Neekon Vafa

Website: neekonvafa.com

Education

Massachusetts Institute of Technology, 2020-present

- Ph.D. Candidate in Mathematics. Advisor: Vinod Vaikuntanathan.
- Cumulative GPA: 5.00 (on a 5.0 scale).

Harvard University, 2015-2019

- B.A. (honors) in Mathematics with a secondary in Computer Science.
- Cumulative GPA: 4.00 (on a 4.0 scale).

Papers

- **Vafa, N.**, Vaikuntanathan, V. Symmetric Perceptrons, Number Partitioning and Lattices. [arXiv, ePrint, ECCC, accepted to STOC 2025]
- Goldwasser, S., Shafer, J., **Vafa, N.**, Vaikuntanathan, V. Oblivious Defense in ML Models: Backdoor Removal without Detection. [arXiv, accepted to STOC 2025]
- Ghosal, R., Jain, A., Lou, P., Sahai, A., **Vafa, N.** Post-Quantum PKE from Unstructured Noisy Linear Algebraic Assumptions: Beyond LWE and Alekhnovich's LPN [Accepted to Eurocrypt 2025]
- Boyle, E., Komargodski, I., **Vafa, N.** The Complexity of Memory Checking with Covert Security. [Accepted to Eurocrypt 2025]
- Ragavan, S., **Vafa, N.**, Vaikuntanathan, V. Indistinguishability Obfuscation from Bilinear Maps and LPN Variants. In: *Theory of Cryptography Conference*. [ePrint, TCC 2024]
- Gupte, A., **Vafa, N.**, Vaikuntanathan, V. Sparse Linear Regression and Lattice Problems. In: *Theory of Cryptography Conference*. [arXiv, TCC 2024]
- Boyle, E., Komargodski, I., **Vafa, N.** Memory Checking Requires Logarithmic Overhead. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing (STOC 2024)*. [ePrint, ECCC, STOC 2024, Journal of the ACM]
- Mathialagan, S., **Vafa, N.** MacORAMa: Optimal Oblivious RAM with Integrity. In: *Annual International Cryptology Conference*. [ePrint, Crypto 2023]
- Gupte, A., **Vafa, N.**, Vaikuntanathan, V. Continuous LWE is as Hard as LWE & Applications to Learning Gaussian Mixtures. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*. [arXiv, ePrint, FOCS 2022]
- Chen, L., Hirahara, S., **Vafa, N.** Average-case Hardness of NP and PH from Worst-case Fine-grained Assumptions. In *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*. [ECCC, ITCS 2022]
- Allender, E., Ilango, R., **Vafa, N.** The Non-hardness of Approximating Circuit Size. *Theory Comput Syst* (2020) [ECCC, CSR 2019, Special Issue: TOCS]
- DeHority, S., Gonzalez, X., **Vafa, N.** *et al.* Moonshine for All Finite Groups. *Res Math Sci* **5**, 14 (2018) [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, and 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

- Algorithms and Randomness Center Colloqium at Georgia Tech (planned for April 2025)
- Plenary talk at the MFO Cryptography Meeting (January 2025)
- CIFRA Institute at Bocconi University (January 2025)
- TCC 2024 (December 2024)
- Guest Lecture for MIT course on Advanced Topics in Cryptography (November 2024)
- STOC 2024 (June 2024)
- CMU CyLab Crypto Seminar (April 2024) [Video]
- 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) [Video]
- Simons Institute: Lower Bounds, Learning, Average-Case Complexity Workshop (Feb. 2023) [Video]
- UC Berkeley: Security Seminar (February 2023)
- Stanford: Security Seminar (January 2023)
- MIT: Cryptography and Information Security (CIS) Seminar (December 2022)
- FOCS 2022 (November 2022) [Video]
- Simons Institute: Quantum and Lattices Joint Reunion Workshop (June 2022) [Video]
- ITCS 2022 (January 2022) [Video]
- Joint Math Meetings 2018 (January 2018)

Visits & Travels

- 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).

Academic Service

- Organizer for MIT's Crypto Group Meeting (Fall 2024-present).
- Reviewer for 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

Grades received in all courses were either an A or an A+.

Massachusetts Institute of Technology (Graduate Level*)

- Quantum Complexity Theory* (Spring 2022)
- An Algorithmist's Toolkit* (Spring 2022)
- Matrix Multiplication and Graph Algorithms* (Fall 2021)
- Randomized Algorithms* (Spring 2021)
- Analysis of Boolean Functions* (Spring 2021)
- Cryptography & Cryptanalysis* (Fall 2020)
- Quantum Computation* (Fall 2020)
- Fine-Grained Algorithms and Complexity (Spring 2018)
- Advanced Complexity Theory* (Fall 2017)

Harvard University (Graduate Level*)

- Information Theory in Theoretical Computer Science* (Spring 2019)
- Systems Programming and Machine Organization (Fall 2018)
- Economics and Computation (Fall 2018)
- Data Structures and Algorithms (Spring 2018)
- Algebraic Topology* (Fall 2017)
- Machine Learning (Spring 2017)
- Algebraic Geometry (Spring 2017)
- Combinatorics (Spring 2017)
- Probability (Fall 2016)

Teaching

Volunteer Prison Computer Science Teaching Assistant, Winter 2025-present

- 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, 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.

Course Assistant for Abstract Algebra (Math 122), Harvard University, 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 at Boston Public Schools, 2016-2017

- Seventh grade at Gardner Pilot Academy (Fall 2016).
- Fourth grade at Henderson Inclusion School (Spring 2017).

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's safe to eat based on user's dietary restrictions.

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