ERROR-IMMUNE AND SECURE QUANTUM COMMUNICATION WITH OPTIMAL RESOURCES

RAJNI BALA

DEPARTMENT OF PHYSICS

INDIAN INSTITUTE OF TECHNOLOGY DELHI

February 2024

Error-immune and secure quantum communication with optimal resources

by

RAJNI BALA

Department of Physics

Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

INDIAN INSTITUTE OF TECHNOLOGY DELHI

February 2024

Dedicated to my parents

Certificate

This is to certify that the thesis entitled **"Error-immune and secure quantum communication with optimal resources"**, submitted by **RAJNI BALA** to the Indian Institute of Technology Delhi, for the award of the degree of **Doctor of Philosophy** in PHYSICS, is a record of the original, bona fide research work carried out by her under my supervision and guidance. The thesis has reached the standards fulfilling the requirements of the regulations related to the award of the degree.

The results contained in this thesis have not been submitted in part or in full to any other University or Institute for the award of any degree or diploma to the best of my knowledge.

Prof. V. Ravishankar
Department of Physics,
Indian Institute of Technology Delhi.

Date:

Acknowledgements

The successful completion of this project would not have been possible without the combined efforts of a group of individuals. Thus, I would like to express my gratitude to all those who contributed to its success. While many individuals deserve recognition, I would like to highlight a few who made exceptional contributions.

First, I extend my sincere gratitude to Prof. V. Ravishankar for providing me with an opportunity to work under his guidance. His dedication, patience, and unwavering support throughout this journey have been immeasurable. I am grateful for the academic freedom he has granted, allowing me to explore and pursue my research interests at my own pace. His motivational words, especially during challenging phases, have been instrumental to my progress. I consider myself fortunate to have had him as my supervisor, and I am deeply grateful for his understanding during moments of self-doubt. I am thankful for the numerous opportunities he provided, enabling both my personal and academic growth. His thoughtfulness and insightful suggestions fostered fruitful discussions that enriched my research endeavors. Engaging in discussions with him greatly enhanced my understanding.

I would also like to express my gratitude to my SRC members, Prof. M. R. Shenoy, Prof. Joyee Ghosh, and Prof. Narayanan D. Kurur, for their valuable suggestions, and feedback over the time.

I extend many thanks to Prof. A K Jha and his group for having me at IIT Kanpur for a couple of days. I would like to express my gratitude to Prof. Pankaj Agarwal, Dr. Chandan Datta, and Abhishek Panda for their time and useful discussions during online meetings. Many thanks to Prof. Jasleen Lugani and Dr. Richa Goyal for various discussions on Quantum key distribution.

I am thankful to Dr. Soumik Adhikary and Dr. Radha Pyari Sandhir for their support during the initial stages of my Ph.D. I express my sincere gratitude to Sooryansh Asthana. I have not only got a wonderful collaborator in him but a friend to cherish for the rest of my life. The kind of support and patience he has offered is exemplary. The way he put things in perspective and his suggestions have greatly helped in my personal growth. Discussions with him have always been brain-storming and have helped me with my academic growth. Though I am blessed to have many people in my life whose

characteristics are rarely found, the kind of sensitivity, self-confidence, and principles he has attained is never seen before. I consider myself fortunate to have had him in my life.

I extend many thanks to all the members of the Einstein Research Scholar room for creating a peaceful atmosphere in the lab. Special mention goes to Laxman Prasad Goswami, who provided exceptional help, even going beyond expectations. Many thanks to Subhasish Bag for his support and help and Subramanya Bhat and Imran Khan for the delicious homemade meals they generously offered. I would like to thank Dr. Kalpak Gupta, and Dr. Mayank Gupta for their help and support during the TA duties in B. Tech. lab. Many thanks extend to my friends Gaytri Arya, Dr. Manish Dwivedi, Awantika Mishra, Dr. Sharadha Mishra, Tania, and Anashwara for their companionship, which brought many lighthearted moments. Gaytri's remarkable support throughout my Ph.D. journey has been truly invaluable. Her truthfulness, kindness and caring nature is something I admire the most. Without her, this journey would have been much more challenging. I would like to express my gratitude to my friends from school and college, Rashmi, Priyanka, Neha, Ramandeep, and Pooja, for their constant support.

