SAPIENZA
UNIVERSITÀ DI ROMA

Photonics Technologies for Quantum Communication and Metrology

Facoltà di Scienze Matematiche Fisiche e Naturali

Dottorato di Ricerca in Fisica – XXXIII Ciclo

Candidate

Mauro Valeri

ID number 1420383

Thesis Advisor

Prof. Fabio Sciarrino

2020/2021

Thesis defended on 06 July 2021
in front of a Board of Examiners composed by:

Prof. Dario Gerace (chairman)

Prof. Stefano Lupi

Prof. Miriam Vitiello

Referees: Prof. Lorenzo Pavesi, Prof. Giuseppe Leo

Photonics Technologies for Quantum Communication and Metrology
Ph.D. thesis. Sapienza – University of Rome

This thesis has been typeset by LaTeX and the Sapthesis class.

Author's email: mauro.valeri@uniroma1.it mauro.valeri91@gmail.com

Quid animo satis

List of publications

- F. Basso Basset[1], **M. Valeri**[1], E. Roccia, V. Muredda, D. Poderini, J. Neuwirth, N. Spagnolo, M. B. Rota, G. Carvacho, F. Sciarrino, and R. Trotta, *Quantum key distribution with entangled photons generated on-demand by a quantum dot*, Science Advances, 7, 12, (2021).

- **M. Valeri**, E. Polino, D. Poderini, N. Spagnolo, I. Gianani, G. Corrielli, A. Crespi, R. Osellame, and F. Sciarrino, *Experimental adaptive Bayesian estimation of multiple phases with limited data*, NPJ Quantum Information, 6, 92, (2020).

- V. Cimini[2], E. Polino[2], **M. Valeri**[2], I. Gianani, N. Spagnolo, G. Corrielli, A. Crespi, R. Osellame, M. Barbieri, F. Sciarrino, *Calibration of multiparameter sensors via machine learning at the single-photon level*, Physical Review Applied, 15(4), 044003, (2021).

- E. Polino[3], **M. Valeri**[3], N. Spagnolo, and F. Sciarrino, *Photonic quantum metrology*, AVS Quantum Sci., 2, 0247034, (2020).

- K. Rambhatla, S. E. D'Aurelio, **M. Valeri**, E. Polino, N. Spagnolo, and F. Sciarrino, *Adaptive phase estimation through a genetic algorithm*, APS Phys. Rev. Research, 2, 3, 033078, (2020).

- D. Poderini, I. Agresti, G. Marchese, E. Polino, T. Giordani, A. Suprano, **M. Valeri**, G. Milani, N. Spagnolo, G. Carvacho, R. Chaves, and F. Sciarrino, *Experimental violation of n-locality in a star quantum network*, Nature communications, 11, 1, 1-8, (2020).

- E. Polino, M. Riva, **M. Valeri**, R. Silvestri, G. Corrielli, A. Crespi, N. Spagnolo, R. Osellame, and F. Sciarrino, *Experimental multiphase estimation on a chip*, Optica, 6, 288-295, (2019).

- D. Cozzolino, E. Polino, **M. Valeri**, G. Carvacho, D. Bacco, N. Spagnolo, L. K. Oxenlowe and F. Sciarrino, *Air-core fiber distribution of hybrid vector vortex-polarization entangled states*, Advanced Photonics, 1, 4, (2019).

[1,2,3]These authors contributed equally.

- S. Atzeni, A.S. Rab, G. Corrielli, E. Polino, **M. Valeri**, P. Mataloni, N. Spagnolo, A. Crespi, F. Sciarrino, and R. Osellame, *Integrated sources of entangled photons at the telecom wavelength in femtosecond-laser-written circuits*, Optica, 5, 311-314, (2018).

Scientific Conference/Workshop Contributions

Oral Presentations

- *February 2020.* Oral presentation at the virtual conference IMEKO TC-4 2020, Palermo, Italy

  Title: Quantum two-phase estimation inside a photonic integrated device

- *February 2019.* Oral presentation at the Italian Conference on CyberSecurity (ITASEC19) in Pisa, Italy

  Title: Integrated photonics devices for quantum cryptography

Posters

- *April 2019.* Poster at Quantum Information and Measurement (QIM) V conference in Rome, Italy

  Title: Integrated source of entangled photon pair at telecom wavelength

- *September 2019.* Poster at Causality in the quantum world workshop in Anacapri, Italy

  Title: Integrated multiarm interferometers for quantum multiphase estimation protocols

Contents

Acronyms

BBO Beta-Barium Borate β-BaB2O4

BiBO Bismuth triborate BiBO2

BS Beam Splitter

BSM Bell-State Measurement

CRB Cramér-Rao Bound

DAG Directed Acyclic Graph

DE Differential Evolution

DI Device-Independent

FBS Fiber Beam Splitter

FI Fisher Information

FLW Femtosecond Laser Writing

FWM Four-Wave Mixing

GHZ Greenberger-Horne-Zeilinger

HBT Hanbury Brown and Twiss

HL Heisenberg Limit

HOM Hong-Ou-Mandel

HWP Half Wave-Plate

KTP Potassium Titanyl Phosphate KTiOPO4

LHV Local Hidden Variable

LN Lithium Niobate LiNbO3

LOCC Local Operations and Classical Communication

MDI Measurement-Device-Independent

MLE Maximum Likelihood Estimator

MSE Mean Square Error

MZI Mach-Zehnder interferometer

NN Neural Network

NCHV Non-Contextual Hidden Variable

NRMSE Normalized Root Mean Square Error

OAM Orbital Angular Momentum

PBS Polarizing Beam Splitter

POVM Positive Operator Valued Measure

PSO Particle Swarm Optimization

QBER Quantum Bit Error Rate

QCRB Quantum Cramér-Rao Bound

QD Quantum Dot

QFI Quantum Fisher Information

QKD Quantum Key Distribution

QL Quadratic Loss

QWP Quarter Wave-Plate

RMSE Root Mean Square Error

SLM Spatial Light Modulator

SMF Single-Mode Fiber

SPDC Spontaneous Parametric Down-Conversion

SQL Standard Quantum Limit

SSN Star-Shaped Network

Introduction

Quantum resources have given rise to new perspectives in the fields of Information and Communication. This is the case of *entanglement*, which is at the heart of most protocols of Quantum Information. It allows to outperform classical approaches, as in *Quantum Metrology* [1, 2] and *Quantum Communication* [3, 4]. The generation, manipulation, and distribution, up to the secure revelation of such quantum properties represent the fundamental tasks of experimental research in Quantum Information. They provide the basic tools that will be the basis of future quantum technologies.
In this context, the photonic implementation of Quantum Information protocols represents a convenient choice [5]. Indeed, using single photons as quantum carriers has several advantages, such as easy mobility and manipulation. Here, different existing approaches can be exploited to manipulate light. On the one hand, *bulk-based quantum technologies* — despite being the first method developed — still represent a reliable and versatile approach to perform different Quantum Information tasks and study foundational problems. On the other hand, *integrated photonics* represents one of the best technological platforms for the realization of Quantum Information protocols, allowing for better stability and scalability of quantum systems involving light.
Unlike static systems such as cold atoms or superconductive materials, the other major advantage of photons is the inherent suitability for the transmission among dislocated parties. *Flying qubits* have paved the way to quantum communications between distant parties: from different setups in the same laboratory to intracity scenarios, and long-distance communication via satellite. To this end, *fiber* networks allow an easy way to develop quantum communication networks covering distances within 100 km. While *free-space* optical communication adopting satellites is the only short-term possibility for a worldwide scale. Furthermore, adopting the existing fiber structure for classical communication to also support its quantum counterpart may be a convenient short-term solution for a real-life implementation, that does not necessarily require the construction of new complex infrastructures. Going in this direction implies the investigation of quantum protocols in *telecom* wavelengths, i.e., the region around 1550 nm, for which current classical fiber networks are built. Indeed, in this wavelength range, optical fibers show minimal signal losses. Conversely, free-space communication is typically developed around 800 nm, where air propagation provides a good compromise as a wavelength window for light propagation. Therefore, developing suitable interfaces to match these different scenarios represents fundamental research. It allows the implementation of variegated solutions and to exploit all the advantages of Photonics.

Distribution of quantum resources is also at the heart of *quantum key distribution (QKD)* [4], where the no-cloning theorem paves the way to an unconditional degree of security. Quantum Cryptography is the part that arouses the most interest in Quantum Communication, and probably the most important. Also in this case,

sending single photons is the only feasible way to enable unconditionally secure communication between distant parties. Improving the rate and the security of the quantum key is the goal of many research groups. The prepare-and-measure scheme, such as BB84, is currently the best approach to provide the highest rate. However, adding entanglement distribution into the protocol allows for an additional degree of security but implies a reduction of the achievable key rate. The evidence that experimental limitations are the main ruin of QKD, together with the growing demand on a world scale, inspires the QKD investigation in the *urban environment* and testing of different photonic solutions. Moreover, some QKD hacking strategies find their strength in the non-deterministic emission of multiple photons in the standard single-photon sources (SPSs), such as those based on spontaneous parametric down-conversion (SPDC). Hence, the development of deterministic SPSs has fundamental importance, and one promising technology is *quantum dots* [5]. Security can also be improved by using high-dimensional quantum spaces. One of the most promising photonic degrees of freedom to handle such states is *orbital angular momentum (OAM)* [6]. Indeed, OAM naturally encodes quantum states of arbitrary dimension, due to its unbounded nature, and even using a single carrier. Nevertheless, the manipulation and fiber-transmission of such states is not an easy task and requires further investigations.

Different light states can be prepared to probe systems involving one or more unknown parameters. The ultimate limits in estimating such parameters achievable with classical resources can be surpassed by using quantum correlations. These are the results of Photonic Quantum Metrology, where entanglement is the key resource for accessing quantum-enhanced performances [1, 2]. Hence, investigating the theoretical and experimental related open questions, as well as developing quantum sensors able to demonstrate enhancement in estimation, is of paramount importance. The first step is to identify a suitable scenario that works as a testbed for many others. One promising possibility is to study *phase estimation* problems, that can be mapped to a series of physical systems. In the specific case of photonic systems, the best platform for handling optical phases is *multiarm interferometers*. Although it is widely studied in the single-phase case, the multi-parameter counterpart still requires investigations, especially on the experimental side.

In addition to improving specific applications, entangled states are highly interesting in fundamental physics. Indeed they reveal non-local behavior of Quantum Mechanics, which became experimentally demonstrable with Bell's theorem [7]. Bell's test paved the way for a new way for certifying the presence of entanglement, that does not require the exact knowledge of the employed devices. Several photonic experiments have demonstrated in a loophole-free manner the violation of Bell's inequality in the standard scheme. Quantum science is now mature to investigate more complex causal structures, such as those involving multipartite entanglement in quantum networks [8, 9]. This is the case for example of *star-shaped networks*, where different independent nodes are linked to the same central node through independent intermediate parties. Testing and developing generalized Bell-like inequalities in similar scenarios represents the next step in this research direction.

During my thesis work, I investigated scenarios involving several photonic technologies, by achieving experimental results in the field of Quantum Information. In particular, in my contributions advanced photonic platforms have been used to study the fields of Quantum Metrology, Quantum Communication, and Cryptography. I participated in the realization of entangled photon sources, entanglement distribution within complex systems, and the development of quantum photonic sensors and machine learning techniques to improve precision in optical phase estimation

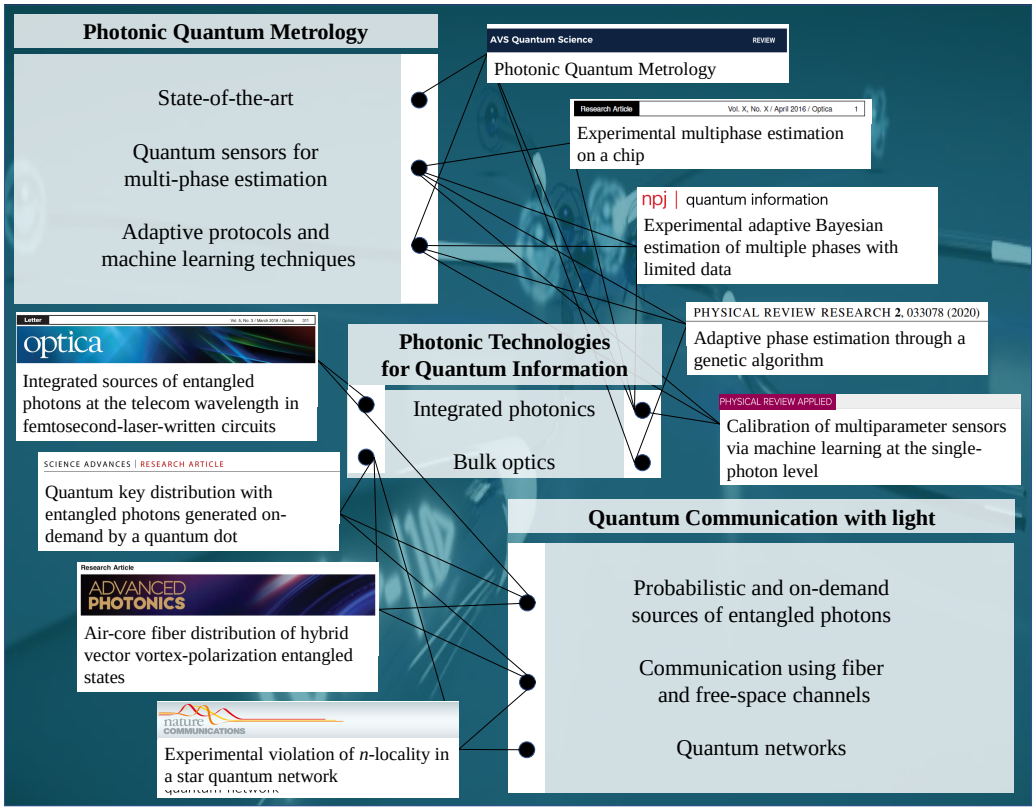

Figure 0.1. Representation of the scientific results achieved during this thesis project. Advanced photonic technologies have been exploited to experimentally investigate the fields of Quantum Communication and Metrology.

problems. Nowadays, photonics technology is highly developed and used for classical communication protocols. Adopting such solutions in the quantum regime is crucial and was the goal of my thesis. In particular, I was concerned with introducing in the quantum regime photonic platforms developed in recent years. This is the case for instance of entangled photons generated by an integrated chip and/or quantum dot, and the adoption of a new fiber, able to support OAM, for applications of Quantum Communication. Then, the exploitation of integrated photonics to realize a multi-arm interferometer capable of efficiently manipulating multiple phases with high stability. A simplified visualization of my thesis work is reported in Fig. 0.1, where the connections between the existing photonic platform and all my scientific results are shown. Then, the description of each contribution is detailed below.

- **Entanglement manipulation.** In the quantum communication framework, entanglement generation and distribution have been studied in different platforms.
  A first work involved the realization of an integrated tunable source of two-photon entangled states in telecom wavelength [10]. The integrated device was realized by the Physics Department of Milan Polytechnic, using the Femtosecond Laser Writing (FLW) technique. This advanced technology allows the realization of photonic chips, by focusing a femtosecond laser in a glass sublayer. Nonlinear effects occur in the beam focus, allowing the realization of waveguides for light.

Further, I participated in the realization of bulk sources of entangled photons in polarization, which have been exploited for different projects. They are based on spontaneous parametric down-conversion (SPDC) process inside bulk crystals: a Sagnac source in polarization and a type-II SPDC source.
Then, during a European collaboration with the Technical University of Denmark (DTU), we demonstrated the possibility to distribute entanglement of high-dimensional hybrid quantum photonic states through an air-core fiber [11].
Finally, I collaborated on entanglement distribution in a more complex scenario, that is a star-shaped quantum network [12]. Here, entanglement was properly distributed and verified within a quantum network between up to four different laboratories, in which five different nodes exploit four independent sources of entangled photon pairs.

- **Quantum Cryptography.** During the last part of my Ph.D. I was involved in the first experimental Ekert-based quantum key distribution protocol using a quantum dot source to generate entangled pairs of single photons [13]. The experiment has been the result of a collaboration with another research group in the Department of Physics. Notably, two photonic quantum channels were employed: a 250m-long fiber link and a 270m-long free-space channel in an urban environment. The latter is a connection between two buildings inside Sapienza University of Rome. Here, I mainly dealt with the free-space optical link, especially planning and implementing the receiver part.

- **Quantum Metrology.** The most important part of my Ph.D. concerns studies in Quantum Metrology.
  In this field, we investigated the photonic state-of-the-art of Quantum Metrology, especially from the experimental point of view, producing the review paper titled "Photonic Quantum Metrology" [1].
  At the same time, we faced the experimental problem of optical phase estimation. On the one hand, we implemented and characterized a quantum sensor capable of handling multiple optical phases. This device is an integrated three-arm interferometer with a high degree of tuning, realized with FLW. Using this device with two-photon input states in a non-adaptive scheme, we demonstrated simultaneous multiparameter estimation of two optical phases with quantum-enhanced performances [14].
  Then, the estimation performances have been experimentally improved in the case of single-photon input, using online adaptive protocols and machine learning techniques [15].
  Further, we investigated the performances that can be achieved by calibrating the quantum sensor using a Neural Network [16].
  As a final contribution to the Metrology studies, I collaborated on the experimental demonstration of a single-phase estimation improved by a genetic algorithm in an offline adaptive scheme [17].

Outline. The thesis is structured as follows: first, the photonic Quantum Information is introduced (Sec. 1), showing its fundamentals, the technologies available to generate and manipulate photonic quantum resources, and the tools capable of certifying them. Then, the broad field of Quantum Communication is discussed (Sec. 2), focusing in particular on Quantum Cryptography and reporting experimental contributions to the field. Finally, the context of Quantum Metrology is introduced using the contents of our review work [1], and then the various experimental demonstrations on phase estimation are presented (Sec. 3).

Chapter 1

Photonic Quantum Information

During the second quantum revolution [18] different platforms have been realized in order to develop quantum technologies. Photons, electrons, trapped atoms, and superconductive materials represent carriers able to encode a quantum state manipulable and measurable [19, 5]. During my Ph.D., the photons are employed as the preferential tool for implementing experimental Quantum Information studies.

In this chapter we introduce the photonic approach to the Quantum Information, by showing its characteristics and abilities to encode qubits and interesting quantum states (Sec. 1.1). Here, particular attention is devoted to the femtosecond laser writing technique for fabricating integrated photonic devices. Then, in Sec. 1.2 the concept of entanglement is introduced, as a fundamental resource of Quantum Information, by showing its foundational interest for Quantum Mechanics studies and how to generate and measure such peculiar property using photonic technologies.

1.1 Photonic quantum technologies

Photons represent one of the most promising physical systems for developing quantum technologies, thanks to different advantageous properties. The versatility in generating single photons (see Sec. 1.2.3), the ability to easily prepare and manipulate quantum states of light with standard optical components, together with the possibility to reveal single photons by suitable single-photon detectors at different working wavelengths, motivate the use of photonics as the basic platform for Quantum Information tasks. Photonic quantum technologies can be realized at different levels, such as bulk optics and integrated photonics. In particular, huge advantages are obtained by integrated photonics, able to realize several optical components on the same device. Such miniaturization allows improving the stability of the optical apparatuses and their complexity. Notably, this has permitted the realization of unprecedented experiments, such as boson sampling [20, 21, 22, 23] and quantum random walks [24, 25, 26], unattainable by standard bulk optics. Moreover, the photons are the more suitable *flying qubits*, enabling the implementation of distant quantum communication. Then, unlike other quantum carriers, their low interaction with the external environment makes the light states less affected by decoherence problems, as well as the easier implementation of multiparticle quantum states encoding non-interactive qubits. These features pave the way to the investigation of more complex frameworks as free-space optical communication or fiber network structures, both in laboratories or into real-world environments, even allowing quantum communication over intra- and inter-cities scales. All these aspects are fundamentals in order to develop a complete and robust quantum technology.

In this section the photonic approach to Quantum Information is introduced. Specifically, in Sec. 1.1.1 and 1.1.2 the definition of quantum bit and the different properties of light to encode quantum states are shown. Then, Sec. 1.1.3 reports some of the current solutions to generate and manipulate photonic quantum states. In particular, the integrated photonics is discussed as a powerful framework to miniaturize quantum schemes, and the advanced femtosecond laser writing technique for fabricating photonic chips is presented.

1.1.1 Quantum bit

The *quantum bit* (or *qubit)* is the building block of the Quantum Information, defined as the state $|\Psi\rangle$ of a 2-dimensional Hilbert space $\mathcal{H}$. It represents the counterpart of the classical bit, but its quantum properties enable non-classical performances. Any qubit can be expressed by an arbitrary basis of the Hilbert space, but the most common are the computational $\{|0\rangle, |1\rangle\}$, the diagonal $\{|+\rangle, |-\rangle\} = \{(|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}\}$ and rotational $\{|L\rangle, |R\rangle\} = \{(|0\rangle + i\,|1\rangle)/\sqrt{2}, (|0\rangle - i\,|1\rangle)/\sqrt{2}\}$. In computational basis any possible qubit reads:

$$|\Psi\rangle = cos(\theta/2)\,|0\rangle + e^{i\phi} sin(\theta/2)\,|1\rangle\,, \tag{1.1}$$

that corresponds to a point of a sphere, the so-called *Bloch-sphere*, having polar coordinates $\theta, \phi \in \mathbb{R}$ and unit radius (Fig. 1.1). These basis are also the eigenvectors of

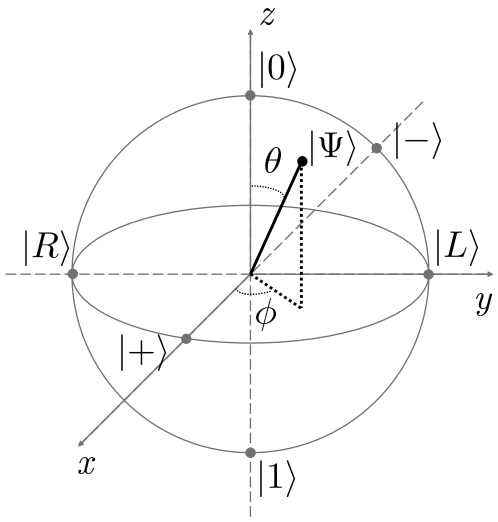

Figure 1.1. Representation of the qubit $|\Psi\rangle$ of Eq. (1.1) in the Bloch sphere. Computational $\{|0\rangle, |1\rangle\}$, diagonal $\{|+\rangle, |-\rangle\} = \{(|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}\}$ and rotational $\{|L\rangle, |R\rangle\} = \{(|0\rangle + i\,|1\rangle)/\sqrt{2}, (|0\rangle - i\,|1\rangle)/\sqrt{2}\}$ bases are the antipodal points of the sphere of unit radius.

the Pauli operators, which expressed in computational basis $\{|0\rangle, |1\rangle\} \equiv \{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\}$ read:

$$\sigma_X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \quad \sigma_Y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} \quad \sigma_Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}. \tag{1.2}$$

Notably, the expectation values of the Pauli observables define exhaustively the point on the Bloch sphere, i.e. the quantum state. Indeed the Cartesian coordinates of a point $\vec{r} = (x, y, z)$ over the Bloch sphere are $x = \langle\Psi|\,\sigma_X\,|\Psi\rangle$, $y = \langle\Psi|\,\sigma_Y\,|\Psi\rangle$, $z = \langle\Psi|\,\sigma_Z\,|\Psi\rangle$. This values describe the system even in presence of mixed states, those defined by $|\vec{r}| < 1$, as each density matrix $\rho = |\Psi\rangle\langle\Psi|$ can be written as $\rho = (\mathbb{1} + \vec{r}\cdot\vec{\sigma})/2$, where $\mathbb{1}$ is the identity operator and $\vec{\sigma} = (\sigma_X, \sigma_Y, \sigma_Z)$. Therefore, it is fundamental to be able to measure Pauli observables in order to fully manipulate and characterize a quantum bit.

1.1.2 Encoding qubits in light properties

The electromagnetic field in quantum regime allows to encode qubits with single photons in various ways, that is using different degrees of freedom of the light [1]. The quantized electromagnetic field has an associated Hamiltonian of a quantum harmonic oscillator, with total energy:

$$H_{\text{em}} = \sum_{\boldsymbol{k}} \hbar\omega_{\vec{k}}(a^\dagger_{\boldsymbol{k}} a_{\boldsymbol{k}} + \frac{1}{2}), \tag{1.3}$$

where $\vec{k}$ is the wave vector, while $\boldsymbol{k}$ represents the electromagnetic mode, that includes wave vector, polarization, frequency, time bin, and in general any degree of freedom of the field. The operators $a_{\boldsymbol{k}}$ and $a^\dagger_{\boldsymbol{k}}$ represent, respectively, the annihilation and creation operators of photons with energy $\hbar\omega_{\vec{k}}$. Such operators obey the following bosonic commutation rules:

$$[a_{\boldsymbol{k_i}}, a_{\boldsymbol{k_j}}] = [a^\dagger_{\boldsymbol{k_i}}, a^\dagger_{\boldsymbol{k_j}}] = 0 \qquad [a_{\boldsymbol{k_i}}, a^\dagger_{\boldsymbol{k_j}}] = \delta_{ij}, \tag{1.4}$$

where $\boldsymbol{k_i}$ and $\boldsymbol{k_j}$ are two modes of the field. The *number operator* $n_{\boldsymbol{k}}$ along mode $\boldsymbol{k}$ is represented by: $n_{\boldsymbol{k}} = a^\dagger_{\boldsymbol{k}} a_{\boldsymbol{k}}$, and the energy can be written as: $H_{\text{em}} = \sum_{\boldsymbol{k}} \hbar\omega_{\vec{k}}(n_{\boldsymbol{k}} + \frac{1}{2})$.

The eigenstates of the Hamiltonian along mode $\boldsymbol{k}$ are the *Fock states*, $|N_{\boldsymbol{k}}\rangle$, having fixed photon-number $N_{\boldsymbol{k}}$, and corresponding energy $E_{N_{\boldsymbol{k}}} = \hbar\omega_{\vec{k}}(N_{\boldsymbol{k}} + \frac{1}{2})$. The action of annihilation (creation) operators on Fock states is to destroy (create) a photon along mode $\boldsymbol{k}$, according to the relations:

$$a_{\boldsymbol{k}} |N_{\boldsymbol{k}}\rangle = \sqrt{N_{\boldsymbol{k}}}\, |N_{\boldsymbol{k}} - 1\rangle \qquad a^\dagger_{\boldsymbol{k}} |N_{\boldsymbol{k}}\rangle = \sqrt{N_{\boldsymbol{k}} + 1}\, |N_{\boldsymbol{k}} + 1\rangle\,. \tag{1.5}$$

The number of photons excited in a particular mode is given by the photon-number operator $n_{\boldsymbol{k}}$:

$$n_{\boldsymbol{k}} |N_{\boldsymbol{k}}\rangle = a^\dagger_{\boldsymbol{k}} a_{\boldsymbol{k}} |N_{\boldsymbol{k}}\rangle = N_{\boldsymbol{k}} |N_{\boldsymbol{k}}\rangle. \tag{1.6}$$

Since the photon-number operators corresponding to different modes are commuting observables [see relations (1.4)], and each acts only on the corresponding mode, it is possible to completely describe the whole radiation field, at fixed number of photons along d modes, by taking the tensor product of the individual states:

$$|\{N_{\boldsymbol{k}}\}\rangle = \prod_{\boldsymbol{k}} |N_{\boldsymbol{k}}\rangle = |N_{\mathbf{k}_1}\rangle |N_{\mathbf{k}_2}\rangle \ldots |N_{\mathbf{k}_d}\rangle \equiv |N_{\mathbf{k}_1} N_{\mathbf{k}_2} \ldots N_{\mathbf{k}_d}\rangle. \tag{1.7}$$

Note that, since in this notation a mode comprises all degrees of freedom, the photons along each single mode $\boldsymbol{k_i}$ $(i = 1, ..., d)$ in Eq. (1.7), are *indistinguishable*.

The state in which the occupation numbers of all modes are 0 is called *vacuum* state $|\{0\}\rangle \equiv |0\rangle$, defined as the state such that $a_{\boldsymbol{k}} |0\rangle = 0 \;\; \forall \boldsymbol{k}$. We can then generate any Fock state from vacuum by iteratively applying creation operators on the modes:

$$|N_{\boldsymbol{k}}\rangle = \frac{a^{\dagger\, N_{\boldsymbol{k}}}_{\boldsymbol{k}}}{\sqrt{N_{\boldsymbol{k}}!}} |0\rangle. \tag{1.8}$$

In conclusion, different degrees of freedom of light can be practically adopted to encode a qubit in a single photon. Path and time of arrival of photons, their frequency, polarization, and orbital angular momentum, represent all favorable choices able two realize a two-level quantum system. Such quantities can be manipulated and measured by means of optical apparatuses, from simple optical elements up to complex interferometers. In order to encode more information, the photonic degrees of freedom can even realize larger Hilbert spaces. A first possibility is considering d photons to create a multipartite system composed of more qubits, thus manipulating d-independent qubit spaces $\mathcal{H}^{(d)}_{\text{tot}} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_d$ having a total dimension 2^d. This approach can be realized also through a hybrid encoding, that is exploiting d different degrees of freedom of the same photon, thus obtaining more qubits on the single carrier. The second possibility is realizing the so-called *qudit*, which is a quantum state living in a d-dimensional Hilbert space. The latter can be conveniently encoded within path and time bin, but one of the most favorable

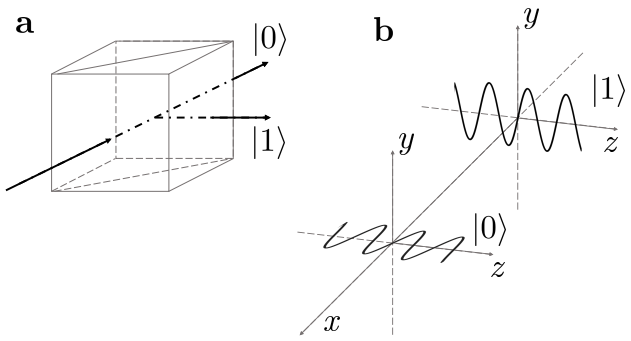

Figure 1.2. Examples of qubit encoding in properties of photons. Elements of the computational basis can be assigned to (a) different paths and/or (b) orthogonal polarizations of light.

choices is represented by the orbital angular momentum (OAM). Indeed, aiming to an infinite-dimensional Hilbert space naturally matches with the unbounded nature of OAM.

Path, polarization, and OAM represent the quantum properties that have been exploited during my Ph.D. and will be discussed in detail in the next sections.

1.1.2.1 Path

The *path* encoding consists in associating two separated spatial directions a_1 and a_2 of a single photon with a qubit: $\{|a_1\rangle, |a_2\rangle\} \equiv \{|0\rangle, |1\rangle\}$ (Fig. 1.2a). Most relevant operators to manipulate the path encoding are beam splitter (BS) and phase shifter (PS), which are unitary operators defined in computational basis as:

$$\mathrm{BS} = \begin{pmatrix} T & R \\ R & T \end{pmatrix} \quad , \quad \mathrm{PS} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}. \tag{1.9}$$

The BS is characterized by a reflectivity (R) and a transmittivity (T), with $R, T \in \mathbb{C}$, while the PS by the phase $\phi \in \mathbb{R}$. Thus, the BS is able to create a superposition of the entering photon over the two output modes, e.g. $|\Psi\rangle_{\mathrm{BS}} = T|a_1\rangle + R|a_2\rangle$. The PS manipulates coherently the relative phase shift ϕ between the two basis modes which encode the path qubit. Notably, using compositions of BS and PS any unitary linear operation in arbitrary dimension is possible [27]. Such decompositions represent the basis for the realization of universal linear optics circuits [28].

1.1.2.2 Angular momentum

Angular momentum of the light can be divided in two contributions, the *spin angular momentum* (SAM), associated to the *polarization*, and *orbital angular momentum* (OAM), associated to the spatial distribution of the beam [29, 30, 31].

Polarization

Exploiting the light polarization, qubits can be encoded by naturally mapping the computational basis into horizontal (H) and vertical (V) polarization of the single photon: $\{|H\rangle, |V\rangle\} \equiv \{|0\rangle, |1\rangle\}$ (Fig. 1.2b). Simple optical components as polarizing-BS (PBS) and waveplates allow the preparation of the Pauli observables,

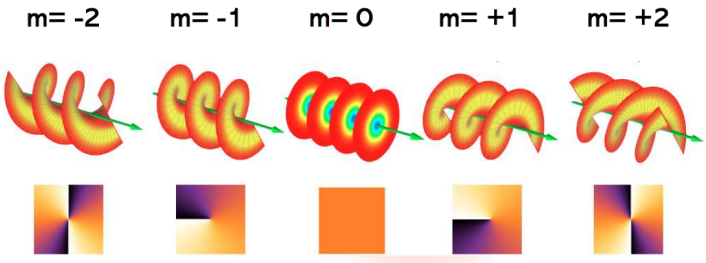

Figure 1.3. Wavefront of light carrying different OAM values. The azimuthal phase of the wavefront depends on the OAM quantum m (bottom). As a result, $m \neq 0$ deforms the wavefront into a helicoidal shape during the light propagation (top).

thus enabling universal quantum computing in polarization. PBS is able to correlate polarization and path, by transmitting H and reflecting V of the entering photon. Half waveplates (HWPs) and quarter waveplates (QWPs) with the optical axis rotated by $\theta = 0°$ respect to V direction, are unitary operators acting as:

$$\mathrm{WP}(0°) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi_r} \end{pmatrix}, \tag{1.10}$$

where $\phi_r = \pi$ for HWP and $\phi_r = \pi/2$ for QWP. A sequence QWP(θ_1)-HWP(θ_2)-QWP(θ_3) can be used to create any possible transformation of polarization state over the Bloch sphere, through a suitable combination of angles $\theta_1, \theta_2, \theta_3$.

Orbital angular momentum

Unlike SAM, OAM of the single photon can assume multiple values of $\hbar$, i.e. discrete quantities $m\hbar$ with the unbounded integer $m = 1, 2, \ldots$ [32]. Therefore, the OAM quanta can be used to encode qubit ($d = 2$) as well as high dimensional qudit ($d \gg 1$) states: $|\Psi\rangle = \Sigma_{m=1}^{d} a_i |m\hbar\rangle$ with $a_i \in \mathbb{C}$. In paraxial approximation, this property can be conveniently described by expressing the solution of Helmholtz equation with the Laguerre-Gauss (LG) modes [33]. Indeed, LG modes depend on two integer indexes, k and p, where $k \equiv m$. Explicitly, the LG modes for describing the propagation of a beam with wavelength λ, in cylindrical coordinates – z along direction of propagation, while radial position r and azimuthal phase ϕ on the traversal plane – read [34]:

$$\mathrm{LG}_{k,p}(r,\phi,z) = A_{k,p}\frac{1}{\omega(z)}\left(\frac{r}{\omega(z)}\right)^{|k|} e^{-\frac{r^2}{\omega^2(z)}} L_p^{|k|}\left(\frac{2r^2}{\omega^2(z)}\right) e^{i\frac{\pi r^2}{\lambda R(z)}} e^{-i(2p+|k|+1)\zeta(z)} e^{ik\phi}, \tag{1.11}$$

where $A_{k,p}$ and $L_p^{|k|}$ are respectively normalization constants and the generalized Laguerre polynomials, with $k, p \in \mathbb{N}$. While the other parameters are standard quantities associated to Gaussian beam [36]: the beam waist $\omega(z)$, the Gouy phase $\zeta(z)$ and the wavefront radius of curvature $R(z)$. Being $k = m$, from Eq. (1.11) it is clear that the OAM quantum is related to the spatial distribution. In particular, $\mathrm{LG}_{k=m,p} \propto e^{im\phi}$: when p is constant, $m \neq 0$ create vortexes in the azimuthal phase ϕ of the wavefront, as depicted in Fig. 1.3. The sign determines the rotational direction, while the value imposes a periodicity of $2\pi/m$ to the wavefront phase. Conversely, different values of p do not change the phase periodicity, but simply add

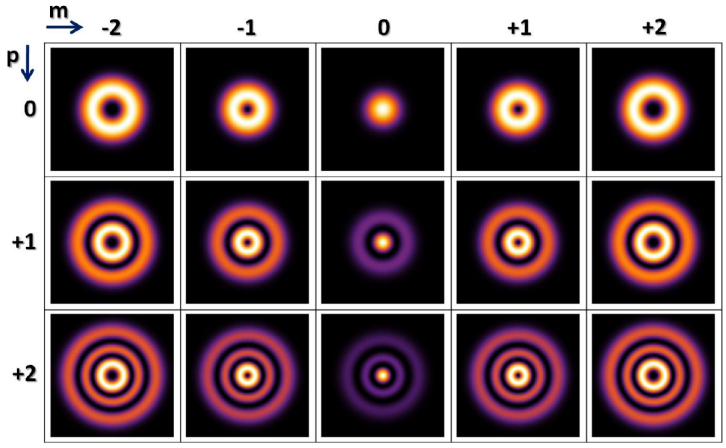

Figure 1.4. Intensity profiles of Laguerre-Gauss modes $LG_{k=m,p}$ as a function of the indexes p and m, defined in Eq. (1.11). This image is taken from [35].

radial nodes to the typical doughnuts shape of $p = 0$ (Fig. 1.4).
In the majority of the experiments, the photonic setups work with photons having zero-OAM, corresponding to the fundamental Gaussian mode TEM_{00} ($\equiv LG_{0,0}$). This choice enables for example the transmission in standard single-mode fibers (SMFs), which allow the propagation of the fundamental eigenmode TEM_{00}. Conversely, light carrying non null-OAM has a more complex profile and SMF are no more suitable for the fiber transmission. Such an example suggests the intuition that OAM property is hard to manipulate due to the difficulty to be coupled and transmitted with standard optical components. It is not a case that a suitable way to measure bidimensional subspaces of OAM is to map the OAM states directly into a polarization measurement, thus facilitating the approach. Components able to manipulate OAM are inhomogeneous anisotropic materials or phase pattern holograms [37, 38, 39, 40, 41, 42, 43], such as Q-Plates and Spatial Light Modulators. In particular, the Q-Plate (QP) [38] is a device composed of a nematic liquid crystal interposed between two glass layers, characterized by an integer topological charge q. The QP has a non-uniform optical axis which rotates around a singularity, with an angular orientation $\alpha(\phi)$ on the transverse plane which depends on the azimuthal phase ϕ. It is described by $\alpha(\phi) = q\phi + \alpha_0$, where α_0 is a constant value computed with respect to the reference axis, i.e. obtained for $\phi = 0$. QP is able to correlate OAM and SAM by shifting of a quantity $|2q|\hbar$ the OAM of a rotating polarization ($|R\rangle$ or $|L\rangle$), based on the polarization value, with the following transformation:

$$\begin{aligned} |L,m\rangle &\xrightarrow{\text{QP}} \cos(\delta/2)|L,m\rangle + ie^{i2(q+\alpha_0)}\sin(\delta/2)|R,m+2q\rangle \\ |R,m\rangle &\xrightarrow{\text{QP}} \cos(\delta/2)|R,m\rangle + ie^{-i2(q+\alpha_0)}\sin(\delta/2)|L,m-2q\rangle, \end{aligned} \tag{1.12}$$

where m is the OAM quantum of the entering photon. The parameter δ is a birefringent retardation due to the liquid crystal and can be tuned electrically through the application of a voltage. Therefore, a QP can partially or completely ($\delta = \pi$) correlate SAM and OAM degrees of freedom, thus providing an useful tool for managing OAM.

During my Ph.D. we exploited a vortex plate, that is a non-tunable Q-Plate, in order to realize a hybrid entangled state encoded in OAM and SAM degrees of freedom, and transmit such state along a special fiber, known as air-core fiber [11]

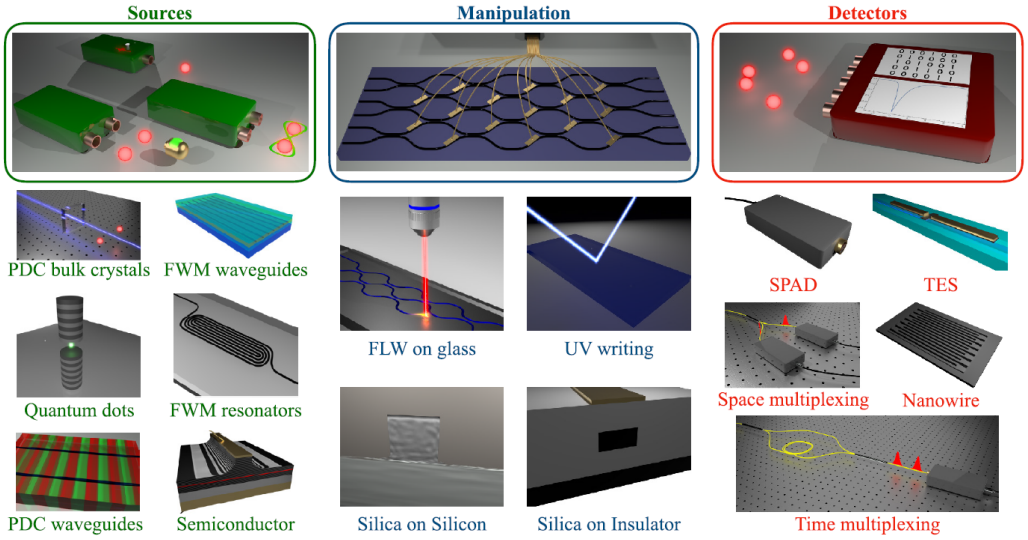

Figure 1.5. State-of-the-art of photonic technologies available for Quantum Information studies developed both in bulk and integrated platforms. Variegate optical platforms are able to generate (left) and manipulate (center) different properties of light in a quantum regime. Detectors have been developed for the revelation of single photons (right). This image is taken from the review [5].

(Sec. 2.3).

1.1.3 Photonic platforms

Despite bulk optics is able to provide full and easy control of the photonic setup, the integration of the components represents the most advantageous as well necessary step, towards the future Quantum Photonics [5, 44, 45, 28, 46, 47]. The miniaturization provides more stability, that is fundamental especially in interferometric setups, reduced costs and compactness, thus realizing a great number of optical elements on the same chip. Notably, thanks to integrated chips unprecedented Quantum Information experiment has been realized, such as boson sampling [20, 21, 22, 23] and quantum random walks [24, 25, 26]. Different techniques can be employed to create integrated chips able to transport and manipulate light [5, 44, 46, 48], such as III-V semiconductors [49, 50, 51, 52, 53], UV writing [54, 55], femtosecond laser writing (FLW) [56, 57, 58, 59, 60], Silica-on-Silicon [61, 62, 63, 64, 65, 66] and Silicon-on-Insulator [61, 67, 68] platforms (Fig. 1.5). Using these techniques it is possible to move many elements of bulk optics to an integrated level. Relevant examples are provided by the directional coupler (the equivalent of the BS), the integrated PSs, and waveplates. The Si-based technologies are probably the most suitable in integrating a large number of elements in path encoding. Indeed, the strong difference in the refraction index between the core waveguide and surrounding cladding allows ultra-small bending radius and very compact structures

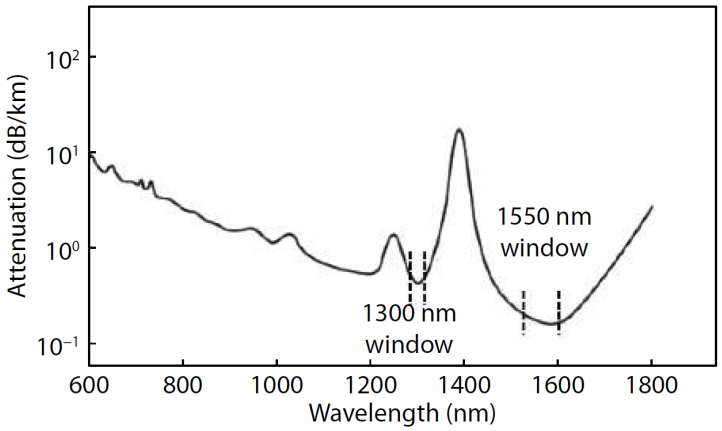

Figure 1.6. Optical fiber losses as a function of the wavelength of the transmitted light. Minimal losses are achieved in the so-called telecom region, that is around 1.3 μm and 1.55 μm.. This image is taken from the review [94].

[69]. However, the same characteristic prevents the integration in such devices of the polarization degree of freedom. Conversely, the FLW is a technology able not only to manage polarization but also to work in 3-dimensional geometry. Otherwise, most other technologies are developed on planar structures, so they can not exploit the third dimension. The goal of the integrated approach for Quantum Photonic is to miniaturize each part of the quantum protocols: generation, manipulation, and detection of quantum resources. Hence, the described technologies have realized efforts for integrate sources of single and entangled photons [70, 71, 72, 73, 74, 75, 76, 10, 77, 78], manipulate them in the described degree of freedom — even OAM [79, 80, 81] and time [82] encoding — up to integrate the single-photon detection [83, 84, 85, 86, 87].

Finally, another fundamental research direction is the study and the developments of quantum fiber networks and free-space channels [88, 89, 90, 91, 3, 92], as they represent the more suitable infrastructure for a worldwide quantum communication [93]. Here, it is important to investigate cases where more distant parties are involved by using different photonic solutions to the Quantum Information protocols, thus testing real-world scenarios. Fiber network represents the most comfortable and versatile approach for relatively short-scale communication, as the metropolitan distribution of quantum resources. The wavelength regime in which fiber distribution is more appropriate for a long-distance task is the telecom band, which is around 1.3 μm and 1.55 μm. Indeed in this regime, the optical fibers show minimal losses (Fig. 1.6), and most of the existing infrastructures for classical fiber communication are realized with such wavelengths.

When dealing with intercity scale, up to international communication, the distance becomes too limiting for fiber communication. The losses allow a reasonable communication with fiber within 100 km. Conversely, free-space channels allow a better scaling with increased distances but still suffer similar limits due to Earth curvature, atmospheric turbulence, and attenuation. For overcoming such distances, the best short-term solution seems to be quantum repeaters [95, 96, 97, 98] and satellite-based quantum communication [99, 100, 101, 102, 103]. The former allows intermediate steps of the quantum signal by using entanglement purification [104, 105], entanglement swapping [106, 107] and quantum memories [108, 109, 110] (Sec. 2.1.1). The latter shows losses which scale only quadratically, compared to the exponentially

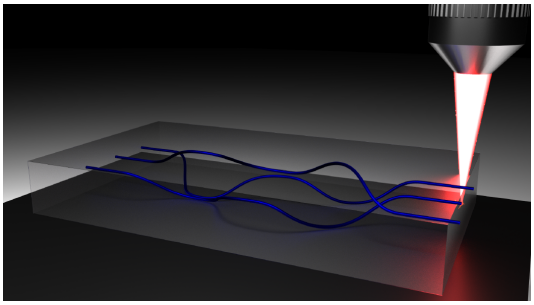

Figure 1.7. Example of femtosecond laser written circuit. The laser beam is focused into the glass substrate and relatively displaced in order to create any three-dimensional structure. This image is taken from [111].

scaling of the fibers, and thus providing possible secure communication over 1000 km.

During my Ph.D. thesis bulk setups and integrated devices based on the FLW technique have been used. The first was exploited for realizing sources of entanglement (Sec. 1.2.3), a Mach-Zehnder interferometer for the phase estimation problem (Sec. 3.3.1) and quantum key distribution in a free-space channel (Sec. 2.5). The second was employed for realizing an integrated source of entangled photons (Sec. 2.2) and an integrated 3-mode Mach-Zehnder interferometer for the estimation of multiple phases (Sec. 3.2). While the bulk solution is made using common optical elements, the integrated technique requires a more detailed explanation.

1.1.3.1 Femtosecond laser writing

Femtosecond laser writing (FLW) is a powerful micromachining technique for the realization of circuits, whose fabrication procedure is based on focusing a strong pulsed laser in femtosecond regime on a substrate of glass [56, 57, 58, 59, 60, 112] (Fig. 1.7). If the pulse energy is lower than the energy gap of the substrate material, in the focus of the radiation the local refractive index is permanently changed through the activation of a series of nonlinear processes. In particular, when the index is increased, translating the sublayer with respect to the focused beam, waveguides for the light are realized, with the same operating principle of the optical fiber. This technology allows the miniaturization of a series of optical devices, both passives and actives, together with the realization of more complex circuits. As previously discussed, the basic elements are directional couplers and phase shifters.

A directional coupler is obtained by approaching two waveguides at a distance of a few micrometers (Fig. 1.8): when propagating light along one waveguide, the evanescent field overlaps the second waveguide, due to the short distance d, thus enabling the tunneling effect towards it. Changing such distance d and the interaction length L the parameters of the integrated-BS [Eq. (1.9)] can be tuned, by controlling the partial overlap between the modes.

The PS can be fabricated for inducing a static relative phase shift between two waveguides or with a reconfigurable structure. The former is realized by means of a mechanical bending of a single waveguide (Fig. 1.9a): the deformation changes the local path of the light and thus the acquired phase during its propagation. The second method is the realization of a reconfigurable PS, controlled by the application of a voltage on a thermo-optics element. More specifically, this element is a resistance which is placed near the circuit and dissipates power, inducing a local variation of the index refraction proportional to the propagation of heat. The optical path

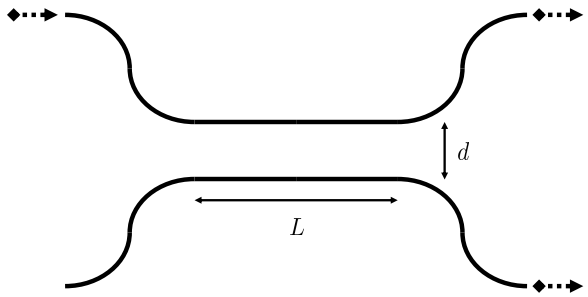

Figure 1.8. Directional coupler is an integrated operator equivalent to the BS. Two waveguides are brought together by a few microns for an interaction length L, having the non-zero probabilities to overlap their modes. This is allowed by the very-low distance d between them, which can be tuned in order to set the BS parameters.

along the surrounding waveguides is changed differently for each waveguide, thus their relative optical phase can be controlled (Fig. 1.9b). Even PBS and waveplates can be integrated by using FLW [113, 114, 115, 116, 117]. In particular, waveplates have been realized by tuning the writing angle of the beam focus to rotate the birefringence axis of the written waveguide [113].

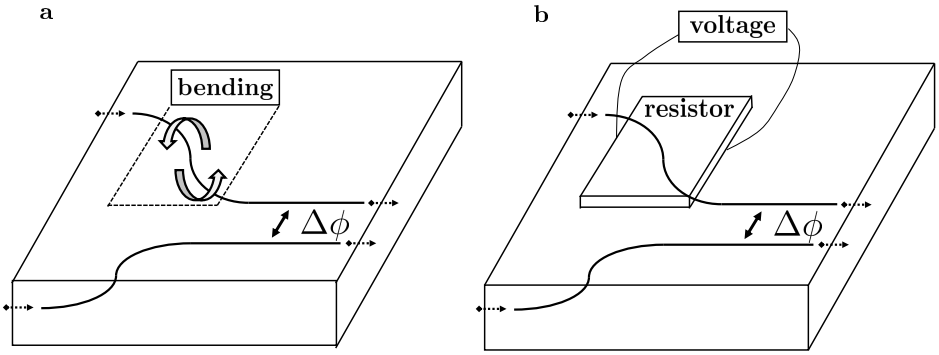

Figure 1.9. Phase shifter operators realized in FLW technique. (a) Static optical phase shift $\Delta\phi$ can be obtained by simply bending the integrated waveguide. (b) An active and reconfigurable phase shifter can be realized by placing an ohmic resistor nearby the waveguide.

Using the FLW technique two different devices have been realized, studied, and employed during my Ph.D.. A first device, composed of three different chips, realizes an integrated source of entangled photons (Sec. 2.2). Then, a second device with a three-arm interferometer structure, suitable for Quantum Metrology studies, was characterized and exploited to manipulate and measure multiple optical phases (Sec. 3.2).

1.2 Photonic Entanglement

Entanglement is the fundamental resource for Quantum Computing, Simulation, and Sensing, at the heart of most Quantum Information and Communication protocols, such as teleportation [118], quantum swapping [119] and repeaters [95]. Indeed, entanglement allows to overcome classical performances in Metrology [2], Cryptography [120] and Computation [121] fields. The capacity to generate, manipulate, and revealing entangled states represents a crucial aspect that any quantum technology has to address. In this context, photonic-based technology represents an optimal solution [5]. As discussed in the previous sections, this is due to the easy manipulation in quantum regime through standard optical elements acting on many degrees of freedom of light. The development of photonic platforms capable of handling entanglement addresses two fundamental experimental aspects. First, the realization of single-photon sources which generate entanglement between photons. Second, the implementation of photonic setups capable of realizing tools for detecting and certifying the presence of entanglement in quantum states of light.

In the following sections we will discuss these topics, by defining entanglement (Sec. 1.2.1) and its peculiarity (Sec. 1.2.2), then providing an overview about how to generate (Sec. 1.2.3) and measure (Sec. 1.2.4) photonic entanglement.

1.2.1 Definition

Entanglement occurs as quantum correlations between the different parties, embedded in the global quantum state of the system, completely described by its density matrix ρ. For example in a 2-qubit system, namely A and B, if the pure quantum state ρ_{AB} can not be separated in the tensorial product of states living on single qubit spaces, respectively ρ_A and ρ_B, then is known as entangled state: $\rho_{AB} \neq \rho_A \otimes \rho_B$. This is the case of the four Bell basis elements, composed by the triplet states

$$|\phi^{\pm}\rangle_{AB} = 1/\sqrt{2}(|00\rangle_{AB} \pm |11\rangle_{AB}),\ |\psi^{+}\rangle_{AB} = 1/\sqrt{2}(|01\rangle_{AB} + |10\rangle_{AB}) \tag{1.13}$$

and the singlet (or EPR-state)

$$|\psi^{-}\rangle_{AB} = 1/\sqrt{2}(|01\rangle_{AB} - |10\rangle_{AB}), \tag{1.14}$$

where we consider $|ij\rangle_{AB} = |i\rangle_A |j\rangle_B$. The generalized definition of bipartite entanglement takes into account possible mixture of states. Here, the general separable state, for any set of $\{\rho_A^i\}$ and $\{\rho_B^i\}$, is:

$$\rho_{AB} = \Sigma_i p_i \rho_A^i \otimes \rho_B^i, \tag{1.15}$$

where each element of the mixture occurs with probability p_i. Hence, general entangled states are defined as the complement of Eq. (1.15): $\rho_{AB}^{\text{ent}} \neq \Sigma_i p_i \rho_A^i \otimes \rho_B^i$.

Analogously, the generalization of an entangled state $\rho^{\text{ent}}_{\{A\}}$ in presence of n-subsystems $\{A_k\}$(with $k = 1, \ldots, n$) is immediate:

$$\rho^{\text{ent}}_{\{A\}} \neq \Sigma_i p_i \rho^i_{A_1} \otimes \rho^i_{A_2} \otimes \cdots \otimes \rho^i_{A_n}, \tag{1.16}$$

where the right term represents the generalization of a separable state.

1.2.2 Bell theorem and non-local causality

Entangled states and their correlations represent one of the most striking quantum effects, that forces a radical departure from a classical vision of the world. These states led Einstein, Podolsky, and Rosen to start a discussion on some critical issues of Quantum Mechanics (EPR paradox [122]). They showed that using entangled states and observing non-commuting observables some contradiction in the assumption simultaneous of reality, locality and completeness in the quantum theory arise. Their conclusion is that Quantum Mechanics must be incomplete, while adding some classical hidden variable to the classical deterministic theory could solve its current incomplete description of physical reality. J. S. Bell introduced its famous theorem [7] for moving the famous EPR debate [122] from a philosophical level to an experimental one. Since 1964, the Bell test have provided an experimental solution to the EPR paradox. Furthermore, to date it is the most used way to detect genuine non-local entanglement inside quantum systems, having the ability to guarantee a device-independent certification. Even in Quantum Cryptography, the violation of Bell inequalities has become the milestone to guarantee an advanced level of security [123].

The Bell scenario is shown in Fig. 1.10. Let us consider a 2-party system, shared between two measurement stations, Alice (A) and Bob (B). Each part can realize two

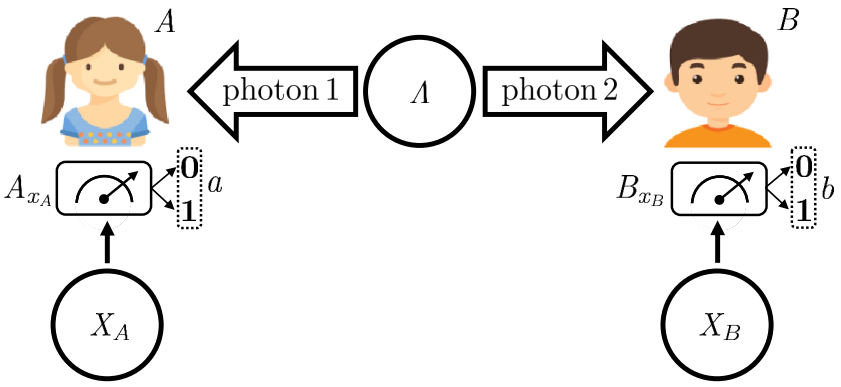

Figure 1.10. Scheme of the Bell test. Two parties, Alice (A) and Bob (B), perform dichotomic measurements (a, b) choosing randomly (x_A, x_B) between two different observables (A_{x_A}, B_{x_B}). During such measurements they can not communicate and/or influence each other, up to some previously locally prepared correlations (Λ).

different dichotomic measurements on its own system. A(B) observes the quantity A_{x_A} (B_{x_B}), choosing it between two different possibilities $x_A \in \{0,1\}$ ($x_B \in \{0,1\}$) and obtaining a result $a \in \{0,1\}$ ($b \in \{0,1\}$). The overall process can be described by the joint probability $p(a,b|x_A,x_B)$, which contains information about correlations between the measurement results of the two observers. In classical physics only local variables can influence the result of the single experiment, that is nonlocal correlations are forbidden. If A and B are space-like separated, the no-signaling principle imposes that they can not communicate, so that no one can directly affect the other, both in terms of measurement choice and measurement result. No nonlocal correlation exists between their experiments unless they are previously locally prepared. Thus, any physical quantity which can correlate the two subsystems is meant as *hidden variable* and is indicated as Λ. Such considerations are summarized by the so-called *local causality* assumption of the conditional probability, concerning the possible measurement results, which factorizes as follows:

$$p(a,b|x_A,x_B,\lambda) = p(a|x_A,\lambda)p(b|x_B,\lambda), \tag{1.17}$$

where λ is the value assigned to Λ. The variable λ is also indicated as *shared randomness*: indeed, for any locally-prepared hidden variables (LHV) theory, it contains any possible information, also unknown, able to predict the correlation between the experiment results of the two parties. Conversely, quantum physics contradicts the local causality assumption, as entangled states allow also non-local correlations: when entanglement is present no factorization of conditional probabilities and no hidden variable can describe exhaustively the overall outcome distribution of the overall system. The first experimental solution to this contradiction between Classical and Quantum Mechanics was provided by the Bell inequalities, which have agreed so far with the Quantum Mechanics in a variety of works [124, 125, 126, 127, 128]. Local causality assumption has a fundamental importance, since not only defines the LHV theories, but it is also sufficient for demonstrating the Bell theorem. Indeed, let us consider the quantity:

$$S = |\langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle|, \tag{1.18}$$

where $\langle A_{x_A}B_{x_B}\rangle$ indicates the expectation value of any possible correlation between A and B. In presence of classical correlations, from Eq. (1.17), it is possible to verify that any set of measures made by A and B must obey to the Bell inequality, which in Clauser-Horne-Shimony-Holt formulation (CHSH, [129]) reads:

$$S_{\text{classical}} \leq 2, \tag{1.19}$$

Conversely, if quantum correlations are present in the 2-qubit state, the bound changes as follows:

$$S_{\text{quantum}} \leq 2\sqrt{2}. \tag{1.20}$$

that is known as *Tsirelson bound* [130]. Comparing Eqs. (1.19) and (1.20), each time measurement results give $S_{\text{exp}} > 2$, a region which only a non-local quantum correlation can achieve is revealed, certifying the presence of entanglement in the quantum state. Each LHV theory must satisfy Eq. (1.19), which is violated by quantum states. In particular, the bound $2\sqrt{2}$ is saturated only by maximally entangled states. This is the case of Bell states in Eqs. (1.13) and (1.14): measuring the subsystem A along the two observables $A_0 = \sigma_X$ and $A_1 = \sigma_Z$, and subsystem B along $B_0 = (\sigma_X + \sigma_Z)/\sqrt{2}$ and $B_1 = -(\sigma_X - \sigma_Z))/\sqrt{2}$, such states provide a maximum degree of entanglement ($S_{\text{Bell}} = 2\sqrt{2}$).

The violation of Eq. (1.19) has been experimentally verified in many works, even including loophole-free scenarios [124, 125, 126, 127, 128], thus demonstrating the incompatibility of Quantum Mechanics with respect to any LHV theory and paved the way to a new approach to certified entanglement. LHV theories that predict completely the quantum results can not exist. Quantum Mechanics is *non-local* and states having $S > 2$ shows non-local correlations. Entanglement is a necessary condition, but not sufficient, for having non-locality. For instance, in the bipartite scenario, pure entangled states are non-local, but entanglement and non-locality do not coincide in presence of mixed entangled states. Such states can be entangled, but not violating any Bell inequality.

Notably, Bell test is said to be *device-independent* (DI). This is because the violation of inequality (1.19) represents the direct certification of entanglement, hypothesizing only the causal structure while having no information about the inner working of the devices employed in the test. Conversely, all other witnesses functions require stricter assumptions (Sec. 1.2.4.3), as the knowledge of the dimension of the relevant Hilbert space [131]. The non-locality of quantum theory is a fundamental aspect concerning a more general property, which makes it deeply different by any LHV model, known as *contextuality*. LHV is a subset of a larger class, called non-contextual hidden variable (NCHV). Non-contextuality is an intuitive classical property for which in each NCHV the expectation values of mutually compatible observables must be independent for both simultaneous and non-simultaneous measurements. However, Quantum Mechanics contradicts this feature, since it shows that results of joint measurement between compatible operators are dependent. This was demonstrated by Kochen, Specker and Bell [132, 133, 134], proving that quantum theory is contextual and non-contextual hidden variables can not explain Quantum Mechanics results. It is possible to demonstrate that non-locality is a special case of contextuality, but the latter, unlike Bell, is state-independent and does not assume space-like separated parties. Moreover, most of the experiments where Bell inequality is violated are made with the lack of space-like separation between the observers, thus demonstrating more precisely the contextuality rather than the non-locality. The entanglement is commonly recognized as the quantum correlation between two dislocated parties, thus allowing the evidence of an unprecedented non-local feature. Despite non-locality is a more interesting quantum feature and it is well-demonstrated considering spatially separable qubits, the contextuality can deal with more general quantum states, for instance, concerning also *single-particle entanglement* [135, 136, 137, 138]. The latter encodes *hybrid entanglement* using different degrees of freedom of the same quantum carrier. Thus, in principle such qubits can not be space-like separated, and strictly speaking non-locality is not demonstrable. In this case, only the contextuality test is a possible certification of a non-classical behavior.

Finally, the generalization to space with a larger number of qubits is possible but still requires additional efforts. Following the same spirit of Bell inequalities, a possibility is computing generalized Bell-like inequalities for more complex scenarios, as the star-shaped network (see Sec. 2.1.2). The generalization to a multi-qubit system is given by considering a set of non-communicating observers $\{A_i\}$, which perform experiments $\{x_{A_i}\}$ with results $\{a_i\}$. In this case the overall process is described by the conditional probabilities $P(a_1, a_2, \ldots | x_{A_1}, x_{A_2}, \ldots)$, which contain the correlations present in the experiment results. Also here, in presence of quantum entanglement within the multiparties system, no LHV model is exhaustive and a global description can be achieved only considering quantum theory. Studying the generalized non-locality and/or contextuality is fundamental in order to exploit

quantum resources in more complex scenarios, composed of any number n of parties, and in particular for building future quantum networks. The certification of n-partite entanglement still requires further investigations and the definition of generalized Bell-like inequalities (see Sec. 2.1.2).

In conclusion, entangled systems can be completely described only assuming the presence of non-classical correlations. Such non-classicality allows entangled states to outperform classical performances in different fields of Quantum Information science, such as Cryptography and Metrology. For instance, in terms of security, when Alice and Bob share an entangled state, since there is no λ to get information about their data, it is not surprising that they can naturally share some secrets. This intuition is the essence of the quantum key distribution, which will be discussed in Sec. 2.1.3.

1.2.3 Generation of photonics entangled state

The realization of *single-photon sources* (SPSs) and the generation of entangled states of light can be achieved in a variety of schemes, using different materials, processes, and geometries. For example, *Spontaneous Parametric Down-Conversion* (SPDC) and *Four-Wave Mixing* (FWM), both in bulk and integrated photonics, microresonators and also deterministic sources, such as *Quantum Dot*-based (QD) scheme, are only some of possible solutions to create single photons [5] to be entangled (Fig. 1.5).

1.2.3.1 Spontaneous parametric down-conversion sources

Among the others, the most common way to generate entangled photons is to exploit the SPDC process inside non-linear material, such as Potassium Titanyl Phosphate KTiOPO4 (KTP), Beta-Barium Borate β-BaB2O4 (BBO), Bismuth triborate BiBO2 (BiBO), and Lithium Niobate LiNbO3 (LN). SPDC occurs when a pump beam impinges a non-linear crystal having $\chi^{(2)} \neq 0$ (non-centrosymmetric) [139, 140]. The unitary transformation of the process is described in second quantization formalism by $U_{\text{SPDC}} = \mathbb{1} + i\gamma a^{\dagger}_{\text{signal}} a^{\dagger}_{\text{idler}} - \gamma^2 (a^{\dagger}_{\text{signal}} a^{\dagger}_{\text{idler}})^2 + \dots$, thus with a probability γ^2 a pump photon is converted into a pair of new photons, signal and idler, respectively with creation operators $a^{\dagger}_{\text{signal}}$ and $a^{\dagger}_{\text{idler}}$, by preserving energy and momentum (*phase matching*) (Fig. 1.11). The global state after the interaction is a squeezed state, with squeezing parameter λ, which reads $|\Psi\rangle_{\text{SPDC}} = \sqrt{1-\lambda^2}\Sigma_{N=0}^{\infty}\lambda^N |N\rangle_{\text{signal}} |N\rangle_{\text{idler}}$. Being $\lambda < 1$, the probability of generating multi-pairs decades exponentially and is commonly negligible. Due to phase-matching condition, only some materials in specific configuration allows SPDC process. Here, different solutions have been found, such as type-0 [141], type-I [142] and type-II [143] layouts in birefringent material. The need of using such materials to satisfy the phase-matching condition represents a first drawback in SPDC. Indeed, the possible materials have not the best nonlinear coefficients. A solution to this problem is represented by the periodically poled approach, that is building a non-linear crystal with alternate ferromagnetic polarization with period Λ (Fig. 1.12a). This technique permits the

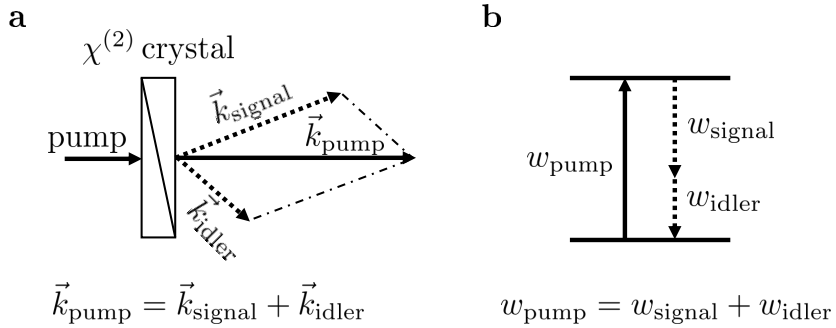

Figure 1.11. Schematic view of SPDC process inside a $\chi^{(2)}$ nonlinear crystal. A photon of the pump beam is converted into new two photons, signal and idler, preserving (a) momentum and (b) energy.

SPDC generation also in non-birefringent crystals, where it would be canceled out by destructive interference. However, the periodic poling allows the compensation of such phenomena and a non-null signal-idler generation. This is known as *quasi-phase matching* as it is artificial and not maximally efficient, but it is advantageous because the employed non-linear coefficient can be definitely high (Fig. 1.12b). Further, this approach enables the generation of SPDC photons collinearly with respect to the pump, which is advantageous in most used schemes.

Exploiting all these opportunities, the signal and idler photons can be differently correlated. Thus, the ability to create such correlations allows to devise entangled states of light, by inserting SPDC process in particular geometries. Most common examples concern setups introduced by Kwiat and coworkers, using a non-collinear type-I [142] and type-II SPDC [143]. The former exploits a pump diagonal-polarized state $|\Psi\rangle_{\text{pump}} = (|H\rangle + |V\rangle)/\sqrt{2}$, which focus on a sequence of two identical BBO crystals having the optical axes perpendicularly oriented (Fig. 1.13a). In this way the generation happens indistinguishably in the first and in the second crystal, providing an entangled state in polarization $|\Psi\rangle_{\text{type-I}} = (|H\rangle_{\text{signal}}|H\rangle_{\text{idler}} + |V\rangle_{\text{signal}}|V\rangle_{\text{idler}})/\sqrt{2}$, along two opposite direction of the phase matching cone [142]. In the latter case, a pump beam with polarization state $|\Psi\rangle_{\text{pump}} = |H\rangle$ focus on a type-II crystal and

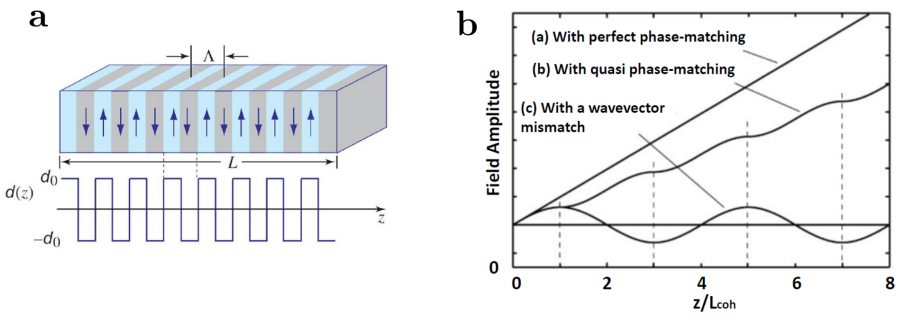

Figure 1.12. The periodically poled crystal can be used as alternative to $\chi^{(2)}$ nonlinear crystal in SPDC process. (a) The structure consist in alternate with periodicity Λ inverted ferromagnetic polarization layers. (b) The efficiency of such approach is lower than using pure nonlinear crystals, but allow to exploit the highest nonlinear coefficients. This image is taken from [36].

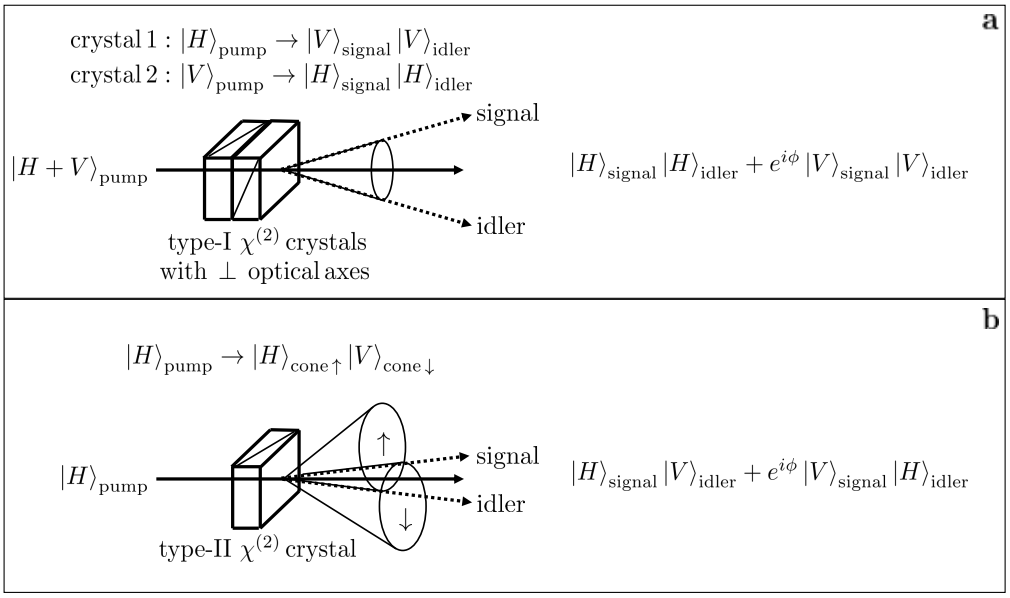

Figure 1.13. Source of entangled photons based on SPDC (a) type-I and (b) type-II.

entangled states in polarization are generated along the intersections of the two phase matching cones (Fig. 1.13b): $|\Psi\rangle_{\text{type-II}} = (|H\rangle_{\text{signal}} |V\rangle_{\text{idler}} + |V\rangle_{\text{signal}} |H\rangle_{\text{idler}})/\sqrt{2}$ [143]. This kind of source has been used in some of our experiments [12, 14, 15, 16]. Then, another possibility is exploiting more complex structures, which not only allow to optimize and improve the generation efficiency and the stability, but also permits encoding entanglement over different degrees of freedom.

This is the case of placing one or two identical non-linear crystals into a *Mach-Zehnder interferometer* (MZI) [10, 144], into a Sagnac interferometer [145, 146, 147], into a *folded sandwich* geometry [148] and also setups of post-selection entanglement [149]. All the discussed solutions can be realized both in bulk optics and integrated photonics. Although the bulk sources have achieved the highest generation record, the integrated approach offers a more attractive future perspective: both in terms of greater stability and scalability, but also its natural compatibility with a possible mass-production. During our experiments we realized and exploited different polarization Sagnac interferometers in bulk, in order to generate polarization entanglement [12, 17] and hybrid entangled state encoded in OAM and polarization [11]. Furthermore, we realized an integrated source of entangled photons in a MZI-based geometry, able to provide entanglement in path or polarization degrees of freedom [10].

1.2.3.2 Quantum dot sources

The non-null generation of multipair events occurs in the SPDC process even if negligible in most applications. It is due to the Poissonian distribution of SPDC generation and can sometimes be a drawback. For instance, this feature becomes relevant in quantum key distribution (see Sec. 2.1.3), allowing unsafe attacks such as beam splitting [150] and number splitting [151]. This limitation can be overcome by employing deterministic single-photon sources, such as colour centers, trapped ions and quantum dots using GaAs, InGaAs, InAsP NW or InAs/GaAs materials.

Quantum-dot based source, currently still working in a quasi-deterministic regime, represents one of the most promising solutions in this direction [152, 153]. QD is realized by electronically or optically exciting a cluster of atoms, from a few hundred to thousands, that is surrounded by a larger semiconductor matrix. The energy gap of the embedded material is typically fewer than the ones of the external matrix, thus confining the potential for electrons (conductive band) and holes (valence band). Further, the confinement has dimensions on the order of the de Broglie wavelength of such charge carriers, thus creating a system of discrete levels (quantized energy). The excitation of the QD can be achieved in various ways, resulting in the fundamental excitonic state X (single electron-hole pair excitation) and other multiparticle states, which decades subsequently emitting single photons in a variety of emission lines. Each generation is distinguishable from the others due to different energy, so that by spectral filtering the single-photon emission is truly deterministic. Among the others, the biexciton state XX (two electron-hole pairs excitation) can be exploited in a biexciton-exciton (XX-X) radiative cascade, in order to create an entangled pair of photons. Therefore, the X emission can be used to realize a single-photon source, while the XX-X cascade is suitable to create on-demand entangled photon pairs [154, 155, 156, 157]. The high quality of single-photon emission is confirmed by autocorrelation measurements $g^{(2)}(\tau = 0)$ via Hanbury Brown and Twiss (HBT) setup [158], which shows the antibunching behavior of the photon statistics (sub-Poissonian light). Indeed, such quantity measures the probability to emit a second photon at the same time of the first one, and an ideal SPS has $g^{(2)}(0) = 0$. The state-of-the-art of QDs are SPSs having an excellent single-photon purity with $g^{(2)} < 0.001$ and the achieved record to date is $g^{(2)}(0) = (7.5 \pm 1.6) \times 10^{-5}$ [159]. Further, the photon generation rate of QD is high thanks to its relatively short radiative lifetime of ~ 1 ns. Then, the experimental advances demonstrated very low decoherence, evaluated in terms of near-perfect indistinguishability [160, 161] between the two consecutive emitted photons, that is measured through the HOM effect (Sec. 1.2.3.3). Finally, the other important factor of a QD source concerns its overall coupling efficiency, which defines its effective brightness depending on various aspects. On the one hand the probability of a single exciting pulse to activate the QD, and the probability of a single QD emission to contain a single photon. Here, excellent results have been achieved for instance in using resonant π-pulse, which provides deterministic excitation [162]. On the other hand the capacity to extract emitted photons from the cavity (β-factor) and to couple it with an external waveguide or a nanophotonic cavity (transfer coupling). Currently the best results are provided by adopting nanostructures, which enable near-unity β-factor [163, 164, 160] and transfer coupling into an optical fiber greater than 80% [165]. Therefore QDs are near-on-demand single-photon sources, which are gradually outperforming the other traditional SPSs, thus representing the future of secure Quantum Communication.

1.2.3.3 Hong-Ou-Mandel effect

A way to generate two-photon entangled states in path is exploiting the quantum interference called the *Hong-Ou-Mandel* effect (HOM), which is attainable in presence of indistinguishable photons. This effect was demonstrated for the first time by Hong, Ou, and Mandel in 1987 [166]. It can occur when two wavepackets interfere in a balanced beam splitter (BS) while entering from different inputs. In the general case, the output state will be a balance superposition of any possible combination of two photons along two output modes, i.e. the terms $|2,0\rangle, |0,2\rangle, |1,1\rangle$, where $|i,j\rangle$ indicate the number $i(j)$ of photons along the output mode 1(2). If their spatio-

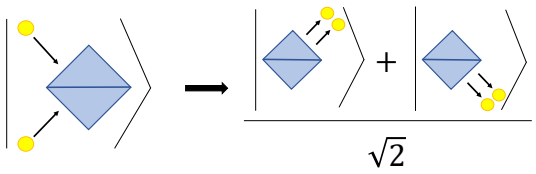

Figure 1.14. Scheme of HOM effect with a symmetric beam splitter. Two indistinguishable photons are injected along the two inputs of a symmetric beam splitter. The final state is a balanced superposition of states in which the two photons are along the same output mode. This image is taken from [1].

temporal superposition is perfect, that is there is no source of distinguishability between them, the output state is reduced to the cases in which they exit from the same output $|\Psi_{\text{out}}\rangle \propto |2,0\rangle + |0,2\rangle$ (Fig. 1.15). This is due to a quantum interference that cancels out the $|1,1\rangle$ terms. Experimentally it is simple to detect this behavior by recording the two-fold coincidence (CC) between the two output arms. Indeed, changing the spatial shift Δx between two identical photons the curve in Fig. 1.15 is typically observed. In presence of perfect HOM, the minimum of CC is zero, realizing the ideal quantum interference. However, this value is impossible to achieve in practical applications for the presence of imperfections in the BS (not ideally balanced) and for the residual degree of distinguishability between the two photons. Therefore, such degree of indistinguishability can be evaluated by considering the HOM visibility:

$$V_{\text{HOM}} = \frac{\max_{\Delta x}(\text{CC}) - \min_{\Delta x}(\text{CC})}{\max_{\Delta x}(\text{CC}) + \min_{\Delta x}(\text{CC})}, \tag{1.21}$$

which is $V_{\text{HOM}} = 1$ in the ideal case of indistinguishable photons impinging an ideal 50:50 beam splitter. The peculiar *dip* of the HOM effect is frequently used for preparing multiphoton quantum states of light and measuring their quality, by providing an upper bound on their indistinguishability. For example, when preparing an entangled state between two degrees of freedom of different photons, unless the properties used for labeling, making the photons identical over all the other properties is the necessary prerequisite.

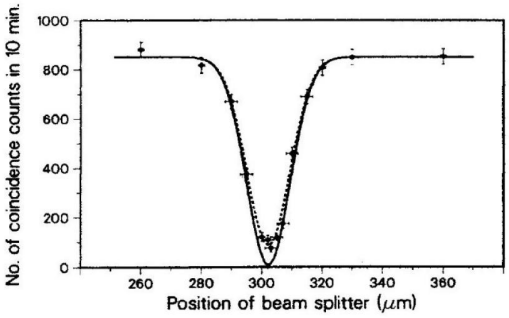

Figure 1.15. When the two photons achieve perfect spatio-temporal overlap, the HOM effect creates a peculiar dip in the number of measured coincidences between the two output modes of the BS. This picture is taken from [166], representing the first observed HOM effect.

1.2.4 Detection of entanglement

The other fundamental aspect, dealing with entanglement in quantum states, is its detection. Here, the Bell test in Sec. 1.2.2 is the most commonly recognized methodology to fully certify the presence of quantum correlations. However, a variety of further tests can be done to estimate the quality of photonic entanglement and more generally for any quantum state of light. Common experimental strategies are represented by entanglement visibility, non-locality and/or contextuality tests, and quantum state tomography. In the following section, we will describe such solutions, in order to provide an exhaustive overview of the tools necessary to experimentally characterize a photonic quantum state and reveal its quantum properties.

1.2.4.1 Density matrix analysis

A first approach to certify a quantum state is provided by testing the population and coherence terms of its density matrix ρ_Ψ. Despite some certification can be realized according to the specific scenario, such as measuring the visibility of the state respect some parameters [10], this approach finds its more general treatment in *quantum state tomography* (QST) [167] and fidelity computation [168]. When we focus on a specific Hilbert space, the experimental procedure which measures the contribution associated with each basis term, i.e. reconstructing the density matrix, is known as tomography. This technique requires a large set of measurements to fully characterize both diagonal and off-diagonal terms of the density matrix. For example in a 2-qubit space, such set corresponds to perform measurements along the three canonical bases, corresponding to Pauli observables: computational (σ_Z), diagonal (σ_X), and circular (σ_Y). Thus, in a N-qubit space this number scales exponentially as 3^N. In the case of large N, approximated versions and machine learning techniques can be used in order to face this problem [169]. In photonic apparatuses, according to the degrees of freedom used to encode the quantum states, different solutions can be employed to measure the matrix terms. For instance the standard setup to characterize the polarization state is made by means of the sequence QWP, HWP and PBS, which is able to realize each Pauli operator. In OAM encoding more general transformation can be realized using computer generated hologram-based devices [37], such as the Spatial Light Modulator [170], while a simple solution is represented by mapping the OAM state in a polarization measure through a suitable Q-Plate [11]. Once measured ρ_Ψ, given a target state ρ_Φ, the fidelity $\mathcal{F}(\rho_\Phi, \rho_\Psi)$ is a quantity able to catch how much the state ρ_Ψ is near to the target. In its general definition, this distance is estimated by [168]

$$\mathcal{F}(\rho_\Phi, \rho_\Psi) = \mathrm{Tr}[(\sqrt{\rho_\Phi}\rho_\Psi\sqrt{\rho_\Phi})^{1/2}]^2. \tag{1.22}$$

Such quantity is bounded between 0 and 1, maximum when $\rho_\Phi \equiv \rho_\Psi$. In the case of pure states, $\rho_\Phi = |\Phi\rangle\langle\Phi|$ and $\rho_\Psi = |\Psi\rangle\langle\Psi|$, Eq. (1.22) simply provides the probability to measure $|\Phi\rangle$ given $|\Psi\rangle$: $\mathcal{F}(\rho_\Phi, \rho_\Psi) = |\langle\Psi|\Phi\rangle|^2 \equiv P(|\Psi\rangle, |\Phi\rangle)$. Further quantifiers of distance between states are given by the *Trace distance* [168]

$$\mathcal{D}(\rho_\Phi, \rho_\Psi) = \frac{1}{2}\mathrm{Tr}[\sqrt{(\rho_\Phi - \rho_\Psi)(\rho_\Phi - \rho_\Psi)^\dagger})] \tag{1.23}$$

and the *Bures distance* [171]

$$\mathcal{D}_B(\rho_\Phi, \rho_\Psi) = \sqrt{1 - \mathcal{F}(\rho_\Phi, \rho_\Psi)}. \tag{1.24}$$

Unlike fidelity, these quantities satisfy also the triangular inequalities and represent metrics on the quantum state. Finally, another relevant parameter directly derived from the tomography is the trace $\mathrm{Tr}[\rho_\Psi^2] \in [0,1]$, called *purity*, which must be unitary for pure states, while lower in presence of decoherence.

1.2.4.2 Hardy test and Mermim inequality

As well the Bell inequalities (Sec. 1.2.2), other tests are able to experimentally demonstrate in a DI manner the inconsistency between any LHV theory and the Quantum Mechanics, such as Hardy test and Mermin inequality. Unlike Bell, such contradiction is demonstrated with logical implications about the allowed conditional probabilities and not considering constraints on correlations.

Let us consider, as in the Bell scenario, two parties, A and B, which can freely perform dichotomic measurements, $\{A_0, A_1\}$ and $\{B_0, B_1\}$, having dichotomic results $\{0,1\}$. For Hardy paradox any LHV theory can not satisfy simultaneously the following statements:

$$p(A_0 = 0, B_1 = 1) = p(A_1 = 1, B_0 = 0) = 0 \tag{1.25}$$
$$p(A_0 = 0, B_0 = 0) > 0 \tag{1.26}$$
$$p(A_1 = 0, B_1 = 0) = 0 \tag{1.27}$$

In particular, the correlations allowed in a LHV model from the conditions (1.25) and (1.27) impose that each event $A_1 = 0$, $B_1 = 0$ can not occur, while violating the (1.26). This logical implication can be simply contradicted by Quantum Mechanics. Indeed, let us consider for instance the state $|\Psi\rangle_{\mathrm{AB}} = (\sin\theta\,|1\rangle_{\mathrm{A}}\,|1\rangle_{\mathrm{B}} + \cos\theta(|1\rangle_{\mathrm{A}}\,|0\rangle_{\mathrm{B}} + |0\rangle_{\mathrm{A}}\,|1\rangle_{\mathrm{B}}))/\sqrt{1+\cos^2(\theta)}$ with $\theta \in (0, \pi/2)$. Then, if A_0 and B_0 correspond to measure on computational basis, while A_1 and B_1 measure on basis $\{\sin\theta\,|0\rangle - \cos\theta\,|1\rangle\,, \cos\theta\,|0\rangle + \sin\theta\,|1\rangle\}$, it is immediate to verified that $p(A_0 = 0,\ B_0 = 0) \neq 0$. A connection between Hardy and Bell paradoxes can be found [172]. In order to bring Hardy argument to an experimental test, is it possible to derive the following inequality from the Hardy conditions [173]:

$$P(A_0 = 0, B_0 = 0) - P(A_0 = 0, B_1 = 1) - P(A_1 = 1, B_0 = 0) - P(A_1 = 0, B_1 = 0) \leq 0, \tag{1.28}$$

which violated by quantum correlations demonstrates the inconsistency of any LHV-based model.

When entanglement involves more than two parties, or even more than two qubits due to hybrid encoding, Eq. (1.20) and Eq. (1.28) could no more fully capture the presence of non-classical behavior. In the case of a tripartite scenario with parties A,B and C, the Mermin test represents a possible solution. Let us consider each part can perform two different measurements having dichotomic results: $\{A_0, A_1\}$, $\{B_0, B_1\}$ and $\{C_0, C_1\}$ for A,B and C, respectively. Further, the causal structure prevents the communication between all parties simultaneously. Conversely, the direct influence between two parties is allowed. In such scenario the Mermin-Ardehali-Belinsky-Klyshko inequality [174, 175, 176] can be used, which reads:

$$\begin{aligned} \mathcal{M} \quad \equiv \quad & |\,\langle A_0 B_1 C_1\rangle + \langle A_1 B_0 C_1\rangle + \\ & + \langle A_1 B_1 C_0\rangle - \langle A_0 B_0 C_0\rangle\,| \leq 2\,. \end{aligned} \tag{1.29}$$

The violation of this inequality guarantees the presence of non-classical correlations, i.e., contextual behavior, ruling out any possible non-contextual LHV model.

Furthermore, if the bound of $2\sqrt{2}$ is overcome, even the presence of genuine multipartite entanglement is certified. The latter occurs when the state is not biseparable, i.e. cannot be separated with respect to some partition [177]. In our 3-qubit space, the non-biseparable state ρ_{ABC} reads:

$$\rho_{\mathrm{ABC}} \neq \Sigma_k(\gamma_A^{(k)}\rho_{\mathrm{BC}}^{(k)} \otimes \rho_A^{(k)} + \gamma_B^{(k)}\rho_{\mathrm{AC}}^{(k)} \otimes \rho_B^{(k)} + \gamma_{\mathrm{C}}^{(k)}\rho_{AB}^{(k)} \otimes \rho_{\mathrm{C}}^{(k)}) \tag{1.30}$$

for any set of 1-qubit states $\{\rho_A^{(k)}\}$, $\{\rho_B^{(k)}\}$, $\{\rho_{\mathrm{C}}^{(k)}\}$, 2-qubit states $\{\rho_{AB}^{(k)}\}$, $\{\rho_{\mathrm{BC}}^{(k)}\}$, $\{\rho_{\mathrm{AC}}^{(k)}\}$ and probabilities $\{\gamma_A^{(k)}\}$, $\{\gamma_B^{(k)}\}$, $\{\gamma_{\mathrm{C}}^{(k)}\}$. Therefore, if $\mathcal{M} > 2\sqrt{2}$ in Eq. (1.29) is measured, no bipartite separation is allowed and genuine tripartite entanglement is certified. This is the case of *Greenberger-Horne-Zeilinger* (GHZ) state [178] which is able to provide maximal violation of (1.29), that is $\mathcal{M}_{\mathrm{GHZ}} = 4$ [179].

