DANA (GLASNER) DACHMAN-SOLED

I. PERSONAL INFORMATION

I.A. UID, Last Name, First Name, Middle Name, Contact Information
UID: 108974807
Dachman-Soled, Dana (Glasner)
Iribe Center 5238
8125 Paint Branch Dr.
College Park, MD 20742, USA
Phone: (301) 405-9927 **Email:** danadach@ece.umd.edu

I.B. Academic Appointments at UMD

Associate Professor
Department of Electrical and Computer Engineering and UMIACS, July 2020-Present

Assistant Professor
Department of Electrical and Computer Engineering and UMIACS, August 2013-June 2020

Affiliate
Department of Computer Science, November 2013-Present

I.D. Other Employment

Postdoc
Microsoft Research, Cambridge Massachusetts, August 2011-June 2013

Research Assistant
Columbia University, New York, NY, July 2010-July 2011

Visiting Researcher
Bar-Ilan University, Israel, June 2009-August 2009

Summer Intern
IBM Research, Hawthorne, NY, June 2006-August 2006

REU Summer Intern in Genomics
Princeton University, Princeton, NJ, June 2004-August 2004

Summer Intern
Brookhaven National Labs, Upton, NY, June 2003-August 2003

I.E. Educational Background

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

II. RESEARCH, SCHOLARLY AND CREATIVE ACTIVITIES

Google Scholar Citation Report (as of 8/28/2022): Total Citations: 1777; h-index: 25; i10-index: 43 (Note: Google Scholar does not provide citation reports without self-citations). Link: `https://scholar.google.com/citations?user=Ss009KUAAAAJ&hl=en`

A "#" sign identifies co-authors I mentored as high school students, undergraduate students, graduate students, or postdoctoral researchers.

II.C. Articles in Refereed Journals

1. D. Dachman-Soled, #H. Gong, #M. Kulkarni, #A. Shahverdi. "(In) Security of Ring-LWE Under Partial Key Exposure." Journal of Mathematical Cryptology 15 (1), pp. 72-86.
2. D. Dachman-Soled, #H. Gong, #M. Kulkarni, #A. Shahverdi. "Towards a Ring Analogue of the Leftover Hash Lemma." Journal of Mathematical Cryptology 15 (1), pp. 87-110.
3. D. Dachman-Soled, #H. Gong, #M. Kulkarni, #A. Shahverdi. "Security of NewHope Under Partial Key Exposure." Research in Mathematics and Public Policy, pp. 93-125
4. M. Chen, #A. Shahverdi, S. Anderson, #S.Y. Park, #J. Zhang, D. Dachman-Soled, K. Lauter, M. Wu. "Transparency Tools for Fairness in AI (Luskin)." Research in Mathematics and Public Policy, pp. 47-80.
5. D. Dachman-Soled, N. Fleischhacker, J. Katz, A. Lysyanskaya, D. Schröder. "Feasibility and Infeasibility of Secure Computation with Malicious PUFs." Journal of Cryptology, 33(2) pp. 595-617, 2020.
6. D. Dachman-Soled, #M. Kulkarni, #A. Shahverdi. "Tight Upper and Lower Bounds for Leakage-Resilient, Locally Decodable and Updatable Non-Malleable Codes." Information & Computation 268, 2019.
7. D. Dachman-Soled, #F.H. Liu, E. Shi, H.S. Zhou. "Locally Decodable and Updatable Non-Malleable Codes and Their Applications." Journal of Cryptology 33(1) pp. 319-355, 2020.
8. D. Dachman-Soled, C. Liu, C. Papamanthou, E. Shi, U. Vishkin. "Oblivious Network RAM and Leveraging Parallelism to Achieve Obliviousness." Journal of Cryptology, 32(3) pp. 941-972, 2019.
9. D. Dachman-Soled, S.D. Gordon, #F.H. Liu, A. O'Neill, H.S. Zhou. "Leakage Resilience from Program Obfuscation." Journal of Cryptology, 32(3) pp. 742-824, 2019.
10. S.G. Choi, D. Dachman-Soled, T. Malkin, H. Wee. "Black-Box Construction of a Non-Malleable Encryption Scheme from Any Semantically Secure One." Journal of Cryptology, 31(1): 172-201, 2018.
11. S.G. Choi, D. Dachman-Soled, T. Malkin, H. Wee. "Improved, Black-Box, Non-Malleable Encryption from Semantic Security." Designs, Codes and Cryptography, 86(3), pp. 641-663, 2018.
12. D. Dachman-Soled, T. Malkin, M. Raykova, M. Yung. "Efficient Robust Private Set Intersection." International Journal of Applied Cryptography 2(4), pp. 289-303 (2012).
13. 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).
14. D. Glasner, R. Servedio. "Distribution-Free Testing Lower Bounds for Basic Boolean Functions." Theory of Computing 5(1), pp. 191-216 (2009).

II.D. Published Conference Proceedings

II.D.1. Refereed Conference Proceedings

"AR" stands for "acceptance rate" below.

1. M. Fahr Jr., #H. Kippen, A. Kwong, T. Dang, J. Lichtinger, D. Dachman-Soled, D. Genkin, A. Nelson, R. Perlner, A. Yerukhimovich, D. Apon. "When Frodo Flips: End-to-End Key Recovery on FrodoKEM via Rowhammer." ACM SIGSAC Conference on Computer and Communications Security (CCS) 2022, to appear.

