Curriculum Vitae
Justin Thaler

Personal Information

Full Name: Justin Ross Thaler
Email: justin.thaler@georgetown.edu
URL: http://people.cs.georgetown.edu/jthaler/

Research Interests

Verifiable Computing, Quantum Computing, Algorithms for Massive Data, Learning Theory

Education

Ph.D. November 2013 - School of Engineering and Applied Sciences,
Harvard University, Cambridge MA
Adviser: Michael Mitzenmacher

B.S. 2005-2009 - Yale University, New Haven, CT
Summa Cum Laude

Positions

- **Associate Professor**. Department of Computer Science, Georgetown University, Washington D.C. August 2021-present.
- **Assistant Professor**. Department of Computer Science, Georgetown University, Washington D.C. August 2016-July 2021.
- **Research Scientist**. Scalable Machine Learning Group. Yahoo Labs, New York, NY. June 2014-July 2016.
- **Research Fellow**. Simons Institute for the Theory of Computing, Berkeley, CA. August 2013-May 2014.
- **Ph.D. Student**. Harvard University, Cambridge, MA. September 2009-July 2013.
- **Adjunct**. Center for Computing Sciences, Institute for Defense Analyses, Bowie, MD (2009-2014), Research Intern during Summer 2009.

Academic Honors

- Best Paper Award, *Symposium on Principles of Database Systems (PODS)* (2021).
- NSF CAREER Award. Project Title: The Polynomial Method in Complexity and Cryptography (2019).
- Best Newcomer Paper Award, *International Conference on Database Theory (ICDT)* (2016).
- Best Paper Award, *Symposium on Parallel Algorithms and Architectures (SPAA)* (2014).
- Best Paper Award, *International Colloquium on Automata, Languages, and Programming (ICALP)*, Track A (2013).
- NSF Graduate Research Fellowship Recipient (2010).
- National Defense Science and Engineering Graduate Fellow (2009-2012).
- Phi Beta Kappa (2009).
- Yale University Computer Science Prize (2009). Awarded by Yale University's Department of Computer Science to the graduating senior who ranks highest in scholarship.
- Anthony D. Stanley Memorial Prize (2009). Awarded by Yale University's Department of Mathematics for excellence in pure and applied mathematics.

Publications

(1) **Proofs, Arguments, and Zero-Knowledge**. Justin Thaler. Foundations and Trends in Privacy and Security, 2022.

(2) **Approximate Degree in Quantum and Classical Computing**. Mark Bun and Justin Thaler. Foundations and Trends in Theoretical Computer Science, 2022. This is a vastly expanded version of publication (9) below.

(3) **Order-Invariant Cardinality Estimators Are Differentially Private**. Charlie Dickens, Justin Thaler, Daniel Ting, In Neural Information Processing Systems *NeurIPS*, 2022.

(4) **Quantum Proofs of Proximity.** Marcel Dall'Agnol Tom Gur, Subhayan Roy Moulik, and Justin Thaler, In *Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC)*, 2021. Journal version in *Quantum*, 2022.

(5) **Relative Error Streaming Quantiles.** Graham Cormode, Zohar Karnin, Edo Liberty, Justin Thaler, Pavel Veselý, In Symposium on *Principles of Database Systems (PODS)*, 2021. **Best Paper Award.** Invited to *J. ACM*.

(6) **Vanishing-Error Approximate Degree and QMA Complexity.** Alexander A. Sherstov and Justin Thaler. Accepted to *Chicago Journal of Theoretical Computer Science*, 2021.

(7) **Streaming Verification for Graph Problems: Optimal Tradeoffs and Nonlinear Sketches.** Amit Chakrabarti, Prantar Ghosh, Justin Thaler, Accepted to *International Conference on Randomization and Computation (RANDOM)*, 2020.

(8) **Improved Approximate Degree Bounds For k-Distinctness.** Nikhil Mande, Justin Thaler, and Shuchen Zhu. In *Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC)*, 2020.

(9) **Guest Column: Approximate Degree in Quantum and Classical Computing.** Mark Bun and Justin Thaler. Invited survey article for *ACM SIGACT News* Complexity Theory Column, December 2020 issue.

(10) **Quantum Lower Bounds for Approximate Counting via Laurent Polynomials.** Scott Aaronson, Robin Kothari, William Kretschmer, and Justin Thaler. In *Computational Complexity Conference (CCC)*, 2020. Preliminary version in *Conference on Quantum Information Processing (QIP)*, 2020.

