

Entanglement assisted quantum communication protocols

Amélie Piveteau



Entanglement assisted quantum communication protocols

Amélie Piveteau

Academic dissertation for the Degree of Doctor of Philosophy in Physics at Stockholm University to be publicly defended on Thursday 19 March 2026 at 13.00 in sal FB55, AlbaNova universitetscentrum, Roslagstullsbacken 21, and online via Zoom, public link is available at the department website.

Abstract

Quantum entanglement plays a central role in many quantum communication protocols. It allows distant particles to share correlations beyond the limits of classical interactions. Entanglement is essential for superdense coding, quantum teleportation, and secure cryptographic key distribution in quantum communication. It is also a pillar for developing quantum networks, where the management and distribution of entanglement are crucial for connecting distant nodes. Although perfect entanglement is a sought-after ideal, experimental imperatives, including entanglement distribution over long distances, often limit the quality of entangled states. An important question is whether weaker entanglement still offers advantages.

First, we study more general tasks than dense coding to show that simpler measurements, combined with entanglement, allow advantageous and sometimes even optimal qubit communication protocols to be obtained. We also demonstrate that simple measurements can generate quantum correlations that cannot be modelled by two classical communication bits and can constitute an optimal protocol with quantum resources.

We implement a novel Bell-type inequality tailored for certifying full network non-locality (FNN) to develop certification methods guaranteeing security on an entanglement-based network. Our experiment uses two pairs of polarised entangled photons in a network configuration with three nodes, briefly referred to as a bilocal network scenario.

Finally, we show that weakly entangled states can improve communication over a qubit channel using only separate (local) measurements on isotropic non-steerable two-qubit states, without interference, of individual photons, across two communication tasks: secret sharing and its stochastic variant.

Keywords: *entanglement, quantum communication, quantum optic, experimental demonstration.*

Stockholm 2026
<http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-252072>

ISBN 978-91-8107-510-6
ISBN 978-91-8107-511-3

Department of Physics

Stockholm University, 106 91 Stockholm



ENTANGLEMENT ASSISTED QUANTUM COMMUNICATION
PROTOCOLS

Amélie Piveteau



Stockholm
University

Entanglement assisted quantum communication protocols

Amélie Piveteau

©Amélie Piveteau, Stockholm University 2026

ISBN print 978-91-8107-510-6

ISBN PDF 978-91-8107-511-3

Printed in Sweden by Universitets service US-AB, Stockholm 2026

Abstract

Quantum entanglement plays a central role in many quantum communication protocols. It allows distant particles to share correlations beyond the limits of classical interactions. Entanglement is essential for superdense coding, quantum teleportation, and secure cryptographic key distribution in quantum communication. It is also a pillar for developing quantum networks, where the management and distribution of entanglement are crucial for connecting distant nodes. Although perfect entanglement is a sought-after ideal, experimental imperatives, including entanglement distribution over long distances, often limit the quality of entangled states. An important question is whether weaker entanglement still offers advantages.

First, we study more general tasks than dense coding to show that simpler measurements, combined with entanglement, allow advantageous and sometimes even optimal qubit communication protocols to be obtained. We also demonstrate that simple measurements can generate quantum correlations that cannot be modelled by two classical communication bits and can constitute an optimal protocol with quantum resources.

We implement a novel Bell-type inequality tailored for certifying full network non-locality (FNN) to develop certification methods guaranteeing security on an entanglement-based network. Our experiment uses two pairs of polarised entangled photons in a network configuration with three nodes, briefly referred to as a bilocal network scenario.

Finally, we show that weakly entangled states can improve communication over a qubit channel using only separate (local) measurements on isotropic non-steerable two-qubit states, without interference, of individual photons, across two communication tasks: secret sharing and its stochastic variant.

Résumé

L'intrication quantique joue un rôle central dans de nombreux protocoles de communication quantique. Elle permet à des particules distantes de partager des corrélations qui dépassent les limites des interactions classiques. En communication quantique, l'intrication est essentielle pour des processus tels que le superdense coding, la téléportation quantique et la distribution de clés cryptographiques sécurisées. Elle constitue également un pilier pour le développement des réseaux quantiques, où la gestion et la distribution de l'intrication sont cruciales pour connecter des nœuds éloignés. Bien que l'intrication parfaite soit un idéal recherché, les impératifs expérimentaux et les contraintes liées à la distribution de l'intrication sur de longues distances limitent souvent la qualité des états intriqués. Une intrication plus faible présente elle encore des avantages ?

Afin de d'apporter des premières réponses à ces questions, nous étudions dans un premier temps des tâches de communication plus générales que le "dense coding", afin de démontrer que des mesures plus simples permettent d'obtenir des protocoles de communication de qubits puissants et parfois même optimaux grâce à l'intrication. Notre étude confirme que des mesures simples suffisent à générer des corrélations quantiques qui ne peuvent être modélisées par deux bits de communication classique et qui peuvent constituer un protocole optimal pour les ressources quantiques. Dans un second temps, Nous nous intéressons au développement de méthodes de certification pour garantir la sécurité sur un réseau basé sur l'intrication. Nous étudions expérimentalement une nouvelle inégalité de type Bell conçue pour certifier la non-localité totale d'un réseau (FNN). Notre expérience est mise en œuvre en utilisant deux paires de photons intriqués polarisés dans une configuration de réseau à trois nœuds, appelée scénario de réseau bilocal.

Finalement, nous montrons que les états faiblement intriqués peuvent améliorer la communication sur un canal qubit en utilisant uniquement des mesures séparées sur des états isotropes non pilotable à deux qubits, sans interférence, de photons individuels, à travers deux tâches de communication : le partage de secret et sa variante stochastique.

Sammanfattning

Sammanflätning spelar en central roll i många kvantkommunikationsprotokoll. Den gör det möjligt för avlägsna partiklar att dela korrelationer som går bortom gränserna för klassiska interaktioner. Sammanflätning är avgörande för supertät kodning, kvantteleportering och säker kryptografisk nyckeldistribution inom kvantkommunikation. Den utgör också en pelare för utvecklingen av kvantnätverk, där hantering och distribution av sammanflätning är avgörande för att koppla samman noder på avstånd. Även om perfekt sammanflätning är ett eftersträvarsvärt ideal, begränsar ofta experimentella krav, inklusive distribution av sammanflätning över långa avstånd, kvaliteten på de sammanflätade tillstånden. En viktig fråga är om svagare sammanflätning fortfarande erbjuder fördelar.

Först studerar vi mer allmänna uppgifter än densitetskodning för att visa att enklare mätningar, i kombination med sammanflätning, gör det möjligt att uppnå fördelaktiga och ibland till och med optimala qubit-kommunikationsprotokoll. Vi visar också att enkla mätningar kan generera kvantkorrelationer som inte kan modelleras av två klassiska kommunikationsbitar och kan utgöra ett optimalt protokoll med kvantresurser.

Vi implementerar en ny Bell-olikhet som är skräddarsydd för att certifiera fullständig nätverks-icke-lokalitet (FNN) för att utveckla certifieringsmetoder som garanterar säkerhet i ett sammanflätningbaserat nätverk. Vårt experiment använder två par polariserat sammanflätade fotoner i en nätverkskonfiguration med tre noder, kortfattat kallat ett bilokalt nätverksscenario.

Slutligen visar vi att svagt sammanflätade tillstånd kan förbättra kommunikationen över en qubitkanal genom att endast använda separata (lokala) mätningar på isotropa, icke-styrbara två-qubit-tillstånd, utan interferens från enskilda fotoner, över två kommunikationsuppgifter: hemlig delning och dess stokastiska variant.

*Que dites-vous?... C'est inutile?... Je le sais!
Mais on ne se bat pas dans l'espoir du succès!
Non! non, c'est bien plus beau lorsque c'est
inutile!*

Edmond Rostand
Cyrano de Bergerac

But who fights ever hoping for success?
I fought for a lost cause, and for a fruitless quest!

The paraphraser, grammar checker, and translation tools from QuillBot were used, as well as Grammarly's grammar and spelling correction option to correct and improve the English in this document.

List of Papers

The following papers, referred to in the text by their Roman numerals, are included in this thesis.

PAPER I: Entanglement-assisted quantum communication with simple measurements

Amélie Piveteau, Jef Pauwels, Emil Håkansson, Sadiq Muhammad, Mohamed Bourennane, Armin Tavakoli *Nat Commun*, **13**, 7878 (2022).

DOI: 10.1038/s41467-022-33922-5

PAPER II: Experimental demonstration of full network nonlocality in the bilocal scenario

Emil Håkansson, Amélie Piveteau, Sadiq Muhammad, Mohamed Bourennane, Submitted

arXiv:2201.06361

PAPER III: Weak entanglement improves quantum communication using only product measurements

Amélie Piveteau, Alastair A. Abbott, Sadiq Muhammad, Mohamed Bourennane, Armin Tavakoli, *Phys. Rev. Applied*, **21**, 034053 (2024).

DOI: 10.1103/PhysRevApplied.21.034053

Reproductions are arXiv versions until permission is obtained from the publishers.

Author's contribution

The following papers, referred to in the text by their Roman numerals, are included in this thesis.

PAPER I: Entanglement-assisted quantum communication with simple measurements

I carried out the experimental work: building the setup, determining the settings to use for the measurements, and measuring and analysing the data. I wrote the experimental section of the supplementary materials, created the diagram and description of the experimental setup, and participated in the reviews and corrections of the entire article.

PAPER II: Experimental demonstration of full network nonlocality in the bilocal scenario

I took part in the discussion on creating the source, aligned the setup with the new source and I participated in the reviews and corrections of the article.

PAPER III: Weak entanglement improves quantum communication using only product measurements

I conducted the experimental work: building the setup, measuring and analysing the data. I participated in the writing of the article: I wrote the experiment section that describes the experimental work and the results obtained, as well as appendices B to I, I also took part in the proofreading and correction of the article.

Relevant papers not included in the thesis

- PAPER 1: **Experimental certification of more than one bit of quantum randomness in the two inputs and two outputs scenario**
Alban Jean-Marie Seguinard, Amélie Piveteau, Piotr Mironowicz, Mohamed Bourenane *New J. Phys.*, **25**, 113022 (2023).
DOI: 10.1088/1367-2630/ad05a6
- PAPER 2: **Optimization of experimental quantum randomness expansion**
Amelie Piveteau, Alban Seguinard, Piotr Mironowicz, Mohamed Bourenane, *Phys. Rev. Applied*, **24**, 044096 (2025).
DOI: 10.1103/hc3f-3pbw
- PAPER 3: **Experimental implementation of dimension-dependent contextuality inequality**
Emil Håkansson, Amelie Piveteau, Alban Seguinard, Muhammad Sadiq, Mohamed Bourenane, Otfried Gühne, and Martin Plávala, *Phys. Rev. Lett.* , **134**, 200202 (2025).
DOI: 10.1103/PhysRevLett.134.200202
-

Contents

| | |
|---|--------------|
| Abstract | vii |
| Résumé | ix |
| Sammanfattning | xi |
| List of Papers | xvii |
| Author's contribution | xix |
| Relevant papers not included in the thesis | xxi |
| List of Figures | xxvii |
| List of Tables | xxix |
| Acknowledgements | xxxii |
| 1 Introduction | 33 |
| 2 Quantum optics and quantum information | 35 |
| 2.1 Superposition | 35 |
| 2.2 Quantum states | 35 |
| 2.2.1 Pure states | 37 |
| 2.2.2 Mixed states | 38 |
| 2.2.3 Multipartite states | 39 |
| 2.3 Measurement | 40 |
| 2.3.1 Projective measurement | 42 |
| 2.3.2 Indistinguishability | 42 |
| 2.4 Qubit | 43 |
| 2.5 Quantum correlation | 46 |
| 2.6 Entanglement | 47 |
| 2.6.1 2-qubit entanglement | 48 |

| | | |
|----------|--|-----------|
| 2.7 | Bell inequality | 49 |
| 2.7.1 | Nonlocality | 49 |
| 2.7.2 | Einstein-Podolsky-Rosen(EPR) paradox | 49 |
| 2.7.3 | Bell's inequality | 50 |
| 2.7.4 | CHSH inequality | 52 |
| 2.8 | Multipartite Entanglement | 54 |
| 2.8.1 | 3-partite entanglement | 54 |
| 2.9 | Polarisation encoding | 55 |
| 2.10 | Polarisation single-photon state preparation | 56 |
| 2.11 | Single photon polarisation transformation | 57 |
| 2.12 | Single Photon Polarisation Measurement | 59 |
| 2.13 | Entanglement source | 61 |
| 2.14 | Quantum interference and HOM | 64 |
| 2.15 | Bell's measurement | 67 |
| 2.15.1 | Bell's states | 67 |
| 2.15.2 | Bell measurement | 68 |
| 2.16 | Application : GHZ state preparation | 69 |
| 2.17 | Steerability | 70 |
| 2.17.1 | Steerability and Bell's States | 72 |
| 2.17.2 | Werner's states | 73 |
| 3 | Quantum communication | 75 |
| 3.1 | Introduction | 75 |
| 3.1.1 | No-cloning | 75 |
| 3.1.2 | Teleportation | 76 |
| 3.1.3 | SuperDense Coding | 78 |
| 3.1.4 | Random Access Code | 79 |
| 4 | Experiments | 83 |
| 4.1 | Entanglement-assisted quantum communication with simple measurements | 83 |
| 4.2 | Quantum Network | 86 |
| 4.3 | Weak entanglement improves quantum communication using only product measurements | 88 |
| 5 | Conclusion and outlook | 91 |
| 5.1 | Entanglement-assisted quantum communication with simple measurements | 91 |
| 5.2 | Quantum Network | 92 |
| 5.3 | Weak entanglement improves quantum communication using only product measurements | 92 |

List of Figures

| | | |
|-----|--|----|
| 2.1 | In this example, the non-orthogonal states blue and green cannot be perfectly distinguished, they each have a component which projects onto state $ \uparrow\rangle$ and one onto state $ \downarrow\rangle$. If we rotate the basis so that one of the states has a component on only one of the two axes, the second state will always have a component on this same axis, and the states cannot be perfectly distinguished i.e any measurement intended to separate them will have a fundamental probability of error. | 44 |
| 2.2 | Representation of a qubit on the surface of the Bloch sphere. | 46 |
| 2.3 | Spatial representation of $ H\rangle$, $ V\rangle$, $ R\rangle$, $ L\rangle$, $ D\rangle$ and $ A\rangle$ on a Bloch Sphere. | 56 |
| 2.4 | To prepare a photon in the desired polarisation, a polarising beam splitter (PBS) followed by a half-wave plate (HWP) and a quarter-wave plate (QWP) can be used to achieve the required configuration polarisation. | 57 |
| 2.5 | Transformation of a PBS to distinguish different orthogonal polarisations. To obtain the circular polarisation basis (left/right), a quarter-wave plate oriented at 45° with respect to the horizontal axis introduces a relative phase shift of $\pi/2$ between the H and V components, converting linear polarisations into circular ones. Alternatively, to access the diagonal basis, a half-wave plate (HWP) aligned at 22.5° relative to the horizontal axis rotates the polarisation direction by 45° , transforming H and V states into the diagonal 45° states. | 59 |
| 2.6 | Measurement station: using PBS, HWP, and QWP, the polarisation of any state can be determined. The optical signal is converted into an electrical signal through the detectors, which are connected to a coincidence unit that counts the number of photons arriving at each detector and the coincidences between them. | 60 |
| 2.7 | Energy level of the second harmonic generation process. | 62 |

| | | |
|------|--|----|
| 2.8 | Spontaneous In the Down Conversion process, (a) Type I exhibits propagation directions that form two concentric cones. (b) Type II shows propagation directions that form two cones symmetrically tilted to the direction of the pump photons. . . . | 64 |
| 2.9 | Two Indistinguishable photons arrive simultaneously at the input channels a and b of a beamsplitter. Two single-photon detectors, c and d, record which of the two paths the photons exit: c or d through. | 65 |
| 2.10 | Hong-Ou-Mandel dip setup. To avoid overloading the figure, only one mode of PBS output is considered here; however, what applies to one mode may also apply to the others. | 66 |
| 2.11 | Partial Bell's states analyser. | 68 |
| 2.12 | Setup for GHZ states preparation. | 69 |
| 2.13 | Hierarchical relationship between entanglement, steerability, and violations of Bell's inequality: States that have a local hidden variable model and therefore do not violate any Bell inequality form a convex subset. States with an LHS model are not steerable and form a convex subset of LHV states. Finally, separable states are a convex subset of LHS states. . . . | 72 |
| 3.1 | Alice performs a BSM on the unknown qubit and a photon from the entangled state. The result does not disclose the state of the qubit but is sent to Bob, who performs a result-dependent operation to complete the teleportation and obtain the same state as Alice's unknown state. | 77 |
| 3.2 | Alice bob and Alice share an entangled pair. Alice performs a unitary transformation and sends a qubit to Bob, who can determine Alice's initial state with a Bell state measurement. . . . | 79 |
| 3.3 | Advantage of QRAC2 \rightarrow 1 over RAC2 \rightarrow 1. | 81 |

List of Tables

| | | |
|-----|--|----|
| 2.1 | Orientation of an HWP to obtain the following states from an initial state $ H\rangle$ | 58 |
| 2.2 | Orientation of a QWP to obtain the following states from an initial state $ H\rangle$ | 58 |

Acknowledgements

It will be very difficult for me to thank everyone, because it is thanks to the help of many people that I was able to complete this thesis.

First and foremost, I would like to thank Mohamed Bourennane, my PhD supervisor in Stockholm, for his trust, support, encouragement and kindness. Thank you to him for giving me the opportunity to work on numerous experiments in his laboratory. Through him, I was able to deepen my knowledge and develop my skills.

A big thank you also to Jean-Marc Merolla, my co-supervisor, for trusting me when I contacted him after graduating from engineering school to ask him to take me on as a PhD student. Thanks to him, I had the opportunity to do my thesis under the joint supervision of two laboratories. Many thanks for his patience and help throughout my thesis.

Thank you to all my collaborators and colleagues with whom I had the opportunity to work, Alastair A. Abbott, Armin Tavakoli, Jef Pauwels, Martin Plávala, Otfried Gühne and Piotr Mironowicz. I learned a lot from working with you.

A very big thank you to Sadiq Muhammad, without whom I would not have been able to complete any of these experiments. Thank you for always taking the time to answer my questions, from the simplest to the most complicated, and for being so often available to help me in the laboratory.

Thank you to all current and former members of the KIKO group, Alban, Amina, Ang, Ashraf, Emil, Hamad, Mario, Merse, Nassim, Robert, Thomas and Walid thank you for your good humour, your advice, and your attentive ears.

And although they did not directly accompany me in this thesis, I would like to warmly thank Yannick Dumeige and Patrice Féron, whose courses in introduction to quantum optics and quantum cryptography at engineering school inspired me to do a thesis in this field.

Finally, I would like to thank all those who contributed, directly or indirectly, to the completion of this manuscript. Through enriching discussions, advice or simply their presence, their contribution has been invaluable. I am deeply grateful to all those who supported me during my thesis; I could not have done it without you.