2. S.G. Choi, D. Dachman-Soled, S.D. Gordon, L. Liu, A. Yerukhimovich. "Secure Sampling with Sublinear Communication." Twentieth IACR Theory of Cryptography Conference (TCC) 2022, to appear.

3. M. Ball, D. Dachman-Soled, J. Loss. "(Nondeterministic) Hardness vs. Non-Malleability." 42nd Annual Cryptology Conference (CRYPTO) 2022, to appear.

4. D. Dachman-Soled, #H. Gong, #H. Kippen, #A. Shahverdi. "BKW Meets Fourier: New Algorithms for LPN with Sparse Parities." Nineteenth IACR Theory of Cryptography Conference (TCC) 2021, pp. 658-688. (AR = 66/161 = 0.41)

5. S.G. Choi, D. Dachman-Soled, D. Gordon, L. Liu, A. Yerukhimovich. "Compressed Oblivious Encoding for Homomorphically Encrypted Search." ACM SIGSAC Conference on Computer and Communications Security (CCS) 2021, pp. 2277-2291. (AR = 196/879 = 0.22)

6. #A. Shahverdi, #M. Shirinov, D. Dachman-Soled. "Database Reconstruction from Noisy Volumes: A Cache Side-Channel Attack on SQLite." 30th USENIX Security Symposium, USENIX Security 2021, pp. 1019-1035.

7. D. Dachman-Soled, I. Komargodski, R. Pass. "Non-Malleable Codes for Bounded Parallel-Time Tampering." 41st Annual Cryptology Conference (CRYPTO (3)) 2021, pp. 535-565. (AR = 103/426 = 0.24)

8. D. Dachman-Soled. "Revisiting Fairness in MPC: Polynomial Number of Parties and General Adversarial Structures." Eighteenth IACR Theory of Cryptography Conference (TCC) 2020, pp. 595-620 (AR = 71/167 = 0.43)

9. D. Dachman-Soled, L. Ducas, #H. Gong, M. Rossi. "LWE with Side Information: Attacks and Concrete Security Estimation." 40th Annual Cryptology Conference (CRYPTO) 2020, pp. 329-358. (AR = 85/371 = 0.23)

10. M. Ball, D. Dachman-Soled, #M. Kulkarni. "New Techniques for Zero-Knowledge: Leveraging Inefficient Provers to Reduce Assumptions, Interaction, and Trust." 40th Annual Cryptology Conference (CRYPTO) 2020, pp. 674-703. (AR = 85/371 = 0.23)

11. S.G. Choi, D. Dachman-Soled, #M. Kulkarni, A. Yerukhimovich. "Differentially-Private Multi-Party Sketching for Large-Scale Statistics." 20th Privacy Enhancing Technologies Symposium (PETS) 2020. Proceedings on Privacy Enhancing Technologies 2020 (3), pp. 153-174. (AR = 16/83 = 0.19)

12. J. Kelsey, D. Dachman-Soled, S. Mishra, M. S. Turan. "TMPS: Ticket-Mediated Password Strengthening." Topics in Cryptology – CT-RSA 2020, The Cryptographer's Track at the RSA Conference 2020, pp. 225-253. (AR = 28/95 = 0.29)

13. S. Hong, #M. Davinroy, Y. Kaya, D. Dachman-Soled, T. Dumitras: "How to 0wn the NAS in Your Spare Time." 8th International Conference on Learning Representations, ICLR 2020. (AR = 687/2594 = 0.26)

14. M. Ball, D. Dachman-Soled, #M. Kulkarni, T. Malkin. "Limits to Non-Malleability." 11th Innovations in Theoretical Computer Science Conference (ITCS) 2020, pp. 80:1-80:32. (AR = 86/204

= 0.42)

15. D. Dachman-Soled, #H. Gong, #M. Kulkarni, #A. Shahverdi. "(In)Security of Ring-LWE Under Partial Key Exposure." The second international Workshop on Mathematical Cryptology (MathCrypt). (AR not available for 2019, 0.33 for 2018).

    [Papers will be published in the proceedings as a Special Issue of the Journal of Mathematical Cryptology.]

16. D. Dachman-Soled, #H. Gong, #M. Kulkarni, #A. Shahverdi. "Towards a Ring Analogue of the Leftover Hash Lemma." The second international Workshop on Mathematical Cryptology (MathCrypt). (AR not available for 2019, 0.33 for 2018).

    [Papers will be published in the proceedings as a Special Issue of the Journal of Mathematical Cryptology.]

