



*Multi-Input Functional Encryption*

S. Dov Gordon, J. Katz, F. Liu, E. Shi and H. Zhou  
Eurocrypt 2014.  
<http://eprint.iacr.org/2013/774>

*On the Relationship between Functional Encryption, Obfuscation, and Fully Homomorphic Encryption*

J. Alwen, M. Barbosa, P. Farshim, R. Gennaro, S. Dov Gordon, S. Tessaro and D. Wilson  
IMA Conference on Cryptography and Coding 2013

*Multi-party Computation of Polynomials and Branching Programs without Simultaneous Interaction.*

S. Dov Gordon, T. Malkin, M. Rosulek and H. Wee  
Eurocrypt 2013

*Secure Two-Party Computation in Sublinear (Amortized) Time.*

S. Dov Gordon, J. Katz, V. Kolesnikov, F. Krell, T. Malkin, M. Raykova and Y. Vahlis  
CCS 2012

*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

Journal of the ACM, 2011

*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

Journal of Cryptology, 2012

**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**

“Applying Secure Multiparty Computation to the Secure Evaluation of TOR Network Statistics”,  
NRL BAA, \$156,664

January 2017 - January 2018

“New Protocols and Systems for RAM-Based Secure Computation”, NSF Medium, \$371,035

September 2016 - September 2019

“Jana: Ensuring Secure, Private, and Flexible Data Access”, DARPA Brandeis, \$415,883

September 2015 - March 2020

“New Directions in Secure Computation: Alternatives to Garbled Circuits”, DARPA PROCEED,  
\$449,987

February 2014 - February 2015

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.)

Supplement for “Secure Computation in Emerging Environments”, NSF (via CRA), \$128,000

September 2011 - September 2012

“Secure Computation in Emerging Environments”, NSF (via CRA), \$140,000

September 2010 - September 2011

---

**Invited Talks**

- *Allowing Bounded Leakage in Secure Computation: A New Application of Differential Privacy*  
High Confidence Software and Systems Conference  
May 2017
- *Secure Computation of MIPS Machine Code*  
Workshop on Cryptography for the RAM Model of Computation  
DIMACS/MACS & June 2016
- *Secure Computation in the RAM Model*  
Workshop on Encrypted Computing and Applied Homomorphic Cryptography  
Associated with Financial Crypto & Data Security, January 2015
- *Secure Computation*  
American Mathematical Society (AMS) Sectional Meeting,  
Special Session on Mathematical Aspects of Cryptography and Cyber Security, September 2011

---

**Service Activities**

- Program Committees: Conference on Computer and Communications Security (CCS), 2017. Crypto, 2016. International Conference on Applied Cryptography and Network Security (ACNS), 2015. Public Key Cryptography (PKC), 2012, 2013 and 2014. Inscrypt, 2011.
- Referee for the following publications: ACM Symposium on Theory of Computing (STOC) 2015; ACM Symposium on Principles of Distributed Computing (PODC) 2011, 2012; Theory of Cryptography Conference (IACR) 2009, 2011, 2012; FOCS (IEEE) 2011; Eurocrypt (IACR), 2011, 2012, 2014; Crypto (IACR), 2010, 2012, 2014; Information Science (Elsevier), Asiacrypt 2010, 2013, 2014 (IACR), Journal of Cryptology (IACR), Workshop on Information Security Applications 2008, Latin American Theoretical Informatics (LNCS) 2008
- Helped organize and run the monthly New York area crypto-day, with invited speakers from around the country.
- 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.

---

**Other 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.