# Stephen David Miller -- Curriculum Vitae

Born 1974, New York, USA
http://www.math.rutgers.edu/~sdmiller
Citizenship: USA miller@math.rutgers.edu

## Faculty Positions Held

| | |
|---|---|
| Chair, Rutgers University Mathematics Department | 2022- |
| Distinguished Professor of Mathematics, Rutgers University | 2019- |
| Graduate Vice-Chair, Rutgers University Mathematics Department | 2014-2016 |
| Professor of Mathematics, Rutgers University | 2012-2019 |
| Associate Professor of Mathematics, Hebrew University, Jerusalem | 2005-2006 |
| Associate Professor of Mathematics, Rutgers University | 2004-2012 |
| Assistant Professor of Mathematics, Rutgers University | 2001-2004 |
| Assistant Professor of Mathematics, Yale University | 1997-2001 |

## Visiting and Postdoctoral Positions

| | |
|---|---|
| Consultant, Microsoft Corporation | 2020-2022 |
| Consultant, Cryptography and Anti-Piracy Group, Microsoft Research | 2004-2008 |
| Consultant, Theory Group, Microsoft Research | 2002 |
| NSF Postdoctoral Fellowship, Harvard University | 1999-2000 |
| NSF Postdoctoral Fellowship, UC San Diego | 1997 |

## Education

Ph.D., Princeton University 1997

Advisor: Peter Sarnak
Dissertation: *Cusp Forms on SL(3,Z)\SL(3,R)/SO(3,R)*

M.A., Princeton University 1994

A.B. University of California, Berkeley 1993

## Awards and Grants

- National Science Foundation grant in Cryptography, CNS-2124692, 2021-2024 ($500,000)
- National Science Foundation grant in Number Theory, DMS-2101841, 2021-2024 ($180,000)
- National Science Foundation grant in Cryptography, CNS-1815562, 2018-2021 ($300,000)
- National Science Foundation grant in Number Theory, DMS-1801417, 2018-2021 ($330,000)
- Fellow of the American Mathematical Society, 2018
- National Science Foundation grant in Cryptography, CNS-1526333, 2015-2018 ($499,522)
- National Science Foundation grant in Number Theory, DMS-1500562, 2015-2018 ($75,000)
- PI on Rutgers University GAANN grant (2014-2018)
- National Science Foundation grant in Number Theory, DMS-1201362, 2012-2015 ($314,500)
- National Science Foundation grant in Number Theory, DMS-0901594, 2009-2012 ($240,000).
- National Science Foundation grant in Number Theory, DMS-0601009, 2006-2009 ($133,047).
- National Science Foundation grant in Number Theory, DMS-0301172, 2003-2006, ($105,000).
- Alfred P. Sloan Fellow, 2003-2005 ($40,000).
- National Science Foundation grant in Number Theory, DMS-0122799, 2001-2003 ($69,190).
- National Security Agency Young Investigators Grant for Number Theory, 1999-2000. ($26,000).
- Yale University Hellman Fellowship for junior faculty, 1998-2001 ($20,000).

- Initial, 3-year funding for the "*Research Opportunities in Mathematics and Economics*" (R.O.M.E. ) program, Yale College Dean's Office, 1998-2001 ($60,000). (This program is now known as "The Herbert Scarf Summer Research
- Opportunities" program.)
- National Science Foundation Travel Grant for the 1998 International Congress of Mathematicians ($1,800).
- National Science Foundation Mathematical Sciences Postdoctoral Research Fellowship,1997-2000 ($75,000).
- National Science Foundation Graduate Research Fellowship, 1994-1997.
- Departmental Citation (Valedictorian), Dorothea Klumpke Roberts Award, and Highest Honors, Department of Mathematics, University of California at Berkeley, May 1993.

## **Publications** (Available at **http://www.math.rutgers.edu/~sdmiller** )

*1.* *Spectral and Cohomological Applications of the Rankin-Selberg Method*, International Mathematics Research Notices, 1996, No. 1, pp. 15-26.

