

# Rahul Jain

**Position** Professor, Department of Computer Science and Principal Investigator, Centre for Quantum Technologies National University of Singapore

**Contact Information** Address: S15-04-01, 3 Science Drive 2, Singapore 117543.  
Email: [rahul@comp.nus.edu.sg](mailto:rahul@comp.nus.edu.sg)  
Homepage: <https://www.comp.nus.edu.sg/~rahul>

## Education

Ph.D. (Computer Science), Tata Institute of Fundamental Research, Mumbai 400005, India, 1998-2003.  
B.Tech. (Electrical and Electronics Engineering), Indian Institute of Technology, Mumbai, India, 1993-1997.

**Research Interests** Quantum Algorithms, Information Theory, Complexity Theory, Cryptography.

## Past Professional Experience

1. Associate Professor, Department of Computer Science, and Principal Investigator, Centre for Quantum Technologies, National University of Singapore. July 2013 - December 2019.
2. Assistant Professor, Department of Computer Science, and Principal Investigator, Centre for Quantum Technologies, National University of Singapore. November 2008 - June 2013.
3. “VAJRA” Adjunct Faculty, Tata Institute of Fundamental Research, Mumbai, India. 2018.
4. Visiting Scientist, SIMONS Institute for the Theory of Computing, Berkeley, USA. Spring 2014, Spring 2015.
5. Visiting Professor, CNRS, Paris. Spring 2015.
6. Postdoctoral research fellow, Computer Science Department and Institute for Quantum Computing, University of Waterloo, ON, Canada. May 2006 - October 2008.
7. Postdoctoral research fellow, Computer Science Department of University of California at Berkeley, California, USA. September 2004 - April 2006.
8. Algorithms Consultant, Cadence Design Systems, NOIDA, U.P. India. January 2004 - August 2004.
9. Software Engineer, Verifone India Private Limited, Bangalore, India. August 1997 - July 1998.

## Awards

1. *VAJRA Faculty Scheme Award*, Department of Science and Technology, Govt. of India, 2017
2. *Best of Computing*, ACM Computing Reviews, 2016.
3. *Young Researcher Award*, National University of Singapore, 2012.
4. *Best Paper Award*, 42nd ACM Symposium on Theory of Computing (STOC), 2010.
5. *IBM Distinguished Dissertation Award*, 2005.
6. *TAA-Sasken Best Thesis Award*, 2005.

Cont'd

## **International Service**

### **Editorial Membership**

1. Associate Editor, Journal of Computer and System Sciences (JCSS), May 2016 onward.
2. Guest Editor, Journal on Selected Areas in Information Theory (JSAIT), Special Issue on Quantum Information Science, 2019.
3. Guest Editor, Information and Computation; Special Issue on the conference Theory and Applications of Models of Computation, 2017.

### **Program Committee Membership**

1. Innovations in Theoretical Computer Science (ITCS), 2025.
2. IEEE Symposium on Foundations of Computer Science (FOCS), 2022.
3. IEEE International Symposium on Information Theory (ISIT), 2021.
4. International Conference on Quantum Cryptography (QCrypt), 2020.
5. ACM Symposium on Theory of Computing (STOC), 2020.
6. Conference on Quantum Information Processing (QIP), 2022, 2018, 2016, 2014.
7. IARCS annual conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS), 2017, 2012.
8. Conference on the Theory of Quantum Communications, Computation and Cryptography (TQC), 2021, 2019, 2018, 2017, 2010.
9. International Colloquium on Automata, Languages and Programming (ICALP), 2016.
10. International Symposium on Theoretical Aspects of Computer Science (STACS), 2016.
11. Conference on Theory and Applications of Models of Computation (TAMC), 2016, 2015 (co-Chair), 2013.
12. International Symposium on Algorithms and Computation (ISAAC), 2014.

## **Internal Service and Outreach**

1. Member, Faculty Hiring Committee, Department of Computer Science, NUS, 2025.
2. Member, Faculty Promotion and Tenure Committee (FPTC), School of Computing, NUS, 2024-25.
3. Chair, Academic Committee at the Centre for Quantum Technologies (CQT), 2023-24.
4. Member, Department Evaluation Committee (DEC) for Promotion and Tenure (P&T), Department of Computer Science, NUS, 2023, 2022, 2020 (Chair), 2016.
5. Member, Department Evaluation Committee (DEC) for Promotion and Tenure (P&T), Department of Electrical Engineering, NUS, 2022.
6. Member, Hiring Committee, Centre for Quantum Technologies (CQT), 2022.
7. Member, Quantum SG Committee (<https://quantumsg.org/>), 2019 onward.

Cont'd

8. Chair, Mid-Term Advisory Report (MTAR) Committee for Promotion and Tenure (P&T), 2019.
9. Member, IT Committee at the Centre for Quantum Technologies (CQT), January 2009-2022.
10. Member, Academic Committee at the Centre for Quantum Technologies (CQT), 2009-2021.
11. International Judge, Singapore International Mathematics Challenge. Singapore, 2022, 2016.
12. Participant and speaker at the SoC-Vietnam Workshop. Vietnam. 2012.
13. Participant in NUS Openhouse, 2010-2017.

