Zachary Ratliff

https://zacharyratliff.org
zacharyratliff@g.harvard.edu

Research Interests

My primary research interests are in cryptography, privacy (specifically, differential privacy), and systems security. I am particularly interested in using techniques from cryptography to make systems more secure and privacy-preserving for the people they serve.

Education

Ph.D., Computer Science – Harvard University, Cambridge, MA, USA 2021 – 2026
Advisors: Prof. Salil Vadhan & Prof. James Mickens
Member of the Theory of Computation Group, Harvard Privacy Tools Project, and OpenDP

B.S., Computer Science – Texas A&M University, College Station, TX, USA 2015 – 2018
Undergraduate Thesis Advisor: Prof. Daniel Ragsdale
Minor in Mathematics, Cybersecurity

Professional Experience

Raytheon BBN, Networks & Cyber Technologies, Cambridge, MA, USA 2019 – Present

- **Staff Scientist** (2021 – Present)
- **Associate Scientist** (2019 – 2021)

I primarily consult on security and privacy where I have contributed to several projects across various business units. I have additionally contributed to the following successful proposals: *NSC Secure 5G MANET* ($6.5m/2yr), *TacNets* ($6.5m/2yr), *Proprietary #1* ($1m/1yr), and *Proprietary #2* ($1.2m/1yr).

Proprietary #1 – **Technical lead**. Cryptographic protocol analysis using formal methods. Used the Tamarin Automated Theorem Prover to model and analyze the security of cryptographic protocols.

MANTIS (AFRL) – Designed and implemented zero-knowledge proofs for verifiable content filtering in cross-domain solutions. I programmed efficient arithmetic circuits for various image processing algorithms using the R1CS language and the libsnark library. (C++).

Proprietary #2 – Cryptographic protocol design.

Oxygen (NSC) – Designed a protocol for mutual authentication of O-RAN subcomponents within decentralized MANETs. Consulted on cryptographic erasure techniques for fast and secure data wiping.

SB-FAC (IARPA) – Performed a red-team analysis of a privacy-preserving bloom filter architecture and developed formal proofs of security.

Network-UP (DARPA) – Designed and implemented algorithms for improving performance in mobile ad hoc networks that experience frequent and severe signal degradation. My contributions include writing reinforcement-learning algorithms for adapting channel access decisions based on environmental conditions. (C, Python).

Brandeis (DARPA) – Integrated privacy-enhancing technologies for mobile Android devices. My contributions include developing Android applications that used secure multi-party computation and differentially private algorithms to protect sensitive user data. (Java, Python, Docker, AWS).

VirtUE (IARPA) – Designed and implemented a Linux kernel module for rule-based packet filtering using the netfilter framework. The functionality fit into a larger system that provided intrusion detection/prevention capabilities in secure computing environments. (C, Python, AWS, Docker).

Internships

(2016-2018) **Undergraduate Research Intern**. Raytheon BBN, Cambridge, MA, USA

(2018) **Undergraduate Researcher**. Texas A&M Cyber Center, College Station, TX, USA

(2016) **Undergraduate Research Fellow**. NIST, Information Technology Lab, Gaithersburg, MD, USA

(2015) **Undergraduate Research Fellow**. NIST, Information Technology Lab, Gaithersburg, MD, USA

Teaching and Service

(Fall 2023) Head Teaching Fellow, Intro. to Algorithms & Their Limitations, Harvard University

(Summer 2023) Organizing Committee Member for OpenDP Community Meeting

(Summer 2023) Mentor for OpenDP summer intern Nicolas Berrios

(Fall 2022) Head Teaching Fellow, Intro. to Algorithms & Their Limitations, Harvard University

- **Awarded Certificate of Distinction for Teaching**

(Summer 2022) Mentor for Harvard undergraduate researcher Wittmann Goh

(Summer 2022) Mentor for OpenDP summer intern Vicki Xu

(Summer 2022) Mentor for OpenDP summer intern Hanwen Zhang

(Fall 2022 – Present) Co-organizer of Harvard's Privacy Tools seminar

Research Talks

(2023) A Framework for Differential Privacy Against Timing Attacks. TPDP 2023 Poster Session.