1. Introduction

Quantum entanglement, a fundamental phenomenon in quantum mechanics where distant particles share correlations that exceed classical limits, is at the core of many advances in quantum communication. It is indispensable for protocols such as superdense coding, quantum teleportation, and quantum key distribution (QKD) [1]. Beyond these applications, entanglement is also the cornerstone of quantum network development, where its management and distribution are crucial for connecting distant nodes.

However, experimental constraints impose limits on the quality of entangled states. Even when achieving near-perfect entanglement, above 99% at the source, the quality of this entanglement is no longer the same if we seek to distribute the photons over several kilometers. Does weaker entanglement still offer advantages once it is degraded? In what context? With what constraints? This thesis explores the advantages of lower-quality entanglement, answering the crucial question of whether "weaker" entanglement can still offer significant benefits for quantum communications.

First, we broaden the scope of communication tasks beyond dense coding to demonstrate that simpler measurements can lead to powerful, even optimal, qubit communication protocols thanks to entanglement. Our research confirms that elementary measurements are sufficient to generate quantum correlations that cannot be surpassed by classical communication, thus laying the foundations for optimal protocols for quantum resources.

Secondly, we focus on developing certification methods to guarantee the security of entanglement-based networks. We are experimentally exploring a new Bell-type inequality designed to certify full network non-locality (FNN). This experiment is performed using two pairs of polarisation-entangled photons in a three-node network configuration, known as a bilocal network scenario.

Finally, we demonstrate how weakly entangled states can improve communication over a qubit channel. This is achieved by using only separate measurements on non-steerable isotropic two-qubit states, without interference from individual photons, through two distinct communication tasks: secret sharing and its stochastic variant.

This thesis thus offers an in-depth exploration, through communication protocols and experimental implementations, of entanglement as a resource,

not only in its ideal forms but also in its more modest yet exploitable manifestations.

2. Quantum optics and quantum information

Information is a quantifiable quantity, and its unit is called a bit or a qubit, depending on whether the physical system used to encode it is classical or quantum [2]. Quantum information is a field of physics that leverages the unique principles of quantum mechanics to process and transmit information in ways that are only possible with quantum systems.

2.1 Superposition

Superposition is one of the fundamental principles of quantum mechanics. Young's double-slit interference experiment with single photons is a classic demonstration of superposition in optics [3]. According to quantum mechanics, particles such as photons can exhibit wave-like behavior [4; 5]. When these wavelike photons pass through the slits, their associated wave functions interfere with each other, producing an interference pattern on a screen placed behind the slits. This pattern results from the superposition of the wave functions originating from both slits.

Remarkably, this interference persists even when photons are sent through the apparatus one at a time. In such cases, each photon behaves as if it has a probability amplitude of passing through both slits simultaneously. Over time, the accumulation of many single-photon detections reconstructs the same interference pattern observed with a continuous beam of light. This phenomenon is explained by the quantum superposition of all possible paths the photon could take.

2.2 Quantum states

A quantum state describes the configuration of a quantum system at a given time. Unlike a classical state, which maps directly to definite physical properties, a quantum state is a mathematical abstraction that yields a probabilistic distribution of observables upon measurement. Examples of quantum states include :

- **The spin of a particle:** The spin of a particle, such as an electron, can exist in a superposition of ‘up’ and ‘down’ states until it is measured.
- **The polarisation of a photon:** The polarisation state of a photon can be vertically or horizontally polarised, or it can exist in a superposition of both [6].

Unlike classical physics, which relies on familiar mathematical symbols such as numbers and vectors, quantum mechanics explores the probabilistic and wavelike nature of particles. Hence, its description is based on a unique mathematical framework using the Hilbert space.

Hilbert space plays a fundamental role in the representation and description of quantum states [6]. This vector space, equipped with a specific mathematical structure, allows us to quantify the properties of quantum systems. It has a Hermitian scalar product, which enables the definition of notions of length, angle, and orthogonality between vectors. In addition, a Hilbert space is complete, which means that all convergent sequences of vectors in this space have a limit that also belongs to the space.

We use Dirac notation with kets ($|\psi\rangle$) and bras ($\langle\psi|$) to represent quantum states. These symbols of kets and bra represent specific configurations (pure states) or more complex superpositions of multiple states (mixed states). The operators, designated by hats ($\hat{}$), represent physical quantities such as momentum or energy. When these operators act on kets, they can modify the state or extract information about its properties. To calculate the probability of finding a system in a state ϕ if it is currently in a state ψ , we use the inner product, written as $\langle\phi|\psi\rangle$.

The Hermitian scalar product is a scalar product between two vectors, denoted by $|\psi\rangle$ and $|\phi\rangle$ in the Hilbert space. The result, written as $\langle\phi|\psi\rangle$, is a complex number with properties: linearity, hermiticity (for all vectors $|\psi\rangle$ and $|\phi\rangle$, $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$ (* represent the complex conjugate)), positivity ($\langle\phi|\phi\rangle \geq 0$ for any vector $|\phi\rangle$. $\langle\phi|\phi\rangle = 0$ if and only if $|\phi\rangle = 0$ the null vector) and completeness.

By manipulating these elements, ket, bra, operators, and inner products, we can express the evolution of quantum systems and calculate probabilities of measurement outcomes.

The state of the system in quantum mechanics is described by a wave function Ψ . This state can be written as a linear combination of states called eigenstates:

$$|\Psi\rangle = \sum_{i=1}^N c_i |u_i\rangle. \quad (2.1)$$

These states $|u_i\rangle$ define a basis. These eigenstates are the ‘observable’ states of the system.

2.2.1 Pure states

A pure state represents a quantum system in a state of maximum possible information. It provides the most complete description allowed by quantum mechanics. However, while the state itself is perfectly defined, the outcomes of measurement remain fundamentally probabilistic for any observable that is not an eigenstate of that system.

A state vector mathematically represents a pure state, denoted $|\psi\rangle$, in the Hilbert space of the system. This state vector must be normalised, meaning that the total probability of finding the system in this state is equal to 1. A pure state cannot be a mixture of other states. It is a unique and defined configuration of the system.

Temporal evolution: The pure state of a system can evolve due to interactions with its environment or the application of external forces. Schrödinger's equation describes this evolution :

$$i\hbar \frac{\partial \Psi(x,t)}{\partial t} = \hat{H}\Psi(x,t) \quad (2.2)$$

with :

- $i\hbar$ is the imaginary unit multiplied by the reduced Planck constant ($\hbar = h/2\pi$).
- $\Psi(x,t)$ is the wave function of the system, which represents the quantum state at position x and time t .
- \hat{H} is the Hamiltonian operator, which describes the total energy of the system.
- $\frac{\partial}{\partial t}$ represents the partial derivative with respect to time.

Examples of pure states are :

- An electron can exist in the $|\psi\rangle = a|\uparrow\rangle + b|\downarrow\rangle$ state, where $|\uparrow\rangle$ and $|\downarrow\rangle$ are spin up and down quantum states and a and b are complex numbers satisfying the normalisation condition $|a|^2 + |b|^2 = 1$.
- A linearly polarised photon $|\psi\rangle = a|H\rangle + b|V\rangle$, with $|H\rangle$ is the horizontally polarised photon state and $|V\rangle$ is the vertically polarised photon state.

Pure states are fundamental elements of quantum mechanics and play a crucial role in understanding the behaviour of quantum systems.

2.2.2 Mixed states

States that are not pure are referred to as mixed states. A mixed state is a probabilistic description of the state of a quantum system at a given time. Unlike a pure state, which corresponds to a single, perfectly defined configuration of the system, a mixed state is a combination of several possible pure states, with probabilities associated with each state.

A mixed state is described as a statistical mixture of pure states. It is mathematically represented by a density matrix, denoted by ρ , which is defined as:

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i| \quad (2.3)$$

where p_i represents the probability of the system being in the pure state $|\psi_i\rangle$, satisfying $0 \leq p_i \leq 1$. For ρ to represent a physically valid state, it must be normalized, meaning its trace must equal one:

$$\text{Tr}(\rho) = \sum_i p_i = 1 \quad (2.4)$$

This normalisation condition ensures that the sum of the probabilities over all possible pure states in the ensemble is exactly unity. Furthermore, the density matrix must be positive semi-definite ($\rho \geq 0$), ensuring that any measurement outcome yields a non-negative probability.

The mixed state of a system can evolve due to interactions with its environment or the application of external forces. A modified version of Schrödinger's equation for mixed states, known as the equation of motion, describes this evolution:

$$i\hbar \frac{\partial \rho(x,t)}{\partial t} = \hat{H}\rho(x,t) - \rho(x,t)\hat{H} \quad (2.5)$$

where :

- \hbar is the imaginary unit multiplied by the reduced Planck constant ($\hbar = h/2\pi$).
- \hat{H} is the Hamiltonian operator, which describes the system's total energy.
- $\frac{\partial}{\partial t}$ represents the partial derivative with respect to time.
- and $\rho(x,t)$ is the density matrix, which represents the probabilities of finding the system in each possible pure state.

Mixed states are, for example :

- A set of identical particles in an excited state, where each particle can be in one of several possible energy states.
- $\rho = a|\uparrow\rangle\langle\uparrow| + b|\downarrow\rangle\langle\downarrow|$.
- A maximally mixed state is as following $\mathbb{1} = \frac{1}{2}|\uparrow\rangle\langle\uparrow| + \frac{1}{2}|\downarrow\rangle\langle\downarrow|$.

Mixed states are much more common than pure states in real quantum systems. Most quantum systems interact with their environment, causing a pure state to evolve into a mixed state, a process known as decoherence.

2.2.3 Multipartite states

Let us start with the case of bipartite systems [7]. Consider two quantum systems A and B , whose associated Hilbert spaces are, respectively, \mathcal{H}_A and \mathcal{H}_B . The Hilbert space of the composite system $A + B$ is then given by the tensor product of the two individual Hilbert spaces :

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B. \quad (2.6)$$

An element of this space, which represents a state of the composite system, is a linear combination of tensor products of states of the subsystems:

$$|\psi\rangle_{AB} = \sum_{i,j} c_{i,j} |i\rangle_A \otimes |j\rangle_B \quad (2.7)$$

with $|i\rangle_A$ and $|j\rangle_B$ are, respectively, the basis of \mathcal{H}_A and \mathcal{H}_B and $c_{i,j}$ are complex coefficients.

Among these multipartite states, we distinguish between separable and non-separable states. A particular state of a composed system is a factorisable state (or direct product) if it can be written in the form :

$$|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B, \quad (2.8)$$

in this case, the states of the two subsystems are independent of each other.

However, not all states of a composite system can be factorised. Some states exhibit quantum correlations between the measurement outcomes in the subsystems. These states are called correlated states. These correlations will play a central role in the following chapters, where we will explore the phenomenon of entanglement in detail.

To illustrate, let us consider two spins of particles, each of which can take the values \uparrow or \downarrow . The Hilbert space of each qubit is of dimension 2. The Hilbert space of the composite system is therefore of dimension 4. An example of a factorisable state is :

$$|\psi\rangle_{AB} = |\uparrow\rangle_A \otimes |\downarrow\rangle_B, \quad (2.9)$$

this state corresponds to a situation where the first spin is in state \uparrow and the second in state \downarrow . An example of a correlated state is as follows:

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|\uparrow\rangle_A \otimes |\downarrow\rangle_B + |\downarrow\rangle_A \otimes |\uparrow\rangle_B), \quad (2.10)$$

this state is not factorisable.

These principles can be generalised to higher dimensions [8]. For a d-dimensional state, the N-partite state is :

$$|\psi\rangle = \sum_{i,j,\dots}^N c_{ij\dots} |ij\dots\rangle \quad (2.11)$$

with $c_{i,j,\dots}$ the probability amplitude for each term.

Here is an example of a three-partite state :

$$|\psi\rangle = \frac{1}{\sqrt{2}}[|\uparrow\uparrow\uparrow\rangle + |\downarrow\downarrow\downarrow\rangle]. \quad (2.12)$$

2.3 Measurement

Measurement could be described as any process that generates values that are linked to a physical quantity. Whereas in classical physics, the system under study can be in a state independent of any observer and be measured without disturbance, in quantum physics, a measurement is a more complex process, in which the state of the object being measured is generally modified. The result of the measurement and its effect on the system are statistically described, since theory can only determine the probability of an outcome.

In quantum mechanics, the state of a system is described by a complex mathematical function called the wave function. This wave function can be decomposed into a combination of specific states, called eigenstates, each with a corresponding eigenvalue. When we measure a particular property, called an observable of the quantum system, the wave function is projected onto one of the eigenstates associated with that observable. The probability of obtaining a particular measurement result is determined by the squared absolute value (modulus squared) of the coefficient of that eigenstate in the original wave function.

The Copenhagen interpretation suggests that some properties of a system corresponding to the eigenstates of the measurement operator, such as its position or momentum, are not definite until measured. If a system is not already

in one of these eigenstates, the property essentially does not have a specific value. The act of measurement "collapses" the system's wave function into one of these eigenstates, giving the property a definite value.

We call an observable a measurable element and describe it using a Hermitian operator. These observables have eigenvalues with associated eigenstates corresponding to the Hermitian operator eigenvectors.

Mathematically, observables are self-adjoint operators, which means that the adjoint of the operator is equal to the operator itself.

Consider an observable \mathcal{A} , we know that the set of orthonormal eigenvectors forms an orthonormal basis of the state space :

$$\{|\alpha_1\rangle, \dots, |\alpha_n\rangle\}, \mathcal{A}|\alpha_i\rangle = a_i|\alpha_i\rangle. \quad (2.13)$$

Any state $|\psi\rangle$ can be expressed as a linear combination of the basis vectors. These basis vectors are often the eigenvectors of an observable quantity: $|\psi\rangle = \sum_i c_i |\alpha_i\rangle$ with $c_i = \langle \alpha_i | \psi \rangle$ the linear decomposition coefficients on this basis.

The norm of a vector must be unity $\langle \psi | \psi \rangle$. The basis being orthonormal, the scalar product between two vectors of the basis is 1 if it is the same vector and 0 in other cases: $\langle \alpha_i | \alpha_j \rangle = \delta_{ij}$. So : $\sum_i |c_i|^2 = 1$.

Let's now calculate the expectation value of the observable \mathcal{A} for the state represented by $|\psi\rangle$. By definition, we should calculate the following scalar product:

$$\begin{aligned} \langle a \rangle &= \langle \psi | \mathcal{A} | \psi \rangle \\ &= \left(\sum_j c_j^* \langle \alpha_j | \right) \mathcal{A} \left(\sum_i c_i |\alpha_i\rangle \right) \\ &= \left(\sum_j c_j^* \langle \alpha_j | \right) \left(\sum_i c_i \mathcal{A} |\alpha_i\rangle \right) \\ &= \left(\sum_j c_j^* \langle \alpha_j | \right) \left(\sum_i c_i a_i |\alpha_i\rangle \right) \\ &= \sum_i a_i |c_i|^2 \end{aligned} \quad (2.14)$$

It is also known that the value is given by the sum of the products of the possible values by the probability of measuring each value:

$$\langle a \rangle = \sum_i p_i a_i, \quad (2.15)$$

hence :

$$p_i = |c_i|^2 \tag{2.16}$$

the squared module of the linear decomposition coefficient corresponds to the probability of measuring the eigenvalue a_i . This provides a physical interpretation for the linear decomposition coefficient.

Let's notice that the result of a measurement can only be an eigenvalue of the observable. Still, the average of a large number of measurements can give a priori any value.

2.3.1 Projective measurement

The projective measure is the most fundamental type of measurement, which I used in my experiments. It corresponds to the collapse of the wave function onto an eigenstate of an observable. This type of measurement is disturbing, discrete, and probabilistic.

During a projective measurement, the wave function collapses and the particle finds itself in a well-defined state, corresponding to one of the possible values of the measurement. Mathematically, the collapse of the wave function is described by a projection onto a subspace associated with the measured value. It is as if we were 'projecting' the wave function onto a particular axis.

Let $|a_i\rangle$ be the system's state vector before the measurement and $|a_i\rangle$ an orthonormal basis of eigenvectors of an observable associated with the measurement. According to the measurement postulate, the probability of obtaining the eigenvalue a_i is given by Born's rule:

$$P(a_i) = |\langle a_i | \psi \rangle|^2, \tag{2.17}$$

if the value a_i is obtained, the system 'collapses' into the state $|a_i\rangle$. This collapse is described mathematically by the projection operator :

$$|\psi'\rangle = \frac{\hat{P}_i |\psi\rangle}{\sqrt{\langle \psi | \hat{P}_i | \psi \rangle}} \tag{2.18}$$

where $\hat{P}_i = |a_i\rangle \langle a_i|$ is the projector on the state $|a_i\rangle$.

2.3.2 Indistinguishability

Suppose two photons, indistinguishable by their spatial or spectral modes, collide in a beam splitter (BS). In that case, it is impossible to distinguish between the scenarios where they have both been transmitted and the instances where they have both been reflected. This uncertainty arises directly from the principle of indistinguishability in quantum mechanics: when two particles are

identical, it is impossible to track them individually, and all information about their trajectory is lost [9].

If two states are orthogonal, it is theoretically possible to distinguish them with certainty through a single measurement. Their lack of overlap ensures that a measurement of one will never be mistaken for the other. By performing a suitable projective measurement, we can project the quantum system onto one of the bases associated with these orthogonal states. The result of this measurement will unambiguously indicate what the state was before the measurement.

However, when two states are not orthogonal, their quantum states partially overlap. This overlap leads to a fundamental uncertainty in the measurement result. If a state is measured on the basis of the other state, there is a non-zero probability of obtaining an erroneous result. This probability is directly related to the degree of overlap between the two quantum states. The greater the overlap, the higher the probability of error.

This impossibility of distinguishing non-orthogonal states with certainty directly reflects Heisenberg's uncertainty principle. This fundamental principle of quantum mechanics asserts that it is impossible to know certain pairs of physical quantities, such as a particle's position and momentum, at the same time and with precision.

For example, the state $|\uparrow\rangle$ and $\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$ cannot be perfectly distinguished because they are non orthogonal.

2.4 Qubit

A classical bit is defined as an elementary unit of information. It is a scalar with two possible values: 0 and 1. The bit can also be viewed as a variable with two states: state zero and state one, without intermediate sub-states.

In quantum information theory, the elementary unit of information is the qubit, which represents the basic unit of information that can be stored in a quantum system as a counterpart of a classical bit [10].

In the formalism of quantum mechanics, the base states of the qubit are represented by two vectors, $|0\rangle$ and $|1\rangle$. They evolve in a 2-dimensional Hilbert space where their states are represented as vectors, $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. These vectors are orthonormal : $\langle 0|0\rangle = \langle 1|1\rangle = 1$ and $\langle 0|1\rangle = \langle 1|0\rangle = 0$.

Unlike a classical bit, which can only be 0 or 1, a qubit can exist in a superposition of these states. This means a qubit can be in a superposition, that is, a combination of both $|0\rangle$ and $|1\rangle$.

