Quantum measurements: Studies of weak measurements describing the past of quantum particles, no-go theorem, and quantum key distributions

Rajendra Singh Bhati

A thesis submitted for the partial fulfillment of
the degree of Doctor of Philosophy

Department of Physical Sciences
Indian Institute of Science Education & Research Mohali
Knowledge city, Sector 81, SAS Nagar, Manauli PO, Mohali 140306, Punjab, India

December 2023

Declaration

The work presented in this thesis has been carried out by me under the guidance of Prof. Arvind at the Indian Institute of Science Education and Research (IISER) Mohali.

This work has not been submitted in part or in full for a degree, diploma or a fellowship to any other University or Institute. Whenever contributions of others are involved, every effort has been made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of original work done by me and all sources listed within have been detailed in the bibliography.

Rajendra Singh Bhati

Place :
Date :

In my capacity as supervisor of the candidate's PhD thesis work, I certify that the above statements by the candidate are true to the best of my knowledge.

Prof. Arvind
Professor
Department of Physical Sciences
IISER Mohali

Place :
Date :

Acknowledgements

The doctoral journey could not have been accomplished without the immeasurable and unwavering support and love bestowed upon me by my parents, Mrs. Bhanwar Kanwar Rathore and Mr. Chiman Singh Bhati. I am forever indebted to their relentless struggle and ceaseless efforts to turn my dream into a reality. Additionally, I am profoundly grateful to my brother, Mr. Gajendra Singh Bhati, whose love and affection have been a constant source of inspiration and motivation. Despite being younger than me, he has consistently been a guiding light on this challenging path, and I am truly fortunate to have him by my side.

I would like to extend my utmost gratitude to my thesis supervisor, Prof. Dr. Arvind, whose guidance, mentorship, and immense support have been invaluable throughout my doctoral journey. Their profound expertise, encouragement, and constructive feedback have been instrumental in shaping the direction of this research and refining my academic and research skills. I am deeply appreciative of their efforts in providing me with a scientific environment that fostered freedom of choice and the opportunity to delve into fundamental research problems. Their firm belief in my capabilities has been an incredible source of motivation, and I am truly grateful for their mentorship.

I am deeply thankful to the members of my dissertation committee, Prof. Dr. Kavita Dorai, Dr. Sandeep Kumar Goyal and Dr. Ananth Venkatesan for their insightful comments, expertise, and commitment to reviewing and evaluating my work. I would also like to express my sincere gratitude to Dr. Manbendra Nath Bera for numerous discussions on various aspects and research problems in quantum foundations. His encouragement and feedback are deeply appreciated. Additionally, I am grateful to Dr. Paramdeep Singh for his technical assistance and cheerful coffee chats.

I am also indebted to the faculty members and researchers who have generously shared their expertise in their respective research fields through in-person discussions, seminars, classroom interactions, and conferences. Their insights and scholarly contributions have significantly shaped my understanding of the field. I extend a special thanks to all the undergraduates who engaged in discussions with me on various aspects of quantum foundations during their summer and master's projects with Prof. Arvind. Their naive yet important doubts have had a significant impact on my own comprehension of the field.

Furthermore, I would like to express my sincere gratitude to the administration of IISER Mohali, without their support my journey could not have been easy and smooth. I especially thank offices of Dean Academics and Dean Students for their efforts in making my work place and stay on campus pleasant. I am indebted to office of Dean R&D for all resources, funding, and facilities they have provided. I am grateful to Mr.

Tarun for all his administrative supports.

I have been fortunate to have had wonderful colleagues in my life. I would like to begin by expressing my gratitude to my research collaborator and dear friend, Dr. Jaskaran Singh, for his cheerful company and engaging discussions, both academic and non-academic. Additionally, I extend my gratitude to Dr. Soumyakanti Bose, Dr. Chandan Kumar, Gurvir Singh, Kirtpreet Singh, Sarbani, Jasmeet, Jorawar Singh, Mohak Sharma, Vaishali, Akshay, Krishna, Akanksha, Dr. Jyotsana, Dr. Sumit Mishra, Gayatri Singh, Dr. Dileep Singh, and Dr. Vikash Mittal, who have been like a family to me. Their presence and support have been invaluable, creating a sense of belonging and fostering a collaborative atmosphere. I am truly grateful for their friendship and the camaraderie we have shared.

What is life without friends and a journey without companions! My journey at IISER Mohali began in August 2011 as a BSMS student. It is truly a rarity to have the privilege of having the best college friends as companions throughout the doctoral journey. In this regard, I consider myself incredibly fortunate to have had Akshay Gaikwad and Love Grover as such companions on this path. Their support, camaraderie, and shared experiences have enriched my journey in immeasurable ways. I am also deeply indebted to Sandeep Rawat, Krishna Shende, Mamta Bhandari, and Mandeep Kaur for their friendship and moral support. Their presence has brought immense joy, laughter, and a sense of belonging to this journey.

Furthermore, I would like to express my heartfelt gratitude to my dearest friends Abhishek, Saurabh, Arjit, Raminder, Nakul, and Varun. Their enduring friendship, encouragement, and belief in me have been constant sources of inspiration and strength. No acknowledgement of mine could ever be complete without mentioning Vaishali Vardhan. Her unwavering support and profound motivation have consistently guided me through the most challenging moments of this journey. I am forever grateful for her presence and belief in my abilities.

Abstract

This thesis focuses on both fundamental and applied aspects of quantum measurements, specifically their role in describing the past of quantum particles, the two-state vector formalism, wave-particle complementarity and quantum key distributions.

We investigate the predictions of the two-state vector formalism and weak values, which are recognized as elements of reality in weak measurements. The combination of weak values and the two-state vector formalism is utilized to operationally define the past of quantum particles. The latter results in inception of various quantum paradoxes known as weak value paradoxes. Through a thought experiment, we demonstrate that weak values cannot consistently describe the past of quantum particles. To address this, we develop novel techniques for describing the past of photons in an interferometer. Our findings reveal that photons provide information about the past that is absent in weak measurement scenarios. These predictions can be experimentally validated.

Furthermore, we explore the role of generalized weak values in quantum information processing tasks. Our research demonstrates that the use of weak values can lead to erroneous conclusions, particularly in quantum state discrimination and quantum key distribution. Moreover, our results shed light on various shortcomings associated with weak values and the weak measurement approach.

Subsequently, we develop a quantum key distribution protocol that employs blockwise processing and post-selections. This protocol exhibits high noise tolerance against collective attacks in asymptotic limits. Building upon the existing six-state protocol, we divide the raw keys obtained into blocks of finite length. By performing specific post-selections on these blocks, we generate new raw keys. The unconditional security of this protocol is proven using information-theoretic proofs.

In addition, we establish a no-go theorem that states the impossibility of manipulating or measuring the internal degrees of freedom of a quantum particle without disturbing its spatial wavefunction. This theorem is derived based on the principle of no-faster-than-light communication. We then apply this no-go result to a quantum Darwinian scenario to explain the emergence of objectivity in the position basis. Furthermore, we consider a decoherence model involving randomized spin-spin interactions between a system in spatial superposition and a spin environment with spins

in arbitrary random states. By formulating the interaction Hamiltonian in accordance with our no-go theorem, we demonstrate that it leads to the emergence of classical objectivity in the position basis.

Finally, we propose an experiment to demonstrate wave-particle complementarity using von Neumann interaction between a Gaussian pointer and a pre- and post-selected qubit. Our research reveals that the complementarity between two observables of a qubit can be operationally translated into a wave-particle complementarity relation. Additionally, we establish that for every pre- and post-selected qubit, there exists an operationally equivalent Mach-Zehnder interferometer. These results can be easily extended to higher-dimensional discrete-level systems.

List of Publications

1. **Rajendra Singh Bhati** and Arvind. Do weak values capture the complete truth about the past of a quantum particle? *Phys.Lett.A2022.127955. arXiv:1807.05341.*

2. Jaskaran Singh, **Rajendra Singh Bhati**, and Arvind. No contextual advantage in nonparadoxical scenarios of the two-state vector formalism. *Phys.Rev.A107.012206. arXiv:2206.02673v1*

3. Jaskaran Singh, **Rajendra Singh Bhati**, and Arvind. Revealing quantum contextuality using a single measurement device. *Phys.Rev.A107.012201* .

4. **Rajendra Singh Bhati** and Arvind, Quantum operations restricted by no faster-than-light communication principle and generic emergence of objectivity in position basis. *arXiv:2310.18133.*

5. **Rajendra Singh Bhati** and Arvind. Limitations of using weak-value formalism in quantum information processing tasks with mixed-states. *Manuscript under preparation.*

6. **Rajendra Singh Bhati** and Arvind. High noise tolerant quantum key distribution using block-wise processing and post-selections. *Manuscript under preparation.*

7. **Rajendra Singh Bhati** and Arvind. Proposal for experimental demonstration of wave-particle complementarity using von Neumann measurements. *Manuscript under preparation.*

8. **Rajendra Singh Bhati** and Arvind. Comment on “Photons are lying about where they have been, again". *Manuscript under preparation.*

Contents

Abstract **ix**

List of Figures **xvii**

List of Tables **xxi**

1 Introduction **1**
1.1 Quantum measurements . . . 2
1.1.1 Postulates of quantum theory . . . 3
1.1.2 von Neumann model of quantum measurements . . . 5
1.2 Two state vector formalism . . . 6
1.2.1 Aharonov, Bergmann and Lebowitz retrodiction . . . 8
1.2.2 Weak values . . . 11
1.2.3 Weak values as witness of counterfactual ABL rule . . . 12
1.2.4 Weak measurements followed by post-selections . . . 13
1.2.5 Weak value paradoxes . . . 15
1.2.5.1 Photons with discontinuous trajectories . . . 15
1.2.5.2 Quantum Cheshire cat paradox . . . 17
1.2.5.3 Hardy's paradox . . . 17
1.3 Quantum key distribution . . . 19
1.3.1 Basic components of quantum key distribution protocols . . . 20
1.3.2 Information theoretic security proofs . . . 22
1.4 Organization of the thesis . . . 23

2 Weak values cannot consistently describe the past of quantum particles **25**
2.1 Introduction . . . 25
2.2 Weak value hypothesis and implications . . . 27
2.3 The gedanken experiment . . . 29
2.3.1 Sampling protocol . . . 34

2.3.2 Where was the photon? . . . 35
2.4 TSVF analysis of the gedanken experiment . . . 36
2.4.1 Measurement of weak values . . . 38
2.4.2 Where was the photon according to TSVF? . . . 38
2.5 Conclusions and Discussion . . . 40

3 Weak-value formalism for mixed-states and quantum key distribution 43
3.1 Introduction . . . 43
3.2 Weak value formalism for mixed states . . . 46
3.3 State discrimination using weak values . . . 47
3.4 QKD Protocol using weak values . . . 50
3.5 Security definition . . . 51
3.6 Security analysis with weak measurement approximation . . . 54
3.6.1 Quantum inputs and measurements . . . 54
3.6.2 Joint probability distribution of Alice and Bob . . . 58
3.6.3 Joint probability distribution for depolarizing channels . . . 59
3.6.4 State of Eve's memory and her side information . . . 62
3.6.5 Secure key rate and the noise tolerance . . . 63
3.7 Security analysis without weak measurement approximation . . . 63
3.7.1 Joint probability distribution of Alice and Bob . . . 64
3.7.2 State of Eve's memory and her side information . . . 66
3.7.3 Secure key rate and the noise tolerance . . . 67
3.8 Discussion and conclusions . . . 67

4 High noise-tolerant quantum key distribution using block-wise processing 71
4.1 Introduction . . . 71
4.2 Protocol steps . . . 73
4.3 Mathematical model of the protocol . . . 77
4.3.1 Quantum inputs and the measurements . . . 77
4.3.2 Sifting process . . . 80
4.4 Security analysis . . . 83
4.4.1 Security criteria . . . 83
4.4.2 Joint probability distribution and Eve's quantum memory . . . 84
4.4.3 Secure key fraction and the noise-tolerance . . . 86
4.5 Discussion and conclusion . . . 88

5 A no-go theorem on restricted measurements and implications thereof 89
5.1 Introduction . . . 89
5.2 The no-go theorem and the proof . . . 91

5.3 Implications in quantum Darwinism 96
5.3.1 Decoherence Model 98
5.3.2 Formation of the broadcast structure 100
5.4 Discussion and conclusion 106

6 Demonstration of wave-particle complementarity using von Neumann measurements 109
6.1 Introduction 109
6.2 Revisiting welcher-weg experiments 110
6.3 Interference and wave-particle complementarity using von Neumann interactions 112
6.4 Welcher-weg detections, quantum erasers and Wheeler's delayed-choice experiments 115
6.5 Conclusion 117

7 Summary 119

References 123

List of Figures

1.1 von Neumann interaction between spin and spatial degree of freedom in the presence of magnetic field gradient. The particle is initially in $|\psi\rangle_S \otimes |\xi\rangle_P$ where the spatial part $|\xi\rangle$ acts as a pointer. After passing through a magnetic field gradient in z-direction, the wavepacket splits into two. The detection of the particle on the screen is a strong measurement in the position basis which induces a collapse on the spin. Whether the spin measurement is sharp or not depends on the overlap between the two wavepackets. 7

1.2 A system is pre-selected in $|\psi\rangle$ by discarding outcomes corresponding to $|\tilde{\psi}\rangle$ in measurement $\mathcal{P}_1$. The system is then post-selected in the state $|\phi\rangle$ by discarding outcomes $|\tilde{\phi}\rangle$ in measurement $\mathcal{P}_2$. The spectrum of the intermediate measurement of the observable $\mathcal{A}$ is depicted between pre-and post-selection. 9

1.3 A pre-and post-selected quantum system is fully described by two-sate vectors $\langle\phi(t)||\psi(t)\rangle$. The state $\langle\phi(t)|$ evolves backward while the state $|\psi(t)\rangle$ evolves forward in time. 11

1.4 The system is pre-selected in state $|\psi\rangle$ and a pointer is prepared in $|\xi\rangle$ at time t_1. Interaction U_{int} takes place between the two at time t. The system is then post-selected in state $|\phi\rangle$ at time t_2. This leaves the pointer in state $|\xi'\rangle$. 14

1.5 (a) Nested Mach-Zehnder interferometer. A Mach-Zehnder interferometer is inserted in on of the arms of a larger Mach-Zehnder interferometer. Beam splitters $BS1$ and $BS4$ has $2/3$ reflectivity, while $BS2$ and $BS3$ are $50-50$. PS is a phase shifter, S is a single photon source, and D is the detector. (2) Single photons coming from S are post-selected at D. The corresponding forward and backward evolving wavefunctions are denoted by solid and dashed lines, respectively. . . 16

1.6 Quantum Cheshire cat setup: a photon is pre-selected in $|\psi\rangle = (|A\rangle + i|B\rangle)|H\rangle/\sqrt{2}$ using a single photon source and a $50-50$ beam splitter; and then post-selected in the state $|\phi\rangle = (|A\rangle|V\rangle + |B\rangle|H\rangle)/\sqrt{2}$ using half-wave plate HWP, phase shifter PS, another $50-50$ beam-splitter $BS2$, polarizing beam splitter PBS, and detector D. 18

1.7 Hardy's setup: Simultaneously produced electron and positron passes through two separate matter-wave Mach-Zehnder interferometers. The interferometers have an overlap in the region X where electron and positron annihilate each other if they meet. 19

1.8 A typical quantum key distribution setup has two parties Alice and Bob who want to share a secure key. Alice and Bob are connected by a quantum communication channel that shares a quantum state between them. Additionally, They are connected with an authenticated classical channel (ACC). Alice and Bob can perform measurements on their respective quantum systems or, in general, shared quantum black-boxes using measurements $\mathcal{M}_a$ and $\mathcal{M}_b$, respectively. Their inputs are locally generated and are random. An eavesdropper Eve can have access to both ACC and the quantum channel. 21

2.1 Six-port interferometer with empty dots showing the input ports and filled dots showing the output ports. The dark square boxes are the beam-splitters (BS), the light boxes are the time-dependent L elements and the long dark rectangle are the mirrors. The top left corner shows the input and output ports for L and BS. 32

2.2 The thick (red) and thin (blue) lines represent the forward and backward evolving state vectors of the single photon, pre and post-selected at source S and detector D, respectively. The solid lines represent the non-vanishing and significant probability amplitude, dashed lines represent insignificant (order ϵ) probability amplitudes, and the absence of a line represents amplitudes that are zero or proportional to higher powers of ϵ. $w_1, w_2, \cdots, w_{10}$ denote weak measurement devices of corresponding projection operators. 37

3.1 P_{err} is plotted as a function of α for $\epsilon/\delta^2 = 0.1$ 48

3.2 Secret key fraction according to weak measurement approximation. The secret fraction is plotted as a function of depolarizing noise η for (a) $\alpha = 0.1$ and (b) $\alpha = 0.2$. 61

3.3 Secret key fraction calculated without assuming the weak measurement approximation. The secret fraction is plotted as a function of depolarizing noise η for (a) $\gamma = 0.1$ and (b) $\gamma = 0.2$, note that plots for $\alpha = 20, 25, 30, 35$ are coinciding. 68

4.1 Schematic diagram of the QKD protocol. Alice, Bob, and Eve share the tripartite system Ψ_{ABE}. The strings of systems or alphabets are symbolic. $R^{\alpha}, R^{\beta}, R^{\pi}$ are locally generated random inputs. Classical communications is denoted by C^{i} where i is the suitable superscript. All the functions, transformations, transcripts, and the alphabets strings are explained in Section 4.2. 74

4.2 The secret fraction computed using the Devetak-Winter key rate formula for different block sizes. 87

5.1 Alice and Bob are stationed in two laboratories separated by distance 2α. They share a common quantum particle which is simultaneously present in both laboratories. Alice chooses an operation based on randomly generated bit a and performs it on the internal degree of freedom of the particle. Bob performs a fixed measurement on the internal degree of freedom and registers the outcome as a bit b. 93

5.2 The system is in superposition of positions $\{x_i\}_{i=1,2,\cdots,d}$. Environment spins $\{E_{ij}\}$ are randomly located near positions $\{x_i\}$. E_{ij} is the j-th subenvironment near x_i. Random spin interactions take place between subenvironments and the system. 99

5.3 The system is in superposition of positions $\{x_i\}_{i=1,2,\cdots,d}$. Environment spins $\{E_{ij}\}$ are randomly located near positions $\{x_i\}$. Subenvironments with the same color constituent a fragment F. For example, all subenvironments in red are part of a fragment F_j, in green form F_k and so on. 107

6.1 $P_{\psi}(x)$ (solid line), $P_{\psi'}(x)$ (dashed line), and $P_{\psi}(x) + P_{\psi'}(x)$ (dotted line) are plotted against x for (a) $\gamma = 4, p = q = 0.5, \alpha = \beta = 0$, (b) $\gamma = 4, p = 0.05, q = 0.5, \alpha = \pi/2, \beta = 0$, (c) $\gamma = 4, p = 0.002, q = 0.5, \alpha = \pi, \beta = 0$, (d) $\gamma = 6, p = q = 0.5, \alpha = \beta = 0$, (e) $\gamma = 6, p = 0.05, q = 0.5, \alpha = 0, \beta = \pi/2$, (f) $pq = 0$. 116

List of Tables

4.1 Noise-tolerance for various block sizes. 88

LIST OF TABLES

Chapter 1

Introduction

Quantum theory, without a doubt, stands as one of the most perplexing and astonishing scientific theories ever formulated. It represents a departure from the classical theory that had governed our understanding of the physical world for centuries. Unlike classical physics, which described the behavior of macroscopic objects with deterministic laws, quantum theory deals with the microscopic realm of particles and their interactions. Its emergence in the early 20th century brought forth a radical shift in our perception of reality, challenging our intuition and defying common sense.

One of the striking features of quantum theory is its inherent uncertainty. In the classical world, the properties of objects were thought to be well-defined and measurable. However, quantum theory reveals that at the fundamental level, particles such as electrons and photons exist in a superposition of multiple states simultaneously, a notion that seems bizarre from a classical standpoint. Moreover, when these particles are measured, their behavior becomes probabilistic, with the outcome being described by a wave function that encompasses all possible states. This probabilistic nature of quantum theory poses a profound challenge to our traditional understanding of causality and determinism. Another mind-boggling aspect of quantum theory is entanglement. Two or more particles can become entangled, forming an inseparable connection that persists even when they are separated by vast distances. Remarkably, the state of one particle instantaneously affects the state of the other, defying the constraints of space and time. This phenomenon, famously referred to by Albert Einstein as "spooky action at a distance," bewildered scientists and continues to perplex researchers to this day.

Despite its perplexing nature, quantum theory has proven to be the most successful and accurate scientific theory in history. Its predictions have been confirmed with extraordinary precision through countless experiments, affirming its remarkable reliability. Quantum mechanics underlies our understanding of a vast range of phenomena, from the behavior of subatomic particles to the properties of materials, the functioning

of electronic devices, and even the behavior of the universe at its most fundamental level. Last few decades have witnessed a wave of technological advancements and applications that harness the unique properties of quantum systems. That includes quantum cryptography [1, 2], quantum computation [3], quantum metrology [4, 5], quantum heat engines [6, 7], quantum batteries [8] and many more.

This thesis presents a study of various aspects of quantum measurements, including weak measurements and the interpretation of weak values. We analyze the existing interpretation of weak measurements and weak values through a gedanken experiment. Our findings indicate that weak values are not suitable for investigating the past of quantum systems, effectively resolving the quantum paradoxes commonly referred to as weak value paradoxes or pre-and post-selection paradoxes.

Additionally, we investigate interactions and measurements that adhere to the no-faster-than-light communication principle. Our research reveals that manipulating the internal degrees of freedom of a system inevitably introduces disturbances to its spatial wavefunction. We apply this result to a decoherence model, shedding light on the emergence of classical objectivity in the position basis.

In a subsequent chapter, we propose an experimental demonstration of wave-particle complementarity that does not rely on conventional interferometers. This can be achieved by utilizing von Neumann interactions between a Gaussian pointer and a pre-and post-selected qubit, providing a novel insight into the complementarity principle.

Furthermore, we present a quantum key distribution protocol that employs post-selection techniques to increase the noise tolerance in standard discrete variable protocols. This protocol offers improved security and noise resistance for quantum key distribution.

Overall, this thesis delves into the intricacies of quantum measurements, explores the limitations and implications of weak values, uncovers the impact of no-faster-than-light communication on quantum systems, investigates wave-particle complementarity through innovative experimental setups, and proposes an enhanced quantum key distribution protocol.

This chapter introduces various concepts mentioned above by providing a technical background to the same. In the subsequent sections, we introduce quantum measurements, von Neumann model, two state vector formalism, weak values paradoxes, quantum key distribution, quantum Darwinism and classical objectivity.

1.1 Quantum measurements

Measurements serve as a crucial link between the abstract mathematical framework of a theory and the tangible experimental predictions. However, in the realm of quantum

theory, the physics of measurements diverges significantly from classical mechanics. Unlike classical measurements where the act of extracting information does not perturb the system, in quantum mechanics, measurement disturbs the state of the system being observed. This fundamental distinction implies that the outcomes of quantum measurements are not predetermined, adding a layer of unpredictability to the quantum world.

These intriguing features find their basis in the no-cloning theorem, which plays a pivotal role in establishing the compatibility between quantum theory and the special theory of relativity. The no-cloning theorem states that it is impossible to create an identical copy of an arbitrary unknown quantum state [9]. This theorem has far-reaching implications, particularly in the field of quantum key distribution [10, 11], where secure communication relies on the inability to clone quantum states. By preventing unauthorized copying, the no-cloning theorem enables the establishment of secure communication channels based on the unique properties of quantum systems.

Moreover, the measurement process itself holds significant importance in the quest to understand the quantum-to-classical transition [12, 13, 14]. Quantum mechanics describes the behavior of microscopic particles, while classical mechanics provides a framework for describing the macroscopic world. The measurement process is seen as the bridge between these two realms, where the probabilistic nature of quantum states collapses into a single definite outcome, resembling classical behavior. This transition from quantum superposition to classical certainty is a topic of active research and continues to be an area of fascination and investigation in quantum theory.

In this section, we briefly review the postulates of quantum theory, and von Neumann model of quantum measurements.

1.1.1 Postulates of quantum theory

Every physical theory consists of three main components: the mathematical depiction of physical states and observables, the transformation of states (known as time evolution), and the measurement of physical quantities (which involves extracting information). For example, in Newtonian mechanics, a complete description of a particle involves its position and momentum vectors in physical space. The transformation is governed by Newton's laws of motion or, equivalently, the Hamilton-Jacobi equation. Measurements are straightforward, involving the projection of position and momentum vectors onto a unit vector. However, these measurements do not disturb the systems. In contrast, quantum theory operates within the realm of complex vector spaces and yields non-trivial consequences. In this context, we provide a brief summary of the postulates of quantum theory, outlining the mathematical framework for states, observables, time evolution, and measurements [15, 16].

1. Introduction

> **Postulate 1: (States and observables)** A Hilbert space is associated with every isolated quantum system, where the state of the system is described by a unit vector in it. Physical observables are defined by Hermitian operators acting over the Hilbert space.

Complex numbers are essential ingredients of quantum theory. In fact, it has been shown recently that quantum theory cannot exist without complex numbers [17]. This makes the theory extremely counter intuitive and hard to perceive its ontology. The Hilbert space framework for isolated single systems is extended to composite systems using tensor products:

> **Postulate 2: (Composite systems)** The state space of a composite system is the tensor product of the state spaces of the component systems. If Hilbert spaces $\mathcal{H}_1, \mathcal{H}_2, \cdots, \mathcal{H}_n$ are associated with the component systems, then the Hilbert space associated with the composite system is $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$.

The observables for composite systems are defined as Hermitian operators acting on the tensor product space. It is the *Postulate-2* that makes quantum theory universally applicable to all scales [18] and gives birth to intriguing phenomena like quantum entanglement and nonlocality [19, 20, 21]. Composite systems where the ontology of component systems may not exist, are physically possible in the tensor product space [22]. Quantum computing is the most practical application of the composite system framework of quantum systems [15]. The transformations on a closed system between preparation and measurement are deterministic, linear and unitary operations governed by its Hamiltonian:

> **Postulate 3: (Evolution)** The evolution of the state of a closed quantum system is a unitary transformation. If the state at time t_1 is $|\psi(t_1)\rangle$, then the state at a later time t_2 is given by $|\psi(t_2)\rangle = U(t_2; t_1)\,|\psi(t_1)\rangle$, where the unitary operation $U(t_2; t_1)$ depends on t_1, t_2 and the Hamiltonian $\hat{H}$ of the system. Moreover, the dynamics of the evolution is given by the Schrödinger time evolution equation,
>
> $$i\hbar \frac{d\,|\psi\rangle}{dt} = \hat{H}\,|\psi\rangle\,. \tag{1.1}$$

The transformation unitary is given as $U(t_2; t_1) = \exp\left(-\frac{i}{\hbar}\int_{t_1}^{t_2} \hat{H} dt\right)$. For a closed system, the evolution of state is deterministic. Even for composite systems of arbitrary scale, the state at an arbitrary time can be predicted if the complete Hamiltonian including all the interactions is known. However, action of measurement breaks this evolution by introducing irreversible collapse to the state.

Postulate 4:(Measurements) Measurements on closed quantum systems are described by a set of projection operators $\mathcal{M} \equiv \{\Pi_k : \Pi_k\Pi_k = \Pi_k, \sum_k \Pi_k^\dagger\Pi_k = \mathbb{1}\}$, where the index k refers to the possible outcome. Set $\{\Pi_k\}$ forms the spectrum of an observable. If the state of the system immediately before the measurement is $|\psi\rangle$, then the probability of getting k-th outcome is given by *Born rule* [15]:

$$p(k) = \langle\psi| \Pi_k |\psi\rangle . \tag{1.2}$$

The state immediately after the measurement is given by the *state update rule*:

$$|\psi'\rangle = \frac{\Pi_k |\psi\rangle}{\sqrt{\langle\psi| \Pi_k^\dagger\Pi_k |\psi\rangle}}. \tag{1.3}$$

Note that $\sum_k p(k) = 1$. Measurements described above are known as *projector-valued measures*. PVMs on a composite system may generate transformations on the component systems which are neither unitary nor projective measurements. Description of these transformations is given by generalized measurements called *positive-operator-valued measures (POVM)*: $\mathcal{M}' \equiv \{M_k : M_k \geq 0, \sum_k M_k^\dagger M_k = \mathbb{1}\}$ [15]. Unlike PVMs, POVMs can be nonorthogonal to each others *i.e.* $M_i M_j \neq 0$ for some $i \neq j$.

Since all the interactions among the constituent systems of composite systems can be modeled by the Schrödinger equation with specification of the Hamiltonian operator of the composite system, it appears that the measurement postulate runs into conflict with the time evolution postulate of the quantum mechanics. This problem is known as quantum measurement problem [14]. It has also been discussed in the literature by the names of Schrödinger's cat [12] and Wigner's friend paradoxes [23].

1.1.2 von Neumann model of quantum measurements

The first mathematical description and model of quantum measurements was presented by John von Neumann [24], known as the von Neumann measurement scheme (vNMS). In vNMS, a (microscopic) quantum system S interacts with a pointer P in such a way that they become maximally entangled in the basis of an observable of S being measured. For instance, consider S in state $|\psi\rangle$ and the pointer in $|\xi\rangle$. The von Neumann interaction corresponding to measurement of observable $\hat{A} \equiv \sum_i a_i |a_i\rangle\langle a_i|$ transforms the composite state $|\psi\rangle \otimes |\xi\rangle$ as

$$|\psi\rangle \otimes |\xi\rangle \xrightarrow{\text{von Neumann interaction}} \sum_i \alpha_i |a_i\rangle \otimes |\xi_i\rangle , \tag{1.4}$$

where, $\{|\xi_i\rangle\}$ is a set of orthogonal states in the Hilbert space associated to P. von Neumann interaction can be realized using interaction Hamiltonian of the form $\hat{H} = g(t)\hat{A} \otimes \hat{p}$. The time function $g(t)$ determines the strength of the measurement. von Neumann proposed that when the size of the pointer is sufficiently large (as a classical object), the pointer collapses to one of the states $\{|\xi_i\rangle\}$ with probabilities $\{\|\alpha_i\|^2\}$, respectively, given by the Born rule. The entire process then becomes equivalent to realization of PVMs $\{|a_i\rangle\langle a_i|\}$. Such measurements are also known by names projective measurements, strong measurements and sharp measurements in the literature.

Relaxing the orthogonality condition for states $\{|\xi_i\rangle\}$ gives rise to unsharp von Neumann measurements [25],

$$|\psi\rangle \otimes |\xi\rangle \xrightarrow{\text{un-sharp von Neumann interaction}} \sum_i \alpha_i |a_i\rangle \otimes |\xi_i'\rangle\,, \tag{1.5}$$

where $\{|\xi_i'\rangle\}$ does not form a set of orthogonal basis. The state after interaction can be re-arranged in such a way that $\sum_i \alpha_i |a_i\rangle \otimes |\xi_i'\rangle = \sum_i \alpha_i' |a_i'\rangle \otimes |\xi_i\rangle$ where $\{|a_i'\rangle\}$ are non-orthogonal states. As the pointer collapses to distinguishable classical configurations described by the set $\{|\xi_i\rangle\}$, the system S collapses to non-orthogonal states $\{|a_i'\rangle\}$. von Neumann interactions extremely weak interaction strength give rise to weak measurements where state of the system remains nearly undisturbed after the localization of the pointer state [26]. Notably, weak measurements are special cases of unsharp measurements.

The interaction between spin and spatial degree of freedom of a silver atom in the Stern–Gerlach (SG) experiment is the suitable example of von Neumann interaction (see Fig. 1.1). The spatial degree of freedom acts as a pointer in SG. The interaction is given by Hamiltonian $H_{int} = \hat{\mu} \cdot \overrightarrow{B}$, where $\hat{\mu}$ and $\overrightarrow{B}$ are spin and magnetic field, respectively. Assuming that the x and y components of the magnetic field are negligible, while the z component is linear in z *i.e.* $B_z \approx B_0 z$, we have simpler expression for the interaction Hamiltonian $H_{int} = -\mu_0 B_0 \sigma_z \otimes \hat{z}$. The constant $\gamma = \mu_0 B_0$ determines the interaction strength. The composite state after the interaction is an entangled state between the wavefunction and the spin. When the atom is detected on the screen, the collapse of pointer in position basis induces collapse in the spin state. The outcomes can be sharply or weakly distinguishable depending on the interaction strength and the time particle spends in the magnetic field gradient.

1.2 Two state vector formalism

The two-state vector formalism (TSVF) extends the standard framework of quantum mechanics by incorporating the future evolution of quantum systems. In this formalism, a quantum system is represented by a ket vector in a Hilbert space, just like in

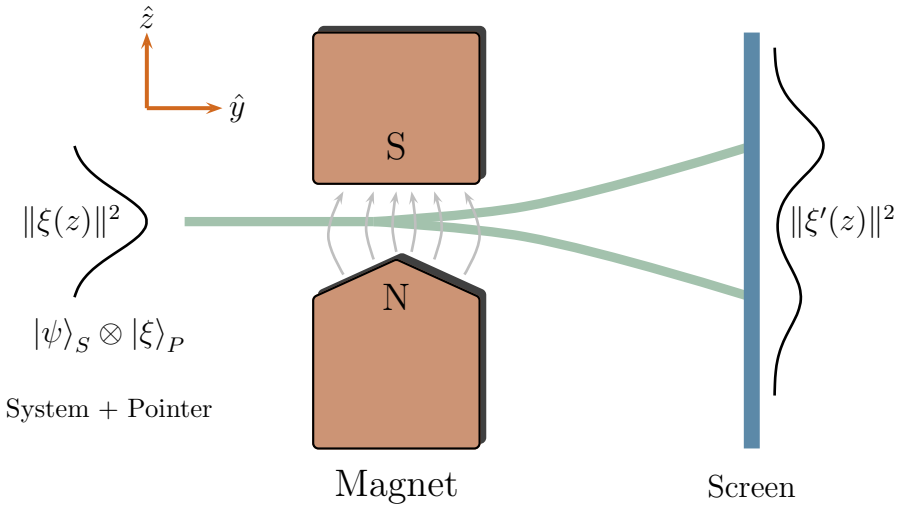


Figure 1.1: von Neumann interaction between spin and spatial degree of freedom in the presence of magnetic field gradient. The particle is initially in $|\psi\rangle_S \otimes |\xi\rangle_P$ where the spatial part $|\xi\rangle$ acts as a pointer. After passing through a magnetic field gradient in z-direction, the wavepacket splits into two. The detection of the particle on the screen is a strong measurement in the position basis which induces a collapse on the spin. Whether the spin measurement is sharp or not depends on the overlap between the two wavepackets.

standard quantum mechanics. However, unlike the latter, TSVF introduces an additional bra vector, representing the future state of the system. TSVF attempts to provide a complete physical description of a pre-and post-selected ensemble. In this section, we will briefly review the key ingredients and implications of TSVF.

1.2.1 Aharonov, Bergmann and Lebowitz retrodiction

In 1964, Aharonov, Bergmann and Lebowitz (ABL) proposed a framework to study time-symmetric measurement scenarios [27]. According to ABL, selection of certain outcomes in sequential measurements make ensemble time-symmetric, in a sense, that reversing the measurements' order does not change the physics. Consider a sequential measurement scenario depicted in Fig. 1.2. A quantum system is pre-selected in the state $|\psi\rangle$ with a preparation measurement $\mathcal{P}_1 \equiv \{|\psi\rangle\langle\psi|, |\tilde{\psi}\rangle\langle\tilde{\psi}|\}$. A subsequent projective measurement $\mathcal{P}_2 \equiv \{|\phi\rangle\langle\phi|, |\tilde{\phi}\rangle\langle\tilde{\phi}|\}$ is preformed and systems corresponding to outcome $|\phi\rangle$ are selected. Such scenarios are called pre-and post-selection (PPS) scenarios. Now suppose an observable $\mathcal{A} = \sum_i a_i |a_i\rangle\langle a_i|$ were measured between the two measurements. ABL derived a retrodiction rule: given that the system is pre-and post-selected in $|\psi\rangle$ and $|\phi\rangle$, respectively, the probability of getting outcome a_i in the intermediate measurement is given by,

$$P(a_i|\psi,\phi) = \frac{|\langle\phi|a_i\rangle|^2 |\langle a_i|\psi\rangle|^2}{\sum_j |\langle\phi|a_j\rangle|^2 |\langle a_j|\psi\rangle|^2}. \tag{1.6}$$

$P(a_i|\psi,\phi)$ is conditioned on PPS states $|\psi\rangle$ and $|\phi\rangle$ and remains invariant if pre-and post-selection are interchanged.

Application of ABL rule in counterfactual attributions of reality to hypothetical measurements' outcomes in the past results in surprising and paradoxical situations. Take the example of three box problem [28]: given that a particle is prepared in superposition of being in three non-overlapping boxes A, B and C with state $|\psi_1\rangle = \frac{1}{\sqrt{3}}(|A\rangle + |B\rangle + |C\rangle)$ and post-selected in state $|\psi_1\rangle = \frac{1}{\sqrt{3}}(|A\rangle + |B\rangle - |C\rangle)$, the probability of finding particle in box A or B upon opening the respective box at an intermediate time is one according to ABL rule. In other words if either of the boxes A and B had been opened at an intermediate time, one would always find the particle there.

The application of ABL rule in time symmetric counterfactual reasoning faced a serious refutation from Kastner [29], Miller [30], Cohen [31] and others on the philosophical ground. Giving an alternative interpretation of ABL rule as being the probability of the outcome of an actual measurement of the observable between pre-selection and post-selection measurements, the authors pinpointed that the paradoxes arise only

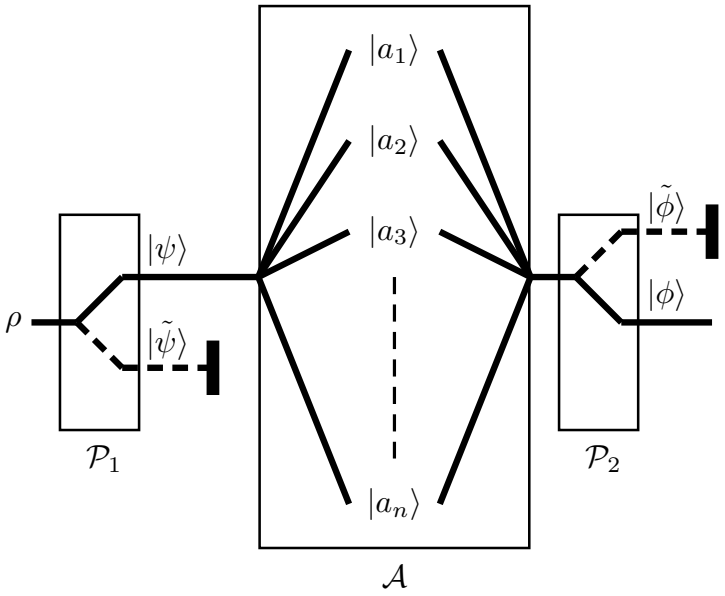


Figure 1.2: A system is pre-selected in $|\psi\rangle$ by discarding outcomes corresponding to $|\tilde{\psi}\rangle$ in measurement $\mathcal{P}_1$. The system is then post-selected in the state $|\phi\rangle$ by discarding outcomes $|\tilde{\phi}\rangle$ in measurement $\mathcal{P}_2$. The spectrum of the intermediate measurement of the observable $\mathcal{A}$ is depicted between pre-and post-selection.

when one uses ABL rule for calculating probabilities of possible outcomes of observables which have not been actually measured at the intermediate time. Taking the criticism as well as the defense of the counterfactual use of ABL rule into consideration, one can write down two distinct interpretations of ABL rule:

> **Non-counterfactual interpretation:** $P(a_i|\psi,\phi)$ is the fraction of the ensemble, which is pre-selected in $|\psi\rangle$ and post-selected in $|\phi\rangle$, that had taken eigenvalue a_i of an observable $\mathcal{A}$ when it was measured at an intermediate time. ABL probabilities are only meaningful when there is an actual intermediate measurement.
>
> **Counterfactual interpretation:** $P(a_i|\psi,\phi)$ is the probability that the system, which is pre-selected in $|\psi\rangle$ and post-selected in $|\phi\rangle$, would have taken eigenvalue a_i of an observable $\mathcal{A}$ if it had been measured at an intermediate time. Assigning ABL probabilities are meaningful even in counterfactual scenarios.

The debate about the interpretation of ABL rule was apparently settled with experimental realizations of counterfactual paradoxes using weak values introduced as a witness of ABL rule. Before going into details of the relation between ABL rule and weak values and the potential impact of this relation on our understanding of foundations of quantum theory, it would be appropriate to emphasized the element of time symmetry present in ABL rule.

Hamiltonian of the system was considered zero to derive ABL rule presented in Eq. (1.6). Let us now consider the general case where the system evolves in time under non-zero Hamiltonian H. The time transformation taking the state of the system from time t_1 to t_2 is $U(t_2;t_1) = \exp\Big(-\frac{i}{\hbar}\int_{t_1}^{t_2} H dt\Big)$. For such case the generalized ABL rule can be re-written as:

$$P(t, a_i|\psi,\phi) = \frac{|\,\langle\phi(t)|\,\Pi_i\,|\psi(t)\rangle\,|^2}{\sum_j |\,\langle\phi(t)|\,\Pi_j\,|\psi(t)\rangle\,|^2} \tag{1.7}$$

where $|\psi(t)\rangle = U(t;t_1)\,|\psi\rangle$, $|\phi(t)\rangle = U(t;t_2)\,|\phi\rangle$, and $\Pi_k = |a_k\rangle\langle a_k|$. It appears in Equation (1.7) that the probability $P(t, a_i|\psi,\phi)$ is determined by a state vector evolving forward in time $|\psi(t)\rangle$ and a state vector evolving backward in time $|\phi(t)\rangle$ (see Fig. 1.3). Moreover, the two vectors are on an equal footing. Aharonov and Vaidman gave a profound meaning to Equation (1.7) by proposing a time symmetric formulation of quantum theory called two state vector formalism (TSVF) [28]: a pre- and post-selected system is completely described by the two vectors $|\psi(t)\rangle$ and $|\phi(t)\rangle$ at an intermediate time t. Formally, the two-states are denoted as $\langle\phi(t)||\psi(t)\rangle$.

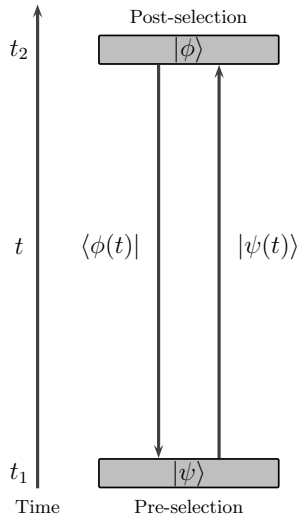


Figure 1.3: A pre-and post-selected quantum system is fully described by two-sate vectors $\langle\phi(t)||\psi(t)\rangle$. The state $\langle\phi(t)|$ evolves backward while the state $|\psi(t)\rangle$ evolves forward in time.

1.2.2 Weak values

The value of an observable does not hold a meaning prior to the measurement in the standard formalism of quantum mechanics [32, 33, 34, 35]; however, in the time-symmetric two-state vector formalism (TSVF) of quantum mechanics such a meaning is alluded to via "weak values" [26, 36, 37]. TSVF and the concept of weak values were introduced to validate the retrodiction formula introduced by Aharonov, Bergmann and Lebowitz (ABL rule) to calculate probabilities of counterfactual-measurement outcomes of an observable for a pre- and post selected ensemble [27]. In TSVF, the weak values fully determine the properties of pre- and post-selected quantum system at all intermediate times. Weak value of an observable A, for a system with two-states $\langle\phi(t)||\psi(t)\rangle$ is

$$A_w(t) = \frac{\langle\phi(t)|A|\psi(t)\rangle}{\langle\phi(t)|\psi(t)\rangle}. \tag{1.8}$$

The weak values can lie outside the range of the values of an observable allowed by standard quantum mechanics and they need not even be real. The interpretation of weak values as values of observables drew criticism from various authors [38, 39, 40, 41]. Despite the scholarly dispute over their physical meaning, weak values have been experimentally measured using weak measurements [42, 43, 44]. The concept of weak values, although formulated for the purpose of fundamental study of quantum mechanics, has been extremely useful in various fields of experimental quantum mechanics.

It has been used in understanding optical telecom networks [45], superluminal and slow light phenomena in birefringent photonic crystals [46, 47], studying optical cross-phase modulation jump [48], quantum process tomography [49], ultrasensitive quantum measurements using weak value amplification [50, 51, 52], and a review is available in reference [53]. Weak values have also been used in direct measurements of wavefunctions and in providing an operational definition to the wavefunction [54, 55].

Apart from their applications, weak values have been thought to provide insights into a number of fundamental issues in quantum mechanics, which include Hardy's paradox [56, 57, 58, 59], quantum tunneling time [60], the Legget-Garg inequality [61], Bohmian trajectories [62, 63] and quantum contextuality [64]. These studies are firmly based on the straightforward interpretation that the weak value is the value of an observable between two successive measurements of a quantum system. Weak values have also been called the weak-measurement elements of reality (WMER) [65]. It has been proposed that the trace a particle leaves at a location is proportional to the weak value of the projection operator onto that particular location [66].

1.2.3 Weak values as witness of counterfactual ABL rule

The refutation of counterfactual ABL rule on the philosophical ground was firmly based on the non-counterfactual interpretation. According to the measurement postulate of quantum theory, performing an actual measurement on quantum system at the intermediate time would destroy the state making counterfactual interpretation no longer valid. Then the question is how to experimentally witness the counterfactualness of ABL rule. The answer lies in Eq. (1.7). Using Eq. (1.8),

$$P(t, a_n|\psi, \phi) = \frac{|\Pi_n^w(t)|^2}{\sum_i |\Pi_i^w(t)|^2} \tag{1.9}$$

here $\Pi_i^w(t)$ is the weak value of the operator $\Pi_i = |a_i\rangle\langle a_i|$ at the intermediate time t which can be experimentally measured using weak measurements [26, 36, 37]. When A is a projection operator $\Pi = |\xi\rangle\langle\xi|$, the ABL rule becomes:

$$P_t(\Pi = 1|\psi, \phi) = \frac{|\Pi^w(t)|^2}{|\Pi^w(t)|^2 + |(\mathbb{1} - \Pi)^w(t)|^2} \tag{1.10}$$

The most compelling fact about the concept of weak values is that it provides a ground for an experimental realization of ABL rule even if no actual measurement is performed at the intermediate time. This gives the counterfactual interpretation an operational meaning.

1.2.4 Weak measurements followed by post-selections

In order to experimentally realize the counterfactual ABL rule, the most essential condition is that the state of the system remains undisturbed between pre- and post-selection. Hence, to observe the ABL rule without an intermediate projective measurement, it becomes necessary to devise a method for experimentally extracting information about the system between two successive measurements without causing any disturbance. The technique of weak measurements makes the latter possible.

