Henry Yuen

Srivani Family Associate Professor of Computer Science
Columbia University

Phone: 212-853-8476
Email: hyuen@cs.columbia.edu
Homepage: henryyuen.net

Research area

Quantum computing, quantum information, cryptography, complexity theory.

Appointments held

2025 – Associate Professor (with Tenure), Columbia University
Department of Computer Science

2024 – 2025 Associate Professor (without Tenure), Columbia University
Department of Computer Science

2021 – 2023 Assistant Professor, Columbia University
Department of Computer Science

2018 – 2021 Assistant Professor, University of Toronto
Departments of Computer Science and Mathematics (*joint appointment*)

2016 – 2018 Postdoctoral Associate in Computer Science, University of California, Berkeley

Education

2011 – 2016 Ph.D. in Computer Science, MIT
Thesis supervisor: Dana Moshkovitz
Thesis title: *Games, Protocols, and Quantum Entanglement*

2006 – 2010 B.A. in Mathematics, University of Southern California

Honors & Awards

2022 Sloan Research Fellow.

2022 NSF CAREER Award.

2020 Simons-Berkeley Research Fellowship.

2015 – 2017 Simons Graduate Fellowship for Theoretical Computer Science

2012 – 2015 NSF Graduate Fellowship

2011 MIT Presidential Fellowship

Grants

2026 - 2029 AFOSR MURI: N-qubit gates: Theory, Systems, and Experiment.

2025 - 2026 Columbia Research Stabilization grant

2025 - 2027 NSF Small: Complexity theory aspects of quantum cryptography
co-PI with Prabhanjan Ananth, Celine Chevalier, Alex Grilo, Damien Vergnaud, Quoc-Huy Vu

2024 - 2027 NSF Small: Theoretical Foundations of Quantum Pseudorandom Primitives
co-PI with Prabhanjan Ananth

2023 - 2025 DOE EXPRESS 2023 Grant
co-PI with Sebastian Will and Dan Rubenstein

2023 - 2028 Air Force Office of Scientific Research Grant

2023 - 2025 Brookhaven National Lab grant: Hybrid Digital-Analog Quantum Algorithms
co-PI with Sebastian Will (Columbia Physics)

2022 - 2024 Sloan Research Fellowship

2022 - 2027 NSF CAREER Award

2020 - 2023 Air Force Office of Scientific Research Grant

2019 Google Quantum Research Award
Held at U. of Toronto
co-PI with Juan Carrasquilla (Vector Institute)

2019 – 2022 NSERC Discovery Grant (Sole PI at U. of Toronto)

Publications

Conference proceedings

2026

C1. Magic and communication complexity
Uma Girish, Alex May, Natalie Parham, Henry Yuen.
In proceedings of *Symposium on Theory of Computing (STOC) 2026*.
Available at https://arxiv.org/abs/2510.07246

C2. Local transformations of bipartite entanglement are rigid.
John Bostanci, Tony Metger, Henry Yuen.
In proceedings of *Innovations in Theoretical Computer Science (ITCS) 2026*.
Available at https://arxiv.org/abs/2509.05257

C3. Random Unitaries in Constant (Quantum) Time
Ben Foxman, Natalie Parham, Francisca Vasconcelos, Henry Yuen.
In proceedings of *Innovations in Theoretical Computer Science (ITCS) 2026*.
Available at https://arxiv.org/abs/2508.11487

C4. The Hardness of Learning Quantum Circuits and its Cryptographic Applications
Bill Fefferman, Soumik Ghosh, Makrand Sinha, Henry Yuen.
In proceedings of *Innovations in Theoretical Computer Science (ITCS) 2026*.
Available at https://arxiv.org/abs/2504.15343

C5. Unitary Complexity and the Uhlmann Transformation Problem.
John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, Henry Yuen.
In proceedings of *Innovations in Theoretical Computer Science (ITCS) 2026*.
Available at https://arxiv.org/abs/2306.13073.

2025

C6. QMA vs QCMA and Pseudorandomness.
Jiahui Liu, Saachi Mutreja, Henry Yuen.
In proceedings of *Symposium on Theory of Computing (STOC) 2025*.
Available at https://arxiv.org/abs/2411.14416

C7. Simultaneous Haar Indistinguishability with Applications to Unclonable Cryptography.
Prabhanjan Ananth, Fatih Kaleoglu, Henry Yuen.
In proceedings of *Innovations in Theoretical Computer Science (ITCS) 2025*.

