MATTHEW GREGOIRE

506 N Greensboro St, Apt. 30 ⋄ Carrboro, NC 27510

(828) · 707 · 1107 ⋄ matthew@igregoire.com

EDUCATION

University of North Carolina at Chapel Hill   *August 2021 - May 2026 (expected)*

Ph.D. Candidate in Computer Science

University of North Carolina at Chapel Hill   *August 2021 - December 2023*

M.S. in Computer Science

Overall GPA: 4.00 (Unweighted)

Relevant courses: Cryptography, Computer Security, Privacy Enhancing Technologies, Logical Foundations

University of North Carolina at Chapel Hill   *August 2017 - May 2021*

B.S. in Computer Science & Mathematics

Overall GPA: 3.98 (Unweighted)

Deans list (all semesters)

Relevant courses: Algorithms, Operating Systems, Digital Logic, Algebraic Structures, Probability

North Carolina School of Science and Mathematics   *August 2015 - May 2017*

High school diploma

Overall GPA: 5.54 (Weighted)

PUBLICATIONS

- **Gregoire, M.**, Schell, G., & Eskandarian, S. (2026). Third-Party Moderation of Abuse Reports for End-to-End Encrypted Messaging with Multiple Moderators. (Preprint).

- Choudhuri, A., Garg, S., **Gregoire, M.**, Lee, K., Lodder, M., Montgomery, H., Policharla, G., & Zhang, J. (2026). Qurrency: a quantum-secure, private, and auditable platform for digital assets. (Preprint).

- **Gregoire, M.**, Pierce, M., & Eskandarian, S. (2025). Onion Franking: Abuse Reports for Mix-Based Private Messaging. Network and Distributed Systems Security (NDSS 2025).

- **Gregoire, M.**, Thomas, R., & Eskandarian, S. (2024). CheckOut: User-Controlled Anonymization for Customer Loyalty Programs. Privacy Enhancing Technologies Symposium (PETS 2024).

- Ryan, K., **Gregoire, M.**, & Sturton, C. (2023). SEIF: Augmented Symbolic Execution for Information Flow Verification. Hardware and Architectural Support for Security and Privacy (HASP 2023), 1.

- Deutschbein, C., Meza, A., Restuccia, F., **Gregoire, M.**, Kastner, R., & Sturton, C. (2022). Toward hardware security property generation at scale. IEEE Security & Privacy, 20(3), 43-51.

TEACHING

UNC Chapel Hill *Fall 2023*
Graduate Teaching Assistant *Chapel Hill, NC*

Held office hours, graded assignments, and helped students to understand concepts in an advanced undergraduate cryptography class (COMP 537).

UNC Chapel Hill *August 2018 - May 2021*
Undergraduate Teaching Assistant *Chapel Hill, NC*

- **COMP 110: Intro to Programming**

  Covered concepts such as loops, recursion, functions and call stacks, and OOP. Taught in Type-Script. Held one-on-one office hours with hundreds of students and wrote questions for quizzes and exams.

- **COMP 283: Discrete Structures**

  Covered sets, counting, graph theory, proofs, and induction for a CS audience. Held group problem-solving sessions for students and graded assignments.

- **COMP 311: Computer Organization**

  Covered computer architecture bottom-up, from logic gates to a simple architecture to a full MIPS processor. Redesigned curriculum around a "simple as possible" computer architecture. Designed and wrote hands-on hardware labs.

Duke Talent Identification Program *Summer 2018, 2019*
Teaching Assistant *Appalachian State and Davidson College*

- **The Intersection of Math and Art** (1 session)

- **Cryptography** (3 sessions)

North Carolina School of Science and Mathematics *August 2016 - May 2017*
Mathematics Teaching Assistant *Durham, NC*

PROFESSIONAL SERVICE

Paper reviews *April-December 2025*

- **ACM Transactions on Privacy and Security Journal**

  Reviewed three iterations of a submitted paper.

INDUSTRY EXPERIENCE

Kaleido *Summer 2025*
Graduate Technical Intern *Raleigh, NC*

Identified and patched critical security errors in a central bank digital currency scheme proposed by researchers at UC Berkeley. Formally modeled and verified the security of three privacy domains in the Linux Foundation's Paladin project, and wrote a whitepaper describing Paladin.

Cisco *Summer 2022*
Graduate Technical Intern *Research Triangle Park, NC*

In an agile development team, worked to sunset a legacy data storage system and migrate to a new platform. Updated bash scripts and managed resources in kubernetes. Wrote and documented JavaScript for production.

PERSONAL PROJECTS

Quantum Discrete Logarithm Problem
Summer 2020

In a team for the North Carolina Qiskit Summer Jam, implemented a quantum algorithm by Burton S. Kaliski Jr. to solve the discrete logarithm problem in Qiskit. Project notebook and presentation on GitHub.

Fundamental Homomorphism Theorem
Summer 2020

Wrote my own explanation of basic group theory, starting from definitions and ending with the fundamental homomorphism theorem. Typeset all text and figures in LaTeX. Full project available on GitHub.

8-Bit Computer
Summer 2019

Built a fully programmable 8-bit computer using integrated circuits, wires, and breadboards, and designed a corresponding assembly language. Based on tutorials by Ben Eater. Full project description on GitHub.

Lorenz Equations Exploration
Spring 2019

Supported by mentor Collin Kofroth and the UNC Directed Reading Program. Studied nonlinear dynamics and chaos and applications to the Lorenz system. Programmed corresponding models of the system and ODE solvers in MATLAB. Final project presentation, figures, and code on GitHub.

HONORS AND RECOGNITIONS

2020	Completion of Qiskit Global Summer School in Quantum Computing
2019	Best Use of BlockStack API, PackHacks Hackathon
2017	NC State Champion, David Ricardo Economics Challenge
2017	Bowman-Brockman Scholar, NCSSM

TECHNICAL STRENGTHS

Languages	Python, Rust, JavaScript, Java, TypeScript, MATLAB, C, Assembly, Verilog
Tools	LaTeX, Bash, Git, Nix, Jupyter notebooks, SQL, Coq, Qiskit
Skills	Cryptography, security, systems programming, algorithm analysis, multithreading, mathematical modeling

OTHER INTERESTS

- Can solve a Rubik's cube in under 15 seconds (WCA Profile: 2017GREG02)
- Proficient at unicycling and juggling
- Play musical instruments, including viola and ukulele
- Play chess and Go casually