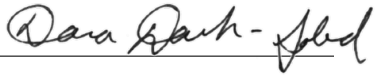
DANA (GLASNER) DACHMAN-SOLED

CURRICULUM VITAE

Notarization. I have read the following and certify that this curriculum vitae is a current and accurate statement of my professional record.

Signature  Date 7/24/26

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@umd.edu
Webpage: `https://user.eng.umd.edu/~danadach/`

I.B. Academic Appointments at UMD

Professor
Department of Electrical and Computer Engineering and UMIACS, July 2026–present
Core member of the *Maryland Cybersecurity Center (MC2)*

Associate Professor
Department of Electrical and Computer Engineering and UMIACS, July 2020–June 2026
Core member of the *Maryland Cybersecurity Center (MC2)*

Assistant Professor
Department of Electrical and Computer Engineering and UMIACS, August 2013–June 2020
Core member of the *Maryland Cybersecurity Center (MC2)*

Affiliate
Department of Computer Science, November 2013–present

Affiliate
Institute for Systems Research (ISR), July 2020–present

Affiliate
Applied Mathematics & Statistics, and Scientific Computation (AMSC) Program, October 2025–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 6/22/2026): Total Citations: 2802; h-index: 31; i10-index: 55 (Note: Google Scholar does not provide citation reports without self-citations). Link: `https://scholar.google.com/citations?user=Ss009KUAAAAJ&hl=en`

ORCID: `https://orcid.org/0000-0001-6797-641X`

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

In the field of cryptography, author ordering is typically in alphabetical order. Publications that are *not* alphatbetically ordered are marked with a †.

II.C. Articles in Refereed Journals

J-18. G. Alagic, **D. Dachman-Soled**, M. Shingane, P. Struck. "Quantum Black-Box Separations: Succinct Non-Interactive Arguments from Falsifiable Assumptions." Communications in Cryptology (CiC), vol. 2, no. 4 (2026).

Available here: `https://doi.org/10.62056/ayfhp2w9p`

J-17. †Z. Lazri, D. Dervovic, A. Polychroniadou, I. Brugere, **D. Dachman-Soled**, F. Huang, M. Wu. "Balancing Fairness and Accuracy in Data-Restricted Binary Classification." ACM Transactions on Knowledge Discovery from Data, 2025.

Available here: `https://doi.org/10.1145/3747850`

J-16. †#M. Liang, S.G. Choi, **D. Dachman-Soled**, L. Liu, A. Yerukhimovich. "On the Privacy of Sublinear-Communication Jaccard Index Estimation via Min-hash." Communications in Cryptology (CiC), vol. 1, no. 4 (2025).

Available here: `https://doi.org/10.62056/ak2i5w7sf`

J-15. †Z. Lazri, I. Brugere, X. Tian, **D. Dachman-Soled**, A. Polychroniadou, D. Dervovic, M. Wu. "A Canonical Data Transformation for Achieving Inter-and Within-group Fairness." IEEE Transactions on Information Forensics and Security, vol. 19, pp. 7449-7464 (2024).

Available here: https://doi.org/10.1109/TIFS.2024.3416040

J-14. **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 (2020).

Available here: https://doi.org/10.1515/jmc-2020-0075

J-13. **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 (2020).

Available here: https://doi.org/10.1515/jmc-2020-0076

J-12. **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 (2020).

Available here: https://doi.org/10.1007/978-3-030-58748-2_6

J-11. †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 (2020).

Available here: https://doi.org/10.1007/978-3-030-58748-2_4

J-10. **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).

Available here: https://doi.org/10.1007/s00145-019-09329-9

J-9. **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).

Available here: https://doi.org/10.1016/j.ic.2019.05.001

J-8. **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).

Available here: https://doi.org/10.1007/s00145-018-9306-z

J-7. **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).

Available here: https://doi.org/10.1007/s00145-018-9301-4

J-6. **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).

Available here: https://doi.org/10.1007/s00145-018-9286-z

J-5. 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).

Available here: https://doi.org/10.1007/s00145-017-9254-z

J-4. 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).

Available here: `https://doi.org/10.1007/s10623-017-0348-2`

J-3. **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).

Available here: `http://doi.org/10.1007/978-3-642-01957-9_8`

J-2. **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).

Available here: `http://doi.org/10.4086/toc.2009.v005a013`

J-1. **D. Glasner**, R. Servedio. "Distribution-Free Testing Lower Bounds for Basic Boolean Functions." Theory of Computing 5(1), pp. 191-216 (2009).