## **Organization**

1. Workshop on “Quantum Algorithms and Complexity Theory”. Singapore. February-March 2018.
2. The 17th Asian Quantum Information Science Conference (AQIS). Singapore. September 2017.
3. IMS workshop on “Semidefinite and Matrix Methods for Optimization and Communication”. Singapore. January-February 2016.
4. “Shannon Centenary Symposium”. Singapore. May 2016.
5. The 12th Annual Conference on Theory and Applications of Models of Computation (TAMC). Singapore. May 2015.
6. The 9th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC). Singapore. May 2014.
7. 14th Annual Workshop on Quantum Information Processing (QIP). Singapore. January 2011.
8. Workshop on “Quantum Algorithms and Complexity Theory”. Singapore. November 2008.

## **Grants**

1. NRF2021-QEP2-02-P05 grant. “Computer science approaches to quantum computing for finance.” Amount SGD 300,000 (co-PI). Duration 2022-2025.
2. Centre for Quantum Technologies core grants. Amount SGD 2,800,000 (PI). Duration 2009-2024.
3. NRF-ANR (Singapore-France) joint grant “VanQuTe”. Amount SGD 130,000 (co-PI). Duration 2018-2020.
4. MOE Tier 3 Grant. Amount SGD 295,000 (co-PI). Duration May2013-Apr2018.
5. Young Researcher Award (YRA), National University of Singapore. Amount SGD 10,000 (PI). Duration May2012-May2015.
6. “STIC-ASIE / ICT-ASIA PROJECTS” grant. Amount Euros 10,000 (co-PI). Duration 2009-2012.

Cont'd

## Teaching

1. CS4268 “Quantum Computing”, Spring 2019, 2020, 2021, 2022, 2023.
2. CS3236, “Introduction to Information Theory”, Spring 2018, 2025.
3. CS6234, “Advanced Algorithms”, Spring 2012, 2013, 2014, 2016, 2017.
4. CS3230, “Design and Analysis of Algorithms”, Fall 2011, 2012, 2014, 2023.
5. CS6209, “Topics in Cryptography”, Spring 2011.
6. CS3231, “Theory of Computation”, Fall 2010, Spring 2010.
7. CS6285, “Foundations of Cryptography”, Spring 2009.
8. QT5198, seminar module offered in the Centre for Quantum Technologies, Spring 2009.
9. CS3230-R, “Design and Analysis of Algorithms-Research”, Spring 2011, Spring 2012, Spring 2013.
10. Linear Algebra, University of Waterloo, Spring 2006.

## Supervision

### 1. Graduate students:

- (a) Yaonan Zhang, Zhili Chen (2024 onward), Rishabh Batra (2021 onward).
- (b) Upendra Kapshikar (2019=2024). Research fellow at the University of Ottawa.
- (c) Naresh B. Goud (2018-2022).
  - i. Applied Research Lead (Quantum Cryptography), JPMorgan Chase, Singapore.
  - ii. Previously a research fellow at the Cryptography and Information Security Laboratories (CIS Lab), NTT Research, USA.
- (d) Srijita Kundu (2017-2021). Research fellow at the Institute for Quantum Computing (IQC), University of Waterloo, Canada.
- (e) Anurag Anshu (2013-2018).
  - i. Assistant Professor, Harvard University, USA.
  - ii. Previously a research fellow at U.C Berkeley, USA. and the Institute for Quantum Computing (IQC), University of Waterloo, Canada.
  - iii. Recipient of Dean’s Graduate Research Excellence Award, School of Computing, NUS, 2017.
- (f) Priyanka Mukhopadhyay (2013-2018). Research fellow at the University of Toronto, Canada; previously a research fellow at the Institute for Quantum Computing (IQC), University of Waterloo, Canada.
- (g) Attila Pereszlényi (2010-2015).
  - i. Associate Software Developer, Morgan Stanley, Budapest, Hungary.
  - ii. Previously a research fellow at SZTAKI (Institute for Computer Science and Control), Budapest, Hungary and IRIF (Institut de Recherche en Informatique Fondamentale), Paris, France.
- (h) Penghui Yao (2009-2013).
  - i. Assistant Professor, Nanjing University, China.
  - ii. Recipient of the “Thousand Talents Award” by Chinese Government (<http://www.1000plan.org/en/>).

Cont’d

- iii. Previously a “Hartree Postdoctoral Fellow” at the University of Maryland, at IQC, University of Waterloo, Canada, and at CWI, Amsterdam, Netherlands.
  - iv. Recipient of Research Achievement Award, School of Computing, NUS, 2012.
2. Undergraduate students:
- (a) Neil Mehta, Chia Jiahua, Boo Ming Hui, Ernest Ong Yuheng, Cheng Jin Ting (FYP 2019-20).
  - (b) Lim Zhimming and Liu Yuheng, Soh Jiong Hao (FYP 2018-19): Recipient of the I&E Practicum@SoC Award by School of Computing, NUS.  
(<https://www.comp.nus.edu.sg/entrepreneurship/awards/iepsoc/>)
  - (c) Venkatesan Harish (FYP 2017-18): Qualified to receive the NUS Alumni Start-up Catalyst (NASC) Award by NUS Enterprise.  
<https://enterprise.nus.edu.sg/entrepreneurial-support/start-up-runway/services-and-support/nus-alumni-start-up-catalyst>
  - (d) Utkarsh Jain, Eric Siu Zi Feng, Vu Dinh Quang Dat (FYP 2017-18).
  - (e) Zhou Jun (UROP 2012-13).
3. Several interns from various IITs in India and other institutes worldwide.

