Boaz Barak – Curriculum Vitae

January 2020

1 Personal Details

Name:	Boaz Barak
Position:	Gordon McKay Professor of Computer Science, John A. Paulson School of Engineering and Applied Sciences, Harvard)
Email:	b@boazbarak.org
Home Page:	http://www.boazbarak.org
Administrator:	Evelyn Santana-Nola santana@seas.harvard.edu 617-496-6257
Work address:	Boaz Barak, Science and Engineering Complex Loading Dock, 150 Western Avenue office 3.309, Allston, MA 02134
Fax:	(617) 496-6404
Year of birth:	1974
Citizenship:	U.S., Israel

2 Academic positions

- **Harvard University.** Gordon McKay Professor of Computer Science in the Harvard John A. Paulson School of Engineering and Applied Sciences.
- **Microsoft Research.** Principal researcher in New England research lab June 2010–January 2016. (Promoted from senior researcher in March 2015.)
- **Princeton University.** Assistant professor of Computer Science July 2005– February 2010. Associate professor (with tenure) February 2010 - June 2011.
- **Institute for Advanced Study.** Member in the school of Mathematics, September 2003–July 2005.

3 Education

- Ph.D Computer Science, 2004. Weizmann Institute of Science, Rehovot, Israel. Title of thesis: Non-Black-Box Techniques in Cryptography. Advisor: Prof. Oded Goldreich.
- B.Sc (summa cum laude) Mathematics and Computer Science, 1999. Tel-Aviv University, Tel-Aviv, Israel.

4 Awards and Honors

- Simons investigator, 2017.
- 2016 SIAM Outstanding Paper Prize for the paper How to "Compress Interactive Communication" with Mark Braverman, Xi Chen, and Anup Rao.

- Selected for Foreign Policy magazine's list of 100 leading global thinkers for 2014.
- Invited speaker, session on "Mathematical Aspects of Computer Science", International Congress of Mathematicians, August 2014.
- Co-winner of FOCS 2010 best paper award for the paper "Subexponential Algorithms for Unique Games and Related Problems" with Sanjeev Arora and David Steurer.
- Alfred Rheinstein '11 junior faculty award, Princeton, April 2008.
- Packard foundation fellowship, November 2007.
- Sloan foundations fellowship, September 2007.
- ACM (Association for Computing Machinery) Dissertation award for best doctoral dissertation in computer science and engineering, 2004.
- Co-winner of FOCS 2002 conference best paper award. Award was given for the paper "Constant-Round Coin-Tossing With a Man in the Middle or Realizing the Shared Random String Model"
- Co-winner of FOCS 2002 Machtey best student paper award for the same paper.
- John F. Kennedy Ph.D distinction prize, Weizmann Institute of Science, June 2003.
- Clore foundation scholarship for graduate students in the sciences. September 2002 - August 2003.
- VATAT[1] scholarship for graduate students in the high-tech area. October 2001 – August 2003.
- Co-winner of FOCS 2001 conference Machtey award for best student paper. Award was given for the paper "How To Go Beyond the Black-Box Simulation Barrier"
- Checkpoint scholarship for graduate students in computer science. January 2001 – September 2002.
- Knesset (Israeli Parliament) Education Committee's outstanding undergraduate students list, academic year 1996-7.
- Tel-Aviv University Rector's list (top 0.1%), academic year 1996-7.
- Member of the special program for outstanding students in Tel-Aviv University, years 1997-9.
- Tel-Aviv University, Faculty of Exact Sciences Dean's list in the years 1996-7,1997-8,1998-9.

[1] Committee for planning and budget in the Israeli council for higher education.

5 Research Grants

(Not including awards listed above.)

