Noah Stephens-Davidowitz

Office	321 Gates Hall	**Phone**	(201) 655-5134
Website	noahsd.com	**Email**	noahsd@gmail.com
		Last updated	January 18, 2026

Education

2012-2017 **New York University**
Ph.D. in Computer Science
Specializing in lattices. My advisors were Professors Oded Regev and Yevgeniy Dodis. My thesis, *On the Gaussian measure over lattices*, won the Dean's Outstanding Dissertation Award in the sciences.

2004 - 2008 **Brown University**
Sc.B. in Mathematics

Selected work experience

Jul 2020- **Cornell University, Department of Computer Science**
Assistant Professor

Aug 2019- **Centre for Quantum Technologies and National University of Singapore**
Visiting Professor
Roughly annual visits to work with Divesh Aggarwal and others.

Jan-May 2020 **Simons Institute, Lattices: Algorithms, Complexity, and Cryptography**
Research Fellow
Microsoft Research Fellow

Sep 2018-Jan 2020 **Massachusetts Institute of Technology**
Postdoctoral Researcher in Computer Science
Supervised by Vinod Vaikuntanathan.

2017-2018 **Princeton University**
Postdoctoral Researcher in Computer Science
Part of the Simons Collaboration on Algorithms and Geometry.

2017-2018 **Institute for Advanced Study**
Visiting Researcher in Mathematics
Part of the Simons Collaboration on Algorithms and Geometry.

July - Oct 2016 **IBM Cryptography Research Group**
Intern and fellowship recipient.

May - July 2016 **University of Michigan**
Visiting Student
Research in cryptography with Chris Peikert.

Summer 2015 **Simons Institute**
Visiting Student
Participated in the cryptography program.

Summer 2014 **Microsoft Research**
Intern
Research in cryptography with Ilya Mironov.

January 2014 **Seven Bridges Genomics**
Intern
Confidential work focusing on faster, more accurate, and more space-efficient algorithms for variants of the string alignment problem for the purposes of genome sequencing.

Summer 2013 **New York University**
Summer Researcher
Research with Daniel Dadush and Oded Regev on the Closest Vector Problem with preprocessing.

2012 **Bakker-Davidowitz Consulting**
Founder
Confidential consulting work with major online poker sites to develop automated systems to detect the use of AIs and other forms of cheating.

Fall 2010 **Cake Gaming**
Independent Security Investigator
Created and employed algorithms to search through eighty million poker hands to determine if anyone exploited an encryption vulnerability on Cake Poker. This was by far the largest independent security audit of an online poker website conducted at the time. Our methods were novel, and we proved their efficacy by designing poker AIs (including subtly cheating AIs) to test them.

2006-2011 **Professional poker player**

Papers

1. Oded Regev and Noah Stephens-Davidowitz. *A simple proof of a reverse Minkowski theorem for integral lattices*. *Journal of Number Theory*, 2026. arXiv:2306.03697.

2. Surendra Ghentiyala, Zeyong Li, and Noah Stephens-Davidowitz. *Range avoidance, Arthur-Merlin, and* TFNP. Manuscipt. ECCC:2025/210.

3. Yevgeniy Dodis, Bernardo Magri, Noah Stephens-Davidowitz, and Yiannis Tselekounis. Guarding the Signal: Secure messaging with reverse firewalls. In *Crypto*, 2025.

4. Divesh Aggarwal, Thomas Espitau, Spencer Peters; and Noah Stephens-Davidowitz. *Recursive lattice reduction—A framework for finding short lattice vectors*. In *SOSA*, 2025. arXiv:2311.15064.

5. Huck Bennett, Surendra Ghentiyala, and Noah Stephens-Davidowitz. *The more the merrier! On total coding and lattice problems and the complexity of finding multicollisions*. In *ITCS*, 2025. ECCC:2024/018.

6. Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz. *Difficulties constructing lattices with exponential kissing number from codes*. *IEEE Transactions on Information Theory*, 2025. arXiv:2410.16660.

7. Surendra Ghentiyala and Noah Stephens-Davidowitz. *More basis reduction for linear codes: backward reduction, BKZ, slide reduction, and more*. In *Approx*, 2024. arXiv:2408.08507.

