International Centre
for Theory of Quantum
Technologies

Information Processing Tasks as a Toolbox for Quantum Information

A thesis submitted by

Chithra Raj

for the title of Doctor of Philosophy (PhD)

Supervisors: dr . hab. Marcin Pawłowski, prof. UG,
dr. Pedro Ruas Dieguez

Faculty of Mathematics, Physics and Informatics
University of Gdańsk
2025

Acknowledgements

Looking back, this journey has been filled with unexpected turns, small victories, doubts, and discoveries. Completing this thesis would not have been possible without the many people who supported me along the way.

I am deeply grateful to my supervisor, Marcin Pawłowski, and co-supervisor, Pedro R. Dieguez, for their guidance, patience, and belief in me. Their encouragement and stimulating discussions shaped my growth as a researcher. I also thank my current group leader, Michał Studziński, for his understanding and support while I was completing this thesis.

To my collaborators and dear friends Tushita, Lucas, and Anubhav, thank you for the inspiration, encouragement, and shared moments of discovery, and for being the brilliant minds you are! I am especially grateful to Ankit for reading my thesis and for his thoughtful comments. My friends from ICTQT: Marco, Paweł, Beata, Vinicius, Bel, John, Some, Ekta, Anuradha, Baldi, Sumit, Amrapali, Matthias, Amanda, Sina, Robin and Abhyoudai, you all brought warmth even to the hardest days, whether over quick coffees, dinners, evenings at pubs, or much-needed venting sessions.

I would also like to thank Marta, Ewa, Gosia, Magda, and Krzysztof for their administrative support and good humour, which made navigating paperwork and deadlines much easier.

To my friends outside work: Lalitha, Athulya, Malavika, Siva, Arun, Evelyn, Aishwarya, Vidya, Akhil and Maneesh, thank you for grounding me and reminding me of life beyond research. To Misha, Merin, Shona, Abi, and Nikhil, I am grateful for your support and for making me feel at home while I focused on finishing this thesis.

Above all, I owe everything to my family. To my parents, Sindhu and Raju, my brothers, Adarsh and Akshay, and my cousin, Gopika: your love, patience, and unwavering confidence carried me through. This achievement is as much yours as it is mine.

This thesis is not only the product of years of research, but also of the experiences, friendships, and support that shaped it. I am deeply grateful to everyone who walked this path with me.

Dedication

To my loving parents and siblings.

****

Abstract

Quantum mechanics continues to challenge our intuitions about reality and information, while offering powerful new tools for communication and security. This thesis explores the interplay between fundamental quantum principles and their operational consequences, weaving together three interrelated threads: device-independent cryptography, semi-device-independent interferometry, and the nature of wave-particle complementarity.

We begin by examining the principle of information causality. Originally proposed to capture the limits of quantum nonlocality without relying on the full formalism of quantum theory, information causality provides profound insights into the security of quantum communication. We show that a multipartite formulation of this principle naturally leads to strong monogamy relations for the violation of Bell inequalities. These relations guarantee the security of device-independent quantum key distribution against individual attacks, even from a potentially post-quantum eavesdropper. In contrast, the simpler bipartite formulation fails to provide such guarantees, highlighting the essential role of multipartite correlations.

Building on this, we investigate wave-particle duality in a semi-device-independent framework. By connecting complementary interferometric quantities, namely visibility and input distinguishability, to entropic measures with direct operational meaning, we develop a method to certify quantum behaviour and security from observable interference patterns. Applying symmetry conditions and exploring tunable interferometers, we identify scenarios where classical bounds are violated and secure communication can be established. These theoretical insights are confirmed through a proof-of-principle experiment using orbital-angular-momentum encoded photons, and an improved security bound expands the parameter region for a reliable semi-device-independent certification.

Finally, we turn to the foundations of quantum realism through delayed-choice experiments. By modifying the causal structure and introducing entanglement-assisted control, we trace how wave and particle properties emerge throughout the interferometer. Using a contextual realism quantifier, we show that the assignment of wave or particle characteristics depends sensitively on the causal order and the available information, even when the final interference visibility remains unchanged.

Together, these investigations illuminate the deep connections between quantum correlations, operational constraints, and the nature of reality. They demonstrate how principles such as information causality and semi-device-independent security are rooted in fundamental features of quantum mechanics, and how causal and contextual structures shape the expression of wave-particle complementarity. This work bridges theory and experiment, offering a richer understanding of both the operational and the conceptual aspects of the quantum world.

Abstrakt

Mechanika kwantowa nadal podważa nasze intuicyjne wyobrażenia o rzeczywistości i informacji, oferując jednocześnie potężne nowe narzędzia komunikacji i bezpieczeństwa. Niniejsza praca bada wzajemne oddziaływanie fundamentalnych zasad kwantowych i ich konsekwencji operacyjnych, łącząc trzy powiązane ze sobą wątki: kryptografię niezależną od urządzenia, interferometrię półniezależną od urządzenia oraz naturę komplementarności falowo-cząsteczkowej.

Zaczynamy od zbadania zasady przyczynowości informacji. Pierwotnie zaproponowana w celu uchwycenia ograniczeń nielokalności kwantowej bez polegania na pełnym formalizmie teorii kwantowej, przyczynowość informacji zapewnia głęboki wgląd w bezpieczeństwo komunikacji kwantowej. Pokazujemy, że wieloczęściowe sformułowanie tej zasady w naturalny sposób prowadzi do silnych relacji monogamicznych w przypadku naruszenia nierówności Bella. Relacje te gwarantują bezpieczeństwo niezależnej od urządzeń kwantowej dystrybucji kluczy przed indywidualnymi atakami, nawet ze strony potencjalnego podsłuchującego w erze postkwantowej. Natomiast prostsze sformułowanie dwuczęściowe nie zapewnia takich gwarancji, co podkreśla istotną rolę korelacji wieloczęściowych.

Opierając się na tym, badamy dualizm falowo-cząsteczkowy w ramach modelu półniezależnego od urządzenia. Łącząc uzupełniające się wielkości interferometryczne, a mianowicie widoczność i rozróżnialność wejściową, z miarami entropii o bezpośrednim znaczeniu operacyjnym, opracowujemy metodę certyfikacji zachowań kwantowych i bezpieczeństwa na podstawie obserwowalnych wzorów interferencyjnych. Stosując warunki symetrii i badając interferometry z możliwością strojenia, identyfikujemy scenariusze, w których naruszane są granice klasyczne i można ustanowić bezpieczną komunikację. Te teoretyczne spostrzeżenia są potwierdzone przez eksperyment potwierdzający zasadę działania z wykorzystaniem fotonów zakodowanych orbitalnym momentem pędu, a ulepszona granica bezpieczeństwa rozszerza obszar parametrów dla niezawodnej certyfikacji półniezależnej od urządzenia.

Na koniec zwracamy się ku podstawom realizmu kwantowego poprzez eksperymenty z opóźnionym wyborem. Modyfikując strukturę przyczynową i wprowadzając kontrolę wspomaganą splątaniem, śledzimy, w jaki sposób właściwości fal i cząstek pojawiają się w interferometrze. Wykorzystując kwantyfikator realizmu kontekstowego, pokazujemy, że przypisanie właściwości fal lub cząstek zależy w sposób wrażliwy od porządku przyczynowego i dostępnych informacji, nawet jeśli ostateczna widoczność interferencji pozostaje niezmieniona.

Wszystkie te badania rzucają światło na głębokie powiązania między korelacjami kwantowymi, ograniczeniami operacyjnymi i naturą rzeczywistości. Pokazują one, w jaki sposób zasady takie jak przyczynowość informacyjna i bezpieczeństwo niezależne od urządzeń są zakorzenione w fundamentalnych cechach mechaniki kwantowej oraz w jaki sposób struktury przyczynowo-kontekstowe kształtują wyrażenie komplementarności falowo-cząsteczkowej. Praca ta łączy teorię z eksperymentem, oferując bogatsze zrozumienie zarówno operacyjnych, jak i

koncepcyjnych aspektów świata kwantowego.

Manuscripts included in the dissertation

Peer-reviewed

[1] Pollyceno, L., Chaturvedi, A., Raj, C., Dieguez, P. R. (2025). Security of device-independent quantum-key distribution via monogamy relations from multipartite information causality.
DOI: https://doi.org/10.1103/jnng-m87v
Accepted in Physical Review A.

[2] Raj, C., Dieguez, P. R. (2025). Wave-Particle Realism in Quantum-Controlled Interferometers Assisted by Entanglement. Open Systems & Information Dynamics, 32(02), 2550009.
https://doi.org/10.1142/S123016122550009X

Pre-prints

[3] Raj, C., Prasad, T., Chaturvedi, A., Pollyceno, L., Spegel-Lexne, D., Gómez, S., Argillander, J., Alarcón A., Xavier, G. B., Pawłowski, M., Dieguez, P. R. (2025). Certifying semi-device-independent security via wave-particle duality experiments.
https://arxiv.org/pdf/2507.00679
Under review in npj Quantum Information.

List of Abbreviations

$\mathcal{IC}$ Information Causality vi

CHSH Clauser-Horne-Shimony-Holt vi

CPTP Completely Positive Trace-Preserving vi

DI Device-Independent vi

DIQKD Device-Independent Quantum Key Distribution vi

EPR Einstein-Podolsky-Rosen vi

EUR Entropic Uncetainity Relations vi

FMF Few-Mode Fiber vi

LHV Local Hidden Variable vi

LOSR Local Operations and Shared Randomness vi

MZI Mach-Zehnder Interferometer vi

OAM Orbital Angular Momentum vi

PL Photonic Lantern vi

PM Prepare-and-Measure vi

POVM Positive Operator-Valued Measure vi

PR Popescu-Rohrlich vi

QGG Quantum Guessing Game vi

QKD Quantum Key Distribution vi

QRAC Quantum Random Access Code vi

RAC Random Access Code vi

SDI Semi-Device-Independent vi

SDIQKD Semi-Device-Independent Quantum Key Distribution vi

TBS Tunable Beam Splitter vi

WPD Wave Particle Duality vi

Table of Contents

List of Figures

Figure **Page**

Chapter 1

Introduction and Background

"There is nothing to writing. All you do is sit down at the typewriter and bleed."

—Ernest Hemingway

From the earliest days of human civilization, secrecy has been a matter of survival, power, and trust. The Spartans developed the *scytale*, a simple transposition cipher using a wooden rod to scramble letters, while Julius Caesar used substitution ciphers to protect military communications. These early schemes were crude, often broken through guesswork or persistence, yet they show that long before the digital age, people recognized the power of shaping and disguising information.

The first real breakthrough in understanding secrecy came much later. In 1917, Gilbert Vernam patented the one-time pad [4], a cipher that, when combined with Claude Shannon's theory of information [5], was shown to provide perfect secrecy. Shannon proved that if two parties share a random key as long as the message, and if the key is used only once, then the encrypted message reveals nothing to an eavesdropper, even one with unlimited computational resources. Yet this absolute security came at a steep cost: distributing long, truly random keys securely was nearly impossible.

For decades, cryptography turned to mathematics for a compromise. Public key schemes such as RSA [6] and Diffie–Hellman key exchange [7] relied on problems believed to be hard, like factoring large integers or computing discrete logarithms. These protocols built the backbone of modern digital security. However, this security was always conditional: if the mathematical problem turned out to be easier than assumed, the system would collapse. Shor's discovery in 1994, that a quantum computer could factor efficiently [8], exposed the fragility of this foundation. Once large-scale quantum computers are built, much of the world's cryptography will be at risk.

Ironically, the same physics that threatens classical cryptography also offers a way out. Quantum mechanics, with its no-cloning theorem [9] and the unavoidable disturbance caused by measurement [10], provides new tools to protect information. In the 1980s, Bennett and Brassard proposed the BB84 protocol [11], showing that quantum states could distribute secret keys securely. A few years later, Ekert's entanglement-based scheme (E91) [12] made the connection to Bell's theorem explicit, linking the violation of Bell inequalities to the security of key distribution. These protocols gave birth to quantum key distribution (QKD), a field that has since grown from table-top demonstrations to continental-scale networks [13–15] and even satellite-based implementations that hint at global quantum communication [16, 17].

At the same time, the conceptual puzzles of quantum theory began to reappear in new light. When Einstein, Podolsky, and Rosen (EPR) published their critique of quantum mechanics in 1935 [18], they raised the question of whether the theory was complete. Bohr [19] countered that quantum correlations reflected a departure from classical ideas of separability and reality. Bell's theorem in 1964 [20] showed that no local hidden-variable (LHV) theory could reproduce all quantum predictions, and the experiments of Aspect in the 1980s [21], followed by loophole-free tests in 2015 [22–24], confirmed that nature truly violates Bell inequalities. What began as a debate over the completeness of quantum mechanics became the foundation for practical cryptographic protocols.

These developments gave rise to the idea of device-independent (DI) cryptography, where security is certified not by trusting the internal design of devices but by observing correlations that violate Bell inequalities [25, 26]. This represents a radical shift: the sender Alice and the receiver Bob need not know how their devices work, or even whether they were constructed by an adversary. If the observed statistics are nonlocal enough, secrecy is guaranteed by the structure of quantum theory itself.

Still, full device-independence remains experimentally demanding, requiring near-perfect detectors and high-quality entanglement [27–29]. This led to the semi-device-independent (SDI) framework, where weaker assumptions replace the need for complete device independence [30–32]. Typically, these assumptions concern the dimension of the underlying system, which is easier to control in the laboratory. SDI protocols often take the form of prepare-and-measure (PM) games, where witnesses built from observable statistics separate classical from quantum strategies. This middle ground between full trust and full distrust makes SDI approaches both practical and conceptually rich.

Parallel to these advances in cryptography, other features of quantum mechanics have been reframed as operational resources. The wave–particle duality (WPD) explored by Bohr and later quantified by Englert [33] demonstrates that a quantum system cannot display full interference visibility and full path distinguishability simultaneously. Experiments in Mach–Zehnder interferometers (MZI) [34, 35] and quantum erasure setups [36, 37] have confirmed this complementarity across different platforms. Similarly, the uncertainty principle has been recast

in information-theoretic terms. Maassen and Uffink [38] showed that the sum of entropies of measurement outcomes has a universal lower bound, while Berta et al. [39] demonstrated how entanglement with quantum memory alters this limit. Entropic uncertainty relations (EURs) now form the backbone of modern security proofs [40–42], linking unpredictability directly to cryptographic secrecy.

Even the long-standing debate over realism has entered the operational realm. EPR argued for hidden elements of reality [18], Bohr rejected the idea [19], and later theorems by Bell [20] and Kochen–Specker [43] ruled out local or noncontextual hidden-variable models. Recent work has gone further by defining and quantifying realism itself [44, 45], turning what was once a philosophical dispute into a measurable resource.

Amid these perspectives, researchers have also sought guiding principles that could explain why quantum correlations look the way they do. Information causality ($\mathcal{IC}$) was proposed as one such principle [46], showing that although stronger-than-quantum correlations like Popescu–Rohrlich (PR) boxes [47] respect no-signaling, they would permit unlimited information transfer and therefore must be excluded. Closely related are monogamy relations, which state that if two parties are maximally correlated in a nonlocal way, quantum mechanics strictly forbids any third party from sharing those correlations [48, 49]. These principles not only clarify the boundary between the quantum and the post-quantum but also connect directly to cryptographic security. Recent extensions of $\mathcal{IC}$ to multipartite scenarios [50] strengthen these connections, revealing new forms of monogamy that guarantee security in device-independent quantum key distribution (DIQKD).

This thesis is structured to follow the progression of these ideas, moving from principles to protocols to experiments, and showing at each step how information processing tasks provide insight into the limits and possibilities of quantum mechanics.

We begin in Chapter 2 by laying out the necessary preliminaries. The central mathematical tools are introduced: DI and SDI frameworks, Bell inequalities and PM scenarios, dimension witnesses, and the entropic quantities used to formalize uncertainty. We also define the realism quantifier that will later allow us to track the emergence of wave- and particle-like behaviour in interferometric experiments. This chapter establishes the notation and operational background against which the rest of the thesis unfolds.

Chapter 3 develops the first major theme: the principle of $\mathcal{IC}$. While the original principle was proposed in a bipartite setting [46], our focus is on its multipartite generalization[50]. We show that this richer formulation leads to nontrivial monogamy relations for the Clauser–Horne–Shimony–Holt (CHSH) inequality [51]. These monogamy constraints exclude correlations that would be allowed by NS but are forbidden by $\mathcal{IC}$, and they provide direct security guarantees for DIQKD. Importantly, we prove that while bipartite $\mathcal{IC}$ fails to enforce these monogamy conditions, the multipartite form recovers the full quantum behaviour: when two parties observe a maximal CHSH violation, multipartite $\mathcal{IC}$ ensures that no third party can share such

correlations. This chapter thus connects a foundational information-theoretic principle with a concrete operational consequence in cryptography: the security of DIQKD.

In Chapter 4, we turn to the SDI setting, where assumptions about system dimension replace the strict requirements of DIQKD. We explore how WPD provides a natural operational foundation for SDI protocols. Starting from the MZI as a canonical setup, we connect duality quantities, interferometric visibility and input distinguishability, to SDI witnesses constructed from PM scenarios. We show how these witnesses can be rewritten in terms of interferometric parameters, making the cryptographic framework directly accessible to experiments. We then develop an entropic reformulation, where min-entropy and max-entropy quantify the unpredictability and uniformity of outcomes in terms of distinguishability and visibility. This establishes a clear bridge between EURs [38, 39, 42] and interferometric complementarity. Finally, we present an improved security bound in the SDI setting, refining earlier results [30] and enlarging the parameter region where security can be certified. These theoretical results are supplemented by a proof-of-principle experiment using orbital-angular-momentum encoded photons, which confirms the feasibility of our approach in practice.

Chapter 5 addresses the theme of realism and delayed-choice experiments. Building on Wheeler's proposal of a delayed-choice interferometer [52], we study how wave- and particle-like behaviour emerges under different causal structures. We extend this to entanglement-assisted delayed-choice scenarios, where the decision to insert or remove the final beamsplitter is controlled by a quantum system. By employing a contextual realism quantifier [44, 45], we show that the assignment of "wave" or "particle" properties depends sensitively on causal order and information availability, even when the final interference visibility remains unchanged. This analysis reveals that realism in quantum mechanics is not an absolute attribute but a contextual and dynamic property, shaped by the flow of information in the experiment.

Finally, Chapter 6 summarizes the contributions and situates them within the broader field. We emphasize how the multipartite formulation of $\mathcal{IC}$ provides security guarantees in the DI regime, how WPD and entropy link naturally to SDI security, and how realism can be operationally probed in delayed-choice experiments. Together, these results demonstrate that information processing tasks form a powerful toolbox for both foundational insights and practical protocols in quantum information.

Chapter 2

Preliminaries

"How strange that nature does not knock, and yet does not intrude!."

—Emily Dickinson

This chapter presents the conceptual and structural foundations that underpin the discussions in the subsequent chapters. While this thesis is rooted in quantum information theory, the emphasis here is on the foundational assumptions and physical principles that govern quantum correlations and their applications in communication and cryptography. In particular, we address the role of nonlocality and entanglement, the assumptions behind Bell-type arguments, and the constraints imposed by physical principles such as no-signaling and information causality ($\mathcal{IC}$), the wave-particle duality (WPD), its connections to entropic uncertainity relations (EURs), and applications in communication tasks. Towards the end of this chapter, we will be positioned to follow the development of the results presented in this thesis, alongwith a sound understanding of both the physical and information-theoretic context in which they are situated.

2.1 Mathematical Framework of Quantum Theory

This section introduces the mathematical formalism of quantum theory required for subsequent discussions in quantum communication and cryptography. We present the structure of quantum states, measurements, dynamics, and channels, following standard treatments in information theory [53, 54].

2.1.1 Quantum States

The state of a finite-dimensional quantum system is described by a density operator $\rho \in \mathcal{L}(\mathcal{H})$, where $\mathcal{H}$ is a complex Hilbert space. The set of valid quantum states is given by:

$$\mathcal{D}(\mathcal{H}) = \{\rho \in \mathcal{L}(\mathcal{H}) \,|\, \rho \geq 0,\ \mathrm{Tr}[\rho] = 1\}\,. \tag{2.1}$$

Pure states are represented as rank-one projectors $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle \in \mathcal{H}$ is a unit vector. Mixed states are convex combinations of pure states and reflect classical uncertainty about the preparation [53].

2.1.2 Observables and Measurements

Physical observables are associated with Hermitian operators $A \in \mathcal{L}(\mathcal{H})$, with spectral decomposition:

$$A = \sum_a a P_a, \tag{2.2}$$

where $a \in \mathbb{R}$ are eigenvalues and $\{P_a\}$ are orthogonal projectors. A more general framework for measurements is given by positive operator-valued measures (POVMs), defined as a set $\{M_a\}$ of positive semidefinite operators satisfying:

$$M_a \geq 0, \quad \sum_a M_a = \mathbb{I}. \tag{2.3}$$

The probability of obtaining outcome a on input state ρ is given by Born's rule: $P(a) = \mathrm{Tr}[M_a\rho]$ [53, 54].

Projective (von Neumann) measurements are a special case of POVMs where each M_a is an orthogonal projector, satisfying $M_aM_b = \delta_{ab}M_a$.

2.1.3 Composite Systems and Tensor Products

For multipartite quantum systems, the overall state space is described by the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$. Given a bipartite state ρ_{AB}, the reduced state on subsystem A is obtained by partial trace: $\rho_A = \mathrm{Tr}_B[\rho_{AB}]$ [53].

Product states have the form $\rho_{AB} = \rho_A \otimes \rho_B$. States that cannot be written as convex combinations of product states are *entangled*, a central resource in information processing tasks in quantum cryptography.

2.1.4 Unitary Evolution

In closed quantum systems, the time evolution is governed by a unitary operator U, i.e., $U^\dagger U = \mathbb{I}$. The state evolves as:

$$\rho \mapsto U\rho U^\dagger.$$

Such unitary evolution is a special case of a more general quantum operation known as completely positive trace-preserving (CPTP) maps [54].

2.1.5 Quantum Channels and CPTP Maps

The most general physical evolution of a quantum system, possibly interacting with an environment, is described by a quantum channel. A quantum channel $\mathcal{E}$ is a CPTP map:

$$\mathcal{E} : \mathcal{L}(\mathcal{H}_{\text{in}}) \to \mathcal{L}(\mathcal{H}_{\text{out}}). \tag{2.4}$$

By the Kraus representation theorem [55], such a map admits a decomposition:

$$\mathcal{E}(\rho) = \sum_i K_i \rho K_i^\dagger, \quad \sum_i K_i^\dagger K_i = \mathbb{I}, \tag{2.5}$$

where $\{K_i\}$ are Kraus operators. Quantum channels describe noise, open-system dynamics, and measurement processes [56]. Examples include:

- *Unitary channels:* $\mathcal{E}(\rho) = U\rho U^\dagger$,
- *Depolarizing channels:* $\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{d}\mathbb{I}$,
- *Measurement channels:* where the output is classical data.

2.1.6 Distance Measures and Fidelity

In quantum cryptography, it is crucial to quantify how distinguishable two quantum states are. The trace distance between two states ρ and σ is defined as:

$$D(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_1, \tag{2.6}$$

where $\|A\|_1 = \text{Tr}[\sqrt{A^\dagger A}]$ denotes the trace norm. The trace distance has an operational interpretation as the maximum probability of distinguishing ρ from σ with a single measurement [54].

The fidelity between ρ and σ, first studied by Uhlmann [57] and later by Jozsa [58], is given by:

$$F(\rho, \sigma) = \left(\text{Tr}\left[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right]\right)^2. \tag{2.7}$$

For pure states $|\psi\rangle, |\phi\rangle$, this simplifies to their overlap $|\langle\psi|\phi\rangle|^2$. Fidelity measures closeness, and is frequently used in security analyses and entanglement verification.

2.2 Some peculiar features of quantum theory

Quantum theory departs radically from classical intuitions about the physical world. This divergence manifests not only in the structure of quantum states, but also in the correlations they permit, and the inferences they forbid. Some features are especially significant in quantum cryptography:

1. *Entanglement*, which enables correlations between space-like separated systems that defy classical explanation;
2. *Nonlocality*, whereby measurement outcomes exhibit statistical dependencies that violate local realism;
3. *Monogamy of entanglement and nonlocality*, which ensures that quantum correlations cannot be freely shared among multiple parties, thereby securing the exclusivity of quantum links;
4. *Realism and the implications of no-go theorems*, which underline the impossibility of reconciling quantum predictions with certain classes of realist interpretations;
5. *WPD as revealed in the Mach–Zehnder interferometer (MZI)*, which highlights the complementary nature of interference and path information, illustrating the limits of classical descriptions of physical systems.

Each of these phenomena illustrates a distinctive way in which quantum mechanics resists assimilation into classical frameworks. Together they provide both the conceptual challenges and the operational resources that shape the design of quantum protocols, particularly in cryptography where security relies directly on the fundamental peculiarities of quantum theory. This section lays out these features with mathematical rigor and positions them in the context of quantum communication and cryptographic protocol design.

2.2.1 Entanglement

Entanglement is one of the most profound and non-classical features of quantum theory. It refers to correlations between subsystems of a composite quantum system that cannot be accounted for by classical statistics. Mathematically, a pure bipartite state $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ is said to be entangled if it cannot be written as a product state $|\psi\rangle_A \otimes |\phi\rangle_B$. For mixed states ρ_{AB}, the state is entangled if it is not separable, i.e., cannot be expressed as a convex combination of product states:

$$\rho_{AB} \neq \sum_i p_i \rho_A^{(i)} \otimes \rho_B^{(i)}, \tag{2.8}$$

where $p_i \geq 0$, $\sum_i p_i = 1$, and $\rho_A^{(i)}$, $\rho_B^{(i)}$ are density operators on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively [59].

A fundamental tool for analyzing pure bipartite entanglement is the Schmidt decomposition. Any pure state $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ can be written as:

$$|\psi\rangle_{AB} = \sum_{i=1}^{r} \lambda_i |e_i\rangle_A \otimes |f_i\rangle_B , \tag{2.9}$$

where $\{|e_i\rangle_A\}$ and $\{|f_i\rangle_B\}$ are orthonormal sets in $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, $\lambda_i \geq 0$, and $\sum_i \lambda_i^2 = 1$. The number r, known as the Schmidt rank, characterizes the entanglement of the state: the state is entangled if $r > 1$ [53].

For mixed states, the problem of detecting entanglement is more subtle. Several operational criteria exist, such as the Peres-Horodecki criterion, which states that for $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, a necessary condition for separability is that its partial transpose $\rho_{AB}^{T_B}$ remains positive semidefinite [60, 61].

Quantifying entanglement is crucial in quantum information. One of the most widely used measures for pure states is the von Neumann entropy of the reduced density matrix:

$$E(|\psi\rangle_{AB}) = S(\rho_A) = -\mathrm{Tr}[\rho_A \log \rho_A], \tag{2.10}$$

where $\rho_A = \mathrm{Tr}_B[|\psi\rangle_{AB} \langle\psi|]$. For mixed states, entanglement measures such as entanglement of formation, concurrence, and negativity are commonly used, though each comes with its own operational interpretation and computational challenges [62].

Entanglement serves as a resource in many quantum information protocols, including quantum teleportation [63], dense coding [64], and entanglement-based quantum key distribution (QKD) [12]. In cryptographic contexts, entanglement provides correlations that cannot be simulated by shared randomness or classical means, enabling security against powerful adversaries with access to quantum systems.

Furthermore, in the context of device-independent (DI) cryptography, the presence of entanglement certified via Bell inequality violations serves as the basis for ensuring security even when the internal workings of devices are untrusted [25]. Thus, entanglement is not merely a conceptual novelty but a fundamental tool for constructing secure quantum communication systems.

2.2.2 Quantum Nonlocality

Nonlocality refers to the phenomenon wherein spatially separated quantum systems exhibit correlations that cannot be explained by any local hidden variable (LHV) theory. Unlike entanglement, which is a property of quantum states, nonlocality is a feature of correlations observed in measurement outcomes, and its presence is typically revealed via violations of Bell-type inequalities.

Consider a bipartite scenario with two spatially separated parties, Alice and Bob, who choose inputs $x, y \in \mathcal{X}, \mathcal{Y}$ and receive outcomes $a, b \in \mathcal{A}, \mathcal{B}$, respectively. A joint probability

distribution $P(a, b|x, y)$ is said to admit a local hidden variable model if it can be expressed as:

$$P(a, b|x, y) = \int_\lambda \mathrm{d}\lambda\, \mu(\lambda) P_A(a|x, \lambda) P_B(b|y, \lambda), \tag{2.11}$$

where λ is a shared classical variable with distribution $\mu(\lambda)$, and P_A, P_B are local response functions [65, 66].

One of the most studied Bell inequalities is the CHSH inequality [51], which involves binary inputs $x, y \in \{0, 1\}$ and binary outcomes $a, b \in \{0, 1\}$. Defining the CHSH parameter as:

$$S = \sum_{x,y=0}^{1} (-1)^{xy} \langle A_x B_y \rangle, \tag{2.12}$$

where $\langle A_x B_y \rangle = \sum_{a,b} (-1)^{a \oplus b} P(a, b|x, y)$, the CHSH inequality states that $|S| \leq 2$ for any LHV theory. However, quantum mechanics permits correlations such that:

$$|S| \leq 2\sqrt{2}, \tag{2.13}$$

known as the Tsirelson bound [67], achieved by measurements on the maximally entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. This inequality reflects the fundamental tension between local realism and quantum predictions: while classical theories impose strict bounds on correlations, quantum mechanics allows stronger correlations that violate this bound, as originally demonstrated by Bell [65] and experimentally verified in many subsequent works [21–24].

Game Formulation. The CHSH scenario can also be expressed as a two-player nonlocal game. In each round, Alice and Bob receive random inputs $x, y \in \{0, 1\}$ and produce outputs $a, b \in \{0, 1\}$ without communicating. They win whenever their outputs satisfy

$$a \oplus b = x \cdot y,$$

where $\oplus$ denotes addition modulo 2. The average winning probability is

$$\beta(\mathcal{A}, \mathcal{B}) = \frac{1}{4} \sum_{x,y} P(a \oplus b = xy \mid x, y) \leq \frac{3}{4}. \tag{2.14}$$

For classical LHV models, the maximum winning probability is bounded by $\beta \leq 3/4$, equivalent to the inequality $|S| \leq 2$. Quantum mechanics, however, allows a higher success probability, reaching the Tsirelson limit

$$\beta_Q = \tfrac{1}{2}\left(1 + \tfrac{1}{\sqrt{2}}\right) \approx 0.8535,$$

achieved by measurements on a maximally entangled state, which is equivalent to (2.13). Beyond quantum theory, no-signaling correlations can reach the algebraic maximum $\beta_{NS} = 1$.

This game-based formulation highlights the operational significance of CHSH: the violation directly corresponds to a higher-than-classical winning probability. Moreover, such nonlocal correlations exhibit *monogamy*, a key feature that underlies their applications in DI cryptography.

These nonlocal correlations cannot be reproduced by any classical mechanism that respects locality and realism, demonstrating the fundamental departure of quantum theory from classical intuitions. Notably, such correlations also obey the no-signaling condition, i.e.,

$$\sum_b P(a,b|x,y) = P(a|x), \quad \forall y, \tag{2.15}$$

ensuring that the choice of Bob's measurement setting y cannot influence Alice's marginal distribution $P(a|x)$ [47].

In cryptographic contexts, Bell inequality violations are employed to certify security in DIQKD [25, 26]. Here, the presence of nonlocality implies the generation of intrinsically private randomness, independent of the internal structure of the measurement devices. This device-independence makes Bell tests central to protocols where one cannot trust the internal functioning of the devices used to prepare and measure quantum states.

From an information-theoretic perspective, nonlocal correlations are also constrained by principles such as $\mathcal{IC}$ [46], which limit the strength of admissible correlations to those consistent with quantum mechanics, excluding stronger but unphysical no-signaling correlations. Such principles help delineate the boundary between classical, quantum, and post-quantum correlations, providing insight into why quantum theory achieves exactly the level of nonlocality it does.

Overall, the CHSH scenario not only illustrates the incompatibility between local realism and quantum predictions but also serves as a cornerstone for modern quantum information theory. Its dual role, both as a fundamental test of quantum foundations and as a practical tool for certifying security, makes it a central object of study in the interface between physics and information.

2.2.3 Monogamy of Entanglement and Nonlocality

One of the most critical structural features of quantum correlations is their *monogamous* nature. Unlike classical correlations, which can be freely shared among many parties, quantum entanglement obeys a strict trade-off: if two systems are maximally entangled, they cannot be entangled with a third. This feature is central to the security of many quantum cryptographic tasks, as it limits the amount of quantum information an eavesdropper can possess.

Mathematically, monogamy is often quantified using entanglement measures such as the tangle τ, where for three qubits A, B, C, the Coffman-Kundu-Wootters (CKW) inequality [68] reads:

$$\tau_{A|BC} \geq \tau_{A|B} + \tau_{A|C}. \tag{2.16}$$

This means that if qubit A is maximally entangled with B, then it cannot be entangled with C.

