

Università degli Studi "Roma Tre"

Department of Science

Dottorato di Ricerca in Scienze della materia e dei
nanomateriali
Cycle XXXVIII°

Quantum metrology beyond
quantum metrology: from
measurements to new
frontiers in quantum
information science

Ph.D. candidate
Gabriele Bizzarri

Supervisor: Prof. Marco Barbieri
Co-supervisor: Prof. Ilaria Gianani

Contents

Introduction	1
1 Photonic quantum information	5
1.1 Discrete variable quantum information	6
1.1.1 The unit of quantum information: the qubit	6
1.1.2 Single-qubit gates	7
1.1.3 Two-qubit gates	10
1.1.4 Density operator formalism	11
1.2 From measurements to information: elements of Quantum Metrology . .	12
1.2.1 Projective measurements	13
1.2.2 Positive-Operator-Valued-Measurements (POVMs)	14
1.2.3 Weak measurements	15
1.2.4 Overview of estimators	16
1.2.5 Single-parameter quantum metrology	18
1.2.6 Multiparameter quantum metrology	20
1.3 Optical platform for quantum information	21
1.3.1 Fock states	23
1.3.2 Quantum information with linear optics	25
1.3.3 Phase estimation via quantum interferometry	29
1.3.4 Spontaneous Parametric Down Conversion (SPDC)	32
2 Metrology-assisted steering certification	35
2.1 From quantum measurements to the EPR paradox	35
2.2 Nonlocal quantum correlations	36
2.2.1 Quantum entanglement	37
2.2.2 Bell non-locality	38
2.2.3 Quantum steering	41
2.2.4 Hierarchy of quantum correlations	42
2.3 Metrology-assisted certification of quantum steering	46
2.3.1 The Yadin-Fadel-Gessner (YFG) approach	47
2.3.2 Working with limited resources	48
2.4 Going experimental	50
2.4.1 C-NOT gate in a Sagnac loop	51
2.4.2 Experimental protocol	52
2.5 Results	54
2.6 Analysis of the robustness of the protocol	57
2.7 Metrology-assisted certification of quantum steering: conclusions	60
3 Secure sensing on networks	61
3.1 Distributed quantum sensing	61
3.1.1 Adding security requirements	62
3.2 Elements of quantum cryptography	62
3.2.1 Mutually Unbiased-Based (MUB) protocols: Bennett-Brassard 1984 (BB84) protocol	63
3.2.2 Entanglement-based protocols: Ekert-1991 (E-91) protocol	65
3.2.3 Quantum cryptography: take-home message	66
3.3 Towards secure DQS	67
3.3.1 The Huang-Machiavello-Maccone (HMM) protocol	68
3.3.2 The Shettell-Kashefi-Markham (SKM) protocol	69
3.4 Faithful and secure phase estimation in a network	72

3.4.1	One-way protocol	72
3.4.2	Experimental test	77
3.4.3	Two-way protocol	78
4	Sloppy behavior in quantum systems	81
4.1	Stiff vs sloppy parameter combinations	81
4.1.1	Sloppiness in quantum systems	82
4.2	Sloppy phase estimation in quantum interferometry	83
4.2.1	Sloppy phase estimation with a tunable weak-measurement	84
4.2.2	Experimental protocol	86
4.2.3	Results	87
	Conclusions	91
	Bibliography	93
	Appendix 1: Quasiprobability distributions with weak measurements	101
	Appendix 2: Experimental protocol for qubit-environment entanglement detection	111

List of Publications

This thesis is based upon the following publications:

1. G. Bizzarri, I. Gianani, M. Manrique, V. Berardi, F. Bruni, G. Capellini, M. Barbieri, *Quantum steering from phase measurements with limited resources*, AVS Quantum Science, 6(2), 024405, 2024, <https://doi.org/10.1116/5.0205469>.
2. G. Bizzarri, I. Gianani, M. Manrique, V. Berardi, F. Bruni, G. Capellini, M. Barbieri, *Finite-size effects in metrology-assisted certification of quantum steering*, Quantum Communications and Quantum Imaging XXII, 13148, 131480E, 2024, <https://doi.org/10.1117/12.3027677>.
3. G. Bizzarri, M. Barbieri, M. Manrique, M. Parisi, F. Bruni, I. Gianani, M. Rosati, *Faithful and secure distributed quantum sensing under general-coherent attacks*, npj Quantum Information 12(33), <https://doi.org/10.1038/s41534-025-01180-0>.
4. G. Bizzarri, M. Parisi, M. Manrique, I. Gianani, A. Chiuri, M. Rosati, V. Giovannetti, M.G.A. Paris, M. Barbieri, *Controlling sloppiness in two-phase estimation with a tunable weak measurement*, Optica Quantum, 3(5), 432–438, 2025, <https://opg.optica.org/opticaq/abstract.cfm?URI=opticaq-3-5-432>.
5. G. Bizzarri, S. Gherardini, M. Manrique, F. Bruni, I. Gianani, M. Barbieri, *Quasiprobability distributions with weak measurements*, Quantum Science and Technology, 10(4), 045008, 2025, <https://doi.org/10.1088/2058-9565/adf573>.
6. G. Bizzarri, L. Sansoni, E. Stefanutti, I. Gianani, M. Barbieri, K. Roszak, A. Chiuri, *Experimental protocol for qubit-environment entanglement detection.*, AVS Quantum Sci. 1 September 2025; 7 (3): 031401, <https://doi.org/10.1116/5.0277965>
7. M. Manrique, M. Barbieri, A. Di Vizio, M. Parisi, G. Bizzarri, I. Gianani, M.G.A. Paris, *Bayesian stepwise estimation of qubit rotations*, arXiv:2512.04898, 2025, <https://arxiv.org/abs/2512.04898>

Introduction

Quantum Mechanics is, without a doubt, one of the major breakthroughs in the history of science, marking a clear watershed with the physics known that far and leading the way for the birth of modern physics. Concepts such as the quantization of energy, the Heisenberg's uncertainty principle and wave-particle duality designed a brand new framework to describe radiation and matter on atomic and subatomic scale, yielding to the so-called *First quantum revolution*. Furthermore, quantum mechanics proved soon to be more than a fundamental theory, featuring an immense predictive capacity and applicability, paving the way for several modern technologies.

Among the first-generation quantum devices, the laser definitely takes its spot: based on the stimulated emission of radiation, predicted by Einstein, it is currently used in a variety of different scenarios, being at the basis of several sensing techniques, as well as in medical surgery, and widely exploited for classical communication. At the same time, the investigation of the quantum properties of electrons led to the creation of diodes, transistors and integrated circuits, paving the way for modern electronics. Nonetheless, electronics is the physical platform behind another fundamental revolution that is still shaping the world around us: the *digital revolution*, represented by computers, smartphones etc.

However, all the devices mentioned above exploit quantum effects at a microscopic, collective scale, with individual quantum systems not being directly assessed. In other words, from the computer science perspective, although the platform works according to the laws of quantum physics, the logic used to encode and process information is fully classical.

Theoretical and technological advancements carried on during the last decades of the XXth and the beginning of the XXIst century allowed the manipulation and control of single quantum systems, setting the stage for the *Second quantum revolution*. Here, differently from the first one, the focus is on the exploitation of peculiar quantum phenomena, such as the superposition principle, quantum coherence and quantum entanglement to encode and process information, implementing, indeed, **a new logic grounded on the quantum nature of matter**. Such a new logic is declined into the modern **Quantum technologies**, grouped in the following main fields, summarized in Fig. 1:

- **Quantum Communication:** Quantum communication relies on the fundamental concepts of quantum mechanics to design communication protocols with security going beyond the standards dictated by classical cryptosystems. Other goal is connecting together quantum devices at different locations, implementing **quantum network** architectures [1];
- **Quantum Computation:** Quantum computing aims at designing quantum processors fully exploiting quantum phenomena, such as state superposition and quantum correlations, to implement algorithms capable of solving problems (almost) unfeasable on classical machines;
- **Quantum Simulation:** Here controllable quantum systems are used to investigate highly complex (both classical and quantum) systems, such as protein structures or the dynamics of many body phenomena, offering a substantial advantage with respect to the most powerful classical devices;
- **Quantum Sensing and Quantum Metrology:** Quantum metrology and sensing rely on quantum states to probe a physical system under exam, achieving estimation performances outperforming any strategy based exclusively on classical resources, as well as designing and building sensor to do so.

All of these disciplines are tightly bounded with the very foundations of quantum mechanics, which offers unvaluable tools for progressively more complex and impactful technological advancements. In turn, technological advancements in the aforementioned fields offer new tool for further investigation of the foundations of quantum theory. Nowadays, a solid expertise on all of the main quantum technologies listed above

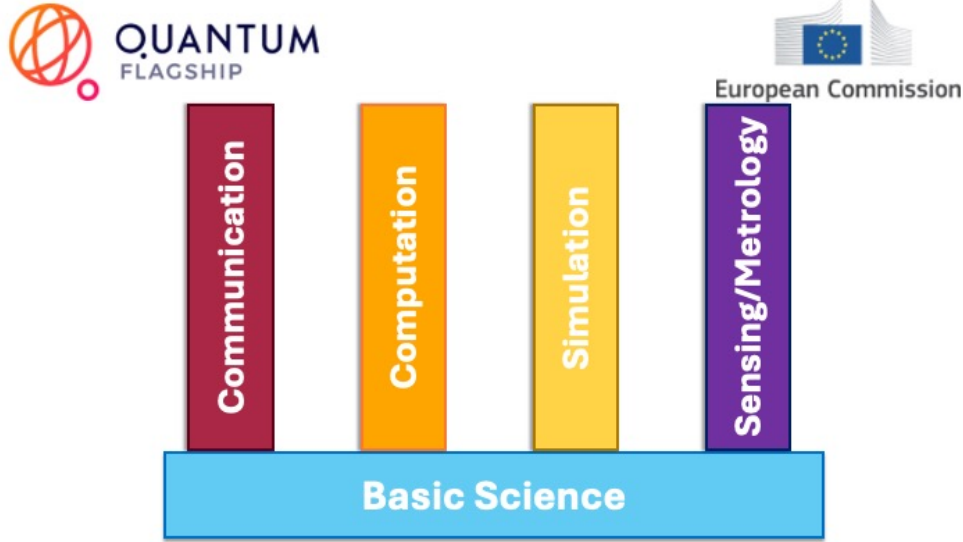


Figure 1: Diagram summarizing the main quantum technologies within the second quantum revolution. Picture inspired and adapted from [2].

has been built, ranging from ground-satellite quantum communication [3], highly re-configurable quantum processors [4], synchronization of atomic clocks [5] and detection of gravitational waves [6].

However, a systematic understanding of the synergies and the interplay among different quantum technologies has been only little explored. Peculiarly, the formulation of common problems among these areas and transferring methods from one field to another one still represent an open challenge, and, at the same time, an unvaluable opportunity to collect new perspectives and achieve cutting-edge results.

In this context, quantum metrology stands as a possibly unifying conceptual framework: originally addressed to assess the ultimate precision limits, imposed by quantum physics, on the estimation of physical parameters, some of its fundamental concepts proved their applicability far beyond the traditional context of measurement it was born for.

This thesis leverages concepts and methods proper of quantum metrology to reformulate and analyze problems belonging to the foundations of quantum mechanics and quantum security, aiming at providing theoretical and experimental paradigms to investigate the new frontiers of quantum information science.

Chapter 1 aims at providing the theoretical background for the works presented in the following chapters. More in detail, the first section 1.1 summarizes the fundamental concepts of quantum information science, such as the notion of *qubit* and the main quantum gates, highlighting the fundamental differences with respect to the classical counterpart. Being physics an experimental science, our knowledge of the physical world unavoidably relies on a (imperfect) measurement process, yielding to an estimate of the physical reality surrounding us, with metrology taking the stage and providing us with the tools to accomplish it in the best way possible. Section 1.2 starts by reviewing the peculiar interpretation quantum mechanics attributes to the measurement process, and reporting the fundamental measurement strategies carried on in quantum experiments. Subsequently, a summary of the most commonly adopted estimators, in both a frequentist and a Bayesian approach, is delivered. The following two subsections 1.2.5 and 1.2.6 provide an overview of the pivotal concepts of single-parameter and multiparameter quantum metrology. A commonly chosen experimental platform to deploy quantum information, photonics stands as a natural testbed for a variety of applications, such as quantum communication, as well as quantum metrology and sensing: subsection 1.3 summarizes the physical toolbox used throughout the experi-

ments discussed in the sequent chapters.

Chapter 2, based on the manuscript [7], addresses the use of quantum metrology as a general framework to certify the presence of a genuine quantum correlation, namely, quantum steering, under the realistic assumptions of noisy probe states and limited resources, particularly relevant for on-site applications to quantum network scenarios. Here, rather than a violation of a properly retrieved inequality holding for unsteerable states, the certification test consists of a statistical test on the significance of the estimation error of an interferometric phase, therefore relying exclusively on the information extracted from experimental data, thus on the metrological power of the probe state. A follow-up, showing the robustness of our protocol against the modelization of the initial information is presented in section 2.6.

Chapter 3 focuses on a state-of-the art problem concerning an estimation task with some security required. A possible example could be the communication of biometrics data, or financial data, encoded in parameters embedded in physical systems, over an untrusted quantum channel, possibly possessed by a malicious user. An alternative setting could be a delegated quantum estimation task, in which a provider shares quantum states across an unsecured quantum network, with each node estimating a parameter meant to be kept confidential from the other users. In section 3.4.1 is reported a one-way protocol, dealing with a provider supplying quantum states to end user, willing to perform the parameter estimation, over an unsecure quantum channel. The proof-of-principle experiment we performed, discussed in 3.4.2, highlights the ability of our protocol of detecting the presence of a potentially malicious user, overestimating, however, their capability of tampering with the shared probe state. Section 3.4.3 concerns the security proof in a two-way protocol, corresponding to a scenario in which one end user has even more limited quantum capabilities, with the probe now traveling back and forth to the provider: allowing the malicious user to act potentially twice during the transmission, the security proof must fulfill more demanding requirements than in the one-way setting. The main reference for the protocols and the security proofs is [8]. Differently, Chapter 4 goes back to a more fundamental metrological aspect, investigating *sloppy* behavior arising in quantum systems. Widely present in complex systems, sloppy models feature only few highly informative combinations (thus retrievable with arbitrarily high precision) of parameters, with others being completely undetermined: only partial information can then be gathered about the system. This behavior can be conveniently reproduced with a quantum two-phase estimation in a linear interferometer. As discussed in [9], the introduction of a tunable weak measurement in between the two parameter encodings enables to counter the sloppiness manifesting in such a setting, allowing experimentalists to retrieve metrological information even when it should be, theoretically speaking, impossible. In addition to its relevance for fundamental quantum metrology, this work promises to host applications outside of quantum metrology as well: due to the reconfigurability degree, the weak measurement technique the method is based upon could be used as a fundamental block for quantum control protocols.

Finally, an appendix contains further works that have resulted from my work. These are not included in the main text for the sake of harmonicity, consistency and focus of this manuscript.

Chapter 1

Photonic quantum information

The first formulation of Quantum Mechanics, developed in the first decades of the XXth century, successfully provided an answer to problems left unsolved by classical physics, such as the description of the black body radiation by Max Planck, or the photoelectric effect by Albert Einstein. Together with special and general relativity, quantum mechanics the birth of modern physics, paving the way for a scientific and technological revolution, known as the **first quantum revolution**, in the sequent decades, aiming at investigating the fundamental properties of quantum systems and their exploitation for technological purposes. This technological revolution is exemplified by two pivotal inventions: the laser and the transistor.

Another theory characterizing the XXth century is certainly information theory: with the fundamental concepts formalized by Alan Turing and Claude E. Shannon, setting the stage for modern computer science, shaping the world evolving in the third millennium. Remarkably, its technological implementation is grounded on the transistor, tightening the bond between computer science and quantum science.

With a more mature comprehension of both quantum mechanics, enabling experimentalists to manipulate the state of single quantum systems, and information theory, in the last decades of the XXth and the beginning of the XXIst centuries a new framework started to be defined: here, quantum mechanics is used not to develop new devices, rather to encode, process and analyze information, giving rise to **quantum information science**. Similarly to what happened at a previous stage, quantum information science led, and is still leading, the **second quantum revolution**, with applications ranging from quantum computing to quantum communication to quantum sensing.

The main element defining quantum information is the **qubit**, i.e. the quantum equivalent of the bit, which allows to define the class of the **discrete-variable (DV) quantum information**, discussed in section 1.1. An insight on the qubit, and the main operation involving a single bit and pair of qubits are discussed in, respectively, sections 1.1.1 to 1.1.3.

A peculiar feature of quantum mechanics is the particular interpretation given to the measurement process and measurement outcome: this is the main matter of section 1.2. This non-trivial trait of quantum mechanics ties it with the science of measurement, giving rise to **quantum metrology**. Its fundamental concepts, are discussed in section 1.2.5, while the extension to a multivariate setting is presented in section 1.2.6.

Among several experimental platforms used to implement quantum technologies, the peculiar properties of photons, such as their weak interaction with the surrounding environment, as well as the possibility of exploiting different degrees of freedom to encode information, make them a definitely valid candidate for quantum technologies, especially quantum communication, as well as metrology. Nonetheless, the quantum theory developed at the beginning of the last century found a natural testbed in electromagnetism and optics, describing phenomena classical models failed to describe, paving the way for the exploration of phenomena in which only few quanta of light are involved: this is the birth of quantum optics, described in section 1.3. The main reference for the section is [10]. Moreover, an insight on the Fock states, also known as *number states* is presented in section 1.3.1. The following paragraph 1.3.2 addresses the main linear optical components used to process quantum information, enabling the

peculiar properties of quantum mechanics to manifest via quantum interference. Furthermore, a distinctive quantum interference effect, known as *Hong-Ou-Mandel (HOM) interference*, named after the scientists who discovered it, is discussed in section 1.3.2. Section 1.3.3 reviews the fundamental problem of quantum phase estimation with linear interferometry, a simple yet insightful example of quantum metrology tasks implemented with photonic platforms. The last subsection of the chapter provides an overview on nonlinear (quantum) optical phenomena, arising whenever multiple electromagnetic fields mutually interact in the matter, giving rise to peculiar effects, namely the *Spontaneous Parametric Down Conversion (SPDC)*, largely used to experimentally generate single photon pairs, lying at the basis of the experiments discussed in the following chapters.

1.1 Discrete variable quantum information

The simplest transposition from classical to quantum information science relies on concepts of quantum mechanics as similar to classical information ones as possible. This is realized by developing a framework with information encoded in distinct, countable quantum state, in which any state is associated with one character of the corresponding classical alphabet. Such a formulation is therefore known as **discrete-variable (DV) quantum information**, and is the most common approach to deal with several problems within the topics of the 2nd quantum revolution, and the one used in the works discussed throughout this thesis.

1.1.1 The unit of quantum information: the qubit

Classical information processed in modern devices relies on a binary alphabet made of two mutually exclusive values (True/False, Yes/No). The unit of information so encoded is therefore called **bit**, whose values are usually labelled as 0 and 1. All the classical information theory is therefore grounded on the rules of the Boole algebra bits must obey.

Similarly, a **quantum bit (qubit for short)** represents the unit of quantum information in the DV formalism. In physical terms, a qubit is represented by a generic two-level system, whose state lives in a two-dimensional Hilbert space $\mathbb{H}_2$. A common choice of states to represent the values 0/1 of a classical bit in such a Hilbert space is

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad (1.1)$$

usually labelled as **computational basis**.

Unlike bits, whose state can be set equal to 0 or 1, the state of a qubit can be represented by an arbitrary superposition of $|0\rangle$ and $|1\rangle$ quantum states:

$$|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle, \quad c_0, c_1 \in \mathbb{C}, \quad (1.2)$$

with $|c_0|^2 + |c_1|^2 = 1$, allowing a (ideally) continuum of possible states to be accessed. The superposition principle (1.2) identifies a peculiar feature of information theory grounded on quantum mechanics, with no classical counterpart. For this reason, it might be tempting to claim that the state of a qubit can be used to store all of the human knowledge. However, a fundamental catch shows up: information about a quantum system can be extracted only by measuring its state, making it unavoidably collapse into one of the states of the computational basis (1.1). The probabilities of such a collapse, thus of retrieving the outcome, respectively, 0 or 1 are given by the celebrated **Born's rule** [11]

$$P_0 = |\langle 0|\psi\rangle|^2 = |c_0|^2 \quad P_1 = |\langle 1|\psi\rangle|^2 = |c_1|^2. \quad (1.3)$$

Interestingly, the dichotomy between the impossibility of observing the superposition states of quantum systems and the actually doable observations is at the heart of the 2nd quantum revolution. In fact, there are operations and mappings whose effects are reflected onto the measurement outcomes, according to the properties of the qubit state. Quantum states have, indeed, real, experimentally verifiable consequences, that are essential to harnessing the power of quantum information and quantum computation [12].

The vector space structure of the Hilbert space $\mathbb{H}_2$ enables other bases to represent the state of a qubit: common choices are

$$\begin{cases} |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{cases} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ \pm 1 \end{pmatrix} \quad \begin{cases} |L\rangle = \frac{|0\rangle+i|1\rangle}{\sqrt{2}} \\ |R\rangle = \frac{|0\rangle-i|1\rangle}{\sqrt{2}} \end{cases} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ \pm i \end{pmatrix}. \quad (1.4)$$

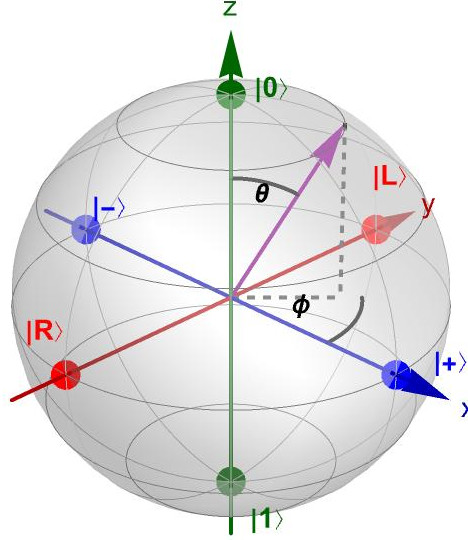


Figure 1.1: Graphical representation of an arbitrary qubit state (1.5), represented by the magenta vector, on the Bloch sphere. The points on the z , x and y axes represent, respectively the states of the computational basis (1.1) and the states of the alternative bases (1.4).

Since quantum states are defined up to a global phase $e^{i\gamma}$, bearing no physical meaning, a general expression for a qubit state is

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\phi} \sin\left(\frac{\theta}{2}\right) |1\rangle, \quad 0 \leq \theta \leq \pi, \quad 0 \leq \phi < 2\pi. \quad (1.5)$$

The numbers θ and ϕ map each superposition state into a point lying on a sphere with radius 1 (due to the normalization condition $|c_0|^2 + |c_1|^2 = 1$), called **Bloch sphere**, providing a graphical representation of the state of a qubit. Nonetheless, basis vectors for the Hilbert space $\mathbb{H}_2$, such as the ones in Eq. (1.4), are identified by points lying at the opposite ends of the sphere with respect to a given axis. Similarly, operations acting on qubits are represented by rotations of the vector identifying the qubit state on the Bloch sphere.

1.1.2 Single-qubit gates

In a classical computer, wires are used to deliver the information (in the form of electric current) across the device, whereas *logic gates* process information encoded in a string of bits. In classical computation, the only non-trivial single-bit operation in the **NOT** (or *bit-flip*) gate, expressed by the truth table 1.1

Moving into the quantum domain, logic operations on qubits, implemented via suitable *quantum gates*, are described via unitary operations $\hat{U}$, i.e. linear operators such that $\hat{U}\hat{U}^\dagger = \hat{U}^\dagger\hat{U} = \mathbb{1}$.

Pauli gates

In quantum information, the class of single-qubit operations is way richer than its classical counterpart. Among these, **Pauli gates** are of fundamental importance. Their

Table 1.1: Truth table for the NOT logic operation.

b	NOT b
0	1
1	0

representation in the computational basis (1.1) is

$$\hat{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \hat{Y} = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \quad \hat{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad (1.6)$$

corresponding to the standard expression of the Pauli matrices $\hat{\sigma}_x$, $\hat{\sigma}_y$ and $\hat{\sigma}_z$.

All of the Pauli gates have eigenvalues $\lambda_{\pm} = \pm 1$, while their eigenstates define bases for the Hilbert space qubit states live in. More specifically, the computational basis (1.1) represents the eigenstates of the Pauli-Z gate, while the other bases (1.4) correspond to the eigenstates of, respectively, Pauli-X and Pauli-Y gates.

Notably, the Pauli-X gate (1.6) represents the NOT operation 1.1 on qubits: $\hat{X}(c_0|0\rangle + c_1|1\rangle) = c_0|1\rangle + c_1|0\rangle$.

The transformations induced by the Pauli gates on a generic qubit state are illustrated in Figs. 1.2a, 1.2b and 1.2c.

Remarkably, the Pauli operators (1.6) have a simple, yet insightful, interpretation in terms of state representation on the Bloch sphere [11]; the expectation value on a generic qubit state (1.5) is

$$\begin{aligned} \langle \psi | \hat{X} | \psi \rangle &= \langle \psi | \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} | \psi \rangle = \sin(\theta) \cos(\phi) = x; \\ \langle \psi | \hat{Y} | \psi \rangle &= \langle \psi | \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} | \psi \rangle = \sin(\theta) \sin(\phi) = y; \\ \langle \psi | \hat{Z} | \psi \rangle &= \langle \psi | \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} | \psi \rangle = \cos(\theta) = z. \end{aligned} \quad (1.7)$$

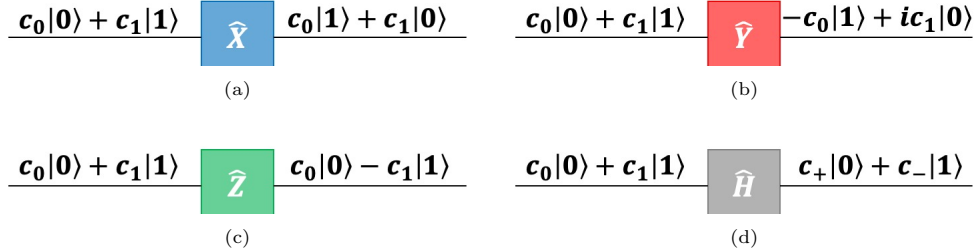


Figure 1.2: Circuit symbol of single-qubit gates: a) Pauli-X gate, b) Pauli-Y gate, c) Pauli-Z gate and d) Hadamard gate. In each of the four panels it is described the effect of the corresponding gate applied to a general qubit state of the form (1.2). The coefficients of the state after the Hadamard gate are $c_{\pm} = \frac{c_0 \pm c_1}{\sqrt{2}}$.

The expectation values (1.7) represent, then, the projections of the qubit state onto the cartesian axes the Bloch sphere is centered with.

Interestingly, Pauli gates are both unitary (so as to describe qubit evolution) and hermitian, i.e. $\hat{U}^\dagger = (\hat{U}^*)^T = \hat{U}$, describing therefore physical observables that can be experimentally measured. For such a reason, Pauli gates find a thriving ground in several quantum information protocols, lying at the basis of more complex operations. More specifically, it is known that the Pauli matrices (1.6), together with the identity matrix (often considered as the zero-Pauli matrix) $\mathbb{1}$, form a basis for the linear space of the 2×2 matrices. As a consequence, any application on a two-dimensional vector space can be expanded as

$$\hat{A} = \alpha_0 \mathbb{1} + \sum_{k=1}^3 \alpha_k \hat{\sigma}_k, \quad (1.8)$$

where $\hat{\sigma}_1 = \hat{X}$, $\hat{\sigma}_2 = \hat{Y}$, $\hat{\sigma}_3 = \hat{Z}$, while the coefficients $\{\alpha_k\}_{k=0}^3$ are generally complex. Hermitian operators can be expanded as in Eq. (1.8), with Pauli matrices now linearly combined with real coefficients.

Hadamard gate

An important, widely used, single-qubit gate is the **Hadamard** gate, represented, in the computational basis (1.1), by the matrix

$$\hat{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad (1.9)$$

whose action on a generic qubit state is depicted in Fig. 1.2d.

Hadamard operation is used to map the computational basis (the eigenstates of the Pauli-Z gate) into the diagonal basis (1.4):

$$\begin{aligned} \hat{H}|0\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle \\ \hat{H}|1\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle. \end{aligned} \quad (1.10)$$

Similarly to the Pauli gates presented in the previous subsection, $\hat{H}^2 = \mathbb{1}$, i.e. $\hat{H}^\dagger = \hat{H}^{-1} = \hat{H}$. As a result, Eqs. (1.10) can be read the other way round. In other words, the Hadamard gate can be used to map back diagonal states into the computational basis. Similarly, Hadamard gate is used to map real Pauli Gates into one another:

$$\begin{aligned} \hat{H}\hat{X}\hat{H} &= \frac{1}{4} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \hat{Z}; \\ \hat{H}\hat{Z}\hat{H} &= \frac{1}{4} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \hat{X}. \end{aligned} \quad (1.11)$$

These latter properties are widely exploited in order to implement more complex operations with few single and two-qubit operations.

Rotation of the Bloch sphere

An other widely used class of single-qubit operations concern the rotation of the Bloch sphere by an angle $0 \leq \delta < 2\pi$ about an arbitrary axis. Rotation gates are described by unitary operations involving an operator $\hat{G}$ such that $\hat{G}^2 = \mathbb{1}$, acting as the **generator** of the aforementioned rotation, and are commonly expressed via the exponential representation of the $SU(2)$ group 2×2 matrices belong to. The general expression is therefore [11, 12]

$$\hat{R}_G(\delta) = e^{-i\hat{G}\frac{\delta}{2}} = \cos\left(\frac{\delta}{2}\right) \mathbb{1} + \sin\left(\frac{\delta}{2}\right) \hat{G}. \quad (1.12)$$

By recalling that the Pauli operators (1.6) span the linear space of 2×2 matrices, the operator $\hat{G}$ can be written as $\hat{G} = \vec{n} \cdot \hat{\sigma}$, where $\hat{\sigma}$ denotes an array whose elements correspond to the Pauli gates, while $\vec{n}$ is a unit vector identifying a axis of the Bloch sphere. Rotations about the Cartesian axes are expressed, but for a global phase shift, as

$$\hat{R}_x(\delta) = \begin{pmatrix} \cos\left(\frac{\delta}{2}\right) & -i\sin\left(\frac{\delta}{2}\right) \\ -i\sin\left(\frac{\delta}{2}\right) & \cos\left(\frac{\delta}{2}\right) \end{pmatrix}, \quad \hat{R}_y(\delta) = \begin{pmatrix} \cos\left(\frac{\delta}{2}\right) & -\sin\left(\frac{\delta}{2}\right) \\ \sin\left(\frac{\delta}{2}\right) & \cos\left(\frac{\delta}{2}\right) \end{pmatrix}, \quad \hat{R}_z(\delta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix}, \quad (1.13)$$

where Eq. (1.12) has been used.

Remarkably, it is easy to verify that $\hat{H} = \frac{\hat{X} + \hat{Z}}{\sqrt{2}} = \hat{R}_{\vec{n}}(\pi)$, i.e. a rotation of the Bloch sphere of a π angle about the axis identified by the vector $\vec{n} = (\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}})$. Equivalently, different bases for the Hilbert space can be mapped into one another via a suitable rotation of the Bloch sphere.

1.1.3 Two-qubit gates

Differently from classical computation, in the quantum world several operations acting on single qubits are available, enabling the possibility of manipulating superposition states, as well as mapping qubit states into an arbitrarily chosen computational basis. Similarly to classical information, scenarios become way richer if more qubits interact with each other: the simplest, yet fundamental for universal quantum computation, class involves the interaction of two qubits via a suitable two-qubit gate. It is known from basic quantum mechanics that the state of composite quantum system lives in the Hilbert space $\mathbb{H}_n = \bigotimes_{i=1}^n \mathbb{H}$: for a two-qubit system the Hilbert space its quantum state lives in has dimension 4 (the Hilbert space of a single qubit has dimension 2. Thus the Hilbert space of a two-qubit system has dimension $2^2 = 4$). A computational basis for such an Hilbert space is given by the tensor product of the basis vectors of the single-qubit computational basis:

$$|0\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |1\rangle = |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |2\rangle = |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |3\rangle = |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \quad (1.14)$$

Likewise the single qubit case, a generic state of a two-qubit system can be decomposed as a linear superposition of the computational basis (1.14).

C-NOT gate and entanglement generation

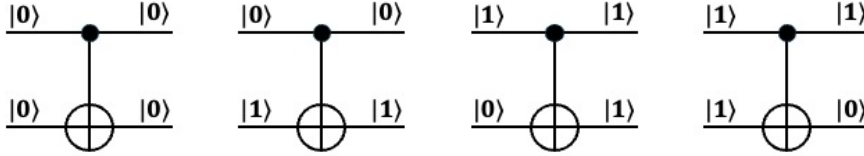


Figure 1.3: Circuitual symbol of the C-NOT gate (1.15). The top line represent the control qubit, whereas the bottom line corresponds to the target qubit. Each panel shows the effect of such a gate on the states of the two-qubit computational basis (1.14).

The prototype of two-qubit gates is the so called *controlled-NOT* (or **C-NOT**). This latter gate couples two input qubits, one used as a *control*, and a second one, the *target*, by applying a XOR operations on the states of the computational basis (1.14): $\hat{U}_{\text{CNOT}}|ij\rangle = |i\rangle|i \oplus j\rangle$, $i, j = 0, 1$. This is an example of *controlled* operations, applying a specific operation on the target according to a given value of the control qubit. The matrix representation of the C-NOT gate is thus

$$\hat{U}_{\text{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad (1.15)$$

and its effect is shown in Fig. 1.3.

Alternatively said, the state of the target qubit is flipped (i.e. a Pauli-X gate is applied) as soon as the state of the control qubit is $|1\rangle$, reason for which it is called **C-X** gate as well. Differently from a classical scenario, C-NOT gate can act on superposition states, enabling the possibility of generating **entangled states**, thoroughly discussed in section 2.2.1. In order to implement such a feature, the control qubit must be in a superposition state: as a matter of example:

$$\hat{U}_{\text{CNOT}}((c_0|0\rangle + c_1|1\rangle) \otimes |1\rangle) = c_0|01\rangle + c_1|10\rangle. \quad (1.16)$$

This latter feature, together with the reversibility granted by the unitary constraint quantum gates obey, make the C-NOT gate a fundamental tool in quantum physics, acting as a building block of other multi-qubit operations, being widely used in several algorithms and protocols.

C-SIGN gate

Controlled gates can be written as the tensor product of a single qubit operation performed on the target qubit and the projector on the qubit state according to which the mapping is implemented. C-NOT gate (1.15) can thus be written as

$$\hat{U}_{\text{CNOT}} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \hat{X}. \quad (1.17)$$

An other controlled gate frequently encountered in quantum algorithms and protocols is the **C-SIGN** gate, applying a π phase to $|11\rangle$ state, i.e. both the control and the target qubit are in the state $|1\rangle$. This behavior arises by applying a Pauli-Z gate to the target qubit whenever the control qubit is in the $|1\rangle$ state:

$$\hat{U}_{\text{CZ}} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \hat{Z} \longrightarrow \hat{U}_{\text{CZ}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad (1.18)$$

where the matrix description is in the computational basis (1.14).

Notably, if the target qubit is in the $\{|\pm\rangle\}$ diagonal basis, then the effect of a C-Z gate is

$$\begin{aligned} \hat{U}_{\text{CZ}} (|1\rangle (c_+ |+\rangle + c_- |-\rangle)) &= |1\rangle \otimes \hat{H} \hat{X} \hat{H} (c_+ |+\rangle + c_- |-\rangle) = \\ &= |1\rangle \otimes \hat{H} \hat{X} (c_+ |0\rangle + c_- |1\rangle) = |1\rangle \otimes \hat{H} (c_+ |1\rangle + c_- |0\rangle) = \\ &= |1\rangle (c_+ |-\rangle + c_- |+\rangle), \end{aligned} \quad (1.19)$$

corresponding to a bit-flip operation conditioned to the control qubit's state set to $|1\rangle$. This result follows from Eq. (1.11): the first Hadamard gate is used to map the $|\pm\rangle$ basis into the computational basis, the standard C-NOT (1.15) is then applied, and the last Hadamard gate maps the state back to the original basis.

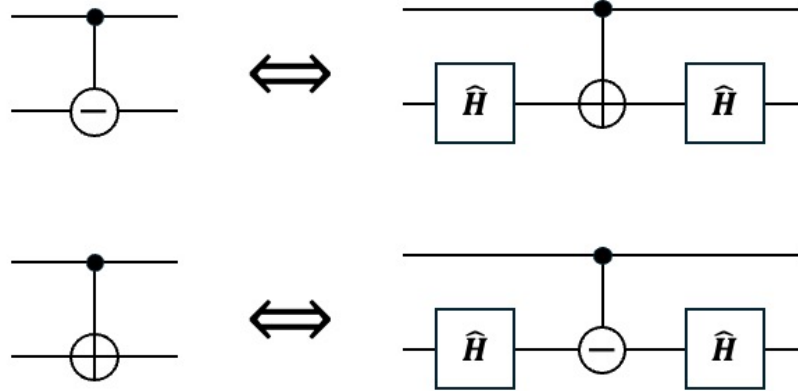


Figure 1.4: Circuitual symbol of the C-SIGN gate (1.18) and its relationship with the C-NOT gate (1.15). The bottom panel represents the inverse expression of the top panel.

As shown in Fig. 1.4, it is possible to express a C-NOT gate as a C-SIGN gate with the target qubit in the $\{|\pm\rangle\}$ basis. In conclusion, C-SIGN and C-NOT gates are the same except for a different encoding of the target qubit, enabling the possibility of implementing the simplest one via a suitable rotation of the target qubit's state. This latter feature is vital for experimental quantum information, since the realization of multiple-qubit operations is usually subject to the specific platform, providing a valuable tool to tackle such complication. Experimental proofs discussed in the next chapters are based exactly on the behavior here discussed.

1.1.4 Density operator formalism

So far we considered the case in which all the replicas of the system could be described by the very same **pure quantum state**, labelled by the ket $|\psi\rangle$. This is hardly the real scenario: in a real setting the quantum system is usually described by a **statistical mixture** of pure states $\{|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle\}$, each appearing with classical probability

$p_i \geq 0$, $1 \leq i \leq n$ such that $\sum_{i=1}^n p_i = 1$.

An alternative formulation of quantum mechanics, encompassing both pure and mixed states involves the so called **density operator**

$$\hat{\rho} = \sum_{i=1}^n p_i |\psi_i\rangle \langle \psi_i|. \quad (1.20)$$

Density operator is characterized by the following properties [12, 13]:

- **It is an hermitian operator:** $\hat{\rho} = \hat{\rho}^\dagger$, thus it can be experimentally characterized;
- **It has unit trace:** $\text{Tr} \hat{\rho} = 1$. This result follows from conservation of total classical probabilities p_i ;
- **It is non negative:** the diagonal terms, representing the population of each pure state of the ensemble, obey the condition $\langle \alpha | \hat{\rho} | \alpha \rangle \geq 0$, $\forall |\alpha\rangle$.

Nonetheless, pure states and statistical mixtures can be distinguished according to the trace of the squared density operator:

$$\text{Tr}(\hat{\rho}^2) \rightarrow \begin{cases} = 1 \iff \text{Pure state;} \\ < 1 \iff \text{Statistical mixture.} \end{cases} \quad (1.21)$$

The density operator formalism provides a simple and effective description of the measurement process, discussed in the next section.

1.2 From measurements to information: elements of Quantum Metrology

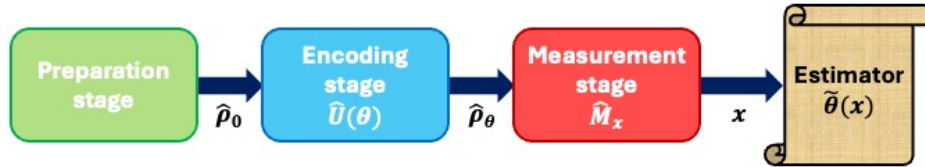


Figure 1.5: Sketch of a generic (quantum) estimation protocol. The probe is initialized into a suitable state $\hat{\rho}_0$ in the preparation stage. Afterwards, the probe interacts with the physical system under exam. As a result, the probe is now described by the state $\hat{\rho}_\theta = \hat{U}(\theta)\hat{\rho}_0\hat{U}^\dagger(\theta)$. Information about the parameter is gathered in the measurement stage, via a properly chosen measurement strategy, involving $\hat{M}_x$ measurement operators. The collection of measurement outcomes $\{x_1, x_2, \dots, x_N\}$ is then used to build up an estimator $\tilde{\theta}$ of the target parameter.

After having discussed the building blocks of quantum information science, this section aims at reviewing the fundamental concepts of quantum metrology, i.e. the science of measurements rooted on quantum mechanics. More specifically, quantum metrology is the discipline aiming at performing the most precise measurements in order to extract information about unknown parameter(s) encoded in the physical system itself.

The general structure of a parameter estimation protocol is presented in Fig. 1.5. Crucially, the metrological probe must be prepared in a parameter-sensitive quantum state, namely, the **probe state**, in order for information on the object parameter to be extracted. As customary, information about it is inferred from experimental results of a properly chosen measurement strategy. Measurement outcomes are then used to construct an **estimator**, i.e. a function $\tilde{\theta} = \tilde{\theta}(x_1, x_2, \dots, x_N)$ of the list of retrieved results, providing an estimate of the value of the unknown parameter. Of course, the choice of a proper measurement strategy and a suitable estimator heavily influences the goodness of the estimation procedure, that is, the possibility of approaching the ultimate precision limits.

More specifically, quantum measurements are described by a set $\{\hat{M}_k\}_k$ of **measurement operators**, one for each possible measurement outcome, acting on the space state of the system under investigation [12].

Remarkably, measurement operators must obey the *completeness* condition

$$\sum_k \hat{M}_k^\dagger \hat{M}_k = \mathbb{1}, \quad (1.22)$$

however, it is not mandatory for them to be orthogonal and/or self-adjoint.

Notably, the probability of the k -th outcome of the measurement (corresponding to the k -th measurement operator) is given by [12, 13]

$$P(k) = \sum_j p_j \langle \psi_j | \hat{M}_k^\dagger \hat{M}_k | \psi_j \rangle = \text{Tr}(\hat{\rho} \hat{M}_k^\dagger \hat{M}_k) \quad \forall k, \quad (1.23)$$

generalizing the Born's rule (1.3).

A milestone of quantum mechanics is the peculiar meaning attributed to the measurement process: as established by the Copenhagen interpretation, the measurement process makes the probe state collapse into one of the eigenstates of the measurement operator, with probabilities given by the Born's rule (1.23). Consequently, the measurement maps the initial state $\hat{\rho}$ into a new state described by a density operator [12, 13]

$$\hat{\rho}' = \sum_j p(j|k) |\psi_j'\rangle \langle \psi_j'| = \sum_j p(j|k) \frac{\hat{M}_k |\psi_j\rangle \langle \psi_j| \hat{M}_k^\dagger}{\langle \psi_j | \hat{M}_k^\dagger \hat{M}_k | \psi_j \rangle}, \quad (1.24)$$

where $p(j|k)$ corresponds to the probability of sorting out the state $|\psi_j'\rangle$ given the k -th measurement outcome. By rewriting the conditioned probability $p(j|k)$ as $p(k|j)p_j/P(k)$ the former equation can be rearranged as [12, 13]

$$\hat{\rho}' = \sum_j p(k|j) \frac{p_j}{P(k)} \frac{\hat{M}_k |\psi_j\rangle \langle \psi_j| \hat{M}_k^\dagger}{\langle \psi_j | \hat{M}_k^\dagger \hat{M}_k | \psi_j \rangle} = \frac{\hat{M}_k \sum_j p_j |\psi_j\rangle \langle \psi_j| \hat{M}_k^\dagger}{\text{Tr}(\hat{\rho} \hat{M}_k^\dagger \hat{M}_k)} = \frac{\hat{M}_k \hat{\rho} \hat{M}_k^\dagger}{\text{Tr}(\hat{\rho} \hat{M}_k^\dagger \hat{M}_k)}, \quad (1.25)$$

where the fact that $\langle \psi_j | \hat{M}_k^\dagger \hat{M}_k | \psi_j \rangle = p(k|j)$ has been used. Remarkably, expression (1.25) concerns only the k -th measurement operator: by considering the whole collection $\{\hat{M}_k\}_k$, it is easy to understand that **the state of a quantum system after a measurement has been performed will be described by a statistical mixture**, regardless the nature of the initial state (pure or mixed).

The measurement operators here discussed obey the completeness condition (1.22) only, with no further requirements. Consequently, they implement the most general measurement strategy. Additional requirements for the measurement operator define more specific measurement strategies, discussed in the following paragraphs.

1.2.1 Projective measurements

The measurement technique most commonly introduced in basic quantum mechanic courses deal with projecting the state of the system onto the eigenstates of the physical observable aimed at estimating: such a class of measurements is therefore known as **projective measurements**.

The measurement operator $\hat{M}_k$ correspond then to the projectors $\hat{\Pi}_k$ onto the eigenspace spanned by the eigenvalues of a given physical observable.

Additional properties of projective measurements are, respectively:

- **Self-adjointness:** $\hat{\Pi}_k^\dagger = \hat{\Pi}_k \quad \forall k$;
- **Orthogonality:** $\hat{\Pi}_k \hat{\Pi}_{k'} = \delta_{kk'} \hat{\Pi}_k \quad \forall k, k'$;
- **Idempotence:** $\hat{\Pi}_k^2 = \hat{\Pi}_k \quad \forall k$.

By employing projective measurement, a generic physical observable $\hat{O}$ admits a *spectral decomposition* as

$$\hat{O} = \sum_k o_k \hat{\Pi}_k = \sum_k o_k |o_k\rangle \langle o_k|, \quad (1.26)$$

where o_k are the possible measurement outcomes. The probability of retrieving the k -th measurement outcome is retrieved according to Eq. (1.23) by replacing $\hat{M}_k \rightarrow \hat{\Pi}_k$. In a projective measurement scheme there is, indeed, a direct connection between the possible measurement outcomes (i.e. the eigenvalues o_k) and the measurement operators $\hat{\Pi}_k$. Following this latter property, projective measurements allow to easily calculate the expectation value of a physical observable:

$$\langle \hat{O} \rangle = \sum_k o_k P(k) = \sum_k o_k \text{Tr}(\hat{\rho} \hat{\Pi}_k) = \text{Tr}(\hat{\rho} \hat{O}) = \sum_j p_j \langle \psi_j | \hat{O} | \psi_j \rangle. \quad (1.27)$$

Physically, the expectation value of the observable is given by the linear combination of the possible measurement outcomes weighted by the corresponding probability, i.e. by the projection of the probe state onto the eigenstates of the observable under test. The variance associated with the observation of $\hat{O}$ is calculated in the very same fashion

$$\Delta^2 O = \langle (\hat{O} - \langle \hat{O} \rangle)^2 \rangle = \langle \hat{O}^2 \rangle - \langle \hat{O} \rangle^2. \quad (1.28)$$

Similarly to the probabilities, the state of the system after a projective measurement is described by the expression (1.25) with $\hat{M}_k \rightarrow \hat{\Pi}_k$. Moreover, if the same observable is measured again the output state will be

$$\hat{\rho}'' = \frac{\hat{\Pi}_k \hat{\rho}' \hat{\Pi}_k}{\text{Tr}(\hat{\Pi}_k \hat{\rho}')} = \frac{\hat{\Pi}_k \hat{\rho} \hat{\Pi}_k}{\text{Tr}(\hat{\Pi}_k \frac{\hat{\Pi}_k \hat{\rho} \hat{\Pi}_k}{\text{Tr}(\hat{\rho} \hat{\Pi}_k)})} = \frac{\hat{\Pi}_k \hat{\rho} \hat{\Pi}_k}{\text{Tr}(\hat{\rho}')} = \hat{\Pi}_k \hat{\rho} \hat{\Pi}_k, \quad (1.29)$$

where the expression (1.25) and the properties of projectors have been used. The second projective measurement does not indeed change the state of the system. Consequently, whenever a projective measurement is implemented, yielding to an outcome o_k with probability $P(k)$, any subsequent measurement of the observable $\hat{O}$ will yield to the same outcome with unit probability. Projective measurements are therefore said to be *repeatable*, and stand as a viable, widely employed choice whenever the measurement process can be repeated an arbitrary number of times under the very same condition [12].

While being a common choice for theoretical models, real scenarios usually prevent repeated measurements from being implemented: a different class of measurement operators, most fitting experimental scenarios, is thus discussed in the next paragraph.

1.2.2 Positive-Operator-Valued-Measurements (POVMs)

As anticipated in the previous paragraph, experimental conditions such as noise affecting the measurement process, as well as imperfection of the detection apparatus make projective measurement not always a viable strategy. Moreover, it may happen that the state of the system after the measurement is of little interest (common in quantum optics experiment). A measurement strategy fitting such requirements is represented by the **Positive-Operator Valued Measurements (POVMs)**, described by measurement operators $\{\hat{E}_k\}_k$ (called *elements of the POVM* associated with the given measurement) such that [12, 13]:

- **Completeness:** $\sum_k \hat{E}_k = \mathbb{1}$;
- **Non-negativity:** $\langle \psi | \hat{E}_k | \psi \rangle \geq 0 \quad \forall |\psi\rangle$.

By means of a simple comparison, it is easy to grasp that, within the formalism discussed in sec. 1.2, POVM elements coincide with $\hat{E}_k = \hat{M}_k^\dagger \hat{M}_k$, $\forall k$. The probability associated with an experimental outcome is therefore

$$P_k = \text{Tr}(\hat{\rho} \hat{E}_k), \quad (1.30)$$

coincident with Eq. (1.23) with $\hat{E}_k = \hat{M}_k^\dagger \hat{M}_k$.

Interestingly, whenever the POVM elements are projectors $\hat{\Pi}_k$, POVM reduces to a projective measurement strategy, enabling the usage of the toolbox discussed in section 1.2.1.

Furthermore, POVMs can be used as a measurement technique for a well defined observable $\hat{O}$: expectation value and variance can be computed, respectively, as [12, 14]:

$$\begin{cases} \langle \hat{O} \rangle_{\text{POVM}} = \sum_k \tilde{o}_k \text{Tr}(\hat{\rho} \hat{E}_k) \\ \Delta^2 O_{\text{POVM}} = \sum_k \tilde{o}_k^2 \text{Tr}(\hat{\rho} \hat{E}_k) - \left(\sum_k \tilde{o}_k \text{Tr}(\hat{\rho} \hat{E}_k) \right)^2. \end{cases} \quad (1.31)$$

These latter expressions mimic Eqs. (1.27) and (1.28); however, a subtle, yet fundamental, difference lies in the definitions in Eq. (1.31). Differently from projective measurements, **the k -th element of the POVM does not correspond to the k -th outcome of the observable $\hat{O}$** . More specifically, coefficients $\tilde{o}_k$ in Eq. (1.31) do not correspond to the eigenvalues of the observable $\hat{O}$. Rather, they refer to the values associated with the possible outcomes of the POVM, which are used to reconstruct the expectation value of $\hat{O}$.

1.2.3 Weak measurements

A widely used class of measurements is that of **weak measurements**, characterized by an arbitrarily weak interaction between the system under investigation and the measurement apparatus. Such a coupling results in a controlled disturbance of the system's state. As a consequence, only partial information can be extracted in a single shot, proportionally to the coupling strength K . Nonetheless, by performing a sufficiently large number of measurements, expectation values can still be inferred.

The common implementation of weak measurements concerns the coupling of the system with an ancillary pointer state via an interaction operator $\hat{U}$ acting on the expanded system+pointer Hilbert space, and then measuring the pointer in a suitable basis.

Here we present a protocol, presented in [15], for the weak measurement of a generic observable $\hat{A} = \sum_{a=0}^{d-1} a |a\rangle \langle a|$, via the coupling of a physical system with dimension d with an ancilla with the same dimensionality. The state of the system is assumed, with no loss of generality, to be described by a pure state $|\psi\rangle$, while the pointer state is labelled as $|\mu\rangle$. System-pointer interaction is implemented by means of the following unitary operator:

$$\hat{U} = \sum_{a=0}^{d-1} \hat{\Pi}_a \otimes \hat{V}^a, \quad \hat{V}^0 = \mathbb{1}, \quad \hat{V} |a\rangle = |a \oplus 1\rangle = |(a+1) \bmod d\rangle, \quad (1.32)$$

where the operator $\hat{V}$ is the so-called *modular increment operator*, shifting each logical state by one position, with periodicity imposed by the dimensionality of the (total) Hilbert space.

Whenever the pointer state is set to $|\mu\rangle = |0\rangle$ the system-pointer coupling yields to the state

$$\hat{U} |\psi\rangle |0\rangle = \sum_{a=0}^{d-1} \hat{\Pi}_a |\psi\rangle \hat{V}^a |0\rangle = \sum_{a=0}^{d-1} c_a |a\rangle |a\rangle. \quad (1.33)$$

A subsequent projective measurement of the pointer state onto the eigenstates of $\hat{A}$ maps the probe state into $|a\rangle$ with probability $|c_a|^2$, implementing, indeed, a projective measurement on the system as well. The completely opposite scenario manifests when the ancilla is prepared in the state $|\mu_0\rangle = \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} |a\rangle$: under such condition

$$\hat{U} |\psi\rangle |\mu_0\rangle = \sum_{a=0}^{d-1} \hat{\Pi}_a |\psi\rangle \otimes \sum_{k=0}^{d-1} \hat{V}^a \frac{|k\rangle}{\sqrt{d}} = \sum_{a=0}^{d-1} \hat{\Pi}_a |\psi\rangle \sum_{k=0}^{d-1} \frac{|k\rangle}{\sqrt{d}} = |\psi\rangle |\mu_0\rangle, \quad (1.34)$$

where the fact that $\hat{V}^a |k\rangle = \hat{V}^{a-1} \hat{V} |k\rangle = \hat{V}^{a-1} |k \oplus 1\rangle$ has been used. Comparing the two sides of Eq. (1.34), we observe whenever the pointer is prepared in a balanced superposition of all eigenstates of $\hat{A}$, the system–pointer coupling vanishes. As a consequence, no measurement of $\hat{A}$ is implemented.

The intermediate case is retrieved by interpolating between the two extremal cases (1.33) and (1.34), by considering a pointer state of the form

$$\begin{aligned} |\mu\rangle &= u_0 |0\rangle + \frac{u_1}{\sqrt{d-1}} \sum_{a=1}^{d-1} |a\rangle = \left(u_0 - \frac{u_1}{\sqrt{d-1}}\right) |0\rangle + \frac{u_1}{\sqrt{d-1}} \sum_{a=0}^{d-1} |a\rangle = \\ &= \left(u_0 - \frac{u_1}{\sqrt{d-1}}\right) |0\rangle + u_1 \sqrt{\frac{d}{d-1}} |\mu_0\rangle = \omega_0 |0\rangle + \omega_1 |\mu_0\rangle, \end{aligned} \quad (1.35)$$

where the coefficients u_0, u_1 , thus ω_0, ω_1 are taken, with no loss of generality, reals. In order for the pointer state (1.35) to be normalized, the following constraints are retrieved:

$$u_0^2 + u_1^2 = 1 \iff \omega_0^2 + \omega_1^2 + \frac{2\omega_0\omega_1}{\sqrt{d}} = 1. \quad (1.36)$$

The measurement operator $\hat{M}_a$ is then calculated, with a pinch of linear algebra, by projecting the coupled pointer onto the eigenstate $|a\rangle$ of $\hat{A}$:

$$\hat{M}_a = \langle a | \hat{U} | \mu \rangle = \omega_0 \langle a | \hat{U} | 0 \rangle + \omega_1 \langle a | \hat{U} | \mu_0 \rangle = \omega_0 \hat{\Pi}_a + \frac{\omega_1}{\sqrt{d}} \mathbb{1}. \quad (1.37)$$

The weak measurement scheme can indeed be implemented by means of a POVM with POVM operator associated with the outcome a given by

$$\hat{E}_a = \hat{M}_a^\dagger \hat{M}_a = \left(\omega_0^2 + \frac{2\omega_0\omega_1}{\sqrt{d}}\right) \hat{\Pi}_a + \frac{\omega_1^2}{d} \mathbb{1} = K \hat{\Pi}_a + \frac{1-K}{d} \mathbb{1}. \quad (1.38)$$

The POVM elements implementing the weak measurement of $\hat{A}$ are described by a linear combination of the standard, projective measurement, and a zero-force measurement. It is therefore possible to define a **strength parameter** K as the coefficient associated with the projective part of the POVM, as stated in the fourth step of Eq. (1.38). By means of simple algebra, the strength parameter K can be expressed in terms of the coefficients ω_0 and ω_1 as $K = \left(\omega_0^2 + \frac{2\omega_0\omega_1}{\sqrt{d}}\right) = 1 - \omega_1^2$. By construction, K takes values in the interval $0 \leq K \leq 1$. Hence, it is clear that as $K \rightarrow 1$ and $K \rightarrow 0$, the weak measurement implemented via the POVM (1.38) reduces to, respectively, Eqs. (1.33) and (1.34), corresponding to the extremal cases of fully projective measurement and no system–pointer coupling. Notably, in the literature the term “*weak measurement*” is often reserved to those acting in the limit $K \rightarrow 0$; here the term is used in a broader sense, indicating generally non projective measurements.

1.2.4 Overview of estimators

As anticipated by Fig. 1.5, the last step of a parameter estimation protocol deals with the construction of a suitable estimator of the unknown parameter, according to a sequence of experimental results $\mathbf{x} = (x_1, x_2, \dots, x_N)$ reflecting the set of possible outcomes $(o_1, o_2, \dots, o_\nu)$, with probabilities depending on the true value of the parameter(s) θ .

The probability of retrieving an experimental outcome x conditioned to the value of the target parameter θ is ruled by the celebrated **likelihood function** $\mathcal{H}(\theta) = P(\mathbf{x}|\theta)$, summarizing the effect of the measurement strategy used to investigate the system. The mapping between the sequence of experimental results and the parameter space is realized by means of an **estimator**, a mathematical function

$$\tilde{\theta} : \mathbf{x} \xrightarrow{f} \tilde{\theta} = \tilde{\theta}(\mathbf{x}) = f(\mathbf{x}) = f(x_1, x_2, \dots, x_n) \quad (1.39)$$

associating a value $\tilde{\theta}$ to the parameter(s) of interest.

Estimators are commonly required to be (**asymptotically**) **unbiased**, meaning that

the expectation value of the estimator corresponds to the true value of the target parameter, possibly in the limit of infinite number of repetitions:

$$\lim_{n \rightarrow +\infty} \tilde{\theta} = \lim_{n \rightarrow +\infty} \mathbb{E}[\tilde{\theta}] = \lim_{n \rightarrow +\infty} \sum_{\mathbf{x}} \tilde{\theta}(\mathbf{x}) P(\mathbf{x}|\theta) = \theta, \quad \forall \theta. \quad (1.40)$$

The quality of a chosen estimator can be quantified by means of several figures of merit, such as the *mean squared error (MSE)*, corresponding to the average squared discrepancy between the estimator and the true value of the parameter:

$$MSE[\tilde{\theta}] = \langle (\tilde{\theta} - \theta)^2 \rangle = \sum_{\mathbf{x}} (\tilde{\theta}(\mathbf{x}) - \theta)^2 P(\mathbf{x}|\theta). \quad (1.41)$$

Nonetheless, the MSE (1.41) can be rearranged as the sum of two distinct terms:

$$MSE[\tilde{\theta}] = \langle (\tilde{\theta} - \theta)^2 \rangle = \langle (\tilde{\theta} - \mathbb{E}[\tilde{\theta}])^2 \rangle + \langle (\mathbb{E}[\tilde{\theta}] - \theta)^2 \rangle, \quad (1.42)$$

the first term of the right-hand side corresponds to the variance of the chosen estimator, while the second one quantifies the (squared) *bias* of the estimation, i.e. the average (squared) discrepancy of the expected value of the estimator with respect to the true value of the parameter, which is, generally, considered inaccessible. Remarkably, in the asymptotic regime, the bias term becomes progressively negligible, with the MSE reducing to the variance of the chosen estimator.

