Samuel Dov Gordon

September 22, 2011

Contact Information

Columbia University
Department of Computer Science
511 CSC
1214 Amsterdam Avenue MC 0401
New York, NY 10027-7003, USA

917-838-9034
dov@dovgordon.com
http://www.cs.columbia.edu/~gordon

Education

University of Maryland, College Park, Maryland USA

Ph.D. Computer Science, July 2010
M.S. Computer Science, May 2008

- Advisor: Jonathan Katz

Columbia University, Columbia College, New York, NY USA

B.A., computer science theory track, May 2003
Minor in physics, May 2003
(Dean's list: 1999-2003)

Research Experience

Columbia University New York, NY USA
Computing Innovations Fellow (Postdoctoral Researcher) with Prof. Tal Malkin **2010-present**

I was awarded the fellowship both to continue my research on the topic of fairness in secure computation, and to begin exploring the application of secure computation in emerging environments, such as cloud computing and online social networks.

University of Maryland College Park, Maryland USA
Research Assistant under Prof. Jonathan Katz **2006-2010**

My graduate research was primarily in the area of secure multi-party computation. My PhD thesis is on fairness in secure computation. Other topics included the application of game theory to cryptography, byzantine agreement, zero knowledge proof systems, and lattice based cryptography.

IBM Resesarch, Hawthorne, New York
Visiting Scientist under Prof. Tal Rabin **Summer 2009**

Research topics included lattice-based signature schemes, aggregate signature schemes, and signatures for network coding.

Weizmann Institute of Science, Rechovot, Israel
Visiting Scientist under Prof. Moni Naor **Summer 2008**

Research topics included secure computation, encryption schemes from new cryptographic assumptions, and secret sharing schemes.

Publications

Conferences:

Secure Computation with Sublinear Amortized Work
S. Dov Gordon, J. Katz, V. Kolesnikov, T. Malkin, M. Raykova and Y. Vahlis
In submission
http://eprint.iacr.org/2011/482

Extending Functional Encryption to the Randomized Setting
J. Alwen, S. Dov Gordon and R. Gennaro
In submission

Efficient Protocols for Secure Computation in the Star Model
S. Dov Gordon, T. Malkin, M. Rosulek and H. Wee
In submission

Group Signature Schemes From Lattice Assumptions
S. Dov Gordon, J. Katz, and V. Vaikuntanathan
Asiacrypt 2010

Authenticated Broadcast With a Compromised Public Key Infrastructure
S. Dov Gordon, J. Katz, R. Kumaresan, and A. Yerukhimovich
International Symposium on Stabilization, Safety, and Security of Distributed Systems, 2010
http://eprint.iacr.org/2009/410

On the Round Complexity of Zero-Knowledge Proofs Based on One-Way Permutations
S. Dov Gordon, H. Wee, D. Xiao and A. Yerukhimovich
LatinCrypt 2010

Partial Fairness in Secure Two-Party Computation
S. Dov Gordon and J. Katz
Eurocrypt 2010
http://eprint.iacr.org/2008/206

On Complete Primitives for Fairness
S. Dov Gordon, Y. Ishai, T. Moran, R. Ostrovsky and A. Sahai
Theory of Cryptography Conference, 2010

Complete Fairness in Multi-Party Computation Without an Honest Majority
S. Dov Gordon and J. Katz
Theory of Cryptography Conference, 2009
http://eprint.iacr.org/2008/458

Complete Fairness in Secure Two-Party Computation
S. Dov Gordon, C. Hazay, J. Katz and Y. Lindell
Symposium on Theory of Computation (STOC), 2008
http://www.cs.umd.edu/users/gordon/papers/fair2party.pdf

Rational Secret Sharing, Revisited
S. Dov Gordon and J. Katz
Security and Cryptography for Networks 2006
(An extended abstract of this work was also accepted for presentation at NetEcon 2006)
http://eprint.iacr.org/2006/142

Journals:
Complete Fairness in Secure Two-Party Computation
S. Dov Gordon, C. Hazay, J. Katz and Y. Lindell
To Appear, Journal of the ACM