In nonlocality-based scenarios, an analogous principle applies: if two parties violate a Bell inequality maximally, then neither can share a strong Bell violation with a third. This was

formalized in [48, 49], where it was shown that the violation of the CHSH inequality satisfies a monogamy relation in no-signaling theories:

$$\text{CHSH}_{AB}^2 + \text{CHSH}_{AC}^2 \leq 8, \tag{2.17}$$

where CHSH_{AB} and CHSH_{AC} represent the CHSH expressions between pairs (A, B) and (A, C), respectively. This result highlights that the total "amount" of nonlocality is bounded when a single party shares entangled states with two others. Each CHSH term is bounded above by $2\sqrt{2}$ in quantum mechanics [67], but must obey this additive constraint across overlapping subsystems in all non-signaling models.

This constraint is crucial in QKD. In protocols such as DIQKD, monogamy ensures that if Alice and Bob share strong nonlocal correlations, any third party (e.g., Eve) cannot be significantly correlated with them. Thus, the observed nonlocality becomes a certificate of secrecy [25, 27].

Monogamy also underpins recent developments in multipartite settings, where stronger forms of Bell inequalities and information principles such as information causality yield generalized trade-offs among correlations across networks [69].

2.2.4 Realism and No-Go Theorems

The classical notion of realism, which assumes physical properties exist prior to measurement, is challenged by quantum mechanics. No-go theorems rigorously formalize this conflict, demonstrating that quantum predictions cannot be explained by any realistic, local, or non-contextual hidden variable models.

Realism in quantum theory posits that physical observables possess definite values prior to and independent of measurement. Formally, a hidden variable model assigns to each observable A a predetermined outcome $v(A) \in \text{Spec}(A)$, where $\text{Spec}(A)$ denotes the spectrum of A.

Bell's theorem [65] demonstrates that no LHV model can reproduce all quantum correlations. Consider a bipartite system with measurement observables A_x and B_y for settings x, y, and outcomes a, b. A local realistic model assumes the existence of a hidden variable λ with probability distribution $\rho(\lambda)$, such that joint probabilities factorize as

$$P(a, b|x, y) = \int \mathrm{d}\lambda\, \rho(\lambda) P_A(a|x, \lambda) P_B(b|y, \lambda). \tag{2.18}$$

Among the family of Bell inequalities, the CHSH inequality

$$|S| = |\langle A_0 B_0\rangle + \langle A_0 B_1\rangle + \langle A_1 B_0\rangle - \langle A_1 B_1\rangle| \leq 2, \tag{2.19}$$

is a commonly studied case. It must be satisfied by any LHV model, while quantum mechanics predicts violations up to Tsirelson's bound $2\sqrt{2}$ [67].

Beyond locality, the Kochen-Specker theorem [43] addresses non-contextual hidden variable models. Non-contextuality demands that the value assignment function v satisfies

$$v(A) = v(A, \mathcal{C}), \tag{2.20}$$

independent of the context $\mathcal{C}$, a set of compatible observables measured jointly with A. Kochen and Specker proved that for Hilbert spaces of dimension $d \geq 3$, there exists no assignment v consistent with the functional relations among observables.

Leggett-type inequalities [70] extend the no-go results to nonlocal realistic theories with constrained nonlocal correlations. Violations of these inequalities experimentally reinforce that quantum mechanics cannot be supplemented by any realistic model obeying these assumptions.

These foundational results imply that any ontological model underlying quantum mechanics must either abandon locality, realism, or non-contextuality, profoundly impacting quantum cryptography. DI protocols exploit Bell inequality violations as a certificate of quantum behaviour and intrinsic randomness, thereby guaranteeing security even when devices are untrusted [25].

2.2.5 The Mach-Zehnder Interferometric Setup and Wave–Particle Duality

The Mach–Zehnder interferometer (MZI) is a foundational optical device used to explore interference phenomena and the dual nature of quantum systems. Its basic structure consists of two beam splitters and two mirrors, forming two possible paths for a photon or qubit. When properly aligned, these paths recombine to produce interference at the output, depending on the relative phase accumulated along each path. If only one path is available, the system behaves as though it took a definite route, exhibiting *particle-like* behaviour. When both paths are open and indistinguishable, interference fringes emerge, revealing *wave-like* behaviour. In the setup of Fig. 2.1, a quantum system (typically a photon) enters the interferometer and is first incident on the beam splitter BS_1, which coherently splits the input state into two distinct paths. For a balanced (50:50) beam splitter, this is equivalent to applying a Hadamard gate H to the initial state $|0\rangle$:

$$|0\rangle \xrightarrow{BS_1} H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right). \tag{2.21}$$

A phase shifter PS in one path introduces a relative phase ϕ:

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \xrightarrow{PS} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\phi}|1\rangle\right). \tag{2.22}$$

The paths are then recombined at BS_2 (also acting as H), producing the final state:

$$H\left(\frac{|0\rangle + e^{i\phi}|1\rangle}{\sqrt{2}}\right) = \frac{1}{2}\left[(1 + e^{i\phi})|0\rangle + (1 - e^{i\phi})|1\rangle\right]. \tag{2.23}$$

Measurement in the computational basis yields detection probabilities:

$$p_0 = \cos^2\left(\frac{\phi}{2}\right), \quad p_1 = \sin^2\left(\frac{\phi}{2}\right), \tag{2.24}$$

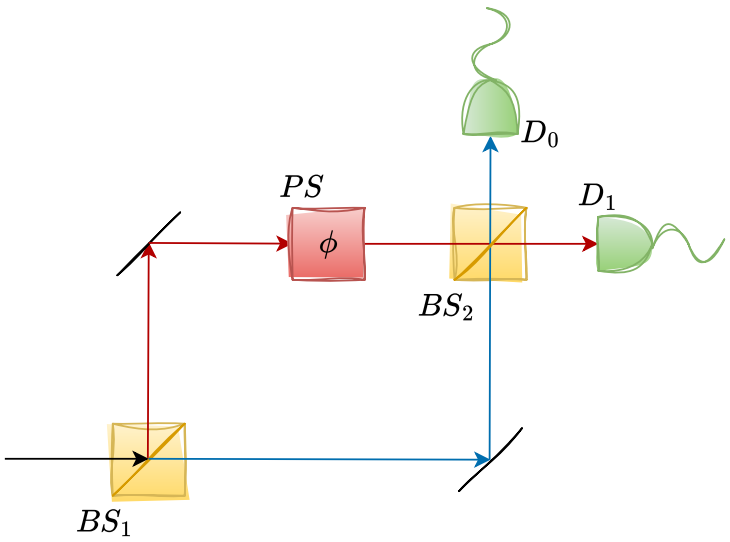

Figure 2.1: **Schematic of the MZI**. A quantum system (e.g. a photon) enters at the input and is split coherently by the first beam splitter (BS_1) into two possible paths. A phase shifter (PS) in one arm introduces a controllable phase ϕ. The paths are then recombined at the second beam splitter (BS_2), and the outputs are measured at detectors D_0 and D_1.

at the respective detectors D_0 and D_1, and these probabilities oscillate with ϕ, producing an interference pattern.

Visibility and Path Distinguishability. The *visibility* $\mathcal{V}$ of the interference pattern, quantifying the wave-like nature, is given by

$$\mathcal{V} = \frac{p_0^{\max} - p_0^{\min}}{p_0^{\max} + p_0^{\min}}, \tag{2.25}$$

where $p_0^{\max}$ and $p_0^{\min}$ are the maximum and minimum values of p_0. For a balanced BS_1, $\mathcal{V} = 1$. If BS_1 is unbalanced, with transmissivity T and reflectivity R ($T + R = 1$), the visibility becomes

$$\mathcal{V} = \frac{2TR}{T^2 + R^2}, \tag{2.26}$$

decreasing as the balance is skewed. A fully unbalanced splitter ($T = 1$ or $R = 1$) yields $\mathcal{V} = 0$.

The *path distinguishability* $\mathcal{D}$, quantifying particle-like behaviour, is the maximal bias for correctly guessing the taken path. Following [40]:

$$\mathcal{D} = |p_0 - p_1|, \tag{2.27}$$

where p_0 and p_1 here denote the probabilities of the system having taken the upper or lower path, respectively. Perfect path knowledge yields $\mathcal{D} = 1$, and complete indistinguishability gives $\mathcal{D} = 0$.

In the most general quantum information-theoretic setting, $\mathcal{D}$ can be defined as the trace distance between the states ρ_0 and ρ_1 of an ideal which-path detector [33]:

$$\mathcal{D} = \frac{1}{2}\|\rho_0 - \rho_1\|_1. \tag{2.28}$$

Wave–Particle Duality and Complementarity. WPD, a cornerstone of quantum mechanics, is embodied in the complementarity between $\mathcal{V}$ and $\mathcal{D}$. For pure states, the Englert duality relation [33] holds:

$$\mathcal{D}^2 + \mathcal{V}^2 \leq 1, \tag{2.29}$$

formalising Bohr's principle: the more one knows about which path was taken, the less visible the interference fringes become. This trade-off persists in various formulations, including entropic uncertainty relations and contextuality frameworks, and has applications in quantum cryptography, where limiting an adversary's which-path knowledge ensures high interference visibility for legitimate parties [71].

Predictive and Retrodictive Scenarios. In the *predictive* scenario, the interferometer configuration (presence or absence of BS_2) is fixed before the system enters. If BS_2 is present, $\mathcal{V}$ is maximised and $\mathcal{D}$ is minimised (wave-like behaviour). If BS_2 is absent, $\mathcal{V} = 0$ and $\mathcal{D}$ is maximised (particle-like behaviour).

In the *retrodictive* scenario, the choice to insert or remove BS_2 is made *after* the particle has passed BS_1. Quantum mechanics predicts that the observed behaviour will match the final configuration regardless of when the choice is made, thereby challenging the classical view that the system had a definite wave or particle character beforehand. Instead, wave- or particle-like behaviour emerges contextually from the measurement arrangement itself.

While the trade-off between $\mathcal{D}$ and $\mathcal{V}$ provides a useful framework for capturing WPD in the MZI, it does not fully account for the role of measurement context or quantum correlations. In particular, the predictive and retrodictive scenarios emphasize that the degree to which a system exhibits wave-like or particle-like properties depends on when and how information is accessed. This suggests the need for a more general formalism, one that treats the notions of "wave realism" and "particle realism" on the same footing and extends beyond the $\mathcal{D}$-$\mathcal{V}$ relation.

To address this, we adopt an information-theoretic approach based on the quantification of realism introduced in Refs. [44, 45]. This framework allows us to rigorously define the degree of reality associated with different observables and to explore how quantum correlations influence wave–particle complementarity.

2.2.5.1 Quantifying Wave and Particle Realism

In order to study the interplay of wave-like and particle-like behaviour in quantum-controlled interferometers, we make use of a quantifier of realism proposed in Refs. [44, 45]. The central

idea is that when a projective measurement is performed on a discrete-spectrum observable $\mathcal{A} = \sum_a a\mathcal{A}_a$, with projectors $\mathcal{A}_a = |a\rangle\langle a|$ acting on a Hilbert space $\mathcal{H}_\mathcal{A}$, the corresponding property of $\mathcal{A}$ acquires an element of "reality." This remains true even if the actual measurement result is not disclosed. Formally, the post-measurement state representing the establishment of such realism is

$$\Phi_\mathcal{A}(\varrho) := \sum_a (\mathcal{A}_a \otimes \mathbb{I})\varrho(\mathcal{A}_a \otimes \mathbb{I}),$$

where ϱ denotes the density operator of a bipartite system defined on $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$. Within this framework, $\Phi_\mathcal{A}(\varrho)$ serves as the reference state encoding $\mathcal{A}$-realism [45, 72].

The realism associated with an observable $\mathcal{A}$ for a given state ρ is quantified by

$$R_\mathcal{A}(\rho) := \log_2 d_\mathcal{A} - \mathfrak{I}_\mathcal{A}(\rho), \tag{2.30}$$

where $d_\mathcal{A} = \dim \mathcal{H}_\mathcal{A}$ and $\mathfrak{I}_\mathcal{A}(\rho)$, termed the *irrealism*, is defined as

$$\mathfrak{I}_\mathcal{A}(\rho) := \min_\varrho S(\rho||\Phi_\mathcal{A}(\varrho)) = S(\Phi_\mathcal{A}(\rho)) - S(\rho). \tag{2.31}$$

Here $S(\rho||\sigma) = \mathrm{Tr}[\rho(\log_2\rho - \log_2\sigma)]$ is the quantum relative entropy, while $S(\rho) := \mathrm{Tr}(\rho\log_2\rho)$ denotes the von Neumann entropy. The irrealism of the pair $\{\mathcal{A}, \rho\}$ is always bounded by $0 \leq \mathfrak{I}_\mathcal{A}(\rho) \leq \log_2 d_\mathcal{A}$, vanishing precisely when $\rho = \Phi_\mathcal{A}(\rho)$, i.e., when ρ is already an eigenstate of $\mathcal{A}$.

An important connection emerges in the presence of quantum discord. For a bipartite state ρ one finds that the irrealism of $\mathcal{A}$ with respect to ρ is greater than the irrealism associated with the local reduced state $\rho_\mathcal{A} = \mathrm{Tr}_\mathcal{B}(\rho)$, namely $\mathfrak{I}_\mathcal{A}(\rho) - \mathfrak{I}_\mathcal{A}(\rho_\mathcal{A}) \geq \mathcal{D}_\mathcal{A}(\rho)$ [44]. Here $\mathcal{D}_\mathcal{A}(\rho) = \min_\mathcal{A}\left[I_{\mathcal{A}:\mathcal{B}}(\rho) - I_{\mathcal{A}:\mathcal{B}}(\Phi_\mathcal{A}(\rho))\right]$ denotes the quantum discord [73–76], and $I_{\mathcal{A}:\mathcal{B}}(\rho) = S(\rho||\rho_\mathcal{A}\otimes\rho_\mathcal{B})$ is the mutual information between subsystems.

A further property concerns pairs of maximally incompatible observables $\mathcal{A}$ and $\mathcal{A}'$ acting on $\mathcal{H}_\mathcal{A}$, for which

$$R_\mathcal{A}(\rho) + R_{\mathcal{A}'}(\rho) \leq \log_2 d_\mathcal{A} + S(\rho_\mathcal{A}) - I_{\mathcal{A}:\mathcal{B}}(\rho). \tag{2.32}$$

This complementarity relation shows that complete realism for both observables cannot be simultaneously achieved unless $\rho = \frac{\mathbb{I}}{d_\mathcal{A}} \otimes \rho_\mathcal{B}$. The inequality also highlights that realism depends not only on the system itself but also on the correlations it shares. For a pure state $\rho = |\psi\rangle\langle\psi|$, the bound simplifies to $\log_2 d_\mathcal{A} - E(\psi)$, where $E(\psi) = S(\rho_{\mathcal{A}(\mathcal{B})})$ is the entanglement entropy [72].

This complementarity bound (2.32) has been applied in the study of WPD in delayed-choice experiments [72]. In the case of a qubit interferometer, one may assign $P \equiv \sigma_z$ and $W \equiv \sigma_\perp$ as the particle and wave observables, with eigenstates $\{|\mathcal{P}_+\rangle, |\mathcal{P}_-\rangle\} \equiv \{|0\rangle, |1\rangle\}$ and $|\mathcal{W}_\pm\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \pm e^{i\theta}|1\rangle\right)$, respectively. Throughout this work we keep these conventions, since $|\mathcal{P}_\pm\rangle$ encode definite path information (particle behaviour) and $|\mathcal{W}_\pm\rangle$ capture interference properties (wave behaviour). In what follows, we investigate how variations in the causal order of an entanglement-assisted delayed-choice experiment influence the complementarity relations framed in terms of realism.

2.3 Foundational physical principles as cryptographic constraints

Quantum cryptographic security does not rest solely on the Hilbert space formalism of quantum mechanics, but rather on a constellation of foundational physical principles that bound the structure of admissible correlations. These principles, namely no-signaling, EURs, WPD, and $\mathcal{IC}$, serve as operational constraints in various security scenarios, ranging from fully device-dependent to SDI and fully DI protocols.

Each of these principles excludes specific classes of adversarial strategies. For instance, the violation of local realism precludes classical simulation attacks, uncertainty relations constrain Eve's simultaneous knowledge of complementary observables, and information causality restricts the exploitable correlations in no-signaling theories. This section lays out these principles with a focus on their role in defining or certifying cryptographic security.

2.3.1 No-Signaling as a Constraint on Adversaries

The no-signaling principle asserts that local measurement choices cannot influence outcomes at space-like separated regions. Formally, for a bipartite probability distribution $P(a, b|x, y)$ over measurement settings x, y and outcomes a, b, the marginal distribution for Alice's outcomes must be independent of Bob's input:

$$\sum_b P(a, b|x, y) = \sum_b P(a, b|x, y'), \quad \forall a, x, y, y'. \tag{2.33}$$

This condition is fundamental to relativity and is respected not only by quantum correlations but also by a broader class of non-signalling correlations [47].

In DI cryptographic protocols, such as those based on Bell inequality violations, the no-signaling condition plays a critical role. It ensures that an adversary cannot gain information about one party's input through correlated outputs alone, unless classical communication is permitted. Any adversarial model must respect this constraint, making it a foundational tool in deriving security bounds [26, 77].

Moreover, the no-signaling condition bounds the power of post-quantum adversaries. While hypothetical "superquantum" correlations such as those in PR boxes respect no-signaling, they still yield implausible information-theoretic consequences (e.g., trivializing communication complexity), underscoring that quantum theory strikes a balance between locality and information access [78].

2.3.2 Monogamy of Nonlocal Correlations

One of the key structural constraints distinguishing quantum from post-quantum correlations is the *monogamy of nonlocality*. Informally, this principle states that if two parties (say, Alice

and Bob) share strong nonlocal correlations, then neither can be equally nonlocally correlated with a third party (say, Charlie). This exclusivity has far-reaching implications for quantum cryptography, particularly in limiting eavesdropper capabilities in DI protocols.

Monogamy of nonlocality is most commonly quantified using the violation strength of Bell-type inequalities, particularly the CHSH inequality. Let CHSH_{AB} and CHSH_{AC} denote the Bell parameters computed for Alice-Bob and Alice-Charlie pairs, respectively. Then, Toner and Verstraete [48] established the following fundamental constraint for any no-signaling theory:

$$\mathrm{CHSH}_{AB}^2 + \mathrm{CHSH}_{AC}^2 \leq 8, \tag{2.34}$$

which saturates for maximal quantum violations $\mathrm{CHSH}_{AB} = \mathrm{CHSH}_{AC} = 2$. This bound implies that if Alice and Bob achieve the maximal quantum value of $2\sqrt{2}$, then $\mathrm{CHSH}_{AC} = 0$, and Charlie's correlations with Alice must be completely local.

The monogamy of CHSH-type nonlocality stems from the linear structure of quantum correlations and the Tsirelson bound [67], which upper-bounds the CHSH expression for quantum states by $2\sqrt{2}$. In contrast, superquantum (PR-box) correlations that attain the algebraic maximum of 4 for CHSH would trivially violate monogamy constraints and therefore contradict information-theoretic security conditions.

More generally, in multipartite settings, monogamy inequalities take the form:

$$\sum_{j \neq A} \left(\mathrm{CHSH}_{Aj}\right)^2 \leq C, \tag{2.35}$$

for some theory-dependent constant C. For quantum mechanics, $C = 8$ for any two pairs, but more complex bounds exist for three or more parties, especially in the presence of mixed or entangled states [68, 79, 80].

From a cryptographic standpoint, monogamy guarantees that an eavesdropper cannot be strongly correlated with both communicating parties. This principle underpins the security of DIQKD protocols, where Bell inequality violations serve as certificates of privacy.

In addition to these structural constraints, monogamy of nonlocality can also be expressed in terms of the CHSH winning probability functional β, which provides a convenient normalization of nonlocal correlations between pairs of parties. Consider a tripartite Bell scenario involving Alice ($\mathcal{A}$), Bob ($\mathcal{B}$), and a potential eavesdropper ($\mathcal{E}$). If Alice and Bob share correlations such that $\beta(\mathcal{A}, \mathcal{B}) > 3/4$, then the correlations between Bob and Eve, quantified by $\beta(\mathcal{B}, \mathcal{E})$, must necessarily be limited. This trade-off is generally captured by a *monogamy relation* of the form

$$\beta(\mathcal{B}, \mathcal{E}) \leq f_T^M\big(\beta(\mathcal{A}, \mathcal{B})\big), \tag{2.36}$$

where $f_T^M : [1/2, 1] \mapsto [0, 1]$ denotes the characteristic monogamy function for a given nonlocal theory T.

Such relations are particularly relevant in DIQKD. In this context, they impose thresholds on the observed violation $\beta(\mathcal{A},\mathcal{B})$ that guarantee secrecy against an adversary constrained by theory T [81–83]. Specifically, the sufficient security condition for individual attacks can be expressed as

$$h(\beta(\mathcal{A},\mathcal{B})) < 3 - 4f_T^M(\beta(\mathcal{A},\mathcal{B})), \tag{2.37}$$

where $h(p) = -p\log p - (1-p)\log(1-p)$ is Shannon's binary entropy. Substituting the appropriate monogamy function yields explicit security thresholds for different physical theories.

For instance, in no-signaling theories, the correlations satisfy a *linear* monogamy constraint [84]:

$$\beta(\mathcal{B},\mathcal{E}) \leq \tfrac{3}{2} - \beta(\mathcal{A},\mathcal{B}). \tag{2.38}$$

At the extremal point $\beta(\mathcal{A},\mathcal{B}) = \beta_{NS} = 1$, this relation enforces that Bob and Eve are completely uncorrelated, i.e., $\beta(\mathcal{B},\mathcal{E}) = 1/2$. The resulting DIQKD security threshold in this case is $\beta(\mathcal{A},\mathcal{B}) \approx 0.881$, which cannot be achieved within quantum mechanics.

By contrast, quantum correlations obey a tighter *quadratic* monogamy relation [48]:

$$\left(\beta(\mathcal{A},\mathcal{B}) - \tfrac{1}{2}\right)^2 + \left(\beta(\mathcal{B},\mathcal{E}) - \tfrac{1}{2}\right)^2 \leq \tfrac{1}{8}. \tag{2.39}$$

This bound implies that when Alice and Bob achieve the maximal quantum violation $\beta_Q = \frac{1}{2}(1+\frac{1}{\sqrt{2}})$, any correlations with Eve are forced to be completely local, $\beta(\mathcal{B},\mathcal{E}) = 1/2$. In this case, the corresponding DIQKD threshold is relaxed to $\beta(\mathcal{A},\mathcal{B}) \approx 0.841$, a value achievable in principle with quantum systems.

Taken together, these formulations highlight the cryptographic relevance of monogamy: the very same trade-offs that forbid simultaneous strong nonlocal correlations across multiple parties provide the foundation for security in DI protocols.

2.3.3 Information Causality

The principle of *Information Causality* ($\mathcal{IC}$), introduced by Pawłowski *et. al.* [46], extends the no-signaling condition and provides a potential boundary for admissible physical theories beyond quantum mechanics. At its core, $\mathcal{IC}$ constrains how much information one party can access about another's data, given limited classical communication and shared correlations.

Original Formulation. Consider a communication game in which Alice holds a string of N random bits $\vec{a} = (a_1, a_2, \ldots, a_N)$. Bob is given a uniformly random index $k \in \{1, 2, \ldots, N\}$, and his goal is to guess a_k as accurately as possible. Alice is allowed to send m classical bits to Bob, and both parties may share pre-established (quantum or non-signaling) correlations (see fig. (2.2)).

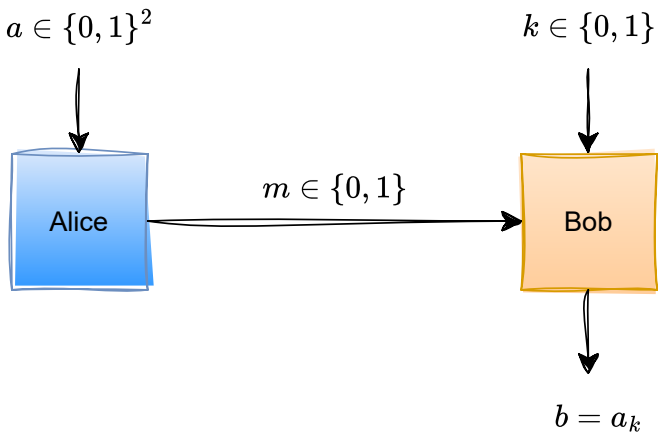

Figure 2.2: **Schematic of the $\mathcal{IC}$ task.** Alice receives a random 2-bit string $a \in \{0,1\}^2$, and Bob receives a random index $k \in \{0,1\}$. Alice is allowed to send m classical bits to Bob, and the two may share prior correlations (classical, quantum, or non-signaling). Bob's objective is to output a guess b for Alice's bit a_k.

The principle OF $\mathcal{IC}$ asserts:

$$\sum_{k=1}^{N} I(a_k : b_k) \leq m, \tag{2.40}$$

where b_k is Bob's guess for a_k, and $I(a_k : b_k)$ is the Shannon mutual information. This inequality holds in both classical and quantum theories, but it can be violated by certain non-signaling theories, such as those involving PR-boxes.

Noisy Information Causality. Miklin and Pawłowski [85] introduced a robust version of $\mathcal{IC}$ that accounts for imperfections and noise in communication and correlations. They consider the same basic scenario but under a model where Alice's bits and Bob's guesses are noisy, and define a parameter ϵ such that:

$$\sum_{k=1}^{N} I_\epsilon(a_k : b_k) \leq m, \tag{2.41}$$

where I_ϵ denotes the mutual information under a noise parameter ϵ. The strength of this formulation lies in its ability to distinguish quantum correlations from certain noisy no-signalling models that would otherwise evade detection using standard $\mathcal{IC}$.

This formulation has found applications in bounding approximate communication tasks and quantifying how much post-quantum correlations can deviate from $\mathcal{IC}$ before becoming unphysical.

Multipartite Reformulation. A more recent contribution by Pollyceno *et. al.* [86] extends $\mathcal{IC}$ to multipartite causal networks using a generalized framework. They define an *operationally motivated constraint* over distributed information flows:

$$\sum_i I(X_i : Y_i|\Lambda_i) \leq \sum_j H(M_j), \tag{2.42}$$

where X_i are inputs, Y_i outputs of receiving parties, Λ_i shared causal resources (e.g., pre-shared entanglement), and M_j classical messages transmitted across the network.

This generalization unifies causal constraints, network entropy inequalities, and resource-based principles, forming a cryptographic framework for distributed quantum tasks. It naturally recovers bipartite $\mathcal{IC}$ and provides bounds on information flow in DI network protocols.

Altogether, $\mathcal{IC}$ serves both as a *cryptographic constraint* and a *foundational principle*, constraining super-quantum correlations that violate core information-theoretic limits.

2.3.4 Entropic Uncertainty Relations, Wave–Particle Duality, and Cryptographic Security

The uncertainty principle is a cornerstone of quantum theory, originally formulated by Heisenberg in terms of variances of measurement outcomes. In modern quantum information theory, this concept is more fruitfully expressed in an information-theoretic form via EURs, which quantify limitations on the simultaneous predictability of incompatible observables in terms of entropy measures. These relations have found deep connections to WPD and play a central role in quantum cryptography.

Entropic Uncertainty Relations. Consider two observables A and B with respective orthonormal eigenbases $\{|a_i\rangle\}$ and $\{|b_j\rangle\}$. For a quantum state ρ, measuring A and B yields probability distributions

$$p_i = \mathrm{Tr}(\rho|a_i\rangle\langle a_i|), \quad q_j = \mathrm{Tr}(\rho|b_j\rangle\langle b_j|), \tag{2.43}$$

with corresponding Shannon entropies

$$H(A) = -\sum_i p_i \log p_i, \quad H(B) = -\sum_j q_j \log q_j. \tag{2.44}$$

The Maassen–Uffink EUR [38] states

$$H(A) + H(B) \geq -\log c, \quad c = \max_{i,j} |\langle a_i|b_j\rangle|^2, \tag{2.45}$$

where c quantifies the overlap between the eigenbases of A and B. This bound captures the incompatibility of the observables: perfect predictability of one implies maximal uncertainty about the other.

Extensions incorporating quantum memory are essential in cryptographic contexts. For a bipartite state ρ_{AB}, where B is a quantum memory correlated with A, Berta *et al.* [39] proved

$$H(A|B) + H(B'|B) \geq -\log c + H(A|B), \tag{2.46}$$

where $H(\cdot|\cdot)$ denotes the conditional von Neumann entropy, and B' denotes a measurement in a basis complementary to that of A.

Wave–Particle Duality from EURs. WPD is a hallmark of quantum physics, asserting that no experimental arrangement can reveal both complete which-path (particle-like) information and perfect interference (wave-like) visibility. In a two-path interferometer, this trade-off is quantified by [33]:

$$\mathcal{D}^2 + \mathcal{V}^2 \leq 1, \tag{2.47}$$

where $\mathcal{D}$ is the path distinguishability and $\mathcal{V}$ the fringe visibility.

Coles *et al.* [40] recast this WPD relation into the language of EURs by associating particle- and wave-like properties with incompatible observables (e.g., Z and X), obtaining

$$H_{\min}(Z|E) + H_{\max}(X|E) \geq \log \frac{1}{c}, \tag{2.48}$$

where E is a quantum memory held by an adversary, and $H_{\min}$, $H_{\max}$ are smooth min- and max-entropies [87]. This formulation bridges foundational complementarity with operational security bounds.

Quantum Guessing Games and Cryptographic Implications. The WPD–EUR connection can be operationally framed as a *quantum guessing game* (QGG) [41]. Suppose Alice prepares a system in one of two mutually unbiased bases (X or Z) and an adversary Eve, holding system E correlated with Alice's system A, attempts to guess Alice's outcome.

Eve's optimal guessing probabilities are given by

$$P_{\text{guess}}(X|E) = 2^{-H_{\min}(X|E)}, \quad P_{\text{guess}}(Z|E) = 2^{-H_{\min}(Z|E)}, \tag{2.49}$$

which satisfy the entropic trade-off

$$-\log P_{\text{guess}}(X|E) - \log P_{\text{guess}}(Z|E) \geq \log \frac{1}{c}. \tag{2.50}$$

This means that high predictability of the path observable (particle-like) necessarily reduces predictability of the interference observable (wave-like), limiting Eve's accessible information and ensuring cryptographic security.

Experimental Demonstrations. Theoretical predictions from (2.48) and (2.50) have been tested in various optical setups [88, 89]. Notably, Spegel-Lexne *et al.* [90] demonstrated a SDI QGG protocol in a photonic interferometer, using visibility as a cryptographic witness and confirming the entropy bounds predicted by the WPD–EUR framework.

In summary, EURs provide a unifying formalism that links quantum complementarity, WPD, and operational cryptographic bounds. By quantifying uncertainty in the presence of quantum memory, and by interpreting duality in terms of entropic trade-offs, one can derive practical, experimentally testable security guarantees for quantum communication protocols.

Having introduced the necessary features of quantum theory and some of its relevant foundational principles, we are now in a position to explore one of the major applications of quantum information theory: *quantum cryptography*. In the following, we discuss DI and SDI approaches, which explore these foundational aspects to provide strong security guarantees even in the presence of untrusted or imperfect devices.

2.4 Device-independent and semi-device-independent quantum cryptography

Quantum cryptography aims to provide information-theoretic security based on the laws of quantum mechanics rather than computational assumptions. Traditionally, security proofs require a detailed and trusted model of the devices used in the protocol: an assumption that can be unrealistic in practice, as real devices may have imperfections, hidden vulnerabilities, or be maliciously altered. DI and SDI approaches seek to relax such assumptions by guaranteeing security even when the internal workings of the devices are uncharacterized or only partially characterized.

2.4.1 Device-Independent Quantum Key Distribution

In DI quantum cryptography, the security is established without relying on any knowledge of the internal functioning of the devices. Instead, security is certified solely from the observed violation of a Bell inequality in the measurement statistics. This approach was pioneered by Mayers and Yao [91] and rigorously developed for QKD by Barrett, Hardy, and Kent [26], and later by Acín et al. [25].

In DIQKD, the devices are treated as "black boxes" that take classical inputs (measurement settings) and produce classical outputs (measurement outcomes). For reference, see fig. 2.3. If the correlations between these outputs violate a Bell inequality beyond the classical bound, they must originate from an entangled quantum state shared between the parties. The monogamy of nonlocal correlations ensures that any eavesdropper cannot have full knowledge of the key.

