Noah Stephens-Davidowitz

Address	16 Vandeventer Ave Princeton, NJ 08542	**Phone**	(201) 655-5134
		Email	noahsd@gmail.com
Website	noahsd.com	**Last updated**	June 4, 2018

Education

2012-2017 **New York University**
Ph.D. in Computer Science

Specializing in lattices, cryptography, and theory. My advisors were Professors Oded Regev and Yevgeniy Dodis.

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

Magna Cum Laude
GPA: 3.96/4.00
Major GPA: 3.91/4.00

Selected Work Experience

Sep 2017-Aug 2018 **Princeton University**
Postdoctoral Researcher in Computer Science

Part of the Simons Collaboration on Algorithms and Geometry.

Sep 2017-Apr 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

Visited Chris Peikert.

Summer 2015 **Simons Institute**
Visiting Student

Participated in the cryptography program.

Summer 2014 **Microsoft Research**
Intern

Research in cryptography with Ilya Mironov. We introduced the notion of reverse firewalls, which provide strong security guarantees even when the user's own machine has been compromised.

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.

Papers

(See noahsd.com for the most up-to-date list of my publications.)

1. Stephen D. Miller and Noah Stephens-Davidowitz. *Generalizations of Banaszczyk's transference theorems and tail bound*. arxiv.org/abs/1802.05708.
2. Divesh Aggarwal and Noah Stephens-Davidowitz. *(Gap/S)ETH Hardness of SVP*. In *STOC*, 2018. arxiv.org/abs/1712.00942.
3. 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.
4. Huck Bennett, Alexander Golovnev, Noah Stephens-Davidowitz. *On the quantitative hardness of CVP*. In *FOCS*, 2017. arxiv.org/abs/1704.03928.
5. Navid Alamati, Chris Peikert, Noah Stephens-Davidowitz. *New (and old) proof systems for lattice problems*. In *PKC*, 2018. eprint.iacr.org/2017/1226.
6. Oded Regev and Noah Stephens-Davidowitz. *A reverse Minkowski theorem*. In *STOC*, 2017. Invited to the special issue of SIAM JoC. arxiv.org/abs/1611.05979.
7. 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.

8. 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.

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

10. 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.

11. 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.

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

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

14. 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.

15. 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.

16. 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.

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

18. 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. Invited to the special issue of Algorithmica. eprint.iacr.org/2014/167.

19. 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*.)

