Jeremiah Blocki

Current Position

(August 2023 to present)
Associate Professor
Computer Science Department
Purdue University
West Lafayette, IN 47907
(August 2016 to July 2023)
Assistant Professor
Computer Science Department
Purdue University
West Lafayette, IN 47907

Phone: (765) 494-9432
Office: 1165 Lawson Computer Science Building
Email: jblocki@purdue.edu
Homepage: https://www.cs.purdue.edu/people/faculty/jblocki/

Previous Positions

(August 2015 - June 2016)
Post-Doctoral Researcher
Microsoft Research
New England Lab
Cambridge, MA

(May 2015-August 2015)
Cryptography Research Fellow
Simons Institute
(Summer of Cryptography)
UC Berkeley
Berkeley, CA

(June 2014-May 2015)
Post-Doctoral Fellow
Computer Science Department
Carnegie Mellon University
Pittsburgh, PA 15213

Education

Ph.D. in Computer Science, Carnegie Mellon University, 2014.

Advisors: Manuel Blum and Anupam Datta.

Committee: Manuel Blum, Anupam Datta, Luis Von Ahn, Ron Rivest

Thesis Title: Usable Human Authentication: A Quantitative Treatment

B.S. in Computer Science, Carnegie Mellon University, 2009. (3.92 GPA).

Senior Research Thesis: Direct Zero-Knowledge Proofs

Allen Newell Award for Excellence in Undergraduate Research

Research

Research Interests

Cryptography, Passwords, Usable and Secure Password Management, Human Computable Cryptography, Password Hashing, Memory Hard Functions, Differential Privacy, Coding Theory, Game Theory and Security

Journal Publications

(*) Denotes Primary Author

1. (*) Blocki, J., Liu, P., Ren, L., and Zhou, S. Bandwidth-Hard Functions: Reductions and Lower Bounds. Journal of Cryptology, Volume 37(16) 2024. [https://doi.org/10.1007/s00145-024-09497-3]

2. (*) Bai, W., (*) Blocki, J. and Ameri, H. Cost-Asymmetric Memory Hard Password Hashing. Information and Computation, Volume 297 (Special papers of the 13th International Conference on Security and Cryptography for Networks (SCN 2022)), March 2024. [https://www.sciencedirect.com/science/article/abs/pii/S0890540123001372]

3. (*) Blocki, J. and Zhang, W. DALock: Password Distribution-Aware Throttling. Proceedings on Privacy Enhancing Technologies (PoPETs), Issue 3, 2022.

4. Blocki, J., Gandikota, V., Grigorescu, G. and Zhou, S. Relaxed Locally Correctable Codes in Computationally Bounded Channels. IEEE Transactions on Information Theory, 2021. [https://ieeexplore.ieee.org/document/9417090]

5. Harsha, B., Morton, R., Blocki, J., Springer, J. and Dark, M. Bicycle Attacks Consider Harmful: Quantifying the Damage of Widespread Password Length Leakage. Computers & Security, Volume 100, 2021. [https://doi.org/10.1016/j.cose.2020.102068]

6. Chong, I., Proctor, R., Li, N. and Blocki, J. Surviving in the Digital Environment: Does Survival Processing Provide and Additional Memory Benefit to Password Generation Strategies. Journal of Applied Research in Memory and Cognition. Volume 9, Issue 3, September 2020. [https://www.sciencedirect.com/science/article/pii/S2211368120300334]

Conference Publications

1. Blocki, J., Grigorescu, E., Mukherjee, T. and Zhou, S. How to Make Your Approximation Algorithm Private: A Black-Box Differentially-Private Transformation for Tunable Approximation Algorithms of Functions with Low Sensitivity. International Conference on Randomization and Computation (RANDOM 2023).

2. Block, A., Blocki, J., Cheng, K., Grigorescu, E., Xin, L., Zheng, Y. and Zhu, M. On Relaxed Locally Decodable Codes for Hamming and Insertion-Deletion Errors. Computational Complexity Conference (CCC 2023).

3. Block, A. and Blocki, J. Computationally Relaxed Locally Decodable Codes, Revisited. IEEE International Symposium on Information Theory (ISIT 2023).