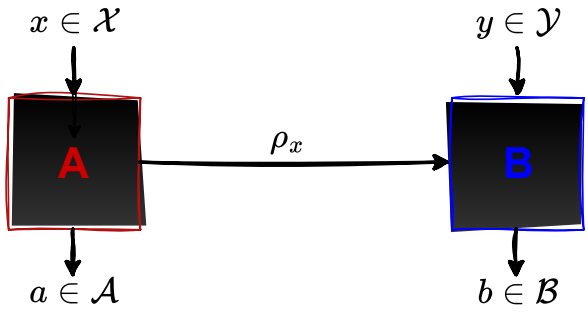

Figure 2.3: **The DI setup.** Alice and Bob each possess a "black-box" preparation or measurement device that takes classical inputs x and y (their chosen measurement settings) and produces classical outputs a and b (measurement outcomes). The security of the generated key is established solely from the observed correlations between a and b. No assumptions are made about the internal functioning of the devices, ensuring security even against adversaries controlling the measurement apparatus.

DI behaviour and constraint sets. A DI experiment is fully specified by conditional probabilities

$$\mathbf{P} := \{P(a,b|x,y)\}_{a,b,x,y}, \tag{2.51}$$

where $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ are Alice's and Bob's inputs (measurement choices), and $a \in \mathcal{A}$, $b \in \mathcal{B}$ are their outputs. The set of all such correlations forms a convex polytope. Three important, nested correlation sets are:

$$\mathcal{L} := \Big\{P(a,b|x,y) = \sum_{\lambda} p(\lambda)\, P(a|x,\lambda)P(b|y,\lambda)\Big\} \qquad \text{(local / LHV)}, \tag{2.52}$$

$$\mathcal{Q} := \Big\{P(a,b|x,y) = \mathrm{Tr}\big[(M_a^x \otimes N_b^y)\,\rho\big]\Big\} \qquad \text{(quantum)}, \tag{2.53}$$

$$\mathcal{NS} := \Big\{P : \sum_b P(a,b|x,y) = \sum_b P(a,b|x,y') \ \wedge \ \sum_a P(a,b|x,y) = \sum_a P(a,b|x',y)\Big\} \qquad \text{(no-signalling)}. \tag{2.54}$$

We have $\mathcal{L} \subsetneq \mathcal{Q} \subsetneq \mathcal{NS}$. DI security relies only on that $\mathbf{P} \notin \mathcal{L}$ (Bell violation), without assuming a model for M_a^x, N_b^y or the dimension of ρ [26, 65–67].

CHSH value, game formulation, and violation. The canonical Bell inequality used in DI-QKD is the CHSH inequality [51]. Defining correlation terms

$$E_{xy} = \sum_{a,b} (-1)^{a\oplus b}\, p(a,b|x,y), \tag{2.55}$$

the CHSH parameter is

$$S = E_{00} + E_{01} + E_{10} - E_{11}. \tag{2.56}$$

Local correlations satisfy $|S| \leq 2$, while quantum mechanics allows $|S| \leq 2\sqrt{2}$, known as the Tsirelson bound [67]. Equivalently, in the CHSH game (winning condition $a \oplus b = x \cdot y$) as described in 2.2.2, the observed winning probability p_w relates to S by [92, 93]

$$p_w = \frac{1}{2} + \frac{S}{8}, \qquad \tfrac{3}{4} \leq p_w \leq \tfrac{1}{2} + \tfrac{\sqrt{2}}{4} \text{ for quantum.} \tag{2.57}$$

No-signaling constraints during the protocol. Security further requires that measurement rounds are space-like (or otherwise enforced) to prevent unwanted signaling between devices. Operationally, the observed $\mathbf{P}$ must satisfy the linear constraints in (2.54) within statistical tolerances, and Bell-violation estimates (e.g., of S) must be obtained on randomly chosen test rounds to preclude memory attacks [26, 27, 94, 95].

Key rate and security. The observed Bell violation can be converted into a bound on the eavesdropper's information using entropic uncertainty relations. In the asymptotic case for collective attacks, the key rate r can be bounded as

$$r \geq 1 - h(Q) - \chi(S), \tag{2.58}$$

where Q is the quantum bit error rate, $h(\cdot)$ the binary entropy function, and $\chi(S)$ a function bounding Eve's Holevo information from the CHSH value [27]. This makes the DI approach robust even against adversaries who manufacture or control the devices.

In summary, DIQKD provides the strongest form of cryptographic security, requiring only minimal physical assumptions. However, it demands high detection efficiency and low noise to close loopholes, making its practical realization technologically challenging.

2.4.2 Semi-device-independent quantum key distribution

SDI approaches provide a middle ground between fully DI and fully device-dependent cryptographic protocols. While DI protocols require no assumptions about the internal workings of the devices, at the cost of stringent experimental demands, SDI protocols relax these requirements by introducing only partial and well-defined assumptions. A common assumption is a bound on the Hilbert space dimension of the prepared states [30]. Under such an assumption, one can construct a *dimension witness*, a quantitative tool used to certify both the security and the quantum nature of an SDI protocol.

A canonical example is the $(4, 2, 2)$ scenario, which is operationally equivalent to a quantum random access code (QRAC). Here, Alice's input is a pair of classical bits $(a_0, a_1) \in \{0, 1\}^2$, while Bob receives a binary setting $y \in \{0, 1\}$ and produces a binary outcome b (see Fig. 2.4).

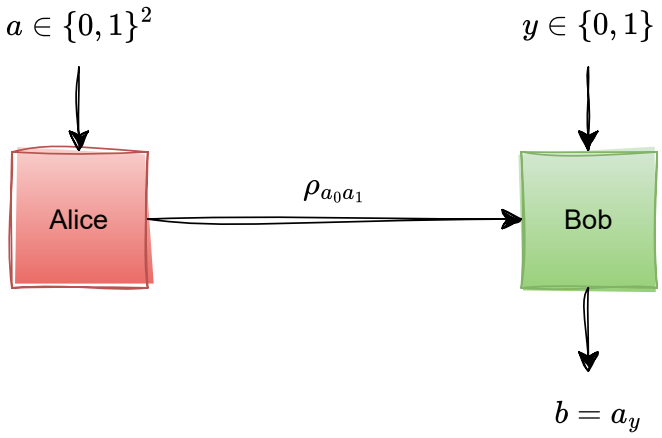

Figure 2.4: **The SDI setup.** Alice encodes two classical bits $(a_0, a_1) \in \{0,1\}^2$ into a single qubit state ρ_{a_0,a_1}, which is sent to Bob. Bob chooses a measurement setting $y \in \{0,1\}$ and produces a binary outcome b aiming to recover a_y, the bit corresponding to his chosen setting. The observed correlators $E_{a_0a_1,y} = P(b = 0 \mid a_0a_1, y)$ are used to construct a dimension witness S that certifies the nonclassical nature of the encoding and bounds the Hilbert space dimension of the quantum system.

In the QRAC picture, Alice encodes the two bits into a single qubit ρ_{a_0,a_1}. Bob, upon choosing y, performs a measurement aiming to recover the bit a_y with the highest possible probability. This scenario defines the correlators

$$E_{a_0a_1,y} := P(b = 0 \mid a_0a_1, y), \tag{2.59}$$

from which the standard SDI dimension witness is constructed:

$$S := E_{00,0} + E_{00,1} + E_{01,0} - E_{01,1} - E_{10,0} + E_{10,1} - E_{11,0} - E_{11,1}. \tag{2.60}$$

When Alice is limited to classical bits, one finds [30] that $S \leq 2$. In contrast, if Alice uses qubits and Bob performs optimal projective measurements, quantum mechanics allows S to reach $2\sqrt{2}$. Observing a violation of the classical bound thus certifies both the nonclassical nature of the communication and the effective dimension of the quantum encoding.

The witness S also has a direct operational meaning in terms of the average success probability of the QRAC:

$$P_B := \frac{1}{8} \sum_{a_0,a_1,y} P(b = a_y \mid a_0, a_1, y) = \frac{S+4}{8}. \tag{2.61}$$

This P_B quantifies Bob's average probability of correctly guessing the target bit a_y given only a single quantum message from Alice. In the $(4, 2, 2)$ scenario, classical strategies cannot exceed $P_B \approx 0.75$. Any value above $P_B \approx 0.8415$ is achievable only with qubit encodings, and

therefore guarantees security under the bounded-dimension assumption. This makes QRAC-based dimension witnesses a central tool for SDI quantum cryptography and randomness generation.

2.5 Summary

This chapter has introduced various essential concepts, with mathematical rigor, that form the foundation for the results to follow. We began by reviewing the distinctive features of quantum theory, namely entanglement, nonlocality, monogamy relations, and no-go theorems, that distinguish quantum mechanics from classical models and serve as key resources for information processing. We then examined WPD through the MZI setup, emphasizing the complementarity between distinguishability and visibility in predictive and retrodictive scenarios, and introduced an information-theoretic realism quantifier to extend this framework. In addition, we outlined foundational principles in quantum theory relevant to this thesis, before turning to DI and SDI approaches, which exploit these nonclassical features to certify correlations and ensure security under minimal assumptions. Collectively, these preliminaries establish the conceptual and technical groundwork for the analyses and cryptographic protocols developed in the subsequent chapters.

Chapter 3

Security of DIQKD via monogamy relations from multipartite information causality

"The mystery of human existence lies not in just staying alive, but in finding something to live for."

—Fyodor Dostoyevsky, The Brothers Karamazov

The study of fundamental principles governing quantum correlations has played a central role in identifying the boundary between classical, quantum, and post-quantum theories. Among these principles, information causality ($\mathcal{IC}$) and monogamy of correlations stand out as particularly powerful.

The principle of $\mathcal{IC}$ was introduced in [46] as a natural generalization of the no-signaling principle. In its original bipartite formulation, $\mathcal{IC}$ constrains the amount of information that one party can gain about another's dataset when only a limited amount of classical communication is allowed, even in the presence of nonlocal resources. The $\mathcal{IC}$ inequality successfully explains why certain post-quantum correlations, such as those displayed by Popescu–Rohrlich (PR) boxes [47], are physically implausible: while consistent with no-signaling, they would otherwise permit unlimited information transfer in violation of $\mathcal{IC}$.

Complementary to this, monogamy relations capture the idea that strong nonlocal correlations between two parties necessarily restrict the correlations that can be shared with additional parties. Originally studied in the context of Bell inequalities [48, 49, 96, 97], these trade-offs lie at the heart of quantum cryptography: if Alice and Bob share correlations that are sufficiently nonclassical, the structure of quantum theory guarantees that no third party can share equally strong correlations with them.

While $\mathcal{IC}$ was originally developed for bipartite scenarios, many cryptographic and foundational tasks naturally involve three or more parties. A multipartite formulation of $\mathcal{IC}$ was first proposed in [50], where it was shown how the principle can be generalized to scenarios with multiple senders. This work opened the way to understanding how $\mathcal{IC}$ constrains correlations in more complex networks.

In this chapter, we take a decisive step toward establishing that the principle of $\mathcal{IC}$ underpins the security of device-independent quantum key distribution (DIQKD). By adopting a refined multipartite information-theoretic framework, we demonstrate that the CHSH-based QKD protocol [98] remains secure whenever the participating parties respect the multipartite operational form of the $\mathcal{IC}$ principle. Importantly, the security holds not only at the point of maximal quantum violation of the CHSH inequality but across a range of quantum-accessible violations.

This result is enabled by a nontrivial monogamy relation for CHSH inequalities that we derive directly from the multipartite formulation of $\mathcal{IC}$. Specifically, when two parties achieve the maximal quantum violation of CHSH, multipartite $\mathcal{IC}$ strictly forbids any residual correlation with a third party, thus fully recovering the quantum monogamy of Bell inequality violations. For sub-maximal violations, the multipartite $\mathcal{IC}$ principle still enforces bounds that are strictly tighter than those implied by no-signaling alone, thereby constraining the nonlocal correlations available to an eavesdropper. This guarantees enhanced security of DIQKD against adversaries that are only required to respect the $\mathcal{IC}$ principle.

Finally, we show that previous bipartite formulations of $\mathcal{IC}$ are insufficient to impose these monogamy constraints on CHSH inequalities, underscoring the necessity of a genuinely multipartite framework. Taken together, these findings establish multipartite information causality as a robust principle both for understanding the structure of quantum correlations and for certifying cryptographic security.

3.1 Setup and minimal notations

Let us begin by revisiting the essentials discussed in subsections 2.3.2 and 2.3.3 of Chapter 2. While the quadratic monogamy relation (2.39) accurately characterizes the constraints imposed by quantum mechanics, our objective here is to explore whether a non-trivial, i.e., stricter than the no-signaling bound (2.38), monogamy relation of the general form (2.36) can be derived from a fundamental physical principle, without explicitly invoking Hilbert space formalism. In this context, we recall the principle of $\mathcal{IC}$, introduced in subsection 2.3.3 of Chapter 2, and note that a detailed discussion of its multipartite formulation, following the framework in [50] and including our generalization to incorporate noise, directly relevant for the analysis in this chapter, will be presented shortly.

3.2 Information causality ($\mathcal{IC}$)

The principle of $\mathcal{IC}$ is most commonly illustrated through a bipartite communication game known as the $(n \mapsto m)$ *random access code* (RAC) [99]. In this setting, the sender $\mathcal{A}$ receives a random n-bit string $\mathbf{x} = (X_1, \ldots, X_n)$ and encodes it into an m-bit classical message M, with $m < n$. The message is transmitted to the receiver $\mathcal{B}$ via a classical channel of effective capacity $C \leq m$, yielding the (possibly noisy) message M'. The receiver's task is then to guess a randomly chosen bit X_i of $\mathbf{x}$, producing an output G_i. Information causality asserts that the total information potentially accessible to $\mathcal{B}$ is upper-bounded by the channel capacity, i.e.,

$$\sum_{i=1}^{n} I(X_i : G_i) \leq C, \tag{3.1}$$

where $I(X_i : G_i)$ denotes the mutual information between $\mathcal{A}$'s ith input and $\mathcal{B}$'s guess. This formulation [100] generalizes the original proposal [101] to account for noisy classical communication.

Quantum mechanics respects this principle, but certain post-quantum, no-signaling correlations, such as the PR-box [102], violate it. For example, in the $(2 \mapsto 1)$ RAC assisted by a PR-box, the van Dam protocol [103] enables perfect recovery of both bits, yielding $I(X_1 : G_1) = I(X_2 : G_2) = 1$, which exceeds the $C = 1$ constraint in Eq. (3.1). Thus, $\mathcal{IC}$ rules out PR-box correlations, and more generally excludes any nonlocal behaviour that would violate the CHSH inequality beyond Tsirelson's bound [100, 101].

A further refinement of the principle can be obtained by considering the causal structure underlying RAC tasks. Using the entropic framework of [104], one derives a generalized inequality valid for non-uniform priors and arbitrary decoding strategies:

$$\begin{aligned} \sum_{i=1}^{n} I(X_i : G_i, M') + \sum_{i=2}^{n} I(X_1 : X_i | G_i, M') \\ \leq C + \sum_{i=2}^{n} H(X_i) - H(X_1, \ldots, X_n), \end{aligned} \tag{3.2}$$

which is satisfied in both classical and quantum theories, but again violated by certain super-quantum correlations.

Up to this point, $\mathcal{IC}$ has been invoked in strictly bipartite settings. However, the analysis relevant for this chapter requires a *multipartite formulation*. Following [105], and extending it to incorporate noisy communication channels, we consider a network of N spatially separated parties: $N-1$ senders $\{\mathcal{A}_k\}_{k=1}^{N-1}$, each holding an n-bit input string $\mathbf{x}^k = (X_1^k, \ldots, X_n^k)$, and a receiver $\mathcal{B}$. Each sender encodes their input into a message M_k of size $m < n$, which is transmitted through a channel of capacity C_k to $\mathcal{B}$. Upon receiving the noisy messages $\{M_k'\}$, the receiver is tasked with producing a guess G_j about a function $f_j(X_j^1, \ldots, X_j^{N-1})$ of the jth input bits. The corresponding causal structure is shown in Fig. 3.1.

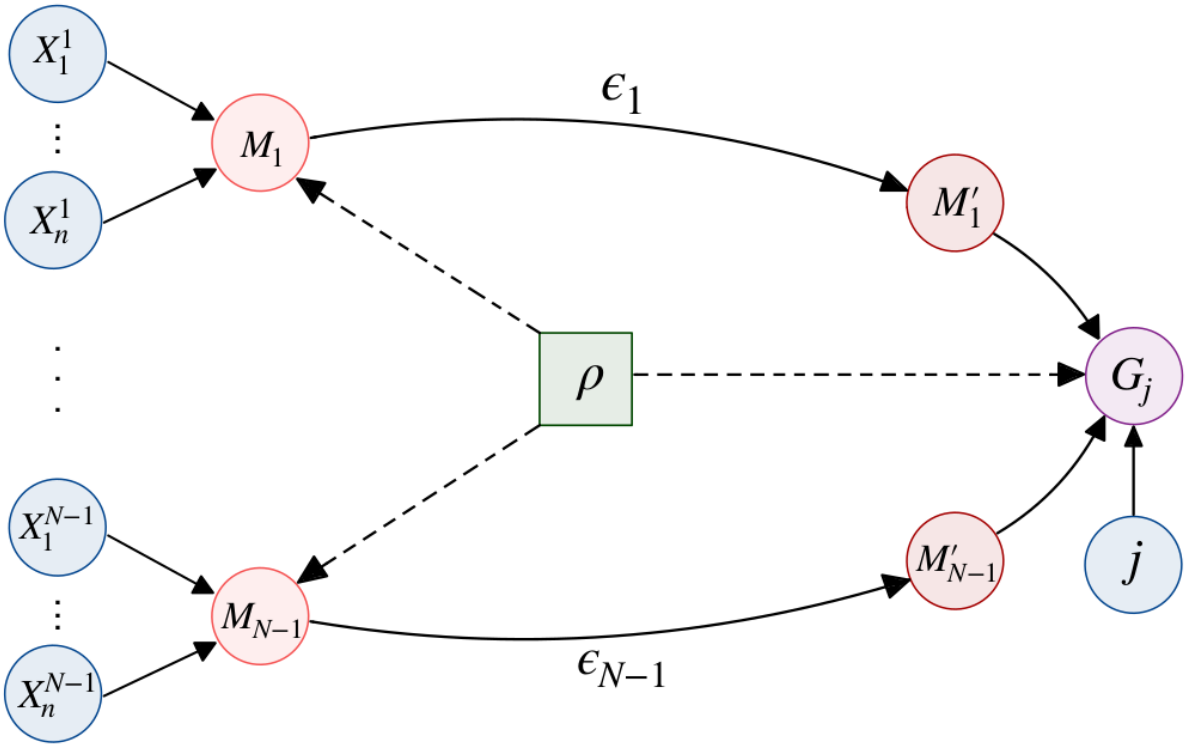

Figure 3.1: **Multipartite $\mathcal{IC}$ protocol.** The figure illustrates the causal structure, represented as a Directed Acyclic Graph (DAG), corresponding to the communication task defined by the multipartite $\mathcal{IC}$ criterion (3.3). The scenario involves $N-1$ senders and a single receiver, who share a pre-established entangled quantum state ρ (green square). Each sender $\{\mathcal{A}_k\}_{k=1}^{N-1}$ receives inputs $\{\{X_j^k\}_{j=1}^n\}_{k=1}^{N-1}$ (blue disks) and encodes them into classical messages $\{M_k\}_{k=1}^{N-1}$ (pink disks). These messages are transmitted through binary-symmetric noisy classical channels, characterized by parameters $\{\epsilon_k\}_{k=1}^N$, to the receiver $\mathcal{B}$. The receiver obtains the potentially corrupted messages $\{M_k'\}_{k=1}^{N-1}$ and, upon selecting an input index $j \in \{1,\ldots,n\}$ at random (green disk), computes a guess G_j (purple disk) of the target function $f_j(\{X_j^k\}_{k=1}^{N-1})$. .

In this scenario, the bipartite inequalities (3.1)–(3.2) are insufficient to constrain post-quantum resources. Instead, the following multipartite $\mathcal{IC}$ criterion holds:

$$\sum_{k,i} I(X_i^k : X_i^1,\ldots,X_i^{k-1},X_i^{k+1},\ldots,X_i^{N-1},\mathbf{M}',G_i) \leq \sum_{k=1}^{N-1} C_k + \sum_{i=1}^{n} I(X_{i+1}^k,\ldots,X_n^k : X_i^k), \tag{3.3}$$

where $\mathbf{M}' = (M_1',\ldots,M_{N-1}')$ is the tuple of received messages. This expression reduces to the bipartite case when $N=2$, while capturing genuinely multipartite information flows for $N>2$.

The key advantage of the multipartite formulation is its ability to exclude correlations that evade the bipartite constraints. For instance, in the tripartite case with $N=3$, certain no-signaling distributions satisfy all bipartite $\mathcal{IC}$ conditions yet still allow perfect information

transfer, thereby violating Eq. (3.3). Hence, the multipartite principle strengthens the boundary between physically realizable and post-quantum correlations, a feature that will be central to our analysis of secrecy in cryptographic protocols under $\mathcal{IC}$.

3.2.1 Proof of multipartite $\mathcal{IC}$ criterion in (3.3)

The proof primarily relies on two foundational axioms from the original formulation of $\mathcal{IC}$: the mutual information chain rule and the data-processing inequality, which can be stated as follows,

$$I(A:B|C) = I(A:B,C) - I(A:C); \tag{3.4}$$

$$I(A:B') \leq I(A:B), \quad \text{where} \quad B \longrightarrow B'. \tag{3.5}$$

The data-processing inequality tells us that any local transformation of data can only decrease information. Here, $I(A:B)$ represents a theory-independent notion of mutual information between systems A and B, while B' results from applying a local operation to B. Alongside these two principles, our proof also invokes another axiom of $\mathcal{IC}$, referred to as *consistency* [101], which requires that $I(A:B)$ reduces to Shannon mutual information whenever A and B are classical systems.

Now, in the multipartite communication setup shown in Figure 3.1, consider the mutual information between the k-th party's bit string, $\mathbf{x}^k$, and the rest of the system—namely, the data of the other parties, the receiver's local resource c, and the set of received messages $\mathbf{M'} = M'kk = 1^{N-1}$. Formally, this is expressed as:

$$I(\mathbf{x}^k : \mathbf{x}^1, \cdots, \mathbf{x}^{k-1}, \mathbf{x}^{k+1}, \cdots, \mathbf{x}^{N-1}, \mathbf{M'}, c). \tag{3.6}$$

This captures the total knowledge the rest of the network holds about party k's dataset. For this quantity, we can directly invoke the relation derived in Ref. [105], which shows that under the assumptions of chain rule and data processing, one can immediately write,

$$\begin{aligned} &I(\mathbf{x}^k : \mathbf{x}^1, \cdots, \mathbf{x}^{k-1}, \mathbf{x}^{k+1}, \cdots, \mathbf{x}^{N-1}, \mathbf{M'}, c) \\ &\geq \sum_{i=1}^{n} I(X_i^k : X_i^1, X_i^2, \cdots, X_i^{k-1}, X_i^{k+1}, \cdots, X_i^{N-1}, \mathbf{M'}, c) - \sum_{i=1}^{n} I(X_{i+1}^k, \cdots, X_n^k : X_i^k). \end{aligned} \tag{3.7}$$

It is important to note that (3.7) holds regardless of the specific dependencies that may exist among the random variables involved.

Since the variables in $\mathbf{M'}$ are classical, we can apply the data-processing inequality (3.5) to further tighten the previous bound, yielding:

$$\begin{aligned} &I(\mathbf{x}^k : \mathbf{x}^1, \cdots, \mathbf{x}^{k-1}, \mathbf{x}^{k+1}, \cdots, \mathbf{x}^{N-1}, \mathbf{M'}, c) \\ &\geq \sum_{i=1}^{n} I(X_i^k : X_i^1, X_i^2, \cdots, X_i^{k-1}, X_i^{k+1}, \cdots, X_i^{N-1}, \mathbf{M'}, G_i) - \sum_{i=1}^{n} I(X_{i+1}^k, \cdots, X_n^k : X_i^k). \end{aligned} \tag{3.8}$$

We next upper-bound $I(\mathbf{x}^k : \mathbf{x}^1, \cdots, \mathbf{x}^{k-1}, \mathbf{x}^{k+1}, \cdots, \mathbf{x}^{N-1}, \mathbf{M}', c)$ by expanding $\mathbf{M}'$ into its component $M'_1, \cdots, M'_k, \cdots, M'_{N-1}$ and then applying the chain rule for mutual information, which yields:

(3.9)
$$\begin{aligned} &I(\mathbf{x}^k : \mathbf{x}^1, \cdots, \mathbf{x}^{k-1}, \mathbf{x}^{k+1}, \cdots, \mathbf{x}^{N-1}, M'_1, \cdots, M'_k, \cdots, M'_{N-1}, c) \\ &\quad = I\left(\mathbf{x}^k : M'_k | \mathbf{x}^1, \cdots, \mathbf{x}^{k-1}, \mathbf{x}^{k+1}, \cdots, \mathbf{x}^{N-1}, M'_1, \cdots, M'_{k-1}, M'_{k+1}, \cdots, M'_{N-1}, c\right) \\ &\quad\quad + I(\mathbf{x}^k : \mathbf{x}^1, \cdots, \mathbf{x}^{k-1}, \mathbf{x}^{k+1}, \cdots, \mathbf{x}^{N-1}, M'_1, \cdots, M'_{k-1}, M'_{k+1}, \cdots, M'_{N-1}, c). \end{aligned}$$

The second term on the right-hand side is zero by virtue of the no-signaling condition. Applying the chain rule to the remaining contribution and invoking the non-negativity of mutual information $I(A : B) \geq 0$, we get

$$\begin{aligned} &I(\mathbf{x}^k : \mathbf{x}^1, \cdots, \mathbf{x}^{k-1}, \mathbf{x}^{k+1}, \cdots, \mathbf{x}^{N-1}, M'_1, \cdots, M'_k, \cdots, M'_{N-1}, c) \\ &\quad \leq I(M'_k : \mathbf{x}^1, \cdots, \mathbf{x}^k, \cdots, \mathbf{x}^{N-1}, M'_1, \cdots, M'_{k-1}, M'_{k+1}, \cdots, M'_{N-1}, c). \end{aligned} \tag{3.10}$$

By using the data processing inequality (3.5) once more, we see that adding M_k to the conditioning on the right-hand side can only lead to an increase in the mutual information,

$$\begin{aligned} &I(\mathbf{x}^k : \mathbf{x}^1, \cdots, \mathbf{x}^{k-1}, \mathbf{x}^{k+1}, \cdots, \mathbf{x}^{N-1}, M'_1, \cdots, M'_k, \cdots, M'_{N-1}, c) \\ &\quad \leq I(M'_k : \mathbf{x}^1, \cdots, \mathbf{x}^k, \cdots, \mathbf{x}^{N-1}, M'_1, \cdots, M'_{k-1}, M'_{k+1}, \cdots, M'_{N-1}, c, M_k). \end{aligned} \tag{3.11}$$

Analyzing the causal structure in Figure 3.1, we observe that M_k acts as a shield for M'_k against all other variables $\mathbf{V}$, implying that $I(M'_k : \mathbf{V} \mid M_k) = I(M'_k : \mathbf{V}, M_k) - I(M'_k : M_k) = 0$. Consequently, the inequality (3.11) can be simplified to,

$$\begin{aligned} &I(\mathbf{x}^k : \mathbf{x}^1, \cdots, \mathbf{x}^{k-1}, \mathbf{x}^{k+1}, \cdots, \mathbf{x}^{N-1}, M'_1, \cdots, M'_k, \cdots, M'_{N-1}, c) \\ &\quad \leq I(M'_k : M_k) = C_k. \end{aligned} \tag{3.12}$$

Ultimately, by merging (3.8) with (3.12) and summing over all indices k, we arrive at the multipartite $\mathcal{IC}$ condition (3.3) as stated in the main text,

(3.13)
$$\sum_{k=1}^{N-1} \sum_{i=1}^{n} I(X_i^k : X_i^1, \ldots, X_i^{k-1}, X_i^{k+1}, \ldots, X_i^{N-1}, \mathbf{M}', G_i) \leq \sum_{k=1}^{N-1} C_k + \sum_{k=1}^{N-1} \sum_{i=1}^{n} I(X_{i+1}^k, \ldots, X_n^k : X_i^k).$$

We emphasize that retaining this specific form of the multipartite $\mathcal{IC}$ criterion is essential for obtaining the results discussed in the main text. Indeed, the earlier formulation in [105] does not explicitly incorporate the received messages when quantifying the receiver's knowledge of the initial data, i.e., $I(X_i^k : X_i^1, \ldots, X_i^{k-1}, X_i^{k+1}, \ldots, X_i^{N-1}, G_i)$. This becomes evident when analyzing the same noiseless three-party scenario and protocol used in the main text. In the

extreme instance where parties share a PR-box, $p(a,b,e|x,y,z) = \delta_{a\oplus b=xy}/4$, the receiver's guess can be written as $G_i = X_i^1 \oplus M_2$, yielding mutual information terms in (3.3) as $I(X_i^k : X_i^{3-k}, M_1, M_2, G_i) = 1$, whereas the previous criterion gives $I(X_i^k : X_i^{3-k}, G_i) = 0$. A similar conclusion holds for the other extreme where $p(a,b,e|x,y,z) = \delta_{e\oplus b=zy}/4$ and $G_i = X_i^2 \oplus M_1$. Consequently, the prior multipartite criterion of [105] expressed as $I(X_i^k : X_i^{3-k}, G_i)$ fails to detect $\mathcal{IC}$ violations for the optimal slice (3.14) using the same encoding and decoding strategies, and thus cannot reproduce the monogamy results shown in Fig. 3.3.

3.3 Optimal slice

As outlined earlier, the secrecy of DIQKD protocols is closely tied to the monogamy of Bell inequality violations, as expressed in Eq. (2.37). To evaluate the capacity of the $\mathcal{IC}$ principle to guarantee security, we therefore examine its implications for monogamy relations of the form (2.36). Concretely, this requires determining the maximum achievable value of $\beta(\mathcal{B},\mathcal{E})$ for a fixed $\beta(\mathcal{A},\mathcal{B})$, optimized over all tripartite no-signaling correlations that respect the corresponding *nonlinear* and *protocol-dependent* $\mathcal{IC}$ constraints. This optimization must be carried out separately for the bipartite conditions (3.1), (3.2) and for the multipartite criterion (3.3).

However, a direct approach is computationally prohibitive, since the convex polytope of tripartite no-signaling correlations contains 53856 extremal points [106]. To make the problem tractable, we now introduce a lemma that drastically simplifies the analysis by reducing the search space to a two-parameter slice of the tripartite no-signaling polytope.

Lemma 3.1. *To find the maximum CHSH value between $\mathcal{B}$ and $\mathcal{E}$, $\beta(\mathcal{B},\mathcal{E})$, permitted by information causality, when $\mathcal{A}$ and $\mathcal{B}$ witness a CHSH value, $\beta(\mathcal{A},\mathcal{B})$, it suffices to consider tripartite no-signaling correlations $p(a,b,e|x,y,z)$ of the form,*

$$p(a,b,e|x,y,z) = \alpha\frac{1}{4}\delta_{a\oplus b,xy} + \gamma\frac{1}{4}\delta_{e\oplus b,zy} + (1-\alpha-\gamma)1/8, \tag{3.14}$$

where $\alpha,\gamma \in [0,1]$, and $\alpha+\gamma \leq 1$.

The proof of Lemma 3.1 follows directly from the *data-processing inequality* and is therefore included below for completeness. For correlations lying on the optimal slice specified by parameters α,γ in (3.14), the corresponding CHSH values are simply $\beta(\mathcal{A},\mathcal{B}) = \frac{1+\alpha}{2}$ and $\beta(\mathcal{B},\mathcal{E}) = \frac{1+\gamma}{2}$. Thus, the problem reduces to determining the maximum γ for a given α, under the requirement that the correlation (3.14) satisfies the relevant $\mathcal{IC}$ criteria, namely (3.1), (3.2), and (3.3). These optimization tasks can then be carried out efficiently, *up to machine precision*, using numerical routines[1]. The resulting trade-off relations are presented in Figure 3.3.

[1]Numerical codes implementing these optimizations are publicly available at [107]

Proof of Lemma 3.1 .

In this section, we present the proof of Lemma 3.1. Specifically, we demonstrate that the correlation slice given in Eq.(3.14) achieves optimality for establishing monogamy relations of the form (2.36), using both the bipartite and multipartite $\mathcal{IC}$ criteria in Eqs (3.1), (3.2), and (3.37), within a tripartite Bell scenario consisting of parties $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{E}$, each with binary inputs $x, y, z \in 0, 1$ and binary outputs $a, b, e \in 0, 1$.

