

Matthew Weidner

 mattweidner.com

Education

- 2019-current **PhD in Computer Science**, *Carnegie Mellon University*, Pittsburgh, PA, Advisor: Heather Miller.
- 2018-2019 **MPhil in Advanced Computer Science**, *University of Cambridge*, Cambridge, UK, Pass with Distinction.
- 2014-2018 **B.S. in Mathematics with Computer Science Minor**, *California Institute of Technology*, Pasadena, CA.

Research

- [1] M. Weidner, M. Kleppmann, D. Hugenroth, and A. R. Beresford. Key Agreement for Decentralized Secure Group Messaging with Strong Security Guarantees. *Cryptology ePrint Archive*, Report 2020/1281, October 2020.
- [2] M. Weidner, H. Miller, and C. Meiklejohn. Composing and decomposing op-based CRDTs with semidirect products. *Proceedings of ACM Programming Languages 4 (ICFP)*, Article 94, August 2020.
- [3] M. Weidner. Group messaging for secure asynchronous collaboration. MPhil dissertation, University of Cambridge, 2019. Advisors: A. R. Beresford and M. Kleppmann.
- [4] A. K. Narayanan and M. Weidner. On decoding Cohen-Haeupler-Schulman tree codes. *Symposium on Discrete Algorithms (SODA) 2020*.
- [5] A. K. Narayanan and M. Weidner. Subquadratic time encodable codes beating the Gilbert-Varshamov bound. *IEEE Transactions on Information Theory*, 65(10):6010–6021, July 2019.
- [6] A. Chiesa, L. Chua, and M. Weidner. On cycles of pairing-friendly elliptic curves. *SIAM Journal on Applied Algebra and Geometry*, 3(2):175–192, 2019.
- [7] M. Weidner. Pseudocharacters of Homomorphisms into Classical Groups. *Transformation Groups*, 2020.
- [8] M. Weidner. On Conjectural Rank Parities of Quartic and Sextic Twists of Elliptic Curves. *International Journal of Number Theory*, 15(9):1895–1918, June 2019.
- [9] M. Hadian and M. Weidner. On Selmer rank parity of twists. *Journal of the Australian Mathematical Society*, 102(3):316–330, June 2017.

Awards

- 2020–2023 **NDSEG Fellowship**, *US DoD*, Computer and Computational Sciences.
 “[A] competitive fellowship that is awarded to U.S. citizens, U.S. nationals, and U.S. dual citizens who intend to pursue a Doctoral degree aligned to the DoD services Broad Agency Announcements (BAAs) in research and development at a U.S. institution of their choice.”
 Sponsor: Office of Naval Research.
- 2018–2019 **Churchill Scholarship**, *Winston Churchill Foundation of the USA*, MPhil in Advanced CS.
 “[P]rovides funding to American students for a year of Master’s study in science, mathematics, and engineering at the University of Cambridge, based at Churchill College.”
- 2018 **George W. Housner Prize for Academic Excellence and Original Research**, *Caltech Undergraduate Academic Standards and Honors Committee*.
 “[G]iven annually to a senior [or seniors] in the upper 20 percent of his or her class who has demonstrated excellence in scholarship and in the preparation of an outstanding piece of original scientific research.”
- 2017 **Eric Temple Bell Undergraduate Mathematics Research Prize**, *Caltech Math Department*.
 “[A]warded to one or more juniors or seniors for outstanding original research in mathematics.”
- 2017 **Honorable Mention**, *2016 William Lowell Putnam Mathematical Competition*.
- 2016 **H. J. Ryser Scholarship**, *Caltech Math Department*.
 “[A]warded to undergraduate students for academic excellence.”
- 2016 **Honorable Mention**, *2015 William Lowell Putnam Mathematical Competition*.

Teaching

- 9/2020– **15-440 (Distributed Systems) Head Teaching Assistant**, *CMU*, Pittsburgh, PA.
 12/2020 Managed 21-TA team for large upper-level distributed systems course.
- 6/2018– **Computer Science Teaching Assistant/Counselor**, *Pennsylvania Governor’s School for the Sciences*, Pittsburgh, PA.
 8/2018 Assisted with lecture, lab, and team project courses in computer science and served as a live-in counselor for high school science summer program.
- 9/2017– **Ma5a (Introduction to Abstract Algebra) Teaching Assistant**, *Caltech*, Pasadena, CA.
 12/2017 Gave office hours and graded problem sets and exams for undergraduate course on group theory.
- 1/2016– **CS21 (Decidability and Tractability) Teaching Assistant**, *Caltech*, Pasadena, CA.
 3/2016; Gave office hours and graded problem sets and exams for undergraduate course on theory of computation and computational complexity.
 1/2017–
 3/2017

Talks Given

- 4/2018 **Subquadratic Time Encodable Codes Beating the Gilbert-Varshamov Bound**, *Caltech CS Theory Group Meeting*.
- 11/2017 **Algebraic Geometry Error-Correcting Codes**, *Caltech Undergraduate Math Club*.

- 4/2017 **2-Selmer Rank Parities and Quadratic Twists of Elliptic Curves**, *Caltech Langlands Program Learning Seminar*.
- 11/2015 **Mordell-Weil Groups of Elliptic Curves**, *Caltech Undergraduate Math Club*.
- 10/2015 **2-Selmer Ranks of Quadratic Twists of (Hyper)elliptic Curves**, *Caltech Number Theory Seminar*.

Selected Coursework

- CMU 15-719 **Advanced Cloud Computing.**
Principles and practice of cloud computing, with hands-on homework using Amazon Web Services.
- Cambridge **Network Architectures.**
ACS R02 Paper reading on current and alternative network architectures for: core IP layer, mobile networks, network topologies, transport services, data centers, IoT, and IPv6.
- Cambridge **Advanced Topics in Computer Systems.**
ACS R01 Paper reading on current and historical topics in computer systems.
- Cambridge **Topics in Concurrency.**
ACS L301 Models and logics for concurrent processes, model checking, cryptographic protocols, and strategies as concurrent processes.
- Caltech **Complexity Theory.**
CS151 Time and space complexity, nondeterminism, circuit complexity, randomness & derandomization, alternation, and interaction.
- Caltech **Analysis and Design of Algorithms.**
CMS/CS139 Approximation algorithms, randomized algorithms, online algorithms, streaming algorithms, and research topics.
- Caltech **Quantum Computation.**
Ph/CS219ab Two terms covering quantum entanglement, quantum circuits, and quantum algorithms; quantum error-correction and fault-tolerant quantum computing.

Activities

- 2019–current CMU Tartan Wind Ensemble.
- 2018–2019 Cambridge University Recorder Ensemble.
- 2014–2018 Caltech-Occidental Concert Band. Band Manager, 2017–2018.
- 2015–2018 Caltech Deans' Office Peer Tutor for abstract algebra and algorithms courses.
- 2016–2018 Student Waiter for dinners in Dabney House (my undergraduate residence). Co-Head Waiter, 2017–2018.
- Winter 2017 Pit Band, Caltech Theater Group production of "Company".