Matthew Gray

matthew.gray@cs.ox.ac.uk • (510) 610 8894 • graytmatter.com • linkedin.com/in/graytmatter

Education

Fall 2022 - *Current* — DPhil in Computer Science,
The University of Oxford, Oxford.
I am researching several questions in Quantum Meta Complexity. I am developing an extension of Impagliazzo's 5 worlds to capture quantum and post quantum complexity and crypto assumptions. I am investigating whether recent efforts towards world collapse such as Liu-Pass's, Illango-Ren-Santhanam's, and Hirahara's characterizations of OWFs can be translated to quantum settings. I am investigating connections to proof complexity and automatability. And I am investigating the characterizations of complexity theory for inherently quantum computation.
Advisor: Prof. Rahul Santhanam

June 2019 — B.A. in Computer Science with Honors and B.A. in Mathematics,
The University of California, Santa Cruz. Gpa: 3.66/4.0
Thesis: Local Order Agnosticism and Bit Flip Effecient Data Structures
Advisor: Prof. Seshadhri Comandur

Fall 2018 — Exchange Term at New College **Oxford University**, Oxford. Gpa: 4.0/4.0
Studied Complexity Theory with Rahul Santhanam and Edith Elkind,
as well as Cryptography with Giacomo Micheli.

Fall 2014 — Web Development Boot Camp at **General Assembly**, San Francisco
12 Week Immersive Program learning the fundamentals of Full Stack Web Development.
Coursework included JavaScript, Ruby, Ruby on Rails, HTML and CSS.

Work Experience

September 2021 - June 2022 — Adjunct Faculty of Computer Science at Renton Technical College: Renton WA
Taught Web Development. Brought in Guest Speakers from across Industry and Academia to expose Students to career paths and show them how to pursue those paths. And redesigned the AAS curriculum to focus on web as a more accessible entry point into the Industry.

Oct 2019-Nov 2020 — Software Engineer at Microsoft, Oslo Norway
Worked with a large team on React Native components used across Office 365 with a focus on iOS and Android development. My most notable project was implementing the accessibility API for React Native macOS.

Jan 2016-June 2019 — Research Assistant at Storage Systems Research Center UCSC
Worked with graduate students and professors on research into storage and security. Notable projects include fooling facial recognition, using Fourier Analysis to investigate MD5, and Designing Data Structures to Minimize Bit Flips on NVM

April 2017 - March 2019 — Teaching Assistant at University of California Santa Cruz
TA-ed several algorithms, data structures, and programming courses. Developed and ran two student lead courses on the Mathematics of Communication (CS42A). Topics I have taught include Number Theoretic Cryptography, Information Theoretic Compression, Error Correcting Codes, Stack Frames, and Memory Management

June 2016 - June 2017	Research and Development Intern at Sandia National Laboratories Livermore Worked on Cyber Security Research, with a focus on on write efficient databases, applied cryptography, secure multi-party computation, and passive data collection. Worked on a large C++ codebase.
Feb 2015 - July 2015	Web Developer at Last Minute Gear San Francisco Maintained and expanded a full stack web app and it's associated testing suite. Regular use of Ruby, Javascript, HTML, CSS, Heroku, git etc. Occasionally did odd jobs as needed since I was half of a two man start up.
Jan 2015 - April 2015	Teaching Assistant - Full Stack at General Assembly San Francisco Explained difficult Javascript and Ruby on Rails concepts. Drew out student's knowledge by listening and asking questions. Guided students through troubleshooting so they could use similar techniques in the future.

Writing and Publications

2021 Matthew Gray. Large Scale Secure Sortition Part 1: Generating Randomness Collectively with In-Person Gatherings `https://equalitybylot.com/?p=16298`, December 2021

2021 Matthew Gray. Large Scale Secure Sortition Part 2: "Voting" from home with Non-Malleable Time Lock Puzzles `https://equalitybylot.com/?p=16303`, December 2021

2021 Matthew Gray. Large Scale Secure Sortition Part 3: What exactly did Cleve show was impossible? And what possibilities are left? `https://equalitybylot.com/?p=16309`, December 2021

2019 Matthew Gray. "LOADS of Space", Local Order Agnosticism and Bit Flip Efficient Data Structure Codes. `https://arxiv.org/abs/1908.05415`, August 2019

