

EMANUELE VIOLA

May 1, 2008

Columbia University, 457 Computer Science Building, 1214 Amsterdam Av., New York, NY
Web: www.cs.columbia.edu/~viola Email: viola@cs.columbia.edu Phone: (646) 301-8470

RESEARCH INTERESTS

Computational complexity theory, pseudorandomness, cryptography

RESEARCH POSITIONS

Columbia University, New York, NY Fall 2007 – present

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

Best Paper Award, IEEE Conf. on Computational Complexity 2008

For the paper *The sum of d small-bias generators fools polynomials of degree d*

SIAM Student Paper Prize 2006

For the paper *Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates*

PROFESSIONAL SERVICE

Program committee

IEEE Symp. on Foundations of Computer Science (FOCS) Fall 2008

Int. Workshop on Randomization and Computation (RANDOM) Summer 2007

Journal refereeing

SIAM J. on Computing (SICOMP) Computational Complexity (CC)

J. of Computer and System Sciences (JCSS) Theoretical Computer Science (TCS)

TEACHING ASSISTANTSHIPS

Harvard University, Cambridge, MA

Computational Complexity Fall 2002 and Spring 2006

Pseudorandomness Spring 2002

OTHER RELEVANT EXPERIENCE

Video game developer

Black Viper, distributed by Neo Software Produktions GmbH, Vienna, Austria 1994 – 1996

Nathan Never, distributed by Softel Ltd., Rome, Italy 1992

Software engineer

Developed database applications for Sogetel Software House, Rome, Italy 1995 – 1996

PAPERS

- [14] Improved separations between nondeterministic and randomized multiparty communication
With Matei David and Toniann Pitassi
Submitted to Int. Workshop on Randomization and Computation 2008
- [13] The sum of d small-bias generators fools polynomials of degree d
To appear in IEEE Conf. on Computational Complexity, **Best Paper Award** CCC 2008
- [12] Hardness amplification proofs require majority
With Ronen Shaltiel
To appear in ACM Symp. on Theory of Computing STOC 2008
- [11] One-way multi-party communication lower bound for pointer jumping with applications
With Avi Wigderson
Submitted to *Combinatorica*; invited to **FOCS special issue**
In IEEE Symp. on Foundations of Computer Science FOCS 2007
- [10] Pseudorandom bits for polynomials
With Andrej Bogdanov
Submitted to *SIAM J. on Computing*; invited to **FOCS special issue**
In IEEE Symp. on Foundations of Computer Science FOCS 2007
- [9] Norms, XOR lemmas, and lower bounds for $GF(2)$ polynomials and multiparty protocols
With Avi Wigderson
To appear in *Theory of Computing*
In IEEE Conf. on Computational Complexity CCC 2007
- [8] On approximate majority and probabilistic time
To appear in *J. of Computational Complexity*
In IEEE Conf. on Computational Complexity CCC 2007
- [7] Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates
SIAM J. on Computing, 36(5):1387-1403, 2007, **SIAM Student Paper Prize** 2006
In IEEE Conf. on Computational Complexity CCC 2005
- [6] On constructing parallel pseudorandom generators from one-way functions
In IEEE Conf. on Computational Complexity CCC 2005
- [5] Constant-depth circuits for arithmetic in finite fields of characteristic two
With Alexander Healy
In Int. Symp. on Theoretical Aspects of Computer Science STACS 2006
- [4] Fooling parity tests with parity gates
With Dan Gutfreund
In Int. Workshop on Randomization and Computation RANDOM 2004
- [3] Using nondeterminism to amplify hardness
With Alexander Healy and Salil Vadhan
SIAM J. on Computing, 35(4):903-931, 2006, **STOC special issue**
In ACM Symp. on Theory of Computing STOC 2004

[2] The complexity of constructing pseudorandom generators from hard functions
J. of Computational Complexity, 13(3-4):147–188, 2004
In IEEE Conf. on Computational Complexity CCC 2003

[1] E-unifiability via narrowing
In Italian Conf. on Theoretical Computer Science ICTCS 2001

TECHNICAL REPORTS

[2] Selected results in additive combinatorics: An exposition
Electronic Colloquium on Computational Complexity, Report 07-103 ECCC 2007

[1] New correlation bounds for GF(2) polynomials using Gowers uniformity
Electronic Colloquium on Computational Complexity, Report 06-097 ECCC 2006

