Dana (Glasner) Dachman-Soled

Microsoft Research New England

Email: dadachma@microsoft.com **Phone:** 814-404-1225

WWW: `http://www.cs.columbia.edu/~dglasner/`

Education

Ph.D., Computer Science, July 2011
Advisor: Prof. Tal Malkin
Thesis: "On Black-Box Complexity and Adaptive, Universal Composability of Cryptographic Tasks."
Columbia University, GPA: 4.27/4.33

M.Phil., Computer Science, March 2010
Columbia University, GPA: 4.27/4.33

M.S., Computer Science, May 2008
Columbia University, GPA: 4.27/4.33

B.A., Computer Science and Math, May 2006
Yeshiva University, GPA: 3.96/4.0 including many CS courses taken at New York University.

Awards

FF SEAS Presidential Fellowship at Columbia University; 4-year fellowship (2006-2010)

Prize for Outstanding Performance in Computer Science, New York University (2006)

CRA Outstanding Undergraduate Finalist (2005)

Golding Distinguished Scholar; 4-year academic scholarship (2002-2006)

Stern College for Women Forchheimer Superior Scholar (2004-2006)

Publications

Journal Articles

D. Dachman-Soled, H. Lee, T. Malkin, R. Servedio, A. Wan, H. Wee. "Optimal Cryptographic Hardness of Learning Monotone Functions." Theory of Computing 5(1), pp. 257-282 (2009).

D. Glasner, R. Servedio. "Distribution-Free Testing Lower Bounds for Basic Boolean Functions." Theory of Computing 5(1), pp. 191-216 (2009).

Articles in Refereed Conferences

N. Bitansky, D. Dachman-Soled, S. Garg, A. Jain, Y. T. Kalai, A. López-Alt, D. Wichs. "Why Fiat-Shamir for Proofs Lacks a Proof." Tenth IACR Theory of Cryptography Conference (TCC), 2013, to appear.

S. G. Choi, D. Dachman-Soled, M. Yung. "On the Centrality of Off-Line E-Cash to Concrete Partial Information Games." Security and Cryptography for Networks - 8th International Conference (SCN), 2012, pp. 264-280.

D. Dachman-Soled, Y. T. Kalai. "Securing Circuits Against Constant-Rate Tampering." 32nd International Cryptology Conference (CRYPTO), 2012, pp. 533-551.

R. Canetti, D. Dachman-Soled, V. Vaikuntanathan, H. Wee. "Efficient Password Authenticated Key Exchange via Oblivious Transfer." 15th International Conference on Practice and Theory in Public Key Cryptography (PKC), 2012, pp. 449-466.

D. Dachman-Soled, R. Gennaro, H. Krawczyk, T. Malkin. "Computational Extractors and Pseudorandomness." Ninth IACR Theory of Cryptography Conference (TCC), 2012, pp. 383-403.

D. Dachman-Soled, R. Servedio. "A Canonical Form for Testing Boolean Function Properties" 15th International Workshop on Randomization and Computaion (RANDOM), 2011, pp. 460-471.

D. Dachman-Soled, T. Malkin, M. Raykova, M. Yung. "Secure Efficient Multiparty Computing of Multivariate Polynomials and Applications." Ninth International Conference on Applied Cryptography and Network Security (ACNS), 2011, pp. 130-146.

D. Dachman-Soled, Y. Lindell, M. Mahmoody, T. Malkin. "On the Black-Box Complexity of Optimally-Fair Coin Tossing." Eighth IACR Theory of Cryptography Conference (TCC), 2011, pp. 450-467.

S. G. Choi, D. Dachman-Soled, T. Malkin and H. Wee. "Improved Non-Committing Encryption with Applications to Adaptively Secure Protocols." Fifteenth Annual International Conference on the Theory and Application of Cryptography and information Security (Asiacrypt), 2009, pp. 287-302.

D. Dachman-Soled, T. Malkin, M. Raykova, M. Yung. "Efficient Robust Private Set Intersection." Seventh International Conference on Applied Cryptography and Network Security (ACNS), 2009, pp. 125-142.

S.G. Choi, D. Dachman-Soled, T. Malkin, H. Wee. "Simple, Black-Box Constructions of Adaptively Secure Protocols." Sixth IACR Theory of Cryptography Conference (TCC), 2009, pp. 387-402.

D. Dachman-Soled, H. Lee, T. Malkin, R. Servedio, A. Wan, H. Wee. "Optimal Cryptographic Hardness of Learning Monotone Functions." 35th International Conference on Automata, Languages and Programming (ICALP), 2008, pp. 36-47.

S.G. Choi, D. Dachman-Soled, T. Malkin, H. Wee. "Black-Box Construction of a Non-Malleable Encryption Scheme from Any Semantically Secure One." Fifth IACR Theory of Cryptography Conference (TCC), 2008, pp. 427-444.

D. Glasner, R. Servedio. "Distribution-Free Testing Lower Bounds for Basic Boolean Functions." 11th International Workshop on Randomization and Computaion (RANDOM), 2007, pp. 494-508.

D. Glasner, V. C. Sreedhar. "Configuration Reasoning and Ontology For Web." IEEE International Conference on Services Computing (SCC), 2007, pp. 384-394.

D. Glasner, A. I. Frenkel. "Geometrical characteristics of regular polyhedra: Application to EXAFS studies of nanoclusters." AIP Conf. Proc. 882, pp. 746-748 (2007).

