Samuel Dov Gordon

July 27, 2020

Contact Information

George Mason University
Department of Computer Science
4400 University Drive MSN 4A5
Fairfax, VA 22030

phone: 703 993 2767

gordon@gmu.edu
`http://www.cs.gmu.edu/~gordon`

Education

University of Maryland, College Park, Maryland USA

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

Employment History

George Mason University Fairfax, VA USA
Assistant Professor **2015–present**

Applied Communication Sciences Basking Ridge, NJ USA
Research Scientist **2012–2015**

Columbia University New York, NY USA
Computing Innovations Fellow (Postdoctoral Researcher) with Prof. Tal Malkin **2010-2012**

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

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

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

Honors and Awards

- NSF Career Award, 2019.
- Google faculty Award, 2020
- Computing Innovations Fellowship, 2010

Publications

Hindex: 16. **Total Citations**: 1436.
Underlined names are my PhD students and postdocs.
In computer theory venues, author names are traditionally alphabetized.
Venues listed in **bold** are counted in csrankings.org.

In Submission:

1. *The More The Merrier: Reducing the Cost of Large Scale MPC*
S. Dov Gordon, D. Starin, and A. Yerukhimovich. Pages: 24.
2. *Differentially Private Mixing for Cryptocurrencies*
F. Baldimtsi, **S. Dov Gordon**, I. Karantaidou, M. Liang, and M. Varia. Pages: 42
3. *Malicious Secure Private Set Intersection From Vector OLE*
P.H. Le, and **S. Dov Gordon**. Pages: 14

Conference Proceedings:

1. *Secure Parallel Computation on National Scale Volumes of Data*
   S. Mazloom, P.H. Le, S. Ranellucci, and **S. Dov Gordon**
   Usenix Security Symposium, 2020 (To Appear. Acceptance rate: N.A.) Pages: 19.
2. *Stormy: Statistics in Tor by Measuring Securely*
   R. Wails, A. Johnson, D. Starin, A. Yerukhimovich, and **S. Dov Gordon**
   ACM Conference on Computer and Communication Security (CCS), 2019, 615-632.
   Acceptance Rate: 16%. Citations: 1.
3. *Two-party Private Set Intersection with an Untrusted Third Party*
   P.H. Le, S. Ranellucci, and **S. Dov Gordon**
   ACM Conference on Computer and Communication Security (CCS), 2019, 2403-2420. Acceptance rate: 16%. Citations: 0
4. *Differentially Private Access Patterns in Secure Computation.*
   S. Mazloom and **S. Dov Gordon**
   ACM Conference on Computer and Communication Security (CCS), 2018, 490-507.
   Acceptance rate: 16%. Citations: 14
5. *Best of Both Worlds in Secure Computation, with Low Communication Overhead.*
   D. Genkin, **S. Dov Gordon**, S. Ranellucci
   Applied Cryptography and Network Security (ACNS), 2018, 340-359.
   Acceptance rate: 19%. Citations: 0
6. *Simple and Efficient Two-Server ORAM.*
   S. Dov Gordon, J. Katz, and X. Wang
   Asiacrypt, 2018, 141-157. Acceptance rate: 27%. Citations: 6
7. *Secure Computation with Low Communication from Cross-Checking.*
   S. Dov Gordon, S. Ranellucci, and X. Wang
   Asiacrypt, 2018, 59-85. Acceptance rate: 27%. Citations: 9
8. *Secure Computation of MIPS Machine Code.*
   X. Wang, **S. Dov Gordon**, A. McIntosh, J. Katz
   Esorics, 2016, 99-117. Acceptance rate: 21%. Citations: 24
9. *Leakage-resilient public-key encryption from obfuscation.*
   D. Dachman-Soled, **S. Dov Gordon**, F.H. Liu, A. O'Neill and H. Zhou
   Public Key Cryptography, 2016, 101-128. Acceptance rate: 24%. Citations: 14

Prior to Mason

10. *Constant-Round MPC with Fairness and Guarantee of Output Delivery.*
    S. Dov Gordon, F.H. Liu, E. Shi
    CRYPTO 2015, 63-82. Acceptance rate: 28%. Citations: 41
11. *Multi-Client Verifiable Computation with Stronger Security Guarantees*
    S. Dov Gordon, J. Katz, F.H. Liu, E. Shi and H. Zhou
    Theory of Cryptography Conference, 2015, 144-168. Acceptance rate: 38%. Citations: 43
12. *Multi-Input Functional Encryption*
    S. Dov Gordon, J. Katz, F.H. Liu, E. Shi and H. Zhou
    Eurocrypt 2014, 678-602.
    Acceptance rate: 19%. Citations: 259
13. *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, 65-84.
    Acceptance rate: N.A.. Citations: 33