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

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

Selected Honors and Awards

- **NYU Outstanding Dean's Dissertation Award** in the sciences, New York University, 2018.
- **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. *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.
2. *A simple proof of a reverse Minkowski inequality.* Invited to IAS Computer Science/Discrete Math Seminar, April 2018. youtube.com/watch?v=9mvPxAKj5BU.
3. *Just take the average! An embarrassingly simple* 2^n*-time algorithm for SVP.* SOSA, 2018.
4. *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.
5. *A reverse Minkowski theorem.* Invited to Rutgers discrete math seminar, October 2017.
6. *On the quantitative hardness of CVP.* Invited to DIMACS/Rutgers theory seminar, September 2017.
7. *On the quantitative hardness of CVP.* Princeton theory seminar, September 2017. youtube.com/watch?v=sd-SMjAl0ks.
8. *On the quantitative hardness of CVP.* Invited to the Harvard Theory of Computing seminar, September 2017.
9. *A reverse Minkowski theorem.* STOC, June 2017.
10. *Pseudorandomness of Ring-LWE for any ring and modulus.* STOC, June 2017.
11. *On the quantitative hardness of CVP.* Invited to MIT Cryptography and Information Security Seminar, May 2017.
12. *A reverse Minkowski theorem.* Invited to TCS+, March 2017. www.youtube.com/watch?v=mgDNeg3U5TQ.
13. *A reverse Minkowski theorem.* Centre for Quantum Computation, National University of Singapore, March 2017.
14. *Pseudorandomness of Ring-LWE for Any Ring and Modulus.* Invited to Nanyang Technological University's Mini-Workshop on Post-Quantum Cryptanalysis, March 2017.
15. *A reverse Minkowski theorem.* Invited to the Cornell probability seminar, November 2016.
16. *A reverse Minkowski theorem.* Invited to the Columbia theory seminar, November 2016.
17. *Search-to-decision reductions for lattice problems with approximation factors (slightly) greater than one.* APPROX, September 2016.
18. *The reverse Minkowski theorem—Proof of a conjecture due to Dadush.* China Theory Week, August 2016.
19. *Message transmission with reverse firewalls—Secure communication on corrupted machines.* CRYPTO, August 2016. www.youtube.com/watch?v=2DOc-9u1EbQ.
20. *Solving SVP (and CVP) in* 2^n *time using discrete Gaussian sampling.* UM student theory reading group, June 2016.
21. *The Halting Problem, incompleteness, and the limits of mathematics.* cSplash program for high school students, New York University, April 2016.
22. *Why lattice problems are awesome.* NYU student theory group, March 2016.
23. *Cryptographic reverse firewalls.* NYU Cryptography Reading Group, February 2016.
24. *Solving SVP (and CVP) in* 2^n *time using discrete Gaussian sampling.* Invited by Centrum Wiskunde & Informatica, January 2016.
25. *Discrete Gaussian Sampling reduces to CVP (and SVP).* SODA, January 2016.

26. *Solving SVP (and CVP) in 2^n time using discrete Gaussian sampling.* Invited by the Weizmann Institute theory seminar, November 2015.
27. *Cryptographic Reverse Firewalls.* Invited by the Greater Tel Aviv Area Crypto Seminar (GTACS), October 2015.
28. *Solving CVP in 2^n time—The discrete Gaussian strikes again!* FOCS, October 2015.
29. *Solving SVP (and CVP) in 2^n time using discrete Gaussian sampling.* Invited by MIT Cryptography and Information Security group, September 2015.
30. *Solving SVP in 2^n time using discrete Gaussian sampling.* Invited by Simons Institute cryptography program, July 2015. youtube.com/watch?v=PWy0ZBRAUxA.
31. *What makes poker awesome?* Invited by Simons Institute cryptography program, July 2015.
32. *Solving SVP in 2^n time using discrete Gaussian sampling.* STOC, June 2015.
33. *Solving SVP in 2^n time using discrete Gaussian sampling.* Invited by the Columbia University theory group, May 2015.
34. *Solving SVP in 2^n time using discrete Gaussian sampling.* Invited by the ENS lattice and cryptography group, May 2015.
35. *Cryptographic reverse firewalls.* Eurocrypt, April 2015.
36. *The Halting Problem, incompleteness, and the limits of mathematics.* cSplash program for high school students, New York University, April 2015.
37. *How to eat your entropy and have it too— Optimal recovery strategies for compromised RNGs.* CRYPTO, 2014. youtube.com/watch?v=CTuA1wY-704.
38. *On the Closest Vector Problem with a distance guarantee.* CCC, June 2014.
39. *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.
40. *The FM-Index.* Invited by Seven Bridges Genomics, January 2014. www.youtube.com/watch?v=jfaCUFkhjwk.
41. *What makes poker awesome (and deep)?* Invited by NYU Game Center, March 2013. youtube.com/watch?v=W2qcWGFFiLA.

Teaching Experience

Fall 2016 **New York University**
Lattices Minicourse

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

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.
External reviews: ANTS; BCS; CCC; COLT; CRYPTO; Eurocrypt; ESA; FOCS; ICALP; ICITS; IPCO; ISAAC; ISIT; ITCS; IPL; JCST; J. of Crypto; Random; SCIS; SIAGA; SIDMA; SOCG; SODA; TCC; TCS; ToC; Trans of Info. Theory