Available here: `http://doi.org/10.4086/toc.2009.v005a010`

II.D. Published Conference Proceedings

II.D.1. Refereed Conference Proceedings

"AR" stands for "acceptance rate" below.

Conferences designated as "top-tier" are marked with a ** (we consider "top-tier" conferences to be those counted by `https://csrankings.org`). Total of 25 top-tier conference publications out of 66 total conference publications. Since starting at UMD in Summer 2013, 24 top-tier conference publications out of 49 conference publications.

C-66. [**ICML] †#Y. Zhou, #M. Liang, I. Brugere, D. Dervovic, Y. Guo, A. Polychroniadou, M. Wu, **D. Dachman-Soled**. "Revisiting ML Training under Fully Homomorphic Encryption: Convergence Guarantees, Differential Privacy, and Efficient Algorithms." Proceedings of the 43rd International Conference on Machine Learning (ICML), 2026, to appear. (AR = 6,352/23,918 = 0.266)

Pre-print available here: `https://arxiv.org/abs/2605.27782`

C-65. [**ICML] †Z. Lazri, A. Nakra, I. Brugere, D. Dervovic, A. Polychroniadou, F. Huang, **D. Dachman-Soled**, M. Wu. "MAFE: Enabling Equitable Algorithm Design in Multi-Agent Multi-Stage Decision-Making Systems." Proceedings of the 43rd International Conference on Machine Learning (ICML), 2026, to appear. (AR = 6,352/23,918 = 0.266)

Pre-print available here: `https://arxiv.org/abs/2502.18534`

C-64. [**Crypto] M. Ball, **D. Dachman-Soled**. "Uniform Black-Box Separations via Non-Malleable Extractors." 45th Annual Cryptology Conference (CRYPTO) 2025, pp. (585-616). (AR = 154/658 = 0.23)

Available here: `https://doi.org/10.1007/978-3-032-01855-7_19`

C-63. [PKC] F. Bergamaschi, A. Costache, **D. Dachman-Soled**, #H. Kippen, #L. LaBuff, #R. Tang. "Revisiting the Security of Approximate FHE with Noise-Flooding Countermeasures." IACR International Conference on Public-Key Cryptography (PKC) 2025, pp. 102-134. (AR = 60/201 = 0.30)

Available here: `https://doi.org/10.1007/978-3-031-91832-2_4`

C-62. [**Eurocrypt] M. Ball, **D. Dachman-Soled**. "(Inefficient Prover) ZAPs from Hard-to-Invert Functions." 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt) 2025, pp. 274–302. (AR = 122/607 = 0.20)

Available here: `https://doi.org/10.1007/978-3-031-91134-7_10`

C-61. [ITC] **D. Dachman-Soled**, J. Loss, A. O'Neill. "Breaking RSA Generically is Equivalent to Factoring, with Preprocessing." 5th Conference on Information-Theoretic Cryptography (ITC) 2024, 8:1–8:24. (AR = 11/21 = 0.52)

Available here: `https://doi.org/10.4230/LIPIcs.ITC.2024.8`

C-60. [**ICML] †#Y. Zhou, #M. Liang, I. Brugere, D. Dervovic, A. Polychroniadou, M. Wu, **D. Dachman-Soled**. "Bounding the Excess Risk for Linear Models Trained on Marginal-Preserving, Differentially-Private, Synthetic Data." Proceedings of the 41st International Conference on Machine Learning (ICML), 235:61979-62001, 2024. (AR = 2,609/9,473 = 0.275)

Available here: `https://dl.acm.org/doi/10.5555/3692070.3694635`

C-59. [**FOCS] M. Ball, **D. Dachman-Soled**, E. Goldin, S. Mutreja. "Extracting Randomness from Samplable Distributions, Revisited." 64th IEEE Annual Symposium on Foundations of Computer Science (FOCS) 2023, pp. 1505-1514. (AR = 141/421 = 0.33)

Available here: `https://doi.org/10.1109/FOCS57990.2023.00092`

C-58. [**Crypto] **D. Dachman-Soled**, #H. Gong, #T. Hanson, #H. Kippen. "Revisiting Security Estimation for LWE with Hints from a Geometric Perspective." 43rd Annual Cryptology Conference (CRYPTO) 2023, pp. (748-781). (AR = 124/479 = 0.26)

Available here: `https://doi.org/10.1007/978-3-031-38554-4_24`

C-57. [TCC] 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 (II), pp. 348-377. (AR = 60/139 = 0.43)

