

Curriculum Vitae

Danny Harnik

Personal Details

Name: Danny Harnik
Address: Department of Computer Science,
Technion, Haifa, 32000 Israel.
Home Phone: ++972-(0)9-7961698
Cell Phone: ++972-(0)54-4790757
Email: harnik@cs.technion.ac.il
Home Page: <http://www.cs.technion.ac.il/~harnik>

Education

Weizmann Institute of Science, Rehovot, Israel
Ph.D student *October 2001 - November 2005*
Thesis Subject: Topics on the Efficiency and Complexity of Secure Computation and Oblivious Transfer.
Advisor: Prof. Moni Naor

Weizmann Institute of Science, Rehovot, Israel
M.Sc in Computer Science *1997 - 1999*
Thesis subject: Lower Bounds for Monotone Size.
Advisor: Prof. Ran Raz

Tel Aviv University, Tel Aviv, Israel
B.Sc in Mathematics and Computer Science
1994 - 1996.

Academic Positions

- *Postdoc* at the Technion, Haifa, Israel, December 2005 - present. Hosted by Yuval Ishai and Eyal Kushilevitz.
- *Postdoc* at IPAM / UCLA, Sept.-Dec. 2006. Special program on Securing Cyberspace.

Awards

- Winner of the best paper award at *CRYPTO* 2006 for the paper "On the Power of the Randomized Iterate" (with Iftach Haitner and Omer Reingold).
- Winner of the best paper award at *ICALP* 2006 track C, for the paper "On Efficient Pseudorandom Generators from exponentially hard One-Way functions" (with Iftach Haitner and Omer Reingold).
- Lady Davis Post Doctoral Fellowship, 2005-2007.
- Israeli Higher Education Planning and Budgeting Committee (VATAT) scholarship for outstanding high-tech Ph.D. students, 2002-2005.
- Weizmann Institute, Dean's Prize for MSc. students, 2000.
- Tel-Aviv University, Avraham Haimovitch Memorial Prize for Distinction, 1996.
- Tel-Aviv University, Faculty of Exact Sciences Dean's list in the academic years 1994, 1995 and 1996.

Work Experience M-Systems Ltd. - Flash Disks.
Field Application Engineer In Taipei office, Taiwan, 1999 – 2001.

Technomatix Ltd.
Software Engineer, Geometry group, 1996 – 1997.

Shonut Ltd.
Software Engineer, OCR Development, 1995.

Teaching *Teaching Assistant for "Cryptographic Protocols", The Weizmann Institute, 2003.*

Teacher of "Introductory Course in Probability" - As part of military duties, 1993 - 1998.

Reviewer *EUROCRYPT(2003, 2004, 2006, 2007), TCC(2004, 2005, 2006, 2007), CRYPTO(2004, 2006), FOCS(2006), JACM(2003, 2004), SIDMA(2004), IPL(2004).*

Publications (see also annotated list of publications on page 4)

Danny Harnik and Ran Raz. “Higher Lower Bounds for Monotone Size”, in the *32nd ACM Symposium on Theory of Computing (STOC)*, pages 378–387, 2000.

Danny Harnik, Moni Naor, Omer Reingold and Alon Rosen. “Completeness in Two-Party Secure Computation - A Computational view”, to appear in the *Journal of Cryptology*. Preliminary version in the *36th ACM Symposium on Theory of Computing (STOC)*, pages 252–261, 2004.

Yan Zong Ding, Danny Harnik, Ronen Shaltiel and Alon Rosen. “Constant Round Oblivious Transfer in the Bounded Storage Model”, to appear in the *Journal of Cryptology*. Preliminary version in the *Theory of Cryptography Conference (TCC)*, LNCS vol. 2951, pages 446–472, 2004.

Danny Harnik, Joe Kilian, Moni Naor, Omer Reingold and Alon Rosen. “On Robust Combiners for Oblivious Transfer and other Primitives”, in *Advances in Cryptology – EUROCRYPT ’05*, LNCS vol. 3494, pages 96–113, 2005.

Iftach Haitner, Danny Harnik and Omer Reingold. “On the Power of the Randomized Iterate”, in *Advances in Cryptology – CRYPTO 2006*, LNCS vol. 4117, pages 22–40, 2006. Winner of the *best paper award*.

Danny Harnik and Moni Naor. “On the Compressibility of NP Instances and Cryptographic Applications”, in *47th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 719–728, 2006.

Danny Harnik and Moni Naor. “On Everlasting Security in the *Hybrid* Bounded Storage Model”, in *ICALP 2006*, Part II., LNCS vol. 4052, pages 192–203, 2006.

