

# EMANUELE VIOLA

November 4, 2020

Northeastern University, 338 West Village H (WV), 440 Huntington Avenue, Boston, MA 02115  
Web: [www.ccs.neu.edu/home/viola](http://www.ccs.neu.edu/home/viola) Email: [viola@ccs.neu.edu](mailto:viola@ccs.neu.edu) Phone: (617) 373-8298  
Blog: <https://emanueleviola.wordpress.com>

## Contents

<b>RESEARCH INTERESTS</b>	<b>2</b>
<b>POSITIONS</b>	<b>2</b>
<b>EDUCATION</b>	<b>2</b>
<b>AWARDS AND DISTINCTIONS</b>	<b>2</b>
<b>RESEARCH PAPERS</b>	<b>2</b>
<b>SURVEYS AND MY PH.D. THESIS</b>	<b>7</b>
<b>PREPRINTS AND NOTES</b>	<b>8</b>
<b>OTHER WORK BY RESEARCH GROUP</b>	<b>9</b>
<b>TALKS</b>	<b>10</b>
<b>VIDEO GAMES</b>	<b>14</b>
<b>EXTERNAL GRANTS</b>	<b>15</b>
<b>INTERNAL GRANTS</b>	<b>15</b>
<b>TEACHING: COURSES</b>	<b>15</b>
<b>RESEARCH TEAM (INCLUDING STUDENTS)</b>	<b>16</b>
<b>SERVICE TO THE INSTITUTION</b>	<b>16</b>
<b>SERVICE TO THE DISCIPLINE</b>	<b>16</b>

## RESEARCH INTERESTS

Theoretical computer science

## POSITIONS

**Northeastern University**, Boston, MA

Associate professor

Spring 2014 – present

Assistant professor

Fall 2008 – Spring 2014

Visiting Scientist at Simons Institute

Fall 2018

Visiting Scientist at Simons Institute

Fall 2015

Visiting scholar at Harvard University

2014 – 2015

**Columbia University**, New York, NY

Fall 2007 – Summer 2008

Postdoctoral fellow; Sponsor: Rocco Servedio

**Institute for Advanced Study**, Princeton, NJ

Fall 2006 – Summer 2007

Postdoctoral fellow; Sponsor: Avi Wigderson

## EDUCATION

**Harvard University**, Cambridge, MA

Fall 2001 – Summer 2006

Ph.D. Computer Science; Advisor: Salil Vadhan

**La Sapienza University**, Rome, Italy

Fall 1995 – Spring 2000

B.S. Computer Science, *summa cum laude*

## AWARDS AND DISTINCTIONS

**Best Paper Award**, IEEE Conf. on Computational Complexity, for the paper [13] 2008

**SIAM Student Paper Prize**, for the paper [7] 2006

**Six papers selected for STOC/FOCS special issues**

**Two papers selected for CCC/ICALP special issues**

## RESEARCH PAPERS

All of the conferences (and journals) below are peer reviewed.