Maximum-likelihood estimator vs Bayesian estimator

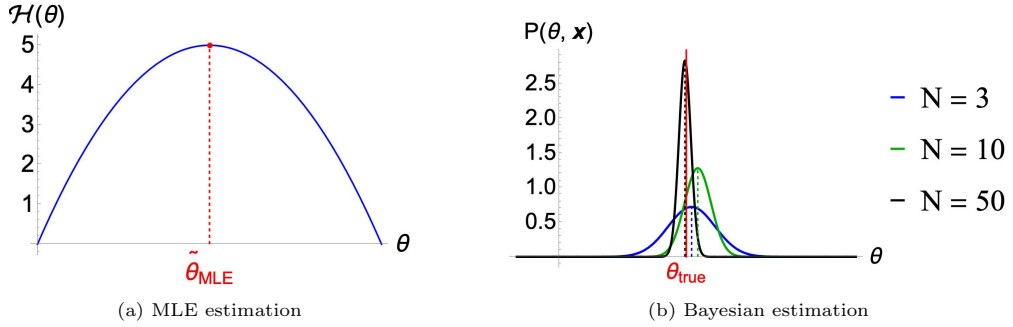


Figure 1.6: Graphical interpretation of estimators. Left panel) Maximum likelihood estimator (MLE): here is presented a plot of the likelihood function $\mathcal{H}$ as a function of the values of the unknown parameter θ . The red point correspond to the maximum value the likelihood function can take, thus to the maximum likelihood estimator (1.43). Right panel) Bayesian estimation: an example of Bayesian estimation with both prior and likelihood function taken as Gaussian distributions. Posterior distribution for different number of observations is plotted as a function of the unknown parameter θ . For each curve, the value of the Bayes estimator (1.45) is identified by a dashed line. The red, continuous line represents the true value of the unknown parameter θ .

A largely employed estimator, strongly tied with the frequentist approach, is the **maximum-likelihood estimator (MLE)**, coincident with the value of θ maximizing the likelihood function describing the measurement strategy [16–19]:

$$\tilde{\theta}_{\text{MLE}} = \arg \max_{\theta} \mathcal{H}(\theta) = \arg \max_{\theta} \prod_{i=1}^N P(\{x_i\}|\theta), \quad (1.43)$$

with the last expression holding for independent experimental runs. A pictorial interpretation is provided in Fig. 1.6a.

Here, the probabilistic nature of the estimator, which is assumed to have a defined yet not known value, is rooted exclusively on the occurrence of experimental results, which are, indeed, random variables.

The diametrically opposite approach considers the target parameter as a random variable itself, with the values it can assume ruled by a suitable *a priori* probability distribution $P_0(\theta)$. A peculiar example of such a class of probabilistic estimators is

represented by the **Bayesian estimator**, relying on the Bayes theorem to update the prior information as more data is collected [16, 17, 20]:

$$P(\theta|\mathbf{x}) = \frac{P(\mathbf{x}|\theta)P_o(\theta)}{\int d\theta P(\mathbf{x}|\theta)P_o(\theta)}. \quad (1.44)$$

The optimal Bayes estimator and its variance are retrieved by optimizing the expected value (calculated with respect to the prior distribution) of the MSE (1.41) with respect to the estimator $\tilde{\theta}$, yielding to:

$$\begin{cases} \tilde{\theta}_{\text{Bayes}} = \int d\theta \theta P(\theta|\mathbf{x}) = \mathbb{E}[\theta]_{P(\theta|\mathbf{x})} \\ \Delta^2 \theta_{\text{Bayes}} = \int d\theta (\theta - \mathbb{E}[\theta]_{P(\theta|\mathbf{x})})^2 P(\theta|\mathbf{x}) \end{cases}; \quad (1.45)$$

coincident with the expected value of the target parameter over the posterior distribution, and the corresponding posterior variance. Nonetheless, central limit theorem ensures that, in the asymptotic limit, the Bayes rule (1.44) updates the posterior distribution $P(\theta|\mathbf{x})$ to a Gaussian distribution with mean and variance given by Eq. (1.45). A graphical interpretation is reported in Fig. 1.6b.

1.2.5 Single-parameter quantum metrology

The unavoidable uncertainty characterizing any measurement process can have two distinct natures, namely:

- **Technical:** mainly represented by accidental errors, due to out-of-control imperfections manifesting during the measurement process;
- **Fundamental:** uncertainty arises from ultimate theoretical limits, dictated by the laws of physics.

Concerning this latter source of uncertainty, metrology aims at retrieving the ultimate precision limits a certain measurement strategy can achieve, compatibly with the fundamental laws of physics.

For a given set of measurements and fixed probes, the amount of information (in the form of estimation accuracy) that can be extracted about an unknown parameter is governed by the likelihood function. More thoroughly, for each experimental result x_i , $i = 1, \dots, N$, accuracy of the parameter's estimate is governed by the degree to which the likelihood function $P(x_i|\theta)$ is clustered around the true value of θ . In other words, higher estimation precision is attained as the discrepancy between the observed outcome and the true value of the parameter decreases.

The maximal amount of information about the unknown parameter θ that can be extracted from a measurement protocol is captured by the **(Classical) Fisher Information (CFI)** [21], defined as:

$$f(\theta) = \sum_{\mathbf{x}} P(\mathbf{x}|\theta) \left(\frac{\partial \ln P(\mathbf{x}|\theta)}{\partial \theta} \right)^2 = \sum_{\mathbf{x}} \frac{(\partial_{\theta} P(\mathbf{x}|\theta))^2}{P(\mathbf{x}|\theta)}. \quad (1.46)$$

Moreover, the capability of the Fisher information of quantifying the sensitivity of the likelihood function, thus the probing system's, with respect to the value of θ is mathematically formalized by the celebrated **Cramér-Rao bound (CRB)** [22, 23]

$$\Delta^2 \tilde{\theta} \geq \frac{1}{N f(\theta)}, \quad (1.47)$$

ensuring that the variance on the unknown parameter given by an asymptotically unbiased estimator follows the $\mathcal{O}(N^{-1})$ trend resulting, again, from the central limit theorem; for this reason it is called **Standard Quantum Limit (SQL)**.

Quantum mechanics takes his spot in metrology

When dealing with quantum probes, the probabilities $P(x|\theta)$ are calculated according to Born's rule (1.23); however, no further quantum feature have been accounted for. Crucially, as discussed in section 1.2, several choices of measurement strategies are viable, as well as different possible estimators. A further step is therefore needed: the optimal estimator will be thus determined not only by attaining the highest precision in inferring the value of the parameter from the collected data, rather it will also require the most suitable measurement scheme for the given task, out of all the possible measurement strategies. Such an optimization over all the viable measurement schemes yields to the so called **Quantum Fisher Information (QFI)**, directly connected, similarly to the classical case, to a corresponding **Quantum Cramér-Rao bound (QCRB)** [16, 17, 24, 25].

In order for the QFI and QCRB to be formally defined, it is noteworthy to introduce the *symetric logarithmic derivative (SLD)* operator $\hat{L}(\theta)$, obeying the following equation [26] :

$$\frac{\partial \hat{\rho}(\theta)}{\partial \theta} = \frac{\hat{L}(\theta)\hat{\rho}(\theta) + \hat{\rho}(\theta)\hat{L}(\theta)}{2} \quad (1.48)$$

first proposed by C.W. Helstrom in [27].

By using the Born's rule (1.23) for the conditional probabilities $P(x|\theta)$ it is possible to write the CFI (1.46) in terms of the SLD operator (1.48):

$$f(\theta) = \sum_{\mathbf{x}} \frac{1}{P(\mathbf{x}|\theta)} \left(\frac{\partial P(\mathbf{x}|\theta)}{\partial \theta} \right)^2 = \sum_{\mathbf{x}} \frac{\left(\text{Re} \left[\hat{\rho}(\theta) \hat{L}(\theta) \hat{E}_x \right] \right)^2}{\text{Tr} \left(\hat{\rho}(\theta) \hat{E}_x \right)}, \quad (1.49)$$

setting the ultimate precision bound for the chosen measurement setting. By optimizing over all the possible quantum measurements the QFI is defined:

$$f_Q[\hat{\rho}(\theta)] = \max_{\hat{E}_x} f(\theta). \quad (1.50)$$

By exploiting the Schwarz inequality $\left| \text{Tr} \left(\hat{A}^\dagger \hat{B} \right) \right|^2 \leq \text{Tr} \left(\hat{A}^\dagger \hat{A} \right) \text{Tr} \left(\hat{B}^\dagger \hat{B} \right)$, an alternative expression for the QFI is retrieved [26]:

$$f(\theta) \leq \sum_{\mathbf{x}} \left| \frac{\text{Tr} \left(\hat{\rho}(\theta) \hat{L}(\theta) \hat{E}_x \right)}{\sqrt{\text{Tr} \left(\hat{\rho}(\theta) \hat{E}_x \right)}} \right|^2 = \text{Tr} \left(\hat{\rho}(\theta) \hat{L}(\theta) \right) = f_Q[\hat{\rho}(\theta)], \quad (1.51)$$

where $\hat{A}_x = \sqrt{\hat{E}_x \hat{\rho}(\theta)}$ and $\hat{B}_x = \sqrt{\hat{E}_x \hat{\rho}(\theta) \hat{L}(\theta)}$. The inequality is saturated as soon as the POVM projects onto the eigenstates of the SLD. The introduction, and the definition, of the QFI defines as well the *Quantum Cramér-Rao bound* [14], as

$$\Delta^2 \tilde{\theta} \geq \frac{1}{N f(\theta)} \geq \frac{1}{N f_Q[\hat{\rho}(\theta)]} = \Delta_{\min}^2 \tilde{\theta}, \quad (1.52)$$

which is, of course, independent on the choice of the measurement, and figures as the very ultimate precision limit attainable in a parameter estimation experiment in the asymptotic limit of large N .

QFI for a pure state

Under the assumption of pure probe states, the SLD, thus the QFI, is expressed by a simple formula: the parameter-encoded density operator will be written as:

$$\hat{\rho}(\theta) = \hat{U}(\theta) |\psi_0\rangle \langle \psi_0| \hat{U}^\dagger(\theta) = |\psi_\theta\rangle \langle \psi_\theta|. \quad (1.53)$$

The derivative of Eq. (1.53) is thus

$$\frac{\partial \hat{\rho}(\theta)}{\partial \theta} = |\partial_\theta \psi_\theta\rangle \langle \psi_\theta| + |\psi_\theta\rangle \langle \partial_\theta \psi_\theta| = \hat{\rho}(\theta) \frac{\partial \hat{\rho}(\theta)}{\partial \theta} + \frac{\partial \hat{\rho}(\theta)}{\partial \theta} \hat{\rho}(\theta). \quad (1.54)$$

By combining Eq. (1.48) with Eq. (1.54) the following expression of the SLD is retrieved:

$$\hat{L}(\theta) = 2 \frac{\partial \hat{\rho}(\theta)}{\partial \theta} = 2(|\partial_\theta \psi_\theta\rangle \langle \psi_\theta| + |\psi_\theta\rangle \langle \partial_\theta \psi_\theta|). \quad (1.55)$$

In conclusion, by inserting the expression (1.55) into (1.50), the following expression of the QFI is retrieved:

$$f_Q[|\psi_\theta\rangle] = 4(\langle \partial_\theta \psi_\theta | \partial_\theta \psi_\theta \rangle - |\langle \psi_\theta | \partial_\theta \psi_\theta \rangle|^2) = 4\Delta^2 G, \quad (1.56)$$

where the right end side holds for unitary parameter encoding $\hat{U}(\theta) = e^{-i\hat{G}\theta}$ generated by the observable $\hat{G}$.

1.2.6 Multiparameter quantum metrology

So far it was considered the problem concerning only one object parameter aimed at being estimated. However, there are scenarios in which more than one parameter are matter of interest. On the same page, some conditions prevent a parameter of interest from being directly estimated, commonly due to its dependency on other parameters. Nonetheless, in some pictures, estimating more than parameter yields to improved performances compared to single parameter estimation [28]. All of these scenario mark the necessity of **multiparameter (quantum) metrology**, supplying tools and techniques to be used whenever multiple parameters have to be estimated at once.

In such a framework, the main concepts introduced in section 1.2.5 must be adapted in order to account for the presence of more than one parameter and the possible dependencies on one another. Looking back at Eq. (1.46), it is clear that the CFI is proportional to $f(\theta) \propto \partial_\theta P(\mathbf{x}|\theta) \partial_\theta P(\mathbf{x}|\theta)$. Whenever p different parameters $\boldsymbol{\theta} = (\theta_1, \theta_2, \dots, \theta_p)$ are concerned, the aforementioned proportionality holds for any pair of parameters. CFI is therefore mapped into a **(Classical) Fisher Information matrix (CFIM)** [24, 25]:

$$F_{\alpha\beta}(\theta) = \sum_{\mathbf{x}} \frac{1}{P(\mathbf{x}|\boldsymbol{\theta})} \frac{\partial P(\mathbf{x}|\boldsymbol{\theta})}{\partial \theta_\alpha} \frac{\partial P(\mathbf{x}|\boldsymbol{\theta})}{\partial \theta_\beta}, \quad \forall \alpha, \beta = 1, \dots, p; \quad (1.57)$$

where $P(\mathbf{x}|\boldsymbol{\theta})$ represents the probability of retrieving a sequence $\mathbf{x}$ of experimental outcomes conditioned to a specific set of values $\boldsymbol{\theta}$ of the unknown parameters. Remarkably, the diagonal terms of the CFIM (1.57) correspond to the Fisher information on the individual p parameters. Like the single parameter picture, CFIM is tied to the (multiparameter) Cramér-Rao bound, now reading as a matrix inequality:

$$\Sigma(\tilde{\boldsymbol{\theta}}) \geq \frac{F^{-1}(\boldsymbol{\theta})}{N}; \quad (1.58)$$

where Σ denotes the covariance matrix of all the estimators $\tilde{\boldsymbol{\theta}} = (\tilde{\theta}_1, \dots, \tilde{\theta}_p)$, while $F^{-1}(\boldsymbol{\theta})$ is the inverse FIM.

The diagonal terms of Eq. (1.58) impose then a lower bound on the accuracy of the estimation of each parameter; correspondingly, the off-diagonal terms provide a lower bound on the correlations among each pair of parameters.

Similarly to the Fisher Information, the QFI (1.51) is promoted to a **Quantum Fisher Information matrix (QFIM)** [29]:

$$(F_Q)_{\alpha\beta}[\hat{\rho}(\boldsymbol{\theta})] = \text{Tr} \left(\hat{\rho}(\boldsymbol{\theta}) \frac{\hat{L}_\alpha \hat{L}_\beta + \hat{L}_\beta \hat{L}_\alpha}{2} \right), \quad \alpha, \beta = 1, \dots, N, \quad (1.59)$$

with each SLD operator being defined as $\frac{\partial \hat{\rho}(\boldsymbol{\theta})}{\partial \theta_\alpha} = (\hat{\rho}(\boldsymbol{\theta}) \hat{L}_\alpha + \hat{L}_\alpha \hat{\rho}(\boldsymbol{\theta}))/2$.

On the very same page as the single parameter's QFIM is involved into the definition of a **multiparameter quantum Cramér-Rao bound**, a matrix inequality

$$\Sigma_{\alpha\beta} \geq \frac{(F^{-1}(\boldsymbol{\theta}))_{\alpha\beta}}{N} \geq \frac{(F_Q^{-1}[\hat{\rho}(\boldsymbol{\theta}))]_{\alpha\beta}}{N}. \quad (1.60)$$

However, unlike the single-parameter scenario, the multiparameter QCRB is not always attainable for all the parameters simultaneously [30–32]. Rather, a necessary condition for the multiparameter QCRB to be saturated is

$$\text{Tr} \left(\left[\hat{L}_\alpha, \hat{L}_\beta \right] \hat{\rho}(\boldsymbol{\theta}) \right) = 0, \quad \forall \alpha, \beta = 1, \dots, p. \quad (1.61)$$

This latter constraint corresponds to requiring compatible optimal measurements for the individual parameters, condition not always met [30].

In conclusion, multiparameter quantum metrology is, therefore, significantly different from the single parameter scenario, both in terms of the choice of the measurement strategy [30, 33], as well as of the arrangement of physical resources for the estimation scheme [28, 34].

1.3 Optical platform for quantum information

Classical electromagnetism, formalized by J.C. Maxwell in the latter XIX century [35], succeeded in describing the wave propagation of electromagnetic field, proving that visible light is just a specific case of electromagnetic radiation.

All electromagnetic phenomena are summarized by the Maxwell's equations, which, in absence of external sources, are written, in CGS-Gaussian units, as

$$\left\{ \begin{array}{l} \vec{\nabla} \cdot \vec{E}(\vec{r}, t) = \vec{\nabla} \cdot \vec{B}(\vec{r}, t) = 0 \\ \vec{\nabla} \times \vec{E}(\vec{r}, t) = -\frac{1}{c} \frac{\partial \vec{B}(\vec{r}, t)}{\partial t} \\ \vec{\nabla} \times \vec{B}(\vec{r}, t) = \frac{1}{c} \frac{\partial \vec{E}(\vec{r}, t)}{\partial t}, \end{array} \right. \quad (1.62)$$

where c is the speed of light in the vacuum¹. Moreover, by expressing the electric and magnetic field via suitable, respectively, scalar and vector potentials [10, 36]

$$\left\{ \begin{array}{l} \vec{E}(\vec{r}, t) = -\vec{\nabla} \phi(\vec{r}, t) - \frac{1}{c} \frac{\partial \vec{A}(\vec{r}, t)}{\partial t} \\ \vec{B}(\vec{r}, t) = \vec{\nabla} \times \vec{A}(\vec{r}, t), \end{array} \right. \quad (1.63)$$

where the Coulomb gauge (consisting of requiring a solenoidal vector potential) has been used, Eqs. (1.62) can be mapped into [10]

$$\nabla^2 \phi(\vec{r}, t) = 0, \quad \nabla^2 \vec{A}(\vec{r}, t) - \frac{1}{c^2} \frac{\partial^2 \vec{A}(\vec{r}, t)}{\partial t^2} = 0. \quad (1.64)$$

Remarkably, the equation for the vector potential in (1.63) is nothing but D'Alembert wave equation; vector potential admits thus, by imposing proper periodic boundary conditions, a Fourier expansion on the form [10, 36]

$$\vec{A}(\vec{r}, t) = \sum_{\vec{k}} \sum_{\lambda} \left(\vec{A}_{\vec{k}\lambda} e^{i(\vec{k} \cdot \vec{r} - \omega_{\vec{k}} t)} + \vec{A}_{-\vec{k}\lambda} e^{-i(\vec{k} \cdot \vec{r} - \omega_{\vec{k}} t)} \right), \quad (1.65)$$

where λ denotes two orthogonal polarization states. Nonetheless, the equality $\vec{A}_{-\vec{k}\lambda} = \vec{A}_{\vec{k}\lambda}^*$ must hold for the vector potential to be real valued; while periodic boundary conditions impose that the wave vectors $\vec{k}$ are discretized as $\vec{k}_n = \frac{(2\pi)^3}{L^3} (n_x, n_y, n_z)$, with $n_x, n_y, n_z \in \mathbb{Z}$. Furthermore, the Coulomb gauge condition $\vec{\nabla} \cdot \vec{A} = 0$ and periodic boundary conditions provide additional conditions, namely

$$\vec{k} \cdot \vec{A}_{\vec{k}\lambda} = 0, \quad \omega_{\vec{k}}^2 = c^2 |\vec{k}|^2, \quad (1.66)$$

¹ $c = 299\,792\,458 \text{ m s}^{-1} \simeq 3 \times 10^8 \text{ m s}^{-1}$

where the first equality ensures that $\vec{A}_{\vec{k}\lambda}$ properly identifies a polarization vector, whereas the second one is the celebrated *dispersion law*. Indeed, by combining Eqs. (1.63) and (1.65) the Fourier expansion for both the electric and magnetic fields is retrieved [10, 36]

$$\begin{cases} \vec{E}(\vec{r}, t) = \sum_{\vec{k}} \sum_{\lambda} \frac{i\omega_{\vec{k}}}{c} \left(\vec{A}_{\vec{k}\lambda} e^{i(\vec{k}\cdot\vec{r} - \omega_{\vec{k}}t)} - \vec{A}_{-\vec{k}\lambda} e^{-i(\vec{k}\cdot\vec{r} - \omega_{\vec{k}}t)} \right) \\ \vec{B}(\vec{r}, t) = \sum_{\vec{k}} \sum_{\lambda} i\vec{k} \times \left(\vec{A}_{\vec{k}\lambda} e^{i(\vec{k}\cdot\vec{r} - \omega_{\vec{k}}t)} - \vec{A}_{-\vec{k}\lambda} e^{-i(\vec{k}\cdot\vec{r} - \omega_{\vec{k}}t)} \right). \end{cases} \quad (1.67)$$

Notably, the pairs $(\vec{k}, \lambda)$ identify the **modes** of the electromagnetic field, i.e. the wavelengths and the oscillation direction of the stationary waves lying within the volume $V = L^3$ considered by the periodic boundary conditions.

The energy of the electromagnetic field stored in the volume V is therefore given by [10, 37]

$$\begin{aligned} \mathcal{H} &= \int_V \frac{d^3r}{8\pi^3} \left(|\vec{E}(\vec{r}, t)|^2 + |\vec{B}(\vec{r}, t)|^2 \right) = \frac{V}{4\pi} \sum_{\vec{k}} \sum_{\lambda} \left(k^2 + \frac{\omega_{\vec{k}\lambda}^2}{c^2} \right) \vec{A}_{\vec{k}\lambda} \cdot \vec{A}_{-\vec{k}\lambda} = \\ &= \sum_{\vec{k}} \sum_{\lambda} \mathcal{E}_{\vec{k}\lambda} = \sum_{\vec{k}} \sum_{\lambda} \left(\frac{P_{\vec{k}\lambda}^2}{2} + \frac{\omega_{\vec{k}\lambda}^2}{2} Q_{\vec{k}\lambda}^2 \right), \end{aligned} \quad (1.68)$$

where the Fourier representation (1.67) of the electric and magnetic fields has been used, and $Q_{\vec{k}\lambda}^2 = \frac{V}{2\pi c^2} \vec{A}_{\vec{k}\lambda} \cdot \vec{A}_{-\vec{k}\lambda}$ and $P_{\vec{k}\lambda}^2 = \frac{Vk^2}{2\pi} \vec{A}_{\vec{k}\lambda} \cdot \vec{A}_{-\vec{k}\lambda}$.

From the right hand side of Eq. (1.68) is clear that each mode of the electromagnetic field is described by an harmonic oscillator with frequency $\omega_{\vec{k}\lambda}$, with the coefficients $P_{\vec{k}\lambda}$ and $Q_{\vec{k}\lambda}$ playing the role of, respectively, momentum and position generalized coordinates. Thus, the quantum description of the electromagnetic field is retrieved by imposing the formalism of the quantum harmonic oscillator to each cavity mode. This can be done by considering the position-like and the momentum-like terms as operators, and expressing them in term of creation $\hat{a}_{\vec{k}\lambda}^\dagger$ and annihilation operators $\hat{a}_{\vec{k}\lambda}$ as

$$\hat{P}_{\vec{k}\lambda} = i\sqrt{\frac{\hbar\omega_{\vec{k}}}{2}}(\hat{a}_{\vec{k}\lambda}^\dagger - \hat{a}_{\vec{k}\lambda}), \quad \hat{Q}_{\vec{k}\lambda} = \sqrt{\frac{\hbar}{2\omega_{\vec{k}\lambda}}}(\hat{a}_{\vec{k}\lambda}^\dagger + \hat{a}_{\vec{k}\lambda}), \quad (1.69)$$

such that the fundamental commutation rules

$$\left[\hat{Q}_{\vec{k}\lambda}, \hat{P}_{\vec{q}\lambda'} \right] = i\hbar\delta_{\vec{k}\vec{q}}\delta_{\lambda\lambda'} \leftrightarrow \begin{cases} \left[\hat{a}_{\vec{k}\lambda}, \hat{a}_{\vec{q}\lambda'}^\dagger \right] = \delta_{\vec{k}\vec{q}}\delta_{\lambda\lambda'} \\ \left[\hat{a}_{\vec{k}\lambda}, \hat{a}_{\vec{q}\lambda'} \right] = \left[\hat{a}_{\vec{k}\lambda}^\dagger, \hat{a}_{\vec{q}\lambda'}^\dagger \right] = 0 \end{cases} \quad (1.70)$$

of the harmonic oscillator are satisfied. Creation/annihilation operators associated with different modes of the electromagnetic field act on different subspaces of the total Hilbert state, called **Fock space** (or, alternatively, **occupation number space**), label clarified in the next paragraph. It is, indeed, possible to focus on single-mode states, and then recombine all together, retrieving the multi-mode state as the tensor product of the single-mode ones, over all the allowed modes.

The energy of the electromagnetic field stored in a volume V (1.68) is therefore described by the following Hamiltonian operator

$$\hat{\mathcal{H}} = \sum_{\vec{k}} \sum_{\lambda} \hbar\omega_{\vec{k}} \left(\hat{a}_{\vec{k}\lambda}^\dagger \hat{a}_{\vec{k}\lambda} + \frac{1}{2} \right). \quad (1.71)$$

The definition of position and momentum-like operators (thus, of the creation/annihilation operators) (1.69) allows to retrieve an expression for the Hamiltonian operators associated with the electric and magnetic fields (1.67) [10]:

$$\begin{cases} \hat{\vec{E}}(\vec{r}, t) = \sum_{\vec{k}} \sum_{\lambda} \sqrt{\frac{2\pi\hbar\omega_{\vec{k}}}{V}} \vec{u}_{\vec{k}\lambda} \left(\hat{a}_{\vec{k}\lambda} e^{-i\chi_{\vec{k}}(\vec{r}, t)} + \hat{a}_{\vec{k}\lambda}^\dagger e^{i\chi_{\vec{k}}(\vec{r}, t)} \right) \\ \hat{\vec{B}}(\vec{r}, t) = \sum_{\vec{k}} \sum_{\lambda} \sqrt{\frac{2\pi\hbar c^2}{\omega_{\vec{k}}V}} \vec{k} \times \vec{u}_{\vec{k}\lambda} \left(\hat{a}_{\vec{k}\lambda} e^{-i\chi_{\vec{k}}(\vec{r}, t)} + \hat{a}_{\vec{k}\lambda}^\dagger e^{i\chi_{\vec{k}}(\vec{r}, t)} \right), \end{cases} \quad (1.72)$$

where $\vec{u}$ denotes a normalized, real-valued² polarization vector, whereas the phase term is $\chi_{\vec{k}}(\vec{r}, t) = \omega_{\vec{k}}t - \vec{k} \cdot \vec{r} - \pi/2$. Nonetheless, the commutation rules (1.70) enable, for each mode (the indices are, for the sake of brevity, dropped) an alternative description involving the so-called **quadrature operators**

$$\hat{X} = \frac{\hat{a}^\dagger + \hat{a}}{2}, \quad \hat{Y} = \frac{\hat{a}^\dagger - \hat{a}}{2} \quad (1.73)$$

the continuous-variable quantum information (CV-QI), not discussed here, is grounded upon.

The commutation rules (1.70) are translated, in the quadrature-operator formalism, into [10]

$$[\hat{X}, \hat{Y}] = \frac{i}{2}, \quad [\hat{X}, \hat{X}] = [\hat{Y}, \hat{Y}] = 0. \quad (1.74)$$

Similarly, it is possible to rewrite the Hamiltonian operator (1.71) and the electric field of each mode in terms of the quadrature operators as [10]

$$\begin{aligned} \hat{\mathcal{H}} &= \hbar\omega \left(\hat{a}^\dagger \hat{a} + \frac{1}{2} \right) = \hbar\omega \left(\hat{X}^2 + \hat{Y}^2 \right); \\ \hat{E}(\chi) &= \hat{u} \left(\hat{X} \cos(\chi) + \hat{Y} \sin(\chi) \right), \end{aligned} \quad (1.75)$$

where the electric field has been taken in units of $\sqrt{(2\pi\hbar\omega)/V}$.

In conclusion, quadrature-operator description of the states of the quantum electromagnetic field, additionally to being fundamental for the CV picture, is used to gather relevant information about their statistical nature, as well as providing a graphical interpretation of the quantum states themselves, in a Gauss-like plane.

1.3.1 Fock states

The simplest state of the quantized electromagnetic field are those identified by the *occupation numbers*, i.e. the number of quanta in each mode, also known as, after this feature, as **number states**, or **Fock states**:

$$|\{n\}\rangle = |n_{\vec{k}_1\lambda_1}\rangle \cdots |n_{\vec{k}_n\lambda_n}\rangle = \bigotimes_{\vec{k}\lambda} |n_{\vec{k}\lambda}\rangle_{\vec{k}\lambda}. \quad (1.76)$$

A particularly important case is the **vacuum state**, i.e. the Fock state in which no mode is populated:

$$|\{0\}\rangle = \bigotimes_{\vec{k}\lambda} |0\rangle_{\vec{k}\lambda}. \quad (1.77)$$

The annihilation and creation operators act on Fock states according to

$$\hat{a} |n\rangle = \sqrt{n} |n-1\rangle, \quad \hat{a}^\dagger |n\rangle = \sqrt{n+1} |n+1\rangle, \quad (1.78)$$

thereby decreasing and increasing the occupation number by one quantum, respectively. The state of a photon with momentum $\vec{k}$ and polarization λ will be described by the Fock state $|1\rangle_{\vec{k}\lambda} = |\vec{k}\rangle_\lambda$.

Following from (1.78), a generic, multi-mode Fock state can be generated by iteratively adding with proper momentum and polarization [10]:

$$|\{n\}\rangle = \bigotimes_{\vec{k}\lambda} \frac{(\hat{a}_{\vec{k}\lambda}^\dagger)^n}{\sqrt{n_{\vec{k}\lambda}}} |\{0\}\rangle. \quad (1.79)$$

Moreover, Fock states are also called *number states* after the following property:

$$\hat{n} |n\rangle = \hat{a}^\dagger \hat{a} |n\rangle = n |n\rangle, \quad (1.80)$$

²The generalization to complex-valued vectors is straightforward.

valid for each mode $(\vec{k}, \lambda)$. The operator $\hat{n} = \hat{a}^\dagger \hat{a}$ is accordingly called **(occupation) number operator**, while the total number operator is simply given by the sum of the occupation number operators over all the allowed modes $\hat{N} = \sum_{\vec{k}} \sum_{\lambda} \hat{n}_{\vec{k}\lambda}$. Moreover, the independence of a specific cavity mode on any other is formalized by the additional commutation rule $[\hat{n}_{\vec{k}\lambda}, \hat{n}_{\vec{q}\lambda'}] = 0$, for any pair of modes. It is straightforward to grasp that field Hamiltonian and number states are compatible observables, with number states being the common eigenstates:

$$[\hat{\mathcal{H}}, \hat{n}_{\vec{k}\lambda}] = 0 \Leftrightarrow \begin{cases} \hat{N} |\{n\}\rangle = \sum_{\vec{k}} \sum_{\lambda} n_{\vec{k}\lambda} |\{n\}\rangle \\ \hat{\mathcal{H}} |\{n\}\rangle = \sum_{\vec{k}} \sum_{\lambda} \hbar \omega_{\vec{k}} (n_{\vec{k}\lambda} + \frac{1}{2}) |\{n\}\rangle. \end{cases} \quad (1.81)$$

The spectrum (1.81) highlight two milestone results:

- Differently from classical electromagnetism, the vacuum state does not have zero energy. Rather, each mode contributes with a zero-point energy, condition met when no photons are present in the corresponding mode, equal to $\hbar \omega_{\vec{k}}/2$;
- Each photon with momentum $\vec{k}$ carries an energy equal to $\hbar \omega_{\vec{k}}$, regardless its polarization state.

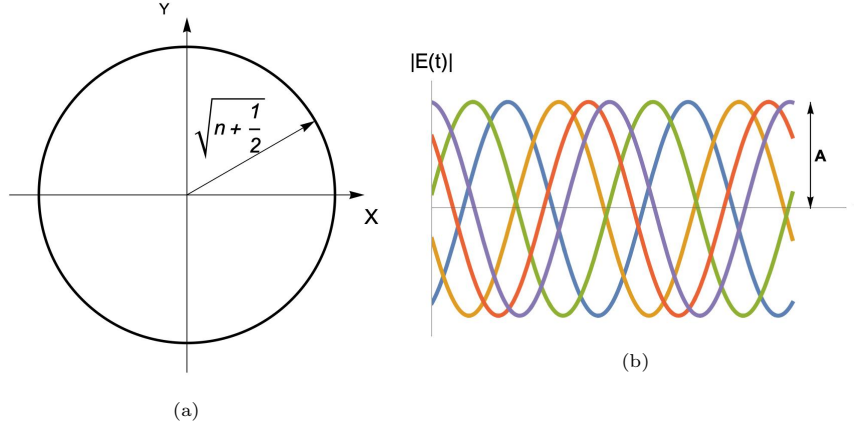


Figure 1.7: Single-mode Fock states in the quadrature operator formalism: a) Phasor representation of a number state, described by a perfectly defined amplitude $A \propto \sqrt{n + 1/2}$ and a uniformly random phase ϕ . b) Electric field amplitude as a function of time excited by a single-mode Fock state. Each curve correspond to a random phase chosen in the $[-\pi, \pi]$ interval. Picture inspired by [10].

To conclude this subsection, here below is provided the description of single-mode Fock states in the quadrature space. Moreover, by using the quadrature operators [10]:

$$\begin{cases} \langle n | \hat{X} | n \rangle = \langle n | \hat{Y} | n \rangle = 0 \\ \Delta^2 X = \langle n | \hat{X}^2 | n \rangle = \Delta^2 Y = \langle n | \hat{Y}^2 | n \rangle = \frac{1}{2} (n + \frac{1}{2}) \\ \langle n | (\hat{n} + \frac{1}{2}) | n \rangle = \langle n | (\hat{X}^2 + \hat{Y}^2) | n \rangle = n + \frac{1}{2}, \end{cases} \quad (1.82)$$

where the last equation corresponds to the expectation value of the single-mode Hamiltonian (1.71) in units of $\hbar \omega$, highlight that the amplitude fluctuations of the radiation field grow as the occupation of the mode increases, with the uncertainty of the quadrature operators lying on a circle with radius $\sqrt{n + \frac{1}{2}} = \sqrt{E_n}$.

Furthermore, as first proposed by P.A.M. Dirac in [38], the following Heisenberg-like uncertainty relation between photon number and a suitably defined Hermitian phase operator holds

$$\Delta \phi \Delta n \geq \frac{1}{2}, \quad (1.83)$$

stating that phase is the conjugate variable to the photon number. Further studies [39, 40] formalized such an idea, proving the existence of quantum states with well-defined phase, as well as introducing phase operators featuring the periodicity characterizing angular variables. Conversely to the total precision about the number of photons, Fock states bear total uncertainty on the phase, with the latter being therefore described by a uniform probability distribution in the $[0, 2\pi)$ interval.

Fock states can, indeed, be represented by a phasor $Ae^{i\phi}$, with perfectly determined amplitude $A = \sqrt{1/2 + n}$ matched by a totally random phase ϕ , as depicted in Fig. 1.7

1.3.2 Quantum information with linear optics

Among the several platforms currently used to experimentally deploy quantum information, linear optical interferometry can be conveniently used to manipulate quantum states at will, both in the DV and CV domain, as well as being an invaluable testbed for different purposes, ranging from quantum metrology and sensing (such as gravitational wave detection [6]) to highly-dimensional quantum simulation algorithms [4]. The common components of all interferometers, from the very basic to the most complex ones are *beam splitters* (*BS*), used to combine electromagnetic fields, and *phase retarders*, employed to introduce a phase shift between two components of the electromagnetic field, regardless the degree of freedom used to encode information.

Phase retarders (or phase shifters)

A phase retarder is an optical element used to introduce a phase between two orthogonal modes of the electromagnetic field. According to the chosen degree of freedom, it can assume the nature of wave plates (polarization), rather than mechanical/thermal shifters (path encoding) or spatial light modulators (spatial modes), and many others. A generic phase retarder is described by a unitary operator of the form [33]

$$\hat{U}_{\text{PS}}(\phi) = e^{i\hat{N}\cdot\phi} = e^{i\sum_j \hat{n}_j \phi_j}, \quad (1.84)$$

where $\hat{n}_j$ identifies the number operator of the j -th mode, and ϕ_j the phase shift induced on such mode. In a m -mode interferometer, the choice of a reference mode implies that only $m-1$ independent phase shifts are physically measurable. A conventional definition is thus $\phi_j \rightarrow \phi_j - \phi_r$, where now the phases are defined with respect to the reference mode.

The matrix representation of Eq. (1.84) in the Fock basis is then

$$\hat{U}_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{in\phi} \end{pmatrix}, \quad (1.85)$$

where, for the sake of brevity, a two-interferometer has been considered, although the generalization to additional modes is straightforward. The phase shift ϕ is of course imparted by an optical path difference between the considered and the reference modes. When dealing with the polarization degree of freedom, which is employed in the experiments discussed in this thesis, a phase shift between two orthogonal polarizations is imparted by means of **wave plates**, optical components made of a *birefringent* material, which exhibits two refractive indices according to the direction and the polarization of the incident light with respect to the *optical axis* of the crystal. More specifically, incident radiation experiences the **ordinary (refractive) index** whenever it propagates with its polarization orthogonal to the optical axis, independently from the propagation direction. On the other hand, **extraordinary (refractive) index** is experienced as soon as the polarization has a non-vanishing component with respect to the optical axis. The phase difference between two orthogonal polarization states arises then by the different propagation velocities inside the plate:

$$\phi = \frac{2\pi d}{\lambda_0} |n_o - n_e|, \quad (1.86)$$

where λ_0 denotes the central wavelength of the incident light (in the vacuum), d the thickness of the crystal, n_o the ordinary axis and n_e the extraordinary axis. The unitary

matrix describing a general wave plate is³ [37]:

$$\hat{U}_{\text{WP}}(\theta, \phi) = \begin{pmatrix} \cos^2 \theta + e^{i\phi} \sin^2 \theta & (1 - e^{i\phi}) \cos \theta \sin \theta \\ (1 - e^{i\phi}) \cos \theta \sin \theta & \sin^2 \theta + e^{i\phi} \cos^2 \theta \end{pmatrix}, \quad (1.87)$$

with θ being the angle between the optical axis and the vertical direction. Notably, Eq. (1.87) describes as well the phase shifter (1.85) in a different basis rotated by an angle θ : $\hat{U}_{\text{WP}}(\theta, \phi) = \hat{R}(\theta) \hat{U}_{\text{PS}}(\phi) \hat{R}(-\theta)$, where $\hat{R}(\theta)$ correspond to $\hat{R}_y(\delta = 2\theta)$ of Eq. (1.13)⁴.

According to the phase shift imparted to orthogonal polarization states, two main types of wave plates can be sorted out, namely:

- The **Half-Wave Plate (HWP)** introduces a π -shift, corresponding to an optical delay $d|n_o - n_e| = \lambda_0/2$ between the o - and e - components of the electromagnetic field. It is described by the matrix [36, 37]

$$\hat{U}_{\text{HWP}}(\theta) = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix}, \quad (1.88)$$

and it is used to rotate the polarization of the incident radiation by an angle 2θ , without changing its nature. Notably, the Hadamard gate (1.9) can be easily implemented by setting a HWP at $\theta = \pi/8$;

- The **Quarter-Wave Plate (QWP)** introduces a $\pi/2$ phase shift, i.e. an optical delay $d|n_o - n_e| = \lambda_0/4$, between the ordinary and extraordinary waves. Its jones representation is, indeed,

$$\hat{U}_{\text{QWP}}(\theta) = \begin{pmatrix} \cos^2 \theta + i \sin^2 \theta & (1 - i) \cos \theta \sin \theta \\ (1 - i) \cos \theta \sin \theta & \sin^2 \theta + i \cos^2 \theta \end{pmatrix}, \quad (1.89)$$

and is used to map linear polarization into elliptical ones, with semi-axes rotated by an angle 2θ with respect to the horizontal (H)/vertical (V) polarization directions.

Beam Splitter

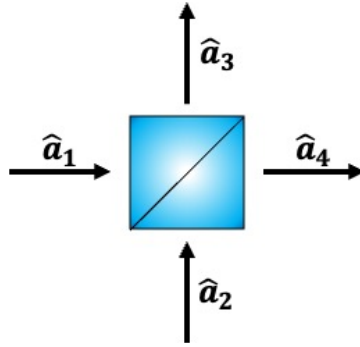


Figure 1.8: Schematic representation of a input/output relations of a beam splitter, mixing together electromagnetic fields entering the input ports (1,2) into the output paths (3,4). In a quantum mechanical description, the input annihilation operators $\hat{a}_1$ and $\hat{a}_2$ are linearly combined into the output annihilation operators $\hat{a}_3$ and $\hat{a}_4$. Picture inspired by [10].

The **Beam Splitter (BS)** is an optical device used to mix two incoming beams and/or to split them in two different spatial paths [10], for this reason largely exploited in interferometry. More specifically, the fields entering in the two input ports $\vec{E}_1$ and $\vec{E}_2$ are rearranged in two output fields $\vec{E}_3$ and $\vec{E}_4$ as [10]:

$$\vec{E}_3 = \mathcal{R}\vec{E}_1 + \mathcal{T}\vec{E}_2, \quad \vec{E}_4 = \mathcal{T}\vec{E}_1 + \mathcal{R}\vec{E}_2. \quad (1.90)$$

³It does coincide with the Jones matrix for an arbitrary waveplate in classical optics.

⁴Crucially, there $\hat{R}(\theta)$ identifies a *purely geometrical* rotation of the coordinate system in the transverse plane, **not** a rotation of the qubit system on the Bloch sphere.

In a quantum mechanical picture, as shown by Fig. 1.8, the BS can be considered a unitary transformation mapping the creation/annihilation operators of the input ports into a new set of operators for the output modes, according to the same equations (1.90) holding in the classical domain [10]:

$$\hat{a}_3 = \mathcal{R}\hat{a}_1 + \mathcal{T}\hat{a}_2, \quad \hat{a}_4 = \mathcal{T}\hat{a}_1 + \mathcal{R}\hat{a}_2, \quad (1.91)$$

where $\mathcal{R} = |\mathcal{R}|e^{i\delta_R}$ and $\mathcal{T} = |\mathcal{T}|e^{i\delta_T}$, obeying the commutation relations [10]

$$[\hat{a}_i, \hat{a}_j^\dagger] = \delta_{ij}, \quad [\hat{a}_i, \hat{a}_j] = 0, \quad \forall i, j = 1, \dots, 4. \quad (1.92)$$

In a vector-matrix formalism, the description of a BS is given by:

$$\begin{pmatrix} \hat{a}_3 \\ \hat{a}_4 \end{pmatrix} = \hat{U}_{\text{BS}}(\mathcal{R}, \mathcal{T}) \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix} \longrightarrow \hat{U}_{\text{BS}}(\mathcal{R}, \mathcal{T}) = \begin{pmatrix} \mathcal{R} & \mathcal{T} \\ \mathcal{T} & \mathcal{R} \end{pmatrix}. \quad (1.93)$$

Under the assumption of lossless beam splitter, two additional requirements on the reflection coefficient $\mathcal{R}$ and transmission coefficient $\mathcal{T}$ have to be satisfied, namely: $|\mathcal{R}|^2 + |\mathcal{T}|^2 = 1$ and $\mathcal{R}\mathcal{T}^* + \mathcal{T}\mathcal{R}^* = 0 \rightarrow \delta_R - \delta_T = \pi/2$.

An emblematic example is represented by the *lossless, balanced beam splitter*, described by the unitary operator [10]

$$\hat{U}_{\text{BS}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}. \quad (1.94)$$

Polarizing Beam Splitter (PBS)

The beam splitter discussed in section 1.3.2 mixes the light beams entering the input ports independently of their polarization. The polarization-dependent counterpart lies in the **Polarizing Beam Splitter (PBS)**, employed whenever information is encoded in the polarization degree of freedom, such as in polarization-dependent interferometry or polarization analysis.

Unlike a standard BS, a PBS couples the polarization degree of freedom with the optical path at both the input and the output ports. In the Fock operator formalism, a PBS is described by a matrix of the form

$$\begin{pmatrix} \hat{a}_{3H} \\ \hat{a}_{4H} \\ \hat{a}_{3V} \\ \hat{a}_{4V} \end{pmatrix} = \hat{U}_{\text{PBS}} \begin{pmatrix} \hat{a}_{1H} \\ \hat{a}_{2H} \\ \hat{a}_{1V} \\ \hat{a}_{2V} \end{pmatrix} \longrightarrow \hat{U}_{\text{PBS}} = \begin{pmatrix} \mathcal{R}_{31}^{(H)} & \mathcal{T}_{32}^{(H)} & 0 & 0 \\ \mathcal{T}_{41}^{(H)} & \mathcal{R}_{42}^{(H)} & 0 & 0 \\ 0 & 0 & \mathcal{R}_{31}^{(V)} & \mathcal{T}_{32}^{(V)} \\ 0 & 0 & \mathcal{T}_{41}^{(V)} & \mathcal{R}_{42}^{(V)} \end{pmatrix}, \quad (1.95)$$

where the input/output relations are defined according to the notation of Fig. 1.8. Notably, since Fock operators for each polarization are given by linear combinations of operators associated with the same polarization, the PBS matrix (1.95) is written in a block-diagonal form. Here, each block describes a BS matrix (1.91) for the given polarization, with no coherence being generated between H and V components.

Moreover, a lossless PBS requires the Fock operators to satisfy the canonical commutation rule $[\hat{a}_{i\lambda}, \hat{a}_{j\lambda'}^\dagger] = \delta_{ij}\delta_{\lambda\lambda'}$ for each path $i, j = 1, \dots, 4$ and polarization $\lambda, \lambda' = H, V$, while the reflection/transmission coefficients obey

$$\begin{aligned} |\mathcal{R}_{31}^{(\lambda)}|^2 + |\mathcal{T}_{41}^{(\lambda)}|^2 &= 1 \quad \lambda = H, V \\ |\mathcal{R}_{24}^{(\lambda)}|^2 + |\mathcal{T}_{32}^{(\lambda)}|^2 &= 1 \quad \lambda = H, V \\ \mathcal{R}_{31}^{(\lambda)}\mathcal{T}_{32}^{(\lambda)*} + \mathcal{T}_{41}^{(\lambda)}\mathcal{R}_{42}^{(\lambda)*} &= 0 \quad \lambda = H, V \end{aligned} \quad (1.96)$$

The most commonly used PBS completely reflects vertical polarization and completely transmits the horizontal component. Imposing $|\mathcal{T}_{41}^{(H)}| = |\mathcal{T}_{32}^{(H)}| = 1$ and $|\mathcal{R}_{31}^{(V)}| = |\mathcal{R}_{42}^{(V)}| = 1$ into Eq. (1.96) the PBS matrix (1.95) reduces, up to an overall, physically

irrelevant phase, to

$$\hat{U}_{\text{PBS}} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \quad (1.97)$$

Interestingly, in the ideal scenario, the PBS (1.97) acts as a unitary, controlled, operation on the spatial path according to the polarization of the input photon.

Hong-Ou-Mandel (HOM) interference

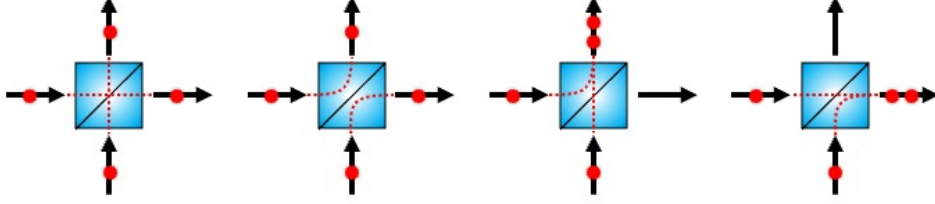


Figure 1.9: The four possible outcomes of two photons entering in a balanced BS.

One of the most peculiar phenomena arising in quantum optics, with no classical counterpart, is the celebrated **Hong-Ou-Mandel (HOM)** effect, named after the researchers who first observed the phenomenon in 1987 [41]. HOM is a quantum interference effect involves two indistinguishable (referring to all the degrees of freedom) photons entering along two ports of a balanced BS: in a classical picture four possible outcomes, summarized in Fig. 1.9 can manifest with equal probability; namely

- Both photons are transmitted;
- Both photons are reflected;
- Photon entering port 1 is reflected, while photon entering port 2 is transmitted;
- Photon entering port 1 is transmitted, while photon entering port 2 is reflected.

Conversely, by adopting the quantum theory of BS, the two-photon state entering the BS is

$$|11\rangle_{12} = |1\rangle_1 |1\rangle_2 = \int dt dt' g(t, t') \hat{a}_1^\dagger \hat{a}_2^\dagger |0\rangle, \quad (1.98)$$

where $g(t, t')$ referring to the joint wavefunction of the input photons, obeying the normalization condition $\int dt dt' |g(t, t')|^2 = 1$ [42]. By using Eq. (1.94), the creation operators of the input modes are mapped into⁵:

$$|11\rangle_{12} = \int dt dt' \frac{g(t, t') + g(t', t)}{2} \frac{i}{2} (\hat{a}_3^\dagger \hat{a}_3^\dagger + \hat{a}_4^\dagger \hat{a}_4^\dagger) |0\rangle. \quad (1.99)$$

The probability of detecting two photons on the same output path (e.g. port 3) is indeed

$$\begin{aligned} P(|11\rangle_{12} \rightarrow |20\rangle_{34}) &= P(|11\rangle_{12} \rightarrow |02\rangle_{34}) = \left| \langle 2_3 0_4 | \hat{U}_{\text{BS}} | 1_1 1_2 \rangle \right|^2 = \\ &= \frac{1}{4} \left| \int dt dt' \frac{g(t, t') + g(t', t)}{2} \right|^2 = \frac{1}{4} (1 + |\tau|^2), \end{aligned} \quad (1.100)$$

being proportional to the time overlap $\tau = \int dt dt' g^*(t, t') g(t, t')$ of the two wave packets.

⁵Following from Eq. (1.93), it is possible to write $\begin{pmatrix} \hat{a}_3^\dagger \\ \hat{a}_4^\dagger \end{pmatrix} = \hat{U}_{\text{BS}}^\dagger \begin{pmatrix} \hat{a}_1^\dagger \\ \hat{a}_2^\dagger \end{pmatrix}$, thus $\begin{pmatrix} \hat{a}_1^\dagger \\ \hat{a}_2^\dagger \end{pmatrix} = \hat{U}_{\text{BS}} \begin{pmatrix} \hat{a}_3^\dagger \\ \hat{a}_4^\dagger \end{pmatrix}$.

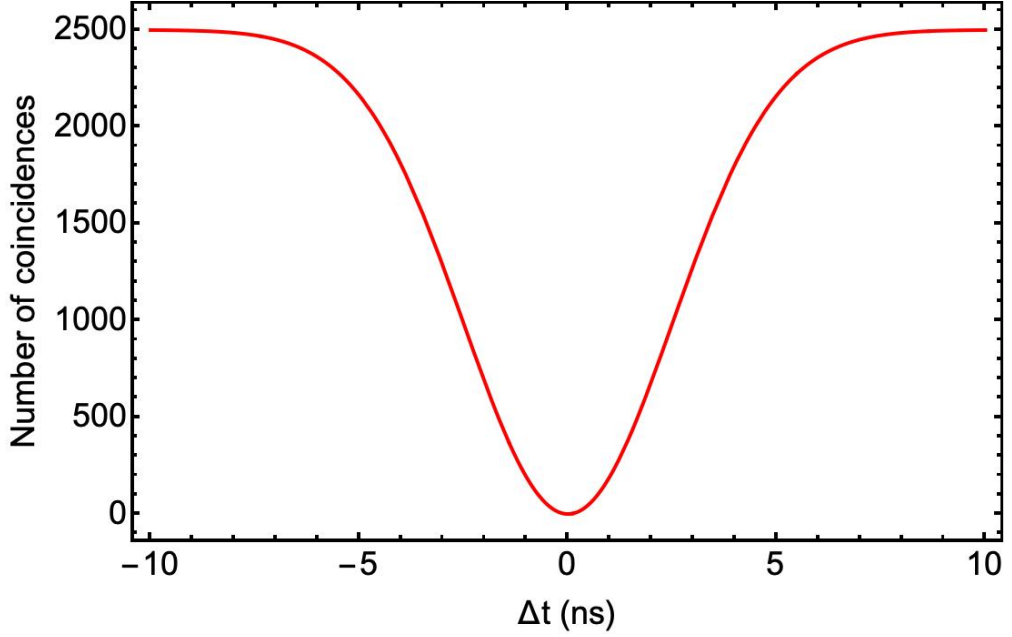


Figure 1.10: Example of the theoretical curve of the Hong-Ou-Mandel dip for Gaussian wave packets. The plot reports the number of coincidence counts between two different output ports of the BS is plotted as a function of the relative time delay between the two optical paths.

Whenever the two photons are perfectly superimposed, i.e. $\tau = 1$, the probabilities of detecting two photons on the same arm become evenly balanced; consequently the probability of coincidence events between two different output ports dropping to zero, as it was retrieved in the original HOM experiment [41]. Referring to Fig. 1.9, with perfectly indistinguishable photons, with no relative time delay, the third and fourth outcome do not show up.

Conversely, for non-zero time delay, the probability of coincidence detections progressively increases, giving birth to the celebrated *HOM dip*, shown in Fig. 1.10, up to the case in which all the four scenarios depicted in Fig. 1.9 are restored with equal probability, corresponding to the perfect distinguishability scenario ($\tau = 0$).

HOM interference is an experimental manifestation of *bosonic coalescence*, and can be used as a verification test for quantum interference experiments, being as well able to flag the swap symmetry of quantum states, crucial for quantum teleportation protocols [43].

Moreover, the output state of a 50:50 BS fed up with two indistinguishable photons on different different paths is

$$|\psi\rangle = \hat{U}_{\text{BS}} |11\rangle_{12} = i \frac{|20\rangle_{34} + |02\rangle_{34}}{\sqrt{2}} \quad (1.101)$$

being, up to a global phase factor, a $n00n$ state with $n = 2$, a fundamental state for quantum phase estimation, described in the next section.

In conclusion, HOM interference acts as a template for a (quasi-)deterministic source of $n00n$ states ($n = 2$), as thoroughly discussed in [44–49].

1.3.3 Phase estimation via quantum interferometry

A simple, yet insightful example of quantum metrology is the quantum phase estimation via linear optical interferometers, such as the **Mach-Zehnder interferometer (MZI)** [17, 50–52], depicted in Fig. 1.11. The main components of a MZI (in its more standard implementation) are, in order:

1. a 50:50 BS used to recombine the light entering the two input ports into the two interferometric path;

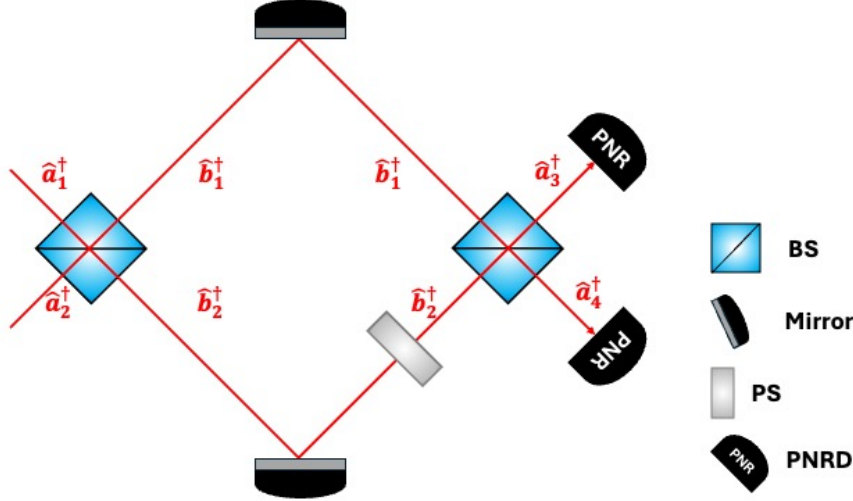


Figure 1.11: Sketch of a quantum phase estimation protocol via a MZI interferometer. Creation operators associated with each path are reported in the diagram. Photons are collected by photon-number-resolving detectors (PNRD), so as to fully exploit the quantum properties of the adopted probe states.

2. a PS implementing a phase shift with respect to the reference arm;
3. an other 50:50 BS combining the light from the two interferometric path into the two output modes, steering light to the measurement stations.

It can be therefore described by the following unitary operator:

$$\hat{U}_{\text{MZI}}(\phi) = \hat{U}_{\text{BS}} \hat{U}_{\text{PS}}(\phi) \hat{U}_{\text{BS}}, \quad (1.102)$$

where $\hat{U}_{\text{BS}}$ coincides with the expression in (1.94), while $\hat{U}_{\text{PS}}(\phi)$ corresponds to the phase shift operator (1.85).

Phase estimation with a Fock state

A common choice for the probe is a Fock state injected into one of the two ports of the first BS, such as $|\psi_0\rangle = |n\rangle_1 |0\rangle_2$, which is mapped into

$$|\psi_0\rangle = |n0\rangle_{12} = \frac{1}{\sqrt{2^n}} \sum_{k=0}^n i^{n-k} \sqrt{\binom{n}{k}} |k\rangle_{b_1} |n-k\rangle_{b_2}, \quad (1.103)$$

where $\binom{n}{k}$ denotes the binomial coefficient $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Subsequently, the phase shifter acts on the photons traveling through the interested path, mapping the state (1.103) into

$$|\psi_\phi\rangle = e^{i\hat{b}_2^\dagger \hat{b}_2 \phi} |\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^n i^{n-k} \sqrt{\binom{n}{k}} e^{i(n-k)\phi} |k\rangle_{b_1} |n-k\rangle_{b_2}. \quad (1.104)$$

The quantum state out the second BS (thus the output state of the MZI) is then

$$|\psi_{\text{out}}\rangle = \sum_{k=0}^n \sqrt{\binom{n}{k}} \cos\left(\frac{\phi}{2}\right)^k \sin\left(\frac{\phi}{2}\right)^{n-k} |k\rangle_3 |n-k\rangle_4. \quad (1.105)$$

The probability of detecting k photons on one output path (thus $n-k$ on the other one) will be described by a binomial distribution [50, 51]

$$P(k|\phi) = \binom{n}{k} \cos\left(\frac{\phi}{2}\right)^{2k} \sin\left(\frac{\phi}{2}\right)^{2(n-k)} \quad (1.106)$$

with success probability given by $p = \cos(\phi/2)^2$. The Fisher information (1.46) associated with the measurement strategy here described is

$$f(\phi) = \sum_{k=0}^n \frac{1}{P(k|\phi)} \left(\frac{\partial P(k|\phi)}{\partial \phi} \right)^2 = n, \quad (1.107)$$

with $P(k|\phi)$ given by Eq. (1.106). The corresponding Cramér-Rao inequality is then

$$\Delta\tilde{\phi} \geq \frac{1}{\sqrt{f(\phi)}} = \frac{1}{\sqrt{n}}, \quad (1.108)$$

corresponding to the standard quantum limit.