(11) **Approximate Degree, Secret Sharing, and Concentration Phenomena.** Andrej Bogdanov, Nikhil Mande, Justin Thaler, and Christopher Williamson. In *International Conference on Randomization and Computation (RANDOM)*, 2019.

(12) **Ad Hoc Multi-Input Functional Encryption.** Shweta Agrawal, Michael Clear, Ophir Frieder, Sanjam Garg, Adam O'Neill, and Justin Thaler. In *Innovations in Theoretical Computer Science (ITCS)*, 2020.

(13) **The Large-Error Approximate Degree of $\mathbf{AC}^0$**. Mark Bun and Justin Thaler. In *International Conference on Randomization and Computation (RANDOM)*, 2019. Journal version in *Theory of Computing*, 2021 **(special issue for best papers of RANDOM 2019)**.

(14) **Sign-Rank Can Increase Under Intersection.** Mark Bun, Nikhil Mande, and Justin Thaler. In *International Colloquium on Automata, Languages and Programming (ICALP)*, 2019. Journal version in ACM *Transactions on Computation Theory*, 2021.

(15) **Quantum Algorithms and Approximating Polynomials for Composed Functions with Shared Inputs.** Mark Bun, Robin Kothari, and Justin Thaler. In *Symposium on Discrete Algorithms (SODA)*, 2019. Journal version in *Quantum*, 2021.

(16) **Approximate Degree and the Complexity of Depth Three Circuits**. Mark Bun and Justin Thaler. In *International Conference on Randomization and Computation (RANDOM)*, 2018.

(17) **Doubly-efficient zkSNARKs without trusted setup**. Riad S. Wahby, Ioanna Tzialla, abhi shelat, Justin Thaler and Michael Walfish. In *IEEE Symposium on Security and Privacy (S&P)*, 2018.

(18) **The Polynomial Method Strikes Back: Tight Quantum Query Bounds via Dual Polynomials**. Mark Bun, Robin Kothari, and Justin Thaler. In *ACM Symposium on the Theory of Computing (STOC)*, 2018. Also presented at the 2018 *Conference on Quantum Information Processing (QIP)* as a **plenary talk**. Journal version in *Theory of Computing*, 2020 **(invited paper)**.

(19) **A Nearly Optimal Lower Bound on the Approximate Degree of AC^0**. Mark Bun and Justin Thaler. In *IEEE Symposium on Foundations of Computer Science* (*FOCS*), 2017. Journal version in *SICOMP*, 2019 **(special issue for the best papers of FOCS 2017)**.

(20) **On the Power of Statistical Zero Knowledge**. Adam Bouland, Lijie Chen, Dhiraj Holden, Justin Thaler, Prashant Nalini Vasudevan. In *IEEE Symposium on Foundations of Computer Science* (*FOCS*), 2017. Journal version in *SICOMP*, 2019 **(special issue for the best papers of FOCS 2017)**.

(21) **Full Accounting for Verifiable Outsourcing**. Riad S. Wahby, Ye Ji, Andrew J. Blumberg, abhi shelat, Justin Thaler, Michael Walfish, and Thomas Wies. In *Conference on Computer and Communications Security (CCS)*, 2017.

(22) **A High-Performance Algorithm for Identifying Frequent Items in Data Streams**. Daniel Anderson, Pryce, Bevin, Kevin Lang, Edo Liberty, Lee Rhodes, and Justin Thaler. In *Internet Measurement Conference (IMC)*, 2017.

(23) **Reliably Learning the ReLU in Polynomial Time**. Surbhi Goel, Varun Kanade, Adam Klivans, and Justin Thaler. In *Conference on Learning Theory (COLT)*, 2017.

(24) **Determining Tournament Payout Structures for Daily Fantasy Sports**. Christopher Musco, Maxim Sviridenko, and Justin Thaler. In *Meeting on Algorithm, Engineering & Experiments (ALENEX)*, 2017. Invited to ACM Journal of Experimental Algorithmics..

(25) **Improved Bounds on the Sign-Rank of AC^0**. Mark Bun and Justin Thaler. In *International Colloquium on Automata, Languages and Programming (ICALP)*, 2016.

(26) **Lower Bounds for the Approximate Degree of Block-Composed Functions**. Justin Thaler. In *International Colloquium on Automata, Languages and Programming (ICALP)*, 2016.

(27) **Semi-Streaming Algorithms for Annotated Graph Streams**. Justin Thaler. In *International Colloquium on Automata, Languages and Programming (ICALP)*, 2016.