4. (*) Peiyuan, L., (*) Blocki, J. and (*) Bai, W. Confident Monte Carlo: Rigorous Analysis of Guessing Curves for Probabilistic Password Models. IEEE Symposium on Security and Privacy (S&P 2023). [12% acceptance rate (historical)]

5. Blocki, J., Lee, S., Mukherjee, T. and (*) Zhou, S. Differentially Private L2-Heavy Hitters in the Sliding Window Model. International Conference on Learning Representations (ICLR 2023). [Spotlight (notable-top-25%); 31.8% acceptance rate overall]

6. (*) Blocki, J. and (*) Peiyuan, L. Towards a Rigorous Statistical Analysis of Empirical Password Datasets. IEEE Symposium on Security and Privacy (S&P 2023). [12% acceptance rate (historical)]

7. (*) Blocki, J., Holman, B. and Seunghoon, L. The Parallel Reversible Pebbling Game: Analyzing the Post-Quantum Security of iMHFs. Theory of Cryptography Conference (TCC 2022) [43% acceptance rate]

8. Ameri, M., (*) Bai, W., and (*) Blocki, J. Cost-Asymmetric Memory Hard Password Hashing. Security and Cryptography for Networks (SCN 2022). [45% acceptance rate (historical)]

9. Ameri, M., Blocki, J. and Block, A. Memory-Hard Puzzles in the Standard Model with Applications to Memory-Hard Functions and Resource-Bounded Locally Decodable Codes. Security and Cryptography for Networks (SCN 2022). [45% acceptance rate (historical)]

10. (*) Blocki, J. and (*) Holman, B. Sustained Space and Cumulative Complexity Trade-offs for Data-Dependent Memory-Hard Functions. CRYPTO 2022. [22.1% acceptance rate]

11. Blocki, J., Mukherjee, T. and Grigorescu, E. Privately Estimating Graph Parameters in Sublinear time. ICALP 2022. [29.6% acceptance rate]

12. (*) Blocki, J. and Lee, S. On the Multi-User Security of Short Schnorr Signatures with Preprocessing. 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2022). [23% acceptance rate]

13. (*) Blocki, J., Cinkoske, M., Lee, S. and Jin Young, S. On Explicit Constructions of Extremely Depth Robust Graphs. 39th International Symposium on Theoretical Aspects of Computer Science (STACS 2022). [27% acceptance rate]

14. Bai, W., (*) Blocki, J., and Harsha, B. Password Strength Signaling: A Counter-Intuitive Defense Against Password Cracking. (GameSec 2021) [42% acceptance rate (estimated)]

15. Bau, Y., Sundararajah, K., Malik, R., Ye, Q., Wagner, C., Jaber, N., Wang, F., Ameri, M., Lu, D., Seto, A., Delaware, B., Samanta, R., Kate, A., Garman, C., Blocki, J., Letourneau, P., Meister, B., Springer, J., Rompf, T. and Kulkarni, M. HACCLE: Metaprogramming for Secure Multi-Party Computation. (GPCE 2021) [50% acceptance rate]

16. Blocki, J., Cheng, K., Grigorescu, E. Li, X. Zheng, Y. and Zhu, M. Exponential Lower Bounds for Locally Decodable Codes Correcting Insertions and Deletions. (FOCS 2021) [34.6% acceptance rate]

17. (*) Blocki, J., Lee, S. and Zhou, S. On the Security of Proofs of Sequential Work in a Post-Quantum World. (ITC 2021) [40% acceptance rate (estimated)]

18. Block, A. and Blocki, J. Private and Resource-Bounded Locally Decodable Codes for Insertions and Deletions. (ISIT 2021)

19. Blocki, J., Grigorescu, E. and Mukherjee, T. Differentially Private Sublinear-Time Clustering. (ISIT 2021)

20. (*) Blocki, J. and Bai, W. DAHash: Distribution Aware Tuning of Password Hashing Costs. (FC 2021) [25.3% acceptance rate]

21. (*) Blocki, J. and Cinkoske, M. A New Connection Between Node and Edge Depth Robust Graphs. (ITCS 2021) [41.5% acceptance rate]

22. Block, A., Blocki, J. Grigorescu, E., Kulkarni, S. and Zhou, M. Locall Decodable/Correctable Codes for Insertions and Deletions. (FSTTCS 2020) [32.6% (historical)]

23. Harsha, B. and Blocki, J. An Economic Model for Quantum Key-Recovery Attacks against Ideal Ciphers (WEIS 2020) [34.9% acceptance rate]