- Oracle labs gift for “”Understanding Deep Learning”.
- NSF large collaborative grant - “AF: Large: Collaborative Research: Algebraic Proof Systems, Convexity, and Algorithms”, 2016. Co-PI’s: Jonathan Kelner, Ankur Moitra and Pablo Parrilo.
- NSF small grant “TWC: Small: Complexity Assumptions for Cryptographic Schemes” , 2016.
- External collaborator on NSF Frontier grant— Center for Encrypted Functionalities, 2014.
- Co-PI on NSF Expeditions grant for Center on Computational Intractability, September 2008.
- NSF grant on “Foundations of Complexity Theory” (co-PI: Moses Charikar, previous PI: Andrew Yao). June 2003 – Jan 2007.
- NSF grant on “Computational Complexity of Interactive Computation” (co-PI: Moses Charikar, pervious PI: Andrew Yao). September 2004 – August 2009.
- NSF grant on “Cryptographic Protocols for Next-Generation Security Applications”. September 2006 – August 2009.
- USA-Israel Binational Science Foundation (BSF). Grant on “Explicit Constructions of Pseudo-Random Objects” (co-PIs: Ran Raz, Avi Wigderson), October 2005 – September 2009.

6 Extended visits

- Weizmann Institute of Science. Weston visiting professor, Spring 2017.
- IBM T.J. Watson Research Center, New York, NY. Visiting student, Summer 2003.
- Institute for Advanced Study, Princeton, NJ. Visiting student, Summer 2001.

7 Research advising.

- Current students: Zhixian Lei, Yueqi Sheng, Chi-Ning Chou, Prayaag Venkat, Preetum Nakkiran (co-advised with Madhu Sudan), Beatrice Nash (co-advised with Mikhail Lukin).
- Former students: Moritz Hardt, David Xiao (co-advised with Avi Wigderson), Sharon Goldberg (co-advised with Jennifer Rexford), Mohammad Mahmoody.
- Former postdocs: Guy Rothblum, Benny Applebaum, Thomas Holenstein, Tselil Schramm.
- Former interns: Moritz Hardt, Jonah Sherman, Yuan Zhou, Li-Yang Tan, Aaron Potechin, Aaron Sidford (co advised with Sham Kakade), Pravesh Kothari, Samuel Hopkins.

- Thesis committee member: Anup Rao (University of Texas, Austin), Manoj Parbhakaran (Princeton), Iannis Tourlakis (Princeton), Adriana Karagiozova (Princeton), Satyen Kale (Princeton), Konstantyn Makarychev (Princeton), Yury Makarychev (Princeton), Eden Chalmatac (Princeton), Seshadri Comandur (Princeton), Wolfgang Mulzer (Princeton), Nadia Heninger (Princeton), Pravesh Kothari (UT Austin), David Witmer (CMU) ,Thomas Steinke (Harvard), Mark Bun (Harvard), Jack Murtaugh (Harvard), Vasileios Nakos (Harvard), Ben Edelman (Harvard).

- Undergraduate research advisor: Jon Ullman (2007/8), Srdjan Krstic (2008/9), Aaron Potechin (2008/9), Mark Stefanski (2008/9), Christina Ilvento (2009/10), Nathan Manohar (2016), Limor Gultchin (2016), Greg Yang (2016), Hikari Sorensen (2020), Jess Huang (2020).

8 Teaching and advising

- **Harvard**. *CS 229br: Advanced topics in the theory of machine learning*, Spring 2021. *CS 182: Artificial Intelligence*, Fall 2020 (co-taught with Milind Tambe). *CS 121: Introduction to Theoretical Computer Science*, Fall 2017, Fall 2018, Fall 2019. *CS 127/227: Cryptography*, Spring 2016, Spring 2018, Spring 2020.*CS 229r / MIT 6.S898:Proofs, beliefs and algorithms through the lens of Sum of Squares*, Fall 2016 (joint Harvard and MIT course). Also serving a first-year and concentration advisor.

- **MIT**. Co-teacher in *MIT 6.889 BU CAS CS 937: New Developments in Cryptography*, Spring 2011. *Sum of squares upper bounds, lower bounds, and open questions*, seminar series, Fall 2014.

- **UCSD winter course**. Mini course (co taught with David Steurer) on the "Sum of Squares Algorithm", January 2017.

- **Addis coder course**. Coding and algorithms for talented high school students from around Ethiopia. Addis Ababa, August 2016, August 2019.

- **Swedish Summer School in Computer Science**. *Sum of Squares*, Summer 2014.

- **Princeton University**. *COS 433: Cryptography*, Fall 2005, Fall 2007, Spring 2010. *COS 522: Complexity*, Spring 2006, Spring 2007, Spring 2009. *COS 598D:Mathematical Methods in Computer Science*, Spring 2008. BSE Freshman advisor 2007/8 and 2008/9, advisor for BSE CS majors class of 2012.

