Noah Stephens-Davidowitz

Office	321 Gates Hall	**Phone**	(201) 655-5134
Website	noahsd.com	**Email**	noahsd@gmail.com
		Last updated	March 2, 2021

Education

2012-2017 **New York University**
Ph.D. in Computer Science
Specializing in post-quantum cryptography and 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

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.

Aug 2019- **Centre for Quantum Technologies, National University of Singapore**
Visiting Researcher
Annual visits to work with Divesh Aggarwal and others.

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**

Published papers

1. 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.org/abs/2007.09556.

2. 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.org/abs/1911.02440.

3. 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.

4. Tamalika Mukherjee and Noah Stephens-Davidowitz. *Lattice Reduction for Modules, or How to Reduce ModuleSVP to ModuleSVP.* In *CRYPTO*, 2020. eprint.iacr.org/2019/1142.

5. Divesh Aggarwal, Jianwei Li, Phong Q. Nguyen, Noah Stephens-Davidowitz. *Slide reduction, revisited–Filling the gaps in SVP approximation.* In *CRYPTO*, 2020. arxiv.org/abs/1908.03724.

6. Divesh Aggarwal and Siyao Guo, Maciej Obremski, João Ribeiro, and Noah Stephens-Davidowitz. *Extractor lower bounds, revisited.* In *RANDOM*, 2020. eccc.weizmann.ac.il/report/2019/173/.

7. Noah Stephens-Davidowitz and Vinod Vaikuntanathan. *SETH-hardness of coding problems.* In *FOCS*, 2019. eccc.weizmann.ac.il/report/2019/159/.

8. 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.org/abs/1802.05708.

9. Noah Stephens-Davidowitz. *A time-distance trade-off for GDD with preprocessing—Instantiating the DLW heuristic*. In *CCC*, 2019. arxiv.org/abs/1902.08340.

10. Divesh Aggarwal and Noah Stephens-Davidowitz. *(Gap/S)ETH Hardness of SVP*. In *STOC*, 2018. arxiv.org/abs/1712.00942.

11. 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.org/abs/1709.01535.

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

13. Huck Bennett, Alexander Golovnev, Noah Stephens-Davidowitz. *On the quantitative hardness of CVP*. In *FOCS*, 2017. arxiv.org/abs/1704.03928.

14. Oded Regev and Noah Stephens-Davidowitz. *A reverse Minkowski theorem*. In *STOC*, 2017. arxiv.org/abs/1611.05979.
Invited to the *STOC* 2017 special issue of SIAM JoC. Submitted to the *Annals of Mathematics*.
Bourbaki Seminar by Jean-Benoît Bost: youtube.com/watch?v=j7YvtVvv3qs (in French).

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

16. Oded Regev and Noah Stephens-Davidowitz. *An inequality for Gaussians on lattices*. *SIAM Journal on Discrete Mathematics (SIDMA)*, 2017, 31(2), 749–757. arxiv.org/abs/1502.04796.

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

18. Huck Bennett, Daniel Dadush, and Noah Stephens-Davidowitz. *On the Lattice Distortion Problem*. In *ESA*, 2016. arxiv.org/abs/1605.03613.

19. Noah Stephens-Davidowitz. *Search-to-decision reductions for lattice problems with approximation factors (slightly) greater than one*. In *APPROX*, 2016. arxiv.org/abs/1512.04138.

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

21. Noah Stephens-Davidowitz. *Discrete Gaussian sampling reduces to CVP and SVP*. In *SODA*, 2016. arxiv.org/abs/1506.07490.

22. 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.org/abs/1504.01995.

23. 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.org/abs/1412.7994.

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

25. 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.iacr.org/2014/167.
Invited to the *CRYPTO* 2014 special issue of *Algorithmica*.

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

Preprints and manuscripts

1. Yevgeniy Dodis, Siyao Guo, Noah Stephens-Davidowitz, and Zhiye Xie. *No time to hash—On super-efficient entropy accumulation.*
2. Yevgeniy Dodis, Siyao Guo, Noah Stephens-Davidowitz, and Zhiye Xie. *Online linear extractors for independent sources.*
3. Zvika Brakerski, Noah Stephens-Davidowitz, and Vinod Vaikuntanathan. *On the hardness of average-case k-SUM.* arxiv.org/abs/2010.08821.
4. Divesh Aggarwal and Noah Stephens-Davidowitz. *An improved constant in Banaszczyk's transference theorem.* arxiv.org/abs/1907.09020.
5. 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.
6. Noah Stephens-Davidowitz. *Dimension-preserving reductions between lattice problems.* Brief survey, 2015. www.noahsd.com/latticeproblems.pdf.
7. Noah Stephens-Davidowitz and Alex Cloninger. *The Cyclic Sieving Phenomenon on the Alternating Sign Matrices.* noahsd.com/papers/ASMCSP.pdf, 2007.
8. Fraser Chiu Kim Hong, Alex Cloninger, and Noah Stephens-Davidowitz. *On link patterns and Alternating Sign Matrices.* noahsd.com/papers/ASMLinks.pdf, 2007.