### **Selected invited talks**

- 1. International Conference on Signal Processing and Communications (SPCOM). Indian Institute of Science (IISc), Bangalore, India, July 2024.
- 2. Workshop on “Quantum Information and Quantum Communication”. Indian Institute of Technology Madras (IITM), Chennai, India, February 2024.
- 3. NII Shonan Meeting, “New Directions in Provable Quantum Advantages”, Shonan Village Center, Japan, December 2023.
- 4. Israel Quantum Information Theory Day. Weizmann Institute of Science, Israel, December 2022.
- 5. Workshop on “Sensitivity, Query Complexity, Communication Complexity and Fourier Analysis of Boolean Function”. Indian Statistical Institute (ISI), Kolkata, India, February 2020.
- 6. TCS Research and Innovation Quantum Computing Symposium. I.I.T Mumbai, India, 2019.
- 7. International Conference on Signal Processing and Communications (SPCOM). Indian Institute of Science (IISc), Bangalore, India, July 2018.
- 8. Bombay Information Theory Seminar. Mumbai, India, January 2018.
- 9. Conference on “Quantum Information Theory”. The Henri Poincaré Institute, Paris, France, December 2017.
- 10. BIRS workshop on “Communication Complexity and Applications, I, II, III”. Canada, August 2014; March 2017; July, 2022.
- 11. Workshop on “Perspectives on Complexity Theory and Cryptography”. National Mathematics Initiative (NMI), Indian Institute of Science (IISc), Bangalore, India, January 2017.
- 12. International workshop on Trustworthy Quantum Information. China, July 2016.
- 13. IEEE Information Theory Workshop (ITW). South Korea, October 2015.

Cont’d

14. Satellite meeting on “Quantum Correlation and its application in communication and cryptography”, Indian Statistical Institute (ISI), Kolkata. September, 2013.
15. ELC Tokyo Complexity Workshop. Japan, March 2013.
16. Workshop on “Recent progress in quantum algorithms”. Institute of Quantum Computing (IQC), University of Waterloo, Canada, April 2012.
17. The 2nd Annual Mysore Park Workshop in Theoretical Computer. India. May 2011.
18. Annual conference on Quantum Information Processing (QIP). Switzerland, January 2010.
19. Microsoft Research. India. May 2009.
20. The 6th Regional Seminar of the ICT-Asia Programme. Thailand, February 2009.
21. Workshop on “Quantum Information Processing”, Institute of Quantum Computing, University of Waterloo, Canada, November, 2003.
22. Workshop on “Quantum Information Processing”, Centrum voor Wiskunde en Informatica (CWI), Amsterdam, Netherlands, June, 2003.

### Journal publications

1. Rishabh Batra, Naresh Goud Boddu, Rahul Jain. “Quantum secure non-malleable randomness encoder and its application.” IEEE Transactions on Information Theory (IEEE-TIT), 2025.
2. Naresh Goud Boddu, Vipul Goyal, Rahul Jain, João Ribeiro. “Split-state non-malleable codes and secret sharing schemes for quantum messages.” IEEE Transactions on Information Theory (IEEE-TIT), 2025.
3. Divesh Aggarwal, Naresh Goud Boddu, Rahul Jain. “Quantum secure non-malleable-codes in the split-state model.” IEEE Transactions on Information Theory (IEEE-TIT), pp. 349-371, Volume: 70, Issue: 1, 2024
4. Divesh Aggarwal, Naresh Goud Boddu, Rahul Jain, Maciej Obremski. “Quantum Measurement Adversary.” IEEE Transactions on Information Theory (IEEE-TIT), pp. 318-335, Volume: 70, Issue: 1, 2024.
5. Anurag Anshu, Shima Bab Hadiashar, Rahul Jain, Ashwin Nayak, Dave Touchette. “One-shot quantum state redistribution and quantum Markov chains”. IEEE Transactions on Information Theory (IEEE-TIT), Volume: 69, Issue: 9, pages 5788-5804, May 2023.
6. Naresh Goud Boddu, Rahul Jain, Han-Hsuan Lin. “On relating one-way classical and quantum communication complexities.” Quantum 7, 1010, May, 2023.
7. Anurag Anshu, Rahul Jain. “Quantum decoupling via efficient ‘classical’ operations and the entanglement cost of one-shot quantum protocols.” Nature Physics Journal Quantum Information (npj QI), 8, Article number: 97, 2022.
8. Anurag Anshu, Min-Hsiu Hsieh and Rahul Jain. “Noisy quantum state redistribution with promise and the Alpha-bit.” IEEE Transactions on Information Theory (IEEE-TIT), pp 7772-7786, Volume: 66, Issue: 12, December 2020.
9. Rahul Jain, Carl A. Miller and Yaoyun Shi. “Parallel device-independent quantum key distribution.” IEEE Transactions on Information Theory (IEEE-TIT), Volume: 66, Issue: 9, pages 5567-5584, September 2020.