9 Professional Services

Program committee chair: FOCS 2014.

Program committee member: **(1)** ACM STOC (Symposium on the Theory of Computing) conference 2004. **(2)** TCC (Theory of Cryptography Conference) 2005. **(3)** IACR CRYPTO conference 2005 **(4)** RANDOM 2005 conference **(5)** IACR CRYPTO conference 2006 **(6)** TCC (Theory of Cryptography Conference) 2008. **(7)** CSR (Computer Science in Russia) 2008, **(8)** IACR CRYPTO conference 2008 **(9)** FOCS 2009 conference **(10)** TCC 2011 **(11)** CCC

(Conference on Computational Complexity) 2012 **(12)** STOC 2013 (executive committee) **(13)** TCC 2013 **(14)** Highlights of Algorithms 2016 **(15)** STOC 2020 **(16)** COLT 2021.

Organizing committees **(1)** Workshop on Foundations of secure multi-party computation, zero-knowledge and its applications, Institute for Pure and Applied Mathematics, UCLA, November 2006. **(2)** Additive combinatorics mini course, Princeton, August 2007 **(3)** Women in Theory workshop, Princeton, June 2008 **(4)** Cryptography and complexity workshop, Princeton/DIMACS, June 2009, **(5)** Women in theory workshop, Princeton, June 2010 **(5)** FOCS 2012 workshop day, **(6)** STOC 2013 workshop day, **(7)** Workshop on "Semidefinite Optimization, Approximation and Applications", Simons institute, September 2014 (chair), **(8)** Workshop "A Celebration of Mathematics and Computer Science" in honor of Avi Wigderson's 60th birthday, October 2016, **(9)** Committee for plenary talk selection, STOC 2017 (chair), **(10)** Special year on combinatorics and computational complexity, Harvard CMSA 2017-8, **(11)** Women in theory workshop, Harvard, June 2018, **(12)** Committee for plenary talk selection, STOC 2018, **(13)** Noncommutative Analysis Workshop, CMSA, Harvard, October 2019, **(14)** Simons institute symposium on new advances in obfuscation, December 2020.

Editor Member of editorial board of the Journal of the ACM and Theory of Computing Journal. Member of scientific board, Electronic Colloquium of Computational Complexity (ECCC). Co editor of special issue for conference on computational complexity 2012.

Other service Member of the Committee for the Advancement of Theoretical Computer Science (CATCS). Trustee and registration chair, computational complexity foundation (2016-2019). Scientific Advisory Board member, Simons Institute for the theory of computing (2018-2021). Board member, AddisCoder Inc.

Patent

U.S. Patent 7,003,677, "Method for operating proactively secured applications on an insecure system" with Amir Herzberg, Dalit Naor and Eldad Shai of IBM Haifa Research Lab. Filed November 1999, granted February 2006.

10 Invited Speaker

- Tutte Colloquium, University of Waterloo, October 2020.
- Keynote, Harvard Science Research Conference (HSRC), October 2020
- CMSA New Technologies in Mathematics, October 2020
- Distinguished Speaker Series, Max Planck Institute for Informatics, October 2020
- Yale Institute for Network Science Distinguished lecturer, November 2020
- Institute for Advanced Study, Princeton, NJ, April 2019.
- Addis Ababa Institute of Technology, Addis Ababa, Ethiopia, August 2019.

