Curriculum Vitae: Sarah Ann Scheffler

sarah.ann.scheffler@gmail.com
https://sarahscheffler.net
https://github.com/sarahscheffler

18 Vandeventer Ave #1
Princeton, NJ 08542
(720) 234 - 6853

EDUCATION

Postdoctoral Research Associate, Princeton University Center for Information Technology Policy
September 2021 - Present

Ph.D. in Computer Science, Boston University, GPA 3.98
Advisor: Prof. Mayank Varia
Thesis: Decrypting Legal Dilemmas
Computer Science Research Excellence Award
September 2016 - June 2021

B.S. joint in Computer Science and Mathematics, Harvey Mudd College, GPA 3.4
Departmental Honors in Computer Science
Graduated with Distinction
September 2011 - May 2015

REFEREED CONFERENCE PUBLICATIONS

[1] Y. Gvili, J. Ha, S. Scheffler, M. Varia, Z. Yang, X. Zhang.
TurboIKOS: Improved Non-interactive Zero Knowledge with Sublinear Memory.
In Applied Cryptography and Network Security 2021.
https://ia.cr/2021/478.

[2] Y. Gvili, S. Scheffler, M. Varia.
BooLigero: Improved Sublinear Zero Knowledge Proofs for Boolean Circuits.
In Financial Crypto 2021.
https://ia.cr/2021/121.

[3] S. Scheffler M. Varia.
Protecting Cryptography against Compelled Self-Incrimination.
In USENIX Security 2021.
https://ia.cr/2020/862.

[4] L. Alcock, S. Asif, J. Bosboom, J. Brunner, C. Chen, E. Demaine, R. Epstein, A. Hesterberg, L. Hirschfeld, W. Hu, J. Lynch, S. Scheffler, L. Zhang.
Arithmetic Expression Construction.
In International Symposium on Algorithms and Computation 2020.
https://arxiv.org/abs/2011.11767.

[5] J. Milligan, S. Scheffler, A. Sellars, T. Tiwari, A. Trachtenberg, M. Varia.
Case Study: Disclosure of Indirect Device Fingerprinting in Privacy Policies.
In Socio-Technical Aspects of Security 2019.
https://arxiv.org/abs/1908.07965.

[6] J. Ani, S. Asif, E. Demaine, Y. Diomidov, D. Hendrickson, J. Lynch, S. Scheffler, A. Suhl.
PSPACE-completeness of Pulling Blocks to Reach a Goal.
In the Japan Conference on Discrete and Computational Geometry, Graphs, and Games 2019.

[7] R. Canetti, A. Cohen, N. Dikkala, G. Ramnarayan, S. Scheffler, A. Smith.
From Soft Classifiers to Hard Decisions: How fair can we be?.
ACM Fairness, Accountability, and Transparency 2019.
https://arxiv.org/abs/1810.02003.

[8] S. Scheffler, S. Smith, Y. Gilad, S. Goldberg.
The Unintended Consequences of Email Spam Prevention.

In International Conference on Passive and Active Network Measurement 2018.
https://link.springer.com/chapter/10.1007/978-3-319-76481-8_12.

JOURNAL PUBLICATIONS

[9] J. Ani, S. Asif, E. Demaine, Y. Diomidov, D. Hendrickson, J. Lynch, S. Scheffler, A. Suhl.
PSPACE-completeness of Pulling Blocks to Reach a Goal.
In the Journal of Information Processing 2020.
https://www.jstage.jst.go.jp/article/ipsjjip/28/0/28_929/_pdf.

WORKS IN PREPARATION

[10] S. Scheffler, A. Kulshrestha, J. Mayer.
Public Verification for Private Hash Matching: Challenges, Policy Responses, and Protocols.
Under submission at IEEE S&P 2022.

[11] S. Scheffler, J. Mayer.
Systemization of Knowledge: Content Moderation and End-to-End Encryption.
Work in progress, planned for submission in Jan 2022.

[12] S. Scheffler.
A U.S. Policy Proposal for Preventing Scope Creep in End-to-End Encrypted Content Moderation.
Work in progress, planned for submission in Jan 2022.

[13] S. Scheffler, E. Tromer, M. Varia.
Formalizing Substantial Similarity.
Work in progress, planned for submission in March 2022.

[14] A. Cohen, S. Scheffler, M. Varia.
A Verifiability-based Technical View of the Foregone Conclusion Doctrine.
Work in progress, planned for submission in March 2022.

MANUSCRIPTS

[15] S. Scheffler, J. Ostling.
Dismantling False Assumptions about Autonomous Weapon Systems.
Manuscript.
Won 2nd place in the Student Paper Competition at the ACM CSLaw Student Paper Competition in 2019.
https://sarahscheffler.net/Autonomous_Weapons_False_Assumptions.pdf.

[16] J. Hennessey, S. Scheffler, M. Varia.
On Resilient Password-Based Key Derivation Functions.
Manuscript.
https://sarahscheffler.net/diskcrypt/draft-2018-bog.pdf.

