STUDY OF VARIOUS ASPECTS OF QUANTUM COMMUNICATIONS

Thesis Submitted For The Degree Of

DOCTOR OF PHILOSOPHY (SCIENCE)

in

Physics (Theoretical)

by

SUBHANKAR BERA

DEPARTMENT OF PHYSICS

JADAVPUR UNIVERSITY

2025

DEDICATION

To

My Parents

ACKNOWLEDGEMENT

I seize this opportunity to convey my heartfelt appreciation and deep gratitude to all those who have played a major role in molding my academic path and accompanied me on this remarkable journey.

First and foremost, I wish to offer my obeisances to my parents, whose guidance and sacrifices since my childhood have played a pivotal role in shaping me into the person I am today. They were my first teachers and continue to be. Always standing by my side as steadfast pillars through thick and thin, they encouraged me endlessly to move forward. Without their unconditional love and support during challenging times, I would not have been able to make this far. As I stand today at the culmination of my PhD journey, I derive solace from the thought of bringing a small smile to their faces and joy to their hearts. I owe them everything, and any words attempting to convey my gratitude would inevitably fall short.

I am profoundly grateful to my Ph.D. mentor, Prof. Archan S. Majumdar. His deep physical insights and adeptness at navigating intricate concepts using pure physical arguments have always amazed me. I have learned much from him during our discussions. He has always encouraged me to think deeply, and from diverse perspectives. From the beginning of my PhD journey, he has consistently encouraged me to move beyond the limitations of specialized fields and embrace a broader understanding of

physics. Besides his depth of understanding. I have greatly benefited from his wise advice, both in professional and personal matters. Equally instrumental in my academic journey has been Dr. Manik Banik. He introduced me to the fascinating field of Quantum Information Theory. His invaluable insights and mentorship have significantly enriched my learning journey. I have learned various technical nuances of the subject from him. What stands out is his consistent encouragement for me to cultivate independent and critical thinking, devoid of external validation. He has been influential in fostering in me a sense of self-reliance and confidence.

I would like thank a lot to my collaborators: Dr. Shashank Gupta, Dr. Debashish Saha, Dr. Ananda G. Maity, Dr. Anubhab Chaturvedi, Dr. Shiladitya Mal, Prof. Hyunseok Jeong, Dr. Soumyakanti Bose, Dr. Souradeep Sasmal, Dr. Arup Roy and Soumyabrata Hazra. I have been privileged to learn a great deal from working and discussing with them. I would also like to acknowledge Prof. Dipankar Home, and Dr. Jashkaran Singh for insightful discussions on various occasions that has enriched me.

I am very much thankful to my seniors: Dr. Ananda G. Maity, Dr. Shashank Gupta, and Dr. Bihalan Bhattacharya, PhD colleagues: Arun Kumar Das, Indrajit Ghose, and Arnab Mukherjee, and juniors: Pritam Roy, Sudip Chakraborty, Bivas Mallick, and Saheli Mukherjee for making PhD journey at S. N. Bose National Centre for Basic Sciences eventful.

I express my gratitude to S. N. Bose National Centre for Basic Sciences for financial support and granting me the resources to pursue my Ph.D. study. This institute has been my academic home, where I have spent the second longest period of my academic life after school.

To be submitted as per this format

CERTIFICATE FROM THE SUPERVISOR

This is to certify that the thesis entitled " **Study of Various Aspects of Quantum Communications**" submitted by Sri **Subhankar Bera** who got his name registered on **23rd June 2022** for the award of Ph.D. (Science) Degree of Jadavpur University, is absolutely based upon his own work under the supervision of **Prof. Archan S. Majumdar** and that neither this thesis nor any part of it has been submitted for either any degree / diploma or any other academic award anywhere before.

Asmajumdar 3/6/25

Dr. Archan S. Majumdar
Senior Professor
S. N. Bose National Centre
for Basic Sciences
Block-JD, Sector-III, Salt Lake
Kolkata-700106

(Signature of the Supervisor date with official seal)

THESIS DECLARATION

I hereby declare that this thesis titled "**Study of Various Aspects of Quantum Communications**" is based on my original research works. I confirm that the work is original and has not been submitted earlier as a whole or in part for a degree at any Institution/University. I have duly acknowledged all the references that are used partially to prepare this thesis.

Subhankar Bera

Subhankar Bera
03/06/2025

ABSTRACT

Quantum communication, a pivotal subfield of quantum information science, explores how inherently nonclassical features of quantum mechanics can be harnessed to perform communication tasks with enhanced security and efficiency. The central objective of this thesis is to investigate how various quantum correlations, including temporal nonclassicality, Bell nonlocality, and contextuality, can be operationally utilized in different communication protocols and foundational scenarios. To begin with, the thesis explores quantum random access codes (QRACs), a fundamental communication protocol wherein a sender encodes multiple classical bits into a quantum system, allowing the receiver to retrieve any one of them with high success probability. We show that this communication advantage has a direct equivalence with the violation of temporal inequalities derived from noninvasive realist assumptions. Thus, temporal quantum correlations, though less studied than their spatial counterparts, are shown to be both necessary and sufficient to realize quantum enhancements in time-ordered communication scenarios. Moreover, this link provides a method to certify genuine randomness based solely on temporal behavior. In the context of secure quantum communication, the thesis examines device-independent quantum key distribution (DI-QKD), where no assumptions are made about the internal functioning of the devices involved. Here, Bell nonlocality plays a crucial role as a certification tool.

We analyze the performance of random two-qubit states, generated Haar-uniformly, and quantify how increasing mixedness (state rank) impacts both nonlocality and secure key rates. The study reveals that while entanglement and Bell violation degrade gradually with rank, the drop in key rate is more severe. Notably, pure and Werner states are identified as extremal cases that bound the achievable key rate for a same amount of entanglement. Contextuality, another powerful nonclassical resource, is investigated through its implications for communication efficiency in restricted scenarios. The thesis constructs a generalized noncontextual polytope that captures both preparation and measurement noncontextuality. It enables scalable derivation of facet inequalities, uncovering new forms of contextuality. These inequalities are then shown to enhance performance in several communication-relevant tasks, including oblivious communication, certification of non-projective measurements, and dimension witnessing, demonstrating contextuality's relevance beyond foundational tests. Finally, the thesis turns to long-distance quantum communication, focusing on hybrid systems that combine continuous-variable and discrete-variable encodings. By employing entanglement swapping on multi-photon coherent states, we show that high-fidelity polarization Bell pairs can be distributed over intercity distances exceeding 200 km. These shared states are then used for quantum teleportation of unknown polarization qubits, where the achieved fidelity remains above classical thresholds even under realistic transmission losses, highlighting the practicality of hybrid-state architectures for scalable quantum networks. Overall, the thesis provides a unified perspective on how different forms of quantum correlations can be operationalized to achieve and enhance various quantum communication tasks. The results underscore the fundamental interplay between nonclassicality and information transfer, while also pointing toward promising directions for secure and scalable quantum technologies.

List of Publications and Communicated Articles

Publications relevant to the Thesis:

1. *"Role of nonclassical temporal correlation in powering quantum random access codes,"* **Subhankar Bera**, Ananda G. Maity, Shiladitya Mal, and A. S. Majumdar, Physical Review A **106**, 042439 (2022).

2. *"Device-independent quantum key distribution using random quantum states,"* **Subhankar Bera**, Shashank Gupta, and A. S. Majumdar, Quantum Inf. Process **22**, 109 (2023).

3. *"Efficient relaxation of generalized noncontextual polytopes and quantum violation of their facet inequalities,"* Soumyabrata Hazra, Debashis Saha, Anubhav Chaturvedi, **Subhankar Bera**, and A. S. Majumdar, arXiv:2406.09111 (2024).

4. *"Sharing quantum nonlocality and teleportation over long distance using optical hybrid states,"* **Subhankar Bera**, Soumyakanti Bose, Hyunseok Jeong, and A. S. Majumdar, arXiv:2502.00707 (2025).

Additional publications during the Ph.D. thesis but not forming part of it:

1. *"Device-independent quantum secure direct communication under non-Markovian quantum channels,"* Pritam Roy, **Subhankar Bera**, Shashank Gupta, and A. S. Majumdar, Quantum Inf Process **23**, 170 (2024).

2. *"Sequential attack impairs security in device-independent quantum key distribution,"* Pritam Roy, Souradeep Sasmal, **Subhankar Bera**, Shashank Gupta, Arup Roy and A. S. Majumdar, arXiv:2411.16822 (2024).

CONTENTS

List of Figures

List of Tables

CHAPTER 1

INTRODUCTION

The development of *communication* has always been tied to physical processes. From early signaling methods such as smoke, drums, and flags, to the invention of the telegraph and telephone, communication has always relied on physical carriers to transmit messages across space and time. As these systems evolved from analog to electronic, scientists and engineers began to investigate not just how to build communication devices, but how to quantitatively model and optimize the communication process itself. This shift in perspective, particularly during the early 20th century, led to the foundational idea that communication is subject to physical and mathematical limits. Harry Nyquist (1924) showed that the rate at which symbols can be transmitted is constrained by the bandwidth and signal levels of the medium, while Ralph Hartley (1928) introduced a measure to quantify how much distinguishable information could be encoded in a signal [1, 2]. These practical challenges in communication eventually motivated a deeper conceptual question: what is information, and how can its transmission be made reliable in the presence of noise? This question led to the birth of

information theory as a formal discipline. In his seminal 1948 work, Claude Shannon proposed a general mathematical framework for communication systems [3]. By treating the message source as a probabilistic process and modeling the effects of noise in the channel, Shannon introduced entropy as a measure of uncertainty and defined the concept of channel capacity, which represents the theoretical maximum rate of error-free transmission. His framework revolutionized communication theory by abstracting messages into symbolic sequences and focusing on their statistical structure rather than semantic content. This abstraction not only simplified the engineering of communication systems but also enabled powerful techniques like error correction and data compression. However, the classical framework developed in Shannon's time was grounded in assumptions that aligned with the macroscopic, classical world, where signals can be duplicated, measured, and stored without fundamentally altering the information itself. These assumptions held true for traditional communication systems based on electromagnetic waves or electrical pulses. Yet, with the miniaturization of devices and the emergence of technologies operating at atomic and subatomic scales, it became increasingly evident that the underlying physical laws governing information carriers could no longer be ignored. At this scale, information is encoded in systems that follow the principles of quantum mechanics, not classical physics.

This realization led to the development of quantum communication, a framework in which information is encoded, transmitted, and processed according to the principles of quantum mechanics. In this setting, the basic unit of communication is the qubit, capable of existing in superposition and entangled states. These characteristics fundamentally change how communication tasks are approached, introducing new possibilities as well as new limitations. Rather than treating communication as the transmission of static symbols, quantum communication views it as a dynamic process constrained by the behavior of quantum systems. The development of this field marks not just a technical advancement, but a conceptual shift: it reframes the process of information transfer in light of the most fundamental laws of nature.

As quantum theory emerged in the early 20th century, it uncovered types of correlations between systems that could not be accounted for by classical theories. In classical physics, correlations are typically attributed to shared causes or inherent proper-

ties of the systems. However, quantum mechanics permits states where subsystems remain fundamentally interconnected, even when separated by vast distances. This phenomenon, which Erwin Schrödinger later referred to as 'entanglement,' posed significant challenges to traditional concepts of locality, realism, and causality [4]. The foundational debate initiated by the Einstein–Podolsky–Rosen (EPR) paper in 1935 questioned whether quantum mechanics offers a complete description of physical reality. The EPR argument questioned whether quantum mechanics could be considered a complete physical theory, suggesting that the theory's allowance for distant, instantaneous correlations implied the existence of "elements of reality" not captured within the quantum formalism [5].

The theoretical landscape shifted dramatically with John Bell's theorem in 1964, which demonstrated that no local hidden variable theory could fully replicate the predictions of quantum mechanics [6]. The subsequent decades saw a surge of experimental efforts to test Bell's predictions. In a pioneering study, Freedman and Clauser reported violations of Bell inequalities in measurements on entangled photon pairs [7]. These results were followed by more sophisticated experiments, such as those conducted by Aspect and colleagues in the early 1980s, which addressed critical loopholes and further solidified Bell nonlocality as an empirically established feature of quantum systems [8,9].

In addition to spatial correlations, it was also discovered that quantum systems exhibit nonclassical behavior in individual measurements. The Kochen–Specker theorem (1967) [10] revealed that the outcome of a measurement can depend on the context in which it is conducted, a feature known as quantum contextuality [11]. Unlike entanglement or Bell nonlocality, which depend on spatial separation, contextuality challenges classical realism without requiring spatial separation. Over time, the concept of contextuality has been generalized beyond projective measurements to encompass more comprehensive operational scenarios, particularly through the framework introduced by Spekkens, which allowed for a deeper understanding of nonclassical behavior in practical settings. Together, entanglement, Bell nonlocality, and contextuality have become integral to the foundations of quantum theory, not only as abstract theoretical concepts but as essential principles for quantum communication and infor-

mation processing.

The foundational concepts of entanglement, nonlocality, and contextuality have transitioned from theoretical curiosities to operational resources within a wide range of quantum information tasks. These distinct quantum characteristics enable novel communication and computational strategies that not only offer superior performance compared to classical methods but also allow for the realization of functionalities that are fundamentally impossible to achieve using classical systems. The translation of fundamental nonclassical phenomena into practical tools has led to the development of an active field of study focused on quantum information theory tasks, encompassing quantum key distribution and teleportation, as well as reducing communication complexity and encoding contextual information.

A fundamental breakthrough in harnessing quantum correlations was realized through the protocol of quantum teleportation, which allows the remote reconstruction of an unknown quantum state without physically transferring the particle, contingent on the prior sharing of entanglement and the exchange of classical information [12]. While the original protocol was developed for discrete variables, recent advances have extended its reach using continous variable system [13, 14], hybrid systems [15, 16].

Another significant class of communication tasks in quantum information theory is represented by quantum random access codes (QRACs), which exemplify the quantum advantage in scenarios constrained by limited communication resources. In a standard QRAC protocol, a sender is provided with a string of classical bits and is allowed to encode this information into a single qubit. The receiver, upon receiving the qubit, attempts to recover any one of the original bits, chosen uniformly at random, with a probability of success exceeding that achievable by any classical strategy constrained to the same communication limit [17]. Recently, QRACs have been studied as a means to demonstrate the quantum advantage in communication using minimal resources. This exploration has led to significant improvements in foundational issues [18, 19], as well as in practical applications, such as Noise-Resilient QRACs [20], two-instance random access codes [21], high-dimensional QRACs [22, 23], and biased random access codes [24], among others.

Alongside the foundational exploration of quantum nonlocality, the operational de-

ployment of quantum correlations in secure communication has evolved rapidly. One particularly notable direction is device-independent quantum key distribution (DI-QKD), which establishes cryptographic security based solely on observed statistical violations of Bell inequalities, removing the need to trust internal details of the devices used. This paradigm, grounded in the concept of self-testing, addresses vulnerabilities in practical implementations of standard QKD. As the field progresses, DI-QKD protocols have undergone major refinements by optimizing efficiency, tolerating higher noise, and expanding into high-dimensional systems. Recent research has introduced schemes based on prepare-and-measure frameworks, high-dimensional entanglement, and new nonlocal games that enable secure key generation even under minimal assumptions and imperfect detection. Over the last few years, DI-QKD has seen substantial theoretical development. Notably, DI-QKD Based on Routed Bell Tests [25], DI-QKD with local Bell test [26], DI-QKD with random postselection [27] and so on. On the experimental side, DI-QKD has achieved a major experimental milestone through the successful implementation of the Twin-Field QKD protocol over 1,002 kilometers of optical fiber [28]. Another major breakthrough in the experimental development of device-independent quantum key distribution (DI-QKD) has been the demonstration of a complete device-independent protocol over a separation of 400 meters between two users [29]. These accomplishments collectively mark a crucial step toward the practical realization of DI-QKD in large-scale quantum communication networks.

Beyond Bell nonlocality, generalized contextuality has emerged as a powerful resource in quantum information processing. The generalized notion of contextuality, particularly in the framework of prepare-and-measure experiments, has proven to be instrumental in enabling advantages unique to quantum systems, notably in generating certified randomness, lowering communication complexity, and enhancing state discrimination capabilities. Recent studies have made significant foundational advances in contextuality [30–33], while also expanding its application to areas such as quantum computing [34], quantum metrology [35], and communication complexity [36]. These developments have broadened the understanding of quantum advantage, moving beyond entanglement-based models and highlighting a richer structure

of nonclassicality in communication protocols.

This thesis is structured as follows:-

Chapter 2:- Chapter 2 provides a recapitulation of the mathematical and physical prerequisites essential for grasping the contents of the thesis. It contains a preliminary outline of quantum correlations, including entanglement, Bell nonlocality, and generalized contextuality. It also provides an overview of selected quantum communication tasks such as quantum random access codes, device-independent quantum key distribution, and quantum teleportation.

Chapter 3:- This chapter delves into the foundational basis of the quantum advantage observed in random access codes. We formulate a new class of temporal inequalities that comply with noninvasive realist frameworks. It is shown that a quantum enhancement, however small, in the $n \mapsto 1$ random access coding task, even when shared randomness is permitted, necessarily implies a violation of the corresponding temporal constraint. From this connection, it follows that the optimal quantum success rate is realized precisely when the related inequality is violated to its maximum extent. Furthermore, we demonstrate that either a non-zero quantum advantage or a measurable violation of the temporal inequality serves as an indicator of genuine quantum randomness.

Chapter 4:- Within this chapter, we generate Haar-distributed random quantum states of rank ranging from 1 to 4, and evaluate their effectiveness in entanglement-assisted quantum key distribution protocols, focusing specifically on two-qubit systems for DI-QKD. Our findings reveal that both entanglement and Bell nonlocal correlations diminish with increasing rank. However, the reduction in the achievable key rate is more pronounced than the loss of quantum correlations. Furthermore, we identify that pure states and Werner states serve as reference points, setting lower and upper thresholds on the secret key rate for mixed two-qubit states possessing the same level of entanglement, both under general and optimal collective attack scenarios.

Chapter 5:- Throughout this chapter, we propose a scheme to efficiently extract quantum advantage through construction of a generalized noncontextual polytope circumscribing both the preparation and measurement noncontextual polytopes, while ensuring that its dimension stays constant irrespective of the number of measurements

and outcomes. The facet inequalities of our constructed polytope can thus be obtained in a computationally efficient manner, serving as necessary conditions for generalized noncontextuality. We illustrate the efficacy of our methodology through several distinct contextuality scenarios. Our approach enables to uncover several hitherto unexplored noncontextuality inequalities and demonstrating applications of quantum contextuality.

Chapter 6:- This chapter explores the distribution of nonlocal correlations in Bell-type states between two distant parties by utilizing optical hybrid entanglement, which merges single-photon polarization modes with multiphoton coherent states. By performing entanglement swapping at an intermediate relay station on the coherent-state components, we demonstrate that such hybrid systems can effectively generate polarization-entangled states capable of violating the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality across distances comparable to those encountered in metropolitan-scale networks. Furthermore, we evaluate the usefulness of the resulting entangled states in a practical quantum information protocol, namely the teleportation of an unknown polarization qubit. Incorporating realistic experimental constraints such as detector inefficiencies and transmission losses, our analysis confirms the feasibility of achieving high-fidelity quantum teleportation over significant distances, aligned with the strength of the underlying nonlocal correlations.

Chapter 7:- Finally, Chapter 7 provides a summary of the key findings of the thesis, along with reflections on potential future research directions.

CHAPTER 2

SOME PRE-REQUISITES OF QUANTUM THEORY

This chapter lays the foundational framework essential for understanding the various phenomena and protocols explored throughout this thesis. Under the broad theme of quantum theory, the discussion begins with a review of its fundamental postulates, forming the conceptual and mathematical basis for all quantum processes. Building upon these principles, the chapter delves into different forms of quantum correlations, including entanglement, Bell nonlocality, and generalized contextuality—as these nonclassical features play a pivotal role in enabling communication tasks that surpass classical limits. The latter part of the chapter focuses on key quantum communication protocols that leverage these nonclassical features, such as quantum random access codes, device-independent quantum key distribution, and quantum teleportation. Together, these topics provide a comprehensive backdrop for the more specialized investigations presented in the subsequent chapters.

2.1 Postulates of Quantum Mechanics

Postulate 1:

A quantum system is characterized by a mathematical object known as the state vector, which exists within a complex vector space called Hilbert space[1] $\mathcal{H}$. This vector contains all possible information about the system.

In mathematical terms, if a quantum system is in a pure state, it is represented as a normalized vector in a Hilbert space:

$$|\psi\rangle \in \mathcal{H}, \quad \text{with } \langle\psi|\psi\rangle = 1. \tag{2.1}$$

In the Dirac notation:

- The quantum state of a system is mathematically represented by a vector $|\psi\rangle$ in a complex Hilbert space.
- The **dual vector** (or bra) $\langle\psi|$ is its conjugate transpose.
- The inner product $\langle\psi|\phi\rangle$ represents the overlap between states $|\psi\rangle$ and $|\phi\rangle$.
- The norm $||\psi||^2 = \langle\psi|\psi\rangle = 1$ ensures unit probability.

Quantum states can be broadly classified into *pure states* and *mixed states*. A *pure state* represents a system with maximum knowledge of its quantum properties. This state vector $|\psi\rangle$ resides in a Hilbert space and may be written as a superposition of orthonormal basis:

$$|\psi\rangle = \sum_i c_i |e_i\rangle, \tag{2.2}$$

Here, $\{|e_i\rangle\}$ constitutes an orthonormal set spanning the Hilbert space, and the coefficients $c_i \in \mathbb{C}$ fulfill the normalization condition $\sum_i |c_i|^2 = 1$.

A *mixed state* refers to a probabilistic combination of pure states, and it is characterized by a density matrix ρ:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{2.3}$$

[1] A **Hilbert space** $\mathcal{H}$ is a complex vector space equipped with an inner product $\langle\psi|\phi\rangle$, which allows us to compute probabilities and define orthonormal bases.

where p_i are probabilities satisfying $\sum_i p_i = 1$.

Key properties of ρ:

- **Hermitian:** $\rho^\dagger = \rho$.
- **Positive Semi-definite:** $\langle\psi|\rho|\psi\rangle \geq 0, \forall\, |\psi\rangle$ or, all eigenvalues of ρ are real and non-negative.
- **Unit Trace:** $\mathrm{Tr}(\rho) = 1$.
- For a pure state, $\rho^2 = \rho$ and it holds that $\mathrm{Tr}(\rho^2) = 1$; for a mixed state, $\rho^2 \neq \rho$ and it follows that $\mathrm{Tr}(\rho^2) < 1$.

A *qubit* serves as the basic building block of quantum information theory and is mathematically described within a two-dimensional complex Hilbert space $\mathbb{C}^2$. It corresponds to a quantum system with two accessible levels, where any valid state can be written as a linear combination:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.4}$$

with $|0\rangle, |1\rangle$ forming an orthonormal basis. The complex amplitudes α and β must satisfy the normalization requirement:

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2.5}$$

The corresponding density matrix for a qubit is:

$$\rho = |\psi\rangle\langle\psi| = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix}. \tag{2.6}$$

A single qubit state can be represented on the Bloch sphere, where any pure state of a qubit can be rewritten as:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle, \tag{2.7}$$

where θ, ϕ are real parameters that define a point on the unit sphere. The Bloch vector

r is given by:

$$\mathbf{r} = (r_x, r_y, r_z) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta), \tag{2.8}$$

and the density matrix of a qubit can be expressed using its Bloch vector as:

$$\rho = \frac{1}{2}(\mathbb{I} + \mathbf{r}\cdot\sigma), \tag{2.9}$$

where $\mathbb{I}$ denotes the identity operator, $\sigma = (\sigma_x, \sigma_y, \sigma_z)$ refers to the set of Pauli operators, and **r** is a real-valued Bloch vector that satisfies the condition $||\mathbf{r}|| \leq 1$.

Bloch Sphere Interpretation:

- **Pure states** correspond to points on the surface of the sphere ($||\mathbf{r}|| = 1$).
- **Mixed states** correspond to points inside the sphere ($||\mathbf{r}|| < 1$).
- **Maximally mixed state** (completely depolarized state) corresponds to the center of the sphere $\mathbf{r} = 0$:

$$\rho = \frac{\mathbb{I}}{2}. \tag{2.10}$$

Postulate 2:

The second postulate of quantum mechanics asserts that the time evolution of an isolated quantum system is governed by a deterministic unitary process. This evolution is described by the time-dependent Schrödinger equation:

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = \hat{H}|\psi(t)\rangle, \tag{2.11}$$

where $|\psi(t)\rangle$ represents the quantum state at time t, $\hbar$ is the reduced Planck constant, and $\hat{H}$ denotes the Hamiltonian operator corresponding to the total energy of the system.

Since the Schrödinger equation is linear, its solution can be expressed using the time evolution operator $\hat{U}(t)$, which acts on the initial state:

$$|\psi(t)\rangle = \hat{U}(t)|\psi(0)\rangle, \tag{2.12}$$

where the time evolution operator is given by:

$$\hat{U}(t) = e^{-i\hat{H}t/\hbar}. \tag{2.13}$$

The time-evolution operator $\hat{U}(t)$ is unitary, implying that inner products between quantum states are conserved under evolution, and the overall probability associated with the state remains unity:

$$\hat{U}^{\dagger}(t)\hat{U}(t) = I. \tag{2.14}$$

Understanding this postulate provides the foundation for studying quantum dynamics, energy measurements, and interactions with external influences.

Postulate 3:

Measurements occupy a foundational role in quantum mechanics, as they directly influence the outcomes of experimental observations. The third postulate lays out the formal mathematical framework and principles that define how quantum measurements are modeled and interpreted.

Consider a quantum system is characterized by a vector $|\psi\rangle$ that is normalized and resides within the system's corresponding Hilbert space $\mathcal{H}$. A measurement is characterized by a set of measurement operators $\{M_m\}$, indexed by the measurement outcomes m, acting on $\mathcal{H}$. The probability that the outcome m occurs upon measuring the system in state $|\psi\rangle$ is given by:

$$P(m) = \langle\psi| M_m^{\dagger} M_m |\psi\rangle . \tag{2.15}$$

After obtaining the outcome m, the post-measurement state of the system collapses to:

$$|\psi_m\rangle = \frac{M_m |\psi\rangle}{\sqrt{P(m)}}, \quad P(m) > 0. \tag{2.16}$$

The measurement operators $\{M_m\}$ must satisfy the **completeness relation**:

$$\sum_m M_m^{\dagger} M_m = \mathbb{I}, \tag{2.17}$$

where $\mathbb{I}$ is the identity operator on $\mathcal{H}$. This condition ensures that the total probability of all possible outcomes sums to 1.

There are two important classes of quantum measurements: Projective Measurements and Positive Operator-Valued Measurements (POVMs).

Projective Measurements: Projective measurements, also called von Neumann measurements, are associated with Hermitian observables. Let A be a Hermitian operator representing an observable, with spectral decomposition, $A = \sum_i a_i P_i$, where each a_i is a real root of the characteristic equation of A, and P_i denotes an orthogonal projector linked to the eigenspace associated with that root. Each projector satisfies the relations: $P_i = P_i^\dagger$ (Hermiticity), $P_i^2 = P_i$ (idempotency), and $P_i P_j = \delta_{ij} P_i$ (orthogonality for $i \neq j$). The set of projectors also obeys the completeness condition: $\sum_i P_i = \mathbb{I}$.

When measuring the observable A in the state $|\psi\rangle$, the probability of obtaining outcome a_i is given by $P(a_i) = \langle\psi| P_i |\psi\rangle$.
After obtaining this result, the system collapses to the normalized post-measurement state

$$|\psi'\rangle = \frac{P_i |\psi\rangle}{\sqrt{P(a_i)}}. \tag{2.18}$$

Projective measurements represent an idealized measurement scenario and are a special case of the general measurement formalism.

Positive Operator-Valued Measurements (POVMs): POVMs extend the notion of standard projective measurements by introducing a more flexible framework. They consist of a collection of positive semi-definite operators E_m, often referred to as the elements of the measurement, that obey the normalization condition: $\sum_m E_m = \mathbb{I}$. Each operator E_m is associated with a potential measurement result and satisfies $E_m \geq 0$, ensuring that for any state $|\phi\rangle \in \mathcal{H}$, the quantity $\langle\phi| E_m |\phi\rangle$ is non-negative. Unlike projectors used in von Neumann measurements, these operators are not necessarily orthogonal or idempotent.

For a system characterized by a density matrix ρ, the probability of measuring outcome m is computed as, $P(m) = \mathrm{Tr}(\rho E_m)$. Although the POVM elements E_m determine the measurement statistics, the specific post-measurement state depends on the physical implementation and cannot be uniquely inferred from the POVM alone.

If a realization of the POVM involves a set of measurement operators $\{M_m\}$ such that $E_m = M_m^\dagger M_m$, then the post-measurement state (given outcome m) is

$$\rho' = \frac{M_m \rho M_m^\dagger}{\mathrm{Tr}(M_m \rho M_m^\dagger)}. \tag{2.19}$$

POVMs are crucial when dealing with imperfect measurement devices or environmental interactions, thus making them particularly important within the realm of quantum information processing and communication.

Postulate 4:

In the realm of quantum mechanics, the representation of a physical system consisting of multiple subsystems is determined by the tensor product structure within Hilbert spaces. The fourth postulate in quantum theory defines the construction of the state space for *composite systems*, as well as how measurements and dynamics are applied to such systems.

Consider a physical system made up of two distinct parts, labeled A and B each associated with its respective Hilbert space, $\mathcal{H}_A$ and $\mathcal{H}_B$. The overall Hilbert space representing the combined system is constructed using the tensor product of these individual spaces:

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B. \tag{2.20}$$

More generally, for n subsystems, the total Hilbert space is

$$\mathcal{H}_{\text{total}} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n. \tag{2.21}$$

The state of the combined system is represented by a density operator ρ_{AB}, which operates on the tensor product space $\mathcal{H}_A \otimes \mathcal{H}_B$. This density matrix must be a positive semi-definite operator with a trace equal to one.
The most general form of a two-qubit mixed state ρ_{AB} can be expressed using the Bloch representation as:

$$\rho_{AB} = \frac{1}{4}\left(\mathbb{I} \otimes \mathbb{I} + \sum_{i=1}^{3} a_i \, \sigma_i \otimes \mathbb{I} + \sum_{j=1}^{3} b_j \, \mathbb{I} \otimes \sigma_j + \sum_{i,j=1}^{3} T_{ij} \, \sigma_i \otimes \sigma_j\right), \tag{2.22}$$

where, σ_i and σ_j are the Pauli matrices acting on systems A and B respectively, $\vec{a} = (a_1, a_2, a_3)$ and $\vec{b} = (b_1, b_2, b_3)$ are the Bloch vectors of the reduced states ρ_A and ρ_B, and $T_{ij} = \mathrm{Tr}(\rho_{AB}\sigma_i \otimes \sigma_j)$ is the correlation matrix.

Measurement and Reduced States: Measurement on a composite system can be global (acting on the full Hilbert space) or local (acting on a subsystem). For example, a measurement on subsystem A corresponds to applying an operator of the form $M_A \otimes I_B$, where M_A acts on $\mathcal{H}_A$ and I_B is the identity on $\mathcal{H}_B$.

To describe the state of a subsystem, one uses the concept of the *partial trace*. Given a composite state ρ_{AB}, the reduced state of subsystem A is defined as: $\rho_A = \mathrm{Tr}_B(\rho_{AB})$, where the trace is taken over the degrees of freedom of subsystem B. This operation preserves positivity and normalization, and ensures that the reduced state ρ_A is a valid density operator on $\mathcal{H}_A$.

2.2 Quantum Correlations

2.2.1 Entanglement

Quantum entanglement represents a core feature of quantum theory, reflecting non-classical correlations between parts of a composite system that defy explanation through classical means.

We have already mentioned in the previous section that if two subsystems, A and B, have individual Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, then the total system is represented in the joint Hilbert space: $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.

A general pure state in this composite space is given by:

$$|\psi\rangle_{AB} = \sum_{i,j} c_{ij} |i\rangle_A \otimes |j\rangle_B , \tag{2.23}$$

where $\{|i\rangle_A\}$ and $\{|j\rangle_B\}$ form orthonormal bases for their respective subsystems, and c_{ij} are complex coefficients.

A separable state in a bipartite system can be written as a direct product:

$$|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\chi\rangle_B , \tag{2.24}$$

where $|\phi\rangle_A$ and $|\chi\rangle_B$ are pure states of the individual subsystems. However, if such a decomposition is not possible, the state is said to be **entangled**.

A widely used method to analyze entanglement is the Schmidt decomposition [37], which expresses a bipartite state as:

$$|\psi\rangle_{AB} = \sum_k \lambda_k |u_k\rangle_A \otimes |v_k\rangle_B , \tag{2.25}$$

where λ_k are non-negative Schmidt coefficients, and $\{|u_k\rangle_A\}$ and $\{|v_k\rangle_B\}$ form orthonormal bases for A and B, respectively. If only one Schmidt coefficient is nonzero, the state is separable; otherwise, it is entangled.

For mixed states, the system is described by a density matrix, a separable mixed state can be written as:

$$\rho_{AB} = \sum_i p_i \rho_A^{(i)} \otimes \rho_B^{(i)}, \tag{2.26}$$

where p_i are probabilities and $\rho_A^{(i)}$ and $\rho_B^{(i)}$ are density matrices of the subsystems. If such a decomposition is not possible, the state is entangled.

One of the most common for identifying entanglement in bipartite quantum systems, particularly in a qubit-qubit ($\mathbb{C}^2 \otimes \mathbb{C}^2$) or qubit-qutrit ($\mathbb{C}^2 \otimes \mathbb{C}^3$) system, is the Peres-Horodecki positive partial transposition (PPT) criterion [38, 39]. This condition asserts that a quantum state in these low-dimensional systems is entangled if and only if its partial transposition possesses at least one negative eigenvalue.

A well-known example of maximally entangled states are the Bell states, given by:

$$\left|\Phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \tag{2.27}$$

$$\left|\Psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \tag{2.28}$$

These states exhibit maximum entanglement, meaning that measuring one qubit instantly determines the state of the second qubit, even if they are physically distant.

2.2.2 Bell-nonlocality

Local Realism and Bell's Theorem: The concept of *local realism* is central to classical physics and refers to two fundamental assumptions:

- *Realism:* The properties of physical systems exist independently of measurement.
- *Locality:* Measurement outcomes at one location cannot instantaneously influence a distant system beyond the speed of light.

These assumptions lead to *local hidden variable (LHV) models*, which attempt to explain correlations observed in experiments using pre-existing but unknown (hidden) variables [6].

Mathematical Formulation of Local Hidden Variable Models:
Consider a scenario where two spatially separated observers, Alice and Bob, share a quantum system. Each observer can independently choose a measurement setting and obtain an outcome. Alice selects a measurement setting denoted by x and obtains an outcome A. Bob selects a measurement setting denoted by y and obtains an outcome B.

The joint probability distribution $P(A, B \mid x, y)$ quantifies the likelihood of observing outcomes x and y when measurements corresponding to inputs A and B are performed. In the framework of a local hidden variable (LHV) model, this probability is mediated by a shared hidden variable λ, distributed according to a probability density $\rho(\lambda)$. Imposing locality leads to the condition:

$$P(A, B \mid x, y) = \int \rho(\lambda)\, P(A \mid x, \lambda)\, P(B \mid y, \lambda) d\lambda. \tag{2.29}$$

Here, λ represents the hidden variable(s), which encapsulate pre-existing information about the system. The probability distribution of the hidden variable is given by $\rho(\lambda)$, satisfying the normalization condition $\int \rho(\lambda) d\lambda = 1$. The term $P(A|x, \lambda)$ denotes the probability that Alice observes outcome x, given her measurement setting A and the hidden variable λ. Similarly, $P(B|y, \lambda)$ denotes the probability that Bob observes outcome y, given his measurement setting B and the value of the hidden variable λ.

This equation reflects the factorization assumption, stating that upon fixing the hidden variable λ, the statistical results obtained by Alice and Bob are no longer interdependent and emerge independently. This reflects both *realism* (outcomes are predetermined) and *locality* (no faster-than-light influence between Alice and Bob).

Implications of Local Realism: The factorization condition imposes strict constraints on the types of correlations that can exist between Alice and Bob's measurements. These constraints lead to **Bell inequalities**, which any LHV model must satisfy. If experimental data violates a Bell inequality, it indicates that at least one of the assumptions, either realism or locality, must be incorrect.

The *Clauser-Horne-Shimony-Holt (CHSH) inequality* is one of the most commonly studied Bell inequalities. It applies to a bipartite quantum system where two spatially separated observers, Alice and Bob, perform measurements on a shared quantum state. Each observer has access to two measurement settings: Alice is assigned the measurement settings $\{A_0, A_1\}$, while Bob is associated with the settings $\{B_0, B_1\}$. Each measurement yields binary outcomes ± 1. The CHSH correlation function is defined as:

$$\mathcal{B} = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle, \tag{2.30}$$

where $\langle A_i B_j \rangle$ denotes the statistical average obtained by multiplying the outcomes recorded by Alice and Bob during the execution of measurements A_i and B_j.

Within any local hidden variable theory, the **CHSH inequality** holds:

$$|\mathcal{B}| \leq 2. \tag{2.31}$$

In quantum mechanics, Alice and Bob perform measurements on a shared quantum state, typically the maximally entangled Bell state. Each observer can choose quantum mechanical operators that maximize Bell violations must be *incompatible* i.e., they must *not commute*, ensuring that Alice and Bob's measurements introduce intrinsic quantum uncertainty.

The optimal choice of measurement observables that maximizes the CHSH expression is:

$$A_0 = \sigma_z, \quad A_1 = \sigma_x, \tag{2.32}$$

$$B_0 = \frac{\sigma_z + \sigma_x}{\sqrt{2}}, \quad B_1 = \frac{\sigma_z - \sigma_x}{\sqrt{2}}, \tag{2.33}$$

where σ_x and σ_z are Pauli matrices.

The expectation values of these operators, when evaluated on the Bell state, lead to the quantum mechanical upper bound:

$$\mathcal{B}_{\max} = 2\sqrt{2}. \tag{2.34}$$

These measurements correspond to different bases on the Bloch sphere, ensuring they are *mutually unbiased* and do not commute. This *incompatibility* is crucial for achieving the maximal Bell violation. If Alice's and Bob's measurements were *compatible* (i.e., commutative), then they would admit a classical LHV description, and Bell inequality violations would not occur.

Feature	Effect on Bell Violation
Commuting Observables ($[A, B] = 0$)	No Bell violation (LHV model possible)
Partially Incompatible Observables ($[A, B] \neq 0$, but suboptimal angles)	Bell violation, but not maximal
Maximally Incompatible Observables (e.g., MUBs)	Maximum Bell violation ($2\sqrt{2}$)

Table 2.1: Effect of Measurement Incompatibility on Bell Violation

The Bell-CHSH expression has an algebraic upper bound of 4. However, quantum mechanics does not permit any combination of quantum states and measurements to attain this maximum value. Instead, the highest quantum violation achievable is limited to $2\sqrt{2}$, a restriction known as Cirelson's bound [40]. This violation directly contradicts local realism, confirming the **nonlocal nature** of quantum correlations.

2.2.3 Generalized Contextuality

Generalized noncontextuality [41] is the logical conjunction of preparation and measurement noncontextuality in scenarios associated with prepare and measure experiments. Analogous to Bell inequality, generalized noncontextuality implies empirical inequalities, referred to as (generalized) noncontextuality inequalities (NCI). Quantum theory prescribes preparations and measurements, which, while satisfying the operational indistinguishable conditions, violate NCI. A contextuality scenario is specified

by the number of preparations, measurements, and measurement outcomes, as well as the operational indistinguishability conditions between preparation and measurement procedures corresponding to their distinct convex mixtures, respectively. Given a contextuality scenario, finding a set of empirical criteria fulfilled by any noncontextual theory is a demanding task of both foundational and operational importance.

Consider, a prepare and measure experiment entailing several distinct preparation and measurement procedures. A preparation procedure is labelled by P_x, where x denotes the specific preparation, and a measurement procedure is denoted by $M_{z|y}$, where z and y represent the outcome and setting of the measurement, respectively. Using an operational theory, such as quantum theory, we can make predictions about the empirical statistics $\{p(z|x,y)\}$, where $p(z|x,y)$ indicates the probability of obtaining outcome z when the measurement specified by y is performed on the preparation specified by x. We say that two preparation procedures, P_x and $P_{x'}$, are operationally equivalent or indistinguishable (denoted as $P_x \sim P_{x'}$) if they yield identical outcome statistics for all measurements,

$$p(z|x,y) = p(z|x',y),\ \forall M_{z|y}. \tag{2.35}$$

Similarly, two measurement procedures $M_{z|y}$ and $M_{z'|y'}$ are operationally equivalent or indistinguishable (denoted as $M_{z|y} \sim M_{z'|y'}$), if they produce identical outcome statistics for all possible preparations

$$p(z|x,y) = p(z'|x,y'),\ \forall P_x. \tag{2.36}$$

Let us consider a prepare and measure experiment involving n_x distinct preparations as $x \in \{0,\ldots,n_x-1\}$ and n_y different measurements as $y \in \{0,\ldots,n_y-1\}$, with each measurement having n_z possible outcomes as $z \in \{0,\ldots,n_z-1\}$. In this experiment, we have a set of hypothetical preparations, each of which is realized by taking convex mixtures of these n_x preparations such that the resultant mixed preparations are indistinguishable. These mixed preparations are labeled by the variable

$s \in \{0, \ldots, n_s\}$ and they are realized by the set of convex coefficients $\{\alpha_{x|s}\}$, satisfying

$$\alpha_{x|s} \geqslant 0, \ \sum_x \alpha_{x|s} = 1, \forall x, s. \tag{2.37}$$

The indistinguishability conditions imply that for all $s, s' \in \{0, \ldots, n_s\}$,

$$\sum_x \alpha_{x|s} P_x \sim \sum_x \alpha_{x|s'} P_x. \tag{2.38}$$

It is important to note that the above set of indistinguishability conditions are taken to be *linearly independent*, meaning that no indistinguishability condition can be deduced from the other conditions. Mathematically, this requires the vectors $\{\vec{u}_s\}_s$ of these convex coefficients,

$$\vec{u}_s = \left(\alpha_{0|s}, \alpha_{1|s}, \cdots, \alpha_{n_x-1|s}\right)$$

to be an linearly independent set of vectors.

Similarly, we have indistinguishable measurement procedures labelled by $t \in \{0, \ldots, n_t\}$, each of them is realized by different taking convex mixtures with the coefficients $\{\beta_{z,y|t}\}$ satisfying

$$\beta_{z,y|t} \geqslant 0, \ \sum_{z,y|t} \beta_{z,y|t} = 1, \ \forall z, y, t. \tag{2.39}$$

Thereupon, these indistinguishability conditions on measurements can be expressed as

$$\sum_{z,y} \beta_{z,y|t} M_{z|y} \sim \sum_{z,y} \beta_{z,y|t'} M_{z|y}\,, \tag{2.40}$$

for all $t, t' \in \{0, \ldots, n_t\}$. Here also, we consider these indistinguishability conditions to be linearly independent, which requires the vectors

$$\vec{v}_t = \left(\beta_{0|t}, \beta_{1|t}, \cdots, \beta_{n_y-1|t}\right)$$

to form an linearly independent set of vectors. The number of preparations, measurements, and measurement outcomes, together with the set of linearly independent indistinguishability conditions, defines a *contextuality scenario*.

In quantum theory, preparations are described by density operators ρ_x, and measurements are described by positive semi-definite operators $\mathbb{M}_{z|y}$, satisfying $\sum_z \mathbb{M}_{z|y} = \mathbb{1}$, where $\mathbb{1}$ is the identity operator. The probability of obtaining outcome z when performing measurement $M_{z|y}$ on preparation P_x is given by $p(z|x,y) = \mathrm{Tr}(\rho_x \mathbb{M}_{z|y})$. Furthermore, quantum preparations and measurements satisfy the indistinguishability conditions given by (2.38) and (2.40) if and only if the following equalities hold:

$$\sum_x \alpha_{x|s}\, \rho_x = \sum_x \alpha_{x|s'}\, \rho_x\ , \quad \forall s, s' \in \{0, \ldots, n_s\}. \tag{2.41}$$

and

$$\sum_{z,y} \beta_{z,y|t} \mathbb{M}_{z|y} = \sum_{z,y} \beta_{z,y|t'} \mathbb{M}_{z|y}\ , \ \forall t, t' \in \{0, \ldots, n_t\}. \tag{2.42}$$

An ontological model offers an explanation to the prediction of an operational theory by considering the state of the system to be an objective reality. This state is called the *ontic state* of the system, denoted by $\lambda \in \Lambda$, where Λ is an arbitrary measurable space referred to as the ontic state space. A preparation procedure P_x prepares the system in an ontic state λ with probability $\mu(\lambda|x)$. The distribution $\mu(\lambda|x)$ is known as the epistemic description associated with the system's configuration. In the context of measurement, the probability of obtaining outcome z is described by the response function $\xi(z|\lambda, y)$, where $M_{z|y}$ acts on the underlying ontic state λ. An ontological model satisfying the generalized notion of noncontextuality assigns identical epistemic states to indistinguishable mixed preparations and identical response functions to indistinguishable mixed measurement procedures [41]. More precisely, the indistinguishability conditions (2.38) and (2.40) in any noncontextual ontological model imply

$$\sum_x \alpha_{x|s} \mu(\lambda|x) = \sum_x \alpha_{x|s'} \mu(\lambda|x), \tag{2.43}$$

for all $s, s' \in \{0, \ldots, n_s\}$ and

$$\sum_{z,y} \beta_{z,y|t} \xi(z|\lambda, y) = \sum_{z,y} \beta_{z,y|t'} \xi(z|\lambda, y), \tag{2.44}$$

for all $t, t' \in \{0, \ldots, n_t\}$, pertaining to every λ. An operational theory is called noncontextual if its predictions can be explained by a noncontextual ontological model.

Given a contextuality scenario, the set of empirical probabilities $\{p(z|x,y)\}$ obtained from any noncontextual operational theory forms a polytope [42]. A general form of a facet inequality of the noncontextual polytope is given by

$$\sum_{x,y,z} c_{x,y,z}\ p(z|x,y) \leqslant \mathcal{C}, \tag{2.45}$$

where $c_{x,y,z}$ are real coefficients and $\mathcal{C}$ is the noncontextual bound. An operational theory whose predictions violate such inequalities is said to be contextual. There exists $\{p(z|x,y)\}$ predicted by quantum theory that violates such inequalities in general.

2.3 Quantum Communication Tasks

2.3.1 Quantum Random Access Codes

Random Access Codes (RACs) play a crucial role in information theory and communication complexity, facilitating the efficient transmission of data in scenarios where resources are constrained. In the RAC protocol, the sender (Alice) converts an n-bit message into a shorter m-bit string, where m is less than n, and then sends this encoded message to the receiver (Bob). Upon receiving the encoded message, Bob randomly selects an index $i \in \{1, 2, \ldots, n\}$ and attempts to retrieve the bit x_i corresponding to that index with a high probability. The efficiency of an RAC is characterized by the probability of Bob successfully decoding the requested bit [43–47].

Mathematically, an RAC satisfies the condition:

$$P(x_i|E(x), i) \geq p, \quad \forall x, i, \tag{2.46}$$

where $P(x_i|E(x), i)$ denotes the probability of correctly retrieving x_i, and p represents the minimum success probability of the decoding process. The parameter p is a measure of the reliability of the RAC, and its value depends on the encoding strategy employed. $E(x)$ represents the encoding function that maps the classical input x (which consists of multiple bits) into a smaller-dimensional representation.

Classical RACs are fundamentally constrained by information-theoretic limits, mak-

ing it challenging to retrieve individual bits with high probability when m is significantly smaller than n. However, the advent of Quantum Random Access Codes (QRACs) has introduced quantum mechanical techniques that surpass these classical limitations by leveraging quantum superposition and non-orthogonality of quantum states.

Classical Random Access Codes: A classical $n \to m$ RAC is characterized by an encoding function:

$$E : \{0,1\}^n \to \{0,1\}^m, \tag{2.47}$$

where Alice encodes her message $x = (x_1, x_2, ..., x_n)$ into an m-bit string $E(x)$. Bob, upon receiving $E(x)$, applies a decoding function:

$$D(E(x), i) = x_i, \quad \forall E(x) \in \{0,1\}^m, \quad \forall i \in \{1, 2, \ldots, n\} \tag{2.48}$$

which allows him to infer the desired bit x_i.

The probability of Bob successfully retrieving x_i is given by:

$$P_{\text{succ}} = \frac{1}{n} \sum_{i=1}^{n} \Pr[D(E(x), i) = x_i]. \tag{2.49}$$

Here, P_{succ} quantifies the success probability across all possible indices i, with the performance of RACs depending on the encoding efficiency and constraints of the communication channel.

Since classical RACs rely solely on classical encoding and retrieval mechanisms, they are limited by classical information-theoretic bounds. The challenge increases as m becomes significantly smaller than n, leading to lower success probabilities.