I would like to acknowledge the University Grants Commission (UGC) for their financial assistance in supporting my research. I am grateful for the financial support provided by the travel grants, Research Scholar Travel Award, and Research Excellence Travel Award, which funded my participation in conferences. Furthermore, I appreciate the funding I received from IIT for two months after completing five years. Additionally, I want to acknowledge the kindness of Scientific Reports for waiving their article publishing charges.

Lastly, I want to express my deepest appreciation to my family for their unwavering support throughout this long journey. My deepest gratitude goes to my parents Mrs. Paramjit Kumari and Mr. Nirmal Kumar for their patience, untiring efforts, and the belief they have shown in me. Their patience in this long journey of almost seven years is remarkable. This acknowledgment remains incomplete without mentioning Mr. Yadwinder. I am thankful to him for the ambitions he instilled and encouraged me to undertake this task. Patience, love, and care he has showered have no substitute and have been the strength throughout to keep going. I would like to thank my mother and father-in-law Mrs. Sarabjit and Mr. Satpal for their patience and support in this journey.

It is possible that I may have inadvertently omitted certain individuals of significant importance in this acknowledgment, an oversight stemming from my memory lapse. Nevertheless, it is essential to note that my acknowledgment extends beyond the scope of these pages.

Rajni Bala

Abstract

In recent times, quantum communication has emerged as a vibrant area of research. The horizon of quantum communication has numerous celebrated and pioneering protocols— quantum teleportation, quantum key distribution, error-correction-assisted quantum communication protocols. Challenges and limitations in the generation of resources required for these protocols nevertheless act as major impediments. An indispensable problem is in making experimental realizations and theoretical assumptions come hand in hand. Elegant protocols like quantum teleportation and Ekert 91 QKD employ entangled states, whose generation poses a challenge. In particular, error correction poses a significant challenge in quantum communication since the application of higher dimensional entangling gates in many degrees of freedom, e.g., OAM is not readily available. This leads us to the question of interest in this thesis: to what extent can we alleviate the need for costly quantum resources and still have a quantum advantage, albeit in some restricted scenarios? We attempt to answer this question in the context of error-immune quantum communication and quantum key distribution — two cornerstones in the area of quantum communication.

In the first part of the thesis, we focus on laying down a resource-friendly approach to error- immune quantum communication. In contrast to the traditional approaches, which encode information in a quantum state, we develop a framework by proposing an altogether new information encoding scheme. This scheme, by construction, encodes information in the invariants of a noisy channel. Notably, this encoding scheme leads to a complete removal of budget overhead for quantum error correction. We construct invariants for several noisy channels which are of practical interest. Interestingly, quantum error-correcting and rejecting codes appear as special cases of this encoding scheme. Finally, we have applied the framework to a practical situation of propagation of OAM modes in turbulence. By performing a study of extensive simulation data, we phenomenologically model the channel as an idealized crosstalk channel and identify the invariants for the same. These invariants serve the purpose of being error-immune information carriers.