24. (*) Blocki, J. and Kulkarni, S. and Zhou, S. On Locally Decodable Codes in Resource Bounded Channels. (ITC 2020) [41% acceptance rate]

25. (*) Ameri, M., Blocki, J. and Zhou, S. Computationally Data-Independent Memory Hard Functions. Innovations in Theoretical Computer Science (ITCS 2020). [34.9% acceptance rate (estimated)]

26. (*) Blocki, J. Lee, S. and Zhou, S. Approximating Cumulative Pebbling Cost is Unique Games Hard. Innovations in Theoretical Computer Science (ITCS 2020). [34.9% acceptance rate (estimated)]

27. (*) Blocki, J., Harsha, B., Kang, S., Lee, S., Xing, L. and Zhou, S. Data-Independent Memory Hard Functions: New Attacks and Stronger Constructions. (CRYPTO 2019). [21.4% acceptance rate]

28. Blocki, J. Gandikota, V. Grigorescu, E. and Zhou, S. Relaxed Locally Correctable Codes in Computationally Bounded Channels. IEEE International Symposium on Information Theory (ISIT 2019).

29. (*) Blocki, J., Ren, L. and Zhou, S. Bandwidth-Hard Functions: Reductions and Lower Bounds. ACM Conference on Computer and Communications Security (CCS 2018). [16.6% acceptance rate]

30. (*) Alwen, J., Blocki, J. and Pietrzak. Sustained Space Complexity. 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2018). [23.5% acceptance rate]

31. Blocki, J., Harsha, B. and Zhou, S. On the Economics of Offline Password Cracking. IEEE Security and Privacy (S&P 2018). [11.5% acceptance rate]

32. Blocki, J. and Zhou, S (student). On the Computational Complexity of Minimal Cumulative Cost Graph Pebbling. Twenty-Second International Converence on Financial Cryptography and Data Security (FC 2018). [26.6% acceptance rate] https://arxiv.org/abs/1609.04449.

33. Harsha, B (student) and Blocki, J. Just-in-time Password Hashing. 3rd IEEE European Symposium on Security and Privacy (Euro S&P 2018). [22.9% acceptance rate]

34. (*) Alwen, J., Blocki, J. and Harsha, B. Practical Graphs for Optimal Side-Channel Resistant Memory-Hard Functions. ACM Conference on Computer and Communications Security (CCS 2017). [18% acceptance rate]

35. (*) Blocki, J. and Zhou, S. On the Depth-Robustness and Cumulative Pebbling Cost of Argon2i. Fifteenth IACR Theory of Cryptography Conference (TCC 2017). [34% acceptance rate]

36. Wang, T (student)., Blocki, J., Li, N. and Jha, S. Locally Differentially Private Protocols for Frequency Estimation. 26th USENIX Security Symposium (USENIX 2017). [16.3% acceptance rate]

37. Alwen, J., Blocki, J. and Pietrzak, K. Depth-Robust Graphs and Their Cumulative Memory Complexity. 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2017). [25.4% acceptance rate]

38. (*) Alwen, J. and Blocki, J. Towards Practical Attacks on Argon2i and Balloon Hashing. Second IEEE European Symposium on Security and Privacy (Euro S&P 2017). [19.6% acceptance rate]

39. (*) Blocki, J., Blum, M. Datta, A. and Vempala, S. Toward Human Computable Passwords. in the 8th conference on *Innovations in Theoretical Computer Science.* [34.9% acceptance rate (estimated)] http://arxiv.org/abs/1404.0024.

40. (*) Blocki, J. and Datta, A. (2016). CASH: A Cost Asymmetric Secure Hash Algorithm for Optimal Password Protection. in the *29th IEEE Computer Security Foundations Symposium* (CSF 2016). [35.6% acceptance rate]

41. (*) Blocki, J. and Sridhar, A. Client-CASH: Protecting Master Passwords against Offline Attacks. Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (AsiaCCS 2016). [19% Acceptance Rate]

42. (*) Alwen, J. and Blocki, J. (2016) Efficiently Computing Data-Independent Memory Hard Functions. CRYPTO 2016. [25.5% acceptance rate]