17. Y. Liu, D. Dachman-Soled, A. Srivastava. "Mitigating Reverse Engineering Attacks on Deep Neural Networks." IEEE Computer Society Annual Symposium on VLSI (ISVLSI) 2019, pp. 657-662. (AR = 53/161 = 0.33)

18. M. Ball, D. Dachman-Soled, #M. Kulkarni, H. Lin, T. Malkin. "Non-Malleable Codes Against Bounded Polynomial Time Tampering." Advances In Cryptology–EUROCRYPT(1) 2019–38th Annual international Conference on the Theory and Applications of Cryptographic Techniques, 2019, pp. 501-530. (AR = 76/327 = 0.23)

19. D. Apon, D. Dachman-Soled, #H. Gong, J. Katz. "Constant-Round Group Key-Exchange from the Ring-LWE Assumption." The Tenth International Conference on Post-Quantum Cryptography (PQCrypto) 2019, pp. 189-205. (AR = 24/97 = 0.25)

20. D. Dachman-Soled, #M. Kulkarni. "Upper and Lower Bounds for Continuous Non-Malleable Codes." 22nd International Conference on Practice and Theory in Public Key Cryptography (PKC) 2019, pp. 519-548. (AR = 42/173 = 0.24)

21. M. Ball, D. Dachman-Soled, S. Guo, T. Malkin, L.Y. Tan. "Non-Malleable Codes for Small-Depth circuits." 59th IEEE Annual Symposium on Foundations of Computer Science (FOCS) 2018, pp. 826-837. (AR = 86/320 = 0.27)

22. M. Ball, D. Dachman-Soled, #M. Kulkarni, T. Malkin. "Non-Malleable Codes from Average-Case Hardness: AC0, Decision Trees, and Streaming Space-Bounded Tampering." Advances In Cryptology–EUROCRYPT 2018–37th Annual international Conference on the Theory and Applications of Cryptographic Techniques, 2018, pp. 618-650. (AR = 69/294 = 0.23)

23. D. Dachman-Soled, #M. Kulkarni, #A. Shahverdi. "Local Non-Malleable Codes in the Bounded Retrieval Model." 21st International Conference on Practice and Theory in Public Key Cryptography PKC (2) 2018, pp. 281-311. (AR = 49/186 = 0.26)

24. D. Dachman-Soled, #M. Kulkarni, #A. Shahverdi. "Tight Upper and Lower Bounds for Leakage-Resilient, Locally Decodable and Updatable Non-Malleable Codes." 20th International Conference on Practice and Theory in Public Key Cryptography (PKC) (1) 2017, pp. 310-332. (AR = 36/160 = 0.23)

25. D. Dachman-Soled. "Towards Non-Black-Box Separations of Public Key Encryption and One Way Functions." 14th IACR Theory of Cryptography Conference (TCC 2016-B) (2), 2016, pp. 161-191. (AR = 45/113 = 0.40)

26. M. Ball, D. Dachman-Soled, #M. Kulkarni, T. Malkin. "Non-Malleable Codes for Bounded Depth, Bounded Fan-in Circuits." Advances In Cryptology–EUROCRYPT 2016–35th Annual international Conference on the Theory and Applications of Cryptographic Techniques, 2016, pp. 881-908. (AR = 62 / 274 = 0.23)

27. D. Dachman-Soled, J. Katz, #A. Thiruvengadam. "10-Round Feistel is Indifferentiable from an Ideal Cipher." Advances In Cryptology–EUROCRYPT 2016–35th Annual international Conference on the Theory and Applications of Cryptographic Techniques, 2016, pp. 649-678. (AR = 62 / 274 = 0.23)

28. D. Dachman-Soled, S.D. Gordon, #F.H. Liu, A. O'Neill, H.S. Zhou. "Leakage Resilient Public-Key Encryption from Obfuscation." 19th International Conference on Practice and Theory in Public Key Cryptography (PKC), 2016, pp. 101-128. (AR = 34/143 = 0.24)

29. C. Cho, D. Dachman-Soled, S. Jarecki. "Efficient Concurrent Covert Computation of String Equality and Set Intersection." Topics in Cryptology – CT-RSA 2016, The Cryptographer's Track at the RSA Conference 2016, pp. 164-179. (AR = 26/76 = 0.34)

30. D. Dachman-Soled, C. Liu, C.Papamanthou, E. Shi, U. Vishkin. "Oblivious Network RAM and Leveraging Parallelism to Achieve Obliviousness." 21st Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), 2015, pp. 337-359. (AR = 64 / 251 = 0.25)

31. D. Dachman-Soled, #F.H. Liu, H.S. Zhou. "Leakage-Resilient Circuits Revisited–Optimal Number of Computing Components Without Leak-Free Hardware." Advances In Cryptology–EUROCRYPT (2) 2015–34th Annual international Conference on the Theory and Applications of Cryptographic Techniques, 2015, pp 131-158. (AR = 57 / 194 = 0.29)

32. D. Dachman-Soled, J. Katz, #V. Rao. "Adaptively Secure, Universally Composable, Multiparty Computation in Constant Rounds." Twelfth IACR Theory of Cryptography Conference (TCC) (2), 2015, pp. 586-613. (AR = 52/137 = 0.38)

33. D. Dachman-Soled, #F.H. Liu, E. Shi, H.S. Zhou. "Locally Decodable and Updatable Non-malleable Codes and Their Applications" Twelfth IACR Theory of Cryptography Conference (TCC) (1), 2015, pp. 427-450. (AR = 52/137 = 0.38)

34. D. Dachman-Soled, V. Feldman, L.Y. Tan, A. Wan, K. Wimmer. "Approximate resilience, monotonicity, and the complexity of agnostic learning." 25th Annual ACM-SIAM Symposiumon Discrete Algorithms (SODA), 2015, pp. 498-511. (AR = 137/495 = 0.28)

35. D. Dachman-Soled, N. Fleischhacker, J. Katz, A. Lysyanskaya, D. Schröder. "Feasibility and Infeasibility of Secure Computation with Malicious PUFs" 34th International Cryptology Conference (CRYPTO) (2) 2014, pp. 405-420. (AR = 60 / 227 = 0.26)