In the second part of thesis, we turn our attention exclusively on resource-friendly quantum key distribution protocols. In this direction, a significant development is the proposal of semi-quantum key distribution protocol. This protocol involves only one quantum

participant who can operate in any basis, in contrast to a classical participant who can operate only in the computational basis. We perform a series of studies to propose quantum and semi-quantum key distribution protocols by employment of OAM states of light, which are arguably at the forefront of realization of high dimensional quantum communication. We start by showing that the task of secure distribution of keys in layered networks can be accomplished with only one quantum participant and multidimensional separable states. We believe that this is a significant development over the protocols proposed in [Pivoluska, 2017], which employ multidimensional entangled states with a very low generation yield. In the second study, we show that corresponding to every nonlocality/ entanglement-based QKD protocol, a contextuality-based QKD protocol may be designed. The security analysis of the latter protocol is, however, completely different and hinges on masking transformations. The key rate of the CQKD protocols, however, is exponentially small. As the next improvement, we show how a suitable change in the key generation rule and the choice of observables may lead to enhancement in the key generation rates with the same resource states. Finally, we show that qubits encoded in qudits may be employed for QKD protocols. The generation yield of these states is significantly high. We have shown robustness of all the protocols to eavesdropping attacks.

सार

नवीनकाल में, क्वांटम संचार शोध का परिस्पन्दी क्षेत्र बनकर उभरा है। क्वांटम संचार का क्षितिज कई प्रसिद्ध एवं नवीन प्रोटोकॉलों से युक्त है, जैसे क्वांटम टेलीपोर्टेशन, क्वांटम कुंजी वितरण तथा त्रुटि–सुधार–सहायित क्वांटम संचार प्रोटोकॉल। तथापि इन प्रोटोकॉलों के लिए आवश्यक संसाधनों के सृजन में चुनौतियां और सीमाएँ प्रमुख बाधाएँ हैं। प्रायोगिक अनुभवों और सैद्धांतिक धारणाओं को एकानुरूप बनाना भी एक अनिवार्य समस्या है। क्वांटम टेलीपोर्टेशन और एकर्ट–91 क्वांटम कुंजी वितरण जैसे सुरुचिपूर्ण प्रोटोकॉलों में जो व्यतिकृत स्टेट्स (entangled states) संसाधन के रूप में प्रयोग करते हैं , उनका सृजन एक चुनौती प्रस्तुत करता है। विशेष रूप से, त्रुटि सुधार (error correction) ने क्वांटम संचार में बड़ी चुनौती प्रस्तुत की है क्योंकि उच्च आयामिक (high–dimensional) एंटलिंग गेट का विनियोग प्रकाश के कक्षीय कोणीय संवेग (orbital angular momentum) जैसी स्वातंत्र्य कोटि में उपलब्ध नहीं हैं। यह हमें इस शोधग्रंथ में दिलचस्पी के प्रश्न पर पहुंचते हैं: हम किस स्तर तक बहुमूल्य क्वांटम संसाधनों की आवश्यकता को कम रखते हुए भी क्वांटम लाभ प्राप्त कर सकते हैं चाहे कुछ सीमित परिस्थियों में ही हो? हम इस प्रश्न का उत्तर देने का प्रयास क्वांटम संचार के क्षेत्र में दो मुख्य स्तंभों– त्रुटि–प्रतिरोधी क्वांटम संचार और क्वांटम कुंजी वितरण— के संदर्भ में करते हैं।

शोधग्रंथ के पहले भाग में, हम त्रुटि–प्रतिरोधी क्वांटम संचार के लिए एक संसाधन–अनुकूल मार्ग प्रस्तुत करने पर ध्यान केंद्रित करते हैं। परंपरागत दृष्टिकोणों के विपरीत, जिनमें सूचना को एक क्वांटम अवस्था में कूटबद्ध किया जाता है, हम एक बिलकुल नई कूटबद्ध सूचना योजना प्रस्तुत करके एक प्रक्रिया विकसित करते हैं। यह योजना, निर्माण के द्वारा, कलुषित चैनल (noisy channel) के अपरिवर्तक परिमाणों में सूचना को कूटबद्ध करती है। विशेष रूप से, यह कूटबद्ध योजना क्वांटम त्रुटि सुधार के लिए संसाधनों का पूरी तरह से निर्मूलन करने के लिए ले जाती है। हम कई व्यवहार में विनियोग के लिए कलुषित चैनलों के लिए अपरिवर्तक प्रस्तुत करते हैं। विशेष रूप से, यह एन्कोडिंग योजना क्वांटम त्रुटि–सुधार कोड को इसके अंशक रूप में प्रस्तुत होती है। अंततः, हमने वायुमण्डल में प्रकाश के ओ ए एम मोड के प्रसारण के एक व्यावहारिक तौर पर प्रक्रिया को विनियोगित किया है। व्यापक अनुक्रम आँकड़ों का अध्ययन करके, हम कोलाहल को

