University of Trento

Department of Physics

# A quantum entropy source based on Single Photon Entanglement

Doctoral Thesis

*for the degree of*

Doctor of Philosophy

*in*

Physics

Nicolò Leone

April 22, 2022

34° PhD Cycle

**Supervisors**
Prof. Lorenzo Pavesi
Prof. Sonia Mazzucchi

**Members of the committee:**
Prof. Stefano Giorgini
Dr. Mario Stipčević
Dr. Paolo Ghiggini

**Colophon**
This document was typeset with the help of KOMA-Script and LaTeX using the kaobook class.
The source code of this book is available at:
`https://github.com/fmarotta/kaobook`

To my extended family

# Acknowledgements

*Nicolò Leone*

# Contents

# List of Figures

# List of Tables

# A quantum entropy source based on Single Photon Entanglement

# Introduction | 1

Quantum mechanics is a fundamental physical theory that describes Nature as something far from the classical idea of determinism that people experience in their everyday life. Indeed, for quantum mechanics, everything has a probabilistic description. It has allowed significant scientific and technological progress. The first quantum revolution has influenced society in many fields: quantum principles like the wave-particle duality and its derived effects, the tunnel and the photoelectric effects, have led to the invention of 20th-century critical devices like the transistor and the laser. These devices are at the basis of the present information society, where data are transmitted and manipulated at unprecedented rates. The ability of humanity to understand Nature thanks to the quantum theory has shaped the entire society. If the first quantum revolution occurred at the beginning of the 20th century, another crucial change is going on: the second quantum revolution. Here, new devices and technologies are developed based on the intrinsic properties of quantum mechanics. Quantum sensing, quantum computing, quantum communication and quantum metrology are emerging fields of application of quantum mechanics that exploit quantum principles. Typical quantum phenomena, like the entanglement or the superposition principle, become tools for improving the performances of existing devices or for building new technologies that can, for example, perform calculations unfeasible with classical computers or enable an unmatched level of privacy in the information exchange. The interest in such quantum technologies is worldwide diffused: different countries are pushing their development and deployment, investing billions of dollars[1–3] .

Among all the quantum technologies, quantum communication is the nearest to producing real devices to the consumer market with Quantum Random Number Generators (QRNGs)[4] . A QRNG is a device that exploits quantum processes to produce random numbers. The latter are fundamental elements in Cryptography, Gamblin and Simulation. In Cryptography, the unconditional unpredictability of a random numbers sequence is a crucial feature to ensure the reliability of cryptographic protocols: their security is based on the inability to predict the random sequence employed to encrypt private information. A sequence of digits, or bits, must be uniformly distributed, uncorrelated and unpredictable to be considered random. Unfortunately, verifying these properties is far from being easy. On the one hand, the first two features can be tested by running suitable statistical tests such as those in the test suite of the National Institute of Standards and Technology (NIST)[5] . Even if this approach is recognized as a methodology to certify Random Number Generators (RNGs)[6] , it is a heuristic approach since no statistical test can comprehensively verify the presence of all the possible correlations inside the sequence. Moreover, such tests analyze samples of the generated raw numbers and, a priori, do not have any control on future generated sequences. On the other hand, the certification of unconditional unpredictability is not possible by running the previously

[1]: Raymer et al. (2019), 'The US national quantum initiative'
[2]: Zhang et al. (2019), 'Quantum information research in China'
[3]: Riedel et al. (2019), 'Europe's quantum flagship initiative'
[4]: Herrero-Collantes et al. (2017), 'Quantum Random Number Generators'

[5]: Zaman et al. (2012), 'Review on fifteen Statistical Tests proposed by NIST'

[6]: Turan et al. (2018), 'Recommendation for the entropy sources used for random bit generation'

introduced statistical tests. A key example is a generator that produces a predeterminate sequence of uncorrelated and uniformly distributed digits. Such a sequence will pass all the statistical tests, but it cannot be considered unpredictable since it is predetermined. A possible solution for RNGs is the calculation of the conditional min-entropy[7] , a property that quantifies the amount of randomness in the generated sequence, taking into account side information accessible to possible eavesdroppers. However, this task is not trivial for many RNGs.

Today RNGs are divided into two main categories: algorithm-based RNGs and physical RNGs. Algorithm-based RNGs or Pseudo-Random Number Generators (PRNGs)[8] are algorithms that start from a limited random or nearly random seed and, by recursive operations, produce random numbers. Even if PRNGs have significant advantages with respect to physical-based RNGs, e.g., disposability and velocity, they cannot be used in cryptographic applications, where unpredictability is mandatory. Algorithm-based RNGs are, indeed, for definition predictable. The generated sequence's security depends upon the initial seed's privacy since the algorithm's structure must be considered public and available to any adversary[9] . For these reasons, physical-based RNGs have been introduced. Physical-based RNGs are RNGs that use physical processes to generate a random output. QRNGs can be considered a sub-category of this class. Another sub-category of Physical RNGs is formed by True Random Number Generators (TRNGs), which are generators that exploit noisy or chaotic processes, such as thermal fluctuations or complex dynamics of objects, to generate a random output. Examples of such physical processes are the thermal noise[10] or the movements of the user pointer on the PC monitor[11] . Being based on processes that can be described by classical physics, TRNGs are not genuinely unpredictable. In fact, in principle, any classical phenomenon, even the most complex one, has a deterministic behavior. Moreover, it is impossible to obtain a robust stochastic model since the quality of the produced numbers is influenced by the physical fluctuations of the system.

These intrinsic problems are not present when considering quantum processes: Einstein himself, talking about quantum mechanics, said its famous quote: "Quantum mechanics is very worthy of respect. But an inner voice tells me that it is not the genuine article after all. The theory delivers much, but does not really bring us any closer to the secret of the Old One. I, at any rate, am convinced that He does not play dice"[12] . Contrary to the thoughts of Einstein, quantum processes are natural candidates to become perfect RNGs: radioactive decay[13] or even single photon's behavior [14] represent excellent sources of entropy indeed. In addition, for QRNGs, the calculation of the conditional min-entropy is easy, even in the presence of eavesdroppers or faulty devices. Remarkably, quantum mechanics also offers the possibility of certifying a priori the amount of entropy present in a sequence. Device Independent Quantum Random Number Generators (DI-QRNGs) can guarantee the presence of randomness even if an eavesdropper can access classical or quantum side information about the physical implementation of the RNG[15] . DI-QRNGs are usually based on entanglement: the randomness comes from the quantum correlations between entangled subsystems. The procedure for the generation of quantum random numbers in DI-QRNGs is usually schematized in four main parts:

[7]: Konig et al. (2009), 'The operational meaning of min-and max-entropy'

[8]: James et al. (2020), 'Review of high-quality random number generators'

[9]: Kerckhoffs (1883), 'La cryptographic militaire'

[10]: Zhun et al. (2001), 'A truly random number generator based on thermal noise'

[11]: Hu et al. (2009), 'A true random number generator based on mouse movement and chaotic cryptography'

[12]: Einstein (2018), *The Collected Papers of Albert Einstein, Volume 15 (Translation Supplement): The Berlin Years: Writings & Correspondence, June 1925–May 1927*

[13]: Manelis (1961), 'Generating random noise with radioactive sources'

[14]: Rarity et al. (1994), 'Quantum random-number generation and key sharing'

[15]: Acín et al. (2016), 'Certified randomness in quantum physics'

1) the entangled state is generated,
2) it is measured on a particular basis chosen between four sets,
3) the Bell correlation function[16] is evaluated,
4) randomness extraction procedure is performed.

[16]: Clauser et al. (1969), 'Proposed experiment to test local hidden-variable theories'

The critical aspect of the protocol is the evaluation of the Bell correlation function: only if the Bell's Inequality (BI) is violated a certain amount of randomness can be certified by the sequence[17] . On the contrary, if the BI is not violated, the sequence of random numbers can be described using classical theory, i.e., it is no longer unpredictable. In this application, the BI is used to witness the presence of intrinsic quantum randomness, providing a quantification of the value of conditional min-entropy attainable. Usually, based on traditional Multi Particles Entanglement (MPE), these DI-QRNGs are, unfortunately, technologically challenging, where non-local coincidence measurements have to be performed employing complicated experimental setups, strongly limiting the applicability of such DI-QRNG to research applications. To relax the technological hurdle, in the last years, a new category of QRNGs, which are more consumer market-oriented, is emerged: these are called Semi-Device Independent Quantum Random Number Generators (SDI-QRNGs). SDI-QRNGs represent a tradeoff between security and feasibility: the entropy certification is still based on fundamental principles of quantum mechanics, but, in addition, a partial knowledge of the device is assumed. This could be the knowledge of the source of the quantum states[18] or the characterization of the measurement operations[19] , or even more complicated assumptions, like energetic bounds[20] . Even a DI-QRNG, where a fixed number of hypotheses are introduced, can be considered a SDI-QRNG[21] .

[17]: Pironio et al. (2010), 'Random Numbers Certified by Bell's Theorem'

[18]: Brask et al. (2017), 'Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination'

[19]: Avesani et al. (2018), 'Source-device-independent heterodyne-based quantum random number generator at 17 Gbps'

[20]: Van Himbeeck et al. (2019), 'Correlations and randomness generation based on energy constraints'

[21]: Mazzucchi et al. (2021), 'Entropy certification of a realistic quantum random-number generator based on single-particle entanglement'

My entire PhD work was devoted to studying Single Photon Entanglement (SPE). As the name suggests, this entanglement does not involve two distinct photons, but it concerns different Degrees of Freedom (DoFs) of a single photon. I am aware that in literature, the term "Single Photon Entanglement" is sometimes associated with the entanglement of a single photon and the vacuum state[22] produced using a beam splitter. Even if these two typologies of entanglement seem similar since only one photon is involved, they have fundamental differences concerning the properties of such states. The DoFs-entanglement has a local and contextual phenomenology, while the one of vacuum-entanglement is non-local and non-contextual. Moreover, the information carriers are different. In the DoFs-entanglement, they are the DoFs, while they are the numbers of particles in the modes for the vacuum-entanglement. At the beginning of my PhD studies, the challenges that I faced these questions:

[22]: Van Enk (2005), 'Single-particle entanglement'

1) "Can Single Photon Entanglement be produced by attenuated sources?",
2) "Can Single Photon Entanglement be integrated into a photonic chip?".

The motivations behind these two questions are purely practical. Concerning the entanglement between two photons, or Multi Particles Entanglement (MPE), writing a SPE state on a single photon requires only linear optical components. However, the generation of a single photon relies on non-linear optical processes, totally spoiling the convenience of the SPE concerning MPE. On the contrary, if entanglement can be produced using attenuated light sources, like the Light-emitting diode (LED), SPE becomes a more convenient resource for applications concerning MPE. This fact could be pushed even forward if SPE can be generated using an integrated approach, resulting in a further reduction of the footprint and the cost. My PhD journey started answering the first question. After some months of work, I was able to answer positively to the first question: indeed, I demonstrated that such an entanglement could be generated using single photons from attenuated light sources (laser, LED and a halogen lamp) using, as DoFs, momentum (direction of propagation) and polarization[23] . A BI violation experiment[24] was performed to verify the presence of the entanglement. Since the BI is a well-known entanglement witness, the entanglement presence is necessary for observing a violation of the inequality. Then, I started to think about how to use the SPE for quantum information tasks: having an apparatus able to witness the violation of the BI, the application of the SPE to QRNG has been proposed.

[23]: Pasini et al. (2020), 'Bell-inequality violation by entangled single-photon states generated from a laser, an LED, or a halogen lamp'

[24]: Bell (1964), 'On the Einstein Podolsky Rosen paradox'

In this way, I focused on implementing a certification protocol based on SPE that can certify the conditional min-entropy of the generated sequence of random numbers using a DI-like approach[21, 25] . Unlike MPE-based DI-QRNG, the randomness of the SPE-QRNG comes from the contextual correlations of the entanglement between the two DoFs. The resulting QRNG is a SDI-QRNG since the certification of the randomness is based on a partial characterization of the experimental setup.

[21]: Mazzucchi et al. (2021), 'Entropy certification of a realistic quantum random-number generator based on single-particle entanglement'

[25]: Leone et al. (2022), 'Certified Quantum Random-Number Generator Based on Single-Photon Entanglement'

The last objective of my PhD work concerned the answer to the second question: the integration of the SPE in a photonic chip in the silicon oxynitride platform. Since the integrated control of polarisation is unfeasible in standard integrated design, the SPE state was generated between waveguides where the photon is propagating. Preliminary validation of this type of entanglement was achieved by performing another BI violation experiment. The initial results confirm that it is possible to generate such entanglement in the designed photonic chip, but further work must be done to validate the method effectively. Future perspectives concerning the integrated version of SPE are connected to the generation of certified quantum random numbers in analogy to what was done for the SPE-SDI-QRNG. Due to the compactness, the cheapness and the low power consumption of such an integrated scheme, the successful implementation of the SDI-QRNG can be considered a further step into the deployment of real certified QRNGs to high volume market.

The thesis is organized as follows: in Chapter 2, the quantum phenomenon of the entanglement is firstly introduced, focusing on the concepts of separability and correlation between qubits. Then, the BI is discussed together with the Einstein, Podolsky and Rosen (EPR) paradox. After this, the SPE of momentum and polarization is presented by introducing the experimental setup used to generate and validate such an entanglement. The validation is obtained by probing the BI violation in the Clauser, Horne, Shimony and Holt (CHSH) form. Discussed the ideal situation, all the non-idealities in the experimental implementation are presented and analyzed, proposing a solution to each of them. Even if these non-idealities were observed chronologically after the experimental test of the BI during the study of the SDI-QRNG since they also interest the estimation of the BI, they are presented in this chapter. Lastly, an experiment is presented to confirm the theory and the results are discussed. Here, my contribution was to implement the numerical approach to the polarization non-idealities and perform experimental measurements. The discussion of the non-idealities was developed in collaboration with Prof. Sonia Mazzucchi and Prof. Valter Moretti. In Chapter 3, QRNGs are firstly introduced. Then, by discussing the concept of entropy, the main figure of merit for a QRNG, the min-entropy, is presented, focusing on its operational meaning. After that, the concept of conditional min-entropy certification is analyzed by discussing DI-QRNGs and SDI-QRNGs. An example of conditional min-entropy estimation in an SDI-QRNG is also provided. Then, particular attention is paid to the estimation of the conditional min-entropy by exploiting BI violation. The latter part is used to present theoretically and experimentally the scheme of the SDI-QRNG based on SPE states of momentum and polarization. Here my contribution was to apply the SDI protocol of [18] to a fully integrated optical chip and fully develop the experiment to validate the SDI-QRNG based on SPE. Chapter 4 discusses the integrated implementation of SPE using absolute and relative positions of photons into a set of waveguides. Firstly, some essential photonics devices are presented and their functionalities underlined. Then, the implementation of the SPE on-chip is proposed by introducing the necessary pieces to generate the entanglement and to perform the BI test. The simulation of each optical component is reported. The produced photonic chip is then experimentally characterized. An experiment is carried out to validate the presence of the entanglement using the BI. The preliminary results are discussed. Here, my contribution was to conceive the experiment, design the integrated chip structure, and perform the measurements. Lastly, in Chapter 5, a summary of the entire thesis is reported together with future perspectives.

[18]: Brask et al. (2017), 'Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination'

# Single-Photon Entanglement 2

In this chapter, the concepts of entanglement, Single Particle Entanglement (SPaE) and Bell's Inequality (BI) are firstly introduced from a fundamental point of view. After that, the specific implementation based on single photons, the Single Photon Entanglement (SPE), is presented, focusing on the implementation based on momentum and polarization. The corresponding BI is also discussed with the help of an experimental setup necessary to test it. Possible non-idealities in the components of the setup and their effect on the BI are also considered. Lastly, to justify the reported theory, a series of experiments towards the violation of BI using SPE states are presented and discussed.

## 2.1 Entanglement and separability

In order to introduce the concept of entanglement, it is useful to describe the concept of separability of a quantum state. In quantum mechanics, only two categories of quantum states exist: separable and not-separable ones. For illustrating this concept, two finite dimensional Hilbert spaces $\mathscr{H}_a$ and $\mathscr{H}_b$ are introduced. A pure state $|\psi\rangle$ in $\mathscr{H}_a \otimes \mathscr{H}_b$ can be described as a linear combination:

$$|\psi\rangle = \sum_{i}^{n} c_i |\psi_a\rangle_i \otimes |\psi_b\rangle_i, \quad \sum_{i}^{n} |c_i|^2 = 1 \tag{2.1}$$

where $\{c_i\}_i \in \mathbb{C}$ are appropriate constants and $\{|\psi_a\rangle_i\}$ and $\{|\psi_b\rangle_i\}$ two orthonormal basis of $\mathscr{H}_a$ and $\mathscr{H}_b$. Note that the discussion can be easily generalized in the case of mixed states and/or considering more Hilbert spaces. This is called the Schmidt decomposition[26] of the state $|\psi\rangle$. The basis $\{|\psi_a\rangle_i\}$ and $\{|\psi_b\rangle_i\}$ are called Schmidt basis and the number of non-zero coefficients $\{c_i\}_i$ is called the Schmidt number or Schmidt rank. The latter is particularly useful since it is used to distinguish between separable and non-separable states: $|\psi\rangle$ is called separable if only one coefficient $c_i$ is different from zero, i.e., its Schmidt rank is equal to 1. On the contrary, if its Schmidt rank is greater than 1, the state $|\psi\rangle$ is called not separable or entangled. It is easy to understand now that the concept of entanglement is strictly connected to the inability of describing the behavior of the state $|\psi\rangle$ as composed of two independent states belonging to the subspaces $\mathscr{H}_a$ and $\mathscr{H}_b$. One of the funding-fathers of the quantum theory, Erwin Schrödinger, tried to explain the properties of quantum mechanics by formulating his famous mental experiment: the Schrödinger's cat[27] . A cat is put in a closed box with a jar of poison and an excited atom. When the excited atom relaxes, a hammer breaks the jar of poison, leading to the cat's death. Besides the cruelty of the experiment, it explains the concept of entanglement in a pretty intuitive way. Indeed, after having prepared the setup and waiting some time, the state of the cat ($|L\rangle$, alive, or $|D\rangle$, dead) results to be entangled, or correlated,

[26]: Nielsen et al. (2002), *Quantum computation and quantum information*

[27]: Schrödinger (1935), 'Die gegenwärtige Situation in der Quantenmechanik'

with the state of the atom ($|E\rangle$, excited or $|G\rangle$, ground). In this way, the cat's state is directly connected to the atom's state and it is impossible to describe one without considering the other. The entanglement, indeed, is a purely quantum phenomenon in which non-classical correlations between the considered subsystems are present.

These correlations are extremely counterintuitive from a classical point of view. Indeed, a property of the entanglement is the non-locality. As an example, consider two particles, labeled as $a$ and $b$, which have been entangled in the z-component of their spin. Assume that their wavefunction can be written as:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|z_+\rangle_a|z_-\rangle_b - |z_-\rangle_a|z_+\rangle_b\right) \tag{2.2}$$

where $|z_+\rangle$ means a positive z-component of the spin, while $|z_-\rangle$ indicates a negative z-component, or equivalently, $\sigma_z|z_+\rangle = +1|z_+\rangle$ and $\sigma_z|z_-\rangle = -1|z_-\rangle$, where $\sigma_z$ is the operator corresponding to the z-Pauli Matrix. Suppose to spatially separate the two particles to avoid possible communication between them. Consider performing a local spin z-direction measurement on the $a$ particle and obtaining the result $|z_+\rangle$. Due to the collapse of the wavefunction, not only the measurement operation has determined the spin of the particle $a$ but it has also fixed the spin of the particle $b$ in the other laboratory, thus it will result to be $|z_-\rangle$. In a non-local manner, the result of the measurement of $\sigma_z$ on the particle $b$ has been influenced by the local operation performed on the particle $a$, thanks to the entanglement. At first glance, this seems to be quite counterintuitive. Einstein himself was skeptical about quantum theory and entanglement. In fact, in 1935, Boris Podolsky, Nathan Rosen and he published their famous work entitled" Can Quantum-Mechanical Description of Physical Reality be Considered Complete?"[28] . In the latter, the three scientists tried to demonstrate the not-completeness of the quantum mechanical theory formulating the famous Einstein, Podolsky and Rosen (EPR) paradox.

[28]: Einstein et al. (1935), 'Can quantum-mechanical description of physical reality be considered complete?'

## 2.2 EPR Paradox and Bell's inequality

For Einstein, Podolsky and Rosen a physical theory must possess two properties:

- Realism: if it is possible to know with unitary probability the value of a physical quantity without disturbing the system, then it exists an element of realism corresponding to that quantity,
- Locality: different elements of reality cannot interact instantaneously at a distance.

Now, consider the state in Equation 2.2. The measurement of the spin of particle $a$ has influenced the outcome of the measurement of the spin of the particle $b$, which is now predictable with unitary probability. Due to the hypotheses of realism and locality, the value of the spin component of the particle $b$ should have been fixed before the measurement performed on the particle $a$, which is not true for the quantum mechanics description. To demonstrate the latter, the reduced density matrix for the subsystem

$b$,

$$\rho_b = \mathrm{Tr_a}\,\rho = \mathrm{Tr_a}\,|\psi\rangle\langle\psi|, \tag{2.3}$$

has to be introduced since it describes the particle $b$ independently of the particle $a$. It is easy to prove that the reduced density matrix for an entangled state like Equation 2.2, corresponds to the density matrix of a totally mixed state:

$$\rho_b = \frac{1}{2}I_2, \tag{2.4}$$

where $I_2$ is the 2×2 identity matrix. For this density matrix, it is impossible to choose an orthonormal basis in $\mathscr{H}_b$ for which $|\psi_b\rangle$ ($\rho_b = |\psi_b\rangle\langle\psi_b|$) is an autovector or, equivalently, it is impossible to predict, with unitary probability, the outcome of the measurement operation. For these reasons, Einstein et al. concluded that quantum mechanics must be incomplete since it cannot predict that value. In addition, they postulated the existence of some hidden (inaccessible) variables $\lambda \in \Lambda$, where $\Lambda$ is a set of parameters, which can deterministically describe the system in the Einstein view.

Just after 1964, the concept of entanglement became more widely used. In that year, John Bell proposed a test to discriminate between the quantum theory and any local hidden variable theory[24] . To understand the result obtained by Bell, here it is reported the Bell's analysis of the EPR paradox proposed by Aharonov and Bohm[29] . Consider a system composed of two entangled particles in spin. Assume that the state that describes the situation is the one reported in Equation 2.2. Suppose to perform spin measurements on the two particles which can have as result only $\{\pm 1\}$. In particular, the outcome $f^c_{\mathbf{n}_c}(\lambda)$ is called the result of the measurement performed on the particle $c \in \{a, b\}$ in the $\mathbf{n}_c \in \{\mathbf{n}_a, \mathbf{n}_b\}$ direction. The operator that performs this operation is:

[24]: Bell (1964), 'On the Einstein Podolsky Rosen paradox'

[29]: Bohm et al. (1957), 'Discussion of Experimental Proof for the Paradox of Einstein, Rosen, and Podolsky'

$$\mathbf{n}_c \cdot \sigma = n_{c_x}\sigma_x + n_{c_y}\sigma_y + n_{c_z}\sigma_z, \quad \mathbf{n}_c \in \mathbb{R}^3, ||\mathbf{n}_c|| = 1. \tag{2.5}$$

Even if $f$ is directly dependent on the hidden variable $\lambda$, the exact value of $\lambda$ is unknown: it is only possible to assume the knowledge of the probability distribution $\mu$ of $\lambda$. It is necessary to define also the quantities $f^a_{\mathbf{n}_a,\mathbf{n}_b}(\lambda)$ and $f^b_{\mathbf{n}_b,\mathbf{n}_a}(\lambda)$, which represent the value of the spin components of the two particles given the measurement performed on the other particle. Introduced this notation, the hypothesis of realism implies that $f^a_{\mathbf{n}_a,\mathbf{n}_b}(\lambda)$ and $f^b_{\mathbf{n}_b,\mathbf{n}_a}(\lambda)$ are defined for every time and for every choice of $\mathbf{n}_a$ and $\mathbf{n}_b$. On the other hand, the hypothesis of locality can be considered by imposing the independence of $f^a_{\mathbf{n}_a,\mathbf{n}_b}(\lambda)$ and $f^b_{\mathbf{n}_b,\mathbf{n}_a}(\lambda)$ from every choice of the direction of measurement on the other particle, i.e., $f^a_{\mathbf{n}_a,\mathbf{n}_b}(\lambda) = f^a_{\mathbf{n}_a}(\lambda)$ and $f^b_{\mathbf{n}_b,\mathbf{n}_a}(\lambda) = f^b_{\mathbf{n}_b}(\lambda)$. By taking two unitary vectors $\mathbf{n}_a$ and $\mathbf{n}_{a'}$, both belonging to $\mathbb{R}^3$, along which the spin for the particle $a$ is measured and two others unitary vectors $\mathbf{n}_b$ and $\mathbf{n}_{b'}$ belonging to $\mathbb{R}^3$, along which the spin for the particle $b$ is measured, it is possible to define the correlation coefficient $\mathbb{E}(f^a_{\mathbf{n}_a}, f^b_{\mathbf{n}_b})$ used to measure the correlation between the results of the spin measurement on the two particles respectively in the direction $\mathbf{n}_a$ and $\mathbf{n}_b$. Mathematically, $\mathbb{E}(f^a_{\mathbf{n}_a}, f^b_{\mathbf{n}_b})$ can be written as:

$$\mathbb{E}\left(f^a_{\mathbf{n}_a}, f^b_{\mathbf{n}_b}\right) = \int_\Lambda f^a_{\mathbf{n}_a}(\lambda) f^b_{\mathbf{n}_b}(\lambda)\mathrm{d}\mu(\lambda). \tag{2.6}$$

Bell demonstrated that if the correlation function $\chi(\mathbf{n}_a, \mathbf{n}_{a'}, \mathbf{n}_b, \mathbf{n}_{b'})$, or

$\chi$-parameter, is constructed as:

$$\begin{aligned}&\chi(\mathbf{n}_a, \mathbf{n}_{a'}, \mathbf{n}_b, \mathbf{n}_{b'}) :=\\ &\mathbb{E}\left(f^a_{\mathbf{n}_a}, f^b_{\mathbf{n}_b}\right) - \mathbb{E}\left(f^a_{\mathbf{n}_a}, f^b_{\mathbf{n}_{b'}}\right) + \mathbb{E}\left(f^a_{\mathbf{n}_{a'}}, f^b_{\mathbf{n}_b}\right) + \mathbb{E}\left(f^a_{\mathbf{n}_{a'}}, f^b_{\mathbf{n}_{b'}}\right)'\end{aligned} \tag{2.7}$$

its absolute value must be upper bounded by 2 for any local hidden variable theory:

$$|\chi(\mathbf{n}_a, \mathbf{n}_{a'}, \mathbf{n}_b, \mathbf{n}_{b'})| < 2. \tag{2.8}$$

This is called the Bell's Inequality (BI). In order to prove Equation 2.8, it is necessary to insert Equation 2.6 into Equation 2.7.

$$\begin{aligned}\chi(\mathbf{n}_a, \mathbf{n}_{a'}, \mathbf{n}_b, \mathbf{n}_{b'}) &=\\ &= \mathbb{E}\left(f^a_{\mathbf{n}_a}, f^b_{\mathbf{n}_b}\right) - \mathbb{E}\left(f^a_{\mathbf{n}_a}, f^b_{\mathbf{n}_{b'}}\right) + \mathbb{E}\left(f^a_{\mathbf{n}_{a'}}, f^b_{\mathbf{n}_b}\right) + \mathbb{E}\left(f^a_{\mathbf{n}_{a'}}, f^b_{\mathbf{n}_{b'}}\right)\\ &= \int_\Lambda f^a_{\mathbf{n}_a}(\lambda) f^b_{\mathbf{n}_b}(\lambda) \mathrm{d}\mu(\lambda) - \int_\Lambda f^a_{\mathbf{n}_a}(\lambda) f^b_{\mathbf{n}_{b'}}(\lambda) \mathrm{d}\mu(\lambda) +\\ &+ \int_\Lambda f^a_{\mathbf{n}_{a'}}(\lambda) f^b_{\mathbf{n}_b}(\lambda) \mathrm{d}\mu(\lambda) + \int_\Lambda f^a_{\mathbf{n}_{a'}}(\lambda) f^b_{\mathbf{n}_{b'}}(\lambda) \mathrm{d}\mu(\lambda)\\ &= \int_\Lambda \Big( f^a_{\mathbf{n}_a}(\lambda) f^b_{\mathbf{n}_b}(\lambda) - f^a_{\mathbf{n}_a}(\lambda) f^b_{\mathbf{n}_{b'}}(\lambda) +\\ &+ f^a_{\mathbf{n}_{a'}}(\lambda) f^b_{\mathbf{n}_b}(\lambda) + f^a_{\mathbf{n}_{a'}}(\lambda) f^b_{\mathbf{n}_{b'}}(\lambda) \Big) \mathrm{d}\mu(\lambda)\\ &= \int_\Lambda \Big( f^a_{\mathbf{n}_a}(\lambda) \left( f^b_{\mathbf{n}_b}(\lambda) - f^b_{\mathbf{n}_{b'}}(\lambda) \right) +\\ &+ f^a_{\mathbf{n}_{a'}}(\lambda) \left( f^b_{\mathbf{n}_b}(\lambda) + f^b_{\mathbf{n}_{b'}}(\lambda) \right) \Big) \mathrm{d}\mu(\lambda)\end{aligned} \tag{2.9}$$

For every choice of $\lambda$, only one term survives inside the integral $\left(f^c_{\mathbf{n}_c}(\lambda) \in \{\pm 1\}\right)$. From this, it is possible to conclude that

$$-2 < \chi(\mathbf{n}_a, \mathbf{n}_{a'}, \mathbf{n}_b, \mathbf{n}_{b'}) < 2 \rightleftharpoons |\chi(\mathbf{n}_a, \mathbf{n}_{a'}, \mathbf{n}_b, \mathbf{n}_{b'})| < 2. \tag{2.10}$$

Bell demonstrated that for quantum mechanics, not only the function $\chi(\mathbf{n}_a, \mathbf{n}_{a'}, \mathbf{n}_b, \mathbf{n}_{b'})$ reaches values greater than 2, but also that the maximum attainable value is $2\sqrt{2}$. In the framework of quantum mechanics[1]

$$\mathbb{E}\left(O^a_{\mathbf{n}_a}, O^b_{\mathbf{n}_b}\right) = \mathrm{Tr}\left[\rho\left(\mathbf{n}_a \cdot \sigma \otimes \mathbf{n}_b \cdot \sigma\right)\right] \tag{2.11}$$

Given $\rho = |\psi\rangle\langle\psi|$, with $|\psi\rangle$ of the form of Equation 2.2, $\forall \mathbf{n}_a, \mathbf{n}_b \in \mathbb{R}^3$, $|\mathbf{n}_a| = |\mathbf{n}_b| = 1$, $\mathbb{E}\left(O^a_{\mathbf{n}_a}, O^b_{\mathbf{n}_b}\right) = -\mathbf{n}_a \cdot \mathbf{n}_b$.

By choosing as measurement directions, the ones reported in Figure 2.1, which correspond to the conditions:

$$\mathbf{n}_a \cdot \mathbf{n}_b = \mathbf{n}_{a'} \cdot \mathbf{n}_b = \mathbf{n}_{a'} \cdot \mathbf{n}_{b'} = \cos\left(\frac{\pi}{4}\right), \tag{2.12}$$

$$\mathbf{n}_a \cdot \mathbf{n}_{b'} = \cos\left(\frac{3\pi}{4}\right), \tag{2.13}$$

[1] The notation $\mathbb{E}\left(f^a_{\mathbf{n}_a}, f^b_{\mathbf{n}_b}\right)$ is changed to $\mathbb{E}\left(O^a_{\mathbf{n}_a}, O^b_{\mathbf{n}_b}\right)$ to distinguish between the two cases: $O^c_{\mathbf{n}_d}$ indicates the operator measured on the particle c in the direction $\mathbf{n}_d$.

it can be obtained that:

$$
\begin{aligned}
&\chi_{\mathrm{MQ}}(\mathbf{n}_a, \mathbf{n}_{a'}, \mathbf{n}_b, \mathbf{n}_{b'}) = \\
&\qquad = \mathbb{E}\left(O^a_{\mathbf{n}_a}, O^b_{\mathbf{n}_b}\right) - \mathbb{E}\left(O^a_{\mathbf{n}_a}, O^b_{\mathbf{n}_{b'}}\right) + \mathbb{E}\left(O^a_{\mathbf{n}_{a'}}, O^b_{\mathbf{n}_b}\right) + \mathbb{E}\left(O^a_{\mathbf{n}_{a'}}, O^b_{\mathbf{n}_{b'}}\right) \\
&\qquad = -\mathbf{n}_a \cdot \mathbf{n}_b + \mathbf{n}_a \cdot \mathbf{n}_{b'} - \mathbf{n}_{a'} \cdot \mathbf{n}_b - \mathbf{n}_{a'} \cdot \mathbf{n}_{b'} \\
&\qquad = -3\cos\left(\frac{\pi}{4}\right) + \cos\left(\frac{3\pi}{4}\right) \\
&\qquad = -4\cos\left(\frac{\pi}{4}\right) = -2\sqrt{2} < -2.
\end{aligned}
\tag{2.14}
$$

Consider now the general case of a composed Hilbert space $\mathcal{H} = \mathcal{H}_a \otimes \mathcal{H}_b = \mathbb{C}^2 \otimes \mathbb{C}^2$. It can be proven that the value $2\sqrt{2}$ could be achieved by properly measuring any one of the maximally entangled states. The latter are called the Bell basis and can be written as:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{2.15}$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \tag{2.16}$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \tag{2.17}$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \tag{2.18}$$

where the notation $|xy\rangle = |x\rangle \otimes |y\rangle$ is introduced. $|0\rangle$ and $|1\rangle$ are just two basis vectors in $\mathbb{C}^2$. It is important to remark a few observations about the BI:

- a necessary condition to violate the BI is the presence of the entanglement;
- a pure entangled state always violates a BI;
- the maximum attainable value of the BI for the quantum mechanics is $2\sqrt{2}$;
- a separable state cannot violate the BI[2] ;
- a mixed entangled state could violate a BI (the Werner states[31] are entangled states which do not necessarily violate the BI).

Returning to the physical implications of the BI, since the quantum

[2] Actually, a separable state cannot violate any BI[30].

[31]: Werner (1989), 'Quantum states with Einstein - Podolsky - Rosen correlations admitting a hidden-variable model'

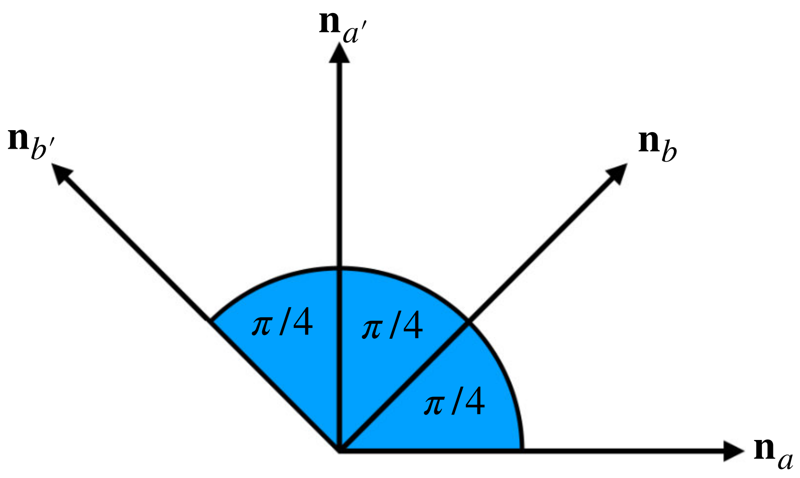


**Figure 2.1:** Geometrical representation of four possible directions of spin measurement that violates BI when performed on the state Equation 2.2.

mechanics leads to a value greater than 2, it is possible to conclude that the quantum mechanics theory is not a local realist theory in the Einstein sense. Today, it is well known that the quantum mechanics phenomenology is non-local, where the non-locality of the entanglement is at the base of many quantum technologies.

## 2.3 Single Photon Entanglement

Up to now, it has been considered only situations in which the entangled subspaces are two particles. Specifically, it is possible to call this type of entanglement as Inter-Particle Entanglement or Multi Particles Entanglement (MPE). Another type of entanglement is the Intra-Particle Entanglement or Single Particle Entanglement (SPaE). As the name suggests, in SPaE only one particle is involved: the two subspaces used are associated to two Degrees of Freedom (DoFs) of the particle. In the literature it is possible to find different examples of this peculiar type of entanglement, involving atoms, photons and neutrons[32–41] . An example of a SPaE state is:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0V\rangle + |1H\rangle\right) \tag{2.19}$$

where $|x\rangle, x = V, H$, refers to the vertical and horizontal polarization of a single photon and $|y\rangle, y = 0, 1$, refers to its direction of propagation in the space. Note that the directions of propagation $|0\rangle$ and $|1\rangle$, must be chosen to have a null overlap, $\langle 0|1\rangle = 0$. The composed Hilbert space is $\mathcal{H} = \mathcal{H}_M \otimes \mathcal{H}_P$, where $M$ stands for momentum and $M$ for polarization. In the state of Equation 2.19 the polarization of the photon cannot be described without considering its direction of propagation. Since its Schmidt rank is 2, the state is entangled. At this point, it could be helpful to introduce the concept of the qubit: in a $\mathbb{C}^2$ system, the qubit is defined as the quantum representation of the information that can be stored in the state. In the case of Equation 2.2, the two qubits are represented by the two particles and the information is codified into their z-spin components. In contrast, in the case of Equation 2.19, the two qubits are the two DoFs. This description is particularly useful since it allows to perform calculations without directly addressing the specific physical implementation behind the encoding of qubits. The two vectors, that compose the two bases for the two qubits, are:

$$|V\rangle = \begin{pmatrix}1\\0\end{pmatrix}, |H\rangle = \begin{pmatrix}0\\1\end{pmatrix}, |0\rangle = \begin{pmatrix}1\\0\end{pmatrix}, |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}, \tag{2.20}$$

for Equation 2.19 and

$$|z_+\rangle_a = \begin{pmatrix}1\\0\end{pmatrix}, |z_-\rangle_a = \begin{pmatrix}0\\1\end{pmatrix}, |z_+\rangle_b = \begin{pmatrix}1\\0\end{pmatrix}, |z_-\rangle_b = \begin{pmatrix}0\\1\end{pmatrix}. \tag{2.21}$$

[32]: Monroe et al. (1996), 'A "Schrödinger Cat" Superposition State of an Atom'
[33]: Michler et al. (2000), 'Experiments towards Falsification of Noncontextual Hidden Variable Theories'
[34]: Gadway et al. (2009), 'Bell-inequality violations with single photons entangled in momentum and polarization'
[35]: Karimi et al. (2010), 'Spin-orbit hybrid entanglement of photons and quantum contextuality'
[36]: Chen et al. (2010), 'Single-photon spin-orbit entanglement violating a Bell-like inequality'
[37]: Basu et al. (2001), 'Bell's inequality for a single spin-1/2 particle and quantum contextuality'
[38]: Hasegawa et al. (2003), 'Violation of a Bell-like inequality in single-neutron interferometry'
[39]: Sponar et al. (2010), 'Violation of a Bell-like inequality for spin-energy entanglement in neutron polarimetry'
[40]: Geppert et al. (2014), 'Improvement of the polarized neutron interferometer setup demonstrating violation of a Bell-like inequality'
[41]: Shen et al. (2020), 'Unveiling contextual realities by microscopically entangling a neutron'

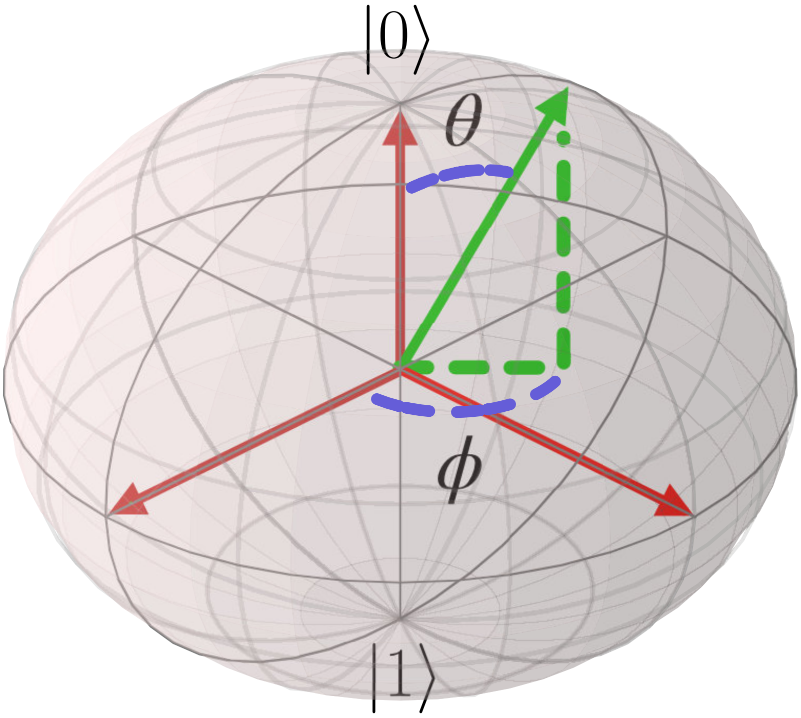


**Figure 2.2:** Example of a Bloch sphere representation. The two orthonormal basis vectors of the qubit are represented at the poles of the sphere. Two angles $\phi$ and $\theta$ can be used for representing each pure state of the sphere, as reported in Equation 2.23.

for Equation 2.2. Consequently, the entangled states of Equation 2.2 and Equation 2.19 can be written in the same way as:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0V\rangle + |1H\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}. \tag{2.22}$$

The Bloch sphere is also introduced for completeness: it provides a geometrical representation of all the possible pure states achievable using a qubit. A generic pure state on the Bloch sphere can be represented by a linear combination of the orthonormal basis vectors $|0\rangle$ and $|1\rangle$ as:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle, \tag{2.23}$$

where the angles $\theta$ and $\phi$ are represented in Figure 2.2.

Even if the mathematical structure of the SPaE is totally analogues to the MPE, a fundamental difference is that SPaE is a local phenomenon, while the MPE is non-local. In Section 2.2, the locality argument is a fundamental piece to derivate the BI, which now have to be generalized also for SPaE states. For this scope, it is necessary to introduce another property called contextuality. Consider the state of Equation 2.19: the two subsystems $\mathcal{H}_P$ and $\mathcal{H}_M$ are independent but not spatially separated and mathematically analogous to $\mathbb{C}^2$. It is important to remark that considering the polarization as a qubit is well justified since vertical and horizontal polarizations are well-defined and orthogonal. The same cannot be done for $\mathcal{H}_M$, since infinite possible momenta are available. In this case, a further assumption must be introduced on $\mathcal{H}_M$ where it is necessary to restrict the available wavevectors only to the ones corresponding to the states $|0\rangle$ and $|1\rangle$. Within this approximation, the structure of $\mathscr{H}_M$ is analogous to $\mathbb{C}^2$. By considering a non-contextual hidden variable theory, these two properties must hold[3] :

- Realism: it exists a pre-defined result for every observable measurable;
- Non-contextuality: the result of a measurement operation $\mathbf{n}_a \cdot \sigma$ must be independent of the choice of two incompatible observables $\mathbf{n}_b \cdot \sigma$ and $\mathbf{n}_{b'} \cdot \sigma$ which can be measured simultaneously with $\mathbf{n}_a \cdot \sigma$.

The reasoning done before to prove the BI with non-locality can be reused now to prove the BI in its more general non-contextual version. The only difference regards the motivations behind the equalities $f^a_{\mathbf{n}_a,\mathbf{n}_b}(\lambda) = f^a_{\mathbf{n}_a}(\lambda)$ and $f^b_{\mathbf{n}_b,\mathbf{n}_a}(\lambda) = f^b_{\mathbf{n}_b}(\lambda)$, which are now justified using non-contextuality. In the case of SPaE, the BI can be used to rule out non-contextual hidden variable theories, which are more general than local hidden variable theories. Indeed, in local hidden variable theory, non-contextuality is implicitly assumed by introducing the space-like separation between the two considered particles. Such a physical motivation is not necessary for non-contextual hidden variable theories, where the independence of the values of the measurement operations from the choice of the other observables that have to be measured is assumed.

## 2.4 Single Photon Entanglement: experimental implementation

In the previous section, it was demonstrated that the BI can be used to rule out possible non-contextual hidden variable theories that try to explain the correlations between the outcomes of two groups of compatible observables applied to a generic SPaE. The key ingredients necessary to test the BI are an entangled state and a set of four observables $\mathbf{n}_c \cdot \sigma$ that have to be measured on the selected entangled state. In this section, it is presented an experimental setup able to generate Single Photon Entanglement (SPE) state, a SPaE state in which the particle is a single photon, and to test a BI in the form due to Clauser, Horne, Shimony and Holt (CHSH) for verifying the presence of the entanglement as in [16, 33, 42] . The experimental setup is shown in Figure 2.3. The employed DoFs are the polarization ($|V\rangle$ and $|H\rangle$ with respect to the propagation plane) and the direction of propagation of a single photon ($|0\rangle$ , east direction and $|1\rangle$, south direction, respect to Figure 2.3). In the following, each macro-stage (generation, rotation and measurement in Figure 2.3) is analyzed presenting the optical components that compose it and explaining its action on the state.