8. Noah Stephens-Davidowitz. *A pretty proof that an exponential function is superpolynomial.* Expository note. noahsd.com/exponential_is_superpolynomial.pdf.

9. Eldon Chung, Alexander Golovnev, Zeyong Li, Maciej Obremski, Sidhant Saraogi, and Noah Stephens-Davidowitz. *The hardness of range avoidance for randomized algorithms implies Minicrypt.* Manuscript. ECCC:2023/193.

10. Oded Regev and Noah Stephens-Davidowitz. *A reverse Minkowski theorem.* *Annals of Mathematics*, 2024. A preliminary version appeared in *STOC*, 2017. arXiv:1611.05979. See also the Bourbaki Seminar by Jean-Benoît Bost: youtube.com/watch?v=j7YvtVvv3qs (in French).

11. Alexander Golovnev, Siyao Guo, Spencer Peters, and Noah Stephens-Davidowitz. *Revisiting time-space tradeoffs for function inversion.* In *Crypto*, 2023. ECCC:2022/145.

12. Divesh Aggarwal, Huck Bennett, Zvika Brakerski, Alexander Golovnev, Rajendra Kumar, Zeyong Li, Spencer Peters, Noah Stephens-Davidowitz, and Vinod Vaikuntanathan. *Lattice problems beyond polynomial time.* In *STOC*, 2023. arXiv:2211.11693.

13. Huck Bennett, Atul Ganju, Pura Peethawatchai, and Noah Stephens-Davidowitz. *Just how hard are rotations of $\mathbb{Z}^n$? Algorithms and cryptography with the simplest lattice.* In *Eurocrypt*, 2023. eprint:2021/1548.

14. Alexander Golovnev, Siyao Guo, Spencer Peters, and Noah Stephens-Davidowitz. *On the (im)possibility of branch-and-bound search-to-decision reductions for approximate optimization.* APPROX, 2023. ECCC:2021/141.

15. Yael Eisenberg, Oded Regev, Noah Stephens-Davidowitz. *A tight reverse Minkowski inequality for the Epstein zeta function. Proceedings of the AMS*, 2022. arXiv:2201.05201.

16. Sandro Coretti, Yevgeniy Dodis, Harish Karthikeyan, Noah Stephens-Davidowitz, and Stefano Tessaro. *On seedless PRNGs and premature next.* In *ITC*, 2022. eprint:2022/558.

17. Yevgeniy Dodis, Siyao Guo, Noah Stephens-Davidowitz, and Zhiye Xie. *No time to hash—On super-efficient entropy accumulation.* In *Crypto*, 2021. eprint:2021/523.

18. Yevgeniy Dodis, Siyao Guo, Noah Stephens-Davidowitz, and Zhiye Xie. *Online linear extractors for independent sources.* In *ITC*, 2021. eprint:2021/1002.

19. Zvika Brakerski, Noah Stephens-Davidowitz, and Vinod Vaikuntanathan. *On the hardness of average-case k-SUM.* In *RANDOM*, 2021 arXiv:2010.08821.

20. Divesh Aggarwal, Zeyong Li, and Noah Stephens-Davidowitz. *A $2^{n/2}$-time algorithm for $\sqrt{n}$-SVP and $\sqrt{n}$-Hermite SVP, and an improved time-approximation tradeoff for (H)SVP.* In *Eurocrypt*, 2021. arXiv:2007.09556.

21. Divesh Aggarwal, Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz *Fine-grained hardness of CVP(P)—Everything that we can prove (and nothing else).* In *SODA*, 2021. arXiv:1911.02440.

22. Divesh Aggarwal, Yanlin Chen, Rajendra Kumar, Zeyong Li, and Noah Stephens-Davidowitz. *Dimension-preserving reductions between SVP and CVP in different p-norms.* In *SODA*, 2021. arXiv:2104.06576.

23. Tamalika Mukherjee and Noah Stephens-Davidowitz. *Lattice Reduction for Modules, or How to Reduce ModuleSVP to ModuleSVP.* In *Crypto*, 2020. eprint:2019/1142.

24. Divesh Aggarwal, Jianwei Li, Phong Q. Nguyen, Noah Stephens-Davidowitz. *Slide reduction, revisited—Filling the gaps in SVP approximation.* In *Crypto*, 2020. arXiv:1908.03724.

