

Dana (Glasner) Dachman-Soled

I. Personal Information

I.A. UID, Last Name, First Name, Middle Name, Contact Information

UID: 108974807

Dachman-Soled, Dana (Glasner)

3407 A.V. Williams Building

College Park, MD 20742, USA

Phone: (301) 405-9927

Email: danadach@ece.umd.edu

I.B. Academic Appointments at UMD

- Assistant Professor, Department of Electrical and Computer Engineering and UMIACS, August 2013-Present
- Affiliate Assistant Professor, 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.

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

II.C. Articles in Refereed Journals

- D. Dachman-Soled, #F.H. Liu, E. Shi, H.S. Zhou. "Locally Decodable and Updatable Non-Malleable Codes and Their Applications." *Journal of Cryptology*, to appear.
- D. Dachman-Soled, C. Liu, C. Papamanthou, E. Shi, U. Vishkin. "Oblivious Network RAM and Leveraging Parallelism to Achieve Obliviousness." *Journal of Cryptology*, to appear.
- D. Dachman-Soled, S.D. Gordon, #F.H. Liu, A. O'Neill, H.S. Zhou. "Leakage Resilient Public-Key Encryption from Obfuscation." *Journal of Cryptology*, to appear.
- 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.
- 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): 641-663, 2018.
- 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).
 - 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).
 - 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

- 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, to appear.
- 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.
- D. Dachman-Soled, #M. Kulkarni, #A. Shahverdi. “Local Non-Malleable Codes in the Bounded Retrieval Model.” *PKC(2) 2018*, pp. 281-311.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.

- 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.
- D. Dachman-Soled, V. Feldman, L.Y. Tang, A. Wan, K. Wimmer. “Approximate resilience, monotonicity, and the complexity of agnostic learning.” 25th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), 2015, to appear.
- 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.
- N. Bitansky, D. Dachman-Soled, H. Lin. “Leakage-Tolerant Computation with Input-Independent Preprocessing ” 34th International Cryptology Conference (CRYPTO) (2) 2014, pp. 146-163.
- 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.
- 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.
- 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.
- D. Dachman-Soled, Y. T. Kalai. “Securing Circuits and Protocols Against $1/\text{poly}(k)$ Tampering Rate.” Eleventh IACR Theory of Cryptography Conference (TCC), 2014, pp. 540-565.
- 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.
- D. Dachman-Soled, T. Malkin, M. Raykova, M. Venkatasubramanian. “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.
- N. Bitansky, D. Dachman-Soled, S. Garg, A. Jain, Y. T. Kalai, #A. L’opez-Alt, D. Wichs. “Why Fiat-Shamir for Proofs Lacks a Proof.” Tenth IACR Theory of Cryptography Conference (TCC), 2013, pp. 182-201.
- 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.
- D. Dachman-Soled, Y. T. Kalai. “Securing Circuits Against Constant-Rate Tampering.” 32nd International Cryptology Conference (CRYPTO), 2012, pp. 533-551.
- 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.
- D. Dachman-Soled, R. Gennaro, H. Krawczyk, T. Malkin. “Computational Extractors and Pseudorandomness.” Ninth IACR Theory of Cryptography Conference (TCC), 2012, pp. 383-403.
- D. Dachman-Soled, R. Servedio. “A Canonical Form for Testing Boolean Function Properties” 15th International Workshop on Randomization and Computation (RANDOM), 2011, pp. 460-471.
- 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.

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- D. Glasner, V. C. Sreedhar. “Configuration Reasoning and Ontology For Web.” IEEE International Conference on Services Computing (SCC), 2007, pp. 384-394.
- D. Glasner, A. I. Frenkel. “Geometrical characteristics of regular polyhedra: Application to EXAFS studies of nanoclusters.” AIP Conf. Proc. 882, pp. 746-748 (2007).
- A. I. Frenkel, L. D. Menard, P. Northrup, J. A. Rodriguez, 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

- **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**
“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, Brookline, 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

- **PKC 2014, Buenos Aires, Argentina**
“On Minimal Assumptions for Sender-Deniable Public Key Encryption,” March 2014.
- **PKC 2014, Buenos Aires, Argentina**
“A Black-Box Construction of a CCA2 Encryption Scheme from a Plaintext Aware Encryption Scheme,” March 2014.
- **TCC 2014, San Diego, California**
“Securing Circuits and Protocols Against $1/\text{poly}(k)$ Tampering Rate,” February 2014.
- **TCC 2014, San Diego, California**