We begin by revisiting the *depolarization* technique outlined in [96, 108], which asserts that any bipartite probability distribution $\mathbb{P}_{\mathcal{A},\mathcal{B}}$ can be converted into an isotropic distribution through local operations and shared randomness (LOSR) without altering its CHSH value. Explicitly, this means:

$$\mathbb{P}_{\mathcal{AB}} \xmapsto{\text{LOSR}_{\mathcal{AB}}} \mathbb{P}^{\text{iso}(\alpha)}_{\mathcal{AB}} = \alpha \text{PR}_{\mathcal{AB}} + (1-\alpha)\text{W}_{\mathcal{AB}}, \tag{3.15a}$$

$$\beta(\mathcal{A},\mathcal{B})_{\mathbb{P}_{\mathcal{AB}}} = \beta(\mathcal{A},\mathcal{B})_{\mathbb{P}^{\text{iso}(\alpha)}_{\mathcal{AB}}} = \frac{1+\alpha}{2}. \tag{3.15b}$$

Here, $\alpha \in [0, 1]$, PR$\mathcal{AB}$ denotes the PR-box achieving the algebraic maximum of the CHSH functional $\beta(\mathcal{A}, \mathcal{B})$ (i.e., $p\text{PR}\mathcal{AB}(a, b|x, y) = \frac{1}{2}\delta a \oplus b, xy$), and W$\mathcal{AB}$ represents the uniform *white noise* distribution (i.e., $p\text{W}_{\mathcal{AB}}(a, b|x, y) = 1/4$).

This depolarization approach can be naturally generalized to tripartite scenarios. Specifically, any tripartite distribution $\mathbb{P}\mathcal{ABE}$ can be mapped, via LOSR$\mathcal{AB}$ applied to parties $\mathcal{A}$ and $\mathcal{B}$, into an isotropic tripartite distribution $\mathbb{P}^{\text{iso}}_{\mathcal{ABE}}$ while preserving the CHSH value $\beta(\mathcal{A}, \mathcal{B})$. Formally, $\mathbb{P}_{\mathcal{ABE}} \xmapsto{\text{LOSR}_{\mathcal{AB}}} \mathbb{P}^{\text{iso}}_{\mathcal{ABE}}$, such that $\beta(\mathcal{A}, \mathcal{B})_{\mathbb{P}_{\mathcal{ABE}}} = \beta(\mathcal{A}, \mathcal{B})_{\mathbb{P}^{\text{iso}}_{\mathcal{ABE}}}$, with:

$$\sum_{\mathcal{E}} \mathbb{P}^{\text{iso}}_{\mathcal{ABE}} = \alpha \text{PR}_{\mathcal{AB}} + (1-\alpha)\text{W}_{\mathcal{AB}}. \tag{3.16}$$

In this expression, $\beta(\mathcal{A}, \mathcal{B})\mathbb{P}\mathcal{ABE}$ denotes the CHSH value computed from the marginal distribution over parties $\mathcal{A}$ and $\mathcal{B}$, obtained by tracing out $\mathcal{E}$. Given that the PR-box is an extremal point in the tripartite Bell scenario with binary inputs and outputs [106], the isotropic tripartite distribution $\mathbb{P}\mathcal{ABE}^{\text{iso}}$ can be expressed as a convex combination of the PR-box and another distribution $\mathbb{P}\mathcal{ABE}'$ that satisfies condition (3.16). Consequently, using (3.15), we obtain:

$$\mathbb{P}_{\mathcal{ABE}} \xmapsto{\text{LOSR}_{\mathcal{AB}}} \mathbb{P}^{\text{iso}(\alpha)}_{\mathcal{ABE}} = \alpha \text{PR}_{\mathcal{AB}} \otimes L_{\mathcal{E}} + (1-\alpha)\mathbb{P}'_{\mathcal{ABE}}, \tag{3.17a}$$

$$\beta(\mathcal{A},\mathcal{B})_{\mathbb{P}_{\mathcal{ABE}}} = \beta(\mathcal{A},\mathcal{B})_{\mathbb{P}^{\text{iso}(\alpha)}_{\mathcal{ABE}}} = \frac{1+\alpha}{2}, \tag{3.17b}$$

Here, $L_{\mathcal{E}}$ represents a local distribution for party $\mathcal{E}$, while $\mathbb{P}'_{\mathcal{ABE}}$ is any tripartite distribution satisfying condition (3.16), i.e., its marginal over $\mathcal{E}$ gives the white-noise distribution $W_{\mathcal{AB}}$, ensuring that $\beta(\mathcal{A}, \mathcal{B})_{\mathbb{P}'_{\mathcal{ABE}}} = 1/2$. Note that $\mathbb{P}'_{\mathcal{ABE}}$ may, in principle, exhibit non-local correlations. Crucially, the product form $\text{PR}_{\mathcal{AB}} \otimes L_{\mathcal{E}}$ arises from the no-signaling constraints: specifically,

the no-signaling condition enforces factorization of the tripartite distribution whenever two parties share a PR-box [84].

Similarly, the transformation in (3.17) can be expressed in terms of the $\mathcal{BE}$ marginal without altering $\beta(\mathcal{B},\mathcal{E})$. Importantly, since depolarization consists solely of bit-flip operations [108], the CHSH value of any marginal remains invariant under the procedure in (3.17). This invariance is transparent because $\beta(\mathcal{A},\mathcal{B})_{\mathbb{P}_{\mathcal{ABE}}}$ depends exclusively on the parameter α defined in Eq. (3.17b). Consequently, performing successive depolarizations, first $\mathrm{LOSR}_{\mathcal{AB}}$ and then $\mathrm{LOSR}_{\mathcal{BE}}$, yields:

$$\mathbb{P}^{\mathrm{iso}(\alpha)}_{\mathcal{ABE}} \xrightarrow{\mathrm{LOSR}_{\mathcal{BE}}} \mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)}_{\mathcal{ABE}} = \gamma \mathrm{PR}_{\mathcal{BE}} \otimes L'_{\mathcal{A}} + (1-\gamma)\mathbb{P}''^{(\alpha)}_{\mathcal{ABE}}, \tag{3.18a}$$

$$\beta(\mathcal{B},\mathcal{E})_{\mathbb{P}^{\mathrm{iso}(\alpha)}_{\mathcal{ABE}}} = \beta(\mathcal{B},\mathcal{E})_{\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)}_{\mathcal{ABE}}}, \tag{3.18b}$$

$$\beta(\mathcal{A},\mathcal{B})_{\mathbb{P}^{\mathrm{iso}(\alpha)}_{\mathcal{ABE}}} = \beta(\mathcal{A},\mathcal{B})_{\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)}_{\mathcal{ABE}}}, \tag{3.18c}$$

Here, $\gamma \in [0,1]$, $L'_{\mathcal{A}}$ denotes a local distribution for party $\mathcal{A}$, and $\mathbb{P}''^{(\alpha)}_{\mathcal{ABE}}$ represents any tripartite distribution satisfying

$$\sum_{\mathcal{A}} \mathbb{P}''^{(\alpha)}_{\mathcal{ABE}} = W_{\mathcal{BE}}, \quad \text{with} \quad \beta(\mathcal{B},\mathcal{E})_{\mathbb{P}''^{(\alpha)}_{\mathcal{ABE}}} = 1/2.$$

From (3.18c), the action of $\mathrm{LOSR}_{\mathcal{BE}}$ leaves the term $\alpha\,\mathrm{PR}_{\mathcal{AB}} \otimes L_{\mathcal{E}}$ in (3.17) unaffected. At most, this contribution may be mapped to a relabeled version of the PR-box, still attaining the maximal CHSH value under some relabeled CHSH inequality. Consequently, we can parametrize $\mathbb{P}''^{(\alpha)}_{\mathcal{ABE}}$ in (3.18a) by introducing an additional parameter $\epsilon \in [0,1]$, such that:

$$\mathbb{P}''^{(\alpha,\epsilon)}_{\mathcal{ABE}} = \epsilon \mathrm{PR}_{\mathcal{AB}} \otimes L_{\mathcal{E}} + (1-\epsilon)\mathbb{P}'''_{\mathcal{ABE}}. \tag{3.19}$$

$\mathbb{P}'''_{\mathcal{ABE}}$ should address the constraints of $\mathbb{P}''^{(\alpha,\epsilon)}_{\mathcal{ABE}}$ and $\mathbb{P}'_{\mathcal{ABE}}$ in (3.17) and (3.18), respectively, i.e., with (3.19) in (3.18a) we have,

$$\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)}_{\mathcal{ABE}} = \alpha \mathrm{PR}_{\mathcal{AB}} \otimes L_{\mathcal{E}} + \gamma \mathrm{PR}_{\mathcal{BE}} \otimes L'_{\mathcal{A}} + (1-\alpha-\gamma)\mathbb{P}'''_{\mathcal{ABE}}. \tag{3.20}$$

and $\mathbb{P}'''_{\mathcal{ABE}}$ should respect,

$$\sum_{\mathcal{E}} \{\gamma \mathrm{PR}_{\mathcal{BE}} \otimes L'_{\mathcal{A}} + (1-\gamma)\mathbb{P}'''_{\mathcal{ABE}}\} = W_{\mathcal{AB}}, \tag{3.21a}$$

$$\sum_{\mathcal{A}} \{\epsilon \mathrm{PR}_{\mathcal{AB}} \otimes L_{\mathcal{E}} + (1-\epsilon)\mathbb{P}'''_{\mathcal{ABE}}\} = W_{\mathcal{BE}}. \tag{3.21b}$$

We note that in (3.20) we have used the relation $\alpha = (1-\gamma)\epsilon$. As a direct consequence of the *depolarization* procedure (3.15), it follows that any tripartite correlation in a Bell scenario with binary inputs and outputs can be mapped to the form given in (3.20), while keeping the CHSH values $\beta(\mathcal{A},\mathcal{B})$ and $\beta(\mathcal{B},\mathcal{E})$ unchanged. Specifically, within each of these slices, the CHSH values

are solely determined by the parameters (α, γ), such that:

$$\beta(\mathcal{A},\mathcal{B})_{\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)}_{\mathcal{ABE}}} = \frac{1+\alpha}{2}; \tag{3.22}$$

$$\beta(\mathcal{B},\mathcal{E})_{\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)}_{\mathcal{ABE}}} = \frac{1+\gamma}{2}. \tag{3.23}$$

We are now in a position to tackle the main task: determining the maximum achievable value of $\beta(\mathcal{B},\mathcal{E})$ for a given fixed $\beta(\mathcal{A},\mathcal{B})$, subject to the constraints imposed by the information causality criteria (3.1), (3.2), and (3.37). This problem can be formulated as the following optimization:

$$\begin{aligned} \max \quad & \beta(\mathcal{B},\mathcal{E})_{\mathbb{P}_{\mathcal{ABE}}} \\ \text{subj to} \quad & \mathcal{I}^q_{\mathbb{P}_{\mathcal{ABE}}} \leq \mathcal{C}^q \\ & \beta(\mathcal{A},\mathcal{B}) = p \end{aligned} \tag{3.24}$$

for a given value $p \in [0.5, 1]$. The $\mathcal{IC}$ constraints in Eqs. (3.1), (3.2), (3.3), and (3.37) can generally be written as $\mathcal{I}^q_{\mathbb{P}_{\mathcal{ABE}}} \leq \mathcal{C}^q$, where $\mathcal{I}^q_{\mathbb{P}_{\mathcal{ABE}}}$ denotes the $\mathcal{IC}$ functional, i.e., a sum of mutual information terms that depend on the distribution $\mathbb{P}_{\mathcal{ABE}}$, and $\mathcal{C}^q$ represents constants determined by the chosen protocol and the communication channel. While the functional $\mathcal{I}$ is generally a function of the joint probability distribution P of all variables in the scenario, for a fixed protocol in (3.24), we can equivalently write $\mathcal{I}^q_P = \mathcal{I}^q_{\mathbb{P}_{\mathcal{ABE}}}$.

Let us consider an optimal tripartite distribution, $\mathbb{P}^*_{\mathcal{ABE}}$, that solves the optimization problem (3.24). As previously shown, this distribution can be mapped via LOSR into $\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)}_{\mathcal{ABE}}$, while preserving the CHSH values $\beta(\mathcal{A},\mathcal{B})$ and $\beta(\mathcal{B},\mathcal{E})$. Moreover, since LOSR corresponds to a local post-processing procedure, the data processing inequality (3.5) implies:

$$\mathcal{I}^q_{\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)}_{\mathcal{ABE}}} \leq \mathcal{I}^q_{\mathbb{P}^*_{\mathcal{ABE}}}. \tag{3.25}$$

Since the upper bounds $\mathcal{C}^q$ do not depend on the specific correlation $\mathbb{P}^*_{\mathcal{ABE}}$, the distribution obtained through the transformation $\mathbb{P}^*_{\mathcal{ABE}} \xmapsto{\text{LOSR}} \mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)}_{\mathcal{ABE}}$ cannot violate any of the $\mathcal{IC}$ constraints. Therefore, the maximal CHSH values allowed under $\mathcal{IC}$ are always realized by $\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)}_{\mathcal{ABE}}$. That is, $\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)}_{\mathcal{ABE}}$ captures all optimal solutions of the problem (3.24), i.e.,

$$\beta(\mathcal{B},\mathcal{E})_{\mathbb{P}^*_{\mathcal{ABE}}} \in \left\{ \beta(\mathcal{B},\mathcal{E})_{\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)}_{\mathcal{ABE}}} \right\}_{\alpha,\gamma}. \tag{3.26}$$

We now focus on determining the explicit forms of the distributions $L'^*_{\mathcal{A}}$, $L^*_{\mathcal{E}}$, and $\mathbb{P}'''^*_{\mathcal{ABE}}$ that solve the optimization problem in Eq. (3.24). Let us first consider $\mathbb{P}'''^*_{\mathcal{ABE}}$. In this context, we observe that the maximally uncorrelated distribution $W_{\mathcal{ABE}}$ ($p_{W_{\mathcal{ABE}}}(a,b,e|x,y,z) = 1/8$) minimizes the $\mathcal{IC}$ functional, i.e., $\mathcal{I}^q_{W_{\mathcal{ABE}}} \leq \mathcal{I}^q_{\mathbb{P}_{\mathcal{ABE}}}$ for all $\mathbb{P}_{\mathcal{ABE}}$. Consequently, any other choice of $\mathbb{P}'''_{\mathcal{ABE}}$ distinct from $W_{\mathcal{ABE}}$ cannot produce a smaller value of the $\mathcal{IC}$ functional. This result follows directly

from the *convexity of mutual information*, which applied to the decomposition in (3.20) yields

$$\mathcal{I}^q_{\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)}_{\mathcal{ABE}}} \leq \alpha\mathcal{I}^q_{\mathrm{PR}_{\mathcal{AB}}\otimes L_{\mathcal{E}}} + \gamma\mathcal{I}^q_{\mathrm{PR}_{\mathcal{BE}}\otimes L'_{\mathcal{A}}} + (1-\alpha-\gamma)\mathcal{I}^q_{\mathbb{P}'''_{\mathcal{ABE}}}, \tag{3.27a}$$

$$\mathcal{I}^q_{\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)W}_{\mathcal{ABE}}} \leq \alpha\mathcal{I}^q_{\mathrm{PR}_{\mathcal{AB}}\otimes L_{\mathcal{E}}} + \gamma\mathcal{I}^q_{\mathrm{PR}_{\mathcal{BE}}\otimes L'_{\mathcal{A}}} + (1-\alpha-\gamma)\mathcal{I}^q_{W_{\mathcal{ABE}}}, \tag{3.27b}$$

Here, $\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)W}_{\mathcal{ABE}}$ refers to the specific case of $\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)}_{\mathcal{ABE}}$ in which $\mathbb{P}'''_{\mathcal{ABE}} = W_{\mathcal{ABE}}$ as in (3.20). By subtracting the two expressions in (3.27) and noting that $\mathcal{I}^q_{W_{\mathcal{ABE}}} \leq \mathcal{I}^q_{\mathbb{P}'''_{\mathcal{ABE}}}$, we obtain

$$\mathcal{I}^q_{\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)W}_{\mathcal{ABE}}} \leq \mathcal{I}^q_{\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)}_{\mathcal{ABE}}}. \tag{3.28}$$

Simultaneously, from (3.21) we see that the distribution $\mathbb{P}'''_{\mathcal{ABE}}$ does not affect the CHSH values, i.e., $\beta(\mathcal{A},\mathcal{B})_{\mathbb{P}'''_{\mathcal{ABE}}} = \beta(\mathcal{B},\mathcal{E})_{\mathbb{P}'''_{\mathcal{ABE}}} = 1/2$. Combining this with (3.28), we infer that any choice of $\mathbb{P}'''_{\mathcal{ABE}}$ other than $W_{\mathcal{ABE}}$ cannot improve upon the performance obtained when $\mathbb{P}'''_{\mathcal{ABE}} = W_{\mathcal{ABE}}$. This is because (3.28) guarantees that any alternative $\mathbb{P}'''_{\mathcal{ABE}}$ increases the value of the $\mathcal{IC}$ functional closer to the upper bound $\mathcal{C}^q$—for any α and γ—without enhancing $\beta(\mathcal{B},\mathcal{E})$. Therefore, any attempt to achieve $\beta(\mathcal{B},\mathcal{E})_{\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)}_{\mathcal{ABE}}} > \max\{\beta(\mathcal{B},\mathcal{E})_{\mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)W}_{\mathcal{ABE}}}\}$ would violate the $\mathcal{IC}$ constraint. Hence, it suffices to consider the optimal distribution $\mathbb{P}^*_{\mathcal{ABE}}$ in the following form:

$$\mathbb{P}^{*(\alpha,\gamma)}_{\mathcal{ABE}} = \mathbb{P}^{\mathrm{iso}'(\alpha,\gamma)W}_{\mathcal{ABE}} = \alpha\mathrm{PR}_{\mathcal{AB}} \otimes L^*_{\mathcal{E}} + \gamma\mathrm{PR}_{\mathcal{BE}} \otimes L'^*_{\mathcal{A}} + (1-\alpha-\gamma)W_{\mathcal{ABE}}, \tag{3.29}$$

This corresponds to a family of two-parameter slices of the tripartite no-signaling polytope, fully specified by the local distributions $L'^*_{\mathcal{A}}, L^*_{\mathcal{E}}$.

We now argue that, for deriving monogamy relations of the type (2.36)—whether using the bipartite criteria (3.1), (3.2) or the multipartite forms (3.3), (3.37) based on $\mathcal{IC}$—the optimal choice for the local distributions is *white noise*. Specifically, we have $L'^*_{\mathcal{A}} = W_{\mathcal{A}}$ and $L^*_{\mathcal{E}} = W_{\mathcal{E}}$, with $p_{W_{\mathcal{A}}}(a|x) = p_{W_{\mathcal{E}}}(e|z) = 1/2$. To justify this, consider the distribution $\bar{\mathbb{P}}^{*(\alpha,\gamma)}_{\mathcal{ABE}}$ obtained from $\mathbb{P}^{*(\alpha,\gamma)}_{\mathcal{ABE}}$ by flipping all outputs, which yields:

$$\begin{aligned} p_{\bar{\mathbb{P}}^{*(\alpha,\gamma)}_{\mathcal{ABE}}}(a,b,e|x,y,z) = \alpha p_{\mathrm{PR}_{\mathcal{AB}}\otimes \bar{L}^*_{\mathcal{E}}}(a,b,e|x,y,z) + \gamma p_{\mathrm{PR}_{\mathcal{BE}}\otimes \bar{L}'^*_{\mathcal{A}}}(a,b,e|x,y,z) \\ + (1-\alpha-\gamma)p_{W_{\mathcal{ABE}}}(a,b,e|x,y,z), \end{aligned} \tag{3.30}$$

where $p_{\bar{L}^*_{\mathcal{E}}}(e|z) = p_{L^*_{\mathcal{E}}}(e\oplus 1|z)$ and $p_{\bar{L}'^*_{\mathcal{A}}}(a|x) = p_{L'^*_{\mathcal{A}}}(a\oplus 1|x)$. Since flipping outputs is merely a local post-processing, the data processing inequality (3.5), as in (3.25), guarantees that the $\mathcal{IC}$ functionals associated with the bipartite criteria (3.1), (3.2) and the multipartite criteria (3.3), (3.37) cannot increase. That is:

$$\mathcal{I}^q_{\bar{\mathbb{P}}^{*(\alpha,\gamma)}_{\mathcal{ABE}}} \leq \mathcal{I}^q_{\mathbb{P}^{*(\alpha,\gamma)}_{\mathcal{ABE}}}. \tag{3.31}$$

Furthermore, as noted for the LOSR transformations, the upper bound $\mathcal{C}^q$ remains unchanged. Therefore, if a distribution $\mathbb{P}^{*(\alpha,\gamma)}_{\mathcal{ABE}}$ satisfies a given $\mathcal{IC}$ criterion, $\mathcal{I}^q_{\mathbb{P}^{*(\alpha,\gamma)}_{\mathcal{ABE}}} \leq \mathcal{C}^q$, the corresponding

flipped-outcomes distribution $\bar{\mathbb{P}}^{*(\alpha,\gamma)}_{\mathcal{ABE}}$ also satisfies the same criterion. Importantly, the CHSH values, $\beta(\mathcal{A},\mathcal{B})$ and $\beta(\mathcal{B},\mathcal{E})$, remain unchanged when all outputs are flipped simultaneously, as they depend solely on the coefficients (α,γ) (3.22), (3.23).

Next, consider a new tripartite distribution $\tilde{\mathbb{P}}^{*(\alpha,\gamma)}_{\mathcal{ABE}}$, constructed by averaging the original distribution $\mathbb{P}^{*(\alpha,\gamma)}_{\mathcal{ABE}}$ with its flipped counterpart $\bar{\mathbb{P}}^{*(\alpha,\gamma)}_{\mathcal{ABE}}$, i.e.,

$$\tilde{\mathbb{P}}^{*(\alpha,\gamma)}_{\mathcal{ABE}} = \frac{1}{2}\Big(\mathbb{P}^{*(\alpha,\gamma)}_{\mathcal{ABE}} + \bar{\mathbb{P}}^{*(\alpha,\gamma)}_{\mathcal{ABE}}\Big),$$

such that

$$p_{\tilde{\mathbb{P}}^{*(\alpha,\gamma)}_{\mathcal{ABE}}}(a,b,e|x,y,z) = \frac{1}{2}p_{\mathbb{P}^{*(\alpha,\gamma)}_{\mathcal{ABE}}}(a,b,e|x,y,z) + \frac{1}{2}p_{\bar{\mathbb{P}}^{*(\alpha,\gamma)}_{\mathcal{ABE}}}(a,b,e|x,y,z), \tag{3.32}$$

and specifically,

$$\begin{aligned} p_{\tilde{\mathbb{P}}^{*(\alpha,\gamma)}_{\mathcal{ABE}}}(a,b,e|x,y,z) = {} & \alpha p_{\mathrm{PR}_{\mathcal{AB}}\otimes W_{\mathcal{E}}}(a,b,e|x,y,z) + \gamma p_{\mathrm{PR}_{\mathcal{BE}}\otimes W_{\mathcal{A}}}(a,b,e|x,y,z) \\ & + (1-\alpha-\gamma)p_{W_{\mathcal{ABE}}}(a,b,e|x,y,z), \end{aligned} \tag{3.33}$$

Here, we have used the relations $\frac{1}{2}(L^*_{\mathcal{B}} + \bar{L}^*_{\mathcal{B}}) = W_{\mathcal{B}}$, $\frac{1}{2}(L^*_{\mathcal{E}} + \bar{L}^*_{\mathcal{E}}) = W_{\mathcal{E}}$, and $\frac{1}{2}(W_{\mathcal{ABE}} + \bar{W}_{\mathcal{ABE}}) = W_{\mathcal{ABE}}$. It is important to note that the CHSH values, $\beta(\mathcal{A},\mathcal{B})$ and $\beta(\mathcal{B},\mathcal{E})$, remain unchanged since they depend only on the coefficients (α,γ) as given in (3.22) and (3.23). At this stage, we apply the *convexity of mutual information* again, which allows us to express the $\mathcal{IC}$ functional for the distribution in (3.32) as:

$$\mathcal{I}^q_{\tilde{\mathbb{P}}^{*(\alpha,\gamma)}_{\mathcal{ABE}}} \leq \frac{1}{2}\mathcal{I}^q_{\mathbb{P}^{*(\alpha,\gamma)}_{\mathcal{ABE}}} + \frac{1}{2}\mathcal{I}^q_{\bar{\mathbb{P}}^{*(\alpha,\gamma)}_{\mathcal{ABE}}}. \tag{3.34}$$

Therefore, if the distribution $\mathbb{P}^{*(\alpha,\gamma)}_{\mathcal{ABE}}$ satisfies a given $\mathcal{IC}$ criterion, i.e., $\mathcal{I}^q_{\mathbb{P}^{*(\alpha,\gamma)}_{\mathcal{ABE}}} \leq \mathcal{C}^q$, the symmetrized distribution $\tilde{\mathbb{P}}^{*(\alpha,\gamma)}_{\mathcal{ABE}}$ constructed in (3.32) will also satisfy the same criterion, while retaining identical CHSH values (3.22) and (3.23). Consequently, any optimal distribution $\mathbb{P}^{*(\alpha,\gamma)}_{\mathcal{ABE}}$ that maximizes (3.24) with local distributions $L'^*_{\mathcal{A}}$ and $L^*_{\mathcal{E}}$ produces the same CHSH values as $\tilde{\mathbb{P}}^{*(\alpha,\gamma)}_{\mathcal{ABE}}$, which also satisfies the $\mathcal{IC}$ criterion. Hence, to determine the maximal CHSH values allowed by the $\mathcal{IC}$ constraints in (3.24), it suffices to consider the slice in (3.33), which corresponds to the form presented in the main text:

$$p_{\mathbb{P}^{*(\alpha,\gamma)}_{\mathcal{ABE}}}(a,b,e|x,y,z) = p_{\tilde{\mathbb{P}}^{(\alpha,\gamma)}_{\mathcal{ABE}}}(a,b,e|x,y,z) = \alpha\frac{1}{4}\delta_{a\oplus b,xy} + \gamma\frac{1}{4}\delta_{b\oplus e,yz} + (1-\alpha-\gamma)1/8. \tag{3.35}$$

This concludes the proof, confirming that the slice given in (3.14) is indeed optimal.

3.4 No monogamy from bipartite $\mathcal{IC}$

Before presenting our main results, we stress why a genuinely multipartite formulation of $\mathcal{IC}$ is essential for deriving monogamy relations. As illustrated in Fig. 3.3, both the original

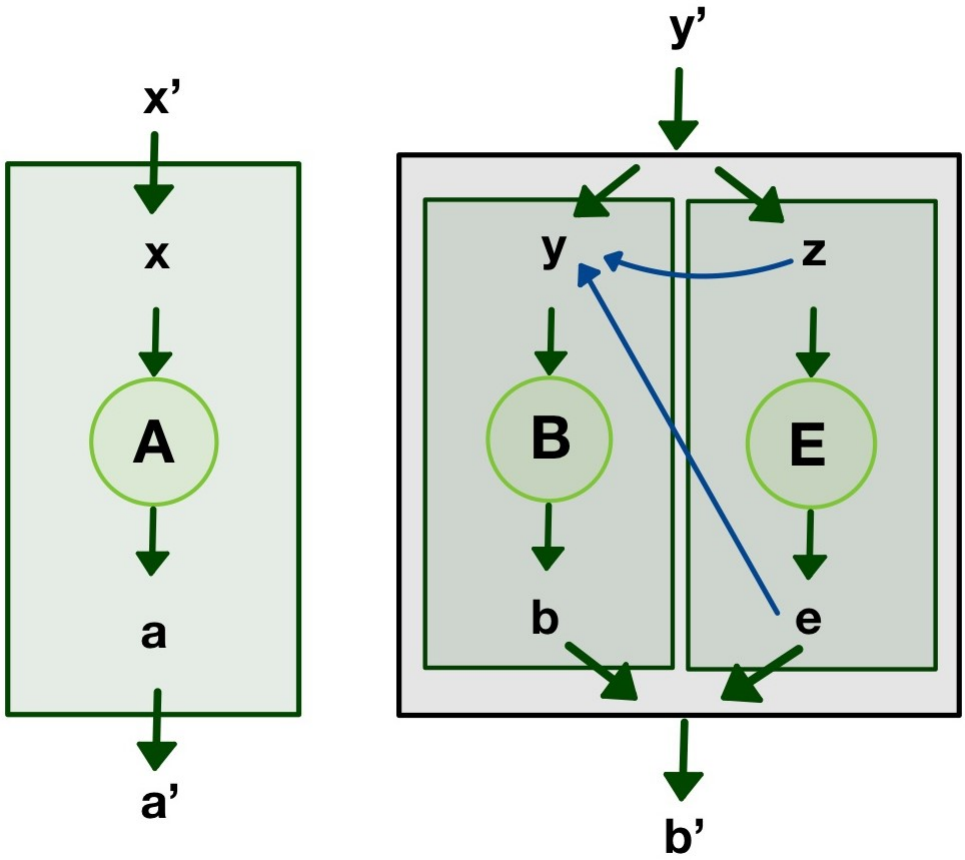

Figure 3.2: **Wiring procedure.** Wiring procedure that maps the original tripartite correlations $p(a, b, e|x, y, z)$ into an effective bipartite distribution $p_{\text{eff}}(a', b'|x', y')$, allowing multipartite scenarios to be analyzed within a bipartite framework.

bipartite condition (3.1) and the generalized bipartite form (3.2) fail to produce non-trivial monogamy constraints for CHSH-type inequalities of the form (2.36). The reason is simple: the inequalities (3.1) and (3.2) are intrinsically bipartite. To test them on a tripartite no-signaling box $p(a, b, e|x, y, z)$ one must first convert the tripartite correlation, by local post-processing, into an effectively bipartite box $\tilde{p}(a', b'|x', y')$. It suffices to consider deterministic local post-processings, commonly called *wirings*. For a concrete bipartition, for example, grouping $\mathcal{B}$ and $\mathcal{E}$ into $\mathcal{B}' \equiv (\mathcal{B}, \mathcal{E})$, a wiring is specified by Boolean functions

$$x = F_1(x'), \qquad a' = F_2(a),$$

$$y = F_3(y', z, e), \qquad z = F_4(y'), \qquad b' = F_5(b, e), \tag{3.36}$$

with $F_i : \{0,1\}^n \to \{0,1\}$ for each i. An example wiring is shown in Fig. 3.2. Note that the grouped parties $\mathcal{B}, \mathcal{E}$ are allowed to signal between themselves under such a wiring. A tripartite box $p(a,b,e|x,y,z)$ therefore violates a bipartite $\mathcal{IC}$ test like (3.2) whenever some wiring produces an effective bipartite box $\tilde{p}(a',b'|x',y')$ that violates the bipartite criterion. This wiring-based approach has been used previously to study $\mathcal{IC}$ in multipartite Bell scenarios [109–111]. In particular, Refs. [112–114] asserted that one can recover the quantum monogamy relation (2.39) from the bipartite $\mathcal{IC}$ conditions (3.1) via appropriate wirings. By contrast, our analysis shows that neither the original criterion (3.1) nor the generalized bipartite form (3.2) implies any stronger-than-no-signaling monogamy relation for *any* wiring of the type (3.36).

To substantiate this claim we proceed as follows. For every tripartite box of the slice (3.14) with parameters $\alpha, \gamma \in [0,1]$, we enumerate all wirings of the form (3.36) to obtain the corresponding effective bipartite distributions $\tilde{p}(a',b'|x',y')$. For each such $\tilde{p}$ we then implement the standard $(2 \mapsto 1)$ RAC protocol, assuming a binary-symmetric noisy classical channel that flips the message bit M with probability $\Pr(M' = M \oplus 1 \mid M) = \epsilon \in (1/2, 1]$. Following the observations in [100], we find that the tightest bounds on the maximal γ for a given α are approached in the limit $\epsilon \to 1/2$. The resulting trade-off curve is plotted in Fig. 3.3 and discussed in the main text.

The numerical and analytical outcome is the following. For $\beta(\mathcal{A},\mathcal{B})$ in the range $[1/2, \frac{1}{2}(2 - 1/\sqrt{2})]$, the bipartite $\mathcal{IC}$ conditions recover the Tsirelson bound, so that $\beta(\mathcal{B},\mathcal{E}) \leq \beta_Q = \frac{1}{2}(1 + 1/\sqrt{2})$. However, for $\beta(\mathcal{A},\mathcal{B})$ in the interval $[\frac{1}{2}(2 - 1/\sqrt{2}), \beta_Q]$ the monogamy constraint implied by these bipartite criteria collapses to the trivial no-signaling monogamy (2.38), namely

$$\beta(\mathcal{B},\mathcal{E}) \leq \tfrac{3}{2} - \beta(\mathcal{A},\mathcal{B}).$$

Therefore the original and generalized bipartite $\mathcal{IC}$ tests do not produce non-trivial monogamy relations beyond those already enforced by no-signaling. In particular, when $\mathcal{A}$ and $\mathcal{B}$ achieve the Tsirelson value $\beta(\mathcal{A},\mathcal{B}) = \beta_Q$, the bipartite $\mathcal{IC}$ criteria place no stronger restriction on $\beta(\mathcal{B},\mathcal{E})$ than no-signaling does. Concretely, whereas the quantum monogamy relation (2.39) would force $\beta(\mathcal{B},\mathcal{E}) \leq \frac{1}{2}$ at $\beta(\mathcal{A},\mathcal{B}) = \beta_Q$, the bipartite $\mathcal{IC}$ bounds only enforce $\beta(\mathcal{B},\mathcal{E}) \leq \frac{1}{2}(2 - 1/\sqrt{2})$.