Available here: `https://doi.org/10.1007/978-3-031-22365-5_13`

C-56. [**CCS] †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, pp. 979-993. (AR = 218/971 = 0.22)

Available here: `https://doi.org/10.1145/3548606.3560673`

Best paper honorable mention

C-55. [**Crypto] M. Ball, **D. Dachman-Soled**, J. Loss. "(Nondeterministic) Hardness vs. Non-Malleability." 42nd Annual Cryptology Conference (CRYPTO) 2022 (I), pp. 148-177. (AR = 100/455 = 0.22)

Available here: `https://doi.org/10.1007/978-3-031-15802-5_6`

C-54. [TCC] **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)

Available here: `https://doi.org/10.1007/978-3-030-90453-1_23`

C-53. [**CCS] 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)

Available here: https://doi.org/10.1145/3460120.3484792

C-52. [**Crypto] **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)

Available here: https://doi.org/10.1007/978-3-030-84252-9_18

C-51. [**USENIX]†#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.

Available here: https://www.usenix.org/system/files/sec21-shahverdi.pdf

C-50. [TCC] **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)

Available here: https://doi.org/10.1007/978-3-030-64378-2_21

C-49. [**Crypto] **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)

Available here: https://doi.org/10.1007/978-3-030-56880-1_12

17th most cited paper from the Crypto conference over the last 5 years.

C-48. [**Crypto] 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)

Available here: https://doi.org/10.1007/978-3-030-56877-1_24

C-47. [PETS] 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)

Available here: https://doi.org/10.2478/popets-2020-0047

C-46. [**ICLR] †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)

Available here: https://openreview.net/pdf?id=S1erpeBFPB

C-45. [CT-RSA] 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)

Available here: https://doi.org/10.1007/978-3-030-40186-3_11

C-44. [ITCS] 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)

Available here: https://doi.org/10.4230/LIPIcs.ITCS.2020.80

C-43. [ISVLSI] †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)

Available here: http://dx.doi.org/10.1109/ISVLSI.2019.00122

C-42. [**Eurocrypt] 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)

Available here: https://doi.org/10.1007/978-3-030-17653-2_17

C-41. [PQCrypto] 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 = 22/76 = 0.29)

Available here: http://dx.doi.org/10.1007/978-3-030-25510-7_11

C-40. [PKC] **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)

Available here: https://doi.org/10.1007/978-3-030-17253-4_18

C-39. [**FOCS] 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)

Available here: https://doi.org/10.1109/FOCS.2018.00083

C-38. [**Eurocrypt] M. Ball, **D. Dachman-Soled**, #M. Kulkarni, T. Malkin. "Non-Malleable Codes from Average-Case Hardness: AC^0, 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)

Available here: https://doi.org/10.1007/978-3-319-78372-7_20

C-37. [PKC] **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)

Available here: https://doi.org/10.1007/978-3-319-76581-5_10

C-36. [PKC] **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)

Available here: https://doi.org/10.1007/978-3-662-54365-8_13

C-35. [TCC] **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)

Available here: https://doi.org/10.1007/978-3-662-53644-5_7

C-34. [**Eurocrypt] 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)

Available here: https://doi.org/10.1007/978-3-662-49896-5_31

C-33. [**Eurocrypt] **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)

Available here: https://doi.org/10.1007/978-3-662-49896-5_23

C-32. [PKC] **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)

Available here: https://doi.org/10.1007/s00145-018-9286-z

C-31. [CT-RSA] 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)

Available here: https://doi.org/10.1007/978-3-319-29485-8_10

C-30. [Asiacrypt] **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)

Available here: https://doi.org/10.1007/s00145-018-9301-4

C-29. [**Eurocrypt] **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)

Available here: https://doi.org/10.1007/978-3-662-46803-6_5

C-28. [TCC] **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)

Available here: https://doi.org/10.1007/s00145-018-9306-z

C-27. [TCC] **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)

Available here: https://doi.org/10.1007/978-3-662-46497-7_23

C-26. [**SODA] **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)

Available here: https://doi.org/10.1137/1.9781611973730.34

C-25. [**Crypto] **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)

Available here: https://doi.org/10.1007/978-3-662-44381-1_23

C-24. [**Crypto] 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)

Available here: https://doi.org/10.1007/978-3-662-44381-1_9

C-23. [PKC] **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)

Available here: https://doi.org/10.1007/978-3-642-54631-0_3

C-22. [PKC] **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)

