# Samuel Dov Gordon

September 21, 2009


Contact Information

3204 A.V. Williams Bldg.
University of Maryland
College Park, MD 20742 USA

917-838-9034
gordon@cs.umd.edu
http://www.cs.umd.edu/users/gordon


## Education

**University of Maryland**, College Park, Maryland USA

Ph.D. Computer Science, expected graduation date: 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

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

My research is primarily in the area of secure multi-party computation; my thesis will be on achieving fairness in secure computation. I am also very interested in practical applications of secure computation. Other interests include 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 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:**

*Complete Fairness in Multi-Party Computation Without an Honest Majority*
S. Dov Gordon and J. Katz
Theory of Cryptography Conference, 2009

*Complete Fairness in Secure Two-Party Computation*
S. Dov Gordon, C. Hazay, J. Katz and Y. Lindell
Symposium on Theory of Computation (STOC), 2008

*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)

*Partial Fairness in Secure Two-Party Computation*
S. Dov Gordon and J. Katz
In submission

*Authenticated Broadcast With a Compromised Public Key Infrastructure*
S. Dov Gordon, J. Katz, R. Kumaresan, and A. Yerukhimovich
In submission

*On Building Fairness Bit by Bit*
S. Dov Gordon, Y. Ishai, T. Moran, R. Ostrovsky and A. Sahai
In submission

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

**Journals:**
*Complete Fairness in Secure Two-Party Computation*
S. Dov Gordon, C. Hazay, J. Katz and Y. Lindell
In submission

## Invited Talks

- *Defining and Achieving Partial Fairness in Two Party Computation*
  UCLA, March 2009
- *Complete Fairness in Two Party Computation*
  Ben Gurion University, Be'er Sheva, Israel, July 2008
- *Game Theory Meets Cryptography: A Survey of Recent Research on Rational Computation*
  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.

## 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.

## Service Activities

- Referee for the following publications: 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.