[16]: Clauser et al. (1969), 'Proposed experiment to test local hidden-variable theories'
[33]: Michler et al. (2000), 'Experiments towards Falsification of Noncontextual Hidden Variable Theories'
[42]: Barreiro et al. (2005), 'Generation of Hyperentangled Photon Pairs'

### 2.4.1 Generation stage

In the generation stage (red box in Figure 2.3 and Figure 2.4), the SPE state is created. The light is injected in the setup by using a collimator, which provides a collimated light path and fixes the direction of propagation (the collimator is not reported in Figure 2.3 and Figure 2.4). The initial polarization of the single photon is fixed by means of a Glan-Thompson Polarizer (GTP). The input state results to be $|\psi\rangle = |0V\rangle$. A balanced 50 : 50 Beam Splitter (BS) is employed to create a superposition of

[3] As before, the first subsystem, or equivalently qubit, is labeled with the letter a and the second qubit with the letter b, while the observables for the two subsystems can be written in the form $\mathbf{n}_c \cdot \sigma$, with $c \in \{a, b\}$.

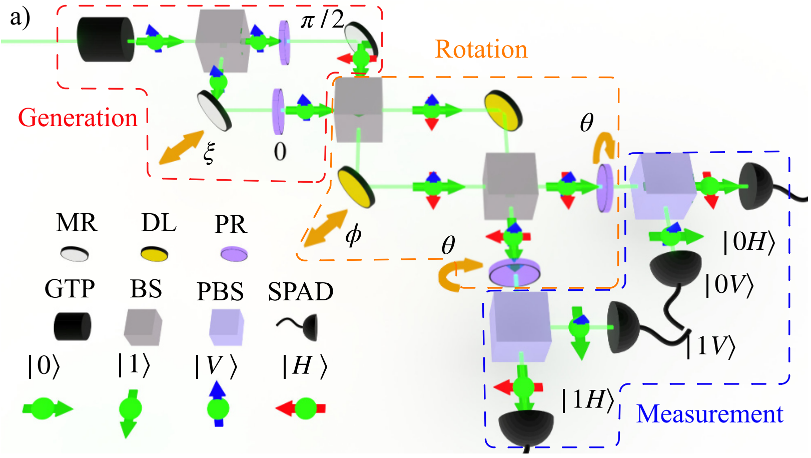


**Figure 2.3:** Scheme for the generation of SPE state and testing of the BI. The circled dashed boxes represent the main parts of the setup: the generation (red box), the rotation (orange box) and the detection (blue box) stages. The optical path is represented by green line while the photon is represented by a green sphere. The colored red and blue arrows represent the polarization of the photon, while the green arrows indicate the momentum. The optical components involved are Glan-Thompson Polarizer (GTP); Beam Splitter (BS); Mirror (MR); Delay Line (DL), composed of three mirrors for optical alignment purposes; Polarized Beam Splitter (PBS); Half-Wave Plate (HWP); Single Photon Avalanche Diode (SPAD). $\xi$ represents the angle used to compensate for phase differences in the generation. $\phi$ is the angle that fixes the direction of measurement for the momentum and $\theta$ is the angle that fixes the direction of measurement for the polarization.

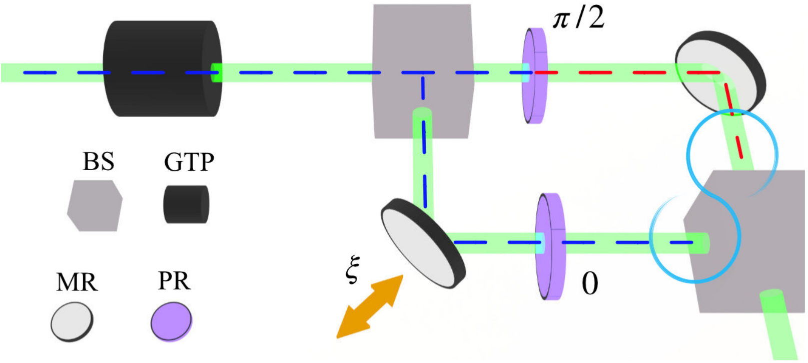


**Figure 2.4:** Details of the generation stage of Figure 2.3. In red and blue is indicated the polarization of the photon in that optical path, respectively, blue for vertical polarization and red for horizontal one. The cyan double circle represents the entangled state created.

momentum states, obtaining $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \otimes |V\rangle$. On the $|0\rangle$ path, a Half-Wave Plate (HWP) rotates the polarization of photons by $\frac{\pi}{2}$ to $|H\rangle$ and then a Mirror (MR) swaps the momentum state to $|1\rangle$. On the other path, a MR, with an adjustable delay of $\xi$, and a HWP in the null position change the momentum state to $|0\rangle$. Therefore, the following entangled state is formed:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(e^{i\xi} i|0V\rangle + |1H\rangle\right). \tag{2.24}$$

By setting $\xi = -\frac{\pi}{2}$[4], which is regulated by displacing the MR, the state $|\phi^+\rangle$ of the Bell basis is obtained:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0V\rangle + |1H\rangle). \tag{2.25}$$

The matrix representation of the state in Equation 2.25 is

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0V\rangle + |1H\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}, \tag{2.26}$$

[4] Note that the phase $\xi$ could be applied also on the other path in Figure 2.3, without any significant difference.

while its density matrix is:

$$\rho = |\phi^+\rangle\langle\phi^+| = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}. \tag{2.27}$$

All of the Bell basis states are achievable by applying the correct phase $\xi$ and by rotating the HWPs.

### 2.4.2 Physical meaning of rotation and detection stages

The aim of the rotation and detection stages (respectively, orange and blue boxes in Figure 2.3) is the construction of the four observables $\{\mathbf{n}_c \cdot \sigma\}_{c=a,a\prime,b,b\prime}$ for the momentum and the polarization. The Projection-valued measure (PVM) associated to $\mathbf{n}_c \cdot \sigma$ is

$$P^{\mathbf{n}_c}_{\pm 1} = \frac{1}{2}(I \pm \mathbf{n}_c \cdot \sigma). \tag{2.28}$$

In this way, the observable can be rewritten as

$$\mathbf{n}_c \cdot \sigma = P^{\mathbf{n}_c}_{+1} - P^{\mathbf{n}_c}_{-1}. \tag{2.29}$$

If $\rho$ is the input state of the composed system $\mathscr{H}_M \otimes \mathscr{H}_P$, the probability of observing the results $x$ for momentum and $y$ for polarization is given by:

$$\mathbb{P}(x, y|\rho, \mathbf{n}_a, \mathbf{n}_b) := \mathrm{Tr}\left[\rho P^{\mathbf{n}_a}_x \otimes P^{\mathbf{n}_b}_y\right], \qquad x, y \in \{+1, -1\}. \tag{2.30}$$

By using relation Equation 2.29, the expectation value of the observable $\mathbf{n}_a \cdot \sigma \otimes \mathbf{n}_b \cdot \sigma$ can be expressed as:

$$\begin{aligned} \mathbb{E}\left(O^M_{\mathbf{n}_a}, O^P_{\mathbf{n}_b}\right) &= \mathrm{Tr}\left[\rho\left(\mathbf{n}_a \cdot \sigma \otimes \mathbf{n}_b \cdot \sigma\right)\right] \\ &= \mathrm{Tr}\left[\rho P^{\mathbf{n}_a}_{+1} \otimes P^{\mathbf{n}_b}_{+1}\right] + \mathrm{Tr}\left[\rho P^{\mathbf{n}_a}_{-1} \otimes P^{\mathbf{n}_b}_{-1}\right] + \\ &- \mathrm{Tr}\left[\rho P^{\mathbf{n}_a}_{+1} \otimes P^{\mathbf{n}_b}_{-1}\right] - \mathrm{Tr}\left[\rho P^{\mathbf{n}_a}_{-1} \otimes P^{\mathbf{n}_b}_{+1}\right] \\ &= \mathbb{P}(1, 1|\rho, \mathbf{n}_a, \mathbf{n}_a) + \mathbb{P}(-1, -1|\rho, \mathbf{n}_a, \mathbf{n}_a) + \\ &- \mathbb{P}(1, -1|\rho, \mathbf{n}_a, \mathbf{n}_a) - \mathbb{P}(-1, 1|\rho, \mathbf{n}_a, \mathbf{n}_a) \end{aligned} \tag{2.31}$$

Moreover, it is possible to rewrite $\mathrm{Tr}\left[\rho P^{\mathbf{n}_a}_x \otimes P^{\mathbf{n}_b}_y\right]$ in a more convenient form. For any unit vector $\mathbf{n}_c \in \mathbb{R}^3$, $U_{\mathbf{n}_c} : \mathscr{H}_d \longrightarrow \mathscr{H}_d$[5] is the unitary operator transforming the PVM of the operator $\sigma^d_z$, $\{P^d_{+1}, P^d_{-1}\}$, into the PVM $\{P^{\mathbf{n}_c}_{+1}, P^{\mathbf{n}_c}_{-1}\}$ of the operator $\mathbf{n}_c \cdot \sigma$:

$$P^{\mathbf{n}_c}_{+1} = U^\dagger_{\mathbf{n}_c} P^z_{+1} U_{\mathbf{n}_c}, \quad P^{\mathbf{n}_c}_{-1} = U^\dagger_{\mathbf{n}_c} P^z_{-1} U_{\mathbf{n}_a}. \tag{2.32}$$

[5] $d = M(P)$ if $c = a(b)$

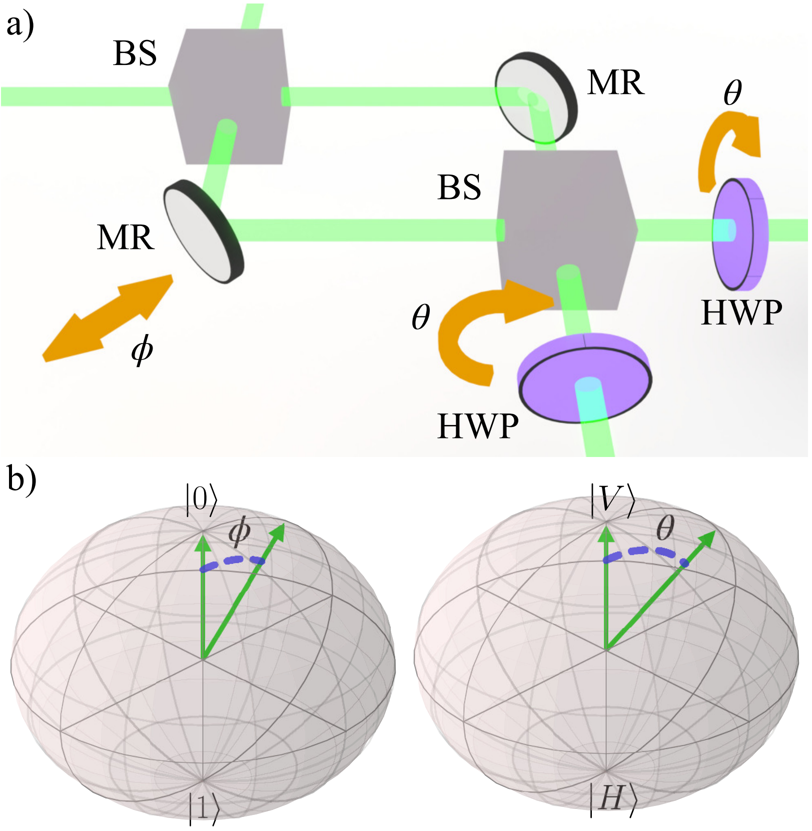


**Figure 2.5:** a) Schematics of the Rotation stage. It is composed of a MZI and by two HWPs. The MZI is constituted by two BS and two MR. The output response is determined by the transmission and reflection coefficients of the optical elements and by the phase $\phi$, the phase difference between the two arms of the MZI. The two HWPs have the scope to rotate by an angle $\theta$ the polarization of the impinging wave. b) Representations of the rotation operations on the Bloch spheres for the two DoFs considered.

Consequently $\mathbb{P}(x, y|\rho, \mathbf{n}_a, \mathbf{n}_b)$ can be rewritten as:

$$\begin{aligned}
\mathbb{P}(x, y|\rho, \mathbf{n}_a, \mathbf{n}_b) &= \mathrm{Tr}[\rho P_x^{\mathbf{n}_a} \otimes P_y^{\mathbf{n}_b}] && (2.33)\\
&= \mathrm{Tr}[\rho U^{\dagger}_{\mathbf{n}_a} P_x^M U_{\mathbf{n}_a} \otimes U^{\dagger}_{\mathbf{n}_b} P_y^P U_{\mathbf{n}_b}] && (2.34)\\
&= \mathrm{Tr}[\rho U^{\dagger}_{\mathbf{n}_a} \otimes U^{\dagger}_{\mathbf{n}_b} P_x^M \otimes P_y^P U_{\mathbf{n}_a} \otimes U_{\mathbf{n}_b}] && (2.35)\\
&= \mathrm{Tr}[U_{\mathbf{n}_a} \otimes U_{\mathbf{n}_b} \rho U^{\dagger}_{\mathbf{n}_a} \otimes U^{\dagger}_{\mathbf{n}_b} P_x^M \otimes P_y^P] && (2.36)\\
&= \mathrm{Tr}[\rho_{\mathbf{n}_a,\mathbf{n}_b} P_x^M \otimes P_y^P], && (2.37)
\end{aligned}$$

where in Equation 2.37

$$\rho_{\mathbf{n}_a,\mathbf{n}_b} = U_{\mathbf{n}_a} \otimes U_{\mathbf{n}_b} \rho U^{\dagger}_{\mathbf{n}_a} \otimes U^{\dagger}_{\mathbf{n}_b} \qquad (2.38)$$

is the density matrix corresponding to a quantum state having the DoFs rotated by the operations $U_{\mathbf{n}_a} \otimes U_{\mathbf{n}_b}$. Remarkably, the statistical distribution of outcomes for the operator $P_x^{\mathbf{n}_a} \otimes P_y^{\mathbf{n}_b}$, over the state $\rho$, coincides with the one of the operator $P_x^M \otimes P_y^P$ over the state $\rho_{\mathbf{n}_a,\mathbf{n}_b}$. Expressed in another way, operating on the state $\rho$ or changing the directions of measurement $\mathbf{n}_a$ and $\mathbf{n}_b$ are equivalent. The scope of the two stages of Figure 2.3 is now explained: the rotation stage acts on the wavefunction rotating the two DoFs and the detection stage projects the wavefunction over the basis vectors $|0V\rangle, |0H\rangle, |1V\rangle, |1H\rangle$ performing the operation $\sigma_z^M \otimes \sigma_z^P$. They essentially set the measurements basis.

### 2.4.3 Rotation stage

The optical components used in the rotation stage are MRs, BSs and HWPs(Figure 2.5). First, it is necessary to analyze the matrix corresponding to the action of the Mach Zehnder Interferometer (MZI). A MZI is a well know optical device composed of two BSs and two MRs. It has two inputs and two outputs. It modulates the intensity of the outputs depending on the phase difference that the light accumulates propagating in the device's two arms. It is possible to model it using the unitary matrix $U_\phi$:

$$U_\phi = U_{\mathrm{MZI}(\phi)} = U_{\mathrm{BS}}\, U_{\mathrm{Ph}}(2\phi)\, U_{\mathrm{MR}}\, U_{\mathrm{BS}} \tag{2.39}$$

where

$$U_{\mathrm{BS}} = \begin{pmatrix} t & ir \\ ir & t \end{pmatrix}, \quad U_{\mathrm{Ph}(\phi)} = \begin{pmatrix} e^{2i\phi} & 0 \\ 0 & 1 \end{pmatrix}, \quad U_{\mathrm{MR}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{2.40}$$

Note that $t$ and $r$ are respectively the amplitude transmission and reflection coefficients of the BSs, while $2\phi$ is the phase difference between the two arms of the MZI. In this general case, the transfer function of the MZI is:

$$U_{\mathrm{MZI}(\phi)} = \begin{pmatrix} irt + ie^{2i\phi}rt & -r^2 + e^{2i\phi}t^2 \\ -e^{2i\phi}r^2 + t^2 & irt + ie^{2i\phi}rt \end{pmatrix}. \tag{2.41}$$

In the case of a balanced BS $\left(t = r = \frac{1}{\sqrt{2}}\right)$, it is possible to simplify Equation 2.41 as:

$$U_{\mathrm{MZI}(\phi)} = ie^{i\phi} \begin{pmatrix} \cos(\phi) & \sin(\phi) \\ -\sin(\phi) & \cos(\phi) \end{pmatrix}, \tag{2.42}$$

which is the matrix that implements a rotation of the input states by an angle $\phi$. Second, two HWP are placed in each momentum direction. The response matrix for the HWP has an analogous form:

$$U_\theta = U_{\mathrm{HWP}(\theta)} = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}. \tag{2.43}$$

It is important to point out the actual physical behavior of a HWP to better understand the matrix form of $U_\theta$. Actually, the physical matrix representation of the action of the HWP is represented in Figure 2.6:

$$U_{\mathrm{HWP}(\delta)} = \begin{pmatrix} \cos(\delta) & -\sin(\delta) \\ \sin(\delta) & \cos(\delta) \end{pmatrix} \tag{2.44}$$

when the fast axis of the HWP is rotated by an angle $\delta/2$ respect to the vertical polarization. By making the substitution of angles $\delta \rightarrow -\theta$, it is possible to obtain the form reported in Equation 2.43. Consequently, to induce a rotation of $U_\theta$, it is necessary to rotate the fast axis by an angle $\delta = -\theta/2$. To keep the discussion clear, however, it is convenient to consider only the angle $\theta$, without considering the angle $\delta$. In the

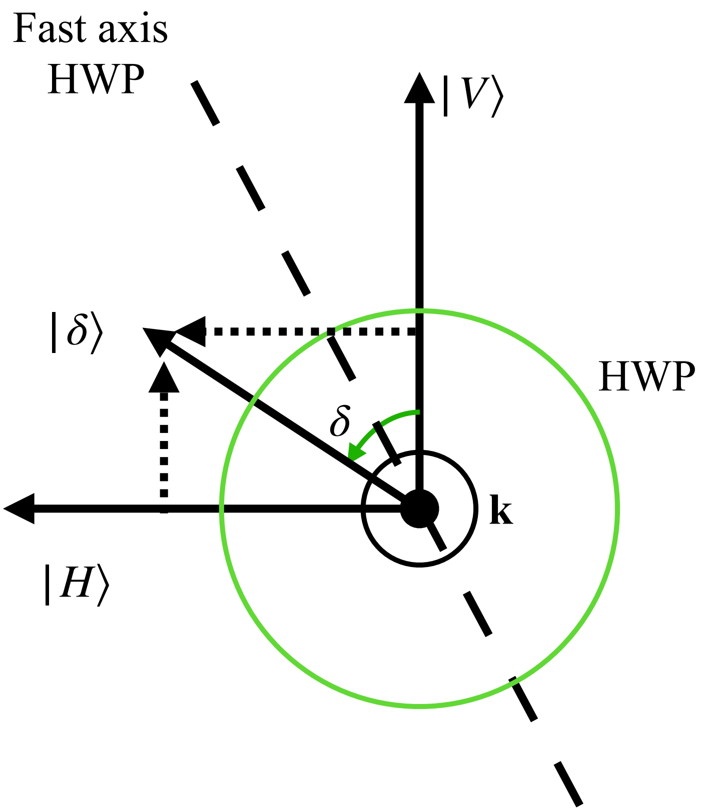


**Figure 2.6:** Schematics of the physical behavior of a rotated HWP. The optical wave has the wavevector $k$ that is pointing outside the plane determined by the $|V\rangle$ and $|H\rangle$ vectors. The fast axis of the HWP is rotated by an angle $\frac{\delta}{2}$ and induces a rotation of polarization of $\delta$.

composed Hilbert space, the two operators assume the form:

$$U_\phi(\phi) \otimes I_2^P = ie^{i\phi} \begin{pmatrix} \cos(\phi) & 0 & \sin(\phi) & 0 \\ 0 & \cos(\phi) & 0 & \sin(\phi) \\ -\sin(\phi) & 0 & \cos(\phi) & 0 \\ 0 & -\sin(\phi) & 0 & \cos(\phi) \end{pmatrix} \tag{2.45}$$

$$I_2^M \otimes U_\theta = \begin{pmatrix} \cos(\theta) & \sin(\theta) & 0 & 0 \\ -\sin(\theta) & \cos(\theta) & 0 & 0 \\ 0 & 0 & \cos(\theta) & \sin(\theta) \\ 0 & 0 & -\sin(\theta) & \cos(\theta) \end{pmatrix}. \tag{2.46}$$

The composed operator becomes:

$$U_\phi \otimes U_\theta = \left(U_\phi \otimes I_2^P\right)\left(I_2^M \otimes U_\theta\right) = ie^{i\phi}$$
$$\begin{pmatrix} \cos(\theta)\cos(\phi) & \sin(\theta)\cos(\phi) & \cos(\theta)\sin(\phi) & \sin(\theta)\sin(\phi) \\ \sin(\theta)(-\cos(\phi)) & \cos(\theta)\cos(\phi) & -\sin(\theta)\sin(\phi) & \cos(\theta)\sin(\phi) \\ -\cos(\theta)\sin(\phi) & -\sin(\theta)\sin(\phi) & \cos(\theta)\cos(\phi) & \sin(\theta)\cos(\phi) \\ \sin(\theta)\sin(\phi) & -\cos(\theta)\sin(\phi) & \sin(\theta)(-\cos(\phi)) & \cos(\theta)\cos(\phi) \end{pmatrix}. \tag{2.47}$$

### 2.4.4 Detection stage

The detection stage is composed of two PBSs and four SPADs[43] . The two PBSs are necessary to discriminate between vertically and horizontally polarized photons by introducing two other directions of propagation:

[43]: Ceccarelli et al. (2021), 'Recent Advances and Future Perspectives of Single-Photon Avalanche Diodes for Quantum Photonics Applications'

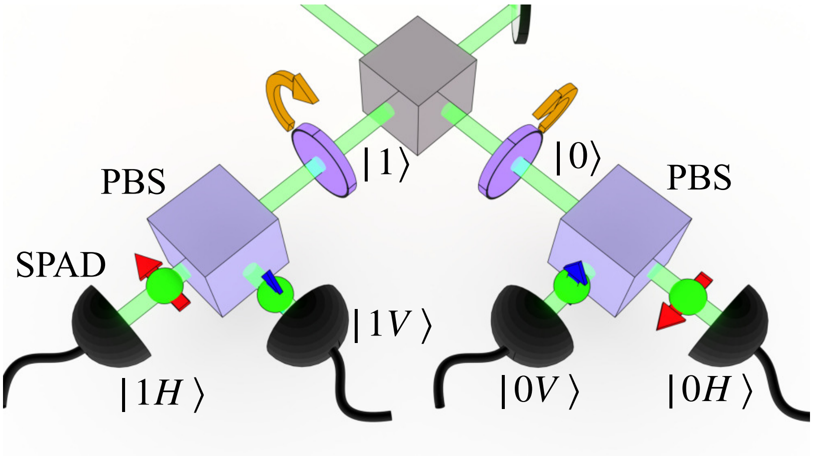


**Figure 2.7:** Schematics of the detection stage. It is composed of four SPADs and by two PBSs. The PBSs are necessary to discriminate between the horizontal and vertical polarizations, while SPADs are used to detect single photons.

each PBS reflects vertically polarized photons and transmits horizontally polarized ones. The single photons are then detected by the SPADs. The detection stage is reported in Figure 2.7. This part of the setup implements the projector operators $\{P_x^M \otimes P_y^P\}_{x,y}$, which can be represented in matrix form as:

$$P_{+1}^M \otimes P_{+1}^P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \tag{2.48}$$

$$P_{+1}^M \otimes P_{-1}^P = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \tag{2.49}$$

$$P_{-1}^M \otimes P_{+1}^P = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \tag{2.50}$$

$$P_{-1}^M \otimes P_{-1}^P = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2.51}$$

## 2.5 Theoretical form of CHSH parameter for SPE

Suppose that the generated state has the form:

$$|\psi\rangle = \frac{1}{\sqrt{\alpha^2 + \beta^2 + \gamma^2 + \delta^2}} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}, \quad \alpha, \beta, \gamma, \delta \in \mathbb{R}. \tag{2.52}$$

$|\psi\rangle$ enters in the rotation stage of Figure 2.3. The function $\chi(\mathbf{n}_a, \mathbf{n}_{a'}, \mathbf{n}_b, \mathbf{n}_{b'})$ (Equation 2.7) depends on the choice of the directions of measurement

$(\mathbf{n}_a, \mathbf{n}_{a'}, \mathbf{n}_b, \mathbf{n}_{b'})$, which are fixed by the choice of angles $(\phi, \phi', \theta, \theta')$ in the rotation stage. For this reason, the direction $\mathbf{n}_{a(b)}$ will be replaced by the angle $\phi(\theta)$ in the following discussions. The fundamental constituents of $\chi(\phi, \phi', \theta, \theta')$ are the probabilitied $\{\mathbb{P}(x, y|\rho, \phi, \theta)\}$, with $\rho = |\psi\rangle\langle\psi|$, where (see Equation 2.37)

$$\mathbb{P}(1,1|\rho,\phi,\theta) = \frac{(\cos(\theta)(\alpha\cos(\phi) + \gamma\sin(\phi)) + \sin(\theta)(\beta\cos(\phi) + \delta\sin(\phi)))^2}{\alpha^2+\beta^2+\gamma^2+\delta^2}, \tag{2.53}$$

$$\mathbb{P}(1,-1|\rho,\phi,\theta) = \frac{(\sin(\theta)(\alpha\cos(\phi) + \gamma\sin(\phi)) - \cos(\theta)(\beta\cos(\phi) + \delta\sin(\phi)))^2}{\alpha^2+\beta^2+\gamma^2+\delta^2}, \tag{2.54}$$

$$\mathbb{P}(-1,1|\rho,\phi,\theta) = \frac{(\cos(\theta)(\gamma\cos(\phi) - \alpha\sin(\phi)) - \sin(\theta)(\beta\sin(\phi) - \delta\cos(\phi)))^2}{\alpha^2+\beta^2+\gamma^2+\delta^2}, \tag{2.55}$$

$$\mathbb{P}(-1,-1|\rho,\phi,\theta) = \frac{(\sin(\theta)(\gamma\cos(\phi) - \alpha\sin(\phi)) + \cos(\theta)(\beta\sin(\phi) - \delta\cos(\phi)))^2}{\alpha^2+\beta^2+\gamma^2+\delta^2}. \tag{2.56}$$

By these, the expectation value $\mathbb{E}\left(O_\phi^M, O_\theta^P\right)$ (see Equation 2.31) is obtained, which, for Equation 2.52, takes the form:

$$\mathbb{E}\left(O_\phi^M, O_\theta^P\right) = \frac{A+B}{\alpha^2+\beta^2+\gamma^2+\delta^2} \tag{2.57}$$

where

$$\begin{aligned} A &= \cos(2\theta)\left(\cos(2\phi)\left(\alpha^2-\beta^2-\gamma^2+\delta^2\right) + 2\sin(2\phi)(\alpha\gamma-\beta\delta)\right), \\ B &= 2\sin(2\theta)(\sin(2\phi)(\alpha\delta+\beta\gamma) + \cos(2\phi)(\alpha\beta-\gamma\delta)). \end{aligned} \tag{2.58}$$

Now, it is finally possible to compute $\chi(\phi, \phi', \theta, \theta')$ (Equation 2.7) as:

$$\begin{aligned} \chi(\phi,\phi',\theta,\theta') = {} & \frac{1}{2(\alpha^2+\beta^2+\gamma^2+\delta^2)} \\ & \cos(2\theta)(\cos(2\phi)+\cos(2\phi'))(\alpha^2-\beta^2-\gamma^2+\delta^2)+ \\ & -(\cos(2\theta')(\cos(2\phi)-\cos(2\phi'))(\alpha^2-\beta^2-\gamma^2+\delta^2))+ \\ & +2\cos(2\phi)(\sin(2\theta)-\sin(2\theta'))(\alpha\beta-\gamma\delta)+ \\ & +4\sin(2\phi)\sin(\theta-\theta')(\sin(\theta+\theta')(\beta\delta-\alpha\gamma)+ \\ & +\cos(\theta+\theta')(\alpha\delta+\beta\gamma))+2\cos(2\phi')(\sin(2\theta)+ \\ & +\sin(2\theta'))(\alpha\beta-\gamma\delta)+ \\ & +4\sin(2\phi')\cos(\theta-\theta')(\sin(\theta+\theta')(\alpha\delta+\beta\gamma)+ \\ & +\cos(\theta+\theta')(\alpha\gamma-\beta\delta)). \end{aligned} \tag{2.59}$$

Consider now the four states of the Bell basis (Equation 2.15 ($\alpha = 1, \beta = 0, \gamma = 0, \delta = 1$), Equation 2.16 ($\alpha = 1, \beta = 0, \gamma = 0, \delta = -1$), Equation 2.17 ($\alpha = 0, \beta = 1, \gamma = 1, \delta = 0$), Equation 2.18 ($\alpha = 0, \beta = 1, \gamma = -1, \delta = 0$) ).

For these states, $\chi(\phi, \phi', \theta, \theta')$ becomes:

$$\begin{aligned}\chi_{|\phi^+\rangle}(\phi, \phi', \theta, \theta') &= \cos(2(\theta - \phi)) + \cos(2(\theta - \phi'))+ \\ &- \cos(2(\theta' - \phi)) + \cos(2(\theta' - \phi'));\end{aligned} \tag{2.60}$$

$$\begin{aligned}\chi_{|\phi^-\rangle}(\phi, \phi', \theta, \theta') &= \cos(2(\theta + \phi)) + \cos(2(\theta + \phi'))+ \\ &- \cos(2(\theta' + \phi)) + \cos(2(\theta' + \phi'));\end{aligned} \tag{2.61}$$

$$\begin{aligned}\chi_{|\psi^+\rangle}(\phi, \phi', \theta, \theta') &= -\cos(2(\theta + \phi)) - \cos(2(\theta + \phi'))+ \\ &+ \cos(2(\theta' + \phi)) - \cos(2(\theta' + \phi')) \\ &= -\chi_{|\phi^-\rangle}(\phi, \phi', \theta, \theta');\end{aligned} \tag{2.62}$$

$$\begin{aligned}\chi_{|\psi^-\rangle}(\phi, \phi', \theta, \theta') &= -\cos(2(\theta - \phi)) - \cos(2(\theta - \phi'))+ \\ &+ \cos(2(\theta' - \phi)) - \cos(2(\theta' - \phi')) \\ &= -\chi_{|\phi^+\rangle}(\phi, \phi', \theta, \theta').\end{aligned} \tag{2.63}$$

Consequently, it is just necessary to find the right conditions for the maximization of $\chi_{|\phi^\pm\rangle}(\phi, \phi', \theta, \theta')$ to have the condition for the minimization for $\chi_{|\psi^\pm\rangle}(\phi, \phi', \theta, \theta')$. By fixing the values of the angles as:

$$2(\theta - \phi) = -2(\theta - \phi') = 2(\theta' - \phi') = \pm\frac{\pi}{4} \tag{2.64}$$

for $\chi_{|\phi^+\rangle}(\phi, \phi', \theta, \theta')$ and

$$2(\theta + \phi) = -2(\theta + \phi') = 2(\theta' + \phi') = \pm\frac{\pi}{4} \tag{2.65}$$

for $\chi_{|\phi^-\rangle}(\phi, \phi', \theta, \theta')$ is possible to obtain the maximum violation of the BI of $2\sqrt{2}$. The minimum of $-2\sqrt{2}$ is instead achievable for

$$2(\theta - \phi) = -2(\theta - \phi') = 2(\theta' - \phi') = \pm\frac{3}{4}\pi \tag{2.66}$$

for $\chi_{|\phi^+\rangle}(\phi, \phi', \theta, \theta')$ and

$$2(\theta + \phi) = -2(\theta + \phi') = 2(\theta' + \phi') = \pm\frac{3}{4}\pi \tag{2.67}$$

for $\chi_{|\phi^-\rangle}(\phi, \phi', \theta, \theta')$. To demonstrate these conditions it is useful to define the arguments of the cosine in Equation 2.60 and Equation 2.61 as

$$\begin{aligned}2(\theta \mp \phi) &= \xi_1, \\ 2(\theta' \mp \phi') &= \xi_2, \\ 2(\theta \mp \phi') &= \xi_3.\end{aligned} \tag{2.68}$$

In this way, it is possible to rewrite Equation 2.60 and Equation 2.61 as:

$$\chi_{|\phi^\pm\rangle}(\phi, \phi', \theta, \theta') = \cos(\xi_1) + \cos(\xi_2) - \cos(\xi_1 + \xi_2 - \xi_3) + \cos(\xi_3). \tag{2.69}$$

The maximum and minimum of the function are solutions of the system:

$$\begin{cases} \frac{\partial \chi}{\partial \xi_1} = -\sin \xi_1 - \sin(\xi_1 + \xi_2 - \xi_3) = 0 \\ \frac{\partial \chi}{\partial \xi_2} = -\sin \xi_2 - \sin(\xi_1 + \xi_2 - \xi_3) = 0 \\ \frac{\partial \chi}{\partial \xi_3} = -\sin \xi_3 + \sin(\xi_1 + \xi_2 - \xi_3) = 0 \end{cases} \tag{2.70}$$

which result to be[6] :

[6] Actually these represent the solutions corresponding to maximum and minimum points. Other critical points are ignored here, i.e., the solutions $\xi_1 = \xi_2 = \xi_3 = 0, \pi$.

$$\xi_1 = \xi_2 = -\xi_3 = \pm\frac{\pi}{4}, \tag{2.71}$$

$$\xi_1 = \xi_2 = -\xi_3 = \pm\frac{3}{4}\pi. \tag{2.72}$$

By introducing the parameter $\xi_1 = \xi_2 = -\xi_3 = \omega$, $\chi_{|\phi^\pm\rangle}(\phi, \phi', \theta, \theta')$ takes the form:

$$\chi_{|\phi^\pm\rangle}(\omega) = 3\cos(\omega) - \cos(3\omega), \tag{2.73}$$

that is represented in blue in Figure 2.8. In this particular case, the angles $(\phi, \phi', \theta, \theta')$ takes the values $(\phi = 0, \phi' = \omega, \theta = \omega/2, \theta' = 3/2\omega)$. It is observed that the BI is violated for different $\omega$ values.

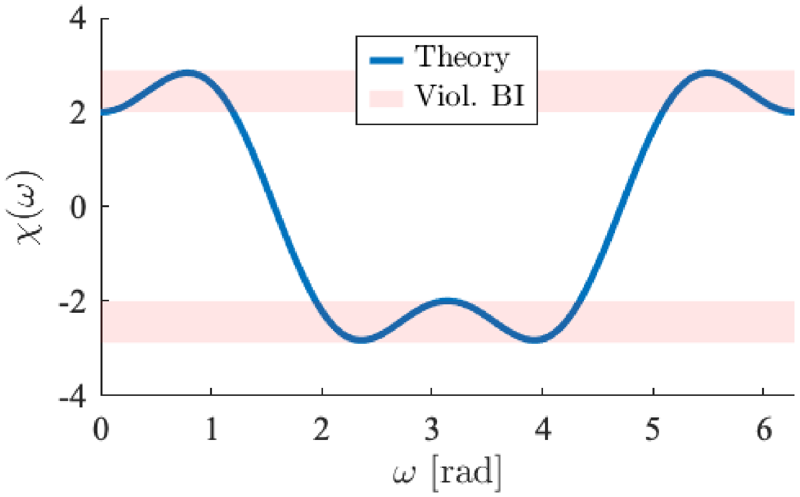


**Figure 2.8:** Graphical representation of Equation 2.73 as a function of the parameter $\omega$. Red boxes represent the values where the BI is violated. As predicted by Equation 2.71 and Equation 2.72, the maximum values are obtained for $\pm\frac{\pi}{4}$ and the minimum values for $\pm\frac{3}{4}\pi$.

In the case instead of separable states ($(\alpha = 1, \beta = \gamma = \delta = 0)$ and $(\alpha = 1, \beta = 1, \gamma = \delta = 0)$ as examples), $\chi(\phi, \phi', \theta, \theta')$ becomes:

$$\begin{aligned}\chi_{(1,0,0,0)}(\phi, \phi', \theta, \theta') = \cos(2\theta)\cos(2\phi) + \cos(2\theta)\cos(2\phi')+ \\ + \cos(2\theta')\cos(2\phi') - \cos(2\theta')\cos(2\phi)\end{aligned} \tag{2.74}$$

for $(\alpha = 1, \beta = \gamma = \delta = 0)$ and

$$\begin{aligned}\chi_{(1,1,0,0)}(\phi, \phi', \theta, \theta') = \cos(2\phi)\sin(2\theta) - \cos(2\phi)\sin(2\theta')+ \\ + \cos(2\phi')\sin(2\theta) + \cos(2\phi')\sin(2\theta')\end{aligned} \tag{2.75}$$

for $(\alpha = 1, \beta = 1, \gamma = \delta = 0)$. If the angles are fixed as before, i.e., $(\phi = 0, \phi' = \omega, \theta = \omega/2, \theta' = 3/2\omega)$ the previous equations become:

$$\chi_{(1,0,0,0)}(\omega) = \frac{1}{2}(4\cos(\omega) - \cos(3\omega) + \cos(5\omega)), \tag{2.76}$$

$$\chi_{(1,1,0,0)}(\omega) = 2\sin(\omega)\cos^2(2\omega). \tag{2.77}$$

As reported in Figure 2.9, no violation of the BI is achieved with $(\alpha = 1, \beta = \gamma = \delta = 0)$ and $(\alpha = 1, \beta = 1, \gamma = \delta = 0)$ since these states are not entangled.

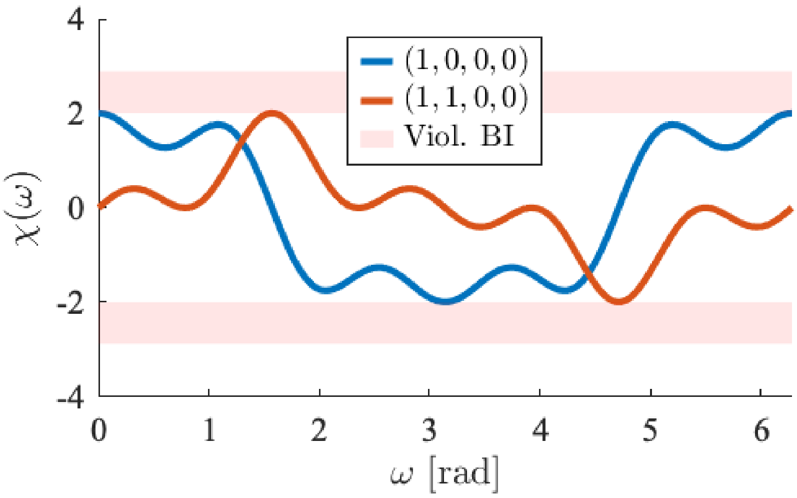


**Figure 2.9:** Graphical representation of Equation 2.76 in blue and Equation 2.77 in orange as a function of the parameter $\omega$. Red boxes represent the values where the BI is violated. As predicted by the theory, the maximum values is 2 and no violation of BI is achievable with these states.

## 2.6 Ideal experimental implementation

For experimentally testing the CHSH inequality with the ideal experimental setup reported in Figure 2.3, the correct procedure for estimating the different probabilities $\{\mathbb{P}(x,y|\rho,\phi_i,\theta_j)\}_{(x=\pm1,y=\pm1)}$ is:

1) select four couples of angles $\{(\phi_i,\theta_j)\}_{(i,j=0,1)}$,
2) randomly choose a couple $(\phi_i,\theta_j)$[7] ,
3) for each $(\phi_i,\theta_j)$, measure the state and store the result $(x,y)$,
4) repeat the points 2) and 3) many times.

The probabilities $\{\mathbb{P}(x,y|\rho,\phi_i,\theta_j)\}_{(x=\pm1,y=\pm1)}$ are then estimated as:

$$\mathbb{P}(x,y|\rho,\phi_i,\theta_j) = \frac{N_{(x,y)}(\phi_i,\theta_j)}{\sum_{x,y} N_{(x,y)}(\phi_i,\theta_j)} = \frac{N_{(x,y)}(\phi_i,\theta_j)}{N(\phi_i,\theta_j)} \tag{2.78}$$

where $N_{(x,y)}(\phi_i,\theta_j)$ is the number of photons revealed by the detector corresponding to the couple $(x,y)$ and $N(\phi_i,\theta_j) = \sum_{x,y} N_{(x,y)}(\phi_i,\theta_i)$. The object $\frac{N_{(x,y)}(\phi_i,\theta_j)}{N(\phi_i,\theta_j)}$ is called the empirical frequency of the outcome $(x,y)$ with respect to the input angles $(\phi_i,\theta_j)$. Obtained the different probabilities $\{\mathbb{P}(x,y|\rho,\phi_i,\theta_j)\}_{(x=\pm1,y=\pm1)}$ for every $(\phi,\theta)\in\{(\phi_i,\theta_j)\}_{(i,j=0,1)}$ it is possible to calculate the correlation coefficients $\mathbb{E}$ and, consequently, the $\chi$-parameter.

## 2.7 Non-idealities in the calculation of $\chi(\phi,\phi',\theta,\theta')$

In this section, the analysis of different sources of non-ideality is reported and it is discussed how they affect the estimation of the $\chi$-parameter. This allows introducing problems in the experimental test of the BI, called BI loopholes. The following aspects are considered:

- the presence of noise;
- the non-idealities of the optical components;
- the source emission statistics;
- the finite coherence time and length of the light source;

[7] Note that the necessity of this input randomness will be commented in the next section, talking about non-idealities.

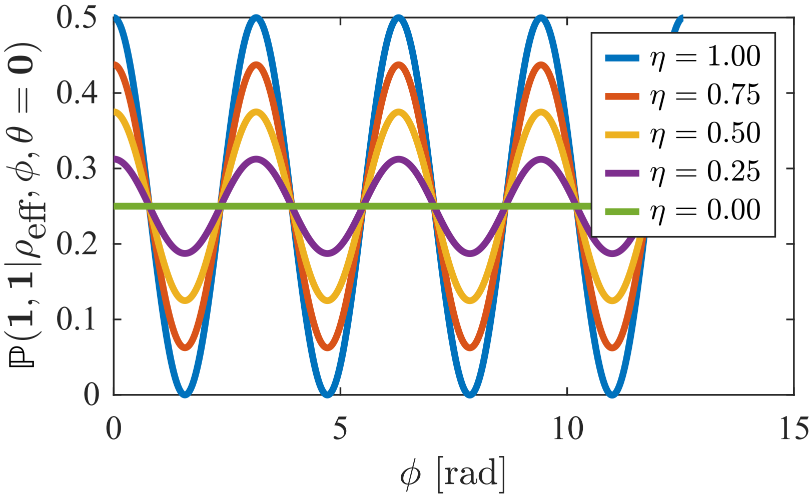


**Figure 2.10:** Graphical representation of Equation 2.80 as a function of the momentum rotation angle $\phi$ for different values of $\eta$. The amplitude of the interference fringes decreases as $\eta$ decreases.

- the non-idealities of the detectors.

### 2.7.1 Presence of noise

In an experiment, signals are affected by noise. This introduces a baseline for every $\mathbb{P}(x, y|\rho, \phi, \theta)$. To consider this effect, it is necessary to define a new density matrix:

$$\rho_{\mathrm{eff}} = \eta|\psi\rangle\langle\psi| + \frac{1-\eta}{4} I_4 \tag{2.79}$$

where $|\psi\rangle$ is one of the states of the Bell basis and $\eta$ is a phenomenological parameter introduced to consider the presence of noise. The physical meaning of $\eta$ becomes evident when the probabilities $\{\mathbb{P}(x, y|\rho, \phi, \theta)\}$ (see Equation 2.33) are considered. In the case of $\rho_{\mathrm{eff}}$, the probability $\mathbb{P}(1, 1|\rho_{\mathrm{eff}}, \phi, \theta)$ becomes:

$$\mathbb{P}(1, 1|\rho_{\mathrm{eff}}, \phi, \theta) = \frac{1}{4}(\eta\cos(2(\theta - \phi)) + 1). \tag{2.80}$$

Defining the visibility parameter $V$ for the probability $\mathbb{P}(1, 1|\rho_{\mathrm{eff}}, \phi, \theta)$ as

$$V = \frac{\max_{(\phi,\theta)}(\mathbb{P}(1, 1|\rho_{\mathrm{eff}}, \phi, \theta)) - \min_{(\phi,\theta)}(\mathbb{P}(1, 1|\rho_{\mathrm{eff}}, \phi, \theta))}{\max_{(\phi,\theta)}(\mathbb{P}(1, 1|\rho_{\mathrm{eff}}, \phi, \theta)) + \min_{(\phi,\theta)}(\mathbb{P}(1, 1|\rho_{\mathrm{eff}}, \phi, \theta))} \tag{2.81}$$

it is found that $V = \eta$. The graphical representation of $\mathbb{P}(1, 1|\rho_{\mathrm{eff}}, \phi, \theta)$ is reported in Figure 2.10 for different value of $\eta$. By observing the interference fringes of Figure 2.10, the visibility $V$ gives information about their amplitude. In particular, for $\eta = 1$ (no noise) the fringes are clearly visible, while, as $\eta$ approaches to 0 (largest noise), the fringes tend to disappear.

