: TOCS]
Invited to the Theory of Computing Systems Special Issue.

14. Samuel DeHority, Xavier Gonzalez, Neekon Vafa, and Roger Van Peski. Moonshine for all finite groups. *Res. Math. Sci.*, 5(1), March 2018.
[Links: arXiv, RMS]

Fellowships & Awards

NSF Graduate Research Fellowship, National Science Foundation 2020 - 2025

– Awarded full funding for 3 out of 5 fellowship years for my Ph.D. research.

Reitano Fellowship, Massachusetts Institute of Technology 2020 - 2021

– Awarded first-year full funding in honor of Professor Gilbert Strang by the Reitano Family.

Bok Center Certificate of Distinction in Teaching, Harvard University 2018

– Awarded for high instructor ratings (4.8/5.0) as course assistant for Math 122 (abstract algebra).

John Harvard Scholar, Harvard University 2016, 2017, 2018

– Awarded annually to freshmen, sophomores, and juniors in top 5% of respective classes.

Detur Book Prize, Harvard University 2016

– Awarded to students with highest first-year academic standings.

Talks

– UT Austin: Theory and AI Alignment Group Meeting (upcoming in) December 2025
– Columbia: Theory Seminar November 2025
– UK AI Security Institute (AISI) Alignment Conference October 2025
– MIT: ML+Cryptography Seminar October 2025
– Stanford: CS Theory Lunch October 2025
– MIT: CSAIL Security Seminar September 2025
– Crypto & ML Reading Group at the Simons Institute's Cryptography Program August 2025
– 🎞 STOC 2025 June 2025
– 🎞 Obfuscation Workshop at the Simons Institute's Cryptography Program June 2025
– Information-Computation Tradeoffs for Statistical Problems Workshop at TTIC June 2025
– 🎞 Eurocrypt 2025 May 2025
– AICrypt 2025 May 2025
– Georgia Tech: Algorithms and Randomness Center Colloquium April 2025
– Plenary talk at the MFO Cryptography Meeting in Oberwolfach January 2025
– CIFRA Institute at Bocconi University January 2025
– TCC 2024 December 2024
– MIT: Guest Lecture in Advanced Topics in Cryptography November 2024
– 🎞 STOC 2024 June 2024
– 🎞 CMU: Crypto Seminar April 2024
– Bay Area Crypto Day April 2024
– Charles River Crypto Day March 2024
– NYU: Crypto Reading Group March 2024
– Columbia: Theory Seminar April 2023
– 🎞 CMU: Theory Lunch Seminar April 2023

– 🎞 Simons Institute: Lower Bounds, Learning, and Average-Case Complexity — February 2023
– UC Berkeley: Security Seminar — February 2023
– Stanford: Security Seminar — January 2023
– MIT: Cryptography and Information Security (CIS) Seminar — December 2022
– 🎞 FOCS 2022 — November 2022
– 🎞 Simons Institute: Quantum and Lattices Joint Reunion Workshop — June 2022
– 🎞 ITCS 2022 — January 2022
– Joint Math Meetings 2018 — January 2018

Academic Service

– Teaching faculty at the CSP-IAS Winter School on Cryptography & ML. — February 2026
– Co-organizer for the Crypto & ML Reading Group at the Simons Institute. — Summer 2025
– Organizer for MIT's Crypto Group Meeting. — Fall 2024 - present
– Reviewer for STOC 2026, SODA 2026, TCC 2025, RANDOM 2025, FOCS 2025, Crypto 2025, STOC 2025, Eurocrypt 2025, ITCS 2025, FSTTCS 2024, FOCS 2024, Crypto 2024, RANDOM 2023, CCC 2023, SODA 2023, TCC 2022, TCC 2021, Eurocrypt 2021.

Selected Coursework

Letter grades received in all courses at MIT and Harvard were either an A or an A+.