Available at https://arxiv.org/abs/2405.10274

2024

C8. Simple constructions of linear-depth t-designs and pseudorandom unitaries.
Tony Metger, Alexander Poremba, Makrand Sinha, Henry Yuen.
In proceedings of *Foundations of Computer Science (FOCS) 2024*.
Available at https://arxiv.org/abs/2404.12647.

C9. Pseudorandom Strings from Pseudorandom Quantum States.
Prabhanjan Ananth, Yao-Ting Lin, Henry Yuen.
In proceedings of *Innovations in Theoretical Computer Science (ITCS) 2024*.
Available at https://arxiv.org/abs/2306.05613.

C10. An efficient quantum parallel repetition theorem.
John Bostanci, Luowen Qian, Nick Spooner, Henry Yuen.
In proceedings of *Symposium on Theory of Computing (STOC) 2024*.
Presented at *Quantum Information Processing (QIP) 2024*.
Available at https://arxiv.org/.

C11. On the Pauli Spectrum of QAC^0.
Shivam Nadimpalli, Natalie Parham, Francisca Vasconcelos, Henry Yuen.
In proceedings of *Symposium on Theory of Computing (STOC) 2024*.
Presented at *Quantum Information Processing (QIP) 2024*.
Available at https://arxiv.org/abs/2311.09631.

2023

C12. On the (Im)plausibility of Public-Key Quantum Money from Collision-Resistant Hash Functions.
Prabhanjan Ananth, Zihan Hu, Henry Yuen.
In proceedings of *AsiaCrypt 2023*.
Available at https://eprint.iacr.org/2023/069.

C13. $\mathsf{stateQIP} = \mathsf{statePSPACE}$.
Tony Metger, Henry Yuen.
In proceedings of *Foundations of Computer Science (FOCS) 2023*.
Presented at *Quantum Information Processing (QIP) 2023*.
Available at https://arxiv.org/abs/2301.07730.

C14. Unitary property testing lower bounds by polynomials.
Adrian She, Henry Yuen.
In proceedings of *Innovations in Theoretical Computer Science (ITCS) 2023*.

Presented at *Quantum Information Processing (QIP) 2023*.
Available at https://arxiv.org/abs/2210.05885

C15. Testing and Learning Quantum Juntas Nearly Optimally.
Thomas Chen, Shivam Nadimpalli, Henry Yuen.
In proceedings of *Symposium on Discrete Algorithms (SODA) 2023*.
Presented at *Quantum Information Processing (QIP) 2023*.
Available at https://arxiv.org/abs/2207.05898

2022

C16. Pseudorandom (Function-Like) Quantum State Generators: New Definitions and Applications.
Prabhanjan Ananth, Aditya Gulati, Luowen Qian, Henry Yuen.
In proceedings of *Theory of Cryptography Conference (TCC) 2022*.
Presented at *QCRYPT 2022*.
Presented at *Quantum Information Processing (QIP) 2023* as **Short plenary**.
Available at https://arxiv.org/abs/2211.01444

C17. Cryptography from Pseudorandom Quantum States.
Prabhanjan Ananth, Luowen Qian, Henry Yuen.
In proceedings of *CRYPTO 2022*.
Presented at *QCRYPT 2022*.
Available at https://arxiv.org/abs/2112.10020

C18. Quantum search-to-decision reductions and the state synthesis problem.
Sandy Irani, Anand Natarajan, Chinmay Nirkhe, Sujit Rao, Henry Yuen.
In proceedings of *Computational Complexity Conference (CCC) 2022*.
Presented at *Quantum Information Processing (QIP) 2022*.
Available at https://arxiv.org/abs/2111.02999

C19. Interactive proofs for synthesizing quantum states and unitaries.
Gregory Rosenthal, Henry Yuen.
In proceedings of *Innovations of Theoretical Computer Science (ITCS) 2022*.
Presented at *Quantum Information Processing (QIP) 2022*.
Available at https://arxiv.org/abs/2108.07192

C20. Quantum Garbled Circuits.
Zvika Brakerski, Henry Yuen.
In proceedings of *Symposium on Theory of Computation (STOC) 2022*.
Presented at *Quantum Information Processing (QIP) 2021*.
Available at https://arxiv.org/abs/2006.01085

