Can (John) Bostanci

Phone: +1 609 977 7629
Email: johnbostanci2@gmail.com
Website: www.johnbostanci.com

Employment

July 2026 – Present	Simons Quantum Postdoctoral Fellow Simons Institute & UC Berkeley, hosted by Umesh Vazirani.

Education

2026	Ph.D. in Computer Science	Columbia University Thesis title: Quantum query complexity, with advice
2022	M.Sc. in Computer Science	University of Waterloo
2018	B.Sc. in Computer Science	Carnegie Mellon University
2018	B.Sc. in Physics	Carnegie Mellon University

Honors and Awards

2026	"Separating QMA from QCMA with a classical oracle" best paper award at STOC 2026
2025	"A General Duality for Representations of Groups with Applications to Quantum Money, Lightning, and Fire" invited plenary talk at QCrypt 2025
2025	Jane Street Graduate Research Fellowship Finalist
2025	"Learning the closest product state" short plenary talk at QIP
2024	"Unitary Complexity and the Uhlmann Transformation Problem" long plenary talk at QIP
2024	"An efficient parallel repetition theorem and applications" short plenary talk at QIP
2020	Mike and Ophelia Lazaridis Fellow at University of Waterloo
2018	Member of Phi Beta Kappa
2018	College and University Honors at CMU
2017	Ranked 295 in the William Lowell Putnam competition

Conference Papers

C1. Separating Separating Quantum and Classical Advice with Good Codes.
John Bostanci, Andrew Huang, and Vinod Vaikuntanathan.
To appear in Symposium On Foundations Of Computer Science (FOCS) 2026.
Available at `https://arxiv.org/abs/2602.09385`.

C2. Separating QMA from QCMA with a classical oracle.
John Bostanci, Jonas Haferkamp, Chinmay Nirkhe, and Mark Zhandry.
In the proceedings of Symposium on Theory of Computation (STOC) 2026, best paper award.
Available at `https://arxiv.org/abs/2511.09551`.

C3. Local transformations of bipartite entanglement are rigid.
John Bostanci, Tony Metger, and Henry Yuen.
In the proceedings of Innovations in Theoretical Computer Science (ITCS) 2026.
Presented at Quantum Information Processing (QIP) 2026.
Available at `https://arxiv.org/abs/2509.05257`.

C4. Commuting Local Hamiltonians Beyond 2D.
John Bostanci and Yeongwoo Hwang.
In the proceedings of Innovations in Theoretical Computer Science (ITCS) 2026.
Presented at Theory of Quantum Computation (TQC) 2025.
Available at `https://arxiv.org/abs/2410.10495`.

C5. Unitary Complexity and the Uhlmann Transformation Problem.
John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, Henry Yuen.
In the proceedings of Innovations in Theoretical Computer Science (ITCS) 2026.
Presented at Quantum Information Processing (QIP) 2024 as a long plenary talk.
Available at `https://arxiv.org/abs/2306.13073`.

C6. Pseudorandom Unitaries in the Haar Random Oracle Model.
Prabhanjan Ananth, John Bostanci, Aditya Gulati, and Yao-Ting Lin.
In the proceedings of Annual International Cryptology Conference (CRYPTO) 2025.
Presented at Quantum Information Processing (QIP) 2026.
Available at `https://arxiv.org/abs/2509.24432` (part 1) and `https://arxiv.org/abs/2510.04085` (part 2).

C7. Efficient Quantum Pseudorandomness from Hamiltonian Phase States.
John Bostanci, Jonas Haferkamp, Dominik Hangleiter, and Alexander Poremba.
In the proceedings of Theory of Quantum Computation (TQC) 2025.
Available at `https://arxiv.org/abs/2410.08073`.

C8. A General Duality for Representations of Groups with Applications to Quantum Money, Lightning, and Fire.
John Bostanci, Barak Nehoran, and Mark Zhandry.
In the proceedings of Symposium on Theory of Computation (STOC) 2025.
Presented at Quantum Information Processing (QIP) 2025, and Quantum Cryptography (QCrypt) 2025 as a invited plenary talk.
Available at `https://arxiv.org/abs/2411.00529`.

C9. Learning the closest product state.
Ainesh Bakshi, John Bostanci, William Kretschmer, Zeph Landau, Jerry Li, Allen Liu, Ryan O'Donnell, and Ewin Tang.
In the proceedings of Symposium on Theory of Computation (STOC) 2025.
Presented at Quantum Information Processing (QIP) 2025 as a merged short plenary talk.
Available at `https://arxiv.org/abs/2411.04283`.

C10. Oracle Separation Between Quantum Commitments and Quantum One-wayness.
John Bostanci, Boyang Chen, and Barak Nehoran.
In the proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques (EuroCrypt) 2025.
Available at `https://arxiv.org/abs/2410.03358`.

C11. Pseudorandomness in the (Inverseless) Haar Random Oracle Model.
Prabhanjan Ananth, John Bostanci, Aditya Gulati, and Yao-Ting Lin.
In the proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques (EuroCrypt) 2025.
Available at `https://arxiv.org/abs/2410.19320`.

C12. An efficient parallel repetition theorem and applications.
John Bostanci, Luowen Qian, Nick Spooner, and Henry Yuen.
In the proceedings of Symposium on Theory of Computation (STOC) 2024.
Presented at Quantum Information Processing (QIP) 2024 as a short plenary talk.
Available at `https://arxiv.org/abs/2311.10681`.