25. Divesh Aggarwal and Siyao Guo, Maciej Obremski, João Ribeiro, and Noah Stephens-Davidowitz. *Extractor lower bounds, revisited.* In *RANDOM*, 2020. ECCC:2019/173.

26. Divesh Aggarwal and Noah Stephens-Davidowitz. *An improved constant in Banaszczyk's transference theorem.* Manuscript, 2019. arXiv:1907.09020.

27. Noah Stephens-Davidowitz and Vinod Vaikuntanathan. *SETH-hardness of coding problems.* In *FOCS*, 2019. ECCC:2019/159.

28. Stephen D. Miller and Noah Stephens-Davidowitz. *Kissing numbers and transference theorems from generalized tail bounds. SIAM Journal on Discrete Mathematics (SIDMA)*, 2019, 33(3). arXiv:1802.05708.

29. Noah Stephens-Davidowitz. *A time-distance trade-off for GDD with preprocessing—Instantiating the DLW heuristic.* In *CCC*, 2019. arXiv:1902.08340.

30. Divesh Aggarwal and Noah Stephens-Davidowitz. *(Gap/S)ETH Hardness of SVP.* In *STOC*, 2018. arXiv:1712.00942.

31. Divesh Aggarwal and Noah Stephens-Davidowitz. *Just take the average! An embarrassingly simple 2^n-time algorithm for SVP (and CVP).* In *SOSA*, 2018. arXiv:1709.01535.

32. Navid Alamati, Chris Peikert, Noah Stephens-Davidowitz. *New (and old) proof systems for lattice problems.* In *PKC*, 2018. eprint:2017/1226.

33. Huck Bennett, Alexander Golovnev, Noah Stephens-Davidowitz. *On the quantitative hardness of CVP.* In *FOCS*, 2017. arXiv:1704.03928.

34. Noah Stephens-Davidowitz. *On the Gaussian measure over lattices.* PhD Thesis, New York University, 2017.
    Winner of the Dean's Outstanding Dissertation Award in the sciences.

35. Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. *Pseudorandomness of Ring-LWE for any ring and modulus.* In *STOC*, 2017. eprint:2017/258.

36. Oded Regev and Noah Stephens-Davidowitz. *An inequality for Gaussians on lattices. SIAM Journal on Discrete Mathematics (SIDMA)*, 2017, 31(2), 749757. arXiv:1502.04796.

37. Shai Halevi, Tzipora Halevi, Victor Shoup, and Noah Stephens-Davidowitz. *Implementing BP-obfuscation using graph-induced encoding.* In *CCS*, 2017. eprint:2017/104.

38. Huck Bennett, Daniel Dadush, and Noah Stephens-Davidowitz. *On the Lattice Distortion Problem.* In *ESA*, 2016. arXiv:1605.03613.

39. Noah Stephens-Davidowitz. *Search-to-decision reductions for lattice problems with approximation factors (slightly) greater than one.* In *APPROX*, 2016. arXiv:1512.04138.

40. Yevgeniy Dodis, Ilya Mironov, and Noah Stephens-Davidowitz. *Message transmission with reverse firewalls—Secure communication on corrupted machines.* In *Crypto*, 2016. eprint:2015/548.

41. Noah Stephens-Davidowitz. *Discrete Gaussian sampling reduces to CVP and SVP.* In *SODA*, 2016. arXiv:1506.07490.

42. Divesh Aggarwal, Daniel Dadush, and Noah Stephens-Davidowitz. *Solving the Closest Vector Problem in 2^n time—The discrete Gaussian strikes again!* In *FOCS*, 2015. arXiv:1504.01995.

43. Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. *Solving the Shortest Vector Problem in 2^n time via discrete Gaussian sampling.* In *STOC*, 2015. arXiv:1412.7994.

44. Ilya Mironov and Noah Stephens-Davidowitz. *Cryptographic reverse firewalls.* In *Eurocrypt*, 2015. eprint:2014/758.

45. Noah Stephens-Davidowitz. *Dimension-preserving reductions between lattice problems.* Brief survey, 2015. www.noahsd.com/latticeproblems.pdf.

46. Yevgeniy Dodis, Adi Shamir, Noah Stephens-Davidowitz, and Daniel Wichs. *How to eat your entropy and have it too—Optimal recovery strategies for compromised RNGs.* In *Crypto*, 2014. eprint:2014/167. Invited to the *Crypto* 2014 special issue of *Algorithmica*.

47. Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. *On the Closest Vector Problem with a distance guarantee.* In *CCC*, 2014. arXiv:1409.8063.
(Previous title: *On Bounded Distance Decoding and the Closest Vector Problem with Preprocessing.*)

48. Noah Stephens-Davidowitz and Alex Cloninger. *The Cyclic Sieving Phenomenon on the Alternating Sign Matrices.* Manuscript, 2007. noahsd.com/papers/ASMCSP.pdf.

49. Fraser Chiu Kim Hong, Alex Cloninger, and Noah Stephens-Davidowitz. *On link patterns and Alternating Sign Matrices.* Manuscript, 2007. noahsd.com/papers/ASMLinks.pdf.

Funding

- **Packard Fellowship**
- **Google Cyber NYC Gift**
- **NSF CCF-2312296**- Theoretical Foundations of Lattice-Based Cryptography (co-PI with Huck Bennett).
- **NSF CCF-2122230**- Cryptographic Hardness of Module Lattices (co-PI with Shi Bai, part of a joint grant with Alice Pellet-Mary, Damien Stehlé, and Benjamin Wesolowski with France's ANR).

PhD Advisees

- Yael Eisenberg (math)
- Surendra Ghentiyala
- Kyle Fridberg (applied math)
- Spencer Peters

Selected honors and awards

- **Cornell Bowers College of Computing and Information Science Teaching and Advising Excellence Award**, 2024.
- **Packard Fellowship for Science and Engineering**, 2023.
- **Microsoft Research Fellowship** for the Simons Lattices: Algorithms, Complexity, and Cryptography program, Spring 2020.
- **Dean's Outstanding Dissertation Award** in the sciences, NYU, 2018 ("best doctoral dissertation in the sciences").
- **Janet Fabri Prize**, NYU, 2018 (for "the dissertation determined to be the [CS] department's most outstanding").
- **IBM Ph.D. Fellowship**, IBM, 2016-2017.
- **NYU Dean's Dissertation Fellowship**, New York University, 2016-2017.
- **Jacob T. Schwartz Fellowship**, New York University, 2014.

Selected talks

1. *Recursive lattice reduction—a framework for finding short lattice vectors.* University of Waterloo, November 2025.
2. *Recursive lattice reduction—a framework for finding short lattice vectors.* Simons Institute Cryptography Program, August 2025.
3. *The more the merrier! On total coding and lattice problems and the complexity of finding multicollisions.* Total Search Problems in TCS, *STOC* workshop, June 2025.
4. *Recursive lattice reduction.* Charm workshop on cryptographic hardness of module lattices, June 2025.
5. *Lattice problems beyond polynomial time.* Fine-grained and Parameterized Complexity Today, June 2025.
6. *Recursive lattice reduction—a framework for finding short lattice vectors.* MIT Cryptography and Information Security Seminar, March 2025.
7. *Recursive lattice reduction—a framework for finding short lattice vectors.* SOSA, January 2025.
8. *On Beating 2^n for CVP.* SOSA, January 2025 (filling in for Rajendra Kumar).
9. *A reverse Minkowski theorem.* Hausdorff Center for Mathematics, workshop on information theory, boolean functions, and lattice problems, November 2024.
10. *A reverse Minkowski theorem.* Binghamton Arithmetic Seminar, September 2024.
11. *Foundations of lattice-based cryptography.* Packard Fellows Meeting, September 2024.
12. *Basis reduction for codes.* National University of Singapore, July 2024.
13. *A reverse Minkowski theorem.* Simons Institute program: Mathematics of computing according to lattices, August 2023, Schloss Elmau, Germany.
14. *Lattice problems beyond polynomial time.* National University of Singapore, August 2023.
15. *Lattice problems beyond polynomial time.* University of Washington, February 2023.
16. *Some recent results showing that lattice problems are (sort of) equivalent in all norms* . Simons Institute Summer cluster: Lattices and beyond, June 2022. simons.berkeley.edu/talks/some-recent-results-showing-lattice-problems-are-sort-equivalent-all-norms.
17. *Worst-case to average-case reductions for Ring-LWE.* CHARM (Cryptographic HArdness of Module lattices) bootcamp, February 2022.
18. *Lattice algorithms.* CHARM (Cryptographic HArdness of Module lattices) bootcamp, November 2021.
19. *On the hardness of average-case k-SUM.* Simons Institute, Average-Case Complexity: From Cryptography to Statistical Learning, November 2021. youtube.com/watch?v=n2wIgnXupCQ
20. *On the relationship between lattice problems across different ℓ_p norms.* Simons Institute, Lattices: Algorithms, Complexity, and Cryptography Reunion, June 2021.
21. *Benefits and risks of post-quantum cryptography.* Georgetown Computer Science colloquium, March 2021.
22. *A reverse Minkowski theorem.* Cornell Computer Science theory seminar, October 2020.
23. *Foundations of lattice-based cryptography.* Cornell Center for Applied Mathematics colloquium, October 2020.