Weak measurements are von Neumann interactions between a system and a pointer with extremely weak interaction strength. Suppose a system interacts with a pointer according to the Hamiltonian $H_{int} = -\hbar\kappa\delta(t'-t)A \otimes P$, where $\delta(t'-t)$ is the Dirac delta function of time t' and κ is the interaction strength. Here, A and P are system and pointer observables, respectively. The corresponding unitary is $U_{int} = \exp(-i\kappa A \otimes P)$. Now consider the scenario presented in Fig. 1.4, the system is pre- and post-selected in states $|\psi\rangle$ and $|\phi\rangle$, respectively. If the initial state of the pointer is $|\xi\rangle$, the state after the post-selection is obtained as,

$$|\xi'\rangle = R(\mathbb{1} + i\kappa A_w^{(1)} P + \frac{i^2}{2!}\kappa^2 A_w^{(2)} P^2 + \cdots)\,|\xi\rangle \tag{1.11}$$

Here, R is a normalization constant, $\mathbb{1}$ is identity on pointer Hilbert space and $A_w^{(i)}$ is weak value of the operator A^i given by:

$$A_w^{(i)} = \frac{\langle\phi(t)|\, A^i\, |\psi(t)\rangle}{\langle\phi(t)|\psi(t)\rangle}$$

The process of weak measurement followed by post-selection displaces the pointer state from $|\xi\rangle$ to $|\xi'\rangle$. The interaction can introduce disturbance to the system as well. Suppose $F(\kappa)$ denotes the fraction of the pre-selected ensemble that gets post-selected in $|\phi\rangle$ when the interaction strength is κ. Then,

$$\begin{aligned} F(\kappa) =& F(0)\,\big[1 - 2\kappa\,\mathrm{Im}(A_w^{(1)})\langle P\rangle \\ &+ 2\kappa^2\left(\frac{|A_w^{(1)}|^2}{2} - \frac{1}{2!}\,\mathrm{Re}(A_w^{(2)})\right)\langle P^2\rangle \\ &+ 2\kappa^3\left(\frac{1}{3!}\,\mathrm{Im}(A_w^{(3)}) + \frac{1}{2!}\,\mathrm{Im}(A_w^{(1)}A_w^{(2)*})\right)\langle P^3\rangle \\ &- \cdots\big] \end{aligned} \tag{1.12}$$

where $\langle P^i\rangle = \langle\xi|\, P^i\, |\xi\rangle$ is the expectation value of pointer observable P^i immediately before the interaction. For $\kappa = 0$, we have $F(\kappa) = |\,\langle\phi(t)|\psi(t)\rangle\,|^2 = F(0)$. For the minimal disturbance, we require $|F(\kappa) - F(0)|$ to be minimum but $\langle\xi'|\xi\rangle \neq 1$ so

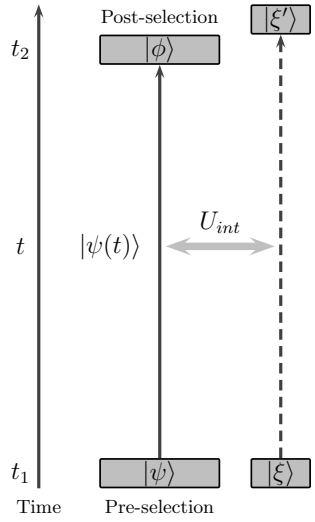


Figure 1.4: The system is pre-selected in state $|\psi\rangle$ and a pointer is prepared in $|\xi\rangle$ at time t_1. Interaction U_{int} takes place between the two at time t. The system is then post-selected in state $|\phi\rangle$ at time t_2. This leaves the pointer in state $|\xi'\rangle$.

that we can extract some amount of information from the pointer. The latter can be achieved by choosing $\kappa \ll 1$ *s. th.* $\kappa^2 \approx 0$. In that case, we have only the first order disturbance in the system. However, an unambiguous information about weak values can be obtained with a large ensemble.

The condition for realization of counterfactual ABL rule: The condition that the interaction is completely absent *i.e.* $\kappa = 0$, is the ideal situation for counterfactual ABL rule. In order to perform a successful experimental realization of counterfactual ABL rule, one must choose the value of interaction strength κ and the state of pointer in such a way that on one hand $F(\kappa)/F_0 \approx 1$ with $F(0) \neq 0$, while on the other hand there is enough displacement in the pointer state so that the effect of interaction with system observable A is measurable. These two requirements, in the light of Eq. (1.11) and (1.12), lead us to consider the necessity of simultaneous fulfilment of conditions:

$$\begin{aligned} &\langle P \rangle = 0 \\ &\kappa^2 N \to 1 \text{ with } N \gg 1 \end{aligned} \tag{1.13}$$

where N is the number of pre- and post-selected systems in the presence of interaction. If these conditions are not satisfied, operational inferences drown about the past of a quantum system are no longer valid for the system with zero interaction with pointer. More detailed discussion on the necessary condition for weak measurements is due to

Aharonov and Vaidman in context of a generalized H_{int} and case of Gaussian pointer state [36].

Measurement of weak values: In scenarios with satisfying conditions Eq. (1.13), the final pointer state with some normalization constant R is given as,

$$|\xi'\rangle \approx R\left(\mathbb{1} + i\kappa A_w^{(1)} P\right)|\xi\rangle \tag{1.14}$$

The displacement in $|\xi\rangle$ is directly proportional to $\kappa A_w^{(1)}$. Remember that $\kappa A_w^{(1)}$ is the weak value of A. Complete state tomography of the state of pointer right after the post-selection of the system reveals the precise value of $A_w^{(1)}$. The requirement for precise quantum state estimation is that the ensemble size must be infinitely large *i.e.* $N \to \infty$. The proportionality relation between the displacement in the pointer state and the weak value motivated the proponents of TSVF to interpret weak values as values of corresponding observables for PPS systems.

1.2.5 Weak value paradoxes

The use of a straightforward interpretation of weak values in a few experimental schemes has resulted in inception of new quantum paradoxes: the paradox of negative number of particles and negative pressure [37, 67], the paradox of discontinuous trajectories of photons [66, 68, 69, 70, 71, 72], and the paradox of quantum Cheshire cat [73, 74, 75, 76]. The last two have been at the center stage of the discussion for researchers working on quantum foundations. The most surprising and 'common sense' defying claim made by Danan *et al.* [69] is that *a pre- and post-selected photon in a nested Mach-Zehnder interferometer* (NMZI) *takes discontinuous trajectories to reach the detector*. The photon visits a region in the NMZI without entering and exiting it. Another 'common sense' defying claim is made by Aharonov *et al.* [73] and Denkmayr *et al.* [74] that *the internal degree of freedom of a quantum system can be separated from its wavefunction.* Many comments and papers have been published in criticism as well as defense of these claims [77, 78, 79, 80, 81, 82, 83, 84, 85].

1.2.5.1 Photons with discontinuous trajectories

An intriguing example of weak value paradox is the past of photons in nested Mach-Zehnder interferometer (NMZI), as investigated by Lev Vaidman [66, 68], where photons take discontinuous trajectories to reach the detector. The experimental setup is shown in Fig. 1.5. Single photons are pre-selected at source S and post-selected at detector D. If the phase shifter PS is tuned in such a way that there is a completely destructive interference near mirror F, then the weak values of projection operators

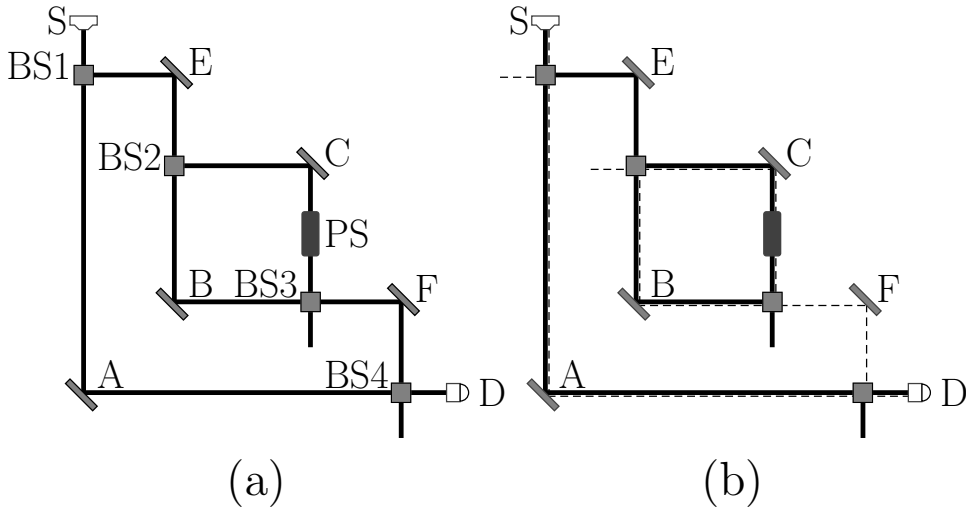


Figure 1.5: (a) Nested Mach-Zehnder interferometer. A Mach-Zehnder interferometer is inserted in on of the arms of a larger Mach-Zehnder interferometer. Beam splitters $BS1$ and $BS4$ has $2/3$ reflectivity, while $BS2$ and $BS3$ are $50-50$. PS is a phase shifter, S is a single photon source, and D is the detector. (2) Single photons coming from S are post-selected at D. The corresponding forward and backward evolving wavefunctions are denoted by solid and dashed lines, respectively.

near mirrors A, B, C, E, and F are $\Pi_A^w = 1, \Pi_B^w = 1, \Pi_C^w = -1, \Pi_E^w = 0$, and $\Pi_F^w = 0$, respectively. The interpretation of weak values as values asserts that the photons were never present near mirror E and F, however, they passed by mirrors A, B and C. This leads us to conclude that the photons took discontinuous trajectories to reach the detector. In language of counterfactual ABL rule, one would get no detection clicks if a detector had been placed near mirrors E and F. Vaidman's predictions were experimentally realized in Danan *et al*. [69] and Zhou *et al*. [70] using weak measurements.

Vaidman's claims and the experimental results of Danan *et al*. have faced serious criticism from various authers. Englert *et al*. [77] using 'unambiguous which-path information' (UWI), and R. B. Griffiths [80] using the consistent histories (CH) approach argued that the paradox of discontinuous trajectories arises from discarding second and higher order perturbation terms in the interaction strength κ. The same has been advocated by Li *et al*. [86] and by D. Sokolovski [87] using different approaches. The critique of the TSVF interpretation of the Danan experiment by these authors is primarily based on their discarding certain higher order terms, which we think is insufficient to reject the main claims because an experimental realization of counterfactual ABL rule requires the least possible disturbance to the system. For that one has to

obey conditions of Eq. (1.13). According to counterfactual ABL rule, in absence of any weak measurement devices, *i.e.*$\kappa = 0$, no photon would have been detected if a photon detector were placed near E or F while in presence an order of κ^2 fraction of pre- and post-selected ensemble would have been detected which is less than one from Eq. (1.13). Griffiths [80] has also agreed to the same in his consistent histories analysis of Danan *et al*. experiment. In order to counter claims made in Danan *et al*. one has to come up with an experimental setting where even the predictions based on the first order perturbation differ.

1.2.5.2 Quantum Cheshire cat paradox

Aharonov *et al*. [73] predicted that the internal degree of freedom of a photon (grin) can be separated from the wavefunction (cat) which has been experimentally supported by Denkmayr *et al*. [74] and Ashby *et al*. [88]. The proposed experimental setup, shown in Fig. 1.6, is a modified Mach-Zehnder interferometer in which a photon source S and beam-splitter $BS1$ are used to pre-select a single photon in the state $|\psi\rangle = (|A\rangle + i\,|B\rangle)\,|H\rangle\,/\sqrt{2}$ and a half wave plate (HWP), phase shifter (PS), a beam splitter (BS2), a polarizing beam splitter (PBS) and a single photon detector (D) are used to post-select the photon in the state $|\phi\rangle = (|A\rangle\,|V\rangle + |B\rangle\,|H\rangle)/\sqrt{2}$. Here states $|A\rangle$ and $|B\rangle$ are spatial state vectors of photon being in arm A and B, respectively. States $|H\rangle$ and $|V\rangle$ represent horizontal and vertical polarization, respectively. Eigen states of circular polarization are denoted $|\pm\rangle = (|H\rangle \pm i\,|V\rangle)/\sqrt{2}$. Let us now ask a question: which arm did photon pass through to reach detector D and what was the value of circular polarization $\sigma_z = |+\rangle\langle+| - |-\rangle\langle-|$ in each arm? To answer the question using TSVF, we calculate weak values of operators $\Pi_A = |A\rangle\langle A|\,, \Pi_B = |B\rangle\langle B|\,, \sigma_z^A = \Pi_A \otimes \sigma_z$ and $\sigma_z^B = \Pi_B \otimes \sigma_z$ as:

$$\begin{aligned} (\Pi_A)^w = 0; \quad (\Pi_B)^w = 1 \\ (\sigma_z^A)^w = 1; \quad (\sigma_z^B)^w = 0 \end{aligned} \tag{1.15}$$

According to TSVF, the circular polarization of the photon in arm A was non-zero but it did not pass through arm A while photon passed through arm B but the circular polarization in that arm was zero. This is how Aharonov *et al*. could disembody photon's polarization (the grin) from its wavefunction (cat).

1.2.5.3 Hardy's paradox

Hardy [56] used a gedanken experiment involving a bipartite system to give a logical proof against local realism just like Greenberger, Horne, and Zeilinger (GHZ) [89] did with tripartite systems, and to show a contradiction between quantum mechanics and any realistic theory which has Lorentz invariant element-of-reality. There is

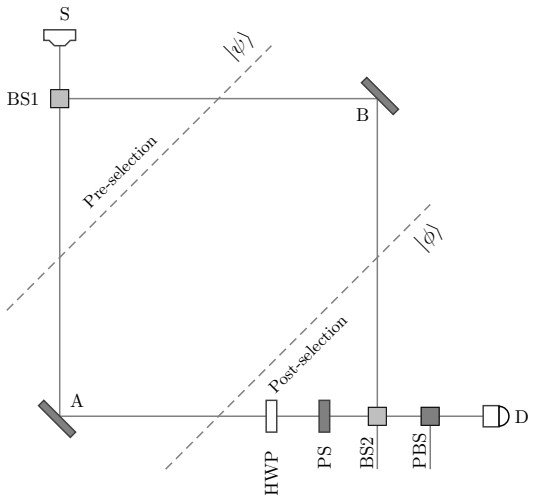


Figure 1.6: Quantum Cheshire cat setup: a photon is pre-selected in $|\psi\rangle = (|A\rangle + i|B\rangle)|H\rangle/\sqrt{2}$ using a single photon source and a $50-50$ beam splitter; and then post-selected in the state $|\phi\rangle = (|A\rangle|V\rangle + |B\rangle|H\rangle)/\sqrt{2}$ using half-wave plate HWP, phase shifter PS, another $50-50$ beam-splitter $BS2$, polarizing beam splitter PBS, and detector D.

no paradox if one drops realism and uses text book quantum mechanics without any counterfactual reasoning. The paradox arises when one uses counterfactual reasoning about the past of system in Hardy's setup [57]. The setup, see Fig. 1.7, consists of two Mach-Zehnder interferometers, one for an electron and another for a simultaneously produced positron. X is an overlapping region of inner arms of both interferometers ($I_{e^\pm}$) such that if positron and electron encounter they annihilate each other with probability one. Arms of interferometers are adjusted in such a way that there is no detection in $D_{e^\pm}$ when the two interferometers are separated in such a way that there is no overlapping region. When there is an overlap between I_{e^+} and I_{e^-}, $e^- - e^+$ annihilation in region X acts as an Elutzer-Vaidman bomb [90] and disturbs the interference causing coincident detection in $D_{e^\pm}$ with probability $1/16$. Let us now ask a question: which arms do e^+ and e^- travel through when both end up in $D_{e^\pm}$ simultaneously? A counterfactual reasoning leads to paradox: if there is coincident detection in $D_{e^\pm}$ then $e^\pm$ must have traveled through region X in order to disturb the interference, but there is no annihilation! Aharonov *et al.* [57] made the paradox even weirder when they used weak values to answer the question. Authers reached the conclusions:

(i) e^+ always had passage through region X.

(ii) e^- always had passage through region X.

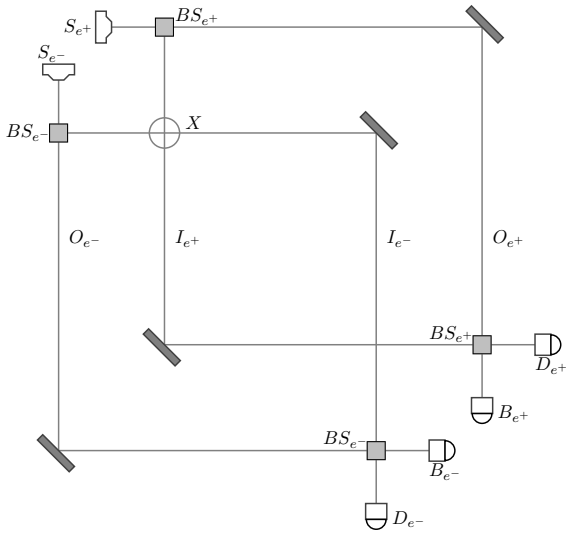


Figure 1.7: Hardy's setup: Simultaneously produced electron and positron passes through two separate matter-wave Mach-Zehnder interferometers. The interferometers have an overlap in the region X where electron and positron annihilate each other if they meet.

(iii) e^- and e^+ never both of them together had passage through region X.

Again, these conclusions are firmly based on the interpretation that weak values are values of observables. One should not get surprised looking at (apparent) contradictory statements because 'e^+ being at X' and 'both e^+ and e^- being together at X' are two different observables and can have simultaneous independent values in TSVF. The weak value version of Hardy's paradox has been experimentally realized using weak measurements [59, 91].

1.3 Quantum key distribution

Quantum Key Distribution (QKD) is a revolutionary cryptographic technique that utilizes the principles of quantum mechanics to enable secure key exchange between two parties. Unlike traditional cryptographic methods that rely on mathematical complexities [92, 93, 94], QKD leverages the inherent properties of quantum particles, such as superposition and entanglement, to ensure the confidentiality and integrity of cryptographic keys [10, 11]. By encoding the key information into quantum states and transmitting them through an optical channel, QKD offers an unprecedented level of security. The fundamental laws of physics make it virtually impossible for an eavesdropper to intercept or measure the quantum states without disturbing them, thereby

alerting the legitimate parties to the presence of an attacker. QKD holds immense promise for enhancing the security of communication systems, particularly in the face of future quantum computing advancements.

In this chapter, we summarize the main components of QKD protocols and information theoretic proofs of the same.

1.3.1 Basic components of quantum key distribution protocols

A general QKD setup is presented in Fig. 1.8. Two parties Alice and Bob, who are willing to share a symmetric key securely, are connected with a quantum communication channel over which they can share a bipartite system. Equivalently, one of them, say Alice, can prepare and share a quantum system to Bob over the quantum channel. They can manipulate their respective systems by performing local measurements choices of which are locally generated with true random number generators. Their measurement outcomes are kept secret inside their respective labs with the assumption of closed lab assumption until and unless they are needed to be announced publicly. All public announcements are made over authenticated classical channels (ACC). An adversary Eve, can have access to the quantum as well as the classical channel. However, attempts of eavesdropping are detectable in Alice's and Bob's lab using principles of quantum theory. The latter ensures the unconditional security of the shared or generated quantum key. A QKD protocol can largely be divided into five steps.

(1) Quantum state sharing or distribution: In this step, a quantum state is shared between two parties over the quantum communication channel. The two parties can either share a bipartite entangled state–entanglement-based protocols–or one of them can prepare and send it to another–prepare-and-measure protocols. The latter is equivalent of the sender holding the purification of the system that is sent to the receiver [95, 96]. In prepare-and-measure protocols, Alice prepares a system in one of two or more complementary basis and send it to Bob [95, 96]. The complementarity ensures that the sent state cannot be guessed perfectly. The latter is a beautiful consequence of the linearity of quantum mechanics. The state may get disturbed due to eavesdropping or the environmental decoherence. BB84 [10] and the six-state protocol [97] are the prime examples of prepare-and-measure protocols. In an entanglement based QKD protocol, they share a bipartite quantum system and performs their local measurements on respective systems. Ekert protocol [98] and B92 [99] fall under this category. The QKD protocol is called discrete variable QKD (DVQKD) or continuous variable QKD (CVQKD), whether or not the systems used are discrete or continuous variable.

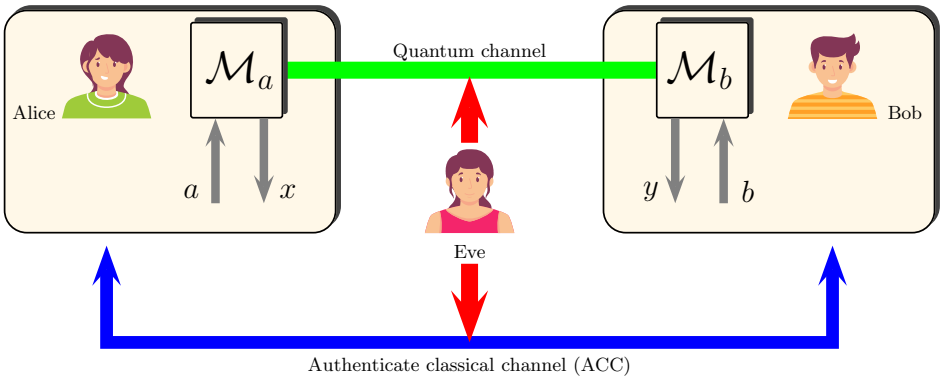


Figure 1.8: A typical quantum key distribution setup has two parties Alice and Bob who want to share a secure key. Alice and Bob are connected by a quantum communication channel that shares a quantum state between them. Additionally, They are connected with an authenticated classical channel (ACC). Alice and Bob can perform measurements on their respective quantum systems or, in general, shared quantum black-boxes using measurements $\mathcal{M}_a$ and $\mathcal{M}_b$, respectively. Their inputs are locally generated and are random. An eavesdropper Eve can have access to both ACC and the quantum channel.

(2) Measurements: After successful state sharing, both parties perform measurements on their respective systems and store the outcomes. Generally, the measurements are dichotomic. The measurements, hence, generate bit strings. The measurements are randomly chosen from a set of complementary basis.

(3) Parameter estimation: Every protocol has a set of parameters that characterize the protocol and quantify the security. In BB84, the parameter is the quantum bit error rate (QBER): the probability of outcome-mismatch when they choose the same measurement basis. Using ACC, both parties estimate the parameters with a fraction of rounds. If the parameters are in range of secure communication, they proceed, else the protocol is aborted.

(4) Sifting and raw key generation: Since both parties choose their measurement inputs randomly, there are usually rounds which are not useful in final key generation. These rounds are needed to be discarded. For instance in BB84, if their measurement basis are not matched, the outcomes have zero correlations and should be discarded. After discarding certain outcomes, they shorten the bit strings and finalized the raw key bit strings. These strings can be partially correlated and insecure *i.e.* an adversary may have access to some bits of Alice or Bob's strings.

(5) Classical post-processing: After the successful generation of partially correlated and partially-secure raw keys, they use methods of classical information theory to obtain a fully correlated and ideally secure symmetric key. First, they perform classical error correction and then the privacy amplification. In the process they loose some of the raw bits as a cost of the error correction.the protocol is secure, if the cost is less than the number of raw bits unknown to the adversary.

1.3.2 Information theoretic security proofs

The earliest security proofs of QKD protocols methods of quantum error correction codes. The advancement in the field of quantum information theory has provided a framework for the information theoretic security proofs which are more robust and easy to prove. Suppose a bipartite quantum state ρ_{AB} is shared between Alice and Bob. The state might have been intercepted by an adversary Eve while the state sharing step. The latter introduces disturbance to the system. Therefore, if can be assumed that the purification of ρ_{AB} might be held by Eve who can use it to extract information about Alice and Bob's measurement outcomes. Let ρ_{ABE} be the corresponding purified state. After N rounds of the protocol, they share state $\rho_{ABE}^{\otimes N}$. Here, it is assumed that the individual state sharing rounds are identical and independent. For asymptotically large N, their state is an ensemble of pure state ρ_{ABE}. Measurements by Alice and Bob generates a classical-classical-quantum (ccq) state:

$$\Omega_{ABE} = \sum_{a,b\in\{0,1\}} P(a,b) \left|a\right\rangle\!\left\langle a\right|_A \otimes \left|b\right\rangle\!\left\langle b\right|_B \otimes \rho_E^{ab} \tag{1.16}$$

where $P(a,b)$ is the joint probability distribution of Alice and Bob's raw key bits and ρ_E^{ab} is Eve's quantum memory when Alice and Bob have key bits a and b, respectively. Eve can protect her memory and postpone her measurements to the classical post-processing step where she can utilize information broadcast by Alice and Bob to maximize her information. This is known as collective attack strategy. The security against collective attacks is considered to be ultimate security against Eve's all strategies. Eve's knowledge in collective attacks is bounded by Devetak-Winter key rat:

$$r_{DW} \geq \mathcal{I}(A:B) - \chi(A:E), \tag{1.17}$$

where $\mathcal{I}(A:B)$ is the mutual information between Alice and Bob determined by the joint probability distribution and $\chi(A:E)$ is the Holevo quantity between Alice's bits and Eve's memory. Holevo quantity is the maximum information about Alice's raw bits that can be obtained from Eve's quantum memory. A protocol is secure against collective attacks in asymptomatic limits when $r_{DW} > 0$.

1.4 Organization of the thesis

This thesis deals with quantum measurements, weak measurements and their role in the investigations of the past of quantum particles, quantum key distributions, measurements restricted by the no-faster-than light communication principle and demonstration of wave-particle duality using von Neumann interactions. The rest of the thesis is organized as follows.

Chapter 2

This chapter proves that the past of quantum particles cannot consistently be described by weak values. To do so, we propose a gedanken experiment that shows that photons reveals their presence at locations where weak values of the position are zero.

Chapter 3

In this chapter, we investigate the generality of the two state vector formalism. We show that weak values for mixed states can lead us to erroneous quantum state discrimination. Which, consequently, can result into false security proofs of quantum key distribution protocols.

Chapter 4

This chapter presents a quantum key distribution protocol where we have used quantum block-wise processing to achieve high-noise tolerance against collective attacks. We have provided an information security proof of the same in asymptomatic limits. Our techniques shows a significant improvement in the noise-tolerance.

Chapter 5

This chapter presents a novel no-go theorem and its applications in quantum Darwinism. We prove that the internal degrees of freedom cannot be manipulated or measured without disturbing particles' spatial wavefunctions. Furthermore, we use our no-go theorem to explain emergence of the classical objectivity in the position basis.

Chapter 6

This chapter presents a proposal for the experimental demonstration of wave-particle complementarity using discrete variable systems and a Gaussian pointer. We show that the complementarity in discrete systems can be transferred to the pointer using

von Neumann interactions and then the corresponding interference phenomena can be observed. Our results provide an operational definition to the coherence in discrete system in terms of fringe visibility of the corresponding interference pattern.

Chapter 7

In this chapter, we briefly summarize results presented in the thesis and discuss the future outlook.

Chapter 2

Weak values cannot consistently describe the past of quantum particles

2.1 Introduction

The ABL rule provides a way to calculate the probability of a counterfactual measurement outcome for a pre- and post-selected ensemble [27]. However, this rule can assign probabilities to unperformed measurements, which may violate classical probability theory and give rise to retro-causal quantum paradoxes. The proponents of the ABL retrodiction rule developed TSVF, a time-symmetric formalism of quantum mechanics for pre-and post-selected ensembles. Claims of TSVF were backed by experimental demonstrations of weak values which are understood as values of physical observables between two successive measurements. Although, the value of an observable does not hold a meaning prior to the measurement in the standard formalism of quantum mechanics [32, 33, 34, 35]; but, in TSVF such a meaning is alluded to via "weak values" [26, 36, 37]. In the TSVF approach, weak values are used to fully describe quantum systems between successive measurements. These weak values may be complex, in contrast to the always-real observable values in standard quantum mechanics, leading to debate about their physical significance and interpretation among various authors.

Despite the lack of a consensus on interpretation [38, 39, 40, 41], weak values have found important applications in quantum information processing [45, 49, 54, 55], quantum metrology [50, 51, 52], and various fields of experimental quantum theory [46, 47]. Apart from their applications, weak values have been thought to provide insights into a number of fundamental issues in quantum mechanics, which includes Hardy's paradox [56, 57, 58, 59], quantum tunneling time [60], the Legget-Garg inequality [61],

Bohmian trajectories [62, 63], and quantum contextuality [64]. These studies are firmly based on the straightforward interpretation that weak values are the values of observables between two successive measurements of a quantum system. The latter is motivated by the fact that when a system is weakly measured with a pointer, the displacement (or translation) in the pointer state is directly proportional to the weak value of the observable. This is strikingly like the projective measurement of an observable in which the translations in the pointer state are proportional to the eigenvalue outcomes of the observable. This led L. Vaidman to define weak values as elements of the reality of weak measurements [65].

The use of the straightforward interpretation of weak values has resulted in the inception of various quantum paradoxes: the paradox of the negative number of particles and the negative pressure [37, 67], the paradox of discontinuous trajectories of a photon [66, 68, 69, 70, 71, 72], weak value version of Hardy's paradox, quantum pigeonhole paradox, and the paradox of quantum Cheshire cat [73, 74, 75, 76]. These paradoxes have been discussed among quantum physicists for a decade. One of the most surprising and 'common sense' defying paradoxes (reported in Danan *et al.* [69]) is that a pre- and post-selected photon in a NMZI takes discontinuous trajectories to reach the detector. The photon visits a region in the NMZI without entering and exiting it. Another 'common sense' defying claim is made by Aharonov *et al.* [73] and Denkmayr *et al.* [74] that the internal degree of freedom of a quantum system can be separated from its wave function. Many comments and papers have been published in criticism as well as defense of these claims [77, 78, 79, 80, 81, 82, 83, 84, 85].

This chapter presents a thought experiment utilizing time-varying Hamiltonians to demonstrate that weak values do not provide a complete picture of a quantum particle's past [100]. This finding contradicts the assertion that the TSVF approach fully describes pre-and post-selected quantum systems. The Hamiltonian evolution and time-dependent elements in the quantum state before measurement may not be apparent in the postselection process, but they can be detected in the probability distribution over time. The thought experiment incorporates oscillating, time-dependent elements inserted at specific locations in the Hamiltonian, and the resulting frequencies in the probability distribution indicate the particle's passage through these locations. Our analysis reveals that weak values within the TSVF formalism occasionally fail to capture the presence of quantum particles. Moreover, we prove that weak values cannot always consistently describe the past of a quantum particle.

The material in this chapter is arranged as follows: Section 2.2 gives a brief review of the ABL rule, TSVF, Weak Values, and their interconnections. Section 2.3 describes our gedanken experiment aimed at providing a counterexample to the weak value-based interpretation of the past of a quantum particle. In Section 2.4 we compare the predictions of our analysis with those of TSVF to demonstrate the mismatch.

Section 2.5 provides conclusions and discussion.

2.2 Weak value hypothesis and implications

According to the ABL rule, the measurement of an observable A of a quantum system at time t which is pre-selected in state $|\psi_1\rangle$ at time $t_1 < t$ and post-selected in state $|\psi_2\rangle$ at time $t_2 > t$ would yield eigenvalue a_n with probability [27, 28]:

$$P_t(a_n|\psi_1,\psi_2) = \frac{|\langle\psi_2(t)|\,\Pi_{a_n}\,|\psi_1(t)\rangle\,|^2}{\sum_i |\langle\psi_2(t)|\,\Pi_{a_i}\,|\psi_1(t)\rangle\,|^2} \tag{2.1}$$

where $\Pi_{a_i} = \sum_\alpha |a_{i,\alpha}\rangle\langle a_{i,\alpha}|$ with $\{|a_{i,\alpha}\rangle\}$ being a complete set of eigen states of A labeled by eigenvalues a_i, and $|\psi_j(t)\rangle = \exp\left[-\frac{i}{\hbar}\int_{t_j}^{t} H dt\right]|\psi_j\rangle$ with $j = 1, 2$. It can be seen that the state $|\psi_1(t)\rangle$ evolves forward while the state $|\psi_2(t)\rangle$ evolves backward in time both being on equal footing in the TSVF formalism.

According to the measurement postulate of quantum theory, performing an actual measurement on a quantum system at the intermediate time would destroy the prepared state making counterfactual interpretation no longer valid. Then the question is how to experimentally witness the counterfactuals of the ABL rule. The answer is that the ABL probabilities given by Equation (2.1) can be inferred using weak values $\Pi^w_{a_i}(t)$ of the projection operators $\{\Pi_{a_i}\}$ at the intermediate time t, given as:

$$\Pi^w_{a_i}(t) = \frac{\langle\psi_2(t)|\,\Pi_{a_i}\,|\psi_1(t)\rangle}{\langle\psi_2(t)|\psi_1(t)\rangle} \tag{2.2}$$

which can be experimentally determined without collapsing the wave function. The concept of weak values has thus been claimed to have the potential to provide a ground for an experimental realization of the ABL rule without performing a projective measurement at intermediate times and thereby giving the counterfactual interpretation an operational meaning.

Let us for a moment revisit, the three-box problem. If any of the boxes A and B had been opened, according to the counterfactual ABL rule, the particle would have been found with certainty (probability one) in the respective box. This raises a serious and natural question: how can a single particle be present in more than one box with certainty? The concept of weak values resolves this problem. It has been hypothesized that *the weak values are values of corresponding observables and fulfill the conditions of being elements of the reality of weak measurements (WMER)* [28, 65]. Let us call it the *weak value hypothesis* (WVH). The validity of WVH naturally leads one to conclude that the weak value of a projection operator $|\eta\rangle\langle\eta|$ is the number of quantum systems present in the state $|\eta\rangle$. Therefore, the number of particles present in boxes

A, B, and C are $1, 1$ and -1 respectively keeping the total number of particles one at any intermediate time. As one can see one has to accept the concept of negative number particles in this explanation!

A natural consequence of WVH is the truthfulness of the following statement:

S-A: *If the weak value of the projection operator $\Pi_x = |x\rangle \langle x|$ at an intermediate time is zero, where $|x\rangle$ is a position eigenstate; then the particle was not present at position x at that time.*

The above statement is just a codification of the counterfactual statement: that if $P_t(a_n|\psi_1, \psi_2) = 0$ then the measurement of observable A on the system at the intermediate state would never yield value a_n. Since the whole purpose of bringing the concept of weak measurements was to provide an operational meaning to the counterfactual ABL rule in terms of weak values, one can write an operational definition of the past of a quantum particle, as has been done by Vaidman, using the concept of weak values and weak trace [66]:

S-B: *A quantum particle was present at a location if and only if it left a weak trace on a pointer located at that location upon interaction.*

A system, here a particle, leaves weak trace of its presence upon interaction with a pointer. Weak traces can be experimentally measured by a complete state tomography of the pointer state after the post-selection of the system state. Since the post-selection measurement leaves the state of the system and the pointer separable, a further measurement of the pointer state will definitely not affect the past of the system in a retrocausality manner.

The adoption of S-A and S-B to investigate the past of quantum systems leads to peculiar paradoxical situations [57, 66, 68, 73]. These paradoxes are being posed as real paradoxes because weak measurements can be realized at an operational level and the ABL rule is thought to be valid as a retrodiction formula for the assignment of probabilities to 'counterfactual events'. Such paradoxes are commonly known as weak value paradoxes or pre-and post-selection paradoxes. These paradoxes have faced serious skepticism which can be broadly divided into two categories. The First kind of criticism focuses primarily on experimental aspects of the realizations of the paradoxes using weak measurements where higher-order perturbation terms are neglected according to the minimal disturbance assumption. It is argued, in this approach, that the paradoxes can be resolved if one retains terms of all orders of the perturbation strength in the analysis [77, 80, 86, 87]. While the second kind of criticism, primarily due to D. Sokolovski [41, 101], focuses on the refutation of the WVH and re-interpretation of weak values as Feynman's transition amplitudes. A critical analysis of some of the weak value paradoxes based on this approach can be found in reference [101]. Even though both approaches contribute significantly to the debate by providing logical solutions to the paradoxes, the existing literature still lacks a concrete operational

refutation of these paradoxes where one can show experimental disagreement with the 'weak trace' approach but to the first order. Here, we fill this gap by proposing an experimental scenario where disagreement with the 'weak trace' approach can be shown to first order. Our results invalidate WVH as it challenges its ability to pin down the past of a quantum particle.

2.3 The gedanken experiment

We now describe our main results where we will consider a situation where the predictions of weak values can be seen to come in contradiction with descriptions based on standard quantum mechanics. Consider A quantum system with a six-dimensional Hilbert space $\mathcal{H}$. For the purpose of the gedanken experiment, we can think of a quantum particle being in six non-overlapping boxes. If the particle is found in the i^{th} box with certainty, the state vector of the particle is written as $|i\rangle$. In the absence of interactions, these states are orthogonal to each other. The boxes are designed in such a way that the interactions can be switched on so that the particle can tunnel between any pair of boxes in a controlled manner. The boxes i and j can be made to interact instantaneously at time t' via the interaction Hamiltonian $H' = g\delta(t-t')\sigma_y^{(ij)}$. Here $\sigma_y^{(ij)} = i(-|i\rangle\langle j| + |j\rangle\langle i|)$ is σ_y Pauli matrix and $\delta(t-t')$ is a Dirac delta function of time t. The tunable parameter g represents the tunneling strength and we call the process a *leakage* process when g is sufficiently small. Further, the *operational condition* $g^2N \approx 1$ has to be satisfied where N is a large number representing the ensemble size is being considered by the experimenter. Therefore, we need to retain only the terms linear in g unless it is multiplied by N. In the rest of the chapter, whenever we neglect the contribution of higher powers of some quantity, it is understood that we are assuming that the *operational condition* is satisfied.

Consider a quantum state $|\psi(t_0)\rangle$ of the particle at t_0 which undergoes time evolution according to the Hamiltonian:

$$H = \sum_{i=1}^{9} H_i, \tag{2.3}$$

with

$$\begin{aligned}
H_1 &= -\hbar\{\sin^{-1}(\sqrt{2/3})\delta(t-t_1)(\sigma_y^{(13)}+\sigma_y^{(24)})\} \\
H_2 &= -\epsilon\hbar\cos(\omega_1 t)\delta(t-t_2)\sigma_y^{(34)} \\
H_3 &= -\frac{\pi}{4}\hbar\delta(t-t_3)(\sigma_y^{(35)}+\sigma_y^{(46)}) \\
H_4 &= -\epsilon\hbar\delta(t-t_4)\{\cos(\omega_2 t)\sigma_y^{(12)}+\cos(\omega_3 t)\sigma_y^{(34)}+\cos(\omega_4 t)\sigma_y^{(56)}\} \\
H_5 &= -\frac{\pi}{2}\hbar\delta(t-t_5)(I^{(56)}-\sigma_z^{(56)}) \\
H_6 &= -\frac{\pi}{4}\hbar\delta(t-t_6)(\sigma_y^{(35)}+\sigma_y^{(46)}) \\
H_7 &= -\epsilon\hbar\cos(\omega_5 t)\delta(t-t_7)\sigma_y^{(34)} \\
H_8 &= -\hbar\{\sin^{-1}(\sqrt{2/3})\delta(t-t_8)(\sigma_y^{(13)}+\sigma_y^{(24)})\} \\
H_9 &= -\frac{\pi}{4}\hbar\delta(t-t_9)\sigma_y^{(12)}
\end{aligned} \tag{2.4}$$

where $I^{(ij)} = |i\rangle\langle i| + |j\rangle\langle j|$ and $\sigma_z^{(ij)} = |i\rangle\langle i| - |j\rangle\langle j|$. The impulsive interaction occurs at moments of time $t_0 < t_1 < t_3 < \cdots < t_8 < t_9$. The parameter $\epsilon \ll 1$ is such that the contributions of higher powers of ϵ in the experimental observations are negligible. Therefore, H_2, H_4, and H_7 generate *leakage* processes between certain boxes. The time intervals between t_i's are kept fixed for repeated runs of the experiment. Since all the transformations generated by H_i are momentary and well separated in time, the state of the particle at time $t > t_9$ is given for infinitesimally small Δ as

$$\begin{aligned}
|\psi(t)\rangle = \exp\left[-\frac{i}{\hbar}\int_{t_9-\Delta}^{t_9+\Delta} H_9 dt\right]\exp\left[-\frac{i}{\hbar}\int_{t_8-\Delta}^{t_8+\Delta} H_8 dt\right]\cdots \\
\cdots\exp\left[-\frac{i}{\hbar}\int_{t_2-\Delta}^{t_2+\Delta} H_2 dt\right]\exp\left[-\frac{i}{\hbar}\int_{t_1-\Delta}^{t_1+\Delta} H_1 dt\right]|\psi(t_0)\rangle
\end{aligned} \tag{2.5}$$

The sequence of momentary interactions presented in Equation (2.4) and the time evolution of the system shown in Equation (2.5) can be understood as a sequence of unitary operations $U_1, U_2, \cdots, U_9$ acting on the system at times $t_1, t_2, \cdots, t_9$ respectively, where

$$U_j = \exp\left[-\frac{i}{\hbar}\int_{t_j-\Delta}^{t_j+\Delta} H_j dt\right] \tag{2.6}$$

Unitary operations $\{U_i\}$ are 6×6 matrices:

$$U_1 = U_8 = \begin{bmatrix} \frac{1}{\sqrt{3}}\mathbf{I} & \sqrt{\frac{2}{3}}\mathbf{I} & \mathbf{0} \\ -\sqrt{\frac{2}{3}}\mathbf{I} & \frac{1}{\sqrt{3}}\mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} \end{bmatrix}; U_2 = \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{L_1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} \end{bmatrix}$$

$$U_3 = U_6 = \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \frac{1}{\sqrt{2}}\mathbf{I} & \frac{1}{\sqrt{2}}\mathbf{I} \\ \mathbf{0} & -\frac{1}{\sqrt{2}}\mathbf{I} & \frac{1}{\sqrt{2}}\mathbf{I} \end{bmatrix}; U_4 = \begin{bmatrix} \mathbf{L2} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{L_3} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{L_4} \end{bmatrix}$$

$$U_5 = \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \sigma_z \end{bmatrix}; U_7 = \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{L_5} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} \end{bmatrix}; U_9 = \begin{bmatrix} \mathbf{R} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} \end{bmatrix}$$

where

$$\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; \mathbf{0} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}; \mathbf{R} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$

$$\mathbf{L_1} = \begin{bmatrix} \cos(\epsilon \cos \omega_1 t_2) & \sin(\epsilon \cos \omega_1 t_2) \\ -\sin(\epsilon \cos \omega_1 t_2) & \cos(\epsilon \cos \omega_1 t_2) \end{bmatrix}$$

$$\mathbf{L_5} = \begin{bmatrix} \cos(\epsilon \cos \omega_5 t_7) & \sin(\epsilon \cos \omega_5 t_7) \\ -\sin(\epsilon \cos \omega_5 t_7) & \cos(\epsilon \cos \omega_5 t_7) \end{bmatrix}$$

and

$$\mathbf{L_i} = \begin{bmatrix} \cos(\epsilon \cos \omega_i t_4) & \sin(\epsilon \cos \omega_i t_4) \\ -\sin(\epsilon \cos \omega_i t_4) & \cos(\epsilon \cos \omega_i t_4) \end{bmatrix}$$

for $i = 2, 3, 4$.

As we shall see, the *leakage* processes described above are engineered to provide us with a tool to investigate the past of the particle. A *leakage* process between two completely empty boxes will definitely not make any contribution to the time evolution of the state of the particle and hence will not have any measurable effects. Therefore, the measurable effect of such a *leakage* process, between any two boxes in the state of the particle is evidence that the amplitude of the particle was not zero at least in one of the boxes involved in the *leakage* interaction. It is easy to see that due to the *leakage* process, the change in the probability amplitude of the particle being in one box is proportional to the probability amplitude of it being in the other box.

The initial state of the particle is prepared in $|1\rangle$ at time t_0. The probability of finding the particle in state $|1\rangle$ according to Born rule at time $t' > t_9$, retaining only terms linear in ϵ, is calculated using Equation (2.5) as:

$$P = \frac{1}{18}\{1 + 2\epsilon(2\cos\omega_1 t_2 - \cos\omega_2 t_4 + \cos\omega_3 t_4 + \cos\omega_4 t_4)\} \tag{2.7}$$

For the purpose of possible experimental realization of the sequence of unitaries on a state in six-dimensional Hilbert space, one can think of a single photon interferometer with six ports as detailed in Figure. (2.1). In this setup a single photon inside the interferometer can be in a superposition of six non-overlapping ports forming a six-dimensional Hilbert space. The single photon prepared in a superposition of being

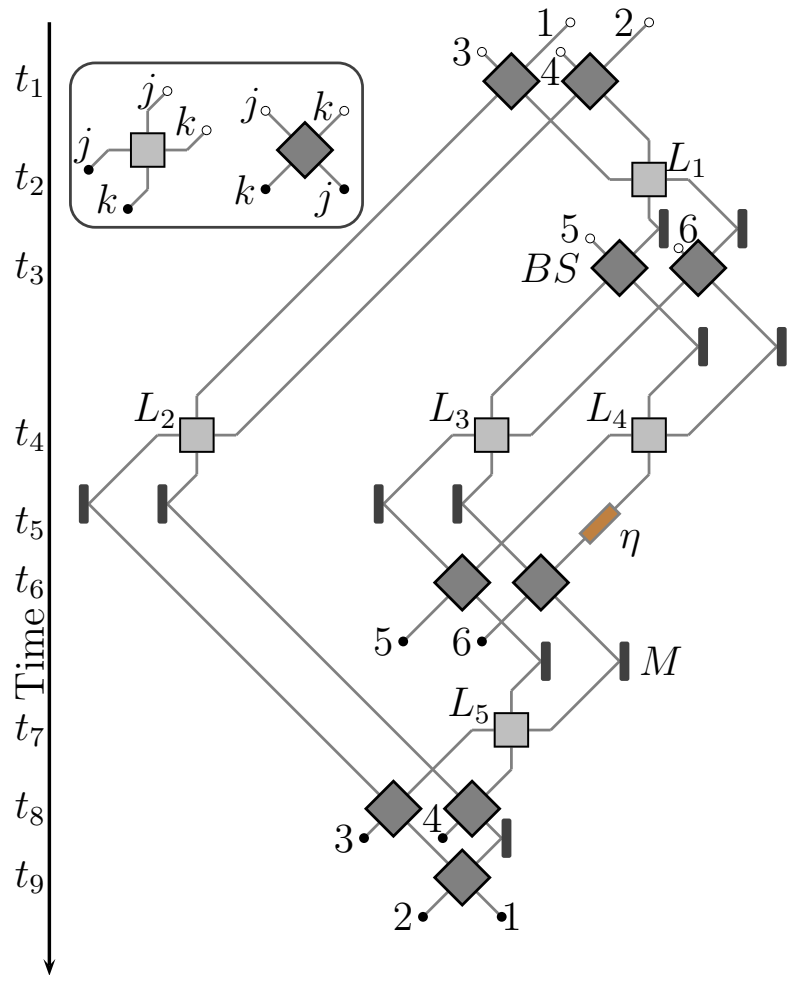


Figure 2.1: Six-port interferometer with empty dots showing the input ports and filled dots showing the output ports. The dark square boxes are the beam-splitters (BS), the light boxes are the time-dependent L elements and the long dark rectangle are the mirrors. The top left corner shows the input and output ports for L and BS.

present in six ports at time $t_0 < t_1$ undergoes the sequence of unitaries $U_1, U_2, \cdots, U_9$ at moments of time $t_1, t_2, \cdots, t_9$ respectively. The first two zero-loss beam-splitters (BS) having transmission and reflection coefficients of one-third and two-thirds respectively act on pairs of ports-$1, 3$, and ports-$2, 4$ to generate the unitary time transformation U_1 at time t_1. U_2 is generated by an element L_1, which is also a beam-splitter but with a time-varying reflectivity, acting on pair of port-3 and port-4. The reflectivity of L_1 is so small that the probability amplitude in either of the input ports (3 or 4) remains unaffected but at the same time, it transfers a very tiny amplitude between the ports in either direction as a leakage process so that it can make a contribution in providing information about the past of the photon in the interferometer. The role of the time dependence of L_1 will become clear from the discussion that follows. The unitary U_5 is generated by a phase shifter η which produces a phase shift of π in the probability amplitude of photon in the port-6. The rest of the unitaries can be easily related to processes presented in Figure (2.1) which are either BS or leakage processes.