एक आदर्श औरिकीरण (crosstalk) चैनल के अनुरूप करते हैं और उसके लिए अपरिवर्तकों की पहचान करते हैं। ये अपरिवर्तक त्रुटि–प्रतिरोधी सूचना वाहक का कार्य निभाते हैं।

शोधग्रंथ के दूसरे भाग में, हम अपना ध्यान विशेष रूप से केवल संसाधन–अनुकूल क्वांटम कुंजी वितरण प्रोटोकॉलों पर देते हैं। इस दिशा में, एक महत्वपूर्ण विकास सेमी–क्वांटम कुंजी वितरण प्रोटोकॉल का प्रस्ताव है। इस प्रोटोकॉल में केवल एक क्वांटम प्रतिभागी होता है जो किसी भी बेसिस (basis) में काम कर सकता है। इसके विपरीत एक शास्त्रीय प्रतिभागी (classical participant) केवल गणनात्मक बेसिस में काम कर सकता है। हम क्वांटम और सेमी–क्वांटम कुंजी वितरण प्रोटोकॉलों की श्रृंखला को प्रस्तावित करते हैं जो प्रकाश के ओ ए एम स्टेट्स का उपयोग करके की गई है, जिन्हें उच्च आयामी क्वांटम संचार में अग्रणी स्थान प्राप्त है। हम पहले दिखाते हैं कि स्तरित नेटवर्कों में कुंजी वितरण का कार्य केवल एक क्वांटम प्रतिभागी और बहुआयामी पृथक्करणीय स्टेट्स (separable states) के साथ संपन्न किया जा सकता है। हम आशा करते हैं कि हमसे प्रस्तावित प्रोटोकॉल [Pivoluska, 2017] में प्रस्तावित प्रोटोकॉलों के सापेक्ष एक महत्वपूर्ण अभिवृद्धि है। [Pivoluska, 2017] बहुआयामी व्यतिकृत स्टेट्स का उपयोग करते हैं जिनका सृजन क्षमता बहुत कम होती है। दूसरे अध्ययन में, हम दिखाते हैं कि प्रत्येक नॉनलोकल/ व्यतिषण –आधारित क्यूकेडी प्रोटोकॉल के सापेक्ष, एक संदर्भात्मकता–आधारित क्यूकेडी प्रोटोकॉल प्रस्तावित किया जा सकता है। यद्यपि इस अंतिम (संदर्भात्मकता–आधारित) प्रोटोकॉल का सुरक्षा विश्लेषण पूरी तरह से विभिन्न है और मास्किंग परिवर्तनों पर निर्भर है। यद्यपि संदर्भात्मकता–आधारित क्यूकेडी प्रोटोकॉलों की कुंजी दर, लघुगतिक कम है। अगले सुधार के रूप में, हम दिखाते हैं कि कुंजी उत्पादन नियम और मापकों के चयन में उपयुक्त परिवर्तन से कुंजी सृजन दरों में वृद्धि हो सकती है। अंततः, हम दिखाते हैं कि क्यूबिट्स को क्यूडिट्स में कूटित (encode) किया जा सकता है और QKD प्रोटोकॉल के लिए इस्तेमाल किया जा सकता है। इन स्टेट्स की सृजन योग्यता बहुत अधिक है। हमने सभी प्रोटोकॉलों को चुगलखोर हमलों (eavesdropping attacks) से सुभद्र दिखाया है।

Contents

List of Figures

List of Tables