- Rabin distinguished lecture, Hebrew University, Jerusalem, Israel, December 2019.
- QIP (Quantum Information Processing) 2018, Delft, Netherlands.
- Workshop on "Beyond Cryptography", Santa Barbara, CA, 2018
- University of Bologna, Bologna, Italy, July 2018
- Workshop on convexity and quantum information, Natal, Brazil, August 2018
- Algorithms and combinatorics seminar, MIT, 2018
- PCP Fest, December 2018, Tel Aviv University
- Oded Goldreich Birthday Celebration, April 2017.
- Open University theory day, Israel, December 2017.
- Harvard CMSA Seminar, November 2016
- University of Texas at Austin theory seminar, October 2016.
- Workshop on Advances in non-convex analysis and optimization, ICML confedrence, New York, June 2016.
- Distinguished speaker, Capital area theory day, Johns Hopkins University, May 2016.
- Northwestern University quarterly theory workshop, May 2016.
- AMS special session on "Pseudorandomness and Its Applications", Joint Mathematics Meetings, Seattle, January 2016.
- FSTTCS conference, Bengalore, India, December 2015.
- Harvard theory of computing colloquium, December 2015.
- Harvard CMSA (Center of Mathematical Sciences and Applications) colloquium, October 2015.
- Cornell Computer Science colloquium, September 2015.
- Session on "Semidefinite Hierarchies for Approximations in Combinatorial Optimization", ISMP 2015, Pittsburgh, August 2015.
- MIT Cryptography and Information Security seminar, September 2014.
- Section on "Mathematical Aspects of Computer Science", International Congress of Mathematicians (ICM), Seoul, August 2014.
- Weizmann distinguished lectures day celebrating the work of Shafi Goldwasser and Silvio Micali, December 2013.
- Walmart Cryptography and Complexity Lecture Series, Weizmann Institute of Science, May 2010.

- Faces of cryptography workshop, CUNY, September 2009.
- First International Computer Science Symposium in Russia, St. Petersburg, June 2006.
- Theory of cryptography conference (TCC), New York, March 2006.

11 Publications

Papers are presented in reverse chronological order. Electronic versions of all papers are available on my home page (`http://www.boazbarak.org/research.html`). Some papers also appear on the Cryptology ePrint, ECCC and arxiv archives.

Textbook.

[1] S. Arora and B. Barak Computational Complexity: A Modern Approach. Cambridge University Press, May 2009.

Papers in refereed conferences.

[61] Y. Bansal, G. Kaplun, and B. Barak. For self-supervised learning, Rationality implies generalization, provably. *ICLR*, abs/2010.08508, 2021.

[60] B. Barak, C. Chou, and X. Gao. Spoofing Linear Cross-Entropy Benchmarking in Shallow Quantum Circuits. *Innovations in Theoretical Computer Science (ITCS)*, abs/2005.02421, 2020.

[59] B. Barak, R. Crubillé, and U. D. Lago. On Higher-Order Cryptography. In A. Czumaj, A. Dawar, and E. Merelli, editors, *47th International Colloquium on Automata, Languages, and Programming, ICALP 2020, July 8-11, 2020, Saarbrücken, Germany (Virtual Conference)*, volume 168 of *LIPIcs*, pages 108:1–108:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

[58] P. Nakkiran, G. Kaplun, Y. Bansal, T. Yang, B. Barak, and I. Sutskever. Deep Double Descent: Where Bigger Models and More Data Hurt. In *8th International Conference on Learning Representations, ICLR 2020, Addis Ababa, Ethiopia, April 26-30, 2020*. OpenReview.net, 2020.

[57] B. Barak, S. B. Hopkins, A. Jain, P. Kothari, and A. Sahai. Sum-of-Squares Meets Program Obfuscation, Revisited. In *EUROCRYPT 2019*, pages 226–250, 2019.

[56] P. Nakkiran, G. Kaplun, D. Kalimeris, T. Yang, B. L. Edelman, F. Zhang, and B. Barak. SGD on Neural Networks Learns Functions of Increasing Complexity. In *NeurIPS 2019 (spotlight)*, volume abs/1905.11604, 2019.

[55] B. Barak, C. Chou, Z. Lei, T. Schramm, and Y. Sheng. (Nearly) Efficient Algorithms for the Graph Matching Problem on Correlated Random Graphs. In *NeurIPS 2019*, 2019.

[54] B. Barak, P. Kothari, and D. Steurer. Small-Set Expansion in Shortcode Graph and the 2-to-2 Conjecture. In *ITCS 2019*, 2019.

[53] B. Barak. The Complexity of Public-Key Cryptography. 2017. Tutorial/survey in honor of Oded Goldreich 60th birthday.

[52] B. Barak, Z. Brakerski, I. Komargodski, and P. Kothari. Limits on Low-Degree Pseudorandom Generators (Or: Sum-of-Squares Meets Program Obfuscation). In *EUROCRYPT*, 2018.