As one would expect, the probability P depends on the reflectivity of the time-dependent beam-splitters $\{L_i\}$ at the moments of time when the localized wave packet of photon passes through them. Looking carefully at the experimental setup shown in Figure (2.1), we can say $t_1, t_2, \cdots, t_9$ are not independent variables present in unitaries but are dependent on the time when the photon enters the interferometer. To make the latter point clearer we emphasize the fact that the optical path length of the photon traveling from one optical device to another is fixed over time. In other words, one can say that the time difference between the unitaries is fixed. Consider the optical path length from the source to the optical device generating U_j to be l_j, then one has $t_j = t_0 + l_j/c$ where t_0 is the time when the photon leaves the source. The time of detection of the photon at port-1 is t' and $t' - t_0 = \tau$ is constant across various repetitions of the experiment. Physically it means that the photon takes τ time to travel from source to detector each time the experiment is carried out. Using the relation $t_j = t' + (l_j/c - \tau)$, Equation (2.7) can be re-written as a function of t' as follows:

$$\begin{aligned} P = \frac{1}{18}[1 + 2\epsilon\{2\cos(\omega_1 t' - \theta_1) - \cos(\omega_2 t' - \theta_2) \\ + \cos(\omega_3 t' - \theta_3) + \cos(\omega_4 t' - \theta_4)\}] \end{aligned} \tag{2.8}$$

Where $\theta_1 = \omega_1(\tau - l_1/c), \theta_i = \omega_i(\tau - l_4/c)$ for $i = 2, 3, 4$ depend on oscillation frequencies of various time-varying beam splitters and the geometry (optical path-length) of the interferometer and hence are constant phases. Further assuming the condition $\omega_j^{-1} \gg \tau$ with $j = 1, 2, \cdots, 5$ which gives $\theta_i \ll 1$ for $i = 1, 2, 3, 4$; Equation (2.8) can be simplified as:

$$P \approx \frac{1}{18}[1 + 2\epsilon(2\cos\omega_1 t' - \cos\omega_2 t' + \cos\omega_3 t' + \cos\omega_4 t')] \tag{2.9}$$

Probability P depends on the reflectivities of various L_j's at the time when the photon passes through them. Equations (2.8) and (2.9) are our main results. We use Equation (2.9) in drawing operational inferences about the past of the photon. It is to be emphasized here that these inferences can be drawn by using Equation 2.8 also to avoid any misunderstanding regarding the approximation $\omega_j^{-1} \gg \tau$, however, Equation 2.9 is simpler and more convenient to use.

Experiments with a single particle cannot reveal any information about the time dependency of probability P, but experimental runs over ensembles with varying times can provide information about the frequencies present in the modulated probability P. As we describe next, the experimental realization of Equation (2.9) can be achieved if we sample a sufficient number of photons in a time window in which the time-dependent optical elements in the circuit do not vary appreciably.

2.3.1 Sampling protocol

The probability P can be experimentally measured by repeating the experiment a large number of times at a certain rate. We need to have the frequencies ω_i sufficiently small so that we can measure over a sufficiently large number of particles before the time-varying elements L_i changes appreciably. Suppose at each time $t = t_0 + 2n\tau$ where $n = 0, 1, 2, \cdots, N_s$, a particle is pre-selected which will undergo a post-selection measurement at time $t = t' + 2n\tau$. N_s is the number of particles pre-selected in one sample run. Note that not all pre-selected particles get post-selected. A particle found in state $|1\rangle$ is counted, otherwise, it is discarded. Right after each post-selection measurement the experimental setup is kept ready to perform pre-selection on a new particle. The sampling time period $T_s = 2\tau N_s$ is the time taken to run an experiment on a sample of N_s particles. N_s and ϵ must be chosen in such a way that the operational condition $\epsilon^2 N_s \approx 1$ is satisfied.

As we shall see this can be easily achieved with photons. For a precise measurement of modulations, the change in the number of post-selected particles in each consecutive sample is required to be smooth, hence $1 \gg T_s\omega_i$ is necessary. The number of post-selected particles in the k^{th} sample is:

$$\begin{aligned} N_k = \frac{N_s}{18} + \frac{\epsilon N_s}{9}[2\cos\{\omega_1(2k-1)\frac{T_s}{2}\} \\ - \cos\{\omega_2(2k-1)\frac{T_s}{2}\} + \cos\{\omega_3(2k-1)\frac{T_s}{2}\} \\ + \cos\{\omega_4(2k-1)\frac{T_s}{2}\}] \end{aligned} \tag{2.10}$$

Due to $\epsilon N_s \gg 1$, the (co)sinusoidal oscillations can be observed. The Fourier analysis of the best fit of (2.10) reveals the frequencies ω_i.

In the case of photon: $\tau = \frac{l}{c}$, here l is the optical path-length - the distance each photon travel from source to detector in the interferometer. The requirements for the weakness of ϵ and sampling are: $\epsilon^2 N_s \approx 1$ and $1 \gg T_s \omega_i$. That gives $\omega_i \ll \frac{c\epsilon^2}{2l}$ (here we have used $N_s = \frac{T_s}{2\tau}$). For an interferometer of length one meter and $\epsilon \approx 10^{-2}$, $\omega_i \ll 15000$. The choice of $\omega_i \approx 100$ is reasonable. For photons with well-localized wave packets, one can increase N_s (hence decrease ϵ) by sending a train of photons with a small spacing between the two successive photons into the interferometer.

2.3.2 Where was the photon?

We make use of Equation (2.9) to draw inferences about the presence of the photon at various locations inside the interferometer. The appearance of any observable signature of a localized device in the post-selection probability is considered an indicator of the presence of the particle at that location. In an experimental setup involving (co)sinusoidal time-varying *leakage processes* L_j's with various frequencies ω_j's, our operational definition of the past says: *it cannot be possible that the particle was not present at the location where L_i is installed if frequency ω_i corresponding to device L_i is present in the modulated probability P of post-selection*. Therefore, we interpret the past using the following principle:
S-C: *A quantum particle cannot carry information about a localized object without interacting with it. In particular, if the particle is a photon inside an interferometer, it cannot not visit the location of a localized optical device and still gain information about it.*

Let us now look at Equation (2.9) and draw valid inferences about the past of a photon inside the interferometer under discussion. Appearances of frequencies $\omega_1, \omega_2, \omega_3$, and ω_4 tell a story about the past of the photon: one cannot say with certainty that the photon, pre- and post-selected at the entrance and exit of port-1 respectively, has not been at anyone or more of the locations where time-varying beam-splitters L_1, L_2, L_3 and L_4 are installed.

The key result of this section to be emphasized for further use is that one cannot claim with certainty that the photon entered the interferometer through port-1 and detected at output port-1 was not present at L_1 at any intermediate time. One may ask an interesting question here, how many of the pre-and post selected particles had visited the optical device L_1? We would like to emphasize here, as a remark, that the answer to this question depends on the ontological interpretation of the quantum theory. For instance, the answer given by De Broglie–Bohm interpretation (a ψ-supplemented ontological model [102]) differs from that given by a ψ-complete interpretation (a quantum theory without any hidden variables). Any further discussion on this matter is out of the reach of this article. The goal of this work is to show that WVH cannot

consistently explain the key result of this section.

2.4 TSVF analysis of the gedanken experiment

Let us now explore the predictions of the TSVF of quantum mechanics for our gedanken experiment. In order to answer the question of whether the particle was present in at least one box of the pair of boxes right before the *leakage* took place, we perform weak measurements on both boxes. The weak traces present in the pointer state after the post-selection will reveal the presence of the particle. For the particle pre-selected in state $|\psi\rangle = |1\rangle$ at time t_0 and post-selected in the state $|\phi\rangle = |1\rangle$ at time t', we calculate the weak values of the projection operators at those boxes at the corresponding times. The weak value of projection at box k (port-k of the interferometer in case of the photon) right before time t_j is written $\Pi_k^w(t_j)$. The weak values of projections $\Pi_k = |k\rangle\langle k|$ right before all the *leakage* processes come out to be:

$$\begin{aligned}
\Pi_3^w(t_2) &= \epsilon(2\cos\omega_1 t' + \cos\omega_3 t' + \cos\omega_4 t') \\
\Pi_1^w(t_4) &= 1 - \epsilon(2\cos\omega_1 t' + \cos\omega_3 t' + \cos\omega_4 t') \\
\Pi_3^w(t_4) &= -1 + \epsilon(2\cos\omega_1 t' - \cos\omega_2 t' + 2\cos\omega_3 t' + \cos\omega_4 t' + \cos\omega_5 t') \\
\Pi_4^w(t_4) &= \epsilon\cos\omega_1 t' \\
\Pi_5^w(t_4) &= 1 - \epsilon(2\cos\omega_1 t' - \cos\omega_2 t' + \cos\omega_3 t' + \cos\omega_5 t') \\
\Pi_6^w(t_4) &= \epsilon\cos\omega_1 t' \\
\Pi_4^w(t_7) &= \epsilon(2\cos\omega_1 t' + \cos\omega_3 t' + \cos\omega_4 t') \\
\Pi_3^w(t_7) &= \Pi_4^w(t_2) = \Pi_2^w(t_4) = 0
\end{aligned} \tag{2.11}$$

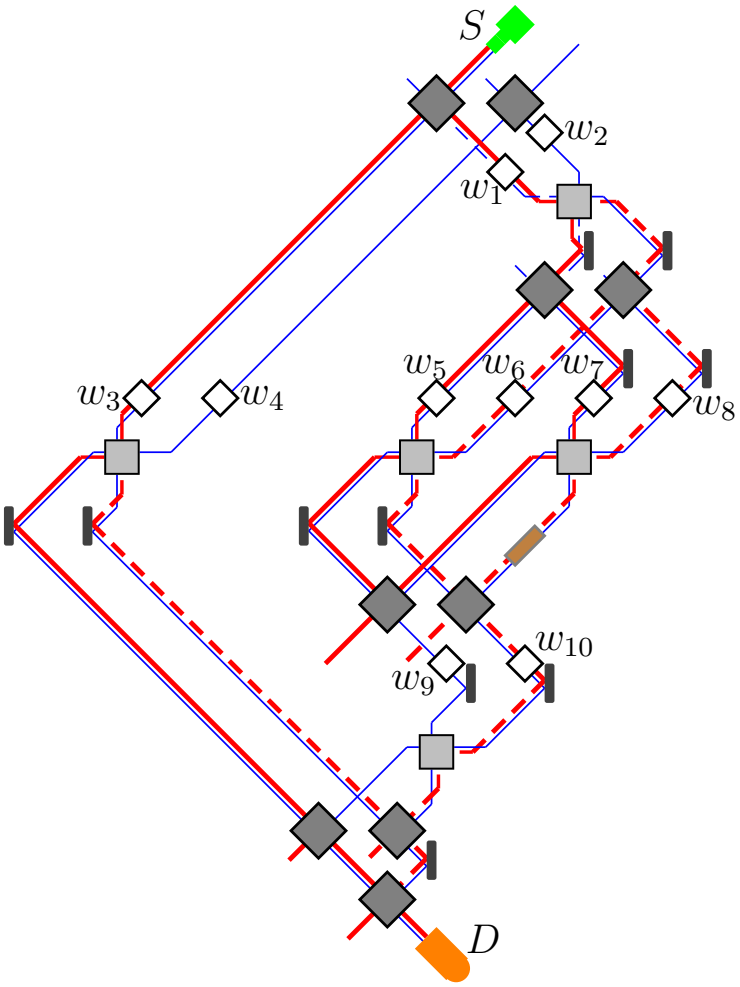


Figure 2.2: The thick (red) and thin (blue) lines represent the forward and backward evolving state vectors of the single photon, pre and post-selected at source S and detector D, respectively. The solid lines represent the non-vanishing and significant probability amplitude, dashed lines represent insignificant (order ϵ) probability amplitudes, and the absence of a line represents amplitudes that are zero or proportional to higher powers of ϵ. $w_1, w_2, \cdots, w_{10}$ denote weak measurement devices of corresponding projection operators.

2.4.1 Measurement of weak values

The weak values can be measured by introducing weak von Neumann-type interaction between the system and the pointer with interaction Hamiltonian between the system and the apparatus given by

$$H_{\mathrm{SA}} = \kappa\delta(t - t')\hat{A} \otimes \hat{p} \tag{2.12}$$

Where κ is the strength of the measurement, $\hat{A}$ is the observable being measured (in our case it is the projection operator onto a particular location) and $\hat{p}$ is the pointer momentum operator. The measurement is weak when $\kappa \ll 1$. After this interaction, the displacement of the pointer state vector is proportional to the weak value of the observable being measured. The initial state of the ancillary system is taken to be a Gaussian with a finite width. In the case of a photon, one can use the frequency space of the photon as a pointer and perform weak coupling using electro-optics phase modulators (EOM) [70]. The weak interaction leads to a small shift in the center of the Gaussian state, which is the measure of the weak trace that the photon leaves on the ancillary system.

The experimenter in a weak measurement scenario has complete control over the size of the pre-and post-selected ensemble, the state of the pointer, and the weak measurement interaction strength; and can tune these parameters suitably so that weak values can be measured up to a desired precision. The weak nature of the measurement implies that the effects of higher powers of coupling strength κ are not recordable experimentally. In an ideal weak measurement scenario, the choice of κ and the size of the ensemble N should be such that $N\kappa^2 \to 1$ when $N \to \infty$. The ideal condition $N \to \infty$ is not feasible, therefore, the experimenter can choose κ and $N < \infty$ such that $N\kappa^2 \approx 1$ while $0 < \kappa \ll 1$ in all practical scenarios.

2.4.2 Where was the photon according to TSVF?

The story told by weak values is surprisingly different. For a single photon, preselected in input port-1 and post-selected in output port-1, the weak values of projection operators at locations of weak measurements $w_1, w_2, \cdots, w_{10}$ shown in Figure (2.2) are detailed in Equation (2.11). The values reveal that the presence of the particle was of the order of 1 at w_3, w_5, and w_7 and of the order of first or higher powers of ϵ at the rest of the locations. Particularly, for port-3 and port-4, between t_1 and t_2, at least one of the forward and backward evolving wave functions vanishes to order ϵ (see Figure (2.2) for pictorial representation). To see the contradiction between the conclusion drawn in subsection 2.3.2 and the retrodiction of TSVF, let us consider the following two cases:

Case 1: The parameter ϵ of the interferometer is tuned in such a way that $N\epsilon^2 \to 1$ when $N \to \infty$. If the experiment (as described in section 2.3) is performed on an infinitely large ensemble ($N \to \infty$), there will be no traces of ϵ^2 or higher orders in the final probability but at the same time one can record deviations of the order ϵ. Once the pre-and post-selected ensemble (which is defined by pre-and post-selection states and all the unitaries including time-varying beam-splitters $_i$) is fixed, the experimenter can deploy weak measurement schemes to investigate the past of the photons according to TSVF. The most optimal weak measurement setup requires $N\kappa^2 \to 1$ when $N \to \infty$. This amounts to $\kappa^2 \approx 0$ and we already have $\epsilon^2 \approx 0$, therefore, we conclude that $\kappa\epsilon \approx 0$, which implies that the weak traces corresponding to weak values of the order ϵ are too small to be observed (even ideally) in this case. In other words, *operational condition*, $N\epsilon^2 \to 1$ and $N\kappa^2 \to 1$ when $N \to \infty$, implies $N\kappa\epsilon \to 1$. Since the weak values of order ϵ (in this case) are not experimentally measurable, according to Equation (2.11); the photon leaves weak traces only at ports $1, 3$, and 5 with nonzero weak values $\Pi_1^w(t_4), \Pi_3^w(t_4)$, and $\Pi_5^w(t_4)$ respectively. The information about the presence of the photon in the pair of ports 3 and 4 just before L_1 is completely absent from the weak signal, which leads us to draw a conclusion on the basis of weak value-based operational definition of the past of a quantum particle: *the photon has not been in the vicinity of time-varying beam-splitter* L_1. This prediction is in direct contradiction with our earlier conclusions based on standard quantum mechanical analysis under the same approximations.

Case 2: Consider a case where the parameter ϵ of the interferometer is tuned in such a way that $N\epsilon^2 \approx 1$ for some finite N and $0 < \epsilon \ll 1$. Under these conditions, the experimenter can choose arbitrarily large ensemble $N' \gg N$ in a weak measurement setup and can easily record weak values of order ϵ. Now, for time being, imagine a situation where the experimenter chooses to perform the experiment with N systems. Although, this is not an optimal weak measurement setup, however, one can draw certain inferences based on TSVF retrodiction using the ABL rule. As we have discussed earlier, TSVF goes hand in hand with the ABL rule. ABL rule can be expressed in terms of weak values, using equations (2.1) and (2.2), as:

$$P_t(a_n|\psi_1, \psi_2) = \frac{|\Pi_{a_n}^w|^2}{\sum_i |\Pi_{a_i}^w|^2} \tag{2.13}$$

Now we ask the following question: given that the experimenter performs an experiment on a finite number of systems N such that $N\epsilon^2 \approx 1$, how many systems would have been found if the box-i were opened at some intermediate time t? The answer,

according to the ABL rule, is $NP_t(i)$, where

$$P_t(i) = \frac{|\Pi_i^w(t)|^2}{|(I-\Pi_i)^w(t)|^2 + |\Pi_i^w(t)|^2}. \tag{2.14}$$

Weak values $\{\Pi_i^w(t)\}$ presented in equation (2.11) dictate us to conclude that less than one out of N systems would have been found in boxes 3 and 4 at t_2 (in ports 3 and 4 just before L_1) if the respective boxes were opened. This leads us further to conclude that no photon was present in the vicinity of L_i if the ensemble size was N. On the other hand, equation (2.9) (more explicitly equation (2.10)) suggests that a given ensemble of N photons or a significant fraction of it (at least of order ϵN) does carry information about the time-varying element L_1. In light of S-C, one can safely conclude that one cannot claim with certainty that out of the N photons, which entered the interferometer through port-1 and were detected at output port-1, no photons (or only at most of order one) were present at L_1.

2.5 Conclusions and Discussion

The truthfulness of S-C asserts that it cannot be the case that the photon did not pass through L_1 with certainty while S-B asserts that it did not have a passage through L_1 with certainty given that the operational condition $N\kappa^2 \approx 1$ and $N\epsilon^2 \approx 1$ with $N \gg 1$ is satisfied. Even when the operational condition is not satisfied, a clear difference in the quantitative presence of photons inside the interferometer at various locations can be seen in both approaches. For instance, TSVF quantifies the presence of a particle in terms of the weak value of the position projection operator, according to which the presence of photons near L_1 is much smaller than those near L_2, L_3 and L_4; while any possible quantification of the presence based on amplitudes of oscillating terms present in equation (2.9) suggests that the presence of the particle near L_1 should be twice of its presences near L_2, L_3 and L_4.

In the language of the counterfactual ABL rule, less than one (which is zero) photon would have been detected if one had tried to detect N pre-and post-selected photons in entrance ports of L_1 indicating no presence of a photon near L_1. The contradictory conclusions inferred from two assertions imply: *at least one of S-C and S-B is false.* Since S-C is based on the fact that all the interactions in nature are local and the operational definition of the past based on weak values itself is implicitly based on S-C, one is forced to forgo S-B. This further leads us to conclude that the S-A is false *i.e.*if the weak value of a projection operator $|x\rangle\langle x|$ is zero, then it is not necessary that the particle is not present at location x. This invalidates the WVH that the weak value of an observable is the value of that observable *i.e.* if the weak value is zero then the system does not carry the corresponding property.

Since all weak value (TSVF) paradoxes are based on the correctness and rationality of WVH more specifically truthfulness of S-A, our results, therefore, have a bearing on these paradoxes. As per our conclusions, the absence of certain traces in the Danan *et al*. [69] experiment does not imply that the photon does not pass through those regions taking discontinuous trajectories to reach the detector. Similarly, zero weak values of certain observables do not imply circular polarization of a photon is separated from the wave function in the quantum Cheshire cat paradox [73]. The same is applicable to the weak value version of Hardy's paradox [57].

A natural question arises: what are weak values if not properties of systems? What do weak values tell about the properties of systems between two successive measurements? A plausible answer is given by D. Sokolovski [41]: the weak value of an observable is the transformation generated by weak measurement unitaries on the pre-selected state which reaches the post-selection. If the observable is projection operator $|a\rangle \langle a|$ then the weak value is the relative transition amplitude of pre-selected state $|\psi\rangle$ to post-selected state $|\phi\rangle$ through state $|a\rangle$.

Before concluding, we want to clarify the scope of this chapter. Our objective is not to propose a comprehensive approach for describing a particle's past but to provide a counter-example to the WVH that can be experimentally validated. Therefore, the purpose of our work is to offer empirical evidence that challenges the WVH. While our methods have been effective, we are cautious about extending their applicability beyond the experimental context presented here. Although our technique has enabled us to draw conclusions about a particle's past, even in the presence of some interference, it remains unclear whether it can consistently describe a quantum system's past in the general case. We defer further investigation of this matter, as well as the question of whether our method could provide a more accurate account of the system's past, to future studies.

To summarize our analysis, we have demonstrated that TSVF and the corresponding weak values (WVH) may not always yield accurate conclusions about the past of a quantum system. Furthermore, caution must be exercised when applying the ABL rule to analyze pre- and post-selected quantum systems and assigning probabilities to counterfactual events. Our experiment has produced measurable probability distributions from regions of the interferometer where the TSVF claims that the photon was never present or its presence was not detectable. Notably, our work presents a significant point of contention with the 'weak value trace' approach, which can be experimentally tested under the condition of 'minimal disturbance' by retaining only the first-order perturbations. Further research is necessary to determine the precise role of weak traces and the circumstances in which they offer valuable insights into particle trajectories. The prospect of conducting interferometric experiments to investigate these issues is intriguing.

Chapter 3

Weak-value formalism for mixed-states and quantum key distribution

3.1 Introduction

The weak values and weak measurement formalism were initially limited to pure states [26, 36, 42]. However, it was later extended to mixed states [103, 104, 105, 106], leading to intriguing applications in quantum information processing tasks [49, 55]. Proponents of the two-state vector formalism consider weak values as abstract properties of a physical system describing a complete picture of the system between successive measurements [28, 36, 106]. They go even further hypothesizing that the weak values are elements of the reality of weak measurements [65]. The remarkable achievements of the weak value formalism in experimental quantum mechanics have persuaded most of quantum physicists that it is impeccable. However, we explore a scenario where the formalism of weak values for mixed states is employed in a quantum communication protocol but discover that it generates inaccurate outcomes. This reinforces our previous conclusion that the weak values may not be elements of the reality of weak measurements, contrary to what the pioneers of weak values proposed [100].

In a weak measurement scenario, the displacement in the pointer state is proportional to the weak value of the observable being measured. Suppose, a pointer is prepared in a state described by a Gaussian wave packet centered at zero in the position basis as

$$\psi(x) = (2\pi\delta^2)^{-1/4} \exp\big(-x^2/4\delta^2\big). \tag{3.1}$$

The pointer then interacts with a system prepared in a mixed state ρ as per the interaction unitary $U_{BP} = \exp(-i\gamma \boldsymbol{A} \otimes \hat{p})$ where $\gamma \ll 1$, $\boldsymbol{A}$ is a system observable, and $\hat{p}$ is the momentum operator of the pointer. After the system is post-selected in state $|\phi\rangle$, the probability of finding the pointer on position x is given by

$$P(x) = (2\pi\delta^2)^{-1/2} \exp\left(-\frac{(x - \gamma \,\mathrm{Re}\{\langle \boldsymbol{A} \rangle_w\})^2}{2\delta^2} \right), \tag{3.2}$$

here, we have assumed $\gamma^2 \approx 0$ *i.e.* retained only the first-order terms in interaction strength considering the measurement to be weak. The quantity $\langle \boldsymbol{A} \rangle_w$ is the weak value of $\boldsymbol{A}$ for the system prepared in ρ and post-selected in $|\phi\rangle$. $\langle \boldsymbol{A} \rangle_w$ can be expressed explicitly as (see refs. [55, 103, 106])

$$\langle \boldsymbol{A} \rangle_w = \frac{\langle \phi | \, \boldsymbol{A} \rho \, | \phi \rangle}{\langle \phi | \, \rho \, | \phi \rangle}. \tag{3.3}$$

As we can see from Eq. (3.2) and (3.3), weak values for mixed states exhibit the same characteristics in pointer-system interaction during weak measurements as they do in the case of pure states, and therefore, the former appears to be a natural extension of the latter. This is made clear by the pioneers of the field in ref. [106]. Furthermore, the authors of ref. [106] has argued that weak values may appear as statistical averages of the pointer displacements, but in reality, their physical significance is far beyond. According to them, weak values are equivalent to eigenvalue outcomes of (weak) measurements.

This chapter thoroughly examines the role of generalized weak values in quantum information processing and identifies a potential flaw that, if overlooked, could result in misleading quantum security in a quantum key distribution protocol. Moreover, we propose a quantum state discrimination scheme that apparently can be deployed in a quantum key distribution (QKD) protocol to reduce the quantum bit error rate. We show that a trivial application of generalized weak values in such a QKD scenario leads us to devise a protocol that appears legitimate and secure according to weak value formalism, but in reality, it is not. As we will show, the misleading proof of security stems from the weak measurement approximation assumption *i.e.* neglecting the higher-order powers of the interaction strength in the calculations.

The problem of quantum state discrimination (QSD) plays an important role in QKD protocols [107, 108, 109]. In a QKD protocol, a sender (Alice) sends a system prepared in one of the several possible states to a receiver (Bob), or equivalently, she can steer the state of a system at Bob's end using nonlocal correlations. Bob's task is to guess the state with minimum error using local resources which boils down to the quantum game of state discrimination. Noisy quantum channels of communication makes information sharing vulnerable to eavesdropping [11, 110, 111]. Because of

such a noisy channel, Bob always receives the system in a mixed state even if Alice sends it in a pure state. This makes Bob's task of guessing Alice's preparation even more difficult and non-trivial. The protocol is secure if the mutual information shared by Alice and Bob is larger than the information leaked to a potential eavesdropper Eve (modeled with Eve's quantum memory) [110, 111, 112]. Security can be improved either by limiting Eve's knowledge by utilizing quantum information processing tasks or by improving Alice and Bob's correlations. The latter can be achieved by improving the state discrimination tasks on Bob's side. The probability of successful state discrimination in a minimum error discrimination (MED) strategy is strictly bounded by Helstrom-Holevo bound [113, 114]. However, it appears that the concept of weak values and weak measurements can be deployed to achieve a low error state discrimination. We deploy formalism of generalized weak values to devise a scheme for QSD that can significantly reduce the quantum bit error rate and, hence, can the increase correlation between Alice and Bob. This increases the noise tolerance–the maximum allowed noise in the channel up to which the communication is proved to be secure against collective attacks–of a protocol. Before introducing the QSD using weak values, we derive Eq. (3.3) from a purely fundamental perspective using two-state vector formalism. Furthermore, we discuss and emphasize the fact that Eq. (3.3) is indeed a legitimate generalization of weak values originally derived for pure states.

This chapter is arranged as follows: Section 3.2 presents a simple derivation for generalized weak values. Section 3.3 presents our scheme of state discrimination using weak values, and Section 3.4 describes the quantum key distribution protocol where we have employed the state-discrimination technique using weak values. The protocol is a modification of the six-state protocol [97]. In our protocol, the receiver (Bob) utilizes a weak value-based state discrimination strategy to guess the sender's (Alice) bit. Section 3.5 defines the security criteria for the protocol. In Section 3.6, we analyze the security of the protocol assuming weak measurement approximation (WMA) that the higher powers of interaction strength are negligible and can be avoided. We would like to emphasize the fact that it is the WMA because of which the displacements in the pointer state are linearly proportional to weak values. Indirectly, by assuming WMA we are accepting that the weak values truly describe elements of the reality of weak measurements. We derive expressions for joint probability distributions of Alice and Bob and estimate the quantum memory of the eavesdropper under the assumption of depolarizing quantum communication channel. We show that the use of weak values gives a higher noise tolerance in the six-state protocol (SSP). Section 3.7 presents a security analysis of the protocol without applying weak measurement approximation. Here, we show that the protocol gives no advantage over the original six-state protocol when all powers of interaction strength are retained during the key-rate calculation. In Section 3.8, we discuss the main results and their implications.

3.2 Weak value formalism for mixed states

Here, we present a derivation of weak values for mixed states using the formalism of weak values for pure states. Weak value of an observable $\boldsymbol{A}$ for a system pre-selected in state $|\psi\rangle$ and post-selected in the state $|\phi\rangle$ is given by [26]

$$\langle \boldsymbol{A} \rangle_w = \frac{\langle \phi | \boldsymbol{A} | \psi \rangle}{\langle \phi | \psi \rangle}. \tag{3.4}$$

Now, instead of pre-selection in the pure state $|\psi\rangle$, let us consider the case where the system is prepared in a mixed state $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ and post-selected in the state $|\phi\rangle$. The purification of ρ, denoted by $|\Psi\rangle$, can be given by introducing an ancillary system with eigenvectors $\{e_i\}$, as

$$|\Psi\rangle = \sum_i \sqrt{p_i} |\psi_i\rangle \otimes |e_i\rangle \tag{3.5}$$

The preparation of the system in ρ is physically equivalent to the pre-selection in the composite state $|\Psi\rangle$ of the system and the ancilla. The post-selection of the system in $|\phi\rangle$ is equivalent to performing a post-selection measurement $\mathcal{M}_{post}$, given by

$$\mathcal{M}_{post} = \{|\phi\rangle\langle\phi| \otimes \mathbb{1}, \mathbb{1} \otimes \mathbb{1} - |\phi\rangle\langle\phi| \otimes \mathbb{1}\}, \tag{3.6}$$

on the combined system and selecting outcomes corresponding to the projection $|\phi\rangle\langle\phi| \otimes \mathbb{1}$. The combined state of the system plus ancilla after the post-selection is given by

$$|\Phi\rangle = N |\phi\rangle \otimes \sum_i \sqrt{p_i} \langle \phi | \psi_i \rangle |e_i\rangle, \tag{3.7}$$

where N is a normalization factor. Since the combined system is pre-and post-selected in pure states, the weak value of $\boldsymbol{A}$ can be calculated as

$$\langle \boldsymbol{A} \rangle_w = \frac{\langle \Phi | \boldsymbol{A} \otimes \mathbb{1} | \Psi \rangle}{\langle \Phi | \Psi \rangle}. \tag{3.8}$$

Using Eqs. (3.5) and (3.7),

$$\begin{aligned} \langle \boldsymbol{A} \rangle_w &= \frac{\langle \phi | \otimes \sum_i \sqrt{p_i} \langle \psi_i | \phi \rangle \langle e_i | \sum_j \sqrt{p_j} \boldsymbol{A} |\psi_j\rangle \otimes |e_j\rangle}{\langle \phi | \otimes \sum_i \sqrt{p_i} \langle \psi_i | \phi \rangle \langle e_i | \sum_j \sqrt{p_j} |\psi_j\rangle \otimes |e_j\rangle} \\ &= \frac{\sum_i p_i \langle \psi_i | \phi \rangle \langle \phi | \boldsymbol{A} | \psi_i \rangle}{\sum_i p_i \langle \psi_i | \phi \rangle \langle \phi | \psi_i \rangle} \\ &= \frac{\langle \phi | \boldsymbol{A} \rho | \phi \rangle}{\langle \phi | \rho | \phi \rangle}. \end{aligned} \tag{3.9}$$

The interesting thing about our derivation of the generalized weak values is that it is derived without considering specifications of the pointer state, weak measurements, or using rigorous mathematics of the density matrix formalism. We have only used the two-state vector formalism that asserts that the physical properties of a system between two successive measurements are represented by Eq. (3.4). Therefore, Eq. (3.3) is a legitimate generalization of Eq. (3.4) and all implications of two state vector formalism should be applicable to mixed states also. Similar has been argued by the authors of ref. [106].

3.3 State discrimination using weak values

There are two major approaches for state discrimination: (1) minimum error discrimination (MED), where states are distinguished with a non-zero error, and (2) unambiguous discrimination (UD) in which the setup can distinguish input states with zero error but can sometimes give inconclusive answers [108, 109]. There can also be a mixture of these two strategies such that the setup discriminates input states with non-zero error and also gives inconclusive answers with some non-zero probability. In such a strategy error probability below Helstrom-Holevo bound can be achieved.

Let us now consider an example where Bob is given a task to distinguish between two Gaussian wavefunctions prepared with equal a prior probability,

$$\begin{aligned}\psi_+(x) &= (2\pi\delta^2)^{-1/4}\exp\left(-\frac{(x-\epsilon)^2}{4\delta^2}\right)\\ \psi_-(x) &= (2\pi\delta^2)^{-1/4}\exp\left(-\frac{(x+\epsilon)^2}{4\delta^2}\right)\end{aligned} \tag{3.10}$$

The minimum error in MED for uniform a prior probability is given by [109, 113, 114]

$$P_{err} = \frac{1}{2}\left(1-\sqrt{1-|\langle\psi_+|\psi_-\rangle|^2}\right) \tag{3.11}$$

Since, $\langle\psi_+|\psi_-\rangle = \int_{-\infty}^{\infty}\psi_+^*(x)\psi_-(x)dx = \exp(-\epsilon^2/2\delta^2)$, we have

$$P_{err} = \frac{1}{2}\left(1-\sqrt{1-\exp(-\epsilon^2/\delta^2)}\right) \tag{3.12}$$

Now, assume that the states given to Bob are very close to each other *i.e.* $\epsilon/\delta \ll 1$. In this case, $P_{err} \approx \frac{1}{2}(1-\epsilon/\delta)$ meaning Bob can only discriminate the given states with the probability of order $\epsilon/\delta \ll 1$ using the MED strategy. Let us now introduce a scheme to distinguish states with higher success probability, but with a cost of inconclusive results. Bob performs measurement on the particle in the position

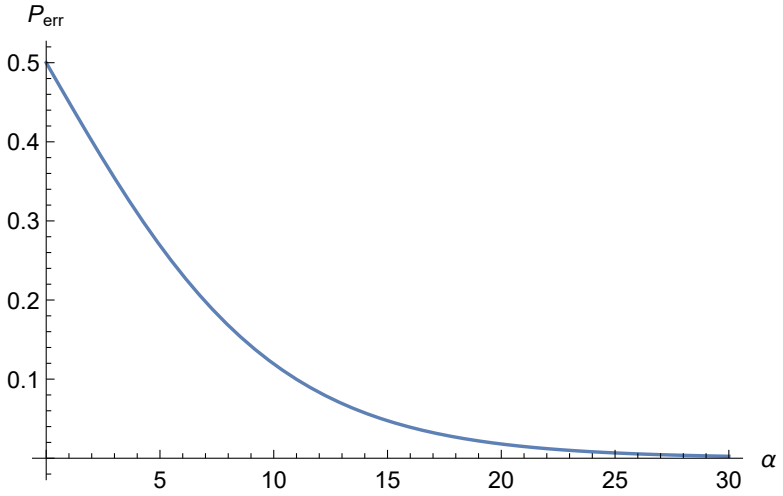


Figure 3.1: P_{err} is plotted as a function of α for $\epsilon/\delta^2 = 0.1$

basis x. If the particle is found at $x = \alpha$, the state is considered to be $|\psi_+\rangle$, and if it is found at $x = -\alpha$, the state is guessed to be $|\psi_-\rangle$ where $\alpha > 0$. The result is inconclusive if the particle is found in any other place. Bob's action can be modeled mathematically by a measurement setting $\mathcal{M} \equiv \{\Pi_+, \Pi_-, \Pi_?\}$ acting on the particle where $\Pi_+ = |\alpha\rangle\langle\alpha|$, $\Pi_- = |-\alpha\rangle\langle-\alpha|$, and $\Pi_? = \mathbb{1} - \Pi_+ - \Pi_-$. Note that outcomes corresponding to Π_+, Π_-, and $\Pi_?$ correspond to $|\psi_+\rangle$, $|\psi_-\rangle$, and inconclusive results, respectively. The probability of incorrect identification of the state conditioned on conclusive results can be evaluated as

$$\begin{aligned} P_{err} &= \frac{\langle\psi_+|\,\Pi_-\,|\psi_+\rangle + \langle\psi_-|\,\Pi_+\,|\psi_-\rangle}{\langle\psi_+|\,\Pi_-\,|\psi_+\rangle + \langle\psi_-|\,\Pi_+\,|\psi_-\rangle + \langle\psi_-|\,\Pi_-\,|\psi_-\rangle + \langle\psi_+|\,\Pi_+\,|\psi_+\rangle} \\ &= \frac{\exp(-(\alpha+\epsilon)^2/2\delta^2)}{\exp(-(\alpha+\epsilon)^2/2\delta^2) + \exp(-(\alpha-\epsilon)^2/2\delta^2)} \\ &= \frac{1}{1+\exp\left(\frac{2\alpha\epsilon}{\delta^2}\right)} \end{aligned} \tag{3.13}$$

As we can see in Figure 3.1, P_{err} decreases as α is increased for some constant ϵ/δ^2. In fact, we can achieve arbitrary low error in state discrimination for given $|\psi_+\rangle$ and $|\psi_-\rangle$ but at a cost of increased probability of inconclusive results.

Applied with weak measurements, the above strategy can be used to discriminate states in Hilbert spaces of discrete dimensions. Suppose Bob is asked to discriminate between two states $|\phi_1\rangle$ and $|\phi_2\rangle$ in Hilbert space $\mathcal{H}$ of dimension d. Bob performs weak measurement of some observable $\mathbf{A}$ of the given system using a pointer state prepared in the Gaussian state $\psi(x) = (2\pi\delta^2)^{-1/4}\exp(-x^2/4\delta^2)$ followed by post-

selection of the system in some state $|\phi\rangle$. With a suitable choice of interaction, the pointer state transforms into

$$\psi_i(x) = (2\pi\delta^2)^{-1/4} \exp\left(-\frac{(x - \gamma\,\mathrm{Re}\{\langle \boldsymbol{A}\rangle_i^w\})^2}{4\delta^2}\right) \tag{3.14}$$

where $i \in \{1, 2\}$ and $\gamma \ll 1$ is a quantification of interaction strength. $\langle \boldsymbol{A}\rangle_i^w$ is the corresponding weak value given by

$$\langle \boldsymbol{A}\rangle_i^w = \frac{\langle\phi|\,\mathbf{A}\,|\phi_i\rangle}{\langle\phi|\phi_i\rangle} \tag{3.15}$$

It is easy to verify that Bob can always choose $\mathbf{A}$ and $|\phi\rangle$ in such a manner that $\mathrm{Re}\{\langle \boldsymbol{A}\rangle_1^w\} = \beta$ and $\mathrm{Re}\{\langle \boldsymbol{A}\rangle_2^w\} = -\beta$ for some $\beta \geq 0$. Bob's action can be modeled by a quantum map $\mathcal{B}(\cdot)$ that transforms $|\phi_i\rangle$ into $\psi_i(x)$ *i.e.* $\mathcal{B}(|\phi_i\rangle) = \psi_i(x)$. Bob can now use the state discrimination strategy described above to discriminate between $\psi_1(x)$ and $\psi_2(x)$ which is equivalent to discriminating $|\phi_1\rangle$ and $|\phi_2\rangle$. The use of weak values in our approach makes mixed-state discrimination promising, which is otherwise a non-trivial and mathematically difficult problem. Suppose, Bob is given a copy of two of possible mixed states ρ_1 and ρ_2. Similar to the pure-state case, Bob can always find a suitable post-selection state and an observable $\mathbf{A}$ such that the pointer state $\psi(x)$ transforms to corresponding $\psi_i(x)$.

In a prepare-and-measure QKD protocol, Alice prepares a system in any of two pure states say $|0\rangle$ and $|1\rangle$ or in $|+\rangle$ and $|-\rangle$ with equal probability (as in BB84 protocol [10]), and sends it to Bob. Assuming the channel to be depolarizing, the sent state $|\psi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ transforms to $\rho_\psi = (1-2\eta)\,|\psi\rangle\langle\psi| + \eta\mathbb{1}$, where $\eta \in [0, 1/2]$ is the channel noise. After guessing the correct basis, Bob applies a strategy to discriminate between ρ_0 and ρ_1 (or between ρ_+ and ρ_-) for raw key generation. In BB84, Bob just measures the system in a correctly guessed preparation basis and generates the key bit with a quantum bit error rate (QBER) equal to η. In security proofs against collective attacks, the depolarizing noise η is attributed to the potential eavesdropping by Eve [2, 95, 96]. From now on, in this and the subsequent chapters, the term 'noise-tolerance' is used to mean 'tolerance of the higher QBER'. Corresponding to every QKD protocol, there is maximally tolerated channel noise η_{tol} above which the protocol is considered to be insecure. The noise tolerance of BB84 against collective attack is $\approx 11\%$, while the six-state protocol [97] has a tolerance of $\approx 12.62\%$ [11, 111].

In this chapter, first, we present a QKD protocol where Bob (the receiver) applies the above-presented quantum state discrimination strategy using weak values for mixed states. Assuming Eq. (3.3) to be a valid expression for the weak values for mixed states, and assuming the first-order approximation of weak measurements, we show that such

a QKD protocol can guarantee a secure key rate at an arbitrary high level of eavesdropping *i.e.* at an arbitrary high η_{tol}. We present an information theoretic security proof of the protocol against collective attacks while assuming the weak measurement approximation (WMA) in which higher order terms in system-pointer interaction unitary are neglected. WMA is at the center of weak measurement methodology and has been validated by various experimental demonstrations [42, 43, 49, 54]. Moreover, WMA has played an important role in studies of various quantum paradoxes and phenomena [45, 46, 48, 61, 62, 69, 74]. We then re-analyze the security of the protocol without assuming WMA *i.e.* retaining all terms in system-pointer interaction unitary. We find that the protocol does not show tolerance against arbitrary high noise levels as it appears in WMA analysis. Furthermore, it is observed that the noise tolerance is in fact not better than BB84 or six-state protocols. Our results teach us non-trivial aspects of WMA and weak values for mixed states. Contrary to what it is generally understood, the use of weak values and weak measurements can mislead into completely wrong conclusions and predictions.

3.4 QKD Protocol using weak values

Alice prepares an entangled qubit pair in state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and sends one of the qubits to Bob via a quantum channel $\mathcal{E}(\cdot)$ while keeping the other in her lab protected from any adversarial access. This step is repeated N number of times, where N is asymptotically large. For simplicity, we assume both parties have quantum memories and measurements can be postponed to the end of the state sharing step. The protocol can easily be generalized to memoryless scenarios as well.

Both parties then, agreeing over an authenticated classical communication (ACC), divide the shared pairs into two parts where one is used for parameter estimation and the second for raw key generation. The choice of whether a pair is used for parameter estimation or key generation is completely random and made after the completion of the successful sharing of systems.

Alice and Bob then use measurement settings of the six-state protocol to estimate the channel noise as a (set of) parameter(s). More specifically, they randomly measure Pauli operators σ_x, σ_y, and σ_z and estimate errors ε_x, ε_y, and ε_z, where $\varepsilon_i = P(a_i \neq b_i)$ is the probability of getting different outcomes when both parties measure the same operator σ_i, $\forall i \in \{x, y, z\}$. For depolarizing channels, $\varepsilon_x = \varepsilon_y = \varepsilon_z = \eta$ is the measure of channel noise. If $\eta \geq \eta_{tol}$, for some $0 \leq \eta_{tol} \leq 1/2$, they abort the protocol, else they continue to raw key generation from the remaining set of pairs.

Alice and Bob then execute the following steps to generate their raw keys X and Y, respectively, from the remaining set of pairs:

1: Bob prepares an ancillary system, we call it pointer here, in state $|\xi\rangle$ specified by a Gaussian wave function $\xi(x) = (2\pi\delta^2)^{-1/4}\exp(-x^2/4\delta^2)$ in position basis. He then applies the unitary $U_{BP} = \exp(-i\gamma\sigma_z \otimes \hat{p})$ on the combined state of his qubit and the pointer such that $\gamma^2/\delta^2 \ll 1$ where $\hat{p}$ is the momentum operator of the pointer.

2: Alice performs measurement of the observable σ_z on her qubit and records binary outcomes as 0 and 1 corresponding to eigenvalues $+1$ and -1, respectively.

3: Bob then post-selects his qubit in the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. The rest of the rounds, *i.e.* corresponding to Bob's outcome $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ in post-selection measurement, are discarded after agreeing over ACC.

4: Thereafter, Bob performs measurement $\mathcal{M} \equiv \{\Pi_0, \Pi_1, \Pi_?\}$ on pointer where $\Pi_0 = |\alpha\rangle\langle\alpha|$, $\Pi_1 = |-\alpha\rangle\langle-\alpha|$, and $\Pi_? = \mathbb{1} - \Pi_0 - \Pi_1$ for some $\alpha \geq 0$. Rounds corresponding to Bob's outcome $\Pi_?$ are discarded after agreeing over ACC. Bob stores outcomes corresponding to Π_0 and Π_1 as 0 and 1, respectively, and keeps them secret and protected from any adversarial access. This is Bob's raw key.

Alice and Bob now have partially secure and non-identical bit strings X and Y (raw keys), respectively, of equal length. They then proceed to perform classical error correction (EC) and privacy amplification (PA) on their raw keys to extract fully secure and completely identical keys.

3.5 Security definition

We consider security against collective attacks where the same measurement strategy is applied on independent and identically distributed (i.i.d.) quantum states and devices during every round of the protocol. Similarly, Eve can also extract information from the quantum channel by interacting with shared systems identically and independently in all rounds. Eve is always allowed to have quantum memory and can postpone her measurements to the end of classical post-processing *i.e.* EC and PA.

Let $\mathcal{H}_A$, $\mathcal{H}_B$, $\mathcal{H}_E$, and $\mathcal{H}_P$ be Hilbert spaces of Alice's system, Bob's system, Eve's quantum memory, and Bob's pointer, respectively. In each round, Alice and Bob share a bipartite state $\rho_{AB} = \mathcal{E}(|\Phi^+\rangle\langle\Phi^+|)$. Any noise introduced by channel $\mathcal{E}(\cdot)$ is attributed to Eve's attempt of eavesdropping and thus the purification of ρ_{AB} is described by a tripartite state $|\Psi\rangle_{ABE}$ distributed among Alice, Bob, and Eve. The combined state, including Bob's pointer, can be expressed (with respect to Bell basis

in $\mathcal{H}_A \otimes \mathcal{H}_B$) as

$$|\Psi\rangle_{ABEP} = \sum_{i=1}^{4} \sqrt{\lambda_i}\, |\Phi_i\rangle_{AB} \otimes |\nu_i\rangle_E \otimes |\xi\rangle_P \tag{3.16}$$

where $|\Phi_1\rangle_{AB}, |\Phi_2\rangle_{AB}, |\Phi_3\rangle_{AB}, |\Phi_4\rangle_{AB}$ are Bell states $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle$, and $|\Psi^-\rangle$, respectively, in $\mathcal{H}_A \otimes \mathcal{H}_B$ and $\{|\nu_i\rangle\}$ denotes a set of orthogonal states forming a basis in Eve's state space $\mathcal{H}_E$.