36. N. Bitansky, D. Dachman-Soled, H. Lin. "Leakage-Tolerant Computation with Input-Independent Preprocessing." 34th International Cryptology Conference (CRYPTO) (2) 2014, pp. 146-163. (AR = 60 / 227 = 0.26)

37. D. Dachman-Soled. "A Black-Box Construction of a CCA2 Encryption Scheme from a Plaintext Aware (sPA1) Encryption Scheme." 17th International Conference on Practice and Theory in Public Key Cryptography (PKC), 2014, pp. 37-55. (AR = 38 / 145 = 0.26)

38. D. Dachman-Soled. "On Minimal Assumptions for Sender-Deniable Public Key Encryption." 17th International Conference on Practice and Theory in Public Key Cryptography (PKC), 2014, 574-591. (AR = 38 / 145 = 0.26)

39. D. Dachman-Soled, G. Fuchsbauer, P. Mohassel, A. O'Neill. "Enhanced Chosen-Ciphertext Security and Applications." 17th International Conference on Practice and Theory in Public Key Cryptography (PKC), 2014, pp. 329-344. (AR = 38 / 145 = 0.26)

40. D. Dachman-Soled, Y.T. Kalai. "Securing Circuits and Protocols Against 1/poly(k) Tampering Rate." Eleventh IACR Theory of Cryptography Conference (TCC), 2014, pp. 540-565. (AR = 30 / 90 = 0.33)

41. D. Dachman-Soled, M. Mahmoody, T. Malkin. "Can Optimally-Fair Coin Tossing be Based on One-Way Functions?" Eleventh IACR Theory of Cryptography Conference (TCC), 2014, pp. 217-239. (AR = 30 / 90 = 0.33)

42. D. Dachman-Soled, T. Malkin, M. Raykova, M. Venkitasubramaniam. "Adaptive and Concurrent Secure Computation from New Adaptive, Non-Malleable Commitments." 19th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT) (1), 2013, pp. 316-336. (AR = 54 / 269 = 0.20)

43. 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, pp. 182-201. (AR = 36 / 98 = 0.37)

44. 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. (AR = 31/72 = 0.43)

45. D. Dachman-Soled, Y.T. Kalai. "Securing Circuits Against Constant-Rate Tampering." 32nd International Cryptology Conference (CRYPTO), 2012, pp. 533-551. (AR = 48 / 225 = 0.21)

46. 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. (AR = 41 / 188 = 0.22)

47. D. Dachman-Soled, R. Gennaro, H. Krawczyk, T. Malkin. "Computational Extractors and Pseudorandomness." Ninth IACR Theory of Cryptography Conference (TCC), 2012, pp. 383-403. (AR = 36 / 131 = 0.27)

48. 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. (AR = 29/64 = 0.45)

49. 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. (AR = 31/172 = 0.18)

50. 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. (AR = 35 / 108 = 0.32)

51. 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. (AR = 41 / 300 = 0.14)

52. 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. (AR = 32/150 = 0.21)

53. 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. (AR = 33 / 109 = 0.30)

54. 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. (AR = 70/269 = 0.26)

55. 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. (AR = 33 / 81 = 0.41)

56. D. Glasner, R. Servedio. "Distribution-Free Testing Lower Bounds for Basic Boolean Functions." 11th International Workshop on Randomization and Computation (RANDOM), 2007, pp. 494-508. (AR = 23/50 = 0.46)
57. D. Glasner, V.C. Sreedhar. "Configuration Reasoning and Ontology For Web." IEEE International Conference on Services Computing (SCC), 2007, pp. 384-394.
58. D. Glasner, A.I. Frenkel. "Geometrical characteristics of regular polyhedra: Application to EXAFS studies of nanoclusters." AIP Conf. Proc. 882, pp. 746-748 (2007).
59. 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).

II.E. Conferences, Workshops, and Talks

II.E.2. Invited Talks

Invited Speaker at ITC (Information Theoretic Cryptography) Conference "Greatest Hits" Track, Online talk
"Non-Malleable Codes: From Split-State to Local to $\mathbf{AC}^0$." June 2020.

DC Area Crypto Day, Washington, D.C.
"Limits to Non-Malleability." November 2019.

Colloquium at Microsoft Research Redmond, Redmond, Washington
"Resilience and Vulnerability of Ring-LWE Cryptosystems to Leakage." June 2019.

NYC CryptoDay, New York, New York
"Limits to Non-Malleability." May 2019.

Cornell Tech Crypto Seminar, New York, NY
"Non-Malleable Codes from Average Case Hardness." January 2019.

Capital Area Theory Day, Washington DC
"Non-Malleable Codes for Small-Depth Circuits." November 2018

Stanford Crypto Seminar, Stanford, CA
"Non-Malleable Codes from Average Case Hardness." October 2018.

UCLA Crypto Seminar, Los Angeles, CA
"Non-Malleable Codes from Average Case Hardness." October 2018.

QuICS Stakeholder's Day, College Park, MD
"On the Leakage Resilience of Ideal-Lattice Based Public Key Encryption." May 2018.

DIMACS Workshop on Complexity of Cryptographic Primitives and Assumptions, New York, NY
"Tight Upper and Lower Bounds for Leakage-Resilient, Locally Decodable and Updatable Non-Malleable Codes," June 2017.