Quantum Random Access Codes: The limitations of classical RACs can be overcome using Quantum Random Access Codes (QRACs), which exploit the unique properties of quantum mechanics to enhance encoding and decoding efficiency. Instead of encoding information into classical bits, Alice encodes the n-bit message into an m-qubit quantum state ρ_x within a Hilbert space of dimension d. The encoding function in a QRAC is:

$$E : \{0,1\}^n \to \mathcal{H}_d, \tag{2.50}$$

where $\mathcal{H}_d$ is a d-dimensional Hilbert space, and the encoded message is represented by a density matrix ρ_x.

Upon receiving the quantum state ρ_x, Bob applies a quantum measurement operation corresponding to his chosen index i to extract the bit x_i. The probability of Bob successfully decoding the requested bit is:

$$P_{\text{succ}} = \frac{1}{n} \sum_{i=1}^{n} \text{Tr}(M_{i,x_i} \rho_x), \tag{2.51}$$

Where, M_{i,x_i} represents the measurement operator associated with Bob's choice of index i.

The quantum advantage in QRACs stems from the non-orthogonality of quantum states, quantum superposition, and mutually unbiased measurements, which allow more efficient encoding than classical RACs. This results in a higher probability of successful bit retrieval compared to classical methods. The improvement in QRACs is achieved through several key strategies, such as using quantum communication [45], or by transmitting classical bits with the help of a shared quantum state [48–51].

QRACs represent a significant quantum advantage in compressed information retrieval. By utilizing quantum states for encoding, QRACs surpass classical RACs in both efficiency and retrieval probability. Their applications span across quantum cryptography, communication complexity, and quantum computing. In chapter (3), we will provide rigorous mathematical formulations and explicit examples, to illustrate the power of quantum information processing in random access coding.

2.3.2 Device-Independent Quantum Key Distributions

Quantum Key Distribution (QKD) [52] enables two separated users, commonly referred to as Alice and Bob, to establish a shared encryption key whose security is inherently based on the fundamental principles of quantum physics. However, conventional QKD methods, such as the BB84 protocol [53] and the E91 protocol [54], rely on precise modeling of the quantum devices involved. This assumption poses a vulnerability: if the devices are imperfect or behave differently than expected, an adversary could exploit these flaws to compromise security. DI-QKD is based on the violation

of Bell inequalities, ensuring that the key distribution process does not rely on trust in the inner workings of quantum devices. Instead, security is guaranteed solely by nonlocal correlations between measurement outcomes. The fundamental concept is that when experimental correlations defy the bounds of a Bell-type inequality, it confirms the genuinely nonlocal nature of the quantum system, thereby eliminating the possibility of any eavesdropper having deterministic control over the outcomes. This significantly strengthens security compared to standard QKD, where device imperfections or adversarial tampering can compromise the key.
DI-QKD is based on the concept of quantum nonlocality, which is fundamentally tested through Bell inequalities. If Alice and Bob observe correlations that violate a Bell inequality, they can be assured that their shared quantum states exhibit nonlocal properties, which an eavesdropper cannot reproduce using classical resources.

In a typical DI-QKD setup:

• Alice and Bob share an entangled quantum state, usually a two-qubit maximally entangled Bell state,

• Each party performs local measurements on their respective qubits,

• The outcomes of these measurements are used to extract a secret key,

• The integrity of the generated key is assessed through the statistical violation of a Bell inequality.

The key assumption is that an adversary cannot reproduce quantum correlations beyond the local-hidden-variable limit while remaining undetected. Hence, a pronounced violation of a Bell inequality alone can act as a certification of the secrecy of the distributed key.

In chapter(4) of this thesis, we explore DI-QKD using random quantum states, based on an E91-like protocol, employing entangled states to ensure security through Bell inequality violations.

2.3.3 Quantum Teleportation

Quantum teleportation is a fundamental protocol in quantum information theory that enables the transfer of an unknown quantum state from one party to another without

physically transmitting the state itself. Unlike classical communication, which enables the direct transmission of information, quantum teleportation leverages *quantum entanglement* and *classical communication* to achieve perfect state transfer, in compliance with the *no-cloning principle* [55]. This technique has significant consequences for quantum computing, secure quantum communication, and distributed quantum networks.

The quantum teleportation protocol was first introduced by Bennett et al. [56], and it involves three fundamental resources:

1. **An entangled state** is distributed between the sender (Alice) and the receiver (Bob).

2. **A quantum measurement** performed by Alice on the system.

3. **Classical communication** from Alice to Bob is essential for completing the teleportation process.

The goal of teleportation is to transfer an *unknown qubit state* (2.4) from Alice to Bob. To initiate the teleportation protocol, Alice and Bob are assumed to possess a shared maximally entangled Bell state, as defined in Eq. (2.27). The complete three-step process is outlined below.

Step 1- Alice Performs a Bell Measurement:

Alice holds the unknown quantum state $|\psi\rangle$ along with her share of the entangled Bell pair. The overall state of the system (Alice's qubit and the entangled pair) can be expressed in the *Bell basis* as:

$$|\psi\rangle \otimes \left|\Phi^{+}\right\rangle_{AB} = (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{2.52}$$

Rewriting the expression in the Bell basis:

$$\begin{aligned}|\psi\rangle \otimes \left|\Phi^{+}\right\rangle = \frac{1}{2}\Big[&\left|\Phi^{+}\right\rangle (\alpha\,|0\rangle + \beta\,|1\rangle) + \left|\Phi^{-}\right\rangle (\alpha\,|0\rangle - \beta\,|1\rangle) + \left|\Psi^{+}\right\rangle (\alpha\,|1\rangle + \beta\,|0\rangle) \\ &+ \left|\Psi^{-}\right\rangle (\alpha\,|1\rangle - \beta\,|0\rangle)\Big].\end{aligned} \tag{2.53}$$

Alice now performs a *Bell measurement* on her pair of qubits, projecting them onto one of the entangled basis states such as $|\Phi^{\pm}\rangle$ and $|\Psi^{\pm}\rangle$. This operation results in

Bob's qubit collapsing into a corresponding state, depending on the outcome of Alice's measurement.

Step 2- Alice communicates classical information to Bob:

Since Bob's qubit is not identical to $|\psi\rangle$ but rather a transformed version, he needs to apply a correction based on Alice's measurement outcome. Alice sends two classical bits to Bob indicating which Bell state she obtained:

- If Alice measures $|\Phi^+\rangle$, Bob's state is already $|\psi\rangle$ (no correction needed).
- If Alice measures $|\Phi^-\rangle$, Bob's state is $\sigma_z |\psi\rangle$ (apply σ_z).
- If Alice measures $|\Psi^+\rangle$, Bob's state is $\sigma_x |\psi\rangle$ (apply σ_x).
- If Alice measures $|\Psi^-\rangle$, Bob's state is $\sigma_z\sigma_x |\psi\rangle$ (apply $\sigma_z\sigma_x$).

Step 3- Bob Applies a Corrective Operation:

Upon receiving Alice's two classical bits, Bob applies the appropriate Pauli correction operator:

$$U = \sigma_x^a \sigma_z^b, \tag{2.54}$$

where $a, b \in \{0, 1\}$ are determined by Alice's measurement. After this correction, Bob's qubit is exactly $|\psi\rangle$, achieving perfect teleportation.

Teleportation fidelity: The fidelity in quantum teleportation quantifies how efficiently and accurately the procedure replicates the original quantum state, based on the overlap between the transmitted state and the input state.
Teleportation fidelity is characterized by the degree of overlap between the initial quantum state $|\psi\rangle$ and the resulting teleported state ρ_{out}. Mathematically, it is expressed as:

$$F = \langle\psi| \rho_{\text{out}} |\psi\rangle . \tag{2.55}$$

Here, F lies in the range $0 \leq F \leq 1$, where: $F = 1$ represents perfect teleportation, meaning that the final state is exactly the same as the input state, $F < 1$ indicates imperfect teleportation, where some information is lost or altered due to experimental

imperfections.

A key aspect of quantum teleportation is that it outperforms classical strategies. If Alice and Bob were to use a purely classical communication scheme (without entanglement), the best possible strategy they could employ would yield a fidelity of at most $\frac{2}{3}$. This is known as the classical bound for teleportation fidelity. A fidelity exceeding $F > \frac{2}{3}$ is a clear indication of the quantum advantage [57], showing that the protocol utilizes quantum entanglement effectively. In ideal quantum teleportation, fidelity reaches $F = 1$, whereas in noisy conditions, it still remains above $\frac{2}{3}$ if entanglement is properly exploited.

CHAPTER 3

FUNDAMENTAL ORIGIN OF THE QUANTUM ADVANTAGE BEHIND RANDOM ACCESS CODE

3.1 Introduction

As mentioned in the previous chapter, Random Access Codes (RACs) are fundamental protocols in quantum communication that demonstrate the advantage of quantum systems over classical counterparts in certain information processing tasks.
RACs were introduced to illustrate the superior information-carrying capacity of quantum systems compared to classical systems of the same dimension. While the Holevo bound [58] establishes that a single qubit cannot reliably transmit more than one classical bit of information to a receiver, this limitation does not fully capture the potential of quantum encoding. An m-qubit system is mathematically represented as a unit

vector in a 2^m-dimensional complex Hilbert space, indicating that classical information can be encoded using exponentially fewer qubits. In general, Bob may not need to know the information of all n bits together, but rather may choose to extract some bits of classical information out of the encoding depending on some task and therefore, may explore some degrees of freedom which otherwise were frozen. This motivates to formulate the task of RAC without contradicting Holevo's result. Random access codes have been shown to possess wide range of applications such as quantum finite automata [44–46], network coding [59, 60], locally decodable codes [61–63], non-local games [64], dimension witness [65–68], quantum communication complexity [69–73], randomness certification [74], quantum cryptography [75], studies of no-signaling resources [76, 77], self-testing of quantum measurements [78], and so on.

The Bell theorem [6,79] establishes that correlations between spatially separated events are subject to stricter constraints in classical theory than in quantum mechanics. In contrast, for time-like separated events, two key no-go theorems—one based on non-contextual hidden variable models (NCVMs) [10, 80] and the other on macro-realism (MR) [81]—align with classical physics. Macro-realism, introduced by Leggett and Garg, serves as a framework to examine the quantumness of macroscopic systems. It is defined by two core principles: macro-realism per se, which asserts that a system always exists in a definite state, and noninvasive measurability, which states that it is possible, in principle, to determine the system's state without disturbing it [81–85]. A related variant, the non-invasive realist model, replaces macro-realism per se with a more general assumption of realism.

Quantum mechanics contradicts the predictions of both models. Specifically, the KCBS inequality, derived from NCVMs [86], and the Leggett-Garg inequality (LGI), which follows from MR [81], are both violated in quantum theory. In recent years, LGI and other forms of temporal correlations have drawn significant attention from both foundational research [85, 87–106] and practical applications [107–113]. For a comprehensive review, see [84, 85].

We consider the framework of the prepare and measure scenario (see, for instance, [114]). We propose new inequalities for temporal correlations arising from sequential

measurements and show that corresponding to every scenario of $n \mapsto 1$ RAC with SR there exists such an temporal inequality. Any quantum advantage of these communication tasks are implied by an associated violation of the derived temporal inequalities. These inequalities are asymmetric with respect to number of measurements. (For space-like separated correlations, asymmetric Bell inequalities were introduced to disprove the Peres conjecture [115].) Moreover, as an immediate consequence of our result, maximal violation of these temporal inequalities provide the maximal success probability of the corresponding RAC with SR. In general, maximal success probability of such RAC is derived numerically for $n \geq 1$ with unproven optimality [47]. Moving on, we find an important application of our scheme in a cryptographically primitive task, *viz.* randomness generation. We show that any non-zero quantum advantage of RAC can be used for certifying randomness, while all previously proposed protocols for randomness generation based on RAC do not generate genuine randomness for any arbitrary success probability. [74, 75, 116].

This chapter is organized as follows. In the next section 3.2, a preliminary discussion on $n \mapsto 1$ RAC is provided. In section 3.3, with the aim of designing operational criteria for testing RAC, temporal inequalities have been proposed for each $n \mapsto 1$ RAC. In section 3.4, it has been shown that any non-zero quantum advantage of $n \mapsto 1$ RAC can be used to generate genuine randomness. Finally, section 3.5 is reserved for summary and some concluding remarks.

3.2 Random Access Codes

3.2.1 $2 \mapsto 1$ RAC

In a $2 \mapsto 1$ RAC, Alice has an input string consisting of two bits $x_1x_2 \in \{00, 01, 10, 11\}$ which she wants to send to Bob by encoding the bits in a qubit $\rho_{x_1x_2}$. Bob's task is to guess one of the bits (which is again chosen randomly) reliably. Therefore, after receiving an input $y \in \{1, 2\}$, he performs a binary outcome measurement B_y and reports the outcome $\beta \in \{0, 1\}$ as his output. In this scenario, the average probability

of perfectly guessing the bit is given by

$$\mathbb{F}_{2\mapsto 1} = \frac{1}{8} \sum_{x_1,x_2,y} P(\beta_y = x_y \mid x_1, x_2, y). \tag{3.1}$$

Now consider the most general preparations and measurements as,

$$\rho_{xx} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a_1}.\vec{\sigma}\right], \;\; \rho_{x\bar{x}} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a_2}.\vec{\sigma}\right], \tag{3.2}$$

$$B_1 = \frac{1}{2}\left[\mathbb{I} + (-1)^{b_1} \hat{b_1}.\vec{\sigma}\right], \;\; B_2 = \frac{1}{2}\left[\mathbb{I} + (-1)^{b_2} \hat{b_2}.\vec{\sigma}\right]. \tag{3.3}$$

Here, $\hat{a_i}$, $\hat{b_j}$ are the Bloch vectors denoting Alice's and Bob's measurement directions respectively and $\vec{\sigma}$ are the Pauli matrices.

Clearly, $\rho_{00} + \rho_{11} = \mathbb{I}$, $\rho_{01} + \rho_{10} = \mathbb{I}$, $B_j^0 + B_j^1 = \mathbb{I}$ for $j = \{1, 2\}$ and the notation $B_j^{b_j}$ denotes the eigenstate corresponding to the outcome b_j of measurement B_j. The average success probability now can be written as

$$\mathbb{F}_{2\mapsto 1} = \frac{1}{8}[\mathrm{Tr}[\rho_{00}B_1^0 + \rho_{00}B_2^0 + \rho_{11}B_1^1 + \rho_{11}B_2^1 + \rho_{01}B_1^0 + \rho_{01}B_2^1 + \rho_{10}B_1^1 + \rho_{10}B_2^0]]. \tag{3.4}$$

The maximum achievable value for the above quantity is $\frac{1}{2}(1 + \frac{1}{2})$ with classical strategy, whereas it can reach up to $\frac{1}{2}(1 + \frac{1}{\sqrt{2}})$ if quantum strategy is used [47].

3.2.2 $3 \mapsto 1$ RAC

In a $3 \mapsto 1$ RAC, a three-bit input string $x_1x_2x_3$ from the set $\{000, 001, 010, 011, 100, 101, 110, 111\}$ is given to Alice uniformly at random. Alice then encodes the input string in a qubit $\rho_{x_1x_2x_3}$ and sends it to Bob. Bob upon receiving an input $y \in \{1, 2, 3\}$, implements a binary outcome measurement B_y and reports the outcome $\beta \in \{0, 1\}$ as his output. The average probability of winning can be calculated as

$$\mathbb{F}_{3\mapsto 1} = \frac{1}{24} \sum_{x_1,x_2,x_3,y} P(\beta_y = x_y \mid x_1, x_2, x_3, y). \tag{3.5}$$

Let us now consider most general preparations

$$\rho_{xxx} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a_1}\cdot\vec{\sigma}\right], \quad \rho_{xx\bar{x}} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a_2}\cdot\vec{\sigma}\right],$$
$$\rho_{x\bar{x}x} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a_3}\cdot\vec{\sigma}\right], \quad \rho_{x\bar{x}\bar{x}} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a_4}\cdot\vec{\sigma}\right], \tag{3.6}$$

and measurements as,

$$B_1 = \frac{1}{2}\left[\mathbb{I} + (-1)^{b_1}\,\hat{b_1}.\vec{\sigma}\right], \quad B_2 = \frac{1}{2}\left[\mathbb{I} + (-1)^{b_2}\,\hat{b_2}.\vec{\sigma}\right], \quad B_3 = \frac{1}{2}\left[\mathbb{I} + (-1)^{b_3}\,\hat{b_3}.\vec{\sigma}\right]. \tag{3.7}$$

Clearly, $\rho_{000} + \rho_{111} = \mathbb{I}$, $\rho_{001} + \rho_{110} = \mathbb{I}$, $\rho_{010} + \rho_{101} = \mathbb{I}$, and $\rho_{011} + \rho_{100} = \mathbb{I}$. The average success probability can be written as

$$\begin{aligned}\mathbb{F}_{3\mapsto 1} = \frac{1}{24}[\mathrm{Tr}[&\rho_{000}(B_1^0 + B_2^0 + B_3^0) + \rho_{001}(B_1^0 + B_2^0 + B_3^1) + \rho_{010}(B_1^0 + B_2^1 + B_3^0)\\ &+ \rho_{011}(B_1^0 + B_2^1 + B_3^1) + \rho_{100}(B_1^1 + B_2^0 + B_3^0) + \rho_{101}(B_1^1 + B_2^0 + B_3^1)\\ &+ \rho_{110}(B_1^1 + B_2^1 + B_3^0) + \rho_{111}(B_1^1 + B_2^1 + B_3^1)]].\end{aligned} \tag{3.8}$$

Here, the average success probability, $\mathbb{F}_{3\mapsto 1}$ can be achieved up to $\frac{1}{2}(1+\frac{1}{3})$ and $\frac{1}{2}(1+\frac{1}{\sqrt{3}})$, by classical and quantum strategies, respectively [47].

3.2.3 $4 \mapsto 1$ RAC

In a $4 \mapsto 1$ RAC, Alice has a four-bits input string $x_1x_2x_3x_4$ which is given to her uniformly at random from the set $\{0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111\}$. She then implements a preparation procedure by encoding in a qubit $\rho_{x_1x_2x_3x_4}$ and sends to Bob. Bob upon receiving an input $y \in \{1,2,3,4\}$, implements a binary outcome measurement B_y and reports the outcome $\beta \in \{0,1\}$ as his output. The average probability of winning is given by

$$\mathbb{F}_{4\mapsto 1} = \frac{1}{64}\sum_{x_1,x_2,x_3,x_4,y} P(\beta_y = x_y \mid x_1, x_2, x_3, x_4, y). \tag{3.9}$$

Let us now consider most general preparations,

$$\rho_{xxxx} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a_1}.\vec{\sigma}\right], \quad \rho_{xxx\bar{x}} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a_2}.\vec{\sigma}\right], \quad \rho_{xx\bar{x}x} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a_3}.\vec{\sigma}\right],$$
$$\rho_{xx\bar{x}\bar{x}} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a_4}.\vec{\sigma}\right], \quad \rho_{x\bar{x}xx} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a_5}.\vec{\sigma}\right], \quad \rho_{x\bar{x}x\bar{x}} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a_6}.\vec{\sigma}\right],$$
$$\rho_{x\bar{x}\bar{x}x} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a_7}.\vec{\sigma}\right], \quad \rho_{x\bar{x}\bar{x}\bar{x}} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a_8}.\vec{\sigma}\right], \tag{3.10}$$

and measurements

$$B_1 = \frac{1}{2}\left[\mathbb{I} + (-1)^{b_1}\, \hat{b_1}.\vec{\sigma}\right], \quad B_2 = \frac{1}{2}\left[\mathbb{I} + (-1)^{b_2}\, \hat{b_2}.\vec{\sigma}\right],$$
$$B_3 = \frac{1}{2}\left[\mathbb{I} + (-1)^{b_3}\, \hat{b_3}.\vec{\sigma}\right], \quad B_4 = \frac{1}{2}\left[\mathbb{I} + (-1)^{b_4}\, \hat{b_4}.\vec{\sigma}\right]. \tag{3.11}$$

Clearly, $\rho_{0000} + \rho_{1111} = \mathbb{I}$, $\rho_{0001} + \rho_{1110} = \mathbb{I}$, $\rho_{0010} + \rho_{1101} = \mathbb{I}$, $\rho_{0011} + \rho_{1100} = \mathbb{I}$, $\rho_{0100} + \rho_{1011} = \mathbb{I}$, $\rho_{0101} + \rho_{1010} = \mathbb{I}$, $\rho_{0110} + \rho_{1001} = \mathbb{I}$, and $\rho_{0111} + \rho_{1000} = \mathbb{I}$. Therefore the explicit form of the average success probability of $4 \mapsto 1$ RAC is calculated to be

$$\begin{aligned}
\mathbb{F}_{4\mapsto 1} = \frac{1}{64}[\mathrm{Tr}[&\rho_{0000}(B_1^0 + B_2^0 + B_3^0 + B_4^0) + \rho_{0001}(B_1^0 + B_2^0 + B_3^0 + B_4^1) + \rho_{0010}(B_1^0 \\
&+ B_2^0 + B_3^1 + B_4^0) + \rho_{0011}(B_1^0 + B_2^0 + B_3^1 + B_4^1) + \rho_{0100}(B_1^0 + B_2^1 + B_3^0 + B_4^0) \\
&+ \rho_{0101}(B_1^0 + B_2^1 + B_3^0 + B_4^1) + \rho_{0110}(B_1^0 + B_2^1 + B_3^1 + B_4^0) + \rho_{0111}(B_1^0 + B_2^1 \\
&+ B_3^1 + B_4^1) + \rho_{1000}(B_1^1 + B_2^0 + B_3^0 + B_4^0) + \rho_{1001}(B_1^1 + B_2^0 + B_3^0 + B_4^1) \\
&+ \rho_{1010}(B_1^1 + B_2^0 + B_3^1 + B_4^0) + \rho_{1011}(B_1^1 + B_2^0 + B_3^1 + B_4^1) + \rho_{1100}(B_1^1 + B_2^1 \\
&+ B_3^0 + B_4^0) + \rho_{1101}(B_1^1 + B_2^1 + B_3^0 + B_4^1) + \rho_{1110}(B_1^1 + B_2^1 + B_3^1 + B_4^0) \\
&+ \rho_{1111}(B_1^1 + B_2^1 + B_3^1 + B_4^1)]].
\end{aligned} \tag{3.12}$$

For $4 \mapsto 1$ RAC, the exact value of classical and quantum average success probabilities are $\frac{1}{2}(1 + \frac{1}{4})$ and $\frac{1}{2}(1 + \frac{1+\sqrt{3}}{4\sqrt{2}})$ respectively [47].

3.2.4 Generalization of $n \mapsto 1$ RAC

In a $n \mapsto 1$ RAC, Alice has an n-bits input string $x_1x_2x_3x_4 \ldots x_n$ which is given to her uniformly at random. She then implements a preparation procedure by encoding this string in a qubit denoted by $\rho_{x_1x_2x_3x_4\ldots x_n}$ and sends it to Bob. Bob upon receiving an

input $y \in \{1, 2, 3, \ldots, n\}$, implements a binary outcome measurement B_y and reports the outcome $\beta \in \{0, 1\}$ as his output. The average probability of winning is given by

$$\begin{aligned}\mathbb{F}_{n\mapsto 1} &= P(\beta_y = \text{y-th bit of Alice}) \\ &= \frac{1}{n2^n} \sum_{x_1,\ldots,x_n,y} P(\beta_y = x_y \mid x_1, ..., x_n, y). \end{aligned} \tag{3.13}$$

For $n \mapsto 1$ RAC, there are 2^{n-1} preparations and n measurements. Let us now consider the most general preparations,

$$\begin{aligned}&\rho_{xxx\ldots xx} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a}_1.\vec{\sigma}\right], \quad \rho_{xxx\ldots x\bar{x}} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a}_2.\vec{\sigma}\right], \quad \rho_{xxx\ldots\bar{x}x} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a}_3.\vec{\sigma}\right], \\ &\qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ &\rho_{xx\bar{x}\ldots\bar{x}\bar{x}} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a}_{2^{n-1}-1}.\vec{\sigma}\right], \quad \rho_{x\bar{x}\bar{x}\ldots\bar{x}\bar{x}} = \frac{1}{2}\left[\mathbb{I} + (-1)^x \hat{a}_{2^{n-1}}.\vec{\sigma}\right], \end{aligned} \tag{3.14}$$

and measurements

$$\begin{aligned}B_1 &= \frac{1}{2}\left[\mathbb{I} + (-1)^{b_1}\hat{b}_1.\vec{\sigma}\right], \quad B_2 = \frac{1}{2}\left[\mathbb{I} + (-1)^{b_2}\hat{b}_2.\vec{\sigma}\right], \\ B_3 &= \frac{1}{2}\left[\mathbb{I} + (-1)^{b_3}\hat{b}_3.\vec{\sigma}\right], \ldots, B_n = \frac{1}{2}\left[\mathbb{I} + (-1)^{b_n}\hat{b}_n.\vec{\sigma}\right].\end{aligned}$$

Clearly, $\rho_m + \rho_{\bar{m}} = \mathbb{I}$, where, m are the elements of the n-bit string set. The exact form of the average success probability of $n \mapsto 1$ RAC can be calculated as

$$\begin{aligned}\mathbb{F}_{n\mapsto 1} = \frac{1}{n2^n}[\mathrm{Tr}[&\rho_{00\ldots00}(B_1^0 + B_2^0 + \cdots + B_{n-1}^0 + B_n^0) + \rho_{00\ldots01}(B_1^0 + B_2^0 + \cdots + B_{n-1}^0 + B_n^1) \\ &+ \rho_{00\ldots10}(B_1^0 + B_2^0 + \cdots + B_{n-1}^1 + B_n^0) + \cdots + \rho_{11\ldots10}(B_1^1 + B_2^1 + \cdots + B_{n-1}^1 + B_n^0) \\ &+ \rho_{11\ldots11}(B_1^1 + B_2^1 + \cdots + B_{n-1}^1 + B_n^1)]]. \end{aligned} \tag{3.15}$$

The average success probability for $n \mapsto 1$ RAC (with SR) using best classical strategy is known to be $\frac{1}{2}(1 + \frac{1}{n})$ [47].

3.3 Temporal Inequalities Associated With The Random Access Codes

We would now like to present a temporal inequality corresponding to each $n \mapsto 1$ RAC. To derive such temporal inequalities, we use the assumptions of realism and noninvasive measurability. The term 'realism' implies *"at any instant, irrespective of any measurement, a system is definitely in any one of the available states such that all its observable properties have definite values"*. On the other hand, the term 'noninvasive measurability' assures that *"it is possible, in principle, to determine which of the states the system is in, without affecting the state itself or the system's subsequent evolution"*. It can be shown that under these two assumptions the joint probability distribution get factorized at the ontological level [81, 84, 85, 89]. Mathematically,

$$P(a_i, b_j \mid A_i, B_j) = \int_\lambda \rho(\lambda) P(a_i \mid A_i, \lambda) P(b_j \mid B_j, \lambda) \tag{3.16}$$

with λ being the hidden variable. Based on this macro-realistic definition of classicality, later we derive temporal inequalities corresponding to each $n \mapsto 1$ RAC and establish that violation of such inequalities implies non-classical temporal correlation. The underlying experimental setup for both the scenarios are the same, as will be clear from the following description.

In a temporal scenario, temporal correlations are obtained by measuring a single system sequentially at different instants of time. In each run of the experiment, two sequential measurements are performed on an identically prepared initial state. We assume that the first measurement is performed by Alice whereas the second one is performed by Bob. If Alice's measurement is thought of as playing the role of preparation, then it is not very difficult to realize the similarity between RACs and macro-realistic inequalities. This observation is further substantiated by formulating the relevant inequalities which build the connection quantitatively. Suppose the measurements performed by Alice and the corresponding outcomes are denoted by A_i and a_i respectively. Similarly, the measurements performed by Bob are denoted by B_j with corresponding outcome b_j. All the measurements performed by both the parties are

considered to be dichotomic *i.e.*, $a_i, b_j \in \{0, 1\}$.

Initially, the state on which Alice performs her measurement is denoted by ρ_{in}. The correlation between Alice's and Bob's measurement outcome depends on ρ_{in}. In the present analysis we took a maximally mixed state, i.e., $\rho_{in} = \mathbb{I}/2$, for reasons that will be clear later. It may be noted here that other states may be chosen for which the same maximum violation for our temporal inequalities can be achieved using different Bloch vectors $(\hat{a_i}, \hat{b_j})$. However, even if the directions of Alice's and Bob's measurements are changed, the maximum violation will remain the same.

Let the probability of obtaining outcome a_i and b_j be denoted by $P(a_i, b_j \mid A_i, B_j)$, when Alice measures A_i at time t_i and Bob measures B_j at some later instant t_j respectively and $a_i, b_j \in \{0, 1\}$. Let us denote, $A_i^{a_i}$, $B_j^{b_j}$ as projectors so that $\sum_{a_i} A_i^{a_i} = \mathbb{I}, \sum_{b_j} B_j^{b_j} = \mathbb{I}$. Now, following the standard procedure, the joint probability distribution can be obtained using Bayes' rule as,

$$\begin{aligned} P(a_i, b_j \mid A_i, B_j) &= P(a_i \mid A_i) P(b_j \mid a_i, A_i, B_j) \\ &= \mathrm{Tr}\left[A_i^{a_i} \rho_{in}\right] \mathrm{Tr}\left[B_j^{b_j} \frac{A_i^{a_i} \rho_{in} A_i^{a_i \dagger}}{\mathrm{Tr}\left[A_i^{a_i} \rho_{in} A_i^{a_i \dagger}\right]}\right]. \end{aligned} \tag{3.17}$$

With this joint probability distribution, the two-time correlation is defined as,

$$C_{ij} = \sum_{a_i, b_j} (-1)^{a_i \oplus b_j} P(a_i, b_j \mid A_i, B_j), \tag{3.18}$$

where $\oplus$ denotes addition modulo 2. In the subsections below we present the temporal inequalities corresponding to cases of $2 \mapsto 1$, $3 \mapsto 1$ and $4 \mapsto 1$ RACs. These inequalities are derived with a close look at the success probabilities of the corresponding RAC games. The general form of the temporal inequality for $n \mapsto 1$ RAC, i.e., $\mathcal{K}_{n \mapsto 1}$ is provided in the Appendix-(A).

As mentioned earlier, in our temporal scenario, the initially prepared state is considered to be $\mathbb{I}/2$. Since we are interested in finding the maximum violation of the temporal inequality $\mathcal{K}_{n \mapsto 1}$, without loss of generality we can stick to projective measurements only. Consider the general form of the measurements on Alice's side to

be

$$A_i^{a_i} = \frac{1}{2}\left[\mathbb{I} + (-1)^{a_i}\hat{a}_i.\vec{\sigma}\right], \tag{3.19}$$

where a_i represents the outcome corresponding the measurement A_i and $\hat{a}_i$ represents the direction along which the A_i measurement is being performed. On the other hand the general form of the measurements performed on Bob's side can be considered to be

$$B_j^{b_j} = \frac{1}{2}\left[\mathbb{I} + (-1)^{b_j}\hat{b}_j.\vec{\sigma}\right], \tag{3.20}$$

where b_j represents the outcome corresponding to measurement B_j and $\hat{b}_j$ represents the direction along which B_j measurement is being performed. In the subsections below we state the explicit form of the quantum strategy for which maximum quantum violation of the temporal inequality $\mathcal{K}_{n\mapsto 1}$ RAC is achieved.

3.3.1 Temporal Inequality for $2 \mapsto 1$ RAC

Now, to derive a temporal inequality corresponding to the $2 \mapsto 1$ RAC, let us first assume that Alice and Bob have two choices of binary measurements, say, $\{A_1, A_2\}$ and $\{B_1, B_2\}$ to perform in each run and $\rho_{in} = \frac{\mathbb{I}}{2}$. Let us now consider the following quantity in terms of the above correlators as,

$$\mathcal{K}_{2\mapsto 1} = C_{11} + C_{21} + C_{12} - C_{22}. \tag{3.21}$$

Following Eq. (3.18), we calculate the C_{11} term explicitly:

$$\begin{aligned}
C_{11} =& P(0,0|A_1,B_1) + P(1,1|A_1,B_1) - P(0,1|A_1,B_1) - P(1,0|A_1,B_1) \\
=& \frac{1}{2}\mathrm{Tr}[A_1^0 B_1^0 + A_1^1 B_1^1 - A_1^0 B_1^1 - A_1^1 B_1^0] \\
=& \frac{1}{2}\mathrm{Tr}[A_1^0 B_1^0 + A_1^1 B_1^1 - A_1^0(\mathbb{I} - B_1^0) - A_1^1(\mathbb{I} - B_1^1)] \\
=& \mathrm{Tr}[A_1^0 B_1^0 + A_1^1 B_1^1] - 1.
\end{aligned}$$

where, $A_i^{a_i}$ represents the eigenstate corresponding to the outcome $a_i \in \{0,1\}$ of the measurement A_i and similarly for Bob. Here, the second equality can be derived using Eq.(3.17), *i.e.*, by evaluating all the probability terms explicitly, and the third equality

follows from the fact that two eigenstate corresponding to the same dichotomic measurement add up to unity, *i.e.*, $A_i^0 + A_i^1 = \mathbb{I}$ and $B_j^0 + B_j^1 = \mathbb{I}$ for all i, j.

Similarly, the other terms can be evaluated as

$$C_{12} = \mathrm{Tr}[A_1^0 B_2^0 + A_1^1 B_2^1] - 1, C_{21} = \mathrm{Tr}[A_2^0 B_1^0 + A_2^1 B_1^1] - 1, C_{22} = -\mathrm{Tr}[A_2^1 B_2^0 + A_2^0 B_2^1] + 1.$$

Hence, the expression for $\mathcal{K}_{2\mapsto 1}$ becomes,

$$\begin{aligned}\mathcal{K}_{2\mapsto 1} &= C_{11} + C_{21} + C_{12} - C_{22} \\ &= \mathrm{Tr}[A_1^0 B_1^0 + A_1^1 B_1^1 + A_1^0 B_2^0 + A_1^1 B_2^1 + A_2^0 B_1^0 + A_2^1 B_1^1 + A_2^1 B_2^0 + A_2^0 B_2^1] - 4. \quad (3.22)\end{aligned}$$

It may be noted here that the eigenstate of the measurements performed by Alice $A_i^{a_i}$ is the same as that of the preparations considered in Eq.(3.2). Now, comparing the above equation with Eq.(3.4), one obtains

$$\mathcal{K}_{2\mapsto 1} = 8(\mathbb{F}_{2\mapsto 1} - \frac{1}{2}). \quad (3.23)$$

Conversely, $\mathbb{F}_{2\mapsto 1} = \frac{1}{2} + \frac{1}{8}\mathcal{K}_{2\mapsto 1}$.

It can be shown that the maximum quantum violation of the temporal inequality $\mathcal{K}_{2\mapsto 1}$ corresponding to $2 \mapsto 1$ RAC can be achieved up to 2.828 for the following sets of measurements:

$$\hat{a}_1 = \frac{1}{\sqrt{2}}(1, 1, 0), \hat{a}_2 = \frac{1}{\sqrt{2}}(1, -1, 0), \quad (3.24)$$

and

$$\hat{b}_1 = (1, 0, 0), \hat{b}_2 = (0, 1, 0). \quad (3.25)$$

One can see that the strategy to reach the maximum violation of the temporal inequality $\mathcal{K}_{2\mapsto 1}$ with initially prepared state $\mathbb{I}/2$ is the same with that of the quantum strategy for which the maximum success probability for $2 \mapsto 1$ RAC is achieved.

Note further, a noninvasive-realist bound for the term $\mathcal{K}_{2\mapsto 1}$ was derived to be 2 (See, Appendix-(A.1)). One can see from this relation that whenever the value of the

term $\mathcal{K}_{2\mapsto 1}$ falls below 2, the success probability of the $2 \mapsto 1$ random access code also falls below $\frac{3}{4}$ which is the maximum probability of success with classical strategy. Moreover, the maximum success probability of $2 \mapsto 1$ RAC reaches $\frac{1}{2}(1+\frac{1}{\sqrt{2}})$ whenever the maximal qubit strategy of $\mathcal{K}_{2\mapsto 1}$ reaches $2\sqrt{2}$, and vice versa. Therefore, any quantum advantage of $2 \mapsto 1$ RAC implies a violation of the corresponding macro-realist model.

3.3.2 Temporal Inequality for $3 \mapsto 1$ RAC

To derive a temporal inequality analogous to $3 \mapsto 1$ RAC, we need to consider four measurements on Alice's side say $\{A_1, A_2, A_3, A_4\}$ and three measurements on Bob's side say $\{B_1, B_2, B_3\}$. In each run of the experiment, Alice performs one out of the four dichotomic measurements on an initially prepared input state, $\rho_{\text{in}} = \frac{\mathbb{I}}{2}$, and then Bob implements one out of the three possible measurements on the post-measurement state of Alice. In this way let us define the following quantity in terms of the correlators (3.18) as,

$$\mathcal{K}_{3\mapsto 1} = C_{11} + C_{12} + C_{13} + C_{22} + C_{21} - C_{23} + C_{31} - C_{32} + C_{33} + C_{41} - C_{42} - C_{43}. \tag{3.26}$$

Following Eq. (3.18) and after some straightforward calculations, one can obtain the general form of the correlators as

$$C_{ij} = (-1)^{a_i}[\text{Tr}[A_i^{a_i} B_j^0 + A_i^{\bar{a}_i} B_j^1] - 1]. \tag{3.27}$$

Here, i and j denotes Alice's and Bob's measurement indices, respectively. The outcome of Alice's measurement $A_i^{a_i}$ are denoted as a_i and $\bar{a}_i$ represents the complement of a_i.

Therefore, the term $\mathcal{K}_{3\mapsto 1}$ becomes,

$$\begin{aligned}\mathcal{K}_{3\mapsto 1} &= \sum_{j=1}^{3}\sum_{i=1}^{4}(-1)^{a_i}[\text{Tr}[A_i^{a_i} B_j^0 + A_i^{\bar{a}_i} B_j^1] - 1] \\ &= \sum_{j=1}^{3}\sum_{i=1}^{4}(-1)^{a_i}\text{Tr}[A_i^{a_i} B_j^0 + A_i^{\bar{a}_i} B_j^1] - 12. \end{aligned} \tag{3.28}$$

Taking the eigenstate of Alice's measurement $A_i^{a_i}$, $i \in \{1,2,3,4\}$ as that of the preparations for $3 \mapsto 1$ RAC, *i.e.*, Eq.(3.6) we obtain the success probability of $3 \mapsto 1$ RAC to be

$$\mathcal{K}_{3\mapsto 1} = 24\mathbb{F}_{3\mapsto 1} - 12 \tag{3.29}$$

or equivalently, $\mathbb{F}_{3\mapsto 1} = \frac{1}{2} + \frac{1}{24}\mathcal{K}_{3\mapsto 1}$.

It can be shown that the maximum violation of the temporal inequality $\mathcal{K}_{3\mapsto 1}$ corresponding to the $3 \mapsto 1$ RAC can be achieved up to 6.928 for the following measurement settings:

$$\begin{aligned} \hat{a}_1 &= \frac{1}{\sqrt{3}}(1,1,1), \hat{a}_2 = \frac{1}{\sqrt{3}}(1,1,-1), \\ \hat{a}_3 &= \frac{1}{\sqrt{3}}(1,-1,1), \hat{a}_4 = \frac{1}{\sqrt{3}}(1,-1,-1). \end{aligned} \tag{3.30}$$

and

$$\hat{b}_1 = (1,0,0), \hat{b}_2 = (0,1,0), \hat{b}_3 = (0,0,1). \tag{3.31}$$

This is again the same strategy for which maximum quantum success probability of $3 \mapsto 1$ RAC is achieved.

A noninvasive-realist bound for the above quantity $\mathcal{K}_{3\mapsto 1}$ is derived in Appendix-(A.2) to be 4. One can see that when $\mathcal{K}_{3\mapsto 1} = 4$, the success probability $\mathbb{F}_{3\mapsto 1}$ reaches $\frac{2}{3}$ which is the best classical strategy to win the $3 \mapsto 1$ RAC. On the other hand, with the maximal qubit strategy, $\mathcal{K}_{3\mapsto 1}$ can however achieve value up to 6.928, and for this the success probability $\mathbb{F}_{3\mapsto 1}$ to win $3 \mapsto 1$ RAC reaches up to $\frac{1}{2}(1 + \frac{1}{\sqrt{3}})$. This is again the maximum success probability of winning $3 \mapsto 1$ RAC using quantum strategy. Therefore, any violation of $3 \mapsto 1$ RAC again does not possess any macro-realist description.

3.3.3 Temporal Inequality for $4 \mapsto 1$ RAC

To derive a temporal inequality corresponding to $4 \mapsto 1$ RAC, Alice and Bob need to perform eight and four measurements respectively in their respective parts. In each run of the experiment Alice performs one out of the eight dichotomic measurements

on an initially prepared input state, $\rho_{\text{in}} = \frac{\mathbb{I}}{2}$, and Bob performs one out of the four dichotomic measurements on the post measurement state of Alice. Let us now consider the following quantity, consisting of thirty-two correlators given by,

$$\begin{aligned}\mathcal{K}_{4\mapsto 1} = & C_{11} + C_{12} + C_{13} + C_{14} + C_{21} + C_{22} + C_{23} - C_{24} + C_{31} + C_{32} - C_{33} + C_{34} \\ & + C_{41} + C_{42} - C_{43} - C_{44} + C_{51} - C_{52} + C_{53} + C_{54} + C_{61} - C_{62} + C_{63} - C_{64} \\ & + C_{71} - C_{72} - C_{73} + C_{74} + C_{81} - C_{82} - C_{83} - C_{84}. \end{aligned} \tag{3.32}$$

Now, the explicit form of the correlators C_{ij} can be evaluated directly from Eq.(3.27). Therefore, the term $\mathcal{K}_{4\mapsto 1}$ reduces to

$$\begin{aligned}\mathcal{K}_{4\mapsto 1} &= \sum_{j=1}^{4}\sum_{i=1}^{8}(-1)^{a_i}[\text{Tr}[A_i^{a_i}B_j^0 + A_i^{\bar{a}_i}B_j^1] - 1] \\ &= \sum_{j=1}^{4}\sum_{i=1}^{8}(-1)^{a_i}\text{Tr}[A_i^{a_i}B_j^0 + A_i^{\bar{a}_i}B_j^1] - 32 \end{aligned} \tag{3.33}$$

with the symbols having usual meanings. Now comparing the eigenstate of Alice's measurement $A_i^{a_i}$, $i \in \{1, 2, ..., 8\}$ with that of the preparations for the $4 \mapsto 1$ *i.e.*, Eq. (3.10), we obtain

$$\mathcal{K}_{4\mapsto 1} = 64(\mathbb{F}_{4\mapsto 1} - \frac{1}{2}). \tag{3.34}$$

Equivalently, $\mathbb{F}_{4\mapsto 1} = \frac{1}{2} + \frac{1}{64}\mathcal{K}_{4\mapsto 1}$.

The maximum quantum violation of the temporal inequality $\mathcal{K}_{4\mapsto 1}$ can be achieved up to 15.454 for the following measurement settings:

$$\begin{aligned}&\hat{a}_1 = \frac{1}{\sqrt{6}}(1,1,2), \hat{a}_2 = \frac{1}{\sqrt{6}}(1,1,-2), \hat{a}_3 = \frac{1}{\sqrt{6}}(1,-1,2), \\ &\hat{a}_4 = \frac{1}{\sqrt{6}}(1,-1,-2), \hat{a}_5 = \frac{1}{\sqrt{6}}(\sqrt{3},\sqrt{3},0), \hat{a}_6 = \frac{1}{\sqrt{6}}(\sqrt{3},-\sqrt{3},0), \\ &\hat{a}_7 = \frac{1}{\sqrt{6}}(\sqrt{3},\sqrt{3},0), \hat{a}_8 = \frac{1}{\sqrt{6}}(\sqrt{3},-\sqrt{3},0). \end{aligned} \tag{3.35}$$

and

$$\hat{b}_1 = (1,0,0), \hat{b}_2 = (0,1,0), \hat{b}_3 = (0,0,1), \hat{b}_4 = (0,0,1). \tag{3.36}$$

This is again the same strategy for which maximum success probability of $4 \mapsto 1$ RAC is achieved.

A noninvasive-realist bound for $\mathcal{K}_{4\mapsto 1}$ is derived in Appendix-(A.3) to be 8. In addition, the best classical strategy to win the $4 \mapsto 1$ RAC is $\frac{5}{8}$. One can see from the above relation that whenever the $\mathcal{K}_{4\mapsto 1}$ rises above 8 there is no macro-realist model, and only in this case the quantum advantage of $4 \mapsto 1$ RAC can be obtained. The term $\mathcal{K}_{4\mapsto 1}$ can reach up to 15.454 with maximal qubit strategy which also matches with the maximum average success probability, $\mathbb{F}_{4\mapsto 1} = 0.741$.

3.3.4 Temporal Inequality for $n \mapsto 1$ RAC

Let us now derive a temporal inequality corresponding to $n \mapsto 1$ RAC. To do so we need to consider 2^{n-1} measurements on Alice's side say $\{A_1, A_2, A_3, \ldots, A_{2^{n-1}}\}$ and n measurements on Bob's side say $\{B_1, B_2, \ldots, B_n\}$. At first, Alice performs one out of the 2^{n-1} dichotomic measurements on an initially prepared input state, $\rho_{\text{in}} = \frac{\mathbb{I}}{2}$ and then, Bob performs one out of the n possible measurements on the post measurement state of Alice. Finally, they evaluate the quantity $\mathcal{K}_{n\mapsto 1}$, represented in terms of the correlators (3.18) as,

$$\begin{aligned}\mathcal{K}_{n\mapsto 1} = {} & C_{11} + C_{12} + C_{13} + \cdots + C_{1n} + C_{21} + C_{22} + C_{23} + \cdots - C_{2n} + C_{31} + C_{32} \\ & + C_{33} + \cdots + C_{3n} + \cdots + C_{(2^{n-1}-1)1} - C_{(2^{n-1}-1)2} - C_{(2^{n-1}-1)3} + \ldots \\ & + C_{(2^{n-1}-1)n} + \cdots + C_{2^{n-1}1} - C_{2^{n-1}2} - C_{2^{n-1}3} - \cdots - C_{2^{n-1}n}. \end{aligned} \tag{3.37}$$

It might be noted here that some of the correlators will contain negative sign. This is because Alice's and Bob's measurements are anti-correlated for those particular terms. Now, the explicit form of the correlators can be written from Eq.(3.27).

Therefore, the term $\mathcal{K}_{n\mapsto 1}$ becomes,

$$\begin{aligned}\mathcal{K}_{n\mapsto 1} &= \sum_{j=1}^{n}\sum_{i=1}^{2^{n-1}} (-1)^{a_i}[\text{Tr}[A_i^{a_i} B_j^0 + A_i^{\bar{a}_i} B_j^1] - 1] \\ &= \sum_{j=1}^{n}\sum_{i=1}^{2^{n-1}} (-1)^{a_i}\text{Tr}[A_i^{a_i} B_j^0 + A_i^{\bar{a}_i} B_j^1] - n2^{n-1}. \end{aligned} \tag{3.38}$$

Now if we take the eigenstate of Alice's measurement $A_i^{a_i}$, $i \in \{1, 2, \ldots, 2^{n-1}\}$ as that of the preparations for $n \mapsto 1$ RAC, *i.e.*, Eq.(3.14), we obtain the success probability of $n \mapsto 1$ RAC to be

$$\mathcal{K}_{n\mapsto 1} = n2^n \mathbb{F}_{n\mapsto 1} - n2^{n-1} \tag{3.39}$$

or equivalently, $\mathbb{F}_{n\mapsto 1} = \frac{1}{2} + \frac{1}{n2^n}\mathcal{K}_{n\mapsto 1}$.

It can be checked that when $\mathcal{K}_{n\mapsto 1} = 2^{n-1}$, the success probability $\mathbb{F}_{n\mapsto 1}$ reaches $\frac{1}{2}(1 + \frac{1}{n})$ which is the best classical strategy to win the $n \mapsto 1$ RAC. In Appendix-(A.4) we derive the noninvasive-realist bound for the temporal inequality corresponding to the $n \mapsto 1$ RAC which turns out to be 2^{n-1}. Now, from the relation between the average success probability $\mathbb{F}_{n\mapsto 1}$ and corresponding temporal inequality $\mathcal{K}_{n\mapsto 1}$, we can conclude that any non-zero quantum advantage of general $n \mapsto 1$ RAC necessitates non-classical temporal correlation. On the basis of the above investigation, following the main idea stated at the beginning of this section, we clearly summarize our first main result, given bellow.

- ***Result 1:-***

> **"For every $n \mapsto 1$ RAC with SR, there exists a temporal inequality where Alice, the first observer has 2^{n-1} measurement settings and Bob who measures later has n measurement settings. The maximum success probability of each $n \mapsto 1$ RAC with best classical strategy is related to the maximum noninvasive-realist bound, and any non-zero quantum advantage of a $n \mapsto 1$ RAC translates to the violation of the corresponding temporal inequality."**

Moreover, based on our analysis for the cases of $2 \mapsto 1$, $3 \mapsto 1$ and $4 \mapsto 1$ RACs, we can further make the following conjecture. If the maximum success probability of $n \mapsto 1$ RAC occurs with a set of encoding states for Alice and decoding measurements for Bob, then maximal violation of the corresponding temporal inequality is obtained with Alice measuring observables whose eigenstates are exactly the encoded states and Bob's measurements are decoding observables with the initially prepared input state $\mathbb{I}/2$.