(28) **Space Lower Bounds for Itemset Frequency Sketches**. Edo Liberty, Michael Mitzenmacher, Justin Thaler, and Jonathan Ullman. In *Principles of Database Systems (PODS)*, 2016.

(29) **A Framework for Estimating Stream Expression Cardinalities**. Anirban Dasgupta, Kevin Lang, Lee Rhodes, and Justin Thaler. In *International Conference on Database Theory (ICDT)*, 2016. **Best Newcomer Paper Award. Invited to ACM Transactions on Database Systems (special issue for the best papers of ICDT 2016).**

(30) **Catching Lies (and Mistakes) in Offloaded Computation**. Michael Mitzenmacher and Justin Thaler. Communications of the ACM (CACM), February 2016. Invited Technical Perspective.

(31) **Streaming Verification in Data Analysis**. Samira Daruki, Justin Thaler, and Suresh Venkatasubramanian. In *International Symposium on Algorithms and Computation (ISAAC)*, 2015.

(32) **Hardness Amplification and the Approximate Degree of Constant-Depth Circuits**. Mark Bun and Justin Thaler. In *International Colloquium on Automata, Languages and Programming (ICALP)*, 2015.

(33) **Variable Selection is Hard**. Dean Foster, Howard Karloff, and Justin Thaler. In *Conference on Learning Theory (COLT)*, 2015.

(34) **Verifiable Stream Computation and Arthur-Merlin Communication**. Amit Chakrabarti, Graham Cormode, Andrew McGregor, Justin Thaler, and Suresh Venkatasubramanian. In *Computational Complexity Conference (CCC)*, 2015. Journal version in *SIAM Journal on Computing*, 2019.

(35) **Parallel Peeling Algorithms**. Jiayang Jiang, Michael Mitzenmacher, and Justin Thaler. In *Symposium on Parallelism in Algorithms and Architectures (SPAA)*, 2014. **Best Paper Award.** Journal version in *ACM Transactions on Parallel Computing*, 2015 (special issue for the best papers of SPAA 2014).

(36) **Distribution-Independent Reliable Learning**. Varun Kanade and Justin Thaler. In *Conference on Learning Theory (COLT)*, 2014.

(37) **Faster Private Release of Marginals on Small Databases**. Karthekeyan Chandrasekaran, Justin Thaler, Jonathan Ullman, Andrew Wan. In *Innovations in Theoretical Computer Science (ITCS)*, 2014.

(38) **Annotations for Sparse Data Streams**. Amit Chakrabarti, Graham Cormode, Navin Goyal, and Justin Thaler. In *Symposium on Discrete Algorithms (SODA)*, 2014.

(39) **Time-Optimal Interactive Proofs for Circuit Evaluation**. Justin Thaler. In *International Cryptology Conference (CRYPTO)*, 2013.

(40) **Dual Lower Bounds for Approximate Degree and Markov-Bernstein Inequalities**. Mark Bun and Justin Thaler. In *International Colloquium on Automata, Languages and Programming (ICALP)*, 2013. **Best Paper Award for Track A.** Journal version in *Information and Computation*, 2015 (special issue for the best papers of ICALP 2013).

(41) **Cache-Oblivious Dictionaries and Multimaps with Negligible Failure Probability**. Michael Goodrich, Dan Hirschberg, Michael Mitzenmacher, and Justin Thaler. In *Mediterranean Conference on Algorithms (MedAlg)*, 2012.

(42) **Verifying Computations with Streaming Interactive Proofs**. Graham Cormode, Justin Thaler, and Ke Yi. In *VLDB*, 2011.

(43) **Faster Algorithms for Privately Releasing Marginals**. Justin Thaler, Jonathan Ullman, and Salil Vadhan. In *International Colloquium on Automata, Languages and Programming (ICALP)*, 2012.

(44) **Attribute-Efficient Learning and Weight-Degree Tradeoffs for Polynomial Threshold Functions**. Rocco Servedio, Li-Yang Tan, and Justin Thaler. In *Conference on Learning Theory (COLT)*, 2012.

(45) **Verifiable Computation with Massively Parallel Interactive Proofs**. Justin Thaler, Mike Roberts, Michael Mitzenmacher, and Hanspeter Pfister. In *USENIX Workshop on Hot Topics in Cloud Computing (HotCloud)*, 2012.

(46) **Continuous Time Channels with Interference**. Ioana Ivan, Michael Mitzenmacher, Justin Thaler, and Henry Yuen. In *International Symposium on Information Theory (ISIT)*, 2012.