43. (*) Blocki, J., Datta, A. and Bonneau, J. Differentially Private Password Frequency Lists. Or, How to release statistics from 70 million passwords (on purpose). Proceedings of the 23rd Annual Network & Distributed System Security Symposium (NDSS 2016), San Diego, California, USA. 2016. [15.4% Acceptance Rate]

44. (*) Blocki, J. and Zhou, H. Designing Proof of Human-work Puzzles for Cryptocurrency and Beyond. Proceedings of the 14th IACR Theory of Cryptography Conference. TCC 2016b. https://eprint.iacr.org/2016/145.pdf. [32.9% acceptance rate (estimated)]

45. Blocki, J., Christin, N., Datta, A., Procaccia, A. and Sinha, A. Audit Games with Multiple Defender Resources. Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence (AAAI'15).

46. (*) Blocki, J., Komanduri, S., Cranor, L., and Datta, A. Spaced Repetition and Mnemonics Enable Recall of Multiple Strong Passwords. Proceedings of the 22nd Annual Network & Distributed System Security Symposium (NDSS 15), San Diego, California, USA. 2014. [16.9% Acceptance Rate]

    Press: ZDNet and Kaspersky Lab Daily

47. (*) Blocki, J., Blum, M., and Datta, A. (2013). GOTCHA Password Hackers! in the 6th ACM Workshop on Artificial Intelligence and Security.

    Press: ArsTechnica, MIT Technology Review (Inaccurate), CMU, Slashdot and Salon

48. (*) Blocki, J., Blum, M., and Datta, A. (2013). Naturally Rehearsing Passwords. in the 19th Annual International Conference on the Theory and Application of Cryptology and Information Security. [20% acceptance rate]

    Press: Scientific American, CMU and Science Daily

49. (*) Blocki, J., Komanduri, S., Procaccia, A., and Sheffet, O. (2013) Optimizing Password Composition Policies. in the 14th ACM Conference on Electronic Commerce. [32% acceptance rate]

50. (*) Blocki, J., Blum, A., Datta, A., and Sheffet, O. (2013). Differentially Private Data Analysis of Social Networks via Restricted Sensitivity. in the 4th conference on *Innovations in Theoretical Computer Science.* [39.8% acceptance rate]

51. (*) Blocki, J., Christin, N., Datta, A., and Sinha, A. (2013). Adaptive Regret Minimization in Bounded Memory Games (Invited Paper). in the 4th *Conference on Decision and Game Theory for Security.*

52. Blocki, J., Christin, N., Datta, A., Procaccia, A. and Sinha, A. (2013) Audit Games. Proceedings of the Twenty-Third International Joint Conference on Artificial Intelligence (IJCAI'13).

53. Blocki, J., Christin, N., Datta, A., and Sinha, A. (2012). Audit Mechanisms for Provable Risk Management and Accountable Data Governance. in the 3rd *Conference on Decision and Game Theory for Security.*

54. Blocki, J., Blum, A., Datta, A., and Sheffet, O. (2012). The Johnson-Lindenstrauss Transform Itself Preserves Differential Privacy. in the *53rd Annual IEEE Symposium on Foundations of Computer Science.* [31.9% acceptance rate]

55. Datta, A., Blocki, J., Christin, N., DeYoung, H., Garg, D., Jia, L., Kaynar, D., Sinha, A. (2011). Understanding and Protecting Privacy: Formal Semantics and Principled Audit Mechanisms (Invited Paper). in the 7th *International Conference on Information Systems Security.*

56. Blocki, J., Christin, N., Datta, A., and Sinha, A. (2011). Audit Mechanisms for Privacy Protection in Healthcare Environments (Position Paper). in the *2nd USENIX Workshop on Health Security and Privacy.*

57. Blocki, J., Christin, N., Datta, A., and Sinha, A. (2011). Regret Minimizing Audits: A Learning-theoretic Basis for Privacy Protection. in the *24th IEEE Computer Security Foundations Symposium.*

58. (*) Blocki, J. and Williams, R. (2010). Resolving the Complexity of Some Data Privacy Problems. in the *37th International Colloquium on Automata, Languages and Programming.* [27% acceptance rate]

Under Submission

Ameri, M. and Blocki, J. Conditional Encryption with Applications to Password Typo Correction.

Blocki, J. and Lee, S. Preprocessing Security in Multiple Idealized Models with Applications to Schnorr Signatures and PSEC-KEM.