This information is a preliminary test for observing the violation of BI, since the visibility is strictly connected to $\mathbb{E}\left(O^M_\phi, O^P_\theta\right)$ and $\chi(\phi, \phi', \theta, \theta')$.

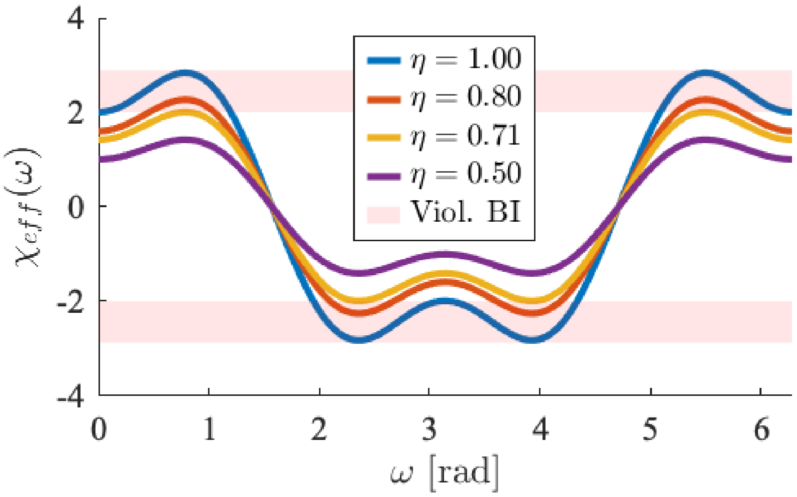


**Figure 2.11:** Graphical representation of $\chi_{\text{eff}}(\phi, \phi', \theta, \theta')$ as a function of the parameter $\omega$ for different values of $\eta$. For $\eta > \frac{1}{\sqrt{2}}$ the BI can be violated for the angles $\pm\frac{\pi}{4}$ and $\pm\frac{3}{4}\pi$, while for $\eta < \frac{1}{\sqrt{2}}$ no violation is achievable. Red boxes indicate the areas where the BI is violated.

For $\rho_{\text{eff}}$

$$\mathbb{E}_{\text{eff}}\left(O^M_\phi, O^P_\theta\right) = \eta\mathbb{E}\left(O^M_\phi, O^P_\theta\right), \tag{2.82}$$

$$\chi_{\text{eff}}(\phi, \phi', \theta, \theta') = \eta\chi(\phi, \phi', \theta, \theta'). \tag{2.83}$$

For $\eta < \frac{1}{\sqrt{2}} \simeq 0.71$, no violation of the BI is observable, since $|\chi_{\text{eff}}(\phi, \phi', \theta, \theta')| < 2, \forall(\phi, \phi', \theta, \theta')$ as reported in Figure 2.11 for $\eta = 0,71$ and $\eta = 0.5$.

### 2.7.2 Polarization dependence of the optical components

In the previous sections, the bound $|\chi_{\text{eff}}(\phi, \phi', \theta, \theta')| < 2$ is obtained by considering four observables $\left(\mathbf{n}_\phi \cdot \sigma^M \otimes I_2\right)\left(I_2 \otimes \mathbf{n}_\theta \cdot \sigma^P\right)$ that are in product form. The latter represents a necessary condition to consider the BI as an entanglement witness: the BI can attain value greater than 2 even with not-entangled systems by measuring observables not in product form. Consequently, such a product form must be ensured in each experimental implementation that tries to observe a violation of the BI. This is the first loophole that will be discussed: the locality loophole. This loophole implies the existence of possible communication channels which allow the two measurements to communicate. In this situation, the outcomes obtained by the measurement operations on the qubits $a$ and $b$ are no longer independent, i.e., $f^a_{\mathbf{n}_a,\mathbf{n}_b}(\lambda) \neq f^a_{\mathbf{n}_a}(\lambda)$ and $f^b_{\mathbf{n}_b,\mathbf{n}_a}(\lambda) \neq f^b_{\mathbf{n}_b}(\lambda)$. From an operational and practical point of view, the locality loophole can be reasonably neglected for MPE by just separating or screening out the two particles. However, this is not trivial in the case of SPE. In the case of momentum and polarization SPE states, one must ensure that the rotation of one DoF leaves the other untouched. It is worth remembering that these operations are performed by using two HWPs and a MZI. While in practical implementation, this is not a concern regarding the action of the HWPs, it results to be a problem considering the polarization response of the optical components that compose the MZI. In particular, the power reflection and and transmission coefficients of the BSs and MRs are polarization-dependent, spoiling the product form of the operator $U_\phi \otimes I_2$. The matrix representation of the BS in the basis $\{|0V\rangle, |0H\rangle, |1V\rangle, |1H\rangle\}$ can be modeled as:

$$U_{\mathrm{BS}}^{\mathrm{real}} = \begin{pmatrix} t_V & 0 & ir_V & 0 \\ 0 & t_H & 0 & ir_H \\ ir_V & 0 & t_V & 0 \\ 0 & ir_H & 0 & t_H \end{pmatrix}, \qquad \begin{array}{l} |t_V|^2 + |r_V|^2 \leq 1 \\ |t_H|^2 + |r_H|^2 \leq 1 \end{array} \tag{2.84}$$

where $t_{V,H}, r_{V,H}$ are the amplitude transmission and reflection coefficients of the BS for the corresponding polarization. The operator $U_{\mathrm{BS}}^{\mathrm{real}}$ is not in product form as long as the amplitude coefficients are different for the two polarizations. The same occurs to the operator $U_{\mathrm{MR}}^{\mathrm{real}}$:

$$U_{\mathrm{MR}}^{\mathrm{real}} = \begin{pmatrix} 0 & 0 & \gamma_{V_1} & 0 \\ 0 & 0 & 0 & \gamma_{H_1} \\ \gamma_{V_2} & 0 & 0 & 0 \\ 0 & \gamma_{H_2} & 0 & 0 \end{pmatrix}, \qquad \begin{array}{l} |\gamma_{x_y}|^2 \leq 1, \\ \forall x \in \{V,H\}, \forall y \in \{1,2\} \end{array} \tag{2.85}$$

where $\gamma_{x_y}$ is the amplitude transmission coefficient for the polarization $x$ of the mirror $y$ of the MZI. The detection probabilities, obtained by the real experimental setup, are represented by:

$$\mathbb{P}^{\mathrm{real}}(x,y|\rho,\phi,\theta) = \frac{\mathrm{Tr}[U_{\phi,\theta}^{\mathrm{real}}\rho(U_{\phi,\theta}^{\mathrm{real}})^\dagger\, P_x^M \otimes P_y^P]}{\mathrm{Tr}[U_{\phi,\theta}^{\mathrm{real}}\rho(U_{\phi,\theta}^{\mathrm{real}})^\dagger]}, \tag{2.86}$$

where

$$U_{\phi,\theta}^{\mathrm{real}} = U_{\mathrm{BS}_2}^{\mathrm{real}} U_{\mathrm{MR}}^{\mathrm{real}} U_{\mathrm{Ph}} U_{\mathrm{BS}_1}^{\mathrm{real}} (I_2 \otimes U_\theta). \tag{2.87}$$

The subscripts 1,2 indicate that, in principle, the transmission and reflection coefficients of the two BSs are different. The appearance of the term $\mathrm{Tr}[U_{\phi,\theta}^{\mathrm{real}}\rho(U_{\phi,\theta}^{\mathrm{real}})^\dagger]$ in the denominator of Equation 2.86 is justified by the presence of losses due to scattering and absorption in the BSs and MRs: the photons detected by the SPADs are only those that go through the entire setup without being lost. For this reason, it is necessary to consider in the probabilities only these photons by renormalizing the probabilities.

The scope of the following calculations is to understand the effects of these non-idealities and provide two theoretical corrections $e_{\mathbb{P}}$ and $e_\chi$ that will link the ideal probabilities and correlation function $\chi$ to those obtained by the real experimental setup. To simplify the analytical calculation, the operator $U_{\mathrm{MR}}^{\mathrm{real}}$ will be assumed as ideal and omitted in the development of the model. Indeed, it is a hermitian operator, which swaps the components $|0\rangle$ and $|1\rangle$ for momentum. This operation will be compensated by just exchanging the role of the $P_{+1}^M$ and $P_{-1}^M$, taking no effect in the final result.

In the evaluation of Equation 2.86 an useful simplification can be achieved if the losses for the polarization are comparable: if $t_{V,k}^2 + r_{V,k}^2 \simeq t_{H,k}^2 + r_{H,k}^2$, for $k = 1,2$, Equation 2.86 can be rewritten as:

$$\mathbb{P}^{\mathrm{real}}(x,y|\rho,\phi,\theta) = \mathrm{Tr}[\tilde{U}_{\phi,\theta}\rho(\tilde{U}_{\phi,\theta})^\dagger\, P_x^M \otimes P_y^P] \tag{2.88}$$

where the operator $\tilde{U}_{\phi,\theta}$ is defined as:

$$\tilde{U}_{\phi,\theta} = (U^{\mathrm{real}}_{\phi} \otimes I_2)(I_2 \otimes U_\theta) = \tilde{U}_{\mathrm{BS}_2} U_{\mathrm{Ph}}(\phi) \tilde{U}_{\mathrm{BS}_1}(I_2 \otimes U_\theta), \tag{2.89}$$

$$\tilde{U}_{\mathrm{BS}_k} = \begin{pmatrix} \tilde{t}_{V,k} & 0 & i\tilde{r}_{V,k} & 0 \\ 0 & \tilde{t}_{H,k} & 0 & i\tilde{r}_{H,k} \\ i\tilde{r}_{V,k} & 0 & \tilde{t}_{V,k} & 0 \\ 0 & i\tilde{r}_{H,k} & 0 & \tilde{t}_{H,k} \end{pmatrix}, \tag{2.90}$$

$$\tilde{r}_{x,k} = \frac{r_{x,k}}{\sqrt{t^2_{x,k} + r^2_{x,k}}}, \qquad \tilde{t}_{x,k} = \frac{t_{x,k}}{\sqrt{t^2_{x,k} + r^2_{x,k}}}, \tag{2.91}$$

with $x = V, H$ and $k = 1, 2$. By making the identification:

$$\tilde{t}_{x,k} = \cos(\alpha_{x,k}) \qquad \tilde{r}_{x,k} = \sin(\alpha_{x,k}) \tag{2.92}$$

it is possible to search for an operator

$$U^{\mathrm{ideal}}_{\phi}(u, v) = (U(u) \otimes I_2)(U_{\mathrm{Ph}}(\phi) \otimes I_2)(U(v) \otimes I_2) \tag{2.93}$$

$$U(x) = \begin{pmatrix} \cos(x) & i\sin(x) \\ i\sin(x) & \cos(x) \end{pmatrix}, \qquad x = u, v \tag{2.94}$$

in product form that minimize the Hilbert-Schmidt norm of the difference operator:

$$R(u, v)_\phi = U^{\mathrm{real}}_{\phi} - U^{\mathrm{ideal}}_{\phi}(u, v) = \tilde{U}_{\mathrm{BS}_2} U_{\mathrm{Ph}}(\phi) \tilde{U}_{\mathrm{BS}_1} - U^{\mathrm{ideal}}_{\phi}(u, v) \tag{2.95}$$

for a particular choice of $(u, v)$. This procedure is based on the implicit assumption that the action of the MZI implements the "nearest" operator $U^{\mathrm{ideal}}_{\phi}(u, v)$ instead of the ideal one $U_\phi$. For this reason, the optimization of $(u, v)$ for minimizing $R(u, v)_\phi$ is well motivated. The operator $U^{\mathrm{real}}_{\phi}$ can be viewed as:

$$U^{\mathrm{real}}_{\phi} = e^{i\phi}\left( U(\theta_V, \hat{n}_V) \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + U(\theta_H, \hat{n}_H) \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right) \tag{2.96}$$

where the operator $U(\theta_V, \mathbf{n}_V)$ and $U(\theta_H, \mathbf{n}_H)$ are:

$$U(\theta_x, \mathbf{n}_x) = \cos(\theta_x)\, I_{2\times 2} + i\sin(\theta_x)\, \mathbf{n}_x \cdot \sigma, \qquad x = V, H \tag{2.97}$$

$$\cos(\theta_x) = \cos(\phi)\cos(\alpha_{x,1} + \alpha_{x,2}), \tag{2.98}$$

$$\sin(\theta_x)\mathbf{n}_x = \begin{pmatrix} \cos(\phi)\sin(\alpha_{x,1} + \alpha_{x,2}) \\ \sin(\phi)\sin(\alpha_{x,1} - \alpha_{x,2}) \\ \sin(\phi)\cos(\alpha_{x,1} - \alpha_{x,2}) \end{pmatrix}. \tag{2.99}$$

It is possible to rewrite also $U^{\mathrm{ideal}}_{\phi}(u, v)$ in the same way

$$U^{\mathrm{ideal}}_{\phi}(u, v) = U(\overline{\theta}, \overline{\mathbf{n}}) \otimes I_2, \tag{2.100}$$

$$U(\overline{\theta}, \overline{\mathbf{n}}) = \cos(\overline{\theta})\, I_{2\times 2} + i\sin(\overline{\theta})\, \overline{\mathbf{n}} \cdot \sigma, \tag{2.101}$$

$$\cos(\overline{\theta}) = \cos(\phi)\cos(u + v), \tag{2.102}$$

$$\sin(\overline{\theta})\overline{\mathbf{n}} = \begin{pmatrix} \cos(\phi)\sin(u + v) \\ \sin(\phi)\sin(u - v) \\ \sin(\phi)\cos(u - v) \end{pmatrix}. \tag{2.103}$$

The difference operator $R_\phi = U_\phi^{\text{real}} - U_\phi^{\text{ideal}}$ takes the form:

$$R_\phi = e^{i\phi/2}\left(f_1(\phi)R_1 + f_2(\phi)R_2\right) \tag{2.104}$$

where $f_1(\phi) = \cos(\phi)$, $f_2(\phi) = \sin(\phi)$ and the two operators $R_1, R_2$ do not depend on $\phi$ and are given by

$$R_1 = \left(R_1^V \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + R_1^H \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right) \tag{2.105}$$

$$R_2 = \left(R_2^V \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + R_2^H \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right) \tag{2.106}$$

where

$$\begin{aligned} R_1^x &= (\cos(\alpha_{x,1} + \alpha_{x,2}) - \cos(u+v))I_{2\times 2} + i(\sin(\alpha_{x,1} + \alpha_{x,2}) \\ &\qquad - \sin(u+v))\sigma_x, \\ R_2^x &= i(\cos(\alpha_{x,1} - \alpha_{x,2}) - \cos(x-y))\sigma_z + i(\sin(\alpha_{x,1} - \alpha_{x,2}) \\ &\qquad - \sin(u-v))\sigma_y, \\ x &= V, H. \end{aligned} \tag{2.107}$$

The Hilbert-Schmidt norm of $R(u,v)_\phi$ can then be written as:

$$\begin{aligned} \|R_\phi(u,v)\|_{\text{HS}}^2 &= \text{Tr}[R_\phi(u,v)R_\phi^\dagger(u,v)] \\ &= 4\big(2 - \cos^2(\phi)(\cos(\alpha_{H,1} + \alpha_{H,2} - u - v) + \\ &+ \cos(\alpha_{V,1} + \alpha_{V,2} - u - v)) + \\ &- \sin^2(\phi)(\cos(\alpha_{H,1} - \alpha_{H,2} - u + v) + \\ &+ \cos(\alpha_{V,1} - \alpha_{V,2} - u + v))\big), \end{aligned} \tag{2.108}$$

and it has the minimal value for

$$u_0 = \frac{\alpha_{H,1} + \alpha_{V,1}}{2}, \qquad v_0 = \frac{\alpha_{H,2} + \alpha_{V,2}}{2}. \tag{2.109}$$

In particular, $R_\phi(u_0,v_0)R_\phi^\dagger(u_0,v_0)$ is a multiple of the identity, i.e., $R_\phi(u_0,v_0)R_\phi^\dagger(u_0,v_0) = cI_{4\times 4}$ with

$$\begin{aligned} c =& 2 - 2\cos^2(\phi)\cos\left(\frac{\alpha_{H,1} - \alpha_{V,1}}{2} + \frac{\alpha_{H,2} - \alpha_{V,2}}{2}\right) + \\ & - 2\sin^2(\phi)\cos\left(\frac{\alpha_{H,1} - \alpha_{V,1}}{2} - \frac{\alpha_{H,2} - \alpha_{V,2}}{2}\right). \end{aligned} \tag{2.110}$$

Hence $\|R_\phi\| = \sqrt{c}$. To remove the dependence of $\phi$ it is useful to take the upper bound of c for $\phi \in [0, 2\pi]$:

$$\begin{aligned} e =& \sup_{\phi\in[0,2\pi]} \|R_\phi(u_0,v_0)R_\phi(u_0,v_0)^\dagger\| \\ =& 2 - 2\min\left\{\cos\left(\frac{\alpha_{V,1} - \alpha_{H,1}}{2} + \frac{\alpha_{V,2} - \alpha_{H,2}}{2}\right),\right. \\ & \left.\cos\left(\frac{\alpha_{V,1} - \alpha_{H,1}}{2} - \frac{\alpha_{V,2} - \alpha_{H,2}}{2}\right)\right\}. \end{aligned} \tag{2.111}$$

It is important to remark that the optimization technique presented here is even more precise: it provides a bound that is accurate also in the general case where $U_\phi^{\text{real}}$ is compared to a generic operator of the type

[21]: Mazzucchi et al. (2021), 'Entropy certification of a realistic quantum random-number generator based on single-particle entanglement'

$U_M \otimes V_P \in \mathcal{H}_M \otimes \mathcal{H}_P$. For detailed proof, see [21] . It is necessary to connect the bound obtained in Equation 2.111 to the difference between the read and the ideal detection probabilities. By exploiting the identity:

$$U_\phi^{\text{ideal}} + R_\phi = U_\phi^{\text{real}}, \tag{2.112}$$

where $R_\phi = R_\phi(u_0, v_0)$, is possible to write:

$$\begin{aligned} \mathbb{P}^{\text{real}}(x, y|\rho, \phi, \theta) = \mathbb{P}^{\text{ideal}}(x, y|\rho, \phi, \theta) + \\ + \mathrm{Tr}[U_\phi^{\text{ideal}} \rho R_\phi^\dagger P_x^M \otimes P_{y,\theta}^P] + \\ + \mathrm{Tr}[R_\phi \rho (U_\phi^{\text{ideal}})^\dagger P_x^M \otimes P_{y,\theta}^P] + \\ + \mathrm{Tr}[R_\phi \rho R_\phi^\dagger 0 P_x^M \otimes P_{y,\theta}^P] \end{aligned} \tag{2.113}$$

in which $P_x^M \otimes P_{y,\theta}^P = (I \otimes U_\theta)^\dagger P_x^M \otimes P_y^P (I \otimes U_\theta)$ and $P^{\text{ideal}}(x, y|\rho, \phi, \theta) = Tr[U_\phi^{\text{ideal}} \rho U_\phi^{\text{ideal}})^\dagger P_x^M \otimes P_{y,\theta}^P]$. For any choice of $(\phi, \theta)$, the difference between the detection probabilities $\mathbb{P}^{\text{real}}(x, y|\rho, \phi, \theta)$ and the ones related to product observables $\mathbb{P}^{\text{ideal}}(x, y|\rho, \phi, \theta)$ can be bounded by

$$\begin{aligned} |\mathbb{P}^{\text{real}} - \mathbb{P}^{\text{ideal}}| = \\ = \mathrm{Tr}[U_\phi^{\text{ideal}} \rho R_\phi^\dagger P_x^M \otimes P_{y,\theta}^P] + \\ + \mathrm{Tr}[R_\phi \rho (U_\phi^{\text{ideal}})^\dagger P_x^M \otimes P_{y,\theta}^P] + \\ + \mathrm{Tr}[R_\phi \rho R_\phi^\dagger P_x^M \otimes P_{y,\theta}^P] \leq \\ \leq 2\sqrt{\|R_\phi R_\phi^\dagger\|} + \|R_\phi R_\phi^\dagger\| \leq \\ \leq 2\sqrt{e} + e = e_{\mathbb{P}}, \end{aligned} \tag{2.114}$$

where $e$ is given by Equation 2.111. The next step consists into the derivation of a similar bound for $\chi(\phi, \phi', \theta, \theta')$. In particular $\chi^{\text{real}}(\phi_0, \phi_1, \theta_0, \theta_1)$[8] is defined as:

$$\chi^{\text{real}} = \mathrm{Tr}[\rho \sum_{i,j} c_{ij} (U_{\phi_i}^{\text{real}})^\dagger (I \otimes U_{\theta_j}^\dagger) \sigma_z \otimes \sigma_z (I \otimes U_{\theta_i}) U_{\phi_i}^{\text{real}}], \tag{2.115}$$

while $\chi^{\text{ideal}}(\phi_0, \phi_1, \theta_0, \theta_1)$ as:

$$\chi^{\text{ideal}} = \mathrm{Tr}[\rho \sum_{i,j} c_{ij} (U_{\phi_i}^{\text{ideal}})^\dagger (I \otimes U_{\theta_j}^\dagger) \sigma_z \otimes \sigma_z (I \otimes U_{\theta_j}) U_{\phi_i}^{\text{ideal}}], \tag{2.116}$$

where $c_{00} = c_{10} = c_{11} = 1$ and $c_{01} = -1$. Using the Equation 2.112 it is possible to write:

$$\begin{aligned} \chi^{\text{real}} = \chi^{\text{ideal}} + \underbrace{\mathrm{Tr}[\rho \sum_{i,j} c_{ij} (R_{\phi_i})^\dagger \sigma_z \otimes \theta_j \cdot \sigma U_{\phi_i}^{\text{ideal}}]}_{\text{P1}} + \\ + \underbrace{\mathrm{Tr}[\rho \sum_{i,j} c_{ij} (U_{\phi_i}^{\text{ideal}})^\dagger \sigma_z \otimes \theta_j \cdot \sigma R_{\phi_i}]}_{\text{P2}} + \\ + \underbrace{\mathrm{Tr}[\rho \sum_{i,j} c_{ij} R_{\phi_i}^\dagger \sigma_z \otimes \theta_j \cdot \sigma R_{\phi_i}]}_{\text{P3}}. \end{aligned} \tag{2.117}$$

[8] For the sake of clarity the notation $\chi(\phi, \phi', \theta, \theta')$ needs to be replaced by $\chi(\phi_0, \phi_1, \theta_0, \theta_1)$ to compress the formulas, otherwise too long.

It is necessary to evaluate each term on the right-side of Equation 2.117. Starting with P1, exploiting Equation 2.104, it can be expressed as:

$$\begin{aligned}
&\mathrm{Tr}[\rho\sum_{i,j} c_{ij}(R_{\phi_i})^\dagger\sigma_z\otimes\theta_j\cdot\sigma U^{\mathrm{ideal}}_{\phi_i}] = \\
&\qquad \mathrm{Tr}[\rho R_1^\dagger\sum_{i,j} c_{ij}e^{-i\phi_i}f_1(\phi_i)\sigma_z\otimes\theta_j\cdot\sigma U^{\mathrm{ideal}}_{\phi_i}]+ \\
&\qquad + \mathrm{Tr}[\rho R_2^\dagger\sum_{i,j} c_{ij}e^{-i\phi_i}f_2(\phi_i)\sigma_z\otimes\theta_j\cdot\sigma U^{\mathrm{ideal}}_{\phi_i}] = \\
&\qquad \mathrm{Tr}[\rho R_1^\dagger O_1] + \mathrm{Tr}[\rho R_2^\dagger O_2], \\
&\qquad O_k = \sum_{i,j} c_{ij}e^{-i\phi_i}f_k(\phi_i)\sigma_z\otimes\theta_j\cdot\sigma U^{\mathrm{ideal}}_{\phi_i}, \\
&\qquad k = 1,2.
\end{aligned} \tag{2.118}$$

The norm of $O_i$ can be upper bounded by the value:

$$\begin{aligned}
&||O_k O_k^\dagger|| \leq 2f_k(\phi_0)^2 + 2f_k(\phi_1)^2 + 2|f_k(\phi_0)^2 - f_k(\phi_1)^2|+ \\
&+ 4|f_k(\phi_0)f_k(\phi_1)| \\
&\leq \max_{|f_k(\phi_i)|\in[0,1]} \big(2f_k(\phi_0)^2 + 2f_k(\phi_1)^2 + 2|f_k(\phi_0)^2+ \\
&-f_k(\phi_1)^2| + 4f_k(\phi_0)f_k(\phi_1)\big) \\
&= 8.
\end{aligned} \tag{2.119}$$

As a consequence, each term $|\,\mathrm{Tr}[\rho R_k^\dagger O_k]|$ can be upper bounded by exploiting the Von Neumann's trace inequality:

$$|\,\mathrm{Tr}[\rho R_k^\dagger O_k]| \leq ||R_k^\dagger O||\,\mathrm{Tr}[\rho] \leq 2\sqrt{2}\sqrt{||R_k^\dagger R_k||}, \tag{2.120}$$

resulting in this upper bound for the term P1:

$$\mathrm{Tr}[\rho\sum_{i,j} c_{ij}(R_{\phi_i})^\dagger\sigma_z\otimes\theta_j\cdot\sigma U^{\mathrm{ideal}}_{\phi_i}] \leq 2\sqrt{2}\sum_k(\sqrt{||R_k^\dagger R_k||}). \tag{2.121}$$

The same reasoning could be applied to the term P2. The last term (P3) can be maximized as follows:

$$\mathrm{Tr}[\rho\sum_{i,j} c_{ij}R^\dagger_{\phi_i}\sigma_z\otimes\theta_j\cdot\sigma R_{\phi_i}] = \sum_{a,b=1,2}\mathrm{Tr}[R_b\rho R_a^\dagger O_{ab}] \tag{2.122}$$

with

$$O_{ab} = \sum_{i,j} c_{ij}f_a(\phi_i)f_b(\phi_i)\sigma_z\otimes\theta_j\cdot\sigma. \tag{2.123}$$

By considering $||O_{ab}O_{ab}^\dagger||$:

$$\begin{aligned}
&||O_{ab}O_{ab}^\dagger|| \leq 2c_0^2 + 2c_1^2 + 2|c_0^2 - c_1^2|, \\
&c_i = f_a(\phi_i)f_b(\phi_i), \\
&k = 0,1,
\end{aligned} \tag{2.124}$$

it is possible to observe that:

- $||O_{ab}|| \leq 2$ if $a = b$,
- $||O_{ab}|| \leq 1$ if $a \neq b$.

Equation 2.122 is then bounded by

$$\sum_{a,b=1,2} \mathrm{Tr}[R_b \rho R_a^\dagger O_{ab}] \leq 2(\|R_1 R_1^\dagger\| + \|R_2 R_2^\dagger\| + \|R_1\|\|R_2\|). \tag{2.125}$$

Using Equation 2.121 for the terms P1 and P2 and Equation 2.125 for the term P3, it is possible to bound the difference between $\chi^{\mathrm{real}}$ and $\chi^{\mathrm{ideal}}$ as:

$$\begin{aligned} |\chi^{\mathrm{real}} - \chi^{\mathrm{ideal}}| \leq & 4\sqrt{2}(\|R_1\| + \|R_2\|) \\ & + 2(\|R_1\|^2 + \|R_2\|^2 + \|R_1\|\|R_2\|) = e_\chi \end{aligned} \tag{2.126}$$

where $\|R_1\|$ and $\|R_2\|$ can be obtained by explicit calculation for $(u, v) = (u_0, v_0)$:

$$R_1 R_1^\dagger = R_1^\dagger R_1 = 4\sin^2\left(\frac{\alpha_{H,1} + \alpha_{H,2} - \alpha_{V,1} - \alpha_{V,2}}{4}\right) I_{4\times 4}, \tag{2.127}$$

$$R_2 R_2^\dagger = R_2^\dagger R_2 = 4\sin^2\left(\frac{(\alpha_{H,1} - \alpha_{H,2}) - (\alpha_{V,1} - \alpha_{V,2})}{4}\right) I_{4\times 4}\,, \tag{2.128}$$

hence obtaining

$$\begin{aligned} \|R_1\| &= 2\left|\sin\left(\frac{\alpha_{H,1} + \alpha_{H,2} - \alpha_{V,1} - \alpha_{V,2}}{4}\right)\right|, \\ \|R_2\| &= 2\left|\sin\left(\frac{(\alpha_{H,1} - \alpha_{H,2}) - (\alpha_{V,1} - \alpha_{V,2})}{4}\right)\right|. \end{aligned} \tag{2.129}$$

**Generally lossy beam splitters**

The previous calculation has to be generalized in the case of not comparable losses for the two polarizations. In that situation, the denominator of Equation 2.86 cannot be "neglected" as done before. In the following, it is estimated an upper bound for the difference between the detection probabilities of Equation 2.86:

$$\mathbb{P}^{\mathrm{real}}(x, y|\rho, \phi, \theta) = \frac{\mathrm{Tr}[U^{\mathrm{real}}_{\phi,\theta}\rho(U^{\mathrm{real}}_{\phi,\theta})^\dagger\, P^M_x \otimes P^P_y]}{\mathrm{Tr}[U^{\mathrm{real}}_{\phi,\theta}\rho(U^{\mathrm{real}}_{\phi,\theta})^\dagger]}$$

and the simplified ones of Equation 2.88[9] :

$$\mathbb{P}^{\mathrm{real}}_{\mathrm{CPL}}(x, y|\rho, \phi, \theta) = \mathrm{Tr}[\tilde{U}^{\mathrm{real}}_{\phi,\theta}\rho(\tilde{U}^{\mathrm{real}}_{\phi,\theta})^\dagger\, P^M_x \otimes P^P_y]. \tag{2.130}$$

In this way, it is possible to use the result developed in the previous calculation to bound the distance between $\mathbb{P}^{\mathrm{real}}(x, y|\rho, \phi, \theta)$ and $\mathbb{P}^{\mathrm{ideal}}(x, y|\rho, \phi, \theta)$:

$$\begin{aligned} &|\mathbb{P}^{\mathrm{real}} - \mathbb{P}^{\mathrm{ideal}}| = |\mathbb{P}^{\mathrm{real}} - \mathbb{P}^{\mathrm{real}}_{\mathrm{CPL}} + \mathbb{P}^{\mathrm{real}}_{\mathrm{CPL}} - \mathbb{P}^{\mathrm{ideal}}| \leq \\ &\leq |\mathbb{P}^{\mathrm{real}} - \mathbb{P}^{\mathrm{real}}_{\mathrm{CPL}}| + |\mathbb{P}^{\mathrm{real}}_{\mathrm{CPL}} - \mathbb{P}^{\mathrm{ideal}}| \end{aligned} \tag{2.131}$$

where $|\mathbb{P}^{\mathrm{real}}_{\mathrm{CPL}} - \mathbb{P}^{\mathrm{ideal}}|$ is the term calculated previously. Moreover, the effect of the polarization losses of the two MRs (assumed equal, i.e, with the same transmission coefficients $\gamma_V$ and $\gamma_H$) will be also considered in the next calculations[10] by inserting the transmission coefficients of the MRs into the action of the second BS. Then, the matrix that represents

[9] The acronym Comparable Polarization Losses (CPL) is used here to distinguish between the real probabilities in the case of comparable polarization losses and the ones of the general case.

[10] As before, the swap operation will be considered ideal and omitted.

the second BS can be written as:

$$U_{\mathrm{BS}_2} = \begin{pmatrix} \gamma_V t_{V,2} & 0 & i\gamma_V r_{V,2} & 0 \\ 0 & \gamma_H t_{H,2} & 0 & i\gamma_H r_{H,2} \\ i\gamma_V r_{V,2} & 0 & \gamma_V t_{V,2} & 0 \\ 0 & i\gamma_H r_{H,2} & 0 & \gamma_H t_{H,2} \end{pmatrix}; \qquad \gamma_V, \gamma_H \in [0,1]. \tag{2.132}$$

The upper bound $\hat{e}$ is defined as:

$$\hat{e} = \sup_{\phi,\theta} \hat{e}(\phi,\theta) = \sup_{\phi,\theta} |\mathbb{P}^{\mathrm{real}}(x,y|\rho,\phi,\theta) - \mathbb{P}^{\mathrm{real}}_{\mathrm{CPL}}(x,y|\rho,\phi,\theta)| \tag{2.133}$$

where $\hat{e}(\phi,\theta)$ is the difference between the detection probabilities (Equation 2.86) and the simplified ones (Equation 2.88). To evaluate this term, an useful simplification consists into assuming the knowledge of the input state $\rho$ that enters into the rotation stage:

$$\rho = \alpha P_H \rho_H P_H + \beta P_V \rho_V P_V + P_V p P_H + P_H p^\dagger P_V \ , \tag{2.134}$$

where $P_V(P_H)$ is the projector associated to the subspace of $\mathcal{H}_M \otimes \mathcal{H}_P$ with fixed vertical(horizontal) polarization, $\rho_{V(H)}$ is the $2 \times 2$ density matrix associated to the vertical(horizontal) polarization, $\alpha, \beta \geq 0$ with $\alpha + \beta = 1$ and $p$ is a linear operator connecting the two subspaces with different polarizations. By introducing the two constants $c_H$ and $c_V$:

$$\begin{aligned} c_H &= \sqrt{(t^2_{H,1} + r^2_{H,1})(t^2_{H,2} + r^2_{H,2})} \\ c_V &= \sqrt{(t^2_{V,1} + r^2_{V,1})(t^2_{V,2} + r^2_{V,2})}, \end{aligned} \tag{2.135}$$

and with the decomposition of Equation 2.134, it is possible to obtain the following form for the upper bound $\hat{e}$[11] :

$$\hat{e} \leq \left| \frac{\alpha\beta(c_H^2 - c_V^2)}{\alpha c_H^2 + \beta c_V^2} \right| + \left| \frac{\sqrt{\alpha\beta}(c_H c_V - \alpha c_V^2 - \beta c_H^2)}{\alpha c_H^2 + \beta c_V^2} \right| . \tag{2.136}$$

The actual values of $\alpha$ and $\beta$ can be defined as:

$$\alpha = \frac{t_H^2}{t_V^2 + t_H^2}, \quad \beta = \frac{t_V^2}{t_V^2 + t_H^2}, \tag{2.137}$$

where $t_V^2, t_H^2$ are the power transmission coefficients for the vertical and horizontal polarizations, which consider the optical responses of the BS, HWPs and MRs in the generation stage of Figure 2.4. Derived the value of $\hat{e}$, by introducing the latter in Equation 2.131, it is possible to obtain that

$$|\mathbb{P}^{\mathrm{real}} - \mathbb{P}^{\mathrm{ideal}}| \leq 2\sqrt{e} + e + \hat{e} = e_{\mathbb{P}} \tag{2.138}$$

with $e$ given by Equation 2.111 and $\hat{e}$ bounded by Equation 2.136.

Now it is necessary to bound the distance between $\chi^{\mathrm{real}}$ and $\chi^{\mathrm{real}}_{\mathrm{CPL}}$. Since the difference $\chi^{\mathrm{real}} - \chi^{\mathrm{real}}_{\mathrm{CPL}}$ can be seen as a linear combination of the 16 distances of the probabilities in the form
$\left(\mathbb{P}^{\mathrm{real}}(x,y|\rho,\phi_i,\theta_j) - \mathbb{P}^{\mathrm{real}}_{\mathrm{CPL}}(x,y|\rho,\phi_i,\theta_j)\right)$, with $i,j = \{0,1\}$, the bound

[11] The details of the derivation can be found in [21]

is easily obtained as:

$$\begin{aligned}
&|\chi^{\text{real}}(\phi_0,\phi_1,\theta_0,\theta_1) - \chi^{\text{real}}_{\text{CPL}}(\phi_0,\phi_1,\theta_0,\theta_1)| = \\
&= \left|\sum_{i,j,x,y} c_{ij}c_{xy}\left(\mathbb{P}^{\text{real}}(x,y|\rho,\phi_i,\theta_j) - \mathbb{P}^{\text{real}}_{\text{CPL}}(x,y|\rho,\phi_i,\theta_j)\right)\right| \leq \\
&\leq \sum_{i,j,x,y}\left|\mathbb{P}^{\text{real}}(x,y|\rho,\phi_i,\theta_j) - \mathbb{P}^{\text{real}}_{\text{CPL}}(x,y|\rho,\phi_i,\theta_j)\right| \leq \\
&\leq \sum_{i,j,x,y}\hat{e} = 16\hat{e}.
\end{aligned} \tag{2.139}$$

In this way it is possible to bound the distance $|\chi^{\text{real}}(\phi_0,\phi_1,\theta_0,\theta_1) - \chi^{\text{ideal}}(\phi_0,\phi_1,\theta_0,\theta_1)|$ as:

$$\begin{aligned}
|\chi^{\text{real}} - \chi^{\text{ideal}}| \leq & 4\sqrt{2}(||R_1|| + ||R_2||) + \\
& + 2(||R_1||^2 + ||R_2||^2 + ||R_1||||R_2||) + 16\hat{e} = e_\chi
\end{aligned} \tag{2.140}$$

where $||R_1||$ and $||R_2||$ were obtained in Equation 2.129.

### Numerical approach

It is important to note that the triangular inequality defined in Equation 2.131 represents an useful simplification, since the direct analytical calculation of $|\mathbb{P}^{\text{real}} - \mathbb{P}^{\text{ideal}}|$ is not easy. This comes at the price of having a larger bound on the probabilities and, consequently, on the difference concerning the $\chi$-parameters. A more direct approach can be implemented by considering a numerical approach. Since the matrix representation of each of the optical elements was already presented both in the ideal and in the real versions, it can be useful to directly calculate the object:

$$\begin{aligned}
e_{\mathbb{P}} &= \min_{\{u,v\}}[e_{\mathbb{P}}(u,v)] \\
&= \min_{\{u,v\}}\left[\max_{\{\phi,\theta,\rho,x,y\}}\left[\left|\frac{\text{Tr}\left[U^{\text{real}}_{\phi,\theta}\rho(U^{\text{real}}_{\phi,\theta})^\dagger P^M_x \otimes P^P_y\right]}{\text{Tr}\left[U^{\text{real}}_{\phi,\theta}\rho(U^{\text{real}}_{\phi,\theta})^\dagger\right]} - \right.\right.\right. \\
&\left.\left.\left. - \text{Tr}\left[U^{\text{ideal}}_{\phi,\theta}(u,v)\rho(U^{\text{ideal}}_{\phi,\theta}(u,v))^\dagger P^M_a \otimes P^P_b\right]\right|\right]\right],
\end{aligned} \tag{2.141}$$

where the minimization and the maximization can be done numerically by using standard optimization programs like the Sequential Quadratic Programming (SQP), which can be implemented using the Global Optimization Toolbox of Matlab(c). A possible algorithm can be:

- fix a pair of $(u,v)$;
- perform a maximization over the variable parameters $\{\phi,\theta,\rho,x,y\}$;
- store the value of $e_{\mathbb{P}}(u,v)$;
- repeat.

The minimum $e_{\mathbb{P}}(u,v)$ is the best one. The same reasoning can be then applied also for the numerical calculation of $e_\chi$, with the difference that now the variable parameters are $\{\phi_0,\phi_1,\theta_0,\theta_1,\rho,x,y\}$. A clarification has to be done for the maximization over the density matrix $\rho$. This is of the form of Equation 2.79, where the only free parameter is the visibility

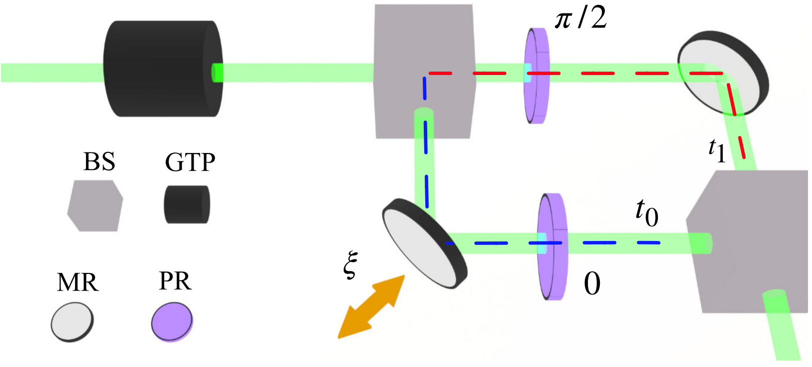


**Figure 2.12:** Details of the generation stage of Figure 2.3 with indicated the amplitude transmission coefficients relative to the direction $|0\rangle$ (blue) and $|1\rangle$ (red).

$\eta \in [0, 1]$. So the maximization has to be performed $\forall \eta \in [0, 1]$. However, an even more precise form of the density matrix $\rho$ can be consider:

$$\rho(\eta) = \begin{pmatrix} \eta|t_{0n}|^2 + (1-\eta) & 0 & 0 & v t_{0n}(t_{1n})^* \\ 0 & 1-\eta & 0 & 0 \\ 0 & 0 & 1-\eta & 0 \\ v t^*_{0n} t_{1n} & 0 & 0 & v|t_{1n}|^2 + (1-\eta) \end{pmatrix}, \tag{2.142}$$

where

$$t_{0n} = \frac{t_0}{\sqrt{t_0^2 + t_1^2}} \qquad t_{1n} = \frac{t_1}{\sqrt{t_0^2 + t_1^2}} \tag{2.143}$$

are the normalized power transmission coefficients of the two paths $|0\rangle$ and $|1\rangle$, as reported in Figure 2.12. This normalization is necessary to have a density matrix $\rho$ normalized. Physically, the observed experimental probabilities only refer to the not adsorbed or scattered photons, so the lost fraction is unimportant. The state $\rho(\eta)$ represents the most detailed description of the real state that enters in the rotation MZI, so it will be used in the numerical maximization.

### 2.7.3 Use of an attenuated source

It is necessary to underline that the previous discussions are related to a single photon over which the SPE state is written. Indeed, until now, a Hilbert space having a fixed dimensionality has been considered, selecting two distinct momenta and polarizations for the single photon. Single-photon states are usually obtained using heralding techniques[44] and non-linear optical processes like Spontaneous Parametric Down Conversion or Four-Wave Mixing [45, 46] , in which a high power laser is used. Remarkably, SPE offers the possibility of being generated starting from attenuated sources like a laser, a Light-emitting diode (LED) and a halogen lamp, without being affected by the different statistics of emission. This represents an important simplification for generating an entangled state, which can be obtained with cheaper components. It is important to remark that such a simplification is advantageous if no precise timing measurements are needed since it is impossible to know the precise time when the photon has been emitted from an attenuated source. Such a problem is not present in heralded single-photon sources. Suppose now that the input state of the electromagnetic field that enters

[44]: Eisaman et al. (2011), 'Invited review article: Single-photon sources and detectors'

[45]: Magnitskiy et al. (2015), 'A SPDC-Based Source of Entangled Photons and its Characterization'

[46]: Takesue et al. (2004), 'Generation of polarization-entangled photon pairs and violation of Bell's inequality using spontaneous four-wave mixing in a fiber loop'

into the experimental setup of Figure 2.3 is no more a single photon, but instead, is one of the following two forms:

- a coherent superposition of pure states, labeled by the number of photon $n_\psi$, all belonging to the same mode:

$$|\Psi\rangle := \sum_{n=0}^{+\infty} C_n |n_\psi\rangle \,, \quad \text{where} \quad \sum_{n=0}^{+\infty} |C_n|^2 = 1, \tag{2.144}$$

  obtained typically by a short time laser pulse;
- an incoherent superposition of pure states of finite number of particles in the same mode:

$$\rho := \sum_{n=0}^{+\infty} P_n |n_\psi\rangle\langle n_\psi| \,, \quad \text{where} \quad \sum_{n=0}^{+\infty} P_n = 1, \tag{2.145}$$

  which it is typically obtained after frequency filtration of an incoherent source (LED/halogen lamp).

$|n_\psi\rangle = \frac{1}{\sqrt{n!}}(a_\psi^\dagger)^n|\text{vac}\rangle$ represents the quantum state having $n$ single photons in the mode $|\psi\rangle = |0V\rangle$, where $|\text{vac}\rangle$ is the vacuum state and $a_\psi^\dagger$ is the creation operator of a photon in the mode $|\psi\rangle$.
Note that the representation of Equation 2.144 is valid also in the case of an ideal laser far above threshold and at the atomic physics timescale, with $C_n = e^{-\mu/2}\frac{\mu^{n/2}}{\sqrt{n!}}$, where $\mu = \langle N\rangle$ is the mean value of the number operator $N$ and $\sigma_n = \sqrt{\langle N\rangle}$. As reported in [47] , however, the relative phase between the different number of photon states $\{|n_\psi\rangle\}$ in Equation 2.144 becomes rapidly undefined due to phase diffusion and the emitted state collapses in Equation 2.145 with a Poissonian distribution $P_n = e^{-\mu}\frac{\mu^n}{n!}$ with $\langle N\rangle = \mu$ and $\sigma_n = \sqrt{\langle N\rangle}$. In the case of mode filtered thermal light at temperature $T$, the coefficients $P_n$ of Equation 2.145 take the form $P_n = \frac{1}{1+\langle n\rangle}\left(\frac{\langle n\rangle}{\langle n\rangle+1}\right)^n$ , where $\langle n\rangle = \frac{1}{\exp\{\hbar\omega/k_B T\}-1}$ and $\omega = c|\mathbf{k}|$. A LED source can be described in this way.