Available here: https://doi.org/10.1007/978-3-642-54631-0_33

C-21. [PKC] **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)

Available here: https://doi.org/10.1007/978-3-642-54631-0_19

C-20. [TCC] **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)

Available here: https://doi.org/10.1007/978-3-642-54242-8_23

C-19. [TCC] **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)

Available here: https://doi.org/10.1007/978-3-642-54242-8_10

C-18. [Asiacrypt] **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)

Available here: https://doi.org/10.1007/978-3-642-42033-7_17

C-17. [TCC] 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)

Available here: https://doi.org/10.1007/978-3-642-36594-2_11

Merge of two papers. Un-merged version available here: https://eprint.iacr.org/2012/706

C-16. [SCN] 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)

Available here: https://doi.org/10.1007/978-3-642-32928-9_15

C-15. [**Crypto] **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)

Available here: https://doi.org/10.1007/978-3-642-32009-5_31

C-14. [PKC] 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)

Available here: https://doi.org/10.1007/978-3-642-30057-8_27

C-13. [TCC] **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)

Available here: https://doi.org/10.1007/978-3-642-28914-9_22

C-12. [RANDOM] **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)

Available here: https://doi.org/10.1007/978-3-642-22935-0_39

C-11. [ACNS] **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)

Available here: https://doi.org/10.1007/978-3-642-21554-4_8

C-10. [TCC] **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)

Available here: https://doi.org/10.1007/978-3-642-19571-6_27

C-9. [Asiacrypt] 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)

Available here: https://doi.org/10.1007/978-3-642-10366-7_17

C-8. [ACNS] **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)

Available here: https://doi.org/10.1007/978-3-642-01957-9_8

C-7. [TCC] 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)

Available here: https://doi.org/10.1007/978-3-642-00457-5_23

C-6. [ICALP] **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)

Available here: https://doi.org/10.1007/978-3-540-70575-8_4

C-5. [TCC] 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)

Available here: https://doi.org/10.1007/978-3-540-78524-8_24

C-4. [RANDOM] **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)

Available here: https://doi.org/10.1007/978-3-540-74208-1_36

C-3. [SCC] **D. Glasner**, V.C. Sreedhar. "Configuration Reasoning and Ontology For Web." IEEE International Conference on Services Computing (SCC), 2007, pp. 384-394.

Available here: `https://doi.org/10.1016/j.eswa.2008.05.026`

C-2. [AIP] **D. Glasner**, A.I. Frenkel. "Geometrical characteristics of regular polyhedra: Application to EXAFS studies of nanoclusters." AIP Conf. Proc. 882, pp. 746-748 (2007).

Available here: `https://doi.org/10.1063/1.2644651`

C-1. [AIP] 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).

Available here: `https://doi.org/10.1063/1.2644652`

II.E. Conferences, Workshops, and Talks

II.E.2. Invited Talks

Workshop on Security of Edge Devices in the Post Quantum Era, College Park, MD
"An Introduction to Post-Quantum Cryptography: Beyond RSA and Diffie-Hellman." July 2026.

Johns Hopkins University Applied Physics Laboratory (APL) (Online Talk)
"Applied Research Challenges in PQC, FHE, and PPML." June 2026.

Booz-Allen Hamilton ECE Colloquium, College Park, MD "A Survey of Results in Modern Cryptography: Beyond RSA and Diffie-Hellman." September 2025.

Third Intel Crypto Frontiers Center Workshop, Hillsboro, OR (Online Talk)
"Recent Applications of the LWE Toolkit to Post-Quantum and FHE Settings." October 2024.

Second Intel Crypto Frontiers Center Workshop, Hillsboro, OR (Online Talk)
"Recent Applications of the LWE Toolkit to Post-Quantum and FHE Settings." October 2023.

REU-CAAR, REU-BRIDGE, REU-Math Joint Seminar, College Park, MD
"Computer Security 101: A Whirlwind Tour." July 2023.

Simons Workshop on Minimal Complexity Assumption for Cryptography (Online talk)
"New Techniques for Zero-Knowledge: Leveraging Inefficient Provers to Reduce Assumptions, Interaction, and Trust." May 2023.

First Intel Crypto Frontiers Center Workshop, Hillsboro, OR
"Refined Security Estimation for LWE with Hints via a Geometric Approach." September 2022.

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.4. Refereed Workshop Papers

W-5. S.G. Choi, **D. Dachman-Soled**, #M. Liang, L. Liu, A. Yerukhimovich. "On the Privacy of Sublinear-Communication Jaccard Index Estimation via Min-hash Sketching." Theory and Practice of Differential Privacy Workshop (TPDP) 2024.

