Recommendation letter for Srijita Kundu

Dear Madam/Sir,

Srijita has broadly conducted research in:

1. Quantum information theory, coding theory.
2. Quantum complexity theory.
3. Quantum cryptography.

Below I describe some of her works.

1. U. Kapshikar and S. Kundu. “On the hardness of the minimum distance problem of quantum codes.” IEEE Transactions on Information Theory (IEEE-T-IT), Volume 69, Issue 10, 2023.

In this work, they study hardness of finding the minimum distance of quantum error correcting codes. The equivalent problem for classical codes is known to be NP-hard, even in the approximate form. They show that finding the distance of stabilizer quantum codes exactly or approximately is NP-hard. This result is obtained by reducing the classical minimum distance problem to the quantum problem, using the CWS framework for quantum codes, which constructs a quantum code using a classical code and a graph. A main technical tool used for their result is a lower bound on the so-called graph state distance of 4-cycle free graphs, which also has implications in characterizing necessary conditions for degeneracy in quantum codes.

2. Rahul Jain, Srijita Kundu. “A direct product theorem for quantum communication complexity with applications to device-independent QKD.” In Proceedings of the 62nd Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2021. **Short plenary talk** at the 25th Conference on Quantum Information Processing (QIP), 2022.

Direct sum and direct product questions are fundamental questions in any model of computation. They ask how a resource required to compute several simultaneous instances of a task, scale as compared to the resource required for a single instance of the same task. They have found several applications in complexity theory, well known examples being: Raz’s parallel-repetition theorem for games with applications (along with the PCP theorem) to inapproximability theory and Yao’s XOR lemma with applications to cryptography and circuit complexity.

In this work, we give a direct product theorem for the entanglement-assisted interactive quantum communication complexity (under product distributions) of an l-player predicate V in terms of “the quantum efficiency or partition bound” introduced by Laplante, Lerays and Roland (2014), which is a lower bound on the distributional quantum communication complexity of computing V.

As an application of our result, we provide a first security proof for device-independent quantum key distribution (DIQKD) under leakage (communication between the devices). We analyze the DIQKD protocol given by [4], and show that it is possible to extract $\Omega(n)$ bits of key from it, even in the presence of $O(n)$ bits of leakage. Our security proof is parallel, i.e., the honest parties can enter all their inputs into their devices at once and works for a leakage model that is arbitrarily interactive, i.e., the devices of the honest parties Alice and Bob can exchange information with each other and with the eavesdropper Eve in any number of rounds, as long as the total number of qubits communicated is bounded.

3. Rahul Jain and Srijita Kundu. "A direct product theorem for one-way quantum communication." IEEE Conference on Computational Complexity (CCC), 2021. Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC), 2021.

In this work we have considered the direct-product question for the one-way-entanglement-assisted quantum communication complexity. We show that if the communication in this model for computing k simultaneous instances of a relation f (including partial/total functions) is less than k times what is needed for a single instance of f, then the overall success is exponentially small in k. This is the first general direct product result holding for all relations in any model of quantum communication complexity. We use information theory and message compression arguments from [1, 2] to arrive at this result. We also use an interesting concept of "anchored-distributions" from [3], where they use it to show a parallel-repetition theorem for quantum games. We simplify their proof, and this simplification is crucial for us to be able to use anchored distributions in our setting of entanglement-assisted-one-way quantum communication protocols.

4. Srijita Kundu and Ernest Tan. "Composably secure and device-independent encryption with certified deletion." Quantum 7, 1047, 2023. The 24th Conference on Quantum Information Processing (QIP), 2021.

In this work the authors use a parallel repetition argument for some involved multi-round games to arrive at a parallel-device-independent proof of security for a cryptographic task of "encryption with certified-deletion".

5. Anurag Anshu, Shalev Ben-David and Srijita Kundu. "On query-to-communication lifting for adversary bounds." IEEE Conference on Computational Complexity (CCC), 2021. Conference on Quantum Information Processing (QIP), 2021.

In this work the authors make progress towards "lifting" the "positive-weights-adversary-bound" for quantum query complexity of a function f to arrive at lower bounds for quantum communication complexity for a composed function (f composed with a constant size function g). There have been several lifting-results obtained recently for classical query and communication complexity. Lifting quantum query complexity to quantum communication complexity remains an important and major open question.

Overall, Srijita has conducted excellent research till now. She has several Tier-1 publications (PODC, IEEE-T-IT, FOCS, Quantum) and several publications in other premium venues (ICALP, CCC). Many of her works have been presented in top quantum information conferences (without proceedings) QIP and TQC. Several of these publications are during her postdoc with several different researchers, exhibiting her versatility and independence.

She is motivated, sharp and hard working. She has a good mathematical acumen and pursues the problems she is interested in with good patience. She has developed good insights with various tools and techniques in quantum information theory and can use them with comfort for direct-sum, direct-product and composition questions. She is also able to find good application of these results, for example in cryptography. She maintains her interest in quantum complexity theory, cryptography and information theory. At the same time, she is happy to explore other areas e.g., quantum algorithms.

I believe with her experiences, she is well placed to follow her research program, explore new areas of research, and further pursue the questions she has been dealing with, in several interesting and challenging directions. She holds excellent promise, and I eagerly look forward to her ventures in the future.

She is a friendly and cooperative person and works well in a collaborative environment. She has a pleasant personality and brings good enthusiasm and energy to her group.

She has helped me as a Teaching Assistant for a few of the courses I have taught before. She helped particularly with setting up weekly assignments and grading. She did a very systematic and meticulous job at that.

I recommend Srijita enthusiastically and wholeheartedly for the tenure-track position that she is applying for. Please let me know if you may need further information.

Rahul Jain,
Professor,
Computer Science Department,
Principal Investigator,
Centre for Quantum Technologies,
National University of Singapore.

Date: 14 December 2024.

References:

1. Rahul Jain, Jaikumar Radhakrishnan and Pranab Sen. “Prior entanglement, message compression and privacy in quantum communication.” The 20th IEEE Conference on Computational Complexity (CCC), pp 285-296, 2005.

2. Rahul Jain, Attila Pereszlényi and Penghui Yao. “A Direct Product Theorem for Two-Party Bounded-Round Public-Coin Communication Complexity.” Algorithmica, 76(3):720–748, 2016.

3. Mohammad Bavarian, Thomas Vidick and Henry Yuen. “Hardness Amplification for Entangled Games via Anchoring.” In Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing (STOC), page 303–316, 2017.