Cont’d

10. Anurag Anshu, Mario Berta, Rahul Jain, Marco Tomamichel. “Partially smoothed information measures.” *IEEE Transactions on Information Theory (IEEE-TIT)*, Volume: 66, Issue: 8, pages 5022-5036, August 2020.
11. Farzin Salek, Anurag Anshu, Min-Hsiu Hsieh, Rahul Jain, Javier R. Fonollos. “One-shot Capacity bounds on the Simultaneous Transmission of Classical and Quantum Information.” *IEEE Transactions on Information Theory (IEEE-TIT)*, Volume: 66, Issue: 4, pages 2141-2164, April 2020.
12. Anurag Anshu, Mario Berta, Rahul Jain, Marco Tomamichel. “A minimax approach to one-shot entropy inequalities.” *Journal of Mathematical Physics (JMP)*, Volume: 60, Issue:12, 2019.
13. Rahul Jain, Hartmut Klauck, Srijita Kundu, Troy Lee, Miklos Santha, Swagato Sanyal, Jevgēnijs Vihrovs. “Quadratically Tight Relations for Randomized Query Complexity.” *Theory of Computing Systems*, Volume 64, pages 101–119, 2020. **Invited to the Topical Collection on Computer Science Symposium in Russia (2018).**
14. Anurag Anshu, Rahul Jain, Naqeeb Ahmad Warsi. “On the near-optimality of one-shot classical communication over quantum channels.” *Journal of Mathematical Physics (JMP)*, Vol.60, Issue 1, 2019.
15. Anurag Anshu, Rahul Jain and Naqeeb Ahmad Warsi. “Convex-split and hypothesis testing approach to one-shot quantum measurement compression and randomness extraction.” *IEEE Transactions on Information Theory (IEEE-TIT)*, Volume: 65, Issue: 9, Sept. 2019.
16. Anurag Anshu, Rahul Jain and Naqeeb A. Warsi. “A hypothesis testing approach for communication over entanglement assisted compound quantum channel”. *IEEE Transactions on Information Theory (IEEE-TIT)*, Vol. 65, Issue 4, pages 2623 - 2636, 2019.
17. Anurag Anshu, Min-Hsiu Hsieh and Rahul Jain. “Quantifying resources in general resource theory with catalysts.” *Physical Review Letters (PRL)*, Volume 121, Issue 19, pp. 504-510, 2018.
18. Anurag Anshu, Rahul Jain and Naqeeb Ahmad Warsi. “Building blocks for communication over noisy quantum networks.” *IEEE Transactions on Information Theory (IEEE-TIT)*, Volume: 65, Issue: 2, pp. 1287–1306.
19. Mika Göös, Rahul Jain and Thomas Watson. “Extension complexity of independent set polytopes.” *SIAM Journal of Computing (SICOMP)*, Volume 47, Issue 1, pp. 241–269, February 2018.
20. Anurag Anshu, Rahul Jain and Naqeeb Ahmad Warsi. “A generalized quantum Slepian-Wolf.” *IEEE Transactions of Information Theory (IEEE-TIT)*, Volume 64, Issue 3, March 2018.
21. Anurag Anshu, Rahul Jain and Naqeeb Ahmad Warsi. “A one-shot achievability result for quantum state redistribution.” *IEEE Transactions of Information Theory (IEEE-TIT)*, Volume: 64, Issue: 3, March 2018.
22. Anurag Anshu, Vamsi Krishna Devabathini and Rahul Jain. “Quantum communication using coherent rejection sampling.” *Physical Review Letters (PRL)*, Vol. 119, Issue 12, September 2017.
23. Rahul Jain, Zhaohui Wei, Penghui Yao and Shengyu Zhang. “Multipartite quantum correlation and communication.” *Computational Complexity (CC)*, Volume 26, Issue 1, pp. 199-228, March 2017.
24. Rahul Jain, Attila Perézszlenyi and Penghui Yao. “A direct product theorem for bounded-round public-coin randomized communication complexity.” **Invited to special issue of Algorithmica on FOCS 2012.** Published, Volume 76 Issue 3, pp. 720-748, November 2016.
25. Anurag Anshu, Rahul Jain, Priyanka Mukhopadhyay, Ala Shayeghi and Penghui Yao. “New one-shot quantum protocols with application to communication complexity.” *IEEE Transactions of Information Theory (IEEE-TIT)*, Volume: 62, Issue: 12, Dec. 2016.

