Sarah Ann Scheffler

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

5 Maxwells Grn #303
Somerville, MA 02144
(720) 234 - 6853

EDUCATION

Second-year Ph.D. candidate, Computer Science (applied cryptography), Boston University, GPA 3.95
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

HONORS AND AWARDS

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)
Dean's List (2012-2015)

RELEVANT COURSEWORK

Cryptography: Multi-Party Computation at Scale, Cryptography, Applied Cryptography, Lattice Cryptography
Computer science: Adaptive Data Analysis, Computer Networks, Computer Security, Malware and Vulnerabilities
Mathematics: Abstract Algebra, Number Theory, Linear Algebra, Numerical Analysis, Probability

COMPUTER SKILLS

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

RESEARCH AND WORK EXPERIENCE

Failure-Resistant Ensemble PBKDF Boston University Boston, MA Jan. 2017 - Present

Ongoing research with Dr. 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 Boston University Boston, MA Jan. 2017 - Present

Ongoing research with a group of students advised by Dr. 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.

Manipulating BGP through MD5 Cryptanalysis Boston University Boston, MA Sep. 2016 - Dec. 2016

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

Codebreakers Coordinator, Lecturer Boston University Boston, MA Summer 2016, 2017

In 2016, as one of a team of three, created and taught a summer cybersecurity class for high-schoolers. Was responsible for creating the curriculum, creating class material and exercises, and leading classes. In 2017, was a guest lecturer.

Assistant Staff MIT Lincoln Laboratory Lexington, MA 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 Lexington, MA 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 Gaithersburg, MD 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.