# Rachel Thomas

rthomase@umd.edu | LinkedIn | Website

## Technical Skills

**Programming**: Python, Java, JavaScript, Rust, C/C++, Swift, Assembly

**Web/Database**: HTML/CSS, SQL

**Functional/Logic**: Lisp, Prolog, ML

## Education

**University of Maryland at College Park** Aug 2024 – Present
*Doctor of Philosophy in Computer Science* *College Park, MD*

**University of North Carolina at Chapel Hill** Jan 2023 – May 2024
*Master of Science in Computer Science* *Chapel Hill, NC*

**University of North Carolina at Chapel Hill** Aug 2018 – Dec 2022
*Bachelor of Science in Computer Science* *Chapel Hill, NC*

- Minor in Mathematics

## Experience

**Teaching Assistant** Aug 2024 – Present
*Department of Computer Science, University of Maryland* *College Park, MD*

- Supported instruction in CMSC 414: *Computer and Network Security* and CMSC 839C: *Governing Algorithms & Algorithmic Governance*, covering topics including cryptography, network protocols, security vulnerabilities, and algorithmic governance in AI systems.
- Managed course logistics, including grading, resource organization, and communication, while holding office hours to provide technical guidance and mentorship to students.

**Research Assistant** Aug 2024 – Present
*Department of Computer Science at University of Maryland* *College Park, MD*

- Collaborated with interdisciplinary research teams at UMD to design and implement privacy-preserving cryptographic protocols, contributing to publications and project development.
- Assisted in grant proposal development, including writing and refining research statements, to secure funding for privacy and security initiatives.

**Research Assistant** Aug 2022 – May 2024
*Department of Computer Science at UNC Chapel Hill* *Chapel Hill, NC*

- Conducted research in privacy-enhancing technologies, cryptography, and side-channel attacks, collaborating with researchers to develop novel cryptographic techniques. Co-authored peer-reviewed publications and presented findings at academic conferences.
- Assisted in mentoring undergraduate students and junior researchers, guiding them through complex research methodologies and experimental designs.

**Learning Assistant** Aug 2021 – Dec 2021
*Department of Mathematics at UNC Chapel Hill* *Chapel Hill, NC*

- Supported instruction for MATH 233 - Calculus of Functions of Several Variables, assisting the professor with course delivery and student engagement.
- Conducted individual and group tutoring sessions during office hours, addressing student inquiries and enhancing their understanding of complex calculus concepts.

## Publications

**CheckOut: User-Controlled Anonymization for Customer Loyalty Programs** July 2024
*Matthew Gregoire,* ***Rachel Thomas****, Saba Eskandarian* *PoPETS 2024*

- Published in the *24th Privacy Enhancing Technologies Symposium (PoPETS)*

## Projects

**California Delete Act Compliance via Secure PSI** June 2025 – Present
*Collaboration with UMD, Purdue, and Brown University* *College Park, MD*

- Designed a malicious-secure PSI protocol with input/output consistency guarantees to enforce compliance with the California Delete Act.
- Addressed variable set sizes (servers vs. large data brokers) and optimized protocol design to minimize auditor and regulator workload for deployability.

**Zero-Knowledge Social Proofs** June 2025 – Present
*Department of Computer Science at University of Maryland* *College Park, MD*

- Engineered a zero-knowledge proof framework using *zkPass (zkTLS)* to enable privacy-preserving verification of user attributes (e.g., citizenship, email, and account ownership) without revealing underlying data.
- Developed a composite construction integrating VDFs and aPAKE protocols to provide secure deduplication, forward secrecy, and resistance to offline brute-force attacks in the event of server compromise.

**Cryptographic Personas: Responsible Pseudonyms without De-Anonymization** Aug 2024 – Present
*Department of Computer Science at University of Maryland* *College Park, MD*

- Developed *cryptographic personas*, an anonymous and pseudonymous messaging framework enabling unlinkable identities with revocable anonymity for moderation.
- Optimized efficiency via offline proof generation and proof folding, and integrated a working prototype into Signal for real-time deployment.

**Side-Channel Analysis of Microsoft Edge Password Leak Detection Protocol** Aug 2023 – May 2024
*Department of Computer Science at UNC Chapel Hill* *Chapel Hill, NC*

- Conducted research uncovering side-channel vulnerabilities in Microsoft Edge's Password Leak Detection Protocol and Microsoft SEAL homomorphic encryption library.
- Designed and tested attack vectors in both native and browser-based environments, building realistic threat models to evaluate protocol security.

**CheckOut: User-Controlled Anonymization for Customer Loyalty Programs** May 2022 – May 2024
*Department of Computer Science at UNC Chapel Hill* *Chapel Hill, NC*

- Built a scalable system for obfuscating loyalty card transactions, enabling equitable benefits while protecting users from retailer tracking.
- Developed a privacy-preserving mobile application and protocol leveraging cryptographic techniques to secure user data and anonymize loyalty barcodes.

## Awards

**Dean's Fellowship** Aug 2024
*University of Maryland at College Park* *Fellowship*

**Degree With Distinction** Dec 2023
*University of North Carolina at Chapel Hill* *Honors*

**Summer Award for Research-Intensive Courses** May 2022
*Office of Undergraduate Research at UNC Chapel Hill* *Fellowship*