Johns Hopkins Theory Seminar, Baltimore, MD
"Tight Upper and Lower Bounds for Leakage-Resilient, Locally Decodable and Updatable Non-Malleable Codes," April 2017.

Women in Cybersecurity (WiCyS) Conference, Tucson, AZ
CRA-W/CDC Distinguished Lecturer
"Cryptography Against Physical Attacks: Recent Results and New Directions," March 2017.

Charles River Crypto Day, Boston, Massachusetts
"Towards Non-Black-Box Separations of Public Key Encryption and One Way Function," December 2016.

Cisco, Online talk
"Analyzing the Robustness of Lattice-Based Schemes Against Side-Channel Attacks," October 2016.

Capital Area Theory Day, Baltimore, Maryland
"Non-Malleable Codes for Bounded Depth, Bounded Fan-in Circuits," May 2016.

Maryland Cybersecurity Center Symposium, College Park, Maryland
"Cryptography Against Physical Attacks," December 2015.

Workshop on Crypto and Hardware Security for the IoT, College Park, Maryland
"A Dialogue on Cryptographic Threat Models," October 2015.

UMD Women in Math (WIM), College Park, Maryland
"Leakage Resilient Public Key Encryption," December 2014.

NYC CryptoDay, New York, New York
"Adaptively Secure, Universally Composable, Multiparty Computation in Constant Rounds," November 2014.

Joint LTS/UMIACS Seminar, College Park, MD
"Cryptography Against Physical Attacks: Recent Results and New Directions," December 2013.

TRUST WISE, San Jose, CA
"Minimal Assumptions for Cryptographic Tasks and Provable Security in Realistic Models," June 2013.

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, Boston, Massachusetts
"Securing Circuits Against Constant-Rate Tampering," March 2012.

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.

II.E.3. Refereed Presentations
Theory of Cryptography Conference (TCC) 2020, Online Talk
"Revisiting Fairness in MPC: Polynomial Number of Parties and General Adversarial Structures," November 2020.

Public Key Cryptography (PKC) 2014, Buenos Aires, Argentina
"On Minimal Assumptions for Sender-Deniable Public Key Encryption," March 2014.

Public Key Cryptography (PKC) 2014, Buenos Aires, Argentina
"A Black-Box Construction of a CCA2 Encryption Scheme from a Plaintext Aware Encryption Scheme," March 2014.

Theory of Cryptography Conference (TCC) 2014, San Diego, California
"Securing Circuits and Protocols Against 1/poly(k) Tampering Rate," February 2014.

Theory of Cryptography Conference (TCC) 2014, San Diego, California
"Can Optimally-Fair Coin Tossing be Based on One-Way Functions?" February 2014.

Randomization and Computation (RANDOM) 2011, Princeton, New Jersey
"A Canonical Form for Testing Boolean Function Properties," August 2011.

Theory of Cryptography Conference (TCC) 2011, Providence, Rhode Island
"On the Black-Box Complexity of Optimally-Fair Coin Tossing," March 2011.

Theory of Cryptography Conference (TCC) 2008, New York, New York
"Black-Box Construction of a Non-Malleable Encryption Scheme from Any Semantically Secure One," March 2008.

Randomization and Computation (RANDOM) 2007, Princeton, New Jersey
"Distribution-Free Testing Lower Bounds for Basic Boolean Functions," August 2007.

II.E.10. Non-Refereed Panels
Women in Cyber & Computing Professional panel at USNA, February 2018

Panel on "Women in Cybersecurity: Past, Present and Future" at the First Workshop on Women in Hardware and Systems Security (WISE 2017), co-located with HOST '17

II.J. Sponsored Research
I have been PI or co-PI on grants and gifts totaling $5,556,320 (with all funding going towards University of Maryland, College Park), with my share being $2,974,101. I have been sole PI on grants and gifts

totaling $1,684,983.

II.J.1. Grants

SaTC: CORE: Medium: Cryptography in a Post-Quantum Future
Investigators: Jonathan Katz (PI), Gorjan Alagic (co-PI), Dana Dachman-Soled (co-PI)
Source of Support: NSF
Total Award Amount: $1,000,400 (my share: $333,466)
Total Award period Covered: 07/28/2022-07/27/2025
Location of Project: University of Maryland, College Park

FAI: Toward Fair Decision Making and Resource Allocation with Application to AI-Assisted Graduate Admission and Degree Completion
Investigators: Furong Huang (PI), Dana Dachman-Soled (co-PI), Min Wu (co-PI)
Source of Support: NSF and Amazon
Total Award Amount: $1,000,000 (my share: $333,333) split between NSF ($625,000) and Amazon ($375,000)
Total Award period Covered: 02/01/2022-01/31/2025
Location of Project: University of Maryland, College Park

Joint Fairness and Privacy Design for Financial Machine Learning Algorithms
Investigators: Dana Dachman-Soled (PI), Min Wu (co-PI)
Source of Support: JPMorgan
Total Award Amount: $120,000 (my share: $60,000)
Total Award period Covered: 08/01/2021-07/31/2022
Location of Project: University of Maryland, College Park

SaTC: CORE: Small: Meta Coding and Applications in Cryptography
Investigators: Dana Dachman-Soled (PI)
Source of Support: NSF
Total Award Amount: $500,000
Total Award period Covered: 09/01/2019-08/31/2022
Location of Project: University of Maryland, College Park