Blocki, J. and Holman, B. Practical Data-Dependent Memory-Hard Functions in the Parallel Random Oracle Model.

Blocki, J., Holman, B., and Lee, S. The Impact of Reversibility on Parallel Pebbling

Blocki, J., Fichtenberger, H., Grigorescu, E. and Mukherjee, T. Differential Privacy and Sublinear Time are Incompatible Sometimes.

In Preparation

Liu, P. and Blocki, J. Tighter Analysis of Password Guessing Curves with Applications to PINs.

Bai, W., Blocki, J., Harsha, B. A Decision Theoretic Framework for Quantum Pre-Image Attacks

Blocki, J., B. Harsha and Zhang, W. Keyboard Based Human Computable Password Schemas.

Blocki, J. On the Amortized Memory Hardness of SCRYPT.

Grants

CAREER: Cryptographic Tools for Usable Human Authentication. $591,881. NSF #2047272. 5/15/2021 to 4/30/2026.

Purdue PRF: Distribution Aware Password Throttling: Protecting Users without Locking Them Out. $31,119. 6/01/2020 to 5/31/2021.My Amount: $31,119

CIF: Small: Ultra-Efficient Codes for Communication and Verifiable Storage. $499,202. NSF #1910659. 10/1/2019 to 9/30/2022. My Amount: $247,405.

Purdue University Big Idea: Purdue pbits. $303,139.

SaTC: CORE: Medium: Collaborative: User-Centered Deployment of Differential Privacy. $343,110.00. NSF #1931443. 1/1/2020 to 12/31/2020. My Amount: $102,743.

Rolls Royce Inc. Ben Harsha Fellowship. $200,000. 8/13/18 to 8/12/21.

HACCLE: High-Assurance Compositional Cryptography: Languages and Environments. $10,732,899. IARPA. 5/01/2018 to 7/30/2020. My Amount (6/30/19 to 3.2.20): $110,550

CRII: SaTC: Towards the Development of Stronger Memory Hard Functions for Secure Password Hashing. NSF #1755708. $175,000. 8/1/2018 to 7/31/2020.

SaTC: CORE: Improving Password Ecosystem: A Holistic Approach. NSF #1704587. $300,000. 10/1/2017 to 9/30/2019 (with Ninghui Li and Robert Proctor). My funds $99,531.

PNC Research Award. $50,000. 9/1/2014 to 9/1/2016 (with Manuel Blum).

Professional Activities

arXiv Moderator: Cryptography and Security (cs.CR)

Program Committee: IEEE Security and Privacy 2024.

Program Committee: EUROCRYPT 2024.

Program Committeee: IEEE Security and Privacy 2024.

Program Committeee: Information Theoretic Cryptography 2023.

Program Committeee: IEEE Security and Privacy 2023.

Andreas Pfitzmann Best Student Paper Award co-Chair: PETS 2022.

Program Committee: Information Theoretic Cryptography 2022.

Program Committee: CRYPTO 2022.

Program Committee: Financial Cryptography 2022.

Program Committee: IEEE Security and Privacy 2022.

Program Committee: CRYPTO 2021.

Program Committee: NDSS 2021.

Program Committee: CRYPTO 2020.

Program Committee: RSA-Cryptographer's Track 2020.

Program Committee: NDSS 2020.

Program Committee: WAY 2019 (Who Are You?! Adventures in Authentication Workshop)

Program Committee: CCS 2019.

Program Committee: ITCS 2019.

Program Committee: Financial Cryptography 2018.

Program Committee: CRYPTO 2018.

Program Committee: Financial Cryptography 2018.

Program Committee: ACM Conference on Computer and Communications Security 2017.

Program Committee: Computer Security Foundations 2017.

Program Committee: Financial Cryptography 2017.

Program Committee: ACM CCS Poster/Demo Session

Program Committee: Passwords 2016.

Program Committee: Security and Cryptography for Networks 2016.

Program Committee: Passwords 2015.

Program Committee: Workshop on Privacy in the Electronic Society, 2014.

Session Chair: CRYPTO 2022, EUROCRYPT 2022, CRYPTO 2020, Financial Cryptography 2018, CCS 2018

(CMU) CSD PhD Admission Committee, 2013.

(CMU) CSD PhD Open House Poster Session Organizer, 2012.

