Boaz Barak – Curriculum Vitae

April 2025

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:	Kristin Maple kmaple@seas.harvard.edu (617) 495-0581
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

- Chosen as Associate Faculty member of Harvard's Kempner Institute for the Study of Natural and Artificial Intelligence
- Fellow of the ACM, 2022

- 2021 IEEE FOCS "Test of Time" Award (awarded in February 2022) for the paper "How to Go Beyond the Black-Box Simulation Barrier" (FOCS 2001)
- Outstanding Paper (Runner-Up) at NeurIPS 2023:"Scaling Data-Constrained Language Models."
- 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.

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

- 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.

5 Research Grants

(Not including awards listed above.)

- Oracle labs gift for ""Understanding Deep Learning".
-
- NSF collaborative grant - "SLES: A Theoretical Lens on Generative AI Safety: Near and Long Term", 2023. Co-PI's: Sitan Chen, Sham Kakade.
- NSF collaborative grant - " Theory of Learned Representations in Artificial and Natural Neural Networks", 2022. Co-PIs: Demba Ba, Lucas Janson, Cengiz Pehlevan.
- DOE collaboarive grant - "Machine learning for accelerated understanding of dynamic cataly", 2021. Co-PIs: Boris Kozinsky et al
- DARPA collaborative grant - "Optimization with Noisy Intermediate-Scale Quantum devices", 2020. Co-PIs: Mikhail Lukin et al.
- 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

- OpenAI. Member of Technical Staff. Since January 2024.
- 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 Teaching and advising

- **Harvard**. *CS 229br: Advanced topics in the theory of machine learning*, Spring 2021, Spring 2023. *CS 182: Artificial Intelligence*, Fall 2020 (co-taught with Milind Tambe). *CS 121: Introduction to Theoretical Computer Science*, Fall 2017, Fall 2018, Fall 2019, Fall 2022, Fall 2023. *CS 127/227: Cryptography*, Spring 2016, Spring 2018, Spring 2020, Fall 20211.*CS 229r / MIT 6.S898:Proofs, beliefs and algorithms through the lens of Sum of Squares*, Fall 2016 (joint Harvard and MIT course). Also served as 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.

8 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, **(15)** New horizons summer school in TCS, 2021, **(16)** Simons special year on LLMs, 2024-5.

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). Scientific advisory board member, Quanta Magazine. Board member, AddisCoder Inc.

9 Invited Speaker

(Not fully updated)

- Simons Institute workshop, February 2025.
- Keynote, Algorithmic Learning Theory conference, Milan, Italy, February 2025.
- Technion Colloquium, January 2023
- OpenAI workshop on AI Alignment, February 2023
- TTIC Seminar, October 2023
- Harvard CMSA seminar, October 2023
- Samsung symposium on deep learning, Seoul, Korea, August 2023.
- Summer course on deep learning, Seoul University, Korea, August, 2023
- Brookings Institute panel on AI, November, 2023
- Workshop on AI alignment, December 2023
- Probabilitas Seminar, Harvard Statistics Department, March 2022

- Exploring and Exploiting High-dimensional Phenomena in Statistical Learning and Inference, Radcliffe workshop, June 2022
- New Directions in Theoretical Machine Learning, Germany, September 2022
- Summer course in Statistical Physics and Machine Learning, Les Houches, France, August 2022
- Boston Tech Hub FWG Session 2 on Post-Quantum Cryptography, October 2022
- Harvard-Radcliffe Society of Physics Students and Harvard Computer Society Quantum Academy workshop, November 2022
- Hebrew University Colloquium, December 2022
- Information Security Group, Royal Holloway University of London, January 2021.
- Understanding deep learning series, ICMC, Sao Paulo, Brazil, April 2021
- Distinguished talk, Max Planck Institute, July 2021
- 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.

10 Publications

Papers are presented in reverse chronological order. Electronic versions of all papers are available on my home page (`http://www.boazbarak.org`). Many papers appear on the arXic or other archives.

[1] W. Zaremba, E. Nitishinskaya, B. Barak, S. Lin, S. Toyer, Y. Yu, R. Dias, E. Wallace, K. Xiao, J. Heidecke, and A. Glaese. Trading Inference-Time Compute for Adversarial Robustness, 2025.