*2.* *Level spacings for regular graphs* , with D. Jakobson, I. Rivin, and Z. Rudnick, The IMA Volumes in Mathematics and its Applications, Volume 109, "Emerging Applications of Number Theory," Dennis Hejhal, Fan Chung, Joel Friedman, Martin Gutzwiller, and Andrew Odlyzko (eds.), Springer-Verlag New York, Inc. (1999), pp. 317-327.

*3.* *Non-vanishing of the Central Derivative of Canonical Hecke L-functions*, with Tonghai Yang, *Math. Res. Letters*, **7** (2000), pp. 263-278.

*4.* *Landau-Siegel zeroes and black hole entropy*, with Gregory Moore, and *Large values of L'/L(1,-p),* appendix. *Asian Journal of Mathematics*, **4**, No. 1, (March 2000 Kodaira volume), pp. 183-212. hep-th/9903267.

*5.* *On the existence and temperedness of cusp forms for SL(3,Z)*, *Journal für die reine und angewandte Mathematik,* **533** (2001), pp. 127–169.

*6.* *The highest-lowest zero and other applications of positivity*, *Duke Mathematical Journal*, **112** (2002), No. 1, pp. 83-116.

7. *Summation Formulas, from Poisson and Voronoi to the Present*, with Wilfried Schmid, in *Noncommutative harmonic analysis,* 419--440, Progr. Math., **220**, *Birkhäuser Boston, Boston, MA,* 2004.

8. *Riemann's zeta function and beyond*, with Stephen Gelbart, *Bull. Amer. Math. Soc.* **41** (2004), 59-112.

9. *Distributions and Analytic Continuation of Dirichlet Series*, with Wilfried Schmid, *Journal of Functional Analysis*, **24** (2004), pp. 155-220.

10. *The Highly Oscillatory Behavior of Automorphic Distributions for SL(2)*, with Wilfried Schmid, *Letters in Math. Phys*., **69** (2004), pp. 265-286.

11. *Automorphic Distributions, L-functions, and Voronoi Summation for GL(3)*, with Wilfried Schmid, *Annals of Mathematics* **164** (2006), pp. 423-488.

12. *Cancellation in additively twisted sums on GL(n), American Journal of Mathematics,* **128** (2006), pp. 699-729.

13. *Do all elliptic curves of the same order have the same difficulty of discrete log?,* with David Jao and Ramarathnam Venkatesan, in *Advances in Cryptology - ASIACRYPT 2005: 11th International Conference on the Theory and Application of Cryptology and Information Security*, Springer Verlag Lecture Notes in Computer Science, **3788** (2005), pp. 21-40.

14. *The Rankin-Selberg method for automorphic distributions*, with Wilfried Schmid, in "Representation Theory and Automorphic Forms", pp. 111-150, Toshiyuki Kobayashi, Wilfried Schmid, and Jae-Hyun Yang, editors, Progress in Mathematics **255**, Birkhauser, Boston, 2008.

15. *Spectral Analysis of Pollard Rho Collisions*, with Ramarathnam Venkatesan, Procedings of the 7th Algorithmic Number Theory Symposium (Berlin), Springer-Verlag Lecture Notes in Computer Science **4076** (2006), pp. 573-581.

16. *MV3 --- A New Stream Cipher Based on Rapidly Mixing Random Walks and Revolving Buffers*, with Nathan Keller, Ilya Mironov, and Ramarathnam Venkatesan, in Topics in Cryptology -- Procedings of CT-RSA 2007, Springer-Verlag Lecture Notes in Computer Science, **4377** (2007), pp. 1-19.

17. *Non-degeneracy of Pollard rho collisions*, with Ramarathnam Venkatesan, *International Mathematics Research Notices* 2009*,* pp.1-10.

18. *Expander graphs based on GRH and an application to elliptic curve cryptography*, with David Jao and Ramarathnam Venkatesan, *Journal of Number Theory* **129** (2009), pp. 1491-1504.

19. *Distinguishing attacks on stream ciphers based on arrays of*

*pseudo-random words*, with Nathan Keller, *Information Processing Letters* **110** (2010), pp. 129-132.

20. *A method for computing general automorphic forms on general groups*, *Forum Mathematicum*, **22** (2010), pp. 1207-1211.