14. *Multi-party Computation of Polynomials and Branching Programs without Simultaneous Interaction.*
    S. Dov Gordon, T. Malkin, M. Rosulek and H. Wee
    Eurocrypt 2013, 575-591. Acceptance rate: 20%. Citations: 18
15. *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, 513-524. Acceptance rate: 19%. Citations: 145
16. *Group Signature Schemes From Lattice Assumptions*
    S. Dov Gordon, J. Katz, and V. Vaikuntanathan
    Asiacrypt 2010, 395-412. Acceptance rate: 16%. Citations: 194
17. *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, 144-158. Acceptance rate: 43%. Citations: 8
18. *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, 189-204. Acceptance rate: 31%. Citations: 6
    (Originally accepted to TCC. Withdrawn for political reasons. Acceptance rate: 33%)
19. *Partial Fairness in Secure Two-Party Computation*
    S. Dov Gordon and J. Katz
    Eurocrypt 2010, 157-176. Acceptance rate: 18%. Citations: 104
20. *On Complete Primitives for Fairness*
    S. Dov Gordon, Y. Ishai, T. Moran, R. Ostrovsky and A. Sahai
    Theory of Cryptography Conference, 2010, 91-108. Acceptance rate: 33%. Citations: 32
21. *Complete Fairness in Multi-Party Computation Without an Honest Majority*
    S. Dov Gordon and J. Katz
    Theory of Cryptography Conference, 2009, 19-35. Acceptance rate: 30%. Citations: 158
22. *Complete Fairness in Secure Two-Party Computation*
    S. Dov Gordon, C. Hazay, J. Katz and Y. Lindell
    Symposium on Theory of Computation (STOC), 2008, 413-422.
    Acceptance rate: 25%. Citations: 166
23. *Rational Secret Sharing, Revisited*
    S. Dov Gordon and J. Katz
    Security and Cryptography for Networks, 2006, 229-241. Acceptance rate: 30%
    (An extended abstract of this work was also accepted for presentation at NetEcon 2006)

Journals:

1. *Leakage Resilience from Program Obfuscation.*
   D. Dachman-Soled, **S. Dov Gordon**, F.H. Liu, A. O'Neill, H.S. Zhou
   Journal of Cryptology, 2019, 742-824.

Prior to Mason

2. *Complete Fairness in Secure Two-Party Computation*
   S. Dov Gordon, C. Hazay, J. Katz and Y. Lindell
   Journal of the ACM, 2011, 1-37.
3. *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, 2014, 17-25.

4. *Partial Fairness in Secure Two-Party Computation*
   S. Dov Gordon and J. Katz
   Journal of Cryptology, 2012, 14-40.

Refereed Workshops:

1. *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
2. *Secure Parallel Computation on National Scale Volumes of Data*
   S. Mazloom, P.H. Le, S. Ranellucci, and **S. Dov Gordon**

Research Grants

Total as PI at GMU:	$1,969,852	**Total as co-PI at GMU:**	$3,400,827
Total as PI, full career:	$2,462,846	**Total as co-PI, full career:**	$4,468,815

1. "Trading Security for Efficiency in Secure Computation"
   NSF Career award, #1942575, $514,202
   February 2020 - January 2025
   PI: S.Dov Gordon
2. "New Approaches for Large Scale Secure Computation"
   NSF Medium, #1955264, Co-PI, $402,009 (GMU portion), Total award: $984,019
   May 2020 - April 2024
   PIs: S.Dov Gordon, Arkady Yerukhimovich (Lead PI, GW), Seung Geol Choi (Naval Academy)
3. "Securely Generating Differentially Private Noise"
   Google Faculty Award, $42,048
   February 2020
   PI: S.Dov Gordon
4. "Jana: Ensuring Secure, Private, and Flexible Data Access"
   Extension: DARPA (Brandeis program), subcontract from Galois Inc. $55,000
   May 2020 - April 2021
   PI: S. Dov Gordon
5. "Applying Secure Multiparty Computation to the Secure Evaluation of TOR Network Statistics"
   NRL BAA, $169,676
   January 2017 - January 2018
   PI: S. Dov Gordon
6. "New Protocols and Systems for RAM-Based Secure Computation"
   NSF Medium, #1564088 Co-PI, $371,035 (GMU portion), Total award: $1,220,000
   September 2016 - September 2019
   PIs: S. Dov Gordon (Lead PI), Jonathan Katz (UMD), Mariana Raykova (Yale)
7. "Jana: Ensuring Secure, Private, and Flexible Data Access"
   DARPA (Brandeis program), subcontract to Galois Inc. $415,883
   September 2015 - March 2020
   PI: S. Dov Gordon

Prior to Mason

8. "New Directions in Secure Computation: Alternatives to Garbled Circuits"
   DARPA (PROCEED program), $449,987
   February 2014 - February 2015
   PI: S. Dov Gordon. Co-PI: Giovanni Di Crescenzo.