[2] M. Y. Guan, M. Joglekar, E. Wallace, S. Jain, B. Barak, A. Helyar, R. Dias, A. Vallone, H. Ren, J. Wei, H. W. Chung, S. Toyer, J. Heidecke, A. Beutel, and A. Glaese. Deliberative Alignment: Reasoning Enables Safer Language Models, 2025.

[3] G. Ahdritz, T. Qin, N. Vyas, B. Barak, and B. L. Edelman. Distinguishing the Knowable from the Unknowable with Language Models. *ICML 2024*, 2024.

[4] J. Tobisch, S. Philippe, B. Barak, G. Kaplun, C. Zenger, A. Glaser, C. Paar, and U. Rührmair. Remote inspection of adversary-controlled environments. *Nature communications*, 14(1):6566, 2023.

[5] B. Barak, Y. Kalai, R. Raz, S. Vadhan, and N. K. Vishnoi. On the works of Avi Wigderson. 2023. To appear in the Abel Prize book series, Springer.

[6] H. Zhang, B. L. Edelman, D. Francati, D. Venturi, G. Ateniese, and B. Barak. Watermarks in the Sand: Impossibility of Strong Watermarking for Large Language Models. *ICML 2024*, abs/2311.04378, 2024.

[7] Y. Sheng, M. Nitzan, and B. Barak. Robust reconstruction of single cell RNA-seq data with iterative gene weight updates. In *Thirty-first Conference on Intelligent Systems for Molecular Biology*, 2023.

[8] N. Vyas, D. Morwani, R. Zhao, G. Kaplun, S. M. Kakade, and B. Barak. Beyond Implicit Bias: The Insignificance of SGD Noise in Online Learning. In *ICML 2024*, 2023.

[9] N. Muennighoff, A. M. Rush, B. Barak, T. L. Scao, A. Piktus, N. Tazi, S. Pyysalo, T. Wolf, and C. Raffel. Scaling Data-Constrained Language Models. In *Thirty-seventh Conference on Neural Information Processing Systems*, 2023. Outstanding Main Track Paper award, Runner-Up.

[10] N. Vyas, S. M. Kakade, and B. Barak. On Provable Copyright Protection for Generative Models. In *International Conference on Machine Learning, ICML 2023, 23-29 July 2023, Honolulu, Hawaii, USA*, volume 202 of *Proceedings of Machine Learning Research*, pages 35277–35299. PMLR, 2023.

[11] D. Chiang, A. M. Rush, and B. Barak. Named Tensor Notation. *Transactions on Machine learning Research*, 2023.

[12] S. Ebadi, A. Keesling, M. Cain, T. T. Wang, H. Levine, D. Bluvstein, G. Semeghini, A. Omran, J.-G. Liu, R. Samajdar, X.-Z. Luo, B. Nash, X. Gao, B. Barak, E. Farhi, S. Sachdev, N. Gemelke, L. Zhou, S. Choi, H. Pichler, S.-T. Wang, M. Greiner, V. Vuletić, and M. D. Lukin. Quantum optimization of maximum independent set using Rydberg atom arrays. *Science*, 376(6598):1209–1215, 2022.

[13] B. Barak and A. Moitra. Noisy tensor completion via the sum-of-squares hierarchy. *Math. Program.*, 193(2):513–548, 2022. Preliminary version in COLT 2016.

[14] G. Kaplun, N. Ghosh, S. Garg, B. Barak, and P. Nakkiran. Deconstructing Distributions: A Pointwise Framework of Learning. *ICLR*, abs/2202.09931, 2023.

[15] B. Barak, B. L. Edelman, S. Goel, S. M. Kakade, E. Malach, and C. Zhang. Hidden Progress in Deep Learning: SGD Learns Parities Near the Computational Limit. *NeurIPS*, 2022.

[16] B. Barak and K. Marwaha. Classical algorithms and quantum limitations for maximum cut on high-girth graphs. In *ITCS*, volume 215 of *LIPIcs*, pages 14:1–14:21, 2022. Also presented as poster in QIP 2022.

[17] Y. Bansal, P. Nakkiran, and B. Barak. Revisiting Model Stitching to Compare Neural Representations. In *NeurIPS*, 2021.

[18] X. Gao, M. Kalinowski, C. Chou, M. D. Lukin, B. Barak, and S. Choi. Limitations of Linear Cross-Entropy as a Measure for Quantum Advantage. *PRX Quantum*, 5(1):010334, 2024.