Moreover, the QFI associated with a Fock state is, according to (1.56), given by [17, 50, 51]

$$F_Q(\phi) = 4 \left(\langle \psi_\phi | (\hat{b}_2^\dagger \hat{b}_2)^2 | \psi_\phi \rangle - (\langle \psi_\phi | \hat{b}_2^\dagger \hat{b}_2 | \psi_\phi \rangle)^2 \right) = n. \quad (1.109)$$

In conclusion, Eq. (1.109) states that the use of Fock states as probe for a phase estimation in a MZI grants any phase value to be estimated with the same precision, corresponding to the SQL scaling $\mathcal{O}(1/\sqrt{n})$.

Phase estimation with a n00n state

A cornerstone in quantum interferometry is represented by the paper authored by H. Lee, P. Kok and J.P. Dowling "A quantum Rosetta stone for interferometry" [53], dealing with an interferometric phase estimation with a n00n state

$$|\psi_0\rangle = \frac{|n0\rangle_{12} + |0n\rangle_{12}}{\sqrt{2}} \quad (1.110)$$

used as metrological probe. The QFI can be computed by exploiting the expression (1.56) as in Eq. (1.109); however, it is worthy to note that $|\psi_\phi\rangle = \hat{U}_{\text{PS}}(\phi)\hat{U}_{\text{BS}}|\psi_0\rangle$, so that the expected value of $\hat{n}_{b_2}^m = (\hat{b}_2^\dagger \hat{b}_2)^m$ are

$$\langle \psi_\phi | (\hat{b}_2^\dagger \hat{b}_2)^m | \psi_\phi \rangle = \langle \psi_0 | (\hat{b}_2^\dagger \hat{b}_2)^m | \psi_0 \rangle \quad \forall m, \quad (1.111)$$

following from the circular properties of the expectation values and the fact that $[\hat{U}_{\text{PS}}, \hat{n}_{b_2}^m] = 0$. The computation of such expected values on the n00n state (1.110) is then $\langle \psi_0 | (\hat{b}_2^\dagger \hat{b}_2)^m | \psi_0 \rangle = n^m/2$; the QFI is then

$$F_Q(\phi) = 4 \left(\langle \psi_0 | (\hat{b}_2^\dagger \hat{b}_2)^2 | \psi_0 \rangle - (\langle \psi_0 | \hat{b}_2^\dagger \hat{b}_2 | \psi_0 \rangle)^2 \right) = n^2, \quad (1.112)$$

yielding to a QCRB

$$\Delta\tilde{\phi} \geq \frac{1}{\sqrt{f(\phi)}} \geq \frac{1}{\sqrt{F_Q(\phi)}} = \frac{1}{n} \rightarrow \Delta\tilde{\phi} \geq \frac{1}{n}. \quad (1.113)$$

This time the standard deviation on the phase estimator is lower bounded by a factor $\mathcal{O}(1/n)$, corresponding to the so-called **Heisenberg limit**: the use of n00n states, having no classical counterpart, enables estimation precision by a factor $\mathcal{O}(\sqrt{n})$ with respect to the QCRB holding for Fock states (see Fig. 1.12). This game changing effect is indeed called **quantum enhancement**, assessing the fundamental advantage of using quantum resources in parameter estimation protocols, being, therefore, the hallmark of state-of-the-art quantum metrological protocols.

In a more realistic setting, experimental imperfections-such as dechoerence, noise and non-perfect visibility-might prevent the Heisenberg limit from being approached. Nevertheless, enhanced estimation performances with respect to strategies not exploiting quantum features still remain achievable.

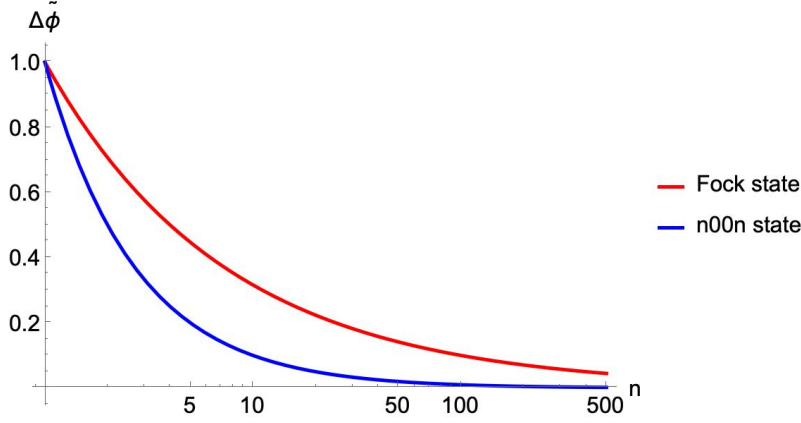


Figure 1.12: Logarithmic plot of the QCRB (in terms of the standard deviation of the phase estimator $\tilde{\phi}$) as a function of the number of photons n , for both the Fock states (red curve) and the $n00n$ state (blue curve). The plot clearly shows the enhanced estimation precision enabled by the $n00n$ state, as assessed by Eq. (1.113).

1.3.4 Spontaneous Parametric Down Conversion (SPDC)

It is well known, from classical electromagnetism [54, 55] that matter reacts to external electric fields by electronic polarization mechanisms, described, in the linear response regime, by the (electronic) polarization vector

$$P_{\alpha}^{(1)}(\vec{r}, t) = \int_{-\infty}^{+\infty} \frac{d\omega}{2\pi} \chi_{\alpha\beta}^{(1)}(\omega) E_{\beta}(\omega) e^{i(\omega t - \vec{k}(\omega) \cdot \vec{r})}, \quad \alpha, \beta = x, y, z, \quad (1.114)$$

where $\chi_{\alpha\beta}^{(1)}(\omega)$ denotes the *electric susceptibility tensor*. As a result, any external perturbation at frequency ω will produce a response, in the form of polarization charges oscillating at the same frequency as the electric field. The total polarization is then retrieved by linearly combining the electronic response at each spectral component. However, it may happen that, for sufficiently intense fields, some **nonlinear effects**, involving more than one electric field at once, are triggered: differently from the linear regime, preserving locality in the frequency domain (as stated by Eq. (1.114)), nonlinear interactions enable the creation of new spectral components. The simplest nonlinear phenomena, showing up in non-centrosymmetric materials, for which $\chi^{(2)} \neq 0$, are *second-order effects*, described by a susceptibility tensor $\chi^{(2)} = \mathcal{O}(1 \times 10^{-3} \chi^{(1)})$, in which two electric fields mutually interact so as to produce a response to different spectral components, namely:

- **Sum-Frequency Generation (SFG)**: manifesting whenever two fields at frequencies ω_1 and ω_2 are combined to give rise to a spectral component at an higher frequency $\omega_3 = \omega_1 + \omega_2$;
- **Second-Harmonic Generation (SHG)**: particular case of the SFG, in which two fields at the same frequency $\omega_1 = \omega_2 = \omega_0$ are mixed to generate a field with double frequency $\vec{E}(2\omega_0)$;
- **Difference-Frequency Generation (DFG)**: phenomenon occurring whenever two fields at frequencies ω_1 and ω_2 are merged, originating a new field at a lower frequency $\omega_3 = \omega_1 - \omega_2$ (all the frequencies are assumed to be positive);
- **Optical Rectification (OR)**: the dual effect to the SHG, featuring two electric fields at the same frequency ω_0 with different sign (similarly to DFG, the frequency ω_0 is taken positive), which, after the interaction in the crystal produce a new field at zero frequency.

A pictorial representation is presented in Fig. 1.13

The energy at time t stored in the volume V occupied by the nonlinear crystal is [54]

$$\mathcal{H}(t) = \int_V \frac{d^3r}{8\pi} \vec{E}^*(\vec{r}, t) \cdot \vec{D}(\vec{r}, t). \quad (1.115)$$

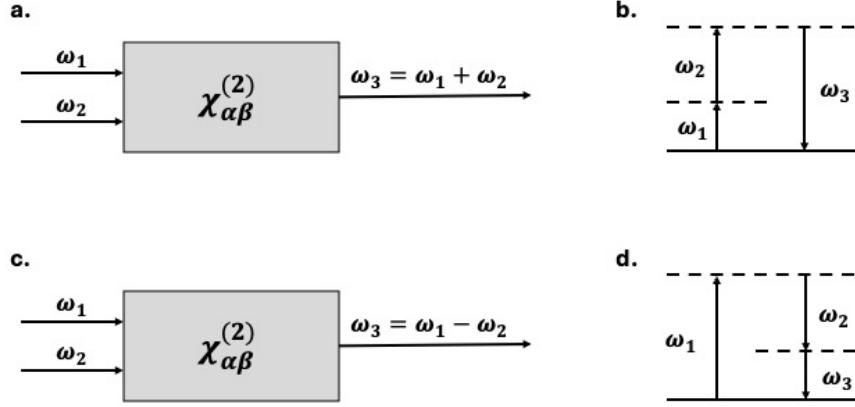


Figure 1.13: Schematic representation of SFG (panels a. and b.) and DFG (panels c. and d.). Panels a. and c. show the concept of nonlinear phenomena, in which a nonlinear crystal is fed with two fields at frequencies ω_1 and ω_2 to produce a new field with spectral component at $\omega_3 = \omega_1 \pm \omega_2$. Panels b. and d. picture the energy conservation for the SFG and DFG. Picture inspired by [55, 56].

By recalling that $\vec{D} = \vec{E} + 4\pi\vec{P}$, it is possible to rewrite Eq. (1.115) as

$$\mathcal{H}(t) = \int_V \frac{d^3r}{8\pi} \vec{E}^*(\vec{r}, t) \cdot \vec{D}^{(0)}(\vec{r}, t) + \int_V \frac{d^3r}{2} \vec{E}^*(\vec{r}, t) \cdot \vec{P}^{(2)}(\vec{r}, t), \quad (1.116)$$

where the first term of the right hand side corresponds to the energy stored via the linear interaction, while the second is due to second-order phenomena. This latter term can be expressed as [42, 57]

$$\mathcal{H}_I(t) = \int_V \frac{d^3r}{2} \int_{\mathbb{R}^3} \frac{d\omega_1 d\omega_2 d\omega_3}{(2\pi)^3} E_\alpha^*(\omega_3) \chi_{\alpha\beta\gamma}^{(2)}(\omega_1, \omega_2) E_\beta(\omega_1) E_\gamma(\omega_2) e^{i(\Delta\omega t - \Delta\vec{k} \cdot \vec{r})}, \quad (1.117)$$

where $\Delta\omega = \omega_1 + \omega_2 - \omega_3$ is the frequency mismatch and $\Delta\vec{k} = \vec{k}(\omega_3) - \vec{k}(\omega_1) - \vec{k}(\omega_2)$ the momentum mismatch.

A DFG-related, genuinely quantum, phenomenon is **Spontaneous Parametric Down-Conversion (SPDC)**. First described by Louisell in [58] and experimentally observed by Burnham and Weinberg [59], SPDC involves a *pump* photon propagating in a nonlinear crystal (typically KTP, BBO, BiBO, LN⁶). During the propagation the pump photon interacts with the vacuum, it generates a *signal* photon and an *idler* photon, emitted in pairs (see Fig. 1.14).

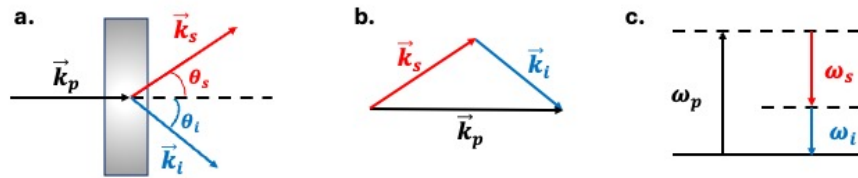


Figure 1.14: Spontaneous Parametric Downconversion: a) a pump photon is absorbed by a nonlinear crystal to generate a signal-idler photon pair, such that energy and momentum conservation are respected; b) Phase matching condition (momentum conservation) $\Delta k = 0$; c) Energy level diagram of the energy conservation $\omega_p = \omega_i + \omega_s$. Picture inspired by [42, 57].

The quantum mechanical description of the SPDC relies on Eq. (1.117), where now

⁶Potassium Titanyl Phosphate ($KTiOPO_4$), Barium Borate (BaB_2O_4), Bismuth Borate (BiB_3O_6) and Lithium Niobate ($LiNbO_3$).

electric fields are replaced with the corresponding field operators (1.72). More specifically, the evolution of the initial quantum state $|\psi_0\rangle = |1\rangle_p |0\rangle_s |0\rangle_i$, featuring only one pump photon, is ruled by a unitary operator

$$|\psi\rangle = \hat{U} |\psi_0\rangle = \hat{U} |1\rangle_p |0\rangle_s |0\rangle_i \quad \hat{U} = e^{-\frac{i}{\hbar} \int_{-\infty}^{+\infty} dt \hat{\mathcal{H}}_I(t)}. \quad (1.118)$$

As already mentioned, since $\mathcal{O}(\chi^{(2)}) \ll 1$ it is possible to write the evolution operator (1.118) via its Dyson series [42]:

$$\hat{U} = e^{-\frac{i}{\hbar} \int_{-\infty}^{+\infty} dt \hat{\mathcal{H}}_I(t)} \simeq \mathbb{1} - \frac{i}{\hbar} \int_{-\infty}^{+\infty} dt \hat{\mathcal{H}}_I(t) + \mathcal{O}(\hat{\mathcal{H}}_I^2). \quad (1.119)$$

The evolved state, at the first perturbative order, is thus

$$\begin{aligned} |\psi\rangle &= |\psi_0\rangle - \frac{i}{2\hbar} \int_{-\infty}^{+\infty} dt \int_V d^3r \int_{\mathbb{R}^2} \frac{d\omega_s d\omega_i}{(2\pi)^2} \hat{E}_\alpha^* \chi_{\alpha\beta\gamma}^{(2)} \hat{E}_\beta(\omega_s) \hat{E}_\gamma(\omega_i) e^{i(\Delta\omega t - \Delta\vec{k} \cdot \vec{r})} |0\rangle = \\ &= |\psi_0\rangle - \frac{i}{2\hbar} \int_{\mathbb{R}^2} \frac{d\omega_s d\omega_i}{(2\pi)^2} \hat{E}_\alpha^* \chi_{\alpha\beta\gamma}^{(2)} \hat{E}_\beta(\omega_s) \hat{E}_\gamma(\omega_i) \int_V d^3r e^{-i\Delta\vec{k} \cdot \vec{r}} \int_{-\infty}^{+\infty} dt e^{i\Delta\omega t} |0\rangle = \\ &= |\psi_0\rangle + g \int_{\mathbb{R}^2} d\omega_s d\omega_i \delta(\omega_s + \omega_i - \omega_p) \text{sinc}\left(\frac{\Delta k_z L}{2}\right) \hat{a}(\omega_p) \hat{a}^\dagger(\omega_s) \hat{a}^\dagger(\omega_i) |0\rangle, \end{aligned} \quad (1.120)$$

where a monochromatic pump field was considered, while g identifies a normalization factor modeling the light-matter interaction [42, 57]. Nonetheless, the following relations have been used: $\int_{\mathbb{R}} dt e^{i\Delta\omega t} \propto \delta(\omega_s + \omega_i - \omega_p)$, and $\int_V d^3r e^{-i\Delta\vec{k} \cdot \vec{r}} \propto \text{sinc}\left(\frac{\Delta\vec{k} \cdot \vec{L}}{2}\right)$,

with $\vec{L}$ identifying the interaction length of the nonlinear crystal. The second term of the right hand side of Eq. (1.120) clearly highlights that a pump photon is annihilated to generate a signal-idler photon pair, with the efficiency of the generation process depending on three factors [42]:

- The total energy is conserved through the nonlinear interaction $\rightarrow \hbar\omega_p = \hbar\omega_s + \hbar\omega_i$;
- Interaction occurs in sufficiently long crystals $L \gg 1$;
- The total photon momentum is conserved, also known as **phase matching (PM)** condition, i.e. $\Delta k = |\Delta\vec{k}| = 0$.

Graphical interpretation of the energy conservation and phase matching requirements are provided in Fig. 1.14. Notably, PM is hardly achievable in isotropic materials due to the refractive index being an increasing function of the frequency. To tackle such an issue, birefringent crystals are commonly used, and study the propagation of electromagnetic fields according to their polarization. Concerning uniaxial crystals, featuring only one optical axis, the phase matching conditions are summarized in Table 1.2. The

Table 1.2: Phase matching conditions for both positive and negative uniaxial crystals. The following hierarchy for the frequencies is assumed $\omega_p > \omega_s \geq \omega_i$. Table inspired by [55, 56].

	Positive uniaxial $n_e > n_o$	Negative uniaxial $n_o > n_e$
Type-I	$n_o(\omega_p)\omega_p = n_e(\omega_s)\omega_s + n_e(\omega_i)\omega_i$	$n_e(\omega_p)\omega_p = n_o(\omega_s)\omega_s + n_o(\omega_i)\omega_i$
Type-II	$n_o(\omega_p)\omega_p = n_e(\omega_s)\omega_s + n_o(\omega_i)\omega_i$	$n_e(\omega_p)\omega_p = n_o(\omega_s)\omega_s + n_e(\omega_i)\omega_i$

relatively simple implementation, not requiring complex source engineering, together with the ability to directly generate entangled photon pairs, makes SPDC sources a widespread choice of single-photon sources in those experiments focusing on the design and the test of quantum communication, quantum metrology and quantum information protocols, as in the case of this thesis.

Chapter 2

Investigating the foundations of quantum mechanics via quantum metrology

Since its first formulation during the 20s of the XXth century, quantum mechanics proved to be an invaluable theory to describe the physical world, able to provide solutions to problems left unsolved by classical physics. One of the most peculiar feature of quantum mechanics is the possibility for quantum states to exhibit nonlocal correlations not reproducible by classical phenomena. This is the heart of the Einstein-Podolsky-Rosen (EPR) paradox, discussed in Section 2.1.

Following the way paved by the EPR work, the nonlocal nature of quantum mechanics has been investigated with the formalization of concepts such as the celebrated quantum entanglement, Bell non-locality and quantum steering, discussed in sections 2.2.1 to 2.2.3.

The differences among these correlations are discussed in depth in section 2.2.4.

A fundamental problem for practical applications is therefore the certification of genuine quantum correlations, ruling out the possibility of reproducing them by means of classical randomness. To this extent, an interesting work by B. Yadin, M. Fadel and M. Gessner (YFG) [60] set the stage for a new class of validation techniques, relying on informational quantities inferred via quantum metrology. This is discussed in section 2.3.1. However, a direct implementation of the YFG method in practical scenarios requires a virtually infinite dataset (the certification of quantum steering is based on the Cramér-Rao bound, valid in the asymptotic regime), as well as not accounting for nuisance unavoidably present in experimental apparatus. Overcoming these issues demands an adaptation of the original YFG protocol, in order to account for the finite-size regime, and the presence of nuisance in the experimental setup: this is presented in section 2.3.2. The extension of the original YFG approach to the multiparameter, non-asymptotic regime, with an experimental demonstration with an optical platform has been published in [7], and is discussed in sections 2.4 and 2.4.2. A follow-up on the theme, addressing the robustness of the protocol presented in 2.4.2 with respect to the modelization of the initial knowledge has been published in [61] and presented in section 2.6.

2.1 From quantum measurements to the EPR paradox

It was highlighted in the previous chapters how the measurement of any physical observable unavoidably affects the quantum state used as a probe. Indeed, the effect of a measurement of a given observable over a generic quantum state is the peculiar ingredient to investigate the celebrated Einstein-Podolsky-Rosen (EPR) paradox. In their seminal paper [62], Einstein, Podolsky and Rosen conjectured about the capability of quantum mechanics of associating every element of physical reality to a corresponding theoretical counterpart (also known as *completeness* of quantum mechanics). The proof EPR provide is grounded on the probabilistic interpretation given to the wavefunction.

The main result of the paper states that:

- the description of physical reality provided by the wavefunction is not complete;
- two incompatible (non-commutative) physical observables are prevented from sharing a simultaneous physical reality, the wavefunction, thus quantum mechanics, is unable to capture.

A key ingredient, yielding to both the aforementioned results, is the choice of a given observable used to query the quantum state of the system under exam, entailing a specific experimental arrangement. This latter feature has been further enforced by the letter authored by N. Bohr [63], replying to EPR's argument.

Here, Bohr points out that a criterion to define "physical reality" not relying on philosophical, *a priori* assumptions, was needed in order to properly agree with the mathematical formalism of quantum mechanics, as well as with experimental evidences. Rather, Bohr stresses the fundamental importance the measurement arrangement has in order to interface ourselves with physical world. As a consequence, Bohr quarrels that the usage of the term "completeness" proposed by the original EPR's work does not suit quantum mechanics, suggesting the term "*complementary*" to fit with the postulate of quantum theory and experimental tests.

EPR paradox continued to be an open problem in the years to come, with many people working on quantum mechanics involved in solving the issue.

A turning point was marked in 1957 by Aharonov and Bohm, who, in their paper [64], proposed an alternative formulation of the EPR paradox, which later would have become the most common formalism to treat it.

They assumed to work with two spin 1/2 particles in a superposition state with total spin equal to zero, i.e. the *singlet state*

$$|\psi_{AB}\rangle = \frac{|\uparrow\rangle_A |\downarrow\rangle_B - |\downarrow\rangle_A |\uparrow\rangle_B}{\sqrt{2}}. \quad (2.1)$$

The two parties are then spatially separated so that the total spin is conserved, and any potential interaction between the two parties ceases. Subsequently, an arbitrary spin component is measured on particle A. As a result, since the total spin of the **system** is 0, the measurement of the very same spin component on the other particle will output the opposite result of A's. More formally, any measurement on particle A will make the quantum system *collapse* into a statistical mixture of $|\uparrow\rangle_A |\downarrow\rangle_B$ and $|\downarrow\rangle_A |\uparrow\rangle_B$, each with probability 1/2:

$$S_z^{(A)} |\psi_{AB}\rangle \rightarrow \begin{cases} |\uparrow\rangle_A |\downarrow\rangle_B & P(s_z^{(A)} = \uparrow) = 1/2 \\ |\downarrow\rangle_A |\uparrow\rangle_B & P(s_z^{(A)} = \downarrow) = 1/2 \end{cases} \rightarrow \begin{cases} P(s_z^{(B)} = \downarrow | s_z^{(A)} = \uparrow) = 1 \\ P(s_z^{(B)} = \uparrow | s_z^{(A)} = \downarrow) = 1 \end{cases}. \quad (2.2)$$

Consequently, any result on particle B will be uniquely determined, regardless of the measurement outcome on the other party. Such a result is achieved by performing exclusively local operations on one party. However, the information about the joint system $A \cup B$ is fully encoded in the wavefunction (2.1). As in the original work authored by Einstein, Podolsky and Rosen [62], there is no need to perturb particle B in order to gather information about its spin state. Moreover, the dependence on the experimental setting is vital, since any measurement of **any other combination of** spin components on the system would lead to maximum uncertainty on the experimental outcomes, obeying thus the uncertainty principle. As Aharonov and Bohm suggest, quantum mechanics must feature some intrinsic *non-local* feature in order to rationally understand the EPR paradox.

EPR paradox and related works shone the light upon the intrinsic non-local nature of quantum mechanics, with quantum entanglement being the most known phenomenon identifying such a feature. However, the formal definition of entanglement needed further investigations, which also identified a class of non-local quantum correlations, discussed in the following section.

2.2 Nonlocal quantum correlations

The intrinsic non-locality quantum mechanics features corresponds to the celebrated "*spooky action at a distance*", as Einstein usually described. However, it is nowadays

known that such peculiarity of the quantum theory manifests in different fashions, according to the specific constraints the state of the quantum system under study obeys.

2.2.1 Quantum entanglement

The EPR work [62] highlighted a clash between the views that classical physics and quantum theory provide about physical reality. The problem caught Schrödinger's attention as well: while he agreed with EPR about their description of correlations of spatially separated systems, he rejected the conclusion about the incompleteness of quantum mechanics. Rather, in his letters [65, 66], Schrödinger suggested that such a behavior was the actual working scheme of quantum reality. To describe this, he introduced the term *entanglement*, defining it as the [...] *the characteristic trait of quantum mechanics*. More specifically, Schrödinger stresses his focus on the fact that the knowledge of the composite system $A \cup B$ does not imply information on its individual constituent subsystems despite being spatially far apart, thus, in principle, possibly known on their own.

However, it was not until the second half of the XXth century that a formal theory, and definition, of entanglement has been developed [67].

The key ingredient, allowing to correctly interpret Schrödinger's argument to EPR's work is the concept of **separability** of a bipartite state. We consider two spatially separated users, Alice (A) and Bob (B): a bipartite state $\hat{\rho}_{AB}$ is said to be **separable** if and only if (iff) it can be generated by means of a *local operations and classical communication* (**LOCC** protocol), i.e. the following conditions hold:

Definition 2.2.1. Local Operations and Classical Communication (LOCC) protocol:

- The two parties can locally generate and manipulate quantum states remaining spatially separated;
- Alice and Bob are allowed to communicate and exchange information via classical communication channels.

Any (bipartite) state generated via such a protocol will be of the form [68]

$$\hat{\rho}_{AB} = \sum_i q_i \hat{\rho}_A^{(i)} \otimes \hat{\rho}_B^{(i)}, \quad (2.3)$$

where $\hat{\rho}_{AB}$ refer to the quantum state generated and manipulated by, respectively, Alice and Bob, whereas q_i denotes the statistical weight¹ attributed to the i -th combination of states generated by Alice and Bob.

Whenever the quantum state Alice and Bob share, i.e. it cannot be expressed as in Eq. (2.3), Alice's and Bob's subsystems are said to be **entangled** (or, equivalently, the quantum state describing the joint Alice's and Bob's system is said to be entangled). Under the assumption of pure bipartite states, the following decomposition must hold

$$|\psi\rangle_{AB} = \sum_{i,j} c_{ij}^{(AB)} |i\rangle_A |j\rangle_B = \sum_{i,j} c_i^{(A)} c_j^{(B)} |i\rangle_A |j\rangle_B. \quad (2.4)$$

To put it differently, for a separable state the coefficients of the expansion in eq. (2.4) are factorized as

$$c_{ij}^{(AB)} = c_i^{(A)} c_j^{(B)} \quad \forall c_i, c_j, c_{ij}, \quad (2.5)$$

i.e. the matrix of coefficients $\{c_{ij}^{(AB)}\}_{i,j}$ must have rank 1 [12].

Indeed, by recalling that $\sum_i c_i^{(\alpha)} |i\rangle_\alpha = |\phi_\alpha\rangle$ with $\alpha = A, B$, then Eq. (2.5) now reads

$$|\psi_{AB}\rangle = |\phi_A\rangle |\phi_B\rangle \rightarrow \hat{\rho}_{AB} = |\phi_A\rangle \langle \phi_A| \otimes |\phi_B\rangle \langle \phi_B| = \hat{\rho}_A \otimes \hat{\rho}_B. \quad (2.6)$$

In the case Alice and Bob perform local operations $\hat{A}_x = \sum_a a \hat{\Pi}_{a|x}^{(A)}$ and $\hat{B}_y = \sum_b b \hat{\Pi}_{b|y}^{(B)}$ with setting, respectively, x and y , the joint probability distribution of the measurement outcomes a and b for a separable state (2.3) is

$$p(a, b|x, y) = \sum_i q_i \text{Tr}(\hat{\Pi}_{a|x}^{(A)} \hat{\rho}_i^{(A)}) \text{Tr}(\hat{\Pi}_{b|y}^{(B)} \hat{\rho}_i^{(B)}) = \sum_i q_i p_i(a|x) p_i(b|y). \quad (2.7)$$

¹ $\sum_i q_i = 1$, $q_i \geq 0 \forall i$ so that eq. (2.3) actually describes a density operator.

Eq.(2.7) highlights that, for separable states, the joint probability distribution of measurement outcomes a and b can be fully explained via classical statistics. In other words, correlations between Alice's and Bob's measurement outcomes can be reproduced via classical randomness.

In his letter [69], Schrödinger proves that, in an EPR setting, probabilities as in Eq. (2.7) cannot be retrieved, regardless the spatial and temporal separation of the two parties. Quantum mechanics, in fact, concerns non-separable states, challenging the realism and locality conditions EPR were addressing.

Nowadays, a way more exhaustive theory of entanglement exists, such as the possibility of having entanglement among more than two parties (c.f. *multipartite entanglement* [68,70]), with several methods to certify the non-separability of multipartite quantum states [71–75].

Besides its fundamental interest, quantum entanglement proved to be an invaluable resource for several practical applications, being at the basis for the celebrated *quantum state teleportation* [76] and its evolutions, quantum communication [77,78], as well as quantum algorithms [79–84] and quantum metrology.

2.2.2 Bell non-locality

A major breakthrough in the investigation of the foundations of quantum mechanics comes from John Stuart Bell. In his seminal paper [85] published in 1964, the author shines a new light on the original EPR work, addressing, specifically, the concept of "completeness": as a consequence of the impossibility of associating every element of the physical reality to a suitable theoretical counterpart, EPR conjectured about the existence of some *hidden variables* which would restore the desired features of causality and locality in quantum mechanics.

Bell consider a very similar setting to Bohm's: two physical systems are generated by the same source, and are then sent to two distant parties, Alice and Bob, as represented in Fig. 2.1.

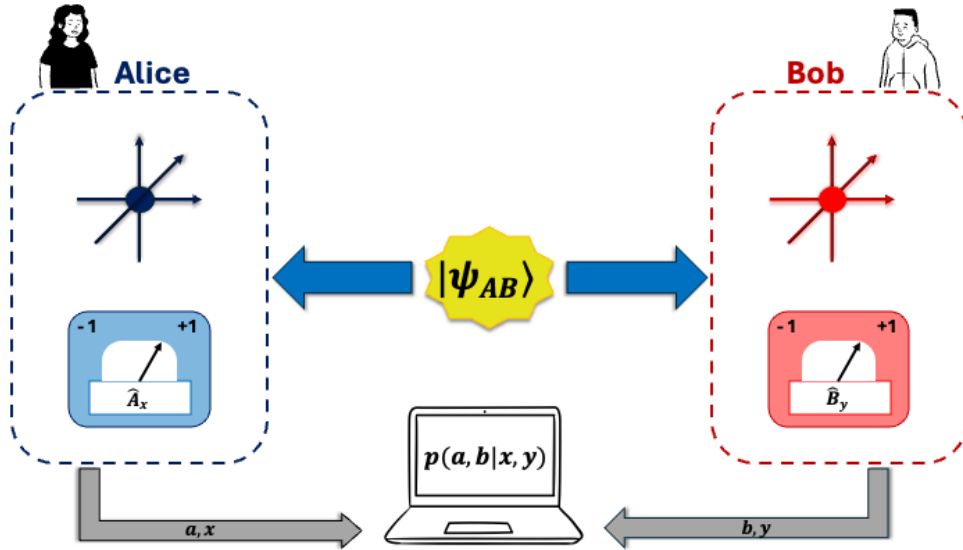


Figure 2.1: Scheme of the conceptual experiment proposed by Bell [85]: two quantum subsystems are sent to distant parties, Alice and Bob, who can perform, respectively, local measurements $\hat{A}_x$ and $\hat{B}_y$, whose outcomes are $a = \pm 1$, $b = \pm 1$. Information arising from measurements is used to infer the joint probability distribution of experimental outcomes, possibly depending on some "hidden variable". In the original Aharonov-Bohm's formulation of the EPR problem [86], a spin-1/2 bipartite state (2.1) is shared between two distant users, who can perform local spin measurements $\hat{S}_i^{(j)} = \hbar/2\hat{\sigma}_i^{(j)}$, where $j = A, B$ and $\hat{\sigma}_i$ refer to the Pauli matrices.

Alice can single out one measurement, labelled by the index x , to perform on her subsystem. Likewise, Bob chooses one observable, labelled by the index y . The measurement outcomes on Alice's and Bob's sides are referred to as, respectively, a and b . These outcomes are ruled by a joint probability distribution $p(a, b|x, y)$. It may happen that experimental results on both sides are not statistically independent of each other

$$p(a, b|x, y) \neq p(a|x)p(b|y).$$

The idea of a *local* theory can be formalized by implying that a set of past events, represented by the hidden variable λ , is able to condition the current measurement results on both Alice's and Bob's side, as well as fully accounting for the mutual dependence between a and b . The residual indeterminacies are then decoupled by factoring the joint probability distribution:

$$p(a, b|x, y, \lambda) = p(a|x, \lambda)p(b|y, \lambda). \quad (2.8)$$

Alternatively said, Eq. (2.8) states that the measurement outcome of each party depends exclusively on the choice of the local measurement performed and on the value of the (hidden) variable λ , being independent from the measurement performed by the distant party.

Assuming that the hidden variable takes its values according to a probability distribution $q(\lambda)$, it is possible to write

$$p(a, b|x, y) = \int_{\Lambda} d\lambda q(\lambda) p(a|x, \lambda) p(b|y, \lambda). \quad (2.9)$$

Any experiment whose outcomes' statistics can be described as in Eq. (2.9) is said to admit a **local hidden variable (LHV)** representation. Whenever such a description is untenable, the system is said to be **(Bell) non-local** [87]. In order to investigate whether quantum mechanics could admit a LHV representation, Bell considered a bipartite state of the form (2.1), and Alice and Bob performing local measurements $\hat{A}$ and $\hat{B}$, with values

$$\begin{aligned} a(x, \lambda) &= \{-1, +1\} & \forall x, \forall \lambda; \\ b(y, \lambda) &= \{-1, +1\} & \forall y, \forall \lambda. \end{aligned} \quad (2.10)$$

The correlator between Alice's and Bob's measurement outcomes is given by

$$C(x, y) = \int_{\Lambda} d\lambda q(\lambda) a(x, \lambda) b(y, \lambda). \quad (2.11)$$

If a third measurement setting is chosen, then Eq. (2.11) reads

$$C(x, y) - C(x, y') = \int_{\Lambda} d\lambda q(\lambda) a(x, \lambda) (b(y, \lambda) - b(y', \lambda)). \quad (2.12)$$

Given the perfect correlation nature of the singlet state (2.1), whenever Alice and Bob share the same measurement setting, their measurement outcomes will be $b(y, \lambda) = -a(y, \lambda)$, $\forall y, \forall \lambda$. By plugging this latter result in Eq. (2.12), the following inequality holds:

$$|C(x, y) - C(x, y')| \leq \int_{\Lambda} d\lambda q(\lambda) |a(y, \lambda) - a(y', \lambda)| \quad (2.13)$$

Moreover, given Eq. (2.10), then $|a(y, \lambda) - a(y', \lambda)| = 1 - a(y, \lambda)a(y', \lambda) = 1 + a(y, \lambda)b(y', \lambda)$. Therefore the following inequality is retrieved

$$|C(x, y) - C(x, y')| \leq 1 + C(y, y') \quad \forall x, y, y' \quad (2.14)$$

where $C(y, y') = \int_{\Lambda} d\lambda q(\lambda) a(y, \lambda) b(y', \lambda)$. Eq. (2.14) is the celebrated **Bell inequality** (in its original formulation) which must be abide by any LHV theory.

It is trivial to retrieve, from Eq. (2.14) and Eq. (2.10), that

$$S = |C(x, y) - C(x, y')| \leq 2 \quad \forall x, y, z. \quad (2.15)$$

Bell's work is widely recognized among the turning point of quantum mechanics, providing relevant arguments concerning its fundamental nature, having inspired several further advancements, both theoretical and experimental.

A crucial contribution has been provided by J.F. Clauser, M.A. Horne, A. Shimony and R.A. Holt who, in 1969, published their milestone paper [88], extending the applicability of the original Bell's work [85].

More specifically, addressed the (in)suitability of a LHV description with no assumption of perfect correlation between the measurement of the two parties. This can be

done by considering an other measurement setting x' such that $C(x, x') = 1 - \delta$, with $0 \leq \delta \leq 1$. Furthermore, the domain Λ of λ is split into two regions $\Lambda_{\pm}$ such that $\Lambda_{\pm} = \{\lambda \in \Lambda | a(x', \lambda) = b(y', \lambda)\}$. Thus

$$\int_{\Lambda} d\lambda q(\lambda) b(y, \lambda) b(y', \lambda) = \int_{\Lambda} d\lambda q(\lambda) a(x', \lambda) b(y', \lambda) - 2 \int_{\Lambda^-} d\lambda q(\lambda) a(x', \lambda) b(y', \lambda). \quad (2.16)$$

Given Eq. (2.10), by noting that the first integral of the right-hand side of Eq. (2.16), it follows that

$$\int_{\Lambda} d\lambda q(\lambda) b(y, \lambda) b(y', \lambda) \geq C(x', y') - \delta, \quad (2.17)$$

since $\int_{\Lambda_{\pm}} d\lambda q(\lambda) = \frac{\delta}{2}$.

Finally, by combining Eq. (2.14) with Eq. (2.17) and some algebra, the celebrated **Clauser-Horne-Shimony-Holt (CHSH) inequality** is retrieved

$$|S| = |C(x, y) + C(x', y) + C(x', y') - C(x, y')| \leq 2. \quad (2.18)$$

Like the original Bell inequality (2.14), any violation of the CHSH inequality (2.18) signals the insuitability of a LHV model. However, compared to the original version, Eq. (2.18) does not require constraints about possible (anti-) correlations between Alice's and Bob's measurement outcomes, at the price of a slightly more complex arrangement (an additional observable is required).

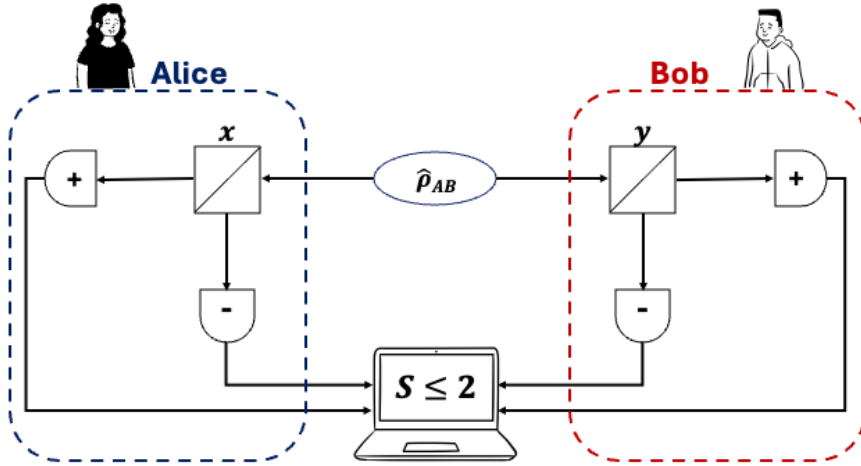


Figure 2.2: Scheme of the CHSH experiment.

If the singlet state (2.1) (with a more general notation $|\uparrow\rangle = |0\rangle$ and $|\downarrow\rangle = |1\rangle$) is used, and the following observables $\hat{A}_0 = \hat{Z}_A$, $\hat{A}_1 = \hat{X}_A$, $\hat{B}_0 = \frac{\hat{X}_B - \hat{Z}_B}{\sqrt{2}}$ and $\hat{B}_1 = -\frac{\hat{X}_B + \hat{Z}_B}{\sqrt{2}}$ are plugged into the CHSH inequality (2.18) the following result is retrieved:

$$|S| = \left| \langle \hat{A}_0 \otimes \hat{B}_0 \rangle + \langle \hat{A}_1 \otimes \hat{B}_1 \rangle + \langle \hat{A}_1 \otimes \hat{B}_0 \rangle - \langle \hat{A}_0 \otimes \hat{B}_1 \rangle \right| = 2\sqrt{2} > 2. \quad (2.19)$$

Indeed, being a violation of the Bell inequality, Eq. (2.19) states the impossibility to reproduce the joint measurement statistics of such an arrangement with a LHV model (2.9), thus highlighting the intrinsic *nonlocal* character of quantum mechanics. There are three other states whose Bell parameter S is equal to $2\sqrt{2}$ as in Eq. (2.19):

$$\begin{aligned} |\psi_{AB}^{\pm}\rangle &= \frac{|0\rangle_A |1\rangle_B \pm |1\rangle_A |0\rangle_B}{\sqrt{2}} \\ |\phi_{AB}^{\pm}\rangle &= \frac{|0\rangle_A |0\rangle_B \pm |1\rangle_A |1\rangle_B}{\sqrt{2}}. \end{aligned} \quad (2.20)$$

These latter states implement the maximal violation of the CHSH inequality (2.18) for bipartite systems, and became popular in the 1980s and 1990s under the collective name of **Bell states**.

Quantum non-locality and states violating Bell inequalities proved to be a key ingredient to investigate the foundations of quantum mechanics. Nevertheless, they are an invaluable resource for several practical applications in quantum technologies, ranging from quantum communications [77], to quantum sensing, to quantum algorithms.

The experimental violation of the Bell inequality earned A. Aspect, J. Clauser and A. Zeilinger the Nobel Prize for Physics in 2022 [88, 89].

2.2.3 Quantum steering

An other milestone in the investigation of the EPR paradox is the paper [90] by H.M. Wiseman, S.J. Jones and A.C. Doherty, in which the authors formalized the capability of one party to manipulate (to *steer*) (by means of the choice of the measurement setting) the state of the other party at a distance, a concept introduced by Schrödinger in [66]. More precisely, whenever Alice performs a local measurement on her subsystem and communicates her measurement outcome and setting to Bob, he is left with a collection, namely, a **quantum assemblage**, of quantum states conditioned by the information Alice provided. Correlations between Alice's measurements and the occurrence of a given Bob's state could be, in principle, reproduced by classical resources, by exploiting a **Local Hidden State (LHS)** model

$$\hat{\rho}_{a|x} = \int_{\Lambda} d\lambda p(a|x, \lambda) q(\lambda) \hat{\sigma}(\lambda) = p(a|x) \int_{\Lambda} d\lambda p(\lambda|a, x) \hat{\sigma}(\lambda). \quad (2.21)$$

Remarkably, these two representations (whose equivalence can be easily proved whenever the choice of the measurement setting x is independent of the parameter λ) address two different interpretations:

- the first one, the original one proposed by Wiseman, Jones and Doherty, concerns a simulation task in which Alice tries to reproduce the assemblage $\{\hat{\rho}_{a|x}, P(a|x)\}_{a,x}$, by sampling the states $\hat{\sigma}(\lambda)$ according to the probability distribution $q(\lambda)$. Simultaneously, she announces an outcome a conditioned to the measurement setting x and a hidden variable λ . Consequently, Bob has no basis to believe that the initial state shared with Alice was quantumly correlated;
- the second representation can be formulated as a Bayesian update task, in which the probability distribution $q(\lambda)$ is updated into $p(\lambda|a, x)$ upon learning the outcome a and the measurement setting x . In such an interpretation, Bob is not required to believe Alice has control over his state, with her measurement simply providing him classical information about the distribution of the hidden states $\hat{\sigma}(\lambda)$ [91].

In both cases, $\hat{\sigma}(\lambda)$ denote the hidden states Alice employs to try to fool Bob.

Whenever a representation as in Eq. (2.21) fits the description of Bob's quantum assemblage, then post-measurement states $\hat{\rho}_{a|x}$ can be reproduced by using classical randomness and local quantum states. The bipartite state $\hat{\rho}_{AB}$ the two parties share is therefore said to be **unsteerable**. Conversely, Bob must believe that Alice can actually steer his own subsystem via some "action at a distance". In this case, $\hat{\rho}_{AB}$ is said to be **steerable**, and the correlation between Alice and Bob is referred to as **quantum steering**.

Of course, the no-signaling condition of quantum theory imposes that

$$\sum_a p(a|x) \hat{\rho}_{a|x} = \hat{\rho}_B, \quad (2.22)$$

i.e. the reduced state on Bob's side cannot depend on Alice's measurement setting.

An alternative definition of quantum steering relies on the joint outcome statistics of Alice's and Bob's measurement outcomes [90–92]: a measurement strategy applied by one party, such as Alice, on a bipartite state $\hat{\rho}_{AB}$ exhibits quantum steering iff the joint probabilities $p(a, b|x, y)$ **cannot** be written as

$$p(a, b|x, y) = \int_{\Lambda} d\lambda q(\lambda) p(a|x, \lambda) \text{Tr}(\hat{\sigma}(\lambda) \hat{\Pi}_{b|y}^B) = \text{Tr}(\hat{\rho}_{a|x} \hat{\Pi}_{b|y}^B), \quad (2.23)$$

for all outcomes $a \in \hat{A}_x, b \in \hat{B}_y$ and all measurement settings x, y . The latter definition of LHS model highly resembles the one of separability (2.7) and LHV theories (2.9); however, the probability $p(a|x, \lambda)$ in Eq. (2.23) denotes a general response function possessed by Alice (i.e., no assumptions have been made on her experimental setting), whereas probabilities of Bob's measurement outcomes are calculated according to Born's rule $p(b|y) = \text{Tr}(\hat{\sigma}(\lambda) \hat{\Pi}_{b|y}^B)$.

Notably, unlike quantum entanglement and Bell nonlocality, quantum steering is inherently *asymmetric* between the two end users (Alice and Bob), concerning the capability of one party to make the state of the other party collapse via a local measurement. Such an intrinsic asymmetry proves to be a pivotal feature to characterize quantum channels, as it will be discussed in the next section.

2.2.4 Hierarchy of quantum correlations

Quantum entanglement, quantum steering and Bell non-locality are widely recognized among the most peculiar traits of quantum mechanics, possibly addressing the *spooky action at a distance* Einstein was used to refer to. These three phenomena were discussed and formalized in different works [66, 69, 85] addressing some loopholes left open by the original EPR paper [62] (or the Aharonov-Bohm [64] formulation of the EPR paradox). However, despite being deeply bonded and, to some extent, similar, there are peculiar differences among the three aforementioned correlations. It was not until 1989, when Werner published a manuscript [67] shedding a new light on such peculiar quantum effects. Here, he introduces the celebrated **Werner states**. For a two-qubit system, a common writing is:

$$\hat{\rho}_{AB} = p |\psi_{AB}^-\rangle \langle \psi_{AB}^-| + \frac{1-p}{4} \mathbb{1}_{AB} \quad p \in [0, 1], \quad (2.24)$$

where $|\psi_{AB}^-\rangle$ identifies the singlet state (2.20), while $\mathbb{1}_{AB}$ is the identity operator. Eq. (2.24) shows that for $p = 0$ Werner state reduces to the fully mixed state $\mathbb{1}_{AB}/4$, being thus completely separable. Conversely, for $p = 1$ the state (2.24) collapses into a pure singlet state (2.20), violating Bell inequalities, as discussed in paragraph 2.2.2, as well as not admitting a separable-state representation (2.4), being therefore an entangled state. Moreover, it can be proved that, for $p \leq 1/3$, Werner state (2.24) is separable. Conversely, as soon as $p > 1/3$, it becomes entangled. Indeed, this property suggests that **entanglement can be activated by tuning the ratio p of fully entangled and mixed state**. However, the Werner state (2.24) violates Bell inequalities if and only if $p > 1/\sqrt{2}$. Indeed, whenever $1/3 < p \leq 1/\sqrt{2}$, it shows entanglement without violating any Bell inequality. This result highlights a fundamental difference between quantum entanglement and Bell non-locality, stating that [87]

Theorem 1. *Quantum entanglement is a necessary but not sufficient condition in order to obtain (Bell) non-local correlations through measurement on a given quantum state.*

A graphical interpretation is presented in Fig. 2.3.

Furthermore, in their work [90], Wiseman et al., after having formally defined quantum steering, showed that Werner states feature a threshold after which the state becomes steerable. For a two-qubit state such a value reads $p > 1/2$. As a result, whenever $1/2 < p \leq 1/\sqrt{2}$ the Werner state (2.24) is entangled, becomes steerable, still it does not violate any Bell inequality:

Theorem 2. *A measurement strategy applied by one party capable of steering the state of the other partner is a necessary condition to retrieve Bell non-local correlations. However, steerability does not grant the unsuitability of LHV descriptions.*

Consequently, **Bell non-locality is a stricter condition than steerability, being again stricter than non separability**. Such hierarchy of quantum correlations updates Fig. 2.3 into Fig. 2.4.

The conditions for Werner states showcasing the hierarchy of quantum correlations are summarized in Fig. 2.5.

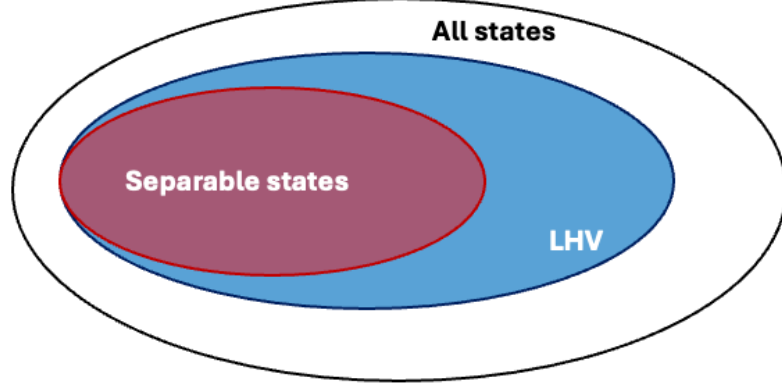


Figure 2.3: Euler-Venn diagram of the hierarchy of quantum correlations. The hierarchy is expressed in terms of separability-LHV model. By looking at Eqs. (2.7) and (2.9), it follows that separability condition implies the existence of a LHV model, with the other way around not necessarily being true.

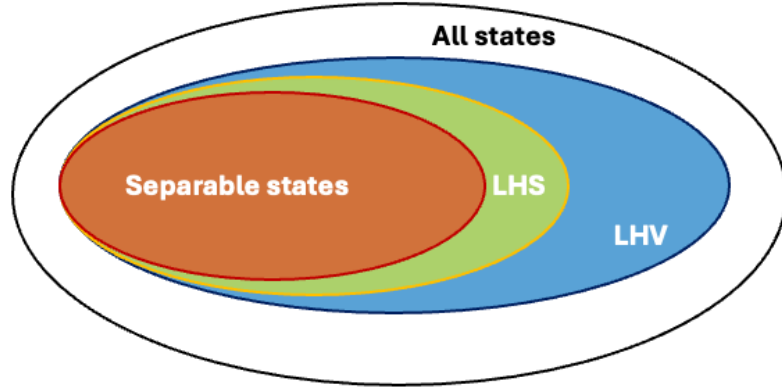


Figure 2.4: Updated version of the Euler-Venn diagram presented in Fig. 2.3, now accounting for LHS models as well, as an intermediate condition between the looser LHV description, and the stricter separability condition.

Since quantum entanglement, Bell non-locality and quantum steering are defined according to the unsuitability of, respectively, a separable, LHV and LHS model, it is desirable to establish a hierarchy for these latter conditions.

More specifically, in terms of probabilities, it is easy to figure that the joint measurement outcome statistics for a LHV model (2.9) can be retrieved from a LHS model (2.23), via the position $p(b|y, \lambda) = \text{Tr} \left(\hat{\Pi}_{b|y}^B \hat{\sigma}(\lambda) \right)$. This latter result suggests that whenever a classical (LHV) description suits the model, then it is always possible to retrieve a theory concerning one party (e.g. Bob) is characterized by a quantum response function conditioned by the classical information the other party (i.e. Alice) supplies. This is nothing but the definition of LHS theory described in sec. 2.2.3.

However, since steerability is usually asymmetric, it is not given that the existence of a LHS theory implies a LHV model:

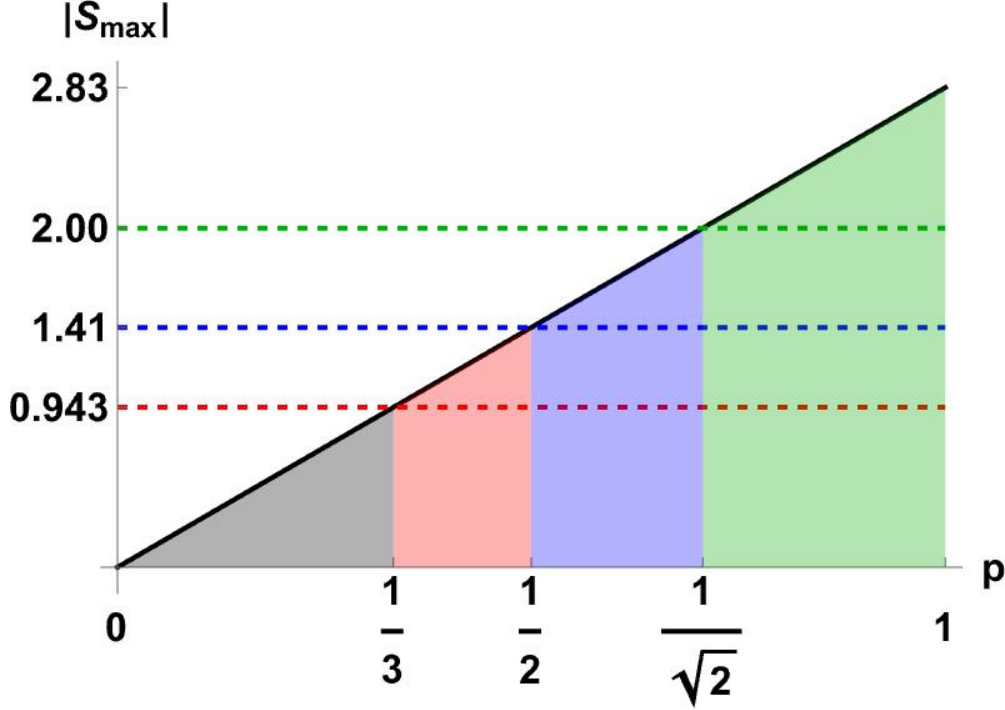


Figure 2.5: Plot of the maximal value of the Bell parameter $|S_{max}|$ of a Werner state (2.24) as a function of the ratio between the completely pure and the completely mixed state p . The grey shaded region $0 \leq p \leq 1/3$ corresponds with the condition in which the fully mixed part is dominant enough to make the Werner state separable. Conversely, the red shaded area $1/3 < p \leq 1/2$ represents the condition in which the Werner state (2.24) exhibits entanglement, but admits a LHS description, not violating, consequently, any Bell inequality. Subsequently, the blue shaded region $1/2 < p \leq 1/\sqrt{2}$ is associated with the capability of Alice to steer the state at Bob's location, with a LHV theory still describing the Werner state. In the end, the green shaded region $1/\sqrt{2} < p \leq 1$ corresponds to the situation in which the Werner state (2.24) is Bell non-local.

$$\text{LHV} \implies \text{LHS}. \quad (2.25)$$

Likewise, whenever Alice performs the measurement of a local observable $\hat{A}$ in the setting x and retrieves the outcome a on a separable state (2.3), the reduced state on Bob's side is:

$$\hat{\rho}_{a|x}^B = \text{Tr}_A \left(\sum_i q_i \hat{\Pi}_{a|x}^A \hat{\rho}_i^A \otimes \hat{\rho}_i^B \right) = \sum_i q_i \text{Tr} \left(\hat{\Pi}_{a|x}^A \hat{\rho}_i^A \right) \hat{\rho}_i^B = \sum_i q_i p_i(a|x) \hat{\rho}_i^B, \quad (2.26)$$

which corresponds to the definition of LHS assemblage (2.21). However, it is possible that some quantum states do admit a LHS representation albeit being non-separable. Indeed

$$\text{LHS} \implies \text{separability}. \quad (2.27)$$

By combining Eqs. (2.25) and (2.27) it is possible to state that

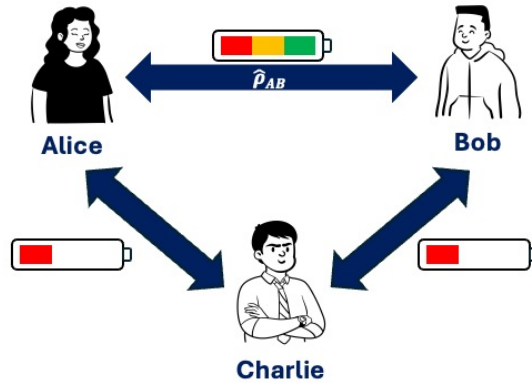
$$\text{LHV} \implies \text{LHS} \implies \text{separability}, \quad (2.28)$$

as depicted in Fig. 2.4.

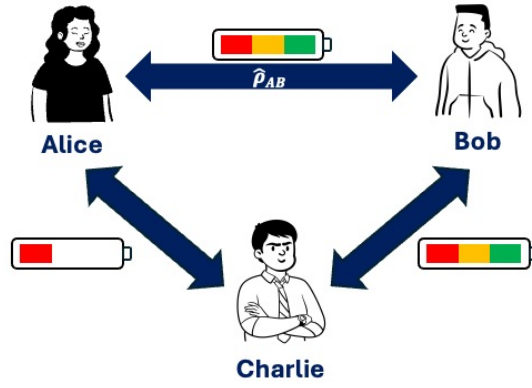
The equivalent hierarchy of quantum correlations is therefore

$$\text{Bell non-locality} \subset \text{quantum steering} \subset \text{quantum entanglement}. \quad (2.29)$$

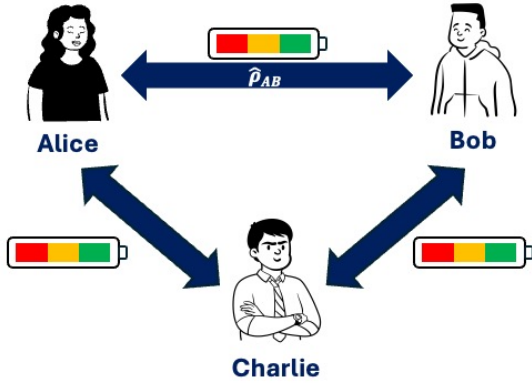
Furthermore, in 2007, Jones, Wiseman and Doherty presented the definition of quantum correlation via an operational quantum information task [93], in which the hierarchy (2.29) is used to certify the degree of trust of the nodes of a quantum network.



(a)



(b)



(c)

Figure 2.6: Definition of quantum correlations as an informational task: a) Bell non-locality, b) quantum steering, c) quantum entanglement. In each picture is reported the level of trust across the nodes.

More specifically, the general setting involves three parties: Alice, Bob and Charlie, who acts as a certifier (see Fig. 2.6). Alice and Bob can arrange a shared bipartite state and measure their respective subsystem at will. Alice and Bob's task (who are allowed to communicate exclusively during the state preparation) is to convince the certifier (whom they are allowed to communicate with) that they share a genuinely entangled state.

According to the level of trust of Charlie with respect to Alice and Bob, who mutually trust themselves, three different scenarios can be identified:

- Charlie does not trust Alice nor Bob. In such a case, whenever correlations between the two parties can be described via a LHV theory, Charlie will not accept Alice's and Bob's claim of having a quantumly correlated state; with their result possibly being retrieved from purely classical randomness. Otherwise, Charlie must believe the two parties share an entangled state. Consequently, Alice and Bob fulfill their task iff they can assess Bell non-locality. Such a task defines, indeed, an operational definition of the violation of Bell inequality;
- Charlie trusts only one party (e.g. he trusts Bob but not Alice). Here, as long as correlations can be explained by adopting a LHS model for Bob, Charlie will reject the claim of Alice and Bob sharing an entangled state. Therefore, in order to accept such a statement, Alice must prove to be able to steer the state at Bob's location. Remarkably, this setting is equivalent to a two-party setting in which Bob does trust himself (i.e. his experimental arrangement) but he does not trust Alice;
- Charlie does trust both Alice and Bob. Given this context, it is sufficient for Alice and Bob to prove Charlie that they share a non-separable state, e.g., via a quantum state tomography. Noteworthy, since there is mutual trust between Alice and Bob, and Charlie trusts both of them, they can freely communicate results one another, this is equivalent to a *one* party task.