Now, suppose that Alice and Bob prepare a bipartite system in the state $|\Phi_i\rangle$ and post-select in $|\psi^a\rangle = |a\rangle \otimes |+\rangle$ where $a \in \{0, 1\}$, after weak measurement of the observable $\boldsymbol{\sigma} = \mathbb{1} \otimes \sigma_z$ using interaction unitary U_{BP}. This generates a translation in the pointer state proportional to the weak value

$$\langle \boldsymbol{\sigma}_i^a \rangle_w = \frac{\langle \psi^a | \, \boldsymbol{\sigma} \, |\Phi_i\rangle}{\langle \psi^a | \Phi_i \rangle}. \tag{3.17}$$

If the initial wave function of the pointer is $\xi(x)$, the wave function after the post-selection event can be written as

$$\xi_i^a(x) = (2\pi\delta^2)^{-1/4} \exp\left(-\frac{(x - \gamma \,\mathrm{Re}\{\langle \boldsymbol{\sigma}_i^a \rangle_w\})^2}{4\delta^2} \right), \tag{3.18}$$

for $\forall a \in \{0, 1\}$. Using Eq. (3.18), the joint state of Alice's register, Eve's memory, and Bob's pointer after the post-selection event (and tracing out Bob's qubit) is given by

$$\rho'_{AEP} = \frac{1}{2} \sum_{a \in \{0,1\}} |a\rangle\langle a|_A \otimes |\chi^a\rangle\langle\chi^a|_{EP} \tag{3.19}$$

where

$$|\chi^a\rangle_{EP} = 2 \sum_{i=1}^{4} \langle \psi^a | \Phi_i \rangle \, \sqrt{\lambda_i}\, |\nu_i\rangle_E \otimes |\xi_i^a\rangle_P \tag{3.20}$$

with $|\xi_i^a\rangle_P$ denoting the state of the pointer specified by wave function $\xi_i^a(x)$. Bob then measures the pointer in the position basis.The state after this is described by

$$\rho''_{AEP} = \frac{1}{2} \sum_{a \in \{0,1\}} |a\rangle\langle a|_A \otimes \int_{-\infty}^{+\infty} P_a(x) \rho_E^a(x) \otimes |x\rangle\langle x| \, dx. \tag{3.21}$$

Here, normalized state $\rho_E^a(x)$ denotes Eve's memory corresponding to Alice's outcome a when the pointer collapses to position eigen state $|x\rangle$, and

$$P_a(x) = (2\pi\delta^2)^{-1/2} \exp\left(-\frac{(x - \gamma \,\mathrm{Re}\{\langle \boldsymbol{\sigma}^a \rangle_w\})^2}{2\delta^2} \right) \tag{3.22}$$

denotes the probability of finding the pointer at position x conditioned on the event that Alice gets outcome a, where

$$\langle \boldsymbol{\sigma}^a \rangle_w = \frac{\langle \psi^a | \, \boldsymbol{\sigma} \rho_{AB} \, | \psi^a \rangle}{\langle \psi^a | \, \rho_{AB} \, | \psi^a \rangle} \tag{3.23}$$

is the weak value of $\boldsymbol{\sigma}$ for the pair prepared in mixed state ρ_{AB} and post-selected in $|\psi^a\rangle$ (given according to Eq. 3.3).

Let $\tilde{P}(a,0) = P_a(\alpha)$ and $\tilde{P}(a,1) = P_a(-\alpha), \forall a \in \{0,1\}$, and

$$\tilde{P} = \sum_{a,b \in \{0,1\}} \tilde{P}(a,b). \tag{3.24}$$

Then, the ccq-state describing raw key registers of Alice and Bob, and corresponding Eve's quantum memory, given that Alice and Bob discard rounds when Bob gets outcome $\Pi_?$ in measurement $\mathcal{M}$, is expressed as

$$\rho_{ABE} = \sum_{a,b \in \{0,1\}} P(a,b) \, |a\rangle\langle a|_A \otimes |b\rangle\langle b|_B \otimes \rho_E^{a,b}. \tag{3.25}$$

Here $|b\rangle\langle b|_B$ denotes the state of Bob's key bit when he gets outcome $\Pi_{b \in \{0,1\}}$. The joint probability distribution $P(a,b)$ is calculated as $P(a,b) = \tilde{P}(a,b)/\tilde{P}$, $\forall a,b \in \{0,1\}$. The state of Eve's memory conditioned on Alice's and Bob's key bits is given by

$$\rho_E^{a,b} = \rho_E^a((-1)^b \alpha), \forall a \in \{0,1\} \tag{3.26}$$

Note that $\mathrm{Tr}\left(\rho_E^{a,b}\right) = 1, \forall a,b \in \{0,1\}$.

The correlation between the raw keys of Alice and Bob is quantified using the mutual information $\mathcal{I}(A:B)$ with the joint probability distribution $P(a,b)$, and the mutual information between Alice and Eve is upper bounded by the Holevo quantity

$$\chi(A:E) = S(\Omega_E) - \frac{1}{2}\left(S(\Omega_E^0) + S(\Omega_E^1)\right), \tag{3.27}$$

where S denotes von Neumann entropy, the state

$$\Omega_E^a = \frac{P(a,0)\rho_E^{a,0} + P(a,1)\rho_E^{a,1}}{P(a,0) + P(a,1)} \tag{3.28}$$

represents Eve's quantum memory corresponding to Alice's bit a, and $\Omega_E = \left(\Omega_E^0 + \Omega_E^1\right)/2$ is Eve's partial state. The secret key rate r in asymptotic limit with one-way optimal error correction is lower bounded with Devetak-Winter rate [112],

$$r \geq \ell_{DW} = \Omega\left[\mathcal{I}(A:B) - \chi(A:E)\right] \tag{3.29}$$

where Ω is the post-selection probability. The protocol is secure when $r > 0$. The tolerable noise for secure protocol is then upper bounded by

$$\eta_{tol} = \max\{\eta | \eta \in [0, 1/2], \ell_{DW} > 0\}. \tag{3.30}$$

3.6 Security analysis with weak measurement approximation

Here we present a mathematical model of the proposed QKD protocol. Moreover, we will derive the classical-classical-quantum (ccq) state of raw key bits held by Alice and Bob, and the corresponding quantum memory of any potential adversary Eve. Since we are only considering the asymptotic case under collective attack with i.i.d. assumption, a mathematical description of only individual rounds is required at the end for the security analysis.

3.6.1 Quantum inputs and measurements

Two parties, Alice and Bob, share an entangled pair of qubits. Qubits are initially prepared in the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and then distributed to them over a quantum channel $\mathcal{E}(\cdot)$. which can introduce noise to the system transforming the pure state into a mixed state,

$$\rho_{AB} = \mathcal{E}\left(\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|\right) \tag{3.31}$$

In collective attacks, any noise introduced by the quantum channel is attributed to the potential adversary Eve. A purification $\rho_{ABE} = |\Psi_{ABE}\rangle\langle\Psi_{ABE}|$ of ρ_{AB} is used to describe the tripartite quantum state of Alice, Bob, and Eve's quantum memory. Bob then prepares an ancillary system (pointer) in state $|\xi\rangle$ with Gaussian wave function in the position basis centered at zero. The combined state is denoted $|\Psi\rangle_{ABEP} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_P \otimes \mathcal{H}_E$. With respect to Bell Basis in $\mathcal{H}_A \otimes \mathcal{H}_B$, we write

$$|\Psi\rangle_{ABPE} = \sum_{i=1}^{4} \sqrt{\lambda_i}\, |\Phi_i\rangle_{AB} \otimes |\xi\rangle_P \otimes |\nu_i\rangle_E \tag{3.32}$$

where

$$\begin{aligned}
|\Phi\rangle_1 &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\
|\Phi\rangle_2 &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\
|\Phi\rangle_3 &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\
|\Phi\rangle_4 &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned} \tag{3.33}$$

State after Bob's pre-measurement unitary U_{BP},

$$\begin{aligned}
|\Psi'\rangle &= U_{BP}\,|\Psi\rangle_{ABPE} \\
&= \sum_{i=1}^{4} \sqrt{\lambda_i} U_{BP}\left(|\Phi_i\rangle_{AB} \otimes |\xi\rangle_P\right) \otimes |\nu_i\rangle_E \\
&= \sum_{i=1}^{4} \sqrt{\lambda_i}\Big[\,|\Phi_i\rangle_{AB} \otimes |\xi\rangle_P - i\gamma\boldsymbol{\sigma}\,|\Phi_i\rangle_{AB} \otimes \hat{p}\,|\xi\rangle_P + \mathcal{O}(\gamma^2)\Big] \otimes |\nu_i\rangle_E
\end{aligned} \tag{3.34}$$

Since measurements by Alice and Bob are performed on different systems, their measurement operators commute. Consequently, the combined effect of the post-selection of Bob's qubit in state $|+\rangle$ followed by Alice's measurement

$$\mathcal{M}_A \equiv \{|0\rangle\langle 0|\,, |1\rangle\langle 1|\}$$

on her qubit can be represented by

$$\mathcal{M}(\cdot) = \frac{\sum_{a\in\{0,1\}} K_a(\cdot)K_a^\dagger}{\mathrm{Tr}\Big\{\sum_{a\in\{0,1\}} K_a(\cdot)K_a^\dagger\Big\}}, \tag{3.35}$$

where $K_a = |a\rangle\langle a|_A \otimes |+\rangle\langle +|_B \otimes \mathbb{1}_P \otimes \mathbb{1}_E$.

Let $|\psi^a\rangle = |a\rangle \otimes |+\rangle$, then

$$\begin{aligned}
K_a\,|\Psi'\rangle &= \sum_{i=1}^{4} \sqrt{\lambda_i}\Big[\,|\Phi_i\rangle_{AB} \otimes |\xi\rangle_P - i\gamma\boldsymbol{\sigma}\,|\Phi_i\rangle_{AB} \otimes \hat{p}\,|\xi\rangle_P + \mathcal{O}(\gamma^2)\Big] \otimes |\nu_i\rangle_E \\
&= \sum_{i=1}^{4} \sqrt{\lambda_i}\,|\psi^a\rangle_{AB} \otimes \Big[\,\langle\psi^a|\Phi_i\rangle\,|\xi\rangle_P - i\gamma\,\langle\psi^a|\,\boldsymbol{\sigma}\,|\Phi_i\rangle\,\hat{p}\,|\xi\rangle_P + \mathcal{O}(\gamma^2)\Big] \otimes |\nu_i\rangle_E \\
&= \sum_{i=1}^{4} \langle\psi^a|\Phi_i\rangle\,\sqrt{\lambda_i}\,|\psi^a\rangle_{AB} \otimes \Big[\,|\xi\rangle_P - i\gamma\frac{\langle\psi^a|\,\boldsymbol{\sigma}\,|\Phi_i\rangle}{\langle\psi^a|\Phi_i\rangle}\hat{p}\,|\xi\rangle_P + \mathcal{O}(\gamma^2)\Big] \otimes |\nu_i\rangle_E \\
&= \sum_{i=1}^{4} \langle\psi^a|\Phi_i\rangle\,\sqrt{\lambda_i}\,|\psi^a\rangle_{AB} \otimes \Big[\,|\xi\rangle_P - i\gamma\langle\boldsymbol{\sigma}_i^a\rangle_w\hat{p}\,|\xi\rangle_P + \mathcal{O}(\gamma^2)\Big] \otimes |\nu_i\rangle_E \\
&= |\psi^a\rangle_{AB} \otimes \sum_{i=1}^{4} \langle\psi^a|\Phi_i\rangle\,\sqrt{\lambda_i}\,|\xi_i^a\rangle_P \otimes |\nu_i\rangle_E
\end{aligned} \tag{3.36}$$

Where we have used notation $\langle\boldsymbol{\sigma}_i^a\rangle_w = \langle\psi^a|\,\boldsymbol{\sigma}\,|\Phi_i\rangle\,/\,\langle\psi^a|\Phi_i\rangle$ and

$$|\xi_i^a\rangle_P = |\xi\rangle_P - i\gamma\langle\boldsymbol{\sigma}_i^a\rangle_w\hat{p}\,|\xi\rangle_P + \mathcal{O}(\gamma^2) \tag{3.37}$$

Note that $\langle\Phi_i\,|\psi^a\rangle\langle\psi^a|\,\Phi_i\rangle = 1/4$, $\forall a \in \{0,1\}, i \in \{1,2,3,4\}$; and therefore we have $\mathrm{Tr}\big\{K_a\,|\Psi'\rangle\langle\Psi'|\,K_a^\dagger\big\} = \langle\Psi'|\,K_a\,|\Psi'\rangle = 1/4$. Consequently,

$$\mathrm{Tr}\left\{\sum_{a\in\{0,1\}} K_a\,|\Psi'\rangle\langle\Psi'|\,K_a^\dagger\right\} = 1/2,$$

and

$$\mathcal{M}\left(|\Psi'\rangle\langle\Psi'|_{ABPE}\right) = \frac{1}{2}\sum_{a\in\{0,1\}} |\psi^a\rangle\langle\psi^a|_{AB}\otimes|\chi^a\rangle\langle\chi^a|_{PE} \tag{3.38}$$

where

$$|\chi^a\rangle_{PE} = 2\sum_{i=1}^{4}\langle\psi^a|\Phi_i\rangle\,\sqrt{\lambda_i}\,|\xi_i^a\rangle_P\otimes|\nu_i\rangle_E \tag{3.39}$$

is a normalized joint state of the pointer and Eve's memory. The joint state of Alice's qubit, (Bob's) pointer, and Eve's memory after operation $\mathcal{M}(\cdot)$ and tracing out Bob's qubit (since it has been post-selected in $|+\rangle$), is given by

$$\rho'_{APE} = \frac{1}{2}\sum_{a\in\{0,1\}} |a\rangle\langle a|_A\otimes|\chi^a\rangle\langle\chi^a|_{PE} \tag{3.40}$$

Measurement on the pointer in position basis is modeled by a completely positive trace preserving (CPTP) map

$$\mathcal{X}(\cdot) = \int_{-\infty}^{+\infty}\Big(\mathbb{1}_A\otimes|x\rangle\langle x|_P\otimes\mathbb{1}_E\Big)(\cdot)\Big(\mathbb{1}_A\otimes|x\rangle\langle x|_P\otimes\mathbb{1}_E\Big)^\dagger dx. \tag{3.41}$$

Therefore, the state after measurement on the pointer is

$$\rho''_{APE} = \frac{1}{2}\sum_{a\in\{0,1\}} |a\rangle\langle a|_A\otimes\int_{-\infty}^{+\infty}\Big(|x\rangle\langle x|_P\otimes\mathbb{1}_E\Big)\,|\chi^a\rangle\langle\chi^a|_{PE}\,\Big(|x\rangle\langle x|_P\otimes\mathbb{1}_E\Big)^\dagger dx \tag{3.42}$$

Using Eq. (3.39),

$$|x\rangle\langle x|_P\otimes\mathbb{1}_E\,|\chi^a\rangle_{PE} = 2\sum_{i=1}^{4}\sqrt{\lambda_i}\,\langle\psi^a|\Phi_i\rangle\,\langle x|\xi_i^a\rangle\,|x\rangle_P\otimes|\nu_i\rangle_E \tag{3.43}$$

That gives

$$\begin{aligned}\rho_x &= \Big(|x\rangle\langle x|_P\otimes\mathbb{1}_E\Big)\,|\chi^a\rangle\langle\chi^a|_{PE}\,\Big(|x\rangle\langle x|_P\otimes\mathbb{1}_E\Big)^\dagger\\ &= |x\rangle\langle x|_E\otimes\Big(4\sum_{i=1}^{4}\sum_{j=1}^{4}\sqrt{\lambda_i\lambda_j}\,\langle\psi^a|\Phi_i\rangle\,\langle\Phi_j|\psi^a\rangle\,\langle x|\xi_i^a\rangle\,\langle\xi_j^a|x\rangle\,|\nu_i\rangle\langle\nu_j|_E\Big)\\ &= |x\rangle\langle x|_P\otimes\tilde{\rho}_E^a(x)\end{aligned} \tag{3.44}$$

Note that $\tilde{\rho}_E^a(x)$ is un-normalized. Let

$$P_a(x) = \mathrm{Tr}\Big\{ \Big(|x\rangle\langle x|_P \otimes \mathbb{1}_E \Big) |\chi^a\rangle\langle\chi^a|_{PE} \Big(|x\rangle\langle x|_P \otimes \mathbb{1}_E \Big)^\dagger \Big\}$$

and $\rho_E^a(x) = \tilde{\rho}_E^a(x)/P_a(x)\ \forall a \in \{0,1\}$. Here state $\rho_E^a(x)$ is normalized *i.e.* $\mathrm{Tr}\{\rho_E^a(x)\} = 1$. Now, we can re-write Eq. (3.42) as

$$\rho''_{APE} = \frac{1}{2} \sum_{a\in\{0,1\}} |a\rangle\langle a|_A \otimes \int_{-\infty}^{+\infty} P_a(x) \, |x\rangle\langle x|_P \otimes \rho_E^a(x) dx \tag{3.45}$$

Bob then registers his key bit as $b = 0$ if measurement on the pointer gives outcome $x = \alpha$, and $b = 1$ if it gives outcome $x = -\alpha$ for some $\alpha > 0$. Else, Bob discards the round and broadcast it to Alice so that she can also discard the corresponding bit. This action can be modeled by a CPTP map $\mathcal{B}_{P\to B}(\cdot)$ followed by a projection $\Pi = |0\rangle\langle 0|_B + |1\rangle\langle 1|_B$. Map $\mathcal{B}_{P\to B}(\cdot)$ is specified as,

$$\mathcal{B}_{P\to B}(|x\rangle\langle x|) = \begin{cases} |0\rangle\langle 0| & \text{if} \quad x = \alpha \\ |1\rangle\langle 1| & \text{if} \quad x = -\alpha \\ |\varnothing\rangle\langle\varnothing| & \text{else} \end{cases} \tag{3.46}$$

where $\{|i\rangle\}_{i\in\{0,1,\varnothing\}}$ forms a set of orthogonal states. Consequently, we have

$$\begin{aligned} \Omega'_{ABE} &= \mathcal{B}_{P\to B}(\rho''_{APE}) \\ &= \frac{1}{2} \sum_{a\in\{0,1\}} |a\rangle\langle a|_A \otimes \Big[|0\rangle\langle 0|_B \otimes P_a(\alpha)\rho_E^a(\alpha) \\ &+ |1\rangle\langle 1|_B \otimes P_a(-\alpha)\rho_E^a(-\alpha) + |\varnothing\rangle\langle\varnothing|_B \otimes \int_{x\notin\{\alpha,-\alpha\}} P_a(x)\rho_E^a(x)dx \Big] \end{aligned} \tag{3.47}$$

After applying Π *i.e.* discarding rounds corresponding to $|\varnothing\rangle\langle\varnothing|_B$,

$$\begin{aligned} \Omega''_{ABE} &= \Pi\Omega'_{ABE}\Pi^\dagger \\ &= \frac{1}{2} \sum_{a\in\{0,1\}} |a\rangle\langle a|_A \otimes \Big[|0\rangle\langle 0|_B \otimes P_a(\alpha)\rho_E^a(\alpha) + |1\rangle\langle 1|_B \otimes P_a(-\alpha)\rho_E^a(-\alpha) \Big] \\ &= \frac{1}{2} \sum_{a\in\{0,1\}} |a\rangle\langle a|_A \otimes \Big[\tilde{P}(a,0) \, |0\rangle\langle 0|_B \otimes \rho_E^{a,0} + \tilde{P}(a,1) \, |1\rangle\langle 1|_B \otimes \rho_E^{a,1} \Big] \\ &= \frac{1}{2} \sum_{a,b\in\{0,1\}} \tilde{P}(a,b) \, |a\rangle\langle a|_A \otimes |b\rangle\langle b|_B \otimes \rho_E^{a,b}. \end{aligned} \tag{3.48}$$

where we have used notations $\tilde{P}(a,0) = P_a(\alpha)$, $\tilde{P}(a,1) = P_a(-\alpha)$, $\rho_E^{a,0} = \rho_E^a(\alpha)$, $\rho_E^{a,1} = \rho_E^a(-\alpha)$. Note that $\rho_E^{a,b}$ is a normalized state of Eve's memory corresponding to the bit pair (a,b) of Alice and Bob. The state Ω''_{ABE}, given in Eq. (3.48), is not yet normalized. Let us denote the corresponding normalized state by $\Omega_{ABE} = \Omega''_{ABE}/\operatorname{Tr}\{\Omega''_{ABE}\}$, then with the notation,

$$P(a,b) = \frac{\tilde{P}(a,b)}{\sum_{a,b\in\{0,1\}} \tilde{P}(a,b)} \tag{3.49}$$

we have

$$\Omega_{ABE} = \sum_{a,b\in\{0,1\}} P(a,b)\, |a\rangle\langle a|_A \otimes |b\rangle\langle b|_B \otimes \rho_E^{a,b}. \tag{3.50}$$

3.6.2 Joint probability distribution of Alice and Bob

In Eq. (3.50), $P(a,b)$ denotes the joint probability distribution of raw key bits a and b of Alice and Bob, respectively. $P(a,b)$ can be numerically computed if the expression for $P_a(x)$ is known $\forall a \in \{0,1\}$. Here we derive the expression for $P_a(x)$. We have

$$\begin{aligned} P_a(x) &= \operatorname{Tr}\Big\{ \Big(|x\rangle\langle x|_P \otimes \mathbb{1}_E \Big) |\chi^a\rangle\langle\chi^a|_{PE} \Big(|x\rangle\langle x|_P \otimes \mathbb{1}_E \Big)^\dagger \Big\} \\ &= 4 \sum_{i=1}^{4} \lambda_i \, \langle\psi^a|\Phi_i\rangle \, \langle\Phi_i|\psi^a\rangle \, \langle x|\xi_i^a\rangle \, \langle\xi_i^a|x\rangle \\ &= 4 \sum_{i=1}^{4} \lambda_i \| \, \langle\psi^a|\Phi_i\rangle \, \xi_i^a(x)\|^2, \end{aligned} \tag{3.51}$$

we have used Eq. (3.39) here. Let us now evaluate an expression for $\xi_i^a(x) = \langle x|\xi_i^a\rangle$. We have

$$\begin{aligned} |\xi_i^a\rangle &= \Big(\mathbb{1} - i\gamma \langle \boldsymbol{\sigma}_i^a \rangle_w \hat{p} + \mathcal{O}(\gamma^2) \Big) \int_{-\infty}^{+\infty} |x\rangle \, \langle x|\xi\rangle \, dx \\ &\approx \int_{-\infty}^{+\infty} \exp(-i\gamma \langle \boldsymbol{\sigma}_i^a \rangle_w \hat{p}) \, |x\rangle \, \langle x|\xi\rangle \, dx \\ &= \int_{-\infty}^{+\infty} |x + \gamma \operatorname{Re}\{\langle \boldsymbol{\sigma}_i^a \rangle_w\}\rangle \, \langle x|\xi\rangle \, dx, \end{aligned} \tag{3.52}$$

Using $\langle x|\xi\rangle = \xi_i^a(x) = (2\pi\delta^2)^{-1/4} \exp\left(-x^2/4\delta^2\right)$, we have

$$\xi_i^a(x) \approx (2\pi\delta^2)^{-1/4} \exp\left(-\frac{(x - \gamma \operatorname{Re}\{\langle \boldsymbol{\sigma}_i^a \rangle_w\})^2}{4\delta^2} \right). \tag{3.53}$$

Assuming $\gamma^2/\delta^2 \ll 1$, Eq. (3.51) can be re-written as

$$\begin{aligned}
P_a(x) &= 4(2\pi\delta^2)^{-1/2}\sum_{i=1}^{4}\lambda_i \| \langle\psi^a|\Phi_i\rangle \|^2 \exp\left(-\frac{(x-\gamma\,\mathrm{Re}\{\langle\boldsymbol{\sigma}_i^a\rangle_w\})^2}{2\delta^2}\right) \\
&\approx 4(2\pi\delta^2)^{-1/2}\sum_{i=1}^{4}\lambda_i \| \langle\psi^a|\Phi_i\rangle \|^2 \exp\left(-\frac{x^2}{2\delta^2}\right)\exp\left(\frac{\gamma\,\mathrm{Re}\{\langle\boldsymbol{\sigma}_i^a\rangle_w\}}{\delta^2}x\right) \\
&= 4\|\xi(x)\|^2\sum_{i=1}^{4}\lambda_i \| \langle\psi^a|\Phi_i\rangle \|^2 \left(1+\frac{\gamma}{\delta^2}\,\mathrm{Re}\{\langle\boldsymbol{\sigma}_i^a\rangle_w\}x+\mathcal{O}(\gamma^2)\right) \\
&= 4\|\xi(x)\|^2\sum_{i=1}^{4}\lambda_i \| \langle\psi^a|\Phi_i\rangle \|^2 \left(1+\frac{\gamma}{\delta^2}\,\mathrm{Re}\left\{\frac{\sum_{i=1}^{4}\lambda_i \| \langle\psi^a|\Phi_i\rangle \|^2\langle\boldsymbol{\sigma}_i^a\rangle_w}{\sum_{i=1}^{4}\lambda_i \| \langle\psi^a|\Phi_i\rangle \|^2}\right\}x+\mathcal{O}(\gamma^2)\right)
\end{aligned} \tag{3.54}$$

Note that

$$\sum_{i=1}^{4}\lambda_i \| \langle\psi^a|\Phi_i\rangle \|^2 = \langle\psi^a|\,\rho_{AB}\,|\psi^a\rangle$$

and

$$\sum_{i=1}^{4}\lambda_i \| \langle\psi^a|\Phi_i\rangle \|^2\langle\boldsymbol{\sigma}_i^a\rangle_w = \langle\psi^a|\,\boldsymbol{\sigma}\rho_{AB}\,|\psi^a\rangle\,.$$

Now, let $\langle\boldsymbol{\sigma}^a\rangle_w = \langle\psi^a|\,\boldsymbol{\sigma}\rho_{AB}\,|\psi^a\rangle \,/\, \langle\psi^a|\,\rho_{AB}\,|\psi^a\rangle$, then

$$\begin{aligned}
P_a(x) &= 4\|\xi(x)\|^2\sum_{i=1}^{4}\lambda_i \| \langle\psi^a|\Phi_i\rangle \|^2 \left(1+\frac{\gamma}{\delta^2}\,\mathrm{Re}\{\langle\boldsymbol{\sigma}^a\rangle_w\}x+\mathcal{O}(\gamma^2)\right) \\
&\approx 4(2\pi\delta^2)^{-1/2}\exp\left(-\frac{(x-\gamma\,\mathrm{Re}\{\langle\boldsymbol{\sigma}^a\rangle_w\})^2}{2\delta^2}\right)\sum_{i=1}^{4}\lambda_i \| \langle\psi^a|\Phi_i\rangle \|^2
\end{aligned} \tag{3.55}$$

Since $\| \langle\psi^a|\Phi_i\rangle \| = 1/4$, $\forall a \in \{0,1\}$ and $i \in \{1,2,3,4\}$, we have

$$P_a(x) = (2\pi\delta^2)^{-1/2}\exp\left(-\frac{(x-\gamma\,\mathrm{Re}\{\langle\boldsymbol{\sigma}^a\rangle_w\})^2}{2\delta^2}\right). \tag{3.56}$$

3.6.3 Joint probability distribution for depolarizing channels

Here we evaluate an expression for the joint probability distribution of Alice and Bob under the usual assumption of depolarizing quantum communication channel $\mathcal{E}(\cdot)$. More specifically, we give expressions for weak values $\langle\sigma^a\rangle_w$ $\forall a \in \{0,1\}$ and corresponding $P_a(x)$. If $\mathcal{E}(\cdot)$ is a depolarizing channel, we have $\lambda_1 = 1-3\eta/2$, and $\lambda_2 = \lambda_3 = \lambda_4 = \eta/2$, where $\eta = \varepsilon_x = \varepsilon_y = \varepsilon_z$, specified in the main text, is the

parameter quantifying channel noise. Therefore, $\rho_{AB} = (1-2\eta)\left|\Phi_1\right\rangle\!\left\langle\Phi_1\right|_{AB} + \frac{\eta}{2}\mathbb{1}_{AB}$ and consequently, we have

$$\begin{aligned}\langle\sigma^a\rangle_w &= \frac{\langle\psi^a|\,\boldsymbol{\sigma}\rho_{AB}\,|\psi^a\rangle}{\langle\psi^a|\,\rho_{AB}\,|\psi^a\rangle} \\ &= \frac{(1-2\eta)\,\langle\psi^a|\,\boldsymbol{\sigma}\,|\Phi_1\rangle\!\langle\Phi_1|\,\psi^a\rangle + \frac{\eta}{2}\,\langle\psi^a|\,\boldsymbol{\sigma}\,|\psi^a\rangle}{(1-2\eta)\langle\psi^a\,|\Phi_1\rangle\!\langle\Phi_1|\,\psi^a\rangle + \frac{\eta}{2}}.\end{aligned} \tag{3.57}$$

Since, $\langle\psi^a|\,\boldsymbol{\sigma}\,|\psi^a\rangle = 0$ and $\langle\psi^a\,|\Phi_1\rangle\!\langle\Phi_1|\,\psi^a\rangle = 1/4$ for $a \in \{0,1\}$, and $\langle\boldsymbol{\sigma}_i^a\rangle_w = \langle\psi^a|\,\boldsymbol{\sigma}\,|\Phi_i\rangle \,/\, \langle\psi^a|\Phi_i\rangle$, we can write

$$\langle\sigma^a\rangle_w = \frac{\langle\boldsymbol{\sigma}_1^a\rangle_w}{1+\frac{2\eta}{1-2\eta}}. \tag{3.58}$$

Note that $\langle\boldsymbol{\sigma}_1^a\rangle_w = (-1)^a$, $\forall a \in \{0,1\}$. Hence,

$$\langle\sigma^a\rangle_w = (-1)^a(1-2\eta) \tag{3.59}$$

In light of Eq. (3.59), we can re-write Eq. (3.56) as

$$P_a(x) = (2\pi\delta^2)^{-1/2}\exp\left(-\frac{(x-(-1)^a(1-2\eta)\gamma)^2}{2\delta^2}\right). \tag{3.60}$$

Using Eq. (3.60), $\tilde{P}(a,b)$ can be expressed as

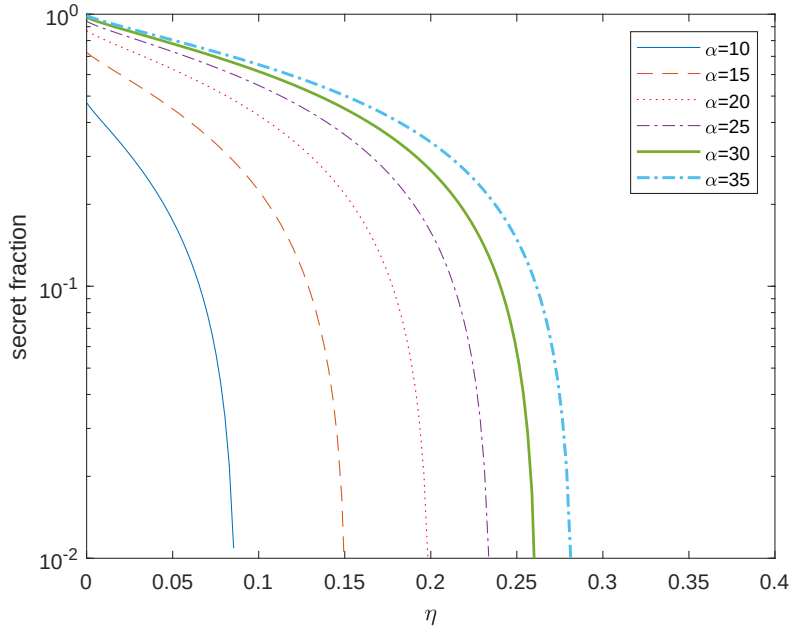
$$\begin{aligned}\tilde{P}(0,0) = \tilde{P}(1,1) &= (2\pi\delta^2)^{-1/2}\exp\left(-\frac{(\alpha-(1-2\eta)\gamma)^2}{2\delta^2}\right), \\ \tilde{P}(0,1) = \tilde{P}(1,0) &= (2\pi\delta^2)^{-1/2}\exp\left(-\frac{(\alpha+(1-2\eta)\gamma)^2}{2\delta^2}\right),\end{aligned} \tag{3.61}$$

Using Eq. (3.49), we can write joint probability distributions of Alice and Bob as

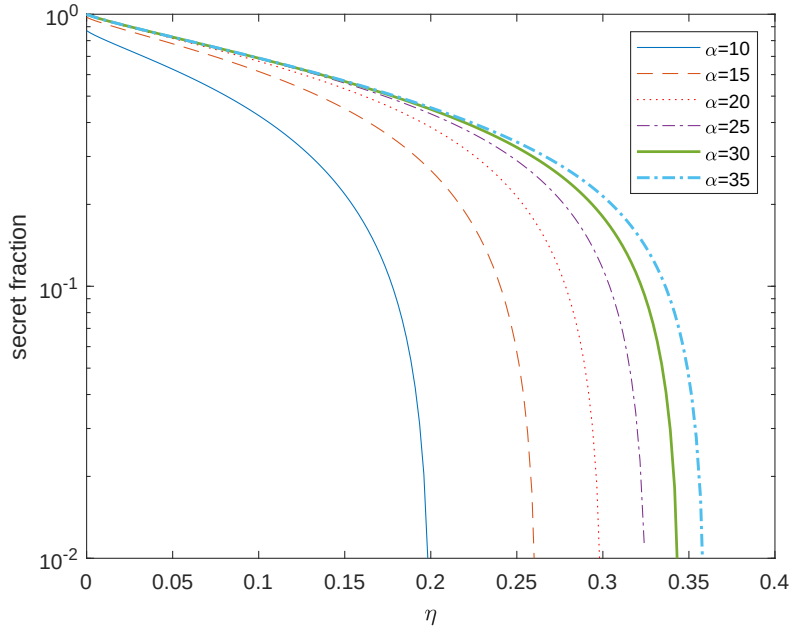
$$P(a,b) = \begin{cases} \frac{1}{2\left(1+\exp\left(-\frac{2(1-2\eta)\gamma\alpha}{\delta^2}\right)\right)} & \text{if} \quad a=b \\ \frac{1}{2\left(1+\exp\left(\frac{2(1-2\eta)\gamma\alpha}{\delta^2}\right)\right)} & \text{if} \quad a\neq b \end{cases} \tag{3.62}$$

Therefore, the raw key-bit error rate $Q = P(a \neq b) = P(0,1) + P(1,0)$, *i.e.* the probability that both parties guess different key bits, is given by

$$Q = \frac{1}{\left(1+\exp\left(\frac{2(1-2\eta)\gamma\alpha}{\delta^2}\right)\right)} \tag{3.63}$$



(a)



(b)

Figure 3.2: Secret key fraction according to weak measurement approximation. The secret fraction is plotted as a function of depolarizing noise η for (a) $\alpha = 0.1$ and (b) $\alpha = 0.2$.

3.6.4 State of Eve's memory and her side information

In order to calculate $\rho_E^{a,b}$, we first need to find $\rho_E^a(x)$ which is given by (see Eq. (3.44) and (3.45))

$$\rho_E^a(x) = \frac{4}{P_a(x)} \sum_{i=1}^{4} \sum_{j=1}^{4} \sqrt{\lambda_i \lambda_j}\, \langle \psi^a | \Phi_i \rangle \, \langle \Phi_j | \psi^a \rangle \, \langle x | \xi_i^a \rangle \, \langle \xi_j^a | x \rangle \, |\nu_i\rangle\langle \nu_j|_E \tag{3.64}$$

Note that $\langle \boldsymbol{\sigma}_1^0 \rangle_w = \langle \boldsymbol{\sigma}_2^0 \rangle_w = \langle \boldsymbol{\sigma}_3^1 \rangle_w = \langle \boldsymbol{\sigma}_4^1 \rangle_w = 1$ and $\langle \boldsymbol{\sigma}_1^1 \rangle_w = \langle \boldsymbol{\sigma}_2^1 \rangle_w = \langle \boldsymbol{\sigma}_3^0 \rangle_w = \langle \boldsymbol{\sigma}_4^0 \rangle_w = -1$. Let us denote $\langle x | \xi_i^a \rangle = \xi^+(x)$ if $\langle \boldsymbol{\sigma}_i^0 \rangle_w = 1$ and $\langle x | \xi_i^a \rangle = \xi^-(x)$ if $\langle \boldsymbol{\sigma}_i^0 \rangle_w = -1$ for all $a \in \{0,1\}$ and $i \in \{1,2,3,4\}$. Clearly,

$$\xi^{\pm}(x) = (2\pi\delta^2)^{-1/4} \exp\left(-\frac{(x \mp \gamma)^2}{4\delta^2} \right). \tag{3.65}$$

For the case of depolarizing noise, we have $\lambda_1 = 1 - 3\eta/2$ and $\lambda_2 = \lambda_3 = \lambda_4 = \eta/2$. Note that $\xi^+(x)\xi^-(x) = \|\xi(x)\|^2 \exp(-\gamma^2/2\delta^2) \approx \|\xi(x)\|^2$. Therefore, after denoting $\kappa = \sqrt{\left(1 - \frac{3\eta}{2}\right) \frac{\eta}{2}}$, we can express $\rho_E^a(x)$ in matrix form as

$$\rho_E^0(x) = \tfrac{1}{P_0(x)} \begin{pmatrix} \left(1 - \frac{3\eta}{2}\right) \|\xi^+(x)\|^2 & \kappa \|\xi^+(x)\|^2 & \kappa \|\xi(x)\|^2 & \kappa \|\xi(x)\|^2 \\ \kappa \|\xi^+(x)\|^2 & \frac{\eta}{2} \|\xi^+(x)\|^2 & \frac{\eta}{2} \|\xi(x)\|^2 & \frac{\eta}{2} \|\xi(x)\|^2 \\ \kappa \|\xi(x)\|^2 & \frac{\eta}{2} \|\xi(x)\|^2 & \frac{\eta}{2} \|\xi^-(x)\|^2 & \frac{\eta}{2} \|\xi^-(x)\|^2 \\ \kappa \|\xi(x)\|^2 & \frac{\eta}{2} \|\xi(x)\|^2 & \frac{\eta}{2} \|\xi^-(x)\|^2 & \frac{\eta}{2} \|\xi^-(x)\|^2 \end{pmatrix},$$

$$\rho_E^1(x) = \tfrac{1}{P_1(x)} \begin{pmatrix} \left(1 - \frac{3\eta}{2}\right) \|\xi^-(x)\|^2 & -\kappa \|\xi^-(x)\|^2 & \kappa \|\xi(x)\|^2 & -\kappa \|\xi(x)\|^2 \\ -\kappa \|\xi^-(x)\|^2 & \frac{\eta}{2} \|\xi^-(x)\|^2 & -\frac{\eta}{2} \|\xi(x)\|^2 & \frac{\eta}{2} \|\xi(x)\|^2 \\ \kappa \|\xi(x)\|^2 & -\frac{\eta}{2} \|\xi(x)\|^2 & \frac{\eta}{2} \|\xi^+(x)\|^2 & -\frac{\eta}{2} \|\xi^+(x)\|^2 \\ -\kappa \|\xi(x)\|^2 & \frac{\eta}{2} \|\xi(x)\|^2 & -\frac{\eta}{2} \|\xi^+(x)\|^2 & \frac{\eta}{2} \|\xi^+(x)\|^2 \end{pmatrix}, \tag{3.66}$$

Eve's memory corresponding to the Alice bit a, say Ω_E^a, is calculated by applying $|a\rangle\langle a|_A \otimes \mathbb{1}_B \otimes \mathbb{1}_E$ on Ω_{ABE} and then tracing out classical bits of Alice and Bob,

$$\Omega_E^a = \mathrm{Tr}_{AB} \Big((|a\rangle\langle a|_A \otimes \mathbb{1}_B \otimes \mathbb{1}_E) \Omega_{ABE} (|a\rangle\langle a|_A \otimes \mathbb{1}_B \otimes \mathbb{1}_E) \Big) \tag{3.67}$$

From Eq. (3.50), we have

$$\begin{aligned}\Omega_E^0 &= P(0,0)\rho_E^{0,0} + P(0,1)\rho_E^{0,1} \\ \Omega_E^1 &= P(1,0)\rho_E^{1,0} + P(1,1)\rho_E^{1,1}\end{aligned} \tag{3.68}$$

After normalization and using the fact that $Q = 2P(0,1) = 2P(1,0)$ and $1-Q = 2P(0,0) = 2P(1,1)$,

$$\begin{aligned}\Omega_E^0 &= (1-Q)\rho_E^{0,0} + Q\rho_E^{0,1} \\ \Omega_E^1 &= (1-Q)\rho_E^{1,1} + Q\rho_E^{1,0}\end{aligned} \tag{3.69}$$

States $\rho_E^{a,b}, \forall a, b \in \{0,1\}$ can be calculated numerically using Eq. (3.26) and (3.66).

3.6.5 Secure key rate and the noise tolerance

In subsections 3.6.3 and 3.6.4, we have calculated joint probability distribution and estimated Eve's memory for collective attacks. The secret fraction (F_{sec}) of raw keys generated by Alice and Bob can be calculated using the Devetak-Winter rate (Eq. (3.29)), as

$$F_{sec} = \mathcal{I}(A:B) - \chi(A:E). \tag{3.70}$$

The mutual entropy for the joint probability distribution given by Eq. (3.62) is calculated numerically using

$$\mathcal{I}(A:B) = 1 - h(Q) \tag{3.71}$$

where $h(Q) = -Q\log_2(Q) - (1-Q)\log_2(1-Q)$ is the binary Shannon entropy for bit error rate Q given by Eq. 3.63. Holevo quantity $\chi(A:E)$ (given by Eq. (3.27)) is numerically calculated using Eq. (3.69). We computed the secret fraction of the raw keys with weak measurement approximations for different values of α and γ. The results are plotted in Figure 3.2. A positive key rate can be achieved at a high noise rate (quantified by η which is also QBER for the six-state protocol). We see that the protocol can be secure even at 35% QBER by choosing the appropriate α. Such a protocol seems to have improved noise tolerance drastically. As we will see, the above results are wrong and the increased noise tolerance is just a consequence of neglecting higher power terms in the calculations. We re-analyze the security in the next section.

3.7 Security analysis without weak measurement approximation

In the previous section, we have calculated the secret fraction assuming weak measurement approximation. Here, we re-analyze the security of the protocol without as-

suming the weak measurement approximation *i.e.* retaining all powers of interaction strength in calculations.

The state after applying U_{BP} on $|\Psi_{ABPE}\rangle$ (Eq. (3.34)) can be written without approximation as

$$\begin{aligned}|\Psi'\rangle &= U_{BP}\,|\Psi\rangle_{ABPE} \\ &= \sum_{i=1}^{4}\sqrt{\lambda_i}U_{BP}\left(|\Phi_i\rangle_{AB}\otimes|\xi\rangle_P\right)\otimes|\nu_i\rangle_E \\ &= \sum_{i=1}^{4}\sqrt{\lambda_i}\Big[\,|\Phi_i\rangle_{AB}\otimes\cos(\gamma\hat{p})\,|\xi\rangle_P - i\boldsymbol{\sigma}\,|\Phi_i\rangle_{AB}\otimes\sin(\gamma\hat{p})\,|\xi\rangle_P\,\Big]\otimes|\nu_i\rangle_E\end{aligned} \tag{3.72}$$

The state of the pointer corresponding to Alice's bit a and Bell state $|\Phi_i\rangle$ can be expressed without approximation as

$$|\xi_i^a\rangle_P = \exp(-i\langle\boldsymbol{\sigma}_i^a\rangle_w\gamma\hat{p})\,|\xi\rangle_P \tag{3.73}$$

The mathematical expression for ccq-state remains the same as calculated for weak measurement approximation given by Eq. (3.50).