2018 Daniel Bittman, Matthew Gray, Justin Raizes, Sinjoni Mukhopadhyay, Matt Bryson, Peter Alvaro, Darrell Long, and Ethan L Miller. Designing Data Structures to Minimize Bit Flips On NVM. In *2018 IEEE 7th Non-Volatile Memory Systems and Applications Symposium(NVMSA)*, pages 85–90. IEEE, 2018

Interests

- Quantum Computing, Quantum Cryptogrpahy, and Quantum Meta-Complexity.
- Complexity Theory, Meta-Complexity, MCSP and Kolmogorov Complexity.
- Cryptogrpahy, Secure Multiparty Computation, Multiparty Coin Flipping, and Sortition.
- Coding Theory, Non-Volatile Memory, Local Order Agnosticism, and Bit-Flip-Effecient Codes.
- Information Theory, Error Correction, Compression, Learning, and Inference.

Major Academic Projects

Spring 2022 - Present	*Quantum Non-Automatability from Crypto Assumptions* Collaborators: Noel Arteche (Lund University) and Gaia Carenini (ENS) Extended Frege is non-automatable assuming the security of RSA or related primitives. We are investigating whether these results translate to the quantum setting. I.e. if post quantum crypto is secure then is Extended Frege non-automatable even by quantum computers?

Winter 2022 - Present

Characterizations of Quantum One Way Cryptographic Primitives
Collaborators: Eli Goldin, and Peter Hall (NYU), Bruno Cavalar (University of Warwick), Angelos Pelecanos, and Xin Lyu (UC Berkeley).
We are investigating whether characterizations of the existence of one way functions by the hardness of meta complexity problems translate to the quantum and post quantum settings. We have made significant progress on translating [IRS '21], and are hopeful that recent work connecting OWFs and symmetry of information may be quantum-ized as well.

Summer 2022 - Present

A Bayesian Resolution to Hume's Problem of Induction
I have shown that any "rational actor" will (in the presence of Uniformity) eventually come to have arbitrarily high confidence in the Uniformity Principle. This provides a complete Bayesian response to Hume's problem, and is a major contribution to a problem that has been open for over 300 years. The paper is written and should be submitted soon.

Spring 2021 - Summer 2021

Multiparty Coin Flipping for Large Scale Sortition
Collaborators: Justin Raizes (CMU) & Paul Gölz (CMU)
Studied the Multiparty Coin Flipping literature hoping to find tools for developing secure procedures for large scale sortition. For instance in selecting US congressional representatives. In three articles published on the sortitionist blog Equality by Lot I propose a tiered system of gatherings, give a back up proposal using Time Lock Puzzles, and explain the structure of Cleve's proof and the tradeoffs we are faced with when trying to create secure procedures for generating randomness.

Winter 2018 - Spring 2019

Bit-Flip-Efficient Coding for Non-Volatile Memory
Collaborators: Justin Raizes (UCSC) & Daniel Bittman (UCSC)
Many implementations of Non-Volatile-RAM deteriorate or consume large amounts of energy with every bit flip. This project focused on developing data structures and data-structure codes that reduced bitflips. I think this area still has some very rich possibilities. Resulted in a paper and my thesis both listed under Publications.

Winter 2018 - Winter 2018

Fourier Analysis of Weak Hash Functions
Collaborators: Seshadhri Comandur (UCSC), Justin Raizes (UCSC), & Will Bolden (UCSC)
We used techniques from the Fourier Analysis of Boolean Functions to search for high influence Juntas in weak Hash functions such as SHA-1. We were fairly successful within the first of the four rounds and discovered other interesting patterns, but did not ultimately discover a mathematically satisfying explanation for why these hash functions were breakable.

Fall 2017 - Spring 2018

Fooling Facial Recognition
Collaborators: Anastasia McTaggart (UCSC), Miriam del Cerro Marazuela (UCSC), Steven Mazliach (UCSC), & Macie Cooper (UCSC)
We investigated techniques for fooling facial recognition software without the use of masks or other large facial coverings. We found some success with drag style makeup, with partial coverings, and with the use of reflective materials. Results, motivations, and methods are summarized at https://ssrc-facial-recognition.herokuapp.com.