Journal Reviews & External Conference Reviews

IACR Journal of Cryptogology

Information Processing Letters

IEEE Foundations of Computer Science.

IEEE Transactions on Knowledge and Data Engineering

IEEE Transactions on Dependable and Secure Computing

ACM Transactions on Information and System Security

IEEE Control Systems Society Conference

Journal of Computer and System Sciences

Computers & Security

1st IEEE European Symposium on Security and Privacy

ACM-SIAM Symposium on Discrete Algorithms.

IEEE Transactions on Information Forensics & Security.

ACM Conference on Computer and Communications Security.

Mathematical Foundations of Computer Science.

IEEE Symposium on Security and Privacy.

IEEE Security and Privacy SP.

Theory of Cryptography Conference TCC.

EUROCRYPT

International Symposium on Parameterized and Exact Computation.

Algorithms. `http://www.mdpi.com/journal/algorithms`

University Service

Diversity Commitee 2023

ACM Advisor 2023

CS Undergraduate Study Committee 2020-2022

CS Graduate Student Admissions Committee 2016-2018, 2019-2020

CS Graduate Study Committee 2018-2019

CS Theory and Algorithms Hiring Committee 2019-2020

CS Graduate Visit Day Committee 2020

CS591: CERIAS Security Seminar (Fall 2017)

Teaching

1. CS655: Advanced Cryptography (Spring 2023)
2. CS251: Data Structures and Algorithms (Fall 2022, Fall 2023)
3. CS580: Algorithm Design and Analysis (Fall 2021, Online Course Development)
4. CS290 & CS390: Competitive Programming 1 & 2 (Fall 2021 [42+29])
5. CS381: Introduction to the Analysis of Algorithms (Fall 2019 [167], Fall 2020 [72+67], Spring 2024)
6. CS580: Algorithm Design and Analysis (Spring 2018 [64], Spring 2019 [62])
7. CS55500: Cryptography (Spring 2017 [16], Fall 2017 [23], Fall 2018 [31], Spring 2021 [11])
8. CS59000: Passwords and Human Authentication Seminar (Fall 2016 [10], Spring 2020 [12]).
9. CS50010: Foundational Principles of Information Security (Summer 2018 [7])
10. CS50010: Foundational Principles of Information Security [Spring 2018, recorded lectures]

PhD Students

Nathan Smearsoll (Purdue CS, 2023-present)

Blake Holman (Purdue CS, 2021-present)

Seunghoon Lee (Purdue CS, 2018-present) [Passed Prelim]

Mohammad Hassan Ameri (Purdue CS, 2018-present)

Peiyuan Liu (Purdue CS, 2018-present) [Passed Prelim]

MS and Undergraduate Students

Mike Cinkoske (Purdue CS Undegraduate, 2018- 2020)

Muqi Zhou (Purdue CS MS, 2018-2020)

Shubhang Kulkarni (Purdue CS MS, 2019-2020)

Past Postdocs

Samson Zhou (Purdue CS, Summer 2018)

Prior Phd Students

Ben Harsha [Graduated: Summer 2021]

Alexander Block [Graduated: Summer 2022]

Tamalika Mukherjee [Graduated: Summer 2023, Co-Advised with Elena Grigorescu]

Wenjie Bai [Graduated: Summer 2023]

Past Undergraduate Students

Anirudh Sridhar (CMU, 2015/2016)

Shaun Allison (CMU, 2014)

Shikun Zhang (CMU, 2013 – Senior Research Thesis)

> Bill Gates Kissing an Igloo : a Password Management Application with Provable Security and Minimal User Effort
> Alcoa Undergraduate Research Award

Calvin Beideman (High School, 2013)
Independent Research In Mathematics: Set Families with Low Pairwise Intersection. Technical Report.

Adidtya Shektar (High School, 2009)
Independent Study: RSA Cryptography

Talks

On the Multi-User Security of Short Schnorr Signatures with Preprocessing. EUROCRYPT 2022

Password Strength Signaling: A Counter-Intuitive Defense Against Password Cracking. CERIAS Security Seminar Fall 2021

Password Strength Signaling: A Counter-Intuitive Defense Against Password Cracking. GameSec 2021

DAHash: Distribution Aware Tuning of Password Hashing Costs. Financial Cryptography 2021

Memory Hard Functions, Random Oracles, Graph Pebbling and Extractor Arguments. CSoI Seminar 2019

Memory Hard Functions and Password Hashing. Purdue PurPL Fest 2019

Data-Independent Memory Hard Functions: New Attacks and Strong Constructions. CRYPTO 2019.