Iftach Haitner, Danny Harnik and Omer Reingold. “On Efficient Pseudorandom Generators from exponentially hard One-Way functions.”, in *ICALP 2006*, Part II, LNCS vol. 4052, pages 228–239, 2006. Winner of the *best paper award*, track C.

Talks

“Higher Lower Bounds for Monotone Size”

- Theory Seminar, The Weizmann Institute, Rehovot, August 1999.
- The 32nd STOC conference, Portland, May 2000.

“Completeness in Two-Party Secure Computation - A Computational view”

- Theory Seminar, The Weizmann Institute, Rehovot, June 2003.
- Hebrew University Theory Seminar, Jerusalem, January 2004.
- Technion CS Colloquium, Haifa, January 2004.
- IBM Research, Watson, NY, February 2004.
- Columbia University Theory Seminar, NY, February 2004.
- The 36th STOC conference, Chicago, June 2004.
- Cryptography seminar at the University of Aarhus, May 2005.

“Constant Round Oblivious Transfer in the Bounded Storage Model”

- Theory Seminar, The Weizmann Institute, Rehovot, January 2004.
- The 1st TCC conference, Boston, February 2004.
- Cryptography reading group seminar at NYU, June 2004.

“On Robust Combiners for Oblivious Transfer and other Primitives”

- Hebrew University Theory Seminar, Jerusalem, March 2005.
- Theory Seminar, The Weizmann Institute, Rehovot, March 2005.
- Theory Seminar, Tel Aviv University, March 2005.
- Oblivious Transfer workshop, Haifa University, May 2005.
- EUROCRYPT 2005, Aarhus, Denmark, May 2005.
- CS Colloquium, Bar-Ilan University, June 2005.

“On the Compressibility of NP instances and Cryptographic Applications”

- Theory Seminar, The Weizmann Institute, Rehovot, February 2006.
- Theory Lunch, Princeton, NJ, March 2006.
- Technion CS Colloquium, Haifa, March 2006.
- FOCS 2006, Berkeley, October 2006.
- IPAM / UCLA Workshop, November 2006.

“On the Power of the Randomized Iterate”

- IBM Research, Watson, NY, March 2006.
- Theory Seminar, Haifa University, June 2006.
- IPAM / UCLA seminar, September 2006.
- UCSD theory seminar, November 2006.
- Microsoft Research, Silicon Valley, November 2006.

“On Everlasting Security in the Hybrid Bounded Storage Model”

- ICALP 2006, Venice, Italy, July 2006.

“On Efficient Pseudorandom Generators from exponentially hard One-Way functions.”

- ICALP 2006, Venice, Italy, July 2006.

List of Publications :

Danny Harnik and Ran Raz. “Higher Lower Bounds for Monotone Size”, in the *32nd ACM Symposium on Theory of Computing (STOC)*, pages 378–387, 2000.

In this paper we prove a new exponential lower bound on the monotone circuit size of an explicit function in monotone- \mathcal{NP} . This bound is higher than any previous lower bound on the monotone size of a function. Our lower bound is proved by the symmetric version of Razborov’s method of approximations. However, we present this method in a new and simpler way: Rather than building approximator functions for all the gates in a circuit, we use a gate elimination argument that is based on a Monotone Switching Lemma. The bound applies for a family of functions, each defined by a construction of a small probability space of c -wise independent random variables.

Danny Harnik, Moni Naor, Omer Reingold and Alon Rosen. “Completeness in Two-Party Secure Computation - A Computational view”, to appear in the *Journal of Cryptology*. Preliminary version in the *36th ACM Symposium on Theory of Computing (STOC)*, pages 252–261, 2004.

We give a characterization of the functions that are *complete* for (asymmetric) two-party secure computation. This study is conducted in a computational setting, where previous works managed to characterize only functions that have a small domain. A corollary of our results is a surprising all-or-nothing behavior: Either there is secure computation for *all* efficiently computable functions or there is secure computation only for select functions that have unconditional (and usually trivial) secure computation.

Yan Zong Ding, Danny Harnik, Ronen Shaltiel and Alon Rosen. “Constant Round Oblivious Transfer in the Bounded Storage Model”, to appear in the *Journal of Cryptology*. Preliminary version in the *Theory of Cryptography Conference (TCC)*, LNCS vol. 2951, pages 446–472, 2004.

