

Curriculum Vitae

Omer Reingold

June 2008

Current Academic Employment:

Associate Professor, Faculty of Mathematics and Computer Science,
Department of Computer Science and Applied Mathematics,
The Weizmann Institute of Science
Start date: January 2004.

Personal Details:

- Address:
Faculty of Mathematics and Computer Science,
The Weizmann Institute of Science,
POB 26, Rehovot 76100,
ISRAEL
- Phone number: +972-8-934-4467
- Fax: +972-8-934-2945
- Email: omer.reingold@weizmann.ac.il
- WWW: <http://www.wisdom.weizmann.ac.il/~reingold/>
- Birth: April 30th, 1969, Tel Aviv, Israel
- Israeli citizenship

Education:

- **1994-1998**
Weizmann Institute of Science, Rehovot, Israel.
Ph.D. in Computer Science.
Thesis title: Pseudo-random synthesizers, functions and permutations (accepted 1999).
Advisor: Prof. Moni Naor.
- **1991-1994**
Tel-Aviv University, Tel-Aviv, Israel.
B.Sc in Mathematics (grade average 98/100) and Computer Science (grade average 99/100) - Summa Cum Laude.

Previous Academic Employment and Short Term Visits:

- **August 17 – November 15, 2005**
Visiting scholar,
Center for Research on Computation and Society,
Division of Engineering and Applied Sciences,
Harvard University.
- **1999 – 2004**
Senior technical staff member,
Department of Secure Systems Research,
AT&T Labs – Research,
Florham Park, NJ, USA.
- **1999 – 2004**
Concurrent to my employment at AT&T,
I was a visiting member of the School of Mathematics,
Institute for Advanced Study, Princeton, NJ, USA.

My visit at the institute was part of the special program in Theoretical Computer Science and Discrete Mathematics. In the academic year of 2000-2001 this program held a special year on Computational Complexity.

- **1998 – 1999**
Postdoctoral fellow,
Dept. of Applied Math and Computer Science,
Weizmann Institute of Science, Rehovot, Israel.
Advisor: Prof. Adi Shamir.

Professional Activities (including talks):

- Co-Chair, Board of Studies, Faculty of Mathematics and Computer Science, Weizmann (starting Jan 2007).
- Guest Editor: Special Issue of Approx-Random 2007, Algorithmica, Springer.
- Editorial Board: ACM Transactions on Computation Theory (ToCT).
- Editorial Board: SIAM Journal on Computing (SICOMP)
- Scientific Board: Electronic Colloquium on Computational Complexity (ECCC)
- Chair of program committee: Random 2007, TCC 2009
- Served on the program committee of CRYPTO 2001 and RANDOM 2001, FOCS 2002, TCC 2004, EUROCRYPT 2004, ICALP 2005, FOCS 2005, TCC 2007, CRYPTO 2007, STOC 2008.
- Talks at numerous conferences, workshops and seminars. Partial list of selected occasions follows:

- Will attend: Analytic Tools in Computational Complexity, Banff International Research Station for Mathematical Innovation and Discovery, August 2008.
- Plenary lecture, Annual Conference of the Israel Mathematical Union, May 2008.
- Expanders in Pure and Applied Mathematics, Institute for Pure and Applied Mathematics (IPAM), Los Angeles, February 2008.
- Workshop on Cryptographic Protocols (WCP 2007), Bertinoro, Italy, March 2007.
- International Congress of Mathematics (ICM 2006), Madrid, SPAIN, August 2006.
- Invited talk, International Computer Science Symposium (CSR 2006), St.Petersburg, Russia, June 2006.
- Invited tutorial on “Black-Box Separations”, The Theory of Cryptography Conference (TCC 2006), New-York, NY, March 2006.
- Workshop on Complexity Theory, The Mathematical Institute, Oberwolfach, Germany. June 2005.
- Workshop on Advances in Complexity Theory, Banff International Research Station. Banff, Canada. July 2004.
- Workshop on Complexity of Boolean Functions, Schloss Dagstuhl, International conference and research center for computer science. Dagstuhl, Germany. March 2004.
- Workshop on Contemporary Methods in Cryptography, Institute for Pure and Applied Mathematics (IPAM), Los Angeles, January 2002.
- Theory Day, Princeton-Area Center for Theory, NEC Research Institute, Princeton, March 2001.
- Research program seminar, IAS/Park City Math Institute, Summer Session on Computational Complexity, July 2000.
- Workshop on Complexity Theory, The Mathematical Institute, Oberwolfach, Germany. November 2000.
- DIMACS Workshop on Cryptography and Intractability, March, 2000.
- DIMACS workshop on Pseudorandomness and Explicit Combinatorial Constructions, October 1999.
- Workshop on Cryptography, The Mathematical Institute, Luminy, France, September 1999.
- Workshop on Randomized Algorithms (RAND2), The Weizmann Institute of Science, Rehovot, Israel. December 1998.
- Workshop on Complexity Theory, The Mathematical Institute, Oberwolfach, Germany. November 1998.
- Workshop on Cryptography and Interactive Proofs, The Fields Institute at the University of Toronto, Toronto, Canada. May 1998.
- The Weizmann Workshop on Cryptography, The Weizmann Institute of Science, Rehovot, Israel. June 1997.
- Workshop on Security in Communication Networks, Amalfi, Italy. September 1996.

