

Henry Yuen

Assistant Professor of Computer Science
Columbia University

Phone: 212-853-8476

Email: hyuen@cs.columbia.edu

Homepage: henryyuen.net

Areas of specialization

Quantum computing, quantum information theory, cryptography, complexity theory.

Appointments held

- 2021 – 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

Grants

- 2022 – 2024 Sloan Research Fellowship (USD 75,000)
- 2022 – 2027 NSF CAREER Award (USD 675,000)
- 2020 – 2023 Air Force Office of Scientific Research Grant (USD 390,000)
- 2019 Google Quantum Research Award (USD 100,000)
- 2019 – 2024 NSERC Discovery Grant (CAD 115,000)

Honors & Awards

- 2022 Sloan Research Fellow.
- 2022 “Nonlocal Games, Compression Theorems, and the Arithmetical Hierarchy” invited as a Plenary Talk at *Quantum Information Processing (QIP) 2022*.

- 2020 Simons-Berkeley Research Fellowship.
- 2017 “Multiplayer parallel repetition for expander games” designated Invited Talk at *Innovations in Theoretical Computer Science (ITCS) 2017*.
- 2016 “Anchoring games for parallel repetition” invited as a Plenary Talk at *Quantum Information Processing (QIP) 2016*.
- 2015 – 2017 Simons Graduate Fellowship for Theoretical Computer Science
- 2012 – 2015 NSF Graduate Fellowship
- 2011 MIT Presidential Fellowship

Publications

Preprints

- 2021 Cryptography from Pseudorandom Quantum States.
Prabhanjan Ananth, Luowen Qian, Henry Yuen.
Available at <https://arxiv.org/abs/2112.10020>
- Quantum search-to-decision reductions and the state synthesis problem.
Sandy Irani, Anand Natarajan, Chinmay Nirkhe, Sujit Rao, Henry Yuen.
Presented at *Quantum Information Processing (QIP) 2022*.
Available at <https://arxiv.org/abs/2111.02999>
- 2020 Rigidity of superdense coding.
Ashwin Nayak, Henry Yuen.
Submitted.
Available at <https://arxiv.org/abs/2012.01672>
- MIP* = RE.
Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, Henry Yuen.
Submitted to *Annals of Mathematics*.
Available at <https://arxiv.org/abs/2001.04383>

Conference proceedings

- 2022 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>
- 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>

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

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

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

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*.

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*.

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

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*.

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 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*.
- 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*.
- 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.
Presented as Invited Talk at ITCS 2017.
- 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 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*.
- 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.
- 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 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 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 Robust Randomness Amplifiers: Upper and Lower Bounds
 Matthew Coudron, Thomas Vidick, and Henry Yuen.

In proceedings of *APPROX-RANDOM 2013*, pp. 468–483.

- 2012 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

- 2021 Anchored parallel repetition for nonlocal games.
Mohammad Bavarian, Thomas Vidick, and Henry Yuen.
To appear in *SIAM Journal on Computing*.
- 2020 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*.
Available at <https://arxiv.org/abs/2008.02941>
- 2016 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.
- 2014 A quantum lower bound for distinguishing random functions from random permutations.
Henry Yuen.
In *Quantum Information and Computation*, 14(9-10), 2014.
- 2010 DNA Sequencing via Data Mining and Quantum Mechanics.
Henry Yuen, Fuyuki Shimojo, Kevin Zhang, Aiichiro Nakano, Kenichi Nomura, Priya Vashishta.
In *International Journal of Computational Science*, Vol. 4, No. 4, 2010.

Manuscripts

- 2020 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>
- Quantum statistical query learning.
Srinivasan Arunachalam, Alex B. Grilo, Henry Yuen.
Manuscript.
Available at <https://arxiv.org/abs/2002.08240>

2016

Raz-McKenzie simulation with the inner product gadget.
Xiaodi Wu, Penghui Yao, Henry Yuen.
Electronic Colloquium on Computational Complexity Technical Report 17-010.

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

Talks

2022

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 $MIP^ = RE$.*
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 Colloquium, 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 Tech-
nologies, Singapore.

2017 *Noise-tolerant testing of high-dimensional entanglement.*
Invited speaker to Asian Quantum Information Science (AQIS) 2017 conference (Sin-
gapore)
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, Mary-
land)
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).

Advising

Postdoc Cunlu Zhou (2019 - 2021. Now postdoctoral fellow at University of New Mexico).

PhD Hamoon Mousavi (CS, Columbia University)
Gregory Rosenthal (CS, University of Toronto, *co-advised with Ben Rossman*).
Adrian She (Math, University of Toronto, *co-advised with Toni Pitassi*).
Arthur Mehta (Ph.D. Math 2021, University of Toronto. Now postdoctoral fellow at University of Ottawa)

Undergrad Yulong Li (Summer 2021)
Smik Patel (Summer 2020)
Hugh Goatcher (Summer 2020)
David Cui (2019)
Sajjad Nezhadi (2019)
Yvette De Sereville (Fall 2019)

Teaching

Spring 2022 COMS 6998 Frontiers of Quantum Complexity and Cryptography

Spring 2021 COMS 4281 Introduction to Quantum Computing (Undergraduate and Graduate)
11th BIU Winter School on Cryptography (February 14 - February 17)

Fall 2020 CSC2429/MAT1752 Advanced Topics in Quantum Information Theory (Graduate)

Fall 2019 MAT344 Introduction to Combinatorics (Undergraduate)
CSC2451/MAT1751 Quantum Computing: Foundations to Frontier (Graduate)

Winter 2019 MAT344 Introduction to Combinatorics (Undergraduate)

Fall 2018

CSC245I/MAT175I Quantum Computing: Foundations to Frontier (Graduate)

Spring 2015 Graduate Instructor in Advanced Complexity Theory, MIT.

Service

Workshop/conference organization

2021 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

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

References

Provided upon request

Last updated: February 15, 2022