21. *A general Voronoi summation formula for GL(n,Z)*, with Wilfried Schmid, in *"Geometric analysis: Present and Future, vol. II",* procedings of a conference held in honor of the 60th birthday of Shing-Tung Yau at Harvard, August 27-Sept 1, 2008, Advanced Lectures in Math, volume 18, pp. 173-224.

22. *Eisenstein series for higher-rank groups and string theory amplitudes*, with Michael Green, Jorge Russo, and Pierre Vanhove, in Communications in Number Theory and Physics, Volume **4** (2010), pp. 551-596.

23. *Adelization of Automorphic Distributions and Mirabolic Eisenstein Series*, with Wilfried Schmid, in *Representation theory and mathematical physics,* J. Adams, B. Lian, and S. Sahi, editors, *Contemporary Mathematics* **557** (2011), pp. 289-334.

24. *Pairings of automorphic distributions*, with Wilfried Schmid, *Mathematische Annalen* **353** (2012), pp. 581-597.

25. *On the rapid decay of cuspidal automorphic forms*, with Wilfried Schmid, *Advances in Mathematics* **231** (2012), pp. 940-964.

26. *The Archimedean theory of the exterior square L-function over Q*, with Wilfried Schmid, *Journal of the American Mathematical Society*, **25** (2012), pp. 465-506.

27. *Fourier coefficients of automorphic forms, character variety orbits, and small representations*, with Siddhartha Sahi, *Journal of Number Theory* **132** (2012), pp. 3070-3108.

28. *Residual automorphic forms and spherical unitary representations of exceptional groups*, *Annals of Mathematics* **177** (2013), pp. 1169-1179.

29. *A p-adic integral for the reciprocal of L-functions*, with Stephen Gelbart, Alexei Pantchichkine, and Freydoon Shahidi, in *Automorphic forms and related geometry: assessing the legacy of I. I. Piatetski-Shapiro,* pp.53–68, Contemp. Math., **614**, Amer. Math. Soc., Providence, RI, 2014.

30. *Small representations, string instantons, and Fourier modes of Eisenstein series*, with Michael Green and Pierre Vanhove; includes appendix "Special unipotent representations" by Dan Ciubotaru and Peter E. Trapa, J. Number Theory **146** (2015), pp. 187–309. http://arxiv.org/PS_cache/arxiv/pdf/1111/1111.2983v1.pdf

31. *Entirety of cuspidal Eisenstein series on loop groups*, with Howard Garland and Manish Patnaik, Amer. J. Math. **139** (2017), pp. 461–512. http://arxiv.org/abs/1304.4913

32. *SL(2,Z)-invariance and D-instanton contributions to the $D^6R^4$ interaction*, with Michael B. Green and Pierre Vanhove, *Communications in Number Theory and Physics* **9** (2015), pp. 307-344. http://arxiv.org/abs/1404.2192

33. *Non-abelian analogs of lattice rounding*, with Evgeni Begelfor and Ramarathnam Venkatesan, Groups Complexity Cryptology **7** (2015), pp. 117–133. http://eprint.iacr.org/2015/024.pdf

34. *The sphere packing problem in dimension 24*, with Henry Cohn, Abhinav Kumar, Danylo Radchenko, and Maryna Viazovska, Ann. of Math. **185** (2017), pp. 1017–1033. http://arxiv.org/pdf/1603.06518v1.pdf

35. *Estimates on Eisenstein distributions for reciprocals of p-adic L-functions: the case of irregular primes*, with Stephen Gelbart, Ralph Greenberg, and Freydoon Shahidi, in *Representation Theory, Number Theory, and Invariant Theory: In Honor of Roger Howe on the Occasion of His 70th Birthday*, Ju-Lee Kim, James Cogdell, and Chengbo Zhu, editors, pp. 193-208, Progress in Mathematics **323**, Birkhauser, 2017. http://front.math.ucdavis.edu/1611.09757

36. *Weights, raising and lowering operators, and K-types for automorphic forms on SL(3,R)*, with Jack Buttcane, in *Representation Theory, Automorphic Forms, and Complex Geometry: A Tribute to Wilfried Schmid*, International Press, 2020.