[51] B. Barak, P. Kothari, and D. Steurer. Quantum entanglement, sum of squares, and the log rank conjecture. In *STOC*, 2017.

[50] B. Barak and A. Moitra. Tensor Prediction, Rademacher Complexity and Random 3-XOR. In *COLT*, 2016.

[49] B. Barak, S. Hopkins, J. Kelner, P. Kothari, A. Moitra, and A. Potechin. A nearly tight Sum-of-Squares lower bound for the Planted Clique problem. In *FOCS*, 2016.

[48] B. Barak. Hopes, Fears, and Software Obfuscation. *Communications of the ACM*, 59(3):88–96, 2016.

[47] B. Barak, A. Moitra, R. O'Donnell, P. Raghavendra, O. Regev, D. Steurer, L. Trevisan, A. Vijayaraghavan, D. Witmer, and J. Wright. Beating the random assignment on constraint satisfaction problems of bounded degree. In *RANDOM-APPROX*, 2015.

[46] B. Barak, S. O. Chan, and P. Kothari. Sum of Squares Lower Bounds from Pairwise Independence. In *STOC*, 2015.

[45] B. Barak, J. A. Kelner, and D. Steurer. Dictionary Learning and Tensor Decomposition via the Sum-of-Squares Method. In *STOC*, 2015.

[44] B. Barak, J. A. Kelner, and D. Steurer. Rounding sum-of-squares relaxations. In *STOC*, pages 31–40, 2014.

[43] B. Barak, N. Bitansky, R. Canetti, Y. T. Kalai, O. Paneth, and A. Sahai. Obfuscation for Evasive Functions. In *TCC*, pages 26–51, 2014.

[42] B. Barak, S. Garg, Y. T. Kalai, O. Paneth, and A. Sahai. Protecting Obfuscation against Algebraic Attacks. In *EUROCRYPT*, volume 8441 of *Lecture Notes in Computer Science*, pages 221–238. Springer, 2014.

[41] B. Barak, G. Kindler, and D. Steurer. On the optimality of semidefinite relaxations for average-case and generalized constraint satisfaction. In *ITCS*, pages 197–214. ACM, 2013.

[40] B. Barak, F. G. S. L. Brandão, A. W. Harrow, J. A. Kelner, D. Steurer, and Y. Zhou. Hypercontractivity, sum-of-squares proofs, and their applications. In *STOC*, pages 307–326, 2012.

[39] B. Barak, P. Raghavendra, and D. Steurer. Rounding Semidefinite Programming Hierarchies via Global Correlation. In *FOCS*, pages 472–481, 2011.

[38] B. Barak, Y. Dodis, H. Krawczyk, O. Pereira, K. Pietrzak, F.-X. Standaert, and Y. Yu. Leftover Hash Lemma, Revisited. In *CRYPTO*, 2011.

[37] B. Barak, Z. Dvir, A. Wigderson, and A. Yehudayoff. Rank Bounds for Design Matrices with Applications to Combinatorial Geometry and Locally Correctable Codes. In *STOC*, 2011. Journal version in PNAS '12.

[36] B. Barak, M. Hardt, T. Holenstein, and D. Steurer. Subsampling Mathematical Relaxations and Average-case Complexity. In *SODA*, pages 512–531, 2011.

[35] S. Arora, B. Barak, and D. Steurer. Subexponential Algorithms for Unique Games and Related problems. In *Proc. of FOCS*, pages 563–572, 2010.

[34] B. Barak, I. Haitner, D. Hofheinz, and Y. Ishai. Bounded Key-Dependent Message Security. In *EUROCRYPT*, pages 423–444, 2010.

[33] B. Applebaum, B. Barak, and A. Wigderson. Public-key cryptography from different assumptions. In *STOC*, pages 171–180, 2010.

[32] B. Barak, M. Braverman, X. Chen, and A. Rao. How to compress interactive communication. In *STOC*, pages 67–76, 2010. Journal version in SICOMP 2013.

[31] B. Barak, A. Rao, R. Raz, R. Rosen, and R. Shaltiel. Strong Parallel Repetition Theorem for Free Projection Games. In *APPROX-RANDOM*, pages 352–365, 2009.