3.7.1 Joint probability distribution of Alice and Bob

The joint probability distribution of Alice and Bob can be calculated numerically using $P_a(x)$, which without approximation is given by

$$\begin{aligned}P_a(x) &= \mathrm{Tr}\Big\{\Big(\,|x\rangle\langle x|_P\otimes\mathbb{1}_E\Big)\,|\chi^a\rangle\langle\chi^a|_{PE}\,\Big(\,|x\rangle\langle x|_P\otimes\mathbb{1}_E\Big)^\dagger\Big\} \\ &= 4\sum_{i=1}^{4}\lambda_i\,\langle\psi^a|\Phi_i\rangle\,\langle\Phi_i|\psi^a\rangle\,\langle x|\xi_i^a\rangle\,\langle\xi_i^a|x\rangle \\ &= \sum_{i=1}^{4}\lambda_i\|\xi_i^a(x)\|^2,\end{aligned} \tag{3.74}$$

Let us now evaluate an expression for $\xi_i^a(x) = \langle x|\xi_i^a\rangle$. From Eq. (3.73), we have

$$\begin{aligned}|\xi_i^a\rangle &= \exp(-i\gamma\langle\boldsymbol{\sigma}_i^a\rangle_w\hat{p})\int_{-\infty}^{+\infty}|x\rangle\,\langle x|\xi\rangle\,dx \\ &= \int_{-\infty}^{+\infty}|x+\gamma\langle\boldsymbol{\sigma}_i^a\rangle_w\rangle\,\langle x|\xi\rangle\,dx,\end{aligned} \tag{3.75}$$

Since $\langle x|\xi\rangle = \xi(x) = (2\pi\delta^2)^{-1/4}\exp\left(-x^2/4\delta^2\right)$, we have

$$\xi_i^a(x) = (2\pi\delta^2)^{-1/4}\exp\left(-\frac{\left(x-\gamma\langle\boldsymbol{\sigma}_i^a\rangle_w\right)^2}{4\delta^2}\right). \tag{3.76}$$

Eq. (3.74) can be re-written as

$$P_a(x) = (2\pi\delta^2)^{-1/2}\sum_{i=1}^{4}\lambda_i\exp\left(-\frac{\left(x-\gamma\langle\boldsymbol{\sigma}_i^a\rangle_w\right)^2}{2\delta^2}\right). \tag{3.77}$$

Since $\langle\boldsymbol{\sigma}_1^0\rangle_w = \langle\boldsymbol{\sigma}_2^0\rangle_w = \langle\boldsymbol{\sigma}_3^1\rangle_w = \langle\boldsymbol{\sigma}_4^1\rangle_w = 1$ and $\langle\boldsymbol{\sigma}_1^1\rangle_w = \langle\boldsymbol{\sigma}_2^1\rangle_w = \langle\boldsymbol{\sigma}_3^0\rangle_w = \langle\boldsymbol{\sigma}_4^0\rangle_w = -1$, we can write

$$\begin{aligned}
P_0(x) &= (2\pi\delta^2)^{-1/2}\left[(\lambda_1+\lambda_2)\exp\left(-\frac{(x-\gamma)^2}{2\delta^2}\right)+(\lambda_3+\lambda_4)\exp\left(-\frac{(x+\gamma)^2}{2\delta^2}\right)\right],\\
P_1(x) &= (2\pi\delta^2)^{-1/2}\left[(\lambda_1+\lambda_2)\exp\left(-\frac{(x+\gamma)^2}{2\delta^2}\right)+(\lambda_3+\lambda_4)\exp\left(-\frac{(x-\gamma)^2}{2\delta^2}\right)\right].
\end{aligned} \tag{3.78}$$

Let us now denote

$$\xi^{\pm}(x) = (2\pi\delta^2)^{-1/4}\exp\left(-\frac{(x\mp\gamma)^2}{4\delta^2}\right). \tag{3.79}$$

Using Eq. (3.79), Eq. (3.78) is re-written as

$$\begin{aligned}
P_0(x) &= (\lambda_1+\lambda_2)\|\xi^+(x)\|^2+(\lambda_3+\lambda_4)\|\xi^-(x)\|^2,\\
P_1(x) &= (\lambda_1+\lambda_2)\|\xi^-(x)\|^2+(\lambda_3+\lambda_4)\|\xi^+(x)\|^2.
\end{aligned} \tag{3.80}$$

Remember that $\tilde{P}(a,b) = P_a((-1)^b\alpha)$. Using Eqs. (3.80), we can now express $\tilde{P}(a,b)$ as

$$\begin{aligned}
\tilde{P}(0,0) &= (\lambda_1+\lambda_2)\|\xi^+(\alpha)\|^2+(\lambda_3+\lambda_4)\|\xi^-(\alpha)\|^2,\\
\tilde{P}(0,1) &= (\lambda_1+\lambda_2)\|\xi^+(-\alpha)\|^2+(\lambda_3+\lambda_4)\|\xi^-(-\alpha)\|^2,\\
\tilde{P}(1,0) &= (\lambda_1+\lambda_2)\|\xi^-(\alpha)\|^2+(\lambda_3+\lambda_4)\|\xi^+(\alpha)\|^2,\\
\tilde{P}(1,1) &= (\lambda_1+\lambda_2)\|\xi^-(-\alpha)\|^2+(\lambda_3+\lambda_4)\|\xi^+(-\alpha)\|^2,
\end{aligned} \tag{3.81}$$

For the case of depolarizing noise, we have $\lambda_1 = 1-3\eta/2$ and $\lambda_2 = \lambda_3 = \lambda_4 = \eta/2$. Therefore,

$$\begin{aligned}
\tilde{P}(0,0) &= \tilde{P}(1,1) = (1-\eta)P_+ + \eta P_-,\\
\tilde{P}(0,1) &= \tilde{P}(1,0) = (1-\eta)P_- + \eta P_+,
\end{aligned} \tag{3.82}$$

where

$$P_{\pm} = (2\pi\delta^2)^{-1/2} \exp\left(-\frac{(\alpha \mp \gamma)^2}{2\delta^2}\right). \tag{3.83}$$

Note that, $P_-/P_+ = \exp(-2\gamma\alpha/\delta^2)$. Thus, using

$$P(a,b) = \frac{\tilde{P}(a,b)}{\sum_{a,b\in\{0,1\}} \tilde{P}(a,b)}, \tag{3.84}$$

we can write joint probability distributions of Alice and Bob as

$$P(a,b) = \begin{cases} \frac{(1-\eta)+\eta\exp\left(-\frac{2\gamma\alpha}{\delta^2}\right)}{2\left(1+\exp\left(-\frac{2\gamma\alpha}{\delta^2}\right)\right)} & \text{if} \quad a=b \\ \frac{(1-\eta)\exp\left(-\frac{2\gamma\alpha}{\delta^2}\right)+\eta}{2\left(1+\exp\left(-\frac{2\gamma\alpha}{\delta^2}\right)\right)} & \text{if} \quad a\neq b \end{cases} \tag{3.85}$$

3.7.2 State of Eve's memory and her side information

In order to calculate $\rho_E^{a,b}$, we first need to find $\rho_E^a(x)$ which is the same as the case of assuming the approximation. $\rho_E^a(x)$ is given by (see Eq. (3.44) and (3.45))

$$\rho_E^a(x) = \frac{4}{P_a(x)} \sum_{i=1}^{4}\sum_{j=1}^{4} \sqrt{\lambda_i\lambda_j}\, \langle\psi^a|\Phi_i\rangle \langle\Phi_j|\psi^a\rangle \langle x|\xi_i^a\rangle \left\langle \xi_j^a\middle| x\right\rangle |\nu_i\rangle\langle\nu_j|_E \tag{3.86}$$

Note that $\langle x|\xi_i^a\rangle = \xi^+(x)$ if $\langle\boldsymbol{\sigma}_i^0\rangle_w = 1$ and $\langle x|\xi_i^a\rangle = \xi^-(x)$ if $\langle\boldsymbol{\sigma}_i^0\rangle_w = -1$ for all $a \in \{0,1\}$ and $i \in \{1,2,3,4\}$. Let us now denote $S^{\pm} = \|\xi^{\pm}(x)\|^2$, and

$$S = \xi^+(x)\xi^-(x) = \|\xi(x)\|^2 \exp\left(-\frac{\gamma^2}{2\delta^2}\right).$$

Here, remember that

$$\|\xi(x)\|^2 = (2\pi\delta^2)^{-1/2} \exp\left(-x^2/2\delta^2\right).$$

Then, the state $\rho_E^0(x)$ can be expressed in matrix form as

$$\frac{1}{P_0(x)} \begin{pmatrix} \left(1-\frac{3\eta}{2}\right)S^+ & \sqrt{\left(1-\frac{3\eta}{2}\right)\frac{\eta}{2}}S^+ & \sqrt{\left(1-\frac{3\eta}{2}\right)\frac{\eta}{2}}S & \sqrt{\left(1-\frac{3\eta}{2}\right)\frac{\eta}{2}}S \\ \sqrt{\left(1-\frac{3\eta}{2}\right)\frac{\eta}{2}}S^+ & \frac{\eta}{2}S^+ & \frac{\eta}{2}S & \frac{\eta}{2}S \\ \sqrt{\left(1-\frac{3\eta}{2}\right)\frac{\eta}{2}}S & \frac{\eta}{2}S & \frac{\eta}{2}S^- & \frac{\eta}{2}S^- \\ \sqrt{\left(1-\frac{3\eta}{2}\right)\frac{\eta}{2}}S & \frac{\eta}{2}S & \frac{\eta}{2}S^- & \frac{\eta}{2}S^- \end{pmatrix}, \tag{3.87}$$

and, similarly, the state $\rho_E^1(x)$ can be expressed as

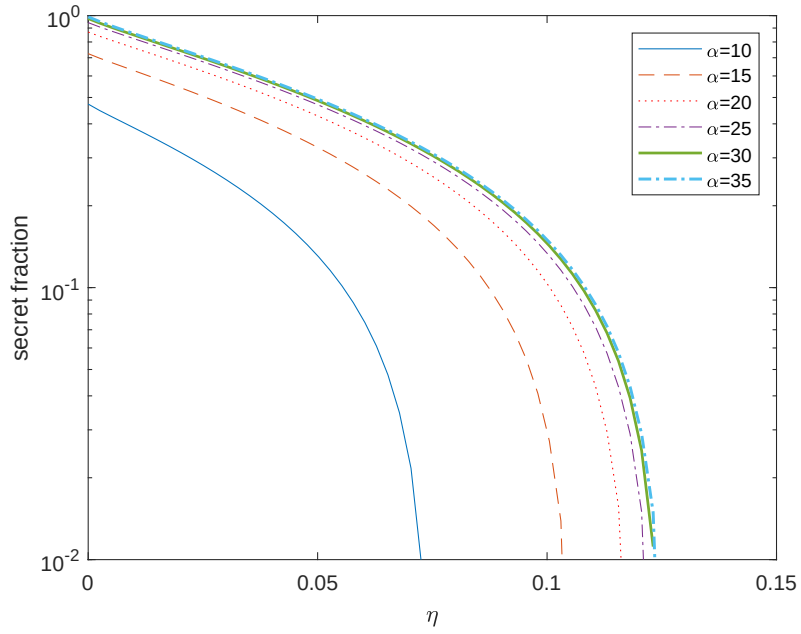
$$\frac{1}{P_1(x)}\begin{pmatrix} \left(1-\frac{3\eta}{2}\right)S^- & -\sqrt{\left(1-\frac{3\eta}{2}\right)\frac{\eta}{2}}S^- & \sqrt{\left(1-\frac{3\eta}{2}\right)\frac{\eta}{2}}S & -\sqrt{\left(1-\frac{3\eta}{2}\right)\frac{\eta}{2}}S \\ -\sqrt{\left(1-\frac{3\eta}{2}\right)\frac{\eta}{2}}S^- & \frac{\eta}{2}S^- & -\frac{\eta}{2}S & \frac{\eta}{2}S \\ \sqrt{\left(1-\frac{3\eta}{2}\right)\frac{\eta}{2}}S & -\frac{\eta}{2}S & \frac{\eta}{2}S^+ & -\frac{\eta}{2}S^+ \\ -\sqrt{\left(1-\frac{3\eta}{2}\right)\frac{\eta}{2}}S & \frac{\eta}{2}S & -\frac{\eta}{2}S^+ & \frac{\eta}{2}S^+ \end{pmatrix}. \tag{3.88}$$

3.7.3 Secure key rate and the noise tolerance

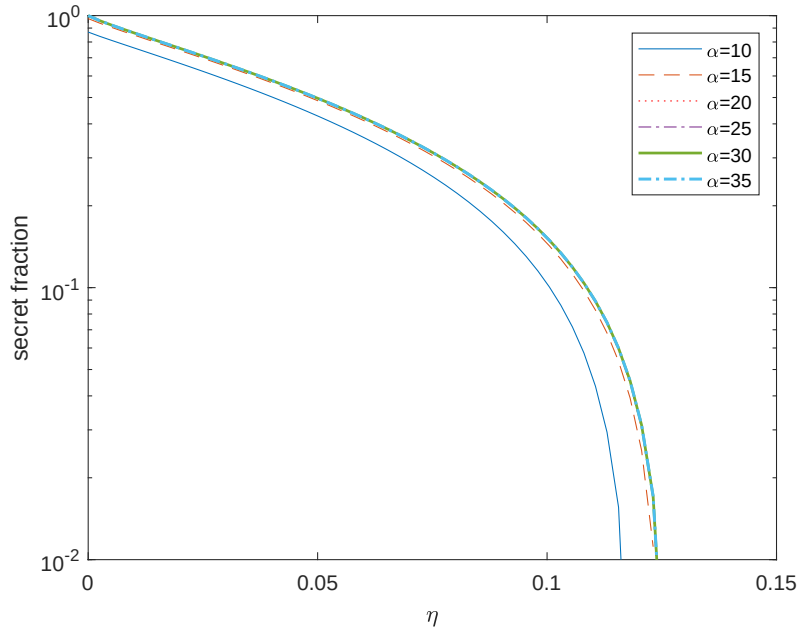
Similar to the case of weak measurement approximation in Subsection 3.6.5, the secret fraction F_{sec} can now be computed using the joint probability given in (3.85), and Eve's memory states described by Eqs. (3.87) and (3.88). In Figure 3.3, we have plotted F_{sec} for different values of α and γ. As it is clear from the plots, no positive secret fraction was observed above the noise tolerance of the six-state protocol *i.e.* 12.62%. In fact, for small α and γ, the secret fraction is smaller than that of six-state protocol for the same noise. If we look carefully, the joint probability distribution $P(a,b)$ in Eq. (3.85) approaches the joint probability of the six-state protocol as α is increased. That means even with the use of a weak value-based state discrimination scheme, the mutual information of Alice and Bob cannot exceed what is observed in the six-state case. The latter is in contrast with what we saw in Section 3.6.

3.8 Discussion and conclusions

In this chapter, we have derived the weak value formalism for mixed states from the assumptions of TSVF. Our generalization of weak values is the same as that proposed by other authors who used different methods to formulate it [103, 104, 105, 106]. We then devised a state discrimination scheme using weak measurements, where we assumed the core properties of weak values and the weak measurement approximation. Our scheme is motivated by the fact that two Gaussian distributions can be distinguished with arbitrarily low error probability by selecting only out-layer events. The formulation of weak values for mixed states was then used to discriminate mixed states in the six-state protocol. This approach apparently increased the noise tolerance drastically, giving an advantage over the original six-state QKD protocol. Moreover, this approach guarantees secure key generation at arbitrary high depolarizing noise. However, we found that these exciting results are wrong and appear only because of first



(a)



(b)

Figure 3.3: Secret key fraction calculated without assuming the weak measurement approximation. The secret fraction is plotted as a function of depolarizing noise η for (a) $\gamma = 0.1$ and (b) $\gamma = 0.2$, note that plots for $\alpha = 20, 25, 30, 35$ are coinciding.

order approximation in weak measurements. Moreover, these approximations are motivated by TSVF and the assumption of weak values as elements of reality in weak measurements. Our results have shown that such approximations must not be used without caution. More interestingly, our quantum state-discrimination scheme may give the correct answer for pure states but can fail in the case of mixed states. This puts a serious caution on the uses and implications of generalized weak values. Contrary to what is implied by TSVF (Section 3.2), weak values for mixed states might not be on equal footing with those for pure states. We would also like to emphasize a direct implication of our analysis that L. Vaidman's proposition that weak values are elements of the reality of weak measurements [65, 106] needs to be revisited and reanalyzed.

Chapter 4

High noise-tolerant quantum key distribution using block-wise processing

4.1 Introduction

Quantum computers threaten the security of modern cryptography which is primarily based on the computational complexities of certain mathematical problems [92, 93, 94]. Even though large-scale quantum computers are a distant reality right now, the *store now, decrypt later* or *retrospective decryption* attacks have made the present long-term strategic communications vulnerable. The quantum theory provides a solution to the problem in the form of quantum key distribution (QKD) [10, 11]. QKD allows two distant parties, Alice and Bob, to exchange symmetric keys using quantum channels which can be unconditionally secure. The security of the keys is ensured by the principles of quantum mechanics such as the no-cloning principle [9], Bell-nonlocality [98, 115, 116], quantum contextuality [117, 118], or entanglement monogamy [119].

In a QKD protocol, Alice and Bob share quantum signals through a quantum channel and generate (partially) correlated bit strings using local measurements. Such channels can introduce noise to the signals. An eavesdropper Eve may replace these noisy channels with more technologically advanced noise-less channels and make use of the respective portion of the exchanged signals to gain information about Alice and Bob's bit strings. However, Alice and Bob can characterize the channel by estimating the security parameters of the protocol which usually quantify the noise of the channel. They then can use quantum mechanical principles to estimate the maximum allowed

Eve's knowledge about Alice or Bob's bits corresponding to the observed parameters. If Eve's correlation with Alice's bit (or Bob's, whichever is larger) is less than the correlations between Alice's and Bob's keys, then their communication can be considered secure in the asymptotic limit. The information accessible to Eve in her collective attack strategies is bounded by Holevo quantity provided that the key length is asymptotically large [112].

The security parameter in BB84 [10], E91 [98], B92 [99], and six-state protocol (SSP) [97] is the quantum bit error rate (QBER). QBER is the probability that the key bits of Alice and Bob do not match. For a *depolarizing channel*, QBER is half the *depolarizing* probability in a qubit-based QKD protocol. QBER is called the channel noise in the context of QKD. Noise-tolerance for BB84 (equivalently E91 and B92) against collective attacks is 11% whereas for the six-state protocol, it is 12.62% with one-way communication in classical post-processing [11, 111]. Devising a QKD protocol that can tolerate as high a quantum channel noise as possible is recommended for long-distance secure quantum communications. Moreover, high noise tolerance is also required for practical purposes.

Various strategies have been adopted in the past to improve channels' noise tolerance. The method of *noisy preprocessing* increases noise tolerance up to 14.1% for one-way SSP [110, 120]. Lo-Chau scheme using quantum computers can tolerate noise up to 18.9% [121]. Gottesman and Lo proposed techniques of two-way classical post-processing that shows 26.4% noise tolerance [122]. Methods of classical advantage distillation in one-way SSP can have a noise tolerance of 27.6% [110, 123, 124]. This is so far the highest noise tolerance in a two-level quantum system-based QKD scheme with one-way classical post-processing. This appears to be a bottleneck in the progress of achieving high noise-tolerant QKD schemes. However, semiquantum approaches with two-way quantum communications have also been used to breach the threshold, but could only achieve noise tolerance of 26% [125, 126]. Noise tolerance against certain individual attacks such as asymmetric error patterns and photons-splitting attacks have been shown to be up to 33% [127, 128]. Another approach to achieving high noise tolerance is the high dimension QKD (HDQKD) [129, 130, 131, 132, 133]. Such schemes do show an increased noise tolerance but they require systems with high dimensions.

In this chapter, we present a QKD scheme using two-level quantum systems that can tolerate noise levels above 30%. We use entanglement-based SSP and then perform block-wise processing by constructing blocks of a finite length say m. If the bipartite state ρ_{AB} is shared over the quantum channel, a key bit is generated from a single copy of ρ_{AB}. In our scheme, we use a block $\rho_{AB}^{\otimes m}$ to generate a single key-bit instead. The state-sharing and measurement strategies for Alice and Bob remain the same as for the six-state protocol. In addition, Alice and Bob use certain permutations on

their respective bit-strings to construct blocks. They then discard certain blocks using classical communications over an authenticated classical channel. From the remaining blocks, they generate their raw keys. This process decreases their key-bit error rate with a huge margin and effectively increases their correlations without error correction. On the other hand, these additional steps do not increase Eve's knowledge significantly. Therefore, the overall effect increases the secret key fraction shared between Alice and Bob. We provide an information-theoretic security proof against collective attacks. The secure key fraction is computed using computer programs. Due to computational limitations, we could only analyze the security of the protocol with block size up to $m = 7$. For $m = 7$, the noise tolerance is found to be 30.53% which is a significant improvement over the advantage distillation scheme that shows 27.6% noise tolerance.

The material in this chapter is arranged as follows. Section 4.2 presents the protocol, Section 4.3 presents a detailed mathematical model of the protocol. In Section 4.4, we analyze the security of the protocol assuming that the channel is *depolarizing*. We begin with defining security criteria in Subsection 4.4.1. Then in Subsection 4.4.2, we derive the joint probability distribution for Alice and Bob's raw keys and the state of corresponding Eve's memory. Then in Subsection 4.4.3, we compute the secret key fraction and noise tolerance for various blocks. Finally, Section 4.5 presents the discussion and conclusions of this chapter.

4.2 Protocol steps

The protocol consists of the following steps: state sharing, measurements, sifting, parameter estimation, and classical post-processing (error correction followed by privacy amplification). The step of state sharing followed by measurements is repeated N number of times where N is asymptotically large. Here, we present all the steps of our protocol.

(1) *State sharing.* Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is shared between Alice and Bob over a quantum channel $\mathcal{E}(\cdot)$. Systems received by Alice and Bob in i-th pair are denoted A_i and B_i, respectively.

(2) *Measurements.* Alice and Bob perform six-state measurements on their respective systems with uniformly random measurement choices. Formally, Alice randomly chooses input $\alpha \in \{0, 1, 2\}$ from a classical register R^α, and performs the measurement $\mathcal{M}_{A_i}^{\alpha} \equiv \{M_{A_i}^{a|\alpha}\}_{a\in\{0,1\}}$ on A_i, where the index a ranges over Alice's outcomes. Similarly, Bob draws the random input $\beta \in \{0, 1, 2\}$ from a classical register R^β and performs the measurement $\mathcal{M}_{B_i}^{\beta} \equiv \{M_{B_i}^{b|\beta}\}_{b\in\{0,1\}}$ on B_i, where the index b ranges over

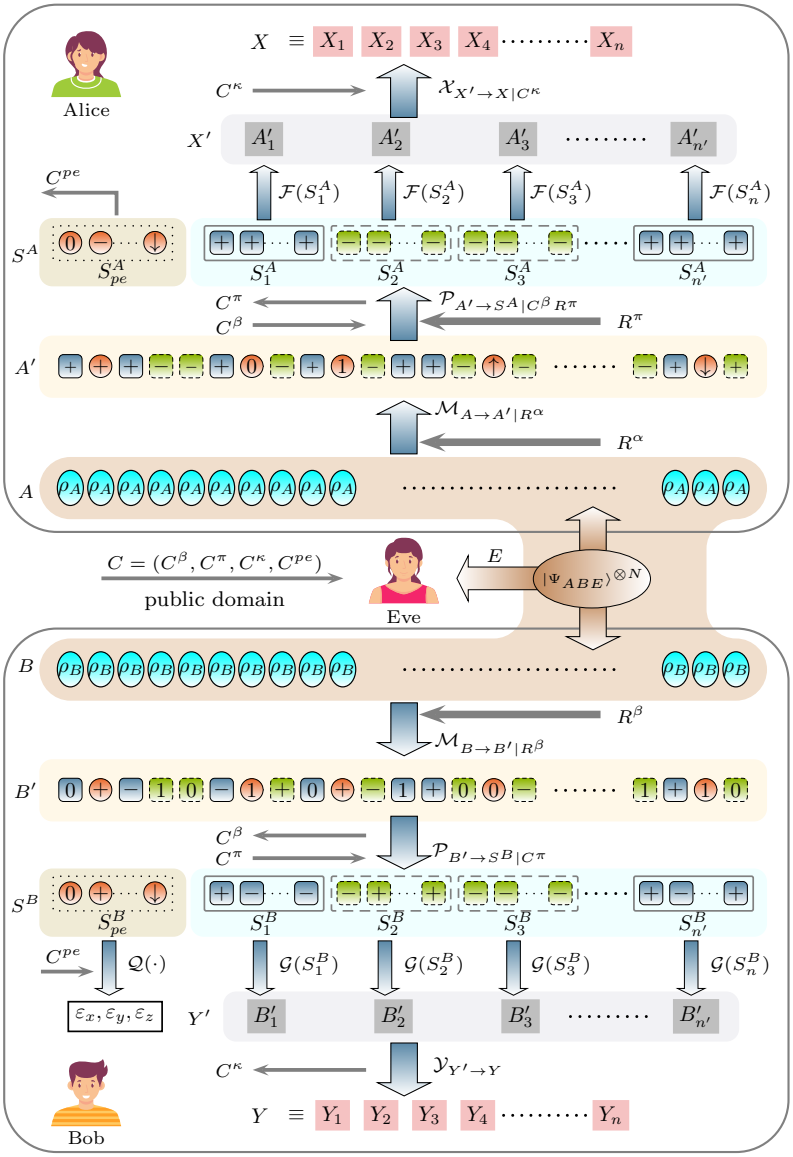


Figure 4.1: Schematic diagram of the QKD protocol. Alice, Bob, and Eve share the tripartite system Ψ_{ABE}. The strings of systems or alphabets are symbolic. $R^{\alpha}, R^{\beta}, R^{\pi}$ are locally generated random inputs. Classical communications is denoted by C^{i} where i is the suitable superscript. All the functions, transformations, transcripts, and the alphabets strings are explained in Section 4.2.

Bob's measurement outcomes. We consider the following measurement settings:

$$\begin{aligned}\mathcal{M}^0_{A_i} &= \mathcal{M}^0_{B_i} \equiv \{|0\rangle\langle 0|, |1\rangle\langle 1|\},\\ \mathcal{M}^1_{A_i} &= \mathcal{M}^1_{B_i} \equiv \{|+\rangle\langle +|, |-\rangle\langle -|\},\\ \mathcal{M}^2_{A_i} &= \mathcal{M}^2_{B_i} \equiv \{|\uparrow\rangle\langle\uparrow|, |\downarrow\rangle\langle\downarrow|\},\end{aligned} \tag{4.1}$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, $|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$, and $|\downarrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$. Suppose the measurement projections of Alice and Bob in the i-th round of the protocol are $M^{a|\alpha}_{A_i} = |A_i\rangle\langle A_i|$ and $M^{b|\beta}_{B_i} = |B_i\rangle\langle B_i|$, respectively. Then, they store their outcomes in the classical registers A' and B' as alphabets A'_i and B'_i, respectively, where $A'_i, B'_i \in \{0, 1, +, -, \uparrow, \downarrow\} \equiv \mathbb{M}$. Note that the alphabets of A' and B' have information about the measurement basis and the outcomes of the corresponding rounds as well. After the completion of N rounds of the system sharing followed by the measurements, Alice and Bob have the alphabet strings $A' = A'_1 A'_2 \cdots A'_N$ and $B' = B'_1 B'_2 \cdots B'_N$ as classical registers. They then proceed to the sifting process which is a very important part of our protocol.

(3) *Sifting.* Both parties then perform the sifting on A' and B' to obtain the raw keys X and Y of an equal length $n \leq N$ by executing the following steps:

3a: Alice and Bob broadcast their measurement inputs (the choices of their measurement basis) in form of the classical transcripts $C^\alpha \in \{0, 1, 2\}^N$ and $C^\beta \in \{0, 1, 2\}^N$ with i-th entries denoted by C^α_i and C^β_i, respectively. Hereafter, we denote the i-th entry of any classical register, transcript or alphabet string S by S_i.

3b: They discard all the rounds for which their measurement basis does not match. Formally, they generate the alphabet strings $\bar{T}^A$ and $\bar{T}^B$ using the following functions

$$\bar{T}^A_i = \begin{cases} A'_i; & \text{if } C^\alpha_i = C^\beta_i \\ \perp; & \text{if } C^\alpha_i \neq C^\beta_i \end{cases}, \tag{4.2}$$

and

$$\bar{T}^B_i = \begin{cases} B'_i; & \text{if } C^\alpha_i = C^\beta_i \\ \perp; & \text{if } C^\alpha_i \neq C^\beta_i \end{cases}. \tag{4.3}$$

They then generate the strings T^A and T^B by discarding all the $\bar{T}^A_i = \bar{T}^B_i = \perp$ from $\bar{T}^A$ and $\bar{T}^B$, respectively. Note that $T^A_i, T^B_i \in \mathbb{M}$, $\forall i$.

3c: Alice divides T^A into two equal parts A^{pe} and A'' by randomly choosing the alphabets of A^{pe} and A'' from T^A. She then discards A''_i if $A''_i \in \{0, 1, \uparrow, \downarrow\}$, $\forall i$. Then, she announces whether A''_i is kept or discarded by sending the following

transcript over the ACC:

$$C_i^{\bullet} = \begin{cases} \circ; & \text{if } T_i^A \text{ is kept, either in } A^{pe} \text{ or in } A'' \\ \bullet; & \text{if } T_i^A \text{ is discarded (after sending it in) } A'' \end{cases} . \tag{4.4}$$

The string formed by the remaining alphabets of A'' is denoted by $\bar{A}$. Note that $\bar{A}_i \in \{+, -\}$, $\forall i$. String A^{pe} will be used for the *parameter estimation* while $\bar{A}$ for the raw key generation.

3d: Alice distributes alphabets of $\bar{A}$ further into the alphabet blocks $A^1, A^2, \cdots, A^{n'}$ of size m in such a way that all the alphabets in a block A^j are either $+$ or all of them are $-$ where the choice of $+$ and $-$ is uniformly random. The choices are drawn from a locally generated random seed R^{π}. Thus, A^j is a random element in the set $\{+++\cdots+, ---\cdots-\}$ with uniform probability.

3e: Alice then prepares a transcript C^{π} of ordered pairs as follows: if T_k^A is relocated to the i-th position in the block A^j, where $j = pe, 1, 2, \cdots, n'$, then $C_k^{\pi} = (j, i)$. It should be noted that C^{π} does not contain any information about the values of the alphabets of A^j *i.e.* whether they are $+$ or $-$. Alice then broadcasts C^{π}.

3f: Bob generates the blocks $B^{pe}, B^1, B^2, \cdots, B^{n'}$ by permuting the alphabets of T^B according to the transcript C^{π}. Formally, he relocates T_k^B to the i-th position in the block B^j if $C_k^{\pi} = (j, i)$. It is to be emphasized here that the i-th alphabets of the two blocks A^j and B^j *i.e.* A_i^j and B_i^j, held by Alice and Bob respectively, $\forall j \in \{pe, 1, 2, \cdots, n'\}$ are generated from the same entangled pair shared by the two parties. Note that, unlike A^j, block B^j can have both $+$ and $-$ alphabets in it $\forall j \in \{1, 2, 3, \cdots, n'\}$. In general, $B^j \in \{+, -\}^m$.

3g: Alice generates a bit string $X' \in \{0, 1\}^{n'}$ from blocks $\{A^j\}$ for all $j \in \{1, 2, 3, \cdots, n'\}$ as follows,

$$X'_j = \begin{cases} 0; & \text{if } A^j \in \{+\}^m \textit{ i.e. } A^j \equiv ++++\cdots++ \\ 1; & \text{if } A^j \in \{-\}^m \textit{ i.e. } A^j \equiv ----\cdots-- \end{cases} . \tag{4.5}$$

Bob generates an alphabet string $Y' \in \{0, 1, \varnothing\}^{n'}$ from blocks $\{B^j\}$ for all $j \in \{1, 2, 3, \cdots, n'\}$ as follows,

$$Y'_j = \begin{cases} 0; & \text{if } A^j \in \{+\}^m \textit{ i.e. } A^j \equiv ++++\cdots++ \\ 1; & \text{if } A^j \in \{-\}^m \textit{ i.e. } A^j \equiv ----\cdots-- \\ \varnothing; & \text{else} \end{cases} . \tag{4.6}$$

The actions of Alice and Bob can be modeled using functions of form $\mathcal{F} : \{+^m, -^m\} \rightarrow \{0, 1\}$ and $\mathcal{G} : \{+, -\}^m \rightarrow \{0, 1, \varnothing\}$, respectively. Formally, $X'_i = \mathcal{F}(A^i)$ and $Y'_i = \mathcal{G}(B^i)$.

3h: Bob prepares a transcript $C^{\kappa} \in \{\checkmark, \varnothing\}^{n'}$ by setting

$$C_i^{\kappa} = \begin{cases} \varnothing; & \text{if } Y_i' = \varnothing \\ \checkmark; & \text{else} \end{cases} . \tag{4.7}$$

He then broadcasts it over the ACC.

3i: Bob generates a bit string $Y \in \{0,1\}^n$ from Y' of length $n \leq n'$ by discarding all $Y_i' = \varnothing$. Alice discards X_i' if $C_i^{\kappa} = \varnothing$. The reduced bit string of Alice is denoted by $X \in \{0,1\}^n$. X and Y are the raw keys of Alice and Bob, respectively.

(4) *Parameter estimation.* In the parameter estimation step, Alice broadcasts the alphabet string A^{pe} as a transcript C^{pe}, *i.e.* $C_i^{pe} = A_i^{pe}$. Bob estimates the probability of error $Q = P\left(C_i^{pe} \neq B_i^{pe}\right)$. The protocol is aborted if $Q \geq Q_{tol}$, where $Q_{tol} \in \left[0, \frac{1}{2}\right]$ is the tolerated error rate of the protocol.

(5) *Classical post-processing.* If the protocol is not aborted, Alice and Bob perform the error correction followed by the privacy amplification on their weakly correlated and partially secure raw keys X and Y to obtain an identical and fully secure key $K \in \{0,1\}^{\bar{n}}$ where $\bar{n} \leq n$ is the bit length of the final key.

4.3 Mathematical model of the protocol

Here, we present a mathematical model of the proposed quantum key distribution protocol. Moreover, we will derive the classical-classical-quantum (ccq) state of the raw key bits held by Alice and Bob and the corresponding quantum memory of any potential adversary Eve. Since we are only considering the asymptotic case under the collective attacks with i.i.d. assumption, the mathematical description of only the individual rounds is required at the end for the security analysis. However, at some intermediate steps of the protocol, like the block-wise processing during sifting, we may need a complete description of all the rounds. Thus, we will provide a complete description whenever it is needed.

4.3.1 Quantum inputs and the measurements

Two parties, Alice and Bob, share entangled qubit-pairs. The pairs are prepared in the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$ by a third party and distributed between them over the quantum channel $\mathcal{E}(\cdot)$, or equivalently, Alice can prepare the pair in $|\Phi^+\rangle$ and send one of the qubits to Bob over $\mathcal{E}(\cdot)$ while keeping the second qubit with herself. The channel $\mathcal{E}(\cdot)$ can introduce noise to the system transforming the state to a mixed state,

$$\rho_{AB} = \mathcal{E}\left(\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|\right). \tag{4.8}$$

The noise introduced by the quantum channel is attributed to the potential eavesdropper Eve. A purification $\rho_{ABE} = |\Psi_{ABE}\rangle\langle\Psi_{ABE}|$ of ρ_{AB} is used to describe the tripartite quantum state of Alice, Bob, and Eve. If the rounds are repeated N times, then the state of all systems, given that all the devices are memoryless and behave identically and independently during the complete execution of the protocol (i.i.d. assumption), is jointly represented as

$$\boldsymbol{\rho}_{ABE} = \rho_{ABE}^{\otimes N} \tag{4.9}$$

The quantum systems held by Alice, Bob, and Eve in the i-th round are denoted by A_i, B_i, and E_i, respectively. The measurements performed by Alice and Bob on the systems A_i and B_i, are modeled by the positive operator-valued measures (POVMs) $\{M_{A_i}^{a|\alpha}\}_{a\in\{0,1\}}$ and $\{M_{B_i}^{b|\beta}\}_{b\in\{0,1\}}$, where $\alpha, \beta \in \{0, 1, 2\}$ are the measurement settings chosen by Alice and Bob, respectively. The register R^α from which the values of α are drawn can be represented by the state of a finite-dimensional quantum system with a set of orthogonal basis $\{|\alpha\rangle\}$ as

$$\rho_{R_i^\alpha} = \frac{1}{3} \sum_{\alpha\in\{0,1,2\}} |\alpha\rangle\langle\alpha|_{R_i^\alpha} \tag{4.10}$$

Similarly, the quantum state corresponding to Bob's register R^β is given by

$$\rho_{R_i^\beta} = \frac{1}{3} \sum_{\beta\in\{0,1,2\}} |\beta\rangle\langle\beta|_{R_i^\beta} \tag{4.11}$$

Eq. (4.10) and (4.11) model only the i-th inputs drawn by the respective parties (*i.e.* R_i^α and R_i^β) during the implementation. With i.i.d. assumption, the quantum state for the register R^α can be expressed as $\rho_{R^\alpha} = \rho_{R_i^\alpha}{}^{\otimes N}$. Similarly, $\rho_{R^\beta} = \rho_{R_i^\beta}{}^{\otimes N}$.

The measurement on A_i with the input α is represented by a completely positive trace-preserving (CPTP) map $\mathcal{M}_{A_i\to A_i'|R_i^\alpha}$ that maps the quantum state of the system A_i to a (classical) alphabet A_i' as a measurement outcome registered in a register A'. Formally, dropping the index i,

$$\mathcal{M}_{A\to A'|R^\alpha}(\rho_{ABE}) = \sum_{a\in\{0,1\}} |\xi_{a|\alpha}\rangle\langle\xi_{a|\alpha}|_{A'} \otimes \mathrm{Tr}_A \left\{ \left(M_A^{a|\alpha} \otimes I_B \otimes I_E\right) \rho_{ABE} \left(M_A^{a|\alpha} \otimes I_B \otimes I_E\right)^\dagger \right\}, \tag{4.12}$$

where the alphabet corresponding to Alice's outcome a with the measurement input α is mathematically modeled by the quantum state $|\xi_{a|\alpha}\rangle\langle\xi_{a|\alpha}|$. Considering all measurement choices $\alpha \in \{0, 1, 2\}$ in a generalized measurement, the map can be represented

as

$$\begin{aligned}\mathcal{M}_{A\to A'}(\cdot) =& \frac{1}{3}\sum_{\alpha\in\{0,1,2\}}\sum_{a\in\{0,1\}} |\alpha\rangle\langle\alpha|_{R^\alpha}\otimes \left|\xi_{a|\alpha}\right\rangle\!\left\langle\xi_{a|\alpha}\right|_{A'}\otimes \\ & \mathrm{Tr}_A\left\{\left(M_A^{a|\alpha}\otimes I_B\otimes I_E\right)(\cdot)\left(M_A^{a|\alpha}\otimes I_B\otimes I_E\right)^\dagger\right\}.\end{aligned} \tag{4.13}$$

Similarly, the map corresponding to Bob's generalized measurement is given by

$$\begin{aligned}\mathcal{M}_{B\to B'}(\cdot) =& \frac{1}{3}\sum_{\beta\in\{0,1,2\}}\sum_{b\in\{0,1\}} |\beta\rangle\langle\beta|_{R^\beta}\otimes \left|\xi_{b|\beta}\right\rangle\!\left\langle\xi_{b|\beta}\right|_{B'}\otimes \\ & \mathrm{Tr}_B\left\{\left(I_A\otimes M_B^{b|\beta}\otimes I_E\right)(\cdot)\left(I_A\otimes M_B^{b|\beta}\otimes I_E\right)^\dagger\right\},\end{aligned} \tag{4.14}$$

where the alphabet corresponding to Bob's outcome b with the measurement input β is mathematically modeled by the quantum state $\left|\xi_{b|\beta}\right\rangle\!\left\langle\xi_{b|\beta}\right|$. Since the two maps $\mathcal{M}_{A\to A'|R^\alpha}$ and $\mathcal{M}_{B\to B'|R^\beta}$ acts on separate systems, they commute. Hence, $\mathcal{M}_{AB\to A'B'}$ $= \mathcal{M}_{A\to A'}\circ\mathcal{M}_{B\to B'} = \mathcal{M}_{B\to B'}\circ\mathcal{M}_{A\to A'}$, and after tracing out R^α, R^β, A, and B, the ccq-state of A', B', and the corresponding Eve's memory is given by

$$\rho_{A'B'E} = \frac{1}{9}\sum_{\alpha\in\{0,1,2\}}\sum_{\beta\in\{0,1,2\}}\sum_{a\in\{0,1\}}\sum_{b\in\{0,1\}} \left|\xi_{a|\alpha}\right\rangle\!\left\langle\xi_{a|\alpha}\right|_{A'}\otimes\left|\xi_{b|\beta}\right\rangle\!\left\langle\xi_{b|\beta}\right|_{B'}\otimes\rho_E^{ab|\alpha\beta}, \tag{4.15}$$

where

$$\rho_E^{ab|\alpha\beta} = \mathrm{Tr}_{AB}\left\{\left(M_A^{a|\alpha}\otimes M_B^{b|\beta}\otimes I_E\right)\rho_{ABE}\left(M_A^{a|\alpha}\otimes M_B^{b|\beta}\otimes I_E\right)^\dagger\right\}. \tag{4.16}$$

Note that the state $\rho_E^{ab|\alpha\beta}$ is not normalized yet. After the normalization, the state becomes

$$\sigma_E^{ab|\alpha\beta} = \frac{\mathrm{Tr}_{AB}\left\{\left(M_A^{a|\alpha}\otimes M_B^{b|\beta}\otimes I_E\right)\rho_{ABE}\left(M_A^{a|\alpha}\otimes M_B^{b|\beta}\otimes I_E\right)^\dagger\right\}}{\mathrm{Tr}\left\{\left(M_A^{a|\alpha}\otimes M_B^{b|\beta}\right)\rho_{AB}\left(M_A^{a|\alpha}\otimes M_B^{b|\beta}\right)^\dagger\right\}}. \tag{4.17}$$

Let us denote

$$P^{ab|\alpha\beta} = \mathrm{Tr}\left\{\left(M_A^{a|\alpha}\otimes M_B^{b|\beta}\right)\rho_{AB}\left(M_A^{a|\alpha}\otimes M_B^{b|\beta}\right)^\dagger\right\}. \tag{4.18}$$

4.3.2 Sifting process

The sifting operation $\mathcal{S} : A'B' \to XY$ maps the states representing alphabet strings $A', B' \in \mathbb{M}^N$ to the states representing bit strings $X, Y \in \{0,1\}^n$ of a shorter length n held by Alice and Bob, respectively. Here we present a mathematical model of all the intermediate steps of the sifting process and derive the ccq-state.

(a) Taking the transcripts C^A and C^B into account, the state up to a normalization factor is given by

$$\rho_{A'B'C^AC^BE} = \sum_{\alpha\in\{0,1,2\}} \sum_{\beta\in\{0,1,2\}} \sum_{a\in\{0,1\}} \sum_{b\in\{0,1\}} \left|\xi_{a|\alpha}\right\rangle\!\left\langle\xi_{a|\alpha}\right|_{A'} \otimes \left|\xi_{b|\beta}\right\rangle\!\left\langle\xi_{b|\beta}\right|_{B'} \otimes |\alpha\rangle\langle\alpha|_{C^A} \otimes |\beta\rangle\langle\beta|_{C^B} \otimes \rho_E^{ab|\alpha\beta} \tag{4.19}$$

(b) Alice and Bob then discard all the rounds for which $\alpha \neq \beta$. This can be modeled by a post-selection projection Π acting upon the state $\rho_{A'B'C^AC^BE}$, where

$$\Pi = \mathbb{1}_{A'} \otimes \mathbb{1}_{B'} \otimes \left(\sum_{i\in\{0,1,2\}} |i\rangle\langle i|_{C^A} \otimes |i\rangle\langle i|_{C^B} \right) \otimes \mathbb{1}_E \tag{4.20}$$

The transformation can be represented by the map $\mathcal{D}(\cdot) = \Pi(\cdot)\Pi^\dagger / \operatorname{Tr}\{\Pi(\cdot)\Pi^\dagger\}$. After tracing out the transcripts C^A and C^B, the ccq-state up to a normalization factor can be written as

$$\begin{aligned}\rho_{T^AT^BE} &= \operatorname{Tr}_{C^AC^B}\left\{\mathcal{D}(\rho_{A'B'C^AC^BE})\right\} \\ &= \sum_{\alpha\in\{0,1,2\}} \sum_{a\in\{0,1\}} \sum_{b\in\{0,1\}} \left|\xi_{a|\alpha}\right\rangle\!\left\langle\xi_{a|\alpha}\right|_{T^A} \otimes \left|\xi_{b|\alpha}\right\rangle\!\left\langle\xi_{b|\alpha}\right|_{T^B} \otimes \rho_E^{ab|\alpha\alpha}\end{aligned} \tag{4.21}$$

(c) Dividing the string T^A into A^{pe} and A'', and the corresponding T^B into B^{pe} and B'', respectively, is equivalent to dividing the ensemble $\rho_{T^AT^BE}$ into two identical ensembles $\rho_{A^{pe}B^{pe}E}$ and $\rho_{A''B''E}$ *i.e.*

$$\rho_{A^{pe}B^{pe}E} = \rho_{A''B''E} = \rho_{T^AT^BE} \tag{4.22}$$

Further sifting operations are performed only on $\rho_{A''B''E}$. The ensemble $\rho_{A^{pe}B^{pe}E}$ is only used for *parameter estimation*. The process of discarding all $A_i'' \in \{0, 1, \uparrow, \downarrow\}$ is equivalent to performing a post-selection corresponding to the projection

$$\Pi' = \left(\sum_{a,b\in\{0,1\}} \left|\xi_{a|1}\right\rangle\!\left\langle\xi_{a|1}\right|_{A''} \otimes \left|\xi_{b|1}\right\rangle\!\left\langle\xi_{b|1}\right|_{B''} \right) \otimes \mathbb{1}_E. \tag{4.23}$$

Note that the alphabets $+$ and $-$ are outcomes of the measurement setting $\alpha = \beta = 1$ *i.e.* $|+\rangle \equiv \left|\xi_{0|1}\right\rangle$ and $|-\rangle \equiv \left|\xi_{1|1}\right\rangle$. The ensemble after this process is represented by the following state up to a normalization factor,

$$\begin{aligned}\rho_{\bar{A}\bar{B}E} &= \mathcal{D}'(\rho_{A''B''E}) \\ &= \sum_{a\in\{0,1\}}\sum_{b\in\{0,1\}} \left|\xi_{a|1}\right\rangle\!\left\langle\xi_{a|1}\right|_{\bar{A}} \otimes \left|\xi_{b|1}\right\rangle\!\left\langle\xi_{b|1}\right|_{\bar{B}} \otimes \rho_E^{ab|11} \\ &= \sum_{a\in\{0,1\}}\sum_{b\in\{0,1\}} P^{ab|11} \left|\xi_{a|1}\right\rangle\!\left\langle\xi_{a|1}\right|_{\bar{A}} \otimes \left|\xi_{b|1}\right\rangle\!\left\langle\xi_{b|1}\right|_{\bar{B}} \otimes \sigma_E^{ab|11}.\end{aligned} \tag{4.24}$$

Here, we have used Eqs. (4.17) and (4.18) in the last step. Let us now denote $P^{ab|11} \equiv \tilde{P}(\xi_{a|1}, \xi_{b|1})$, $\sigma^{ab|11} \equiv \sigma_E^{\xi_{a|1},\xi_{b|1}}$, and $+ \equiv \xi_{0|1}, - \equiv \xi_{1|1}$. Eq. (4.24) is then re-written as

$$\rho_{\bar{A}\bar{B}E} = \sum_{a,b\in\{+,-\}} P(a,b)\, |a\rangle\!\langle a|_{\bar{A}} \otimes |b\rangle\!\langle b|_{\bar{B}} \otimes \sigma_E^{a,b}, \tag{4.25}$$

where

$$P(a,b) = \frac{\tilde{P}(a,b)}{\sum_{a,b\in\{+,-\}} \tilde{P}(a,b)}. \tag{4.26}$$

(d-f) Let us denote the process of forming the blocks $A^1, A^2, \cdots, A^{n'}$ from the string $\bar{A}$ *s. th.* either $A^j = +++\cdots+$ or $A^j = ---\cdots-$ for $j = 1, 2, \cdots, n'$ using the function $\mathcal{P}_{\bar{A}\to S^A|R^\pi}$, where R^π is the random choice for the permutation, and S^A denotes the string of blocks $\{A^j\}$ *i.e.* $\{S_i^A \equiv A^i\}$. The process of generating the transcript C^π is denoted by $\mathcal{C}_{S^A\to S^A C^\pi}$. Furthermore, let $\mathcal{P}_{\bar{B}\to S^B|C^\pi}$ denote Bob's action of generating the block-string S^B by performing the permutation on $\bar{B}$ as per the transcript C^π. The overall effect of these operations can be represented by

$$\mathcal{P}_{\bar{A}\bar{B}ER^\pi\to S^A S^B E R^\pi C^\pi} = \mathcal{P}_{\bar{B}\to S^B|C^\pi} \circ \mathcal{C}_{S^A\to S^A C^\pi} \circ \mathcal{P}_{\bar{A}\to S^A|R^\pi}. \tag{4.27}$$

The process $\mathcal{P}_{\bar{A}\bar{B}ER^\pi\to S^A S^B E R^\pi C^\pi}$ followed by tracing out C^π and R^π is mathematically equivalent to performing a post-selection

$$\mathcal{K} = \left(|+\rangle\!\langle+|_{\bar{A}}^{\otimes m} + |-\rangle\!\langle-|_{\bar{A}}^{\otimes m}\right) \otimes \mathbb{1}_{\bar{B}}^{\otimes m} \otimes \mathbb{1}_E^{\otimes m} \tag{4.28}$$

on a block of m copies of the state $\rho_{\bar{A}\bar{B}E}$ *i.e.* $\rho_{\bar{A}\bar{B}E}^{\otimes m}$. The un-normalized state after applying $\mathcal{K}$ is given as

$$\begin{aligned}\tau_{S^A S^B E} &= \mathcal{K}\left(\rho_{\bar{A}\bar{B}E}^{\otimes m}\right)\mathcal{K}^\dagger \\ &= \sum_{a\in\{+,-\}} \left(|a\rangle\!\langle a|^{\otimes m}\right)_{S^A} \otimes \sum_{\lambda\in\{+,-\}^m} P_m(a,\lambda)\, |\lambda\rangle\!\langle\lambda|_{S^B} \otimes \sigma_E^{a,\lambda},\end{aligned} \tag{4.29}$$

where the index λ runs over the 2^m binomial permutations of the symbols $\{+,-\}$. Now suppose that we can represent the index λ as $\lambda \equiv \lambda_1\lambda_2\lambda_3\cdots\lambda_m$ where $\lambda_i \in \{+,-\}\forall i \in \{1,2,3,\cdots,m\}$, then the state $|\lambda\rangle\langle\lambda|$ is given by

$$|\lambda\rangle\langle\lambda| = \bigotimes_{i\in\{1,2,\cdots,m\}} |\lambda_i\rangle\langle\lambda_i|\,, \tag{4.30}$$

and the corresponding block of Eve's memory is given by

$$\rho_E^{a,\lambda} = \bigotimes_{i\in\{1,2,\cdots,m\}} \rho_E^{a,\lambda_i}. \tag{4.31}$$

The joint probability distribution $P_m(a,\lambda)$ is given by

$$P_m(a,\lambda) = \prod_{i\in\{1,2,\cdots,m\}} P(a,\lambda_i), \tag{4.32}$$

where $P(a,\lambda_i)$ is the joint probability of Alice and Bob getting $a \in \{+,-\}$ and $\lambda_i \in \{+,-\}$, respectively, in a single round of the state sharing followed by the measurements. If the state shared between Alice and Bob in a single round is ρ_{AB}, then with i.i.d. assumption, the joint probability $P_m(a,\lambda)$ is given as

$$P_m(a,\lambda) = \prod_{i=1}^{m} \mathrm{Tr}\left\{\rho_{AB}\,|a\rangle\langle a|_A \otimes |\lambda_i\rangle\langle\lambda_i|_B\right\}. \tag{4.33}$$

(g) The maps corresponding to the functions $\mathcal{F}$ and $\mathcal{G}$ are represented by $\mathcal{F}_{S^A\to X'}(\cdot)$ and $\mathcal{G}_{S^B\to Y'}(\cdot)$, respectively, *s. th.*

$$\begin{aligned}
\mathcal{F}_{S^A\to X'}\left(|+\rangle\langle+|_{S^A}^{\otimes m}\right) &= |0\rangle\langle 0|_{X'}\,,\\
\mathcal{F}_{S^A\to X'}\left(|-\rangle\langle-|_{S^A}^{\otimes m}\right) &= |1\rangle\langle 1|_{X'}\,,\\
\mathcal{G}_{S^B\to Y'}\left(|+\rangle\langle+|_{S^B}^{\otimes m}\right) &= |1\rangle\langle 1|_{Y'}\,,\\
\mathcal{G}_{S^B\to Y'}\left(|-\rangle\langle-|_{S^B}^{\otimes m}\right) &= |1\rangle\langle 1|_{Y'}\,,\\
\mathcal{G}_{S^B\to Y'}\left(|\psi\rangle\langle\psi|_{S^B}\right) &= |\varnothing\rangle\langle\varnothing|_{Y'}\,,
\end{aligned} \tag{4.34}$$

where $|\psi\rangle\langle\psi| \notin \left\{|+\rangle\langle+|^{\otimes m}, |-\rangle\langle-|^{\otimes m}\right\}$. The map $\mathcal{F}_{S^A\to X'} \circ \mathcal{G}_{S^B\to Y'}(\cdot)$ transforms $\tau_{S^AS^BE}$ into the state (up to a normalization factor)

$$\begin{aligned}
\tau_{X'Y'E} =& \mathcal{F}_{S^A\to X'} \circ \mathcal{G}_{S^B\to Y'}(\tau_{S^AS^BE})\\
=& \sum_{x,y\in\{0,1\}} Q'(x,y)\,|x\rangle\langle x|_{X'} \otimes |y\rangle\langle y|_{Y'} \otimes \omega_E^{x,y}\\
&+ \sum_{x\in\{0,1\}} |x\rangle\langle x|_{X'} \otimes |\varnothing\rangle\langle\varnothing|_{Y'} \otimes \bar{\rho}_E^{x},
\end{aligned} \tag{4.35}$$

where using Eq. (4.32) and Eq. (4.33)

$$\begin{aligned} Q'(0,0) &= P(+,+)^m, \quad Q'(1,0) = P(-,+)^m, \\ Q'(0,1) &= P(+,-)^m, \quad Q'(1,1) = P(-,-)^m, \end{aligned} \tag{4.36}$$

and using Eq. (4.31), we have

$$\begin{aligned} \omega_E^{0,0} &= \left(\sigma_E^{+,+}\right)^{\otimes m}, \quad \omega_E^{1,0} = \left(\sigma_E^{-,+}\right)^{\otimes m}, \\ \omega_E^{0,1} &= \left(\sigma_E^{+,-}\right)^{\otimes m}, \quad \omega_E^{1,1} = \left(\sigma_E^{-,-}\right)^{\otimes m}. \end{aligned} \tag{4.37}$$

Specification of the state $\bar{\rho}_E^x$ is not required here.