Authenticated Broadcast With a Compromised Public Key Infrastructure (full version)
S. Dov Gordon, J. Katz, R. Kumaresan, and A. Yerukhimovich
Invited for submission to a special issue of Elsevier's Information and Computation, 2011
Currently under review.
http://eprint.iacr.org/2009/410

Partial Fairness in Secure Two-Party Computation
S. Dov Gordon and J. Katz
To Appear, Journal of Cryptology

Refereed Workshops:
Amortized Sublinear Secure Multi Party Computation
S. Dov Gordon, J. Katz, V. Kolesnikov, T. Malkin, M. Raykova, Y. Vahlis
Workshop on Cryptography and Security in Clouds, Zurich 2011

Research Grants

"Secure Computation in Emerging Environments", NSF (via CRA), $140,000
September 2010 - September 2011

Supplement for "Secure Computation in Emerging Environments", NSF (via CRA), $128,000
September 2011 - September 2012

AF: Small: "How to Let an Adversary Compute for You", NSF, $350,000
September 2011 - August 2014
(Not officially listed as a co-PI due to Columbia University restrictions.)

Invited Talks and Seminars

- *Secure Computation*
  American Mathematical Society (AMS) Sectional Meeting,
  Special Session on Mathematical Aspects of Cryptography and Cyber Security, September 2011
- *Secure Computation with Sublinear Amortized Work*
  Bar Ilan University, Ramat Gan, Israel, June 2011
  Cornell University, July 2011
- *Fairness in Secure Computation*
  New York Area Crypto Day, New York, September 2010
  Georgia Tech, April 2010
  University of Virginia, April 2010
  Columbia University, April 2010
  University of Toronto, March 2010
  Cornell University, March 2010
- *Partial Fairness in Secure Computation*
  UCLA, March 2009
- *Complete Fairness in Secure Computation*
  Ben Gurion University, Be'er Sheva, Israel, July 2008
- *On Rational Cryptography*
  Bar Ilan University, Ramat Gan, Israel, July 2008

Teaching Experience

University of Maryland, College Park, Maryland USA

Instructor: Math, Game Theory and the Theory of Games **2006**
Co-developed the curriculum and independently taught the course to advanced high school students enrolled in the University of Maryland's Young Scholar's Program. The course covered various topics in mathematics motivated by games, such as modular arithmetic, probability and expectation, recurrence relations, Nash equilibrium and other mathematical topics

Teaching Assistant: CMSC451 Design and Analysis of Computer Algorithms and CMSC131 Object Oriented Programming **2004-2006**
Responsibilities included teaching recitation sections, holding office hours and grading. CMSC451 is a senior level undergraduate theory course, and CMSC131 is an introductory course that includes students from a wide range of backgrounds and interests.

Service Activities

- Program Committees: Public Key Cryptography (PKC) 2012, Inscrypt 2011
- Referee for the following publications: ACM Symposium on Principles of Distributed Computing(PODC) 2011, Theory of Cryptography Conference (IACR) 2011, FOCS 2011 (IEEE), Information Science (Elsevier), Asiacrypt 2010 (IACR), Journal of Cryptology (IACR), Theory of Cryptography Conference (IACR) 2009, Workshop on Information Security Applications 2008, Latin American Theoretical Informatics (LNCS) 2008
- Department Council: elected as a graduate representative to the Department Council committee, to present student concerns to the department chair. 2007-2008, 2008-2009
- Education Committee: elected as a graduate student representative to the Education Committee, which decides matters of academic direction for the department. 2009-2010.
- Executive Council: volunteer member of the Executive Council, the graduate student governing body for promoting interaction among students and faculty in the computer science department, 2005-present.

Professional Experience

Bloomberg L.P, New York, NY USA

Research and Development **2003-2004**

Served as backup team leader for a group that developed software to facilitate stock trades between the company's various clients. Designed new software with implementation in C. Received valuable experience in both team leading and development.

National Institute of Standards and Technology, Gaithersburg, Maryland USA

Physical Science Trainee **2002**

Assisted in the research and development of a tracking system to monitor the movement of construction workers or emergency crews through a building, using 802.11b technology. Advised on a research project that involved the robotic placement of steel beams in construction sites.