As we demonstrate below, overcoming this limitation requires the multipartite $\mathcal{IC}$ criterion (3.3), which inherently accounts for genuinely multipartite information flows and is therefore capable of producing non-trivial monogamy relations.

3.5 Monogamy from multipartite $\mathcal{IC}$

Using this multipartite perspective, we investigate tripartite correlations of the type (3.14) in the context of a specific communication task. Concretely, for each correlation $p(a,b,e|x,y,z)$ of the form (3.14), we implement the protocol described earlier for the simplest non-trivial multipartite scenario, corresponding to $(N = 3, n = 2)$. We further assume that classical communication channels between $\mathcal{A}$ and $\mathcal{B}$, as well as between $\mathcal{E}$ and $\mathcal{B}$, are independent binary symmetric

noisy channels, flipping the transmitted bit with probabilities $p(M_1' = M_1 \oplus 1|M_1) = \epsilon_1$ and $p(M_2' = M_2 \oplus 1|M_2) = \epsilon_2$, respectively. Under these assumptions, the multipartite $\mathcal{IC}$ condition (3.3) becomes

$$\sum_{k=1}^{2}\sum_{j=1}^{2} I(X_j^k : X_j^{3-k}, M_1', M_2', G_j) \leq 2 - \sum_{k=1}^{2} h(1-\epsilon_k). \tag{3.37}$$

Unlike the bipartite $\mathcal{IC}$ conditions (3.1),(3.2), there exist correlations of the type (3.14) which respect the no-signaling monogamy relation (2.38), yet violate the tripartite $\mathcal{IC}$ condition (3.37) for certain values of $\epsilon_1, \epsilon_2 \in (1/2, 1]$. Put differently, the tripartite $\mathcal{IC}$ condition imposes a genuinely non-trivial monogamy constraint of the form (2.14), as illustrated in Figure 3.3. Crucially, when $\mathcal{A}$ and $\mathcal{B}$ reach the Tsirelson bound $\beta(\mathcal{A}, \mathcal{B}) = \frac{1}{2}(1 + \frac{1}{\sqrt{2}})$, the tripartite $\mathcal{IC}$ condition is violated for all $\beta(\mathcal{B}, \mathcal{E}) > 1/2$, up to numerical precision. This establishes our first key result:

Result 3.1. *When $\mathcal{A}$ and $\mathcal{B}$ witness the maximum quantum violation of the CHSH inequality such that $\beta(\mathcal{A}, \mathcal{B}) = \beta_Q$, tripartite information causality (3.37) implies $\mathcal{B}$ must be completely uncorrelated with any third party $\mathcal{E}$, such that the CHSH value between $\mathcal{B}$ and $\mathcal{E}$ must be $\beta(\mathcal{B}, \mathcal{E}) = 1/2$, thereby recovering the quantum monogamy (2.36).*

Furthermore, the tripartite condition (3.37) yields monogamy bounds that are stricter than those imposed by the no-signaling principle for $\beta(\mathcal{A}, \mathcal{B}) \in [0.8333, \beta_Q]$. In 3.2.1, we provide a detailed explanation of how the refinement introduced in Eq. (3.3) is essential for establishing this result. We next show that, although the monogamy relation derived from (3.37) is not as tight as the quantum monogamy bound (2.36), it is nevertheless sufficient to improve the information-theoretic security of DIQKD protocols.

3.6 Secure DIQKD from $\mathcal{IC}$

As previously discussed, generic monogamy relations of the type (2.36) can be employed to establish the security condition (2.37) for DIQKD protocols based on the CHSH scenario, even against eavesdroppers limited only by no-signaling principle[81–83, 98]. In Figure 3.3, we illustrate this security condition for DIQKD. It is evident that neither the no-signaling constraint (2.38) nor the bipartite $\mathcal{IC}$ criteria (3.1),(3.2) provide security for quantum correlations within the achievable range $\beta(\mathcal{A}, \mathcal{B}) \leq \beta_Q$. By contrast, for $\beta(\mathcal{A}, \mathcal{B}) \in [0.8471, \beta_Q]$, the monogamy relation resulting from the tripartite $\mathcal{IC}$ criterion (3.37) meets the condition (2.37), thus guaranteeing DIQKD security. This constitutes the central result of our work.

Result 3.2. *Tripartite information causality (3.37) ensures security of DIQKD whenever $\mathcal{A}$ and $\mathcal{B}$ witness the CHSH value in the realizable range of quantum correlations, $\beta(\mathcal{A}, \mathcal{B}) \in [0.8471, \beta_Q]$.*

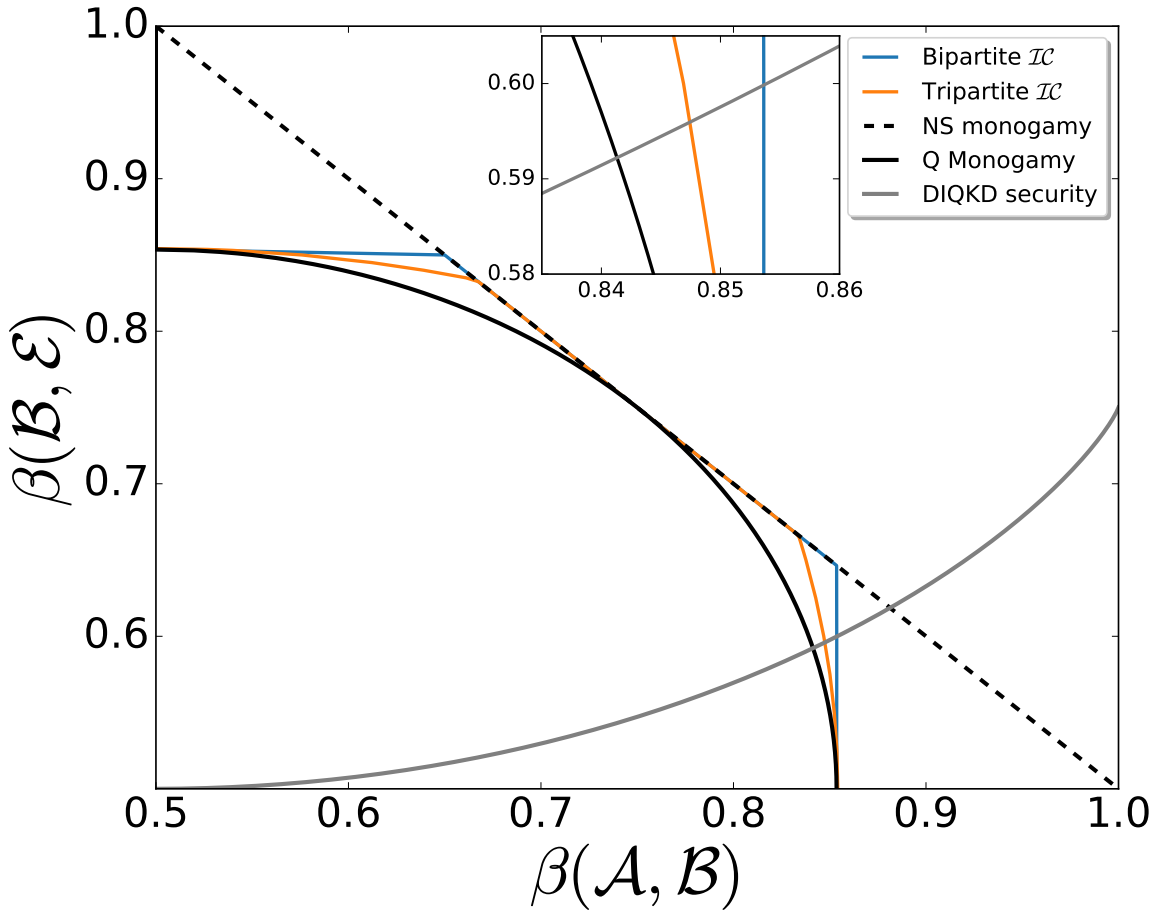

Figure 3.3: **Plot of the maximum value of the CHSH functional $\beta(\mathcal{B},\mathcal{E})$, as determined by the monogamy relations of the form (2.36) analyzed in this work, plotted against the CHSH functional $\beta(\mathcal{A},\mathcal{B}) \in [1/2, 1]$.** The dashed and solid black curves correspond to the monogamy relations implied by the no-signaling condition (2.38) and by quantum theory (2.39), respectively. The solid blue curve shows the monogamy relation obtained from the bipartite $\mathcal{IC}$ criteria (3.1), (3.2), accounting for all wirings of the form (3.36). The solid orange curve represents the monogamy relation derived from the tripartite $\mathcal{IC}$ criterion (3.37). The solid gray line illustrates the DIQKD security condition (2.37). Unlike the bipartite criterion, the tripartite $\mathcal{IC}$ framework produces a nontrivial monogamy relation for $\beta(\mathcal{A},\mathcal{B}) \in [0.8333, \beta_Q = \frac{1}{2}(1+\frac{1}{\sqrt{2}})]$, and guarantees DIQKD security for $\beta(\mathcal{A},\mathcal{B}) \in [0.8471, \beta_Q]$.

These findings highlight a meaningful bridge between foundational principles and practical cryptographic applications. In particular, the security guarantee derived from $\mathcal{IC}$ is strictly stronger than that obtained from no-signaling monogamy relations, and it applies throughout the interval $\beta(\mathcal{A},\mathcal{B}) \in [0.8471, \beta_Q]$, a region accessible in quantum experiments. This naturally prompts the broader question of whether $\mathcal{IC}$-based arguments can generally provide tighter security assurances than those relying only on the no-signaling principle. Developing sharper

security bounds and incorporating randomness amplification protocols could further strengthen this approach. More broadly, since $\mathcal{IC}$ enforces stricter limits on correlations than no-signaling alone, our results point toward a promising avenue for advancing DI security proofs in QKD.

3.7 Summary

To summarize, most theoretical security proofs in DIQKD rely solely on the no-signaling principle, without assuming any specific physical model of the devices. Yet, principles such as $\mathcal{IC}$ indicate that many no-signaling correlations cannot occur in nature, as they lead to implausible consequences. This motivates the fundamental question of whether stronger-than-no-signaling principles can provide the basis for security proofs.

In this work, we showed that assuming parties are constrained by the multipartite $\mathcal{IC}$ principle ensures security for a range of experimentally realizable parameters. Importantly, even if $\mathcal{IC}$ does not fully characterize the quantum set, our results demonstrate that, provided $\mathcal{IC}$ is a fundamental principle of nature, secure cryptographic keys can be established against supra-quantum adversaries. This conclusion follows from the nontrivial monogamy of Bell inequality violations implied by the multipartite formulation of $\mathcal{IC}$, which, strikingly, recovers strong quantum-like monogamy for maximal CHSH violations without reference to Hilbert space structure.

Our analysis also highlights the necessity of a multipartite perspective: bipartite versions of $\mathcal{IC}$ alone fail to impose monogamy constraints on CHSH correlations. Since every $\mathcal{IC}$ criterion is inherently protocol-dependent, it remains open whether these limitations can be overcome by alternative protocols or by extending the framework beyond binary symmetric noisy channels.

Building on prior developments that connect no-signaling with DIQKD security, our results lay the groundwork for incorporating stricter operational principles into practical quantum cryptography. Natural directions for future research include extending security proofs to more general adversarial models, such as collective and coherent attacks [115], studying amplification protocols [96], and adapting the multipartite $\mathcal{IC}$ framework to cryptographic tasks based on more general families of Bell inequalities [116]. Together, these directions point to a promising research program for deepening the foundational and applied role of information causality in quantum cryptography.

Chapter 4

Certification of semi-device-independent security through wave-particle duality experiments

"Indulge your imagination in every possible flight."

—Jane Austen, Pride and Prejudice

Bohr's principle of complementarity, the idea that quantum systems can exhibit wave-like or particle-like properties depending on how they are measured, has long been central to discussions of the foundations of quantum mechanics [19, 117]. Traditionally, complementarity has been demonstrated in interferometric experiments: interference fringes reflect wave-like behaviour, while the ability to unambiguously determine which path a particle takes reflects particle-like behaviour. The key feature is that one cannot simultaneously maximize both and depends on how the system is measured [33].

Over the past two decades, this qualitative notion has been sharpened into quantitative relations. Specifically, complementarity has been expressed as a duality inequality relating path distinguishability $\mathcal{D}$ and interference visibility $\mathcal{V}$, as well as through entropic uncertainty relations involving min- and max-entropies. These entropic quantities are directly relevant in quantum information theory because they bound guessing probabilities, randomness, and secrecy [40, 41].

This connection is particularly powerful in the *semi-device-independent (SDI) framework*. In SDI protocols, one assumes only a bound on the dimension of the physical system (for example, that Alice transmits a qubit), but otherwise treats the preparation and measurement devices as black boxes [30]. By linking wave–particle duality relations to SDI witnesses, it becomes possible to certify quantum security without requiring full trust in the devices.

In this chapter, we develop this connection in detail. We begin by formalizing the SDI prepare-and-measure scenario and the dimension witness relevant for the $(4, 2, 2)$ quantum random access code (QRAC) case (four preparations, two measurements, and binary outcomes). We then show how this witness can be decomposed into experimentally accessible interferometric quantities: $\mathcal{D}$ and $\mathcal{V}$. A symmetric case of the tunable beam splitter (TBS) measurement then reduces the witness to a remarkably simple form, $S = 2(\mathcal{D} + \mathcal{V})$. This chapter includes both a theoretical framework and a proof-of-principle optical experiment using orbital angular momentum states in a fiber-based interferometer. Additionally, we tighten existing security bounds for SDI-QRAC schemes, contributing to stronger and more reliable quantum communication protocols. The chapter also provides the full theoretical interferometer model linking the beam splitter phases to the operational quantities $\mathcal{D}$ and $\mathcal{V}$, and expresses the results in both operational and entropic terms.

4.1 Redefining the interferometric quantities

We now introduce the operational definitions of $\mathcal{D}$ and $\mathcal{V}$, as defined in [40], which quantify the which-path information and interference in a two-path interferometer. Particle-like behaviour is captured by measurements in the Z basis, which identifies the path taken by the system. In contrast, wave-like behaviour is associated with phase coherence and spatial delocalization. For a qubit system $\mathcal{H}_A$, this corresponds to observables in the X–Y plane of the Bloch sphere, which are mutually unbiased with respect to Z.

The input distinguishability $\mathcal{D}$ measures the bias in optimally determining which path (Z) the photon follows, given the interferometer state. Formally, it is defined as

$$\mathcal{D} := 2p_{\text{guess}}(Z) - 1, \tag{4.1}$$

where $p_{\text{guess}}(Z)$ denotes the maximum probability of correctly inferring the photon's path, optimized over all possible measurement strategies.

Experimentally, $\mathcal{D}$ is obtained by alternately blocking the upper (U) and lower (L) interferometer arms and measuring the detection probabilities p_0 and p_1 at detectors D_0 and D_1. The asymmetry in these detection rates reflects the degree of distinguishability. This leads to the operational definition:

$$\mathcal{D} := \tfrac{1}{2}(\mathcal{D}_U + \mathcal{D}_L), \tag{4.2}$$

with

$$\mathcal{D}_{U(L)} := \left[\tfrac{|p_0 - p_1|}{p_0 + p_1}\right]_{\text{path } U(L) \text{ blocked}}. \tag{4.3}$$

The interferometric visibility $\mathcal{V}$, on the other hand, quantifies the ability to predict the output phase W when interference is present. It is given by

$$\mathcal{V} := \max_{W \in XY} [2p_{\text{guess}}(W) - 1], \tag{4.4}$$

where $p_{\text{guess}}(W)$ is the probability of correctly predicting the detection outcome from the interference pattern, maximized over all observables in the X–Y plane of the Bloch sphere.

Operationally, $\mathcal{V}$ is measured by varying the relative phase ϕ_x between the two paths and recording detection rates at both output ports. For each detector $j = 0, 1$, visibility is evaluated as

$$\mathcal{V}_j := \frac{p_j^{\max} - p_j^{\min}}{p_j^{\max} + p_j^{\min}}, \tag{4.5}$$

and the overall visibility is obtained by averaging:

$$\mathcal{V} := \tfrac{1}{2}(\mathcal{V}_0 + \mathcal{V}_1). \tag{4.6}$$

As an example, consider the interferometric arrangement shown in Fig. 4.1. A single photon first passes through a balanced (50:50) beam splitter (BS_1), creating a coherent superposition of two spatial paths. A tunable phase ϕ_x is then applied to one arm, preparing the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + ie^{i\phi_x}|1\rangle)$. The two paths are subsequently recombined at a tunable beam splitter (TBS), and interference is observed by monitoring the output probabilities as ϕ_x is varied.

Together, $\mathcal{D}$ and $\mathcal{V}$ provide complementary measures of particle- and wave-like behaviour. Importantly, they satisfy the wave–particle duality relation (2.47), which can also be expressed in terms of guessing probabilities as

$$p_{\text{guess}}(Z)(1 - p_{\text{guess}}(Z)) + p_{\text{guess}}(W)(1 - p_{\text{guess}}(W)) \geq \tfrac{1}{4}. \tag{4.7}$$

This perspective is inspired by earlier work, in particular Ardehali's delayed-choice-based QKD protocol [118]. In that scheme, the cryptographic task is embedded into a delayed-choice interferometric setup, where both the input and output beam splitters play a role. Key generation is achieved when both beam splitters are removed, corresponding to direct preparation and measurement in the computational basis. Security checks are carried out by monitoring interference statistics: with both beam splitters inserted, the protocol tests resilience against intercept-and-forward attacks, while configurations with only one beam splitter inserted enable the detection of intercept-and-reprepare strategies. In this way, control over both beam splitters unifies key distribution and eavesdropping detection within a single delayed-choice-inspired framework. Motivated by this idea, we reinterpret the SDI prepare-and-measure (PM) scenario as a WPD game, in which the SDI witness can be expressed directly in terms of interferometric quantities (see Fig. 4.1).

4.2 Linking the SDI witness to interferometric quantities

In subsection 2.4.2 of Chapter 2, we introduced the SDI framework and the SDI witness (2.60) built from the eight conditional probabilities in (2.59) in the $(4, 2, 2)$ PM scenario. Our goal in this section is to rewrite that witness in a form that makes its dependence on the interferometer's operational quantities $\mathcal{D}$ and $\mathcal{V}$ explicit.

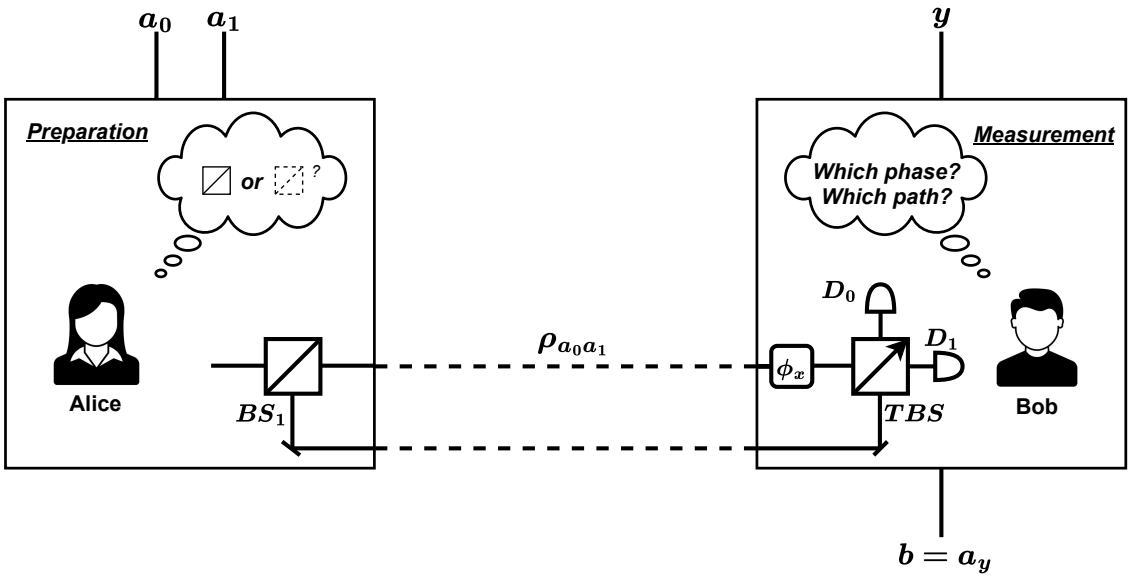

Figure 4.1: **SDI Witness and Wave–Particle Games**: In the *preparation stage*, Alice is given two classical bits (a_0, a_1), which she encodes into a two-dimensional quantum state $\rho_{a_0a_1}$. The encoding procedure involves deciding whether or not to insert an unbiased beam splitter (BS_1) for each computational-basis preparation. In the *measurement stage*, the encoded state undergoes a phase shift ϕ_x before reaching Bob, who then performs a measurement determined by his chosen input. Bob's apparatus features a tunable beam splitter (TBS), enabling him to continuously interpolate between particle-like and wave-like measurement settings. Because of wave-particle duality and the principle of complementarity, Bob is subject to intrinsic trade-offs: it is impossible for him to access both which-path and which-phase information with unlimited accuracy. These operational constraints, expressed through interferometric visibility $\mathcal{V}$ and path distinguishability $\mathcal{D}$, form the foundation for assessing the SDI witness.

For the task at hand, Alice's encodings are chosen as

$$\begin{aligned} \rho_{00} &= |0\rangle\langle 0|, \quad \rho_{01} = |-\rangle\langle -|, \\ \rho_{10} &= |+\rangle\langle +|, \quad \rho_{11} = |1\rangle\langle 1|, \end{aligned} \tag{4.8}$$

with $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ the equal superpositions of the path states. Thus, parity-even inputs $(00, 11)$ correspond to computational basis states (path information), while parity-odd inputs $(01, 10)$ correspond to superposition states (wave information).

On the receiving end, Bob is allowed two measurement settings, $y = 0$ and $y = 1$. In the interferometric picture, these settings correspond to two orthogonal binary observables: $y = 0$ represents a measurement in the computational basis $\{|0\rangle, |1\rangle\}$, revealing which-path information, while $y = 1$ represents a measurement in the Hadamard basis $\{|+\rangle, |-\rangle\}$, probing interference. Operationally, these two settings are realized by the tunable beam splitter (TBS) and subsequent detection at output ports. In practice, Bob's choice of y dictates whether the

interferometer is effectively set to extract particle-like or wave-like information from Alice's signal.

Recall the witness (2.60):

$$S = E_{00,0} + E_{00,1} + E_{01,0} - E_{01,1} - E_{10,0} + E_{10,1} - E_{11,0} - E_{11,1}, \tag{4.9}$$

where $E_{a_0a_1,y} = P(b = 0 \mid a_0, a_1, y)$ are the conditional probabilities of Bob's outcomes.

Hence, two natural groupings appear in equation (4.9): the four terms with parity-even inputs $(00, 11)$ and the four terms with parity-odd inputs $(01, 10)$. We now analyze each in turn.

Even-parity block. In a prepare-and-measure scenario, the behaviour of the system is fully characterized by Alice's prepared state ρ_{a_0,a_1} and Bob's measurement choice M_y. Building on the operational definition of $\mathcal{D}$ in (4.1), we refine the notion of distinguishability for each configuration (a_0, a_1, y, b) as

$$\mathcal{D}^b_{a_0,a_1,y} := 2p^{a_0,a_1,y}_{\text{path},\phi_x} - 1, \tag{4.10}$$

where

$$p^{a_0,a_1,y}_{\text{path},\phi_x} \equiv P_{\phi_x}(b = a_0 \mid a_0, a_1, y)\, \delta_{a_0\oplus a_1=0}. \tag{4.11}$$

The Kronecker delta ensures that path information contributes only for even-parity inputs, i.e. when $a_0 \oplus a_1 = 0$. This is consistent with the encoding in Eq. (4.8), since $\rho_{00} = |0\rangle\langle 0|$ and $\rho_{11} = |1\rangle\langle 1|$ contain explicit which-path information.

The average path-guessing probability across all even-parity configurations is then

$$p_{\text{path},\phi_x} = \frac{1}{4} \sum_{a_0,a_1,y} P_{\phi_x}(b = a_0 \mid a_0, a_1, y)\, \delta_{a_0\oplus a_1=0}, \tag{4.12}$$

which is independent of ϕ_x due to the structure of the encoding. Substituting this into the definition of the SDI witness shows that the even-parity contribution to S_{ϕ_x} is exactly governed by the distinguishabilities $\mathcal{D}_{a_0,a_1,y}$:

$$S_{\phi_x}(\text{even}) = \tfrac{1}{2} \sum_{a_0,a_1,y} \mathcal{D}_{a_0,a_1,y}\, \delta_{a_0\oplus a_1=0}. \tag{4.13}$$

Odd-parity block. For odd-parity inputs, $(a_0, a_1) = (0, 1)$ or $(1, 0)$, Alice prepares the superposition states $|-\rangle$ or $|+\rangle$, respectively. These encodings exhibit interference, and their contribution to the witness is captured by the visibility of the corresponding fringes. At the level of individual configurations we define

$$\mathcal{V}^b_{a_0,a_1,y} := 2p^{b,a_0,a_1,y}_{\text{max}} - 1, \tag{4.14}$$

with

$$p^{b,a_0,a_1,y}_{\text{max}} \equiv \max_{\phi_x} P_{\phi_x}(b \mid a_0, a_1, y)\, \delta_{a_0\oplus a_1=1}. \tag{4.15}$$

Here the maximization over ϕ_x reflects the tunability of the interferometer phase, which determines the amplitude of the interference pattern. The delta factor ensures that visibility is only considered for odd-parity encodings.

Using these definitions, the odd-parity terms in the SDI witness can be expressed as a sum over visibilities:

$$S_{\phi_x}(\text{odd}) = \tfrac{1}{2} \sum_{a_0,a_1,y,b} \mathcal{V}^b_{a_0,a_1,y}\, \delta_{a_0\oplus a_1=1}\, \delta_{b=a_y}. \tag{4.16}$$

Maximization over ϕ_x guarantees that each contribution is taken at its optimal interference visibility.

Final SDI witness. Putting the even- and odd-parity contributions together, the witness takes the compact form

$$\max_{\phi_x} S_{\phi_x} = \tfrac{1}{2} \sum_{a_0,a_1,y} \mathcal{D}_{a_0,a_1,y}\, \delta_{a_0\oplus a_1=0} + \tfrac{1}{2} \sum_{a_0,a_1,y,b} \mathcal{V}^b_{a_0,a_1,y}\, \delta_{a_0\oplus a_1=1}\, \delta_{b=a_y}. \tag{4.17}$$

This decomposition makes clear that the SDI witness directly quantifies the sum of optimal distinguishabilities and visibilities across the relevant configurations of the game. Crucially, the derivation requires only a single parameter optimization (over ϕ_x), while the distinguishability part remains phase-independent by construction.

4.2.1 Symmetric TBS scenario

The general decomposition of Eq. (4.17) shows that the SDI witness is the sum of contributions from even-parity distinguishabilities and odd-parity visibilities, each optimized over the interferometer phase. We now focus on the SDI witness as realized in a concrete wave–particle duality (WPD) guessing game implemented with a simple photonic interferometer. The interferometer we analyze consists of an input 50:50 beam splitter, a controllable relative phase in one arm, and a tunable beam splitter (TBS) that plays the role of the second beam splitter. The setup is illustrated in Fig. 4.1. The key observation is that data collected in two complementary interferometer settings, namely a given phase setting ϕ_x and the shifted setting $\phi_x + \pi$, suffice to reconstruct the SDI witness and to assess both nonclassicality and the SDI security conditions in terms of the interferometric observables.

Following the geometry depicted in Fig. 4.2, Bob's two measurement settings in the SDI guessing game are identified with the following qubit observables:

$$\begin{aligned} M_0(\phi_s,\phi_x) &= \cos\phi_s\,\sigma_z + \sin\phi_s\,(\cos\phi_x\,\sigma_x + \sin\phi_x\,\sigma_y)\,, \\ M_1(\phi_s,\phi_x) &= M_0(\phi_s,\phi_x+\pi), \end{aligned} \tag{4.18}$$

where $0 \le \phi_s \le \pi/2$ denotes the TBS parameter that interpolates continuously between particle-like and wave-like measurement regimes, and $\phi_x \in [0, 2\pi N]$ with $N \in \mathbb{N}$ is the controllable

interferometer phase. Operationally, the σ_z contribution probes which-path information (particle behaviour), while the σ_x and σ_y components probe interference fringes (wave behaviour). By tuning ϕ_s, the measurement interpolates between these two regimes.

The symmetry of the interferometer and the structure of the measurements impose the following relations among the conditional probabilities:

$$E_{00,0} = E_{00,1}, \qquad E_{11,0} = E_{11,1}, \\ E_{01,0} = E_{10,1}, \qquad E_{10,0} = E_{01,1}. \tag{4.19}$$

These identities reflect the fact that interchanging the measurement label y while appropriately permuting the preparation labels leaves the statistics invariant in this symmetric interferometer.

Two additional operational constraints further restrict the possible values of the correlators. First, parity-obliviousness of the encoding ensures that the preparations do not reveal any information about the parity bit $a_0 \oplus a_1$. Second, blocking one interferometer path allows particle-like behaviour to be probed directly, isolating which-path information independently of interference. Together, these features imply the normalization conditions

$$E_{00,0} + E_{11,0} = 1, \\ E_{01,0} + E_{10,0} = 1. \tag{4.20}$$

Specializing the general decomposition of the SDI witness (4.17) to this interferometer and exploiting the symmetries (4.19)–(4.20), we can reduce the configuration-dependent distinguishabilities and visibilities to global parameters. In particular,

$$\mathcal{V}^b_{0,1,y} = \mathcal{V}^b_{1,0,y} = \mathcal{V}, \qquad \mathcal{D}^b_{0,0,y} = \mathcal{D}^b_{1,1,y} = \mathcal{D}, \tag{4.21}$$

so that all odd-parity contributions share the same visibility $\mathcal{V}$, and all even-parity contributions share the same distinguishability $\mathcal{D}$.

With these identifications, the sums in Eq. (4.17) collapse: each parity sector contributes four identical terms, accounting for two preparations and two measurement settings. The resulting expression for the maximized witness is

$$\max_{\phi_x} S_{\phi_x} = 2(\mathcal{D} + \mathcal{V}). \tag{4.22}$$

Equation (4.22) constitutes the central relation in this setting. It demonstrates that, within the symmetric TBS implementation, the SDI witness is directly and simply determined by the two operational quantities embodying wave–particle duality: the input distinguishability $\mathcal{D}$ and the interferometric visibility $\mathcal{V}$. Measuring these two parameters therefore suffices to evaluate the witness, test for violation of classical dimension bounds, and assess SDI security.

4.2.2 Experimental setup

The ideas developed in this work were confirmed in a proof-of-principle experiment conducted by our collaborators (illustrated in Fig. 4.2), which verified the SDI witness and supported our

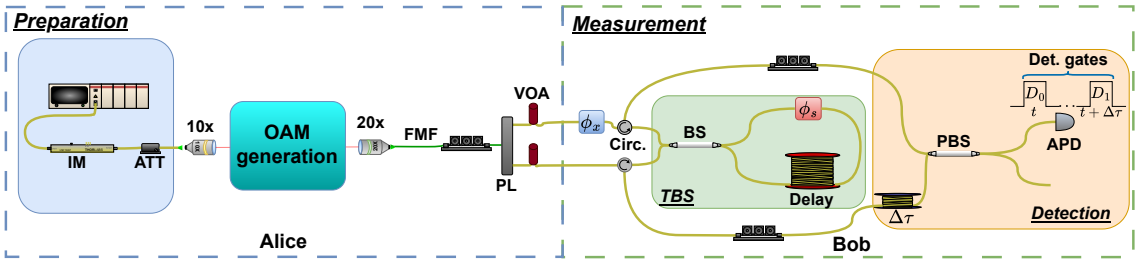

Figure 4.2: **Implementation of the SDI witness.** Alice generates weak coherent states (WCS) encoded in orbital angular momentum (OAM) modes, obtained from strongly attenuated optical pulses. These OAM states are injected into a few-mode fiber (FMF), which is first routed through a manual polarization controller wound around the FMF and then connected to a photonic lantern (PL). The PL decomposes the OAM state into its two linearly polarized components, $|LP_{11a}\rangle$ and $|LP_{11b}\rangle$, assigning them to the two arms of a Mach–Zehnder interferometer. On Bob's side, the two paths are directed into a tunable beamsplitter (TBS) realized with a fiber-optic Sagnac interferometer. This module incorporates a phase modulator ϕ_s and a 300 m fiber delay. After counter-propagating through the Sagnac loop, the paths recombine at a fiber beamsplitter (BS), and the outputs are separated from the inputs by means of two optical circulators (Circ.). The circulator outputs are then time-multiplexed by introducing a fiber delay $\Delta\tau$ in the lower arm, after which they are recombined at a polarization beam splitter (PBS). The transmission of both input paths is optimized using manual polarization controllers. This configuration allows detection with a single-photon detector: the outputs of the TBS are rendered distinguishable by the temporal separation $\Delta\tau$, corresponding to two distinct detection time slots, labeled D_0 and D_1. A second phase modulator ϕ_x is inserted inside the interferometer to enable visibility measurements.

theoretical predictions. The experiment used a fiber-optical MZI with a photonic lantern (PL) as the input beam splitter, decomposing a few-mode fiber (FMF) into its linearly polarized modes. The encoded OAM state $|OAM_{+1}\rangle$ was prepared from attenuated laser pulses via a spatial light modulator and coupled into the FMF, with the $|LP_{11a}\rangle$ and $|LP_{11b}\rangle$ modes forming the two paths of the interferometer.