54. AC0 unpredictability

To appear in ACM Trans. Computation Theory

53. More on bounded independence plus noise: Pseudorandom generators for read-once polynomials

With Chin Ho Lee

Theory of Computing, vol. 16, pp. 1–50, 2020

52. Lower bounds for data structures with space close to maximum imply circuit lower bounds

Theory of Computing, vol. 15, pp. 1–9, 2019

51. Sampling lower bounds: boolean average-case and permutations  
SIAM J. on Computing, vol. 49, num. 1, 2020
50. How to Store a Random Walk  
With Omri Weinstein and Huacheng Yu  
In ACM-SIAM Symp. on Discrete Algorithms (SODA), 2020
49. Constant-error pseudorandomness proofs from hardness require majority  
ACM Trans. Computation Theory, vol. 11, num. 4, pp. 19:1–19:11, 2019
48. What do humans perceive in asset returns?  
With Jasmina Hasanhodzic and Andrew Lo  
Journal of Portfolio Management, vol. 45, num. 4, pp. 49-60, 2019
47. Indistinguishability by adaptive procedures with advice, and lower bounds on hardness amplification proofs  
With Aryeh Grinberg and Ronen Shaltiel  
In IEEE Symp. on Foundations of Computer Science (FOCS), 2018
46. Revisiting Frequency Moment Estimation in Random Order Streams  
With Vladimir Braverman and David P. Woodruff and Lin F. Yang  
In Coll. on Automata, Languages and Programming (ICALP), 2018
45. The coin problem for product tests  
With Chin Ho Lee  
ACM Trans. Computation Theory, vol. 10, num. 3, 2018
44. Local Expanders  
With Avi Wigderson  
Computational Complexity, vol. 27, num. 2, pp. 225-244, 2018
43. Bounded independence plus noise fools products  
With Elad Haramaty and Chin Ho Lee  
SIAM J. on Computing, vol. 47, num. 2, pp. 295-615, 2018  
Preliminary version in Conf. on Computational Complexity (CCC), 2017
42. Block-symmetric polynomials correlate with parity better than symmetric  
With Frederic Green and Daniel Kreymer  
Computational Complexity, vol. 26, num. 2, pp. 323-364, 2017
41. Some limitations of the sum of small-bias distributions  
With Chin Ho Lee  
Theory of Computing, vol. 13, 2017
40. Interleaved group products  
With W. T. Gowers  
SIAM J. on Computing, vol. 48, num. 3, pp. 554–580, 2019  
Preliminary version in IEEE Symp. on Foundations of Computer Science (FOCS), 2016  
**FOCS Special Issue.** The journal version includes the results appearing in the STOC 2015 and FOCS 2016 conference versions

39. Bounded Independence versus Symmetric Tests  
 With Ravi Boppana and Johan Håstad and Chin Ho Lee  
 ACM Trans. Computation Theory, vol. 11, num. 4, pp. 21:1–21:27, 2019  
 Preliminary version in Workshop on Randomization and Computation (RANDOM), 2016
38. Bounded indistinguishability and the complexity of recovering secrets  
 With Andrej Bogdanov and Yuval Ishai and Christopher Williamson  
 In Int. Cryptology Conf. (CRYPTO), 2016
37. Quadratic maps are hard to sample  
 ACM Trans. Computation Theory, vol. 8, num. 4, 2016
36. Local reductions  
 With Hamid Jahanjou and Eric Miles  
 Information and Computation, vol. 261, num. 2, 2018  
 Preliminary version in Coll. on Automata, Languages and Programming (ICALP), 2015  
 ICALP Special issue
35. The communication complexity of interleaved group products  
 With W. T. Gowers  
 In ACM Symp. on the Theory of Computing (STOC), 2015
34. On Randomness Extraction in AC0  
 With Oded Goldreich and Avi Wigderson  
 In IEEE Conf. on Computational Complexity (CCC), 2015
33. 3SUM, 3XOR, Triangles  
 With Zahra Jafargholi  
 Algorithmica, pp. 1-18, 2014
32. Short PCPs with projection queries  
 With Eli Ben-Sasson  
 In Coll. on Automata, Languages and Programming (ICALP), 2014
31. Real advantage  
 With Alexander Razborov  
 ACM Trans. Computation Theory, vol. 5, num. 4, pp. 17, 2013
30. Shielding circuits with groups  
 With Eric Miles  
 In ACM Symp. on the Theory of Computing (STOC), 2013
29. On the complexity of information spreading in dynamic networks  
 With Chinmoy Dutta and Gopal Pandurangan and Rajmohan Rajaraman and Zhifeng Sun  
 In ACM-SIAM Symp. on Discrete Algorithms (SODA), 2013
28. The communication complexity of addition  
 Combinatorica, pp. 1-45, 2014  
 Preliminary version in ACM-SIAM Symp. on Discrete Algorithms (SODA), 2013