3.4 Certification of True Randomness

For the purpose of certifying randomness we describe here an alternative derivation of temporal inequalities, instead of the one based on realism and noninvasive measurability. This alternative derivation was proposed based on some operational assumptions which can be tested in a real experiment. In this alternative derivation the pertaining assumptions are *no signaling in time* (NSIT) and *predictability* [89, 97, 117]. The NSIT condition states that the measurement statistics are not influenced by the earlier measurements, or mathematically, $P(b_j|B_j) = P(b_j|A_i, B_j)\ \forall A_i, B_j, b_j$ [89]. On the other hand a model is said to be predictable if $P(a_i, b_j|A_i, B_j) \in \{0, 1\}\ \forall a_i, b_j, A_i, B_j$ [118].

Now, if λ denotes some classical variable at the ontological level, then in order to predict the experimental results at the operational level one needs to integrate over all λ, *i.e.*, $p(a_i, b_j|A_i, B_j) = \int_\lambda d\lambda p(\lambda) p(a_i, b_j|A_i, B_j, \lambda)$. Note that a crucial step to derive the temporal inequality is to show that the probability distribution at ontological level gets factorised, i.e.,

$$p(a_i, b_j|A_i, B_j, \lambda) = p(a_i|A_i, \lambda) p(b_j|B_j, \lambda) \tag{3.40}$$

Now, using predictability one can write $p(a_i, b_j|A_i, B_j, \lambda) = p(a_i, b_j|A_i, B_j)$ as further conditioning does not change the deterministic probability distribution. Using Bayes' rule one can write the probability distribution $p(a_i, b_j|A_i, B_j) = p(a_i|A_i, B_j, b_j)$ $\times\ p(b_j|A_i, B_j)$. Now, from the NSIT conditions one has $p(b_j|A_i, B_j) = p(b_j|B_j)$. Also, from a physically reasonable perspective, it is broadly accepted that a later measurement cannot influence the past measurement result, and hence $p(a_i|A_i, B_j, b_j) = p(a_i|A_i)$. Since, at the ontological level $p(a_i|A_i, \lambda) = p(a_i|A_i)$ and $p(b_j|B_j, \lambda) = p(b_j|B_j)$, the probability distribution can be written in a factorized form $p(a_i, b_j|A_i, B_j, \lambda) = p(a_i|A_i, \lambda)$ $\times\ p(b_j|B_j, \lambda)$. Therefore,

$$\text{NSIT} \wedge \text{predictability} \implies \text{factorizability} \tag{3.41}$$

or

$$\neg\ \text{factorizability} \wedge \text{NSIT} \implies \neg\ \text{predictability}. \tag{3.42}$$

Hence, if we consider a set of probability distributions which satisfies the NSIT conditions but does not fulfill the conditions for factorizability, then it is sure that predictability must be violated. In other words, if for a set of probability distributions the NSIT conditions hold and the temporal inequality is violated simultaneously, then predictability must not hold. Let us quantify this randomness by min-entropy $H_\infty(X)$ which captures the associated randomness that a particular distribution X contains. Therefore, any probability distribution $P(a_i, b_j|A_i, B_j)$ will not be predictable and hence some genuine randomness must be associated with that probability distribution [119]. For some distribution $P(a_i, b_j|A_i, B_j)$, the min-entropy is defined as

$$\begin{aligned} H_\infty(a_i, b_j|A_i, B_j) &= -\log_2[\max_{a_i,b_j} P(a_i, b_j|A_i, B_j)] \\ &= \min_{a_i,b_j}[-\log_2[P(a_i, b_j|A_i, B_j)]]. \end{aligned} \tag{3.43}$$

To calculate the randomness associated with the $\mathcal{K}_{n\mapsto 1}$, we need to find the maximum probability distribution $P(a_i, b_j|A_i, B_j)$ corresponding to some violation of this inequality. In other words, we need to solve the following optimization problem [120].

$$\begin{aligned} P^*(a_i, b_j|A_i, B_j) = \max & P(a_i, b_j|A_i, B_j) \\ & \text{constraints to } \mathcal{K}_{n\mapsto 1} = \mathcal{K}^{MR}_{n\mapsto 1} + \epsilon, \\ & P(a_i, b_j|A_i, B_j) \geq 0, \\ & \sum_{a_i,b_j} P(a_i, b_j|A_i, B_j) = 1 \ \ \forall A_i, B_j, \\ & \text{and } P(a_i, b_j|A_i, B_j) \text{ satisfy NSIT} \end{aligned} \tag{3.44}$$

where $P^*(a_i, b_j|A_i, B_j)$ denotes the maximized value of $P(a_i, b_j|A_i, B_j)$ and $\mathcal{K}^{MR}_{n\mapsto 1}$ is the MR bound of the temporal inequality $\mathcal{K}_{n\mapsto 1}$ corresponding to $n \mapsto 1$ RAC. We use linear programming to solve this optimization problem. The parameters α and β are chosen in such a way that the inequality maintain its linear form. By putting some boundary conditions, α and β are calculated for each $\mathcal{K}_{n\mapsto 1}$ so that $P^*(a_i, b_j|A_i, B_j) \leq \alpha\mathcal{K}_{n\mapsto 1} + \beta$. Here, it may be noted that for any particular $n \mapsto 1$ RAC, if α and β depend on a_i, b_j, A_i, B_j, then assuming $P^*(a_i, b_j|A_i, B_j) \leq \alpha\mathcal{K}_{n\mapsto 1} + \beta$ is not consistent, since we chose α and β to be some constant so that the linear form of the inequality

can be maintained. However, in case of a different $n \mapsto 1$ RAC, this α and β in general depends on the inequality corresponding to $\mathcal{K}_{n\mapsto 1}$ as well as on $P^*(a_i, b_j|A_i, B_j)$. Therefore, in general it may depend on a_i, b_j, A_i, B_j. A more detailed discussion on the choice of α and β (for the Bell-scenario) is provided explicitly in Ref. [120].

Note for example, in the case of $2 \mapsto 1$ RAC, the MR or classical bound of $\mathcal{K}_{2\mapsto 1}$ is 2. Now, $\mathcal{K}_{2\mapsto 1} = 2 + \epsilon$ (with $\epsilon > 0$) implies a non-zero violation of the inequality $\mathcal{K}_{2\mapsto 1}$. Therefore, optimization of $P(a_i, b_j|A_i, B_j)$ under the constraints $\mathcal{K}_{n\mapsto 1} = \mathcal{K}^{MR}_{n\mapsto 1} + \epsilon$ enables one to determine the maximum value of $P(a_i, b_j|A_i, B_j)$ for a certain amount of violation ϵ. The other constraints $P(a_i, b_j|A_i, B_j) \geq 0$ and $\sum_{a_i,b_j} P(a_i, b_j|A_i, B_j) = 1 \ \forall A_i, B_j$ can be easily understood from the properties of a valid probability distribution. The last constraint that $P(a_i, b_j|A_i, B_j)$ satisfies NSIT implies that the probability distribution $P(a_i, b_j|A_i, B_j)$ satisfies the NSIT condition given by $P(b_j|B_j) = P(b_j|A_i, B_j) \ \forall A_i, B_j, b_j$.

We are now interested to obtain a lower bound on the min-entropy $H_\infty(a_i, b_j|A_i, B_j)$ as a function of $\mathcal{K}_{n\mapsto 1}$, *i.e.*, we need to derive an inequality of the form $H_\infty(a_i, b_j|A_i, B_j) \geq f(\mathcal{K}_{n\mapsto 1})$. Below we provide a general lower bound of $H_\infty(a_i, b_j|A_i, B_j)$ from the perspective of no-signalling in time conditions. Using linear programming and imposing NSIT conditions, it can be shown that solving Eq.(3.44) one can obtain $P^*(a_i, b_j|A_i, B_j) \leq \alpha\mathcal{K}_{n\mapsto 1} + \beta$, where α and β in general may depend on a_i, b_j, A_i, B_j.

For $2 \mapsto 1$ RAC, in the case of the classical strategy, a deterministic point can achieve $P(a_i, b_j|A_i, B_j)$ upto 1, *i.e.*, $P^*(a_i, b_j|A_i, B_j) \leq 1$ when $\mathcal{K}_{2\mapsto 1} = 2$, and for the no signaling (in time) box (which is equivalent to the Popescu-Rorlich box for spatial correlation), $P(a_i, b_j|A_i, B_j) = 1/2$ *i.e.*, when $\mathcal{K}_{2\mapsto 1} = 4$, $P^*(a_i, b_j|A_i, B_j) \leq 1/2$. Therefore, analyzing the above inequalities one can obtain the values of α and β to be $-1/4$ and $3/2$, respectively [97, 120]. Hence,

$$P^*(a_i, b_j|A_i, B_j) \leq \frac{3}{2} - \frac{\mathcal{K}_{2\mapsto 1}}{4} \text{ or}$$
$$H_\infty(a_i, b_j|A_i, B_j) \geq -\log_2[\frac{3}{2} - \frac{\mathcal{K}_{2\mapsto 1}}{4}]. \tag{3.45}$$

In Fig.(3.1), a graphical representation of the lower bound of $H_\infty(a_i, b_j|A_i, B_j)$ corresponding to $2 \mapsto 1$ RAC is provided.

A similar approach based on NSIT conditions can also be applied to other $n \mapsto 1$

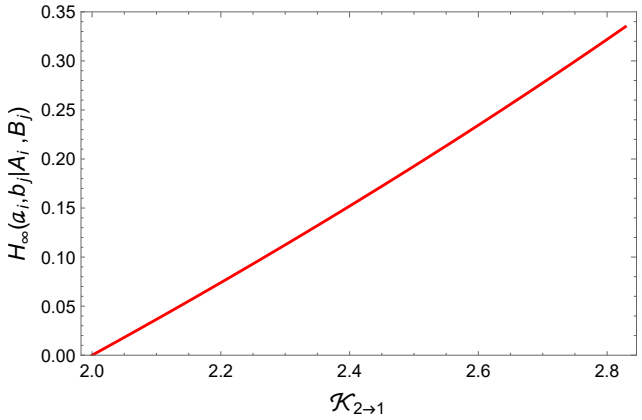


Figure 3.1: Min entropy $H_\infty(a_i, b_j|A_i, B_j)$ is plotted with $\mathcal{K}_{2\mapsto1}$

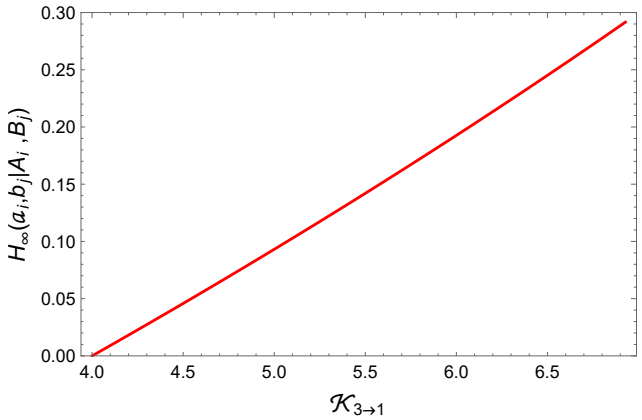


Figure 3.2: Min entropy $H_\infty(a_i, b_j|A_i, B_j)$ is plotted with $\mathcal{K}_{3\mapsto1}$

RAC. For the case of $3 \mapsto 1$ RAC, the no-signalling polytope can achieve the value of $\mathcal{K}_{3\mapsto1}$ up to 12 and for $4 \mapsto 1$ the value of $\mathcal{K}_{4\mapsto1}$ up to 32. Therefore, solving linear equations one can obtain $P^*(a_i, b_j|A_i, B_j) \leq \frac{5}{4} - \frac{\mathcal{K}_{3\mapsto1}}{16}$ and $P^*(a_i, b_j|A_i, B_j) \leq \frac{7}{6} - \frac{\mathcal{K}_{4\mapsto1}}{48}$ for $3 \mapsto 1$ and $4 \mapsto 1$ RAC, respectively. The lower bound of $H_\infty(a_i, b_j|A_i, B_j)$ corresponding to $\mathcal{K}_{3\mapsto1}$ and $\mathcal{K}_{4\mapsto1}$ RAC are plotted in Fig.(3.2) and Fig.(3.3) respectively. Here, it may be pertinent to mention that if instead of $P^*(a_i, b_j|A_i, B_j)$, randomness is certified from $P^*(b_j|A_i, B_j, a_i)$, then one obtains the maximum value of $H_\infty(a_i, b_j|A_i, B_j)$ to be 1 for any $n \mapsto 1$ RAC, because $P^*(b_j|A_i, B_j, a_i)$ is $1/2$ in this case irrespective of the value of n. Below, we summarize our key findings for the generation of genuine randomness based on our protocol.

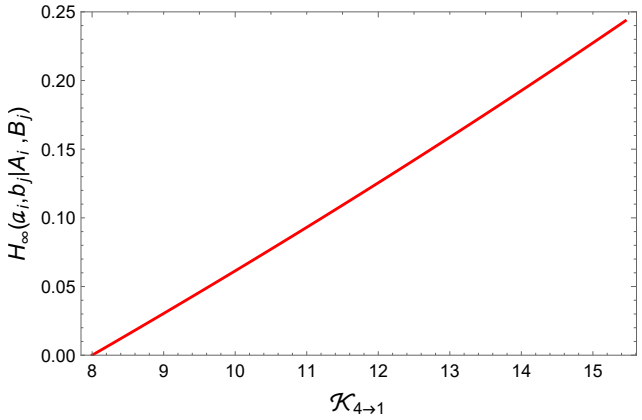


Figure 3.3: Min entropy $H_\infty(a_i, b_j|A_i, B_j)$ is plotted with $\mathcal{K}_{4\mapsto1}$

- ***Result 2:-***

> **"Any violation of the noninvasive-realist model of the temporal inequalities with initially prepared input state $\mathbb{I}/2$, or equivalently, any non-zero quantum advantage of $n \mapsto 1$ RAC with SR can be exploited to generate genuine randomness."**

It might be noted here that previous results to generate genuine randomness exploiting RAC do not guaranty genuine randomness for any non-zero quantum advantage of $n \mapsto 1$ RAC [75, 116].

3.5 Summary and Conclusion

Although the random access code has extensive applications in information processing and communication tasks, the underlying reason for its advantage remained largely unexplored until now. Here we showed that any non-zero quantum advantage of RAC with shared randomness necessarily violates a noninvasive-realist model. We proposed temporal inequalities corresponding to each $n \mapsto 1$ RAC with SR using the assumption of *realism* and *noninvasive measurability*. We have then established the fact that the maximum success probability of each $n \mapsto 1$ RAC with best classical strategy is connected to the maximum noninvasive-realist bound. Moreover, any non-zero quantum advantage of a $n \mapsto 1$ RAC was equivalent to the violation of the corresponding temporal inequality.

Next, using an alternative derivation of the noninvasive-realist model, we showed that any non-zero advantage of RAC can be used to certify genuine randomness.

This is particularly significant as all the previously proposed protocols based on RAC do not exhibit genuine randomness for the arbitrary quantum advantage of RAC [74, 75, 116]. Before concluding a few remarks are in order. The maximum success probability using quantum strategy for a general $n \mapsto 1$ RAC is hard to compute for large n, and numerical strategies may be needed to tackle this problem. Finally, it may be reemphasized that our proposed protocol based on LGI violation is amenable for experimental realization [106], and hence, the generation of genuine randomness without entanglement based on our protocol might be exemplary for practical purposes.

CHAPTER 4

DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION USING RANDOM QUANTUM STATES

4.1 Introduction

In the realm of encryption, Quantum Cryptography [121] offers safe encryption solution that leverages the inherent principles of quantum mechanics rather than relying on the computational difficulty of classical algorithms like the Rivest-Shamir-Adleman (RSA) algorithm. The most well-established protocol in this field is Quantum Key Distribution (QKD) [122], which enables two parties to share a secret key with security guaranteed by the laws of quantum mechanics.

An alternative approach, known as Post-Quantum Cryptography, leverages classical cryptographic techniques to construct public-key encryption schemes that remain

resistant to attacks from quantum computers [123]. However, while these methods are designed to withstand currently known quantum attacks, the security of QKD remains independent of any future advancements in computational power or algorithms.

As we already mentioned in chapter 2, this chapter is based on entanglement-based QKD.

Device imperfections and implementation loopholes in realistic QKD setups can compromise the security of any QKD protocol. However, device-independent QKD protocols based on entanglement remove such concern over imperfections by demonstrating QKD using uncharacterized devices [124, 125]. Security can be checked using classical constraints on correlations between the parties via Bell's inequalities [6], though it has been shown recently, that violation of Bell-CHSH inequality is not sufficient for secure QKD [126, 127]. Device-independence allows QKD with uncharacterized devices [124, 128–131]. Its security has been proven effective against collective attacks [132, 133]. On a different front, device-independent quantum secure direct communication has been recently proposed [134–136]. Moreover, several interesting works have been proposed on QKD such as long-distance continuous-variable QKD using optical fiber [137], twin-field QKD [138, 139], reference-frame independent QKD using coherent states [140], and so on.

The majority of previous research on quantum key distribution (QKD) has predominantly focused on specific classes of pure states [141]. However, in practical scenarios, maintaining perfect pure states is highly challenging due to environmental decoherence, which naturally leads to the formation of mixed states. A comprehensive understanding of QKD requires investigating the role of these mixed states. While the performance of two-qubit and qutrit pure states in entanglement-based QKD has been extensively studied [54, 121, 142–144], research on mixed states remains limited [121, 143]. This is primarily due to the complexity introduced by multiple state parameters, which lead to multivariate optimization problems. In this chapter, we aim to bridge this gap by thoroughly analyzing the performance of two-qubit mixed states of all ranks in entanglement-based QKD.

Random states appear naturally in any experimental system. They not only arise naturally in chaotic processes, but can be generated also in a systematic manner based on

randomness in the outcome of quantum measurements [145]. Moreover, against the intuition of observing random behavior, it has been found that random states exhibit some universal features. Examples include the performance of random states for certain communication tasks wherein it has been shown that the dense coding capacity as well as the teleportation fidelity decrease with increase in the rank of randomly generated states [146].

Randomly generated density matrices [147–150] serve as a crucial tool for analyzing the behavior of typical quantum states within the state space. These random states have played a significant role in addressing fundamental questions in quantum information theory, including the disproof of a long-standing conjecture regarding the additivity of minimal output entropy [151]. Additionally, they have been employed in understanding system-environment interactions, particularly in leveraging non-Markovian noise for constructive feedback [152]. Recently, advantage of employing two random key basis instead of one in device independent(DI)-QKD has been demonstrated [153]. Some recent interesting works have been proposed on DI-QKD such as rate–distance limit of DI-QKD [154], photonic demonstration of DI-QKD [155], and so on. The above studies motivate us to explore whether some universal understanding of DI-QKD tasks could be obtained using random states.

Here, we analyze the performance of Haar-uniformly generated random states in entanglement-based QKD protocols. Specifically, we evaluate the average secure key rate for states of varying ranks in device-independent QKD (DI-QKD). To begin, we assess the quantum resources of these random states by measuring their entanglement and Bell nonlocality. Our findings reveal that the secure key rate in DI-QKD diminishes as the rank of the random state increases. Furthermore, we establish that for two-qubit mixed states of any rank with a fixed degree of entanglement, the secure key rate in DI-QKD falls within a spectrum defined by the secure key rates of pure states and Werner states, under both general and optimal collective attack strategies.

The chapter is organised in the following way. In the next section we recapitulate the generation of random states of different ranks with the aim of utilizing them as resource for DI-QKD. In Sec.(4.3), we present the normalized distribution of entangle-

ment . In Sec.(4.4), we present the device-independent QKD scenario under consideration and provide our analysis for the resourcefulness of the randomly generated states in terms of Bell-nonlocality, as well as their secure key rates. In Sec.(4.5), we have shown the upper and lower bounds on the minimum secure key rate of mixed two-qubit random states. Finally, we summarized and conclude this chapter in Sec.(4.6).

4.2 Haar Uniform Quantum Random States

Let us first briefly describe the procedure to generate random states. We randomly simulate complex numbers from a Gaussian distribution with mean 0 and standard deviation unity, denoted $G(0,1)$. This ensures that the measure is Haar uniform.

Pure states: Two-qubit pure states are then randomly generated using four such random complex numbers.

$$|\psi_1\rangle = \sum_{ij} c_{ij} |i\rangle \otimes |j\rangle \tag{4.1}$$

Here, $|i\rangle, |j\rangle \in \{|0\rangle, |1\rangle\}$ form the computational basis of the first and second qubit respectively.

Mixed states: Random two-qubit mixed states of various ranks are generated from an appropriate pure state in a product Hilbert space by partial tracing of the suitable subsystem.

Rank-2: Mixed two-qubit density matrices of rank-2 are generated from random tripartite pure states in $2 \otimes 2 \otimes 2$ by tracing out any one of the three qubits [146, 152].

$$|\psi_2\rangle = \mathrm{Tr}_i \Big[\sum_{i,j,k=0,1} c_{ijk} |i\rangle \otimes |j\rangle \otimes |k\rangle \Big] \tag{4.2}$$

Rank-3: Mixed two-qubit density matrices of rank-3 are generated from random tripartite pure states in $3 \otimes 2 \otimes 2$ by tracing out the qutrit [146, 152].

$$|\psi_3\rangle = \mathrm{Tr}_i \Big[\sum_{i=0,1,2} \sum_{j,k=0,1} c_{ijk} |i\rangle \otimes |j\rangle \otimes |k\rangle \Big] \tag{4.3}$$

Rank-4: Mixed two-qubit density matrices of rank-4 are generated from random quadripartite pure states in $2 \otimes 2 \otimes 2 \otimes 2$ by tracing out any two of the four qubits

[146, 152].

$$|\psi_4\rangle = \mathrm{Tr}_{ij}\Big[\sum_{i,j,k,l=0,1} c_{ijkl}\,|i\rangle \otimes |j\rangle \otimes |k\rangle \otimes |l\rangle\Big] \tag{4.4}$$

4.3 Normalized Distribution of Entanglement

Quantum mechanics offers several non-classical resources that give advantage in different communication tasks. Here, we are interested in the following resources: **entanglement** and **Bell-nonlocality**. In this section, we only discuss the entanglement part, and in the next section, we will discuss the Bell-Nonlocality part.

Entanglement: Entanglement of any two-qubit state can be quantified using Negativity and Logarithmic Negativity. Using Eq.(1) to (4) we generate rank-1 to rank-4 random states respectively, and we take partial transpose of those numerically generated states and determine the eigenvalues $\{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$. Logarithmic Negativity is defined as $LN = \log_2(2N + 1)$ (where, $N(= |\sum_j \lambda_j|)$ is Negativity and λ_j are the negative eigenvalues of the partially transposed state).

We study the performance of randomly generated states in DI-QKD tasks. Our entire calculations and analysis are based on 10^6 Haar uniformly generated states for each rank. The distribution of states is quantified in terms of the following parameters, as defined below.

For a given rank of random state, the normalized distribution of quantum resource is defined as the ratio between the number of states having an amount of QR, i.e., $a \leq Q_c \leq b$, with Q_c being the measure of quantum correlation (entanglement or Bell nonlocality) and the total number of generated random states. Mathematically,

$$\mathbb{F}_D^n = \frac{\text{Number of states with } Q_c \in [a, b]}{N_0} \tag{4.5}$$

with N_0 being the total number of simulated states. Here, 'n' stands for normalized and 'D' stands for distribution. Q_c denotes logarithmic negativity and violation of Bell-CHSH inequlity, in case of entanglement and Bell-nonlocality, respectively. We divide the range of $Q_c \in (0, 1]$ in 10 parts to determine the normalized distribution of quantum resource in simulated random states. The normalized distribution of entan-

glement is given by

$$E_{nD} = \frac{\text{Number of states with} LN \in [a, b]}{N_0} \tag{4.6}$$

We investigate the performance of the random states based on entanglement and Bell-nonlocality . As observed from previous studies [146], the number of resourceful state decreases as the rank increases. For a particular rank, the fraction of Bell-nonlocal states is lower than that of entangled states, exemplifying the hierarchy of these correlations for a large number of random states [156].

In Fig. (4.1) we plot the normalized distribution of entangled random two-qubit states against Logarithmic negativity. As shown in fig. (4.1), a large fraction of simulated pure states 85% have higher value of logarithmic negativily (0.5 and above), whereas mixed state have percentage 43.8, 16.6, 5.5 respectively for rank-2, 3, 4 states that have logarithmic negativity 0.5 and above. This implies that as the rank of the state increases, its tendency to have higher value of entanglement decreases. We observed that the quantum resourcefulness of the state decreases as the rank increases. The rest of the chapter attempts to answer whether similar behavior is observed in the entanglement based quantum key distribution task. Specifically, we address the effect of rank and QR of the random state on its performance in DI-QKD.

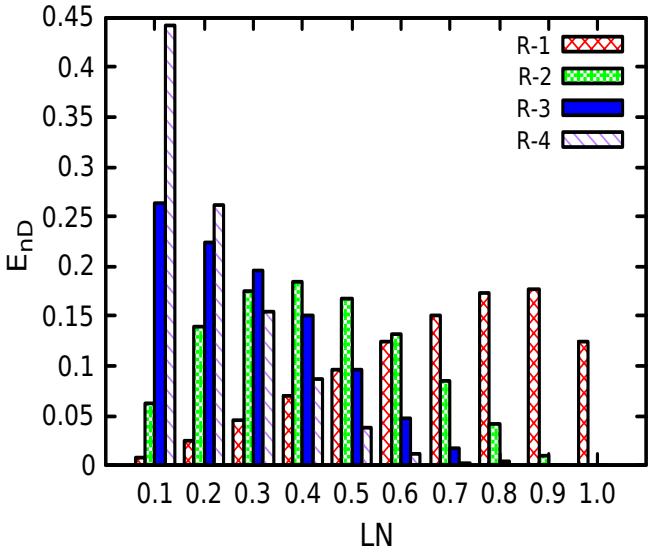


Figure 4.1: (Color online) Normalized distribution of entangled (E_{nD}) random two-qubit states (vertical axis) against Logarithmic Negativity (LN) (horizontal axis). We mention only the upper value of LN in the horizontal axis for brevity. Thus, 0.1 denotes the range (0, 0.1].

4.4 Bell-Nonlocality and Secure Key Rate

4.4.1 DI-QKD protocol

Let us first briefly recapitulate the protocol of DI-QKD. Consider the two uncharacterized parties Alice and Bob sharing a bipartite entangled state ρ_{AB} in $\mathbb{C}^2 \otimes \mathbb{C}^2$ as shown in fig.(4.2). The two parties want to establish a secure key. For this, each of them perform dichotomic measurements in two mutually unbiased measurement bases (MUBs) and get two outcomes. Alice performs measurement of the observables randomly chosen from the input $x \in \{0,1\}$ and gets the outcome $a \in \{0,1\}$. Similarly, Bob randomly chooses the input measurement $y \in \{0,1\}$ and gets the outcome $b \in \{0,1\}$. In the post-processing stage, both the parties publicly compare their input measurements and keep only those outcomes for which their inputs are correlated.

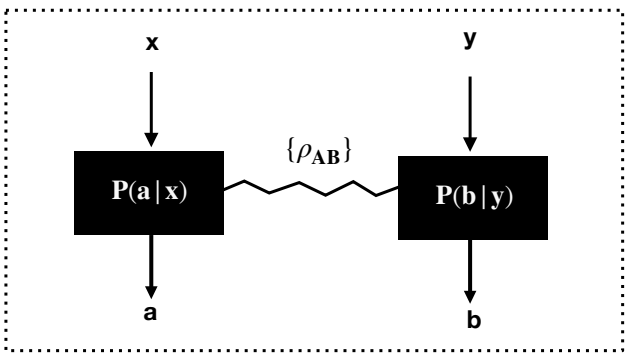


Figure 4.2: (Coloronline) The device-independent quantum key distribution task.

Our protocol is similar to E91 protocol [54]. In a DI-QKD protocol, the devices are untrusted. The security is guaranteed by checking Bell-inequality violation from the measurement statistics. The basic steps of our DI-QKD protocol are as follows:

Quantum state preparation: Alice generates a pair of entangled photons at her lab (random two-qubit state). She keeps one of the entangled photons and sends the other to Bob's lab through a quantum channel.

Quantum measurement: Alice performs measurement of the observable randomly chosen from the input $x \in \{0,1\}$ and gets the outcome $a \in \{0,1\}$. Similarly, Bob randomly chooses the input measurement $y \in \{0,1\}$ and gets the outcome $b \in \{0,1\}$.

During post-processing stage, Alice and Bob keep the cases when their inputs are correlated and discard all other cases.

Bell-inequality violation: Alice and Bob use a fraction of inputs and outputs to ensure the Bell-inequality violation. Those cases are also discarded as the output values are disclosed.

Secure symmetric key generation: Alice and Bob perform bi-directional error correction on their output values and perform privacy amplification on the corrected keys depending upon the information disclosed (function of the quantum bit error rate (QBER)) and Eve's attacking strategy. The final keys are the secured symmetric keys. The equality can be verified using a family of universal hash functions.

4.4.2 Secret key rate under different Eve's attack strategies

Let us determine the secret key rate under different Eve's attack strategies. In the ideal scenario with no attack, Alice and Bob are left with perfectly identical keys. However, imperfections in state preparation, transmission, measurement processes and eavesdropping can yield differences in their key strings. Alice and Bob can estimate the error rate after comparing a small portion of their secure key. Formally, QBER for a given state ρ_{AB} is defined as the average mismatch between the outcomes of Alice and Bob. Let us denote Alice's two MUBs as $\{|x_a^\alpha\rangle\}_{a=0}^1$ (for $\alpha \in (0,1)$) which are correlated to Bob's MUBs $\{|y_b^\alpha\rangle\}_{b=0}^1$ (for $\alpha \in (0,1)$). The perfect correlation between Alice and Bob would implies that Alice and Bob perform measurements in the same basis and when Alice's outcome is $|x_a^1\rangle$, Bob's outcome must be $|y_b^1\rangle$. In the non-ideal scenario, there can be non-zero probability of observing $|x_a^1\rangle$ in Alice's subsystem and $|y_b^1\rangle$ in Bob's subsystem where $a \neq b$. Hence, the QBER which is an average of all these mismatch probabilities can be expressed as

$$\begin{aligned} QBER &= \frac{1}{2}\sum_{\alpha=0}^{1}\sum_{a\neq b=0}^{1}\langle x_a^\alpha y_b^\alpha|\rho_{AB}|x_a^\alpha y_b^\alpha\rangle \\ &= \frac{1}{4}(2-|\lambda_1|-|\lambda_2|) \end{aligned} \tag{4.7}$$

where λ_1 and λ_2 are the two largest singular values of the correlation matrix T ($t_{ij} = \mathrm{Tr}[(\sigma_i \otimes \sigma_j).\rho_{AB}]$, where $\sigma_{i(j)}$ are the Pauli matrices) each of which is bounded from

above by 1.

The security of entanglement based QKD necessarily requires the demonstration of nonlocal correlations. So, for example, violation of Bell-CHSH inequality is required for the security of a DI-QKD since, none of the two parties are trusted in this scenario. Note that the violation of the Bell-CHSH inequality is the necessary criterion and not sufficient [127], and hence, there are states that violate the Bell-CHSH inequality but still are not useful for the task of key distribution.

Note that for a given two-qubit state ρ_{AB} the maximum value of Bell-CHSH inequality that can be achieved for optimal measurements is $2\sqrt{\lambda_1^2 + \lambda_2^2}$ (say, S). Using Eq.(4.7) QBER can be written in terms of Bell-Nonlocality (S) as

$$QBER = \frac{1}{2}\left(1 - \sqrt{\frac{S^2}{16} + \frac{1}{2}|\lambda_1||\lambda_2|}\right) \tag{4.8}$$

From this above equation we can see that with increase of Bell-Nonlocality (S), the QBER may decrease. The security proof provides a bound on the rate at which Alice and Bob can extract a secure key. The rate at which unconditionally secure key against Eve's attacks can be extracted is given by

$$r(\rho_{ABE}) = I(A:B) - I(A:E) \tag{4.9}$$

where, ρ_{ABE} is the joint state between Alice, Bob and Eve and I is the Holevo quantity or the quantum mutual information. Usually, the joint state ρ_{ABE} is not known to Alice and Bob. So, the key rate is calculated from the QBER estimation after the error correction algorithm and the effective state after the postselection (sifting etc.) is given by

$$\xi(\rho_{AB}) = \sum_u p(u)\rho_{XYE}^u \otimes |u\rangle\langle u| \tag{4.10}$$

The effective key rate is then,

$$\bar{r}(\xi(\rho_{AB})) = \mathbb{I}(\xi(\rho_{AB})) - \mathbb{I}'(\xi(\rho_{AB})) \tag{4.11}$$

where, $\mathbb{I}(\xi(\rho_{AB})) = \sum_u p(u) I_u(X:Y)$ and $\mathbb{I}'(\xi(\rho_{AB})) = \sum_u p(u) I_u(X:E)$. Eve has the freedom to choose any attack, if it creates a state ρ_{AB} contained in the set of all bipartite

states $\{\rho_{AB}\}$ that are compatible with the measurement outcomes $p(a,b|x,y)$, and have a given reduced state ρ_A. The minimum secure key rate under such assumption is

$$r_{\min} = \inf_{\{\rho_{AB}\}} \bar{r}(\xi(\rho_{AB})) \tag{4.12}$$

Since the global state shared between Alice, Bob and Eve are not known, the secure key rate can be determined as a function of the QBER using Eq. (4.10), (4.11) and (4.12).

Secret key rate under collective attacks(CA): In the case of collective attacks, the eavesdropper applies the same attack on each system of Alice and Bob. Here the minimum secure key rate is a function of QBER(Q) and S. The minimum secure key rate is given by [132]

$$r_{\text{Cmin}} \geq 1 - h(Q) - h\left(\frac{1+\sqrt{(S/2)^2-1}}{2}\right) \tag{4.13}$$

Where h is binary entropy and S (= $2\sqrt{\lambda_1^2+\lambda_2^2}$) is the Bell-CHSH violation.

Secret key rate under optimal symmetric collective attacks(OSCA): For the case of optimal symmetric collective attacks (attack optimised over the symmetries of the protocol, state and measurements of the communicating parties) by the eavesdropper in entanglement assisted protocols for two-qubit states with two measurement settings per qubit, the minimum secure key rate is given by [133]

$$r_{\text{Smin}} = 1 + 2(1-Q)\log_2(1-Q) + 2Q\log_2 Q \tag{4.14}$$

We have two separate conditions for the security of a DI-QKD protocol. One being $r_{\text{C(S)min}} > 0$ for a secure key to be distilled while the second is the requirement that the underlying entangled state violates the Bell-CHSH inequality. While it can be seen that there exist no states with non-vanishing secure key and no Bell-CHSH violation, there do exist states which show Bell-CHSH violation but have vanishing secure key.

4.4.3 Normalized and mean distribution of Bell-nonlocality

We now study the behaviour of Bell-nonlocal correlations and minimum secure key rate of random states in DI-QKD.

The normalized distribution of Bell-nonlocality is defined as

$$N_{nD} = \frac{\text{Number of states with Bell violation} \in [a, b]}{N_0} \tag{4.15}$$

The mean distribution of quantum resource is the ratio between the total number of quantum resourceful state and the total number of generated random states for a fixed rank, given by

$$\mathbb{F}_D^m = \frac{\sum \mathbb{F}_D^n}{N_0} \tag{4.16}$$

where we have summed over the entire range of a and b. Here, 'm' stands for mean distribution. This quantity represents the fraction of resourceful states. We consider Bell-nonlocal correlations as quantum resource and analyse the mean distribution of the Bell-nonlocality for the randomly simulated random states as follows:

$$N_{mD} = \frac{\text{Number of states violating Bell-inequality}}{N_0} \tag{4.17}$$

In particular, we first analyse the normalised distribution of Bell-nonlocal correlations (Eq.(4.5)) as shown in fig. (4.3). It is seen that the tendency of a random state to achieve large value of Bell-CHSH inequality (2.5 and above) decreases with increasing rank. We find 39.9, 1.9, 0.05, and 0.001 to be the respective percentage of the simulated rank-1, 2, 3 and 4 states that achieve Bell-inequality value of 2.5.

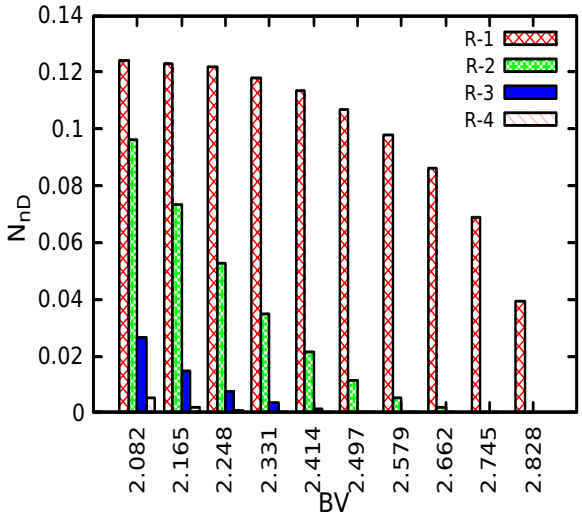


Figure 4.3: (Color online) Normalized distribution of Bell nonlocal (N_{nD}) random two-qubit states (vertical axis) against the violation of the Bell-CHSH inequality (BV) (horizontal axis). We mention only the upper value of the Bell's inequality violation in the horizontal axis for brevity of notation. Thus, 2.082 denotes the range (2,2.082].

We next perform a comparative study of the mean distribution of $r_{\mathrm{C(S)\,min}}$ and Bell-nonlocality of all four ranks. The fraction of random states that have non-zero value of the secure key rate is given by

$$\mathbb{F}_D^r = \frac{N^r}{N_0} \tag{4.18}$$

where N^r is the number of states that have non-zero value of secure key rate in DI-QKD. Using Eqs. (4.16) and (4.18), we plot the respective distributions for all four ranks in Fig.(4.4).

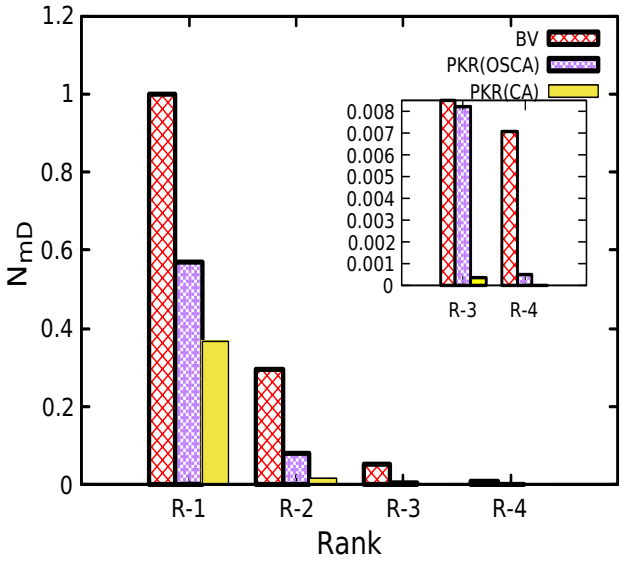


Figure 4.4: (Coloronline) The mean distribution of Bell-nonlocal (N_{mD}) random two-qubit states as well as the fraction of random two-qubit states that have minimum secure positive key rate (PKR), $r_{\mathrm{C(S)min}}$ for the given rank of the states under optimal symmetric collective attacks(OSCA) and collective attacks(CA) for different rank of the random two-qubit state.

It is seen that the number of randomly simulated states that are Bell-nonlocal as well as the states which provide positive minimum secure key rate decreases with the increase of the rank of the states. The percentages of states that are Bell-nonlocal and give positive secure key rate are 56.8, 8.2, 0.70 and 0.05 for rank-1, 2, 3 and 4, respectively under optimal symmetric collective attacks. Similarly, under collective attacks, the percentages are 36.8, 1.6, 0.04 and 0.001 for rank-1, 2, 3 and 4, respectively, under collective attacks. Hence, the number of states giving positive secret key rate under general collective attack are less than that under optimal symmetric collective attacks.

Note that the respective percentage of Bell-nonlocal states are higher in both cases. This again implies that all Bell-nonlocal states are not suitable for DI-QKD, reinforcing a similar claim in a recent work [127]. Moreover, the rate of decrease in $r_{\mathrm{C(S)min}}$ is more prominant than Bell-nonlocality implying that higher rank Bell-nonlocal states are less useful for DI-QKD. The number of states that are Bell non-local and have positive secure key rate under general collective attacks is less in comparison to that in the optimal symmetric collective attack for every rank. This behaviour is expected because in the general collective attack strategy, Eve has the freedom to devise a strategy to maximise mutual information whereas in the optimal symmetric attack, the quantum protocol, state and measurement symmetries put constraints over the strategy of Eve. This constrains Eve's mutual information and relaxes the secure key rate requirements.

4.4.4 Average Key rates of Quantum Random States

For a given rank of the random state, the average secure key rate is given by the ratio of the sum of the secure key rate of the simulated states to the number of states that have non-zero value of the secure key rate, as

$$\bar{r} = \frac{\sum_i r_i}{N'} \tag{4.19}$$

where, r_i is the secure key rate of the i^{th} state and N' is the total number of states that have non-zero value of the secure key rate. The average key rate computed using Eq. (4.19) in DI-QKD under optimal symmetric collective attacks is 0.36, 0.15, 0.09 and 0.07 for rank-1, 2, 3 and 4 states, whereas, under collective attacks, the average key rate is 0.34, 0.14, 0.09 and 0.06 for rank-1, 2, 3 and 4 states, respectively, as shown in Table-(4.1). The average key rate in both situations where Eve does a general or optimal collective attack decreases with increasing rank implying that the tendency to generate positive secure key rate decreases with increasing rank. The average key rates in both the attack strategies are nearly the same for a given rank. Our entire calculations are based on 10^6 Haar uniformly generated states for each case. We find that a large fraction of pure states have positive value of minimum secure key rate and are Bell-nonlocal in comparison with the mixed two-qubit states. This is in accordance with a previous study [152] where it was observed that large fraction of randomly generated

mixed states are Bell local states. However, this is in contrast with the observation for teleportation fidelity where it was found that with increasing rank, relative number of states that are local but gives non-classical fidelity increases [146].

Table 4.1: Average secure key rate in DI scenario

	No. of random states that violate the Bell-CHSH inequality (among 10^6 random states)	No. of random states that have positive secure key rate under OSCA	No. of random states that have positive secure key rate under CA	Average secure key rate (OSCA)	Average secure key rate (CA)
R-1	1000000	568522	368453	0.36	0.34
R-2	297642	82314	16662	0.15	0.14
R-3	54464	7060	423	0.09	0.09
R-4	8258	498	11	0.07	0.06

4.5 Upper and Lower bound on the minimum secure key rate of random states

We observe that on average, the quantum resourcefulness of the randomly generated states decreases with an increase in rank and this could be the reason that the performance of the state also decreases in the DI-QKD task as its rank increases. In particular, pure states perform better than rank-2 states, and in turn, rank-2 states perform better than rank-3 and rank-4 states. Interestingly, there are states of different rank which have the same value of the entanglement, but have different value of the minimum secure key rate. To illustrate this feature, we next perform a comparative study of pure states, general rank-2 states and Werner states. Werner states are the simplest and most studied two-qubit mixed states that help in understanding the effect of noise on maximally entangled Bell states. We determine the minimum secure key rate of these three states in terms of the negativity to show the distinction in performance for the same value of the entanglement.

An arbitrary two-qubit pure state in a Schmidt decomposition has the form

$$|\psi_p\rangle = \cos\frac{\theta}{2}|00\rangle + \sin\frac{\theta}{2}|11\rangle \tag{4.20}$$

where, $|0\rangle$ and $|1\rangle$ are the eigenstates of the reduced density matrices, and eigenvalues of the local density matrices are $\cos^2\frac{\theta}{2}$ and $\sin^2\frac{\theta}{2}$. The negativity of the pure state is

given by the the square root of the determinant of its reduced density matrix, i.e., $\frac{\sin\theta}{2}$.

Any two qubit mixed state of rank-2 can be expressed as,

$$\rho_2^2 = p_1|\psi_1\rangle\langle\psi_1| + (1-p_1)|\psi_2\rangle\langle\psi_2| \tag{4.21}$$

where, $|\psi_1\rangle = \alpha|0\eta_1\rangle + \beta|1\eta_2\rangle$, $|\psi_2\rangle = \alpha|0\eta_1^{\perp}\rangle + \beta|1\eta_2^{\perp}\rangle$, $|\eta_1\rangle = a|0\rangle + b|1\rangle$ and $|\eta_2\rangle = a'|0\rangle + b'|1\rangle$ with $|\eta_1^{\perp}\rangle$ and $|\eta_2^{\perp}\rangle$ being orthogonal states to $|\eta_1\rangle$ and $|\eta_2\rangle$ respectively. The coefficients are taken to be real for simplicity and each of the states are normalised, i.e., $a^2 + b^2 = a'^2 + b'^2 = \alpha^2 + \beta^2 = 1$ and $0 \leq p_1 \leq 1$ The entanglement of state ρ_2^2 in Eq. (4.21) is given by

$$N_2 = \frac{1}{2}\left[\sqrt{p_1^2 - x} - p_1\right], \quad \text{if } p_1 < 0.5 \tag{4.22}$$

$$N_2 = \frac{1}{2}\left[\sqrt{(1-p_1)^2 + x} - (1-p_1)\right], \text{ if } p_1 > 0.5 \tag{4.23}$$

where, $x = 4\alpha^2\beta^2(a'b - ab')^2(2p_1 - 1)$. The state parameter p_1 of rank-2 state (4.21) can be expressed in terms of the negativity, as

$$p_1 = \frac{N^2 - \alpha^2\beta^2(a'b - ab')^2}{N - 2\alpha^2\beta^2(a'b - ab')^2}, \text{ if } p_1 < 0.5 \tag{4.24}$$

$$p_1 = \frac{N(N+1) + \alpha^2\beta^2(a'b - ab')^2}{2\alpha^2\beta^2(a'b - ab')^2 + N}, \text{if } p_1 > 0.5 \tag{4.25}$$

Next, the two qubit Werner state is given by

$$\rho_W = p|\phi^+\rangle\langle\phi^+| + \frac{(1-p)}{4}I_4 \tag{4.26}$$

where $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with $0 \leq p \leq 1$ and I_4 being the identity matrix in Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2$. One can take any other maximally entangled Bell state instead of $|\phi^+\rangle$ in the expression of the Werner state but the final expression of the minimum secure key rate is same. The negativity of the Werner state is $\frac{3p-1}{4}$.

We now calculate the secure key rate of the rank-2 state (4.21) in terms of negativity (N). Similarly, we calculate the secure key rate of the pure state and Werner state in terms of the negativity (see Appendix (B) for the respective expressions). In Fig. (4.5) we plot the minimum secure key rate of the pure state, the general rank-2 state and the

Werner state in terms of negativity. From the figure it is clear that states with the same value of the negativity can have different performance ($r_{\mathrm{C(S)min}}$) in the DI-QKD task. It can also be seen that the secure key rate of the rank-2 two-qubit state lies in between the secure key rate of pure state and the Werner state at same value of negativity for both categories of collective attack, i.e.,

$$r_{C(S)\mathrm{min}}(\rho_p) \geq r_{C(S)\mathrm{min}}(\rho_2^2) \geq r_{C(S)\mathrm{min}}(\rho_W) \tag{4.27}$$

where $r_{C(S)\mathrm{min}}$ is the minimum secure key rate in our DI-QKD scenario (4.14).

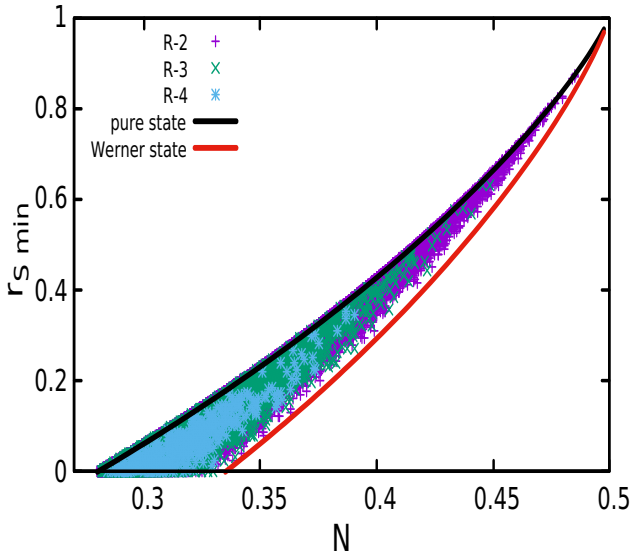


Figure 4.5: (Coloronline) Minimum secure key rate of randomly generated rank-2, rank-3, rank-4 states, pure state and the Werner state in DI-QKD are plotted versus the negativity for the case of optimal symmetric collective attacks. It is clear that the pure state and the Werner state provides the upper and lower bound respectively, on the minimum secure key rate of mixed two-qubit states in DI-QKD.