W-4. †M. Fahr Jr., #H. Kippen, A Kwong, T. Dang, J. Lichtinger, **D. Dachman-Soled**, D. Genkin, A.H. Nelson, R. Perlner, A. Yerukhimovich, D. Apon. "When Frodo Flips: End-to-End Key Recovery on FrodoKEM via Rowhammer." Real World Crypto (RWC) 2023.

W-3. †#Y. Zhou, I. Brugere, **D. Dachman-Soled**, D. Dervovic, #M. Liang, A. Polychroniadou, M. Wu. "Bounding the Accuracy Loss for Graphical Model Based Synthetic Data Generation in Privacy-Preserving Machine Learning." CRYPTO Privacy-Preserving Machine Learning Workshop (PPML) 2023.

W-2. **D. Dachman-Soled**, #H. Gong, #M. Kulkarni, #A. Shahverdi. "Towards a Ring Analogue of the Leftover Hash Lemma." Mathcrypt 2019.

W-1. **D. Dachman-Soled**, #H. Gong, #M. Kulkarni, #A. Shahverdi. "(In)Security of Ring-LWE Under Partial Key Exposure." Mathcrypt 2019.

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.F. Professional Publications

II.F.1. Reports and Non-Refereed Monographs

PP-4. **D. Dachman-Soled**, E. Ghosh, #M. Liang, I. Miers, M. Rosenberg. "Anonymous Outsourced Statekeeping with Reduced Server Storage." Cryptology ePrint Archive, Report 2024/1139. (2024)

Available here: `https://eprint.iacr.org/2024/1139`

PP-3. S. Hong, #M. Davinroy, Y. Kaya, #S.N. Locke, #I. Rackow, #K. Kulda, **D. Dachman-Soled**, T. Dumitras. "Security Analysis of Deep Neural Networks Operating in the Presence of Cache Side-Channel Attacks." CoRR abs/1810.03487. (2018) *Project with REU and high school students.*

Available here: `https://arxiv.org/abs/1810.03487`

PP-2. **D. Dachman-Soled**, #A. Park, #B. San Nicolas. "Towards a Characterization of the Related-Key Attack Security of the Iterated Even-Mansour Cipher." IACR Cryptology ePrint Archive, Report 2016/707. (2016) *Project with ACES (Honor's College Advanced Cybersecurity Experience for Students) and high school student.*

Available here: `https://eprint.iacr.org/2016/707`

PP-1. **D. Dachman-Soled**, A. Jain, Y.T. Kalai, #A. López-Alt. "On the (In)security of the Fiat-Shamir Paradigm, Revisited." Cryptology ePrint Archive, Report 2012/706. (2012) *Paper merged for publication (see Section II.D.1 C-17).*

Available here: `https://eprint.iacr.org/2012/706`

II.K. Sponsored Research and Programs–Administered by the Office of Research Administration (ORA)

I have been PI or co-PI on grants and gifts totaling $6,298,739 (with $5,998,739 going towards University of Maryland, College Park), with my share being $3,345,310. I have been sole PI on grants and gifts totaling $1,684,983.

II.K.1. Grants

Collaborative Research: AF: NSF-BSF: Beyond Information-Theoretic Limits: Randomness Extraction and Coding Against Computational Adversaries
Investigators: Dana Dachman-Soled (PI, UMD), Marshall Ball (PI, NYU)
Source of Support: NSF
Total Award Amount: $600,000 (my share: $300,000)
Total Award period Covered: 08/01/2026-07/31/2029
Location of Project: University of Maryland, College Park

Collaborative Research: Conference: 2025 Workshop for Aspiring PIs in Secure and Trusted Cyberspace
Investigators: Micelle Mazurek (PI), Dana Dachman-Soled (co-PI)
Source of Support: NSF
Total Award Amount: $62,419 (my share: $31,209)
Total Award period Covered: 07/15/2025-07/14/2026
Location of Project: University of Maryland, College Park

An Integrated Approach to Long-Term Fairness and Privacy in ML
Investigators: Dana Dachman-Soled (PI), Min Wu (co-PI)
Source of Support: JPMorgan
Total Award Amount: $80,000 (my share: $40,000)
Total Award period Covered: 01/01/2025-12/31/2025
Location of Project: University of Maryland, College Park

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: 07/28/2022-07/31/2026

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: Split between NSF and Amazon
Total Award Amount: $1,000,000 (my share: $333,333)
Total Award period Covered: 02/01/2022-01/31/2026
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.L. Gifts and Funded Research not administered by ORA

II.L.1. 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: funds received in 06/2021 and do not expire
Location of Project: University of Maryland, College Park

II.L.4. 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

II.N. Patents

II.N.2. Other

P-2. **D. Dachman-Soled**, I. Komargodski, R. Pass. "Tamper-resistant data encoding secure against unbounded polynomial size attack complexity." US Patent Number: 12244687. Filing date: 06/22/2021. Application granted: 03/04/2025.