27. Extractors for Turing-machine sources  
In Workshop on Randomization and Computation (RANDOM), 2012
26. Substitution-permutation networks, pseudorandom functions, and natural proofs  
With Eric Miles  
J. of the ACM, vol. 62, num. 6, 2015  
Preliminary version in Int. Cryptology Conf. (CRYPTO), 2012
25. Tight bounds on computing error-correcting codes by bounded-depth circuits with arbitrary gates  
With Anna Gál and Kristoffer Arnsfelt Hansen and Michal Koucký and Pavel Pudlák  
IEEE Transactions on Information Theory, vol. 59, num. 10, pp. 6611-6627, 2013  
Preliminary version in ACM Symp. on the Theory of Computing (STOC), 2012
24. Extractors for circuit sources  
SIAM J. on Computing, vol. 43, num. 2, pp. 355-972, 2014  
Preliminary version in IEEE Symp. on Foundations of Computer Science (FOCS), 2011  
**FOCS Special Issue**
23. On beating the hybrid argument  
With Bill Fefferman and Ronen Shaltiel and Christopher Umans  
Theory of Computing, vol. 9, pp. 809-843, 2013  
Preliminary version in ACM Innovations in Theoretical Computer Science conf. (ITCS), 2012
22. Randomness buys depth for approximate counting  
Computational Complexity, vol. 23, num. 3, pp. 479-508, 2014  
Preliminary version in IEEE Symp. on Foundations of Computer Science (FOCS), 2011
21. On the complexity of constructing pseudorandom functions (especially when they don't exist)  
With Eric Miles  
J. of Cryptology, pp. 1-24, 2013  
Preliminary version in Theory of Cryptography Conf. (TCC), 2011
20. A Computational View of Market Efficiency  
With Jasmina Hasanhodzic and Andrew W. Lo  
Quantitative Finance, vol. 11, num. 7, 2011
19. Bounded-depth circuits cannot sample good codes  
With Shachar Lovett  
Computational Complexity, vol. 21, num. 2, pp. 245-266, 2012  
Preliminary version in IEEE Conf. on Computational Complexity (CCC), 2011  
CCC Special issue
18. The complexity of distributions  
SIAM J. on Computing, vol. 41, num. 1, pp. 191-218, 2012  
Preliminary version in 51th IEEE Symp. on Foundations of Computer Science (FOCS), 2010
17. Cell-probe lower bounds for succinct partial sums  
With Mihai Pătraşcu  
In 21th ACM-SIAM Symp. on Discrete Algorithms (SODA), 2010

16. Bounded Independence Fools Halfspaces  
 With Ilias Diakonikolas and Parikshit Gopalan and Ragesh Jaiswal and Rocco A. Servedio  
 SIAM J. on Computing, vol. 39, num. 8, pp. 3441-3462, 2010  
 Preliminary version in 50th IEEE Symp. on Foundations of Computer Science (FOCS), 2009
15. Bit-probe lower bounds for succinct data structures  
 SIAM J. on Computing, vol. 41, num. 6, pp. 1593-1604, 2012  
 Preliminary version in 41th ACM Symp. on the Theory of Computing (STOC), 2009  
**STOC Special Issue**
14. Improved separations between nondeterministic and randomized multiparty communication  
 With Matei David and Toniann Pitassi  
 ACM Trans. Computation Theory, vol. 1, num. 2, pp. 1-20, 2009  
 Preliminary version in 12th Workshop on Randomization and Computation (RANDOM), 2008
13. The sum of  $d$  small-bias generators fools polynomials of degree  $d$   
 Computational Complexity, vol. 18, num. 2, pp. 209-217, 2009  
 Preliminary version in IEEE Conf. on Computational Complexity (CCC), 2008  
**Best paper award**
12. Hardness amplification proofs require majority  
 With Ronen Shaltiel  
 SIAM J. on Computing, vol. 39, num. 7, pp. 3122-3154, 2010  
 Preliminary version in 40th ACM Symp. on the Theory of Computing (STOC), 2008
11. One-way multiparty communication lower bound for pointer jumping with applications  
 With Avi Wigderson  
 Combinatorica, vol. 29, num. 6, pp. 719-743, 2009  
 Preliminary version in 48th IEEE Symp. on Foundations of Computer Science (FOCS), 2007  
 Invited to **FOCS Special Issue**
10. Pseudorandom bits for polynomials  
 With Andrej Bogdanov  
 SIAM J. on Computing, vol. 39, num. 6, pp. 2464-2486, 2010  
 Preliminary version in IEEE Symp. on Foundations of Computer Science (FOCS), 2007  
**FOCS Special Issue**
9. Norms, XOR lemmas, and lower bounds for polynomials and protocols  
 With Avi Wigderson  
 Theory of Computing, vol. 4, pp. 137-168, 2008  
 Preliminary version in IEEE Conf. on Computational Complexity (CCC), 2007
8. On approximate majority and probabilistic time  
 Computational Complexity, vol. 18, num. 3, pp. 337-375, 2009  
 Preliminary version in IEEE Conf. on Computational Complexity (CCC), 2007
7. Pseudorandom Bits for Constant-Depth Circuits with Few Arbitrary Symmetric Gates  
 SIAM J. on Computing, vol. 36, num. 5, pp. 1387-1403, 2007