24. *A reverse Minkowski theorem.* Simons Institute Lattices: Geometry, Algorithms, and Hardness, February 2020. youtube.com/watch?v=tZx7K0Or70Y.

25. *Algorithms for lattice problems.* Simons Institute Lattices: Geometry, Algorithms, and Hardness, January 2020. youtube.com/watch?v=o4Pl-0Q5-q0.

26. *Complexity of lattice problems.* Simons Institute Lattices: Geometry, Algorithms, and Hardness, January 2020. youtube.com/watch?v=Bi9Hs26TJa0.

27. *SETH-hardness of coding problems.* MIT theory seminar, December 2019.

28. *SETH-hardness of coding problems.* FOCS, November 2019. youtube.com/watch?v=rWLqnQn1eRQ.

29. *Will lattice-based cryptography be broken in practice?* Charles River Crypto Day, November 2019.

30. *SETH-hardness of coding problems.* Harvard students and postdocs theory seminar, October 2019.

31. *SETH-hardness of coding problems.* NUS theory seminar, August 2019.

32. *SETH-hardness of coding problems.* NYU theory seminar, May 2019.

33. *Benefits and risks of post-quantum cryptography from lattices.* Centre for Quantum Technologies colloquium, April 2019. youtube.com/watch?v=4BND9TrFr70.

34. *On the quantitative security of lattice cryptography.* Northwestern Quarterly Theory Workshop, November 2018.

35. *A reverse Minkowski theorem.* MIT, September 2018.

36. *(Gap/S)ETH hardness of SVP.* STOC, June 2018.

37. *Fine-grained hardness of lattice problems.* Lattice Crypto and Algorithms workshop in Bertinoro, May 2018. crypto-events.di.ens.fr/LATCA/program/nsd.pdf.

38. *A simple proof of a reverse Minkowski inequality.* IAS Computer Science/Discrete Math Seminar, April 2018. youtube.com/watch?v=9mvPxAKj5BU.

39. *Just take the average! An embarrassingly simple 2^n-time algorithm for SVP.* SOSA, January 2018.

40. *An embarrassingly simple 2^n-time algorithm for SVP—and how we hope to improve it.* FSTTCS Lattice Algorithms and Cryptography Workshop, December 2017.

41. *A reverse Minkowski theorem.* Rutgers discrete math seminar, October 2017.

42. *On the quantitative hardness of CVP.* DIMACS/Rutgers theory seminar, September 2017.

43. *On the quantitative hardness of CVP.* Princeton theory seminar, September 2017. youtube.com/watch?v=sd-SMjAl0ks.

44. *On the quantitative hardness of CVP.* Harvard Theory of Computing seminar, September 2017.

45. *A reverse Minkowski theorem.* STOC, June 2017.

46. *Pseudorandomness of Ring-LWE for any ring and modulus.* STOC, June 2017.

47. *On the quantitative hardness of CVP.* MIT Cryptography and Information Security Seminar, May 2017.

48. *A reverse Minkowski theorem.* TCS+, March 2017. www.youtube.com/watch?v=mgDNeg3U5TQ.

49. *A reverse Minkowski theorem.* Centre for Quantum Computation, National University of Singapore, March 2017.

50. *Pseudorandomness of Ring-LWE for Any Ring and Modulus.* Nanyang Technological University's Mini-Workshop on Post-Quantum Cryptanalysis, March 2017.