[47]: Wiseman (2016), 'How many principles does it take to change a light bulb. . . into a laser?'

It is important to recall that the generation stage (Figure 2.4) and rotation stage (Figure 2.5) are composed of linear optical elements, whose action can be described by two unitary[12] operators, $U_G$ and $U_R(\phi,\theta) = U_\phi \otimes U_\theta$ acting in the composed Hilbert space of the single photon $\mathcal{H}_M \otimes \mathcal{H}_P$. Considering the generation stage, its action is to transform the state $|\psi\rangle$ into one of the four states that compose the Bell basis[13] :

$$|\psi\rangle = |0V\rangle \rightarrow U_G|\psi\rangle = |\phi^+\rangle. \tag{2.146}$$

On the other hand, the action of the rotation stages is similarly described as

$$|\phi^+\rangle \longrightarrow |\psi_{\phi,\theta}\rangle = U_R(\phi,\theta)|\phi^+\rangle \,. \tag{2.147}$$

Considering the linearity of the optical elements involved, the action of the two stages on the multi-particles state is represented by the unitary operator $U^M = U_R^M(\phi,\theta)U_G^M$, acting in the Fock space, defined by the requirements

- $U^M a_\psi^\dagger (U^M)^\dagger = a_{\psi_{\phi,\theta}}^\dagger$, the number of photons is conserved, only the mode in which they are created is changed,

[12] In the following discussion the experimental setup is assumed to be ideal for simplicity.

[13] $|\phi^+\rangle$ in the following example.

- $U^M|\mathrm{vac}\rangle = |\mathrm{vac}\rangle$, the vacuum is invariant under the operator $U^M$,
- $|\psi_{\phi,\theta}\rangle = U^M_R|\psi\rangle$.

Therefore, the net action on the states of Equation 2.144 and Equation 2.145 is:

$$\begin{aligned} |\Psi\rangle \mapsto |\Psi_{\phi,\theta}\rangle &:= U^M|\Psi\rangle = \sum_{n=0}^{+\infty} C_n|n_{\psi'}\rangle\,, \\ \rho \mapsto \rho_{\phi,\theta} &:= U^M\rho(U^M)^\dagger = \sum_{n=0}^{+\infty} P_n|n_{\psi'}\rangle\langle n_{\psi'}|. \end{aligned} \tag{2.148}$$

The last part that needs to be analyzed in this multi-photon scenario is the detection stage (Figure 2.7), in which the measurement of the observables is performed. In the detection stage, four tests $Q_{(x,y)}$, are implemented: the possible outcomes are 0, no photon detected, or 1, a photon detected. Considering the two possible states that enter into this stage ($|\Psi_{\phi,\theta}\rangle, \rho_{\phi,\theta}$) the probability of obtaining the outcome 1 by one of the tests $Q_{(x,y)}$ is given by:

$$\langle\Psi_{\phi,\theta}|Q_{(x,y)}|\Psi_{\phi,\theta}\rangle := \sum_{n,m=0}^{+\infty} \overline{C_m}C_n\langle m_{\psi_{\phi,\theta}}|Q_{(x,y)}|n_{\psi_{\phi,\theta}}\rangle, \tag{2.149}$$

$$\mathrm{Tr}(\rho_{\phi,\theta}Q_{(x,y)}) := \sum_{n=0}^{+\infty} P_n\langle n_{\psi_{\phi,\theta}}|Q|n_{\psi_{\phi,\theta}}\rangle. \tag{2.150}$$

It is important to remark that each used test $Q_{(x,y)}$ commutes with the observable number of particles. Therefore, in the case of Equation 2.149, $\langle m_{\psi'}|Q_{(x,y)}|n_{\psi'}\rangle = 0$, when $m \neq n$, allowing to rewrite that as:

$$\langle\Psi_{\phi,\theta}|Q_{(x,y)}|\Psi_{\phi,\theta}\rangle := \sum_{n=0}^{+\infty} |C_n|^2\langle n_{\psi_{\phi,\theta}}|Q|n_{\psi_{\phi,\theta}}\rangle\,. \tag{2.151}$$

Equation 2.151 has the same form of Equation 2.150, which means that the detection stage cannot distinguish between a coherent superposition of pure number states and an incoherent superposition having $P_n = |C_n|^2$. Consequently, the entire analysis can be performed for each single pure state with a fixed number of particles separately and then it is possible to combine all of them with the weights $P_n$ or $|C_n|^2$. According to this, suppose that the Fock state $|n_\psi\rangle$ enters into the setup. On each photon belonging to $|n_\psi\rangle$, the values of the momentum and polarization are measured obtaining one of the results: $(1,1),(1,-1),(-1,1),(-1.-1)$. Those test $\{Q_{(x,y)}\}$ are:

$$\textit{mutually compatible} \quad [Q_{(x,y)}, Q_{(x',y')}] = 0, \tag{2.152}$$

$$\textit{pairwise exclusive} \quad Q_{(x,y)}Q_{(x',y')} = 0 \quad \text{for } (x,y) \neq (x',y'), \tag{2.153}$$

$$\textit{exhaustive} \quad \sum_{x,y} Q_{x,y} = I_4. \tag{2.154}$$

When n photons enter into the setup, the four single particle tests determine a class of tests $\{Q_\mathbf{n}\}$, where $\mathbf{n} = (n_1,n_2,n_3,n_4) \in \mathbb{N}^4$ and $n_1+n_2+n_3+n_4 = n$. The particular test $Q_\mathbf{n}$ occurs only if $n_1$ photons have produced the result $(1,1)$, $n_2$ the result $(1,-1)$, $n_3$ the result $(-1,1)$

and $n_4$ the result $(-1,-1)$. These multi-particle tests are:

$$\textit{mutually compatible} \quad [Q_{\mathbf{n}}, Q_{\mathbf{m}}] = 0, \tag{2.155}$$

$$\textit{pairwise exclusive} \quad Q_{\mathbf{n}}, Q_{\mathbf{m}} = 0 \quad \text{for } \mathbf{n} \neq \mathbf{m} \tag{2.156}$$

$$\textit{exhaustive} \quad \sum_{n_1+n_2+n_3+n_4=n} Q_{\mathbf{n}} = I \tag{2.157}$$

and they take into account every possible combination of outcomes obtainable having $n$ indistinguishable photons. Considering the one-particle tests $\{Q_{(x,y)}\}$, these multi-particle test $Q_{\mathbf{n}}$ are defined as

$$\begin{aligned} Q_{\mathbf{n}} \equiv \\ \sum_{\pi} Q_{(1,1)}^{\pi(1)} \cdots Q_{(1,1)}^{\pi(n_1)} Q_{(1,-1)}^{\pi(n_1+1)} \cdots Q_{(1,-1)}^{\pi(n_1+n_2)} Q_{(-1,1)}^{\pi(n_1+n_2+1)} \cdots \\ \cdots Q_{(-1,1)}^{\pi(n_1+n_2+n_3)} Q_{(-1,-1)}^{\pi(n_1+n_2+n_3+1)} \cdots Q_{(-1,-1)}^{\pi(n_1+n_2+n_3+n_4)}, \end{aligned} \tag{2.158}$$

where $\pi$ indicates all the permutations of the set of indexes $\{1, \ldots, n\}$. The operator $Q_1^{j_1} \cdots Q_n^{j_n}$, with $\{j_1, ..., j_n\} = \{1, ..., n\}$ acts on the tensor product of $n$ copies of the Hilbert space $\mathcal{H}_M \otimes \mathcal{H}_P$, and $Q_{(x,y)}^{j_l}$ indicates the operator

$$Q_{(x,y)}^{j_l} \equiv \underbrace{I \otimes \cdots \otimes I}_{j_l-1 \text{ factors } I} \otimes \underbrace{Q_{(x,y)}}_{j_l \text{ th position}} \otimes \underbrace{I \otimes \cdots \otimes I}_{n-j_l \text{ factors } I} . \tag{2.159}$$

Now, the probability of finding the outcome $\{(x, y)\}$ for $\{n_i\}_{i=1,2,3,4}$ particles for the state $|n_{\psi_{\phi,\theta}}\rangle$ can be computed from Equation 2.158 as:

$$\langle n_{\psi_{\phi,\theta}}|Q_{\mathbf{n}}|n_{\psi_{\phi,\theta}}\rangle = \frac{n!}{n_1!n_2!n_3!n_4!} \prod_{(x=0,y=0)}^{(x=1,x=1)} \langle \psi_{\phi,\theta}|Q_{(x,y)}|\psi_{\phi,\theta}\rangle^{n_i} \tag{2.160}$$

Equation 2.160 corresponds to the multinomial distribution of $n$ independent random variables $\{\xi_j\}_{j=1,...,n}$ with four possible results $i = (1,1),(1,-1),(-1,1),(-1.-1)$ and having as elementary probabilities:

$$\mathbb{P}(\xi_j = (x, y)) = \langle \psi_{\phi,\theta}|Q_{(x,y)}|\psi_{\phi,\theta}\rangle, \qquad j = 1, ..., n. \tag{2.161}$$

From Equation 2.160 is clear that the photons of the beam can be treated as independent and identically distributed random variables, $\{\xi_j\}_{j\in\mathbb{N}}$, with four possible outcomes and corresponding probabilities reported in Equation 2.161. In other words, the linear optical transformation performed by the experimental setup is applied individually on each photon, independently of the statistics of emission of the source of light. Consequently, there are no differences between an attenuated beam of photons and a heralded single-photon source, provided ideal detectors are used and Poissonian statistics is applied. More precisely, the discrimination of the number of incoming photons is possible due to the ideal detector where non-idealities, such as dead time and dynamic range, are neglected. Given this assumption, the detection stage observes a flux of photons in both cases. The only difference is that the time of arrival on the detector can be determined within a certain confidence level for heralded single-photon sources, while it is a stochastic process for attenuated sources.

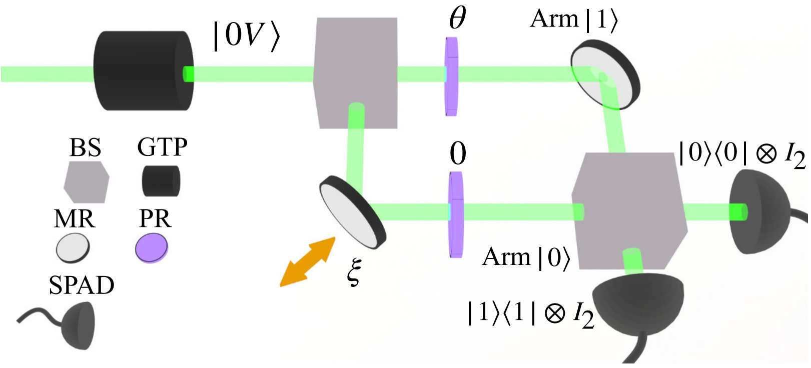


**Figure 2.13:** Schematics of the experimental setup to analyze the coherence properties of the SPE state. Note that it is only constituted by the generation stage of Figure 2.3, with the addition of one BS and two detectors that perform the projection operation in the two momentum states, without considering the polarization DoF.

### 2.7.4 Broadband spectrum of the source of photons

As previously introduced, the generation of SPE states does not depend on the form of the input state, which can be a coherent superposition or a statistical mixture of pure states. Indeed, they can be generated even using attenuated incoherent sources, such as a lamp or a LED. In this case, it is necessary to consider the short coherence time $\tau_c$ and, consequently, the short coherence length $l_c$ of the input source.

To analyze this, it is necessary to introduce the setup of Figure 2.13. A precise description of the state that exits from the first BS of Figure 2.4 is:

$$|\psi\rangle = \psi_j(\mathbf{k}), |\theta\rangle \qquad |\theta\rangle := \cos(\theta)|V\rangle - \sin(\theta)|H\rangle. \tag{2.162}$$

The state $|\theta\rangle$ takes into account the polarization of the photons, while the function $\psi_j$ refers to its momentum, which is concentrated around $\mathbf{k}_j \in \mathbb{R}^3$. More precisely, the momentum $\mathbf{k}_j$ is the center of a small ball $B_j \subset \mathbb{R}^3$: each wavevector belonging to the ball $B_j$ is an allowed momentum wavevector for the state. Note that the shape of $B_j$ is determined by the source, or more precisely, by the collimator used to inject the light into the optical setup of Figure 2.13. The momenta $\hbar\mathbf{k}_0$ and $\hbar\mathbf{k}_1$ define the two momentum states $|0\rangle, |1\rangle$ which are an effective approximations of the functions $\psi_0$ and $\psi_1$. It holds $\omega_0 = c|\mathbf{k}_0| = c|\mathbf{k}_1|$ where $\frac{\omega_0}{2\pi}$ is the central frequency of the light that enters into the setup. Note that since $\langle 1|0\rangle = 0$, the two small ball $B_j \subset \mathbb{R}^3$ in which $\mathbf{k}_j$ are defined, must be disjoint. To describe the effect of the coherence time, or equivalently length, it is necessary to introduce the time evolution operator $U_t$ of the following form:

$$U_t\psi(\mathbf{k})|\theta\rangle = e^{-ic|\mathbf{k}|t}\psi(\mathbf{k})|\theta\rangle\,. \tag{2.163}$$

Due to the dependence of the term $e^{-ic|\mathbf{k}|t}$ on $\mathbf{k}$, the approximation of having a finite dimension Hilbert space is no longer valid since the state changes with time. The entangled state entering the second BS of Figure 2.13, assuming $\xi = 0$, is no longer the Bell state

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0V\rangle + |1H\rangle\right), \tag{2.164}$$

but instead

$$|\phi^+_{(\text{precise})}\rangle := \frac{1}{\sqrt{2}}\left(i\psi_0(\mathbf{k})|V\rangle + e^{-icT|\mathbf{k}|}\psi_1(\mathbf{k})|\theta\rangle\right). \tag{2.165}$$

An absolute phase $e^{-ict|\mathbf{k}|}$ is omitted in the following discussion, since it is irrelevant for the calculation. $T$ in Equation 2.165 represents the time delay between the two arms (Arm $|0\rangle$ and Arm $|1\rangle$ in Figure 2.13) exiting from the first BS. In other words, $cT|\mathbf{k}| = \delta$ represents the phase difference between the two paths. To better highlight the phase difference between the term $|0V\rangle$ and the term $|1H\rangle$, it is useful to ignore an overall phase of $e^{i\pi/2}$. Consequently, the state of Equation 2.165 can be rewritten as:

$$|\phi^{+}_{(\text{precise})}\rangle := \frac{1}{\sqrt{2}}\left(\psi_0(\mathbf{k})|V\rangle - ie^{-icT|\mathbf{k}|}\psi_1(\mathbf{k})|\theta\rangle\right). \tag{2.166}$$

The robustness of the SPE is evaluated by observing the interference between the two terms $\psi_0(\mathbf{k})|V\rangle$ and $\psi_1(\mathbf{k})|\theta\rangle$ by using a second BS and two SPADs as reported in Figure 2.13. Consider an ideal BS that acts on the state in Equation 2.166 transforming it into:

$$\begin{aligned} |\phi^{\text{out}}_{(\text{precise})}\rangle =& \\ &=(U_{BS}\otimes I_2)|\phi^{+}_{(\text{precise})}\rangle \\ &=\frac{1}{2}(\psi_0(\mathbf{k}) + i\psi_1(\mathbf{k}))|V\rangle+ \\ &-\frac{i}{2}e^{-ict|\mathbf{k}|}(i\psi_0(\mathbf{k}) + \psi_1(\mathbf{k}))|\theta\rangle. \end{aligned} \tag{2.167}$$

In the simplified vision of two separated momentum states, the two SPADs of Figure 2.13 implement the projection operations over the momentum basis $|0\rangle, |1\rangle$. In the more accurate description, the orthogonal projector acts as multiplicative operators $P_j := \xi_{K_j}(\mathbf{k})$ in the space of momentum packets. In particular:

$$\begin{aligned} \xi_{K_j}(\mathbf{k}) = 0 \quad \text{if} \quad \mathbf{k} \notin K_j, \\ \xi_{K_j}(\mathbf{k}) = 1 \quad \text{if} \quad \mathbf{k} \in K_j. \end{aligned} \tag{2.168}$$

$K_j$ indicates a set of momenta which includes the corresponding ball $B_j$ and such that $K_0 \cap K_1 = \emptyset$. Note that the detector fixes the shape of $K_j$. This is a truncated cone having its axis parallel to $\mathbf{k}_j$ and its bases are pieces of parallel spherical surfaces. The device's maximal and minimal frequencies detectable define the distance of the two bases from the origin of the space of momenta. The probability to detect a photon in the $j$-th detector is given by:

$$\begin{aligned} &\langle\phi^{\text{out}}_{(\text{precise})}|P_j\otimes I_2|\phi^{\text{out}}_{(\text{precise})}\rangle = \\ &\frac{1}{2}\left(1 + (-1)^j\cos(\theta)\int_{\mathbb{R}^3}\cos(cT|\mathbf{k}|)|\psi_j(\mathbf{k})|^2 d^3k\right) = \\ &\frac{1}{2}\left(1+\alpha_j(T)\right). \end{aligned} \tag{2.169}$$

Note that, when the $\alpha_j = 0$, the result coincides to the case of an incoherent superposition

$$\rho_{\text{Mixed}} = \frac{1}{2}\left(|0\rangle\langle 0|\otimes|V\rangle\langle V| + |1\rangle\langle 1|\otimes|\theta\rangle\langle\theta|\right) \tag{2.170}$$

entering in Figure 2.13. The term $\alpha_j$ represents the contribution due to the quantum interference and it is a function of the delay time $T$. Moreover, it holds that:

$$\int_{\mathbb{R}^3} \cos(cT|k|)|\psi_j(\mathbf{k})|^2 d^3k = \mathrm{Re}\left[\int_0^{+\infty} e^{iT\omega} f(\omega) d\omega\right], \tag{2.171}$$

and

$$f(\omega) = \frac{\omega^2}{c^3} \int |\psi_j(\omega/c, \vartheta, \varphi)|^2 \sin(\vartheta) d\vartheta d\varphi. \tag{2.172}$$

The right-hand side represents the integral of $|\psi_j(\mathbf{k})|^2$ over the two polar angles $\vartheta, \varphi$ of the vector $\mathbf{k}$ whose norm is $\omega/c$. To evaluate the integral, the following assumption is introduced: the function $f$ can be approximated by a Gaussian function centered in $\omega_0 = c|\mathbf{k}_0| = c|\mathbf{k}_1|$ and having a standard deviation $\sigma_\omega$:

$$f(\omega) = \frac{e^{-\frac{(\omega-\omega_0)^2}{2\sigma_\omega^2}}}{\sqrt{2\pi\sigma_\omega^2}}. \tag{2.173}$$

$\sigma_\omega$ represents the width of the spectrum of the input light. Under the previous approximation and the condition $\omega_0 \gg \sigma_\omega$ the integral of Equation 2.171 can be estimated as:

$$\begin{aligned} &\mathrm{Re}\int_0^{+\infty} e^{iT\omega} f(\omega) d\omega \simeq \mathrm{Re}\int_{-\infty}^{+\infty} e^{iT\omega} f(\omega) d\omega = \\ &\mathrm{Re}(e^{iT\omega_0} g(T)) = \cos(\omega_0 T) g(T) \end{aligned} \tag{2.174}$$

where

$$g(T) = e^{-\frac{1}{2}\sigma_\omega^2 T^2}. \tag{2.175}$$

The function $g$ is the density of a centered Gaussian function with standard deviation given by $\sigma_T = 1/\sigma_\omega$, up to normalization terms. In the case $|T| \gg 1/\sigma_\omega$, the quantum interference term $\alpha_j(T)$ is negligible in Equation 2.169. In this situation the state represented in Equation 2.167 can be replaced by the incoherent superposition of Equation 2.170. In the case where the delay time $|T|$ is lower that the coherence time, i.e., $|T| \ll 1/\sigma_\omega$, the initial assumption on the two distinct packets is applicable: the phase $e^{-icT|k|}$ in Equation 2.169 is approximated by $e^{-iT\omega_0}$, and the entangled state entering the second BS can be defined as:

$$|\phi^+_{(\mathrm{simpl})}\rangle := \frac{1}{\sqrt{2}}\left(|0V\rangle - ie^{-iT\omega_0}|1\theta\rangle\right). \tag{2.176}$$

At the output of the second BS the state becomes

$$\begin{aligned} |\phi_{\mathrm{out}}\rangle =& \frac{i}{2}|0\rangle\left[(1 + e^{-iT\omega_0}\cos(\theta))|V\rangle - e^{-iT\omega_0}\sin(\theta)|H\rangle\right] + \\ &+ \frac{1}{2}|1\rangle\left[(-1 + e^{-iT\omega_0}\cos(\theta))|V\rangle - e^{-iT\omega_0}\sin(\theta)|H\rangle\right] \end{aligned} \tag{2.177}$$

and, consequently, the probability of detecting a photon results to be

$$\begin{aligned} &\langle\phi_{\mathrm{out}}|P_j \otimes I_2|\phi_{\mathrm{out}}\rangle = \\ &\quad = \frac{1}{4}\left[|1 + (-1)^j e^{-iT\omega_0}\cos(\theta)|^2 + \sin^2(\theta)\right] \\ &\quad = \frac{1}{2}(1 + (-1)^j\cos(\theta)\cos(T\omega_0)). \end{aligned} \tag{2.178}$$

Note that the same arguments apply to any other state of the Bell basis that can be generated using the setup presented in Figure 2.13. In conclusion, it is necessary that the two components of the SPE have a time delay within the coherence time of the source of light of the experiment, otherwise no violation of the BI can be achieved since the state is replaced by the incoherent superposition of Equation 2.170

**Effective analysis of the coherence length/time**

The previous discussion allows to explain the phenomenological description presented in [48] . In the latter, the desnsity matrix $|\phi^+_{\text{precise}}\rangle\langle\phi^+_{\text{precise}}|$ is replaced by a phenomenological density matrix $\rho_\epsilon$:

[48]: Vallés et al. (2014), 'Generation of tunable entanglement and violation of a Bell-like inequality between different degrees of freedom of a single photon'

$$\rho_\epsilon = (1-\epsilon)|\phi_{\text{entangled}}\rangle\langle\phi_{\text{entangled}}| + \epsilon\rho_{\text{Mixed}}. \tag{2.179}$$

$\rho_{\text{Mixed}}$ represents the totally mixed state given by Equation 2.170, while $|\phi_{\text{entangled}}\rangle$ is the pure state reported in Equation 2.176. Lastly, $0 \leq \epsilon \leq 1$ is a phenomenological coherence parameter. In particular:

- $\epsilon = 0$ corresponds to a phase difference within the coherence region. The state is the maximally entangled one;
- $\epsilon = 1$ corresponds to a phase difference outside the coherence region. The state is the totally mixed one and no entanglement is present.

The aim of the following discussion is to determine the functional form of $\epsilon$ as a function of the delay time $T$. Considering the action of the second BS, the resulting state is given by

$$\rho_{\epsilon,\text{out}} = (U_{BS}\otimes I)\rho_\epsilon(U_{BS}\otimes I)^\dagger. \tag{2.180}$$

Up to now, it has been considered only observables of the form $|j\rangle\langle j|\otimes Q_j$ and their infinite dimensional counterparts $P_j \otimes Q$ in the infinite dimensional Hilbert space, where the precise time evolution (Equation 2.163) has been introduced. The operator $Q$ works, instead, in the polarization space. Therefore, the state $\rho_{\epsilon,\text{out}}$ must satisfy:

$$\text{Tr}\left[\rho_{\epsilon,\text{out}}|j\rangle\langle j|\otimes Q\right] = \langle\phi^{(out)}_{(\text{precise})}|P_j\otimes Q|\phi^{(out)}_{(\text{precise})}\rangle. \tag{2.181}$$

Inserting Equation 2.179 in the latter equation, it can be written:

$$\begin{aligned}\langle\phi^{(out)}_{(\text{precise})}&|P_j\otimes Q|\phi^{(out)}_{(\text{precise})}\rangle = \\ =&(1-\epsilon)\langle\phi_{\text{entangled}}|(U_{BS}\otimes I)^\dagger(|j\rangle\langle j|\otimes Q)(U_{BS}\otimes I)|\phi_{\text{entangled}}\rangle \\ &+\epsilon\,\text{Tr}[(U_{BS}\otimes I)\rho_{\text{Mixed}}(U_{BS}\otimes I)^\dagger(|j\rangle\langle j|\otimes Q)].\end{aligned} \tag{2.182}$$

By manipulating Equation 2.182 considering $\langle V|Q|\theta\rangle = |\langle V|Q|\theta\rangle|e^{i\varphi}$ and the previously introduced discussion on the coherence length, within the approximation $e^{-icT|k|} \simeq e^{-iT\omega_0}$, it is possible to obtain the final functional relation between $\epsilon$ and $T$:

$$\epsilon(T) = 1 - \int_{-\infty}^{+\infty}\frac{\cos(\omega T+\varphi)}{\cos(\omega_0 T+\varphi)}\frac{e^{-\frac{(\omega-\omega_0)^2}{2\sigma_\omega^2}}}{\sqrt{2\pi\sigma_\omega^2}}d\omega = 1 - e^{-\frac{1}{2}\sigma_\omega^2T^2}. \tag{2.183}$$

It is important to note that the form of the $\epsilon$ parameter is in accordance with the result obtained in the previous section. Indeed, for $|T| \gg \frac{\sqrt{2}}{\sigma_\omega}$ the coherence is lost, and the state results to be the totally mixed one (Equation 2.170), while for $|T| \ll \frac{\sqrt{2}}{\sigma_\omega}$ the state is of the form of Equation 2.167 and can be approximated by using Equation 2.177.

### CHSH inequality for partially incoherent states

Lastly, the form of the CHSH correlation function $\chi$ has to be modified in the case of partially incoherent states of the form given by Equation 2.179. The pure state $|\phi^+\rangle$ entering the rotation stage of Figure 2.3 is replaced by the state:

$$\rho^\epsilon = (1-\epsilon)|\phi^+\rangle\langle\phi^+| + \epsilon\rho_{\text{Mixed}} \tag{2.184}$$

with $\rho_{\text{Mixed}} = \frac{1}{2}(|1H\rangle\langle 1H| + |0V\rangle\langle 0V|)$. Recalling the operation induced by the MZI (apart for a global phase term $ie^{i\phi}$) and the HWPs:

$$\begin{aligned} U(\phi)|0\rangle &= \cos(\phi)|0\rangle - \sin(\phi)|1\rangle, \\ U(\phi)|1\rangle &= \cos(\phi)|1\rangle + \sin(\phi)|0\rangle, \\ U(\theta)|V\rangle &= \cos(\theta)|V\rangle - \sin(\theta)|H\rangle, \\ U(\theta)|H\rangle &= \cos(\theta)|V\rangle + \sin(\theta)|H\rangle, \end{aligned} \tag{2.185}$$

and considering $\rho' = U(\phi)\otimes U(\theta)\rho_{Mixed}(U(\phi)\otimes U(\theta))^\dagger$, the following probabilities are obtained:

$$\mathbb{P}(1,1|\rho,\phi,\theta) = Tr[\rho'|0V\rangle\langle 0V|] = \frac{1}{4}\left(1+\cos(2\phi)\cos(2\theta)\right), \tag{2.186}$$

$$\mathbb{P}(1,-1|\rho,\phi,\theta) = Tr[\rho'|0H\rangle\langle 0H|] = \frac{1}{4}\left(1-\cos(2\phi)\cos(2\theta)\right), \tag{2.187}$$

$$\mathbb{P}(-1,1|\rho,\phi,\theta) = Tr[\rho'|1V\rangle\langle 1V|] = \frac{1}{4}\left(1-\cos(2\phi)\cos(2\theta)\right), \tag{2.188}$$

$$\mathbb{P}(-1,-1|\rho,\phi,\theta) = Tr[\rho'|1H\rangle\langle 1H|] = \frac{1}{4}\left(1+\cos(2\phi)\cos(2\theta)\right). \tag{2.189}$$

Hence,

$$\mathbb{E}\left(O^M_\phi, O^P_\theta\right) = \cos(2\phi)\cos(2\theta). \tag{2.190}$$

Eventually, it is obtained

$$\begin{aligned} \chi(\phi,\phi',\theta,\theta')_{\text{Mixed}} = &\cos(2\phi)\cos(2\theta) + \cos(2\phi')\cos(2\theta) + \\ &+ \cos(2\phi')\cos(2\theta') - \cos(2\phi)\cos(2\theta'). \end{aligned} \tag{2.191}$$

For $\phi = 0$, $\theta = \omega/2$, $\phi' = \omega$, $\theta' = 3/2\omega$, $\chi$ takes the form:

$$\chi_{\text{Mixed}}(\omega) = \frac{1}{2}(4\cos(\omega) - \cos(3\omega) + \cos(5\omega)) \tag{2.192}$$

which is exactly the result that was obtained previously in Equation 2.76. Using the result obtained in Equation 2.73 for $|\phi^+\rangle$ and Equation 2.192, the complete form of the $\chi$-parameter is achieved:

$$\begin{aligned} \chi^\epsilon(\omega) = &(1-\epsilon)\left(3\cos\omega - \cos(3\omega)\right) + \\ &+ \epsilon\left(\frac{1}{2}(4\cos(\omega) - \cos(3\omega) + \cos(5\omega))\right). \end{aligned} \tag{2.193}$$

The time delay $T$ can be connected to the length difference ($\Delta L$) between the two optical path $|0\rangle$ and $|1\rangle$. Therefore, it is possible to provide the $\epsilon$ also as a function of $\Delta L$

$$\epsilon(\Delta L) = 1 - e^{-(\Delta L)^2/l_c^2}, \tag{2.194}$$

where $l_c$ is the coherence length of the source of photons. Now, for $\Delta L = 0$, $\epsilon = 0$ and the coherence is preserved, while for $\Delta L > 0$ the coherence starts to decrease till being totally lost ($\epsilon = 1$) for $\Delta L \gg l_c$. Note that the previous discussion about the coherence length can be generalized also to the case where the non-idealities of the optical setup reduce the visibility of the four detected signals. In this situation, the state $\rho^\epsilon$ has to be replaced with $\rho^\epsilon_{\text{eff}}$, defined as:

$$\rho^\epsilon_{\text{eff}} = \eta\rho^\epsilon + (1-\eta)\frac{I_4}{4}, \tag{2.195}$$

where $\eta \in [0, 1]$ is the visibility parameter introduced in Equation 2.81. In this situation, the correlation function $\chi$ results to be

$$\chi^\epsilon_{\text{eff}}(\omega) = \eta\chi^\epsilon(\omega). \tag{2.196}$$

### 2.7.5 Not-ideal detectors

In the previous sections, it has been shown that the building blocks of the correlation function $\chi(\phi_0, \phi_1, \theta_0, \theta_1)$ are the probabilities $\{\mathbb{P}(x, y|\rho, \phi, \theta)\}_{(x,y)}$ and experimentally these are obtained as reported in Equation 2.78. In Equation 2.78 it is implicitly assumed that the detectors can reveal each photon arriving to the detection stage. However, detectors have always not unitary detection efficiencies in real experimental implementations. Even though efficiencies > 90% have been reported for the Superconducting Nanowire Single Photon Detectors (SNSPDs), these devices are particularly expensive and technological demanding due to their working temperature (~ few kelvin)[49] . On the other hand, SPADs are less efficient (< 80%) but are cheaper and easier to be used. The detection efficiencies $\{\eta_{(x,y)}\}$ of the detectors must be considered for the estimation of $\mathbb{P}(x, y|\rho, \phi, \theta)$. The raw probabilities obtained experimentally by the detectors $\hat{\mathbb{P}}(x, y|\rho, \phi^*, \theta^*)$ with a fixed $(\phi^*, \theta^*)$, can be written as:

[49]: Holzman et al. (2019), 'Superconducting Nanowires for Single-Photon Detection: Progress, Challenges, and Opportunities'

$$\hat{\mathbb{P}}(x, y|\rho, \phi^*, \theta^*) = \frac{\hat{N}_{(x,y)}(\phi^*, \theta^*)}{\sum_{x,y} \hat{N}_{(x,y)}(\phi^*, \theta^*)}. \tag{2.197}$$

where $\hat{N}_{(x,y)}(\phi^*, \theta^*)$ are the effective number of photons detected by the detector $(x, y)$. The probabilities $\{\hat{\mathbb{P}}\}$ are the estimators for the probabilities $\{\tilde{\mathbb{P}}\}$, which are connected to the probabilities $\{\mathbb{P}\}$ by the efficiencies of the single detectors $\{\eta_{(x,y)}\}$:

$$\tilde{\mathbb{P}}(x, y|\rho, \phi^*, \theta^*) = \frac{\eta_{(x,y)}\mathbb{P}(x, y|\rho, \phi^*, \theta^*)}{\sum_{x,y} \eta_{(x,y)}\mathbb{P}(x, y|\rho, \phi^*, \theta^*)}. \tag{2.198}$$

By solving the following system for the probabilities $\{\mathbb{P}(x, y|\rho, \phi^*, \theta^*)\}$:

$$\begin{cases} \tilde{\mathbb{P}}(1,1|\rho,\phi^*,\theta^*) = \frac{\eta_{(1,1)}\mathbb{P}(1,1|\rho,\phi^*,\theta^*)}{\sum_{x,y}\eta_{(x,y)}\mathbb{P}(x,y|\rho,\phi^*,\theta^*)} \\ \tilde{\mathbb{P}}(1,-1|\rho,\phi^*,\theta^*) = \frac{\eta_{(1,-1)}\mathbb{P}(1,-1|\rho,\phi^*,\theta^*)}{\sum_{x,y}\eta_{(x,y)}\mathbb{P}(x,y|\rho,\phi^*,\theta^*)} \\ \tilde{\mathbb{P}}(-1,1|\rho,\phi^*,\theta^*) = \frac{\eta_{(-1,1)}\mathbb{P}(-1,1|\rho,\phi^*,\theta^*)}{\sum_{x,y}\eta_{(x,y)}\mathbb{P}(x,y|\rho,\phi^*,\theta^*)} \\ \tilde{\mathbb{P}}(-1,-1|\rho,\phi^*,\theta^*) = \frac{\eta_{(-1,-1)}\mathbb{P}(-1,-1|\rho,\phi^*,\theta^*)}{\sum_{x,y}\eta_{(x,y)}\mathbb{P}(x,y|\rho,\phi^*,\theta^*)} \end{cases}, \tag{2.199}$$

it is possible to obtain the actual probabilities that enter in the estimation of $\chi(\phi_0, \phi_1, \theta_0, \theta_1)$. Note that, if the efficiency $\{\eta_{(x,y)}\}$ are artificially equalized, i.e., $\eta_{(1,1)} = \eta_{(1,-1)} = \eta_{(-1,1)} = \eta_{(-1,-1)}$, they cancel out and the resolution of the system is simply $\tilde{\mathbb{P}}(x, y|\rho, \phi^*, \theta^*) = \mathbb{P}(x, y|\rho, \phi^*, \theta^*)$. In this situation, the raw experimental probabilities $\{\hat{\mathbb{P}}\}$ can be used to directly estimate the probabilities $\{\mathbb{P}\}$. However, to perform the previous simplification, one must invoke a rather simple but important assumption: the fair sampling assumption. This assumption states that the detected fraction of photons revealed by the detectors is a faithful representation of the entire amount of photons involved, or equivalently, that the losses do not depend on the measurement conditions, i.e., $\eta_{(x,y,\phi,\theta)} = \eta_{(x,y)}$[16, 50] . Even if it seems pretty reasonable in the case of losses due to a not unitary detection efficiency, in principle, it is necessary to exclude that those are not selectively controlled to emulate the observed quantum correlations. This discussion enables the introduction of another loophole: the detection loophole. This loophole is strictly connected to the fair sampling assumption: if the detected photons are not a faithful sample of the entire sequence, then it is possible to artificially mimic a BI violation even with non-entangled photons.

[16]: Clauser et al. (1969), 'Proposed experiment to test local hidden-variable theories'

[50]: Pearle (1970), 'Hidden-Variable Example Based upon Data Rejection'

**Not random input sequence**

As pointed out in Section 2.6, for a correct estimation of the probabilities $\{\mathbb{P}(x, y|\rho, \phi, \theta)\}$ it is necessary to choose the measurement angles $(\phi, \theta)$ randomly in every round of the experiments. Such a necessity is at the heart of the free-will loophole. This loophole implies that the measurement operations, or, equivalently, the measurement outcomes can be modified based on the knowledge of a certain couple of angles $(\phi, \theta)$ used as input. This can be seen as an enhanced version of the detection loophole: while before only the detection efficiency $\eta$ must be independent of the measurement setting, now the entire experimental setup can be used to fake a violation of the BI. For achieving this purpose, it is enough to change the measurement basis or the state in a deterministic way, based on the knowledge of which couple of $(\phi, \theta)$ will be used: essentially, the parameter $\lambda$, representing the hidden variables used in Equation 2.6, depends on the choice of $(\phi, \theta)$, i.e., $\lambda(\phi, \theta)$. Despite this problem, in a trusted scenario like performing the experiment in a research laboratory, it seems quite catastrophic to say that the behavior of the physical system depends on the choice of the observables to measure. For this reason, using a predefined sequence of $(\phi, \theta)$ can be suitable, under the assumption that the setup is not malicious. In this situation, it can be even easier to adopt a systematic approach:

- fix one $(\phi^*, \theta^*)$;
- acquire a large amount of detection events;

- estimate all the four probabilities $\{\mathbb{P}(x, y|\rho, \phi^*, \theta^*)\}_{(x=\pm1,y=\pm1)}$;
- repeat the previous points for all four couples of angles.

This simplifies the experimental implementation since there is no need to switch the measurement basis repeatedly, but only to change them four times. Moreover, the detectors have to acquire the time sequence of the detection events and no random sequence is required at the beginning of the experiment.

However, such a simplification comes at the price of introducing correlations between the different outcomes. Indeed, SPADs present other non-idealities in addition to the not unitary detection efficiency. These are the dead time, the afterpulsing and the Dark count rate (DCR). The dead time is the time $T_d$ in which the SPAD, after having detected a photon, is unable to reveal any other photon. The afterpulsing, instead, is the possibility of triggering a false detection event after the arrival of a photon. Lastly, the DCR is the presence of a rate of fake detection events, essentially a noise, even without any light illumination. For a physical explanation of these non-idealities, see [43] . These non-idealities introduce memory effects that modify the sequence of the detection events. Consequently, the $\{\mathbb{P}(x, y|\rho, \phi^*, \theta^*)\}$ cannot be estimated by simply observing the empirical frequencies since the events in the time sequence are no longer independent and identically distributed. This is called the memory loophole. To cope with this fact, a Markov model is developed to estimate the different probabilities $\{\mathbb{P}(x, y|\rho, \phi^*, \theta^*)\}$ in the case of such memory effects. The model is based on the following assumptions[14] :

- the provider of the detectors is considered trusted and the parameters of the detectors are fixed and characterized. Moreover they are similar for all the detectors involved;
- the effective intensity of the flux of photons is $\lambda_e = \eta\lambda$, where $\eta$ is the efficiency of the detectors and $\lambda$ is the real intensity of the beam.
- the probability of afterpulsing, $p_a$, is assumed to be of the order of $10^{-2}$ or less;
- the probability that $n$ photons arrive on the detector during the dead time $T_d$ is $\mathbb{P}(N(T_d) = 1)$ and it is assumed to be of the order of $\epsilon \simeq 10^{-2}$ or less. In the case of an attenuated laser $\mathbb{P}(N(T_d) = 1) = \lambda_e T_d e^{-\lambda_e T_d} \sim \lambda_e T_d$ and $\mathbb{P}(N(T_d) > 1) = 1 - e^{-\lambda_e T_d} - \lambda_e T_d e^{-\lambda_e T_d}$. If the mean value $\lambda_e T_d$ of $N(T_d)$ is of order $10^{-2}$, then $\mathbb{P}(N(T_d) = 1) \sim \lambda_e T_d$ and $\mathbb{P}(N(T_d) > 1) \sim (\lambda_e T_d)^2/2 = o(\lambda_e T_d)$;
- the timing of afterpulsing and dead time are of the same order $T_a \sim CT_d$ with $C = O(1)$ and, correspondingly, $\mathbb{P}(N(T_a) = 1) = O(\epsilon)$ and $\mathbb{P}(N(T_a) > 1) = o(\epsilon)$.

Consider the sequence $\{\xi_n\}_{n\geq1}$ of random variables with 4 possible outcomes $i = 1, 2, 3, 4$[15] corresponding to the time sequence of the outcomes produced by the four detectors during the measurement operation. Initially, it is helpful to assume that the DCRgives a negligible contribution. If the first detected photon is taken under consideration, since the real SPADs are neither in the dead time condition nor an afterpulsing can appear, the first variable $\xi_1$ has the same distribution of $\xi_1^{\text{ideal}}$, which is the time sequence of the outcomes produced by four detectors with negligible DCR, afterpulsing and dead time, i.e., $\mathbb{P}(\xi_1 =$

[43]: Ceccarelli et al. (2021), 'Recent Advances and Future Perspectives of Single-Photon Avalanche Diodes for Quantum Photonics Applications'

[14] In the following discussion, the notation $A = O(\omega)$ indicates that A is of the same order of magnitude of $\omega$, while $A = o(\omega)$ means that $A \ll \omega$.

[15] To simplify the notation, here the couple $(x = 1, y = 1)$ is identified with the outcome $i = 1$, $(1, -1)$ with $i = 2$, $(-1, 1)$ with $i = 3$ and $(-1, -1)$ with $i = 4$. In the same manner, $\mathbb{P}(x, y|\rho, \phi^*, \theta^*)$ is simplified to $p_i$.