- “Can Optimally-Fair Coin Tossing be Based on One-Way Functions?” February 2014.
- **RANDOM 2011, Princeton, New Jersey**
“A Canonical Form for Testing Boolean Function Properties,” August 2011.
- **TCC 2011, Providence, Rhode Island**
“On the Black-Box Complexity of Optimally-Fair Coin Tossing,” March 2011.
- **TCC 2008, New York, New York**
“Black-Box Construction of a Non-Malleable Encryption Scheme from Any Semantically SecureOne,” March 2008.
- **RANDOM 2007, Princeton, New Jersey**
“Distribution-Free Testing Lower Bounds for Basic Boolean Functions,” August 2007.

II.F. Professional Publications

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

- D. Dachman-Soled, #H. Gong, #M. Kulkarni, #A. Shahverdi. “Partial Key Exposure in Ring-LWE-Based Cryptosystems: Attacks and Resilience.” IACR Cryptology ePrint Archive 2018: 1068 (2018).
- 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).
- D. Dachman-Soled, #M. Kulkarni. “Upper and Lower Bounds for Continuous Non-Malleable Codes.” IACR Cryptology ePrint Archive 2018: 517 (2018).
- M. Ball, D. Dachman-Soled, S. Guo, T. Malkin, L.Y. Tan. “Non-Malleable Codes for Small-Depth Circuits.” CoRR abs/1802.07673 (2018).
- M. Ball, D. Dachman-Soled, S. Guo, T. Malkin, L.Y. Tan. “Non-Malleable Codes for Small-Depth Circuits.” Electronic Colloquium on Computational Complexity (ECCC) 25: 40 (2018).
- M. Ball, D. Dachman-Soled, S. Guo, T. Malkin, L.Y. Tan. “Non-Malleable Codes for Small-Depth Circuits.” IACR Cryptology ePrint Archive 2018: 207 (2018).
- D. Dachman-Soled, #H. Gong, #M. Kulkarni, #A. Shahverdi. “On the Leakage Resilience of Ideal-Lattice Based Public Key Encryption.” IACR Cryptology ePrint Archive 2017: 1127 (2017).
- M. Ball, D. Dachman-Soled, #M. Kulkarni, T. Malkin. “Non-Malleable Codes from Average-Case Hardness: AC0, Decision Trees, and Streaming Space-Bounded Tampering.” IACR Cryptology ePrint Archive 2017: 1061 (2017).
- D. Dachman-Soled, #M. Kulkarni, #A. Shahverdi. “Locally Decodable and Updatable Non-Malleable Codes in the Bounded Retrieval Model.” IACR Cryptology ePrint Archive 2017: 303 (2017).
- D. Dachman-Soled, #M. Kulkarni, #A. Shahverdi. “Tight Upper and Lower Bounds for Leakage-Resilient, Locally Decodable and Updatable Non-Malleable Codes.” IACR Cryptology ePrint Archive, Report 2017/015.
- D. Dachman-Soled. “Towards Non-Black-Box Separations of Public Key Encryption and One Way Function.” IACR Cryptology ePrint Archive, Report 2016/812.
- S. G. Choi, D. Dachman-Soled, T. Malkin, H. Wee. “Improved, Black-Box, Non-Malleable Encryption from Semantic Security.” IACR Cryptology ePrint Archive, Report 2016/842.
- S. G. Choi, D. Dachman-Soled, T. Malkin, H. Wee. “A Black-Box Construction of Non-Malleable Encryption from Semantically Secure Encryption.” IACR Cryptology ePrint Archive, Report 2016/720.
- 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.
- D. Dachman-Soled, S. D. Gordon, F. H. Liu, A. O’Neill, H. S. Zhou. “Leakage-Resilient