51. *A reverse Minkowski theorem.* Cornell probability seminar, November 2016.

52. *A reverse Minkowski theorem.* Columbia theory seminar, November 2016.

53. *Search-to-decision reductions for lattice problems with approximation factors (slightly) greater than one.* APPROX, September 2016.

54. *The reverse Minkowski theorem—Proof of a conjecture due to Dadush.* China Theory Week, August 2016.

55. *Message transmission with reverse firewalls—Secure communication on corrupted machines.* CRYPTO, August 2016. www.youtube.com/watch?v=2DOc-9u1EbQ.

56. *Solving SVP (and CVP) in 2^n time using discrete Gaussian sampling.* UM student theory reading group, June 2016.

57. *The Halting Problem, incompleteness, and the limits of mathematics.* cSplash program for high school students, New York University, April 2016.

58. *Why lattice problems are awesome.* NYU student theory group, March 2016.

59. *Cryptographic reverse firewalls.* NYU Cryptography Reading Group, February 2016.

60. *Solving SVP (and CVP) in 2^n time using discrete Gaussian sampling.* Centrum Wiskunde & Informatica, January 2016.

61. *Discrete Gaussian Sampling reduces to CVP (and SVP).* SODA, January 2016.

62. *Solving SVP (and CVP) in 2^n time using discrete Gaussian sampling.* Weizmann Institute theory seminar, November 2015.

63. *Cryptographic Reverse Firewalls.* Greater Tel Aviv Area Crypto Seminar (GTACS), October 2015.

64. *Solving CVP in 2^n time—The discrete Gaussian strikes again!* FOCS, October 2015.

65. *Solving SVP (and CVP) in 2^n time using discrete Gaussian sampling.* MIT Cryptography and Information Security group, September 2015.

66. *Solving SVP in 2^n time using discrete Gaussian sampling.* Simons Institute cryptography program, July 2015. youtube.com/watch?v=PWy0ZBRAUxA.

67. *What makes poker awesome?* Simons Institute cryptography program, July 2015.

68. *Solving SVP in 2^n time using discrete Gaussian sampling.* STOC, June 2015.

69. *Solving SVP in 2^n time using discrete Gaussian sampling.* Columbia University theory group, May 2015.

70. *Solving SVP in 2^n time using discrete Gaussian sampling.* ENS lattice and cryptography group, May 2015.

71. *Cryptographic reverse firewalls.* Eurocrypt, April 2015.

72. *The Halting Problem, incompleteness, and the limits of mathematics.* cSplash program for high school students, New York University, April 2015.

73. *How to eat your entropy and have it too— Optimal recovery strategies for compromised RNGs.* CRYPTO, 2014. youtube.com/watch?v=CTuA1wY-704.

74. *On the Closest Vector Problem with a distance guarantee.* CCC, June 2014.

75. *The Halting Problem, incompleteness, and the limits of mathematics.* cSplash program for high school students, New York University, April 2014. youtube.com/watch?v=CYSqeNjZzOU.

76. *The FM-Index.* Invited by Seven Bridges Genomics, January 2014. www.youtube.com/watch?v=jfaCUFkhjwk.

77. *How Hard Is a Problem—Complexity theory.* cSplash program for high school students, New York University, April 2013.

78. *What makes poker awesome (and deep)?* NYU Game Center, March 2013. youtube.com/watch?v=W2qcWGFFiLA.

Teaching

Spring 2026 **Seminar on Cryptography and Complexity**

Cornell CS 7800 (PhD-level seminar).

Fall 2025 **Introduction to Cryptography**

Cornell CS 4830 (undergrad), CS 5830 (masters), and CS 6830 (PhD).

Spring 2025 **Lattices: Geometry, Cryptography, and Algorithms**

Cornell CS 6802 (grad), cross-listed as Math 6302. An original course.

Fall 2024 **Introduction to Cryptography**

Cornell CS 4830 (undergrad), CS 5830 (masters), and CS 6830 (PhD).

Spring 2024 **Lattices: Geometry, Cryptography, and Algorithms**

Cornell CS 6802 (grad), cross-listed as Math 6302. An original course.

Fall 2023 **Discrete Structures**

Cornell CS 2800 (undergrad).

Spring 2023 **Introduction to Cryptography**

Cornell CS 4830 (undergrad).