37. *The balanced Voronoi formulas for GL(n),*with Fan Zhou, *Internatonal Mathematics Research Notices*, **2019**, pp. 3473-3484. https://arxiv.org/abs/1612.04886

38. *What mathematics is really behind the distributional Gamma-factors?* To appear in *Representation Theory, Automorphic Forms, and Complex Geometry: A Tribute to Wilfried Schmid*, International Press, 2020.
http://math.harvard.edu/conferences/schmid_2013/problems/8.pdf

39. *A Spectral reciprocity formula and non-vanishing for L-functions on GL(4)xGL(2),* with Valentin Blomer and Xiaoqing Li, *Journal of Number Theory Prime,* **205** (2019), pp. 1-43. https://arxiv.org/abs/1705.04344

40. *Generalizations of Banaszczyk's transference theorems and tail bound*, with Noah Stephens-Davidowitz. *SIAM Journal on Discrete Mathematics,* **33** (2019), pp. 1313-1325 https://arxiv.org/abs/1802.05708

41. *On the nonexistence of automorphic eigenfunctions of exponential growth on SL(3,Z)\SL(3,R)/SO(3,R)*, with Tien D. Trinh, *Research in Number Theory* **5**:31 (2019).

42. *Coppersmith's lattices and ``focus groups'': an attack on small-exponent RSA*, with Bhargav Narayanan and Ramarathnam Venkatesan, Journal of Number Theory **222** (2021), pp. 376-392. https://eprint.iacr.org/2017/835

43. *A template method for Fourier coefficients of Langlands Eisenstein series*, with Dorian Goldfeld and Michael Woodbury, Riv. Math. Univ. Parma (N.S.) **12** (2021), no. 1, 63–117. https://arxiv.org/abs/2007.13268

44. Generating cryptographically-strong random lattice bases and recognizing rotations of $Z^n$, with Tamar Lichter Blanks, Post Quantum Cryptography 2021, Lecture Notes in Comput. Sci. **12841**, Springer, pp. 319-338. https://eprint.iacr.org/2021/154.pdf

45. *On Arthur's unitarity conjecture for split real groups*, with Joseph Hundley, American Journal of Mathematics **144** (2022), pp. 1561-1600. https://arxiv.org/abs/1908.04363

46. *Universal optimality of the $E_8$ and Leech lattices and interpolation formulas*, with Henry Cohn, Abhinav Kumar, Danylo Radchenko, and Maryna Viazovska, Annals of Mathematics **196** (2022), pp. 983-1082. https://arxiv.org/abs/1902.05438

47. *On the convergence of Kac-Moody Eisenstein series*, with Lisa Carbone, Howard Garland, Kyu-Hwan Lee, and Dongwen Liu, American Journal of Mathematics, to appear. https://arxiv.org/abs/2005.13636

48. *Jerry Tunnell (1950–2022)*, with Joe Buhler and Alex Kontorovich, Notices Amer. Math. Soc. **70** (2023), pp. 945-952.

# Books edited

49. *Representation theory, automorphic forms, and complex geometry: a tribute to Wilfried Schmid*, Stephen D. Miller and Shing-Tung Yau, editors, International Press, 2020.

# Preprints (See Website)

50. *Stopping time signatures for some algorithms in cryptography*, with Percy Deift and Thomas Trogdon. https://arxiv.org/abs/1905.08408

# Technical Notes

51. *Some properties of optimal functions for sphere packing in dimensions 8 and 24*, with Henry Cohn. http://arxiv.org/pdf/1603.04759v1.pdf

52. *Summary of the Langlands-Shahidi method*. http://www.arxiv.org/abs/math.NT/0204148

53. *A simpler way to show zeta(3) is irrational.* http://www.math.rutgers.edu/~sdmiller/simplerzeta3.pdf

54. *The eigenvalue spacings of typical large matrices*.

55. *Cryptanalysis of the NFL schedule (expository piece)*

56. *Identifying RSA implementations via stopping time signatures*

**Lectures Transcribed/Edited for Publication**

*Selberg's Eigenvalue Conjecture*, Peter Sarnak, *Notices of the A.M.S.,* November 1995, 1272-1277.