$i) = \mathbb{P}(i), i = 1, ..., 4$. In the second detection, $\xi_2$, the memory effects have to be considered: the set of conditional probabilities $\mathbb{P}(\xi_2 = j|\xi_1 = i)$, with $i, j = 1, ..., 4$ that describe the correlations between $\xi_1$ and $\xi_2$ can be written as:

$$\begin{aligned}\mathbb{P}(\xi_2 = j|\xi_1 = i) =&\mathbb{P}(\xi_2 = j|\xi_1 = i \cap AFP)p_a+\\&+ \mathbb{P}(\xi_2 = j|\xi_1 = i \cap AFP^c)(1-p_a),\end{aligned} \tag{2.200}$$

where the afterpulsing event is called $AFP$ and $AFP^c$ is the complementary event. Denoted by $\tau$ the interarrival time between the first and the second photon, the first term $\mathbb{P}(\xi_2 = j|\xi_1 = i \cap AFP)$ can be expressed as:

$$\begin{aligned}&\mathbb{P}(\xi_2 = j|\xi_1 = i \cap AFP) =\\&=\mathbb{P}(\xi_2 = j|\xi_1 = i \cap AFP \cap \tau < T_a)\mathbb{P}(\tau < T_a|\xi_1 = i \cap AFP)+\\&\quad+ \mathbb{P}(\xi_2 = j|\xi_1 = i \cap AFP \cap \tau > T_a)\mathbb{P}(\tau > T_a|\xi_1 = i \cap AFP)\\&=\mathbb{P}(\xi_2 = j|\xi_1 = i \cap AFP \cap \tau < T_a)\mathbb{P}(N(T_a) > 0)\\&\quad+ \delta_{ij}\mathbb{P}(N(T_a) = 0).\end{aligned} \tag{2.201}$$

$\mathbb{P}(\xi_2 = j|\xi_1 = i \cap AFP)$ has to be multiplied by $p_a \sim 10^{-2}$, so, in the case where $\mathbb{P}(N(T_a) > 0) = O(\epsilon)$, it is possible to neglect the first term obtaining:

$$\mathbb{P}(\xi_2 = j|\xi_1 = i \cap AFP) \sim \delta_{ij}\mathbb{P}(N(T_a) = 0). \tag{2.202}$$

$\mathbb{P}(\xi_2 = j|\xi_1 = i \cap AFP^c)$ represents the probability of obtaining the result $j$ for the second measurement, having observed the result $i$ in the first measurement and no afterpulsing event occurs.

$$\begin{aligned}&\mathbb{P}(\xi_2 = j|\xi_1 = i \cap AFP^c)\\&= \sum_{k=0} \mathbb{P}(\xi_2 = j \cap N(T_d) = k|\xi_1 = i \cap AFP^c)\\&= \sum_{k=0} \mathbb{P}(\xi_2 = j|\xi_1 = i \cap AFP^c \cap N(T_d) = k)\mathbb{P}(N(T_d) = k)\\&= \mathbb{P}(\xi_2 = j|\xi_1 = i \cap AFP^c \cap N(T_d) = 0)\mathbb{P}(N(T_d) = 0)\\&+ \mathbb{P}(\xi_2 = j|\xi_1 = i \cap AFP^c \cap N(T_d) = 1)\mathbb{P}(N(T_d) = 1) + o(\epsilon)\\&= p_j(1 - \epsilon + o(\epsilon)) + q_{ij}\epsilon + o(\epsilon)\end{aligned} \tag{2.203}$$

where

$$q_{ij} = \begin{cases}\mathbb{P}(\xi_2 = j|\xi_1 = i \cap AFP^c \cap N(T_d) = 1) = p_j^2 & i = j\\ \mathbb{P}(\xi_2 = j|\xi_1 = i \cap AFP^c \cap N(T_d) = 1) = p_j + p_i p_j & i \neq j\end{cases} \tag{2.204}$$

The conditional probabilities satisfy the Markov property:

$$\begin{aligned}&\mathbb{P}(\xi_{n+1} = i_{n+1}|\xi_1 = i_1, \ldots, \xi_n = i_n) =\\&\quad= \mathbb{P}(\xi_{n+1} = i_{n+1}|\xi_n = i_n) = \mathbb{P}(\xi_2 = i_{n+1}|\xi_1 = i_n),\end{aligned} \tag{2.205}$$

under the assumption that $\epsilon$ is so small that all the terms of order $o(\epsilon)$ can be neglected. Indeed, Equation 2.205 holds if $N(T_d) \geq 2$ has a negligible probability. In this situation, the random variables sequence $\{\xi_n\}_{n\geq 1}$ is a stationary Markov chain with transition probabilities $\mathbb{P}(\xi_{n+1} = j|\xi_n = i) = P_{ij}$ given (up to term of order $o(\epsilon)$) by:

$$P_{ij} = p_a \delta_{ij} + (1 - p_a)\left((1-\epsilon)p_j + \epsilon q_{ij}\right). \tag{2.206}$$

The stochastic matrix $P$ is equal to

$$P = p_a I_{4\times4} + (1 - p_a)\left((1-\epsilon)\tilde{P} + \epsilon Q\right), \tag{2.207}$$

where

$$\tilde{P} = \begin{pmatrix} p_1 & p_2 & p_3 & p_4 \\ p_1 & p_2 & p_3 & p_4 \\ p_1 & p_2 & p_3 & p_4 \\ p_1 & p_2 & p_3 & p_4 \end{pmatrix} \tag{2.208}$$

and

$$Q = \begin{pmatrix} p_1^2 & p_2(1+p_1) & p_3(1+p_1) & p_4(1+p_1) \\ p_1(1+p_2) & p_2^2 & p_3(1+p_2) & p_4(1+p_2) \\ p_1(1+p_3) & p_2(1+p_3) & p_3^2 & p_4(1+p_3) \\ p_1(1+p_4) & p_2(1+p_4) & p_3(1+p_4) & p_4^2 \end{pmatrix}. \tag{2.209}$$

In the case where $\forall i, p_i > 0$, the Markov chain is irreducible. By exploiting the ergodic theorem, the empirical frequencies converge to the unique invariant distributions $\{f_i\}_{i=1,\ldots 4}$. In particular, by introducing $N_n^i := \sum_{k=1}^n 1_{\xi_k = i}$,

$$\mathbb{P}\left(\lim_{n\to\infty} \frac{N_n^i}{n} - f_i = 0\right) = 1 \tag{2.210}$$

where $(f_1, f_2, f_3, f_4)$ are the left eigenvector of the matrix $P$ with eigenvalue 1. The distributions $\{f_i\}$ can be written as:

$$f_i = \frac{p_i}{1+\epsilon p_i}\left(\sum_{j=1}^{4} \frac{p_j}{1+\epsilon p_j}\right)^{-1} \sim p_i + \epsilon\, p_i(\sum_j p_j^2 - p_i). \tag{2.211}$$

Inverting the previous relation and ignoring terms of order $o(\epsilon)$, it is possible to obtain:

$$p_i \sim f_i\left(1 + \epsilon\left(f_i + \sum_{j=1}^{4} f_j^2\right)\right). \tag{2.212}$$

Equation 2.212 represents a rough estimator of the theoretical probabilities $\{p_i\}$ as a function of the empirical frequencies $\{f_i\}$. A more precise estimator can be obtained by exploiting the maximum likelihood principle. Given a sequence of outcomes $\{x_i\}_{i=1,\ldots,n}$, with $x_i = 1, 2, 3, 4$, described by the Markov chain previously introduced, its probability can be computed as:

$$p_{x_1} \prod_{i=1}^{n-1} P_{x_i x_{i+1}} \tag{2.213}$$

and the corresponding log-likelihood is equal to

$$l(P) := \log(p_{x_1} \prod_{i=1}^{n-1} P_{x_i x_{i+1}}) \tag{2.214}$$

$$= \log(p_{x_1}) + \sum_{i,j=1,2,3,4} N_{ij} \log(P_{ij}), \tag{2.215}$$

where $N_{ij}$ represents the number of transitions from $i$ to $j$. The parameter $\{\hat{p}_i\}$ that maximize Equation 2.215 under the constrains $\sum_j P_{ij} = 1$, $i = 1, \dots, 4$ are actually the unbiased estimator of the theoretical probabilities $\{p_i\}^{16}$ .

Up to now, the presence of the DCR has been consider negligible. In the case where this hypothesis is not true, the distribution of the initial random variables $\xi_n$

$$\mathbb{P}(\xi_n = i) = p_i, \qquad i = 1, 2, 3, 4, \tag{2.216}$$

has to be replaced by the corrected one

$$\mathbb{P}(\xi_n = i) = \tilde{p}_i = (1 - p_{\text{DCR}})p_i + \frac{p_{\text{DCR}}}{4}, \qquad i = 1, 2, 3, 4, \tag{2.217}$$

where $p_{\text{DCR}}$ represents the total fraction of detected photons due to the DCR.

## 2.8 Experimental validation

The experimental result here presented are reported in [23] .

### 2.8.1 The experimental setup

To validate the presented theory, an experiment is set up. The whole experimental setup is reported in Figure 2.14a, while the details of the optical setup are reported in Figure 2.14b. Three sources of light are used as input:

- a single-mode green HeNe laser, with nominal power of 5 mW and center wavelength 541 nm. The laser is fiber-coupled and attenuated by a variable optical attenuator (VOA).
- a commercial through-hole 5 mm LED emitting at 517 nm with a spectral width of 30 nm. The light is filtered using an Interference filter (IF) centered at 531 nm with a bandwidth of 1 nm.
- a Halogen lamp, model: HL-2000-FHSA-LL from Ocean Optics with a broad spectrum (360 − 2400 nm). The light is filtered using the same IF of the LED.

The sources are fiber-coupled to a single-mode visible optical fiber and injected into the optical setup by using a Collimator (C). As detailed in Section 2.4, the SPE state is first generated using the different optical elements reported in red in Figure 2.14b. The relative phase shift $\xi$, used to compensate for any phase difference between the two paths, is controlled by moving the MR using a Piezoelectric transducer (PZT). The MZI and the two HWPs used to rotate the two DoFs are reported in orange in

[16] The theory is reported in [51, 52]

[23]: Pasini et al. (2020), 'Bell-inequality violation by entangled single-photon states generated from a laser, an LED, or a halogen lamp'

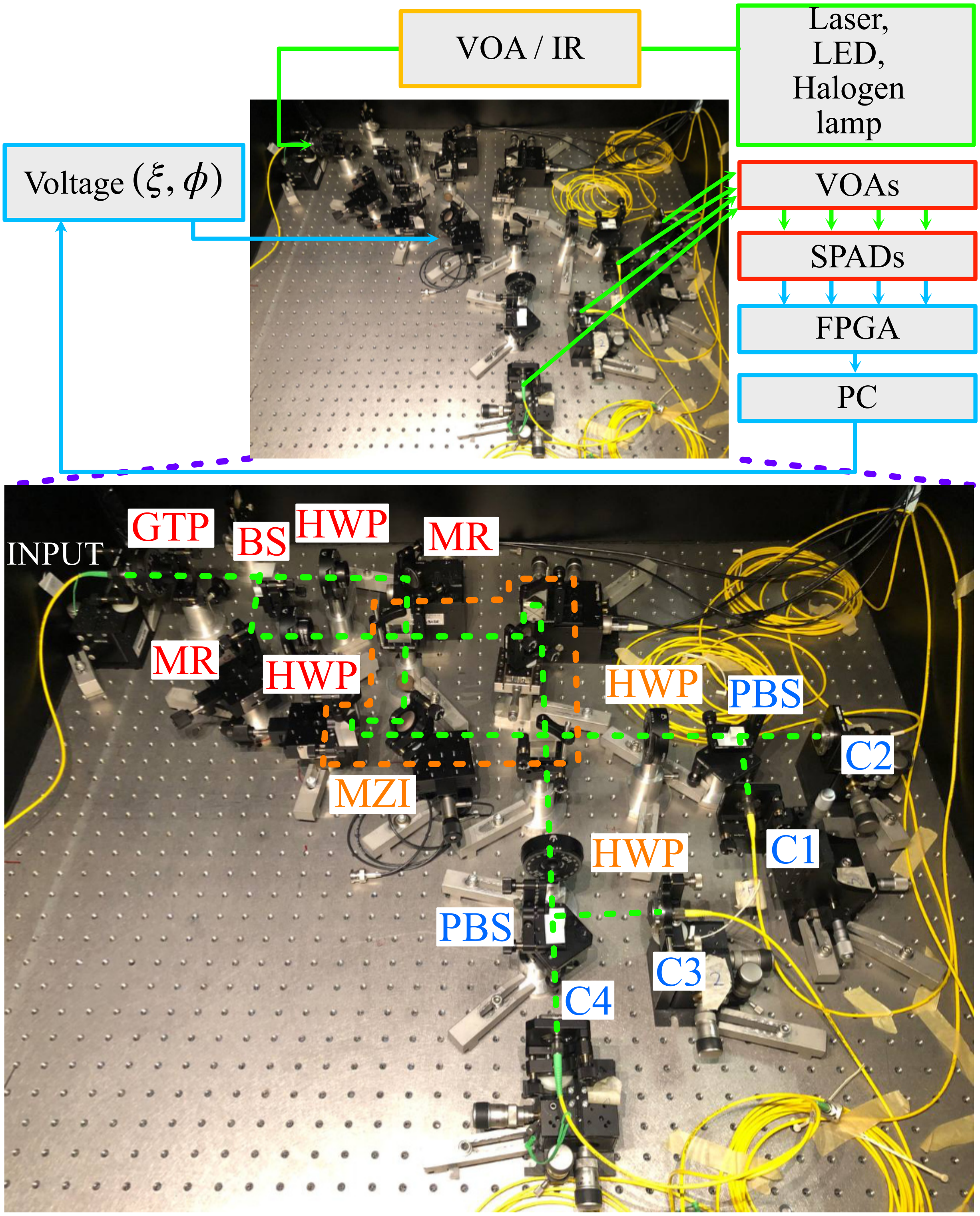


**Figure 2.14:** a) Experimental setup used to demonstrate violation of BI. With a green arrow is indicated the optical signal, while with a cyan arrow is reported the electrical signal. Color code of the boxes: green, source, orange, optical components used to prepare the light before the injection into the optical setup (VOA or IF), red, detection elements (VOAs and SPADs), cyan, electrical components used to control the phases $\xi$ and $\phi$ and to store the data obtained (PC and Field programmable gate array (FPGA)). b) Details of the optical bulk setup. Color code: white, input port of the setup, red, generation stage, orange, rotation stage and blu, detection stage. The fiber couplers $\{\text{Collimators (Cs)i}\}_{i=1..4}$ are used to couple the photons inside the fibers connected to the SPADs.

Figure 2.14b. The phase $\phi$ that induces the rotation on the momentum is controlled electronically by using another PZT. The single photons are detected in the detection stage, whose optical elements are reported in blue in Figure 2.14b. The different fiber couplers C$i$ are used to couple the photons to four long (> 1 m) optical fibers, which are connected at the other end to four Si-SPADs. Such long fibers are employed to avoid correlations between the detections observed by the different SPADs. The detection events collected by the SPADs are stored in a PC by using a Field programmable gate array (FPGA). Since the four SPADs have different efficiencies, these are equalized by varying the fiber-coupling of the signal to each detector by using VOAs. The dead time of the SPADs is of the order of 20 ns, while the afterpulsing probability is of the order of 0.5%. The DCR of the SPADs is < 1.5 kHz. These characteristics imply a linear dynamic range for count rates lower than 1 MHz. The use of fluxes of photons <= 0.5 MHz is a safe choice to avoid the loss of real counts due to the detectors' imperfections. To reduce the noise on the phase $\phi$ of MZI, the setup is shielded using a black box. Note that the sources and the detectors are not shielded. The working wavelength is chosen for practical purposes:

- performances of the optical components,
- price of the optical components,
- possibility of using Si-SPADs, which have less imperfections (DCR and efficiency) compared to 1.5 $\mu$m-SPADs,
- easy alignment (eye-visible light).

The estimation of the $\chi$-parameter in the case of the attenuated laser is done by acquiring all the four signals, while, in the case of the LED and the Halogen lamp, only the projections over $|0H\rangle$ and $|0V\rangle$ are considered. The others are constructed using symmetry arguments, as done in [34] . For the case of the attenuated laser, the average flux of photon is set to be $\simeq$ 40 KHz, considering the sum of counts recorded by four SPADs, while for the LED and the Halogen lamp $\simeq$ 10 KHz, considering now the sum of only two SPADs. The difference is justified by the difficulty of coupling a considerable amount of light from LED and the Halogen lamp in the optical setup due to the non-directionality of these sources. The measurements are performed by setting an angle $\theta_i$ on the two HWPs and by performing a sweep of the angle $\phi$. This is done by varying the voltage $V$ applied to the PZT, which controls the phase $\phi$ of the MZI. The relation $\phi(V)$ is fitted in post-processing. Experimentally, the measured data are the empirical frequencies $N_{(x,y)}(\phi, \theta)/N(\phi, \theta)$, which allow to build the probabilities $\mathbb{P}(x, y|\rho, \phi, \theta)$ as reported in Equation 2.78. Note that the fair sampling assumption is introduced, while the Markov correction to the $\mathbb{P}(x, y|\rho, \phi, \theta)$ is assumed to be negligible. A justification of the latter assumption will be provided in Chapter 3. The polarization dependence of the optical components has to be considered in the estimation of the $\mathbb{P}(x, y|\rho, \phi, \theta)$. Here the numerical evaluation is considered, since it provides the tighter bounds $e_{\mathbb{P}}$ and $e_{\chi}$. To compute them, in Table 2.1 are reported the measured power transmission coefficients associated to the different momenta necessary to model the state $\rho$ that enters in the MZI. For the MZI, in Table 2.2 there are reported the power reflection and transmission coefficients of its BSs. To facilitate the optical alignment, the two DLs in the MZI of Figure 2.3 are actually composed of a series of three MRs, as shown in Figure 2.15. In Table 2.3 are reported the corresponding

[34]: Gadway et al. (2009), 'Bell-inequality violations with single photons entangled in momentum and polarization'

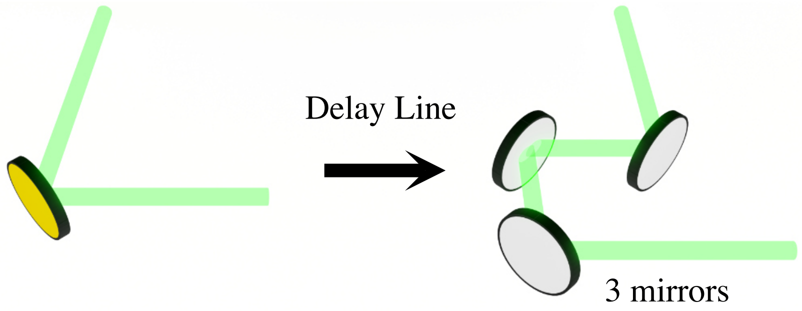


**Figure 2.15:** Details of the DL. It is composed of three mirrors for optical alignment purposes. Reprinted figure with permission from Nicolò Leone, Stefano Azzini, Sonia Mazzucchi, Valter Moretti, and Lorenzo Pavesi, "Certified Quantum Random-Number Generator Based on Single-Photon Entanglement", Physical Review Applied 17, 034011. Copyright 2022 by the American Physical Society.

**Table 2.1:** Power transmission coefficients for each momentum $|0\rangle$ and $|1\rangle$ in the generation stage. The coefficients are measured at 543.5 nm. The standard deviation is obtained by repeated measurements. Reprinted table with permission from Nicolò Leone, Stefano Azzini, Sonia Mazzucchi, Valter Moretti, and Lorenzo Pavesi, "Certified Quantum Random-Number Generator Based on Single-Photon Entanglement", Physical Review Applied 17, 034011. Copyright 2022 by the American Physical Society.

| | |
|---|---|
| $\lvert t_0\rvert^2$ | $0.421 \pm 0.002$ |
| $\lvert t_1\rvert^2$ | $0.456 \pm 0.001$ |

power transmission coefficients. Note that the previous values are not precisely measured at the central wavelength of the filter in the case of LED and halogen lamp. However, due to the weak spectral dependence of the parameters, as reported by the website of the constructor[53] , the differences between the coefficients at 531 nm and the ones at 543.5 nm are effectively negligible.

[53]: Thorlabs (2021), *Thorlabs Non-Polarizing Cube Beamsplitters (400 - 700 nm)*

By exploiting the MultiStart solver in the Global Optimization Toolbox of Matlab(c), using the standard SQP algorithm, the values of

$$e_{\mathbb{P}} = 0.066 \pm 0.002$$

and

$$e_{\chi} = 0.0026 \pm 0.0007$$

are obtained. To verify the correctness of the result, the optimization is performed starting from several initial points: $3 \times 10^3$ random initial points are chosen for $e_{\mathbb{P}}$, while $10^4$ for $e_{\chi}$. Respectively, the errors are estimated by considering normal distributions of the transmission and reflection coefficients of the different optical elements having as mean

**Table 2.2:** Power transmission and reflection coefficients for the two BSs in MZI for each polarization. The measurements were done at 543.5 nm for the two incident light polarizations (V vertical, H horizontal) and the standard deviation is obtained by repeated measurements. Reprinted figure with permission from Nicolò Leone, Stefano Azzini, Sonia Mazzucchi, Valter Moretti, and Lorenzo Pavesi, "Certified Quantum Random-Number Generator Based on Single-Photon Entanglement", Physical Review Applied 17, 034011. Copyright 2022 by the American Physical Society.

| | $BS_1$ | $BS_2$ |
|---|---|---|
| $\lvert t_V\rvert^2$ | $0.502 \pm 0.005$ | $0.476 \pm 0.003$ |
| $\lvert r_V\rvert^2$ | $0.423 \pm 0.003$ | $0.416 \pm 0.001$ |
| $\lvert t_H\rvert^2$ | $0.511 \pm 0.002$ | $0.4865 \pm 0.001$ |
| $\lvert r_H\rvert^2$ | $0.349 \pm 0.001$ | $0.3583 \pm 0.0007$ |

| | $\mathrm{DL}_1$ | $\mathrm{DL}_2$ |
|---|---|---|
| $\lvert\gamma_V\rvert^2$ | 0.898 ± 0.005 | 0.872 ± 0.006 |
| $\lvert\gamma_H\rvert^2$ | 0.798 ± 0.004 | 0.771 ± 0.002 |

**Table 2.3:** Power transmission and reflection coefficients for the two MRs in MZI for each polarization. The measurements were done at 543.5 nm for the two incident light polarizations (V vertical, H horizontal) and the standard deviation is obtained by repeated measurements. Reprinted figure with permission from Nicolò Leone, Stefano Azzini, Sonia Mazzucchi, Valter Moretti, and Lorenzo Pavesi, "Certified Quantum Random-Number Generator Based on Single-Photon Entanglement", Physical Review Applied 17, 034011. Copyright 2022 by the American Physical Society.

and standard distribution the values reported in Table 2.2 and Table 2.3. From each of these distributions, one value is randomly extracted creating a set of parameters$\{\lambda\}_i$. With the latter set, $e_{\mathbb{P}_i}$ and $e_{\chi_i}$ are calculated using the values of $\{\phi, \theta, \rho, x, y\}$ that maximize $e_{\mathbb{P}}$ and $e_\chi$. By repeating this procedure $4 \times 10^3$ the errors are evaluated as the standard deviation of the sequences $\{e_{\mathbb{P}_i}\}$ and $\{e_{\chi_i}\}$ obtained.

## 2.8.2 Results

### Attenuated laser

First, it is considered the case in which the light from the attenuated laser is injected into the optical setup. In Figure 2.16 the experimental data point of $\chi(\theta)$ are reported as a function of the polarization angle $\theta$. A violation of the BI is witnessed in this situation. Each experimental point represents the average of different measurements and the errors are obtained by error propagation. Recalling the choice done in Equation 2.73, i.e., $(\phi = 0, \phi' = \omega, \theta = \omega/2, \theta' = 3/2\omega)$, it results that $\theta = 2\omega$ and the expression for the ideal $\chi$-parameter becomes:

$$\chi(\theta) = (3\cos(2\theta) - \cos(6\theta)) \,. \tag{2.218}$$

In the real case, when the mean visibility $\eta$ and the coherence parameter $\epsilon$ are considered, the $\chi$-parameter is:

$$\begin{aligned}\chi^{\epsilon}_{\text{eff}}(\theta) = \eta\chi^{\epsilon}(\theta) =& \eta(1-\epsilon)\,(3\cos(2\theta) - \cos(6\theta)) + \\ &+ \eta\epsilon\left(\frac{1}{2}(4\cos(2\theta) - \cos(6\theta) + \cos(10\theta))\right) .\end{aligned} \tag{2.219}$$

Actually Equation 2.219 for $\epsilon = 0$ and $\eta = 0.95 \pm 0.01$ (dashed curve in Figure 2.16) reproduces the experimental data obtained. The obtained maximum and minimum values of the $\chi$-parameter are reported in Table 2.4. The effect of the correction $e_\chi$ is negligible compared to the experimental errors considered.

| | No Correction | Correction |
|---|---|---|
| $\chi_{\text{Max}}$ | 2.60 ± 0.08 | 2.60 ± 0.08 |
| $\chi_{\text{Min}}$ | −2.41 ± 0.07 | −2.41 ± 0.07 |

**Table 2.4:** Maximum and minimum value of $\chi(\theta)$ in the case of an attenuated laser source. The values are reported here with no correction ($e_\chi = 0$) and with the correction estimated ($e_\chi = 0.0026 \pm 0.0007$).

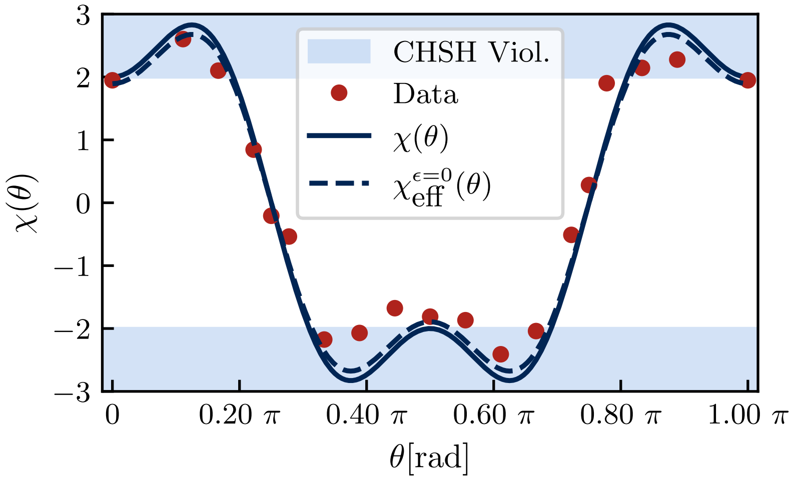


**Figure 2.16:** Evaluation of $\chi$-parameter using as a light source an attenuated laser beam in the coherent regime. The experimental data, here reported as red dots, are plotted as a function of the rotation angle $\theta$ induced by the two HWPs in the rotation stage (Figure 2.5). Note that the error bars are within the size of the red dots and not visible. Respectively, the solid and the dashed curve represent the theoretical forms of the $\chi$-parameter in the cases of Equation 2.218 and Equation 2.219 with $\eta = 0.95 \pm 0.01$ and $\epsilon = 0$. Lastly, in blue are indicated the areas in which the violation of the CHSH inequality can be achieved. A violation of the CHSH inequality is observed. Reprinted figure with permission from Matteo Pasini, Nicolò Leone, Sonia Mazzucchi, Valter Moretti, Davide Pastorello, and Lorenzo Pavesi, "Bell-inequality violation by entangled single-photon states generated from a laser, an LED, or a halogen lamp", Physical Review A 102, 063708 (2020). Copyright 2022 by the American Physical Society.

### LED and Halogen lamp

As discussed previously, SPE states can be generated by any source of light without being affected by its statistics of emission. The only concern regards the spectrum of emission of the source. Indeed, a short coherence length and, consequently, time is problematic: considering the Bell state $|\phi^+\rangle$, no violation of the BI is observable when the relative time delay $T$ between the terms $|0V\rangle$ and $|1H\rangle$ is greater than the coherence time $\tau_c$. The IF is used to increase the coherence time and length of the light. Consider the emission spectrum of the LED when the filter is not present. Under the assumption that the LED's spectrum is a gaussian of the form $f(\omega) = Ae^{-\frac{(\omega-\omega_0)^2}{2\sigma_\omega^2}}$, it is possible to obtain an estimation of its coherence time and length. In Figure 2.17, the spectrum is reported in blue while the fit is reported in red. The following parameters are obtained: $A = 0.932 \pm 0.002$, $\omega_0 = (3611.4 \pm 0.4)(2\pi \times \text{THz})$ and $\sigma_\omega = (134 \pm 9)(2\pi \times \text{THz})$. Eventually it is obtained that $\tau_c = \frac{1}{\sigma_\omega} = (7.43 \pm 0.02)$fs and $l_c = \tau_c c = (2.227 \pm 0.006)\mu$m. In this situation the optical setup of Figure 2.13 is used to measure the LED autocorrelation, which is reported in Figure 2.18 as a function of the time delay between the two optical paths. The displacement of the PZT is enough to lose the coherence of the light.

In the filtered situation, instead, the spectrum of the LED is reported in Figure 2.19. Performing the gaussian fit on the filtered spectrum, the obtained parameters are $A = (0.985 \pm 0.006)$, $\omega_0 = (3547.24 \pm 0.04)$ $(2\pi \times \text{THz})$ and $\sigma_\omega = (6.5 \pm 0.8)$ $(2\pi \times \text{THz})$. The coherence time results to be increased to $\tau_c = (154 \pm 1)$ fs and, consequently, the coherence length is $l_c = (46.0 \pm 0.3)\mu$m. Contrary to the unfiltered situation, the autocorrelation does not decrease significatively over the 20 $\mu$m range of the displacement of the PZT, as shown in Figure 2.20.

In the coherent regime, the $\chi$-parameter is reported in Figure 2.22 for the LED and in Figure 2.23 for the Halogen lamp. As in the case of the attenuated laser, a violation of the CHSH is observed with both the sources.

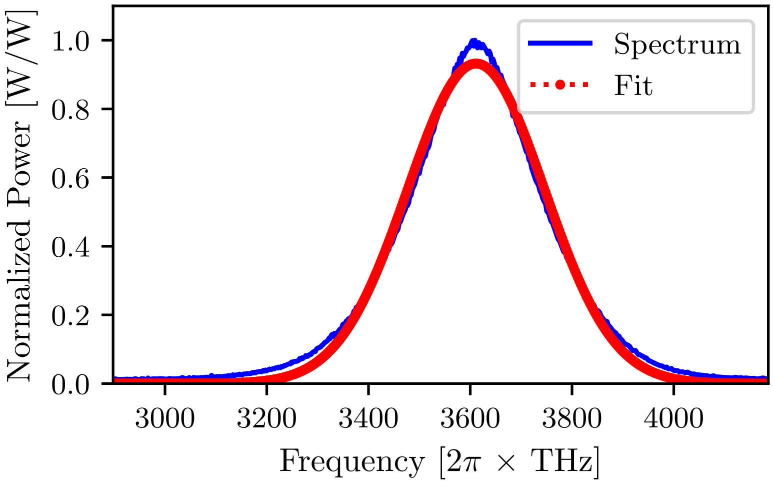


**Figure 2.17:** Spectrum of the unfiltered LED used in the experiments with the relative gaussian fit $f(\omega)$.

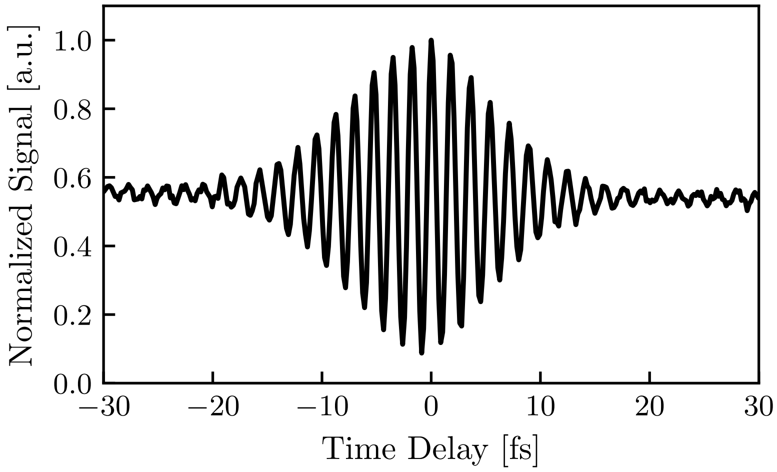


**Figure 2.18:** Autocorrelation of the unfiltered LED. It is acquired by moving the PZT by 20$\mu$m. Reprinted figure with permission from Matteo Pasini, Nicolò Leone, Sonia Mazzucchi, Valter Moretti, Davide Pastorello, and Lorenzo Pavesi, "Bell-inequality violation by entangled single-photon states generated from a laser, an LED, or a halogen lamp", Physical Review A 102, 063708 (2020). Copyright 2022 by the American Physical Society.

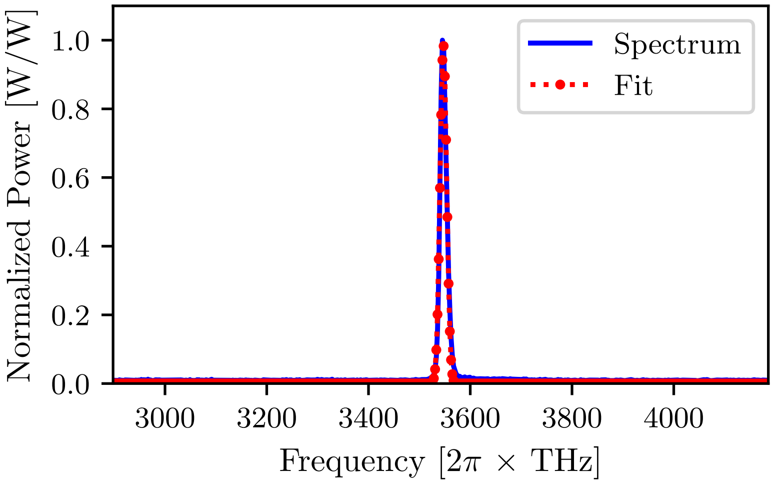


**Figure 2.19:** Spectrum of the filtered LED used in the experiments with the relative gaussian fit $f(\omega)$.

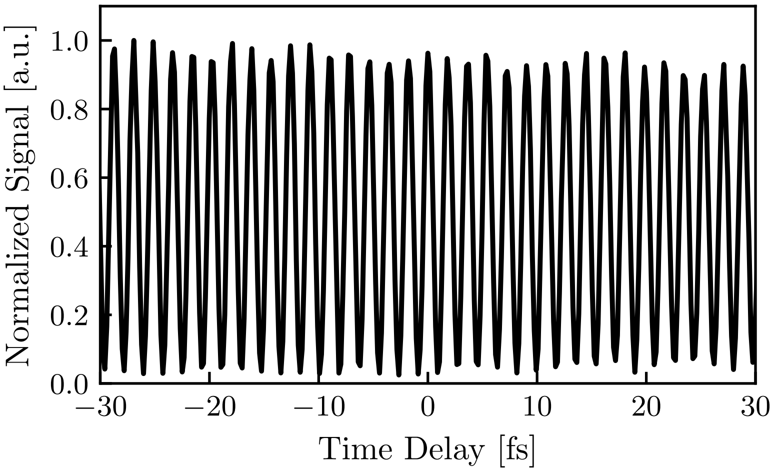


**Figure 2.20:** Autocorrelation of the filtered LED. It is acquired by moving the PZT by 20$\mu$m. Reprinted figure with permission from Matteo Pasini, Nicolò Leone, Sonia Mazzucchi, Valter Moretti, Davide Pastorello, and Lorenzo Pavesi, "Bell-inequality violation by entangled single-photon states generated from a laser, an LED, or a halogen lamp", Physical Review A 102, 063708 (2020). Copyright 2022 by the American Physical Society.

The maximum and minimum values for both sources are reported in Table 2.5. As in the laser case, the correction $e_\chi$ is negligible compared to the experimental errors considered. Moreover, the normalized signal for the $|0H\rangle$-channel is reported in Figure 2.21, where the visibility of the interference fringes is constant for every value of $\theta$.

**Table 2.5:** Maximum and minimum value of $\chi(\theta)$ in the case of the LED and halogen lamp sources. The values are reported here with no correction ($e_\chi = 0$) and with the correction estimated ($e_\chi = 0.0026 \pm 0.0007$).

| | No Correction | Correction |
|---|---|---|
| $\chi_{\text{Max, LED}}$ | 2.69 ± 0.06 | 2.69 ± 0.06 |
| $\chi_{\text{Min, LED}}$ | −2.51 ± 0.07 | −2.51 ± 0.07 |
| $\chi_{\text{Max, Lamp}}$ | 2.72 ± 0.06 | 2.72 ± 0.06 |
| $\chi_{\text{Min, Lamp}}$ | −2.45 ± 0.07 | −2.45 ± 0.06 |

In the case of the LED, a further measurement of the $\chi$-parameter is performed in the incoherent regime ( Figure 2.24 and Figure 2.25) by introducing a path difference $\Delta L$ between the $|0\rangle$ path and the $|1\rangle$ path in the generation stage of Figure 2.3, such as $\Delta L \gg l_c$. The result is reported in Figure 2.24, where no violation is witnessed. The experimental data points are in agreement with the theoretical prediction of $\chi^{\epsilon}_{\text{eff}}$ in the case of $\epsilon = 1$, i.e., when the coherence is lost. In this situation the visibility of the $|0H\rangle$-channel is a function of $\theta$ and approaches 0 for $\theta \approx \frac{\pi}{4}$, as shown in Figure 2.25.

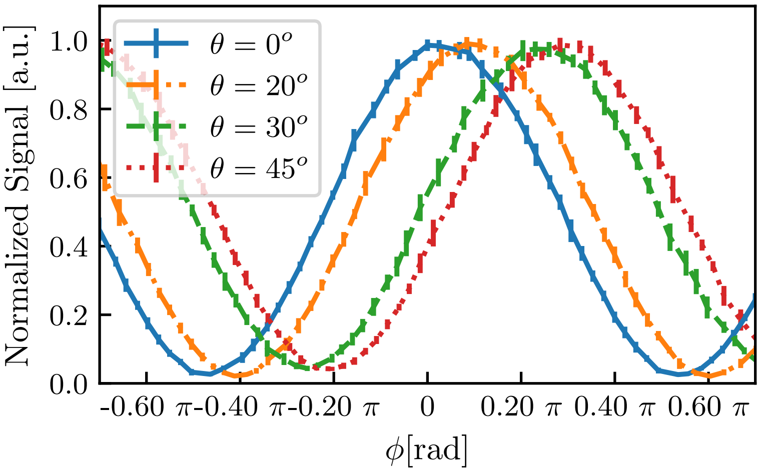


**Figure 2.21:** Normalized signal acquired by one single SPAD ($N_{OH}^{(\phi,\theta)}$) as a function of $\phi$ for different polarization angles $\theta$ in the coherent case. The counts are normalized with respect to their maximum value. Reprinted figure with permission from Matteo Pasini, Nicolò Leone, Sonia Mazzucchi, Valter Moretti, Davide Pastorello, and Lorenzo Pavesi, "Bell-inequality violation by entangled single-photon states generated from a laser, an LED, or a halogen lamp", Physical Review A 102, 063708 (2020). Copyright 2022 by the American Physical Society.

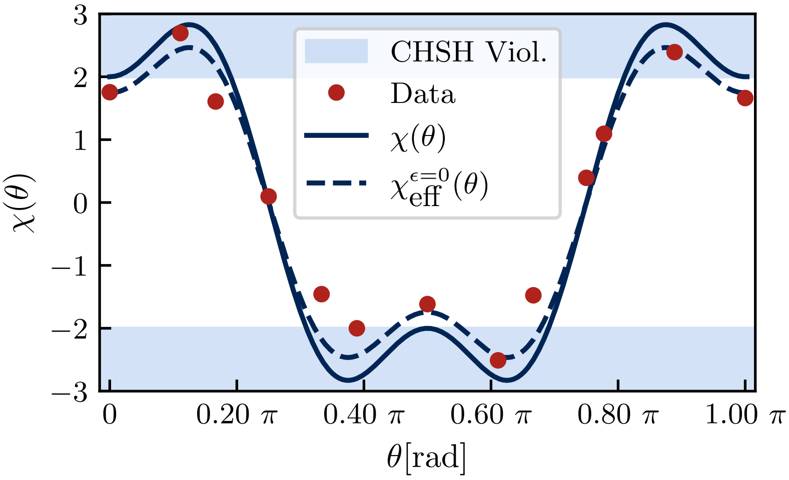


**Figure 2.22:** Evaluation of $\chi$-parameter using as light source a 1 nm filtered LED in the coherent regime. The experimental data, here reported as red dots, are plotted as a function of the rotation angle $\theta$ induced by the two HWPs in the rotation stage (Figure 2.5). Note that the error bars are within the size of the red dots and not visible. Respectively, the solid and the dashed curve represent the theoretical forms of the $\chi$-parameter in the cases of Equation 2.218 and Equation 2.219 with $\eta = 0.87 \pm 0.02$ and $\epsilon = 0$. Lastly, in blue are indicated the areas in which the violation of the CHSH inequality is observable. A violation of the CHSH inequality is observed. Reprinted figure with permission from Matteo Pasini, Nicolò Leone, Sonia Mazzucchi, Valter Moretti, Davide Pastorello, and Lorenzo Pavesi, "Bell-inequality violation by entangled single-photon states generated from a laser, an LED, or a halogen lamp", Physical Review A 102, 063708 (2020). Copyright 2022 by the American Physical Society.

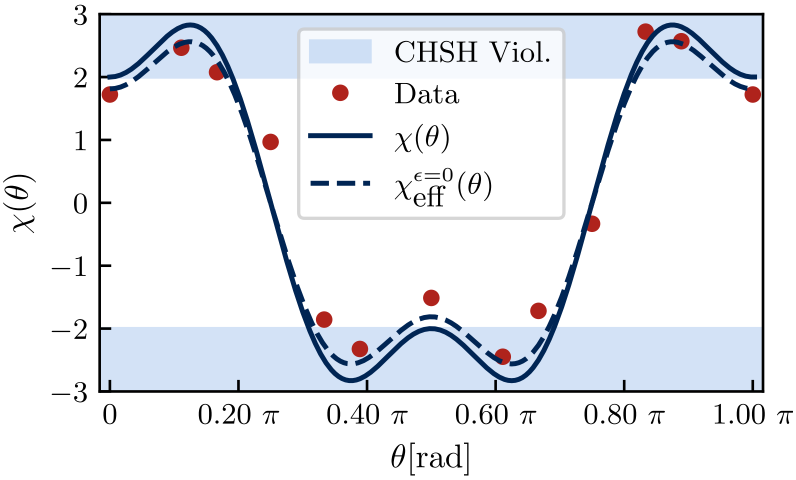


**Figure 2.23:** Evaluation of $\chi$-parameter using as light source a 1 nm filtered halogen lamp in the coherent regime. The experimental data, here reported as red dots, are plotted as a function of the rotation angle $\theta$ induced by the two HWPs in the rotation stage (Figure 2.5). Note that the error bars are within the size of the red dots and not visible. Respectively, the solid and the dashed curve represent the theoretical forms of the $\chi$-parameter in the cases of Equation 2.218 and Equation 2.219 with $\eta = 0.91 \pm 0.01$ and $\epsilon = 0$. Lastly, in blue are indicated the areas in which the violation of the CHSH inequality is observable. A violation of the CHSH inequality is observed. Reprinted figure with permission from Matteo Pasini, Nicolò Leone, Sonia Mazzucchi, Valter Moretti, Davide Pastorello, and Lorenzo Pavesi, "Bell-inequality violation by entangled single-photon states generated from a laser, an LED, or a halogen lamp", Physical Review A 102, 063708 (2020). Copyright 2022 by the American Physical Society.

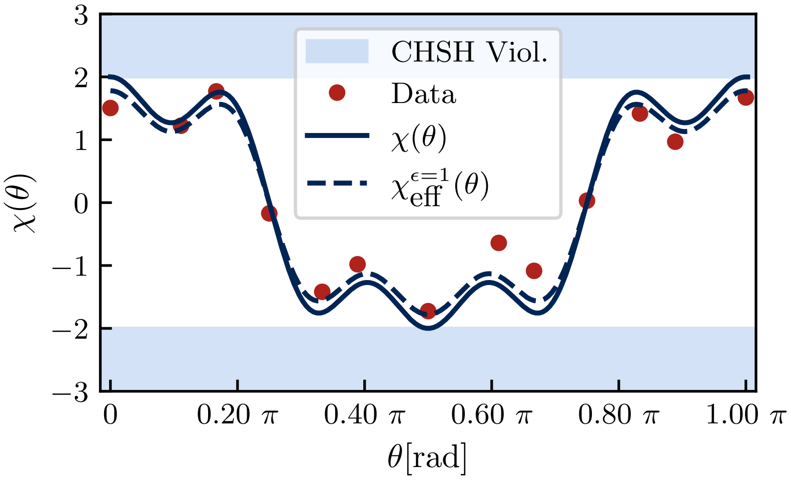


**Figure 2.24:** Evaluation of $\chi$-parameter using as light source a 1 nm filtered LED in the incoherent regime. The experimental data, here reported as red dots, are plotted as a function of the rotation angle $\theta$ induced by the two HWPs in the rotation stage (Figure 2.5). Note that the error bars are within the size of the red dots and not visible. Respectively, the solid and the dashed curve represent the theoretical forms of the $\chi$-parameter in the cases of Equation 2.218 and Equation 2.219 with $\eta = 0.89 \pm 0.01$ and $\epsilon = 1$. Lastly, in blue are indicated the areas in which the violation of the CHSH inequality is observable. A violation of the CHSH inequality is not observed. Reprinted figure with permission from Matteo Pasini, Nicolò Leone, Sonia Mazzucchi, Valter Moretti, Davide Pastorello, and Lorenzo Pavesi, "Bell-inequality violation by entangled single-photon states generated from a laser, an LED, or a halogen lamp", Physical Review A 102, 063708 (2020). Copyright 2022 by the American Physical Society.

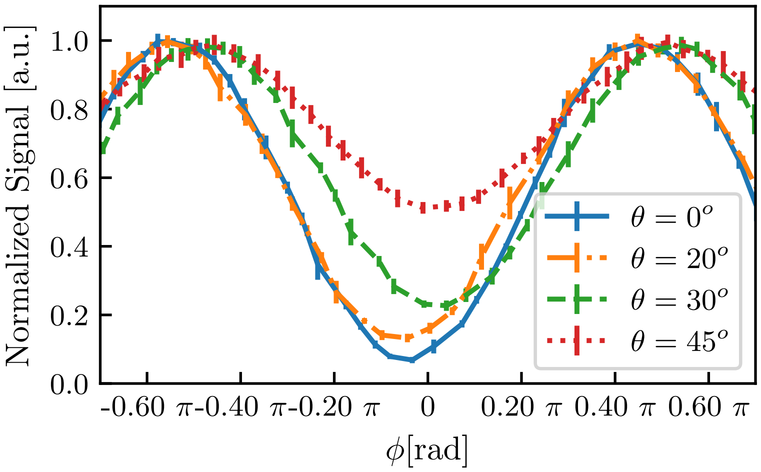


**Figure 2.25:** Normalized signal acquired by one single SPAD ($N_{OH}^{(\phi,\theta)}$) as a function of $\phi$ for different polarization angles $\theta$ in the incoherent case. The counts are normalized respect to their maximum value. Reprinted figure with permission from Matteo Pasini, Nicolò Leone, Sonia Mazzucchi, Valter Moretti, Davide Pastorello, and Lorenzo Pavesi, "Bell-inequality violation by entangled single-photon states generated from a laser, an LED, or a halogen lamp", Physical Review A 102, 063708 (2020). Copyright 2022 by the American Physical Society.