- Public-Key Encryption from Obfuscation.” IACR Cryptology ePrint Archive, Report 2016/730.
- M. Ball, D. Dachman-Soled, #M. Kulkarni, T. Malkin. “Non-Malleable Codes for Bounded Depth, Bounded Fan-in Circuits.” IACR Cryptology ePrint Archive, Report 2016/307.
- D. Dachman-Soled, J. Katz, #A. Thiruvengadam. “10-Round Feistel is Indifferentiable from an Ideal Cipher.” Cryptology ePrint Archive, Report 2015/876.
- D. Dachman-Soled, N. Fleischhacker, J. Katz, A. Lysyanskaya, D. Schroder. “Feasibility and Infeasibility of Secure Computation with Malicious PUFs.” Cryptology ePrint Archive, Report 2015/405.
- D. Dachman-Soled, C. Liu, C. Papamanthou, E. Shi, U. Vishkin. “Oblivious Network RAM.” Cryptology ePrint Archive, Report 2015/073.
- D. Dachman-Soled, J. Katz, #V. Rao. “Adaptively Secure, Universally Composable, Multi-Party Computation in Constant Rounds.” Cryptology ePrint Archive, Report 2014/858.
- D. Dachman-Soled, #F.H. Liu, H.S. Zhou. “Leakage-Resilient Circuits Revisited—Optimal Number of Computing Components without Leak-free Hardware.” Cryptology ePrint Archive, Report 2014/856.
- D. Dachman-Soled, #F.H. Liu, E. Shi, H.S. Zhou. “Locally Decodable and Updatable Non-Malleable Codes and Their Applications.” Cryptology ePrint Archive, Report 2014/663.
- D. Dachman-Soled, V. Feldman, L.Y. Tang, A. Wan, K. Wimmer. “Approximate resilience, monotonicity, and the complexity of agnostic learning.” arXiv, Report 1405.5268.
- D. Dachman-Soled. “A Black-Box Construction of a CCA2 Encryption Scheme from a Plaintext Aware (sPA1) Encryption Scheme.” Cryptology ePrint Archive, Report 2013/680.
- D. Dachman-Soled. “On the Impossibility of Sender-Deniable Public Key Encryption.” Cryptology ePrint Archive, Report 2013/727.
- D. Dachman-Soled, A. Jain, Y. T. Kalai, #A. López-Alt. “On the (In)security of the Fiat-Shamir Paradigm, Revisited.” (Cryptology ePrint Archive).
- D. Dachman-Soled, G. Fuchsbauer, P. Mohassel, A. O’Neill. “Enhanced Chosen-Ciphertext Security and Applications.” Cryptology ePrint Archive, Report 2012/543.
- D. Dachman-Soled, Y.T. Kalai. “Securing Circuits Against Constant-Rate Tampering.” Cryptology ePrint Archive, Report 2012/366.
- D. Dachman-Soled, R. Gennaro, H. Krawczyk, T. Malkin. “Computational Extractors and Pseudorandomness.” Cryptology ePrint Archive, Report 2011/708.
- D. Dachman-Soled, T. Malkin, M. Raykova, M. Venkatasubramanian. “Adaptive and Concurrent Secure Computation from New Notions of Non-Malleability.” Cryptology ePrint Archive, Report 2011/611.

II.E.10. Non-Refereed Panels

- Women in Cyber&Computing Professional 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

II.J.1. Grants

- **Investigators:** Dana Dachman-Soled (PI)
Proposal/Project Title: Faithfulness, Side-Channels, and Anonymity in Lattice-Based Cryptosystems
Source of Support: Cisco Systems, Incorporated
Total Award Amount: \$76,914.00
Total Award period Covered: 09/01/2018-08/31/2019
Location of Project: University of Maryland, College Park
- **Investigator:** Dana Dachman-Soled (PI)

Proposal/Project Title: EAGER: SaTC: Post-Quantum Indifferentiability

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

- **Investigators:** Dana Dachman-Soled (PI)

Proposal/Project Title: Analyzing the Side-Channel Resistance of Lattice-Based Key Exchange

Source of Support: Cisco Systems, Incorporated

Total Award Amount: \$75,525.00

Total Award period Covered: 05/31/2017-05/30/2018

Location of Project: University of Maryland, College Park

- **Investigators:** Dana Dachman-Soled (PI)

Proposal/Project Title: Analyzing the Robustness of Lattice-Based Schemes Against Side-Channel Attacks

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

- **Investigators:** Dana Dachman-Soled (PI)

Proposal/Project Title: Data Integrity for Dynamic Memory via Locally Decodable and Updatable Non-Malleable Codes

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

- **Investigators:** Jonathan Katz (PI), Dana Dachman-Soled (co-PI), Babis Papamanthou (co-PI)

Proposal/Project Title: Provable Security for Next-Generation Cryptography

Source of Support: NIST

Total Award Amount: \$1,097,937 (my share: \$362,319)

Total Award period Covered: 09/01/2015-08/31/2018

Location of Project: University of Maryland, College Park

- **Investigator:** Dana Dachman-Soled (PI)