C21. Nonlocal Games, Compression Theorems, and the Arithmetical Hierarchy.
Hamoon Mousavi, Seyed Sajjad Nezhadi, Henry Yuen.
In proceedings of *Symposium on Theory of Computation (STOC) 2022*.
Presented at *Quantum Information Processing (QIP) 2022* as a **Plenary talk**.
Available at https://arxiv.org/abs/2110.04651

2021

C22. Quantum soundness of testing tensor codes.
Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, Henry Yuen.
In proceedings of *Foundations of Computer Science (FOCS) 2021*.
Available at https://arxiv.org/abs/2111.08131

2020

C23. On the complexity of zero gap MIP^*.
Hamoon Mousavi, Seyed Sajjad Nezhadi, Henry Yuen.
Presented at *TQC 2020*.
In proceedings of *Int'l Coll. on Automata, Languages, and Programming (ICALP) 2020*.

2019

C24. Perfect zero knowledge for quantum multiprover interactive proofs.
Alex B. Grilo, William Slofstra, Henry Yuen.
Presented at *QCRYPT 2019*.
Presented at *Quantum Information Processing (QIP) 2020*.
In proceedings of *Foundations of Computer Science (FOCS) 2019*.

C25. Good approximate quantum LDPC codes from spacetime circuit Hamiltonians.
Thomas C. Bohdanowicz, Elizabeth Crosson, Chinmay Nirkhe, Henry Yuen.
Presented at *Quantum Information Processing (QIP) 2019*.
In proceedings of *Symposium on Theory of Computing (STOC) 2019*.

C26. Quantum proof systems for iterated exponential time, and beyond.
Joseph Fitzsimons, Zhengfeng Ji, Thomas Vidick, Henry Yuen.
Presented at *Quantum Information Processing (QIP) 2019*.
In proceedings of *Symposium on Theory of Computing (STOC) 2019*.

2018

C27. Approximate low-weight check codes and circuit lower bounds for noisy ground states.
Chinmay Nirkhe, Umesh Vazirani, Henry Yuen.

In proceedings of *Int'l Coll. on Automata, Languages, and Programming (ICALP) 2018*. pp. 91:1-11.
Presented at *TQC 2018*.

C28. Noise-tolerant testing of high entanglement of formation
Rotem Arnon-Friedman, Henry Yuen.
In proceedings of *Int'l Coll. on Automata, Languages, and Programming (ICALP) 2018*. pp. 11:1-12.

2017

C29. New security notions and feasibility results for authentication of quantum data
Sumegha Garg, Henry Yuen, and Mark Zhandry.
In proceedings of *Annual International Cryptology Conference (CRYPTO) 2017*, pp. 342–371. Presented at *QCrypt 2016*.

C30. Anchoring games for parallel repetition
Mohammad Bavarian, Thomas Vidick, and Henry Yuen.
In proceedings of *Symposium on Theory of Computing (STOC) 2017*, pp. 303–316.
Presented as a Plenary Talk at *Quantum Information Processing (QIP) 2016*.

C31. Multiplayer parallel repetition for expander games
Irit Dinur, Prahladh Harsha, Rakesh Venkat, and Henry Yuen.
In proceedings of *Innovations in Theoretical Computer Science (ITCS) 2017*, pp. 37:1–37:16. **Highlighted Talk** at ITCS 2017.

C32. Parallel repetition via fortification: analytic view and the quantum case
Mohammad Bavarian, Thomas Vidick, and Henry Yuen.
In proceedings of *Innovations in Theoretical Computer Science (ITCS) 2017*, pp. 22:1–22:33.
Presented at *TQC 2016*.

2016

C33. A parallel repetition theorem for all entangled games
Henry Yuen.
In proceedings of *Int'l Coll. on Automata, Languages, and Programming (ICALP) 2016*, pp. 77:1–77:13.
Presented at *Quantum Information Processing (QIP) 2017*.

C34. A No-Go Theorem for Derandomized Parallel Repetition: Beyond Feige-Kilian
Dana Moshkovitz, Govind Ramnarayan, and Henry Yuen
In proceedings of *APPROX-RANDOM 2016*, pp. 43:3–42:29.