## 2.9 Quantum signature

In this section, the SPE is discussed respect to *classical entanglement*[54] . To introduce the concept of classical entanglement, it is necessary to consider the electric field of a paraxial beam with propagation direction $z$:

$$\mathbf{E}(\rho, z) = \mathbf{e}_x f_x(\rho, z) + \mathbf{e}_y f_y(\rho, z)\,. \tag{2.220}$$

In Equation 2.220, the unit vectors $\mathbf{e}_x, \mathbf{e}_y$ express the polarizations, the scalar functions $f_x, f_y$ describe the wavefronts and $\rho = x\mathbf{e}_x + y\mathbf{e}_y$ defines the transverse position vector. The electric field $\mathbf{E}(\rho, z)$ is in the tensor product $\mathscr{H}_M \otimes \mathscr{H}_P$, where the spaces $\mathscr{H}_M$ and $\mathscr{H}_P$ are the classical ones of classical momentum and classical polarization. Analogously to the Schmidt decomposition introduced in the Section 2.1 for quantum states, the same reasoning can be applied also in this situation: by properly fixing a $\mathscr{H}_P$ basis $\{\mathbf{u}_1, \mathbf{u}_2\}$ and a $\mathscr{H}_M$ basis $\{g1, g2\}$, it is possible to write $\mathbf{E}(\rho, z)$ as:

$$\mathbf{E}(\rho, z) = \sqrt{\lambda_1}\mathbf{u}_1 g_1(\rho, z) + \sqrt{\lambda_2}\mathbf{u}_2 g_2(\rho, z). \tag{2.221}$$

Now, if only one of the Schmidt coefficients $\{\lambda_1, \lambda_2\}$, where $\lambda_i \in [0, 1]$ is different from 0, the state is considered separable, otherwise, it is considered not separable or classically entangled. Mathematically, for $\lambda_1 = \lambda_2 = 1/2$, Equation 2.221 and a maximally entangled state of two qubits are identical. Indeed, it is possible to obtain a classical version of the BI for classical entanglement. The correlation coefficient can be defined as

$$\mathbb{E}\left(O_\phi^M, O_\theta^P\right) = \frac{I_{++}^{(\phi,\theta)} + I_{--}^{(\phi,\theta)} - I_{+-}^{(\phi,\theta)} - I_{-+}^{(\phi,\theta)}}{I_{++}^{(\phi,\theta)} + I_{--}^{(\phi,\theta)} + I_{+-}^{(\phi,\theta)} + I_{-+}^{(\phi,\theta)}} \tag{2.222}$$

where $I_{\pm\pm}^{(\phi,\theta)}$ are now light intensities, and, consequently, a $\chi$-parameter with the same structure of the quantum one can be obtained. Even if a violation of this classical CHSH inequality can be obtained for a suitable choice of the angles $(\phi, \phi', \theta, \theta')$, what really changes is the meaning of such a violation. First, intensities are classical notions which can be completely described in the classical framework[55] . Second, they refer to collective behavior of the photons considered: the classical version of the CHSH inequality does not predict anything about the characteristics of the single photons that constitute the light beam, even assuming their existence. This is not true, instead, for the quantum mechanical version of the BI, where the violation rules out any (classical) realistic non contextual theory that tries to completely explain the phenomenology of the measurement operations on single photons. Indeed, as long as it is possible to access the behavior of the single constituents of light, i.e., to detect single photons, the violation of the BI is a direct evidence of quantum contextuality[56] and has to be ascribed to the properties of the single photons.

[54]: Spreeuw (1998), 'A classical analogy of entanglement'

[55]: Khrennikov (2020), 'Quantum Versus Classical Entanglement: Eliminating the Issue of Quantum Nonlocality'

[56]: Marcin Markiewicz et al. (2019), 'From contextuality of a single photon to realism of an electromagnetic wave'

# Single Photon Entanglement for Quantum Random Number Generation

# 3

A random number sequence is a succession of digits, usually 0 and 1, which are unpredictable, not correlated and uniformly distributed. These three properties are the key features that enable each application based on random numbers: cryptography, scientific simulation, gaming and lotteries. While the requirements for random numbers in computer science are to be uniformly distributed and the absence of correlations and patterns, a different level of security is necessary for gaming, lotteries and cryptography. Indeed, in these applications, the secrecy of the sequence represents an additional essential characteristic. Before moving on, it is necessary to specify the difference between unpredictable and secret: the former indicates the impossibility of predicting the digits of the sequence given any previous knowledge (except for the knowledge of the sequence itself), while the latter specifies that the sequence is not accessible to anyone except the interested parties. Note that an unpredictable sequence could be public, and, on the contrary, a secret sequence could be predicted given a certain initial knowledge. Quantum mechanics cannot certify secrecy, while it can ensure unpredictability. In other words, no one can guarantee that a random sequence can be safely used in cryptographic applications if it has been stored in a malicious PC that is sending the digits to an adversary. For this reason, in the following discussion, it is assumed that the provider of the components is a trusted person, which, however, can sell imperfect and noisy devices and that the place, in which the random sequence is generated, is a safe place in which the adversary cannot enter to install any trojan horse in the electronics. In this chapter, firstly, Quantum Random Number Generators (QRNGs) are introduced, focusing on their physical principles and structures. Then, the concept of conditional min-entropy is discussed for the process of randomness extraction. After that, Device Independent Quantum Random Number Generators (DI-QRNGs) and Semi-Device Independent Quantum Random Number Generators (SDI-QRNGs) are introduced, also providing an example of an integrated SDI-QRNG. Finally, the certification scheme over which the Single Photon Entanglement (SPE)-based SDI-QRNG is discussed from a theoretical and experimental point of view, for different levels of trust in the source of SPE states.

## 3.1 Quantum random number generators

A Quantum Random Number Generator (QRNG) is a Random Number Generator (RNG) that exploits quantum processes to generate random numbers. The probabilistic description of the Nature that quantum mechanics offers can be exploited to obtain real devices that produce real randomness. Historically, the first QRNGs were based on radioactive decay[13, 57–59]. To generate randomness, this class of QRNGs uses the Poissonian distribution of the detection events of $\alpha$, $\beta$, and $\gamma$-particles

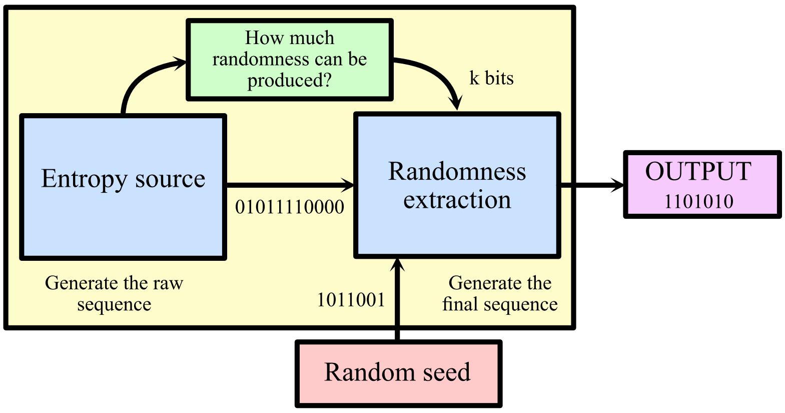

How much randomness can be produced?
k bits
Entropy source
01011110000
Randomness extraction
OUTPUT
1101010
Generate the raw sequence
1011001
Generate the final sequence
Random seed

**Figure 3.1:** Schematic of a typical QRNG. The raw random bits produced by the quantum entropy source are processed by the randomness extractor, which provides, as output, a sequence of unbiased random numbers. The additional inputs required by the randomness extractor are a random seed and an estimation of the number of truly random bits produced by the entropy source.

emitted during a decay reaction. Nowadays, the largest class of QRNGs is based on photonics and uses quantum optics principles[4] like:

- superposition of paths and measurements[14, 60–62];
- photon arrival time[63–74];
- photon counting measurements[75–81];
- attenuated pulse[82–86];
- quantum vacuum instability[87–89];
- phase fluctuations[90–98].

The above list is far to be complete, but it provides an overview of the research interest on this type of QRNGs. These are the best candidates to be widely used in real-life applications, with some big manufacturer groups that have already implemented them in consumer electronics[99, 100] . The typical structure of a QRNG is explained in Figure 3.1. The "magic" is contained in the quantum entropy source box, where a quantum state is manipulated and measured to generate a raw sequence of random numbers. These usually contain bias and are correlated due to the imperfections of the experimental apparatus or the presence of noise. For these reasons, the sequence is then "cleaned" using the post-processing techniques of randomness extraction. The output of this stage is a sequence of perfectly uncorrelated and unbiased bits. The key ingredients, that must be provided to the randomness extraction stage, are an initial random seed and an estimation of how many uniform random bits can be extracted from the considered entropy source. To estimate such a quantity, it is helpful to introduce the concept of entropy.

## 3.2 The concept of entropy: definitions and examples

The entropy is a physical quantity related to the quantification of randomness. However, there exist many entropy definitions in information theory. In this section, these will be introduced and their meaning discussed. The following notation will be used: a discrete random variable $\Lambda$ is considered, which is distributed according to a probability distribution $\mathbb{P}_\Lambda$. Taking now an alphabet $\mathscr{A}$ with $N$ possible outcomes $\{\lambda_i\}_{i=1..N}$, the probability of obtaining the result $\lambda_i$ is defined as $\mathbb{P}_\Lambda(\lambda_i)$. The following discussion follows the work of [4] .

[4]: Herrero-Collantes et al. (2017), 'Quantum Random Number Generators'

[99]: IDQuantique (2021), *IDQuantique ID Quantique and SK Telecom unveil the Samsung Galaxy Quantum2, the newest QRNG-Powered 5G smartphone with even more embedded secured applications*

[100]: IDQuantique (2021), *IDQuantique ID Quantique integrates its quantum chip in Vsmart Aris 5G Smartphone*

[4]: Herrero-Collantes et al. (2017), 'Quantum Random Number Generators'

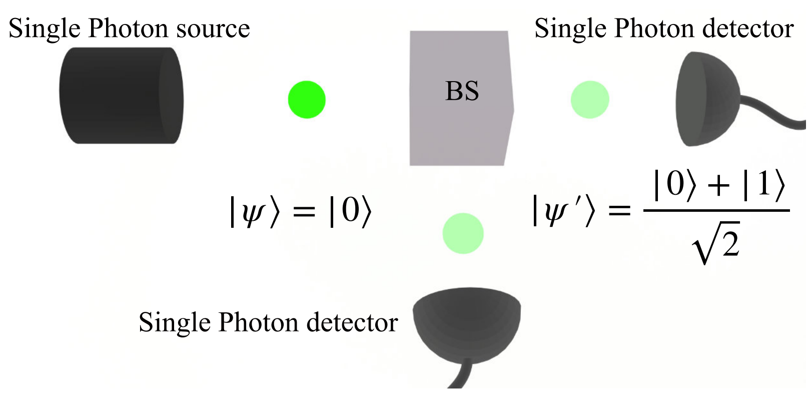

Single Photon source
BS
Single Photon detector
$|\psi\rangle = |0\rangle$
$|\psi'\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$
Single Photon detector

**Figure 3.2:** Schematic of a simple optical QRNG based on the superposition of the output paths created by the Beam Splitter (BS). In the case of a 50:50 BS, a single photon source and ideal detectors, it represents a perfect QRNG.

### 3.2.1 Shannon Entropy

The Shannon Entropy[101] provides the *average* number of bits that an entropy source can generate, or, equivalently, the number of bits necessary to store the digits produced by the source in each round (Shannon's noiseless coding theorem[102] ). It is defined as:

[101]: Shannon (1948), 'A Mathematical Theory of Communication'

[102]: Nielsen et al. (2001), 'Quantum computation and quantum information'

$$H(\Lambda) := -\sum_{\lambda_i \in \mathcal{A}} \mathbb{P}_\Lambda(\lambda_i) \log_2 \left[\mathbb{P}_\Lambda(\lambda_i)\right]. \tag{3.1}$$

Consider now the optical QRNG reported in Figure 3.2: a single photon emitted by a single photon source that encounters a Beam Splitter (BS). At the output ports of the BS, there are two ideal single photon detectors that click every time a single photon arrives. If the single photon comes from the $|0\rangle$ direction, the BS creates a superposition of the paths $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = |0\rangle \rightarrow |\psi'\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle). \tag{3.2}$$

The mean values of the projectors $P_j$ over the direction $j$ is:

$$\langle\psi'|P_0|\psi'\rangle = \langle\psi\prime|P_1|\psi\prime\rangle = \frac{1}{2}. \tag{3.3}$$

In this optical QRNG it is enough to assign the outcome 0 every time a photon is detected in $|0\rangle$ and 1 every time the photon is detected in $|1\rangle$. The Shannon Entropy of the process is:

$$\begin{aligned} H(\Lambda) &= -\sum_{\lambda_i \in \{0,1\}} \mathbb{P}_\Lambda(\lambda_i) \log_2 \left[\mathbb{P}_\Lambda(\lambda_i)\right] \\ &= -\mathbb{P}_\Lambda(0) \log_2 \left[\mathbb{P}_\Lambda(0)\right] - \mathbb{P}_\Lambda(1) \log_2 \left[\mathbb{P}_\Lambda(1)\right] \\ &= -2\frac{1}{2} \log_2 \left[\frac{1}{2}\right] \\ &= 1. \end{aligned} \tag{3.4}$$

For each single photon, one bit of randomness is produced. The discussion can be generalized to more complicated QRNGs: for a uniform distribution of $N$ equally probable outcomes, the Shannon Entropy is $\log_2 N$.

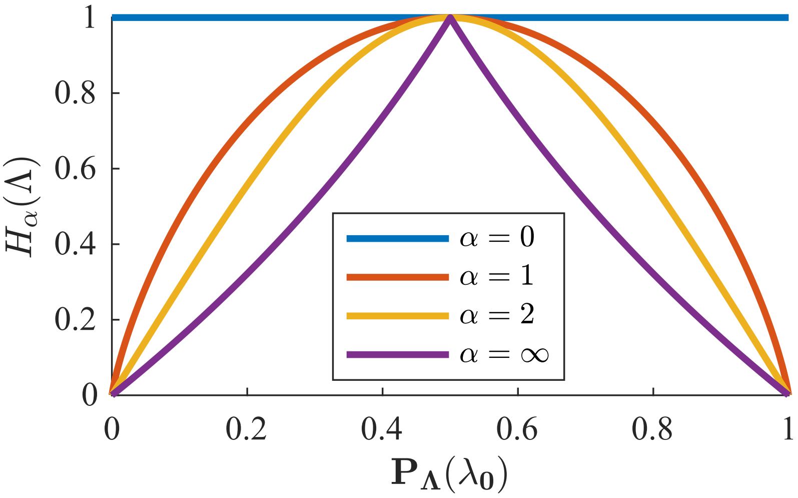


**Figure 3.3:** Plot of the Rényi entropy for different $\alpha$, in the case of binary outcomes $\{\lambda_0, \lambda_1\}$. Here there are reported, in blue, $H_0(\Lambda)$, in red, $H_1(\Lambda) = H(\Lambda)$, in yellow, $H_2(\Lambda)$ and in purple, $H_{\inf}(\Lambda)$ as a function of the outcome $\lambda_0$ probability.

### 3.2.2 Family of Rényi entropies

The Shannon entropy $H(\Lambda)$ can be generalized considering the Rényi entropies[103] , a family of entropies defined as:

[103]: Rényi (1961), 'On measures of entropy and information'

$$H_\alpha(\Lambda) := \frac{1}{1-\alpha}\log_2\left[\sum_{\lambda_i \in \mathcal{A}} \mathbb{P}_\Lambda(\lambda_i)^\alpha\right]. \tag{3.5}$$

In the limit $\alpha \longrightarrow 1$, $H_\alpha(\Lambda)$ is exactly the Shannon entropy $H(\Lambda)$. A remarkable property of the Rényi entropies is that

$$H_\beta(\Lambda) \leq H_\alpha(\Lambda), \quad \alpha \leq \beta. \tag{3.6}$$

Consider now a binary entropy source where only two outcomes are available $\{\lambda_0, \lambda_1\}$. In this case it is possible to graphically represent the Rényi entropies for selected values of $\alpha$. These plots are reported in Figure 3.3, confirming the validity of Equation 3.6.

### 3.2.3 Max-entropy

The max-entropy $H_0(\Lambda)$ or $H_{\max}(\Lambda)$ is defined as the limit for $\alpha \longrightarrow 0$ of $H_\alpha(\Lambda)$:

$$H_{\max}(\Lambda) = \log_2 [N] . \tag{3.7}$$

which correspond to the Shannon entropy of a uniform probability distribution of $N$ outcomes. This entropy is the upper bound of all the Rényi entropies.

### 3.2.4 Min-entropy

The min-entropy $H_\infty(\Lambda)$ or $H_{\min}(\Lambda)$ is defined as the limit for $\alpha \longrightarrow \infty$ of $H_\alpha(\Lambda)$, or, equivalently, as the logarithm of the most probable outcome $\lambda_i$:

$$H_{\min}(\Lambda) := -\log_2\left[\max_{\lambda_i \in \mathcal{A}} \mathbb{P}_\Lambda(\lambda_i)\right]. \tag{3.8}$$

It is possible to define also the guessing probability of the sequence as:

$$\mathbb{P}_{\text{guess}}(\Lambda) := \max_{\lambda_i \in \mathcal{A}} \mathbb{P}_{\Lambda}(\lambda_i). \tag{3.9}$$

Using the guessing probability definition, the min-entropy $H_{\text{min}}(\Lambda)$ can be rewritten as:

$$H_{\text{min}}(\Lambda) = -\log_2 \left[\mathbb{P}_{\text{guess}}(\Lambda)\right]. \tag{3.10}$$

Equavalently, the guessing probability is:

$$\mathbb{P}_{\text{guess}}(\Lambda) = 2^{-H_{\text{min}}(\Lambda)}. \tag{3.11}$$

As a consequence of Equation 3.6, $H_{\text{min}}(\Lambda)$ represents the lower-bound of all the Rényi entropies. To understand the meaning of $H_{\text{min}}(\Lambda)$, consider now to have an adversary who tries to guess a single outcome of the QRNG and assume that the eavesdropper knows $\mathbb{P}_{\Lambda}$. The best strategy for the adversary is to bet on the highest probability outcome. Essentially, this is the information that $H_{\text{min}}$ provides: in the presence of an adversary that knows $\mathbb{P}_{\Lambda}$, $H_{\text{min}}(\Lambda)$ quantifies the number of bits that can be considered random or, equivalently, how many uniform random bits can be extracted from the considered probability distribution[4] . This can be understood since:

[4]: Herrero-Collantes et al. (2017), 'Quantum Random Number Generators'

1) each outcome $\lambda_i$ has a probability less or equal than the guessing probability $\mathbb{P}_{\text{guess}}(\Lambda)$

$$\mathbb{P}_{\Lambda}(\lambda_i) \leq 2^{-H_{\text{min}}(\Lambda)} = \mathbb{P}_{\text{guess}}(\Lambda), \quad \forall \lambda_i \in \mathcal{A}; \tag{3.12}$$

2) it is possible to write any probability distribution with a bounded min-entropy $H_{\text{min}}(\Lambda)$ as a convex combination of uniform distributions of $H_{\text{min}}(\Lambda)$ bits.

Compared to the other entropies, $H_{\text{min}}$ is the important parameter when considering RNG, since the worst-case scenario must be assumed to provide conservative and safe results. To explain the importance of the min-entropy, consider again the case of the single photon impinging on the BS. For an ideal BS it can be observed that, since $\mathbb{P}_{\Lambda}(\lambda_0) = \mathbb{P}_{\Lambda}(\lambda_1) = \mathbb{P}_{\text{guess}}(\Lambda) = 0.5$:

$$H_{\text{min}}(\Lambda) = H(\Lambda) \tag{3.13}$$

as reported in Figure 3.3. Consider now the situation in which the ideal BS is replaced by a non-ideal one: for example, assume that the power transmission and reflection coefficients of the new BS are respectively $T = 0.60$ and $R = 0.40$. In this situation, the Shannon Entropy is:

$$H(\Lambda) = -0.60 \log_2 [0.60] - 0.40 \log_2 [0.40] = 0.97, \tag{3.14}$$

while the min-entropy is:

$$H_{\text{min}}(\Lambda) = -0.60 \log_2 [0.60] = 0.44. \tag{3.15}$$

which is a value $\simeq 45\%$ lower compared to 0.97. In such a situation, the use of the Shannon entropy to estimate the randomness also implies the assumption that the adversary does not know about the characterization of the faulty BS.

**Conditional Min-entropy**

There exist some situations in which the eavesdropper has a more detailed knowledge of the QRNG with respect to the knowledge of $\mathbb{P}_{\Lambda}$. For example, it can be aware of the measurements that are performed or even of the purification of the used mixed state in the QRNG. For these reasons, the guessing probability $\mathbb{P}_{\text{guess}}(\Lambda)$ is not enough to estimate the probability of guessing the outcomes for such an eavesdropper. In these situations, the quantity that must be considered is the conditional guessing probability $\mathbb{P}_{\text{guess}}(\Lambda|\Delta)$. This parameter quantifies the probability of guessing the outcome $\lambda$ in the presence of the side-information $\Delta$ available to the eavesdroppers. As before, the conditional guessing probability is directly connected with the min-entropy: the conditional min-entropy $H_{\text{min}}(\Lambda|\Delta)$ is defined as:

$$H_{\text{min}}(\Lambda|\Delta) := -\log_2 \left[\mathbb{P}_{\text{guess}}(\Lambda|\Delta)\right] . \tag{3.16}$$

It provides an estimation of how many uniform random bits can be extracted, from the generated sequence, in the presence of an adversary which uses the best strategy and has the side information $\Delta$[7] . In thefollowing, two examples of estimation of the conditional min-entropy $H_{\text{min}}$ will be discussed.

[7]: Konig et al. (2009), 'The operational meaning of min-and max-entropy'

## 3.3 Randomness extractor

This introduction to randomness extractor follows what is reported in [4, 104] .

[4]: Herrero-Collantes et al. (2017), 'Quantum Random Number Generators'
[104]: Ma et al. (2013), 'Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction'

The necessity of estimating the min-entropy $H_{\text{min}}(\Lambda)$ or the conditional min-entropy $H_{\text{min}}(\Lambda|\Delta)$ in the presence of the side information $\Delta$, is well motivated considering randomness extraction. The randomness extraction is a post-processing technique used in most RNG for removing correlations and biases due to errors in the produced random sequence. Ideally, the output of a randomness extractor is a uniform sequence of bits, genuinely random. To provide a brief overview, it is necessary to introduce the concept of statistical distance between two probability distribution $X$ and $Y$, which is defined as:

$$\begin{aligned} ||X - Y|| := & \max_{V \subseteq T} \left| \sum_{v \in V} \mathbb{P}_X(v) - \mathbb{P}_Y(v) \right| \\ = & \frac{1}{2} \sum_{v \in T} |\mathbb{P}_X(v) - \mathbb{P}_Y(v)| , \end{aligned} \tag{3.17}$$

where $T$ is the common domain of the two probability distributions. This notion of distance is useful in the context of randomness extractors. Indeed, the goal of any extractor is to extract, from the probability distribution $X$ produced by the RNG, a $Y$ distribution which is near enough ($\epsilon$-near) to the uniform distribution $U$, or, equivalently:

$$||Y - U|| \leq \epsilon, \tag{3.18}$$

where $\epsilon$ is a security parameter. Now it possible to define the extractor as the function $(k, d, n, m, \epsilon) - \text{Ext}$

$$\text{Ext} : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m \tag{3.19}$$

such that

$$|| \,\text{Ext}(\Lambda, U_d) - U_m|| \leq \epsilon, \tag{3.20}$$

$\forall \Lambda \in \{0,1\}^n$ having a min-entropy $H_{\min}(\Lambda) \geq k$. In Equation 3.20, $U_m$ is the target uniform distribution, while $U_d \in \{0,1\}^d$ is the random seed of the extractor. It seems a little bit awkward to use a perfect RNG to generate a uniform random seed, being used to obtain another perfectly random sequence: why it is not simply used the initial RNG to generate other random numbers? Despite possible motivations about speed and availability of such a RNG, the use of the random seed becomes reasonable in the case of *strong* randomness extractors. A strong randomness extractor is a function $(k, d, n, m, \epsilon) - \text{Ext}$ for which

$$|| \,\text{Ext}(\Lambda, U_d) \circ U_d - U_{d+m}|| \leq \epsilon. \tag{3.21}$$

Using a strong extractor, it is possible to reuse multiple times the same input random seed, which, however, has to be maintained private. In such a way, the generation of the seed can be performed once and then the extractor can use it multiple times, without any consequence. Example of strong extractors are the Trevisan extractor[105] and the Toepliz matrix multiplication[106] , which is a particular case of hashing function extractors[104, 107] .

## 3.4 Methodology for certifying randomness

In the previous example of the QRNG reported in Figure 3.2, it was showed how the min-entropy varies, introducing an unbalance between the transmission and detection power coefficients. Such an example suggests that a QRNG must be perfectly characterized to certify the amount of randomness effectively produced. Moreover, such a characterization must be repeated to ensure that the components' aging or other phenomena have not changed it. This limits the trust and the applicability of any QRNG. Even the presence of eavesdroppers could be a problem in this situation: they can have a better characterization of the device and utilize it to extract some information about the generated sequence. Remarkably, quantum mechanics offers ways to certify the amount of conditional min-entropy even in the presence of faulty devices and eavesdroppers, which have side information, such as a better knowledge of the considered QRNG. These QRNGs are called Device Independent Quantum Random Number Generators (DI-QRNGs). DI-QRNGs[15, 17, 108–111] are considered the golden standard of the quantum random number generation. Indeed, the entropy certification that these QRNGs offer is extremely powerful: with a DI-QRNG, it is possible to certify randomness, i.e., the conditional min-entropy of the sequence, without any prior characterization of the devices used and even in the presence of an eavesdropper with unlimited computational power and side information. These QRNGs are usually based on the violation of the Bell's Inequality (BI). In particular, when a violation is observed ($\chi > 2$, where

[105]: (2001), 'Extractors and Pseudorandom Generators'

[106]: Mansour et al. (1990), 'The computational complexity of universal hashing'

[107]: Nisan et al. (1999), 'Extracting Randomness: A Survey and New Constructions'

[104]: Ma et al. (2013), 'Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction'

[17]: Pironio et al. (2010), 'Random Numbers Certified by Bell's Theorem'

[108]: Pironio et al. (2013), 'Security of practical private randomness generation'

[109]: Plesch et al. (2014), 'Device-independent randomness amplification with a single device'

[15]: Acín et al. (2016), 'Certified randomness in quantum physics'

[110]: Arnon-Friedman et al. (2018), 'Practical device-independent quantum cryptography via entropy accumulation'

[111]: Arnon-Friedman et al. (2019), 'Simple and tight device-independent security proofs'

$\chi$ is the correlation function introduced in Chapter 2) in a loopholes-free scenario, the conditional min-entropy of the outcomes $(x, y)$, observed in the BI test, can be lower bounded by a function of $\chi$ itself. Conceptually, the certification offered by the BI is elegant: when a violation of the BI is observed, no hidden local variable model can deterministically explain the distribution of the observed outcomes. As a consequence, these are not predetermined and are necessarily distributed randomly, according to quantum mechanics. In the last years, some experimental works have demonstrated DI-generation of quantum random numbers[112–118] . However, DI-QRNGs represent technological challenges. Closing all the loopholes imposes separated measurement stages (locality loophole) equipped with high-efficiency detectors (detection loophole: to avoid making assumptions on the efficiencies of the implied detectors, near-unity detection efficiencies are required) and complex coincidence electronics. These facts, together with the slow generation rates obtained in the experiments, seriously compromise any deployment of such QRNG in real-life applications. The idea of transforming the DI-approach, i.e., to use fundamental quantum principles to certificate the min-entropy, in a more market-oriented approach, has pushed the development of a new class of QRNGs: the Semi-Device Independent Quantum Random Number Generators (SDI-QRNGs). In a SDI-QRNG, one or more parts of the setup are left uncharacterized, while a certain amount of assumptions are introduced. As an example, a DI-QRNG could be considered a SDI-QRNG if the characterization of the detectors or the source is assumed. In the years, many SDI-QRNGs have been proposed based on different physical principles. A non-exhaustive list is reported in Table 3.1. Respect to DI-QRNGs, SDI-QRNGs have simpler experimental implementations and, moreover, achieve generation rates comparable to standard QRNG (MHz) at the cost of being less secure, since assumptions on the internal behaviour of these QRNGs are introduced. However, they represent a good trade-off between feasibility and security.

[112]: Bierhorst et al. (2018), 'Experimentally generated randomness certified by the impossibility of superluminal signals'
[113]: Liu et al. (2018), 'Device-independent quantum random-number generation'
[114]: Liu et al. (2018), 'High-speed device-independent quantum random number generation without a detection loophole'
[115]: Shen et al. (2018), 'Randomness extraction from bell violation with continuous parametric down-conversion'
[116]: Zhang et al. (2020), 'Experimental low-latency device-independent quantum randomness'
[117]: Shalm et al. (2021), 'Device-independent randomness expansion with entangled photons'
[118]: Liu et al. (2021), 'Device-independent randomness expansion against quantum side information'

**Table 3.1:** Non-exhaustive list of SDI-QRNGs. For each SDI-QRNG it is reported how it generates randomness, its classification based on the assumptions introduced in the certification protocols and the reported random bit generation rate if experimentally implemented or simulated(*). Acronyms: Source Independent (SI), Positive operator-valued measure (POVM), Measurement Independent (MI), Bounded states overlap (BSO), Bounded energy (BE), Bounded system dimensionality (BSD), Quantum steering (QS), Quantum contextuality (QC), Device independent + assumptions (DI+A) .

| Randomness | Type | Gen. Rate [bits] | Ref |
|---|---|---|---|
| Uncertainty principle | SI | - | [119] |
| Uncertainty principle | SI | 5 kHz | [120] |
| Uncertainty principle | SI | 1.7 GHz | [121] |
| Overcomplete set of POVMs | SI | 17.42 GHz | [122] |
| Uncertainty principle | SI | 8.2 kHz | [123] |
| Phase Randomization | SI | 270 MHz | [124] |
| Extremality of Gaussian states | SI | 15.07 GHz | [125] |
| Uncertainty principle | SI | 1.81 MHz | [126] |
| Probability Estimation Factors | SI | 22 kHz | [127] |
| POVMs set + tomography | MI | 50 kHz* | [128] |
| POVMs set + tomography | MI | 5.7 kHz | [129] |
| Trusted Shutter | Variable SI and MI | 37.2 MHz | [130] |
| State discrimination | BSO+BE | 16.5 MHz | [18] |
| State discrimination | BE | 6.9 kHz | [131] |
| State discrimination | BE | - | [132] |
| State discrimination | BE | 1.25 MHz | [133] |
| State discrimination | BE | - | [20] |
| State discrimination | BE | 145.5 MHz | [134] |
| State discrimination | BE | 113 MHz | [135] |
| State discrimination | BE | - | [136] |
| State discrimination | BE | - | [137] |
| State discrimination | BSD | - | [138] |
| Dimension witness | BSD | - | [139] |
| Dimension witness | BSD | - | [140] |
| Dimension witness | BSD | 23 Hz | [141] |
| Steering | QS | - | [142] |
| Value indefiniteness | QC | - | [143] |
| Entanglement | DI+A | 4.4 kHz | [25] |

## 3.5 Example of Conditional Min-entropy estimation using an SDI-QRNG

To provide an example of a SDI-QRNG in which the conditional min-entropy is certified, here it is reported the case of a fully integrated optical QRNG[72] in which a semi-independent protocol of generation of random numbers[18] is implemented. The original work is reported in [131] .

### 3.5.1 Description of the semi-device independent protocol

The SDI protocol is a prepare and measure protocol that uses the number of particles implementation reported in [18]. It requires a controllable emitter of photons and a detector able to reveal single photons. The source must be partially characterized: it must generate two states $\rho_1$, $\rho_2$ depending on the value of an input variable $x$. The detector, instead, is left uncharacterized: it only provides, as output, a binary digit $b$ for each

[72]: Acerbi et al. (2018), 'A Robust Quantum Random Number Generator Based on an Integrated Emitter-Photodetector Structure'

[18]: Brask et al. (2017), 'Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination'

[131]: Leone et al. (2020), 'An optical chip for self-testing quantum random number generation'

state sent by the emitter. Now, the only requirement for the protocol is a lower bound over the fidelity of the two states $\rho_1$, $\rho_2$, which must be kept fixed for the measurement device and any possible observer. The fidelity between the two states $\rho_1$, $\rho_2$ is defined as

$$F\left(\rho_1, \rho_2\right) := \mathrm{Tr}\left(\sqrt{\rho_1}\rho_2\sqrt{\rho_1}\right) \tag{3.22}$$

and it must be lower bounded by a certain value $\delta$:

$$F\left(\rho_1, \rho_2\right) \geq \delta. \tag{3.23}$$

If the fidelity is big enough, the two state $\rho_1$, $\rho_2$ are not perfectly distinguishable, independently on the characteristics of the two state considered. This is the key intuition behind the protocol: the measurement device is supposed to perform a perfect Unambiguous State Discrimination (USD) measurement[144–147] , i.e., is able to find a measurement that

1) maximize $\mathbb{P}(x = b)$
   and for which
2) $\mathbb{P}(x \neq b) = 0$.

Quantum mechanics allows finding such a measurement. Moreover, this is the one that best discriminates between the two states. However, this comes at the price of introducing a certain amount of inconclusive events: these represent the occurrences in which neither an error nor an event is observed. These inconclusive events are not only present but they must be distributed randomly. This is a direct consequence of having used the USD strategy: if the "positions" of the inconclusive events are predictable, a better measurement can be found to avoid them systematically. Now, the probability of observing an inconclusive event is strictly connect to $\delta$ and, in particular, $\mathbb{P}(b = \emptyset) \geq \delta$, where $\emptyset$ represents the inconclusive occurrence. Given the idea behind the protocol[1] , it can be proven that the conditional min-entropy $H_{\min} = -\log_2(\mathbb{P}_{\text{guess}}(B|\Lambda))$ can be lower-bounded using a Semi-Definite Program (SDP), starting from the conditional probabilities $\{\mathbb{P}(b|x)\}_{b,x=0,1}$ and $\delta$[18] . Here $\mathbb{P}_{\text{guess}}(B|\Lambda)$ represents the guessing probability of the output string $B = \{b_i\}_i$ knowing the value of $\Lambda$, which is a classical random variable that accounts for all the possible measurement strategies. In this example, the On-Off-Keying (OOK) version is used. The input variable $x$ is used to directly control the source: for $x = 0(1)$, it is switched On(Off). The state prepared and sent when $x = 0$ is the vacuum state

$$\rho_0 = |0\rangle\langle 0|. \tag{3.24}$$

For $x = 1$, instead, the state

$$\rho_1 = \sum p(n)|n\rangle\langle n| \tag{3.25}$$

is sent. Here $\rho_1$ is a classical mixture of Fock's states, with $p(n)$ super-Poissonian coefficients[148] . In this situation, the fidelity of these two states is given by:

$$F\left(\rho_1, \rho_2\right) = \sqrt{p(0)} \tag{3.26}$$

where $p(0)$ is the probability that the source emits the vacuum state when On. As experimentally reported in [148] , the average number of photons

[144]: Ivanovic (1987), 'How to differentiate between non-orthogonal states'
[145]: Dieks (1988), 'Overlap and distinguishability of quantum states'
[146]: Peres (1988), 'How to differentiate between non-orthogonal states'
[147]: Barnett et al. (2009), 'Quantum state discrimination'

[1] The description of the complexity of the protocol is out of the scope of this section, so the reader is referred to [18] for a more detailed description.

[18]: Brask et al. (2017), 'Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination'

[148]: Bisadi (2017), 'All-Silicon-Based Photonic Quantum Random Number Generators'

[148]: Bisadi (2017), 'All-Silicon-Based Photonic Quantum Random Number Generators'

$\mu$ for this super-poissonian distribution, is lower than 1. For this reason, the Poissonian estimate $e^{-\frac{\mu}{2}}$ can be used to lower bound the fidelity[131] :

$$F(\rho_0, \rho_1) = \sqrt{p(0)} \geq e^{-\frac{\mu}{2}}. \tag{3.27}$$

This proves that it is just necessary to bound the mean number of emitted photons $\mu$ to fulfill the assumption of the SDI protocol.

[131]: Leone et al. (2020), 'An optical chip for self-testing quantum random number generation'

### 3.5.2 Hardware structure

The hardware structure of the optical QRNG is reported in Figure 3.4a and it is composed of two parts[131] :

1) the optical part (detailed in Figure 3.4b);
2) the electronic part (read-out + control).

[131]: Leone et al. (2020), 'An optical chip for self-testing quantum random number generation'

The optical part is composed of a Silicon Photomultiplier (SiPM), that acts as the emitter of photons through avalanche impact ionization[149] and by two integrated passively-quenched Single Photon Avalanche Diodes (SPADs) that act as detectors of photons. These are placed at 20 $\mu$m apart from the emitter. The emitter and the detectors are p-n junctions on an n-type epi-substrate working in Geiger-mode and passively quenched by integrated resistors. In particular, the SiPM emitter is composed of sixteen cells. The dimension of each cell is about 20 $\mu$m × 20 $\mu$m. To enhance the probability of photon emission, the emitter operates with an emitter's bias voltage above its breakdown voltage ($V_{br} = -32.5$ V at 20°C). The electronic read-out part is integrated into the circuit reported in Figure 3.4a. It has the goal to make readable the detection signal emitted by the integrated SPADs: the signal is amplified and thresholded with the use of a fast comparator and digitalized using a monostable. The electronic control part (not integrated) has the objective to electronically control the QRNG. It provides a voltage of −37 V applied to the common cathode of the SiPM and the SPADs and a voltage bias $V_e$ applied to the anode of the emitter. The value of $V_e$ is controlled by a Field programmable gate array (FPGA), by means of pseudo-random 1 MHz Transistor-transistor logic (TTL) signal: the TTL $x = 0 (x = 1)$ state enables(disables) the emission of photons, since the emitter is totally biased above(below) the breakdown voltage. See Figure 3.5 for an example. To correctly set the value of $V_e$ an Amplification and Manipulation stage (AMS) is used (see Figure 3.4a), to amplify and shift the TTL signal: in this way, the mean number of emitted photons $\mu$ per time interval is controlled by changing the offset voltage.

[149]: Akil et al. (1999), 'A multimechanism model for photon generation by silicon junctions in avalanche breakdown'

### 3.5.3 Experimental implementation

As previously explained in the Subsection 3.5.1 is necessary to estimate:

1 the conditional probabilities $\{\mathbb{P}(b|x)\}_{b,x=0,1}$:
2 the mean number of emitted photons $\mu$ per time interval.

The conditional probabilities are estimated using a FPGA and only one of the integrated SPAD. The experimental setup is reported in Figure 3.6. For every bit $x$ applied to the emitter, the FPGA checks if one or more photons have been revealed in the same time window, independently of the value

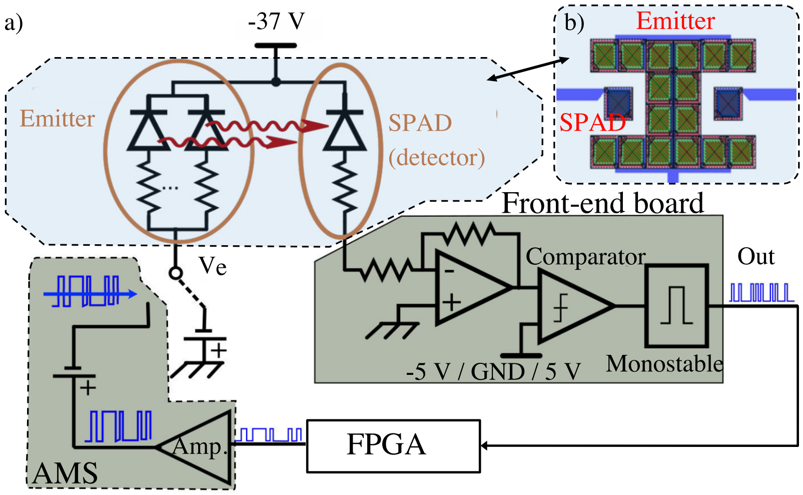
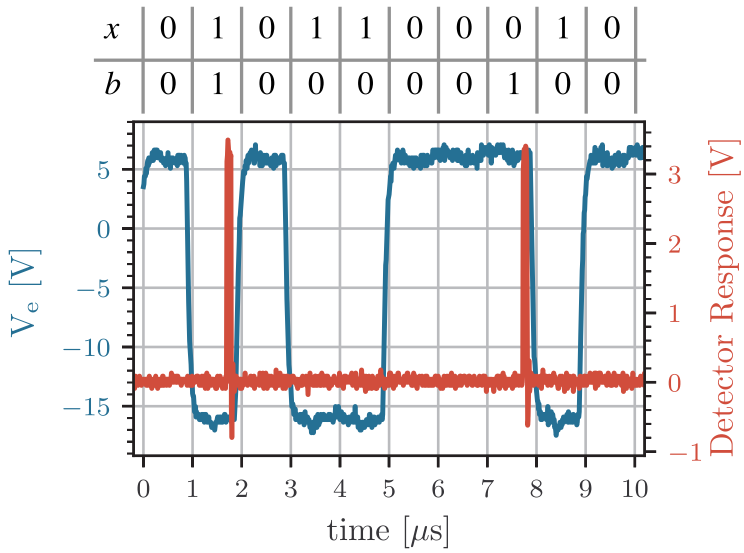


**Figure 3.4:** a) Structure of the integrated chip: the optical structures are reported inside the light blue box, while the electronic components that compose the AMS and the front-end board are inside the olive boxes. A constant or pulsed voltage bias $V_e$ can be applied to the emitter. The pulsed one is a signal obtained by amplifying and voltage shift, through the AMS, a square TTL signal generated by the FPGA. b) Details of the integrated QRNG: it is constituted by a SiPM emitter, composed of an array of sixteen cells, and two SPADs used as detectors (only one used). The metals and the bonding PADs, blue-colored in the figure, deliver the bias voltage to the different structures. Reproduced from [131], with the permission of AIP Publishing.



| $x$ | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|---|---|
| $b$ | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |

**Figure 3.5:** Example of the resulting traces. $V_e$ is shown in blue, while the detector signal is represented in red. The values of $x$ and $b$ are reported in the upper part of the figure. Reproduced from [131], with the permission of AIP Publishing.

of the $x$ bit. In the case of a positive answer, the bit $b = 1$ is registered and stored by the FPGA. Otherwise, $b = 0$ is stored. An oscilloscope monitors the emitter voltage $V_e$. The generated random number sequence is constituted by the sequence of the observed $B = \{b_i\}_{(i=1..N)}$ and, consequently, it is possible to evaluate the conditional probabilities.

The mean number of emitted photons $\mu$ is estimated by using a large core diameter optical fiber (600 $\mu$m, NA=0.22) placed on top of the emitter as shown in Figure 3.6b. A commercial SPAD module is used to detect the collected photons as a function of the voltage bias. The mean number of photons vertically emitted $\mu_v$, which have been collected by the fiber, can be estimated as:

$$\mu_v = \frac{\mu_{\text{mon}}}{\alpha \eta_{mon}} \tag{3.28}$$

where $\mu_{\text{mon}}$ is the mean number of photons detected by the SPAD in a 1 $\mu$s time window for each constant $V_e$ applied, $\alpha \simeq 4\%$ is the optical transmission between the fiber and the SPAD and $\eta_{mon}$ is an effective

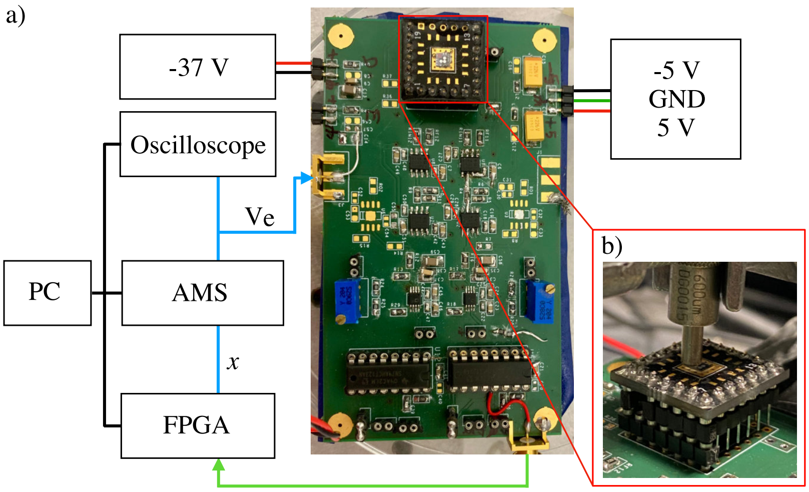


**Figure 3.6:** a) Schematic of the experimental setup. Both the emitter and the detector are reverse-biased at −37 V, while the voltage ±5 V is used to power the electronic board. The voltage bias $V_e$, applied to the emitter (cyan arrow), is directly controlled by the FPGA through the bit value $x$, which is converted to the correct voltage by the AMS. An oscilloscope is used to monitor the voltage applied. For every applied $x$, the FPGA checks if a detection event is occurred by observing the response of the integrated SPAD(green arrow) and store the result. All the instruments are controlled using a PC. b) The fully-integrated optical chip with on the top the optical fiber used to characterize the relation between $\mu$, the mean number of photons emitted per pulse, and the bias voltage $V_e$. The distance between the input facet of the fiber and the emitter surface is within 1 mm. Reproduced from [131], with the permission of AIP Publishing.