(47) **Hierarchical Heavy Hitters with the Space Saving Algorithm**. Michael Mitzenmacher, Thomas Steinke, and Justin Thaler. In *Meeting on Algorithm, Engineering & Experiments (ALENEX)*, 2012.

(48) **Practical Verified Computation with Streaming Interactive Proofs**. Graham Cormode, Michael Mitzenmacher, and Justin Thaler. In *Innovations in Theoretical Computer Science (ITCS)*, 2012.

(49) **Annotations in Data Streams**. Amit Chakrabarti, Graham Cormode, Andrew McGregor, and Justin Thaler. *ACM Transactions on Algorithms*, 2014.

(50) **External-Memory Multimaps**. Elaine Angelino, Michael T. Goodrich, Michael Mitzenmacher, and Justin Thaler. In *International Symposium on Algorithms and Computation (ISAAC)*, 2011. Journal version in *Algorithmica*, 2013 (special issue devoted to ISAAC 2011).

(51) **Streaming Graph Computations with a Helpful Advisor**. Graham Cormode, Michael Mitzenmacher, and Justin Thaler. In *European Symposium on Algorithms (ESA)*, 2010. Journal version in *Algorithmica*, 2013.

(52) **Graph Covers and Quadratic Minimization**. Nicholas Ruozzi, Justin Thaler, and Sekhar Tatikonda. In *Allerton Conference on Communication, Control, and Computing*, 2009.

Workshop Papers and Reference Articles

(I1) **Community Proposal: A Benchmarking Framework for (Zero-Knowledge) Proof Systems**. Daniel Benarroch, Aurélien Nicolas, Justin Thaler, and Eran Tromer. 3rd ZKProof Standardization Workshop, April 2020. Awarded best paper at the workshop.

(I2) **Data Stream Verification**. Justin Thaler. *Encyclopedia of Algorithms*. Springer Berlin Heidelberg, 2015. (Invited Survey Article).

(I3) **Peeling Arguments and Double Hashing**. Michael Mitzenmacher and Justin Thaler. Appears as an invited paper in *Allerton Conference on Communication, Control, and Computing*, 2012.

(I4) **On the Zero-Error Capacity Threshold for Deletion Channels**. Ian Kash, Michael Mitzenmacher, Justin Thaler, and Jonathan Ullman. In *Information Theory and Applications Workshop (ITA)*, 2011.

Manuscripts

(M1) **Linear-time zero-knowledge SNARKs for R1CS.** Jonathan Lee, Srinath Setty, Justin Thaler, and Riad Wahby, 2021.

(M2) **A Note on the GKR Protocol.** Justin Thaler. 2015.

(M3) **Verifiable Computation Using Multiple Provers.** Andrew J. Blumberg, Justin Thaler, Victor Vu, and Michael Walfish. 2014.

Selected Invited Talks and Lecture Series

- **Linear-time SNARKs for R1CS and Friends**.
  - 5th ZKProof Workshop (plenary talk), November 2022.
- **SNARK Design**.
  - Three-part talk series delivered to a16z crypto research, Summer 2022.
- **Quantum Lower Bounds via Laurent Polynomials**.
  - Dartmouth Theory of Computing Seminar, Fall 2020.
  - Harvard Theory of Computing Seminar, Fall 2019.
- **Interactive Proofs**.
  - Two-hour survey talk during Boot Camp for the Simons Institute Proofs, Consensus, and Decentralizing Society Program, Fall 2019.
  - Additional two-hour followup talk given internally at Simons Institute Proofs, Consensus, and Decentralizing Society Program, Fall 2019.
  - Delivered related tutorial at NIST Crypto reading group, Fall 2019.
- **Approximate Degree: A Survey**.
  - Invited talk at CMO 2018 workshop on Analytic Techniques in Theoretical Computer Science
- **The Polynomial Method Strikes Back**.
  - Invited talk at the Harvard/MIT/MSR Theory Reading Group (October 2017)
  - Invited talk at NYU Theory Seminar (December 2017)
  - Invited talk at University of Maryland's QuICS Seminar (January 2017)
- **Verifiable Computing: Between Theory and Practice**.
  - Invited survey talk at the *STOC* 2017 workshop on *Probabilistically Checkable and Interactive Proofs (PCP/IP): Between Theory and Practice* (June 2017).
- **A Nearly Optimal Lower Bound on the Approximate Degree of AC^0**.
  - Invited talk at BIRS 2017 workshop on Communication Complexity and its Applications II
  - Invited talk at Columbia University Theory Seminar (April 2017)
- **Chebyshev Polynomials, Approximate Degree, and their Applications**.
  - Invited survey talk at the *FOCS* 2016 workshop on *(Some) Orthogonal Polynomials and their Applications to TCS*.
- **Verifiable Computation.**
  - Invited speaker at the Fourteenth Bellairs' Crypto-Workshop (Invited Lecture Series). Delivered 15 hours of lectures surveying modern techniques for proof-based verifiable computation. Workshop organized by Claude Crépeau.
- **Interactive Proofs and Argument Systems.**
  - Invited speaker at the Summer School on Secure and Oblivious Computation and Outsourcing at the University of Notre Dame. Delivered 3 hours of lectures surveying modern techniques for proof-based verifiable computation. Summer school organized by Marina Blanton.