We further find numerically, that rank-3 and rank-4 states also have the minimum secure key rate within the envelope formed by the pure state and the Werner state for the same value of negativity. From Fig.(4.5) it can be observed that 78.6% of rank-2 states, 39.8% of rank-3 states, and 22.7% of rank-4 states have r_{Smin} 0.1 and above under OSCA. Further, from Fig.(4.6), it follows that 74.6% of rank-2 states, 28.2% of rank-3 states, and 16.4% of rank-4 states have r_{Cmin} equals 0.1 or above under CA. All of them are inside the envelope formed by the pure state and the Werner state. Our above analysis can be summarized as following result:

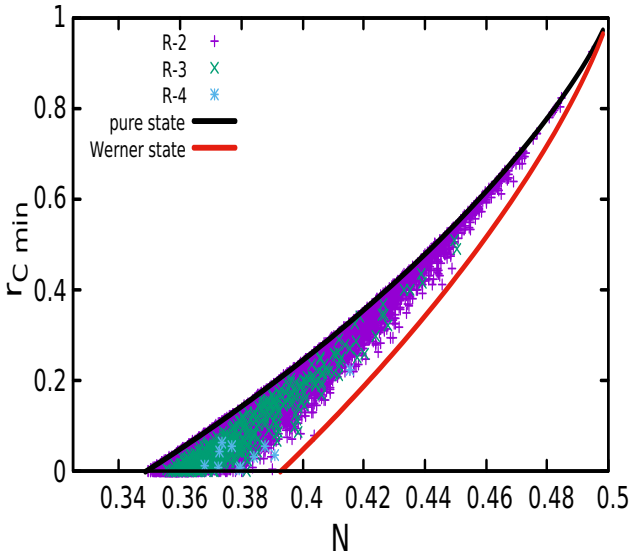


Figure 4.6: (Coloronline) Minimum secure key rate of randomly generated rank-2, rank-3, rank-4 states, pure state and the Werner state in DI-QKD are plotted versus the negativity for the case of collective attacks. It is clear that the pure state and the Werner state provides the upper and lower bound respectively, on the minimum secure key rate of mixed two-qubit states in DI-QKD.

Result:

> **"The secure key rate of any mixed two qubit state in DI-QKD is lower bounded by the secure key rate of the two qubit Werner state and upper bounded by the secure key rate of the pure state possessing the same value of the negativity under general as well as optimal collective attacks by Eve."**

4.6 Summary and Conclusion

Quantum key distribution is set to become an integral part of modern cryptographic applications. In theory, unconditional security has been shown for the prepare and measure as well as the entanglement based schemes. However, in practice, perfect quantum key distribution cannot be achieved due to the presence of different decohering factors, device imperfections and implementation loopholes. Therefore, it is of prime importance to study quantum key distribution protocols using randomly generated states rather than confining to specific set of states, with the aim of obtining a universal perspective.

In this work, we have studied the secure key rate of randomly generated two-qubit states of all four ranks in entanglement based QKD. Our analysis is based on numerical results obtained by considering 10^6 states corresponding to each rank. We first estimate the fraction of states in each rank which are Bell-nonlocal, and the fraction of states which yield positive secure key rate in DI-QKD under general as well as optimal collective attacks by Eavesdropper. We show that both Bell-nonlocality and the minimum secure key rate decrease with the increase of rank in general as well as optimal attack strategy, which is a fundamental feature of such randomly generated states.

From our analysis we have observed that with increasing rank the decrease in secure key rate is more pronounced compared to Bell-CHSH violation. The ratio of the number of states that have quantum resource (entangled as well as Bell-nonlocal) as a function of rank decreases slowly in comparison to the ratio of the number of states that give positive secure key rate as a function of rank. For example, the ratio of the number of rank-3 states that are Bell-nonlocal to the number of rank-2 states that are Bell-nonlocal is 0.183, whereas the respective ratio for the number of states that give positive key rate is only 0.085 under optimal symmetric collective attacks and 0.025 under collective attack respectively. It may be noted that quantum resourcefulness is a necessary condition to obtain secure key rate. However, the secure key rate generation is more demanding, and hence, the number of states that give secure key rate is lesser compared to the number of resourceful states.

Our results further show that states with the same magnitude of entanglement can lead to different values of the secure key rate. We demonstrate that the minimum secure key rate of all two-qubit mixed states is upper bounded by the key rate of the pure state, and lower bounded by the key rate of the Werner state possessing the same value of entanglement quantified by their negativity in both optimal as well as general collective attack strategy. It would be worth studying if the above bounds can be obtained using analytical methods. It might also be interesting to study in future the effect of statistical fluctuations in the number of randomly generated states on the above bounds. Moreover, our present analysis should motivate further studies on the resilience of random states against particular quantum attacks in QKD protocols, as well as under other sources of error such as channel loss and misalignment rate [157].

A detailed study using random state provides a source-independent analysis and establishes an efficiency and performance profile of the quantum task under consideration. For example, the random states can give a precise idea about the performance of higher rank mixed states in tasks like quantum multiparty cryptography [158], secure quantum secret sharing [159], quantum conference key agreement [160], quantum private query [161] and quantum secure direct communication [134, 135]. This in turn should further be useful in understanding the efficiency of such tasks under decoherence. This is so because decoherence can be modelled as a black box whose input may be a random state and the output is some different random state, in order to analyse the efficacy of employing random states in various quantum information protocols.

CHAPTER 5

HARNESSING QUANTUM ADVANTAGE FROM GENERAL CONTEXTUALITY SCENARIOS

5.1 Introduction

The discrepancy between quantum theory and the framework of generalized noncontextuality, commonly termed generalized quantum contextuality, is a fundamental indication of the nonclassical nature of quantum mechanics [41, 42, 162–182]. From an operational standpoint, contextuality plays a crucial role in enabling quantum advantages over classical systems in a variety of information processing and communication protocols [183–193].

Noncontextuality adheres to the Leibnizian principle that assigns identical realist descriptions to operationally equivalent experimental procedures. For example, prepara-

tion noncontextuality assigns identical epistemic states to preparation procedures that are indistinguishable, meaning all measurements yield identical statistics. Similarly, measurement noncontextuality assigns identical response schemes to operationally indistinguishable measurement procedures. Generalized noncontextuality combines both preparation and measurement noncontextuality in scenarios involving prepare-and-measure experiments. Like Bell inequalities, generalized noncontextuality implies empirical inequalities known as noncontextuality inequalities (NCI). Quantum theory prescribes preparations and measurements that satisfy operational indistinguishability yet violate NCI.

Quantum theory can exhibit preparation contextuality by violating noncontextual inequalities that involve indistinguishability conditions among mixtures of preparation procedures. Other fundamental nonclassical phenomena, including violations of Bell inequalities and implications from the Kochen-Specker theorem [10], also highlight the presence of preparation contextuality in quantum mechanics. Beyond its foundational importance, preparation contextuality has been explored for its practical applications in areas such as oblivious communication [183,184,186], state discrimination [173,191], and randomness certification [192].

A contextuality scenario is defined by the number of preparations, measurements, and measurement outcomes, along with the operational indistinguishability conditions for preparation and measurement procedures in their various convex mixtures. Given a contextuality scenario, finding a set of empirical criteria fulfilled by any noncontextual theory is a demanding task of both foundational and operational importance. As pointed out by Schmid *et al.* [42], in a contextuality scenario, the set of empirical statistics possessing noncontextual explanations forms a convex polytope. Consequently, the inequalities representing the facets of that polytope combine to provide the necessary and sufficient criteria for empirically witnessing noncontextuality. Schmid *et al.* [42] also formulate a computational technique to retrieve all the facet inequalities applicable to arbitrary contextuality scenarios.

However, the method for determining the facets of the noncontextual polytope is computationally expensive. In particular, the noncontextual polytope is a product of two polytopes, one for preparations and the other for measurements. To obtain the facet

inequality of the noncontextual polytope, one needs to compute the extremal points of a D_P-dimensional polytope associated with the preparations to find the extremal epistemic states, which are probability distributions over the ontic state space and the extremal points of a D_T-dimensional polytope associated with product polytope. It turns out, typically, D_P increases polynomially with the number of measurements and D_T increases polynomially with the number of measurements times the number of measurements, owing to the polynomial increase in the number of distinct ontic states one needs to consider. This feature of the noncontextual polytope differs strikingly from the respective polytopes of local correlations in Bell scenarios and noncontextual correlations in Kochen-Specker contextuality scenarios, wherein it suffices to consider a single ontic state.

The computational challenge of retrieving all facet inequalities for arbitrary contextuality scenarios is significant. Unlike the polytopes of local correlations in Bell scenarios and noncontextual correlations in Kochen-Specker scenarios, which require only a single ontic state, the noncontextual polytope involves more complexity. Thus, it is highly desirable to find efficient methods to identify empirical conditions within the generalized noncontextuality framework, specifically statistical inequalities necessarily satisfied by noncontextual theories. In order to address these fundamental aspects of contextuality, we have proposed a novel and efficient method for retrieving noncontextuality inequalities in any contextuality scenario, needing only a single ontic state to characterize the polytope for preparations. This approach, unlike conventional methods [42], maintains a constant polytope dimension regardless of the number of measurements and their outcomes. This allows us to obtain a polytope that includes the noncontextual polytope more quickly. The facet inequalities of this polytope are noncontextuality inequalities that any noncontextual theory must satisfy. Violations of these inequalities provide sufficient conditions for identifying generalized quantum contextual correlations. We also investigate the robustness with respect to the experimental noise of the quantum violations.

This chapter is organized as follows. In Sec. (5.2) we present details of our approach for obtaining the set of necessary conditions for noncontextuality in an arbitrary contextuality scenario. We describe our method explicitly by elaborating on the signifi-

cant steps of the algorithm for obtaining noncontextuality inequalities, and discuss its merits in contrast to the standard approach. In Sec. (5.3) we discuss computational advantage over finding facets of exact noncontextual polytope. In Sec. (5.4) we investigate various different contextuality scenarios using our methodology by considering six scenarios with indistinguishability conditions only among preparations, as well as two additional scenarios with indistinguishability conditions among both preparations and measurements. These scenarios encompass a range of four to nine preparations and a maximum of three measurements. Consequently, we retrieve a large number of novel NCI as necessary conditions for noncontextuality in these scenarios. In Sec. (5.5) we delve into various intriguing applications stemming from quantum violations of our discovered noncontextuality inequalities. We demonstrate that the quantum violation of some of these inequalities can serve to certify the dimensionality of quantum systems, non-projective measurements, and quantum randomness. Finally, we conclude in Sec. (5.6) with a summary of this chapter.

5.2 Construction of the polytope and method to obtain necessary conditions for noncontextuality

The fundamental underpinning concept entails retrieving the extremal points of a polytope that characterizes the epistemic states corresponding to the preparations in an ontological model. Crucially, these extremal points are formulated to be independent of the number of ontic states while encompassing all feasible response functions describing the measurements.

5.2.1 Polytope characterizing preparations

Let us recall that the presence of indistinguishability conditions in a given contextuality scenario enforces the relationship (2.43) on the epistemic states $\mu(\lambda|x)$, where ontic state λ can take arbitrary possible values. Let us now introduce the following additional variable,

$$q(x,\lambda) = \frac{\mu(\lambda|x)}{\sum_x \alpha_{x|s}\mu(\lambda|x)} =: \frac{\mu(\lambda|x)}{\overline{\mu}(\lambda)}. \tag{5.1}$$

Also, $\overline{\mu}(\lambda) \neq 0$ for all λ. Note that the denominator of the above expression is a constant for all s, and has the expression

$$\overline{\mu}(\lambda) = \sum_x \alpha_{x|s} \mu(\lambda|x). \tag{5.2}$$

By dividing both sides of Eq. (2.43) by $\overline{\mu}(\lambda)$, we find that our new variables $\{q(x,\lambda)\}$ satisfy the following conditions for all λ,

$$\forall s, \sum_x \alpha_{x|s} q(x,\lambda) = 1. \tag{5.3}$$

Hence, for each λ, the collection of variables $\{q(x,\lambda)\}_x$ constitutes a convex polytope that adheres to the positivity constraint $q(x,\lambda) \geqslant 0$, as well as to the constraints implied by Eq. (5.3). Let's denote the extremal points of this polytope as e_p, and the corresponding values at these extremal points as $q(x|e_p)$. In simpler terms, any $q(x,\lambda)$ can be expressed in the following manner:

$$q(x,\lambda) = \sum_{e_p} w(e_p|\lambda) q(x|e_p), \tag{5.4}$$

where $w(e_p|\lambda)$ are convex weights relative to each specific λ.

5.2.2 Polytope characterizing measurements

On the other side, for each λ, the set of quantities $\{\xi(z|\lambda,y)\}_{z,y}$ forms a convex polytope that fulfills the criteria of positivity ($\xi(z|\lambda,y) \geqslant 0$), normalization ($\sum_z \xi(z|\lambda,y) = 1$), and adheres to the constraints dictated by the indistinguishability condition in Eq. (2.44). We assign the label e_m to the extremal points of this polytope, with the corresponding value at these points denoted by $\xi(z|y,e_m)$. Consequently, any $\xi(z|\lambda,y)$ can be represented in the following way

$$\xi(z|\lambda,y) = \sum_{e_m} w(e_m|\lambda) \xi(z|y,e_m). \tag{5.5}$$

Here, $w(e_m|\lambda)$ constitutes a valid set of convex weights pertaining to each λ.

5.2.3 Polytope characterizing combination of preparations and measurements

We now articulate the empirical probability $p_{NC}(z|x,y)$ stemming from non-contextual operational theories in terms of the extremal distributions $q(x|e_p)$ and $\xi(z|y,e_m)$ using following sequence of mathematical relations:

$$\begin{aligned}
p_{NC}(z|x,y) &= \int_\lambda \xi(z|\lambda,y)\mu(\lambda|x)\, d\lambda \\
&= \int_\lambda \sum_{e_m} w(e_m|\lambda)\xi(z|y,e_m)\mu(\lambda|x)\, d\lambda \\
&= \sum_{e_m} \xi(z|y,e_m) \left(\int_\lambda w(e_m|\lambda)\mu(\lambda|x)\, d\lambda \right) \\
&= \sum_{e_m} \xi(z|y,e_m) \left(\int_\lambda \overline{\mu}(\lambda) w(e_m|\lambda) q(x,\lambda) d\lambda \right) \\
&= \sum_{e_m} \xi(z|y,e_m) \left(\int_\lambda \overline{\mu}(\lambda) w(e_m|\lambda) \left(\sum_{e_p} w(e_p|\lambda) q(x|e_p) \right) d\lambda \right) \\
&= \sum_{e_p,e_m} q(x|e_p)\xi(z|y,e_m) \left(\int_\lambda \overline{\mu}(\lambda) w(e_m|\lambda) w(e_p|\lambda) d\lambda \right). \qquad (5.6)
\end{aligned}$$

The second, fourth, and fifth lines can be deduced from their respective preceding lines through the application of Eqs. (5.5), (5.1), and (5.4), respectively. The third and sixth lines involve a rearrangement of the summation terms. At this juncture, we can introduce the variables

$$w(e_p, e_m|\lambda) := w(e_p|\lambda) w(e_m|\lambda), \qquad (5.7)$$

which form a set of convex weights since they satisfy $w(e_p, e_m|\lambda) \geqslant 0$ and $\sum_{e_p,e_m} w(e_p, e_m|\lambda) = 1$ for all λ. Additionally, by summing over λ on both sides of Eq. (5.2), it is apparent that $\int_\lambda \overline{\mu}(\lambda) = 1$. Hence, we have

$$\int \overline{\mu}(\lambda) w(e_p, e_m|\lambda) d\lambda \leqslant \max_\lambda w(e_p, e_m|\lambda) =: w^*(e_p, e_m), \qquad (5.8)$$

substituting this into Eq. (5.6), we arrive at the ensuing relation

$$p_{NC}(z|x,y) \leqslant \sum_{e_p,e_m} w^*(e_p,e_m) q(x|e_p) \xi(z|y,e_m). \tag{5.9}$$

Thus, the probabilities $p(z|x,y)$ in any non-contextual theory are necessarily bounded by and confined within the polytope whose extremal points emerge from the multiplication of e_p and e_m. In other words, the probabilities $p(z|x,y)$ lie within the polytope determined by the extremal probability distributions $\{q(x|e_p)\xi(z|y,e_m)\}$. Let's denote the probabilities associated with this bigger polytope as

$$p(z|x,y) = \sum_{e_p,e_m} w(e_p,e_m) q(x|e_p) \xi(z|y,e_m). \tag{5.10}$$

We can reconfirm, using the above relation, that $p(z|x,y)$ indeed satisfy the indistinguishability conditions (2.38) since

$$\begin{aligned} & \sum_x \alpha_{x|s} p(z|x,y) \\ = & \sum_{e_p,e_m} w(e_p,e_m) \left(\sum_x \alpha_{x|s} q(x|e_p) \right) \xi(z|y,e_m) \\ = & \sum_{e_m} w(e_m) \xi(z|y,e_m) \end{aligned} \tag{5.11}$$

remains constant for all s, in accordance with Eq. (5.3). Similarly, $p(z|x,y)$ also adheres to the indistinguishability condition (2.40). However, the expression

$$\sum_z p(z|x,y) = \sum_{e_p} w(e_p) q(x|e_p) \tag{5.12}$$

does not necessarily equate to 1, thus violating the normalization condition. Nevertheless, all observed probabilities should satisfy the normalization requirement:

$$\sum_z p(z|x,y) = 1. \tag{5.13}$$

In fact, there exists a polytope wherein the probabilities conform solely to the normalization conditions (5.13). To rectify this issue with the extended polytope, our strategy

is to identify the facet inequalities of the polytope defined by Eq. (5.10) while it is constrained by the polytope where probabilities adhere to the normalization conditions (5.13). These inequalities form NCI since the actual noncontextual polytope lies within both these polytopes. For a visual representation, refer to Fig. (5.1). Prior to presenting the succinct algorithm outlining our method to derive NCI, we first demonstrate the method by explicitly applying it to the simplest contextuality scenario.

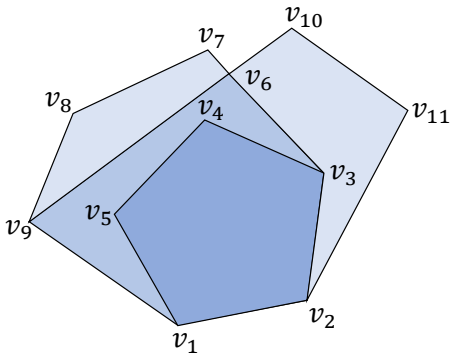


Figure 5.1: The extended polytope ($\mathbb{P}_{\mathrm{P}}$) encompassing the probabilities specified by (5.10), is defined by the collection of vertices as, $\mathbb{P}_{\mathrm{P}} = \{v_1, v_2, v_3, v_7, v_8, v_9\}$. The polytope adhering solely to the normalization condition (5.13), is defined as, $\mathbb{P}_{\mathrm{NP}} = \{v_1, v_2, v_{11}, v_{10}, v_9\}$. $\mathbb{P}_{\mathrm{NCP}} = \{v_1, v_2, v_3, v_4, v_5\}$ is the precise non-contextual polytope, which exists within the confines of the other two polytopes. The derived noncontextuality inequalities (NCI) are essentially the facet inequalities of the polytope formed by the intersection of $\mathbb{P}_{\mathrm{P}}$ and $\mathbb{P}_{\mathrm{NP}}$, which is defined by $\{v_1, v_2, v_3, v_6, v_9\}$.

5.2.4 Algorithm to obtain the set of noncontextuality inequalities

Now, we summarize our algorithm, outlining the step-by-step process for deriving NCI for any prepare and measure contextuality scenario.

- First obtain the extremal points $\{q(x|e_p)\}$ of the polytope for the variables $\{q(x)\}$ satisfying the conditions:

$$(i)\ q(x) \geqslant 0; \tag{5.14}$$

$$(ii)\ \forall s,\ \textstyle\sum_x \alpha_{x|s} q(x) = 1. \tag{5.15}$$

- Next, evaluate the extremal points $\{\xi(z|y, e_m)\}$ of the polytope of the variables

$\{\xi(z|y)\}$ satisfying the conditions:

$$(i)\ \xi(z|y) \geqslant 0; \tag{5.16}$$

$$(ii)\ \forall y,\ \textstyle\sum_z \xi(z|y) = 1; \tag{5.17}$$

$$(iii)\ \forall t, t',\ \textstyle\sum_{z,y} \beta_{z,y|t}\xi(z|y) = \sum_{z,y} \beta_{z,y|t'}\xi(z|y). \tag{5.18}$$

In the case of only indistinguishability conditions on preparations, the polytope is obtained using conditions (i) and (ii) only.

- Multiply the extremal points obtained in the previous steps to yield the extremal points of the extended polytope as $q(x|e_p) \cdot \xi(z|y, e_m)$. Subsequently, determine the facet inequalities of the extended polytope.

- Impose the normalization condition (5.13) to the derived facet inequalities. For example, $p(z = k-1|x, y)$ can be replaced by $1 - \sum_{z=0}^{k-2} p(z|x, y)$ for all x, y, so that the revised facet inequalities do not contain $p(k-1|x, y)$. Further reduce number of probabilities $\{p(z|x, y)\}$ in the facet inequalities using the indistinguishability conditions (2.38) and (2.40),

$$\forall s, s', \forall z, y,\ \sum_x \alpha_{x|s} p(z|x, y) = \sum_x \alpha_{x|s'} p(z|x, y), \tag{5.19}$$

$$\forall t, t', \forall x,\ \sum_{z,y} \beta_{z,y|t} p(z|x, y) = \sum_{z,y} \beta_{z,y|t'} p(z|x, y). \tag{5.20}$$

- Finally, identify the symmetries on the variables x, y, z, such that the extremal points $\{q(x|e_p) \cdot \xi(z|y, e_m)\}$ remain invariant, and apply these symmetries to the revised facet inequalities obtained in the previous step in order to obtain distinct in-equivalent classes of NCI.

5.2.5 An explicit example

The simplest contextuality scenario involves four preparations indexed by $x \in \{0,1,2,3\}$, such that obey the following indistinguishability condition

$$\frac{1}{2}(P_0 + P_1) \sim \frac{1}{2}(P_2 + P_3). \tag{5.21}$$

Furthermore, there are two measurements, indexed by $y \in \{0,1\}$, each yielding binary outcomes $z \in \{0,1\}$. No non-trivial indistinguishable conditions are applied to the measurements in this contextuality scenario. According to Eq. (5.3), the variables $\{q(x)\}$ describing the preparations adhere to the relations

$$q(x) \geqslant 0,\ q(0) + q(1) = q(2) + q(3) = 2, \tag{5.22}$$

while the variables $\{\xi(z|y)\}$ characterizing the measurements satisfy

$$\xi(z|y) \geqslant 0,\ \xi(0|0) + \xi(1|0) = \xi(0|1) + \xi(1|1) = 1. \tag{5.23}$$

Clearly, the set of allowed values of these variables form convex polytopes. It is easy to see that there are four extremal points of both these polytopes which are labeled as $e_p, e_m \in \{1,2,3,4\}$,

e_p	$q(0\|e_p)$	$q(1\|e_p)$	$q(2\|e_p)$	$q(3\|e_p)$
1	2	0	2	0
2	2	0	0	2
3	0	2	2	0
4	0	2	0	2

e_m	$\xi(0\|0,e_m)$	$\xi(1\|0,e_m)$	$\xi(0\|1,e_m)$	$\xi(1\|1,e_m)$
1	1	0	1	0
2	1	0	0	1
3	0	1	1	0
4	0	1	0	1

By combining these extremal points, we obtain 16 extremal distributions $\{q(x|e_p)\xi(z|y,e_m)\}$, each corresponding to a specific pair (e_p, e_m). Subsequently, we

extract the facet inequalities of the polytope defined by these 16 extremal distributions, resulting in a total of 24 facet inequalities for this case. First, by utilizing the indistinguishable condition (5.21),

$$\forall y,\ p(z|3,y) = p(z|0,y) + p(z|1,y) - p(z|2,y), \tag{5.24}$$

we can substitute the probabilities $\{p(z|3,y)\}$ in the facet inequalities to make them simpler. Secondly, the polytopes of variables $\{q(x)\}$ and $\{\xi(z|y)\}$ satisfy symmetry conditions with respect to interchanging variables. For example, if variables $x = 0$ and $x = 1$ are interchanged, then the four extremal points $\{q(x|e_p)\}$ remain unchanged, and consequently, the associated polytope retains the same form. Let us denote such symmetry by $P_0 \longleftrightarrow P_1$. Similarly, we can identify all the symmetries in this scenario

$$\begin{aligned} P_0 &\longleftrightarrow P_1 \\ P_2 &\longleftrightarrow P_3 \\ M_{0|y} &\longleftrightarrow M_{1|y} \quad \forall y = 0,1 \\ M_{z|0} &\longleftrightarrow M_{z|1} \quad \forall z = 0,1. \end{aligned} \tag{5.25}$$

When an inequality becomes identical to another after applying any of the symmetries, it indicates that these two inequalities are equivalent. After systematically applying all of the symmetries (5.25), we can identify a set of inequalities that are equivalent to each other and form an equivalence class. It is sufficient to consider any one representative inequality from that equivalent set or equivalent class of inequalities. The 'orbit size' signifies the number of inequalities within a specific equivalence class. Among the 24 inequalities initially obtained, the different in-equivalent classes of facet inequalities are enlisted below, where we have used a short-hand notation $p^z_{x,y} := p(z|x,y)$.

Some of these inequalities are violated by quantum theory. It is apparent that the normalization condition does not hold since the quantity (5.12) is not 1 for any of the extremal points of e_p given above. Therefore, we will consider the facet inequalities of the polytope intersected with the polytope where the probabilities satisfy the normalization conditions (5.13). This can be readily done by substituting $p(1|x,y)$ in the facet

orbit size	Inequalities
9	$-p^1_{2,0} \leqslant 0$
3	$p^0_{0,0} + p^0_{1,0} + p^1_{2,0} \leqslant 2$
2	$-p^0_{0,0} - p^1_{0,0} + p^1_{0,1} \leqslant 0$
1	$p^0_{0,0} + p^1_{0,0} + p^1_{1,1} \leqslant 2$
3	$p^0_{1,0} + p^1_{2,0} + p^1_{0,1} - p^1_{2,1} \leqslant 2$
3	$-p^0_{2,1} - p^1_{0,0} + p^1_{2,0} - p^1_{1,1} \leqslant 0$
1	$-p^0_{0,0} - p^0_{1,0} + p^0_{2,1} - p^1_{2,0} + p^1_{2,1} \leqslant 0$
1	$p^0_{0,0} + p^0_{1,0} - p^0_{2,1} + p^1_{0,0} + p^1_{2,0} - p^1_{0,1} \leqslant 0$
1	$-p^0_{0,0} - p^0_{1,0} + p^0_{2,1} - p^1_{0,0} - p^1_{2,0} + p^1_{0,1} \leqslant 0$

inequalities using the normalization condition

$$p(1|x,y) = 1 - p(0|x,y) \; \forall x, y. \tag{5.26}$$

Further, imposing the symmetries (5.25), we find that the number of in-equivalent classes reduces to only two,

orbit size	Inequalities
16	$p^0_{2,0} \leqslant 1$
8	$p^0_{1,0} - p^0_{2,0} - p^0_{0,1} + p^0_{2,1} \leqslant 1$

Table 5.1: We obtained 24 inequalities for the simplest contextuality scenario described in (5.21). This set of inequalities reduces to two in-equivalent classes after applying the indistinguishable conditions, symmetries, and normalization conditions.

While the first inequality is trivial, the second inequality is violated in quantum theory, achieving the maximum value $\sqrt{2} \approx 1.414$. It is interesting to note that this second inequality is identical to the success metric of the parity oblivious random access codes [183].

5.3 Computational advantage over finding facets of exact noncontextual polytope

Method to find the exact noncontextual polytope was provided by Schmid *et al.* [42]. The polytope presented in this work is notably larger than this exact noncontextual polytope. Consequently, the violation of the inequalities we derive here serves as a

sufficient criterion (though not necessary) for operational certification of generalized contextuality. However, our approach presents a two-folded and substantial advantage over the method for identifying the exact noncontextual polytope in terms of efficiency.

We recall that n_x, n_y, and n_z refer to the number of preparations, measurements, and outcomes, respectively, in a contextuality scenario. Say, the number of extremal points obtained for the variables $\{\xi(z|y)\}$ satisfying (5.16)-(5.18) is r. According to the method in [42], the total number of ontic states λ sufficient to characterize the preparations is $n_x \cdot r$. However, owing to the normalization conditions and the independent indistinguishability conditions (2.43), n_x and $r \cdot n_s$ number of variables are eliminated, respectively. As a result, the dimension of the polytope $\{\mu(\lambda|x)\}$ characterizing the preparations becomes, $D_P = (n_x - n_s)r - n_x$ [194].

In contrast, our method involves a fixed number of independent variables for characterizing the preparations $\{q(x)\}$, which is $n_x - n_s$ (see (5.14)-(5.15)) irrespective of the settings of the measurement side. Therefore, the difference between the dimensions of the two polytopes, whose extremal points are computed in the two different methods, is given by

$$\Delta_P = (n_x - n_s)r - 2n_x + n_s. \tag{5.27}$$

Furthermore, the method in [42] involves $r \cdot n_y \cdot n_z$ number of variables $\{\xi(z|y,\lambda)\}$ that describe the measurements. And, owing to the normalization conditions and the independent indistinguishability conditions (2.44), we can eliminate $r \cdot n_y$ and $r \cdot n_t$ number of variables, respectively. As a result, the dimension of the polytope characterizing the measurements becomes $r(n_y n_z - n_y - n_t)$. One needs to compute the extremal points of the product of the two polytopes involving the variables $\{\mu(\lambda|x)\}$ and $\{\xi(z|y,\lambda)\}$ by multiplying the extremal points of these two polytopes. The product polytope has a dimension of $D_T = (n_x - n_s)r - n_x + r(n_y n_z - n_y - n_t)$, which follows from the fact that the dimension of a product polytope is the sum of the dimensions of the individual polytopes [194]. On the other hand, the product polytope, for which we compute the facet inequalities in our method, possesses a dimension of $n_x - n_s + n_y n_z - n_y - n_t$. Hence, the difference in dimensions between these two product polytopes, whose extremal points are computed through these two methods

is given by

$$\Delta_T = (r-1)(n_x + n_y n_z - n_s - n_y - n_t) - n_x. \tag{5.28}$$

As an example, when there are no indistinguishability conditions for measurements, we know that $r = n_z^{n_y}$ and $n_t = 0$. Consequently, Δ_P scales in the order of $n_z^{n_y}$, and Δ_T scales in the order of $n_y n_z^{n_y}$, leading to an exponential increment with the number of measurements.

5.4 Noncontextuality inequalities (NCIs) for various scenarios and their quantum violations

In this section, we explore various elementary contextuality scenarios in detail. First, we retrieve all the NCI using the aforementioned method. Subsequently, we conduct a comprehensive study of their quantum violations and establish upper bounds on the maximum quantum violations. Before presenting the results, we introduce a *Fact* that greatly aids in obtaining quantum violation for any preparation NCI with binary outcomes.

Fact 1. *Consider any linear figure of merit in any contextuality scenario where there are no nontrivial indistinguishability conditions on measurements, and the outcomes are binary, that is, $z \in \{0,1\}$. Since the outcomes are binary, we can replace $p(1|x,y)$ by $1 - p(0|x,y)$ and express any linear expression as $\sum_{x,y} c_{x,y} p(0|x,y)$ where $c_{x,y}$ are some real numbers. Given any quantum preparation strategy $\{\rho_x\}$ satisfying the indistinguishability conditions, the best possible quantum measurement strategy $\{\mathbb{M}_{z|y}\}$ is fully determined by the preparation strategy as*

$$\mathbb{M}_{0|y} = \sum_{a>0} \mathbb{P}_a, \tag{5.29}$$

where $\mathbb{P}_a$ is the eigenprojector of the operator $\left(\sum_x c_{x,y}\rho_x\right)$ corresponds to positive eigenvalue a, that is, $\left(\sum_x c_{x,y}\rho_x\right)\mathbb{P}_a = a\mathbb{P}_a$.

Proof. By splitting the sum and replacing the probabilities with quantum states and

measurements, we find that

$$\begin{aligned}\sum_{x,y} c_{x,y} p(0|x,y) &= \sum_{y} \left(\sum_{x} c_{x,y} p(0|x,y) \right) \\ &= \sum_{y} \mathrm{Tr} \left[\left(\sum_{x} c_{x,y} \rho_x \right) \mathbb{M}_{0|y} \right]. \end{aligned} \tag{5.30}$$

Given $\{\rho_x\}$, the quantity $\sum_x c_{x,y}\rho_x$ is fixed and Hermitian, having only real eigenvalues. Thus, for every y, the best possible quantum measurement strategy is to take $\mathbb{M}_{0|y}$ sum of eigenprojectors corresponding to the positive eigenvalues of $\sum_x c_{x,y}\rho_x$. Finally, we have $\mathbb{M}_{1|y} = \mathbb{1} - \mathbb{M}_{0|y}$. □

To identify quantum violations, two semi-definite programming-based methods [166] are employed. The first method entails alternating sequences of semi-definite programs and is commonly referred to as the see-saw method. It provides a lower bound on the quantum violation of the NCI, along with the corresponding quantum states and measurements that lead to such violation. This optimization involves the following steps. Initially, random quantum states of fixed dimension are generated, adhering to the indistinguishability conditions on preparations. Quantum measurements are then optimized to maximize the relevant linear function of probabilities (the left-hand-side of the relevant NCI) while satisfying the indistinguishability conditions on measurements. In general, this set forms a semi-definite program, except in cases where there are no indistinguishability conditions on measurements and outcomes are binary, and *Fact* 1 is used to determine the optimal quantum measurements for the generated quantum states. In the subsequent step, the optimized measurements from the previous step are fixed, and the best quantum states are found that optimize the relevant expression while satisfying indistinguishability conditions on preparations. Yet again, this step forms a semi-definite program. This two-fold optimization process is iterated until the value of the relevant expression saturates. Moreover, this entire optimization is performed for different choices of initial random quantum states, and the best value along with the associated quantum strategy among these is retained. The value obtained through this see-saw method is denoted as $\mathcal{Q}_s^d$ for the chosen dimension (d) of the quantum states and measurements. While the value $\mathcal{Q}_s^d$ may not

be the optimal quantum value, the method is useful as it delivers the corresponding quantum states and measurements that achieve this value.

Additionally, the robustness of the quantum violations is studied as a means of comparing violations of different NCI inequalities. Here, we consider the robustness with respect to the presence of white noise, which is the maximum amount of white noise that can be added while the quantum violation persists. Specifically, given the quantum states $\{\rho_x\}_x$ and quantum measurements $\{\mathbb{M}_{z|y}\}_{z,y}$ acting on $\mathbb{C}^d$ achieving $\mathcal{Q}_s^d$ found from the see-saw method, we take the noisy states $\omega(\mathbb{1}/d) + (1-\omega)\rho_x$, where $\omega \in [0,1]$ being the noise parameter. As the measure of robustness, the minimum value of ω, denoted by ω_c^d, is then determined so that the left-hand side of NCI coincides with the noncontextual bound $\mathcal{C}$. It can be readily verified that, for a general inequality (2.45),

$$\omega_c^d = \frac{\mathcal{Q}_s^d - \mathcal{C}}{\mathcal{Q}_s^d - \gamma}, \tag{5.31}$$

where $\gamma = (1/d)\sum_{x,y,z} c_{x,y,z} \operatorname{Tr}(\mathbb{M}_{z|y})$ is the value of left-hand-side of (2.45) for the maximally mixed state. The larger value of ω_c^d the more robust is the quantum violation arising from $\{\rho_x\}_x$ and $\{\mathbb{M}_{z|y}\}_{z,y}$.

The second method involves implementing the semi-definite hierarchy introduced in [170] up to the first level, which yields a dimension independent upper bound on the maximum quantum violation of NCI. We denote this upper bound by $\mathcal{Q}_1$. Therefore, if $\mathcal{Q}_1$ matches with $\mathcal{Q}_s^d$, it indicates the exact maximum violation (up to machine precision).

The simplest scenario of four preparations satisfying indistinguishability conditions (5.21) has been discussed rigorously in Sec. (5.2). Eight other scenarios with their quantum violations are discussed in the following subsections. The respective polytopes and symmetries have been found using `'polymake'`, and the bounds on the quantum violations based on the aforementioned semi-definite programming methods are found using `'Matlab'` and `'sdpt3'`. The codes are available in [195]. We enlist the NCI except the *trivial* NCI that are of the form $p(z|x,y) \leqslant 1$ or $p(z|x,y) \geqslant 0$. Apart from the last scenario, all other scenarios involve only binary outcomes. For the sake of convenience thereof, we express the NCI only in terms of outcome $z = 0$ and further

use the following short-hand notation to denote the probabilities

$$p_{x,y} := p(0|x,y). \tag{5.32}$$

Scenario 2

The contextuality scenario is defined as follows:

$$x \in \{0,1,2,3\},\ y \in \{0,1,2\},\ z \in \{0,1\}, \quad \frac{1}{3}\left(P_0 + P_1 + P_2\right) \sim \frac{1}{2}\left(P_0 + P_3\right). \tag{5.33}$$

orbit size	Inequalities	$\mathcal{Q}_s^2$	ω_c^2	$\mathcal{Q}_1$
24	$\mathcal{I}_2 = -p_{0,0} + 2p_{1,0} + p_{0,1} - 2p_{2,1} \leqslant 2$	2.6458	0.244	2.7321
5	$p_{0,2} - 2p_{1,2} - 2p_{2,2} \leqslant 0$	0	0	0

Table 5.2: We obtain 48 inequalities in the contextuality scenario (5.33). Out of these inequalities, 19 are trivial. The rest of them are reduced to 2 inequivalent classes after applying the indistinguishable conditions and symmetries mentioned below.

$$\forall y,z,\ p(z|x=3,y) = \frac{2}{3}p(z|x=1,y) + \frac{2}{3}p(z|x=2,y) - \frac{1}{3}p(z|x=0,y); \tag{5.34}$$

$$P_1 \longleftrightarrow P_2;\ M_{0|y} \longleftrightarrow M_{1|y}\ \forall y;\ \ M_{z|0} \longleftrightarrow M_{z|1};\ \ M_{z|1} \longleftrightarrow M_{z|2};\ M_{z|0} \longleftrightarrow M_{z|2} \forall z. \tag{5.35}$$

The set of inequivalent nontrivial NCI is enlisted in Table (5.2), and the quantum strategy that achieves the highest quantum violation of $\mathcal{I}_2$ is illustrated in Fig. (5.2). An interesting aspect of this contextuality scenario deserves attention. We define an ontic distribution as deterministic when $\mu(\lambda|x) \in \{0,1\}$; otherwise, it's probabilistic. Notably, the noncontextual bound 2 of the NCI $\mathcal{I}_2$ (in Tab.5.2) can only be attained through a probabilistic ontic distribution in any ontological model. For instance, consider the following model where $\lambda_1, \lambda_2 \in \Lambda$:

x	0	1	2	3
$\mu(\lambda_1\|x)$	0	1	0	$\frac{2}{3}$
$\mu(\lambda_2\|x)$	1	0	1	$\frac{1}{3}$

$p_d(0\|0,\lambda_1)$	1
$p_d(0\|0,\lambda_2)$	0
$p_d(0\|1,\lambda_2)$	0

This model satisfies

$$\frac{1}{3}(\mu(\lambda|0)+\mu(\lambda|1)+\mu(\lambda|2))=\frac{1}{2}(\mu(\lambda|0)+\mu(\lambda|3)). \tag{5.36}$$

while simultaneously yielding $\mathcal{I}_2 = 2$. On the other hand, to determine the maximum value of $\mathcal{I}_2$ for deterministic epistemic states, it is sufficient to examine all feasible deterministic epistemic states considering at most four distinct ontic states. The optimization reveals that the value is 1.

Scenario 3

The contextuality scenario consists of five preparations and two binary outcome measurements and is defined as follows:

$$x \in \{0,1,2,3,4\},\ y \in \{0,1\},\ z \in \{0,1\}, \quad \frac{1}{2}\left(P_0+P_1\right) \sim \frac{1}{3}\left(P_2+P_3+P_4\right). \tag{5.37}$$

The set of inequivalent NCI for the contextuality scenario is given in Table (5.3), and the strategy that attains maximum quantum violation of $\mathcal{I}_3$ is illustrated in Fig. (5.2).

orbit size	Inequalities	Q_s^2	ω_c^2	Q_1
2	$-3p_{0,0}-3p_{1,0}+2p_{2,0}+2p_{3,0}\leqslant 0$	0	0	0
24	$\mathcal{I}_3 = -3p_{0,0}+2p_{2,0}-3p_{1,1}+2p_{2,1}\leqslant 2$	3.1231	0.272	3.1815

Table 5.3: We obtain 44 inequalities in this scenario, among which 18 are trivial. The rest of the inequalities are reduced to 2 inequivalent classes after employing the following indistinguishability conditions and symmetries.

$$p(z|x=4,y) = \frac{3}{2}\left(p(z|x=0,y)+p(z|x=1,y)\right)-p(z|x=2,y)-p(z|x=3,y)\ \forall y,z \tag{5.38}$$

$$P_0 \longleftrightarrow P_1; P_2 \longleftrightarrow P_3; P_2 \longleftrightarrow P_4; P_3 \longleftrightarrow P_4 \tag{5.39}$$

$$M_{0|y} \longleftrightarrow M_{1|y}\ \forall y; M_{z|0} \longleftrightarrow M_{z|1}\ \forall z \tag{5.40}$$

$$M_{0|0} \longrightarrow M_{0|1}\ ,\ M_{0|1} \longrightarrow M_{1|0}\ ,\ M_{1|0} \longrightarrow M_{1|1}\ ,\ M_{1|1} \longrightarrow M_{0|0}. \tag{5.41}$$

The symmetry operation $M_{z|y} \longrightarrow M_{z'|y'}$ corresponds to the relabeling of the variables z, y to z', y' that together $\forall y, z$ describes a symmetry of this scenario. In what follows, symmetry operations separated by $\{,\}$ are meant to be applied together.

Scenario 4

Table (5.4) contains the inequivalent NCI for the contextuality scenario defined as follows:

$$x \in \{0,1,2,3,4\}, y \in \{0,1\}, z \in \{0,1\} \quad \frac{1}{4}\left(P_0 + P_1 + P_2 + P_3\right) \sim \frac{1}{3}\left(P_0 + P_1 + P_4\right). \tag{5.42}$$

orbit size	Inequalities	Q_s^2	ω_c^2	Q_1
4	$p_{0,0} + p_{1,0} - 3p_{2,0} - 3p_{3,0} \leqslant 0$	0	0	0
8	$p_{0,0} + p_{1,0} - 3p_{2,0} + p_{0,1} + p_{1,1} - 3p_{3,1} \leqslant 2$	3.1231	0.272	3.1815
16	$p_{1,0} - 3p_{2,0} + p_{1,1} - 3p_{3,1} \leqslant 1$	1.7417	0.198	1.9168

Table 5.4: We obtain 44 inequalities including 16 trivial ones. The 28 nontrivial NCI are reduced to 3 inequivalent classes after applying the following indistinguishability conditions and symmetries.

$$p(z|x=4,y) = \frac{3}{4}(p(z|x=2,y) + p(z|x=3,y)) - \frac{1}{4}(p(z|x=0,y) + p(z|x=1,y)) \;\forall y,z \tag{5.43}$$

$$P_0 \longleftrightarrow P_1; P_2 \longleftrightarrow P_3; \tag{5.44}$$

$$M_{0|y} \longleftrightarrow M_{1|y} \;\forall y; \;\; M_{z|0} \longleftrightarrow M_{z|1} \;\forall z \tag{5.45}$$

$$M_{0|0} \longrightarrow M_{0|1}\,,\; M_{0|1} \longrightarrow M_{1|0}\,,\; M_{1|0} \longrightarrow M_{1|1}\,,\; M_{1|1} \longrightarrow M_{0|0}. \tag{5.46}$$

Scenario 5

The contextuality scenario consisting of six preparations and three binary outcome measurements is defined as follows:

$$x \in \{0,1,2,3,4,5\}, y \in \{0,1,2\}, z \in \{0,1\}, \quad \frac{1}{2}\left(P_0 + P_1\right) \sim \frac{1}{2}\left(P_2 + P_3\right) \sim \frac{1}{2}\left(P_4 + P_5\right). \tag{5.47}$$

The set of inequivalent NCI is given in Table (5.5), and the qubit strategy that achieves the maximum quantum violation of $\mathcal{I}_5$ is provided in Fig. (5.2).

orbit size	Inequalities	Q_s^2	ω_c^2	Q_1
24	$p_{0,0} + p_{1,0} - p_{4,0} \leqslant 1$	1	0	1
24	$p_{0,0} - p_{2,0} - p_{1,2} + p_{2,2} \leqslant 1$	1.4142	0.293	1.4142
24	$p_{1,0} - p_{4,0} + p_{0,2} - p_{4,2} \leqslant 1$	1.4142	0.293	1.4142
24	$p_{2,1} - p_{4,1} - p_{0,2} - p_{1,2} + p_{2,2} + p_{4,2} \leqslant 1$	1.4142	0.293	1.4142
192	$\mathcal{I}_5 = p_{2,0} - p_{4,0} + p_{1,1} - p_{2,1} - p_{4,1} - p_{0,2} + p_{2,2} + p_{4,2} \leqslant 2$	2.5	0.2	2.6571
192	$-p_{0,0} + p_{2,0} + p_{4,0} + p_{1,1} - p_{2,1} - p_{1,2} - p_{2,2} + p_{4,2} \leqslant 2$	2.5	0.2	2.6571
192	$p_{1,0} - p_{4,0} + p_{0,1} + p_{2,1} - p_{4,1} - 2p_{0,2} - p_{1,2} + p_{2,2} + p_{4,2} \leqslant 2$	2.5	0.2	2.6571

Table 5.5: Here we obtain 684 inequalities. Among these, 12 are trivial. The remaining inequalities are reduced to 8 inequivalent classes after applying the following indistinguishability conditions and symmetry transformations.

$$p(z|x=3,y) = p(z|x=0,y) + p(z|x=1,y) - p(z|x=2,y)\ \forall y,z \tag{5.48}$$

$$p(z|x=5,y) = p(z|x=0,y) + p(z|x=1,y) - p(z|x=4,y)\ \forall y,z \tag{5.49}$$

$$P_0 \longleftrightarrow P_1; P_2 \longleftrightarrow P_3; P_4 \longleftrightarrow P_5 \tag{5.50}$$

$$M_{0|y} \longleftrightarrow M_{1|y}\ \forall y;\ M_{z|0} \longleftrightarrow M_{z|1};\ M_{z|1} \longleftrightarrow M_{z|2};\ M_{z|0} \longleftrightarrow M_{z|2}\ \forall z. \tag{5.51}$$

Scenario 6

The contextuality scenario consisting of seven preparations and three measurements is defined as follows:

$$x \in \{0,1,2,3,4,5,6\}, y \in \{0,1,2\}, z \in \{0,1\}, \quad \frac{1}{4}\left(P_0 + P_1 + P_2 + P_3\right) \sim \frac{1}{3}\left(P_4 + P_5 + P_6\right). \tag{5.52}$$

Table (5.6) presents the collection of inequivalent NCI obtained in this scenario. In contrast to previous scenarios, qubit strategy in this context did not yield the optimal results (using the see-saw method). In particular, there is a substantial enhancement in Q_s when considering states and measurements of higher dimensions. We have documented these values up to $d = 4$. Notably, for $\mathcal{I}_6^2$ and $\mathcal{I}_6^4$, we obtain $Q_s^7 = 14.9711$ and $Q_s^7 = 15.6163$, respectively, which are more than Q_s^4 given in table (5.6). In Fig. (5.2), we provide the details of the qubit strategy which violates $\mathcal{I}_6^3$. Here, we present the 3-dimensional quantum states and measurements that yield a quantum violation of $\mathcal{I}_6^1 = 8.7764 > 6$:

$$\rho_0 = \begin{pmatrix} 0.7865 & -0.1091 & 0.3950 \\ -0.1091 & 0.0151 & -0.0548 \\ 0.3950 & -0.0548 & 0.1983 \end{pmatrix}, \rho_1 = \begin{pmatrix} 0.0004 & 0.0186 & 0.0077 \\ 0.0186 & 0.8526 & 0.3540 \\ 0.0077 & 0.3540 & 0.1470 \end{pmatrix}, \rho_2 = \begin{pmatrix} 0.0004 & 0.0186 & 0.0077 \\ 0.0186 & 0.8526 & 0.3540 \\ 0.0077 & 0.3540 & 0.1470 \end{pmatrix},$$

$$\rho_3 = \begin{pmatrix} 0.3904 & 0.2225 & -0.4341 \\ 0.2225 & 0.1268 & -0.2474 \\ -0.4341 & -0.2474 & 0.4828 \end{pmatrix} \rho_4 = \begin{pmatrix} 0.1713 & 0.2578 & 0.1378 \\ 0.2578 & 0.5426 & 0.0428 \\ 0.1378 & 0.0428 & 0.2860 \end{pmatrix}, \rho_5 = \begin{pmatrix} 0.5406 & -0.4028 & -0.2935 \\ -0.4028 & 0.3000 & 0.2187 \\ -0.2935 & 0.2187 & 0.1593 \end{pmatrix},$$
$$\rho_6 = \begin{pmatrix} 0.1713 & 0.2579 & 0.1378 \\ 0.2579 & 0.5427 & 0.0429 \\ 0.1378 & 0.0429 & 0.2860 \end{pmatrix}, \mathbb{M}_{0|0} = \begin{pmatrix} 0.8633 & -0.3370 & 0.0668 \\ -0.3370 & 0.1315 & -0.0261 \\ 0.0668 & -0.0261 & 0.0052 \end{pmatrix},$$
$$\mathbb{M}_{0|1} = \begin{pmatrix} 0.5859 & -0.0485 & -0.4902 \\ -0.0485 & 0.0040 & 0.0406 \\ -0.4902 & 0.0406 & 0.4101 \end{pmatrix}, \mathbb{M}_{0|2} = \begin{pmatrix} 0.7889 & 0.3566 & 0.1984 \\ 0.3566 & 0.3976 & -0.3351 \\ 0.1984 & -0.3351 & 0.8136 \end{pmatrix}. \tag{5.53}$$