[30] B. Barak and M. Mahmoody-Ghidary. Merkle Puzzles are Optimal — an $O(n^2)$-query attack on key exchange from a random oracle. In *Proc. IACR (International Association for Cryptographic Research) CRYPTO '09*, 2009.

[29] B. Barak, M. Hardt, and S. Kale. The Uniform Hardcore Lemma via Approximate Bregman Projections. In *Proceedings of ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2009.

[28] B. Barak, M. Hardt, I. Haviv, A. Rao, O. Regev, and D. Steurer. Rounding Parallel Repetitions of Unique Games. In *Proc. 49th Foundations of Computer Science (FOCS)*. IEEE, 2008.

[27] B. Applebaum, B. Barak, and D. Xiao. On Basing Lower-Bounds for Learning on Worst-Case Assumptions. In *Proc. 49th Foundations of Computer Science (FOCS)*. IEEE, 2008.

[26] B. Barak, S. Goldberg, and D. Xiao. Protocols and Lower Bounds for Failure Localization in the Internet. In *Proceedings of Eurocrypt 2008*, 2008.

[25] S. Goldberg, D. Xiao, E. Tromer, B. Barak, and J. Rexford. Path-Quality Monitoring in the Presence of Adversaries. In *Proceedings of SIGMETRICS 2008*, 2008.

[24] B. Barak and M. Mahmoody-Ghidary. Lower bounds on signatures from symmetric primitives. In *Proc. 48th Foundations of Computer Science (FOCS)*. IEEE, 2007.

[23] B. Barak, K. Chaudhuri, C. Dwork, S. Kale, F. McSherry, and K. Talwar. Privacy, accuracy, and consistency too: a holistic solution to contingency table release. In L. Libkin, editor, *Proceedings of ACM PODS*, pages 273–282. ACM, 2007.

[22] B. Barak, M. Prabhakaran, and A. Sahai. Concurrent Non-Malleable Zero Knowledge. In *Proc. 47th Foundations of Computer Science (FOCS)*. IEEE, 2006.

[21] B. Barak, A. Rao, R. Shaltiel, and A. Wigderson. 2-source dispersers for sub-polynomial entropy and Ramsey graphs beating the Frankl–Wilson construction. In *Proc. 38th Symposium on Theory of Computing (STOC)*, pages 671–680. ACM, 2006. Journal version in Annals of Mathematics, 2012.

[20] B. Barak and A. Sahai. How to Play Almost Any Mental Game Over the Net - Concurrent Composition Using Super-Polynomial Simulation. In *Proc. 46th Foundations of Computer Science (FOCS)*. IEEE, 2005.

[19] B. Barak and S. Halevi. An architecture for robust pseudo-random generation and Applications to /dev/random. In ACM, editor, *Proc. Computing and Communication Security (CCS)*, 2005.

[18] B. Barak, R. Canetti, Y. Lindell, R. Pass, and T. Rabin. Secure Computation Without Authentication. In *Proc. IACR (International Association for Cryptographic Research) CRYPTO '05*, 2005.

[17] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov, and A. Wigderson. Simulating Independence: New Constructions of Condensers, Ramsey Graphs, Dispersers, and Extractors. In *Proc. 37th Symposium on Theory of Computing (STOC)*. ACM, 2005. Journal version in JACM 2010.

[16] B. Barak, R. Canetti, J. B. Nielsen, and R. Pass. Universally Composable Protocols with Relaxed Setup Assumptions. In *Proc. 45th Foundations of Computer Science (FOCS)*. IEEE, 2004.

[15] B. Barak, R. Impagiliazzo, and A. Wigderson. Extracting Randomness from Few Indepenent Sources. In *Proc. 45th Foundations of Computer Science (FOCS)*. IEEE, 2004. Journal version in SICOMP.

[14] B. Barak and R. Pass. On the Possibility of One-Message Weak Zero-Knowledge. In *Proc. 1st Theory of Cryptography Conference (TCC)*, 2004.

[13] B. Barak, Y. Lindell, and S. Vadhan. Lower Bounds for Non-Black-Box Zero Knowledge. In *Proc. 44th Foundations of Computer Science (FOCS)*. IEEE, 2003. Journal version in JCSS.