1.2.4.3 Entanglement Measures and Witness

When the task is directly revealing or even quantifying the presence of entanglement in a quantum state ρ, different tools are available, commonly known as entanglement measures $E(\rho)$. *Entanglement monotones* are entanglement quantifiers $E(\rho)$ which satisfy general properties [180, 181], such as:

- $E(\rho_{\mathrm{sep}}) = 0$ if ρ_{sep} is separable.
- $E(\rho)$ is convex: $E(\rho) = \Sigma_i p_i E(\rho_i)$ if $\rho = \Sigma_i p_i \rho_i$.
- $E(\rho)$ does not increase under *local operations and classical communication* (LOCC) U^{LOCC}: $E(U^{\mathrm{LOCC}}\rho) \leq E(\rho)$.
- Given two entangled systems A and B, $E(\rho_{AB})$ is invariant under local unitary transformation $U_A \otimes U_B$: $E(\rho_{AB}) = E(U_A \otimes U_B \rho_{AB} U_A^\dagger \otimes U_B^\dagger)$.

In the bipartite scenario, one of the most adopted monotone $E(\rho)$ is the *concurrence*, defined as:

$$\mathcal{C}(\rho) = \max(0, 1 - v1 - v2 - v3 - v4), \tag{1.31}$$

where v_i $(i = 1, 2, 3, 4)$ are the eigenvalues of matrix $[\sqrt{\rho}(\sigma_Y \otimes \sigma_Y)\rho^\dagger(\sigma_Y \otimes \sigma_Y)\sqrt{\rho}]^{1/2}$. In the case of a pure state $|\Phi\rangle$ the Eq. (1.31) becomes $\mathcal{C}(|\Phi\rangle\langle\Phi|) = [2(1-\mathrm{Tr}(\rho_{\mathrm{red}}))]^{1/2}$, where ρ_{red} is the reduced density matrix of one of the two subspaces.

$E(\rho)$ generally requires the knowledge of ρ. However, as previously discussed, depending on the Hilbert space the QST can be hard to be computed (see Sec. 1.2.4.1). If the task is only certifying the presence of quantum correlations, an advantageous approach is represented by *entanglement witnesses* functions $\mathcal{W}$. These functions can be different observables, able to recognize the presence of entanglement without needing the full state tomography. In particular, an observable of the state ρ is witness of entanglement if its expectation value $\langle\mathcal{W}\rangle = \mathrm{Tr}[\rho\mathcal{W}]$ can distinguish at least a subset of entangled states from the entire class of separable states, that is:

- $\mathrm{Tr}[\rho_{\mathrm{sep}}\mathcal{W}] \geq 0$ if ρ_{sep} is separable.
- $\mathrm{Tr}[\rho_{\mathrm{ent}}\mathcal{W}] < 0$ for at least a subset of entangled states $\{\rho_{\mathrm{ent}}\}$.

Therefore, for a given $\mathcal{W}$ not all the entangled states can be distinguished from the separable class. On the contrary, for each entangled state we can define a witness $\mathcal{W}$ able to certify the presence of entanglement (Hahn-Banach theorem [180]). Unlike Bell inequalities, in general the entangled witnesses are not device-independent but can require more assumptions like the validity of the quantum theory to work correctly. In particular, a witness function suitable for the Bell state $|\phi^-\rangle$ [Eq. (1.13)] is provided by $\mathcal{W}_{\phi^-} = 1 - S_{\phi^-}$, where $S_{\phi^-} = \Sigma_{i=X,Y,Z}|\langle\sigma_i \otimes \sigma_i\rangle|$.

1.3 Final remarks

Photonics represents a convenient field to encode and manipulate quantum states, and realize quantum information protocols.
First, it is possible to encode the quantum state into different degrees of freedom of light, such as path, polarization, and orbital angular momentum. This capability makes it possible to choose the most suitable one for the specific task.
Then, photonic technology offers several solutions, such as bulk optics and integrated photonics to realize optical setups, or free-space and fiber links to distribute light between distant parties. Using such devices, it is possible to generate and manipulate optical quantum resources, e.g. entanglement, with different schemes. For instance, the main probabilistic sources of entangled photons are based on placing nonlinear crystals within interferometric structures. On-demand single-photon sources, such as those based on quantum dot devices, can also be realized. Then, the availability of single-photon detectors allows for the revelation of light in the quantum regime.
Finally, different methodologies exist to measure the quantum state of light and in particular to reveal the presence of quantum correlation inside it. This is the case of quantum state tomography, visibility, or witness of entanglement, while the most commonly recognized one is Bell's inequality violation. The latter allows for the revelation of the non-local behavior of Quantum Mechanics and a device-independent certification of entanglement.

Chapter 2

Distribution of optical entanglement

Quantum entanglement lies at the heart of most protocol of Quantum Information theory, bringing the highest advantages such as the estimation enhancement in Quantum Metrology [1], enabling teleportation in Quantum Communication protocols [3] and improving the unconditional security in quantum key distribution (QKD) [182, 4]. Therefore, manipulation and distribution of entanglement are as fundamental as its generation, representing the basis of Quantum Communication. Quantum entanglement embedded in photonic states can be accessible by using different platforms and degrees of freedom, providing a large variety of possibilities (Sec. 1.1). The ultimate challenge is the possibility to bring photonic quantum communication on a real-world scale, up to an intercontinental scale as revealed by recent demonstrations [93, 99, 101]. Here, basic elements are represented by quantum teleportation and entanglement swapping protocols, quantum relays, quantum memories, and repeaters [3]. These possibilities integrated with fiber systems and free-space channels inside always more complex quantum network implementations, can realize the suitable infrastructures for intra-city and inter-cities quantum communication, up to covering intercontinental distances [93]. Using satellite-based quantum technologies the entanglement resource has been distributed over 1000 km [183, 99], even opening the possibility to unprecedented quantum physics experiments. The workhorse is doubtless the Quantum Cryptography, which has been attracting many companies because of the improved communication security. Notably, it has been used by banks and governments, and the first telecommunication by using QKD was realized between Austria and China [100]. Therefore, the distribution of optical entanglement in all its meanings, applications, and advantages in the fields, represents one of the main topics of Quantum Communication. The investigation of such solutions, interfacing photonic technologies at different levels and using quantum states encoded by various photonic degrees of freedom is one of the aims of this thesis.

My thesis work has provided different contributions in this context. In this chapter, after a brief introduction on Quantum Communication (Sec. 2.1), my contributions in the fields are reported. On the one hand, the generation of useful entanglement has been demonstrated using SPDC both in bulk and integrated platforms, and even exploiting a quantum dot. In particular, the integrated source [10] of entangled photons at telecom wavelength, composed of three cascaded chips realized through FLW, turned out to be a novelty in the field: different output states in the path and polarization degrees of freedom are generated by using a

modular and hybrid approach, together with a reconfigurable PS (Sec. 2.2). On the other hand, the generated entangled states of light have been manipulated and distributed in different scenarios. In [11], a hybrid entangled state involving OAM and polarization of photons has been firstly generated and then fiber-distributed, by exploiting the special air-core fiber (Sec. 2.3). In [12] a star-shaped quantum network has been realized and the distribution of multipartite entanglement in polarization inside the network has been demonstrated (Sec. 2.4). Finally, an Ekert91-based QKD protocol has been realized [13] by distributing maximally entangled singlet states in polarization, that were generated using a quantum dot source. Those states have been sent by air in a 270 m long free-space quantum channel, connecting two distant buildings, for realizing the QKD experiment. The same experiment has been replicated using a fiber quantum channel of similar length (Sec. 2.5). In the following sections, all these experiments are presented in-depth.

2.1 Quantum Communication

Quantum Communication is the art to communicate by using quantum technologies and protocols. Here, the most relevant part is represented by Quantum Cryptography, i.e. the ability to make the communication between different parties secure by exploiting quantum resources. More generally, Quantum Communication is a large research field, which comprises other scopes, such as the fascinating quantum teleportation, the study of increasingly complex quantum networks, quantum internet, together with the investigation of ways to enlarge the achievable distance in the distribution of quantum resources, such as entanglement swapping, quantum repeaters, and memories. In the following sections, all the basic elements concerning the large field of Quantum Communication are introduced. In Sec. 2.1.1 various ways of distributing quantum resources and entanglement are presented. Then, particular attention is devoted to the study of entanglement distribution in quantum networks by means of DAG formalism (Sec. 2.1.2). Finally, in Sec. 2.1.3 the quantum key distribution is widely discussed.

2.1.1 Communication with quantum channels

Protocols of Quantum Information seem to achieve unbelievable performances with respect to their classical counterparts. This is due to the exploitation of unique resources deriving from quantum theory, such as superposition and entanglement. The adoption of these resources for a real quantum communication scenario requires necessarily infrastructures able to distribute quantum states without loss of quantum properties, thus permitting the right realization of each quantum protocol. Therefore the study of quantum channels and more in general of quantum networks is a fundamental step in order to make future communications with a quantum approach.

The simplest quantum communication scenario concerns the transmission of information between two parties, Alice (A) and Bob (B), exploiting a channel able to preserve one (or more) quantum state(s), namely a *quantum channel* (Fig. 2.1a). The more general version also includes the presence of classical communication (Fig. 2.1c), which can be done by appropriate classical channels between A and B (Fig. 2.1b). The main problems of a quantum channel are related to the loss of quantum properties during the propagation of the state along the channel. These losses are divided into *decoherence* and *amplitude losses*. The first reduces the purity of the quantum state, while the second attenuates the probability that the signal will arrive at the receiver part. Using photon heralding-based protocols is possible to control the effects of fidelity attenuation. Conversely, the reduction of the transmission rate is not reversible. In order to minimize losses in a given photonic-based architecture it is necessary to exploit characteristics of light that optimally match such architecture. Here, telecom wavelengths are ideal for fiber distribution, while infrared light offers a better single-photon detection efficiency and it is suitable for free-space channels (Sec. 1.1.3). On the other hand, the right choice of the degree of freedom to use for encoding quantum states has paramount importance: for instance, high dimensional

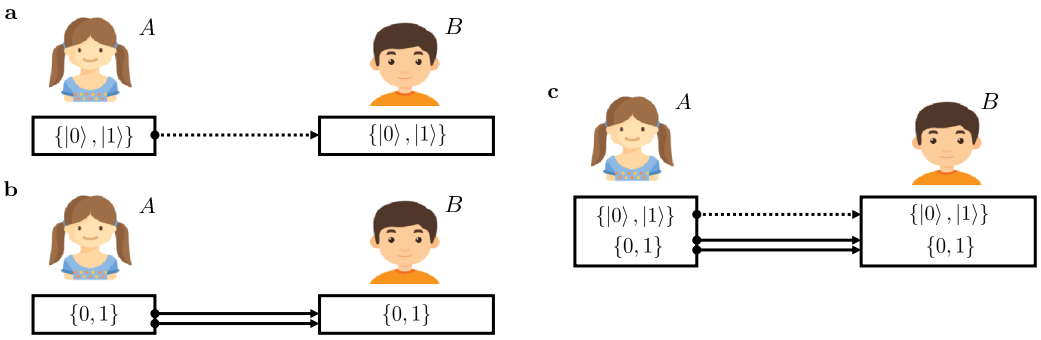

Figure 2.1. Schemes of the communication channel between two parties, from Alice (A) to Bob (B). (a) A quantum channel is able to transmit quantum information, e.g. a qubit, without losing the quantum state prepared by Alice. (b) A classical channel enables the communication of information encoded through classical bits. (c) The more general scheme of the communication channel provides both quantum and classical transmission of information. In all panels, the dashed (double solid) lines represent quantum (classical) channels.

Quantum Information well suits OAM in free-space [6]; time encoding is one of the most frequently used in Quantum Communication and Cryptography schemes [6]; while polarization and path often represent optimal choices in fiber and integrated devices [5].

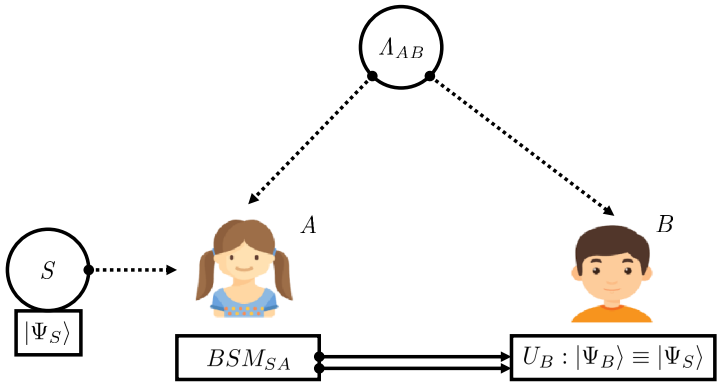

Figure 2.2. Quantum teleportation protocol. A source (Λ_{AB}) distributes bipartite entanglement between Alice and Bob. Arbitrary qubit $|\Psi_S\rangle$ can be transmitted from Alice to Bob without being directly sent to Bob. The protocol requires a BSM measure of Alice between her state and $|\Psi_S\rangle$. The result is sent with a classical channel to Bob, who is able to retrieve the state $|\Psi_S\rangle$ by applying a suitable operator U_B on his state.

The most important Quantum Communication protocols which involve bipartite communication are QKD (Sec. 2.1.3) and *quantum teleportation*. The latter concerns the possibility to transmit any single-qubit quantum state $|\Psi_S\rangle$ from A to B, without sending directly the state along a quantum channel [184] (Fig. 2.2). More specifically, first a bipartite entangled state $|\Psi_{AB}\rangle$ is shared between A and B using a quantum channel. Notably, after this step, the quantum channel could be in principle removed. Then, A performs a Bell-state measurement (BSM) between the subsystem S of the interested state and its own system [185]. Using a classical channel, A tells B her

result, so that B understands what unitary operation to perform on his apparatus in order to retrieve the state $|\Psi_S\rangle$, such that $|\Psi_B\rangle \equiv |\Psi_S\rangle$. Quantum teleportation is one of the most fascinating protocols of quantum science, having no classical counterpart. The most critical point is represented by the BSM [3]. For example, in linear optics, no way exists to perform a complete BSM with efficiency greater than 50% [186]. Quantum teleportation not only represents a fundamental scheme for conceptual comprehension of Quantum Information but also created the basis for many developments of the quantum theory, such as quantum swapping and repeaters, measured-based quantum computing, quantum gate, and port-based teleportation [187].

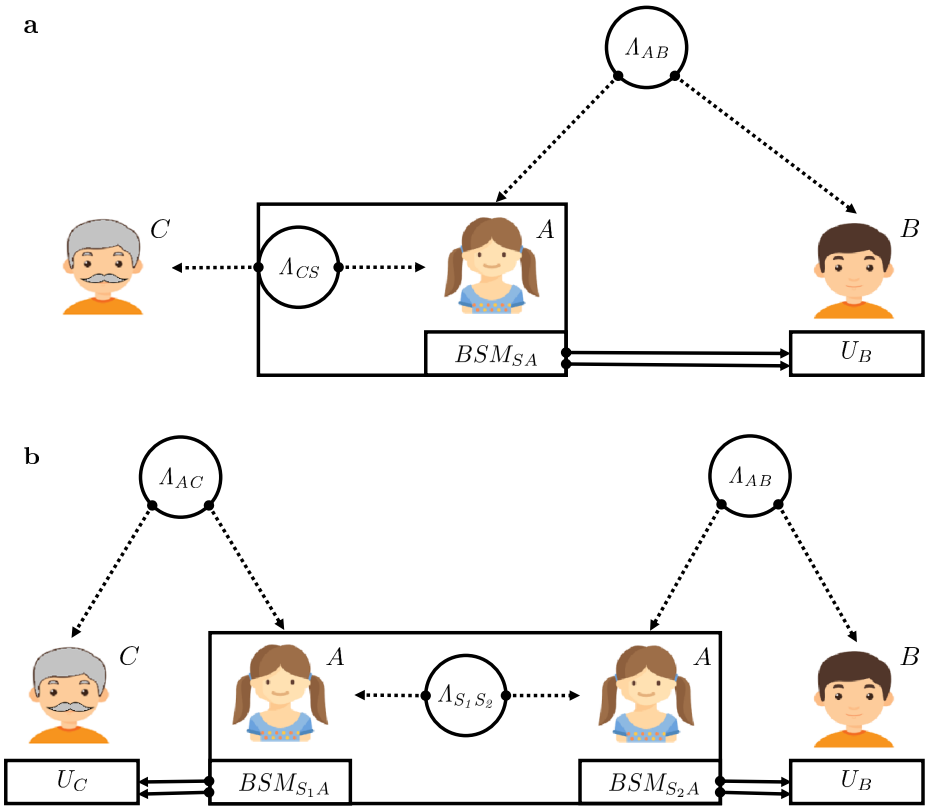

Figure 2.3. Quantum swapping protocol and quantum relay scheme. (a) An entanglement swapping is realized between two parties, Charlie and Bob, that do not communicate directly. Alice prepares an entangled state between the qubits C and S (Λ_{CS}). Then, she sends the qubit C to Charlie and teleports the qubit S to Bob exploiting a further entangled state shared with him (Λ_{AB}). (b) In a quantum relay, Alice first prepares an entangled state between the qubits S_1 and S_2 ($\Lambda_{S_1S_2}$). Then, she performs an entanglement swapping of both the subsystems towards Charlie and Bob. In this way, the initial entangled state can be totally teleported between two distant parties which never directly interacted.

Let us consider now quantum teleportation in a tripartite scenario, in which A can communicate with two independent nodes, B and C. A prepares an entangled pair of photons, in order to send one photon to B and one photon to C. He can teleport the photon to B realizing the so-called *entanglement swapping* between the photon owned by C and the photon received by B (Fig. 2.3a). Notably, although

the two photons of B and C have never interacted, they realize an entangled state. If the photon towards C is also teleported (Fig. 2.3b), then it is exactly the entanglement that is teleported between two parties, realizing a *quantum relay* [106, 107]. Exploiting quantum relays it is possible sometimes to attenuate some drawbacks due to single-photon detector dark-counts [3]. However, quantum relays can not improve the distance and rate in QKD, since it depends on the probability of losing the entangled photons along the two quantum channels. This probability is substantially equal to the case in which entanglement is established directly between the external nodes using a single quantum channel [3].

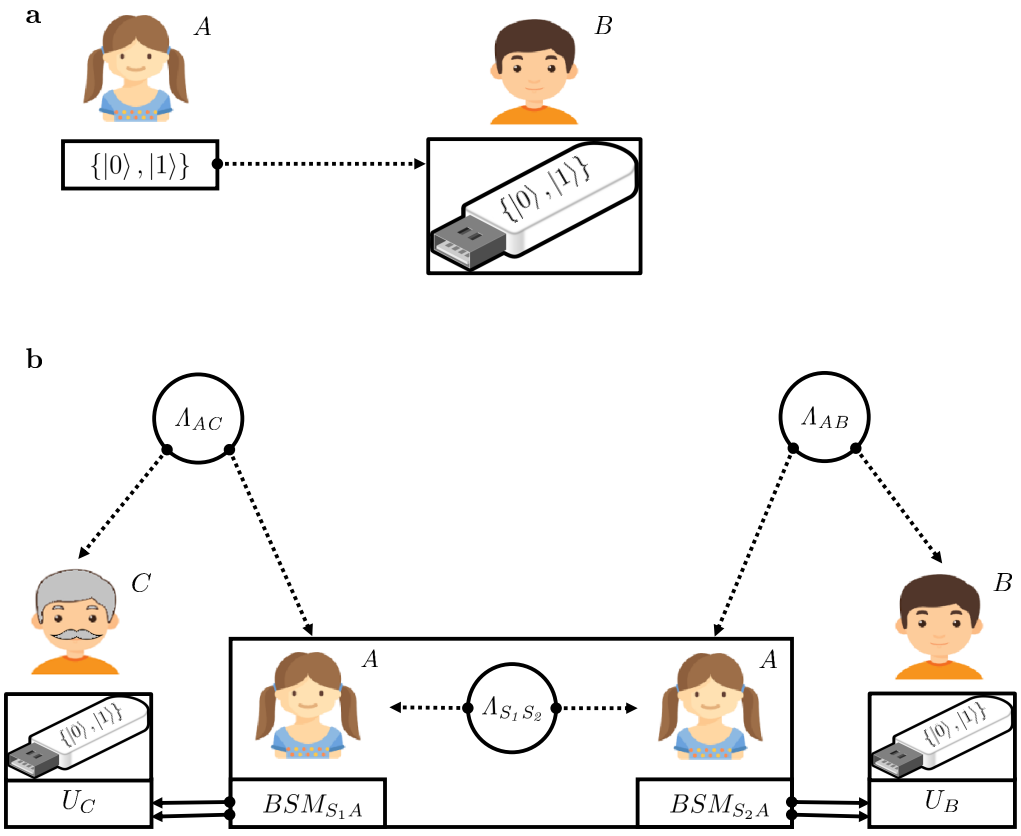

Figure 2.4. Quantum memory and repeater. (a) A device able to store quantum information sent from Alice to Bob for a sufficient period of time is called quantum memory. (b) Exploiting quantum memories in the quantum relay protocol enables an efficient quantum communication between Bob and Charlie, realizing a so-called quantum repeater.

Currently, the only way to improve the distance using a chain of different quantum channels without losing rate, is the exploitation of *quantum repeaters* [95]. The working principle of a quantum repeater is based on exploiting quantum relays and *quantum memories* [96]. The latter are physical quantum systems able to store quantum information, for instance a qubit, for a *sufficient* period of time (Fig. 2.4a). In the case of Quantum Communication protocols, several milliseconds of storing are typically required. A quantum memory should also have other properties: the capability to reveal if it has been loaded, e.g. through a heralding mechanism; or the ability to efficiently release the encoded information into photons suitable

for communication tasks, e.g. having favorable wavelengths. Several proposals exist for realizing quantum memories, such as fiber-loops, atomic ensembles and vapours, rare-hearts ions, Nitrogen-vacancy centers in diamonds and polarization of photon-atom systems [3]. The standard scheme of a quantum repeater is similar to the swapping one, but having the availability of quantum memories in the final nodes (Fig. 2.4b). When A tries to establish an entangled state with B and C separately, if one of the two fails, the other can be recorded in the quantum memory until the first retrying succeeds. Thus, considering the losses in both channels is no more necessary and an improvement with respect to the direct single-channel entanglement distribution arises. It is not a case that realization and study on quantum repeaters is one of the most interesting challenges of the modern epoch [3]. When more than two parties want to communicate using quantum resources, the natural generalization is the development of a network of quantum channels. The *quantum network* can in principle have any structure and shape, allowing direct links between each part or only some of them. Such structures naturally show more complex characterization and problems, and the distribution of quantum resources across them is anything but obvious. One of the theories able to study network scenarios is the graph theory, which is introduced in Sec. 2.1.2.

In this context, we demonstrated the distribution of hybrid entanglement through a fiber system [11]. Here, the quantum state has been encoded in polarization and OAM degrees of freedom, requiring a special fiber to be transmitted, namely the air-core fiber (see Sec. 2.3). Then, in a second work [12] we demonstrated the realization of a quantum network with 5 nodes — 1 central and 4 peripheral nodes — which share four independent entangled states. In this case, we certificated the successful distribution of multiparties entanglement through generalized Bell inequalities (see Sec. 2.4).

2.1.2 Directed acyclic graphs for quantum networks

Studying a given physical system made in terms of the causal structures represents a very useful way to approach the general comprehension of the correlations present within the system. Casual structures can be easily visualized using *directed acyclic graphs* (DAGs), which contain the essence of Bayesian networks. Examples of DAGs are reported in Figure 2.5. A DAG is an ensemble of nodes (or vertices) and directed edges (or arrows) between them, in which no cycles are allowed (Fig. 2.5d). The correspondence with physical systems is given by considering nodes as random variables and arrows as the causal influence of one variable to another. The variables are relevant parameters of the structure, whose values are associated with certain probability distributions. They can be latent or known variables, such as measurement choices or results, and so on. Also noise can be considered as a node but it is often omitted as usually it is latent and does not produce correlations between relevant variables. The causal influence (arrow) can be represented mathematically by conditional probability $P(X_j|X_i)$, indicating the possible influence of a certain variable X_i to a variable X_j. The requirement of having no cycles allows preserving the physical causal order, so avoiding retro-causal influences. Using this formalism is

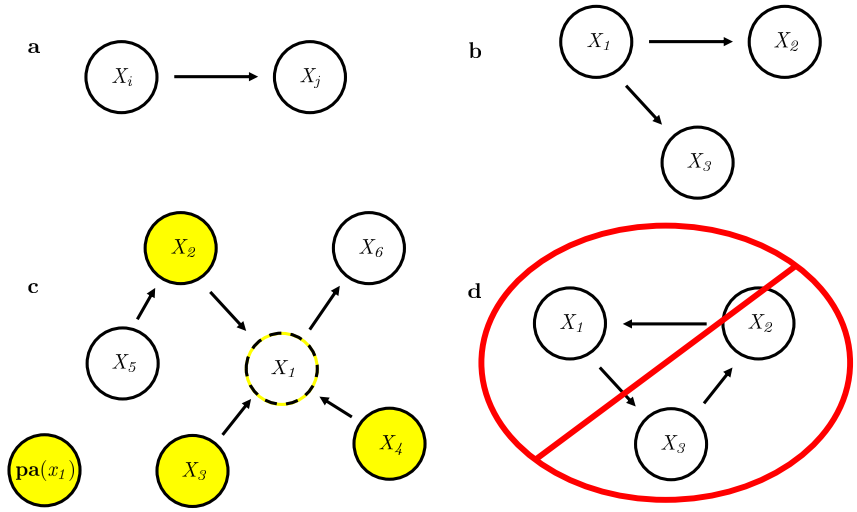

Figure 2.5. Directed acyclic graphs (DAGs). (a-c) Examples of allowed DAGs. (c) In particular, the parent nodes $\mathrm{pa}(x_1)$ (yellow) correspond to the nodes which influence directly the value x_1 of the node variable X_1. (d) DAG with cycles is not allowed to avoid retro-causal influence.

possible to devise and study any scheme involving an arbitrary number of nodes and causal influences. A node value x_i can be always expressed as $x_i = f_i(\mathrm{pa}(x_i), u_i)$, that is the deterministic result of its noise u_i and parent nodes $\mathrm{pa}(x_i)$. The latter represent all the variables that have direct influence over x_i (Fig. 2.5c), ruling out its direct noise. In a system with n nodes, the Markov condition [188] maps the causal structure involving the nodes into a constraint on the conditional probabilities, which reads:

$$p(\boldsymbol{x}) = \Pi_{i=1}^{n} p(x_i|\mathrm{pa}(x_i)), \tag{2.1}$$

where $\boldsymbol{x} = (x_1, \ldots, x_n)$ represents the set of variable values associated to the nodes. The Eq. (2.1) provides a device-independent condition for the factorization of the conditional probabilities, in which there are no assumptions on the inner working of the exploited apparatus, that is the adopted function f_i, but only on the realized causal structure. Also, a physical system is said *compatible* with a given causal structure if its correlations observe Eq. (2.1). These aspects suggest the power of this formalism: each time experimental data provide correlations outside a certain considered structure, i.e. are not in agreement with its Markov condition, then that specific structure can be automatically ruled out. This is the same spirit of Bell inequality. Indeed, the typical Bell scenario represents a particular case of DAG and more general Bell-like scenarios, which involve multiple parties in several correlation schemes, can be studied using the same approach.

The causal structure of the typical Bell scheme is reported in Fig. 2.6. Two independent parties, Alice ($X_1 = A$) and Bob ($X_2 = B$), are initially correlated by a certain variable Λ, the *correlation source*, whose value is λ. Then, two independent measurement choices, $x_A \in \{0, 1\}$ and $x_B \in \{0, 1\}$, are performed over the two parties, affecting their dichotomic result $a \in \{0, 1\}$ and $b \in \{0, 1\}$, respectively for nodes A and B. No arrows connect A and B, so that one can not affect the other. The resulting values a and b of the observables A and B, respectively, can be described by conditional probability $p(a, b|x_A, x_B, \lambda)$, which from Markov condition

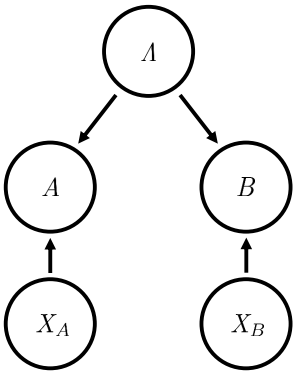

Figure 2.6. Bell scenario in DAG formalism.

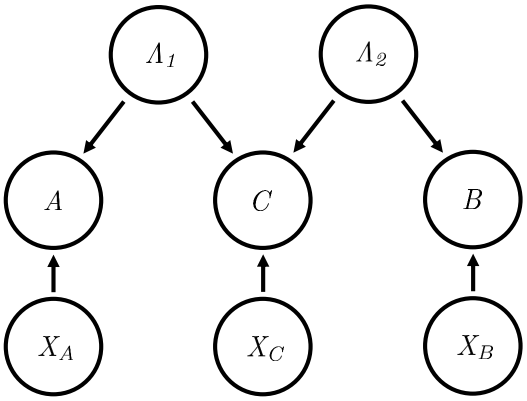

Figure 2.7. Bilocality scenario in DAG formalism.

reads:

$$p(a, b|x_A, x_B, \lambda) = p(a|x_A, \lambda)p(b|x_B, \lambda). \tag{2.2}$$

This equation corresponds to the local causality condition [Eq. (1.17)], from which Bell theorem is derived, as discussed in Sec. 1.2.2. Therefore, if Λ is an entanglement source, it is possible to violate any LHV model having the typical Bell causal structure. With the same logic it is possible to investigate more complex scenarios.

Let us consider for example the case of more parties sharing two systems with a unique central one, called *star-shaped network* (SSN). The simplest case of SSN is the *bilocal* scenario, where two parties are linked with a central node (Fig. 2.7). This is the scheme typically exploited for entanglement swapping protocols (Fig. 2.3). Here, two independent variables, Λ_1 and Λ_2, distribute correlations between the three parties Alice (A), Bob (B) and Charlie (C). The sources are considered fully independent, that is $p(\lambda_1, \lambda_2) = p(\lambda_1)p(\lambda_2)$. Following the same notation of the Bell scheme, but considering also the variables associated to Charlie's nodes (x_c, c), the probability distribution of results reads:

$$p(a, b, c|x_A, x_B, x_C) = \sum_{\lambda_1,\lambda_2} p(\lambda_1)p(\lambda_2)p(a|x_A, \lambda_1)p(b|x_B, \lambda_2)p(c|x_C, \lambda_1, \lambda_2), \tag{2.3}$$

in which each measurement is chosen between two possibilities ($x_A, x_B, x_C \in \{0, 1\}$) and has dichotomic results ($a, b, c \in \{0, 1\}$). From this condition can be found a

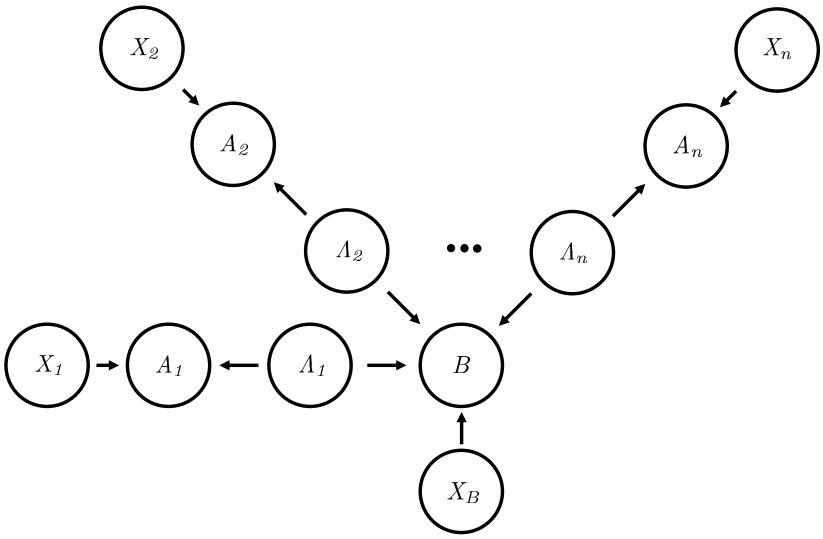

Figure 2.8. n-locality scenario in DAG formalism.

non-linear Bell-like inequality, that each bilocal model must satisfy:

$$S = \sqrt{|I_1|} + \sqrt{|I_2|} \leq 1. \tag{2.4}$$

where

$$\begin{aligned} I_1 &= \frac{1}{4} \sum_{x_A, x_B} \langle A^{x_A} B^{x_B} C^0 \rangle, \\ I_2 &= \frac{1}{4} \sum_{x_A, x_B} (-1)^{x_A + x_B} \langle A^{x_A} B^{x_B} C^1 \rangle, \\ \langle A^{x_A} B^{x_B} C^{x_C} \rangle &= \sum_{a,b,c} (-1)^{a+b+c} p(a, b, c | x_A, x_B, x_C). \end{aligned} \tag{2.5}$$

The violation of Eq. (2.4) has been demonstrated experimentally by different photonic setup [189, 190, 191, 192, 128] by using entangled quantum states. In particular, this result can be achieved also using separable measurements [128, 191, 193, 194], thus allowing exploitation of different sources of entanglement and an easier generalization to a more complex quantum network. This is the case of n-locality SSN, corresponding to a generalization of the bilocality SSN ($n = 2$). In the n-local scheme (see Fig. 2.8) n independent nodes $\boldsymbol{A} = (A_1, \ldots, A_n)$ are interconnected by the same number of independent correlation sources $\boldsymbol{\Lambda} = (\Lambda_1, \ldots, \Lambda_n)$, respectively, to a single central node B. We consider each node making k dichotomic measurements ($k \leq n$) and the sources fully independents: $p(\lambda_1 \ldots \lambda_n) = \prod_{i=1}^{n} p(\lambda_i)$. Thus, the output probabilities factorize as follow:

$$p(\boldsymbol{a}, b | \boldsymbol{x}, x_B) = \sum_{\boldsymbol{\lambda}} p(b | x_B, \boldsymbol{\lambda}) \prod_{i=1}^{n} p(\lambda_i) p(a_i | x_{A_i}, \lambda_i), \tag{2.6}$$

where $\boldsymbol{a} = (a_1, \ldots, a_n)$, $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_n)$. In a LHV model, Eq. (2.6) must fulfill the generalized non-linear Bell-like relation:

$$S_n^k = \sum_{l=1}^{k} |I_l|^{1/n} \leq k - 1, \tag{2.7}$$

known as *chained n-locality inequality* [195]. Considering $\boldsymbol{A}^{\boldsymbol{x}} = \prod_{j=1}^{n} A_j^{x_j}$, each element I_l of Eq. (2.7) reads:

$$\begin{aligned} I_l &= \frac{1}{2^n} \sum_{\boldsymbol{x}} \langle \boldsymbol{A}^{\boldsymbol{x}} B^{x_B} \rangle, \\ \langle \boldsymbol{A}^{\boldsymbol{x}} B^{x_B} \rangle &= \sum_{\boldsymbol{a}} (-1)^{\sum_{i=1}^{n} a_i + b} p(\boldsymbol{a}, b | \boldsymbol{x}, x_B). \end{aligned} \tag{2.8}$$

Notably, the greater is the number k of measurements performed by the nodes, the higher is the violation achievable by entangled quantum states, with respect to LHV models. Therefore, tuning k can provide advantages in device-independent protocols, either by reducing the experimental constraints for their violation [196] or by leading to better security tests [197]. The violations of Eq. (2.7) have been demonstrated experimentally in a photonic quantum network by our recently work [12] (See Sec. 2.4). The study of more complex quantum networks allows the investigation of novel non-classical behaviors [198, 8], together with having less stringent experimental requirement in terms of detection efficiency [199], as well as testing device-independent protocols over different networks topologies [200].

2.1.3 Quantum Cryptography

Quantum Cryptography is based on the secret sharing of a key between two parties, Alice and Bob, which want to communicate in a secure way. Such key is used to encrypt and decrypt their messages using the standard *one-time pad* technique [201, 202]. Indeed, this technique guarantees perfect security in principle, provided that the key is random, is as long as the message and is used only once. Thus, all the communication security depends on the secret exchanging of such a key. Distributing quantum resources for this task allows enhancing the secrecy of conventional communication. *Quantum key distribution* (QKD) is one of the Quantum Information protocols nearest to real-life applications. Indeed, several commercial companies are trying to make QKD systems available to everyone [1]. The great worldwide interest comes from the possibility for QKD to allow an *unconditional secure communication*. Indeed, unlike classical protocols of cryptography, QKD security is based on physical assumption rather than on the computational capacity of any possible eavesdropper (Eve). Thus the term "unconditional" indicates that the level of secrecy is guaranteed to be the same for any computational power of Eve. However, even if the key can not be stolen, it is always possible to guess the secret shared key randomly during a brute force attack[2]. Quantum advantages in cryptography are strictly related to *no-cloning theorem* [203], that is the impossibility for Eve to clone completely the same quantum information exchanged between Alice and Bob. An alternative way to understand the phenomenology of QKD is to think that any possible attempt of Eve to extract information is a generalized measure on the system. And contrary to what happens classically, every measurement on a quantum system inevitably

[1] idQuantique, Geneva, Switzerland (www.idquantique.com); MagiQ Technologies, Inc., New York (www.magiqtech.com); and Smartquantum, Lannion France (www.smartquantum.com).

[2] The key is guessed randomly.

changes the state. When Alice sends a single photon to Bob, Eve can not intercept the signal without revealing its presence, which is modifying the single-photon quantum state (Fig. 2.9). Therefore, the presence of Eve in a quantum channel can be commonly statistically estimated by the two parties, through the so-called quantum bit error rate (QBER) [Eq. (2.9)]. Surprisingly, the strength of QKD does not rely on the ability to detect Eve's presence, but on the ability to extract a certainly secret key despite Eve's presence. Although there is huge interest in the realization of experimental QKD [182, 4], this non-classical potential is still not achievable in realistic scenarios due to technological limitations, which do not allow us to completely satisfy the assumptions of the QKD protocols, together with the effects of real-life environments. Indeed, even if all the assumptions of the quantum protocols are respected, only QBER values lower than specific quantities allow a possible unconditional secure QKD. Thus, photon losses constrain the validity of QKD protocol to scale as the transmittivity t of the involved quantum channel [4]. The other fundamental limitation in realizing QKD concerns the non-deterministic multiphoton emission in existing SPSs. This is the case of the photon number splitting attack [151], which makes QKD protocols currently insecure. Here, Eve can measure one of the multiple photons produced by the source and send the other to Bob without changing its state and taking information about it (Sec. 2.1.3.3). Consideration of such an attack imposes a scaling of t^2 with distance, i.e., reducing the achievable QKD by a factor of t [4]. Lots of QKD experimental realizations exploited attenuated laser pulses as SPS. Here, each wavepacket has an average number of photons below 1, distributed according to a Poissonian statistic. As seen in Sec. 1.2.3, also the other types of SPS suffer the possible emission of multiple photons. This means that non-deterministic multiphoton emissions can generally occur, opening serious loopholes on the QKD security. The only other way to improve long-distance QKD is to exploit quantum repeaters [95, 204, 96] and QKD networks [205], which currently represent hot topic investigations [206]. The current QKD records in optical fiber was performed in telecom regime covering a distance of 404 km [207] in prepare-and-measure scheme and 421 km [208] in measurement-device-independent scheme (see Sec. 2.1.3.1). In satellite-based technology the best long-distance QKDs have exceeded 1000 km [102, 100, 99], using the Micius satellite [100], with the highest record of 7600 km [100]. Furthermore, over the last years a growing research interest is attracting the study of QKD protocols on chip [209, 210, 211, 212, 213], showing advantages in stability, compactness, and costs.

Therefore, on the one hand it is fundamental to investigate deterministic SPSs. On the other hand, photonic quantum channels compatible with QKD requirements must be realized and investigated. Remarkably, during my thesis it has been successfully demonstrated the first quantum key distribution along a free-space channel connecting two distant buildings, using a quantum dot SPS [13] (Sec. 2.5.2). In this section, the fundamentals of quantum key distribution are introduced.

2.1.3.1 QKD protocols

In the final stage of the key distribution, the two communicators use the key only if it is secure, otherwise the protocol is aborted. In order to exchange a secure quantum key, Alice and Bob must follow a series of instructions. QKD protocols can be divided in two main stages: the distribution of quantum information and the post-processing of classical information. The first concerns all the exploitation of quantum resources allowing the distribution of bits, with secrecy guaranteed by quantum laws. The second deals with all the post-processing necessary to elaborate

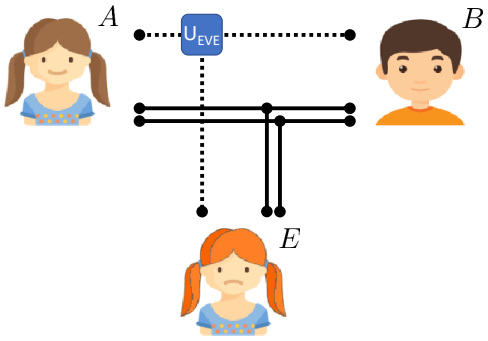

Figure 2.9. General scheme of hacked quantum communication between two parties, Alice and Bob. Any possible eavesdropper (Eve) operates on the quantum link (dashed line) whenever she tries to catch information. Conversely, she can only hear the information of the classical channel (double solid line) without changing it.

the results, in order to have the shared key correctly clean and completely sure from both sides. Therefore, the protocols typically require the presence of both a quantum and a classical channel connecting Alice and Bob. There are three main families of QKD protocols [182, 4]: discrete variable encoding, continuous variable encoding and distributed phase reference encoding. In this thesis, we are interested in the discrete variable approach, whose most used implementations are BB84 (or 4-state BB84), E91 and SARG84. Further solutions exist, such as 6-state BB84, BBM92 or B92 [182, 4].

While the post-processing step is similar for all existing schemes, several strategies can be adopted in distributing the quantum key. The simplest scheme — and the first historically studied — is the *prepare-and-measure* (P&M). Here, Alice prepares the quantum state and sends it to Bob. Bob measures and the results are used to estimate both the key and the presence of a possible Eve. A second possibility is the *entangled-based* (EB) scheme. In this case Alice prepares and measures an entangled state. A signal correlated to the measurement result is sent to Bob, which acts as in P&M. EB protocols have been demonstrated to be equivalent to P&M ones [214]. However, this is not strictly true, as EB shows a degree of device-independence security that can not be reproduced by P&M with separable states [131]. Finally, a third possibility is represented by a *device-independent* scheme, particularly interesting in *measurement-device-independent* (MDI) version [215, 216]. In MDI both Alice and Bob prepare and send a state to an external node, which performs the measurements and distributes the secret key. In the following, the most common approaches to discrete variable encoding are reported. Finally, a modified version of E91 is presented, which shows some advantages in practical implementations.

BB84

BB84 is a P&M protocol (Fig. 2.10), introduced by Bennett-Brassard for the first time in 1984 [217]. Here, Alice sends to Bob a sequence of single bits encoded in quantum bits. On the Alice side, one random bit is first selected, and then it is randomly encoded in computational or diagonal basis (Sec. 1.1.1). The prepared qubit $|\Psi_{\mathrm{A}}^{(b)}\rangle$, encoded in basis b, is sent to Bob along the quantum channel. On the Bob side, a measurement basis b' is randomly selected between the computational

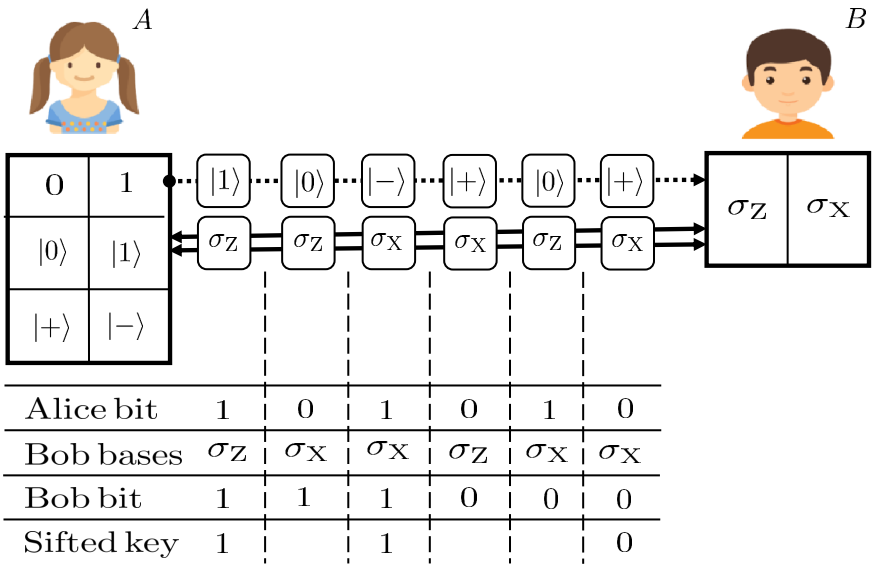

Figure 2.10. QKD according to the BB84 protocol. One of four different quantum states is prepared randomly for encoding a bit. The qubit is sent along the quantum channel and it is revealed by Bob choosing randomly the measurement basis. Then they proceed with the sifting procedure and classical post-processing in order to obtain an unconditionally secure distributed key.

and the diagonal ones, and the received qubit is measured. Thus, the quantum state collapses along one eigenstate $|\Psi_{\mathrm{B}}^{(b')}\rangle$ of the chosen basis, proving the correct bit with probability $P(\Psi_{\mathrm{A}}^{(b)} = \Psi_{\mathrm{B}}^{(b')}) = |\langle\Psi_{\mathrm{A}}^{(b)}|\Psi_{\mathrm{B}}^{(b')}\rangle|^2 = 1$ if it correspond to the Alice encoding ($b = b'$), while $P(\Psi_{\mathrm{A}}^{(b)} = \Psi_{\mathrm{B}}^{(b')}) = 0.5$ otherwise ($b \neq b'$). At the end of this process Alice and Bob have a chain of N bits with the associated basis choices (*raw data*). Thus, they perform classical processing of data, known as *sifting* procedure, whose result is a shared *sifted raw key*: they declare on a public channel — the classical channel — the N basis performed (not the bits!) and keep only the n bits ($n \leq N$) in which the encoding basis was the same of the decoding basis (50% of cases on average). Therefore, in the ideal case at the end of this process they share the same n bits. However, two phenomena can introduce errors in the key bits, by changing the qubits sent from Alice to Bob during the transmission in the quantum channel. First the presence of losses in the channel and second the signal interaction with a possible Eve during the communication. Here, Quantum Mechanics acts, by changing unavoidably the state, each time external elements try to interact with the transmitted qubit. Alice and Bob can measure with certainty the amount of risk in the transmission, by randomly declaring a part $\tilde{n}$ of the n distributed key — the same for Alice and Bob — and estimating the quantum bit error rate (QBER):

$$\mathrm{QBER} = \frac{n_{\mathrm{err}}}{\tilde{n}}, \tag{2.9}$$

where n_{err} are the wrong bits arising from the comparison of the declared $\tilde{n}$ strings of Alice and Bob. Notably such a statistical quantity represents an upper bound to the amount of information acquired by a possible Eve, since it includes also the errors due to losses. The security of QKD protocols is demonstrated in a pessimistic

scenario, i.e. considering that all errors present are key information accessible to Eve. Approaches that optimize the actual knowledge of Eve about the system are the *decoy-state* techniques [218]. Such a technique is even able to improve the experimental feasibility of QKD up to t scaling with the channel length [219, 220]. The subsequent instructions for completing the protocol concern post-processing operations. They are quantum error correction and privacy amplification, which provide a final secure key shorter than the original sifted key. These procedures are described in detail in Sec. 2.1.3.2. Several works [221, 222, 223, 224, 225, 226] demonstrated that the quantity of QBER must be lower than specific values in order to guarantee different degrees of safety. In particular, if QBER$<11\%$ the unconditional security of the QKD protocol is achieved [221]. Notably, during the various stages of the QKD protocol the original number N of bits that Alice sent to Bob is importantly reduced, before creating the final n_k-long key. Thus, it can be useful to define a quantity, the *secure key rate* (R), which estimates such conversion efficiency of the specific protocol: $R = n_k/N$.

SARG04

A similar version of BB84 is represented by SARG04 (Scarani, Acin, Ribordy and Gisin, 2004) [227, 228]. This protocol is less efficient than BB84 in terms of the secure key rate, but shows higher robustness to photon number splitting attack, showing an improved scaling with the distance equal to $t^{3/2}$ [4]. Here, Alice encodes the random bit in the basis choice: for example bit 0 is codified by computational basis, while bit 1 by diagonal basis. Then, the qubit is sent to Bob which measures by randomly selecting one of the two bases. Bob declares the resulting bit (not the basis!) and Alice agrees only the cases in which the bit is opposite to the one prepared. Indeed, while all the other cases are ambiguous, this event is possible only in one way: if Alice prepares a bit in a specific basis, e.g. 0 in computational ($|0\rangle$), and Bob measures in the different basis, e.g. the diagonal, in half events the state collapses into the opposite bit 1 ($|-\rangle$). Therefore Bob can share the same bit of Alice by simply flipping his result. From here on, the development of the protocol is the same as for BB84. Thus, in this case the sifting procedure discards the 75% of data, which is less advantageous compared to the BB84, achieving on average the 50% of its secure key rate.

E91

Ekert91 (E91) was introduced by Ekert in 1991 [123]. It is an EB protocol where an entangled state is shared by Alice and Bob. Alice prepares a bipartite maximally entangled state, correlating the elements of the so-called *key basis* ($\{A_k, B_k\}$). Then, she sends one qubit along the quantum channel and the other qubit to her apparatus. Bob receives the qubit, knowing the original entangled state prepared. Then, both the sides perform measurements by randomly selecting between the key basis (A_k for Alice; B_k for Bob) or the basis able to violate the Bell inequality ($\{A_0, A_1\}$ for Alice; $\{B_0, B_1\}$ for Bob)(Sec. 1.2.2). As well as BB84, they publicly declare the bases used and suppress the cases in which they are different (sifting). In this way, they obtain sometimes results along the key basis and the other times on the Bell-test basis. Therefore, ideally each side produces a string of n bits on the key basis which is correlated (or anti-correlated) to the string of the other side, that they use as the shared key. In total analogy with the BB84, the presence of losses or Eve introduces errors in such strings. Those can be estimated by declaring a subset of $\tilde{n}$ bits in the public channel, measuring the QBER and then proceeding with the

same post-processing. Remarkably, this protocol shows a further layer of security. If Alice and Bob declares the results obtained in Bell-test basis, they can compute also the parameter $S = |\langle A_0 B_0\rangle + \langle A_0 B_1\rangle + \langle A_1 B_0\rangle - \langle A_1 B_1\rangle|$ and certify the expected violation of Bell inequality: $2 < S \leq 2\sqrt{2}$. Such a test is not only sensitive to interactions in the transmission along the quantum channel, but also shows some additional degree of device independence [131] due to the Bell test nature (Sec. 1.2.2).

Modified E91. The security of E91 shows some advantages over what the BB84 can offer. However, while BB84 uses all sifting data results for the key generation, the E91 protocol gets half the rate, since on average the 50% of the resources is employed for the Bell observables. Furthermore, in the current photonic QKD implementations the BB84 can exploit SPSs with the highest recorded rate. Conversely, the photonic entangled sources still do not achieve the same performances. Therefore, it is important to develop schemes able to provide E91-like security, while aiming at the BB84 key rate. In order to optimize the experimental implementation of E91, a possibility is exploiting the approach developed in [229]. Here, the scheme is asymmetric: Alice uses three basis $\{A_k, A_0, A_1\}$, while Bob only two $\{B_0, B_1\}$. As well as in standard E91, $\{A_0, A_1\}$ and $\{B_0, B_1\}$ are used for monitoring the Bell test. At the same time, it is possible to consider B_0 also as the key basis on the Bob side, thus correlating the entangled state on the basis $\{A_k, B_0\}$. In this way the procedure is the same as E91, but requiring at least one less single-photon detector than the standard scheme. Furthermore, the asymmetry allows to statistically encode more bits in the key basis, thus enhancing the key rate. Despite the historical importance of E91, these reasons make such a modified version of E91 more interesting for practical implementations [230, 231].

2.1.3.2 Post-processing of classical information

After the quantum distribution of the key, the starting sifted raw key is manipulated by the two parties, Alice and Bob, in order to correct any errors (error correction) and achieve the best security (privacy amplification). These steps of *information reconciliation* are made by exploiting the classical channel and classical operations. In particular, direct or reverse reconciliation is possible, if it is Bob or Alice to post-process its own data, respectively. Even two-way schemes exist, where this action is made by both parties.

Error correction. Possible errors can occur due to a possible Eve, malfunctions of hardware or software components in each side, losses or even for unclear reasons. These errors are estimated with the QBER and correspond to having some flip bits at certain positions of the sifted key. Therefore such errors must be found and corrected. The standard steps of the error-correcting protocol are described in the following:

(i) the n_{raw}-long sifted raw key is divided in strings of length L_1 — the same for Alice and Bob —, such that the probability to find one error in a string is very small: $L_1 \cdot \text{QBER} \ll 1$.

(ii) A *parity check* is performed over each string: the XOR sum of the L_1 bits provides a number that is different only if the selected string has one error. Double errors are neglected since $L_1 \cdot \text{QBER} \ll 1$. Alice and Bob declare on the public channel their parity-check results. The comparison allows them to certify if the selected string is good (no error) or not (error). In both cases,

at the end of the parity check the last bit of such string is discarded, thus avoiding to provide additional information to Eve.

(iii) If the selected string shows no error, it becomes part of the final key. Otherwise, it is subsequently divided into shorter strings and the protocol restarts from (ii).

At the end of the iterative cycle each error in the final key is eliminated, at the cost of having a reduced key size.

Privacy amplification. As discussed before, measuring the QBER Alice and Bob compute an upper bound on the external influence to the communication, that is the best Eve's knowledge on the key. After error correction the shared key becomes the same for both, but Eve preserves a partial knowledge about it. Such Eve-own information must be deleted, in order to establish a final key definitely secure. This is the goal of the privacy amplification procedure [232], which is able to create a new shared key, random and independent by the partial eavesdropper information. A demonstrated possibility is based on *two-universal hashing* [233, 182]. Alice chooses a seed s for applying a random hash function $f^{(s)}$ to her n-long key k_n, obtaining a new shorter m-long key ($m < n$): $k_m = f^{(s)}(k_n)$. The seed is declared publicly, thus allowing Bob to apply the same function. In this way, Alice and Bob obtained the same final key, while Eve did not, despite having access to the seed. Indeed, if Eve has a slightly different key k'_n, the probability of obtaining the same key k_m is negligible, upper bounded by $1/2^m$ [4]. Thus, its final information is automatically uncorrelated by the final key of the two communicators. At the end of this procedure, a secure key is distributed between Alice and Bob, but also in this case the price to pay remains the key size.

2.1.3.3 Attacks and security

Several hacker attacks are known in the information theory. Although QKD represents an ideal solution, practical QKD still suffers some of them. The main threats to QKD security are represented by attacks such as photon number splitting, man-in-the-middle, intercept-resend, side-channel, and Trojan horse [234, 4, 3].

- One of the most famous attacks in photonic QKD is represented by photon number splitting [235, 151]. As already discussed, this problem is due to the non-ideal emission of SPSs, which randomly produce a multiphoton emission. When Eve intercepts the wavepacket, she can selectively suppress single-photon states and preserve only multiphoton cases; Then, she can send to Bob a "fake" single photon extracted by such cases, but having a copy of the state thanks to the other elements of the emission. In this way, Eve has access to the same information exchanged between Alice and Bob, completely unbeknownst to Alice and Bob.

- In the intercept-resend approach, Eve measures each signal sent by Alice in the quantum channel, by performing the same measurements that Bob would do. Then, she encodes the bit measured similarly to Alice and sends it to Bob. In this way, after the sifting procedure Eve has the same bits of Bob, but introducing an error of 50% with respect to Alice's raw key. It is possible to demonstrate that no secure quantum key in BB84 can be obtained if Eve detects more than 68% of the qubits sent by Alice [4].

- During a Trojan horse attack [236, 237], Eve tries to probe information on Alice and Bob by sending signals to their apparatuses. More generally, this danger is related to the presence of side-channels due to hardware limitations. Indeed, the success of such Eve's strategy is related to the possibility that Alice correlates the prepared state with other degrees of freedom unwittingly. Thus, Eve probes the two systems to obtain such informative property, in order to extract information on the communication. No general solutions are known about this attack, but the related security is based on the well-characterization of the involved quantum channel [238, 239]. In some specific setups, it can be solved by using particular scheme-dependent defense elements, such as an optical isolator [239] or a spatial filter [240],

- In a man-in-the-middle situation [3, 241], Eve is placed inside the direct communication from Alice to Bob, such that each information exchanged passes through the apparatus of Eve. In other words, Eve represents Bob for Alice and vice versa. This attack can be avoided if Alice and Bob share some initial secret, i.e. a short secret key. This is possible as the QKD uses fewer key bits than the amount produced.

For all these attacks, the security of the key distribution is measured in terms of Shannon's mutual information (I) [242] between the various parties. The QKD security is based on the consideration that the Bob's (B) knowledge of Alice's (A) data is bigger than the Eve's (E) one, i.e. $I(\mathrm{A}:\mathrm{E}) < I(\mathrm{A}:\mathrm{B})$ [243, 244]. This relation guarantees that some secret is shared between Alice and Bob, which is not accessible by the Eve information. Unlike classical investigation, quantum cryptography must consider the possibility that Eve can even take advantage of quantum technologies and infinite computational resources. Eve could entangle the quantum signal in the quantum channel and measure her sub-system only after the key is created and used. Thus, in this case the classical mutual information $I(\mathrm{A}:\mathrm{E})$ is defined only after such measure. Therefore, a quantum counterpart of $I(\mathrm{A}:\mathrm{E})$ must be seriously considered. Fortunately, also in this case the security of QKD has been rigorously demonstrated [222, 245]. Finally, the practical implementation of QKD suffers additional flaws, due to the non-ideal characteristics of hardware components. A relevant problem concerns the weakness of the detection stage [246]. Even if solutions to specific vulnerabilities can be found, only the MDI scheme can offer a more general solution to all these kinds of attacks.

2.2 On-chip entanglement generation

Most protocols of Quantum Information and Communication theory found their power in entanglement, which represents the indispensable resource, such as in teleportation [118], entanglement swapping [119] and quantum key distribution [120]. Even overcoming classical performances in Quantum Computation [121] and Metrology [2] requires the use of such quantum correlations. Therefore, tackling the generation of entanglement is the first fundamental step to achieve in order to take delight in any quantum advantages. The benefit of the photonic implementation has been largely discussed yet (see Sec. 1) but notably, the easy manipulation of different degrees of freedom of light, with respect to other quantum carriers, makes entangled photons a really attractive solution. Several photonic platforms have been developed so far for generating entangled states of light, whose encoding ranges between the various degrees of freedom of light. Bulk interferometer, folded sandwich configuration, post-selection entanglement (Sec. 1.2.3), are only some of the possible solutions. Even hybrid and hyper entangled states can be realized, correlating simultaneously different light properties [11, 247]. Quantum photonic sources is already a well-defined technology, which is aiming in the last period to optimize its generation rate, stabilization, and miniaturization. Moreover, the large variety of photon solutions require the ability to interface quantum states of light between different technological levels. The integrated level provides the possibility to compact dozens of optical components on the same chip, paving the way to previously impossible implementations [20, 21, 22, 23, 24, 25, 26]. To further scale up the complexity and fully capitalize on the advantages of the integrated optics approach, quantum photonics is moving towards the integration of sources on-chip as well. In bulk optics, sources of entangled photon pairs can be typically achieved by spontaneous parametric down-conversion (SPDC) in nonlinear crystals [143] (Sec. 1.2.3). A promising strategy to realize their integrated counterparts is represented by employing waveguides in nonlinear substrates. Due to the enhanced light-matter interaction, a boost in source brightness adds up to the standard advantages of the integrated approach, such as miniaturization and optical phase stability. Path-entangled states can be generated by down-conversion in coupled nonlinear waveguides [248, 249], while generation of polarization entanglement in an integrated device requires additional effort. In dielectric waveguides, polarization entanglement has been achieved either outside the chip [250, 251] or exploiting non-degenerate photon pairs [252]. Recently, an on-chip source of degenerate polarization-entangled photons has been demonstrated in lithium niobate waveguides; however, the pumping scheme was not fully integrated and required a bulk Sagnac loop configuration [253]. Polarization-entangled photon generation has also been demonstrated in semiconductor materials, either based on SPDC [52, 254] or exploiting spontaneous four-wave mixing [255]. Finally, the wavelength of generated photons provides another important experimental choice, which has to consider the specific photonic scenario, such as free-space or fiber communication, together with the efficiency of the detection components.

In [10], we realized an integrated photonic source of entangled photons, based on interfacing different integrated components. The modular approach with hybrid materials allows us to easily tailor each component to its specific task. First, single-mode waveguides at different wavelength ranges can be employed for manipulating both the pump and the generated photons. Then, waveguides in the nonlinear crystal are used only for the generation of photon pairs, while waveguides in glass

are exploited to manipulate the pump beam. In addition, the use of linear and low-birefringence glass circuits allows one to neglect any unwanted nonlinear effects and to easily manipulate the polarization state of the propagating photons. The device is fabricated through the advanced FLW technique and can be reconfigured thanks to the presence of a thermo-optical phase-shifter. This architecture allows us to tune the output state simply by controlling an electric voltage and even the entanglement encoding, by exchanging the last chip component, passing from a path entanglement to a polarization one. All these aspects represent important advantages, which make our device suitable for a plethora of possible applications. Furthermore, the output photons are generated at telecom wavelength, where the standard optical fibers show minimal losses. This property guarantees an optimal coupling of our integrated entanglement generation with the standard fiber communication networks.

2.2.1 Description of the integrated device

The photon pair generation system is composed of three integrated devices (See Fig. 2.11a): (1) a reconfigurable balanced directional coupler at 780 nm; (2) two identical waveguides in a periodically poled lithium niobate (PPLN) chip; (3a–b) a third interchangeable device operating at 1560 nm for the preparation of different output states. The combination of such devices permits the generation of identical photon pairs at the telecom wavelength and to engineer their quantum state through a reconfigurable Mach–Zehnder interferometer.

The first directional coupler splits the pump equally to feed the two laser-written waveguides in the PPLN device. Single-photon pairs are generated in both waveguides through a Type 0 SPDC process. Dynamical control of the phase between the two paths is ensured by a thermo-optic phase shifter fabricated in the first device. The third device closes the interferometer and recombines the generated photons to obtain the desired output. We employed two different devices, giving access to different classes of output states. In a first case, the third device (3a) consists in a balanced directional coupler, leading to an output state of the form

$$|\Psi_{(3a)}\rangle = \frac{|0,2\rangle - |2,0\rangle}{\sqrt{2}}\cos(\frac{\phi}{2}) + |1,1\rangle \sin(\frac{\phi}{2}), \tag{2.10}$$

where $|i,j\rangle$ stands for a state with i and j photons on the two waveguides, respectively. Here, a NOON state or a product state $|1,1\rangle$ can be selected, controlling the phase ϕ between the two output arms of the directional coupler in the first device.

In the second case, the third device (3b) is composed of a half-wave plate at 22.5° (on mode 1), a half-wave plate at −22.5° (on mode 2), and a balanced polarization-insensitive directional coupler. Conditioned to the detection of a single photon on each output mode of the device, the output state is a polarization-entangled state of the form

$$|\Psi_{(3b)}\rangle = \frac{1}{\sqrt{2}}(|+,+\rangle + e^{i\phi}|-,-\rangle), \tag{2.11}$$

where $|\pm\rangle = 2^{-1/2}(|H\rangle \pm |V\rangle)$ are diagonal linear polarization states at 45°. As in the previous case, ϕ can be tuned by the thermo-optic phase shifter in the first device.

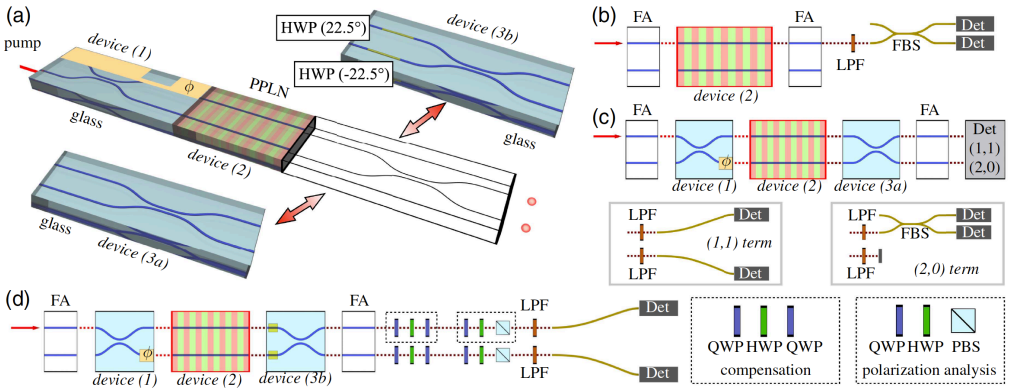

Figure 2.11. **a**, Overall scheme of the integrated source, comprising three cascaded integrated devices. Device (3a) or (3b) can be exchanged depending on the desired output state. **b**, Apparatus employed to characterize the photon pair generation in PPLN waveguides. Device (2) is directly interfaced with input and output FAs. The output of each waveguide is directly sent to the detection apparatus, where a FBS separates the output to two detectors to discriminate two-photon events. **c**, Apparatus for the characterization of the output state by inserting device (3a). The output state, coupled via input and output FAs, is detected to alternatively characterize the (1,1) and (2,0)/(0,2) terms, the latter by inserting a FBS on the measured mode. (d) Apparatus for the characterization of the polarization-entangled state generated when device (3b) is used. The output state, collected by a FA, undergoes polarization compensation through a set of wave plates and is then analyzed in polarization by means of wave plates and a PBSs. Legend: PPLN, periodically poled lithium niobate; FA, fiber array; LPF, long-pass filter; HWP, half-wave plate; QWP, quarter-wave plate; PBS, polarizing beam-splitter; FBS, fiber beam-splitter; Det, detector. This image is taken from [10].

2.2.2 Experimental characterization

In order to characterize the generation of photon pairs in each PPLN waveguide, a Ti:Sapphire oscillator operating in the continuous-wave regime (CW) is coupled to the integrated device by means of single-mode fiber arrays. A combination of long-pass filters (leading to a total extinction ratio of 102 dB at 780 nm) is used at the output to suppress the residual pump beam. The generated photon pairs are measured by coupling the output of one PPLN waveguide at a time to a fiber beam splitter (FBS). Two-fold detection is performed by two avalanche photodiodes: the first operates free running with efficiency $\eta^1_{\text{eff}} = 25\%$ (ID230 by ID Quantique) and a dead time of 10 μs, while the second one is employed in the external gating mode with efficiency $\eta^2_{\text{eff}} = 25\%$ (ID210 by ID Quantique) and a dead time of 30 μs. Detection of one photon on one mode of the FBS triggers the second detector on the other FBS mode for the detection of the second photon. This configuration reduces the dark count rate and maximizes the detection efficiency. A proper time delay is introduced to allow the communication between the detectors. By controlling the internal trigger delay and the gate width of the second detector, it is possible to optimize the signal-to-noise ratio (SNR). The generation rate of the PPLN waveguides has been verified individually with 30 μW of pump power. The detection rate for each waveguide is $\sim$ 26000 Hz single counts and $\sim$ 10 Hz coincidences with a maximum SNR value of $\sim$ 140 for the twofold coincidences and a Klyshko efficiency of 0.04%. We believe that the main factors that limit this figure

of merit are the PPLN waveguide propagation loss (1.5 dB/cm at 1560 nm), the collection efficiency of the detection setup ($\sim 22\%$), and the detector efficiency.

We performed the characterization of the final output state reported in Eq. (2.10). This is achieved by exploiting the configuration of Fig. 2.11c, thus connecting device (3a) in cascade to the PPLN waveguide structures. We measured separately the $|1,1\rangle$ and the $|0,2\rangle$ terms as a function of the dissipated power by the thermo-optic phase shifter, which is linearly related to ϕ. The $|1,1\rangle$ contribution was measured directly at the two outputs of the system, while the $|0,2\rangle$ contribution was measured by coupling one output to an in-fiber beam splitter. The possibility to engineer the path-entangled state is highlighted by the anti-phase oscillations of the two contributions in the coincidence counts, corresponding to $cos^2(\phi/2)$ and $sin^2(\phi/2)$, respectively (Fig. 2.12). The visibilities of the coincidence oscillations are $V^{\text{raw}}_{|1,1\rangle} = 0.877 \pm 0.004$ and $V^{\text{raw}}_{|0,2\rangle} = 0.935 \pm 0.003$ for raw measurements. Subtracting accidental coincidences, the visibilities become: $V_{|1,1\rangle} = 0.970 \pm 0.004$ and $V_{|0,2\rangle} = 0.980 \pm 0.004$ showing the high quality of the generated state.

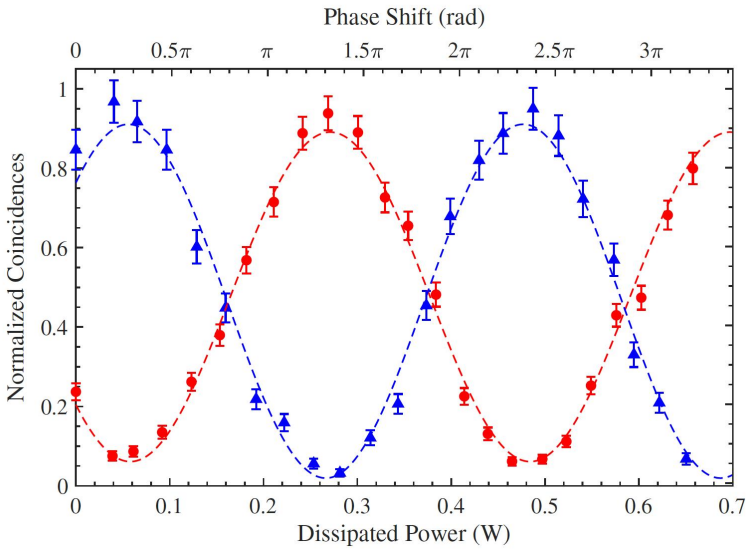

Figure 2.12. Measured interference fringes in the path-entangled configuration for the states $|1,1\rangle$ (red dots) and $|0,2\rangle$ (blue triangles) as a function of the dissipated power in the thermo-optic phase shifter (lower scale) and of the corresponding phase shift (upper scale). Dashed lines correspond to sinusoidal fitted curves. This image is taken from [10].

We then carried out the characterization of the polarization entangled state, which is obtained conditioned to the detection of a photon on each output mode, employing the setup of Fig. 2.11d. In this case, device (3b) is employed after the PPLN waveguides. Before being analyzed and detected, the generated state undergoes polarization compensation to cancel undesired rotations occurring in the output fiber array. In the polarization compensation stage, we also rotated the basis of the entangled pair so as to obtain an output state of the form $2^{-1/2}(|H,H\rangle + |V,V\rangle)$. For $\phi = 0$ ($\phi = \pi$) this corresponds to a polarization Bell state $|\phi^+\rangle(|\phi^-\rangle)$. In order to characterize the generated output state, we first measured the fringe pattern as a function of the dissipated power in two different polarization bases. More specifically, in the diagonal $|\pm\rangle$ basis the output state is expected to present

a sinusoidal oscillation pattern, while a measurement in the $|H/V\rangle$ basis should present no dependence on the phase ϕ. The experimental results are shown in Fig. 2.13 and are in agreement with the expected behavior. The measured visibilities in the different bases are $V^{\text{raw}}_{|+,+\rangle} = 0.858 \pm 0.019$ and $V^{\text{raw}}_{|+,-\rangle} = 0.834 \pm 0.018$ for raw data ($V_{|+,+\rangle} = 0.957 \pm 0.015$ and $V_{|+,-\rangle} = 0.929 \pm 0.017$ by subtracting the accidental coincidences). Furthermore, we observe that the pattern in the $|H/V\rangle$ basis is almost constant. These results provide evidences of the correct operation of the source. To further characterize the generated state, we chose a specific value for the phase $\phi = \pi$, corresponding to the generation of the Bell state $|\phi^-\rangle$. Hereafter, all experimental values we report have the accidental coincidences subtracted. We first measured the expectation values of Pauli matrices products $\langle \sigma_i \otimes \sigma_i \rangle$, where $i = X, Y, Z$, which correspond to evaluating polarization correlations in three different bases. We obtained $\langle \sigma_X \otimes \sigma_X \rangle = 0.942 \pm 0.008$($|H/V\rangle$ basis), $\langle \sigma_Y \otimes \sigma_Y \rangle = 0.895 \pm 0.010$ ($|\pm\rangle$ basis), and $\langle \sigma_Z \otimes \sigma_Z \rangle = 0.944 \pm 0.008$ ($|R/L\rangle$ basis), showing the presence of correlation in all three bases. This allows us to apply an entanglement test on the generated state [256], namely, $S = \Sigma_{i=X,Y,Z} |\langle \sigma_i \otimes \sigma_i \rangle| \leq 1$ for all separable states. The experimental value is $S_{\text{exp}} = 2.782 \pm 0.015$, thus violating the inequality by ~ 115 standard deviations and confirming the presence of polarization entanglement. We also performed a full-state tomography [167], to fully reconstruct the state density matrix. The results are shown in Fig. 2.14, where the obtained density matrix ρ_{exp} is compared to the one for an ideal state ρ_{ϕ^-}. We achieved a value of the fidelity $F(\rho_{\text{exp}}, \rho_{\phi^-}) = \text{Tr}[(\sqrt{\rho_{\text{exp}}}\rho_{\phi^-}\sqrt{\rho_{\text{exp}}})^{1/2}]^2$ between theory and experiment equal to $F = 0.929 \pm 0.011$, thus showing the quality of the generated state. The purity and amount of entanglement are quantified respectively by $\text{Tr}[\rho^2_{\text{exp}}] = 0.908 \pm 0.018$ and by the concurrence $C = 0.905 \pm 0.022$, which is comparable to the state of the art of on-chip polarization-entangled sources.

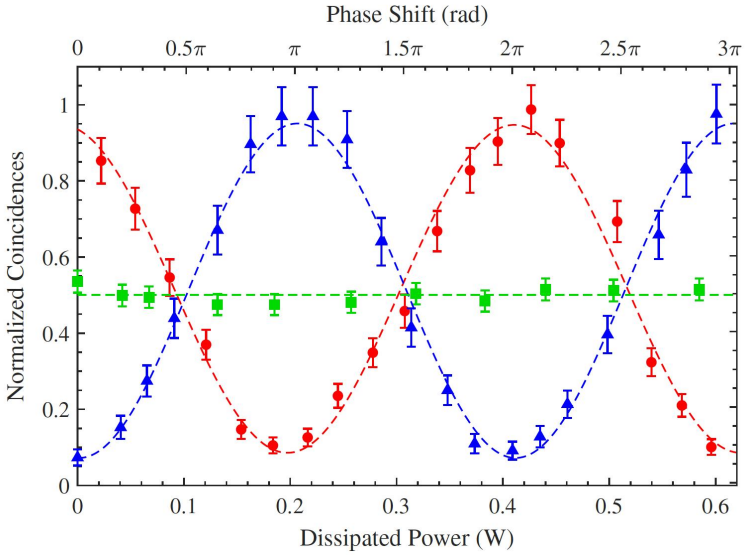

Figure 2.13. Fringe pattern in the polarization-entangled configuration obtained by measuring the output contributions, $|+,+\rangle$ (red dots), $|+,-\rangle$ (blue triangles), and $|H,H\rangle$ (green squares), as a function of the dissipated power (lower scale) and of the corresponding phase shift (upper scale). Dashed lines correspond to the fitted curves. This image is taken from [10].

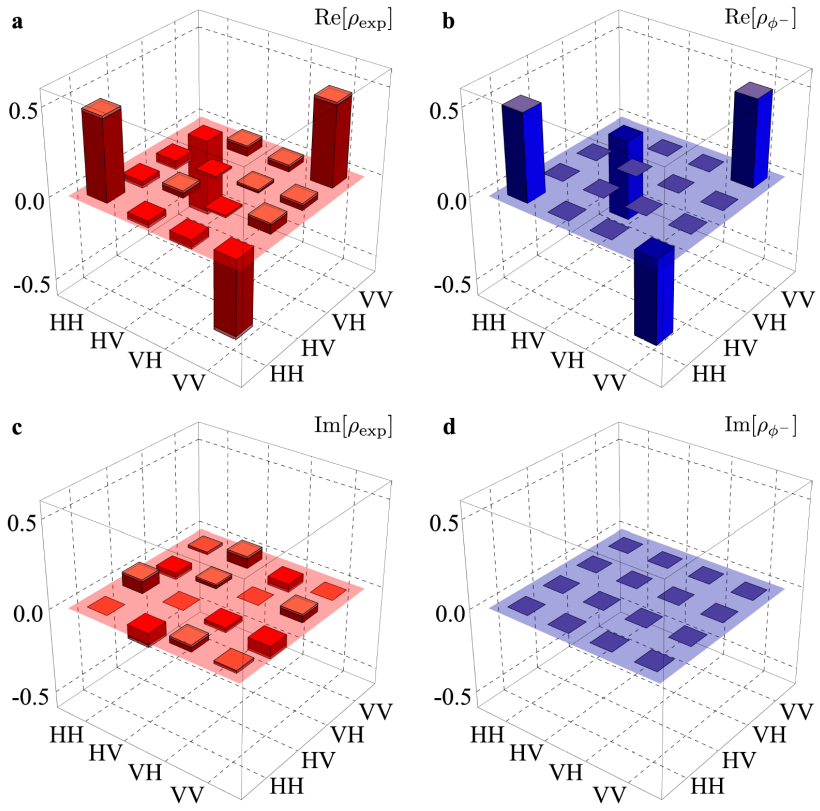

Figure 2.14. Results of the quantum state tomography performed for a value of the phase set to $\phi = \pi$, corresponding to the $|\phi^-\rangle$ Bell state. **a**, Real part of the experimental density matrix ρ_{exp}. **b**, Real part of the theoretical density matrix ρ_{ϕ^-}. **c**, Imaginary part of the experimental density matrix ρ_{exp}. **d**, Imaginary part of the theoretical density matrix ρ_{ϕ^-}. This image is taken from [10].

2.2.3 Conclusions and perspectives

We have proposed novel Mach–Zehnder interferometers to generate different quantum states of light as product, path- and polarization-entangled photon states. We have shown the versatility and the modularity of the proposed strategy based on the combination of integrated optical circuits realized in different materials. We validated the adopted design, realizing the photonic chips by femtosecond laser micromachining and characterizing properties of the resulting quantum states. We expect that these results will encourage the choice of hybrid-material approach for integrated entangled sources, since it potentially allows maximization of the performances of these devices by choosing the best substrate and component for each functionality. In particular, glass chips allow easy manipulation of all polarization states and realize both polarization-sensitive and polarization-insensitive devices, which would be hard to achieve in a monolithic approach based on a single nonlinear birefringent substrate. The main limitation of our integrated source is the low coincidence rate, which could be improved by reducing the losses of the laser-written waveguides in the nonlinear crystal or by employing other fabrication technologies, providing better transmissivities for this specific component (another advantage of

the modular approach). In perspective, the continuous wave and very low pump power required for operating this integrated source would allow the use of a compact fiber-coupled diode laser, directly connected to the device, producing a ready-to-use integrated source of spectrally degenerate entangled photons. Exploiting the modularity of the approach, it would be possible to directly add devices for photon manipulation and for performing logic operations. More complex architectures may be also devised to directly generate path-polarization hyperentangled states [247].

2.3 Hybrid entanglement distribution through OAM-supporting fiber

Entanglement is the necessary prerequisite for having non-local correlations, which are typically achieved by encoding the multiple qubits of the quantum state over different carriers. In this way indeed each carrier can be space-like separated and non-locality pointed out. However, a multipartite quantum state is feasible also using different degrees of freedom of a single carrier, thus allowing the generation of a so-called hybrid entangled state (Sec. 1.2). Despite this entangled state is no more correlated in the non-local sense, its quantum properties can be still used for quantum protocols, showing contextual behavior (Sec. 1.2.2). Hybrid states are advantageous because they allow multiple qubits to be encoded in the same carrier. On the other hand, the adoption of high-dimensional quantum states can reduce detrimental effects due to environmental interaction [6]. This is related to the ability of the single carrier to transport more information. Qubit is a two-level quantum system able to encode at most one bit of information. Achieving more information requires a d-level quantum system, i.e. a qudit (Sec. 1.1.2). Enlarging the dimension of the Hilbert space allows not only to increase the information capacity but also to encode this information using fewer carriers, thus improving the noise resilience during the propagation [6]. The standard properties of the light used to encode qudit states are the path and the arrival of the photon (time bin), or its orbital angular momentum (OAM). These degrees of freedom are indeed able to encode potentially infinite level quantum states. In particular, OAM seems to be very advantageous because it allows tuning the d parameters simply by changing the azimuthal phase of the beam (Sec. 1.1.2.2), without requiring complex spatio-temporal interferometers. Also, the entanglement can be used to improve the dimension capacity of a quantum channel, for example, using a dense coding scheme [6]. Similar results have been experimentally demonstrated by using qudit in a bipartite system [257, 258, 259].

If on the one hand the study and generation of such quantum resources are of great importance, as largely discussed, their distribution also plays a fundamental role in Quantum Communication. In particular, great interest has been devoted to the coherent distribution through optical fibers of quantum correlations, since it constitutes the cornerstone for the future quantum networks [183, 260, 261, 262]. Further, in fiber-based quantum communication it is particularly important to exploit photons within the C-band (1530 to 1565 nm), or more general telecom band, where optical fibers show minimal losses (Sec. 1.1.3).

Within this context, during a collaboration with the Technical University of Denmark, we adopted the polarization and the OAM properties of the light to generate and transmit a hybrid entangled state at telecom wavelength [11]. Due to the non-zero OAM used, the spatial profile is not a fundamental Gaussian mode (Sec. 1.1.2.2) and the quantum state of the light generated is no more transportable by using standard single-mode fibers. Therefore we demonstrated the capability of a special fiber, namely air-core fiber, to correctly transmit such state, i.e., a doughnut-shaped beam with an inhomogeneous polarization pattern, by preserving its quantum properties. The entanglement distribution between distant parties represents an important and challenging task, thus remarking the fundamental importance of our result.

2.3.1 Description of the experiment

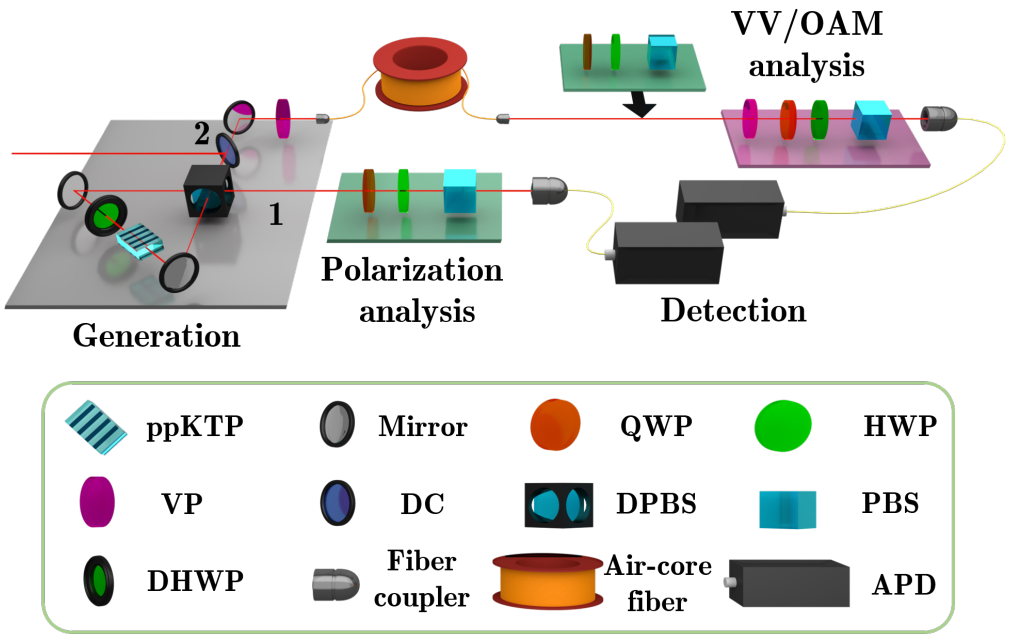

Figure 2.15. Experimental apparatus for the generation, distribution and analysis of the hybrid entangled states. Pairs of telecom polarization entangled photons are generated by exploiting a periodically poled titanyl phosphate crystal (ppKTP) in a Sagnac interferometer, which contains a dual-wavelength polarizing beam splitter (DPBS) and a dual half-wave plate (DHWP). Photons exiting along mode 1 are sent to a polarization analysis stage, composed of a quarter-wave plate (QWP), half-wave plate (HWP) and a polarization beam splitter (PBS). Photons along mode 2 pass through a dichroic mirror (DC), which separates the pump from the photons. Photons in mode 2 impinge on a vortex plate (VP) to generate a VV beam state and, in turn, the desired hybrid entangled state. The VV states are coupled to an air-core fiber and then measured with an OAM-polarization analysis stage composed of a second VP followed by a polarization analysis setup. To perform the measurements on the polarization and OAM degrees of freedom independently, an additional polarization measurement stage has to be inserted before the OAM-to-Gaussian conversion regulated by the second VP. Finally, both photons are coupled into single-mode fibers linked to avalanche photodiode single-photon detectors (APDs). This image is taken from [11].

The employed apparatus is reported in Fig. 2.15. A bulk polarization Sagnac source emits single-photon pairs at 1550 nm wavelength in an entangled polarization state $(|H\rangle|V\rangle + e^{i\phi}|V\rangle|H\rangle)/\sqrt{2}$. This preliminary state is generated by pumping the nonlinear crystal PPKTP with a continuous-wave laser at 775 nm. The pumping beam is a gaussian mode TEM_{00}, thus the same for the resulting entangled photons. The relative phase shift between the superposition terms is properly adjusted using a liquid crystal in order to generate a single Bell state:

$$|\psi\rangle_s = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2) \tag{2.12}$$

where the subscripts 1 and 2 indicate the two interferometer output modes. Let us consider the quantum state in the enlarged space polarization-OAM. For example,

$|R,m\rangle$ ($|L,m\rangle$) describes a photon with uniform right (left) circular polarization carrying $m\hbar$ of OAM. To manipulate the OAM we exploit a vortex plate (VP). VP can be considered as a nontunable Q-Plate (Sec. 1.1.2.2), that is an operator able to correlate polarization and OAM in the following way: $|L,k\rangle \xrightarrow{\text{VP}} |R,k+2q\rangle$ and $|R,k\rangle \xrightarrow{\text{VP}} |L,k-2q\rangle$, where q is the topological charge of the VP and k is the OAM quantum of the photon impinging the VP. In other words such light property is shifted of a quantity $|2q|$, whose sign depends on its polarization.

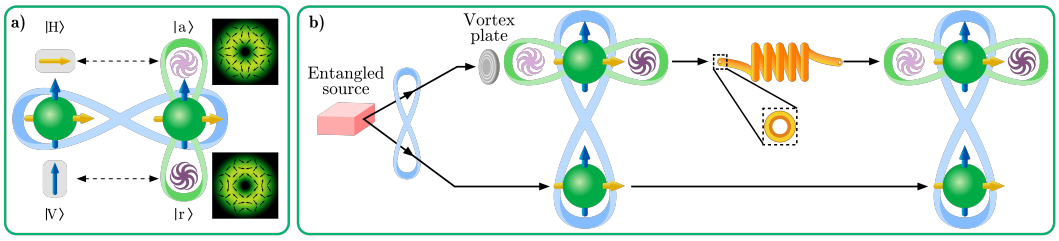

Figure 2.16. Hybrid entangled state transmission. **a)** Hybrid VV-polarization entangled photon pair generated in the experiment: entanglement in polarization of the photon pair (blue ribbon) and entanglement between polarization and OAM of the single photon (green ribbon, VV state) are sketched. The inhomogeneous polarization patterns of the VV state $|r\rangle$ (bottom) and $|a\rangle$ (up) are explicitly shown. **b)** Schematic of the experiment: hybrid VV-polarization entangled state is generated by an initial polarization entangled photon pair. One photon of the pair encodes the VV state by the action of a vortex plate. The VV beam is transmitted through the air-core fiber. Finally, state detection shows that hybrid VV-polarization entanglement (blue and green ribbons) is preserved after fiber transmission. This image is taken from [11].

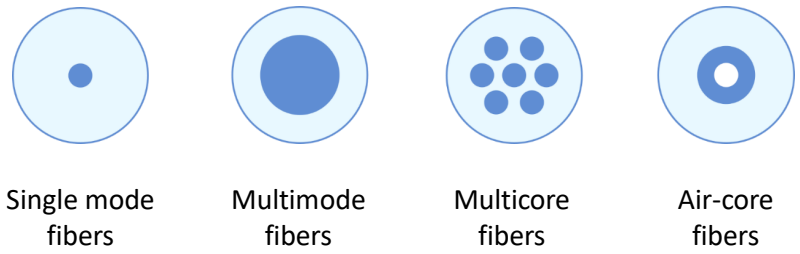

Figure 2.17. Examples of transverse profiles of optical fibers. Different fiber-cores can be developed in order to transmit different light modes. Standard employed fibers are single- and multi-mode fibers. Our experiment exploits the novel air-core fiber for transporting OAM states.