9. “How to Let an Adversary Compute for You”
   NSF small, $350,000
   September 2011 - August 2014
   (Not officially listed as a co-PI due to Columbia University restrictions.)
10. Supplement for “Secure Computation in Emerging Environments”
    NSF (via CRA), $128,000
    September 2011 - September 2012
    PI: S. Dov Gordon
11. “Secure Computation in Emerging Environments”
    NSF (via CRA), $140,000
    September 2010 - September 2011
    PI: S. Dov Gordon

Courses taught

- CS600: Theory of Computation.
  - Course redesigned, Fall, 2015. Students: 17. Teacher ranking: 4.20. Course ranking: 4.07.
  - Spring, 2018. Students: 31. Teacher ranking: 3.96. Course ranking: 3.64.
- Introduction to Cryptography.
  - CS795: Course designed, Fall, 2016. Students: 4. Teacher ranking: 4.67. Course ranking: 4.67.
  - CS 499 / CS 587: Spring, 2020. Students: 34. Rankings N.A.
- CS330: Formal Methods and Models.
  - Spring, 2017. Students: 57. Teacher ranking: 3.98. Course ranking: 3.54.
  - Spring, 2019. Students: 70. Teacher ranking: 4.12. Course ranking: 3.6.
- ISA562: Introduction to Information Security, Theory and Practice.
  Course redesigned, Fall, 2017. Students: 45. Teacher ranking: 4.23. Course ranking: 4.03.
- CS 795: Topics in Data Privacy and Anonymity.
  Course design, Fall 2018. Students: 6. Teacher ranking: 5.0 Course ranking: 5.0

Students and Postdocs

- Daniel McVicker. PhD student. Advised starting Fall, 2020.
- Mingyu Liang. PhD student. Advised since Fall, 2018.
- Phi Hung Le. PhD student. Advised since Summer, 2017.
  Comprehensive exam: 05/2019 (passed.)
  Thesis proposal: 05/2020 (passed.)
  Expected Graduation: Fall 2020.
- Sahar Mazloom. PhD student. Advised since Summer, 2016.
  Comprehensive exam: 11/2018 (passed).
  Thesis proposal: 07/2019 (passed).
  Expected graduation: Fall, 2020.
- Jiayu Xu. Postdoc (2019-2021).
- Samuel Ranellucci. Postdoc (2016-2018). Joint position at UMD.
- Michael Clear. Postdoc (2016-2017). Joint position at Georgetown.

Thesis committees

- Mohammad Karami, IT PhD, April 2016. Adviser: Damon McCoy.
- Mohammad Rezaeirad, IT PhD defense, 03/2019. Adviser: Damon McCoy.

Selected Talks

- *MPC for thousands, or millions, of parties*
  Theory and Practice of Multi-Party Computation Workshop
  Invited talk, May, 2020
- *Secure 4-party Computation with Low Communication from Cross-checking*
  DIMACS/MACS Workshop on Usable, Efficient, and Formally Verified Secure Computation.
  Invited talk, March, 2019
- Schloss Dagstuhl Workshop: Practical Yet Composably Secure Cryptographic.
  Invited to attend, January, 2019

- *Differentially Private Access Patterns in Secure Computation*
  Workshop at MIT and BU: Differential Privacy Meets Secure Multiparty Computation.
  Invited talk, June, 2018
- *Allowing Bounded Leakage in Secure Computation: A New Application of Differential Privacy*
  High Confidence Software and Systems Conference
  Invited talk, May 2017
- *Secure Computation of MIPS Machine Code*
  Workshop on Cryptography for the RAM Model of Computation
  Invited talk, DIMACS/MACS. June, 2016
- *Secure Computation in the RAM Model*
  Workshop on Encrypted Computing and Applied Homomorphic Cryptography
  Invited talk, Associated with Financial Crypto & Data Security, January 2015
- *Secure Computation*
  American Mathematical Society (AMS) Sectional Meeting,
  Invited talk, Special Session on Mathematical Aspects of Cryptography and Cyber Security, September 2011

Service Activities

Mason:

- Computer Science, Faculty Hiring Committee, 2020.
- Information Security and Assurance, M.S. Admissions committee, 2015-2020.
- Computer Science, Space Committee, 2017 - 2020.
- Computer Science, Organizer of the Distinguished Lecturer Series, 2019 - 2020.
- Faculty adviser to Patriot Hackers. Fall 2017 - 2018.

External Service:

- Program Committees: Conference on Computer and Communications Security (CCS), 2020. Crypto, 2018. 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 funding agencies: NSF 2018, 2019; Israel Science Foundation 2017, 2020.
- Referee for the following publications: Crypto (IACR), 2010, 2012, 2014, 2017, 2020 ; Eurocrypt (IACR), 2011, 2012, 2014, 2016, 2017, 2018; 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; Information Science (Elsevier); Asiacrypt (IACR) 2010, 2013, 2014; Journal of Cryptology (IACR) 2014, 2016, 2017; Financial Cryptography 2017; Symposium on Security and Privacy (IEEE) 2013; Workshop on Information Security Applications 2008, Latin American Theoretical Informatics (LNCS) 2008
- Organizer of the DC Area Crypto Day. Summer 2018 - present.
- 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.