C35. On the sum-of-squares degree of symmetric quadratic functions
Troy Lee, Anupam Prakash, Ronald de Wolf, and Henry Yuen.
In proceedings of *Computational Complexity Conference (CCC) 2016*, pp. 17:1–17:31.

2015

C36. Parallel repetition for entangled k-player games via fast quantum search
Kai-min Chung, Xiaodi Wu and Henry Yuen.
In proceedings of *Computational Complexity Conference (CCC) 2015*, pp. 512–536

2014

C37. Infinite Randomness Expansion and Amplification with a Constant Number of Devices
Matthew Coudron and Henry Yuen.
In proceedings of *Symposium on Theory of Computing (STOC) 2014*, pp. 427–436.
Presented at *Quantum Information Processing (QIP) 2014*

2013

C38. Robust Randomness Amplifiers: Upper and Lower Bounds
Matthew Coudron, Thomas Vidick, and Henry Yuen.
In proceedings of *APPROX-RANDOM 2013*, pp. 468–483.

2012

C39. Continuous Time Channels with Interference
Ioana Ivan, Michael Mitzenmacher, Justin Thaler, and Henry Yuen.
In proceedings of *International Symposium on Information Theory (ISIT) 2012*, pp. 860-864

Journal articles

2023

J1. Rigidity of superdense coding.
Ashwin Nayak, Henry Yuen.
In *ACM Transactions on Quantum Computing, Vol. 4, Iss. 4, pp 1–39 (2023). Available at* https://doi.org/10.1145/3593593

J2. An Improved Sample Complexity Lower Bound for Quantum State Tomography.
Henry Yuen.
In *Quantum 7, 890 (2023)*.
Available at https://quantum-journal.org/papers/q-2023-01-03-890/

2022

J3. Quantum soundness of testing tensor codes.
Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, Henry Yuen.
In *Discrete Analysis, 2022:17*.
Available at https://doi.org/10.19086/da.55554

J4. Anchored parallel repetition for nonlocal games.
Mohammad Bavarian, Thomas Vidick, and Henry Yuen.
In *SIAM Journal on Computing, Vol. 51, No. 2, pp. 214–253* (2022).
Available at https://doi.org/10.1137/21M1405927

2020

J5. Exploring entanglement and optimization within the Hamiltonian Variational Ansatz.
Roeland Wiersema, Cunlu Zhou, Yvette de Sereville, Juan Felipe Carrasquilla, Yong Baek Kim, Henry Yuen.
In *Physical Review X Quantum Vol. 1, Iss. 2* (2020).
Available at https://doi.org/10.1103/PRXQuantum.1.020319

2016

J6. Rescuing Complementarity With Little Drama.
Ning Bao, Adam Bouland, Aidan Chatwin-Davies, Jason Pollack, and Henry Yuen.
In *Journal of High Energy Physics (JHEP)*, 2016:26.
Available at https://doi.org/10.1007/JHEP12(2016)026

2014

J7. A quantum lower bound for distinguishing random functions from random permutations.
Henry Yuen.
In *Quantum Information and Computation*, 14(9-10), 2014.
Available at https://dl.acm.org/doi/10.5555/2685164.2685166

Preprints

2026

P1. Private proofs of when and where.
Uma Girish, Greg Gluch, Shafi Goldwasser, Tal Malkin, Leo Orshansky, Henry Yuen.
Available at https://arxiv.org/abs/2601.18961

P2. Digital signatures with classical shadows on near-term quantum computers.
Pradeep Niroula, Minzhao Liu, Sivaprasad Omanakuttan, David Amaro, Shouvanik Chakrabarti, Soumik Ghosh, Zichang He, Yuwei Jin, Fatih Kaleoglu, Steven Kordonowy, Rohan Kumar, Michael A. Perlin, Akshay Seshadri, Matthew Steinberg, Joseph Sullivan, Jacob Watkins, Henry Yuen, Ruslan Shaydulin.
Available at https://arxiv.org/abs/2602.04859

P3. Computer Science Challenges in Quantum Computing: Early Fault-Tolerance and Beyond.
Jens Palsberg, Jason Cong, Yufei Ding, Bill Fefferman, Moinuddin Qureshi, Gokul Subramanian Ravi, Kaitlin N. Smith, Hanrui Wang, Xiaodi Wu, Henry Yuen.
Available at https://arxiv.org/abs/2601.20247