In the *bounded storage model*, a long random string is initially broadcast and security is based on the sole assumption that no adversary can store all of this broadcast string. We present a constant round oblivious transfer protocol in the bounded storage model. Our construction improves over previous constructions in its simplicity and communication requirements, but most notably, reduces the number of communication rounds from a polynomial in the security parameter to 5 messages. At the heart of our protocol lies a novel 4 round *interactive hashing* protocol that may be of independent interest. Our techniques utilize explicit constructions from the theory of derandomization.

Danny Harnik, Joe Kilian, Moni Naor, Omer Reingold and Alon Rosen. “On Robust Combiners for Oblivious Transfer and other Primitives”, in *Advances in Cryptology – EUROCRYPT ’05*, LNCS vol. 3494, pages 96–113, 2005.

We define the notion of a *robust combiner* for a cryptographic primitive. Generally speaking, a combiner is a method of taking two candidate schemes for achieving a cryptographic task and combining them into one scheme that is secure if at least one of the two candidates was secure. Robust combiners are a very natural method for enhancing security of a primitive as well as a handy tool for constructing new implementations of a primitive. We show several combiners for various tasks and show that on the other hand simple combiners cannot exist for oblivious transfer.

Iftach Haitner, Danny Harnik and Omer Reingold. “On the Power of the Randomized Iterate”, in *Advances in Cryptology – CRYPTO 2006*, LNCS vol. 4117, pages 22–40, 2006.

Winner of the *best paper award*.

The construction of pseudorandom generators based on one-way functions (Haståad et al. [HILL99]) is one of the most fundamental results in cryptography. In this paper we address this task along with the important task of the amplification of weak one-way functions into strong one-way functions. We use a technique that we call the *randomized iterate* to give significantly better constructions (in terms of security and efficiency) for both of the above mentioned tasks in the case of *regular* one-way functions. In addition, somewhat surprisingly we show that this technique can be used to introduce improvements to the general “HILL” case of constructing a pseudorandom generator from *any* one-way function.

Danny Harnik and Moni Naor. “On the Compressibility of \mathcal{NP} Instances and Cryptographic Applications”, in *47th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 719–728, 2006.

We initiate the study of the compressibility of \mathcal{NP} problems. In general the question is, can one efficiently compress an instance for an \mathcal{NP} language and store a shorter representation that maintains the information of whether the original input is in the language or not. Such compression enables to succinctly store instances until a future setting will allow solving them. Our motivation for studying this form of compression stems from its powerful implications in cryptography. We show that the existence of certain compression algorithms may resolve some important open questions in cryptography. For instance, compression algorithms can enable a construction of collision resistant hash functions from *any* one-way function. We study this intriguing new question from a complexity point of view, giving a classification (in form of a structured hierarchy) that indicates which \mathcal{NP} problems are potentially easier or harder for compression. We discuss the differences between this notion and seemingly similar notions from parameterized complexity.

Danny Harnik and Moni Naor. “On Everlasting Security in the *Hybrid* Bounded Storage Model”, in *ICALP 2006, Part II*, LNCS vol. 4052, pages 192–203, 2006.

The *bounded storage model* uses a broadcast of a long random string and relies on the assumption that the adversary cannot store all of this string. The *hybrid* bounded storage model adds an additional assumption that the adversary’s running is limited up until the time of the broadcast (but not after it). The question is whether this hybrid between computational and storage assumptions may allow *everlasting security* in encryption schemes and oblivious transfer protocols that require only low storage from the honest parties (solutions based solely on storage assumptions require high capabilities from the honest parties). We suggest two augmentations of the hybrid model that allow everlasting security with low storage requirements (one setting contains a random oracle while the other is a *bounded accessibility model*). On the other hand we show that such results cannot be proved in a black-box manner in the standard hybrid bounded storage model.

Iftach Haitner, Danny Harnik and Omer Reingold.

“On Efficient Pseudorandom Generators from exponentially hard One-Way functions.”, in *ICALP 2006, Part II*, LNCS vol. 4052, pages 228–239, 2006.

Winner of the *best paper award*, track C.

We show a construction of a pseudorandom generator from any exponentially hard one-way function where the generator takes an input of length only $O(n^2)$ (where the one-way function takes an input of length n). This improves on the construction of Holenstein (TCC 06) that incurred a blowup of $O(n^5)$. The input length of such constructions has a crucial effect on the security of the generator and thus reducing the input length is a central goal when considering such reductions. Unlike Holenstein’s result, our technique deviates from the path of the seminal generator of Hastad et al. and follows by further developing the *randomized iterate* methodology presented in our previous paper.