Preliminary version in 20th IEEE Conf. on Computational Complexity (CCC), 2005  
**SIAM Student Paper Prize**

6. On Constructing Parallel Pseudorandom Generators from One-Way Functions  
In 20th IEEE Conf. on Computational Complexity (CCC), 2005
5. Constant-Depth Circuits for Arithmetic in Finite Fields of Characteristic Two  
With Alexander Healy  
In 23rd Symp. on Theoretical Aspects of Computer Science (STACS), 2006
4. Fooling Parity Tests with Parity Gates  
With Dan Gutfreund  
In 8th Workshop on Randomization and Computation (RANDOM), 2004
3. Using Nondeterminism to Amplify Hardness  
With Alexander Healy and Salil P. Vadhan  
SIAM J. on Computing, vol. 35, num. 4, pp. 903-931, 2006  
Preliminary version in ACM Symp. on the Theory of Computing (STOC), 2004  
**STOC Special Issue**
2. The Complexity of Constructing Pseudorandom Generators from Hard Functions  
Computational Complexity, vol. 13, num. 3-4, pp. 147-188, 2004  
Preliminary version in IEEE Conf. on Computational Complexity (CCC), 2003
1. E-unifiability via Narrowing  
In 7th Italian Conference on Theoretical Computer Science (ICTCS), 2001

## **SURVEYS AND MY PH.D. THESIS**

All of the surveys below are peer reviewed.

6. Non-abelian combinatorics and communication complexity  
SIGACT News, Complexity Theory Column, vol. 50, num. 3, 2019  
Invited survey
5. Challenges in computational lower bounds  
SIGACT News, Open Problems Column, vol. 48, num. 1, 2017
4. Selected Results in Additive Combinatorics: An Exposition  
Theory of Computing Library, Graduate Surveys series, vol. 3, pp. 1-15, 2011
3. On the power of small-depth computation  
Foundations and Trends in Theoretical Computer Science, vol. 5, num. 1, pp. 1-72, 2009  
Invited survey
2. Correlation bounds for polynomials over  $\{0, 1\}$   
SIGACT News, Complexity Theory Column, vol. 40, num. 1, 2009  
Invited survey

1. The Complexity of Hardness Amplification and Derandomization  
Ph.D. thesis, Harvard University, 2006

## PREPRINTS AND NOTES

11. New lower bounds for probabilistic degree and AC0 with parity gates  
Manuscript, 2020
10. Matching Smolensky's correlation bound with majority  
Manuscript, 2019
9. Approximate Degree-Weight and Indistinguishability  
With Xuangui Huang  
Manuscript, 2019
8. Pseudorandom bits and lower bounds for randomized Turing machines  
Manuscript, 2019
7. Special topics in complexity theory  
Manuscript, 2017  
Lecture notes of the class taught at Northeastern University
6. Succinct and explicit circuits for sorting and connectivity  
With Hamid Jahanjou and Eric Miles  
Manuscript, 2014
5. On a special case of rigidity  
With Rocco A. Servedio  
Manuscript, 2012
4. From RAM to SAT  
With NEU  
Manuscript, 2012
3. Think like the pros  
Manuscript, 2011  
Lecture notes aimed towards students lacking mathematical maturity
2. Reducing 3XOR to listing triangles, an exposition  
Manuscript, 2011
1. Gems of Theoretical Computer Science  
Manuscript, 2009  
Lecture notes of the class taught at Northeastern University