Relaxed Locally Correctable Codes in Computationally Bounded Channels. IEEE Symposium On Information Theory. ISIT 2019

Memory Hard Functions, Random Oracles, Graph Pebbling and Extractor Arguments. CSoI Seminar 2019.

Memory Hard Functions and Password Hashing. Purdue PuRPL Fest 2019.

Sustained Space Complexity. Purdue Crypto Reading Group. Spring 2019.

Bandwidth-Hard Functions: Reductions and Lower Bounds. 25th ACM Conference on Computer and Communications Security CCS 2018.

On the Economics of Offline Password Cracking. 39th IEEE Symposium on Security and Privacy. S&P 2018.

On the Depth-Robustness and Cumulative Pebbling Cost of Argon2i. Theory of Cryptography Conference. TCC 2017.

Memory Hard Functions and Human Authentication. CERIAS Security Seminar 2017.

Releasing a Differentially Private Password Frequency Corpus from 70 Million Yahoo! Passwords. Invited talk at DIMACS/Northeast Big Data Hub Workshop on Overcoming Barriers to Data Sharing including Privacy and Fairness. Fall 2017.

Practical Graphs for Optimal Side-Channel Resistant Memory-Hard Functions. ACM Conference on Computer and Communications Security. CCS 2017.

Memory Hard Functions and Password Hashing. CERIAS Security Seminar Fall 2017.

Memory Hard Functions and Password Hashing. CERIAS Security Symposium 2017.

Towards a Theory of Data-Independent Memory Hard Functions. Real World Crypto 2017. RWC 2017.

Towards a Theory of Data-Independent Memory Hard Functions. Charles River Crypto Day 2016 at MIT.

Differentially Private Integer Partitions and Their Applications. Spotlight Talk at Theory and Practice of Differential Privacy Workshop. TPDP 2016.

CSF 2016. CASH: A Cost Asymmetric Secure Hash Algorithm for Optimal Password Protection.

Carnegie Mellon University Distinguished Lecture: Attacking Data-Independent Memory-Hard Functions (March 2016).

NDSS 2016. Differentially Private Password Frequency Lists: Or, how to release statistics from 70 million passwords (on purpose).

Heidelberg Laureate Forum Workshop: Towards Usable Human Authentication Protocols. . 2015.

Boston University Security Seminar: Towards Usable Human Authentication Protocols. 2015.

GameSec 2013. Adaptive Regret Minimization in Bounded Memory Games.

Naturally Rehearsing Passwords, ASIACRYPT 2013.

Naturally Rehearsing Passwords, NSF TRUST Fall Conference 2013.

GOTCHA Password Hackers!, AISec 2013.

Optimizing Password Composition Policies, EC 2013.

Differentially Private Analysis of Social Networks via Restricted Sensitivity, ITCS 2013.

Usable and Secure Password Management, Cylab Research Talk, 2012.

Password Management, 18-739: Foundations of Security and Privacy (Guest Lecture) 2011.

Regret Minimization in Bounded Memory Games, Theory Lunch 2010.

Resolving the Complexity of Some Data Privacy Problems, ICALP 2010.

Honors, Awards, & Fellowships

NSF CAREER Award 2021.

Purdue Seed for Success Award 2019. From Intelligence Advanced Research Projects Activity, HACCLE: High-Assurance Compositional Cryptography: Languages and Environments.

Most Influential Professor (Graduate Student Board). Purdue CS Awards Banquet 2019.

National Science Foundation Computer and Information Science and Engineering (CISE) Research Initiation Initiative (CRII), 2018.

National Science Foundation Graduate Research Fellowship, 2009.

Allen Newell Award for Excellence in Undergraduate Research, 2009.

Outstanding Undergraduate Research Award (Honorable Mention), 2009.

Andrew Carnegie Society Scholar, 2009.

School of Computer Science Honors, 2009.

Carnegie Mellon University Dean's List: Fall 2005, Spring 2006, Fall 2006, Spring 2007, Fall 2007, Fall 2008.

CMU Math Club: Spring Problem Contest Winner, 2007.

Last updated: April 4, 2024