Foundations for Next-Generation Cryptographic Standards
Investigators: Jonathan Katz (PI), Dana Dachman-Soled (co-PI), Babis Papamanthou (co-PI)
Source of Support: NIST
Total Award Amount: $600,000 (my share: $200,000)
Total Award period Covered: 09/01/2019-08/31/2021
Location of Project: University of Maryland, College Park

Mitigating Reverse Engineering Attacks on Deep Neural Networks
Investigators: Ankur Srivastava (PI), Dana Dachman-Soled (co-PI)
Source of Support: Northrop Grumman/UMD
Total Award Amount: $53,000
Total Award period Covered: 02/01/2019-01/31/2020
Location of Project: University of Maryland, College Park

Faithfulness, Side-Channels, and Anonymity in Lattice-Based Cryptosystems
Investigator: Dana Dachman-Soled (PI)
Source of Support: Cisco Systems, Incorporated

Total Award Amount: $76,914
Total Award period Covered: 10/17/2018-10/16/2019
Location of Project: University of Maryland, College Park

EAGER: SaTC: Post-Quantum Indifferentiability
Investigator: Dana Dachman-Soled (PI)
Source of Support: NSF
Total Award Amount: $100,000
Total Award period Covered: 10/1/2018-09/30/2019
Location of Project: University of Maryland, College Park

Analyzing the Side-Channel Resistance of Lattice-Based Key Exchange
Investigator: Dana Dachman-Soled (PI)
Source of Support: Cisco Systems, Incorporated
Total Award Amount: $75,525
Total Award period Covered: 05/31/2017-05/30/2018
Location of Project: University of Maryland, College Park

Analyzing the Robustness of Lattice-Based Schemes Against Side-Channel Attacks
Investigators: Dana Dachman-Soled (PI)
Source of Support: Cisco Systems, Incorporated
Total Award Amount: $73,544
Total Award period Covered: 05/24/2016-05/23/2017
Location of Project: University of Maryland, College Park

Data Integrity for Dynamic Memory via Locally Decodable and Updatable Non-Malleable Codes
Investigator: Dana Dachman-Soled (PI)
Source of Support: UMD Research and Scholarship Grant (RASA)
Total Award Amount: $9,000
Total Award period Covered: 06/01/2016-07/31/2016
Location of Project: University of Maryland, College Park

Provable Security for Next-Generation Cryptography
Investigators: Jonathan Katz (PI), Dana Dachman-Soled (co-PI), Babis Papamanthou (co-PI)
Source of Support: NIST
Total Award Amount: $1,097,937 (my share: $362,319)
Total Award period Covered: 09/01/2015-08/31/2020 (with two year extension)
Location of Project: University of Maryland, College Park

Threat Models and Practical, Provably Secure Architecture for the Secure Scan-Chain Problem
Investigator: Dana Dachman-Soled (PI)
Source of Support: Matching funds from ORAU and UMD (Ralph E. Powe Junior Faculty Award)
Total Award Amount: $10,000
Total Award period Covered: 06/01/2015-05/31/2016
Location of Project: University of Maryland, College Park

CAREER: Non-Black-Box Cryptography: Defending Against and Benefiting from Access to Code
Investigator: Dana Dachman-Soled (PI)

Source of Support: NSF
Total Award Amount: $495,000
Total Award period Covered: 03/15/2015-03/14/2020
Location of Project: University of Maryland, College Park

Cryptography in Diverse Models: Physical Security and Adaptive Security
Investigator: Dana Dachman-Soled (PI)
Source of Support: Minta Martin Research Fund
Total Award Amount: $75,000
Total Award period Covered: 2015-2016
Location of Project: University of Maryland, College Park

II.K. Fellowships, Gifts and Other Funded Research

II.K.2. Gifts

New Tools for Concrete Security Analysis of LWE
with Applications to Post-Quantum and FHE Cryptosystems
Investigator: Dana Dachman-Soled (PI)
Source of Support: Intel
Total Award Amount: $270,000
Total Award period Covered: 06/15/2021-06/14/2024
Location of Project: University of Maryland, College Park

II.K.3. Other

Simons Institute for the Theory of Computing, supported by the Simons Foundation and by the DIMACS/Simons Collaboration in Cryptography through NSF grant #1523467
Investigator: Dana Dachman-Soled
Total Award Amount: $9,495 Total Award period Covered: June-August 2015

III. TEACHING, MENTORING AND ADVISING.

III.A. Courses Taught

Fall 2022: Computer Systems Security (ENEE 457), 35 students
Undergraduate Cryptography course. Course evaluation: TBD

Spring 2022: Cryptography (ENEE/CMSC/MATH456), 50 students enrolled as of 2/2/2022
Undergraduate Cryptography course. Course evaluation: TBD

Fall 2021: Computer Systems Security (ENEE 457), 56 students
Undergraduate Cryptography course. Course evaluation: 3.3

Fall 2020: Computer Systems Security (ENEE 457), 46 students
Undergraduate Cryptography course. Course evaluation: 3.7

Spring 2020: Cryptography (ENEE/CMSC/MATH456), 53 students
Undergraduate Cryptography course.