Non-zero OAM states can be conveniently described using Laguerre-Gauss (LG) mode, where the mode dependence on k corresponds to a phase change in the transverse mode profile. Therefore, varying the OAM quanta changes the transverse beam shape. As a consequence, it is impossible to transmit such states through the standard single-mode fiber, which is eigenfunction of TEM_{00} (Gaussian transverse profile). For this reason we exploit a special fiber, the air-core fiber. This fiber has the transverse profile shown in Fig. 2.17, and it demonstrated the capacity to transmit non-zero OAM quantum states [263]. A special class of states that can be transported by air-core fiber is the vector vortex (VV) beam. VV is a light state belonging to the Hilbert space spanned by $\{|R,m\rangle, |L,-m\rangle\}$ [264], that is the superposition of polarization-OAM eigenmodes ($|pol,oam\rangle$). VV beam is characterized by an

inhomogeneous polarization pattern in the transverse profile [265]. More precisely, it has an azimuthally varying polarization pattern, surrounding a central optical singularity [266, 267, 264]. Due to their distinctive polarization distributions, VV beams have shown unique features, making them appealing for different research purposes, *e.g.* microscopy [268], optical trapping [269, 270], metrology [271, 272], nanophotonics [273] and communication [274, 275, 276, 277, 278, 279, 280, 281]. Generally, each state $|pol, oam\rangle$ has a different velocity inside the air-core fiber, due to its birifrangence [263]. A possibility to correctly propagate the superposition state in polarization-OAM encoding is to employ a pre-compensation stage [282]. Another possibility is the exploitation of particular VV beam, $|r_m\rangle$ and $|a_m\rangle$, given by the equally distributed superpositions: $|r_m\rangle = (|R, +m\rangle + |L, -m\rangle)/\sqrt{2}$ and $|a_m\rangle = (|R, +m\rangle - |L, -m\rangle)/\sqrt{2}$. Indeed, these VV beams are characterized by superposition of anti-aligned states, which provides time-degeneracy into the air-core fiber, thus allowing their propagation without using a precompensation scheme [263]. If $m = 1$, radially ($|r_1\rangle$) and azimuthally ($|a_1\rangle$) polarized beams are obtained [266, 267]. In our case we exploited a VP of charge $q = 7/2$, providing an OAM order-shift of $m = |2q| = 7$, aiming at generate:

$$|r_7\rangle = \frac{|R, +7\rangle + |L, -7\rangle}{\sqrt{2}} \tag{2.13}$$

$$|a_7\rangle = \frac{|R, +7\rangle - |L, -7\rangle}{\sqrt{2}} \ . \tag{2.14}$$

The polarization patterns associated with states $|r_7\rangle$ and $|a_7\rangle$ are shown in Fig. 2.16a. In the following, we will refer to $|r_7\rangle$ ($|a_7\rangle$) as $|r\rangle$ ($|a\rangle$). In order to obtain Eqs. (2.13) and (2.14), one photon of the TEM_{00} singlet pair (photon 2) passes through the VP, thus generating a global hybrid entangled state, which reads:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle_1 |a\rangle_2 - |V\rangle_1 |r\rangle_2) \ . \tag{2.15}$$

The resulting state shows a non-local quantum correlation between photon 1 (polarization) and photon 2 (vector vortex), but having a further hybrid correlation of polarization-OAM properties along the photon 2. Then, the global VV-polarization entangled state is distributed by injecting the photon in hybrid superposition into a 5 m-long air-core fiber. The conceptual scheme is depicted in Fig. 2.16b. Finally, the hybrid entangled state is suitably measured by different measurement apparatus, in order to study independently diversified aspects. The detailed explanation of each employed measurement setup is shown in the next section.

2.3.2 Experimental results

The generated hybrid entangled states have been evaluated by using correlation tests, such as Bell test, for certifying the presence of entanglement, and fidelity test for verifying the distance from the expected ones (Sec. 1.2.4). For analyzing the degrees of freedom involved, it is necessary to study independently the polarization

and the OAM of the photons. In each of the employed measurement setups the polarization analysis is made through the standard polarization measurement stage, composed by HWP, QWP and PBS (Sec. 1.1). While the OAM measurement stage is composed by a second VP which provides the inverse operation of the first one, followed by a polarization analysis setup and single-mode fiber coupling. The VP indeed is able to convert the problem of measuring the OAM property to the polarization space, thus allowing its identification by the polarization measurement stage. This is achieved unequivocally by the final single mode-spatial filter, which traces out all OAM contributions different from the zero order.

Source state. Firstly, we characterized the entangled state generated by the source [Eq. (2.12)]. Polarization measurement setups and single-photon detectors are placed along the output modes of the interferometer, thus recording twofold detections between them. The quantum state tomography in polarization space (see Fig. 2.19a) provides a fidelity with respect to ideal singlet $F_s = (93.5 \pm 0.2)\%$. While, the Bell test provides the maximum S-value $S_s^{(raw)} = 2.67 \pm 0.01$. Subtracting the accidental coincidences from $S_s^{(raw)}$, such parameter becomes $S_s = 2.68 \pm 0.01$. The CHSH violations confirm the presence of non-local correlations in the polarization of the photon pairs.

Then, after the VP action and the fiber propagation, we analyzed the global state. This analysis is divided in two step: the study of the two-qubit hybrid entanglement between two photons, and the two-qubit intra-system correlation encoded by the photon 2.

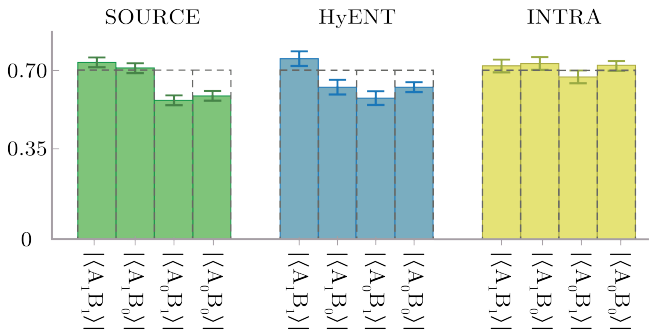

Figure 2.18. CHSH measurement operators. Expectation values moduli of the measured operators that maximize the violation of the CHSH parameter $S = \langle A_1 B_1 \rangle - \langle A_1 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_0 B_0 \rangle$. The values are relative to the polarization entangled state generated by the source (green bars), the hybrid VV-polarization entangled state (blue bars) and the intra-system entangled VV state embedded in the photon 2 and transmitted through the air-core fiber (yellow bars). All error bars are due to Poissonian statistics of the measured events. This image is taken from [11].

Hybrid entangled state (HyEnt). First, we consider the space composed by the polarization of photon 1 and VV states of photon 2, that is the space spanned by the basis $\{|H\rangle_1 |a\rangle_2 , |V\rangle_1 |a\rangle_2 , |H\rangle_1 |r\rangle_2 , |V\rangle_1 |r\rangle_2\}$. The qubit encoded in photon 1 is measured by a polarization analysis stage (green platform in Fig. 2.15). Conversely, the measurements of the VV qubit, *i.e.* photon 2, are implemented by OAM measurement stage (purple platform in Fig. 2.15). In this way, the VV states $|r\rangle$ and $|a\rangle$ are directly mapped into polarization states $|H\rangle$ and $|V\rangle$, which

are measured with the usual polarization analysis (see Fig. 2.15) [275, 283, 284]. The corresponding quantum state tomography in the four-dimensional space is reported in Fig. 2.19b. We consider as target state the ideal evolution of the density matrix describing the experimental state generated by the source. The resulting fidelity between such state and the state measured after the fiber propagation is $F_h = (97.9 \pm 0.2)\%$. Furthermore, we observe violation of the CHSH inequality, obtaining the value $S_h^{(raw)} = 2.62 \pm 0.03$ for raw data and value $S_h = 2.67 \pm 0.03$ by subtracting for accidental coincidences, thus violating by 21 and 22 standard deviations the separable limit $S = 2$, respectively.

Intra-system entangled state (Intra). Now, we focus on the VV state embedded in photon 2 and its transmission through the air-core fiber. Such analysis quantifies the quality of the VV beam state generation, transmission through the air-core fiber and conversion to the fundamental Gaussian mode. The single-photon VV states $|r\rangle$ and $|a\rangle$, (2.13) and (2.14), are maximally entangled in the OAM and polarization degrees of freedom. They correspond to single-particle entanglement states, referred to as *intra-system* entanglement. The non-separability between polarization and OAM states is not related to non-local properties, since they are relative to the same physical system. However, Bell-like inequalities can be exploited to demonstrate the single-particle entanglement, ruling out models that assume realism and non-contextuality of commuting observables, relative to such systems [134, 285, 286, 287](Sec. 1.2.2). Hence, we certify the presence of intra-system entanglement carrying out quantum state tomography and performing CHSH-like inequality in the space of polarization and OAM degrees of freedom of photon 2. Horizontally polarized heralded single photons are sent to the VP to conditionally prepare state state $|r\rangle$ for photon 2. The measurements on the polarization and the OAM degrees of freedom of photon 2 are performed independently. For this purpose, two cascaded measurement stages are needed (green and purple platforms in Fig. 2.15). A first stage performs the polarization analysis (green platform in Fig. 2.15) and then, a second stage the OAM analysis (purple platform in Fig. 2.15). The measured quantum state tomography is shown in Fig. 2.19c and the relative fidelity calculated with respect to the Bell state $|\Phi^+\rangle$ is $F_i = (99.4 \pm 0.6)\%$. The corresponding parameters S_i obtained from the CHSH-like inequality violations are $S_i^{(raw)} = 2.76 \pm 0.05$ and $S_i = 2.82 \pm 0.05$, for raw data and with data from which accidental counts are subtracted, respectively.

The set of CHSH violations measured for each state (source, HyEnt and Intra) is summarized in Table 2.1 and the mean values of the measured operators are shown in Fig. 2.18.

Three qubits HyEnt. The previous measurements have independently certified the high fidelity of both the hybrid VV-polarization entangled state and the single-photon VV beam state after propagation in the air-core fiber. Finally, we reinforced the characterization of the hybrid VV-polarization entangled state in (2.15) by considering all the degrees of freedom involved in the process, without assuming a 2-dimensional Hilbert space for photon 2 spanned by $\{|r\rangle, |a\rangle\}$. Conversely, we characterized the final state by considering the global three-qubit space spanned by the superposition of the eigenmodes $|pol\rangle_1 |pol\rangle_2 |oam\rangle_2$. In order to access to the three qubit independently has been necessary to add the polarization analysis stage for photon 1 respect to the intra-system setup (Fig. 2.15). Thus, by performing the three-qubit quantum state tomography of the transmitted state (Fig. 2.20), a final

State	Measurement time	$S^{(raw)}$	S
Source	160s	2.67 ± 0.01	2.68 ± 0.01
HyEnt	2560s	2.62 ± 0.03	2.67 ± 0.03
Intra	1920s	2.76 ± 0.05	2.82 ± 0.05

Table 2.1. CHSH violations. The CHSH violation parameters obtained from raw data (S^{raw}) and by subtracting for accidental coincidences (S), are reported for the polarization entangled state generated by the source, the hybrid VV-polarization entangled state (HyEnt) and the intra-system entangled VV state embedded in the photon 2 and transmitted through the air-core fiber (Intra).

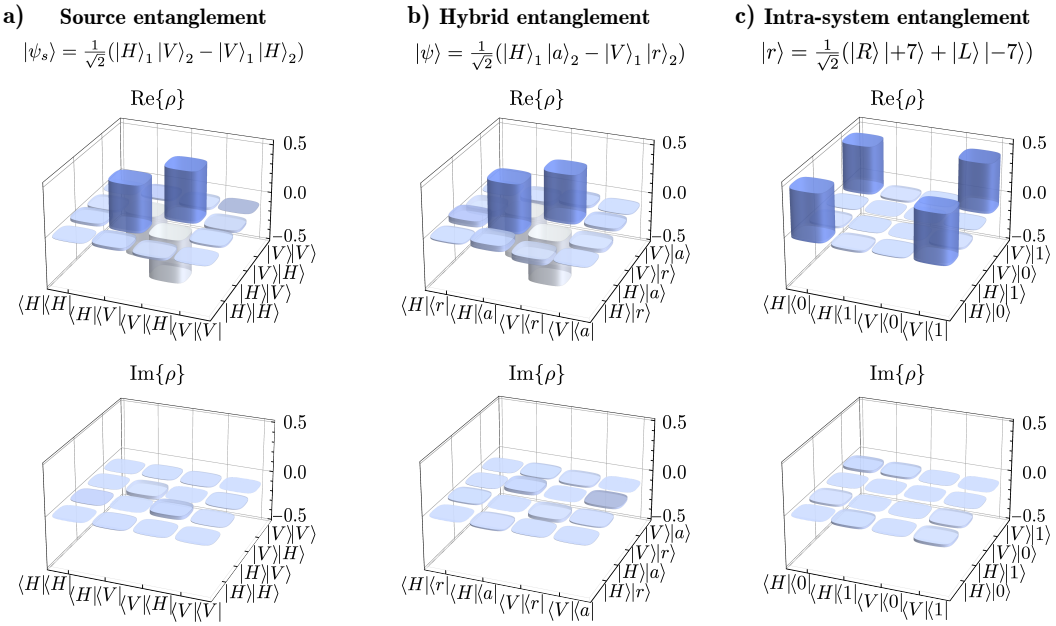

Figure 2.19. Two-qubit quantum tomographies. a) Real (top) and imaginary (bottom) parts of the measured density matrix of the polarization entangled state generated by the source, before conversion in OAM. **b)** Real (top) and imaginary (bottom) parts of the measured density matrix of the two-photon VV-polarization entangled state after the transmission of photon 2 through the OAM fiber. **c)** Real (top) and imaginary (bottom) parts of the measured density matrix of the VV state on photon 2, transmitted through the OAM fiber. The OAM states $|0\rangle$ and $|1\rangle$ in the tomography are defined by the relations: $|0\rangle \equiv (|+7\rangle + |-7\rangle)/\sqrt{2}$ and $|1\rangle \equiv i(|-7\rangle - |+7\rangle)/\sqrt{2}$. Real and imaginary parts of the experimental density matrices are reconstructed via quantum state tomographies. This image is taken from [11].

fidelity $F = (88.1 \pm 0.2)\%$ with respect to the ideal state in Eq. (2.15) is obtained.

This shows that the fiber preserves the injected state without adding noise contributions. These results provide additional evidence that the fiber is suitable for the transmission of higher-dimensional quantum states. As for the other cases, also for the three-qubit case we perform a device-independent test of the quantum correlations, showing their preservation after fiber transmission of the VV state.

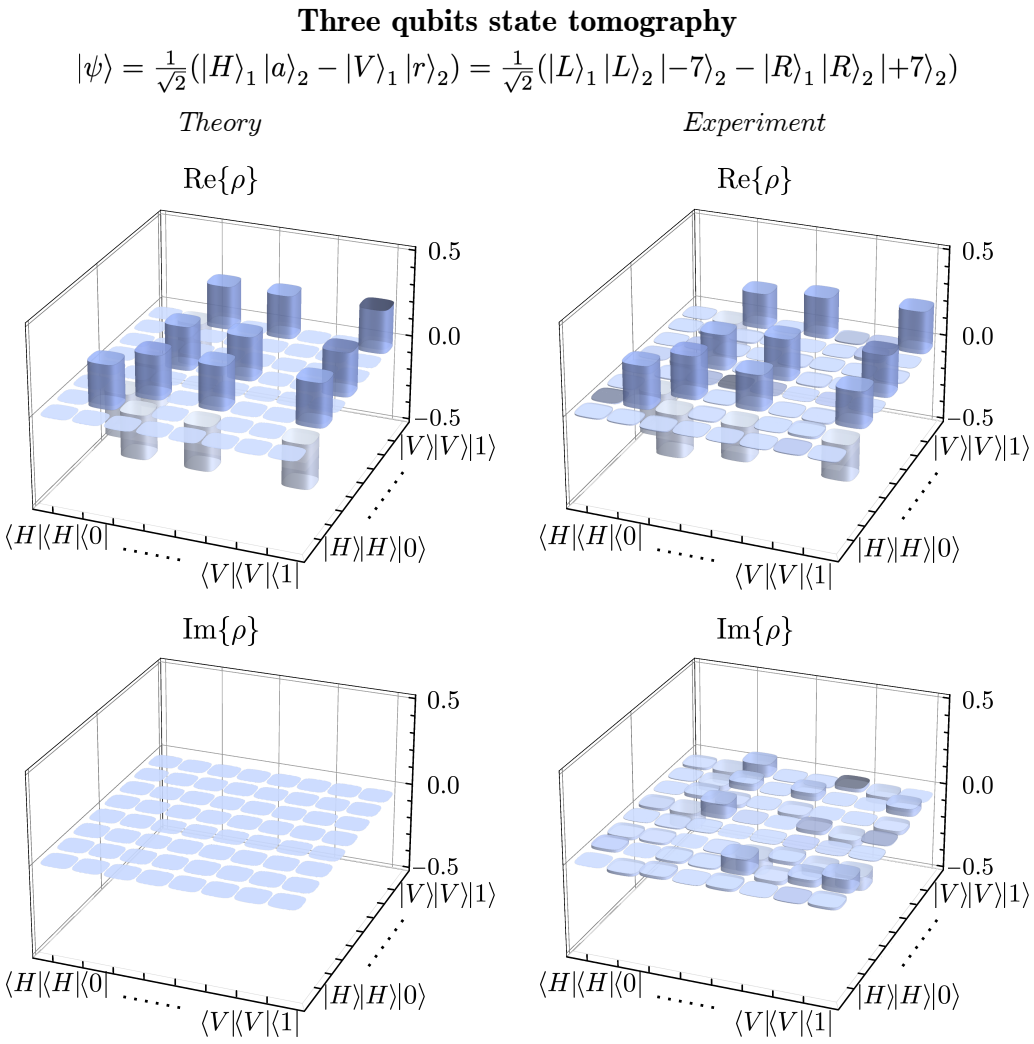

Figure 2.20. Three-qubit quantum tomography. Real and imaginary parts of the measured density matrix of the hybrid VV-polarization state in space $\{|pol\rangle_1 |pol\rangle_2 |oam\rangle_2\}$ after the fiber transmission (right) and of the theoretical density matrix of state in (2.15) (left). The OAM states $|0\rangle$ and $|1\rangle$ in the tomography are defined by the relations: $|0\rangle \equiv (|+7\rangle + |-7\rangle)/\sqrt{2}$ and $|1\rangle \equiv i(|-7\rangle - |+7\rangle)/\sqrt{2}$. Real and imaginary parts of the experimental density matrices are reconstructed via quantum state tomography. This image is taken from [11].

First, we test the Mermin-Ardehali-Belinskiĭ-Klyshko inequality (Sec. 1.2.4.2), which provides an upper bound for contextual hidden variable theories describing the correlations between observables relative to three qubits:

$$\begin{aligned} \mathcal{M} \quad \equiv \quad & |\langle A_1 B_2 C_2\rangle + \langle A_2 B_1 C_2\rangle + \\ & + \langle A_2 B_2 C_1\rangle - \langle A_1 B_1 C_1\rangle| \leq 2 \,. \end{aligned} \tag{2.16}$$

The observables A_i, B_i and C_i $(i = 1, 2)$ are dichotomic (with eigenvalues ± 1) and relative to the first, the second and the third qubit, respectively. Violation of such inequality certifies the nonclassical correlations of tripartite states. Furthermore, if a value $\mathcal{M} \geq 2\sqrt{2}$ is found, models in which quantum correlations are allowed between

just two of the three qubits (biseparable quantum models), are ruled out as well [288, 289]. The state (2.15) in the three-qubit space is able to reach the algebraic value of $\mathcal{M} = 4$ by choosing the operators: $A_1 = -\sigma_Z^A$, $A_2 = \sigma_X^A$, $B_1 = -\sigma_Z^B$, $B_2 = \sigma_X^B$, where σ_i $(i = X, Z)$ are the Pauli operators relative to photons 1 (A) and 2 (B) in the polarization in basis $\{|H\rangle, |V\rangle\}$; and $C_1 = \sigma_Z^C$, $C_2 = \sigma_X^C$, where the Pauli operators are in the OAM basis $\{|0\rangle \equiv (|+7\rangle + |-7\rangle)/\sqrt{2},\ |1\rangle \equiv i(|-7\rangle - |+7\rangle)/\sqrt{2}\}$ relative to photon 2. Measuring such operators after the VV state transmission and calculating the parameter $\mathcal{M}$, we obtain $\mathcal{M}^{(raw)} = 3.43 \pm 0.04$ from raw data, and the value $\mathcal{M} = 3.53 \pm 0.04$ by subtracting accidental coincidences. In this way, we violated the classical bound by 35 and 38 standard deviations and the quantum biseparable bound by 15 and 17 standard deviations, respectively.
Finally, we further study the correlation of the state in (2.15) by performing a Hardy test [290, 291], recently generalized in a suitable form for more than two parties by [292]. Given a system with certain null correlation probabilities, a paradox arises when other events are automatically forbidden in the framework of noncontextual hidden variable models, while they can happen within a quantum context. Since experimentally measuring null probabilities represents a difficult task, Hardy logical contradictions can be conveniently mapped into more general inequalities. In Ref. [292] an extended multi-party version of Hardy's paradox is proposed, leading to an inequality that for three qubits reads:

$$\begin{aligned} \mathcal{H} \quad \equiv \quad & P(A_1A_2A_3) - P(A_1B_2B_3) - P(A_1\bar{B}_2\bar{B}_3) + \\ & - P(B_1A_2B_3) - P(\bar{B}_1A_2\bar{B}_3) - P(B_1B_2A_3) + \\ & - P(\bar{B}_1\bar{B}_2A_3) \leq 0 \,, \end{aligned} \tag{2.17}$$

where A_i (B_i) represents a dichotomic operator A (B) acting on qubit $i = 1, 2, 3$ with eigenvalues ± 1, $\bar{B}_i \equiv -B_i$ and the probabilities $P(X_1Y_2Z_3) \equiv P(X_1 = 1, Y_2 = 1, Z_3 = 1)$. In our case, the transmitted 3-qubit state permits to maximally violate the generalized Hardy test by choosing the operators: $A_1 = A_2 = -A_3 = \sigma_Z$ and $B_1 = B_2 = B_3 = \sigma_X$ relative to the qubits $|pol\rangle_1$ and $|pol\rangle_2$ (in basis $\{|H\rangle, |V\rangle\}$) and $|oam\rangle_2$ (in basis $\{|0\rangle, |1\rangle\}$), respectively. The experimental value $\mathcal{H}$ obtained for raw data is $\mathcal{H}^{(raw)} = 0.085 \pm 0.008$ and by accounting for accidental coincidences it becomes $\mathcal{H} = 0.104 \pm 0.008$ (theoretical value for the ideal state is $\mathcal{H} = 0.25$). Such values allow to violate the noncontextual bound by 10 and 12 standard deviations, respectively. Note that the tripartite correlations obtained are generated by both contextual (intrasystem) and nonlocal (intersystem) entanglement. Thus, the correlations lie between three qubits and not between three different and spatially separated parties.

2.3.3 Conclusion and perspectives

Future quantum communication will require distributing quantum states over long distances. The protocols implemented within such systems will include the distribution of high-dimensional and entangled quantum states. Indeed, spanning Hilbert spaces of greater dimensions allows higher information capacity and noise

resilience, leading to enhanced Quantum Information processing [293, 294, 295]. In this context, VV states represent a powerful resource for classical and quantum applications.
Here, we demonstrated the feasibility of distributing complex VV states through an OAM supporting fiber, also permitting to preserve entanglement with a different system. In particular, we achieved the transmission of a VV state, presenting correlations between polarization and OAM, entangled with the polarization of a separate second photon. To fully assess the robustness to decoherence and quality of the transmitted complex entangled state, we performed quantum state tomographies, violations of CHSH-like inequalities and multipartite entanglement tests. The achieved fidelities of the transmitted state demonstrate the capability to perform high fidelity distribution in an OAM supporting fiber of a hybrid VV-polarization entangled state at telecom wavelength. In particular, the possibility to simultaneously encode and distribute information in the polarization and OAM degrees of freedom of a single particle represents a useful resource due to the higher robustness to losses, while tools for their processing have been identified [296]. This work paves the way towards the adoption of high-dimensional entanglement in quantum networks. Further perspectives of this work involve the investigation of the fiber-based distribution of different orders of OAM entangled states and their distribution over longer distances, exploiting the potential scalability arising from a fiber-based approach. Indeed, the results presented here are expected to be extended to long-distance transmission, since low mode mixing can be achieved in longer fiber [282]. Other perspectives involve interfacing of OAM integrated circuits [80, 79, 81] through OAM supporting fibers for future quantum networks.

2.4 Experimental quantum network

Bell's test has been one of the most relevant results of the last 60 years in Physics. However, only recently the phenomenon of Bell nonlocality has been proven in a loophole-free manner in a series of independent experiments [124, 125, 126, 127, 128]. Beyond its importance at fundamental level (Sec. 1.2.2), it provides an indispensable witnessing tool (Sec. 1.2.2), at the heart of many protocol of Quantum Information, such as in Quantum Metrology, Quantum Cryptography [123] and Communication [3], and randomness generation [297, 298]. The generalization of Bell inequalities for more complex scenarios brought first to the bilocal scheme, i.e. the one adopted for entanglement swapping, and then to more general multipartite structures (Sec. 2.1.2). This further step requires not only the definition of general Bell-like inequalities but also the possibility to distribute and certify entanglement between any number of parties. This is one of the most interesting theoretical investigations as much as from the experimental point of view. Such study represents only a part of the quantum network investigation, which is one of the most attractive and active fields of research, aiming at the so-called quantum internet [9, 299]. The first aspect is the generation of multipartite entanglement to be distributed, where an ideal possibility would be to exploit the GHZ states [300]. These states however suffer from high experimental drawbacks [301], thus do not provide a good near-term solution. Multipartite scenarios are much more likely to be composed of independent sources, each one generating small size entangled states but at much higher quality and rate. The second aspect concerns the study of distributed quantum correlations inside more complex networks and their experimental realization. Despite its importance and the theoretical advances, the non-locality has been so far experimentally demonstrated only in the simplest tripartite system of a bilocal scheme [128, 189, 190, 191, 302, 193].

We studied the extended n-local scenario [12], providing the quantum enhancement in Bell terms achievable in the general star-shaped multinode scheme. Then, we provided a proof of principle demonstration of how to move beyond experimental bilocality, realizing such a quantum network in which we varied the number of nodes from 2 ($n = 1$) up to 5 ($n = 4$). We distributed and certified the presence of non-local quantum correlation between states generated by independent entangled photon sources, pumped by different lasers, in order to fulfill all assumptions of n-locality scenario (see Sec. 2.1.2). Our photonic approach is scalable and allows for the testing of other general networks of increasing size and complexity. Thus, it represents a building block for future quantum internet implementations [9, 299].

2.4.1 Description of the experiment

Any n-locality scheme involving one central node and up to 4 external nodes is reported as DAG representation (Sec. 2.1.2) in Fig. 2.21. In order to realize such scenarios we exploited up to 4 different laboratories, each having one independent source of entangled photons in polarization (Fig. 2.22).

These are based on the non-linear interaction with 4 independent pump lasers, having even different electrical sources. This is an important feature in order to

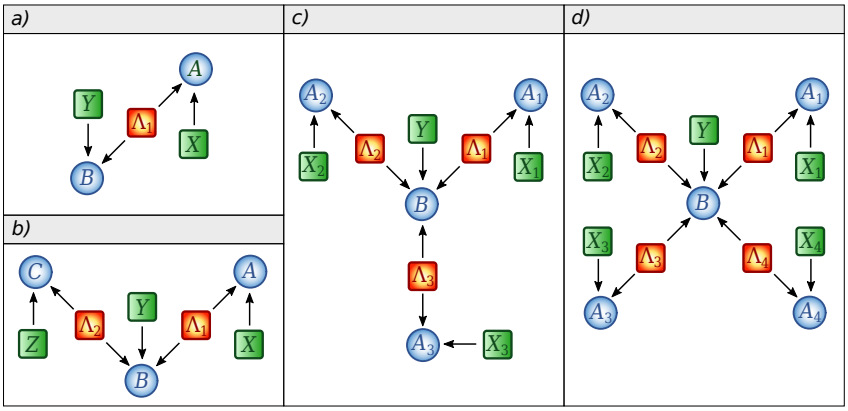

Figure 2.21. Directed Acyclic Graph (DAG) representation for the star scenario with different number of sources.
a) Causal structure of the standard Bell scenario in which a single source Λ mediates the correlations between the two measurement stations with outcomes A and B and measurement choices X and Y, respectively. **b)** DAG for the bilocal scenario where two independent hidden variables Λ_1 and Λ_2 distribute the correlations to three measurement stations with outcomes A_1, A_2 and B and choice of measurements X_1, X_2 and Y, respectively. **c-d)** DAG for the star-network with three and four independent sources $\Lambda_1, \Lambda_2, \Lambda_3$ and $\Lambda_1, \ldots, \Lambda_4$ respectively. Each non-central measurement station has outcomes A_i (measurement choices X_i) and the central has outcome B (measurement choices Y). This image is taken from [12].

completely realize the n-locality assumptions. Each of the n peripheral nodes (called A_i) is connected through the source Λ_i to the central node of the network (called B). Central and external nodes can perform k measurements described by dichotomous observables. The peripheral nodes are placed into the different laboratories: Lab 1, Lab 2, Lab 3 and Lab 4 (Fig. 2.22). The central node B, which is located in Lab 1, has to perform not only the measurement over its own source, but also reveal the photons arriving from other laboratories. For these reasons, polarization measurement apparatuses composed of HWP and PBS are present in each external node, unlike for the central one, where up to four different polarization analyzers can be found (depending on the specific employed scheme). Singlet states in polarization encoding are prepared in each laboratory and a complex synchronization is made between the central part and all peripheral ones. The distribution of light in the network occurs through single-mode fibers and their compensation is made in order to correctly control the polarization states. The maximum fiber length is 25 m. As shown is Sec. 2.1.2, labeling the measurements for B and external nodes A_i by y and x_i and their outcomes by b and a_i, respectively, the LHV in general star-shaped scheme with $n+1$ nodes reads [Eqs. 2.7,2.8]:

$$S_n^k = \sum_{i=1}^{k} |I_i|^{1/n} \leq k - 1 \tag{2.18}$$

$$\text{where } I_i = \frac{1}{2^n} \sum_{x_1,\ldots,x_n=i-1}^{i} \langle A_1^{x_1} \cdots A_n^{x_n} B^{i-1} \rangle \tag{2.19}$$

with $A_i^k = -A_i^0$ and $\langle A_1^{x_1} A_2^{x_2} \cdots A_n^{x_n} B^y \rangle$ being the expectation value of the measure-

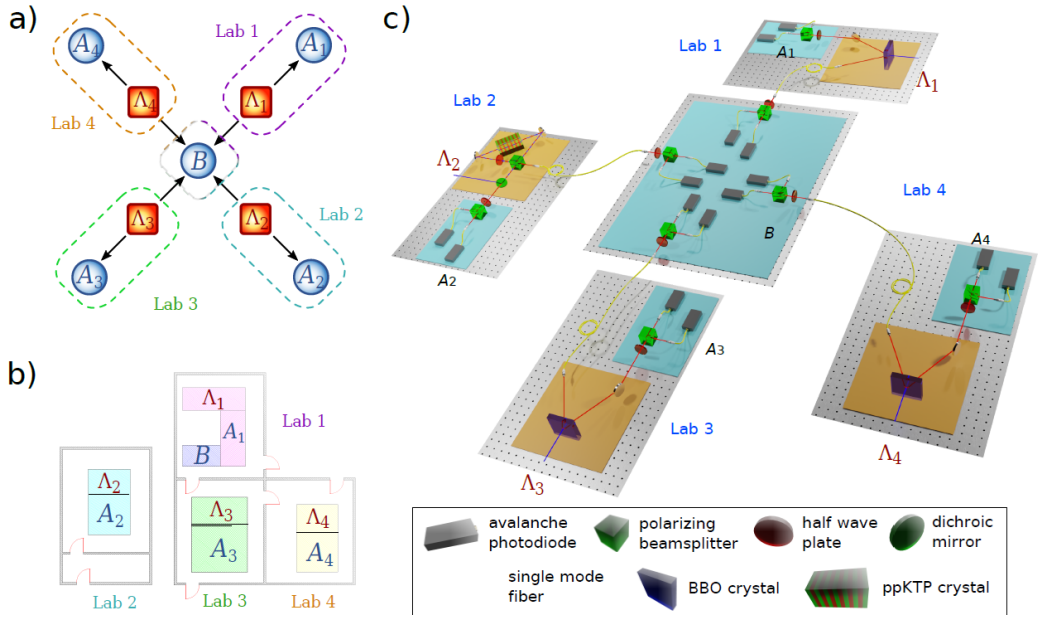

Figure 2.22. Experimental apparatus. a) Four independent polarization-entangled photon pair sources and five measurement stations are available for the experimental realization of violation of the chained n-locality inequality (2.18) in a star-network configuration. **b)** Physical location of the laboratories and scheme of the experimental apparatus. Distinct laboratories contain one source and one measurement station each, with the exception of Lab. 1, which also contains the central node B of the star-network on a separate optical table. **c)** The entangled photon sources $\Lambda_1, \Lambda_3, \Lambda_4$ are realized using a Beta-Barium Borate (BBO) crystal, pumped in a pulsed regime, which emits photon pairs at 785 nm using spontaneous parametric down-conversion (SPDC) of type II. The source Λ_2 instead is pumped in continuous-wave regime and employs a periodically poled KTP crystal placed inside a Sagnac interferometer to generate entangled photon pairs at 808 nm via a type II SPDC process. Single photons are then measured in polarization using a half-wave plate (HWP) followed by a polarizing beam splitter (PBS). This image is taken from [12].

ments outcomes of the $n+1$ nodes:

$$\langle A_1^{x_1} A_2^{x_2} \cdots A_n^{x_n} B^y \rangle = \sum_{a_1,a_2,\ldots,a_n,b=0,1} (-1)^{a_1+a_2+\ldots+a_n+b} p(a_1, a_2, \ldots, a_n, b|x_1, x_2, \ldots, x_n, y). \tag{2.20}$$

Considering single states shared between the nodes, the Eq. (2.18) is violated by the presence of quantum correlations, and the corresponding quantum bound is:

$$S_n^k = k \cos(\pi/2k). \tag{2.21}$$

This bound depends exclusively on the number of measurement settings k, but not on the number of nodes. A list of classical and quantum bounds varying n and k with values $2, 3, 4$ is shown in Table 2.3. It is possible to demonstrate that the bound (2.21) is the maximum achievable by quantum states. Further, its reachability is guaranteed even by using separable measurements [193, 194, 303]. This characteristic is fundamental, as allow a scalable implementation of the apparatus. Indeed, in the central node the general measurement strategy is represented by measurement in an entangled basis, which can require measurements in GHZ basis to reveal the presence of non-locality [8]. However, realization of measurements involving simultaneously n

physical systems is usually a hard task, requiring a difficult synchronization between different sources. Furthermore, complete Bell measurements cannot be implemented using linear optics, without resorting to hybrid or nonlinear approaches [304, 186]. To obtain the maximum quantum violation of inequality (2.18), all the peripheral parties A_i must perform the following projective measurements on their subsystem:

$$\begin{aligned} |\Psi^0_{k,x}\rangle &= \cos(x\pi/2k)\,|0\rangle + \sin(x\pi/2k)\,|1\rangle\,, \\ |\Psi^1_{k,x}\rangle &= \cos(x\pi/2k)\,|1\rangle - \sin(x\pi/2k)\,|0\rangle\,, \end{aligned} \tag{2.22}$$

for each setting $x_i = x$. In turn, the central node B measures each of its n subsystems in the local basis:

$$\begin{aligned} |\Phi^0_{k,y}\rangle &= \cos\frac{(2y+1)\pi}{4k}\,|0\rangle + \sin\frac{(2y+1)\pi}{4k}\,|1\rangle\,, \\ |\Phi^1_{k,y}\rangle &= \cos\frac{(2y+1)\pi}{4k}\,|1\rangle - \sin\frac{(2y+1)\pi}{4k}\,|0\rangle\,, \end{aligned} \tag{2.23}$$

for each setting $y_i = y$, where the index i refers to the system B shares with the i-th non-central part. The resulting measurement corresponds to $B_y = B^1_y \otimes \cdots \otimes B^n_y$, where B^j_y represents the measurement performed on each subsystem. Hence, to evaluate the quantum violation in (2.18), we need to perform $k2^n$ combinations of measurement settings, 2^n for each term I_i appearing in (2.18). In the following section, the experimental results obtained for each scenario, varying n from 1 to 4 with $k = 2, 3, 4$, are shown.

2.4.2 Experimental results

The schemes described above have been experimentally tested. Notably, measurement and data analysis for each configuration was done using sophisticated software, whose detailed description can be found in Supplementary information of [12]. In particular, the photon detection events were collected and timed by a different time tagger device for each party, located in the corresponding laboratory (see Fig. 2.22b). For each 1 s of data acquisition the events were sent to a central server, along with a random clock signal shared between all the time-taggers, which was used to synchronize the timestamps of events relative to different devices. To filter out part of the noise the raw data was first pre-processed by keeping only double coincidence events for each photon source, using a narrow coincidence window of 3.24 ns. Then coincidence events between multiple sources were counted every time one of such double coincidence event was recorded for each source in a window of 80 μs.

Characterization of the sources

In our experiment, we exploited four different photon sources generating polarization entangled photon pairs in the singlet state[305]: $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ through a type-II SPDC process (Sec. 1.2.3). Within three laboratories (Lab 1,

Lab 3 and Lab 4), the generation was carried out by pumping 2 mm-thick BBO crystals with a Ti:Sapphire mode locked laser, with repetition rate of 76 MHz. The generation in Lab 2, instead, was accomplished with a continuous wave diode laser which pumped a PPKTP crystal inside a Sagnac interferometer [147, 306]. The photons generated in all the sources are filtered in wavelength and spatial mode by using narrow band interference filters and single-mode fibers, respectively. In order to characterize the quality of the entangled state we performed CHSH tests (Sec. 1.2.2) between each peripheral node and the central one. This is made by local measuring one photon of the generated pair, while revealing the other one in the central laboratory after propagation in fiber. The results for each source are shown in Table 2.2.

Source	Crystal	Lab.	λ(nm)	Pump laser	Two-fold CC^1 (Hz)	Experimental $CHSH^1$	Estimated Visibility
Λ_1	BBO	1	785	Pulsed (76 MHz)	25 000	2.408 ± 0.018	0.763 ± 0.010
Λ_2	ppKTP	2	808	Continuous	45 000	2.395 ± 0.021	0.755 ± 0.012
Λ_3	BBO	3	785	Pulsed (76 MHz)	1 000	2.388 ± 0.020	0.751 ± 0.011
Λ_4	BBO	4	785	Pulsed (76 MHz)	5 000	2.463 ± 0.013	0.793 ± 0.007

Table 2.2. Experimental details for the different laboratories: In the table are listed the crystals, wavelength, type of pump laser, coincidence rate and experimental violation of the CHSH inequality within each laboratory. The visibilities were obtained by exploiting the noise model and the experimental violation of the CHSH inequality. The superscript ^{1} refers to the average values upon all the collected data.

Violations of n-locality with $k = 2$ measurement settings

First, we consider the case with two measurement settings ($k = 2$, see Fig. 2.23). In our apparatus such configuration is realized by correctly tuning HWPs of external nodes and the central one: the optimal measurements (2.22) and (2.23) are obtained by setting B to angles 11.25° and 33.75°, respectively for $y = 0$ and $y = 1$. While each involved external node $A_i^{x_i}$ has to be set to angles 0° and 22.5°, respectively for $x_i = 0$ and $x_i = 1$. All experimental results for $n = 2, 3, 4$ show non-local violation of (2.18) and are reported in Table 2.3. In particular, we can realize 6 possible configurations having $n = 2$ in our network. Here, we obtained a maximum value of $S_{\max}^{\text{obs}} = 1.218 \pm 0.002$, violating the classical bound by 109 standard deviations. Instead, for $n = 3$ and $n = 4$ the number of possible configurations are 4 and 1, obtaining maximum values of $S_{\max}^{\text{obs}} = 1.199 \pm 0.004$ and $S_{\max}^{\text{obs}} = 1.192 \pm 0.005$, violating of 50 and 38 standard deviations with respect to their classical bounds, respectively. Notably, for each considered configuration, the same values of S should be in principle obtained by using a unique source shared between all network nodes, as shown in Fig. 2.23. This possibility makes our assumption about the independence of the sources still more fundamental, which is realized in our setup as previously discussed.

Violations of n-locality with $k > 2$ measurement settings

Despite the study with $k = 2$ is sufficient to show the non-locality of the system, as well as being more experimentally feasible and then a scalable perspective, the investigation of $k > 2$ can be still interesting, as it brings some advantages. This is the case for instance of DI protocols, which can be demonstrated while using less stringent requirements [200]. Therefore, we consider and realize the n-locality scenario with

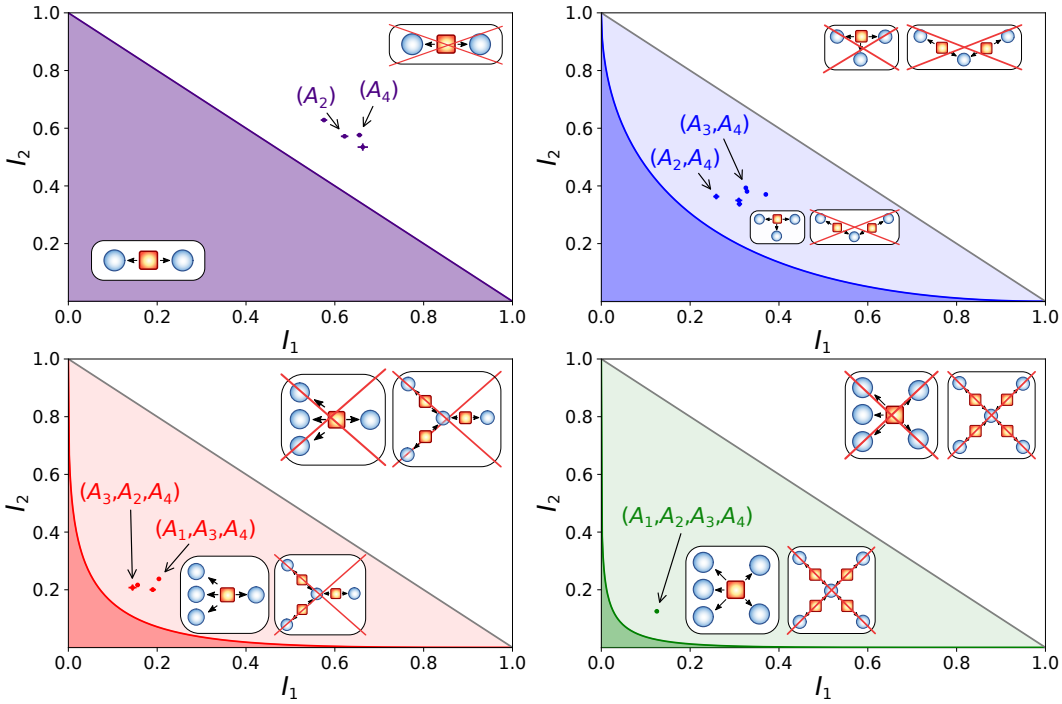

Figure 2.23. Experimental correlations represented in the I_1, I_2 plane ($k = 2$ settings). The purple, blue, red and green regions represent the classical correlations for 1-, 2-, 3- and 4-local scenarios, respectively. The 2-local case corresponds to the bilocal inequality while the 1-local reduces to the paradigmatic CHSH inequality. For $n \geq 2$ the gray line bounds the correlations allowed by a local model with no assumption on sources independence. The green point represents the I_1, I_2 values measured in the case of $n = 4$ sources. The red, blue and purple points represent the experimental values for all the possible combinations of laboratories which are 4, 6 and 4 in the 3-, 2 and 1-star cases, respectively. Error bars represent the standard error of the mean taken over different sequential acquisitions. This image is taken from [12].

$k = 4$. This choice required several experimental drawbacks, as the necessity to realize 4- 6- and 8-fold coincidence events, together with the measure in 1024 different combinations. Nevertheless, we were able to experimentally demonstrate the violation of the corresponding classical bounds. All results are reported in Fig. 2.24 and Table 2.4. In the particular case of $n = 4$ with $k = 4$, we surpassed the bound of 71 standard deviations, providing a value $S_{\max}^{\text{obs}} = 3.157 \pm 0.002$. Our experimental results are also compatible with models including noise effects. Note that in our demonstration the measurements are not performed with space-like separation and so we do not close the locality loophole. However, we demonstrate that reducing the coincidence window the quantum violation is still valid (Fig. 2.25), thus providing an enforcement of the assumption about the absence of mutual causal influence between the parties.

Noise dependence of n-locality violation

Different sources of noise must be considered within the experimental implementation. The noise can be taken into account by adding decoherence terms when modelling the quantum state shared by the parties [189]. The photon pairs in our experiment are generated in the singlet state ρ_{sing}, that in the base

n Sources	Combination	I_1	I_2	S^{obs}
1	A_1	0.576 ± 0.007	0.628 ± 0.002	1.204 ± 0.009
	A_2	0.622 ± 0.008	0.572 ± 0.006	1.197 ± 0.010
	A_3	0.662 ± 0.011	0.534 ± 0.012	1.194 ± 0.010
	A_4	0.655 ± 0.006	0.576 ± 0.004	1.232 ± 0.007
2	A_2, A_4	0.259 ± 0.007	0.363 ± 0.010	1.111 ± 0.011
	A_3, A_4	0.325 ± 0.004	0.393 ± 0.004	1.198 ± 0.005
	A_3, A_2	0.310 ± 0.008	0.350 ± 0.010	1.147 ± 0.011
	A_1, A_4	0.3279 ± 0.0017	0.381 ± 0.003	1.190 ± 0.003
	A_1, A_2	0.311 ± 0.006	0.337 ± 0.009	1.138 ± 0.010
	A_1, A_3	0.370 ± 0.003	0.371 ± 0.003	1.217 ± 0.003
3	A_3, A_2, A_4	0.145 ± 0.009	0.207 ± 0.010	1.116 ± 0.015
	A_1, A_2, A_4	0.156 ± 0.005	0.217 ± 0.007	1.139 ± 0.009
	A_1, A_3, A_4	0.204 ± 0.005	0.238 ± 0.005	1.208 ± 0.006
	A_1, A_3, A_2	0.190 ± 0.007	0.200 ± 0.008	1.160 ± 0.010
4	A_1, A_2, A_3, A_4	0.125 ± 0.005	0.125 ± 0.005	1.190 ± 0.008

Table 2.3. Experimental results for different number of sources n and $k = 2$ measurement settings. The table shows the experimental values of I_1, I_2 and S^{obs} for each possible combination of parties $\{A_1, \ldots, A_4\}$.

n Sources	k Settings	S^{obs}	Classical	Violation σ	S^{sim}	S^{Q}
2	2	1.217 ± 0.003	1	72	1.201 ± 0.007	1.41
	3	2.253 ± 0.002	2	127	2.237 ± 0.010	2.60
	4	3.2261 ± 0.0014	3	162	3.182 ± 0.014	3.70
3	2	1.208 ± 0.006	1	35	1.211 ± 0.005	1.41
	3	2.227 ± 0.003	2	76	2.225 ± 0.009	2.60
	4	3.195 ± 0.002	3	97	3.165 ± 0.013	3.70
4	2	1.190 ± 0.008	1	24	1.207 ± 0.005	1.41
	3	2.177 ± 0.005	2	35	2.218 ± 0.008	2.60
	4	3.135 ± 0.004	3	34	3.154 ± 0.012	3.70

Table 2.4. Experimental results for different number of sources n and measurement settings k. The values of $S^{\text{obs}}, S^{\text{sim}}$ and S^{Q} are the observed, the expected and the maximum quantum violation respectively. S^{sim} has been computed using the state visibility estimated by Bell violations performed in each single source.

$\{|HH\rangle, |HV\rangle, |VH\rangle, |VV\rangle\}$ can be expressed by the following matrix form:

$$\rho_{\text{sing}} = \frac{1}{2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{2.24}$$

In particular, two different classes of noise affect the SPDC sources [307]:

- White noise, which consists in an isotropic depolarization of the states:

$$\rho_{\text{w}} = v|\psi^-\rangle\langle\psi^-| + (1-v)\frac{\mathbb{I}}{4}, \tag{2.25}$$

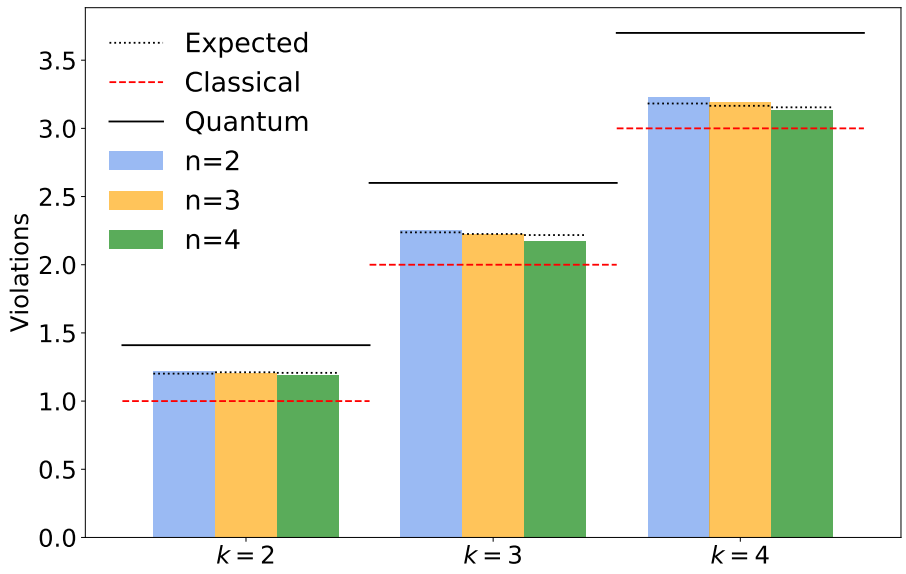

Figure 2.24. Experimental violation of the chained Bell inequality (2.18) for a $2, 3$ and 4 sources n, depicted in different colors, and $2, 3$ and 4 measurement settings k. Solid and dashed lines represent the classical and quantum bounds in (2.18) respectively, while dotted lines represent the expected value of the violation for noisy states. Measurement errors are not visible in the plot, numerical values are summarized in Table 2.4. This image is taken from [12].

where $\frac{\mathbb{I}}{4}$ is the completely mixed state.

- Colored noise, which is depolarization along a preferred direction, intrinsic of the SPDC generation process, described by the following matrix:

$$M_{\text{colored}} = \frac{1}{2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{2.26}$$

The resulting noisy state, then, is the following:

$$\rho_c = v|\psi^-\rangle\langle\psi^-| + (1-v)M_{\text{colored}} = v|\psi^-\rangle\langle\psi^-| + \frac{(1-v)}{2}(|\psi^-\rangle\langle\psi^-| + |\psi^+\rangle\langle\psi^+|). \tag{2.27}$$

The final state can be modelled combining these different contributions in a normalized form:

$$\rho = v|\psi^-\rangle\langle\psi^-| + (1-v)[\lambda\frac{|\psi^-\rangle\langle\psi^-| + |\psi^+\rangle\langle\psi^+|}{2} + (1-\lambda)\frac{\mathbb{I}}{4}], \tag{2.28}$$

where the parameters v and λ represent the total noise and the fraction of colored noise, respectively. The effects generated by white and colored noise can be extended

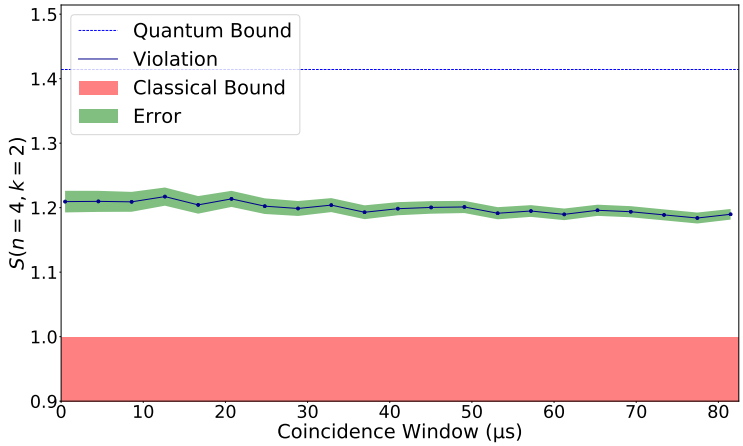

Figure 2.25. Signal for violation as a function of the coincidence window length: The coincidences identified by our software depend on the choice of time window within which events are considered as simultaneous. In order to choose the best value for this time interval and to check how this value influences the signal for violation, we analyzed $S(n,k)$ as a function of the window. In the plot we are showing the violation in the case $n=4, k=2$, evaluated with the data from multiple exposures for a total time of 34.2 s. The blue line is the experimental value of $S(4,2)$. The green region represents the Poissonian error of the expected violation computed from the number of two-fold coincidences observed. The blue dashed line is the quantum bound while the red region is the value of $S(4,2)$ achievable within a classical model. This image is taken from [12].

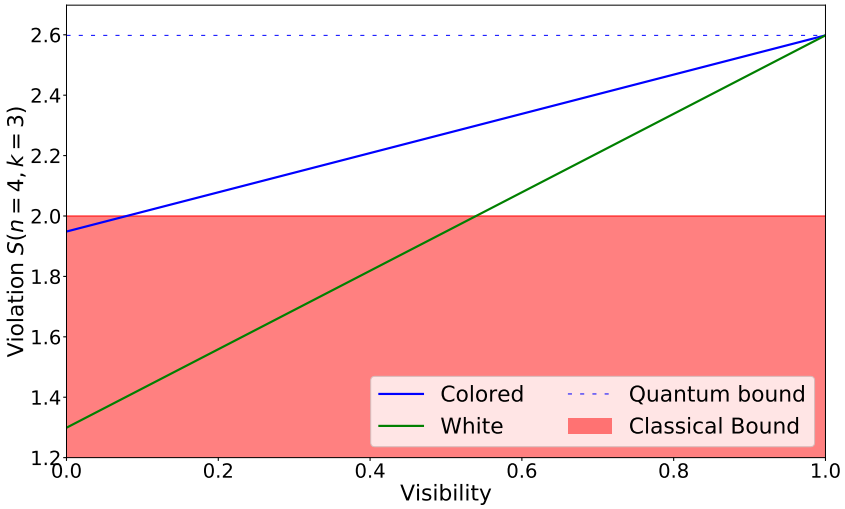

Figure 2.26. Comparison of different noise types affecting S: Plot of the simulation results for the S value in a 4-points star-network, where each agent performs $k=3$ measurements. As the visibility decreases, the violation S drops from the quantum to the classical bound. The blue curve refers to violation against coloured noise, while the green one to violation against white noise. We observe that the amount of violation is more sensitive to white noise. This image is taken from [12].

to the more complex case of the network, where all of the nodes contain separate noise contributions. However, as preliminary analysis we consider noise parameters equal for all of the sources. In such case, the action of both white and colored noises not only decrease the visibility of the singlet states, but is also observed in the

reduction of the amount of violation of the chained n-locality inequality [Eq. (2.20)]. By comparing quantitatively the two effects for the same noise strength, we observe that white noise provides a larger reduction of S. An example of this behavior is depicted in Fig. 2.26 that shows how white and colored noise affects the experimental violation for the particular case of 4-nodes star-shaped network, where each agent performs $k = 3$ measurements. The more general model, where every source has individual noise parameters, has to be used for an overall laboratory-efficiency estimation. From the CHSH violations of each entangled source, we inferred the experimental visibility (Table 2.2), that is the amount of noise v affecting each source [Eq. (2.28)]. Then, for our generation method, it is known [307] that the white and colored noises affecting the generated pair are correlated. In particular, we assume the amount of white noise to double the colored one, i.e. $\lambda = \frac{1}{3}$ in Eq. (2.28).

2.4.3 Conclusions and perspectives

Despite the importance of Bell-like test in Quantum Information protocols, its experimental investigation over more general scenarios, such as complex quantum networks, is still almost uncharted territory. Here, we realized the first experimental implementation of a star-shaped quantum network, consisting of an increasing number of nodes, independent entangled sources and laboratories, besides the measurement settings. Lately, this topology has received particular attention [302, 193, 194, 303, 308]. Via our platform, we detected nonlocal correlations among the nodes of the multipartite networks, by violating polynomial chained Bell inequalities. Notably, we showed that maximum quantum violation is achievable by using separable measurements, representing a significant advantage from the experimental side. Our implementation relies on a scalable approach, which paves the way to the experimental investigation of future quantum networks, such as quantum internet [299], nonlocality of topologically different scenarios [198], secret sharing involving multiparties protocols [309, 310, 95], as well as tests for device-independent protocols of information processing [200]. We didn't provide a locality loophole-free demonstration, but showed the possibility to improve the security by reducing the coincidence interval which approximates the simultaneity of the events. This approach is limited only by the rate of the sources and therefore can be controlled. As in our scheme the sources are all independent, the possibility of tuning these parameters, rate and interval time, becomes a really interesting chance in the establishment of any quantum network. For instance, this versatile structure can be used for cryptographic tasks to design the Lee and Hoban proposal [200], or to study new attractive structures, such as triangle network [198] or linear chain topologies underlying quantum repeaters [95].

2.5 Long-distance quantum key distribution

The most important part of communication is providing a secure way to exchange information between the parties. This is achieved by cryptographic protocols that are commonly based on exchanging a secret key to encrypt the message, which must be owned only by the communicators. Classically, this approach can so far guarantee a high level of security, but not total. Quantum key distribution (QKD) paves the way to a new level of security, having no classical counterparts (Sec. 2.1.3). This is because its strength depends on the physical laws of Quantum Mechanics and not from assumptions over the computational capability of some eavesdropper. Using photons for quantum communication represents a really convenient choice, able to realize secret communication even within quantum networks [5]. In this framework several scenarios, exploiting different configurations and protocols has been demonstrated [311, 312, 313] (Sec. 2.1.3.1). BB84 [314] was the first protocol to guarantee unconditional communication security beyond any classical approach. Entangled-based protocols can give access to improved security, such us Ekert91 [123]. The exploitation of EPR non-locality [315, 123] establishes another crucial tool for the prevention of key errors, and a subsequent improvement on security of the communication procedure against individual attacks [316, 317]. Finally, under certain experimental requirements, it could also provide device-independent operation [318, 319]. Despite proof-of-principle demonstrations, so far QKD can not provide a real quantum alternative to the classical approach, due to technological limitations. One of the most important drawbacks in photonic QKD is the multi-photon emission of single-photon sources [320], which allows different hacking strategies, such as beam splitting [150] and number splitting [151] attack (Sec. 2.1.3.3). The short-term solution is the adoption of quasi-deterministic single-photon sources, which aim to become deterministic in the future. On-demand photon emitters offer a good solution to these issues at the hardware level [321] in order to make the photon distribution nearly unassailable. This feature is measured by the auto-correlation function $g^{(2)}(0)$ of the source, indicating the photon number distribution of the light (Sec. 1.2.3). Sub-Poisson light with low $g^{(2)}(0)$ can improve communication security even in presence of channel losses [322, 323]. Semiconductor quantum dots (QDs) are a promising platform for the accomplishment of all these tasks, due to their low multi-photon emission rate [159], increasing brightness [324, 325] and on-demand production of high-purity entangled states [326]. The other fundamental point to address the real-world scenario in quantum communication concerns testing the infrastructure suitable for intra-city communication. The most viable technology in this direction is represented by fiber networks and free-space channels (Sec. 1.1.3). The former provides the most simple and comfortable photonic platform for short-range communication, within 100 km for guaranteeing sufficient quantum key rates. The latter becomes the necessary solution to allow more distant communications, by providing lower absorption losses in long-space propagation. Indeed, such losses scale exponentially in fiber, while scaling only quadratically in free space. The ultimate solution, able to cover international distances, is represented by satellite-based communication, which demonstrated QKD beyond 1000 km [99, 102]. In this solution indeed the light propagating from a satellite to another one experiences negligible absorption losses due to propagation in a quasi-free atmosphere area.

In this context, we realized the first experimental demonstration of a QKD E91 protocol having a quasi-deterministic source, a quantum dot, between parties distant more than 250 m [13]. So far, the application of QD-based light sources has focused

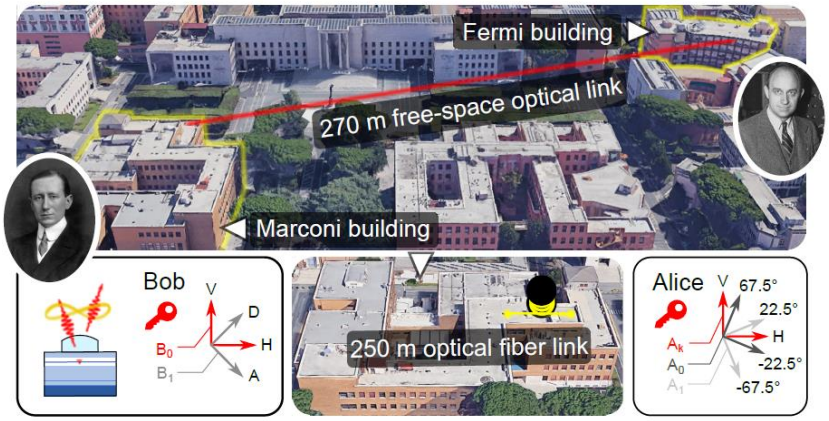

Figure 2.27. Entanglement-based QKD and optical links overview. Entangled photon pairs generated by a single QD are shared across the Sapienza University campus in Rome over a 270 m free-space distance and, in addition, between two laboratories in the same building via a 250 m SMF. Map data: Google Earth. We illustrate the main concepts of the asymmetrical Ekert approach: after traveling through the optical link connecting the users, the photons are measured by Alice and Bob on the measurement bases $\{A_k, A_0, A_1\}$ and $\{B_0, B_1\}$ in the Fermi and Marconi building respectively. In this case, the combination of the horizontal and vertical polarization states $\{A_k, B_0\}$ constitute the basis to share the secure key. In parallel, the other pairs ensure verification of the entanglement quality, by measuring the Bell parameter of the two-photon state. This image is taken from [13].

on single-photon prepare-and-measure protocols, exploring polarization [323, 327] and time-bin encoding [328], electrical [329] and optical pumping, lab tests and field demonstrations [330], possibly even with spectral multiplexing [331]. Most recent works foresee even the possibility to outperform state-of-the-art solutions based on the decoy-state protocol and weak coherent pulse sources [332]. One pioneering demonstration of the entanglement-based BBM92 protocol displaying abysmal throughput [333]. Moreover, in none of these works entangled photons have been generated on demand, one of the key features distinguishing QDs from standard sources based on parametric down-conversion. We adopted a version of E91, proposed by [229], which allows some experimental advantages with respect to the original implementation [123] (Sec. 2.1.3.1). We compare the performances of such protocol using two different quantum channels: a 270 m long free-space channel, and a 250 m long fiber link. Notably, the free-space case realizes a real urban channel between two separated buildings, established within the campus of Sapienza University of Rome. The double approach is motivated by the fact that, on the one hand, networks based on fiber communication are the common solution within urban environments, due to their scalability with moderate losses for short distances. On the other hand, over long distances, free-space links still represent the best choice to connect users due to their low signal attenuation [334, 99] and the possibility of sending complex states such as those exploiting the OAM of light – something still under development with optical fibers – despite the need for more complex sender and receiver systems.

2.5.1 Description of the experiment

Figure 2.27 illustrates the principle of operation of the realized QKD protocol. The employed procedure is a convenient variation of the well-known Ekert proposal, described in Sec. 2.1.3.1. An entangled pair of photons is distributed between two parties, Alice and Bob. They randomly select a measurement to perform on their subsystem from a set of linear polarization bases. In a quarter of the cases, Alice and Bob pick a combination of the $\{A_k, B_0\}$ bases, and their local reference frames are aligned in such a way that they will get the same result out of the measurement. When Alice and Bob share among themselves the information that they performed the same measurement, its random outcome is a bit added to the shared secret key. In presence of noise or imperfect entangled states, the keys may differ by an amount quantified by the quantum bit error rate (QBER),

$$\mathrm{QBER} = (1 - E(A_k, B_0))/2 \tag{2.29}$$

where $E(A_k, B_0)$ is the correlation coefficient, i.e., the expectation value on the $\{A_k, B_0\}$ pair of measurements. When the two parties select a different combination of polarization bases, they use the results of the measurement to estimate entanglement and monitor the security of the QKD The measurement bases on Alice ($\{A_0, A_1\}$) and Bob ($\{B_0, B_1\}$) sides are chosen in order to obtain the maximum value of the Bell parameter S, checking the violation of Bell inequality $|S| < 2$, accordingly to the CHSH figure of merit [129] (Sec. 1.2.2). The asymmetrical scheme of the modified E91 reduces the number of required detectors with respect to the original Ekert91 protocol, as reported in the practical implementation illustrated in Fig. 2.29a. At the same time, the fraction of photons dedicated to the key exchange is increased, while the security check is still performed by monitoring the Bell inequalities [229]. Additionally, the scheme has been demonstrated viable for device-independent operation [318].

In our experiment Bob is placed near the entangled photon source, while Alice is on the other side of the employed long-distance quantum channel. The generation apparatus adopts the single XX-X cascade of a quantum dot cavity to create an entangled state in polarization, that is $1/\sqrt{2}\{|\,|HH\rangle + |VV\rangle\}$ (the working principle of the QD emission is described is described in Sec. 1.2.3.2). Finally, the mentioned measurements on Alice ($\{A_k, A_0, A_1\}$) and Bob ($\{B_0, B_1\}$) sides are associated to single-photon detection on different avalanche photodiodes. The key transmission along the two different quantum channels — SMF and free-space links — was performed using two QDs with very similar features.

- The SMF quantum channel consists of a 780-HP fiber with 80% transmission after its 250 m of length at the wavelength of operation (785 nm).

- In the free-space experiment, a 850 nm diode laser is collected through a 30 m SMF together with the photon associated to the exciton line and brought to the transmission platform. Here, the beam is magnified by a factor of 6 by exploiting a telescope, with the aim of keeping collimation and reducing the effect of beam wandering during the 270 m travel in air, where the atmospheric attenuation losses amount at 10%. A mirror with piezoelectric adjusters is used to compensate for slow drifts in the pointing direction. On the receiver side, the beam diameter is reduced with a telescope similar to the one used by the sender. This permits to couple the signal in a SMF connected to Alice's apparatus. The 850 nm laser is separated from the QD signal using a dichroic

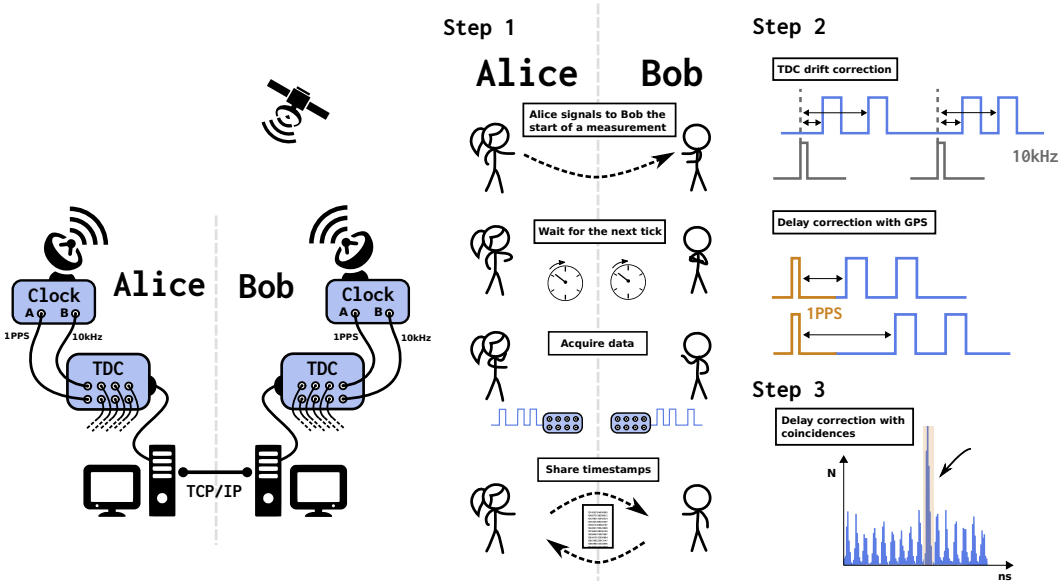

Figure 2.28. Synchronization scheme. Compressed timestamps are shared between the two stations over TCP/IP using the university network. Two GPS-locked oscillators are connected to the input channels of Alice's and Bob's TDCs (Time-to-Digital Converter). The 10 kHz signal of the oscillator is used to correct the internal drift of the TDCs while the 1 Hz pulse provides a coarse measurement of the delay between the parties which is then refined using the actual coincidences events. This image is taken from [13].

mirror, and sent to two position-sensitive detectors that provide feedback for an active beam stabilization system implemented using two mirrors with piezoelectric adjusters. The single-photon signal is finally collected in the SMF with an average coupling efficiency of 40% and sent to Alice's measurement apparatus. A more detailed account of the stabilization strategy and the channel losses is presented in the Sec. 2.5.2.

Finally, in order to realize the protocol, it is necessary to identify the coincidence events between Alice and Bob. During the key exchange process, photon arrival events are registered by the single-photon detectors of the two parties. These events are sorted and timed by a TDC (time-to-digital converter), with a resolution of 81 ps, and later filtered to select only two-fold coincidences, i.e. simultaneous arrival of a photon at each of the two stations. Since each party has his/her own independent TDC device, there is the need of a common time reference, and a synchronization procedure that allows both Alice and Bob to recover the coincidences events, and hence, the key. The solution used in this work makes use of two independent GPS-locked oscillators to generate a common clock signal, and then exploits the photon coincidences themselves to get to sub-ns accuracy. The scheme used for the synchronization is depicted in Fig. 2.28.

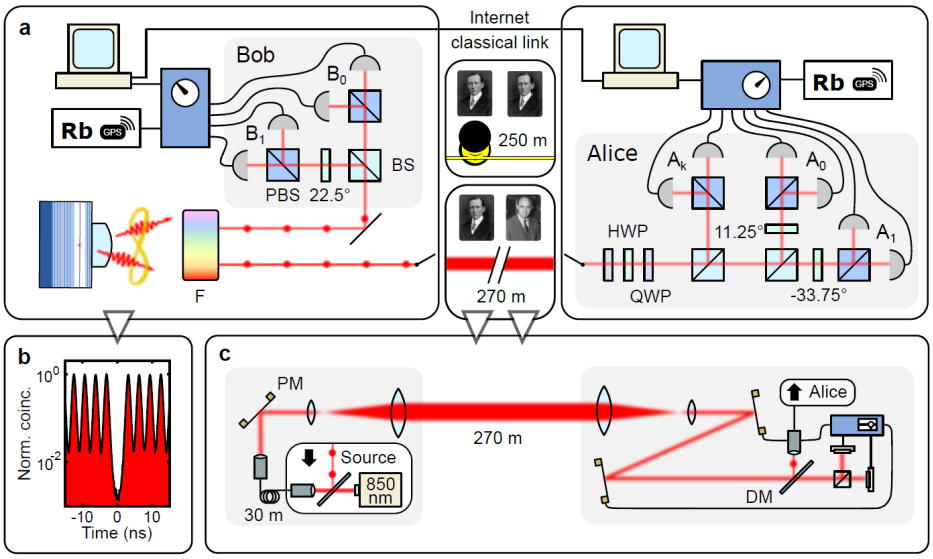

Figure 2.29. Experimental realization of the QKD protocol. a, Illustration of the setup used for the entanglement-based QKD protocol. On the Bob side, the single GaAs QD generates two entangled photons that are separated by spectral filtering (F). One photon goes directly to the Bob measurement apparatus, while the other travels through one of the quantum channels depicted in Fig. 2.27. The photons arriving at Alice's station are compensated in polarization with a set of two quarter-wave plates (QWPs) and a half-wave plate (HWP). After a random splitting with 50 : 50 beam splitters (BS) – which also mirror the polarization of the reflected beam – the polarization states are measured in the bases $\{B_0, B_1\}$ on Bob and $\{A_k, A_0, A_1\}$ on Alice using HWPs and polarizing beam splitters (PBS). The photons are finally collected and detected by avalanche photodiodes connected to two independent time taggers. These are synchronized combining a GPS signal and Rb oscillators. **b,** Autocorrelation histogram of the X emission line, showing the low multi-photon component of the source. **c** Sender and receiver in free-space communication. A diode laser beam at 850 nm is sent together with the single-photon signal and feeds a closed stabilization system, which controls the piezoelectric mirror mounts (PM). The QD signal is selected by a dichroic mirror (DM) and then coupled into a SMF directed to Alice's measurement apparatus. This image is taken from [13].

2.5.2 Free-space quantum channel

The global scheme of the experiment using the free-space channel is reported in Fig. 2.29c. As previously mentioned, the QD source is placed in the same building of Bob measurement setup. While Alice's setup is located in the other building apart 270 m. A SMF brings one photon of the entangled pair to Bob, while a 30 m-fiber brings the other photon to the building terrace for being sent in the free-space channel. A suitable platform placed on the terrace first increases the beam waist of the photon and then sends it along the air-channel. In the second buildings, Alice exploits two separated cascade tables, for stabilizing and measuring respectively the received signal.

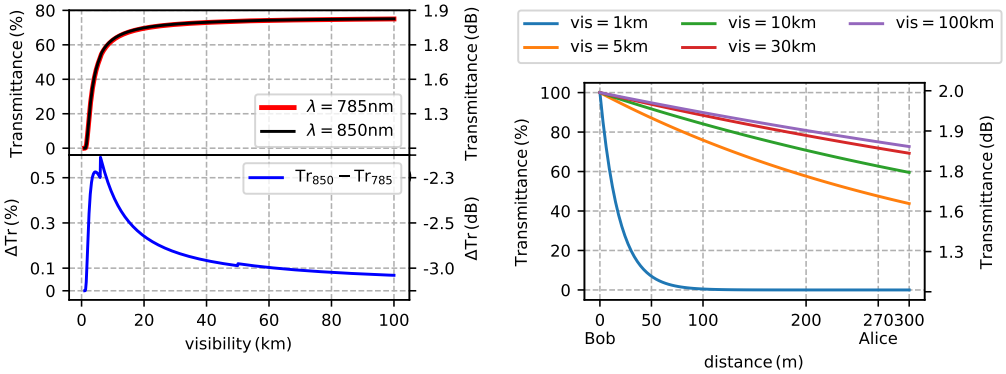

Figure 2.30. Light propagation in urban environment. Study of transmittance in urban environment as a function of the visibility, defined as the distance at which the radiation power of a 550 nm-beam is attenuated to 2% [338]. Left panel: simulations as a function of the visibility for a 270 m-long channel ($= d_{AB}$), at the wavelengths of both signal (785 nm) and stabilization laser (850 nm). The transmission difference ΔTr between these two wavelengths is less than 2% (bottom). Right panel: transmittance for channel lengths comparable with our experimental distance, investigated for different possible values of the visibility (vis). Furthermore, in our case we measured a transmission of 90%, thus expecting an experimental visibility within $10 - 20$ km. This image is taken from [13].

Stabilization

Experimental quantum key distribution in long-distance communication requires non-trivial setups. In free-space scenarios, the optical link between distant parties suffers from different effects such as atmospheric absorption, turbulence, bright background, humidity, or beam wander [335, 336, 337]. These effects contribute significantly to optical instabilities, increasing scattering, diffraction, beam deviation and noise while implementing the communication between distant parties. In our experimental implementation the air-distance between the transmitter (Bob) and the receiver (Alice) was $d_{AB} \simeq 270$ m.

Signal attenuation due to absorption and scattering by propagation through air is unavoidable. A simulation about these expected losses is reported in Fig. 2.30, considering our working wavelengths and the attenuation model reported in [335, 336, 337]. Among the different problems, signal stability due to beam wander oscillations turns out to be crucial while establishing a free-space communication channel. Differently from attenuation phenomena, there are several ways to reduce the effect of this problem.

(i) An optimal choice of the beam waist to minimize fluctuation and maximize collimation has been employed. Minimal waist decreases random oscillations from optical axes, while reducing Rayleigh collimation range, and viceversa. Therefore, a trade-off between these opposite phenomena has been used, and every optical element adopted on the receiver part has a sufficient size to match the beam oscillations.

(ii) An advanced stabilization system has been employed (see Fig. 2.31), to allow fiber coupling of the 785 nm-signal into a single-mode fiber. The implementation of such apparatus requires an additional laser (850 nm) which is employed as “control". At Bob’s station, the control laser and the 785 nm-signal are

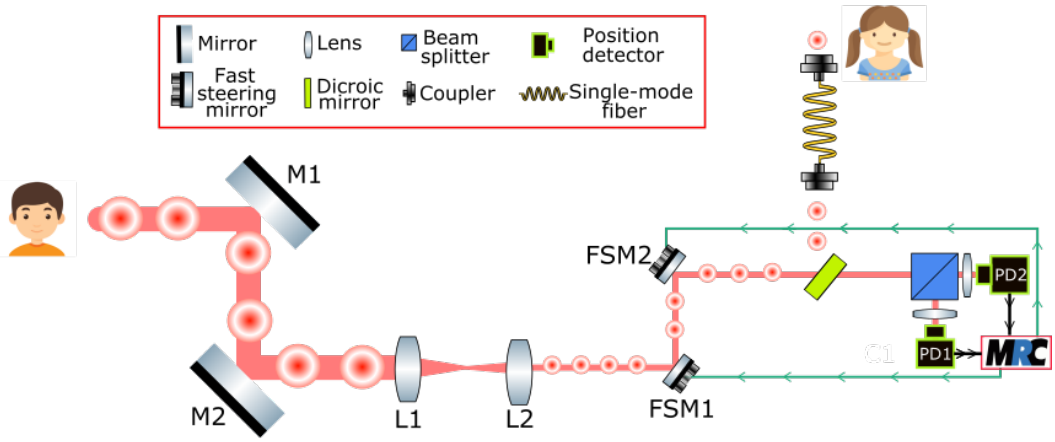

Figure 2.31. Experimental setup used for stabilization of the optical channel. Two overlapped beams get in the apparatus after 270 m of air propagation with a beam waist of 2.2 cm. The two largest mirrors send the light into a telescope, reducing the waist size of a factor 6.25 (focals $f_{L1} = 50$ cm, $f_{L2} = 8$ cm). The resulting beams are stabilized by means of two fast piezoelectric mirrors (FSMs) connected to two corresponding position-tracking detectors (PDs), driven by the control unit (MRC). An efficient stabilization is provided by keeping a suitable distance between FSMs and PDs: a series of three-inches mirrors produces 3 m of optical path (not shown in figure). The single-photon signal is divided from the stabilization laser thanks to a dichroic mirror, before being coupled in single-mode fiber. Finally, the fiber brings the signal to Alice's measurement setup. This image is taken from [13].

coupled into the same single-mode fiber before being sent to Alice, to ensure the same fluctuations while travelling through the overall channel. Once arrived at the stabilization platform, the control laser drives the stabilization mechanism, while the signal is separated to be sent to Alice setup. This operation is made by means of a dichroic mirror, which transmits the control beam to the stabilization system, while reflects 785 nm-photons to the fiber coupling. The wavelength 850 nm of the control laser has been chosen according to a trade-off condition. On the one hand the wavelength must be as near as possible to signal one, thus guaranteeing similar features in propagating both in free-space and through the same optical elements. On the other hand, after the dichroic mirror, the residual power of the control laser in the signal path must be minimal, in order to avoid disturbance while measuring single photons. In this way, we divide the stabilization platform from the measurement platform of Alice. A real picture of the receiver and stabilization platform is shown in Fig. 2.32. Such modular approach permits to control the stabilization system without modifying the receiver measurement apparatus, and vice versa. One of the most critical stages for establishing a functional free-space channel concerns the alignment between the sender launch platform and the receiver collection table. Indeed, accidental misalignment not only worsens the collimation and the coupling into the single-mode fiber, but it also damages the correct functionality of the active stabilization system. On the contrary, the second table is highly stable in its operations.

In the following sections the solutions (i) and (ii) are described in detail. Table 2.5 reports the list of the experimental losses affecting our free-space transmission

Figure 2.32. Picture of the receiver table used for collecting and stabilizing the signal from the free-space optical channel. Two 4' mirrors collect the signal propagated through the free-space link. Then, the signal is reduced by means of a telescope, consisting of two achromatic doublets. The reduced-size beam is reflected by a series of mirrors, which include a pair with piezoelectric adjusters driven by the MRC system. Finally, the reference laser beam is transmitted by a dichroic mirror and reaches a beam splitter and two position sensitive detector, while the QD photons are reflected and coupled into a single-mode fiber, before being sent to the measurement table. This image is taken from [13].

system, as measured with a diode laser with the same center wavelength as QD signal (but much larger bandwidth due to the multimode output). The cumulative transmission is higher than what reported in the main text, as estimated from the single-photon count rates. We currently attribute the discrepancy to gradual drifts in the pointing of the sender's system, which is also cause of instability and could be mitigated in the future by increasing the mechanical and thermal stability of the sender's platform or by having an active control of its pointing mirror, and to minor misalignment induced by introducing spectral filters in the receiving setup after the initial positioning with the diode laser.

(i) Choice of beam specifications

The first fundamental steps towards an efficient stabilization process are to perform an appropriate choice of the beam waist and of the optical elements for beam handling. During air propagation, Gaussian beams experience fluctuations and losses due to phenomena such as diffraction and absorption, related to diversified composition of the atmosphere. Furthermore, Gaussian beams naturally diverge as the travel distance increases. Thus, optimal choice of beam waist must take into account both collimation and low oscillation requirements. To satisfy this condition, we adopt a beam waist of $\omega_{\text{air}} \simeq 2.2$ cm, thus guaranteeing a Rayleigh's collimation range almost 2 km long ($\gg d_{AB}$) and a beam wander with maximum random shift inside $s_{\max} = 0.5$ cm (strong turbulence regime) (see Fig. 2.33). Therefore, using four- and three-inches optical elements has been sufficient to correctly manage the beam. The former are adopted as initial receiver mirrors, which inject the beam to a telescope employed to reduce the beam waist at the receiving station. After reduction of a factor 6.25, smaller-size optical elements are sufficient.

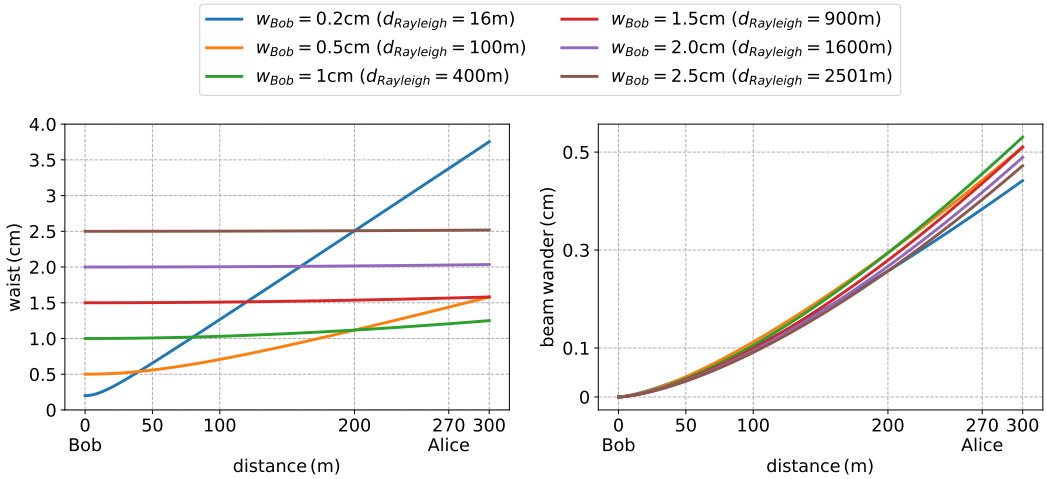

Figure 2.33. Simulation of Gaussian beam propagation in urban environment. Starting from beam collimation at Bob station, different waist sizes are studied in terms of waist divergence (left) and waist displacement due to beam wander effect (right). The latter is calculated in presence of strong turbulence condition ($C_n \simeq 10^{-13}$) [339, 337]. Comparison between the results highlights an optimal choice of the Bob waist around $w_{\text{air}} \simeq 2.2$ cm. Indeed, this value guarantees both high Rayleigh range ($d_{\text{Rayleigh}} \simeq 2$ km) and minimal random deviation from the optical axis. This image is taken from [13].

(ii) Stabilization system

The stabilization system adopted is the MRC-Laser Beam Stabilization (MRC Systems GmbH). It consists of two fast steering mirrors (FSMs), connected to a control unit. The control unit sends a correction signal to the FSMs according to the information revealed by two position detectors (PDs). The FSMs replace a couple of three-inches mirrors of the receiver apparatus. The stabilization system is initialized when the reference spot of the beam hits the center of both PDs simultaneously (target position). When fluctuations change the beam position, the control unit drives the FSMs to bring again the spot to the target position. The system achieves its task with accuracy below 0.1μm, which is suitable for single-mode coupling. The presence of two FSMs guarantees the retrieval of both the target

position and incoming directions over the detectors. Inside the maximum angular deviation corrected ($\theta_{\max} = 4$ mrad) and below the maximum frequency supported by MRC system (< 200 Hz), the expected low frequency oscillation of the beam wander should be efficiently corrected. In order to keep the fluctuations within angular tolerance of the MRC system, we consider a relative distance at least of ~ 3 m ($> s_{\max}/\theta_{\max}$) from FSMs to the detectors. The MRC system compensates for fluctuations in the signal overlapped to stabilization laser. Hence, the stabilization system cannot compensate for the last part of the optical path where the signal is separated from the 850 nm-laser. Therefore, the single mode coupling is placed as close as possible to the dichroic mirror that performs such separation.

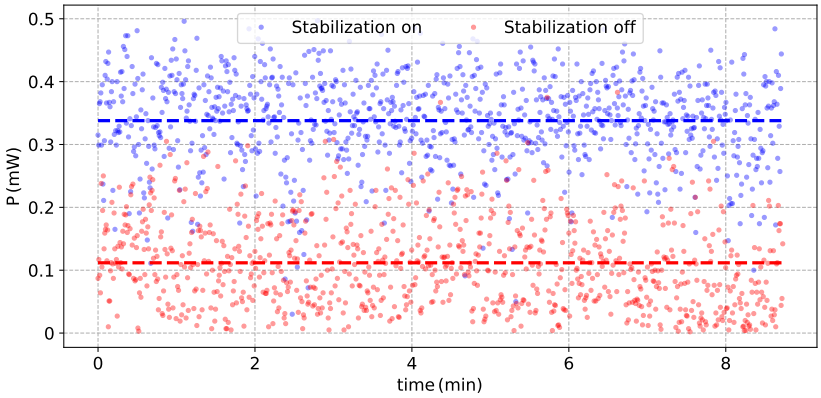

Figure 2.34. Test of the stabilization mechanism. Results of power coupling into a single-mode fiber by turning on and off the MRC-Laser Beam Stabilization system (MRC Systems GmbH). The study exploits a simulation laser at 785 nm (signal wavelength). Measurements (dots) are made over about 10 minutes of acquisition time. Dashed lines represent the coupled mean value of the two configurations, showing a reduction in the coupled power of 70% without stabilization. This image is taken from [13].

To verify the quality of the stabilization process we exploited an additional simulation laser with the same frequency of the single-photon signal. At Bob's station, this 785 nm-laser is coupled inside the single-mode fiber shared by the control and signal light, before being sent into the channel. In this way, travelling towards the receiver, the new laser beam experiences identical perturbations. Analogously the single-photon signal, the simulation laser is reflected by dichroic mirror and coupled in single-mode fiber directed to Alice setup. Differences in stabilization with and without activation of the MRC system are shown in Fig. 2.34, where the in-fiber power coupling of the simulation laser is measured. Furthermore, we observe that the efficiency of the correction depends also on the power which arrives at the detectors. Minimization of the 850 nm-noise in the 785 nm-signal requires an accurate choice of the power $P_{850\text{nm}}$ of the stabilization laser reaching the detectors. The condition in which the MRC system works guaranteeing best performances with minimal power is $P_{850\text{nm}} \sim 100$ μW. Using this approach we obtained a single-mode coupling efficiency of the 785 nm-signal of approximately 40%, at best up to 50%. This value could be further improved using a spatial light modulator.

Source of loss	Optical Losses
Bob side	
signal filtering	3%
propagation in the sending table	15%
free-space channel	
air propagation	10%
Alice side	
propagation in the stabilization table	28%
SMF coupling of the stabilized beam	60%
signal filtering	2%

Table 2.5. Experimental losses budget. List of all losses experienced by the optical signal which propagates from Bob to Alice. We note that when the signal arrives on the measurement table of Alice, it is split by two BSs among the three different polarization bases for measuring (see Fig. 2.29), composed by waveplates and PBSs. Legend: SMF, single-mode fiber; BS, beam splitter; PBS, polarizing BS.

2.5.3 Experimental results

Characterization of the entangled photon source

Polarization-entangled photons are generated by a single GaAsQD embedded in a crystalline matrix of $Al_{0.4}Ga_{0.6}As$ (Sec. 1.2.3.2), pumped with a 320-MHz repetition rate laser . The QDs are fabricated using the Al droplet etching technique, as described in reference [340]. Due to the presence of distributed Bragg reflectors in the sample structure and to the use of a hemispherical solid immersion lens, an extraction efficiency of approximately 8% is achieved in the investigated sample. This value allows to employ the source in realistic quantum communication schemes, but further improvements are required to overcome state-of-the-art SPDC as shown in Fig. 2.35. The entangled photon source is kept at 5 K in a low-vibration closed cycle He cryostat. The optical excitation is performed with a Ti:Sapphire laser together with a 4f pulse shaper, to reduce its bandwidth to 0.1 nm, and two Mach-Zehnder interferometers, to increase its repetition rate four-fold. The signal is collected from the QD using a 0.81 NA objective and the backscattered laser light is filtered out with notch filters. The two photons from a single XX-X cascade are then separated by two volume Bragg gratings, collected by two SMFs and distributed. Two different QDs from the same sample and with similar characteristics were used in the two parts of the experiment. In order to completely characterize the two QDs, we implement fidelity test and auto-correlation measurements.