Cont’d

26. Gábor Braun, Rahul Jain, Troy Lee, Sebastian Pokutta. “Information-theoretic approximations of the nonnegative rank.” *Computational Complexity (CC)*, pp. 1-51, 2016.
27. Lila Fontes, Rahul Jain, Iordanis Kerenidis, Mathieu Laurière, Sophie Laplante and Jérémie Roland. “Relative discrepancy does not separate information and communication complexity.” *ACM Transactions on Computation Theory (TOCT)*, Volume 9, Issue 1, Article No. 4, December 2016.
28. Christopher Perry, Rahul Jain and Jonathan Oppenheim. “Communication tasks with infinite quantum-classical separation.” *Phys. Rev. Lett. (PRL)* 115, 030504, July 2015.
29. Rahul Jain. “New strong direct product results in communication complexity.” *Journal of the ACM (JACM)*, Vol. 62, Issue 3, Article No. 20, June 2015.
30. Rahul Jain and Ashwin Nayak. “The space complexity of recognizing well-parenthesized expressions in the streaming model: the Index Function revisited.” *IEEE Transactions on Information Theory (IEEE-TIT)*, vol. 60:10, pp.1-23, 2014.
31. Somshubhro Bandyopadhyay, Rahul Jain, Jonathan Oppenheim and Christopher Perry. “Conclusive exclusion of quantum states.” *Physical Review A. (PRA)* vol. 89(2), pp. 22336-22349, 2014.
32. Rahul Jain, Yaoyun Shi, Zhaohui Wei and Shengyu Zhang. “Efficient protocols for generating bipartite classical distributions and quantum states.” *IEEE Transactions on Information Theory (IEEE-TIT)*, vol. 59(8), pp. 5171-5178, 2013.
33. Rahul Jain and Ashwin Nayak. “Short proofs of the quantum Substate Theorem.” *IEEE Transactions on Information Theory (IEEE-TIT)*, Volume: 58(6), pp. 3664-3669, 2012.
34. Rahul Jain. “Resource requirements of private quantum channels and consequence for oblivious remote state preparation.” *Journal of Cryptology (JoC)*, Volume 25, Issue 1, pp. 1-13, 2012.
35. Rahul Jain and Shengyu Zhang. “The influence lower bound via query elimination.” *Theory of Computation (ToC)*, Volume 7, Article 10 pp. 147-153, 2011.
36. Prahladh Harsha, Rahul Jain, David McAllester and Jaikumar Radhakrishnan. “The communication complexity of correlation.” *IEEE Transactions on Information Theory (IEEE-TIT)*, 56(1), pp. 438-449, 2010.
37. Rahul Jain, Hartmut Klauck and Miklos Santha. “Optimal direct sum results for deterministic and randomized decision tree complexity.” *Information Processing Letter (IPL)*, 110 (2010), pp. 893-897.
38. Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay and John Watrous. “QIP = PSPACE.” **Invited to the Journal of the ACM (JACM)**. Published as Article no. 30, Volume 58, Issue 6, December 2011. Research highlights in Communications of the ACM (CACM), Vol. 53 No. 12, 2010.
39. Rahul Jain, Iordanis Kerenidis, Greg Kuperberg, Miklos Santha, Or Sattath and Shengyu Zhang. “On the power of a unique quantum witness.” *Theory of Computation (ToC)*, Volume 8, Article 17, pp. 375-400, 2012.
40. Rahul Jain, Alexandra Kolla, Gatis Midrijanis and Ben W. Reichardt. “On the parallel composition of zero-knowledge proofs with black-box quantum simulators.” *Quantum Information and Computation (QIC)*, 2009, Vol.9, No.5 and 6, pp. 0513-0532.
41. Richard Cleve, Dmitry Gavinsky and Rahul Jain. “Entanglement-Resistant Two-Prover Interactive Proof Systems and Non-Adaptive Private Information Retrieval Systems.” *Quantum Information and Computation (QIC)*, 2009, Vol.9 No.7 and 8, pp. 0648-0656.
42. Rahul Jain and Shengyu Zhang. “New bounds on classical and quantum one-way communication complexity.” *Theoretical Computer Science (TCS)*, Elsevier, 2009, (410) pp. 2463-2477.

Cont'd



43. Rahul Jain, Jaikumar Radhakrishnan and Pranab Sen. “A new information-theoretic property about quantum states with an application to privacy in quantum communication.” *Journal of the ACM (JACM)*, 2009, Volume 56, Issue 6, Article No.: 33.
44. Rahul Jain, Ashwin Nayak and Yi Su. “A separation between divergence and Holevo information for ensembles.” **Invited to a special issue of Mathematical Structures in Computer Science (MSCS) on TAMC 2008**. Published as *Lecture Notes in Computer Science* Volume 4978, 2008, pp 526-541.
45. Rahul Jain. “New binding-concealing trade-offs for quantum string commitment.” *Journal of Cryptology (JoC)*, 2008, Vol. 21 (4), pp. 579-592.
46. Rahul Jain. “Communication complexity of remote state preparation with entanglement.” In *Quantum Information and Computation (QIC)*, Vol.6 No.4&5 pp. 461-464, 2006.
47. Amit Deshpande, Rahul Jain, Satyanarayana V. Lokam, Jaikumar Radhakrishnan and Kavitha Telikapalli. “Lower bounds for adaptive locally decodable codes.” In *Random Structures and Algorithms (RSA)*, pp. 358-378, 2005.

### Conference publications

1. Naresh Goud Boddu, Vipul Goyal, Rahul Jain, João Ribeiro. “Split-state non-malleable codes and secret sharing schemes for quantum messages.” *Theory of Cryptography Conference (TCC)*, 2024.
2. Rishabh Batra, Rahul Jain. “Commitments are equivalent to one-way state generators.” *Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2024.
3. Michael X. Cao, Rahul Jain, Marco Tomamichel. “Quantum channel simulation under purified distance is no more difficult than state splitting.” *IEEE International Symposium on Information Theory (ISIT)*, 2024.
4. Itai Arad, Raz Firkko, Rahul Jain. “Area law for the maximally mixed ground state in degenerate 1D gapped systems.” *ACM Symposium on Theory of Computing (STOC)*, page 1311-1322, 2024.
5. Sayantan Chakraborty, Rahul Jain, and Pranab Sen. “One-shot non-catalytic distributed purity distillation.” *The 59th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1-8, 2023.
6. Rahul Jain, Georgios Piliouras, Ryann Sim. “Matrix multiplicative weights updates in quantum zero-sum games: conservation laws and recurrence.” *Conference on Neural Information Processing Systems (NeurIPS)*, 2022.
7. Rahul Jain, Srijita Kundu. “A direct product theorem for quantum communication complexity with applications to device-independent QKD.” *Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2021.
8. Rahul Jain. “Chain-rules for channel capacity.” *IEEE International Symposium on Information Theory (ISIT)*, 2021.
9. Rahul Jain, Srijita Kundu. “A direct product theorem for one-way quantum communication.” *IEEE Conference on Computational Complexity (CCC)*, 2021.
10. Anurag Anshu, Mario Berta, Rahul Jain, Marco Tomamichel. “Partially smoothed information measures.” *IEEE International Symposium on Information Theory (ISIT)*, 2019.