(2023) Provable Security for Fun & Profit. Raytheon BBN Networks & Cyber Lunch Talk.

(2023) Mitigating Timing Attacks on Differential Privacy. SEAS Research Showcase.

(2023) Private Resource Allocators and their Applications. Harvard Theory Group TGINF Seminar.

(2022) Verifiable Computation for Cross-Domain Systems. Raytheon BBN Networks & Cyber Lunch Talk.

(2021) Towards Decentralized and Provably Secure Cross-Domain Solutions. Online at the ESORICS Workshop on Security and Trust Management.

(2019) Detecting Vulnerabilities in Android Applications using Event Sequences. Sofia, Bulgaria, Conference on Software Quality, Reliability and Security.

Honors, Fellowships, & Awards

(2020) Innovation Award, Raytheon Intelligence & Space

(2020) Honorable Mention, National Science Foundation Graduate Research Fellowship Program

(2018) Undergraduate Research Scholar Honors Distinction, Texas A&M University

(2016) Research Poster Scholarship, 1st place, Texas A&M Industrial Affiliates Program

(2016) Undergraduate Research Fellowship, National Institute of Standards & Technology

(2015) NIST Reference Data Challenge Finalist

(2015) Undergraduate Research Fellowship, National Institute of Standards & Technology

Publications

Ratliff, Z., Goh, W., Wieland, C., Mickens, J., & Williams, R., (2024, May). Holepunch: Fast, Secure File Deletion with Crash-Consistency. In 2024 IEEE Symposium on Security and Privacy (SP). IEEE.

Ratliff, Z., Vadhan, Salil. (2023, September). A Framework for Differential Privacy against Timing Attacks. In Theory and Practice of Differential Privacy (TPDP).

Khoury, J., **Ratliff, Z**., & Atighetchi, M. (2021, October). Towards Decentralized and Provably Secure Cross-Domain Solutions. In International Workshop on Security and Trust Management (pp. 185-203).

Angel, S., Kannan, S., & **Ratliff, Z**. (2020, May). Private resource allocators and their applications. In 2020 IEEE Symposium on Security and Privacy (SP). IEEE.

Z. Ratliff, D. R. Kuhn, and D. Ragsdale. Detecting Vulnerabilities in Android Applications using Event Sequences. In 2019 IEEE 19th International Conference on Software Quality, Reliability and Security (QRS), 2019.

(Undergraduate Thesis) **Z. Ratliff**, (2018). Black-box Testing Mobile Applications Using Sequence Covering Arrays.

Z. Ratliff, D. R. Kuhn, R. N. Kacker, Y. Lei, and K. S. Trivedi. The Relationship between Software Bug Type and Number of Factors Involved in Failures. In 2016 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), 2016.

Patents

Ratliff, Z.., Khoury, J. (2021). Privacy-preserving contact tracing. US Patent App. 17/326,498.

Khoury, J., Atighetchi, M., & **Ratliff, Z.** (2021). Verifiable computation for cross-domain information sharing. US Patent App. 17/172,825

Miscellaneous

Programming: C/C++, Java, Rust, Python

Skills: Amazon AWS, Bash/Shell scripting, Linux Kernel development, Android application development, QEMU+KVM, gdb, Assembly language, Tamarin automated theorem prover

Relevant Coursework:

- **Harvard**: Cryptography, Systems Security, Information Theory, Applied Data Privacy, Algorithmic Fairness, Advanced Computer Architecture
- **MIT**: Advanced Topics in Cryptography
- **Texas A&M**: Intro to Modern Cryptography, Structures & Methods of Combinatorics, Probability Theory, Networks & Distributed Processing, Wireless & Mobile Systems, Artificial Intelligence, Computer Security, Software Reverse Engineering