

Boaz Barak – Curriculum Vitae

June 2011

1 Personal Details

Name: Boaz Barak
Position: Senior Researcher, Microsoft Research New England
Email: b@boazbarak.org
Home Page: <http://www.boazbarak.org>
Work address: Microsoft Corporation— Boaz Barak, One Memorial Drive,
Cambridge, MA 02142

2 Academic positions

- **Microsoft Research.** Senior researcher in New England research lab since June 2010.
- **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

- 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.
- VATAT¹ 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.

5 Research advising.

- Current advisor Moritz Hardt. Former students: David Xiao (co-advised with Avi Wigderson), Sharon Goldberg (co-advised with Jennifer Rexford), Mohammad Mahmoody.
- Former postdocs: Guy Rothblum, Benny Applebaum and Thomas Holenstein.
- Thesis committee member: Anup Rao (University of Texas, Austin), Manoj Parbhakaran (Princeton), Iannis Turlakis (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).
- Undergraduate research advisor: Jon Ullman (2007/8), Srdjan Krstic (2008/9), Aaron Potechin (2008/9), Mark Stefanski (2008/9), Christina Ilvento (2009/10).

6 Teaching and advising

- **Princeton University.** COS 433 — Cryptography, COS 522 — Complexity, COS 598D — Mathematical Methods in Computer Science. Preceptor in COS 226 — Algorithms and Data Structures . BSE Freshman advisor 2007/8 and 2008/9, advisor for BSE CS majors class of 2012.
- **Academic College of Tel-Aviv Jaffa,** Israel. Teaching assistant in ‘Logic and Set theory’ and “Introduction to Computer Science using the C programming Language”.
- **World Wide Commerce, Inc.,** Ramat Gan, Israel. Crash course on Java programming language.

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

7 Professional Services

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.

Organizing committee (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.

Editor Member of editorial board, Theory of Computing Journal. Member of scientific board, Electronic Colloquium of Computational Complexity (ECCC).

Reviews for journals: Journal of the ACM, Theoretical Computer Science A journal, IEEE Transactions on Information Theory, Geometric and Functional Analysis (GAFA), Combinatorica.

Reviews for conferences: STOC (Symposium on the Theory of Computing), FOCS (Foundations of Computer Science), Eurocrypt, CRYPTO, TCC (Theory of Cryptography Conference), CCC (Conference on Computational Complexity).

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.

8 Invited Speaker

- Workshop on classical and quantum information security, Caltech, December 2005
- Theory of cryptography conference (TCC), March 2006
- First International Computer Science Symposium in Russia, St. Petersburg, June 2006.
- Faces of cryptography workshop, CUNY, September 2009.
- Walmart Cryptography and Complexity Lecture Series, Weizmann Institute of Science, May 2010.

9 Publications

Papers are presented in chronological order. Electronic versions of all papers are available on my home page (<http://www.cs.princeton.edu/~boaz>). 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.

Journal papers.

- [1] S. Arora, B. Barak and D. Steurer. Computational complexity and information asymmetry in financial products. *Commun. ACM*, 54(5):101–107, 2011.
- [2] 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.
- [3] 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.
- [4] B. Barak, R. Impagliazzo, and A. Wigderson. Extracting Randomness Using Few Independent Sources. *SIAM Journal on Computing*, 36(4):1095–1118, 2006. Preliminary version appeared in FOCS 2004.
- [5] 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.
- [6] 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.
- [7] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov and A. Wigderson Simulating independence: New constructions of condensers, ramsey graphs, dispersers, and extractors. *Jornal of the ACM*, 57(4): (2010) Preliminary version appeared in STOC 2005.

Papers in refereed conferences.

- [1] B. Barak, A. Herzberg, D. Naor, and E. Shai. The Proactive Security Toolkit and Applications. In *Proc. 6th ACM Conference on Computer and Communications Security (CCS)*. ACM, 1999.
- [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.
- [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.
- [4] B. Barak. How to Go Beyond the Black-box Simulation Barrier. In *Proc. 42nd Foundations of Computer Science (FOCS)*, pages 106–115. IEEE, 2001.

- [5] B. Barak, O. Goldreich, S. Goldwasser, and Y. Lindell. Resettably-Sound Zero-Knowledge and its Applications. In *Proc. 42nd Foundations of Computer Science (FOCS)*. IEEE, 2001.
- [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)*.
- [7] B. Barak and Y. Lindell. Strict Polynomial-time in Simulation and Extraction. In *Proc. 34th Symposium on Theory of Computing (STOC)*. ACM, 2002. Journal version in *SIAM Journal of Computing (SICOMP)*.
- [8] B. Barak. Constant-Round Coin-Tossing With a Man in the Middle or Realizing the Shared Random String Model. In *Proc. 43rd Foundations of Computer Science (FOCS)*. IEEE, 2002.
- [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.
- [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*.
- [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.
- [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.
- [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*.
- [14] B. Barak and R. Pass. On the Possibility of One-Message Weak Zero-Knowledge. In *Proc. 1st Theory of Cryptography Conference (TCC)*, 2004.
- [15] B. Barak, R. Impagliazzo, and A. Wigderson. Extracting Randomness from Few Independent Sources. In *Proc. 45th Foundations of Computer Science (FOCS)*. IEEE, 2004. Journal version in *SICOMP*.
- [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.
- [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.
- [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.

- [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.
- [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.
- [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.
- [22] B. Barak, M. Prabhakaran, and A. Sahai. Concurrent Non-Malleable Zero Knowledge. In *Proc. 47th Foundations of Computer Science (FOCS)*. IEEE, 2006.
- [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.
- [24] B. Barak and M. Mahmoody-Ghidary. Lower bounds on signatures from symmetric primitives. In *Proc. 48th Foundations of Computer Science (FOCS)*. IEEE, 2007.
- [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.
- [26] B. Barak, S. Goldberg, and D. Xiao. Protocols and Lower Bounds for Failure Localization in the Internet. In *Proceedings of Eurocrypt 2008*, 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.
- [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.
- [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.
- [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.
- [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.
- [32] B. Barak, M. Braverman, X. Chen, and A. Rao. How to compress interactive communication. In *STOC*, pages 67–76, 2010.
- [33] B. Applebaum, B. Barak, and A. Wigderson. Public-key cryptography from different assumptions. In *STOC*, pages 171–180, 2010.
- [34] B. Barak, I. Haitner, D. Hofheinz, and Y. Ishai. Bounded Key-Dependent Message Security. In *EUROCRYPT*, pages 423–444, 2010.

- [35] B. Barak, M. Hardt, T. Holenstein, and D. Steurer. Subsampling Mathematical Relaxations and Average-case Complexity. In *SODA*, pages 512–531, 2011.
- [36] 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.
- [37] B. Barak, Y. Dodis, H. Krawczyk, O. Pereira, K. Pietrzak, F.-X. Standaert, and Y. Yu. Leftover Hash Lemma, Revisited. In *CRYPTO*, 2011.