## OTHER WORK BY RESEARCH GROUP

11. Space Hardness of Solving Structured Linear Systems  
Xuanguai Huang  
In Int. Symp. on Algorithms and Computation (ISAAC), 2020
10. Absolutely Sound Testing of Lifted Codes  
Elad Haramaty and Noga Ron-Zewi and Madhu Sudan  
Theory of Computing, vol. 11, pp. 299–338, 2015
9. Optimal Dynamic Distributed MIS  
Keren Censor-Hillel and Elad Haramaty and Zohar S. Karnin  
In Symp. on Principles of Distributed Computing (PODC), 2016
8. Robust Testing of Lifted Codes with Applications to Low-Degree Testing  
Alan Guo and Elad Haramaty and Madhu Sudan  
In IEEE Symp. on Foundations of Computer Science (FOCS), 2015
7. Amplifying Privacy in Privacy Amplification  
Divesh Aggarwal and Yevgeniy Dodis and Zahra Jafargholi and Eric Miles and Leonid Reyzin  
In Int. Cryptology Conf. (CRYPTO), 2014
6. Non-malleable Codes from Additive Combinatorics  
Divesh Aggarwal and Yevgeniy Dodis and Shachar Lovett  
In ACM Symp. on the Theory of Computing (STOC), 2014
5. Key Derivation Without Entropy Waste  
Yevgeniy Dodis and Krzysztof Pietrzak and Daniel Wichs  
In Int. Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2014
4. Iterated group products and leakage resilience against  $NC^1$   
Eric Miles  
In ACM Innovations in Theoretical Computer Science conf. (ITCS), 2014
3. Coalescing-Branching Random Walks on Graphs  
Chinmoy Dutta and Gopal Pandurangan and Rajmohan Rajaraman and Scott Roche  
In ACM Symp. on Parallelism in Algorithms and Architectures (SPAA), 2013
2. Split and Join: Strong Partitions and Universal Steiner Trees for Graphs  
Costas Busch and Chinmoy Dutta and Jaikumar Radhakrishnan and Rajmohan Rajaraman and Srivathsan Srinivasagopalan  
In IEEE Symp. on Foundations of Computer Science (FOCS), 2012
1. More on a Problem of Zarankiewicz  
Chinmoy Dutta and Jaikumar Radhakrishnan  
In Int. Symp. on Algorithms and Computation (ISAAC), 2012

## TALKS

81. Boston University, Boston, MA BU; Fall 2019  
Why do lower bounds stop “just before” proving major results?
80. Simons Institute, Berkeley, CA Simons; Fall 2018  
Sampling lower bounds
79. Simons Institute, Berkeley, CA Simons; Fall 2018  
Bounded independence plus noise, and the communication complexity of decoding
78. Session on Math. Perspectives in Quantum Information Theory, Boston, MA AMS; Spring 2018  
The complexity of distributions: boolean average-case lower bounds
77. Northeastern Univ. Applied and Interdisciplinary Math. Seminar, Boston, MA NEU; Spring 2018  
Interleaved group products
76. Harvard workshop on additive combinatorics, Cambridge, MA Harvard; Fall 2017  
Interleaved group products
75. IEEE Symp. on Foundations of Computer Science, New Brunswick, NJ FOCS; Fall 2016  
The multiparty communication complexity of interleaved group products
74. Simons Institute, Berkeley, CA Simons; Fall 2015  
3SUM, 3XOR, Triangles
73. Simons Institute, Berkeley, CA Simons; Fall 2015  
Local reductions
72. ACM Symp. on Theory of Computing, Portland, OR STOC; Summer 2015  
The communication complexity of interleaved group products
71. Conf. on Computational Complexity, Portland, OR CCC; Summer 2015  
On randomness extractors in AC0
70. University of Tuzla, Bosnia Tuzla; Spring 2015  
The communication complexity of interleaved group products
69. Institute for Advanced Study, Princeton, NJ IAS; Spring 2015  
The communication complexity of interleaved group products
68. FOCS workshop on higher-order Fourier analysis, Philadelphia, PA FOCS workshop; Fall 2014  
Interleaved products in special linear groups
67. Harvard University, Cambridge, MA Harvard; Fall 2014  
Local reductions
66. Banff workshop on communication complexity, Banff, Canada Banff; Summer 2014  
The communication complexity of addition
65. Stanford University, Palo Alto, CA Stanford; Summer 2013  
Local reductions