2.3 Metrology-assisted certification of quantum steering

The presence of quantum steering in a bipartite system can be certified by reconstructing suitable witnesses, similarly to what is usually done for Bell nonlocality or quantum entanglement. The common ground for all of these criteria is the construction of suitable correlators, comparing them with a bound T_{LHS} holding for unsteerable states; namely

$$\left| \langle \hat{Q} \rangle \right| = \left| \sum_i w_i \langle \hat{A}_i \otimes \hat{B}_i \rangle \right| \leq \sum_i w_i \left| \langle \hat{A}_i \otimes \hat{B}_i \rangle \right| \leq T_{LHS}. \quad (2.30)$$

Criteria expressed as in Eq. (2.30) are usually called *linear convex (steering) criteria*, since the left-hand side is a linear convex combination of the correlators $\langle \hat{A}_i \otimes \hat{B}_i \rangle$. For two-qubit system and Pauli operators, the steering criterion (2.30) for LHS theories imposes $T_{LHS} = \sqrt{3}$ [91, 94]. Any violation of such an inequality states that a LHS description is forbidden, thus assessing the presence of quantum steering; for a singlet state ($|\psi^-\rangle$ of (2.20)) and Pauli measurements on both Alice's and Bob's side the linear steering criterion (2.30) can reach $\left| \langle \hat{Q} \rangle \right| = 3 \geq \sqrt{3}$, flagging the presence of quantum steering.

Another approach to certify the presence of quantum steering, proposed well before the formal definition of quantum steering in the contest of the EPR paradox, relies on uncertainty relations resembling the Heisenberg uncertainty inequality. In her work [95], Margareth Reid retrieves an uncertainty inequality holding for LHS models in terms of quadrature-like operators (very much inspired by the original formulation of the EPR argument [62]). However, the very same argument can be used to retrieve uncertainty relations valid for qubits [96, 97]. The general scenario resembles Bohm's formulation of the EPR setting: a bipartite state $\hat{\rho}_{AB}$ is shared by two end users, Alice and Bob, who can perform local measurements. After measuring her observable $\hat{K}$ with setting x , Alice communicates information about her measurement outcome and setting to Bob, who exploits it to build up a suitable estimator $h_{est}(k)$ to predict the result of the measurement of a local observable $\hat{H} = \sum_h h |h\rangle \langle h|$ on his side. The average discrepancy between Bob's prediction and actual result is quantified by the **inference variance**

$$\Delta^2 H_{est} = \sum_{h,k} p(k, h|x, y) (h_{est}(k) - h)^2, \quad (2.31)$$

with y being the chosen setup for Bob's measurement.

The optimal estimator Bob can use is the quantum average $h_{est}^{best}(k) = \text{Tr}(\hat{H}\hat{\rho}_{k|x})$ over the states forming his assemblage, leading to the following bound

$$\Delta^2 H_{est} \geq \sum_k p(k|x) \text{Var}[\hat{\rho}_{k|x}, \hat{H}] = \sum_k p(k|x) \Delta^2 H[\hat{\rho}_{k|x}], \quad (2.32)$$

where $\text{Var}[\hat{\rho}_{k|x}, \hat{H}] = \langle \hat{H}^2 \rangle_{\hat{\rho}_{k|x}} - \langle \hat{H} \rangle_{\hat{\rho}_{k|x}}^2$ denotes the quantum variance, whereas

$$\text{Var}_{B|A} H = \Delta_{B|A}^2 H = \sum_k p(k|x) \Delta^2 H[\hat{\rho}_{k|x}] \quad (2.33)$$

is the (quantum) **conditional variance**. For any pair of non-compatible observables $\hat{H}$ and $\hat{G}$, the **Reid's criterion** states that [96]

$$\Delta_{B|A}^2 H \Delta_{B|A}^2 G \geq \Delta_{\min}^2 H \Delta_{\min}^2 G \geq \frac{|\langle [\hat{H}, \hat{G}] \rangle_{\hat{\rho}_B}|^2}{4}, \quad (2.34)$$

where the conditional variances are expressed as in Eq. (2.33), while $\Delta_{\min}^2 H$, $\Delta_{\min}^2 G$ are the optimization of the conditional variances of the corresponding observables over all the possible Alice's settings.

2.3.1 The Yadin-Fadel-Gessner (YFG) approach

From a quantum information theory outlook, Reid's inequality (2.34) relies on a LHS description of Bob's assemblage. Therefore, any violation of Eq. (2.34) witnesses Alice's capability of steering the state at Bob's location.

A new approach, built upon Reid's criterion, to certify the presence of quantum steering in a bipartite state has been proposed in 2021 by B. Yadin, M. Fadel and M. Gessner in [60], who formulated the problem of assessing the unsuitability of LHS description as a metrological task.

The cornerstone of the protocol is the complementarity principle of quantum mechanics from the perspective of quantum metrology. The key assumption is that a generic quantum observable $\hat{G}$ can be seen as the generator of a local parameter θ , imparted on Bob's subsystem via a unitary map $\hat{U}(\theta) = e^{-i\hat{G}\theta}$. The precision bound on the estimation of the parameter θ encoded in Bob's system is established from the metrological power of the quantum state used as a probe, conditioned on the information Alice communicates. Accordingly, Bob will choose his observable as a function of the assemblage function $\mathcal{A}(k, x) = p(k|x)\hat{\rho}_{k|x}$ so as to approach the maximal information $f_Q[\hat{\rho}_{k|x}, \hat{G}]$ on the parameter θ . With such a strategy, the average sensitivity Bob can achieve in his estimation will match the **conditional quantum Fisher information**

$$f_Q^{B|A}[\hat{\mathcal{A}}, \hat{G}] = \sum_k p(k|x) f_Q[\hat{\rho}_{k|x}, \hat{G}]. \quad (2.35)$$

By adopting a LHS description (the second form presented in Eq. (2.21)) for Bob's assemblage, the conditional QFI can be upper bounded as follows [60]:

$$\begin{aligned} f_Q^{B|A}[\hat{\mathcal{A}}, \hat{G}] &= \sum_k p(k|x) f_Q \left[\int_{\Lambda} d\lambda p(\lambda|k, x) \hat{\sigma}(\lambda), \hat{G} \right] \\ &\leq \max_x \sum_k p(k|x) \int_{\Lambda} d\lambda p(\lambda|k, x) f_Q[\hat{\sigma}(\lambda), \hat{G}] = \int_{\Lambda} d\lambda q(\lambda) f_Q[\hat{\sigma}(\lambda), \hat{G}], \end{aligned} \quad (2.36)$$

where the convexity of the FI, the maximization of the FI, the Bayesian update rule $p(\lambda|k, x) = q(\lambda)p(k|x, \lambda)/p(k|x)$ and the completeness condition $\sum_k p(k|x, \lambda) = 1 \forall x, \forall \lambda$ have been used.

With a the very same pattern, by exploiting the concavity property of the variance, we

can retrieve the following bound for the conditional variance:

$$\Delta_{B|A}^2 G = \sum_k p(k|x) \Delta^2 G \left[\int_{\Lambda} d\lambda p(\lambda|k, x) \hat{\sigma}(\lambda) \right] \quad (2.37)$$

$$\geq \min_x \int_{\Lambda} d\lambda \sum_k p(k|x) p(\lambda|k, x) \Delta^2 G[\hat{\sigma}(\lambda)] = \int_{\Lambda} d\lambda q(\lambda) \Delta^2 G(\lambda), \quad (2.38)$$

where, for the sake of brevity, it has been written $\Delta^2 G[\hat{\sigma}(\lambda)] = \Delta^2 G(\lambda)$. Here, by inserting the bound (2.38) into Eq. (2.37), and by recalling the general result $f_Q[\hat{\rho}, \hat{G}] \leq 4\Delta^2 G$ the main result of YFG's paper [60] is retrieved:

$$f_Q^{B|A}[\hat{A}, \hat{G}] \leq 4\Delta_{B|A}^2 G. \quad (2.39)$$

Hence, the combination of Eq. (2.39) with the QCRB $1 \leq N\Delta^2 \theta f_Q$ leads to the **Yadin-Fadel-Gessner (YFG) inequality**

$$\Delta^2 \theta \Delta_{B|A}^2 G \geq \frac{1}{4N}, \quad (2.40)$$

holding for any unsteerable state. Therefore, any violation of Eq. (2.40) flags out the presence of quantum steering.

Compared to Reid's type criteria (2.34) an N -sample average of the observable $\hat{H}$ is mapped into a N -size estimation of the parameter θ encoded in the bipartite $\hat{\rho}_{AB}$.

2.3.2 Working with limited resources

YFG's approach consists in a metrological-task formulation of the EPR problem, leading to a metrological equivalent of the uncertainty-inequality-based witnessing of quantum steering.

However, a direct assessment of the YFG method via the Fisher information demands a sufficiently large amount of resources in order for the CRB to be approached. In different terms, a large number of copies of the (possibly) steerable state under exam is needed for a satisfactory reconstruction of the Fisher information from measurement data.

This latter requirement poses an unavoidable limit for the use of the metrology-assisted approach on practical quantum network scenarios, with the two main reasons being:

- The majority of the available resources should be addressed to the specific task the network is operating for;
- The CRB becomes progressively tighter as the number N of repetition grows (or, equivalently, the number of probes increases). Whenever resources are insufficient to neglect significant deviations of the parameter θ from its expected value, finite-size effects should be accounted for. Nonetheless, it is generally not appropriate to assume that all the information on the unknown parameter arises from measurement outcomes.

Given that, new figures of merit, providing more relevant information in the finite-dataset regime than the standard Fisher information should be adopted. A viable solution is embracing the Bayesian estimation framework, and replacing the Fisher information with the **Van Trees information** [98, 99]

$$V(N) = \int_{\Theta} d\theta \mathcal{P}(\theta) f(\theta) + \frac{1}{N} \int_{\Theta} d\theta \frac{(\partial_{\theta} \mathcal{P}(\theta))^2}{\mathcal{P}(\theta)}, \quad (2.41)$$

where $\mathcal{P}(\theta)$ denotes the information available *a priori* on the parameter θ . The Van Trees information (2.41) consists of two terms: the first one corresponds to the average Fisher information calculated over the prior distribution $\mathcal{P}(\theta)$, while the second term, usually called score, identifies the informational content of the prior distribution itself (its expression strongly resembles the one for the Fisher information (1.46), with the

prior distribution replacing the likelihood function). The Van Trees information (2.41) is used to establish a lower bound on the average MSE on the estimation of θ [98,99]:

$$V(N)\langle MSE[\tilde{\theta}] \rangle \geq \frac{1}{N}. \quad (2.42)$$

Differently from the standard CRB, the Van Trees inequality (2.42) lower bounds the average MSE rather than the variance of the estimator. As a consequence, it encompasses the possible estimation bias deviating the expectation value of the estimator $\tilde{\theta}$ from the true value of the parameter θ , property not necessarily negligible in the finite-size regime.

However, in the large ensemble limit, the weight $1/N$ makes the score term negligible with respect to the information content extracted from data, i.e. the average Fisher information, which becomes progressively clustered about the true value of θ , so $\langle g(\theta) \rangle \rightarrow f(\theta)$. On the same page, as $N \rightarrow \infty$, the expectation value of $\tilde{\theta}$ converges to the true value of θ (the Bayesian estimator is asymptotically unbiased), therefore $MSE[\tilde{\theta}]$ is reduced to $\Delta^2\theta$. As a result, the standard Cramér-Rao inequality is retrieved

$$V(N)\langle MSE[\tilde{\theta}] \rangle \geq \frac{1}{N} \xrightarrow{N \rightarrow \infty} \langle \Delta^2\theta \rangle f(\theta) \geq \frac{1}{N}. \quad (2.43)$$

Furthermore, in a practical scenario, experimental imperfections unavoidably affect the apparatus and so the estimation process. Thus, experimental imperfection sources should be accounted as extra nuisance parameter(s) v in order to properly characterize the experiment. This latter feature demands an adaptation to a multiparameter metrological approach. The simplest model that can be made concerns the target parameter

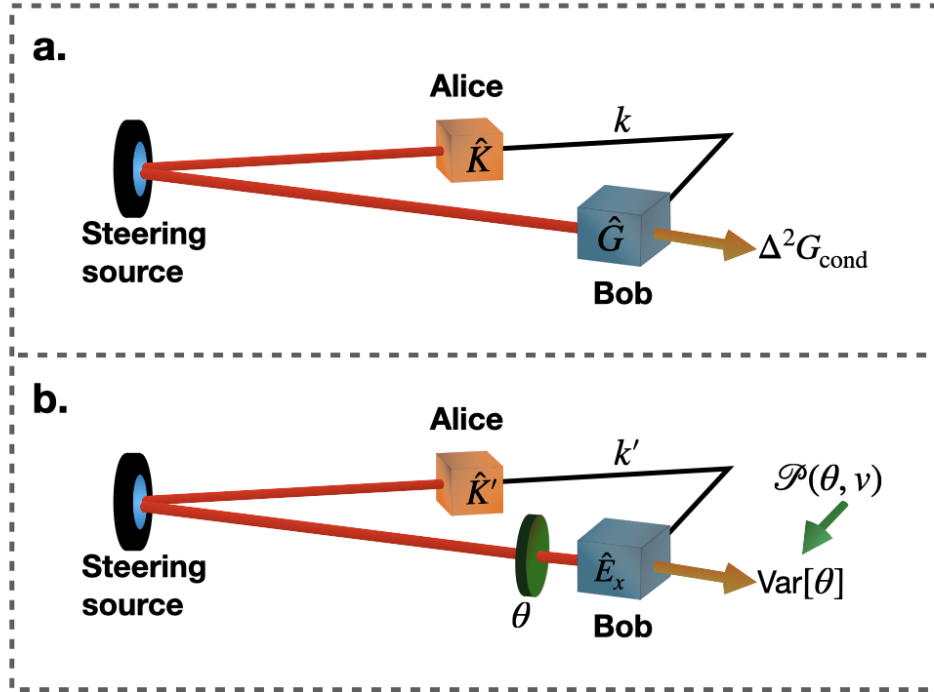


Figure 2.7: Certification of quantum steering as a metrological problem. Top panel) Alice communicates a classical message k arising from the measurement of her observable $\hat{K}$. Bob exploits such information to predict the outcome and the conditional variance of his local observable $\hat{G}$. Bottom panel) Bob makes use of the measurement outcome of a POVM $\{\hat{E}_x\}_x$ and the prior distribution $\mathcal{P}(\theta, v)$ to retrieve the variance on an unknown parameter θ encoded in the state he shares with Alice. Picture adapted from [7].

θ and a nuisance v affecting the bipartite state Alice and Bob share.

A sketch of the adapted YFG method is reported in Fig. 2.7.

Likewise the Fisher information, the Van Trees information is turned into a matrix

$V_{\alpha\beta}$, whose elements are now given by

$$V_{\alpha\beta} = \int d\theta dv \mathcal{P}(\theta, v) F_{\alpha\beta}(\theta, v) + \frac{1}{N} \int d\theta dv \frac{\partial_{\alpha} \mathcal{P}(\theta, v) \partial_{\beta} \mathcal{P}(\theta, v)}{\mathcal{P}(\theta, v)} \quad \alpha, \beta = \theta, v, \quad (2.44)$$

where $\{F_{\alpha\beta}\}_{\alpha\beta}$ is the Fisher information matrix, and the score term is now generalized to a score matrix.

The metrological bound (2.42) is now turned into a matrix inequality (similarly to the multiparameter CRB)

$$\Sigma_{\alpha\beta} \geq \frac{1}{N} (V^{-1}(N))_{\alpha\beta} \quad \alpha, \beta = \theta, v, \quad (2.45)$$

where $\{\Sigma_{\alpha\beta}\}_{\alpha\beta}$ is the covariance matrix (unbiased estimators are assumed for θ and v).

2.4 Going experimental

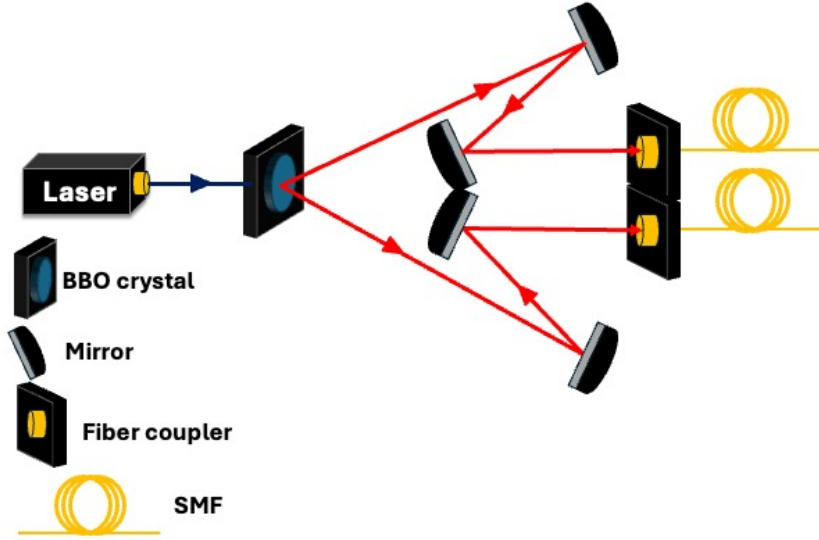


Figure 2.8: Sketch of the single photon source used throughout the experiment(s). A continuous-wave (CW) laser at wavelength $\lambda = 405$ nm pumps a 3 mm-thick β -barium borate (BBO) crystal, which produces photon pairs at $\lambda = 810$ nm via degenerate, type-I SPDC process. Photon pairs are then collected in single-mode fibers (SMF) and sent to the following part of the experiment. The bandwidth of the generated photons is fixed to $\Delta\lambda = 7.5$ nm by means of interference filters (not depicted in figure) placed in front of the fiber couplers.

The concepts delivered in the previous section have been tested in an optical platform with polarization encoding.

Photonic qubits are generated via the SPDC source depicted in Fig. 2.8. As it is commonly adopted, horizontal/vertical polarization states correspond to the eigenstates of the Pauli-Z-gate $|H\rangle = |0\rangle$ and $|V\rangle = |1\rangle$. The $\pm 45^\circ$ and clockwise/counter-clockwise polarization states, i.e. the eigenstates of, respectively, Pauli-X and Pauli-Y gate, can be expressed via linear combinations of the $|H\rangle/|V\rangle$ polarization states:

$$\begin{cases} |+\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}} \\ |-\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}} \end{cases} \quad \begin{cases} |L\rangle = \frac{|H\rangle + i|V\rangle}{\sqrt{2}} \\ |R\rangle = \frac{|H\rangle - i|V\rangle}{\sqrt{2}} \end{cases} \quad (2.46)$$

The unknown parameter to be estimated is an interferometric phase ϕ between the horizontal and vertical polarization component. Such a phase shift is encoded via the unitary operator

$$\hat{U}(\phi) = e^{-i\hat{Y}\frac{\phi}{2}}. \quad (2.47)$$

Consequently, by comparing Eq. (2.47) with the general representation of a unitary operator, it is easy to grasp that the generator $\hat{G}$ of the interferometric phase ϕ is $\hat{G} = \hat{Y}/2$.

The probe state used in the experiment is locally equivalent a singlet state (2.20) affected by nuisance degrading the superposition terms:

$$\hat{\rho}_{AB} = \frac{1}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -v & 0 \\ 0 & -v & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad 0 \leq v \leq 1 \quad (2.48)$$

2.4.1 C-NOT gate in a Sagnac loop

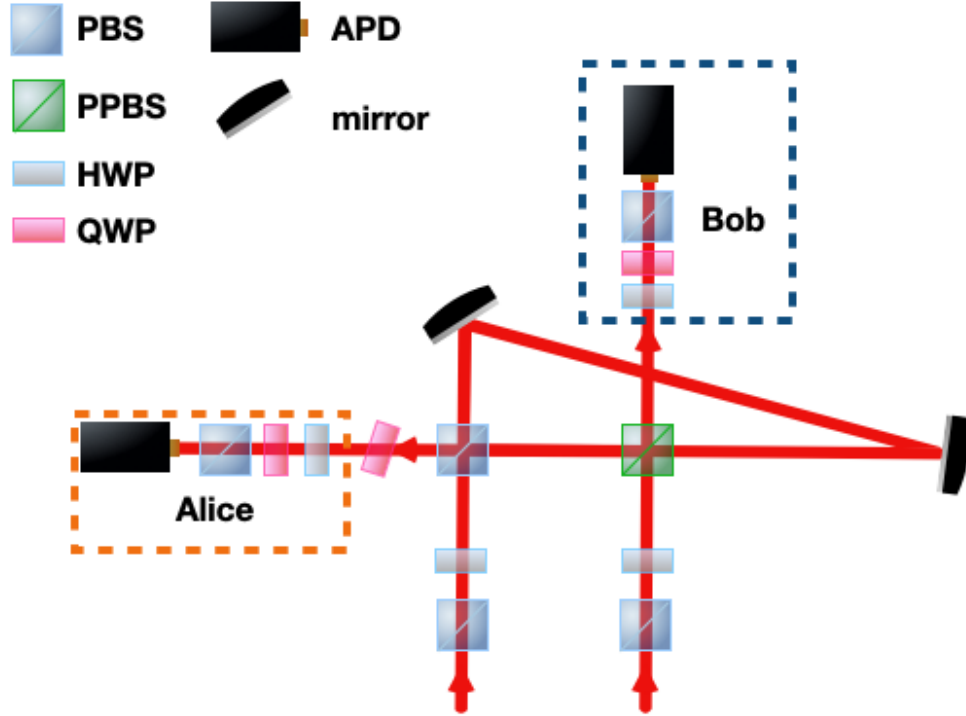


Figure 2.9: Experimental realization of the C-Z gate preparing the states exhibiting quantum steering. Photonic qubits are prepared in a suitable polarization state as close to maximal entanglement as possible. Then, they are injected into a C-Z gate embedded in a Sagnac loop, where polarization-dependent interference occurs. An additional QWP (on Alice's side) is necessary so as to compensate the resulting phase. Polarization analysis is performed via standard tomographic setup. Photons are then fiber-coupled to avalanche photodiodes (APDs) single-photon detectors. Picture taken from [7].

Photons from the SPDC source (Fig. 2.8) are coupled, in single-mode optical fibers, to the next part of the setup, where suitable two-photon polarization states are prepared and analyzed. The component enabling the generation of steerable states is a Control-Z (C-Z) gate (i.e. a C-NOT gate where the target qubit is expressed in terms of the eigenstates of the Pauli-X matrix) embedded in a Sagnac interferometer (see Fig. 2.9). The active element of the gate is the *partially-polarizing beam splitter* (PPBS) with transmittivities for horizontal and vertical polarization, respectively, $T_H = 1$ and $T_V = 1/3$. Such an asymmetry in the transmittivities is what implements a polarization-dependent, non-classical interferometry, crucial to encode quantum correlated states. Noteworthy, the Sagnac arrangement allows to control and reduce the impact of the imperfection of the PPBS onto the two orthogonal polarizations [100]. Before being injected in the C-Z gate, both photons are prepared, via HWPs, in the polarization state $|\hat{A}\rangle = \cos(\frac{\pi}{3})|H\rangle - \sin(\frac{\pi}{3})|V\rangle$, where the coefficients of the H/V polarization states are necessary to compensate the different transmittivities for the corresponding polarizations, in order to balance the populations for the following

polarization-dependent interference [101]. After the interference in the C-Z gate, the system is described by an entangled state of the form

$$|\psi\rangle_{AB} = \frac{|-H\rangle_{AB} - |+V\rangle_{AB}}{\sqrt{2}} \quad (2.49)$$

when post-selecting on coincidence events. More in detail, only the coincidence events corresponding to measurement outcomes with the combinations listed in (2.49) recorded in a coincidence window of 2 ns are kept, with all the others discarded. Noteworthy, the two-photon state (2.49) is, but for a different polarization encoding of Bob's qubit, equivalent to the singlet state (2.48) for $v = 1$. Pauli operators $\hat{X}$, $\hat{Y}$ and $\hat{Z}$ can be measured by both parties by means of a standard polarization analyzer composed by an HWP, a QWP and a PBS. The target phase ϕ is encoded by properly tuning the HWP in Bob's measurement stage.

Remarkably, the experimental arrangement reported in Fig. 2.9 encompasses both a preparation and a measurement stage, the very same platform can be used for a wide range of experiments, as it will be presented in the following chapters.

2.4.2 Experimental protocol

In the previous section, the bipartite state (2.48), as well as the experimental platform used to generate and manipulate photonic qubits, have been introduced. This section is addressed to discuss the experimental protocol aiming at certifying the presence of quantum steering in a bipartite state, in the finite-size regime.

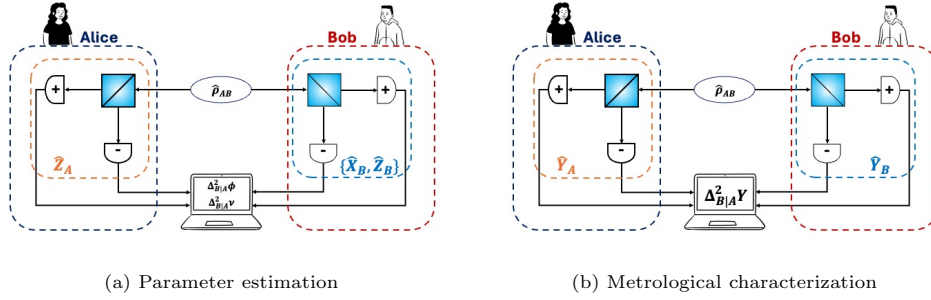


Figure 2.10: Experimental protocol for the metrology-assisted certification of quantum steering. a) Parameter estimation: Estimation for target phase ϕ and nuisance v are retrieved by coincidence measurements of Pauli-Z gate on Alice's side and Pauli-X, Pauli-Z gates on Bob's side. b) Metrological performances: Metrological bounds on the Fisher information matrix are assessed through coincidence measurements of the Pauli-Y gate, the generator of the target phase ϕ , on both Alice's and Bob's side.

The protocol is structured in two distinct blocks, with different tasks, as described in Fig. 2.7.

Joint parameter estimation

In this part of the protocol Bob aims at estimating the target phase ϕ , as well as characterizing the nuisance v (mainly due to non-perfect interference in the C-Z gate) affecting the quantum state he shares with Alice. Thus, for any of Alice's measurement in the $|H\rangle/|V\rangle$ basis, Bob implements a POVM by measuring the polarization of his photon in the $|+\rangle/|-\rangle$ and $|H\rangle/|V\rangle$ bases with equal probability. For this task, N_Z total resources are allocated. It follows, then that $N_{XZ} + N_{ZZ} = N_Z$, where N_{XZ} and N_{ZZ} are the number of times Bob chooses to measure in, respectively, the X and Z diagonal basis. The states of Bob's assemblage, conditioned by Alice's measurement are, respectively

$$\hat{\rho}_H^B = \frac{1}{4} \begin{pmatrix} 1 + v \sin(\phi) & -v \cos(\phi) \\ -v \cos(\phi) & 1 - v \sin(\phi) \end{pmatrix} \quad \hat{\rho}_V^B = \frac{1}{4} \begin{pmatrix} 1 - v \sin(\phi) & v \cos(\phi) \\ v \cos(\phi) & 1 + v \sin(\phi) \end{pmatrix}, \quad (2.50)$$

where $\hat{\rho}_{H/V}^B = \text{Tr}_A(\hat{\rho}_{AB} |H/V\rangle_A \langle H/V| \otimes \mathbb{1}_B)$. The probabilities of Bob's measurement outcomes are, respectively:

$$\begin{cases} p_{+|H} = p_{-|V} = \frac{1-v \cos(\phi)}{4} \\ p_{+|V} = p_{-|H} = \frac{1+v \cos(\phi)}{4} \end{cases} \quad \begin{cases} p_{H|H} = p_{V|V} = \frac{1+v \sin(\phi)}{4} \\ p_{V|H} = p_{H|V} = \frac{1-v \sin(\phi)}{4} \end{cases}, \quad (2.51)$$

where each probability $p_{\alpha|\beta} = p(\alpha|\beta)$ (the first index indicates Bob's measurement outcome, while the second one refers to Alice's) is calculated according to Born's rule. According to the probabilities listed in Eq. (2.51) it is possible to calculate the FIM for a given Alice's outcome:

$$F_{H/V}(\phi, v) = \begin{pmatrix} \frac{v^2}{2} \left(\frac{\cos^2(\phi)}{1-v^2 \sin^2(\phi)} + \frac{\sin^2(\phi)}{1-v^2 \cos^2(\phi)} \right) & -\frac{v^3 \sin(2\phi) \cos(2\phi)}{4(1-v^2) + v^4 \sin^2(2\phi)} \\ -\frac{v^3 \sin(2\phi) \cos(2\phi)}{4(1-v^2) + v^4 \sin^2(2\phi)} & \frac{\sin^2(\phi)}{2(1-v^2 \sin^2(\phi))} + \frac{\cos^2(\phi)}{2(1-v^2 \cos^2(\phi))} \end{pmatrix}. \quad (2.52)$$

The total FIM is retrieved by linearly combining the matrices in Eq. (2.52) with the probabilities of Alice's measurement outcomes $F_{B|A}(\phi, v) = p_A(H)F_H(\phi, v) + p_A(V)F_V(\phi, v)$. However, since the probability of Alice measuring $|H\rangle$ or $|V\rangle$ on the bipartite state (2.48) is $p_A(H) = p_A(V) = 1/2$, it follows that $F_{B|A} = (F_H(\phi, v) + F_V(\phi, v))/2 = F_H(\phi, v)$.

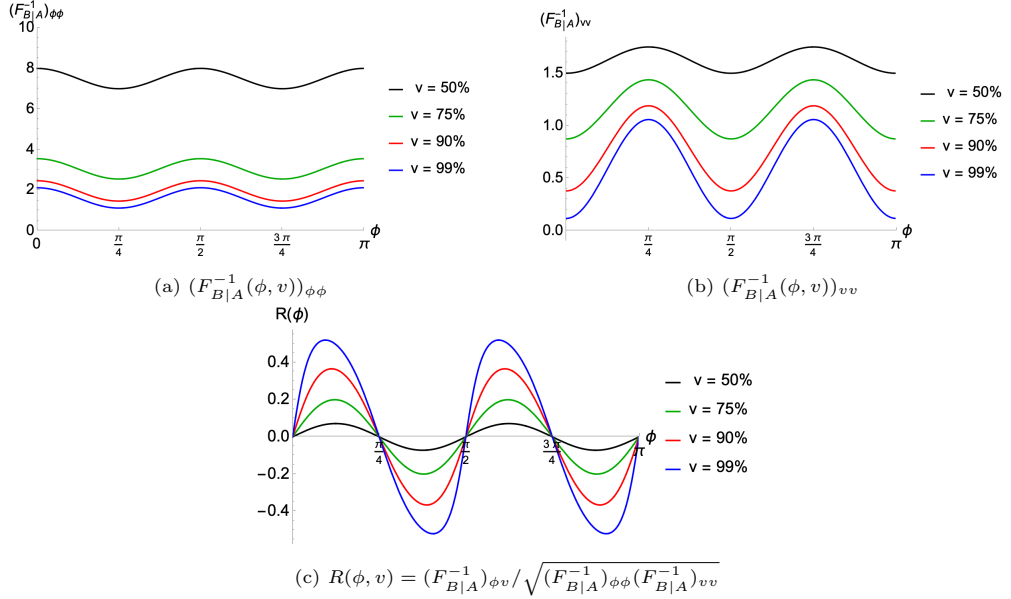


Figure 2.11: Element of the inverse conditional FIM as a function of the phase, for given values of the nuisance parameter v . a) First diagonal element, lower bounding the estimation of the phase. b) Second diagonal term, lower bounding the estimation of the nuisance. c) Correlation coefficient $R(\phi)$, providing a lower bound on the (normalized) correlations between ϕ and v . Plots adapted from [7].

The matrix element of the inverse Van Trees information matrix- the quantities actually relevant for metrological bounds, are depicted in Fig. 2.11.

As highlighted in Fig. 2.11a, the values of the phase minimizing $(F_{B|A}^{-1})_{\phi\phi}$, thus associated with maximally informative condition are $\phi = \pi/4$ and its odd multiples: being the precision bound at its lowest, this provides a malicious Alice the hardest condition to replicate the performances of the quantum correlated state by exploiting a LHS theory. Such optimal condition is experimentally implemented by adjusting the angle of the HWP in Bob's measurement stage (see Fig. 2.9).

Assessing a bound on the Fisher information

The second part of the protocol deals with the assessment of metrological bounds on the Fisher information matrix. For such a task, represented in Fig. 2.10b, N_Y resources are allocated, and both Alice and Bob perform a local measurement of the Pauli-Y observable. The states forming Bob's assemblage are now

$$\hat{\rho}_L^B = \frac{1}{4} \begin{pmatrix} 1 & iv \\ -iv & 1 \end{pmatrix} \quad \hat{\rho}_R^B = \frac{1}{4} \begin{pmatrix} 1 & -iv \\ iv & 1 \end{pmatrix}. \quad (2.53)$$

Likewise the previous case, the probability of measuring either $|L\rangle$ or $|R\rangle$ on the state (2.48) is $p_A(L) = p_A(R) = 1/2$.

The conditional variance of the phase generator is $\Delta_{B|A}^2 = \Delta_{B|A}^2 Y/4$

$$\Delta_{B|A}^2 Y = \sum_a^{L,R} p_A(a) \Delta_a^2 Y = 1 - v^2, \quad (2.54)$$

where the variance on $\hat{Y}_B$ for a given Alice's result is $\Delta_a^2 Y = \langle \hat{Y}_B^2 \rangle_{\hat{\rho}_a^B} - \langle \hat{Y}_B \rangle_{\hat{\rho}_a^B}^2 = 1 - v^2$. This latter result, combined with the one retrieved in the previous paragraph, is the main ingredient for the certification test of genuine quantum steering, as discussed in the next section.

2.5 Results

The main outcomes of the two parts of the certification protocol are, respectively

$$\begin{cases} N_Z \Delta^2 \phi \geq (F_{B|A}^{-1}(\phi, v))_{\phi\phi} & \text{Cramér-Rao bound} \\ N_Z \Delta^2 \phi \Delta_{B|A}^2 Y_B \geq 1 & \text{Reid's criterion} \end{cases} \quad (2.55)$$

where the fact that $\Delta^2 H = \Delta^2 Y/4$ has been used. By combining the two equations in (2.55), and by recalling that $(F_{B|A}^{-1}(\phi, v))_{\phi\phi} \geq (F_{\min}^{-1})_{\phi\phi} = (F_{B|A}^{-1}(\phi = \pi/4, v))_{\phi\phi}$, the following inequality holding for any assemblage admitting a LHS description is retrieved:

$$\Delta_{B|A}^2 Y_B \geq \frac{1}{(F_{\min}^{-1})_{\phi\phi}} \longrightarrow 1 - v^2 \geq \frac{v^2}{2 - v^2}. \quad (2.56)$$

Equation (2.56) poses a constraint on the visibility range for which YFG's inequality (2.40) can be violated. As shown in Fig. 2.12, the effective Fisher information $1/(F_{\min}^{-1})_{\phi\phi}$ becomes greater than the variance of the generator $\Delta_{B|A}^2 Y_B$ only for $v > \sqrt{2 - \sqrt{2}}$. The presence of noise degrading the bipartite states is then reflected on the violation range of the YFG's inequality, possible only for sufficiently coherent states. Moving to the non-asymptotic regime, the informational quantity of reference is the Van Trees information matrix, whose elements are calculated according to Eq. (2.44), with the metrological bound now being the Van Trees bound (2.45).

As anticipated in the previous section, the estimation of both phase and nuisance is carried on in a Bayesian framework, according to N_Z independent runs performed by Alice. For any of these rounds, the probability of detecting a specific result b on Bob's side given the outcome a on Alices, will be proportional to $p(b|a)^{n_{ba}}$, with $p(b|a)$ being the corresponding probability (see Eq. (2.51)) and n_{ba} the occurrence of the given b, a combination of outcomes. The collection of all of Bob's results is summarized by the **conditional likelihood function**

$$\mathcal{H}_a(\phi, v) = \Pi_b p(b|a)^{n_{ba}}, \quad (2.57)$$

for any of Alice's outcomes H or V , and $b = H, V, +, -$. The total resources are arranged such that $\sum_b \sum_a b_{ba} = N_Z$. The Bayes estimator for the phase ϕ and its variance, for a fixed Alice's result a are, respectively

$$\begin{cases} \bar{\phi}_a = \frac{\int d\phi dv \mathcal{H}_a(\phi, v) \mathcal{P}(\phi, v) \phi}{\int d\phi dv \mathcal{H}_a(\phi, v) \mathcal{P}(\phi, v)} \\ \Delta_a^2 \phi = \frac{\int d\phi dv \mathcal{H}_a(\phi, v) \mathcal{P}(\phi, v) (\phi - \bar{\phi}_a)^2}{\int d\phi dv \mathcal{H}_a(\phi, v) \mathcal{P}(\phi, v)}. \end{cases} \quad (2.58)$$

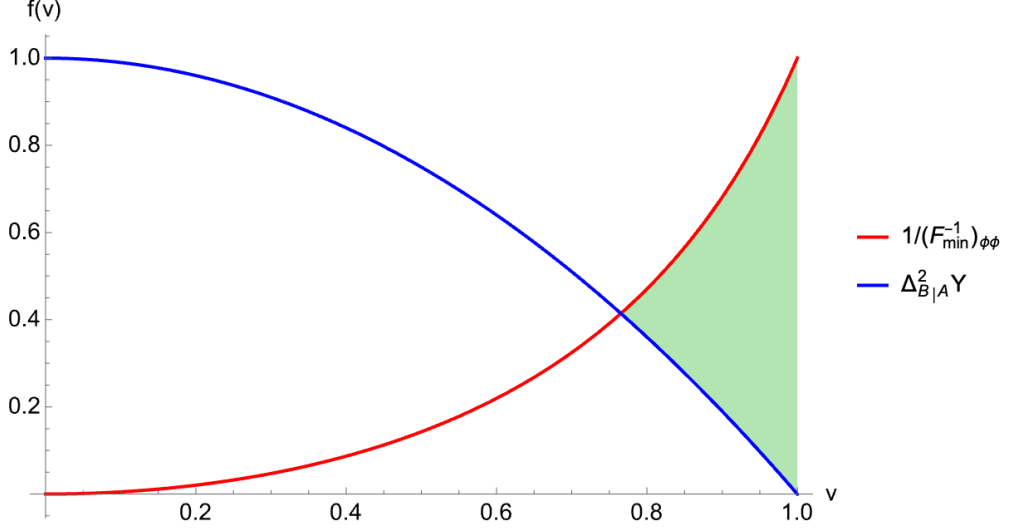


Figure 2.12: Violation of the YFG inequality. The maximal effective Fisher information on the phase $1/(F_{\min}^{-1})_{\phi\phi}$ (red curve) and the conditional variance $\Delta_{B|A}^2 Y_B$ (blue curve) are plotted as a function of the nuisance parameter v . The green shaded area corresponds to the visibility range for which YFG's inequality (2.40) can be violated. Picture taken from [7].

On the same page as the YFG's method described previously, the **conditional Bayes estimators** for the phase ϕ and the corresponding variance are given by the linear combination of such estimators for a given Alice's outcome, weighted by the relative occurrence of the corresponding result (squared relative occurrence for the variance estimator):

$$\begin{cases} \bar{\phi}_{\text{cond}} = \frac{\sum_a \sum_b n_{ba} \bar{\phi}_a}{\sum_a \sum_b n_{ba}} \\ \Delta_{B|A}^2 \phi = \frac{\sum_a (\sum_b n_{ba})^2 \Delta_a^2 \phi}{(\sum_a \sum_b n_{ba})^2} \end{cases} \quad a = H, V. \quad (2.59)$$

Similar expressions to (2.58) and (2.59) hold for the Bayesian estimation of the nuisance v and its associated variance.

The metrological bound on $\Delta_{B|A}^2 \phi$, requires the calculation of the inverse Van Trees information matrix:

$$V_{\alpha\beta} = n_H V_{\alpha\beta}^{(H)} + n_V V_{\alpha\beta}^{(V)}, \quad (2.60)$$

where $V_{\alpha\beta}^{(j)}$ are the Van Trees information for a fixed Alice's outcome, calculated as in Eq. (2.44) by using n_a resources, where $a = H, V$.

The metrological performances of the protocol, in terms of the phase estimation uncertainty $\text{Var}[\phi] = \Delta_{B|A}^2 \phi$ are presented in Fig. 2.13. Experimental data align with the trend paved by the Van Trees' bound, extending the customary Cramér-Rao bound so as to include the information content embedded in the prior distribution $\mathcal{P}(\phi, v)$, decreasing as N_Z increases. Slight deviation of the experimental data from the theoretical bound may stem from some effects not accounted in the model here tested; mainly a slight unbalance in the populations compared to the equal superposition of $|H\rangle/|V\rangle$ polarizations. Together with a non-asymptotic metrological bound, a new inequality, in place of the original YFG's one (2.40), is required to assess the presence of genuine quantum steering in the finite-size regime. In order to proceed, it is necessary to build a new figure of merit playing the role of the conditional variance of the parameter generator.

Similarly to what has been done for the Fisher information (matrix), we extend the former $4\Delta_{B|A}^2 G$ to a new figure of merit

$$\mathcal{L}(N) = 4\Delta_{B|A}^2 G + \frac{1}{N} \int d\phi dv \frac{(\partial_\phi \mathcal{P}(\phi, v))^2}{\mathcal{P}(\phi, v)} \quad (2.61)$$

which accounts for both the conditional variance of the generator $4\Delta_{B|A}^2 H = \Delta_{B|A}^2 Y$ in the LHS limit, as well as for Bob's *a priori* information, becoming progressively more

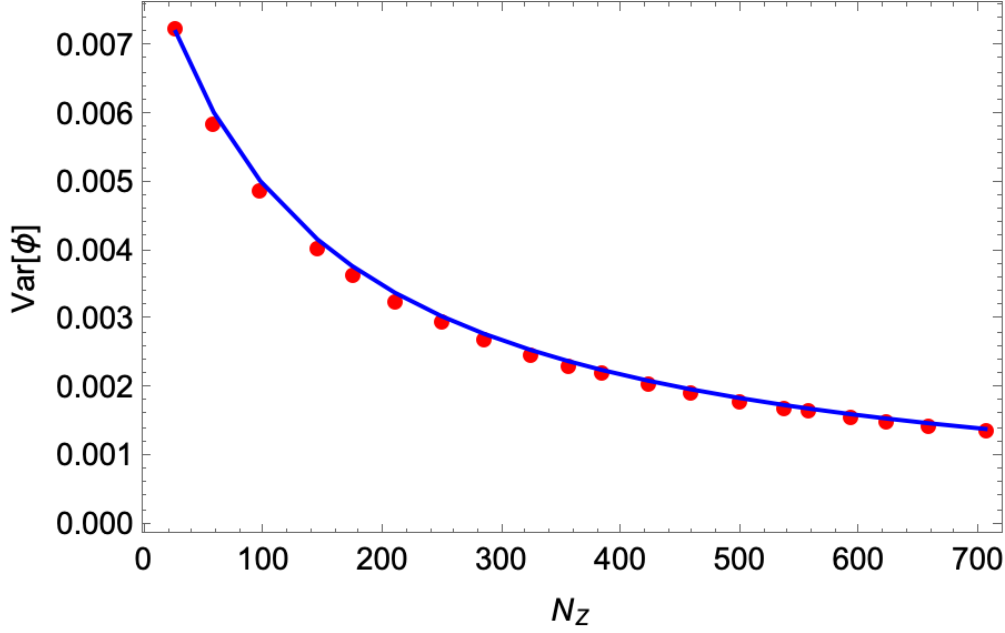


Figure 2.13: Metrological performances of the Bayesian phase estimation. Scaling of the variance of the target phase ϕ as a function of the total number of resources N_Z used in the protocol. Red points correspond to the conditional variance (2.59) for the phase ϕ , while the blue, solid line is the Van Trees limit, with standard deviation $\sigma = \pi/24$. Picture adapted from [7].

negligible in the large data regime, as it is weighted by the factor N^{-1} , recovering the standard YFG bound. Remarkably, the conditional variance of the generator is reconstructed by using N_Y resources (It is the part of the protocol described by Fig. 2.10b), while the number of resources weighting the *a priori* information in Eq. (2.61) is N_Z , i.e. the number of resources spent to build the phase estimator.

Notably, all the quantities of (2.61) can be experimentally assessed. Likewise the phase and nuisance estimator, the generator is reconstructed relying on the coincidence counts m_{ba} of Alice's and Bob's results of the measurement of Pauli-Y gate, such that $\sum_b \sum_a m_{ba} = N_Y$. Given the occurrences m_{ba} of all the possible combinations of measurement outcomes of $\hat{Y}$ by both parties, the value $\bar{Y}_a$ measured by Bob at a given Alice's result is calculated as the average value of Y :

$$\bar{Y}_a = \frac{m_{La} - m_{Ra}}{m_{La} + m_{Ra}}, \quad (2.62)$$

where the $+1$ outcome is associated with $|L\rangle$ state, whereas -1 with $|R\rangle$ polarization state.

The conditioned estimator is again calculated as the weighted average of the Y-estimators for a fixed Alice's result (2.62):

$$\bar{Y}_{\text{cond}} = \frac{m_L}{N_Y} \bar{Y}_L + \frac{m_R}{N_Y} \bar{Y}_R, \quad (2.63)$$

where $m_a = \sum_{b=L,R} m_{ba}$ $a = L, R$. By making use of the property $\hat{\sigma}_j^2 = \mathbb{1}$ for all the Pauli matrices, the conditional variance on the generator is established as

$$\Delta_{B|A}^2 Y = 1 - Y_{\text{cond}}^2. \quad (2.64)$$

A new figure of merit is needed to certify the presence of genuine quantum steering in the finite-size regime. By combining the Van Trees inequality (2.45) with the new figure of merit (2.61) the following inequality, called **Van Trees-YFG (VT-YFG) inequality**, holding for any bipartite state admitting a LHS description, is retrieved

$$N \text{Var}[\phi] \mathcal{L} \geq 1, \quad (2.65)$$

which replaces the former YFG inequality (2.40).

The variable $\xi^2 = N_Z \text{Var}[\phi] \mathcal{L}$, i.e. the left-hand-side of Eq. (2.65) has the form of a

normalized variance: it is therefore expected to be distributed according to a normalized χ^2 distribution (since, as already said, all the quantities defining the informational quantity $\mathcal{L}$, thus the reciprocal of a variance, can be experimentally retrieved). The **steering criterion** can be thus formulated as a **one-sided hypothesis test** with $N_Z - 1$ degrees of freedom, with the non-asymptotic YFG inequality (2.65) identifying the null hypothesis.

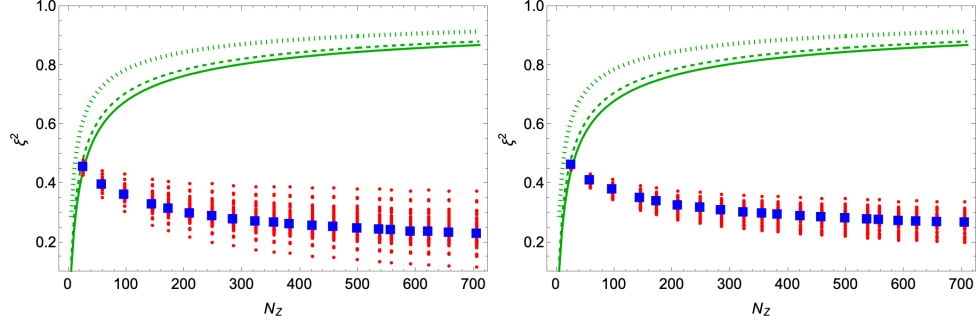


Figure 2.14: Certification of the violation of the VT-YFG inequality (2.65) with respect to the number of resources N_Z used to estimate the phase. In both panels blue points refer to the experimental values of ξ^2 , while the red points are calculated via a bootstrap Monte Carlo strategy with 50 iterations. The three green lines represent the critical values of the χ^2 distribution for three different confidence levels: $p = 0.05$ (dotted line), $p = 0.01$ (dashed line) and $p = 0.005$ (continuous line). The two plots correspond to different number of resources used to evaluate $\Delta^2 Y$, reflected onto $\mathcal{L}$: left panel) $N_Y = 200$, right panel) $N_Y = 495$. Picture taken from [7].

The validation test concerns the comparison of the values of test variable ξ^2 with the critical values $\chi_{\text{cr},p}^2$ of the χ^2 distribution at a given confidence p : whenever $\xi^2 < \chi_{\text{cr},p}^2$ the description of Bob's assemblage in terms of LHS model is unsuitable, certifying then, with confidence p , the presence of genuine quantum steering.

Notably, the error on $\mathcal{L}$, which is experimentally retrieved, prevents the standard Fisher-Snedecor test from being applied directly to compare two estimated variances (the reference value $1/(N_Z \mathcal{L})$ is not χ^2 -distributed).

An alternative approach, the one that was used in the experiment here described, revolves around a Monte Carlo-based method, relying on multiple values on $\mathcal{L}_{\text{mc}}$ generated by bootstrapping on the observed statistics, assuming (as customary) a Poissonian distribution for the coincidence counts.

Experimental results are shown in Fig. 2.14: the dispersion of experimental data is ruled by the number of physical resources N_Y addressed to the characterization of the generator (or, equivalently, to the estimation of the figure of merit (2.61)), as highlighted by a direct comparison of the two panels. Interestingly, large deviations of the data from a LHS model do not require a large N_Y in order to certify the authenticity of quantum steering.

In terms of the scaling with N_Z , the violation of the VT-YFG bound lacks statistical significance for a small amount of resources, for which a stricter test at $p = 0.005$ is needed. Far from such a condition, it becomes progressively harder for Alice to reproduce the correlations data highlight by relying on classical randomness and LHS models, with very weak dependence on the number of resources used to assess the informational bound (2.61), and even weaker dependence on the confidence level of the test.

2.6 Analysis of the robustness of the protocol

The metrology-assisted certification technique described in this section extends the original YFG's work [60] for the assessment of genuine quantum steering in the finite-size regime, accounting, at the same time, for unavoidable imperfections affecting the quantum state used throughout the experiment.

This has been done by formulating the problem in the multiparameter scenario, and by adopting a Bayesian framework for the parameter estimation. The milestone of the protocol, allowing to explore Van Trees bound, replacing the more common Cramér-Rao bound.

Crucially, both the Bayesian estimation and the Van Trees bound depend on the *a priori* information available to Bob on the phase ϕ and the nuisance v (in the form of reduced visibility of the interference fringes). The prior distribution $\mathcal{P}(\phi, v)$ plays, indeed, a crucial role in the VT-YFG approach; for this reason it is interesting to investigate how changes in the prior distribution are reflected onto both the estimation and the violation of (2.65).

As shown in Fig. 2.11c, correlations between the phase and the visibility of the interference fringes v drop to 0 at the maximally informative phases: by centering the prior distribution on the phase ϕ around such values, it is possible to take $\mathcal{P}(\phi, v)$ as the product of a phase-prior distribution and a nuisance-prior distribution:

$$\mathcal{P}(\phi, v) = \mathcal{P}_\phi(\phi)\mathcal{P}_v(v). \quad (2.66)$$

Moreover, the Van Trees bound require some regularity conditions (mainly continuity and derivability within all the definition interval) to be fulfilled. As a consequence, a cautious choice of the prior distributions is needed.

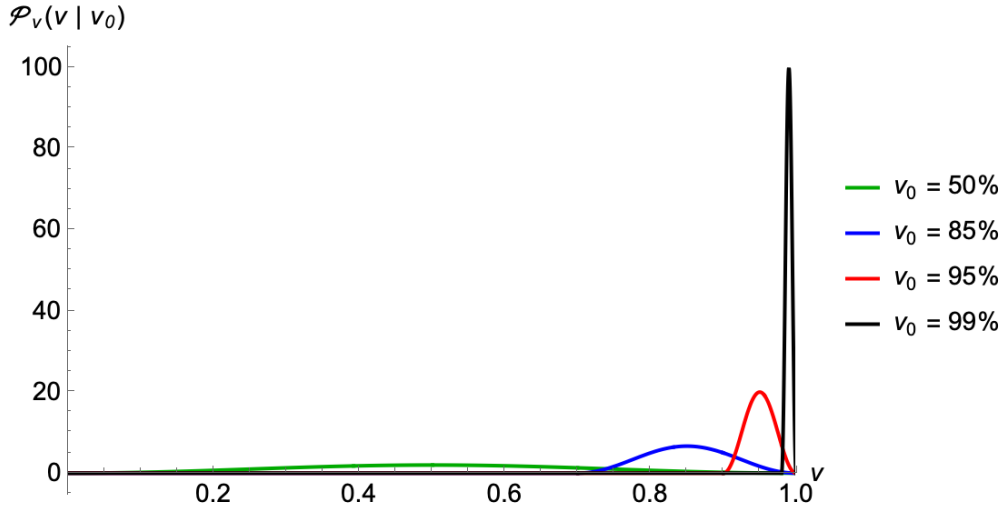


Figure 2.15: Plot of the prior distribution on the visibility, for different choices of the expected nuisance v_0 . Picture adapted from [61].

A possible choice to represent the prior information on the nuisance v is a raised cosine distribution

$$\mathcal{P}_v(v|v_0) = \frac{\Theta(v - (2v_0 - 1))}{2(1 - v_0)} \left(1 + \cos\left(\pi \frac{v - v_0}{1 - v_0}\right) \right), \quad (2.67)$$

where v_0 is the expected nuisance. The Heaviside step function $\Theta(v - (2v_0 - 1))$ bounds the prior distribution in the interval $[2v_0 - 1, 1]$, where it is regular and going to 0 at the endpoints of such an interval. A plot of the probability distribution (2.67) for different expected nuisances is shown in Fig. 2.15. Clearly, it is highly desirable for the expected visibility to lie in the violation range $[\sqrt{2} - \sqrt{2}, 1]$ of the VT-YFG's inequality.

The choice of the phase prior distribution is slightly subtle: in addition to obeying the regularity conditions needed to the define the Van Trees information, they must feature some tunable internal parameter allowing the user to disambiguate among different phase values having the same conditional Fisher Information. In this specific case, due to the $\pi/2$ - periodicity of the Fisher information matrix (see Fig. 2.11), the phase prior distribution should be non-zero in a range of width $\pi/2$, centered around $\phi_0 = \pi/4$. A reasonable choice is a Gaussian distribution

$$\mathcal{P}_\phi(\phi|\sigma) = \frac{e^{-\frac{(\phi - \pi/4)^2}{2\sigma^2}}}{\sqrt{2\pi\sigma^2}}, \quad (2.68)$$

with the standard deviation σ restricted to $\sigma \leq \pi/8$ so as to obey to the aforementioned requirement. This has been the prior distribution used to run the protocol and retrieve

the results discussed in the previous section.

An alternative, commonplace choice is the **Von Mises distribution** [102, 103]

$$\mathcal{P}_\phi(\phi|\kappa) = \frac{e^{\kappa \cos(\phi - \pi/4)}}{2\pi I_0(\kappa)}, \quad (2.69)$$

where $I_0(\kappa)$ is the 0-order Bessel function, while the parameter κ quantifies the concentration² of experimental data around the target phase $\phi = \pi/4$. These latter probability distributions are shown in Fig. 2.16.

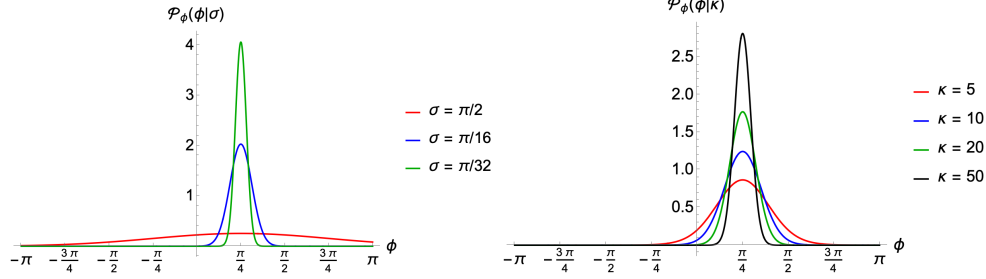


Figure 2.16: Phase prior distributions centered at $\phi = \pi/4$. Left panel) Gaussian prior distribution (2.68) for different standard deviations σ . The value $\sigma = \pi/2$ clearly does not satisfy the regularity conditions imposed by the Van Trees bound. Right panel) Von Mises distribution (2.69) at different values of the internal parameter κ . Picture adapted from [61].

After defining the prior distributions, experimental data have been analyzed by changing the prior distribution (2.68) and (2.69) and by tuning the respective parameters, and investigating the effect on both the estimation performances, as well as on the validation test.

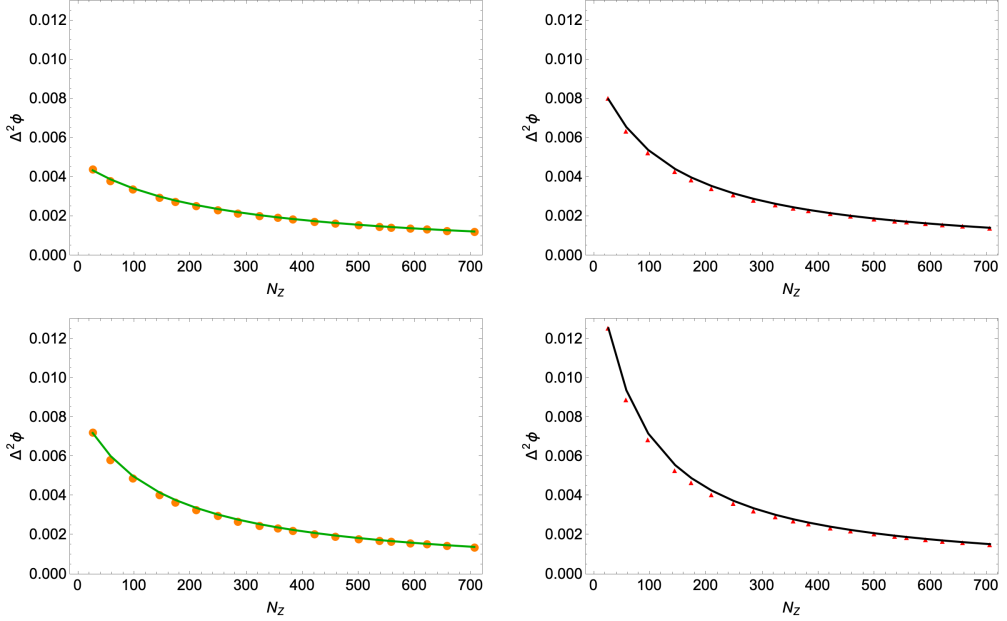


Figure 2.17: Effect of different phase prior distributions on the scaling of the variance $\Delta^2 \phi$ versus the number of resources N_Z . The panels on the left represent the metrological performances retrieved by employing a Gaussian prior with, respectively, $\sigma = \pi/24$ (top panel) and $\sigma = \pi/32$ (bottom panel). Similarly, the plots on the right depict the estimation performances arising from a Von Mises distribution, with κ such that the circular variance match the corresponding Gaussian's standard deviation. In each plot, experimental data is represented by red (Von Mises) and orange points (Gaussian), with the, respectively, black/green solid curve identifying the Van Trees limit. Picture taken from [61].

Fig. 2.17 shows that experimental data follow the trend led by the Van Trees bound,

²More thoroughly, the quantity $1/s^2$ is a dispersion measure, similarly to the variance σ^2 for a Normal distribution.

with no substantial difference between the employment of a Gaussian distribution rather than a Von Mises; with a definitely weak dependence on the specific values of the internal parameters σ or κ . Furthermore, the (slight) deviation of experimental points from theoretical bounds is not corrected by a different setting of the prior distribution, enforcing thus the hypothesis of other possible sources not accounted in the model [104].

