MATTHEW GREGOIRE

101 Shadowood Drive, Apt. J ◇ Chapel Hill, NC 27514
(828) · 707 · 1107 ◇ matthew@igregoire.com

EDUCATION

University of North Carolina at Chapel Hill *December 2023 - Present*
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)

RESEARCH

Private Supermarket Reward Points January 2022 - Present

Working under Saba Eskandarian to design a cryptographic protocol which allows shoppers to accumulate rewards points, while still maintaining privacy of purchase history.

Hardware Security and Information Flow August 2021 - Present

Working with researchers at UNC, UC San Diego, and Intel to use information flow tracking to mine for vulnerabilities in hardware designs. Our aim is to efficiently extract information flow properties from symbolic execution of hardware.

Symbolic Execution in Coq January 2021 - August 2022

Worked towards specifying formal proofs in Coq of three properties of symbolic execution laid out in the seminal paper (King 77).

PUBLICATIONS

- C. Deutschbein, A. Meza, F. Restuccia, M. Gregoire, R. Kastner and C. Sturton, "**Toward Hardware Security Property Generation at Scale**," in IEEE Security & Privacy, vol. 20, no. 3, pp. 43-51, May-June 2022.

TEACHING

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 TypeScript. 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 processors. 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)

  Helped students creatively explore topics such as knot theory, topology, and hyperbolic geometry.
- **Cryptography** (3 sessions)

  Covered topics from cryptanalysis of Caesar ciphers to RSA and elliptic curve cryptosystems, and discussed the societal impacts of different cryptographic protocols. Led lectures on undergraduate-level topics such as group theory and linear algebra. Worked with students aged 12-14.

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

- Held weekly evening study hours for a variety of math classes.

INDUSTRY EXPERIENCE

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.

Artificial Intelligence Explorations Summer 2020

Built AIs to play against humans (and each other) at Tic-Tac-Toe and Checkers, using minimax and alpha-beta algorithms, respectively. Also built corresponding GUIs in Java using javafx. Full project code 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

Computer Languages	Python, Java, TypeScript, MATLAB, C, Verilog, Assembly
Tools	LaTeX, Vim, Bash, Git, Jupyter notebooks, SQL, MongoDB, Coq, Qiskit
Skills	Cryptography, security, systems programming, 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