

Jeffrey Hoffstein

jhoff@math.brown.edu

Department of Mathematics
Brown University
151 Thayer Street
Providence, RI 02912
(401) 863-1123

Research Interests: Number theory, automorphic forms, cryptography

Education

Ph. D., Mathematics MIT, 1978
B. A., Mathematics Cornell University, 1974

Positions

Associate Director	ICERM	2010 - present
Professor (Chair 2009-2013)	Brown University	1989 - present
Chair, special year in automorphic forms	MSRI	1994 - 1995
Assistant, Associate Professor	University of Rochester	1982 - 1989
Visitor	Institute for Advanced Study	1986 - 1987
Visitor	SFB at Göttingen	Spring 1986
Visitor	Institute for Advanced Study	Fall 1985
Visiting Professor	University of Texas at Austin	Spring 1984
J.D. Tamarkin Asst. Professor of Mathematics	Brown University	1980 - 1982
AMS Fellowship	Cambridge University	1979 - 1980
Visitor	Institute for Advanced Study	1978 - 1979

Ph. D. Students supervised at Brown University

Daniel Lieman	1992
Shamita Dutta-Gupta	1995
Xiaotie She	1995
Adrian Diaconu	1999
Ben Brubaker	2003
Alina Bucur	2006
Tom Hulse	2013
Li-Mei Lim	2013
Chan Kuan	2014
Mehmet Kiral	2014

Awards and grants

Indo-American Fulbright fellowship at TIFR, Spring 1984
NSF summer support 1984 - 2013, NSF institute (ICERM) 2010-2020, NSF EAGER grant 2013-2016, IARPA through Security Innovation 2014-2015.

Invited Lectures and outreach activities 2015

1. Conference for Jyoti Sengupta, Mubai, January 2015;
2. Lecture on cryptography for Brown DUG, February 2015;
3. Organized Cyber Security Workshop at ICERM, April 2015
4. International Conference on Number Theory and Physics, Rio de Janeiro, June 2015;
5. Conference on Cryptography, Simons Institute for Theoretical Computer Science, Berkeley, June 2015;
6. Workshop on Cryptography and Lattices, UC Irvine, August 2015;
7. Conference for Joe Silverman, Brown University, August 2015;

8. Invited Lecture at “20 years of cryptography at WPI”, October 2015;
9. Invited Lecture at Hong Kong University, November 2015;
10. Was Associate Director in charge of running the Fall program on computational aspects of the Langlands program at ICERM, Fall of 2015;

