Sam Gunn

CONTACT

Massachusetts Institute of Technology
Building 2, Room 246-A
Cambridge, MA 02139 USA

Email: gunn@mit.edu
Website: samuel-gunn.github.io

POSITIONS

Massachusetts Institute of Technology
C.L.E. Moore Instructor of Mathematics (Summer 2026 to Present)

EDUCATION

The University of California, Berkeley
Ph.D. in Computer Science (Fall 2020 to Summer 2026)
Advisor: Umesh Vazirani

The University of Texas at Austin
B.S. in Mathematics (Fall 2016 to Spring 2020)
Advisors: Scott Aaronson and Cameron Gordon

RESEARCH

Journal publications

1. Omar Alrabiah, Prabhanjan Ananth, Miranda Christ, Yevgeniy Dodis, and Sam Gunn. "Ideal pseudorandom codes." *SIAM Journal on Computing*, Special Issue for the 57th Annual ACM Symposium on Theory of Computing (STOC). ePrint: 2024/1840.
2. Sam Gunn, Nathan Ju, Fermi Ma, and Mark Zhandry. "Commitments to quantum states." *SIAM Journal on Computing*, Special Issue for the 55th Annual ACM Symposium on Theory of Computing (STOC). ePrint: 2022/1358.
3. Scott Aaronson and Sam Gunn. "On the classical hardness of spoofing linear cross-entropy benchmarking." *Theory of Computing* 16(11):1–8 (2020). DOI: 10.4086/toc.2020.v016a011. arXiv: 1910.12085.

Conference publications

1. Miranda Christ, Noah Golowich, Sam Gunn, Ankur Moitra, and Daniel Wichs. "Improved pseudorandom codes from permuted puzzles." *Proceedings of the 58th Annual ACM Symposium on Theory of Computing (STOC)*. 2026. DOI: 10.1145/3798129.3800916. ePrint: 2025/2222.
2. Sanjam Garg, Sam Gunn, and Mingyuan Wang. "Black-box crypto is useless for pseudorandom codes." *Proceedings of the 23rd Theory of Cryptography Conference (TCC)*. 2025. DOI: 10.1007/978-3-032-12290-2_7. ePrint: 2025/1021. Outstanding Paper Award.
3. Sam Gunn, Xuandong Zhao, and Dawn Song. "An undetectable watermark for generative image models." *The Thirteenth International Conference on Learning Representations (ICLR)*. 2025. arXiv: 2410.07369.
4. Xuandong Zhao, Sam Gunn, Miranda Christ, Jaiden Fairoze, Andres Fabrega, Nicholas Carlini, Sanjam Garg, Sanghyun Hong, Milad Nasr, Florian Tramer, Somesh Jha, Lei Li, Yu-Xiang Wang, and Dawn Song. "SoK: Watermarking for AI-generated content." *Proceedings of the 46th IEEE Symposium on Security and Privacy (S&P)*. 2025. DOI: 10.1109/SP61157.2025.00178. arXiv: 2411.18479.
5. Omar Alrabiah, Prabhanjan Ananth, Miranda Christ, Yevgeniy Dodis, and Sam Gunn. "Ideal pseudorandom codes." *Proceedings of the 57th Annual ACM Symposium on Theory of Computing (STOC)*. 2025. DOI: 10.1145/3717823.3718309. ePrint: 2024/1840.
6. Sam Gunn and Ramis Movassagh. "Quantum one-time protection of any randomized algorithm." *Proceedings of the 45th Annual International Cryptology Conference (CRYPTO)*. 2025. DOI: 10.1007/978-3-032-01878-6_11. ePrint: 2024/1798.
7. Sam Gunn, Yael Tauman Kalai, Anand Natarajan, and Ági Villányi. "Classical commitments to quantum states." *Proceedings of the 57th Annual ACM Symposium*

on Theory of Computing (STOC). 2025. DOI: 10.1145/3717823.3718264. ePrint: 2024/606. Presented at *Quantum Information Processing (QIP)*.