INVITED TALKS

[5] **Cornell University workshop** on discrete harmonic analysis, Ithaca, NY
Polynomials Spring 2008

[4] **IBM Research/NYU/Columbia Theory Day**, New York, NY
Polynomials Fall 2007

[3] **Oberwolfach meeting** on complexity theory, Oberwolfach, Germany
One-way multi-party communication lower bound for pointer jumping Summer 2007

[2] **Dagstuhl seminar** on the complexity of boolean functions, Wadern, Germany
On approximate majority and probabilistic time Spring 2007

[1] **American Math. Society meeting** on randomness in computation, Lincoln, NE
Pseudorandom bits for low complexity classes: new results and applications Fall 2005

CONFERENCE AND SEMINAR TALKS

[31] Columbia University, New York, NY Columbia; Spring 2008
Hardness amplification proofs require majority

[30] Northeastern University, Boston, MA Northeastern; Spring 2008
Pseudorandomness

[29] University of Illinois at Chicago, Chicago, IL UIC; Spring 2008
Polynomials

[28] The University of Chicago, Chicago, IL UChicago; Spring 2008
Lower bounds

[27] Institute for Advanced Study, Princeton, NJ IAS; Spring 2008
Hardness amplification proofs require majority

[26] IEEE Symp. on Foundations of Computer Science, Providence, RI FOCS; Fall 2007
One-way multi-party communication lower bound for pointer jumping with applications

[25] IEEE Symp. on Foundations of Computer Science, Providence, RI FOCS; Fall 2007
Pseudorandom bits for polynomials

- [24] Columbia University, New York, NY
Selected results in additive combinatorics Columbia; Fall 2007
- [23] IEEE Conf. on Computational Complexity, San Diego, CA
Norms, XOR lemmas, and lower bounds for GF(2) polynomials and multiparty protocols CCC; Summer 2007
- [22] IEEE Conf. on Computational Complexity, San Diego, CA
On approximate majority and probabilistic time CCC; Summer 2007
- [21] New York University, New York, NY
Pseudorandomness: New results and applications NYU; Spring 2007
- [20] Institute for Advanced Study, Princeton, NJ
One-way multi-party communication lower bound for pointer jumping with applications IAS; Spring 2007
- [19] IBM Watson Research Center, Hawthorne, NY
Pseudorandomness: New results and applications IBM; Spring 2007
- [18] Institute for Advanced Study, Princeton, NJ
On approximate majority and probabilistic time IAS; Spring 2007
- [17] 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
- [16] Institute for Advanced Study, Princeton, NJ
Norms, XOR lemmas, and lower bounds for GF(2) polynomials and multiparty protocols IAS; Spring 2007
- [15] Toyota Technical Institute at Chicago, Chicago, IL
Derandomization: New results and applications TTI; Spring 2006
- [14] La Sapienza University, Rome, Italy
Derandomization: New results and applications La Sapienza; Spring 2006
- [13] Harvard University, Cambridge, MA
On approximate majority and probabilistic time Harvard; Spring 2006
- [12] Center for Math. and Comp. Science, Amsterdam, the Netherlands
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates CWI; Summer 2005
- [11] IEEE Conf. on Computational Complexity, San Jose, CA
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates CCC; Summer 2005
- [10] Berkeley University, Berkeley, CA,
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates Berkeley; Spring 2005
- [9] Microsoft Research, Mountain View, CA
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates Microsoft; Spring 2005
- [8] Harvard University, Cambridge, MA
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates Harvard; Spring 2004
- [7] IEEE Conf. on Computational Complexity, San Jose, CA
On constructing parallel pseudorandom generators from one-way functions CCC; Summer 2005
- [6] Institute for Advanced Study, Princeton, NJ
Using nondeterminism to amplify hardness IAS; Fall 2004

- [5] ACM Symp. on Theory of Computing, Chicago, IL
Using nondeterminism to amplify hardness STOC; Summer 2004
- [4] Radcliffe Inst. for Adv. Study, Cambridge, MA
Using nondeterminism to amplify hardness Radcliffe; Fall 2003
- [3] IEEE Conf. on Computational Complexity, Aarhus, Denmark
The complexity of constructing pseudorandom generators from hard functions CCC; Summer 2003
- [2] Harvard University, Cambridge, MA
The complexity of constructing pseudorandom generators from hard functions Harvard; Spring 2003
- [1] Harvard University, Cambridge, MA
E-unifiability via narrowing Harvard; Fall 2001