(h-i) The collective effect of the preparation and broadcast of C^κ followed by discarding the blocks corresponding to $|\varnothing\rangle\langle\varnothing|_{Y'}$ is mathematically equivalent to applying a post-selection of the form

$$\mathcal{L} = \sum_{x,y\in\{0,1\}} |x\rangle\langle x|_{X'} \otimes |y\rangle\langle y|_{Y'} \otimes \mathbb{1}_E. \tag{4.38}$$

Hence, the state after the completion of these steps is given by

$$\begin{aligned} \tau_{XYE} &= \mathcal{X}_{X'\to X} \circ \mathcal{Y}_{Y'\to Y}(\tau_{X'Y'E}) \\ &= \mathcal{L}(\tau_{X'Y'E})\mathcal{L}^\dagger \\ &= \sum_{x,y\in\{0,1\}} Q'(x,y)\, |x\rangle\langle x|_{X'} \otimes |y\rangle\langle y|_{Y'} \otimes \omega_E^{x,y}. \end{aligned} \tag{4.39}$$

After the normalization, τ_{XYE} can be re-written as

$$\tau_{XYE} = \sum_{x,y\in\{0,1\}} Q(x,y)\, |x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y \otimes \omega_E^{x,y}, \tag{4.40}$$

where

$$Q(x,y) = \frac{Q'(x,y)}{\sum_{x,y\in\{0,1\}} Q'(x,y)}. \tag{4.41}$$

Note that, here, we have used the fact that $\mathrm{Tr}\{\omega_E^{x,y}\} = 1, \forall x, y \in \{0,1\}$.

4.4 Security analysis

4.4.1 Security criteria

The protocol is secure against all the collective attacks in asymptotic limits if the Devetak-Winter key rate is greater than zero. The Devetak-Winter key rate is given by

$$r \geq \ell_{DW} = \mathcal{I}(A:B) - \chi(A:E) \tag{4.42}$$

where $\mathcal{I}(A:B)$ is the mutual information between Alice and Bob's raw keys X and Y, respectively, and $\chi(A:E)$ is the corresponding Holevo information. The mutual information and the Holevo quantity can be evaluated using the ccq-state of Alice, Bob, and Eve's memory.

4.4.2 Joint probability distribution and Eve's quantum memory

Here, we evaluate the joint probability distribution of Alice and Bob's raw bits, and the state of the corresponding Eve's quantum memory. Let us denote the state shared between Alice and Bob by $\rho_{AB} = \mathcal{E}\left(|\Phi^+\rangle\langle\Phi^+|\right)$, where $|\Phi^+\rangle\langle\Phi^+| = \frac{1}{\sqrt{2}}\left(|00\rangle + \langle 11|\right)$. Let us now attribute the noise introduced by the channel to the eavesdropper Eve. In that case, we can assume that the purification of the mixed state ρ_{AB} is held by Eve as a quantum memory. She can utilize her quantum memory corresponding to all rounds and all the classical information shared between Alice and Bob collectively to estimate the final key shared between them. Let the Hilbert spaces associated with qubits of Alice and Bob, and Eve's quantum memory be $\mathcal{H}_A, \mathcal{H}_B$, and $\mathcal{H}_E$, respectively. The purification $|\Psi_{ABE}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ can be written in Bell-basis of Alice and Bob's qubits as

$$|\Psi\rangle_{ABE} = \sum_{i=1}^{4} \sqrt{\lambda_i}\, |\Phi_i\rangle_{AB} \otimes |\nu_i\rangle_E\,, \tag{4.43}$$

where $|\Phi_1\rangle_{AB}, |\Phi_2\rangle_{AB}, |\Phi_3\rangle_{AB}, |\Phi_4\rangle_{AB}$ are the Bell states $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle$, and $|\Psi^-\rangle$, respectively, and $\{\nu_i\}$ forms a set of orthogonal basis which span $\mathcal{H}_E \equiv \mathbb{C}^4$. For a depolarizing channel, we have $\lambda_1 = 1 - 3\eta/2, \lambda_2 = \lambda_3 = \lambda_4 = \eta/2$, where $\eta \in [0, 1/2]$ is the depolarizing noise. In six-state and BB84, η is equal to the quantum bit error rate. Eq. (4.43) can now be re-written as

$$\begin{aligned} |\Psi\rangle_{ABE} =& \sqrt{1 - \frac{3\eta}{2}}\, |\Phi^+\rangle_{AB} \otimes |\nu_1\rangle_E + \sqrt{\frac{\eta}{2}}\, |\Phi^-\rangle_{AB} \otimes |\nu_2\rangle_E \\ &+ \sqrt{\frac{\eta}{3}}\, |\Psi^+\rangle_{AB} \otimes |\nu_3\rangle_E + \sqrt{\frac{\eta}{2}}\, |\Psi^-\rangle_{AB} \otimes |\nu_4\rangle_E\,. \end{aligned} \tag{4.44}$$

The corresponding bipartite state $\rho_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ is given by

$$\rho_{AB} = (1 - 2\eta)\, |\Phi^+\rangle\langle\Phi^+|_{AB} + \frac{\eta}{2} \mathbb{1}_A \otimes \mathbb{1}_B \tag{4.45}$$

Note that for $\eta = 0$, the state remains unchanged *i.e.* $\rho_{AB} = |\Phi^+\rangle\langle\Phi^+|$, and for $\eta = 1/2$ the state is completely destroyed *i.e.* $\rho_{AB} = \mathbb{1}_A \otimes \mathbb{1}_B/4$. Suppose Alice and Bob perform the measurements $\mathcal{M}_A^1$ and $\mathcal{M}_B^1$ *i.e.* they measure their respective systems in

x-basis. The probability distribution $P(a,b)$ for $a,b \in \{+,-\}$ can be evaluated using Eq. (4.33) as

$$\begin{aligned} P(+,+) = P(-,-) &= \frac{1-\eta}{2} \\ P(+,-) = P(-,+) &= \frac{\eta}{2} \end{aligned} \tag{4.46}$$

Using Eqs. (4.36),(4.41), and (4.46), the joint probability distribution $Q(x,y)$ for the ccq-state given in Eq. (4.40) is given by

$$Q(x,y) = \begin{cases} \frac{\left(\frac{1-\eta}{2}\right)^m}{2\left(\left(\frac{1-\eta}{2}\right)^m + \left(\frac{\eta}{2}\right)^m\right)}; & \text{if } x = y \\ \frac{\left(\frac{\eta}{2}\right)^m}{2\left(\left(\frac{1-\eta}{2}\right)^m + \left(\frac{\eta}{2}\right)^m\right)}; & \text{if } x \neq y \end{cases}. \tag{4.47}$$

Let us now calculate the state corresponding to Eve's memory. The state $\sigma_E^{a,b}$ for $a,b \in \{+,-\}$ represents Eve's quantum memory when Alice and Bob's outcomes are a and b, respectively. The state $\sigma_E^{a,b}$ can be calculated using Eqs. (4.17) and (4.18) as (also see the notations for $\sigma_E^{a,b}$ presented before Eq. (4.25))

$$\begin{aligned} \sigma_E^{+,+} &= \tfrac{1}{1-\eta} \begin{pmatrix} 1-\frac{3\eta}{2} & 0 & \sqrt{\left(1-\frac{3\eta}{2}\right)\frac{\eta}{2}} & 0 \\ 0 & 0 & 0 & 0 \\ \sqrt{\left(1-\frac{3\eta}{2}\right)\frac{\eta}{2}} & 0 & \frac{\eta}{2} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \\ \sigma_E^{-,-} &= \tfrac{1}{1-\eta} \begin{pmatrix} 1-\frac{3\eta}{2} & 0 & -\sqrt{\left(1-\frac{3\eta}{2}\right)\frac{\eta}{2}} & 0 \\ 0 & 0 & 0 & 0 \\ -\sqrt{\left(1-\frac{3\eta}{2}\right)\frac{\eta}{2}} & 0 & \frac{\eta}{2} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \end{aligned} \tag{4.48}$$

$$\sigma_E^{+,-} = \frac{1}{\eta}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{\eta}{2} & 0 & -\frac{\eta}{2} \\ 0 & 0 & 0 & 0 \\ 0 & -\frac{\eta}{2} & 0 & \frac{\eta}{2} \end{pmatrix},$$
$$\sigma_E^{-,+} = \frac{1}{\eta}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{\eta}{2} & 0 & \frac{\eta}{2} \\ 0 & 0 & 0 & 0 \\ 0 & \frac{\eta}{2} & 0 & \frac{\eta}{2} \end{pmatrix}, \tag{4.49}$$

Eve's quantum memory $\omega_E^{a,b}$ corresponding to the Alice and Bob's raw key bits a and b, respectively, generated from the blocks of size m can be computed using Eq. (4.37) and Eqs. (4.48), (4.49).

4.4.3 Secure key fraction and the noise-tolerance

Let us now denote the state of Eve's memory corresponding to Alice's bit x by Ω_E^x. The state Ω_E^x is calculated by projecting the state τ_{XYE} (given in Eq. (4.40)) into $|x\rangle\langle x|_X \otimes \mathbb{1}_Y \otimes \mathbb{1}_E$ and then tracing out X and Y as

$$\begin{aligned} \Omega_E^x &= \frac{\mathrm{Tr}_{XY}\left\{\left(|x\rangle\langle x|_X \otimes \mathbb{1}_Y \otimes \mathbb{1}_E\right)\tau_{XYE}\left(|x\rangle\langle x|_X \otimes \mathbb{1}_Y \otimes \mathbb{1}_E\right)\right\}}{\mathrm{Tr}\left\{\left(|x\rangle\langle x|_X \otimes \mathbb{1}_Y \otimes \mathbb{1}_E\right)\tau_{XYE}\left(|x\rangle\langle x|_X \otimes \mathbb{1}_Y \otimes \mathbb{1}_E\right)\right\}} \\ &= \frac{Q(x,0)\omega_E^{x,0} + Q(x,1)\omega_E^{x,1}}{Q(x,0)+Q(x,1)}. \end{aligned} \tag{4.50}$$

Here, $\omega_E^{x,y}$ are computed using Eqs. (4.37), (4.48), and (4.49). Note that for $x \in \{0,1\}$, $\Omega_E^x \in \mathcal{H}_E^{\otimes m}$ is a 4^m dimensional state and needs to be computed using a computer program. The mutual information between Alice and Bob is computed as

$$\mathcal{I}(A:B) = 1 - h(Q) \tag{4.51}$$

where

$$h(Q) = -Q\log_2 Q - (1-Q)\log_2(1-Q) \tag{4.52}$$

is the binary Shannon entropy for the bit error rate $Q = Q(0,1) + Q(1,0)$ in Alice and Bob's strings. Using Eq. (4.47), Q is given as

$$Q = \frac{\left(\frac{\eta}{2}\right)^m}{\left(\frac{1-\eta}{2}\right)^m + \left(\frac{\eta}{2}\right)^m} \tag{4.53}$$

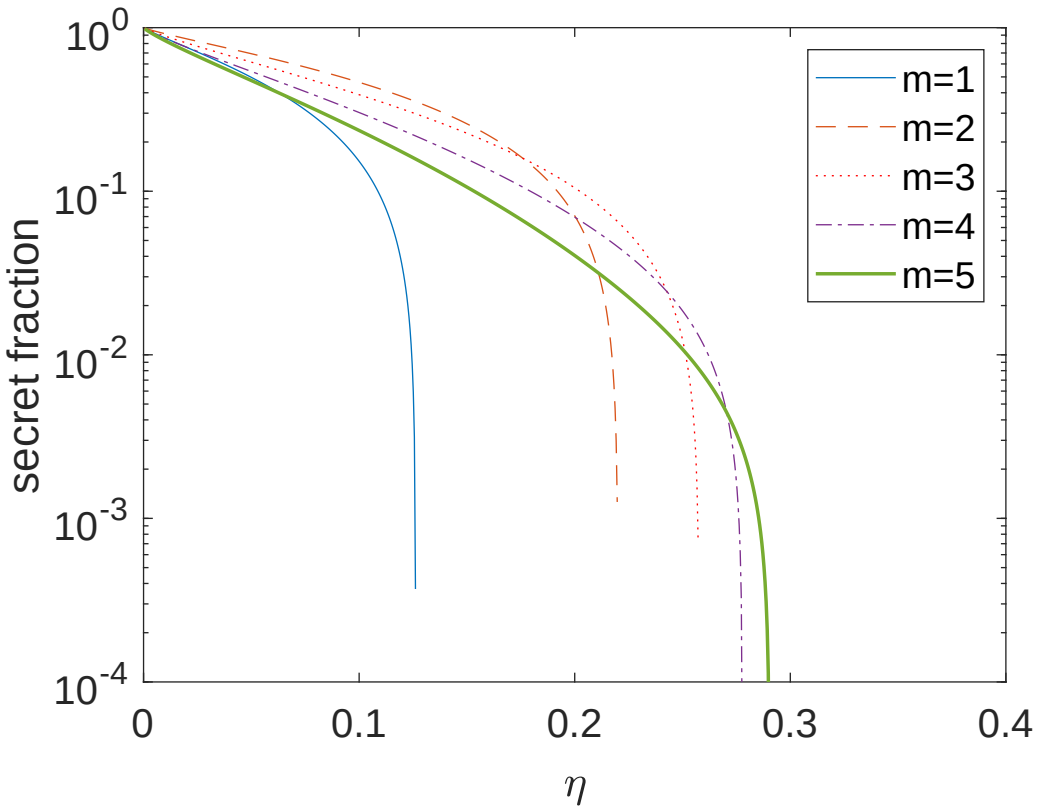


Figure 4.2: The secret fraction computed using the Devetak-Winter key rate formula for different block sizes.

The Holevo quantity corresponding to Eve's memory is given as

$$\chi(A:E) = S(\Omega_E) - \frac{1}{2}\left(S(\Omega_E^0) + S(\Omega_E^1)\right), \tag{4.54}$$

where $\Omega_E = \left(\Omega_E^0 + \Omega_E^1\right)/2$ and $S(\rho)$ is the von Neumann entropy of ρ. We computed the Devetak-Winter secure key fraction using Eqs. (4.42), (4.51) and (4.54). The secret fractions for different values of m are presented in Fig. 4.2. We evaluated the noise tolerance for varying block size and listed them in Table 4.1. The dimension of Eve's memory increases exponentially with m. Hence, the computation of Holevo quantity becomes difficult as m increases. Due to computational limitations, we could compute noise tolerance and secret key fraction only up to $m = 7$.

Table 4.1: Noise-tolerance for various block sizes.

m	1	2	3	4	5	6	7
η_{tol}	12.62%	22.01%	25.77%	27.78%	29.04%	29.90%	30.53%

4.5 Discussion and conclusion

In this chapter, we presented a QKD scheme based on block-wise processing. Our scheme increases the noise-tolerance by a significant margin with respect to the earlier protocols. Against collective attacks, our protocol can tolerate up to 30% of the depolarizing noise. Security is evaluated against collective attacks which are considered to be general attacks. The core assumptions that go into our security proof are the following: we assumed that the devices of Alice and Bob are fully trusted but the quantum channel is insecure. The labs of Alice and Bob are sealed and all operations corresponding to the discarding certain outcomes are done within the labs. The systems and devices used by both parties are identically and independently prepared (i.i.d. assumption) and the protocol rounds are repeated an asymptotically large number of times. Furthermore, all the permutations and the random variables are locally generated in the sealed labs. These are the usual assumptions for the trusted device QKD schemes. Our protocol appears complicated and hard to implement, however, it opens possibilities for the high noise-tolerance QKD. As a future prospect, it would be interesting to see the generalization of such methods to continuous variable QKD, and semi-device independent QKD. Another future prospect can be the finite-key analysis of our QKD scheme.

Chapter 5

A no-go theorem on restricted measurements and implications thereof

5.1 Introduction

The postulate of state description in quantum mechanics associates a Hilbert space to every closed quantum system and the states are represented by unit vectors in it. However, quantum theory does not tell us what the Hilbert space is for a given closed system [134]. Discovering a Hilbert space is not a trivial task. One pragmatic way to discover a Hilbert space associated with a closed quantum system is that an observable of the system is measured and all the distinguishable outcomes are considered to be orthogonal vectors spanning the space. For instance, energy levels of monochromatic electromagnetic radiation inside a cavity gives Hilbert space spanned by photon number states, or the measurement of magnetic dipole of silver atoms in the Stern–Gerlach experiment reveals the associated discrete Hilbert space of the angular momentum. Once the associated Hilbert space is identified, the arena of quantum mechanics for the corresponding closed quantum system is fixed. The postulate of composite systems tells us how to construct the Hilbert space associated with the closed composite systems when the Hilbert spaces associated with the component systems are known. If $\mathcal{H}_1$ and $\mathcal{H}_2$ are the Hilbert spaces associated with two closed quantum systems S_1 and S_2, respectively, then the space associated with the composite system is the tensor product $\mathcal{H}_1 \otimes \mathcal{H}_1$. If we look carefully, it is this postulate that underlies the phenomena of quantum entanglement and makes quantum theory universally applicable to any scale.

5. A no-go theorem on restricted measurements and implications thereof

One of the most intriguing feature of quantum theory is that it can treat every degree of freedom of a particle as an independent quantum system and associate a Hilbert space to it. For example, x, y and z coordinates form three different Hilbert spaces $\mathcal{H}_x$, $\mathcal{H}_y$, and $\mathcal{H}_z$ and the wave function of the particle is written in the composite Hilbert space $\mathcal{H}_x \otimes \mathcal{H}_y \otimes \mathcal{H}_z$. Here, three different spatial degrees of freedom of a quantum particle behave like they are three independent physical systems. Similarly, spatial and internal degrees of freedom can be treated as two separate systems. If the Hilbert spaces associated with the spatial degree of freedom and the spin of an electron are $\mathcal{H}_r$ and $\mathcal{H}_s$, respectively, then the Hilbert space associated with the composite system is $\mathcal{H}_r \otimes \mathcal{H}_s$.

Quantum mechanics allows manipulations on the internal degrees of freedom without involving the spatial degree of freedom. In other words, quantum states in Hilbert spaces associated with the internal degrees of freedom like spin of the electron or the energy levels of a hydrogen atom can be prepared, transformed and measured unrestricted without disturbing the spatial wave function of the system. Formally, we can apply operations of the form $\mathbb{1}_r \otimes \mathcal{T}_s$ on $\mathcal{H}_r \otimes \mathcal{H}_s$, where $\mathcal{T}_s$ is a valid quantum operation acting on $\mathcal{H}_s$. Such operations are trivial and have been used frequently in quantum literature.

In this chapter, we present a no-go theorem stating that the internal degree of freedom of quantum particles cannot be manipulated without introducing disturbance to the spatial wavefunctions. Our no-go theorem is implied by the no-faster-than speed of light communication principle. Formally, we show that operations of the form $\mathbb{1}_r \otimes \mathcal{T}_s$ on $\mathcal{H}_r \otimes \mathcal{H}_s$ can enable faster than speed of light communications and, hence, cannot be physically possible. Furthermore, we show that the no-go result has a very interesting implication in explaining the emergence of classical objectivity in the position basis. Quantum Darwinism and quantum decoherence paradigm attempt to explain objectivity withing the framework of standard quantum theory [135, 136, 137, 138, 139, 140]. However, all the previous works have considered oversimplified decoherence models which are considered to be far from practicality. For instance, the spin-spin interaction model assumes all the constituent subsystems of the environment are in pure and same state [135, 139]. The interactions are also considered to be of restricted forms. In addition, quantum Darwinism demands system-environment interaction to happen in a preferred system-basis [136]. In reality, the classical objectivity is seen to take place in the position basis all the time. To explain this, earlier works have considered dielectric sphere illumination model in which interaction with thermal photons localizes a dielectric sphere in the position basis [141, 142]. Our no-go result makes the position a universally preferred basis in all interactions. We show that random spin-spin interactions between environment and a system lead to emergence of objectivity in the position basis of the latter.

5.2 The no-go theorem and the proof

Special theory of relativity does not allow faster than speed of light communications. Speed of light is a fundamental constant of nature and it has been observed to be valid at all scales in the observed universe. All phenomena in classical mechanics are intrinsically local in the sense that all variables and observables of the theory remain completely undisturbed by space-like separated events. However, in quantum theory, we observe that collapse of a quantum state is non-local. In the famous Einstein-Bohr debate, Einstein introduced the notion of non-local collapse of the wavefunction of a quantum particle [143, 144]. He proposed a thought experiment where a particle is prepared in a superposition of wave packets localized at two spatially separated locations [145]. Detection of the particle at one location instantaneously collapses the wavefunction to nothing at the other location. In ψ-ontic theories, the wavefunction itself is an ontic variable *i.e*. it represents the reality. Therefore, the non-local collapses can steer the element of reality in space-like separated events. Einstein called it a spooky action at a distance [102].

The collapse of wavefunction is a faster than speed of light phenomena. This was later utilized in the famous Einstein–Podolsky–Rosen (EPR) paradox [143] that eventually led to discovery of Bell non-locality [20]. However, the non-local collapse of wavefunctions cannot be used to send information faster than speed of light [146]. The latter is ensured by the linear structure of the quantum theory and more generally by the no-signaling principle [147, 148]. According to the no-signaling principle, the statistics of a subsystem of a composite system remains undisturbed when local measurements are performed on the other subsystem. In simple words, an observer cannot use local measurements on a subsystem to send information to another observer who can have access to the other half of the composite system.

Here, we use no faster-than-light communication principle as a more general version of the no-signaling principle. We assume that quantum systems cannot be used for faster-than-light communication. Formally, we define our version of no signaling principle as follows.

Theorem 5.2.1. ***(The no faster-than-light communication principle)*** *Consider that Alice and Bob are two observers and they have black boxes* $\mathbf{A}$ *and* $\mathbf{B}$*, respectively, in their labs in such a way that* $\mathbf{A}$ *only takes inputs and* $\mathbf{B}$ *gives only outputs. Suppose Alice generates a random bit string* A *in the space-time region* E_A *and feed it into* $\mathbf{A}$ *as an input. Bob then generates a bit string* B *as an output from* $\mathbf{B}$ *in the space-time region* E_B*. If* E_A *and* E_B *are space-like separated then* $\mathfrak{I}(A:B)=0$*, where* $\mathfrak{I}(A:B)$ *is the mutual information between strings* A *and* B*.*

The mutual information quantifies the correlation between two strings. Theo-

rem 5.2.1 states that any locally and independently generated bit string is completely uncorrelated with any bit string that is generated in a space-like separated region. Freely generated information cannot be sent to space-like separated regions. Any black box scenario that violates Theorem 5.2.1 is physically impossible. We use this principle to show that internal degrees of freedom of a quantum particle cannot be manipulated without disturbing its spatial wavefunction. Formally, we prove the following theorem.

Theorem 5.2.2. ***(The no-go theorem)*** *Suppose $\mathcal{H}_S$ and $\mathcal{H}_I$ are the Hilbert spaces associated with the spatial and internal degrees of freedom of a quantum particle, respectively. Then,*

(a) Unitary operations of the form $U = \mathbb{1}_S \otimes U_I$ on the state space $\mathcal{H}_S \otimes \mathcal{H}_I$ are restricted by the no faster-than-light communication principle.

(b) Measurements of the form $\mathbb{M} = \{\mathbb{1}_S \otimes \Pi_I, \mathbb{1}_S \otimes \tilde{\Pi}_I\}$ on the state space $\mathcal{H}_S \otimes \mathcal{H}_I$ are restricted by the no faster-than-light communication principle, where Π_I and $\tilde{\Pi}_I$ are projection operators and $\Pi_I + \tilde{\Pi}_I = \mathbb{1}_I$.

Proof. We prove the theorem using contradiction. Consider, without loss of generality, that the internal degree of freedom is a two-level system. For simplicity, we consider an electron and its spin. Using gedanken experiments, we show that the operations mentioned in the theorem enable the faster-than-light communication. Suppose a single electron is prepared in a wavefunction that spreads over arbitrary large distances. Without loss of generality, we assume that the electron is prepared in a superposition of being in the labs of observers Alice and Bob who are stationed at $x = -\alpha$ and $x = \alpha$, respectively (see Fig. 5.1). Furthermore, the spin of the electron is prepared in the state $|0\rangle$. More specifically, the composite state of the electron describing its spatial degree of freedom and the spin is given by $|\Psi\rangle_{SI} = |\psi\rangle_S \otimes |0\rangle_I \in \mathcal{H}_S \otimes \mathcal{H}_I$, *s. th.*

$$\psi_S(x) = \langle x|\psi\rangle_S = N\left[\exp\left(-\frac{(x-\alpha)^2}{4\sigma^2}\right) + \exp\left(-\frac{(x+\alpha)^2}{4\sigma^2}\right)\right] \tag{5.1}$$

where N is a normalization constant and $\sigma \ll \alpha$. The wavefunction $\psi(x)$ is a superposition of two Gaussian wave packets, one of which is centered in Alice's lab while the other in Bob's lab. Here, we assume that the distance between the two labs is large *i.e.* $1 \ll \alpha$. Since the electron is spread over two labs, it can act as a long black box accessible to both observers. It is intriguing that quantum mechanics does not

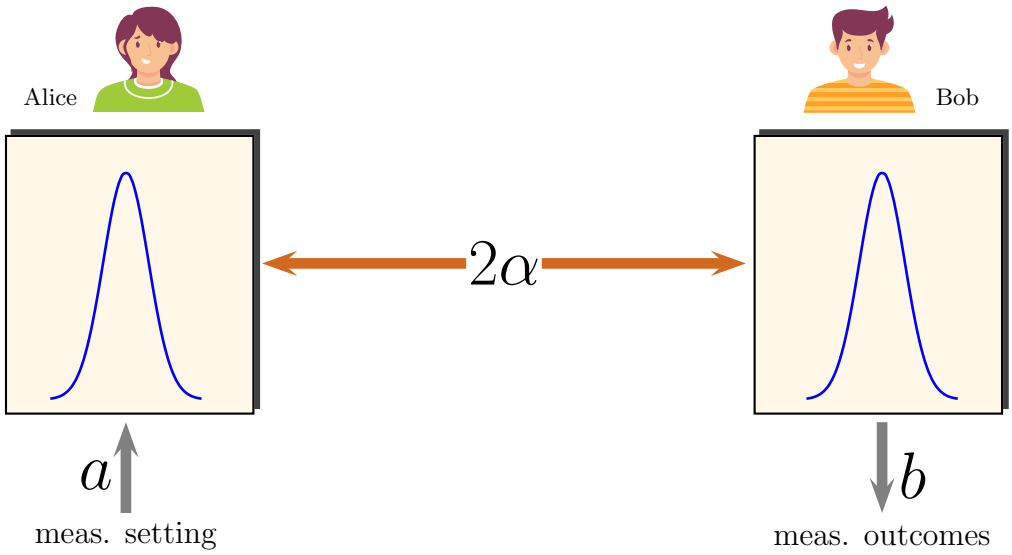


Figure 5.1: Alice and Bob are stationed in two laboratories separated by distance 2α. They share a common quantum particle which is simultaneously present in both laboratories. Alice chooses an operation based on randomly generated bit a and performs it on the internal degree of freedom of the particle. Bob performs a fixed measurement on the internal degree of freedom and registers the outcome as a bit b.

associate a sense of 'physical space' to the spin degree of freedom. Therefore, it is legitimate to assume that the spin of the electron is available where ever its wavefunction is non-vanishing. We use this setup to prove the theorem.

(a) Alice generates a uniformly random bit a as a message to send it to Bob. The quantum state representing the bit can be written as

$$\rho_A = \frac{1}{2} \sum_{a\in\{0,1\}} |a\rangle\langle a| \,. \tag{5.2}$$

The classical-quantum (cq) state of Alice's bit and the electron can be expressed as

$$\rho_{ASI} = \frac{1}{2} \sum_{a\in\{0,1\}} |a\rangle\langle a|_A \otimes |\psi\rangle\langle\psi|_S \otimes |0\rangle\langle 0|_I \,. \tag{5.3}$$

If Alice wants to send the bit a to Bob, she applies an operation U_a on the electron state $|\Psi\rangle_{SI}$, where

$$U_a = \begin{cases} \mathbb{1} \otimes \mathbb{1}; & \text{if } a = 0, \\ \mathbb{1} \otimes \sigma_x; & \text{if } a = 1, \end{cases} \tag{5.4}$$

The state after Alice's operation becomes

$$\rho'_{ASI} = \frac{1}{2} \sum_{a\in\{0,1\}} |a\rangle\langle a|_A \otimes |\psi\rangle\langle\psi|_S \otimes |a\rangle\langle a|_I \,. \tag{5.5}$$

Bob measures the operator σ_z on the electron and records the outcome as a bit $b \in \{0,1\}$. After tracing out electron wavefunction and its spin state, we have classical-classical (cc) state of Alice and Bob's bits as

$$\rho_{AB} = \frac{1}{2} \sum_{a,b\in\{0,1\}} |a\rangle\langle a|_A \otimes |a\rangle\langle a|_B \,. \tag{5.6}$$

Now assume that τ is the time difference between Alice's bit generation (call it event E_A) and Bob's act of recording his measurement outcome (event E_B) *s. th.* $c\tau \ll 2\alpha$, where c is the speed of light. From Eq. (5.6), the mutual information between A and B is $\mathcal{I}(A:B) = 1$. This contradicts the *no faster-than-light communication principle* (Theorem 5.2.1). Hence, the part (a) is proved.

(b) Similar to the previous case, Alice generates a bit $a \in \{0,1\}$, the state of which can be given by Eq. (5.2) and the cq-state of Alice's bit and electron is given by Eq. (5.3). To send bit $a = 0$, Alice performs $\mathbb{1}_S \otimes \mathbb{1}_I$ on the electron *i.e.* she does not disturb the electron state. To send the bit $a = 1$, she perform following measurement on the electron state $|\Psi\rangle_{SI}$,

$$\mathbb{M}_x = \{\mathbb{1} \otimes |+\rangle\langle+| \,, \mathbb{1} \otimes |-\rangle\langle-|\} \tag{5.7}$$

Note that measurement $\mathbb{M}_x$ is a measurement on the internal degree of freedom without disturbing the spatial wavefunction. The state after Alice's operation becomes

$$\rho'_{ASI} = \frac{1}{2} |0\rangle\langle 0|_A \otimes |\psi\rangle\langle\psi|_S \otimes |0\rangle\langle 0|_I + \frac{1}{4} |1\rangle\langle 1|_A \otimes |\psi\rangle\langle\psi|_S \otimes \sum_{k\in\{+,-\}} |k\rangle\langle k|_I \,. \tag{5.8}$$

Bob measures σ_z on the electron and records the outcome as a bit $b \in \{0,1\}$. After tracing out electron wavefunction and its spin state, we have classical-classical (cc) state of Alice and Bob's bits as

$$\rho_{AB} = \frac{1}{2} |0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B + \frac{1}{4} |1\rangle\langle 1|_A \otimes |1\rangle\langle 1|_B + \frac{1}{4} |1\rangle\langle 1|_A \otimes |0\rangle\langle 0|_B \tag{5.9}$$

Using Eq. (5.9), the mutual information between Alice and Bob is

$$\begin{aligned} \mathcal{I}(A:B) &= 1 - h\left(\frac{1}{4}\right) \\ &= 1 + \frac{1}{4}\log_2\frac{1}{4} + \frac{3}{4}\log_2\frac{3}{4} \\ &\approx 0.19 \end{aligned} \tag{5.10}$$

Suppose that the time difference between Alice's bit generation (the event E_A) and Bob's bit recording (the event E_B) is τ *s. th.* $c\tau \ll 2\alpha$ *i.e.* events E_A and E_B are space-like separated. Clearly, the result in Eq. (5.10) contradicts the *no faster-than-light communication principle* (Theorem 5.2.1). Hence, the part (b) is proved.

□

Remark 5.2.1. *We have only considered specific operations in our proof. However, the proof is valid without loss of generality. For instance, in case (a), we can choose the spin state in such a way that a given unitary acts as a bit flip operation. In our case we have only considered the state* $|0\rangle$ *and the unitary* σ_x*. Similarly, in case (b), for an arbitrary measurement setting* $\mathbb{M} \equiv \{\mathbb{1}\otimes\Pi, \mathbb{1}\otimes\tilde{\Pi}\}$*, we can prepare the spin in a state that belongs to a mutually unbiased basis to* $\{\Pi, \tilde{\Pi}\}$*. Bob then measures the spin in the preparation basis. In our proof, we have used the measurement* $\mathbb{M}_x$ *and, therefore, prepared the spin in* $|0\rangle$*.*

Our main argument is based on the assumption that the spin of the electron (or the internal degree of any quantum particle) is accessible at locations where ever the wavefunction is non-zero. Moreover, we implicitly assume that the internal degree has no association with the spatial degree of freedom and, thus, any manipulation at any point in space updates the spin-state at all points in the space and that is how Alice and Bob are able to signal. In order to make all operations spatially local, we need to include the notion of spatially localized quantum operations such as

$$U' = |-\alpha\rangle\langle-\alpha| \otimes \sigma_x + (\mathbb{1} - |-\alpha\rangle\langle-\alpha|) \otimes \mathbb{1}, \tag{5.11}$$

or measurement of the form

$$\mathbb{M}' \equiv \{|-\alpha\rangle\langle-\alpha| \otimes |+\rangle\langle+|\,, |-\alpha\rangle\langle-\alpha| \otimes |-\rangle\langle-|\,, (\mathbb{1} - |-\alpha\rangle\langle-\alpha|) \otimes \mathbb{1}\}\,. \tag{5.12}$$

Eqs. (5.11) and (5.12) incorporate the fact that manipulations on spin that take place inside Alice's lab do not disturb the spin in Bob's lab. It is easy to follow that such

operations do not violate the no faster-than-light communication principle. At first glance, Theorem 5.2.2 and its proof appear very trivial. However, our proof using no faster-than-light communication principle highlights a deeper aspect of the connection between the spatial wavefunction and the internal degree of freedom. Moreover, our theorem has established that no manipulations (unitary or measurements) on the internal degree can be performed without disturbing the spatial wavefunction. If operations of the form U or $\mathbb{M}$ (as specified in Theorem 5.2.2) are not permitted, it may be questioned what types of operations are permissible under the no faster-than-light communication principle. An accurate answer to this question may not be plausible here. However, we propose a possible solution which can be used in a crude way in certain physical scenarios to get interesting results.

Proposition 5.2.1. *Suppose an observer, localized at some position x, performs an operation $\mathcal{E}$ on the internal degree of freedom of a quantum particle, then*

(i) if $\mathcal{E}$ is a unitary U, the operation on the composite state of spatial and internal degrees of freedom is given by

$$\mathbb{U} = |x\rangle\langle x| \otimes U + (\mathbb{1} - |x\rangle\langle x|) \otimes \mathbb{1}.$$

(ii) if $\mathcal{E}$ is a measurement operation of the form $\{\Pi, \tilde{\Pi}\}$ s. th. $\Pi + \tilde{\Pi} = \mathbb{1}$, then the measurement on the composite state of spatial and internal degrees of freedom is given by

$$\mathbb{M} \equiv \left\{ |x\rangle\langle x| \otimes \Pi, |x\rangle\langle x| \otimes \tilde{\Pi}, (\mathbb{1} - |x\rangle\langle x|) \otimes \mathbb{1} \right\}.$$

Here, we have assumed that the observer is sharply localized at a position x. This is an unrealistic scenario. In a more practical situation, we can assume the effects of observer's action are reachable in a spatial region $x \pm \delta$. In that case, we can replace the projection operator $|x\rangle\langle x|$ by $\int_{x-\delta}^{x+\delta} |x'\rangle\langle x'| \, dx'$. So far, we have only considered the simple case of one dimensional spatial degree of freedom. However, the generalization to three dimensional space is straightforward and more realistic.

5.3 Implications in quantum Darwinism

Quantum Darwinism attempts to explain the emergence of classical reality from the underlying quantum world. The theory proposes that the environment plays a crucial role in selecting which quantum states are accessible to us as observers, leading

to the emergence of objective, classical reality. According to the theory, the environment continually monitors and records information about the quantum system, which is then redundantly imprinted on many different fragments in the environment. Multiple observers now can have access to separate fractions and gain information about the system (or the corresponding pointer) observable. Due to the redundant imprinting of the information, every observer has the same knowledge about the system. Such a wide availability of the information about the system is reflected in the emergence of classical reality that we all experience.

The framework of quantum Darwinism is based on concepts of quantum information theory and deals less with the dynamics of decoherence. However, the dynamical emergence of the objectivity demands strong constraints on the pointer-environment interaction Hamiltonian. The key result of quantum Darwinism is: if a sufficiently large number of observers have access to complete information about different observables of the pointer just by probing disjoint fragments of the environment, then their observables commute. In simpler words, different observers can only have complete information about a set of compatible observables of the pointer. Such a post-interaction structure can only emerge if the pointer-environment interaction singles out a preferred observable of the pointer. This leads to consideration of simplified decoherence models such as, the spin model with C-NOT or C-MAYBE interactions [149, 150], central spin decoherence with non-interacting spins [149, 151, 152, 153, 154, 155], quantum Brownian motion model [156], and illuminated dielectric sphere model [141, 142]. These models consider pointer-environment coupling in the pointer-observable basis. Additionally, the initial states of environment subsystems are assumed to be in pure and identical states, except for the illuminated dielectric sphere model where the environment is initially in a mixed state of optical plane waves. However, pointer-environment interactions remains controlled-unitary type with the assumption of symmetric environments in all models. These assumptions are strong and limit the applicability of quantum Darwinism to a specific set of decoherence mechanisms. In real world scenarios, environments can interact to a system with randomized interaction Hamiltonian. Such scenarios do not usually fulfill the required dynamical conditions for the quantum Darwinism.

Here, we preset a model where a randomized interaction Hamiltonian can produce effects of quantum Darwinism. In fact, we show that, as a direct consequence of our no-go theorem (Theorem 5.2.2), any random interactions between internal degrees of freedom of system and environment-subsystems result into emergence of objective reality in the position basis. This solves a long-standing problem in the decoherence paradigm.

Instead of using information theoretic approach established by W. H. Zurek and his collaborators [135, 136, 138, 140], we here use approach of structural broadcast

structure [157, 158] to show the emergence of objectivity in our decoherence model. Suppose an environment E is divided into fragments (collections of subsystems of E) $E_1, E_2, \cdots, E_n$ after its interaction with a system S in such a way that the joint state can be expressed as

$$\varrho_{S:E_n} = \sum_i p_i \left|i\right\rangle\!\left\langle i\right|_S \otimes \varrho_i^{E_1} \otimes \varrho_i^{E_2} \otimes \cdots \otimes \varrho_i^{E_n} \tag{5.13}$$

where $\{|i\rangle\}$ is some orthogonal basis in the system's Hilbert space, $\{p_i\}$ is a valid probability distribution and states $\varrho_i^{E_k}$ are perfectly distinguishable:

$$\varrho_i^{E_k} \varrho_j^{E_k} = 0 \;\; \forall i \neq j, \quad k = 1, 2, \cdots, n. \tag{5.14}$$

Then, $\varrho_{S:E_n}$ is called a spectrum broadcast structure. According to the main theorem proven in [157], the appearance of the spectral broadcast structure is a necessary and sufficient condition for objectivity. Here, eventually, we will show that arbitrary interactions between internal degrees of freedom of system and subsystems of environment lead to emergence of objectivity in the position basis.

5.3.1 Decoherence Model

The system S is a quantum particle that can be located only at d locations $\{\overrightarrow{x}_i\}_{i\in\{1,2,\cdots,d\}}$. Additionally, S has an internal degree of freedom described by states in a two dimensional Hilbert space denoted by $\mathcal{H}_S$. Suppose S is initially in the state:

$$\varrho_S = \left|\Psi\right\rangle\!\left\langle\Psi\right| \otimes \rho_S \tag{5.15}$$

where

$$\left|\Psi\right\rangle = \sum_{i=1}^{d} \alpha_i \left|\overrightarrow{x}_i\right\rangle, \tag{5.16}$$

s. th. $\sum_{i=1}^{d} \|\alpha_i\|^2 = 1$, $\langle\overrightarrow{x}_i|\overrightarrow{x}_j\rangle = \delta_{ij}$, and $\rho_S \in \mathcal{H}_S$ is the state of the internal degree of freedom that, we assume here, is the spin. The particle is assumed to be point-like or a sphere of an arbitrary small radius. Here, the particle is present in a superposition of all possible locations $\{\overrightarrow{x}_k\}_{k\in\{1,2,\cdots,d\}}$. The particle is surrounded by an environment E made of N subsystems. Here we consider that the subsystems of E are pin-$1/2$ point-like particles localized in the position space. We assume that the state of the k-th subenvironment E_k^{sub} before system-environment interaction is of the form:

$$\varrho_{E_k^{sub}} = \left|\psi_k\right\rangle\!\left\langle\psi_k\right| \otimes \rho_k \tag{5.17}$$

where $|\psi_k\rangle \in \{|\overrightarrow{x}_i\rangle\}_{i\in\{1,2,\cdots,d\}}$ and ρ_k is an arbitrary spin-$1/2$ state of E_k^{sub} before the interaction takes place. Note that unlike all the previous models, we do not make

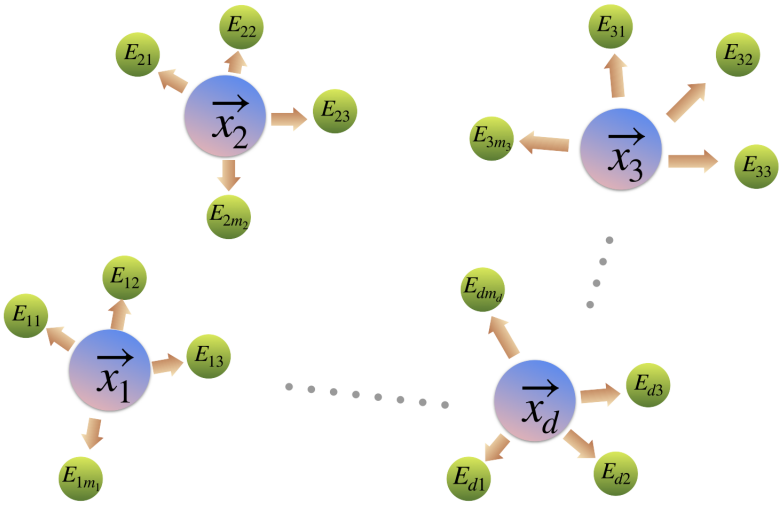


Figure 5.2: The system is in superposition of positions $\{x_i\}_{i=1,2,\cdots,d}$. Environment spins $\{E_{ij}\}$ are randomly located near positions $\{x_i\}$. E_{ij} is the j-th subenvironment near x_i. Random spin interactions take place between subenvironments and the system.

any assumption about the initial spin states of subenvironments. Our only assumption about the states of subenvironments is that they are well localized in the position space. Subenvironments can indeed be present at locations other than $\{\overrightarrow{x}_k\}_{k\in\{1,2,\cdots,d\}}$ but they do not interact with system S and, thus, play no role in the process of decoherence. It is noteworthy that $\{E_k^{sub}\}$ are present at random locations $\{\overrightarrow{x}_k\}_{k\in\{1,2,\cdots,d\}}$ and there can be multiple subenvironments present at a location. The initial state of the system plus environment is as usually assumed to be a product form:

$$\varrho_{S:E} = \varrho_S \otimes \varrho_{E_1^{sub}} \otimes \varrho_{E_2^{sub}} \otimes \varrho_{E_3^{sub}} \cdots \otimes \varrho_{E_N^{sub}} \tag{5.18}$$

Note that the state of E here is more general than the previous models where it is assumed to be of the form $(\varrho_{E^{sub}})^{\otimes N}$.