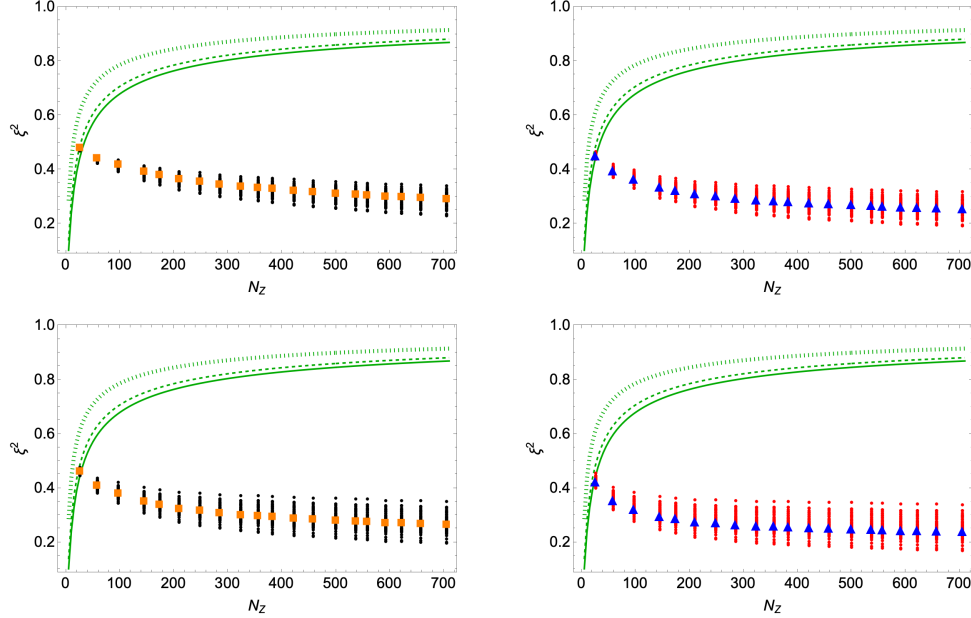


Figure 2.18: Effect of different phase prior distributions on the validation test of quantum steering. Likewise Fig. 2.17, left panels are associated with a Gaussian prior with, respectively, $\sigma = \pi/32$ (top-left panel) and $\sigma = \pi/24$ (bottom-left panel), while plots on the right column with a Von Mises distribution with κ corresponding to the σ s of the plots on the left. Experimental values of the test variable ξ^2 are represented by, respectively, orange and blue points. All the plots here reported feature $N_Y = 495$ resources used to estimate $\Delta_{B|A}^2 Y$. Picture taken from [61].

The effect of different phase priors on the certification test of quantum steering is presented in Fig. 2.18.

Similarly to the estimation performances, the choice of a different prior distribution bears almost no significance in the validation test, regardless the number of resources N_Z used to perform the experiment.

2.7 Metrology-assisted certification of quantum steering: conclusions

In conclusion, genuine quantum steering has been certified by adopting a metrology-assisted strategy, with particular focus on the limited-data regime, particularly relevant in contexts such as multiple-party scenarios.

Besides its applicability for the investigations of the foundations of quantum mechanics, the protocol here described promises to host several applications in quantum technologies, ranging from quantum communication to quantum sensing to quantum networks. More specifically, such a metrology-assisted certification technique could be relevant for distributed and delegated quantum sensing, with the main appeal being the possibility of the very same setting for both the certification of the quantum channel and the estimation task. Nonetheless, the protocol presented in sections 2.3.2, 2.4 and 2.5 proved to be robust against different encoding of the initial information available to Bob, with respect to both the metrological performances and, more importantly, to the certification test of genuine quantum steering. Such a weak dependence on the prior distribution further improves the applicability of such a metrology-assisted certification technique to practical network scenarios.

Chapter 3

Secure sensing on networks

Chapter 2 showed how quantum metrology can be used to certify the presence of genuinely quantum correlation, ruling out the possibility of reproducing the observed correlations via LHS models. The certification of quantum steering has been formulated as a phase estimation task, with the violation of a suitable metrological bound ruling out the suitability of the LHS description.

Section 2.2.4 presented how progressively stronger quantum correlations are associated with different levels of trust of the nodes of a network. A further step is granting that information about the metrological task (i.e. parameter estimation) is accessible only to the meant users, thereby preventing any malicious user from accessing such information.

Section 3.1 provides an overview of how quantum metrology can be implemented on distributed architectures, with an insight into desirable security requirements against possible malicious users discussed in section 3.1.1.

On such a path, a concise review about quantum security, particularly on quantum cryptography, is provided in section 3.2, with two representative protocols presented in sections 3.2.1 and 3.2.2. Section 3.2.3 summarizes the fundamental concepts borrowed from quantum cryptography to design secure distributed quantum sensing protocols. Building upon this framework, section 3.3 focuses on two different protocols adding some security constraints to the sensing task implemented on networks.

A new class of secure phase estimation protocols, based on the manuscript [8] is presented in section 3.4. Here, a first protocol in which one user is addressed to the metrological task is discussed in section 3.4.1, with an experimental proof delivered in section 3.4.2. A two-way protocol, in which one user is in charge of both the state preparation and the state measurement, is briefly discussed in section 3.4.3.

3.1 Distributed quantum sensing

The main pillars of the second quantum revolution (computing, communication, metrology and simulation), shown in Fig. 1, are nowadays established research fields, featuring broad literature, with several experimental proofs, ranging from proof-of-concept experiments to commercial applications. The solid expertise on their fundamental aspects, together with recent technological advancements, opens up the possibility of using quantum resources to perform the former tasks on a network architecture.

In this framework the perspective of connecting together spatially separated sensors has attracted much attention from the community. The main goal of this perspective is the exploitation of quantum resources distributed among the nodes of the network to implement metrological tasks. For this reason, it is named **distributed quantum sensing (DQS)**. It has been shown that a network architecture for sensing protocol may lead to an advantage in term of performances compared to non-distributed settings, not concerning quantum resources [105,106]. Experimental proofs with different platforms can be found in [107,108]. A particular subset of DQS scenarios, exhaustively discussed in [106], concerns the case in which a provider supplies quantum resources to some end parties with limited quantum capabilities: this is what is usually called **delegated quantum sensing** [106,109,110]. A major challenge, involving the merging of concepts quantum communication and quantum metrology, is the assessment of the correct functioning of the network under adversarial conditions, demanding,

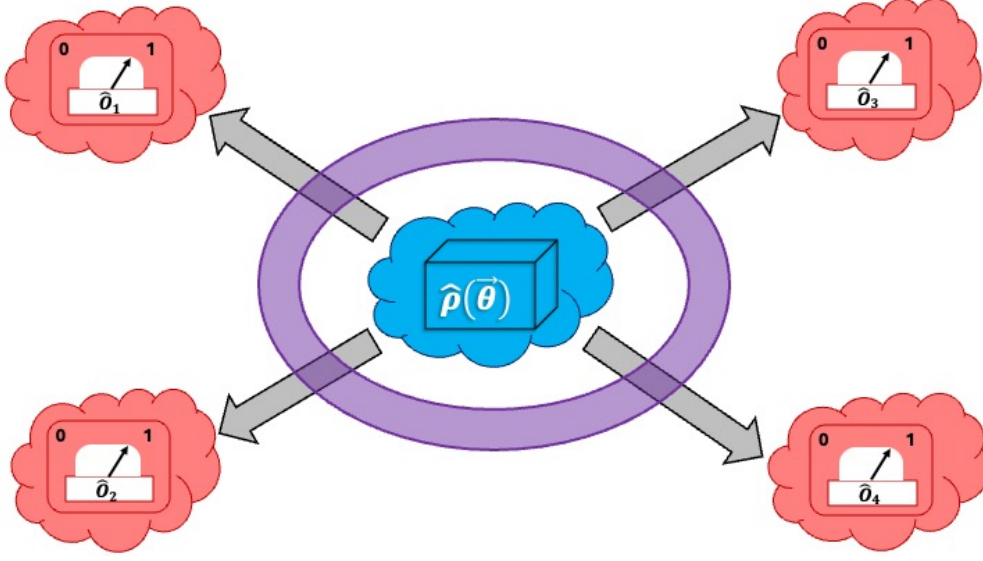


Figure 3.1: Pictorial representation of a DQS setting. The central node supplies the other end nodes with quantum probes, described by the state $\hat{\rho}$ via untrusted quantum channels. Each of the end user are aimed at estimating the parameters encoded in the distributed probe state. The effect of a potentially malicious user are here represented by the violet shaded area. Picture inspired by [111].

thus, additional security requirements. An brief overview is delivered in the following subsection.

3.1.1 Adding security requirements

In Chapter 2 it was shown how it is possible to certify quantum channels via quantum metrology. A natural question concerns, indeed, the possibility of securing quantum estimation in a network. Additional security and privacy requirements are therefore needed to prevent any interference introduced from an eavesdropper from spoiling the correct working scheme of the sensing network.

Some desirable security constraint include, and are not limited to:

- **Privacy of locally retrieved information:** Local parameters belonging to each node might be desired to be kept private with respect to other nodes or potential adversaries, with only global information being fully accessible;
- **Secrecy of the target parameter:** The feature of the probe state are desired to be robust against leakage of information about the parameter(s) by unauthorized users;
- **Robustness against noise and resource loss:** The protocols are usually required to guarantee security and privacy of information retrieved from measurements even in presence of nuisance, decoherence or loss of metrological probes;
- **Integrity of the shared quantum resources:** Preliminarily to the actual operation, it is crucial to validate the shared quantum resources, such as entanglement, across the nodes of the network.

A common ground for many requirements lies in concepts borrowed from quantum communication, mainly **Quantum Key Distribution (QKD)**, commonly adopted to assess the security of a channel via secret key exchange, discussed in the following section.

3.2 Elements of quantum cryptography

Among the quantum technologies encompassed in the Second Quantum Revolution 1, quantum communication, and more specifically, quantum key distribution, is among

the fastest growing and most impactful disciplines, with already commercial applications in cybersecurity.

QKD relies on the fundamental properties of quantum mechanics in order to guarantee unprecedented levels of security in information exchange, at the price of a lower transmission rate. Advances on quantum communication are motivated by the fragility of current, classical cryptosystems, with attention to attacking strategies potential malicious users may adopt today, as well as in the (near) future. Together with a trade-off between security and secret key rate, another challenge for practical, widespread QKD, is the trade-off between secrecy (secret key rate) and the distance between sender and receiver in the network. For such a purpose, several protocols, such as those relying on continuous-variable (CV-QKD) and Gaussian states, and experimental implementations (earth-satellite links, quantum repeaters) have been developed [112, 113].

Any QKD protocol is generally structured as follows:

1. The sender (Alice) encodes the instances of a classical random variable (e.g. the value 0 or 1 of a classical bit) α into non-orthogonal states of a quantum alphabet;
2. Alice delivers the encoded qubits to the receiver, Bob, onto a quantum channel, where potentially malicious user may act, with the goal of eavesdropping the encrypted information;
3. The user at the receiving end measures the incoming signal, retrieving a classical random variable β . After a certain number of repetitions a **raw key** is retrieved from Alice's and Bob's correlated variables α and β ;
4. Raw data is used to estimate the capacity of the channel, so as to quantify the amount of post-processing necessary to extract a private, shared key. A **sifting** strategy, possibly involving error correction techniques is used to detect communication errors and to bound the amount of information possibly leaked by a malicious user.

An alternative strategy to the **prepare and measure** just described relies on an entanglement-based representation to assess security and retrieve the secret key.

3.2.1 Mutually Unbiased-Based (MUB) protocols: Bennett-Brassard 1984 (BB84) protocol

One of the simplest, yet insightful, most commonly used QKD protocol is the one proposed by Charles H. Bennett and Gilles Brassard in 1984 [114] (BB84). The protocol relies on a prepare-and-measure scheme, as discussed in Section 3.2, with security granted by encoding the logical bit into physical qubit with eigenstates corresponding to two non-commuting operations. Such an approach is thus called **mutually unbiased-based (MUB)** protocol. The key ingredient here is the non-orthogonality of the states encoding the same logical bit in the two alphabets: non-orthogonality condition, together with the no-cloning theorem of quantum mechanics, prevent an eavesdropper, usually referred to as Eve, from copying or measuring the quantum states associated with the same logical bit with perfect fidelity.

As a result, a malicious user cannot perfectly extract information encoded by Alice, adding some disturbance that can be detected by the trusted parties.

The BB84 protocol can be sketched as follows:

1. Alice generates a random string of logical bits. For any of these, she chooses a random alphabet to encode it into a physical qubit. A commonplace choice is the Pauli-Z alphabet ($|0\rangle, |1\rangle$) and the Pauli-X alphabet ($|+\rangle, |-\rangle$). After the encoding, she sends the encoded string of qubits to Bob via the untrusted channel;
2. For each qubit received, Bob chooses at random which alphabet (from the same choices as Alice's) to use to measure the qubit state.

In a noiseless scenario, whenever Alice and Bob have chosen the same basis to, respectively, encode and decode the qubit state, they share the same value of the logical bit. Conversely, whenever the encoding and decoding alphabets do not match, the value of Bob's bit will agree with Alice's only half of the times, in an unpredictable manner.

3. After the transmission is over Bob and Alice employ a classical, public channel to communicate each other the alphabets used to, respectively, measure and prepare the physical qubit state. The non-matching events are then discarded. The remaining bits form the **raw (or sifted) key**;
4. The two end users put under test part of their raw key in order to estimate the **quantum bit error rate (QBER)**, a figure of merit quantifying the amount of noise present during the communication and/or the amount of information possibly gathered by Eve. According to the QBER, two possible conclusions are possible:
 - Whenever the QBER is too high, the protocol is aborted, and a new run is started from the beginning;
 - If the QBER is lower than a chosen upper bound t , the protocol proceeds with a sifting algorithm, mainly composed by a **privacy amplification** and a **information reconciliation** stages, in order to retrieve the **(complete) secret key**.

In the latter instance, assuming no further communication or detection errors, any disagreement between Alice's and Bob's bits is ascribed to the action of an eavesdropper on the quantum channel. Privacy amplification and error correction are thus used to discard such errors, yielding to a secure key unknown to Eve. A graphical sketch of

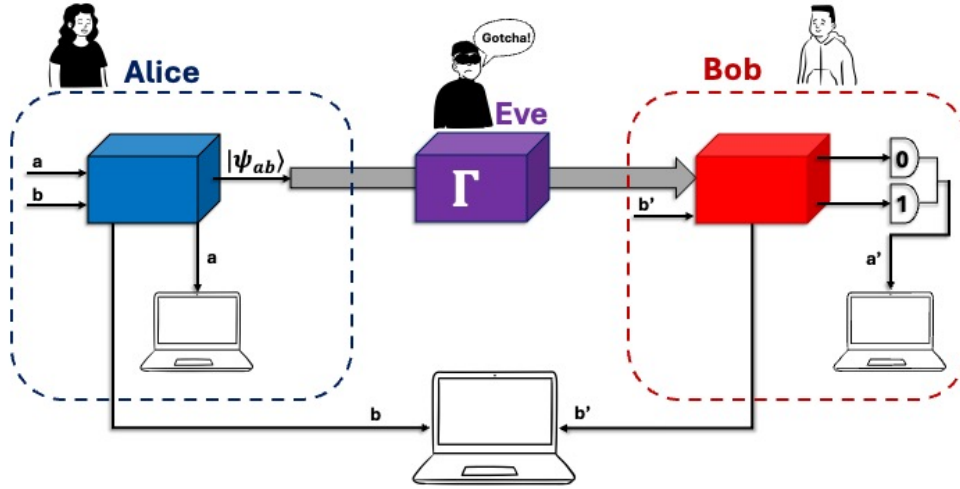


Figure 3.2: Sketch summarizing the BB84 protocol. Alice creates two strings of random bits a and b according to which she chooses, respectively, the state and the alphabet to use to encode her bit of information into the qubit state $|\psi_{ab}\rangle$ she delivers to Bob. The qubit travels through a quantum channel where Eve can act. The effect of Eve's action, together with the noise, is represented by the quantum channel $\Gamma(|\psi_{ab}\rangle\langle\psi_{ab}|)$. Bob uses a string of random bits b' to select an alphabet to measure the qubit he receives, retrieving a string of bits a' according to his measurement outcomes. The string of bits b and b' are communicated via a classical public channel to discard the non-matching rounds. After the raw key is retrieved, and the QBER test has been passed, Alice and Bob use their strings a and a' to perform the sifting algorithm.

the BB84 is presented in Fig. 3.2.

Table 3.1 proposes an example of a 15-bit BB84 protocol, with the eavesdropper implementing an intercept and resend attack strategy. In such an example Eve introduces an error during the tenth round. Differently, despite having correctly leaked the bit of information during the fourth and the ninth round, these latter are discarded due to a different choice of the encoding/decoding bases by, respectively, Alice and Bob. The output is a 12-bit sifted key (arising from the rounds 1 – 2 – 3 – 5 – 6 – 7 – 8 – 10 – 11 – 12 – 13 – 14 – 15), with Eve knowing 7 bits out of 12 of the sifted key (rounds 2 – 4 – 5 – 8 – 9 – 11 – 12 – 15), while being totally uncertain in the other ones. In one

Table 3.1: Example of a 15-bit BB84 protocol, with Eve implementing an intercept and resend attack strategy. The letter a identifies the bit of information, with 0 and 1 values referring to the eigenstates corresponding to the eigenvalues, respectively $+1$ and -1 of the suitable encoding basis. The b letter denotes the encoding basis of the bit of information into the physical qubit: 0 corresponds to the Pauli-Z basis, while the value 1 to the Pauli-X basis. The green lines refer to the accepted qubits, whereas the red lines correspond to the discarded ones. The violet lines identify the round where Eve correctly leaks the bit of information during the communication.

Alice			Eve				Bob		
a	b	$ \psi_{ab}\rangle$	b_E	a_E	$\Gamma(\psi_{ab}\rangle\langle\psi_{ab})$		b'	$ \psi_{Bob}\rangle$	a'
0	0	$ 0\rangle$	1	0	$ +\rangle\langle+ $		0	$ 0\rangle$	0
1	1	$ -\rangle$	1	1	$ -\rangle\langle- $		1	$ -\rangle$	1
0	1	$ +\rangle$	0	1	$ 1\rangle\langle 1 $		1	$ +\rangle$	0
1	0	$ 1\rangle$	1	1	$ -\rangle\langle- $		1	$ -\rangle$	1
0	0	$ 0\rangle$	0	0	$ 0\rangle\langle 0 $		0	$ 0\rangle$	0
1	1	$ -\rangle$	0	1	$ 1\rangle\langle 1 $		1	$ -\rangle$	1
0	0	$ 0\rangle$	1	1	$ -\rangle\langle- $		0	$ 0\rangle$	0
1	1	$ -\rangle$	1	1	$ -\rangle\langle- $		1	$ -\rangle$	1
0	0	$ 0\rangle$	0	0	$ 0\rangle\langle 0 $		1	$ +\rangle$	0
1	1	$ -\rangle$	0	1	$ 1\rangle\langle 1 $		1	$ +\rangle$	0
0	1	$ +\rangle$	1	0	$ +\rangle\langle+ $		1	$ +\rangle$	0
1	0	$ 1\rangle$	0	1	$ 1\rangle\langle 1 $		0	$ 1\rangle$	1
0	1	$ +\rangle$	0	0	$ 0\rangle\langle 0 $		0	$ -\rangle$	1
1	0	$ 1\rangle$	1	1	$ -\rangle\langle- $		0	$ 1\rangle$	1
0	1	$ +\rangle$	1	0	$ +\rangle\langle+ $		1	$ +\rangle$	0

case (namely, round 10), despite having correctly leaked the bit of information, Eve introduces an error (Alice's and Bob's bits of information do not coincide) that can be detected during the sifting stage. In conclusion, Alice and Bob will share 11 bits out of 12 of the sifted key, with Eve knowing 6 bits of it. Due to Alice and Bob having larger mutual information than Alice and Eve, it is possible to distill a secret key via suitable sifting algorithms.

In a MUB-based QKD protocol, the choice of non-commuting observables is crucial to discard some rounds, in order to prevent a malicious user from leaking an arbitrarily large amount of bits of the sifted key. Moreover, being the probability of measuring the eigenstates of one basis evenly distributed on the other, it allows to detect errors introduced by Eve during the communication. A different approach to QKD relies on quantum correlations, and will be discussed in the next paragraph.

3.2.2 Entanglement-based protocols: Ekert-1991 (E-91) protocol

An other widely used QKD protocol, based on quantum-correlated bipartite states, is the one proposed by Arthur Ekert in 1991 in [77] (for this reason usually labelled **Ekert91 (E91)**).

Here, differently from the BB84 protocol discussed in section 3.2.1, the security of the communication relies on entangled (more specifically, Bell-nonlocal) pairs and on Bell test, as presented in section 2.2.2, to rule out a potentially malicious user.

The general setting of the E91 protocol is:

1. A Bell non-local state (2.20), such as the singlet state $|\psi_{AB}^-\rangle$ is distributed between the two end users Alice and Bob;
2. Alice and Bob perform local random measurements of conjugated CHSH observables (see Section 2.2.2): $\hat{A}_0 = \hat{Z}_A$, $\hat{A}_1 = (\hat{X}_A + \hat{Z}_A)/\sqrt{2}$, $\hat{A}_2 = \hat{X}_A$ for Alice, and $\hat{B}_0 = (\hat{X}_B + \hat{Z}_B)/\sqrt{2}$, $\hat{B}_1 = \hat{X}_B$, $\hat{B}_2 = (\hat{X}_B - \hat{Z}_B)/\sqrt{2}$ for Bob;
3. Similarly to the BB84 protocol, Alice and Bob publicly announce their measurement settings over a classical, authenticated channel. The measurement outcomes

corresponding to specific combinations of measurement settings are used to generate the sifted key. The remaining data are used to calculate the Bell parameter S , as in Eq. (2.18), in order to assess the security of the channel and detect potential eavesdropping.

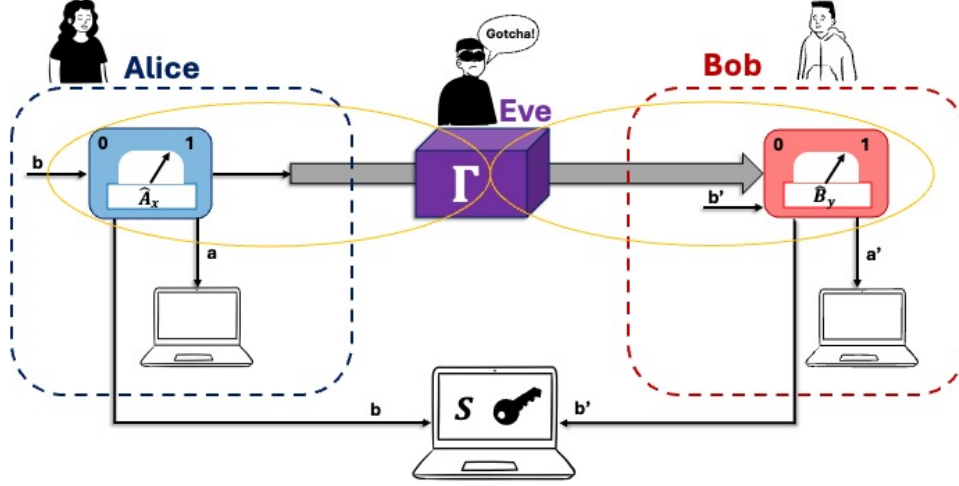


Figure 3.3: Sketch of the E91 protocol [77]. Alice and Bob share a maximally entangled state such as $|\psi_{AB}^-\rangle$. Alice and Bob perform measurement according to the values of suitable strings of characters, respectively, b and b' . They then communicate each other the performed measurement, storing locally their measurement outcomes. According to the corresponding measurement bases, they use their data to either retrieve the secret key or estimate the Bell parameter S (2.14), discarding the useless data. As soon as $|S| \leq 2$ the protocol is aborted, not being possible to exclude that entanglement is being deteriorated by a potentially malicious user, whose action is, again, represented by a quantum channel $\hat{\Gamma}$.

More thoroughly, whenever $|S| \leq 2$ the protocol is aborted: such a value for the Bell parameter flags out either that the two parties are not truly quantumly correlated, that might be an attempt of eavesdropping by a malicious user, or some fault in the measurement devices.

Conversely, a maximal violation of the CHSH inequality rules out the presence of an eavesdropper, under the assumption of no experimental faults. When the security test is passed, the protocol proceeds:

4. In the bases-matching rounds, Alice and Bob expect perfectly (anti-)correlated results: they then process their outcomes (via a proper sifting algorithm) to retrieve a secret, shared key.

An example of E-91 protocol is presented in Tab. 3.2. Given the aforementioned choice of observables, the CHSH (Bell) parameter is calculated as $S = \left| \langle \hat{A}_0 \hat{B}_0 \rangle + \langle \hat{A}_0 \hat{B}_1 \rangle + \langle \hat{A}_2 \hat{B}_0 \rangle - \langle \hat{A}_2 \hat{B}_1 \rangle \right|$.

Rather, whenever the $(b = 1, b' = 0)$ and $(b = 2, b' = 0)$ the measurement outcomes on Alice's and Bob's side experience the maximal correlation: these latter rounds are therefore used to retrieve the secret key. Other round with different combinations of measurement settings are discarded, being not useful for neither the validation of Bell-nonlocality, nor experiencing correlations in the measurement outcomes.

Differently from a MUB-based protocol (such as BB84), with security proofs usually relying on no-cloning theorem and the impossibility of perfect distinguishability between non-orthogonal states, E91 protocol capitalizes over the non-local nature of quantum mechanics, with eavesdropping strategies inducing elements of physical reality affecting the non-local features of quantum theory.

3.2.3 Quantum cryptography: take-home message

Quantum cryptography, regardless the theoretical paradigm and the experimental platform used to implement the protocols, relies on distinctive feature of quantum mechan-

Table 3.2: Example of a 10-round E-91 protocol, adopting the singlet state (2.20). Likewise the example for the BB84 protocol 3.1, a and a' correspond to the results of, respectively, Alice's and Bob's measurement. a and a' are string of bits, with values 0 and 1 associated with the possible measurement outcomes. Similarly, b and b' , with $0 \leq b, b' \leq 2$ identify the chosen measurement setting for, respectively, Alice and Bob. The green lines identify the round used to retrieve the secret key, while the black lines those used to perform the Bell test. In conclusion, red lines correspond to discarded rounds: the chosen measurement settings prevent their exploitation for either the secret key or the Bell test.

Alice		Bob	
a	b	b'	a'
0	0	0	1
0	1	0	0
1	1	2	0
1	0	1	0
0	2	1	0
1	2	0	0
0	1	1	0
1	2	2	1
1	1	0	1
0	0	2	1

ics to spot the presence of adversarial users compromising the communication. More specifically, unconditional security in QKD is grounded on the unavoidable modification a measurement by Eve introduces on the state of the information carrier, together with the impossibility of cloning the state of a quantum system with arbitrary fidelity (**no-cloning theorem**). Moreover, a degree of randomness is vital to prevent an eavesdropping from building patterns to design specific attack strategies. In a MUB-based protocol, such as the BB84 discussed in section 3.2.1, this is translated into a randomized choice of qubit-preparation bases and measurement bases by, respectively, Alice and Bob; while in an entanglement-based protocol (e.g. the E91 protocol, presented in section 3.2.2), randomness arises in the choice of the measurement observable by both Alice and Bob. Furthermore, part of the exchanged bits are required to be sacrificed in order to distill the secret key (in first instance, to retrieve the raw key. Subsequently, sifting strategies may require additional bits to be discarded to obtain the secret key).

Overall, QKD is capable of granting unconditional security in communication, not achievable by using exclusively classical resources, at the price of introducing randomness in the protocol so as to detect malicious adversaries, and potentially the sacrifice of a large amount of data in order to retrieve a secret key on which eavesdropper have no information.

3.3 Towards secure DQS

After having pinpointed the very foundational working scheme of QKD, here are reported to different DQS protocols with security proofs inspired by QKD concepts discussed in the previous section.

The first one, proposed by Z. Huang, C. Machiavello and L. Maccone, relies on randomized probe states and operations to certify security while performing the estimation task. In the second approach, proposed by N. Shettel, E. Kashefi and D. Markham, security is guaranteed by ensuring that any adversarial introduces detectable interference. The security proof is then grounded on cryptographic concepts, such as integrity, soundness and privacy, used to retrieve formal bounds on the estimation performances under potential tampering attacks.

3.3.1 The Huang-Machiavello-Maccone (HMM) protocol

In [115] Z. Huang, C. Machiavello and L. Maccone propose a general secure sensing protocol of a unitary-encoded parameter, relying on different quantum states used for the estimation task and the securization part.

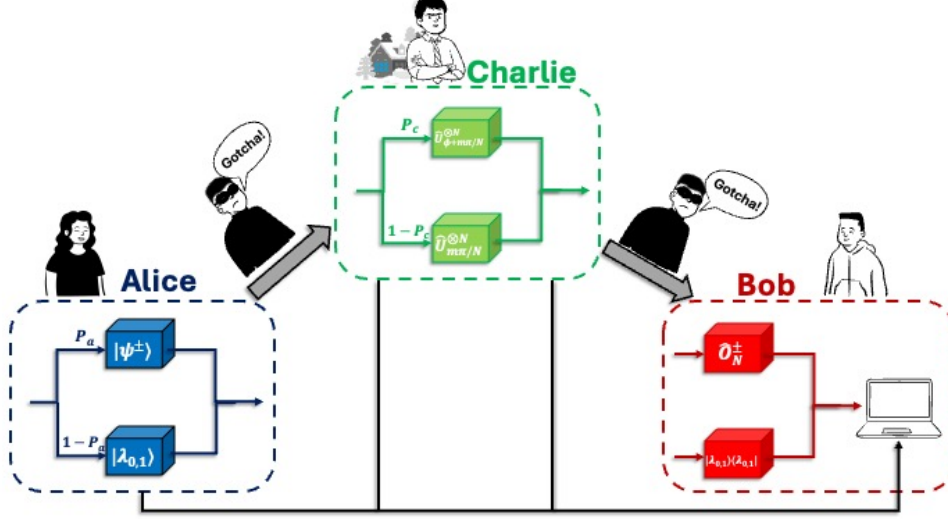


Figure 3.4: Sketch of the secure DQS protocol proposed in [115]. A provider, Alice prepares phase-sensitive states $|\psi_N^\pm\rangle$ with probability P_a . An intermediate, possibly remote party, Charlie, encodes the phase shift ϕ Alice and Bob aim at estimating, with probability P_c . The other end user, Bob, performs suitably chosen measurement according to the instructions provided by Alice and Bob. Quantum states are delivered on quantum, untrusted channel, whereas communication among the parties occur on a classical channel.

The protocol is sketched in Fig. 3.4 and presented below:

1. Alice, who acts as a provider, chooses to prepare the following probe states with given probabilities:

$$\begin{aligned} \frac{P_a}{2} : \quad |\psi_N^\pm\rangle &= \frac{|\lambda_m\rangle^{\otimes N} \pm |\lambda_M\rangle^{\otimes N}}{\sqrt{2}}; \\ \frac{1-P_a}{2} : \quad |\lambda_0\rangle &= |\lambda_m\rangle^{\otimes N}, \quad |\lambda_1\rangle = |\lambda_M\rangle^{\otimes N}, \end{aligned} \quad (3.1)$$

where $|\psi_N^\pm\rangle$ are the metrologically relevant states, while $|\lambda_{0,1}\rangle$ are quantum states used for security checks. Here $|\lambda_m\rangle, |\lambda_M\rangle$ correspond the eigenstates associated with, respectively, the maximal and the minimal eigenvalues of the generator $\hat{G}$ of the encoded parameter. She sends then each probe to Charlie, a trusted intermediate party;

2. Charlie keeps count of how many probes are going through its node, in order to assess the presence of an eavesdropper using their own probes: if it is the case, the protocol is aborted. Conversely, he chooses to randomly encode the phase, or to just reroute the state to the other end party, Bob. Charlie's action can be summarized as follows:

$$\begin{aligned} \text{Encoding } P_c & \quad \hat{U}_{\phi+\pi j/N}^{\otimes N}; \\ \text{Rerouting } 1-P_c & \quad \hat{U}_{\pi j/N}^{\otimes N}; \end{aligned} \quad (3.2)$$

with Charlie broadcasting the same operation on all the qubits of the probe state. j is randomly chosen in the range $[0, N-1]$, so that the quantum channel connecting Charlie and Bob is dephasing.

Charlie's operation has no effect on the decoy states used for the check rounds, while applies a phase difference on the metrological probes: Similar result holds for the rerouting action. The possible output state are, respectively,

$$\begin{aligned}
 P_a P_c : \quad \hat{U}_{\phi+\pi j/N}^{\otimes N} |\psi_N^\pm\rangle &= \frac{|\lambda_m\rangle^{\otimes N} \pm e^{i(N\phi+j\pi)(\lambda_M-\lambda_m)} |\lambda_M\rangle^{\otimes N}}{\sqrt{2}}, \\
 P_a(1-P_c) : \quad \hat{U}_{\pi j/N}^{\otimes N} |\psi_N^\pm\rangle &= \frac{|\lambda_m\rangle^{\otimes N} \pm |\lambda_M\rangle^{\otimes N}}{\sqrt{2}}, \\
 (1-P_a) : \quad \hat{U}_{\pi j/N}^{\otimes N} |\lambda_{0,1}\rangle &= |\lambda_{0,1}\rangle.
 \end{aligned} \tag{3.3}$$

3. Charlie sends the probe to Bob;
4. Alice communicates to Bob what state she did prepare on each round. Communication takes place on a public, classical channel. According to Alice's information, Bob performs suitable measurements. More specifically,

$$\begin{aligned}
 \text{Metrological probe: } \hat{O}_\pm^N &= \left(\frac{(|\lambda_m\rangle \pm |\lambda_M\rangle)(\langle\lambda_m| \pm \langle\lambda_M|)}{2} \right)^{\otimes N}; \\
 \text{Decoy states: } &|\lambda_0\rangle \langle\lambda_0|, |\lambda_1\rangle \langle\lambda_1|;
 \end{aligned} \tag{3.4}$$

5. **Security check:**

- If the preparation and the measurement of the decoy states $|\lambda_{0,1}\rangle$ does not match, the presence of an eavesdropper tampering the state is flagged. The protocol is therefore aborted;
- Whenever Alice's preparation and Bob's measurement of the phase-sensitive states do not match, the latter informs Charlie, who will inform whether he did apply the rerouting strategy. More specifically:

$$\hat{U}_{m\pi/N} |\psi_N^\pm\rangle = \begin{cases} |\psi_N^\pm\rangle & m \text{ even,} \\ |\psi_N^\mp\rangle & m \text{ odd.} \end{cases} \tag{3.5}$$

If the measured states differ from the expected ones, an eavesdropping attempt is detected, and the protocol is aborted;

6. Under the assumption of noiseless communication, Charlie discloses the value of m , and Bob exploits the phase-encoded probes to provide an estimation of ϕ via the quantity

$$\langle \hat{O}_+^N \rangle + \langle \hat{O}_-^N \rangle = \cos(N\phi + m\pi)(\lambda_M - \lambda_m). \tag{3.6}$$

The HMM protocol therefore is rooted on two different types of rounds (namely, check rounds and estimation rounds) decided by the combination of the preparation of a suitable probe state and an action delegated to a third, possibly remote, party who ultimately select how the probe state shall be used, and on an accept/abort strategy. The ultimate precision limit on the reconstruction of the parameter ϕ will depend on the probability of Alice sending a phase sensitive state and Charlie encoding the target phase. On the adversary's side, it is possible for them to gain some information, at the risk of being detected, and the protocol aborted.

3.3.2 The Shettell-Kashefi-Markham (SKM) protocol

A different theoretical framework for secure sensing on networks has been proposed by N. Shettell, E. Kashefi and D. Markham (SKM) in [111]. Here, the authors define general figures of merit derived from cryptographic background, in order to evaluate the robustness of a metrological strategy against malicious users potentially eavesdropping the estimation task. More thoroughly, SKM focus on the following three concepts:

Definition 3.3.1. Privacy: A DQS protocol is said to be **private** if a malicious adversary is prevented from gaining any information.

Consequently, the quantum state possessed by the eavesdropper is represented by a fully mixed state $\hat{\rho}_E = \mathbb{1}/2^m$. Such a requirement follows directly from cryptographic considerations, assessing the inability of a non-authorized user of estimating the object parameter.

Definition 3.3.2. Soundness: A DQS protocol is said to be δ -sound whenever the action of a malicious adversary spoils the ideal state no more than a suitable threshold δ .

Definition 3.3.2 can be quantified as

$$\frac{1}{|\mathcal{K}|} \sum_{\kappa \in \mathcal{K}} \text{Tr} \left(\hat{\Pi}_\kappa \hat{\rho}_{\text{out}}(\kappa, \hat{\Gamma}) \right) \leq \delta, \quad (3.7)$$

where $\mathcal{K}$ identifies the set of all the possible classical keys κ , $\hat{\rho}_{\text{out}}(\kappa, \hat{\Gamma})$ is the quantum state encrypted by the κ -th key, undergoing attack $\hat{\Gamma}$, and $\hat{\Pi}_\kappa$ is the projector over the accepted output of proper flag qubits and orthogonal complement to the ideal, untampered output state. Under the assumption of pure output states, Eq. 3.7 is simplified as

$$\mathbb{E} [p_{\text{acc}}(1 - F(\hat{\rho}_{\text{id}}, \hat{\rho}'))] \leq \delta, \quad (3.8)$$

with p_{acc} referring to the acceptance probability, and $\hat{\rho}_{\text{id}}$, $\hat{\rho}'$ to, respectively, the ideal and the tampered probe state. Remarkably, the set of possible cryptographic keys, as well as the acceptance probabilities etc depend on the specific DQS protocol. As a consequence, the soundness as well is model dependent.

Definition 3.3.3. Integrity: A DQS protocol is said to be **integer** whenever it retains the correct working scheme in the presence of malicious adversaries.

Integrity is that property ensuring that the eavesdropping attack biases the metrological performances up to a cutoff ε , depending on the specific DQS algorithm.

More specifically, the sensing protocol aims at estimating an unknown parameter θ via a suitable observable $\hat{O}$: measurement outcomes are used to infer the expectation value of the observable $f(\theta) = \langle \hat{O} \rangle_{\hat{\rho}_\theta} = \text{Tr}(\hat{\rho}_\theta \hat{O})$, and then apply f^{-1} so as to retrieve the estimation of θ . Given the spectrum $\{o_i\}_i$ of the observable $\hat{O}$, its expectation value can be experimentally estimated as

$$\tilde{f} = \frac{1}{n} \sum_{j=1}^n o_j, \quad (3.9)$$

where n denotes the number of probes used for the estimation.

In the scenario in which a malicious user may have tampered with physical resources, the estimation remains meaningful as long as the real quantum state is close to the ideal resource up to a distance ε :

$$\frac{1}{n} \sum_{j=1}^n D(\hat{\rho}'^{(j)}, \hat{\rho}_\theta) \leq \varepsilon, \quad (3.10)$$

where $\hat{\rho}'^{(j)}$ is the reduced real state with only the j -th block preserved (no assumptions are made on the possible attacks the adversary may attempt), while $D(\cdot)$ is the trace distance. The bias possibly introduced by the eavesdropper can be bounded as follows:

$$\left| \mathbb{E}(\tilde{f}') - \tilde{f} \right| = \frac{1}{n} \left| \sum_{j=1}^n \text{Tr} \left(\hat{O} (\hat{\rho}'^{(j)} - \hat{\rho}_\theta) \right) \right| \leq \frac{2o}{n} \sum_{j=1}^n D(\hat{\rho}'^{(j)}, \hat{\rho}_\theta) = 2o\varepsilon, \quad (3.11)$$

where o is the maximum eigenvalue of $\hat{O}$, and inequality (3.10) has been used. The precision discrepancy in the malicious setting compared to the ideal setting is calculated similarly:

$$\left| \Delta^2 \tilde{f}' - \Delta^2 \tilde{f} \right| \leq \frac{4o^2}{n^2} \sum_{j=1}^n D(\hat{\rho}'^{(j)} \otimes \hat{\rho}'^{(j)}, \hat{\rho}_\theta \otimes \hat{\rho}_\theta) + 4o^2 \varepsilon^2 \leq \frac{8o^2 \varepsilon}{n} + 4o^2 \varepsilon^2, \quad (3.12)$$

where the triangle inequality $D(\hat{\rho}'^{(j)} \otimes \hat{\rho}'^{(j)}, \hat{\rho}_\theta \otimes \hat{\rho}_\theta) \leq 2D(\hat{\rho}'^{(j)}, \hat{\rho}_\theta)$ and the result in Eq. (3.11) have been used.

Crucially, for sufficiently small ε , i.e. tampered states ε -distant from the ideal one, a linear expansion of $\tilde{f}'$ about $\tilde{f}$ (and viceversa) figures as a reasonable approximation. Consequently, the upper bounds (3.11) and (3.12) read, respectively,

$$\begin{cases} |\mathbb{E}[(\theta' - \theta)]| = \frac{\mathbb{E}[(\tilde{f}' - \tilde{f})]}{|\partial_\theta \langle \hat{O} \rangle_\theta|} \leq \frac{2o\varepsilon}{|\partial_\theta \langle \hat{O} \rangle_\theta|} \\ |\Delta^2 \theta' - \Delta^2 \theta| = \frac{|\Delta^2 \tilde{f}' - \Delta^2 \tilde{f}|}{|\partial_\theta \langle \hat{O} \rangle_\theta|^2} \leq \frac{4o^2(2\varepsilon/n) + \varepsilon^2}{|\partial_\theta \langle \hat{O} \rangle_\theta|^2} \end{cases} \quad (3.13)$$

In their work [111], SKM put under test these concepts with two different abort-based

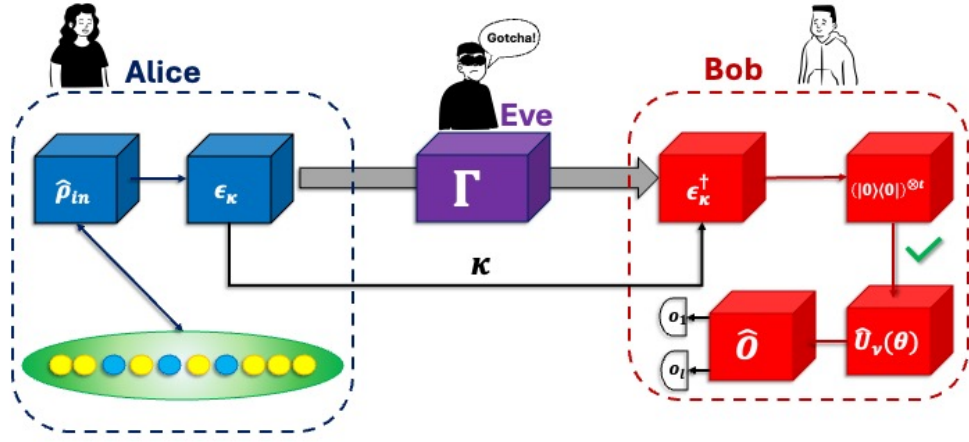


Figure 3.5: General sketch of the SKM approach. Alice prepares the initial state $\hat{\rho}_{in}$, composed by a ν -qubit (yellow circles) metrological probe and t flag qubits (cyan circles), each prepared in the $|0\rangle$ state, randomly placed in the initial state. She then delivers the encrypted state (via the operator $\hat{\epsilon}_\kappa$) to Bob over an untrusted quantum channel. The eavesdropper's action is represented by a map $\hat{\Gamma}$, producing the output state $\hat{\rho}_{out}$. Bob decrypts the received state by applying $\hat{\epsilon}_\kappa^\dagger$, then performs a security involving the ancillary qubits. Only provided that $|0\rangle\langle 0|$ is measured on all the flag qubits, he then proceeds with the metrological task. The black continuous line represents a classical, authenticated channel used by Alice and Bob to communicate the encryption/decryption scheme.

protocols, represented in Fig. 3.5 and sketched below

1. As a preliminary step, the two end users, Alice and Bob, randomly choose a key $\kappa \in \mathcal{K}$, corresponding to a proper encryption operation;
2. Alice prepares a $m = \nu + t$ -qubit initial state $\hat{\rho}_{in}$, made of the metrologically relevant state (with probe size ν) and t ancillary qubits in the state $|0\rangle$, acting as a trap for the eavesdropper's activity;
3. Alice delivers the encrypted state to Bob over the untrusted quantum channel. Bob then decrypts the received state by using the chosen encryption/decryption scheme;
4. Bob performs a security check by measuring the flag qubits in the computational basis. The test is accepted only provided that $|0\rangle\langle 0|$ is measured on all the trap qubits. Conversely, protocol is aborted;
5. On the accepted quantum states, Bob uses the metrological probe to perform the estimation task.

3.4 Faithful and secure phase estimation in a network

Previous work on DQS either relied on entanglement-based protocols [109,110] or MUB-based approaches [116]. Moreover, security has been proved against individual attacks only. A more general setting, dealing with two trusted parties communicating and implementing the estimation task via communication channels possessed by Eve, has been described by the HMM and SKM papers [111,115], presented in section 3.1.1.

Remarkably, SKM work [111] introduced fully cryptographic methods holding for discrete-variable quantum estimation protocols. The major downside regarding the practical implementations of these general protocols lies in the considerable amount of resources needed to achieve an acceptable security level (e.g., because of the abort-based strategy) and the optimal estimation performance. Furthermore, encryption/decryption schemes usually involve demanding algorithms, further complicating the issue.

Here are presented two new protocols, based on the setting proposed by HMM paper [115] and the theoretical concepts introduced by SKM [111], also encompassing collective attack among subsequent rounds, representing the most general attack allowed in QKD. In order to do so, the two protocols, presented in [8], are analyzed under the following requirements: *faithfulness* and *security*, related to, respectively, the capability of the trusted parties of estimating how much the malicious user has tampered with the optimal probe state, leading to a biased estimation with respect to the ideal conditions, and the amount of information *leaked* by Eve on the target parameter.

More specifically:

Definition 3.4.1. Faithfulness: A DQS protocol is ε -faithful if, when proceeding to estimation, it guarantees that the true phase-encoded state is ε -distant from the ideal parameter-encoded state for a suitable distance [8].

Such a concept quantifies the resilience against tampering attacks after the parameter's encoding, thus bounding the estimation quality. This is a combination of the *privacy* and *soundness* concepts introduced in [111].

Definition 3.4.2. Security: A DQS protocol is ε -secure if, at any point, Eve's state is ε -distant from the completely mixed state, for a suitable distance measure.

Remarkably, security quantifies the robustness against leakage attacks via the distance of Eve's share of the quantum state from the maximally mixed one, preventing any possible estimation strategy from being implemented [8].

Differently from previous works on the topic [111,115], no assumptions on the quantum adversary's attack capabilities are made, thus allowing what are referred to in QKD as **general-coherent (GC)** attacks, i.e. the possibility of storing ancillae entangled with the probe states across several runs in a quantum memory, and using them for subsequent collective post-processing [117]. Nonetheless, both protocols presented in section 3.4.2 and section 3.4.3 can be equivalently formulated in an entanglement-based or a MUB-based framework (see [116]). Table 3.3 compares the protocols discussed in the following sections to other state-of-the-art works present in literature.

3.4.1 One-way protocol

The first DQS protocol here proposed deals with a provider with full quantum capabilities, Alice, supplying a remote end user, Bob, with quantum states $|\psi\rangle$ over a public quantum channel, where a potentially malicious user have full access. In the one-way picture here described, Bob exploits the quantum resources he receives through the quantum channel to either encode the target parameter via a unitary operation $\hat{U}(\theta)$ or implement a security check, and measure the quantum state he holds. Any communication between the two end users, Alice and Bob, is assumed to be public, thus controlled by the malicious adversary.

The protocol is sketched in Fig. 3.6

With no loss of generality, the probe state has probe size ν , while the parameter is assumed to be a phase shift ϕ encoded via the unitary rotation $\hat{U}(\phi) = e^{-i\hat{Y}\phi}$ on each qubit.

Table 3.3: Comparison of several DQS protocol present in literature. Eavesdropping attacks are labelled according to the quantum capabilities Eve can deploy; perfect security is granted whenever the malicious user possesses a parameter-independent, completely mixed state, whereas zero-tolerance corresponds to passed security checks; faithfulness is classified in threshold-based, whenever the protocol allows for a safety margin in the detected errors, abort-based when no such a margin is allowed. Differently, *a posteriori* protocols rely on full tomographic analysis of the received probe.

DQS Protocol	Quantum communication	Attacks	Security	Faithfulness	Entanglement-based
Protocol 3.4.1	1- & 2-way	General-coherent	Perfect (1w), None (2w)	Threshold-based	Yes
Protocol 3.4.3	1- & 2-way	General-coherent	Perfect (1w), None (2w)	Threshold-based	No
[109, 110]	1-way	Classical	Perfect	A posteriori	Yes
[116, 118]	1-way	Individual	Perfect	A posteriori	No
[115]	1- & 2-way	Individual	Perfect (1w), None (2w)	Abort-based	No
[111]	1- & 2-way	Individual	Perfect (1w), Zero-tolerance (2w)	Abort-based	No (trap code), Yes (Clifford code)

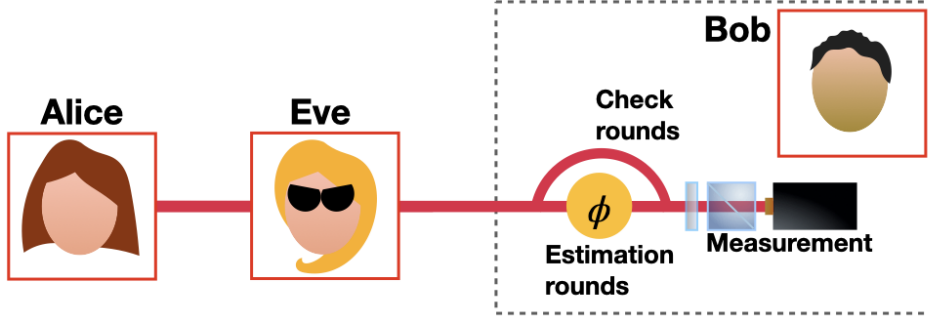


Figure 3.6: Conceptual sketch of the one-way protocol described in this section. Here, Alice supplies Bob with quantum probes in order to estimate a phase ϕ at his own location. Transmission takes place on a quantum channel potentially controlled by an eavesdropper, who can tamper with the probe state so as to compromise the estimation. Picture inspired by [8].

It is known in literature [16,17,24,25] that the optimal probe states for phase estimation are of the form

$$\begin{aligned} |0/1\rangle &= \frac{|R\rangle^{\otimes \nu} \pm |L\rangle^{\otimes \nu}}{\sqrt{2}}; \\ |\pm\rangle &= \frac{|R\rangle^{\otimes \nu} \pm i|L\rangle^{\otimes \nu}}{\sqrt{2}}, \end{aligned} \quad (3.14)$$

where $|R/L\rangle$ are the eigenstates of the Pauli-Y matrix. For the sake of brevity, in this chapter, Pauli matrices written in bold characters $\hat{\mathbf{X}}$, $\hat{\mathbf{Y}}$, $\hat{\mathbf{Z}}$ refer to collective operations applied to the states in Eq. (3.14).

The entanglement-based formulation of the one-way protocol is here presented:

One-way Entanglement-based DQS protocol

- 1) **Preparation:** Alice prepares the entangled state

$$|\psi_{\nu+1}^+\rangle_{AB} = \frac{|0\rangle_A |\pm\rangle_B + |1\rangle_A |\pm\rangle_B}{\sqrt{2}}, \quad (3.15)$$

where $|0/1\rangle$ is a one-qubit state, kept by Alice. She sends the ν -qubit register B to Bob via the quantum channel;

- 2) **Encoding:** After receiving his register, Bob chooses one out of three possible actions, at random:
 - a) with probability p_c , he does not encode the phase. The state is therefore used to perform security checks;
 - b) with probability p_e , he encodes the target phase ϕ via the unitary operation $\hat{U}(\phi)$;
 - c) with probability $p_d = 1 - p_e - p_c$, he discards the received state and proceeds to the next step of the protocol;
- 3) **Measurement:** Alice randomly measures one of the Pauli matrices $\hat{X}_A$, $\hat{Y}_A$ and $\hat{Z}_A$. In turn, Bob performs one out of two actions, according to what he did in the encoding step:
 - a) if the phase has not been encoded, he measures one of the Pauli matrices $\hat{\mathbf{X}}_B$, $\hat{\mathbf{Y}}_B$ and $\hat{\mathbf{Z}}_B$, chosen with uniform probability;
 - b) if the phase has been encoded, he measure either $\hat{\mathbf{X}}_B$ or $\hat{\mathbf{Z}}_B$, chosen at random;

- 4) **Reconciliation and sifting:** After T repetitions of the previous steps, Alice communicates to Bob the measured observables and the corresponding results. Bob then saves the following rounds, discarding all the others:

- a) $\hat{X}_A \otimes \hat{Z}_B, \hat{Z}_A \otimes \hat{X}_B, \hat{Y}_A \otimes \hat{Y}_B$ if the phase has not been encoded;
- b) $\hat{X}_A \otimes \hat{Z}_B, \hat{Z}_A \otimes \hat{X}_B$ if the phase has been encoded;

- 5) **Fidelity check:** From the type-a) sifted rounds, Bob estimates the fidelity of the actual state with respect to the ideal one as

$$F = \frac{1 + \langle \hat{X}_A \otimes \hat{Z}_B \rangle + \langle \hat{Z}_A \otimes \hat{X}_B \rangle + \langle \hat{Y}_A \otimes \hat{Y}_B \rangle}{2}, \quad (3.16)$$

where the expectation value taken with respect to the (possibly) tampered state. Provided that the fidelity $F \geq 1 - \varepsilon^2$, with ε being a suitable security threshold, Bob proceeds to the next step. Conversely, the protocol is aborted;

- 6) **Estimation:** From the type-b) sifted rounds, Bob estimates the target phase as follows:

$$\hat{\phi} = \frac{1}{2} \arccos \left(\frac{\langle \hat{X}_A \otimes \hat{Z}_B \rangle + \langle \hat{Z}_A \otimes \hat{X}_B \rangle}{2} \right), \quad (3.17)$$

with the expectation value taken with respect to the phase-encoded tampered state.

The protocol's essence lies in the alternating types of rounds on Bob's side: check rounds, used to spot and quantify the presence of Eve; estimation rounds, actually used for the metrological task, and discarded rounds, used to grant security against GC attacks, as it is customary in QKD.

Probabilities p_c , p_e and $p_d = 1 - p_e - p_c$, together with measurement randomization, define the fraction of rounds addressed to check, estimation and discard after sifting. In the large T limit, such fractions are expected to be, respectively, $N_c \simeq \frac{Tp_c}{3}$, $N_e \simeq \frac{Tp_e}{3}$ and $N_d = \frac{(2+p_d)T}{3}$. The latter rounds assess robustness against GC attacks in the limit $N_d \gg N_e + N_c$, via a suitable $p_d \gg 0$. Remarkably, if the analysis is restricted to individual attacks only, $p_d = 0$ is sufficient.

The alternative formulation of the one-way protocol, this time rooted on a MUB-based approach, is listed here below:

One-way MUB-based DQS protocol

- 1) **Preparation:** Alice prepares the ν - qubit state $|\hat{\mathbf{P}}, +\rangle$, where $\hat{\mathbf{P}} = \{\pm\hat{\mathbf{X}} \pm \hat{\mathbf{Y}} \pm \hat{\mathbf{Z}}\}$, and sends the prepared state through the untrusted quantum channel;
- 2) **Encoding:** Bob chooses one of the following three actions, at random:
 - a) with probability p_c , he does not encode the phase. The state is therefore used to perform security checks;
 - b) with probability p_e , he encodes the target phase ϕ via the unitary operation $\hat{U}(\phi)$;
 - c) with probability $1 - p_e - p_c$, he discards the received state and proceeds to the next step of the protocol;
- 3) **Measurement:** Bob performs one out of two actions, according to what he did in the encoding step:
 - a) if the phase has not been encoded, he measures one of the Pauli matrices $\hat{\mathbf{X}}_B$, $\hat{\mathbf{Y}}_B$ and $\hat{\mathbf{Z}}_B$, chosen with uniform probability;

- b) if the phase has been encoded, he measure either $\hat{\mathbf{X}}_B$ or $\hat{\mathbf{Z}}_B$, chosen at random;
- 4) **Reconciliation and sifting:** After T repetitions of the previous steps, Alice informs Bob about her preparation for each round. Bob then keeps the rounds where his measurement match Alice's preparation, discarding all the others;
- 5) From the type-a) rounds, Bob estimates the fidelity of the received state with respect to the ideal one $|\hat{\mathbf{P}}, +\rangle$ as

$$F_P = \frac{1 + \langle \hat{\mathbf{P}} \rangle}{2}, \quad (3.18)$$

where the Pauli operator $\hat{\mathbf{P}}$ is averaged over the tampered state. Whenever $F_P \geq 1 - \varepsilon^2$ for all the Pauli operators $\hat{\mathbf{P}}$ and a given security threshold ε , Bob proceed with the parameter estimation. Otherwise, the protocol is aborted;

- 6) **Estimation:** From the type-b) sifted rounds, Bob provides an estimation of the target phase as

$$\hat{\phi} = \frac{1}{2} \arccos \left(\frac{1}{4} \sum_{\hat{\mathbf{P}} \in \{\pm \hat{\mathbf{X}}, \pm \hat{\mathbf{Z}}\}} \langle \hat{\mathbf{P}} \rangle \right). \quad (3.19)$$

The faithfulness and security of the entanglement-based protocol 3.4.1 is stated by the following theorem:

Theorem 3. *The one-way entanglement-based DQS Protocol 3.4.1 is perfectly secure and its faithfulness is determined by ε . Indeed, the difference of bias and variance of an unbiased estimator $\hat{\phi}$ calculated on the ideal probe state with respect to the same estimator $\hat{\phi}'$ on the tampered state are bounded, under general-coherent attacks, as*

$$\begin{aligned} |\mathbb{E}\hat{\phi} - \mathbb{E}\hat{\phi}'| &\leq \frac{\varepsilon_0}{\nu |\sin(2\nu\phi)|} \\ |\Delta^2\hat{\phi} - \Delta^2\hat{\phi}'| &\leq \frac{2\varepsilon_0 + \varepsilon_0^2}{|\nu \sin(2\nu\phi)|^2}, \end{aligned} \quad (3.20)$$

with $\varepsilon_0 = \sqrt{\frac{2}{3}\varepsilon^2 + 4f(T, N_d, \nu)}$ and $f(T, x, \nu) = (T - x - 1)\sqrt{\frac{\nu}{2x}}$ [8].

Furthermore, under the assumption of individual attacks, it is sufficient to put $N_d = 0$ and adopt the same bound on the bias as in (3.20) with $\varepsilon_0 \rightarrow \sqrt{\frac{2}{3}\varepsilon}$, while the bound on the variance distortion now reads

$$|\Delta^2\hat{\phi} - \Delta^2\hat{\phi}'| \leq \frac{2\varepsilon_0/N_e + \varepsilon_0^2}{|\nu \sin(2\nu\phi)|^2}. \quad (3.21)$$

The very same bounds (3.20) hold for the MUB-based protocol 3.4.1, provided a rescaling of the security threshold $\varepsilon^2 = \frac{2}{3}\varepsilon^2$.