Selected honors and awards

- **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. *Benefits and risks of post-quantum cryptography.* Georgetown Computer Science colloquium, March 2021.
2. *A reverse Minkowski theorem.* Cornell Computer Science theory seminar, October 2020.
3. *Foundations of lattice-based cryptography.* Cornell Center for Applied Mathematics colloquium, October 2020.
4. *A reverse Minkowski theorem.* Simons Institute Lattices: Geometry, Algorithms, and Hardness, February 2020. youtube.com/watch?v=tZx7K0Or70Y.
5. *Algorithms for lattice problems.* Simons Institute Lattices: Geometry, Algorithms, and Hardness, January 2020. youtube.com/watch?v=o4Pl-0Q5-q0.
6. *Complexity of lattice problems.* Simons Institute Lattices: Geometry, Algorithms, and Hardness, January 2020. youtube.com/watch?v=Bi9Hs26TJa0.
7. *SETH-hardness of coding problems.* MIT theory seminar, December 2019.

8. *SETH-hardness of coding problems.* MIT theory seminar, December 2019.
9. *SETH-hardness of coding problems.* FOCS, November 2019. youtube.com/watch?v=rWLqnQn1eRQ.
10. *Will lattice-based cryptography be broken in practice?* Invited to Charles River Crypto Day, November 2019.
11. *SETH-hardness of coding problems.* Invited to the Harvard students and postdocs theory seminar, October 2019.
12. *SETH-hardness of coding problems.* Invited to the NUS theory seminar, August 2019.
13. *SETH-hardness of coding problems.* Invited to the NYU theory seminar, May 2019.
14. *Benefits and risks of post-quantum cryptography from lattices.* Invited to the Centre for Quantum Technologies colloquium, April 2019. youtube.com/watch?v=4BND9TrFr70.
15. *On the quantitative security of lattice cryptography.* Invited to the Northwestern Quarterly Theory Workshop, November 2018.
16. *A reverse Minkowski theorem.* MIT, September 2018.
17. *(Gap/S)ETH hardness of SVP.* STOC, June 2018.
18. *Fine-grained hardness of lattice problems.* Invited to the Lattice Crypto and Algorithms workshop in Bertinoro, May 2018. crypto-events.di.ens.fr/LATCA/program/nsd.pdf.
19. *A simple proof of a reverse Minkowski inequality.* Invited to IAS Computer Science/Discrete Math Seminar, April 2018. youtube.com/watch?v=9mvPxAKj5BU.
20. *Just take the average! An embarrassingly simple* 2^n*-time algorithm for SVP.* SOSA, January 2018.
21. *An embarrassingly simple* 2^n*-time algorithm for SVP—and how we hope to improve it.* Invited to FSTTCS Lattice Algorithms and Cryptography Workshop, December 2017.
22. *A reverse Minkowski theorem.* Invited to Rutgers discrete math seminar, October 2017.
23. *On the quantitative hardness of CVP.* Invited to DIMACS/Rutgers theory seminar, September 2017.
24. *On the quantitative hardness of CVP.* Princeton theory seminar, September 2017. youtube.com/watch?v=sdSMjAl0ks.
25. *On the quantitative hardness of CVP.* Invited to the Harvard Theory of Computing seminar, September 2017.
26. *A reverse Minkowski theorem.* STOC, June 2017.
27. *Pseudorandomness of Ring-LWE for any ring and modulus.* STOC, June 2017.
28. *On the quantitative hardness of CVP.* Invited to MIT Cryptography and Information Security Seminar, May 2017.
29. *A reverse Minkowski theorem.* Invited to TCS+, March 2017. www.youtube.com/watch?v=mgDNeg3U5TQ.
30. *A reverse Minkowski theorem.* Centre for Quantum Computation, National University of Singapore, March 2017.
31. *Pseudorandomness of Ring-LWE for Any Ring and Modulus.* Invited to Nanyang Technological University's Mini-Workshop on Post-Quantum Cryptanalysis, March 2017.
32. *A reverse Minkowski theorem.* Invited to the Cornell probability seminar, November 2016.
33. *A reverse Minkowski theorem.* Invited to the Columbia theory seminar, November 2016.
34. *Search-to-decision reductions for lattice problems with approximation factors (slightly) greater than one.* APPROX, September 2016.

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

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

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

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

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

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

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

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

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

44. *Cryptographic Reverse Firewalls.* Invited by the Greater Tel Aviv Area Crypto Seminar (GTACS), October 2015.

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

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

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

48. *What makes poker awesome?* Invited by Simons Institute cryptography program, July 2015.

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

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

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

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

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

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

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

56. *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.

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

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

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

Teaching

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 — **Advanced Topics in Cryptography: 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.
External reviews: Approx, ANTS; BCS; CCC; 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; STOC; TCC; TCS; ToC; Trans. of Info. Theory.
Dissertation committees: Shravas Rao (NYU), Rajendra Kumar (IIT Kanpur).