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 that use them.

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

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

Proprietary #1 – **Technical lead**. Cryptographic protocol analysis using formal methods.

Proprietary #2 – Cryptographic protocol design.

MANTIS (AFRL) – Designed and implemented zero-knowledge proofs for verifiable content filtering. Programmed efficient arithmetic circuits for various image processing algorithms using the libsnark library. (C++).

Oxygen (NSC) – Consulted on protocols for mutual authentication and secure data wiping in MANETs.

SB-FAC (IARPA) – Performed a red-team analysis of a privacy-preserving bloom filter architecture.

Network-UP (DARPA) – Designed and implemented Q-Learning algorithms for adapting channel access decisions in mobile ad hoc networks that experience frequent and severe signal degradation. (C, Python).

Brandeis (DARPA) – Integrated secure multi-party computation and differential privacy into privacy-enhancing Android applications designed to protect sensitive user data. (Java, Python, Docker, AWS).

VirtUE (IARPA) – Designed and implemented a Linux kernel module that performed rule-based packet filtering for 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

(Spring 2025) Head Teaching Fellow, Applied Privacy for Data Science, Harvard University

(Summer 2024 - Present) Co-lead of the Privacy Attacks and Auditing Task Force for OpenDP Working Group

(Summer 2024) Organizing Committee Member for OpenDP Community Meeting

(Spring 2024) Co-organizer of 2024 Sydney Privacy Workshop

(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

(2025) Securing Unbounded Differential Privacy Against Timing Attacks. **TPDP 2025 Poster Session**.

(2024) A Framework for Differential Privacy Against Timing Attacks. **Boston University Security Seminar**.

(2024) A Framework for Differential Privacy Against Timing Attacks. **Google Algorithms Seminar**.

(2024) A Framework for Differential Privacy Against Timing Attacks. **ACM CCS 2024**.

(2024) Differential Privacy in the Presence of Side Channels. **Raytheon BBN Networks & Cyber Seminar**.

(2024) Pure Timing-Private Programs. **Harvard Theory Group TGINF Seminar**.

(2024) Holepunch: Fast, Secure Deletion with Crash Consistency. **IEEE S&P 2024**.

(2024) A Framework for Differential Privacy Against Timing Attacks. **Sydney Privacy Workshop**.

(2024) A Framework for Differential Privacy Against Timing Attacks. **University of Sydney SACT Seminar**.

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

(2023) Provable Security for Fun & Profit. **Raytheon BBN Networks & Cyber Seminar**.

(2023) Mitigating Timing Attacks on Differential Privacy. **Harvard 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 Seminar**.

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

(2019) Detecting Vulnerabilities in Android Applications using Event Sequences. **IEEE QRS 2019**.

Honors, Fellowships, & Awards

(2026) Siebel Scholar

(2024) ACM CCS 2024 Distinguished Artifact Award

(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., Bai, A., Yang, D., Berger, H., Sherr, M., & Mickens, J., (2025, April). Mirage: Private Mobility-based Routing for Censorship Evasion. (to appear at NDSS 2026).

Ratliff, Z., & Vadhan, S., (2025, May). Securing Unbounded Differential Privacy Against Timing Attacks. (To appear at TCC 2025).

Ratliff, Z., Berrios, N., & Mickens, J., (2025, February). Timing Attacks on Differential Privacy are Practical. (To appear at CCS 2025).

Ratliff, Z., & Vadhan, S., (2024, October). A Framework for Differential Privacy Against Timing Attacks. In 2024 ACM Conference on Computer and Communications Security (CCS). ACM. **(*Distinguished Artifact Award)**

Ratliff, Z., Berrios, N., & Mickens, J., (2024, August). The Pervasiveness of Timing Side-Channels in Differential Privacy. In Theory and Practice of Differential Privacy (TPDP 2024).

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 2023).

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, Formal Methods for Computer Security, Cybersecurity Policy & Law
- **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