A qubit is written as :

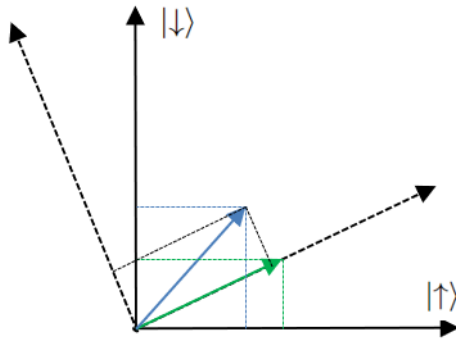


Figure 2.1: In this example, the non-orthogonal states blue and green cannot be perfectly distinguished, they each have a component which projects onto state $|\uparrow\rangle$ and one onto state $|\downarrow\rangle$. If we rotate the basis so that one of the states has a component on only one of the two axes, the second state will always have a component on this same axis, and the states cannot be perfectly distinguished i.e any measurement intended to separate them will have a fundamental probability of error.

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle$$

when the basis states are $|0\rangle, |1\rangle$ and the qubit amplitudes are (α, β) the probability of measuring the qubit in state $|0\rangle$ is $|\alpha|^2$ (absolute value squared). Similarly, the probability of measuring the qubit in state $|1\rangle$ is $|\beta|^2$. These probabilities always sum to 1: $|\alpha|^2 + |\beta|^2 = 1$.

In the special case of equal probability for both states (equiprobability), we have $\alpha = \beta = \frac{1}{\sqrt{2}}$.

A qubit's state is described relative to a specific basis set. The most common basis, known as the computational basis, uses the z-axis of the Bloch sphere [11] and consists of the states:

- $|0\rangle$: represents the state with the spin pointing "up" along the z-axis,
- $|1\rangle$: represents the state with the spin pointing "down" along the z-axis.

Other common basis sets include the x-basis and the y-basis. These bases are related to the z-basis by rotations around the Bloch sphere. The x-basis states are:

- $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$: a superposition of $|0\rangle$ and $|1\rangle$ with equal coefficients,

- $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$: another superposition of $|0\rangle$ and $|1\rangle$ but with opposite coefficients.

The y-basis states are:

- $|R\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}$,
- $|L\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$.

Unlike the z-basis and x-basis, which lie on the real plane of the Bloch sphere, the y-basis states involve imaginary components.

The Bloch sphere (figure 2.2) is a tool that allows us to visualise the state of a quantum system, particularly a two-level system like a qubit. Points on the surface of the Bloch sphere represent pure states, while points inside the sphere represent mixed states. The closer a point is to the centre of the sphere, the more mixed the state is, indicating greater uncertainty about the actual state of the system. The coordinates of a point on or within the sphere encode information about the probability of finding the system in each possible state [12].

The qubit is as follows:

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\phi}|1\rangle,$$

the state $|0\rangle$ corresponds to a special state where $\theta = 0^\circ$ and the state $|1\rangle$ to another special state where $\theta = \pi^\circ$, located at the North and South Poles, while the equator corresponds to the states $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)$.

As long as the photon is not measured in a specific state, it has a probability amplitude of being in each state of the basis. To measure a state, one must list the paths leading to that state and associate a probability amplitude with each path. The probability of measuring the state is then equal to the magnitude squared of the sum of the probability amplitudes.

The qubits can exist in a superposition of the two base states: $|0\rangle$ and $|1\rangle$. When one of a qubit's observables is measured, the qubit collapses into one of its eigenstates, which is reflected in the measured value. If a qubit is in a superposition state with equal coefficients, a measurement will cause it to collapse into one of its two basis states: $|0\rangle$ or $|1\rangle$, with a 50 percent chance of each. The basis states $|0\rangle$ and $|1\rangle$ are eigenstates of the computational basis. A measurement of a qubit in the state $|0\rangle$ yields the outcome 0 with a probability of 1, leaving the state unchanged (or "collapsed" into itself). Conversely, a measurement of $|1\rangle$ yields the outcome 1 with certainty.

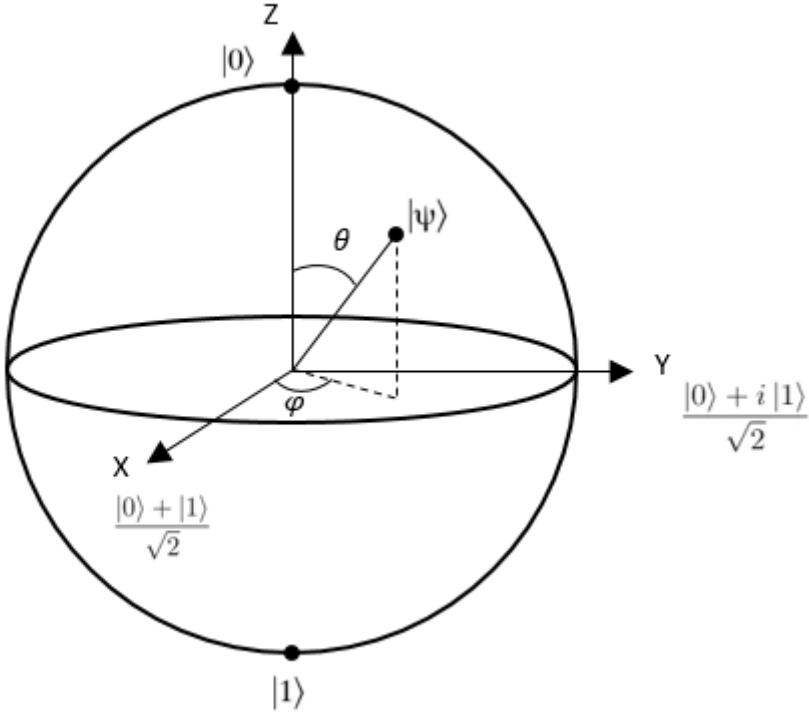


Figure 2.2: Representation of a qubit on the surface of the Bloch sphere.

2.5 Quantum correlation

Let $\mathcal{O}^{(1)}$ and $\mathcal{O}^{(2)}$ be two observables defined by the projectors $\mathcal{P}_i^{(1)}$ and $\mathcal{P}_j^{(2)}$. The conditional probability of finding result j on $\mathcal{O}^{(2)}$ knowing that i has been found on $\mathcal{O}^{(1)}$ is:

$$P_{(j|i)} = \frac{\text{Tr}[\rho \mathcal{P}_i^{(1)} \mathcal{P}_j^{(2)} \mathcal{P}_i^{(1)}]}{\text{Tr}[\rho \mathcal{P}_i^{(1)}]}. \quad (2.19)$$

If each observable forms a complete metric set (non-degenerate eigenspaces i and j), $p_{(j|i)}$ is independent of the state of the system:

$$P_{(j|i)} = |\langle j|i \rangle|^2. \quad (2.20)$$

In this case, the correlation is independent of the order of the measurements:

$$P_{(j|i)} = P_{(i|j)} = |\langle j|i \rangle|^2. \quad (2.21)$$

If $\mathcal{O}^{(1)}$ and $\mathcal{O}^{(2)}$ correspond to two independent parts of a bipartite system, they commute and so do the projectors on their eigenspaces. The joint probability of finding the results i and j , independent of the order of the measurements, is:

$$P(i, j) = P_{(j|i)}P_i^1 = P_{(i|j)}P_j^2 = \text{Tr}[\rho P_i^{(1)}P_j^{(2)}]. \quad (2.22)$$

2.6 Entanglement

Quantum entanglement is a special connection between two (or more) qubits [13], whose first experimental demonstration was carried out by Chien-Shiung Wu and Irving Shaknov in 1950 [14].

An entangled state is defined as a non-separable state of a system containing different parts that are quantum correlated. This is one of the most perplexing phenomena in quantum physics. A pair or group of particles is entangled when the quantum state of each particle cannot be described independently of the quantum state of the other particle or particles. Although the parts of the system are not distinct, the quantum state of the entire system can be stated.

Entanglement can be created in various ways. For example, we can bring two qubits close together, perform an operation to entangle them, and then separate them again. Regardless of distance, entanglement is maintained. The results of measurements taken on these qubits reveal this entanglement. When measured, these qubits will always yield either zero or one in a perfectly random manner. Nonetheless, no matter how far apart they are, whenever you measure them together, they will always be correlated, e.g. in case maximally entangled states their results will be opposite (one 0 and one 1) or complementary (both 0 or both 1).

Entanglement has two qualities that enable all the applications that follow. The first property is entanglement's monogamy. Unlike classical correlations, which allow sharing information with many parties, entanglement cannot be freely shared. If two qubits are maximally entangled, they cannot share that entanglement with any other qubit.

The second property is perfect correlation for the singlet state. The measurement on the qubits demonstrates this characteristic. When you measure two entangled qubits locally in a specific way (same basis), even if vast distances separate them, their results will always be linked and complementary. This means that if one qubit is 0, the other will be 1, and vice versa. This

result is not predetermined, the individual measurement outcomes are entirely random and determined at the moment of the measurement.

When dealing with entangled photons, it's impossible to describe the polarisation state of just one photon individually : we can only describe the combined state of both photons. What defines entanglement is the impossibility of factoring. Let us imagine two photons, each in a superposed state and independent:

$$|\psi_1\rangle = a|0\rangle + b|1\rangle \quad (2.23)$$

$$|\psi_2\rangle = c|0\rangle + d|1\rangle, \quad (2.24)$$

the complete "product" state of the system can be created:

$$|\psi_1\rangle \otimes |\psi_2\rangle = ac(|0\rangle \otimes |0\rangle) + ad(|0\rangle \otimes |1\rangle) + bc(|1\rangle \otimes |0\rangle) + bd(|1\rangle \otimes |1\rangle). \quad (2.25)$$

In this state, the particles exist in a superposition of all four possible polarisation combinations. However, since this state can be expressed as a simple product of individual states for each particle, it is not entangled. The two particles behave independently.

An example of a maximally entangled state is as follows: $\frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$. This state is maximally entangled because the measurements of the states of the two photons are perfectly correlated in three different orthogonal measurement basis. There is no classical explanation for this type of correlation, which is a characteristic of quantum entanglement. If you measure qubit A and see that it is 0, you instantly know that qubit B must be 1.

2.6.1 2-qubit entanglement

There are four classic bit pairs: 00, 01, 10, and 11. To these classical bit pairs, we can map two-qubits: $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$. A two-qubit state will be written :

$$|q\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

with :

- $\sum_{i,j} |\alpha_{ij}|^2 = 1$
- $|ij\rangle = |i\rangle \otimes |j\rangle$.

We can rewrite this 2-qubit as :

$$\begin{aligned}
|q\rangle &= \sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2} \frac{\alpha_{00} |00\rangle + \alpha_{01} |01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} + \sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2} \frac{\alpha_{10} |10\rangle + \alpha_{11} |11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}} \\
&= \beta_0 |q_0\rangle + \beta_1 |q_1\rangle.
\end{aligned}$$

A two-qubit state can be reduced to the superposition of two two-qubits: one two-qubit with 0 as first bit $|q_0\rangle$ and one two-qubit with 1 as first bit $|q_1\rangle$. $|0\rangle$ and $|1\rangle$ are the post measurement states of the first bit.

2.7 Bell inequality

2.7.1 Nonlocality

The principle of nonlocality is particular to quantum physics [15]. Consider an entangled state of two photons:

$$|\phi\rangle = \frac{1}{\sqrt{2}} |0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B \quad (2.26)$$

with A,B the spatial modes and 0,1 the particle states.

If we spatially separate these two particles, the previous equation still describes their state. If a measurement is made on one of the particles now, the state of the second particle is immediately known. An action on one of the particles instantly affects its entangled partner, which seems to contradict relativity, as it requires communication faster than the speed of light. This makes quantum mechanics a non-local theory.

2.7.2 Einstein-Podolsky-Rosen(EPR) paradox

The EPR paradox arises from a discussion about the principle of nonlocality introduced by Einstein, Podolsky, and Rosen [7]. This paradox originates from the incompatibility of entangled photons, as described by quantum mechanics, with local realism. Locality is a physical concept asserting that a system can react causally only.

If we take our entangled particles from the equation 2.26 and send these particles in two opposite directions, far apart to Alice and Bob, let's imagine that Alice measures her entangled particle and finds it in state $|0\rangle$. As the particles are entangled, the moment Alice measures her particle, the two-particle state becomes $|\phi\rangle = |0\rangle_A |1\rangle_B$. We can therefore predict that the state of the second particle is $|1\rangle$ without measuring it. Thus, there is a reality $|1\rangle$ associated with the state of this second particle. However, the probability of measuring

the first particle in the $|0\rangle$ state is only $\frac{1}{2}$. If the measurement result had been $|1\rangle$, then the two-particle state would have been $|\phi\rangle = |1\rangle_A |0\rangle_B$, and the reality associated with the state of the second particle would have been $|0\rangle$. The reality of the second particle's state depends on the measurement of the first, leading to the paradox: If the two particles are measured in a time interval shorter than the travel time of light between them, then there can be no local influence of the measurement of one on the other. Yet the reality of the latter's state always relies on the measurement of the former's state. Therefore, there is a contradiction between local realism and the complete description of the two photons' state by quantum mechanics. Einstein proposes as a solution that the state of measurement is probabilistic solely due to a lack of knowledge about the system. In other words, there exists a hidden variable that enables the measurement outcome to be predicted with a certain probability.

Bohr argues that the description of quantum mechanics is complete, that the outcome of a measurement is indeed probabilistic, and that it is sufficient to accept the existence of non-local realism.

2.7.3 Bell's inequality

Bell's inequality provided a crucial test of local realism. Experiments have violated Bell's inequality, thereby supporting the predictions of quantum mechanics over those of local realism.

In 1965, John Bell discovered that the existence of hidden variables leads to quantitatively different predictions compared to those of quantum mechanics in certain situations [15]. By conducting experiments corresponding to these situations, it is possible to determine the validity of the theory regarding hidden variables. This represents an inequality that local realism theories cannot violate, whereas quantum mechanics predicts its violation.

As mentioned in the paradox statement, we consider a source S that emits special pairs of particles, such as photons, in opposite directions toward Alice and Bob. These particles possess two possible properties, often represented as vertical and horizontal polarisation (like two paths). These paths are combined by black boxes, which split them into two orthogonal results, $+1$ and -1 . Alice and Bob can respectively modify the parameters a and b , adjusting the measurement basis of the black boxes through rotation.

Let us imagine that there is indeed a hidden variable that we will call λ . This variable has the property that:

$$\int_{-\infty}^{+\infty} P(\lambda) d\lambda = 1 \quad (2.27)$$

because P is a normalised probability distribution.

To maintain the locality characteristic, it is crucial that B does not depend in any way on A or the parameter a . The probabilities for Alice and Bob are:

$$A(a, \lambda) = \pm 1 \quad (2.28)$$

$$B(b, \lambda) = \pm 1 \quad (2.29)$$

The correlation function is such that :

$$E(a, b) = \int_{-\infty}^{+\infty} A(a, \lambda)B(b, \lambda)P(\lambda) d\lambda \quad (2.30)$$

As only two values $+1$ and -1 are possible:

$$-1 \leq E(a, b) = \int_{-\infty}^{+\infty} A(a, \lambda)B(b, \lambda)P(\lambda) d\lambda \leq +1 \quad (2.31)$$

$E(a, b) = -1$ with $a = b$ only if $A(a, \lambda) = -B(b, \lambda)$. Now let's rewrite:

$$E(a, b, \lambda) = - \int_{-\infty}^{+\infty} A(a, \lambda)A(b, \lambda)P(\lambda) d\lambda \quad (2.32)$$

The parameters a and b each have two possible values a_1, a_2 and b_1, b_2 . Let's look at :

$$E(a_1, b_1) - E(a_1, b_2) = - \int_{-\infty}^{+\infty} [A(a_1, \lambda)A(b_1, \lambda) - A(a_1, \lambda)A(b_2, \lambda)]P(\lambda) d\lambda \quad (2.33)$$

$$= \int_{-\infty}^{+\infty} A(a_1, \lambda)A(b_1, \lambda)[A(a_1, \lambda)A(b_2, \lambda) - 1]P(\lambda) d\lambda \quad (2.34)$$

However, we know that:

$$A(a_1, \lambda)A(b_1, \lambda) \geq -1 \quad (2.35)$$

Hence:

$$|E(a_1, b_1) - E(a_1, b_2)| \leq \int_{-\infty}^{+\infty} [1 - A(a_1, \lambda)A(b_2, \lambda)] P(\lambda) d\lambda \quad (2.36)$$

And as:

$$E(b_1, b_2) = - \int_{-\infty}^{+\infty} A(b_1, \lambda)A(b_2, \lambda)P(\lambda) d\lambda \quad (2.37)$$

We obtain Bell's inequality:

$$1 + E(b_1, b_2) \geq |E(a_1, b_1) - E(a_1, b_2)|. \quad (2.38)$$

This inequality follows from the separability proposed by Einstein, which requires that the measurement on one system be independent of the measurement on any other system from which it is spatially separated. If we impose locality while ensuring that Alice’s measurement is not influenced by Bob’s measurement, we must have a hidden variable. This variable implies that the result of the measurements is predetermined. Bell’s theorem constructs mean value expressions as a function of the detector angles to satisfy the photon correlation relations. These mean values are derived from the measurement results of Alice and Bob, who are independent of each other.

By factoring Alice’s expression and minimising it, an inequality can be formed that cannot be satisfied for certain angles. The factorisation contradicts the definition of an entangled state.

Einstein’s separability, which states that any system is independent of another system from which it is spatially separated, cannot hold unless one rejects the predictions of quantum mechanics. This result does not condemn all hidden-variable theories; it only rejects those that are local.

2.7.4 CHSH inequality

The original Bell inequality is challenging to prove experimentally and only rules out the existence of local hidden variables [16]. Indeed, achieving perfect correlation between the two photons may be difficult in physics. Additionally, Bell’s inequality necessitates hidden variables that are established at the moment of the creation of the singlet state, specifically when the particles are separated. However, other theories of local hidden variables exist, in which the variables remain undetermined at the time the singlet state is created. Consequently, Bell’s theorem does not encompass these theories and therefore cannot definitively resolve the outcome of the debate.