Moreover, the following set of $4-$dimensional quantum states and measurements achieve the quantum violation $\mathcal{Q}_s = 15.5037 > 12$ of $\mathcal{I}_6^4$ in Tab. (5.6),

$$\rho_0 = \begin{pmatrix} 0.1537 & -0.1618 & -0.1204 & -0.2990 \\ -0.1618 & 0.1704 & 0.1268 & 0.3148 \\ -0.1204 & 0.1268 & 0.0943 & 0.2342 \\ -0.2990 & 0.3148 & 0.2342 & 0.5816 \end{pmatrix}, \rho_1 = \begin{pmatrix} 0.3830 & -0.3343 & 0.0919 & 0.3408 \\ -0.3343 & 0.2917 & -0.0802 & -0.2974 \\ 0.0919 & -0.0802 & 0.0220 & 0.0818 \\ 0.3408 & -0.2974 & 0.0818 & 0.3032 \end{pmatrix},$$
$$\rho_2 = \begin{pmatrix} 0.1411 & 0.2127 & -0.1319 & 0.0790 \\ 0.2127 & 0.4379 & -0.0719 & 0.0026 \\ -0.1319 & -0.0719 & 0.2609 & -0.2001 \\ 0.0790 & 0.0026 & -0.2001 & 0.1601 \end{pmatrix} \rho_3 = \begin{pmatrix} 0.1411 & 0.2127 & -0.1319 & 0.0790 \\ 0.2127 & 0.4379 & -0.0718 & 0.0026 \\ -0.1319 & -0.0718 & 0.2609 & -0.2001 \\ 0.0790 & 0.0026 & -0.2001 & 0.1601 \end{pmatrix},$$
$$\rho_4 = \begin{pmatrix} 0.1570 & -0.2543 & -0.0758 & 0.2489 \\ -0.2543 & 0.4119 & 0.1227 & -0.4031 \\ -0.0758 & 0.1227 & 0.0366 & -0.1201 \\ 0.2489 & -0.4031 & -0.1201 & 0.3945 \end{pmatrix}, \rho_5 = \begin{pmatrix} 0.0102 & 0.0748 & -0.0141 & 0.0657 \\ 0.0748 & 0.5477 & -0.1035 & 0.4811 \\ -0.0141 & -0.1035 & 0.0196 & -0.0909 \\ 0.0657 & 0.4811 & -0.0909 & 0.4225 \end{pmatrix},$$
$$\rho_6 = \begin{pmatrix} 0.4470 & 0.1266 & -0.1294 & -0.1646 \\ 0.1266 & 0.0438 & -0.0921 & -0.0610 \\ -0.1294 & -0.0921 & 0.4225 & 0.1478 \\ -0.1646 & -0.0610 & 0.1478 & 0.0867 \end{pmatrix}, \mathbb{M}_{0|0} = \begin{pmatrix} 0.0406 & -0.1190 & -0.0263 & -0.1552 \\ -0.1190 & 0.3488 & 0.0772 & 0.4550 \\ -0.0263 & 0.0772 & 0.0171 & 0.1007 \\ -0.1552 & 0.4550 & 0.1007 & 0.5935 \end{pmatrix},$$
$$\mathbb{M}_{0|1} = \begin{pmatrix} 0.1083 & 0.1665 & -0.1530 & 0.2133 \\ 0.1665 & 0.9667 & 0.0656 & -0.0115 \\ -0.1530 & 0.0656 & 0.3433 & -0.4447 \\ 0.2133 & -0.0115 & -0.4447 & 0.5816 \end{pmatrix}, \mathbb{M}_{0|2} = \begin{pmatrix} 0.3099 & -0.3260 & 0.0207 & 0.3274 \\ -0.3260 & 0.3429 & -0.0217 & -0.3444 \\ 0.0207 & -0.0217 & 0.0014 & 0.0218 \\ 0.3274 & -0.3444 & 0.0218 & 0.3459 \end{pmatrix}. \tag{5.54}$$

$$p(z|x=6,y) = \frac{3}{4}\left(p(z|x=0,y) + p(z|x=1,y) + p(z|x=2,y) + p(z|x=3,y)\right)$$
$$- p(z|x=4,y) - p(z|x=5,y)\ \forall y,z \tag{5.55}$$

$$P_0 \longleftrightarrow P_1; P_0 \longleftrightarrow P_2; P_0 \longleftrightarrow P_3; P_1 \longleftrightarrow P_2; P_1 \longleftrightarrow P_3; P_2 \longleftrightarrow P_3; P_4 \longleftrightarrow P_5;$$
$$P_4 \longleftrightarrow P_6; P_5 \longleftrightarrow P_6 \tag{5.56}$$

$$M_{0|y} \longleftrightarrow M_{1|y}\ \forall y; \quad M_{z|0} \longleftrightarrow M_{z|1};\ M_{z|1} \longleftrightarrow M_{z|2};\ M_{z|0} \longleftrightarrow M_{z|2}\ \forall z. \tag{5.57}$$

orbit size	Inequalities	Q_s^2	ω_c^2	Q_s^3	ω_c^3	Q_s^4	ω_c^4	Q_1	Q_{UB}^2
4	$3p_{0,0}+3p_{1,0}+3p_{2,0}+3p_{3,0}-4p_{4,0}-4p_{5,0}\leqslant 4$	4	0	4	0	4	0	4	4
864	$\mathcal{I}_6^1=-3p_{1,0}-3p_{2,0}-3p_{3,0}+4p_{5,0}-3p_{0,1}-3p_{1,1}$ $-3p_{2,1}+4p_{5,1}+3p_{0,2}+3p_{3,2}-4p_{5,2}\leqslant 6$	7.6833	0.144	8.7764	0.257	8.7764	0.270	9.2621	7.6833
864	$\mathcal{I}_6^2=-6p_{0,0}-3p_{2,0}-3p_{3,0}+4p_{4,0}+8p_{5,0}$ $-3p_{0,1}-3p_{1,1}+4p_{4,1}-6p_{1,2}-3p_{2,2}$ $-3p_{3,2}+4p_{4,2}+8p_{5,2}\leqslant 12$	12	0	14.4414	0.161	14.6929	0.171	16.9615	12
864	$-3p_{3,0}+4p_{4,0}-3p_{0,1}-3p_{2,1}$ $+4p_{4,1}+3p_{1,2}-4p_{4,2}\leqslant 7$	8.9692	0.197	8.9692	0.197	9.472	0.236	10.5888	8.9692
288	$-3p_{1,0}+4p_{5,0}+3p_{0,2}+3p_{2,2}+3p_{3,2}-4p_{5,2}\leqslant 9$	10.8281	0.233	10.8281	0.267	10.8281	0.277	11.1229	10.8281
216	$\mathcal{I}_6^3=-3p_{1,0}-3p_{3,0}+4p_{5,0}+3p_{0,2}$ $+3p_{2,2}-4p_{5,2}\leqslant 6$	8.2462	0.272	8.2462	0.296	8.2462	0.310	8.3631	8.2462
288	$-3p_{0,0}-3p_{3,0}+4p_{4,0}+4p_{5,0}-3p_{1,1}-3p_{2,1}$ $+4p_{5,1}-3p_{1,2}-3p_{2,2}+4p_{4,2}\leqslant 8$	9.8167	0.167	11	0.272	11	0.272	11.7279	9.8167
192	$3p_{1,0}-4p_{5,0}-3p_{0,1}-3p_{2,1}-3p_{3,1}+4p_{4,1}$ $+4p_{5,1}-3p_{1,2}+4p_{4,2}\leqslant 7$	8.6241	0.178	8.6241	0.188	9.1366	0.221	10	8.6241
192	$3p_{1,0}+3p_{2,0}+3p_{3,0}-4p_{4,0}-3p_{1,1}-3p_{2,1}$ $-3p_{3,1}+4p_{5,1}-3p_{0,2}+4p_{4,2}+4p_{5,2}\leqslant 13$	14.2154	0.103	15.658	0.249	15.658	0.249	15.8923	14.2154
1728	$\mathcal{I}_6^4=-3p_{1,0}-6p_{2,0}-6p_{3,0}+4p_{4,0}+8p_{5,0}$ $-6p_{0,1}-3p_{1,1}+4p_{4,1}+8p_{5,1}-3p_{0,2}$ $-3p_{2,2}-3p_{3,2}+4p_{4,2}\leqslant 12$	12.3578	0.024	15.1551	0.199	15.5037	0.218	17.2706	12.3578

Table 5.6: In this case, we obtain 5538 inequalities, among which 38 are trivial. The rest of the 5500 inequalities reduce to 10 inequivalent class as mentioned above. To obtain the inequivalent NCI, we apply the following indistinguishability conditions and symmetry transformations.

Scenario 7

This contextuality scenario involves eight preparations and three measurements, that is, $x \in \{0,1,2,3,4,5,6,7\}, y \in \{0,1,2\}, z \in \{0,1\}$, satisfying the following indistinguishability conditions:

$$\begin{aligned} &\frac{1}{4}(P_0+P_1+P_6+P_7) \sim \frac{1}{4}(P_2+P_3+P_4+P_5) \sim \frac{1}{4}(P_0+P_2+P_5+P_7) \\ \sim &\frac{1}{4}(P_1+P_3+P_4+P_6) \sim \frac{1}{4}(P_0+P_3+P_4+P_7) \sim \frac{1}{4}(P_1+P_2+P_5+P_6) \\ &\sim \frac{1}{4}(P_0+P_3+P_5+P_6) \sim \frac{1}{4}(P_1+P_2+P_4+P_7)\,. \end{aligned} \tag{5.58}$$

It is worth noting that the indistinguishability conditions in this scenario are not entirely independent. Interestingly, this scenario resembles the 3-bit parity oblivious multiplexing task, which has been previously explored in [183]. In this communication task, the sender possesses a 3-bit string $x = x_0x_1x_2$ selected uniformly, and the receiver's goal is to guess the yth bit of x while adhering to the constraint that all potential parities of the input bits must remain oblivious in the communication.

We find four inequivalent NCI in this scenario, as detailed in Table 5.7. To achieve quantum violations of $\mathcal{I}_7$, a specific strategy can be employed wherein ρ_x corresponds to qubit states representing the vertices of the cube on the Bloch sphere shown in Table (5.7), and the receiver's measurements are $\sigma_y, \sigma_x, \sigma_z$ for $y = 0, 1, 2$, respectively.

Orbit Size	Inequalities	Q_s^2	ω_c^2	Q_1
48	$-2p_{0,0}+p_{1,0}+p_{2,0}+p_{4,0} \leqslant 1$	1	0	1
144	$-p_{0,0}+p_{2,0}-p_{0,2}+p_{1,2} \leqslant 1$	1.4142	0.293	1.4142
144	$2p_{0,0}-p_{2,0}-2p_{4,0}-p_{0,1}+p_{1,1} \leqslant 1$	1.3371	0.183	1.3638
48	$\mathcal{I}_7 = p_{0,0}-p_{1,0}+p_{0,1}-p_{4,1}+p_{0,2}-p_{2,2} \leqslant 1$	1.7321	0.423	1.7321

Table 5.7: We obtained 384 nontrivial inequalities that are grouped into 4 inequivalent classes. It turns out that by rearranging the indistinguishability conditions, we can express the probabilities for four input variables using the other four input variables in the following manner.

The reduction of probabilities is given by:

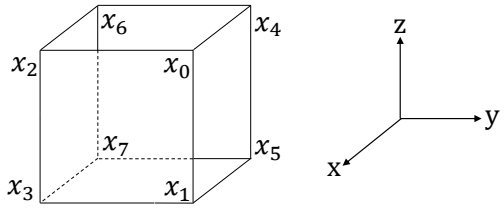
$$p(z|x=3,y) = p(z|x=1,y) + p(z|x=2,y) - p(z|x=0,y)\ \forall y,z \tag{5.59}$$

$$p(z|x=5,y) = p(z|x=1,y) + p(z|x=4,y) - p(z|x=0,y)\ \forall y,z \tag{5.60}$$

$$p(z|x=6,y) = p(z|x=2,y) + p(z|x=4,y) - p(z|x=0,y)\ \forall y,z \tag{5.61}$$

$$p(z|x=7,y) = p(z|x=1,y) + p(z|x=2,y) + p(z|x=4,y) - 2p(z|x=0,y)\ \forall y,z. \tag{5.62}$$

Interestingly, the symmetries possessed by the preparations $\{P_x\}$ exhibit a fascinating connection to the symmetries of a cube. A cube contains 23 symmetry elements that include centre of symmetry, plane of symmetry and axis of symmetry. The symmetry operations on the preparations along with the corresponding cube symmetries that we apply to find the equivalent NCI are described below.



$$P_0 \longleftrightarrow P_1, P_6 \longleftrightarrow P_7, P_2 \longleftrightarrow P_3, P_4 \longleftrightarrow P_5; \text{(reflection with respect to x-y plane)} \tag{5.63}$$

$$P_0 \longleftrightarrow P_4, P_3 \longleftrightarrow P_7, P_2 \longleftrightarrow P_6, P_1 \longleftrightarrow P_5; \text{(reflection with respect to y-z plane)} \tag{5.64}$$

$$P_0 \longleftrightarrow P_7, P_3 \longleftrightarrow P_4, P_2 \longleftrightarrow P_6, P_1 \longleftrightarrow P_5; (\pi \text{ rotation about an axis dissecting the edges containing } x_2x_6 \text{ and } x_1x_5) \tag{5.65}$$

$$P_0 \longleftrightarrow P_4, P_3 \longleftrightarrow P_7, P_2 \longleftrightarrow P_5, P_1 \longleftrightarrow P_6; (\pi \text{ rotation about an axis dissecting the edges containing } x_3x_7 \text{ and } x_0x_4) \tag{5.66}$$

$$P_0 \longleftrightarrow P_7, P_3 \longleftrightarrow P_4, P_2 \longleftrightarrow P_5, P_1 \longleftrightarrow P_6; \text{(inversion between opposite points about centre of symmetry)} \tag{5.67}$$

$$P_0 \longleftrightarrow P_6, P_1 \longleftrightarrow P_7; \text{(reflection with respect to the diagonal plane containing } x_2, x_3, x_5, x_4) \tag{5.68}$$

Note that there are more symmetries, but the ones listed above are enough to group all the NCI into the inequivalent classes. The symmetry transformations implemented on the measurements are given by (5.51).

Scenario 8

Until this point, we have considered contextuality scenarios involving indistinguishability conditions on preparations. However, in this particular scenario, we examine eight preparations, with $x \in \{0,1,2,3,4,5,6,7\}$ adhering to the same conditions as specified in (5.58), and three binary outcome measurements, $y \in \{0,1,2\}, z \in \{0,1\}$, which satisfy the indistinguishability condition,

$$\frac{1}{3}\{M_{0|0} + M_{0|1} + M_{0|2}\} \sim \frac{1}{3}\{M_{1|0} + M_{1|1} + M_{1|2}\}. \tag{5.69}$$

The resulting inequivalent NCI can be found in Table (5.8). An important observation here is that, for all the NCI, $Q_s^2 = Q_1$ up to machine precision, indicating we have found the exact maximum quantum violations. Moreover, $Q_1^{\Pi} = Q_1$, implying that projective measurements are sufficient to obtain the maximum quantum violations of all the NCI. A set of qubit states and measurements yielding the maximal violation of $\mathcal{I}_8$ is provided in Fig. (5.2).

Orbit Size	Inequalities	Q_s^2	ω_c^2	Q_1
48	$-4p_{0,0} + 2p_{1,0} + 2p_{2,0} + 2p_{4,0} - 4p_{0,1} + 2p_{1,1} + 2p_{2,1} + 2p_{4,1} \leqslant 3$	3	0	3
288	$-2p_{0,0} + 2p_{1,0} + 2p_{2,0} - p_{0,1} + 2p_{1,1} \leqslant 3$	3.3660	0.196	3.3660
288	$5p_{0,0} - 3p_{1,0} - 2p_{2,0} - 2p_{4,0} + 2p_{0,1} - 2p_{4,1} \leqslant 1$	1.6458	0.244	1.6458
288	$p_{1,0} - p_{2,0} + p_{4,0} + 2p_{0,1} \leqslant 3$	3.3660	0.196	3.3660
144	$-p_{0,0} + p_{2,0} - p_{0,1} + p_{4,1} \leqslant 1$	1.3660	0.268	1.3660
144	$-4p_{0,0} + p_{1,0} + p_{4,0} - 2p_{0,1} + 2p_{2,1} \leqslant 1$	1.6458	0.244	1.6458
144	$p_{0,0} - 3p_{2,0} - 4p_{0,1} + 2p_{1,1} + 2p_{4,1} \leqslant 1$	1.6458	0.244	1.6458
144	$-3p_{0,0} + p_{1,0} + p_{2,0} + p_{4,0} - 2p_{0,1} + p_{1,1} + p_{4,1} \leqslant 1$	1.3660	0.268	1.3660
48	$\mathcal{I}_8 = -p_{1,0} + p_{4,0} - 2p_{0,1} + p_{2,1} + p_{4,1} \leqslant 1$	1.5	0.333	1.5
576	$p_{0,0} - 2p_{1,0} + p_{2,0} - 4p_{0,1} + 3p_{2,1} + 3p_{4,1} \leqslant 3$	3.6889	0.256	3.6889
576	$4p_{0,0} - 4p_{1,0} - 2p_{4,0} - 5p_{0,1} + 4p_{2,1} + 3p_{4,1} \leqslant 3$	3.9210	0.235	3.9210

Table 5.8: We obtain 2688 nontrivial NCI that reduced to 11 inequivalent classes. For the preparations, we apply the same indistinguishability relations given by (5.59)-(5.62) as in Scenario 7. For the measurements, the following relation is imposed.

$$p(z=0|x,y=2) = 3/2 - p(z=0|x,y=1) - p(z=0|x,y=0)\ \forall x. \tag{5.70}$$

Moreover, we apply the same set of symmetry transformations on both preparations and measurements, as in scenario 7.

Scenario 9

Finally, we consider a scenario where the measurements have three possible outcomes, $z \in \{0,1,2\}$. The indistinguishability conditions in this scenario, consisting of six preparations and two measurements, are given by,

$$\frac{1}{2}(P_0+P_1) \sim \frac{1}{2}(P_2+P_3) \sim \frac{1}{2}(P_4+P_5); \quad \frac{1}{2}\{M_{0|0}+M_{0|1}\} \sim \frac{1}{2}\{M_{1|0}+M_{1|1}\}, \tag{5.71}$$

where $x \in \{0,1,2,3,4,5\}, y \in \{0,1\}$. The set of inequivalent NCI is given in Table (5.9), and the quantum violation of $\mathcal{I}_3$ for qubit systems is illustrated in Fig. (5.2). For most of the NCI, where $\mathcal{Q}_1^{\Pi} < \mathcal{Q}_s^2$ and the noncontextual bounds are the same as $\mathcal{Q}_1^{\Pi}$, any quantum violation certifies nonprojective measurements.

orbit size	Inequalities	$\mathcal{Q}_s^2$	ω_c^2	$\mathcal{Q}_1$	$\mathcal{Q}_1^{\Pi}$
6	$p^0_{4,0}+2p^0_{4,1}-p^1_{4,0} \leqslant 1$	1	0	2	0
6	$-2p^0_{1,0}-2p^0_{1,1}+2p^1_{1,0} \leqslant 0$	0	0	0	0
6	$-2p^1_{0,0}-2p^1_{1,0}+2p^1_{4,0} \leqslant 0$	0	0	0	0
8	$-2p^0_{0,0}-2p^0_{1,0}+3p^0_{2,0}-2p^0_{0,1}-2p^0_{1,1}+2p^0_{2,1}+$ $2p^0_{4,1}+2p^1_{0,0}+2p^1_{1,0}-p^1_{2,0}-2p^1_{4,0} \leqslant 1$	1.4536	0.312	2.8284	1
8	$-2p^0_{0,0}-2p^0_{1,0}+3p^0_{4,0}-2p^0_{2,1}+2p^0_{4,1}+2p^1_{2,0}-p^1_{4,0} \leqslant 1$	1.4536	0.312	2.8284	1
16	$\mathcal{I}_9 = p^0_{1,0}+2p^0_{1,1}-2p^0_{2,1}-2p^1_{0,0}-p^1_{1,0}+2p^1_{2,0} \leqslant 1$	1.4536	0.312	2.8284	1
8	$-2p^0_{0,0}-2p^0_{0,1}-2p^0_{1,1}+2p^0_{4,1}+2p^1_{0,0}-2p^1_{4,0} \leqslant 0$	0.5	0.2	0.8284	0
16	$-2p^0_{0,0}-2p^0_{1,0}+3p^0_{4,0}-2p^0_{1,1}+2p^0_{4,1}+2p^1_{1,0}-p^1_{4,0} \leqslant 1$	1.4536	0.312	2.8284	1
8	$-2p^0_{0,0}-2p^0_{1,0}+2p^0_{4,0}-2p^0_{1,1}+2p^1_{1,0}-2p^1_{4,0} \leqslant 0$	0.5	0.2	0.8284	0
4	$-2p^0_{2,0}-2p^0_{0,1}-2p^0_{1,1}+2p^0_{4,1}+2p^1_{2,0}-2p^1_{4,0} \leqslant 0$	0.5	0.2	0.8284	0
2	$-p^0_{0,0}-p^0_{1,0}+p^0_{4,0}-p^0_{0,1}-p^0_{1,1}+p^0_{2,1}+p^1_{0,0}+p^1_{1,0}-p^1_{2,0}-p^1_{4,0} \leqslant 0$	0.25	0.2	0.4142	0
2	$-2p^0_{4,0}-2p^0_{2,1}-2p^1_{0,0}-2p^1_{1,0}+2p^1_{2,0}+2p^1_{4,0} \leqslant 0$	0.5	0.2	0.8284	0

Table 5.9: Here, we opt for the notation $p^z_{x,y} = p(z|x,y)$. We obtain 107 inequalities, out of which 17 are trivial. The remaining inequalities are reduced to 12 inequivalent classes that are listed above. In order to identify the equivalent NCI, the following indistinguishability relations and symmetry transformations are implemented.

$$p(z|x=3,y) = p(z|x=0,y) + p(z|x=1,y) - p(z|x=2,y)\ \forall y,z \tag{5.72}$$

$$p(z|x=5,y) = p(z|x=0,y) + p(z|x=1,y) - p(z|x=4,y)\ \forall y,z \tag{5.73}$$

$$p(2|x,y) = 1 - p(0|x,y) - p(1|x,y)\ \forall x,y \tag{5.74}$$

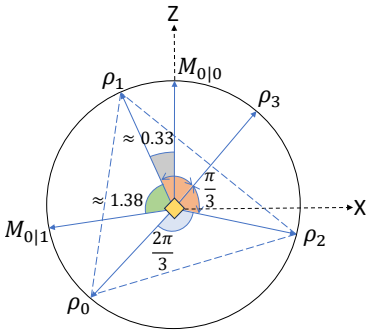
$$P_0 \longleftrightarrow P_1; P_2 \longleftrightarrow P_3; P_4 \longleftrightarrow P_5 \tag{5.75}$$

$$P_0 \longleftrightarrow P_2, P_1 \longleftrightarrow P_3;\ P_0 \longleftrightarrow P_4, P_1 \longleftrightarrow P_5;\ P_2 \longleftrightarrow P_4, P_3 \longleftrightarrow P_5 \tag{5.76}$$

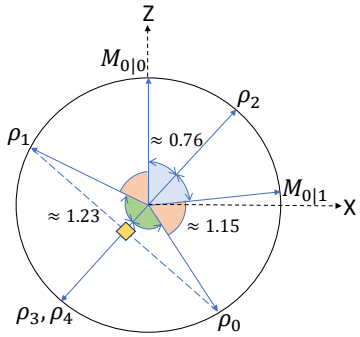
$$P_0 \longleftrightarrow P_3, P_1 \longleftrightarrow P_2;\ P_0 \longleftrightarrow P_5, P_1 \longleftrightarrow P_4;\ P_2 \longleftrightarrow P_5, P_3 \longleftrightarrow P_4 \tag{5.77}$$

$$M_{0|y} \longleftrightarrow M_{1|y} \; \forall y \tag{5.78}$$

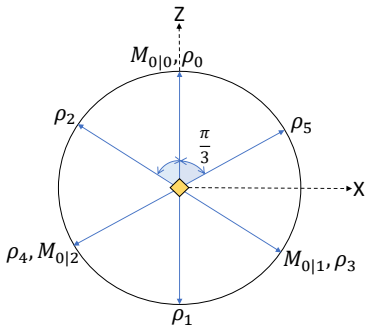
$$M_{z|0} \longleftrightarrow M_{z|1} \; \forall z. \tag{5.79}$$



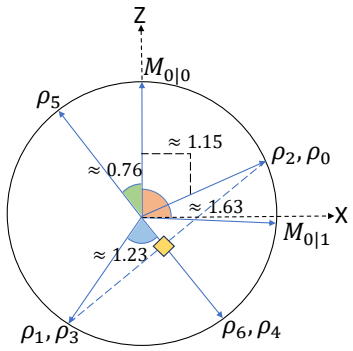
(a): $\mathcal{I}_2 = 2.6458$ (from Tab. 5.2)



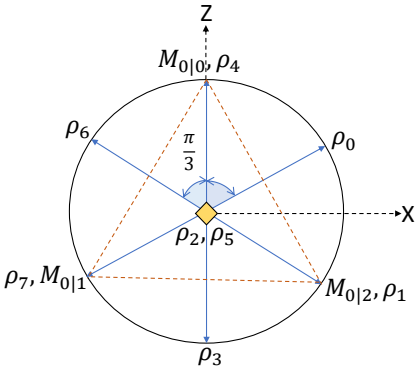
(b): $\mathcal{I}_3 = 3.1231$ (from Tab. 5.3)



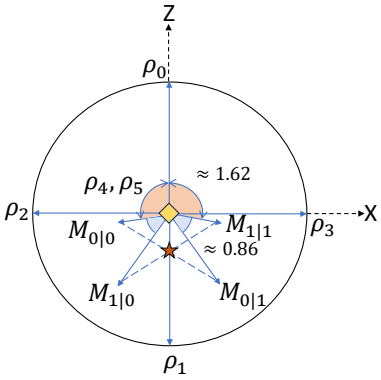
(c): $\mathcal{I}_5 = 2.5$ (from Tab. 5.5)



(d): $\mathcal{I}_6^3 = 8.2462$ (from Tab. 5.6)



(e): $\mathcal{I}_8 = 1.5$ (from Tab. 5.8)



(f): $\mathcal{I}_9 = 1.4536$ (from Tab. 5.9)

Figure 5.2: The x-z plane of the Bloch sphere is considered to pinpoint the quantum states and measurements that yield the maximum violations of some of the NCI, as determined by the see-saw optimization technique for two-dimensional quantum systems. The symbols $\diamond$ and $\star$ represent the indistinguishable mixed state and the indistinguishable measurement effects in the respective scenario. In Figure (5.1(f)), the length of the Bloch vectors representing $M_{0|0}$ and $M_{1|1}$ is approximately 0.3689, and the length of the Bloch vectors representing $M_{1|0}, M_{0|1}$ is approximately 0.674.

Figure (5.2) illustrates the qubit strategies attaining the maximum quantum violations. In many instances, up to machine precision, the maximal quantum violations have been found whenever $\mathcal{Q}_s^d$ matches with $\mathcal{Q}_1$. Of all the NCI, the most resilient one emerges from Scenario 7, with the critical robustness parameter equal to 0.423. Intriguingly, the best obtained quantum violations do not always stem from cases where the indistinguishable state is the maximally mixed state. Scenario 6, which features seven preparations and binary outcomes, represents the simplest scenario showcasing variations in quantum violations for different dimensional

quantum systems.

Based on the see-saw optimization, a range of NCI exist, violations of which serve as witnesses of the dimension of the quantum systems. For instance, if a quantum violation of $\mathcal{I}_6^1$ surpasses 7.6833, then the dimension of the quantum systems must be at least three. Moreover, Scenario 9 provides several NCI whose violations using qubits certify three outcome non-projective measurements. In fact, non-projective measurements are necessary for achieving quantum violations of all the NCI in this contextuality scenario.

5.5 Applications of newly found NCI

5.5.1 Quantum advantage in oblivious communication

Oblivious transfer is a crucial task in information theory with myriad applications in cryptography. In [186], the oblivious transfer task has been generalized, and it is shown that any quantum advantage in such tasks, namely, oblivious communication task, implies preparation contextuality. Moreover, quantum violations of preparation NCIs in prepare-and-measure scenarios directly translate into quantum advantages in oblivious communication tasks. Here, the oblivious condition is associated with the indistinguishable condition on the preparations, and the expression of the respective NCI corresponds to the figure of merit of that task. Consequently, any quantum violation of newly discovered preparation NCIs can be interpreted as a quantum advantage in an oblivious communication task.

In light of our present analysis, it may be worthwhile to mention the following examples. NCI obtained from the simplest contextuality scenario discussed in Section III serves as the success metric of the parity oblivious random access codes [183]. Next, an interesting fact emerges from the discussion after Table (5.2). The optimal classical encoding strategy for the sender in the oblivious communication task with respect to $\mathcal{I}_2$ must be probabilistic for saturating the noncontextual bound 2, and the maximum value of $\mathcal{I}_2$ for deterministic encoding strategies is 1. Further, as already noted earlier, the inequality $\mathcal{I}_7$ can be employed for the 3-bit parity oblivious multiplexing task [183]. Moreover, the optimal classical encoding strategy for the sender in the oblivious communication task with respect to $\mathcal{I}_6^2$ is bounded by 12, and a quantum advantage ensues whenever $\mathcal{I}_6^2 > 12$.

5.5.2 Certification of non-projective measurements

The study by Chaturvedi *et al.* [170] points out that the maximum value of an NCI can always be achieved using projective measurement, where no indistinguishability conditions on measurements are imposed. Consequently, certification of non-projective measurements through the violation of NCIs can only occur with nontrivial indistinguishable conditions on measurements. To accomplish this, it is necessary to establish an upper bound on the expression of NCIs when measurements are restricted to be projective for arbitrary dimensional quantum states and measurements. As outlined in [166], the semi-definite hierarchy can be modified to obtain upper bounds when the measurements are projective. Let us denote these upper bounds by $\mathcal{Q}_1^{\Pi}$.

We have implemented this optimization to obtain $\mathcal{Q}_1^{\Pi}$ in the last two scenarios under consideration, both featuring nontrivial indistinguishability conditions for measurements. Among these scenarios, it was found that in scenario VIII, $\mathcal{Q}_1$ is the same $\mathcal{Q}_1^{\Pi}$ for all NCIs, suggesting this scenario is unable to certify non-projective measurements. However, in scenario IX, the $\mathcal{Q}_1^{\Pi}$ values are lower than $\mathcal{Q}_s^2$ for all NCIs whenever a quantum violation occurs. These precise values are documented in the final column of Table (5.9). For example, corresponding to quantum violation of $\mathcal{I}_9$, the lower bound $\mathcal{Q}_s^2 = 1.453$ and the upper bound $\mathcal{Q}_1 = 2.828$ are obtained. Further, $\mathcal{Q}_1^{\Pi} = 1$, certifying non-projectiveness of the measurements. Notably, the upper bounds for projective measurement coincide with the noncontextual values for all NCIs, indicating that any violation of these NCIs implies unequivocally that the measurements are non-projective.

5.5.3 NCIs as dimension witnesses

As a consequence of our extensive investigations, we reveal a noteworthy aspect of the interplay between quantum preparation contextuality and quantum Hilbert space dimension. Specifically, we implement a *novel* hierarchy of SDP relaxations. In particular, the novel scheme employs the scheme described in [166] over the basis generated from the Navascués-Vértesi method for bounding finite-dimensional quantum correlations and retrieve tight upper bounds $Q_{UB}^2 = Q_s^2$ with level 3 for inequalities in Table (5.6). Moreover, without the operational equivalences, the dimension restriction fails to yield non-trivial bounds on the inequalities; the operational equivalences are *necessary* to witness the Hilbert dimension $d > 2$ with these noncontextuality inequalities.

Notably, the lower bounds obtained from the see-saw for dimension $d > 2$ violate the upper bounds for seven noncontextuality inequalities, thereby forming hitherto unknown nontrivial dimension witnesses. In particular, we find that *seven* of ten noncontextuality inequalities in Scenario 6, Table (5.6), double as dimension witnesses for Hilbert space dimension $d > 2$. It is worth mentioning that $\mathcal{I}_6^2$ in Tab.(5.6) is violated by qutrit systems, while qubit states fail to produce any violation.

5.5.4 Randomness certification

Here we demonstrate that novel instances of quantum contextuality found through our approach can be used for semi-device-independent quantum randomness certification with operational equivalences. To exemplify this observation, we consider the inequality $\mathcal{I}_7$ in Table (5.7) found in Scenario 7. In particular, We evaluate the extractable randomness in Bob's output associated with the violation of the noncontextuality inequality $\mathcal{I}_7 \in (1, 1.7321]$. Let us suppose that the parties decide to extract randomness from Bob's first measurement $y = 0$ performed on Alice's first input $x = 0$. The certified randomness in this case is gauged min-entropy $H_{min} = -\log_2 p^*$ where $p^* = \max\{p_{0,0}, 1 - p_{0,0}\}$ given the value of $\mathcal{I}_7$. We use the hierarchy of SDP programs [166] to retrieve upper bounds on p^*, which translate to lower bounds on the H_{min}.

In FIG. (5.3) we plot the lower bounds on certified randomness H_{min} obtained from level 3 of the SDP hierarchy against the violation of $\mathcal{I}_7$. We find that non-zero randomness can be certified in the range $\mathcal{I}_7 \in [1.52, 1.7321]$ with maximum 0.34147 coinciding with the maximum attainable violation $\mathcal{I}_7 = Q_s^2 = Q_1$ (up to machine precision). We note here that the choice of $x = 0, y = 0$ turns out be optimal and equivalent to $x = 0, y = 1$ and $x = 0, y = 2$.

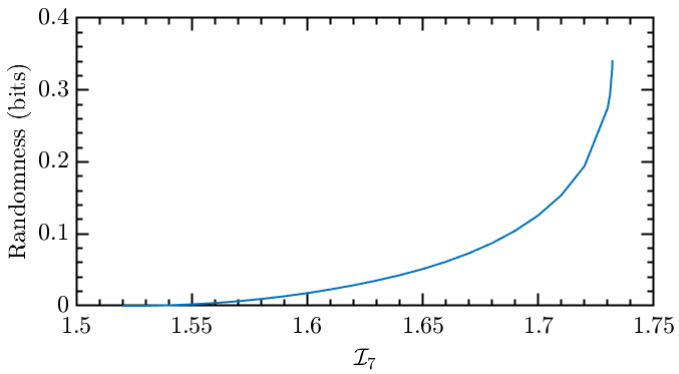


Figure 5.3: Randomness (H_{min}) as a function of $\mathcal{I}_7 \in [1.5, 1.7321]$ from Table (5.7).

5.6 Summary and Conclusion

The generalized concept of quantum contextuality encompasses both preparation and measurement contextuality. However, the traditional method of deriving facet inequalities from the associated noncontextual polytope is computationally challenging due to the polynomial growth in the dimension of the polytope describing the preparations with the number of measurements. We introduced an innovative scheme for constructing a polytope that encompasses the actual noncontextual polytope while ensuring that the complexity of the method remains minimal, leading to necessary conditions for noncontextuality represented by the facet inequalities resulting from the intersection of the extended polytope with the normalization polytope (see Fig. (5.1)). In the present work we have provided a detailed description of our formalism, presenting intricacies of the analysis and explanations of the results obtained.

In particular, here we have comprehensively validated our methodology by applying it to nine contextuality scenarios comprising four to nine preparations and two to three measurements, leading to a large number of the respective sets of hitherto unexplored inequalities. By incorporating the effect of noise within this framework, we have obtained the maximum quantum violations of our newly found imequalities utilizing two different SDP techniques. Figure (5.2) illustrates the qubit strategies attaining the maximum quantum violations. In many instances, up to machine precision, the maximal quantum violations have been found whenever $\mathcal{Q}_s^d$ matches with $\mathcal{Q}_1$. Intriguingly, the best obtained quantum violations do not always stem from cases where the indistinguishable state is the maximally mixed state. Of all the NCI, the most resilient one emerges from Scenario 7, with the critical robustness parameter equal to 0.423.

We have discussed a range of information processing applications where violations of our derived NCI could be employed to obtain quantum advantage of contextuality. For instance, a set of NCI exist, violations of which serve as witnesses of the dimension of the quantum systems. Scenario 6, which features seven preparations and binary outcomes, represents the simplest scenario showcasing variations in quantum violations for different dimensional quantum systems. Moreover, Scenario 9 provides several NCI whose violations using qubits certify three outcome non-projective measurements. In fact, non-projective measurements are necessary for achieving quantum violations of all the NCI in this contextuality scenario.

It is worth noting that there could potentially be further symmetries present in certain contextuality scenarios that haven't been accounted for during the process of deriving the inequiv-

alent classes of NCI. These unexplored symmetries might lead to a reduction in the number of distinct sets of NCI. Further, it's possible to consider scenarios with more than one set of indistinguishability conditions, each corresponding to convex decompositions of mixed preparations (or measurements) [166]. Extending our method to cover such scenarios is a straightforward task that could be explored more thoroughly in future research. Finally, the present work should motivate exploration of general contextuality scenarios to leverage quantum advantage in information processing tasks other than the tasks of oblivious comunication, non-projective measurements, dimension witness and randomness certification, considered herein.

CHAPTER 6

SHARING QUANTUM NONLOCALITY AND TELEPORTATION OVER LONG DISTANCE USING OPTICAL HYBRID STATES

6.1 Introduction

Bell nonlocality [6, 196, 197] allows two parties to establish correlations that surpass the constraints of local hidden variable theories. This fundamental phenomenon underpins several advanced quantum applications, including secure communication [198–202], enhanced computational methods [203–205], and key foundational studies such as self-testing [206–209] and device-independent certification [210–214].

Despite extensive theoretical and experimental advancements [215, 216], achieving Bell nonlocal correlations over long distances in ground-based optical fiber networks [217–226] remains a significant hurdle. Overcoming these limitations is crucial for the development of a

reliable and scalable quantum internet [227, 228].

Bell nonlocality is primarily studied in two distinct physical systems: discrete-variable (DV) spin-like systems [215, 216] and continuous-variable (CV) optical states with a Gaussian profile [229–232]. While both DV and CV frameworks present distinct advantages and limitations [233–235], even with advancements in generating weak coherent pulses [236–239], the search for an optimal system for quantum information processing within a linear-optics-based telecommunication infrastructure remains an open challenge.

An alternative class of physical systems that combines both DV and CV components—known as optical hybrid states [240–243]—exhibits comparable intrinsic correlations [244–246] under both particle- and wave-like measurement scenarios [247]. These hybrid states play a crucial role in quantum teleportation [248–254], fault-tolerant quantum computation [255–258], and offer a viable alternative for distributing quantum correlations beyond the conventional DV- and CV-only approaches [259].

Despite their successful generation across various experimental platforms [251, 260–268], further investigation is needed to explore their potential in sustaining stronger correlations beyond entanglement over long distances.

In this chapter, we explore entanglement-swapping protocols [259, 269, 270] within the framework of modern quantum architectures [271–274]. Our focus is on utilizing optical hybrid states as an initial resource to establish discrete-variable (DV) Bell pairs between two distant laboratories. The proposed scheme relies on entanglement swapping performed on the continuous-variable (CV) components at an intermediate location between the two laboratories. This effectively doubles the distance between them compared to a direct point-to-point transmission. This method offers two key advantages: **(i)** It ultimately generates a DV polarization Bell pair, which can be efficiently measured. **(ii)** Unlike conventional methods, it eliminates the need for homodyne detection, which suffers from low efficiency at the telecommunication wavelength ($\sim$ 1550nm).

We further assess the quality of the shared Bell-CHSH correlation in terms of quantum teleportation [275] of an unknown qubit that serves as a prototypical quantum information processing task facilitating the possibility of distributed quantum computing [276]. Alongside different proposed schemes to witness quantum teleportation with entangled states [277] as well as noisy channels [278], Bell-CHSH nonlocality plays a significant role in ensuring teleportation beyond the classical limit [279, 280]. Our numerical results that indicate the possibility of quantum teleportation in fiber optical setups [226, 281–285], provides an operational characterization of our proposed scheme representing its efficacy in implementation of Bell-CHSH

violation over large distances.

We evaluate our scheme under transmission losses with ideal detectors, demonstrating that optical hybrid states enable long-distance entanglement distribution (250 km) with high Bell-CHSH violation and near-perfect teleportation fidelity. While Bell-CHSH violation decreases with lab separation and coherent amplitude, the success probability follows a non-monotonic trend—initially increasing with coherent amplitude due to higher photon transmission but eventually declining due to greater susceptibility to losses. This leads to an optimal coherent amplitude (α) maximizing success probability.

To access the impact of detector inefficiency, in presence of transmission losses, we next analyze the Bell-CHSH violation and teleportation of the input qubit with non-ideal detectors. We observe that the performance drops sharply with decrease of the detection efficiency as it scales as the square of the detection efficiency. Here, we present corresponding results for 5% and 10% detection inefficiencies for which both the Bell-CHSH violation and teleportation fidelity drops to $\sim$ 90% and 81% respectively. However, even with the inefficient detectors one can still achieve a large distance ($\sim$ 200 km). These results signify the efficacy of our scheme for sharing quantum correlation with optical hybrid states in fiber-optics-based architecture. Moreover, it also advocates the viability of an alternate class of systems in quantum communication compared to the conventional DV-only and CV-only approaches as observed earlier [259].

The chapter is organized as follows. In Sec. (6.2) we first describe our protocol for sharing Bell-type nonlocal correlation between two distant parties. Sec. (6.3) contains mathematical descriptions and analytical results on the success of generating the DV Bell pair, corresponding Bell-CHSH violation and teleportation of an unknown qubit with the shared state. In Sec. (6.4) we provide our simulation results on Bell nonlocality and teleportation in presence of transmission losses. In Sec. (6.5) we analyze the effect of inefficient detectors on the Bell nonlocality and the fidelity of teleportation for the shared DV state. Finally, in Sec. (6.6) we summarized and conclude this chapter.

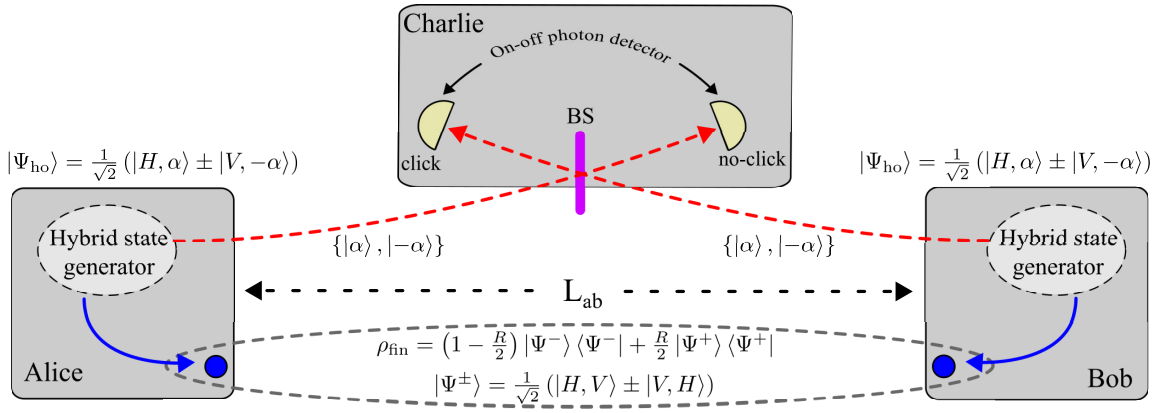


Figure 6.1: Schematic for sharing distant DV Bell-pair using hybrid-optical states. Two parties, say alice and Bob, send the coherent states $\{|\alpha\rangle, |-\alpha\rangle\}$ to a third party in the middle, say Charlie. Subsequently, Charlie mixes the incoming signals through a balanced beam splitter followed by photon measurement by two on-off detectors. Upon receiving the information about which detectors clicks, Alice and Bob post-select the overall state to the desired form.

6.2 Protocol

We consider a particular type of hybrid-optical state that represents entanglement between a polarization states (H/V) and the coherent state ($|\alpha\rangle$) as [251]

$$|\psi_{\rm ho}\rangle = \frac{1}{\sqrt{2}}\left(|H,\alpha\rangle + |V,-\alpha\rangle\right), \tag{6.1}$$

where H (V) stands for the horizontal (vertical) polarization. For the sake of simplicity, we have considered real α. Our protocol for sharing correlation with the hybrid states (6.1), schematically shown in Fig. (6.1), proceeds as described below:

- **Step 1 - channel transmission:** Alice and Bob first prepare their individual hybrid-optical states and send the coherent state signal ($\{|\alpha\rangle, |-\alpha\rangle\}$) to a third party, say Charlie. We consider that the transmission channels (optical fiber) are lossy described by the transmission coefficient T ($0 \leq T \leq 1$) such that $T = 1$ corresponds to an ideal lossless channel and $T = 0$ stands for complete loss. For a standard optical cable, channel transmittance is given by $T = 10^{-lL_{ab}/10}$, where L_{ab} is the channel length (in km) and $l = 0.2$ dB/km is the average photon loss per km. Here we consider a symmetric setup, i.e., Charlie sits midway between Alice and Bob. As a consequence, for the coherent signals from Alice and Bob to travel a distance of L, the lab separation becomes $L_{ab} = 2L$. One may also consider a more general transmission channel with additional thermal

noise. However, the loss-only channels closely mimic these general channels as shown earlier [259].

- **Step 2 - swapping measurement:** Charlie then mixes the two incoming signals in a balanced (50 : 50) beam splitter followed by detection through two single-photon detectors. The individual detectors at Charlie's laboratory are described by the measurement setting $\mathcal{M} = \{\Pi_1, \Pi_{\neg 1}\}$, where $\Pi_1 = |1\rangle\langle 1|$ is the projection along the photon-number state $|1\rangle$ and $\Pi_{\neg 1} = \mathbb{1} - \Pi_1$. This step is considered successful only if one of the detectors click while the other remain dormant (no-click event). For the sake of simplicity (without loss of generality) let us consider that the detector on the left (Fig. 6.1) clicks which correspondss to the measurement operator $\mathcal{M}_{\text{succ}} = \Pi_1^{\text{left}} \otimes \Pi_{\neg 1}^{\text{right}}$. To model the detectors realistically, we also consider that the efficiency of the detectors is given by η_0 ($0 \leq \eta_0 \leq 1$) where $\eta_0 = 1$ represents perfect detector. Once the click event successfully takes place, Charlie declares it.

- **Step 3 - sharing final state:** After Step 2 completes successfully, Charlie declares which of the detectors have clicked. Charlie then announces the information, allowing Alice and Bob to post-select their state.

Let us now define the 4-Bell states in the polarization basis as

$$\begin{aligned} |\Psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}\left(|H,V\rangle \pm |V,H\rangle\right) \\ |\Phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}\left(|H,H\rangle \pm |V,V\rangle\right). \end{aligned} \tag{6.2}$$

Considering that the detector on the left side (as shown in the Fig. (6.1)) clicks, the final shared state between Alice and Bob (see Appendix F for further details) is given by

$$\rho_{\text{fin}} = \left(1 - \frac{R}{2}\right)|\Psi^-\rangle\langle\Psi^-| + \frac{R}{2}|\Psi^+\rangle\langle\Psi^+| \tag{6.3}$$

with probability (D.7)

$$\text{Pr} = T\eta_0\alpha^2 e^{-2T\eta_0\alpha^2}, \tag{6.4}$$

where $R = \frac{1-e^{-4(1-T\eta_0)\alpha^2}}{2}$ is the overall effective loss factor.

6.3 Bell-nonlocality and teleportation

In this section, we first analyze the Bell nonlocal character of the shared DV state (6.3) by using polarization-based measurements. To characterize the operational utility of the shared non-locality we further analyze an information processing task, to be precise, the teleportation of an unknown input qubit state. Here, we provide the mathematical expressions for various quantities related to Bell-CHSH violation as well as derive the fidelity of teleportation of an unknown polarization qubit state using the shared DV state. It must be noted that for the sake of generality we consider all the detectors to be imperfect with the efficiency η_0 ($0 \leq \eta_0 \leq 1$).