C13. Quantum Event Learning and Gentle Random Measurements/
Adam Bene Watts and John Bostanci.
In the proceedings of Innovations of Theoretical Computer Science (ITCS) 2024.
Available at `https://arxiv.org/abs/2210.09155`.

Journal Papers

J1. Quantum game theory and the complexity of approximating quantum Nash equilibria.
John Bostanci and John Watrous.
In Quantum 6, 882 (2022).
Available at `https://arxiv.org/abs/2102.00512`.

J2. Finding the disjointness of stabilizer codes is NP-complete.
John Bostanci and Aleksander Kubica.
In Physical Review Research 3, 043192 (2021).
Available at `https://arxiv.org/abs/2108.04738`.

Conference Talks

1. "Separating QMA from QCMA with a classical oracle". Best paper session talk at STOC 2026.
2. "Unitary Complexity and the Uhlmann Transformation Problem". Contributed talk at ITCS 2026.
3. "Commuting Local Hamiltonians Beyond 2D". Contributed talk at ITCS 2026.
4. "Local transformations of bipartite entanglement are rigid". Contributed talk at ITCS 2026.
5. "Local transformations of bipartite entanglement are rigid". Contributed talk at QIP 2026.
6. "Efficient Quantum Pseudorandomness from Hamiltonian Phase States". Contributed talk at TQC 2025.
7. "Learning the closest product state". Contributed talk at STOC 2025.
8. "A General Quantum Duality for Representations of Groups with Applications to Quantum Money, Lightning, and Fire". Contributed talk at STOC 2025.
9. "Oracle Separation Between Quantum Commitments and Quantum One-wayness". Contributed talk at Eurocrypt 2025.
10. "Learning the closest product state". Short plenary talk at QIP 2025.
11. "An efficient quantum parallel repetition theorem and applications". Short plenary talk at QIP 2024.
12. "Quantum event learning and gentle random measurements". Contributed talk at ITCS 2024.

Invited Talks

1. "Separating QMA from QCMA with a classical oracle". Invited talk at UT Austin (Febuary 2026).
2. "Sampling probability bounds from bosons". Invited talk at the EPFL Quantum IC seminar (January 2026).
3. "Separating QMA from QCMA with a classical oracle". Invited talk at the EPFL QSE seminar (January 2026).
4. "Separating QMA from QCMA with a classical oracle". Invited talk at the Chicago Junior Theorists Workshop (December 2025).
5. "Separating QMA from QCMA with a classical oracle". Invited talk at the Harvard Quantum Initiative (December 2025).
6. "A computational lens on quantum information". Invited talk at the Princeton Quantum Initiative (November 2025).
7. "Separating QMA from QCMA with a classical oracle". Invited talk at the Simons Institute (November 2025).
8. "Local transformations of bipartite entanglement are rigid". Invited talk at the Institute for Quantum Computing (November 2025).
9. "A General Duality for Representations of Groups with Applications to Quantum Money, Lightning, and Fire". Invited talk at the Quantum Innovators workshop (October 2025).
10. "Quantum lightning from non-Abelian group actions". Invited talk at the Kyoto quantum cryptography workshop (October 2025).
11. "Learning the closest product state". Invited talk at the Harvard Quantum Initiative (April 2025).
12. "Quantum money from non-Abelian group actions". Invited talk at the CWI QuSoft Seminar (April 2025).
13. "Quantum money from non-Abelian group actions". Invited talk at the University of Waterloo IQC Math and CS Seminar (April 2025).
14. "Quantum money from non-Abelian group actions". Invited talk at the Honghai (Foxconn) quantum computing group meeting (July 2025).
15. "Efficient Quantum Pseudorandomness from Hamiltonian Phase States". Invited talk at the University of Santa Barbara (November 2024).
16. "Unitary complexity theory and the Uhlmann transformation problem". Invited talk at the Korean Institute of Advanced Studied (KIAS) (April 2024).
17. "Unitary complexity theory and the Uhlmann transformation problem". Invited talk at Harvard University (October 2023).
18. "Unitary complexity theory and the Uhlmann transformation problem". Invited talk at the University of Chicago (June 2023).
19. "The complexity of stabilizer code disjointness". Invited talk at ORCA computing (November 2021).

Other Research Experience

2018 CMU Senior Thesis: Approximations to the Ordered Medians Problem.
2017 Deep Learning Researcher, CMU NavLab.
2016 Undergraduate Researcher, National Energy Technology Laboratory.
2015 Undergraduate Researcher, CMU Math Department.

Teaching Experience

June 2026 Lecturer, "Pseudo-random unitaries"
24th Bellairs Crypto workshop

Other Teaching Experience

Fall 2025 Columbia COMS W4281 (Introduction to Quantum Computing) teaching assistant.
Fall 2022 Columbia COMS W4281 (Introduction to Quantum Computing) teaching assistant.
Spring 2018 CMU 15-451 (Design and Analysis of Algorithms) head teaching assistant.
Fall 2017 CMU 15-451 (Design and Analysis of Algorithms) teaching assistant.
Spring 2017 CMU 15-210 (Parallel and Sequential Data Structures and Algorithms) teaching assistant.
Fall 2016 CMU 15-210 (Parallel and Sequential Data Structures and Algorithms) teaching assistant.
Fall 2015 CMU 33-106 (Physics I for Engineering Students) teaching assistant assistant

Other Experience

May 2024 – Aug. 2024 Research Intern @ NTT Research CIS Labs.
Aug. 2020 – Jan. 2023 Senior Software Engineer @ Kalshi.
Jun. 2017 – Jan. 2020 Quantitative Research Engineer @ Citadel.