[19] M. Bafna, B. Barak, P. Kothari, T. Schramm, and D. Steurer. Playing Unique Games on Certified Small-Set Expanders. *STOC*, abs/2006.09969, 2021.

[20] B. Barak, C. Chou, and X. Gao. Spoofing Linear Cross-Entropy Benchmarking in Shallow Quantum Circuits. In J. R. Lee, editor, *12th Innovations in Theoretical Computer Science Conference, ITCS 2021, January 6-8, 2021, Virtual Conference*, volume 185 of *LIPIcs*, pages 30:1–30:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

[21] B. Barak. Work with what you've got. *Nature Physics*, Feb 2021.

[22] Y. Bansal, G. Kaplun, and B. Barak. For self-supervised learning, Rationality implies generalization, provably. In *International Conference on Learning Representations*, 2021.

[23] 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.

[24] A. Glaser, B. Barak, M. Kütt, and S. Philippe. Physical public templates for nuclear warhead verification. *Science & Global Security*, 28(1):48–59, 2020.

[25] M. Kütt, S. Philippe, B. Barak, A. Glaser, and R. J. Goldston. Authenticating nuclear warheads with high confidence. In *Proceedings of the 55th Annual INMM Meeting*, 2014.

[26] S. Philippe, B. Barak, and A. Glaser. Designing protocols for nuclear warhead verification. In *Proc. 56th Annual INMM Meeting*, 2015.

[27] J. Yuval, M. Nitzan, N. R. Tannenbaum, and B. Barak. Optimizing testing policies for detecting COVID-19 outbreaks. *arXiv preprint arXiv:2007.04827*, 2020.

[28] 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.

[29] P. Nakkiran, G. Kaplun, Y. Bansal, T. Yang, B. Barak, and I. Sutskever. Deep Double Descent: Where Bigger Models and More Data Hurt. In *ICLR 2020*, 2020. Also appeared in Journal of Statistical Mechanics, 2021.

[30] 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.

[31] 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.

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

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

[34] 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.

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

[36] 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.

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

[38] 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.

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

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

[41] A. Glaser, B. Barak, and R. J. Goldston. A zero-knowledge protocol for nuclear warhead verification. *Nature*, 510:497–502, 2014. See also article by R. Stone (Science, June 2014).

[42] B. Barak and D. Steurer. Sum-of-squares proofs and the quest toward optimal algorithms. In *Proceedings of International Congress of Mathematicians (ICM)*, 2014.

[43] B. Barak. Fun and Games with Sums of Squares. Also appeared on the "Windows on Theory" blog, 2014.

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

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

[46] 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.

[47] A. Glaser, B. Barak, and R. J. Goldston. Toward a Secure Inspection System for Nuclear Warhead Veri

cation Without Information Barrier. Presented at 54th Annual INMM (Institute of Nuclear Materials Management) meeting, 2013.

[48] B. Barak. Truth vs. Proof in Computational Complexity. *Bulletin of the European Association for Theoretical Computer Science*, (108), October 2012. Appeared in Logic in Computer Science column. Also posted in Windows on theory blog.

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

[50] 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".

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

[52] B. Barak, P. Gopalan, J. Håstad, R. Meka, and P. Raghavendra. Making the Long Code Shorter. In *FOCS*, 2012.

[53] 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.

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

[55] B. Barak, Y. Dodis, H. Krawczyk, O. Pereira, K. Pietrzak, F.-X. Standaert, and Y. Yu. Leftover Hash Lemma, Revisited. In *CRYPTO*, 2011. According to the New Yorker, this was one of the more obscure titles in the CRYPTO '11 conference, see highlighted text in 4th page linked below.

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

[57] B. Barak, M. Hardt, T. Holenstein, and D. Steurer. Subsampling Mathematical Programs and Average-Case Complexity. In *SODA*, 2011.

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

[59] B. Applebaum, B. Barak, and A. Wigderson. Public Key Cryptography from Different Assumptions. In *Proc. of STOC*, 2010. Preliminary version as cryptology eprint report 2008/335 by Barak and Wigderson.

[60] B. Barak, I. Haitner, D. Hofheinz, and Y. Ishai. Bounded Key-Dependent Message Security. In *EUROCRYPT*, 2010.

[61] B. Barak, A. Rao, R. Raz, R. Rosen, and R. Shaltiel. Strong Parallel Repetition Theorem for Free Projection Games. In *Proceedings RANDOM 2009*, page 365. Springer, 2009.