Bibliography

1. J. Hoffstein, M. Lee, Second moments and simultaneous non-vanishing of $GL(2)$ automorphic L -series, <http://arxiv.org/pdf/1308.5980.pdf> (70 pages - presently under revision)
2. J. Hoffstein, M. Lee, Shifted multiple Dirichlet series and moments of Rankin-Selberg L -functions (85 pages) <http://arxiv.org/abs/1412.5917> (Under review by Proceedings of the London Mathematical Society)
3. J. Hoffstein, J. Silverman, PASS-Encrypt: a public key cryptosystem based on partial evaluation of polynomials, *Designs, Codes and Cryptography* December 2015, Volume 77, Issue 2, pp 541-552
4. J. Hoffstein, J. Pipher, J. Schanck, J. Silverman, W. Whyte, PASS-RS: Practical signatures from the partial Fourier recovery problem, I. Boureau, P. Owesarski, and S. Vaudenay (Eds.): *ACNS 2014*, LNCS 8479, pp. 476–493, 2014. © Springer International Publishing Switzerland 2014 <http://eprint.iacr.org/2013/757>
5. J. Hoffstein, J. Pipher, J. Schanck, J. Silverman, W. Whyte, Transcript Secure Signatures Based On Modular Lattices, *PQCrypto 2014*, *Lecture Notes in Comput. Sci.* 8772, Springer, 142–159, to appear. <http://eprint.iacr.org/2014/457>
6. R. Broker, J. Hoffstein, Fourier coefficients of sextic theta series (27 pages), *Mathematics of Computation*, <http://dx.doi.org/10.1090/mcom3044>, Article electronically published on October 21, 2015
7. J. Hoffstein, T. Hulse, Multiple Dirichlet Series and Shifted Convolutions, *Journal of Number Theory* 161 (2016) 457–533
8. J. Hoffstein, A. Kontorovich, The First Non-Vanishing Quadratic Twist of an Automorphic L -series, preprint (2010), 36 pp. arXiv:1008.0839 (30 pages)
9. B. Brubaker, D. Bump, J. Hoffstein, S. Friedberg, Coefficients of the n -fold theta function and Weyl group multiple Dirichlet series, *Contributions in Analytic and Algebraic Number Theory* (eds. Blomer, Mihailescu), Springer Proceedings in Math., Vol. 9, 2012.
10. G. Chinta, S. Friedberg, J. Hoffstein Double Dirichlet series and theta functions, *Contributions in Analytic and Algebraic Number Theory* (eds. Blomer, Mihailescu), Springer Proceedings in Math., Vol. 9, 2012.
11. S. Ganguly, J. Hoffstein and J. Sengupta, Determining modular forms on $SL_2(\mathbb{Z})$ by central values of convolution L -functions, *Math. Annalen* 345 Number 4 pp 843-857
12. P. Hirschhorn, J. Hoffstein, N. Howgrave-Graham, W. Whyte, Choosing NTRU parameters in light of combined lattice reduction and MITM approaches, *Applied Cryptography and Network Security*, LNCS, Volume 5536/2009, pp 437–455
13. J. Hoffstein, J. Pipher, J. Silverman, *An introduction to mathematical cryptography*, Undergraduate texts in mathematics, Springer, 2008
14. J. Hoffstein, N. Howgrave-Graham, J. Pipher, W. Whyte, Practical lattice-based cryptography: NTRUEncrypt and NTRUSign, *Proceedings of the conference LLL + 25*, Springer, 2008.
15. B. Brubaker, D. Bump, J. Hoffstein and S. Friedberg, Weyl group multiple Dirichlet series III: Eisenstein series and twisted unstable A_r , *Annals of Mathematics* 166 (2007), 293–316
16. B. Brubaker, D. Bump, J. Hoffstein and S. Friedberg, Metaplectic Eisenstein series on $GL(3)$, web preprint.

