

Boaz Barak – Curriculum Vitae

October 15, 2004

1 Personal Details

Name: Boaz Barak
Current Position: Postdoctoral researcher in IAS, Princeton.
Email: boaz@ias.edu
Home Page: <http://www.math.ias.edu/~boaz>
Work Address: School of Mathematics, Institute for advanced study (IAS),
1 Einstein Drive, Princeton, NJ 08540

2 Education

Weizmann Institute of Science

Rehovot, Israel

Ph.D Computer Science 1999 – 2004

Title of thesis: Non-Black-Box Techniques in Cryptography.

Advisor: Prof. Oded Goldreich

Tel-Aviv University

Tel-Aviv, Israel

B.Sc (summa cum laude) Mathematics and Computer Science 1996 – 1999.

GPA: Mathematics: 97/100 , Computer Science: 99/100

3 Awards and Honors

3.1 During graduate studies

- Checkpoint scholarship for graduate students in computer science. January 2001 – September 2002.
- 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”
- VATAT¹ scholarship for graduate students in the high-tech area. October 2001 – August 2003.
- Clore foundation scholarship for graduate students in the sciences. September 2002 - August 2003.
- Co-winner of FOCS 2002 conference Machtey award for best student paper. Award was given for the paper “Constant-Round Coin-Tossing With a Man in the Middle or Realizing the Shared Random String Model”

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

- Co-winner of FOCS 2002 conference best paper award for the same paper.
- John F. Kennedy Ph.D distinction prize, Weizmann Institute of Science, June 2003.

3.2 During undergraduate studies

- Knesset (Israeli Parliament) Education Committee's outstanding students list, academic year 1996-7.
- Tel-Aviv University Rector's list (top 0.1%), academic year 1996-7.
- Tel-Aviv University, Faculty of Exact Sciences Dean's list in the years 1996-7,1997-8,1998-9.
- Member of the special program for outstanding students in Tel-Aviv University, years 1997-9.

4 Short Visits

Institute for Advanced Study

Princeton, New Jersey.

Student visitor in the school of mathematics during summer 2001

IBM T.J. Watson Research Center

Hawthorne, New York.

Student visitor in cryptography research group during summer 2003

5 Work Experience

Institute for Advanced Study

Princeton, New Jersey.

September 2003 – present

Member in the school of mathematics.

IBM Haifa Research Lab

Network and Security department,

Tel-Aviv, Israel.

December 1998 – June 2000

Part-time student working on the Proactive Security Project.

Uptime Information Systems

Beer-Sheva, Israel.

July 1997 - December 1998

Programmer.

6 Teaching Experience

Academic College of Tel-Aviv Jaffa

Tel-Aviv, Israel.

October 2000 – June 2002.

Teaching assistant in the courses “Logic and Set theory” and “Introduction to Computer Science using the C programming Language”.

World Wide Commerce Inc.

Ramat-Gan, Israel.

August 2000.

Gave a short (4 sessions) crash course on the Java programming language to the workers of this start-up company.

7 Professional Services

Program committee member: (1) ACM STOC (Symposium on the Theory of Computing) 2004. (2) TCC (Theory of Cryptography Conference) 2005. (3) IACR CRYPTO 2005

Editor Associate editor, Theory of Computing Journal.

Reviews for journals: Journal of the ACM, Theoretical Computer Science A journal, IEEE Transactions on Information Theory.

Reviews for conferences: STOC (Symposium on the Theory of Computing), Eurocrypt, CRYPTO, TCC (Theory of Cryptography Conference).

8 Publications

Papers are presented in chronological order. Electronic versions of all papers are available on my home page (<http://www.math.ias.edu/~boaz>). Some papers also appear on the Cryptology ePrint and ECCS archives.

Journal papers.

- [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.

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. Sahay, 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. Resetably-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.
- [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.
- [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. To appear in the Journal of Computer and System Sciences (JCSS): Special issue for FOCS 2003.
- [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.
- [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.

9 Talks

- “On the (Im)possibility of Obfuscating Software”. Given on: **(1)** Oberwolfach Complexity Theory Workshop. Oberwolfach, Germany, October 2000. **(2)** Weizmann Institute of Science, Rehovot, Israel, January 2001. **(3)** Institute for Advanced Study, Princeton, New-Jersey, USA, August 2001. **(4)** Harvard University, Cambridge Massachusetts, USA, August 2001. **(5)** CRYPTO 2001 conference, Santa-Barbara California, USA, August 2001.

- “*How To Go Beyond the Black-Box Simulation Barrier*”. Given on: (1) Institute for Advanced Study, Princeton, New-Jersey, USA, October 2001. (2) IEEE Foundations of Computer Science (FOCS) 2001 conference, Las-Vegas, Nevada, USA, October 2001. (3) Hebrew University, Jerusalem, Israel, February 2002. (4) Weizmann Institute of Science, Rehovot, Israel, March 2002. (5) Tel-Aviv University, Tel-Aviv, Israel, March 2002. (6) IBM T.J. Watson Research Center, New York, USA, November 2002.
- “*Strict Polynomial-time in Simulation and Extraction*”. Given on ACM Symposium on the Theory of Computing (STOC) 2002, Montreal, Canada, May 2002.
- “*Universal Arguments and their Applications*”. Given on IEEE Conference on Computational Complexity (CCC) 2002, Montreal, Canada, May 2002.
- “*Constant-Round Coin-Tossing With a Man in the Middle or Realizing the Shared Random String Model*”. Given on: (1) DIMACS workshop on Cryptographic Protocols in Complex Environments, DIMACS center, Piscataway, New-Jersey, May 2002. (2) IBM T.J. Watson Research Center, New York, USA, November 2002. (3) IEEE Foundations of Computer Science (FOCS) 2002 conference, Vancouver, Canada, November 2002. (4) Harvard University, Cambridge, Massachusetts, USA, November 2002. (5) Weizmann Institute of Science, Rehovot, Israel, May 2003. (6) New York University (NYU), New York, NY, July 2003.
- “*Derandomization in Cryptography*”. Given in IBM T.J. Watson Research Center, July 2003.
- “*Pseudorandom Generators Secure in a Changing Environment*”. Given in IBM T.J. Watson Research Center, July 2003.
- “*Computational Analogues of Entropy*”. Given on International Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM), Princeton, New Jersey, August 2003.
- “*Lower Bounds on Non-Black-Box Zero-Knowledge*”. Given on: (1) DIMACS Mixer seminar, AT&T research lab, New Jersey, September 2003. (2) Institute for Advanced Study, Princeton, New Jersey, September 2003. (3) Massachusetts Institute of Technology (MIT), Cambridge, Massachusetts, USA, October 2003. (4) IEEE Foundations of Computer Science (FOCS) conference, Cambridge, Massachusetts, October 2003.
- “*Extracting Randomness from Few Independent Sources*”. Given on: (1) Institute for Advanced Study, Princeton, New Jersey, March 2004. (2) New York University cryptography seminar, New York, March 2004. (3) Radcliffe Institute for Advanced Study, Harvard university, May 2004.