P-1. V.C. Sreedhar, **D. Glasner**. "Method and Apparatus for configuration modeling and consistency checking of Web applications." US Patent Application Number: 11620143 (patent application only). Filing date: 01/05/2007.

II.Q. Research Fellowships, Prizes, Awards, and Honors

- JPMorgan Faculty Research Award (2021 and 2024)
- CCS 2022 Best Paper Honorable Mention
- Selected as one of 5 out of 23 invited proposals to participate in the Intel Cryptographic Frontiers Institute (2021-2024)
- Summer 2016 Research and Scholarship Award (RASA) (2016)
- Ralph E. Powe Junior Faculty Enhancement Award (2015-2016)
- Invited to Simons Institute at UC Berkeley as a visiting researcher in Summer 2015
- NSF Faculty Early Career Development (CAREER) Award (2015-2020)
- Invited to Rising Stars of EECS workshop at MIT in 2012 as one of two selected participant speakers
- Visiting researcher in Cryptography group at IBM Research, Hawthorne in Summer 2010
- 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)

III. TEACHING, MENTORING AND ADVISING.

III.A. Courses Taught

In addition to the courses listed below, I have been teaching the Computer Security module in the ENEE 101 course every semester since Fall 2021. This involves teaching one lecture per semester and developing two labs for the unit.

Cryptography (ENEE/CMSC/MATH456)
Description: Undergraduate Cryptography course.

Semester	S19	S20	S22	S23	S24	S25	S26
Enrollment	38	53	43	42	43	62	49
Course Eval	3.3	N/A	3.67	2.60	3.25*	3.23*	3.07*

* Course Eval is the average of all 15 questions provided in the instructor's report.

Computer Systems Security (ENEE 457)
Description: Undergraduate Computer Security course.

Semester	F17	F19	F20	F21	F22	F24
Enrollment	56	35	46	56	37	54
Course Eval	3.28	3.5	3.7	3.3	3.47	3.33*

* Course Eval is the average of all 20 questions provided in the instructor's report.

Introduction to Cryptology (ENEE459E/CMSC498R)
Description: Undergraduate Cryptography course.

Semester	S14	S15	S16	S17	S18
Enrollment	35	34	39	34	30
Course Eval	3.02	3.45	3.57	3.71	3.6

Digital Logic (ENEE 244)
Description: Undergraduate 200-level required course.

Semester	F14	F15
Enrollment	50	63
Course Eval	3.18	3.23

Cryptography Against Physical Attacks (ENEE759O/CMSC858T)
Description: Graduate special topics course in Cryptography.

Semester	F13
Enrollment	6
Course Eval	3.40

III.B. Teaching Innovations
III.B.6. Course or Curriculum Development

Introduction to Electrical & Computer Engineering (ENEE 101)
Created a new lab and made major modifications to a second lab, both for the cybersecurity module

of the course. Regularly give the cybersecurity lecture in the course.

Computer Systems Security (ENEE 457)
Made major modifications to the curriculum to make the ECE course more consistent with Computer and Network Security (CMSC 414). In addition, added an in-class, lab-based network security module to the course, added lecture-based modules on Bitcoin/Blockchain, Adversarial Machine Learning, and Differential Privacy.

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. Completed a Gemstones project in Spring '25 with 7 undergraduate students (including one underrepresented minority). Ben SanNicolas is co-author on a paper posted on ePrint (See Section II.F.1 PP-2). Kevin Kulda and Michael Davinroy are co-authors on a paper posted on arXiv with 123 citations as of 6/16/26 (see Section II.F.1 PP-3), Michael Davinroy is a co-author on a paper appearing at ICLR 2020 (See Section II.D C-46). Mahammad Shirinov is a co-author on a paper appearing at USENIX 2021 (See Section II.D C-51). Lucas LaBuff is a co-author on a paper to appear at PKC 2025 (See Section II.D C-63).