The entanglement fidelity (Sec. 1.2.4) has been obtained after reconstructing the density matrix of the entangled-photon state by taking a full quantum state tomography [342]. The results are 95.8(1.2)% in the free-space case and 94.1(1.0)% in the in-fiber case (see Fig. 2.36), guaranteeing a high quality of the generated state for both cases. These values are only slightly different and are due to the different sub-μeV fine structure splitting (FSS), 0.35 (free-space) and 0.85 (in-fiber) μeV respectively.

The impact of multi-photon emission events is characterized using intensity auto-correlation measurements in a Hanbury Brown and Twiss setup (Sec. 1.2.3).

Figure 2.37a shows the coincidence histograms for both the exciton and biexciton emission lines. The zero-time delay coincidences normalized to the side peaks, due to consecutive excitation laser pulses, return the values $g_X^{(2)}(|\tau| < 0.8ns) = 0.0034(2)$ and $g_X^{(2)}X(|\tau| < 0.8ns) = 0.0041(3)$ for the QD used in the fiber experiment, $g_X^{(2)}(|\tau| < 0.8ns) = 0.0040(4)$ and $g_X^{(2)}X(|\tau| < 0.8ns) = 0.0045(4)$ for the QD used in the free-space experiment. This result demonstrates a very similar multi-photon emission of the two employed QDs. Furthermore, achieving these values does not require polarization suppression for the cancellation of background radiation from the laser. In Fig. 2.37b we report instead the cross-correlation measurement between the two emission lines, acquired without selecting any polarization state. This measurement is used to infer the preparation fidelity of the biexciton state [343] using a resonant two-photon excitation process. Note that the central peak appears taller than the side ones in part due to the higher probability of detecting one photon if its entangled counterpart from the same cascade has already been detected, and in part due to its narrower temporal width. Indeed, the preparation fidelity estimated from the integrated intensity of the coincidence peaks of Fig. 2.37b for the QD used in the free-space QKD demonstration is 94.3(3)%. A value of 90(1)% is estimated for the SMF case. By extending the correlation range to 100 μs we also identify a blinking dynamics on the microseconds scale, with a characteristic on-time fraction β equal to 0.22 and 0.26 for the free-space and SMF protocol implementations respectively.

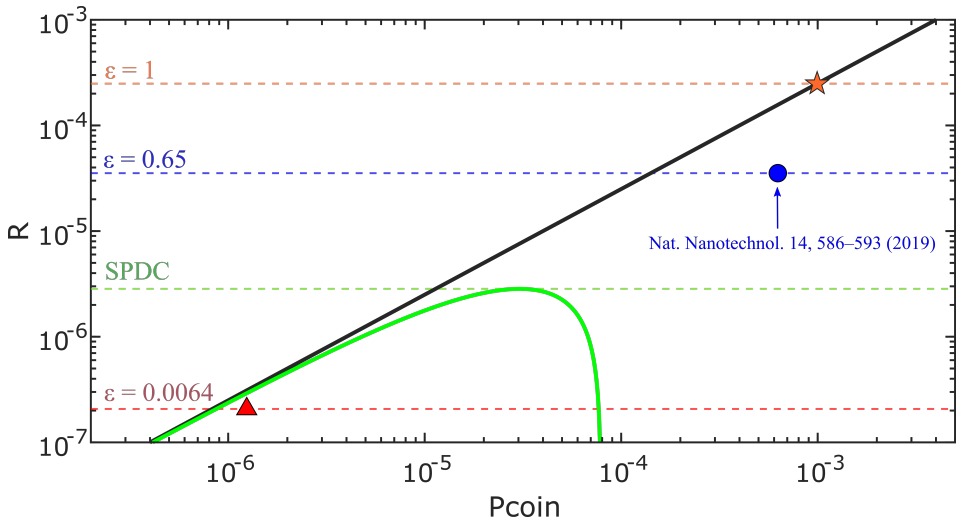

Figure 2.35. Secure key rate as function of the total coincidence probability for one pump pulse. Ideal quantum dot (solid black line) and SPDC (solid green line) secure key rates are calculated with $d = 2.5 \times 10^{-6}$, $t = 0.031$ and unitary entanglement fidelity. For this simulation we fit the parameters with the source in Ref.[341], where the parameter $\chi = \beta\sqrt{I}$ depends on the pulse intensity ($\beta = 10^{-8}$). Ideal quantum dot with unitary fidelity and perfect photon pair extraction $\epsilon = 1$ (orange dashed line, star); Circular Bragg resonator quantum dot source with photon pair extraction $\epsilon = 0.65$ [324] and entanglement fidelity $F = 88\%$ (blue dashed line, circle); the maximum secure key rate extraction of the SPDC (green dashed line); the quantum dot we use in the free-space experiment, with photon pair extraction $\epsilon = 0.0064$ (red dashed line, triangle) and fidelity $F = 95.8\%$. From the experiment this last point is estimated as $R_{\text{exp}} = 1.88 \times 10^{-7}$. All the curves and points in the figure are obtained with the same experimental parameters. This image is taken from [13].

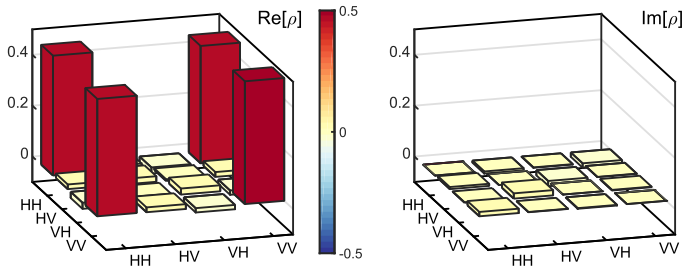

Figure 2.36. Entangled-photon pair density matrix. The reconstructed density matrix of the polarization state of the photon pairs generated through the biexciton-exciton radiative cascade from a QD. Specifically, the matrix is the result of the full quantum state tomography performed in laboratory conditions on the QD used in the QKD demonstration with the SMF quantum channel. The Bell-state fidelity is 94.1%. This image is taken from [13].

Finally, the resulting single-photon count at the output of the first SMF, disregarding losses in the quantum channels and in the Alice and Bob apparatuses, is 700 and 620 kcps for the free-space and in-fiber QD respectively.

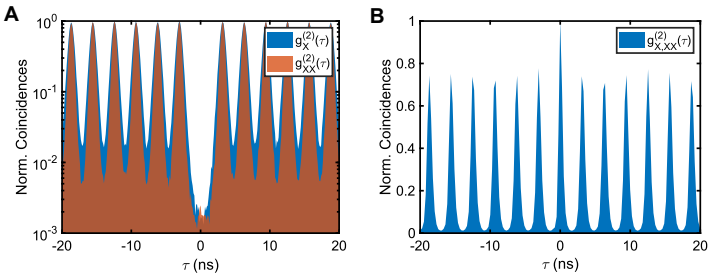

Figure 2.37. Intensity correlation histograms. (**A**) Auto-correlation histograms of both the exciton and biexciton lines collected in laboratory conditions on the QD used in the QKD demonstration on the SMF quantum channel. The zero-time delay coincidences normalized to the side peaks are $g_X^{(2)}(|\tau| < 0.8\ ns) = 0.0034(2)$ and $g_{XX}^{(2)}(|\tau| < 0.8\ ns) = 0.0041(3)$. (**B**) Cross-correlation histogram between the exciton and biexciton lines collected in laboratory conditions on the QD used in the QKD demonstration on the free-space quantum channel. The estimated preparation fidelity is 94.3(3)%. This image is taken from [13].

Test with common time-to-digital converter

A preliminary simulation of the experiment was performed by registering all the detection events with a single multi-channel time-to-digital converter from Swabian Instruments. While this option does not qualify as quantum key distribution, since all the measurement outcomes are recorded and analyzed by a single user, it is a good benchmark to assess the performance of the source independently from technical aspects related to the synchronization between the communication parties. This test was performed using a QD with 1.15 μeV fine structure splitting, 93.6% entanglement fidelity, a single-photon count of 850 kcps at the output of the first SMF (disregarding losses in the quantum channels and in the Alice and Bob apparatuses), a preparation fidelity of 90.5%, and a characteristic on-time fraction β equal to 0.3. The results are reported in Fig. 2.38. While the stable acquisition and synchronization conditions

grant a sustained raw key rate of 785 bit s^{-1}, the other performance figures of the protocol – the average quantum bit error rate (QBER) Q = 0.037(1) and the mean Bell's parameter S = 2.61(4) – are not superior with respect to our realistic implementation.

Quantum key distribution

The comparison of the experimental results between the fiber and free-space approaches is illustrated in Fig. 2.39. The data is synchronously collected on the two sides in packets of 1.2 s acquisition time and shared over the university network, for a total time of 224 minutes. For both optical links, we measure the QBER, the Bell parameter S and the amount of key shared among the two parties. Using the fiber communication approach, in Fig. 2.39a, a total 217.76 kB key is shared, with a mean key rate of 486 bit s^{-1}. The mean QBER of the key is $Q_{\mathrm{SMF}} = 0.0337(2)$, while the mean Bell parameter is $S_{\mathrm{SMF}} = 2.647(2)$. In free-space communication, see Fig. 2.39b, we manage to share a 34.589 kB-long key string, relying on 60 bit s^{-1} of mean key rate. In this case, the average values of QBER and Bell parameter are $Q_{\mathrm{FS}} = 0.040(2)$ and $S_{\mathrm{FS}} = 2.37(10)$ respectively. Both optical link choices showed a substantial violation of Bell inequality, demonstrating the two-photon entanglement preservation over the quantum communication channel. The reliability of the key quality shared during the communication is verified in both cases by monitoring the QBER, which remains consistently well below the critical insecure value of 11%. These results constitute a successful field demonstration of QKD using a QD-based deterministic source of entangled photons. Notably, due to experimental imperfections, the bits measured during the key exchange process are expected to be not uniformly distributed, hence, after the binary error correction process described in [344], one needs to further polish the key to obtain a uniformly distributed bit string. The class of algorithms that allows one to get a perfectly random (but shorter) bit string from a non uniform one are called *randomness*

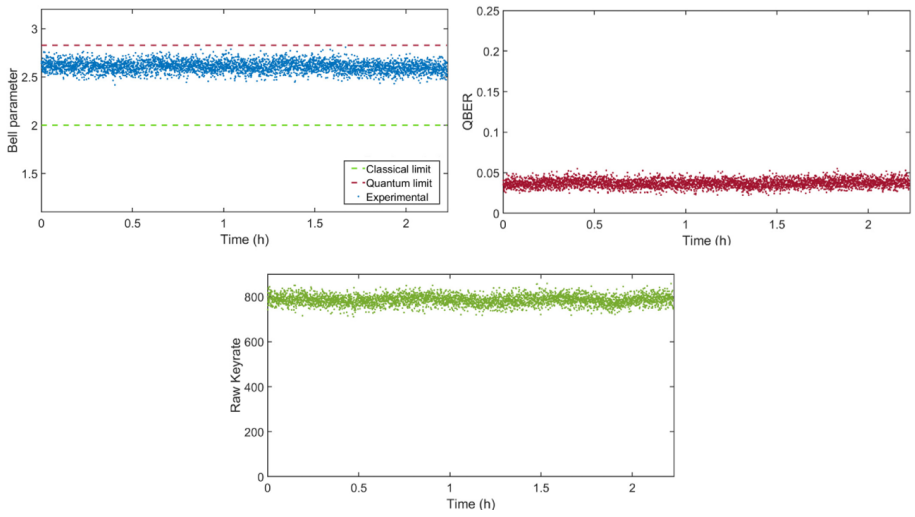

Figure 2.38. QKD simulation with a common time-to-digital converter. The Bell parameter, QBER and raw key rate measured with a single time-to-digital converter, collecting the timestamps from both Alice and Bob detection setups. The signal is transferred from the source to Alice's apparatus through a coiled 250 meter SMF with 80% transmission. This image is taken from [13].

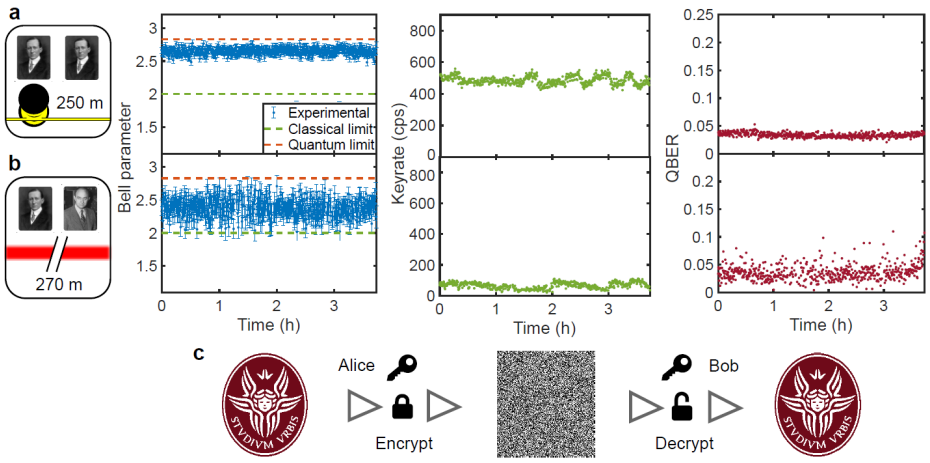

Figure 2.39. Experimental key sharing via the modified Ekert protocol. The Bell parameter, QBER and raw key rate measured with both **a,** the SMF optical link and **b,** the free-space optical link. In the latter case, the data transmission was conducted overnight and interrupted at dawn. Each data point corresponds to 5 acquisitions of 1.2 s. The error bars in the Bell parameter are calculated by Gaussian propagation assuming a Poissonian distribution for the coincidence counts. **c,** The encryption and decryption of Sapienza logo using the one-time pad technique with the shared free-space key, after the error correction and randomness enhancement steps. This image is taken from [13].

extractors, and they usually work by consuming a third uniformly distributed source of randomness, called the *seed*. In particular here we use the *Trevisan extractor* [345], following the implementation presented in [346]. The advantage of using the Trevisan's construction is that the extracted bit string is practically independent of the seed (strong extractor), which therefore can be publicly shared among the two parties. Moreover it is known that this kind of extractor is secure also in the presence of quantum side information, making it an ideal choice for device-independent quantum protocols [347, 348]. In our case, calling d the length of the seed, we need: $d \sim \log_2(m)\log_2^2(n)\log_2^2(1/\epsilon)$, where n is the length and k is the total amount of entropy of the input bit string, while m denotes the length of the output string. The parameter ϵ represents the maximum allowed discrepancy between the output distribution and a uniform one (intuitively, we can think of the output single bit probability as being $1/2 + \epsilon$). In particular to extract $m = 26$ kB bits from a source with entropy $s \approx 0.992$ per bit, of length $n = 27.938$ kB we employed a seed of $d \approx 579$ MB. Therefore, after the binary error correction process [349], we apply a Trevisan extractor to restore uniform randomness [346] and compensate for a setup-induced polarization changes. Part of the uniformly distributed key was used to encrypt and decrypt the Sapienza logo as depicted in Fig. 2.39c.

2.5.4 Conclusions and perspectives

In conclusion, we have experimentally performed an entanglement-based QKD protocol with the use of a QD photon-pair source, demonstrated to be viable both with in-fiber and free-space quantum communication channels. The comparison of the measurements between the two different employed links, highlights some interesting considerations on the quantum channel choice performing an EPR-based QKD approach using QDs. Atmospheric turbulence and the complex stability requirements of optical apparatuses for free-space communication lead to signal loss and performance degradation when compared with the in-fiber solution for short distances. This is unavoidable to a certain degree, even if we can identify excessive losses and room for optimizationin our current implementation. The complete characterization of the quantum channel is important for controlling hacking strategies such as side-channel attacks. In this regard, a potentially useful feature in our free-space implementation is the modular approach of the receiver apparatus, dividing the collection table from the table dedicated to the measurements (see Supplementary Materials). In particular, the former is employed for the correct stabilization of the signal, but in general it could be used for adding particular scheme-dependent defense elements, such as an optical isolator [239] or a spatial filter [240], in order to avoid possible attacks based on hardware limitations. While we do not consider an a priori defense against possible side-channel attacks, our setup is robust, for instance, to spatial-mode side-channel attacks, since we do not allow multiple spatial modes at the detectors by filtering the signal through a single-mode fiber. In a more general context of applications, by increasing the distance between the QKD users, the free-space communication is expected to deteriorate less dramatically, becoming a more advisable solution. Moreover, it allows to use the orbital angular momentum degree of freedom, which can be employed in QKD schemes, e.g. for independence from local reference frames [350]. Up to date the generation of OAM states using QD-based light sources is mostly unexplored, but there is a developing effort to make use of semiconductor microcavities designed to control the chirality of emitted light [351, 352] and embed QDs in them for the generation of single photons carrying OAM [353, 354]. Therefore, exactly 20 years after the first theoretical proposal on the possibility of using quantum dots to generate regulated and entangled photons [355], our study demonstrates that this semiconductor-based quantum technology is mature to go out of the lab, and further improvements will soon open the way to real-life quantum communication. In particular, we envisage that the possibility of interfacing entangled photons from QDs with the same or other quantum systems [356], together with the prospect of enhancing photon extraction [324, 325], will be the key to boost secure quantum cryptography over large distances.

2.6 Final remarks

Quantum communication aims at distributing quantum resources between different and/or distant parties. This is made in order to realize quantum communication protocols, such as entanglement swapping, teleportation, and quantum key distribution. Photonic entanglement can be easily distributed by using optical fibers and free-space links. Its manipulation can take advantage of bulk-based setup or most advanced integrated platforms. In this chapter, the contributions of my thesis project to the quantum communication fields have been reported.

The generation of entangled photon pairs at the telecom wavelength has been demonstrated in an integrated device [10]. Three photonic chips, fabricated by femtosecond laser writing technique, are cascaded to form a Mach-Zehnder interferometer with two nonlinear waveguides of light along the inner arms. The output state can be tuned by using a phase shifter in the first device, or by interchanging the third component in order to realize path or polarization encoding of the final quantum state. The search for a complete on-chip realization of the entire quantum protocol — generation, manipulation, and detection — represents a hot topic in Photonic Quantum Communication. Our result is a building block in this research direction, especially for the modular composition of hybrid materials. This feature allows us to better select the various components to optimize specific functionalities.

In a second work [11], we demonstrated the fiber distribution of complex hybrid entangled states, by using a new special fiber: the air-core fiber. In particular, the hybrid state corresponds to a vector vortex state — where polarization is correlated with orbital angular momentum — encoded in a photon, in turn entangled with the polarization of a second photon. Our result is a crucial step towards the adoption of high-dimensional entanglement in quantum networks, where the OAM distribution could cover a crucial role due to its unbounded nature.

Then, the distribution of quantum resources was realized in a quantum network [12], which represents the most general scheme in the distribution scenario. Our scheme consists of four independent laboratories connected to a central one. This allows us to realize a star-shaped quantum network, in which n nodes are connected with a central one, by means of n independent sources of entangled photon pairs. Our laboratories are used by varying the network architecture from $n = 1$ to $n = 4$. The multipartite entanglement distributed in the network has been revealed and certified by means of generalized Bell-like inequalities. Our implementation has a scalable photonic structure, allowing experimental testing of other general quantum networks. This is crucial for studying nonlocality inside different topological scenarios or in order to implement a future quantum internet.

Finally, an experimental quantum key distribution was demonstrated between two buildings of the Physics Department of Sapienza University of Rome [13]. The entangled-based protocol used is a modified version of the Ekert91. The distributed entanglement was generated by means of a quantum dot source. This source aims at the on-demand generation that can provide a boost in cryptographic quantum protocols as photon distribution could become unassailable. Further, the same experiment was performed twice, distributing entanglement with two different quantum channels: a fiber link and an urban free-space channel. Our studies refer to fundamental points of Quantum Communication for the real-life scenario. On the

one hand, they show that quantum dot technology is mature to go out of the lab. On the other hand, addressing both fiber and free-space quantum channels allows for testing the most viable technology for a real-world scenario.

Chapter 3

Photonic platforms for Quantum Metrology

The measurement process has always interested the Physics and the science of measurement it is known as Metrology. Quantum Information theory explains straightforwardly the difference between classical and quantum uncertainty, and Quantum Metrology is the most advanced physics theory which aims at achieving ultimate limits in the measurement of physical quantities. Further, quantum sensing devices are among the most promising quantum technologies. Their implementation relies on the use of quantum probes to attain enhanced performances in the estimation of one or more parameters compared to classical ones. Given an unknown parameter to be estimated and m classical probes (with $m \gg 1$), each interacting a single time with the system under study, the estimation error will scale at best as $\sim m^{-1/2}$. This classical limit is a consequence of the central limit theorem and is called standard quantum limit (SQL). The term "classical" stands for probes that are at most classically correlated. If quantum probes are allowed, the SQL can be surpassed so that the uncertainty of the estimator reaches the more fundamental scaling $\sim m^{-1}$, improving the precision by a factor $\sqrt{m}$ with respect to the SQL. Such new scaling represents the ultimate limit on estimation precision and is called the Heisenberg limit. Quantum Metrology aims at identifying the best strategy able to provide this quantum advantage [357, 358, 359, 360, 2, 361, 234]. This is achieved by carefully tailoring the probe state, the interaction, and the measurement, in order to extract the information on the relevant parameter, and by the optimal choice of the estimator through data post-processing [362]. Here, the presence of entanglement in the prepared probe plays a fundamental role, since it is the necessary resource in order to achieve estimation enhancement. Application of Quantum Metrology are many [1], since different research branches can benefit quantum-enhanced sensitivity, such as: measurement on biological systems [363, 364], gravitational waves detection [365], atomic clocks [366, 367], interferometry with atomic and molecular matter waves [368, 369, 370, 371], plasmonic sensing [372, 373], magnetometry [374, 375], spectroscopy and frequency measurements [376, 377, 378], lithography [379, 380, 381, 382], microscopy and imaging [383, 384, 385, 386, 387, 388, 389, 390, 391], localization of incoherent point sources [392, 393], Hamiltonian estimation [394, 395, 396], fundamental physics effects [397, 398], coordinates transfer, synchronization and navigation [399, 400, 401, 402], absorption measurements [403], thermometry [404] and general sensing technologies [405, 406].

Also in this case, the photonic approach to estimation theory provides a convenient choice and phase estimation is suitably treated with interferometry. Indeed,

single or multiple optical phases can be manipulated and measured with standard interferometers, such as the Mach-Zehnder interferometer. MZI even represents the optimal platform to use in order to access the best estimation of a single phase (Sec. 3.1.3). In addition to the various advantages offered by Quantum Photonics (Sec. 1.1), quantum states of light can be conveniently prepared to probe quantum sensors and achieve enhancements in metrological tasks [1]. The most exciting application is the gravitational wave detection [407, 408, 409], representing a very challenging research area and the first actual application of Quantum Metrology [410, 411, 412, 413, 414, 415, 416, 417]. The small amplitude ($\sim 10^{-22}$) of gravitational waves needs very long interferometers to be measured, together with very low overall noise [360, 418]. Quantum metrological techniques, such as adopting the squeezing resource as the input state into the interferometer [419], seem to be the only possible short-term solution for improving the signal-to-shot noise ratio of such interferometers. Starting from 2007, GEO600 gravitational wave detector has successful adopted squeezed light for its detection [365, 420]. Recently, after preliminary tests [421], squeezed vacuum states have been used in the Advanced LIGO detectors [422, 423]. Other gravitational wave detectors have almost achieved the best technological performances in their several components [424, 409, 425, 426], and seems to find further improvements only in squeezing enhancement.

Despite single parameter estimation has been largely studied both theoretically and experimentally, the scenario involving more parameters still presents several open questions [1]. Also in this case quantum resources can enhance the simultaneous estimation of all parameters [427, 428]. This represents a relatively new research area with different experimental and theoretical open questions, such as the capability of reaching the quantum ultimate bounds in the simultaneous estimation of all parameters. On the other hand, surprisingly few photonic platforms have been realized to test the simultaneous multiparameter estimation. Here, photons can be employed with different schemes and approaches [427, 428, 429, 430]. In this context, besides direct mapping of problems to quantum imaging, the multiphase estimation can represent a benchmark suitable for tests of quantum multiparameter protocols. Its importance and generality derives also from the fact that unitary evolutions generally introduce a phase in the evolved states. For these reasons, experimental multiphase estimation is a really interesting area to investigate. Finally, the study of adaptive strategies for quantum sensing, in both single e multiparameter scenarios, represents a further important investigation. Indeed, tuning the operation of the quantum sensor during the estimation process allows improvements such as optimal performances in a limited data regime, or an achievable quantum enhancement for a larger space of unknown parameters (Sec. 3.1.4).

In this thesis a review work has been realized on Photonic Quantum Metrology [1], in order to provide the basis for an experimental Quantum Metrology, to assess the state-of-the-art of such field and identify the ultimate challenges. Such work introduces the photonic technologies available for metrological tasks, with particular attention to the phase estimation problem. Finally, it shows the multiparameter scenario and the current theoretical and experimental open questions, by discussing the quantum-enhanced performances in the presence of noise. Thus, we adopt the review contents in order to provide fundamentals of Quantum Metrology in Sec. 3.1. Besides such theoretical work, we gave different experimental contributions in this context. An integrated device has been developed for testing a multiparameter estimation scenario (Sec. 3.2). Specifically, the chip is a 3-arm interferometer, representing the 3-mode generalization of the MZI, which is able to investigate two optical independent phase shifts. The high degree of reconfigurability due to the

presence of several PSs allows even the study of adaptive phase estimation. Thus it is possible to optimally change some control parameters during the estimation process in order to achieve the best-generalized performances for the two-phase estimation. First, such device has been fully characterized in the classical and quantum regime, demonstrating experimentally the quantum-enhanced capability for two-phase estimation in a non-adaptive scenario (Sec. 3.2.1). Then, a reliable characterization has been demonstrated by using a Neural Network approach (Sec. 3.2.2). Subsequently, my thesis work moved to adaptive protocols for optimizing the phase estimation. Here, the best results have been achieved using the same integrated device. In Sec. 3.3.2, a machine learning technique proposed by [394], based on a Bayesian inference which exploits a Monte Carlo-like approximation, has been successfully applied for our simultaneous two-phase estimation problem. We demonstrated improved performances by reducing the number of employed resources and enlarging the phase interval in which a quantum enhancement is possible. Finally, further work concerned the study of a genetic protocol suitably tailored for optimizing the estimation of a single phase in a standard MZI (Sec. 3.3.1).

3.1 Quantum Metrology: Fundamentals

Photonic Quantum Metrology has attracted a large research effort in the last years, leading to notable progresses both theoretically and experimentally as reported in previous review papers. They concern advances in general photonic technologies [5, 44], theoretical aspects of Quantum Metrology and phase estimation problem [431, 432, 361, 433, 434, 2, 359], multiparameter estimation scenario [428, 435, 427], optical metrology [385, 436, 437, 234, 390, 438, 384, 363, 439, 440, 360], and metrological tasks performed by different physical systems [361, 405, 364, 441]. The Table 3.1 reports a list of these mentioned works.

Review	Topic
[5, 44]	photonic quantum technologies
[385, 436, 437, 234, 390, 438] [384, 363, 439, 440, 360]	quantum optical metrology
[431, 432, 361, 433, 434, 2, 359]	fundamental of Quantum Metrology and phase estimation problem
[434]	precision bounds of quantum states
[234, 432]	photonic quantum sensing
[428, 435, 427]	multiparameter Quantum Metrology
[442, 443]	continous variable and gaussian states
[361, 405, 364, 441]	metrology performed by other physical systems

Table 3.1. List of more relevant works which addressed topics around photonic Quantum Metrology studies.

In this section we describe the fundamentals of single parameter estimation and the problem of estimating more than one parameter. In particular some results of the former scenario do not apply for the latter one. Such descriptions are taken from [1]. In Secs. 3.1.1 and 3.1.2 the definitions of the basic quantities are introduced, such as Fisher Information and Cramér-Rao bound, that characterize a general estimation process. Sec. 3.1.4 is devoted to adaptive protocols able to enhance the estimation processes. In Sec. 3.1.3 we describe single- and multi-phase estimation problems. Finally, we describe the state-of-the-art of experimental photonic realizations of simultaneous multiphase estimation.

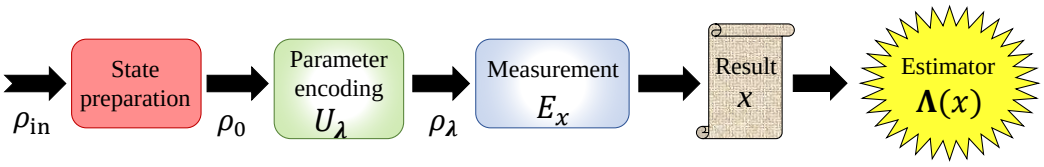

Figure 3.1. Conceptual scheme of an estimation of parameters. An initial probe is prepared (red box) in a state ρ_0 (eventually, from an initial state ρ_{in}). Then, it interacts with the unknown parameters $\boldsymbol{\lambda}$ through an evolution $U_{\boldsymbol{\lambda}}$ (green box). The state $\rho_{\boldsymbol{\lambda}}$ encoding the information on $\boldsymbol{\lambda}$ is measured by a POVM E_x (blue box) generating outcome x. Based on the outcomes x, a suitable estimator provides an estimate $\boldsymbol{\Lambda}(x)$ of the parameters $\boldsymbol{\lambda}$. This image is taken from [1].

3.1.1 Estimation process

The realization of a sensor for measuring a quantity λ embedded in a physical system requires the study of how to interact with the system and how to extract the interested information after the interaction. In a more general and complex scenario the number of parameters can be more than one: $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \dots)$. The general estimation process can be described by a cycle repeated ν independent times composed of four steps (Fig. 3.1):

(i) the preparation of a probe state ρ_0, as sensitive as possible to variations of the unknown parameters;

(ii) the interaction between the probe and the physical system for encoding the information on the unknown parameters. This interaction depends on $\boldsymbol{\lambda}$ and can be described as a unitary evolution $U_{\boldsymbol{\lambda}}$ which evolves the state ρ_0 in $\rho_{\boldsymbol{\lambda}} = U_{\boldsymbol{\lambda}} \rho_0 U_{\boldsymbol{\lambda}}^\dagger$ — for simplicity we consider only unitary evolution but this can be extended to non-unitary maps;

(iii) the measurement for extracting information by means of a suitable positive operator valued measure (POVM) E_x, which provides the projected result x collapsing the state along the corresponding eigenvector;

(iv) finally, a suitable estimator function provides an estimate $\boldsymbol{\Lambda}(\boldsymbol{x}) = (\Lambda_1(\boldsymbol{x}), \Lambda_2(\boldsymbol{x}), \dots)$ of the unknown parameters, which at the iteration k of the cycle depends on all previous measurement results $\boldsymbol{x} = (x_1, x_2, \dots, x_k)$.

The goal of the Metrology in choosing the estimator and preparing all the stages of the estimation process is to optimally converge to the real value of the parameters. In particular, an estimator is said *unbiased* if its mean value over all the possible sequences of $\boldsymbol{x}$, coincides with the unknown parameters:

$$\bar{\boldsymbol{\Lambda}} = \sum_{\boldsymbol{x}} P(\boldsymbol{x}|\boldsymbol{\lambda}) \boldsymbol{\Lambda}(\boldsymbol{x}) = \boldsymbol{\lambda} \qquad \forall \boldsymbol{\lambda}, \tag{3.1}$$

where $P(\boldsymbol{x}|\boldsymbol{\lambda})$ is called *likelihood* and it represents the conditional output probability of obtaining a sequence of measurement results $\boldsymbol{x}$, given certain values of the parameters $\boldsymbol{\lambda}$. The relation (3.1) is valid independently from the values of the parameters. A less stringent requirement is considering *locally unbiased* estimators,

which are unbiased only for limited range of $\boldsymbol{\lambda}$ in which is satisfied the relation

$$\sum_{\boldsymbol{x}} \Lambda_k(\boldsymbol{x}) \, \frac{\partial P(\boldsymbol{x}|\boldsymbol{\lambda})}{\partial \lambda_i} = \delta_{ik}, \tag{3.2}$$

which corresponds to $\partial\bar{\Lambda}/\partial\lambda = 1$ in the single parameter case. Finally, an estimator is *asymptotically unbiased* (locally or not) when it converges to the real value in the limit of infinite number of probes: $\lim_{\nu\to\infty} \bar{\boldsymbol{\Lambda}} = \boldsymbol{\lambda}$. The likelihood depends by the measurement results through the Born rule:

$$P(x_i|\boldsymbol{\lambda}) = \mathrm{Tr}(E_{x_i}\rho_{\boldsymbol{\lambda}}), \tag{3.3}$$

which describes the conditional probability for the single measurement. In presence of independent repetitions of the estimation cycle, the final likelihood is given by $P(\boldsymbol{x}|\boldsymbol{\lambda}) = \prod_{i=1}^{\nu} P(x_i|\boldsymbol{\lambda})$. When we consider a single parameter problem, the accuracy of the estimation can be studied by two figure of merits: the *mean square error* (MSE) defined as

$$\mathrm{MSE}(\lambda) = \sum_{\boldsymbol{x}} (\Lambda(\boldsymbol{x}) - \lambda)^2 P(\boldsymbol{x}|\lambda), \tag{3.4}$$

and the *variance* of the estimator, given by

$$\Delta\lambda^2 = \sum_{\boldsymbol{x}} (\Lambda(\boldsymbol{x}) - \bar{\Lambda})^2 P(\boldsymbol{x}|\lambda). \tag{3.5}$$

The Eq. (3.4) indicates how close the estimate is to the real value. While the Eq. (3.5) provides an interval of confidence for each estimation, without requiring knowledge of the true value of the parameter λ. Therefore, MSE highlights the presence of errors in the calibration of the sensor (e.g. due to a potential calibration bias), while the variance is the more interesting quantity to investigate the actual achievable precision for a given measurement. The generalization of Eqs. (3.4) and (3.5) to multiparameter problem is represented by two matrices, the *quadratic loss* (QL) function and the *covariance* matrix, whose generic elements are:

$$\mathrm{QL}(\boldsymbol{\lambda})_{ij} = \sum_{\boldsymbol{x}} (\boldsymbol{\Lambda}(\boldsymbol{x}) - \boldsymbol{\lambda})_i (\boldsymbol{\Lambda}(\boldsymbol{x}) - \boldsymbol{\lambda})_j P(\boldsymbol{x}|\boldsymbol{\lambda}) \tag{3.6}$$

$$\mathrm{Cov}(\boldsymbol{\lambda})_{ij} = \sum_{\boldsymbol{x}} (\boldsymbol{\Lambda}(\boldsymbol{x}) - \bar{\boldsymbol{\Lambda}})_i (\boldsymbol{\Lambda}(\boldsymbol{x}) - \bar{\boldsymbol{\Lambda}})_j P(\boldsymbol{x}|\boldsymbol{\lambda}), \tag{3.7}$$

where $i, j \in \{1, \ldots, d\}$ in presence of d unknown parameters. In addition to the variance terms of the single parameters these matrices contain also the correlation contributions, respectively given by diagonal and off-diagonal matrix terms. Furthermore, in the case of an unbiased estimator the relations (3.6) and (3.7) are the same.

3.1.2 Quantum estimation limits

Realizing the best estimation requires the optimization of the sensor over each aspect of the estimation process, from choosing the probe state to adopt, to setting the measurement to implement, up to selecting the estimator function. This optimization research reveals the uniqueness of a quantum sensor, able to achieve a precision unreachable by any classical counterpart. Let us consider the estimation scenario where probes and measurements are fixed. For clarity, in the following discussion both single- and multi- parameters will be described in parallel, generalizing the first case with matrix relations when the parameters are more than one. A fundamental tool allowing to study the achievable bounds on estimation uncertainties is the *Fisher Information* (FI). It is a quantity able to catch the amount of information encoded in output probabilities of the estimation process, and is defined as [444]:

$$\begin{aligned} &\text{[single-parameter]} \quad F(\lambda) = \sum_x \frac{1}{P(x|\lambda)} \left(\frac{\partial P(x|\lambda)}{\partial \lambda} \right)^2, \\ &\text{[multi-parameters]} \quad \mathbb{F}(\boldsymbol{\lambda})_{ij} = \sum_x \left[\frac{1}{P(x|\boldsymbol{\lambda})} \frac{\partial P(x|\boldsymbol{\lambda})}{\partial \lambda_i} \frac{\partial P(x|\boldsymbol{\lambda})}{\partial \lambda_j} \right]. \end{aligned} \tag{3.8}$$

where the sum is made over the possible outcome values of a single projective measurement x. In particular in the multiparameter scenario the FI generalizes to the real-valued symmetric Fisher Information matrix ($\mathbb{F}$). Intuitively, being $F(\mathbb{F})$ proportional to the derivative(s) with respect to the parameter(s) of the output probabilities, it allows to quantify the sensitivity of the system to a change of $\lambda(\boldsymbol{\lambda})$. More specifically, a larger amount of information is associated with larger variations of the output probabilities. This intuition was formalized with a fundamental result, called *Cramér-Rao bound* (CRB). It links the FI to the ultimate bound achievable by the precision of *any* arbitrary estimator, with fixed ν identical and independent probes and measurements [445, 446]. In the presence of a locally unbiased estimator [Eq. (3.2)], the CRB reads [447, 448]:

$$\begin{aligned} &\text{[single-parameter]} \quad \Delta\lambda^2 \geq \frac{1}{\nu\, F(\lambda)}, \\ &\text{[multi-parameter]} \quad \mathrm{Cov}(\boldsymbol{\lambda})_{ij} \geq \frac{\mathbb{F}^{-1}(\boldsymbol{\lambda})_{ij}}{\nu}, \end{aligned} \tag{3.9}$$

where $i, j \in \{1, \ldots, d\}$ in presence of d unknown parameters. Notably, in the multiparameter case the CRB is well defined only when $\mathbb{F}$ is strictly positive, and thus invertible. An estimator that is able to saturate the inequality (3.9) is said to be *efficient*. The inequality (3.9) indicates the ultimate limits achievable by unbiased estimators when the optimization is made over all possible estimators, but having both probes and measurement fixed. Maximizing the estimation process over all possible quantum measurement, a tighter precision bound is given by the *Quantum Cramér-Rao bound* (QCRB) [1]:

$$\begin{aligned} &\text{[single-parameter]} \quad \Delta\lambda^2 \geq \frac{1}{\nu\, F(\lambda)} \geq \frac{1}{\nu\, F_Q^{-1}(\lambda)}, \\ &\text{[multi-parameter]} \quad \mathrm{Cov}(\boldsymbol{\lambda})_{ij} \geq \frac{\mathbb{F}^{-1}(\boldsymbol{\lambda})_{ij}}{\nu} \geq \frac{\mathbb{F}_Q^{-1}(\boldsymbol{\lambda})_{ij}}{\nu}. \end{aligned} \tag{3.10}$$

where

$$\begin{aligned} &\text{[single-parameter]} \quad F_Q(\lambda) = \max_{E_x} F(\lambda) \\ &\text{[multi-parameter]} \quad \mathbb{F}_Q(\boldsymbol{\lambda}) = \max_{E_x} \mathbb{F}(\boldsymbol{\lambda}) \end{aligned} \tag{3.11}$$

is called *Quantum Fisher Information* (QFI), computed by maximixing the FI over all possible POVMs E_x, having outcome x. The QFI, i.e., represents the amount of information encoded in the interacted probe state $\rho_\lambda(\rho_{\boldsymbol{\lambda}})$, regardless of the measurement. In the multiparameter case, by summing over the diagonal elements of the matrix inequality (3.10), one can estimate the precision of a multiparameter estimator as the trace of the covariance matrix in Eq. (3.7): $\mathrm{Tr}\left[\mathrm{Cov}(\boldsymbol{\lambda})\right] = \sum_i (\Delta\lambda_i)^2$, that obeys the scalar bound

$$\sum_i (\Delta\lambda_i)^2 \geq \frac{\mathrm{Tr}\left[\mathbb{F}^{-1}(\boldsymbol{\lambda}))\right]}{\nu} \geq \frac{\mathrm{Tr}\left[\mathbb{F}_{\mathrm{Q}}^{-1}(\boldsymbol{\lambda}))\right]}{\nu}. \tag{3.12}$$

The QCRB is saturated when the equality in the second part of Eq. (3.10) is reached. Note that it is also possible to define other quantities and bounds, and classify different multiparameter problems [428, 449]. As well as FI, two fundamental properties of the QFI are *additivity* and *convexity*:

$$\mathbb{F}_{\mathrm{Q}}(\bigotimes_i \rho^i_{\boldsymbol{\lambda}}) = \sum_i \mathbb{F}_{\mathrm{Q}}(\rho^i_{\boldsymbol{\lambda}}) \tag{3.13}$$

$$\mathbb{F}_{\mathrm{Q}}(\sum_i c_i\, \rho^i_{\boldsymbol{\lambda}}) \leq \sum_i c_i\, \mathbb{F}_{\mathrm{Q}}(\rho^i_{\boldsymbol{\lambda}}), \tag{3.14}$$

where $\{\rho^i_{\boldsymbol{\lambda}}\}$ in Eqs. (3.13) and (3.14) are respectively, a set of independent prepared probes and the pure states of a general mixed state $\sum_i c_i\, \rho^i_{\boldsymbol{\lambda}}$ (with $\sum_i c_i = 1$). The maximum sensitivity of a quantum state for a parameter estimation is intimately related with the metric of the state [450, 451, 431, 452]. In particular the distinguishability of the probe state for small variation of the parameters is directly linked to the QFI. The distinguishability between two states, ρ_1 and ρ_2 can be quantified by the normalized Bures geometric distance: $\tilde{D}_{\mathrm{B}}(\rho_1, \rho_2) = \sqrt{1 - \tilde{F}(\rho_1, \rho_2)}$, where $\tilde{F}(\rho_1, \rho_2) = \mathrm{Tr}\left[\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}}\right]^2$ is the standard fidelity (Sec. 1.2.4.1). Given the state $\rho_\lambda(\rho_{\boldsymbol{\lambda}})$ and an infinitesimal change $\delta\lambda(\delta\boldsymbol{\lambda}_i)$ of the parameter(s), the normalized distance squared between ρ_λ and $\rho_{\lambda+\delta\lambda}$ ($\rho_{\boldsymbol{\lambda}}$ and $\rho_{\boldsymbol{\lambda}+\delta\boldsymbol{\lambda}}$) is proportional to $F_{\mathrm{Q}}(\rho_\lambda)(\mathbb{F}_{\mathrm{Q}\,ij}(\rho_{\boldsymbol{\lambda}}))$ [453, 359]:

$$\begin{aligned} &\text{[single-parameter]} \quad \tilde{D}_{\mathrm{B}}(\rho_\lambda, \rho_{\lambda+\delta\lambda})^2 = \frac{1}{8} F_{\mathrm{Q}}(\rho_\lambda)\, (\delta\lambda)^2, \\ &\text{[multi-parameter]} \quad \tilde{D}_{\mathrm{B}}(\rho_{\boldsymbol{\lambda}}, \rho_{\boldsymbol{\lambda}+\delta\boldsymbol{\lambda}})^2 = \frac{1}{8} \sum_{ij} \mathbb{F}_{\mathrm{Q}\,ij}(\rho_{\boldsymbol{\lambda}})\, \delta\lambda_i\, \delta\lambda_j. \end{aligned} \tag{3.15}$$

From these expressions it is clear that the more ρ_λ and $\rho_{\lambda+\delta\lambda}$ ($\rho_{\boldsymbol{\lambda}}$ and $\rho_{\boldsymbol{\lambda}+\delta\boldsymbol{\lambda}}$) are "distant", i.e. distinguishable, the greater is $F_{\mathrm{Q}}(\rho_\lambda)(\mathbb{F}_{\mathrm{Q}\,ij}(\rho_{\boldsymbol{\lambda}}))$ and thus the sensibility of the state to $\lambda(\boldsymbol{\lambda})$.

One of the goals of Quantum Metrology is to find measurements that are able, given a probe state, to reach the ultimate precision and then to saturate the QCRB in Eq. (3.10). This task is equivalent to find the POVM such that the FI associated

to the process becomes equal to the corresponding QFI associated to the probe state. The aim is then to find the measurement such that $F = F_{\mathrm{Q}}$. Indeed, if a large number of probes is available, the estimators to asymptotically saturate QCRB are known, such as maximum likelihood and Bayesian estimators (Sec. 3.1.2.2). Nevertheless, in the case of limited measurements and data, the saturation of the CRB is no more guaranteed [454].

3.1.2.1 Standard quantum limit and Heisenberg limit

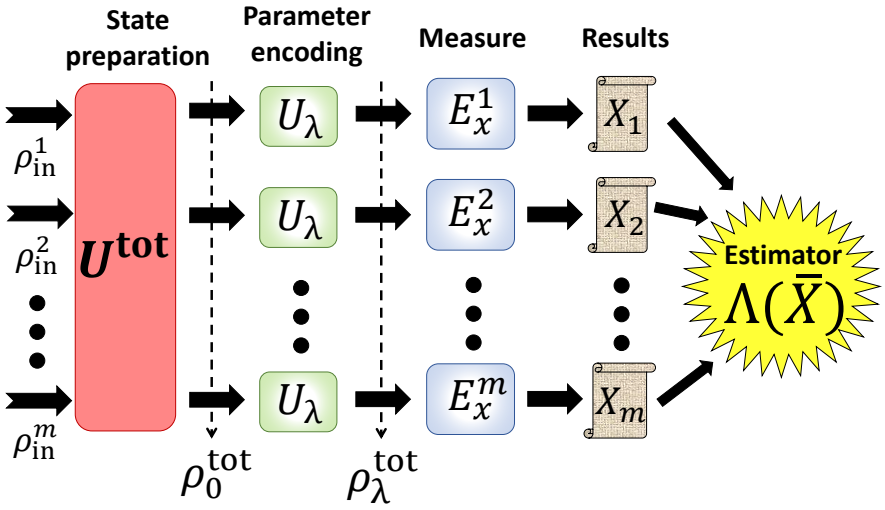

Figure 3.2. Conceptual scheme of a parallel parameter estimation. The measurements here considered are separable. Indeed, employing entanglement in the measurement process does not allow to obtain better performances than the optimal separable strategy. Conversely, state preparation can lead to quantum enhancement by exploiting entanglement between probes [358]. This image is taken from [1].

In the single parameter case it is always possible to saturate the QCRB through suitable measurements [451]. Because of F_{Q}'s additivity property [Eq. (3.13)] it is possible to saturate QCRB using local adaptive measurements for each probe without entangling measurements [455, 456, 457, 458, 358, 459]. Then quantum resources in the measurement stage do not enhance the estimation process [357, 358]. Since in general the optimal POVMs can depend on λ-value, it may be necessary to have a priori knowledge on the parameter. This difficulty can be overcome through adaptive estimation protocols (Sec. 3.3). The last step, in order to find the ultimate fundamental bounds, is the optimization over all possible input states. This task can be done by optimizing F_{Q} over the initial probes. If the evolution of the interaction is unitary, $\rho_\lambda = e^{i\lambda H}\rho_0 e^{-i\lambda H}$, or equivalently $\partial_\lambda \rho_\lambda = i[\rho_\lambda, H]$, where H is an Hermitian operator, F_{Q} does not depend on the unknown parameter. Therefore, the QCRB depends only on the state of the probe ρ_λ after the interaction and there is a crucial difference between quantum and classical states. Quantum states can outperform classical ones, reaching the ultimate quantum limits. In this way there is a precision region achievable only by exploiting quantum probes, meaning that a quantum enhancement in the Metrology task can be obtained. Let us consider the parallel strategy depicted in Fig. 3.2. Here, m probes interact with the system,

independently, with a separable linear unitary $U^{\rm tot} = \bigotimes_{i=1}^{m} U_\lambda^i$, with U_λ^i acting only on the i-th probe and such that $U_\lambda^i = U_\lambda \; \forall \, i$. The first property of optimal probes can be derived from the convexity (3.14) of $F_{\rm Q}$: the maximum of $F_{\rm Q}$ is always achieved by pure states.

We initially focus on m probes that are classically correlated, that is, non entangled. The total state can be then written as a convex combination of separable states, each one of the following form: $\rho^{\rm tot} = \rho_1 \otimes \rho_2 \cdots \otimes \rho_m$. The value of $F_{\rm Q}$ for a separable state is:

$$F_{\rm Q}(\rho_1 \otimes \rho_2 \cdots \otimes \rho_m) = \sum_i^m F_{\rm Q}(\rho_i) \leq m \;\; F_{\rm Q}^{\rm max}, \tag{3.16}$$

where for the first equality the additivity of $F_{\rm Q}$ has been exploited, and $F_{\rm Q}^{\rm max}$ represents the maximum of $F_{\rm Q}$ over the states ρ_m. Then, in presence of ν independent packets of m classical correlated probes, from Eq. (3.10) the minimum uncertainty $\Delta\lambda$ scales as [358, 460]:

$$\Delta\lambda \geq \frac{1}{\sqrt{\nu \; m \; F_{\rm Q}^{max}}}. \tag{3.17}$$

Since $F_{\rm Q}^{\rm max}$ is a constant factor, the error scaling with the number of the probes m is $\Delta\lambda \propto 1/\sqrt{m}$. Namely this statistical bound is called *standard quantum limit* (SQL) (or *shot noise limit* when dealing with setups involving interferometers). Such bound corresponds to the QCRB optimized over any arbitrary classically correlated probe state and can be seen as a consequence of the central limit theorem. We have seen that quantum resources in the measurement stage are not necessary to reach the QCRB. Conversely, quantum resources employed for the preparation of probe states can enhance the sensitivity with respect to classical approaches, beating the SQL [410, 461, 376, 462, 357, 358, 2].

A key role to obtain quantum enhancement is played by entanglement. In particular, assuming unitary evolution and calling $h_{\rm S}$ ($h_{\rm s}$) the maximum (minimum) eigenvalue of the generator H, the relation:

$$F_{\rm Q}(\rho_0, H) > m \; (h_{\rm S} - h_{\rm s}), \tag{3.18}$$

is a sufficient condition for the presence of entanglement in the probe state ρ_0 [460]. It turns out that entanglement, in the considered estimation scheme, is necessary in order to have an enhancement in estimation. Eq. (3.18) can be exploited to detect entanglement [463, 464, 465, 434, 466]: if the Fisher Information, that can be extracted for instance from an experimental characterization of the state, satisfies Eq. (3.18) then the state is entangled. Furthermore, this condition is necessary and sufficient to achieve estimation precision beyond SQL [361, 433]. This captures the fundamental relation between entanglement and quantum enhanced metrology. However not all entangled states are able to satisfy inequality (3.18) then this condition is sufficient but not necessary for the presence of entanglement. Then, such relation defines also the concept of *useful entanglement* for Quantum Metrology [460]. In particular, in Refs. [440, 467] the authors investigate the role of mode- and particle-entanglement for quantum-enhanced performances in parameters estimation.

In order to identify the states which provide the best quantum enhancement, let us consider pure states and unitary evolution $e^{-i\lambda H}$. In this case, the QCRB is saturated by states of the form:

$$\frac{|h_{\rm max}\rangle + e^{i\gamma} \, |h_{\rm min}\rangle}{\sqrt{2}}, \tag{3.19}$$

where $\gamma \in \mathbb{C}$, while $|h_{\max}\rangle$ and $|h_{\min}\rangle$ are the eigenvectors corresponding to the maximum and minimum eigenvalues $h_{\max}$ and $h_{\min}$ of H, respectively. If we define $|h_{\rm S}\rangle$ ($|h_{\rm s}\rangle$) as the single probe eigenstate of the generator H relative to the maximum (minimum) eigenvalue $h_{\rm S}$ ($h_{\rm s}$), then the optimal state in Eq. (3.19) is realized by [358]:

$$\frac{|h_{\rm S}\rangle^{\otimes m} + e^{i\gamma}\,|h_{\rm s}\rangle^{\otimes m}}{\sqrt{2}}. \tag{3.20}$$

where m is the number of employed probes. Such state is a maximally entangled state and has $F = m^2(h_{\rm S} - h_{\rm s})^2 (\equiv F_Q)$, which is useful entanglement for $m > 1/(h_{\rm S} - h_{\rm s})$. For ν independent packets of states in Eq. (3.20), the QCRB becomes [358]:

$$\Delta\lambda \geq \frac{1}{\sqrt{\nu}\; m\; (h_{\rm S} - h_{\rm s})}. \tag{3.21}$$

The term $(h_{\rm S} - h_{\rm s})$ is a constant so, here, the error scaling with the number m of probes is $\Delta\lambda \propto 1/m$, that corresponds to an improvement of the precision by a factor $\sqrt{m}$ with respect to SQL. This enhanced scaling is the ultimate limit on estimation precision and is called *Heisenberg limit* (HL). The Heisenberg limit in Eq. (3.21) is saturable in the limit of large independent repetitions ν of m entangled states.

Until now, we have defined the HL scaling for the case of parallel estimation strategies and linear unitary evolutions, in which the Hamiltonian does not generate correlations between different probes. If we consider schemes with non-linear interactions between probes and system, the scaling can be different [468, 469, 470, 471]. Furthermore, if one exploits resources other than the number of particles, the SQL can also be beaten with non-entangled probes [358]. This is obtained for instance through multiround protocols [472, 473, 474, 475, 476, 477], in which the additional employed resource is the running time of the estimation process.

Also the multiparameter case can be enhanced by using quantum resources. In order to find the best possible accuracy in the estimation, it is fundamental to find necessary and sufficient conditions to saturate the QCRB. However, the possibility of achieving the ultimate quantum bounds in multiparameter estimations is not guaranteed [478, 447, 479, 480, 481, 482], at variance with the single parameter case [359]. Indeed, when different parameters have to be estimated, the corresponding optimal measurements may not commute, thus making impossible their implementation in a single experiment [483]. In this way, the capability of achieving the ultimate bounds is forbidden. A necessary condition for the attainability of the multiparameter QCRB inequality is provided when the optimal measurements for the estimation of the single parameters are compatible observables [484, 480], which in general may not be satisfied. Importantly, for pure states with invertible $\mathbb{F}_{\rm Q}$ there exists a necessary and sufficient condition for the saturation of the QCRB [480]. In Ref. [482] the authors generalize such results. In particular, in the case of pure states necessary and sufficient conditions on projective measurements are derived such that the Fisher Information matrix $\mathbb{F}$ is equal to $\mathbb{F}_{\rm Q}$ even if $\mathbb{F}_{\rm Q}$ is not invertible. If $\mathbb{F}_{\rm Q}$ is invertible, such conditions are necessary and sufficient also for the saturation of QCRB. When the generators of the parameters commute and the probe state is pure the QCRB can be saturated [484, 482]. Several studies, such as Refs. [485, 484, 467, 486, 487], have investigated, in different scenarios, the potential advantages of performing multiparameter estimation with respect to sequential single-parameter strategies. Despite the broad range of applications, the number of experimental implementations of quantum multiparameter estimation

tasks is surprisingly few. In this scenario, photons can be employed with different schemes and approaches [427, 428, 429, 430]. In Sec. 3.1.3.1 we list some of the problems involving multiple phases that have been approached through photonic platforms.

As a conclusion, a table reporting each relevant optimization of the estimation process is shown in Table 3.2.

Quantity	Probe $\boldsymbol{\rho_0}$	POVM $\boldsymbol{E_x}$	Estimator $\boldsymbol{\Lambda(x)}$
Qloss($\boldsymbol{\lambda}$) [Eq. (3.6)]	fixed	fixed	fixed
$\mathbb{F}(\boldsymbol{\lambda})$ [Eq. (3.8)]	fixed	fixed	optimized
$\mathbb{F}_{\mathrm{Q}}(\boldsymbol{\lambda})$ [Eq. (3.11)]	fixed	optimized	optimized
SQL [Eq. (3.17)]	classically optimized	optimized	optimized
HL [Eq. (3.21)]	quantum optimized	optimized	optimized

Table 3.2. Table of the relevant metrology quantities, indicating which step of the estimation protocol is optimized.

3.1.2.2 Estimators

Different approaches exist to post-process experimental data and provide an optimal estimation of the unknown parameter [432].

One of the most widely adopted estimators is the *maximum likelihood estimator* (MLE) [444]. It is the value of the multiparameter vector $\boldsymbol{\lambda}$ that, given a list of experimental results $\boldsymbol{x}$, maximizes the likelihood probability $P(\boldsymbol{x}|\boldsymbol{\lambda})$:

$$\boldsymbol{\Lambda}^{\mathrm{MLE}}(\boldsymbol{x}) = \arg\left[\max_{\{\boldsymbol{\lambda}\}} P(\boldsymbol{x}|\boldsymbol{\lambda})\right] . \tag{3.22}$$

In the asymptotic limit the MLE is unbiased, consistent and saturates the Cramer Rao bound (see Sec. 3.1.2). Other estimators are *Bayesian estimator* or the *Method of Moments*, the latter not requiring full knowledge of the likelihood function [433].

While MLE with the relative estimation bounds (see Sec. 3.1.2) is based on a frequentist interpretation of the probability, in the Bayesian approach the conceptual meaning of probability is that of a degree of belief. In this sense Bayesian approach can be exploited as a framework to devise estimation protocols [488, 489, 490, 491]. In this approach, the unknown parameters $\boldsymbol{\lambda}$ and the experimental result x are treated as random variables. Here the relevant quantity is the degree of ignorance (or knowledge, equivalently) about the parameter. During a Bayesian estimation such knowledge, that can be regarded as subjective (degree of belief), is updated according to the measurement results.

The starting point of the process is the *prior distribution* $P(\boldsymbol{\lambda})$ that quantifies the initial ignorance on the unknown parameter. The experimental setup probing the system is described by the likelihood function $P(x|\boldsymbol{\lambda})$ [Eq. (3.3)]. Once a measurement result x is obtained, the degree of knowledge, described by the *posterior probability* $P(\boldsymbol{\lambda}|x)$, is updated by the Bayes' rule:

$$P(\boldsymbol{\lambda}|x) = \frac{P(\boldsymbol{\lambda})\ P(x|\boldsymbol{\lambda})}{\int P(\boldsymbol{\lambda})\ P(x|\boldsymbol{\lambda}) \prod_i d\lambda_i} , \tag{3.23}$$

where the integral in the normalization term has to be replaced by a sum when the unknown parameters $\boldsymbol{\lambda}$ assume discrete values. The posterior in Eq. (3.23) contains the updated information from which interesting quantities can be calculated.

For instance, the quadratic loss of an estimator $\boldsymbol{\Lambda}(x)$ [Eq. (3.6)], averaged over the parameters $\boldsymbol{\lambda}$, is obtained as:

$$\langle \mathrm{QL}(\boldsymbol{\lambda}) \rangle = \int P(\boldsymbol{\lambda}) P(x|\boldsymbol{\lambda}) \, (\boldsymbol{\Lambda}(x) - \boldsymbol{\lambda})^2 \, dx \prod_i d\lambda_i \, . \tag{3.24}$$

By minimizing Eq. (3.24), the optimal Bayesian estimator $\boldsymbol{\Lambda}^{\mathrm{opt}}(x)$ is calculated:

$$\boldsymbol{\Lambda}^{\mathrm{opt}}(x) = \int \boldsymbol{\lambda} \, P(\boldsymbol{\lambda}|x) \prod_i d\lambda_i \, , \tag{3.25}$$

that corresponds to the mean value of the parameters over the posterior distribution. Also other moments, such as the third moment, of this distribution can be informative on the estimation, especially to detect possible biases [492].

This thesis is particularly interested in the phase estimation problem (Sec. 3.1.3). The case of a single phase shift ϕ estimated inside an interferometer is a circular parameter, where $\phi = \phi + 2k\pi$ with $k \in \mathbb{Z}$. For such parameter a circular mean, calculated over the posterior distribution, can be defined:

$$\langle \phi \rangle^{\mathrm{circ}} = \arg \left[\int d\phi e^{i\phi} \, P(\phi|x) \right] . \tag{3.26}$$

The standard variance with circular variables is no more adequate and the *Holevo variance* V^{H} can be defined, as function of a quantity S called *Sharpness* [493]:

$$V^{\mathrm{H}} = S^{-2} - 1 \qquad\qquad S = |\langle e^{i\phi} \rangle|, \tag{3.27}$$

where the mean $\langle \cdot \rangle$ is calculated over the probability distribution of the estimation process under study. The Holevo variance can describe the variance of unbiased phase estimators, $V^{\mathrm{H}}_{\mathrm{unbias}} = \left| \langle e^{i\Phi} \rangle \right|^{-2} - 1$, and coincides with the standard variance for sufficiently sharply picked distribution. With biased estimators, the variance is: $V^{\mathrm{H}}_{\mathrm{bias}} = |\langle \cos(\Phi - \phi) \rangle|^{-2} - 1$. A Bayesian analysis of the sensitivity of coherent states in an optical interferometer for the estimation of a phase shift, has been carried in Ref. [494]. A fundamental feature of a Bayesian approach is its direct application to adaptive protocols, described in Sec. 3.1.4. Note that, since a Bayesian approach allows to exploit prior knowledge on the parameters, the sensitivity bounds can be different from those relative to the frequentist approach [495, 496]: for MLE (frequentist approach) the error is defined by the mean square fluctuations, while in a Bayesian approach the uncertainty is quantified by the variance of the posterior, that is a different concept respect to MSE.

3.1.3 Single- and multi-phase estimation problem

Single-phase estimation

One of the most relevant scenarios for Quantum Metrology is phase estimation [497, 357, 433]. The problem consists of estimating an unknown phase shift ϕ between two different modes, such as polarization, OAM or different paths. A lot of physical problems can be cast in a general phase shift estimation, and different physical probes can be employed. Tasks such as measurements of atomic properties [498, 499], atomic clocks [500, 366], measurements of forces [501, 502], require the use of atomic probes [361]. Conversely, for tasks like the estimation of phase shifts produced by gravitational waves [365], lithography [379, 380, 381, 382], imaging [383, 384, 385, 386, 389, 387, 390, 388, 403, 391], sensing on biological systems [363], quantum key distribution [503], measurements of velocity, displacements and lengths [2], photons are the most suitable systems. Besides the practical applications, phase estimation represents also a standard benchmark for general metrological protocols.

Consider an estimation of a phase shift ϕ between two paths. The transition of a system through a phase shift along a mode, say mode 1, is described by the unitary evolution:

$$U_{\rm ps} = e^{i\phi H_{\rm ps}} = e^{i\phi a_1^\dagger a_1}, \tag{3.28}$$

where a_1 is the particle annihilation operator along mode 1. The generator and conjugated operator [504] of the phase shift is the number operator n_1 along the corresponding mode:

$$H_{\rm ps} = a_1^\dagger a_1 = n_1. \tag{3.29}$$

For the number operator n_1, the difference of possible eigenvalues, with a single probe, is $h_{\rm S} - h_{\rm s} = 1$. Then, following the same notation as in Sec. 3.1.2.1, Eq. (3.17) for phase estimation reads:

$$\Delta\phi_{\rm SQL} \geq \frac{1}{\sqrt{\nu\, m}}. \tag{3.30}$$

corresponding to the SQL for the single phase estimation. Conversely, the HL then reads:

$$\Delta\phi_{\rm HL} \geq \frac{1}{\sqrt{\nu}\, m}. \tag{3.31}$$

Since a general definition of a standard selfadjoint operator associated to phase shift measurement is problematic, its direct sharp measurement is not possible [505]. Nevertheless, a phase shift can be treated as an evolution parameter and estimated from other observables whose values depend on it. In particular in optical phase estimation, the phase shifts are differences between optical paths that can be estimated through interferometers. One of the most common and simple two-mode optical interferometers, suitable for phase estimation, is the *Mach-Zehnder interferometer* (MZI) [506].

The two key elements of a MZI are the PS and the BS (Sec. 1.1.2.1). The former adds a phase shift ϕ between two modes whose annihilation operators are a_1 and a_2 [Eq. (1.9)]. The BS represents a basic optical element that allows mixing between two input electromagnetic modes. It can be realized with a partially reflective mirror that transmits or reflects the incoming light. In particular we consider here the

balanced BS whose transmission and reflection probabilities are equal to 0.5, whose action is described by:

$$\mathrm{BS}_{\pm} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & \pm i \\ \pm i & 1 \end{pmatrix}, \tag{3.32}$$

where BS_+ and BS_- differ of an irrelevant, for our purpose, phase shift. The mode operator $b_i^\dagger$ generated by a unitary evolution U on modes $a_k^\dagger$, will be: $b_i^\dagger = \sum_k U_{ik}\, a_k^\dagger$. A MZI interferometer is composed of cascaded two BS interspersed with a PS (Fig. 3.3). In the lossless scenario, up to a global phase, it is described by:

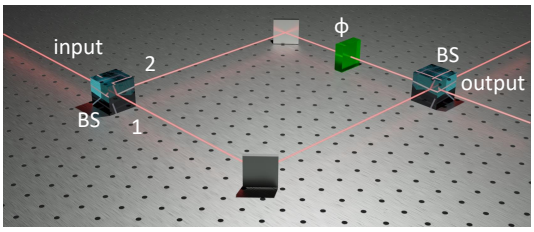

Figure 3.3. Scheme of a Mach-Zehnder interferometer. A MZI is composed of two beam splitters (BS) and a phase shift ϕ between the modes, 1 and 2, of the interferometer. This image is taken from [1].

$$\mathrm{MZI}(\phi) = \mathrm{BS}_+\, \mathrm{PS}(\phi)\, \mathrm{BS}_- = \begin{pmatrix} \cos(\frac{\phi}{2}) & -\sin(\frac{\phi}{2}) \\ \sin(\frac{\phi}{2}) & \cos(\frac{\phi}{2}) \end{pmatrix}. \tag{3.33}$$

The first BS can be seen as a preparation step of the estimation process, while the last one as part of the measurement step. In general the output probabilities of photons exiting from a MZI depend on the phase ϕ. Since the Fisher Information depends on the derivatives of the output probabilities, the probe is more sensitive to a phase shift change for larger variation of the fringe pattern.

A convenient way to express the MZI operation on electromagnetic modes is based on Pauli matrices [Eqs. (1.2)] expressed through the annihilation operators for modes 1 and 2 (a_1 and a_2): $\sigma_X = a_1^\dagger a_2 + a_2^\dagger a_1$, $\sigma_Y = -i(a_1^\dagger a_2 - a_2^\dagger a_1)$ and $\sigma_Z = a_1^\dagger a_1 - a_2^\dagger a_2$. The following relations hold [507]:

$$\begin{aligned} \mathrm{PS}(\phi) &= e^{-\imath\phi\sigma_Z/2} \quad \mathrm{BS}_{\pm} = e^{\pm\imath\pi\sigma_X/4} \\ \mathrm{MZI}(\phi) &= \mathrm{BS}_+\, \mathrm{PS}(\phi)\, \mathrm{BS}_- = e^{-\imath\phi\sigma_Y/2}. \end{aligned} \tag{3.34}$$

Two cascaded independent PSs interspersed by a MZI can realize any unitary belonging to Lie SU(2) group. MZI transformation is used also as interferometer in other degrees of freedom like polarization, for which the BSs are replaced by HWPs rotated by 22.5°.

Besides the applications to Quantum Metrology and in general to quantum information tasks, a MZI can be also the testbed for foundational tests, like those exploring wave-particle duality of photons [508, 509, 510] or even quantum gravity phenomena when the probes are massive systems [511, 512].

Estimation of multiple phases

An important task in quantum multiparameter estimation is provided by those problems where the physical quantities to be estimated are multiple phases. This

scenario has been intensively studied in the last years [486, 429, 513, 514, 485, 515, 516, 517, 487, 518, 482, 467, 519, 520, 521, 14, 15]. More specifically, the unknown parameters are relative phases corresponding to different paths in an interferometer with respect to a common reference. Besides direct mapping of this problem to quantum imaging, multiphase estimation can represent a benchmark suitable for tests of quantum multiparameter protocols. Its importance and generality derives also from the fact that unitary evolutions generally introduce a phase in the evolved states.

Let us now consider multiphase estimation in a multiarm interferometer. Here, the unknown parameters are a set of phases (relative to a reference) along d arms of an interferometer: $\boldsymbol{\phi} = (\phi_1, \phi_2, ..., \phi_d)$. The general scheme of a multiphase estimation is sketched in Fig. 3.4. Preparation of the probe along the $(d+1)$ paths

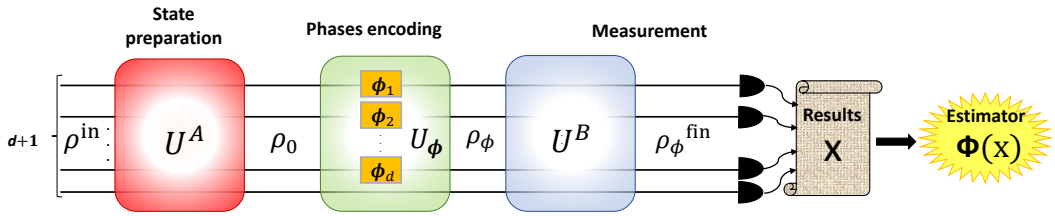

Figure 3.4. Multiphase estimation scheme. An initial probe ρ^{in}, living in the space of the $(d+1)$ paths, is prepared in a state ρ_0 through a unitary evolution U^A. Then, the probe interacts with the phases $\phi_1, ..., \phi_d$ according to an evolution $U_{\boldsymbol{\phi}}$. The state is measured by means of a unitary U^B followed by a projective measurement, giving outcome $\boldsymbol{x}$. Finally, an estimate of the unknown phases is given by a suitable estimator $\boldsymbol{\Phi}(\boldsymbol{x})$. This image is taken from [1].

is realized by an operation U^A, considered to be unitary for simplicity. After the evolution $U_{\boldsymbol{\phi}}$, that depends on the unknown phases $\phi_1, ..., \phi_d$, the state is measured through a second unitary U^B and projective measurements performed on the output paths. Finally, a suitable estimator $\boldsymbol{\Phi}(\boldsymbol{x}) = [\Phi_1(\boldsymbol{x}), \Phi_2(\boldsymbol{x}), ..., \Phi_d(\boldsymbol{x})]$ provides an estimate of the phases by exploiting the m measurement outcomes $\boldsymbol{x} = (x_1, ..., x_m)$.

For pure input probes, prepared in $|\Psi_0\rangle$, the state after the phase unitary evolution $U_{\boldsymbol{\phi}}$ reads $|\Psi_{\boldsymbol{\phi}}\rangle = U_{\boldsymbol{\phi}}|\Psi_0\rangle$, where $U_{\boldsymbol{\phi}} = e^{(i\sum_{i=1}^{d} O_i\phi_i)}$. In this expression, each O_i represents the generator of the phase shift ϕ_i along the mode i. When the operators O_i mutually commute, and hence $[O_i, O_j] = 0\ \forall i, j$, the Quantum Fisher Information matrix $\mathbb{F}_{\text{Q}}$ takes the following form:

$$\mathbb{F}_{\text{Q}}(\boldsymbol{\phi})_{ij} = 4[\langle O_i O_j\rangle - \langle O_i\rangle\langle O_j\rangle], \tag{3.35}$$

where the average $\langle\cdot\rangle$ is calculated with respect to state $|\Psi_{\boldsymbol{\phi}}\rangle$. When the phases are those corresponding to independent modes, the generators are $O_i = n_i$, where n_i is the photon number operator for mode i. Since $[n_i, n_j] = 0\ \forall i, j$, from (3.35) we find that $\mathbb{F}_{\text{Q}}(\boldsymbol{\phi})_{ij} = 4[\langle n_i n_j\rangle - \langle n_i\rangle\langle n_j\rangle]$. Hence, the Quantum Fisher Information $F_{\text{Q}\phi_i}$ of a single phase ϕ_i corresponds to:

$$F_{\text{Q}\phi_i} = \mathbb{F}_{\text{Q}ii} = 4\langle(\Delta n_i)^2\rangle, \tag{3.36}$$

where $(\Delta n_i)^2$ is the variance of the photon number operator n_i.

One of the first studies on simultaneous quantum enhanced estimation of multiple independent phases was performed in Ref. [485]. The authors considered probe states with a fixed number of photons, and a number d of independent phase differences to

be estimated for d modes of an interferometer with respect to an additional reference mode. The simultaneous estimation of the phases can provide an advantage in the variance that scales as $O(d)$, with respect to the best quantum strategy that estimates such phases individually [485]. In particular, this result is demonstrated using suitable optimized projective measurements on the optimal quantum probe states of the form:

$$|\Psi\rangle_{\text{opt}} = \frac{1}{\sqrt{d+\sqrt{d}}}[|0,N,\ldots,0,0\rangle + ... + |0,0,\ldots,N,0\rangle + \\ + |0,0,\ldots 0,N\rangle] + \sqrt{\frac{\sqrt{d}}{d+\sqrt{d}}}|N,0,\ldots 0,0\rangle, \tag{3.37}$$

where N is the number of photons contained in the probe state. The state is distributed along $d+1$ modes and the last term of the superposition indicates N photons occupying the reference arm. Such optimal states lead to a total variance equal to:

$$\sum_{i=1}^{d}(\Delta\phi_i)^2_{\text{opt}} \geq \text{Tr}\left[\mathbb{F}_{\text{Q}}^{\text{opt}\,-1}\right] = \frac{(1+\sqrt{d})^2\,d}{4\,N^2}, \tag{3.38}$$

This leads to an advantage (in the variance) of a factor $O(d)$ with respect to the optimal separate quantum single-phase estimation leading to $\text{Tr}\left[\mathbb{F}_{\text{Q}}^{\text{sep}\,-1}\right] \geq d^3/N^2$. This enhancement achieved by performing simultaneous estimation can be found also with noncommuting unitary parameter generators [522] and in the presence of small amount of losses [479]. A simultaneous multiphase estimation can even provide a higher advantage by using entangled coherent states [516, 513]. In particular, Ref. [513], generalizes the result of Ref. [485] studying generalized multimode N00N-like states with arbitrary states along the non-vacuum mode.

Multiphase estimation in multimode interferometers has been theoretically studied in Refs. [518, 523]. A bound on the achievable sensitivity using separable probe states has been obtained [518], providing conditions of useful entanglement for the simultaneous estimation. A multimode interferometer is composed of two cascaded $(d+1)$-mode balanced multiport splitters (the $(d+1)$-mode extension of beam splitters), resembling the structure of a Mach-Zehnder interferomer. The internal modes include d independent phase shifts between the different internal paths with respect to one of the modes acting as a reference. In Ref. [518] the authors study input multimode Fock states $|1\rangle_1 \otimes |1\rangle_2 \cdot\cdot \otimes |1\rangle_{d+1} \equiv |11\cdot\cdot1\rangle$, where $|1\rangle_i$ represent a single photon along the mode i. The benchmark for the sensitivity in Eq. (3.12) is given by the lower estimator variance, achievable by using m separable photons to jointly estimate the d phases [460, 518]:

$$\sum_{i=1}^{d}\Delta\phi_i^2 \geq \frac{\text{Tr}\left[\mathbb{F}^{-1}(\boldsymbol{\phi})\right]}{m} \geq \frac{d}{m}. \tag{3.39}$$

This limit is valid for each separable state transformed by the action of the phase generators, and for all possible POVMs. Hence, it represents the classical limit in this scenario. Useful entanglement is then present in the state when the variance of the estimator is lower than the bound (3.39). Such bound can be surpassed by injecting indistinguishable photons into the multimode interferometer [518]. To reach optimal and symmetric bounds for each value of the jointly estimated phases, an adaptive estimation protocol can be in principle exploited (Sec. 3.1.4). This is obtained by

employing additional control phases along the mode of the interferometer to perform adaptive measurements [518].

A deeper insight in multiphase estimation is obtained by using the CRB/QCRB inequality in its matrix formulation of Eq. (3.10): $\mathrm{Cov}(\boldsymbol{\phi}) \geq \mathbb{F}^{-1}(\boldsymbol{\phi})/\nu \geq \mathbb{F}_{\mathrm{Q}}^{-1}(\boldsymbol{\phi})/\nu$, being ν the number of repeated independent measurements. The relevance of considering the covariance matrix $\mathrm{Cov}(\boldsymbol{\phi})$ to study the sensitivity bounds is highlighted by the possibility to compare any target scenario, with corresponding Fisher information matrix $\mathbb{F}_{\mathrm{target}}$, with a benchmark state associated to a Fisher information $\mathbb{F}_{\mathrm{bench}}$. As shown by Ref. [467] such comparison can be studied through the matrix $\mathbb{F}_{\mathrm{target}}$ - $\mathbb{F}_{\mathrm{bench}}$. Indeed, the number of positive eigenvalues of this matrix corresponds to the number of independent combinations of the unknown parameters [467] for which the target state provides an enhancement compared to the benchmark state.

3.1.3.1 Photonic platforms for multiphase estimation

Photonic systems represent the most natural platform for multiphase estimation problems. Surprisingly, not many experimental realizations of quantum multiphase estimation have been reported.

As previously discussed, a relevant benchmark problem is represented by the estimation of different optical phases along different spatial paths, with direct application in the vast area of imaging. Integrated circuits represent an ideal and scalable platform to investigate experimentally such scenario. Besides the quality of spatial mode interactions, integrated photonics provides the stability that is necessary to estimate relative phases along different paths, which is almost impossible to achieve in bulk optics platforms because of thermal fluctuations and mechanical vibrations.

The work [14] realized during this thesis, represents the first experimental implementation of multiphase estimation enhanced by quantum states (Sec. 3.2.1). The employed platform is an integrated three-mode interferometer realized through the femtosecond laser writing technique (Fig.3.5a). After calibrating the device, the capability to achieve quantum advantage in multiphase estimation was experimentally demonstrated by performing two-photon measurements [14]. In particular, the Fisher Information of the device $\mathbb{F}_{\mathrm{exp}}$ was estimated from experimental data and compared with that relative to the optimal simultaneous strategy with separable probes ($\mathbb{F}_{\mathrm{cl}}$). For some values of the unknown phases, the matrix $\mathbb{F}_{\mathrm{exp}}$ - $\mathbb{F}_{\mathrm{cl}}$ has two positive eigenvalues demonstrating a quantum advantage reached by the circuit. Such advantage can be in principle extended to all pairs of phases through adaptive protocols (Sec. 3.1.4). The sensitivity enhancement was achieved experimentally with respect to classical strategies, considering as resources the number of effectively detected coincidences [14]. The same setup has also been exploited in Ref. [15] for the implementation of a Bayesian adaptive multiphase estimation [394] using single photons inputs (Sec. 3.3.2).

Recently, distributed quantum sensing of the linear combination (arithmetic average) of multiple small phases along four distant nodes was performed [520]. The scenario [528] is a network of M nodes along which independent relative phase shifts ϕ_i, with $i = 1, ..., M$, one for each node, are experienced by the probes. The final goal is to estimate the arithmetic average of the phases: $\bar{\phi} = \sum_{i=1}^{M} \phi_i/M$. The employed probe state is a squeezed coherent state of the form $D(\alpha)S(r)\left|0\right\rangle$, where $D(\alpha)$ is the displacement operator with amplitude α, and $S(r)$ is the squeezing single mode operator with squeezing parameter r [1]. The output state is detected through homodyne detectors along each node, thus measuring the phase quadratures P_i $(i = 1, ..., M)$ representing the estimators for the phases. Given such kind of state, two classes of estimation experiments are possible: (i) separable estimation in

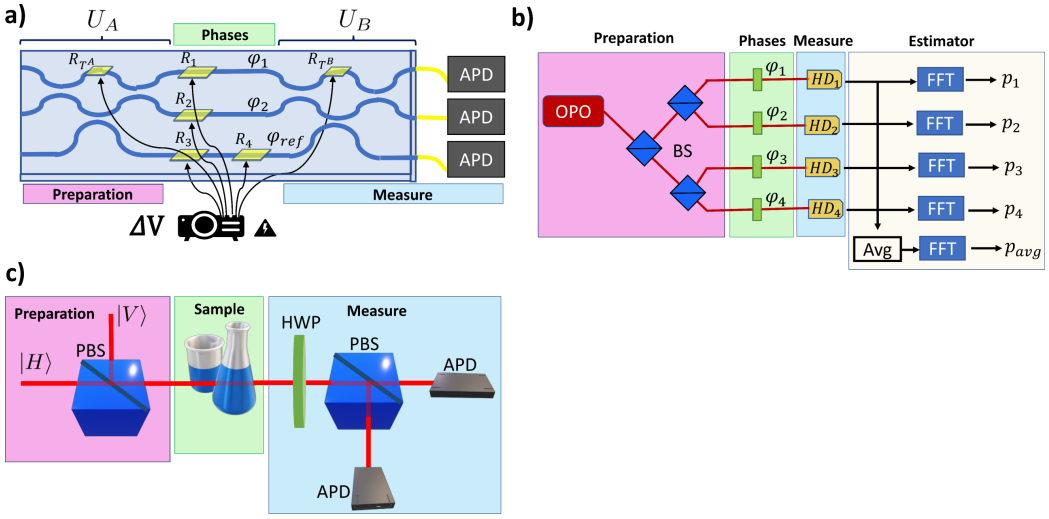

Figure 3.5. Photonic platforms for multiparameter problems. a Integrated platform for the simultaneous estimation of two phases $\Delta\phi_1 = \varphi_1 - \varphi_{\text{ref}}$ and $\Delta\phi_2 = \varphi_2 - \varphi_{\text{ref}}$. The probe states are two indistinguishable photons. The unitaries $U_{A/B}$ represent the 2-D decomposition of tritters, while R_i are the resistors used to tune the phases. Described in Ref.[14]. **b** Scheme of the apparatus for the distributed sensing of the average of four phases $\varphi_1, ..., \varphi_4$. In the entangled estimation, the probes are squeezed coherent states generated in the optical parametric oscillator (OPO) and distributed along the four nodes through 50 : 50 beam splitters (BS). The measurement of the phase quadrature p_i, along each node i, is performed by the homodine detection HD_i. Finally the average estimation is performed. Described in Ref. [524]. **c** Scheme of the Mach-Zehnder interferometer in polarization, realized to perform measurements of phase and visibility of different samples. The probes are two-photon N00N state in polarization. Described in Refs. [525, 526, 527]. This image is taken from [1].

which M independent and identical squeezed coherent probes are sent each along a single node, thus separately estimating the associated phases, and (ii) entangled estimation in which a single initial squeezed coherent state is equally divided along the M nodes by initial beam splitters, that generate mode entanglement in the probe state (Fig. 3.5b). The authors in Ref. [520] showed that, in the ideal case of unitary transmission, the optimal sensitivity for the entangled estimation shows a Heisenberg scaling $1/(MN)$ in both the number of modes M and mean number of photon N. This is obtained by optimizing over the initial probe state. Conversely, a separable estimation leads to a SQL scaling in M and Heisenberg scaling in N: $1/(\sqrt{M}N)$. The authors experimentally demonstrated this entangled advantage in a network of $M = 4$ nodes and a probe state generated by an optical parametric oscillator at wavelength 1550 nm. In particular, using optimal probes containing $N \approx 2.5$ photons per mode, the measured standard deviation of $\bar{\phi}$ estimated was found equal to $\sigma_{\text{ent}} = 0.099 \pm 0.003$ for the entangled estimation strategy, while being equal to $\sigma_{\text{sep}} = 0.118 \pm 0.002$ for the separable estimation one [520]. The optimality of the demonstrated setup for estimating the average phase has been proved in a general framework by Ref. [521].

A similar implementation of an entangled sensor network, based on Ref. [528], was experimentally realized in Ref. [529] through a reconfigurable radiofrequency photonic platform. The probe is a phase squeezed state that is prepared through tunable beam splitters that allow to generate a continuous variables multipartite

entangled state along three separated sensors. Tuning the beam splitters, different states can be produced in order to maximize the sensitivity for different tasks, such as phase gradient and mean amplitude estimations.

Finally, realistic scenarios involve the unavoidable presence of noisy channels. Here, multiparameter estimation of both phase and noise represents a valid solution. A possible approach can be performing an a-priori characterization of noise before the estimation process. However, in many cases time-varying systematical errors cannot be characterized in advance, such as phase oscillations due to thermal or mechanical fluctuation of optical systems [530, 531]. In these cases simultaneous estimation of phase and noise is necessary [532]. All these studies generally require calculation of multiparameter bounds in which noise is considered as a non-unitary evolution. An experimental implementation of simultaneous phase and dephasing estimation was demonstrated in Ref. [533]. In a different work[534], weak measurements were exploited to experimentally perform multiparameter estimation of a phase shift and its phase diffusion with classical probes. In Ref. [525] an optical phase shift ϕ and noise over the probe state, measured in terms of visibility v of the interference fringes, have been simultaneously estimated (Fig. 3.5c). Other photonic quantum sensors exploited in multiparameter scenarios that do not involve phase estimation are reported in [1].

3.1.4 Adaptive protocols for phase estimation

Different estimation protocols have been defined [358, 535], and can be included in a few fundamental categories. A first example is provided by parallel protocols (Fig. 3.2) in which all the probes, entangled or not, interact in parallel with the system [536, 478]. A second class is composed of sequential (or multiround) protocols [537, 538, 473] where single probes interacts multiple times with the system. Finally, ancilla-assisted schemes [472, 539, 540, 541, 542, 543] are those where a part of the probe, generally entangled with the other part, does not interact with the system and is directly measured. All these protocols can be *non-adaptive* [2] or *adaptive* [544, 491]. Here we focus on adaptive techniques, that represent a powerful tool to enhance the performances of estimation processes [544, 491, 545, 546, 547, 548, 473]. In non-adaptive estimation protocols, the available probes are sent through a fixed apparatus and, after collecting the full data set, a final estimate of the unknown parameter λ is obtained. Conversely, adaptive techniques make use of suitable controls on the experimental setup, namely some physical parameters $\boldsymbol{\theta}$, such as additional feedback phase shifts, that can be adjusted during the estimation. Adaptive and entangled protocols can enhance metrology tasks, especially in presence of noise [535, 549]. Adaptive protocols do not give advantages with respect to non adaptive schemes when the estimation involves quantum channels that are (jointly) covariant with teleportation, such as the Pauli or erasure channels. In this case, Ref. [550] showed that the optimal performance is limited to the SQL, by adapting techniques previously developed for Quantum Communication [551]. A discrete-time class of adaptive protocols can be schematically represented through the repetition, for each probe, of the four-step cycle as shown in Fig. 3.6.

(i) The first step is dedicated to the preparation of an initial probe ρ_{in}, through a

process $U_{\boldsymbol{\theta}}(\boldsymbol{x})$ that depends on certain parameters $\boldsymbol{\theta}$ and, if available, on the results $\boldsymbol{x}$ of previous measurements.

(ii) At a second stage, the prepared probe $\rho_0(\boldsymbol{\theta})$ interacts with the studied system and evolves under a unitary U_λ (for simplicity we are assuming unitary evolution) in $\rho_{\text{fin}}(\boldsymbol{\theta}, \lambda)$.

(iii) Then, a measurement Π_x is performed and its outcome x is recorded.

(iv) The final step of the cycle is post-processing of the measurement results. This step includes the choice of the parameters $\boldsymbol{\theta}$ determining the action $U_{\boldsymbol{\theta}}(\boldsymbol{x})$ to apply to the initial probe of the successive cycle.

This cycle is repeated for all the probes. Finally, an estimator $\Lambda(\boldsymbol{x})$ based on all measurement results $\boldsymbol{x}$ provides an estimation of the unknown parameter λ.

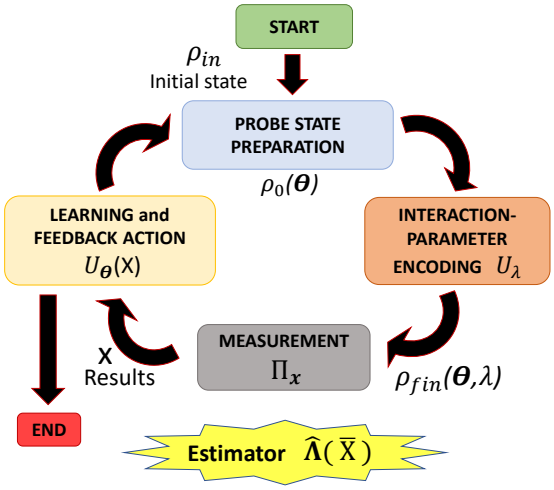

Figure 3.6. Conceptual scheme of an adaptive estimation protocol. The cycle of a general adaptive estimation protocol starts from an initial state ρ_{in}, that is prepared (blue box) in a state $\rho_0(\theta)$ through the action of U_θ. Such state interacts with the unknown parameter λ (brown box), and then the output state $\rho_{\text{fin}}(\theta, \lambda)$ undergoes an appropriately chosen measurement Π_x (gray box). After such measurement, the results X are exploited to define a suitable action $U_\theta(X)$ (orange box), employed to prepare the initial state of the next probe. In this way, the cycle is repeated for all the probes. At the end of the process, an estimator provides the final estimate of θ. This image is taken from [1].

Exploiting adaptive protocols for Quantum Metrology was proposed in 1995 by Wiseman [544]. Such protocols are necessary in order to overcome different issues. For instance, they can be used for the realization of the optimal POVM to saturate the QCRB. In certain scenarios, such POVMs can be hard or impossible to implement. In this case, approximation of such measurements can be achieved by adaptive techniques [546, 455]. In particular, to approach the QCRB one has to maximize the Fisher Information of a given setup. However, the latter quantity depends in general on the unknown parameter. More specifically, given an initial probe, the QCRB is attainable only when the unknown parameter takes a value which maximizes the Fisher Information. Nevertheless, it can be demonstrated

that, even with no prior knowledge on the unknown parameter, the QCRB can be asymptotically saturated by exploiting adaptive techniques [483].