Teaching

October 2022 - December 2022 — TA University of Oxford
Advanced Complexity Theory

I ran sections on advanced topics in complexity theory. These included natural proofs, branching programs, switching lemmas, oracle complexity, and pseudo-randomness. About a third of my students thought I should be considered for a departmental teaching award.

January 2019 - March 2019 — Instructor: CMPS 42A at UC Santa Cruz
Survey of Applied Computational Science

I led a group of 5 instructors (most of whom were alumni from my CMPS 198) in teaching a streamlined and matured version of the same curriculum to 30 students. This time the curriculum focused explicitly on the mathematics of communication. We taught them how to send information efficiently with range encoding, securely with RSA, and robustly with error correcting codes. To do this we taught them elementary number theory and information theory. Teaching this class was one of the highlights of my time at UCSC. The students also responded very positively to it. As far as I know this was **the first ever Student Directed Seminar in UCSC's CS department.**

September 2018 - December 2018 — CS Tutor: CMPS 101 at UC Santa Cruz
Algorithms and Abstract Data Types

Took on the role of TA. Ran labs, office hours, midterm and final review sessions. My main responsibility was to answer student's questions about algorithms questions. This would typically mean standing in front of 20 students for an hour getting algorithms questions tossed at me, having to solve them, explain them in an accessible way, and guide the students to the answers. This was fantastic teaching training, and even better technical interview training.

September 2017 - December 2017 — CS Tutor: CMPS 12B at UC Santa Cruz
Introduction to Data Structures

Gave students individualized help on Data Structures related Java code. The class assignments focused on a series of logical chess challenges such as N-Queens.

September 2017 - December 2017 — Instructor: CMPS 198 at UC Santa Cruz
Independent Study: Survey of Advance Computer Science

Justin Raizes and I created and ran a small survey course focusing on Shamir secret splitting, number theory and RSA, line ECCs, range encoding, and Gödel's incompleteness theorem. We had wanted to run a Student Directed Seminar but since no CS student has run one in at least a decade no professors were familiar with the paperwork. We instead ran this as an independent study practically out of a closet.

April 2017 - June 2017 — CS Tutor: CMPS 12B at UC Santa Cruz
Introduction to Data Structures

Took on the role of TA. Ran labs, office hours, graded, helped develop curriculum, and ran weekend help sessions for the massive homework assignments. The class was taught in C and included memory management, trees, stacks, queues, Huffman coding, and more. I helped run an advanced C session for interested students, ran the final review session, and gave my first "thank you all so much, and good luck on your final" applause line.

Jan 2015 - April 2015 — CS Tutor: CS61A at UC Berkeley
The Structure and Interpretation of Computer Programs

Helped teach UC Berkeley students. Introduced Python and abstraction techniques including higher order functions, recursion, and stack frames. Drew out student's knowledge by listening and asking questions. Once helped a student open their laptop and put some wood inside the case to stop the hard drive from falling out of place.

Jan 2015 - April 2015 — Teaching Assistant General Assembly San Francisco
Full Stack Web Development Bootcamp

Explained difficult Javascript and Ruby on Rails concepts. Drew out student's knowledge by listening and asking questions. Guided students through troubleshooting so they could use similar techniques in the future.

Schools and Workshops

Berkeley, Aug 2018	[Simons Institute] Lower Bounds in Computational Complexity
Oxford, July 2018	[Clay Institute] Workshop on Complexity Theory
Prague, June 2018	[ICALP] Summary School on Algorithms and Lower Bounds

Technical Strengths

Programing Languages	LaTeX, Python, Sage, C/C++, Objective C, Swift, Ruby, JavaScript, Typescript, HTML/CSS, Java
Frameworks	React, React Native, React Native Accessibility, Web Aria, Android Studios & XCode, Azure DevOPs, CI Tools.

References

R. Santhanam	Professor, Computer Science, Magdalen College, Oxford. Email: rahul.santhanam@cs.ox.ac.uk
C. Seshadhri	Professor, Computer Science and Engineering, University of California, Santa Cruz. Email: sesh@ucsc.edu
T. Larrabee	Professor, Computer Science and Engineering, University of California, Santa Cruz. Email: larrabee@soe.ucsc.edu
My Students	Student Letter