- Avital Pinsky, Summer 2026
- Harikesh Kailad, Spring 2023-Spring 2024.
- Alexander Yelovich, Spring 2023-Spring 2025 (Gemstones advisor)
- Avery Parker, Spring 2023-Spring 2025 (Gemstones advisor)
- Lucas LaBuff, Spring 2023-Spring 2025 (Gemstones advisor)
- Julian Javillo, Spring 2023-Spring 2025 (Gemstones advisor)
- Sahil Gaba, Spring 2023-Spring 2025 (Gemstones advisor)
- Ayman Chowdhury, Spring 2023-Spring 2025 (Gemstones advisor)
- Adnan Benchaaboun, Spring 2023-Spring 2025 (Gemstones advisor)
- Michael Gonzalez, Summer 2022 (REU advisor)
- Alex Lindenbaum, Summer 2022 (REU advisor)

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

III.C.2. Master's

- Brendan Zember, Fall 2025-Spring 2026–Master's with thesis
- Phuong Le, Fall 2022-Spring 2024 (advisor)–Master's with scholarly paper
- Lambros Mertzanis, Fall 2019-Spring 2021 (advisor)–Master's with scholarly paper
- Nithin Bhardwaj, Summer 2018–Spring 2019 (GRA)
- Gregory Coard, Fall 2015-Spring 2017 (advisor)–Master's with scholarly paper

III.C.3. Doctoral

I have co-advised one graduated PhD student, **Aishwarya Thiruvengadam** (first position, postdoctoral fellow at UCSB; currently Assistant Professor at IIT Madras) and solely advised four graduated PhD students, **Mukul Kulkarni** (first position, postdoctoral fellow at UMass Amherst; currently Lead Cryptographer at Technology Innovation Institute Abu Dhabi), **Huijing Gong** (first and current position Intel Labs), **Aria Shahverdi** (first and current position SoC Security Software Engineer at Google), and **Hunter Kippen** (first and current position Staff Engineer at Samsung Research America). I am currently advising three PhD students: Yvonne Zhou, Rui Tang, and Jinghan Wang. In total, 3 out of 8 of my past and present PhD students have been female.

- Jinghan Wang, Spring 2026–present (advisor).
- Russell Chiu, Fall 2023–Fall 2026 (advisor).
- Rui Tang, Spring 2023–present (advisor).
- Yvonne Zhou, Fall 2022–present (advisor).
- Hunter Kippen (PhD ECE 4/2024), Clark Doctoral Fellow, Fall 2019–Spring 2024 (advisor).
- Aria Shahverdi (PhD ECE 3/2022), Future Faculty Fellow, Fall 2015–Spring 2022 (advisor).
- Huijing Gong (PhD CS 4/2021), Fall 2017–Spring 2021 (advisor).
- Mukul Kulkarni (PhD ECE 7/2019), Fall 2014–Summer 2019 (advisor).

- Aishwarya Thiruvengadam (PhD CS 7/2017), Spring 2016-Summer 2017 (advisor, co-advised with Prof. Jonathan Katz).

III.C.4. Post-doctoral

- Natalie Lang, Fall 2025–present.
- Mingyu Liang, Spring 2023–Spring 2024 (first position: Snap).
- Jacob Alperin-Sheriff, Fall 2015–Spring 2016 (first position: researcher at NIST).
- Feng-Hao Liu, Fall 2014–Spring 2015 (first position: assistant prof at Florida Atlantic University).

III.C.5. Other Directed Research (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 (See Section II.F.1 PP-2). High school students Stuart Nevans Locke and Ian Rackow are co-authors on a paper posted on arXiv with 123 citations as of 6/16/26 (see Section II.F.1 PP-3).

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

III.H. Teaching Awards

- George Corcoran Award for Faculty (2018)

IV. SERVICE AND OUTREACH

IV.A. Editorships, Editorial Boards, and Reviewing Activities

IV.A.2. Editorial Boards

- IACR Communications in Cryptology (2024)

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, 2023, 2025
- Israel Science Foundation Reviewer, 2014 and 2016

IV.A.5. Reviewing Activities for Conferences

ITCS 2025, ISIT 2024, 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. Committees, Professional & Campus Service