2025

P4. A complexity theory for non-local quantum computation.
Andreas Bluhm, Simon Höfer, Alex May, Mikka Stasiuk, Philip Verduyn Lunel, Henry Yuen.
Available at https://arxiv.org/abs/2505.23893

2020

P5. $\mathsf{MIP}^* = \mathsf{RE}$.
Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, Henry Yuen.
Under review.
Available at https://arxiv.org/abs/2001.04383

P6. Quantum soundness of the classical low-individual degree test.
Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, Henry Yuen.
Available at https://arxiv.org/abs/2009.12982

P7. Quantum statistical query learning.
Srinivasan Arunachalam, Alex B. Grilo, Henry Yuen.
Available at https://arxiv.org/abs/2002.08240

2016

P8. Raz-McKenzie simulation with the inner product gadget.
Xiaodi Wu, Penghui Yao, Henry Yuen.
Electronic Colloquium on Computational Complexity 17-010.
Available at https://eccc.weizmann.ac.il/report/2017/010/

P9. A simple proof of Renner's exponential de Finetti theorem.
Thomas Vidick, Henry Yuen.
Available at https://arxiv.org/abs/1608.04814

Talks

2025 *Private proofs of when and where*
Kyoto Quantum Crypto Workshop.

Quantum Position Verification: From Cryptography to Complexity to Quantum Gravity
Stevens Institute of Technology Physics Seminar.

The power and limits of constant-time quantum computation
KITP workshop on Quantum many-body physics through the lens of quantum error-correction.
Clay Math Workshop on P vs NP and Complexity Lower Bounds.

Quantum Cryptography: From Quantum Money to Quantum Gravity
UNESCO International Year of Quantum Symposium.
Columbia Qiskit Fall Fest.

Myths and Realities of Quantum Computing
Columbia Faculty Spotlight at Orientation.
Columbia Business School BRITE Conference.
Columbia Engineering Reunion.

Beyond the lightcone argument in quantum circuit complexty
Princeton CS Theory Seminar.

The Hardness of Learning Quantum Circuits and its Cryptographic Applications
Harvard Quantum Initiative Colloquium.

QMA vs. QCMA and Pseudorandomness
Cornell CS Theory Seminar.

2024

QMA vs. QCMA and Pseudorandomness
IAS Computer Science and Discrete Mathematics Seminar.

The Hardness of Learning Quantum Circuits and its Cryptographic Applications
Yale Quantum Institute Colloquium.
NY Quantum Day 2.

On the Pauli Spectrum of QAC0
Princeton Quantum Technology Conference 2024.

Towards a Complexity Theory for Fully Quantum Problems
Institute for Advanced Study Workshop on Quantum Physics and Information.
University of Arkansas Quantum Seminar.

New developments in quantum pseudorandomness
International Congress of Mathematical Physics 2024.

Some Thoughts on Quantum Complexity Theory, Then and Now
UmeshFest (Simons Institute).

A Tale of Turing Machines, Quantum-Entangled Particles, and Operator Algebras
Nelson Lecture at McMaster University.

Aspects of pseudorandom unitaries, and a construction
Quantum pseudorandomness workshop at the Simons Institute.

Towards a Complexity Theory for the Quantum Age
MIT CS Theory Colloquium.
Harvard Quantum Seminar.

2023 *On the Pauli Spectrum of QAC0*
IBM Quantum Technical Talk.

The Compression Paradigm, and Parallel Repetition
Simons-Laufer Mathematical Sciences Institute Workshop on MIP* = RE.

A Complexity Theory for the Quantum Age?
UC Berkeley Theory Lunch.
University of Maryland, QuICS Seminar.
NYU CS Theory Seminar.
Eastern Great Lakes Theory of Computation Workshop.
University of Ottawa QUASAR Seminar.
NYU Quantum Summit.

Efficient, stable presentations from error-correcting codes

Fields Institute Workshop on Operator Algebras and Applications.

Quantum Pseudorandom States
QCrypt 2023 Invited Tutorial.

Unitary Complexity and the Uhlmann Transformation Problem
Princeton University CS Theory Lunch.

When do we get quantum advantage?
Panel discussion at Columbia Physics Colloquium.

A Tale of Turing Machines, Quantum Entanglement, and Operator Algebras.
Plenary talk at ITA 2023 Workshop.