[12] B. Barak, R. Shaltiel, and E. Tromer. True Random Number Generators Secure in a Changing Environment. In *Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, pages 166–180, 2003. LNCS no. 2779.

[11] B. Barak, R. Shaltiel, and A. Wigderson. Computational Analogues of Entropy. In *Proc. 7th Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM)*, 2003.

[10] B. Barak, S. J. Ong, and S. Vadhan. Derandomization in Cryptography. In *Proc. IACR (International Association for Cryptographic Research) CRYPTO '03*, 2003. Journal version in SICOMP.

[9] B. Barak. A Probabilistic-Time Hierarchy Theorem for "Slightly Non-Uniform" Algorithms. In *Proc. 6th Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM)*, 2002.

[8] B. Barak. Constant-Round Coin-Tossing With a Man in the Middle or Realizing the Shared Random String Model. In *Proc.* 43*rd Foundations of Computer Science (FOCS)*. IEEE, 2002.

[7] B. Barak and Y. Lindell. Strict Polynomial-time in Simulation and Extraction. In *Proc.* 34*th Symposium on Theory of Computing (STOC)*. ACM, 2002. Journal version in SIAM Journal of Computing (SICOMP).

[6] B. Barak and O. Goldreich. Universal Arguments and their Applications. In *Proc. Conference on Computational Complexity (CCC)*. IEEE, 2002. Full version in SIAM Journal on Computing (SICOMP).

[5] B. Barak, O. Goldreich, S. Goldwasser, and Y. Lindell. Resettably-Sound Zero-Knowledge and its Applications. In *Proc.* 42*nd Foundations of Computer Science (FOCS)*. IEEE, 2001.

[4] B. Barak. How to Go Beyond the Black-box Simulation Barrier. In *Proc.* 42*nd Foundations of Computer Science (FOCS)*, pages 106–115. IEEE, 2001.

[3] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, and K. Yang. On the (Im)possibility of Obfuscating Programs. In *Proc. IACR (International Association for Cryptographic Research) CRYPTO '01*, 2001. LNCS No. 2139.

[2] B. Barak, S. Halevi, A. Herzberg, and D. Naor. Clock Synchronization with Faults and Recoveries. In *Proc. 19th ACM Principles of Distributed Computing (PODC)*. ACM, 2000.

[1] B. Barak, A. Herzberg, D. Naor, and E. Shai. The Proactive Security Toolkit and Applications. In *Proc.* 6^{th} *ACM Conference on Computer and Communications Security (CCS)*. ACM, 1999.

Surveys.

[7] B. Barak The complexity of public-key cryptography, In *Tutorials on the Foundations of Cryptography*, Springer, 45–77, 2017.

[6] B. Barak Hopes, fears, and software obfuscation In *Commun. ACM*, 59(3), 88–96, 2016.

[5] B. Barak Hopes, fears, and software obfuscation In *Commun. ACM*, 59(3), 88–96, 2016.

[4] B. Barak A breakthrough in software obfuscation: technical perspective In *Commun. ACM*, 59(5), 112, 2016

[3] B. Barak and S. Steurer, Sum-of-Squares Proofs and the Quest toward Optimal Algorithms In *Proc. of International Congress of Mathematicians (ICM)*, 2014.

[2] B. Barak, Structure vs Combinatorics in Computational Complexity In *Bulletin of the European Association for Theoretical Computer Science*, Logic in Computer Science column, February 2014.

[1] B. Barak, Truth vs. Proof in Computational Complexity In *Bulletin of the European Association for Theoretical Computer Science*, Logic in Computer Science column, October 2012.

Journal papers.

[17] A. Glaser, B. Barak, M. Kütt, S. Philippe. Physical Public Templates for Nuclear Warhead Verification *Science & Global Security*, 28(1):48-59, 2020

[16] B. Barak, S. B. Hopkins, J. A. Kelner, P. K. Kothari, A. Moitra, and A. Potechin. A Nearly Tight Sum-of-Squares Lower Bound for the Planted Clique Problem. *SIAM J. Comput.*, 48(2):687–735, 2019. Special issue for FOCS 2016.