Massachusetts Institute of Technology († for internal A+, * for graduate level)

– 6.845: Quantum Complexity Theory†* — Spring 2022
– 18.408: An Algorithmist's Toolkit* — Spring 2022
– 6.890: Matrix Multiplication and Graph Algorithms* — Fall 2021
– 6.856: Randomized Algorithms†* — Spring 2021
– 18.218: Analysis of Boolean Functions* — Spring 2021
– 18.425: Cryptography & Cryptanalysis†* — Fall 2020
– 18.435: Quantum Computation†* — Fall 2020

Harvard University († for unofficial A+, * for graduate level)

– COMPSCI 229R: Information Theory in Theoretical Computer Science* — Spring 2019
– MATH 118R: Dynamical Systems — Spring 2019
– COMPSCI 61: Systems Programming and Machine Organization — Fall 2018
– COMPSCI 136: Economics and Computation — Fall 2018
– COMPSCI 124: Data Structures and Algorithms — Spring 2018
– 6.S078: Fine-Grained Algorithms and Complexity† *(cross-registered at MIT)* — Spring 2018
– 6.841: Advanced Complexity Theory* *(cross-registered at MIT)* — Fall 2017
– MATH 231A: Algebraic Topology* — Fall 2017
– COMPSCI 181: Machine Learning — Spring 2017
– MATH 137: Algebraic Geometry — Spring 2017

– MATH 155R: Combinatorics Spring 2017
– STAT 110: Probability Fall 2016
– MATH 131: Topological Spaces and the Fundamental Group Fall 2016
– MATH 132: Smooth Manifolds Spring 2016
– PHYSICS 153: Electrodynamics Spring 2016
– MATH 122: Theory of Groups and Vector Spaces† Fall 2015
– PHYSICS 16: Mechanics and Special Relativity† Fall 2015

Teaching & Mentoring

Volunteer Prison Computer Science Teaching Assistant Winter - Spring 2025
– Teaching Assistant for "Python and Web Development II" as part of the Brave Behind Bars program, with 4 hours of teaching per week.
– Students are inmates at various penal institutions across Maine and Massachusetts.

Volunteer Prison Math Tutor, Boston Pre-Release Center Spring - Summer 2024
– Tutored and taught secondary school mathematics to inmates at the Boston Pre-Release Center.

Teaching Assistant for Cryptography (6.5620/18.425), MIT Fall 2023
– Primary Instructor: Vinod Vaikuntanathan.
– Designed problem sets, held office hours, and more for graduate course on cryptography.
– Rated 6.5/7 overall as an instructor.

Grad-Undergrad Math Mentor Initiative (GUMMI), MIT 2022 - 2024
– Mentored three students in their graduate school application processes as part of GUMMI.

Course Assistant for Abstract Algebra (Math 122), Harvard Fall 2017
– Primary instructor: Hiro Lee Tanaka.
– Held twice-weekly office hours and graded problem sets.
– Awarded Bok Center Certificate of Distinction in Teaching for high instructor ratings (4.8/5).

Volunteer Computer Programming Teacher, Boston Public Schools 2016 - 2017
– Seventh grade at Gardner Pilot Academy (Fall 2016).
– Fourth grade at Henderson Inclusion School (Spring 2017).

Visits

– Visited the "Cryptography 10 Years Later" program at the Simons Institute. Summer 2025
– Visited Alon Rosen at the CIFRA Institute at Bocconi University. January 2025
– Research Intern at NTT Research with Elette Boyle and Ilan Komargodski. Summer 2023
– Visited Aayush Jain at CMU. April 2023
– Visiting Student Researcher at "Meta-Complexity" program at Simons Institute. January 2023
– Visiting Student Researcher at "Lattices and Beyond" program at Simons Institute. June 2022

Industry Experience

NTT Research, Sunnyvale, CA — Summer 2023

Research Intern (Cryptography & Information Security Laboratories)

– Worked with Elette Boyle and Ilan Komargodski on cryptography research.

Google (YouTube), San Bruno, CA — September 2019 - July 2020

Software Engineer

– Supported YouTube Music's [Web, iOS, Android] server-side stack as part of the Playback team.

Jane Street Capital, New York, NY — Winter 2017

Quantitative Trading Intern

Facebook, Menlo Park, CA — Summer 2016

Facebook University for Engineering Intern

– Designed and implemented Android app with two other interns.

– App scans food-product barcodes to indicate if it is safe to eat based on user's dietary restrictions.

Miscellaneous

Languages	English (native), Farsi (bilingual), Spanish (proficient), French (elementary).
Skills	C++, Python, Java, Android, OCaml, SageMath, Mathematica, LaTeX.
Interests	Curling, Tennis, Filmmaking, Comedy, Travel, Prediction Markets.