IV.B.1. Campus Service – Department

- Departmental Council 2017–2019, 2020–2022, 2024–present
- Committee on Diversity, Equity, and Inclusion 2021–present
- Graduate Studies and Research Committee 2017-2018, 2022-2024
- MC2 Faculty Search Committee 2021-2022, 2022-2023
- Human Relations and Welfare Committee 2014-2015, 2020-2022
- Undergraduate Affairs Committee 2020–2022
- ECE Faculty Search Committee 2019-2020
- GAAC representative from Computer Engineering Group 2018–2020
- Facilities and Services Committee 2018–2020
- PhD Qualifying Exam Committee 2015–2019
- UMIACS APT (Appointment, Promotion, and Tenure) Committee 2016-2018
- MC2 Senior Hire Search Committee 2017
- ECE Strategic Planning Committee 2017
- UMIACS Retreat Committee on Publicity and Outreach 2014

I have served on the following PhD and Master's Thesis Committees:

- Alperen Keles (PhD thesis committee member, Summer 2026)
- Manasi Shingane (PhD thesis committee member, Summer 2026)
- Ali Ahad (PhD thesis committee member, Spring 2026)
- Kasra Abbaszadeh (PhD thesis committee member, Spring 2026)
- Isaac McDaniel (PhD thesis committee member, Spring 2025)
- Georgios Tsimos (PhD thesis committee member, Spring 2025)
- Doruk Gur (PhD thesis committee member, Spring 2025)
- Zachary Lazri (PhD thesis committee member, Spring 2025)

- Noemi Glaeser (PhD thesis committee member, Fall 2024)
- Erin Avllazagaj (PhD thesis committee member, Summer 2024)
- Michael Rosenberg (PhD thesis committee member, Spring 2024)
- Chen Bai (PhD thesis committee member, Spring 2024)
- Shravan Srinivasan (PhD thesis committee member, Spring 2023)
- Erica Blum (PhD thesis committee member, Spring 2023)
- Priya Mittu (Master's thesis committee member, Fall 2021)
- Sana Awan (Master's thesis committee member, Fall 2015)
- Mingliang Chen (PhD thesis committee member, Summer 2021)
- Shih-Han Hung (PhD thesis committee member, Summer 2021)
- Sanghyun Hong (PhD thesis committee member, Summer 2021)
- Abhishek Chakraborty (PhD thesis committee member, Spring 2021)
- Ioannis Demertzis (PhD thesis committee member, Summer 2020)
- Doowon Kim (PhD thesis committee member, Spring 2020)
- Yuntao Liu (PhD thesis committee member, Spring 2020)
- Danny Kim (PhD thesis committee member, Spring 2019)
- Yupeng Zhang (PhD thesis committee member, Summer 2018)
- Xiao Wang (PhD thesis committee member, Summer 2018)
- Xi Chen (PhD thesis committee member, Summer 2018)
- Yang Xie (PhD thesis committee member, Spring 2018)
- Daniel Apon (PhD thesis committee member, Summer 2017)
- Kristopher Micinski (PhD thesis committee member, Summber 2017)
- Chongxi Bao (PhD thesis committee member, Spring 2017)
- Carson Dunbar (PhD thesis committee member, Spring 2015)
- Vanishree Rao, UCLA (PhD thesis committee member, Summer 2015) (Also a visiting summer student in Summer 2014. First position: research scientist at PARC).

IV.B.2. Campus Service - College

- College APT/APPTK (Appointment, Promotion, and Tenure, Appointment and Promotion for Professional Track Faculty) Committee Member, Fall 2022–Spring 2024.

IV.B.3. Campus Service – University

- UMIACS Director Search Committee (Spring 2025)
- UMIACS Steering Committee member Fall 2022–Spring 2023
- UMIACS director review committee 2021-2022
- ACES Director Review Committee 2017

IV.B.9. Leadership Roles in Meetings and Conferences

- Co-Program Chair of the Theory of Cryptography Conference (TCC) 2026.
- Area chair, CRYPTO 2026
- Area Chair for the Information-Theoretic and Complexity-Theoretic Cryptography area, CRYPTO 2024.
- 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.B.10. Offices and Committee Memberships

- Eurocrypt 2026 Program Committee member
- ITC 2025 Program Committee member
- 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.C External Service and Consulting

IV.C.1. Community Engagements, Local, State, National, International

- Participated as a mentor in the 4th Edition of WinC (Women in Cryptography) Coffee Breaks, March 2025.
- Visited Berman Hebrew Academy Middle School a total of 3 times in June 2024 and January 2025 to give a presentation and lead interactive activities on Cryptography.
- Served on a Women in STEM panel at Berman Hebrew Academy Middle School, March 2024.
- Participant in NSF CISE invite-only workshop on broadening participation in computing (BPC) in 2018 (CISE BPCnet Workshop)
- 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.