Teaching:

- **Teaching** the course: *Topics in Pseudorandomness* at the Weizmann Institute of Science, both semesters of 2006/07 (second semester as a seminar).
- **Co-teaching** the course: *Introduction to Computational Learning Theory* with Amir Shpilka, both semesters of 2004/5.
- **Co-teaching** the course: *Topics in Pseudorandomness* with Ronen Shaltiel at the Weizmann Institute of Science on the 2nd semester of 2003/04.
- **Co-teaching** the course: *Probabilistic Methods in Computer Science: Derandomization*, with Moni Naor at the Weizmann Institute of Science on the 2nd semester of 1998/99.

Awards and Fellowships:

- The 2006 **Prof. Pazy Memorial Research Award**, given annually to the most outstanding and original BSF supported project in mathematics and computer science (awarded for my BSF grant joint with Prof. Luca Trevisan and Prof. Salil Vadhan).
- 2007 **Morris L. Levinson Prize in Mathematics** awarded yearly by the Scientific Council of the Weizmann Institute to a single member of the Weizmann Institute.
- **CRYPTO 2006 best paper award** for the paper “On the Power of the Randomized Iterate” (joint with Iftach Haitner and Danny Harnik).
- **ICALP 2006, track C, best paper award** for the paper “Efficient Pseudorandom Generators from Exponentially Hard One-Way Functions” (joint with Iftach Haitner and Danny Harnik).
- 2005 **ACM Grace Murray Hopper Award**. Awarded by the Association for Computing Machinery (ACM) to “the outstanding young computer professional of the year.”
- **STOC 2005 best paper award** for the paper “Undirected ST-connectivity in log-space”.
- **Rothschild award for postdoctoral studies**, 1999. Awarded yearly by Yad-Hanadiv, Jerusalem, Israel to up to eighteen Israeli students of all areas, for postdoctoral studies abroad.
- **J. F. Kennedy prize for achievements in Ph.D. studies**, 1999. Awarded yearly by the Weizmann Institute of Science, Israel to four Ph.D. students of the Weizmann Institute.
- **Levi Eshkol scholarship for postdoctoral studies**, 1998, Israel. Awarded by the ministry of science to students of Israeli universities.
- **The Dimitris N. Chorafas foundation prize for engineering and technology**, 1998, Switzerland. Awarded yearly to 20-30 students of 26 “partner universities.”
- **Clore scholars award for Ph.D. studies**, 1996, Israel. Awarded yearly to ten students of Israeli universities, in all fields of the natural sciences, including

mathematics, physics, chemistry, the life sciences, earth sciences, agriculture, engineering and technology.

- **Undergraduate studies in the Excelling Program, Tel-Aviv University, Israel.**
- **Yekutiel Federman scholarship, 1992, Israel.**
- **Dean's honors lists, Tel-Aviv University, 1991-1994, Israel.**

Grants:

- United States–Israel Binational Science Foundation (BSF), 2007, duration: four years, co-PI's: Prof. Luca Trevisan, UC Berkeley and Salil Vadhan, Harvard University. **Title:** Pseudorandomness and Combinatorial Constructions.

Awarded the 2006 Prof. Pazy Memorial Research Award, given annually to the most outstanding and original BSF supported project in mathematics and computer science.

- Israel Science Foundation (ISF), 2005, duration: four years. **Title:** The Space Complexity of Graph Connectivity, Beyond the Symmetric Case.
- United States–Israel Binational Science Foundation (BSF), 2003, duration: four years, co-PI's: Prof. Luca Trevisan, UC Berkeley and Salil Vadhan, Harvard University. **Title:** Pseudorandomness and Combinatorial Constructions.

Students and Postdoctoral fellows:

- Eyal Rozenman, Postdoctoral fellow, year of 2004/2005.
- Shachar Lovett, Ph.D., started 2006.
- Ronen Gradwohl, direct Ph.D., started 2004.
- Iftach Haitner, Ph.D., started 2004, completed 2008.
- Tal Kramer, Masters, started 2006, completed 2007.
- Michal Igell, Masters, started 2004, completed 2005.

Publications:

Each of my publications appears only once in this list. In case a paper was published both in a conference and in a journal, then usually the journal reference will appear first, directly followed by reference to the preliminary version.

