Matthew Gray

matt.t.gray@gmail.com • +1 (510) 610 8894 • www.linkedin.com/in/graytmatter

Education

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 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 - *Current* | Adjunct Faculty at Renton Technical College: Renton WA

Teaching Web Development. Bringing in Guest Speakers from across Industry and Academia to expose Students to career paths and show them how to pursue those paths. And helping redesign 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

Working 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.

Publications

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 Secure Multiparty Quantum Computation.
- Cryptogrpahy, Secure Multiparty Computation, Multiparty Coin Flipping, and Sortition.
- Coding Theory, Non-Volatile Memory, Local Order Agnosticism, and Bit-Flip-Effecient Codes.
- Complexity Theory, Circuit Complexity, and The Minimum Size Circuit Problem.
- Information Theory, Error Correction, Compression, Learning, and Inference.
- Fourier Analysis of Boolean Fucntions and Hash Fucntion Analysis.
- Write Effecient Data Structures, Monotonicity Testing, and Sublinear Algorithms.

Major Academic Projects

Fall 2021 - Present

Secure Multiparty Quantum Computation for Single Output Functions
Collaborators: Justin Raizes (CMU) & Chen-Da Liu (CMU)
Ongoing research into whether improvements to protocol parameters can be achieved when doing SMPQC for functions with a solitary output. Because of the No Cloning Theorem, quantum results paralel to the classical results of Halevi et. al 2019 present a natural problem and seem likely to be achievable.

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. Based on a deep understanding of the requirements for Cleve’s impossibility result I developed several approaches which will be published in an upcoming Equality by Lot article.

Fall 2018 - Spring 2019

Proving Depth 3 Formula-MCSP NP Complete
Collaborators: Rahul Santhanam (Oxford)
I investigated proof techniques for proving the depth 3-formula Minimum Circuit Size Problem NP Complete. While the choice of open problem turned out to be good (Rahul Ilango solved it in 2020) the tools I developed never got to the level of sophistication required to complete the proof.

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.

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] Summer School on Algorithms and Lower Bounds

Technical Strengths

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

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