Harvard John A. Paulson
School of Engineering
and Applied Sciences

The Selection Committee,

I am pleased to write this letter of recommendation for Srijita, an exceptional quantum computing researcher whose work bridges quantum complexity theory and quantum cryptography. Srijita and I first collaborated about six years ago as graduate students at NUS, Singapore. Since then, although we have pursued different directions in research, I have followed Srijita's remarkable achievements during her postdoc at IQC, Waterloo, and her final PhD years in Singapore. It is clear that Srijita is one of the leading researchers at the intersection of quantum complexity theory and quantum cryptography, equipped with all the skills necessary to excel as a faculty member.

Here are some of my favorite works by Srijita:

1. "**A direct product theorem for quantum communication complexity with applications to device-independent cryptography**" (https://arxiv.org/abs/2106.04299)

Direct product theorems are foundational in complexity theory, serving as the building blocks for more intricate composition theorems. Achieving direct product results for quantum communication complexity has been particularly challenging due to our limited understanding of quantum protocols. Srijita's work accomplishes one of the rare direct product results, demonstrating that quantum protocols cannot save communication resources without incurring significant errors. She further explores applications of this result in device-independent quantum cryptography. A remarkable aspect of this work is

the demonstration of a "phase transition" phenomenon in the trade-off between error and communication, which is generally not well understood and can be recognized as analogous to the strong converse theorems in Shannon theory.

2. “**Oracle separation of QMA and QCMA with bounded adaptivity**"
[https://arxiv.org/abs/2402.00298]

One major open question that has recently gained considerable attention is the oracle separation between QMA and QCMA. Identifying such an oracle separation has been surprisingly difficult, with recent works achieving separation only in restricted settings. Srijita’s work makes significant progress by presenting an oracle separation for protocols with bounded-adaptive queries to the oracle. In this study, she identifies an intriguing "slipperiness" property of the well-known Yamakawa-Zhandry oracle, and charts a very promising approach to resolving the QMA vs QCMA conjecture.

3. "**Separations in query complexity for total search problems**"
(https://arxiv.org/abs/2410.16245)

In this work, Srijita extends the Yamakawa-Zhandry results by examining the query complexity of search problems. She demonstrates a series of separations between various complexity measures for such problems, paving the way for substantial follow-up work. This study showcases her ability to delve deeply into latest breakthroughs and extract far-reaching generalizations.

These examples highlight the remarkable depth and insight in Srijita’s work. Her well-crafted research statement outlines an exciting trajectory for future projects in quantum complexity and cryptography – notably the quantum lifting conjecture (a major open question in quantum communication complexity) and the QMA vs QCMA oracle separation. Through my interactions with her, I have observed that she takes a thoughtful and principled approach to problem selection, ensuring that her research aligns with pressing challenges in quantum complexity.

In conclusion, Srijita is an outstanding quantum computing researcher whose contributions are leading to significant advancements in quantum query complexity and cryptography. Furthermore, Srijita's collaborative spirit is evident from the diverse range of her co-authored works within a relatively short span. I strongly recommend her without hesitation, and I am confident in her ability to thrive as a faculty member.

Sincerely,

Anurag Anshu

Assistant Professor of Computer Science,

John A. Paulson School of Engineering and Applied Sciences,

Harvard University