6.3.1 Bell Violation

In the polarization basis ($\{|H\rangle, |V\rangle\}$), the binary (2-outcome) operator $\Pi = |H\rangle\langle H| - |V\rangle\langle V|$ yields either of ± 1 based on the state of the polarization. The influence of noise (D.4) leads to the noisy binary measurement $\Pi \to \Pi(\eta_0) = \eta_0 (|H\rangle\langle H| - |V\rangle\langle V|)$. Now, a unitary rotation between the polarization degrees of freedom could be implemented through a polarization-beam-splitter (PBS) with phase components defined by the unitary matrix

$$U(\eta, \theta) = \begin{pmatrix} \sqrt{\eta} & \sqrt{1-\eta}e^{i\theta} \\ -\sqrt{1-\eta}e^{-i\theta} & \sqrt{\eta} \end{pmatrix}. \tag{6.5}$$

This leads to the polarization-rotated-binary-operator (PRBO) as (E.1)

$$\begin{aligned} \hat{O}(\eta, \theta) &= U(\eta, \theta)\Pi(\eta_0)U^{\dagger}(\eta, \theta) \\ &= N_{hh}(\eta, \theta)|H\rangle\langle H| + N_{vv}(\eta, \theta)|V\rangle\langle V| \\ &\quad - N_{hv}(\eta, \theta)|H\rangle\langle V| - N^{*}_{hv}(\eta, \theta)|V\rangle\langle H|, \end{aligned} \tag{6.6}$$

where $N_{hh}(\eta, \theta) = -\eta_0(1-2\eta)$, $N_{vv}(\eta, \theta) = \eta_0(1-2\eta)$ and $N_{hv}(\eta, \theta) = 2e^{i\theta}\eta_0\sqrt{\eta(1-\eta)}$.

Taking into consideration the joint binary-outcome measurement, described by $\hat{O}_{a_1,b_1}(\eta, \theta, \zeta, \phi) = \hat{O}_{a_1}(\eta, \theta) \otimes \hat{O}_{b_1}(\zeta, \phi)$ and its expectation value as $\mathcal{E}(\eta, \theta, \zeta, \phi)$ $= \mathrm{Tr}\left[\rho_{a_1b_1}\hat{O}_{a_1,b_1}(\eta, \theta, \zeta, \phi)\right]$, one can recast the Bell-function as

$$\mathcal{B} = \mathcal{E}(\eta_1, \zeta_1) + \mathcal{E}(\eta_1, \zeta_2) + \mathcal{E}(\eta_2, \zeta_2) - \mathcal{E}(\eta_2, \zeta_1) \tag{6.7}$$

which implies CHSH Bell non-locality for $\mathcal{B} > 2$ [196]. To obtain the optimal measurement set-

ting for Bell nonlocality one needs to optimize the Bell-function ($\mathcal{B}$) over the set of $\{|\eta|, \theta, |\zeta|, \phi\}$ where $0 \leq \{|\eta|, |\zeta|\} \leq 1$ and $0 \leq \{\theta, \phi\} \leq 2\pi$. It should also be noted the optimal setting also varies with the distance between the laboratories ($L_{\rm ab}$). We evaluate the Bell function (6.7) numerically (see Sec. 6.4).

6.3.2 Teleportation of unknown qubit input state

Let us now consider the case of teleporting an unknown input pure-state $|\psi_{\rm in}\rangle = \sqrt{p}\,|H\rangle + \sqrt{1-p}e^{i\theta}\,|V\rangle$ using the shared resource (6.3). In the ideal case, Alice's measurements are given by the 4 Bell-state projectors (6.2) $\Pi^{\pm}_{\Psi} = |\Psi^{\pm}\rangle\langle\Psi^{\pm}|$ and $\Pi^{\pm}_{\Phi} = |\Phi^{\pm}\rangle\langle\Phi^{\pm}|$ over the input mode (we denote it by "in") and mode a_1. However, in the presence of inefficient detectors (D.4), these ideal Bell-state measurements change to $\Pi^{\pm}_{\Psi}(\eta_0) = \eta_0^2\Pi^{\pm}_{\Psi}$ and $\Pi^{\pm}_{\Phi}(\eta_0) = \eta_0^2\Pi^{\pm}_{\Phi}$.

For an input pure state $|\psi_{\rm in}\rangle$ and the output mixed state $\rho^{\rm out}$, the fidelity of teleportation is given by $F = {\rm Tr}\left(|\psi_{\rm in}\rangle\langle\psi_{\rm in}|\,\rho^{\rm out}\right)$. This, given the probabilistic nature of the Bell-state measurements $P^{\pm}_{\Psi/\Phi}(\eta_0)$, leads to the average fidelity of teleportation for the chosen measurement settings as (see Appendix D for further details)

$$F_{\rm meas} = \sum_{\xi,\pm} P^{\pm}_{\xi}(\eta_0) F^{\pm}_{\xi}(\eta_0), \tag{6.8}$$

where $F^{\pm}_{\xi}(\eta_0) = \langle\psi_{\rm in}|\,U^{\pm}_{\xi}\rho^{\pm}_{b_1,\xi}(\eta_0)\left(U^{\pm}_{\xi}\right)^{\dagger}|\psi_{\rm in}\rangle$ such that $U^{\pm}_{\xi}$ is the suitable unitary operator to be applied on output state in mode b_1, i.e., $\rho^{\pm}_{b_1,\xi}(\eta_0)$, corresponding to the operator $\Pi^{\pm}_{\xi}(\eta_0)$ ($\xi = \Psi, \Phi$).

Here, we are interested in the fidelity of teleportation averaged over all possible input states, i.e.,

$$F_{\rm av} = \frac{1}{2\pi}\int_0^1 dp \int_0^{2\pi} d\theta F_{\rm meas}. \tag{6.9}$$

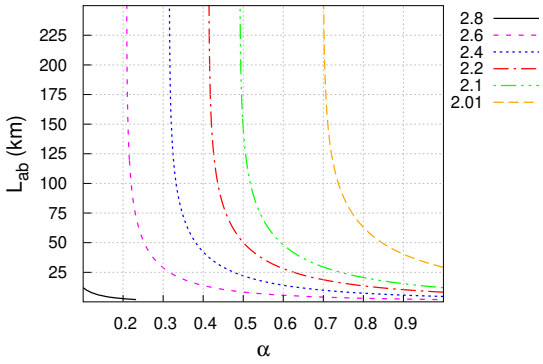
Accordingly, the quantum teleportation for the unknown input state can be characterized as $F_{\rm av} > 2/3$. The average fidelity of teleportation with noisy/imperfect detectors can be shown to be (F.7)

$$F_{\rm av} = \eta_0^2\frac{2-R}{2} = \eta_0^2\frac{1+e^{-4(1-T\eta_0)\alpha^2}}{2}. \tag{6.10}$$

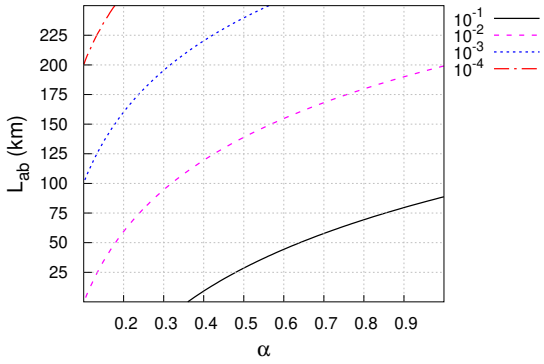
We evaluate the Bell-CHSH violation and quantum teleportation of the input polarization qubit for the shared DV entangled state in the next section.

6.4 Teleportation in presence of transmission losses only

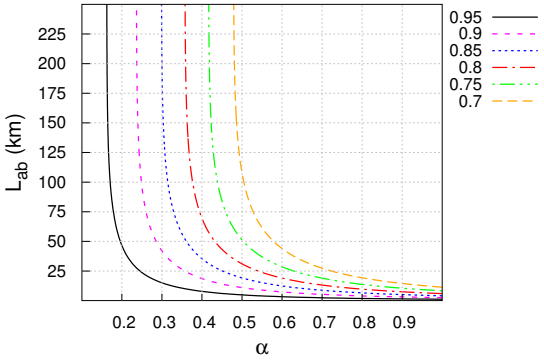
We analyze the efficacy of our scheme by considering its robustness against the transmission losses. To facilitate that, we consider the detector ideal, i.e., $\eta_0 = 1$. The violation of Bell inequality ($\mathcal{B} > 2$) and quantum teleportation ($F_{\text{av}} > 2/3$) are first considered for the case of perfect detectors, i.e.,



(a) Bell-CHSH violation ($\mathcal{B} > 2$)



(b) Probability (Pr) of obtaining the shared DV state



(c) Average fidelity (F_{av}) of the final shared state

Figure 6.2: Contour plots showing (a) Bell-CHSH violation ($\mathcal{B} > 2$), (b) probability (Pr) of obtaining the shared DV state, and (c) average fidelity (F_{av}) of the final shared state, each plotted against lab separation L_{ab} and coherent amplitude α for perfect detectors ($\eta_0 = 1$).

In Fig. 6.2(a) we plot the contour graph for Bell-violation of the shared DV state as a function of the lab separation (L_{ab}) and the coherent amplitude (α). It may be noted that, for the sake of simplicity, here we have displayed the results up to a distance ($\sim$ 250 km). However, from Fig. 6.2(a) it is evident that our hybrid-optical state-based scheme can asymptotically lead to much larger distances. The amount of Bell-CHSH violation drops with an increase in

both the lab separation (L_{ab}) and the coherent amplitude (α).

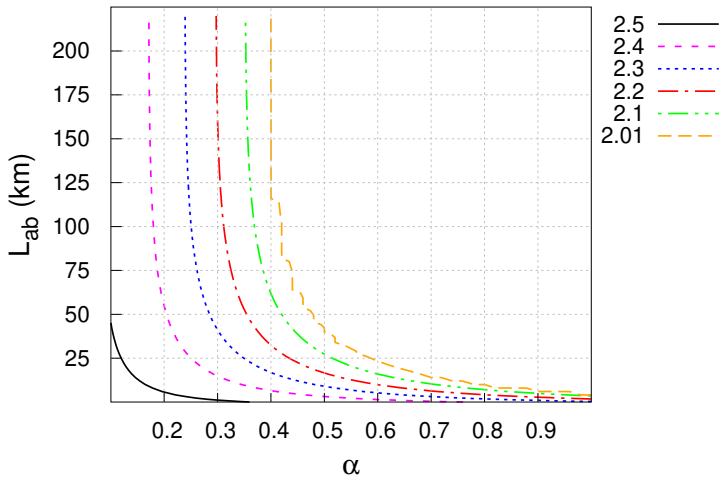
In Fig. 6.2(b) we plot the contour graph for the probability of generating the DV state with L_{ab} and α. It may be noted that the success probability (6.4) manifests a non-monotonic character [259]. For a fixed lab separation, the probability of sharing the DV entangled pair first increases and then drops with increase in the coherent amplitude (α). This could be understood in terms of the interplay between the probability of successful detection and the loss-robustness of the transmitted signal. As the α increases, it enhances the chances of non-zero photon being detected by the click event after passing through lossy optical fiber. On the other hand, an increase in α also increases the mean photon number of the signal, which, in turn, makes it more vulnerable to transmission losses. Our results indicate that teleportation could be implemented up to a distance of $\sim 50-80$ Kms with a ~ 10 % success probability for intermediate values of the coherent amplitude (α).

It is evident from Figs. 6.2(a) and 6.2(b) that for a fixed lab separation (L_{ab}), with an increase in α, Bell-violation drops while the probability of generating the state increases. This could be understood as follows. For a very small α (~ 0.1), the shared DV-state provides an almost Bell state $\rho \sim |\Psi^-\rangle\langle\Psi^-|$; however, its probability is negligible, i.e., Pr $\rightarrow 10^{-4}$. On the other hand, for a relatively large value of α ($\gtrsim 1$) the shared state is considerably away from an ideal Bell state ($|\Psi^-\rangle$) and thus manifests a small violation; however, its probability increases by $2-3$ order of magnitude with Pr $\sim 10^{-1}-10^{-2}$. This indicates from a practical perspective that one needs to find an optimal choice of α, given the physical context.

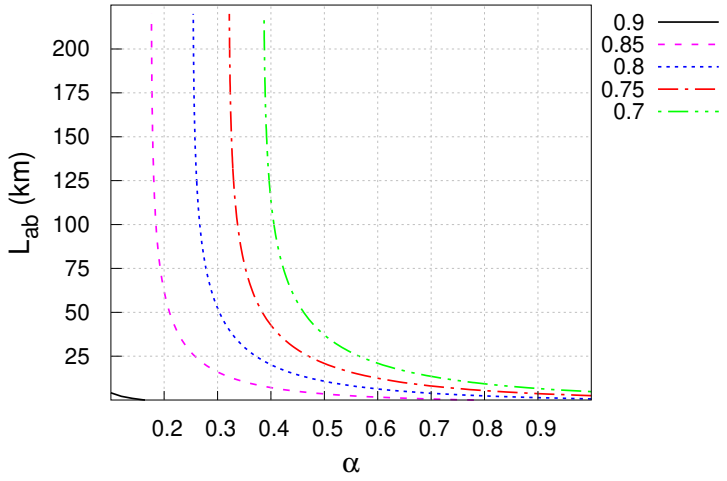
In Fig. 6.2(c) we elaborate on our results on the fidelity of teleportation of a polarization qubit (F_{av}) against the total transmission distance (L_{ab}) and coherent amplitude (α). Similar to the case of Bell-CHSH violation, here also we observe that in the absence of any detection inefficiency, it is possible to perform quantum teleportation over long distances with standard optical fibers. However, the parameter region for quantum teleportation is smaller than that for Bell-CHSH violation. This could be attributed to the fact that Bell non-locality is not sufficient to ensure the success of quantum teleportation [279, 280].

6.5 Effect of detection inefficiency

We now analyze the effect of inefficient detectors on the Bell non-locality and the fidelity of teleportation for the shared DV state. We elaborate on our results on the Bell-CHSH violation ($\mathcal{B} > 2$) and average fidelity ($F_{\text{av}} > 2/3$) in Figs. (6.3) and (6.4) with 95% ($\eta_0 = 0.95$) and 90% ($\eta_0 = 0.9$) detection efficiencies, respectively, in the presence of transmission losses.



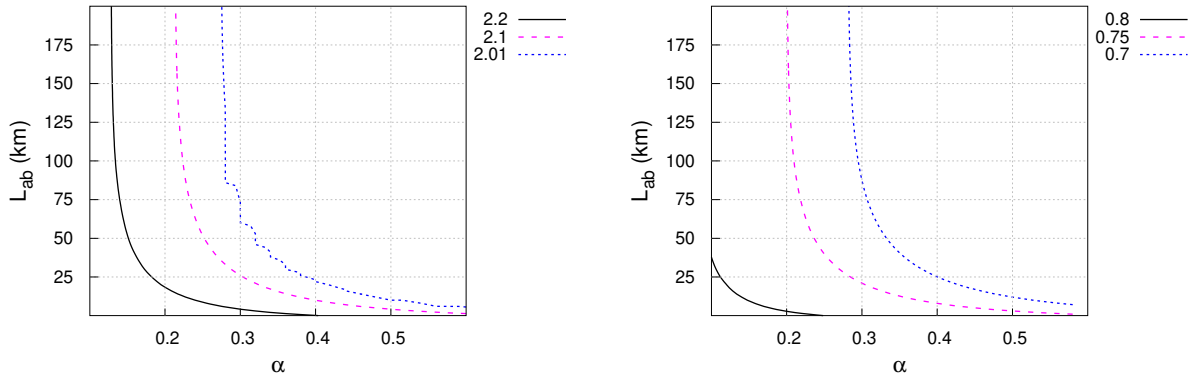
(a) Bell-CHSH violation



(b) Average fidelity

Figure 6.3: Contour plots of (a) Bell-CHSH violation ($\mathcal{B} > 2$) and (b) average fidelity of teleportation ($F_{\text{av}} > 2/3$), as functions of lab separation L_{ab} and coherent amplitude α, assuming 5% detection inefficiency ($\eta_0 = 0.95$).

As it is evident from the Figs. (6.3) and (6.4), the maximum Bell-CHSH violation as well as the highest fidelity of teleportation get significantly reduced as the detection efficiency decreases. The sharp drop in the performance of both noisy Bell-measurement (6.6) and fidelity of teleportation (6.10) is a reflection of the nonlinear nature of their dependence on the detector efficiency. However, it may be noted that our scheme allows us to achieve a distance ($\sim$ 200 km) between the laboratories in the presence of both transmission losses and inefficient detectors for measurable Bell-CHSH violation and teleportation fidelity of an unknown qubit.



(a) Bell-CHSH violation

(b) Average fidelity

Figure 6.4: Contour plots of (a) Bell-CHSH violation ($\mathcal{B} > 2$) and (b) average fidelity of teleportation ($F_{\text{av}} > 2/3$), as functions of lab separation L_{ab} and coherent amplitude α, assuming 10% detection inefficiency ($\eta_0 = 0.90$).

6.6 Summary and Conclusion

In this chapter, we have analyzed the efficacy of the hybrid-optical states in generating a polarization-entangled DV state sharing Bell-CHSH correlation within the telecommunication architecture. By combining the respective advantages of both the DV and the CV systems, we have shown that the hybrid-optical states enable Bell-CHSH violation over a large distance—a major obstacle in fiber-optics based quantum communication [217–226]. While our numerical results indicate the feasibility of achieving high Bell-CHSH violation that results in near-perfect teleportation of unknown qubits over a distance of ($\sim$ 250 km), the performance of both Bell-CHSH violation as well as the fidelity of teleportation is limited by the detector inefficiencies. Nonetheless, we have presented the case that indicates the possibility of achieving non-vanishing Bell-CHSH violation as well as quantum teleportation over $\sim$ 200 km of lab separation under lossy transmission and 10% detection error.

It may be noted that the issue of phase randomization of the transmitted signal inherent to the hybrid-optical state-based scheme can be taken care of by using a proper phase-locking mechanism [286] or by using tailored algorithms that do not require any phase-locking [287]. Moreover, the deterministic generation of the hybrid-optical states with high purity at 780nm to 1064nm wavelength band [263–265] makes our analysis more practically feasible when combined with technologies like frequency conversion to telecommunication wavelength ($\sim$ 1550nm) [226] as well as time-bin encoding [266]. It may be also noted that in the case of atom-light based setups [226], performance of Bell-CHSH violation as well as teleportation with the shared DV state would be further interesting to explore since the atomic states

could measured with higher efficiencies.

In view of previous results on sharing Bell nonlocal correlations [219, 220, 222, 223, 225], our analysis indicates the possibility of significant improvement in enhancing the lab separation to more than an intercity distance. Moreover, our analysis also indicates the possibility of considerably enhancing the distance over which faithful quantum teleportation could be achieved [226]. Besides enhancing the distance between the labs, the hybrid-optical setup further provides a unique platform that enables quantum communication protocols beyond the paradigm of weak coherent pulse [288, 289] as well as avoids inefficient homodyne measurements typically used for CV systems [290, 291].

Our results on the viability of achieving Bell-CHSH violation with hybrid states over intercity distances further bolster the promise of an alternate platform for quantum information processing compared to DV-only and CV-only approaches, as advocated through similar results on entanglement distribution [259, 269, 270]. One may also consider a loophole-free model for the hybrid-optical-state based schemes leading to device-independent quantum key distribution [198–202]. In view of these, we believe that our results on sharing Bell-CHSH non-locality over long distances using hybrid states could be useful for practical quantum information processing [292], memoryless quantum communication [293], as well as in studies with foundational interest [294].

CHAPTER 7

CONCLUSIONS & FUTURE DIRECTIONS

This chapter summarises numerous key aspects of quantum communications discussed in this dissertation, along with inferences on potential future developments. As previously mentioned in the introduction, entanglement and other quantum correlations are shown to be valuable resources in several information-theoretic tasks that are not achievable in classical theory. This thesis presents many information-theoretical challenges in the realm of quantum communications. We demonstrated DI-QKD using random quantum states, long-distance teleportation employing hybrid entangled states and discussed the origin of quantum advantage associated with RAC. Apart from these, in this dissertation, we present many applications of generalised quantum contextuality by deriving several novel nontrivial noncontextuality inequalities.

In Chapter 3, we establish that any nonzero quantum advantage in an random access code (RAC) with shared randomness necessarily entails a violation of the noninvasive-realist model. To formalize this connection, we derive temporal inequalities for each $n \mapsto 1$ RAC based on the assumptions of realism and noninvasive measurability, demonstrating that the maximum

success probability achievable through optimal classical strategies is inherently constrained by the noninvasive-realist bound. Furthermore, we show that any nonzero quantum advantage in an RAC can serve as a witness for genuine randomness, a property absent in previously proposed RAC-based protocols. However, determining the maximum quantum success probability for a general $n \mapsto 1$ RAC becomes computationally challenging for large values of n, necessitating numerical techniques. Finally, we emphasize the experimental feasibility of our proposed protocol, which leverages Leggett-Garg inequality (LGI) violation, thereby offering a robust and practical approach for generating genuine randomness without entanglement.

In Chapter 4, we investigate the secure key rate of randomly generated two-qubit states across all four ranks in entanglement-based quantum key distribution (QKD). Our analysis is based on extensive numerical simulations, considering 10^6 states for each rank. Initially, we quantify the fraction of states within each rank that exhibit Bell nonlocality and those capable of generating a positive secure key rate in device-independent QKD (DI-QKD) under both general and optimal collective attacks by an eavesdropper. Our findings reveal a fundamental trend: as the rank of the states increases, both Bell nonlocality and the minimum secure key rate decreases under both attack scenarios, which is a fundamental feature of such randomly generated states.

Furthermore, our study indicates that when the rank of the states increases, the decrease in the secure key rate is more significant than the diminution in Bell-CHSH violation. Moreover, the fraction of states possessing quantum resources, such as entanglement and Bell nonlocality, decreases at a slower rate compared to the fraction of states capable of generating a positive secure key rate. While quantum resourcefulness is a necessary condition for secure key generation. The process of generating a secure key imposes more stringent requirements, resulting in a significantly lower number of states that can achieve a positive key rate compared to those that exhibit quantum correlations.

Additionally, we observe that states with the same magnitude of entanglement can yield different secure key rates, emphasizing that entanglement alone does not determine the key rate. We establish upper and lower bounds for the minimum secure key rate of all two-qubit mixed states, demonstrating that it is upper bounded by the key rate of a pure state and lower bounded by the key rate of a Werner state with the same negativity. This holds for both general and optimal collective attack strategies, providing crucial insights into the interplay between entanglement, nonlocality, and security in DI-QKD.

In Chapter 5, the conventional method of extracting facet inequalities from the pertinent noncontextual polytope is computationally demanding due to the polynomial growth in the

dimension of the polytope describing the preparations with the number of measurements. In this work, we introduce an innovative approach for constructing a polytope that encompasses the actual noncontextual polytope while ensuring that the complexity of the method remains minimal. The facet inequalities resulting from the intersection of our extended polytope with the normalization polytope constitute necessary conditions for noncontextuality. Our formalism is applicable to any general contextuality scenario with an arbitrarily large number of preparation and measurement indistinguishability conditions and demonstrates how quantum advantage of contextuality could be revealed from a given scenario in a computationally efficient manner.

We demonstrate the efficacy of our proposed method by applying it here to several examples of contextuality scenarios. Consequently, we retrieve a large number of novel NCIs, violations of which serve as sufficient conditions for demonstrating quantum contextuality in these scenarios. We employ two semi-definite programming techniques for retrieving the lower and upper bounds, respectively, on the maximum quantum violations of the NCI. We further study the robustness of the quantum violations against noise. Our investigation uncovers hitherto unexplored non-trivial noncontextuality inequalities and reveals intriguing aspects of quantum contextual correlations, including applications in information processing tasks such as oblivious communication, dimension witness, certification of non-projective measurements, and randomness generation.

In Chapter 6, we explore the use of optical hybrid states to generate a polarization-entangled DV state exhibiting Bell-CHSH correlations within telecommunication systems. By combining the benefits of DV and CV systems, we show that hybrid states enable Bell-CHSH violation over long distances, addressing a major challenge in fiber-optic-based quantum communication. Our simulations demonstrate the feasibility of Bell-CHSH violation and near-perfect teleportation over $\sim$ 250 km, although performance is limited by detector inefficiencies. Despite this, we show that quantum teleportation over $\sim$ 200 km is possible even under 10% detection error and lossy transmission. This setup offers a unique platform for enhancing quantum communication protocols and bypassing inefficiencies in typical CV systems. Overall, our results suggest that long-distance Bell-CHSH nonlocality using hybrid states could significantly impact quantum information processing and memoryless quantum communication.

The research conducted in this thesis gives rise to several open questions that merit further investigation in future studies:

In Chapter 3, We demonstrated that any nonzero quantum advantage in a random access code (RAC) with shared randomness inherently leads to a violation of the noninvasive-realist model. However, this present study result is based on a qubit system. Extending this analysis to qudit systems remains an avenue for future research.

In Chapter 4, We establish that the minimum secure key rate for all two-qubit mixed states is constrained between an upper bound given by the key rate of a pure state and a lower bound determined by the key rate of a Werner state with the same entanglement, quantified by negativity, under both optimal and general collective attack strategies. It might also be interesting to study in future the effect of statistical fluctuations in the number of randomly generated states on the above bounds.

Our present study is based on certain quantum resources, like entanglement and Bell nonlocality. However, a steering-based study might be interesting for future research, as it could be useful for semi-device-independent quantum communication tasks.

In Chapter 5, our present study has focused on sets of indistinguishability conditions regarding preparations and measurements, respectively, to render them indistinguishable from each other. It is possible to consider scenarios with more than one set of indistinguishability conditions for a given scenario, each corresponding to convex decompositions of mixed preparations or measurements. Extending our method to cover such scenarios could be explored more thoroughly in future research. The inherently contextual nature of quantum theory offers several distinct advantages in cryptographic and computational tasks. Our present analysis should motivate future endeavours to leverage newfound instances of quantum contextuality for a wide range of information theoretic applications.

In Chapter 6, our results on the viability of achieving Bell-CHSH violation with hybrid states over intercity distances further bolster the promise of an alternate platform for quantum information processing compared to DV-only and CV-only approaches, as advocated through similar results on entanglement distribution.

One may also consider a loophole-free model for optical-hybrid-state-based schemes leading to device-independent quantum key distribution for future research. In view of these, we believe that our results on sharing Bell-CHSH nonlocality over long distances using hybrid states could be useful for practical quantum information processing and memoryless quantum communication as well as in studies with foundational interest.

Appendices

APPENDIX $\mathcal{A}$

DERIVATION OF THE CLASSICAL BOUND FOR THE TEMPORAL INEQUALITY USING MACROREALISM

A.1 Ontic model of $2 \mapsto 1$ RAC

The average of a quantum operator in the Heisenberg picture can be written as an average over a set of hidden variables λ. The role of the initial state $\rho(\lambda)$ is to provide a probability distribution on the set of hidden variables, called the ontic state. The average of an observable A (measurement carried out at time t can be written as)

$$\langle A_t \rangle = \int d\lambda A_t(\lambda)\rho(\lambda) \tag{A.1}$$

where $A_t(\lambda)$ is the value taken by the observable on the hidden variable λ. The correlation between two observables A_{t_i} (measured at some time t_i), B_{t_j} (measured at some later time t_j)

is given by

$$\langle A_{t_i} B_{t_j} \rangle = \int d\lambda A_{t_i}(\lambda) B_{t_j}(\lambda) \rho(\lambda \mid A_{t_i}) \tag{A.2}$$

In general, we can always ignore the effect of final measurement due to noninvasive measurability (NIM). NIM can be defined as $\rho(\lambda \mid A_{t_i}, B_{t_j}, \dots) = \rho(\lambda)$, i.e., a measurement does not change the distribution of λ. In Eq.(A.2), $\rho(\lambda)$ not depends on observable B_{t_j} due to observable B_{t_j} being measured after the measurement of observable A_{t_i}.

Let us take Alice's preparations to be eigenstates of observables $\{A_1, A_2\}$ and Bob's measurements to be $\{B_1, B_2\}$. Let, measurement A be carried out at some time t_i, and measurement B be carried out at some later time t_j. Now, imposing the conditions of realism and NIM, we obtain

$$\begin{aligned}
&\langle A_1 B_1 \rangle + \langle A_2 B_1 \rangle = \int d\lambda [A_1(\lambda) B_1(\lambda) \rho(\lambda \mid A_1) + A_2(\lambda) B_1(\lambda) \rho(\lambda \mid A_2)] \\
&= \int d\lambda A_1(\lambda) B_1(\lambda) [1 \mp A_2(\lambda) B_2(\lambda)] \rho(\lambda \mid A_1) + \int d\lambda A_2(\lambda) B_1(\lambda) [1 \pm A_1(\lambda) B_2(\lambda)] \rho(\lambda \mid A_2).
\end{aligned}$$

Taking the modulus on both sides and using the triangle inequality we obtain,

$$|\langle A_1 B_1 \rangle + \langle A_2 B_1 \rangle| \leq 2 \pm [\int d\lambda A_1(\lambda) B_2(\lambda) \rho(\lambda \mid A_1) - \int d\lambda A_2(\lambda) B_2(\lambda) \rho(\lambda \mid A_2)].$$

Now invoking NIM, we have,

$$|\langle A_1 B_1 \rangle + \langle A_2 B_1 \rangle| \mp [\langle A_1 B_2 \rangle - \langle A_2 B_2 \rangle] \leq 2.$$

or,

$$\mathcal{K}_{2 \mapsto 1} \leq 2. \tag{A.3}$$

This is the four term Leggett-Garg inequality.

A.2 Ontic model of $3 \mapsto 1$ RAC

Let us take Alice's preparations to be eigenstates of $\{A_1, A_2, A_3, A_4\}$ and Bob's measurements to be $\{B_1, B_2, B_3\}$. Now, following similar steps as in the derivation of the Bell inequality, we obtain the sum of four correlations,

$$\langle A_1 B_1 \rangle + \langle A_4 B_1 \rangle + \langle A_2 B_1 \rangle + \langle A_3 B_1 \rangle = \int d\lambda [A_1(\lambda) B_1(\lambda) \rho(\lambda \mid A_1) + A_4(\lambda) B_1(\lambda) \rho(\lambda \mid A_4) +$$

$$
\begin{aligned}
&A_2(\lambda)B_1(\lambda)\rho(\lambda \mid A_2) + A_3(\lambda)B_1(\lambda)\rho(\lambda \mid A_3)] \\
&= \int d\lambda A_1(\lambda)B_1(\lambda)[1 \mp A_4(\lambda)(B_2(\lambda) + B_3(\lambda))]\rho(\lambda \mid A_1) \\
&+ \int d\lambda A_4(\lambda)B_1(\lambda)[1 \pm A_1(\lambda)(B_2(\lambda) + B_3(\lambda))]\rho(\lambda \mid A_4) \\
&+ \int d\lambda A_2(\lambda)B_1(\lambda)[1 \mp A_3(\lambda)(B_2(\lambda) - B_3(\lambda))]\rho(\lambda \mid A_2) \\
&+ \int d\lambda A_3(\lambda)B_1(\lambda)[1 \pm A_2(\lambda)(B_2(\lambda) - B_3(\lambda))]\rho(\lambda \mid A_3) \qquad \text{(A.4)}
\end{aligned}
$$

Now, we take the modulus of both sides and use the triangle inequality to obtain,

$$
\begin{aligned}
&|\langle A_1B_1\rangle + \langle A_4B_1\rangle + \langle A_2B_1\rangle + \langle A_3B_1\rangle| \leq 4 \pm [\int d\lambda A_1(\lambda)(B_2(\lambda) + B_3(\lambda))\rho(\lambda \mid A_1) \\
&- \int d\lambda A_4(\lambda)(B_2(\lambda) + B_3(\lambda))\rho(\lambda \mid A_4) + \int d\lambda A_2(\lambda)(B_2(\lambda) - B_3(\lambda))\rho(\lambda \mid A_2) \\
&- \int d\lambda A_3(\lambda)(B_2(\lambda) - B_3(\lambda))\rho(\lambda \mid A_3)]. \qquad \text{(A.5)}
\end{aligned}
$$

Invoking NIM, we have,

$$
\begin{aligned}
&|\langle A_1B_1\rangle + \langle A_4B_1\rangle + \langle A_2B_1\rangle + \langle A_3B_1\rangle| \mp [\langle A_1(B_2 + B_3)\rangle - \langle A_4(B_2 + B_3)\rangle + \langle A_2(B_2 - B_3)\rangle \\
&- \langle A_3(B_2 - B_3)] \leq 4.
\end{aligned}
$$

or,

$$
\mathcal{K}_{3\mapsto 1} \leq 4. \qquad \text{(A.6)}
$$

A.3 Ontic model of $4 \mapsto 1$ RAC

Similarly, for $4 \mapsto 1$ RAC, here Alice has 8 preparations to be eigenstates of $\{A_1, A_2, ..., A_8\}$ and Bob has 4 measurements to be $\{B_1, B_2, B_3, B_4\}$. Now using a similar procedure presented for deriving the classical bound corresponding to $2 \mapsto 1$ RAC, we can obtain

$$
\begin{aligned}
&\langle A_1B_1\rangle + \langle A_5B_1\rangle + \langle A_1B_3\rangle + \langle A_2B_3\rangle + \langle A_2B_1\rangle + \langle A_6B_1\rangle + \langle A_3B_1\rangle + \langle A_7B_1\rangle + \langle A_4B_1\rangle \\
&+ \langle A_8B_1\rangle + \langle A_5B_3\rangle + \langle A_6B_3\rangle - \langle A_4B_3\rangle - \langle A_7B_3\rangle - \langle A_8B_3\rangle - \langle A_3B_3\rangle \\
&= \int d\lambda [A_1(\lambda)B_1(\lambda)\rho(\lambda \mid A_1) + A_5(\lambda)B_1(\lambda)\rho(\lambda \mid A_5) + \\
&A_1(\lambda)B_3(\lambda)\rho(\lambda \mid A_1) + A_2(\lambda)B_3(\lambda)\rho(\lambda \mid A_2) + A_2(\lambda)B_1(\lambda)\rho(\lambda \mid A_2) + A_6(\lambda)B_1(\lambda)\rho(\lambda \mid A_6) + \\
&A_3(\lambda)B_1(\lambda)\rho(\lambda \mid A_3) + A_7(\lambda)B_1(\lambda)\rho(\lambda \mid A_7) + A_4(\lambda)B_1(\lambda)\rho(\lambda \mid A_4) + A_8(\lambda)B_1(\lambda)\rho(\lambda \mid A_8) + \\
&A_5(\lambda)B_3(\lambda)\rho(\lambda \mid A_5) + A_6(\lambda)B_3(\lambda)\rho(\lambda \mid A_6) - A_4(\lambda)B_3(\lambda)\rho(\lambda \mid A_4) - A_7(\lambda)B_3(\lambda)\rho(\lambda \mid A_7) -
\end{aligned}
$$

$$
\begin{aligned}
&A_8(\lambda)B_3(\lambda)\rho(\lambda \mid A_8) - A_3(\lambda)B_3(\lambda)]\rho(\lambda \mid A_3)] \\
&= \int d\lambda A_1(\lambda)B_1(\lambda)[1 \mp A_5(\lambda)B_2(\lambda)]\rho(\lambda \mid A_1) \\
&+ \int d\lambda A_5(\lambda)B_1(\lambda)[1 \pm A_1(\lambda)B_2(\lambda)]\rho(\lambda \mid A_5) + \int d\lambda A_1(\lambda)B_3(\lambda)[1 \mp A_2(\lambda)B_4(\lambda)]\rho(\lambda \mid A_1) \\
&+ \int d\lambda A_2(\lambda)B_3(\lambda)[1 \pm A_1(\lambda)B_4(\lambda)]\rho(\lambda \mid A_2) + \int d\lambda A_2(\lambda)B_1(\lambda)[1 \mp A_6(\lambda)B_2(\lambda)]\rho(\lambda \mid A_2) \\
&+ \int d\lambda A_6(\lambda)B_1(\lambda)[1 \pm A_2(\lambda)B_2(\lambda)]\rho(\lambda \mid A_6) + \int d\lambda A_3(\lambda)B_1(\lambda)[1 \mp A_7(\lambda)B_2(\lambda)]\rho(\lambda \mid A_3) \\
&+ \int d\lambda A_7(\lambda)B_1(\lambda)[1 \pm A_3(\lambda)B_2(\lambda)]\rho(\lambda \mid A_7) + \int d\lambda A_4(\lambda)B_1(\lambda)[1 \mp A_8(\lambda)B_2(\lambda)]\rho(\lambda \mid A_4) \\
&+ \int d\lambda A_8(\lambda)B_1(\lambda)[1 \pm A_4(\lambda)B_2(\lambda)]\rho(\lambda \mid A_8) + \int d\lambda A_5(\lambda)B_3(\lambda)[1 \mp A_6(\lambda)B_4(\lambda)]\rho(\lambda \mid A_5) \\
&+ \int d\lambda A_6(\lambda)B_3(\lambda)[1 \pm A_5(\lambda)B_4(\lambda)]\rho(\lambda \mid A_6) - \int d\lambda A_4(\lambda)B_3(\lambda)[1 \mp A_7(\lambda)B_4(\lambda)]\rho(\lambda \mid A_4) \\
&- \int d\lambda A_7(\lambda)B_3(\lambda)[1 \pm A_4(\lambda)B_4(\lambda)]\rho(\lambda \mid A_7) - \int d\lambda A_8(\lambda)B_3(\lambda)[1 \mp A_3(\lambda)B_4(\lambda)]\rho(\lambda \mid A_8) \\
&- \int d\lambda A_3(\lambda)B_3(\lambda)[1 \pm A_8(\lambda)B_4(\lambda)]\rho(\lambda \mid A_3) \qquad \text{(A.7)}
\end{aligned}
$$

Taking the modulus on both sides and using the triangle inequality we obtain,

$$
\begin{aligned}
&|\langle A_1B_1\rangle + \langle A_5B_1\rangle + \langle A_1B_3\rangle + \langle A_2B_3\rangle + \langle A_2B_1\rangle + \langle A_6B_1\rangle + \langle A_3B_1\rangle + \langle A_7B_1\rangle + \langle A_4B_1\rangle \\
&+ \langle A_8B_1\rangle + \langle A_5B_3\rangle + \langle A_6B_3\rangle - \langle A_4B_3\rangle - \langle A_7B_3\rangle - \langle A_8B_3\rangle - \langle A_3B_3\rangle| \\
&\leq 8 \pm [\int d\lambda A_1(\lambda)B_2(\lambda)\rho(\lambda \mid A_1) - \int d\lambda A_5(\lambda)B_2(\lambda)\rho(\lambda \mid A_5) + \int d\lambda A_1(\lambda)B_4(\lambda)\rho(\lambda \mid A_1) \\
&- \int d\lambda A_2(\lambda)B_4(\lambda)\rho(\lambda \mid A_2) + \int d\lambda A_2(\lambda)B_2(\lambda)\rho(\lambda \mid A_2) - \int d\lambda A_6(\lambda)B_2(\lambda)\rho(\lambda \mid A_6) \\
&+ \int d\lambda A_3(\lambda)B_2(\lambda)\rho(\lambda \mid A_3) - \int d\lambda A_7(\lambda)B_2(\lambda)\rho(\lambda \mid A_7) + \int d\lambda A_4(\lambda)B_2(\lambda)\rho(\lambda \mid A_4) \\
&- \int d\lambda A_8(\lambda)B_2(\lambda)\rho(\lambda \mid A_8) + \int d\lambda A_5(\lambda)B_4(\lambda)\rho(\lambda \mid A_5) - \int d\lambda A_6(\lambda)B_4(\lambda)\rho(\lambda \mid A_6) \\
&+ \int d\lambda A_7(\lambda)B_4(\lambda)\rho(\lambda \mid A_4) - \int d\lambda A_4(\lambda)B_4(\lambda)\rho(\lambda \mid A_7) + \int d\lambda A_3(\lambda)B_4(\lambda)\rho(\lambda \mid A_8) \\
&- \int d\lambda A_8(\lambda)B_4(\lambda)\rho(\lambda \mid A_3)]. \qquad \text{(A.8)}
\end{aligned}
$$

Invoking NIM, we have,

$$
\begin{aligned}
&|\langle A_1B_1\rangle + \langle A_5B_1\rangle + \langle A_1B_3\rangle + \langle A_2B_3\rangle + \langle A_2B_1\rangle + \langle A_6B_1\rangle + \langle A_3B_1\rangle + \langle A_7B_1\rangle \\
&+ \langle A_4B_1\rangle + \langle A_8B_1\rangle + \langle A_5B_3\rangle + \langle A_6B_3\rangle - \langle A_4B_3\rangle - \langle A_7B_3\rangle - \langle A_8B_3\rangle - \langle A_3B_3\rangle| \\
&\mp [\langle A_1B_2\rangle - \langle A_5B_2\rangle + \langle A_1B_4\rangle - \langle A_2B_4\rangle + \langle A_2B_2\rangle - \langle A_6B_2\rangle + \langle A_3B_2\rangle \\
&- \langle A_7B_2\rangle + \langle A_4B_2\rangle - \langle A_8B_2\rangle + \langle A_5B_4\rangle - \langle A_6B_4\rangle - \langle A_4B_4\rangle + \langle A_7B_4\rangle \\
&- \langle A_8B_4\rangle + \langle A_3B_4\rangle] \leq 8.
\end{aligned}
$$

or,

$$\mathcal{K}_{4\mapsto 1} \leq 8. \tag{A.9}$$

A.4 Ontic model of $n \mapsto 1$ RAC

Here Alice has 2^{n-1} preparations which are the eigenstates corresponding to $\{A_1, A_2, ..., A_{2^{n-1}}\}$ and Bob has n measurements, $\{B_1, B_2, B_3, ..., B_n\}$. Following Eq.(3.37) the term $\mathcal{K}_{n\mapsto 1}$ can be explicitly written as,

$$\begin{aligned}
&\mathcal{K}_{n\mapsto 1} = \langle A_1B_1\rangle + \langle A_1B_2\rangle + \langle A_1B_3\rangle + \langle A_1B_4\rangle + \cdots + \langle A_1B_n\rangle + \langle A_2B_1\rangle + \langle A_2B_2\rangle + \\
&\langle A_2B_3\rangle + \langle A_2B_4\rangle - \langle A_2B_n\rangle + \langle A_3B_1\rangle + \langle A_3B_2\rangle + \langle A_3B_3\rangle + \langle A_3B_4\rangle + \langle A_3B_n\rangle + \cdots + \\
&\langle A_{2^{n-1}-1}B_1\rangle - \langle A_{2^{n-1}-1}B_2\rangle - \langle A_{2^{n-1}-1}B_3\rangle - \cdots + \langle A_{2^{n-1}-1}B_n\rangle + \langle A_{2^{n-1}}B_1\rangle - \langle A_{2^{n-1}}B_2\rangle \\
&- \langle A_{2^{n-1}}B_3\rangle - \cdots - \langle A_{2^{n-1}}B_{n-3}\rangle - \langle A_{2^{n-1}}B_{n-1}\rangle - \langle A_{2^{n-1}}B_n\rangle.
\end{aligned} \tag{A.10}$$

Now, we can obtain the classical bound for $n \mapsto 1$ RAC if we adopt a similar procedure as presented for deriving the classical bound corresponding to $2 \mapsto 1$ RAC. Let us now derive the classical bound explicitly when n is even.

$$\begin{aligned}
&\langle A_1B_1\rangle + \langle A_1B_3\rangle + \cdots + \langle A_2B_1\rangle + \langle A_2B_3\rangle + \cdots + \langle A_3B_1\rangle + \langle A_3B_3\rangle + \cdots + \langle A_{2^{n-1}-1}B_1\rangle \\
&- \langle A_{2^{n-1}-1}B_3\rangle - \cdots + \langle A_{2^{n-1}}B_1\rangle - \langle A_{2^{n-1}}B_3\rangle - \cdots - \langle A_{2^{n-1}}B_{n-3}\rangle - \langle A_{2^{n-1}}B_{n-1}\rangle \\
&= \int d\lambda [A_1(\lambda)B_1(\lambda)\rho(\lambda \mid A_1) + A_1(\lambda)B_3(\lambda)\rho(\lambda \mid A_1) + \cdots + A_2(\lambda)B_1(\lambda)\rho(\lambda \mid A_2) \\
&+ A_2(\lambda)B_3(\lambda)\rho(\lambda \mid A_2) + \cdots + A_3(\lambda)B_1(\lambda)\rho(\lambda \mid A_3) + A_3(\lambda)B_3(\lambda)\rho(\lambda \mid A_3) \\
&+ \cdots + A_{2^{n-1}-1}(\lambda)B_1(\lambda)\rho(\lambda \mid A_{2^{n-1}-1}) - A_{2^{n-1}-1}(\lambda)B_3(\lambda)\rho(\lambda \mid A_{2^{n-1}-1}) - \cdots + \\
&A_{2^{n-1}}(\lambda)B_1(\lambda)\rho(\lambda \mid A_{2^{n-1}}) - A_{2^{n-1}}(\lambda)B_3(\lambda)\rho(\lambda \mid A_{2^{n-1}}) - \cdots - A_{2^{n-1}}(\lambda)B_{n-3}(\lambda)\rho(\lambda \mid A_{2^{n-1}}) \\
&- A_{2^{n-1}}(\lambda)B_{n-1}(\lambda)\rho(\lambda \mid A_{2^{n-1}})] \\
&= \int d\lambda A_1(\lambda)B_1(\lambda)[1 \mp A_{2^{n-1}}(\lambda)B_2(\lambda)]\rho(\lambda \mid A_{2^{n-1}}) \\
&+ \int d\lambda A_2(\lambda)B_1(\lambda)[1 \mp A_{2^{n-1}-1}(\lambda)B_2(\lambda)]\rho(\lambda \mid A_{2^{n-1}-1}) \\
&+ \int d\lambda A_1(\lambda)B_{n-1}(\lambda)[1 \mp A_2(\lambda)B_n(\lambda)]\rho(\lambda \mid A_1) + \int d\lambda A_2(\lambda)B_{n-1}(\lambda)[1 \pm A_1(\lambda)B_n(\lambda)]\rho(\lambda \mid A_2) \\
&+ \cdots + \int d\lambda A_{2^{n-1}-1}(\lambda)B_1(\lambda)[1 \pm A_2(\lambda)B_2(\lambda)]\rho(\lambda \mid A_{2^{n-1}-1}) \\
&+ \int d\lambda A_{2^{n-1}}(\lambda)B_1(\lambda)[1 \pm A_1(\lambda)B_2(\lambda)]\rho(\lambda \mid A_{2^{n-1}}) + \ldots \\
&- \int d\lambda A_{2^{n-1}-1}(\lambda)B_{n-1}(\lambda)[1 \mp A_{2^{n-1}}(\lambda)B_n(\lambda)]\rho(\lambda \mid A_{2^{n-1}-1})
\end{aligned}$$

$$- \int d\lambda A_{2^{n-1}}(\lambda) B_{n-1}(\lambda)[1 \pm A_{2^{n-1}-1}(\lambda) B_n(\lambda)] \rho(\lambda \mid A_{2^{n-1}}) \tag{A.11}$$

Taking the modulus on both sides and using the triangle inequality we obtain,

$$\begin{aligned}
&|\langle A_1 B_1 \rangle + \langle A_1 B_3 \rangle + \cdots + \langle A_2 B_1 \rangle + \langle A_2 B_3 \rangle + \cdots + \langle A_3 B_1 \rangle + \langle A_3 B_3 \rangle + \cdots + \langle A_{2^{n-1}-1} B_1 \rangle \\
&- \langle A_{2^{n-1}-1} B_3 \rangle - \cdots + \langle A_{2^{n-1}} B_1 \rangle - \langle A_{2^{n-1}} B_3 \rangle - \cdots - \langle A_{2^{n-1}} B_{n-3} \rangle - \langle A_{2^{n-1}} B_{n-1} \rangle| \leq 2^{n-1} \\
&\pm [\int d\lambda A_1(\lambda) B_2(\lambda) \rho(\lambda \mid A_1) + \int d\lambda A_2(\lambda) B_2(\lambda) \rho(\lambda \mid A_2) + \cdots + \int d\lambda A_1(\lambda) B_n(\lambda) \rho(\lambda \mid A_1) \\
&- \int d\lambda A_2(\lambda) B_n(\lambda) \rho(\lambda \mid A_2) + \cdots - \int d\lambda A_{2^{n-1}-1}(\lambda) B_2(\lambda) \rho(\lambda \mid A_{2^{n-1}-1}) \\
&- \int d\lambda A_{2^{n-1}}(\lambda) B_2(\lambda) \rho(\lambda \mid A_{2^{n-1}}) - \cdots - \int d\lambda A_{2^{n-1}-1}(\lambda) B_n(\lambda) \rho(\lambda \mid A_{2^{n-1}-1}) \\
&- \int d\lambda A_{2^{n-1}}(\lambda) B_n(\lambda) \rho(\lambda \mid A_{2^{n-1}})].
\end{aligned} \tag{A.12}$$

Invoking NIM, we have,

$$\begin{aligned}
&|\langle A_1 B_1 \rangle + \langle A_1 B_3 \rangle + \cdots + \langle A_2 B_1 \rangle + \langle A_2 B_3 \rangle + \cdots + \langle A_3 B_1 \rangle + \langle A_3 B_3 \rangle + \cdots + \langle A_{2^{n-1}-1} B_1 \rangle \\
&- \langle A_{2^{n-1}-1} B_3 \rangle - \cdots + \langle A_{2^{n-1}} B_1 \rangle - \langle A_{2^{n-1}} B_3 \rangle - \langle A_{2^{n-1}} B_{n-3} \rangle - \langle A_{2^{n-1}} B_{n-1} \rangle| \\
&\mp [\langle A_1 B_2 \rangle + \langle A_1 B_4 \rangle + \cdots + \langle A_1 B_n \rangle - \langle A_2 B_2 \rangle + \langle A_2 B_4 \rangle + \cdots - \langle A_2 B_n \rangle + \langle A_3 B_2 \rangle \\
&+ \langle A_3 B_4 \rangle + \cdots + \langle A_3 B_n \rangle + \cdots - \langle A_{2^{n-1}-1} B_2 \rangle - \cdots + \langle A_{2^{n-1}-1} B_n \rangle - \langle A_{2^{n-1}} B_2 \rangle \\
&- \cdots - \langle A_{2^{n-1}} B_n \rangle] \leq 2^{n-1}.
\end{aligned}$$

or,

$$\mathcal{K}_{n \mapsto 1} \leq 2^{n-1}. \tag{A.13}$$

Similarly, one can also obtain the same classical bound for $\mathcal{K}_{n \mapsto 1}$ when n is odd.