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

[63] S. Arora, B. Barak, M. Brunnermeier, and R. Ge. Computational Complexity and Information Asymmetry in Financial Products. In *Innovations in Computer Science (ICS) conference*, 2010.

[64] 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.

[65] B. Barak, M. Hardt, I. Haviv, A. Rao, O. Regev, and D. Steurer. Rounding Parallel Repetitions of Unique Games. In *Proceedings of 49th FOCS*, 2008.

[66] B. Applebaum, B. Barak, and D. Xiao. On Basing Lower-Bounds for Learning on Worst-Case Assumptions. In *Proceedings of 49th FOCS*, 2008.

[67] B. Barak and M. Mahmoody-Ghidary. Merkle Puzzles are Optimal — an $O(n^2)$ attack on key exchange from a random oracle. In *Proceedings of CRYPTO '09*, 2009.

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

[69] 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.

[70] B. Barak and M. Mahmoody-Ghidary. Lower bounds on signatures from symmetric primitives. In *Proceedings of FOCS '07*, 2007.

[71] 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.

[72] B. Barak, M. Prabhakaran, and A. Sahai. Concurrent Non-Malleable Zero Knowledge. In *Proceedings of FOCS '06*, 2006.

[73] B. Barak, A. Rao, R. Shaltiel, and A. Wigderson. 2-source dispersers for $n^{o(1)}$ entropy, and Ramsey graphs beating the Frankl-Wilson construction. *Annals of Mathematics*, 176(3):1483–1543, 2012. Preliminary version in STOC '06.

[74] B. Barak. Delegateable Signatures. Technical report, 2001.

[75] 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.

[76] B. Barak and A. Sahai. How to Play Almost Any Mental Game Over the Net - Concurrent Composition Using Super-Polynomial Simulation. In *Proceedings of FOCS '05*, 2005.

[77] B. Barak, R. Canetti, Y. Lindell, R. Pass, and T. Rabin. Secure Computation Without Authentication. In *Proceedings of CRYPTO '05*, 2005.

[78] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov, and A. Wigderson. Simulating Independence: New Constructions of Condensers, Ramsey Graphs, Dispersers, and Extractors. In *Proceedings of STOC '05*, 2005.

[79] B. Barak. *Non-Black-Box Techniques in Cryptography*. PhD thesis, Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot, Israel, 2004.

[80] B. Barak, R. Canetti, J. B. Nielsen, and R. Pass. Universally Composable Protocols with Relaxed Set-Up Assumptions. In *Proceedings of FOCS '04*, pages 186–195, 2004.

[81] B. Barak, R. Impagliazzo, and A. Wigderson. Extracting Randomness Using Few Independent Sources. *SIAM Journal on Computing*, 36(4):1095–1118, 2006. Preliminary version in FOCS' 04.

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

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

[84] 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)*, number 2779 in LNCS, pages 166–180, 2003.

[85] B. Barak, R. Shaltiel, and A. Wigderson. Computational analogues of entropy. In *Proc. of 7th Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM)*, 2003. See erratum note in abstract.

[86] B. Barak, S. J. Ong, and S. Vadhan. Derandomization in Cryptography. In *Proceedings of CRYPTO '03*, 2003.

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

[88] B. Barak. Constant-Round Coin-Tossing With a Man in the Middle or Realizing the Shared Random String Model. In *Proceedings of FOCS '02*, 2002. See also my thesis.

[89] B. Barak and Y. Lindell. Strict Polynomial-Time in Simulation and Extraction. *SIAM Journal on Computing*, 33(4):783–818, August 2004. Extended abstract appeared in STOC 2002.

[90] B. Barak and O. Goldreich. Universal Arguments and their Applications. *SIAM Journal on Computing*, 38(5):1661–1694, 2008. Preliminary version in CCC' 02.

[91] B. Barak, O. Goldreich, S. Goldwasser, and Y. Lindell. Resettably-Sound Zero-Knowledge and its Applications. In *Proceedings of FOCS '01*, pages 116–125, 2001.

[92] B. Barak. How to go beyond the black-box simulation barrier. In *Proceedings of FOCS '01*, pages 106–115, 2001. Winner, FOCS 2021 Test of Time Award.

[93] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. P. Vadhan, and K. Yang. On the (im)possibility of obfuscating programs. *J. ACM*, 59(2):6, 2012. Preliminary version in CRYPTO 2001.

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

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