HONORS, AWARDS, AND FELLOWSHIPS

Boston University Computer Science Research Excellence Award (2021)
RSA Conference Security Scholar (2020)
ACM CSLaw Student Paper Competition: 2nd Place (2019)
Google Ph.D. Fellowship (2019-2021)
Clare Boothe Luce Graduate Fellowship (2017-2019)
Clinic Team Award, HMC Computer Science Department (2015, awarded for an exceptional capstone project)

International Mathematical Competition in Modeling: Meritorious Winner (2014), Honorable Mention (2015)

INVITED TALKS

USENIX Security (Aug. 2021)
Privacy Law Scholars Conference (June 2021)
Cryptic Commons Workshop (May 2021)
Georgetown Data Co-Ops Meeting (March 2021)
Data Co Ops Meeting (Mar. 2021)
Duke Privacy and Security Seminar (Mar. 2021)
Stanford Security Seminar (Feb. 2021)
Berkeley Cryptography Seminar (Jan. 2021)
Winter Security Seminar Series at Carnegie Mellon University (Jan. 2021)
Real World Crypto (Jan. 2021)
MIT Security Seminar (Dec. 2020)
Guest lecturer at ETH Zurich course "Approaches to Authentication and Security: Views from Law, Economics, and the Scientific Disciplines" (Nov. 2020)
Northeastern Privacy Scholars Workshop (Nov. 2020)
DIMACS Workshop on the Co-Development of Computer Science and Law (Nov. 2020)
Boston University Security Seminar (Oct. 2020)
Cybersecurity Law and Poicy Scholars Conference (planned Apr. 2020, two papers accepted for discussion, event postponed to Dec. 2020 due to COVID-19)
Bridging Privacy seminar at Berkman Klein Center for Internet and Society (Dec. 2019)
Cornell Crypto Seminar (Nov. 2019)
Carnegie Mellon University AI Seminar (Oct. 2019)
Boston University CyberAlliance Seminar (Dec. 2018)

PROGRAM COMMITTEES

Program Committee:
Workshop on Foundations of Computer Security 2021

Shadow Program Committee:
IEEE S&P 2020

External Reviewer:
USENIX Security 2022
IEEE Security & Privacy 2021
ISCA Symposium on Security and Privacy in Speech Communication 2021
Theory of Cryptography Conference 2020
Eurocrypt 2020
IEEE Security & Privacy 2020
ACM Conference on Fairness, Accountability, and Transparency 2020
IEEE Computer Security Foundations Symposium 2018
International Conference on Cryptology and Network Security 2017
International Conference on Information Theoretic Security 2016

K12 OUTREACH

RACECAR Crash Course: From Oct. 2018 - Jan. 2019, volunteered as a teaching assistant for this program to prepare high school students for the Beaver Works Summer Institute RACECAR course in the summer.
Code Creative: From Jan. 2017 - Jan. 2018, was a mentor for Code Creative, a computer science education program for Boston-area high school students who do not have access to a computer science course at their schools. Was responsible for creating slides and labs, lecturing, organizing, and in-class tutoring. https://www.codecreative-ll.org/

Codebreakers: In summer 2016, as one of a team of three, created and taught a summer cybersecurity class for high school girls. Was responsible for creating the curriculum, creating class material and exercises, and leading classes. In 2017, 2018, and 2019, was a guest lecturer. https://www.bu.edu/lernet/cyber/

TEACHING EXPERIENCE

Teaching Fellow: Applied Cryptography, Boston University Computer Science Department (Spring 2018, Spring 2017)
Head Grader: Linear Algebra (2013) and Differential Equations (2013), HMC Department of Mathematics
Tutor/Grader: Programming Languages (2014) and Principles of Computer Science (2013) and Intro to Computer Science (2013), HMC Computer Science Department
Grader: Multivariable Calculus (2013) and Calculus (2012) and Probability and Statistics (2012), HMC Department of Mathematics

TRAVEL GRANTS

Real World Crypto (2020), Crypto (2019, 2018), ACM Symposium on Theory of Computing (2019)

WORK EXPERIENCE

Assistant Staff MIT Lincoln Laboratory Sep. 2015 - June 2016

Worked in the Secure and Resilient Systems and Technology group within the Cybersecurity and Information Sciences division. Assisted in the implementation and testing of a library that adds confidentiality and integrity guarantees to the Accumulo database, protecting it against a malicious server or sysadmin.

Implementing Oblivious RAM MIT Lincoln Laboratory Summer 2015

Designed and implemented an Oblivious RAM for the Accumulo database in Java, to hide a querying client's access patterns from a malicious server as part of a larger project within the Secure and Resilient Systems and Technology group.

Quantifying Latent Fingerprint Quality The MITRE Corporation and HMC Fall 2014 - Spring 2015

Worked on a team of four students to design, implement, and test a system that uses image processing and machine learning techniques to evaluate the suitability of crime scene fingerprint images for identification by Automated Fingerprint Identification Systems.

Statistical Testing of Cryptographic Entropy Sources NIST Summer 2014

Worked with Dr. Allen Roginsky in the Computer Security Division of the National Institute of Standards and Technology (NIST) to improve NIST's statistical tests for entropy sources in cryptographic random number generators. Also made adjustments to the process for generating large primes for cryptography.

COMPUTER SKILLS

Programming: Rust, Python, C++, C, Haskell, Java, Prolog
Software and Frameworks: NTL, SCALE-MAMBA (SPDZ-2), Mathematica, Sage, R, Matlab, LaTeX

RELEVANT COURSEWORK

Cryptography: Multi-Party Computation at Scale, Cryptography, Applied Cryptography, Lattice Cryptography
Computer science: Privacy in Machine Learning, Adaptive Data Analysis, Networks, Security, Malware/Vulnerabilities
Law: Law and Algorithms (joint between BU, Harvard, UC Berkeley, and Georgetown), National Security and Technology
Mathematics: Abstract Algebra, Probability, Number Theory, Linear Algebra, Numerical Analysis