A. I. Frenkel, L. D. Menard, P. Northrup, J. A. Rodriquez, F. Zypman, D. Glasner, S.P. Gao, H. Xu, J.C. Yang, R.G. Nuzzo. "Geometry and Charge State of Mixed-Ligand Au13 Nanoclusters" AIP Conf. Proc. 882, pp. 749-751 (2007).

Other

D. Dachman-Soled, A. Jain, Y. T. Kalai, A. López-Alt. "On the (In)security of the Fiat-Shamir Paradigm, Revisited." (Cryptology ePrint Archive).

D. Dachman-Soled, G. Fuchsbauer, P. Mohassel, A. O'Neill. "Enhanced Chosen-Ciphertext Security and Applications." (Cryptology ePrint Archive).

D. Dachman-Soled. "On the Possibility of Sender-Deniable Encryption." (Manuscript).

D. Dachman-Soled, T. Malkin, M. Raykova, M. Venkitasubramaniam. "Adaptive and Concurrent Secure Computation from New Notions of Non-Malleability." (Cryptology ePrint Archive).

Patents Filed

V. C. Sreedhar, D. Glasner. ”Method and Apparatus for configuration modeling and consistency checking of Web applications.” US Patent Filing YOR8-2006-0629.

Invited Talks and Conference Presentations

NYC CryptoDay, **New York, New York**
”Securing Circuits Against Constant-Rate Tampering,” December 2012.

Rising Stars in EECS, **Cambridge, Massachusetts**
“Securing Circuits Against Constant-Rate Tampering,” November 2012.

BU Security Seminar, **Brookline, Massachusetts**
“Securing Circuits Against Constant-Rate Tampering,” March 2012.

RANDOM 2011, **Princeton, New Jersey**
“A Canonical Form for Testing Boolean Function Properties,” August 2011.

TCC 2011, **Providence, Rhode Island**
“On the Black-Box Complexity of Optimally-Fair Coin Tossing,” March 2011.

NYC CryptoDay, **New York, New York**
”Efficient Password Authenticated Key Exchange via Oblivious Transfer ,” January 2011.

Columbia Theory Seminar, **New York, New York**
“On the Black-Box Complexity of Optimally-Fair Coin Tossing,” November 2010.

NYU Cryptography Seminar, **New York, New York**
“On the Black-Box Complexity of Optimally-Fair Coin Tossing,” November 2010.

China Theory Week 2010, **Beijing, China**
“Toward a canonical form for Boolean function property testing algorithms,” September 2010.

IBM Cryptography and Network Security Seminar, **Hawthorne, New York**
“PAKE from OT,” August 2010.

IBM Cryptography Seminar, **Hawthorne, New York**
“Improved Non-committing Encryption: Applications to Adaptively Secure Protocols,” July 2010.

TCC 2008, **New York, New York**
“Black-Box Construction of a Non-Malleable Encryption Scheme from Any Semantically Secure One,” March 2008.

RANDOM 2007, **Princeton, New Jersey**
“Distribution-Free Testing Lower Bounds for Basic Boolean Functions,” August 2007.

Technical Experience

Microsoft Research — **Cambridge, Massachusetts**
Postdoc — **August 2011-Present**
Mentor: Dr. Yael Tauman Kalai
Worked on various questions relating to leakage, tampering, delegation and black-box complexity.

IBM — **Hawthorne, New York**
Intern, Cryptography Group — **Summer 2010**
Mentors: Dr. Rosario Gennaro and Dr. Vinod Vaikuntanthan
Researched efficient protocols for password-based key exchange.

Bar-Ilan University — **Ramat-Gan, Israel**
Intern, Computer Science Department — **Summer 2009**
Mentor: Prof. Yehuda Lindell
Investigated black-box complexity of basic cryptographic primitives.

IBM — **Hawthorne, New York**
Intern, Secure Software and Services Department — **Summer 2006**
Mentors: Dr. Doug Schales and Dr. Vugranam Sreedhar
Explored modeling application configuration using a logical framework.

Princeton University — **Princeton, New Jersey**
Intern in Genomics — **Summer 2004**
Mentor: Prof. Mona Singh
Contributed to developing a method for gene function determination through clustering; NSF REU.

Brookhaven National Labs — **Upton, New York**
Intern — **Summer 2003**
Mentor: Dr. Anatoly Frenkel
Researched computational methods for determining geometric properties of nanoparticles. Results presented in ACS convention undergraduate poster session in Anaheim 2004.

Teaching

Columbia University — **New York, New York**
Teaching Assistant for Advanced Cryptography — **Spring 2010**

Columbia University — **New York, New York**
Teaching Assistant for Introduction to Computational Learning Theory — **Fall 2008**

Columbia University — **New York, New York**
Teaching Assistant for Introduction to Cryptography — **Spring 2008**

Academic Service

Program Committee: CRYPTO 2013, SCN 2012.

Conference Referee:
EUROCRYPT 2013, ASIACRYPT 2012, CRYPTO 2012, CCC 2012, PKC 2012, EUROCRYPT 2012, TCC 2012, FOCS 2011, CRYPTO 2011, EUROCRYPT 2011, TCC 2011, ASIACRYPT 2010, ACITA 2010, SCN 2010, RANDOM 2010, CRYPTO 2010, PETS 2010, FOCS 2010, RSA 2010, STOC 2009, TCC 2009, CRYPTO 2008.

December 18, 2012