8. Miranda Christ and Sam Gunn. "Pseudorandom error-correcting codes." *Proceedings of the 44th Annual International Cryptology Conference (CRYPTO)*. 2024. DOI: 10.1007/978-3-031-68391-6_10. ePrint: 2024/235.
9. Miranda Christ, Sam Gunn, and Or Zamir. "Undetectable watermarks for language models." *Proceedings of the 37th Annual Conference on Learning Theory (COLT)*. 2024. ePrint: 2023/763. Presented at *Real World Crypto (RWC)*.
10. Andrea Coladangelo and Sam Gunn. "How to use quantum indistinguishability obfuscation." *Proceedings of the 56th Annual ACM Symposium on Theory of Computing (STOC)*. 2024. DOI: 10.1145/3618260.3649779. ePrint: 2023/1756.
11. Thiago Bergamaschi, Louis Golowich, and Sam Gunn. "Approaching the quantum Singleton bound with approximate error correction." *Proceedings of the 56th Annual ACM Symposium on Theory of Computing (STOC)*. 2024. DOI: 10.1145/3618260.3649680. arXiv: 2212.09935. Presented at *Quantum Information Processing (QIP)*.
12. Sam Gunn, Nathan Ju, Fermi Ma, and Mark Zhandry. "Commitments to quantum states." *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC)*. 2023. DOI: 10.1145/3564246.3585198. ePrint: 2022/1358. Presented at *Quantum Information Processing (QIP)*.
13. Scott Aaronson and Sam Gunn. "On the classical hardness of spoofing linear cross-entropy benchmarking." 2020. arXiv: 1910.12085. Presented at the *Twenty-Second Annual Southwest Quantum Information and Technology Workshop (SQuInT)*.

Manuscripts

1. Sam Gunn. "How to sketch a learning algorithm." 2026. arXiv: 2604.07328. In submission.

Awards

- Google PhD Fellowship 2022–2025
- Lotfi A. Zadeh Prize 2024–2025

Talks

"How to Sketch a Learning Algorithm"

- MIT ML+Cryptography Seminar — May 2026
- Institute for Advanced Study — May 2026
- Flatiron Institute — June 2026
- Theory for Trustworthy and Interpretable AI at STOC 2026 — June 2026
- Invited talk at ITC 2026 — August 2026

"On Undetectable Backdoors"

- UT Austin Theory and Alignment Group — November 2025

"Pseudorandom Error-Correcting Codes"

- NTT Research — March 2024
- Google Research NYC — April 2024
- CRYPTO 2024 — August 2024
- NYU Cryptography Seminar — March 2025
- Harvard Theory Seminar — September 2025
- TCC 2025 — December 2025

"Undetectable Watermarks for Language Models"

- Google Research Mountain View — July 2023
- MIT Cryptography Group — August 2023
- NYU Cryptography Seminar (video) — September 2023
- Berkeley ML Theory Seminar — September 2023

"Quantum One-Time Protection of Any Randomized Algorithm"
- CRYPTO 2025 — August 2025

"Quantum Indistinguishability Obfuscation"
- CIQC Spark Talk — March 2024
- University of Ottawa Quantum Seminar — April 2024

"Approaching the Quantum Singleton Bound with Approximate Error Correction"
- Simons Quantum Colloquium (video) — December 2022

"Commitments to Quantum States"
- STOC 2023 (video) — June 2023

"Unclonable Cryptography"
- Guest lecture for Quantum Complexity, UC Berkeley — December 2022

"Certified Entropy from Random Circuit Sampling"
- Berkeley Theory Lunch — March 2022

SERVICE

Program Committee, ITCS — 2027
MIT Computer Science UROP Mentor — Summer 2026
Berkeley Computer Science DRP Mentor — Spring 2021

REVIEWING

STOC, FOCS, SODA, CRYPTO, EUROCRYPT, TCC, NeurIPS, ICLR, QIP, Annals of Statistics