17. J. Hoffstein, N. Howgrave-Graham, J. Pipher, W. Whyte, NTRUEncrypt and NTRUSign: efficient public key algorithms for a post-quantum world, Proceedings of PQCrypto 2006
18. D. Bump, J. Hoffstein, S. Friedberg, D. Goldfeld editors: Multiple Dirichlet series, automorphic forms, and analytic number theory: Proceedings of the Bretton Woods Workshop on Multiple Dirichlet Series, Bretton Woods, New Hampshire, July 11-14, 2005, Published by the American Mathematical Society, Proceedings of Symposia in Pure Mathematics, Vol 75 (2006).
19. G. Chinta, J. Hoffstein and S. Friedberg, Multiple Dirichlet series and automorphic forms, Proc. Symp. Pure Math. 75 (2006), 3–41
20. B. Brubaker, D. Bump, G. Chinta, J. Hoffstein and S. Friedberg, Weyl group multiple Dirichlet series I, Proc. Symp. Pure Math. 75 (2006), 91–114.
21. G. Chinta, S. Friedberg and J. Hoffstein, Asymptotics for sums of twisted L -functions and applications, Automorphic representations, L -functions and applications: progress and prospects, Ohio State University Mathematical Research Institute Publications 11, de Gruyter, Berlin, 2005, pp. 75–94
22. J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. Silverman, W. Whyte, Performance Improvements and a Baseline Parameter Generation Algorithm for NTRUSign, Workshop on Mathematical Problems and Techniques in Cryptology, Barcelona, Spain, June 2005.
23. B. Brubaker, S. Friedberg and J. Hoffstein, Cubic twists of $GL(2)$ automorphic L -functions, Invent. Math. 160, no. 1 (2005), 31–58.
24. B. Brubaker, A. Bucur, G. Chinta, F. Frechette and J. Hoffstein, Nonvanishing twists of $GL(2)$ automorphic L -functions, Int. Math. Res. Not. 78, (2004), 4211–4239.
25. D. Bump, S. Friedberg and J. Hoffstein, Sums of twisted $GL(3)$ automorphic L -functions, Contributions to automorphic forms, geometry, and number theory, Johns Hopkins Univ. Press, 2004, pp. 131–162.
26. Nick Howgrave-Graham, Jeff Hoffstein, Jill Pipher, Joseph H. Silverman, and William Whyte, NTRUSign: Digital Signatures Using the NTRU Lattice, Proceedings of the RSA conference, 2003.
27. J. Hoffstein and J.H. Silverman, Random small hamming weight products with applications to cryptography, Discrete Applied Mathematics 130 (2003), pp 37–49.
28. A. Diaconu, D. Goldfeld and J. Hoffstein, Multiple Dirichlet series and moments of zeta and L -functions, Compositio Math. 139 (2003, no. 3), 297–360.
29. S. Friedberg, J. Hoffstein, D. Lieman, Double Dirichlet series and the n^{th} order twists of Hecke L -series, Mathematische Annalen 327 (2003), 315–338.
30. J. Hoffstein, J. Pipher and J. H. Silverman, NSS: an NTRU lattice-based signature scheme, Advances in cryptology EUROCRYPT 2001 (Innsbruck), Lecture Notes in Comput. Sci., 2045, Springer, 2001, pp. 211–228
31. J. Hoffstein and J.H. Silverman, MiniPASS: Authentication and digital signatures in a constrained environment, Workshop on Cryptographic Hardware and Embedded Systems (CHES 2000) (C.K. Koc and C. Paar, eds.), Springer-Verlag, 2000.
32. J. Hoffstein and J. Silverman, Optimizations for NTRU, Public Key Cryptography and Computational Number Theory, DeGruyter, 2000, pp 11–15.
33. J. Hoffstein and D. Lieman, The Distribution of the Quadratic Symbol in Function Fields and a Faster Mathematical Stream Cipher, Proceedings of Singapore workshop in cryptography, Springer-Verlag, 2000.
34. J. Hoffstein and J.H. Silverman, Polynomial Rings and Efficient Public Key Authentication II, Proceedings of a Conference on Cryptography and Number Theory (CCNT 99) (I. Shparlinski, ed.), Birkhauser, 1999.