Clauser, Horne, Shimony, and Holt generalised Bell’s equation to cover all possible hidden variables [17], without assuming that the values of the hidden variables are predetermined during the propagation of photons. This generalisation also allows for an experiment derived from Bell’s inequality to test the locality hypothesis. The advantage of the CHSH generalisation is that it does not impose any constraints on the hidden variables. The only assumption made is the normalisation of their density:

$$\int_{-\infty}^{+\infty} P(\lambda) d\lambda = 1. \tag{2.39}$$

This generalisation does not impose a perfect correlation, but we still retain :

$$A(a, \lambda) = \pm 1 \Leftrightarrow |A(a, \lambda)| \leq 1 \quad (2.40)$$

$$B(b, \lambda) = \pm 1 \Leftrightarrow |B(b, \lambda)| \leq 1 \quad (2.41)$$

as for Bell's version :

$$E(a, b) = \int_{-\infty}^{+\infty} A(a, \lambda)B(b, \lambda)P(\lambda) d\lambda \quad (2.42)$$

$$E(a_1, b_1) - E(a_1, b_2) = \int_{-\infty}^{+\infty} [A(a_1, \lambda)B(b_1, \lambda) - A(a_1, \lambda)B(b_2, \lambda)]P(\lambda) d\lambda \quad (2.43)$$

$$= \int_{-\infty}^{+\infty} A(a_1, \lambda)[B(b_1, \lambda) - B(b_2, \lambda)]P(\lambda) d\lambda \quad (2.44)$$

because $|A(a, \lambda)| \leq 1$

$$|E(a_1, b_1) - E(a_1, b_2)| \leq \int_{-\infty}^{+\infty} |B(b_1, \lambda) - B(b_2, \lambda)| P(\lambda) d\lambda \quad (2.45)$$

and:

$$|E(a_2, b_1) + E(a_2, b_2)| \leq \int_{-\infty}^{+\infty} |B(b_1, \lambda) + B(b_2, \lambda)| P(\lambda) d\lambda \quad (2.46)$$

by combining the two previous equations, we obtain:

$$\begin{aligned} & |E(a_2, b_1) + E(a_2, b_2)| + |E(a_1, b_1) - E(a_1, b_2)| \\ & \leq \int_{-\infty}^{+\infty} \left[|B(b_1, \lambda) - B(b_2, \lambda)| + |B(b_1, \lambda) + B(b_2, \lambda)| \right] P(\lambda) d\lambda \end{aligned} \quad (2.47)$$

it is known that $|B(b, \lambda)| \leq 1$, so :

$$|B(b_1, \lambda) - B(b_2, \lambda)| + |B(b_1, \lambda) + B(b_2, \lambda)| \leq 2 \quad (2.48)$$

and as $\int_{-\infty}^{+\infty} P(\lambda) d\lambda = 1$, we obtain :

$$|E(a_2, b_1) + E(a_2, b_2)| + |E(a_1, b_1) - E(a_1, b_2)| \leq 2 \quad (2.49)$$

then we can rewrite :

$$|E(a_2, b_1) + E(a_2, b_2) + E(a_1, b_1) - E(a_1, b_2)| \leq 2 \quad (2.50)$$

knowing that the correlation function is:

$$E(a,b) = P^{++}(a,b) - P^{+-}(a,b) - P^{-+}(a,b) + P^{--}(a,b) \quad (2.51)$$

with $P^{++}(a,b)$, the probability of obtaining +1 at measurement A with parameter a and +1 at measurement B with parameter b, as well as similarly for the other terms in the equation, is evaluated.

Knowing that the probability of obtaining two identical results ($\{+1,+1\}$ or $\{-1,-1\}$) is $\frac{1}{2}\cos^2(\theta)$, while the probability of receiving two different outcomes ($\{+1,-1\}$ or $\{-1,+1\}$) is $\frac{1}{2}\sin^2(\theta)$, with $\theta = b - a$ representing the difference between the two measurement angles, we can conclude:

$$E(a,b) = \cos(2(b-a)). \quad (2.52)$$

Using this in the CHSH inequality, with $a_1 = 0^\circ, b_1 = 22,5^\circ, a_2 = 45^\circ$ and $b_2 = 67,5^\circ$ ($b - a = 22,5^\circ; d - a = 67,5^\circ; b - c = -22,5^\circ$ and $d - c = 22,5^\circ$), we get:

$$|E(a_2,b_1) + E(a_2,b_2) + E(a_1,b_1) - E(a_1,b_2)| = 2\sqrt{2} \geq 2 \quad (2.53)$$

this violates inequality and disproves the existence of a hidden variable [18].

2.8 Multipartite Entanglement

Multipartite entanglement refers to a type of quantum entanglement involving three or more particles or subsystems. Here, we will examine only the case of 3-partite entanglement, but this information can be generalised to include a larger number of particles.

2.8.1 3-partite entanglement

A general three-qubit is written :

$$|\psi\rangle = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle + \alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle$$

with :

- $\sum_{i,j,k} |\alpha_{ijk}|^2 = 1$
- $|ijk\rangle = |i\rangle \otimes |j\rangle \otimes |k\rangle$.

Similarly to two qubits, a three-qubit system can be separable or non-separable.

An example of a complete, separable state is $|000\rangle_{ABC}$.

Unlike a two-qubit system, a three-qubit system can be bi-separable, such as:

$$|0\rangle_A \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{BC}, \quad (2.54)$$

in that example, A is separable and B and C are non-separable.

Fully non-separable states are, for example, W and GHZ states.

W state is :

$$|W\rangle_{ABC} = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)_{ABC}. \quad (2.55)$$

W states are robust against the loss of particles. The loss of one particle doesn't destroy the entanglement among the remaining particles.

We refer to the GHZ state, named after Greenberger-Horne-Zeilinger, as a state with N qubits ($N \geq 3$) such as:

$$|GHZ\rangle_{ABC} = \frac{1}{\sqrt{2}}(|0_1 0_2 \dots 0_N\rangle + |1_1 1_2 \dots 1_N\rangle)_{ABC}, \quad (2.56)$$

here, the equation illustrates a superposition of two states:

- The first term, with all qubits in state 0 $|0_1 0_2 \dots 0_N\rangle$, represents a scenario where all qubits are zero.
- The second term, with all qubits in state 1 $|1_1 1_2 \dots 1_N\rangle$, represents a scenario where all qubits are one.

A GHZ state is an example of a state in which all the parties are entangled.

2.9 Polarisation encoding

For the experiments in this thesis, we chose photons as our preferred quantum qubits. This decision is based on several reasons. First, photons are highly stable particles. Second, they can be easily transmitted over long distances without significant degradation. Finally, regarding the encoding of qubits in photons, we specifically focused on the property of polarisation.

Polarisation is a characteristic of light that describes the direction of the electric field tangent to the wavefront [19].

We have seen that the Bloch sphere is a useful tool for visualising the quantum states of a single qubit; figure 2.3 shows some examples of particular states. These states can be represented mathematically using the Pauli matrices, which are special 2x2 matrices:

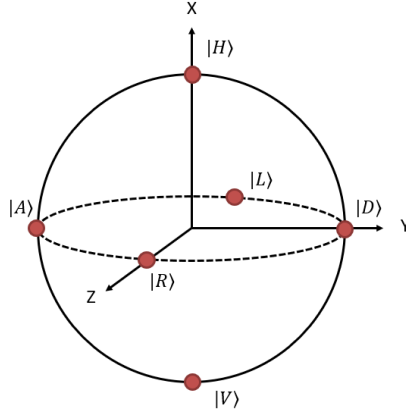


Figure 2.3: Spatial representation of $|H\rangle$, $|V\rangle$, $|R\rangle$, $|L\rangle$, $|D\rangle$ and $|A\rangle$ on a Bloch Sphere.

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad (2.57)$$

which, when coupled with the identity matrix $\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, form a basis of matrices. Any single-qubit state can be described as a linear combination of these Pauli matrices and the identity matrix.

These matrices are also associated with operators of the same kind. Classically, it is the orthogonal polarisations $|H\rangle$ and $|V\rangle$, the eigenvectors of the operator σ_z , which are used as the basis as $|0\rangle$ and $|1\rangle$.

2.10 Polarisation single-photon state preparation

The polarised states $|H\rangle$ and $|V\rangle$ are orthogonal, which means that $\langle H|V\rangle = \langle V|H\rangle = 0$ and therefore no $|H\rangle$ photon will exit through the V output of a PBS and vice versa.

We know our states are normalised, meaning they represent pure quantum states. Since horizontal (H) and vertical (V) form a basis for polarisation states, any other polarisation state can be expressed as a linear combination of these basis states. So:

$$|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \quad (2.58)$$

$$|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) \quad (2.59)$$

$$|R\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle) \quad (2.60)$$

$$|L\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle). \quad (2.61)$$

We can represent an arbitrary polarisation state $|P\rangle$ as :

$$|P\rangle = \alpha |H\rangle + e^{i\phi} \beta |V\rangle, \quad (2.62)$$

here, $\{\alpha, \beta, \phi\} \in \mathbb{R}$ that determine the coefficients of the horizontal $|H\rangle$ and vertical $|V\rangle$ components in the state, and $e^{i\phi}$ is a complex number with magnitude 1 and phase ϕ . It accounts for the relative phase difference between the horizontal and vertical components.

In the special case of a coherent state, such as the light emitted from a laser, the phase i is well-defined. This indicates that the relative orientation of the electric field in the horizontal and vertical components is fixed.

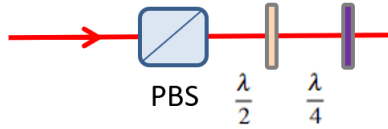


Figure 2.4: To prepare a photon in the desired polarisation, a polarising beam splitter (PBS) followed by a half-wave plate (HWP) and a quarter-wave plate (QWP) can be used to achieve the required configuration polarisation.

2.11 Single photon polarisation transformation

A qubit stays in the state it was prepared in as long as it is not subjected to external interaction. In the formalism of quantum mechanics, any transformation affecting the state of a qubit is associated with a unitary operator. This operator acts on the state and modifies it as follows:

$$|FinalState\rangle = Op |InitialState\rangle. \quad (2.63)$$

Photons emitted by a source often have a specific polarisation. We utilise various optical components to manipulate their polarisation:

- **Polarisers:** These act as filters, allowing only light with a specific linear polarisation to pass through. We can describe them as gates that permit light to vibrate in a particular direction.
- **Wave plates:** These are more versatile tools. They can not only alter the polarisation of light but also introduce a specific phase shift. We can describe them as instruments that can twist and turn the orientation and timing of the light wave.

An HWP, a QWP, and a PBS are needed to analyse the polarisation encoding of a photon [20], as shown in Figure 2.11.

- A half-wave plate (HWP) is a component that alters the polarisation of light by introducing a π phase shift between the orthogonal polarization.
- A quarter-wave plate (QWP) is a plate that creates a 90-degree phase shift between two orthogonal polarisation components.
- A polarising beam splitter (PBS) is a device that divides the input signal into two beams of orthogonal polarisation.

Suppose one has a one-photon state in linear polarisation, which is achievable with a polariser. By using only an HWP and a QWP, it is possible to transform this state into any other state on the Bloch sphere. From the $|H\rangle$ state, the $|H\rangle$, $|V\rangle$, $|D\rangle$ and $|A\rangle$ states can be obtained from a half-wave plate ($\frac{\lambda}{2}$).

| Output polarisation | $ H\rangle$ | $ V\rangle$ | $ D\rangle$ | $ A\rangle$ |
|---------------------------------|-------------|-------------|-------------|-------------|
| HWP rotation angle (in degrees) | 0 | 45 | 22,5 | -22,5 |

Table 2.1: Orientation of an HWP to obtain the following states from an initial state $|H\rangle$.

To go from a $|H\rangle$ state to the $|L\rangle$ and $|R\rangle$ states, this time we need a quarter-wave plate ($\frac{\lambda}{4}$).

| Output polarisation | $ L\rangle$ | $ R\rangle$ |
|---------------------------------|-------------|-------------|
| QWP rotation angle (in degrees) | 45 | -45 |

Table 2.2: Orientation of a QWP to obtain the following states from an initial state $|H\rangle$.

2.12 Single Photon Polarisation Measurement

To determine the polarisation state of a photon, we use a polarising beam splitter (PBS). A PBS is an optical component that divides an optical field into two orthogonal modes. The amplitude of these two modes corresponds to the projection of the polarisation vector along these two orthogonal axes. The two directions of polarisation of a PBS are horizontal and vertical polarisation. However, decomposing diagonal and anti-diagonal polarisation, as well as right and left circular polarisation, is also possible with a PBS.

A diagonally polarised photon is in a superposition of horizontal and vertical polarisation states. When encountering a PBS designed to distinguish horizontal and vertical light, the photon has a 50% probability of exiting from either the horizontal or vertical output. This reflects the probabilistic nature of quantum mechanics. Similarly, a horizontally polarised photon will give a random result when faced with a D/A distinguishing PBS.

The transformation from the horizontal/vertical polarisation basis to other bases can be achieved using wave plates. These optical elements enable the analysis of photons in different polarisation bases using polarising beam splitters originally designed for the H/V basis as shown in the figure 2.5.

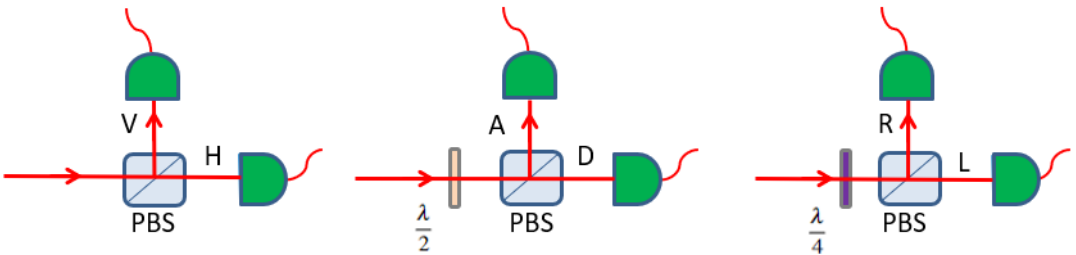


Figure 2.5: Transformation of a PBS to distinguish different orthogonal polarisations. To obtain the circular polarisation basis (left/right), a quarter-wave plate oriented at 45° with respect to the horizontal axis introduces a relative phase shift of $\pi/2$ between the H and V components, converting linear polarisations into circular ones. Alternatively, to access the diagonal basis, a half-wave plate (HWP) aligned at 22.5° relative to the horizontal axis rotates the polarisation direction by 45° , transforming H and V states into the diagonal 45° states.

Let's remind ourselves of Heisenberg's principle of uncertainty: One cannot simultaneously measure two properties defined by observables that do not commute. Two conjugate quantities cannot be measured accurately and simul-

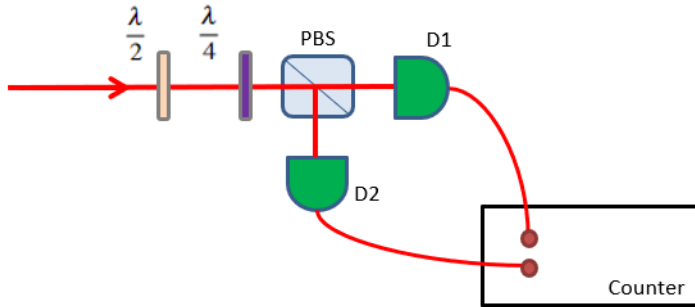


Figure 2.6: Measurement station: using PBS, HWP, and QWP, the polarisation of any state can be determined. The optical signal is converted into an electrical signal through the detectors, which are connected to a coincidence unit that counts the number of photons arriving at each detector and the coincidences between them.

taneously. In particular, obtaining a high degree of accuracy in measuring the velocity of a particle is impossible without also obtaining a low degree of accuracy in its position, and vice versa. This uncertainty does not depend on how careful the experimenter is in trying not to 'disturb' the system; it constitutes a limit on the precision of any measuring instrument.

Regarding the detection itself, light is not detected directly, it is first converted into an electrical signal, which is then detected and analysed. Detection can be performed using two methods: field detection and intensity detection. The field detection method focuses on the electric and magnetic field properties of light waves. It can provide information about the light's phase and polarisation. In contrast, the intensity detection method measures the overall intensity (strength) of the light without capturing details about the wave's properties.

The quantum efficiency η is the probability that incoming light is converted into a measurable signal.

Notice that even in darkness, thermal effects within the detector can cause a small electric current to flow, generating a weak signal. This unwanted signal is referred to as dark count or dark noise.

A photon carries a weak energy. Its energy is inversely proportional to its wavelength, as described by the equation $E = h\nu$, where E is the energy, ν is the frequency, and h is the Planck constant. This energy is typically around $10^{-19}J$ in the visible spectrum. A mechanism is needed to convert this small amount of energy into a macroscopic signal.

In the lab, we use a specialised type of detector known as an avalanche photodiode (APD) to convert light signals into measurable electrical signals. This conversion relies on the principle of the photoelectric effect: when light strikes the surface of a material like silicon, it can eject an electron from the atom. For this process to occur, the energy of the light photon must exceed the energy gap between the electron's bound state (valence band) and its free state (conduction band).

APDs are specialised photodetectors made from silicon. They exploit the photoelectric effect but take it a step further. Light interacts with the material, creating electron-hole pairs (an electron and a vacancy where the electron used to be). These initial charge carriers are then accelerated by an internal electric field within the APD, gaining enough energy to produce additional electron-hole pairs. This cascading effect, known as an avalanche, significantly amplifies the original signal.

For applications that require continuous light detection, APDs operate in a specific mode called continuous mode. In this mode, the internal electric field is very high, leading to an avalanche process that is quenched either passively or actively. After a recovery time (deadtime), the detector is rearmed, allowing for the sensitive detection of even weak light signals.

Our lab detectors are approximately 55% efficient, meaning they convert roughly 55% of incoming light into a usable signal. They also have a dead time of 55 nanoseconds. Dead time is a crucial factor in detector performance. It represents the minimum duration a detector requires to reset after registering a photon before it can detect another one.

2.13 Entanglement source

All the experiments presented here require a source of polarisation-entangled photon pairs. The creation of these entangled photon pairs occurs in two steps.

The first step involves frequency doubling. The second step consists of generating photon pairs using the spontaneous parametric down-conversion (SPDC) phenomenon.

A 780nm laser pumps a 1mm thick BiBO (Bismuth Triborate) nonlinear crystal, which creates photons at 390nm through second harmonic generation (SHG), its frequency doubling. This step is required because we do not have a 390nm laser.

Second harmonic generation represents a particular instance of frequency sum generation. This phenomenon is classified as nonlinear optical, wherein photons interacting with a nonlinear medium combine to produce new photons possessing twice the energy, which corresponds to twice the frequency or half the wavelength of the original photons.

To eliminate this residual pump signal, a series of dichroic mirrors are used which reflect the signal at $390nm$ and transmit the signal at $780nm$. Thus, the residual pump signal does not follow the same path as the photon pair signal.

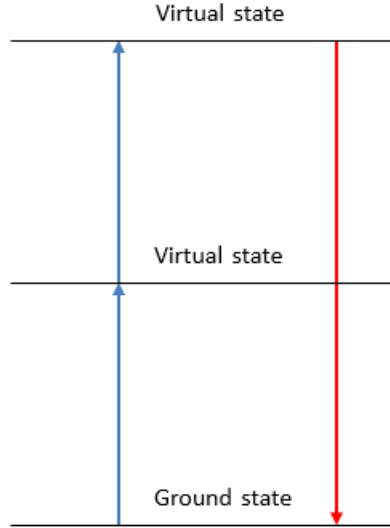


Figure 2.7: Energy level of the second harmonic generation process.

The converted signal, filtered at $390nm$, is then used to pump a BBO crystal to generate photon pairs via the SPDC process [21].