APPENDIX $\mathcal{B}$

DERIVATION OF MINIMUM SECURE KEY RATE IN DI-QKD

• **General rank-2 state:**

The matrix form of general rank-2 state (4.21) is as follows:

$$\rho_2^2 = \begin{pmatrix} \alpha^2\left(p_1\left(a^2-b^2\right)+b^2\right) & a\alpha^2 b\left(2p_1-1\right) & \alpha\beta\left(ap_1a'-b\left(p_1-1\right)b'\right) & \alpha\beta\left(b\left(p_1-1\right)a'+ap_1b'\right) \\ a\alpha^2 b\left(2p_1-1\right) & \alpha^2\left(p_1\left(b^2-a^2\right)+a^2\right) & \alpha\beta\left(p_1\left(ba'+ab'\right)-ab'\right) & \alpha\beta\left(\left(a-ap_1\right)a'+bp_1b'\right) \\ \alpha\beta\left(ap_1a'-b\left(p_1-1\right)b'\right) & \alpha\beta\left(p_1\left(ba'+ab'\right)-ab'\right) & \beta^2\left(p_1\left(\left(a'\right)^2-\left(b'\right)^2\right)+\left(b'\right)^2\right) & \beta^2\left(2p_1-1\right)a'b' \\ \alpha\beta\left(b\left(p_1-1\right)a'+ap_1b'\right) & \alpha\beta\left(\left(a-ap_1\right)a'+bp_1b'\right) & \beta^2\left(2p_1-1\right)a'b' & \beta^2\left(p_1\left(b'\right)^2-\left(p_1-1\right)\left(a'\right)^2\right) \end{pmatrix} \tag{B.1}$$

Next, we compute the eigenvalues of the correlation matrix (T) of the general rank-2 state. The

matrix elements of the correlation matrix are $t_{ij} = \mathrm{Tr}[(\sigma_i \otimes \sigma_j).\rho_2^2]$. The correlation matrix is:

$$\begin{pmatrix} 2\alpha\beta\,(2p_1-1)\,(ba'+ab') & 0 & 2\alpha\beta\,(2p_1-1)\,(aa'-bb') \\ 0 & 2\alpha\beta\,(ba'-ab') & 0 \\ 2\,(2p_1-1)\,(a\alpha^2 b-\beta^2 a'b') & 0 & (2p_1-1)\left(\alpha^2\left(a^2-b^2\right)-\beta^2\left(a'\right)^2+\beta^2\left(b'\right)^2\right) \end{pmatrix} \tag{B.2}$$

The eigenvalues of the correlation matrix (B.2) are:

$$\begin{aligned} \lambda_1 &= y \\ \lambda_2 &= \frac{1}{2}(1-2p_1)\Big[\alpha^2(b^2-a^2)+\beta^2(a'^2-b'^2)-y' \\ &\quad +\sqrt{(2ab\alpha^2-y+\beta^2(1-2a'b')-z)(\beta^2(1+2a'b')-2ab\alpha^2-y+z)}\Big] \\ \lambda_3 &= \frac{1}{2}(1-2p_1)\Big[\alpha^2(b^2-a^2)+\beta^2(a'^2-b'^2)-y' \\ &\quad -\sqrt{(2ab\alpha^2-y+\beta^2(1-2a'b')-z)(\beta^2(1+2a'b')-2ab\alpha^2-y+z)}\Big] \end{aligned} \tag{B.3}$$

where, $y = 2\alpha\beta(ab'-a'b)$, $y' = 2\alpha\beta(a'b+ab')$ and $z = 2\alpha\beta(a'a-bb')$. We determine the quantum bit error rate (QBER) in DI-QKD using Eq.(4.7) for the case $(ab' = a'b)$.

$$\begin{aligned} QBER &= \frac{1}{4}(2-|\lambda_2|-|\lambda_3|) \\ &= \frac{1}{4}\Big[2-|(1-2p_1)(\alpha^2(b^2-a^2)+\beta^2(a'^2-b'^2)-y')|\Big] \end{aligned} \tag{B.4}$$

The $r_{\mathrm{Smin}}(\rho_2^2)$ under optimal symmetric collective attacks(OSCA), is calculated using Eq.(4.14)

$$\begin{aligned} r_{\mathrm{Smin}}(\rho_2^2(p_1,a,a',\alpha)) = \frac{1}{2\log(2)}\Big[&\left((1-2p_1)\left(\alpha^2\left(b^2-a^2\right)+\beta^2\left(\left(a'\right)^2-\left(b'\right)^2\right)-y'\right)+2\right) \\ &\log\left(\frac{1}{4}\left((1-2p_1)\left(\alpha^2\left(b^2-a^2\right)+\beta^2\left(\left(a'\right)^2-\left(b'\right)^2\right)-y'\right)+2\right)\right) \\ &+\left(2-(1-2p_1)\left(\alpha^2\left(b^2-a^2\right)+\beta^2\left(\left(a'\right)^2-\left(b'\right)^2\right)-y'\right)\right) \\ &\log\left(\frac{1}{4}\left(2-(1-2p_1)\left(\alpha^2\left(b^2-a^2\right)+\beta^2\left(\left(a'\right)^2-\left(b'\right)^2\right)-y'\right)\right)\right)+\log(4)\Big] \end{aligned} \tag{B.5}$$

Substituting p_1 in terms of N using Eq.(4.24) for the case $(ab' = a'b)$, we get

$$\begin{aligned} r_{Smin}(\rho_2^2) =& \frac{1}{2\log 2}\Bigg[\log 4+\log\left(\frac{1}{4}(2-(1-2N)((b^2-a^2)\alpha^2-4b\alpha\beta a'+\beta^2(a'^2-b'^2)))\right) \\ & (2-(1-2N)((b^2-a^2)\alpha^2-4b\alpha\beta a'+\beta^2(a'^2-b'^2))) \end{aligned}$$

$$+\log\left(\frac{1}{4}(2+(1-2N)((b^2-a^2)\alpha^2-4b\alpha\beta a'+\beta^2(a'^2-b'^2)))\right)$$
$$(2+(1-2N)((b^2-a^2)\alpha^2-4b\alpha\beta a'+\beta^2(a'^2-b'^2)))\Bigg] \tag{B.6}$$

Similarly for the case of collective attacks(CA), using Eq.(4.7) and Eq.(4.13) we obtain the $r_{\text{Cmin}}(\rho_p)$ in terms of negativity N,

$$r_{\text{Cmin}(\rho_2^2)} = \frac{1}{\log 16}\Bigg[-2\log 16+(2-\Omega)\log(2-\Omega)+(2+\Omega)\log(2+\Omega)$$
$$+2(1+\sqrt{\Delta-1})\log(1+\sqrt{\Delta-1})+2(1-\sqrt{\Delta-1})\log(1-\sqrt{\Delta-1})\Bigg] \tag{B.7}$$

Where, $\Omega = (1-2N)((b^2-a^2)\alpha^2-4b\alpha\beta a'+\beta^2(a'^2-b'^2))$,
$\Delta = 2(1-2N)^2\Big((2ab\alpha^2+\beta^2+2\alpha\beta bb'-2a'(a\alpha\beta+\beta^2b'))(-2ab\alpha^2+\beta^2-2bb'\alpha\beta+2a'(a\alpha\beta+b'\beta^2))+((b^2-a^2)\alpha^2+((a')^2-(b')^2)^2\beta^2)\Big)$.

We vary the state parameters in the step size of 0.01 to numerically determine the minimum secure key rate as function of the negativity (N).

• **General pure state:**

The matrix form of a general pure state (4.20) is as follows:

$$\rho_p = \begin{pmatrix} \cos^2\frac{\theta}{2} & 0 & 0 & \frac{\sin\theta}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{\sin\theta}{2} & 0 & 0 & \sin^2\frac{\theta}{2} \end{pmatrix} \tag{B.8}$$

The correlation matrix $t_{ij} = \text{Tr}[(\sigma_i \otimes \sigma_j).\rho_p]$ is:

$$\begin{pmatrix} \sin\theta & 0 & 0 \\ 0 & -\sin\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{B.9}$$

We obtain $r_{\text{Smin}}(\rho_p)$ under optimal symmetric collective attacks(OSCA), for the pure state using Eq.(4.7) and Eq.(4.14) in terms of negativity N,

$$r_{\text{Smin}(\rho_p)} = \frac{-\log 64+(1-2N)\log(1-2N)+(3+2N)\log(3+2N)}{\log 4} \tag{B.10}$$

For the case of collective attacks(CA), using Eq.(4.7) and Eq.(4.13) we obtain the $r_{\text{Cmin}}(\rho_p)$

in terms of negativity N,

$$r_{\mathrm{Cmin}(\rho_p)} = \frac{1}{\log 16}\Big[-8\log 2 + (3+2N)\log(3+2N) + (3-6N)\log(1-2N) + (2+4N)\log(1+2N)\Big] \tag{B.11}$$

• **Werner state:**

The matrix form of the Werner state (4.26) is as follows:

$$\rho_w = \begin{pmatrix} \frac{1+p}{4} & 0 & 0 & \frac{p}{2} \\ 0 & \frac{1-p}{4} & 0 & 0 \\ 0 & 0 & \frac{1-p}{4} & 0 \\ \frac{p}{2} & 0 & 0 & \frac{1+p}{4} \end{pmatrix} \tag{B.12}$$

For the Werner state, the correlation matrix are $t_{ij} = \mathrm{Tr}[(\sigma_i \otimes \sigma_j).\rho_w]$ is:

$$\begin{pmatrix} p & 0 & 0 \\ 0 & -p & 0 \\ 0 & 0 & p \end{pmatrix} \tag{B.13}$$

We obtain $r_{\mathrm{Smin}}(\rho_w)$ under optimal symmetric collective attacks(OSCA), for the Werner state using Eq.(4.7) and Eq.(4.14) in terms of negativity N,

$$r_{\mathrm{Smin}(\rho_w)} = \frac{\log 8 + (2-4N)\log(\frac{1-2N}{3}) + 4(1+N)\log(\frac{2(1+N)}{3})}{\log 8} \tag{B.14}$$

Using Eq.(4.7) and Eq.(4.13) we obtain the $r_{\mathrm{Cmin}}(\rho_w)$ under collective attacks(CA), in terms of negativity N,

$$r_{\mathrm{Cmin}(\rho_w)} = \frac{1}{6\log 2}\Big[-12\log 3 + 2(1-2N)\log(1-2N) + (4+4N)\log(2+2N) + (3-\delta)\log(3-\delta) + (3+\delta)\log(3+\delta)\Big] \tag{B.15}$$

Where, $\delta = \sqrt{-7+16N+32N^2}$.

APPENDIX C

HYBRID ENTANGLED STATE AFTER PASSING THROUGH LOSS-ONLY CHANNEL

We consider a hybrid entangled (HE)-state in modes a and b given as [251]

$$|\Psi_{ab}\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_a |\alpha\rangle_b + |V\rangle_a |-\alpha\rangle_b\right). \tag{C.1}$$

Here, the single-photon-polarization-state $|H\rangle$ ($|V\rangle$) represents the discrete-variable (DV) part and the coherent state $|\alpha\rangle$ ($|-\alpha\rangle$) forms the continuous-variable (CV) part. Let us now consider that only the CV part passes through the loss-only channel that can be modelled as mixing the signal with an ancilla vacuum through a BS with transmittance T, and then tracing out the ancilla. Considering the action of such a BS on an incoming coherent state, $U_{\rm bs}(T) : |\alpha, 0\rangle \rightarrow \left|\sqrt{T}\alpha, \sqrt{1-T}\alpha\right\rangle$, the HE-state after passing through the channel becomes

$$\rho_{ab}^{\rm ch,cv} = {\rm Tr}_c\left[U_{\rm bs}^{bc}(T)\left(\rho_{ab}\otimes|0\rangle_c\langle 0|\right)\left(U_{\rm bs}^{bc}(T)\right)^\dagger\right]$$

$$= \frac{1}{2}\Big[\rho_a^{HH} \otimes \Big|\sqrt{T}\alpha\Big\rangle_b \Big\langle\sqrt{T}\alpha\Big| + \rho_a^{VV} \otimes \Big|-\sqrt{T}\alpha\Big\rangle_b \Big\langle-\sqrt{T}\alpha\Big| \\ + e^{-2(1-T)\alpha^2}\left(\rho_a^{HV} \otimes \Big|\sqrt{T}\alpha\Big\rangle_b \Big\langle-\sqrt{T}\alpha\Big| + \rho_a^{VH} \otimes \Big|-\sqrt{T}\alpha\Big\rangle_b \Big\langle\sqrt{T}\alpha\Big|\right)\Big], \tag{C.2}$$

where, $\rho^{x,y} = |x\rangle\langle y|$ $(x, y = H, V)$.

APPENDIX $\mathcal{D}$

OBTAINING THE SHARED DV-STATE AFTER NOISY TRANSMISSION FOLLOWED BY ON-OFF MEASUREMENT AT CHARLIE'S LAB

D.1 4-mode state transmission through noisy channel and mixing

Let us consider that both Alice and Bob prepare their individual HE-states in modes $\{a_1, a_2\}$ and $\{b_1, b_2\}$, respectively.

$$\rho_{a_1a_2} = |\Psi_{a_1a_2}\rangle \langle\Psi_{a_1a_2}|, \quad \text{and} \quad \rho_{b_1b_2} = |\Psi_{b_1b_2}\rangle \langle\Psi_{b_1b_2}|. \tag{D.1}$$

For the sake of convenience we use a compact notation for the DV and the CV parts as $\rho^{xy,uv} = \rho^{xy}_{a_1} \otimes \rho^{uv}_{b_1}$ $(x, y, u, v = H, V)$ and $|\alpha, \beta\rangle = |\alpha\rangle_{a_2} |\beta\rangle_{b_2}$ $(\alpha, \beta \in \mathcal{C}^2)$.

After Alice and Bob send their coherent states through the loss-only channel to Charlie, the 4-mode state is given by

$$
\begin{aligned}
\rho_{\text{charlie}} &= \rho^{\text{ch}}_{a_1 a_2} \otimes \rho^{\text{ch}}_{b_1 b_2} \\
&= \frac{1}{4}\Big(\Big\{\Big[\rho^{HH,HH} \otimes \Big|\sqrt{T}\alpha, \sqrt{T}\alpha\Big\rangle\Big\langle\sqrt{T}\alpha, \sqrt{T}\alpha\Big| + \rho^{HH,VV} \otimes \Big|\sqrt{T}\alpha, -\sqrt{T}\alpha\Big\rangle\Big\langle\sqrt{T}\alpha, -\sqrt{T}\alpha\Big|\Big] \\
&\quad + e^{-2(1-T)\alpha^2}\Big[\rho^{HH,HV} \otimes \Big|\sqrt{T}\alpha, \sqrt{T}\alpha\Big\rangle\Big\langle\sqrt{T}\alpha, -\sqrt{T}\alpha\Big| + \rho^{HH,VH} \otimes \Big|\sqrt{T}\alpha, -\sqrt{T}\alpha\Big\rangle\Big\langle\sqrt{T}\alpha, \sqrt{T}\alpha\Big|\Big]\Big\} \\
&\quad + \Big\{\Big[\rho^{VV,HH} \otimes \Big|-\sqrt{T}\alpha, \sqrt{T}\alpha\Big\rangle\Big\langle-\sqrt{T}\alpha, \sqrt{T}\alpha\Big| + \rho^{VV,VV} \otimes \Big|-\sqrt{T}\alpha, -\sqrt{T}\alpha\Big\rangle\Big\langle-\sqrt{T}\alpha, -\sqrt{T}\alpha\Big|\Big] \\
&\quad + e^{-2(1-T)\alpha^2}\Big[\rho^{VV,HV} \otimes \Big|-\sqrt{T}\alpha, \sqrt{T}\alpha\Big\rangle\Big\langle-\sqrt{T}\alpha, -\sqrt{T}\alpha\Big| + \rho^{VV,VH} \otimes \Big|-\sqrt{T}\alpha, -\sqrt{T}\alpha\Big\rangle\Big\langle-\sqrt{T}\alpha, \sqrt{T}\alpha\Big|\Big]\Big\} \\
&\quad + e^{-2(1-T)\alpha^2}\Big\{\Big[\rho^{HV,HH} \otimes \Big|\sqrt{T}\alpha, \sqrt{T}\alpha\Big\rangle\Big\langle-\sqrt{T}\alpha, \sqrt{T}\alpha\Big| + \rho^{HV,VV} \otimes \Big|\sqrt{T}\alpha, -\sqrt{T}\alpha\Big\rangle\Big\langle-\sqrt{T}\alpha, -\sqrt{T}\alpha\Big|\Big] \\
&\quad + e^{-2(1-T)\alpha^2}\Big[\rho^{HV,HV} \otimes \Big|\sqrt{T}\alpha, \sqrt{T}\alpha\Big\rangle\Big\langle-\sqrt{T}\alpha, -\sqrt{T}\alpha\Big| + \rho^{HV,VH} \otimes \Big|\sqrt{T}\alpha, -\sqrt{T}\alpha\Big\rangle\Big\langle-\sqrt{T}\alpha, \sqrt{T}\alpha\Big|\Big]\Big\} \\
&\quad + e^{-2(1-T)\alpha^2}\Big\{\Big[\rho^{VH,HH} \otimes \Big|-\sqrt{T}\alpha, \sqrt{T}\alpha\Big\rangle\Big\langle\sqrt{T}\alpha, \sqrt{T}\alpha\Big| + \rho^{VH,VV} \otimes \Big|-\sqrt{T}\alpha, -\sqrt{T}\alpha\Big\rangle\Big\langle\sqrt{T}\alpha, -\sqrt{T}\alpha\Big|\Big] \\
&\quad + e^{-2(1-T)\alpha^2}\Big[\rho^{VH,HV} \otimes \Big|-\sqrt{T}\alpha, \sqrt{T}\alpha\Big\rangle\Big\langle\sqrt{T}\alpha, -\sqrt{T}\alpha\Big| + \rho^{VH,VH} \otimes \Big|-\sqrt{T}\alpha, -\sqrt{T}\alpha\Big\rangle\Big\langle\sqrt{T}\alpha, \sqrt{T}\alpha\Big|\Big]\Big\}\Big).
\end{aligned}
\tag{D.2}
$$

Upon mixing at the 50 : 50 BS ($T = 1/2$) by Charlie, the state becomes

$$
\begin{aligned}
\rho^{\text{mix}}_{\text{charlie}} &= U^{a_2 b_2}_{\text{bs}}(1/2)\rho_{\text{charlie}}\Big[U^{a_2 b_2}_{\text{bs}}(1/2)\Big]^{\dagger} \\
&= \frac{1}{4}\Big(\Big\{\Big[\rho^{HH,HH} \otimes \Big|\sqrt{2T}\alpha, 0\Big\rangle\Big\langle\sqrt{2T}\alpha, 0\Big| + \rho^{HH,VV} \otimes \Big|0, -\sqrt{2T}\alpha\Big\rangle\Big\langle0, -\sqrt{2T}\alpha\Big|\Big] \\
&\quad + e^{-2(1-T)\alpha^2}\Big[\rho^{HH,HV} \otimes \Big|\sqrt{2T}\alpha, 0\Big\rangle\Big\langle0, \sqrt{2T}\alpha\Big| + \rho^{HH,VH} \otimes \Big|0, \sqrt{2T}\alpha\Big\rangle\Big\langle\sqrt{2T}\alpha, 0\Big|\Big]\Big\} \\
&\quad + \Big\{\Big[\rho^{VV,HH} \otimes \Big|0, -\sqrt{2T}\alpha\Big\rangle\Big\langle0, -\sqrt{2T}\alpha\Big| + \rho^{VV,VV} \otimes \Big|-\sqrt{2T}\alpha, 0\Big\rangle\Big\langle-\sqrt{2T}\alpha, 0\Big|\Big] \\
&\quad + e^{-2(1-T)\alpha^2}\Big[\rho^{VV,HV} \otimes \Big|0, -\sqrt{2T}\alpha\Big\rangle\Big\langle-\sqrt{2T}\alpha, 0\Big| + \rho^{VV,VH} \otimes \Big|-\sqrt{2T}\alpha, 0\Big\rangle\Big\langle0, -\sqrt{2T}\alpha\Big|\Big]\Big\} \\
&\quad + e^{-2(1-T)\alpha^2}\Big\{\Big[\rho^{HV,HH} \otimes \Big|\sqrt{2T}\alpha, 0\Big\rangle\Big\langle0, -\sqrt{2T}\alpha\Big| + \rho^{HV,VV} \otimes \Big|0, -\sqrt{2T}\alpha\Big\rangle\Big\langle-\sqrt{2T}\alpha, 0\Big|\Big] \\
&\quad + e^{-2(1-T)\alpha^2}\Big[\rho^{HV,HV} \otimes \Big|\sqrt{2T}\alpha, 0\Big\rangle\Big\langle-\sqrt{2T}\alpha, 0\Big| + \rho^{HV,VH} \otimes \Big|0, \sqrt{2T}\alpha\Big\rangle\Big\langle0, -\sqrt{2T}\alpha\Big|\Big]\Big\} \\
&\quad + e^{-2(1-T)\alpha^2}\Big\{\Big[\rho^{VH,HH} \otimes \Big|0, -\sqrt{2T}\alpha\Big\rangle\Big\langle\sqrt{2T}\alpha, 0\Big| + \rho^{VH,VV} \otimes \Big|-\sqrt{2T}\alpha, 0\Big\rangle\Big\langle0, \sqrt{2T}\alpha\Big|\Big] \\
&\quad + e^{-2(1-T)\alpha^2}\Big[\rho^{VH,HV} \otimes \Big|0, -\sqrt{2T}\alpha\Big\rangle\Big\langle0, \sqrt{2T}\alpha\Big| + \rho^{VH,VH} \otimes \Big|-\sqrt{2T}\alpha, 0\Big\rangle\Big\langle\sqrt{2T}\alpha, 0\Big|\Big]\Big\}\Big).
\end{aligned}
\tag{D.3}
$$

D.2 Post-measurement shared DV-state

After mixing the incoming signal Charlie checks whether the single-photon-detector (SPD) clicks. An inefficient SPD is described the set of operators $\{\Pi_1, \Pi_{\neg 1} = \mathbf{I} - \Pi_1\}$ such that [248]

$$\Pi_m = \eta_0^m \sum_k {}^{k+m}C_m (1-\eta_0)^k \left|k+m\right\rangle \left\langle k+m\right| \tag{D.4}$$

represents the noisy m-photon detection, where η_0 is the efficiency of the SPD and $|k\rangle$ represents the k-photon-number state. ${}^{k+m}C_m = \frac{(k+m)!}{k!m!}$ represents the binomial coefficient. Charlie's measurement is described by the operator $\mathcal{M}_{a_2 b_2} = \Pi_{1,\neg 1}$, such that $\Pi_{\alpha,\beta} = \Pi_\alpha \otimes \Pi_\beta$ $(\alpha, \beta = 1, \neg 1)$ where the first and the second operator operates on modes a_2 and b_2, respectively.

The shared DV-state between Alice and Bob, after Charlie's measurement, becomes $\rho_{a_1 b_1} = \frac{1}{P_{\rm dv}} \rho^{1,\neg 1}_{a_1 b_1}$ where $P_{\rm dv} = {\rm Tr}_{a_1 b_1}\left(\rho^{1,\neg 1}_{a_1 b_1}\right)$ is the probability of obtaining the state $\rho_{a_1 b_1}$ and $\rho^{1,\neg 1}_{a_1 b_1} = {\rm Tr}_{a_2 b_2}\left(\Pi_{1,\neg 1} \rho^{\rm mix}_{\rm charlie}\right)$. Now, applying the following results

$$\begin{aligned}
{\rm Tr}\left(\Pi_1 \left|\alpha\right\rangle \left\langle\beta\right|\right) &= \eta_0 \sum_k {}^{k+1}C_1 (1-\eta_0)^k \left\langle\beta|k+1\right\rangle \left\langle k+1|\alpha\right\rangle \\
&= \eta_0 e^{-\frac{\alpha^2+\beta^2}{2}} \alpha\beta \sum_k \frac{\left[\beta\alpha(1-\eta_1)\right]^k}{k!} \\
&= \eta_0 \alpha\beta \left\langle\beta|\alpha\right\rangle e^{-\eta_0\beta\alpha} \\
{\rm Tr}\left(\Pi_{\neg 1} \left|\alpha\right\rangle \left\langle\beta\right|\right) &= {\rm Tr}\left[\left(\mathbf{I} - \Pi_1\right) \left|\alpha\right\rangle \left\langle\beta\right|\right] \\
&= \left\langle\beta|\alpha\right\rangle \left(1 - \eta_0\alpha\beta e^{-\eta_0\beta\alpha}\right),
\end{aligned} \tag{D.5}$$

leads to the projected DV state onto the modes a_1 and b_1 as

$$\begin{aligned}
\rho^{1,\neg 1}_{a_1 b_1} &= {\rm Tr}_{a_2 b_2}\left(\Pi_{1,\neg 1} \rho^{\rm mix}_{\rm charlie}\right) \\
&= \frac{1}{4}\Big[\rho^{HH,VV} \eta_0 (2T\alpha^2) e^{-2T\eta_0\alpha^2} + \rho^{VV,HH} \eta_0 (2T\alpha^2) e^{-2T\eta_0\alpha^2} + e^{-2(1-T)\alpha^2} e^{-2(1-T)\alpha^2} \rho^{HV,VH} \\
&\quad \times \eta_0 (-2T\alpha^2) e^{-4T\alpha^2} e^{2T\eta_0\alpha^2} + e^{-2(1-T)\alpha^2} e^{-2(1-T)\alpha^2} \rho^{VH,HV} \eta_0 (-2T\alpha^2) e^{-4T\alpha^2} e^{2T\eta_0\alpha^2}\Big] \\
&= \frac{T\eta_0\alpha^2}{2} e^{-2T\eta_0\alpha^2} \left[\left(\rho^{HH,VV} + \rho^{VV,HH}\right) - e^{-4(1-T\eta_0)\alpha^2} \left(\rho^{HV,VH} + \rho^{VH,HV}\right)\right] \\
&= \frac{T\eta_0\alpha^2}{2} e^{-2T\eta_0\alpha^2} \Big\{ \Big(\left|H,V\right\rangle \left\langle H,V\right| + \left|V,H\right\rangle \left\langle V,H\right| \Big) - e^{-4(1-T\eta_0)\alpha^2} \\
&\quad \times \Big(\left|H,V\right\rangle \left\langle V,H\right| + \left|V,H\right\rangle \left\langle H,V\right| \Big) \Big\}.
\end{aligned} \tag{D.6}$$

with probability

$$P^{1,\neg 1} = \mathrm{Tr}\left(\rho^{1,\neg 1}_{a_1 b_1}\right) = T\eta_0\alpha^2 e^{-2T\eta_0\alpha^2} (= \mathrm{Pr}) \tag{D.7}$$

Thus the final normalized shared DV state is given by

$$\begin{aligned}\rho_{a_1 b_1} &= \frac{1}{P^{1,\neg 1}}\rho^{1,\neg 1}_{a_1 b_1} \\ &= \frac{1}{2}\left[\left(|H,V\rangle\langle H,V| + |V,H\rangle\langle V,H|\right) - e^{-4(1-T\eta_0)\alpha^2}\left(|H,V\rangle\langle V,H| + |V,H\rangle\langle H,V|\right)\right].\end{aligned} \tag{D.8}$$

APPENDIX $\mathcal{E}$

BELL FUNCTION FOR THE SHARED DV-STATE BETWEEN ALICE AND BOB

The PRBOs are given as

$$\begin{aligned}\hat{O}(\eta,\theta) &= U(\eta,\theta)\Pi(\eta_0)U^{\dagger}(\eta,\theta)\\ &= \eta_0\begin{pmatrix}|H\rangle & |V\rangle\end{pmatrix}\begin{pmatrix}\sqrt{\eta} & \sqrt{1-\eta}e^{i\theta}\\ -\sqrt{1-\eta}e^{-i\theta} & \sqrt{\eta}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}\sqrt{\eta} & -\sqrt{1-\eta}e^{i\theta}\\ \sqrt{1-\eta}e^{-i\theta} & \sqrt{\eta}\end{pmatrix}\begin{pmatrix}\langle H|\\ \langle V|\end{pmatrix}\\ &= \eta_0\begin{pmatrix}|H\rangle & |V\rangle\end{pmatrix}\begin{bmatrix}N_{hh}(\eta,\theta) & -N_{hv}(\eta,\theta)\\ -N^{*}_{hv}(\eta,\theta) & N_{vv}(\eta,\theta)\end{bmatrix}\begin{pmatrix}\langle H|\\ \langle V|\end{pmatrix}, \qquad \text{(E.1)}\end{aligned}$$

where $N_{hh}(\eta,\theta) = -\eta_0(1-2\eta)$, $N_{vv}(\eta,\theta) = \eta_0(1-2\eta)$ and $N_{hv}(\eta,\theta) = 2e^{i\theta}\eta_0\sqrt{\eta(1-\eta)}$. This leads to the joint binary-outcome measurement, described by $\hat{O}_{a_1,b_1}(\eta,\theta,\zeta,\phi) = \hat{O}_{a_1}(\eta,\theta)\otimes\hat{O}_{b_1}(\zeta,\phi)$, as

$$
\begin{aligned}
\hat{O}(\eta,\theta,\zeta,\phi) &= \hat{O}(\eta,\theta)\otimes\hat{O}(\zeta,\phi)\\
&= \Big\{\Big[\{N_{hh}(\eta,\theta)\,|H\rangle\langle H| + N_{vv}(\eta,\theta)\,|V\rangle\langle V|\Big] - \Big[N_{hv}(\eta,\theta)\,|H\rangle\langle V| + N^{*}_{hv}(\eta,\theta)\,|V\rangle\langle H|\Big]\Big\}\otimes\\
&\quad\Big\{\Big[N_{hh}(\zeta,\phi)\,|H\rangle\langle H| + N_{vv}(\zeta,\phi)\,|V\rangle\langle V|\Big] - \Big[N_{hv}(\zeta,\phi)\,|H\rangle\langle V| + N^{*}_{hv}(\zeta,\phi)\,|V\rangle\langle H|\Big]\Big\}\\
&= \Big\{\Big[N_{hh}(\eta,\theta)N_{vv}(\zeta,\phi)\,|H,V\rangle\langle H,V| + N_{vv}(\eta,\theta)N_{hh}(\zeta,\phi)\,|V,H\rangle\langle V,H|\Big]\\
&\quad + \Big[N_{hv}(\eta,\theta)N^{*}_{hv}(\zeta,\phi)\,|H,V\rangle\langle V,H| + N^{*}_{hv}(\eta,\theta)N_{hv}(\zeta,\phi)\,|V,H\rangle\langle H,V|\Big]\Big\} + \mathcal{O}_{hv},
\end{aligned}
\tag{E.2}
$$

where $\mathcal{O}_{h,v}$ contains all other terms where the same polarization state occurs in either "ket" or "bra" vectors. The expectation value of the joint measurement, $\hat{O}_{a_1,b_1}(\eta,\theta,\zeta,\phi)$ is hence given by

$$
\begin{aligned}
\mathcal{E}\,(\eta,\theta,\zeta,\phi) &= \big\langle \hat{O}_{a_1,b_1}(\eta,\theta,\zeta,\phi)\big\rangle_{\rho_{a_1b_1}} = \mathrm{Tr}\left[\rho_{a_1b_1}\hat{O}_{a_1,b_1}(\eta,\theta,\zeta,\phi)\right]\\
&= \frac{1}{2}\Big\{\Big[N_{hh}(\eta,\theta)N_{vv}(\zeta,\phi) + N_{vv}(\eta,\theta)N_{hh}(\zeta,\phi)\Big]\\
&\quad - e^{-4(1-T\eta_0)\alpha^2}\Big[N_{hv}(\eta,\theta)N^{*}_{hv}(\zeta,\phi) + N^{*}_{hv}(\eta,\theta)N_{hv}(\zeta,\phi)\Big]\Big\}\\
&= -\eta_0^2\left[(1-2\eta)(1-2\zeta) + 4e^{-4(1-T\eta_0)\alpha^2}\sqrt{\eta(1-\eta)\zeta(1-\zeta)}\cos 2(\theta-\phi)\right].
\end{aligned}
\tag{E.3}
$$

APPENDIX $\mathcal{F}$

FIDELITY OF TELEPORTATION FOR AN INPUT POLARIZATION QUBIT

The 4 Bell-states in polarization basis are

$$\begin{aligned}\left|\Psi^{\pm}\right\rangle &= \frac{1}{\sqrt{2}}\left(|H,V\rangle \pm |V,H\rangle\right)\\ \left|\Phi^{\pm}\right\rangle &= \frac{1}{\sqrt{2}}\left(|H,H\rangle \pm |V,V\rangle\right).\end{aligned} \tag{F.1}$$

Using (F.1) we recast the shared DV state (D.8) as

$$\begin{aligned}\rho_{a_1b_1} &= \frac{1}{2}\left[\left(|H,V\rangle\langle H,V| + |V,H\rangle\langle V,H|\right) - \left(|H,V\rangle\langle V,H| + |V,H\rangle\langle H,V|\right)\right]\\ &\quad + \frac{1-e^{-4(1-T\eta_0)\alpha^2}}{2}\Big(|HV\rangle\langle VH| + |VH\rangle\langle HV|\Big)\\ &= \left|\Psi^-\right\rangle\left\langle\Psi^-\right| + \frac{R}{2}\left(\left|\Psi^+\right\rangle\left\langle\Psi^+\right| - \left|\Psi^-\right\rangle\left\langle\Psi^-\right|\right) = \left(1-\frac{R}{2}\right)\left|\Psi^-\right\rangle\left\langle\Psi^-\right| + \frac{R}{2}\left|\Psi^+\right\rangle\left\langle\Psi^+\right|.\end{aligned} \tag{F.2}$$

Let us now consider the teleportion of an unknown input pure-state $|\psi_{\rm in}\rangle = \sqrt{p}\,|H\rangle + \sqrt{1-p}e^{i\theta}\,|V\rangle$. In the present case, the total tripartite state is given by

$$\begin{aligned}\rho_{\rm tot} &= |\psi_{\rm in}\rangle\langle\psi_{\rm in}| \otimes \rho_{a_1b_1} \\ &= \left(1-\frac{R}{2}\right)\left|\Psi^{(1)}\right\rangle\left\langle\Psi^{(1)}\right| + \frac{R}{2}\left|\Psi^{(2)}\right\rangle\left\langle\Psi^{(2)}\right|, \end{aligned} \tag{F.3}$$

where

$$\begin{aligned}\left|\Psi^{(1)}\right\rangle &= |\psi_{\rm in}\rangle\left|\Psi^-\right\rangle \\ &= \frac{1}{2}\Big\{ -\left|\Psi^+\right\rangle_{{\rm in},a_1}\otimes\sigma_z|\psi_{\rm in}\rangle_{b_1} - \left|\Psi^-\right\rangle_{{\rm in},a_1}\otimes|\psi_{\rm in}\rangle_{b_1} + \left|\Phi^+\right\rangle_{{\rm in},a_1}\otimes\sigma_x\sigma_z|\psi_{\rm in}\rangle_{b_1} \\ &+ \left|\Phi^-\right\rangle_{{\rm in},a_1}\otimes\sigma_x|\psi_{\rm in}\rangle_{b_1}\Big\} \\ \left|\Psi^{(2)}\right\rangle &= |\psi_{\rm in}\rangle\left|\Psi^+\right\rangle \\ &= \frac{1}{2}\Big\{ +\left|\Psi^+\right\rangle_{{\rm in},a_1}\otimes|\psi_{\rm in}\rangle_{b_1} + \left|\Psi^-\right\rangle_{{\rm in},a_1}\otimes\sigma_z|\psi_{\rm in}\rangle_{b_1} + \left|\Phi^+\right\rangle_{{\rm in},a_1}\otimes\sigma_x|\psi_{\rm in}\rangle_{b_1} \\ &+ \left|\Phi^-\right\rangle_{{\rm in},a_1}\otimes\sigma_x\sigma_z|\psi_{\rm in}\rangle_{b_1}\Big\} \end{aligned} \tag{F.4}$$

The Bell-state measurement $\Pi^{\pm}_{\psi/\phi}(\eta_0)$ yields the state in mode b_1 as $\rho^{\pm}_{b_1,\psi/\phi}(\eta_0) = {\rm Tr}_{{\rm in},a_1}\left[\Pi^{\pm}_{\psi/\phi}(\eta_0)\rho_{\rm tot}\right]$ with probability $P^{\pm}_{\psi/\phi}(\eta_0) = {\rm Tr}_{{\rm in},a_1,b_1}\left[\Pi^{\pm}_{\psi/\phi}(\eta_0)\rho_{\rm tot}\right] = {\rm Tr}\left[\rho^{\pm}_{b_1,\psi/\phi}(\eta_0)\right]$. This leads to the normalised state corresponding to the Bell-state measurement $\Pi^{\pm}_{\psi/\phi}(\eta_0)$ as $\rho^{\pm}_{\psi/\phi}(\eta_0) = \frac{\rho^{\pm}_{b_1,\psi/\phi}(\eta_0)}{P^{\pm}_{\psi/\phi}(\eta_0)}$.

In a straightforward calculation it can be shown that

$$\begin{aligned}\rho^{+}_{b_1,\psi} &= \frac{\eta_0^2}{4}\left[\left(1-\frac{R}{2}\right)\sigma_z|\psi_{\rm in}\rangle\langle\psi_{\rm in}|\sigma_z + \frac{R}{2}|\psi_{\rm in}\rangle\langle\psi_{\rm in}|\right] \\ \rho^{-}_{b_1,\psi} &= \frac{\eta_0^2}{4}\left[\left(1-\frac{R}{2}\right)|\psi_{\rm in}\rangle\langle\psi_{\rm in}| + \frac{R}{2}\sigma_z|\psi_{\rm in}\rangle\langle\psi_{\rm in}|\sigma_z\right] \\ \rho^{+}_{b_1,\phi} &= \frac{\eta_0^2}{4}\left[\left(1-\frac{R}{2}\right)\sigma_x\sigma_z|\psi_{\rm in}\rangle\langle\psi_{\rm in}|\sigma_z\sigma_x \right. \\ &\qquad \left. + \frac{R}{2}\sigma_x|\psi_{\rm in}\rangle\langle\psi_{\rm in}|\sigma_x\right] \\ \rho^{-}_{b_1,\psi} &= \frac{\eta_0^2}{4}\left[\left(1-\frac{R}{2}\right)|\psi_{\rm in}\rangle\langle\psi_{\rm in}| + \frac{R}{2}\sigma_x|\psi_{\rm in}\rangle\langle\psi_{\rm in}|\sigma_x\right] \end{aligned} \tag{F.5}$$

with the corresponding probability $P^{\pm}_{\psi/\phi} = \frac{\eta_0^2}{4}$. The corresponding unitary operations are given as - Π^{+}_{ψ} : σ_z, Π^{-}_{ψ} : $\mathbf{I}$, Π^{+}_{ϕ} : $-i\sigma_y = \sigma_z\sigma_x$ and Π^{-}_{ϕ} : σ_x. It can be easily seen from (F.5) that with these choices of the unitary rotations, in the limit $R \to 0$ ($\eta_0 \to 1, T \to 1$), we recover the ideal case.

After applying the suitable unitary rotation, the fidelity of teleportation for the four Bell-state measurements is given by

$$\begin{aligned} F^{\pm}_{\psi/\phi}(\eta_0) &= \left(1-\frac{R}{2}\right) + \frac{R}{2}\left|\langle\psi_{\text{in}}|\,\sigma_z\,|\psi_{\text{in}}\rangle\right|^2 \\ &= \left(1-\frac{R}{2}\right) + \frac{R}{2}\,(2p-1) \\ &= (1-R) + Rp. \end{aligned} \tag{F.6}$$

Consequently, after summing over the Bell-state measurements and averaging over the probability amplitude p, we get

$$F_{\text{av}} = \eta_0^2\frac{2-R}{2} = \eta_0^2\frac{1+e^{-4(1-T\eta_0)\alpha^2}}{2}. \tag{F.7}$$

It is evident from (F.7) that with ideal detector ($\eta_0 = 1$) and no-loss ($T = 1$) we obtain the perfect teleportation fidelity, i.e., $F_{\text{av}} = 1$.

BIBLIOGRAPHY

[1] Harry Nyquist. Certain factors affecting telegraph speed. *Bell System Technical Journal*, 3(4):324–346, 1924.

[2] Ralph Hartley. Transmission of information. *Bell System Technical Journal*, 7(3):535–563, 1928.

[3] Claude E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, 1948.

[4] Erwin Schrödinger. Discussion of probability relations between separated systems. *Proceedings of the Cambridge Philosophical Society*, 31(4):555–563, 1935.

[5] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, 1935.

[6] J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1:195, 1964.

[7] Stuart J. Freedman and John F. Clauser. Experimental test of local hidden-variable theories. *Physical Review Letters*, 28:938–941, 1972.

[8] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental tests of realistic local theories via bell's theorem. *Physical Review Letters*, 47:460–463, 1981.

[9] Alain Aspect, Jean Dalibard, and Gérard Roger. Experimental test of bell's inequalities using time-varying analyzers. *Physical Review Letters*, 49:1804–1807, 1982.

[10] S. Kochen and E. P. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics*, 17:59, 1967.

[11] Simon Kochen and Ernst Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics*, 17(1):59–87, 1967.

[12] Charles H. Bennett, Gilles Brassard, Claude Crepeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical Review Letters*, 70(13):1895–1899, 1993.

[13] Mingjian He and Shouyin Liu. Performance optimization of continuous-variable quantum teleportation with generalized photon-varying non-gaussian operations. *Physical Review A*, 110(1):012425, 2024.

[14] Kunal Sharma, Barry C. Sanders, and Mark M. Wilde. Optimal tests for continuous-variable quantum teleportation and photodetectors. *Physical Review Research*, 4(2):023066, 2022.

[15] Zhao-Di Liu, Olli Siltanen, Tom Kuusela, Rui-Heng Miao, Chen-Xi Ning, Chuan-Feng Li, Guang-Can Guo, and Jyrki Piilo. Overcoming noise in quantum teleportation with multipartite hybrid entanglement. *Science Advances*, 10(18):eadj3435, 2024.

[16] Mingjian He and Robert Malaney. Teleportation of hybrid entangled states with continuous-variable entanglement. *Scientific Reports*, 12(1):17169, 2022.

[17] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols. Quantum random access codes with shared randomness. *arXiv preprint arXiv:0810.2937*, 2008.

[18] Som Kanjilal, Chellasamy Jebarathinam, Tomasz Paterek, and Dipankar Home. Sufficient conditions for quantum advantage in random access code protocols with two-qubit states. *Physical Review A*, 108(1):012617, 2023.

[19] Máté Farkas, Nikolai Miklin, and Armin Tavakoli. Simple and general bounds on quantum random access codes. *Quantum*, 9:1643, February 2025.

[20] H. S. Karthik, S. Gómez, F. M. Quinteros, Akshata Shenoy, M. Pawłowski, S. P. Walborn, G. Lima, and E. S. Gómez. Noise-resilient quantum random access codes. *Physical Review A*, 111(3):032613, 2025.

[21] Nitica Sakharwade, Michał Studziński, Michał Eckstein, and Paweł Horodecki. Two instances of random access code in the quantum regime. *New Journal of Physics*, 25(5):053038, 2023.

[22] Rui-Heng Miao, Zhao-Di Liu, Yong-Nan Sun, Chen-Xi Ning, Chuan-Feng Li, and Guang-Can Guo. High-dimensional multi-input quantum random access codes and mutually unbiased bases. *Physical Review A*, 106(4):042418, 2022.

[23] Andris Ambainis, Dmitry Kravchenko, Sk Sazim, Joonwoo Bae, and Ashutosh Rai. Quantum advantages in $(n, d) \to 1$ random access codes. *New Journal of Physics*, 26(12):123023, 2024.

[24] Gabriel Pereira Alves, Nicolas Gigena, and Jędrzej Kaniewski. Biased random access codes. *Physical Review A*, 108(4):042608, 2023.

[25] Tristan Le Roy-Deloison, Edwin Peter Lobo, Jef Pauwels, and Stefano Pironio. Device-independent quantum key distribution based on routed bell tests. *PRX Quantum*, 6(2):020311, 2025.

[26] Ernest Y.-Z. Tan and Ramona Wolf. Entropy bounds for device-independent quantum key distribution with local bell test. *Phys. Rev. Lett.*, 133:120803, Sep 2024.

[27] Feihu Xu, Yu-Zhe Zhang, Qiang Zhang, and Jian-Wei Pan. Device-independent quantum key distribution with random postselection. *Phys. Rev. Lett.*, 128:110506, Mar 2022.

[28] Yang Liu, Wei-Jun Zhang, Cong Jiang, Jiu-Peng Chen, Chi Zhang, Wen-Xin Pan, Di Ma, Hao Dong, Jia-Min Xiong, Cheng-Jun Zhang, Hao Li, Rui-Chun Wang, Jun Wu, Teng-Yun Chen, Lixing You, Xiang-Bin Wang, Qiang Zhang, and Jian-Wei Pan. Experimental twin-field quantum key distribution over 1000 km fiber distance. *Phys. Rev. Lett.*, 130:210801, May 2023.

[29] Wei Zhang, Tim van Leent, Kai Redeker, Robert Garthoff, Rene Schwonnek, Florian Fertig, Sebastian Eppelt, Wenjamin Rosenfeld, Valerio Scarani, Charles C.-W. Lim, and Harald Weinfurter. A device-independent quantum key distribution system for distant users. *Nature*, 607(7911):687–691, 2022.

[30] Cihan Okay, Aziz Kharoof, and Selman Ipek. Simplicial quantum contextuality. *Quantum*, 7:1009, 2023.

[31] John H. Selby, David Schmid, Elie Wolfe, Ana Belen Sainz, Ravi Kunjwal, and Robert W. Spekkens. Contextuality without incompatibility. *Physical Review Letters*, 130(23):230201, 2023.

[32] Farid Shahandeh. Contextuality of general probabilistic theories. *PRX Quantum*, 2(1):010330, 2021.

[33] Xiao-Dong Yu, Isadora Veeren, and Otfried Gühne. Characterizing high-dimensional quantum contextuality. *Physical Review A*, 109(3):L030201, 2024.

[34] David Schmid, Haoxing Du, John H. Selby, and Matthew F. Pusey. Uniqueness of noncontextual models for stabilizer subtheories. *Physical Review Letters*, 129(12):120403, 2022.

[35] Jeongwoo Jae, Jiwon Lee, M. S. Kim, Kwang-Geol Lee, and Jinhyoung Lee. Contextual quantum metrology. *npj Quantum Information*, 10(1):68, 2024.

[36] Shiv Akshar Yadavalli and Ravi Kunjwal. Contextuality in entanglement-assisted one-shot classical communication. *Quantum*, 6:839, 2022.

[37] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[38] A. Peres. Separability criterion for density matrices. *Physical Review Letters*, 77(8):1413–1415, 1996.

[39] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: Necessary and sufficient conditions. *Physics Letters A*, 223(1-2):1–8, 1996.

[40] B. S. Cirel'son. Quantum generalizations of bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980.

[41] R. W. Spekkens. Contextuality for preparations, transformations, and unsharp measurements. *Phys. Rev. A*, 71:052108, May 2005.

[42] David Schmid, Robert W. Spekkens, and Elie Wolfe. All the noncontextuality inequalities for arbitrary prepare-and-measure experiments with respect to any fixed set of operational equivalences. *Phys. Rev. A*, 97:062103, Jun 2018.

[43] S. Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.

[44] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Dense quantum coding and a lower bound for 1-way quantum automata. In *Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC'99)*, pages 376–383, 1999.

[45] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Dense quantum coding and a lower bound for 1-way quantum automata. *Journal of the ACM*, 49:496, 2002.

[46] A. Nayak. Optimal lower bounds for quantum automata and random access codes. In *40th Annual Symposium on Foundations of Computer Science*, pages 369–376, 1999.

[47] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols. Quantum random access codes with shared randomness. *arXiv*, 0810.2937, 2008.

[48] M. Pawlowski and M. Zukowski. Entanglement-assisted random access codes. *Physical Review A*, 81:042326, 2010.

[49] T. K. C. Bobby and T. Paterek. Quantum random access codes using shared entanglement. *New Journal of Physics*, 16:093063, 2014.

[50] C. Jebarathinam, D. Das, S. Kanjilal, R. Srikanth, D. Sarkar, I. Chattopadhyay, and A. S. Majumdar. Quantum random access codes using non-maximally entangled states. *Physical Review A*, 100:012344, 2019.

