Jeremiah Blocki

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

Publications

(*) Denotes Primary Author

Password Hashing and Memory Hard Functions:

1. Blocki, J., Harsha, B. and Zhou, S. On the Economics of Offline Password Cracking. IEEE Security and Privacy (S&P 2018). [$<$ 13% acceptance rate (historical)]
2. (*) 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]
3. (*) Blocki, J. and Zhou, S. On the Depth-Robustness and Cumulative Pebbling Cost of Argon2i. Fifteenth IACR Theory of Cryptography Conference (TCC 2017). [32.9% acceptance rate (historical)]
4. Alwen, J., Blocki, J. and Pietrzak, K. 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2017). [20.3% acceptance rate (historical)]

5. (*) 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]

6. (*) 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]

7. (*) 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]

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

9. (*) 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 (historical)]

Usable and Secure Human Authentication:

10. (*) Blocki, J., Blum, M. Datta, A. and Vempala, S. Toward Human Computable Passwords. in the 8th conference on *Innovations in Theoretical Computer Science.* [41% acceptance rate (historical)] http://arxiv.org/abs/1404.0024.

11. (*) 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

12. (*) 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

13. (*) 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

14. (*) 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]

Privacy Preserving Data Analysis:

15. 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]

16. (*) 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]

17. (*) 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]

18. 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]

19. (*) 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]

Game Theory and Security:

20. 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).

21. (*) 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.*

22. 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).

23. 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.*

24. 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.*

25. 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.*

26. 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.*

Working Papers

Blocki, J. On the Amortized AT Complexity of SCRYPT and Argon2id.

Blocki, J. and Harsha, B (student). Just-in-time Password Hashing.

Blocki, J. and Zhou, S (student). On the Computational Complexity of Minimal Cumulative Cost Graph Pebbling. https://arxiv.org/abs/1609.04449.

Beideman, C and Blocki, J. Set Families with Low Pairwise Intersection. http://arxiv.org/abs/1404.4622.

Grants

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

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

Professional Activities and Service

Internal

Graduate Student Admissions Committee 2016-2018

External

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`

Teaching

1. CS580: Algorithms (Spring 2018)
2. CS55500: Cryptography (Fall 2017, Spring 2017)
3. CS59000: Passwords and Human Authentication Seminar (Fall 2016).

Graduate

Teaching Assistant for 15-453: Formal Languages, Automata and Computation (Spring 2012).

Head Teaching Assistant for 15-451: Algorithms (Fall 2010).

Undergraduate

Teaching Assistant for 15-859P: Introduction to Theoretical Cryptography (Fall 2009)

Teaching Assistant for 15-251: Great Theoretical Ideas in Computer Science (Spring 2008).

Teaching Assistant for Calculus 1 (Summer 2008).

Students

Ben Harsha (Purdue CS, 2016- present)

Alina Nesen (Purdue CS, 2017-present)

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

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

Lectures

Course: 18-739: Foundations of Security and Privacy (Fall 2009).
Lecture: Differentially Private Recommender Systems: Building Privacy into the Netflix Prize Contenders.

Course: 15-451: Algorithms (Fall 2010).
Lecture: Fun with BFS and DFS.

Course: 18-739: Foundations of Security and Privacy (Fall 2011).
Lecture: Passwords II.

Course: 15-453: Formal Languages, Automata and Computation (Spring 2012).
Lecture: Undecidable Problems.

Course: 15-453: Formal Languages, Automata and Computation (Spring 2012).
Lecture: Usable and Secure Password Management.

Course: 18-734: Foundations of Privacy.
Lecture: Zero-Knowledge Proofs.

Course: 15-455: Undergraduate Complexity Theory.
Lecture: Passwords.

Talks

Releasing a Differentially Private Password Frequency Corpus from 70 Million Yahoo! Passwords. 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 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.

Posters

Naturally Rehearsing Passwords, NSF TRUST Fall Conference 2013.

Differentially Private Analysis of Social Networks via Restricted Sensitivity, Poster Fair on Privacy Research and Education at Carnegie Mellon University 2013.

Guessing Games: Evaluating the Security of a Password Management Scheme, GameSec 2013.

Usable and Secure Password Management, CMU SCS Open House 2013.

Regret Minimization in Bounded Memory Games, STOC 2011.

Honors, Awards, & Fellowships

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.

Employment

Research with Professor Manuel Blum: Direct Zero-Knowledge Proofs (Summer 2008).

Research Experience for Undergraduates at Carnegie Mellon University (Summer 2007)

Peer Tutoring at CMU Academic Development (2006-2008)

Software Engineering Intern at Haley Systems (Summer 2006)

Software Engineering Intern at CMU Software Systems Lab (Summer 2005)

Miscellaneous

Interests and Activities

Graduate Christian Fellowship

Basketball

Softball

Last updated: November 7, 2017