Let us now specify the interaction model. The subenvironment spins are assumed to be independent and do not interact with each other. Furthermore, the interactions between subenvironment spins and the spin of S are considered to be the most general and random. The latter is inspired by the fact that the environments in real scenarios are uncontrollable and random. All previous decoherence models in quantum Darwinism paradigm have assumed controlled-unitary interaction models where actions on the subenvironments are controlled by an unjustified preferred basis of the system

or pointer space. For instance, following form of interaction is considered in spin-interaction models assuming all subenvironment spins are initially in $|0\rangle$:

$$H_{S:E} = \sigma_z^S \otimes \sum_{i=1}^{N} g_i(t) \sigma_x^{E_i^{sub}} \bigotimes_{j \neq i} \mathbb{1}^{E_j^{sub}} \tag{5.19}$$

It is easy to visualize that $U_{S:E} = \exp\{-\iota \int H_{S:E} dt\}$, where $\iota = \sqrt{-1}$, is a series of unsharp von Neumann interactions with varying strength $\epsilon_i = \int g_i(t) dt$ where the subenvironments $\{E_i^{sub}\}$ play the role of ancilla qubits. Furthermore, it can be argued that $U_{S:E}$ is a sequential unsharp measurement of σ_z spin on the system S. Therefore, the emergence of objectivity in z-basis is expected. Thus, the form of $U_{S:E}$ in Eq. (5.19) is a strong assumption. It was also argued that a preferred basis-interaction is required for the emergence of Darwinian structure. Showing emergence of objectivity for arbitrary interaction is still a challenging problem.

In our model we assume the most general spin-spin interaction model where spin of S has arbitrary interactions with $\{E_i^{sub}\}$:

$$H_{S:E} = -\sum_{i=1}^{N} g_i(t) \sigma_i^S \otimes \sigma^{E_i^{sub}} \bigotimes_{j \neq i} \mathbb{1}^{E_j^{sub}} \tag{5.20}$$

where $\sigma_i^S = \hat{a}_i \cdot \sigma$, $\sigma^{E_i^{sub}} = \hat{b}_i \cdot \sigma$ and $\hat{a}_i, \hat{b}_i$ are random unit vectors in the physical space. Every subenvironment in this model interacts with the system differently. Here we assume that subenvironments do not interact with each others. We will show that the system becomes objective in the position basis when Theorem 5.2.2 is taken into account.

5.3.2 Formation of the broadcast structure

Let the state spaces associated with the position and the spin of E_k^{sub} be $\mathcal{H}_k^x$ and $\mathcal{H}_k$, respectively. Clearly, the initial state $\varrho_{E_k^{sub}} \in \mathcal{H}_k^x \otimes \mathcal{H}_k$. The composite state space of system plus environment is:

$$\mathcal{H}_{S:E} = (\mathcal{H}_S^x \otimes \mathcal{H}_S) \otimes (\mathcal{H}_1^x \otimes \mathcal{H}_1) \otimes (\mathcal{H}_2^x \otimes \mathcal{H}_2) \otimes \cdots \otimes (\mathcal{H}_N^x \otimes \mathcal{H}_N), \tag{5.21}$$

where $\mathcal{H}_S^x$ is the space associated with the position of S. According to Theorem 5.2.2, any interaction between S and a subenvironment must be mediated by the spatial degree of freedom. Therefore, the interaction unitary between S and E_k^{sub} has the form

in the rearranged space $\mathcal{H}_S^x \otimes \mathcal{H}_1^x \otimes \mathcal{H}_S \otimes \mathcal{H}_k$:

$$\begin{aligned}\bar{U}_{S:E_k^{sub}} = &\sum_{i=j} |\overrightarrow{x}_i\rangle\langle\overrightarrow{x}_i|_S \otimes |\overrightarrow{x}_j\rangle\langle\overrightarrow{x}_j|_{E_k^{sub}} \otimes U^{x_i}_{S:E_k^{sub}} \\ &+ \sum_{i\neq j} |\overrightarrow{x}_i\rangle\langle\overrightarrow{x}_i|_S \otimes |\overrightarrow{x}_j\rangle\langle\overrightarrow{x}_j|_{E_k^{sub}} \otimes \mathbb{1}\end{aligned} \tag{5.22}$$

where

$$U^{x_i}_{S:E_k^{sub}} = \exp\left\{\iota\sigma^S_{k,x_i} \otimes \sigma^{E_k^{sub}}_{x_i} \int g^{x_i}_k(t)dt\right\} \tag{5.23}$$

is a unitary operation acting over the space $\mathcal{H}_S \otimes \mathcal{H}_k$ with arbitrary spin operators σ^S_{k,x_i} and $\sigma^{E_k^{sub}}_{x_i}$. The position dependencies of spin operators signifies that the factors which determine the interaction between the system and subenvironments at a location $\overrightarrow{x}_i$ are local and random. Note that this condition is an implication of the Theorem 5.2.2 rather an assumption. The complete interaction between the system and environment can now be expressed as:

$$\bar{U}_{S:E} = \prod_{k=1}^{N} \bar{U}_{S:E_k^{sub}} \bigotimes_{j\neq k} \mathbb{1}^{E_j^{sub}}, \tag{5.24}$$

where $\mathbb{1}^{E_j^{sub}}$ is identity over $\mathcal{H}_j^x \otimes \mathcal{H}_j$. Since we have assumed localized subenvironments in our model (see Eq. 5.17), we can rearrange the state of environment (specified in Eq. 5.18) depending on the position of subenvironments $\{E_i^{sub}\}$ as

$$\begin{aligned}\varrho_E = &\underbrace{(|\overrightarrow{x_1}\rangle\langle\overrightarrow{x_1}| \otimes \rho_1^{x_1}) \otimes (|\overrightarrow{x_1}\rangle\langle\overrightarrow{x_1}| \otimes \rho_2^{x_1}) \otimes \cdots \otimes \left(|\overrightarrow{x_1}\rangle\langle\overrightarrow{x_1}| \otimes \rho_{m_1}^{x_1}\right)}_{\varrho_1^{mac}} \\ &\otimes \underbrace{(|\overrightarrow{x_2}\rangle\langle\overrightarrow{x_2}| \otimes \rho_1^{x_2}) \otimes (|\overrightarrow{x_2}\rangle\langle\overrightarrow{x_2}| \otimes \rho_2^{x_2}) \otimes \cdots \otimes \left(|\overrightarrow{x_2}\rangle\langle\overrightarrow{x_2}| \otimes \rho_{m_2}^{x_2}\right)}_{\varrho_2^{mac}} \otimes \cdots \\ &\otimes \underbrace{(|\overrightarrow{x_d}\rangle\langle\overrightarrow{x_d}| \otimes \rho_1^{x_d}) \otimes (|\overrightarrow{x_d}\rangle\langle\overrightarrow{x_d}| \otimes \rho_2^{x_d}) \otimes \cdots \otimes \left(|\overrightarrow{x_d}\rangle\langle\overrightarrow{x_d}| \otimes \rho_{m_d}^{x_d}\right)}_{\varrho_d^{mac}} \\ &\equiv \varrho_1^{mac} \otimes \varrho_2^{mac} \otimes \cdots \otimes \varrho_d^{mac}.\end{aligned} \tag{5.25}$$

Here, we assume that m_k subenvironments are localized at position $\overrightarrow{x}_k$ *s. th.* $\sum_k m_k = N$. The subenvironments localized at $\overrightarrow{x}_k$ form a macroscopic fraction of the environment specified by the state ϱ_k^{mac}. State $\varrho_{S:E}$ can be written using Eq. (5.25):

$$\begin{aligned}\varrho_{S:E} &= \varrho_S \otimes \varrho_1^{mac} \otimes \varrho_2^{mac} \otimes \cdots \otimes \varrho_d^{mac} \\ &= \left(\sum_{i,j} \alpha_i\alpha_j^* |\overrightarrow{x}_i\rangle\langle\overrightarrow{x}_j| \otimes \rho\right)_S \otimes \varrho_1^{mac} \otimes \varrho_2^{mac} \otimes \cdots \otimes \varrho_d^{mac}\end{aligned} \tag{5.26}$$

Let us assume without loss of generality that the system interacts with macroscopic fractions one by one in the order $E_1^{mac}, E_2^{mac}, \cdots, E_d^{mac}$. Furthermore, let E_{ij}^{sub} denote the j-th subenvironment in the fraction E_i^{mac}. Clearly, the initial state of $E_{ij}^{sub} \in \left\{E_k^{sub}\right\}_{k=1,2,\cdots,N}$ is $|\overrightarrow{x}_i\rangle\langle\overrightarrow{x}_i| \otimes \rho_j^{x_i}$ (see Eq. (5.25)). Without loss of generality, we can assume that subenvironments interact with the system one by one within a macroscopic fraction. The interaction unitary $\bar{U}_{S:E_{11}^{sub}}$ transforms the system plus environment state as

$$\begin{aligned}\varrho_{S:E} \quad \xrightarrow{\bar{U}_{S:E_{11}^{sub}}} \quad & \|\alpha_1\|^2 |\overrightarrow{x}_1\rangle\langle\overrightarrow{x}_1|_S \otimes |\overrightarrow{x}_1\rangle\langle\overrightarrow{x}_1|_{E_{11}^{sub}} \otimes \\ & \left(U_{S:E_{11}^{sub}}^{x_1}\right) \rho_{S:E_{11}} \left(U_{S:E_{11}^{sub}}^{x_1}\right)^\dagger \bigotimes_{E_{ij\neq 11}^{sub}} \varrho_{E_{ij}^{sub}} \\ & + \sum_{k,l\neq 1} \alpha_k \alpha_l^* |\overrightarrow{x}_k\rangle\langle\overrightarrow{x}_l|_S \otimes |\overrightarrow{x}_1\rangle\langle\overrightarrow{x}_1|_{E_{11}} \otimes \\ & \rho_{S:E_{11}} \bigotimes_{E_{ij\neq 11}^{sub}} \varrho_{E_{ij}^{sub}}\end{aligned} \tag{5.27}$$

where we used the notation $\rho_{S:E_{ij}} \equiv \rho_S \otimes (\rho_j^{x_i})_{E_{ij}^{sub}}$. Let us denote

$$\begin{aligned}\bar{U}_{S:E_k^{mac}} &= \bar{U}_{S:E_{km_1}^{sub}} \cdots \bar{U}_{S:E_{k2}^{sub}} \bar{U}_{S:E_{k1}^{sub}}, \\ U_{S:E_k^{mac}}^{x_k} &= U_{S:E_{km_1}^{sub}}^{x_k} \cdots U_{S:E_{k2}^{sub}}^{x_k} U_{S:E_{k1}^{sub}}^{x_k},\end{aligned} \tag{5.28}$$

and

$$\rho_{S:E_k^{mac}} = \rho_S \bigotimes_{l=1}^{m_k} (\rho_l^{x_k})_{E_{kl}^{sub}}. \tag{5.29}$$

Let us now evaluate the state after all interactions. The interaction $\bar{U}_{S:E_1^{mac}}$ transforms $\varrho_{S:E}$ into:

$$\begin{aligned}\varrho_{S:E} \quad \xrightarrow{\bar{U}_{S:E_1^{mac}}} \quad & \|\alpha_1\|^2 |\overrightarrow{x}_1\rangle\langle\overrightarrow{x}_1|_S \otimes \left(|\overrightarrow{x}_1\rangle\langle\overrightarrow{x}_1|^{\otimes m_1}\right)_{E_1^{mac}} \\ & \otimes \left(U_{S:E_1^{mac}}^{x_1}\right) \rho_{S:E_1^{mac}} \left(U_{S:E_1^{mac}}^{x_1}\right)^\dagger \bigotimes_{E_{k\neq 1}^{mac}} \varrho_{E_k^{mac}} \\ & + \sum_{k,l\neq 1} \alpha_k \alpha_l^* |\overrightarrow{x}_k\rangle\langle\overrightarrow{x}_l|_S \otimes \left(|\overrightarrow{x}_1\rangle\langle\overrightarrow{x}_1|^{\otimes m_1}\right)_{E_1^{mac}} \\ & \otimes \rho_{S:E_1^{mac}} \bigotimes_{E_{k\neq 1}^{mac}} \varrho_{E_k^{mac}}\end{aligned} \tag{5.30}$$

It is easy to evaluate that the series of unitary operations $\bar{U}_{S:E_1^{mac}}, \bar{U}_{S:E_2^{mac}}, \cdots, \bar{U}_{S:E_d^{mac}}$ gives,

$$\begin{aligned}\varrho'_{S:E} &= \left(\bar{U}_{S:E}\right) \varrho_{S:E} \left(\bar{U}_{S:E}\right)^\dagger \\ &= \sum_{i=1}^{d} \|\alpha_1\|^2 \, |\overrightarrow{x}_i\rangle\langle\overrightarrow{x}_i|_S \otimes \left(|\overrightarrow{x}_i\rangle\langle\overrightarrow{x}_i|^{\otimes m_i}\right)_{E_i^{mac}} \\ &\quad \otimes \left(U^{x_i}_{S:E_i^{mac}}\right) \rho_{S:E_i^{mac}} \left(U^{x_i}_{S:E_i^{mac}}\right)^\dagger \bigotimes_{E^{mac}_{k\neq i}} \varrho_{E_k^{mac}}\end{aligned} \tag{5.31}$$

After tracing out the spatial degree of freedom of the subenvironments, we have

$$\begin{aligned}\varrho'_{S:E} &= \sum_{i=1}^{d} \|\alpha_i\|^2 \, |\overrightarrow{x}_i\rangle\langle\overrightarrow{x}_i|_S \otimes \left(U^{x_i}_{S:E_i^{mac}}\right) \rho_{S:E_i^{mac}} \left(U^{x_i}_{S:E_i^{mac}}\right)^\dagger \bigotimes_{E^{mac}_{k\neq i}} \rho_{E_k^{mac}} \\ &\equiv \sum_{i=1}^{d} \|\alpha_i\|^2 \, |\overrightarrow{x}_i\rangle\langle\overrightarrow{x}_i|_S \otimes \rho'_{S:E_i^{mac}} \bigotimes_{E^{mac}_{k\neq i}} \rho_{E_k^{mac}},\end{aligned} \tag{5.32}$$

where $\rho'_{S:E_i^{mac}}$ is the post-interaction state of system plus i-th macro-environment spin. Since $\rho'_{S:E_i^{mac}}$ is generated by random interactions, the derivation of the general form of $\rho'_{S:E_i^{mac}}$ is highly nontrivial and unimportant. State $\varrho'_{S:E}$ reduces to spectrum broadcast structure when a sufficiently large fraction of the environment is traced out. The proof of the latter is difficult due to generality of the randomized interactions and, therefore, not in scope of this thesis. However, the emergence of Born probabilities $\{\|\alpha_i\|^2\}$ is already visible in Eq. (5.32). Nonetheless, we show the formation of broadcast structure for an specific case.

Suppose the spin of the system is initially in maximally mixed state *i.e.* $\rho_S = \frac{\mathbb{1}_S}{2}$. Let $\rho^{(k)}_{S:E_i^{mac}}$ denote the state of system plus i-th macro-environment after interaction with k subenvironments:

$$\rho^{(k)}_{S:E_i^{mac}} = \left(U^{x_i}_{S:E_{ik}^{sub}} \cdots U^{x_i}_{S:E_{i2}^{sub}} U^{x_i}_{S:E_{i1}^{sub}}\right) \rho^{S:E_i^{mac}} \left(U^{x_i}_{S:E_{ik}^{sub}} \cdots U^{x_i}_{S:E_{i2}^{sub}} U^{x_i}_{S:E_{i1}^{sub}}\right)^\dagger. \tag{5.33}$$

Note that $\rho^{(m_i)}_{S:E_i^{mac}} = \rho'_{S:E_i^{mac}}$. From Eq. (5.23), we have

$$U^{x_i}_{S:E_{ij}^{sub}} = \left(\cos(\theta_{ij})\mathbb{1}_S \otimes \mathbb{1}_{E_{ij}^{sub}} + \iota \sin(\theta_{ij}) \sigma^S_{j,x_i} \otimes \sigma_{x_i}^{E_{ij}^{sub}}\right) \bigotimes_{k\neq j} \mathbb{1}_{E_{ik}^{sub}}, \tag{5.34}$$

where we have denoted $\theta_{ij} = \int g_j^{x_i}(t)dt$. Using Eq. (5.34), we obtain

$$\begin{aligned}\rho^{(1)}_{S:E_i^{mac}} &= \left(U^{x_i}_{S:E_{i1}^{sub}}\right) \rho_{S:E_i^{mac}} \left(U^{x_i}_{S:E_{i1}^{sub}}\right)^\dagger \\ &= \left(\frac{\mathbb{1}}{2} \otimes \omega_1^{x_i} + \Omega_1^{x_i}\right)_{S:E_{i1}^{sub}} \bigotimes_{j\neq 1} \left(\rho_j^{x_i}\right)_{E_{ij}^{sub}}\end{aligned} \tag{5.35}$$

where

$$\begin{aligned}\omega_1^{x_i} &= \left(\cos^2(\theta_{i1})\rho_1^{x_i} + \sin^2(\theta_{i1})\sigma_{x_i}^{E_{i1}^{sub}}\rho_1^{x_i}\sigma_{x_i}^{E_{i1}^{sub}}\right) \\ &\equiv \left(\cos^2(\theta_{i1})\rho_1^{x_i} + \sin^2(\theta_{i1})\tilde{\rho}_1^{x_i}\right), \\ \Omega_{S:E_{i1}^{sub}} &= \iota\sin(2\theta_{i1})\frac{\sigma_{1,x_i}^{S}}{2}\otimes\frac{\sigma_{x_i}^{E_{i1}^{sub}}\rho_1^{x_i} - \rho_1^{x_i}\sigma_{x_i}^{E_{i1}^{sub}}}{2}.\end{aligned} \tag{5.36}$$

Note that $\mathrm{Tr}\{\omega_1^{x_i}\} = 1$ and $\mathrm{Tr}_S\left(\left(\Omega_1^{x_i}\right)_{S:E_{i1}^{sub}}\right) \equiv 0$. Similarly,

$$\begin{aligned}\rho_{S:E_i^{mac}}^{(2)} &= \left(U_{S:E_{i2}^{sub}}^{x_i}\right)\rho_{S:E_i^{mac}}^{(1)}\left(U_{S:E_{i2}^{sub}}^{x_i}\right)^{\dagger} \\ &= \left(\frac{\mathbb{1}}{2}\otimes\omega_1^{x_i}\otimes\omega_2^{x_i} + \Omega_2^{x_i}\right)_{S:E_{i1}^{sub}E_{i2}^{sub}}\bigotimes_{j\neq 1,2}\left(\rho_j^{x_i}\right)_{E_{ij}^{sub}}\end{aligned} \tag{5.37}$$

where

$$\begin{aligned}\omega_2^{x_i} &= \left(\cos^2(\theta_{i2})\rho_2^{x_i} + \sin^2(\theta_{i2})\sigma_{x_i}^{E_{i2}^{sub}}\rho_2^{x_i}\sigma_{x_i}^{E_{i2}^{sub}}\right) \\ &\equiv \left(\cos^2(\theta_{i2})\rho_2^{x_i} + \sin^2(\theta_{i2})\tilde{\rho}_2^{x_i}\right),\end{aligned} \tag{5.38}$$

and $\left(\Omega_2^{x_i}\right)_{S:E_{i1}^{sub}E_{i2}^{sub}}$ is a traceless operator. More specifically, we have

$$\mathrm{Tr}_S\left(\left(\Omega_2^{x_i}\right)_{S:E_{i1}^{sub}E_{i2}^{sub}}\right) \equiv 0. \tag{5.39}$$

It is straightforward that

$$\rho'_{S:E_i^{mac}} = \left(\frac{\mathbb{1}_S}{2}\bigotimes_j\left(\omega_j^{x_i}\right)_{E_{ij}^{sub}} + \left(\Omega_2^{x_i}\right)_{S:E_i^{mac}}\right), \tag{5.40}$$

s. th.

$$\mathrm{Tr}_S\left(\left(\Omega_j^{x_i}\right)_{S:E_i^{mac}}\right) \equiv 0. \tag{5.41}$$

and

$$\omega_j^{x_i} = \cos^2(\theta_{ij})\rho_j^{x_i} + \sin^2(\theta_{ij})\tilde{\rho}_j^{x_i}, \tag{5.42}$$

where

$$\tilde{\rho}_j^{x_i} = \sigma_{x_i}^{E_{ij}^{sub}}\rho_j^{x_i}\sigma_{x_i}^{E_{ij}^{sub}}. \tag{5.43}$$

After tracing out system's spin, we obtain

$$\rho'_{E_i^{mac}} = \left(\omega_1^{x_i}\right)_{E_{i1}^{sub}}\otimes\left(\omega_2^{x_i}\right)_{E_{i2}^{sub}}\otimes\cdots\otimes\left(\omega_{m_i}^{x_i}\right)_{E_{im_i}^{sub}}. \tag{5.44}$$

Using Eqs. (5.32) and (5.44), we obtain the post-interaction state of the system's spatial degree of freedom and the environment-spins as:

$$\varrho'_{S:E} = \sum_{i=1}^{d}\|\alpha_i\|^2\,|\overrightarrow{x}_i\rangle\langle\overrightarrow{x}_i|_S\otimes\rho'_{E_i^{mac}}\bigotimes_{E_{k\neq i}^{mac}}\rho_{E_k^{mac}}. \tag{5.45}$$

Remember that the spatial degrees of freedom of subenvironments and spin of the system are traced out. As we will see, Eq. (5.45) is a spectrum broadcast structure where the information of about the system's position is redundantly imprinted on multiple fragments of environment-spins. Since we have discarded the spatial degrees of freedom of all the subenvironments, our environment E consists of only subenvironment-spins hereafter. Let us now divide E into fragments $F_1, F_2, \cdots, F_n$ in such a way that F_k for all $k \in \{1, 2, \cdots, n\}$ has randomly chosen subenvironments from all macro-environments $\{E_j^{mac}\}_{j\in\{1,2,\cdots,d\}}$. This can be easily achieved by applying a random permutation on all subenvironment-spins in Eq. (5.45) and then dividing them into n fragments of equal size. In this way have fragments consisting of asymptotically $l = N/n$ subenvironments. Let us denote the post-interaction state of the environment corresponding to the system's position $\overrightarrow{x}_i$ by

$$\Xi_i^E = \rho'_{E_i^{mac}} \bigotimes_{E_{k\neq i}^{mac}} \rho_{E_k^{mac}}. \tag{5.46}$$

With re-indexing (as in Eq. (5.18)), the state Ξ_i^E can be rewritten as:

$$\Xi_i^E = \rho_1 \otimes \rho_2 \otimes \cdots \otimes \underbrace{\rho'_{s+1} \otimes \rho'_{s+2} \otimes \rho'_{s+3} \cdots \otimes \rho'_{s+m_i}}_{\rho'_{E_i^{mac}}} \otimes \rho_{s+m_i+1} \otimes \cdots \otimes \rho_N, \tag{5.47}$$

where ρ_j and ρ'_j are the initial and the post-interaction states of the j-th subenvironment, respectively. States $\{\rho'_j\}$ are specified by Eq. (5.42) *i.e.* we can write

$$\rho'_j = \cos^2(\theta_j)\rho_j + \sin^2(\theta_j)\tilde{\rho}_j, \tag{5.48}$$

where θ_j is a random angle and $\tilde{\rho}_j = \sigma_j\rho_j\sigma_j$ *s. th.* σ_j is a random spin operator. Therefore, $\tilde{\rho}_j$ is also a valid density matrix. After a random shuffling (permutation) and re-indexing on the subenvironments, we obtain

$$\begin{aligned}\Xi_i^E =& \underbrace{\rho_1 \otimes \rho'_2 \otimes \rho_3 \cdots}_{F_1} \otimes \underbrace{\rho'_{r+1} \otimes \rho'_{r+2} \otimes \rho_{r+3} \cdots}_{F_2} \otimes \underbrace{\rho'_{s+1} \otimes \rho_{s+2} \otimes \rho'_{s+3} \cdots}_{F_3} \\ & \otimes \underbrace{\rho'_{t+1} \otimes \rho_{t+2} \otimes \rho_{t+3} \cdots}_{F_n} \\ \equiv& \xi_i^{F_1} \otimes \xi_i^{F_2} \otimes \xi_i^{F_3} \otimes \cdots \otimes \xi_i^{F_n}\end{aligned} \tag{5.49}$$

where $\xi_i^{F_k}$ is the state of k-th fragment corresponding to the system's position $\overrightarrow{x}_i$. Note that $\xi_i^{F_k}$ has multiple disturbed (post-interaction) and undisturbed (initial) subenvironment spins in the product state. Eq. (5.45) can now be re-expressed as:

$$\varrho'_{S:E} = \sum_{i=1}^{d} \|\alpha_i\|^2 \, |\overrightarrow{x}_i\rangle\langle\overrightarrow{x}_i|_S \otimes \xi_i^{F_1} \otimes \xi_i^{F_2} \otimes \xi_i^{F_3} \otimes \cdots \otimes \xi_i^{F_n}. \tag{5.50}$$

Let us now prove that states $\xi_i^{F_k}$ are perfectly distinguishable *i.e.*

$$\xi_i^{F_k}\xi_j^{F_k} = 0 \,\forall\, i \neq j, \quad k = 1, 2, 3, \cdots, n, \tag{5.51}$$

or equivalently, the fidelity of states $\xi_i^{F_k}$ and $\xi_j^{F_k}$ for $i \neq j$ is zero:

$$\mathcal{F}\left(\xi_i^{F_k}, \xi_j^{F_k}\right) = 0 \tag{5.52}$$

where the fidelity of two density matrices ρ and σ is defined as

$$\mathcal{F}(\rho, \sigma) = \mathrm{Tr}\,\sqrt{\rho^{1/2}\sigma\rho^{1/2}}. \tag{5.53}$$

Fidelity $\mathcal{F}$ is multiplicative under tensor products:

$$\mathcal{F}(\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2) = \mathcal{F}(\rho_1, \sigma_1)\,\mathcal{F}(\rho_2, \sigma_2). \tag{5.54}$$

Since the fidelity for same states is one *i.e.* $\mathcal{F}(\rho, \rho) = 1$, we obtain

$$\mathcal{F}\left(\xi_i^{F_k}, \xi_j^{F_k}\right) = \prod_{u \in \mathbb{F}_{ij}^k} \mathcal{F}(\rho_u, \rho_u'), \tag{5.55}$$

where $\mathbb{F}_{ij}^k$ is the set of subenvironments in the fraction F_k *s. th.* their states corresponding to $\overrightarrow{x}_i$ and $\overrightarrow{x}_j$ are unequal. It is easy to verify that one of the states is the initial state while the other one has the form specified by Eq. (5.48). Since $\rho_u \neq \rho_u' \,\forall u \in \mathbb{F}_{ij}^k$, we can assume without loss of generality that

$$\mathcal{F}(\rho_u, \rho_u') = 1 - \varepsilon_u, \tag{5.56}$$

where $0 \leq \varepsilon_u < 1$. Therefore, in the asymptomatic case where the size of the environment is infinitely large, we have

$$\mathcal{F}\left(\xi_i^{F_k}, \xi_j^{F_k}\right) = 0 \quad \forall\, i \neq j, \quad k = 1, 2, 3, \cdots, n. \tag{5.57}$$

This proves our main claim.

5.4 Discussion and conclusion

In this chapter, beginning with no faster-than-light communication principle we have proved a no-go theorem according to which all interactions are mediated by spatial degree of freedom. More specifically, interactions in the internal degree of freedom

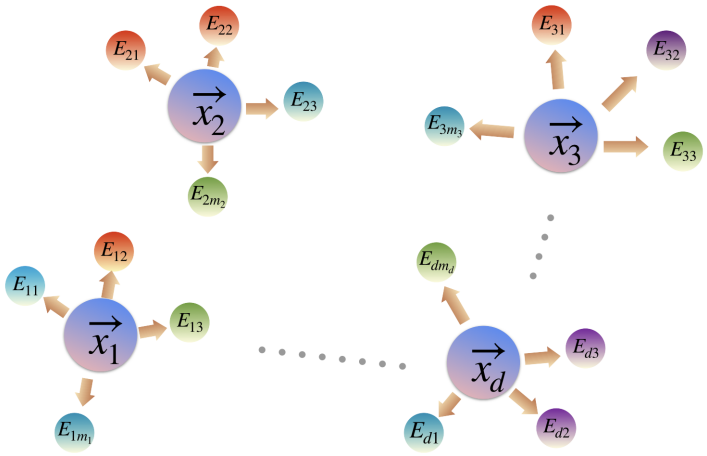


Figure 5.3: The system is in superposition of positions $\{x_i\}_{i=1,2,\cdots,d}$. Environment spins $\{E_{ij}\}$ are randomly located near positions $\{x_i\}$. Subenvironments with the same color constituent a fragment F. For example, all subenvironments in red are part of a fragment F_j, in green form F_k and so on.

are localized in the position basis. Due to this the internal degrees of freedom cannot be measured or manipulated without disturbing the spatial degree of freedom.

Our result can be interpreted using many world interpretation: suppose a system has a spatial wavefunction $\psi(x)$ and the state corresponding to the internal degree of freedom (spin) is $|\phi\rangle$. In many world interpretation, there exists infinitely many worlds each corresponding to a different position x. When the system interacts with another system located at some position x', the spin in only the world where the particle is located at x' interacts with the spin of another particle. In this way, the branching takes place only in the position basis. It naturally asserts that all valid transformations must always be written carefully taking the spatial degree of freedom into account.

We then applied the no-go result in a decoherence model to demonstrate the generic emergence of objectivity in the position basis. So far only a set of specific decoherence models have been studied in the decoherence paradigm to demonstrate quantum Darwinism and consequently the emergence of objectivity. These models are over simplified and far from practical. Another shortcoming is that they do not explain emergence of objectivity in the position basis. In this chapter, we have considered most general form of spin interactions and using our no-go theorem we could show the emergence of objectivity in the position basis. A point-like particle initially in superposition at different locations leaves redundant imprinting of the information about the

position on environment fragments made of spins. More specifically, we showed that randomized spin interactions generate a spectrum broadcast structure in the position basis. Our results show that position basis is special and preferred by nature.

Chapter 6

Demonstration of wave-particle complementarity using von Neumann measurements

6.1 Introduction

Wave-particle complementarity is a fundamental concept in quantum mechanics that explores the dual nature of particles and waves [32, 35]. It arises from the realization that at the microscopic level, matter and energy can exhibit both particle-like and wave-like behavior, depending on how they are observed or measured. This concept challenges our classical intuition and forms the basis of the wave-particle duality principle.

According to wave-particle complementarity, particles such as electrons, photons, or even larger objects like atoms, can exhibit wave-like properties under certain conditions. This wave-like behavior is characterized by phenomena such as interference and diffraction, similar to what is observed with classical waves like water waves or sound waves. When particles exhibit these wave-like properties, they can spread out, interfere with each other, and display patterns of constructive or destructive interference.

On the other hand, particles can also exhibit particle-like properties. They can be localized, possess definite positions, and can be individually detected or measured. This behavior is reminiscent of classical particles, which occupy specific points in space and can be observed independently of each other.

The intriguing aspect of wave-particle complementarity is that a particle's behavior can change depending on how it is observed or measured [35, 159]. When we try to measure a particle's position precisely, its wave-like behavior diminishes, and it

manifests more as a localized particle. Conversely, when we try to measure a particle's momentum or energy precisely, its wave-like behavior becomes more prominent, and its position becomes uncertain. The phenomena is well understood with Wheeler's delayed choice [159] and welcher-weg delayed choice [35] experiments

Experimental investigations of the wave-particle complementarity with welcher-weg, quantum erasers and delayed choice experiments have drawn attention in recent years [160, 161, 162, 163]. Wheeler's delayed choice experiment with quantum mechanically controlled beam splitter [164] has been demonstrated in various experiments [165, 166, 167, 168]. Recently, the possibility of a superposition in wave and particle nature was investigated [169]. The quantitative complementarity and the duality relations in asymmetric interference is also under experimental and theoretical investigations [170, 171].

The experimental investigations of complementarity require sophisticated interferometers and high experimental skills. Here, we present a scheme in which wave-particle complementarity can be experimentally investigated without requiring conventional interferometers. The von Neumann coupling between a Gaussian ancilla and a pre- and post-selected two-level quantum system can induce interference patterns on the ancilla wavefunction. Furthermore, we demonstrate that the setup is operationally equivalent to a Mach-Zehnder interferometer. Our proposal makes the quantum superposition of beam splitters in Wheeler's delayed choice scenario much easier compared to earlier experiments. Similarly, it simplifies the experimental investigation of nonlocal features of wave-particle duality.

6.2 Revisiting welcher-weg experiments

Mach–Zehnder interferometer (MZI) is a classic setup for the demonstration of wave-particle duality. The Mach-Zehnder interferometer is an optical device widely used in interferometry and quantum optics experiments. It consists of a beam splitter BS_1, two mirrors, and two output ports. The input light beam is split into two arms by the beam splitter, and each arm travels a different path before recombining at the output ports with the help of another beam splitter BS_2. By adjusting the relative path lengths or introducing phase shifts in one of the arms, interference occurs when the light waves recombine, leading to constructive or destructive interference at the output ports. This interference pattern reveals valuable characteristics about the wave-particle nature of a single photon inside the interferometer.

When a single photon is injected into one of the ports of BS_1, *e. g.* arm A, it is split into two possible paths A and B. For a single photon setup, beam splitters can be thought as basis transformation operators on path degree of freedom. A beam splitter in

such a scenario with transmittance t can be specified by the following transformation:

$$\begin{aligned} |A\rangle &\xrightarrow{BS} \sqrt{t}\,|A\rangle + \sqrt{1-t}\,|B\rangle \\ |B\rangle &\xrightarrow{BS} \sqrt{1-t}\,|A\rangle - \sqrt{t}\,|B\rangle \end{aligned} \tag{6.1}$$

where we have assumed that the beam splitter itself does not introduce any phase different between the paths. With transmittance t_1 for BS_1, the state after the first split can be given as

$$|\psi\rangle = \sqrt{t_1}\,|A\rangle + \sqrt{1-t_1}e^{i\eta}\,|B\rangle \tag{6.2}$$

where $0 \leq t_1 \leq 1$ the transmittance of BS_1 and η is the phase difference introduced by a possible asymmetric optical path inside the interferometer. Generally the phase shift η is generated by a phase shifter inserted in one of the paths. BS_2 with transmittance t_2 transforms $|\psi\rangle$ into

$$\begin{aligned} |\psi'\rangle =& \sqrt{t_1}\left(\sqrt{t_2}\,|A\rangle + \sqrt{1-t_2}\,|B\rangle\right) \\ &+ \sqrt{1-t_1}e^{i\eta}\left(\sqrt{1-t_2}\,|A\rangle - \sqrt{t_2}\,|B\rangle\right) \\ =& \left(\sqrt{t_1 t_2} + e^{i\eta}\sqrt{(1-t_1)(1-t_2)}\right)|A\rangle \\ &+ \left(\sqrt{t_1(1-t_2)} - e^{i\eta}\sqrt{(1-t_1)t_2}\right)|B\rangle \end{aligned} \tag{6.3}$$

Probabilities of finding the photon in arms A and B after BS_2 are:

$$\begin{aligned} P(A) &= 1 - t_1 - t_2 + 2t_1t_2 + 2\sqrt{t_1t_2(1-t_1)(1-t_2)}\cos\eta \\ P(B) &= t_1 + t_2 - 2t_1t_2 - 2\sqrt{t_1t_2(1-t_1)(1-t_2)}\cos\eta \end{aligned} \tag{6.4}$$

Probabilities $P(A)$ and $P(B)$ are periodic functions of the phase shift η. Since η is the phase difference between the two paths inside the interferometer, these probabilities are interference patterns manifesting the wave nature of the photon. Note that when either of t_1 or t_2 is zero or one, the interference patterns disappear. In that case the photon behaves like it followed only one of the two paths revealing its particle nature. A quantification of wave nature at port A is given by the fringe visibility [172]:

$$\begin{aligned} \mathcal{V}_A &= \frac{\max\limits_{\eta} P(A) - \min\limits_{\eta} P(A)}{\max\limits_{\eta} P(A) + \min\limits_{\eta} P(A)} \\ &= \frac{2\sqrt{t_1t_2(1-t_1)(1-t_2)}}{1 - t_1 - t_2 + 2t_1t_2} \end{aligned} \tag{6.5}$$

Similarly the fringe visibility for port B is:

$$\mathcal{V}_B = \frac{2\sqrt{t_1t_2(1-t_1)(1-t_2)}}{t_1 + t_2 - 2t_1t_2} \tag{6.6}$$

The fringe visibility, in a sense, is a measure of how unlikely is the path indistinguishability of a photon inside an interferometer. If the guessing probability of the path taken by the photon is one half, the fringe visibility is one *i.e*. photon behaves like a perfect wave. And if the guessing probability is one, the photon behaves like a particle and, hence, the fringe visibility becomes equal to zero. If one guesses the most probable way then the probability of success is $(1+\mathcal{P})/2$, where $\mathcal{P}$ and $\mathcal{V}$ are constrained by the complementarity inequality [173]:

$$\mathcal{P}^2 + \mathcal{V}^2 \leq 1 \tag{6.7}$$

where $\mathcal{P}$ is known as predictability of the path. Welcher-weg (which path) experiments establish the wave-particle or indisputably known as the 'interferometic duality' in a beautiful manner: the observation of an interference pattern and the acquisition of welcher-weg information are mutually exclusive.

One of the most striking and somewhat strange fact about the single photon MZI experiment is that it is simply an experiment on a two-level quantum system. In this way, actions of beam splitters, phase shifters, and detectors can simply be implemented on a spin system or the energy levels of an atom. The only wave-particle picture arises when we visualize a photon traveling in the space. Can one really talk of wave-particle duality when all above quantum operations are performed on a spin-$1/2$ system? Although, one can easily reproduce results of welcher-weg experiment using a spin-$1/2$ but it may lack an interpretation of the results. Indeed, one can face similar difficulties in the welcher-weg experiment with MZI if the setup is slightly reformulated: suppose the photon before BS_2 is as usual in state $|\psi\rangle = \sqrt{t_1}\,|A\rangle + \sqrt{1-t_1}e^{i\eta}\,|B\rangle$. The action of BS_2 followed by detection in arm A can be interpreted as post-selection in the state $|\phi\rangle = \sqrt{t_2}\,|A\rangle + \sqrt{1-t_2}\,|B\rangle$. In this case, we only have a pre-and post-selection scenario where a photon is prepared in $|\psi\rangle$ and measured in $|\phi\rangle$. Here, the interpretation of wave-particle duality is nontrivial, although the results are same. In this chapter we will present a technique that enable us to visualize the wave-particle complementarity.

6.3 Interference and wave-particle complementarity using von Neumann interactions

In this section, we present a technique where a duality relation between properties of discrete level systems can be translated into wave-particle duality of a photon in an interferometer. In fact, we will demonstrate that there exists a single-photon-double-slit experimental scenario associated with a pre-and post-selected scenario with two-level quantum systems. Suppose a qubit S is prepared in the state:

$$|\psi\rangle = \sqrt{p}\,|0\rangle + e^{i\alpha}\sqrt{1-p}\,|1\rangle\,, \tag{6.8}$$

where $0 \leq p \leq 1$ and α is an arbitrary phase. Additionally, an ancilla A is prepared in a Gaussian wave function in the position basis as:

$$\xi(x) = (2\pi\delta^2)^{-1/4} \exp\left(-\frac{x^2}{4\delta^2}\right). \tag{6.9}$$

The ancilla couples with the system with a von Neumann interaction of the form:

$$H_{int} = -g(t)\sigma_z \otimes \hat{x} \tag{6.10}$$

where $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ is the usual z-Pauli operator and $\hat{x}$ is the position operator of the ancilla. Suppose interaction takes place for a time period Δt. Let us denote $\gamma = \int_t^{t+\Delta t} g(t)dt$. The entangling unitary corresponding to the interaction is given evaluated as:

$$U = \mathbb{1} \otimes \cos(\gamma\hat{x}) + i\sigma_z \otimes \sin(\gamma\hat{x}) \tag{6.11}$$

Let $|\Psi\rangle = |\psi\rangle \otimes |\xi\rangle$ be the initial composite state of S and A, where $\xi(x) = \langle x|\xi\rangle$. The post-interaction state $|\Psi'\rangle = U|\Psi\rangle$ is obtained as:

$$|\Psi'\rangle = \sqrt{p}\,|0\rangle \otimes |\xi_0\rangle + e^{i\alpha}\sqrt{1-p}\,|1\rangle \otimes |\xi_1\rangle\,, \tag{6.12}$$

where

$$\begin{aligned} |\xi_0\rangle &= \exp(i\gamma\hat{x})\,|\xi\rangle\,, \\ |\xi_1\rangle &= \exp(-i\gamma\hat{x})\,|\xi\rangle\,. \end{aligned} \tag{6.13}$$

The position wavefunctions corresponding to $|\xi_0\rangle$ and $|\xi_1\rangle$ are evaluated as:

$$\begin{aligned} \xi_0(x) &= (2\pi\delta^2)^{-1/4} \exp\left(i\gamma x - \frac{x^2}{4\delta^2}\right), \\ \xi_1(x) &= (2\pi\delta^2)^{-1/4} \exp\left(-i\gamma x - \frac{x^2}{4\delta^2}\right). \end{aligned} \tag{6.14}$$

The ancilla is coupled with the system in its z-basis which destroys its coherence. However, a post-selection can transfer the initial coherence in the z basis to the ancilla wave-function making it behave like a particle in a double-slit experimental setup. The system is post-selected in state $|\phi\rangle$ after the coupling:

$$|\phi\rangle = \sqrt{q}\,|0\rangle + e^{i\beta}\sqrt{1-q}\,|1\rangle\,, \tag{6.15}$$

where $0 \leq p \leq 1$ and β is the relative phase. After the post-selection, the ancilla wavefunction up to a normalization factor is given as:

$$\xi'(x) = \sqrt{pq}\xi_0(x) + \sqrt{(1-p)(1-q)}e^{i(\alpha-\beta)}\xi_1(x) \tag{6.16}$$

The probability density $P(x) = \|\xi'(x)\|^2$ is obtained as:

$$\begin{aligned} P(x) =& pq\|\xi_0(x)\|^2 + (1-p)(1-q)\|\xi_1(x)\|^2 \\ &+ 2\sqrt{pq(1-p)(1-q)}\,\mathrm{Re}\{e^{i(\alpha-\beta)}\xi_0^*(x)\xi_1(x)\} \end{aligned} \tag{6.17}$$

Since $\|\xi(x)\| = \|\xi_0(x)\| = \|\xi_1(x)\|$, we have

$$P(x) = N\|\xi(x)\|^2\left(1-p-q+2pq+2\sqrt{pq(1-p)(1-q)}\cos(2\gamma x+\alpha-\beta)\right), \tag{6.18}$$

where N is the normalization factor. The distribution $P(x)$ manifests a fringe pattern enveloped in a Gaussian distribution $\|\xi(x)\|^2$. The fringe pattern is exactly same as if it is produced in a MZI output port except that the fringes are in real space *i.e*. position and the pattern is Gaussian shaped. $P(x)$ has more resemblance with the fringe pattern of a double slit experiment. One can quantify the fringe visibility as it is done in the case of MZI and double slit experiments.

It is worth noting that any pre-and post-selection scenario with a two-level quantum system is operationally equivalent to a MZI scenario where the post-selected state can reveal information about the coherence in a particular basis. The information it can reveal is bounded by the corresponding complementarity inequality. For example, if a system prepared in $|\psi\rangle$ is post selected in $|\phi\rangle$, the maximum predictability whether the system was in $|0\rangle$ or $|1\rangle$ is upper bounded by $\mathcal{P} \leq \sqrt{1-\mathcal{V}^2}$, where $\mathcal{V}$ is the fringe visibility of the corresponding interference pattern generated by the von Neumann interaction $H_{int} = -g(t)\sigma_z \otimes \hat{x}$ with a Gaussian pointer. In a sense, it quantifies the coherence in the σ_z basis: *e. g*. a perfect interference pattern *i.e*. $\mathcal{V} = 1$ has zero predictability meaning that $|\psi\rangle$ is a uniform superposition of $|0\rangle$ and $|1\rangle$. In other words, it is in a complementary basis. Similarly, $\mathcal{V} = 0$ signifies error-free predictability of the state. The system in this case is operationally equivalent to a system well localized in σ_z basis.

The post-selection measurement can have outcomes other then $|\phi\rangle$ which are discarded. Suppose it has two outcomes $|\phi\rangle$ and $|\phi'\rangle$ *s. th*. $\langle\phi'|\phi\rangle = 0$. The interference pattern corresponding to the post-selection $|\phi'\rangle$ is obtained as:

$$\tilde{P}(x) = \tilde{N}\|\xi(x)\|^2\left(p+q-2pq-2\sqrt{pq(1-p)(1-q)}\cos(2\gamma x+\alpha-\beta)\right) \tag{6.19}$$

where $\tilde{N}$ is a normalization factor.

