Seyoon Ragavan

sragavan@mit.edu | sragavan99.github.io

32 Vassar St, G-578 - Cambridge, MA 02139 - USA

Education

- **Massachusetts Institute of Technology** *June 2024 - present*
  Ph.D. Candidate in Electrical Engineering and Computer Science Cambridge, MA
- **Massachusetts Institute of Technology** *September 2023 - May 2024*
  S.M. in Electrical Engineering in Computer Science Cambridge, MA
- **Princeton University** *September 2017 - May 2021*
  Bachelor of Arts in Mathematics, Highest Honours Princeton, NJ
  - Certificates in Applications of Computing, Applied Mathematics, and Cognitive Science
  - GPA: 3.96/4

Publications

[1] Gregory D. Kahanamoku-Meyer, Seyoon Ragavan, Vinod Vaikuntanathan, and Katherine Van Kirk. The Jacobi factoring circuit: quantum factoring with near-linear gates and sublinear space. [STOC 2025, ePrint]

[2] Seyoon Ragavan, Neekon Vafa, and Vinod Vaikuntanathan. Indistinguishability obfuscation from bilinear maps and LPN variants. [TCC 2024, ePrint]

[3] Seyoon Ragavan and Vinod Vaikuntanathan. Space-efficient and noise-robust quantum factoring. **Best Paper Award, invited to the Journal of Cryptology.** [CRYPTO 2024, ePrint]

[4] Orestis Plevrakis, Seyoon Ragavan, and S. Matthew Weinberg. On the cut-query complexity of approximating max-cut. [ICALP 2024, arXiv]

[5] Ryan Arbon, Mohammed Mannan, Michael Psenka, and Seyoon Ragavan. A proof of the triangular Ashbaugh–Benguria–Payne–Pólya–Weinberger inequality. [Journal of Spectral Theory 2022]

[6] Arjun Sai Krishnan and Seyoon Ragavan. Morphology-aware meta-embeddings for Tamil. [NAACL Student Research Workshop 2021]

Manuscripts

[1] Gregory D. Kahanamoku-Meyer, Seyoon Ragavan, and Katherine Van Kirk. Parallel spooky pebbling makes Regev factoring more practical. [ePrint]

[2] Alexander Poremba, Seyoon Ragavan, and Vinod Vaikuntanathan. Cloning games, black holes and cryptography. [ePrint]

[3] Seyoon Ragavan. Regev factoring beyond Fibonacci: optimizing prefactors. [ePrint]

Talks

The Jacobi Factoring Circuit: Classically Hard Factoring in Sublinear Quantum Space and Depth

- Tufts University Quantum Computing Seminar *September 2025*
- UNSW Number Theory Days *August 2025*
- Ruhr University Bochum Quantum Information Workshop *April 2025*
- Simons Institute Quantum Colloquium *March 2025*
- MIT Quantum Information Seminar *March 2025*
- CMU Theory Seminar *March 2025*

Cloning Games, Black Holes and Cryptography

- CMU CyLab Crypto Seminar *March 2025*

Factoring with a Quantum Computer: The State of the Art

- University of Technology Sydney *August 2025*
- University of Sydney *August 2025*
- QuEra Computing, with Gregory D. Kahanamoku-Meyer and Katherine Van Kirk *April 2025*
- MIT Schwarzman College of Computing Cryptography and Security Day *January 2025*

Indistinguishability Obfuscation from Bilinear Maps and LPN Variants

- MIT Cryptography and Information Security Seminar *September 2024*

Space-Efficient and Noise-Robust Quantum Factoring

- CRYPTO 2024 *August 2024*
- IBM Quantum Seminar *November 2023*
- Yale Quantum Institute *November 2023*

The Cut-Query Complexity of Approximating Max-Cut

- ICALP 2024 *July 2024*

Awards and Fellowships

- **William A. Martin S.M. Thesis Award** *2025*
  Massachusetts Institute of Technology (for outstanding master's theses in computer science)
- **Jane Street Graduate Research Fellowship**, finalist *2025*
- **CRYPTO 2024 Best Paper Award** *August 2024*
- **Akamai Presidential Fellowship**, MIT *September 2023 - May 2024*
- **George B. Covington Prize in Mathematics** *May 2021*
  Princeton University (top prize for overall excellence in mathematics)
- **Phi Beta Kappa**, elected to the Princeton chapter *May 2021*
- **Sigma Xi**, elected to the Princeton chapter *May 2021*
- **Peter Greenberg Memorial Prize** *May 2020*
  Princeton University (for junior accomplishments in mathematics)
- **Putnam Competition** *2017-2019*
  Honourable Mention (top 100 participants across colleges in the USA)
- **Shapiro Prize for Academic Excellence** *2019*
  Princeton University (top 2% of undergraduate students)
- **Manfred Pyka Memorial Prize in Physics**, Princeton University *2018*
- **International Mathematical Olympiad** *2013-2016*
  Represented Australia four times: 1 gold and 3 bronze medals

Selected Coursework

Massachusetts Institute of Technology

- Foundations of Cryptography
- Quantum Cryptography
- Advanced Topics in Cryptography: Proof Systems
- Advanced Topics in Cryptography: From Lattices to Program Obfuscation
- Advanced Complexity Theory

Princeton University

- Advanced Algorithm Design
- Information Theory
- Graph Algorithms
- Learning Theory
- Natural Language Processing
- Analytic Number Theory
- Quantum Mechanics

Teaching and Service

- **Program Committee Member**, QIP *2025-2026*
- **Teaching Assistant**, MIT (Mathematics for Computer Science) *Fall 2025*
- **International Mathematical Olympiad** *2025*
  Problem Selection Committee Member and Coordinator (Grader)
- **Trainer and Grader**, for Australia's International Mathematical Olympiad team *2017, 2020-2024*
- **Teaching Assistant**, Princeton University (Economics and Computing) *Spring 2019*
- **Peer Academic Advisor**, Princeton University (for 30 first-years and sophomores) *2019-2021*

Experience

- **Citadel Securities**, Quantitative Research Analyst *August 2021 - January 2023*
- **Citadel Securities**, Quantitative Research Analyst Intern *Summer 2020*
- **Princeton University**, Research Intern, Theoretical Machine Learning *Summer 2019*
- **Afari** (student-founded social media startup), Software Engineering Intern *Summer 2018*

Interests and Skills

Languages: English, Tamil
Technical: Python, NumPy, pandas, scikit-learn, xarray, PyTorch, Slurm, AWS, C++, Java
Music: Mridangam (South Indian classical drum), drum kit, voice