The Spontaneous Parametric Down-Conversion (SPDC) represents a non-linear process of second order in which a pump photon is converted into two distinct photons within a nonlinear crystal, specifically referred to as the signal photon and the idler photon. This mechanism adheres to the principles of energy conservation and momentum relations:

$$\omega_p = \omega_s + \omega_i \text{ and } \vec{k}_p = \vec{k}_s + \vec{k}_i. \quad (2.64)$$

The success of SPDC in generating entangled photons depends on a unique property of the nonlinear crystal known as birefringence. Birefringence refers to the way the crystal behaves differently for light waves based on their polarisation. When light enters a birefringent crystal, its path is affected by its polarisation. The crystal has a "fast axis" and a "slow axis" for light propagation. By carefully controlling the angle at which the pump photon enters the crystal, we can ensure that the generated signal and idler photons travel along the crystal's fast and slow axes, respectively[21].

This separation, based on polarisation, enables the simultaneous fulfillment of energy and momentum conservation relations. We focus on the specific case of degeneracy, which occurs when the signal and idler photons have the same frequency: $\omega_i = \omega_s$.

Polarisation entanglement is achieved using a BBO crystal. This optically uniaxial negative birefringent crystal can be utilised in either type I or type II phase matching.

The BBO crystal is birefringent (this is also the case for the BiBo crystal), meaning that light propagates anisotropically. Anisotropy refers to the property of being direction-dependent: depending on the orientation of the crystal, specific characteristics will vary. In a birefringent medium, the refractive index is not singular; it depends on the direction of polarisation of the light wave.

If we consider a linearly polarised light beam in this birefringent medium, its speed of propagation will depend on the polarisation of the beam. However, there is a preferred direction for which the index remains constant regardless of the polarisation direction, known as the optical axis of the medium. Our crystal is uniaxial, meaning it has only one optical axis and two refractive indices: the ordinary and extraordinary indices, which correspond to the ordinary and extraordinary axes.

One significant effect of birefringence is double refraction, in which a ray of light entering the crystal is split into two along the crystal's ordinary and extraordinary axes.

In type I phase matching, a specific method for achieving SPDC in the BBO crystal, the generated signal and idler photons (the "twin photons") share the same polarisation. This polarisation is perpendicular to the crystal's optical axis, while the pump photon's polarisation is parallel to that axis. By arranging two BBO crystals consecutively with their optical axes perpendicular, we can realise a specific entangled state for the signal and idler photons: $\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$.

Type II phase matching is another method for achieving SPDC in the BBO crystal. The pump photon, which has extraordinary polarisation, interacts with the crystal and splits into a signal photon and an idler photon. Interestingly, these two photons can have different polarisations: either extraordinary (EE) or one extraordinary (E) and one ordinary (O). This can occur in two configurations: EE or EO/OE. The generated photon pairs are emitted in two cones that are symmetrically arranged around the pump beam. Consequently, we cannot determine which photon originated from the extraordinary wave and which one came from the ordinary wave in the split pump photon. The intersection of the two cones thus formed results in indistinguishable entangled photon pairs in the state. $\frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle)$.

Regardless of the chosen method, the pairs of photons produced by the

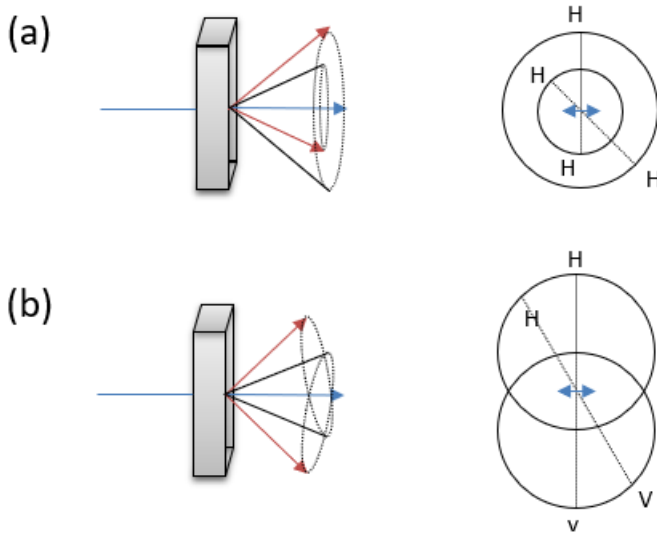


Figure 2.8: Spontaneous In the Down Conversion process, (a) Type I exhibits propagation directions that form two concentric cones. (b) Type II shows propagation directions that form two cones symmetrically tilted to the direction of the pump photons.

source are correlated but not entangled in a definitive state. Indeed, there are still degrees of discernment among these photons. To render the photons indistinguishable and consequently entangled in pairs, spatial, spectral, and temporal filtering is applied, using filters, delay lines, and optical fibers.

We now have entangled photons, indicating that their properties are linked. In this instance, the entanglement specifically relates to their frequencies.

2.14 Quantum interference and HOM

The Hong, Ou, Mandel (HOM) experiment [22; 23], conducted in 1987, was the first to observe a two-photon quantum interference effect. This effect occurs when two indistinguishable photons arrive simultaneously at the two input channels of a semi-reflecting plate. The distribution of the two photons in the output channels of the cube then exhibits behavior that classical light theory cannot explain [24]. When a photon encounters a beam splitter, it has a 50/50 chance of being transmitted or reflected. When two photons arrive simultaneously at the beam splitter, each through an input channel (a or b), there are four

possibilities (see figure 2.9).

- the photon entering via channel a exits via channel c, and the photon entering via channel b exits via channel d
- the photon entering via channel a emerges via channel d, and the photon entering via channel b emerges via channel c
- both photons exit via channel c
- both photons exit via channel d.

If we consider photons to be ‘classical’ particles, the four cases will always be equiprobable, provided that the separator transmits and reflects the photons with equal probability. However, quantum theory presents a completely different possibility. According to quantum theory, it may be impossible to experimentally distinguish two particles. In our case, this happens when the two photons share all their properties.

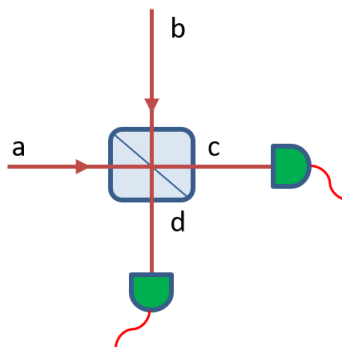


Figure 2.9: Two Indistinguishable photons arrive simultaneously at the input channels a and b of a beamsplitter. Two single-photon detectors, c and d, record which of the two paths the photons exit: c or d through.

Let’s consider two photons entering a beamsplitter (BS). These photons are identical; they cannot be distinguished based on their spatial or spectral modes (position or wavelength). The probabilities, or amplitudes, of these photons traveling through one specific path of the BS (say, transmission) have opposite signs. In simpler terms, one photon is more likely to be transmitted while the other is more likely to be reflected. If the BS is designed for equal transmission and reflection (50/50 chance for each path), these opposite amplitudes result

in a phenomenon called destructive interference. This implies that the probabilities of both photons emerging from the same path (both transmitted or both reflected) cancel each other out, leading to a very low probability of detecting them together in that specific output.

Hong Ou Mandel's 1987 experiment demonstrated this. A pair of photons is separated and sent through two paths of nearly equal length before being recombined with a 50/50 beamsplitter in a perfectly superimposed manner; spatial and frequency filters are utilised to eliminate anything that might distinguish the photons. The length difference between the two paths can be adjusted. When the delay is zero, indicating that the two paths are perfectly equal in length, the coincidence count rate vanishes and is about half of the total count rate for a large delay, which aligns with the expected result for discernible particles.

The theoretical dip equation is as follows:

$$C = \alpha\chi(1 - e^{-\sigma\tau^2}) \quad (2.65)$$

Where χ is the photon pair production rate, σ the Gaussian beam bandwidth, τ the delay, and α a proportionality coefficient.

The main limitation to the visibility of a Hong Ou Mandel dip is the quality of the spatial superposition at the beam splitter.

To assess the quality of our photon indistinguishability, we measure the visibility of the H-O-M dip, defined as the number of coincidences outside the dip minus the number of coincidences inside the dip, divided by the sum. In practice, in the set of experiments presented here, we do not use a BS to superimpose the photons but a PBS. Therefore, to suppress the polarisation distinction that persists after superimposition, it is necessary to place a HWP at 22.5° to make our photons indistinguishable and a second PBS to observe the dip. The setup required for the dip is shown in the figure 2.10.

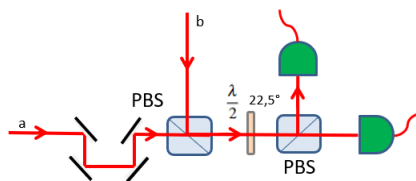


Figure 2.10: Hong-Ou-Mandel dip setup. To avoid overloading the figure, only one mode of PBS output is considered here; however, what applies to one mode may also apply to the others.

Photons are split and sent through nearly equal-length paths. By varying the path length difference (delay τ), we can observe changes in the coincidence count rate. When the path length difference is zero, maximum interference occurs, resulting in a dip in the coincidence count (the HOM dip), which indicates the indistinguishability of the photons.

The visibility, V , of this dip, defined as:

$$V = \frac{C_{max} - C_{min}}{C_{max}}, \quad (2.66)$$

it is a measure of photon indistinguishability. High visibility (close to 1) indicates almost perfect indistinguishability, while lower values imply distinguishable photons due to misalignment or varying photon properties. In our experimental setup (Figure 2.10), we use a polarising beam splitter (PBS) and a half-wave plate (HWP) set at 22.5° to eliminate polarisation distinguishability, creating the conditions necessary to observe the HOM dip. The second PBS allows us to detect the bunched photons, thereby providing a method to measure the visibility of the dip and evaluate the quality of photon indistinguishability.

2.15 Bell's measurement

2.15.1 Bell's states

Out of all the possible combinations of quantum states like $|ij\rangle|jk\rangle$, we're particularly interested in Bell states, also known as EPR pairs:

$$\begin{aligned} |\phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned}$$

Bell states are special because they demonstrate the strongest violation of Bell's inequality. These states involve two entangled qubits (quantum bits) and possess the following properties:

- **Maximum entanglement:** The qubits are maximally linked, meaning their fates are intertwined in a way that classical physics cannot explain,

- Orthogonality: Each Bell state is completely distinct from the others, like opposite sides of a coin.

2.15.2 Bell measurement

The Bell measurement is a specific type of measurement in quantum mechanics. It involves two entangled qubits. This measurement determines which of the four possible 'Bell states' these entangled qubits are projected into [25].

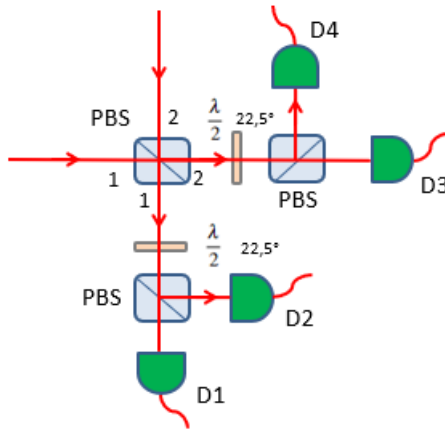


Figure 2.11: Partial Bell's states analyser.

While Bell measurements determine the entangled state of two qubits, some techniques, like those based on linear optics, can only distinguish between certain Bell states. These techniques cannot differentiate between two specific pairs of Bell states [26]. At best, the measurements using linear optics are generally successful 50% of the time, but it's possible to increase that to 62,5% [27–29].

The Bell analyser shown in Figure 2.11 can be used to distinguish ϕ^+ and ϕ^- .

Indeed, if we consider ϕ^+ at the level of the first PBS :

$$\frac{1}{\sqrt{2}} (H_1 H_2 + V_1 V_2), \quad (2.67)$$

after passing the first PBS, we will have :

$$\frac{1}{\sqrt{2}} (H_2 H_1 + V_1 V_2), \quad (2.68)$$

the passage from HWP at $22,5^\circ$ will give :

$$\begin{aligned} (H_2 + V_2)(H_1 + V_1) + (H_1 - V_1)(H_2 - V_2) \\ H_2H_1 + H_2V_1. \end{aligned} \quad (2.69)$$

2.16 Application : GHZ state preparation

The preparation of a GHZ report is an example of the use of Bell measurements.

Remember that a GHZ state is written as :

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|0_1 0_2 \dots 0_N\rangle + |1_1 1_2 \dots 1_N\rangle). \quad (2.70)$$

For $N = 3$ and $N = 4$, we need two sources producing the states :

$$\frac{1}{\sqrt{2}}(|H_1 H_2\rangle + e^{i\phi_1} |V_1 V_2\rangle) \quad (2.71)$$

$$\frac{1}{\sqrt{2}}(|H_3 H_4\rangle + e^{i\phi_2} |V_3 V_4\rangle) \quad (2.72)$$

as presented in the figure 2.12

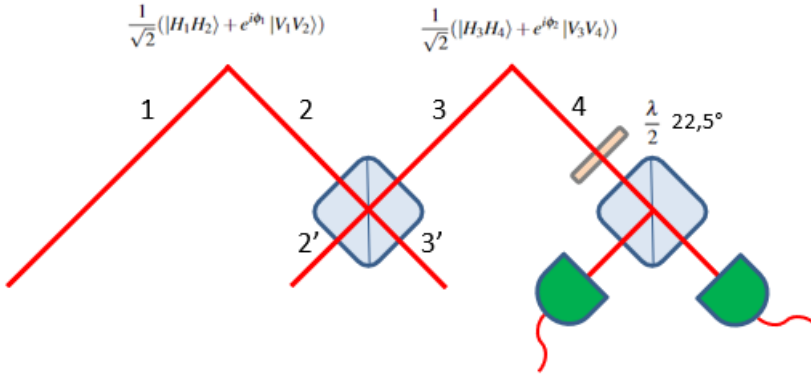


Figure 2.12: Setup for GHZ states preparation.

The 4-photon state thus created at the source outputs is :

$$|\phi\rangle_{12} |\phi\rangle_{34} = \frac{1}{2}(|H_1 H_2\rangle + e^{i\phi_1} |V_1 V_2\rangle)(|H_3 H_4\rangle + e^{i\phi_2} |V_3 V_4\rangle) \quad (2.73)$$

after PBS, the state becomes :

$$\begin{aligned} & \frac{1}{2}(|H_1H_{3'}\rangle + e^{i\phi_1}|V_1V_{2'}\rangle)(|H_2H_4\rangle + e^{i\phi_2}|V_3V_4\rangle) \\ &= \frac{1}{2}(|H_1H_2H_3'H_4\rangle + e^{i\phi_2}|H_1H_3'V_3'V_4\rangle + e^{i\phi_1}|V_1V_{2'}H_2H_4\rangle - e^{i(\phi_1+\phi_2)}|V_1V_{2'}V_3'V_4\rangle). \end{aligned} \quad (2.74)$$

The terms $e^{i\phi_2}|H_1H_3'V_3'V_4\rangle$ and $e^{i\phi_1}|V_1V_{2'}H_2H_4\rangle$ do not produce coincidences. We will have 4-photon coincidences only with the terms :

$$\frac{1}{\sqrt{2}}(|H_1H_2H_3'H_4\rangle - e^{i(\phi_1+\phi_2)}|V_1V_{2'}V_3'V_4\rangle). \quad (2.75)$$

By adjusting the phase $\phi_1 + \phi_2$ we can obtain a GHZ state at 4 photons.

To obtain a GHZ state of 3 photons, it is sufficient to add a HWP on branch 4 and to use one of the outputs as a trigger, depending on the angle of the HWP chosen, one of the following states is obtained :

$$\frac{1}{\sqrt{2}}|H_4\rangle(|H_1H_2H_3'\rangle - e^{i(\phi_1+\phi_2)}|V_1V_{2'}V_3'\rangle) \quad (2.76)$$

$$\frac{1}{\sqrt{2}}|V_4\rangle(|H_1H_2H_3'\rangle + e^{i(\phi_1+\phi_2)}|V_1V_{2'}V_3'\rangle). \quad (2.77)$$

2.17 Steerability

Earlier, we examined the EPR paradox and the resulting inequalities. Schrödinger noted an interesting phenomenon in the argument: one side can influence the state of the other side towards a specific position or momentum by choosing the measurement. Although this cannot be used to transmit information, it is still notable. In the modern view, steerability refers to the impossibility of describing the conditional states of one part through a local hidden state model. Therefore, steerability pertains to a quantum correlation between entanglement and Bell non-locality.

Two particles are considered entangled when they share a single quantum state, regardless of the distance between them. A measurement performed on one particle instantly influences the state of the other.

Steerability, on their part, implies that one part of a quantum system can influence the state of another part non-locally, thanks to local measurements. It also certifies that this influence is indeed quantum and not a result of classical hidden variables. This means that in a system shared between two parties (say Alice and Bob), Alice can affect Bob's reduced state by choosing a specific

measurement basis on her side. Steerability enables the establishment of a quantum cause-and-effect relationship between the two systems.

In a steering protocol, Alice and Bob share an entangled quantum state ρ_{AB} . Alice measures her part of the state using a set of bases or observables, and Bob can observe changes in his subsystem B. If Alice can demonstrate that a local model cannot explain her results, the state is considered steerable [30].

Steerability lies between entanglement and complete non-locality. A steerable state is indeed entangled, but it doesn't always signify non-locality in the context of violating a Bell inequality. While all steerable systems are entangled, not every entangled system is steerable. This attribute is more robust than mere entanglement as it not only shows a correlation between the two systems but also indicates a directionality in that correlation. The connection among these three concepts—entanglement, steerability, and non-locality—forms a hierarchy:

- Entanglement: This is the most general property. Every steerable state is entangled, but not all entangled states are steerable.
- Steerability: A subset of entangled states can exhibit steering, detectable through specific inequalities. These states demonstrate stronger non-locality than mere entanglement.
- Non-locality in the sense of Bell inequalities: A state that violates a Bell inequality is also steerable and entangled, but the reverse is not necessarily true.

This hierarchy can be represented as follows:

$$\text{Bell's non-locality} \subset \text{Steerability} \subset \text{Entanglement},$$

and can be represented as in Figure 2.13. The closer we get to the centre, the stronger the constraints imposed by classical description models become. Thus, separable states form the smallest subset, as they must satisfy all locality and classicity constraints. A state outside the LHV set is by definition Bell-non-local, while a state outside the Unsteerable set exhibits steering. The nesting of classical description models therefore defines, by complementarity, the hierarchy of observed non-classical correlations.

The following states are examples of steerable states :

- The Bell's state $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ maximises steering. Alice can influence Bob in any chosen base. This is not true for the other Bell's states.