64. ACM-SIAM Symp. on Discrete Algorithms, New Orleans, LA SODA; Spring 2013  
The communication complexity of addition
63. La Sapienza University, Rome, Italy La Sapienza; Fall 2012  
The communication complexity of addition
62. Oberwolfach meeting on complexity theory, Oberwolfach, Germany Oberwolfach; Fall 2012  
Block-symmetric polynomials correlate with parity better than symmetric
61. Int. Workshop on Randomization and Computation, Cambridge, MA RANDOM; Summer 2012  
Extractors for Turing-machine sources
60. ACM Symp. on Theory of Computing, New York, NY STOC; Spring 2012  
Tight bounds on computing error-correcting codes by bounded-depth circuits with arbitrary gates
59. Institute for Advanced Study, Princeton, NJ IAS; Spring 2012  
The complexity of distributions
58. IEEE Symp. on Foundations of Computer Science, Palm Springs, CA FOCS; Fall 2011  
Extractors for circuits sources
57. IEEE Symp. on Foundations of Computer Science, Palm Springs, CA FOCS; Fall 2011  
Randomness buys depth for approximate counting
56. Northeastern University, Boston, MA NEU; Fall 2011  
The communication complexity of addition
55. Bertinoro workshop on Ramsey Theory, Bertinoro, Italy Bertinoro; Summer 2011  
The disproof of the inverse conjecture for Gowers' norm via Ramsey Theory
54. Dagstuhl workshop on the complexity of discrete problems, Germany Dagstuhl; Spring 2011  
Extractors for circuit sources
53. Massachusetts Institute of Technology, Cambridge, MA MIT; Spring 2011  
The complexity of distributions
52. Northeastern University, Boston, MA NEU; 16 November 2010  
Williams' breakthrough
51. IEEE Symp. on Foundations of Computer Science, Las Vegas, NV FOCS; Fall 2010  
The complexity of distributions
50. Banff workshop on complexity theory, Banff, Canada Banff; Summer 2010  
The complexity of distributions
49. La Sapienza University, Rome, Italy La Sapienza; Summer 2010  
The complexity of distributions
48. Laci Babai's 60th birthday, Columbus, OH Babai is 60; Spring 2010  
The complexity of distributions

47. Microsoft Research New England  
The complexity of distributions  
Microsoft; Spring 2010
46. Harvard University, Cambridge, MA  
Lower bounds for succinct data structures  
Harvard; Fall 2009
45. La Sapienza University, Rome, Italy  
Lower bounds for succinct data structures  
La Sapienza; Summer 2009
44. ACM Symp. on Theory of Computing, Bethesda, MD  
Bit-probe lower bounds for succinct data structures  
STOC; Spring 2009
43. Northeastern University, Boston, MA  
Bit-probe lower bounds for succinct data structures  
NEU; Spring 2009
42. Institute for Advanced Study, Princeton, NJ  
Bounded independence fools halfspaces  
IAS; Spring 2009
41. Northeastern University, Boston, MA  
What is a proof? What is knowledge? What is randomness?  
NEU; Fall 2008
40. Boston University, Boston, MA  
Polynomials over  $\{0, 1\}$   
BU; Fall 2008
39. Banff workshop on analytic tools in computational complexity, Banff, Canada  
Hardness amplification proofs require majority  
Banff; Summer 2008
38. IEEE Conf. on Computational Complexity, College Park, MD  
The sum of  $d$  small-bias generators fools polynomials of degree  $d$   
CCC; Summer 2008
37. ACM Symp. on Theory of Computing, Victoria, Canada  
Hardness amplification proofs require majority  
STOC; Spring 2008
36. Columbia University, New York, NY  
Hardness amplification proofs require majority  
Columbia; Spring 2008
35. Northeastern University, Boston, MA  
Pseudorandomness  
NEU; Spring 2008
34. University of Illinois at Chicago, Chicago, IL  
Polynomials  
UIC; Spring 2008
33. The University of Chicago, Chicago, IL  
Lower bounds  
UChicago; Spring 2008
32. Institute for Advanced Study, Princeton, NJ  
Hardness amplification proofs require majority  
IAS; Spring 2008
31. Cornell workshop on discrete harmonic analysis, Ithaca, NY  
Polynomials  
Cornell; Spring 2008