A fiber-optical Sagnac loop acted as a TBS, with the relative phase ϕ_s controlling the output probabilities at a single-photon detector. To detect both outputs using a single detector, a time-multiplexing scheme was employed by introducing a fiber delay on one output and recombining the paths via a polarizing beam splitter. Detection events were recorded assuming fair sampling for no-click outcomes.

This setup allowed the experimental observation of the wave-particle trade-off and the measurement of the SDI witness, providing a verification of the theoretical predictions discussed in this work, including the relationship between path distinguishability $\mathcal{D}$, interferometric visibility $\mathcal{V}$, and the SDI witness S.

4.3 Interferometric model

To make the link between the abstract SDI witness and the physical setup transparent, we now present an explicit interferometric model. The configuration under study is illustrated in Fig. 4.1 and Fig. 4.2 and consists of a balanced input beam splitter, a relative phase shifter in one arm, and a tunable beam splitter (TBS) acting as the output coupler. Each element is represented by a matrix acting on the two-dimensional Hilbert space spanned by the path states $\{|0\rangle, |1\rangle\}$, with $|0\rangle$ denoting the upper path and $|1\rangle$ the lower path.

Optical elements. The input and output beam splitters are modeled as

$$BS_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \qquad BS_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} i & -1 \\ -1 & i \end{pmatrix}. \tag{4.23}$$

The controllable phase shifters are represented as

$$PM_1 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi_x} \end{pmatrix}, \qquad PM_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi_s} \end{pmatrix}. \tag{4.24}$$

Here ϕ_x is the relative phase scanned in the interferometer arm, while ϕ_s parametrizes the TBS, interpolating between particle- and wave-sensitive measurement regimes.

Output state. The complete transformation acting on the input state is

$$U = BS_2\, PM_2\, PM_1\, BS_1.$$

Applying U to the input $|0\rangle$ produces the state at the detectors:

$$\begin{aligned} |\psi\rangle = \frac{1}{2\sqrt{2}}\Big[& i\big((1+e^{i\phi_s}) + e^{i\phi_x}(1-e^{i\phi_s})\big)\,|D_0\rangle \\ & + \big((e^{i\phi_s}-1) - e^{i\phi_x}(1+e^{i\phi_s})\big)\,|D_1\rangle\Big]. \end{aligned} \tag{4.25}$$

The coefficients in front of $|D_0\rangle$ and $|D_1\rangle$ capture the interference between the two optical paths, with the relative weights determined by ϕ_x and ϕ_s.

Detection probabilities. From Eq. (4.25), the probabilities of detecting the photon at the two output ports are

$$p_0 = |\langle D_0|\psi\rangle|^2 = \tfrac{1}{2}(1+\sin\phi_x \sin\phi_s), \tag{4.26}$$

$$p_1 = |\langle D_1|\psi\rangle|^2 = \tfrac{1}{2}(1-\sin\phi_x \sin\phi_s). \tag{4.27}$$

These sinusoidal dependencies on ϕ_x are the interference fringes observed at the detectors. Their modulation depth is set by the TBS parameter ϕ_s.

Visibility. Maximizing and minimizing p_0 or p_1 with respect to ϕ_x yields the fringe visibility,

$$\mathcal{V} = \sin\phi_s, \tag{4.28}$$

in agreement with the operational definition introduced earlier.

Distinguishability via blocking. To compute the distinguishability, we consider the scenario in which one interferometer arm is blocked, thereby removing all interference contributions. For example, blocking the upper path results in the output state

$$|\psi\rangle = \tfrac{1}{2}\left[i(1+e^{i\phi_s})\,|D_0\rangle + (1-e^{i\phi_s})\,|D_1\rangle\,\right], \tag{4.29}$$

which no longer depends on ϕ_x. In this regime, the bias in detection probabilities corresponds directly to which-path information. Evaluating the difference gives

$$\mathcal{D} = \cos\phi_s. \tag{4.30}$$

Complementarity relation. Equations (4.28) and (4.30) show explicitly that

$$\mathcal{D}^2 + \mathcal{V}^2 = \cos^2\phi_s + \sin^2\phi_s = 1, \tag{4.31}$$

which is the canonical quantitative form of wave–particle complementarity. In this implementation, tuning ϕ_s smoothly interpolates between purely particle-like ($\mathcal{D}=1, \mathcal{V}=0$) and purely wave-like ($\mathcal{D}=0, \mathcal{V}=1$) regimes, with intermediate values tracing the complementarity circle.

This explicit model confirms that the interferometer's operational quantities $\mathcal{D}$ and $\mathcal{V}$ arise naturally from the beam splitter and phase settings, and that they obey the complementarity trade-off exactly. Combined with Eq. (4.22), the witness becomes

$$S = 2(\mathcal{D} + \mathcal{V}),$$

providing a direct link between the optical implementation and the SDI framework.

4.4 Improving the security bound in the SDI scenario

The security framework introduced in Ref. [30] established that in the $2 \to 1$ QRAC scenario, SDI security is guaranteed whenever Bob's success probability exceeds

$$P_B > 0.8415, \tag{4.32}$$

where P_B denotes the average probability that Bob correctly infers the input bit chosen by Alice. In this section we derive a tighter bound on P_B, thereby refining the security condition for SDI quantum key distribution (SDI-QKD).

Joint success probabilities. Consider the task where both Bob and an eavesdropper Eve attempt to guess the parity $a_0 \oplus a_1$ of Alice's two input bits. Clearly,

$$\begin{aligned} P_{B,E}(a_0 \oplus a_1) &\geq P_{B,E}(a_0, a_1) \\ &\geq P_{B,E}(a_0) + P_{B,E}(a_1) - 1, \end{aligned} \tag{4.33}$$

where $P_{B,E}(a_0, a_1)$ (equivalently, $P_{B,E}(a_0 \cap a_1)$) denotes the probability that both a_0 and a_1 are correctly guessed. The second inequality follows from the identity

$$P_{B,E}(a_0 \oplus a_1) = P_{B,E}(a_0 \cup a_1) - P_{B,E}(a_0 \cap a_1),$$

together with the fact that

$$P_{B,E}(a_0 \cup a_1) = P_{B,E}(a_0) + P_{B,E}(a_1) - P_{B,E}(a_0 \cap a_1) \leq 1.$$

Uniform inputs. Assuming that Alice's inputs (a_0, a_1) are uniformly distributed random variables, we have $P_{B,E}(a_0) = P_{B,E}(a_1)$. Denoting this quantity by $P_{B,E}$, inequality (4.33) becomes

$$\begin{aligned} P_{B,E}(a_0 \oplus a_1) &\geq 2P_{B,E}(a_0) - 1 \\ &= 2P_{B,E} - 1. \end{aligned} \tag{4.34}$$

Here $P_{B,E}$ represents the average joint success probability of Bob and Eve.

Worst-case assumptions. In the worst-case scenario, Bob and Eve may collaborate. This imposes the constraints

$$P_{B,E}(a_i) \geq P_B(a_i), \qquad P_{B,E}(a_i) \geq P_E(a_i),$$

for $i = 0, 1$. Using these inequalities in (4.34), we obtain

$$P_{B,E}(a_0 \oplus a_1) \geq 2P_E - 1, \tag{4.35}$$

which relates the joint parity-guessing probability to Eve's individual success probability.

Geometric inequality. To bound $P_{B,E}(a_0 \oplus a_1)$, we employ a geometric inequality involving the expectation values of a_0, a_1, and $a_0 \oplus a_1$:

$$[E(a_0)]^2 + [E(a_1)]^2 + [E(a_0 \oplus a_1)]^2 \leq 1. \tag{4.36}$$

This relation first appeared in Ref. [119]; for completeness we now sketch an independent derivation. Without loss of generality, the prepared state can be written as

$$\rho = \tfrac{1}{2}\left(I + \mathbf{n} \cdot \boldsymbol{\sigma}\right),$$

with $\mathbf{n}$ a Bloch vector and $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. A measurement operator along a unit vector $\mathbf{m}_i$ takes the form

$$M_i = \tfrac{1}{2}\left(I + \mathbf{m}_i \cdot \boldsymbol{\sigma}\right).$$

The expectation value associated with M_i is then

$$E_i = 2\mathrm{Tr}[\rho M_i] - 1 = \mathbf{n} \cdot \mathbf{m}_i.$$

Applying this to the three observables corresponding to $f_j \in \{a_0, a_1, a_0 \oplus a_1\}$, we obtain

$$\sum_j [E(f_j)]^2 = \sum_j (\mathbf{n} \cdot \mathbf{m}_j)^2 \leq |\mathbf{n}|^2 \sum_j |\mathbf{m}_j|^2 \leq 1,$$

since $|\mathbf{n}| \leq 1$ and $\sum_j |\mathbf{m}_j|^2 \leq 1$. This reproduces the inequality (4.36).

Bounding Eve's success. Using the relations

$$E(a_0 \oplus a_1) = 2P_{B,E}(a_0 \oplus a_1) - 1, \quad E(a_i) = 2P_{B,E}(a_i) - 1,$$

inequality (4.36) yields

$$\begin{aligned} P_{B,E}(a_0 \oplus a_1) &\leq \frac{1 + \sqrt{1 - 2(2P_{B,E} - 1)^2}}{2} \\ &\leq \frac{1 + \sqrt{1 - 2(2P_B - 1)^2}}{2}. \end{aligned} \tag{4.37}$$

Combining this with (4.35) gives an explicit upper bound on Eve's success probability:

$$P_E \leq \frac{3 + \sqrt{1 - 2(2P_B - 1)^2}}{4}. \tag{4.38}$$

Improved threshold. Inequality (4.38) implies that the security condition $P_B > P_E$ holds whenever

$$P_B > 0.833, \tag{4.39}$$

which improves upon the earlier threshold of 0.8415. This translates to

$$S > 2.664. \tag{4.40}$$

Thus, the improved security threshold corresponds to requiring that the SDI witness exceed 2.664, refining the previous condition based on $P_B > 0.8415$ (i.e. $S > 2.732$). This relaxed threshold expands the range of experimental parameters under which SDI-QKD can be certified.

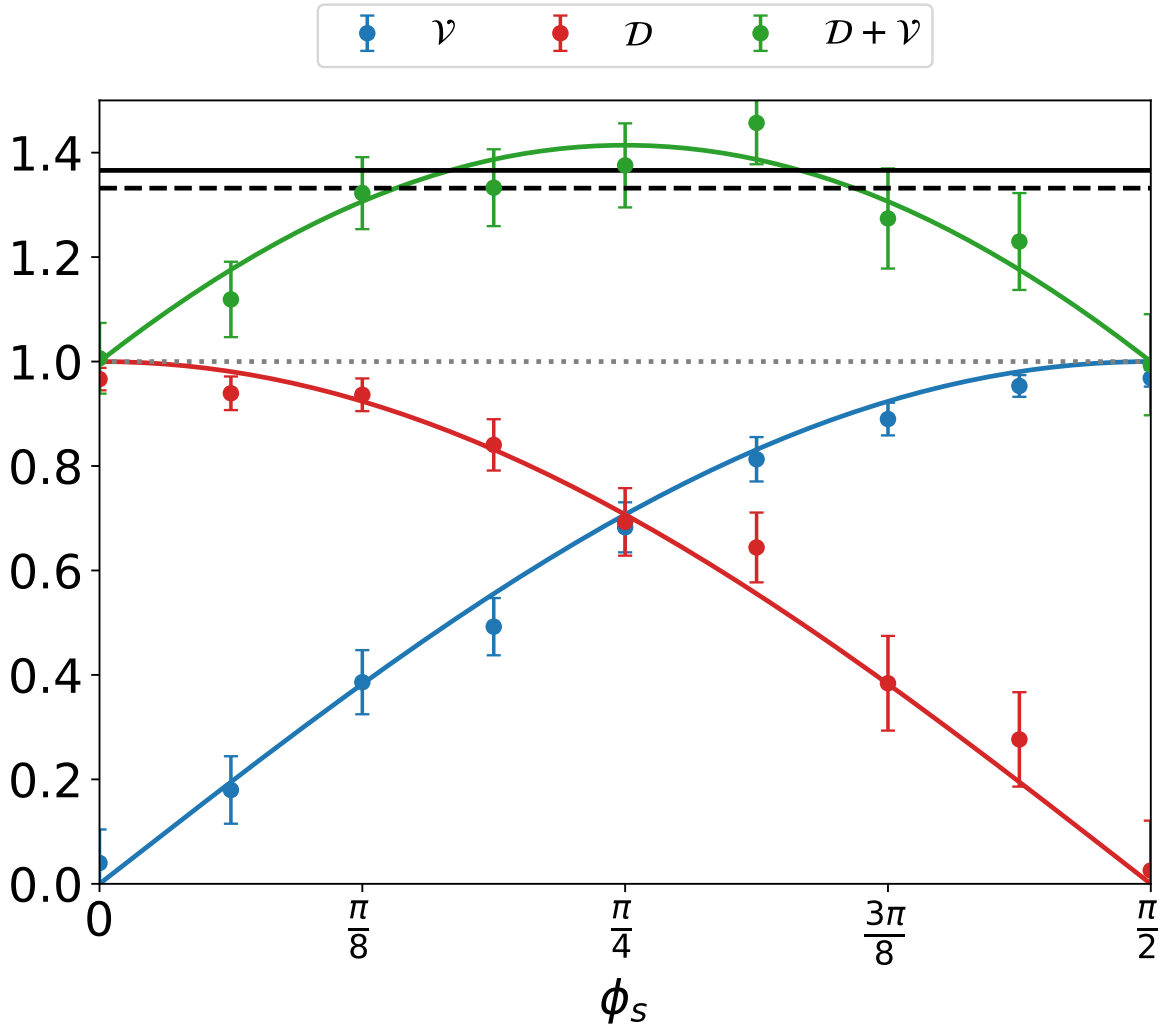

Figure 4.3: **SDI witness from wave–particle duality.** The red and blue curves correspond to the averaged distinguishability $\mathcal{D}$ and visibility $\mathcal{V}$, respectively, while the green curve shows the semi–device-independent (SDI) witness, expressed as $S/2 = \mathcal{D} + \mathcal{V}$. The dotted black line indicates the classical threshold, $\mathcal{D} + \mathcal{V} > 1$. The dashed and solid horizontal lines represent two security limits: the earlier bound at 1.366 and the improved bound at 1.332. Experimental results are shown as circular markers, with error bars determined by error propagation under the assumption of Poissonian statistics for the photon detection counts.

4.4.1 Experimental assessment of SDI witness via wave-particle quantities

In our analysis, we further compare two security thresholds in terms of the interferometric quantities. The original SDI criterion from [30] requires $\mathcal{D}+\mathcal{V} > 1.366$ for secure communication, whereas the improved bound derived in 4.4 relaxes this condition to $\mathcal{D} + \mathcal{V} > 1.332$, thereby enlarging the range of experimentally certifiable security. This demonstrates that a combination of both wave-like and particle-like contributions is necessary to exceed classical limits, with the optimal violation observed when $\mathcal{D} = \mathcal{V} = \sqrt{2}/2$, corresponding to a phase setting of $\phi_s = \pi/4$. Small deviations between experimental points and theoretical predictions arise primarily from the finite interferometer visibility due to the extinction ratio of the photonic lantern, and from statistical limitations imposed by the finite number of experimental repetitions and passive isolation against environmental phase drifts. These results are illustrated in Fig. 4.3 in detail.

Building on this, in the next section we exploit the operational equivalence between wave-particle duality and optimized entropic uncertainty relations to express the SDI witness directly on the $(H_{\max}(W), H_{\min}(Z))$ plane.

4.5 Entropic representation of the SDI witness

An alternative and particularly insightful way of analyzing the SDI witness is to recast it in the *entropic plane*, defined by the pair of quantities $(H_{\max}(W), H_{\min}(Z))$. From a cryptographic perspective, the min-entropy quantifies the unpredictability of Alice's raw key bits against an eavesdropper, that is, it determines how well Eve can guess the outcome. The max-entropy, on the other hand, quantifies the uniformity of the key after privacy amplification and is thus a measure of the extractable secrecy [120].

In the context of MZI implementations, these entropic quantities can be directly expressed in terms of the interferometric parameters $\mathcal{D}$ and $\mathcal{V}$ [40, 41]:

$$H_{\min}(Z) = 1 - \log_2(1 + \mathcal{D}), \tag{4.41a}$$

$$H_{\max}(W) = \log_2\left(1 + \sqrt{1 - \mathcal{V}^2}\right). \tag{4.41b}$$

Equation (4.41a) shows that the larger the distinguishability $\mathcal{D}$, the lower the min-entropy (since Eve's guessing ability improves with which-path information). Conversely, Eq. (4.41b) shows that higher visibility $\mathcal{V}$ lowers the max-entropy, reflecting the increased predictability of interference outcomes.

These two quantities are not independent, but are connected through the *entropic uncertainty relation* (EUR),

$$H_{\min}(Z) + H_{\max}(W) \geq 1, \tag{4.42}$$

which provides an entropic form of the complementarity principle [40]. Indeed, inserting Eqs. (4.41a)–(4.41b) into (4.42) naturally recovers the quadratic complementarity relation $\mathcal{D}^2 + \mathcal{V}^2 \leq 1$ derived in the previous subsection.

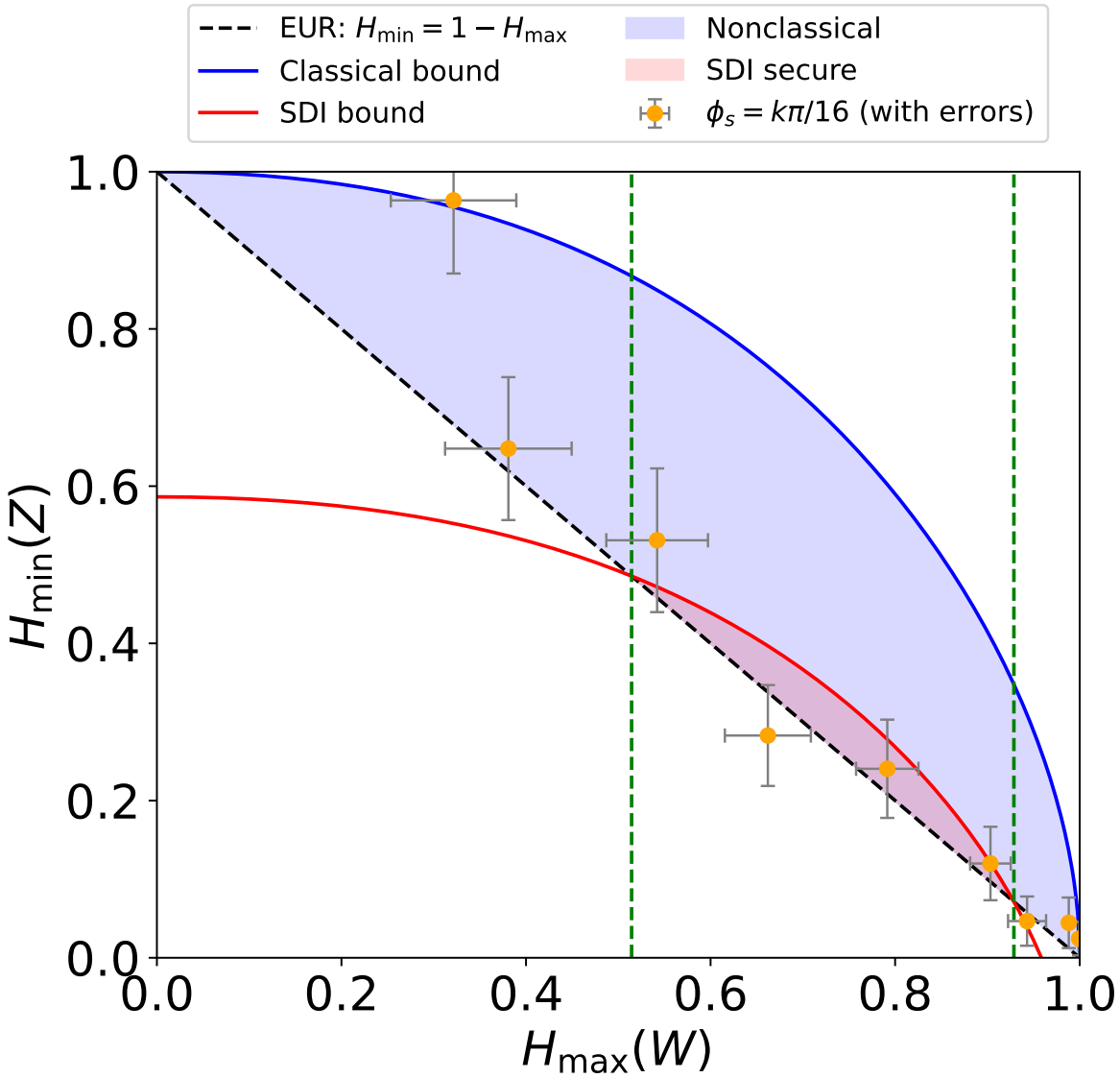

Figure 4.4: **Hierarchy bounds in the entropic plane** $(H_{\max}(W), H_{\min}(Z))$**.** The dashed black curve shows the entropic uncertainty relation (EUR), which represents the most general constraint and is always satisfied. The solid blue line indicates the classical boundary given by the inequality $S \leq 2$; points above this line are classically attainable, while the blue band between the EUR and the classical curve corresponds to genuinely quantum correlations with $S > 2$. The solid red curve represents the semi–device-independent (SDI) security threshold, with the shaded red region beneath it identifying the parameter space where security can be certified. Vertical green dashed lines highlight the compatibility window where the SDI bound intersects with the EUR. Orange data points, with error bars, correspond to the experimental outcomes measured at phase settings $\phi_s = k\pi/16$ for $k = 0, \ldots, 8$. The error bars are determined through error propagation under the assumption of Poissonian statistics for the detected photon counts.

Classical bound. The classical bound on the SDI witness, $S \leq 2$, can also be expressed in the entropic plane. Using Eq. (4.22) and the mapping (4.41), this bound becomes

$$1 - H_{\min}(Z) \leq \log_2\left(2 - \sqrt{1 - \left(2^{H_{\max}(W)} - 1\right)^2}\right). \tag{4.43}$$

The region above this curve is classically accessible, while points lying below it correspond to statistics that cannot be reproduced by any classical dimension-limited strategy. Notably, this bound is always tighter than the generic EUR (4.42), since $H_{\max}(W) \in [0, 1]$ ensures that Eq. (4.43) automatically implies the EUR.

Quantum advantage and SDI security. Surpassing the classical bound (4.43) is thus a necessary condition for demonstrating nonclassicality in the SDI framework. Quantum mechanics achieves this in the region centered at the optimal balance point $\mathcal{D} = \mathcal{V} = 1/\sqrt{2}$, corresponding to equal particle- and wave-like contributions. Importantly, however, not all quantum correlations satisfying the EUR guarantee security: only those for which Bob's success probability exceeds Eve's improved guessing bound are useful for key distribution.

As derived in Sec. 4.4, SDI security is ensured whenever the witness satisfies $S \geq 2.664$. Translated into the entropic plane using (4.41), this becomes

$$1 - H_{\min}(Z) > \log_2\left(2.332 - \sqrt{1 - \left(2^{H_{\max}(W)} - 1\right)^2}\right). \tag{4.44}$$

This inequality carves out a region in the entropic plane, bounded below by the SDI security curve and above by the EUR, within which security can be certified.

Experimental confirmation. Figure 4.4 summarizes these entropic bounds. The dashed black line corresponds to the EUR (4.42), the solid blue curve to the classical bound (4.43), and the solid red curve to the SDI security threshold (4.44). The overlap of the red and black regions defines the *compatibility window* in which both uncertainty and security conditions are simultaneously satisfied. Experimental results (orange points with error bars), obtained at TBS phase settings $\phi_s = k\pi/16$ for $k = 0, \ldots, 8$, fall within the physically allowed region defined by the EUR. Within experimental error, several of these points lie below the SDI security curve, thereby certifying that secure key generation is indeed possible. Quantitatively, security is achieved whenever

$$H_{\max}(W) \in [0.5144,\, 0.9287],$$

corresponding to the range of visibilities that yield witness values above the improved security threshold.

This entropic representation provides an elegant unification: the min- and max-entropies link the physical interferometric parameters $(\mathcal{D}, \mathcal{V})$ to cryptographic guarantees via the EUR. The entropic plane thus makes visually explicit the hierarchy of constraints: the general uncertainty bound, the stricter classicality bound, and the even stronger SDI security condition.

4.6 Summary

In this chapter we have developed a detailed theoretical account of how the SDI witness can be expressed, analyzed, and ultimately assessed through interferometric experiments. Beginning with the QRAC scenario, we showed how the SDI witness naturally decomposes into even- and odd-parity blocks, corresponding to particle-like distinguishability and wave-like visibility, respectively. This revealed the operational meaning of the witness as the sum of two complementary contributions.

Focusing on the case of a symmetric TBS, we demonstrated that the configuration-dependent parameters collapse to two global quantities. This led to the compact relation

$$S = 2(\mathcal{D} + \mathcal{V}),$$

which directly links the SDI witness to the interferometer's operational quantities. The explicit optical model, constructed from beam splitters and phase modulators, confirmed this connection by yielding closed-form expressions $\mathcal{D} = \cos\phi_s$ and $\mathcal{V} = \sin\phi_s$, thereby recovering the standard complementarity relation $\mathcal{D}^2 + \mathcal{V}^2 = 1$ within the SDI framework. We also provide a proof-of-principle experiment that verifies our theoretical claims.

On the security side, we revisited the condition for SDIQKD. By refining the analysis of Bob's and Eve's guessing probabilities, we derived a tighter bound on Bob's success probability, improving the threshold from $P_B > 0.8415$ to

$$P_B > 0.833,$$

which equivalently translates into a witness threshold

$$S > 2.664.$$

This relaxation enlarges the parameter region in which secure key generation can be certified.

Finally, we mapped these results into the entropic plane, where min- and max-entropies provide an alternative lens through which to view wave–particle duality and security. In this representation, the general entropic uncertainty relation sets the broadest boundary, the classical bound defines the stricter region of nonclassicality, and the SDI security condition imposes the most demanding constraint. Experimental points plotted within this plane confirm the theoretical predictions and demonstrate that the SDI framework can indeed certify security under realistic conditions.

Taken together, these results establish a coherent picture: the SDI witness is not only a compact measure of wave–particle duality in interferometric implementations, but also a direct indicator of security in SDI protocols. By connecting distinguishability and visibility to entropic uncertainty and cryptographic thresholds, we provide both conceptual clarity and operational tools for assessing SDI quantum cryptography in practice.

CHAPTER 5

Wave-particle realism in quantum-controlled interferometers assisted by entanglement

"Whatever it is you're seeking won't come in the form you're expecting."

—Haruki Murakami, Kafka on the Shore

One of the most profound lessons of quantum mechanics is that physical systems cannot always be assigned definite properties independent of measurement [45]. Classical intuition suggests that an object should behave either as a particle or as a wave, but quantum theory asserts that such descriptions depend crucially on the measurement context [18, 121]. This tension is most clearly exposed in delayed-choice experiments, originally proposed by Wheeler in [122] and further extensions [123–127], where the decision to measure wave-like or particle-like behaviour can be postponed until after the system has already entered the interferometer.

More recently, *quantum delayed-choice experiments* have extended Wheeler's original proposal by introducing a quantum control system, thereby allowing the interferometer itself to exist in a coherent superposition of being open and closed [128–133]. When entanglement is used as part of the control, additional subtleties emerge: the order of operations, post-selection, and correlations with external degrees of freedom reshape how complementarity and realism must be understood [134].

Delayed-choice experiments test whether a quantum system "decides" to behave as a wave or a particle only at the end of an interferometric run. When the choice is placed under quantum control, and especially when that control is entangled, the final detector visibility is often taken as a proxy for wave-like behaviour. This chapter revisits that intuition through a contextual realism measure that depends on both the observable under consideration (wave or particle)

and the state at the moment it is probed. Building on earlier work, we analyze how changes in causal order affect the interpretation of quantum behaviour. Although the detection statistics remain the same as in standard delayed-choice setups, the degree of realism attributed to wave or particle observables varies with physical context: whether one post-selects, traces out, or measures the ancillary system. This perspective deepens the notion of complementarity: rather than being captured solely by detector visibility, it manifests differently across contexts, as argued in [72]. The chapter proceeds by presenting a sequence of entanglement-assisted interferometric scenarios. As a warm up, we begin with the canonical delayed-choice experiment, then analyze variations with reversed causal order, discarded information, and post-selection. In each case, we quantify wave and particle realism using an entropy-based measure and highlight how complementarity is enforced across contexts.

5.1 Setups and minimal notations

We consider three qubits $\mathcal{A}$ (the interferometric system), $\mathcal{B}$ and $\mathcal{C}$ (the entangled control). System $\mathcal{A}$ is initialized in the state $|\psi\rangle_{\mathcal{A}} = |0\rangle$. Systems $\mathcal{B}$ and $\mathcal{C}$ form an entangled pair of the form:

$$|\psi\rangle_{\mathcal{BC}} = \sqrt{\eta}\,|00\rangle + \sqrt{1-\eta}\,|11\rangle\,, \tag{5.1}$$

where $\eta \in [0,1]$ controls the degree of entanglement. A Hadamard H on $\mathcal{A}$ puts it in a superposition of both paths and a phase shifter adds a relative phase θ. A controlled-Hadamard from $\mathcal{B}$ to $\mathcal{A}$ toggles "open/closed" MZI, and a rotation $R_y(\alpha) = e^{-i\alpha\sigma_y}$ with $0 \leq \alpha \leq \pi$ acts on $\mathcal{C}$. We analyze the following contexts:

1. the standard entanglement-assisted delayed-choice (EADC) [134],
2. the controlled-reality version with swapped order and no postselection,
3. same but discarding $\mathcal{C}$,
4. same with postselection on $\mathcal{C}$,
5. the $\mathcal{C}$-realist context (non-selective measurement on $\mathcal{C}$).

Throughout the chapter, "particle" means the observable $P \equiv \sigma_z$ with eigenstates $\mathcal{P} = \{|0\rangle, |1\rangle\}$ and "wave" means $W \equiv \sigma_\perp$ with eigenstates

$$|\mathcal{W}_\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\theta}\,|1\rangle), \tag{5.2}$$

so that "particle-like" means definite path, and "wave-like" means definite phase superposition. A contextual realism quantifier for an observable $\mathcal{A}$ on $d_{\mathcal{A}}$-level system is given by the equations (2.30) and (2.31). For qubits, $d_{\mathcal{A}} = 2$. This measure is operational (perform the non-read measurement and compare entropies) and contextual (depends on both ρ and which $\mathcal{A}$ we choose). It underlies all statements below.