Minimal assumptions for quantum cryptography.
Simons Institute Meta-Complexity Seminar.

Noncommutative Property Testing.
UC San Diego Functional Analysis Seminar.

2022 *A complexity theory for the Quantum Age?*
Princeton Quantum Initiative Colloquium.
Center for Quantum Information and Control Conference, University of Toronto.

Cryptography from Pseudorandom Quantum States.
Illinois Quantum Information Seminar.

2021 *Noncommutative Property Testing.*
Simons Workshop on High-Dimensional Expanders.
Oberwolfach Complexity Workshop.
University of Delaware Quantum Information Seminar.

Interactive Proofs for Synthesizing Quantum States and Unitaries.
Quantum Wave Reunion Workshop, Simons Institute.

Einstein meets Turing: the computability of nonlocal games. (Keynote talk)
Computability in Europe Conference.

Products of games.
American Institute of Mathematics, Nonlocal Games Workshop.

The role of proofs in $\mathsf{MIP}^* = \mathsf{RE}$.
Quantum Information for Mathematics, Economics, and Statistics Workshop.
Simons Quantum Colloquium.

Low-Degree Testing in the Noncommutative Setting.
Global Noncommutative Geometry Seminar.

Quantum Garbled Circuits.
QuSoft seminar (CWI).
Ben-Gurion University Computer Science Seminar.
UC Berkeley Crypto Seminar.

A Tale of Turing Machines, Quantum-Entangled Particles, and Operator Algebras.
USC CS Theory Lunch.
Canada Quantum Days Keynote.

2020 *A Tale of Turing Machines, Quantum-Entangled Particles, and Operator Algebras.*
Richard M. Karp Distinguished Lecture.
University of Toronto Computer Science Distinguished Lecture Series.
Machine Learning in Science and Engineering (organized by Columbia Data Science Institute).

Quantum entanglement through the computational lens
University of Washington.
Columbia University.

MIP* = RE
Canadian Operator Symposium.
Perimeter Institute Seminar.
University of Ottawa CRM Distinguished Speaker Colloquium.
UT Austin Groups & Dynamics seminar.
TCS+ (online).
Institute for Advanced Study (Princeton, New Jersey).
Fields Institute Set Theory Seminar (Toronto, Canada).

Multiprover protocols
Quantum Wave Bootcamp workshop (Berkeley, California).

Perfect zero knowledge for quantum multiprover interactive proofs
Quantum Information Processing 2020 conference (Shenzhen, China).

2019 *Connes' Embedding Problem through the lens of complexity theory*
QLA meets QIT workshop at Purdue University (West Lafayette, Indiana).
University of Waterloo Pure Math Colloquium (Waterloo, Ontario).

Perfect zero knowledge for quantum multiprover interactive proofs
MIT Cryptography and Information Seminar (Cambridge, Massachusetts).

Quantum proof systems for iterated exponential time, and beyond

BIRS Workshop on the Many Faceted Connes Embedding Problem (Banff, Alberta).
Symposium on Theory of Computing (STOC) 2019 conference (Phoenix, Arizona).
Quantum Information Processing (QIP) 2019 conference (Boulder, Colorado).

Circuit Hamiltonians, Hamiltonian complexity, and approximate error correction.
Perimeter Institute Quantum Information Seminar (Waterloo, Ontario).

2018 *Quantum proof systems for iterated exponential time, and beyond*
Theoretical Computer Science seminar, University of Texas, Austin.
Institute for Quantum Computing Colloqiuium, University of Waterloo.
QuICS seminar, University of Maryland.

Quantum Computing: Our Journey So Far
Trinity College, University of Toronto.

Noise-tolerant testing of high entanglement of formation
International Colloquium on Automata, Languages, and Programming (ICALP) 2018
(Prague, Czech Republic).

Approximate low-weight check codes and circuit lower bounds for noisy ground states.
International Colloquium on Automata, Languages, and Programming (ICALP) 2018 conference (Prague, Czech Republic).
Workshop on Quantum Algorithms and Complexity Theory, Center for Quantum Technologies, Singapore.