Cont'd

11. Salek F, Anshu A, Hsieh M-H, Jain R, Fonollosa JR. “One-shot Capacity Bounds on the Simultaneous Transmission of Public and Private Information Over Quantum Channels”. IEEE International Symposium on Information Theory (ISIT), 2018.
12. Anurag Anshu, Rahul Jain and Naqeeb A. Warsi. “One-shot entanglement assisted classical and quantum communication over noisy quantum channels: A hypothesis testing and convex split approach”. IEEE International Symposium on Information Theory (ISIT), 2018.
13. Anurag Anshu, Rahul Jain and Naqeeb A. Warsi. “A hypothesis testing approach for communication over entanglement assisted compound quantum channel”. IEEE International Symposium on Information Theory (ISIT). 2018.
14. Dmitry Gavinsky, Rahul Jain, Hartmut Klauck, Srijita Kundu, Troy Lee, Miklos Santha, Swagato Sanyal, Jevgenijs Vihrovs. “Quadratically tight relations for randomized query complexity”. The 13th International Computer Science Symposium in Russia (CSR), 2018.
15. Anurag Anshu, Dmitry Gavinsky, Rahul Jain, Srijita Kundu, Troy Lee, Priyanka Mukhopadhyay, Miklos Santha and Swagato Sanyal. “A composition theorem for randomized query complexity.” In proceedings of The 37th Foundations of Software Technology and Theoretical Computer Science (FSTTCS), 2017.
16. Anurag Anshu, Shalev Ben-David, Ankit Garg, Rahul Jain, Robin Kothari and Troy Lee. “Separating quantum communication and approximate rank.” In proceedings of the 32nd IEEE Conference on Computational Complexity (CCC), LIPIcs, pp. 24:1-24:33, 2017.
17. Mika Göös, Rahul Jain and Thomas Watson. “Extension Complexity of Independent Set Polytopes.” In proceedings of The 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS), pp. 565-572, 2016.
18. Anurag Anshu, Aleksandrs Belovs, Shalev Ben-David, Mika Göös, Rahul Jain, Robin Kothari, Troy Lee and Miklos Santha. “Separations in communication complexity using cheat sheets and information complexity.” In proceedings of The 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS), pp. 555-564, 2016.
19. Prahladh Harsha, Rahul Jain and Jaikumar Radhakrishnan. “Partition bound is quadratically tight for product distributions.” In proceedings of The 43rd International Colloquium on Automata, Languages, and Programming (ICALP), pp. 135:1-135:13, 2016.
20. Lila Fontes, Rahul Jain, Iordanis Kerenidis, Mathieu Laurière, Sophie Laplante and Jérémie Roland. “Relative discrepancy does not separate information and communication complexity.” In proceedings of The 42nd International Colloquium on Automata, Languages, and Programming (ICALP 2015), vol. 9134, LNCS, pp. 506-516, 2015. **Listed among “Best of Computing, 2016” by ACM Computing Reviews.**
21. Nathanaël François, Rahul Jain and Frédéric Magniez. “Input/Output Streaming Complexity of Reversal and Sorting.” In proceedings of the 18th International Workshop on Randomization and Computation (RANDOM), pp. 654-668, 2014.
22. Rahul Jain, Attila Pereszlényi and Penghui Yao. “A parallel repetition theorem for entangled two-player one-round games under product distributions.” In proceedings of 29th IEEE Conference on Computational Complexity (CCC), pp. 209 - 216, 2014.
23. Prahladh Harsha and Rahul Jain. “A strong direct product theorem for the Tribes function via the smooth-rectangle bound.” In proceedings of the 33rd Foundations of Software Technology and Theoretical Computer Science (FSTTCS), pp. 141-152, 2013.