A second scenario where an adaptive approach represents a useful resource is found for those systems where the output probabilities, calculated at different values of unknown parameter, take the same value. For instance, if we consider $\lambda = \phi$ the internal phase of a Mach-Zehnder interferometer seeded by single photons, the output probability ($P_1 = 1 - P_0 = \cos^2 \frac{\phi}{2}$) is such that, in the range $\phi \in [0, 2\pi]$, two different values of the phases lead to the same probability $P_1 \neq 0$. Indeed, the latter is not an injective function of the phase. Hence, without changing the relative phase shift during the experiment, it is impossible to discern the two equivalent phases leading to the same probability. Conversely, by changing the total phase shift during the estimation process, for instance through another known control phase, it is possible to solve such issue. In any case, when the output probabilities are periodic with a period less then 2π, it is impossible to distinguish some phases. In such cases, one could employ an adaptive protocol where the probe state can change at each iteration, thus changing the likelihood function and its periodicity. For instance, during the first steps one can employ probes whose likelihood has no periodicity, in order to restrict the range of possible unknown phase values. When the range is sufficiently small, more sensible states with smaller periodicity can be used [552]. However, the validity of such recipe depends on the problem symmetries.

Furthermore, an important task where adaptive protocols can be helpful is the convergence to the ultimate precision bounds in the limited data scenario [454, 553]. The latter regime characterizes different realistic conditions where the amount of resources that can be employed is restricted. In the single-parameter case, theorems guarantee that it is always possible to define suitable measurements and estimators, allowing to reach the minimum error achievable with a given probe state (Sec. 3.1.2). However, this capability of reaching the ultimate bounds is guaranteed only in the asymptotic regime. Conversely, when only a limited number of probes is available, identifying the optimal strategies is a difficult task. To this end, one can employ adaptive protocols, leading to a boost in the convergence to the asymptotic limits.

Finally, adaptive protocols have to be taken into account to achieve the true quantum limits [554]. Importantly, feedback and error-correction schemes can be exploited to face noises and/or time-varying parameters [555, 556, 557, 558, 559, 560, 561, 562, 563, 549, 564, 565, 566, 567, 568].

There exist two prominent approaches to feedback-based phase estimation:

- *Online schemes:* At each step of the estimation protocol, the feedback is calculated according to the previous measurement result and a heuristic. An important class of these schemes is represented by Bayesian adaptive protocols (Sec. 3.1.4.1). Here, at each step of the protocol, the posterior probability evolves based on measurement results. In this way, the posterior is used to calculate the optimal feedback action to be applied at next step. Note that optimality is defined depending on the particular problem and heuristic.

- *Offline schemes:* The feedback values used during the experiments are computed before the estimation process. The goal is then the optimization of such sequence of feedback values. Different optimization techniques based on trial and error approaches can be exploited, such as those based on Particle Swarm Optimization (PSO) [569, 570] and Differential Evolution (DE) [571, 572, 573].

Finally, adaptive protocols can be also exploited to enhance state discrimination and more general in quantum tomography [574, 575, 576, 577]. This has been

experimentally demonstrated in the estimation of the photons polarization [578, 579, 580, 581, 582].

3.1.4.1 Adaptive Bayesian protocols

Bayesian estimation (Sec. 3.1.2.2) naturally fits the requirements for adaptive protocols. In this framework, the posterior distribution is updated at each repetition of the estimation cycle [Eq. (3.23)]. The information encoded in this distribution can be exploited to choose the optimal feedback action according to the protocol heuristic.

One of the first adaptive phase estimation, providing an experimental demonstration of the proposal in Ref. [544], was realized exploiting adaptive homodyne phase measurements on coherent states [583]. Coherent states with homodyne measurements were also employed for adaptive estimation of a continuously varying phase, beating the non adaptive filtering limit [584]. HL scaling, in this kind of schemes, cannot be achieved by employing coherent states as probes. However, an enhancement of a constant factor with respect to SQL can be obtained. Also coherent states discrimination can be performed through adaptive schemes [585].

When employing quantum states, one can reach improved scaling in the estimation process. In this regime, when the phase to be estimated is completely unknown (flat prior distribution) adaptive techniques can be employed [491, 586]. This is the goal of an *ab-initio* quantum phase estimation experiment that was experimentally realized by Ref. [587]. In such realization, a sequence of different states is used and detected by a probabilistic photon-number resolving detection. The employed Bayesian protocol is composed of a first step with random feedback. Subsequently, after the measurement of a group of single-photon events, the posterior probability is updated and the next feedback is calculated by optimizing the expected sharpness function [Eq. (3.27)] over the possible results of the next measurements. Using suitable sequences of states (with photon numbers $N = 1, 2, 4$), the SQL was surpassed [587].

The SQL can be overcome by employing other classes of states, such as Gaussian squeezed states with squeezing parameter r that reach a value for the variance [588, 589] equal to $V = 1/[2N \sinh(2r)]$. Since for this resource state the optimal Fisher Information depends on the unknown phase, an adaptive protocol has to be employed, and Bayesian estimation can be exploited for this purpose. Given this class of input states, a Bayesian protocol for *ab-initio* phase estimation has been experimentally realized using squeezed states and homodyne detection, together with real-time feedback [590]. The phase of a squeezed state is measured with respect to a local oscillator through homodyne detection. More specifically, a first set of data is exploited to perform a rough estimation of the phase. Then, the local oscillator phase is adjusted to the value that lead to the minimum error in the estimation process [590]. Finally, also two mode squeezed states can be exploited in adaptive protocols [591].

Bayesian adaptive estimation can be used to reach the HL with single photons in multipass configuration without the need of entanglement as demonstrated in Ref. [473]. In this case, single photons are employed for a multipass polarization interferometer estimating phases through a generalized Kitaev's algorithm [592]. An adaptive hybrid approach, exploiting simultaneously polarization entangled 2-photon states and a multipass configuration (with $N = 3$ passes per state, two for one photon and one for the other), achieved within 4% the exact value of HL at finite number of resources [593]. This implementation demonstrated the theoretical proposal of Ref. [546]. The optimal state for this protocol is [546, 593]: $|\psi_{\text{opt}}\rangle = c_0 |\Phi^+\rangle + c_1 |\Psi^+\rangle$, with $|\Phi^+\rangle = (|0,0\rangle + |1,1\rangle)/\sqrt{2}$, $|\Psi^+\rangle = (|1,0\rangle + |0,1\rangle)/\sqrt{2}$ and

$c_j = \sin[(j+1)\pi/5]/\sqrt{\sum_{k=0}^{1}\sin[(k+1)\pi/5]^2}$ and was realized through a probabilistic control-Z gate [594] between two SPDC photons.

An efficient and robust adaptive Bayesian phase estimation protocol, called rejection filtering [595], was realized exploiting the evolution of pairs of photons in a silicon circuit. The latter implemented adaptive unitaries that depend on single events, extracted from collections of photon statistics [596].

An adaptive estimation experiment based on single-photon inputs was realized in a bulk Mach-Zehnder interferometer in the path degree of freedom, implementing two different Bayesian techniques [597]: (i) particle guess heuristic, in which at each step the feedback phase is randomly drawn from the posterior distribution [595] and (ii) an optimal heuristic, which is derived analytically by optimizing the Bayesian mean square error of the future events over the feedback, under the assumption of narrow Gaussian prior [597]. In particular, the last optimized technique shows better performances than the PSO (discussed in details below) and the particle guess heuristics. Furthermore, such optimized technique has been experimentally demonstrated to be robust against different classes of noise.

3.1.4.2 Machine Learning offline estimation techniques

Offline machine learning techniques can be exploited to enhance quantum phase estimations. Machine learning techniques [598, 599] applied to physical problems represent a new, rich and continuously growing research area in which learning tools are used to enhance quantum information tasks [1]. Such techniques can be also used to calibrate quantum sensors [600]. Remarkably, machine learning-based protocols have been developed also for adaptive Quantum Metrology [569, 570, 595, 596, 597, 572, 573, 571, 601, 602] and entanglement-assisted supervised learning in an entangled sensor networks can be exploited for sensing tasks [603].

Two significant machine learning techniques employed for Quantum Metrology with an offline approach are PSO [569, 570] and DE [572, 573]. Such techniques are able to self-learn the optimal feedback strategy to reach the ultimate limits on the scaling of the phase estimation uncertainty, with limited number of measurements. They are both based on reinforcement learning that is model-free, since it does not necessarily rely on the explicit model of the problem, but mainly on experience acquired from data. Even if a mathematical model is available, reinforcement learning techniques can surpass gradient-based greedy algorithms for non-convex optimizations in high-dimensional problems. In particular, PSO and DE are evolutionary algorithms [604, 605]. Such algorithms often resemble biological evolution mechanisms and are characterized by the following features: the presence of a population of points in the search space, the existence of a figure of merit called *fitness* to be maximized and, finally, stochastic evolution of the solutions. One of the biggest advantage of evolutionary computation is the low probability of getting stuck at local optima of the function, since the space is explored by many candidate solutions and the optimization of the searching process happens in a quasi-random way.

For phase estimation tasks, such approaches are applied to calculate, prior to the experiment, the sequence of optimal feedback phases shifts to be used during the adaptive experiments with N probes. Considering a Mach-Zehnder interferometer, at each step k of the experiment, the optimal feedback phase Φ_k can be updated according to the following Markovian rule with a logarithmic-search heuristic:

$$\Phi_k = \Phi_{k-1} - (-1)^{x_{k-1}}\Delta\Phi_k, \tag{3.40}$$

where Φ_{k-1} is the feedback phase at previous step, and $x_{k-1} \in \{0,1\}$ is the result of the measurement at step $k-1$. The list of optimal phase shifts $\{\Delta\Phi_k\}$ for

$k = 1, \dots N$ is called *policy*. The final estimate for the unknown phase ϕ coincides with the last value Φ_N of the adaptive feedback phase at the end of the process according to $\Phi_{\text{est}} = \Phi_N$.

PSO is part of a class of unsupervised reinforcement learning algorithms for optimization problems [606, 607], and can be exploited to compute the list of phase shifts $\{\Delta\Phi_k\}$ discussed above. The goodness of a policy is quantified by the sharpness of Eq. (3.27) relative to the estimation errors. Hence, the average of the sharpness is calculated over $P(\theta|\rho)$, that is the probability distribution of the error θ on the estimate given a policy ρ. In this way, the sharpness in Eq. (3.27) is the objective function that is maximized by PSO over the policies, and is related to the Holevo variance. When the sharpness is maximized, the Holevo variance is minimized. Given the number N of employed photons in the estimation process, the goal of the PSO algorithm is to find the optimal policy by maximizing the associated sharpness. At each iterative step of the algorithm, every policy is mapped to a vector and compares its fitness with those relative to its neighborhood and to its past history. Then, the policies are updated according to a stochastic evolution rule depending on global and local optima. After a certain number of iterations, the last global optimum represents the solution of PSO. In Ref. [597], an adaptive scheme using PSO policies was realized using single photons in a path Mach-Zehnder interferometer, and SQL was approached after few photons (~ 20).

However, it has been observed that PSO algorithm converges to optimal solutions only when the number of probes is small, and this limitation can be overcome by other techniques like Differential Evolution [571, 572]. DE is an evolutionary algorithm that performs a global optimization in the policies space by selecting and rejecting candidate policies according to their sharpness value. In particular, after a random initialization of candidate policies, at each iteration of the algorithm new polices are generated by combining randomly chosen policies. The policies with highest fitness values are then selected for the next step. This procedure is iterated until a halting condition for the fitness of the best policy is reached. These techniques are also resilient to different models of noise [573].

3.2 Experimental estimation of multiple phases inside a multiarm interferometer

The simultaneous estimation of more parameters inside a physical system represents the natural generalization of the single parameter problem (Sec. 3.1). While the single parameter case has a well-established theoretical framework [359], with more parameters there are still open questions. This is the case for example of non-commutative quantum measurements, in which the general strategies to achieve the ultimate bound are not defined [478, 447, 479, 481, 482]. This is due to the impossibility in some cases to simultaneously optimize these measurements over all parameters [483]. On the other hand, in presence of d-compatible parameters, the multiparameter scenario shows advantages of a factor d with respect to the separate estimation of the single parameters in terms of variance [484]. Further, in many problems, different parameters can not be treated separately and their simultaneous estimation becomes necessary. For all these reasons, the multiparameter Quantum Metrology finds lots of applications [427], such as phase imaging [608] and measurements on biological systems [609], quantum process tomography [610], gravitational waves parameters estimation [360] and more general quantum sensing [486]. Here, both the theoretical and the experimental investigations represent necessary steps to improve the research [1], but the number of experimental demonstrations is surprisingly few (Sec. 3.1.3.1). This is the case of simultaneous estimation of optical phase and its diffusion noise [532, 533, 534], phase and probe visibility [611], parameters in a quantum tomography process [610], quadratures [612] and finally the indirect inference of a single physical quantity depending by the simultaneous measure of multiple phases [520]. Conversely, several theoretical works have been reported in this direction. Remarkably, single-phase estimation is a fundamental problem in Quantum Metrology, as well as the estimation of multiple phases. Indeed, as shown in Sec. 3.3.1 these scenarios allow not only the mapping of several physical systems, but also represent crucial tools for testing the corresponding Quantum Metrology frameworks. Several theoretical works have been reported multiphase estimation scenario [517, 518, 460, 486, 485, 613, 361, 514, 516], while no experimental realizations have been reported yet.

Thus, the main investigation of our Metrology research exploited an integrated multiarm interferometer injected by multiphoton states, representing the most suitable platform for the simultaneous estimation of multiple phases [518]. This platform presents several advantages in terms of stability, tunability, and compactness [614, 28]. The first fundamental point for Metrology purposes concerns the correct calibration of the device [14, 16], allowing the correct identification of the effective achievable performances. Then, using the interferometer, a quantum-enhanced two-phase estimation in a non-adaptive regime [14] was experimentally realized for the first time.

3.2.1 Multiphase estimation on chip

Calibration of the device

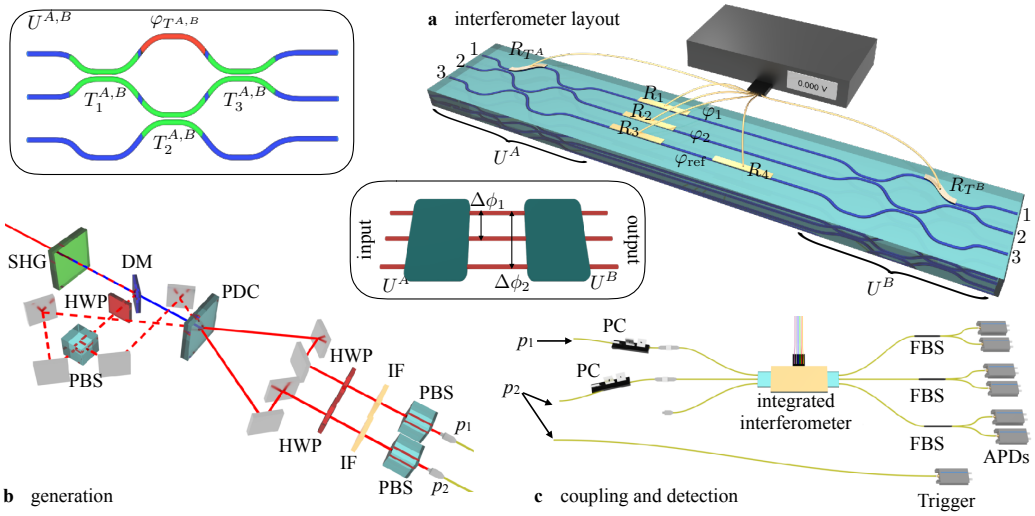

Figure 3.7. Experimental apparatus. **a**, Layout of the integrated reconfigurable device. Three straight waveguide segments are included between two multiport splitters U_A and U_B. The dynamical control of the phases is achieved by thermo-optic phase shifters. Central inset: conceptual scheme of the interferometer. Top left inset: layout of the multiport splitters $U^{A,B}$, each composed of three directional couplers ($T^{A,B}_{1,2,3}$, green regions) and a dynamically reconfigurable phase ($\varphi_{T^{A,B}}$, red). By appropriately tuning $\varphi_{T^{A,B}}$ the two multiport splitters can be set to operate as balanced tritters. **b**, Parametric down-conversion source for generation of single-photon and two-photon states. The dotted path is employed to inject classical light into the device for the device alignment. The generated photons (p_1 and p_2) are coupled in single-mode fibers and sent to the integrated device. **c**, Coupling and detection stage. Photons are coupled to the device by an input fiber array (single-mode operation), and collected with a second fiber array (multimode operation). For single-photon inputs, photon (p_2) is directly measured to act as a trigger. For two-photon inputs, both photons are injected in the interferometer, and the output state is measured by adding a set of fiber beam-splitters to detect bunching events. Legend - PDC: parametric down-conversion, SHG: second harmonic generation, DM: dichroic mirror, HWP: half wave plate, PBS: polarizing beam-splitter, IF: interference filter, PC: polarization controller, FBS: fiber beam-splitter, APD: avalanche photodiode. This image is taken from [14].

The employed device is a three arm interferometer working at 785 nm, fabricated by FLW (see Fig. 3.7a). The chip has a highly degree of reconfigurability, given by six thermo-optics phase shifters. These are resistors placed near the integrated waveguides, generating phase shift along them when dissipating power (Sec. 1.1.3.1). The structure of the interferometer is composed by two external tritter operators (U^A, U^B) interposed by phase shifters along three internal arms. A fine tuning of each tritter is possible by changing an optical phase, respectively ϕ_A and ϕ_B. In particular, $U^A\,(U^B)$ realizes a balance tritter when $|\phi_A| = \pi/2\,(|\phi_B| = \pi/2)$, thus engineering a reconfigurable 3-mode Mach Zehnder. The mathematical description of a tritter in a two-dimensional decomposition, in the lossless case, is given by a unitary matrix U^A defined by its decomposition into cascaded two-mode beam splitters and a phase shifter [615], as shown in Fig. 3.7. The first directional coupler

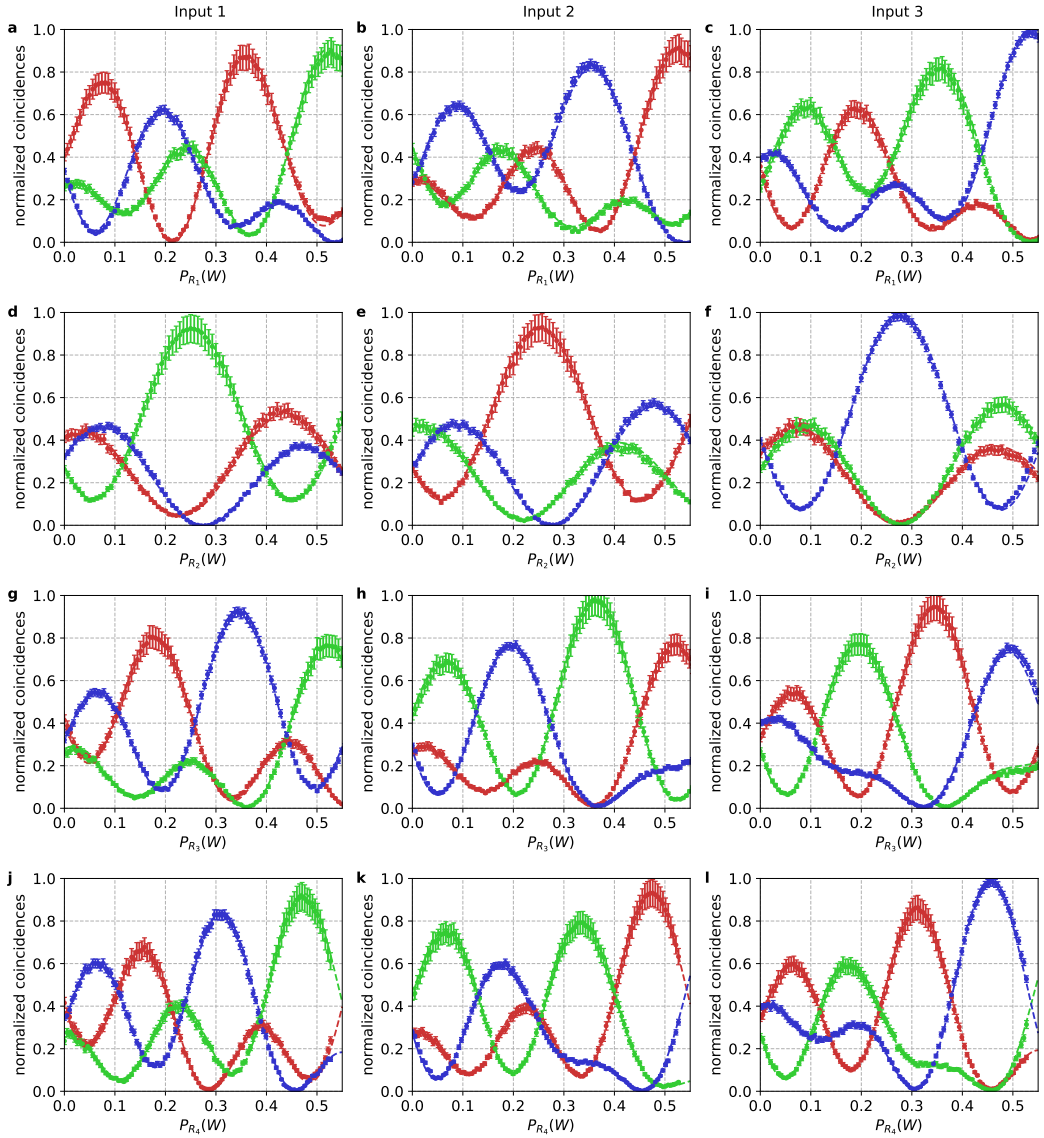

Figure 3.8. Measured input-output probabilities (points) and relative fitted curves (dashed lines) as a function of the dissipated power by resistor R_1 (**a-c**), R_2 (**d-f**), R_3 (**g-i**) and R_4 (**j-l**), where each resistor has been tuned separately. **a,d,g,j**: Input 1. **b,e,h,k**: Input 2. **c,f,i,l**: Input 3. For each plot, output 1 corresponds to red points and lines, output 2 to green ones, and output 3 to blue ones. Those data are fitted to retrieve the values of the device parameters. This image is taken from [14].

mixes the first two modes of the interferometer. Assuming a lossless evolution, the reflectivity and transmission coefficients of the coupler R_1^A and T_1^A are related according to $R_1^A + T_1^A = 1$. Hence, the directional coupler is described by the unitary matrix $U_{T_1}^A$:

$$U_{T_1}^A = \begin{pmatrix} \sqrt{1-T_1^A} & i\sqrt{T_1^A} & 0 \\ i\sqrt{T_1^A} & \sqrt{1-T_1^A} & 0 \\ 0 & 0 & 1 \end{pmatrix} . \tag{3.41}$$

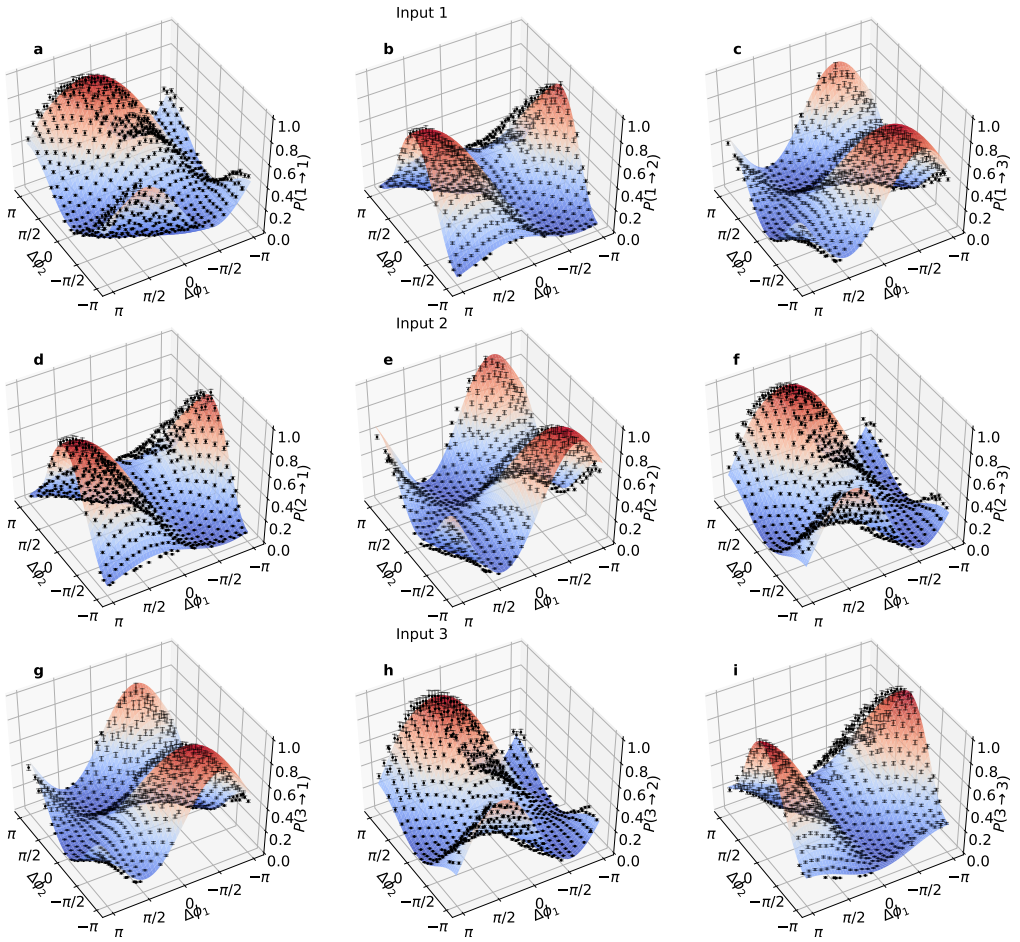

Figure 3.9. Measured single-photon input-output probabilities $P(i \to j)$ as a function of phase differences $\Delta\phi_1$ and $\delta\phi_2$, tuned by simultaneously varying the dissipated power in resistors R_1 and R_2. Points: experimental data. Surfaces: curves obtained from the characterized parameters and from the employed model. **a-c**, Input 1, **d-f**, input 2 and **g-i**, input 3. For each input, the three plots correspond to the three different output modes. This image is taken from [14].

The second directional coupler mixes the second and the third modes and is described by the unitary matrix:

$$U_{T_2}^A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{1-T_2^A} & i\sqrt{T_2^A} \\ 0 & i\sqrt{T_2^A} & \sqrt{1-T_2^A} \end{pmatrix}, \tag{3.42}$$

where T_2^A is the transmission coefficient of the second directional coupler. To obtain the tritter transformation, an additional phase shifter $PS_{\varphi_{T^A}}$ that introduces a phase φ_{T^A} between the first arm and the other two is required. Such transformation is described by the following matrix:

$$PS_{\varphi_{T^A}} = \begin{pmatrix} e^{i\varphi_{T^A}} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{3.43}$$

Finally the first two modes interfere again in a third directional coupler $U^A_{T_3}$, whose action is described by the same matrix of Eq. (3.41) (with T^A_3 as the transmission coefficient). The first tritter is then described by a unitary matrix obtained as an appropriate product of the previously defined transformations:

$$U^A = U^A_{T_3} \cdot PS_{\varphi_{T^A}} \cdot U^A_{T_2} \cdot U^A_{T_1} \,. \tag{3.44}$$

The values of the transmission coefficients and the phase shift to obtain a symmetric tritter described by $U^{(3)}$ are: $T^A_1 = T^A_3 = 1/2$, $T^A_2 = 2/3$ and $|\varphi_{T^A}| = \pi/2$.

After the first transformation, the three phases embedded within the three internal arms of the interferometer (Fig. 3.7) are described by the matrices:

$$\begin{aligned} PS_1(\varphi_1) &= \begin{pmatrix} e^{i\varphi_1} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \\ PS_2(\varphi_2) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{i\varphi_2} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \\ PS_3(\varphi_{\text{ref}}) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & e^{i\varphi_{\text{ref}}} \end{pmatrix}, \end{aligned} \tag{3.45}$$

where the latter term is chosen as the reference phase. The final transformation U^B has the same form of U^A, Eq. (3.44), with transmission coefficients T^B_1, T^B_2, T^B_3 and internal phase φ_{T^B}. The overall matrix U^{int} of the interferometer is:

$$U^{\text{int}} = U^B \cdot PS_3(\varphi_{\text{ref}}) \cdot PS_2(\varphi_2) \cdot PS_1(\varphi_1) \cdot U^A \,. \tag{3.46}$$

Therefore, the device is described by several parameters: the transmission coefficients of the tritters directional couplers $T^{A,B}_{1,2,3}$, phases $\varphi_{T^{A,B}}$ embedded in $U^{A,B}$, and the three internal phases φ_1, φ_2 and φ_{ref} of the interferometer. The output probabilities for single- or multi-photon states entering in the device can be thus calculated by using the evolution in Eq. (3.46).

In order to exploit the device and control its reconfigurability, a correct and complete characterization of these parameters is of paramount importance. The calibration of a quantum sensor represents a fundamental step as well as its implementation [16]. This step requires reconstructing all relevant static and dynamical parameters. The former, described above, are given by beam-splitter transmittivities and internal phases when no voltage is applied. The latter represent the coefficients of dynamical response of the device. Considering P_{R_i} as the power dissipated by resistor R_i, the dynamic description of the multiple action of different resistors can be computed as:

$$\Delta\phi_j = \sum_{i=1}^{6} \left(\alpha_{ji} P_{R_i} + \alpha^{\text{NL}}_{ji} P^2_{R_i} \right), \tag{3.47}$$

where $\Delta\phi_j$ $(j = 1, 2)$ represent the two optical independent phase shifts generated by dissipated powers, namely $\Delta\phi_1 = \varphi_1 - \varphi_{\text{ref}}$ and $\Delta\phi_2 = \varphi_2 - \varphi_{\text{ref}}$. The coefficients α_{ij} and α^{NL}_{ij} are respectively, the linear and nonlinear response coefficients associated to the dissipation P_{R_i}. The linear terms depend on all the geometric, thermal, and optical properties of the device [614], while non-linear terms are associated with variations in the resistance value due to temperature increase. The experimental

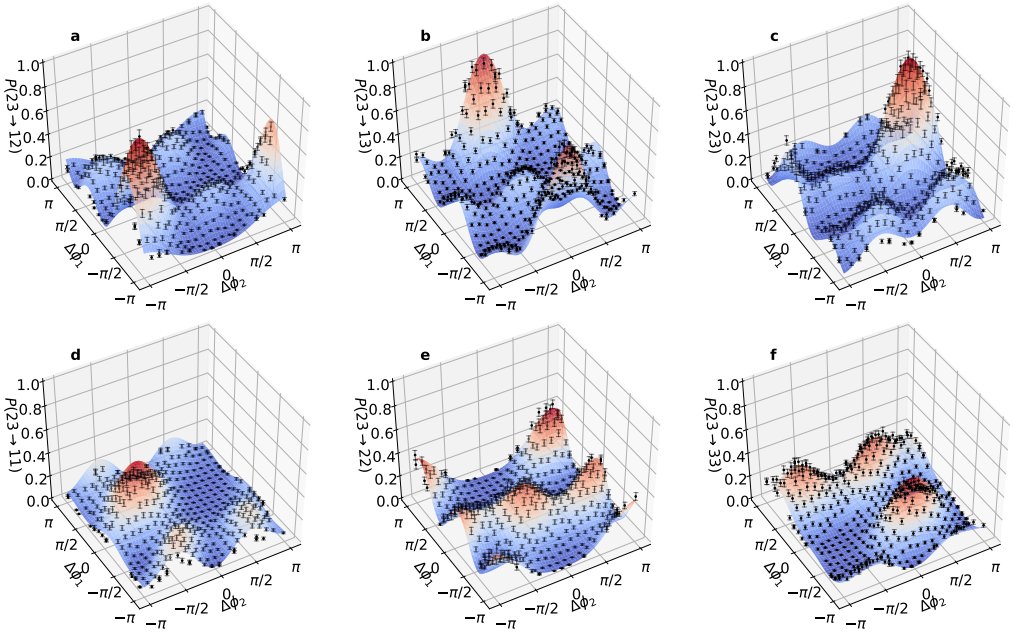

Figure 3.10. a-f, Two-photon probabilities $P(23 \to ij)$ as a function of the phase differences $\Delta\phi_1$ and $\Delta\phi_2$. The latter are varied by changing the dissipated powers on resistors R_1 and R_2. In all plots, dots are experimental data while surfaces are the theoretical expectations from the circuit characterization process. Error bars are standard deviations due to the Poissonian statistics of the measured single-photon counts and two-photon coincidences. This image is taken from [14].

apparatus used to characterize the chip is shown in Fig. 3.7b-c. Pairs of single photons at 785 nm are generated with SPDC process, by pumping a type-II BBO nonlinear crystal with a 392.5 nm-impulsed laser beam. One photon of the pair is injected into the device while the other is used as an external trigger for revealing the first one. Coincidence between these photons are measured by four avalanche photodiode detectors (APDs), placed at the outputs of the chip and along the external trigger channel. This allowed us to measure the input-output probabilities $P(i \to j)$ from input i to output j. To fully characterize the response of the device we measured the detected output coincidences in each input configuration as a function of the power dissipated by the single resistor. Each resistor is studied independently, by keeping the other resistors off. Calibration results are shown in Fig. 3.8. The high quality of operation of the device is confirmed by the average fidelity of the device with respect to the ideal set of achievable transformations. Indeed, the fidelity $\langle F \rangle_{\Delta\phi_1,\Delta\phi_2}$, averaged over the interferometer phase differences $(\Delta\Phi_1, \Delta\Phi_2)$, reaches a value $\langle F \rangle_{\Delta\phi_1,\Delta\phi_2} = 0.963 \pm 0.015$. Here the fidelity is defined as $F = |\mathrm{Tr}[\tilde{U}(\Delta\phi_1, \Delta\phi_2)U^\dagger(\Delta\phi_1, \Delta\phi_2)]|/m$, while $U(\Delta\phi_1, \Delta\phi_2)$ and $\tilde{U}(\Delta\phi_1, \Delta\phi_2)$ are respectively the ideal and reconstructed transformation for phases $(\Delta\Phi_1, \Delta\Phi_2)$. By exploiting the results of the characterization process, it is possible to control arbitrary phase differences between the interferometer arms by applying a suitable voltage on resistors R_i.

After performing the characterization process, in order to confirm the goodness of the obtained parameters, we test the device and the quality of our reconstruction. As a first step, we analyzed the results when multiple resistors are simultaneously active, by setting transformations U^A and U^B as balanced tritters. Comparison

between theoretical prediction with experimental data dissipating power over two resistors, are reported in Figs. 3.9 and 3.10. This study is made both in single- and two-photon regime. In particular, two photon input states are produced by injecting both the two photons of the generated pair by SPDC process into the device (without external trigger), still recording output coincidences between them. Notably, two-photon predictions are studied changing the degree of distinguishability of the photons pair (Fig. 3.11). This is varied by tuning their relative time delay $\delta\tau$ through adjustable delay lines. All the experimental results show very good agreement with the expected ones, thus demonstrating the good quality of our characterization process. This demonstrates the capability to control the device transformation by simultaneously operating on multiple thermo-optic phase shifters, also preserving quantum coherence during the evolution. Furthermore, the reported data in the two photon regime show a clear signature of quantum interference when tuning the regime from indistinguishable to distinguishable particles.

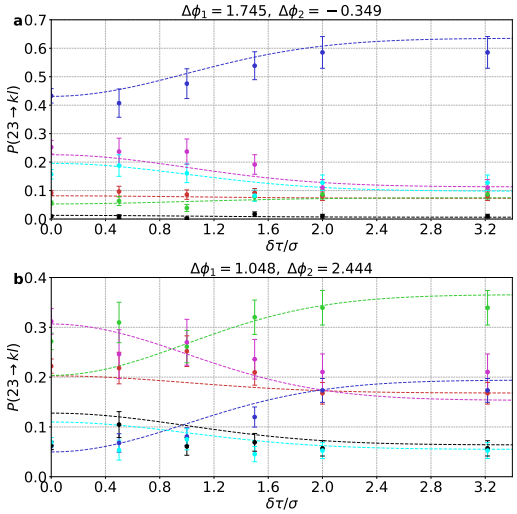

Figure 3.11. Two-photon measurements $P(23 \to kl)$ for an input state with a single photon on modes (2,3) as a function of the relative time delay $\delta\tau$, normalized over the photon Hong-Ou-Mandel width σ. **a**, Phase values set at $\Delta\Phi_1 = 1.745$ and $\Delta\Phi_2 = -0.349$. **b**, Phase values set at $\Delta\Phi_1 = 1.048$ and $\Delta\Phi_2 = 2.444$. Points are experimental data, while dashed lines are predictions from the reconstructed parameters. [Red: output (1,2), Green: output (1,3), Blue: output (2,3), Black: output (1,1), Cyan: output (2,2), Purple: output (3,3)]. Photon indistinguishability is introduced in the predictions by mixing the probability with indistinguishable and distinguishable photons with a parameter $e^{-(\delta\tau/\sigma)^2}$. Error bars are standard deviations due to the Poissonian statistics of the measured two-photon coincidences. This image is taken from [14].

Experimental multiphase estimation

The results of the characterization process allow us to calculate the estimation performances of the device. As shown in Sec. 3.1.2, the best achievable precision over the two-phase estimation, quantified by its covariance matrix, can be computed evaluating the Fisher Information Matrix of the system. Here, we consider two-photon inputs and balanced tritters as U_A and U_B. The total error in terms of overall variance is bounded by the trace [Eq. (3.12)] and the optimal precision is

achieved when the equality is reached. The comparison between the ideal three-mode balanced interferometer and the resulting one from the fitting parameters is reported in Fig. 3.12. The results show for all input states the presence of special regions in the phases space, i.e. the ones within the white circles, where the device performs quantum enhancement. Indeed, in these regions the corresponding QCRB by injecting classical probes, i.e. distinguishable photons, is higher than the CRB relative to indistinguishable photons [613, 485, 518]. While regions corresponding to quantum-enhanced performances are less extended than the ideal device, the minimum of $\mathrm{Tr}(\mathcal{I}^{-1})$ achieved by the implemented interferometer is close to the ideal value. Nevertheless, by exploiting adaptive protocols such performances can be extended in the full phases interval if only a single region performs better than classical resources.

Then, we verified the actual performances by implementing a simultaneous two-phase estimation experiment, by injecting pair of indistinguishable photons into input (2,3) of the device. In order to demonstrate quantum enhancement we fix the device in $(\Delta\phi_1, \Delta\phi_2) = (-1.159, 2.810)$, i.e. within one of the white circles. Then, we adopted a maximum likelihood estimator in a local framework to efficiently estimate the phases, from which we expect asymptotic saturation of the CRB. Results are reported in Fig. 3.13. We observe that the overall error on both parameters, quantified by $\sum_i \mathrm{Var}(\Delta\phi_i)$, drops below the bound with the optimal separable inputs. More specifically, the achieved performance overcomes the scenario in which the phases are estimated simultaneously or separately with classical inputs having the same overall number of photons [485]. Furthermore, the estimation of both parameters is achieved with comparable errors, thus leading to a symmetric estimation of the two phases.

Quantum-enhanced performance can be extended to the full phase interval by considering the application of adaptive estimation protocols [15, 597, 518, 596, 394]. This can be achieved with our device by exploiting the additional resistors R_3 and R_4 present in the circuit. The capability of performing adaptive protocols is particularly crucial in this multiparameter scenario, where the achievement of optimal [447, 479] or symmetric [518] errors in all parameters are not always achievable.

Tuning input and output transformations

In order to realize a quantum sensor able to measure reaching the ultimate precision limits, the optimization of each step of the estimation process becomes fundamental. Such sensor requires the capability to tune both preparation and measurement stage, in order to saturate the corresponding QCRB and maximizing its Quantum Fisher Information. Our device represents an important technological step in this direction, thanks to its high degree of reconfigurability, allowing us to implement different interferometers by tuning U^A and U^B. In a multiparameter scenario, the optimization of some estimation problems is possible when the measurement operator and the preparation one satisfy $U^B U^A = I$. This is the case of [482], which provides conditions for projective measurements to saturate QCRB, showing that such measurements include the projection over the initial state. Therefore, we test the ability of our integrated interferometer to realize such transformation. In particular we exploited the tunable phase of the tritter operators together with two additional resistors, i.e. R_3 and R_4. The adopted layout is shown in Fig. 3.14a. The additional phases on R_3 and R_4 are employed to configure the device such that $U^B U^A = I$ (up to a set of output phases). In this way, when $(\Delta\phi_1, \Delta\phi_2) = (0, 0)$ the interferometer realizes the identity. The results are shown in Fig. 3.14b-c. More

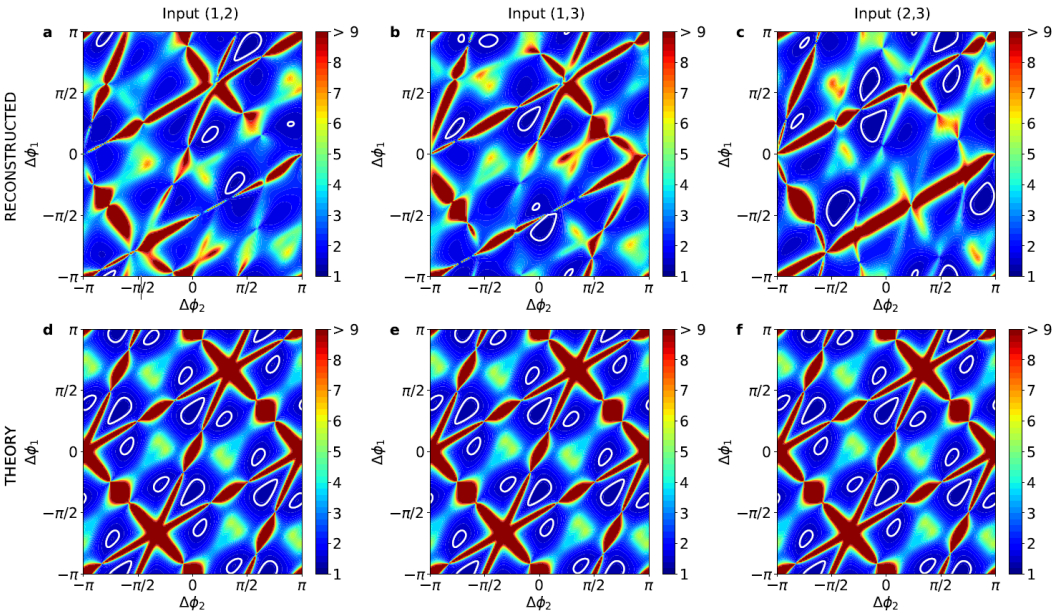

Figure 3.12. Cramer-Rao bound $\mathrm{Tr}(\mathcal{I}^{-1})$ for multiphase estimation with two-photon input states. **a-c**, CRB for the implemented device evaluated from the reconstructed parameters. **a**, Input (1,2), **b**, Input (1,3) and **c**, Input (2,3). **d-f**, CRB for the ideal three-mode interferometer. **d**, Input (1,2), **e**, Input (1,3) and **f**, Input (2,3). In the ideal interferometer case, points where the Fisher information matrix is singular are not shown. Regions included within white closed curves highlight the presence of quantum-enhanced performances with respect to the QCRB with two distinguishable single-photon inputs. This image is taken from [14].

specifically, we observe that the single-photon input-output probabilities $P(i \to j)$ closely resembles the identity matrix (see Fig. 3.14b) at $(\Delta\phi_1, \Delta\phi_2) = (0, 0)$, with a similarity $S = \frac{1}{3}\sum_{i=1}^{3} P(i \to i) = 0.979 \pm 0.008$. Similar results are observed for two-photon inputs (see Fig. 3.14c), thus showing the capability of tuning the input and output transformations by exploiting the additional phases embedded in the interferometer. The resulting transformations U^A and U^B and the characterization of their resistors are reported in Supplementary Information of [14].

Conclusions and perspectives

The experimental multiparameter estimation still requires a deep investigation, in order to realize a quantum sensor which shows real quantum enhancement [1]. The presented three mode MZI represents a building block in this direction. The integrated structure realized via the femtosecond micromachining technology allows stability and scalability, unreachable with bulk optics. The large number of tunable elements, i.e. thermo-optics phase-shifters, paves the way to the reconfigurability necessary to optimize each step of the estimation process and achieving ultimate measurement bounds. Our platform can be used to develop new methodologies and to benchmark their performances. In particular, using this photonic device we demonstrated experimentally the capability of performing quantum-enhanced estimation of two optical phases. The simultaneous estimation using as quantum probes pairs of indistinguishable photons, has revealed performances better than

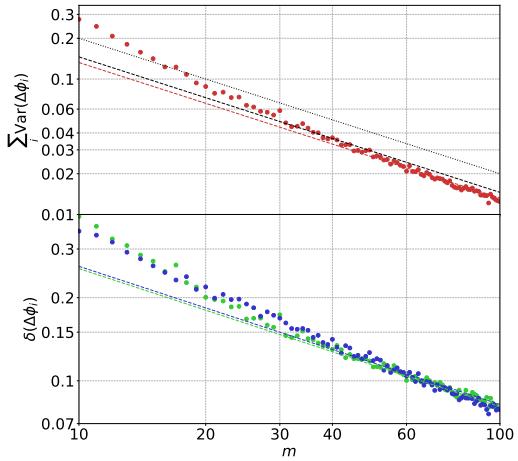

Figure 3.13. Results of a maximum likelihood estimator for local phase estimation at $(\Delta\phi_1, \Delta\phi_2) = (-1.159, 2.810)$ with input (2,3). Points: experimental data, obtained by averaging over 100 random sequences of m events drawn from the measured $N_{\mathrm{ev}} = 1230$ two-photon events. Top plot: red dashed line corresponds to $\mathrm{Tr}(\mathcal{I}^{-1})$, black dashed line to the optimal sensitivity $\mathrm{Tr}(\mathcal{H}^{-1})$ with $2m$ distinguishable single-photon inputs, black dotted line to the optimal sensitivity when the phases are estimated separately with classical inputs. Bottom plot: green points (data) and line $(\mathcal{I}^{-1})^{1/2}_{11}$ correspond to $\delta(\Delta\phi_1)$, blue points (data) and line $(\mathcal{I}^{-1})^{1/2}_{22}$ correspond to $\delta(\Delta\phi_2)$. This image is taken from [14].

any other classical strategies, in which the adopted probes were separable states. Quantum-enhanced performances in multiphase estimation with the implemented

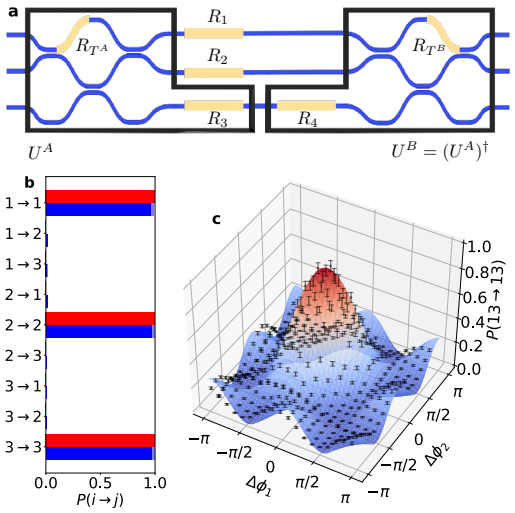

Figure 3.14. **a**, Conceptual layout employed to tune the input and output transformations U^A and U^B **b**, Experimental single-photon probability measurements (blue bars) at $(\Delta\phi_1, \Delta\phi_2) = (0, 0)$, compared with the identity corresponding to the ideal case (red bars). **c**, Experimental two-photon probability measurements for input (1,3) and output (1,3) as a function of $(\Delta\phi_1, \Delta\phi_2)$ by tuning voltages applied to resistors R_1 and R_2. **b-c**, Transformations U^A and U^B are set to reach the condition $U^B U^A = I$ (up to a set of output phases) as described in the main text. This image is taken from [14].

device can be further improved by changing the input state. For instance, let us consider a three-photon input where all modes are injected with a single photon. By evaluating the Quantum Fisher information matrix $\mathcal{H}$ obtained after application of U^A we obtain $\mathrm{Tr}(\mathcal{H}^{-1}) \simeq 0.527$, which is close to the value 0.5 obtained for an ideal interferometer. The actual sensitivity after measuring the output state by applying transformation U^B is quantified by the CRB $\mathrm{Tr}(\mathcal{I}^{-1})$, shown in Fig. 3.15. We observe that quantum-enhanced performances can be achieved with the implemented device, leading to $\min \mathrm{Tr}(\mathcal{I}^{-1}) \simeq 0.584$, lower than the bound $\simeq 0.5 + \sqrt{2}/3$ obtained by sending three distinguishable single photons prepared in the optimal state. Other interesting perspectives can be envisaged starting from the presented results. On the one hand, enlarging the dimensionality of the system will enable the investigation of a richer landscape [518]. In parallel, the capability of fabricating devices with additional controlled phases will allow to develop and test novel adaptive protocols [597, 596, 394, 518], or to tune the detection operator searching for the optimal measurement [482]. These ingredients can be combined in the same platform to develop a novel class of optimal quantum-enhanced protocols, allowing to efficiently extract information on an unknown set of parameters with minimal resource commitment.

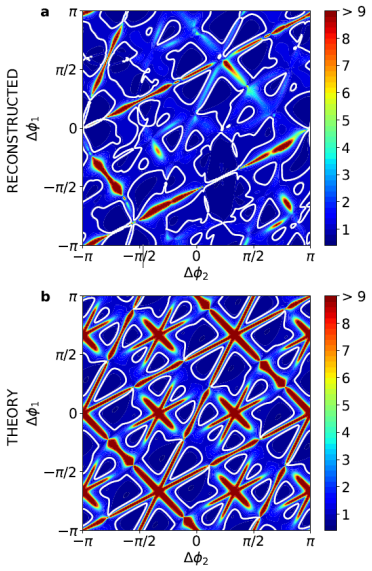

Figure 3.15. Cramer-Rao bound $\mathrm{Tr}(\mathcal{I}^{-1})$ for multiphase estimation with a three-photon input state (1,2,3). **a**, CRB for the implemented device evaluated from the reconstructed parameters, and **b**, CRB for the ideal three-mode interferometer. In the ideal interferometer case, points where the Fisher information matrix is singular are not shown. Regions included within white closed curves highlight the presence of quantum-enhanced performances with respect to the QCRB with three optimal distinguishable single-photon inputs. This image is taken from [14].

3.2.2 Quantum sensor calibration through a Neural Network

As seen so far, Quantum Metrology is a promising research field that allows precision unreachable by any classical sensor. However, a crucial point in the exploitation of a quantum sensor is the calibration of its functionality [362]. Indeed possible biases can add errors not visible to standard measurement using tools as the variance. With the rising complexity of the probed system, such as the case of multiparameter estimation, the number of variables which threaten the measurement apparatus and its correct functionality increase. Conventional characterization methods of the sensors are based on modeling the system starting with theoretical prediction of the involved physical processes, but the possibility to have hidden variables arise as the complexity increases. Further, in realistic sensors, the user has typically access and control over a set of physical parameters, which in turn modify the internal characteristics of the device. Therefore, the target parameters are not directly evaluated, but inferred from measured quantities. Optical phases, determined by electrical signals via thermo-optic effects, are a case in point [614, 28, 616, 617]: here, voltages are the parameters of interest, but the measured optical signal derives from variations of optical phases. Therefore, the sensor inherently works as a transductor, mapping the parameters to be estimated onto measured quantities through a suitable response function, which needs to be characterized as well. In this respect, spurious effects also concur to determining the response function, and must be taken into account. This poses major difficulties in the modeling, and increases the complexity of an experimental characterisation via conventional methods. Then, these standard techniques generally require a lot of data to be correctly implemented, together with intensive post-processing. Alternatively, one could rely on refined a-priori physical models of the sensors, including noise effects, based on measured quantities. Such intensive approaches, however, become impractical for sensors of increasing complexity, and unfeasible in the perspective of commercial devices. Therefore the search for novelty strategies to calibrate a quantum sensor is interesting as well as necessary in the direction of complex system investigation for Metrology purposes. Here, machine learning could provide a favorable tool in order to enhance the calibration process. These are capable of handling large datasets and of solving tasks for which they have not been explicitly programmed. In the last few years, several applications of machine learning methods in the quantum domain have been reported [618, 619, 620], including state and unitary tomography [621, 622, 623, 624, 625, 626, 627, 628, 629], design of quantum experiments [630, 631, 632, 633, 634, 635, 636], validation of quantum technology [637, 638, 639], identification of quantum features [640, 641], and the adaptive control of quantum devices [569, 570, 571, 642, 572, 643, 596, 597, 573, 644, 645, 601, 17, 15, 646, 647, 648]. Also, photonic platforms can be exploited for the realization of machine learning protocols [649, 650]. Recently, a first insight on the application of machine learning methods for the calibration of a quantum sensor has been reported [600]. In detail, the characterization of an optical phase sensor was carried out by means of artificial Neural Networks (NNs) [651]. This has demonstrated its advantages, in that it required no detailed model, relied on the same states for the calibration as for the estimation, and demonstrated robustness to finite-size datasets when compared to standard methods. When extending the use of NNs to multiple parameter scenarios, these features can be preserved, and help to solve a crucial issue. Variations of the parameters can affect the sensor with expected behaviors, as well as with undesired cross-talk effects, with the latter generally hard to model, due to their spurious nature. The effective, non-analytical approach of NNs evades

these difficulties.

In the work [16], we studied the application of a Neural Network for calibrating a quantum sensor for the estimation of multiple optical phases. Furthermore, the approach is proven to be versatile and promising for mass production, as the same Neural Network is able to calibrate different devices having the same structure. Such devices are the same reported in the Sec. 3.2.1 and Sec. 3.3.2, that are integrated three-arms interferometers suitable for a two-phase estimation. Each device is fabricated through FLW and its structure is highly reconfigurable thanks to the presence of several thermo-optic phase shifters. In the following paragraph, the work [16] is presented providing first a brief introduction on the Neural Network tool.

Neural Network

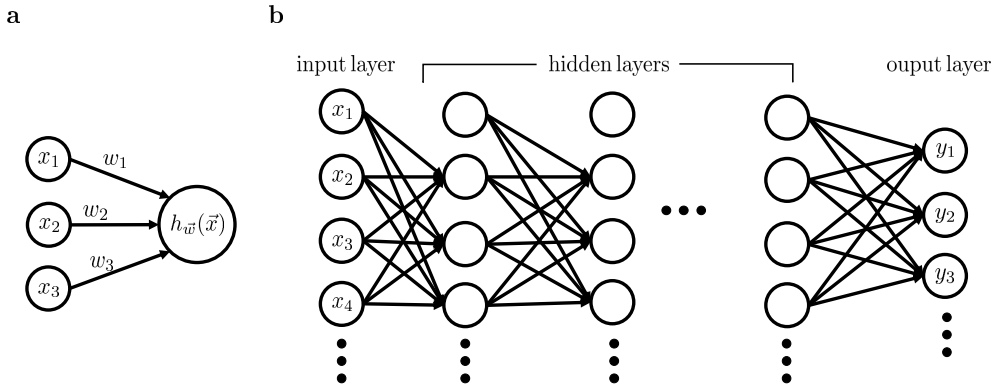

Figure 3.16. Examples of Neural Network. **a)** Each node value of a layer is the results of the activation function $h_{\vec{w}}(\vec{x})$, which depends on the values $\vec{x}$ of the previous layer and a set of corresponding weight $\vec{w}$. **b)** The NN maps a feature vector $\vec{x}$ to a prediction $\vec{\hat{y}}$: the $\vec{x}$ values are associated to the nodes of an input layer, and the output layer provides $\vec{\hat{y}}$ by means of a series of hidden layers, ruled by the chosen activation functions.

Neural Network (NN) is a machine learning technique able to solve supervised learning problems [651, 652]. Its functionality looks like the one of the human brain, and it is highly studied in the artificial intelligence context. NN is able to create a nonlinear map $\vec{y} = f(\vec{x})$ between a set of features $\vec{x}$ and the learning task $\vec{y}$. The $\vec{y}$ values can be continuous variables, resolving regression problems, as stock prices predictions [653, 654]. Also the case of discrete variables, concerning the field of discrimination problems, can be solved by NN, such as for the analysis of medical diseases [655]. In all supervised learning problems, the starting point is a training set, typically very large, which provides pairs of $(\vec{x}, \vec{y})$. The NN is a reconfigurable tool, which takes the $\vec{x}$ values as input and provides output values $\vec{\hat{y}} = f_{\mathrm{NN}}(\vec{x})$, representing the prediction of $\vec{y}$. Such tunable structure is controlled during the learning process in order to correctly predict the right values of the training set. The main advantage of a NN is the ability to find $f(\vec{x})$ without requiring a-priori modelization of the system and the possibility to be applied to a large set of scenarios and problems with very promising results. Conversely, in order to realize an efficient NN it requires a good choice of the features to be used and its architecture. The structure of a NN is reported in Fig. 3.16. The feature vector $\vec{x}$ corresponds to the

input layer, with each element of $\vec{x}$ assigned to a different layer node (or neuron). Then, a series of hidden layers manipulates the starting input nodes calculating the values of subsequent nodes through certain activation functions $h_{\vec{w}}(\vec{x})$. The computation of these functions depends on some weights $\vec{w}$, which are reconfigurable network parameters that connect each node of the previous layer to each node of the next one. Standard choices of activation function are sigmoid (Logistic function) $h^{\text{sig}}_{\vec{w}}(\vec{x})$ and rectified linear unit (ReLu function) $h^{\text{ReLu}}_{\vec{w}}(\vec{x})$ [651, 652]:

$$h^{\text{sig}}_{\vec{w}}(\vec{x}) = \frac{1}{1+e^{-\vec{w}\cdot\vec{x}}}\,, \qquad h^{\text{ReLu}}_{\vec{w}}(\vec{x}) = \max\{0, \vec{w}\cdot\vec{x}\}. \tag{3.48}$$

The last layer is the output layer, which provides a prediction $\vec{\hat{y}}$ of the $\vec{y}$ values. The training of the NN consists of continuous iterations, called *epochs*, during which the network is interrogated and reconfigured over the weights parameters. When the network is fixed, the error on the NN predictions can be estimated by the total Root-MSE (RMSE). As the epochs increase, the network is changed in order to decrease the next RMSE. Network training typically requires a lot of time and resources, and more common algorithms that optimize this process take advantage of the computation of the RMSE gradient with respect to the tuned parameters. Therefore, the weight connecting the different nodes are tuned during the training process of the NN, in order to provide a prediction $\vec{\hat{y}}$ as near as possible to the true $\vec{y}$, thus reconstructing the f-map. Correct construction of the NN characteristics, such as the choice of the activation function to exploit, the number of hidden layers as well the number of nodes for each layer to use, up to the features $\vec{x}$ more informative to describe the system, represents the fundamental point, whose right realization is far from being obvious. Heuristic techniques are commonly used for the research of the NN characteristic to implement. Here, the analysis of the NN response over a further independent validation set is the principal way to test different NN architectures. Specifically, when the architecture is fixed, the NN parameters are trained on the initial set, while the final RMSE is measured on the validation set. Varying the NN structure, the best RMSE on the validation set determines the best architecture to use. Indeed the strength of the validation set relies on its independence from the set used for the training, thus providing a statistical analysis of the NN performances totally uncorrelated from the training stage. Indeed, the RMSE over the training set necessarily decreases as the number of epochs increases. However, while initially this process represents an improvement of the NN-precision, after a certain number of iterations, the procedure unavoidable starts to overfit the training set. Conversely, the independent set of cases (validation set) after the initial decreasing of the RMSE, starts to grow up as the training set begins to be overfitted. In conclusion, the right number of iterations necessary to train a given NN with the best precision is provided by the minimum of the RMSE over the validation set. This number of epochs strictly depends on the specific problem under study. At last, once the architecture to use is decided, the final performances of the NN are commonly computed by a new independent test set. This stage is used to generalize the NN over new uncorrelated cases, and can be exploited for testing the given NN over any condition, e.g. when realistic noisy scenarios are involved.

Three mode interferometer calibration enhanced by NN

We implemented a NN to calibrate a quantum sensor for the simultaneous estimation of two optical phases. This implementation is divided in two stages.

During a first stage we adopt simulated data to investigate the correct structure of the NN to use, both in terms of the architecture (number of layers, number of nodes, etc) and the amount of data necessary for a complete NN training. Then, in the second stage we experimentally tested the performances of a NN, which uses a structure resulting from the previous study. These performances are evaluated by training the NN with experimental data and by subsequently using it to predict values of another experimental validation set. Notably, the simulated data used for the first stage are reconstructed by exploiting a maximum likelihood technique over experimental data. In our case, during the experimental data recording, the parameters controlled by the user are the electric voltages and not directly the internal phases (Sec. 3.2.1). If one is interested in the physical relative phase-shifts $\Delta\phi_1$ and $\Delta\phi_2$ resulting from the application of the two voltages V_1 and V_2, a preliminary calibration step is required. The characterization of the voltage-to-phase response is unavoidable for any similar sensor and can result in additional calibration errors of the global response. A possible model [14] is provided by Eq. (3.47). Therefore, in standard characterisation, a theoretical model of the circuit is necessary to recover the output probabilities through a fit of the measured probabilities. This, in turn, allows extrapolating dynamic and static parameters of the chip [14, 15]. Conversely, the aim of this work is to avoid relying on knowledge about both the theoretical model of the circuit and the response function in Eq. (3.47). In fact, this would prove inefficient for the characterisation of mass-produced devices. The goal, instead, is to generate a mapping between voltages and output probabilities using only a limited set of measurements. We exploit the NN approach exactly to realize this goal (Fig. 3.17).

Stage 1: NN architecture analysis

The preliminary step has the only purpose of arranging the structure of the NN for the calibration of a general three-arm interferometer. As described above, we start considering as training set the data reconstructed by exploiting a fit over experimental data. While it is instrumental for our verification of the NN method, it is not required for its actual use. Specifically such a probability was obtained from the same reconstruction method employed in [14] (Sec. 3.2.1). In this way, the simulated data represent roughly the typical approximate probabilities of interest. In particular, we simulate new output events, distributed according to Poissonian statistics whose mean values correspond to measured experimental events. Such events are recorded by tuning in the model the pair of voltages applied over two internal resistors of the interferometer. The simulated events are converted in new output probabilities — $P(i \to j)$ with input i and output j — and data for the training are extracted for any possible combination of input-output in a single-photon regime. In this way we construct a training set of size N, whose single element is:

$$\{\vec{x}, \vec{y}\}_k = \{P(i \to j), (V_1, V_2)\}_k \text{ for } i, j = 1, 2, 3. \tag{3.49}$$

The index $k = 1, \ldots, N$ refers to each training example and N represents the total number of training data. Considering the Poisson distribution for the simulation procedure is an important step in order to properly study the NN in our scenario, taking into account the presence of the typical source of uncertainty in photonic implementations. A part of the data, i.e. 15% of the whole set, is used as a validation set: it is not directly employed for the training, but rather to obtain an independent estimate on the training error. As described in the previous paragraph, this is necessary to avoid overfitting. Using the training data we studied different

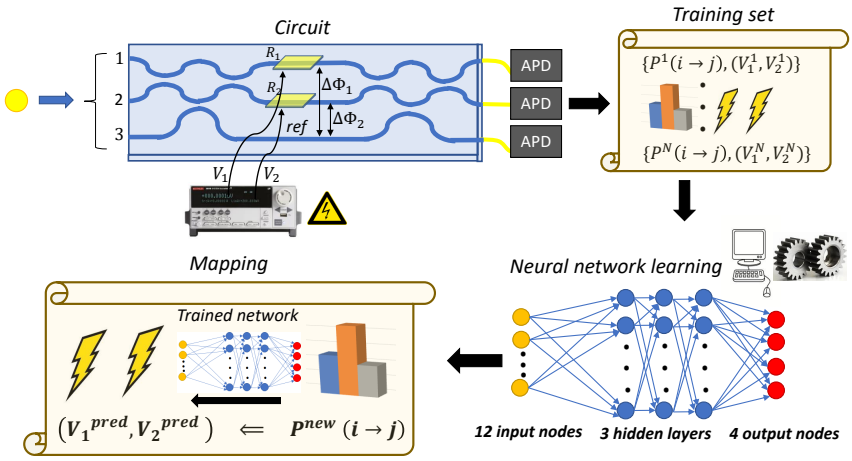

Figure 3.17. Conceptual scheme, showing the calibration steps in clockwise sense. Circuit: single photons are sent along the inputs of the three-arm interferometer and revealed by avalanche photodiodes (APDs). Training set: the output probabilities $P(i \to j)$ (with $i, j = 1, 2, 3$) are measured as function of the two applied voltages V_1 and V_2, collecting a total number of N training examples. As explained in the main text, the kick values $(\Delta V_1, \Delta V_2)$ and its probabilities $\tilde{P}(i \to j)$ (not shown in the figure), are also considered for removing ambiguous points. For this reason the NN has four output nodes. NN learning: a small portion of the data set, is used to train the neural network. Mapping: after the training the NN is able to map any output probability $P^{\text{new}}(i \to j)$ to the corresponding pair of voltages, predicting the values $(V_1^{\text{pred}}, V_2^{\text{pred}})$ and the kick ones. This image is taken from [16].

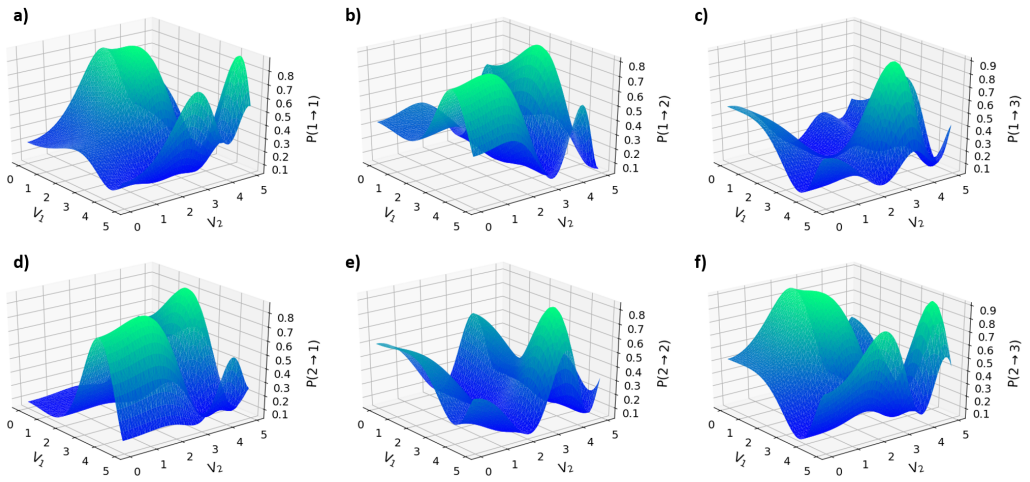

Figure 3.18. Examples of input-output probabilities $P(i \to j)$ for each input i and output j $(i, j = 1, 2, 3)$ of the chip, resulting from predictions of a NN trained with simulated data, as function of the applied voltages V_1,V_2 over two ohmic resistors. **a)-c)** Output probabilities $P(1 \to j)$ obtained by injecting single photons along input 1. **d)-f)** Output probabilities $P(2 \to j)$ obtained by injecting single photons along input 2. This image is taken from [16].

architecture for the NN. We varied the number of hidden layers and the number of nodes for each layer. We tested different activation functions, initialization parameters and optimization algorithms. Finally we chose the configuration which provided better results, obtaining the lower value for the RMSE calculated over the validation set. Here, the network is trained using $53 \times 53 = 2809$ different tension pairs in the training set and the corresponding output probabilities. The Adam algorithm [656] is adopted to tune the model's parameters, by optimizing the cost function, given by total RMSE. This algorithm exploits the gradient descent, whose value at each step is computed through the backpropagation technique [651, 652, 657]. Thus, a first version is a NN configuration with 9 nodes in the input layer and 2 in the output ones, associated respectively to the 9 configuration of probability and the 2 values of the voltages pair. Further, we notice that the probabilities are not independent, due to the constraints imposed by the unitarity of the transformation, and the full set of 9 probabilities is redundant for the network training. Indeed, only 4 of them are required, plus their normalization. Given this redundancy, satisfactory results can be achieved training the network with the 6 probabilities obtained when injecting a photon respectively in the first and second input of the device.

However, the above versions suffer the non-injectivity of the likelihood function, which constrains the application range over the voltages of the NN. Indeed such characteristic makes different pairs of voltages correspond to the same output probabilities, thus having multiple equivalent points. This ambiguity is strictly related to the physical process involved, and solving it is fundamental in order to guarantee the correct and wider functionality of the sensor. We removed this ambiguity by adding a further set of probabilities $\tilde{P}(i \to j)$, namely a "kick", to each element of the training set, in this way:

$$\{\vec{x}, \vec{y}\}_k = \{(P(i \to j), \tilde{P}(i \to j)), (V_1, V_2, V_1 + \Delta V_1, V_2 + \Delta V_2)\}_k \tag{3.50}$$

where the values $\tilde{P}(i \to j)$ are added by considering the probabilities obtained

by changing V_1 (V_2) of a fixed value ΔV_1 (ΔV_2). The kick is *de facto* treated as additional input probabilities by the NN, and as such, once chosen, to allow for the NN to correctly associate their values to the voltages, they need to be kept fixed between the training and the test. The optimal values for ΔV_i need to be tailored to the functions at hand, as they depend on the steepness and periodicity of the probabilities. In our case, we have implemented kicks associated to $\Delta V_1 = 0.57\,V$ and $\Delta V_2 = 2.27\,V$. Adding this information allows not only to apply the NN limitless over the voltage values, but even the improvement of the performances measured over the whole validation set. Indeed, when evaluated in the full range of tension values, the global RMSE of the validation set is enhanced of a factor 85% respect to the NN without kick. The advantage obtained is independent from the specific value of ΔV_1 and ΔV_2, as long as they are large enough to give information about different regions of the inspected functions. In conclusion, the best performances are obtained from a NN having 3 hidden layer with 200 neurons per layer, 12 nodes (6 from kick) in the input layer and 4 nodes (2 from kick) in the output ones (Fig. 3.17).

All the nodes, except the output ones which are activated by a linear function, are activated by a ReLu function initializing their weights with random values extracted from a normal distribution centred in zero and with variance $\sigma^2 = 2/n$, where n is the number of neurons in the previous layer. The number of epochs resulted from minimizing the loss function on the validation set is 250. During each epoch, all the training data are passed to the NN which adjusts its internal weights. Moreover, to make the algorithm more efficient the whole training set can be divided in small random batches which are iteratively analyzed during each training epoch. The trends of the values predicted by the trained-NN are reported in Fig. 3.18 as a function of the applied voltages on the two selected resistors.

Stage 2: generalization of NN performances

Testing the chosen NN on different data scenarios is a fundamental step in order to provide a correct estimate of its generalization capacity. First of all, to analyze the variability among different trainings, we study the results obtained, starting from the same datasets, after performing 50 independent trainings of the network. The mean value of the normalized-RMSE (NRMSE) achieved on the validation set in such configuration is NRMSE $= (1.5 \pm 0.1)\%$. After the network has been trained, its performances have been evaluated on a further independent test set of 100 different examples selected randomly among the possible tensions pairs of the 53×53 grid. For these elements, new values of probabilities are computed by adding random Poissonian noise on the detection events corresponding to the selected voltages in the initial set. Notably, since both the training and the test data are corrupted by random Poissonian noise, the resulting NN is robust when evaluating new noisy examples. In this way, the NN efficiency over data conditions having realistic noise of an optical interferometer can be tested. To quantify how close the network estimation of the tension values is to the true ones, we evaluate the *cosine similarity* between the vector of network outputs $\vec{y}$, corresponding to the 4 tensions for all the test examples, and the expected results $\hat{\vec{y}}$, as follows:

$$c = \frac{\vec{y} \cdot \hat{\vec{y}}}{||\vec{y}|| \cdot ||\hat{\vec{y}}||}. \tag{3.51}$$

In the ideal case, when the prediction $\hat{\vec{y}}$ is equal to the true value $\vec{y}$, the cosine similarity provides $c = 1$. Moreover, to estimate how much the cosine similarity depends on the random sample selected, we compute its value on 500 repetitions each

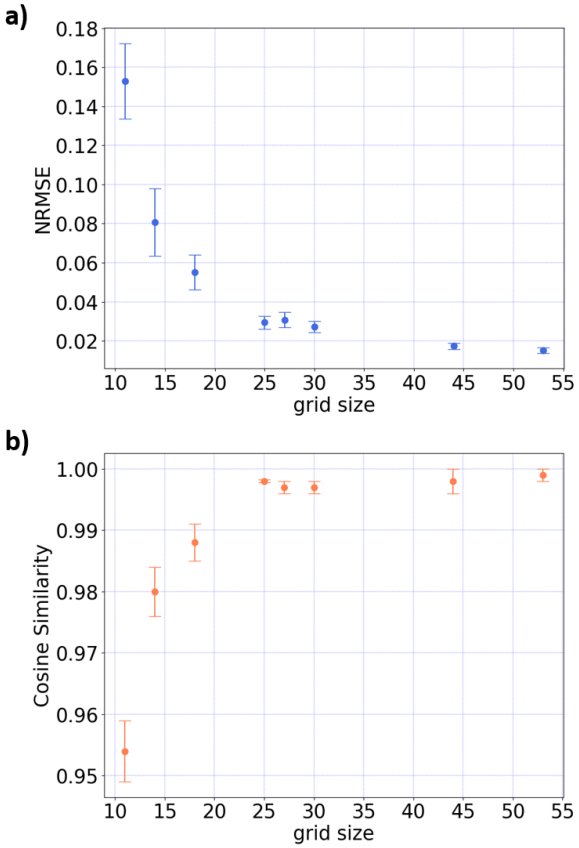

Figure 3.19. NN training with different amounts of data grid size. Training performances are shown in terms of **a)** NRMSE computed over the validation set and **b)** cosine similarity on the test one. This image is taken from [16].

containing 100 examples extracted randomly among the available ones, obtaining a value of $c = 0.999 \pm 0.001$.

Then, we investigate how the NRMSE on the validation set and the cosine similarity between the network estimation and the true tensions values change reducing the number of tension pairs used for the training. For all the different configurations the size of the training set, and consequently of the validation one, changes depending on the dimension of the tension grid used. Conversely, the number of examples making up the test set remains fixed to 100. For all the new training configurations the test data are still extracted randomly from the largest grid. This choice is performed to assess how much reducing the data for the training affects the final network estimation of new examples. In Fig. 3.19 are reported the NRMSE on the validation set, obtained from multiple trainings of the network and the cosine similarity among the network estimation and the expected values in the test set. As expected, the NRMSE achieved by the network decreases as the number of training examples increases, allowing a better reconstruction of the function mapping the input vector onto the output one. A better reconstruction of this function grants higher network performances on the independent test set, as shown by the growth of the cosine similarity between the reconstructed tensions vectors by the NN and the real one. The error on the cosine similarity values gives an indication about the

variability linked to the analysis of different examples that randomly fall in different regions of the probabilities functions. In parallel, the error on the NRMSE values depends on the results of different trainings of the algorithm that, starting with random initial parameters, can end up in slightly different conditions.

Table 3.3 reports the most characteristic final parameters of each step performed.

Set	Parameters	
Training	size	2809 (grid 53×53)
	epochs	250
Validation	size	421
	NRMSE	$(1.5 \pm 0.1)\%$
Test	size	100
	cosine similarity	$c = 0.999 \pm 0.001$

Table 3.3. Parameters of the employed Neural Network resulted from simulated data.

Stage 3: experimental NN evaluation

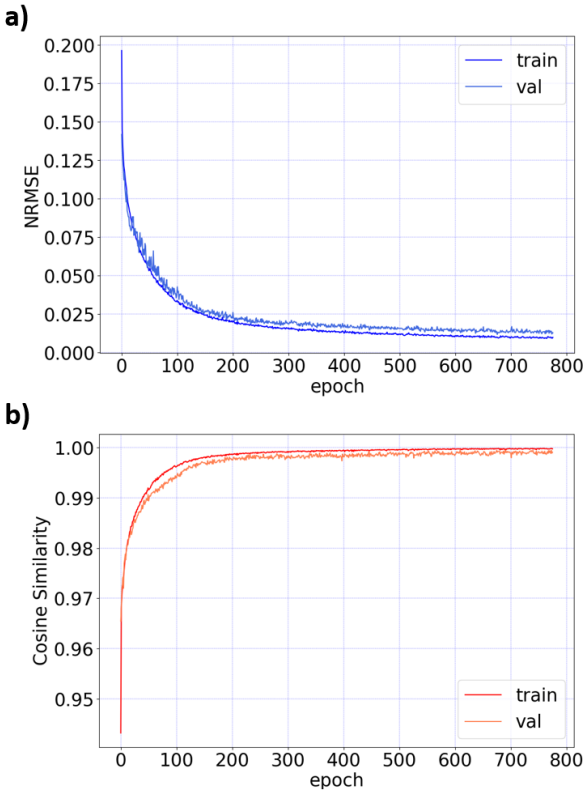

Figure 3.20. Study of NN performances by using experimental dataset for both training and validation stages. **a)** NRMSE and **b)** cosine similarity are shown as function of the computed epochs. This image is taken from [16].

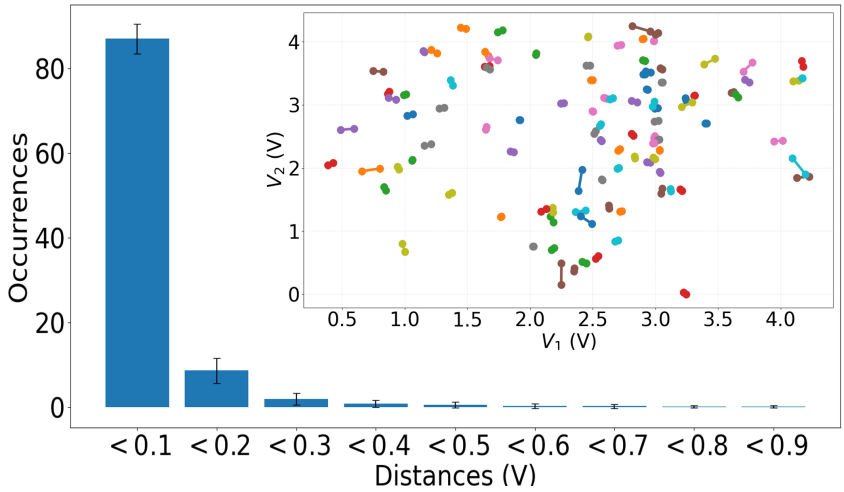

Figure 3.21. Histogram of the two-point distances obtained over the test set of 100 points. The error bar represents the standard deviation computed over 500 different random batches of test sets. Inset: We report one of the 500 random test sets consisting of 100 points represented in the same color and linked by a line to the 100 predicted tension pairs by the NN. This image is taken from [16].

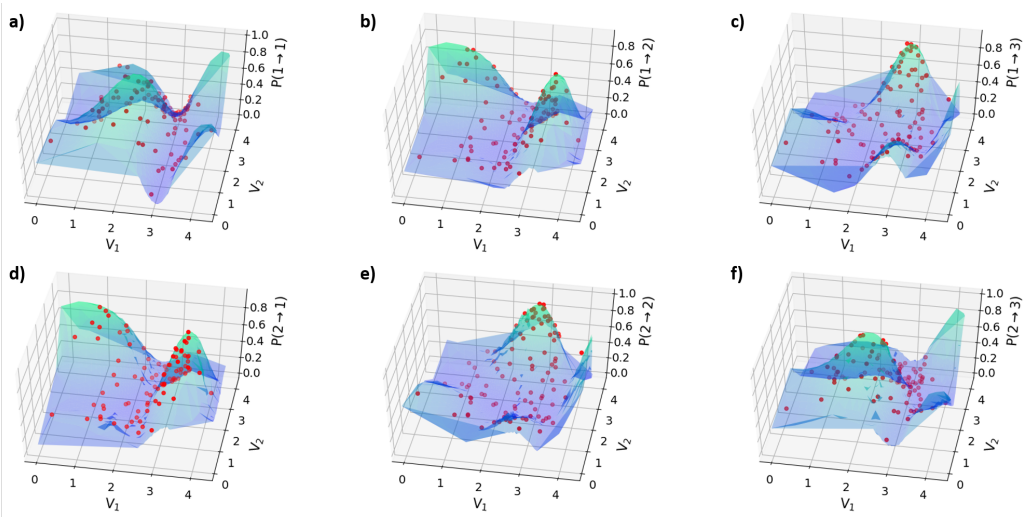

Figure 3.22. Comparison between voltages predicted from NN (red dots) and grid of experimental values (blue surface) for different single-photon input-output probabilities. This image is taken from [16].

Finally, the network architecture resulting from the previous analysis has been implemented and tested training the NN directly on actual experimental data. This is possible thanks to the network efficiency to learn the function which maps the input-output probabilities to the tensions applied. In this way, a good estimate of the tensions values is obtained. If the explicit model of the voltage-to-phase response is available, this same procedure is also effective to calibrate the device explicitly in terms of the phases; the exact description of the further propagation and measurement steps is not needed. We want to test the robustness of the developed NN with respect

to its hyper-parameters, such as the number of nodes and layers. For this purpose, we calibrate another integrated circuit with different output probabilities but the same structure of the first one. More specifically, we use the data obtained from a 50×50 tensions grid applied on a second integrated device with the same layout, to train the same network as the one described above. The training with such data takes longer to reach the region where the loss function on the validation set stops decreasing. This is shown in Fig. 3.20, where the NRMSE and the cosine similarity are reported as a function of the training epochs. The network tensions estimations when 100 new data are acquired are reported in Fig. 3.22, showing the ability of the network to make accurate predictions of the applied voltages. To visualize clearly the difference among the predictions obtained by the NN and the expected tension values we report in the inset of Fig. 3.21 the same points of Fig. 3.22 together with the true tension values. To study the variability among multiple test batches we compute the standard deviation over the NRMSE obtained on 500 different random test sets obtaining a value of NRMSE $= 0.022 \pm 0.009$ which, as expected, it is compatible with the results obtained on the validation set and reported in panel **a)** of Fig. 3.20. To quantify the difference among the predictions and the true values we also compute the two-point distances of all the 100 points for all the 500 test repetitions. The histogram reported in Fig. 3.21 shows that more than the 80% of the predicted points are at a distance from the true tension values less than $0.1V$, demonstrating the accuracy of the NN predictions. In this way, we have shown that the parameters chosen for the NN can be applied also for calibrating different circuits sharing the same structure. This feature is key in the perspective of mass-produced devices with the same layout. This black-box approach is by no means limited to calibrations for Metrology, and can find more extensive applications. For instance, the same NN could be used to extract the voltage settings necessary to obtain target splitting ratios among the three output probabilities. Also in this case, in which our device is operated as an intensity partitioner, NN could provide a practical solution to assess its actual capabilities.

Conclusions and perspectives

We have reported on the application of a NN based algorithm to perform the calibration of integrated devices depending on two parameters. In this investigation we relied on knowledge of a model to identify the most appropriate regime for collecting the training set. However, this is by no means a necessary step in that the use of the NN itself incorporates the same information that would be present in the model. Remarkably, the NN is able to account for spurious effects such as, in our case, cross-talk between thermal actuators, which are otherwise intricate to describe. Concerning the scalability of the NN approach, two aspects need to be considered. First, this method is not expected to mitigate the growth of the required number of collected data points for increasing system size. The gradients of the response function also significantly affect the collection size. Second, the scaling of the network itself will depend on the complexity of the studied system. However, these aspects are well balanced by the fact that NNs are intrinsically well suited to handle large data sets. Overall, this approach still can be beneficial in tackling more complex systems, depending on a large number of parameters, otherwise intractable through standard fitting procedures. Moreover, even if the NN approach does not require a full description of the device, it can be foreseen that some basic modeling of it could be nevertheless beneficial. The successful characterization of two devices based on a single approximate model shows that the NN performance does not

heavily depend on the model's level of detail. In the same vein, some anticipation of the device output, might reveal whether ambiguities may be present in the chosen range of parameters. We have shown that this is easily accounted for by introducing additional data as input to the NN.

This study brings forward machine learning applications in two respects: it goes beyond optimization of the employed resources when these are severely constrained and shows that this characterization method extends beyond the single parameter regime. The obtained results give evidence that NN can provide an effective, robust and reliable tool for the calibration of complex sensors that depend on multiple parameters, with the advantage of requiring no detailed model of their internal operation.

3.3 Adaptive phase estimation enhanced by machine learning protocols in single-photon regime

In many realistic scenarios, the number of probes that can be exploited in the estimation process is limited. Examples are provided by highly sensitive biological samples that can be damaged by high fluxes of photons [363, 658, 527], fragile atomic or molecular systems [659, 660, 661, 662, 663], or communication scenarios where few photons are employed [3]. Theorems guarantee the possibility to reach the fundamental bounds achievable by using a given probe. However, such capability is guaranteed only in the asymptotic regime where a large number of copies of the probe state are employed (Sec. 3.1.2). In the case of limited data [664, 553] the asymptotic recipes do not represent necessarily the optimal solutions and other kinds of estimation must be investigated. Tuning adaptively the system during the estimation process seems the only valid alternative (Sec. 3.1.4). In phase estimation problems this can be done by exploiting further layers of phases that are controlled as feedback during the learning process. Adaptive protocols have demonstrated the ability to saturate CRB also when the number of available probes is limited and avoiding ambiguity problems related to the geometry of the likelihood. The optimal control phases to be applied can be computed online or offline, respectively, before or during the estimation process (Sec. 3.1.4). Here, machine learning techniques represent an efficient solution to improve complex computations in adaptive schemes. Notable examples of protocols lying in the online category are adaptive Bayesian techniques (Sec. 3.1.4.1). Those protocols lying in the offline class are crucial for different practical scenarios. For instance, they are necessary when the computational power available during the estimation process is limited, or when feedback controls are used for fast processes and the time available for an online calculation is small. However, the space of all possible actions for the feedback parameters to be calculated in an offline approach can be huge, and many parameters functions optimization in such space is a computationally expensive task. In order to handle the complexity of this optimization, an effective solution is provided by machine learning. In the context of phase estimation, different machine learning techniques have been used to calculate feedback actions in the offline approach. As shown in Sec. 3.1.4.2, two relevant examples are DE and PSO. These are evolutionary algorithms [604, 605] inspired by biological dynamics, which are able to solve optimization problems using a trial and error approach, and thus finding global maxima. The solution of such algorithms, applied in the context of phase estimation, are lists of optimal feedback phases to be employed during the process. Such lists live in a high-dimensional space and are optimal in the sense that they maximize a chosen figure of merit, called *fitness*, related to the precision of the estimation. The choice of the fitness function is performed depending on the specific problem at hand. In general, some machine learning techniques can be more suitable than others, depending on the task. It is then of crucial importance to find and explore different approaches able to enhance phase estimation processes.

On the other hand, the realization of quantum sensors, able to perform estimations in realistic scenarios, poses a second constraint to sensing devices: not only the demands for the optimization of the limited resources, but also the systems can show high complexity, often involving more than one parameter. Measuring multiple parameters at once might be necessary in complex systems characterized by a set of parameters, where a time or spatial dependency can prevent the successful realization of subsequent single-parameter estimations. The parameters considered can

span from multiple phases [14, 485, 482], to phase and phase diffusion in frequency-resolved phase measurements [665, 532, 534], and phase and loss in absorbing systems [666, 667]. In other instances where a system depends solely on one parameter, a multiparameter approach could still be favorable as other parameters can be interrogated as a control to monitor the quality of the sensor itself [525, 526, 527]. Different theoretical works have studied a non-asymptotic Bayesian approach in quantum multiparameter estimation [668, 435, 669, 670, 671], thus providing bounds and protocols to generally address limited-data Quantum Metrology. In this context, it becomes of paramount importance to identify both a suitable estimation scenario and a corresponding platform for an experimental investigation of adaptive multiparameter estimation protocols. A notable scenario to investigate is multiphase estimation [514, 485, 515, 516, 517, 482, 487, 518, 467, 519, 524, 14, 672]. Not only does such scenario provide a benchmark for multiparameter Quantum Metrology, but it has a plethora of practical applications in quantum imaging [427, 428]. A fundamental step is to find a suitable experimental platform to realize multiphase estimation. A viable solution is provided by integrated photonics, which enables the implementation of complex circuits with reconfiguration capabilities [28, 47, 673, 10, 617, 674] with applications ranging from Quantum Simulation to Computation and Communication. This platform represents a promising system for optical Quantum Metrology since interferometers with several embedded phases can be employed as a benchmark platform to study multiparameter estimation problems. In this direction, we recently reported the first results on multiphase estimation with quantum input probes [14], using a three-arm interferometer fabricated by femtosecond laser writing (Sec. 3.2.1).

In the following section two studies of adaptive phase estimation will be presented, where online and offline protocols are developed and used in two experimental platforms. In a first work [17] we studied and implemented an adaptive protocol for the efficient estimation of a single phase in a bulk interferometer (Sec. 3.3.1). The optimal feedback phases to be applied are calculated offline through a genetic algorithm. The second platform (Sec. 3.3.2) is a photonic chip with the same structure adopted in the Sec. 3.2.1, that is an integrated three-arm interferometer, suitable for the simultaneous estimation of multiple phases. Using the interferometer, the implementation of an efficient adaptive online protocol for two-phase estimation in limited data regime [15] was experimentally realized.