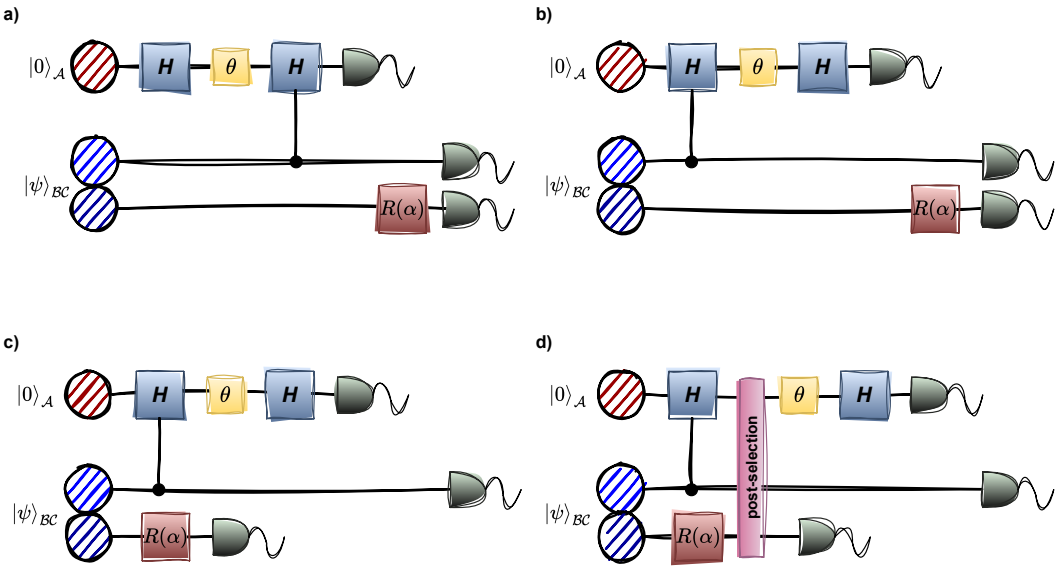

Figure 5.1: **Different physical contexts and their associated wave and particle realism for the system traveling the interferometer.** In all setups, system $\mathcal{A}$ starts in a definite state $|0\rangle$ while the pair $\mathcal{BC}$ starts in an EPR-pair parametrized by the parameter η. a) *Entanglement-assisted delayed-choice setup.* The wave and particle $\mathcal{A}$-realism are evaluated before the interaction with the H-controlled operation between $\mathcal{AB}$ and the $\mathcal{C}$-rotation. b) *Entanglement-assisted controlled-reality arrangement without post-selection.* The wave and particle $\mathcal{A}$-realism are evaluated after the H-controlled operation between $\mathcal{AB}$ and the $\mathcal{C}$-rotation, and before the last $\mathcal{A}$-Hadamard and final detectors. c) *Entanglement-assisted controlled-reality arrangement with $\mathcal{C}$-nonselective measurements.* The wave and particle $\mathcal{A}$-realism are evaluated as in b) except that we anticipate the $\mathcal{C}$-measurements. d) *Entanglement-assisted controlled-reality arrangement with $\mathcal{C}$-postselection.* The wave and particle $\mathcal{A}$-realism are evaluated as in c) but now we consider a postselection to purify the bipartite state $\mathcal{AB}$.

5.2 Entanglement-assisted delayed-choice experiment

Output state. After the operations (Hadamard/phase on $\mathcal{A}$, controlled-H from $\mathcal{B}$ to $\mathcal{A}$, and $R_y(\alpha)$ on $\mathcal{C}$), the output state (before detection) can be written compactly as

$$
\begin{aligned}
|\psi_f\rangle = &\left(\sqrt{\eta}\cos\alpha\,|\mathcal{W}_+\rangle_{\mathcal{A}}\,|0\rangle_{\mathcal{B}} + \sqrt{1-\eta}\sin\alpha\,|w\rangle_{\mathcal{A}}\,|1\rangle_{\mathcal{B}}\right)\otimes|0\rangle_{\mathcal{C}} \\
&- \left(\sqrt{\eta}\sin\alpha\,|\mathcal{W}_+\rangle_{\mathcal{A}}\,|0\rangle_{\mathcal{B}} - \sqrt{1-\eta}\cos\alpha\,|w\rangle_{\mathcal{A}}\,|1\rangle_{\mathcal{B}}\right)\otimes|1\rangle_{\mathcal{C}}\,,
\end{aligned}
\tag{5.3}
$$

where $|w\rangle_{\mathcal{A}} = H\,|W_+\rangle$ is the state after "closed MZI".

Detector probability and visibility (no postselection). The probability of D_0 clicking (i.e., projecting $\mathcal{A}$ onto $|0\rangle$ without postselection on $\mathcal{C}$) is the diagonal matrix element of

$\rho_{\psi_f} = |\psi_f\rangle\langle\psi_f|$:

$$p_{\mathcal{A}_0} = \mathrm{Tr}[(|0\rangle\langle 0| \otimes \mathbb{1}_{\mathbb{BC}})\rho_{\psi_f} = \frac{1}{2}\left(1 + (1-\eta)\cos\theta\right), \tag{5.4}$$

Maximizing and minimizing over θ gives

$$p_{max} = \frac{1}{2}(1 + |1-\eta|) = 1 - \frac{\eta}{2} \tag{5.5}$$

and

$$p_{min} = \frac{1}{2}(1 - |1-\eta|) = \frac{\eta}{2}, \tag{5.6}$$

hence the interferometric visibility

$$\mathcal{V}_{\mathcal{A}}(\eta) := \frac{(p^{\max}_{\mathcal{A}_0} - p^{\min}_{\mathcal{A}_0})}{(p^{\max}_{\mathcal{A}_0} + p^{\min}_{\mathcal{A}_0})} = 1 - \eta, \tag{5.7}$$

So $\eta = 0$ produces full interference (closed MZI), while $\eta = 1$ kills it (open MZI).

Postselecting $\mathcal{C}$. Projecting $\mathcal{C}$ onto $|0\rangle$ and normalizing yields the conditional $\mathcal{A}$-probability:

$$R_{\mathcal{A}_0|\mathcal{C}_0} = \frac{1}{2}\eta\cos^2\alpha + (1-\eta)\sin^2\alpha\cos^2\left(\frac{\theta}{2}\right), \tag{5.8}$$

with the subensemble visibility

$$\mathcal{V}_{\mathcal{A}|\mathcal{C}_0}(\eta,\alpha) = \frac{(1-\eta)\sin^2\alpha}{\eta\cos^2\alpha + (1-\eta)\sin^2\alpha}. \tag{5.9}$$

Analogously, the other branch corresponding to $|1\rangle_{\mathcal{C}}$ gives

$$\mathcal{V}_{\mathcal{A}|\mathcal{C}_1}(\eta,\alpha) = \frac{(1-\eta)\cos^2\alpha}{\eta\sin^2\alpha + (1-\eta)\cos^2\alpha}. \tag{5.10}$$

Note the "dual" behaviour: increasing $\mathcal{V}_{\mathcal{A}|\mathcal{C}_0}$ decreases $\mathcal{V}_{\mathcal{A}|\mathcal{C}_1}$, and both reduce to $1-\eta$ at $\alpha = \pi/4$. Even though the postselected visibilities change with the parameter α, the quantum state of system $\mathcal{A}$ inside the interferometer stays the same. This means that any claim about wave- or particle-like behaviour based only on the final visibility is really a retroinference from the measurement outcomes, not a description of what the system was during its evolution. By contrast, if one uses a realism quantifier, defined in relation to the system's state at a specific time and the observable being measured, the result agrees with the findings reported in [72] for the quantum delayed-choice experiment.

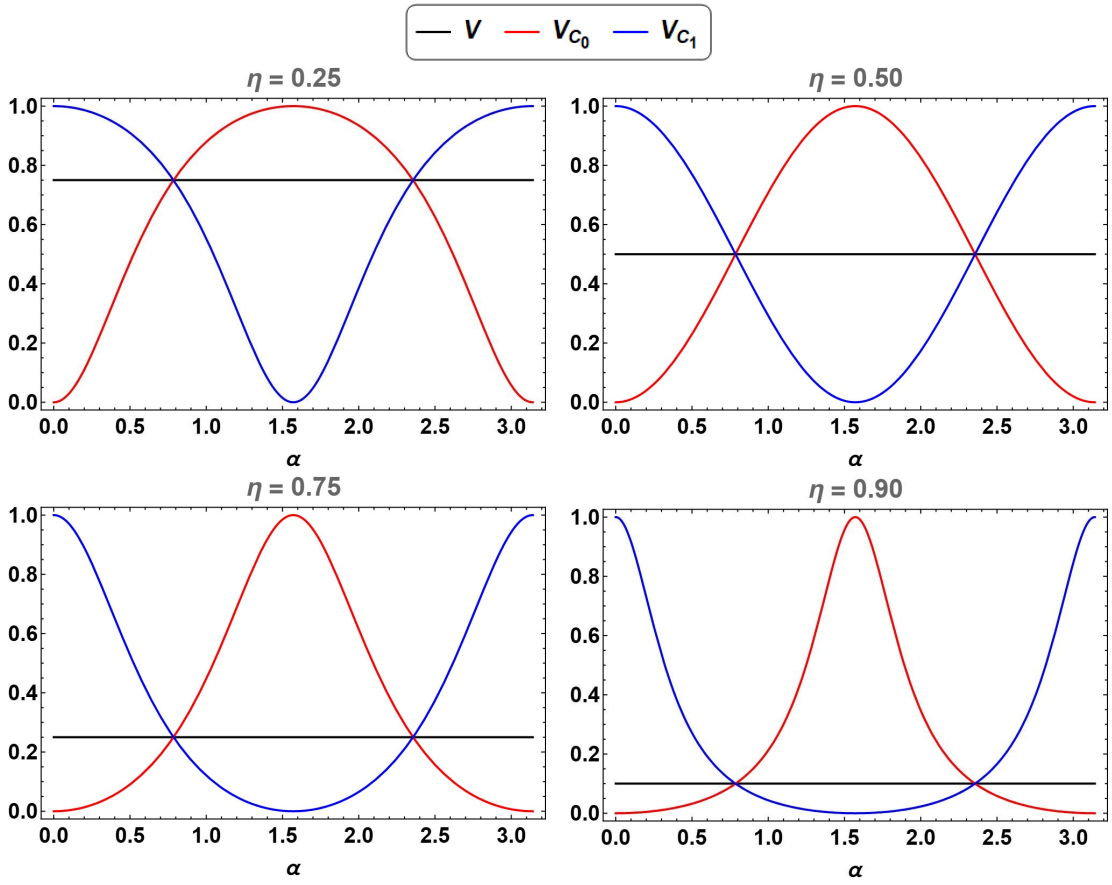

Figure 5.2: **Comparison of the interferometric visibility $\mathcal{V}_{\mathcal{A}}$ across three scenarios:** (i) without postselection (black line), (ii) with postselection on the outcome $\mathcal{C}_0$ (red curve), and (iii) with postselection on the outcome $\mathcal{C}_1$ (blue curve). The curves are shown as functions of the interferometric parameter α for fixed values of the entanglement parameter $\eta \in \{0.25, 0.5, 0.75, 0.9\}$. In the absence of postselection, the visibility remains fixed at $1 - \eta$, whereas in the postselected cases the subensemble visibilities vary with α, highlighting the complementary behaviour of the two branches.

Realism *inside* the interferometer. If one evaluates realism not at the detectors but *during* the interferometer traversal, the contextual measure reports

$$R_P\left(|\mathcal{W}_\pm\rangle\langle\mathcal{W}_\pm|\right) = 0, \tag{5.11}$$

and

$$R_W\left(|\mathcal{W}_\pm\rangle\langle\mathcal{W}_\pm|\right) = 1, \tag{5.12}$$

i.e., the "so-called particle-like" branch is perfectly wave-real in this framework [72]. This already warns us against reading "visibility at the end" as "reality along the way." A strong physical argument supporting this perspective is given in Ref. [135], where it is demonstrated that the state $|\mathcal{W}_\pm\rangle$ carries a well-defined and observable relative phase in the particle basis $|\mathcal{P}_\pm\rangle$ and can even serve as a resource for entangling systems at different locations. This result questions the assumption that low visibility automatically corresponds to particle-like behaviour inside the interferometer.

Building on this idea, a modification of the causal structure in the delayed-choice setup was proposed: the order of the quantum-controlled operations is rearranged to more faithfully capture hybrid wave–particle features through the contextual realism measure. Following this rationale, we consider what we call the *entanglement-assisted quantum-controlled reality experiment*, in which variations in causal order and postselection on subsystem $\mathcal{C}$ generate distinct physical contexts. As we demonstrate, performing measurements or conditioning on $\mathcal{C}$ reveals a complementarity between wave and particle realism that cannot be inferred from the detection statistics alone.

5.3 Entanglement-assisted reality experiment without post-selection

Here we consider a modified delayed-choice setup in which the order of operations is rearranged. Instead of inserting the controlled-Hadamard only after the first Hadamard and phase gates on system $\mathcal{A}$, we perform all operations, including the quantum-controlled one, before the final measurement. By restructuring the sequence in this way, we can evaluate wave- and particle-like realism at an intermediate stage of the system's dynamics, without invoking retrocausal explanations.

State. Starting from the same initial three-qubit state in (5.1), and applying the $\mathcal{AB}$-controlled-Hadamard, then $R_y(\alpha)$ on $\mathcal{C}$, then the phase-shifter on $\mathcal{A}$, we get the "mid-circuit" state:

$$\begin{aligned} |\phi_m\rangle = &\left(\sqrt{\eta}\cos\alpha\,|0\rangle_\mathcal{A}|0\rangle_\mathcal{B} + \sqrt{1-\eta}\sin\alpha\,|W_+\rangle_\mathcal{A}|1\rangle_\mathcal{B}\right)\otimes|0\rangle_\mathcal{C} \\ &- \left(\sqrt{\eta}\sin\alpha\,|0\rangle_\mathcal{A}|0\rangle_\mathcal{B} - \sqrt{1-\eta}\cos\alpha\,|W_+\rangle_\mathcal{A}|1\rangle_\mathcal{B}\right)\otimes|1\rangle_\mathcal{C}, \end{aligned} \tag{5.13}$$

A final Hadamard on $\mathcal{A}$ gives $|\phi_f\rangle$:

$$
\begin{aligned}
|\phi_f\rangle = &\left(\sqrt{\eta}\cos\alpha\,|+\rangle_{\mathcal{A}}\,|0\rangle_{\mathcal{B}} + \sqrt{1-\eta}\sin\alpha\,|w\rangle_{\mathcal{A}}\,|1\rangle_{\mathcal{B}}\right)\otimes|0\rangle_{\mathcal{C}} \\
&-\left(\sqrt{\eta}\sin\alpha\,|+\rangle_{\mathcal{A}}\,|0\rangle_{\mathcal{B}} - \sqrt{1-\eta}\cos\alpha\,|w\rangle_{\mathcal{A}}\,|1\rangle_{\mathcal{B}}\right)\otimes|1\rangle_{\mathcal{C}}\,,
\end{aligned}
\tag{5.14}
$$

Visibility. The detection probability $p_{\mathcal{A}_0}$ and visibility remains *unchanged*:

$$
p_{\mathcal{A}_0} = \frac{1}{2}\left(1 + (1-\eta)\cos\theta\right), \tag{5.15}
$$

and

$$
\mathcal{V}_{\mathcal{A}}(\eta) = 1 - \eta \tag{5.16}
$$

All detector-level conclusions from section 5.2 carry over.

A *different* realism inside the interferometer. Even though the output statistics look the same as in the original delayed-choice setup discussed in Section 5.2, what happens inside the interferometer is not identical. The wave- and particle-like traits of qubit $\mathcal{A}$ evolve differently here because the quantum-controlled operation takes place in a different causal order. The wave and particle realism are

$$
R_P(\phi_m)_{\mathcal{ABC}} = 1 - h\left(\tfrac{\mathcal{V}_{\mathcal{A}}}{2}\right), \tag{5.17}
$$

and

$$
R_W(\phi_m)_{\mathcal{ABC}} = 1 - h\left(\tfrac{1-\mathcal{V}_{\mathcal{A}}}{2}\right), \tag{5.18}
$$

where $h(u) := -u\log_2 u - (1-u)\log_2(1-u)$ is the binary entropy function. These results show that wave realism R_W grows steadily as visibility increases, while particle realism R_P diminishes. At the extremes, full particle realism is obtained when $\eta = 1$, which corresponds to an open interferometer with no interference, whereas full wave realism appears when $\eta = 0$, meaning the interferometer is closed and interference is maximal. An important point is that these realism values do not depend on the rotation angle α. This indicates that the interpolation between particle-like and wave-like behaviour is dictated by the initial entanglement between qubits $\mathcal{B}$ and $\mathcal{C}$, rather than by later local operations. For intermediate values of η, the system falls into a hybrid regime, displaying both wave and particle realism at the same time. Note that the two cannot both be maximal: the general realism complementarity bound for maximally incompatible observables,

$$
R_W(\phi_m)_{\mathcal{ABC}} + R_P(\phi_m)_{\mathcal{ABC}} \leq 1 - E_{\mathcal{A}:\mathcal{BC}}, \tag{5.19}
$$

where $E_{\mathcal{A}:\mathcal{BC}} = h\left(\frac{1+\lambda_{\mathcal{V}_{\mathcal{A}}}}{2}\right)$ stands for the entropy of entanglement between system $\mathcal{A}$ and the control pair $\mathcal{BC}$ with $\lambda_{\mathcal{V}_{\mathcal{A}}} \equiv \sqrt{2\mathcal{V}_{\mathcal{A}}{}^2 - 2\mathcal{V}_{\mathcal{A}} + 1}$. This cleanly links "hybrid" wave-particle

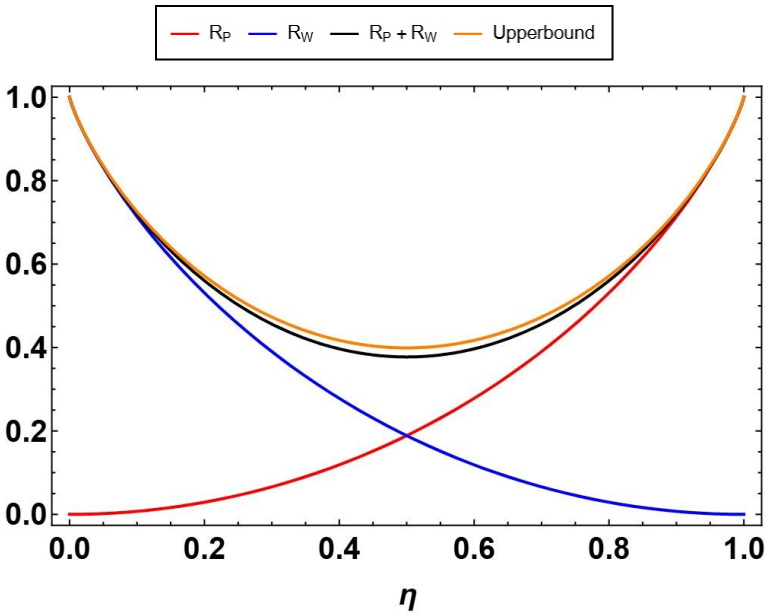

Figure 5.3: **Wave and particle realism in the entanglement-assisted delayed-choice experiment without postselection.** The figure shows (i) particle realism R_P (red), (ii) wave realism R_W (blue), (iii) their combined value $R_P + R_W$ (black), and (iv) the upper bound $1 - E_{\mathcal{A}:\mathcal{BC}}$ (yellow), all plotted as functions of the entanglement parameter η. The results illustrate the smooth trade-off between wave and particle realism as the entanglement between $\mathcal{B}$ and $\mathcal{C}$ increases, and demonstrate that their complementarity is constrained by the global entanglement shared between system $\mathcal{A}$ and its environment.

behaviour to how the initial $\mathcal{BC}$ entanglement is distributed across the $\mathcal{A} : \mathcal{BC}$ bipartition in this causal ordering. Figure 5.3 depicts the behaviour of wave- and particle-realism together with the inequality 5.19. As the parameter η increases, visibility decreases according to $\mathcal{V}_{\mathcal{A}}(\eta) = 1 - \eta$, leading to a gradual reduction in wave realism and a corresponding growth in particle realism. This illustrates a smooth trade-off between the two, with their combined value always bounded above by $1 - E_{\mathcal{A}:\mathcal{BC}}$. The result confirms the complementarity principle and highlights the role of entanglement in restricting the simultaneous expression of both forms of realism.

Up to this point, our results indicate that the degree of initial entanglement shared between the control qubits dictates whether system $\mathcal{A}$ displays predominantly wave-like, particle-like, or mixed realism. This assessment is carried out at the level of the intermediate pure state, which still retains the full global information. Having clarified how interferometric visibility connects to realism without postselection, and recalling the complementary visibilities observed in postselected subensembles of the entanglement-assisted delayed-choice experiment (see Ref. [134]), we are naturally led to ask: how do wave and particle realism manifest inside the interferometer when postselection is introduced before the final Hadamard, i.e., during the evolution of system $\mathcal{A}$ itself? In the next subsection, we address this by calculating realism

measures for each postselected subensemble. Our findings reveal that wave and particle realism in this case remain directly tied to the visibilities of the respective subensembles and, strikingly, they display a complementary dual pattern mirroring that of the visibilities.

5.4 Entanglement-assisted reality experiment with discarded subsystem $\mathcal{C}$

We now examine what happens if information carried by the ancillary qubit $\mathcal{C}$ is completely disregarded. Physically, this corresponds to ignoring outcomes of any operations on $\mathcal{C}$, or equivalently, tracing it out of the joint state. The visibility at the detectors should remain unchanged, but the internal realism trade-off may simplify, since correlations with $\mathcal{C}$ are erased.

State after discarding $\mathcal{C}$. From the mid-circuit state $|\phi_m\rangle$ (5.13), the reduced state on subsystems $\mathcal{A}$ and $\mathcal{B}$ is obtained by partial trace:

$$\rho_{\mathcal{AB}} = \mathrm{Tr}_{\mathcal{C}}[|\phi_m\rangle\langle\phi_m|]\,. \tag{5.20}$$

Carrying out the trace explicitly yields

$$\begin{aligned}\rho_{\mathcal{AB}} = (1-\mathcal{V})|00\rangle\langle 00| + \frac{\mathcal{V}}{2}\Big(&|01\rangle\langle 01| + |11\rangle\langle 11| \\ &+ e^{-i\theta/2}|01\rangle\langle 11| + e^{i\theta/2}|11\rangle\langle 01|\Big),\end{aligned} \tag{5.21}$$

where $\mathcal{V} \equiv \mathcal{V}_{\mathcal{A}}(\eta) = 1-\eta$. This state has a block structure: a classical contribution $|00\rangle\langle 00|$ plus a two-dimensional subspace spanned by $\{|01\rangle, |11\rangle\}$. Its concurrence vanishes, showing that no entanglement remains between $\mathcal{A}$ and $\mathcal{B}$.

Visibility. Since discarding $\mathcal{C}$ involves only a partial trace, and the visibility is determined by local interference on $\mathcal{A}$, the visibility remains

$$\mathcal{V}_{\mathcal{A}}(\eta) = 1-\eta. \tag{5.22}$$

Wave and particle realism. Applying a non-selective measurement in the wave basis of $\mathcal{A}$ gives

$$\begin{aligned}\Phi_W(\rho_{\mathcal{AB}}) = (1-\mathcal{V})&(|00\rangle\langle 00| + |10\rangle\langle 10|) \\ &+ \frac{\mathcal{V}}{2}\Big(|01\rangle\langle 01| + |11\rangle\langle 11| \\ &\quad + e^{-i\theta/2}|01\rangle\langle 11| + e^{i\theta/2}|11\rangle\langle 01|\Big).\end{aligned} \tag{5.23}$$

From this we obtain

$$R_W(\rho)_{\mathcal{AB}} = \mathcal{V}. \tag{5.24}$$

Likewise, dephasing in the particle basis yields

$$\Phi_P(\rho_{\mathcal{AB}}) = (1-\mathcal{V})|00\rangle\langle 00| + \frac{\mathcal{V}}{2}(|01\rangle\langle 01| + |11\rangle\langle 11|), \tag{5.25}$$

leading to

$$R_P(\rho)_{\mathcal{AB}} = 1 - \mathcal{V}. \tag{5.26}$$

Thus,

$$R_W(\rho)_{\mathcal{AB}} + R_P(\rho)_{\mathcal{AB}} = 1, \tag{5.27}$$

for all η.

Even after discarding subsystem $\mathcal{C}$, the same detector-level visibility survives. However, the realism trade-off simplifies dramatically: wave and particle realism now share a linear relation, as shown in Fig. 5.4. In this sense, discarding ancillary information collapses the subtle interplay of entanglement and context down to a clean wave–particle complementarity.

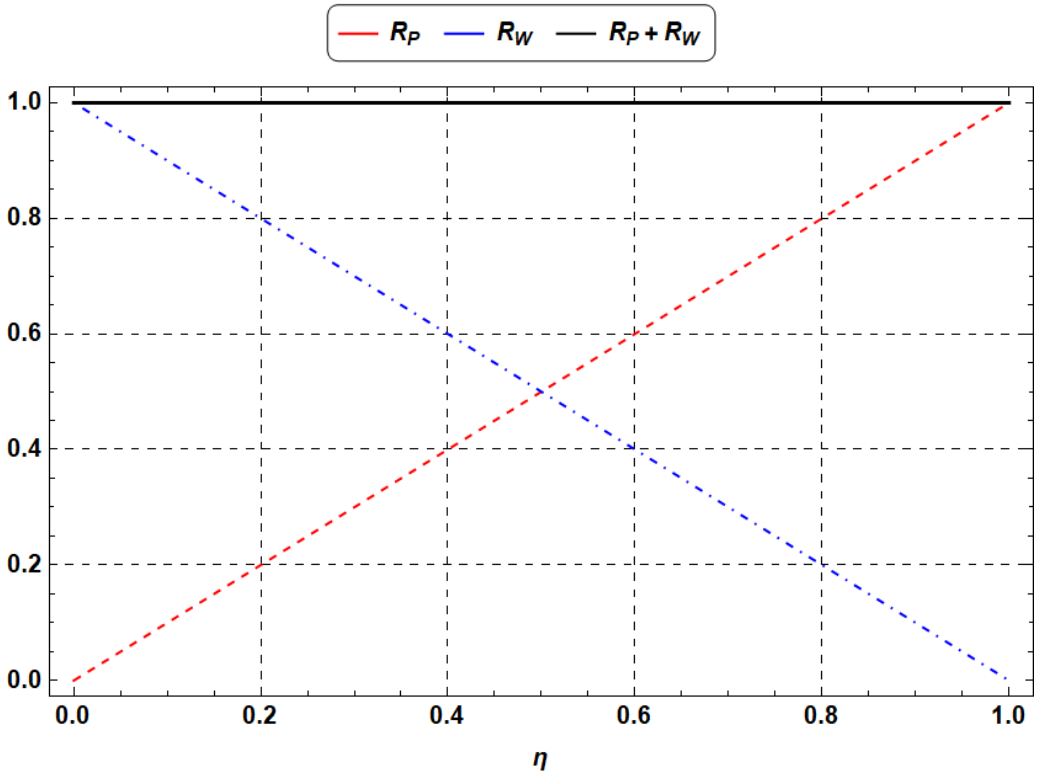

Figure 5.4: **Wave realism R_W and particle realism R_P plotted against the visibility $V_{\mathcal{A}}(\eta)$ after tracing out (discarding) subsystem $\mathcal{C}$.** The relation $R_W + R_P = 1$ is satisfied for all values of η.

5.5 Entanglement-assisted reality experiment with $\mathcal{C}$-postselection

We now turn to the case where subsystem $\mathcal{C}$ is measured before the final detection of system $\mathcal{A}$. In this setting, the causal structure is altered: a projective measurement is carried out on qubit $\mathcal{C}$ in the computational basis, and only the subensemble associated with a chosen outcome is retained. This allows us to study how postselection modifies the balance between wave and particle realism inside the interferometer, rather than inferring it only from the final measurement outcomes.

State after postselection. From Eq. (5.13), if the measurement outcome corresponds to

$$\mathcal{C}_0 = |0\rangle\langle 0|\,, \tag{5.28}$$

the probability of obtaining this result is

$$p_{\mathcal{C}_0} = \frac{1}{2}\left(1 + (2\eta - 1)\cos(2\alpha)\right). \tag{5.29}$$

After renormalization, the resulting state is

$$|\phi_m\rangle_{\mathcal{AB}|\mathcal{C}_0} = \sqrt{\eta}\cos\alpha\,|0\rangle_{\mathcal{A}}\,|0\rangle_{\mathcal{B}} + \sqrt{1-\eta}\sin\alpha\,|W_+\rangle_{\mathcal{A}}\,|1\rangle_{\mathcal{B}}\,. \tag{5.30}$$

The postselected ensemble is now entangled, and this entanglement has a direct impact on the observed complementarity. To illustrate this, consider the action of the final Hadamard gate on system $\mathcal{A}$, which produces the output state

$$|\phi_f\rangle_{\mathcal{AB}|\mathcal{C}_0} = \sqrt{\eta}\cos\alpha\,|+\rangle_{\mathcal{A}}\,|0\rangle_{\mathcal{B}} + \sqrt{1-\eta}\sin\alpha\,|w\rangle_{\mathcal{A}}\,|1\rangle_{\mathcal{B}}\,. \tag{5.31}$$

Visibility. This expression leads to the same subensemble visibility encountered in the entanglement-assisted delayed-choice experiment with postselection, since the conditional probability of detecting outcome $\mathcal{A}_0$ given $\mathcal{C}_0$ is

$$p_{\mathcal{A}_0|\mathcal{C}_0} = \frac{1}{2}\eta\cos^2\alpha + (1-\eta)\sin^2\alpha\cos^2\left(\frac{\theta}{2}\right), \tag{5.32}$$

with the corresponding visibility

$$\mathcal{V}_{\mathcal{A}|\mathcal{C}_0}(\eta,\alpha) = \frac{(1-\eta)\sin^2\alpha}{\eta\cos^2\alpha + (1-\eta)\sin^2\alpha}. \tag{5.33}$$

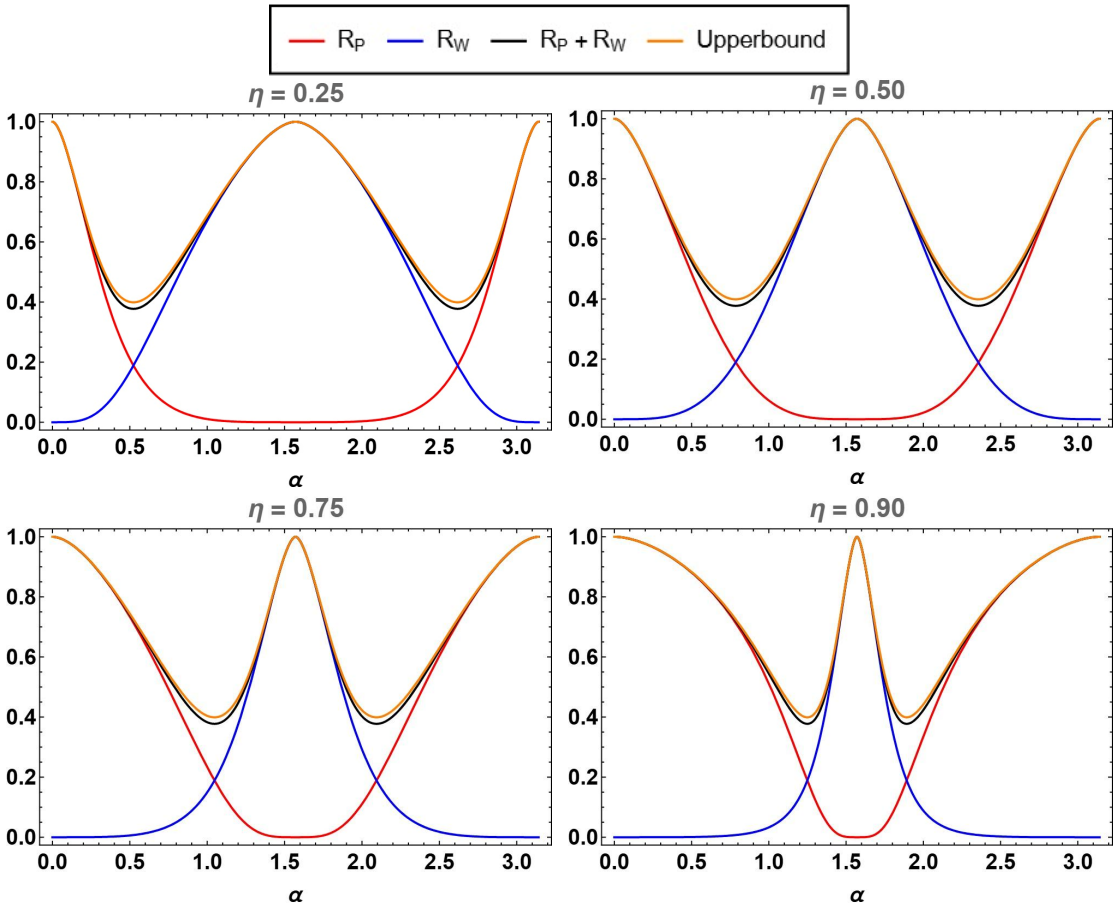

Figure 5.5: **Wave and particle realism for the post-selected sub-ensemble conditioned on outcome $\mathcal{C}_0$ in the entanglement-assisted delayed-choice experiment.** Each panel displays (i) particle realism R_P (red), (ii) wave realism R_W (blue), (iii) their combined value $R_P + R_W$ (black), and (iv) the upper bound $1 - E_{\mathcal{A}:\mathcal{B}}$ (yellow), plotted as functions of the rotation angle α. Results are shown for different values of the initial entanglement parameter $\eta \in \{0.25, 0.5, 0.75, 0.9\}$.