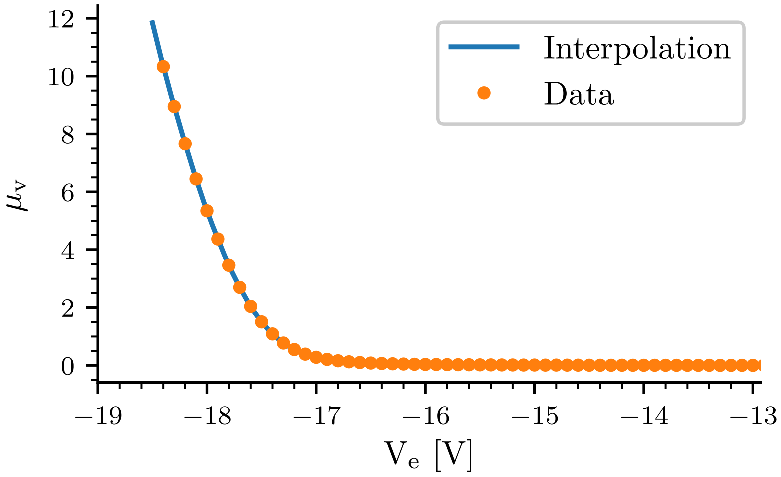


**Figure 3.7:** Characterization curve of the mean number of photons $\mu_v(V_e)$ per microsecond. For every $V_e$ the mean number of photons $\mu_v$ per microsecond vertically emitted is collected by the optical fiber. The experimental data are reported as orange dots, while the spline interpolation is shown in blue. Reproduced from [131], with the permission of AIP Publishing.

detection efficiency obtained as:

$$\eta_{mon} = \int \eta(\lambda)s(\lambda)\mathrm{d}\lambda \simeq 60\%. \tag{3.29}$$

$\eta(\lambda)$ and $s(\lambda)$[148] are respectively the SPAD's nominal detection efficiency as a function of the wavelength and the source's emission spectrum. In Figure 3.7 it is reported in blue the characterization curve $\mu_v(V_e)$, obtained by interpolating the experimental data obtained (orange dots in the same figure).

[148]: Bisadi (2017), 'All-Silicon-Based Photonic Quantum Random Number Generators'

### 3.5.4 Results and discussion

The conditional min-entropy $H_{min}$ is calculated by using the experimentally estimated conditional probabilities $\{\mathbb{P}(b|x)\}_{b,x=0,1}$ and the mean number of photon *effectively* emitted towards the integrated SPAD. Indeed, only a part of the source's light reaches the integrated detector: it is necessary to estimate the relation between $\mu_v$, the number of photons collected by the optical fiber and $\mu_h$, the flux of photons that reaches the

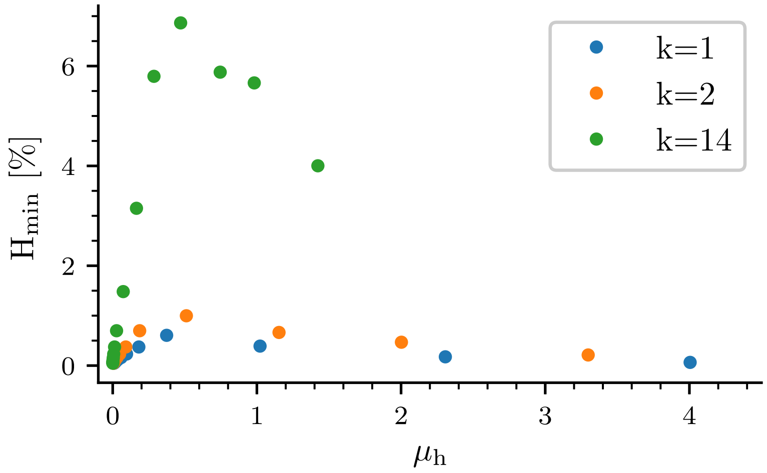


**Figure 3.8:** Calculated minimum entropy $H_{\min}$ as a function of $\mu_{\mathrm{h}}$, the mean number of horizontally emitted photons, for different levels of modelling of the emitter ($k = 1, 2, 14$). Reproduced from [131], with the permission of AIP Publishing.

integrated SPAD. It is possible to define the $k$ parameter as:

$$k := \mu_{\mathrm{v}}/\mu_{\mathrm{h}}. \tag{3.30}$$

In Figure 3.8 and in Table 3.2 the different estimated values of $\mathrm{H}_{\min}$ are reported as a function of $\mu_{\mathrm{h}} = \mu_{\mathrm{v}}/k$ for different values of $k$. Furthermore, in the same table, it is shown the random bit generation rates assuming an instantaneous and perfect randomness extraction. $k = 1$ (blue dots in Figure 3.8) represents the most conservative assumption: the light emitted horizontally by the source ( see $s(\lambda)$ in [148] ) is indeed severely attenuated in the material due to silicon absorption[150] , while this does not occur in the vertical propagation. Under this assumption, a maximum observed min-entropy of 0.61% ± 0.01% is obtained for $\mu_{\mathrm{h}} \simeq 0.4$.

[148]: Bisadi (2017), 'All-Silicon-Based Photonic Quantum Random Number Generators'

[150]: Aspnes et al. (1983), 'Dielectric functions and optical parameters of Si, Ge, GaP, GaAs, GaSb, InP, InAs, and InSb from 1.5 to 6.0 eV'

The assumption $k = 2$ comes from the idea that only half of the emitter cells, the ones facing the SPAD, actually contributes to $\mu_{\mathrm{h}}$, while the emission of the other half is entirely absorbed by the material. In this situation (orange dots of Figure 3.8) a maximum of $\mathrm{H}_{\min} = 0.99\% \pm 0.02\%$ is estimated. A more realistic model (see Figure 3.9) can be made considering the sixteen single emitting cells of the SiPM as point emitters. Each one of these emits isotropically photons with the spectrum $s(\lambda)$. Different solid angles ($\Omega_{\mathrm{v}}$ and $\Omega_{\mathrm{h}}$) and two different detection paths ($\mathrm{L}_{\mathrm{v}}(\Omega_{\mathrm{v}})$ and $\mathrm{L}_{\mathrm{h}}(\Omega_{\mathrm{h}})$) are considered for the vertical and horizontal photon fluxes. Specifically, to calculate $\mu_{\mathrm{v}}$, these factors are assumed:

- sixteen equal cells;
- the silicon absorption coefficient $\alpha(\lambda)$;
- the acceptance angle $\Omega_{\mathrm{v}}$ of the optical fiber;
- the transmission $T(\lambda)$ through the silicon surface: a normal incidence is assumed, so $T(\lambda) = 1 - \left(\frac{\mathrm{n_{Si}}(\lambda)-1}{\mathrm{n_{Si}}(\lambda)+1}\right)^2$ where $\mathrm{n_{Si}}$ is the refractive index of silicon.

For $\mu_{\mathrm{h}}$, instead, it is considered only the spatial distribution of the SiPM cells respect to the detector (sum over $i$ in Equation 3.31). $k$ is then estimated as:

$$k \simeq \frac{16 \int_{\lambda} \int_{\Omega_{\mathrm{v}}} \mathrm{T}(\lambda) e^{-\alpha(\lambda)\mathrm{L_v}(\theta,\phi)} s(\lambda) \mathrm{d}\lambda \mathrm{d}\theta \mathrm{d}\phi}{\sum_{i=1}^{16} \int_{\lambda} \int_{\Omega_{\mathrm{h},i}} e^{-\alpha(\lambda)\mathrm{L_{h,i}}(\theta_i,\phi_i)} s(\lambda) \mathrm{d}\lambda \mathrm{d}\theta \mathrm{d}\phi} \simeq 14 \tag{3.31}$$

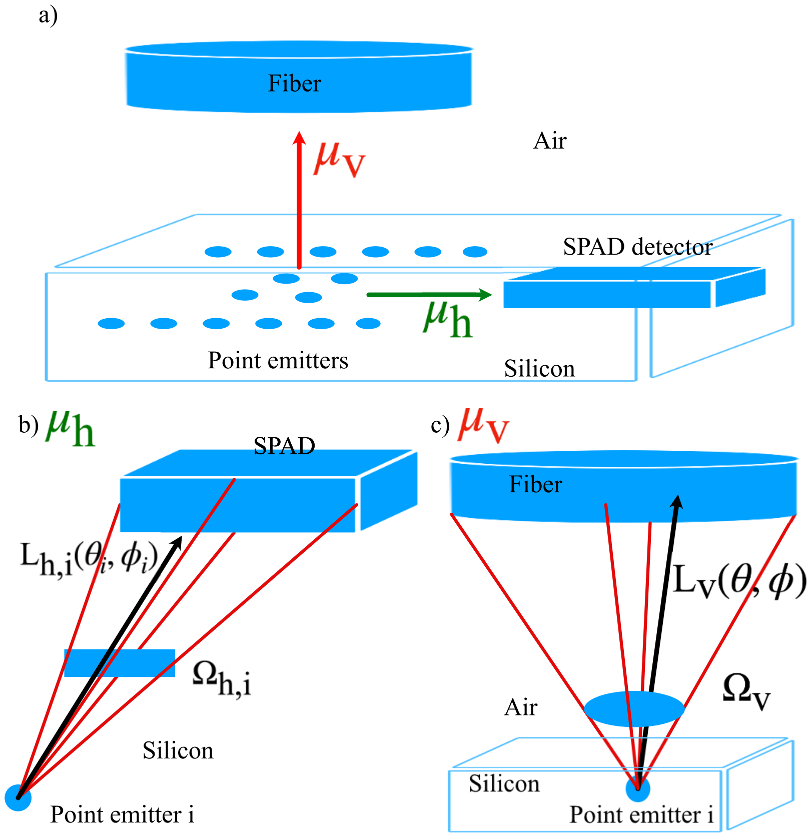


**Figure 3.9:** a)Schematic representation of the estimation of $\mu_h$ and $\mu_v$ when considering the emitter as composed of sixteen point emitters. b) Estimation of $\mu_h$: for each point emitter, it is determined the solid angle $\Omega_{h,i}$ in which the photons are detected by the SPAD. $\Omega_{h,i}$ has a rectangular shape determined by the dimension of the detector. $L_{h,i}(\theta_i, \phi_i)$ is the distance between the point emitter *i* and a point on the detector's surface. The entire process occurs in the silicon material, so the the silicon absorption coefficient $\alpha(\lambda)$ (not reported) has to be considered. c) Estimation of $\mu_v$: the sixteen emitters are considered equal and, for each of them, is considered the acceptance solid angle $\Omega_v$ of the optical fiber placed on the chip. $L_v(\theta, \phi)$ is the distance between the point emitter and the surface of the fiber. Since the process occur in two materials, silicon and air, it is necessary to consider also the transmission $T(\lambda)$ of the surface between the silicon and the air (not reported).

| $k$ | $H_{min}$% | Generation rate [kHz] |
|---|---|---|
| 1 | 0.61% ± 0.01 | 6.1 |
| 2 | 0.99% ± 0.02 | 9.9 |
| 14 | 6.9% ± 0.1% | 69 |

**Table 3.2:** Conditional min-entropy and generation rate of the SDI-QRNG of [131] for different values of the k parameter.

For $k = 14$, $H_{min}$ is reported in green dots in Figure 3.8. A maximum value of $H_{min} = 6.9\% \pm 0.1\%$ is obtained. Note that it exists a trade-off between introducing more complicated but precise assumptions and, consequently, increasing the min-entropy and the overall security of the QRNG. Each additional assumption introduces a possible way to cheat the protocol. Indeed, if only one of those is not valid, the entire min-entropy estimation is incorrect. The analysis based on $k = 1$ is safer because it provides a min-entropy lower bound with respect to the other cases ($k > 1$).

Assuming now a perfect extraction procedure, i.e., all the random bits are perfectly extracted, the generation rate of the random number is obtained by multiplying the conditional min-entropy by the working frequency of the QRNG. For $k = 1$, the generation rate obtained is 6.1 kHz, while for $k = 2$, 9.9 kHz is obtained. Eventually, for $k = 14$ the generation rate corresponds to 69 kHz.

## 3.6 Generating quantum randomness using CHSH violation

[30]: Scarani (2019), *Bell nonlocality*
[151]: Acín et al. (2012), 'Randomness versus nonlocality and entanglement'

In this section, it is introduced the typical min-entropy proof used in DI-QRNG for certifying the conditional min-entropy. This discussion follows the Refs.[30, 151] . Such result will be used in the certification scheme of the SPE-based SDI-protocol. Consider the typical Bell scenario introduced in Chapter 2. Since the discussion is general, the notation used in the initial sections of the Chapter 2 is re-introduced, i.e., $\mathbf{n}_a, \mathbf{n}_b$ are used instead of $\phi, \theta$. The objective of the DI-certification scheme is to obtain a realization independent upper bound to the guessing probability:

$$\mathbb{P}_{\text{guess}}(\psi, \mathbf{n}_a, \mathbf{n}_b) := \max_{(x,y)} \mathbb{P}(x, y|\psi, \mathbf{n}_a, \mathbf{n}_b). \tag{3.32}$$

For the most general input state $\rho = \sum_\lambda p_\lambda |\psi_\lambda\rangle\langle\psi_\lambda|$, the guessing probability is defined as:

$$\mathbb{P}_{\text{guess}}(\rho, \mathbf{n}_a, \mathbf{n}_b) := \max_{p_\lambda, \psi_\lambda} \sum_\lambda p_\lambda \mathbb{P}_{\text{guess}}(\psi_\lambda, \mathbf{n}_a, \mathbf{n}_b). \tag{3.33}$$

The max is taken over all the possible decomposition of the state $\rho$: $\mathbb{P}_{\text{guess}}(\rho, \mathbf{n}_a, \mathbf{n}_b)$ takes into account that the adversary knows precisely in which particular pure state $|\psi_\lambda\rangle$ $\rho$ has been prepared. This knowledge is considered as side information accessible to the eavesdropper. In this situation, it is necessary to define the *realization* of the quantum distribution $\mathbb{P}(\ |\rho, \mathbf{n}_a, \mathbf{n}_b)$ as the set $\mathcal{Q}$ of all the triples $\{(\rho, P_\pm^{\mathbf{n}_a}, P_\pm^{\mathbf{n}_b})\}$, for which:

$$\mathbb{P}(x, y|\rho, \mathbf{n}_a, \mathbf{n}_b) = \text{Tr}[\rho P_x^{\mathbf{n}_a} \otimes P_y^{\mathbf{n}_b}], \qquad x, y \in \{+1, -1\}, \tag{3.34}$$

where $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$, while $P_\pm^{\mathbf{n}_a} = \frac{1}{2}(I_2 \pm \mathbf{n}_a \cdot \sigma)$ and $P_\pm^{\mathbf{n}_b} = \frac{1}{2}(I_2 \pm \mathbf{n}_b \cdot \sigma)$ are Projection-valued measure (PVM), respectively, on $\mathcal{H}_A$ and $\mathcal{H}_B$. Consequently, the realization-independent quantum guessing probability $\mathbb{P}_{\text{guess}}(\mathbb{P})$ associated to the distribution $\mathbb{P}_{\rho\mathbf{n}_a\mathbf{n}_b} := \mathbb{P}(\ |\rho, \mathbf{n}_a, \mathbf{n}_b)$, is defined as:

$$\mathbb{P}_{\text{guess}}(\mathbb{P}_{\rho\mathbf{n}_a\mathbf{n}_b}) := \max_{(\rho, P_\pm^{\mathbf{n}_a}, P_\pm^{\mathbf{n}_b}) \in \mathcal{Q}} \mathbb{P}_{\text{guess}}(\rho, \mathbf{n}_a, \mathbf{n}_b). \tag{3.35}$$

Regarding this guessing probability is possible to observe that:

- it provides a robust bound, independent of the side information that an adversary can have on $\rho$;
- it is effectively realization independent: it does not depend on the particular choice of the couple $(\rho, P_\pm^{\mathbf{n}_a}, P_\pm^{\mathbf{n}_b}) \in \mathcal{Q}$;
- it depends only on the observed outcomes, that comes from the measurements of observables in product form.

Since this certification scheme is usually applied to situation in which a traditional Bell test is performed, two distant particles are considered. It is interesting to define the marginals of the joint distribution $P(\ |\rho, \mathbf{n}_a, \mathbf{n}_b)$ respect to the measurement of observables $O^{\mathbf{n}_a}$ and $O^{\mathbf{n}_b}$:

$$\mathbb{P}_{\rho\mathbf{n}_a}(x) := \mathbb{P}(x|\rho, \mathbf{n}_a) := \sum_y \mathbb{P}(x, y|\rho, \mathbf{n}_a, \mathbf{n}_b) = \text{Tr}[\rho P_x^{\mathbf{n}_a} \otimes I], \tag{3.36}$$

$$\mathbb{P}_{\rho\mathbf{n}_b}(y) := \mathbb{P}(y|\rho, \mathbf{n}_b) := \sum_x \mathbb{P}(x, y|\rho, \mathbf{n}_a, \mathbf{n}_b) = \text{Tr}[\rho I \otimes P_y^{\mathbf{n}_b}]. \tag{3.37}$$

The associated realization-independent guessing probability $\mathbb{P}_{\text{guess}}(\mathbb{P}_{\rho\mathbf{n}_a})$ and $\mathbb{P}_{\text{guess}}(\mathbb{P}_{\rho\mathbf{n}_b})$ are defined as:

$$\mathbb{P}_{\text{guess}}(\mathbb{P}_{\rho\mathbf{n}_a}) := \max_{(\rho, P_{\pm}^{\mathbf{n}_a}, P_{\pm}^{\mathbf{n}_b}) \in \mathcal{Q}} \mathbb{P}_{\text{guess}}(\rho, \mathbf{n}_a), \tag{3.38}$$

$$\mathbb{P}_{\text{guess}}(\mathbb{P}_{\rho\mathbf{n}_b}) := \max_{(\rho, P_{\pm}^{\mathbf{n}_a}, P_{\pm}^{\mathbf{n}_b}) \in \mathcal{Q}} \mathbb{P}_{\text{guess}}(\rho, \mathbf{n}_b), \tag{3.39}$$

where $\mathbb{P}_{\text{guess}}(\rho, \mathbf{n}_a)$ and $\mathbb{P}_{\text{guess}}(\rho, \mathbf{n}_b)$ are constructed in the same way as $\mathbb{P}_{\text{guess}}(\rho, \mathbf{n}_a, \mathbf{n}_b)$ in the case where respectively $P_x^{\mathbf{n}_a} \otimes I_2$ and $I_2 \otimes P_x^{\mathbf{n}_b}$ are used instead of $P_x^{\mathbf{n}_a} \otimes P_y^{\mathbf{n}_b}$. Due to the definition of $\mathbb{P}_{\text{guess}}(\mathbb{P}_{\rho\mathbf{n}_a})$ and $\mathbb{P}_{\text{guess}}(\mathbb{P}_{\rho\mathbf{n}_b})$, it can be observed that:

$$\begin{aligned} \mathbb{P}_{\text{guess}}(\mathbb{P}_{\rho\mathbf{n}_a}) &\geq \mathbb{P}_{\text{guess}}(\mathbb{P}_{\rho\mathbf{n}_a\mathbf{n}_b}), \\ \mathbb{P}_{\text{guess}}(\mathbb{P}_{\rho\mathbf{n}_b}) &\geq \mathbb{P}_{\text{guess}}(\mathbb{P}_{\rho\mathbf{n}_a\mathbf{n}_b}). \end{aligned} \tag{3.40}$$

From the discussions in Chapter 2, the BI in the Clauser, Horne, Shimony and Holt (CHSH) form is:

$$|\chi(\mathbf{n}_{a_1}, \mathbf{n}_{a_2}, \mathbf{n}_{b_1}, \mathbf{n}_{b_2})| \leq 2. \tag{3.41}$$

Consider now a pure state $|\psi\rangle$ of the form:

$$|\psi\rangle = \cos(\theta)|00\rangle + \sin(\theta)|11\rangle, \tag{3.42}$$

where the Schmidt decomposition is used. Clearly $|00\rangle$ and $|11\rangle$ represent vectors of a basis of $\mathscr{H}_A$ and $\mathscr{H}_B$ and $\theta \in [0, \pi/2]$. It can be proved that, for pure states of the kind of Equation 3.42 in the case of measurement of four observables $\mathbf{n}_{a_i} \cdot \sigma \otimes \mathbf{n}_{b_j} \cdot \sigma$ with $i, j = 1, 2$, $\chi(\mathbf{n}_{a_1}, \mathbf{n}_{a_2}, \mathbf{n}_{b_1}, \mathbf{n}_{b_2})$ is upper bounded[152] by:

[152]: Horodecki et al. (1995), 'Violating Bell inequality by mixed spin-12 states: necessary and sufficient condition'

$$\chi(\mathbf{n}_{a_1}, \mathbf{n}_{a_2}, \mathbf{n}_{b_1}, \mathbf{n}_{b_2}) \leq 2\sqrt{1 + \sin^2 2\theta}. \tag{3.43}$$

Such an inequality can be used to provide a bound on the angle $\theta$:

$$\cos^2(2\theta) \leq 2 - \chi^2/4. \tag{3.44}$$

By explicit computation of the expectation values of the operators $\{\mathbf{n}_{a_i} \cdot \sigma \otimes \mathbf{n}_{b_j} \cdot \sigma\}_{i,j=1,2}$, in the case of pure state of the form of Equation 3.42, it is possible to demonstrate that such a values are bounded by:

$$-\cos(2\theta) \leq \langle \mathbf{n}_{a_i} \cdot \sigma \otimes I_2 \rangle \leq \cos(2\theta), \tag{3.45}$$

$$-\cos(2\theta) \leq \langle I_2 \otimes \mathbf{n}_{b_j} \cdot \sigma \rangle \leq \cos(2\theta). \tag{3.46}$$

Now it is just necessary to recall that $\langle \mathbf{n}_{a_i} \cdot \sigma \otimes I \rangle = \mathbb{P}(+1|\psi, \mathbf{n}_a) - \mathbb{P}(-1|\psi, \mathbf{n}_a) = \mathbb{P}(+1|\psi, \mathbf{n}_a) - (1 - \mathbb{P}(+1|\psi, \mathbf{n}_a)$ to obtain:

$$\max_{x=\pm1} \mathbb{P}(x|\psi, \mathbf{n}_a) \leq \frac{1 + \cos(2\theta)}{2} \leq \frac{1}{2} + \frac{1}{2}\sqrt{2 - \chi^2/4}. \tag{3.47}$$

An analogous reasoning could be applied to $I \otimes \mathbf{n}_{b_j} \cdot \sigma$. Noticing that Equation 3.47 is independent on $\mathbf{n}_a$ is possible to write that:

$$\mathbb{P}_{\text{guess}}(\mathbb{P}_{\psi\mathbf{n}_a}) \leq \frac{1+\cos(2\theta)}{2} \leq \frac{1}{2} + \frac{1}{2}\sqrt{2-\chi^2/4} = f(\chi) \tag{3.48}$$

$$,\mathbb{P}_{\text{guess}}(\mathbb{P}_{\psi\mathbf{n}_b}) \leq \frac{1+\cos(2\theta)}{2} \leq \frac{1}{2} + \frac{1}{2}\sqrt{2-\chi^2/4} = f(\chi). \tag{3.49}$$

It is necessary to extend these bounds in the case of a generic state $\rho$, having a not-fixed dimensionality. Consider two operators $O^a$ and $O^b$ acting on $\rho$: if they have only the eigenvalues ±1 then, by using the Jordan lemma, it is possible to find a basis in which both operators are diagonal[30] . Moreover, the dimensionality of the blocks must be $\leq 2$. The same can be done to the unknown state $\rho$: by linearity, if $\rho = \sum_\lambda p_\lambda |\psi_\lambda\rangle\langle\psi_\lambda|$, then the observed probabilities $\mathbb{P}$ can be decomposed into the sum of the observed probabilities $\mathbb{P}_\lambda$ related to each $|\psi_\lambda\rangle\langle\psi_\lambda|$. The same reasoning can apply to the $\chi$-parameter:

[30]: Scarani (2019), *Bell nonlocality*

$$\chi = \sum_\lambda p_\lambda \chi_\lambda. \tag{3.50}$$

For any set of four realizations $\{(\rho, P_\pm^{\mathbf{n}_{a_i}}, P_\pm^{\mathbf{n}_{b_j}})\}_{i,j=1,2}$ having the same $\rho$ and providing the same value $\chi$, it results that:

$$\begin{aligned}\mathbb{P}_{\text{guess}}(\rho, \mathbf{n}_{a_i}, \mathbf{n}_{b_j}) &= \max_{p_\lambda,\psi_\lambda} \sum_\lambda p_\lambda \mathbb{P}_{\text{guess}}(\psi_\lambda, \mathbf{n}_{a_i}, \mathbf{n}_{b_j}) \\ &\leq \max_{p_\lambda,\psi_\lambda} \sum_\lambda p_\lambda \max_{\mathbf{n}_a} \mathbb{P}_{\text{guess}}(\psi_\lambda, \mathbf{n}_a) \quad (1) \\ &\leq \max_{p_\lambda,\psi_\lambda} \sum_\lambda p_\lambda f(\chi_\lambda) \quad (2) \\ &\leq \max_{p_\lambda,\psi_\lambda} f\left(\sum_\lambda p_\lambda \chi_\lambda\right) \quad (3) \\ &= \max_{p_\lambda,\psi_\lambda} f(\chi) \quad (4) \\ &= f(\chi).\end{aligned} \tag{3.51}$$

where

(1) is due to Equation 3.40,
(2) is due to Equation 3.49,
(3) is due to the concavity of the $f$ function,
(4) is due to the independence of $f$ respect to the $p_\lambda$ and to the two-qubit state $\psi_\lambda$.

Remarkably, $f(\chi)$ is independent of the particular realization $(\rho, P_\pm^{\mathbf{n}_{a_i}}, P_\pm^{\mathbf{n}_{b_j}})$ chosen. Consequently, the realization independent guessing probability can be bounded, using Equation 3.35, as

$$\mathbb{P}_{\text{guess}}(\mathbb{P}_{\rho\mathbf{n}_{a_i}\mathbf{n}_{b_j}}) \leq f(\chi) = \frac{1}{2} + \frac{1}{2}\sqrt{2 - \frac{\chi^2}{4}}, \tag{3.52}$$

which is valid for every choice of $i, j \in \{1,2\}$. The bound obtained in Equation 3.52 is valid also in the case of the marginal realization independent guessing probabilities:

$$\mathbb{P}_{\text{guess}}(\mathbb{P}_{\rho \mathbf{n}_a}) \leq f(\chi) = \frac{1}{2} + \frac{1}{2}\sqrt{2 - \frac{\chi^2}{4}}, \tag{3.53}$$

$$\mathbb{P}_{\text{guess}}(\mathbb{P}_{\rho \mathbf{n}_b}) \leq f(\chi) = \frac{1}{2} + \frac{1}{2}\sqrt{2 - \frac{\chi^2}{4}}. \tag{3.54}$$

It is important to notice that $f(\chi)$ is lower than 1 only for $\chi > 2$: for $\chi = 2$, $f(\chi) = 1$ and there exists a strategy for which the outcomes can be deterministically predicted. The violation of the BI is a necessary condition to extract a certain amount of randomness from the outcomes of the measurements in DI-QRNG.

## 3.7 Quantum random numbers generation based on SPE

In this section, it is described the SPE-based SDI-QRNG[21, 25]. The protocol of randomness certification is based on two key points: first, the violation of the BI using SPE of momentum and polarization and, second, the modeling of the non-idealities of the experimental setup. In particular, memory effects introduced by detectors and the polarization dependence of the optical components are considered here. Before starting to describe the protocol, it is useful to introduce all the assumptions on which it relies:

- the SDI-QRNG is in a safe place where no eavesdropper has ever entered[2] ;
- the provider of all the devices is not-malicious, but sell real, imperfect objects;
- a characterization of the non-idealities of the detectors is available;
- a characterization of the polarization non-idealities of the optical element of the Mach Zehnder Interferometer (MZI) is available;
- the generation and measurement parameters are stable during the acquisition time.

Under these assumptions, the eavesdropper can be identified as a person who has:

- classical side information about the experiment, in particular the decomposition of the involved state $\rho$ into pure states and the knowledge of the sequence of measurements that have to be performed;
- an unlimited computational power;
- a quantum description of the experiment.

The same protocol can provide robustness against errors in the system if one or more components suddenly stop working as expected. Clarified these points, the SPE state considered is of the kind given by Equation 2.19:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0V\rangle + |1H\rangle\right), \tag{3.55}$$

where momentum and polarization are defined analogously to what was done in Section 2.3 of Chapter 2.

[2] This assumption is required to avoid that any adversary has installed a malicious program or trojan horse to steal the generated sequence. This, indeed, would be a more effective, simpler and less detectable attack than deterministically controls any electrical and optical elements during the experiment.

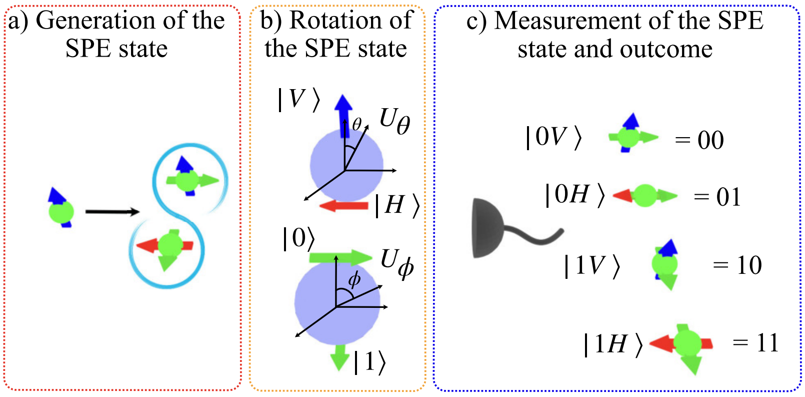


**Figure 3.10:** Protocol's steps to generate quantum random numbers: a) generate a SPE state of momentum and polarization; b) apply two unitary rotation operators $(U_\phi, U_\theta)$ to the SPE to rotate the two considered DoFs; c) project the rotated SPE state over the four basis vectors $(|0V\rangle, |1V\rangle, |0H\rangle, |1H\rangle)$ using SPADs and, depending in which state the wavefunction has collapsed, assign a couple of bits. Repeat the previous points many times to obtain a sequence of pairs of raw random numbers. Reprinted figure with permission from Nicolò Leone, Stefano Azzini, Sonia Mazzucchi, Valter Moretti, and Lorenzo Pavesi, "Certified Quantum Random-Number Generator Based on Single-Photon Entanglement", Physical Review Applied 17, 034011. Copyright 2022 by the American Physical Society.

It is necessary to remark that the use of such an entanglement is conceptually different to the use of Multi Particles Entanglement (MPE): the intrinsic randomness of outcomes is due to *contextuality* instead of *non-locality*[153] . A theory is considered contextual if, chosen two or more compatible observables, the result of one observable measurement is influenced by choice of the other observables to be measured on the same system. Note that all non-contextual realistic hidden variable theories are unable to explain the experiment's outcomes if a BI violation is observed[23, 154] . This impossibility is directly translated into the negation of one (or both) characteristics of the hidden variable theory: the latter has to be contextual and realist or non-contextual and non-realistic.[3]

Assuming contextuality in an experiment is as strange as accepting non-locality: both the situations are against the common intuition since it is straightforward to consider that distant objects cannot interact (non-locality) and that an object's property cannot change depending on which other properties of the object are considered (contextuality). What seems more reasonable is assuming that the theory is not realistic or, in other words, that the outcomes of a measurement are not predetermined. Note that standard quantum mechanics is a non-realistic, non-contextual theory. Therefore, the BI acts as a randomness witness: if a violation of the BI is observed, then the measurement outcomes are effectively random as stated by the quantum mechanical description.

Done this important consideration, it is time to analyze the QRNG based on SPE. Using SPE, the random numbers are generated accordingly to what schematized in Figure 3.10: every time a SPE state is generated (Figure 3.10a), separate rotations of the momentum (angle $\phi$) and polarization (angle $\theta$) are performed (Figure 3.10b). Then the rotated state is measured producing the outcome $(x, y)$, depending on in which state of the base $|0V\rangle, |1V\rangle, |0H\rangle, |1H\rangle$ the single photon has been detected. This procedure is repeated many times to accumulate a sequence of measurement outcomes. Note that the couple $(x, y)$ is stored as a binary number (Figure 3.10c) instead of the traditional values ±1 just for simplicity. An example of the time sequence of the detection events is reported in Figure 3.11. This scheme is implemented with the same optical setup reported in Figure 2.3 of Chapter 2.

[153]: Moretti (2019), *Fundamental Mathematical Structures of Quantum Theory*

[23]: Pasini et al. (2020), 'Bell-inequality violation by entangled single-photon states generated from a laser, an LED, or a halogen lamp'

[154]: Azzini et al. (2020), 'Single-Particle Entanglement'

[3] Even the case of a non-realist contextual theory could in principle work, but it is unfeasible.

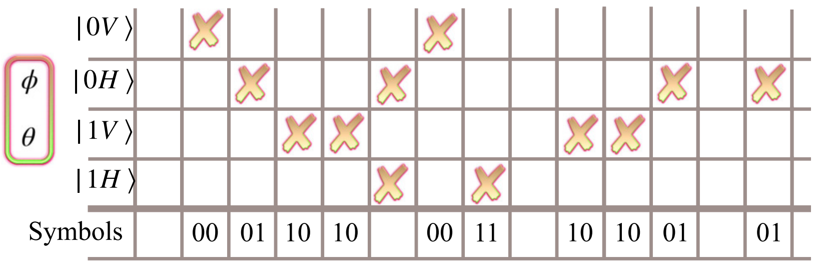


**Figure 3.11:** Example of the time trace of the detection events corresponding to the generated raw random number sequence. Fixed a couple of angles ($\phi$,$\theta$), the raw sequence is produced depending on which SPAD has detected the photon. Bits in which multiple detection events or no detection has been observed are discarded.

### 3.7.1 Protocol for entropy certification

From a practical point of view, the maximum amount of min-entropy is given when the four detection probabilities are equal. Indeed for $\{\mathbb{P}(x,y|\phi,\theta)=\frac{1}{4}\}_{x,y}$ the min-entropy is $H_{\min}=-\log_2\frac{1}{4}=2$: two bits of entropy are generated for each detection outcome. However, in this way, it is just implemented a more complex version of a BS-based QRNG, without exploiting the main feature of the SPE: the entanglement. As remarked in Chapter 2, in such an experiment, a violation of the BI can be observed and, consequently, used. The goal is to detect a sequence of outcomes for four couples of angles $\{(\phi_i,\theta_j)\}_{i,j=0,1}$ over which the CHSH is evaluated: if a violation is observed, the randomness of the results can be certified. Particular attention must be given to the non-idealities presented in the experimental setup (Section 2.7 in Chapter 2) that have to be considered in the protocol. The estimator $\hat{\chi}$ used to evaluate the CHSH violation is defined as:

$$\begin{aligned}&\hat{\chi}(\phi_0,\phi_1,\theta_0,\theta_1)=\\&=\hat{\mathbb{E}}\left(O^M_{\phi_0},O^P_{\theta_0}\right)-\hat{\mathbb{E}}\left(O^M_{\phi_0},O^P_{\theta_1}\right)+\hat{\mathbb{E}}\left(O^M_{\phi_1},O^P_{\theta_0}\right)+\hat{\mathbb{E}}\left(O^M_{\phi_1},O^P_{\theta_1}\right),\\&\hat{\mathbb{E}}\left(O^M_{\phi_i},O^P_{\theta_j}\right)=\hat{\mathbb{P}}(x=y|\phi_i,\theta_j)-\hat{\mathbb{P}}(x\neq y|\phi_i,\theta_j).\end{aligned} \tag{3.56}$$

$\{\hat{\mathbb{P}}\}$ are the probabilities obtained directly from the outcomes. When $\{\mathbb{P}\}$ are evaluated using four continuous acquisitions ( the couple of angles $(\phi_i,\theta_j)$ is kept constant ), the probabilities $\{\hat{\mathbb{P}}(x,y|\phi_i,\theta_j)\}$ must be computed using the Markov maximum likelihood estimators reported in Subsection 2.7.5 of Chapter 2, due to the presence of the memory effects introduced by the SPADs. Inserting $\hat{\chi}$ in the bound on the guessing probability of Equation 3.52, yields:

$$\mathbb{P}_{\text{guess}}(x,y|\phi_i,\theta_j)\leq\frac{1}{2}+\frac{1}{2}\sqrt{2-(|\hat{\chi}|)^2/4}. \tag{3.57}$$

The estimator $\hat{\chi}(\phi_0,\phi_1,\theta_0,\theta_1)$ has to be further corrected considering the polarization non-idealities of the optical components: the quantity $e_{\mathbb{P}}(e_\chi)$, which bounds the difference between the ideal probabilities($\chi$-parameter) and the real ones, obtainable with the real experimental setup, has to be introduced to estimate $\mathbb{P}_{\text{guess}}(x,y|\phi_i,\theta_j)$. Note that an important modification has to be made in the numerical evaluation of $e_{\mathbb{P}}$ and $e_\chi$: the state $\rho$, on which $e_{\mathbb{P}}$ and $e_\chi$ are calculated (see the numerical approach of Subsection 2.7.2 in Chapter 2), has to be modelled as the most general density matrix in the two qubits space, since the bounds must be independent on the form of the input state. To model a general semi-definite density matrix $\rho$, the Cholesky decomposition[155] is used:

[155]: Loan (1996), *Matrix computations(3rd ed.)*

$$\rho = (\Theta_1 + i\Theta_2)^\dagger(\Theta_1 + i\Theta_2) \tag{3.58}$$

where $\Theta_1$ and $\Theta_2$ are

$$\begin{aligned}\Theta_1 &= \begin{pmatrix} x_1 & x_5 & x_8 & x_{10} \\ 0 & x_2 & x_6 & x_9 \\ 0 & 0 & x_3 & x_7 \\ 0 & 0 & 0 & x_4 \end{pmatrix}, \\ \Theta_2 &= \begin{pmatrix} 0 & x_{11} & x_{14} & x_{16} \\ 0 & 0 & x_{12} & x_{15} \\ 0 & 0 & 0 & x_{13} \\ 0 & 0 & 0 & 0 \end{pmatrix},\end{aligned} \tag{3.59}$$

and $\{x_i\}_{i=1..16}$ are the spherical 16-dimensional coordinates. These can be fixed as:

$$\begin{aligned} x_1 &= r\cos(\eta_1), \\ x_2 &= r\cos(\eta_2)\sin(\eta_1), \\ x_3 &= r\cos(\eta_3)\sin(\eta_2)\sin(\eta_1), \\ x_4 &= r\cos(\eta_4)\sin(\eta_3)\sin(\eta_2)\sin(\eta_1), \\ x_5 &= r\cos(\eta_5)\sin(\eta_4)...\sin(\eta_1), \\ &... \\ x_{15} &= r\cos(\eta_{15})\sin(\eta_{14})...\sin(\eta_1), \\ x_{16} &= r\sin(\eta_{15})...\sin(\eta_1). \end{aligned} \tag{3.60}$$

where r is the radius and $\{\eta_i\}_{i=1..15}$ are 15 angles. To ensure that $\rho$ is normalized, the radius r has to be fixed to 1. Lastly, to obtain a positive semi-definite matrix, the diagonal terms $x_1, x_2, x_3$ and $x_4$ has to be positive: by restricting the domains of the angles $\{\eta_i\}_{i=1..4}$ to $[0, \pi/2]$ the goal is achieved. The other angles have to be chosen between $[0, \pi]$ except for the last angle $\eta_{15}$, that is free in $[0, 2\pi]$. This model allows to obtain the two state-independent bounds $e_{\mathbb{P}}, e_\chi$ using the same numerical approach[4] reported in Subsection 2.7.2 in Chapter 2. Thus, as long as these bounds are satisfied, Equation 3.57 becomes

$$\mathbb{P}_{\text{guess}}(x, y|\phi_i, \theta_j) \leq \frac{1}{2} + \frac{1}{2}\sqrt{2 - (|\hat{\chi}_{\text{real}}| - e_\chi)^2/4} + e_{\mathbb{P}} := p_{\text{bound}}. \tag{3.61}$$

Note that it is necessary to further correct this bound re-introducing the Markov model: calling $\mathbb{P}^*_{\text{guess}}(a, b|\phi_x, \theta_y)$ the Markov corrected guessing probability, the final bound is obtained as:

$$\mathbb{P}^*_{\text{guess}}(x, y|\phi_i, \theta_j) \leq \mathbb{M}\left(p_{\text{bound}}\right), \tag{3.62}$$

where $\mathbb{M}$ is a function derived by the Markov model. This model was initially used to estimate the probabilities for the evaluation of the $\chi$-parameter. The estimated $\hat{\chi}_{\text{real}}$ is then used to determine the bound $p_{\text{bound}}$ on the guessing probability as reported in Equation 3.61. $p_{\text{bound}}$, however, corresponds to a bound for the guessing probability of a sequence of independent identically distributed variables for which the $\chi$-parameter $\hat{\chi}_{\text{real}}$ is observed. The hypothesis of independent identically distributed variables does not apply to this SDI-QRNG since the produced raw numbers are correlated due to memory effects. Therefore, the Markov

[4] The use of the analytic approach (Subsection 2.7.2 in Chapter 2.) into the calculation of $e_{\mathbb{P}}, e_\chi$ is still possible, but it implies the introduction of further assumptions on the state $\rho$. Moreover, it provides two bounds that are less precise than the numerical approach. Due to these reasons, since the goal of a QRNG is usually to maximize the achievable randomness with the least assumptions, only the numerical approach will be then considered.

model has to be reapplied. $p_{\text{bound}}$ has to be modified considering the detector's non-idealities: in the presence of such correlations, indeed, the guessing probability corresponds to the maximum value of the probability of the $n_{th}$-readout $\xi_n$ given the previous ones[25] :

[25]: Leone et al. (2022), 'Certified Quantum Random-Number Generator Based on Single-Photon Entanglement'

$$\mathbb{P}^*_{\text{guess}} := \sup_{i_0,\ldots,i_n} \mathbb{P}(\xi_n = i_n | \xi_{n-1} = i_{n-1}, \ldots \xi_0 = i_0). \tag{3.63}$$

The same notation of Subsection 2.7.5 of Chapter 2 is used: in particular, $T_d$ is the dead time of the detectors, $p_a$ is the afterpulsing probability, $\lambda_e$ is the effective flux of photons considered, $P_{i,j}$ is the transition probability of the Markov model and $i, j = 1, 2, 3, 4$ indicates the possible four outcomes of the measurement operation. Using the Markov property, this reduces to

$$\begin{aligned} \mathbb{P}^*_{\text{guess}} &= \sup_{i,j} P_{ij} = \\ &\sup_{i,j} \left(p_a \delta_{ij} + (1-p_a)\left((1-\lambda_e T_d)p_j + \lambda_e T_d q_{ij}\right)\right). \end{aligned} \tag{3.64}$$

By using the inequality $\sup_j p_j \leq p_{\text{bound}}$, eventually it is possible to obtain $\mathbb{P}^*_{\text{guess}} \leq \mathbb{M}(p_{\text{bound}})$, where the function $\mathbb{M}$ is defined as:

$$\begin{aligned} &\mathbb{M}(p_{\text{bound}}) := \\ &\sup_{\substack{i,j=1,\ldots,4 \\ p_j \leq p_{\text{bound}}}} \left(p_a \delta_{ij} + (1-p_a)\left((1-\lambda_e T_d)p_j + \lambda_e T_d q_{ij}\right)\right) \\ &= \max\left\{p_a + (1-p_a)\left((1-\lambda_e T_d)p_{\text{bound}} + \right.\right. \\ &\left.\left.\lambda_e T_d p^2_{\text{bound}}\right), (1-p_a)(p_{\text{bound}} + \lambda_e T_d p_{\text{bound}}(1-p_{\text{bound}}))\right\}. \end{aligned} \tag{3.65}$$

Estimated $\mathbb{P}^*_{\text{guess}}$, the $H^*_{\min}$ for each measurement outcome is calculated as:

$$H^*_{\min} = -\log_2\left[\mathbb{P}^*_{\text{guess}}(x, y|\phi_i, \theta_j)\right], \tag{3.66}$$

and the min-entropy of the whole sequence $R$ as:

$$\begin{aligned} H_{\min}(R|S) &= nH^*_{\min} \\ &= -n \log_2\left[\mathbb{P}^*_{\text{guess}}(x, y|\phi_i, \theta_j)\right]. \end{aligned} \tag{3.67}$$

$S$ is the sequence of the input angle $(\phi_i, \theta_j)$, known by the adversary.

