Jeremiah Blocki

Current Position

(August 2016 to present)
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

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

Conference Publications

(*) Denotes Primary Author

1. (*) 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)]
2. (*) 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)]
3. (*) 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]

4. 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).

5. (*) 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]

6. (*) 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]

7. 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]

8. 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.

9. 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]

10. (*) 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]

11. (*) 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]

12. 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]

13. 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]

14. (*) 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]

15. (*) 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.

16. (*) 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]

17. (*) 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]

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

19. (*) 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]

20. (*) 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)]

21. 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).

22. (*) 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

23. (*) 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

24. (*) 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

25. (*) 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]

26. (*) 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]

27. (*) 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.*

28. 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).

29. 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.*

30. 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]

31. 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.*

32. 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.*

33. 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.*

34. (*) 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

Blocki, J. and Bai, W. Not All Equal: Stronger Password Protection via Differentiated Hashing Costs.

Blocki, J., Kulkarni, S. and Zhou S. On Locally Decodable Codes in Resource Bounded Channels.

Harsha, B. and Blocki, J. An Economic Model for Quantum Key-Recover Attacks.

Morton, R. Harsha, B. Blocki, J. and Spring J. Bicycle Attacks Considered Harmful: Quantifying the Damage of Widespread Password Length Leakage

Ameri, M. and Blocki, J. Memory Hard Functions in the Standard Model.

In Preparation

Blocki, J. and Wuwei, Z. DALock: Distribution Aware Password Lockout Policies.

Blocki, J., Liu, P., Ren, L. and Zhou, S. Bandwidth-Hard Functions: Reductions and Lower Bounds (Extended Journal Version).

Blocki, J. and Cinkoske, M. A Tight Relationship between Edge and Node Depth-Robustness.

Grants

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 4/30/2023. 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: 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.

(CMU) CSD PhD Admission Committee, 2013.

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

Journal Reviews & External Conference Reviews

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 2017.

International Symposium on Parameterized and Exact Computation.

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

University Service

CS Graduate Student Admissions Committee 2016-2018

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. CS381: Introduction to the Analysis of Algorithms (Fall 2019 [167])
2. CS580: Algorithm Design and Analysis (Spring 2018 [64], Spring 2019 [62])

3. CS55500: Cryptography (Spring 2017 [16], Fall 2017 [23], Fall 2018 [31])
4. CS59000: Passwords and Human Authentication Seminar (Fall 2016 [10], Spring 2020 [12]).
5. CS50010: Foundational Principles of Information Security (Summer 2018 [7])
6. CS50010: Foundational Principles of Information Security [Spring 2018, recorded lectures]

[# students]

PhD Students

Ben Harsha (Purdue CS, 2016- present) [Passed Prelim, Anticipated Graduation: Fall 2020]

Seunghoon Lee (Purdue CS, 2018-present)

Mohammad Hassan Ameri (Purdue CS, 2018-present)

Wenjie Bai (Purdue CS, 2018-present)

Peiyuan Liu (Purdue CS, 2018-present)

Wuwei Zhang (Purdue CS, 2014-present) [Advisor since 2019]

Alexander Block (Purdue CS, 2015-present) [Advisor since 2019]

Haoyu Song (Purdue CS, 2019-present)

Amin Mohammadi (Purdue CS, 2019-present)

MS and Undergraduate Students

Mike Cinkoske (Purdue CS Undegraduate, 2018- present)

Muqi Zhou (Purdue CS MS, 2018-present)

Shubhang Kulkarni (Purdue CS MS, 2019-present)

Past Postdocs

Samson Zhou (Purdue CS, Summer 2018)

Past 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

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

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: January 8, 2020