Cont’d

24. Rahul Jain, Yaoyun Shi, Zhaohui Wei and Shengyu Zhang. "Efficient protocols for generating bipartite classical distributions and quantum states." In proceedings of the ACM-SIAM Symposium on Discrete Algorithms (SODA), pp. 1503-1512, 2013.
25. Rahul Jain, Attila Per  szlenyi and Penghui Yao. "A direct product theorem for bounded-round public-coin randomized communication complexity." In proceedings of The 53rd Annual IEEE Symposium on Foundations of Computer Science (FOCS), pp. 167-176, 2012.
26. Rahul Jain and Penghui Yao. "A parallel approximation algorithm for positive semidefinite programming." In proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS), pp. 463-471, 2011.
27. Rahul Jain, Hartmut Klauck and Shengyu Zhang. "Depth-Independent Lower bounds on Communication Complexity of Read-Once Boolean Functions." In proceedings of the 16th Annual International Computing and Combinatorics Conference (COCOON), 2010. Lecture Notes in Computer Science, 2010, Volume 6196/2010, 54-59.
28. Rahul Jain and Hartmut Klauck. "The Partition Bound for Classical Communication Complexity and Query Complexity." In proceedings of the 25th IEEE Conference on Computational Complexity (CCC), 2010, pp. 247-258.
29. Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay and John Watrous. "QIP = PSPACE." In proceedings of The 42nd ACM Symposium on Theory of Computing (STOC), pp. 573-582, 2010. **Recipient of the best paper award.**
30. Rahul Jain, Iordanis Kerenidis, Greg Kuperberg, Miklos Santha, Or Sattath and Shengyu Zhang. "On the power of a unique quantum witness." In proceedings of the 1st Annual Conference on Innovations in Theoretical Computer Science (ITCS), pp. 470-481, 2010.
31. Rahul Jain, Sarvagya Upadhyay and John Watrous. "Two-message quantum interactive proofs are in PSPACE." In proceedings of the 50th Annual Symposium on Foundations of Computer Science (FOCS), 2009, pp. 534-543.
32. Rahul Jain and Hartmut Klauck. "New Results in the Simultaneous Message Passing Model via Information theoretic techniques." In proceedings of the 24th IEEE Conference on Computational Complexity (CCC), 2009, pp. 369-378.
33. Rahul Jain and John Watrous. "Parallel approximation of non-interactive zero-sum quantum games." In proceedings of the 24th IEEE Conference on Computational Complexity (CCC), 2009, pp. 243-253.
34. Rahul Jain, Ashwin Nayak and Yi Su. "A separation between divergence and Holevo information for ensembles." In proceedings of The 5th Annual Conference on Theory and Applications of Models of Computation (TAMC), 2008, pp. 526-541.
35. Rahul Jain, Hartmut Klauck and Ashwin Nayak. "Direct product theorems for communication complexity via subdistribution bounds." In proceedings of The 40th ACM Symposium on Theory of Computing (STOC), 2008, pp. 599-608.
36. Prahladh Harsha, Rahul Jain, David McAllester and Jaikumar Radhakrishnan. "The communication complexity of correlation." In proceedings of 22nd IEEE Conference on Computational Complexity (CCC), pp. 10-23, 2007.
37. Rahul Jain, Jaikumar Radhakrishnan and Pranab Sen. "Prior entanglement, message compression and privacy in quantum communication." In proceedings of 20th IEEE Conference on Computational Complexity (CCC), pp. 285-296, 2005.

Cont'd

38. Rahul Jain, Jaikumar Radhakrishnan and Pranab Sen. “Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states.” In proceedings of 43rd IEEE Symposium on Foundations of Computer Science (FOCS), 2002, pp. 429-438.
39. Amit Deshpande, Rahul Jain, Satyanarayana V. Lokam, Jaikumar Radhakrishnan and Kavitha Telikapalli. “Better lower bounds for locally decodable codes.” In proceedings of 17th IEEE Conference on Computational Complexity (CCC), pp. 184-193, 2002.
40. Rahul Jain, Jaikumar Radhakrishnan and Pranab Sen. “A lower bound for bounded round quantum communication complexity of set disjointness.” In proceedings of 44th IEEE Symposium on Foundations of Computer Science (FOCS), 2003, pp. 220-229.
41. Rahul Jain, Jaikumar Radhakrishnan and Pranab Sen. “A direct sum theorem in communication complexity via message compression.” In proceedings of 30th International Colloquium on Automata, Languages and Programming (ICALP), 2003, pp. 300-315. **Invited to a special issue of Theoretical Computer Science (TCS) on ICALP 2003.**
42. Rahul Jain, Jaikumar Radhakrishnan and Pranab Sen. “The quantum communication complexity of the pointer chasing problem: the bit version.” In proceedings of 22nd conference on the Foundations of Software Technology and Theoretical Computer Science (FSTTCS), 2002, pp. 218-229.

### Conferences without publications

1. Rishabh Batra, Rahul Jain. “Commitments are equivalent to one-way state generators.” International Conference of Quantum Cryptography (QCrypt), 2024.
2. Itai Arad, Raz Firanko, Rahul Jain. “Area law for the maximally mixed ground state in degenerate 1D gapped systems.” Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC), 2024.
3. Naresh Goud Boddu, Vipul Goyal, Rahul Jain, João Ribeiro. “Split-state non-malleable codes and secret sharing schemes for quantum messages.” International Conference of Quantum Cryptography (QCrypt), 2023.
4. Rishabh Batra, Naresh Goud Boddu, Rahul Jain. “Quantum secure non-malleable randomness encoder and its application.” International Conference of Quantum Cryptography (QCrypt), 2023.
5. Naresh Goud Boddu, Rahul Jain, Upendra Kapshikar. “Quantum secure non-malleable-extractors.” Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC), 2022.
6. Rahul Jain, Srijita Kundu. “A direct product theorem for quantum communication complexity with applications to device-independent QKD.” Conference on Quantum Information Processing (QIP), 2022. **Short Plenary talk.**
7. Naresh Goud Boddu, Rahul Jain, Han-Hsuan Lin. “On relating one-way classical and quantum communication complexities.” Asian Quantum Information Science Conference (AQIS), 2021.
8. Rahul Jain, Srijita Kundu. “A direct product theorem for one-way quantum communication.” Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC), 2021.
9. Anurag Anshu, Shima Bab Hadiashar, Rahul Jain, Ashwin Nayak, Dave Touchette. “One-shot quantum state redistribution and quantum Markov chains”. Beyond I.I.D. in Information Theory, 2020. Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC), 2021.
10. Rahul Jain, Carl A. Miller and Yaoyun Shi. “Parallel device-independent quantum key distribution.” The 8th International Conference of Quantum Cryptography (QCrypt), 2018.

