Curriculum Vitae: Sarah Ann Scheffler

sarah.ann.scheffler@gmail.com
https://cs-people.bu.edu/sscheff
https://github.com/sarahscheffler

25 Lake St#2
Somerville, MA 02143
(720) 234 - 6853

EDUCATION

Fifth-year Ph.D. student in Computer Science, (advisor: Prof. Mayank Varia), Boston University, GPA 3.98

Bachelor of Science, Computer Science and Mathematics, Harvey Mudd College (HMC), GPA 3.4
Graduated with Distinction and with Honors in Computer Science, May 2015

PUBLICATIONS

[1] Y. Gvili, S. Scheffler, & M. Varia. *BooLigero: Improved Sublinear Zero Knowledge Proofs for Boolean Circuits.* Forthcoming in Financial Crypto 2021.

[2] S. Scheffler & M. Varia. *Protecting Cryptography against Self-Incrimination.* Forthcoming in USENIX Security 2021. https://ia.cr/2020/862

[3] 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

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

[5] 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 (JCDCGˆ3) 2019 and the Journal of Information Processing 2020.

[6] 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 (ACM FAT*) 2019. https://arxiv.org/abs/1810.02003

[7] S. Scheffler, S. Smith, Y. Gilad, & S. Goldberg. *The Unintended Consequences of Email Spam Prevention.* In International Conference on Passive and Active Network Measurement. https://link.springer.com/chapter/10.1007/978-3-319-76481-8_12.

HONORS, AWARDS, AND FELLOWSHIPS

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

Stanford Security Seminar (Jan. 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

Shadow PC for IEEE S&P 2020
Subreviewer for: IEEE S&P 2021, TCC 2020, Eurocrypt 2020, IEEE S&P 2020, FAT* 2020, CSF 2018, CANS 2017, ICITS 2016

K12 OUTREACH

Titanoboa Intro to Programming: Planned for Spring of 2021, proposed and co-organized a course covering an introduction to Python as well as several other computing-related topics, aimed at teaching students of races underrepresented in STEM.
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)

RESEARCH PROJECTS

Efficient Blacklists for E2E Encrypted Messaging BU Sep. 2018 - Present

Ongoing research with Prof. Mayank Varia and students, using Private Set Intersection and Searchable Encryption methods to create a method for using a server-side blacklist to allow a receiving client to flag banned messages in end-to-end encrypted chat, in an efficient manner that maintains small ciphertext size and sufficiently low delivery time.

Protecting Cryptography from Self-Incrimination BU Jan. 2019 - Present

Ongoing research with Prof. Mayank Varia, technical analysis of the current state of affairs with regard to whether various cryptographic constructs can be compelled in a government subpoena as a "foregone conclusion" exception to the U.S. 5th Amendment right against self-incrimination.

Legality of Lethal Autonomous Weapons BU Jan. 2018 - Oct. 2019

In a partnership with a law student, corrected false assumptions in the ongoing debate over whether to ban or otherwise regulate fully autonomous weapons systems, and analyzing how their "predictability" influences their legality under the Law of Armed Conflict. Won 2nd place in the ACM CSLaw Student Paper Competition.

Fairly Post-Processing Calibrated Classifiers BU Jan. 2018 - Jan. 2019

Ongoing research with Prof. Ran Canetti and Prof. Adam Smith, seeking to analyze the algorithmic fairness properties that can be achieved when post-processing a non-binary classifier that is calibrated into a binary decision. [6]

Privacy Policy Disclosure of Device Fingerprinting BU Dec. 2018 - Jun. 2019

Joint work with Prof. Mayank Varia, Prof. Ari Trachtenberg, Prof. Andrew Sellars, Prof. Julissa Milligan, and Trishita Tiwari. An investigation into major websites' disclosure methods for Canvas fingerprinting and a dichotomy of fingerprinting practices into "direct" and "indirect," with predictions for the future of privacy on the web. [4]

Failure-Resistant Ensemble PBKDF BU Jan. 2017 - Present

Ongoing research with Prof. Mayank Varia and Dr. Jason Hennessey, proposing a new approach to Password-Based key Derivation Functions (PBKDFs) that has failure-resistance, is optimized for specific platforms, and resistance to pipelining and parallelism.

DNS Vulnerabilities through Email BU Jan. 2017 - Jan. 2018

Ongoing research with a group of students advised by Prof. Sharon Goldberg, use spam prevention techniques like SPF and DKIM to exploit vulnerabilities in the Domain Name System to cause denial of service attacks or DNS cache poisoning. [7]

Manipulating BGP through MD5 Cryptanalysis BU Sep. 2016 - Dec. 2016

As part of a research group advised by Prof. Sharon Goldberg, exploited known cryptographic vulnerabilities in the MD5 message digest algorithm to cause a subprefix hijack attack on the Border Gateway Protocol (BGP).

Accountability of Risk Assessment Systems BU Sep. 2018 - Dec. 2018

A non-technical analysis of the accountability properties of three government-endorsed risk assessment tools: Unified Passenger (a U.S. Customs and Border Protection tool designed to detect criminal or terrorist connections at border crossings), the COMPAS Risk & Needs Assessment tool for criminal sentencing, and FICO credit scores.

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