

# 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 and Quantum Cryptography. 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 between quantum cryptography and proof complexity. 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: "LOADS of Space", Local Order Agnosticism and Bit Flip Efficient 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

---

- |                            |   |
|----------------------------|---|
| SEPT 2021 -<br>JUNE 2022   | Adjunct Faculty of Computer Science at RENTON TECHNICAL COLLEGE: Renton WA<br>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 -<br>NOV 2020     | Software Engineer at MICROSOFT, Oslo Norway<br>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 -<br>JUNE 2019    | Research Assistant at STORAGE SYSTEMS RESEARCH CENTER UCSC<br>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 -<br>MARCH 2019 | Teaching Assistant at UNIVERSITY OF CALIFORNIA Santa Cruz<br>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 -	Research and Development Intern at SANDIA NATIONAL LABORATORIES Livermore
JUNE 2017	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 -	Web Developer at LAST MINUTE GEAR San Francisco
JULY 2015	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 -	Teaching Assistant - Full Stack at GENERAL ASSEMBLY San Francisco
APRIL 2015	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

---

- 2023 Bruno Cavalari, Eli Goldin, Matthew Gray, Peter Hall, Yanyi Liu, and Angelos Pelecanos. On the Computational Hardness of Quantum One-Wayness <https://arxiv.org/abs/2312.08363>, December 2023
- 2023 Noel Arteche, Gaia Carenini, Matthew Gray. On the Quantum Automatability of Propositional Proof Systems, September 2023
- 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 Cryptography, and Quantum Complexity Theory.
- Complexity Theory, Meta-Complexity, MCSP, and Kolmogorov Complexity.
- Cryptography, Secure Multiparty Computation, Multiparty Coin Flipping, and Sortition.
- Coding Theory, Non-Volatile Memory, Local Order Agnosticism, and Bit-Flip-Efficient Codes.
- Information Theory, Error Correction, Compression, Learning, and Inference.
- Fourier Analysis of Boolean Functions and Hash Function Analysis.

## TEACHING

---

- OCTOBER 2022 - Teaching Assistant: UNIVERSITY OF OXFORD  
DECEMBER 2022 Advanced Complexity Theory  
I graded and led small group sessions going over the weeks' assignment. The class covered many advanced topics in complexity theory including lower bounds against weak circuit classes, the natural proofs barrier, and cryptographic generators. I was not as familiar as I would have liked with the material and so attended the class as preparation. Despite this, my students gave excellent feedback to my sessions, and were highly appreciative.
- JANUARY 2022 - Instructor: CSI 242 at RENTON TECHNICAL COLLEGE  
JUNE 2022 Client Side Scripting  
I developed and taught a curriculum covering JavaScript fundamentals with a focus on scoping rules and application development. Students deployed four live projects using github hosting including a personal website, an original game, a utility application, and a final unique project. Several students even worked to build an original environment for creating codecademy style lessons.
- SEPTEMBER 2020 - Teaching Assistant: LE WAGON Oslo  
OCTOBER 2020 Web Development Boot Camp  
I assisted students during their final weeks of a web development immersive. I helped them understand API documentation, database diagrams and migrations, and presentation techniques.
- JANUARY 2019 - Instructor: CMPS 42A at UC SANTA CRUZ  
MARCH 2019 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 - CS Tutor: CMPS 101 at UC SANTA CRUZ  
DECEMBER 2018 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 - CS Tutor: CMPS 12B at UC SANTA CRUZ  
DECEMBER 2017 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 - Instructor: CMPS 198 at UC SANTA CRUZ  
DECEMBER 2017 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 - CS Tutor: CMPS 12B at UC SANTA CRUZ  
 JUNE 2017 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 - CS Tutor: CS61A at UC BERKELEY  
 APRIL 2015 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 - Teaching Assistant GENERAL ASSEMBLY San Francisco  
 APRIL 2015 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, SPRING 2022 [Simons Institute] Meta-Complexity
- Berkeley, AUG 2018 [Simons Institute] Lower Bounds in Computational Complexity
- Oxford, JULY 2018 [Clay Institute] Workshop on Complexity Theory
- Prague, JUNE 2018 [ICALP] Summer School on Algorithms and Lower Bounds

## REFERENCES

---

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