Grants and Funding

- **DARPA Award (Agreement No. HR00112020022)**.
  - Project Title: ZK Proofs Unbound: Next-Generation Pipelines for Real-world Applications.
  - DARPA Program: Securing Information for Encrypted Verification and Evaluation (SIEVE).
  - Role: Georgetown PI (collaborative work with NYU, UPenn, Columbia, and Stanford).
  - Amount: $5,715,365. Georgetown's share: $500,000.
  - Dates: May 2020-March 2024.
- **National Science Foundation Award #1918989**.
  - Project Title: Automatically Parallelizing Approximate Data Analysis with Mergeable Summaries.
  - NSF Program: Scalable Parallelism in the Extreme.
  - Role: PI.
  - Amount: $614,203.
  - Dates: October 2019-September 2023.
- **National Science Foundation CAREER Award #1845125**.
  - Project Title: The Polynomial Method in Complexity and Cryptography.
  - NSF Program: Algorithmic Foundations.
  - Role: PI.
  - Amount: $549,045.
  - Dates: June 2019-May 2024.
- **Award from The Graph Foundation**.
  - Project title: Zero-Knowledge Proofs for the Decentralized Web.
  - Amount: $69,000.
  - Role: PI
  - Year awarded: 2021
- **Research Seed Grant (Internal) from Georgetown University's Massive Data Institute**.
  - Project Title: Enabling Analysis of Sensitive Data via Zero-Knowledge Proofs.
  - Role: PI.
  - Amount: $40,000.
  - Dates: July 2017-June 2018

U.S. Patents

- **Automatic Fantasy Sports Data Analysis Method and Apparatus**. Michael Lazarus, Maxim Sviridenko, and Justin Thaler. Patent number: US10463975B2. Type: Grant. Filed: June 30, 2016. Date of Patent: November 5, 2019. Assignee: OATH INC.
- **Fantasy Sports Data Analysis for Game Structure Development**. Justin Thaler, Maxim Sviridenko, Edo Liberty, Ron Belmarch, Jerry Shen, and Prerit Uppal. Patent number: US10207188B2. Date of Patent: Feb. 19, 2019. Assignee: OATH INC.

Open Source Software Development

- Co-creator and core contributor to an open source library of highly optimized streaming algorithms, called *DataSketches* (url: `https://datasketches.apache.org/`). The library is used within several companies, including Verizon, Netflix, Nielsen, and Splice Machine. It also has been incorporated into a popular open source graph database library called Gaffer that is maintained by the British intelligence agency GCHQ, and into a low-latency open source data store called Druid. In April 2019, the library was accepted by the Apache Software Foundation (ASF) as an Apache Incubation project and was promoted to a top-level ASF project in December 2020.

Teaching

- COSC 548 – Streaming Algorithms (Fall 2016, Fall 2018)
- ANLY 550 – Structures and Algorithms for Analytics (Spring of: 2017, 2018 (2 sections), 2019)
- COSC 544 – Probabilistic Proof Systems (Fall 2017, Fall 2020)
- COSC 547 – Analytic Techniques in Computer Science (Fall 2022)
- ANLY 558 – Advanced Algorithms for Analytics (Spring 2021)