Remarkably, bounds (3.20) are retrieved from (3.13), with $\langle \partial_\phi \hat{O} \rangle = 2\nu \sin(2\nu\phi)$. Faithfulness of both the entanglement-based 3.4.1 and MUB-based 3.4.1 protocols against GC attacks can be proved by using a refined version the quantum de-Finetti theorem (see [119, 120]) for quantum states processed by means of local-operations-and-classical-communication (LOCC) measurements, with a corresponding distance between the ideal and real, tampered state. The full proof can be found in [8].

3.4.2 Experimental test

Here is presented a proof-of-principle experiment of the entanglement-based protocol 3.4.1 under simplified assumptions. The goal is not, indeed, reproducing all the features of a full implementation, rather obtaining some data compatible with it, by setting $p_c = p_e = 1/2$ and $p_d = 0$, assessing, thus, individual attacks.

The experimental setting is the very same as the one described in chapter 2, with photon pairs generated via the SPDC source 2.8 and polarization-encoded qubits prepared via the C-Z gate 2.9. (Quasi-) Maximally entangled states of the form $|\psi\rangle = \frac{|H+\rangle_{AB} + |V-\rangle_{AB}}{\sqrt{2}}$ produced by the C-Z gate are then analyzed via standard polarization arrangement, made of QWP, HWP and a PBS. Coincidence windows are set at 0.1ns, each containing about 100 coincidence counts. Analogously to the phase-assisted certification of quantum steering discussed in section 2.4, the target phase ϕ is encoded directly via the HWP on Bob's measurement stage.

All the correlators involved either in the check or the estimation rounds are reconstructed as

$$\langle \hat{A} \otimes \hat{B} \rangle = \frac{\sum_{i,j} (-1)^{i+j} N_{ij}}{\sum_{i,j} N_{ij}} \quad i, j = 0, 1 \quad (3.22)$$

with $\hat{A}, \hat{B}$ being the suitable Pauli operators, and N_{ij} the coincidence counts registered. As customary, $i = 0$ corresponds to $+45^\circ$, L or H polarization states, whereas $i = 1$ to -45° , R or V polarization states.

Check rounds highlight a fidelity $F = 0.937 \pm 0.017$, thus $\varepsilon = 0.251 \pm 0.034$, retrieved from events collected in 200 detection windows.

All of the discrepancies are attributed to the tampering attack deployed by Eve. The phase estimator (3.17) has been employed, whereas the variance of the tampered phase estimator has been retrieved via the error propagation on Eq. (3.22):

$$\Delta^2 \hat{\phi}' = \frac{\Delta^2(\hat{Z}_A \otimes \hat{X}_B) + \Delta^2(\hat{X}_A \otimes \hat{Z}_B)}{4 \left(4 - \left(\langle \hat{X}_A \otimes \hat{Z}_B \rangle + \langle \hat{Z}_A \otimes \hat{X}_B \rangle \right)^2 \right)}, \quad (3.23)$$

where the overbar symbol identifies the average over 200 experimental values.

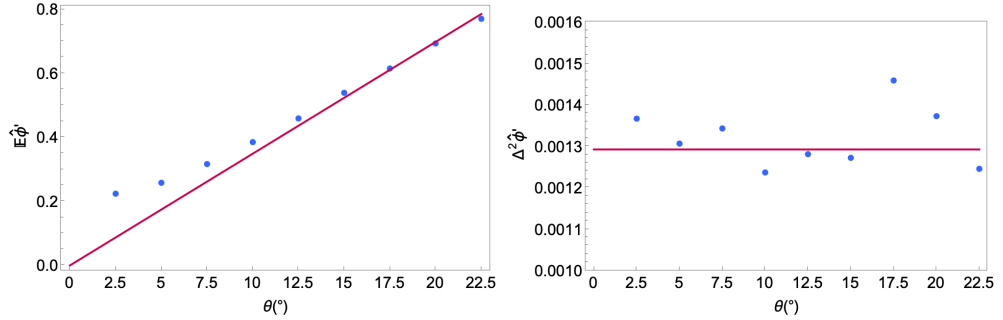


Figure 3.7: Result of the phase estimation as a function of Bob's HWP tuning angle $\theta = \phi/2$. Left panel) Expectation value of the tampered phase estimator $E\hat{\phi}'$ (blue points) compared with the theoretical dependence $\phi' = 2\theta$ (solid red line). Right panel) Variance of the experimental phase estimation $\Delta^2 \hat{\phi}'$ (blue points) compared with the Cramér-Rao bound holding for the ideal, maximally entangled state (solid red line). Picture taken from [8].

The analysis of the phase estimator (3.17) as a function of Bob's HWP angle is presented in Fig. 3.7. Here it is highlighted a more significant impact of tampering attack on smaller values of ϕ . Interestingly, such a behavior is not mirrored in the variance, which features a scattered distribution around the ideal CRB.

Deviations of the biased estimator and variance distortion with respect to the ideal scenario as a function of the experimental setting are reported in Fig. 3.8. Here, both the plots clearly show that the experimental bias and the variance distortion theoretically predicted by theorem 3 overestimate the experimental ones. Correspondingly, Eve's tampering capabilities may be significantly overestimated. This feature follows

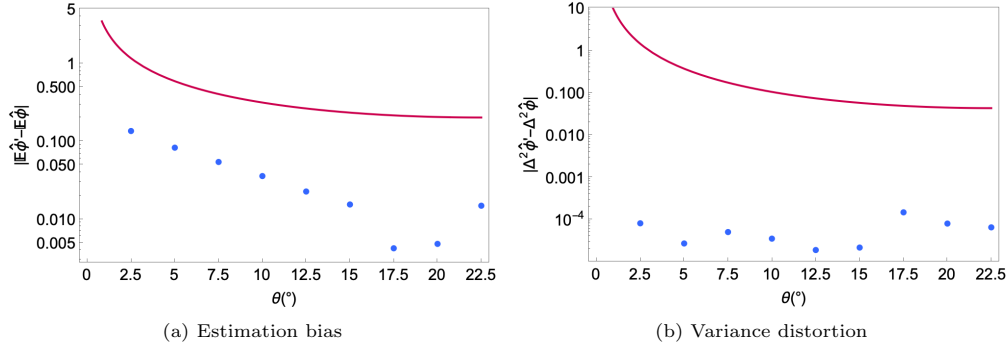


Figure 3.8: Analysis of the estimation precision. In both the plots, blue points represent experimental data, whereas solid red lines correspond to the bounds (3.20) on the discrepancies between the tampered estimation and the ideal one. All the quantities here assessed are based on the experimental fidelity and the available events. Picture taken from [8].

from the fact that theoretical bounds 3.20 are upper bounded by the trace distance between the tampered and the ideal state; while they must be estimated via the fidelity. Consequently, more refined bound accounting for the actual observable under measurement have to be addressed. On the other hand, it may also occur that, without more specific information on the transmitted probe state, a quantification of the metrological performances built on cryptographic parameters only (e.g., faithfulness) is intrinsically limited.

3.4.3 Two-way protocol

An other DQS scenario is presented in Fig. 3.9.

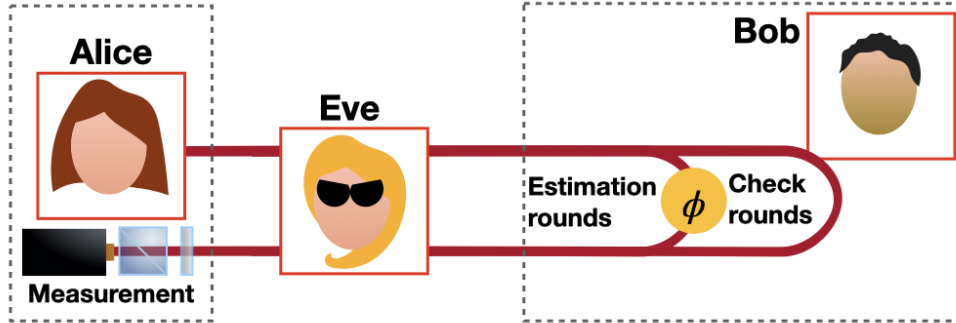


Figure 3.9: Conceptual sketch of the two-way DQS protocols described in this section. Alice supplies Bob with quantum probes in order to estimate a phase ϕ in a distributed/delegated setting. Transmission occurs on a quantum channel potentially controlled by an eavesdropper, who can: i) tamper with the probe state so as to compromise the estimation, ii) leak information in order to retrieve a phase estimation herself. Unlike the one-way scenario presented in section 3.4.1, here Bob has no measurement capabilities: he acts thus just as an encoder, with the quantum probe traveling back to Alice, who performs the estimation.

Here, Bob's quantum capabilities are even more limited than in the one-way protocol discussed in section 3.4.1, being now only able to encode the parameter. Alice is therefore in charge of both the preparation of the probe state, as well as its measurement. The quantum state travels through the channel twice, with the malicious user possibly acting on it on both the forth and the back round. For this reason, the protocol discussed here below is referred to as **two-way DQS protocol**.

The protocol is built upon minor adaptations of the one-way entanglement-based and MUB-based protocols discussed in section 3.4.1, dictated by the more passive role Bob plays in this instance.

The additional back round from Bob to Alice does not spoil the faithfulness of the

scheme; the security is, however, no longer guaranteed. The main issue lies in the intrinsic difficulty for Alice of evaluating the amount of information potentially leaked by Eve relying exclusively on the received probes.

The two-way protocol mimics either the entanglement-based 3.4.1 or the MUB-based 3.4.1 one-way protocol, with, however, different bounds for the bias and variance distortion. More specifically, the bounds holding for the two-way, entanglement-based protocol are, respectively,

$$\begin{aligned} \left| \mathbb{E}\hat{\phi} - \mathbb{E}\hat{\phi}' \right| &\leq \frac{\varepsilon_{2w}}{\nu |\sin(2\nu\phi)|} \\ \left| \Delta^2 \hat{\phi} - \Delta^2 \hat{\phi}' \right| &\leq \frac{2\varepsilon_{2w} + \varepsilon_{2w}^2}{|\nu \sin(2\nu\phi)|^2}, \end{aligned} \quad (3.24)$$

with $\varepsilon_{2w} = \sqrt{\frac{2}{3}\varepsilon^2 + 4f(T, N_d, \nu) + |\sin(\min\{\nu\phi, \pi/2\})|}$. Likewise the one-way protocols, bounds (3.24) hold for the MUB-based formulation by replacing $\varepsilon^2 \rightarrow \frac{2}{3}\varepsilon^2$. The main difference between the bounds (3.24) and (3.20), valid in, respectively, the two-way and one-way scenario lies in the term $|\sin(\min\{\nu\phi, \pi/2\})|$, gauging the capability of Eve of discriminating the presence/absence of the encoded phase ϕ with the highest probability quantum mechanics would allow.

A detailed proof of the faithfulness of the two-way DQS protocol is presented in [8].

In conclusion, in a two-way setting, faithfulness is preserved via proper adaptations of the bounds holding in the one-way setting (3.20). In contrast, due to Alice's inability to estimate Eve's intervention by relying solely on the received qubits, security can no be longer guaranteed; reflecting an intrinsic asymmetry in the information available to the legitimate users. Nonetheless, the back round emerges as the critical step enabling more effective eavesdropping strategies as captured by the additional term $|\sin(\min\{\nu\phi, \pi/2\})|$ in the security threshold, quantifying Eve's optimal capability to discriminate the presence of the encoded parameter.

Overall, the two-way secure sensing protocol here discussed provides a general benchmark to understand the limits of passive-user architectures, supporting the need for additional assumptions or modified protocols so that security can be restored.

Chapter 4

Sloppy behavior in quantum systems

Despite being a well established field, with already existing commercial applications, quantum metrology still offers avenues for fundamental research and investigation. In particular, many open question, both theoretical and experimental, still need to be addressed in the multi-parameter setting, where the saturation of the ultimate precision limits is not guaranteed [16, 17, 24, 25]. In this framework, complex systems have attracted, and are still attracting, much interest from the metrological community, due to the intrinsic difficulty of characterizing their behavior. More in detail, their description commonly requires an increasingly large amount of parameters as the complexity of the system grows. Typically, only few combinations of parameters suffice to describe its evolution, with other combinations providing little to no relevant information.

Such a phenomenon, frequently encountered in biological systems, is known under the name of **sloppiness**, and is described in section 4.1. Nonetheless, sloppiness happens to show up in quantum system as well, with a very representative case being quantum interferometry, discussed in section 4.2.

The possible reduction of complexity due to stiff combinations of parameters has its counterpart in terms of informational quantity, allowing an experimentalist to have access only to partial information about the system. A possible way to explore, and tackle sloppiness involves a controlled evolution of the system under study, implemented by means of a weak quantum measurement scheme. The new estimation protocol is thoroughly discussed in section 4.2.1. Furthermore, an experimental test has been carried on, with experimental details delivered in section 4.2.2 and results presented in section 4.2.3. These latter three sections are based on the work published in [9]. The method, together with the experimental demonstration performed, open up new perspective on the implementation of techniques based on weak measurements, aiming at proficiently extracting information from the system under study. In parallel to its relevance for metrological applications, the technique discussed in this chapter can be used as well as a fundamental block to control the dynamics and the evolution of a generic quantum system, possibly detecting interactions with other systems or potentially malicious users.

4.1 Stiff vs sloppy parameter combinations

A thorough comprehension of the dynamics of complex systems, ranging from biological systems to economics to climate, commonly relies on a model capable of describing such systems. Further predictive power can be earned via a comparison between experimental observations and theoretical predictions, allowing the experimenter to infer the relevant parameter for the evolution dynamics.

As a downside, more refined models often require an increasing number of parameters describing the system; mirrored by the more complex metrological scenario, generally preventing all the parameter from being simultaneously estimated with maximum precision (as already discussed in Chapter 1, section 1.2.6). Interestingly, some complex systems exhibit a peculiar behavior, with only specific combinations of few parameters actually governing the evolution dynamics of the system. Complex systems described

by such models are said to exhibit a **sloppy** behavior, and are matter of interest in several research fields, from fundamental metrology [121,122], to biology [123,124]. The combinations of parameters ruling the evolution of a sloppy model are known as **stiff** combinations (term borrowed from biological complex systems) carry substantial information about system itself; correspondingly, they can be estimated with relatively small uncertainty.

However, such stiff combination coexist with other, **sloppy** combinations of parameters, not directly involved in the evolution dynamics but, conversely, fundamental for a full characterization. Under a metrological perspective, sloppy combinations bear no information regardless the applied measurement strategy, yielding to loose precision bounds on their estimation.

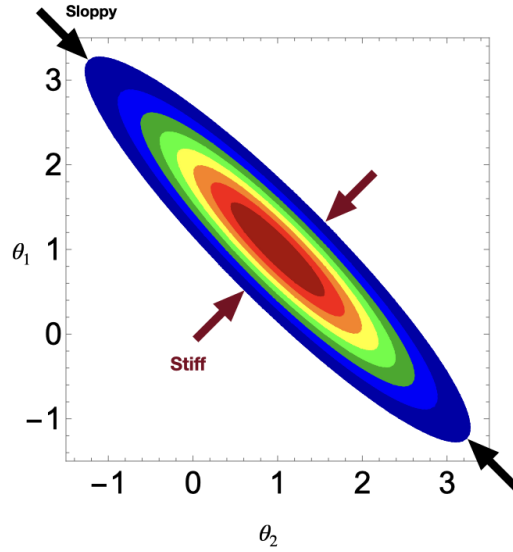


Figure 4.1: Pictorial idea of stiff and sloppy parameter combinations. A controlled evolution of the system enables the estimation of θ_1 and θ_2 , with the joint uncertainty qualitatively depicted as an ellipse, with its semi-axes corresponding to the, respectively, sloppy and stiff combinations $\theta_1 + \theta_2$ and $\theta_1 - \theta_2$. Picture adapted from [9].

A pictorial idea of stiff and sloppy combinations of parameters is presented in Fig. 4.1. The existence of stiff parameters marks the robustness of the system to external perturbation, identifying the fundamental quantities shaping the observed dynamics. This latter feature plays a crucial role in systems described by a massive amount of parameters: here, an experimenter can focus on the estimation of such parameters with maximum precision. Remarkably, the presence of unknown sloppy parameters yields to a global loss of precision. To counter such an inconvenience, it is possible to insert a controlled perturbation of the system, so as to guide its evolution under specific conditions set by the experimenter, increasing the amount of available information and, therefore, tackling sloppiness. Nonetheless, it might be desirable to marginally perturb the system, in order to investigate the sloppy systems keeping its dynamics as close as possible to the unperturbed condition. A commonplace solution for both these issues is presented in Fig. 4.2, consisting in an ancillary measurement in between the two encodings.

4.1.1 Sloppiness in quantum systems

Together with classical complex systems, sloppiness has been proved to arise in quantum systems as well [124–129], the main reason being some asymmetry in the information associated with stiff and sloppy combinations, together with the interplay of quantum observables' incompatibility used in parameter estimation protocols.

Remarkably, the toolbox of controlled perturbations to monitor a systems requires overcoming the standard prepare-evolve-measure scheme of quantum metrology [24,25,130]: evolution step is usually considered inaccessible by external users, while now an exter-

nal perturbation is necessary to tackle and monitor sloppy behavior. Techniques and strategies to do so can be classified in two main categories:

- the first option, such the one proposed by Y. Yang *et al* in [127], similarly to open-loop schemes (terms borrowed from control theory), deals with the introduction of a unitary operation during the course of the evolution. As highlighted in [127], the goal is unraveling the parameters encoded via the very same generator. On the same page, Frigerio's and Paris' work [128] stated that scramble strategies may as well be employed, with no significant impact on the precision scaling.
- the second possibility, built on close-loop schemes, involves coupling of the system under study with an ancillary one. A downside of such an approach consists in keeping the interaction times sufficiently short compared to other timescales during the evolution, granting, thus, only limited action range. Other physical constraints on the interaction and the minimization of perturbations to the natural model may limit even further the amount of information extracted from measurements.

4.2 Sloppy phase estimation in quantum interferometry

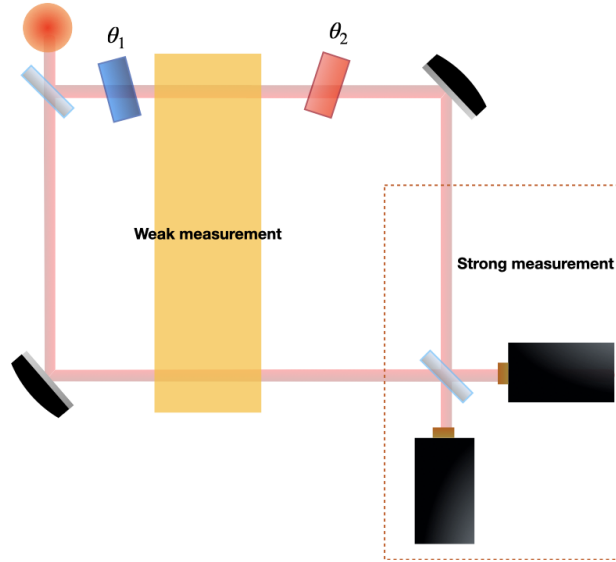


Figure 4.2: Sloppy two-phase estimation in a linear interferometer. propagating through the setup acquires two phases θ_1 and θ_2 by means of two subsequent objects. A weak measurement is placed in between the two encodings, in order to disambiguate between the two phases and counter the arising sloppiness. Picture adapted from [9].

As already anticipated in section 4.1.1, sloppiness can arise in quantum systems as well: a simple, yet insightful example, consists of two subsequent parameter encodings via unitary maps generated by the same observable $\hat{U}(\theta_j) = e^{-i\hat{G}\theta_j}$, $j = 1, 2$: it is easy to prove that the resulting state depends exclusively on the sum $\theta_1 + \theta_2$

$$\hat{U}(\theta_1)\hat{U}(\theta_2)|\psi\rangle = e^{-i\hat{G}\theta_1}e^{-i\hat{G}\theta_2}|\psi\rangle = e^{-i\hat{G}(\theta_1+\theta_2)}|\psi\rangle, \quad (4.1)$$

with no dependence on the difference $\theta_1 - \theta_2$, preventing, thus, full information on θ_1 and θ_2 from being gathered.

Such an idea can be tested via photon interference in a linear interferometer, such as the one presented in Fig. 4.2. Assuming to have interferometric phases generated by Pauli-Y gate, and the two arms of a Mach-Zehnder interferometer (MZI) corresponding to two orthogonal polarizations of a single spatial mode. A photon horizontally polarized

$|H\rangle$ entering the interferometer will experience two subsequent phase shifts, given by $\hat{U}(\phi_1)$ and $\hat{U}(\phi_2)$. The resulting state will be then of the form

$$|\psi\rangle = \hat{U}(\phi_1)\hat{U}(\phi_2)|H\rangle = \cos(\phi_1 + \phi_2)|H\rangle + \sin(\phi_1 + \phi_2)|V\rangle. \quad (4.2)$$

Any measurement of the qubit state (4.2) yields to the following probabilities:

$$\begin{aligned} P_0(\phi_1, \phi_2) &= |\langle 0|\psi\rangle|^2 = \cos^2(\phi_1 + \phi_2), \\ P_1(\phi_1, \phi_2) &= |\langle 1|\psi\rangle|^2 = \sin^2(\phi_1 + \phi_2), \end{aligned} \quad (4.3)$$

where $|0\rangle, |1\rangle$ form the orthonormal polarization basis in which the qubit state is expressed (e.g. the Pauli-Z diagonal basis for the qubit state (4.2)).

The Fisher Information matrix associated with such a measurement scheme will be

$$F(\phi_1, \phi_2) = 4 \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad (4.4)$$

constant everywhere, regardless the values of the phases ϕ_1 and ϕ_2 , as well as that of their combination. The determinant of the Fisher Information matrix (4.4) is $\det(F) = 4(1-1) = 0$, yielding to a fully singular inverse matrix, thus to a no lower bound on the estimation uncertainty on the phases ϕ_1 and ϕ_2 . To summarize, in the unperturbed scenario, as a result of the two parameters being generated by the same observable, the effect of the single phases cannot be isolated. Sloppiness therefore is a result of classical statistics, rather than rooting its origin in purely quantum phenomena, such as non-commutativity.

4.2.1 Sloppy phase estimation with a tunable weak-measurement

In order to tackle sloppiness arising in two-phase estimation, here is reported a protocol, fully described in [9], involving a weak measurement [131] in between the two phase encodings coupling the metrological probe with an auxiliary qubit acting as a meter.

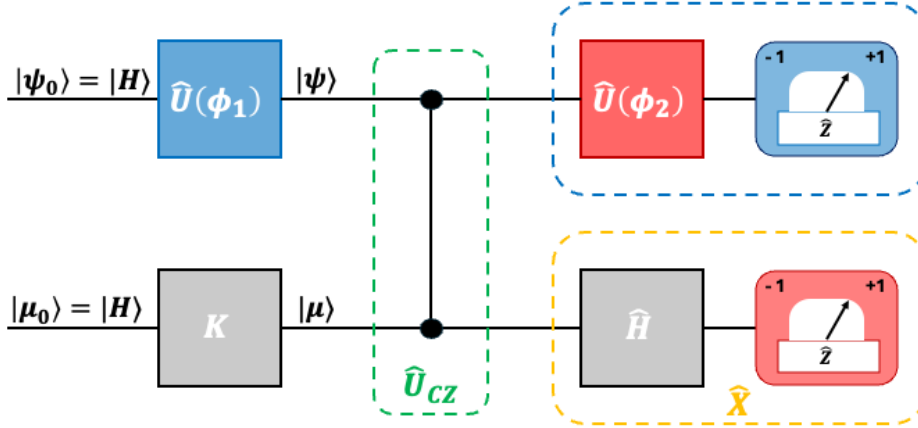


Figure 4.3: Conceptual sketch of a sloppy two-phase estimation assisted by a tunable weak measurement: a metrological probe, with the first phase encoded, is coupled to a meter qubit via a C-Z operation. The strength of the coupling is tuned by suitably preparing the meter state. The second phase on the system qubit is directly encoded in the measurement stage. A post-selection according to the measurement outcome of the auxiliary qubit implements a suitable weak measurement of the state of the system qubit, able to counter sloppiness present in the model.

Remarkably, weak measurement can be used to tackle sloppiness only provided that sensitivity to coherence between the two interferometric modes is preserved: the coupling interaction must then be associated with an incompatible observable with respect

to the phase generator.

An example of such an approach is sketched in Fig. 4.3: here a phase-encoded qubit is coupled to a suitably prepared meter state, tuning the strength of the interaction, via a C-Z gate. By post-selecting on the outcomes of a measurement of the meter qubit, an indirect measurement of the system qubit is carried out, allowing to retrieve information about its quantum state.

Referring to Fig. 4.3, the quantum state of the system and the meter qubit before the coupling are, respectively:

$$\begin{aligned} |\psi\rangle &= \cos(\phi_1) |H\rangle + \sin(\phi_1) |V\rangle \\ |\mu\rangle &= \kappa |+\rangle + \sqrt{1-\kappa^2} |-\rangle = \frac{\kappa + \sqrt{1-\kappa^2}}{\sqrt{2}} |H\rangle + \frac{\kappa - \sqrt{1-\kappa^2}}{\sqrt{2}} |V\rangle, \end{aligned} \quad (4.5)$$

where $|H/V\rangle$ refer to the horizontal/vertical polarization states, whereas $|\pm\rangle$ to the eigenstates of Pauli-X matrix, i.e., diagonal polarization states.

The system-meter state after the coupling via the C-Z gate is

$$|\psi'\rangle = \cos(\phi_1) |H\rangle \left(\kappa |+\rangle + \sqrt{1-\kappa^2} |-\rangle \right) + \sin(\phi_1) |V\rangle \left(\kappa |-\rangle + \sqrt{1-\kappa^2} |+\rangle \right). \quad (4.6)$$

By looking at Eq. (4.6), it is clear that for $\kappa = 1$ the classical action of a C-Z gate (see Eq. (1.19)) is retrieved, corresponding, therefore, to a fully projective measurement.

Conversely, as soon as $\kappa = 1/\sqrt{2}$, the state (4.6) reduces to

$$(\cos(\phi_1) |H\rangle + \sin(\phi_1) |V\rangle) \left(\frac{|+\rangle + |-\rangle}{\sqrt{2}} \right) = |\psi\rangle |H\rangle,$$

equivalent to not coupling the system and the meter qubits. The interaction range is therefore fully spanned by the $\frac{1}{\sqrt{2}} \leq \kappa \leq 1$ interval. A **strength parameter** K is then defined as:

$$K = 2\kappa^2 - 1 \quad (4.7)$$

ranging in the interval $[0, 1]$ for the corresponding $\kappa \in [\frac{1}{\sqrt{2}}, 1]$.

The second phase shift ϕ_2 is then applied via the unitary encoding $\hat{U}(\phi_2)$ on the system qubit. In the end, system and meter qubits are measured in the, respectively, Pauli-Z and Pauli-X diagonal bases.

The probabilities for all the measurement outcomes combinations are then

$$\begin{aligned} P_{H+}(\phi_1, \phi_2) &= \frac{1 + K \cos(2\phi_1) + (K + \cos(2\phi_1)) \cos(2\phi_2) - \sqrt{1-K^2} \sin(2\phi_1) \sin(2\phi_2)}{4}; \\ P_{H-}(\phi_1, \phi_2) &= \frac{((\sqrt{1-K} - \sqrt{1+K}) \cos(\phi_1 - \phi_2) + (\sqrt{1-K} + \sqrt{1+K}) \cos(\phi_1 + \phi_2))^2}{8}; \\ P_{V\pm}(\phi_1, \phi_2) &= \frac{((\sqrt{1-K} - \sqrt{1+K}) \sin(\phi_1 - \phi_2) \pm (\sqrt{1-K} + \sqrt{1+K}) \sin(\phi_1 + \phi_2))^2}{8}, \end{aligned} \quad (4.8)$$

each calculated via the Born's rule $P_{j\pm} = |\langle j | \langle \pm | \hat{U}(\phi_2) \otimes \mathbb{1} | \psi' \rangle|^2$ $j = H, V$; yielding to the following Fisher Information matrix

$$F(K) = 4 \begin{pmatrix} \frac{1}{\sqrt{1-K^2}} & \sqrt{1-K^2} \\ \sqrt{1-K^2} & 1 \end{pmatrix}. \quad (4.9)$$

Matrix (4.9) can now be inverted, giving rise to the following QCRB on the phase estimators:

$$F^{-1}(K) = \frac{1}{4K^2} \begin{pmatrix} \frac{1}{-\sqrt{1-K^2}} & -\sqrt{1-K^2} \\ -\sqrt{1-K^2} & 1 \end{pmatrix} \longrightarrow \Delta^2 \phi \geq \frac{1}{4NK^2} \quad (4.10)$$

for both ϕ_1 and ϕ_2 , where N identifies the number of probes involved in the estimation. The natural modes of the model are retrieved by the eigenvalues of the CFI matrix

(4.9), being, respectively:

$$\begin{aligned} F_+ &= 4 \left(1 + \sqrt{1 - K^2} \right) \rightarrow \phi_1 + \phi_2 \text{ is the stiff combination;} \\ F_- &= 4 \left(1 - \sqrt{1 - K^2} \right) \rightarrow \phi_1 - \phi_2 \text{ is the sloppy combination.} \end{aligned} \quad (4.11)$$

The amount of sloppiness is quantified by $\det(F) = F_+ F_- = 16K^2$, as stated in [122]. Differently from Eq. (4.4), the new Fisher Information matrix (4.9) is singular only for $K = 0$, providing a meaningful CRB for any other interaction strength K .

The ultimate precision limit (4.10) highlights how the coupling of the system qubit with an ancillary one, and the possibility of tuning the strength of such an interaction is capable of breaking the sloppiness experienced under free evolution. More in detail:

- At $K = 1$, i.e., for **full-strength measurements**, the phase estimators experience the minimum uncertainty $\Delta_{\min}^2 \phi = \frac{1}{4N}$, as if ϕ_1 and ϕ_2 were estimated in separate experiments;
- At $K = 0$, i.e., whenever no interaction occurs between the system and the meter, the original situation, described by the fully singular CFI matrix (4.4), is recovered. Phase estimation carries therefore no information.

Nonetheless, the measurement strength K affects the phase-phase correlations as well via the lower bound $\Sigma_{\phi_1, \phi_2} \geq \frac{\sqrt{1-K^2}}{4N}$.

Notably, whenever a target phase variance $\Delta^2 \bar{\phi}$ is sought, the weak measurement scheme 4.3 with at the given strength K requires at least $O(K^{-2})$ additional resources compared to the standard, projective case.

It is important to stress that the measurement strength K sets both the amount of information on the first phase ϕ_1 extracted from the first measurement, as well as the amount of coherence available for the final, projective measurement, similarly to what commonly happens for multiparameter metrological protocols involving system-ancilla entanglement [132–135], with the main difference being a joint measurement possibly required by the latter schemes.

4.2.2 Experimental protocol

The weak-measurement approach proposed in section 4.2.1 has been tested via our optical platform with polarization-encoded qubits.

Single photons generated via the SPDC source depicted in Fig. 2.8, pumped by a CW laser with nominal power $P_{\text{pump}} = 50 \text{ mW}$ are delivered to the manipulation and detection stage presented in Fig. 4.4, similar to the one presented in section 2.4.1. Target phases are set via the rotation of the HWPs by an angle $\theta_j = \phi_j/2$ $j = 1, 2$. Like what has been presented in Chapters 2 and 3, all the results will be presented in terms of the tuning angle of the HWP: the CFIM (4.9) is thus rescaled by a factor 4. Similarly, the strength parameter K is tuned by setting the polarization of the meter photon via a HWP, so the quantum state of the meter can be expressed as

$$|\mu\rangle = \cos(2\varphi) |H\rangle + \sin(2\varphi) |V\rangle. \quad (4.12)$$

By comparing the expressions (4.12) and (4.5) the following relations between interaction strength and corresponding tuning angle are retrieved:

$$\varphi(K) = \frac{1}{2} \arctan \left(\frac{1 - \sqrt{1 - K^2}}{K} \right) \quad (4.13)$$

The probe and the meter photon are then coupled via the C-Z gate discussed in section 2.4.1. The entangling gate relies on the PPBS, featuring the transmittivities $T_H = 1$ and $T_V = 1/3$ [15, 136, 137]. Consequently, the tuning angles of the HWPs for both the system and the meter qubit need a rescale factor, in order to account for the polarization-dependent losses introduced by the PPBS [101], mapping Eq. (4.13) into

$$\varphi(K) = \frac{1}{2} \arctan \left(\sqrt{3} \frac{1 - \sqrt{1 - K^2}}{K} \right). \quad (4.14)$$

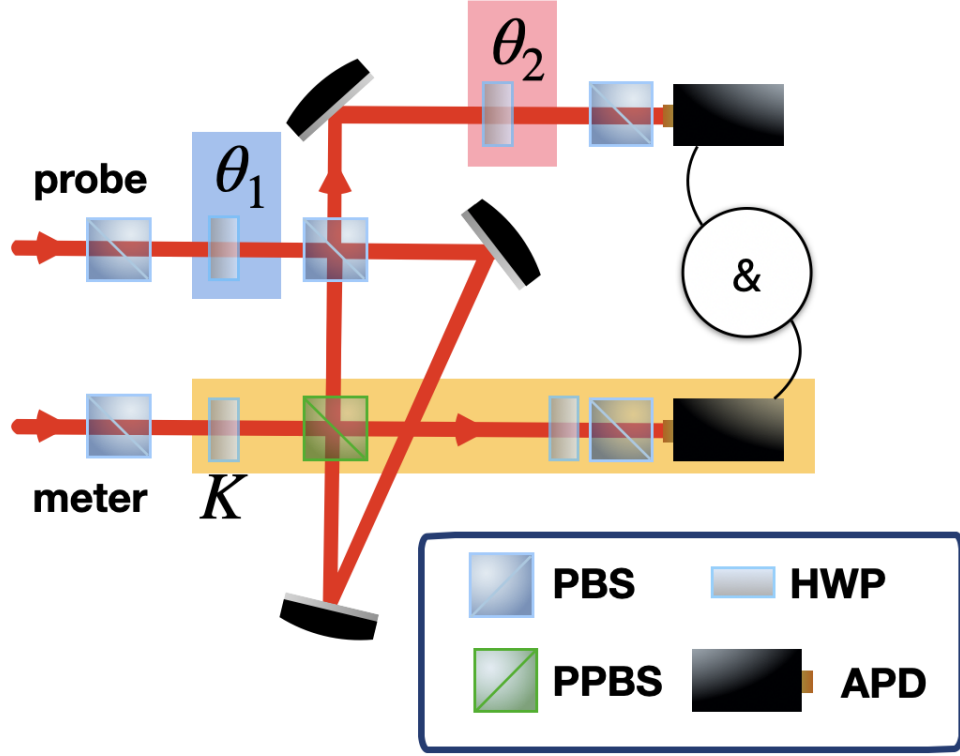


Figure 4.4: Experimental setup for sloppy phase estimation. Photons with central wavelength $\lambda_0 = 810\text{nm}$ arising from SPDC, one acting as the system qubit and the other behaving as a meter, are sent onto a C-Z gate embedded in a Sagnac loop. Polarization states, as well as the measurement strength, are properly set via HWPs, while the measurement stations consist of a standard HWP-PBS-APD sequence. Picture taken from [9].

After interacting in the C-Z gate, the two photon proceed to the measurement stations: likewise the metrology-assisted certification of quantum steering experiment, discussed in Chapter 2, the second target phase is encoded directly while measuring the system qubit, by properly rotating the HWP in the measurement stage.

4.2.3 Results

The first part of the estimation process concerns the calibration of the experimental setup: this has been done by collecting, at high statistics, i.e. with acquisition window $\Delta t = 5\text{s}$, coincidence counts at different settings of (θ_1, θ_2) , spanning the range $[0^\circ, 22.5^\circ]$, respectively, in the range with uneven spacing for θ_1 , and in steps of 2.5° for θ_2 . The output of the calibration process is an estimation of the probabilities $P(x_w, x_s | \theta_1, \theta_2)$ of all the possible measurement outcomes combinations. Calibration data are then interpolated through third-order polynomials, enabling to retrieve the probabilities for arbitrary values of (θ_1, θ_2) .

The second step is the properly said- estimation experiment: here data corresponding to settings (θ_1, θ_2) not included in the calibration set have been collected.

Experimental data are now collected with a smaller sample size than in the calibration part (acquisition window is now set at $\Delta t = 0.1\text{s}$ for each outcome combination), aiming at limiting the impact of the precision on the reference [138].

Experimental coincidence counts n_{ij} , with $i = H, V$ and $j = +, -$, have been used to retrieve a logarithmic maximum likelihood estimator of the form

$$(\bar{\theta}_1, \bar{\theta}_2) = \arg \max_{\theta_1, \theta_2} \sum_{i,j} n_{i,j} \log (P(i, j | \theta_1, \theta_2)), \quad (4.15)$$

with optimization run via numerical methods.

Similarly to the experiment discussed in Chapter 2, the covariance matrix, for each

phase setting, is retrieved via a Monte Carlo method by bootstrapping over the observed statistics, based on a Poissonian law with Poisson parameter equal to the experimentally observed coincidence counts. The estimation experiment has been performed

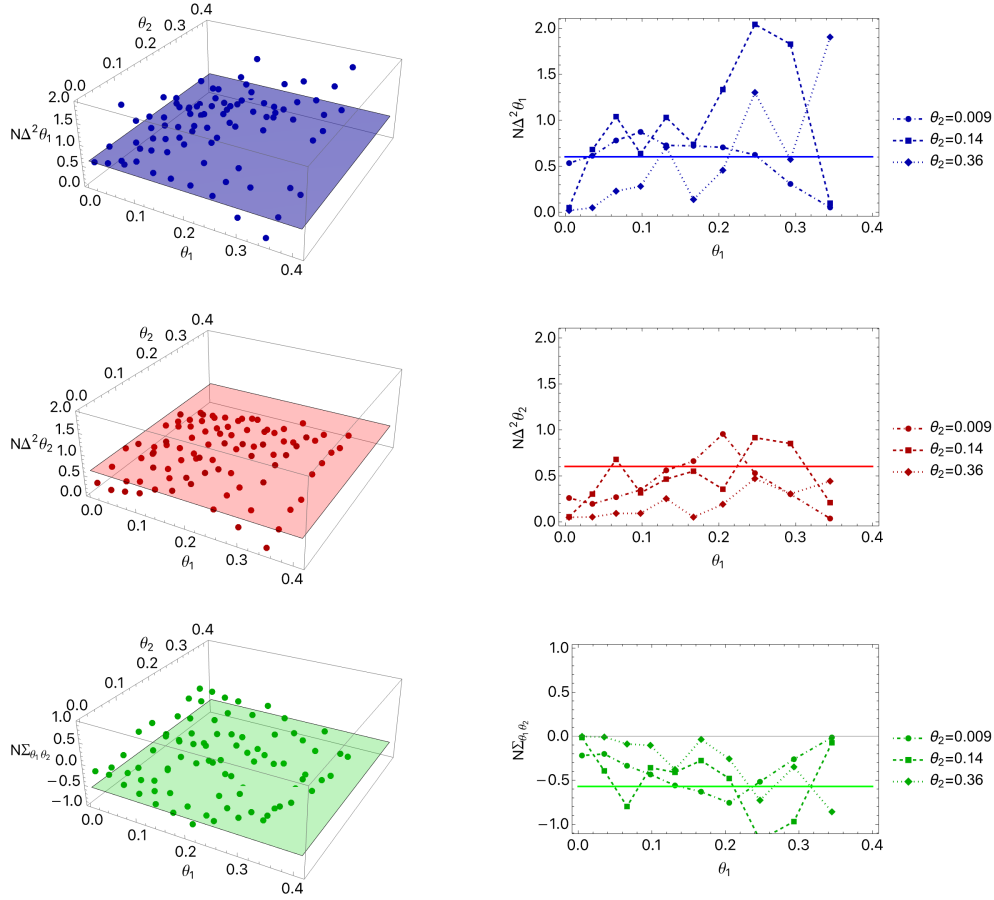


Figure 4.5: Elements of the covariance matrix Σ for the two estimated tuning angles θ_1 and θ_2 for the weak-coupling regime $K = 0.322$. From top to bottom, the panels show, respectively, the total variance of phase θ_1 , the total variance of phase θ_2 , and their covariance. Here three-dimensional plots are presented, along with slices at given values of θ_2 . In every plot, data points correspond to the experimentally retrieved variances, while the solid curves refer to the theoretical predictions provided by the Cramér-Rao bound. Picture adapted from [9].

for three different strength levels, ranging from a weak coupling regime, at $K = 0.322$, an intermediate-strength run, with $K = 0.785$, to an almost projective measurement, with interaction strength $K = 0.934$. Metrological performances in these three scenarios are presented in, respectively, Figs. 4.5 to 4.7.

Under the weak measurement strength condition, as shown in Fig. 4.5, significant deviations from the expected behavior at the ultimate precision bound (i.e. the Cramér-Rao bound) arise. Such discrepancies can be ascribed to experimental limitations, mainly to imperfect quantum interference between the system and the meter photons. Consequently, measurements yield to a retrieval of the values for θ_1 and θ_2 according to the likelihood function (see Eq. (4.15)). However, even under perfect conditions, the so retrieved estimates bear little significance, due to the weak interaction of the system and the meter qubits. Practically, experimental imperfections may impart additional features, comparable with the ones determined by the likelihood function, preventing the optimization scheme from converging to meaningful values. This is further supported by the instances in which the variance lies below the CRB, clearly marking the presence of bias in the estimation.

The aforementioned effect becomes progressively less relevant as the strength of the first measurement increases, as highlighted by the experimental runs at $K = 0.789$ and $K = 0.934$.

Interestingly, experimental imperfections limit the performance enhancement for stronger

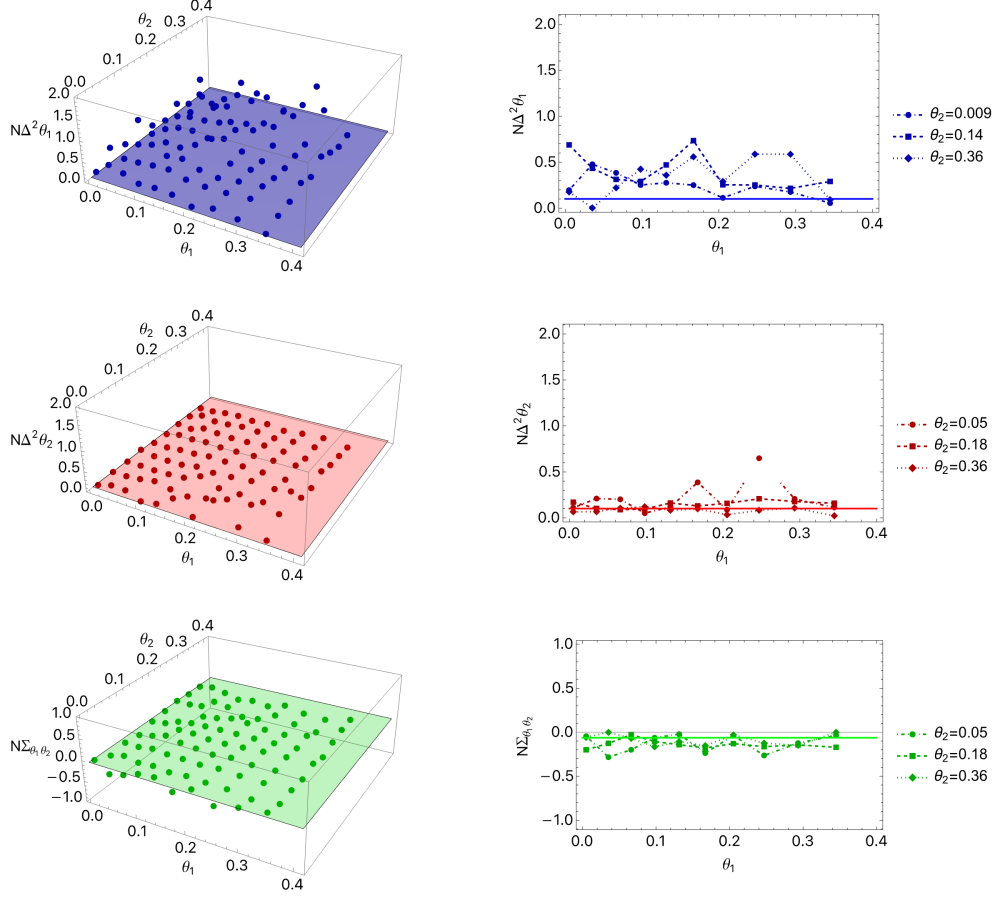


Figure 4.6: Elements of the covariance matrix Σ for the two estimated tuning angles θ_1 and θ_2 for the weak-coupling regime $K = 0.789$. From top to bottom, the panels show, respectively, the total variance of phase θ_1 , the total variance of phase θ_2 , and their covariance. Here three-dimensional plots are presented, along with slices at given values of θ_2 . In every plot, data points correspond to the experimentally retrieved variances, while the solid curves refer to the theoretical predictions provided by the Cramér-Rao bound. Picture adapted from [9].

system-meter interaction, making the value $K = 0.934$ close enough to the maximum strength achievable in practice. Noteworthy, $K = 1$ corresponds to the limit of maximal and perfect entanglement between the two involved photons.

The experiment here discussed suggests that the $O(K^{-2})$ scaling of the variance with the strength of the first measurement, as stated in Eq. (4.10), should be interpreted as an optimistic dependence, since experimental imperfections appear to exert a more deleterious action for weaker system-meter interactions, partially counterable by means of a larger data sample (it is known that larger statistics is not necessarily a remedy for biased estimation). Furthermore, the expected symmetry between the two phases (see Eq. (4.10)) is not matched in the experimental test, with the first phase featuring a larger (quadratic) error. Hence, the loss of information, due to experimental limitations, is more impactful for the first parameter, directly accessed by the non-projective measurement.

In conclusion, the weak measurement-based protocol discussed in section 4.2.2 and its experimental implementation, delivered in this section, shows how a tunable interaction between a quantum system with an ancilla allows to counter the sloppiness arising from two subsequent parameter encodings, at the price of retrieving a progressively less reliable information as the interaction strength diminishes. The method here proposed can be further extended to more complex scenarios, such as sequence of multiple phases encoded in a two-arm interferometer, rather than phase pairs in multimode interferometers. Remarkably, the ground idea of modifying the natural evolution in a controlled fashion may still hold, but the optimal arrangement might be setup-dependent.

The results here presented shed a new light of the interplay between sloppiness and

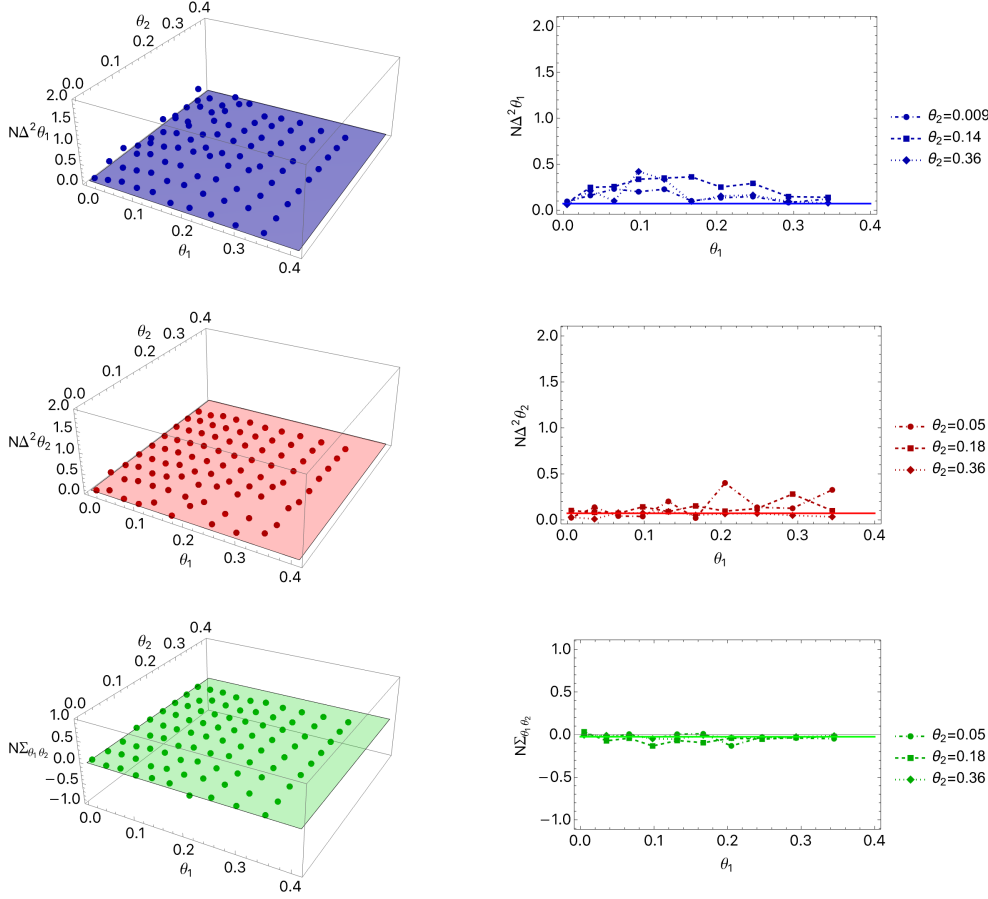


Figure 4.7: Elements of the covariance matrix Σ for the two estimated tuning angles θ_1 and θ_2 for the weak-coupling regime $K = 0.934$. From top to bottom, the panels show, respectively, the total variance of phase θ_1 , the total variance of phase θ_2 , and their covariance. Here three-dimensional plots are presented, along with slices at given values of θ_2 . In every plot, data points correspond to the experimentally retrieved variances, while the solid curves refer to the theoretical predictions provided by the Cramér-Rao bound. Picture adapted from [9].

measurement-back-action, assessing how a distinctive quantum trait, i.e. weak measurements, can help tackling complex, multi-parameter estimation tasks, deploying invaluable tools in quantum metrology contexts, promising applications in quantum security and quantum monitoring as well.

Conclusions

Like the first quantum revolution, which solved problems left unsolved by classical physics, and led to a mastodontic technological revolution represented by the rise of computer science, the second quantum revolution promises to be a cornerstone shaping the present and the future. The possibility of exploiting quantum mechanics at a single-system level enables to develop technologies outclassing the performances achieved by the most powerful classical devices. More in detail, quantum computing and quantum simulations aim at running algorithms and simulating system hardly doable, if not impossible, on classical hardware. The goal of quantum communication is, instead, the exploitation of quantum features to establish communication links among distant parties with unprecedented security with respect to hacking attacks. Last, but not least, quantum metrology and sensing ground on quantum mechanics to develop estimation protocols achieving precisions far beyond the most promising classical scenarios, with applications ranging from gravimetry to quantum enhanced medical imaging.

Just to mention a few milestones achieved in the last decade, quantum mechanics proved to be pivotal in the discovery of gravitational waves [6], further confirming the theory of General Relativity proposed by Einstein. In 2017 a group of Chinese scientists was able to perform entanglement distribution over more than 1000 km via satellite-based quantum communication [3]. Under the computing/simulation spotlight, in 2022 it was proved that a photonic simulator succeeded to perform random sampling from a probability distribution in a time window completely outclassing the most powerful classical supercomputer [4].

All of the applications mentioned above rely on optical platforms for their implementation: the nowadays broad expertise on the generation, manipulation and distribution of quantum light makes photonics a valid and solid testbed for all the quantum technologies. Nonetheless, two recent Nobel prizes, the one awarded in 2022 to A. Aspect, J. Clauser and A. Zeilinger for the experimental violation of the Bell inequality, and in 2023 to M. Bawendi, L.E. Brus and A. Ekimov for the synthesis of quantum dots, further confirm the key role quantum optics in the second quantum revolution.

Furthermore, in recent years new scientific disciplines emerged, born from the transfer of methods and knowledge from one field to another one, among others, artificial intelligence, econophysics and chemoinformatics. On the same page, the study of the interplay among the main pillars of the quantum technologies offers open challenges for impactful scientific and technological progress, but has been very little investigated so far.

In this thesis work, indeed, it was explored the role of quantum metrology as a unifying conceptual and practical framework to address problems ranging from the very foundations of quantum mechanics to quantum communication and security, moving metrology beyond its conventional purview. Rather, it has been employed as a general and versatile toolbox to reformulate and analyze issues of broad relevance within quantum information science.

After a preliminar introduction to quantum information and quantum measurement theory, Chapter 1 stressed on the fundamental concept that the estimation process -unavoidably constrained by quantum physics- can be exploited not only to design optimal measurement protocol, achieving the ultimate precision limits, but also to identify the manifestation of genuine quantum features, assess trust in adversarial communication and sensing scenarios, and gain insight into the structure of (possibly complex) quantum systems.

In Chapter 2 a metrology-assisted technique for the certification of quantum steering was presented, addressing, thus, the fundamental problem of the validation of genuine quantum correlations. Rather than relying on the retrieval of a witness, and the violation of a suitably defined inequality holding for unsteerable states, the approach

here proposed casts the certification of such a correlation as a parameter-estimation problem. More thoroughly, the significance of the estimation error is linked to the insuitability of a LHS model describing the experimental outcomes. By adopting a multiparameter metrological framework to account for nuisance intrinsically affecting the probe state, and the Van Trees bound in place of the standard CRB, we were able to rule out a LHS description of our assemblage with a very limited amount of physical resources. Our work paves then the way for the implementation of such an approach on practical quantum networks, where only a small amount of resources is addressed to the securization of each node, with the majority of them being exploited for the task the network was built for. Furthermore, the possibility of formulating metrology-assisted criteria to validate quantum entanglement and Bell nonlocality would define an alternative paradigm for the securization of quantum links in a quantum network, relying on the very same setup for both the characterization and the operational task. Chapter 3 aims at merging together theoretical concepts of quantum cryptography with metrological and informational quantities, in the context of secure phase estimation (to some extent, it can be considered as the dual problem to Chapter 2: with the former aiming at certifying a quantum link via quantum parameter estimation, while the latter assessing the degree of trust of a parameter estimation over an unsecured quantum channel). Here a single-way and a two-way protocol have been proposed and analyzed, in the realistic setting of quantum states shared across untrusted quantum channels possibly accessed by a malicious user. The presented security proofs, based on those discussed in [111, 116], ensure the faithfulness of the estimation process, highlighting how metrological bounds can be used to detect and estimate the amount of tampering introduced by an end adversary having potentially full quantum capabilities. Our work then sets a general framework for practical distributed quantum sensing, with both its strengths and current limitations, leading the way for more refined protocols and security proofs in the future. Crucially, upper bounds on the information leaked by Eve still need a formalization, particularly in delegated quantum sensing scenarios.

Finally, Chapter 4 goes back on a more fundamental aspect of quantum metrology, focusing on the investigation of sloppiness in multiparameter quantum estimation. More thoroughly, sloppy behavior has been reproduced in a controlled interferometric setup. Notably, the introduction of a tunable weak measurement in the midst of two subsequent parameter estimations proved to be able to counter such an issue, allowing the user to retrieve metrological information otherwise inaccessible. Beyond its contribution to fundamental metrology, where the investigation of sloppy models, particularly in quantum systems, is only partially explored, our results foster promising applications, once again, outside the context of pure science of measurements: remarkably, the possibility to span the interaction of the system under exam with an ancillary pointer from a buffer situation to a full-strength coupling suggests the adoption of this approach to dynamically control the evolution of quantum systems and, potentially, to identify anomalous or malicious behavior in systems expected to exhibit sloppy dynamics (suggesting, once again, the applicability of methods proper of quantum metrology to quantum security).

Overall, the works presented in this thesis support the idea of using techniques and methods of quantum metrology as a general language to (re-)interpret problems belonging to different domains of quantum technologies. However, several open questions, both theoretical and experimental, still need to be faced to fruitfully bring together the pillars of the second quantum revolution. Particularly, a deep comprehension of the current limitations of these fields, and possible solutions to tackle them, is vital to design ad-hoc strategies to bring quantum metrology, quantum communication, quantum computing and quantum simulation close to each other, reinforcing their bond with the foundations of quantum theory.

Ultimately, this thesis proposes quantum metrology not merely as a toolbox of (precision) limits, rather as a toolbox of possibilities; a framework through which the purest nature of information can be probed, certified and secured at the most fundamental level.

Bibliography

- [1] S. Wehner, D. Elkouss, and R. Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412):eaam9288, 2018.
- [2] European Commission. Quantum technology flagship, 2025.
- [3] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, et al. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.
- [4] L.S. Madsen, F. Laudenbach, M.F. Askarani, F. Rortais, T. Vincent, J.F.F. Bulmer, F.M. Miatto, L. Neuhaus, L.G. Helt, M.J. Collins, et al. Quantum computational advantage with a programmable photonic processor. *Nature*, 606(7912):75–81, 2022.
- [5] L. Pezzè and A. Smerzi. Heisenberg-limited noisy atomic clock using a hybrid coherent and squeezed state protocol. *Physical Review Letters*, 125(21):210503, 2020.
- [6] B.P. Abbott, R. Abbott, T.D. Abbott, M.R. Abernathy, F. Acernese, K. Ackley, C. Adams, T. Adams, P. Addesso, R.X. Adhikari, et al. Observation of gravitational waves from a binary black hole merger. *Physical Review Letters*, 116(6):061102, 2016.
- [7] G. Bizzarri, I. Gianani, M. Manrique, V. Berardi, F. Bruni, G. Capellini, and M. Barbieri. Quantum steering from phase measurements with limited resources. *AVS Quantum Science*, 6(2):024405, 05 2024.
- [8] G. Bizzarri, M. Barbieri, M. Manrique, M. Parisi, F. Bruni, I. Gianani, and R. Rosati. Faithful and secure distributed quantum sensing under general-coherent attacks. *npj Quantum Information*, 2026.
- [9] G. Bizzarri, M. Parisi, M. Manrique, I. Gianani, A. Chiuri, M. Rosati, V. Giovannetti, M. G. A. Paris, and M. Barbieri. Controlling sloppiness in two-phase estimation with a tunable weak measurement. *Optica Quantum*, 3(5):432–438, Oct 2025.
- [10] R. Loudon. *The quantum theory of light*. OUP Oxford, 2000.
- [11] G. Benenti, G. Casati, and G. Strini. *1: Basic concepts / Giuliano Benenti and Giulio Casati, Giuliano Strini*. World Scientific, New Jersey [etc, c2004.
- [12] M.A. Nielsen and I.L. Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.
- [13] G. Benenti, G. Casati, and G. Strini. *Principles of Quantum Computation and Information-Volume II: Basic Tools and Special Topics*. World Scientific Publishing Company, 2007.
- [14] A.S. Holevo. *Probabilistic and statistical aspects of quantum theory*, volume 1. Springer Science & Business Media, 2011.
- [15] G. Bizzarri, S. Gherardini, M. Manrique, F. Bruni, I. Gianani, and M. Barbieri. Quasiprobability distributions with weak measurements. *Quantum Science and Technology*, 10(4):045008, aug 2025.