A version of most papers appear in my web page:

<http://www.wisdom.weizmann.ac.il/~reingold/>

Publications appear in chronological order according to date of first publication:

- M. Naor and O. Reingold, *Synthesizers and their application to the parallel construction of pseudorandom functions*, Journal of Computer and System Sciences (JCSS), 58(2), pp. 336-375, 1999.

Preliminary Version: Proc. 36th IEEE Symp. of Foundations of Computer Science (FOCS 1995), pp. 170-181, 1995.

- M. Naor and O. Reingold, *On the construction of pseudorandom permutations: Luby-Rackoff revisited*, J. of Cryptology, vol. 12, pp. 29-66, 1999.

Preliminary Version: Proc. 29th Ann. ACM Symp. on Theory of Computing, (STOC 1997), pp. 189-199, 1997.

- M. Naor and O. Reingold, *Number-Theoretic constructions of efficient pseudorandom functions*, J. ACM vol. 51(2), pp. 231-262, 2004.

Preliminary Version: Proc. 38th IEEE Symp. on Foundations of Computer Science (FOCS 1997), pp.458-467, 1997.

- R. Canetti, D. Micciancio and O. Reingold, *Perfectly one-way probabilistic hash functions*, Proc. 30th Ann. ACM Symp. on Theory of Computing (STOC 1998), pp. 131-140, 1998.

- M. Naor and O. Reingold, *From unpredictability to indistinguishability: A simple construction of pseudorandom functions from MACs*, Advances in Cryptology - CRYPTO 1998, pp. 267-282, 1998.

- E. Biham, D. Boneh and O. Reingold, *Breaking generalized Diffie-Hellmann modulo a composite is no easier than factoring*, Information Processing Letters 70(2), pp. 83-87, 1999.

- R. Raz and O. Reingold, *On recycling the randomness of states in space bounded computation*, STOC 1999, pp. 159-168, 1999.

- R. Raz, O. Reingold and S. Vadhan, *Extracting all the randomness and reducing the error in Trevisan's extractors*, J. Comput. Syst. Sci. (JCSS), vol. 65(1), pp. 97-128, 2002.

Preliminary Version: STOC 1999, pp. 149-158, 1999.

- M. Naor, B. Pinkas and O. Reingold, *Distributed pseudorandom functions and KDCs*, Advances in Cryptology - EUROCRYPT 1999, pp. 327-346, 1999.

- C. Dwork, M. Naor, O. Reingold and L. J. Stockmeyer, *Magic functions*, J. ACM vol. 50(6), pp. 852-921, 2003.

Preliminary Version: FOCS 1999, pp. 523-534, 1999.

- R. Raz, O. Reingold and S. Vadhan, *Error reduction for extractors*, FOCS 1999, pp. 191-201, 1999.
- M. Naor, O. Reingold and A. Rosen, *Pseudorandom functions and factoring*, SIAM J. Comput., vol. 31(5), pp. 1383-1404, 2002.

Preliminary Version: STOC 2000, pp. 11-20, 2000.

- Y. Gertner, S. Kannan, T. Malkin, O. Reingold and M. Viswanathan, *The relationship between public key encryption and oblivious transfer*, FOCS 2000, pp. 325-335, 2000.
- O. Reingold, R. Shaltiel and A. Wigderson, *Extracting randomness via repeated condensing*, SIAM J. Comput., 35(5), 1185-1209, 2006.

Preliminary Version: FOCS 2000, pp. 22-31, 2000.

- O. Reingold, S. Vadhan and A. Wigderson, *Entropy waves, the Zig-Zag graph product, and new constant-degree expanders and extractors*, FOCS 2000, pp. 3-13, 2000.

Full Version of part of this work: Annals of Mathematics, vol. 155(1), 2001.

- W. Aiello, Y. Ishai and O. Reingold, *Priced oblivious transfer: how to sell digital goods*, EUROCRYPT 2001, pp. 119-135, 2001.
- M. Naor and O. Reingold: *Constructing pseudorandom permutations with a prescribed structure*, J. Cryptology, vol. 15(2), pp. 97-102, 2002.

Preliminary Version: SODA 2001, pp. 458-459, 2001.

- W. Aiello, S. M. Bellovin, M. Blaze, R. Canetti, J. Ioannidis, A. D. Keromytis, and O. Reingold: *Just fast keying: Key agreement in a hostile internet*. ACM Trans. Inf. Syst. Secur. vol. 7(2), pp. 242-273, 2004.

Preliminary Version: *Efficient, DoS-Resistant, Secure Key Exchange for Internet Protocols*. Security Protocols Workshop 2001: pp. 27-39, 2001.

- Y. Gertner, T. Malkin and O. Reingold, *On the impossibility of basing trapdoor functions on trapdoor predicates*, FOCS 2001, pp. 126-135, 2001.