35. J. Hoffstein, D. Lieman, J.H. Silverman, Polynomial Rings and Efficient Public Key Authentication, Proceeding of the International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC 99), Hong Kong (M. Blum and C.H. Lee, eds.), City University of Hong Kong Press.
36. J. Hoffstein, J. Pipher, J.H. Silverman, NTRU: A Ring Based Public Key Cryptosystem, Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, Lecture Notes in Computer Science 1423 (J.P. Buhler, ed.), Springer-Verlag, Berlin, 1998, pp. 267–288.
37. J. Hoffstein and W. Luo, Nonvanishing of L -series and the combinatorial sieve, *Math. Res. Lett.* 4 (1997, no. 2-3), 435–444.
38. J. Hoffstein and P. Lockhart, Omega results for automorphic L -functions, Automorphic forms, automorphic representations, and arithmetic, *Proc. Sympos. Pure Math., Part 2, Amer. Math. Soc.*, 1996, pp. 239–250.
39. D. Farmer, J. Hoffstein and D. Lieman, Average values of cubic L -series, Automorphic forms, automorphic representations, and arithmetic, *Proc. Sympos. Pure Math., Part 2, Amer. Math. Soc.*, 1996, pp. 27–34.
40. D. Bump, D. Ginzburg and J. Hoffstein, The symmetric cube, *Invent. Math.* 125 (1996), 413–449.
41. D. Bump, S. Friedberg and J. Hoffstein, On some applications of automorphic forms to number theory, *Bull. Amer. Math. Soc. (N.S.)* 33 (1996, no. 2), 157–175.
42. J. Hoffstein and D. Ramakrishnan, Siegel zeros and cusp forms, *Internat. Math. Res. Notices* (1995, no. 6), 279–308.
43. S. Friedberg and J. Hoffstein, Nonvanishing theorems for automorphic L -functions on $GL(2)$ S , Friedberg and J. Hoffstein, *Ann. of Math. (2)* 142 (1995, no. 2), 385–423.
44. J. Hoffstein, P. Lockhart, Coefficients of Maass forms and the Siegel zero, *Ann. of Math. (2)* 140 (1994, no. 1), 161–181.
45. D. Goldfeld, J. Hoffstein and D. Lieman, Appendix to: Coefficients of Maass forms and the Siegel zero, *Ann. of Math. (2)* 140 (1994, no. 1).
46. J. Hoffstein, Eisenstein series and theta functions on the metaplectic group, Theta functions: from the classical to the modern, *Amer. Math. Soc.*, pp. 65–104.
47. D. Goldfeld and J. Hoffstein, On the number of Fourier coefficients that determine a modular form D. Goldfeld and J. Hoffstein, A tribute to Emil Grosswald: number theory and related analysis, *Contemp. Math.*, 143, Amer. Math. Soc., pp. 385–393.
48. D. Bump, W. Duke, H. Iwaniec, and J. Hoffstein, An estimate for the Hecke eigenvalues of Maass forms, *Internat. Math. Res. Notices* (1992, no. 4), 75–81.
49. J. Hoffstein and M. Rosen, Average values of L -series in function fields, *J. Reine Angew. Math.* 426 (1992), 117–150.
50. J. Hoffstein, Theta functions on the n -fold metaplectic cover of $SL(2)$ - the function field case, *Invent. Math.* 107 (1992, no. 1), 61–86.
51. D. Bump, S. Friedberg and J. Hoffstein, p -adic Whittaker functions on the metaplectic group, *Duke Math. J.* 63 (1991, no. 2), 379–397.
52. D. Bump, S. Friedberg and J. Hoffstein, Nonvanishing theorems for L -functions of modular forms and their derivatives *Invent. Math.* 102 (1990, no. 3,) pp 543–618.
53. D. Bump, S. Friedberg and J. Hoffstein, The Kubota symbol for $S p(4, \mathbb{Q}(i))$, *Nagoya Math. J.* 119 (1990,) 173–188.
54. D. Bump, S. Friedberg and J. Hoffstein, Exterior algebra and the Iwasawa decomposition (appendix to On explicit integral formulas for $GL(n, \mathbb{R})$ -Whittaker functions by E. Stade), *Duke Math. J.* 60 (1990, no. 2), 313–362.

55. D. Bump, S. Friedberg and J. Hoffstein, Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic L -functions and their derivatives, *Ann. of Math. (2)* 131 (1990), no. 1), 53–127.
56. D. Bump, S. Friedberg and J. Hoffstein, On Waldspurgers theorem, *Automorphic forms and analytic number theory*, Univ. Montr?eal, 1990, pp. 25–36.
57. J. Hoffstein and N. Jochnowitz, On Artins conjecture and the class number of certain CM fields I, *Duke Math. J.* 59 (1989, no. 2,), 553–563.
58. J. Hoffstein and N. Jochnowitz, On Artins conjecture and the class number of certain CM fields II, *Duke Math. J.* 59 (1989, no. 2,), 565–584.
59. D. Bump, S. Friedberg and J. Hoffstein, A nonvanishing theorem for derivatives of automorphic L -functions with applications to elliptic curves, *Bull. Amer. Math. Soc. (N.S.)* 21 (1989, no. 1), 89–93.
60. J. Hoffstein and M. R. Murty, L -series of automorphic forms on $GL(3, R)$, *Theorie des nombres (Quebec, PQ, 1987)*, de Gruyter, Berlin, 1989, pp. 398–408.
61. D. Bump and J. Hoffstein, On Shimuras correspondence, *Duke Math. J.* 55 (1987, no. 3), pp 661–691.
62. D. Bump and J. Hoffstein, Some Euler products associated with cubic metaplectic forms on $GL(3)$, *Duke Math. J.* 53 (1986, no. 4), 1047–1072.
63. D. Bump and J. Hoffstein, Cubic metaplectic forms on $GL(3)$, *Invent. Math.* 84 (1986, no. 3), 481–505.
64. D. Bump and J. Hoffstein, Some conjectured relationships between theta functions and Eisenstein series on the metaplectic group, *Number theory (New York, 1985/1988)*, *Lecture Notes in Math.*, 1383, Springer, Berlin, 1989, pp. 1–11.
65. D. Goldfeld and J. Hoffstein, Eisenstein series of $1/2$ - integral weight and the mean value of real Dirichlet L -series, *Invent. Math.* 80 (1985, no. 2), 185–208.
66. J. Hoffstein, Real zeros of Eisenstein series, *Math. Z.* 181 (1982, no. 2), 179–190.
67. D. Goldfeld, J. Hoffstein and S. J. Patterson, On automorphic functions of half-integral weight with applications to elliptic curves, *Number theory related to Fermats last theorem (Cambridge, Mass., 1981)*, *Progr. Math.*, 26, Birkhauser, Boston, Mass., 1982, pp. 153–193.
68. J. Hoffstein, On the Siegel-Tatuzawa theorem, *Acta Arith.* 38 (1980/81, no. 2), 167–174.
69. J. Hoffstein, Some results related to minimal discriminants, *Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979)*, *Lecture Notes in Math.*, 751, Springer, Berlin, 1979, pp. 185–194.
70. J. Hoffstein, Some analytic bounds for zeta functions and class numbers J. Hoffstein, *Invent. Math.* 55 (1979), no. 1, 37–47.