Proposal/Project Title: Threat Models and Practical, Provably Secure Architecture for the Secure Scan-Chain Problem

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

- **Investigator:** Dana Dachman-Soled (PI)

Proposal/Project Title: CAREER: Non-Black-Box Cryptography: Defending Against and Benefiting from Access to Code

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

- **Investigator:** Dana Dachman-Soled (PI)

Proposal/Project Title: Cryptography in Diverse Models: Physical Security and Adaptive Security

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.3. Other

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

III. Teaching, Mentoring and Advising.

III.A. Courses Taught

- Spring 2018: Introduction to Cryptology (ENEE459E/CMSC498R), 30 students.
- Fall 2017: Computer Systems Security (ENEE 457/CMSC 498E), 56 students
- Spring 2017: Introduction to Cryptology (ENEE459E/CMSC498R), 34 students.
- Spring 2016: Introduction to Cryptology (ENEE459E/CMSC498R), 39 students.
- Fall 2015: Digital Logic (ENEE 244), 63 students.
- Spring 2015: Introduction to Cryptology (ENEE459E/CMSC498R), 34 students.
- Fall 2014: Digital Logic (ENEE 244), 50 students.
- Spring 2014: Introduction to Cryptology (ENEE459E/CMSC498R), 35 students.
- Fall 2013: Cryptography Against Physical Attacks (ENEE759O/CMSC858T), 6 students.

III.B. Teaching Innovations

III.B.5. Course or Curriculum Development

- Theoretical Foundations of Computer Engineering (ENEE 351)
- Introduction to Cryptology (ENEE459E/CMSC498R)
- Cryptography Against Physical Attacks (ENEE759O/CMSC858T)

III.C. Advising: Research or Clinical

III.C.1. Undergraduate

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

III.C.2. Master's

- Gregory Coard, Fall 2015—Spring 2017 (advisor)

- Sana Awan (committee member, Fall 2015)

III.C.3. Doctoral

- Vanishree Rao, UCLA (committee member, Summer 2015) (now a research scientist at PARC).
- Carson Dunbar (committee member, Spring 2015)
- Mukul Kulkarni, Fall 2014--- (advisor)
- Aria Shahverdi, Fall 2015--- (advisor)
- Aishwarya Thiruvengadam, Spring 2016—Summer 2017 (advisor, co-advised with Prof. Jonathan Katz) (now a postdoc at UCSB)
- Huijing Gong, Fall 2017--- (advisor)
- Chongxi Bao (committee member, Spring 2017)
- Kristopher Micinski (committee member, Summer 2017)
- Daniel Apon (committee member, Summer 2017)
- Yang Xie (committee member, Spring 2018)
- Xi Chen (committee member, Summer 2018)
- Xiao Wang (committee member, Summer 2018)
- Yupeng Zhang (committee member, Summer 2018)

III.C.4. Post-doctoral

- Feng-Hao Liu, Fall 2014-Spring 2015 (now an assistant prof at Florida Atlantic University)
- Jacob Alperin-Sheriff, Fall 2015-Spring 2016 (now a researcher at NIST)

III.C.5. Other Research Directions (*K-12 Interactions*)

- Angela Park, Spring 2015 (junior at Montgomery Blair High School for math, science and computer science magnet program)
- Stuart Nevans Locke, Summer 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)

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.5. Reviewing Activities for Conferences

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

- Human Relations and Welfare Committee 2014-2015
- UMIACS Retreat Committee on Publicity and Outreach
- UMIACS APT Committee FY '16, '17, '18
- PhD Qualifying Exam Committee 2015--
- Graduate Studies and Research Committee 2017-2018

- MC2 Senior Hire Search Committee
- ECE Strategic Planning Committee
- Facilities and Services Committee 2018--
- Departmental Council 2017--
- GAAC 2018--

IV.B.3. Campus Service – University

- ACES Director Review Committee 2017

IV.B.6. Offices and Committee Memberships

- Eurocrypt 2019 PC member
- Crypto 2018 PC member
- PKC 2018 PC member
- TCC 2017 PC member
- CRYPTO 2017 PC member
- PKC 2017 PC member
- NDSS 2017 PC member
- CCS 2016 PC member
- PKC 2016 PC member
- TCC 2016 PC member
- CRYPTO 2013 PC member
- SCN 2012 PC member

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

- Session Chair Crypto 2017 and TCC 2017.

IV.F Community & Other Service

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

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

- 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