

Boaz Barak – Publication List

October 16, 2004

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 ECCC 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.