Fall 2019: Computer Systems Security (ENEE 457), 35 students
Undergraduate Cryptography course. Course evaluation: 3.5

Spring 2019: Cryptography (ENEE/CMSC/MATH456), 38 students
Undergraduate Cryptography course. Course evaluation: 3.30

Spring 2018: Introduction to Cryptology (ENEE459E/CMSC498R), 30 students
Undergraduate Cryptography course. Course evaluation: 3.6

Fall 2017: Computer Systems Security (ENEE 457/CMSC 498E), 56 students
Undergraduate Computer Security course. Course evaluation: 3.28

Spring 2017: Introduction to Cryptology (ENEE459E/CMSC498R), 34 students
Undergraduate Cryptography course. Course evaluation: 3.71

Spring 2016: Introduction to Cryptology (ENEE459E/CMSC498R), 39 students
Undergraduate Cryptography course. Course evaluation: 3.57

Fall 2015: Digital Logic (ENEE 244), 63 students
Undergraduate 200-level required course. Course evaluation: 3.23

Spring 2015: Introduction to Cryptology (ENEE459E/CMSC498R), 34 students
Undergraduate Cryptography course. Course evaluation: 3.45

Fall 2014: Digital Logic (ENEE 244), 50 students
Undergraduate 200-level required course. Course evaluation: 3.18

Spring 2014: Introduction to Cryptology (ENEE459E/CMSC498R), 35 students
Undergraduate Cryptography course. Course evaluation: 3.02

Fall 2013: Cryptography Against Physical Attacks (ENEE759O/CMSC858T), 6 students
Graduate special topics course in Cryptography. Course evaluation: 3.40

III.B. Teaching Innovations
III.B.5. Course or Curriculum Development

Theoretical Foundations of Computer Engineering (ENEE 351)
This course is now titled "Algorithms and Data Structures." It was developed together with faculty from the CE group for the new Computer Engineering minor.

Introduction to Cryptology (ENEE459E/CMSC498R)
New undergraduate course in Cryptography. This course has now been given a permanent course number (ENEE 456) and is cross-listed with CMSC/MATH 456. Significant innovations in teaching

methods and course materials involved.

Cryptography Against Physical Attacks (ENEE759O/CMSC858T)
This is a graduate, special topics course that focuses on cryptographic security against side-channel and tampering attacks.

III.C. Advising: Research or Clinical

III.C.1. Undergraduate

Led projects as part of the REU-CAAR program at University of Maryland in Summers 2017, 2018, and 2022 with a total of 7 undergraduate and 3 high school students. Of the undergraduate students, two were female, one was an underrepresented minority, and two were returning students. Led projects with a total of 7 ACES students. Ben SanNicolas is co-author on a paper posted on ePrint. Kevin Kulda and Michael Davinroy are co-authors on a paper posted on arXiv.

- Jeremy Krach, Summer 2014 (ACES student, advisor)
- Grant Orndorf, Summer 2014 (ACES student, advisor)
- Monica Katzen, Fall 2014-Spring 2015 (ACES student, advisor)
- Justin Vernick, Fall 2014 (ACES student, advisor)
- Lev Gorbunov, Spring 2015 (RISE student, advisor)
- Thomas Anthony Rubino, Spring 2015 (ACES student, advisor)
- Mihir Yavalkar, Spring 2015 (ACES student, advisor)
- Ben SanNicolas, Fall 2015 (ACES student, advisor)
- Robert Metzger, Summer 2017 (REU advisor)
- Shir Maimon, Summer 2017 (REU advisor)
- Laura Sullivan-Russett, Summer 2017 (REU advisor)
- Kevin Kulda, Summer 2018 (REU advisor)
- Michael Davinroy, Summer 2018 and 2019 (REU advisor in 2018)
- Mahammad Shirinov, Summer 2019
- Alex Lindenbaum, Summer 2022 (REU advisor)
- Michael Gonzalez, Summer 2022 (REU advisor)

III.C.2. Master's

- Nithin Bhardwaj, Summer 2018–Spring 2019 (GRA)
- Gregory Coard, Fall 2015-Spring 2017 (advisor)
- Lambros Mertzanis, Fall 2019-Spring 2021 (advisor)

III.C.3. Doctoral

I have co-advised one graduated PhD student, Aishwarya Thiruvengadam (first position, postdoctoral fellow at UCSB) and solely advised three graduated PhD students, Mukul Kulkarni (first position, postdoctoral fellow at UMass Amherst), Huijing Gong (first position Intel Labs), and Aria Shahverdi (first position Google). I am currently advising PhD students Hunter Kippen (Clark Doctoral Fellow) and Tom Hanson.

- Mukul Kulkarni, Fall 2014–Summer 2019 (advisor) (first position: postdoc at UMass Amherst)
- Aria Shahverdi, Future Faculty Fellow, Fall 2015–Spring 2022 (advisor) (first position: Google)
- Aishwarya Thiruvengadam, Spring 2016-Summer 2017 (advisor, co-advised with Prof. Jonathan Katz) (first position: postdoc at UCSB)
- Huijing Gong, Fall 2017–Spring 2021 (advisor) (first position: Intel Labs)
- Hunter Kippen, Clark Doctoral Fellow, Fall 2019–present (advisor)
- Tom Hanson, Fall 2020–present (advisor)

III.C.4. Post-doctoral

- Feng-Hao Liu, Fall 2014-Spring 2015 (first position: assistant prof at Florida Atlantic University)
- Jacob Alperin-Sheriff, Fall 2015-Spring 2016 (first position: researcher at NIST)

III.C.5. Other Research Directions (K-12 Interactions)
High school student Angela Park submitted her project to the Intel competition, where it received the research report award. She is co-author of a paper posted on ePrint. High school students Stuart Nevans Locke and Ian Rackow are co-authors on a paper posted on arXiv.