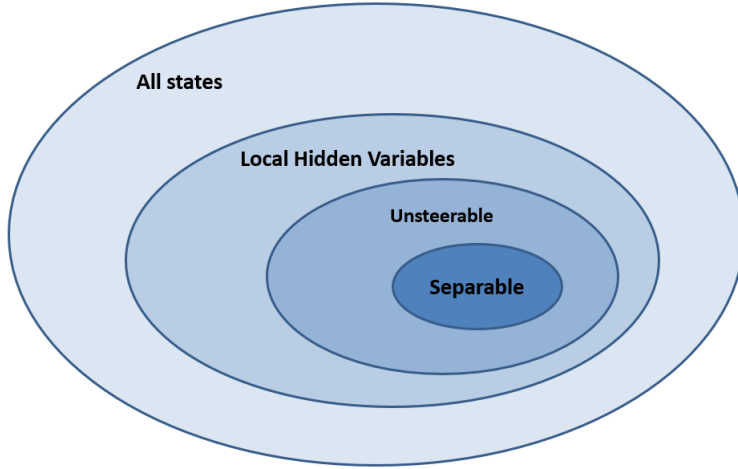


Figure 2.13: Hierarchical relationship between entanglement, steerability, and violations of Bell’s inequality: States that have a local hidden variable model and therefore do not violate any Bell inequality form a convex subset. States with an LHS model are not steerable and form a convex subset of LHV states. Finally, separable states are a convex subset of LHS states.

- Werner’s state $\mathcal{W} = p |\psi^-\rangle \langle \psi^-| + (1-p) \frac{\mathbb{1}}{4}$, for $p > \frac{1}{2}$, the state is steerable but not necessarily local in the sense of Bell’s inequalities.

In opposition, the following states are not steerable :

- Werner’s state $\mathcal{W} = p |\psi^-\rangle \langle \psi^-| + (1-p) \frac{\mathbb{1}}{4}$, for $p \leq \frac{1}{2}$, this shows that entanglement alone does not imply steerability.
- Separable states, such as $\rho = \frac{1}{2} |00\rangle \langle 00| + \frac{1}{2} |11\rangle \langle 11|$, if there is no entanglement, there is no steerability.

2.17.1 Steerability and Bell’s States

The four Bell states ($|\psi^+\rangle, |\psi^-\rangle, |\phi^+\rangle, |\phi^-\rangle$), although maximising entanglement equally, do not all maximise steerability. This depends on the observables and measurements chosen in the experimental scenarios.

Although the other Bell states are also maximally entangled, their steerability depends on the measurement basis chosen. For example, $\phi^+ = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ will maximised their steerability in σ_Z basis, but not in the other.

2.17.2 Werner's states

A Werner state is a composite state that exhibits a particular combination of quantum entanglement and classical mixing. For two qubits, a Werner state can be expressed as follows:

$$\mathcal{W} = p|\psi^-\rangle\langle\psi^-| + (1-p)\frac{\mathbb{1}}{4} \quad (2.78)$$

where :

- p is a real parameter between 0 and 1 that determines the relative weight of the entangled state and the mixed state.
- $|\psi^-\rangle$ is a Bell state, a maximally entangled.
- $\frac{\mathbb{1}}{4}$ represents the completely mixed state, i.e. a statistical mixture of all possible states with equal probabilities.

The properties of this state vary according to the value of p .

- If $p = 1$, the state is purely entangled. The two qubits are perfectly correlated, and a measurement on one instantaneously determines the state of the other, whatever the distance separating them.
- If $p = 0$, the state is completely mixed. There is no correlation between the two qubits, and they are described by a diagonal matrix density.
- If $0 < p < 1$, the state is a superposition of an entangled state and a mixed state. The closer p is to 1, the greater the entanglement.
- If $p > \frac{1}{3}$ the state is entangled.
- If $p \leq \frac{1}{\sqrt{2}}$ quantum correlations are no longer sufficient to overcome the classical limit of 2 of Bell's inequality, and the state becomes local in the CHSH context.
- If $p > \frac{1}{\sqrt{2}}$, the state retains sufficient entanglement to demonstrate non-locality in the Bell framework and violate the CHSH inequality.
- If $p \leq \frac{1}{2}$, the state is not steerable.
- If $p > \frac{1}{2}$, the state is steerable.

3. Quantum communication

3.1 Introduction

Quantum communication is the art of transferring a quantum state from one place to another. It is a crucial driver for the advancement of quantum technology. Some quantum properties, such as the no-cloning theorem, may seem restrictive but offer numerous advantages in their applications, including completely secure information transfer. Furthermore, quantum communication offers the potential for long-distance information transmission with enhanced accuracy and reliability.

Quantum communications use photons to transmit qubits between distant locations. Photons are very well isolated from disturbances, which results in long-lived superposition states for photonic qubits. In addition, they can propagate with low attenuation (up to $0.2\text{dB}/\text{km}$ at $1.55\mu\text{m}$) in optical fibers.

3.1.1 No-cloning

It is impossible to clone, that is, make identical copies of unknown quantum states [31]. Presented in another way, an observer cannot clone a quantum state if he does not know how it was prepared. This result is equivalent to the impossibility of discerning two non-orthogonal quantum states with certainty. If the states are known, then copying them is akin to copying classical bits, making it feasible.

Similarly, it is impossible to erase or hide the information contained in the correlations of a quantum state between two systems. These results suggest that the information associated with quantum states is permanent and cannot be duplicated or destroyed. Assume there is a unitary transformation \mathcal{U}_{clone} that clones a system into an unknown state.

For two states $|\phi\rangle$ and $|\psi\rangle$, we get :

- $\mathcal{U}_{clone} |\phi\rangle |0\rangle = |\phi\rangle |\phi\rangle$
- $\mathcal{U}_{clone} |\psi\rangle |0\rangle = |\psi\rangle |\psi\rangle$.

Now let us take the state $|\sigma\rangle = \frac{1}{\sqrt{2}}(|\phi\rangle + |\psi\rangle)$:

$$\begin{aligned}
U_{clone} |\sigma\rangle |0\rangle &= U_{clone} \frac{1}{\sqrt{2}}(|\phi\rangle + |\psi\rangle) |0\rangle = \frac{1}{\sqrt{2}}(|\phi\rangle |\phi\rangle + |\psi\rangle |\psi\rangle) \\
&\neq |\sigma\rangle |\sigma\rangle = \frac{1}{2}(|\phi\rangle |\phi\rangle + |\phi\rangle |\psi\rangle + |\psi\rangle |\phi\rangle + |\psi\rangle |\psi\rangle)
\end{aligned}$$

This demonstrates the non-cloning theorem.

The non-cloning theorem concerns pure states only, but it is possible to generalise the statement to mixed states using the non-diffusion theorem.

3.1.2 Teleportation

Teleportation [32] is a perfect communication of all quantum information from one place to another without loss [33].

To teleport a photon from one place to another, we copy the state of the photon to be teleported onto a photon present at the desired location. This process is known as quantum teleportation. However, because of the non-cloning principle, copying a quantum state is impossible. As a result, teleportation can only occur if the teleportation system does not retain any information about the teleported state and the original state is destroyed during the process.

When Alice and Bob share a pair of entangled photons, their communication is enhanced. However, the entanglement itself does not carry any information. By sending a classical message, Alice can convey an unknown qubit to Bob.

Without entanglement, Alice can measure the qubit in a randomly chosen basis and ask Bob to recreate the qubit corresponding to her result. If the basis Alice has selected is correct, then Bob's qubit will match hers; otherwise, it will not. The average fidelity of Bob's qubit with respect to Alice's is $\frac{2}{3}$. However, with entanglement, Alice and Bob share a pair of entangled qubits, for example, $|0\rangle_a |0\rangle_b + |1\rangle_a |1\rangle_b$. If Alice also owns a random qubit $\mu |0\rangle_{a'} + \nu |1\rangle_{a'}$ she doesn't know, but wants to send to Bob. Bob's qubit can be written as an equal superposition of four states corresponding to Alice's unknown qubit with σ_X or σ_Z . So, the state of the three-qubit can be written:

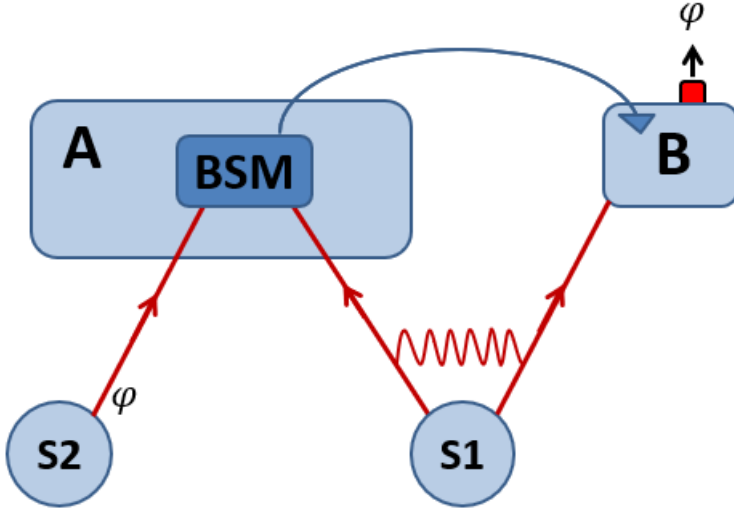


Figure 3.1: Alice performs a BSM on the unknown qubit and a photon from the entangled state. The result does not disclose the state of the qubit but is sent to Bob, who performs a result-dependent operation to complete the teleportation and obtain the same state as Alice's unknown state.

$$\begin{aligned}
 (\mu |0\rangle_{a'} + \nu |1\rangle_{a'}) (|0\rangle_a |0\rangle_b + |1\rangle_a |1\rangle_b) = & \\
 & (|0\rangle_{a'} |0\rangle_a + |1\rangle_{a'} |1\rangle_a) (\mu |0\rangle_b + \nu |1\rangle_b) \\
 & + (|0\rangle_{a'} |0\rangle_a - |1\rangle_{a'} |1\rangle_a) (\mu |0\rangle_b - \nu |1\rangle_b) \\
 & + (|0\rangle_{a'} |1\rangle_a + |1\rangle_{a'} |0\rangle_a) (\mu |1\rangle_b + \nu |0\rangle_b) \\
 & + (|0\rangle_{a'} |1\rangle_a - |1\rangle_{a'} |0\rangle_a) (\mu |1\rangle_b - \nu |0\rangle_b).
 \end{aligned}
 \tag{3.1}$$

By performing a Bell measurement, Alice can determine which of the four Bell's states Bob has.

- If she get $|\Phi^+\rangle$, Bob doesn't have to do anything
- If she get $|\Phi^-\rangle$, Bob needs to apply σ_Z
- If she get $|\Psi^+\rangle$, Bob needs to apply σ_X
- If she get $|\Psi^-\rangle$, Bob needs to apply $\sigma_X \sigma_Z$.

Bob can transform his qubit into the exact copy of Alice's unknown qubit with only the sending of two classical messages from Alice.

3.1.3 SuperDense Coding

Quantum dense coding is one of the most essential quantum communication protocols [34]. The principle is to use quantum resources to boost quantum communication.

If Alice sends a bit to Bob, Bob will receive a single bit of information. If Alice sends a qubit to Bob, he will receive a single bit of information. But if Alice and Bob share an entangled pair and Alice sends a qubit, then Bob gets two bits of information. The entangled pair does not have any information. It is just part of the network.

Consider Alice and Bob who share an entangled state $|0\rangle_a |0\rangle_b + |1\rangle_a |1\rangle_b$. Alice performs one of the following operations on her qubit:

- Do nothing and leave the qubit unchanged
- Perform σ_X which transform $|0\rangle \rightarrow |1\rangle$ and $|1\rangle \rightarrow |0\rangle$
- Perform σ_Z which doesn't affect $|0\rangle$ and changes the sign of $|1\rangle$ ($|1\rangle \rightarrow -|1\rangle$ and $-|1\rangle \rightarrow |1\rangle$)
- Perform σ_X and σ_Z .

Then, she sends her qubit to Bob, who ends up with one of four Bell's states:

- $|\Phi^+\rangle = |0\rangle_a |0\rangle_b + |1\rangle_a |1\rangle_b$
- $|\Psi^+\rangle = |1\rangle_a |0\rangle_b + |0\rangle_a |1\rangle_b$
- $|\Phi^-\rangle = |0\rangle_a |0\rangle_b - |1\rangle_a |1\rangle_b$
- $|\Psi^-\rangle = |1\rangle_a |0\rangle_b - |0\rangle_a |1\rangle_b$.

As these states are orthogonal, Bob can use a Bell measurement to determine which state they are. Thus, Alice communicates two bits of information to Bob by sending him a single qubit. This is called quantum dense coding [35].

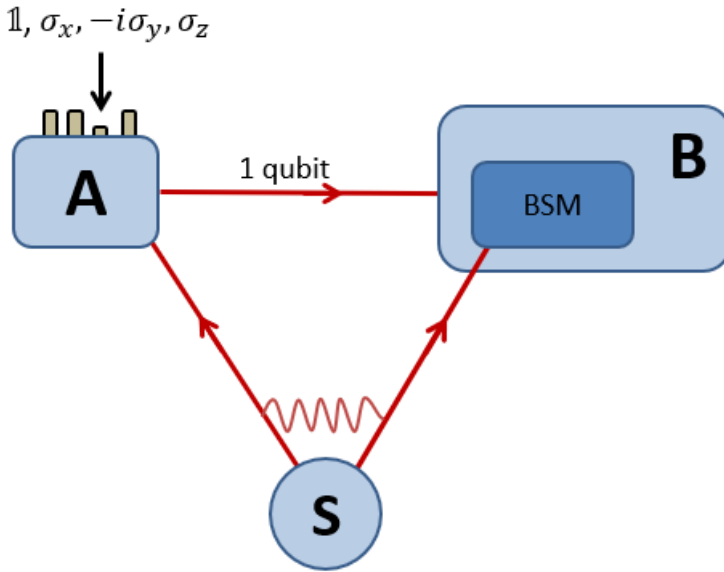


Figure 3.2: Alice and Bob share an entangled pair. Alice performs a unitary transformation and sends a qubit to Bob, who can determine Alice's initial state with a Bell state measurement.

3.1.4 Random Access Code

Random access codes (RACs) are communication tasks in which several (n) bits are encoded into a smaller number (m) of bits [36]. Original bits can be recovered individually with a certain probability of success (p). These one-way communication tasks are denoted as $n \mapsto m$ [37].

Let us focus on two-dimensional RACs: $2 \mapsto 1$. First, let us examine the classical case.

This is the simplest scenario where two bits are encoded into a single bit. Alice has an input string consisting of two bits $x = x_1x_2$, but can only send a single bit to Bob, who might be interested in either of the two bits.

The strategy that yields the best result is as follows: Alice consistently sends the first bit, x_1 . If the bit of interest to Bob is x_1 , as this is the bit sent systematically by Alice, he receives it directly. If Bob is interested in x_2 , he guesses its value with a probability of success of $1/2$. Bob's overall probability of success is, therefore, :

$$P_{2 \rightarrow 1}^C = \frac{3}{4} \quad (3.2)$$

Note that in attempting to recover all results from the input chain, which fall outside the Random Access Code framework, the maximum probability of success is only 50%.

Let us now examine quantum RACs (QRACs) [38]. There are two types of quantum RACs:

- Quantum communication RAC: Alice prepares and sends a qubit
- Entangled assisted RAC: Alice and Bob share an entangled pair, and communication occurs over a classical channel.

Their effectiveness is comparable, but the optimal choice often depends on the specific situation. A key advantage over conventional RACs is that once Bob makes a measurement, no further information can be obtained.

For QRACs, Alice's input string has 2^n possible values. As we are interested in two-dimensional QRACs, here $n = 2$ and Alice's input string contains 4 possible values corresponding to four values of the equatorial plane of the Bloch Sphere separated by $\frac{\pi}{2}$. These values can be expressed using a two-level quantum system:

$$|\psi_{x_1 x_2}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \frac{(-1)^{x_1} + i(-1)^{x_2}}{\sqrt{2}}|1\rangle) \quad (3.3)$$

with $x_1, x_2 \in \{0, 1\}^2$. The coordinates of this state on the Bloch Sphere are the following: $r(x) = \frac{1}{\sqrt{2}} \begin{pmatrix} (-1)^{x_1} \\ (-1)^{x_2} \\ 0 \end{pmatrix}$.

The four encoded states are the corners of a square $\frac{1}{\sqrt{2}}(\pm 1, \pm 1, 0)$, i.e. $\left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ -1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} \right)$, drawn in the unit circle of the xy plane. These encoding states are symmetrically distributed on the equator of the Bloch sphere's surface. They present the optimal choice considering that all encoding points should be as far as possible from the two planes orthogonal to the x and y axes, which divide the sphere into four parts, thus maximising the probability of success in the worst-case scenario.

Bob uses two pairs of mutually orthogonal vectors of the Bloch sphere that are opposed. Let us take the following two bases as an example, but any pair of bases obtained by rotating them on the Bloch sphere is equivalent:

- the diagonal/antidiagonal basis $B_1 : \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$
- the left/right basis $B_2 : \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \right\}$.

To find the desired input goal, Bob measures on the basis he is interested (B_1 to find x_1 and B_2 to find x_2).

Bob's probability of success always remains the same and is independent of the measurement he performs or the encoding state he receives:

$$p_{2 \rightarrow 1}^Q = \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}} \right) \approx 0,854 \quad (3.4)$$

This principle can be generalised to more complex systems with a greater number n of bits in the input chain [39]. It should be noted that the probability of success decreases as the number of bits in the input chain increases and that the QRAC still has an advantage over the classical RAC; however, this advantage decreases as n increases.

The advantage of using a quantum RAC over a classical RAC can be calculated by $\frac{p^Q}{p^C}$. When the result is greater than 1, this shows the advantage of quantum RACs.

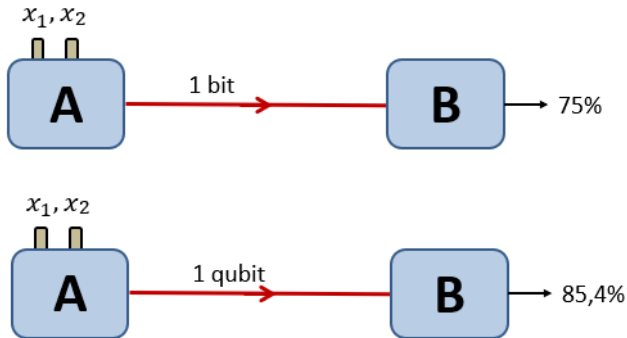


Figure 3.3: Advantage of QRAC2 \rightarrow 1 over RAC2 \rightarrow 1.

4. Experiments

In each of the subsections of this chapter, corresponding respectively to **Paper I, II and III**, we examine three specific cases to answer the following question: Considering different qualities of entanglement and different types of measurement, what kind of protocol can I perform?

4.1 Entanglement-assisted quantum communication with simple measurements

Entanglement and quantum communication are both essential resources in quantum information science, crucial for understanding the non-classical nature of quantum theory. Entanglement has been studied for decades through Bell-type experiments, where communication between parts is excluded. More recently, quantum communication has been explored in preparation and measurement experiments without the aid of shared entanglement. It is therefore natural to analyse the general scenario in which entanglement and quantum communication coexist.