11. Anurag Anshu, Mario Berta, Rahul Jain, Marco Tomamichel. “Partially smoothed information measures.” *Beyond I.I.D. in Information Theory*, 2018.
12. Anurag Anshu, Rahul Jain and Naqeeb Ahmad Warsi. “Building blocks for communication over noisy quantum networks.” *The 21st Annual Conference on Quantum Information Processing (QIP)*, 2018.
13. Anurag Anshu, Rahul Jain and Naqeeb A. Warsi. “A hypothesis testing approach for communication over entanglement assisted compound quantum channel”. *The 21st Annual Conference on Quantum Information Processing (QIP)*, 2018.
14. Anurag Anshu, Shalev Ben-David, Ankit Garg, Rahul Jain, Robin Kothari and Troy Lee. “Separating quantum communication and approximate rank.” *The 21st Annual Conference on Quantum Information Processing (QIP)*, 2018.
15. Anurag Anshu, Min-Hsiu Hsieh and Rahul Jain. “Quantifying resources in general resource theory with catalysts.” *The 21st Annual Conference on Quantum Information Processing (QIP)*, 2018.
16. Anurag Anshu, Rahul Jain and Naqeeb Ahmad Warsi. “A one-shot achievability result for quantum state redistribution.” *The 21st Annual Conference on Quantum Information Processing (QIP)* 2018. **Invited talk at the IEEE Information Theory Workshop (ITW)**, 2017.
17. Anurag Anshu, Rahul Jain and Naqeeb Ahmad Warsi. “Convex-split and hypothesis testing approach to one-shot quantum measurement compression and randomness extraction.” *Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC)*, 2017.
18. Anurag Anshu, Rahul Jain and Naqeeb Ahmad Warsi. “A generalized quantum Slepian-Wolf.” *The 17th Asian Quantum Information Science Conference (AQIS)* 2017.
19. Anurag Anshu, Aleksandrs Belovs, Shalev Ben-David, Mika Göös, Rahul Jain, Robin Kothari, Troy Lee and Miklos Santha. “Separations in communication complexity using cheat sheets and information complexity.” *The 20th Annual Conference on Quantum Information Processing (QIP)*, 2017.
20. Anurag Anshu, Rahul Jain and Naqeeb A. Warsi. “One-shot entanglement assisted classical and quantum communication over noisy quantum channels: A hypothesis testing and convex split approach”. **Invited talk at Beyond I.I.D. in Information Theory**, 2017.
21. Somshubhro Bandyopadhyay, Rahul Jain, Jonathan Oppenheim and Christopher Perry. “Conclusive exclusion of quantum states.” *The 13th Asian Quantum Information Science Conference (AQIS)* 2013.
22. Rahul Jain, Ashwin Nayak. “The space complexity of recognizing well-parenthesized expression.” *The 15th Annual Conference on Quantum Information Processing (QIP)*, 2012.
23. Rahul Jain, Iordanis Kerenidis, Greg Kuperberg, Miklos Santha, Or Sattath and Shengyu Zhang. “On the power of a unique quantum witness.” *The 13th Annual Conference on Quantum Information Processing (QIP)*, 2010.
24. Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay and John Watrous. “QIP = PSPACE.” **Invited talk at the 13th Annual Conference on Quantum Information Processing (QIP)**, 2010.
25. Rahul Jain, Jaikumar Radhakrishnan and Pranab Sen. “A lower bound for bounded round quantum communication complexity of set disjointness.” *The 6th Annual Conference on Quantum Information Processing (QIP)*, 2004.
26. Rahul Jain, Jaikumar Radhakrishnan and Pranab Sen. “Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states.” *The 5th Annual Conference on Quantum Information Processing (QIP)*, 2003.

## Manuscripts

1. Rishabh Batra, Sayantan Chakraborty, Rahul Jain, Upendra Kapshikar. “Robust and composable device-independent quantum protocols for oblivious transfer and bit commitment.” ArXiv:2404.11283.
2. Kishor Bharti, Rahul Jain. “On the power of geometrically-local classical and quantum circuits.” ArXiv:2310.01540.
3. Srinivasan Arunachalam, João F. Doriguello, Rahul Jain. “A note on the partition bound for one-way classical communication complexity.” ArXiv:2302.10431.
4. Anurag Anshu, Rahul Jain, Alexander Streltsov. “Quantum state redistribution with local coherence. 2018. ArXiv:1804.04915.
5. Anurag Anshu, Rahul Jain and Naqeeb Ahmad Warsi. “A unified approach to source and message compression.” 2017. ArXiv:1707.03619.
6. Rahul Jain, Troy Lee and Nisheeth K. Vishnoi. “A quadratically tight partition bound for classical communication complexity and query complexity.” 2014. ArXiv:1401.4512.
7. Rahul Jain and Penghui Yao. “A strong direct product theorem in terms of the smooth rectangle bound.” 2012. ArXiv:1209.0263.
8. Rahul Jain and Ashwin Nayak. “Accessible versus Holevo information for a binary random variable.” 2006. At quant-ph/0603278.
9. Rahul Jain. “An approach from classical information theory to lower bounds for smooth codes.” 2007. At cs.CR/0607042.
10. Rahul Jain. “Distinguishing sets of quantum states.” 2005. ArXiv:quant-ph/0506205.