30. Theory Day, New York, NY  
Polynomials Theory Day; Fall 2007
29. IEEE Symp. on Foundations of Computer Science, Providence, RI  
One-way multi-party communication lower bound for pointer jumping with applications FOCS; Fall 2007
28. IEEE Symp. on Foundations of Computer Science, Providence, RI  
Pseudorandom bits for polynomials FOCS; Fall 2007
27. Columbia University, New York, NY  
Selected results in additive combinatorics Columbia; Fall 2007
26. IEEE Conf. on Computational Complexity, San Diego, CA  
Norms, XOR lemmas, and lower bounds for GF(2) polynomials and multiparty protocols CCC; Summer 2007
25. IEEE Conf. on Computational Complexity, San Diego, CA  
On approximate majority and probabilistic time CCC; Summer 2007
24. Oberwolfach meeting on complexity theory, Oberwolfach, Germany  
One-way multi-party communication lower bound for pointer jumping Oberwolfach; Summer 2007
23. Dagstuhl workshop on the complexity of discrete problems, Germany  
On approximate majority and probabilistic time Dagstuhl; Spring 2007
22. New York University, New York, NY  
Pseudorandomness: New results and applications NYU; Spring 2007
21. Institute for Advanced Study, Princeton, NJ  
One-way multi-party communication lower bound for pointer jumping with applications IAS; Spring 2007
20. IBM Watson Research Center, Hawthorne, NY  
Pseudorandomness: New results and applications IBM; Spring 2007
19. Institute for Advanced Study, Princeton, NJ  
On approximate majority and probabilistic time IAS; Spring 2007
18. Center for Discrete Math. and Theor. C. S., Rutgers, NJ  
Norms, XOR lemmas, and lower bounds for GF(2) polynomials and multiparty protocols DIMACS; Spring 2007
17. Institute for Advanced Study, Princeton, NJ  
Norms, XOR lemmas, and lower bounds for GF(2) polynomials and multiparty protocols IAS; Spring 2007
16. Toyota Technical Institute at Chicago, Chicago, IL  
Derandomization: New results and applications TTI; Spring 2006
15. La Sapienza University, Rome, Italy  
Derandomization: New results and applications La Sapienza; Spring 2006
14. Harvard University, Cambridge, MA  
On approximate majority and probabilistic time Harvard; Spring 2006

13. American Math. Society meeting on randomness in computation, Lincoln, NE      AMS; Fall 2005  
Pseudorandom bits for low complexity classes: new results and applications
12. Center for Math. and Comp. Science, Amsterdam, the Netherlands      CWI; Summer 2005  
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates
11. IEEE Conf. on Computational Complexity, San Jose, CA      CCC; Summer 2005  
On constructing parallel pseudorandom generators from one-way functions
10. IEEE Conf. on Computational Complexity, San Jose, CA      CCC; Summer 2005  
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates
9. Berkeley University, Berkeley, CA,      Berkeley; Spring 2005  
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates
8. Microsoft Research, Mountain View, CA      Microsoft; Spring 2005  
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates
7. Harvard University, Cambridge, MA      Harvard; Spring 2004  
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates
6. Institute for Advanced Study, Princeton, NJ      IAS; Fall 2004  
Using nondeterminism to amplify hardness
5. ACM Symp. on Theory of Computing, Chicago, IL      STOC; Summer 2004  
Using nondeterminism to amplify hardness
4. Radcliffe Inst. for Adv. Study, Cambridge, MA      Radcliffe; Fall 2003  
Using nondeterminism to amplify hardness
3. IEEE Conf. on Computational Complexity, Aarhus, Denmark      CCC; Summer 2003  
The complexity of constructing pseudorandom generators from hard functions
2. Harvard University, Cambridge, MA      Harvard; Spring 2003  
The complexity of constructing pseudorandom generators from hard functions
1. Harvard University, Cambridge, MA      Harvard; Fall 2001  
E-unifiability via narrowing

## VIDEO GAMES

**ARORA**, web game to study the perception of randomness      2009 – present  
**Black Viper**, distributed by Neo Software Produktions GmbH, Vienna, Austria      1994 – 1996  
**Nathan Never**, distributed by Softel Ltd., Rome, Italy      1992

## EXTERNAL GRANTS

NSF CCF-1813930, PI, <i>AF: Small: Research in Complexity Theory</i> \$499,896	6/1/2018-5/31/2021
REU supplements \$8,000	2019
NSF CCF-1319206, PI, <i>Research in complexity theory and related areas</i> \$493,824	9/1/2013-8/31/2017
MIT, PI, <i>Experiment on the perception of randomness</i> \$31,100	1/2013–1/2014
NSF CAREER Award, 0845003, PI, <i>Pseudorandom generators</i> \$452,009	2/2009–1/2014
REU supplements \$16,000	2010, 2011

## INTERNAL GRANTS

Co-op funding award \$6,000	7/1/2020-12/31/2020
--------------------------------	---------------------