As a reminder, we saw earlier that superdense coding is a quantum communication protocol, first introduced by Charles Bennett and Stephen Wiesner in their article of 1992 [34], which allows the transmission of a quantity of classical bits of information by sending only a small number of qubits, provided that the sender and receiver share an entangled quantum resource.

Dense coding illustrates the power of entangled quantum communication. By sharing an EPR pair, this protocol enables the transmission of two bits of classical information through a single qubit. In contrast, a single qubit can carry only one bit of information. No protocol that sends a qubit and utilises entanglement can transmit more than two bits. In addition to requiring an EPR pair, dense coding also necessitates measurement on the Bell basis, which involves joint measurement of the two qubits in an entanglement-maximising basis. Separable measurements, however, provide no advantage over conventional communication, regardless of the entangled state shared.

In its basic form, this protocol allows Alice to communicate two classical bits ('00', '01', '10' or '11') to Bob by transmitting only one qubit, provided that they first share a pair of maximally entangled qubits, referred to as a Bell

state. This method is inherently secure for quantum communication, as Bob must possess both qubits – the one received from Alice and his own entangled qubit – to decode the information, effectively eliminating the risk of interception. Any attempt at measurement by a spy would collapse the state of the qubit, immediately alerting Alice and Bob [34].

Like quantum teleportation, it is fundamentally based on quantum entanglement as a resource. However, they serve different purposes: superdense coding optimises the transmission of classical information, while quantum teleportation enables the transfer of quantum states [40].

The first experimental demonstration of this protocol was carried out in 1996 by Mattle et al. [41], who used entangled photons in polarisation to validate its feasibility in the laboratory. Then variations were made around it, in particular it was simulated in nuclear magnetic resonance using temporal averaging[42], studied theoretically [43–45] and experimentally [46; 47] in the context of continuous variables.

This protocol has also been considered for more than two entangled bits[48–52] or entangled degrees of freedom[53].

In 2004, a superdense coding experiment was carried out using trapped Be^+ ions[54], and in the same year, a densencoding experiment was carried out over a long distance using fibre optics[55]. In 2017, an improved capacity of 1.665 bits with a fidelity of 0.87 was achieved using fibre optics [56].It is also possible to perform superdense coding using qudits to increase information transmission capacity: high-dimensional superdense coding. This approach allows more than two classical bits to be encoded per transmitted qudit. Recently, a channel capacity of 3.021 bits with a fidelity of 0.973 was demonstrated using an eight-dimensional entangled state on a quantum photonic chip. [57]. More recently, experiments have exploited high-dimensional ququarts, states formed by pairs of photons, to achieve a capacity of 2.09 bits (with a theoretical limit of 2.32 bits) and a fidelity of 0.98 [58].

The research has also extended superdense coding to multi-partner scenarios, where multiple parties share entangled states to transmit classical information. A protocol based on a three-qubit GHZ state can generate eight mutually orthogonal states, which is sufficient to encode three bits of information. This approach can be generalised to N-qubit GHZ states, allowing Alice to generate (2^N) mutually orthonormal states, suitable for encoding N bits of classical information [59].

Although theory and experiments on superdense coding have made significant progress, its large-scale implementation and reliability in the real world still face several major challenges that limit its large-scale deployment and robustness in real-world environments. This is particularly true for projects involving satellites. The protocol would require infinite quantum memory or

the use of dual quantum channels, which are unfortunately highly vulnerable to signal loss between a satellite and Earth. This makes the implementation of this system extremely difficult for telescope-satellite-ground links [60].

Noise and decoherence are also unavoidable factors in our environment. They degrade the quality of entanglement and, as a result, reduce the fidelity and capacity of the superdense coding channel. For the protocol to work, very fragile quantum states are required, which decoherence tends to destroy [61; 62].

However, optical systems, unlike other platforms, do not allow measurements to be made directly in the Bell basis on separate photons. While optics is an ideal platform for quantum communication, such measurements are impossible to achieve with linear optics without recourse to auxiliary degrees of freedom. Nevertheless, demonstrations of dense two-qubit coding have been accomplished in optics, notably through partial measurements in the Bell basis or using continuous variables, or by introducing additional qubits via hyper-driving. Beyond qubits, partial measurements of the Bell basis have recently been implemented on systems of dimension four, enabling the exceeding of the two-bit communication limit. However, the deterministic implementation of such sophisticated measures remains challenging, especially without auxiliary qubits, and scaling these measures beyond a few dimensions poses a considerable challenge.

In this project, we extend the framework of dense coding to more general communication tasks that involve entanglement and quantum communication. When these resources are available, little is known about the predictions of quantum theory. We focus on the minimal resources needed: a qubit message and a shared EPR state. We demonstrate that specific correlation scenarios enable the generation of quantum correlations that are impossible to simulate with only two classical communication bits, i.e., unfeasible for an ideal dense coding protocol. We first introduce a correlation task in which a standard partial Bell state analyzer generates quantum correlations that cannot be simulated using two communication bits. We then turn to a well-known communication task, the random access code, and show that product measurements are sufficient to outperform classical models and even reach the predictive limits of quantum theory for a two-qubit system. Therefore, there are communication tasks where an entangled quantum channel, with no interference between the two photonic carriers, achieves optimum performance.

4.2 Quantum Network

Quantum cryptography officially came into being in 1983, when Bennett and Brassard discovered that photons could be used to transmit quantum states, introducing the concept of quantum key distribution (QKD), as one of the solutions considered to strengthen information security. Thanks to the no-cloning theorem, any attempt to spy by intercepting photons alters their state, thus revealing the interception. In 1991, Ekert proposed a quantum key distribution (QKD) protocol based on quantum entanglement, where security is ensured through the verification of Bell's inequalities. Other significant advances in quantum communication followed, such as quantum teleportation, which allows a quantum state to be transferred using two classical bits and one entanglement bit, and superdense coding, where a qubit accompanied by an entanglement bit can transmit as much information as two classical bits. Since then, numerous other methods have been developed by theorists to integrate the principles of classical communication with those of quantum physics, resulting in the emergence of quantum information science.

QKD is based on the principle of unconditional security guaranteed by the laws of physics. However, the practical realisation of QKD systems faces constraints related to the imperfections of the components. These imperfections create vulnerabilities that can be exploited by attackers, casting doubt on the absolute security promised by the theory.

The measurement-device-independent quantum key distribution (MDI-QKD) protocol, which is insensitive to side-channel attacks and compatible with physical constraints, provides an unparalleled security guarantee. Its principle relies on the use of quantum entanglement sources, facilitating the creation of non-local correlations between various nodes in a network. These correlations are utilised in nonlocality protocols, such as the total nonlocality protocol, to ensure the security of key distribution. Consequently, MDI-QKD is a vital solution for building large-scale quantum networks and achieving a quantum Internet. We perform, for the first time, an experimental study on a new full-network nonlocality protocol proposed in a bilocal scenario.

Quantum non-locality is a phenomenon where the measurement statistics of a multipartite quantum system cannot be explained by local realism [63]. It has become an indispensable operational resource for device-independent quantum technologies. While early demonstrations focused on two-party scenarios, the emergence of quantum networks has introduced new complexities and opportunities, requiring a more nuanced understanding of non-locality.

While early demonstrations focused on two-party scenarios, the emergence of quantum networks has introduced new complexities. Network Non-locality (NN) was introduced to characterise correlations that cannot be explained by

local hidden variables in such a multi-source network. Full Network Non-locality (FNN) is an even stronger notion, describing correlations that require all sources in the network to be non-classical. In other words, if even a single source in the network can be described by a classical model of local variables, then the correlations are not considered FNN. This stricter definition is crucial for certifying the integrity of sources in distributed quantum architectures and for device-independent quantum cryptography protocols.

The generalisation of the definition of non-locality was motivated by the advent of device-independent quantum information protocols, where non-locality is identified as a new quantum information resource, distinct from entanglement [64]. The fact that non-locality is recognised as an operational resource, alternative to entanglement and necessary for device-independent protocols, is a major development. This means that non-locality is no longer just a subject of fundamental curiosity, but a practical and indispensable element. Device-independent protocols, which guarantee high security without requiring trust in the internal workings of devices, are made possible by the existence of non-local correlations. This is particularly useful in areas such as cryptography and random number generation.

Recent experimental breakthroughs, particularly in the bilocal scenario, have succeeded in demonstrating this complete network non-locality by closing critical experimental loopholes, thereby validating the non-classical nature of all sources involved. These advances have profound implications for quantum communication security, randomness and entanglement certification, and the development of topologically robust quantum networks. Despite persistent challenges related to scalability, noise, and remaining experimental loopholes, research continues to advance, paving the way for transformative applications in distributed computing, cryptography, and quantum sensing.

A network is a set of interconnected parties that exchange data and resources. The main objective is to enable the transmission of information from one point to another. In a quantum network [65; 66], a source creates entanglement and shares it with several participants. These participants then use entangled measurements to extend the reach of this entanglement across the network [67]. The concept of network nonlocality has been studied in various configurations, including chain, star, triangle, and ring networks. (n, m, p) -type quantum network configuration and its nonlocality.

The bilocal scenario is the simplest of the quantum networks. It involves three observers (Alice, Bob, Charlie) and two independent entanglement sources. One source connects Alice and Bob, and the other connects Bob and Charlie. Bob is the intermediate observer. This scenario is particularly relevant because it is the basis for many entanglement swapping experiments [68].

Although the bipartite scenario (involving two parties and a shared source)

has been the most studied, configurations involving more than two parties reveal qualitatively distinct features. Network nonlocality extends the concept of Bell nonlocality to configurations involving multiple independent sources and parties [69]. It indicates that correlations within the network cannot be explained by models where local variables are emitted by independent sources.

4.3 Weak entanglement improves quantum communication using only product measurements

Although entanglement is a crucial resource in quantum communication, its quality plays an essential role. Traditionally, only forms of entanglement robust enough to generate non-locality and violate Bell’s inequalities were considered essential for surpassing the limits of classical communication. According to this established perspective, weakly entangled states, incapable of violating Bell’s inequality, did not offer such an advantage. In a less efficient context, quantum correlations can still be used to control quantum states. This demonstrates that even if one of the parties is unreliable, Alice and Bob still share entanglement [70].

Erwin Schrödinger introduced the concept of quantum steering [71] in response to Einstein, Podolsky and Rosen’s EPR ‘paradox’ [16]. This phenomenon illustrates the ability to produce different groups of quantum states at a distance by performing measurements on one particle of an entangled pair, which highlights the paradox. Depending on the measurement and its random outcome, the distant system is adjusted to a different state; nevertheless, the unconditional distant state remains constant, preventing any communication exceeding the speed of light.

Quantum steering has been redefined in a quantum information framework [70] promising novel applications such as quantum communication using unreliable devices [72]. This structure also offers the possibility of directly comparing the notions of Bell non-locality, steering and entanglement: steering is necessary for Bell non-locality, and entanglement is indispensable for steering [70]. As with Bell’s inequalities, it is possible to develop experimental criteria to prove steering [73]: steering inequalities impose restrictions on the correlations observed that can be justified without resorting to quantum steering. These inequalities have been violated experimentally [74]. Recent work shows that it is possible to manipulate the direction of steering, i.e. to switch from double ‘one-way’ steering to no steering, by adding noise (phase damping or depolarisation) [75].

An isotropic state $\rho_v = v|\phi^+\rangle\langle\phi^+| + \frac{1-v}{4}$, characterised by its visibility $v \in [0, 1]$, confers an advantage to the transmission of a qubit only when v

exceeds $1/3$. This threshold, corresponding to the separability limit of the state, underlines the importance of sufficient entanglement to take advantage of quantum resources. This result should be put into perspective with the higher thresholds required for more demanding tasks such as quantum steering or the violation of Bell inequalities.

Dense coding relies on measurement in the Bell basis, a complex operation to implement in linear optics with separated photons [26]. Although experiments have been performed, achieving a scalable Bell measurement in this context remains a significant challenge. However, recent studies have highlighted the possibility of exploiting entanglement to enhance the performance of quantum communication using less demanding measurements, which are compatible with passive linear optics. These schemes, while promising, require very high-quality entangled states, capable of violating Bell inequalities, which restricts their experimental applicability.

We aim to show that highly noisy partially entangled states, including those that do not exhibit quantum steering, can nevertheless offer advantages in terms of communication. To do this, we introduce a communication task that corresponds to the cryptographic primitive known as secret sharing. This task involves Alice generating a random secret bit to share with Bob and Charlie, so that they individually have no knowledge of this bit, but can learn its value if they cooperate. Bob and Charlie secretly select random bits and communicate messages to Alice, who then decodes them based on a binary input. Bob and Charlie do not share any prior entanglement and send messages encoded in qubit states. Alice uses a general quantum measurement for decoding.

For the experimental demonstration, polarisation qubits generated by spontaneous parametric down-conversion (SPDC) are used. Two main measurement approaches are employed:

- Product measurements: separate, non-interfering measurements of individual photons.
- Partial Bell state analysers: For a stochastic variant of secret sharing, we consider these more sophisticated measurements, which require optical interference but remain feasible with standard passive linear optics. These analysers reveal advantages for a range of non-directional isotropic states.

Dense coding relies on measurement in the Bell basis, a complex operation to implement in linear optics with separate photons. Although experiments have been conducted, achieving scalable Bell measurement in this context remains a significant challenge. However, recent studies have highlighted the possibility of exploiting entanglement to improve quantum communication

performance using less demanding measurements compatible with passive linear optics. These schemes, although promising, require very high-quality entangled states capable of violating Bell inequalities, which limits their experimental applicability.

Here, we explore the limits of entanglement to improve quantum communication. The central hypothesis of our study is that even weakly entangled states can improve communication over a qubit channel. We demonstrate that secret sharing tasks can be performed using highly noisy entangled states and simple measurements, such as non-interfering single-photon product measurements or slightly more sophisticated but nevertheless standard partial Bell state analysers. The importance of this approach lies in the fact that such measurements are experimentally less demanding than schemes requiring high-quality entanglement or the violation of Bell inequalities. We identify the conditions in entangled states for which these protocols are effective and demonstrate the feasibility of our approach experimentally. These results contribute to broadening the scope of quantum entanglement in quantum communication.

5. Conclusion and outlook

5.1 Entanglement-assisted quantum communication with simple measurements

Since it was theorised by Bennett and Wiesner in 1992, this protocol has undergone numerous improvements and has been found to have major implications for secure data transmission over long distances. By encoding classical information on entangled qubits, superdense coding enables the development of secure communication protocols that are resistant to eavesdropping attacks. This is particularly relevant for quantum cryptography, where secure key distribution is crucial. It plays an important role in improving quantum error correction protocols. By enabling the transmission of multiple bits of error correction information per qubit, it increases the efficiency of the correction process and allows for the correction of more complex errors. Superdense coding is not an isolated protocol, but an essential component of an interconnected quantum ecosystem.

However, significant challenges remain. The generation and distribution of high-quality entanglement over long distances, the fight against decoherence and noise in quantum channels, as well as scalability issues and the complexity of Bell state measurements, particularly for high-dimensional systems, are all obstacles to be overcome for practical large-scale implementation.

In **Paper I**, we have come to the conclusion that simple measurements are sufficient to generate quantum correlations that cannot be modelled by two bits of classical communication and can be an optimal protocol for quantum resources—justifies moving from dense coding to larger quantum communication tasks. Conceptually, this paves the way for new research into entangled-assisted correlations based on product measurements. A natural question that arises is understanding when and why such measurements are useful for quantum communication. These protocols offer significant practical advantages by avoiding complex entangled measurements and by making do with devices that only require measurements on individual systems. This could make the implementation of high-dimensional, multi-particle quantum protocols more accessible while offering a viable approach for fundamental experiments using these natural quantum resources.

5.2 Quantum Network

Non-local quantum correlations form the basis of innovative, device-independent protocols such as quantum key distribution (QKD). By exploiting this non-locality, quantum networks can guarantee cryptographic security without requiring trust in the hardware [64]. This is known as ‘trustless security’, a much stronger guarantee than simple ‘secure communication’.

Full network non-locality provides robust, device-independent certification for all sources in a network. This means that it can prove the absence of classical sources in the network. Unlike standard Bell tests, which can only certify the non-classicality of a single link, full network non-locality validates the integrity of the quantum resources of the entire network [76].

Research is also exploring the certification of entanglement and true network non-locality [77]. Recent studies on the sharing and recycling of complete network non-locality in extended bilocal scenarios have revealed important distinctions [78]. Passive sharing, where intermediate observers do not actively cooperate, is impossible. In contrast, active sharing, which requires increased cooperation from intermediate observers via specific measures, can be achieved [79].

The impossibility of passive sharing shows that the mere presence of entangled sources is not sufficient.

In this context, in **Paper II**, we have deepened our study of quantum key distribution by developing protocols and hardware for multi-user quantum networks. Our innovative approach involves certifying the security of an entangled network using a bilocal configuration. As a result, we were able to highlight the nonlocality of the entire network and refute a Bell inequality, thereby strengthening confidence in the security of our communications.

5.3 Weak entanglement improves quantum communication using only product measurements

In **Paper III**, we demonstrate that weakly entangled quantum states can improve communication over a qubit channel without requiring interference between photons. To achieve this, we use only separate measurements and not joint measurements. By employing these separate measurements, we show that all isotropic two-qubit states, even those with weak entanglement, offer a quantum advantage for a secret-sharing task. Furthermore, these exact measurements can also provide communication advantages from partially entangled and noisy states, which do not have a clear quantum direction.

This research fundamentally changes the understanding of the practical

usefulness of entanglement. Previously, strong (non-local Bell) entanglement was considered indispensable for obtaining a quantum advantage in communication. This work demonstrates that even weak or noisy entanglement, when combined with specific and simpler measurement techniques, can confer a quantum advantage. Product measurements and partial Bell state analysers, being ‘much less experimentally demanding’, make it possible to achieve this result. The way in which measurements are performed is just as important as the quality of the entanglement itself. This allows us to use a wider range of quantum states, including those that are only weakly entangled and are easier to preserve in noisy environments. This suggests that robust quantum communication systems can be built without the need for perfect entanglement.

The fundamental result that weak entanglement with simple measurements can offer a quantum advantage implies a crucial shift: from searching for ‘perfect’ or ‘maximally entangled’ states (which are very sensitive to decoherence) to developing robust protocols that can work effectively with “imperfect” or ‘noisy’ states. Maintaining high-quality entanglement is difficult in real, noisy environments. If weak and noisy entanglement can nevertheless offer an advantage with simple measurements, this significantly lowers the experimental and engineering barrier for practical quantum communication. This approach suggests that quantum communication can prioritise robustness and fault tolerance in noisy channels, much like classical communication. This paves the way for building quantum networks with current technologies, rather than waiting for perfect quantum hardware.