Professional Activities

- **Editorial Board Member**: SIAM Journal on Computing (2023-present).
- **PC Member**: RANDOM 2022, TCC 2021, ESA 2021, TCC 2020, ZKProof Standardization Proposal Committee (2019, 2020), STOC 2019, SOSA 2019, SODA 2018, FSTTCS 2017, ICALP 2016, ALENEX 2016, SDM 2015.
- **Steering Committee**: ZKProof (2023-present)
- **Grant Reviews and Panels**: National Science Foundation Panel (2017, 2019, 2020), Computing Innovation Fellows 2020 Reviewer, External reviewer for Research Grants Council of Hong Kong (2018) and Israel Science Foundation (2019, 2020).
- **Workshop Organization**: Co-organizer of Capital Area Theory Day (2018). Co-organizer and chair of the 5-day workshop on Probabilistically Checkable and Interactive Proof Systems at Simons Institute for the Theory of Computing (October 2019).
- **Journal reviewer**: *SICOMP*, *Computational Complexity*, *Journal of Cryptology*, *Theory of Computing*, *SIAM Journal on Discrete Mathematics*, *Information and Computation*, *Algorithmica*, *Communications of the ACM*, *Discrete and Computational Geometry*, *Theoretical Computer Science*, *Frontiers in ICT (Big Data Section)*, *Information Processing Letters*.
- **External conference reviewer**: STOC, FOCS, CCC, SODA, CRYPTO, ICALP, ITCS, RANDOM, PODS, NIPS, ICDT, PODC, DISC, TCC, ESORICS, ESA, MFCS.

Advising and Mentorship

- Ph.D. advisor for Shuchen Zhu, currently a fifth-year Ph.D. student in Georgetown University's Department of Computer Science (Spring 2018-present).
- Ph.D. advisor for Sidhant Saraogi, currently a third-year Ph.D. student in Georgetown University's Department of Computer Science (Fall 2020-present).
- Co-mentor of postdoctoral scholar Alex Block (Fall 2022-present).
- Mentor of postdoctoral scholar Nikhil Mande (Spring 2019-Spring 2021).
- Co-mentor of postdoctoral scholar Michael Clear, joint with Adam O'Neill (Fall 2017-Fall 2018).
- Hosted 5-week visit from Nikhil Mande, graduate student at Tata Institute of Fundamental Research.
- Mentored two Georgetown University undergraduates, Pryce Bevan and Daniel Anderson, on a year-long research project on streaming algorithms that led to publication (22) above.
- Co-host for Yahoo Labs intern Christopher Musco, Ph.D. student at MIT (Summer 2015).

Service to Georgetown University

- CS Graduate Committee (Fall 2019-Spring 2020, Spring 2021, Fall 2022).
- Department of Computer Science Student Engagement Committee (Fall 2020-present).
- CS Colloquium Committee (Fall 2016-Spring 2019).
- Steering Committee Member for Georgetown's M.S. in Analytics (Fall 2017-Spring 2018).
- Computer Science Faculty Advisory Committee (Fall 2018-Spring 2019)
- Admissions Committee Member for Georgetown's M.S. in Analytics (Spring 2017).
- Participant in Campaign Planning: Big Ideas—Big Data. Fall 2017.

Thesis Committee Membership

- Ph.D. proposal and thesis committee member for Prantar Ghosh, Darmouth University Department of Computer Science. Thesis defense occurred in May 2022.
- Ph.D. proposal and thesis committee member for Jakob Prange, Georgetown University Department of Computer Science. Thesis defense occurred in April 2022.
- Ph.D. proposal and thesis committee member for Robert Churchill, Georgetown University Department of Computer Science. Thesis defense occurred in December 2021.
- External Ph.D. thesis examiner for Christopher Hickey, University of Warwick Department of Computer Science. Viva exam occurred in December 2020.
- Ph.D. proposal and thesis committee member for Hao-Ren Yao, Georgetown University Department of Computer Science. Thesis defense occurred in March 2021.
- Ph.D. proposal and thesis committee member for Sean Macavaney, Georgetown University Department of Computer Science. Thesis defense in March 2021.
- Ph.D. proposal and thesis committee member for Christopher Flagg, Georgetown University Department of Computer Science. Thesis defense in April 2021.
- Ph.D. qualifying and thesis committee member for Jeffrey Cohn, Georgetown University Department of Physics. Thesis defense in April 2019.
- Ph.D. proposal and thesis committee member. Samira Daruki, University of Utah. Thesis defense in May 2017.

Other Writings

- Measuring SNARK performance: Frontends, backends, and the future. a16zcrypto blog post. August 2022.
- SNARK Security and Performance. a16zcrypto blog post. September 2022.
- Zero-knowledge canon: an annotated reading list. a16zcrypto blog post, September 2022.

Scientific Advisory Positions

- QEDIT Systems LTD (Scientific Advisory Board: September 2019-present)
- Protocol Labs (Advisor: 2021-2022)