- M. R. Capalbo, O. Reingold, S. Vadhan and A. Wigderson, Randomness conductors and constant-degree lossless expanders, Joint session: STOC 2002, pp. 659-668, and IEEE Conference on Computational Complexity 2002, pp. 15, 2002.
- Bar-Yossef, O. Reingold and R. Shaltiel and L. Trevisan, *Streaming computation of combinatorial objects*, IEEE Conference on Computational Complexity 2002, pp. 165-174, 2002.
- N. Alon, M. Merritt, O. Reingold, G. Taubenfeld, R. N. Wright, *Tight bounds for shared memory systems accessed by Byzantine processes*, Distributed Computing 18(2), 99-109, 2005.

Preliminary Version: DISC 2002, pp. 222-236, 2002.

- C.-J. Lu, O. Reingold, S. Vadhan, and A. Wigderson: *Extractors: optimal up to constant factors*, STOC 2003, 602-611, 2003.
- D. Harnik, M. Naor, O. Reingold, and A. Rosen, *Completeness in two-party secure computation: a computational view*, J. Cryptology 19(4), 521-552, 2006.

Preliminary Version: STOC 2004, pp. 252-261, 2004.

- O. Reingold, L. Trevisan, S. Vadhan, *Notions of reducibility between cryptographic primitives*, TCC 2004, 1-20, 2004.
- C. Dwork, M. Naor, O. Reingold, *Immunizing encryption schemes from decryption errors*, EUROCRYPT 2004, 342-360, 2004.
- I. Dinur and O. Reingold, *Assignment-Testers: towards a combinatorial proof of the PCP-Theorem*, SIAM J. Comput. 36(4): 975-1024 (2006) - special issue on "Randomness and Computation".

Preliminary Version: FOCS 2004, 155-164, 2004.

- M. J. Freedman, Y. Ishai, B. Pinkas and O. Reingold *Keyword search and oblivious pseudorandom functions*, TCC 2005, 303-324.
- D. Harnik, J. Kilian, M. Naor, O. Reingold, and A. Rosen, *On robust combiners for oblivious transfer and other primitives*, EUROCRYPT 2005: 96-113, 2005.
- Omer Reingold: *Undirected ST-connectivity in log-space*. STOC 2005: 376-385, 2005. Best paper award.
- E. Kaplan, M. Naor and O. Reingold, *Derandomized Constructions of k-Wise (Almost) Independent Permutations*, The 9th International Workshop on Randomization and Computation (RANDOM), 354-365, 2005.

- R. Gradwohl, G. Kindler, O. Reingold and A. Ta-Shma, On the Error Parameter of Dispersers, The 9th International Workshop on Randomization and Computation (RANDOM), 294-305, 2005.
- O. Reingold, L. Trevisan and S. Vadhan, Pseudorandom walks on regular digraphs and the RL vs. L problem. STOC 2006: 457-466, 2006.
- I. Haitner, D. Harnik, O. Reingold, Efficient Pseudorandom Generators from Exponentially Hard One-Way Functions, ICALP 2006, 228-239, 2006. Track C best paper award.
- I. Haitner, D. Harnik, O. Reingold, *On the Power of the Randomized Iterate*, 2005, CRYPTO 2006, 22-40, 2006. Best paper award.
- I. Haitner and O. Reingold, *Statistically-Hiding Commitment from Any One-Way Function*, STOC 2007, 1-10, 2007.
- K.-M. Chung, O. Reingold and S. Vadhan, *S-T Connectivity on Digraphs with Known Stationary Distribution*, CCC 2007, 236-249, 2007.
- I. Haitner and O. Reingold, *A New Interactive Hashing Theorem*, CCC 2007, 319-332, 2007.
- I. Haitner, J. J. Hoch, O. Reingold and G. Segev, Finding Collisions in Interactive Protocols -- A Tight Lower Bound on the Round Complexity of Statistically-Hiding Commitments, FOCS 2007, 669-679, 2007.
- R. Gradwohl and O. Reingold, Fault Tolerance in Large Games, To appear in: ACM Conference on Electronic Commerce (EC 2008).
- O. Reingold, L. Trevisan, M. Tulsiani and S. Vadhan, Dense Subsets of Pseudorandom Sets, to appear in: 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS 08).

Unpublished manuscripts and submissions:

- C. Dwork, M. Langberg, M. Naor, K. Nissim and O. Reingold, *Succinct proofs for NP and spooky interactions*, manuscript, 2001.
- R. Gradwohl and O. Reingold, Partial Exposure and Correlated Types in Large Games, submission, 2008.
- R. Gradwohl, O. Reingold, A. Yadin and A. Yehudayoff, The Player's Effect, submission, 2008.