Fall 2022 **Lattices: Geometry, Cryptography, and Algorithms**

Cornell CS 6802 (grad), cross-listed as Math 6302. An original course.

2022-2024 **CSMore**
Co-professor of discrete mathematics
A summer program for rising cornell sophomores, largely from underrepresented groups.

Spring 2022 **Introduction to Cryptography**

Cornell CS 4830 (undergrad).

Fall 2021 **Lattices: Geometry, Cryptography, and Algorithms**

Cornell CS 6802 (grad). An original course.

Spring 2021 **Introduction to Cryptography**

Cornell CS 4830 (undergrad).

Fall 2020 **Cryptography**

Cornell CS 6830 (grad).

Fall 2019 **Cryptography and Cryptanalysis**

MIT 6.875 (mixed grad and undergrad)

Fall 2018 **Learning with Errors and Post-Quantum Cryptography, MIT**
Guest lecturer
Taught the classes on Ring-SIS and Ring-LWE in Vinod Vaikuntanathan's course on LWE.

Fall 2016 **Lattices Minicourse, NYU**

An original introductory class on lattices and computational lattice problems for PhD students and postdocs.

2013-2016 **cSplash**
Teacher and organizer
cSplash is an annual lecture series (and meet up) at NYU for mathematically inclined high school students in the New York area.

Fall 2007 **CS51: Models of Computation, Brown University**
Teaching assistant
Worked with Professor Anna Lysyanskaya. Subject matter included various representations of computation (finite-state automata, Turing machines, etc.), decidability, and basic complexity theory.

Fall 2006 **CS2: Concepts and Challenges in Computer Science, Brown University**
Teaching assistant
Worked with Professor Don Stanford. Subject matter included PHP and SQL.

Service

- **Program committees**: Africacrypt 2018; Approx 2018; Crypto 2018; C2SI 2019; Africacrypt 2019; TCC 2019; Africacrypt 2020; ICALP 2021; CRYPTO 2022; TCC 2022; FOCS 2023; SOSA 2024; ITC 2024; Random 2025.
- **External reviews**: Annals of Math; ANTS; Approx; BCS; CCC; Computational Complexity; Computational Geometry; COLT; CRYPTO; DESI; Eurocrypt; ESA; FOCS; ICALP; ICITS; IPCO; IPL; ISAAC; ISIT; ITCS; JCST; J. of Crypto; Math. Rev.; RANDOM; SCIS; SIAGA; SIDMA; SoCG; SODA; SOSA; STOC; TCC; TCS; ToC; Trans. of Info. Theory.
- **Dissertation committees**: Shravas Rao (NYU), Rajendra Kumar (IIT Kanpur and NUS), Moritz Venzin (EPFL), Wessel van Woerden (Universiteit Leiden), Tao Yu (Cornell). Yael Eisenberg (Cornell, chair), Spencer Peters (Cornell, chair).
- **A exam committees** (Cornell's version of a depth-qualifying exam): James Augsten, Philip (Daniel) Brous, Benjamin Chan, Yael Eisenberg (chair), Surendra Ghentiyala (chair), Mohit Gurumukhani, Yanyi Liu, Princewill Okoroafor, Spencer Peters (chair), Noam Ringach, Pengzhi Huang, Tao Yu.
- **M exam committees** (for master's students): Ellie Fassman (chair), Atul Ganju, Santiago Lai (chair).

Organized events, workshops, seminars, etc.

- **CHarM seminar series**, as part of an NSF grant on Cryptographic Hardness of Module lattices (organized jointly with Shi Bai, Alice Pellet–Mary, Damien Stehlé, and Benjamin Wesolowski).
- **Workshop on Fine-grained Cryptography** as part of FSTTCS, 2022 (organized jointly with Divesh Aggarwal, Huck Bennett, Alexander Golovnev, and Rajendra Kumar).
- **Cornell Junior Theorists Workshop**, an annual workshop featuring talks by PhDs and postdocs (organized jointly with Eshan Chattopadhyay).
- **TCS+**, an online seminar series (co-organized with many people, and frankly I deserve very little credit).
- **Eastern Great Lakes Theory of Computation Workshop**, an annual regional workshop (organized jointly with Eshan Chattopadhyay, Kaave Hosseini, and Anson Kahng).