Realism inside the interferometer. As before, final detection probabilities do not distinguish between the different causal orders. The difference emerges when we examine realism inside the interferometer. For the postselected ensemble, wave realism is given by

$$R_W(\phi_m)_{\mathcal{ABC}_0} = 1 - h\left(\tfrac{1-\mathcal{V}_{\mathcal{A}|\mathcal{C}_0}}{2}\right), \tag{5.34}$$

which increases with visibility, while particle realism is

$$R_P(\phi_m)_{\mathcal{ABC}_0} = 1 - h\left(\tfrac{\mathcal{V}_{\mathcal{A}|\mathcal{C}_0}}{2}\right), \tag{5.35}$$

which decreases correspondingly. These measures obey the realism–entanglement complementarity relation

$$R_W(\phi_m)_{\mathcal{AB}|\mathcal{C}_0} + R_P(\phi_m)_{\mathcal{AB}|\mathcal{C}_0} \leq 1 - E_{\mathcal{A}:\mathcal{B}}, \tag{5.36}$$

where $E_{\mathcal{A}:\mathcal{B}}$ is the entanglement entropy between $\mathcal{A}$ and $\mathcal{B}$ under this postselection,

$$E_{\mathcal{A}:\mathcal{B}} = h\left(\frac{1+\lambda_{\mathcal{V}_{\mathcal{A}|\mathcal{C}_0}}}{2}\right), \lambda_{\mathcal{V}_{\mathcal{A}|\mathcal{C}_0}} \equiv \sqrt{2\mathcal{V}^2_{\mathcal{A}|\mathcal{C}_0} - 2\mathcal{V}_{\mathcal{A}|\mathcal{C}_0} + 1}\,. \tag{5.37}$$

The corresponding behaviours of R_W, R_P, and their bound are shown in Fig. 5.5.

A similar analysis can be carried out for the alternative postselection

$$\mathcal{C}_1 = |1\rangle\langle 1|\,. \tag{5.38}$$

In this case, the realism measures read

$$R_W(\phi_m)_{\mathcal{ABC}_1} = 1 - h\left(\tfrac{1-\mathcal{V}_{\mathcal{A}|\mathcal{C}_1}}{2}\right), \tag{5.39}$$

and

$$R_P(\phi_m)_{\mathcal{ABC}_1} = 1 - h\left(\tfrac{\mathcal{V}_{\mathcal{A}|\mathcal{C}_1}}{2}\right), \tag{5.40}$$

with the results summarized in Fig. 5.6.

Thus, postselection preserves the monotonic dependence of wave and particle realism on the subensemble visibility, ensuring that a complementarity relation holds in each branch. The dual behaviour previously seen in the subensemble visibilities is also mirrored in the realism measures. In particular, when the initial entanglement between $\mathcal{B}$ and $\mathcal{C}$ is maximal ($\eta = 1/2$), postselection produces a symmetric inversion between wave and particle realism across the two branches. These findings highlight that quantum realism is context-dependent, shaped jointly by entanglement, the available information, and the choice of postselection.

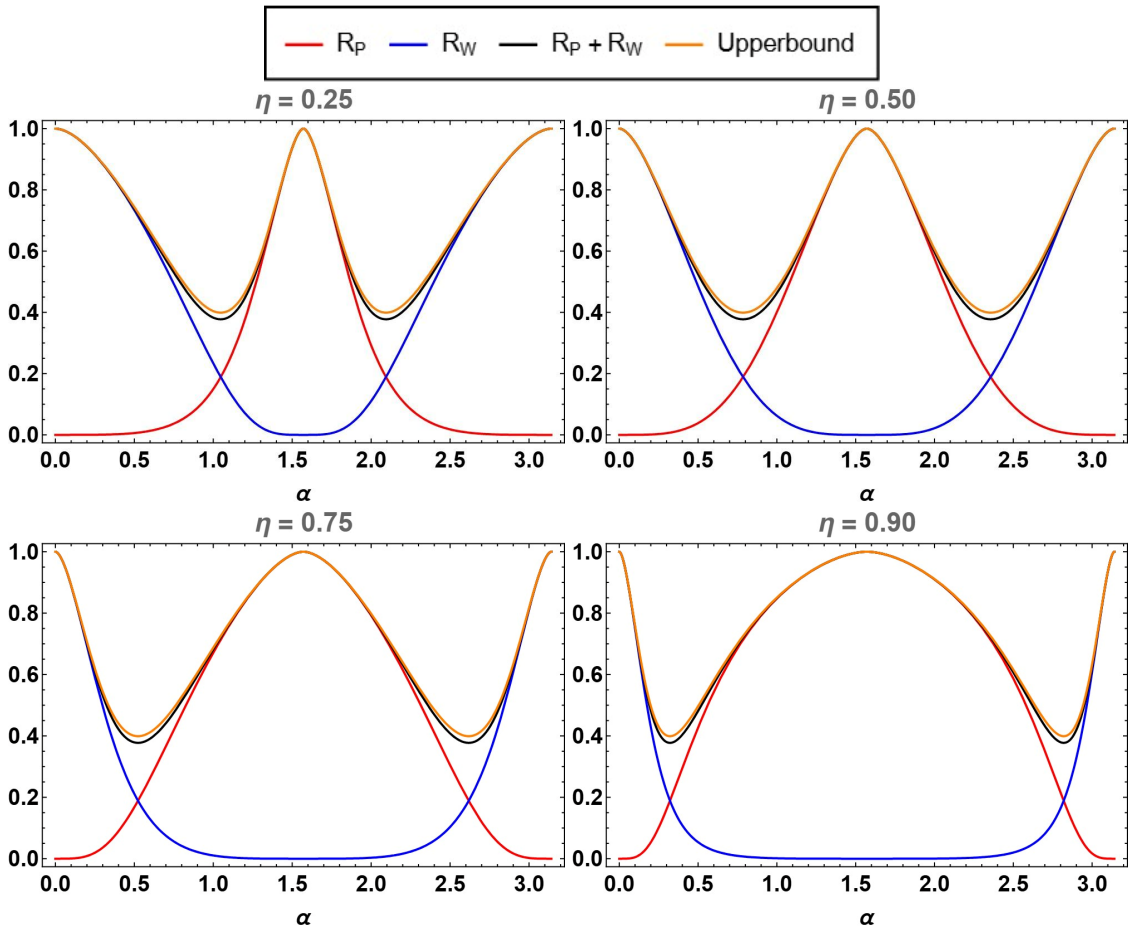

Figure 5.6: **Wave and particle realism for the post-selected sub-ensemble conditioned on outcome $\mathcal{C}_1$ in the entanglement-assisted delayed-choice experiment.** The plots present (i) particle realism R_P (red), (ii) wave realism R_W (blue), (iii) their sum $R_P + R_W$ (black), and (iv) the entropic upper bound $1 - E_{\mathcal{A}:\mathcal{B}}$ (yellow), each shown as a function of the interferometer rotation angle α. Results are displayed for four values of the initial entanglement parameter $\eta \in \{0.25, 0.5, 0.75, 0.9\}$.

5.6 Entanglement-Assisted reality experiment with $\mathcal{C}$-non-selective measurements

In this scenario, we perform a non-selective measurement on subsystem $\mathcal{C}$ in the computational basis. That is, we establish "realism" for $\mathcal{C}$ without recording which outcome occurred. This differs from discarding $\mathcal{C}$: here, an actual local measurement is performed, and the system becomes a mixture over the two possible outcomes. While the final visibility for $\mathcal{A}$ remains unchanged, the contextual realism of $\mathcal{A}$ may change, because the act of enforcing realism on $\mathcal{C}$ introduces nonlocal effects.

State after non-selective measurement on $\mathcal{C}$. Starting again from $|\phi_m\rangle$ in (5.13), the post-measurement state is

$$\Phi_{\mathcal{C}}(\rho_m) = |\phi_{m_0}\rangle\langle\phi_{m_0}| \otimes |0\rangle\langle 0| + |\phi_{m_1}\rangle\langle\phi_{m_1}| \otimes |1\rangle\langle 1|, \tag{5.41}$$

with

$$|\phi_{m_0}\rangle = \sqrt{\eta}\cos\alpha\,|0\rangle_{\mathcal{A}}|0\rangle_{\mathcal{B}} + \sqrt{1-\eta}\sin\alpha\,|W^+\rangle_{\mathcal{A}}|1\rangle_{\mathcal{B}}, \tag{5.42}$$

$$|\phi_{m_1}\rangle = \sqrt{\eta}\sin\alpha\,|0\rangle_{\mathcal{A}}|0\rangle_{\mathcal{B}} - \sqrt{1-\eta}\cos\alpha\,|W^+\rangle_{\mathcal{A}}|1\rangle_{\mathcal{B}}. \tag{5.43}$$

This is a classical mixture with weights

$$p_{\mathcal{C}_0} = \tfrac{1}{2}\left(1 + (2\eta - 1)\cos 2\alpha\right), \quad p_{\mathcal{C}_1} = 1 - p_{\mathcal{C}_0}. \tag{5.44}$$

Visibility. Local probabilities of $\mathcal{A}$ are unaffected by non-selective measurements on $\mathcal{C}$. Therefore, the detector-level visibility remains

$$\mathcal{V}_{\mathcal{A}}(\eta) = 1 - \eta, \tag{5.45}$$

independent of α.

Wave and particle realism. The realism quantifier is computed by dephasing each branch in the relevant basis and averaging entropies:

$$R_{\mathcal{A}}(\Phi_{\mathcal{C}}(\rho_m)) = 1 - \left[p_{\mathcal{C}_0}\, h(q_{\mathcal{A}}^{(0)}) + p_{\mathcal{C}_1}\, h(q_{\mathcal{A}}^{(1)})\right], \tag{5.46}$$

where $h(u) = -u\log_2 u - (1-u)\log_2(1-u)$.

Particle realism:

$$q_P^{(0)} = \frac{\eta\cos^2\alpha + \frac{1}{2}(1-\eta)\sin^2\alpha}{\eta\cos^2\alpha + (1-\eta)\sin^2\alpha}, \tag{5.47}$$

$$q_P^{(1)} = \frac{\eta\sin^2\alpha + \frac{1}{2}(1-\eta)\cos^2\alpha}{\eta\sin^2\alpha + (1-\eta)\cos^2\alpha}. \tag{5.48}$$

Thus,

$$R_P(\Phi_{\mathcal{C}}(\rho_m)) = 1 - \left[p_{\mathcal{C}_0}\, h(q_P^{(0)}) + p_{\mathcal{C}_1}\, h(q_P^{(1)})\right]. \tag{5.49}$$

Wave realism:

$$q_W^{(0)} = \frac{\frac{1}{2}\eta\cos^2\alpha + (1-\eta)\sin^2\alpha}{\eta\cos^2\alpha + (1-\eta)\sin^2\alpha}, \tag{5.50}$$

$$q_W^{(1)} = \frac{\frac{1}{2}\eta\sin^2\alpha + (1-\eta)\cos^2\alpha}{\eta\sin^2\alpha + (1-\eta)\cos^2\alpha}. \tag{5.51}$$

Hence,

$$R_W(\Phi_{\mathcal{C}}(\rho_m)) = 1 - \left[p_{\mathcal{C}_0}\, h(q_W^{(0)}) + p_{\mathcal{C}_1}\, h(q_W^{(1)})\right]. \tag{5.52}$$

Here the striking result (as depicted in Fig. 5.7) is that, while visibility is fixed solely by η,

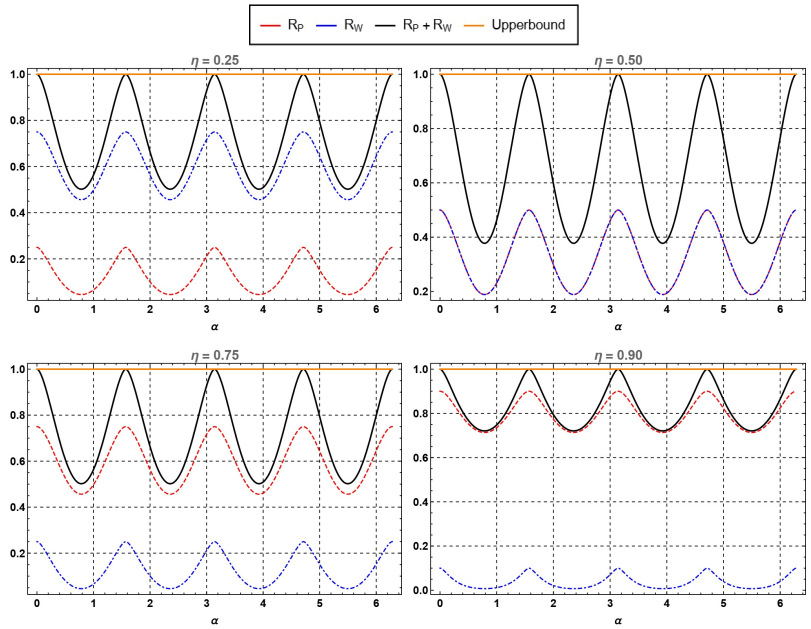

Figure 5.7: **Wave realism R_W and particle realism R_P for subsystem $\mathcal{A}$ when realism is established with respect to subsystem $\mathcal{C}$.** Their dependence on the rotation angle α reveals a nonlocal effect that does not manifest at the level of detector visibility.

the contextual realism of $\mathcal{A}$ oscillates with the rotation angle α. This is a clear manifestation of realism-based nonlocality: by establishing realism on the remote system $\mathcal{C}$, the degree of realism for $\mathcal{A}$'s wave or particle observable is altered, even though local detection statistics on $\mathcal{A}$ remain unaffected.

5.7 Summary

In this chapter, we have revisited the question of wave-particle duality in the context of entanglement-assisted delayed-choice and controlled-reality experiments. By employing a contextual quantifier of realism, we moved beyond the traditional reliance on detector-level visibility as the sole indicator of wave-like or particle-like behaviour. This approach allowed us to analyze not only the final statistics, but also the state of the system as it propagates through the interferometer, and to explore how realism depends on the broader physical context.

We began by revisiting the standard entanglement-assisted delayed-choice arrangement, confirming that the final visibility interpolates between particle-like and wave-like regimes as the entanglement parameter η varies. However, the realism analysis revealed that the state usually interpreted as "particle-like" actually possesses full wave realism inside the interferometer, highlighting the limitations of retro-inference from output statistics alone.

Next, by reversing the causal order of operations, we showed that while the final visibility remains identical, the internal trade-off between wave and particle realism is now monotonic and directly linked to the distribution of entanglement between system $\mathcal{A}$ and the $\mathcal{BC}$ pair. This demonstrated that complementarity is not merely a property of measurement outcomes, but also of how correlations are structured within the experimental sequence.

We then studied scenarios where subsystem $\mathcal{C}$ is either discarded or explicitly postselected. When $\mathcal{C}$ is traced out, wave and particle realism obey a simple linear complementarity relation $R_W + R_P = 1$, with no entanglement left between $\mathcal{A}$ and $\mathcal{B}$. By contrast, postselection on $\mathcal{C}$ restores entanglement between $\mathcal{A}$ and $\mathcal{B}$, and realism becomes bounded by the entanglement entropy of the conditional state. The dual behaviour of the two subensembles confirmed the central role of physical context in shaping the manifestation of wave-particle duality.

Finally, we considered the case where realism is explicitly established on $\mathcal{C}$ through a non-selective measurement. Here, the visibility of $\mathcal{A}$ remains fixed by η, but the contextual realism of $\mathcal{A}$ oscillates as a function of the local rotation angle α applied to $\mathcal{C}$. This constitutes a clear instance of realism-based nonlocality: local operations on $\mathcal{C}$ that establish its realism have nontrivial consequences for the degree of realism attributed to $\mathcal{A}$, despite leaving local statistics unchanged.

Taken together, these results emphasize that complementarity in quantum mechanics must be understood not only in terms of visibility, but in terms of the full physical context that includes causal order, subsystem correlations, and postselection as demonstrated in [72]. Entanglement-assisted delayed-choice experiments thus provide a powerful platform to probe the boundary between operational statistics and contextual realism, enriching our understanding of how wave and particle aspects coexist and compete in quantum systems.

Chapter 6

Conclusion and Outlook

Quantum mechanics has long fascinated both physicists and philosophers with its counterintuitive phenomena, some of them being entanglement, superposition, and wave-particle duality. While these phenomena often appear as abstract curiosities, this thesis has taken a different approach, demonstrating that fundamental quantum principles can be harnessed as practical tools for information processing. Across three distinct but interconnected lines of inquiry, we have explored how information-theoretic and operational frameworks reveal the deep utility of quantum mechanics in both foundational studies and applied protocols.

In the first part of this thesis, we examined the principle of information causality ($\mathcal{IC}$). Originally formulated to provide an intuitive bound on nonlocal correlations, $\mathcal{IC}$ has far-reaching implications for device-independent quantum key distribution (DIQKD). By generalizing it to a multipartite setting, we showed that it implies a strong monogamy of nonlocal correlations, which in turn guarantees the security of QKD against individual attacks even from post-quantum adversaries. Notably, the bipartite formulation of $\mathcal{IC}$ was insufficient for security, highlighting the necessity of a broader framework. This work demonstrates that abstract information-theoretic principles can serve as operational tools for certifying privacy in realistic quantum protocols, connecting foundational concepts with practical applications.

The second thread of this thesis focused on semi-device-independent (SDI) security derived from wave-particle duality (WPD). By linking the min- and max-entropic uncertainty relations with complementary interferometric quantities, visibility and input distinguishability, we established SDI security in an operationally meaningful manner. The use of a tunable beam splitter (TBS) enabled a direct exploration of the balance between particle-like and wave-like behaviours, leading to improved bounds on the SDI security condition. Importantly, these results show that complementarity is not just a philosophical statement but a quantifiable resource, capable of certifying non-classicality and ensuring secure communication directly from

measurable interference patterns.

The final line of investigation concerned realism, context, and causal structures, explored through entanglement-assisted delayed-choice experiments. By modifying the causal order and introducing post-selection, we showed that wave-particle realism can be meaningfully assigned at intermediate stages within an interferometric setup. This analysis extends the operational understanding of quantum complementarity and demonstrates the sensitivity of quantum correlations to the informational and causal structure of experiments. It emphasizes that quantum mechanics provides a rich landscape in which the context of operations, including timing, entanglement, and measurement choices, plays a central role in the manifestation of observable phenomena.

Taken together, these three threads support a unifying perspective: quantum mechanics offers a toolbox of information processing tasks, where features such as nonlocality, complementarity, and contextuality are not merely theoretical curiosities but operational resources. By framing quantum phenomena in terms of tasks, whether certifying security, quantifying wave-particle trade-offs, or probing causal structures, we gain both conceptual as well as practical advantages, linking abstract foundations to implementable protocols.

Looking forward, this toolbox perspective opens multiple exciting avenues. Extending information-theoretic principles such as $\mathcal{IC}$ and monogamy to fully DI protocols could further strengthen quantum cryptography in realistic, noisy settings. Exploring higher-dimensional and continuous-variable systems in SDI frameworks may reveal richer trade-offs between complementarity and security. Finally, understanding how causal structures influence quantum information processing could pave the way for novel protocols that exploit the temporal ordering and control of quantum operations, potentially in networked or distributed quantum systems.

In conclusion, the title *Information Processing Tasks as a Toolbox for Quantum Information* aptly captures the essence of this thesis: quantum mechanics is not only a theory of what is possible in the physical world but also a framework for encoding, certifying, and controlling information. By translating fundamental quantum phenomena into concrete information-processing tasks, we show how quantum mechanics serves as a practical toolbox: one that connects abstract questions about the nature of reality with secure communication and emerging technologies.

Bibliography

[1] L. Pollyceno, A. Chaturvedi, C. Raj, P. R. Dieguez, and M. Pawłowski, Phys. Rev. A , (2025).

[2] C. Raj and P. R. Dieguez, Open Systems & Information Dynamics **32**, 2550009 (2025).

[3] C. Raj, T. Prasad, A. Chaturvedi, L. Pollyceno, D. Spegel-Lexne, S. Gómez, J. Argillander, A. Alarcón, G. B. Xavier, M. Pawłowski, *et al.*, arXiv preprint arXiv:2507.00679 (2025).

[4] G. S. Vernam, Journal of the AIEE **45**, 109 (1926).

[5] C. E. Shannon and W. Weaver, Urbana, IL: University of Illinois Press **11**, 11 (1949).

[6] R. L. Rivest, A. Shamir, and L. Adleman, Communications of the ACM **21**, 120 (1978).

[7] W. Diffie and M. E. Hellman, in *Democratizing cryptography: the work of Whitfield Diffie and Martin Hellman* (2022) pp. 365–390.

[8] P. W. Shor, SIAM review **41**, 303 (1999).

[9] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[10] J. v. Neumann, (1955).

[11] C. H. Bennett and G. Brassard, Theoretical computer science **560**, 7 (2014).

[12] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[13] C. Elliott, Proceedings of SPIE **5815**, 138 (2005).

[14] M. Peev, C. Pacher, R. Alléaume, and et al., New Journal of Physics **11**, 075001 (2009).

[15] M. Sasaki, M. Fujiwara, H. Ishizuka, and et al., Optics Express **19**, 10387 (2011).

[16] S.-K. Liao, W.-Q. Cai, J. Handsteiner, and et al., Nature **549**, 43 (2017).

[17] J. Yin, Y.-H. Li, S.-K. Liao, and et al., Nature **582**, 501 (2020).

[18] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[19] N. Bohr, Phys. Rev. **48**, 696 (1935).

[20] J. S. Bell, Physics Physique Fizika **1**, 195 (1964).

[21] A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **49**, 91 (1982).

[22] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. Vermeulen, R. N. Schouten, C. Abellán, *et al.*, Nature **526**, 682 (2015).

[23] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, Phys. Rev. Lett. **115**, 250402 (2015).

[24] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, Phys. Rev. Lett. **115**, 250401 (2015).

[25] A. Acín *et al.*, Phys. Rev. Lett. **98**, 230501 (2007).

[26] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).

[27] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L.-M. Luo, T. A. Manning, and C. Monroe, New Journal of Physics **11**, 045021 (2009).

[28] A. Acín and L. Masanes, Nature **540**, 213 (2016).

[29] U. Vazirani and T. Vidick, Communications of the ACM **62**, 133 (2019).

[30] M. Pawłowski and N. Brunner, Physical Review A—Atomic, Molecular, and Optical Physics **84**, 010302 (2011).

[31] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Physical Review A—Atomic, Molecular, and Optical Physics **85**, 052308 (2012).

[32] Y.-C. Liang, T. Vértesi, and N. Brunner, Physical Review A—Atomic, Molecular, and Optical Physics **83**, 022108 (2011).

[33] B.-G. Englert, Phys. Rev. Lett. **77**, 2154 (1996).

[34] V. Jacques, E. Wu, F. Grosshans, F. Treussart, P. Grangier, A. Aspect, and J.-F. Roch, Physical review letters **100**, 220402 (2008).

[35] X.-s. Ma, J. Kofler, and A. Zeilinger, Reviews of Modern Physics **88**, 015005 (2016).

[36] M. O. Scully and K. Drühl, Physical Review A **25**, 2208 (1982).

[37] Y.-H. Kim, R. Yu, S. P. Kulik, Y. Shih, and M. O. Scully, Physical Review Letters **84**, 1 (2000).

[38] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).

[39] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nature Physics **6**, 659 (2010).

[40] P. J. Coles, J. Kaniewski, and S. Wehner, Nature communications **5**, 5814 (2014).

[41] P. J. Coles, Phys. Rev. A **93**, 062111 (2016).

[42] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Reviews of Modern Physics **89**, 015002 (2017).

[43] S. Kochen and E. P. Specker, J. Math. Mech. **17**, 59 (1967).

[44] A. L. O. Bilobran and R. M. Angelo, Europhys. Lett. **112**, 40005 (2015).

[45] P. R. Dieguez and R. M. Angelo, Phys. Rev. A **97**, 022107 (2018).

[46] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, Nature **461**, 1101 (2009).

[47] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).

[48] B. Toner and F. Verstraete, Monogamy of bell correlations and tsirelson's bound (2006), arXiv:quant-ph/0611001 [quant-ph] .

[49] M. Pawłowski, Phys. Rev. A **82**, 032313 (2010).

[50] F. Pollyceno, A. B. Sainz, E. Wolfe, and R. Chaves, arXiv preprint arXiv:2302.07301 (2023).

[51] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[52] J. A. Wheeler, in *Mathematical Foundations of Quantum Theory*, edited by A. R. Marlow (Academic Press, New Orleans, LA, 1978) pp. 9–48.

[53] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. (Cambridge University Press, 2010).

[54] J. Watrous, Cambridge University Press (2018).

[55] K. Kraus, Annals of Physics **64**, 311 (1971).

[56] I. L. Chuang and M. A. Nielsen, Journal of Modern Optics **44**, 2455 (1997).

[57] A. Uhlmann, Reports on Mathematical Physics **9**, 273 (1976).

[58] R. Jozsa, Journal of Modern Optics **41**, 2315 (1994).

[59] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).

[60] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[61] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[62] M. B. Plenio and S. Virmani, Quant. Inf. Comput. **7**, 1 (2007).

[63] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).

[64] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[65] J. S. Bell, Physics Physique Fizika **1**, 195 (1964).

[66] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).

[67] B. Tsirelson, Letters in Mathematical Physics **4**, 93 (1980).

[68] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).

[69] R. Rabelo, R. Gallego, and N. Brunner, Phys. Rev. Lett. **107**, 210403 (2011).

[70] A. J. Leggett, Found. Phys. **33**, 1469 (2003).

[71] G. Chiribella, H. Yang, and N. Brunner, npj Quantum Information **5**, 1 (2019).

[72] P. R. Dieguez, J. R. Guimarães, J. P. Peterson, R. M. Angelo, and R. M. Serra, Commun. Phys. **5**, 82 (2022).

[73] H. Ollivier and W. H. Zurek, Phys. Rev. Lett. **88**, 017901 (2001).

[74] L. Henderson and V. Vedral, J. Phys. A **34**, 6899 (2001).

[75] L. C. Céleri, J. Maziero, and R. M. Serra, Int. J. Quantum Inf. **9**, 1837 (2011).

[76] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, Reviews of Modern Physics **84**, 1655 (2012).

[77] L. Masanes, A. Acín, and N. Gisin, Phys. Rev. A **73**, 012112 (2006).

[78] W. van Dam, arXiv preprint arXiv:quant-ph/0501159 (2013).

[79] M. Seevinck, Quantum Inf. Process. **9**, 273 (2010).

[80] J.-D. Bancal, D. Cavalcanti, V. Scarani, and S. Pironio, Phys. Rev. A **88**, 014102 (2013).

[81] M. Pawłowski, Phys. Rev. A **82**, 032313 (2010).

[82] W.-Y. Hwang and O. Gittsovich, Phys. Rev. A **85**, 046301 (2012).

[83] M. Pawłowski, Phys. Rev. A **85**, 046302 (2012).

[84] M. Pawłowski and i. c. v. Brukner, Phys. Rev. Lett. **102**, 030403 (2009).

[85] N. Miklin and M. Pawlowski, Phys. Rev. A **100**, 022326 (2019).

[86] L. Pollyceno, R. Chaves, and R. Rabelo, Physical Review A **107**, 042203 (2023).

[87] M. Tomamichel and R. Renner, Physical review letters **106**, 110506 (2011).

[88] Y. Yuan, Z. Hou, Y.-Y. Zhao, H.-S. Zhong, G.-Y. Xiang, C.-F. Li, and G.-C. Guo, Optics express **26**, 4470 (2018).

[89] Y. L. Len, J. Dai, B.-G. Englert, and L. A. Krivitsky, Physical Review A **98**, 022110 (2018).

[90] D. Spegel-Lexne, S. Gómez, J. Argillander, M. Pawłowski, P. R. Dieguez, A. Alarcón, and G. B. Xavier, Science Advances **10**, eadr2007 (2024).

[91] D. Mayers and A. Yao, arXiv preprint quant-ph/0307205 (2003).

[92] R. Cleve, P. Hoyer, B. Toner, and J. Watrous, in *Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004.* (IEEE, 2004) pp. 236–249.

[93] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, *et al.*, Nature **464**, 1021 (2010).

[94] A. Acin, S. Massar, and S. Pironio, New Journal of Physics **8**, 126 (2006).

[95] R. Colbeck, arXiv preprint arXiv:0911.3814 (2009).

[96] V. Scarani, N. Gisin, N. Brunner, L. Masanes, S. Pino, and A. Acín, Phys. Rev. A **74**, 042339 (2006).

[97] J. Barrett, A. Kent, and S. Pironio, Physical review letters **97**, 170409 (2006).

[98] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).

[99] A. Chaturvedi, M. Pawlowski, and K. Horodecki, Phys. Rev. A **96**, 022125 (2017).

[100] N. Miklin and M. Pawłowski, Phys. Rev. Lett. **126**, 220403 (2021).

[101] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, Nature **461**, 1101 (2009).

[102] S. Popescu and D. Rohrlich, Foundations of Physics **24**, 379 (1994).

[103] W. van Dam, Implausible consequences of superstrong nonlocality (2005), arXiv:quant-ph/0501159 [quant-ph] .

[104] R. Chaves, C. Majenz, and D. Gross, Nature Communications **6**, 10.1038/ncomms6766 (2015).

[105] L. Pollyceno, R. Chaves, and R. Rabelo, Phys. Rev. A **107**, 042203 (2023).

[106] S. Pironio, J.-D. Bancal, and V. Scarani, Journal of Physics A: Mathematical and Theoretical **44**, 065303 (2011).

[107] L. Pollyceno, Code concerning the figure 3.3 (2022).

[108] L. Masanes, A. Acin, and N. Gisin, Phys. Rev. A **73**, 012112 (2006).

[109] T. H. Yang, D. Cavalcanti, M. L. Almeida, C. Teo, and V. Scarani, New Journal of Physics **14**, 013061 (2012).

[110] R. Gallego, L. E. Würflinger, A. Acín, and M. Navascués, Phys. Rev. Lett. **107**, 210403 (2011).

[111] Y. Xiang and W. Ren, Quantum Info. Comput. **11**, 948–956 (2011).

[112] L.-Y. Hsu, Phys. Rev. A **85**, 032115 (2012).

[113] E. Adlam, Tsirelson's bound and the quantum monogamy bound from global determinism (2021), arXiv:2011.08284v1 [quant-ph] .

[114] E. Adlam, Tsirelson's bound and the quantum monogamy bound from global determinism (2021), arXiv:2011.08284v2 [quant-ph] .

[115] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[116] A. Acín, S. Massar, and S. Pironio, New Journal of Physics **8**, 126 (2006).

[117] N. Bohr, Nature **121**, 580 (1928).

[118] M. Ardehali, Physics Letters A **217**, 301 (1996).

[119] M. Pawłowski and A. Winter, Phys. Rev. A **85** (2012).

[120] R. Konig, R. Renner, and C. Schaffner, IEEE Transactions on Information theory **55**, 4337 (2009).

[121] N. Bohr, Phys. Rev. **48**, 696 (1935).

[122] J. A. Wheeler and W. H. Zurek, *Quantum theory and measurement*, Vol. 15 (Princeton University Press, 2014).

[123] V. Jacques, E. Wu, F. Grosshans, F. Treussart, P. Grangier, A. Aspect, and J.-F. Roch, Science **315**, 966 (2007).

[124] A. G. Manning, R. I. Khakimov, R. G. Dall, and A. G. Truscott, Nat. Phys. **11**, 539 (2015).

[125] F. Vedovato, C. Agnesi, M. Schiavon, D. Dequal, L. Calderaro, M. Tomasin, D. G. Marangon, A. Stanco, V. Luceri, G. Bianco, *et al.*, Sci. Adv. **3**, e1701180 (2017).

[126] T. Jennewein, Č. Brukner, M. Aspelmeyer, and A. Zeilinger, International Journal of Quantum Information **3**, 73 (2005).

[127] X.-s. Ma, S. Zotter, J. Kofler, R. Ursin, T. Jennewein, Č. Brukner, and A. Zeilinger, Nature Physics **8**, 479 (2012).

[128] R. Ionicioiu and D. R. Terno, Phys. Rev. Lett. **107**, 230406 (2011).

[129] R. Auccaise, R. M. Serra, J. G. Filgueiras, R. S. Sarthour, I. S. Oliveira, and L. C. Céleri, Phys. Rev. A **85**, 032121 (2012).

[130] S. S. Roy, A. Shukla, and T. S. Mahesh, Phys. Rev. A **85**, 022109 (2012).

[131] A. Peruzzo, P. Shadbolt, N. Brunner, S. Popescu, and J. L. O'Brien, Science **338**, 634 (2012).

[132] F. Kaiser, T. Coudreau, P. Milman, D. B. Ostrowsky, and S. Tanzilli, Science **338**, 637 (2012).

[133] G. Adesso and D. Girolami, Nat. Photonics **6**, 579 (2012).

[134] R. Ionicioiu, T. Jennewein, R. B. Mann, and D. R. Terno, Nat. Comm. **5**, 4997 (2014).

[135] R. M. Angelo and A. D. Ribeiro, Found. Phys. **45**, 1407 (2015).