3.3.1 Single-phase estimation in a two-mode MZI

Photonic phase estimation employs light probes in an interferometric scheme to estimate an unknown phase shift between two optical modes. A paradigmatic scheme for this task is a Mach-Zehnder interferometer (MZI) (Sec. 3.1.3). Here two input modes interfere in a first optical element. Then, the two modes of the MZI, after acquiring a relative phase shift ϕ, interfere in a second optical element. A MZI can be encoded in photon path, where photons interfere in beam-splitters as shown in Fig. 3.23a. The same structure can be obtained in other degrees of freedom, such as polarization, where modes are mixed via half wave-plates (Fig. 3.23b) [1]. The goal of the process is to estimate the unknown phase shift ϕ by

measuring the probe states after propagation through the interferometer. When the probes are composed of single photons, the phase-dependent output probabilities corresponding to the two possible measurement results ($x = 0, 1$) are $\cos^2(\phi/2)$ and $\sin^2(\phi/2)$ respectively. Through the dependence of the output probabilities from the unknown phase, one can extract information on the parameter. The amount of information available is quantified by the Fisher Information [Eq. (3.8)], defined as $\mathcal{F}(\phi) = \sum_x P(x|\phi)(\partial \log(P(x|\phi))/\partial\phi)^2$, where $P(x|\phi)$ is the likelihood function that corresponds to the probability to obtain a measurement result x, given a certain value of the phase ϕ. The Fisher Information is related to the bound on the variance achievable with any arbitrary unbiased estimator by the CRB [Eq. (3.9)]: $\Delta\phi^2 \geq 1/[N\,\mathcal{F}(\phi)]$, where N represents the number of identical independent probes. For the case of a MZI seeded by single photons, the Fisher Information is constant for any phase ϕ and the CRB reads $\Delta\phi^2 \geq 1/N$, that is, the SQL for the single phase estimation [Eq. (3.30)], which represents the maximum precision achievable with classical probe states. In the limit of a large amount of measurements, estimators such as maximum likelihood or Bayesian ones permit to saturate the SQL [359]. However, this is no more true when the measurements and data are limited [454]. In this regime the Fisher Information may not represent the ultimate achievable bound, and non-trivial approaches have to be adopted to optimize the convergence of an estimation process to the ultimate limits. In this way, even if the Fisher Information does not depend on the unknown phase, the convergence of the estimation process (in terms of the number of resources N necessary to saturate the bound) can be

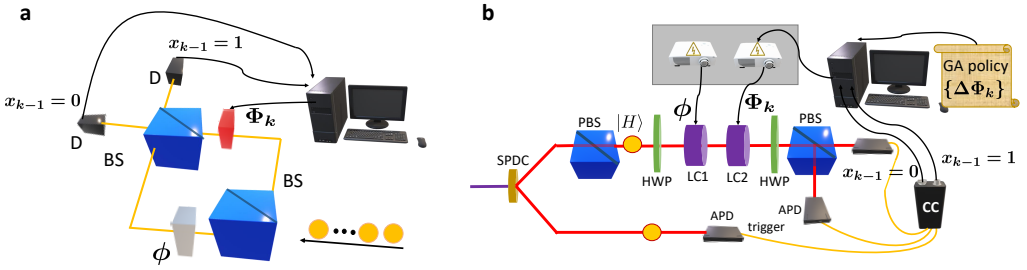

Figure 3.23. Adaptive phase estimation. a, Conceptual scheme of a Mach-Zehnder interferometer in the photon path degree of freedom. The interferometer is composed of two cascaded beam splitters (BS) and relative phase shifts are inserted between the two paths. Single photons are injected along an input of the interferometer in order to estimate the unknown phase shift ϕ. At each step k of the adaptive protocol, the control phase shift Φ_k is calculated by a processing unit, according to an heuristic that exploits the previous dichotomous measurement result $x_k = 0, 1$ at step $k - 1$ from detectors (D). **b**, Experimental setup, corresponding to a MZI in the polarization degree of freedom able to implement adaptive phase estimation. A spontaneous parametric down-conversion source generates pairs of photons: one photon (signal) of each pair enters in the interferometer, while the other acts as a trigger. After a polarizing beam splitter (PBS) and a first half-waveplate (HWP) rotated by 22.5°, the signal photon is prepared in a diagonal polarization state and experiences the unknown phase shift ϕ between the two polarizations H and V, inserted by the first liquid crystal LC1. The control phase shift Φ_k at step k is applied by a second liquid crystal LC2, which is driven by a processing unit that applies the GA-optimized feedback according to the previous measurement result x_{k-1}. The measurement stage is composed of a final HWP rotated by 22.5°, a PBS and single-photon detectors (APD) at the interferometer outputs. The result x is generated by the coincidence between the signal photon and the trigger one. This image is taken from [17].

faster around certain phases when the number of data is limited.
Hence, one of the most powerful approaches for this problem is provided by adaptive protocols [544, 556]. In an adaptive protocol for phase estimation, an additional controllable known phase shift Φ can be introduced in the interferometer. The value of Φ can be changed depending on the previous measurement results, so as to tune the total phase shift inside the interferometer near the optimal point during the estimation process. Consider N single photons which are injected, one by one, in one input port of a MZI. The feedback phase at step k will be chosen according to some heuristic and to all previous measurement results $\{x_1, x_2, ..., x_{k-1}\}$. In the case of offline protocols, the rules to change the feedback phase Φ are calculated in advance before the experiment. The list of all the feedback actions is called a *policy*. Different machine learning techniques have been exploited to calculate such policies [569, 570, 571, 572]. Here, we introduce a novel technique exploiting a genetic algorithm as an offline approach to calculate the policies for phase estimation.

Genetic Algorithm

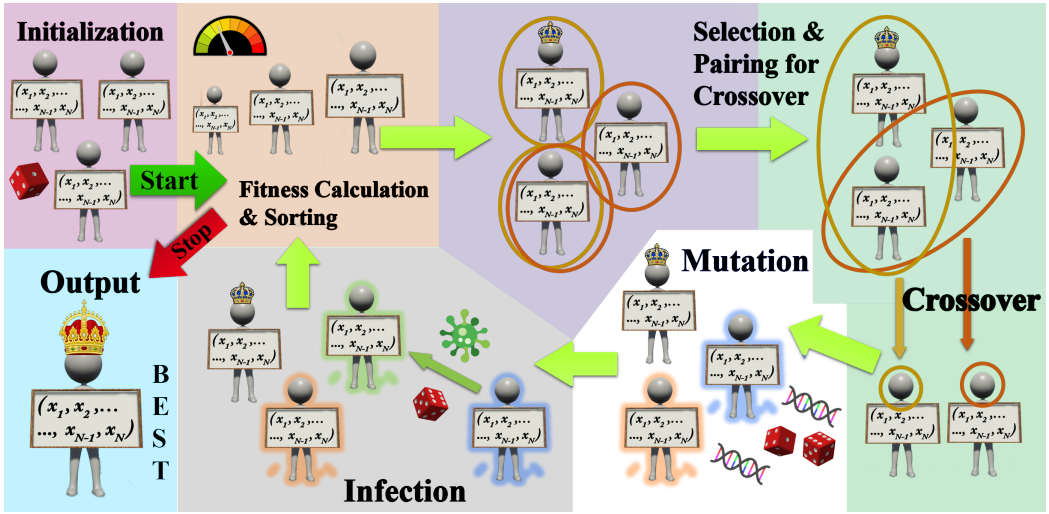

Figure 3.24. Conceptual model for the evolution employed by genetic algorithm. The humans shown represent an individual or chromosome, with a set of properties known as genes shown by the board they hold. The algorithm starts with the initialization of a group of random individuals, known as population. The population then proceeds to start a cycle of application of *Genetic Operators*, namely *Fitness calculation, Selection, Crossover, Mutation* and *Infection*. The cycle ends depending on a halting condition and returns the best individual as output. The *Fitness* operation assigns a fitness score to all individuals and sorts them accordingly on that basis. The *Selection* operator selects an individual from the population each time it is used. The *Crossover* operation uses the selection operation to pair up two individuals and produce offspring from them. This reproduction is repeated till the population size is achieved. The produced offspring then mutate randomly using the *Mutation* operation and the *Infection* operation with some probability replaces one of the individuals with a randomly created new individual. Further, during all the process the individual with highest fitness after the sorting process, shown by the king, is immune to mutation, infection and is not replaced by the offspring. The king may or may not change at each cycle. This image is taken from [17].

Genetic algorithms (GAs) represent a class of evolutionary computation approach

inspired by Darwin's theory of natural selection [675]. Different search-based optimization problems can be faced by GAs. The elements of the search space are termed *individuals* and represent the possible solutions of the optimization. The aim of the algorithm is to find the individual which optimizes a certain figure of merit called *fitness*. Starting from a *population*, which is a group of individuals, the GA evolves it in the search space. The evolution of the population corresponds to moving in the search space. The main principle of the algorithm is biological evolution based on survival of the fittest individuals. GAs are suitable for problems with large search space, requiring no initial information about the nature of the solutions, which is a common scenario for many real world problems. The algorithm decision making also has an advantage in the exploration-exploitation trade-off helping the algorithm to avoid local extremas, and move towards a globally optimum solution in the search space. GAs can be used in a large variety of problems like image processing, artificial intelligence in robotics, computer games, optimization of parameters of other machine learning algorithms like the weights of Neural Networks, and a variety of engineering problems among others [676, 677].

Each candidate solution of the optimization problem has a defined structure (chromosome), that is composed of genes. In some problems, the solutions are represented with binary encoding of the genes, as arrays of 0s and 1s, but encoding using other structures is also possible, for instance the genes can be encoded in the elements of a vector of real values. The goodness of each solution is quantified by the so-called fitness score, calculated through a fitness function that is determined by the objective function of the problem. Such objective function is at the basis of the optimization in the algorithm. During the evolution process, some of the initial set of solutions are selected for reproduction and recombination, according to particular techniques, to move towards new solutions (offspring) in the searching space. The offspring produced solutions for the next generation (or iteration) undergo a process of mutation, leading to the creation of a new generation of individuals. In particular, the genes of the offspring solutions depend on the properties inherited from the previous generation through crossover and random mutation processes. The individuals with higher fitness scores have a larger probability of being selected for the mating process, that allows the production of new fitter individuals. This method ensures the survival of better solutions in the iterative evolutionary process, until the termination criteria is reached or the search saturates in some extrema, either global or local.

In this work we exploit a modified version of genetic algorithm (see Fig. 3.24) suitable to perform optimization in the continuous search space of real vectors representing the policies to be employed in the phase estimation process. We mention in detail the steps of the used GA (for pseudo-code, see Algorithm 2).

Population initialization and Fitness calculation

The first step of the protocol is the initialization of a population: a set of lists $\{\boldsymbol{\Delta\Phi}\}$ of feedback phase shifts, corresponding to the algorithm chromosomes, is randomly generated. This initialization can be realized also taking into account eventual prior information on where the optimal solutions are expected to be located in the search space. In our case, we consider a search space limiting the possible unknown phases in the range $[0, \pi]$. In the case of a phase estimation experiment using N single photons, the chromosome associated to each individual is represented by a vector $\boldsymbol{\Delta\Phi} \in \mathcal{R}^N$ of N real values. Such quantity corresponds to the policy to be applied during the experiment. In particular, during the optimization of the

policy with N probes, the population is initialized with the first two chromosomes taken from the best policy for $N-1$ probes, with a Gaussian shift in each gene value having a standard deviation linearly decreasing as SQL. Instead, the last value (N^{th} value) in such policies is chosen as 0. Then, the rest of the population is initialized with completely randomly created chromosomes. This kind of initialization ensures that information from previous optimal policies is properly exploited during the following search processes.

Each candidate solution is then associated with a fitness score, which quantifies the sensitivity of the policy in the estimation of the unknown phases. Then, it is necessary to simulate the estimation of different unknown phases to calculate the fitness. After each step in the simulation, the feedback phase Φ_k to be applied at k^{th} step, is updated according to the following logarithmic-search heuristic [569, 570]:

$$\Phi_k = \Phi_{k-1} - (-1)^{x_{k-1}} \boldsymbol{\Delta\Phi}_k, \tag{3.52}$$

where $x_{k-1} \in \{0, 1\}$ is the dichotomous outcome of the measurement at $(k-1)^{\text{th}}$ step. In this approach the estimator ϕ_{est} for the unknown phase ϕ is provided, up to a constant phase, by the last value Φ_N of the feedback phase, updated after the last measurement result [569]. The fitness S of a policy $\boldsymbol{\Delta\Phi}$, is given by $S(\boldsymbol{\Delta\Phi}) = |\int_{-\pi}^{\pi} p(\theta|\boldsymbol{\Delta\Phi}) e^{\imath\theta} d\theta|$, where $\theta = \phi_{\text{est}} - \phi$ is the error on the estimated value of the phase, and $p(\theta|\boldsymbol{\Delta\Phi})$ is the probability of the error θ using the policy $\boldsymbol{\Delta\Phi}$ in the estimation. Such quantity is computed averaging over 10^5 values of unknown phases, uniformly drawn in the interval $[0, \pi]$. The chosen figure of merit to be minimized during the phase estimation problem is the Holevo variance V^H, that is related to the fitness function as follows [Eq. (3.27)]:

$$V^H = S(\boldsymbol{\Delta\Phi})^{-2} - 1. \tag{3.53}$$

Genetic Operators

The initial population is improved through an iterative process of genetic operations applied on the individual solutions of the population. The fitness score assigned to the individuals determines the best element of the population and also the halting criteria of the optimization process. Three genetic operators, namely Selection, Crossover and Mutation are applied to the population during the iteration process. In particular, we employ the process of elitism among the individuals: certain individuals with a very high fitness are immune to the crossover and mutation techniques. This method ensures the survival of the best solutions of the previous generation into the new generation, creating a better mating pool for the next iteration, and preserving the quality of the best candidate solutions. Our algorithm uses a population size of 12 individuals, with a single elite solution immune to changes during each generation.

Selection. In each consecutive iteration, an appropriate number of pairs of individuals, the parents, are selected to reproduce and form the new generation. The parents are selected through a method where the solutions with higher fitness have a better chance to be extracted for the mating process. A selection technique could select the two individuals with highest fitness, but this voids the use of genetic diversity which is the basis of evolution. This would also restrict the search for a particular bias, which could get stuck in a local minima. The selection technique used here is the Tournament Selection method [678] (see Algorithm 1). In particular, it corresponds to running numerous tournaments among the individuals in a randomly

chosen subset of the population. The victor is determined by the fitness value, and is selected for mating. A large number of tournaments ensures the selection of almost every individual in the randomly chosen subset at least once, creating the possibility of existence of weak and strong individuals together in a given generated subset. This selection technique also maintains the diversity in the genomes during the crossover process by mixing the good genes of parents with the weaker parents, thus ensuring the survival of the fittest along with the selection of a very small proportion of weaker individuals. We use a tournament selection size of 5 solutions, which is the size of the subset of the total population composed of 12 candidate solutions. The selection technique returns the best individual from the 5 randomly chosen individuals. The selection is then exploited different times to extract pairs of individuals used to generate new children chromosome through the process of crossover.

Algorithm 1: Tournament Selection (P, τ)

Input: A population P containing a set of individuals $P := \{i_1, i_2 \ldots, i_n\}$;
Tournament size: τ
Output: Selected individual $i_x \in P$, $x \in \{1, 2 \ldots, n\}$

```
P' ← Initialize empty population
for k ← 1 to τ do
    j ← random Int (between 1 and n);
    Insert i_j into P'
end
Sort P' in decreasing order of fitness of i, ∀i ∈ P';
return Fittest individual from P';
```

Crossover. Analogously to the crossover that happens during the biological reproduction, the newly generated offspring of the parent solutions share genetic information belonging to its parents. We select two parents by repeating the selection process two times, which then proceeds to generate one offspring solution. The crossover process used in our problem is the uniform crossover technique, in which each element of the new chromosome (gene) is randomly chosen from one of the two parents with equal probability. This spreads out the genetic information evenly among the genes of the offspring, ensuring equal contribution from both the parents. This also ensures the exploitation, or the preservation of better solutions. The mating process is repeated with the selection of other pairs of parents, and their crossover to produce other offspring until a new population generation with the suitable size is produced. In our case, a size of 12 individuals has been employed. The elite chromosomes are immune to crossover, that is, they are the only solutions not replaced by the new generated child solutions. However, elite chromosomes can take part in the mating process as parents.

Mutation and Halting. The newly generated children solutions then proceed to be subjected to the mutation operator. Mutation alters the genetic information in the individuals from its initial state, modifying the solution from the previous one. In our algorithm, chromosomes $\mathbf{\Delta\Phi}$ with higher fitness values $S(\mathbf{\Delta\Phi})$ have more immunity to the mutation process. In particular, the mutation probability of each gene of a chromosome is equal to $0.55[1 - S(\mathbf{\Delta\Phi})]$. This rule has been chosen in order to save the fitter individuals from mutation and expose the weaker or less fit chromosomes to it, ensuring the increase in genetic diversity as well as preventing the good solutions from alterations. The number 0.55 signifies the rate of mutation, and has been chosen using trial and error methods for better exploration of the

search space when the algorithm reaches saturation near local minima. Every i^{th} gene is mutated by changing the value of the original gene to a value drawn from a Gaussian distribution with mean equal to the original gene, and with variance equal to $1/i$, where i represents the position of the gene in the chromosome vector. This mutation variance follows the intuition that, increasing the number of probes, the difference of feedback phase decreases approximately like SQL. Indeed as the number of probes increases, the necessary variation around the corresponding gene to find the optimal solution is expected to be smaller. During the mutation, we also introduce an infected individual, that is, a randomly created chromosome, in place of one of the two worse individuals. When the number N of photons is less than 25, such infection process happens with a probability of 0.25, otherwise for $N \geqslant 25$ the probability of infection is $N/100$. In this way the infection ensures a proper random exploration of the search space, maintaining the genetic diversity in the mating pool for the succeeding generations. The new generation, produced through the application of these genetic operators, commonly has an increased average fitness value. The whole described processes of selection, crossover, mutation and infection are repeated in a cycle until a halting criterion is fulfilled. The halting criterion of the algorithm is the attainment of a threshold fitness value approximately equal to the SQL for the respective value of N, or when the number of generations exceeds a fixed limit. In the latter case the fitness value can be far from SQL and thus the algorithm fails to reach a value near to the bound.

In Table 3.4 are reported the values of all the relevant parameters employed for the GA algorithm.

Algorithm 2: Genetic algorithm (M, n, χ, μ, β)

Input: Number of generations after which the evolution is halted: M; Size of the population: n; Number of elite individuals immune to evolution: χ; Infection rate: β; Mutation rate: μ; Threshold fitness value: F_T

Output: Optimized solution having fitness near threshold value

// Initialize generation 0: ;
$k \leftarrow 0$;
$P_k \leftarrow$ a population of n randomly-generated individuals;
// Evaluate P_k:
Compute *Fitness*(i), $\forall i \in P_k$;
Sort P_k in decreasing order of fitness of i, $\forall i \in P_k$;
while *Fitness(first individual* $\in P_k$*)* $\sim F_T$ *or* $k > M$ **do**
    // 1. Copy Elites:
    for $i \leftarrow 1$ ***to*** χ **do**
        Insert i into P_{k+1}, $\forall i \in P_k$;
    end
    // 2. Crossover:
    for *iterator* $\leftarrow \chi + 1$ ***to*** n **do**
        Select $i, j \in P_k$ using **Tournament selection**;
        Create empty individual q;
        for *geneindex* $\leftarrow$ *Length of* i *(or* j*)* **do**
            $x \leftarrow$ random Boolean;
            if x *is True* **then**
                Insert gene value from i into q;
            else
                Insert gene value from j into q;
            end
        end
        Insert q into P_{k+1};
    end
    // 3. Mutate and Infect:
    for $i \leftarrow \chi + 1$ ***to*** n **do**
        $y1 \leftarrow$ random Float (between 0 and 1);
        if $y1 < \mu$ **then**
            $y2 \leftarrow$ random Float (between 0 and 1);
            if $y2 < 1 - $*Fitness*($i$), $i \in P_{k+1}$ **then**
                $i_x \leftarrow i_x +$ random number from gauss distribution around i_x, $\forall i_x \in i$, $i \in P_{k+1}$;
            end
        end
        if $i = n - 2$, $i \in P_{k+1}$ **then**
            $y3 \leftarrow$ random Float (between 0 and 1);
            if $y3 < \beta$ **then**
                $i \leftarrow$ Re-initialize with random values, $i \in P_{k+1}$;
            end
        end
    end
    // Evaluate P_{k+1}:
    Compute *Fitness*(i), $\forall i \in P_{k+1}$;
    Sort P_{k+1} in decreasing order of fitness of i, $\forall i \in P_{k+1}$;
    $k \leftarrow k + 1$;
end
return *Fittest individual from* P_k;

Parameter	Value
No. of averaged phases for Fitness calculation	10000
Population size	12
Mutation rate	0.55
Infection rate	0.25 for $N < 25$, else $N/100$
No. of Elite chromosomes	1
Tournament Selection size	5

Table 3.4. Parameters employed for the GA. List of all parameters value for the adaptive estimation algorithm based on a GA approach.

Numerical simulations of algorithm performances

In this section, we perform numerical simulation to study the optimal policies generated by our GA algorithm for phase estimation. We consider values of probes numbers N ranging from 1 to 80. In Fig. 3.25a we report the average of V^H obtained by the estimation of 10^5 uniformly distributed unknown phases, showing that the SQL is attained after small values of N. Furthermore, the inset focuses on different distant values of N independently, and demonstrates in both cases a good convergence to every unknown phase. Fig. 3.25b shows the results of estimations at each independently optimized N-policy, obtained for two different values of unknown phases. Performances of the policies are studied in terms of Holevo variance V^H scaling as function of N. These results show the high efficiency of the algorithm even if a small number of resources is used. In particular, the scaling of V^H shows

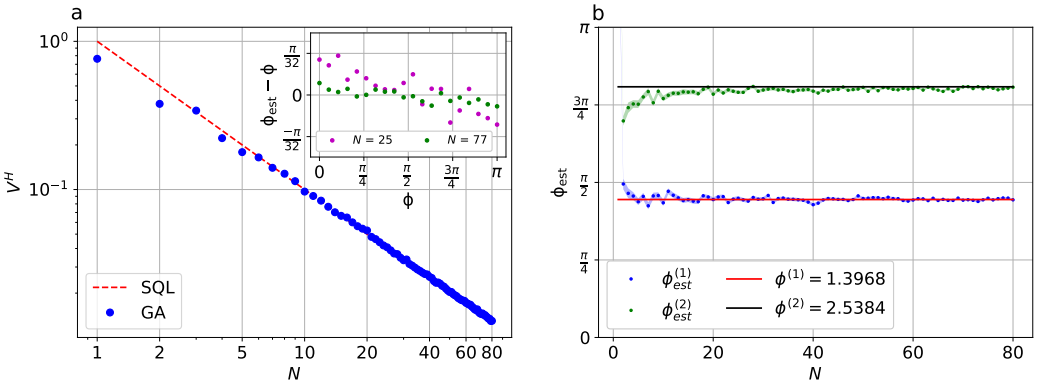

Figure 3.25. Numerical results. Performances of the learning protocol using policies optimized by GA algorithm for different number N of input photons. **a**, Comparison between SQL (red dashed line) and the Holevo variance V^H obtained by simulations (blue dots), averaged over 10^5 phases in the interval $[0, \pi]$. GA searching finds different optimal feedback strategies for different values of N. The inset graph shows the difference between simulated value of estimated phase ϕ_{est} and the actual phase value ϕ, reported as a function of ϕ. Here, results show same performances for two distant values of N: $N = 25$ and $N = 77$. **b**, Numerical phase estimation of two different phases $\phi^{(i)}$ $(i = 1, 2)$ as function of N adopted probes. The estimated phase value $\phi_{\text{est}}^{(i)}$ (dot) converges to the true phase value (solid line) in a few number of probes. Each dot is averaged over 100 independent experiments, and its error (color filled area) is computed by normalizing the variance to the number of experiments. This image is taken from [17].

the high quality of optimal solutions found by GA research, by which the estimation process reaches the true values of the unknown phases. The value of V^H for $N < 5$ lower than SQL depends on the fact that the algorithm is optimized for phases lying in the interval $[0, \pi]$. Conversely for greater N, the SQL retains its role as a suitable limit on the estimation precision. In the optical system under analysis, the algorithm finds that the optimal feedbacks are those where the relative phase shift $\phi - \Phi$ between the two modes of the MZI is $\pi/2$, which corresponds to the point in which the likelihood function has a maximum of the derivative modulus.

These numerical evidences demonstrate the effectiveness of the offline policies found by GA optimization, able to optimally estimate unknown phases with sensitivities that reach SQL after few data.

Experimental Results

We experimentally tested the GA approach to estimate unknown relative phase shifts inside a MZI injected by single photons. The employed apparatus (Fig. 3.23b) is a MZI in the polarization degree of freedom, where the optical phase to be estimated is a relative one between the vertical (V) and horizontal (H) polarizations of the photon. Photons are generated by injecting a $\lambda = 404$nm continuous wave pump beam in a periodically poled potassium titanyl phosphate (PPKTP). Through the SPDC process inside the crystal, two degenerate photons with $\lambda = 808$nm are generated. One photon of each pair is sent directly to the trigger avalanche photo-diode (APD), while the other one is employed for the phase estimation process after its polarization state is prepared through a polarizing beam splitter (PBS). The interferometer is composed of two half-waveplates (HWPs) rotated by 22.5° and two adjacent liquid crystals (LCs) interposed between the HWPs. The first LC controls the unknown phase shift ϕ and the second one acts as feedback phase Φ. After the second HWP, a final PBS separates H and V polarizations in two different spatial modes that are measured by two APDs. The complete process is automatically controlled by a dedicated software. In particular, all three APDs are connected to an electronic system that reads all the single-photon counts and provides digital timestamps to the computer. Through an analysis of such timestamps, two-fold coincidences between trigger and one of the two measurement detectors are recorded by choosing a coincidence window of 3 ns. The first coincidence recorded within a fixed amount of time of 0.5 s generates the single event used in the estimation process. After each recorded event, the processing unit recovers the feedback phase to be applied from the pre-calculated list, and consequently drives the corresponding LC. An additional time interval of 0.3 s between two consecutive events is inserted due to the switching time of LC. In this way, all steps of the experiments, including phase tuning, photon detection and application of the GA policies, are controlled by the processing unit.

The apparatus described above has been employed to perform the estimation of different phases. Experimental results are shown in Fig. 3.26a, for different phases between 0 and π. Each point, at fixed N, is an average of 100 estimates using the optimal policy for that N. The results show that the estimation reaches the true values of the phases after a few photons (~ 25). While in an ideal MZI the Fisher Information does not depend on the phase $\phi_{\text{tot}} = \phi - \Phi$, the presence of experimental imperfection may cause the bound to be phase-related (see Fig. 3.26b) which is observed when non-adaptive strategies are employed. This different behavior can be predicted by taking into account the effect of noise in calculation of the likelihood function of the system. More specifically, our apparatus is characterized

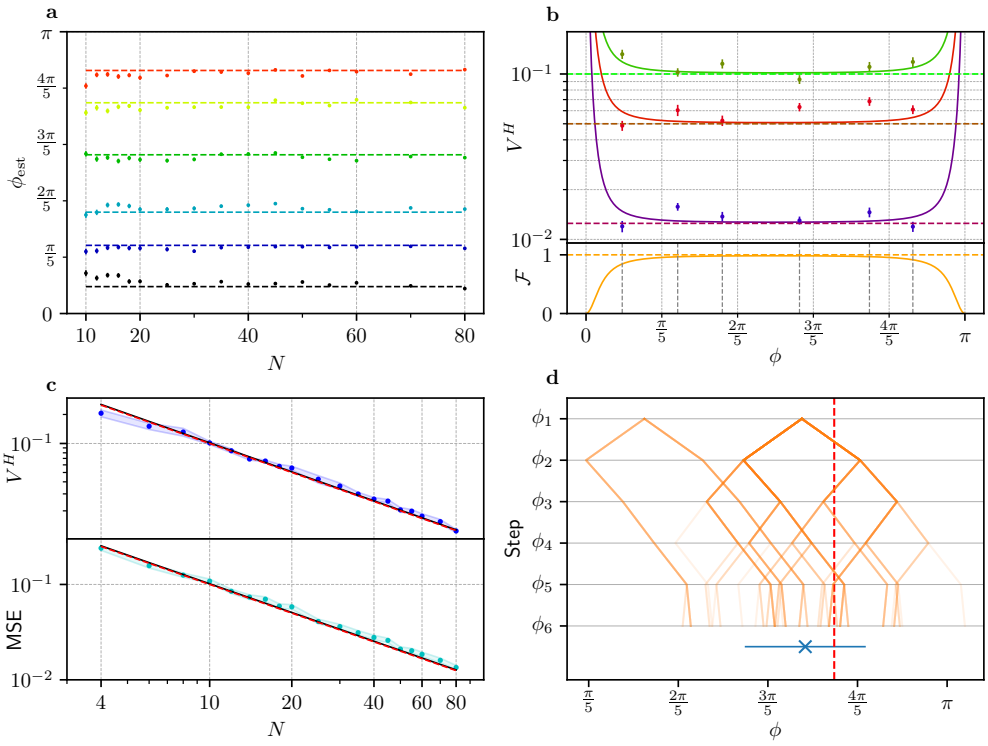

Figure 3.26. Experimental results. Six different phases have been estimated 100 independent times, using adaptive GA protocols. **a**, Estimation of different phases as a function of the number of photons N. Dashed lines are the real applied unknown phase shifts, while dots represent the circular mean of the repetitions with same N. **b**, Top: Holevo Variance (V^H) as function of the phase for three different values of N: $N = 10$ (green dots), $N = 20$ (red dots) and $N = 80$ (blue dots). Straight lines are ideal bounds, while dashed ones represent the bounds corrected by depolarizing noise, considering $p_{\text{exp}} = (7.93 \pm 0.16) \times 10^{-3}$ (see main text). Bottom: Fisher information as a function of the phase. Orange solid line represents the experimental information, while orange dashed line represents the ideal case. **c**, Holevo variance V^H and mean square error, MSE, as function of the number N of exploited photons. Blue (cyan) dots are the mean value of V^H (MSE) over the six different phases. Filled band represents the confidence interval inside the standard deviation. The red line is the ideal SQL, the black dotted line instead is the minimum over all ϕ of SQL in presence of noise. **d**, Example of experimental decision tree. Values of the feedback phases employed during the estimation process of the phase $\phi = 2.35$, using the first $N = 6$ single photons. For any process, after each photon measurement, the feedback phase is updated according to the rule in Eq. (3.52), realizing a branch of the tree. Red dashed line represents the real value of ϕ, while the orange branches of the tree are 100 independent processes of estimation. The intensity of the colour is proportional to the number of times the estimation follows that branch. The blue cross is the final mean of all estimations: $\phi_{\text{est}} = 2.15 \pm 0.42$. This image is taken from [17].

by a non-unitary visibility of the polarization fringe pattern. This effect can be expressed by correcting the likelihood function with a parameter $p \in [0, 1]$, related to the visibility as $V = (1 - p) \neq 1$, leading to the following output probabilities:

$$\mathrm{P}_0 = 1 - \mathrm{P}_1 = (1 - p)\cos^2\left(\frac{\phi - \Phi}{2}\right) + p/2 \tag{3.54}$$

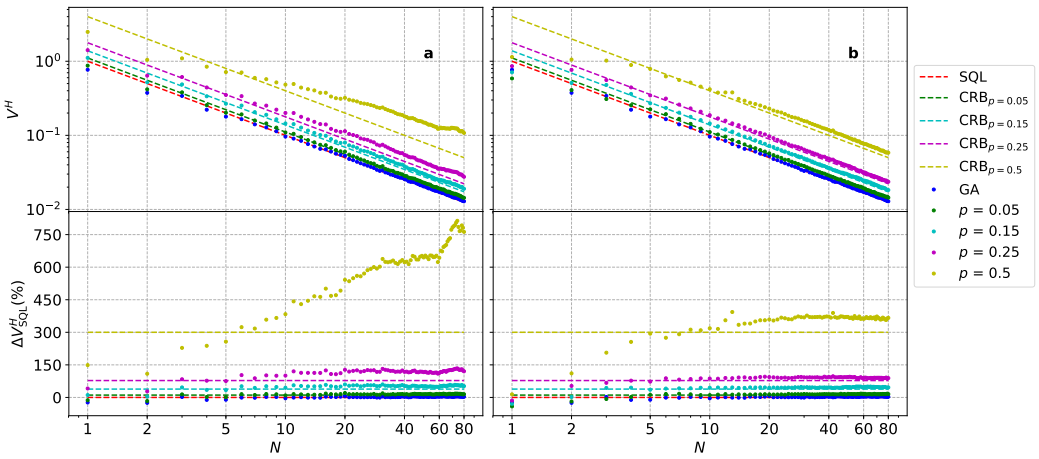

Figure 3.27. Robustness to depolarizing noise. Numerical analysis of GA protocol performances in terms of Holevo variance V^H (top panels), for different values of depolarizing noise parameter $p = 0, 0.05, 0.15, 0.25, 0.5$. When N probes are adopted, the dependence on p of the achievable precision CRB_p can be computed by considering the noisy likelihood in calculation of $\mathcal{F}^{-1}_{\mathrm{exp}}(\phi, p)$. The applied policies to the noisy scenario can be calculated via the GA approach by taking into account (right panel **b**) or not (left panel **a**) the noise model. In the bottom panels, we report an equivalent representation in terms of the ratio $\Delta V^H_{\mathrm{SQL}} = (V^H - \mathrm{SQL})/\mathrm{SQL}$. This image is taken from [17].

Where P_0 (P_1) is the probability to find the photons with polarization H (V). By measuring the output probabilities, we characterized both the phase shifts associated to the voltages applied to the LCs, and the experimental likelihood function, obtaining the following estimate for p: $p_{\mathrm{exp}} = (7.93 \pm 0.16) \times 10^{-3}$. The noisy likelihood is associated with a different Fisher Information $\mathcal{F}^{-1}_{\mathrm{exp}}(\phi)$, which leads to different limits on precision for the experimental apparatus, as shown in Fig. 3.26b. The difference with the ideal noiseless case becomes significant at the edges of the $[0, \pi]$ interval. Since the sensitivity depends on the value of the unknown phase, different phases would be estimated with different precision if non-adaptive techniques are employed. Conversely, adaptive strategies allow us to obtain a phase-independent behavior for the estimation error. Indeed, the feedback phase is adjusted throughout the protocol by the adaptive strategy to exploit the most informative points of the likelihood. In this way, we observe a phase-independent behavior as shown in Fig. 3.26b, where the sensitivities achieve the optimal CRB $\min_\phi \mathcal{F}^{-1}_{\mathrm{exp}}/N \simeq 1.016/N$ obtained from experimental probabilities (see for instance the case $N = 80$ in Fig. 3.26b). As a result, the error of the estimations, shown in Fig. 3.26c, quickly approaches the SQL as a function of N. In our analysis we consider as figures of merit not only the averaged Holevo variance V^H over the M measured phases (blue dots), but also the circular-MSE (cyan dots), which is defined as:

$$\mathrm{MSE}(\phi) = \sum_{k=1}^{M} (\arg[e^{i(\phi - \phi^{(k)}_{\mathrm{est}})}])^2 / M. \tag{3.55}$$

Finally, in Fig. 3.26d we show how the algorithm works in terms of policies applied. Then, after sending and measuring each photon, the feedback phase is updated depending on the outcome according to Eq. (3.52). The feedback phase shifts are the optimal ones provided by GA protocol. At each step there are 2

possible outcome values, and the estimation generates a branch. Among all 2^N possible branches relative to each estimation, only the ones observed during the experiment are represented, with intensity proportional to the number of times a given path is followed. In general the change in the feedback phase, that is, the policy, decreases with the step number, meaning an increasing precision of estimation. Finally, the comparison between the unknown phase and the resulting estimation is reported, together with its circular variance over all 100 independent runs.

Robustness to noise

We perform some numerical simulations to study the robustness of the policies generated by our genetic algorithm against different sources of noise. In particular we consider depolarizing and phase errors, which are two of the most common noise models in interferometric setups.

Depolarizing noise is caused by the presence of dark counts or by the limited visibility of the interferometer. This effect is introduced in the simulations via an additional parameter p, which gives the probability of a random click. In this way, the simulated data are drawn by a noisy likelihood distribution having the following form: $P_{\text{noisy}}(x) = (1-p)P(x) + p/2$, where $x = 0, 1$ are the measurement outcomes and $P(x)$ is the probability in noiseless condition. This kind of noise has been considered to describe the experimental results of the previous section. We now analyze numerically the robustness of the policies generated by our GA approach. More specifically, the policies are calculated by assuming a noiseless experiment ($p = 0$) and applied to a noisy estimation process ($p \neq 0$), where we considered different noise levels corresponding to $p = 0.05, 0.15, 0.25$ and 0.5. This analysis is performed to quantify the robustness of policies, generated using an ideal model, in noisy conditions. The results of the simulations are reported in Fig. 3.34a. These data show that the policies are robust against noises with $p \leq 0.25$ even if they are trained with ideal conditions. This implies that this technique can be employed also in systems with moderate unknown values of depolarizing noise without losing the capability to reach the ultimate limit provided by the CRB. More specifically the CRB of the optimal point in a depolarizing noisy interferometer, using single photons, is equal to: $\text{CRB}_p = 1/[N(1-p)^2]$. For larger p, the policies fail to reach the sensitivity bounds.

As a second step, we consider the scenario in which the noise parameter is calibrated before the experiment. In this case, the GA approach can be adapted to generate policies optimized for this scenario by taking into account the actual noise level during the computation. Hence, we generated policies using knowledge of the depolarizing noise parameter. The analysis of the estimation of unknown phase shifts using policies trained in the presence of noises is shown in Fig. 3.34b. Here, as expected, the performances of the estimation processes are improved when compared with those achieved with the policies for $p = 0$. In particular, the optimal CRB associated with each noise is approached by the estimations using noisy policies. Such improvement is larger for increasing values of p. Note that, for large values of noise ($p = 0.5$), a difference with the CRB is still obtained, which is to be attributed to the probabilistic feature of genetic algorithms which may fail to reach convergence in a given number of iterations. In conclusion, our protocol is not only robust against depolarizing noise, but can also be adapted to approach the ultimate bound in such noisy conditions.

Finally, we considered the effect of phase noise, due to random errors in setting the feedback phase. For instance, this can be attributed to random imperfections in

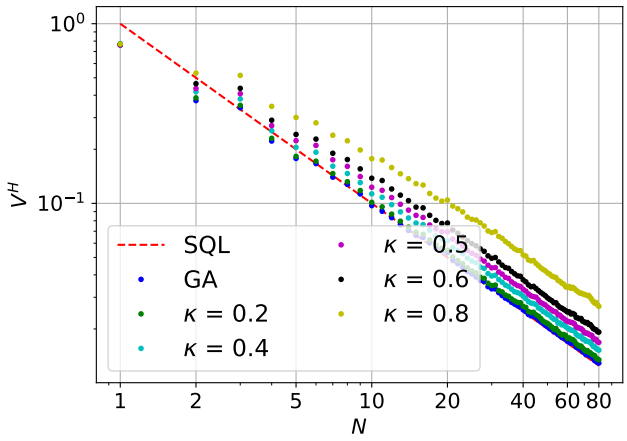

Figure 3.28. Robustness to phase noise. Plot of Holevo variance V_H as function of the number N of photon probes, in the presence of phase noise for $\kappa = 0.2, 0.4, 0.5, 0.6$ and 0.8. Simulations are performed by using the policies calculated in absence of noise, applied to noisy simulated phase estimation processes. More specifically, A random shift around the feedback phase is added at each step of the experiment, according to the normal distribution around the original value with variance κ^2. Results for different noise intensities are compared with the noiseless case (dark blue dots) and the SQL (red dashed line). Each shown acquisition is averaged over 100 simulated rounds of the estimation process. The distance of the achievable precision from the SQL becomes significant only for high value of the noise. This image is taken from [17].

the phase control or to phase fluctuations between the arms of the interferometer. We have numerically simulated phase estimation processes under this noise by altering the value of the feedback phase Φ_k by an amount $\delta\Phi$. Such amount is randomly generated at each step according to a normal distribution with mean equal to the original value, and standard deviation described by the parameter κ. In these conditions, we test the policies calculated for a noiseless scenario. The results of the simulated estimation processes for different values of the parameter κ are shown in Fig. 3.28. We observe that the policies generated via GA are robust to this kind of error, even for a considerable amount of phase noise with $\kappa \leq 0.6$.

Conclusions and perspectives

In this work we presented a novel technique based on a genetic algorithm, able to find optimal feedback actions for single phase estimations, that are also robust against different sources of noises. We then performed an experimental demonstration of such protocol through a photonic platform showing fast convergence of the estimation error to the ultimate limits after few probes. Such demonstration opens the way to further applications in Quantum Metrology tasks with limited data. Future steps will require to devise and test experimentally such class of algorithms with different probes enabling quantum-enhanced performances. Even the study of photonic realization of probes states can be improved by GA algorithms [639, 630, 633], giving rise to accessible and robust-to-noise states for metrology tasks. Then, a natural generalization of this approach is to apply GA optimization for offline protocols in multiparameter Quantum Metrology problems [427, 428, 14, 1], with particular attention to the limited data regime [679]. While online adaptive Bayesian techniques for multiphase estimation were demonstrated [15], offline solutions have

still to be explored and GA promises to be a useful tool for this task. Notably, this kind of approach can be applied to other quantum information tasks, in which an optimization of multiple feedbacks is needed.

3.3.2 Two-phase estimation in an integrated three-mode MZI

Multiparameter estimation is a fundamental problem for the realization of realistic quantum sensors in several scenarios [427, 428, 1]. In this task, there are still several open problems and a comprehensive framework has yet to be defined. For instance no general strategies are available for the construction of optimal probes and measurements in different multiparameter scenarios. While a general framework for Bayesian quantum multiparameter estimation exists [435], there are several remaining open questions. In particular, the operational application of optimal strategies, measurements and probes preparation, is a field that needs to be largely explored, even if some theoretical results are available also in the limited data regime [671]. Furthermore, further progresses are still required on the technological platforms towards reaching unconditional violation of the standard quantum limit [680] in complex sensors. Hence, it is crucial to identify an experimental platform versatile enough to address different possible approaches. Multiphase estimation provides an ideal scenario with different practical applications. Furthermore, it represents a testbed for different multiparameter estimation protocols. Applying these to real world scenarios requires a further step, that is, the optimization of the available resources, so as to attain the minimum reachable uncertainties after a sufficiently small number of measurements. This can be achieved by implementing adaptive strategies. In the limited data scenario, theoretical works have shown the number of required resources to saturate the lower bounds [664, 671], but the multiparameter experimental counterpart still lacks its investigation. Therefore, the study of adaptive strategies in single phase estimation is as important as in the more general scenario involving multiple phases. Also here, it is crucial to identify and test experimentally protocols to saturate the ultimate bounds with a very limited number of probes. Integrated multiarm interferometers are suitable for achieving this goal, as they can perform simultaneous estimation of multiple phases. Indeed, such platform guarantees high phase stability for each optical phase and the easy scalability of the number of involved parameters. Then, the other fundamental resource is represented by the possibility to tune the device, in order to allow the adaptive change of the apparatus. For all these reasons we employed a similar device for adaptively estimating two optical phases, which has the same structure of the one presented in Sec. 3.2.1.

In the following sections, we provide a brief introduction to the general Bayesian multiparameter framework for adaptive estimation. Then, the particular multiphase estimation scenario is shown, by focusing on our two-phase estimation problem. Finally, the study of the adaptive algorithm and experimental results of its implementation are reported [15].

Bayesian multiparameter estimation

In multiparameter estimation, the aim is to measure simultaneously an unknown set of parameters $\mathbf{x} = (x_1, \dots, x_n)$ reaching the maximum precision allowed by the amount of resources employed in the process (Sec. 3.1). In general, the set of parameters is encoded within the evolution of a system, either described through a unitary operator $U_{\mathbf{x}}$ or a more general map $\mathcal{L}_{\mathbf{x}}$. The value of the unknown parameters $\mathbf{x}$ can be estimated by preparing a suitable probe state ρ and sending it to evolve throughout the system. Information on the unknown parameters can be retrieved by measuring the output state $\rho_{\mathbf{x}}$ with a set of measurement operators $\{\Pi_d\}$, where $d = 1, \dots, m$ represents the number of possible outcomes. Such process is then repeated N times to improve precision in the estimation process. After N probes have been prepared and measured, the obtained sequence of measurement outcomes $\mathbf{d} = (d_1, \dots, d_N)$ has to be converted in a set of parameters estimates $\hat{\mathbf{x}}$ through a suitably chosen function $\hat{\mathbf{x}} = \hat{\mathbf{x}}(d_1, \dots, d_N)$. As discussed in Sec. 3.1.2.2, a possible choice of estimator is provided by Bayesian protocols [478, 681, 490, 495]. This class of estimators is based on encoding the initial knowledge on the parameters in a probability function $p(\mathbf{x})$, called prior distribution, which is updated according to the Bayes rule at each step of the estimation protocol. The posterior distribution after N probes reads $p(\mathbf{x}|\mathbf{d}) = \mathcal{N}^{-1} p(\mathbf{d}|\mathbf{x}) p(\mathbf{x})$, where $p(\mathbf{d}|\mathbf{x})$ is the likelihood function of the system expressing the conditional probability of obtaining the measurement sequence $\mathbf{d}$ for given values of the parameters $\mathbf{x}$, and $\mathcal{N}$ is a normalization constant. Then, the mean of the posterior distribution can be exploited as the estimate of the unknown parameters $\hat{x}_i = \int x_i p(\mathbf{x}|\mathbf{d}) \prod_i dx_i$. Bayesian protocols present several important properties. In particular, it can be shown that such approach is asymptotically unbiased, meaning that the estimated values converge to the true values when N is large enough. This is related to the quadratic loss $L(\mathbf{x}, \hat{\mathbf{x}}; \tilde{\mathbf{w}}) = \sum_i \tilde{w}_i (x_i - \hat{x}_i)^2$, whose average value over all measurement sequences $\mathbf{d}$ is commonly employed as a figure of merit to quantify the convergence of the estimation process. The average of posterior distribution is the optimal estimator for minimizing this figure of merit [1, 496, 490]. The coefficients $\tilde{w}_i$ can be chosen to reflect different weights between the parameters, while for equally relevant parameters they can be set as $\tilde{w}_i = 1$. Hereafter, we will consider this latter scenario and thus define the quadratic loss as $L(\mathbf{x}, \hat{\mathbf{x}}) = \sum_i (x_i - \hat{x}_i)^2$. Furthermore, in a Bayesian framework the posterior distribution also provides a confidence region for the parameters estimates, which is represented by the covariance matrix $\mathrm{Cov}(\hat{\mathbf{x}})$ of $p(\mathbf{x}|\mathbf{d})$. This figure of merit is obtained for each single estimation experiment composed of a sequence of N probes, and has no counterpart in frequentist approaches [496]. In general, Bayesian bounds for both the quadratic loss and the covariance matrix depend on the amount of a-priori knowledge $p(\mathbf{x})$ available [496, 664, 553, 671]. Asymptotically for large values of N, corresponding to the regime where the amount of information acquired in the estimation process far exceeds the a priori knowledge, the covariance matrix satisfies the Cramér-Rao inequality [Eq. (3.9)]. In the considered case the CRB reads $\mathrm{Cov}(\mathbf{x}) \geq \mathcal{F}^{-1}/N$, where $\mathcal{F}$ is the Fisher information matrix [682] and thus $\mathcal{F}^{-1}$ corresponds to its inverse. Such quantity also provides an asymptotic bound for the quadratic loss as $L(\mathbf{x}, \hat{\mathbf{x}}) \geq \mathrm{Tr}[\mathcal{F}^{-1}]/N$.

Adaptive protocols can be employed when, besides the set of unknown parameters $\mathbf{x}$, the user has access to an additional set of control parameters $\mathbf{c} = (c_1, \dots, c_l)$ that can be changed throughout the estimation process (Sec. 3.1.4). More specifically, after each of the N probes is sent and measured, the acquired knowledge is employed to change the values of $\mathbf{c}$ for the next probe to maximize the extraction of information

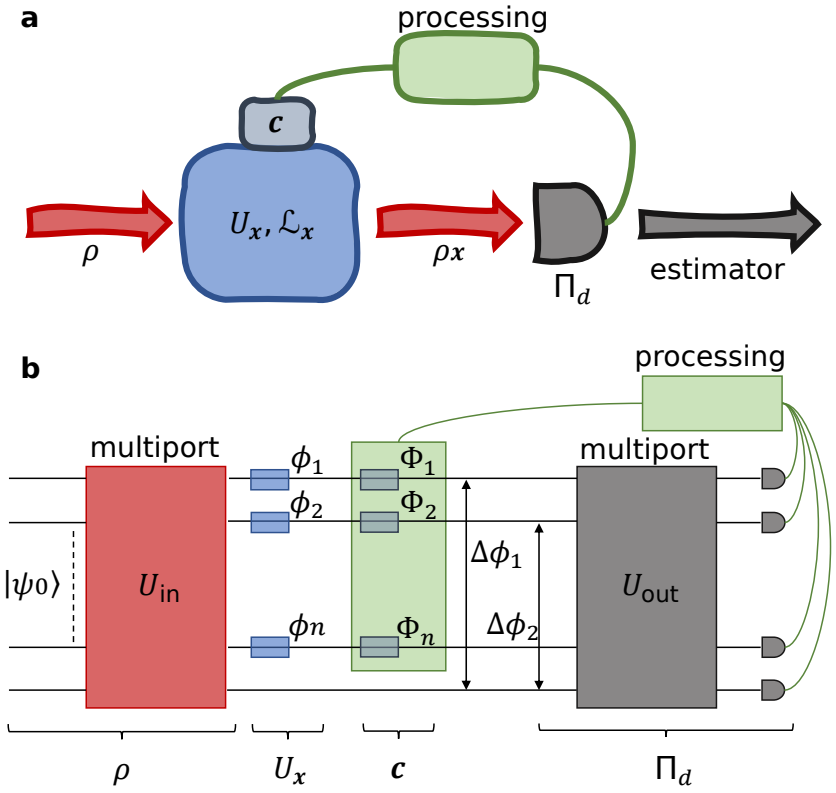

Figure 3.29. Schemes of adaptive estimation. **a**, General layout of an adaptive multiparameter estimation protocol. A sequence of probes ρ are sent to estimate the parameters $\mathbf{x}$. At each step the results of the measurement Π_d and the current knowledge on $\mathbf{x}$ are employed to optimize the control parameters $\mathbf{c}$. **b**, Multiarm interferometer for multiphase estimation. An m-mode interferometer embeds $n = m - 1$ unknown phase shifts $\boldsymbol{\phi}$, while additional controlled phases $\boldsymbol{\Phi}$ can be employed for adaptive protocols. This image is taken from [15].

in the subsequent measurement. Within a Bayesian framework, such knowledge is encoded in the posterior distribution. Hence, after each step of the estimation protocol, the user can decide the values of the control parameters $\mathbf{c}$ starting from $p(\mathbf{x}|\{\mathbf{c}\}, \mathbf{d})$ (see Fig. 3.29a). Considering the presence of these tunable control parameters during the estimation process, the likelihood after N probes reads $p(\mathbf{d}|\mathbf{x}, \{\mathbf{c}\}) = \prod_{i=1}^{N} p(d_i|\mathbf{x}, \mathbf{c}_i)$, where d_i is the measurement result of the probe i after application of control values $\mathbf{c}_i$. Therefore, the Bayes rule for updating posterior distribution becomes $p(\mathbf{x}|\{\mathbf{c}\}, \mathbf{d}) \propto p(\mathbf{d}|\mathbf{x}, \{\mathbf{c}\})p(\mathbf{x})$, where $p(\mathbf{x})$ does not depend on $\{\mathbf{c}\}$, as control phases have no role in the prior knowledge. Adaptive protocols represent a relevant tool in phase estimation process. Indeed, the adoption of adaptive strategies becomes a crucial requirement even in the single-parameter case to optimize the algorithm performances [544, 491, 583, 569, 584, 394, 571, 595, 596, 597, 17], with the aim of achieving the ultimate bounds provided by the Cramér-Rao inequality for small values of N [597]. Furthermore, in more complex systems characterized by a phase-dependent Fisher information matrix, adaptive strategies become crucial to reach equal performances for all values of the unknown parameter(s) [527]. Indeed, in several scenarios the quantum Cramér-Rao bound, namely the ultimate precision for a given probe, is parameter-independent. However, construction of the optimal

measurement for its saturation requires in general significant a-priori knowledge on the parameter(s) since it can be defined in a local estimation framework [485, 482]. Thus, in a scenario where limited or no a-priori knowledge on the parameter is available, and limited resources can be employed, adaptive protocols represent a powerful tool.

Adaptive protocols for multiarm interferometers

Given the general scenario described in the previous section, it is crucial to identify and test experimentally protocols to saturate the ultimate bounds with a very limited number of probes. In this context, multiarm interferometers represent a benchmark platform to perform simultaneous estimation of multiple phases. The platform is schematically shown in Fig. 3.29b, and represents the m-mode generalization of a Mach-Zehnder interferometer in the multimode regime [613, 683, 518, 14]. More specifically, it is composed by a sequence of a first multiport splitter, employed to prepare the probe state, a series of phase shifts between all the optical modes, and a second multiport splitter which defines the output measurement. Both multiport splitters can be in principle designed according to appropriate decompositions [615, 684] to implement any linear unitary transformation. The internal phase shifts can be divided in two layers. The first one $\boldsymbol{\phi} = (\phi_1, \ldots, \phi_n)$ corresponds to the unknown parameters to be measured, while the second one $\boldsymbol{\Phi} = (\Phi_1, \ldots, \Phi_n)$ takes the role of the control parameters for adaptive estimation; we note that in our implementation the number of controls is $l = n$. Here, $n = m - 1$ is the number of independent parameters, since one of the phases is considered as the reference mode. Both the unknown parameters and the control ones contribute to the overall phase differences $\boldsymbol{\Delta\phi} = (\Delta\phi_1, \ldots, \Delta\phi_n)$ within the interferometer.

We study different adaptive protocols for Bayesian learning of the unknown phases of this platform injected by a single-photon state, by focusing both theoretically and experimentally on the three-mode scenario ($m = 3$) with two independent parameters ($n = 2$). More specifically, we choose both for state preparation and state measurement transformation a balanced tritter described by unitary matrix U with $|U_{i,j}|^2 = 1/3$, $\forall(i,j)$ [523]. Injecting a single photon on input port 1 corresponds to generating a sequence of probe states of the form $|\psi_{\text{in}}\rangle = 3^{-1/2}(|1,0,0\rangle + |0,1,0\rangle + |0,0,1\rangle)$, which represents a single-photon state exiting in the balanced superposition of the three modes. The Fisher information matrix in this scenario shows a phase-dependent profile $\mathcal{F}(\Delta\phi_1, \Delta\phi_2)$, meaning that without adaptive strategies the asymptotic precision will be different depending on the actual phase values. In particular, by looking at the inverse of $\mathcal{F}$, we obtain $\min_{\Delta\phi_1,\Delta\phi_2} \text{Tr}(\mathcal{F}^{-1}) \simeq 3.866$, which is obtained for six different phase pairs $(\Delta\tilde{\phi}_1, \Delta\tilde{\phi}_2)$. For those pairs, minimum asymptotic quadratic loss is achieved. Note that, by using the results of Refs. [485, 482, 672], an optimal measurement can be in principle constructed saturating the quantum Cramér-Rao bound. For instance, for small values of the unknown phases a measurement including the projector over the initial state can be employed, thus requiring a-priori knowledge on the parameters or adoption of a large number of probes.

Bayesian protocols require in general expensive computational resources, due to the need of evaluating complex integrals to determine the normalization constant $\mathcal{N}$, as well as the estimated values and their corresponding covariance matrices. A possible solution is to perform a discretization of the parameters space, thus converting integrals to sums. In this case, the bin size has to be chosen depending on the minimum error expected at the end of the estimation process. However, such

solution becomes quickly unmanageable when the number of parameters increases, since such a discretization has to be performed in a n-dimensional space. A different solution has been explored in [394] for Bayesian learning problems by using a Sequential Monte Carlo (SMC) approach. Indeed, Monte Carlo methods seem to be a natural solution, due to their capability of reaching convergence independently from the integration space dimension. The SMC method approximates the infinite dimensional support $\boldsymbol{\phi}$ with a finite number M of elements $\boldsymbol{\phi}_i$, called particles, with associated probability weights w_i. The error in the approximation can be arbitrarily reduced by increasing the number of particles, leading to a trade-off between computational time and accuracy of the approximation. In the context of Bayesian analysis, any distribution $\tilde{p}(\boldsymbol{\phi})$ in the particles approximation is expressed as $\tilde{p}(\boldsymbol{\phi}) \approx \sum_{i=1}^{M} w_i \delta(\boldsymbol{\phi} - \boldsymbol{\phi}_i)$.

We now consider the case of an initial prior knowledge $p(\boldsymbol{\phi})$ corresponding to a uniform distribution. In the particles scenario, this prior information is approximated by a set of M randomly drawn pair of phases $\boldsymbol{\phi}_i$ with equal weights $w_i = 1/M$ to satisfy the normalization condition ($\sum_{i=1}^{M} w_i = 1$). During the experiment, the information about the unknown phases $\boldsymbol{\phi}$ is updated according to the Bayes rule after each measurement outcome d. In the particle approximation, having fixed control phases, this corresponds to updating the particle weights as $w_i \to w_i\, p(d|\boldsymbol{\phi}_i, \boldsymbol{\Phi})$, while keeping the particles $\{\boldsymbol{\phi}_i\}$ unchanged. The estimation of $\boldsymbol{\phi}$ is then provided by the expectation value of the posterior distribution $\hat{\boldsymbol{\phi}} = \int d\boldsymbol{\phi}\, \boldsymbol{\phi}\, p(\boldsymbol{\phi}|d, \boldsymbol{\Phi}) \approx \sum_{i=1}^{M} w_i \boldsymbol{\phi}_i$. As discussed in [394], the particle approximation needs some additional steps to avoid the introduction of further errors throughout the estimation process. In particular, after a few iterations the non-zero weights will be mostly concentrated on a small subset of $\{\boldsymbol{\phi}_i\}$, reducing the validity of the approximation. To avoid such effect, it is possible to employ resampling techniques [685]. More specifically, when the particle weights become too concentrated according to a given threshold condition, a new set of particles $\{\boldsymbol{\phi}'_i\}$ is generated by adding a small random perturbation to the original particles. The weights are then reset to $w'_i = 1/M$, and the estimation process restarts.

Within this framework, we now have to define the adaptive rule to determine the value of the control parameters at each step depending on the actual knowledge. More specifically, at each step of the estimation process one has to decide the control parameters $\mathbf{c}$ (here, the additional phases $\boldsymbol{\Phi}$) for the next probe. To this end, we consider different strategies.

(i) A first approach is based on choosing the control phases according to $\hat{\boldsymbol{\phi}} + \boldsymbol{\Phi} \simeq \boldsymbol{\delta\phi}$, where $\boldsymbol{\delta\phi} = \mathrm{argmin}_{\Delta\phi_1, \Delta\phi_2} \mathrm{Tr}(\mathcal{F}^{-1})$. This strategy looks to set the interferometer phases $\boldsymbol{\Delta\phi}$ to those values leading to a minimum bound for $L(\boldsymbol{\phi}, \hat{\boldsymbol{\phi}})$ according to the Cramér-Rao inequality. While this approach is tailored to work in the asymptotic regime of large N, its performances are not guaranteed to be optimal for small N. An upside of this approach is that setting the control parameters does not require complex optimization steps, since an analytic rule can be easily defined.

(ii) In order to devise a strategy working in the small N regime, one can consider a second strategy which is specifically tailored to work for all values of N. To this end, we adapted the protocol described in [394] to the multiparameter scenario implemented by our system. By this approach, the choice of the control phases is performed to optimize a given figure of merit, known as utility function ($\mathcal{U}$). Canonical choices for $\mathcal{U}$ are information gain or quadratic loss. In our case, we choose $\mathcal{U}(\hat{\boldsymbol{\phi}}) = \mathrm{Tr}[\mathrm{Cov}(\hat{\boldsymbol{\phi}})]$, calculated over the posterior

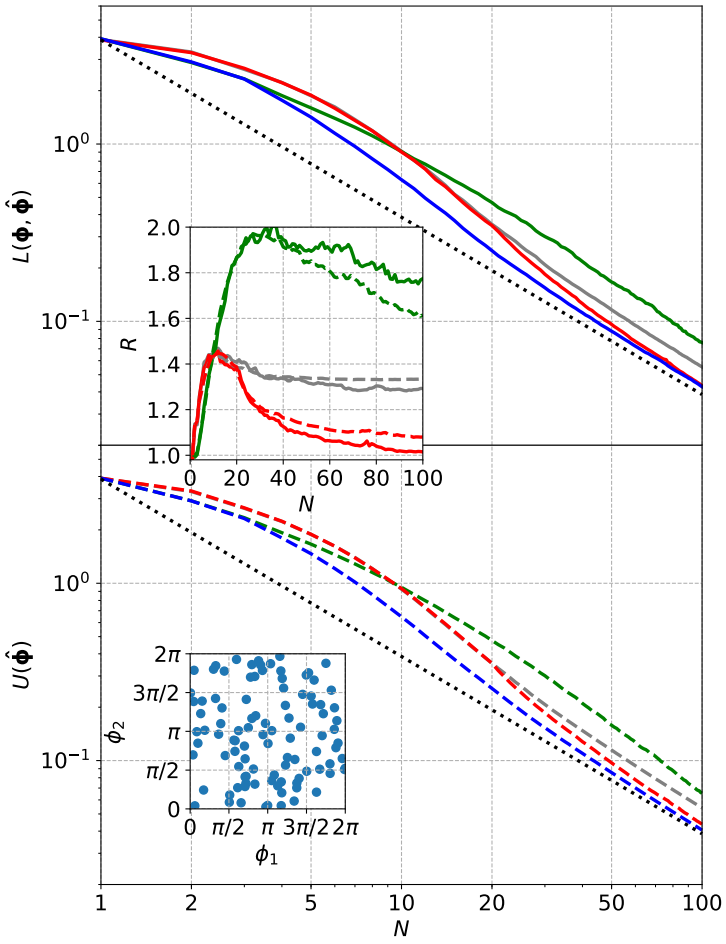

Figure 3.30. Numerical simulations of Bayesian adaptive protocols. For $N_{\text{ph}} = 100$ pair of phases, we simulated the performance of the different strategies described in the main text, by averaging for each phase over $N_{\text{exp}} = 100$ different runs and by performing spline interpolation on the obtained curves. Top: quadratic loss $L(\boldsymbol{\phi}, \hat{\boldsymbol{\phi}})$ (solid lines). Bottom: utility function $\mathcal{U}(\hat{\boldsymbol{\phi}}) = \text{Tr}[\text{Cov}(\hat{\boldsymbol{\phi}})]$ (dashed lines), corresponding to the sum of the parameters confidence intervals. Inset: (top) ratio R between the performances of each protocol, compared with the optimized strategy (ii). R is computed both for $L(\boldsymbol{\phi}, \hat{\boldsymbol{\phi}})$ (solid lines) and $\mathcal{U}(\hat{\boldsymbol{\phi}})$ (dashed lines), referring the same colors of the main panels. (bottom) two-dimensional map of uniform-distributed couples of phases drawn for the simulations. Green lines: approach (i) based on the Fisher information matrix. Red lines: approach (i') which includes first $N = 20$ events with random control parameters, while for $N > 20$ works as (i). Blue lines: optimized approach (ii). Grey lines: benchmark approach with random control parameters (iii). Dotted black lines: Cramér-Rao bound for the asymptotic regime. This image is taken from [15].

distribution. Note that this approach is general and different utility functions can be chosen, based on the specific estimation scenario. For instance, if the parameter of interest is the correlation between the phases, the utility function should involve the off-diagonal terms of the covariance matrix. Hence, at each step the minimization algorithm finds the best control phases $\boldsymbol{\Phi}$ that, averaged over all possible measurement outcomes, leads to a minimum value for the sum of the parameters confidence intervals. This is thoroughly discussed in

the final Supplementary Information 3.3.2. Given that this method relies on numerical optimization steps, it is more expensive in terms of computational resources than the previous strategy based on the Fisher information matrix. Conversely, it provides the advantage of searching the optimal control phases for all values of N, thus covering the limited data regime where asymptotic approaches may not be the proper choice.

We have then performed numerical simulations to characterize the performances of the two algorithms. More specifically, we have sampled $N_{\text{ph}} = 100$ random pairs of phases (ϕ_1, ϕ_2) in the interval $[0, 2\pi] \times [0, 2\pi]$. For each pair, we simulated $N_{\text{exp}} = 100$ estimation processes where $N = 100$ single-photon probes are sent in the interferometer. The results are shown in Fig. 3.30. We first tested the performances of both algorithms (i) and (ii). We observe that, concerning strategy (i), the protocol fails to approach the Cramér-Rao bound even for $N \sim 100$. This is related to the non-injectivity of the likelihood function. In this way, a given probability can be associated to different possible pairs of phases. Approach (i) seeks for setting the phase differences $\boldsymbol{\Delta\phi}$ to a fixed point, and it is not able to resolve such ambiguity issue.

(iii) Better results are obtained by applying at each step a random (but known) set of control phases (iii), which shows better convergence while not reaching the Cramér-Rao bound. However, the application of this strategy is capable of resolving the ambiguity.

(i') One can then consider a modified version of the asymptotic protocol (i), where the first K control phases are drawn from a uniform distribution, while for $N > K$ the strategy works as (i). Numerical evidence shows that the best choice for this parameter is $K \sim 20$. We observe that, with this modified strategy, the Cramér-Rao bound is approached for $N \sim 50$.

Better results are obtained with the optimized strategy (ii), in particular in the small N regime. For $N > 60$, we observe that both strategies (i') and (ii) provide similar performances since the experiment progressively approaches a large N scenario where the Fisher information matrix defines the system sensitivity.

Finally, we perform some numerical simulations to show the superior performance of the optimized adaptive protocol with respect to non-adaptive strategies, that are not capable of resolving unambiguously the estimation process in the full $[0, 2\pi] \times [0, 2\pi]$ interval. After, we experimentally implement the optimal strategy to guarantee a faster convergence of the estimation process.

Comparison with non adaptive estimation

The advantages of our technique can be also found when comparing the performances with respect to non-adaptive scheme. We investigate such aspect by performing some numerical simulations. More specifically, when performing the estimation with non-adaptive strategies the likelihood function suffers from injectivity issues. Indeed, when there is very limited a-priori knowledge on the parameters, thus resulting in an almost flat prior distribution, multiple pairs of phases can lead to the same outcome probabilities. Hence, in this case a phase estimation experiment is not able to distinguish between the different pairs, and the posterior distribution evolves concentrating around multiple equivalent peaks (Fig. 3.31). As a consequence, the overall error does not scale as CRB, as it represents the variance calculated

along the multi-peaked posterior. Furthermore, the result of the estimator is not reliable since the average of the posterior does not correspond to any of the multiple pairs. Conversely, adaptive scheme allows to remove this injectivity issue, thus achieving the CRB and providing a reliable estimation. Comparison between these two approaches with a flat prior over the full 2π interval is reported in Fig. 3.32a.

Additionally, let us consider the scenario when the prior distribution is sharp enough to avoid ambiguities, and the measurement is fixed. Fig. 3.32b shows a comparison between the performance of two schemes with a prior knowledge of width $2\pi/10$. Also in this scenario, the adaptive algorithm shows improved performances

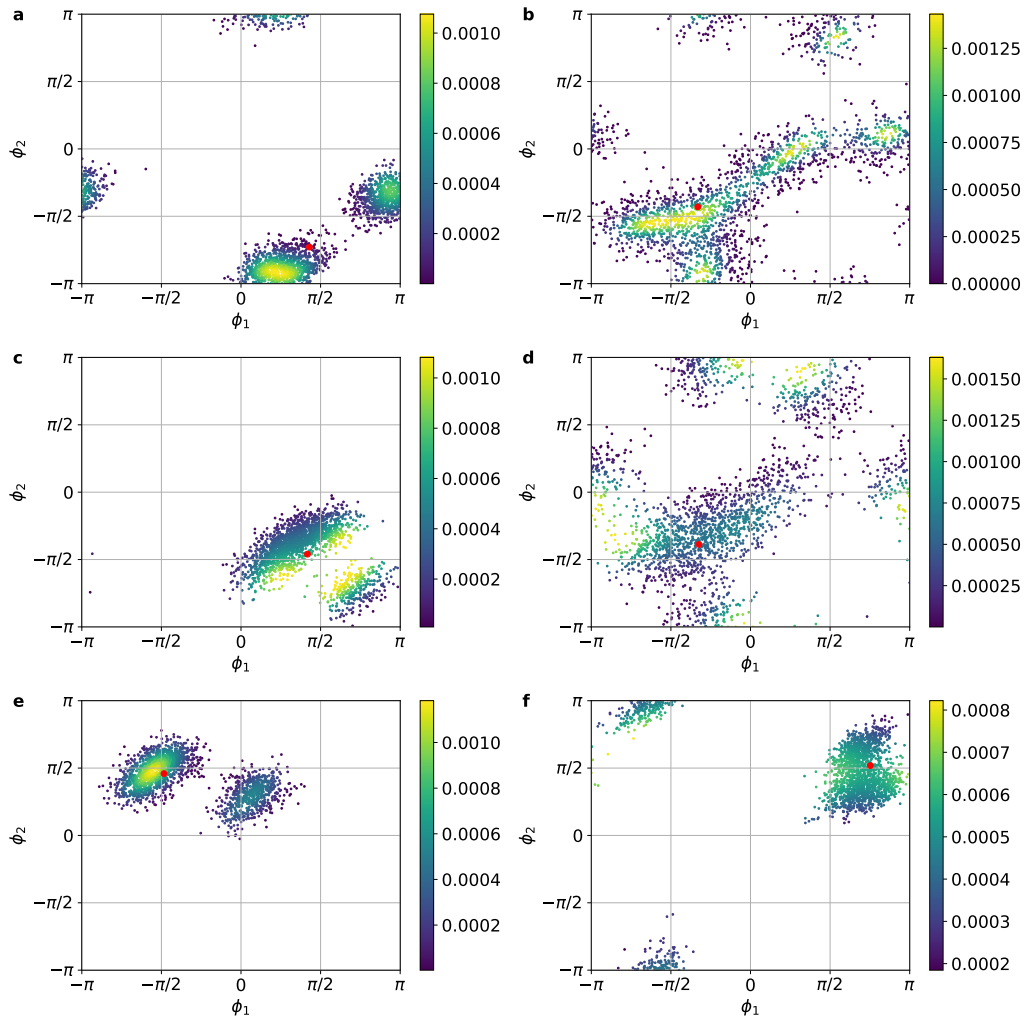

Figure 3.31. Examples of non-adaptive two-phase estimation. Posterior evolution after $N = 100$ photons using non-adaptive Bayesian estimation for six different pairs of unknown phases (red dots): **a**, $(\phi_1, \phi_2) = (1.350, -2.289)$; **b**, $(\phi_1, \phi_2) = (-1.040, -1.350)$; **c**, $(\phi_1, \phi_2) = (1.311, -1.445)$; **d**, $(\phi_1, \phi_2) = (-1.016, -1.218)$; **e**, $(\phi_1, \phi_2) = (-1.520, 1.441)$; **f**, $(\phi_1, \phi_2) = (2.365, 1.628)$. When limited or no a-priori knowledge is available on the phases (here, we assume a flat prior), each outcome probability can belong to different equivalent pairs of phases. This results in the presence of multiple peaks in the posterior distribution during the estimation process. In all plots, particle colors represent the corresponding weight. This image is taken from [15].

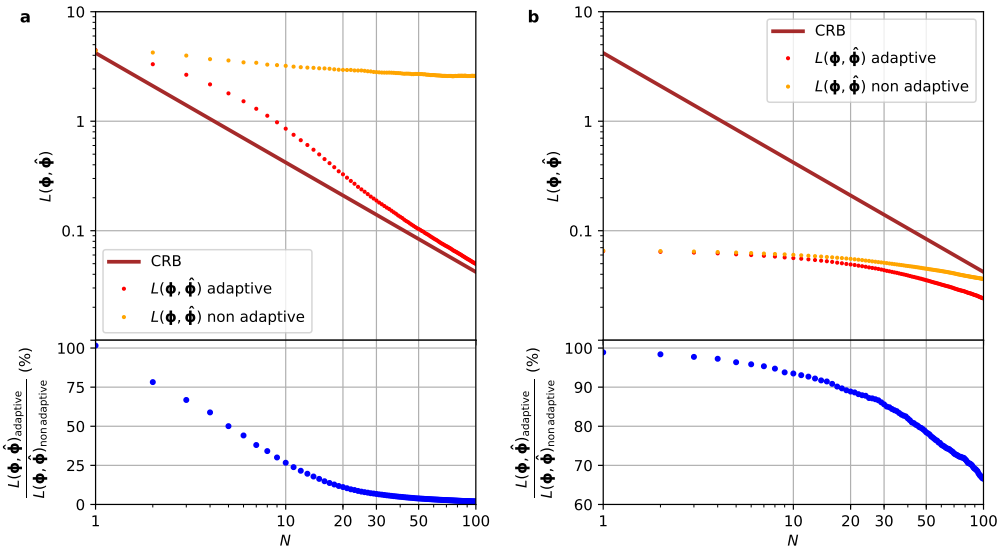

Figure 3.32. Comparison between adaptive and non-adaptive strategies. Numerical simulations of Bayesian estimation protocols having both **a**, a flat prior distribution and **b**, a narrow prior distribution of width $2\pi/10$. In the top panels, the overall quadratic loss $L(\boldsymbol{\phi}, \hat{\boldsymbol{\phi}})$ is shown as function of the number N of employed photons using an adaptive (red) and a non-adaptive technique (orange). Results have been averaged over $N_{\text{ph}} = 100$ random pairs of phases, estimated $N_{\text{exp}} = 100$ independent times. In the bottom panels, the performances are compared by considering the ratio between the $L(\boldsymbol{\phi}, \hat{\boldsymbol{\phi}})$ of the two techniques. This image is taken from [15].

with respect to the non-adaptive one, since it is capable of progressively find the working point with higher sensitivity for the chosen measurement.

Integrated circuit for multiphase estimation

The platform employed in this experiment is an integrated three-arm interferometer. This system has been employed in Ref. [14] for the simultaneous estimation of two relative phase shifts $\boldsymbol{\phi} = (\phi_1, \phi_2)$ between the arms of a three mode interferometer (Fig. 3.33). We first discuss the circuit layout and parameters, while we subsequently describe the working condition used for the multiphase estimation experiments reported below.

The platform is a three-arm interferometer realized in a glass chip through femtosecond laser writing [56, 60]. The interferometer, optimized for operation at $\lambda = 785$ nm, is implemented by two cascaded tritters (three-mode beam splitters) A and B interspersed with phase shifters. Each tritter is decomposed in a 2-D planar configuration [615] consisting of three balanced directional couplers and one phase shifter $\phi_{\text{T}}^{\text{A}}$ ($\phi_{\text{T}}^{\text{B}}$) for tritter A (B). These phase shifters, as well as those placed between the two tritters, can be tuned by means of the thermo-optic effect, using microresistors that are patterned in a thin gold layer covering the chip surface. When an electrical current is applied to the resistor, an optical path change on the waveguide is induced by the dissipated heat [614]. In particular, let us consider the dissipated power $P_i = R_i I_{R_i}^2$ on resistor R_i subjected to a current I_{R_i}, where we also include that the value of the resistor depends on the current due to its temperature

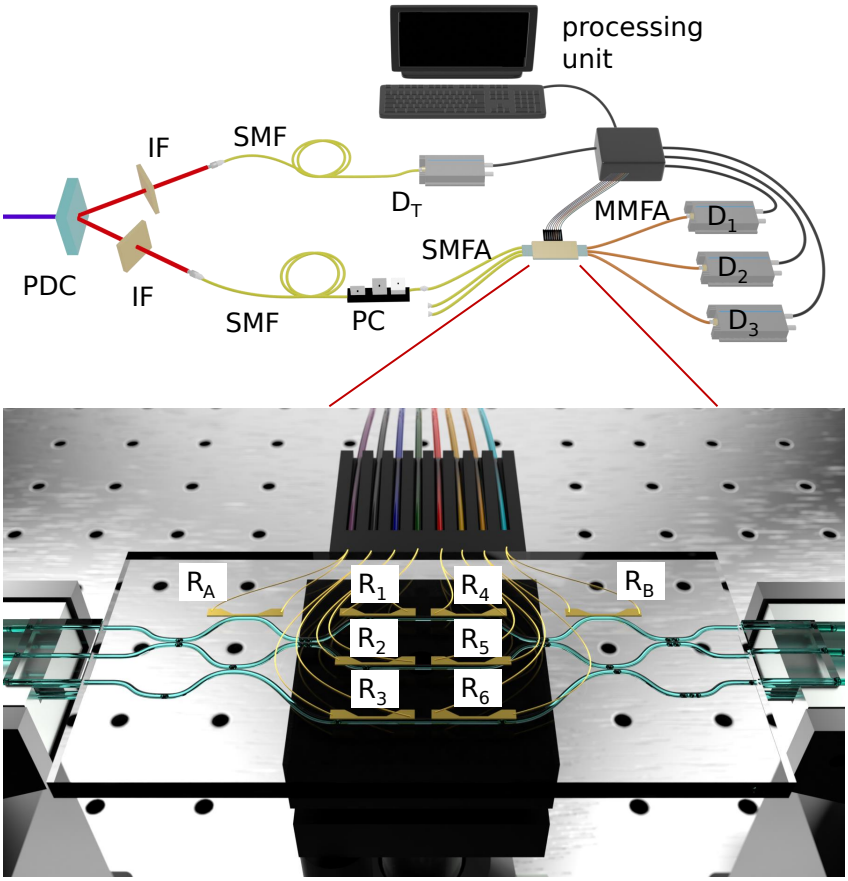

Figure 3.33. Experimental platform. A type-II parametric down-conversion source (PDC) generates photon pairs, which are spectrally selected via interference filters (IF) and coupled to single-mode fibers (SMF). One of the photons is directly measured by detector D_T acting as a trigger for the experiment. The other photon, after polarization compensation (PC), can be injected in any of the three input ports of the interferometer via a single-mode fiber array (SMFA). After evolution, photons are collected via a multi-mode fiber array (MMFA) and measured through detectors D_i, with $i = 1, 2, 3$. Coincidences between D_T and any of D_i are recorded via a time-to-digital converter. The results of the measurement are processed and employed to apply the adaptive protocols. The layout of the integrated circuit (shown in the bottom panel) includes 8 resistors to modulate the input transformation ($R_{\rm A}$), the output one ($R_{\rm B}$), and the internal phases (R_i, with $i = 1, \ldots, 6$) as described in the main text. This image is taken from [15].

change. The two induced relative phase shifts $\boldsymbol{\Delta\phi} = (\Delta\phi_1, \Delta\phi_2)$ between the arms of the interferometer with respect to the reference mode, have the following general dependence on the dissipated powers:

$$\Delta\phi_j = \phi_{j0} + \sum_{i=1}^{6} \left(\alpha_{ji} P_i + \sum_{k=i}^{6} \alpha_{jik}^{\rm NL} P_i P_k \right), \tag{3.56}$$

where $j = 1, 2$ and ϕ_{j0} stands for the static phases of the interferometer. Parameters α_{ji} and $\alpha_{j,i=k}^{\rm NL}$ are the linear and quadratic response coefficients relative to the dissipated power P_i, respectively, while $\alpha_{j,i\neq k}^{\rm NL}$ represent the nonlinear coefficients associated to the product of the two powers P_i and P_k to include cross-talk effects.

In our device 8 independent resistors are present (Fig. 3.33). Resistors R_{A} and R_{B} are exploited to tune tritter phases $\phi_{\mathrm{T}}^{\mathrm{A}}$ and $\phi_{\mathrm{T}}^{\mathrm{B}}$, respectively. Conversely, resistors R_1, R_4 along mode 1, R_2, R_5 along mode 2 and R_3, R_6 along mode 3, are employed to tune the internal relative phase shifts of the interferometer, according to (3.56). The operations of tritters A and B are described through the unitary evolutions U_{A} and U_{B}, respectively, while the action of each phase shifter along mode i is described through a unitary matrix PS_i ($i = 1, 2, 3$). The overall evolution U^{tot} of the interferometer is given by $U^{\mathrm{tot}} = U_{\mathrm{B}}(\prod_{i=1}^{3} \mathrm{PS}_i)U_{\mathrm{A}}$.

In order to characterize the relevant parameters necessary to fully describe the evolution of the interferometer, we measure the output probabilities when single photons are injected along input 1, tuning the current applied on each resistor. The probabilities have been theoretically modeled by modifying the ideal expression with additional terms, taking into account non-ideal visibilities and dark counts of the detectors. In this way, we performed an overall fit of all the measured probabilities to determine the 58 chip parameters (see Supplementary Information of [15] for more details) and finely reconstruct the likelihood probability $p(d|\boldsymbol{\Delta\phi})$ of our system. According to the scheme of Fig. 3.29b, the unknown phases to be estimated are the pairs (ϕ_1, ϕ_2), relative to the chosen reference arm ϕ_{ref}. The 8 resistors allow us to finely tune and control all the relevant phase shifts of the interferometer. The tritters phases can be tuned and are chosen in order to maximize the sensitivity of the interferometer. Thus, after the characterization of all parameters, we reconstructed the Fisher Information matrix $\mathcal{F}_{\mathrm{exp}}$. Then, we optimized the quantity $\mathrm{Tr}[(\mathcal{F}_{\mathrm{exp}})^{-1}(\Delta\phi_1, \Delta\phi_2, \phi_{\mathrm{T}}^{\mathrm{A}}, \phi_{\mathrm{T}}^{\mathrm{B}})]$ over the phases $\Delta\phi_1, \Delta\phi_2, \phi_{\mathrm{T}}^{\mathrm{A}}, \phi_{\mathrm{T}}^{\mathrm{B}}$, in the range of total dissipated power permitted by the circuit. Indeed, a total dissipated power greater than 1 W could damage the resistors. We found that the minimum value of this quantity is reached when the single photons are injected along input 1, arm 2 of the circuit is chosen as a reference, and the values of tritter and internal phases are the following: $\phi_{\mathrm{T}}^{\mathrm{A}} = 1.49$ rad, $\phi_{\mathrm{T}}^{\mathrm{B}} = 0.72$ rad, $\Delta\phi_1 = -3.07$ rad and $\Delta\phi_2 = 0.34$ rad.

Fixing these conditions we reconstruct the Fisher Information matrix, obtaining:

$$\mathcal{F}_{\mathrm{exp}} = \begin{pmatrix} 0.548 & -0.226 \\ -0.226 & 0.585 \end{pmatrix} \qquad \mathcal{F}_{\mathrm{exp}}^{-1} = \begin{pmatrix} 2.171 & 0.839 \\ 0.839 & 2.034 \end{pmatrix}. \tag{3.57}$$

Hence, estimating the two phases with N probes, the bound over the sum of the quadratic losses is:

$$NL(\boldsymbol{\phi}, \hat{\boldsymbol{\phi}}) \geq \mathrm{Tr}[(\mathcal{F}_{\mathrm{exp}})^{-1}] = 4.2 \tag{3.58}$$

Such minimized value of $\mathrm{Tr}[(\mathcal{F}_{\mathrm{exp}})^{-1}]$ represents the (phase-dependent) Cramér-Rao bound of our device, where the aim of the protocol is to saturate such bound for all phase pairs by using limited probes. In absence of adaptive strategies, such precision cannot be reached for all phase pairs, thus rendering the sensitivity of the sensor phase-dependent. The aim of our strategy is thus also to reach the bound $\mathrm{Tr}[(\mathcal{F}_{\mathrm{exp}})^{-1}] = 4.2$ for all values of the parameters.

In order to achieve this goal, we discuss below how we exploit the phases in our interferometer. The unknown phases $\boldsymbol{\phi} = (\phi_1, \phi_2)$ are tuned by means of resistors R_4, R_5 and R_6, according to (3.56), while the control phases $\boldsymbol{\Phi} = (\Phi_1, \Phi_2)$ are tuned by resistors R_1 and R_2.

Tuning of circuit parameters for adaptive two-phase estimation

In the employed interferometer the pair (ϕ_1, ϕ_2) represents the unknown phases relative to a reference arm with phase ϕ_{ref} (Fig. 3.29b). All the relevant phases of the circuit can be finely tuned by means of 8 resistors.

The first step performed aimed at finding the optimal choice for the tritter phases $\phi_{\text{T}}^{\text{A}}$, $\phi_{\text{T}}^{\text{B}}$ to maximize the sensitivity of the interferometer. As previously discussed, the best scenario for our interferometer corresponds to use mode 2 as reference mode and arm 1 as input mode for single photons, with the following values of phases: $\phi_{\text{T}}^{\text{A}} = 1.49$ rad, $\phi_{\text{T}}^{\text{B}} = 0.72$ rad, $\Delta\phi_1 = -3.07$ rad and $\Delta\phi_2 = 0.34$ rad. In this working point, the trace of the inverse of the Fisher Information matrix is $\text{Tr}[(\mathcal{F}_{\text{exp}})^{-1}] = 4.2$. We now have to assign each resistor R_i $(i = 1, \ldots, 6)$ to tune both the unknown phase shifts $\boldsymbol{\phi} = (\phi_1, \phi_2)$, and the control phases $\boldsymbol{\Phi} = (\Phi_1, \Phi_2)$ for the adaptive algorithms. More specifically, we choose to employ resistors R_4, R_5 and R_6 to tune $\boldsymbol{\phi}$. Conversely, the control phases $\boldsymbol{\Phi}$ are those modified by dissipating power in R_1 and R_2. Hence, considering (3.56) as $\boldsymbol{\Delta\phi} = \boldsymbol{\phi} + \boldsymbol{\Phi}$, we find the following expressions:

$$\phi_j = \phi_{j0} + \sum_{i=4}^{6} \left(\alpha_{ji} P_i + \sum_{k=i}^{6} \alpha_{jik}^{\text{NL}} P_i P_k \right) \tag{3.59}$$

$$\Phi_j = \sum_{i=1}^{2} \left(\alpha_{ji} P_i + \sum_{k=i}^{2} \alpha_{jik}^{\text{NL}} P_i P_k \right) , \tag{3.60}$$

with $j = 1, 2$. In setting all phases of the device (equations 3.59 and 3.60) the effective number of applicable phases is finite, due to the upper damage threshold of global power (< 1 W) and to the limited precision of the power supply (Keithley 2230). In particular, the generated control phases are distributed uniformly and quite densely over all the interval $[0, 2\pi] \times [0, 2\pi]$, sufficient to guarantee the correct functionality of the tested algorithms. Note that, in principle, only 4 resistors would be sufficient to tune independently the 4 phase shifts (2 unknown and 2 controls). However, we employed 5 resistors in order to obtain large tunability of the device within limits of the damage threshold of each resistor.

Experimental results

We perform the experiment by continuously adapting the present tunable circuit following the optimized Bayesian-SMC method [strategy (ii)]. This allows us to achieve best attainable estimation with a limited number of resources. The probes are heralded single photons at 785 nm generated by a degenerate type-II SPDC process inside a BBO crystal, pumped by a pulsed 392.5 nm laser. A photon from each pair is sent through the circuit, entering in input 1, and acts as a probe, while the other photon acts as the trigger for the heralding process (see Fig. 3.33). An event is then recorded as the coincidence between the trigger detector and one of the three outputs of the circuit. The interaction of the probe with the chip operator encodes information about $\boldsymbol{\phi}$ onto its state. Finally, the result of the measurement is collected and used to identify the optimal settings for the next experimental step.

The phases $\boldsymbol{\phi}$ to be estimated can be chosen by setting the currents flowing in three resistors R_4, R_5, R_6 [Eq. (3.59)]. In order to test the protocol over different estimation experiments, we have identified $N_{\text{ph}} = 15$ pair of phases uniformly distributed (Fig. 3.34). Resistors R_1, R_2 are used to tune the control phases necessary for the adaptive strategy [Eq. (3.60)]. After the first event, where currents

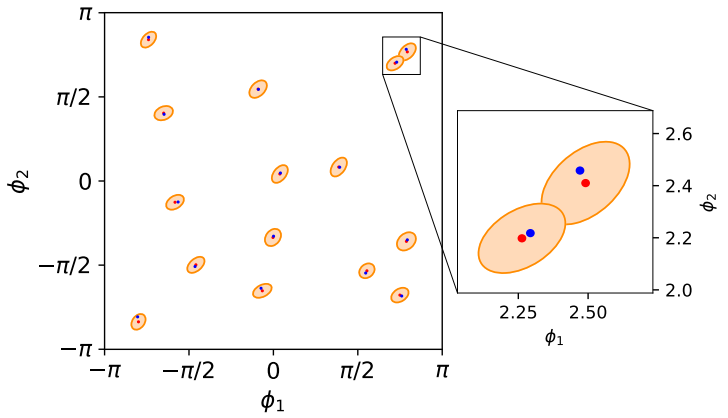

Figure 3.34. Final distribution of the estimated phases. Experimental simultaneous estimations of $N_{\text{ph}} = 15$ different uniform-distributed pairs of phases. The estimation process uses an amount of $N = 100$ resources and Bayesian adaptive approach. Dark orange regions represent the error in the estimation obtained from the covariance matrix. Each estimated pair (red dot) is distant from the true set value (blue dot) within the error (orange area), thus confirming the good performance of the algorithm. This image is taken from [15].