- [16] E. Polino, M. Valeri, N. Spagnolo, and F. Sciarrino. Photonic quantum metrology. *AVS Quantum Science*, 2(2), 2020.
- [17] M. Barbieri. Optical quantum metrology. *PRX Quantum*, 3(1):010202, 2022.
- [18] M.G.A. Paris, G.M. D’Ariano, and M.F. Sacchi. Maximum-likelihood method in quantum estimation. *arXiv preprint quant-ph/0101071*, 2001.
- [19] Y. Li, L. Pezzè, M. Gessner, Z. Ren, W. Li, and A. Smerzi. Frequentist and bayesian quantum phase estimation. *Entropy*, 20(9):628, 2018.
- [20] Z. Hradil, R. Myška, J. Peřina, M. Zawisky, Y. Hasegawa, and H. Rauch. Quantum phase in interferometry. *Physical Review Letters*, 76(23):4295, 1996.
- [21] R.A. Fisher. On the mathematical foundations of theoretical statistics. *Philosophical transactions of the Royal Society of London. Series A, containing papers of a mathematical or physical character*, 222(594-604):309–368, 1922.
- [22] H. Cramér. *Mathematical methods of statistics*, volume 9. Princeton university press, 1999.
- [23] C.R. Rao et al. Information and the accuracy attainable in the estimation of statistical parameters. *Bull. Calcutta Math. Soc.*, 37(3):81–91, 1945.
- [24] G. Giovannetti, S. Lloyd, and L. Maccone. Quantum metrology. *Physical review letters*, 96(1):010401, 2006.
- [25] V. Giovannetti, S. Lloyd, and L. Maccone. Advances in quantum metrology. *Nature photonics*, 5(4):222–229, 2011.
- [26] S.L. Braunstein and C.M. Caves. Statistical distance and the geometry of quantum states. *Physical Review Letters*, 72(22):3439, 1994.
- [27] C.W. Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1(2):231–252, 1969.
- [28] W. Górecki and R. Demkowicz-Dobrzański. Multiple-phase quantum interferometry: Real and apparent gains of measuring all the phases simultaneously. *Physical Review Letters*, 128(4):040504, 2022.
- [29] J. Liu, H. Yuan, X.-M. Lu, and X. Wang. Quantum fisher information matrix and multiparameter estimation. *Journal of Physics A: Mathematical and Theoretical*, 53(2):023001, 2020.
- [30] M. Szczykulska, T. Baumgratz, and A. Datta. Multi-parameter quantum metrology. *Advances in Physics: X*, 1(4):621–639, 2016.
- [31] C.W. Helstrom and R.S. Kennedy. Noncommuting observables in quantum detection and estimation theory. *IEEE Transactions on Information Theory*, 20(1):16–24, 2003.
- [32] H.P. Yuen and M. Lax. Multiple-parameter quantum estimation and measurement of nonselfadjoint observables. *IEEE Transactions on Information Theory*, 19(6):740–750, 2003.
- [33] P.C. Humphreys, M. Barbieri, A. Datta, and I.A. Walmsley. Quantum enhanced multiple phase estimation. *arXiv preprint arXiv:1307.7653*, 2013.
- [34] W. Górecki and R. Demkowicz-Dobrzański. Multiparameter quantum metrology in the heisenberg limit regime: Many-repetition scenario versus full optimization. *Physical Review A*, 106(1):012424, 2022.
- [35] J.C. Maxwell. Viii. a dynamical theory of the electromagnetic field. *Philosophical transactions of the Royal Society of London*, (155):459–512, 1865.
- [36] E. Hecht. *Optics*. Pearson, 2012.
- [37] G.R. Fowles. *Introduction to modern optics*. Courier Corporation, 2012.

- [38] P.A.M. Dirac. The quantum theory of the emission and absorption of radiation. *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character*, 114(767):243–265, 1927.
- [39] L. Susskind and J. Glogower. Quantum mechanical phase and time operator. *Physica Physique Fizika*, 1(1):49, 1964.
- [40] D.T. Pegg and S.M. Barnett. Unitary phase operator in quantum mechanics. *EPL (Europhysics Letters)*, 6(6):483, 1988.
- [41] C.-K. Hong, Z.-Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Physical Review Letters*, 59(18):2044, 1987.
- [42] Gabriele Bizzarri. Experimental multiparameter quantum metrology, 2020/2021.
- [43] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660):575–579, 1997.
- [44] K. Tsujino, H.F. Hofmann, S. Takeuchi, and K. Sasaki. Distinguishing genuine entangled two-photon-polarization states from independently generated pairs of entangled photons. *Physical Review Letters*, 92(15):153602, 2004.
- [45] N. Killoran, M. Cramer, and M.B. Plenio. Extracting entanglement from identical particles. *Physical Review Letters*, 112(15):150501, 2014.
- [46] R. Lo Franco and G. Compagno. Indistinguishability of elementary systems as a resource for quantum information processing. *Physical Review Letters*, 120(24):240403, 2018.
- [47] A. Castellini, R. Lo Franco, L. Lami, A. Winter, G. Adesso, and G. Compagno. Indistinguishability-enabled coherence for quantum metrology. *Physical Review A*, 100(1):012308, 2019.
- [48] B. Morris, B. Yadin, M. Fadel, T. Zibold, P. Treutlein, and G. Adesso. Entanglement between identical particles is a useful and consistent resource. *Physical Review X*, 10(4):041012, 2020.
- [49] F. Schlue, T. Nomura, P. Held, F. Pegoraro, M. Stefszky, B. Brecht, S.M. Barnett, and C. Silberhorn. How to entangle or disentangle gaussian states with hong-ou-mandel interference. *arXiv preprint arXiv:2502.06570*, 2025.
- [50] L. Pezzé and A. Smerzi. Phase sensitivity of a mach-zehnder interferometer. *Physical Review A*, 73(1):011801, 2006.
- [51] L. Pezzé, A. Smerzi, G. Khoury, J.F. Hodelin, and D. Bouwmeester. Phase detection at the quantum limit with multiphoton mach-zehnder interferometry. *Physical Review Letters*, 99(22):223602, 2007.
- [52] L. Pezzé and A. Smerzi. Mach-zehnder interferometry at the heisenberg limit with coherent and squeezed-vacuum light. *Physical Review Letters*, 100(7):073601, 2008.
- [53] H. Lee, P. Kok, and J.P. Dowling. A quantum rosetta stone for interferometry. *Journal of Modern Optics*, 49(14-15):2325–2338, 2002.
- [54] J.D. Jackson. *Classical electrodynamics*. John Wiley & Sons, 2021.
- [55] R.W. Boyd, A.L. Gaeta, and E. Giese. Nonlinear optics. In *Springer Handbook of Atomic, Molecular, and Optical Physics*, pages 1097–1110. Springer, 2008.
- [56] Valeria Cimini. *New Methods of Data Analysis for Quantum Metrology*. PhD thesis, University of Roma Tre, 2020/2021.
- [57] Mauro Valeri. Sorgenti di coppie di fotoni entangled alla lunghezza d’onda telecom, 2016/2017.
- [58] W.H. Louisell, A. Yariv, and A.E. Siegman. Quantum fluctuations and noise in parametric processes. i. *Physical Review*, 124(6):1646, 1961.

- [59] D.C. Burnham and D.L. Weinberg. Observation of simultaneity in parametric production of optical photon pairs. *Physical Review Letters*, 25(2):84, 1970.
- [60] B. Yadin, M. Fadel, and M. Gessner. Metrological complementarity reveals the einstein-podolsky-rosen paradox. *Nature communications*, 12(1):2410, 2021.
- [61] G. Bizzarri, I. Gianani, M. Manrique, V. Berardi, F. Bruni, G. Capellini, and M. Barbieri. Finite-size effects in metrology-assisted certification of quantum steering. In Keith S. Deacon and Ronald E. Meyers, editors, *Quantum Communications and Quantum Imaging XXII*, volume 13148, page 131480E. International Society for Optics and Photonics, SPIE, 2024.
- [62] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.
- [63] N. Bohr. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 48(8):696, 1935.
- [64] D. Bohm and Y. Aharonov. Discussion of experimental proof for the paradox of einstein, rosen, and podolsky. *Physical Review*, 108(4):1070, 1957.
- [65] E. Schrödinger. Discussion of probability relations between separated systems. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 31, pages 555–563. Cambridge University Press, 1935.
- [66] E. Schrödinger. Probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 32(3):446–452, 1936.
- [67] R.F. Werner. Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model. *Physical Review A*, 40(8):4277, 1989.
- [68] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Reviews of modern physics*, 81(2):865–942, 2009.
- [69] E. Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31(4):555–563, 1935.
- [70] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of n-particle mixed states: necessary and sufficient conditions in terms of linear maps. *Physics Letters A*, 283(1-2):1–7, 2001.
- [71] A. Peres. Collective tests for quantum nonlocality. *Physical Review A*, 54(4):2685, 1996.
- [72] O. Gühne and G. Tóth. Entanglement detection. *Physics Reports*, 474(1-6):1–75, 2009.
- [73] M. Barbieri, F. De Martini, G. Di Nep, P. Mataloni, G.M. D’Ariano, and C. Macchiavello. Detection of entanglement with polarized photons: Experimental realization of an entanglement witness. *Physical review letters*, 91(22):227901, 2003.
- [74] B.M. Terhal. Bell inequalities and the separability criterion. *Physics Letters A*, 271(5-6):319–326, 2000.
- [75] G. Tóth, W. Wieczorek, R. Krischek, N. Kiesel, P. Michelberger, and H. Weinfurter. Practical methods for witnessing genuine multi-qubit entanglement in the vicinity of symmetric states. *New Journal of Physics*, 11(8):083002, 2009.
- [76] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical review letters*, 70(13):1895, 1993.
- [77] A.K. Ekert. Quantum cryptography based on bell’s theorem. *Physical review letters*, 67(6):661, 1991.
- [78] C.H. Bennett and S.J. Wiesner. Communication via one-and two-particle operators on einstein-podolsky-rosen states. *Physical review letters*, 69(20):2881, 1992.

- [79] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.
- [80] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.
- [81] D. Coppersmith. An approximate fourier transform useful in quantum factoring. *arXiv preprint quant-ph/0201067*, 2002.
- [82] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, 439(1907):553–558, 1992.
- [83] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 454(1969):339–354, 1998.
- [84] L.K. Grover. A fast quantum mechanical algorithm for database search. *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.
- [85] J.S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.
- [86] D. Bohm. A suggested interpretation of the quantum theory in terms of” hidden” variables. i. *Physical review*, 85(2):166, 1952.
- [87] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. *Reviews of modern physics*, 86(2):419–478, 2014.
- [88] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt. Proposed experiment to test local hidden-variable theories. *Physical review letters*, 23(15):880, 1969.
- [89] A. Aspect, P. Grangier, and G. Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: a new violation of bell’s inequalities. *Physical review letters*, 49(2):91, 1982.
- [90] H. M. Wiseman, S. J. Jones, and A. C. Doherty. Steering, entanglement, nonlocality, and the einstein-podolsky-rosen paradox. *Physical review letters*, 98:140402, Apr 2007.
- [91] R. Uola, A.C.S. Costa, H.C. Nguyen, and O. Gühne. Quantum steering. *Reviews of Modern Physics*, 92(1):015001, 2020.
- [92] H.M. Wiseman, S.J. Jones, and A.C. Doherty. Steering, entanglement, nonlocality, and the einstein-podolsky-rosen paradox. *Physical review letters*, 98(14):140402, 2007.
- [93] S.J. Jones, H.M. Wiseman, and A.C. Doherty. Entanglement, einstein-podolsky-rosen correlations, bell nonlocality, and steering. *Physical Review A*, 76(5):052116, 2007.
- [94] E.G. Cavalcanti, S.J. Jones, H.M. Wiseman, and M.D. Reid. Experimental criteria for steering and the einstein-podolsky-rosen paradox. *Physical Review A*, 80(3):032112, 2009.
- [95] M.D. Reid. Demonstration of the einstein-podolsky-rosen paradox using nondegenerate parametric amplification. *Physical Review A*, 40(2):913, 1989.
- [96] M.D. Reid, P.D. Drummond, W.P. Bowen, E.G. Cavalcanti, P.K. Lam, H.A. Bachor, U.L. Andersen, and G. Leuchs. Colloquium: the einstein-podolsky-rosen paradox: from concepts to applications. *Reviews of Modern Physics*, 81(4):1727–1751, 2009.
- [97] E.G. Cavalcanti and M.D. Reid. Uncertainty relations for the realization of macroscopic quantum superpositions and epr paradoxes. *Journal of Modern Optics*, 54(16-17):2373–2380, 2007.

- [98] H.L. Van Trees. *Detection, estimation, and modulation theory, part I: detection, estimation, and linear modulation theory*. John Wiley & Sons, 2004.
- [99] R.D. Gill and B.Y. Levit. Applications of the van trees inequality: a bayesian cramér-rao bound. 1995.
- [100] V. Cimini, S. Gherardini, M. Barbieri, I. Gianani, M. Sbroscia, L. Buffoni, M. Paternostro, and F. Caruso. Experimental characterization of the energetics of quantum logic gates. *npj Quantum Information*, 6(1):96, 2020.
- [101] R. Okamoto, H.F. Hofmann, S. Takeuchi, and K. Sasaki. Demonstration of an optical quantum controlled-not gate without path interference. *Physical review letters*, 95(21):210506, 2005.
- [102] K.V. Mardia and P.E. Jupp. *Directional statistics*. John Wiley & Sons, 2009.
- [103] N.I. Fisher. *Statistical analysis of circular data*. cambridge university press, 1995.
- [104] I. Gianani, M.G. Genoni, and M. Barbieri. Assessing data postprocessing for quantum estimation. *IEEE Journal of Selected Topics in Quantum Electronics*, 26(3):1–7, 2020.
- [105] Q. Zhuang, Z. Zhang, and J.H. Shapiro. Distributed quantum sensing using continuous-variable multipartite entanglement. *Physical Review A*, 97(3):032329, 2018.
- [106] Z. Zhang and Q. Zhuang. Distributed quantum sensing. *Quantum Science and Technology*, 6(4):043001, 2021.
- [107] X. Guo, C.R. Breum, J. Borregaard, S. Izumi, M.V. Larsen, T. Gehring, M. Christandl, J. S. Neergaard-Nielsen, and U.L. Andersen. Distributed quantum sensing in a continuous-variable entangled network. *Nature Physics*, 16(3):281–284, 2020.
- [108] B.K. Malia, Y. Wu, J. Martínez-Rincón, and M.A. Kasevich. Distributed quantum sensing with mode-entangled spin-squeezed atomic states. *Nature*, 612(7941):661–665, 2022.
- [109] Y. Takeuchi, Y. Matsuzaki, K. Miyanishi, T. Sugiyama, and W.J. Munro. Quantum remote sensing with asymmetric information gain. *Physical Review A*, 99(2):022325, 2019.
- [110] P. Yin, Y. Takeuchi, W.-H. Zhang, Z.-Q. Yin, Y. Matsuzaki, X.-X. Peng, X.-Y. Xu, J.-S. Xu, J.-S. Tang, Z.-Q. Zhou, et al. Experimental demonstration of secure quantum remote sensing. *Physical Review Applied*, 14(1):014065, 2020.
- [111] N. Shettell, E. Kashefi, and D. Markham. Cryptographic approach to quantum metrology. *Physical Review A*, 105(1):L010401, 2022.
- [112] N. Jain, H.-M. Chin, H. Mani, C. Lupo, D.S. Nikolic, A. Kordts, S. Pirandola, T.B. Pedersen, M. Kolb, B. Ömer, et al. Practical continuous-variable quantum key distribution with composable security. *Nature communications*, 13(1):4740, 2022.
- [113] A.A.E. Hajomer, I. Derkach, V.C. Usenko, U.L. Andersen, and T. Gehring. Co-existence of continuous-variable quantum key distribution and classical data over 120 km fiber. *Physical Review Letters*, 135:170804, Oct 2025.
- [114] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, 560:7–11, 2014.
- [115] Z. Huang, C. Macchiavello, and L. Maccone. Cryptographic quantum metrology. *Physical Review A*, 99(2):022314, 2019.
- [116] S.W. Moore and J.A. Dunningham. Secure quantum remote sensing without entanglement. *AVS Quantum Science*, 5(1):014406, 02 2023.
- [117] S. Pirandola, U.L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, et al. Advances in quantum cryptography. *Advances in optics and photonics*, 12(4):1012–1236, 2020.

- [118] W. He, C. Huang, R. Guan, Y. Chen, X. Zhang, and K. Wei. Experimental secure entanglement-free quantum remote sensing over 50 km of optical fiber. *Physical Review A*, 111(6):062607, 2025.
- [119] K. Li and G. Smith. Quantum de finetti theorem under fully-one-way adaptive measurements. *Physical review letters*, 114(16):160503, 2015.
- [120] F.G.S.L. Brandao and A.W. Harrow. Quantum de finetti theorems under local measurements with applications. In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*, pages 861–870, 2013.
- [121] K.S. Brown, C.C. Hill, G.A. Calero, C.R. Myers, K.H. Lee, J.P. Sethna, and R.A. Cerione. The statistical mechanics of complex signaling networks: nerve growth factor signaling. *Physical Biology*, 1(3):184, oct 2004.
- [122] K.S. Brown and J.P. Sethna. Statistical mechanical approaches to models with many poorly known parameters. *Phys. Rev. E*, 68:021904, Aug 2003.
- [123] J.J. Waterfall, F.P. Casey, R.N. Gutenkunst, K.S. Brown, C.R. Myers, P.W. Brouwer, V. Elser, and J.P. Sethna. Sloppy-model universality class and the vandermonde matrix. *Physical Review Letters*, 97(15):150601, 2006.
- [124] B.B. Machta, R. Chachra, M.K. Transtrum, and J.P. Sethna. Parameter space compression underlies emergent theories and predictive models. *Science*, 342(6158):604–607, 2013.
- [125] L.J. Fiderer, T. Tufarelli, S. Piano, and G. Adesso. General expressions for the quantum fisher information matrix with applications to discrete quantum imaging. *PRX Quantum*, 2(2):020308, 2021.
- [126] A.Z. Goldberg, J.L. Romero, A.S. Sanz, and L.L. Sánchez-Soto. Taming singularities of the quantum fisher information. *International Journal of Quantum Information*, 19(08):2140004, 2021.
- [127] Y. Yang, F. Belliardo, V. Giovannetti, and F. Li. Untwining multiple parameters at the exclusive zero-coincidence points with quantum control. *New Journal of Physics*, 24(12):123041, 2023.
- [128] M. Frigerio and M.G.A. Paris. Overcoming sloppiness for enhanced metrology in continuous-variable quantum statistical models. *arXiv preprint arXiv:2410.02989*, 2024.
- [129] J. Wang and G.S. Agarwal. Exact quantum fisher matrix results for distributed phases using multiphoton polarization greenberger-horne-zeilinger states. *Physical Review A*, 111(1):012414, 2025.
- [130] M.G.A. Paris. Quantum estimation for quantum technology. *International Journal of Quantum Information*, 7(supp01):125–137, 2009.
- [131] J. Dressel, M. Malik, F.M. Miatto, A.N. Jordan, and R.W. Boyd. Colloquium: Understanding quantum weak values: Basics and applications. *Reviews of Modern Physics*, 86(1):307–316, 2014.
- [132] M. Sbroscia, I. Gianani, L. Mancino, E. Roccia, Z. Huang, L. Maccone, C. Macchiavello, and M. Barbieri. Experimental ancilla-assisted phase estimation in a noisy channel. *Physical Review A*, 97(3):032305, 2018.
- [133] K. Wang, X. Wang, X. Zhan, Z. Bian, J. Li, B.C. Sanders, and P. Xue. Entanglement-enhanced quantum metrology in a noisy environment. *Physical Review A*, 97(4):042112, 2018.
- [134] Z. Hou, Y. Jin, H. Chen, J.-F. Tang, C.-J. Huang, H. Yuan, G.-Y. Xiang, C.-F. Li, and G.-C. Guo. “super-heisenberg” and heisenberg scalings achieved simultaneously in the estimation of a rotating field. *Physical Review Letters*, 126(7):070503, 2021.

- [135] Z. Hou, J.-F. Tang, H. Chen, H. Yuan, G.-Y. Xiang, C.-F. Li, and G.-C. Guo. Zero-trade-off multiparameter quantum estimation via simultaneously saturating multiple heisenberg uncertainty relations. *Science Advances*, 7(1):eabd2986, 2021.
- [136] G.J. Pryde, J.L. O’Brien, A.G. White, S.D. Bartlett, and T.C. Ralph. Measuring a photonic qubit without destroying it. *Physical Review Letters*, 92(19):190402, 2004.
- [137] J. Ho, J.W. Webb, R.M.J. Brooks, F. Grasselli, E. Gauger, and A. Fedrizzi. Quantum-private distributed sensing. *arXiv preprint arXiv:2410.00970*, 2024.
- [138] V. Cimini, I. Gianani, N. Spagnolo, F. Leccese, F. Sciarrino, and M. Barbieri. Calibration of quantum sensors by neural networks. *Physical Review Letters*, 123(23):230502, 2019.

Appendix 1: Quasiprobability distributions with weak measurements

Quasiprobability distributions with weak measurements

G. Bizzarri,^{1,*} S. Gherardini,^{2,3,*} M. Manrique,¹ F. Bruni,¹ I. Gianani,¹ and M. Barbieri^{1,2}

¹*Dipartimento di Scienze, Università degli Studi Roma Tre, Via della Vasca Navale, 84, 00146 Rome, Italy*

²*Istituto Nazionale di Ottica - CNR, Largo E. Fermi 6, 50125 Florence, Italy*

³*European Laboratory for Non-linear Spectroscopy,
Università degli Studi di Firenze, 50019 Sesto Fiorentino, Italy.*

We discuss and experimentally demonstrate the role of quantum coherence in a sequence of two measurements collected at different times using weak measurements. For this purpose, we have realized a weak-sequential measurement protocol with photonic qubits, where the first measurement is carried out as a positive operator-valued measure, whereas the second one is a projective operation. We determine the quasiprobability distributions associated to this procedure using both the commensurate and the Margenau-Hill quasiprobabilities approaches. By tuning the weak measurements, we obtain a quasidistribution that may or may not exhibit negative parts, depending on the suitability of a contextual model for describing the experiment. Our results show how quasidistributions may find application in inspecting quantum monitoring, when part of the initial quantum coherence needs to be preserved.

INTRODUCTION

The standard description of a quantum state adopts a wave-function or a density matrix [1]. Although their ontological status is disputed [2–6], they offer the most complete physical insight quantum mechanics is able to provide in its standard form. By means of Born’s rule one can derive proper probability distributions associated with the measurement at single times of any physical observable [7]. To attain such a task, projective measurements suffice.

In the case of multiple observables, noncommutativity prevents from obtaining an analogue joint distribution built on projective measurements. A solution was proposed by Wigner, leading to his celebrated function [8]. A so-called quasiprobability distribution is obtained for which negative values can arise, thus representing a signature of genuine quantumness for the state. It has also been linked to the possibility of associating a local hidden-variable model, depending on the specific physical context, with the quantum state [9–13], as well as to inefficient simulation by classical computers [14–17].

These results have inspired the search for protocols to describe the statistics of outcome pairs returned from measuring noncommuting observables at multiple times [18–22]. In the case of two sequential measurements, often called two-point measurement (TPM) scheme in quantum thermodynamics [23, 24], commensurate quasiprobabilities (CQs) have been defined to capture the contextuality of the measurements’ action via the presence of negative values [25, 26]. Negativity of CQs arises from the state-collapse induced by the first measurement of the sequence, causing a modification of the coherence properties of the initial state that conversely are erased by the TPM scheme.

As proved in [27], going beyond the TPM scheme entails that a unique description of the outcome statistics at distinct times is no longer valid, as long as the observ-

ables do not commute. In this regard, descriptions using quasiprobabilities, alternative to CQs, have been adopted to fully account for the incompatibility between measurement observables and the initial state [28–33]. A case in point is the Kirkwood-Dirac quasiprobability [27, 34–36], and its real part known as the Margenau-Hill quasiprobability (MHQ) [37].

In all these approaches, measurements are typically taken as projective operations in Von Neumann’s terms [38], but they result in a collapse of the system’s wave-function, hence in the disruption of the corresponding quantum state. On the other hand, weak measurements are a viable option to carry out *sequential measurements* [39]. These can be interpreted as coarse-grained measurements [40], in that their outcomes cannot unambiguously distinguish between orthogonal states of the system. Despite this, averaging over many instances still yields the correct expectation value [41–44]. The resulting loss of information can be related to the violation of macrorealism in Leggett-Garg inequalities [45–47], and, based on anomalous values arising in post-selection, to a witness of contextuality [48–52]. Although the original definitions of quasidistributions [25] are suited to generalized measurement, virtually all investigations have only considered projective measurements, making the physical picture of quasiprobabilities based on weak measurements almost unexplored. Further, while the use of generalized measurements has received some attention [36], weak measurements deserve a special place since they preserve an intuitive physical meaning and are characterized by a parameter tuning over different regimes.

In this article, we describe theoretically weak variants of CQs and MHQs, in discrete quantum systems with arbitrary, finite dimension. Further, we obtain them in an experiment on weak measurements of qubits coded in the polarisation of single photons, retrieved from the direct implementation of the *weak-sequential measurement scheme*, shown in Fig. 2a. In such a scheme the

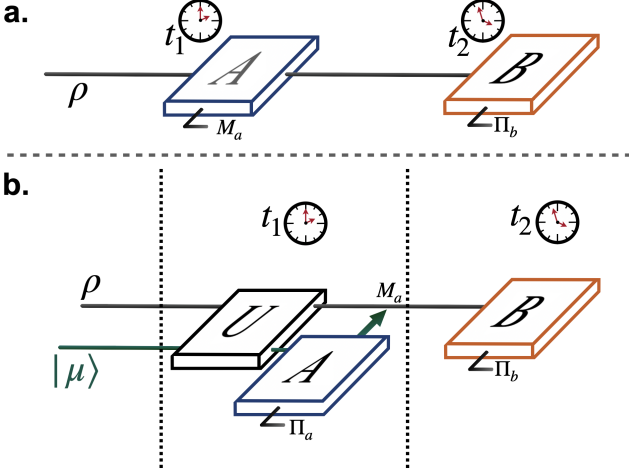


FIG. 1. Weak-sequential measurements on a quantum system initialized in a generic density operator ρ . a) Pictorial representation of the two-time measurement scheme where the first measurement associated to the observable A is carried out by a POVM with elements M_a , and the second is a standard strong measurement of B by means of projectors Π_b . b) Conceptual approach to the implementation of the weak-sequential measurement scheme. The unitary operator U couples the system, initially in the state ρ (black line), with a pointer in the state $|\mu\rangle$ (green line). Following this operation, a strong projective measurement of A on the pointer can yield information about the system, depending on the initial preparation $|\mu\rangle$. The system thus is still available for further measurements at later times.

first standard strong measurement is replaced by a positive operator-valued measure (POVM), expressed as a function of a parameter tuning from strong to a weak regime. The weak-CQ and weak-MHQ distributions so introduced set a natural way to draw the line between the incompatibility of measurement observables, and measurement coarse-graining. The marginals of weak-CQ and weak-MHQ distributions retain their physical meaning, also encompassing features and limitations of the weak measurement scheme. These concepts are demonstrated in an experiment using the weak measurement of photonic qubits.

BACKGROUND

We consider a generic density operator ρ describing a quantum state, undergoing the process in Fig. 1a. At the time t_1 the value a of the observable $A = \sum_a a \Pi_a^A$ is recorded, thus collapsing the wave-function onto the corresponding eigenvector. At a later time, $t_2 > t_1$ a measurement of $B = \sum_b b \Pi_b^B$ (with $[A, B] \neq 0$) yields the value b . It can also encompass in-between quantum dynamics by replacing Π_b^B with the corresponding time-evolved operator in the Heisenberg picture, e.g., $\hat{\Pi}_b^B = e^{iH(t_2-t_1)/\hbar} \Pi_b^B e^{-iH(t_2-t_1)/\hbar}$ for unitary dynamics

governed by a Hamiltonian H [35]. As a result, the joint probability of recording these two measurement outcomes is

$$p(a, b) \equiv \text{Tr} [\Pi_b^B \Pi_a^A \rho \Pi_a^A], \quad (1)$$

which is returned by the TPM scheme [23].

The joint probabilities $p(a, b)$ form a valid distribution that is nevertheless insensitive to initial coherences in the eigenstates of A due to the invasivity of the first measurement. Consequently, the marginal $\sum_a p(a, b)$ is generally different from $p_{\text{fin}}(b) = \text{Tr} [\Pi_b^B \rho]$, i.e., the probability of obtaining the value b for the observable B directly on the initial state ρ . The definition of the CQ, originally introduced in [25, 26, 38], makes use of the unmeasured state's statistics, in order to account for the disturbance caused by the measurement of A :

$$q_C(a, b) \equiv p(a, b) + \frac{1}{d} (p_{\text{fin}}(b) - p_{\text{post}}(b)), \quad (2)$$

where $p_{\text{post}}(b) \equiv \sum_a p(a, b) = \sum_a \text{Tr} [\Pi_b^B \Pi_a^A \rho \Pi_a^A] = \sum_a p_{\text{in}}(a) \text{Tr} [\Pi_b^B \Pi_a^A]$ is the marginal distribution of the TPM joint probability over a , with $p_{\text{in}}(a) = \text{Tr} [\Pi_a^A \rho]$ and d denoting the dimension of the system. In Eq. (2), the term in the parenthesis quantifies how much $p_{\text{post}}(b)$ differs from $p_{\text{fin}}(b)$, computed on the initial density operator ρ .

Refs [25, 26] demonstrated CQs are valid quasidistributions. These are linear in ρ , sum to 1 and their marginal distributions return the unperturbed probabilities $p_{\text{fin}}(b)$, $p_{\text{in}}(a)$ of measuring B and A separately. While they can be rigorously grounded in a suitable characteristic function for the sequential measurement scheme, the definition (2) is operational, and easier to interpret [38]. When $[\rho, A] = 0$, the joint probability of the TPM scheme is recovered. If $[\rho, A] \neq 0$, instead, the quantities $q_C(a, b)$ may attain negative values. It has been established this is a manifestation of the failure of non-contextual models at describing the experiment [25].

While the CQs amend the TPM probability distribution by including measurement disturbance, MHQ directly identifies observables incompatibility [27, 35, 36]. The two concepts are intimately linked to each other. For rank-1 projectors $\Pi_a^A = |a\rangle\langle a|$, $\Pi_b^B = |b\rangle\langle b|$, MHQ is defined as

$$q_{\text{MH}}(a, b) \equiv \text{Re} [\text{Tr} [\Pi_b^B \Pi_a^A \rho]] = | \langle b|a \rangle |^2 \text{Re} \left[\frac{\langle b| \rho |a \rangle}{\langle b|a \rangle} \right]. \quad (3)$$

By construction, $q_{\text{MH}}(a, b)$ are real numbers that sum to 1, returning the correct marginal distributions for both A and B , and are linear in ρ . Moreover, being quasiprobabilities, $q_{\text{MH}}(a, b)$ can also assume negative values. The latter scenario explicitly targets the incompatibility of ρ and A , given that MHQs are equal to the joint probabilities in Eq. (1) of the TPM scheme for $[\rho, A] = 0$.

WEAK-QUASIPROBABILITIES

Replacing the strong measurement of A at time t_1 by its weak version, implemented by a general POVM with elements M_a^A , amounts to introduce coarse-graining [40]. This may lead to a classical description of the outcomes' statistics in that they can be modelled by a positive two-time probability distribution.

Let us refer to the scheme detailed in Fig. 1. At t_1 the system in the state ρ is coupled to an ancillary pointer state prepared in the state $|\mu\rangle$ with the same dimensionality d as the system. The coupling between the system and the pointer is realized by means of a modular unitary U defined on the system computational basis $|a\rangle$ as

$$U = \sum_{a=0}^{d-1} |a\rangle\langle a| \otimes V^a, \quad (4)$$

where V is such that $V|a\rangle = |a \oplus 1\rangle = |a+1 \bmod d\rangle$, $V^0 = \mathbb{I}$, and $V^n = V \cdot V^{n-1}$ for $n > 0$.

We can illustrate how the scheme works by first considering the case of a pure input: $\rho = |\psi\rangle\langle\psi|$ with $|\psi\rangle = \sum_a c_a |a\rangle$. When $|\mu\rangle = |0\rangle$, then

$$U |\psi\rangle|0\rangle = \sum_a c_a |a\rangle|a\rangle. \quad (5)$$

In these conditions, a strong measurement of the observable A on the pointer would yield the outcome a with probability $|c_a|^2$. Therefore, this operation realizes a measurement of the observable A on the system. Instead, $|\mu_0\rangle \equiv \frac{1}{\sqrt{d}} \sum_a |a\rangle$ has the property that $V|\mu_0\rangle = |\mu_0\rangle$; hence,

$$U |\psi\rangle|\mu_0\rangle = |\psi\rangle|\mu_0\rangle. \quad (6)$$

Any projective measurement on the pointer bears no implication for the system. By interpolating between the two cases with $|\mu\rangle = |0\rangle$ or $|\mu_0\rangle$, we can realize a weak measurement of A with arbitrary strength. Indeed, taking the initial state of the pointer as

$$|\mu\rangle = u_0 |0\rangle + \frac{u_1}{\sqrt{d-1}} \sum_{a \neq 0} |a\rangle \quad (7)$$

with real coefficients u_0 and u_1 , one obtains

$$U |\psi\rangle|\mu\rangle = \omega_0 \sum_a c_a |a\rangle|a\rangle + \omega_1 |\psi\rangle|\mu_0\rangle, \quad (8)$$

where $\omega_0 \equiv u_0 - u_1/\sqrt{d-1}$ and $\omega_1 \equiv u_1\sqrt{d/(d-1)}$. Thanks to the correlations introduced by the unitary U , from Eq. (8) we have that a strong measurement of the observable A on the pointer can realize a weak measurement of the same observable A on the system. At t_2 the observable B is measured with a standard strong

measurement. Therefore, the probabilities of the weak-sequential measurement scheme in Fig. 2 are given by

$$p_{\text{weak}}(a, b) \equiv |\langle b|\langle a|U|\psi\rangle|\mu\rangle|^2 = \omega_0^2 |c_a|^2 |\langle b|a\rangle|^2 + \frac{\omega_1^2}{d} |\langle b|\psi\rangle|^2 + \frac{2\omega_0\omega_1}{\sqrt{d}} \text{Re}[c_a \langle b|a\rangle \langle\psi|b\rangle] \quad (9)$$

where the normalization $\omega_0^2 + \omega_1^2 + 2\omega_0\omega_1/\sqrt{d} = 1$ holds.

By linearity, this formulation generalizes for a generic mixed state input ρ , whereby the state of the system after the measurement is $(m_a^A)^\dagger \rho m_a^A / \text{Tr}[(m_a^A)^\dagger m_a^A]$ with $m_a^A = \omega_0 \Pi_a^A + \omega_1 \mathbb{I}/\sqrt{d}$. The latter realizes a d -outcome POVM with elements [53, 54]

$$M_a^A = (m_a^A)^\dagger m_a^A = (1 - \omega_1^2) \Pi_a^A + \omega_1^2 \frac{\mathbb{I}}{d}. \quad (10)$$

The measurement strength is captured by the parameter $K = 1 - \omega_0^2$, ranging from $K = 0$ for no measurement to $K = 1$ for a fully projective measurement. The quantity K can be identified as a formalisation of which-path information in interferometry [44, 55]. In this general setting, the joint probability of the weak-sequential measurement scheme satisfy the relation

$$p_{\text{weak}}(a, b) = \omega_0^2 p(a, b) + \frac{\omega_1^2}{d} p_{\text{fin}}(b) + \frac{2\omega_0\omega_1}{\sqrt{d}} q_{\text{MH}}(a, b). \quad (11)$$

We can now elaborate on the definition of a new class of quasiprobabilities suited to such weak sequential schemes. A weak version of the CQs demand substituting $p(a, b)$ with $p_{\text{weak}}(a, b)$ in the definition of Eq. (2):

$$\tilde{q}_C(a, b) = p_{\text{weak}}(a, b) + \frac{1}{d} \left(p_{\text{fin}}(b) - \sum_a p_{\text{weak}}(a, b) \right). \quad (12)$$

The expression in (12) can be related more clearly to the ordinary quasiprobabilities by using Eq. (11) and the fact that $p_{\text{fin}}(b) - \sum_a p_{\text{weak}}(a, b) = \omega_0^2 (p_{\text{fin}}(b) - p_{\text{post}}(b))$:

$$\tilde{q}_C(a, b) = \omega_0^2 q_C(a, b) + \frac{\omega_1^2}{d} p_{\text{fin}}(b) + \frac{2\omega_0\omega_1}{\sqrt{d}} q_{\text{MH}}(a, b). \quad (13)$$

Importantly, $\tilde{q}_C(a, b)$ sum to 1, have $p_{\text{fin}}(b)$ as the marginal when summing over a , and are so that

$$\sum_b \tilde{q}_C(a, b) = \sum_b p_{\text{weak}}(a, b) = K p_{\text{in}}(a) + \frac{(1-K)}{d} \quad (14)$$

from marginalizing over b . This represents the expected marginal allowed by the weak measurement, thus supporting the validity of $\tilde{q}_C(a, b)$ as meaningful quasiprobabilities.

As for weak-MHQs, we replace in Eq. (3) the projector Π_a^A with its weak version M_a^A that yields to

$$\tilde{q}_{\text{MH}}(a, b) = K q_{\text{MH}}(a, b) + \frac{(1-K)}{d} p_{\text{fin}}(b). \quad (15)$$

Marginalizing $\tilde{q}_{\text{MH}}(a, b)$ over the outcomes a or b returns the same marginal distributions as for the weak-CQs $\tilde{q}_{\text{C}}(a, b)$. For qubit systems ($d = 2$), $\tilde{q}_{\text{MH}}(a, b) = \tilde{q}_{\text{C}}(a, b)$ for all strengths.

These weak quasidistributions can attain negative values, and their meaning remains the same for their counterparts based on projective measurements: they now also weight-in the effect of coarse-graining on the possibility of using a classical or quantum probability description. Considering the weak-MHQ in (15), it is easy to identify a limit value $\bar{K}(a, b)$ below which the single instance $q_{\text{MH}}(a, b)$ is non negative:

$$\bar{K}(a, b) = \frac{1}{1 - \frac{d q_{\text{MH}}(a, b)}{p_{\text{fin}}(b)}}. \quad (16)$$

Any coarse-graining of the measurements of A such that $K < \bar{K}$ makes the experiment compatible with a classical, noncontextual description.

EXPERIMENT AND RESULTS

We realized the weak-sequential scheme, depicted in Fig. 2 on photonic qubits coded in the polarisation of single photons from parametric down conversion. The system is prepared in the superposition $\cos(2\theta_0)|H\rangle + \sin(2\theta_0)|V\rangle$, where we use the standard notation for the horizontal and vertical polarisations rotated by the angle $2\theta_0$. The first measurement of the Pauli observable $A = Z$ is weak and is realized by means of a control-Z gate, with a second qubit acting as its target [42]; our implementation corresponds to taking $V = Z$ in the coupling unitary (4). The initial diagonal pointer state $|0\rangle = |D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ leads to a full-strength measurement ($K = 1$), while $|\mu_0\rangle = |H\rangle$ corresponds to no measurement. The logical states of the two qubits, system and pointer, are encoded as different polarisation bases. Hence, the most general state we employ to tune the measurement strength K is

$$|\mu\rangle = \cos(2\phi)|D\rangle + \sin(2\phi)|D^\perp\rangle, \quad (17)$$

with $|D^\perp\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$ and $K = 2\cos^2(2\phi) - 1$ [55]. The pointer is projected into the basis defined by $\{|D\rangle, |D^\perp\rangle\}$, while either the POVM element $M_0^Z = K|H\rangle\langle H| + (1-K)\mathbb{I}/2$ or $M_1^Z = K|V\rangle\langle V| + (1-K)\mathbb{I}/2$ is applied to the system. The latter is projected by a conventional polarisation measurement to assess the Pauli observable $B = X$. The corresponding experimental probabilities of the weak-sequential measurement scheme are reported in Fig. 3, and have served as the starting point for our analysis. The values of $p_{\text{fin}}(b)$ are obtained by running the measurement at $K = 0$, and then tracing out the pointer.

In Fig. 4 we plot the four possible weak-CQs $\tilde{q}_{\text{C}}(a, b)$ as a function of the measurement strength K , as ob-

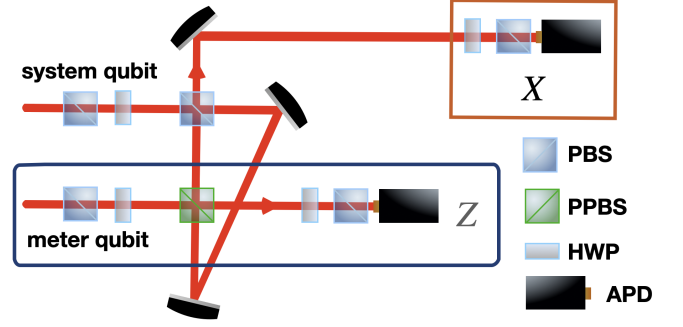


FIG. 2. Setup for the experimental test with photon qubits. Photon pairs are produced by a parametric down-conversion source (3 mm barium borate crystal pumped by a 100 mW cw laser at 405 nm), and delivered to a control-Z gate by single-mode fibres. The gate uses a partially polarising beam splitter (PPBS) with transmissions $T_H = 1$, $T_V = 1/3$ embedded within a Sagnac interferometer [56]. Polarisation-sensitive interference and post-selection of coincidence events result in the control-Z operation. Linear polarisation states are prepared and measured by means of half-waveplates (HWPs) and polarisation beam splitters (PBSs). Photons are finally sent on fibre-coupled avalanche photo-diodes (APDs).

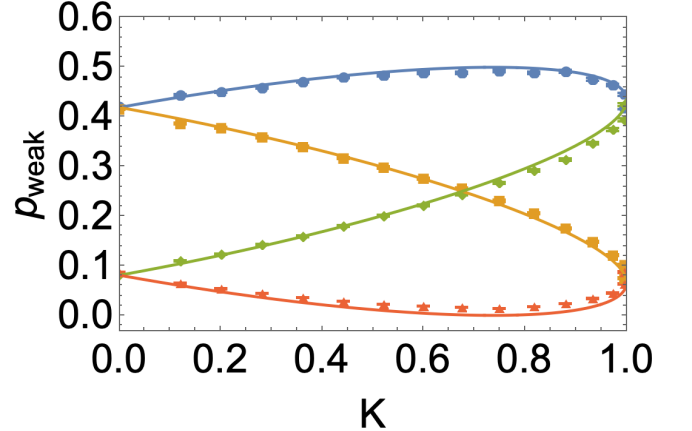


FIG. 3. Experimental probabilities $p_{\text{weak}}(a, b)$, from the weak measurement device depicted in Fig. 2, as a function of the measurement strength K . In the figure, $(a, b) = (H, D)$ (blue), (V, D) (yellow), $(H, D^\perp)$ (green), $(V, D^\perp)$ (red) for the input wave-function $|\psi\rangle = \cos(2\theta_0)|H\rangle + \sin(2\theta_0)|V\rangle$ ($\theta_0 = 10.6^\circ$). The solid curves denote the theoretical prediction, and the points are the experimental data.

tained by the definition in Eq. (12) using the probabilities $p_{\text{weak}}(a, b)$ retrieved from the experiment. The data refer to $\theta_0 = 10.6^\circ$ that corresponds to the almost maximal negativity in the ordinary CQs $q_{\text{C}}(a, b)$. The weak quasiprobability can show a negative part, and its origin can be traced back to two effects: the incompatibility of the observables A and B (in general, non-commuting operators), and the presence of quantum coherence in the initial state. For qubits both effects are quantified by the

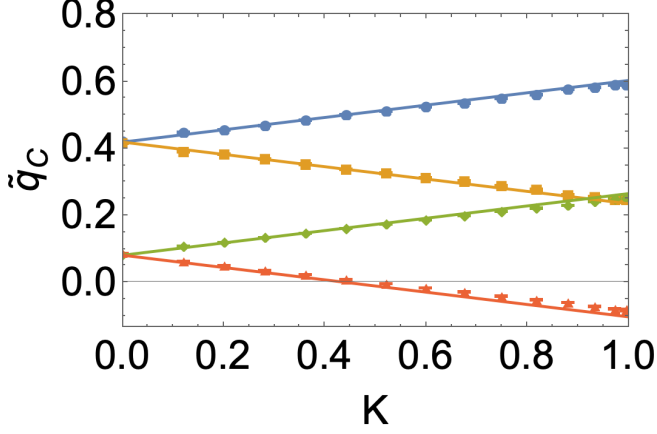


FIG. 4. Weak-quasiprobabilities $\tilde{q}_C(a, b)$, with $(a, b) = (H, D)$ (blue), (V, D) (yellow), $(H, D^\perp)$ (green), $(V, D^\perp)$ (red) for the input wave-function $|\psi\rangle = \cos(2\theta_0)|H\rangle + \sin(2\theta_0)|V\rangle$ ($\theta_0 = 10.6^\circ$), as a function of the measurement strength K . The solid curves denote the theoretical predictions, while the points are the experimental data. The size of the error bars is of the order of $2 \cdot 10^{-3}$, hence not visible on the plot.

MHQs $q_{\text{MH}}(a, b)$. Conversely, for a quantum system with generic dimension, the incompatibility of the observables and quantum coherence in the initial state can manifest in a distinct way, and are associated with the (strong) CQ and MHQ distributions, respectively. From the figure, we can thus observe the effect of the coarse-graining on the (first) measurement of A , which we experimentally obtain by decreasing K . There is indeed a threshold value of K under which all $\tilde{q}_C(a, b)$ become positive, and a classical description of the data becomes attainable.

The expression for the weak quasiprobability (11) spells out that each $p_{\text{weak}}(a, b)$ is constituted by three contributions with an intuitive physical meaning. In particular, the two terms $p(a, b)$ and $p_{\text{fin}}(b)/d$ capture the extreme cases, in which a full-strength measurement of A is carried out and no measurement of A is performed, respectively. Under those conditions, the coherence of ρ in the eigenbasis of A is irrelevant. The third term $C(a, b) = (2\omega_0\omega_1/\sqrt{d}) q_{\text{MH}}(a, b)$, thus, identifies the impact of such coherence in the joint statistics of A 's and B 's outcomes, given that part of it is preserved by the weak measurement. Using Eq. (11), we measure it as $C(a, b) \equiv p_{\text{weak}}(a, b) - \omega_0^2 p(a, b) - (\omega_1^2/d) p_{\text{fin}}(b)$, where the three quantities are obtained in separated experiments ran at strengths K equal to 1 and 0, respectively. Fig. 5 reports the measured values as a function of the measurement strength K , together with the theoretical predictions. We observe that in any experimental routine we performed, quantum coherence in the initial state affects the statistics originating from A and B , in terms of MHQs. In the experiments, we are able to detect it directly from implementing the weak-sequential measurement scheme of Fig. 2. In Fig. 5, it is also shown that

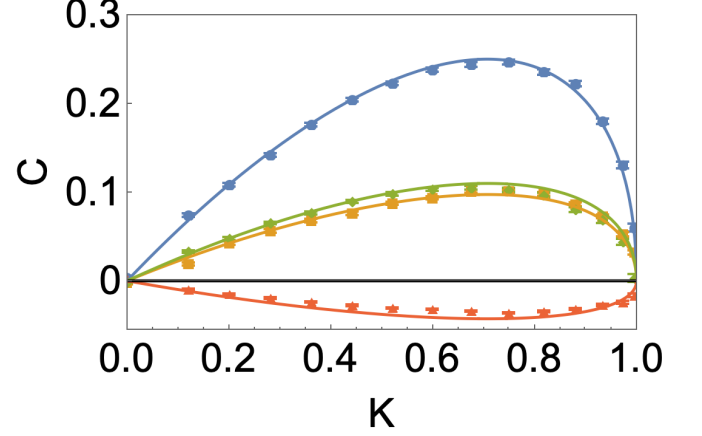


FIG. 5. Coherent content $C(a, b)$ detected by $p_{\text{weak}}(a, b)$, with $(a, b) = (H, D)$ (blue), (V, D) (yellow), $(H, D^\perp)$ (green), $(V, D^\perp)$ (red) for the input wave-function $|\psi\rangle = \cos(2\theta_0)|H\rangle + \sin(2\theta_0)|V\rangle$ ($\theta_0 = 10.6^\circ$), as a function of the measurement strength K . The solid curves denote the theoretical predictions, while the points are the experimental data. Discrepancies can be attributed mostly to the imperfect non-classical interference contrast at the gate. Errors on data are calculated by means of a Monte Carlo procedure, assuming the measured counts follow the Poisson distribution. These errors are quite small and not visible on the plot.

$C(a, b)$ can take both positive and negative values, as the real part of a quantum coherence does. Interestingly, being $C(a, b)$ directly proportional to $q_{\text{MH}}(a, b)$, the negative parts of $C(a, b)$ witness the negativity of CQ and MHQ distributions, as well as of their weak counterparts (see also Fig. 4).

The weak-sequential measurement scheme and in particular Eq. (11) provide an alternative way to reconstruct MHQs, with respect to the weak-TPM scheme [18, 27, 35, 57], and brings suggestions on how to extend to weak measurements the use of quasiprobabilities. The weak-TPM scheme relies on the relation

$$q_{\text{MH}}(a, b) = p(a, b) + \frac{1}{2} \left(p_{\text{fin}}(b) - w(a, b) \right). \quad (18)$$

In Eq. (18), $w(a, b) \equiv \text{Tr} [\Pi_b^B \rho_{\text{NS}}(a)]$ denotes the weak-TPM joint probabilities, where $\rho_{\text{NS}}(a) \equiv \Pi_a^A \rho \Pi_a^A + (\mathbb{I} - \Pi_a^A) \rho (\mathbb{I} - \Pi_a^A)$ is the density operator returned by performing non-selective projective measurements with projectors Π_a and $\Pi_a^\perp \equiv \mathbb{I} - \Pi_a^A$. Interestingly, for qubits ($d = 2$), Eq. (18) coincides with Eq. (2).

The advantage of using Eq. (11) instead of realizing the weak-TPM scheme lies in the fact that it is no longer necessary to implement projectors such as $\Pi_a^\perp$ that are more demanding in terms of the preparation and the manipulation of ancillary pointers. The normalization condition $\omega_0^2 + \omega_1^2 + 2\omega_0\omega_1/\sqrt{d} = 1$ guarantees that the MHQ distribution got from Eq. (11) has correct marginals. The weak-sequential measurement scheme resembles the one allowing for the direct reconstruction of the quantum

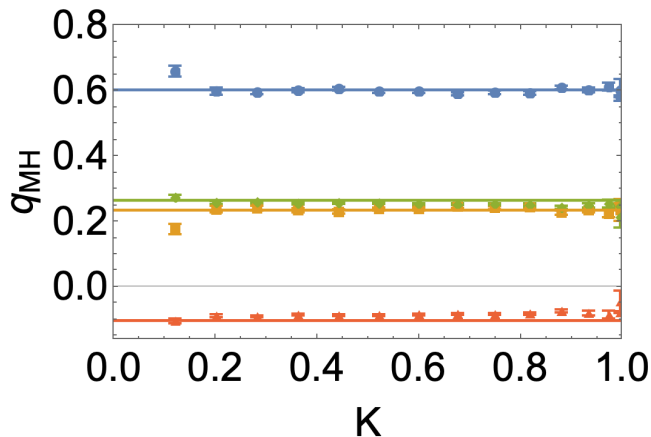


FIG. 6. Margenau-Hill quasiprobabilities $q_{\text{MH}}(a, b)$, with $(a, b) = (H, D)$ (blue), (V, D) (yellow), $(H, D^\perp)$ (green), $(V, D^\perp)$ (red) for the input wave-function $|\psi\rangle = \cos(2\theta_0)|H\rangle + \sin(2\theta_0)|V\rangle$ ($\theta_0 = 10.6^\circ$), as a function of the measurement strength K . The solid curves denote the theoretical prediction, and the points are the experimental data. Errors are calculated by means of a Monte Carlo procedure, assuming Poisson distribution of the measured counts.

state [58–60]. Here, the coarse-graining is instrumental to the reconstruction, as it enables access to quantum coherence in the initial state [61, 62].

In Fig. 6 we report the experimental reconstruction of $q_{\text{MH}}(a, b)$ using Eq. (11), where we have taken the same input quantum state as in Fig. 4. It is worth noting that more reliable performance are obtained away from the extreme conditions $K = 0, 1$ in terms of both precision and accuracy. When K is nearly zero, little is learned about A , while for K close to 1 there is small coherence between the eigenstates $|a\rangle$ of A left for the measurement of B . The experimental imperfections then lead to a relatively more severe impact, especially with a small informational content.

CONCLUSION

We have shown how two classes of quasiprobabilities (CQs and MHQs) can be defined when the first measurement in a sequence of measurements is weak. These weak-quasiprobabilities can still attain negative values, linked to contextuality. Realizing a sequential scheme measuring negativity—here the weak-sequential measurement scheme (Fig. 2)—can be implemented but at the price of refraining full information on the initial conditions.

The weak-sequential measurement scheme is an alternative tool for the analysis of extended protocols with sequential measurements at two or multiple times, with a rate of invasivity that one could control by the disappearance of negative values of a weak-quasiprobability.

These can be thought of as a complementary description of quantum states at multiple times [63, 64], and provide a tool for the monitoring of quantum objects with applications to quantum sensing [53, 65–68], and quantum thermodynamic processes [35, 57, 69–73]. A concrete example could be the realization of a quantum engine [74] fueled by quantum coherence through a thermodynamic cycle (e.g., in Otto configuration) run on weak measurements.

ACKNOWLEDGEMENTS

We thank R. Grasland for support during data collection and J. Sperling for valuable discussion. This work was supported by the PRIN project PRIN22-RISQUE-2022T25TR3 of the Italian Ministry of University. S.G. acknowledges support from the PRIN project 2022FEXLYB Quantum Reservoir Computing (QuReCo), and the PNRR MUR project PE0000023-NQSTI funded by the European Union–Next Generation EU. G.B. is supported by Rome Technopole Innovation Ecosystem (PNRR grant M4-C2-Inv). IG acknowledges the support from MUR Dipartimento di Eccellenza 2023–2027.

* These authors contributed equally to this work

- [1] J. von Neumann, *Mathematical Foundations of Quantum Mechanics*, new ed. (Princeton University Press, 2018).
- [2] R. Colbeck and R. Renner, Is a System’s Wave Function in One-to-One Correspondence with Its Elements of Reality?, *Phys. Rev. Lett.* **108**, 150402 (2012).
- [3] P. G. Lewis, D. Jennings, J. Barrett, and T. Rudolph, Distinct Quantum States Can Be Compatible with a Single State of Reality, *Phys. Rev. Lett.* **109**, 150404 (2012).
- [4] M. F. Pusey, J. Barrett, and T. Rudolph, On the reality of the quantum state, *Nat. Phys.* **8**, 475 (2012).
- [5] M. Ringbauer, B. Duffus, C. Branciard, E. G. Cavalcanti, A. G. White, and A. Fedrizzi, Measurements on the reality of the wavefunction, *Nat. Phys.* **11**, 249 (2015).
- [6] D. Frauchiger and R. Renner, Quantum theory cannot consistently describe the use of itself, *Nat. Commun.* **9**, 3711 (2018).
- [7] D. Deutsch, Quantum theory of probability and decisions, *Proc. R. Soc. A* **455**, 3129 (1999).
- [8] U. Leonhardt, *Measuring the Quantum State of Light* (Cambridge University Press, United Kingdom, 1997).
- [9] A. Cetto, L. de-la Peña, and E. Santos, A bell inequality involving position, momentum and energy, *Phys. Lett. A* **113**, 304 (1985).
- [10] K. Banaszek and K. Wódkiewicz, Testing quantum non-locality in phase space, *Phys. Rev. Lett.* **82**, 2009 (1999).
- [11] N. Delfosse, C. Okay, J. Bermejo-Vega, D. E. Browne, and R. Raussendorf, Equivalence between contextuality and negativity of the wigner function for qudits, *New Journal of Physics* **19**, 123024 (2017).