[15] B. Barak, P. Gopalan, J. Håstad, R. Meka, P. Raghavendra, and D. Steurer Making the Long Code Shorter *SIAM J. Comput.*, 44(5): 1287–1324, 2015. Preliminary version in FOCS 2012.

[14] A. Glaser, B. Barak, and R. J. Goldston. A zero-knowledge protocol for nuclear warhead verification. *Nature*, 510:497—-502, 2014.

[13] S. Goldberg, D. Xiao, E. Tromer, B. Barak, and J. Rexford. Path-Quality Monitoring in the Presence of Adversaries: The Secure Sketch Protocols *IEEE/ACM Transactions on Networking*, 23(6): 1729-1741, 2015. Preliminary versions in SIGMETRICS 2008 and EUROCRYPT 2008.

[12] B. Barak, M. Braverman, X. Chen, and A. Rao. How to Compress Interactive Communication. *SIAM J. Comput.*, 42(3):1327–1363, 2013. Special issue for STOC 2010.

[11] B. Barak, A. Rao, R. Shaltiel, and A. Wigderson. 2-source dispersers for no (1) entropy, and Ramsey graphs beating the Frankl-Wilson construction. *Annals of Mathematics*, 176(3):1483–1543, 2012. Preliminary version in STOC '06.

[10] B. Barak, Z. Dvir, A. Wigderson, and A. Yehudayoff. Fractional Sylvester–Gallai theorems. *Proceedings of the National Academy of Sciences*, 2012. Journal version of STOC '11 paper "Rank Bounds for Design Matrices with Applications to Combinatorial Geometry and Locally Correctable Codes".

[9] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, and K. Yang. On the (Im)possibility of Obfuscating Programs. *J. ACM*, 59(2), 2012. Preliminary version appeared in CRYPTO 2001.

[8] B. Barak, R. Canetti, Y. Lindell, R. Pass, and T. Rabin. Secure Computation Without Authentication *J. Cryptology*, 24(4):720–760, 2011 Preliminary version appeared in CRYPTO 2005.

[7] S. Arora, B. Barak, M. Brunnermeier, and R. Ge. Computational complexity and information asymmetry in financial products. *Commun. ACM* , 54(5):101–107, 2011.

[6] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov and A. Wigderson Simulating independence: New constructions of condensers, ramsey graphs, dispersers, and extractors. *Jorunal of the ACM*, 57(4): (2010) Preliminary version appeared in STOC 2005.

[5] B. Barak and O. Goldreich Universal Arguments and their Applications *SIAM Journal on Computing*, 38(5):1661–1694, 2008. Preliminary version appeared in CCC 2002.

[4] B. Barak, S.J. Ong, and S. Vadhan Derandomization in Cryptography. *SIAM Journal on Computing*, 37(2):380–400, 2007. Preliminary version appeared in CRYPTO 2003.

[3] B. Barak, R. Impagliazzo, and A. Wigderson. Extracting Randomness Using Few Independent Sources. *SIAM Journal on Computing*, 36(4):1095–1118, 2006. Special issue on randomness and complexity. Preliminary version appeared in FOCS 2004.

[2] B. Barak, Y. Lindell, and S. Vadhan. Lower bounds for non-black-box zero knowledge. *J. Comput. Syst. Sci*, 72(2):321–391, 2006. Special Issue for FOCS' 03 conference.

[1] B. Barak and Y. Lindell. Strict polynomial-time in simulation and extraction. *SIAM J. Comput.*, 33(4):783–818 (electronic), 2004. Preliminary version appeared in STOC 2002.

Unrefereed conference papers

[3] S. Philippe, B. Barak, and A. Glaser Designing Protocols for Nuclear Warhead Verification In *56th Annual INMM Meeting*. Institute of Nucclear Materials Management, 2015.

[2] A. Glaser, B. Barak, and R. J. Goldston. Toward a Secure Inspection System for Nuclear Warhead Verification Without Information Barrier. In *54th Annual INMM meeting*. Institute of Nuclear Materials Management, 2013.

[1] A. Glaser, B. Barak, and R. J. Goldston, A New Approach to Nuclear Warhead Verification Using a Zero-Knowledge Protocol In *53rd Annual INMM meeting*, Institute of Nuclear Materials Management, 2012.