I_{R_1}, I_{R_2} are chosen at random, we implement strategy (ii): optimal control phases $\mathbf{\Phi}$ are calculated by minimizing the expected posterior variance. The nearest available control currents I_{R_1}, I_{R_2}, limited by the precision of our power supply (Keithley 2230) and by maximum dissipation power (< 1 W), are calculated and effective control phases are applied to the device. The calculation of the prior distribution for each step is made through the particle approximation. A uniform grid of $M = 2000$ pairs of phases (Fig. 3.35a) is assumed as the initial set for the prior distribution. This choice is performed to avoid any possible harmful periodicity during the estimation process. Examples of prior information evolution during an experiment are reported in Fig. 3.35b-d. In Fig. 3.35c the resampling step is shown, where particles with zero weight of the previous step (Fig. 3.35b) are rearranged in more significant locations (see the final Supplementary Information 3.3.2 for more details). Each pair is estimated $N_{\text{exp}} = 100$ times, adopting $N = 100$ resources (photons) as for the numerical simulations discussed above. Some examples of single experiments are reported in detail in Fig. 3.36. Algorithm performances are shown in Fig. 3.37. A first evaluation consists in averaging the experimental quadratic loss for each pair of phases over all N_{exp} independent runs. As a result, the overall quadratic loss $L(\boldsymbol{\phi}, \hat{\boldsymbol{\phi}})$ saturates the CRB with a limited number of resources, in agreement with the numerical simulations described above. Furthermore, saturation occurs both for off- and diagonal matrix elements of the CRB. In particular, the latter show that the CRB is reached with similar performances in the estimation of both phases. This result is a fundamental feature for multiparameter metrology tasks when both parameters are treated equally. We observe from Fig. 3.37c that our algorithm reaches the CRB also when looking at the correlations between the parameters. This means that the employed estimation approach does not add additional sources of undesired correlations in the estimation process, which is relevant given the addressed multiparameter scenario. In our case the resulting difference in estimation of the two parameters is less than 10%, when compared to the sensitivity bound. Furthermore, a heuristic estimation of the convergence time to saturate the CRB can

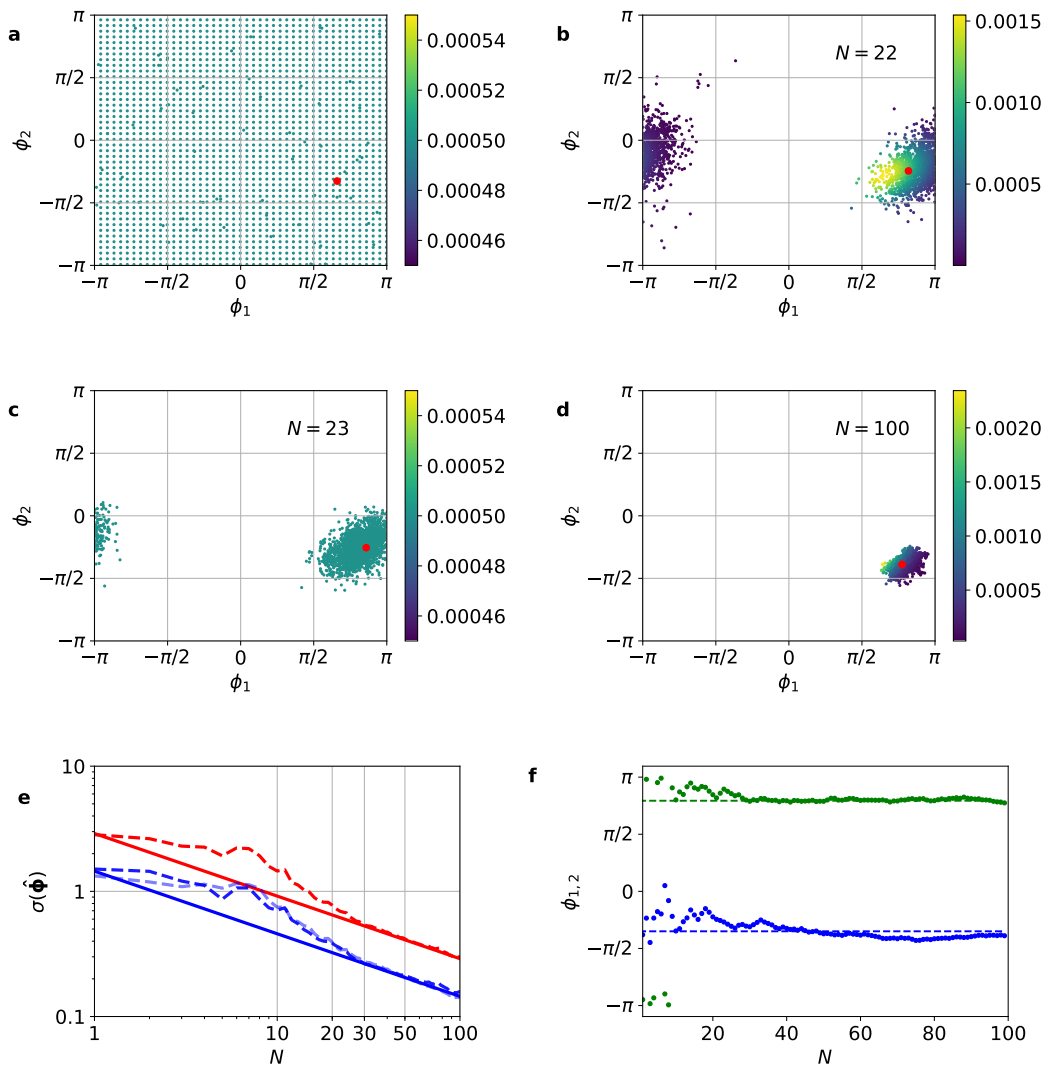

Figure 3.35. Example of experiment. A typical estimation of two phases (red dots) is reported. **a**, A uniform grid is generated as initial support for the prior distribution. **b-d**, Evolution of the posterior distribution during experiment for three subsequent moments. In particular, the distribution before and after the resampling are shown respectively in **b** and **c**, where particles are rearranged in order to eliminate zero weight cases. The new posterior weights are uniform, while particles are distributed closer to the estimated phases. In **a-d**, particle colors represent the corresponding weight. **e**, Study of standard deviation in estimation of the single phases (blue dashed lines) and their sum (red dashed lines). The saturation of their CRB (solid lines) occurs for small N. **f**, Experimental estimated pair of phases as function of the number N of adopted probes (dots). Dashed lines indicate true set values of the phases. This image is taken from [15].

be calculated by studying the difference $L(\boldsymbol{\phi}, \hat{\boldsymbol{\phi}}) - \mathrm{Tr}[(\mathcal{F}_{\mathrm{exp}})^{-1}]/N$. A characteristic time can be computed by using $a + b\exp(-N/\tau_N)$ as fit function, with $a, b, \tau_N \in \mathbb{R}$ the fitting parameters. The value obtained for τ_N is $\tau_N^{\mathrm{fit}} = 5.6$, which underlines the good performance of the adaptive adopted technique in using a small number of probes. Note that the number of probes necessary to achieve the bound is generally

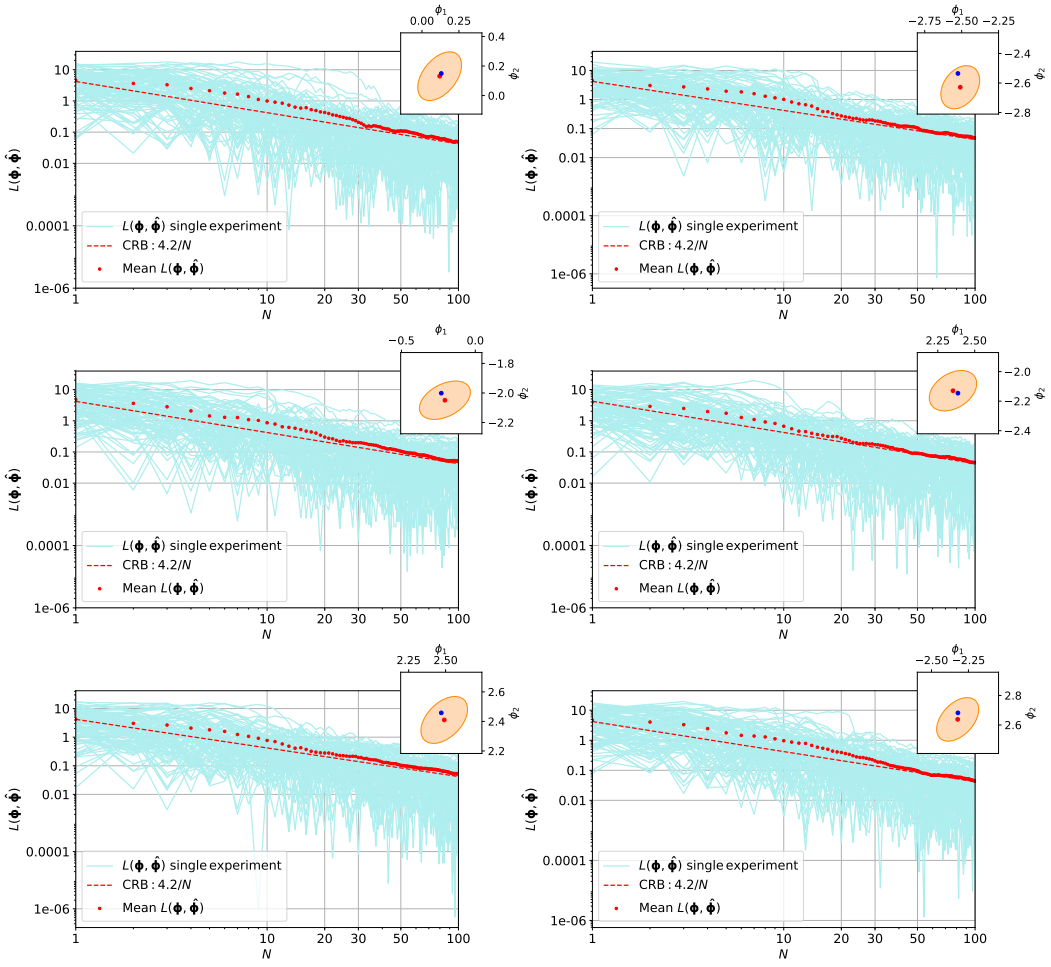

Figure 3.36. Examples of adaptive two-phase estimation experiments. $L(\phi,\hat{\phi})$ from $N_{\text{exp}} = 100$ independent experiments (light blue solid lines) are reported for six different pairs of phases: **a**, $(\phi_1,\phi_2) = (0.131, 0.149)$; **b**, $(\phi_1,\phi_2) = (-2.525, -2.535)$; **c**, $(\phi_1,\phi_2) = (-0.230, -2.001)$; **d**, $(\phi_1,\phi_2) = (2.386, -2.146)$; **e**, $(\phi_1,\phi_2) = (2.471, 2.458)$; **f**, $(\phi_1,\phi_2) = (-2.321, 2.682)$. The average over all experiments (red dots) saturates the CRB ($\text{Tr}[(\mathcal{F}_{\text{exp}})^{-1}]/N = 4.2/N$) (dashed lines). The inset shows the average estimated phases (red dots), the true phases to be estimated (blue dot) and the confidence interval associated to the covariance matrix (orange region). This image is taken from [15].

scheme-dependent, as it can be seen studying different multiparameter scenarios [671]. Another significant property of Bayesian approach is the ability to provide the statistical error in each step of the estimation process, calculated as the variance of the posterior distribution. Final estimated pairs fall on average within the error from true set values of phases (Fig. 3.34).

All these experimental results demonstrate the quality of Bayesian-SMC strategy, confirming it as largely suitable for multiparameter estimation problems. While the convergence to CRB in limited data regime has been accurately studied by theoretical works in both single- [664, 553, 686] and multi- [670, 671] parameter estimation, the obtained results show the robustness of the employed Bayesian approach when applied to a realistic sensor, where calibration of the system has to be performed before it can be employed for phase estimation experiments. Indeed,

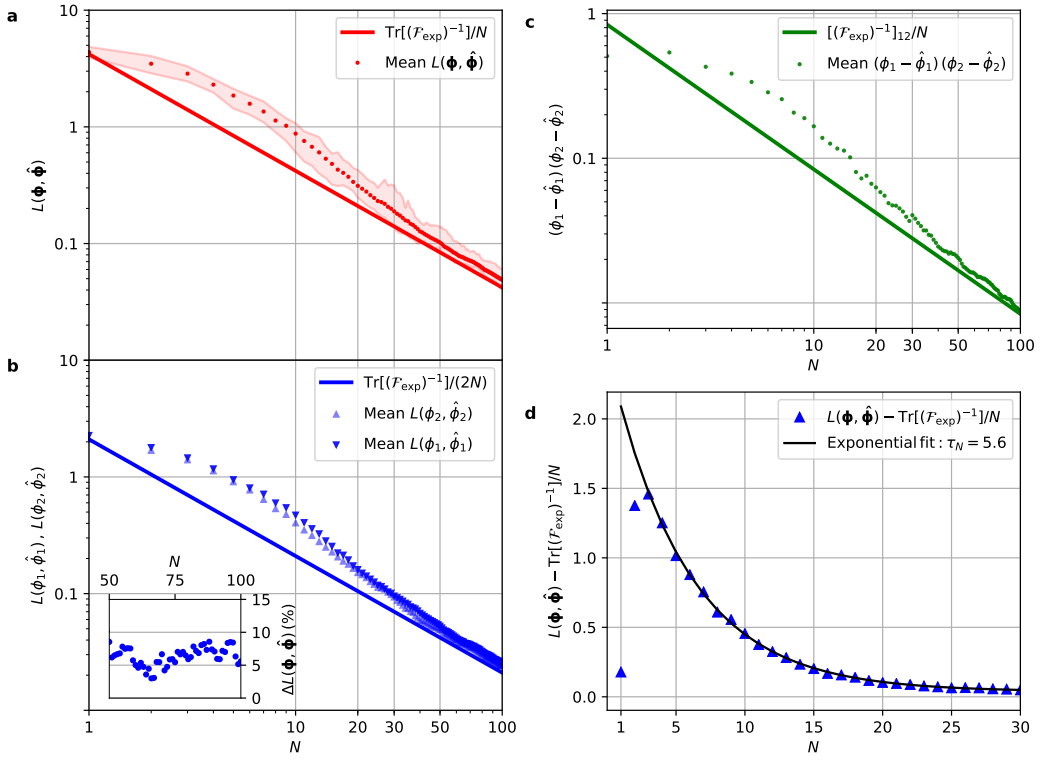

Figure 3.37. Experimental results. Simultaneous estimations of $N_{\rm ph} = 15$ different pairs of phases using Bayesian adaptive protocol. Quadratic loss is averaged for each phase over $N_{\rm exp} = 100$ independent runs. **a**, Comparison between overall quadratic loss $L(\boldsymbol{\phi},\hat{\boldsymbol{\phi}})$ (red dots) and $\mathrm{Tr}[(\mathcal{F}_{\rm exp})^{-1}]/N$ (red solid line). The performances are in agreement with the numerical simulations. Red shaded regions represent the one-standard deviation interval where $L(\boldsymbol{\phi},\hat{\boldsymbol{\phi}})$ can be found. **b**, Analysis of diagonal elements of CRB by comparing quadratic loss relative to the single phase of the estimated pair $L(\phi_i,\hat{\phi}_i)$ (with $i = 1, 2$) (blue triangles) and $\mathrm{Tr}[(\mathcal{F}_{\rm exp})^{-1}]/(2N)$ (blue solid line). The algorithm shows symmetric optimal performances for estimation of both parameters, by using the same amount of resources. This feature is highlighted by the inset panel, where the ratio $\Delta L(\boldsymbol{\phi},\hat{\boldsymbol{\phi}})$ between the difference of the two estimations and the bound value is reported. **c**, Analysis of phase correlations by comparing off-diagonal terms of $\mathcal{F}^{-1}_{\rm exp}$ [Eq. (3.57)] and $[(\mathcal{F}_{\rm exp})^{-1}]_{12}/N$ (green solid line). **d**, Estimation of convergence time (τ_N) to CRB. The value can be estimated by fitting the distance between the averaged $L(\boldsymbol{\phi},\hat{\boldsymbol{\phi}})$ and CRB, after $N > 2$. The adopted fit function is $a + b\exp(-N/\tau_N)$, with $a, b, \tau_N \in \mathbb{R}$ the fitting parameters, leading to $\tau_N = 5.6$. The choice of this function is performed to provide a reasonable estimation of τ_N, as the number of probes necessary to approach the CRB. This image is taken from [15].

we have shown the capability of saturating the Cramér-Rao bound by using limited probes when the calibration procedure is performed with finite size data. Note that such result is non-trivial, and shows that the actual sensor modeling permits a high degree of device control to be reached, even when a larger number of phases is simultaneously tuned. Implementation of this strategy has been enabled only by the high reconfigurability of our employed integrated device, which highlights the fundamental role of an appropriate platform for metrology tasks which involve more than one parameter. These features characterise our proof-of-principle experiment,

defining it as a necessary step towards the realisation of adaptive multiparameter algorithms for technological applications.

Conclusions and perspectives

We have reported the experimental implementation of a multiphase Bayesian adaptive protocol on an integrated platform, optimized to operate in the limited data regime. We have reviewed different adaptive strategies and selected the one optimizing the cost function given by the trace of the covariance matrix. This has been employed to perform several simultaneous estimations of uniformly distributed pairs of phases. As we have shown, the achievable bounds are attained for both unknown phases after a limited number of $N \sim 40$ probes. Our experiment permits to underline the suitability of such an integrated circuit for performing multiparameter estimation tasks, as well as to exploit the capabilities of the proposed Bayesian adaptive strategy.

This work provides a versatile approach for future perspectives in multiparameter Quantum Metrology. In particular, these techniques can be directly generalized for multi-photon quantum probes which would provide insight on the achievable quantum accuracy limit. Indeed, the framework behind this approach is general, and thus different probe states can be employed by suitable choice of the system likelihood function. At the same time, the algorithm here described can be applied to more complex integrated platforms, which enable optimized extraction of information. The realized platform can be exploited also for the realization of different optimal multiphase Bayesian protocols, such as that proposed in Ref. [671]. In this paper, given an arbitrary state, prior knowledge and number of repetitions of the experiment, explicit recipes for the optimal measurements are provided in the case where the estimators commute. Further perspectives include the study of different multiparameter scenarios, as well as practical applications to quantum sensing of delicate samples [687] and quantum error correcting algorithms [688, 689, 690].

Supplementary information

The machine learning technique exploited to realize two-phase estimation experiments is based on approximating the prior probability distribution support with M discrete particles [394]. More specifically, a probability weight w_i is associated with each $i-$particle by keeping normalization $\sum_{i=1}^{M} w_i = 1$. Then, the posterior distribution is updated according to the Bayes rule. In this section we discuss two aspects of this technique: the resampling strategy, and the utility function chosen to tune the control parameters.

Resampling strategy

Fig. 3.35a shows that the initial support is uniformly covered by particles. During the estimation protocol, the updating process according to the Bayes rule modifies the particles weights towards more likely phases values. Greater weights are attributed to particles closer to the estimated values. Conversely, distant particles tend to zero weights according to the normalization rule (Fig. 3.35b), thus bringing no useful information. Furthermore, the estimation sensitivity of the unknown phase pairs is limited by the initial density of particles around the true values. To solve these problems, resampling techniques can be adopted to update particles in

more significant positions. Following Ref. [394], the employed resampling technique is based on introducing, at particular steps of the process, perturbations on the particles ($\{\boldsymbol{\phi}\}$) to move them on more likely position ($\{\boldsymbol{\phi}'\}$), according to the posterior probability. First, M particles are selected randomly following the prior distribution. Then, the selected particles are moved randomly according to the multivariate distribution defined by:

$$p(\boldsymbol{\phi}) = \sum_{i=1}^{M} w_i \frac{1}{\sqrt{(2\pi)^k |\boldsymbol{\Sigma}|}} \exp\left(-\frac{1}{2}(\boldsymbol{\phi} - \boldsymbol{\mu}_i)^T \boldsymbol{\Sigma}^{-1} (\boldsymbol{\phi} - \boldsymbol{\mu}_i)\right). \tag{3.61}$$

The various distribution peaks are generated by displacing the original estimated pair ($\boldsymbol{\mu}$) in the direction of each $\boldsymbol{\phi}_i$, of a quantity $\boldsymbol{\mu}_i = a\boldsymbol{\phi}_i + (1-a)\boldsymbol{\mu}$. The parameter a is the resampling parameter, that we set to $a = 0.98$ as suggested in Ref. [394]. The covariance matrix ($\boldsymbol{\Sigma}$) is calculated by multiplying $(1 - a^2)$ with the covariance matrix of the initial particles. As a result, the particles are rearranged by increasing the density around the estimated phase values. Then, the weights of new particles are set to a uniform distribution ($w_i = 1/M$), and the learning process restarts. Resampling is performed when the following condition is fulfilled: $1/\sum_{i=1}^{M} w_i^2 < M/2$ [394].

Utility function

The utility function U defines the figure of merit that is employed to tune the control parameters $\boldsymbol{\Phi}$ during the estimation process. Canonical choices for the utility function are the information gain or the quadratic loss. In our case we chose to minimize the expected variance of the posterior distribution after each step. Given the prior distribution $\{w\}$, each output d of three possible cases ($d = 1, 2, 3$) will update the posterior following the Bayes rule, and a precise overall variance can be assigned to that specific output. The overall variance is computed by tracing the covariance matrix associated to the posterior distribution: $U(d|\{w\}) = \mathrm{Tr}[\mathrm{Cov}(\boldsymbol{\phi}|d, \{w\})]$. The expected variance $U(\boldsymbol{\Phi})$ is computed by averaging this quantity over the probability to obtain that specific output $p(d|\boldsymbol{\Phi})$. More specifically, the utility function reads:

$$U(\boldsymbol{\Phi}) = \sum_{d=1}^{3} p(d|\boldsymbol{\Phi}) U(d|\{w\}) \tag{3.62}$$

where $p(d|\boldsymbol{\Phi})$ is given by $p(d|\boldsymbol{\Phi}) = \sum_{i=1}^{M} w_i p(d|\boldsymbol{\phi}, \boldsymbol{\Phi})$. Finally, we note that $p(d|\boldsymbol{\phi}, \boldsymbol{\Phi})$ represents the likelihood of the system. A suitable characterization of the device is thus crucial to correctly apply the algorithm.

3.4 Final remarks

Photonic Quantum Metrology is an active research field, in which quantum states of light are employed to improve the estimation precision in the measurement process. Here, the phase estimation scenario is a relevant framework that can be used as a benchmark for many others. Furthermore, the realization of quantum sensors, able to perform estimations in realistic scenarios, poses two main constraints to sensing devices. On the one hand, the demands for the optimization of the limited resources, for which adaptive strategies provide a valid solution. On the other hand, the systems can show high complexity, often involving more than one parameter. Here, the estimation of multiple parameters in the quantum regime has reported few experimental investigations to date, although it is crucial to generalize the single parameter case. During my thesis work I contributed to such research directions realizing first a review on Photonic Quantum Metrology [1], and then several experimental studies on phase estimation.

The first experimental results exploited an integrated photonic platform, realized through the femtosecond laser writing technique. The device is a three-arm Mach-Zehnder interferometer able to manipulate two independent optical phase shifts [14]. Such quantities can be tuned using different phase shifters placed along the interferometer. The high degree of tunability of the platform, together with the phase stability provided by the integrated level, allowed us to study the multiphase estimation performance of the sensor in the quantum regime. In particular, by characterizing the device, we showed that it achieves quantum-enhanced performances over classical strategies when injected by multi-photon states. This result was subsequently tested, by performing the first non-adaptive simultaneous two-phase estimation experiment with two-photon input states. Our platform represents a building block for tasks of multiparameter Quantum Metrology. On the one hand, it can be used to test protocols for a practical multiparameter estimation, e.g. adaptive strategies. On the other hand, our integrated platform can be generalized enlarging the dimensionality of the system and considering more complex interferometers. Furthermore, we tested the performance of a Neural Network in calibrating the same device [16]. The approach provides optimal results, by showing the ability to not require a detailed model of the internal operation. This study showed that the Neural Network is an effective, robust, and reliable tool for the practical calibration of complex sensors that depend on multiple parameters. Moreover, it provides a useful methodology for a mass-production characterization of similar quantum sensors.

Other works concerned the study of adaptive strategies for phase estimation. Using a device similar to the previous one, we tested adaptive strategies during the multiphase estimation process [15]. Exploiting the high number of phase shifters of the photonic platform, we identified some feedback phases to tune the chip transformation. Different online adaptive strategies have been studied, and the best one — a Bayesian-Sequential Monte Carlo technique — was selected for the experimental estimation. In this way, we demonstrated an efficient experimental adaptive two-phase estimation with limited data. Such an approach is general and can be used with different probes and systems. More complex integrated platforms can be used to optimize information extraction. Then, different probe states can be employed by suitable choice of the system likelihood function. A final study concerned the investigation of an offline adaptive strategy for the estimation of a single phase into a bulk Mach-Zehnder interferometer in polarization [17]. The

presented novel technique, based on a genetic algorithm, is able to find optimal solutions for the feedback phases with a large research space. The obtained results showed that the genetic algorithm provides optimal performances even when the system is affected by two types of common losses. This algorithm is a promising candidate for investigating adaptive phase estimation problems in an offline fashion. In perspective, it could be tested with different probes or in a multiphase estimation scheme.

Conclusions

Quantum Communication and Quantum Metrology have been growing significantly in recent decades, showing an ever-increasing interest, that is reaching not only research institutions but even governments and private companies, especially regarding the quantum key distribution (QKD) and the realization of quantum sensors. Such fields find their power in the laws of Quantum Mechanics and particularly in the non-classical resource of entanglement. The generation, the distribution of such resources, as well as their implementation to enhance the classical limits is a fundamental direction of Quantum Information, representing the purpose of my Ph.D.. During this thesis work, these two fields have been intensively studied exploiting Quantum Optics as the main framework for their optimal experimental investigation. Indeed, photons provide a variety of solutions that can be opportunely chosen according to the specific task. Furthermore, photons are currently the only feasible flying qubits, which give access to quantum communication between distant parties. In my Ph.D. thesis different contributions have been experimentally demonstrated for both Quantum Communication [10, 11, 12, 13] and Metrology [14, 15, 16, 17]. Moreover, a review on the state-of-the-art in Photonic Quantum Metrology has been realized [1].

In Quantum Communication the role of entanglement has been largely shown and studied for different scenarios. In Sec. 2.2 it is shown how to generate entanglement in telecom wavelength — the most suitable region to enable fiber communication — using an integrated photonic platform realized in femtosecond laser writing [10]. The hybrid and modular approaches of such device, together with the presence of a tunable element, i.e. an integrated phase shifter, allow the preparation of several output states; such states are even encoded using different degrees of freedom of light, that are photon path and polarization. This realization has potentially a plethora of future applications, since it is compatible with fiber networks and suitable for possible all-in-chip circuits, simply by adding components in the same modular fashion. A second telecom distribution of quantum resources is presented in Sec. 2.3. Here, the distribution of a hybrid entangled state is demonstrated, i.e., exploiting different properties of the same photon. Specifically, after the generation of the photon pair in the telecom regime, the polarization of one photon is quantum correlated with the vector vortex state of the second one. The latter is a further entanglement between its OAM and polarization degrees of freedom. Such state has been successfully transmitted through a particular fiber, namely the air-core fiber, preserving its quantum properties [11]. Indeed, the involved spatial transverse profile is peculiar due to the presence of a non-zero OAM quantum. Thus standard single-mode fibers can not be used for this task. This work not only improves the research for hybrid entangled state exchange between distant parties, but also paves the way to high-dimensional entanglement distribution in future quantum networks, where telecom generation of OAM quantum states can be interfaced with OAM-supporting fibers. Then, more complex structures have been investigated

where to distribute photonic entanglement. First, a photonic star-shaped quantum network was experimentally realized in [12] (Sec. 2.4). This scenario was achieved using up to four different laboratories, each containing an independent source of entangled photons. We successfully certified the presence of distributed multipartite entanglement in the system by adopting generalized Bell-like inequalities. Finally, the entanglement distribution between two parties more than 250 m apart led to the realization of a QKD protocol based on a modified version of Ekert91 (Sec. 2.5). This contribution represents the first realization in the field that exploits the quantum dot (QD) as a single-photon source to generate the distributed quantum state [13]. The QD aims to have a deterministic generation in the future. The same experiment has been realized using two different quantum channels: a fiber link and a free-space connection between two buildings, belonging to the Physics Department of Sapienza University of Rome. Remarkably, the last solution represents an urban free-space channel. The achieved results demonstrated that QD technology represents a promising solution for real-life secure quantum communication: it is mature to be used outside the laboratory, enabling QKD in both fiber and free-space links, as well as it can be interfaced with other quantum systems.

In Quantum Metrology, the realized review work [1] analyzes the state-of-the-art in Photonic Quantum Metrology. It first introduces the basic concepts of Quantum Metrology for experimental implementations and then reviews existing photonic solutions. Here, the problem of phase estimation is discussed, together with the role of the adaptive approach during the learning process and the multiparameter scenario, which to date shows surprisingly few experimental investigations. Elements of this review work have been used to introduce the Chapter 3 and integrating the subsequent experimental results achieved. Besides the review contribution, several works have been demonstrated in the context of phase estimation. First of all, it was realized the first quantum sensor capable of attaining quantum enhancement for a two-phase estimation problem (Sec. 3.2.1). In [14] such device has been characterized in both classical and quantum regimes, thus revealing its actual potential. The platform is an integrated interferometer with highly reconfigurable capabilities, thanks to the presence of several phase shifters. This sensor has been used to investigate multiphase estimation protocols in the adaptive online regime (Sec. 3.3.2). Thus, different machine learning-based algorithms for the Bayesian learning framework were studied and tested with simulations in the online mode. Then, the best one was employed to demonstrate the actual experimental realization with the aforementioned integrated platform [15]. Furthermore, if one is interested in the realization of a quantum sensor, a key aspect concerns the characterization of its response. In Sec. 3.2.2, we demonstrated how to tackle this problem for our device using a Neural Network attaining reliable performances [16]. A final contribution dealt with the adaptive single-phase estimation (Sec. 3.3.1). Here, an offline algorithm was studied to increase the performance in estimating a single phase inside a two-mode MZI in polarization [17]. The technique investigated is a genetic algorithm inspired by the natural selection process, in order to deal with the search for optimal solutions within an extremely large search space. All the results described within the framework of phase estimation represent benchmark scenarios for single and multiparameter problems, providing testbeds for a great number of applications. They show the attempt to face a multiparameter quantum sensor in a regime of single photons, studying the optimization of different features, from the calibration to the study of its adaptive control. In the latter, we have provided contributions in both online and offline approaches, thus increasing the optimization of estimation problems in the limited data regime. This task is particularly relevant

for the adaptive multiphase scenario, where optimizing the simultaneous estimation of multiple unknown parameters is far from obvious.

Bibliography

[1] Emanuele Polino, Mauro Valeri, Nicolò Spagnolo, and Fabio Sciarrino. Photonic quantum metrology. *AVS Quantum Science*, 2(2):024703, 2020.

[2] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Advances in quantum metrology. *Nature Photonics*, 5(4):222, 2011.

[3] Nicolas Gisin and Rob Thew. Quantum communication. *Nature photonics*, 1(3):165–171, 2007.

[4] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301, 2009.

[5] Fulvio Flamini, Nicolo Spagnolo, and Fabio Sciarrino. Photonic quantum information processing: a review. *Reports on Progress in Physics*, 82(1):016001, 2018.

[6] Daniele Cozzolino, Beatrice Da Lio, Davide Bacco, and Leif Katsuo Oxenløwe. High-dimensional quantum communication: Benefits, progress, and future challenges. *Advanced Quantum Technologies*, 2(12):1900038, 2019.

[7] John S Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

[8] Daniel Cavalcanti, Mafalda L Almeida, Valerio Scarani, and Antonio Acin. Quantum networks reveal quantum nonlocality. *Nature communications*, 2(1):1–6, 2011.

[9] H Jeff Kimble. The quantum internet. *Nature*, 453(7198):1023–1030, 2008.

[10] Simone Atzeni, Adil S. Rab, Giacomo Corrielli, Emanuele Polino, Mauro Valeri, Paolo Mataloni, Nicolò Spagnolo, Andrea Crespi, Fabio Sciarrino, and R. Osellame. Integrated sources of entangled photons at the telecom wavelength in femtosecond-laser-written circuits. *Optica*, 5(3), 2018.

[11] Daniele Cozzolino, Emanuele Polino, Mauro Valeri, Gonzalo Carvacho, Davide Bacco, Nicolò Spagnolo, Leif K Oxenløwe, and Fabio Sciarrino. Air-core fiber distribution of hybrid vector vortex-polarization entangled states. *Advanced Photonics*, 1(4):046005, 2019.

[12] Davide Poderini, Iris Agresti, Guglielmo Marchese, Emanuele Polino, Taira Giordani, Alessia Suprano, Mauro Valeri, Giorgio Milani, Nicolò Spagnolo, Gonzalo Carvacho, et al. Experimental violation of n-locality in a star quantum network. *Nature communications*, 11(1):1–8, 2020.

[13] Francesco Basso Basset, Mauro Valeri, Emanuele Roccia, Valerio Muredda, Davide Poderini, Julia Neuwirth, Nicolò Spagnolo, Michele B. Rota, Gonzalo Carvacho, Fabio Sciarrino, and Rinaldo Trotta. Quantum key distribution with entangled photons generated on demand by a quantum dot. *Science Advances*, 7(12), 2021.

[14] Emanuele Polino, Martina Riva, Mauro Valeri, Raffaele Silvestri, Giacomo Corrielli, Andrea Crespi, Nicolò Spagnolo, Roberto Osellame, and Fabio Sciarrino. Experimental multiphase estimation on a chip. *Optica*, 6(3):288–295, 2019.

[15] Mauro Valeri, Emanuele Polino, Davide Poderini, Ilaria Gianani, Giacomo Corrielli, Andrea Crespi, Roberto Osellame, Nicolò Spagnolo, and Fabio Sciarrino. Experimental adaptive bayesian estimation of multiple phases with limited data. *npj Quantum Information*, 6(92):1–11, 2020.

[16] Valeria Cimini, Emanuele Polino, Mauro Valeri, Ilaria Gianani, Nicolò Spagnolo, Giacomo Corrielli, Andrea Crespi, Roberto Osellame, Marco Barbieri, and Fabio Sciarrino. Calibration of multiparameter sensors via machine learning at the single-photon level. *Physical Review Applied*, 2020.

[17] Kartikeya Rambhatla, Simone Evaldo D'Aurelio, Mauro Valeri, Emanuele Polino, Nicolò Spagnolo, and Fabio Sciarrino. Adaptive phase estimation through a genetic algorithm. *Physical Review Research*, 2(3):033078, 2020.

[18] Jonathan P Dowling and Gerard J Milburn. Quantum technology: the second quantum revolution. *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 361(1809):1655–1674, 2003.

[19] Thaddeus D Ladd, Fedor Jelezko, Raymond Laflamme, Yasunobu Nakamura, Christopher Monroe, and Jeremy Lloyd O'Brien. Quantum computers. *Nature*, 464(7285):45–53, 2010.

[20] Justin B Spring, Benjamin J Metcalf, Peter C Humphreys, W Steven Kolthammer, Xian-Min Jin, Marco Barbieri, Animesh Datta, Nicholas Thomas-Peter, Nathan K Langford, Dmytro Kundys, et al. Boson sampling on a photonic chip. *Science*, 339(6121):798–801, 2013.

[21] Max Tillmann, Borivoje Dakić, René Heilmann, Stefan Nolte, Alexander Szameit, and Philip Walther. Experimental boson sampling. *Nature photonics*, 7(7):540–544, 2013.

[22] Andrea Crespi, Roberto Osellame, Roberta Ramponi, Daniel J Brod, Ernesto F Galvao, Nicolo Spagnolo, Chiara Vitelli, Enrico Maiorino, Paolo Mataloni, and Fabio Sciarrino. Integrated multimode interferometers with arbitrary designs for photonic boson sampling. *Nature photonics*, 7(7):545–549, 2013.

[23] Matthew A Broome, Alessandro Fedrizzi, Saleh Rahimi-Keshari, Justin Dove, Scott Aaronson, Timothy C Ralph, and Andrew G White. Photonic boson sampling in a tunable circuit. *Science*, 339(6121):794–798, 2013.

[24] Alberto Peruzzo, Mirko Lobino, Jonathan CF Matthews, Nobuyuki Matsuda, Alberto Politi, Konstantinos Poulios, Xiao-Qi Zhou, Yoav Lahini, Nur Ismail, Kerstin Wörhoff, et al. Quantum walks of correlated photons. *Science*, 329(5998):1500–1503, 2010.

[25] Linda Sansoni, Fabio Sciarrino, Giuseppe Vallone, Paolo Mataloni, Andrea Crespi, Roberta Ramponi, and Roberto Osellame. Two-particle bosonic-fermionic quantum walk via integrated photonics. *Physical review letters*, 108(1):010502, 2012.

[26] Andrea Crespi, Roberto Osellame, Roberta Ramponi, Vittorio Giovannetti, Rosario Fazio, Linda Sansoni, Francesco De Nicola, Fabio Sciarrino, and Paolo Mataloni. Anderson localization of entangled photons in an integrated quantum walk. *Nature Photonics*, 7(4):322–328, 2013.

[27] Pieter Kok, William J Munro, Kae Nemoto, Timothy C Ralph, Jonathan P Dowling, and Gerard J Milburn. Linear optical quantum computing with photonic qubits. *Reviews of Modern Physics*, 79(1):135, 2007.

[28] Jacques Carolan, Christopher Harrold, Chris Sparrow, Enrique Martín-López, Nicholas J Russell, Joshua W Silverstone, Peter J Shadbolt, Nobuyuki Matsuda, Manabu Oguma, Mikitaka Itoh, et al. Universal linear optics. *Science*, 349(6249):711–716, 2015.

[29] P Coullet, L Gil, and F Rocca. Optical vortices. *Optics Communications*, 73(5):403–408, 1989.

[30] M Brambilla, F Battipede, LA Lugiato, V Penna, F Prati, Chr Tamm, and CO Weiss. Transverse laser patterns. i. phase singularity crystals. *Physical Review A*, 43(9):5090, 1991.

[31] M Brambilla, LA Lugiato, V Penna, F Prati, Chr Tamm, and CO Weiss. Transverse laser patterns. ii. variational principle for pattern selection, spatial multistability, and laser hydrodynamics. *Physical Review A*, 43(9):5114, 1991.

[32] Les Allen, Marco W Beijersbergen, RJC Spreeuw, and JP Woerdman. Orbital angular momentum of light and the transformation of laguerre-gaussian laser modes. *Physical review A*, 45(11):8185, 1992.

[33] Stephen M Barnett, Mohamed Babiker, and Miles J Padgett. Optical orbital angular momentum, 2017.

[34] Anthony E Siegman. Lasers university science books. *Mill Valley, CA*, 37(208):169, 1986.

[35] Ebrahim Karimi. *Generation and manipulation of laser beams carrying orbital angular momentum for classical and quantum information applications*. PhD thesis, Ph. D. dissertation (Universita degli studi di Napoli "Federico II", 2009.

[36] Robert W Boyd. *Nonlinear optics*. Academic press, 2020.

[37] NR Heckenberg, R McDuff, CP Smith, and AG White. Generation of optical phase singularities by computer-generated holograms. *Optics letters*, 17(3):221–223, 1992.

[38] Lorenzo Marrucci, Carlo Manzo, and Domenico Paparo. Optical spin-to-orbital angular momentum conversion in inhomogeneous anisotropic media. *Physical review letters*, 96(16):163905, 2006.

[39] Marco W Beijersbergen, Les Allen, HELO Van der Veen, and JP Woerdman. Astigmatic laser mode converters and transfer of orbital angular momentum. *Optics Communications*, 96(1-3):123–132, 1993.

[40] MW Beijersbergen, RPC Coerwinkel, M Kristensen, and JP Woerdman. Helical-wavefront laser beams produced with a spiral phaseplate. *Optics communications*, 112(5-6):321–327, 1994.

[41] Jonathan Leach, Miles J Padgett, Stephen M Barnett, Sonja Franke-Arnold, and Johannes Courtial. Measuring the orbital angular momentum of a single photon. *Physical review letters*, 88(25):257901, 2002.

[42] S Slussarenko, Vincenzo D'Ambrosio, Bruno Piccirillo, Lorenzo Marrucci, and Enrico Santamato. The polarizing sagnac interferometer: a tool for light orbital angular momentum sorting and spin-orbit photon processing. *Optics Express*, 18(26):27205–27216, 2010.

[43] Martin PJ Lavery, David J Robertson, Gregorius CG Berkhout, Gordon D Love, Miles J Padgett, and Johannes Courtial. Refractive elements for the measurement of the orbital angular momentum of a single photon. *Optics express*, 20(3):2110–2115, 2012.

[44] Sergei Slussarenko and Geoff J Pryde. Photonic quantum information processing: A concise review. *Applied Physics Reviews*, 6(4):041303, 2019.

[45] Jeremy L O'brien, Akira Furusawa, and Jelena Vučković. Photonic quantum technologies. *Nature Photonics*, 3(12):687–695, 2009.

[46] Sébastien Tanzilli, Anthony Martin, Florian Kaiser, Marc P De Micheli, Olivier Alibart, and Daniel B Ostrowsky. On the genesis and evolution of integrated quantum optics. *Laser & Photonics Reviews*, 6(1):115–143, 2012.

[47] Adeline Orieux and Eleni Diamanti. Recent advances on integrated quantum communications. *Journal of Optics*, 18(8):083002, 2016.

[48] Simeon Bogdanov, MY Shalaginov, Alexandra Boltasseva, and Vladimir M Shalaev. Material platforms for integrated quantum photonics. *Optical Materials Express*, 7(1):111–132, 2017.

[49] Jianwei Wang, Alberto Santamato, Pisu Jiang, Damien Bonneau, Erman Engin, Joshua W Silverstone, Matthias Lermer, Johannes Beetz, Martin Kamp, Sven Höfling, et al. Gallium arsenide (gaas) quantum photonic waveguide circuits. *Optics Communications*, 327:49–55, 2014.

[50] Chi Xiong, Wolfram Pernice, Kevin K Ryu, Carsten Schuck, King Y Fong, Tomas Palacios, and Hong X Tang. Integrated gan photonic circuits on silicon (100) for second harmonic generation. *Optics express*, 19(11):10462–10470, 2011.

[51] Carlos Abellan, Waldimar Amaya, David Domenech, Pascual Muñoz, Jose Capmany, Stefano Longhi, Morgan W Mitchell, and Valerio Pruneri. Quantum entropy source on an inp photonic integrated circuit for random number generation. *Optica*, 3(9):989–994, 2016.

[52] Adeline Orieux, Andreas Eckstein, Aristide Lemaître, Pascal Filloux, Ivan Favero, Giuseppe Leo, Thomas Coudreau, Arne Keller, Pérola Milman, and Sara Ducci. Direct bell states generation on a iii-v semiconductor chip at room temperature. *Physical review letters*, 110(16):160502, 2013.

[53] Christof P Dietrich, Andrea Fiore, Mark G Thompson, Martin Kamp, and Sven Höfling. Gaas integrated quantum photonics: Towards compact and multi-functional quantum photonic integrated circuits. *Laser & Photonics Reviews*, 10(6):870–894, 2016.

[54] Brian J Smith, Dmytro Kundys, Nicholas Thomas-Peter, PGR Smith, and IA Walmsley. Phase-controlled integrated photonic quantum circuits. *Optics Express*, 17(16):13516–13525, 2009.

[55] Dmytro O Kundys, James C Gates, Sonali Dasgupta, Corin BE Gawith, and Peter GR Smith. Use of cross-couplers to decrease size of uv written photonic circuits. *IEEE Photonics Technology Letters*, 21(13):947–949, 2009.

[56] Giuseppe Della Valle, Roberto Osellame, and Paolo Laporta. Micromachining of photonic devices by femtosecond laser pulses. *Journal of Optics A: Pure and Applied Optics*, 11(1):013001, 2008.

[57] Thomas Meany, Markus Gräfe, René Heilmann, Armando Perez-Leija, Simon Gross, Michael J Steel, Michael J Withford, and Alexander Szameit. Laser written circuits for quantum photonics. *Laser & Photonics Reviews*, 9(4):363–384, 2015.

[58] Roberto Osellame, Stefano Taccheo, Marco Marangoni, Roberta Ramponi, Paolo Laporta, Dario Polli, Sandro De Silvestri, and Giulio Cerullo. Femtosecond writing of active optical waveguides with astigmatically shaped beams. *JOSA B*, 20(7):1559–1567, 2003.

[59] Martin Ams, GD Marshall, DJ Spence, and MJ Withford. Slit beam shaping method for femtosecond laser direct-write fabrication of symmetric waveguides in bulk glasses. *Optics express*, 13(15):5676–5681, 2005.

[60] Rafael R Gattass and Eric Mazur. Femtosecond laser micromachining in transparent materials. *Nature photonics*, 2(4):219–225, 2008.

[61] Joshua W Silverstone, J Wang, D Bonneau, P Sibson, R Santagati, C Erven, JL O'Brien, and MG Thompson. Silicon quantum photonics. In *2016 International Conference on Optical MEMS and Nanophotonics (OMN)*, pages 1–2. IEEE, 2016.

[62] Alberto Politi, Martin J Cryan, John G Rarity, Siyuan Yu, and Jeremy L O'brien. Silica-on-silicon waveguide quantum circuits. *Science*, 320(5876):646–649, 2008.

[63] Alberto Politi, Jonathan CF Matthews, Mark G Thompson, and Jeremy L O'Brien. Integrated quantum photonics. *IEEE Journal of Selected Topics in Quantum Electronics*, 15(6):1673–1684, 2009.

[64] Anthony Laing, Alberto Peruzzo, Alberto Politi, Maria Rodas Verde, Matthaeus Halder, Timothy C Ralph, Mark G Thompson, and Jeremy L O'Brien. High-fidelity operation of quantum photonic circuits. *Applied Physics Letters*, 97(21):211109, 2010.

[65] Peter J Shadbolt, Maria R Verde, Alberto Peruzzo, Alberto Politi, Anthony Laing, Mirko Lobino, Jonathan CF Matthews, Mark G Thompson, and Jeremy L O'Brien. Generating, manipulating and measuring entanglement and

mixture with a reconfigurable photonic circuit. *Nature Photonics*, 6(1):45–49, 2012.

[66] Alberto Peruzzo, Anthony Laing, Alberto Politi, Terry Rudolph, and Jeremy L O'brien. Multimode quantum interference of photons in multiport integrated devices. *Nature communications*, 2(1):1–6, 2011.

[67] Laurent Vivien and Lorenzo Pavesi. *Handbook of silicon photonics*. Taylor & Francis, 2016.

[68] Xiaogang Qiang, Xiaoqi Zhou, Jianwei Wang, Callum M Wilkes, Thomas Loke, Sean O'Gara, Laurent Kling, Graham D Marshall, Raffaele Santagati, Timothy C Ralph, et al. Large-scale silicon quantum photonics implementing arbitrary two-qubit processing. *Nature photonics*, 12(9):534–539, 2018.

[69] Sailong Wu, Xin Mu, Lirong Cheng, Simei Mao, and HY Fu. State-of-the-art and perspectives on silicon waveguide crossings: A review. *Micromachines*, 11(3):326, 2020.

[70] Joshua W Silverstone, Damien Bonneau, Kazuya Ohira, Nob Suzuki, Haruhiko Yoshida, Norio Iizuka, Mizunori Ezaki, Chandra M Natarajan, Michael G Tanner, Robert H Hadfield, et al. On-chip quantum interference between silicon photon-pair sources. *Nature Photonics*, 8(2):104–108, 2014.

[71] Joshua W Silverstone, Raffaele Santagati, Damien Bonneau, Michael J Strain, Marc Sorel, Jeremy L O'Brien, and Mark G Thompson. Qubit entanglement between ring-resonator photon-pair sources on a silicon chip. *Nature communications*, 6(1):1–7, 2015.

[72] Jay E Sharping, Kim Fook Lee, Mark A Foster, Amy C Turner, Bradley S Schmidt, Michal Lipson, Alexander L Gaeta, and Prem Kumar. Generation of correlated photons in nanoscale silicon waveguides. *Optics express*, 14(25):12388–12393, 2006.

[73] Marcelo Davanco, Jun Rong Ong, Andrea Bahgat Shehata, Alberto Tosi, Imad Agha, Solomon Assefa, Fengnian Xia, William MJ Green, Shayan Mookherjea, and Kartik Srinivasan. Telecommunications-band heralded single photons from a silicon nanophotonic chip. *Applied Physics Letters*, 100(26):261104, 2012.

[74] Iman Esmaeil Zadeh, Ali W Elshaari, Klaus D Jons, Andreas Fognini, Dan Dalacu, Philip J Poole, Michael E Reimer, and Val Zwiller. Deterministic integration of single photon sources in silicon based photonic circuits. *Nano Letters*, 16(4):2289–2294, 2016.

[75] Svetlana Khasminskaya, Felix Pyatkov, Karolina Słowik, Simone Ferrari, Oliver Kahl, Vadim Kovalyuk, Patrik Rath, Andreas Vetter, Frank Hennrich, Manfred M Kappes, et al. Fully integrated quantum photonic circuit with an electrically driven light source. *Nature Photonics*, 10(11):727–732, 2016.

[76] Lucia Caspani, Chunle Xiong, Benjamin J Eggleton, Daniele Bajoni, Marco Liscidini, Matteo Galli, Roberto Morandotti, and David J Moss. Integrated sources of photon quantum states based on nonlinear optics. *Light: Science & Applications*, 6(11):e17100–e17100, 2017.

[77] Evan Meyer-Scott, Nidhin Prasannan, Christof Eigner, Viktor Quiring, John M Donohue, Sonja Barkhofen, and Christine Silberhorn. High-performance source of spectrally pure, polarization entangled photon pairs based on hybrid integrated-bulk optics. *Optics express*, 26(25):32475–32490, 2018.

[78] Justin B Spring, Paolo L Mennea, Benjamin J Metcalf, Peter C Humphreys, James C Gates, Helen L Rogers, Christoph Söller, Brian J Smith, W Steven Kolthammer, Peter GR Smith, et al. Chip-based array of near-identical, pure, heralded single-photon sources. *Optica*, 4(1):90–96, 2017.

[79] Yuan Chen, Jun Gao, Zhi-Qiang Jiao, Ke Sun, Wei-Guan Shen, Lu-Feng Qiao, Hao Tang, Xiao-Feng Lin, and Xian-Min Jin. Mapping twisted light into and out of a photonic chip. *Physical Review Letters*, 121(23):233602, 2018.

[80] Xinlun Cai, Jianwei Wang, Michael J Strain, Benjamin Johnson-Morris, Jiangbo Zhu, Marc Sorel, Jeremy L O'Brien, Mark G Thompson, and Siyuan Yu. Integrated compact optical vortex beam emitters. *Science*, 338(6105):363–366, 2012.

[81] Jun Liu, Shi-Mao Li, Long Zhu, An-Dong Wang, Shi Chen, Charalambos Klitis, Cheng Du, Qi Mo, Marc Sorel, Si-Yuan Yu, et al. Direct fiber vector eigenmode multiplexing transmission seeded by integrated optical vortex emitters. *Light: Science & Applications*, 7(3):17148–17148, 2018.

[82] C Xiong, X Zhang, A Mahendra, J He, D-Y Choi, CJ Chae, D Marpaung, Arne Leinse, RG Heideman, M Hoekman, et al. Compact and reconfigurable silicon nitride time-bin entanglement circuit. *Optica*, 2(8):724–727, 2015.

[83] Simone Ferrari, Carsten Schuck, and Wolfram Pernice. Waveguide-integrated superconducting nanowire single-photon detectors. *Nanophotonics*, 7(11):1725–1758, 2018.

[84] Faraz Najafi, Jacob Mower, Nicholas C Harris, Francesco Bellei, Andrew Dane, Catherine Lee, Xiaolong Hu, Prashanta Kharel, Francesco Marsili, Solomon Assefa, et al. On-chip detection of non-classical light by scalable integration of single-photon detectors. *Nature communications*, 6(1):1–8, 2015.

[85] Julian Münzberg, Andreas Vetter, Fabian Beutel, Wladick Hartmann, Simone Ferrari, Wolfram HP Pernice, and Carsten Rockstuhl. Superconducting nanowire single-photon detector implemented in a 2d photonic crystal cavity. *Optica*, 5(5):658–665, 2018.

[86] Jan Philipp Höpker, Thomas Gerrits, Adriana Lita, Stephan Krapick, Harald Herrmann, Raimund Ricken, Viktor Quiring, Richard Mirin, Sae Woo Nam, Christine Silberhorn, et al. Integrated transition edge sensors on lithium niobate waveguides. *arXiv preprint arXiv:1812.08483*, 2018.

[87] Brice Calkins, Paolo L Mennea, Adriana E Lita, Benjamin J Metcalf, W Steven Kolthammer, Antia Lamas-Linares, Justin B Spring, Peter C Humphreys, Richard P Mirin, James C Gates, et al. High quantum-efficiency photon-number-resolving detector for photonic on-chip information processing. *Optics express*, 21(19):22657–22670, 2013.

[88] Ivan B Djordjevic. On global quantum communication networking. *Entropy*, 22(8):831, 2020.

[89] Siddarth Koduru Joshi, Djeylan Aktas, Sören Wengerowsky, Martin Lončarić, Sebastian Philipp Neumann, Bo Liu, Thomas Scheidl, Guillermo Currás Lorenzo, Željko Samec, Laurent Kling, et al. A trusted node–free eight-user metropolitan quantum communication network. *Science advances*, 6(36):eaba0959, 2020.

[90] Sheng-Kai Liao, Hai-Lin Yong, Chang Liu, Guo-Liang Shentu, Dong-Dong Li, Jin Lin, Hui Dai, Shuang-Qiang Zhao, Bo Li, Jian-Yu Guan, et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nature Photonics*, 11(8):509–513, 2017.

[91] Majid Safari and Murat Uysal. Relay-assisted free-space optical communication. *IEEE Transactions on Wireless Communications*, 7(12):5441–5449, 2008.

[92] Vincent WS Chan. Free-space optical communications. *Journal of Lightwave technology*, 24(12):4750–4762, 2006.

[93] Samuraí Brito, Askery Canabarro, Daniel Cavalcanti, and Rafael Chaves. Satellite-based photonic quantum networks are small-world. *PRX Quantum*, 2(1):010304, 2021.

[94] Xin Cao, Michael Zopf, and Fei Ding. Telecom wavelength single photon sources. *Journal of Semiconductors*, 40(7):071901, 2019.

[95] H-J Briegel, Wolfgang Dür, Juan I Cirac, and Peter Zoller. Quantum repeaters: the role of imperfect local operations in quantum communication. *Physical Review Letters*, 81(26):5932, 1998.

[96] L-M Duan, Mikhail D Lukin, J Ignacio Cirac, and Peter Zoller. Long-distance quantum communication with atomic ensembles and linear optics. *Nature*, 414(6862):413–418, 2001.

[97] Nicolas Sangouard, Christoph Simon, Hugues De Riedmatten, and Nicolas Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Reviews of Modern Physics*, 83(1):33, 2011.

[98] Sreraman Muralidharan, Jungsang Kim, Norbert Lütkenhaus, Mikhail D Lukin, and Liang Jiang. Ultrafast and fault-tolerant quantum communication across long distances. *Physical review letters*, 112(25):250501, 2014.

[99] Juan Yin, Yu-Huai Li, Sheng-Kai Liao, Meng Yang, Yuan Cao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Shuang-Lin Li, et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature*, pages 1–5, 2020.

[100] Sheng-Kai Liao, Wen-Qi Cai, Johannes Handsteiner, Bo Liu, Juan Yin, Liang Zhang, Dominik Rauch, Matthias Fink, Ji-Gang Ren, Wei-Yue Liu, et al. Satellite-relayed intercontinental quantum network. *Physical review letters*, 120(3):030501, 2018.

[101] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, et al. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[102] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, et al. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, 2017.

[103] Giuseppe Vallone, Davide Bacco, Daniele Dequal, Simone Gaiarin, Vincenza Luceri, Giuseppe Bianco, and Paolo Villoresi. Experimental satellite quantum communications. *Physical Review Letters*, 115(4):040502, 2015.

[104] Jian-Wei Pan, Christoph Simon, Časlav Brukner, and Anton Zeilinger. Entanglement purification for quantum communication. *Nature*, 410(6832):1067–1070, 2001.

[105] Jian-Wei Pan, Sara Gasparoni, Rupert Ursin, Gregor Weihs, and Anton Zeilinger. Experimental entanglement purification of arbitrary unknown states. *Nature*, 423(6938):417–422, 2003.

[106] Marek Żukowski, Anton Zeilinger, Michael A Horne, and Artur K Ekert. "event-ready-detectors"bell experiment via entanglement swapping. *Physical Review Letters*, 71(26):4287, 1993.

[107] Jian-Wei Pan, Dik Bouwmeester, Harald Weinfurter, and Anton Zeilinger. Experimental entanglement swapping: entangling photons that never interacted. *Physical review letters*, 80(18):3891, 1998.

[108] Chin-Wen Chou, Julien Laurat, Hui Deng, Kyung Soo Choi, Hugues De Riedmatten, Daniel Felinto, and H Jeff Kimble. Functional quantum nodes for entanglement distribution over scalable quantum networks. *Science*, 316(5829):1316–1320, 2007.

[109] David L Moehring, Peter Maunz, Steve Olmschenk, Kelly C Younge, Dzmitry N Matsukevich, L-M Duan, and Christopher Monroe. Entanglement of single-atom quantum bits at a distance. *Nature*, 449(7158):68–71, 2007.

[110] Zhen-Sheng Yuan, Yu-Ao Chen, Bo Zhao, Shuai Chen, Jörg Schmiedmayer, and Jian-Wei Pan. Experimental demonstration of a bdcz quantum repeater node. *Nature*, 454(7208):1098–1101, 2008.

[111] Emanuele Polino, Giacomo Corrielli, Andrea Crespi, Nicolò Spagnolo, Roberto Osellame, and Fabio Sciarrino. Platforms for telecom entangled photon sources. *Schoolof Physics "Nanoscale Quantum Optics"*, 2019.

[112] Roberto Osellame, Giulio Cerullo, and Roberta Ramponi. *Femtosecond laser micromachining: photonic and microfluidic devices in transparent materials*, volume 123. Springer Science & Business Media, 2012.

[113] Giacomo Corrielli, Andrea Crespi, Riccardo Geremia, Roberta Ramponi, Linda Sansoni, Andrea Santinelli, Paolo Mataloni, Fabio Sciarrino, and Roberto Osellame. Rotated waveplates in integrated waveguide optics. *Nature communications*, 5(1):1–6, 2014.

[114] Luís A Fernandes, Jason R Grenier, Peter R Herman, J Stewart Aitchison, and Paulo VS Marques. Femtosecond laser fabrication of birefringent directional couplers as polarization beam splitters in fused silica. *Optics express*, 19(13):11992–11999, 2011.

[115] Andrea Crespi, Roberta Ramponi, Roberto Osellame, Linda Sansoni, Irene Bongioanni, Fabio Sciarrino, Giuseppe Vallone, and Paolo Mataloni. Integrated photonic quantum gates for polarization qubits. *Nature communications*, 2(1):1–6, 2011.

[116] René Heilmann, Markus Gräfe, Stefan Nolte, and Alexander Szameit. Arbitrary photonic wave plate operations on chip: Realizing hadamard, pauli-x, and rotation gates for polarisation qubits. *Scientific reports*, 4:4118, 2014.

[117] Ci-Yu Wang, Jun Gao, and Xian-Min Jin. On-chip rotated polarization directional coupler fabricated by femtosecond laser direct writing. *Optics letters*, 44(1):102–105, 2019.

[118] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660):575–579, 1997.

[119] Hugues de Riedmatten, Ivan Marcikic, JAW Van Houwelingen, Wolfgang Tittel, Hugo Zbinden, and Nicolas Gisin. Long-distance entanglement swapping with photons from separated sources. *Physical Review A*, 71(5):050302, 2005.

[120] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of modern physics*, 74(1):145, 2002.

[121] Jeremy L O'Brien, Geoffrey J Pryde, Andrew G White, Timothy C Ralph, and David Branning. Demonstration of an all-optical quantum controlled-not gate. *Nature*, 426(6964):264–267, 2003.

[122] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[123] Artur K Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6):661, 1991.

[124] Bas Hensen, Hannes Bernien, Anaïs E Dréau, Andreas Reiserer, Norbert Kalb, Machiel S Blok, Just Ruitenberg, Raymond FL Vermeulen, Raymond N Schouten, Carlos Abellán, et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.

[125] Marissa Giustina, Marijn AM Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, et al. Significant-loophole-free test of bell's theorem with entangled photons. *Physical review letters*, 115(25):250401, 2015.

[126] Lynden K Shalm, Evan Meyer-Scott, Bradley G Christensen, Peter Bierhorst, Michael A Wayne, Martin J Stevens, Thomas Gerrits, Scott Glancy, Deny R Hamel, Michael S Allman, et al. Strong loophole-free test of local realism. *Physical review letters*, 115(25):250402, 2015.

[127] Wenjamin Rosenfeld, Daniel Burchardt, Robert Garthoff, Kai Redeker, Norbert Ortegel, Markus Rau, and Harald Weinfurter. Event-ready bell test using entangled atoms simultaneously closing detection and locality loopholes. *Physical review letters*, 119(1):010402, 2017.

[128] BIG Bell Test Collaboration et al. Challenging local realism with human choices. *Nature*, 557(7704):212, 2018.

[129] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical review letters*, 23(15):880, 1969.

[130] Boris S Cirel'son. Quantum generalizations of bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980.

[131] Antonio Acin, Nicolas Gisin, and Lluis Masanes. From bell's theorem to secure quantum key distribution. *Physical review letters*, 97(12):120405, 2006.

[132] Ernst Specker. Die logik nicht gleichzeitig entscheidbarer aussagen. In *Ernst Specker Selecta*, pages 175–182. Springer, 1990.

[133] John S Bell. On the problem of hidden variables in quantum mechanics. *Reviews of Modern Physics*, 38(3):447, 1966.

[134] Simon Kochen and Ernst P Specker. The problem of hidden variables in quantum mechanics. In *The logico-algebraic approach to quantum mechanics*, pages 293–328. Springer, 1975.

[135] Aonan Zhang, Huichao Xu, Jie Xie, Han Zhang, Brian J Smith, MS Kim, and Lijian Zhang. Experimental test of contextuality in quantum and classical systems. *Physical review letters*, 122(8):080401, 2019.

[136] Ebrahim Karimi and Robert W Boyd. Classical entanglement? *Science*, 350(6265):1172–1173, 2015.

[137] Robert JC Spreeuw. A classical analogy of entanglement. *Foundations of physics*, 28(3):361–374, 1998.

[138] Thomas Konrad and Andrew Forbes. Quantum mechanics and classical light. *Contemporary Physics*, 60(1):1–22, 2019.

[139] WH Louisell, A Yariv, and AE Siegman. Quantum fluctuations and noise in parametric processes. i. *Physical Review*, 124(6):1646, 1961.

[140] Francesco De Martini and Fabio Sciarrino. Non-linear parametric processes in quantum information. *Progress in quantum electronics*, 29(3-5):165–256, 2005.

[141] MV Jabir and GK Samanta. Robust, high brightness, degenerate entangled photon source at room temperature. *Scientific Reports*, 7(1):1–8, 2017.

[142] Paul G Kwiat, Edo Waks, Andrew G White, Ian Appelbaum, and Philippe H Eberhard. Ultrabright source of polarization-entangled photons. *Physical Review A*, 60(2):R773, 1999.

[143] Paul G Kwiat, Klaus Mattle, Harald Weinfurter, Anton Zeilinger, Alexander V Sergienko, and Yanhua Shih. New high-intensity source of polarization-entangled photon pairs. *Physical Review Letters*, 75(24):4337, 1995.

[144] Marco Fiorentino, Gaétan Messin, Christopher E Kuklewicz, Franco NC Wong, and Jeffrey H Shapiro. Generation of ultrabright tunable polarization entanglement without spatial, spectral, or temporal constraints. *Physical Review A*, 69(4):041801, 2004.

[145] Terence E Stuart, Joshua A Slater, Félix Bussières, and Wolfgang Tittel. Flexible source of nondegenerate entangled photons based on a two-crystal sagnac interferometer. *Physical Review A*, 88(1):012301, 2013.

[146] Han Chuen Lim, Akio Yoshizawa, Hidemi Tsuchida, and Kazuro Kikuchi. Stable source of high quality telecom-band polarization-entangled photon-pairs based on a single, pulse-pumped, short ppln waveguide. *Optics express*, 16(17):12460–12468, 2008.

[147] Taehyun Kim, Marco Fiorentino, and Franco NC Wong. Phase-stable source of polarization-entangled photons using a polarization sagnac interferometer. *Physical Review A*, 73(1):012316, 2006.

[148] Fabian Steinlechner, Sven Ramelow, Marc Jofre, Marta Gilaberte, Thomas Jennewein, Juan P Torres, Morgan W Mitchell, and Valerio Pruneri. Phase-stable source of polarization-entangled photons in a linear double-pass configuration. *Optics express*, 21(10):11943–11951, 2013.

[149] Christopher E Kuklewicz, Marco Fiorentino, Gaétan Messin, Franco NC Wong, and Jeffrey H Shapiro. High-flux source of polarization-entangled photons from a periodically poled ktiopo 4 parametric down-converter. *Physical Review A*, 69(1):013807, 2004.

[150] Miloslav Dušek, Ondřej Haderka, and Martin Hendrych. Generalized beam-splitting attack in quantum cryptography with dim coherent states. *Optics communications*, 169(1-6):103–108, 1999.

[151] Norbert Lütkenhaus and Mika Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4(1):44, 2002.

[152] Peter Lodahl. Quantum-dot based photonic quantum networks. *Quantum Science and Technology*, 3(1):013001, 2017.

[153] Sven Rodt, Stephan Reitzenstein, and Tobias Heindel. Deterministically fabricated solid-state quantum-light sources. *Journal of Physics: Condensed Matter*, 32(15):153003, 2020.

[154] N Akopian, NH Lindner, E Poem, Y Berlatzky, J Avron, D Gershoni, BD Gerardot, and PM Petroff. Entangled photon pairs from semiconductor quantum dots. *Physical review letters*, 96(13):130501, 2006.

[155] Robert J Young, R Mark Stevenson, Paola Atkinson, Ken Cooper, David A Ritchie, and Andrew J Shields. Improved fidelity of triggered entangled photons from single quantum dots. *New Journal of Physics*, 8(2):29, 2006.

[156] Tobias Heindel, Alexander Thoma, Martin von Helversen, Marco Schmidt, Alexander Schlehahn, Manuel Gschrey, Peter Schnauber, J-H Schulze, André Strittmatter, Jörn Beyer, et al. A bright triggered twin-photon source in the solid state. *Nature communications*, 8(1):1–7, 2017.

[157] Stefano T Moroni, Simone Varo, Gediminas Juska, Tung-Hsun Chung, Agnieszka Gocalinska, and Emanuele Pelucchi. Vanishing biexciton binding energy from stacked, movpe grown, site-controlled pyramidal quantum dots for twin photon generation. *Journal of Crystal Growth*, 506:36–39, 2019.

[158] R Hanbury Brown and Richard Q Twiss. A test of a new type of stellar interferometer on sirius. *Nature*, 178(4541):1046–1048, 1956.

[159] Lucas Schweickert, Klaus D Jöns, Katharina D Zeuner, Saimon Filipe Covre da Silva, Huiying Huang, Thomas Lettner, Marcus Reindl, Julien Zichi, Rinaldo Trotta, Armando Rastelli, et al. On-demand generation of background-free single photons from a solid-state source. *Applied Physics Letters*, 112(9):093106, 2018.

[160] Niccolo Somaschi, Valerian Giesz, Lorenzo De Santis, JC Loredo, Marcelo P Almeida, Gaston Hornecker, Simone Luca Portalupi, Thomas Grange, Carlos Antón, Justin Demory, et al. Near-optimal single-photon sources in the solid state. *Nature Photonics*, 10(5):340–345, 2016.

[161] Xing Ding, Yu He, Z-C Duan, Niels Gregersen, M-C Chen, S Unsleber, Sebastian Maier, Christian Schneider, Martin Kamp, Sven Höfling, et al. On-demand single photons with high extraction efficiency and near-unity indistinguishability from a resonantly driven quantum dot in a micropillar. *Physical review letters*, 116(2):020401, 2016.

[162] Yu-Ming He, Yu He, Yu-Jia Wei, Dian Wu, Mete Atatüre, Christian Schneider, Sven Höfling, Martin Kamp, Chao-Yang Lu, and Jian-Wei Pan. On-demand semiconductor single-photon source with near-unity indistinguishability. *Nature nanotechnology*, 8(3):213–217, 2013.

[163] Marta Arcari, Immo Söllner, Alisa Javadi, S Lindskov Hansen, Sahand Mahmoodian, Jin Liu, Henri Thyrrestrup, Eun Hye Lee, Jin Dong Song, Søren Stobbe, et al. Near-unity coupling efficiency of a quantum emitter to a photonic crystal waveguide. *Physical review letters*, 113(9):093603, 2014.

[164] Joël Bleuse, Julien Claudon, Megan Creasey, Nitin S Malik, Jean-Michel Gérard, Ivan Maksymov, Jean-Paul Hugonin, and Philippe Lalanne. Inhibition, enhancement, and control of spontaneous emission in photonic nanowires. *Physical review letters*, 106(10):103601, 2011.

[165] Raphaël S Daveau, Krishna C Balram, Tommaso Pregnolato, Jin Liu, Eun H Lee, Jin D Song, Varun Verma, Richard Mirin, Sae Woo Nam, Leonardo Midolo, et al. Efficient fiber-coupled single-photon source based on quantum dots in a photonic-crystal waveguide. *Optica*, 4(2):178–184, 2017.

[166] Chong-Ki Hong, Zhe-Yu Ou, and Leonard Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Physical review letters*, 59(18):2044, 1987.

[167] Daniel FV James, Paul G Kwiat, William J Munro, and Andrew G White. On the measurement of qubits. In *Asymptotic Theory of Quantum Statistical Inference: Selected Papers*, pages 509–538. World Scientific, 2005.

[168] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[169] Giacomo Torlai, Guglielmo Mazzola, Juan Carrasquilla, Matthias Troyer, Roger Melko, and Giuseppe Carleo. Neural-network quantum state tomography. *Nature Physics*, 14(5):447–450, 2018.

[170] Eliot Bolduc, Nicolas Bent, Enrico Santamato, Ebrahim Karimi, and Robert W Boyd. Exact solution to simultaneous intensity and phase encryption with a single phase-only hologram. *Optics letters*, 38(18):3546–3549, 2013.

[171] Donald Bures. An extension of kakutani's theorem on infinite product measures to the tensor product of semifinite w*-algebras. *Transactions of the American Mathematical Society*, 135:199–212, 1969.

[172] L Mančinska and S Wehner. A unified view on hardy's paradox and the clauser–horne–shimony–holt inequality. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424027, 2014.

[173] N David Mermin. Quantum mysteries refined. *American Journal of Physics*, 62(10):880–887, 1994.

[174] N David Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Physical Review Letters*, 65(15):1838, 1990.

[175] Mohammad Ardehali. Bell inequalities with a magnitude of violation that grows exponentially with the number of particles. *Physical Review A*, 46(9):5375, 1992.

[176] AV Belinskiĭ and David Nikolaevich Klyshko. Interference of light and bell's theorem. *Physics-Uspekhi*, 36(8):653, 1993.

[177] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of modern physics*, 81(2):865, 2009.

[178] Daniel M Greenberger, Michael A Horne, and Anton Zeilinger. Going beyond bell's theorem. In *Bell's theorem, quantum theory and conceptions of the universe*, pages 69–72. Springer, 1989.

[179] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2):419, 2014.

[180] Otfried Gühne and Géza Tóth. Entanglement detection. *Physics Reports*, 474(1-6):1–75, 2009.

[181] Vlatko Vedral, Martin B Plenio, Michael A Rippin, and Peter L Knight. Quantifying entanglement. *Physical Review Letters*, 78(12):2275, 1997.

[182] Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, et al. Advances in quantum cryptography. *arXiv preprint arXiv:1906.01645*, 2019.

[183] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, Guang-Bing Li, Qi-Ming Lu, Yun-Hong Gong, Yu Xu, Shuang-Lin Li, Feng-Zhi Li, Ya-Yun Yin, Zi-Qing Jiang, Ming Li, Jian-Jun Jia, Ge Ren, Dong He, Yi-Lin Zhou, Xiao-Xiang Zhang, Na Wang, Xiang Chang, Zhen-Cai Zhu, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[184] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical review letters*, 70(13):1895, 1993.

[185] Harald Weinfurter. Experimental bell-state analysis. *EPL (Europhysics Letters)*, 25(8):559, 1994.

[186] N Lütkenhaus, J Calsamiglia, and K-A Suominen. Bell measurements for teleportation. *Physical Review A*, 59(5):3295, 1999.

[187] Stefano Pirandola, Jens Eisert, Christian Weedbrook, Akira Furusawa, and Samuel L Braunstein. Advances in quantum teleportation. *Nature photonics*, 9(10):641–652, 2015.

[188] Judea Pearl. *Causality*. Cambridge university press, 2009.

[189] Gonzalo Carvacho, Francesco Andreoli, Luca Santodonato, Marco Bentivegna, Rafael Chaves, and Fabio Sciarrino. Experimental violation of local causality in a quantum network. *Nature communications*, 8(1):1–6, 2017.

[190] Dylan J Saunders, Adam J Bennet, Cyril Branciard, and Geoff J Pryde. Experimental demonstration of nonbilocal quantum correlations. *Science advances*, 3(4):e1602743, 2017.

[191] Francesco Andreoli, Gonzalo Carvacho, Luca Santodonato, Marco Bentivegna, Rafael Chaves, and Fabio Sciarrino. Experimental bilocality violation without shared reference frames. *Physical Review A*, 95(6):062315, 2017.

[192] Qi-Chao Sun, Yang-Fan Jiang, Bing Bai, Weijun Zhang, Hao Li, Xiao Jiang, Jun Zhang, Lixing You, Xianfeng Chen, Zhen Wang, et al. Experimental demonstration of non-bilocality with truly independent sources and strict locality constraints. *Nature Photonics*, 13(10):687–691, 2019.

[193] Cyril Branciard, Denis Rosset, Nicolas Gisin, and Stefano Pironio. Bilocal versus nonbilocal correlations in entanglement-swapping experiments. *Physical Review A*, 85(3):032119, 2012.

[194] Armin Tavakoli, Paul Skrzypczyk, Daniel Cavalcanti, and Antonio Acín. Nonlocal correlations in the star-network configuration. *Physical Review A*, 90(6):062109, 2014.

[195] Samuel L Braunstein and Carlton M Caves. Wringing out better bell inequalities. *Annals of Physics*, 202(1):22–56, 1990.

[196] Tamás Vértesi, Stefano Pironio, and Nicolas Brunner. Closing the detection loophole in bell experiments using qudits. *Physical review letters*, 104(6):060401, 2010.

[197] Lluís Masanes, Stefano Pironio, and Antonio Acín. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature communications*, 2(1):1–7, 2011.

[198] Marc-Olivier Renou, Elisa Bäumer, Sadra Boreiri, Nicolas Brunner, Nicolas Gisin, and Salman Beigi. Genuine quantum nonlocality in the triangle network. *Physical review letters*, 123(14):140401, 2019.

[199] Alejandro Pozas-Kerstjens, Rafael Rabelo, Łukasz Rudnicki, Rafael Chaves, Daniel Cavalcanti, Miguel Navascués, and Antonio Acín. Bounding the sets of classical and quantum correlations in networks. *Physical review letters*, 123(14):140503, 2019.

[200] Ciarán M Lee and Matty J Hoban. Towards device-independent information processing on general quantum networks. *Physical review letters*, 120(2):020504, 2018.

[201] Gilbert S Vernam. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the AIEE*, 45(2):109–115, 1926.

[202] Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949.

[203] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[204] W Dür, H-J Briegel, J Ignacio Cirac, and P Zoller. Quantum repeaters based on entanglement purification. *Physical Review A*, 59(1):169, 1999.

[205] Rodney Van Meter. *Quantum networking*. John Wiley & Sons, 2014.

[206] Koji Azuma and Go Kato. Aggregating quantum repeaters for the quantum internet. *Physical Review A*, 96(3):032332, 2017.

[207] Hua-Lei Yin, Teng-Yun Chen, Zong-Wen Yu, Hui Liu, Li-Xing You, Yi-Heng Zhou, Si-Jing Chen, Yingqiu Mao, Ming-Qi Huang, Wei-Jun Zhang, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical review letters*, 117(19):190501, 2016.

[208] Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussières, Ming-Jun Li, et al. Secure quantum key distribution over 421 km of optical fiber. *Physical review letters*, 121(19):190502, 2018.

[209] Philip Sibson, Chris Erven, Mark Godfrey, Shigehito Miki, Taro Yamashita, Mikio Fujiwara, Masahide Sasaki, Hirotaka Terai, Michael G Tanner, Chandra M Natarajan, et al. Chip-based quantum key distribution. *Nature communications*, 8(1):1–6, 2017.

[210] Darius Bunandar, Anthony Lentine, Catherine Lee, Hong Cai, Christopher M Long, Nicholas Boynton, Nicholas Martinez, Christopher DeRose, Changchen Chen, Matthew Grein, et al. Metropolitan quantum key distribution with silicon photonics. *Physical Review X*, 8(2):021009, 2018.

[211] Gong Zhang, Jing Yan Haw, Hong Cai, Feng Xu, SM Assad, Joseph F Fitzsimons, Xianzhong Zhou, Y Zhang, S Yu, J Wu, et al. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. *Nature Photonics*, 13(12):839–842, 2019.

[212] M Avesani, L Calderaro, M Schiavon, A Stanco, C Agnesi, A Santamato, M Zahidy, A Scriminich, G Foletto, G Contestabile, et al. Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. *arXiv preprint arXiv:1907.10039*, 2019.

[213] Henry Semenenko, Philip Sibson, Andy Hart, Mark G Thompson, John G Rarity, and Chris Erven. Chip-based measurement-device-independent quantum key distribution. *Optica*, 7(3):238–242, 2020.

[214] Charles H Bennett, Gilles Brassard, and N David Mermin. Quantum cryptography without bell's theorem. *Physical review letters*, 68(5):557, 1992.

[215] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical review letters*, 108(13):130503, 2012.

[216] Samuel L Braunstein and Stefano Pirandola. Side-channel-free quantum key distribution. *Physical review letters*, 108(13):130502, 2012.

[217] CH BENNET. Quantum cryptography: Public key distribution and coin tossing. In *Proc. of IEEE Int. Conf. on Comp., Syst. and Signal Proc., Bangalore, India, Dec. 10-12, 1984*, 1984.

[218] Won-Young Hwang. Quantum key distribution with high loss: toward global secure communication. *Physical Review Letters*, 91(5):057901, 2003.

[219] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical review letters*, 94(23):230504, 2005.

[220] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical review letters*, 94(23):230503, 2005.

[221] Peter W Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical review letters*, 85(2):441, 2000.

[222] Barbara Kraus, Nicolas Gisin, and Renato Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Physical review letters*, 95(8):080501, 2005.

[223] Graeme Smith, Joseph M Renes, and John A Smolin. Structured codes improve the bennett-brassard-84 quantum key rate. *Physical Review Letters*, 100(17):170502, 2008.

[224] Hoi Fung Chau. Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate. *Physical Review A*, 66(6):060302, 2002.

[225] Daniel Gottesman and Hoi-Kwong Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Transactions on Information Theory*, 49(2):457–475, 2003.

[226] Joonwoo Bae and Antonio Acín. Key distillation from quantum channels using two-way communication protocols. *Physical Review A*, 75(1):012334, 2007.

[227] Antonio Acin, Nicolas Gisin, and Valerio Scarani. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks. *Physical Review A*, 69(1):012309, 2004.

[228] Valerio Scarani, Antonio Acin, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical review letters*, 92(5):057901, 2004.

[229] Antonio Acin, Serge Massar, and Stefano Pironio. Efficient quantum key distribution secure against no-signalling eavesdroppers. *New Journal of Physics*, 8(8):126, 2006.

[230] Alexander Ling, Matthew P Peloso, Ivan Marcikic, Valerio Scarani, Antia Lamas-Linares, and Christian Kurtsiefer. Experimental quantum key distribution based on a bell test. *Physical Review A*, 78(2):020301, 2008.

[231] Mikio Fujiwara, Ken-ichiro Yoshino, Yoshihiro Nambu, Taro Yamashita, Shigehito Miki, Hirotaka Terai, Zhen Wang, Morio Toyoshima, Akihisa Tomita, and Masahide Sasaki. Modified e91 protocol demonstration with hybrid entanglement photon source. *Optics Express*, 22(11):13616–13624, 2014.

[232] Charles H Bennett, Gilles Brassard, Claude Crépeau, and Ueli M Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995.

[233] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.

[234] Stefano Pirandola, Bhaskar Roy Bardhan, Tobias Gehring, Christian Weedbrook, and Seth Lloyd. Advances in photonic quantum sensing. *Nature Photonics*, 12(12):724, 2018.

[235] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C Sanders. Limitations on practical quantum cryptography. *Physical Review Letters*, 85(6):1330, 2000.

[236] Nitin Jain, Birgit Stiller, Imran Khan, Vadim Makarov, Christoph Marquardt, and Gerd Leuchs. Risk analysis of trojan-horse attacks on practical quantum key distribution systems. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):168–177, 2014.

[237] Artem Vakhitov, Vadim Makarov, and Dag R Hjelme. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *Journal of modern optics*, 48(13):2023–2038, 2001.

[238] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A*, 74(2):022313, 2006.

[239] Nicolas Gisin, Sylvain Fasel, Barbara Kraus, Hugo Zbinden, and Grégoire Ribordy. Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A*, 73(2):022320, 2006.

[240] Shihan Sajeed, Poompong Chaiwongkhot, Jean-Philippe Bourgoin, Thomas Jennewein, Norbert Lütkenhaus, and Vadim Makarov. Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch. *Physical Review A*, 91(6):062301, 2015.

[241] Yang-Yang Fei, Xiang-Dong Meng, Ming Gao, Hong Wang, and Zhi Ma. Quantum man-in-the-middle attack on the calibration process of quantum key distribution. *Scientific reports*, 8(1):1–10, 2018.

[242] M Cover Thomas and A Thomas Joy. Elements of information theory. *New York: Wiley*, 3:37–38, 1991.

[243] Imre Csiszár and Janos Korner. Broadcast channels with confidential messages. *IEEE transactions on information theory*, 24(3):339–348, 1978.

[244] Ueli M Maurer. Secret key agreement by public discussion from common information. *IEEE transactions on information theory*, 39(3):733–742, 1993.

[245] Renato Renner and Stefan Wolf. Smooth rényi entropy and applications. In *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, page 233. IEEE, 2004.

[246] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature photonics*, 4(10):686–689, 2010.

[247] Mario Arnolfo Ciampini, Adeline Orieux, Stefano Paesani, Fabio Sciarrino, Giacomo Corrielli, Andrea Crespi, Roberta Ramponi, Roberto Osellame, and Paolo Mataloni. Path-polarization hyperentangled and cluster states of photons on a chip. *Light: Science & Applications*, 5(4):e16064–e16064, 2016.

[248] Regina Kruse, Linda Sansoni, Sebastian Brauner, Raimund Ricken, Craig S Hamilton, Igor Jex, and Christine Silberhorn. Dual-path source engineering in integrated quantum optics. *Physical Review A*, 92(5):053841, 2015.

[249] Frank Setzpfandt, Alexander S Solntsev, James Titchener, Che Wen Wu, Chunle Xiong, Roland Schiek, Thomas Pertsch, Dragomir N Neshev, and Andrey A Sukhorukov. Tunable generation of entangled photons in a nonlinear directional coupler. *Laser & Photonics Reviews*, 10(1):131–136, 2016.

[250] Florian Kaiser, Amandine Issautier, Lutfi A Ngah, Olivier Alibart, Anthony Martin, and Sébastien Tanzilli. A versatile source of polarization entangled photons for quantum network applications. *Laser Physics Letters*, 10(4):045202, 2013.

[251] Harald Herrmann, Xu Yang, Abu Thomas, Andreas Poppe, Wolfgang Sohler, and Christine Silberhorn. Post-selection free, integrated optical source of non-degenerate, polarization entangled photon pairs. *Optics express*, 21(23):27981–27991, 2013.

[252] Anthony Martin, Amandine Issautier, Harrald Herrmann, Wolfgang Sohler, Daniel Barry Ostrowsky, Olivier Alibart, and Sébastien Tanzilli. A polarization entangled photon-pair source based on a type-ii ppln waveguide emitting at a telecom wavelength. *New Journal of Physics*, 12(10):103005, 2010.

[253] Linda Sansoni, Kai Hong Luo, Christof Eigner, Raimund Ricken, Viktor Quiring, Harald Herrmann, and Christine Silberhorn. A two-channel, spectrally degenerate polarization entangled source on chip. *npj Quantum Information*, 3(1):1–5, 2017.

[254] Rolf T Horn, Piotr Kolenderski, Dongpeng Kang, Payam Abolghasem, Carmelo Scarcella, Adriano Della Frera, Alberto Tosi, Lukas G Helt, Sergei V Zhukovsky, John E Sipe, et al. Inherent polarization entanglement generated from a monolithic semiconductor chip. *Scientific reports*, 3:2314, 2013.

[255] Nobuyuki Matsuda, Hanna Le Jeannic, Hiroshi Fukuda, Tai Tsuchizawa, William John Munro, Kaoru Shimizu, Koji Yamada, Yasuhiro Tokura, and Hiroki Takesue. A monolithically integrated polarization entangled photon pair source on a silicon chip. *Scientific reports*, 2:817, 2012.

[256] HS Eisenberg, G Khoury, GA Durkin, Christoph Simon, and D Bouwmeester. Quantum entanglement of a large number of photons. *Physical review letters*, 93(19):193901, 2004.

[257] Julio T Barreiro, Tzu-Chieh Wei, and Paul G Kwiat. Beating the channel capacity limit for linear photonic superdense coding. *Nature physics*, 4(4):282–286, 2008.

[258] Xiao-Min Hu, Yu Guo, Bi-Heng Liu, Yun-Feng Huang, Chuan-Feng Li, and Guang-Can Guo. Beating the channel capacity limit for superdense coding with entangled ququarts. *Science advances*, 4(7):eaat9304, 2018.

[259] P Ben Dixon, Gregory A Howland, James Schneeloch, and John C Howell. Quantum mutual information capacity for high-dimensional entangled states. *Physical review letters*, 108(14):143603, 2012.

[260] Rupert Ursin, F Tiefenbacher, T Schmitt-Manderbach, H Weier, Thomas Scheidl, M Lindenthal, B Blauensteiner, T Jennewein, J Perdigues, P Trojek, et al. Entanglement-based quantum communication over 144 km. *Nature physics*, 3(7):481–486, 2007.

[261] Toshimori Honjo, Sae Woo Nam, Hiroki Takesue, Qiang Zhang, H Kamada, Y Nishida, O Tadanaga, M Asobe, Burm Baek, Robert Hadfield, S. Miki, M. Fujiwara, M. Sasaki, Z. Wang, and Y Inoue, K. and. Yamamoto. Long-distance entanglement-based quantum key distribution over optical fiber. *Optics Express*, 16(23):19118–19126, 2008.

[262] Takahiro Inagaki, Nobuyuki Matsuda, Osamu Tadanaga, Masaki Asobe, and Hiroki Takesue. Entanglement distribution over 300 km of fiber. *Optics Express*, 21(20):23241–23249, 2013.

[263] P Gregg, P Kristensen, and S Ramachandran. Conservation of orbital angular momentum in air-core optical fibers. *Optica*, 2(3):267–270, 2015.

[264] Giovanni Milione, H. I. Sztul, D. A. Nolan, and R. R. Alfano. Higher-order Poincaré sphere, stokes parameters, and the angular momentum of light. *Physical Review Letters*, 107:053601, 2011.

[265] Mark R. Dennis, Kevin O'Holleran, and Miles J. Padgett. Singular optics: Optical vortices and polarization singularities. volume 53 of *Progress in Optics*, pages 293 – 363. Elsevier, 2009.

[266] Qiwen Zhan. Cylindrical vector beams: from mathematical concepts to applications. *Advances in Optics and Photonics*, 1(1):1–57, 2009.

[267] Filippo Cardano, Ebrahim Karimi, Sergei Slussarenko, Lorenzo Marrucci, Corrado de Lisio, and Enrico Santamato. Polarization pattern of vector vortex beams generated by q-plates with different topological charges. *Applied Optics*, 51(10):C1–C6, 2012.

[268] Ayman F Abouraddy and Kimani C Toussaint Jr. Three-dimensional polarization control in microscopy. *Physical Review Letters*, 96(15):153901, 2006.

[269] Brian J Roxworthy and Kimani C Toussaint Jr. Optical trapping with π-phase cylindrical vector beams. *New Journal of Physics*, 12(7):073012, 2010.

[270] H Moradi, V Shahabadi, E Madadi, E Karimi, and F Hajizadeh. Efficient optical trapping with cylindrical vector beams. *Optics Express*, 27:7266, 2019.

[271] Vincenzo D'Ambrosio, Nicolo Spagnolo, Lorenzo Del Re, Sergei Slussarenko, Ying Li, Leong Chuan Kwek, Lorenzo Marrucci, Stephen P Walborn, Leandro Aolita, and Fabio Sciarrino. Photonic polarization gears for ultra-sensitive angular measurements. *Nature Communications*, 4:2432, 2013.

[272] Fredrik K Fatemi. Cylindrical vector beams for rapid polarization-dependent measurements in atomic systems. *Optics Express*, 19(25):25143–25150, 2011.

[273] A. Büse, M. L. Juan, N. Tischler, V. D'Ambrosio, F. Sciarrino, L. Marrucci, and G. Molina-Terriza. Symmetry protection of photonic entanglement inthe interaction with a single nanoaperture. *Physical Review Letters*, 121:173901, 2018.