- Angela Park, Spring 2015 (junior at Montgomery Blair High School for math, science and computer science magnet program)
- Stuart Nevans Locke, Summers 2017 and 2018 (student at Montgomery Blair High School for math, science and computer science magnet program)
- Ian Rackow, Summer 2018 (student at Montgomery Blair High School for math, science and computer science magnet program)
- Justin Zhang, Summer 2019 (student at Montgomery Blair High School for math, science and computer science magnet program)
- Se Yong Park, Summer 2019 (student at Montgomery Blair High School for math, science and computer science magnet program)
- Anna Weisman, Summer 2019 (student at Yeshiva of Greater Washington, Girls' Division)
- Maya Kotek, Summer 2019 (student at Yeshiva of Greater Washington, Girls' Division)
- Harikesh Kailad, Summer 2022 (student at Montgomery Blair High School for math, science and computer science magnet program)

IV. SERVICE AND OUTREACH

IV.A. Editorships, Editorial Boards, and Reviewing Activities
IV.A.3. Reviewing Activities for Journals and Presses

- Journal of Cryptology
- ACM Transactions on Computation Theory
- SIAM Journal on Computing (SICOMP)

IV.A.4 4. Reviewing Activities for Agencies and Foundations

- NSF CCF Panelist, 2018

- NSF SaTC Panelist, 2019
- Israel Science Foundation Reviewer, 2014 and 2016

IV.A.5. Reviewing Activities for Conferences

STOC 2021, CRYPTO 2020, ASIACRYPT 2019, CRYPTO 2019, STOC 2019, TCC 2018, ICML 2018, EUROCRYPT 2018, EUROCRYPT 2016, CRYPTO 2015, ICALP 2015, TCC 2015, PKC 2015, SCN 2014, ASIACRYPT 2014, CRYPTO 2014, STOC 2014, EUROCRYPT 2014, PKC 2014, 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.

IV.B.6. Offices and Committee Memberships

- STOC 2023 Program Committee member
- Eurocrypt 2022 Program Committee member
- Asiacrypt 2021 Program Committee member
- PKC 2020 Program Committee member
- ISC 2019 Program Committee member
- Emerging Technologies track at Grace Hopper Celebration 2019 Program Committee member
- TCC 2019 Program Committee member
- Eurocrypt 2019 Program Committee member
- Crypto 2018 Program Committee member
- PKC 2018 Program Committee member
- TCC 2017 Program Committee member
- Crypto 2017 Program Committee member
- PKC 2017 Program Committee member
- NDSS 2017 Program Committee member
- CCS 2016 Program Committee member
- PKC 2016 Program Committee member
- TCC 2016-A Program Committee member
- Crypto 2013 Program Committee member
- SCN 2012 Program Committee member

IV.B.7. Leadership Roles in Meetings and Conferences

- Program Chair of Conference on Information-Theoretic Cryptography (ITC) 2022.
- Led one of three cyber groups in the Women in Mathematics and Public Policy (WPOL) workshop held at IPAM/Luskin Center at UCLA in January 2019. This workshop was organized by the RAND Corporation, public policy think tank, and UCLA's Institute for Pure and Applied

Mathematics. It was partially supported by NSF-HRD 1500481–AWM ADVANCE grant. Beginning in June 2017 I was substantially involved in the writing of the proposal that obtained the funding for this workshop.

- Co-organized International Workshop on Cyber Deception and Defenses 2018 at University of Maryland. This workshop was an ARO-funded workshop whose goal was to bring together experts on Cyber Deception from academia, industry, government, and funding agencies.
- Served as the Session Chair for the "Multiparty Computation" session at Crypto 2017.
- Served as the Session Chair for the "MPC Tools" session at TCC 2017.

IV.F Community & Other Service

- Gave a presentation for "Career Awareness Week" at Yeshiva of Greater Washington, an all-girls' high school, December 2018.
- Visited 4th and 5th grades at Leo Bernstein Jewish Academy of Fine Arts to give a hands-on presentation about cryptography, February 2018.
- Participated in "Hour of Code" at Yeshiva of Greater Washington, an all-girls' high school, December 2017.

V. AWARDS, HONORS AND RECOGNITION

V.1. Research Fellowships, Prizes and Awards

- Summer 2016 Research and Scholarship Award (RASA) (2016)
- Ralph E. Powe Junior Faculty Enhancement Award (2015-2016)
- NSF Faculty Early Career Development (CAREER) Award (2015-2020)
- 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)

V.2 Teaching Awards

- George Corcoran Award for Faculty (2018)

V.5 Other Special Recognition

- Participant in NSF CISE invite-only workshop on broadening participation in computing (BPC) in 2018 (CISE BPCnet Workshop)
- Invited to Simons Institute at UC Berkeley as a visiting researcher in Summer 2015
- Invited to Rising Stars of EECS workshop at MIT in 2012 as one of two selected speakers
- Visiting researcher in Cryptography group at IBM Research, Hawthorne in Summer 2010