**Editorial Activities**

Associate Editor, Journal of Number Theory 2013-

Editorial consultant, Notices of the American Mathematical Society 2015-2018

**Postdoctoral Research Supervised**

Andrew Sinton, Hebrew University, 2005-2006

Adi Akavia, Rutgers University (DIMACS), 2008-2009

Maksym Radziwill, Rutgers University, 2015

Zhi Qi, Rutgers University, 2015-2018

Alexander Walker, Rutgers University, 2018-2021

Nicholas Genise, Rutgers University, 2019-2020

Kim Klinger-Logan, NSF postdoc, Rutgers University, 2020-2023

Vladimir Sedlacek, Rutgers University, 2022-2023

Zhuohui Zhang, Rutgers University, 2022-2023

**Graduate Research Supervised**

Brandon Bate, Rutgers University (PhD October 2013)

Tien Duy Trinh, Rutgers University (PhD May 2016)

Edward Karasiewicz, Rutgers University (PhD October 2017)

Zhuohui Zhang, Rutgers University (PhD October 2018)

Doyon Kim, Rutgers University (PhD expected May 2023)

George Hauser, Rutgers University (PhD October 2023)

Forrest Thurman, Rutgers University (PhD expected May 2024)

Nicholas Backes, Rutgers University (PhD expected May 2025)

**Undergraduate Research Supervised**

Swaminathan Kumaresan, Fall 1998 (Yale University): Spacings and Schinzel's Conjecture.

Kevin Chan, Spring 2001 (Yale University): Designing a Robot to track analysts' stock upgrades and downgrades.

Rebecca Landy, Summer 2005 (Oxford University): Eigenvalue statistics of expanders based on Z/NZ.

**Seminars and Conferences Organized**

Maass Forms Seminar, Harvard University, Fall 1999.

Summer Seminar on Serre's *A Course in Arithmetic,* Yale University, 2001.

Number Theory Seminar, Rutgers University, 2002-

Number Theory Seminar, Courant Institute, New York University, Fall 2002.

Special Session in Automorphic Forms and Analytic Number Theory, AMS Eastern Sectional Meeting, Lawrenceville, NJ, April 17-18, 2004.

Summer analytic number theory seminar, Hebrew University, 2004.

Special Session on L-functions and Automorphic Forms, AMS Eastern Sectional Meeting, New York, NY, March 15-16, 2008.

Analytic Number Theory and Higher Rank Groups, conference at Courant Institute, New York, May 19-23, 2008.

Third Conference of Tsinghua Sanya International Mathematics Forum, Geometric methods in representation theory and number theory, January 5-8, 2013, Sanya, China.

Representation Theory, Automorphic Forms, and Complex Geometry, conference in honor of Wilfried Schmid's 70th birthday, Harvard University, May 20-23, 2013.

Analysis, Spectra, and Number Theory, conference in honor of Peter Sarnak's 61st birthday, Princeton University and Institute for Advanced Study, December 14-19, 2014.

Mathematics of Lattices and Cryptography, ICERM workshop, Brown University, April 21-23, 2015

Conference in honor of Howard Garland, Yale University, April 26, 2015

Eisenstein series on Kac-Moody groups and applications to physics, KIAS, Seoul, November 12-20, 2015.

Automorphic forms, mock modular forms and string theory, Simons Center for Geometry and Physics, September-October 2016

Automorphic forms, mock modular forms, and string theory, Banff International Research Station, October 29-November 3, 2017.

Breakout Session on Applied Mathematics for Secure and Trustworthy Cyberspace, SaTC NSF PI meeting, Alexandria, VA, October 28-29, 2019.

Automorphic structures in string theory, Simons Center for Geometry and Physics, March-April 2019.

Mini-workshop on the Unitary Dual, Rutgers University, January 29-30, 2020

## Outreach Activities

- "Careers, Technology, and Mathematics," Society of Black Engineers, Program for New Haven High School students, Yale University, April 1999.
- "What do Mathematicians do all day?" (April 2002 and May 2004), and "Sharing Secrets in Public" (May 2007 and December 2010), Bamford-Nightingale Girls High School, New York City.
- Presentation in BBC Horizons (NOVA) documentary, aired internationally beginning November, 2003.
- Cryptanalysis of the NFL Schedule 25-minute segment on *Wharton Moneyball Radio* (SiriusXM Satellite Radio), January 2016.