2017 *Noise-tolerant testing of high-dimensional entanglement.*
Invited speaker to Asian Quantum Information Science (AQIS) 2017 conference (Singapore)
Centre for Quantum Information and Control (CQIQC) seminar (Toronto, Canada)

Parallel repetition for entangled games.
Innovations in Theoretical Computer Science (ITCS) 2017 conference (Berkeley, CA)
Symposium on Theory of Computing (STOC) 2017 conference (Montreal, Canada)

2016 *Quantum parallel repetition with polynomial decay.*
Joint Center for Quantum Information and Computer Science (College Park, Maryland)
ICALP conference (Rome, Italy)
Quantum Information Processing (QIP) 2017 conference (Seattle, WA)

Anchoring games for parallel repetition.
Caltech IQIM seminar (Pasadena, CA)
Quantum Information Processing (QIP) 2016 conference (Banff, Canada)

Hebrew University Quantum seminar (Jerusalem, Israel)
Weizmann Institute of Science (Rehovot, Israel)
NYU Theory Seminar (New York, NY)

2015 *Parallel repetition for entangled free games.*
MIT Algorithms and Complexity Seminar (Cambridge, MA)
Simons Institute Workshop on Information Theory in Complexity and Combinatorics (Berkeley, CA)
CWI Seminar (Amsterdam, Netherlands)
Computational Complexity Conference 2015 (Portland, OR)
Caltech IQIM Group Meeting (Pasadena, CA).

Infinite randomness expansion.
Princeton CS Theory Group Meeting (Princeton, NJ)
Foundations of Randomness Workshop (Stellenbosch Institute of Advanced Study, Stellenbosch, South Africa)

2014 *Infinite randomness expansion.*
Simons Institute Quantum Gathering seminar, Simons Institute Quantum Games Workshop (Berkeley, CA)
Symposium on the Theory of Computing (STOC) 2014 conference (New York, NY)
CWI Seminar (Amsterdam, Netherlands)
MIT Quantum Computing Group Meeting (Cambridge, MA).

Advisees

PhD

Leo Orshansky (co-advised with Tal Malkin. Fall 2024 -)

Saachi Mutreja (Fall 2023 -)

Natalie Parham (Fall 2022 -)

John Bostanci (Fall 2022 -)

Hamoon Mousavi (Spring 2019 - Summer 2023,
Current position: Postdoc at UC Berkeley
Thesis: *Some Aspects of Noncommutativity in Polynomial Optimization*)

Adrian She (Spring 2019 - Summer 2024, University of Toronto,
co-advised with Toni Pitassi
Current Position: Lecturer at University of Toronto
Thesis: *Algebraic Methods in Query and Proof Complexity.*)

Gregory Rosenthal (Spring 2020 - Summer 2023, University of Toronto,
co-advised with Ben Rossman,
Current position: Postdoc at Institute for Quantum Computing, U. Waterloo
Thesis: *Quantum State and Unitary Complexity*).

Arthur Mehta (Spring 2019 - Spring 2021, Ph.D. Math, University of Toronto.
Current Position: Assistant Professor at University of Ottawa,
Thesis: *Entanglement and non-locality in games and graphs*).

Postdoc

Barak Nehoran (Fall 2025 -)

Uma Girish (Fall 2024 - Summer 2026.
Next position: Assistant Professor at University of Toronto).

Cunlu Zhou (University of Toronto, Fall 2019 - Summer 2021.
Current Position: Assistant Professor at Université de Sherbrooke).

Undergrad

Akshat Yaparla, Ryan Anselm
Yulong Li (Summer 2021), Thomas Chen (Spring 2022), Zihan Hu (2022)
Smik Patel (Summer 2020), Hugh Goatcher (Summer 2020), David Cui (2019),
Sajjad Nezhadi (2019), Yvette De Sereville (Fall 2019)

Other Thesis Committees

Vahid Asadi (Ph.D. C&O 2026, University of Waterloo)
Chuhan Lu (Ph.D. CS 2025, Portland State University)
Jeremy Johnston (Ph.D. EE 2025, Columbia University)
Marcel Dall'Agnol (Ph.D. CS 2023, University of Warwick)
Ian Mertz (Ph.D. CS 2022, University of Toronto)
Mihai Albiou (Ph.D. Math 2021, University of Toronto)

Teaching

Spring 2026 COMS 6998: Machine-Assisted Mathematics

Fall 2025 COMS 4281 Introduction to Quantum Computing
Enrollment: 82
Evaluations: Overall course quality (4.52/5), Instructor quality (4.65/5)
Response Rate: (31/82)