References

- [1] CHARLES H. BENNETT AND GILLES BRASSARD. **Quantum Cryptography: Public Key Distribution and Coin Tossing.** In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, Bangalore, India, 1984. 33
- [2] MICHAEL A. NIELSEN AND ISAAC L. CHUANG. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, Cambridge, 2010. 35
- [3] THOMAS YOUNG. **I. The Bakerian Lecture. Experiments and calculations relative to physical optics.** *Philosophical Transactions of the Royal Society of London*, pages 1 – 16. 35
- [4] A. EINSTEIN. **Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt.** *Annalen der Physik*, **322**(6):132–148, 1905. 35
- [5] LOUIS DE BROGLIE. *Recherches sur la théorie des Quanta.* Theses, Migration - université en cours d'affectation, November 1924. 35
- [6] PAUL ADRIEN MAURICE DIRAC. *The Principles of Quantum Mechanics.* Oxford University Press, Oxford, 1930. 36
- [7] ALBERT EINSTEIN, BORIS PODOLSKY, AND NATHAN ROSEN. **Can quantum-mechanical description of physical reality be considered complete?** *Physical review*, **47**(10):777–780, 1935. 39, 49
- [8] DANIEL M. GREENBERGER, MICHAEL A. HORNE, AND ANTON ZEILINGER. **Going beyond Bell's Theorem.** In MINAS KAFATOS, editor, *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, pages 69–72. Kluwer Academic Publishers, Dordrecht, 1989. 40
- [9] PAUL ADRIEN MAURICE DIRAC. **On the Theory of Quantum Mechanics.** *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character*, **112**:661–677, 1926. 43
- [10] HARRY BUHRMAN, RICHARD CLEVE, SERGE MASSAR, AND RONALD DE WOLF. **Nonlocality and communication complexity.** *Rev. Mod. Phys.*, **82**:665–698, Mar 2010. 43
- [11] F. BLOCH. **Nuclear Induction.** *Phys. Rev.*, **70**:460–474, Oct 1946. 44
- [12] MICHAEL A. NIELSEN AND ISAAC L. CHUANG. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, 2010. 45
- [13] REINHARD F. WERNER. **Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model.** *Phys. Rev. A*, **40**:4277–4281, Oct 1989. 47
- [14] C. S. WU AND I. SHAKNOV. **The Angular Correlation of Scattered Annihilation Radiation.** *Phys. Rev.*, **77**:136–136, Jan 1950. 47
- [15] J. S. BELL. **On the Einstein Podolsky Rosen paradox.** *Physics Physique Fizika*, **1**:195–200, Nov 1964. 49, 50

- [16] A. EINSTEIN, B. PODOLSKY, AND N. ROSEN. **Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?** *Phys. Rev.*, **47**:777–780, May 1935. 52, 88
- [17] JOHN F. CLAUSER, MICHAEL A. HORNE, ABNER SHIMONY, AND RICHARD A. HOLT. **Proposed Experiment to Test Local Hidden-Variable Theories.** *Phys. Rev. Lett.*, **23**:880–884, Oct 1969. 52
- [18] B. S. CIREL'SON. **Quantum generalizations of Bell's inequality.** *Letters in Mathematical Physics*, **4**:93–100, 1980. 54
- [19] ÉTIENNE-LOUIS MALUS. **Sur une propriété de la lumière réfléchie.** *Mémoires de physique et de chimie de la Société d'Arcueil*, **2**:143–158, 1809. 55
- [20] BERTHOLD-GEORG ENGLERT, CHRISTIAN KURTSIEFER, AND HARALD WEINFURTER. **Universal unitary gate for single-photon two-qubit states.** *Phys. Rev. A*, **63**:032303, Feb 2001. 58
- [21] PAUL G. KWIAT, KLAUS MATTLE, HARALD WEINFURTER, ANTON ZEILINGER, ALEXANDER V. SERGIENKO, AND YANHUA SHIH. **New High-Intensity Source of Polarization-Entangled Photon Pairs.** *Phys. Rev. Lett.*, **75**:4337–4341, Dec 1995. 62
- [22] C. K. HONG, Z. Y. OU, AND L. MANDEL. **Measurement of subpicosecond time intervals between two photons by interference.** *Phys. Rev. Lett.*, **59**:2044–2046, Nov 1987. 64
- [23] L. MANDEL. **Quantum effects in one-photon and two-photon interference.** *Rev. Mod. Phys.*, **71**:S274–S282, Mar 1999. 64
- [24] A OURJOUNTSEV, M-C DHEUR, T AVIGNON, AND L JACUBOWIEZ. **Two-photon quantum interference for an undergraduate lab.** *European Journal of Physics*, **36**(6):065034, 2015. 64
- [25] MARKUS MICHLER, KLAUS MATTLE, HARALD WEINFURTER, AND ANTON ZEILINGER. **Interferometric Bell-state analysis.** *Phys. Rev. A*, **53**:R1209–R1212, Mar 1996. 68
- [26] N. LÜTKENHAUS, J. CALSAMIGLIA, AND K.-A. SUOMINEN. **Bell measurements for teleportation.** *Phys. Rev. A*, **59**:3295–3300, May 1999. 68, 89
- [27] MATTHIAS J. BAYERBACH, SIMONE E. D'AURELIO, PETER VAN LOOCK, AND STEFANIE BARZ. **Bell-state measurement exceeding 50% success probability with linear optics.** *Science Advances*, **9**(32):eadf4080, 2023. 68
- [28] PHILIP WALTHER AND ANTON ZEILINGER. **Experimental realization of a photonic Bell-state analyzer.** *Phys. Rev. A*, **72**:010302, Jul 2005.
- [29] LING-JUN KONG, YONGNAN LI, YU SI, RUI LIU, CHENGHOU TU, AND HUI-TIAN WANG. **Near-complete polarization Bell-state analysis based on symmetry-broken scheme with linear optics,** 2015. 68
- [30] ROOPE UOLA, ANA C. S. COSTA, H. CHAU NGUYEN, AND OTFRIED GÜHNE. **Quantum steering.** *Rev. Mod. Phys.*, **92**:015001, Mar 2020. 71
- [31] D. DIEKS. **Communication by EPR devices.** *Physics Letters A*, **92**(6):271–272, 1982. 75
- [32] DIK BOUWMEESTER, JIAN-WEI PAN, KLAUS MATTLE, MANFRED EIBL, HARALD WEINFURTER, AND ANTON ZEILINGER. **Experimental quantum teleportation.** , **390**(6660):575–579, December 1997. 76
- [33] CHARLES H. BENNETT, GILLES BRASSARD, CLAUDE CRÉPEAU, RICHARD JOZSA, ASHER PERES, AND WILLIAM K. WOOTTERS. **Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels.** *Phys. Rev. Lett.*, **70**:1895–1899, Mar 1993. 76
- [34] CHARLES H. BENNETT AND STEPHEN J. WIESNER. **Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states.** *Phys. Rev. Lett.*, **69**:2881–2884, Nov 1992. 78, 83, 84

- [35] ANDRIS AMBAINIS, ASHWIN NAYAK, AMMON TA-SHMA, AND UMESH VAZIRANI. **Dense quantum coding and a lower bound for 1-way quantum automata.** In *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing*, STOC '99, page 376–383, New York, NY, USA, 1999. Association for Computing Machinery. 78
- [36] STEPHEN WIESNER. **Conjugate coding.** *SIGACT News*, **15**(1):78–88, January 1983. 79
- [37] JOÃO DORIGUELLO AND ASHLEY MONTANARO. **Quantum Random Access Codes for Boolean Functions.** *Quantum*, **5**:402, 03 2021. 79
- [38] ARMIN TAVAKOLI, ALLEY HAMEEDI, BRENO MARQUES, AND MOHAMED BOURENNANE. **Quantum Random Access Codes Using Single d -Level Systems.** *Phys. Rev. Lett.*, **114**:170502, Apr 2015. 80
- [39] ANDRIS AMBAINIS, ASHWIN NAYAK, AMMON TA-SHMA, AND UMESH VAZIRANI. **Dense quantum coding and a lower bound for 1-way quantum automata.** In *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing*, STOC '99, page 376–383, New York, NY, USA, 1999. Association for Computing Machinery. 81
- [40] ERIC CHITAMBAR AND FELIX LEDITZKY. **On the Duality of Teleportation and Dense Coding.** *Physical Review A*, **94**(5):052329, 2016. 84
- [41] KLAUS MATTLE, HARALD WEINFURTER, PAUL G. KWIAT, AND ANTON ZEILINGER. **Dense Coding in Experimental Quantum Communication.** *Phys. Rev. Lett.*, **76**:4656–4659, Jun 1996. 84
- [42] XIMING FANG, XIWEN ZHU, MANG FENG, XI'AN MAO, AND FEI DU. **Experimental implementation of dense coding using nuclear magnetic resonance.** *Phys. Rev. A*, **61**:022307, Jan 2000. 84
- [43] MASASHI BAN. **Quantum dense coding via a two-mode squeezed-vacuum state.** *Journal of Optics B: Quantum and Semiclassical Optics*, **1**(6):L9, dec 1999. 84
- [44] SAMUEL L. BRAUNSTEIN AND H. J. KIMBLE. **Dense coding for continuous variables.** *Phys. Rev. A*, **61**:042302, Mar 2000.
- [45] T. C. RALPH AND E. H. HUNTINGTON. **Unconditional continuous-variable dense coding.** *Phys. Rev. A*, **66**:042321, Oct 2002. 84
- [46] XIAOYING LI, QING PAN, JIETAI JING, JING ZHANG, CHANGDE XIE, AND KUNCHI PENG. **Quantum Dense Coding Exploiting a Bright Einstein-Podolsky-Rosen Beam.** *Phys. Rev. Lett.*, **88**:047904, Jan 2002. 84
- [47] JUN MIZUNO, KENTARO WAKUI, AKIRA FURUSAWA, AND MASAHIDE SASAKI. **Experimental demonstration of entanglement-assisted coding using a two-mode squeezed vacuum state.** *Phys. Rev. A*, **71**:012304, Jan 2005. 84
- [48] S. BOSE, V. VEDRAL, AND P. L. KNIGHT. **Multiparticle generalization of entanglement swapping.** *Phys. Rev. A*, **57**:822–829, Feb 1998. 84
- [49] JIU-CANG HAO, CHUAN-FENG LI, AND GUANG-CAN GUO. **Controlled dense coding using the Greenberger-Horne-Zeilinger state.** *Phys. Rev. A*, **63**:054301, Apr 2001.
- [50] HYUK-JAE LEE, DOYEOL AHN, AND SUNG WOO HWANG. **Dense coding in entangled states.** *Phys. Rev. A*, **66**:024304, Aug 2002.
- [51] ANTONI WÓJCIK AND ANDRZEJ GRUDKA. **Comment I on “Dense coding in entangled states”.** *Phys. Rev. A*, **68**:016301, Jul 2003.
- [52] O. AKHAVAN AND A. T. REZAKHANI. **Comment II on “Dense coding in entangled states”.** *Phys. Rev. A*, **68**:016302, Jul 2003. 84

- [53] KAORU SHIMIZU, NOBUYUKI IMOTO, AND TAKAAKI MUKAI. **Dense coding in photonic quantum communication with enhanced information capacity.** *Phys. Rev. A*, **59**:1092–1097, Feb 1999. 84
- [54] T. SCHAEZT, M. D. BARRETT, D. LEIBFRIED, J. CHIAVERINI, J. BRITTON, W. M. ITANO, J. D. JOST, C. LANGER, AND D. J. WINELAND. **Quantum Dense Coding with Atomic Qubits.** *Phys. Rev. Lett.*, **93**:040505, Jul 2004. 84
- [55] J.-C. BOILEAU, R. LAFLAMME, M. LAFOREST, AND C. R. MYERS. **Robust Quantum Communication Using a Polarization-Entangled Photon Pair.** *Phys. Rev. Lett.*, **93**:220501, Nov 2004. 84
- [56] BRIAN P. WILLIAMS, RONALD J. SADLER, AND TRAVIS S. HUMBLE. **Superdense Coding over Optical Fiber Links with Complete Bell-State Measurements.** *Phys. Rev. Lett.*, **118**:050501, Feb 2017. 84
- [57] Y. LI, H. ZHU, W. LUO, C. LUO, X. HUANG, H. WU, J. YANG, D. ZHENG, Q. WANG, Y. LU, J. GAO, S. ZHU, M. CAO, K. CHEN, X. YANG, L. CHEN, L. LI, S. YU, S. DUAN, AND K. YU. **Realizing ultrahigh capacity quantum superdense coding on quantum photonic chip.** *npj Quantum Information*, **11**(49), 2025. 84
- [58] XIAO-MIN HU, BI-HENG LIU, YUN-FENG HUANG, CHUAN-FENG LI, AND GUANG-CAN GUO. **Beating the channel capacity limit for superdense coding with entangled ququarts.** *Science Advances*, **4**(7):eaar3900, 2018. 84
- [59] SAGNIK DUTTA, ASMITA BANERJEE, AND PRASANTA K. PANIGRAHI. **Absolutely secure distributed superdense coding: entanglement requirement for optimality.** *Physica Scripta*, **98**(2):025104, 2023. 84
- [60] TRENT GRAHAM, CHRISTOPHER ZEITLER, JOSEPH CHAPMAN, PAUL KWIAT, HAMID JAVADI, AND HERBERT BERNSTEIN. **Superdense teleportation and quantum key distribution for space applications.** In *2015 IEEE International Conference on Space Optical Systems and Applications (ICSOS)*, pages 1–7, 2015. 85
- [61] SYED EMAD UDDIN SHUBHA AND TASNIVA FARHEEN. **Enhancing Quantum Dense Coding Robustness Using Information Entropy-Based Metrics.** arXiv, 2025. 85
- [62] LORENZO VALENTINI, KRISTIAN SKAFTE JENSEN, RENÉ BØDKER CHRISTENSEN, MARCO CHIANI, AND PETAR POPOVSKI. **Quantum Two-Way Protocol Beyond Superdense Coding: Joint Transfer of Data and Entanglement.** *IEEE Transactions on Quantum Engineering*, **6**, 2025. 85
- [63] JOHN F CLAUSER, MICHAEL A HORNE, ABNER SHIMONY, AND RICHARD A HOLT. **Proposed experiment to test local hidden-variable theories.** *Physical Review Letters*, **23**(15):880–884, 1969. 86
- [64] RODRIGO GALLEGO, LARS ERIK WÜRFLINGER, ANTONIO ACÍN, AND MIGUEL NAVASCUÉS. **Operational Framework for Nonlocality.** *Phys. Rev. Lett.*, **109**:070401, Aug 2012. 87, 92
- [65] STEPHANIE WEHNER, DAVID ELKOUSS, AND RONALD HANSON. **Quantum internet: A vision for the road ahead.** *Science*, **362**(6412):1–9, 2018. Accepted Author Manuscript. 87
- [66] SHENG-KAI LIAO, WEN-QI CAI, JOHANNES HANDSTEINER, BO LIU, JUAN YIN, LIANG ZHANG, DOMINIK RAUCH, MATTHIAS FINK, JI-GANG REN, WEI-YUE LIU, YANG LI, QI SHEN, YUAN CAO, FENG-ZHI LI, JIAN-FENG WANG, YONG-MEI HUANG, LEI DENG, TAO XI, LU MA, TAI HU, LI LI, NAI-LE LIU, FRANZ KOIDL, PEIYUAN WANG, YU-AO CHEN, XIANG-BIN WANG, MICHAEL STEINDORFER, GEORG KIRCHNER, CHAO-YANG LU, RONG SHU, RUPERT URSIN, THOMAS SCHEIDL, CHENG-ZHI PENG, JIAN-YU WANG, ANTON ZEILINGER, AND JIAN-WEI PAN. **Satellite-Relayed Intercontinental Quantum Network.** *Phys. Rev. Lett.*, **120**:030501, Jan 2018. 87

- [67] M. ŻUKOWSKI, A. ZEILINGER, M. A. HORNE, AND A. K. EKERT. **“Event-ready-detectors” Bell experiment via entanglement swapping.** *Phys. Rev. Lett.*, **71**:4287–4290, Dec 1993. 87
- [68] SULTAN M ZANGI, CHITRA SHUKLA, ATTA UR RAHMAN, AND BO ZHENG. **Entanglement Swapping and Swapped Entanglement.** *Entropy*, **25**(3):415, 2023. 87
- [69] ZJ LI, YQ HE, D DING, J SONG, T ZHANG, W HUANG, AND H FENG. **(n, m, p)-type quantum network configuration and its nonlocality.** *Quantum Information Processing*, **23**(1):338, 2024. 88
- [70] H. M. WISEMAN, S. J. JONES, AND A. C. DOHERTY. **Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox.** *Phys. Rev. Lett.*, **98**:140402, Apr 2007. 88
- [71] ERWIN SCHRÖDINGER. **Die gegenwärtige Situation in der Quantenmechanik.** *Naturwissenschaften*, **23**:807–812, 1935. 88
- [72] CYRIL BRANCIARD, ERIC G. CAVALCANTI, STEPHEN P. WALBORN, VALERIO SCARANI, AND HOWARD M. WISEMAN. **One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering.** *Phys. Rev. A*, **85**:010301, Jan 2012. 88
- [73] E. G. CAVALCANTI, S. J. JONES, H. M. WISEMAN, AND M. D. REID. **Experimental criteria for steering and the Einstein-Podolsky-Rosen paradox.** *Phys. Rev. A*, **80**:032112, Sep 2009. 88
- [74] D. J. SAUNDERS, S. J. JONES, H. M. WISEMAN, AND G. J. PRYDE. **Experimental EPR-steering using Bell-local states.** *Nature Physics*, **6**:845–849, 2010. 88
- [75] SHUO WANG, YA XIAO, AND YONG-JIAN GU. **Reliable experimental manipulation of quantum steering direction.** *Optics Express*, **31**(10):15886–15894, 2023. 88
- [76] XUE-MEI GU, LIANG HUANG, ALEJANDRO POZAS-KERSTJENS, YANG-FAN JIANG, DIAN WU, BING BAI, QI-CHAO SUN, MING-CHENG CHEN, JUN ZHANG, SIXIA YU, QIANG ZHANG, CHAO-YANG LU, AND JIAN-WEI PAN. **Experimental Full Network Nonlocality with Independent Sources and Strict Locality Constraints.** *Phys. Rev. Lett.*, **130**:190201, May 2023. 92
- [77] SADRA BOREIRI, TAMÁS KRIVÁCHY, PAVEL SEKATSKI, ANTOINE GIRARDIN, AND NICOLAS BRUNNER. **Topologically Robust Quantum Network Nonlocality.** *Phys. Rev. Lett.*, **134**:010202, Jan 2025. 92
- [78] YA-LI MAO, ZHENG-DA LI, ANNA STEFFINLONGO, BIXIANG GUO, BIYAO LIU, SHUFENG XU, NICOLAS GISIN, ARMIN TAVAKOLI, AND JINGYUN FAN. **Recycling nonlocality in quantum star networks.** *Phys. Rev. Res.*, **5**:013104, Feb 2023. 92
- [79] ZINUO CAI AND CHANGLIANG REN. **Full network nonlocality sharing in extended bilocal scenario via weak measurements with the optimal pointer.** *Journal of Physics A: Mathematical and Theoretical*, **57**(19):195302, 2024. 92