[274] Valentina Parigi, Vincenzo D'Ambrosio, Christophe Arnold, Lorenzo Marrucci, Fabio Sciarrino, and Julien Laurat. Storage and retrieval of vector beams of light in a multiple-degree-of-freedom quantum memory. *Nature Communications*, 6:7706, 2015.

[275] Vincenzo D'Ambrosio, Gonzalo Carvacho, Francesco Graffitti, Chiara Vitelli, Bruno Piccirillo, Lorenzo Marrucci, and Fabio Sciarrino. Entangled vector vortex beams. *Physical Review A*, 94(3):030304, 2016.

[276] Bienvenu Ndagano, Isaac Nape, Mitchell A Cox, Carmelo Rosales-Guzman, and Andrew Forbes. Creation and detection of vector vortex modes for classical and quantum communication. *Journal of Lightwave Technology*, 36(2):292–301, 2018.

[277] Yisa S Rumala, Giovanni Milione, Thien An Nguyen, Sebastião Pratavieira, Zabir Hossain, Daniel Nolan, Sergei Slussarenko, Ebrahim Karimi, Lorenzo Marrucci, and Robert R Alfano. Tunable supercontinuum light vector vortex beam generator using a q-plate. *Optics Letters*, 38(23):5083–5086, 2013.

[278] V. D'Ambrosio, E. Nagali, S. P. Walborn, L. Aolita, S. Slussarenko, L. Marrucci, and F. Sciarrino. Complete experimental toolbox for alignment-free quantum communication. *Nature Communication*, 3:961, 2012.

[279] G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi. Free-space quantum key distribution by rotation-invariant twisted photons. *Physical Review Letters*, 113:060503, 2014.

[280] G. Carvacho, F. Graffitti, V. D'Ambrosio, and F. Hiesmayr, B. Sciarrino. Experimental investigation on the geometry of GHZ states. *Scientific Reports*, 7:13265, 2017.

[281] F. Bouchard, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. Sánchez-Soto, and E. Karimi. Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons. *Quantum*, 2:111, 2018.

[282] Daniele Cozzolino, Davide Bacco, Beatrice Da Lio, Kasper Ingerslev, Yunhong Ding, Kjeld Dalgaard, Poul Kristensen, Michael Galili, Karsten Rottwitt, Siddharth Ramachandran, et al. Orbital angular momentum states enabling fiber-based high-dimensional quantum communication. *Physical Review Applied*, 11(6):064058, 2019.

[283] Lorenzo Marrucci, Ebrahim Karimi, Sergei Slussarenko, Bruno Piccirillo, Enrico Santamato, Eleonora Nagali, and Fabio Sciarrino. Spin-to-orbital conversion of the angular momentum of light and its classical and quantum applications. *Journal of Optics*, 13(6):064001, 2011.

[284] Eleonora Nagali, Fabio Sciarrino, Francesco De Martini, Lorenzo Marrucci, Bruno Piccirillo, Ebrahim Karimi, and Enrico Santamato. Quantum information transfer from spin to orbital angular momentum of photons. *Physical Review Letters*, 103(1):013601, 2009.

[285] Ebrahim Karimi, Jonathan Leach, Sergei Slussarenko, Bruno Piccirillo, Lorenzo Marrucci, Lixiang Chen, Weilong She, Sonja Franke-Arnold, Miles J Padgett, and Enrico Santamato. Spin-orbit hybrid entanglement of photons and quantum contextuality. *Physical review A*, 82(2):022115, 2010.

[286] Andrea Aiello, Falk Töppel, Christoph Marquardt, Elisabeth Giacobino, and Gerd Leuchs. Quantum- like nonseparable structures in optical beams. *New Journal of Physics*, 17(4):043024, 2015.

[287] Melanie McLaren, Thomas Konrad, and Andrew Forbes. Measuring the nonseparability of vector vortex beams. *Physical Review A*, 92(2):023833, 2015.

[288] Daniel Collins, Nicolas Gisin, Sandu Popescu, David Roberts, and Valerio Scarani. Bell-type inequalities to detect true n-body nonseparability. *Physical review letters*, 88(17):170405, 2002.

[289] Jean-Daniel Bancal. Device-independent witnesses of genuine multipartite entanglement. In *On the Device-Independent Approach to Quantum Physics*, pages 73–80. Springer, 2014.

[290] Lucien Hardy. Quantum mechanics, local realistic theories, and lorentz-invariant realistic theories. *Physical Review Letters*, 68(20):2981, 1992.

[291] Lucien Hardy. Nonlocality for two particles without inequalities for almost all entangled states. *Physical Review Letters*, 71(11):1665, 1993.

[292] Shu-Han Jiang, Zhen-Peng Xu, Hong-Yi Su, Arun Kumar Pati, and Jing-Ling Chen. Generalized hardy's paradox. *Physical review letters*, 120(5):050403, 2018.

[293] Manuel Erhard, Robert Fickler, Mario Krenn, and Anton Zeilinger. Twisted photons: new quantum perspectives in high dimensions. *Light: Science & Applications*, 7(3):17146–17146, 2018.

[294] Helle Bechmann-Pasquinucci and Wolfgang Tittel. Quantum cryptography using larger alphabets. *Physical Review A*, 61(6):062308, 2000.

[295] Nicolas J Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin. Security of quantum key distribution using d-level systems. *Physical review letters*, 88(12):127902, 2002.

[296] Chiara Vitelli, Nicolò Spagnolo, Lorenzo Aparo, Fabio Sciarrino, Enrico Santamato, and Lorenzo Marrucci. Joining the quantum state of two photons into one. *Nature Photonics*, 7(7):521–526, 2013.

[297] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzmitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning, et al. Random numbers certified by bell's theorem. *Nature*, 464(7291):1021–1024, 2010.

[298] Yang Liu, Xiao Yuan, Ming-Han Li, Weijun Zhang, Qi Zhao, Jiaqiang Zhong, Yuan Cao, Yu-Huai Li, Luo-Kan Chen, Hao Li, et al. High-speed device-independent quantum random number generation without a detection loophole. *Physical review letters*, 120(1):010503, 2018.

[299] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412), 2018.

[300] Yao Fu, Hua-Lei Yin, Teng-Yun Chen, and Zeng-Bing Chen. Long-distance measurement-device-independent multiparty quantum communication. *Physical review letters*, 114(9):090501, 2015.

[301] Xi-Lin Wang, Luo-Kan Chen, Wei Li, H-L Huang, Chang Liu, Chao Chen, Y-H Luo, Z-E Su, Dian Wu, Z-D Li, et al. Experimental ten-photon entanglement. *Physical review letters*, 117(21):210502, 2016.

[302] Cyril Branciard, Nicolas Gisin, and Stefano Pironio. Characterizing the nonlocal correlations created via entanglement swapping. *Physical review letters*, 104(17):170401, 2010.

[303] Francesco Andreoli, Gonzalo Carvacho, Luca Santodonato, Rafael Chaves, and Fabio Sciarrino. Maximal qubit violation of n-locality inequalities in a star-shaped quantum network. *New Journal of Physics*, 19(11):113020, 2017.

[304] Lev Vaidman and Nadav Yoran. Methods for reliable teleportation. *Physical Review A*, 59(1):116, 1999.

[305] Matthew D Eisaman, Jingyun Fan, Alan Migdall, and Sergey V Polyakov. Invited review article: Single-photon sources and detectors. *Review of scientific instruments*, 82(7):071101, 2011.

[306] Alessandro Fedrizzi, Thomas Herbst, Andreas Poppe, Thomas Jennewein, and Anton Zeilinger. A wavelength-tunable fiber-coupled source of narrowband entangled photons. *Optics Express*, 15(23):15377–15386, 2007.

[307] Adán Cabello, Álvaro Feito, and Antia Lamas-Linares. Bell's inequalities with realistic noise for polarization-entangled photons. *Physical Review A*, 72(5):052112, 2005.

[308] Armin Tavakoli, Marc Olivier Renou, Nicolas Gisin, and Nicolas Brunner. Correlations in star networks: from bell inequalities to network inequalities. *New Journal of Physics*, 19(7):073003, 2017.

[309] George Robert Blakley. Safeguarding cryptographic keys. In *1979 International Workshop on Managing Requirements Knowledge (MARK)*, pages 313–318. IEEE, 1979.

[310] Amos Beimel. Secret-sharing schemes: a survey. In *International Conference on Coding and Cryptology*, pages 11–46. Springer, 2011.

[311] Daniel Moskovich. An overview of the state of the art for practical quantum key distribution. *arXiv preprint arXiv:1504.05471*, 2015.

[312] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. Secure quantum key distribution. *Nature Photonics*, 8(8):595–604, 2014.

[313] Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan. Practical challenges in quantum key distribution. *npj Quantum Information*, 2(1):1–12, 2016.

[314] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*, 2020.

[315] Charles H Bennett. Quantum cryptography using any two nonorthogonal states. *Physical review letters*, 68(21):3121, 1992.

[316] Edo Waks, Assaf Zeevi, and Yoshihisa Yamamoto. Security of quantum key distribution with entangled photons against individual attacks. *Physical Review A*, 65(5):052310, 2002.

[317] Norbert Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61(5):052304, 2000.

[318] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

[319] Xiongfeng Ma, Chi-Hang Fred Fung, and Hoi-Kwong Lo. Quantum key distribution with entangled photon sources. *Physical Review A*, 76(1):012307, 2007.

[320] Masahiro Takeoka, Rui-Bo Jin, and Masahide Sasaki. Full analysis of multi-photon pair effects in spontaneous parametric down conversion based photonic quantum information processing. *New Journal of Physics*, 17(4):043030, 2015.

[321] Romain Alléaume, François Treussart, Gaëtan Messin, Yannick Dumeige, Jean-François Roch, Alexios Beveratos, Rosa Brouri-Tualle, Jean-Philippe Poizat, and Philippe Grangier. Experimental open-air quantum key distribution with a single-photon source. *New Journal of physics*, 6(1):92, 2004.

[322] Edo Waks, Charles Santori, and Yoshihisa Yamamoto. Security aspects of quantum key distribution with sub-poisson light. *Physical Review A*, 66(4):042315, 2002.

[323] Edo Waks, Kyo Inoue, Charles Santori, David Fattal, Jelena Vuckovic, Glenn S Solomon, and Yoshihisa Yamamoto. Quantum cryptography with a photon turnstile. *Nature*, 420(6917):762–762, 2002.

[324] Jin Liu, Rongbin Su, Yuming Wei, Beimeng Yao, Saimon Filipe Covre da Silva, Ying Yu, Jake Iles-Smith, Kartik Srinivasan, Armando Rastelli, Juntao Li, et al. A solid-state source of strongly entangled photon pairs with high brightness and indistinguishability. *Nature nanotechnology*, 14(6):586–593, 2019.

[325] Hui Wang, Hai Hu, T-H Chung, Jian Qin, Xiaoxia Yang, J-P Li, R-Z Liu, H-S Zhong, Y-M He, Xing Ding, et al. On-demand semiconductor source of entangled photons which simultaneously has high fidelity, efficiency, and indistinguishability. *Physical review letters*, 122(11):113602, 2019.

[326] Daniel Huber, Marcus Reindl, Saimon Filipe Covre Da Silva, Christian Schimpf, Javier Martín-Sánchez, Huiying Huang, Giovanni Piredda, Johannes Edlinger, Armando Rastelli, and Rinaldo Trotta. Strain-tunable gaas quantum dot: A nearly dephasing-free source of entangled photon pairs on demand. *Physical review letters*, 121(3):033902, 2018.

[327] RJ Collins, PJ Clarke, V Fernández, KJ Gordon, MN Makhonin, JA Timpson, A Tahraoui, M Hopkinson, AM Fox, MS Skolnick, et al. Quantum key distribution system in standard telecommunications fiber using a short wavelength single photon source. *Journal of Applied Physics*, 107(7):073102, 2010.

[328] Kazuya Takemoto, Yoshihiro Nambu, Toshiyuki Miyazawa, Yoshiki Sakuma, Tsuyoshi Yamamoto, Shinichi Yorozu, and Yasuhiko Arakawa. Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors. *Scientific reports*, 5:14383, 2015.

[329] Tobias Heindel, Christian A Kessler, Markus Rau, Christian Schneider, Martin Fürst, Fabian Hargart, Wolfgang-Michael Schulz, Marcus Eichfelder, Robert Roßbach, Sebastian Nauerth, et al. Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range. *New Journal of Physics*, 14(8):083001, 2012.

[330] Markus Rau, Tobias Heindel, Sebastian Unsleber, Tristan Braun, Julian Fischer, Stefan Frick, Sebastian Nauerth, Christian Schneider, Gwenaelle Vest, Stephan Reitzenstein, et al. Free space quantum key distribution over 500 meters using electrically driven quantum dot single-photon sources—a proof of principle experiment. *New Journal of Physics*, 16(4):043003, 2014.

[331] Thomas Aichele, Gaël Reinaudi, and Oliver Benson. Separating cascaded photons from a single quantum dot: Demonstration of multiplexed quantum cryptography. *Physical Review B*, 70(23):235329, 2004.

[332] Timm Kupko, Martin von Helversen, Lucas Rickert, Jan-Hindrik Schulze, André Strittmatter, Manuel Gschrey, Sven Rodt, Stephan Reitzenstein, and Tobias Heindel. Tools for the performance optimization of single-photon quantum key distribution. *npj Quantum Information*, 6(1):1–8, 2020.

[333] B Dzurnak, RM Stevenson, J Nilsson, JF Dynes, ZL Yuan, J Skiba-Szymanska, I Farrer, DA Ritchie, and AJ Shields. Quantum key distribution with an entangled light emitting diode. *Applied Physics Letters*, 107(26):261101, 2015.

[334] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling. Progress in satellite quantum key distribution. *npj Quantum Information*, 3(1):1–13, 2017.

[335] Olivier Bouchet, Hervé Sizun, Christian Boisrobert, and Frederique De Fornel. *Free-space optics: propagation and communication*, volume 91. John Wiley & Sons, 2010.

[336] Hemani Kaushal and Georges Kaddoum. Free space optical communication: challenges and mitigation techniques. *arXiv preprint arXiv:1506.04836*, 2015.

[337] Alberto Carrasco-Casado, Verónica Fernández, and Natalia Denisenko. Free-space quantum key distribution. In *Optical Wireless Communications*, pages 589–607. Springer International Publishing, 2016.

[338] Janusz Mikołajczyk, Zbigniew Bielecki, Maciej Bugajski, Józef Piotrowski, Jacek Wojtas, Waldemar Gawron, Dariusz Szabra, and Artur Prokopiuk. Analysis of free-space optics development. *Metrology and Measurement Systems*, 24(4), 2017.

[339] Valerian Ilich Tatarski. *Wave propagation in a turbulent medium*. Courier Dover Publications, 2016.

[340] F Basso Basset, Michele B Rota, Christian Schimpf, Davide Tedeschi, Katharina D Zeuner, SF Covre da Silva, Marcus Reindl, Val Zwiller, Klaus D Jöns, Armando Rastelli, et al. Entanglement swapping with photons generated on demand by a quantum dot. *Physical Review Letters*, 123(16):160501, 2019.

[341] Matthias Bock, Andreas Lenhard, Christopher Chunnilall, and Christoph Becher. Highly efficient heralded single-photon source for telecom wavelengths based on a ppln waveguide. *Optics express*, 24(21):23992–24001, 2016.

[342] J. B. Altepeter, E. R. Jeffrey, P. G. Kwiat, S. Tanzilli, N. Gisin, and A. Acín. Experimental methods for detecting entanglement. *Physical Review Letters*, 95(3):033601, July 2005.

[343] Michele Beniamino Rota, Francesco Basso Basset, Davide Tedeschi, and Rinaldo Trotta. Entanglement teleportation with photons from quantum dots: towards a solid-state based quantum network. *IEEE Journal of Selected Topics in Quantum Electronics*, 2020.

[344] Farinaz Koushanfar and Azalia Mirhoseini. A unified framework for multimodal submodular integrated circuits trojan detection. *IEEE Transactions on Information Forensics and Security*, 6(1):162–174, 2010.

[345] Luca Trevisan. Extractors and pseudorandom generators. *Journal of the ACM*, 48(4):860–879, 2001.

[346] Wolfgang Mauerer, Christopher Portmann, and Volkher B Scholz. A modular framework for randomness extraction based on trevisan's construction. *arXiv preprint arXiv:1212.0520*, 2012.

[347] Umesh Vazirani and Thomas Vidick. Fully device independent quantum key distribution. *Communications of the ACM*, 62(4):133–133, 2019.

[348] Anindya De, Christopher Portmann, Thomas Vidick, and Renato Renner. Trevisan's extractor in the presence of quantum side information. *SIAM Journal on Computing*, 41(4):915–940, 2012.

[349] Brice Colombier, Lilian Bossuet, Viktor Fischer, and David Hély. Key reconciliation protocols for error correction of silicon puf responses. *IEEE Transactions on Information Forensics and Security*, 12(8):1988–2002, 2017.

[350] Giuseppe Vallone, Vincenzo D'Ambrosio, Anna Sponselli, Sergei Slussarenko, Lorenzo Marrucci, Fabio Sciarrino, and Paolo Villoresi. Free-space quantum key distribution by rotation-invariant twisted photons. *Physical review letters*, 113(6):060503, 2014.

[351] Huanlu Li, David B Phillips, Xuyang Wang, Ying-Lung Daniel Ho, Lifeng Chen, Xiaoqi Zhou, Jiangbo Zhu, Siyuan Yu, and Xinlun Cai. Orbital angular momentum vertical-cavity surface-emitting lasers. *Optica*, 2(6):547–552, 2015.

[352] N Carlon Zambon, Philippe St-Jean, Marijana Milićević, Aristide Lemaître, Abdelmounaim Harouri, Luc Le Gratiet, Olivier Bleu, DD Solnyshkov, Guillaume Malpuech, Isabelle Sagnes, et al. Optically controlling the emission chirality of microlasers. *Nature Photonics*, 13(4):283–288, 2019.

[353] Chee Fai Fong, Yasutomo Ota, Satoshi Iwamoto, and Yasuhiko Arakawa. Scheme for media conversion between electronic spin and photonic orbital angular momentum based on photonic nanocavity. *Optics express*, 26(16):21219–21234, 2018.

[354] Yanjun Bao, Qiaoling Lin, Rongbin Su, Zhang-Kai Zhou, Jindong Song, Juntao Li, and Xue-Hua Wang. On-demand spin-state manipulation of single-photon emission from quantum dot integrated with metasurface. *Science advances*, 6(31):eaba8761, 2020.

[355] Oliver Benson, Charles Santori, Matthew Pelton, and Yoshihisa Yamamoto. Regulated and entangled photons from a single quantum dot. *Physical review letters*, 84(11):2513, 2000.

[356] Rinaldo Trotta, Javier Martín-Sánchez, Johannes S Wildmann, Giovanni Piredda, Marcus Reindl, Christian Schimpf, Eugenio Zallo, Sandra Stroj, Johannes Edlinger, and Armando Rastelli. Wavelength-tunable sources of entangled photons interfaced with atomic vapours. *Nature communications*, 7(1):1–7, 2016.

[357] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum-enhanced measurements: beating the standard quantum limit. *Science*, 306(5700):1330–1336, 2004.

[358] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum metrology. *Physical review letters*, 96(1):010401, 2006.

[359] Matteo GA Paris. Quantum estimation for quantum technology. *International Journal of Quantum Information*, 7(supp01):125–137, 2009.

[360] Roman Schnabel, Nergis Mavalvala, David E McClelland, and Ping K Lam. Quantum metrology for gravitational wave astronomy. *Nature Communications*, 1:121, 2010.

[361] Luca Pezzè, Augusto Smerzi, Markus K Oberthaler, Roman Schmied, and Philipp Treutlein. Quantum metrology with nonclassical states of atomic ensembles. *Reviews of Modern Physics*, 90(3):035005, 2018.

[362] Ilaria Gianani, Marco G Genoni, and Marco Barbieri. Assessing data postprocessing for quantum estimation. *IEEE Journal of Selected Topics in Quantum Electronics*, 26(3):1–7, 2020.

[363] Michael A Taylor and Warwick P Bowen. Quantum metrology and its application in biology. *Physics Reports*, 615:1–59, 2016.

[364] Romana Schirhagl, Kevin Chang, Michael Loretz, and Christian L Degen. Nitrogen-vacancy centers in diamond: nanoscale sensors for physics and biology. *Annual review of physical chemistry*, 65:83–105, 2014.

[365] J Abadie, BP Abbott, R Abbott, TD Abbott, M Abernathy, C Adams, R Adhikari, C Affeldt, B Allen, GS Allen, et al. A gravitational wave observatory operating beyond the quantum shot-noise limit. *Nature Physics*, 7(12):962, 2011.

[366] Andrew D Ludlow, Martin M Boyd, Jun Ye, Ekkehard Peik, and Piet O Schmidt. Optical atomic clocks. *Reviews of Modern Physics*, 87(2):637, 2015.

[367] Luca Pezzè and Augusto Smerzi. Heisenberg-limited noisy atomic clock using a hybrid coherent and squeezed states protocol. *arXiv preprint arXiv:2003.10943*, 2020.

[368] Jonathan P Dowling. Correlated input-port, matter-wave interferometer: Quantum-noise limits to the atom-laser gyroscope. *Physical Review A*, 57(6):4736, 1998.

[369] Alexander D Cronin, Jörg Schmiedmayer, and David E Pritchard. Optics and interferometry with atoms and molecules. *Reviews of Modern Physics*, 81(3):1051, 2009.

[370] Yanming Che, Jing Liu, Xiao-Ming Lu, and Xiaoguang Wang. Multiqubit matter-wave interferometry under decoherence and the heisenberg scaling recovery. *Physical Review A*, 99(3):033807, 2019.

[371] DV Tsarev, SM Arakelian, You-Lin Chuang, Ray-Kuang Lee, and AP Alodjants. Quantum metrology beyond heisenberg limit with entangled matter wave solitons. *Optics express*, 26(15):19583–19595, 2018.

[372] Da Xu, Xiao Xiong, Lin Wu, Xi-Feng Ren, Ching Eng Png, Guang-Can Guo, Qihuang Gong, and Yun-Feng Xiao. Quantum plasmonics: new opportunity in fundamental and applied photonics. *Advances in Optics and Photonics*, 10(4):703–756, 2018.

[373] Mohammadjavad Dowran, Ashok Kumar, Benjamin J Lawrie, Raphael C Pooser, and Alberto M Marino. Quantum-enhanced plasmonic sensing. *Optica*, 5(5):628–633, 2018.

[374] Sourav Bhattacharjee, Utso Bhattacharya, Wolfgang Niedenzu, Victor Mukherjee, and Amit Dutta. Quantum magnetometry using two-stroke thermal machines. *New Journal of Physics*, 22(1):013024, 2020.

[375] John F Barry, Jennifer M Schloss, Erik Bauch, Matthew J Turner, Connor A Hart, Linh M Pham, and Ronald L Walsworth. Sensitivity optimization for nv-diamond magnetometry. *Reviews of Modern Physics*, 92(1):015004, 2020.

[376] David J Wineland, John J Bollinger, Wayne M Itano, FL Moore, and Daniel J Heinzen. Spin squeezing and reduced quantum noise in spectroscopy. *Physical Review A*, 46(11):R6797, 1992.

[377] M Naghiloo, AN Jordan, and KW Murch. Achieving optimal quantum acceleration of frequency estimation using adaptive coherent control. *Physical review letters*, 119(18):180801, 2017.

[378] Francesco Albarelli, Matteo AC Rossi, and Marco G Genoni. Quantum frequency estimation with conditional states of continuously monitored independent dephasing channels. *International Journal of Quantum Information*, page 1941013, 2020.

[379] Agedi N Boto, Pieter Kok, Daniel S Abrams, Samuel L Braunstein, Colin P Williams, and Jonathan P Dowling. Quantum interferometric optical lithography: exploiting entanglement to beat the diffraction limit. *Physical Review Letters*, 85(13):2733, 2000.

[380] EJS Fonseca, CH Monken, and S Pádua. Measurement of the de broglie wavelength of a multiphoton wave packet. *Physical Review Letters*, 82(14):2868, 1999.

[381] Yoshio Kawabe, Hideki Fujiwara, Ryo Okamoto, Keiji Sasaki, and Shigeki Takeuchi. Quantum interference fringes beating the diffraction limit. *Optics express*, 15(21):14244–14250, 2007.

[382] Milena D'Angelo, Maria V Chekhova, and Yanhua Shih. Two-photon diffraction and quantum lithography. *Physical review letters*, 87(1):013602, 2001.

[383] LA Lugiato, A Gatti, and E Brambilla. Quantum imaging. *Journal of Optics B: Quantum and semiclassical optics*, 4(3):S176, 2002.

[384] Marco Genovese. Real applications of quantum imaging. *Journal of Optics*, 18(7):073002, 2016.

[385] Paul-Antoine Moreau, Ermes Toninelli, Thomas Gregory, and Miles J Padgett. Imaging with quantum states of light. *Nature Reviews Physics*, 1(6):367–380, 2019.

[386] Mankei Tsang, Ranjith Nair, and Xiao-Ming Lu. Quantum theory of superresolution for two incoherent optical point sources. *Physical Review X*, 6(3):031033, 2016.

[387] Takafumi Ono, Ryo Okamoto, and Shigeki Takeuchi. An entanglement-enhanced microscope. *Nature communications*, 4:2426, 2013.

[388] Fan Yang, Arina Tashchilina, Eugene S Moiseev, Christoph Simon, and Alexander I Lvovsky. Far-field linear optical superresolution via heterodyne detection in a higher-order local oscillator mode. *Optica*, 3(10):1148–1152, 2016.

[389] Evangelia Bisketzi, Dominic Branford, and Animesh Datta. Quantum limits of localisation microscopy. *New Journal of Physics*, 21(12):123032, 2019.

[390] Ivano Ruo Berchera and Ivo Pietro Degiovanni. Quantum imaging with sub-poissonian light: challenges and perspectives in optical metrology. *Metrologia*, 2018.

[391] Thomas Gregory, P-A Moreau, Ermes Toninelli, and Miles J Padgett. Imaging through noise with quantum illumination. *Science Advances*, 6(6):eaay2652, 2020.

[392] Mankei Tsang. Quantum limits to optical point-source localization. *Optica*, 2(7):646–653, 2015.

[393] Ranjith Nair and Mankei Tsang. Far-field superresolution of thermal electromagnetic sources at the quantum limit. *Physical review letters*, 117(19):190801, 2016.

[394] Christopher E Granade, Christopher Ferrie, Nathan Wiebe, and David G Cory. Robust online hamiltonian learning. *New Journal of Physics*, 14(10):103013, 2012.

[395] Jun Zhang and Mohan Sarovar. Quantum hamiltonian identification from measurement time traces. *Physical review letters*, 113(8):080401, 2014.

[396] Nathan Wiebe, Christopher Granade, Christopher Ferrie, and David G Cory. Hamiltonian learning and certification using quantum resources. *Physical review letters*, 112(19):190501, 2014.

[397] I Ruo Berchera, IP Degiovanni, Stefano Olivares, and Marco Genovese. Quantum light in coupled interferometers for quantum gravity tests. *Physical review letters*, 110(21):213601, 2013.

[398] Jan Kohlrus, David Edward Bruschi, and Ivette Fuentes. Quantum-metrology estimation of spacetime parameters of the earth outperforming classical precision. *Physical Review A*, 99(3):032350, 2019.

[399] Nicolas Gisin and Sandu Popescu. Spin flips and quantum information for antiparallel spins. *Physical Review Letters*, 83(2):432, 1999.

[400] Giulio Chiribella, GM D'Ariano, P Perinotti, and MF Sacchi. Efficient use of quantum resources for the transmission of a reference frame. *Physical Review Letters*, 93(18):180503, 2004.

[401] E Bagan, M Baig, and Ramon Muñoz-Tapia. Aligning reference frames with quantum states. *Physical Review Letters*, 87(25):257903, 2001.

[402] Matthias Fink, Fabian Steinlechner, Johannes Handsteiner, Jonathan P Dowling, Thomas Scheidl, and Rupert Ursin. Entanglement-enhanced optical gyroscope. *New Journal of Physics*, 21(5):053010, 2019.

[403] Ming Li, Chang-Ling Zou, Di Liu, Guo-Ping Guo, Guang-Can Guo, and Xi-Feng Ren. Enhanced absorption microscopy with correlated photon pairs. *Physical Review A*, 98(1):012121, 2018.

[404] Masazumi Fujiwara, Simo Sun, Alexander Dohms, Yushi Nishimura, Ken Suto, Yuka Takezawa, Keisuke Oshimi, Li Zhao, Nikola Sadzak, Yumi Umehara, et al. Real-time nanodiamond thermometry probing\textit {in-vivo} thermogenic responses. *arXiv preprint arXiv:2001.02844*, 2020.

[405] Christian L Degen, F Reinhard, and P Cappellaro. Quantum sensing. *Reviews of Modern Physics*, 89(3):035002, 2017.

[406] Tuvia Gefen, Amit Rotem, and Alex Retzker. Overcoming resolution limits with quantum sensing. *Nature communications*, 10(1):1–9, 2019.

[407] Benjamin P Abbott, Richard Abbott, TD Abbott, MR Abernathy, Fausto Acernese, Kendall Ackley, Carl Adams, Thomas Adams, Paolo Addesso, RX Adhikari, et al. Observation of gravitational waves from a binary black hole merger. *Physical Review Letters*, 116(6):061102, 2016.

[408] Benjamin P Abbott, R Abbott, TD Abbott, MR Abernathy, F Acernese, K Ackley, C Adams, T Adams, P Addesso, RX Adhikari, et al. Gw151226: observation of gravitational waves from a 22-solar-mass binary black hole coalescence. *Physical review letters*, 116(24):241103, 2016.

[409] Junaid Aasi, BP Abbott, Richard Abbott, Thomas Abbott, MR Abernathy, Kendall Ackley, Carl Adams, Thomas Adams, Paolo Addesso, RX Adhikari, et al. Advanced ligo. *Classical and quantum gravity*, 32(7):074001, 2015.

[410] Carlton M Caves. Quantum-mechanical noise in an interferometer. *Physical Review D*, 23(8):1693, 1981.

[411] R_E Slusher, LW Hollberg, Bernard Yurke, JC Mertz, and JF Valley. Observation of squeezed states generated by four-wave mixing in an optical cavity. *Physical Review Letters*, 55(22):2409, 1985.

[412] Min Xiao, Ling-An Wu, and H Jeffrey Kimble. Precision measurement beyond the shot-noise limit. *Physical review letters*, 59(3):278, 1987.

[413] Ph Grangier, RE Slusher, B Yurke, and A LaPorta. Squeezed-light–enhanced polarization interferometer. *Physical review letters*, 59(19):2153, 1987.

[414] E Oelker, L Barsotti, S Dwyer, D Sigg, and N Mavalvala. Squeezed light for advanced gravitational wave detectors and beyond. *Optics express*, 22(17):21106–21121, 2014.

[415] Henning Vahlbruch, Dennis Wilken, Moritz Mehmet, and Benno Willke. Laser power stabilization beyond the shot noise limit using squeezed light. *Physical review letters*, 121(17):173601, 2018.

[416] Man Leong Chan, Chris Messenger, Ik Siong Heng, and Martin Hendry. Binary neutron star mergers and third generation detectors: Localization and early warning. *Physical Review D*, 97(12):123014, 2018.

[417] Stefan L Danilishin, Farid Ya Khalili, and Haixing Miao. Advanced quantum techniques for future gravitational-wave detectors. *Living Reviews in Relativity*, 22(1):2, 2019.

[418] Benjamin P Abbott, R Abbott, TD Abbott, MR Abernathy, K Ackley, C Adams, P Addesso, RX Adhikari, VB Adya, C Affeldt, et al. Exploring the sensitivity of next generation gravitational wave detectors. *Classical and Quantum Gravity*, 34(4):044001, 2017.

[419] Ryan Lynch, Salvatore Vitale, Lisa Barsotti, Sheila Dwyer, and Matthew Evans. Effect of squeezing on parameter estimation of gravitational waves emitted by compact binary systems. *Physical Review D*, 91(4):044032, 2015.

[420] H Grote, K Danzmann, KL Dooley, R Schnabel, J Slutsky, and H Vahlbruch. First long-term application of squeezed states of light in a gravitational-wave observatory. *Physical review letters*, 110(18):181101, 2013.

[421] Junaid Aasi, J Abadie, BP Abbott, Richard Abbott, TD Abbott, MR Abernathy, Carl Adams, Thomas Adams, Paolo Addesso, RX Adhikari, et al. Enhanced sensitivity of the ligo gravitational wave detector by using squeezed states of light. *Nature Photonics*, 7(8):613, 2013.

[422] M Tse, Haocun Yu, N Kijbunchoo, A Fernandez-Galiana, P Dupej, L Barsotti, CD Blair, DD Brown, SE Dwyer, A Effler, et al. Quantum-enhanced advanced ligo detectors in the era of gravitational-wave astronomy. *Physical Review Letters*, 123(23):231107, 2019.

[423] F Acernese, M Agathos, L Aiello, A Allocca, A Amato, S Ansoldi, S Antier, M Arène, N Arnaud, S Ascenzi, et al. Increasing the astrophysical reach of the advanced virgo detector via the application of squeezed vacuum states of light. *Physical Review Letters*, 123(23):231108, 2019.

[424] KL Dooley, JR Leong, T Adams, C Affeldt, A Bisht, C Bogan, J Degallaix, C Gräf, S Hild, J Hough, et al. Geo 600 and the geo-hf upgrade program: successes and challenges. *Classical and Quantum Gravity*, 33(7):075009, 2016.

[425] F Acernese, M Agathos, K Agatsuma, D Aisa, N Allemandou, A Allocca, J Amarni, P Astone, G Balestri, G Ballardin, et al. Advanced virgo: a second-generation interferometric gravitational wave detector. *Classical and Quantum Gravity*, 32(2):024001, 2014.

[426] Yoichi Aso, Yuta Michimura, Kentaro Somiya, Masaki Ando, Osamu Miyakawa, Takanori Sekiguchi, Daisuke Tatsumi, Hiroaki Yamamoto, KAGRA Collaboration, et al. Interferometer design of the kagra gravitational wave detector. *Physical Review D*, 88(4):043007, 2013.

[427] Magdalena Szczykulska, Tillmann Baumgratz, and Animesh Datta. Multi-parameter quantum metrology. *Advances in Physics: X*, 1(4):621–639, 2016.

[428] Francesco Albarelli, Marco Barbieri, Marco G Genoni, and Ilaria Gianani. A perspective on multiparameter quantum metrology: from theoretical tools to applications in quantum imaging. *Physics Letters A*, page 126311, 2020.

[429] Chenglong You, Sushovit Adhikari, Yuxi Chi, Margarite L LaBorde, Corey T Matyas, Chenyu Zhang, Zuen Su, Tim Byrnes, Chaoyang Lu, Jonathan P Dowling, et al. Multiparameter estimation with single photons—linearly-optically generated quantum entanglement beats the shotnoise limit. *Journal of Optics*, 19(12):124002, 2017.

[430] Manuel Gessner, Augusto Smerzi, and Luca Pezzè. Metrological multiparameter squeezing. *arXiv preprint arXiv:1910.14014*, 2019.

[431] Jasminder S Sidhu and Pieter Kok. Geometric perspective on quantum parameter estimation. *AVS Quantum Science*, 2(1):014701, 2020.

[432] Ilaria Gianani, Marco G Genoni, and Marco Barbieri. Assessing data postprocessing for quantum estimation. *arXiv preprint arXiv:1909.02313*, 2019.

[433] Luca Pezzé and Augusto Smerzi. Quantum theory of phase estimation. In *Atom Interferometry, Proceedings of the International School of Physics Enrico Fermi*, page 691. edited by G. M. Tino and M. A. Kasevich (IOS Press, Amsterdam), 2014.

[434] Géza Tóth and Iagoba Apellaniz. Quantum metrology from a quantum information science perspective. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424006, 2014.

[435] Rafal Demkowicz-Dobrzanski, Wojciech Gorecki, and Madalin Guta. Multi-parameter estimation beyond quantum fisher information. *arXiv preprint arXiv:2001.11742*, 2020.

[436] Chuan Xu, Lidan Zhang, Songtao Huang, Taxue Ma, Fang Liu, Hidehiro Yonezawa, Yong Zhang, and Min Xiao. Sensing and tracking enhanced by quantum squeezing. *Photonics Research*, 7(6):A14–A26, 2019.

[437] Kok Chuan Tan and Hyunseok Jeong. Nonclassical light and metrological power: An introductory review. *AVS Quantum Science*, 1(1):014701, 2019.

[438] Roman Schnabel. Squeezed states of light and their applications in laser interferometers. *Physics Reports*, 684:1–51, 2017.

[439] Jonathan P Dowling and Kaushik P Seshadreesan. Quantum optical technologies for metrology, sensing, and imaging. *Journal of Lightwave Technology*, 33(12):2359–2370, 2015.

[440] Rafal Demkowicz-Dobrzański, Marcin Jarzyna, and Jan Kołodyński. Quantum limits in optical interferometry. In *Progress in Optics*, volume 60, pages 345–435. Elsevier, 2015.

[441] Jian Ma, Xiaoguang Wang, Chang-Pu Sun, and Franco Nori. Quantum spin squeezing. *Physics Reports*, 509(2-3):89–165, 2011.

[442] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J Cerf, Timothy C Ralph, Jeffrey H Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84(2):621, 2012.

[443] Gerardo Adesso, Sammy Ragy, and Antony R Lee. Continuous variable quantum information: Gaussian states and beyond. *Open Systems & Information Dynamics*, 21(01n02):1440001, 2014.

[444] Ronald 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.

[445] H. Cramer. *Mathematical Methods of Statistics*. Princeton University, 1946.

[446] CR Rao. Information and accuracy attainable in the estimation of statistical parameters. *Bull Calcutta. Math. Soc.*, 37:81–91, 1945.

[447] CW Helstrom and R Kennedy. Noncommuting observables in quantum detection and estimation theory. *IEEE Transactions on Information Theory*, 20(1):16–24, 1974.

[448] Erich L Lehmann and George Casella. *Theory of point estimation*. Springer Science & Business Media, 2006.

[449] Jun Suzuki. Information geometrical characterization of quantum statistical models in quantum estimation theory. *Entropy*, 21(7):703, 2019.

[450] William K Wootters. Statistical distance and hilbert space. *Physical Review D*, 23(2):357, 1981.

[451] Samuel L Braunstein and Carlton M Caves. Statistical distance and the geometry of quantum states. *Physical Review Letters*, 72(22):3439, 1994.

[452] Luca Pezzè, Yan Li, Weidong Li, and Augusto Smerzi. Witnessing entanglement without entanglement witness operators. *Proceedings of the National Academy of Sciences*, 113(41):11459–11464, 2016.

[453] Hans-Jürgen Sommers and Karol Zyczkowski. Bures volume of the set of mixed quantum states. *Journal of Physics A: Mathematical and General*, 36(39):10083, 2003.

[454] Jesús Rubio. Non-asymptotic quantum metrology. *arXiv preprint arXiv:1912.02324*, 2019.

[455] Richard D Gill and Serge Massar. State estimation for large ensembles. *Physical Review A*, 61(4):042312, 2000.

[456] Akio Fujiwara. Strong consistency and asymptotic efficiency for adaptive quantum estimation problems. *Journal of Physics A: Mathematical and General*, 39(40):12489, 2006.

[457] Masahito Hayashi. *Quantum Information Theory*. Springer, 2017.

[458] Masahito Hayashi and Keiji Matsumoto. Asymptotic performance of optimal state estimation in qubit system. *Journal of Mathematical Physics*, 49(10):102101, 2008.

[459] Hiroshi Nagaoka. On the parameter estimation problem for quantum statistical models. In *Asymptotic Theory Of Quantum Statistical Inference: Selected Papers*, pages 125–132. World Scientific, 2005.

[460] Luca Pezzé and Augusto Smerzi. Entanglement, nonlinear dynamics, and the heisenberg limit. *Physical Review Letters*, 102(10):100401, 2009.

[461] Samuel L Braunstein. Quantum limits on precision measurements of phase. *Physical Review Letters*, 69(25):3598, 1992.

[462] Hwang Lee, Pieter Kok, and Jonathan P Dowling. A quantum rosetta stone for interferometry. *Journal of Modern Optics*, 49(14-15):2325–2338, 2002.

[463] Bernd Lücke, Manuel Scherer, Jens Kruse, Luca Pezzé, Frank Deuretzbacher, Phillip Hyllus, Jan Peise, Wolfgang Ertmer, Jan Arlt, Luis Santos, et al. Twin matter waves for interferometry beyond the classical limit. *Science*, 334(6057):773–776, 2011.

[464] Roland Krischek, Christian Schwemmer, Witlef Wieczorek, Harald Weinfurter, Philipp Hyllus, Luca Pezzé, and Augusto Smerzi. Useful multiparticle entanglement and sub-shot-noise sensitivity in experimental phase estimation. *Physical Review Letters*, 107(8):080504, 2011.

[465] Philipp Hyllus, Wiesław Laskowski, Roland Krischek, Christian Schwemmer, Witlef Wieczorek, Harald Weinfurter, Luca Pezzé, and Augusto Smerzi. Fisher information and multiparticle entanglement. *Physical Review A*, 85(2):022321, 2012.

[466] Helmut Strobel, Wolfgang Muessel, Daniel Linnemann, Tilman Zibold, David B Hume, Luca Pezzè, Augusto Smerzi, and Markus K Oberthaler. Fisher information and entanglement of non-gaussian spin states. *Science*, 345(6195):424–427, 2014.

[467] Manuel Gessner, Luca Pezzè, and Augusto Smerzi. Sensitivity bounds for multiparameter quantum metrology. *Physical review letters*, 121(13):130503, 2018.

[468] Alfredo Luis. Nonlinear transformations and the heisenberg limit. *Physics Letters A*, 329(1-2):8–13, 2004.

[469] Sergio Boixo, Steven T Flammia, Carlton M Caves, and John M Geremia. Generalized limits for single-parameter quantum estimation. *Physical Review Letters*, 98(9):090401, 2007.

[470] S Choi and B Sundaram. Bose-einstein condensate as a nonlinear ramsey interferometer operating beyond the heisenberg limit. *Physical Review A*, 77(5):053613, 2008.

[471] Marcin Zwierz, Carlos A Pérez-Delgado, and Pieter Kok. Ultimate limits to quantum metrology and the meaning of the heisenberg limit. *Physical Review A*, 85(4):042112, 2012.

[472] Wim van Dam, G Mauro D'Ariano, Artur Ekert, Chiara Macchiavello, and Michele Mosca. Optimal quantum circuits for general phase estimation. *Physical review letters*, 98(9):090501, 2007.

[473] Brendon L Higgins, Dominic W Berry, Stephen D Bartlett, Howard M Wiseman, and Geoff J Pryde. Entanglement-free heisenberg-limited phase estimation. *Nature*, 450(7168):393, 2007.

[474] Kevin J Resch, Kenneth L Pregnell, Robert Prevedel, Alexei Gilchrist, Geoff J Pryde, Jeremy L O'Brien, and Andrew G White. Time-reversal and superresolving phase measurements. *Physical Review Letters*, 98(22):223601, 2007.

[475] Dominic W Berry, Brendon L Higgins, Stephen D Bartlett, Morgan W Mitchell, Geoff J Pryde, and Howard M Wiseman. How to perform the most accurate possible phase measurements. *Physical Review A*, 80(5):052114, 2009.

[476] BL Higgins, DW Berry, SD Bartlett, MW Mitchell, HM Wiseman, and GJ Pryde. Demonstrating heisenberg-limited unambiguous phase estimation without adaptive measurements. *New Journal of Physics*, 11(7):073023, 2009.

[477] Itai Afek, Oron Ambar, and Yaron Silberberg. Classical bound for mach-zehnder superresolution. *Physical Review Letters*, 104(12):123602, 2010.

[478] Carl Wilhelm Helstrom. *Quantum detection and estimation theory*. Academic press, 1976.

[479] Horace Yuen and Melvin Lax. Multiple-parameter quantum estimation and measurement of nonselfadjoint observables. *IEEE Transactions on Information Theory*, 19(6):740–750, 1973.

[480] Keiji Matsumoto. A new approach to the cramér-rao-type bound of the pure-state model. *Journal of Physics A: Mathematical and General*, 35(13):3111, 2002.

[481] Akio Fujiwara. Estimation of su (2) operation and dense coding: An information geometric approach. *Physical Review A*, 65(1):012316, 2001.

[482] Luca Pezzè, Mario A Ciampini, Nicolò Spagnolo, Peter C Humphreys, Animesh Datta, Ian A Walmsley, Marco Barbieri, Fabio Sciarrino, and Augusto Smerzi. Optimal measurements for simultaneous quantum estimation of multiple phases. *Physical review letters*, 119(13):130504, 2017.

[483] OE Barndorff-Nielsen and RD Gill. Fisher information in quantum statistics. *Journal of Physics A: Mathematical and General*, 33(24):4481, 2000.

[484] Sammy Ragy, Marcin Jarzyna, and Rafał Demkowicz-Dobrzański. Compatibility in multiparameter quantum metrology. *Physical Review A*, 94(5):052108, 2016.

[485] Peter C Humphreys, Marco Barbieri, Animesh Datta, and Ian A Walmsley. Quantum enhanced multiple phase estimation. *Physical review letters*, 111(7):070403, 2013.

[486] Timothy J Proctor, Paul A Knott, and Jacob A Dunningham. Multiparameter estimation in networked quantum sensors. *Physical review letters*, 120(8):080501, 2018.

[487] Wenchao Ge, Kurt Jacobs, Zachary Eldredge, Alexey V Gorshkov, and Michael Foss-Feig. Distributed quantum metrology with linear networks and separable inputs. *Physical review letters*, 121(4):043604, 2018.

[488] Steven M Kay. *Fundamentals of statistical signal processing*. Prentice Hall PTR, 1993.

[489] Z Hradil, R Myška, J Peřina, M Zawisky, Y Hasegawa, and H Rauch. Quantum phase in interferometry. *Physical review letters*, 76(23):4295, 1996.

[490] George EP Box and George C Tiao. *Bayesian inference in statistical analysis*, volume 40. John Wiley & Sons, 2011.

[491] DW Berry and HM Wiseman. Optimal states and almost optimal adaptive measurements for quantum interferometry. *Physical Review Letters*, 85(24):5098, 2000.

[492] Valeria Cimini, Marco G. Genoni, Ilaria Gianani, Nicolò Spagnolo, Fabio Sciarrino, and Marco Barbieri. Diagnosing imperfections in quantum sensors via generalized cramér-rao bounds. *Physical Review Applied*, 13(2):024048, 2020.

[493] AS Holevo. Covariant measurements and imprimitivity systems. In *Quantum Probability and Applications to the Quantum Theory of Irreversible Processes*, pages 153–172. Springer, 1984.

[494] L Pezzé, A Smerzi, G Khoury, JF Hodelin, and D Bouwmeester. Phase detection at the quantum limit with multiphoton mach-zehnder interferometry. *Physical review letters*, 99(22):223602, 2007.

[495] Harry L Van Trees and Kristine L Bell. Bayesian bounds for parameter estimation and nonlinear filtering/tracking. *AMC*, 10:12, 2007.

[496] Yan Li, Luca Pezzè, Manuel Gessner, Zhihong Ren, Weidong Li, and Augusto Smerzi. Frequentist and bayesian quantum phase estimation. *Entropy*, 20(9):628, 2018.

[497] GM D'Ariano, C Macchiavello, and MF Sacchi. On the general problem of quantum phase estimation. *Physics Letters A*, 248(2-4):103–108, 1998.

[498] Christopher R Ekstrom, Jörg Schmiedmayer, Michael S Chapman, Troy D Hammond, and David E Pritchard. Measurement of the electric polarizability of sodium with an atom interferometer. *Physical Review A*, 51(5):3883, 1995.

[499] Rym Bouchendira, Pierre Cladé, Saïda Guellati-Khélifa, François Nez, and François Biraben. New determination of the fine structure constant and test of the quantum electrodynamics. *Physical Review Letters*, 106(8):080801, 2011.

[500] Scott A Diddams, James C Bergquist, Steven R Jefferts, and Christopher W Oates. Standards of time and frequency at the outset of the 21st century. *Science*, 306(5700):1318–1324, 2004.

[501] Achim Peters, Keng Yeow Chung, and Steven Chu. Measurement of gravitational acceleration by dropping atoms. *Nature*, 400(6747):849, 1999.

[502] Karol Gietka, Farokh Mivehvar, and Helmut Ritsch. Supersolid-based gravimeter in a ring cavity. *Physical review letters*, 122(19):190801, 2019.

[503] Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto. Differential phase shift quantum key distribution. *Physical review letters*, 89(3):037902, 2002.

[504] Jeffrey H Shapiro and Scott R Shepard. Quantum phase measurement: A system-theory perspective. *Physical Review A*, 43(7):3795, 1991.

[505] Robert Lynch. The quantum phase problem: a critical review. *Physics Reports*, 256(6):367–436, 1995.

[506] Luca Pezzé and Augusto Smerzi. Phase sensitivity of a mach-zehnder interferometer. *Physical Review A*, 73(1):011801, 2006.

[507] BC Sanders and GJ Milburn. Optimal quantum measurements for phase estimation. *Physical Review Letters*, 75(16):2944, 1995.

[508] He-Liang Huang, Yi-Han Luo, B Bai, Y-H Deng, H Wang, Q Zhao, H-S Zhong, Y-Q Nie, W-H Jiang, X-L Wang, et al. Compatibility of causal hidden-variable theories with a delayed-choice experiment. *Physical Review A*, 100(1):012114, 2019.

[509] Emanuele Polino, Iris Agresti, Davide Poderini, Gonzalo Carvacho, Giorgio Milani, Gabriela Barreto Lemos, Rafael Chaves, and Fabio Sciarrino. Device-independent test of a delayed choice experiment. *Phys. Rev. A*, 100:022111, Aug 2019.

[510] Adil S Rab, Emanuele Polino, Zhong-Xiao Man, Nguyen Ba An, Yun-Jie Xia, Nicolò Spagnolo, Rosario Lo Franco, and Fabio Sciarrino. Entanglement of photons in their dual wave-particle nature. *Nature communications*, 8(1):915, 2017.

[511] Chiara Marletto and Vlatko Vedral. Gravitationally induced entanglement between two massive particles is sufficient evidence of quantum effects in gravity. *Physical review letters*, 119(24):240402, 2017.

[512] Marios Christodoulou and Carlo Rovelli. On the possibility of laboratory evidence for quantum superposition of geometries. *Physics Letters B*, 792:64–68, 2019.

[513] Lu Zhang and Kam Wai Clifford Chan. Quantum multiparameter estimation with generalized balanced multimode noon-like states. *Physical Review A*, 95(3):032321, 2017.

[514] Chiara Macchiavello. Optimal estimation of multiple phases. *Physical Review A*, 67(6):062302, 2003.

[515] Manuel A Ballester. Entanglement is not very useful for estimating multiple phases. *Physical Review A*, 70(3):032310, 2004.

[516] Jing Liu, Xiao-Ming Lu, Zhe Sun, and Xiaoguang Wang. Quantum multiparameter metrology with generalized entangled coherent state. *Journal of Physics A: Mathematical and Theoretical*, 49(11):115302, 2016.

[517] Christos N Gagatsos, Dominic Branford, and Animesh Datta. Gaussian systems for quantum-enhanced multiple phase estimation. *Physical Review A*, 94(4):042342, 2016.

[518] Mario A Ciampini, Nicolò Spagnolo, Chiara Vitelli, Luca Pezzè, Augusto Smerzi, and Fabio Sciarrino. Quantum-enhanced multiparameter estimation in multiarm interferometers. *Scientific reports*, 6:28881, 2016.

[519] Dario Gatto, Paolo Facchi, Frank A Narducci, and Vincenzo Tamma. Distributed quantum metrology with a single squeezed-vacuum source. *Physical Review Research*, 1(3):032024, 2019.

[520] Xueshi Guo, Casper R Breum, Johannes Borregaard, Shuro Izumi, Mikkel V Larsen, Tobias Gehring, Matthias Christandl, Jonas S Neergaard-Nielsen, and Ulrik L Andersen. Distributed quantum sensing in a continuous-variable entangled network. *Nature Physics*, 16(3):281–284, 2020.

[521] Changhun Oh, Changhyoup Lee, Seok Hyung Lie, and Hyunseok Jeong. Optimal distributed quantum sensing using gaussian states. *arXiv preprint arXiv:1910.00823*, 2020.

[522] T Baumgratz and A Datta. Quantum enhanced estimation of a multidimensional field. *Physical review letters*, 116(3):030801–030801, 2016.

[523] Nicolò Spagnolo, Chiara Vitelli, Lorenzo Aparo, Paolo Mataloni, Fabio Sciarrino, Andrea Crespi, Roberta Ramponi, and Roberto Osellame. Three-photon bosonic coalescence in an integrated tritter. *Nature communications*, 4:1606, 2013.

[524] Xueshi Guo, Casper R Breum, Johannes Borregaard, Shuro Izumi, Mikkel V Larsen, Tobias Gehring, Matthias Christandl, Jonas S Neergaard-Nielsen, and Ulrik L Andersen. Distributed quantum sensing in a continuous-variable entangled network. *Nature Physics*, pages 1–4, 2019.

[525] Emanuele Roccia, Valeria Cimini, Marco Sbroscia, Ilaria Gianani, Ludovica Ruggiero, Luca Mancino, Marco G Genoni, Maria Antonietta Ricci, and Marco Barbieri. Multiparameter approach to quantum phase estimation with limited visibility. *Optica*, 5(10):1171–1176, 2018.

[526] Valeria Cimini, Ilaria Gianani, Ludovica Ruggiero, Tecla Gasperi, Marco Sbroscia, Emanuele Roccia, Daniela Tofani, Fabio Bruni, Maria Antonietta Ricci, and Marco Barbieri. Quantum sensing for dynamical tracking of chemical processes. *Physical Review A*, 99(5):053817, 2019.

[527] Valeria Cimini, Marta Mellini, Giordano Rampioni, Marco Sbroscia, Emanuele Roccia, Livia Leoni, Marco Barbieri, and Ilaria Gianani. Adaptive tracking of enzymatic reactions with quantum light. *Optics Express*, 27(24):35245–35256, 2019.

[528] Quntao Zhuang, Zheshen Zhang, and Jeffrey H Shapiro. Distributed quantum sensing using continuous-variable multipartite entanglement. *Physical Review A*, 97(3):032329, 2018.

[529] Yi Xia, Wei Li, William Clark, Darlene Hart, Quntao Zhuang, and Zheshen Zhang. Entangled radiofrequency-photonic sensor network. *arXiv preprint arXiv:1910.08825*, 2019.

[530] Toshimitsu Musha, Jun-ichi Kamimura, and Masataka Nakazawa. Optical phase fluctuations thermally induced in a single-mode optical fiber. *Applied optics*, 21(4):694–698, 1982.

[531] Jiangbing Du and Zuyuan He. Sensitivity enhanced strain and temperature measurements based on fbg and frequency chirp magnification. *Optics express*, 21(22):27111–27118, 2013.

[532] Mihai D Vidrighin, Gaia Donati, Marco G Genoni, Xian-Min Jin, W Steven Kolthammer, MS Kim, Animesh Datta, Marco Barbieri, and Ian A Walmsley. Joint estimation of phase and phase diffusion for quantum metrology. *Nature communications*, 5(1):1–7, 2014.

[533] Emanuele Roccia, Ilaria Gianani, Luca Mancino, Marco Sbroscia, Fabrizia Somma, Marco G Genoni, and Marco Barbieri. Entangling measurements for multiparameter estimation with two qubits. *Quantum Science and Technology*, 3(1):01LT01, 2017.

[534] Matteo Altorio, Marco G Genoni, Mihai D Vidrighin, Fabrizia Somma, and Marco Barbieri. Weak measurements and the joint estimation of phase and phase diffusion. *Physical Review A*, 92(3):032114, 2015.

[535] Rafal Demkowicz-Dobrzański and Lorenzo Maccone. Using entanglement against noise in quantum metrology. *Physical review letters*, 113(25):250801, 2014.

[536] Samuel L Braunstein, Carlton M Caves, and Gerard J Milburn. Generalized uncertainty relations: theory, examples, and lorentz invariance. *annals of physics*, 247(1):135–173, 1996.

[537] Alfredo Luis. Phase-shift amplification for precision measurements without nonclassical states. *Physical Review A*, 65(2):025802, 2002.

[538] Terry Rudolph and Lov Grover. Quantum communication complexity of establishing a shared reference frame. *Physical review letters*, 91(21):217905, 2003.

[539] Masahiro Hotta, Tokishiro Karasawa, and Masanao Ozawa. Ancilla-assisted enhancement of channel estimation for low-noise parameters. *Physical Review A*, 72(5):052334, 2005.

[540] Zixin Huang, Chiara Macchiavello, and Lorenzo Maccone. Usefulness of entanglement-assisted quantum metrology. *Physical Review A*, 94(1):012101, 2016.

[541] Zixin Huang, Chiara Macchiavello, and Lorenzo Maccone. Noise-dependent optimal strategies for quantum metrology. *Physical Review A*, 97(3):032333, 2018.

[542] Marco Sbroscia, Ilaria Gianani, Luca Mancino, Emanuele Roccia, Zixin Huang, Lorenzo Maccone, Chiara Macchiavello, and Marco Barbieri. Experimental ancilla-assisted phase estimation in a noisy channel. *Physical Review A*, 97(3):032305, 2018.

[543] Kunkun Wang, Xiaoping Wang, Xiang Zhan, Zhihao Bian, Jian Li, Barry C Sanders, and Peng Xue. Entanglement-enhanced quantum metrology in a noisy environment. *Physical Review A*, 97(4):042112, 2018.

[544] Howard M Wiseman. Adaptive phase measurements of optical modes: Going beyond the marginal q distribution. *Physical Review Letters*, 75(25):4587, 1995.

[545] Andrew C Doherty, Salman Habib, Kurt Jacobs, Hideo Mabuchi, and Sze M Tan. Quantum feedback control and classical control theory. *Physical Review A*, 62(1):012105, 2000.

[546] Howard M Wiseman, Dominic W Berry, Stephen D Bartlett, Brendon L Higgins, and Geoffrey J Pryde. Adaptive measurements in the optical quantum information laboratory. *IEEE Journal of Selected Topics in Quantum Electronics*, 15(6):1661–1672, 2009.

[547] Alessio Serafini. Feedback control in quantum optics: An overview of experimental breakthroughs and areas of application. *ISRN Optics*, 2012, 2012.

[548] Jing Zhang, Yu-xi Liu, Re-Bing Wu, Kurt Jacobs, and Franco Nori. Quantum feedback: theory, experiments, and applications. *Physics Reports*, 679:1–60, 2017.

[549] Rafał Demkowicz-Dobrzański, Jan Czajkowski, and Pavel Sekatski. Adaptive quantum metrology under general markovian noise. *Physical Review X*, 7(4):041009, 2017.

[550] Stefano Pirandola and Cosmo Lupo. Ultimate precision of adaptive noise estimation. *Physical review letters*, 118(10):100502, 2017.

[551] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature communications*, 8(1):1–15, 2017.

[552] MW Mitchell. Metrology with entangled states. In *Quantum Communications and Quantum Imaging III*, volume 5893, page 589310. International Society for Optics and Photonics, 2005.

[553] Jesús Rubio and Jacob Dunningham. Quantum metrology in the presence of limited data. *New Journal of Physics*, 21(4):043037, 2019.

[554] Wojciech Górecki, Rafał Demkowicz-Dobrzański, Howard M Wiseman, and Dominic W Berry. π-corrected heisenberg limit. *Physical Review Letters*, 124(3):030501, 2020.

[555] Giacomo M D'Ariano, Matteo GA Paris, and Raffaella Seno. Feedback-assisted homodyne detection of phase shifts. *Physical Review A*, 54(5):4495, 1996.

[556] Dominic W Berry and Howard M Wiseman. Adaptive quantum measurements of a continuously varying phase. *Physical Review A*, 65(4):043803, 2002.

[557] Hidehiro Yonezawa, Daisuke Nakane, Trevor A Wheatley, Kohjiro Iwasawa, Shuntaro Takeda, Hajime Arao, Kentaro Ohki, Koji Tsumura, Dominic W Berry, Timothy C Ralph, et al. Quantum-enhanced optical-phase tracking. *Science*, 337(6101):1514–1517, 2012.

[558] Eric M Kessler, Igor Lovchinsky, Alexander O Sushkov, and Mikhail D Lukin. Quantum error correction for metrology. *Physical review letters*, 112(15):150802, 2014.

[559] W Dür, M Skotiniotis, Florian Froewis, and B Kraus. Improved quantum metrology using quantum error correction. *Physical Review Letters*, 112(8):080801, 2014.

[560] Shibdas Roy, Ian R Petersen, and Elanor H Huntington. Robust adaptive quantum phase estimation. *New Journal of Physics*, 17(6):063020, 2015.

[561] Martin B Plenio and Susana F Huelga. Sensing in the presence of an observed environment. *Physical Review A*, 93(3):032123, 2016.

[562] Shengshi Pang and Andrew N Jordan. Optimal adaptive control for quantum metrology with time-dependent hamiltonians. *Nature communications*, 8:14695, 2017.

[563] Pavel Sekatski, Michalis Skotiniotis, Janek Kołodyński, and Wolfgang Dür. Quantum metrology with full and fast quantum control. *Quantum*, 1:27, 2017.

[564] Cristian Bonato and Dominic W Berry. Adaptive tracking of a time-varying field with a quantum sensor. *Physical Review A*, 95(5):052348, 2017.

[565] David Layden and Paola Cappellaro. Spatial noise filtering through error correction for quantum sensing. *npj Quantum Information*, 4(1):1–6, 2018.

[566] Sisi Zhou, Mengzhen Zhang, John Preskill, and Liang Jiang. Achieving the heisenberg limit in quantum metrology using quantum error correction. *Nature communications*, 9(1):1–11, 2018.

[567] Lidan Zhang, Kaimin Zheng, Fang Liu, Wei Zhao, Lei Tang, Hidehiro Yonezawa, Lijian Zhang, Yong Zhang, and Min Xiao. Quantum-limited fiber-optic phase tracking beyond π range. *Optics express*, 27(3):2327–2334, 2019.

[568] Quntao Zhuang, John Preskill, and Liang Jiang. Distributed quantum sensing enhanced by continuous-variable error correction. *New Journal of Physics*, 2020.

[569] Alexander Hentschel and Barry C Sanders. Machine learning for precise quantum measurement. *Physical review letters*, 104(6):063603, 2010.

[570] Alexander Hentschel and Barry C Sanders. Efficient algorithm for optimizing adaptive quantum metrology processes. *Physical review letters*, 107(23):233601, 2011.

[571] Neil B Lovett, Cécile Crosnier, Martí Perarnau-Llobet, and Barry C Sanders. Differential evolution for many-particle adaptive quantum metrology. *Physical review letters*, 110(22):220501, 2013.

[572] Pantita Palittapongarnpim, Peter Wittek, Ehsan Zahedinejad, Shakib Vedaie, and Barry C Sanders. Learning in quantum control: High-dimensional global optimization for noisy quantum dynamics. *Neurocomputing*, 268:116–126, 2017.

[573] Pantita Palittapongarnpim and Barry C Sanders. Robustness of quantum-enhanced adaptive phase estimation. *Physical Review A*, 100(1):012106, 2019.

[574] Takanori Sugiyama, Peter S Turner, and Mio Murao. Adaptive experimental design for one-qubit state estimation with finite data based on a statistical update criterion. *Physical Review A*, 85(5):052107, 2012.

[575] Ferenc Huszár and Neil MT Houlsby. Adaptive bayesian quantum tomography. *Physical Review A*, 85(5):052120, 2012.

[576] Dylan H Mahler, Lee A Rozema, Ardavan Darabi, Christopher Ferrie, Robin Blume-Kohout, and AM Steinberg. Adaptive quantum state tomography improves accuracy quadratically. *Physical review letters*, 111(18):183601, 2013.

[577] Christopher Granade, Joshua Combes, and DG Cory. Practical bayesian tomography. *New Journal of Physics*, 18(3):033024, 2016.

[578] Ryo Okamoto, Minako Iefuji, Satoshi Oyama, Koichi Yamagata, Hiroshi Imai, Akio Fujiwara, and Shigeki Takeuchi. Experimental demonstration of adaptive quantum state estimation. *Physical review letters*, 109(13):130404, 2012.

[579] KS Kravtsov, SS Straupe, IV Radchenko, NMT Houlsby, F Huszár, and SP Kulik. Experimental adaptive bayesian tomography. *Physical Review A*, 87(6):062122, 2013.

[580] Gleb I Struchalin, Ivan A Pogorelov, Stanislav S Straupe, Konstantin S Kravtsov, Igor V Radchenko, and Sergei P Kulik. Experimental adaptive quantum tomography of two-qubit states. *Physical Review A*, 93(1):012103, 2016.

[581] Bo Qi, Zhibo Hou, Yuanlong Wang, Daoyi Dong, Han-Sen Zhong, Li Li, Guo-Yong Xiang, Howard M Wiseman, Chuan-Feng Li, and Guang-Can Guo. Adaptive quantum state tomography via linear regression estimation: Theory and two-qubit experiment. *npj Quantum Information*, 3(1):1–7, 2017.

[582] Ryo Okamoto, Satoshi Oyama, Koichi Yamagata, Akio Fujiwara, and Shigeki Takeuchi. Experimental demonstration of adaptive quantum state estimation for single photonic qubits. *Physical Review A*, 96(2):022124, 2017.

[583] Michael A Armen, John K Au, John K Stockton, Andrew C Doherty, and Hideo Mabuchi. Adaptive homodyne measurement of optical phase. *Physical Review Letters*, 89(13):133602, 2002.

[584] TA Wheatley, DW Berry, H Yonezawa, D Nakane, H Arao, DT Pope, TC Ralph, HM Wiseman, A Furusawa, and EH Huntington. Adaptive optical phase estimation using time-symmetric quantum smoothing. *Physical Review Letters*, 104(9):093601, 2010.

[585] Robert L Cook, Paul J Martin, and John M Geremia. Optical coherent state discrimination using a closed-loop quantum measurement. *Nature*, 446(7137):774, 2007.

[586] Dominic W Berry, HM Wiseman, and JK Breslin. Optimal input states and feedback for interferometric phase estimation. *Physical Review A*, 63(5):053804, 2001.

[587] Guo-Yong Xiang, Brendon Lloyd Higgins, DW Berry, Howard Mark Wiseman, and GJ Pryde. Entanglement-enhanced measurement of a completely unknown optical phase. *Nature Photonics*, 5(1):43, 2011.

[588] Alex Monras. Optimal phase measurements with pure gaussian states. *Physical Review A*, 73(3):033821, 2006.

[589] Stefano Olivares and Matteo GA Paris. Bayesian estimation in homodyne interferometry. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 42(5):055506, 2009.

[590] Adriano A Berni, Tobias Gehring, Bo M Nielsen, Vitus Händchen, Matteo GA Paris, and Ulrik L Andersen. Ab initio quantum-enhanced optical phase estimation using real-time feedback control. *Nature Photonics*, 9(9):577, 2015.

[591] Zixin Huang, Keith R Motes, Petr M Anisimov, Jonathan P Dowling, and Dominic W Berry. Adaptive phase estimation with two-mode squeezed vacuum and parity measurement. *Physical Review A*, 95(5):053837, 2017.

[592] AY KITAEV. Quantum measurements and the abelian stabilizer problem. In *Electronic Colloq. on Computational Complexity*, 1996.

[593] Shakib Daryanoosh, Sergei Slussarenko, Dominic W Berry, Howard M Wiseman, and Geoff J Pryde. Experimental optical phase measurement approaching the exact heisenberg limit. *Nature communications*, 9(1):4606, 2018.

[594] Tim C Ralph and Geoff J Pryde. Optical quantum computation. In *Progress in optics*, volume 54, pages 209–269. Elsevier, 2010.

[595] Nathan Wiebe and Chris Granade. Efficient bayesian phase estimation. *Physical review letters*, 117(1):010503, 2016.

[596] Stefano Paesani, Andreas A Gentile, Raffaele Santagati, Jianwei Wang, Nathan Wiebe, David P Tew, Jeremy L O'Brien, and Mark G Thompson. Experimental bayesian quantum phase estimation on a silicon photonic chip. *Physical review letters*, 118(10):100503, 2017.

[597] Alessandro Lumino, Emanuele Polino, Adil S Rab, Giorgio Milani, Nicolò Spagnolo, Nathan Wiebe, and Fabio Sciarrino. Experimental phase estimation enhanced by machine learning. *Physical Review Applied*, 10(4):044033, 2018.

[598] Kevin P Murphy. *Machine learning: a probabilistic perspective*. MIT press, 2012.

[599] Phil Simon. *Too big to ignore: the business case for big data*, volume 72. John Wiley & Sons, 2013.

[600] Valeria Cimini, Ilaria Gianani, Nicolò Spagnolo, Fabio Leccese, Fabio Sciarrino, and Marco Barbieri. Calibration of quantum sensors by neural networks. *Physical Review Letters*, 123(23):230502, 2019.

[601] Yi Peng and Heng Fan. Feedback ansatz for adaptive-feedback quantum metrology training with machine learning. *Physical Review A*, 101(2):022107, 2020.

[602] Jonas Schuff, Lukas Jan Fiderer, and Daniel Braun. Improving the dynamics of quantum sensors with reinforcement learning. *New Journal of Physics*, 22(3):035001, 2020.

[603] Quntao Zhuang and Zheshen Zhang. Physical-layer supervised learning assisted by an entangled sensor network. *Physical Review X*, 9(4):041023, 2019.

[604] Agoston E Eiben, James E Smith, et al. *Introduction to evolutionary computing*, volume 53. Springer, 2003.

[605] Pradnya A Vikhar. Evolutionary algorithms: A critical review and its future prospects. In *2016 International conference on global trends in signal processing, information computing and communication (ICGTSPICC)*, pages 261–265. IEEE, 2016.

[606] Russell Eberhart and James Kennedy. A new optimizer using particle swarm theory. In *MHS'95. Proceedings of the Sixth International Symposium on Micro Machine and Human Science*, pages 39–43. Ieee, 1995.

[607] Christian Blum and Xiaodong Li. Swarm intelligence in optimization. In *Swarm intelligence*, pages 43–85. Springer, 2008.

[608] Heedeuk Shin, Kam Wai Clifford Chan, Hye Jeong Chang, and Robert W Boyd. Quantum spatial superresolution by optical centroid measurements. *Physical review letters*, 107(8):083603, 2011.

[609] Michael A Taylor, Jiri Janousek, Vincent Daria, Joachim Knittel, Boris Hage, Hans-A Bachor, and Warwick P Bowen. Biological measurement beyond the quantum limit. *Nature Photonics*, 7(3):229–233, 2013.

[610] Xiao-Qi Zhou, Hugo Cable, Rebecca Whittaker, Peter Shadbolt, Jeremy L O'Brien, and Jonathan CF Matthews. Quantum-enhanced tomography of unitary processes. *Optica*, 2(6):510–516, 2015.

[611] Emanuele Roccia, Valeria Cimini, Marco Sbroscia, Ilaria Gianani, Ludovica Ruggiero, Luca Mancino, Marco G Genoni, Maria Antonietta Ricci, and Marco Barbieri. Multiparameter quantum estimation of noisy phase shifts. *arXiv preprint arXiv:1805.02561*, 2018.

[612] Sebastian Steinlechner, Jöran Bauchrowitz, Melanie Meinders, Helge Müller-Ebhardt, Karsten Danzmann, and Roman Schnabel. Quantum-dense metrology. *Nature Photonics*, 7(8):626–630, 2013.

[613] Nicolò Spagnolo, Lorenzo Aparo, Chiara Vitelli, Andrea Crespi, Roberta Ramponi, Roberto Osellame, Paolo Mataloni, and Fabio Sciarrino. Quantum interferometry with three-dimensional geometry. *Scientific reports*, 2(1):1–6, 2012.

[614] Fulvio Flamini, Lorenzo Magrini, Adil S Rab, Nicolò Spagnolo, Vincenzo D'ambrosio, Paolo Mataloni, Fabio Sciarrino, Tommaso Zandrini, Andrea Crespi, Roberta Ramponi, et al. Thermally reconfigurable quantum photonic circuits at telecom wavelength by femtosecond laser micromachining. *Light: Science & Applications*, 4(11):e354–e354, 2015.

[615] Michael Reck, Anton Zeilinger, Herbert J Bernstein, and Philip Bertani. Experimental realization of any discrete unitary operator. *Physical review letters*, 73(1):58, 1994.

[616] Nicholas C Harris, Gregory R Steinbrecher, Mihika Prabhu, Yoav Lahini, Jacob Mower, Darius Bunandar, Changchen Chen, Franco NC Wong, Tom Baehr-Jones, Michael Hochberg, et al. Quantum transport simulations in a programmable nanophotonic processor. *Nature Photonics*, 11(7):447, 2017.

[617] Caterina Taballione, Tom A. W. Wolterink, Jasleen Lugani, Andreas Eckstein, Bryn A. Bell, Robert Grootjans, Ilka Visscher, Dimitri Geskus, Chris G. H. Roeloffzen, Jelmer J. Renema, Ian A. Walmsley, Pepijn W. H. Pinkse, and Klaus-J. Boller. 8×8 reconfigurable quantum photonic processor based on silicon nitride waveguides. *Optics Express*, 27:26842–26857, 2019.

[618] Vedran Dunjko and Hans J Briegel. Machine learning & artificial intelligence in the quantum domain: a review of recent progress. *Reports on Progress in Physics*, 81(7):074001, 2018.

[619] Pankaj Mehta, Marin Bukov, Ching-Hao Wang, Alexandre GR Day, Clint Richardson, Charles K Fisher, and David J Schwab. A high-bias, low-variance introduction to machine learning for physicists. *Physics reports*, 810:1–124, 2019.

[620] Giuseppe Carleo, Ignacio Cirac, Kyle Cranmer, Laurent Daudet, Maria Schuld, Naftali Tishby, Leslie Vogt-Maranto, and Lenka Zdeborová. Machine learning and the physical sciences. *Reviews of Modern Physics*, 91(4):045002, 2019.

[621] N. Spagnolo, E. Maiorino, C. Vitelli, M. Bentivegna, A. Crespi, R. Ramponi, P. Mataloni, R. Osellame, and F. Sciarrino. Learning an unknown transformation via a genetic approach. *Scientific Reports*, 7:14316, 2017.

[622] Juan Carrasquilla, Giacomo Torlai, Roger G Melko, and Leandro Aolita. Reconstructing quantum states with generative models. *Nature Machine Intelligence*, 1(3):155, 2019.

[623] Adriano Macarone Palmieri, Egor Kovlakov, Federico Bianchi, Dmitry Yudin, Stanislav Straupe, Jacob D Biamonte, and Sergei Kulik. Experimental neural network enhanced quantum tomography. *npj Quantum Information*, 6(1):1–5, 2020.

[624] Andrea Rocchetto, Scott Aaronson, Simone Severini, Gonzalo Carvacho, Davide Poderini, Iris Agresti, Marco Bentivegna, and Fabio Sciarrino. Experimental learning of quantum states. *Science advances*, 5(3):eaau1946, 2019.

[625] Juan Miguel Arrazola, Thomas R Bromley, Josh Izaac, Casey R Myers, Kamil Brádler, and Nathan Killoran. Machine learning method for state preparation and gate synthesis on photonic quantum computers. *Quantum Science and Technology*, 4(2):024004, 2019.

[626] Taira Giordani, Alessia Suprano, Emanuele Polino, Francesca Acanfora, Luca Innocenti, Alessandro Ferraro, Mauro Paternostro, Nicolò Spagnolo, and Fabio Sciarrino. Machine learning-based classification of vector vortex beams. *Physical Review Letters*, 124(16):160401, 2020.

[627] 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. *Physical Review A*, 102(4):042604, 2020.

[628] Giacomo Torlai, Brian Timar, Evert PL van Nieuwenburg, Harry Levine, Ahmed Omran, Alexander Keesling, Hannes Bernien, Markus Greiner, Vladan Vuletić, Mikhail D Lukin, et al. Integrating neural networks with a quantum simulator for state reconstruction. *Physical review letters*, 123(23):230504, 2019.

[629] Egor S Tiunov, VV Tiunova, Alexander E Ulanov, AI Lvovsky, and AK Fedorov. Experimental quantum homodyne tomography via machine learning. *Optica*, 7(5):448–454, 2020.

[630] Rosanna Nichols, Lana Mineh, Jesús Rubio, Jonathan CF Matthews, and Paul A Knott. Designing quantum experiments with a genetic algorithm. *Quantum Science and Technology*, 4(4):045012, 2019.

[631] Alexey A Melnikov, Hendrik Poulsen Nautrup, Mario Krenn, Vedran Dunjko, Markus Tiersch, Anton Zeilinger, and Hans J Briegel. Active learning machine learns to create new quantum experiments. *Proceedings of the National Academy of Sciences*, 115(6):1221–1226, 2018.

[632] Mario Krenn, Mehul Malik, Robert Fickler, Radek Lapkiewicz, and Anton Zeilinger. Automated search for new quantum experiments. *Physical Review Letters*, 116(9):090405, 2016.

[633] L O'Driscoll, R Nichols, and PA Knott. A hybrid machine learning algorithm for designing quantum experiments. *Quantum Machine Intelligence*, 1(1-2):5–15, 2019.

[634] Krishna Kumar Sabapathy, Haoyu Qi, Josh Izaac, and Christian Weedbrook. Production of photonic universal quantum gates enhanced by machine learning. *Physical Review A*, 100(1):012326, 2019.

[635] Mario Krenn, Manuel Erhard, and Anton Zeilinger. Computer-inspired quantum experiments. *arXiv preprint arXiv:2002.09970*, 2020.

[636] Xiaoqin Gao, Manuel Erhard, Anton Zeilinger, and Mario Krenn. Computer-inspired concept for high-dimensional multipartite quantum gates. *Physical Review Letters*, 125(5):050501, 2020.

[637] Iris Agresti, Niko Viggianiello, Fulvio Flamini, Nicolò Spagnolo, Andrea Crespi, Roberto Osellame, Nathan Wiebe, and Fabio Sciarrino. Pattern recognition techniques for boson sampling validation. *Physical Review X*, 9(1):011013, 2019.

[638] Fulvio Flamini, Nicolò Spagnolo, and Fabio Sciarrino. Visual assessment of multi-photon interference. *Quantum Science and Technology*, 4(2):024008, 2019.

[639] PA Knott. A search algorithm for quantum state engineering and metrology. *New Journal of Physics*, 18(7):073033, 2016.

[640] Valeria Cimini, Marco Barbieri, Nicolas Treps, Mattia Walschaers, and Valentina Parigi. Neural networks for detecting multimode wigner-negativity. *arXiv preprint arXiv:2003.03343*, 2020.

[641] Valentin Gebhart and Martin Bohmann. Neural-network approach for identifying nonclassicality from click-counting data. *Physical Review Research*, 2(2):023150, 2020.

[642] Cristian Bonato, Machiel S Blok, Hossein T Dinani, Dominic W Berry, Matthew L Markham, Daniel J Twitchen, and Ronald Hanson. Optimized quantum sensing with a single electron spin using real-time adaptive measurements. *Nature nanotechnology*, 11(3):247–252, 2016.

[643] Jing Liu and Haidong Yuan. Control-enhanced multiparameter quantum estimation. *Physical Review A*, 96(4):042114, 2017.

[644] Hossein T Dinani, Dominic W Berry, Raul Gonzalez, Jeronimo R Maze, and Cristian Bonato. Bayesian estimation for quantum sensing in the absence of single-shot detection. *Physical Review B*, 99(12):125413, 2019.

[645] Genyue Liu, Mo Chen, Yi-Xiang Liu, David Layden, and Paola Cappellaro. Repetitive readout enhanced by machine learning. *Machine Learning: Science and Technology*, 1(1):015003, 2020.

[646] K Craigie, EM Gauger, Y Altmann, and C Bonato. Resource-efficient adaptive bayesian tracking of magnetic fields with a quantum sensor. *arXiv preprint arXiv:2008.08891*, 2020.

[647] Samuel P Nolan, Augusto Smerzi, and Luca Pezzè. A machine learning approach to bayesian parameter estimation. *arXiv preprint arXiv:2006.02369*, 2020.

[648] Lukas J Fiderer, Jonas Schuff, and Daniel Braun. Neural-network heuristics for adaptive bayesian quantum estimation. *arXiv preprint arXiv:2003.02183*, 2020.

[649] Liane Bernstein, Alexander Sludds, Ryan Hamerly, Vivienne Sze, Joel Emer, and Dirk Englund. Freely scalable and reconfigurable optical hardware for deep learning. *arXiv preprint arXiv:2006.13926*, 2020.

[650] Fulvio Flamini, Arne Hamann, Sofiène Jerbi, Lea M Trenkwalder, Hendrik Poulsen Nautrup, and Hans J Briegel. Photonic architecture for reinforcement learning. *New Journal of Physics*, 22(4):045002, 2020.

[651] Simon Haykin. *Neural Networks and Learning Machines*. Pearson Prentice Hall, 2009.

[652] Charu C. Aggarwal. *Neural Networks and Deep Learning*. Springer, 2018.

[653] Jonathan L Ticknor. A bayesian regularized artificial neural network for stock market forecasting. *Expert Systems with Applications*, 40(14):5501–5506, 2013.

[654] David Enke, Manfred Grauer, and Nijat Mehdiyev. Stock market prediction with multiple regression, fuzzy type-2 clustering and neural networks. *Procedia Computer Science*, 6:201–206, 2011.

[655] N Ganesan, K Venkatesh, MA Rama, and A Malathi Palani. Application of neural networks in diagnosing cancer disease using demographic data. *International Journal of Computer Applications*, 1(26):76–85, 2010.

[656] Diederik P. Kingma and Jimmy Ba. Adam: A method for stochastic optimization. *arXiv:1412.6980*, 2014.

[657] Ian Goodfellow, Yoshua Bengio, and Aaron Courville. *Deep Learning*. The MIT Press, 2016.

[658] Peter M Carlton, Jérôme Boulanger, Charles Kervrann, Jean-Baptiste Sibarita, Jean Salamero, Susannah Gordon-Messer, Debra Bressan, James E Haber, Sebastian Haase, Lin Shao, Lukman Winoto, Atsushi Matsuda, Peter Kner, Satoru Uzawa, Mats Gustafsson, Zvi Kam, David A. Agard, and John W. Sedat. Fast live simultaneous multiwavelength four-dimensional optical microscopy. *Proceedings of the National Academy of Sciences*, 107(37):16016–16022, 2010.

[659] Kai Eckert, Oriol Romero-Isart, Mirta Rodriguez, Maciej Lewenstein, Eugene S Polzik, and Anna Sanpera. Quantum non-demolition detection of strongly correlated systems. *Nature Physics*, 4(1):50–54, 2008.

[660] M Pototschnig, Y Chassagneux, J Hwang, G Zumofen, A Renn, and Vahid Sandoghdar. Controlling the phase of a light beam with a single molecule. *Physical Review Letters*, 107(6):063001, 2011.

[661] Syed Abdullah Aljunid, Meng Khoon Tey, Brenda Chng, Timothy Liew, Gleb Maslennikov, Valerio Scarani, and Christian Kurtsiefer. Phase shift of a weak coherent beam induced by a single atom. *Physical Review Letters*, 103(15):153601, 2009.

[662] YLA Rezus, SG Walt, R Lettow, A Renn, G Zumofen, S Götzinger, and V Sandoghdar. Single-photon spectroscopy of a single molecule. *Physical Review Letters*, 108(9):093601, 2012.

[663] Florian Wolfgramm, Chiara Vitelli, Federica A Beduini, Nicolas Godbout, and Morgan W Mitchell. Entanglement-enhanced probing of a delicate material system. *Nature Photonics*, 7(1):28, 2013.

[664] Jesús Rubio, Paul Knott, and Jacob Dunningham. Non-asymptotic analysis of quantum metrology protocols beyond the cramér–rao bound. *Journal of Physics Communications*, 2(1):015027, 2018.

[665] Marco G Genoni, Stefano Olivares, Davide Brivio, Simone Cialdi, Daniele Cipriani, Alberto Santamato, Stefano Vezzoli, and Matteo GA Paris. Optical interferometry in the presence of large phase diffusion. *Physical Review A*, 85(4):043817, 2012.

[666] Philip JD Crowley, Animesh Datta, Marco Barbieri, and Ian A Walmsley. Tradeoff in simultaneous quantum-limited phase and loss estimation in interferometry. *Phys. Rev. A*, 89(2):023845, 2014.

[667] Francesco Albarelli, Jamie F Friel, and Animesh Datta. Evaluating the holevo cramér-rao bound for multiparameter quantum metrology. *Phys. Rev. Lett.*, 123(20):200503, 2019.

[668] Richard D Gill. Conciliation of bayes and pointwise quantum state estimation. In *Quantum Stochastics and Information: Statistics, Filtering and Control*, pages 239–261. World Scientific, 2008.

[669] Yu-Ran Zhang and Heng Fan. Quantum metrological bounds for vector parameters. *Phys. Rev. A*, 90(4):043818, 2014.

[670] Xiao-Ming Lu and Mankei Tsang. Quantum weiss-weinstein bounds for quantum metrology. *Quantum Sci. Technol.*, 1(1):015002, 2016.

[671] Jesús Rubio and Jacob Dunningham. Bayesian multi-parameter quantum metrology with limited data. *Phys. Rev. A*, 101:032114, 2020.

[672] Xinwei Li, Jia-Hao Cao, Qi Liu, Meng Khoon Tey, and Li You. Multi-parameter estimation with multi-mode ramsey interferometry. *New Journal of Physics*, 22(4):043005, 2020.

[673] Jianwei Wang, Stefano Paesani, Yunhong Ding, Raffaele Santagati, Paul Skrzypczyk, Alexia Salavrakos, Jordi Tura, Remigiusz Augusiak, Laura Mancinska, Davide Bacco, Damien Bonneau, Joshua W. Silverstone, Qihuang Gong, Acin Antonio, Karsten Rottwitt, Leif K. Oxenlowe, Jeremy L. O'Brien, Anthony Laing, and Mark G. Thompson. Multidimensional quantum entanglement with large-scale integrated optics. *Science*, 360:285–291, 2018.

[674] Jianwei Wang, Fabio Sciarrino, Anthony Laing, and Mark G Thompson. Integrated photonic quantum technologies. *Nat. Photonics*, 14:273–284, 2019.

[675] Melanie Mitchell. *An introduction to genetic algorithms*. MIT press, 1998.

[676] Manoj Kumar, Mohamed Husain, Naveen Upreti, and Deepti Gupta. Genetic algorithm: Review and application. *Available at SSRN 3529843*, 2010.

[677] F. H. F. Leung, H. K. Lam, S. H. Ling, and P. K. S. Tam. Tuning of the structure and parameters of a neural network using an improved genetic algorithm. *IEEE Transactions on Neural Networks*, 14(1):79–88, 2003.

[678] David E Goldberg and Kalyanmoy Deb. A comparative analysis of selection schemes used in genetic algorithms. In *Foundations of genetic algorithms*, volume 1, pages 69–93. Elsevier, 1991.

[679] Jesús Rubio and Jacob Dunningham. Bayesian multiparameter quantum metrology with limited data. *Physical Review A*, 101(3):032114, 2020.

[680] Sergei Slussarenko, Morgan M Weston, Helen M Chrzanowski, Lynden K Shalm, Varun B Verma, Sae Woo Nam, and Geoff J Pryde. Unconditional violation of the shot-noise limit in photonic quantum metrology. *Nat. Photonics*, 11(11):700–703, 2017.

[681] Edwin T Jaynes. *Probability theory: The logic of science*. Cambridge university press, 2003.

[682] Jing Liu, Haidong Yuan, Xiao-Ming Lu, and Xiaoguang Wang. Quantum fisher information matrix and multiparameter estimation. *J. Phys. A Math. Theor.*, 53(2):023001, 2020.

[683] Zachary Chaboyer, Thomas Meany, LG Helt, Michael J Withford, and MJ Steel. Tunable quantum interference in a 3d integrated circuit. *Scientific reports*, 5:9601, 2015.

[684] William R Clements, Peter C Humphreys, Benjamin J Metcalf, W Steven Kolthammer, and Ian A Walmsley. Optimal design for universal multiport interferometers. *Optica*, 3(12):1460–1465, 2016.

[685] Jane Liu and Mike West. Combined parameter and state estimation in simulation-based filtering. In *Sequential Monte Carlo methods in practice*, pages 197–223. Springer, 2001.

[686] Samuel L Braunstein. How large a sample is needed for the maximum likelihood estimator to be approximately gaussian? *J. Phys. A: Math. Gen.*, 25(13):3813, 1992.

[687] Andrea Crespi, Mirko Lobino, Jonathan CF Matthews, Alberto Politi, Chris R Neal, Roberta Ramponi, Roberto Osellame, and Jeremy L O'Brien. Measuring protein concentration with entangled photons. *Appl. Phys. Lett.*, 100(23):233704, 2012.

[688] F Martínez-García, D Vodola, and M Müller. Adaptive bayesian phase estimation for quantum error correcting codes. *New J. Phys.*, 21(12):123027, 2019.

[689] Markus Müller, A Rivas, EA Martinez, D Nigg, P Schindler, T Monz, R Blatt, and MA Martin-Delgado. Iterative phase optimization of elementary quantum error correcting codes. *Phys. Rev. X*, 6(3):031030, 2016.

[690] Daniel Nigg, Markus Mueller, Esteban A Martinez, Philipp Schindler, Markus Hennrich, Thomas Monz, Miguel A Martin-Delgado, and Rainer Blatt. Quantum computations on a topologically encoded qubit. *Science*, 345(6194):302–305, 2014.