Matthew Gray

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

Education

Fall 2022 - June 2026
DPhil in Computer Science,
The University of Oxford, Oxford.
Primary research is characterizing the existence of quantum cryptography by the hardness of meta-complexity problems. Also working on a personalist Bayesian resolution to Hume's problem of induction and breaking renaissance era ciphers.
Advisor: Prof. Rahul Santhanam

June 2019
B.A. in Computer Science with Honors and B.A. in Mathematics,
The University of California, Santa Cruz.
Thesis: "LOADS of Space", Local Order Agnosticism and Bit Flip Efficient Data Structures
Advisor: Prof. Seshadhri Comandur

Spring 2018
Exchange Term at New College **Oxford University**, Oxford.
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 on the fundamentals of Full Stack Web Development.
Coursework included JavaScript, Ruby, Ruby on Rails, HTML and CSS.

Work Experience

Sept 2024 - June 2025
Stipendiary Lecturer at Balliol College, Oxford
Taught Computational Models as well as Algorithms and Data Structures to small groups of second year undergraduates at Balliol College.

Sept 2022 - Dec 2022
Teaching Assistant at University of Oxford
Helped teach Advanced Complexity Theory and Lower Bounds course under Rahul Santhanam.

Sept 2021 - June 2022
Adjunct Faculty of Computer Science at Renton Technical College
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 Cybersecurity 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.

Publications and other Writing

In submission — Bruno Cavalar, Eli Goldin, Matthew Gray, Taiga Hiroka, Tomoyuki Morimae. On Cryptography and Verification of Sampling, with Applications to Quantum Advantage. `https://arxiv.org/abs/2510.05028`

In submission — Bruno Cavalar, Boyang Chen, Andrea Coladangelo, Matthew Gray, Zihan Hu, Zhengfeng Ji, Xingjian Li†. A Meta-Complexity Characterization of Minimal Quantum Cryptography. `https://arxiv.org/abs/2510.07859`

Eurocrypt 2025 — Bruno Cavalar, Eli Goldin, Matthew Gray, Peter Hall. A Meta-Complexity Characterization of Quantum Cryptography `https://arxiv.org/abs/2410.04984`

Quantum 2025 — Bruno Cavalar, Eli Goldin, Matthew Gray, Peter Hall, Yanyi Liu, and Angelos Pelecanos. On the Computational Hardness of Quantum One-Wayness `https://quantum-journal.org/papers/q-2025-03-27-1679/`

Crypto 2024 — Kai-Min Chung, Eli Goldin, Matthew Gray. On Central Primitives for Quantum Cryptography with Classical Communication `https://arxiv.org/abs/2402.17715`

CCC 2024 — Noel Arteche, Gaia Carenini, Matthew Gray. Quantum Automating TC^0-Complexity Frege Is LWE-Hard `https://arxiv.org/abs/2402.10351`

2021 — Matthew Gray. Large Scale Secure Sortition Part 1, Part 2, and Part 3. Equality by Lot. December 2021

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

NVMSA 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 Meta-Complexity.
- Complexity Theory, Meta-Complexity, and Quantum Kolmogorov complexities.
- Cryptography, Secure Multiparty Computation, Multiparty Coin Flipping, and Sortition.

- Information Theory, Error Correction, Compression, Learning, and Inference.
- Analytic Philosophy, Subjective Bayesianism, and Hume's Problem of Induction.
- Historical Cryptography, Renaissance Era Ciphers, and Cryptanalysis.
- Coding Theory, Non-Volatile Memory, Local Order Agnosticism, and Bit-Flip-Efficient Codes.
- Write Efficient Data Structures, Property Testing, and Sublinear Algorithms.

Teaching

Oct 2024 - June 2025
Stipendiary Lecturer: University of Oxford
Models of Computation & Algorithms and Data Structures

I marked and gave tutorials for Balliol's nine computer science second year undergraduate students. We covered topics including Finite Automata, Regular Expressions, Pumping Lemmas, Context Free Languages, Turing Machines, Rice's Theorem, NP Completeness, Amortized Analysis, Red-Black Trees, Max Flow/Min Cut, Linear Programming, and Approximation Algorithms.

Oct 2022 - Dec 2022
Teaching Assistant: University of Oxford
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.

Jan 2022 - June 2022
Instructor: CSI 242 at Renton Technical College
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.

Sept 2020 - Oct 2020
Teaching Assistant: Le Wagon Oslo
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.

Jan 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.**

Sept 2018 - Dec 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.

Sept 2017 - Dec 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.

Sept 2017 - Dec 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

Oxford, Sept 2025	[Clay Mathematical Institute] P vs NP and Complexity Lower Bounds
Oxford, Aug 2025	[University of Oxford] Proof Complexity
Berkeley, Summer 2025	[Simons Institute] Cryptography 10 Years Later: Obfuscation, Proof Systems, and Secure Computation
Berkeley, Summer 2025	[Simons Institute] Quantum Summer Cluster Workshop
Berkeley, Spring 2023	[Simons Institute] Quantum Algorithms, Complexity, and Fault Tolerance
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

Service

I have sub-reviewed for the following conferences:
2025: CRYPTO, FOCS, STACS, STOC, TQC. 2024: FOCS.

References

R. Santhanam	Professor, Computer Science, Magdalen College, University of Oxford. Email: rahul.santhanam@cs.ox.ac.uk
Bruno Cavalar	Post-doctoral Researcher, Computer Science, University of Oxford. Email: bruno.cavalar@cs.ox.ac.uk
Andrea Coladangelo	Assistant Professor & Computer Science, University of Washington. Email: coladan@cs.washington.edu
My Students	Student Letter