Fall 2024 COMS 4281 Introduction to Quantum Computing
Enrollment: 109
Evaluations: Overall course quality (4.03/5), Instructor quality (4.20/5)
Response Rate: (40/109)

Fall 2023 COMS 4281 Introduction to Quantum Computing
Enrollment: 69
Evaluations: Overall course quality (4.20/5), Instructor quality (4.52/5)
Response Rate: (25/69)

COMS 4236 Introduction to Computational Complexity
Enrollment: 25
Evaluations: Overall course quality (4.25/5), Instructor quality (5/5)
Response Rate: (12/25)

Fall 2022 COMS 4281 Introduction to Quantum Computing
Enrollment: 53
Evaluations: Overall course quality (4.48/5), Instructor quality (4.71/5)
Response Rate: (22/53)

Spring 2022 COMS 6998 Frontiers of Quantum Complexity and Cryptography
Enrollment: 17
Evaluations: Overall course quality (4.83/5), Instructor quality (5/5)
Response Rate: (6/17)

Spring 2021

COMS 4281 Introduction to Quantum Computing
Enrollment: 64
Evaluations: Overall course quality (4.32/5), Instructor quality (4.36/5)
Response Rate: (24/64)

Courses prior to Spring 2021 were taught at University of Toronto.

Fall 2020 CSC2429/MAT1752 Advanced Topics in Quantum Information Theory
Enrollment: 20
Evaluations: Overall course quality (4.7/5)

Fall 2019 MAT344 Introduction to Combinatorics
Enrollment: 155
Evaluations: Overall course quality (4.1/5)

CSC2451/MAT1751 Quantum Computing: Foundations to Frontier
Enrollment: 44
Evaluations: Overall course quality (4.6/5)

Winter 2019 MAT344 Introduction to Combinatorics (Undergraduate)

Fall 2018 CSC2451/MAT1751 Quantum Computing: Foundations to Frontier (Graduate)

Spring 2015 Graduate Instructor in Advanced Complexity Theory, MIT.

Service

University/departmental service

2023 - PhD Admissions Vice-Chair.

2021 - Computer Science Masters Program Advisor (Machine Learning/Foundations Track).
Columbia Quantum Initiative Distinguished Lecture Series organizer.
Columbia CS Theory Seminar organizer.

2021, 2022 PhD Fellowships committee.

Service prior to Spring 2021 was performed at University of Toronto.

2018 - 2020 Computer Science/Mathematics faculty search committee at University of Toronto.
International liaison committee.
Undergraduate research experience committee.

Quantum Information faculty search committee.
Working group on graduate admissions.
Undergraduate Curriculum Committee.

Workshop/conference organization

2025 Co-organizer of the Banff International Research Station workshop on Quantum Cryptography.

2024 Co-organizer of New York City Quantum Day.

2023 Co-organizer of the Simons Laufer Mathematical Sciences Institute (SLMSI) Hot Topics workshop on MIP* = RE.

2023 Workshop & Tutorial Co-chair for Foundations of Computer Science (FOCS) conference.

2021 Co-organizer of the *Summer Cluster in Quantum Computation* program at the Simons Institute in 2021.

2020 Chair organizer of the *Quantum Protocols: Testing & PCPs* workshop at the Simons Institute *The Quantum Wave in Computing* program in 2020.

2019 Main lecturer of the 5-day *Eighteenth Bellair's Crypto Workshop 2019* on "Applications of non-local games to quantum complexity and quantum cryptography".

Program committees

Quantum Information Processing (QIP) 2026 (Subject chair)
Innovations in Theoretical Computer Science (ITCS) 2026
Symposium on Theory of Computing (STOC) 2025
QCrypt 2024
Quantum Information Processing (QIP) 2024
International Colloquium on Automata, Languages, and Programs (ICALP) 2023
Innovations in Theoretical Computer Science (ITCS) 2023
Computational Complexity Conference (CCC) 2021
Quantum Information Processing (QIP) 2021
Quantum Information Processing (QIP) 2020
Symposium on Theory of Computing (STOC) 2020
Theory of Quantum Computing (TQC) 2018
Computational Complexity Conference (CCC) 2018
Innovations in Theoretical Computer Science (ITCS) 2017