[51] D. Das, A. Ghosal, A. G. Maity, S. Kanjilal, and A. Roy. Randomness certification using quantum nonlocality in a device-independent scenario. *Physical Review A*, 104:L060602, 2021.

[52] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, 2002.

[53] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, Bangalore, India, 1984. IEEE.

[54] A. K. Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letters*, 67:661, 1991.

[55] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[56] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[57] M. Horodecki, P. Horodecki, and R. Horodecki. Limitations of quantum operations in entanglement distribution. *Physical Review A*, 60:1888–1898, 1999.

[58] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problems of Information Transmission*, 9(3):177–183, 1973.

[59] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita. Quantum network coding. *New Journal of Physics*, 8:129, 2006.

[60] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita. Quantum network coding. In *Proceedings of the 24th International Symposium on Theoretical Aspects of Computer Science (STACS 2007)*, volume 4393 of *Lecture Notes in Computer Science*, pages 610–621, 2007.

[61] I. Kerenidis and R. de Wolf. Quantum and classical locally decodable codes and private information retrieval schemes. *Journal of Computer and System Sciences*, 69:395–420, 2004.

[62] S. Wehner and R. de Wolf. Improved lower bounds for locally decodable codes and private information retrieval. In *32nd International Colloquium on Automata, Languages and Programming (ICALP 05)*, volume 3580 of *Lecture Notes in Computer Science*, pages 1424–1436, 2005.

[63] A. Ben-Aroya, O. Regev, and R. de Wolf. A hypercontractive inequality for matrix-valued functions with applications to quantum computing and ldcs. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS'08)*, page 477–486, 2008.

[64] S. Muhammad, A. Tavakoli, M. Kurant, M. Pawłowski, M. Żukowski, and M. Bourennane. Quantum bidding in bridge-like games. *Physical Review X*, 4:021047, 2014.

[65] S. Wehner, M. Christandl, and A. C. Doherty. A lower bound on the dimension of a quantum system given measured data. *Physical Review A*, 78:062112, 2008.

[66] J. Ahrens, P. Badziag, M. Pawłowski, M. Żukowski, and M. Bourennane. Experimental violation of a bell-like inequality with symmetric measurements. *Physical Review Letters*, 112:140401, 2014.

[67] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane. Quantum random access codes using single d-level systems. *Physical Review Letters*, 114:170502, 2015.

[68] M. Czechlewski, D. Saha, A. Tavakoli, and M. Pawłowski. Operational characterization of quantum correlations. *Physical Review A*, 98:062305, 2018.

[69] H. Klauck. On quantum and approximate privacy. In *Proceedings of the IEEE Symposium on Foundations of Computer Science (FOCS 2001)*, page 288, 2001.

[70] S. Wehner and R. de Wolf. Improved lower bounds for quantum communication complexity. In *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, pages 320–332, 2004.

[71] D. Gavinsky, J. Kempe, O. Regev, and R. de Wolf. Bounded-error quantum state identification and exponential separations in communication complexity. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing (STOC'06)*, page 594–603, 2006.

[72] H. Buhrman and R. de Wolf. Communication complexity lower bounds by polynomials. In *Proceedings of the 16th Annual IEEE Conference on Computational Complexity*, page 120–130, 2001.

[73] D. Martínez, A. Tavakoli, M. Casanova, G. Cañas, B. Marques, and G. Lima. High-dimensional quantum communication complexity beyond strategies based on bell inequalities. *Physical Review Letters*, 121:150504, 2018.

[74] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han. Semidefinite programming bounds for device-independent randomness generation. *Physical Review A*, 84:034301, 2011.

[75] M. Pawlowski and N. Brunner. Semi-device-independent security of one-way quantum key distribution. *Physical Review A*, 84:010302(R), 2011.

[76] A. Grudka, K. Horodecki, M. Horodecki, W. Kłobus, and M. Pawłowski. Quantifying contextuality. *Physical Review Letters*, 113:100401, 2014.

[77] A. Grudka, M. Horodecki, R. Horodecki, and A. Wójcik. Quantifying bell nonlocality via nonlocality distillation. *Physical Review A*, 92:052312, 2015.

[78] K. Mohan, A. Tavakoli, and N. Brunner. Sequential random access codes and self-testing of quantum measurements. *New Journal of Physics*, 21:083034, 2019.

[79] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880, 1969.

[80] J. S. Bell. On the problem of hidden variables in quantum mechanics. *Reviews of Modern Physics*, 38:447, 1966.

[81] A. J. Leggett and A. Garg. Quantum mechanics versus macroscopic realism: Is the flux there when nobody looks? *Physical Review Letters*, 54:857, 1985.

[82] A. J. Leggett. Testing the limits of quantum mechanics: motivation, state of play, prospects. *Journal of Physics: Condensed Matter*, 14:R415, 2002.

[83] A. J. Leggett. Realism and the physical world. *Reports on Progress in Physics*, 71:022001, 2008.

[84] C. Emary, N. Lambert, and F. Nori. Leggett–garg inequalities. *Reports on Progress in Physics*, 77:016001, 2014.

[85] J. M. Yearsley. Macroscopic realism: What is it, and what do we know about it from experiment? *arXiv preprint*, 2013.

[86] A. A. Klyachko, M. A. Can, S. Binicioglu, and A. S. Shumovsky. Simple test for hidden variables in spin-1 systems. *Physical Review Letters*, 101:020403, 2008.

[87] J. Kofler and C. Brukner. Classical world arising out of quantum physics under the restriction of coarse-grained measurements. *Physical Review Letters*, 99:180403, 2007.

[88] S. G. Naik, E. P. Lobo, S. Sen, R. K. Patra, M. Alimuddin, T. Guha, S. S. Bhattacharya, and M. Banik. Violation of macrorealism and classical physics via quantum violation of the leggett-garg inequalities. *Physical Review Letters*, 128:140401, 2022.

[89] J. Kofler and C. Brukner. Condition for macroscopic realism beyond the leggett-garg inequalities. *Physical Review A*, 87:052115, 2013.

[90] C. Brukner, S. Taylor, S. Cheung, and V. Vedral. Quantum entanglement in time. *arXiv preprint*, 2004.

[91] S. Mal and A. S. Majumdar. Quantum violation of the pigeonhole principle and the nature of nonclassical correlations. *Physics Letters A*, 380:2265, 2016.

[92] S. Bose, D. Home, and S. Mal. Nonclassicality of the harmonic-oscillator coherent state persistently surviving under free evolution. *Physical Review Letters*, 120:210402, 2018.

[93] S. Mal, D. Das, and D. Home. Leggett-garg inequality and the reality of the quantum state. *Physical Review A*, 94:062117, 2016.

[94] S. Mukherjee, A. Rudra, D. Das, S. Mal, and D. Home. Violation of macrorealism: Stronger tests with finite-precision measurements. *Physical Review A*, 100:042114, 2019.

[95] T. Fritz. Quantum correlations in the temporal clauser-horne-shimony-holt (chsh) scenario. *New Journal of Physics*, 12:083055, 2010.

[96] C. Budroni, T. Moroder, M. Kleinmann, and O. Gühne. Bounding temporal quantum correlations. *Physical Review Letters*, 111:020403, 2013.

[97] S. Mal, M. Banik, and S. K. Choudhury. Quantum violation of macrorealism and the transition from quantum to classical physics. *Quantum Information Processing*, 15:2993, 2016.

[98] C. Budroni and C. Emary. Temporal quantum correlations and leggett-garg inequalities in multilevel systems. *Physical Review Letters*, 113:050401, 2014.

[99] S. Brierley, A. Kosowski, M. Markiewicz, T. Paterek, and A. Przysiężna. Nonclassicality of temporal correlations. *Physical Review Letters*, 115:120404, 2015.

[100] A. R. Usha Devi, H. S. Karthik, Sudha, and A. K. Rajagopal. Macrorealism from the perspective of an information-theoretic uncertainty principle. *Physical Review A*, 87:052103, 2013.

[101] S. Kumari and A. K. Pan. Revealing the role of compatibility and predictability in a leggett-garg test. *Physical Review A*, 96:042107, 2017.

[102] D. Das, S. Mal, and D. Home. Probing the role of interference in a leggett-garg test of macrorealism. *Physics Letters A*, 382:1085, 2018.

[103] H.-Y. Ku, S.-L. Chen, N. Lambert, Y.-N. Chen, and F. Nori. Hierarchies of generalized leggett-garg inequalities. *Physical Review A*, 98:022104, 2018.

[104] T. Chanda, T. Das, S. Mal, A. Sen De, and U. Sen. Probing quantum correlations: Leggett-garg-type inequalities in information-theoretic settings. *Physical Review A*, 98:022138, 2018.

[105] A. K. Pan. Revisiting the leggett-garg test: Why the usual criterion of macrorealism is problematic for quantum systems. *Physical Review A*, 102:032206, 2020.

[106] K. Joarder, D. Saha, D. Home, and U. Sinha. Contextual advantage in a multi-time quantum game. *PRX Quantum*, 3:010307, 2022.

[107] G. C. Knee, S. Simmons, E. M. Gauger, J. J. L. Morton, H. Riemann, N. V. Abrosimov, P. Becker, H.-J. Pohl, K. M. Itoh, M. L. W. Thewalt, G. A. D. Briggs, and S. C. Benjamin. Violation of a leggett-garg inequality with ideal non-invasive measurements. *Nature Communications*, 3:606, 2012.

[108] C. Robens, W. Alt, D. Meschede, C. Emary, and A. Alberti. Ideal negative measurements in quantum walks disprove theories based on classical trajectories. *Physical Review X*, 5:011003, 2015.

[109] G. C. Knee, K. Kakuyanagi, M.-C. Yeh, Y. Matsuzaki, H. Toida, H. Yamaguchi, S. Saito, A. J. Leggett, and W. J. Munro. A strict experimental test of macroscopic realism in a superconducting flux qubit. *Nature Communications*, 7:13253, 2016.

[110] H.-Y. Ku, N. Lambert, F.-R. Jhan, C. Emary, Y.-N. Chen, and F. Nori. Experimental test of non-macrorealistic cat states in the cloud. *npj Quantum Information*, 6:98, 2020.

[111] S. S. Majidy, H. Katiyar, G. Anikeeva, J. Halliwell, and R. Laflamme. Violation of the leggett-garg inequality with qutrits. *Physical Review A*, 100:042325, 2019.

[112] C. Spee, H. Siebeneich, T. F. Gloger, P. Kaufmann, M. Johanning, M. Kleinmann, C. Wunderlich, and Otfried Gühne. Entanglement-assisted quantum communication over noisy channels. *New Journal of Physics*, 22:023028, 2020.

[113] D. Das, A. G. Maity, D. Saha, and A. S. Majumdar. Contextuality in quantum random access codes: Advantage beyond quantum nonlocality. *arXiv preprint*, 2021.

[114] A. Tavakoli. Quantum correlations in self-testing and certification. *Physical Review Letters*, 126:210503, 2021.

[115] T. Vértesi and N. Brunner. Disproving the peres conjecture: Bell nonlocality from bound entanglement. *Nature Communications*, 5:5297, 2014.

[116] H.-W. Li, M. Pawlowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han. Semi-device-independent random-number expansion without entanglement. *Physical Review A*, 85:052308, 2012.

[117] A. G. Maity, S. Mal, C. Jebarathinam, and A. S. Majumdar. Quantum advantage in random access codes using bell nonlocality and contextuality. *Physical Review A*, 103:062604, 2021.

[118] E. G. Cavalcanti and H. M. Wiseman. Bell nonlocality, signal locality and unpredictability (open access). *Foundations of Physics*, 42:1329, 2012.

[119] R. Koenig, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory*, 55:4337, 2009.

[120] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by bell's theorem. *Nature*, 464:1021, 2010.

[121] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74:145, 2002.

[122] F. Xu, X. Ma, Q. Zhang, H. K. Lo, and J. W. Pan. Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 92:025002, 2020.

[123] D. J. Bernstein and T. Lange. Post-quantum cryptography. *Nature*, 549:23461, 2017.

[124] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98:230501, 2007.

[125] U. Vazirani and T. Vidick. Fully device independent quantum key distribution. *Physical Review Letters*, 113:140501, 2014.

[126] J. Singh, S. Ghosh, Arvind, and S. K. Goyal. Role of bell-chsh violation and local filtering in quantum key distribution. *Physics Letters A*, 392:127158, 2021.

[127] M. Farkas, M. B. Juandó, K. Łukanowski, J. Kołodyński, and A. Acín. Bell nonlocality is not sufficient for the security of standard device-independent quantum key distribution protocols. *Physical Review Letters*, 127:050503, 2021.

[128] J. Kołodyński, A. Máttar, P. Skrzypczyk, E. Woodhead, D. Cavalcanti, K. Banaszek, and A. Acín. Device-independent quantum key distribution with single-photon sources. *Quantum*, 4:260, 2020.

[129] T. Metger, Y. Dulek, A. Coladangelo, and R. A. Friedman. Device-independent quantum key distribution from computational assumptions. *New Journal of Physics*, 23:123021, 2021.

[130] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal. Experimental quantum key distribution certified by bell's theorem. *Nature*, 607:682–686, 2022.

[131] F. Xu, Y. Z. Zhang, Q. Zhang, and J. Pan. Device-independent quantum key distribution with random post selection. *Physical Review Letters*, 128:110506, 2022.

[132] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11:045021, 2009.

[133] A. Ferenczi and N. Lütkenhaus. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Physical Review A*, 85:052310, 2012.

[134] L. Zhou, Y. B. Sheng, and G. L. Long. Device-independent quantum secure direct communication against collective attacks. *Science Bulletin*, 65, 2020.

[135] L. Zhou and Y. B. Sheng. One-step device-independent quantum secure direct communication. *Science China Physics, Mechanics & Astronomy*, 65:250311, 2022.

[136] W. Zhang, D. S. Ding, Y. B. Sheng, L. Zhou, B. S. Shi, and G. C. Guo. Quantum secure direct communication with quantum memory. *Physical Review Letters*, 118:220501, 2017.

[137] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Physical Review Letters*, 125:010502, 2020.

[138] J. Park, J. Lee, and J. Heo. Improved statistical fluctuation analysis for twin-field quantum key distribution. *Quantum Information Processing*, 20:127, 2021.

[139] Y. F. Lu, Y. Wang, M. S. Jiang, F. Liu, X. X. Zhang, and W. S. Bao. Finite-key analysis of sending-or-not-sending twin-field quantum key distribution with intensity fluctuations. *Quantum Information Processing*, 20:135, 2021.

[140] L. G. She and C. M. Zhang. Reference-frame-independent quantum key distribution with modified coherent states. *Quantum Information Processing*, 21:161, 2022.

[141] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim. Quantum key distribution based on private states: Unconditional security over untrusted channels

with zero quantum capacity. *IEEE Transactions on Information Theory*, 54(6):2604–2620, 2008.

[142] C. H. Bennett and G. Brassard. Quantum cryptography, public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 2014.

[143] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68:3121, 1992.

[144] D. Kaszlikowski, D. K. L. Oi, M. Christandl, K. Chang, A. K. Ekert, L. C. Kwek, and C. H. Oh. Quantum cryptography based on qutrit bell inequalities. *Physical Review A*, 67:012310, 2003.

[145] R. Banerjee, A. K. Pal, and A. Sen(De). Uniform decoherence effect on localizable entanglement in random multiqubit pure states. *Physical Review A*, 101:042339, 2020.

[146] R. Gupta, S. Gupta, S. Mal, and A. Sen(De). Performance of dense coding and teleportation for random states: Augmentation via preprocessing. *Physical Review A*, 103:032608, 2021.

[147] V. M. Kendon, K. Życzkowski, and W. J. Munro. Bounds on entanglement in qudit subsystems. *Physical Review A*, 66:062310, 2002.

[148] W. Kłobus, A. Burchardt, A. Kołodziejski, M. Pandit, T. Vértesi, K. Życzkowski, and W. Laskowski. k-uniform mixed states. *Physical Review A*, 100:032112, 2019.

[149] D. Gross, S. T. Flammia, and J. Eisert. Most quantum states are too entangled to be useful as computational resources. *Physical Review Letters*, 102:190501, 2009.

[150] S. Rethinasamy, S. Roy, T. Chanda, A. Sen(De), and U. Sen. Universality in distribution of monogamy scores for random multiqubit pure states. *Physical Review A*, 99:042302, 2019.

[151] B. Schumacher and M. A. Nielsen. Quantum data processing and error correction. *Physical Review A*, 54:2629, 1996.

[152] R. Gupta, S. Gupta, S. Mal, and A. Sen(De). Constructive feedback of non-markovianity on resources in random quantum states. *Physical Review A*, 105:012424, 2022.

[153] R. Schwonnek, K. T. Goh, I. W. Primaatmaja, E. Y. Z. Tan, R. Wolf, V. Scarani, and C. C. W. Lim. Device-independent quantum key distribution with random key basis. *Nature Communications*, 12:2880, 2021.

[154] Y. M. Xie, B. H. Li, Y. S. Lu, X. Y. Cao, W. B. Liu, H. L. Yin, and Z. B. Chen. Overcoming the rate–distance limit of device-independent quantum key distribution. *Optics Letters*, 46:1632, 2021.

[155] W. Z. Liu, Y. Z. Zhang, Y. Z. Zhen, M. H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, and J. W. Pan. Toward a photonic demonstration of device-independent quantum key distribution. *Physical Review Letters*, 129:050502, 2022.

[156] H. M. Wiseman, S. J. Jones, and A. C. Doherty. Steering, entanglement, nonlocality, and the einstein-podolsky-rosen paradox. *Physical Review Letters*, 98:140402, 2007.

[157] B. H. Li, Y. M. Xie, Z. Li, C. X. Weng, C. L. Li, H. L. Yin, and Z. B. Chen. Long-distance twin-field quantum key distribution with entangled sources. *Optics Letters*, 46:5529, 2021.

[158] Y. Fu, H. L. Yin, T. Y. Chen, and Z. B. Chen. Long-distance measurement-device-independent multiparty quantum communication. *Physical Review Letters*, 114:090501, 2015.

[159] J. Gu, Y. M. Xie, W. B. Liu, Y. Fu, H. L. Yin, and Z. B. Chen. Secure quantum secret sharing without signal disturbance monitoring. *Optics Express*, 29:32244, 2021.

[160] Z. Li, X. Y. Cao, C. L. Li, C. X. Weng, J. Gu, H. L. Yin, and Z. B. Chen. Finite-key analysis for quantum conference key agreement with asymmetric channels. *Quantum Science and Technology*, 6:045019, 2021.

[161] A. Maitra, G. Paul, and S. Roy. Device-independent quantum private query. *Physical Review A*, 95:042344, 2017.

[162] Yeong-Cherng Liang, Robert W. Spekkens, and Howard M. Wiseman. Specker's parable of the overprotective seer: A road to contextuality, nonlocality and complementarity. *Physics Reports*, 506(1):1–39, 2011.

[163] Michael D Mazurek, Matthew F Pusey, Ravi Kunjwal, Kevin J Resch, and Robert W Spekkens. An experimental test of noncontextuality without unphysical idealizations. *Nature communications*, 7:11780, 2016.

[164] Matthew F. Pusey. Robust preparation noncontextuality inequalities in the simplest scenario. *Phys. Rev. A*, 98:022112, Aug 2018.

[165] Zhen-Peng Xu, Debashis Saha, Hong-Yi Su, Marcin Pawłowski, and Jing-Ling Chen. Reformulating noncontextuality inequalities in an operational approach. *Phys. Rev. A*, 94:062103, Dec 2016.

[166] Anubhav Chaturvedi, Máté Farkas, and Victoria J Wright. Characterising and bounding the set of quantum behaviours in contextuality scenarios. *Quantum*, 5:484, June 2021.

[167] Costantino Budroni, Adán Cabello, Otfried Gühne, Matthias Kleinmann, and Jan-Åke Larsson. Kochen-specker contextuality. *Rev. Mod. Phys.*, 94:045007, Dec 2022.

[168] Robert W. Spekkens. Negativity and contextuality are equivalent notions of nonclassicality. *Phys. Rev. Lett.*, 101:020401, Jul 2008.

[169] Anubhav Chaturvedi and Debashis Saha. Quantum prescriptions are more ontologically distinct than they are operationally distinguishable. *Quantum*, 4:345, October 2020.

[170] Anubhav Chaturvedi, Marcin Pawłowski, and Debashis Saha. Quantum description of reality is empirically incomplete, 2021.

[171] Matthew F. Pusey. Anomalous weak values are proofs of contextuality. *Phys. Rev. Lett.*, 113:200401, Nov 2014.

[172] Matteo Lostaglio. Quantum fluctuation theorems, contextuality, and work quasiprobabilities. *Phys. Rev. Lett.*, 120:040602, Jan 2018.

[173] David Schmid and Robert W. Spekkens. Contextual advantage for state discrimination. *Phys. Rev. X*, 8:011015, Feb 2018.

[174] David Schmid, John H. Selby, Matthew F. Pusey, and Robert W. Spekkens. A structure theorem for generalized-noncontextual ontological models, 2020.

[175] David Schmid, John H. Selby, and Robert W. Spekkens. Unscrambling the omelette of causation and inference: The framework of causal-inferential theories, 2020.

[176] Lorenzo Catani, Matthew Leifer, David Schmid, and Robert W. Spekkens. Why interference phenomena do not capture the essence of quantum theory. *Quantum*, 7:1119, September 2023.

[177] Lorenzo Catani, Matthew Leifer, Giovanni Scala, David Schmid, and Robert W. Spekkens. What is nonclassical about uncertainty relations? *Phys. Rev. Lett.*, 129:240401, Dec 2022.

[178] John H. Selby, Elie Wolfe, David Schmid, and Ana Belén Sainz. An open-source linear program for testing nonclassicality, 2022.

[179] Lorenzo Catani, Matthew Leifer, Giovanni Scala, David Schmid, and Robert W. Spekkens. Aspects of the phenomenology of interference that are genuinely nonclassical. *Phys. Rev. A*, 108:022207, Aug 2023.

[180] Matteo Lostaglio and Gabriel Senno. Contextual advantage for state-dependent cloning. *Quantum*, 4:258, April 2020.

[181] Armin Tavakoli, Emmanuel Zambrini Cruzeiro, Roope Uola, and Alastair A. Abbott. Bounding and simulating contextual correlations in quantum theory. *PRX Quantum*, 2:020334, Jun 2021.

[182] Victoria J. Wright and Máté Farkas. Invertible map between bell nonlocal and contextuality scenarios. *Phys. Rev. Lett.*, 131:220202, Nov 2023.

[183] Robert W. Spekkens, D. H. Buzacott, A. J. Keehn, Ben Toner, and G. J. Pryde. Preparation contextuality powers parity-oblivious multiplexing. *Phys. Rev. Lett.*, 102:010401, Jan 2009.

[184] André Chailloux, Iordanis Kerenidis, Srijita Kundu, and Jamie Sikora. Optimal bounds for parity-oblivious random access codes. *New Journal of Physics*, 18(4):045003, apr 2016.

[185] Debashis Saha and Anubhav Chaturvedi. Preparation contextuality as an essential feature underlying quantum communication advantage. *Phys. Rev. A*, 100:022108, Aug 2019.

[186] Debashis Saha, Paweł Horodecki, and Marcin Pawłowski. State independent contextuality advances one-way communication. *New J. Phys.*, 21(9):093057, sep 2019.

[187] Alley Hameedi, Armin Tavakoli, Breno Marques, and Mohamed Bourennane. Communication games reveal preparation contextuality. *Phys. Rev. Lett.*, 119:220402, Nov 2017.

[188] Shouvik Ghorai and A. K. Pan. Optimal quantum preparation contextuality in an n-bit parity-oblivious multiplexing task. *Phys. Rev. A*, 98:032110, Sep 2018.

[189] Andris Ambainis, Manik Banik, Anubhav Chaturvedi, Dmitry Kravchenko, and Ashutosh Rai. Parity oblivious d-level random access codes and class of noncontextuality inequalities. *Quantum Information Processing*, 18(4):111, Mar 2019.

[190] David Schmid, Haoxing Du, John H. Selby, and Matthew F. Pusey. Uniqueness of noncontextual models for stabilizer subtheories. *Phys. Rev. Lett.*, 129:120403, Sep 2022.

[191] Kieran Flatt, Hanwool Lee, Carles Roch I Carceller, Jonatan Bohr Brask, and Joonwoo Bae. Contextual advantages and certification for maximum-confidence discrimination. *PRX Quantum*, 3:030337, Sep 2022.

[192] Carles Roch i Carceller, Kieran Flatt, Hanwool Lee, Joonwoo Bae, and Jonatan Bohr Brask. Quantum vs noncontextual semi-device-independent randomness certification. *Phys. Rev. Lett.*, 129:050501, Jul 2022.

[193] Shashank Gupta, Debashis Saha, Zhen-Peng Xu, Adán Cabello, and Archan S Majumdar. Quantum contextuality provides communication complexity advantage. *Phys. Rev. Lett.*, 130(8):080802, 2023.

[194] Martin Henk, Jürgen Richter-Gebert, and Günter M Ziegler. Basic properties of convex polytopes. In *Handbook of discrete and computational geometry*, pages 383–413. Chapman and Hall/CRC, 2017.

[195] https://github.com/soumya-s3/noncontextual polytope and quantum advantage, 2024.

[196] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.

[197] J. S. Bell and Alain Aspect. *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy*. Cambridge University Press, 2 edition, 2004.

[198] Wei Zhang, Tim van Leent, Kai Redeker, Robert Garthoff, Rene Schwonnek, Florian Fertig, Sebastian Eppelt, Wenjamin Rosenfeld, Valerio Scarani, Charles C.-W. Lim, and Harald Weinfurter. A device-independent quantum key distribution system for distant users. *Nature*, 607:687–691, 2022.

[199] Wen-Zhao Liu, Yu-Zhe Zhang, Yi-Zheng Zhen, Ming-Han Li, Yang Liu, Jingyun Fan, Feihu Xu, Qiang Zhang, and Jian-Wei Pan. Toward a photonic demonstration of device-independent quantum key distribution. *Phys. Rev. Lett.*, 129:050502, Jul 2022.

[200] Víctor Zapatero, Tim van Leent, Rotem Arnon-Friedman, Wen-Zhao Liu, Qiang Zhang, Harald Weinfurter, and Marcos Curty. Advances in device-independent quantum key distribution. *npj Quantum Information*, page 10, 2023.

[201] Lewis Wooltorton, Peter Brown, and Roger Colbeck. Device-independent quantum key distribution with arbitrarily small nonlocality. *Phys. Rev. Lett.*, 132:210802, May 2024.

[202] Ernest Y.-Z. Tan and Ramona Wolf. Entropy bounds for device-independent quantum key distribution with local bell test. *Phys. Rev. Lett.*, 133:120803, Sep 2024.

[203] Austin K. Daniel, Yingyue Zhu, C. Huerta Alderete, Vikas Buchemmavari, Alaina M. Green, Nhung H. Nguyen, Tyler G. Thurtell, Andrew Zhao, Norbert M. Linke, and Akimasa Miyake. Quantum computational advantage attested by nonlocal games with the cyclic cluster state. *Phys. Rev. Res.*, 4:033068, Jul 2022.

[204] Jelena Mackeprang, Daniel Bhatti, and Stefanie Barz. Non-adaptive measurement-based quantum computation on ibm q. *Scientific Reports*, page 15428, 2023.

[205] Yael Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. Quantum advantage from any non-local game. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC 2023)*, STOC 2023, page 1617–1628. Association for Computing Machinery, 2023.

[206] Andrea Coladangelo, Koon Tong Goh, and Valerio Scarani. All pure bipartite entangled states can be self-tested. *Nature Communications*, 8:15485, 2017.

[207] Suchetana Goswami, Bihalan Bhattacharya, Debarshi Das, Souradeep Sasmal, C. Jebaratnam, and A. S. Majumdar. One-sided device-independent self-testing of any pure two-qubit entangled state. *Phys. Rev. A*, 98:022311, Aug 2018.

[208] Wen-Hao Zhang, Geng Chen, Xing-Xiang Peng, Xiang-Jun Ye, Peng Yin, Xiao-Ye Xu, Jin-Shi Xu, Chuan-Feng Li, and Guang-Can Guo. Experimental realization of robust self-testing of bell state measurements. *Phys. Rev. Lett.*, 122:090402, Mar 2019.

[209] Wen-Hao Zhang, Geng Chen, Peng Yin, Xing-Xiang Peng, Xiao-Min Hu, Zhi-Bo Hou, Zhi-Yuan Zhou, Shang Yu, Xiang-Jun Ye, Zong-Quan Zhou, Xiao-Ye Xu, Jian-Shun Tang, Jin-Shi Xu, Yong-Jian Han, Bi-Heng Liu, Chuan-Feng Li, and Guang-Can Guo. Experimental demonstration of robust self-testing for bipartite entangled states. *npj Quantum Information*, 5:4–5, 2019.

[210] Peter Bierhorst, Emanuel Knill, Scott Glancy, Yanbao Zhang, Alan Mink, Stephen Jordan, Andrea Rommal, Yi-Kai Liu, Bradley Christensen, Sae Woo Nam, Martin J. Stevens, and Lynden K. Shalm. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature*, 556:223–226, 2018.

[211] Antonio Acín, Stefano Pironio, Tamás Vértesi, and Peter Wittek. Optimal randomness certification from one entangled bit. *Phys. Rev. A*, 93:040102, Apr 2016.

[212] Antonio Acín and Lluis Masanes. Certified randomness in quantum physics. *Nature*, 540:213–219, 2016.

[213] Joseph Bowles, Ivan Šupić, Daniel Cavalcanti, and Antonio Acín. Device-independent entanglement certification of all entangled states. *Phys. Rev. Lett.*, 121:180503, Oct 2018.

[214] Ole Andersson, Piotr Badzikag, Irina Dumitru, and Adan Cabello. Device-independent certification of two bits of randomness from one entangled bit and gisin's elegant bell inequality. *Phys. Rev. A*, 97:012314, Jan 2018.

[215] Mojtaba Ghadimi, Michael J. W. Hall, and Howard M. Wiseman. Nonlocality in bell's theorem, in bohm's theory, and in many interacting worlds theorising. *Entropy*, 20:567, 2018.

[216] Valerio Scarani. *Bell Nonlocality*. Oxford University Press, 1 edition, 2019.

[217] Jean-Charles Forgues, Christian Lupien, and Bertrand Reulet. Experimental violation of bell-like inequalities by electronic shot noise. *Phys. Rev. Lett.*, 114:130403, Apr 2015.

[218] Shashi Prabhakar, Salla Gangi Reddy, A. Aadhi, Chithrabhanu Perumangatt, G. K. Samanta, and R. P. Singh. Violation of bell's inequality for phase-singular beams. *Phys. Rev. A*, 92:023822, Aug 2015.

[219] Juan P. Dehollain, Stephanie Simmons, Juha T. Muhonen, Rachpon Kalra, Arne Laucht, Fay Hudson, Kohei M. Itoh, David N. Jamieson, Jeffrey C. McCallum, Andrew S. Dzurak, and Andrea Morello. Bell's inequality violation with spins in silicon. *Nature Nanotechnology*, 11:242–246, 2016.

[220] Martin Ringbauer, Christina Giarmatzi, Rafael Chaves, Fabio Costa, Andrew G. White, and Alessandro Fedrizzi. Experimental test of nonlocal causality. *Science Advances*, 2(8):e1600162, 2016.

[221] Gonzalo Carvacho, Francesco Andreoli, Luca Santodonato, Marco Bentivegna, Rafael Chaves, and Fabio Sciarrino. Experimental violation of local causality in a quantum network. *Nature Communications*, 8:14775, 2017.

[222] Igor Marinkovic, Andreas Wallucks, Ralf Riedinger, Sungkun Hong, Markus Aspelmeyer, and Simon Gröblacher. Optomechanical bell test. *Phys. Rev. Lett.*, 121:220404, Nov 2018.

[223] Oliver Thearle, Jiri Janousek, Seiji Armstrong, Sara Hosseini, Melanie Schünemann (Mraz), Syed Assad, Thomas Symul, Matthew R. James, Elanor Huntington, Timothy C. Ralph, and Ping Koy Lam. Violation of bell's inequality using continuous variable measurements. *Phys. Rev. Lett.*, 120:040406, Jan 2018.

[224] Dongkai Zhang, Xiaodong Qiu, Wuhong Zhang, and Lixiang Chen. Violation of a bell inequality in two-dimensional state spaces for radial quantum number. *Phys. Rev. A*, 98:042134, Oct 2018.

[225] Y. P. Zhong, H.-S. Chang, K. J. Satzinger, M.-H. Chou, A. Bienfait, C. R. Conner, E. Dumur, J. Grebel, G. A. Peairs, R. G. Povey, D. I. Schuster, and A. N. Cleland. Violating bell's inequality with remotely connected superconducting qubits. *Nature Physics*, 15:741–744, 2019.

[226] Tim van Leent, Matthias Bock, Florian Fertig, Robert Garthoff, Sebastian Eppelt, Yiru Zhou, Pooja Malik, Matthias Seubert, Tobias Bauer, Wenjamin Rosenfeld, Wei Zhang, Christoph Becher, and Harald Weinfurter. Entangling single atoms over 33km telecom fibre. *Nature*, 607:69, 2022.

[227] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412):eaam9288, 2018.

[228] Koji Azuma, Sophia E. Economou, David Elkouss, Paul Hilaire, Liang Jiang, Hoi-Kwong Lo, and Ilan Tzitrin. Quantum repeaters: From quantum networks to the quantum internet. *Rev. Mod. Phys.*, 95:045006, Dec 2023.

[229] H. M. Wiseman, S. J. Jones, and A. C. Doherty. Steering, entanglement, nonlocality, and the einstein-podolsky-rosen paradox. *Phys. Rev. Lett.*, 98:140402, Apr 2007.

[230] D Buono, G Nocerino, S Solimeno, and A Porzio. Different operational meanings of continuous variable gaussian entanglement criteria and bell inequalities. *Laser Physics*, 24(7):074008, may 2014.

[231] Eric Lantz, Mehdi Mabed, and Fabrice Devaux. Violation of bell inequalities by stochastic simulations of gaussian states based on their positive wigner representation. *Physica Scripta*, 96(4):045103, feb 2021.

[232] Michael G. Jabbour and Jonatan Bohr Brask. Constructing local models for general measurements on bosonic gaussian states. *Phys. Rev. Lett.*, 131:110202, Sep 2023.

[233] Feihu Xu, Marcos Curty, Bing Qi, Li Qian, and Hoi-Kwong Lo. Discrete and continuous variables for measurement-device-independent quantum cryptography. *Nature Photonics*, 9:772–773, 2015.

[234] Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias Gehring, Christian S. Jacobsen, and Ulrik L. Andersen. Reply to 'discrete and continuous variables for measurement-device-independent quantum cryptography'. *Nature Photonics*, 9:773–775, 2015.

[235] Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan. Practical challenges in quantum key distribution. *npj Quantum Information*, 2:16025, 2016.

[236] Luca S. Costanzo, Antonio S. Coelho, Nicola Biagi, Jaromír Fiurášek, Marco Bellini, and Alessandro Zavatta. Measurement-induced strong kerr nonlinearity for weak quantum states of light. *Phys. Rev. Lett.*, 119:013601, Jul 2017.

[237] Adarsh Jain, Parthkumar V Sakhiya, and R K Bahl. Design and development of weak coherent pulse source for quantum key distribution system. In *2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, pages 1–5, 2020.

[238] Howard M. Wiseman, Aephraim M. Steinberg, and Matin Hallaji. Obtaining a single-photon weak value from experiments using a strong (many-photon) coherent state. *AVS Quantum Science*, 5(2):024401, 04 2023.

[239] Stefano Duranti, Sören Wengerowsky, Leo Feldmann, Alessandro Seri, Bernardo Casabone, and Hugues de Riedmatten. Efficient cavity-assisted storage of photonic qubits in a solid-state quantum memory. *Opt. Express*, 32(15):26884–26895, Jul 2024.

[240] Hyunseok Jeong. Using weak nonlinearity under decoherence for macroscopic entanglement generation and quantum computation. *Phys. Rev. A*, 72:034305, Sep 2005.

[241] Yan Li, Hui Jing, and Ming-Sheng Zhan. Optical generation of a hybrid entangled state via an entangling single-photon-added coherent state. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 39(9):2107, apr 2006.

[242] Bing He, Qing Lin, and Christoph Simon. Cross-kerr nonlinearity between continuous-mode coherent states and single photons. *Phys. Rev. A*, 83:053826, May 2011.

[243] Dat Thanh Le, Warit Asavanant, and Nguyen Ba An. Heralded preparation of polarization entanglement via quantum scissors. *Phys. Rev. A*, 104:012612, Jul 2021.

[244] Hyukjoon Kwon and Hyunseok Jeong. Violation of the bell–clauser-horne-shimony-holt inequality using imperfect photodetectors with optical hybrid states. *Phys. Rev. A*, 88:052127, Nov 2013.

[245] Yanna Li, Manuel Gessner, Weidong Li, and Augusto Smerzi. Hyper- and hybrid nonlocality. *Phys. Rev. Lett.*, 120:050404, Feb 2018.

[246] Morteza Moradi, Juan Camilo López Carreño, Adam Buraczewski, Thomas McDermott, Beate Elisabeth Asenbeck, Julien Laurat, and Magdalena Stobińska. Chsh bell tests for optical hybrid entanglement. *New Journal of Physics*, 26(3):033019, mar 2024.

[247] Daniel Cavalcanti, Nicolas Brunner, Paul Skrzypczyk, Alejo Salles, and Valerio Scarani. Large violation of bell inequalities using both particle andwave measurements. *Phys. Rev. A*, 84:022105, Aug 2011.

[248] Kimin Park, Seung-Woo Lee, and Hyunseok Jeong. Quantum teleportation between particlelike and fieldlike qubits using hybrid entanglement under decoherence effects. *Physical Review A*, 86(6):062301, Dec 2012.

[249] Seung-Woo Lee and Hyunseok Jeong. Near-deterministic quantum teleportation and resource-efficient quantum computation using linear optics and hybrid qubits. *Phys. Rev. A*, 87:022326, Feb 2013.

[250] Alexander E. Ulanov, Demid Sychev, Anastasia A. Pushkina, Ilya A. Fedorov, and A. I. Lvovsky. Quantum teleportation between discrete and continuous encodings of an optical qubit. *Phys. Rev. Lett.*, 118:160501, Apr 2017.

[251] Demid V. Sychev, Alexander E. Ulanov, Egor S. Tiunov, Anastasia A. Pushkina, A. Kuzhamuratov, Valery Novikov, and A. I. Lvovsky. Entanglement and teleportation between polarization and wave-like encodings of an optical qubit. *Nature Communications*, 9(1):3672, 2018.

[252] Soumyakanti Bose and Hyunseok Jeong. Quantum teleportation of hybrid qubits and single-photon qubits using gaussian resources. *Phys. Rev. A*, 105:032434, Mar 2022.

[253] Mingjian He and Robert Malaney. Teleportation of hybrid entangled states with continuous-variable entanglement. *Scientific Reports*, 12:17169, 2022.

[254] M El Kirdi, A Slaoui, N Ikken, M Daoud, and R Ahl Laamara. Controlled quantum teleportation between discrete and continuous physical systems. *Physica Scripta*, 98(2):025101, jan 2023.

[255] Srikrishna Omkar, Yong Siah Teo, and Hyunseok Jeong. Resource-efficient topological fault-tolerant quantum computation with hybrid entanglement of light. *Phys. Rev. Lett.*, 125:060501, Aug 2020.

[256] S. Omkar, Y. S. Teo, Seung-Woo Lee, and H. Jeong. Highly photon-loss-tolerant quantum computing using hybrid qubits. *Phys. Rev. A*, 103:032602, Mar 2021.

[257] Tom Darras, Beate Elisabeth Asenbeck, Giovanni Guccione, Adrien Cavaillès, Hanna Le Jeannic, and Julien Laurat. A quantum-bit encoding converter. *Nature Photonics*, 17:165–170, 2023.

[258] Jaehak Lee, Nuri Kang, Seok-Hyung Lee, Hyunseok Jeong, Liang Jiang, and Seung-Woo Lee. Fault-tolerant quantum computation by hybrid qubits with bosonic cat code and single photons. *PRX Quantum*, 5:030322, Aug 2024.

[259] Soumyakanti Bose, Jaskaran Singh, Adán Cabello, and Hyunseok Jeong. Long-distance entanglement sharing using hybrid states of discrete and continuous variables. *Phys. Rev. Appl.*, 21:064013, Jun 2024.

[260] Hyunseok Jeong, Alessandro Zavatta, Minsu Kang, Seung-Woo Lee, Luca S. Costanzo, Samuele Grandi, Timothy C. Ralph, and Marco Bellini. Generation of hybrid entanglement of light. *Nature Photonics*, 8:564–569, 2014.

[261] Olivier Morin, Kun Huang, Jianli Liu, Hanna Le Jeannic, Claude Fabre, and Julien Laurat. Remote creation of hybrid entanglement between particle-like and wave-like optical qubits. *Nature Photonics*, 8:570–574, 2014.

[262] H. Le Jeannic, A. Cavaillès, J. Raskop, K. Huang, and J. Laurat. Remote preparation of continuous-variable qubits using loss-tolerant hybrid entanglement of light. *Optica*, 5(8):1012–1015, Aug 2018.

[263] Kun Huang, Hanna Le Jeannic, Olivier Morin, Tom Darras, Giovanni Guccione, Adrien Cavaillès, and Julien Laurat. Engineering optical hybrid entanglement between discrete- and continuous-variable states. *New Journal of Physics*, 21(8):083033, aug 2019.

[264] Bastian Hacker, Stephan Welte, Severin Daiss, Armin Shaukat, Stephan Ritter, Lin Li, and Gerhard Rempe. Deterministic creation of entangled atom–light schrödinger-cat states. *Nature Photonics*, 13:110–115, 2019.

[265] Giovanni Guccione, Tom Darras, Hanna Le Jeannic, Varun B. Verma, Sae Woo Nam, Adrien Cavaillès, and Julien Laurat. Connecting heterogeneous quantum networks by hybrid entanglement swapping. *Science Advances*, 6(22):eaba4508, 2020.

[266] Élie Gouzien, Floriane Brunel, Sébastien Tanzilli, and Virginia D'Auria. Scheme for the generation of hybrid entanglement between time-bin and wavelike encodings. *Phys. Rev. A*, 102:012603, Jul 2020.

[267] Jianming Wen, Irina Novikova, Chen Qian, Chuanwei Zhang, and Shengwang Du. Hybrid entanglement between optical discrete polarizations and continuous quadrature variables. *Photonics*, 8(12):552, 2021.

[268] Shujing Li, Yaya He, Qiqi Deng, Jiaoyang Xue, Zhongxiao Xu, and Hai Wang. Improvement of hybrid entanglement by dual-way photon polarization measurement. *Quantum Information Processing*, 20:295, 2021.

[269] Youngrong Lim, Jaewoo Joo, Timothy P. Spiller, and Hyunseok Jeong. Loss-resilient photonic entanglement swapping using optical hybrid states. *Phys. Rev. A*, 94:062337, Dec 2016.

[270] Ryan C Parker, Jaewoo Joo, Mohsen Razavi, and Timothy P Spiller. Hybrid photonic loss resilient entanglement swapping. *Journal of Optics*, 19(10):104004, sep 2017.

[271] Michael Zopf, Robert Keil, Yan Chen, Jingzhong Yang, Disheng Chen, Fei Ding, and Oliver G. Schmidt. Entanglement swapping with semiconductor-generated photons violates bell's inequality. *Phys. Rev. Lett.*, 123:160502, Oct 2019.

[272] Yoshiaki Tsujimoto, Chenglong You, Kentaro Wakui, Mikio Fujiwara, Kazuhiro Hayasaka, Shigehito Miki, Hirotaka Terai, Masahide Sasaki, Jonathan P Dowling, and Masahiro Takeoka. Heralded amplification of nonlocality via entanglement swapping. *New Journal of Physics*, 22(2):023008, feb 2020.

[273] Cen-Xiao Huang, Xiao-Min Hu, Yu Guo, Chao Zhang, Bi-Heng Liu, Yun-Feng Huang, Chuan-Feng Li, Guang-Can Guo, Nicolas Gisin, Cyril Branciard, and Armin Tavakoli. Entanglement swapping and quantum correlations via symmetric joint measurements. *Phys. Rev. Lett.*, 129:030502, Jul 2022.

[274] Anders J. E. Bjerrum, Jonatan B. Brask, Jonas S. Neergaard-Nielsen, and Ulrik L. Andersen. Proposal for a long-distance nonlocality test with entanglement swapping and displacement-based measurements. *Phys. Rev. A*, 107:052611, May 2023.

[275] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[276] Marcello Caleffi, Michele Amoretti, Davide Ferrari, Jessica Illiano, Antonio Manzalini, and Angela Sara Cacciapuoti. Distributed quantum computing: A survey. *Computer Networks*, 254:110672, Dec 2024.

[277] Nirman Ganguly, Satyabrata Adhikari, A. S. Majumdar, and Jyotishman Chatterjee. Entanglement witness operator for quantum teleportation. *Phys. Rev. Lett.*, 107:270501, Dec 2011.

[278] Satyabrata Adhikari, Archan S. Majumdar, Sovik Roy, Biplab Ghosh, and Nilkantha Nayak. Teleportation via maximally and non-maximally entangled mixed states. *Quant. Inf. Compt.*, 10, May 2010.

[279] N. Gisin. Nonlocality criteria for quantum teleportation. *Physics Letters A*, 210(3):157–159, 1996.

[280] Ryszard Horodecki, Michał Horodecki, and Paweł Horodecki. Teleportation, bell's inequalities and inseparability. *Physics Letters A*, 222(1):21–25, 1996.

[281] Hiroki Takesue, Shellee D. Dyer, Martin J. Stevens, Varun Verma, Richard P. Mirin, and Sae Woo Nam. Quantum teleportation over 100 km of fiber using highly efficient superconducting nanowire single-photon detectors. *Optica*, 2(10):832–835, Oct 2015.

[282] Meiru Huo, Jiliang Qin, Jialin Cheng, Zhihui Yan, Zhongzhong Qin, Xiaolong Su, Xiaojun Jia, Changde Xie, and Kunchi Peng. Deterministic quantum teleportation through fiber channels. *Science Advances*, 4(10):eaas9401, 2018.

[283] Hao Zhao, Jinxia Feng, Jingke Sun, Yuanji Li, and Kuanshou Zhang. Real time deterministic quantum teleportation over 10 km of single optical fiber channel. *Opt. Express*, 30(3):3770–3782, Jan 2022.

[284] Si Shen, Chenzhi Yuan, Zichang Zhang, Hao Yu, Ruiming Zhang, Chuanrong Yang, Hao Li, Zhen Wang, You Wang, Guangwei Deng, Haizhi Song, Lixing You, Yunru Fan, Guangcan Guo, and Qiang Zhou. Hertz-rate metropolitan quantum teleportation. *Light: Science & Applications*, 12:115, 2023.

[285] Dario Lago-Rivera, Jelena V. Rakonjac, Samuele Grandi, and Hugues de Riedmatten. Long distance multiplexed quantum teleportation from a telecom photon to a solid-state qubit. *Nature Communications*, 14:1889, 2023.

[286] Adnan A. E. Hajomer, Florian Kanitschar, Nitin Jain, Michael Hentschel, Runjia Zhang, Norbert Lütkenhaus, Ulrik L. Andersen, Christoph Pacher, and Tobias Gehring. Experimental composable key distribution using discrete-modulated continuous variable quantum cryptography, 2024.

[287] Wei Li, Likang Zhang, Yichen Lu, Zheng-Ping Li, Cong Jiang, Yang Liu, Jia Huang, Hao Li, Zhen Wang, Xiang-Bin Wang, Qiang Zhang, Lixing You, Feihu Xu, and Jian-Wei Pan. Twin-field quantum key distribution without phase locking. *Phys. Rev. Lett.*, 130:250802, Jun 2023.

[288] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.*, 92:025002, May 2020.

[289] Kejin Wei, Wei Li, Hao Tan, Yang Li, Hao Min, Wei-Jun Zhang, Hao Li, Lixing You, Zhen Wang, Xiao Jiang, Teng-Yun Chen, Sheng-Kai Liao, Cheng-Zhi Peng, Feihu Xu, and Jian-Wei Pan. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. *Phys. Rev. X*, 10:031030, Aug 2020.

[290] G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, and A. Q. Liu. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. *Nature Photonics*, 13:839–842, 2019.

[291] Mi Zou, Yingqiu Mao, and Teng-Yun Chen. Rigorous calibration of homodyne detection efficiency for continuous-variable quantum key distribution. *Opt. Express*, 30(13):22788–22797, Jun 2022.

[292] Ulrik L. Andersen, Jonas S. Neergaard-Nielsen, Peter van Loock, and Akira Furusawa. Hybrid discrete- and continuous-variable quantum information. *Nature Physics*, 11:713–719, 2015.

[293] Pei-Zhe Li and Peter van Loock. Memoryless quantum repeaters based on cavity-qed and coherent states. *Advanced Quantum Technologies*, 6(8):2200151, 2023.

[294] E. Agudelo, J. Sperling, L. S. Costanzo, M. Bellini, A. Zavatta, and W. Vogel. Conditional hybrid nonclassicality. *Phys. Rev. Lett.*, 119:120403, Sep 2017.