Our results are applicable to mixed states as well. Suppose the system is in a mixed state ρ initially:

$$\rho = p\,|0\rangle\langle 0| + \Gamma e^{i\alpha}\,|0\rangle\langle 1| + \Gamma e^{-i\alpha}\,|1\rangle\langle 0| + (1-p)\,|1\rangle\langle 1|\,, \tag{6.20}$$

where $0 \leq p \leq 1$, $0 \leq \Gamma$ and α the coherence factor and coherence phase, respectively. With the ancilla prepared in $|\xi\rangle$, interaction U and post-selection of the system in $|\phi\rangle$, we obtain the corresponding fringe pattern:

$$P(x) = N\|\xi(x)\|^2 \left(1 - p - q + 2pq + 2\Gamma\sqrt{q(1-q)}\cos(2\gamma x + \alpha - \beta)\right), \quad (6.21)$$

Note that for $q = 1/2$, the fringe visibility is $\mathcal{V} = 2\Gamma$.

6.4 Welcher-weg detections, quantum erasers and Wheeler's delayed-choice experiments

Consider the MZI arrangement of Section 6.2. Now suppose, an observer uses a quantum memory, initially prepared in state $|\chi\rangle$, to record the path of the photon inside the interferometer. The interaction between the photon and the memory is specified by:

$$\begin{aligned} |A\rangle \otimes |\chi\rangle &\xrightarrow{int} |A\rangle \otimes |0\rangle \\ |B\rangle \otimes |\chi\rangle &\xrightarrow{int} |B\rangle \otimes |1\rangle \end{aligned} \quad (6.22)$$

The interaction stores the path information in the memory. One can find out the path by simply measuring the memory in the $\{|0\rangle, |1\rangle\}$ basis. The state after BS_2 becomes:

$$\begin{aligned} |\Psi'\rangle =& \sqrt{t_1}\left(\sqrt{t_2}\,|A\rangle + \sqrt{1-t_2}\,|B\rangle\right) \otimes |0\rangle \\ &+ \sqrt{1-t_1}e^{i\eta}\left(\sqrt{1-t_2}\,|A\rangle - \sqrt{t_2}\,|B\rangle\right) \otimes |1\rangle \\ =& |A\rangle \otimes \left(\sqrt{t_1 t_2}\,|0\rangle + e^{i\eta}\sqrt{(1-t_1)(1-t_2)}\,|1\rangle\right) \\ &+ |B\rangle \otimes \left(\sqrt{t_1(1-t_2)}\,|0\rangle - e^{i\eta}\sqrt{(1-t_1)t_2}\,|1\rangle\right), \end{aligned} \quad (6.23)$$

Consequently,

$$\begin{aligned} P(A) &= 1 - t_1 - t_2 + 2t_1 t_2 \\ P(B) &= t_1 + t_2 - 2t_1 t_2. \end{aligned} \quad (6.24)$$

The fringe visibility is zero. Leaving out the path information wipes out the interference. The fringes can be retrieved by erasing the quantum memory with delayed choice. Suppose after the detection of photon, the memory is projected into $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. The corresponding probability densities of ancilla are equal to $P(A)$ and $P(B)$ of Eq. (6.4). Just by choosing a measurement on quantum memory in a different basis regenerates the interference patterns. A measurement in a complementary basis to $\{|0\rangle, |1\rangle\}$ erases the path information and photons start to behave like waves.

6. Demonstration of wave-particle complementarity using von Neumann measurements

To demonstrate the same with von Neumann interaction scenario, we consider a two qubit entangled state:

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B \right). \tag{6.25}$$

where the qubits A and B are held by Alice and Bob, respectively. Bob couples qubit B to the ancilla in σ_z basis and then post-selects in the state $|\phi\rangle$ (given in Eq. (6.15)). The corresponding probability density of the ancilla is $P(x) = \|\xi(x)\|^2$ with zero fringe visibility. It is obvious that the the qubit A carries the information about the coherence of B in the σ_z basis which destroys the wave nature. Suppose qubit A undergoes a measurement in the basis $\{|\psi\rangle, |\psi'\rangle\}$, where $|\psi\rangle$ is given by Eq (6.8) and $\langle\psi'|\psi\rangle = 0$. The interference patterns corresponding to Alice's outcomes $\{|\psi\rangle$ and $|\psi'\rangle\}$ are obtained:

$$\begin{aligned} P_\psi(x) &= \|\xi(x)\|^2 \left(1 - p - q + 2pq + 2\sqrt{pq(1-p)(1-q)}\cos(2\gamma x + \alpha - \beta)\right) \\ P_{\psi'}(x) &= \|\xi(x)\|^2 \left(p + q - 2pq - 2\sqrt{pq(1-p)(1-q)}\cos(2\gamma x + \alpha - \beta)\right) \end{aligned} \tag{6.26}$$

$P_\psi(x)$ and $P_{\psi'}(x)$ are complementary to each other *i.e.* the sum $P_\psi(x) + P_{\psi'}(x)$ has zero fringe visibility.

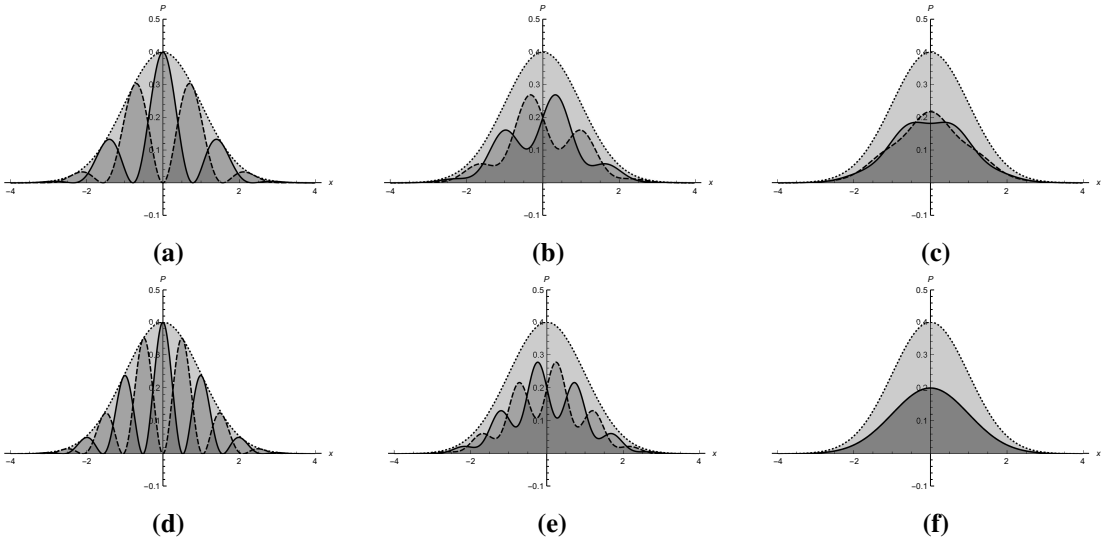


Figure 6.1: $P_\psi(x)$ (solid line), $P_{\psi'}(x)$ (dashed line), and $P_\psi(x) + P_{\psi'}(x)$ (dotted line) are plotted against x for (a) $\gamma = 4, p = q = 0.5, \alpha = \beta = 0$, (b) $\gamma = 4, p = 0.05, q = 0.5, \alpha = \pi/2, \beta = 0$, (c) $\gamma = 4, p = 0.002, q = 0.5, \alpha = \pi, \beta = 0$, (d) $\gamma = 6, p = q = 0.5, \alpha = \beta = 0$, (e) $\gamma = 6, p = 0.05, q = 0.5, \alpha = 0, \beta = \pi/2$, (f) $pq = 0$.

As we discussed, a photon's nature whether it is a particle or a wave is somehow determined by the beam splitters and the detection events in MZI scenario. Equivalently, in the von Neumann interaction scenario, it is determined by the pre-and post-selections. When BS_2 is not inserted in the MZI, the photon takes a deterministic path to reach the detector revealing its particle nature while behaves like a wave when it is inserted. It appears, in quite a strange manner, that the photon knows about the apparatus in advance. The situation becomes even weirder with Wheeler's delayed choice experiment: suppose BS_2 is randomly inserted or removed from the setup by an external observer with free choice just after the photon passes through BS_1 and before it reaches BS_2. Furthermore, it is ensured that the observer's choice exists outside of the photon's light cone. In this scenario, photon must never know whether the two arms interfere in the future or not. However, contrary to the expectation, the wave-particle nature is correlated with the observer's choice. Wheeler's thought experiment plays a central role in the investigations on the wave-particle complementarity. The loophole free experimental realization of this experiment has gained a momentum in recent years. Quantum implementation of remote insertion and removal of a beam splitter is exceptionally difficult. Our methods with von Neumann interaction scenario make the realization of Wheeler's delayed choice experiment relatively convenient.

Instead of a single qubit system, let us consider a three qubit GHZ state:

$$|\Phi\rangle = \frac{1}{\sqrt{2}} \left[|00\rangle_A \otimes |0\rangle_B + |11\rangle_A \otimes |1\rangle_B \right] \tag{6.27}$$

Alice keeps a pair of qubits while the third is sent to remotely located Bob. Alice performs von Neumann scenario on the first qubit while post-selects the second in $|+\rangle$ which acts as a welcher-weg memory. Bob can freely chose to measure either of the basis $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$. The fringe visibility corresponding to Bob's outcomes is:

$$\begin{aligned} \mathcal{V}_0 &= \mathcal{V}_1 = 0 \\ \mathcal{V}_+ &= \mathcal{V}_- = 1, \end{aligned} \tag{6.28}$$

where the subscript notation is understood. The space-like separated choice of Bob's measurement basis determines whether the ancilla is a wave or a particle. This reveals the nonlocal nature of wave-particle duality: the element of reality corresponding to the property whether the system is a wave or particle does not exist locally before the measurement.

6.5 Conclusion

In this chapter, we propose a scheme to demonstrate wave-particle complementarity without requiring an actual interferometer. Effects equivalent to those of a MZI or

a double-slit interferometer are generated on a particle with a Gaussian wavefunction using a von Neumann-type interaction with a two-level quantum system in a pre- and post-selection scenario. Contrary to sophisticated optical and matter-wave interferometers, our setup is easier to realize. It only requires a qubit, an ancilla with a Gaussian wavefunction, and measurement setups for qubits. Our scheme facilitates the implementation of welcher-weg and quantum eraser experiments. Furthermore, we demonstrate how it can play a crucial role in investigations on Wheeler's delayed choice gedanken experiments and experimental research on the nonlocality of wave-particle duality. Since pre- and post-selections on the qubit manifest the configuration of an interferometer, a nonlocal manipulation of the latter is easily implementable using entangled qubits.

Our approach associates wave-particle complementarity with the incompatibility of observables in discrete-level systems. Additionally, the framework presented here provides an operational definition of quantum coherence in a two-level system: the coherence factor is directly proportional to the fringe visibility of the associated von Neumann interference.

Chapter 7

Summary

The physics of quantum measurements play a crucial role in quantum foundations and quantum information theory, bridging the gap between the quantum and classical worlds. Despite the well-established mathematical framework of quantum measurement theory, the dynamics of measurements and the quantum-to-classical transition continue to puzzle physicists. This thesis explores various aspects of quantum measurements, including the investigation of the past behavior of quantum particles, interactions that adhere to special relativity, the emergence of classical objectivity in the position basis, and wave-particle duality. Additionally, a novel quantum key distribution technique utilizing post-selections on qubit blocks is presented.

In the first chapter, the predictions of the two-state vector formalism (TSVF), a time symmetric framework for sequential quantum measurements, are examined. Furthermore, a gedanken experiment is proposed to challenge the claim that weak values represent observables, which contributes to the legitimacy of several quantum paradoxes. The analysis demonstrates that a zero weak value of the position operator does not imply the absence of the particle, thereby resolving paradoxes such as the quantum Cheshire cat, weak value version of Hardy's paradox, three-box paradox, and more. Experimental realization of our gedanken experiment is an interesting future prospect. Since weak values are known to be useful in quantum state and process tomography, it would be interesting to see whether our techniques deployed here to investigate the past of a quantum system can be useful for the same purpose.

The following chapter investigates the weak value framework for mixed states. According to the TSVF, weak values extend beyond statistical averages and offer insights into the physics of pre- and post-selected quantum systems. A quantum state discrimination scheme based on weak values for mixed states is devised, allowing for the apparent discrimination of arbitrary mixed states with high precision. This scheme can be employed in secure quantum key distribution protocols, even in the presence

of significant noise. The security proof of the protocol is reanalyzed without relying on weak values and weak measurement approximations, revealing potential flaws in the previous approach. These findings challenge the notion that weak values for mixed states represent elements of reality in weak measurements, as advocated by proponents of TSVF.

The subsequent chapter introduces a quantum key distribution protocol that utilizes novel techniques of quantum block-wise processing and post-selections. This protocol builds upon the six-state protocol and involves forming blocks of finite length after successful raw key generation, utilizing an authenticated classical channel. These blocks undergo random permutations and post-selections, resulting in a significant reduction in the bit error rate and increased noise tolerance. This approach enables secure quantum key distribution over highly noisy quantum channels, presenting a promising solution for long-distance quantum communications. It would be intriguing to see whether our methods can be applied to continuous variable quantum key distributions as well. Another important prospect is proving the security for finite length keys. Since our protocol offers low bit error rate in the presence of high noise, it would be interesting to investigate whether the computation cost in classical post-processing is significantly lower.

In the next chapter, a no-go theorem is presented, highlighting the non-feasibility of certain quantum operations and their implications in explaining the emergence of classical objectivity within the framework of quantum theory. The theorem states that internal degrees of freedom cannot be manipulated or measured without disturbing the spatial wavefunction of the corresponding physical system, necessitating local interactions in physical space. Based on the no-faster-than-light communication principle, this proof holds fundamental significance. The theorem is then applied to a general decoherence model with a spin environment, demonstrating the emergence of objectivity in the position basis through a quantum Darwinian approach. These results resolve a long-standing problem in the decoherence paradigm, showing that arbitrary interactions between a system and environment subsystems always localize the system in its position basis, leaving a redundant imprint on the environment. Our theorem can have far-reaching implications in the fields of quantum foundations and quantum information. Investigations on the process of information dissipation in open quantum systems due to decoherence are an active field of research. Various decoherence models attempt to characterize the system-environment interaction Hamiltonian. Such studies play crucial roles in quantum controls and physical realizations of quantum computers. The prospect of modeling decoherence and open quantum system dynamics in light of our no-go theorem is intriguing. Implications in the dynamics of quantum thermalization and quantum many-body interactions are also worth investigating. An experimental test of our no-go result is an intriguing avenue of research.

The final chapter investigates novel aspects of von Neumann interactions in connection with the wave-particle complementarity principle. While wave-particle complementarity is typically associated with interferometry, this chapter proposes a mechanism that defines wave-particle duality for discrete variable systems. It is shown that a von Neumann interaction between a Gaussian pointer and a pre- and post-selected two-level quantum system is operationally equivalent to a Mach-Zehnder interferometer with single photons. Fringe visibility and which-way predictability for a qubit can be defined within this framework, providing an operational interpretation of quantum coherence for discrete systems in terms of wave-particle complementarity. We have only investigated two-level quantum systems here. However, our methods are extendable to higher dimensional discrete-level systems as well. As a future prospect, it would be interesting to quantify the coherence of a higher dimensional system in terms of the fringe visibility of the corresponding von Neumann scenario. Experimental realizations of our proposal are also an important prospect. Quantum state interferography is a newly proposed experimental technique for state reconstruction and tomography that deploys interference phenomena as a key tool. Our results can make quantum state tomography for discrete-dimensional systems.

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145–195 (Mar 2002). 2

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301–1350 (Sep 2009). 2, 49

[3] R. P. Feynman et al., Simulating physics with computers, Int. j. Theor. phys **21**(6/7) (2018). 2

[4] C. L. Degen, F. Reinhard, and P. Cappellaro, Quantum sensing, Rev. Mod. Phys. **89**, 035002 (Jul 2017). 2

[5] L. Pezzè, A. Smerzi, M. K. Oberthaler, R. Schmied, and P. Treutlein, Quantum metrology with nonclassical states of atomic ensembles, Rev. Mod. Phys. **90**, 035005 (Sep 2018). 2

[6] H. E. D. Scovil and E. O. Schulz-DuBois, Three-Level Masers as Heat Engines, Phys. Rev. Lett. **2**, 262–263 (Mar 1959). 2

[7] K. Maruyama, F. Nori, and V. Vedral, Colloquium: The physics of Maxwell's demon and information, Rev. Mod. Phys. **81**, 1–23 (Jan 2009). 2

[8] F. Campaioli, F. A. Pollock, and S. Vinjanampathy, Quantum Batteries - Review Chapter, 2018. 2

[9] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, Nature **299**(5886), 802–803 (Oct 1982). 3, 71

[10] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theoretical Computer Science **560**, 7–11 (2014), Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84. 3, 19, 20, 49, 71, 72

[11] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301–1350 (Sep 2009). 3, 19, 44, 49, 71, 72

[12] E. Schrödinger, Die gegenwartige Situation in der Quantenmechanik, Naturwissenschaften **23**(48), 807–812 (Nov 1935). 3, 5

[13] P. Mittelstaedt, *Philosophical problems of modern physics*, D Reidel, Netherlands, 1976. 3

[14] A. Bassi, K. Lochan, S. Satin, T. P. Singh, and H. Ulbricht, Models of wavefunction collapse, underlying theories, and experimental tests, Rev. Mod. Phys. **85**, 471–527 (Apr 2013). 3, 5

[15] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge University Press, 2011. 3, 4, 5

[16] C. Cohen-Tannoudji, B. Diu, and F. Laloë, *Quantum mechanics; 1st ed.*, Wiley, New York, NY, 1977, Trans. of : Mécanique quantique. Paris : Hermann, 1973. 3

[17] M.-O. Renou, D. Trillo, M. Weilenmann, T. P. Le, A. Tavakoli, N. Gisin, A. Acín, and M. Navascués, Quantum theory based on real numbers can be experimentally falsified, Nature **600**(7890), 625–629 (Dec 2021). 4

[18] D. Deutsch, Quantum theory as a universal physical theory, International Journal of Theoretical Physics **24**(1), 1–41 (Jan 1985). 4

[19] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865–942 (Jun 2009). 4

[20] J. S. Bell, On the einstein-podolsky-rosen paradox, Physics **1**(3), 195–200 (1964). 4, 91

[21] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419–478 (Apr 2014). 4

[22] J. S. Bell, *Speakable and unspeakable in quantum mechanics*, Collected papers on quantum philosophy, Cambridge Univ. Press, Cambridge, 1987. 4

[23] E. P. Wigner, *Remarks on the Mind-Body Question*, pages 247–260, Springer Berlin Heidelberg, Berlin, Heidelberg, 1995. 5

[24] J. von Neumann, *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, Princeton, 2018. 5

[25] E. B. Davies, *Quantum theory of open systems*, Academic Press London, London, 1976. 6

[26] Y. Aharonov, D. Z. Albert, and L. Vaidman, How the result of a measurement of a component of the spin of a spin-1/2 particle can turn out to be 100, Phys. Rev. Lett. **60**, 1351–1354 (Apr 1988). 6, 11, 12, 25, 43, 46

[27] Y. Aharonov, P. G. Bergmann, and J. L. Lebowitz, Time Symmetry in the Quantum Process of Measurement, Phys. Rev. **134**, B1410–B1416 (Jun 1964). 8, 11, 25, 27

[28] Y. Aharonov and L. Vaidman, Complete description of a quantum system at a given time, Journal of Physics A: Mathematical and General **24**(10), 2315–2328 (may 1991). 8, 10, 27, 43

[29] R. E. Kastner, The Three-Box "Paradox" and Other Reasons to Reject the Counterfactual Usage of the ABL Rule, Foundations of Physics **29**(6), 851–863 (Jun 1999). 8

[30] D. Miller, Realism and time symmetry in quantum mechanics, Physics Letters A **222**(1), 31 – 36 (1996). 8

[31] O. Cohen, Pre- and postselected quantum systems, counterfactual measurements, and consistent histories, Phys. Rev. A **51**, 4373–4380 (Jun 1995). 8

[32] N. BOHR, The Quantum Postulate and the Recent Development of Atomic Theory1, Nature **121**(3050), 580–590 (Apr 1928). 11, 25, 109

[33] J. A. Wheeler, The "Past" and the "Delayed-Choice" Double-Slit Experiment, in *Mathematical Foundations of Quantum Theory*, edited by A. Marlow, pages 9 – 48, Academic Press, 1978. 11, 25

[34] W. Heisenberg, *Physics and Philosophy;*, New York: Harper, 1958. 11, 25

[35] M. O. Scully, B.-G. Englert, and H. Walther, Quantum optical tests of complementarity, Nature **351**(6322), 111–116 (May 1991). 11, 25, 109, 110

[36] Y. Aharonov and L. Vaidman, Properties of a quantum system during the time interval between two measurements, Phys. Rev. A **41**, 11–20 (Jan 1990). 11, 12, 15, 25, 43

[37] Y. Aharonov and L. Vaidman, Complete description of a quantum system at a given time, Journal of Physics A: Mathematical and General **24**(10), 2315 (1991). 11, 12, 15, 25, 26

[38] A. J. Leggett, Comment on "How the result of a measurement of a component of the spin of a spin-(1/2 particle can turn out to be 100", Phys. Rev. Lett. **62**, 2325–2325 (May 1989). 11, 25

[39] C. Ferrie and J. Combes, How the Result of a Single Coin Toss Can Turn Out to be 100 Heads, Phys. Rev. Lett. **113**, 120404 (Sep 2014). 11, 25

[40] D. Sokolovski and E. Akhmatskaya, An even simpler understanding of quantum weak values, Annals of Physics **388**, 382 – 389 (2018). 11, 25

[41] D. Sokolovski, Weak measurements measure probability amplitudes (and very little else), Physics Letters A **380**(18), 1593 – 1599 (2016). 11, 25, 28, 41

[42] N. W. M. Ritchie, J. G. Story, and R. G. Hulet, Realization of a measurement of a "weak value", Phys. Rev. Lett. **66**, 1107–1110 (Mar 1991). 11, 43, 50

[43] G. J. Pryde, J. L. O'Brien, A. G. White, T. C. Ralph, and H. M. Wiseman, Measurement of Quantum Weak Values of Photon Polarization, Phys. Rev. Lett. **94**, 220405 (Jun 2005). 11, 50

[44] A. Romito, Y. Gefen, and Y. M. Blanter, Weak Values of Electron Spin in a Double Quantum Dot, Phys. Rev. Lett. **100**, 056801 (Feb 2008). 11

[45] N. Brunner, A. Acín, D. Collins, N. Gisin, and V. Scarani, Optical Telecom Networks as Weak Quantum Measurements with Postselection, Phys. Rev. Lett. **91**, 180402 (Oct 2003). 12, 25, 50

[46] D. R. Solli, C. F. McCormick, R. Y. Chiao, S. Popescu, and J. M. Hickmann, Fast Light, Slow Light, and Phase Singularities: A Connection to Generalized Weak Values, Phys. Rev. Lett. **92**, 043601 (Jan 2004). 12, 25, 50

[47] N. Brunner, V. Scarani, M. Wegmüller, M. Legré, and N. Gisin, Direct Measurement of Superluminal Group Velocity and Signal Velocity in an Optical Fiber, Phys. Rev. Lett. **93**, 203902 (Nov 2004). 12, 25

[48] R. M. Camacho, P. B. Dixon, R. T. Glasser, A. N. Jordan, and J. C. Howell, Realization of an All-Optical Zero to π Cross-Phase Modulation Jump, Phys. Rev. Lett. **102**, 013902 (Jan 2009). 12, 50

[49] Y. Kim, Y.-S. Kim, S.-Y. Lee, S.-W. Han, S. Moon, Y.-H. Kim, and Y.-W. Cho, Direct quantum process tomography via measuring sequential weak values of incompatible observables, Nature Communications **9**(1), 192 (2018). 12, 25, 43, 50

[50] M. Hallaji, A. Feizpour, G. Dmochowski, J. Sinclair, and A. M. Steinberg, Weak-value amplification of the nonlinear effect of a single photon, Nature Physics **13**(6), 540–544 (Jun 2017). 12, 25

[51] O. S. Magaña Loaiza, M. Mirhosseini, B. Rodenburg, and R. W. Boyd, Amplification of Angular Rotations Using Weak Measurements, Phys. Rev. Lett. **112**, 200401 (May 2014). 12, 25

[52] A. Feizpour, X. Xing, and A. M. Steinberg, Amplifying Single-Photon Nonlinearity Using Weak Measurements, Phys. Rev. Lett. **107**, 133603 (Sep 2011). 12, 25

[53] J. Dressel, M. Malik, F. M. Miatto, A. N. Jordan, and R. W. Boyd, Colloquium: Understanding quantum weak values: Basics and applications, Rev. Mod. Phys. **86**, 307–316 (Mar 2014). 12

[54] J. S. Lundeen, B. Sutherland, A. Patel, C. Stewart, and C. Bamber, Direct measurement of the quantum wavefunction, Nature **474**(7350), 188–191 (Jun 2011). 12, 25, 50

[55] J. S. Lundeen and C. Bamber, Procedure for Direct Measurement of General Quantum States Using Weak Measurement, Phys. Rev. Lett. **108**, 070402 (Feb 2012). 12, 25, 43, 44

[56] L. Hardy, Quantum mechanics, local realistic theories, and Lorentz-invariant realistic theories, Phys. Rev. Lett. **68**, 2981–2984 (May 1992). 12, 17, 25

[57] Y. Aharonov, A. Botero, S. Popescu, B. Reznik, and J. Tollaksen, Revisiting Hardy's paradox: counterfactual statements, real measurements, entanglement and weak values, Physics Letters A **301**(3), 130 – 138 (2002). 12, 18, 25, 28, 41

[58] W. T. M. Irvine, J. F. Hodelin, C. Simon, and D. Bouwmeester, Realization of Hardy's Thought Experiment with Photons, Phys. Rev. Lett. **95**, 030401 (Jul 2005). 12, 25

[59] J. S. Lundeen and A. M. Steinberg, Experimental Joint Weak Measurement on a Photon Pair as a Probe of Hardy's Paradox, Phys. Rev. Lett. **102**, 020404 (Jan 2009). 12, 19, 25

[60] A. M. Steinberg, How Much Time Does a Tunneling Particle Spend in the Barrier Region?, Phys. Rev. Lett. **74**, 2405–2409 (Mar 1995). 12, 25

[61] N. S. Williams and A. N. Jordan, Weak Values and the Leggett-Garg Inequality in Solid-State Qubits, Phys. Rev. Lett. **100**, 026804 (Jan 2008). 12, 25, 50

[62] S. Kocsis, B. Braverman, S. Ravets, M. J. Stevens, R. P. Mirin, L. K. Shalm, and A. M. Steinberg, Observing the Average Trajectories of Single Photons in a Two-Slit Interferometer, Science **332**(6034), 1170–1173 (2011). 12, 26, 50

[63] D. H. Mahler, L. Rozema, K. Fisher, L. Vermeyden, K. J. Resch, H. M. Wiseman, and A. Steinberg, Experimental nonlocal and surreal Bohmian trajectories, Science Advances **2**(2), e1501466 (2016). 12, 26

[64] M. F. Pusey, Anomalous Weak Values Are Proofs of Contextuality, Phys. Rev. Lett. **113**, 200401 (Nov 2014). 12, 26

[65] L. Vaidman, Weak-measurement elements of reality, Foundations of Physics **26**(7), 895–906 (Jul 1996). 12, 26, 27, 43, 69

[66] L. Vaidman, Past of a quantum particle, Phys. Rev. A **87**, 052104 (May 2013). 12, 15, 26, 28

[67] K. Resch, J. Lundeen, and A. Steinberg, Experimental realization of the quantum box problem, Physics Letters A **324**(2), 125 – 131 (2004). 15, 26

[68] L. Vaidman, Impossibility of the Counterfactual Computation for All Possible Outcomes, Phys. Rev. Lett. **98**, 160403 (Apr 2007). 15, 26, 28

[69] A. Danan, D. Farfurnik, S. Bar-Ad, and L. Vaidman, Asking Photons Where They Have Been, Phys. Rev. Lett. **111**, 240402 (Dec 2013). 15, 16, 26, 41, 50

[70] Z.-Q. Zhou, X. Liu, Y. Kedem, J.-M. Cui, Z.-F. Li, Y.-L. Hua, C.-F. Li, and G.-C. Guo, Experimental observation of anomalous trajectories of single photons, Phys. Rev. A **95**, 042121 (Apr 2017). 15, 16, 26, 38

[71] Y. Aharonov, E. Cohen, A. Landau, and A. C. Elitzur, The Case of the Disappearing (and Re-Appearing) Particle, Scientific Reports **7**(1), 531 (2017). 15, 26

[72] B. de Lima Bernardo, A. Canabarro, and S. Azevedo, How a single particle simultaneously modifies the physical reality of two distant others: a quantum nonlocality and weak value study, Scientific Reports **7**(1), 39767 (Jan 2017). 15, 26

[73] Y. Aharonov, S. Popescu, D. Rohrlich, and P. Skrzypczyk, Quantum Cheshire Cats, New Journal of Physics **15**(11), 113015 (2013). 15, 17, 26, 28, 41

[74] T. Denkmayr, H. Geppert, S. Sponar, H. Lemmel, A. Matzkin, J. Tollaksen, and Y. Hasegawa, Observation of a quantum Cheshire Cat in a matter-wave interferometer experiment, Nature Communications **5**, 4492 EP – (Jul 2014), Article. 15, 17, 26, 50

[75] D. Das and A. K. Pati, Can two quantum Cheshire cats exchange grins?, New Journal of Physics **22**(6), 063032 (jun 2020). 15, 26

[76] Z.-H. Liu, W.-W. Pan, X.-Y. Xu, M. Yang, J. Zhou, Z.-Y. Luo, K. Sun, J.-L. Chen, J.-S. Xu, C.-F. Li, and G.-C. Guo, Experimental exchange of grins between quantum Cheshire cats, Nature Communications **11**(1), 3006 (Jun 2020). 15, 26

[77] B.-G. Englert, K. Horia, J. Dai, Y. L. Len, and H. K. Ng, Past of a quantum particle revisited, Phys. Rev. A **96**, 022126 (Aug 2017). 15, 16, 26, 28

[78] F. A. Hashmi, F. Li, S.-Y. Zhu, and M. S. Zubairy, Two-state vector formalism and quantum interference, Journal of Physics A: Mathematical and Theoretical **49**(34), 345302 (2016). 15, 26

[79] M. A. Alonso and A. N. Jordan, Can a Dove prism change the past of a single photon?, Quantum Studies: Mathematics and Foundations **2**(3), 255–261 (Sep 2015). 15, 26

[80] R. B. Griffiths, Particle path through a nested Mach-Zehnder interferometer, Phys. Rev. A **94**, 032115 (Sep 2016). 15, 16, 17, 26, 28

[81] H. Geppert-Kleinrath, T. Denkmayr, S. Sponar, H. Lemmel, T. Jenke, and Y. Hasegawa, Multifold paths of neutrons in the three-beam interferometer detected by a tiny energy kick, Phys. Rev. A **97**, 052111 (May 2018). 15, 26

[82] M. Wieśniak, Spectra in nested Mach–Zehnder interferometer experiments, Physics Letters A **382**(36), 2565 – 2568 (2018). 15, 26

[83] D. P. Atherton, G. Ranjit, A. A. Geraci, and J. D. Weinstein, Observation of a classical Cheshire cat in an optical interferometer, Opt. Lett. **40**(6), 879–881 (Mar 2015). 15, 26

[84] R. Corrêa, M. F. Santos, C. H. Monken, and P. L. Saldanha, 'Quantum Cheshire Cat' as simple quantum interference, New Journal of Physics **17**(5), 053042 (2015). 15, 26

[85] Q. Duprey, S. Kanjilal, U. Sinha, D. Home, and A. Matzkin, The Quantum Cheshire Cat effect: Theoretical basis and observational implications, Annals of Physics **391**, 1 – 15 (2018). 15, 26

[86] Z.-H. Li, M. Al-Amri, and M. S. Zubairy, Comment on "Past of a quantum particle", Phys. Rev. A **88**, 046102 (Oct 2013). 16, 28

[87] D. Sokolovski, Asking photons where they have been in plain language, Physics Letters A **381**(4), 227 – 232 (2017). 16, 28

[88] J. M. Ashby, P. D. Schwarz, and M. Schlosshauer, Observation of the quantum paradox of separation of a single photon from one of its properties, Phys. Rev. A **94**, 012102 (Jul 2016). 17

[89] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Bell's theorem without inequalities, American Journal of Physics **58**(12), 1131–1143 (1990). 17

[90] A. C. Elitzur and L. Vaidman, Quantum mechanical interaction-free measurements, Foundations of Physics **23**(7), 987–997 (Jul 1993). 18

[91] K. Yokota, T. Yamamoto, M. Koashi, and N. Imoto, Direct observation of Hardy's paradox by joint weak measurement with an entangled photon pair, New Journal of Physics **11**(3), 033011 (2009). 19

[92] P. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994. 19, 71

[93] D. J. Bernstein and T. Lange, Post-quantum cryptography, Nature **549**(7671), 188–194 (Sep 2017). 19, 71

[94] D. Bruss, G. Erdélyi, T. Meyer, T. Riege, and J. Rothe, Quantum Cryptography: A Survey, ACM Comput. Surv. **39**(2), 6–es (jul 2007). 19, 71

[95] M. Tomamichel and A. Leverrier, A largely self-contained and complete security proof for quantum key distribution, Quantum **1**, 14 (July 2017). 20, 49

[96] C. Portmann and R. Renner, Security in quantum cryptography, Rev. Mod. Phys. **94**, 025008 (Jun 2022). 20, 49

[97] D. Bruß, Optimal Eavesdropping in Quantum Cryptography with Six States, Phys. Rev. Lett. **81**, 3018–3021 (Oct 1998). 20, 45, 49, 72

[98] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661–663 (Aug 1991). 20, 71, 72

[99] C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. **68**, 3121–3124 (May 1992). 20, 72

[100] R. S. Bhati and Arvind, Do weak values capture the complete truth about the past of a quantum particle?, Physics Letters A **429**, 127955 (2022). 26, 43

[101] D. Sokolovski, Path probabilities for consecutive measurements, and certain "quantum paradoxes", Annals of Physics **397**, 474–502 (2018). 28

[102] N. Harrigan and R. W. Spekkens, Einstein, Incompleteness, and the Epistemic View of Quantum States, Foundations of Physics **40**(2), 125–157 (Feb 2010). 35, 91

[103] H. M. Wiseman, Weak values, quantum trajectories, and the cavity-QED experiment on wave-particle correlation, Phys. Rev. A **65**, 032111 (Feb 2002). 43, 44, 67

[104] R. Silva, Y. Guryanova, N. Brunner, N. Linden, A. J. Short, and S. Popescu, Pre- and postselected quantum states: Density matrices, tomography, and Kraus operators, Phys. Rev. A **89**, 012121 (Jan 2014). 43, 67

[105] D. Tan, S. J. Weber, I. Siddiqi, K. Mølmer, and K. W. Murch, Prediction and Retrodiction for a Continuously Monitored Superconducting Qubit, Phys. Rev. Lett. **114**, 090403 (Mar 2015). 43, 67

[106] L. Vaidman, A. Ben-Israel, J. Dziewior, L. Knips, M. Weißl, J. Meinecke, C. Schwemmer, R. Ber, and H. Weinfurter, Weak value beyond conditional expectation value of the pointer readings, Phys. Rev. A **96**, 032114 (Sep 2017). 43, 44, 47, 67, 69

[107] A. Peres, How to differentiate between non-orthogonal states, Physics Letters A **128**(1), 19 (1988). 44

[108] A. Chefles, Quantum state discrimination, Contemporary Physics **41**(6), 401–424 (Nov 2000). 44, 47

[109] J. Bae and L.-C. Kwek, Quantum state discrimination and its applications, Journal of Physics A: Mathematical and Theoretical **48**(8), 083001 (jan 2015). 44, 47

[110] R. Renner, Security of Quantum Key Distribution, 2006. 44, 45, 72

[111] R. Renner, N. Gisin, and B. Kraus, Information-theoretic security proof for quantum-key-distribution protocols, Phys. Rev. A **72**, 012332 (Jul 2005). 44, 45, 49, 72

[112] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. A. **461**, 207–235 (Oct 2005). 45, 53, 72

[113] C. W. Helstrom, Quantum detection and estimation theory, Journal of Statistical Physics **1**, 231–252 (1969). 45, 47

[114] A. S. Holevo, *Probabilistic and statistical aspects of quantum theory*, volume 1, Springer Science & Business Media, 2011. 45, 47

[115] A. K. Ekert, *Quantum Cryptography and Bell's Theorem*, pages 413–418, Springer US, Boston, MA, 1992. 71

[116] A. Acín, N. Gisin, and L. Masanes, From Bell's Theorem to Secure Quantum Key Distribution, Phys. Rev. Lett. **97**, 120405 (Sep 2006). 71

[117] E. S. Simon Kochen, The Problem of Hidden Variables in Quantum Mechanics, Indiana Univ. Math. J. **17**, 59–87 (1968). 71

[118] J. Singh, K. Bharti, and Arvind, Quantum key distribution protocol based on contextuality monogamy, Phys. Rev. A **95**, 062333 (Jun 2017). 71

[119] M. Pawłowski, Security proof for cryptographic protocols based only on the monogamy of Bell's inequality violations, Phys. Rev. A **82**, 032313 (Sep 2010). 71

[120] J. M. Renes and G. Smith, Noisy Processing and Distillation of Private Quantum States, Phys. Rev. Lett. **98**, 020502 (Jan 2007). 72

[121] H.-K. Lo and H. F. Chau, Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances, Science **283**(5410), 2050–2056 (1999). 72

[122] D. Gottesman and H.-K. Lo, Proof of security of quantum key distribution with two-way classical communications, IEEE Transactions on Information Theory **49**(2), 457–475 (2003). 72

[123] U. Maurer, Secret key agreement by public discussion from common information, IEEE Transactions on Information Theory **39**(3), 733–742 (1993). 72

[124] H. F. Chau, Practical scheme to share a secret key through a quantum channel with a 27.6Phys. Rev. A **66**, 060302 (Dec 2002). 72

[125] M. Boyer, D. Kenigsberg, and T. Mor, Quantum Key Distribution with Classical Bob, Phys. Rev. Lett. **99**, 140501 (Oct 2007). 72

[126] O. Amer and W. O. Krawec, Semiquantum key distribution with high quantum noise tolerance, Phys. Rev. A **100**, 022319 (Aug 2019). 72

[127] M. Curty, M. Lewenstein, and N. Lütkenhaus, Entanglement as a Precondition for Secure Quantum Key Distribution, Phys. Rev. Lett. **92**, 217903 (May 2004). 72

[128] N. Lutkenhaus and M. Jahma, Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack, New Journal of Physics **4**(1), 44 (jul 2002). 72

[129] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits, npj Quantum Information **3**(1), 25 (Jun 2017). 72

[130] S. Etcheverry, G. Cañas, E. S. Gómez, W. A. T. Nogueira, C. Saavedra, G. B. Xavier, and G. Lima, Quantum key distribution session with 16-dimensional photonic states, Scientific Reports **3**(1), 2316 (Jul 2013). 72

[131] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, High-dimensional quantum key distribution using dispersive optics, Phys. Rev. A **87**, 062322 (Jun 2013). 72

[132] D. Bunandar, Z. Zhang, J. H. Shapiro, and D. R. Englund, Practical high-dimensional quantum key distribution with decoy states, Phys. Rev. A **91**, 022336 (Feb 2015). 72

[133] S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, Experimental quantum cryptography with qutrits, New Journal of Physics **8**, 75 (May 2006). 72

[134] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000. 89

[135] W. H. Zurek, Quantum Theory of the Classical: Einselection, Envariance, Quantum Darwinism and Extantons, Entropy **24**(11) (2022). 90, 97

[136] H. Ollivier, D. Poulin, and W. H. Zurek, Environment as a witness: Selective proliferation of information and emergence of objectivity in a quantum universe, Phys. Rev. A **72**, 042113 (Oct 2005). 90, 97

[137] W. H. Zurek, Environment-Assisted Invariance, Entanglement, and Probabilities in Quantum Physics, Phys. Rev. Lett. **90**, 120404 (Mar 2003). 90

[138] H. Ollivier, D. Poulin, and W. H. Zurek, Objective Properties from Subjective Quantum States: Environment as a Witness, Phys. Rev. Lett. **93**, 220401 (Nov 2004). 90, 97

[139] W. H. Zurek, Decoherence, einselection, and the quantum origins of the classical, Rev. Mod. Phys. **75**, 715–775 (May 2003). 90

[140] W. H. Zurek, Quantum Darwinism, Nature Physics **5**(3), 181–188 (Mar 2009). 90, 97

[141] C. J. Riedel and W. H. Zurek, Quantum Darwinism in an Everyday Environment: Huge Redundancy in Scattered Photons, Phys. Rev. Lett. **105**, 020404 (Jul 2010). 90, 97

[142] C. J. Riedel and W. H. Zurek, Redundant information from thermal illumination: quantum Darwinism in scattered photons, New Journal of Physics **13**(7), 073038 (jul 2011). 90, 97

[143] A. Einstein, B. Podolsky, and N. Rosen, Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?, Phys. Rev. **47**, 777–780 (May 1935). 91

[144] P. Marage and G. Wallenborn, *The Debate between Einstein and Bohr, or How to Interpret Quantum Mechanics*, pages 161–174, Birkhäuser Basel, Basel, 1999. 91

[145] M. Fuwa, S. Takeda, M. Zwierz, H. M. Wiseman, and A. Furusawa, Experimental proof of nonlocal wavefunction collapse for a single particle using homodyne measurements, Nature Communications **6**(1), 6665 (Mar 2015). 91

[146] S. Popescu and D. Rohrlich, Quantum nonlocality as an axiom, Foundations of Physics **24**(3), 379–385 (Mar 1994). 91

[147] A. Peres and D. R. Terno, Quantum information and relativity theory, Rev. Mod. Phys. **76**, 93–123 (Jan 2004). 91

[148] P. H. Eberhard and R. R. Ross, Quantum field theory cannot provide faster-than-light communication, Foundations of Physics Letters **2**(2), 127–149 (Mar 1989). 91

[149] R. Blume-Kohout and W. H. Zurek, A Simple Example of "Quantum Darwinism": Redundant Information Storage in Many-Spin Environments, Foundations of Physics **35**(11), 1857–1876 (Nov 2005). 97

[150] A. Touil, B. Yan, D. Girolami, S. Deffner, and W. H. Zurek, Eavesdropping on the Decohering Environment: Quantum Darwinism, Amplification, and the Origin of Objective Classical Reality, Phys. Rev. Lett. **128**, 010401 (Jan 2022). 97

[151] M. Zwolak, H. T. Quan, and W. H. Zurek, Quantum Darwinism in a Mixed Environment, Phys. Rev. Lett. **103**, 110402 (Sep 2009). 97

[152] M. Zwolak, H. T. Quan, and W. H. Zurek, Redundant imprinting of information in nonideal environments: Objective reality via a noisy channel, Phys. Rev. A **81**, 062110 (Jun 2010). 97

[153] M. Zwolak, C. J. Riedel, and W. H. Zurek, Amplification, Redundancy, and Quantum Chernoff Information, Phys. Rev. Lett. **112**, 140406 (Apr 2014). 97

[154] M. Zwolak, C. J. Riedel, and W. H. Zurek, Amplification, Decoherence and the Acquisition of Information by Spin Environments, Scientific Reports **6**(1), 25277 (May 2016). 97

[155] N. Mirkin and D. A. Wisniacki, Many-Body Localization and the Emergence of Quantum Darwinism, Entropy **23**(11) (2021). 97

[156] R. Blume-Kohout and W. H. Zurek, Quantum Darwinism in Quantum Brownian Motion, Phys. Rev. Lett. **101**, 240405 (Dec 2008). 97

[157] R. Horodecki, J. K. Korbicz, and P. Horodecki, Quantum origins of objectivity, Phys. Rev. A **91**, 032122 (Mar 2015). 98

[158] J. K. Korbicz, P. Horodecki, and R. Horodecki, Objectivity in a Noisy Photonic Environment through Quantum State Information Broadcasting, Phys. Rev. Lett. **112**, 120402 (Mar 2014). 98

[159] J. A. Wheeler, The "Past" and the "Delayed-Choice" Double-Slit Experiment, in *Mathematical Foundations of Quantum Theory*, edited by A. Marlow, pages 9–48, Academic Press, 1978. 109, 110

[160] V. Jacques, E. Wu, F. Grosshans, F. Treussart, P. Grangier, A. Aspect, and J.-F. Roch, Experimental Realization of Wheeler's Delayed-Choice Gedanken Experiment, Science **315**(5814), 966–968 (2007). 110

[161] A. G. Manning, R. I. Khakimov, R. G. Dall, and A. G. Truscott, Wheeler's delayed-choice gedanken experiment with a single atom, Nature Physics **11**(7), 539–542 (Jul 2015). 110

[162] P. Shadbolt, J. C. F. Mathews, A. Laing, and J. L. O'Brien, Testing foundations of quantum mechanics with photons, Nature Physics **10**(4), 278–286 (Apr 2014). 110

[163] X.-s. Ma, J. Kofler, and A. Zeilinger, Delayed-choice gedanken experiments and their realizations, Rev. Mod. Phys. **88**, 015005 (Mar 2016). 110

[164] R. Ionicioiu and D. R. Terno, Proposal for a Quantum Delayed-Choice Experiment, Phys. Rev. Lett. **107**, 230406 (Dec 2011). 110

[165] A. Peruzzo, P. Shadbolt, N. Brunner, S. Popescu, and J. L. O'Brien, A Quantum Delayed-Choice Experiment, Science **338**(6107), 634–637 (2012). 110

[166] F. Kaiser, T. Coudreau, P. Milman, D. B. Ostrowsky, and S. Tanzilli, Entanglement-Enabled Delayed-Choice Experiment, Science **338**(6107), 637–640 (2012). 110

[167] K. Liu, Y. Xu, W. Wang, S.-B. Zheng, T. Roy, S. Kundu, M. Chand, A. Ranadive, R. Vijay, Y. Song, L. Duan, and L. Sun, A twofold quantum delayed-choice experiment in a superconducting circuit, Science Advances **3**(5), e1603159 (2017). 110

[168] S.-B. Zheng, Y.-P. Zhong, K. Xu, Q.-J. Wang, H. Wang, L.-T. Shen, C.-P. Yang, J. M. Martinis, A. N. Cleland, and S.-Y. Han, Quantum Delayed-Choice Experiment with a Beam Splitter in a Quantum Superposition, Phys. Rev. Lett. **115**, 260403 (Dec 2015). 110

[169] K. Wang, Q. Xu, S. Zhu, and X.-s. Ma, Quantum wave–particle superposition in a delayed-choice experiment, Nature Photonics **13**(12), 872–877 (Dec 2019). 110

[170] T. H. Yoon and M. Cho, Quantitative complementarity of wave-particle duality, Science Advances **7**(34), eabi9268 (2021). 110

[171] D.-X. Chen, Y. Zhang, J.-L. Zhao, Q.-C. Wu, Y.-L. Fang, C.-P. Yang, and F. Nori, Experimental investigation of wave-particle duality relations in asymmetric beam interference, npj Quantum Information **8**(1), 101 (Sep 2022). 110

[172] B.-G. Englert, Fringe Visibility and Which-Way Information: An Inequality, Phys. Rev. Lett. **77**, 2154–2157 (Sep 1996). 111

[173] B.-G. Englert, Fringe Visibility and Which-Way Information: An Inequality, Phys. Rev. Lett. **77**, 2154–2157 (Sep 1996). 112