- [12] J. Haferkamp and J. Bermejo-Vega, [Equivalence of contextuality and wigner function negativity in continuous-variable quantum optics](#) (2021), [arXiv:2112.14788 \[quant-ph\]](#).
- [13] R. I. Booth, U. Chabaud, and P.-E. Emeriau, Contextuality and wigner negativity are equivalent for continuous-variable quantum measurements, *Phys. Rev. Lett.* **129**, 230401 (2022).
- [14] A. Mari and J. Eisert, Positive Wigner Functions Render Classical Simulation of Quantum Computation Efficient, *Phys. Rev. Lett.* **109**, 230503 (2012).
- [15] V. Veitch, C. Ferrie, D. Gross, and J. Emerson, Negative quasi-probability as a resource for quantum computation, *New J. Phys.* **14**, 113011 (2012).
- [16] S. Rahimi-Keshari, T. C. Ralph, and C. M. Caves, Sufficient conditions for efficient classical simulation of quantum optics, *Phys. Rev. X* **6**, 021039 (2016).
- [17] M. Frigerio, A. Debray, N. Treps, and M. Walschaers, [Resourcefulness of non-classical continuous-variable quantum gates](#) (2025), [arXiv:2410.09226 \[quant-ph\]](#).
- [18] L. M. Johansen, Quantum theory of successive projective measurements, *Phys. Rev. A* **76**, 012119 (2007).
- [19] H. F. Hofmann, How Weak Values Emerge in Joint Measurements on Cloned Quantum Systems, *Phys. Rev. Lett.* **109**, 020408 (2012).
- [20] H. F. Hofmann, Sequential measurements of non-commuting observables with quantum controlled interactions, *New J. Phys.* **16**, 063056 (2014).
- [21] F. Piacentini, A. Avella, M. P. Levi, M. Gramegna, G. Brida, I. P. Degiovanni, E. Cohen, R. Lussana, F. Villa, A. Tosi, F. Zappa, and M. Genovese, Measuring Incompatible Observables by Exploiting Sequential Weak Values, *Phys. Rev. Lett.* **117**, 170402 (2016).
- [22] D. R. M. Arvidsson-Shukur, J. Chevalier Drori, and N. Yunger Halpern, Conditions tighter than noncommutation needed for nonclassicality, *J. Phys. A: Math. Theor.* **54**, 284001 (2021).
- [23] M. Campisi, P. Hänggi, and P. Talkner, Colloquium: Quantum fluctuation relations: Foundations and applications, *Rev. Mod. Phys.* **83**, 771 (2011).
- [24] M. Esposito, U. Harbola, and S. Mukamel, Nonequilibrium fluctuations, fluctuation theorems, and counting statistics in quantum systems, *Rev. Mod. Phys.* **81**, 1665 (2009).
- [25] J. Ryu, J. Lim, S. Hong, and J. Lee, Operational quasiprobabilities for qudits, *Phys. Rev. A* **88**, 052123 (2013).
- [26] J. Jae, J. Ryu, and J. Lee, Operational quasiprobabilities for continuous variables, *Phys. Rev. A* **96**, 042121 (2017).
- [27] M. Lostaglio, A. Belenchia, A. Levy, S. Hernández-Gómez, N. Fabbri, and S. Gherardini, Kirkwood-Dirac quasiprobability approach to the statistics of incompatible observables, *Quantum* **7**, 1128 (2023).
- [28] P. Solinas and S. Gasparinetti, Probing quantum interference effects in the work distribution, *Phys. Rev. A* **94**, 052103 (2016).
- [29] P. Hofer, Quasi-probability distributions for observables in dynamic systems, *Quantum* **1**, 32 (2017).
- [30] M. Lostaglio, Quantum Fluctuation Theorems, Contextuality, and Work Quasiprobabilities, *Phys. Rev. Lett.* **120**, 040602 (2018).
- [31] P. Solinas, M. Amico, and N. Zanghì, Quasiprobabilities of work and heat in an open quantum system, *Phys. Rev. A* **105**, 032606 (2022).
- [32] G. Francica, Class of quasiprobability distributions of work with initial quantum coherence, *Phys. Rev. E* **105**, 014101 (2022).
- [33] G. Francica, Most general class of quasiprobability distributions of work, *Phys. Rev. E* **106**, 054129 (2022).
- [34] N. Yunger Halpern, B. Swingle, and J. Dressel, Quasiprobability behind the out-of-time-ordered correlator, *Phys. Rev. A* **97**, 042105 (2018).
- [35] S. Gherardini and G. De Chiara, Quasiprobabilities in Quantum Thermodynamics and Many-Body Systems, *PRX Quantum* **5**, 030201 (2024).
- [36] D. R. M. Arvidsson-Shukur, W. F. Braasch Jr., S. De Bievre, J. Dressel, A. N. Jordan, C. Langrenetz, M. Lostaglio, J. S. Lundeen, and N. Yunger Halpern, Properties and applications of the kirkwood-dirac distribution, *New J. Phys.* **26**, 121201 (2024).
- [37] H. Margenau and R. N. Hill, Correlation between measurements in quantum theory, *Prog. Theor. Phys.* **26**, 722 (1961).
- [38] J. Ryu, S. Hong, J.-S. Lee, K. H. Seol, J. Jae, J. Lim, J. Lee, K.-G. Lee, and J. Lee, Optical experiment to test negative probability in context of quantum-measurement selection, *Sci. Rep.* **9**, 19021 (2019).
- [39] Y. Aharonov, D. Z. Albert, and L. Vaidman, How the result of a measurement of a component of the spin of a spin-1/2 particle can turn out to be 100, *Phys. Rev. Lett.* **60**, 1351 (1988).
- [40] J. Kofler and C. Brukner, Classical World Arising out of Quantum Physics under the Restriction of Coarse-Grained Measurements, *Phys. Rev. Lett.* **99**, 180403 (2007).
- [41] G. J. Pryde, J. L. O'Brien, A. G. White, S. D. Bartlett, and T. C. Ralph, Measuring a photonic qubit without destroying it, *Phys. Rev. Lett.* **92**, 190402 (2004).
- [42] G. J. Pryde, J. L. O'Brien, A. G. White, T. C. Ralph, and H. M. Wiseman, Measurement of Quantum Weak Values of Photon Polarization, *Phys. Rev. Lett.* **94**, 220405 (2005).
- [43] H. M. Wiseman, Weak values, quantum trajectories, and the cavity-qed experiment on wave-particle correlation, *Phys. Rev. A* **65**, 032111 (2002).
- [44] T. C. Ralph, S. D. Bartlett, J. L. O'Brien, G. J. Pryde, and H. M. Wiseman, Quantum nondemolition measurements for quantum information, *Phys. Rev. A* **73**, 012113 (2006).
- [45] N. S. Williams and A. N. Jordan, Weak values and the leggett-garg inequality in solid-state qubits, *Phys. Rev. Lett.* **100**, 026804 (2008).
- [46] Y. Suzuki, M. Iinuma, and H. F. Hofmann, Violation of leggett-garg inequalities in quantum measurements with variable resolution and back-action, *New Journal of Physics* **14**, 103022 (2012).
- [47] L. Clemente and J. Kofler, Necessary and sufficient conditions for macroscopic realism from quantum mechanics, *Phys. Rev. A* **91**, 062103 (2015).
- [48] A. Bednorz and W. Belzig, Quasiprobabilistic Interpretation of Weak Measurements in Mesoscopic Junctions, *Phys. Rev. Lett.* **105**, 106803 (2010).
- [49] M. F. Pusey, Anomalous Weak Values Are Proofs of Contextuality, *Phys. Rev. Lett.* **113**, 200401 (2014).
- [50] F. Piacentini, A. Avella, M. P. Levi, R. Lussana, F. Villa, A. Tosi, F. Zappa, M. Gramegna, G. Brida, I. P. Degiovanni, and M. Genovese, Experiment Investigating the Connection between Weak Values and Contextual-

- ity, *Phys. Rev. Lett.* **116**, 180401 (2016).
- [51] V. Cimini, I. Gianani, F. Piacentini, I. P. Degiovanni, and M. Barbieri, Anomalous values, Fisher information, and contextuality, in generalized quantum measurements, *Quantum Sci. Technol.* **5**, 025007 (2020).
 - [52] J. Monroe, N. Yunger Halpern, T. Lee, and K. Murch, Weak Measurement of a Superconducting Qubit Reconciles Incompatible Operators, *Phys. Rev. Lett.* **126**, 100403 (2021).
 - [53] G. G. Gillett, R. B. Dalton, B. P. Lanyon, M. P. Almeida, M. Barbieri, G. J. Pryde, J. L. O'Brien, K. J. Resch, S. D. Bartlett, and A. G. White, Experimental Feedback Control of Quantum Systems Using Weak Measurements, *Phys. Rev. Lett.* **104**, 080503 (2010).
 - [54] L. Mancino, M. Sbroscia, E. Roccia, I. Gianani, F. Somma, P. Mataloni, M. Paternostro, and M. Barbieri, The entropic cost of quantum generalized measurements, *Npj Quantum Inf.* **4**, 20 (2018).
 - [55] B.-G. Englert, Fringe visibility and which-way information: An inequality, *Phys. Rev. Lett.* **77**, 2154 (1996).
 - [56] V. Cimini, S. Gherardini, M. Barbieri, I. Gianani, M. Sbroscia, L. Buffoni, M. Paternostro, and F. Caruso, Experimental characterization of the energetics of quantum logic gates, *Npj Quantum Inf.* **6**, 96 (2020).
 - [57] S. Hernández-Gómez, S. Gherardini, A. Belenchia, M. Lostaglio, A. Levy, and N. Fabbri, Projective measurements can probe nonclassical work extraction and time correlations, *Phys. Rev. Res.* **6**, 023280 (2024).
 - [58] J. S. Lundeen, B. Sutherland, A. Patel, C. Stewart, and C. Bamber, Direct measurement of the quantum wavefunction, *Nature* **474**, 188 (2011).
 - [59] L. Calderaro, G. Foletto, D. Dequal, P. Villoresi, and G. Vallone, Direct reconstruction of the quantum density matrix by strong measurements, *Phys. Rev. Lett.* **121**, 230501 (2018).
 - [60] L. Xu, H. Xu, T. Jiang, F. Xu, K. Zheng, B. Wang, A. Zhang, and L. Zhang, Direct characterization of quantum measurements using weak values, *Phys. Rev. Lett.* **127**, 180401 (2021).
 - [61] A. Budiyono and H. K. Dipojono, Quantifying quantum coherence via kirkwood-dirac quasiprobability, *Phys. Rev. A* **107**, 022408 (2023).
 - [62] A. Budiyono, J. F. Sumbowo, M. K. Agusta, and B. E. Nurhandoko, Quantum coherence from Kirkwood–Dirac nonclassicality, some bounds, and operational interpretation, *J. Phys. A-Math.* **57**, 255301 (2024).
 - [63] D. Horsman, C. Heunen, M. F. Pusey, J. Barrett, and R. W. Spekkens, Can a quantum state over time resemble a quantum state at a single time?, *Proc. R. Soc. A* **473**, 20170395 (2017).
 - [64] J. Fullwood and A. J. Parzygnat, Operator representation of spatiotemporal quantum correlations, arXiv preprint arXiv:2405.17555 [10.48550/arXiv.2405.17555](https://arxiv.org/abs/2405.17555) (2024).
 - [65] F. Sciarrino, M. Ricci, F. De Martini, R. Filip, and L. Mišta, Realization of a Minimal Disturbance Quantum Measurement, *Phys. Rev. Lett.* **96**, 020408 (2006).
 - [66] M. S. Blok, C. Bonato, M. L. Markham, D. J. Twitchen, V. V. Dobrovitski, and R. Hanson, Manipulating a qubit through the backaction of sequential partial measurements and real-time feedback, *Nat. Phys.* **10**, 189 (2014).
 - [67] L. Zhang, A. Datta, and I. A. Walmsley, Precision Metrology Using Weak Measurements, *Phys. Rev. Lett.* **114**, 210801 (2015).
 - [68] H.-J. Kim, J.-H. Jung, K.-J. Lee, and Y.-S. Ra, Recovering quantum entanglement after its certification, *Sci. Adv.* **9**, eadi5261 (2023), <https://www.science.org/doi/pdf/10.1126/sciadv.adi5261>.
 - [69] A. Levy and M. Lostaglio, Quasiprobability Distribution for Heat Fluctuations in the Quantum Regime, *PRX Quantum* **1**, 010309 (2020).
 - [70] M. Maffei, C. Elouard, B. O. Goes, B. Huard, A. N. Jordan, and A. Auffèves, Anomalous energy exchanges and Wigner-function negativities in a single-qubit gate, *Phys. Rev. A* **107**, 023710 (2023).
 - [71] F. Cerisola, F. Mayo, and A. J. Roncaglia, A Wigner Quasiprobability Distribution of Work, *Entropy* **25**, 1439 (2023).
 - [72] S. S. Pratapsi, S. Deffner, and S. Gherardini, Quantum speed limit for Kirkwood–Dirac quasiprobabilities, *Quantum Sci. Technol.* **10**, 035019 (2025).
 - [73] S. Hernández-Gómez, T. Isogawa, A. Belenchia, A. Levy, N. Fabbri, S. Gherardini, and P. Cappellaro, Interferometry of quantum correlation functions to access quasiprobability distribution of work, *Npj Quantum Inf.* **10**, 115 (2024).
 - [74] L. M. Cangemi, C. Bhadra, and A. Levy, Quantum engines and refrigerators, *Phys. Rep.* **1087**, 1 (2024).

Appendix 2: Experimental protocol for qubit-environment entanglement detection

Experimental protocol for qubit–environment entanglement detection

G. Bizzarri^{*,1}, L. Sansoni^{*,2}, E. Stefanutti², I. Gianani¹, M. Barbieri^{1,3}, K. Roszak⁴, and A. Chiuri²

¹Dipartimento di Scienze, Università degli Studi Roma Tre, Via della Vasca Navale 84, 00146 Rome, Italy

²ENEA - Nuclear Department, Via E. Fermi 45, 00100 Frascati, Italy

³Istituto Nazionale di Ottica - CNR, L.go Enrico Fermi 6, 50126, Florence, Italy

⁴FZU - Institute of Physics of the Czech Academy of Sciences, Na Slovance 1999/2, 182 00 Prague, Czech Republic

Decoherence is a manifestation of the coupling of a system with its environment. The resulting loss of information can hamper the functioning of quantum devices, hence the need of understanding its origin and dynamics. Decoherence can stem from entanglement, but it can also be classical in nature. Indeed, methods have been developed to understand whether qubit–environment entanglement (QEE) is actually present in some important classes of quantum channels - pure dephasing. Their practicality resides in the fact they only require accessing the system qubit. In this article we show an implementation of this technique in a photonic quantum channel simulator via a scheme that has been tailored to the system under study. By controlling the input state of the environment in our simulation, we can check the occurrence of qubit environment entanglement in simple, yet insightful test cases. Our results showcase the usefulness and experimental relevance of the QEE witnessing technique.

1 Introduction

Detecting entanglement directly from a quantum state is not possible in general, as entanglement measures are nonlinear functions of the states. The usual solution is to perform quantum state tomography first [1, 2, 3, 4] followed by calculation of entanglement from the density matrix [5, 6]. However, if prior information is available, the problem can be vastly simplified. When the state is known to be reasonably close to a target, then an entanglement witness represents a handy solution [7, 8, 9, 10]. It consists of an

observable, built from separable measurements, capable of assessing the presence of entanglement. This technique requires fewer measurement settings than full quantum tomography, and has prompted similar investigations applied to channels, for instance to set bounds on their quantum capacity [11, 12].

For pure states, entanglement is inversely proportional to the purity of the reduced state of either entangled subsystems. This implies that one can extract meaningful information addressing a much-reduced space, with a conspicuous advantage in terms of the number of measurement settings. For mixed states, such shortcuts only work for special classes of density matrices, such as X-states [13]. One such class of density matrices involves qubit–environment (QE) states obtained via an interaction that can only lead to pure dephasing of the qubit once the environment is traced out. Such a case is particularly relevant for solid-state qubits: a mismatch between the energy difference of the qubit states and that of the environmental modes (either natural or induced by external parameters, such as the magnetic field), prohibits energy exchange. Remarkably, it is possible to give qualitative [14] and quantitative [15] information on qubit environment entanglement (QEE) that can be generated via such a pure dephasing interaction. The only requirement is that the initial qubit state must be pure. There are no limitations on the initial state of the environment, which can be (and often is) mixed and can be of an arbitrary dimension. Thus, there is a distinct asymmetry between the two subsystems which lies at the core of the methods of characterizing entanglement for such states. This asymmetry remains for pure dephasing of larger systems, and it is possible to use methods reminiscent of methods used for the treatment of QEE for the study of arbitrary system–environment entanglement [16].

Generation of QEE via pure dephasing evolutions

* G.B. and L.S. should be considered joint first authors.

is unambiguously connected with the transfer of information from the system state to the state of the environment, while qubit decoherence which is not accompanied by the generation of entanglement does not involve any information transfer [17]. This means that the QE state is qualitatively different for entangling and separable evolutions: at least in principle, entanglement could be detected by measurements on a single subsystem, the environment [14]. As the environment is, almost by definition, hardly accessible, addressing the qubit is the obvious choice. The measurement of QEE accessing only the qubit is feasible, paying the modest prize of a slightly more complicated scheme [18, 19, 20], in order to transfer information about entanglement from the state of the environment to the state of the qubit.

In this article, we provide an experimental demonstration of QEE detection in an optical setup, based on the methods of Ref. [18] for indirect detection. This allowed us to merge the idea of only addressing a single subsystem with the use of a witness observable. The enabling element realising decoherence is a Controlled-NOT (CNOT) gate between the qubit and its environment - itself in the form of a pure or mixed qubit. As the CNOT gate is an entangling operation, one could conjecture any such decoherence process to be entangling: this is actually true when the QE is in a pure state as long as the CNOT gate leads to decoherence (the initial state of the environmental qubit is not an equal superposition state of the form $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$). For mixed states, decoherence without entanglement is possible, and even relatively common [21, 22, 23, 24, 25].

The direct application of the scheme of Ref. [18], which involves the use of the same interaction between the qubit and the environment that leads to decoherence, to probe entanglement, is not sufficient to witness the entangling power of the CNOT gate. This is due to the inherent asymmetry of the gate, which has no effect when the control qubit is in the $|0\rangle$ state. To counter this, we take advantage of the control over the interaction which is possible in optical scenarios, and use the controlled phase gate in the second step.

We probe two classes of initial states of the environment for their suitability to generate entanglement under the CNOT operation. The first class consists of pure state superpositions of the $|0\rangle$ and $|1\rangle$ states that differ by the probability of obtaining state $|0\rangle$ quantified by a single parameter θ . The second class of states involves corresponding mixed states, which have no coherence. For both classes of envi-

ronmental states, we observe qualitatively correct behavior of the entanglement witness, which properly signifies qubit-environment entanglement. Quantitatively, we observe a discrepancy which is due to the imbalance between the two polarizations in the experimental setup. The nature of the discrepancy is well understood and it can be taken into account, so that the theory perfectly reproduces experimental curves.

The paper is organized as follows. In Sec. 2 we discuss qubit-environment entanglement in our setup, introduce the measurement scheme, and model the measurement in an idealized scenario. In Sec. 3 we describe the experiment, as well as present and discuss the results. Sec. 4 concludes the paper.

2 Theory

We consider a system qubit (Q) interacting with the environment (E). Although we represent both with single-qubit states, they serve different roles and should be treated asymmetrically: for instance, the environment must only dephase the qubit, but the qubit can cause more general decoherence to the environment. The initial state of Q is required to be pure, while for the environment, we can recur to a more general form of its density matrix

$$R_E(0) = \begin{pmatrix} c_0 & d \\ d^* & c_1 \end{pmatrix}, \quad (1)$$

where c_0 and c_1 are real, while d is a complex number. The condition for Eq. (1) to be a density matrix is that $|d|^2 \leq c_0 c_1$, which amounts to non-negative definiteness. The initial state of the joint QE arrangement is

$$\sigma(0) = |\psi_i\rangle_Q \langle\psi_i| \otimes R_E(0), \quad (2)$$

with $|\psi_i\rangle_Q = \alpha|0\rangle_Q + \beta|1\rangle_Q$, and $\alpha, \beta \neq 0$. As shown in Refs [14, 16], any state obtained using a conditional quantum gate

$$U = |0\rangle_Q \langle 0| \otimes w_{0,E} + |1\rangle_Q \langle 1| \otimes w_{1,E} \quad (3)$$

where $w_{i,E}$, $i = 0, 1$ are conditional environmental operators on state (2), is entangled if and only if $R_{00} \neq R_{11}$. Here the conditional density matrices of the environment are defined as

$$R_{ii} = w_{i,E} R_E(0) w_{i,E}^\dagger. \quad (4)$$

The analysis of the entangling character of the decoherence process thus requires a comparison of R_{00} and R_{11} , that can be carried out only if these are fiducially prepared. This can be achieved by initialising

Q in the pointer state $|i\rangle_Q$ and applying the gate (3), so that the state R_{ii} of the environment is prepared. The joint state remains separable, since pure dephasing cannot affect pointer states, but there is information on the interaction in the density matrix of the environment, and linearity can be employed to invert what could happen in the more general instance.

This available information can be extracted from the QE system through measurements of decoherence using a gate in the form (3), possibly with different conditional environmental operators w'_{iE} . The exact choice of operators w'_{iE} in relation to the operators w_{iE} , which describe the effect of the original conditional gate, determines the set of entangled states that can be witnessed by the procedure. Therefore, the initial QE state for the actual measurement to indirectly detect QEE is

$$\sigma(0) = |i\rangle_Q \langle i| \otimes R_E(0), \quad (5)$$

with $i = 0, 1$. The QE system undergoes a two-step evolution, which we implement by applying a series of quantum gates, *viz.* a CNOT, a Hadamard on Q and a Controlled-Z (CZ) gate.

Step 1: CNOT

The CNOT gate is used for the environment to decohere the qubit, and its action is defined as

$$U_1 = |0\rangle_Q \langle 0| \otimes \mathbb{1}_E + |1\rangle_Q \langle 1| \otimes \sigma_{x,E}. \quad (6)$$

When applied to the state (5), this leads to the joint QE state for $i = 0$

$$\sigma_0(t) = U\sigma(0)U^\dagger = |0\rangle_Q \langle 0| \otimes R_E(0), \quad (7)$$

and for $i = 1$,

$$\sigma_1(t) = U\sigma(0)U^\dagger = |1\rangle_Q \langle 1| \otimes \sigma_{x,E} R_E(0) \sigma_{x,E}. \quad (8)$$

Looking at the reduced density matrix of the environment, it follows that $R_{00} = R_E(0)$ and $R_{11} = \sigma_{x,E} R_E(0) \sigma_{x,E}$. Since QEE is proportional to how different these two density matrices are, we can use any measure of their similarity in order to obtain a proper entanglement measure [15]: here we use the trace norm [26], which yields particularly simple analytical results

$$T(R_{00}, R_{11}) = \frac{1}{2} \text{Tr} \sqrt{\Delta R^\dagger \Delta R} = \sqrt{\Delta c^2 + e^2}. \quad (9)$$

Here $\Delta R = R_{00} - R_{11}$ is the difference between the two conditional density matrices of the environment,

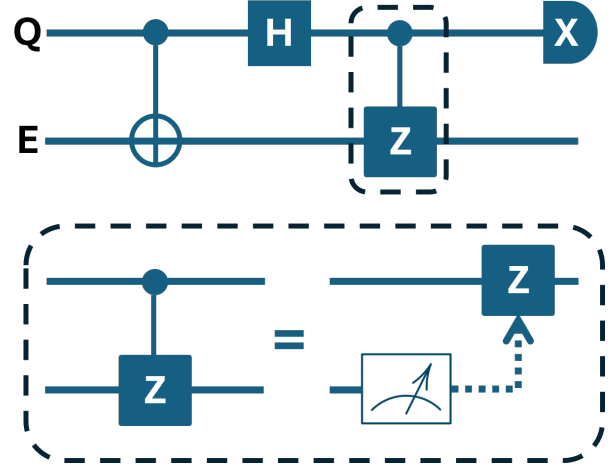


Figure 1: Schematic representation of the experimental protocol for QEE detection. Q: qubit, E: environment, H: Hadamard gate, Z (X): σ_Z (σ_X). In the dashed box the feed-forward implementation of a $C - \sigma_Z$ gate used in the experimental protocol as proposed in [27] [See the Appendix B for more details].

$\Delta c = c_0 - c_1$ is the difference between the occupations of the initial density matrix of the environment $R_E(0)$, while $e = 2\text{Im}(d)$ is twice the imaginary part of the coherence of that matrix (1). This means that entanglement is generated only if $\Delta c \neq 0$ and/or $\text{Im}(d) \neq 0$. We stress that the trace norm is not a unique choice and other measures, such as the fidelity, can be employed, yielding the same information about quantum correlations.

Step 2: Hadamard on Q + CZ

The original scheme of Ref. [18] calls for a Hadamard gate on Q in order to map its pointer states to equal superpositions after initial decoherence. This transformation is realised almost instantaneously and embedded in between free evolutions of the joint QE system. The difference in decoherence experienced after the superposition is excited depending on the qubit pointer state, can serve as a probe for QEE. The intuition is that, once the environment has been initialised, the qubit should be left to experience the maximal effect from decoherence, making it possible to witness entanglement. The necessary condition for the same QE interaction to be able to witness entanglement as was used to prepare the environmental states is $[w_{0,E}, w_{1,E}] \neq 0$. This condition is not fulfilled by the CNOT gate, since $w_{0,E} = \mathbb{1}$, thus a different controlled operation is required to witness entanglement that is probed.

In our scheme, we take advantage of the control

over the QE interaction that is granted by the optical setup, and use a CZ operation on both qubit and environment after the Hadamard gate is applied. A schematic representation of the protocol is shown in Fig. 1. The Hadamard gate transforms the QE density matrices (7) and (8) into

$$\sigma_0^*(t) = |+\rangle_Q \langle +| \otimes R_E(0), \quad (10)$$

$$\sigma_1^*(t) = |-\rangle_Q \langle -| \otimes \sigma_{x,E} R_E(0) \sigma_{x,E}, \quad (11)$$

respectively. Here the qubit states are denoted $|\pm\rangle_Q = \frac{1}{\sqrt{2}}(|0\rangle_Q \pm |1\rangle_Q)$. The CZ gate, applied on these new states, is given by

$$U_2 = |0\rangle_Q \langle 0| \otimes \mathbb{1}_E + |1\rangle_Q \langle 1| \otimes \sigma_{z,E}. \quad (12)$$

This can be thought of as resulting from a further interaction within the QE system, or as a part of the measurement process, as we will do in the following.

When acting on the state (10), resulting from the initial qubit state $|0\rangle_Q$, our procedure yields the joint QE density matrix

$$\sigma'_0 = \frac{1}{2} \begin{pmatrix} R_E(0) & R_E(0)\sigma_z \\ \sigma_z R_E(0) & \sigma_z R_E(0)\sigma_z \end{pmatrix}. \quad (13)$$

Note that the QE state (13) is written in matrix form only with respect to Q, while the degrees of freedom of the environment are incorporated in this notation within the matrix elements. Tracing out the environment yields no change in the occupations of the qubit, since $\text{Tr}_E R_E(0) = 1$, but its coherence does change as

$$\rho_{01}^{(0')} = \frac{1}{2} \text{Tr}_E (R_E(0)\sigma_z) = \frac{1}{2}(c_0 - c_1). \quad (14)$$

In the second instance, when the initial state of the qubit is $|1\rangle_Q$, the final joint state is,

$$\sigma'_1 = \frac{1}{2} \begin{pmatrix} \sigma_x R_E(0)\sigma_x & -\sigma_x R_E(0)\sigma_x \sigma_z \\ -\sigma_z \sigma_x R_E(0)\sigma_x & \sigma_z \sigma_x R_E(0)\sigma_x \sigma_z \end{pmatrix} \quad (15)$$

and the qubit coherence at the end is given by

$$\rho_{01}^{(1')} = -\frac{1}{2} \text{Tr}_E (\sigma_x R_E(0)\sigma_x \sigma_z) = \rho_{01}^{(0')} \quad (16)$$

(while the diagonal elements of the density matrix of E remain constant).

In order to detect the presence of entanglement in the QE system, we define an entanglement witness following Ref. [18],

$$W = \rho_{01}^{(0')} + \rho_{01}^{(1')} = 2\rho_{01}^{(0')} = (c_0 - c_1). \quad (17)$$

As expected, the value of this witness depends on the difference between the conditional density matrices ΔR , although the specific action of the controlled-phase gate allows entanglement to be detected only for $c_0 \neq c_1$. Entanglement for $c_0 = c_1$ with $e \neq 0$ can be detected using an analogous scheme utilizing a controlled-Y gate (this scheme is described in the Appendix A, B). Notably, W can be assessed by means of a measurement of the σ_x Pauli observable on the qubit only. Since we expect $\rho_{01}^{(0')}$ and $\rho_{01}^{(1')}$ to be real, we can directly estimate them as follows: $\frac{1}{2}\langle \sigma_x \rangle_\alpha = \frac{1}{2} \text{Tr}[\sigma_x \rho^\alpha] = (\rho^\alpha)_{01}$ with $\alpha = 0, 1$. Thus as the entanglement witness we consider the quantity

$$W = \frac{\langle \sigma_x \rangle_0 + \langle \sigma_x \rangle_1}{2}. \quad (18)$$

3 Experiment

Our example, however simplified, highlights the essential features of the detection scheme in Ref [18], and its modular articulation leads itself to a direct transposition with quantum gates [28]. In our implementation, qubit and environment are both implemented in the polarisation of two single photons, with the choice $|0\rangle_Q$ along the horizontal polarisation and $|1\rangle_Q$ along the vertical for the qubit system, while the choice $|0\rangle_E$ along the diagonal polarisation and $|1\rangle_E$ along the antidiagonal polarization for the environment. The CNOT gate is implemented by means of the setup shown in Fig. 2. As reported in Ref. [29], the gate is based on a partially polarising beam splitter within a Sagnac interferometer. While the following Hadamard gate can be implemented by a half-waveplate, the probabilistic functioning of the CNOT gate prevents from putting two of them in cascade [30]. This could be remedied by using initial entanglement [31] or, since the second gate is the last operation in the sequence, we can take inspiration from the Griffiths-Niu theorem [27] and realise it by means of measurement and classical feedback [32]. We have taken this second option for the sake of experimental simplicity.

Input states can be controlled by setting half-waveplates, but, due to additional polarisation-dependent loss from the partially polarising beam splitters, when the state $\cos 2\theta|0\rangle_E + \sin 2\theta|1\rangle_E$ is targeted, the angle setting α on the plate should be biased according to $\tan(\theta/2) = \tan(2\alpha)/\sqrt{3}$ [33, 32]. In addition, our gate is effectively a Controlled-Z gate, but it can be mapped onto a proper CNOT operation by using additional Hadamard gates on the en-

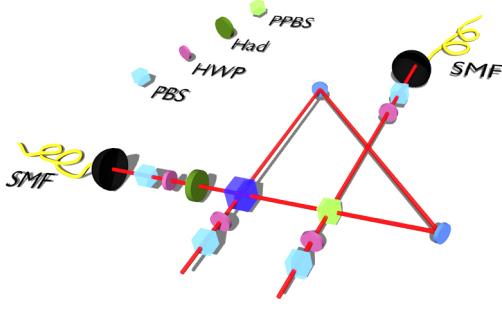


Figure 2: Experimental setup. The two photons representing the system and the environment are prepared in a suitable polarization state by means of a polarizing beam splitter (PBS) and a halfwaveplate (HWP). These two enter the CNOT gate embedded within a Sagnac arrangement with the two paths showing different polarizations. Here interference between the two photons takes place on a PBS, while a partial polarizing beam splitter (PPBS) ensures balancement between the two polarization. A Hadamard gate on the qubit system is applied at the output through a HWP at 22° . The analysis is performed by a tomographic setup composed by a HWP and a PBS. The setup is in free space, but photons are delivered to it by means of single-mode fibers. Likewise, the outputs are fiber-coupled to avalanche photodiodes (APDs) detectors.

vironment - these have been included at the preparation and measurement stage in order to keep the setup compact.

3.1 Environment in a pure state

The initial QE state is given by $|\Psi\rangle_{in}^j = |j\rangle_Q (\cos \frac{\theta}{2} |0\rangle_E + \sin \frac{\theta}{2} |1\rangle_E)$, where $j = 0, 1$ and θ is a real parameter that can be experimentally set. After undergoing the transformation described above, the output states are:

$$|\Psi\rangle_{out}^0 = \cos \frac{\theta}{2} |+\rangle_Q |0\rangle_E + \sin \frac{\theta}{2} |-\rangle_Q |1\rangle_E \quad (19)$$

$$|\Psi\rangle_{out}^1 = \cos \frac{\theta}{2} |+\rangle_Q |1\rangle_E + \sin \frac{\theta}{2} |-\rangle_Q |0\rangle_E \quad (20)$$

where $|\pm\rangle_Q = \frac{1}{\sqrt{2}}(|0\rangle_Q \pm |1\rangle_Q)$. Both states are obviously entangled as long as $\cos \frac{\theta}{2} \neq 0, 1$ and maximum entanglement is reached for $\cos \frac{\theta}{2} = \sin \frac{\theta}{2} = \frac{1}{\sqrt{2}}$. As we only target the qubit, we trace out the environment obtaining the following mixed state for both outputs (19-20):

$$\rho_{out} = \frac{1}{2} \begin{pmatrix} 1 & \cos \theta \\ \cos \theta & 1 \end{pmatrix}. \quad (21)$$

As witness for the entanglement, we use the operator (18), which can be rewritten as

$$W(\theta) = \text{Tr}(\rho_{out} \cdot \sigma_x) = \cos \theta, \quad (22)$$

for the initial states under study. The quantity is equal to zero only for the initial state of the environment that cannot be entangled via the CNOT gate, with $\theta = \pm\pi/2$. For all other values of θ , the pure initial state of E would be entangled with any superposition on Q, which is signified by the non-zero value of the witness given by eq. (22).

In the experiment, for each environmental state corresponding to a specific value of θ , we set the initial qubit state in either $|0\rangle_Q$ or $|1\rangle_Q$ and project the output as explained so far. The obtained results for the witness (18) as a function of θ are shown in Fig. 3. To account for the expected statistical fluctuations and estimate uncertainties associated with the experimental photon counts, a statistical approach based on a simplified Monte Carlo-like method was adopted. Specifically, the Poisson distribution represents the proper statistical model for describing counting processes in photon detection. Therefore, for each coincidence count n we have generated a set of random variables (i.e. 200) sampled from a Poisson distribution with n as expectation value. This simulated dataset was then used to calculate the standard deviation associated to the corresponding experimental data.

As can be seen, the experimentally obtained data-points all correspond to non-zero values of the witness, correctly signifying QEE for all of the measured values of θ . The curve fitted to these points (red, solid curve) perfectly captures the θ -values for which the witness $W(\theta) = 0$ and there is no entanglement, namely $\theta = \pm\pi/2$. The measured and fitted witness curve shows some deviations from the theoretical behavior (plotted using the dashed line in Fig. 3). This deviation between measured and expected behavior is greatest when the values of the witness are large while it is near zero in the vicinity of the $W(\theta) = 0$ points, thus the witness which is meant to only signify the presence of entanglement and not to act as a measure for it, fulfills its purpose. The deviation is due to the imbalance between the two polarizations in the experimental setup as well as a non perfect indistinguishability between the qubit and environment photons. Both these contributions can be accounted for. In fact, the solid curve used to fit the experimental points is obtained when this unavoidable asymmetry is included in the model (see Appendix C for

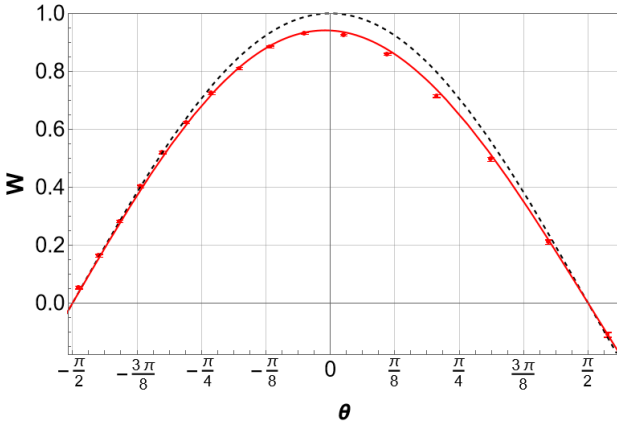


Figure 3: QEE Witness as a function of θ for pure initial states of the environment. Dots refer to experimental data. The red dashed line represents the theoretical fit of the experimentally obtained data-points, taking into account known experimental imperfections. Black dashed line shows the idealised theoretical behavior.

more details). The data points follow this model with a high accuracy, thus confirming our expected behavior.

3.2 Mixed environment

A second experiment has been performed encoding the initial state of the environment as the mixed state

$$\rho_E^{\text{in}}(p) = c_0|0\rangle_E\langle 0| + c_1|1\rangle_E\langle 1|$$

with $c_0 \in [0, 1]$ and $c_0 + c_1 = 1$. This corresponds to the state (1) with the off-diagonal elements set to zero, $d = 0$, and describes a statistical mixture of states, where state $|0\rangle$ has probability c_0 and state $|1\rangle$ has probability c_1 . According to Eq. (17), the proposed witness reads as follows:

$$W(p) = 2c_0 - 1. \quad (23)$$

For such initial states of E, QEE will be generated by the CNOT gate as long as the probabilities corresponding to states $|0\rangle_E$ and $|1\rangle_E$ differ from one another.

The parameter c_0 has been experimentally varied by accumulating the counts obtained for each measurement when the input state for the environment was either $|0\rangle_E$ or $|1\rangle_E$, and setting different integrating intervals. The proposed witness has been applied to a suitable mixing of these datasets obtained in post-processing. This procedure has been repeated for both input qubit states $|0\rangle_Q$ and $|1\rangle_Q$ and the results are reported in Fig. 4.

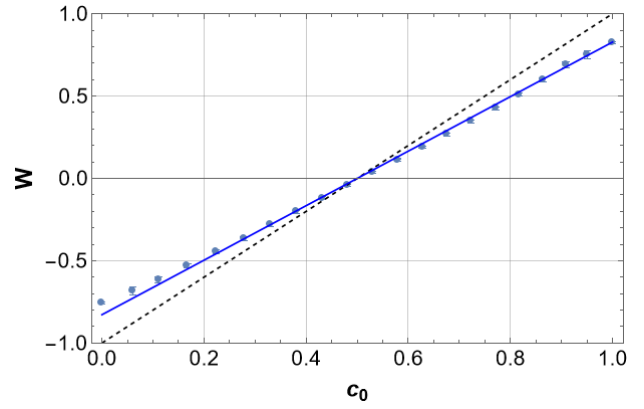


Figure 4: QEE Witness for mixed initial states of the environment as a function of c_0 . Dots refer to experimental data. The blue solid line represents the theoretical fits considering the experimental parameters. The black dashed line plots the expected theoretical behavior without any imperfection.

The experimental data perfectly reproduces the expected linear dependence of the entanglement witness on the probability c_0 and correctly signifies the only initial state of the environment incapable of QEE generation under the CNOT operation as $c_0 = 1/2$ (maximally mixed initial state of the environment). The discrepancy between the expected behavior (dashed black line) of the QEE witness given by eq. (23) and the observed behavior (solid blue line) amounts to a difference in slope of the linear c_0 -dependence and does not result in any qualitative changes. Thus the experiment identifies the parameter ranges for the class of mixed environmental states that will entangle with a qubit in a superposition state under the CNOT gate, without taking the imbalance between the two polarizations in the experimental setup into account. As in the case of the pure states of the environment discussed before, this asymmetry can be described theoretically, and the corrected theoretical curves are plotted with a blue solid line in Fig. 4.

3.3 Discussion

It is important to stress here that the presented mixed-state results are the core of the paper. The pure state results serve to demonstrate the applicability of the method to different states, but the methods for the study of QEE in pure dephasing evolutions have been devised for mixed-state environments and their superiority over standard methods of experimental study of entanglement becomes evident for such states. For pure states, entanglement and decoherence are un-

ambiguously linked and the presence of decoherence signifies the presence of QEE. Thus quantum state tomography of the QE system is not necessary as long as it is known that the whole QE state is pure - information about QEE is present in the density matrix of the qubit. When considering mixed states, this is no longer the case since the build up of classical correlations can lead to qubit decoherence just as well as the generation of QEE.

The mixed state results presented here were generated by mixing results obtained with the environment initially in state $|0\rangle_E$ and state $|1\rangle_E$ in post-processing. This means that in each run of the experiment, entanglement has been signified, and the CNOT gate would generate entanglement if the qubit was initially in a superposition state. This is seen on Fig. 4 for $c_0 = 0$ and $c_0 = 1$, which both have non-zero values of the witness. For all intermediate states, the value of the QEE witness is obtained as a mean average of the values at the boundary with the probabilities c_0 and c_1 . Thus mixed state results can be obtained from pure state results in a straightforward manner as in the case of any other observable.

This demonstrates the primary advantage of the presented entanglement witnessing scheme over direct calculation of any mixed state entanglement measure, outside of the fact that the operations and measurements are performed only on the qubit. Once the value of the QEE witness for all states in any pure state decomposition of a given mixed state is known, the witness can be easily found by averaging. For measures that can be applied generally (the scheme only works for pure dephasing), each mixed state has to be treated separately, since averaging of pure state entanglement is known to lead to wrong results.

This is a distinct advantage even for the two-qubit case and the mixed state which is experimentally studied in this paper is a perfect example. The states obtained via the CNOT gate for the qubit in an equal superposition state and the environment in either state $|0\rangle_E$ or state $|1\rangle_E$ are both maximally entangled. This means that the average of entanglement of any mixture of these states is also the maximum value. Nevertheless, it is known that any mixture of the two states is not maximally entangled as long as $c_0 \neq 0, 1$ and for $c_0 = 1/2$ the state is separable. This information is easily obtained by averaging the values of the QEE witness over the eigendecomposition of the initial state of the environment, but cannot be found from a straightforward study of the average entanglement in eigendecompositions of the QE state.

4 Conclusions

In summary, we demonstrated the implementation of a QEE witness within a quantum photonic simulator. The procedure has been tailored to a specific experimental platform and takes advantage from the possibility of tuning the qubit-environment interaction. We managed to detect correlations using straightforward measurements on just the qubit, using a series of operations on the qubit in order to transfer the information about entanglement present in the state of the environment via a QE interaction. This success hinges on the straightforward distinction between decoherence that is the result of QEE and decoherence that is classical in nature, evident in pure dephasing channels. This is at a stark difference from the typical scenario which requires joint measurement of both potentially entangled systems, and customized approaches targeting specific cases remain important.

The key ability for successful QEE detection consisted of implementing a Hadamard operation with good fidelity and over timescales that are much shorter than the natural timescale of the joint qubit-environment state. This allows to treat the two decoherence processes as separate from other operations on the qubit. Faulty behavior of other components resulted in deviation of the observed value of the witness with respect to the ideal, but have not compromised its reliability for QEE detection, meaning that entanglement has been detected correctly and only the magnitude of the observed signal has been affected. All this makes us confident that the QEE witness may earn its place among the everyday toolkit for experimental open quantum systems.

Acknowledgment – KR, AC, and ES: This project is funded within the QuantERA II Programme that has received funding from the EU H2020 research and innovation programme under GA No 101017733, and with funding organizations MEYS (Czech Republic) and NQSTI (Italy). GB is supported by Rome Technopole Innovation Ecosystem (PNRR grant M4-C2-Inv). IG and MB acknowledge support from MUR Dipartimento di Eccellenza 2023-2027 and PRIN project PRIN22-RISQUE-2022T25TR3 of the Italian Ministry of University.

References

- [1] Daniel F. V. James, Paul G. Kwiat, William J. Munro, and Andrew G. White. “Measurement of qubits”. *Phys. Rev. A* **64**, 052312 (2001).

- [2] Matthias Christandl and Renato Renner. “Reliable quantum state tomography”. *Phys. Rev. Lett.* **109**, 120403 (2012).
- [3] Shahnawaz Ahmed, Carlos Sánchez Muñoz, Franco Nori, and Anton Frisk Kockum. “Quantum state tomography with conditional generative adversarial networks”. *Phys. Rev. Lett.* **127**, 140502 (2021).
- [4] Chang-Kang Hu, Chao Wei, Chilong Liu, Liangyu Che, Yuxuan Zhou, Guixu Xie, Haiyang Qin, Guantian Hu, Haolan Yuan, Ruiyang Zhou, Song Liu, Dian Tan, Tao Xin, and Dapeng Yu. “Experimental sample-efficient quantum state tomography via parallel measurements”. *Phys. Rev. Lett.* **133**, 160801 (2024).
- [5] Marcel Neugebauer, Laurin Fischer, Alexander Jäger, Stefanie Czischek, Selim Jochim, Matthias Weidemüller, and Martin Gärttner. “Neural-network quantum state tomography in a two-qubit experiment”. *Phys. Rev. A* **102**, 042604 (2020).
- [6] Guilherme P. Temporão, Pedro Ripper, Thiago B. Guerreiro, and Gustavo C. do Amaral. “Two-photon quantum state tomography of photonic qubits”. *Phys. Rev. A* **109**, 022402 (2024).
- [7] M. Barbieri, F. De Martini, G. Di Nepi, P. Mataloni, G. M. D’Ariano, and C. Macchiavello. “Detection of entanglement with polarized photons: Experimental realization of an entanglement witness”. *Phys. Rev. Lett.* **91**, 227901 (2003).
- [8] Mohamed Bourennane, Manfred Eibl, Christian Kurtsiefer, Sascha Gaertner, Harald Weinfurter, Otfried Gühne, Philipp Hyllus, Dagmar Bruß, Maciej Lewenstein, and Anna Sanpera. “Experimental detection of multipartite entanglement using witness operators”. *Phys. Rev. Lett.* **92**, 087902 (2004).
- [9] Zheng-Da Li, Qi Zhao, Rui Zhang, Li-Zheng Liu, Xu-Fei Yin, Xingjian Zhang, Yue-Yang Fei, Kai Chen, Nai-Le Liu, Feihu Xu, Yu-Ao Chen, Li Li, and Jian-Wei Pan. “Measurement-device-independent entanglement witness of tripartite entangled states and its applications”. *Phys. Rev. Lett.* **124**, 160503 (2020).
- [10] You Zhou, Qi Zhao, Xiao Yuan, and Xiongfeng Ma. “Detecting multipartite entanglement structure with minimal resources”. *npj Quantum Information* **5**, 83 (2019).
- [11] Álvaro Cuevas, Massimiliano Proietti, Mario Arnolfo Ciampini, Stefano Duranti, Paolo Mataloni, Massimiliano F. Sacchi, and Chiara Macchiavello. “Experimental detection of quantum channel capacities”. *Phys. Rev. Lett.* **119**, 100502 (2017).
- [12] Chiara Macchiavello and Massimiliano F. Sacchi. “Efficient accessible bounds to the classical capacity of quantum channels”. *Phys. Rev. Lett.* **123**, 090503 (2019).
- [13] Paulo E.M.F. Mendonça, Marcelo A. Marchioli, and Diógenes Galetti. “Entanglement universality of two-qubit x-states”. *Annals of Physics* **351**, 79–103 (2014).
- [14] Katarzyna Roszak and Łukasz Cywiński. “Characterization and measurement of qubit-environment-entanglement generation during pure dephasing”. *Phys. Rev. A* **92**, 032310 (2015).
- [15] Katarzyna Roszak. “Measure of qubit-environment entanglement for pure dephasing evolutions”. *Phys. Rev. Research* **2**, 043062 (2020).
- [16] Katarzyna Roszak. “Criteria for system-environment entanglement generation for systems of any size in pure-dephasing evolutions”. *Phys. Rev. A* **98**, 052344 (2018).
- [17] Katarzyna Roszak and Łukasz Cywiński. “Equivalence of qubit-environment entanglement and discord generation via pure dephasing interactions and the resulting consequences”. *Phys. Rev. A* **97**, 012306 (2018).
- [18] Katarzyna Roszak, Damian Kwiatkowski, and Łukasz Cywiński. “How to detect qubit-environment entanglement generated during qubit dephasing”. *Phys. Rev. A* **100**, 022318 (2019).
- [19] Bartosz Rzepkowski and Katarzyna Roszak. “A scheme for direct detection of qubit-environment entanglement generated during qubit pure dephasing” (2020). [arXiv:2002.10901](https://arxiv.org/abs/2002.10901).
- [20] Małgorzata Strzałka and Katarzyna Roszak. “Detection of entanglement during pure dephasing evolutions for systems and environments of any size”. *Phys. Rev. A* **104**, 042411 (2021).

- [21] Jens Eisert and Martin B. Plenio. “Quantum and classical correlations in quantum brownian motion”. *Phys. Rev. Lett.* **89**, 137902 (2002).
- [22] Julius Helm and Walter T. Strunz. “Quantum decoherence of two qubits”. *Phys. Rev. A* **80**, 042108 (2009).
- [23] J. Maziero, T. Werlang, F. F. Fanchini, L. C. Céleri, and R. M. Serra. “System-reservoir dynamics of quantum and classical correlations”. *Phys. Rev. A* **81**, 022116 (2010).
- [24] A. Pernice and W. T. Strunz. “Decoherence and the nature of system-environment correlations”. *Phys. Rev. A* **84**, 062121 (2011).
- [25] R. Lo Franco, B. Bellomo, E. Andersson, and G. Compagno. “Revival of quantum correlations without system-environment back-action”. *Phys. Rev. A* **85**, 032318 (2012).
- [26] Lian-He Shao, Zhengjun Xi, Heng Fan, and Yongming Li. “Fidelity and trace-norm distances for quantifying coherence”. *Phys. Rev. A* **91**, 042120 (2015).
- [27] Robert B. Griffiths and Chi-Sheng Niu. “Semi-classical fourier transform for quantum computation”. *Phys. Rev. Lett.* **76**, 3228–3231 (1996).
- [28] He Lu, Chang Liu, Dong-Sheng Wang, Luo-Kan Chen, Zheng-Da Li, Xing-Can Yao, Li Li, Nai-Le Liu, Cheng-Zhi Peng, Barry C. Sanders, Yu-Ao Chen, and Jian-Wei Pan. “Experimental quantum channel simulation”. *Phys. Rev. A* **95**, 042310 (2017).
- [29] V. Cimini, S. Gherardini, M. Barbieri, I. Gi-anani, M. Sbroscia, L. Buffoni, M. Paternostro, and F. Caruso. “Experimental characterization of the energetics of quantum logic gates”. *npj Quantum Information* **6**, 96 (2020).
- [30] T. C. Ralph, K. J. Resch, and A. Gilchrist. “Efficient toffoli gates using qudits”. *Phys. Rev. A* **75**, 022313 (2007).
- [31] Stefanie Barz, Borivoje Dakić, Yannick Ole Lipp, Frank Verstraete, James D. Whitfield, and Philip Walther. “Linear-optical generation of eigenstates of the two-site xy model”. *Phys. Rev. X* **5**, 021010 (2015).
- [32] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White. “Experimental demonstration of a compiled version of shor’s algorithm with quantum entanglement”. *Phys. Rev. Lett.* **99**, 250505 (2007).
- [33] Ryo Okamoto, Holger F. Hofmann, Shigeki Takeuchi, and Keiji Sasaki. “Demonstration of an optical quantum controlled-not gate without path interference”. *Phys. Rev. Lett.* **95**, 210506 (2005).
- [34] Till J Weinhold, Alexei Gilchrist, Kevin J Resch, Andrew C Doherty, Jeremy L O’Brien, Geoffrey J Pryde, and Andrew G White. “Understanding photonic quantum-logic gates: The road to fault tolerance” (2008). [arXiv:0808.0794](https://arxiv.org/abs/0808.0794).

A Step 2: Hadamard on Q + CY

We have studied the operation of a protocol for the detection of QEE that can only detect entanglement which is the result of a difference in the occupations of the initial state of the environment. Nevertheless, entanglement will also be present if the initial coherences of E have non-zero imaginary parts, as discussed in Sec. 2. Such entanglement can be witnessed if the controlled-phase (CZ) gate in the second step is replaced by a controlled Y gate, as shown below.

The CY gate, to be applied on the states (10) and (11), is given by:

$$U'_2 = |0\rangle_Q \langle 0| \otimes \mathbb{1}_E + |1\rangle_Q \langle 1| \otimes \sigma_{y,E}. \quad (24)$$

Following the procedure detailed in the main text while replacing the gate U_2 of eq. (12) with the CY gate, we get coherence terms analogous to (14) and (16) that now read as follows:

$$\rho_{01}^{(0')} = \frac{1}{2} \text{Tr}_E(R_E(0)\sigma_y) = \frac{i}{2}(d - d^*) = -\frac{e}{2}, \quad (25)$$

$$\rho_{01}^{(1')} = -\frac{1}{2} \text{Tr}_E(\sigma_x R_E(0)\sigma_x \sigma_y) = -\frac{e}{2} = \rho_{01}^{(0')}. \quad (26)$$

The witness (17) in this case can detect entanglement for $e \neq 0$, which can be present in the system also when $c_0 = c_1$:

$$W = \rho_{01}^{(0')} + \rho_{01}^{(1')} = -2\text{Im}(d) = -e. \quad (27)$$

B Feed-Forward approach

Here we propose an alternative approach, exploiting two photons with polarization encoding for both the qubit and the environment, relying on a feed-forward method. As stated in [27], whenever the last operation before the measurement stage involves two- (or more) qubit gates, it is possible to map it into single-qubit operations controlled by a classical signal, acting as a feedback. It is then necessary to design a feed-forward operation equivalent to $C - \sigma_Z$ and $C - \sigma_Y$ operations, in order to retrieve the witnesses (17) and (27).

Feed-forward $C - \sigma_Z$

The qubit-environment joint state after the interaction and a subsequent rotation of the qubit (see 1) is, respectively (10) or (11), according to the initial qubit state.

A measurement of the environment (in the computational basis) leads to, respectively,

$$\begin{aligned} \text{Tr}_E(|0\rangle_E \langle 0| \cdot \sigma_0) &= c_0 |+\rangle_Q \langle +|, \\ \text{Tr}_E(|1\rangle_E \langle 1| \cdot \sigma_0) &= c_1 |+\rangle_Q \langle +|, \end{aligned}$$

and

$$\begin{aligned} \text{Tr}_E(|0\rangle_E \langle 0| \cdot \sigma_1) &= c_1 |-\rangle_Q \langle -|, \\ \text{Tr}_E(|1\rangle_E \langle 1| \cdot \sigma_1) &= c_0 |-\rangle_Q \langle -|. \end{aligned}$$

Indeed, regardless the initial input state, a measurement of the environment leads to the same qubit state. In order to distinguish between the two possible outcomes of the environment's measurement, a single-qubit operation on the qubit must be implemented.

By applying a σ_Z gate on the qubit whenever 1 is measured on the environment we retrieve

$$\begin{cases} \text{Tr}_E(|0\rangle_E \langle 0| \cdot \sigma_0) = c_0 |+\rangle_Q \langle +| \xrightarrow{Id} c_0 |+\rangle_Q \langle +|, \\ \text{Tr}_E(|1\rangle_E \langle 1| \cdot \sigma_0) = c_1 |+\rangle_Q \langle +| \xrightarrow{\sigma_Z} c_1 |-\rangle_Q \langle -|, \end{cases} \quad (28)$$

for σ_0 , and

$$\begin{cases} \text{Tr}_E(|0\rangle_E \langle 0| \cdot \sigma_1) = c_1 |-\rangle_Q \langle -| \xrightarrow{Id} c_1 |-\rangle_Q \langle -|, \\ \text{Tr}_E(|1\rangle_E \langle 1| \cdot \sigma_1) = c_0 |-\rangle_Q \langle -| \xrightarrow{\sigma_Z} c_0 |+\rangle_Q \langle +|. \end{cases} \quad (29)$$

By measuring in the σ_Z diagonal basis the states (28) and (29) the (17) is retrieved.

Therefore, the $C - \sigma_Z$ gate is mapped to a simple σ_Z acting on the qubit according to the measure outcome of the environment, in the computational basis.

Feed-forward $C - \sigma_Y$

The $C - \sigma_Y$ gate is mapped into a conditional application of a proper single-qubit operation on the initial states (10) or (11). However, in order for the imaginary part of the density matrix to be reconstructed, the environment state has to be mapped into the σ_Y diagonal basis via the rotation matrix,

$$IH = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ i & -1 \end{pmatrix}, \quad (30)$$

thus the environment state becomes:

$$IHR_E(0)IH = \frac{1}{2} \begin{pmatrix} 2i(d - \text{Re}(d)) + c_0 + c_1 & -2\text{Re}(d) - i(c_0 - c_1) \\ -2\text{Re}(d) - i(c_0 - c_1) & -2i(d - \text{Re}(d)) + c_0 + c_1 \end{pmatrix}.$$

In this case, a projective measurement of the environment in the computational basis leads to

$$\begin{cases} \text{Tr}_E(|0\rangle_E \langle 0| \cdot |+\rangle_Q \langle +| \otimes IHR_E(0)IH) = (-\text{Im}(d) + \frac{c_0+c_1}{2}) |+\rangle_Q \langle +|, \\ \text{Tr}_E(|1\rangle_E \langle 1| \cdot |+\rangle_Q \langle +| \otimes IHR_E(0)IH) = (\text{Im}(d) + \frac{c_0+c_1}{2}) |+\rangle_Q \langle +|, \end{cases} \quad (31)$$

and we get

$$IH \cdot \sigma_X R_E(0) \sigma_X \cdot IH = \frac{1}{2} \begin{pmatrix} -2i(d - \text{Re}(d)) + c_0 + c_1 & -2\text{Re}(d) + i(c_0 - c_1) \\ -2\text{Re}(d) - i(c_0 - c_1) & 2i(d - \text{Re}(d)) + c_0 + c_1 \end{pmatrix},$$

which maps Eq. (11) into

$$\begin{cases} \text{Tr}_E(|0\rangle_E \langle 0| \cdot |-\rangle_Q \langle -| \otimes IH \cdot \sigma_X R_E(0) \sigma_X \cdot IH) = (\text{Im}(d) + \frac{c_0+c_1}{2}) |-\rangle_Q \langle -|, \\ \text{Tr}_E(|1\rangle_E \langle 1| \cdot |-\rangle_Q \langle -| \otimes IH \cdot \sigma_X R_E(0) \sigma_X \cdot IH) = (-\text{Im}(d) + \frac{c_0+c_1}{2}) |-\rangle_Q \langle -|. \end{cases} \quad (32)$$

In order to distinguish between the environment's measurement outcome on Eqs (31), (32), a σ_Z gate is applied on the qubit when $|1\rangle_E \langle 1|$ is measured, which yields

$$\begin{cases} \text{Tr}_E(|0\rangle_E \langle 0| \cdot |+\rangle_Q \langle +| \otimes IHR_E(0)IH) \xrightarrow{Id} \frac{-e+c_0+c_1}{2} |+\rangle_Q \langle +|, \\ \text{Tr}_E(|1\rangle_E \langle 1| \cdot |+\rangle_Q \langle +| \otimes IHR_E(0)IH) \xrightarrow{\sigma_X} \frac{+e+c_0+c_1}{2} |-\rangle_Q \langle -|, \end{cases} \quad (33)$$

and

$$\begin{cases} \text{Tr}_E(|0\rangle_E \langle 0| \cdot |-\rangle_Q \langle -| \otimes IH \cdot \sigma_X R_E(0) \sigma_X \cdot IH) \xrightarrow{Id} \frac{e+c_0+c_1}{2} |-\rangle_Q \langle -|, \\ \text{Tr}_E(|1\rangle_E \langle 1| \cdot |-\rangle_Q \langle -| \otimes IH \cdot \sigma_X R_E(0) \sigma_X \cdot IH) \xrightarrow{\sigma_X} \frac{-e+c_0+c_1}{2} |+\rangle_Q \langle +|, \end{cases} \quad (34)$$

respectively, from which a feed-forward operation equivalent to a $C - \sigma_Y$ gate is implemented. A graphical sketch of the operation is presented in Fig. 5.

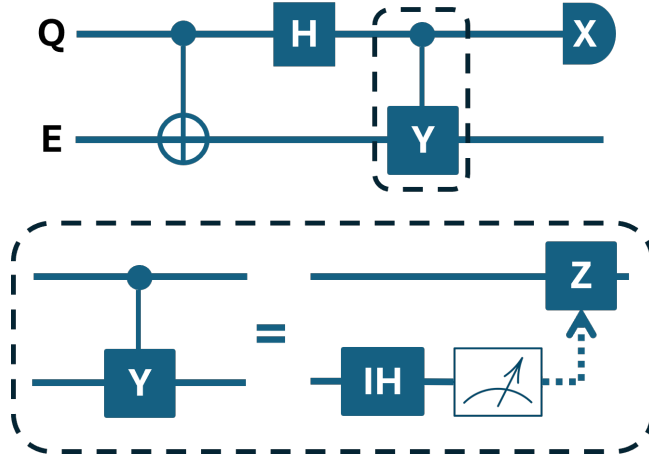


Figure 5: Schematic representation of the experimental protocol for QEE detection. Q: qubit, E: environment, H: Hadamard gate, Z: σ_Z , X: σ_X , Y: σ_Y . In the dashed box the proposed feed-forward implementation of a $C - \sigma_Y$ gate as reported in [27].

C Modeling of experimental imperfections

In our experiment, we must account for two potential sources of deviation from an ideal setup: the imperfect transmittivities of the partial polarizing beam splitter (PPBS) and the lack of perfect indistinguishability between the qubit and environment photons. The latter affects the visibility of the Hong-Ou-Mandel (HOM) interference, which is crucial for the CNOT operation. The model employed for our setup is derived from the one presented in Ref. [34]. Let T_h and T_v represent the transmittivities of the PPBS for horizontal and vertical polarizations, respectively, while V denotes the visibility of the HOM interference. The qubit and environment photons are directed into the two input modes of the PPBS, where they undergo one of the following transformations, depending on their polarizations:

$$\begin{aligned}
 |0\rangle_Q &\rightarrow \sqrt{T_h}|0\rangle_Q, \\
 |1\rangle_Q &\rightarrow \sqrt{T_v}|1\rangle_Q + \sqrt{1-T_v}|1\rangle_E, \\
 |+\rangle_E &\rightarrow \sqrt{1-\varepsilon^2}\sqrt{T_h}|+\rangle_E + \varepsilon\sqrt{T_h}|+\rangle'_E, \\
 |-\rangle_E &\rightarrow \sqrt{1-\varepsilon^2}(\sqrt{T_v}|-\rangle_Q + \sqrt{1-T_v}|-\rangle_E) + \varepsilon(\sqrt{T_v}|-\rangle'_Q + \sqrt{1-T_v}|-\rangle'_E),
 \end{aligned}$$

where $\varepsilon = \sqrt{1 - \frac{V}{V_{id}}}$, and $V_{id} = 0.8$ is the ideal HOM visibility, while the states $|j'\rangle$ ($j = \pm$) indicate photons which do not interfere, but still can give some contribution to the measurements. Note that for the Environment system the horizontal and vertical polarized photons correspond to the diagonal and antidiagonal logic state, respectively. According to Eq. (22), the measurements yield the probability of the QE system being in a particular polarization state. This probability consists of two independent contributions: one from the expected interference between indistinguishable photons (with weight $\sqrt{1-\varepsilon^2}$) and the other from the spurious contributions of distinguishable states (with weight ε).

In our experiment the parameters measured for the transmittivities of the PPBS and the visibility of the HOM interference were $T_h = 0.983 \pm 0.002$, $T_v = 0.324 \pm 0.002$ and $V = 0.75 \pm 0.1$. The models shown in Figs 3,4 are calculated according to these transformations and measured parameters.