## TEACHING: COURSES

Sp=Spring, Fa=Fall, Su=Summer

<i>Online MS Algorithms, newly developed course</i>	Su'20, Su'19, Sp'19
<i>Special topics in complexity theory, newly developed course</i>	Fa '17
<i>PhD Gems of Theoretical Computer Science, newly developed course</i>	Sp '09
<i>Undergraduate Theory of Computation</i>	Fa'16, Sp'14, Fa'12, Sp'12, Fa'11, Fa'10
<i>MS Algorithms</i>	Fa '20, Su '20, Su '19, Sp '19 x 2, Sp '17 x 2, Sp 2016, Su 2015, Fa '12
<i>PhD (core) Theory of Computation</i>	Sp '14, Sp '13, Sp '12, Sp '11, Sp '10
<i>PhD (core) Advanced Algorithms</i>	Fa '09, Fa '08

<b>Nominated for Excellence in Teaching Award</b>	2013
---	------

## RESEARCH TEAM (INCLUDING STUDENTS)

- Visitor** Elena Grigorescu (Spring 2020)  
Yevgeniy Dodis (Spring and Summer 2013)
- Postdoc** Elad Haramaty (Fall 2014 - Summer 2016 ).  
**First job: Postdoc at Harvard.**  
Chinmoy Dutta (partial mentoring, January 2011 - January 2013).  
**First job: Tweeter Engineering.**
- Ph. D.** Peter Ivanov (Summer 2019 - present)  
Xuanguai Huang (Fall 2017 - present)  
Chin Ho Lee (Fall 2013-Summer 2019)  
**First job: Postdoc at Columbia University.**  
Tanay Mehta (Summer 2016-Summer 2017)  
Hamid Jahanjou (Fall 2011-Summer 2014), then worked with Rajmohan Rajaraman  
Zahra Jafargholi (Fall 2011-Summer 2013), then worked with Daniel Wichs  
**First job: Postdoc at Aarhus University.**  
Eric Miles (Fall 2008-Spring 2014).  
**First job: postdoc at UCLA.**
- M. S.** Dolphy Fernandes (Summer 2009) ARORA project
- B. S.** Liam Pavlovic (Summer 2020 – Fall 2020)  
Daniel Kreymer (2009-2012) Block-symmetric polynomials project.  
**First job: Amazon.**  
Sky O’Mara (Summer 2009) Block-symmetric polynomials project

## SERVICE TO THE INSTITUTION

<b>Faculty search committee</b> , joint Computer Science and Game Design position	2010 – 2011
<b>Faculty search committee</b> , joint Computer Science and Mathematics position	2009 – 2010
<b>Seminar organizer</b> , Northeastern University theory seminar	2008 – 2015
<b>Merit committee</b>	2012 – 2013
<b>Sabbatical committee</b>	2012 – 2013
<b>Ph.D. admission committee</b>	2008 – 2009, 2016 – 2017, 2018–2019, 2019–2020
<b>M.S. committee</b>	2010 (?) – 2013
<b>M.S. curriculum committee</b>	2019 – 2020

## SERVICE TO THE DISCIPLINE

<b>Associate editor</b>	
SIAM Journal on Computing	SICOMP 2019 – present
ACM Transactions on Computation Theory	TOCT 2015 – present



### **Program committee**

Conference on Computational Complexity	CCC 2021
58th Annual IEEE Symposium on Foundations of Computer Science	FOCS 2017
ACM-SIAM Symposium on Discrete Algorithms	SODA 2014
28th IEEE Conference on Computational Complexity	CCC 2013
16th Int. Workshop on Randomization and Computation	RANDOM 2012
25th IEEE Conference on Computational Complexity	CCC 2010
13th Int. Workshop on Randomization and Computation	RANDOM 2009
49th IEEE Symp. on Foundations of Computer Science	FOCS 2008
11th Int. Workshop on Randomization and Computation	RANDOM 2007

### **Grant reviewing**

National Science Foundation (NSF) panelist	2008, 2009, 2011, 2014, 2015, 2016, 2019, 2020
Israel Science Foundation	2009, 2010
American University of Beirut	2012

**Ph.D. committees**, Laura Poplawski (Northeastern), Joshua Brody (Dartmouth) 2008 – 2009

**Local co-organizer**, 25th IEEE Conference on Computational Complexity CCC 2010

**Scientific board**, Electronic Colloquium on Computational Complexity 2009 – present

**Contribution to popular-science book**, *The Evolution of Technical Analysis*, Wiley 2010

**Paper refereeing**, (J. of ACM, SIAM J. on Computing, STOC, FOCS, ...)