Patents

1. Jeffrey Hoffstein, Burton S Kaliski Jr, Daniel Bennett Lieman, Matthew John Barton Robshaw, Yiqun Lisa Yin: Secure user identification based on constrained polynomials. RSA Security June 2000: US 6076163
2. Jeffrey Hoffstein, Jill Pipher, Joseph H Silverman: Public key cryptosystem method and apparatus. NTRU Cryptosystems June 2000: US 6081597
3. Jeffrey Hoffstein, Jill Pipher, Joseph H Silverman: Digital signature and authentication method and apparatus. September 2002: US 20020136401
4. Jeffrey Hoffstein, Joseph H Silverman: Speed enhanced cryptographic method and apparatus. April 2002: US 20020041681

5. Jeffrey Hoffstein, Nicholas A Howgrave-Graham, Jill C Pipher, Joseph H Silverman, William J Whyte: Digital signature and authentication method and apparatus. NTRU Cryptosystems June 2003: US 20030120929
6. Jeffrey Hoffstein, Joseph H Silverman, Daniel Lieman: Secure user identification based on ring homomorphisms. NTRU Cryptosystems October 2005: US 6959085
7. Jeffrey Hoffstein, Jill Pipher, Joseph H Silverman: Ring-based public key cryptosystem method. NTRU Cryptosystems October 2001: US 6298137
8. Jeffrey Hoffstein, Joseph H Silverman: Speed enhanced cryptographic method and apparatus. NTRU Cryptosystems April 2006: US 7031468
9. Jeffrey Hoffstein, Nicholas A Howgrave-Graham, Jill C Pipher, Joseph H Silverman, William J Whyte: Digital signature and authentication method and apparatus. NTRU Cryptosystems December 2007: US 7308097
10. Jeffrey Hoffstein, Nicholas A Howgrave-Graham, Jill C Pipher, Joseph H Silverman, William J Whyte: Digital signature and authentication method and apparatus. NTRU Cryptosystems March 2011: US 7913088
11. Hoffstein Jeffrey, Howgrave-Graham Nicholas, Pipher Jill, Silverman Joseph, Whyte William: Digital signature and authentication method and apparatus. / Signature numerique et procede et dispositif d'authentification. Ntru Cryptosystems NTRU CRYPTOSYSTEMS February 2013: CA 2469198
12. Jeffrey Hoffstein, Jill Pipher, Joseph H Silverman: Public key cryptosystem method and apparatus. Ntru Cryptosystems July 2000: HK 1021855
13. Jeffrey Hoffstein, Nicholas A Howgrave-Graham, Jill C Pipher, Joseph H Silverman, William J Whyte: Digital signature and authentication method and apparatus. NTRU Cryptosystems March 2009: US 20090070590
14. Jeffrey Hoffstein, Jill Piller, Joseph H Silverman: Public key cryptosystem method and apparatus. Ntru Cryptosystems October 1999: CN 97198451