### 3.7.2 Introducing more assumptions on the input state

It was discussed how the bound obtained in Equation 3.62 is independent of the particular form of $\rho$ in the two qubits space. However, it is interesting to evaluate also a situation in which the state $\rho$, obtained by the generation stage of Figure 2.3, has a different form, with respect to $\rho = |\phi^+\rangle\langle\phi^+|$, only due to experimental defects or erroneous calibration of the optical components. In this situation, $\rho$ can be described as:

$$\rho(\eta, \delta, \pi_1, \pi_2) = R(\pi_1, \pi_2)\rho_s(\eta, \delta)R(\pi_1, \pi_2)^\dagger. \tag{3.68}$$

$R(\pi_1, \pi_2)$ represents unwanted rotations of the two HWPs, shown in Figure 3.12, by the angles $\pi_1 \in [0, 2\pi]$ and $\pi_2 \in [0, 2\pi]$. Its explicit matrix

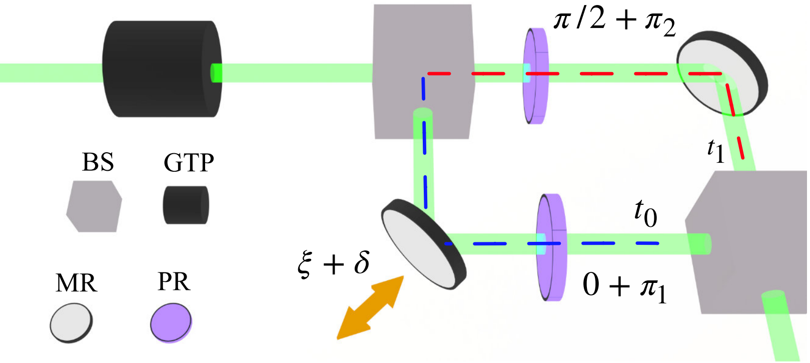


**Figure 3.12:** Details of non-idealities of the optical components in the generation stage of Figure 2.3. Respectively $\delta$ is an additional phase-shift between the two paths, while $\pi_1$ and $\pi_2$ are additional angles of rotation of the HWPs with respect to the nominal values of $\pi/2$ and 0. Instead, $t_0$ and $t_1$ are the transmission coefficients of the blue dashed ($|0\rangle$) and red dashed ($|1\rangle$) paths already introduced in Subsection 2.7.2 in Chapter 2. Reprinted figure with permission from Nicolò Leone, Stefano Azzini, Sonia Mazzucchi, Valter Moretti, and Lorenzo Pavesi, "Certified Quantum Random-Number Generator Based on Single-Photon Entanglement", Physical Review Applied 17, 034011. Copyright 2022 by the American Physical Society.

description is given by:

$$R(\pi_1,\pi_2) := \begin{pmatrix} \cos(\pi_1) & \sin(\pi_1) & 0 & 0 \\ -\sin(\pi_1) & \cos(\pi_1) & 0 & 0 \\ 0 & 0 & \cos(\pi_2) & \sin(\pi_2) \\ 0 & 0 & -\sin(\pi_2) & \cos(\pi_2) \end{pmatrix}. \tag{3.69}$$

$\rho_s(\eta,\delta)$ represents the entangled state:

$$\rho_s(\eta,\delta) = \eta\left(|\psi(\delta)\rangle\langle\psi(\delta)|\right) + \frac{1-\eta}{4}I_4, \tag{3.70}$$

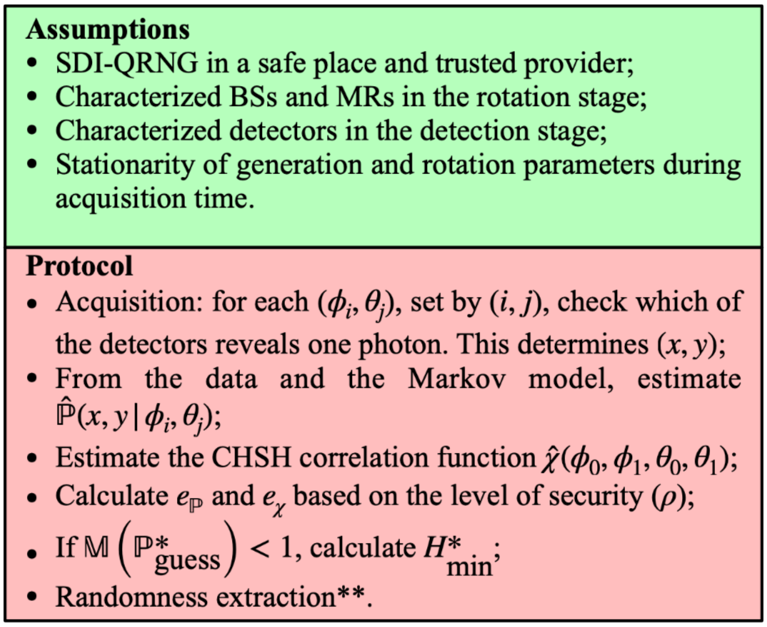
where $\eta \in [0,1]$ is the visibility parameter and $\delta \in [0,2\pi]$ is an additional relative phase. $|\psi(\delta)\rangle$ is defined as:

$$|\psi(\delta)\rangle := \left(t_{0n}e^{i\delta}|0V\rangle + t_{1n}|1H\rangle\right) \tag{3.71}$$

and $I_4$ is the identity matrix. The coefficients $t_{0n}$ and $t_{1n}$ represent the normalized amplitude transmission coefficients of the optical paths $|0\rangle$ and $|1\rangle$ (see Figure 3.12) already introduced in Subsection 2.7.2 in Chapter 2. The matrix representation of $\rho_s(\eta,\delta)$ is given by:

$$\rho_s(\eta,\delta) = \begin{pmatrix} \eta|t_{0n}|^2+(1-\eta) & 0 & 0 & \eta t_{0n}e^{i\delta}(t_{1n})^* \\ 0 & 1-\eta & 0 & 0 \\ 0 & 0 & 1-\eta & 0 \\ \eta(t_{0n}e^{i\delta})^*t_{1n} & 0 & 0 & \eta|t_{1n}|^2+(1-\eta) \end{pmatrix}. \tag{3.72}$$

The different values of the parameters $\pi_1,\pi_2,\delta,\eta$ could be due to erroneous calibrations of the optical devices in the generation stage of Figure 2.3. Having introduced such a $\rho$ model, now the two bounds $e_{\mathbb{P}}$ and $e_\chi$ can be recalculated by considering the parameters $\pi_1,\pi_2,\delta,\eta$ as known from the experimental values or free to vary in the respective domains. The introduction of additional hypotheses on $\rho$ represents a way to increase the min-entropy lowering the bounds $e_{\mathbb{P}}$ and $e_\chi$ with respect to the most general situation. Such an increment comes at the price of having a less secure QRNG, since every time a parameter is fixed, an additional assumption, or, in other words, a new possible way to cheat the QRNG is introduced. The final users of the QRNG can indeed decide



**Assumptions**

- SDI-QRNG in a safe place and trusted provider;
- Characterized BSs and MRs in the rotation stage;
- Characterized detectors in the detection stage;
- Stationarity of generation and rotation parameters during acquisition time.

**Protocol**

- Acquisition: for each $(\phi_i, \theta_j)$, set by $(i, j)$, check which of the detectors reveals one photon. This determines $(x, y)$;
- From the data and the Markov model, estimate $\hat{\mathbb{P}}(x, y \mid \phi_i, \theta_j)$;
- Estimate the CHSH correlation function $\hat{\chi}(\phi_0, \phi_1, \theta_0, \theta_1)$;
- Calculate $e_{\mathbb{P}}$ and $e_{\chi}$ based on the level of security $(\rho)$;
- If $\mathbb{M}\left(\mathbb{P}^*_{\text{guess}}\right) < 1$, calculate $H^*_{\text{min}}$;
- Randomness extraction**.

**Figure 3.13:** Resume of the assumptions and the steps of the SDI-QRNG.(**The randomness extraction procedure is not a necessary step to certificate the $H^*_{\text{min}}$ but a requirement to have a fully working SDI-QRNG).

the level of security for the QRNG based on their level of trust. Figure 3.13 resumes the entire protocol for the generation of the quantum random numbers.

Note that the hypotheses of the SPE-based SDI-QRNG are similar to the ones of the typical SI-SDI-QRNGs[19, 121] : in all these protocols, the input state is left under the eavesdropper's control. What differs is the measurement operations: in a typical SI-SDI-QRNG, the measurement observables have to be perfectly characterized. On the contrary, in the proposed SPE-based SDI-QRNG, only a partial characterization of the measurement apparatus is necessary, without any assumptions on the forms of the observables. Indeed, the certification scheme is independent of the specific product forms of the operators that have to be measured.

[121]: Marangon et al. (2017), 'Source-Device-Independent Ultrafast Quantum Random Number Generation'
[19]: Avesani et al. (2018), 'Source-device-independent heterodyne-based quantum random number generator at 17 Gbps'

## 3.8 Experimental validation of the SDI-QRNG

### 3.8.1 Experimental setup

To validate the model of the SDI-QRNG, an experiment is set up and performed: the whole experimental setup is reported in Figure 3.14. The same optical setup of Section 2.8 of Chapter 2 is used. An attenuated single-mode CW green He:Ne laser is used as the light source. The laser emits at 543.5 nm with a nominal power of 4 mW. The laser is fiber-coupled and attenuated through a variable optical attenuator (VOA). For every polarization angle $\theta_{0,1}$ set on the two HWPs, the angle $\phi$ is continuously varied, changing the voltage $V$ applied to a Piezoelectric transducer (PZT) over which is mounted one of the mirrors (Figure 2.3) of the MZI. The obtained experimental data points (empty squares in Figure 3.15) are fitted (solid lines in Figure 3.15) and used to obtain the calibration curve $\phi(V)$. Obtained the latter, four angles that yields a

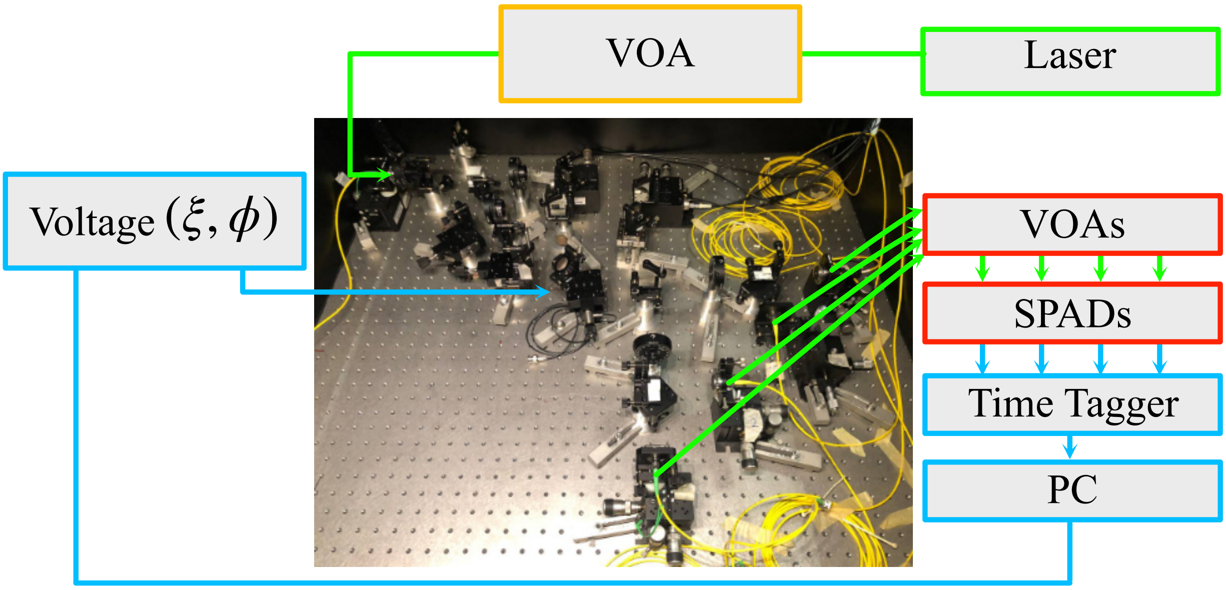


**Figure 3.14:** Experimental setup used to generate certified quantum random numbers. A green arrow indicates the optical signal, while the electrical signal is shown with a cyan arrow. Color code of the boxes: green, source, orange, VOA used to attenuate the laser source, red, detection elements (VOAs and SPADs), cyan, electrical components used to control the phases $\xi$ and $\phi$ and to store the data obtained (PC and Time Tagger). With respect to the experimental setup reported in Figure 2.14 only the laser source is used and the FPGA is substituted by the Time Tagger. The details of the optical setup are reported in Figure 2.14b.

**Table 3.3:** Typical values for the dead time $T_d$, afterpulsing probability $p_a$ and dark count rate for the SPADs. Reprinted table with permission from Nicolò Leone, Stefano Azzini, Sonia Mazzucchi, Valter Moretti, and Lorenzo Pavesi, "Certified Quantum Random-Number Generator Based on Single-Photon Entanglement", Physical Review Applied 17, 034011. Copyright 2022 by the American Physical Society.

| | $T_d$ [ns] | $p_a$[%] | DCRHz |
|---|---|---|---|
| SPAD | 22 | 0.5 | < 100 |

maximal violation of the BI are chosen: $\phi_0 = \frac{3}{8}\pi$, $\phi_1 = \frac{5}{8}\pi$,$\theta_0 = 0$ and $\theta_1 = \frac{\pi}{4}$. For each couple of angles $(\phi_x, \theta_y)$, a 50 seconds time sequence of single photon detection events is acquired by using a Time Tagger, interfaced with the PC, with a time-bin of 1 $\mu$s. This time bin value was chosen to discriminate between two subsequent detection events, i.e., the time bin is lower than the typical time between two photons detection events ($\frac{1}{\lambda_e} \simeq 5\mu$s), and to have a time sequence which can be stored in a standard PC memory. Since the values of the dead time, afterpulsing probability and Dark count rate (DCR) represent essential parameters for the Markov model, their typical values for the used SPADs, as provided by the manufacturer, are reported in Table 3.3.

### 3.8.2 Results

For the 50 s of the acquisition time, the measured count rates are reported as solid dots inside the green boxes in Figure 3.15 and the numbers of counts in Table 3.4. Note that time bins in which multiple photons have been detected are neglected and discarded in post-processing. These events are due to the emission statistics of the laser and constitute the

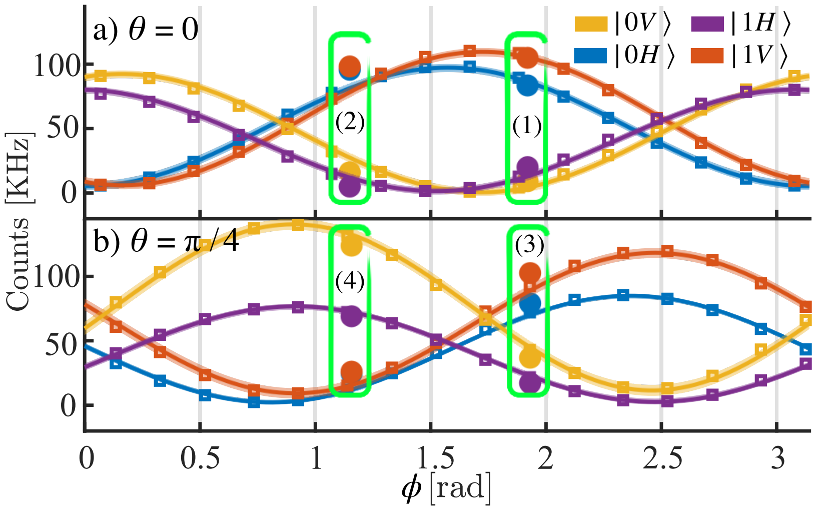


**Figure 3.15:** Experimental count rates acquired (empty squares and solid dots) and fits as a function of $\phi$ for a) $\theta = 0$, and b) $\theta = \frac{\pi}{4}$. The color-code: yellow $|0V\rangle$, purple $|1H\rangle$, blue $|0V\rangle$ and red $|1V\rangle$. The sinusoidal fits are reported as solid lines with the respective 99%−confidence intervals (shaded area). The experimental points corresponding to the 50 s long data acquisitions are circled in green: (1) corresponds to $(\phi_1, \theta_0)$, (2) to $(\phi_0, \theta_0)$, (3) to $(\phi_1, \theta_1)$ and (4) to $(\phi_0, \theta_1)$. The corresponding total count rates are reported with solid dots. Reprinted figure with permission from Nicolò Leone, Stefano Azzini, Sonia Mazzucchi, Valter Moretti, and Lorenzo Pavesi, "Certified Quantum Random-Number Generator Based on Single-Photon Entanglement", Physical Review Applied 17, 034011. Copyright 2022 by the American Physical Society.

| Channel | $(\phi_0, \theta_0)$(2) | $(\phi_1, \theta_0)$(1) | $(\phi_0, \theta_1)$(4) | $(\phi_1, \theta_1)$(3) |
|---|---|---|---|---|
| $\|0V\rangle$ | 643132 | 371255 | 4754594 | 1426837 |
| $\|1H\rangle$ | 202823 | 779771 | 2589956 | 652294 |
| $\|0H\rangle$ | 3804170 | 3311003 | 964121 | 3078159 |
| $\|1V\rangle$ | 3855004 | 4108774 | 996276 | 3945250 |
| Total | 8505129 | 8570803 | 9304947 | 9102540 |

**Table 3.4:** Experimental counts acquired during the whole 50 s acquisition time window. The counts are reported for each experimental set of angles $\{(\phi_i, \theta_j)\}_{i,j=0,1}$, respectively labelled as $\{(k)\}_{k=1,2,3,4}$ respect to the green boxes of Figure 3.15. Reprinted table with permission from Nicolò Leone, Stefano Azzini, Sonia Mazzucchi, Valter Moretti, and Lorenzo Pavesi, "Certified Quantum Random-Number Generator Based on Single-Photon Entanglement", Physical Review Applied 17, 034011. Copyright 2022 by the American Physical Society.

12.0 ± 0.4% of the entire raw data. The same occurs for the time bin in which no photons are detected.

Figure 3.16 shows the raw probabilities $\mathbb{P}(x, y|\phi_i, \theta_j)$ estimated from the raw data considering a time interval of 10 ms. The data are noisy, but this is not an issue because the protocol is robust under this type of non-idealities. In Table 3.5 are reported the average raw probabilities estimated considering a time interval of 10 s. A $\sigma \simeq 0.2\%$ standard deviation is calculated for these raw probabilities. Between parenthesis, in Table 3.5 there are also the probabilities $\hat{\mathbb{P}}(x, y|\phi_i, \theta_j)$ estimated using the Markov model. As it is possible to observe, the correction due to the memory effects on the probabilities is negligible in this situation since it is within the standard deviation of the measurements. The $\chi$-parameter estimator $\hat{\chi}$ is calculated using the probabilities $\hat{\mathbb{P}}(x, y|\phi_i, \theta_j)$, for which it is obtained:

$$|\hat{\chi}(\phi_0, \phi_1, \theta_0, \theta_1)| = 2.656 \pm 0.003. \tag{3.73}$$

Considering the setup non-idealities, in the most general scenario, i.e., for a $\rho$ with no constrains, the two correction terms result to be $e_{\mathbb{P}} = 0.080 \pm 0.002$ and $e_{\chi} = 0.332 \pm 0.008$[5] . These are obtained applying the numerical method, since it provides more precise, i.e., smaller, correction terms. Following Equation 3.62 and Equation 3.66 these values certify a conditional min-entropy for bit of $H^*_{min} = (2.5 \pm 0.5)\%$. If this value is compared to the case where no correction is necessary, i.e., $e_{\chi} = e_{\mathbb{P}} = 0$ a conditional min entropy of $H^*_{\text{min}} = (42.8 \pm 0.4)\%$ is obtained: the

[5] The correctness of these and the future numerical bounds is verified as in Section 2.8 of Chapter 2.

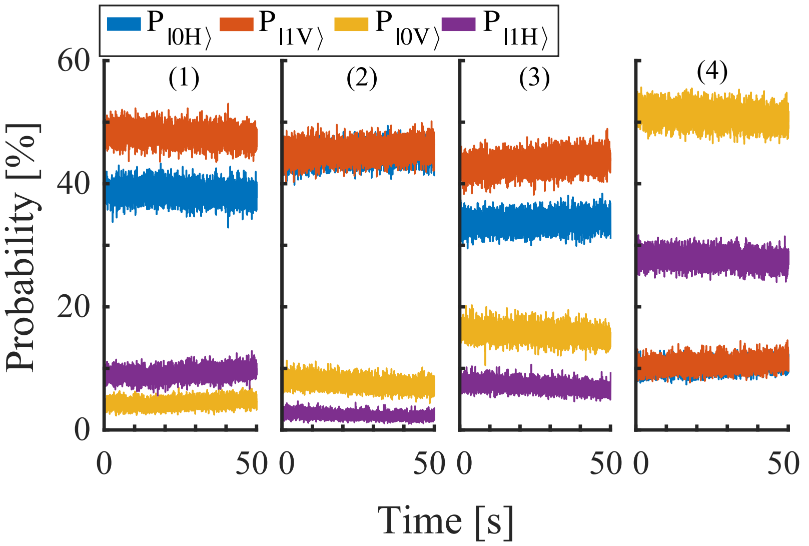


**Figure 3.16:** Raw probabilities $\mathbb{P}$ estimated from the raw data considering a time interval of 10 ms for each measurement outcome. Yellow corresponds to $|0V\rangle$, purple to $|1H\rangle$, blue to $|0V\rangle$ and red to $|1V\rangle$. The latter are reported for the four working points Markov(1), (2), (3), (4) of Figure 3.15 and Table 3.4, corresponding to $(\phi_1, \theta_0)$, $(\phi_0, \theta_0)$, $(\phi_1, \theta_1)$, $(\phi_0, \theta_1)$. Reprinted figure with permission from Nicolò Leone, Stefano Azzini, Sonia Mazzucchi, Valter Moretti, and Lorenzo Pavesi, "Certified Quantum Random-Number Generator Based on Single-Photon Entanglement", Physical Review Applied 17, 034011. Copyright 2022 by the American Physical Society.

**Table 3.5:** Raw probabilities and corrected probabilities estimated over the raw data. For each mean values of the experimental ($\mathbb{P}$) probabilities, the corresponding Markov maximum-likehood estimator ($\hat{\mathbb{P}}$) is reported within parenthesis. This is done for each couple of angles $\{(\phi_x, \theta_y)\}_{x,y=0,1}$ and outcomes. The difference between the raw and maximum-likehood probabilities is within the estimated error $\simeq$ 0.2%. In the columns header, between parenthesis, there is reported the number which refers to the measurement points shown in Figure 3.15. Reprinted table with permission from Nicolò Leone, Stefano Azzini, Sonia Mazzucchi, Valter Moretti, and Lorenzo Pavesi, "Certified Quantum Random-Number Generator Based on Single-Photon Entanglement", Physical Review Applied 17, 034011. Copyright 2022 by the American Physical Society.

| Channel | $(\phi_0, \theta_0)$(2) | $(\phi_1, \theta_0)$(1) | $(\phi_0, \theta_1)$(4) | $(\phi_1, \theta_1)$(3) |
|---|---|---|---|---|
| $\lvert 0V\rangle$ | 7.6(7.6) | 4.3(4.3) | 51.1(51.1) | 15.7(15.7) |
| $\lvert 1H\rangle$ | 2.4(2.4) | 9.1(9.1) | 27.8(27.8) | 7.2(7.2) |
| $\lvert 0H\rangle$ | 44.7(44.7) | 38.6(38.6) | 10.4(10.4) | 33.8(33.8) |
| $\lvert 1V\rangle$ | 45.3(45.3) | 47.9(48.0) | 10.7(10.7) | 43.3(43.4) |

**Table 3.6:** Values of min-entropy $H^*_{\text{min}}$ and random bits throughput for different modelling of the source $\rho$. For each level the value of $e_{\mathbb{P}}, e_\chi$ are obtained by the numerical approach. Accordingly, the min-entropy $H^*_{\text{min}}$ is calculated using Equation 3.66. From the value of the min-entropy, the random bit throughput is estimated from the total number of data acquired divided by the effective time of acquisition (200 s) assuming an instantaneous extraction procedure. To clarify the four level in the first column there are the free parameters of the model, while in the second column, there are the parameters fixed using the actual values measured in the experimental implementation. In particular, in the second row the value of $t_{0n}, t_{1n}$ are fixed using the value reported in Table 2.1 following Equation **??** and Equation **??** of Subsection 2.7.2 in Chapter 2. In the third row, $\pi_1$ and $\pi_2$ are fixed as $\pi_1 = \pi_2 = 0$, while in the fourth row, $\delta = 0$. Reprinted table with permission from Nicolò Leone, Stefano Azzini, Sonia Mazzucchi, Valter Moretti, and Lorenzo Pavesi, "Certified Quantum Random-Number Generator Based on Single-Photon Entanglement", Physical Review Applied 17, 034011. Copyright 2022 by the American Physical Society.

| Variable | Fixed | $e_{\mathbb{P}} \cdot 10^{-2}$ | $e_\chi \cdot 10^{-2}$ | $H^*_{\text{min}}$ | Random bits generation rate [kHz] |
|---|---|---|---|---|---|
| $\rho$ general | - | $8.0 \pm 0.2$ | $33.2 \pm 0.8$ | $(2.5 \pm 0.5)\%$ | 4.4 |
| $\delta, \pi_1, \pi_2, \eta$ | $t_{0n}, t_{1n}$ | $8.0 \pm 0.2$ | $26.4 \pm 0.8$ | $(6.3 \pm 0.6)\%$ | 11.0 |
| $\delta, \eta$ | $t_{0n}, t_{1n}, \pi_1, \pi_2$ | $7.8 \pm 0.2$ | $1.2 \pm 0.2$ | $(26.9 \pm 0.5)\%$ | 47.1 |
| $\eta$ | $t_{0n}, t_{1n}, \pi_1, \pi_2, \delta$ | $6.6 \pm 0.2$ | $0.26 \pm 0.07$ | $(30.1 \pm 0.5)\%$ | 52.7 |

non-idealities have decreased its value of approximately one order of magnitude. A more ideal optical setup could be used in a future implementation to increase the amount of certified min-entropy. Since in the previous sections, it was demonstrated that the upper bound on $\mathbb{P}_{\text{guess}}(a, b|x, y)$ represents also a bound for the marginal guessing probability, e.g., $\mathbb{P}_{\text{guess}}(b|y) = \max \sum_a \mathbb{P}_{\text{guess}}(a, b|x, y)$ it is possible to use only one DoF to label each outcome $(x, y)$. Each photon observed with vertical polarization is, then, labeled with $y = 0$ while $y = 1$ is used to label each photon detected with horizontal polarization, independently of their momentum. Since during the experiment a total amount of $\simeq 35{\times}10^6$ raw data are acquired in 200 s, assuming a perfect randomness extraction procedure, $\simeq 0.88 \times 10^6$ random bits can be certified, corresponding to a certified generation rate of about ≃ 4.4 kHz. Introducing the assumptions about the input state $\rho$, as discussed in Subsection 3.7.2, corresponds to an increment of the min-entropy. The same maximization procedure is then performed only on the non-fixed parameters of the input state $\rho$. The results are reported in Table 3.6. As expected, the min-entropy increases as more parameters are known. In particular, four levels of trust of the input state are considered. When all the parameters are fixed, except for the visibility $\eta$[6] the min-entropy results to be $H^*_{min} = (30.1 \pm 0.5)\%$. This represents the best scenery for the min-entropy, while it is the worst concerning security. Intermediate situations can be reached by letting other parameters free: if the phase $\delta$ is let free to vary, a value of min-entropy of $H^*_{min} = (26.9 \pm 0.5)\%$ is estimated. Lastly, the two HWPs of Figure 3.12 can in any positions introducing the angle $\pi_1$ and/or $\pi_2$. This yields to $H^*_{min} = (6.3 \pm 0.6)\%$.

[6] This case is the one used to correct the experimental value of $\chi$ reported in Chapter 2

### 3.8.3 Discussion of results

The experimental results obtained in this section confirm that a SDI-QRNG based on SPE states of momentum and polarization is feasible: the simple experimental setup combined with the accurate modeling of the optical elements and the detectors is enough to certify a violation of the BI and the presence of randomness using imperfect devices, providing a kHz generation rate that goes from 4.4 kHz to 52.7 kHz. This SDI-QRNG represents a trade-off between the security offered by the DI-QRNGs and the easiness of implementation of DD-QRNGs allowing to a secure and simple generation of certified random numbers. Indeed, the experimental implementation is simpler compared to traditional DI-QRNGs: no separate detection stages are required and no coincidence measurements have to be performed to test the BI and generate random numbers. Moreover, an initial random seed is not required.

To compare the demonstrated SPE-based SDI-QRNG with the other works in the literature, three parameters will be discussed: security, velocity and possibility of integration. The simplicity of the physical implementation is here not considered since, in general, all the SDI-QRNGs of Table 3.1 are simple to be implemented. Concerning the security, this QRNG is more secure than a typical SI SDI-QRNG (see Table 3.1), where the measurement apparatus is totally characterized. Indeed, in the SPE-based SDI-QRNG, the measurements are only partially characterized: the certification scheme is independent of the particular product forms of the operators that have to be measured. Moreover, the introduced assumptions are necessary to keep the experimental implementation simple. Without this requirement, such a QRNG can aspire to be a fully DI-QRNG being based on entanglement. Just by only introducing more efficient detectors and the random input seed will enhance the protocol's security, removing the assumption of stationarity and the fair sampling assumption. Concerning the velocity, it is worth stressing that the obtained random number generation rate is not remarkable compared to other SDI-QRNG that can reach MHz or GHz velocities (see Table 3.1). However, velocity is not the primary goal of this proof of principle experiment, which was conceived to demonstrate that SPE can be used to generate certified quantum random numbers. A further comment can be added about the velocity: the only limiting factor to the generation rate is the dead-time of the SPADs, which caps the maximal achievable rates to ≃ few MHz before detectors saturation. A simple solution consists of using multiple SPADs, a SiPM, as a detector for every single channel: such solution can be suitable to further increase the velocity of the QRNG to tens of MHz. Supposing to have an ideal SiPM composed of ten cells illuminated uniformly, it is possible to estimate that the max achievable rate before saturation will be increased by ten times, obtaining a ten times faster SDI-QRNG. Lastly, the proposed protocol is particularly interesting concerning the possibility of integration. Thanks to the ability to generate SPE states starting from incoherent sources like LEDs, the proposed SDI-QRNG can be fully integrated on a silicon photonic chip, where only the detectors are off-chip, even though some works about the integration of SPADs in photonic chips has appeared[156, 157] . The integration of SPE will be the main discussion of the next chapter. Most of the MHz/GHz rate SDI-QRNGs[122, 134, 158] are based on homodyne or heterodyne detection, two techniques that rely on the use of a laser source in their scheme. Even if the system is fully integrable[134], the integration of a laser source is less economically favorable than the integration of an LED source. For this reason, the proposed SDI-QRNG results to be more suitable for all those applications that necessitate having low production costs, like Internet of Things devices.

[156]: Martinez et al. (2017), 'Single photon detection in a waveguide-coupled Ge-on-Si lateral avalanche photodiode'
[157]: Bernard et al. (2021), 'Top-down convergence of near-infrared photonics with silicon substrate-integrated electronics'

[122]: Avesani et al. (2018), 'Source-device-independent heterodyne-based quantum random number generator at 17 Gbps'
[158]: Avesani et al. (2021), 'Semi-Device-Independent Heterodyne-Based Quantum Random-Number Generator'
[134]: Rusca et al. (2020), 'Fast self-testing quantum random number generator based on homodyne detection'

# Single Photon Entanglement on an integrated optical chip 4

The aim of this chapter is to describe a photonic chip able to generate Single Photon Entanglement (SPE) states. Even though the bulk components can be encapsulated in a smaller device ($\simeq$ dm$^2$) than the implemented bulk version ($\simeq$ m$^2$), a better approach consists of rethinking the implementation and building it using integrated photonics ($\simeq$ mm$^2$). Integrated silicon photonics allows mass manufacturable optical devices, significantly reducing cost and dimension and, so, facilitating the disposability of such products. Optical Quantum Random Number Generators (QRNGs) are categories of quantum devices that can surely benefit from the integration. Indeed, despite being considered more secure than Pseudo-Random Number Generators (PRNGs) and True Random Number Generators (TRNGs), the high cost of such devices has slowed down their spread. Integration could resolve this problem and provide cost-effective QRNGs: indeed, many research groups have focused their attention on integrated QRNGs[68–73, 75, 77, 94–98, 134].

Considering SPE, in the previous chapters only momentum and polarization Degrees of Freedom (DoFs) were used to produce SPE states since they can be easily manipulated using bulk optics. However, polarization is difficult to tune in integrated photonics, although some solutions have already been proposed and implemented[159] . For these reasons, an approach based on Hidden Subsystems of Path (HSP)[160] is proposed and exploited in a fashion similar to traditional gate based quantum computing. In this chapter firstly the key photonics components (waveguides, Multi-Mode Interferometer (MMI), Crossing (CR), Phase shifter (PS) and Mach Zehnder Interferometer (MZI)) are presented. Introduced these concepts, the ideal structure of the integrated optical chip is detailed. Each optical component is simulated, given the optical properties of the material, to find the correct geometrical parameters for the selected working wavelength. The produced optical chip is then experimentally characterized to verify that each photonic device behaves as expected. Lastly, the test of the Bell's Inequality (BI) is performed.

[159]: Li et al. (2019), 'Multimode silicon photonics'

[160]: Moretti (2019), *Fundamental Mathematical Structures of Quantum Theory*

## 4.1 Required optical integrated components

### 4.1.1 Optical waveguides

The optical waveguide is the essential element of every optical circuit: it is where the photons are confined and travel. It is composed of two parts: the core and the cladding. The cladding has a refractive index $n_1$, lower than the refractive index of the core medium, $n_2$. The light propagates in the core layer if the waveguide is appropriately designed. A typical example of a channel waveguide is reported in Figure 4.1. The waveguide's physical working principle is the total internal reflection: the light coupled inside the waveguide's core propagates being reflected

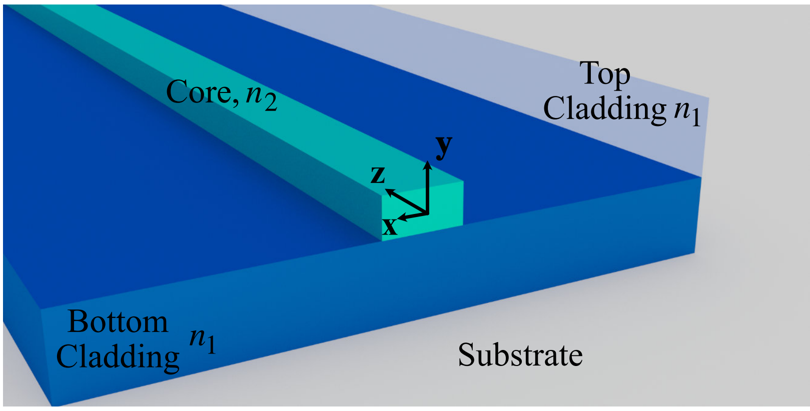


**Figure 4.1:** Example of a channel waveguide. The core material (cyan) has a refractive index $n_2$, while the cladding material has a refractive index $n_1$ (blue, bottom cladding, light transparent blue, top cladding). The top cladding material is nearly transparent to highlight the waveguide structure. The light propagates in the z-direction. The core and the cladding are deposited over a material called the substrate (grey).

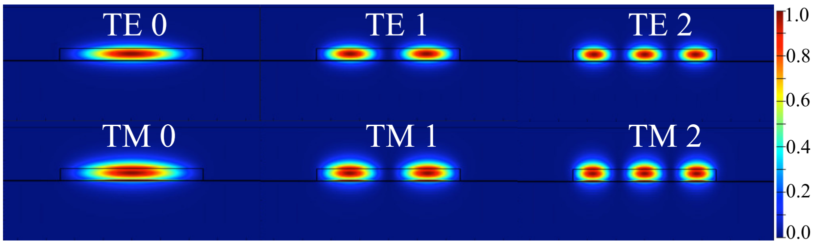


**Figure 4.2:** Example of the intensity profile $|E_x|^2 + |E_y|^2$ for the first three modes of a channel waveguide for the two polarizations TE and TM.

by the surfaces of the core, which act like mirrors. For the orientation of the electrical and magnetic fields, it is possible to define two linear polarizations: Transverse electric (TE) and Transverse magnetic (TM). TE is the polarization in which the electric field is oriented in the $x$-direction. On the contrary, the TM polarization has the magnetic field oriented in the $x$-direction. By imposing boundary conditions and solving the wave equation, their solutions are the propagating optical modes with a specific wavevector $\beta_m$ and a field profile $u_m(x, y)$. Moreover the two polarizations, TE and TM have different modes[161] . An example of the mode profile $u_m(x, y)$ for TE and TM polarizations is reported in Figure 4.2. Given the waveguide geometrical parameters, the modal wavevectors $\{\beta_{p,m}\}$, where $p$ indicates the polarization and $m$ the mode number, are found with numerical approaches using softwares like Comsol Multiphysics[162] and Lumerical[163] . In particular, from the simulations, the effective modal indexes $\{n_{\text{eff}_{(p,m)}}\}$ are found. $n_{\text{eff}_{(p,m)}}$ is a complex number: its real part is connected to the wavevector $\beta_{(p,m)}$ as:

[161]: Saleh et al. (2019), *Fundamentals of photonics*

[162]: Multiphysics (2021), *Comsol Multiphysics Comsol Multiphysics main page*
[163]: Lumerical (2021), *Ansys / Lumerical Lumerical main page*

$$\beta_{(p,m)} := \frac{2\pi\,\text{Re}\left[n_{\text{eff}_{(p,m)}}\right]}{\lambda}, \tag{4.1}$$

while its imaginary part is related to losses. The attenuation coefficient $\alpha$ is defined as:

$$\alpha_{(p,m)} := \frac{2\pi\,\text{Im}\left[n_{\text{eff}_{(p,m)}}\right]}{\lambda}. \tag{4.2}$$

The effective index $n_{\text{eff}_{(p,m)}}$ depends on the properties of the materials, on the geometry of the structure, on the wavelength and on the polarization. Obtained the modal structure, each field propagating in the waveguide is a superposition of different modes[161] :

[161]: Saleh et al. (2019), *Fundamentals of photonics*

$$E_p(x, y, z) = \sum_{m=0}^{M} c_{p,m} u_{p,m}(x, y) e^{-i\beta_{p,m} z}, \tag{4.3}$$

where $E_p(x, y, z)$ is a generic electric field and $\{c_{p,m}\}$ are coefficients related to how much the $m$ mode is excited given a certain input profile of light $s_p(x, y)$. The coefficients $\{c_{p,m}\}$ are computed from the overlap integral:

$$c_{p,m} := \int_A s_p(x, y)u(x, y)_{p,m}\mathrm{d}A \tag{4.4}$$

where $A$ is the area of the section of the waveguide[1] . From Equation 4.4, if the input light is polarized, it is impossible to excite modes of the other polarization.

To provide a historical perspective on how the SPE was planned to be generated on the optical chip, it is possible to observe that the structure of the modes can be easily considered as a DoF suitable to replace the polarization. Different modes are indeed orthogonal between each other[161] , i.e., $\langle u_{p,n}|u_{p,m}\rangle = \delta_{n,m}$ for two modes $m$ and $n$. Moreover, the geometry of the waveguide can be tailored to support only two modes for a certain polarization, creating a qubit system: the photon propagates in one mode or the other. The generation of an entangled state of momentum and mode of propagation can then be achieved by exploiting an integrated optical component called asymmetric directional coupler[126] . Such a component can be used to convert one mode into another, exploiting the evanescent coupling of two near waveguides[161] . The main difficulty of using modes is their manipulation. This task is far to be trivial[164] and an incredible precision in the lithographic process is required, implying the use of electron-beam lithography[165] . An additional difficulty is caused by the difference between the two modes' wavevectors $\beta_m$ and $\beta_n$. This introduces an increasing relative phase difference between the two modes during the propagation. For those reasons, this option was not considered as the primary solution for implementing SPE on the integrated photonic chip.

[161]: Saleh et al. (2019), *Fundamentals of photonics*

[126]: Li et al. (2019), 'Quantum random number generation with uncharacterized laser and sunlight'

[161]: Saleh et al. (2019), *Fundamentals of photonics*

[164]: Mohanty et al. (2017), 'Quantum interference between transverse spatial waveguide modes'

[165]: Bojko et al. (2011), 'Electron beam lithography writing strategies for low loss, high confinement silicon optical waveguides'

### 4.1.2 Multi-Mode Interferometer (MMI) and Crossing (CR)

A Multi-Mode Interferometer (MMI) is a device composed of $N$ identical waveguides as input that inject light into a wide waveguide supporting many modes. After the wide waveguide, there are $M$ output waveguides. By tuning the structure's geometry, it is possible to obtain a considerable amount of transformations by exploiting the concept of multimode interference. In particular, in the case $N = M = 2$, it is possible to obtain a $50 : 50$ integrated Beam Splitter (BS). An example of this structure is reported in Figure 4.3. To better describe the behavior of such an integrated object, the work of [166] is illustrated, since it provides a quite intuitive picture. Consider the situation reported in Figure 4.4, in which the multimode waveguide is long $L$ and has a width $W$. By using the effective index method[167] , the 3D-geometry can be effectively approximated using a 2D geometry where the $y$ coordinate has collapsed. An effective refraction index is assigned to each 2D element to "emulate" its 3D optical properties. These effective indexes are called $n_{\text{clad}} \neq n_1$ for the cladding material and $n_{\text{mw}} \neq n_2$ for the multimode waveguide. The input light injected in the multimode waveguide comes from the waveguide centered in $(x^*, 0)$. As discussed before, the different modes of a multimodal waveguide are excited depending on the overlap between

[166]: Soldano et al. (1995), 'Optical multi-mode interference devices based on self-imaging: principles and applications'

[167]: Knox et al. (1970), 'Integrated circuits for the millimeter through optical frequency range'

[1] The definition of overlap integral reported in Equation 4.4 assumes normalized quantities.

the input spatial profile and the supported mode profiles. In particular, Equation 4.3 can be rewritten as:

$$E_p(x^*, 0, z) = e^{-i\beta_0 z} \sum_{m=0}^{M} c_{p,m} u_{p,m}(x^*, 0) e^{i(-\beta_{p,m}+\beta_0)z} \tag{4.5}$$

where it was factorized the phase term $e^{-i\beta_0 z}$. It can be demonstrated that[166] :

[166]: Soldano et al. (1995), 'Optical multi-mode interference devices based on self-imaging: principles and applications'

$$\beta_0 - \beta_m = \frac{m(m+2)\pi}{3L_\pi} \tag{4.6}$$

where $L_\pi$ is called the beating length between the two lowest order modes:

$$L_\pi \simeq \frac{4n_{mw}W}{3\lambda}. \tag{4.7}$$

Inserting Equation 4.6 into Equation 4.5 is possible to obtain that:

$$E_p(x^*, 0, z) = e^{-i\beta_0 z} \sum_{m=0}^{M} c_{p,m} u_{p,m}(x^*, 0) e^{i(\frac{m(m+2)\pi}{3L_\pi})z}. \tag{4.8}$$

By observing that for $z = 3L_\pi$, $e^{i(\frac{m(m+2)\pi}{3L_\pi})z} = (-1)^m$, Equation 4.8 can be rewritten as:

$$E_p(x^*, 0, 3L_\pi) = e^{-i\beta_0 3L_\pi} \sum_{m=0}^{M} c_{p,m}(-1)^m u_{p,m}(x^*, 0). \tag{4.9}$$

An important property of the modes is that for $m$ even the mode is even, while for $m$ odd the mode is odd respect to the $x$ coordinate, so it is possible to absorb the term $(-1)^m$ into the term $u_{p,m}(x^*, 0)$ by just changing the sign of $x^*$:

$$E_p(x^*, 0, 3L_\pi) = e^{-i\beta_0 3L_\pi} \sum_{m=0}^{M} c_{p,m} u_{p,m}(-x^*, 0) = e^{-i\beta_0 3L_\pi} E_p(x^*, 0, 0), \tag{4.10}$$

obtaining a copy of $E_p(x^*, 0, 0)$ in the location $(-x^*, 0, 3L_\pi)$. Now repeating the same reasoning for $z = 6L_\pi$, it is possible to attain, apart from the phase factor, an exact copy of the input field at the position $(x^*, 0, 3L_\pi)$. It is interesting to observe what happens for $z = 3/2L_\pi$. For such a length, $E_p(x^*, 0, z = 3/2L_\pi)$ becomes

$$E_p(x^*, 0, 3/2L_\pi) = \frac{1-i}{2} E_p(x^*, 0, 0) + \frac{1+i}{2} E_p(-x^*, 0, 0) \tag{4.11}$$

which is the quadrature representation of a signal having an amplitude of $\frac{1}{\sqrt{2}}$. In this way, an MMI can be used as an integrated structure that implement the matrix transformation of a BS[168] .

[168]: Peruzzo et al. (2011), 'Multimode quantum interference of photons in multiport integrated devices'

A Crossing (CR) is a device that is used when one or more waveguides have to cross each other. They are designed using as a building block the MMIs: an example is reported in Figure 4.5. The aim of the CR is to enable the crossing of two waveguides without inducing a coupling between the light that propagates in each of them. A near unitary transmission coefficient and low crosstalk between the different waveguides are desired for these devices. Such parameters are obtained exploiting the physical principle of the MMI. Consider the situation of Figure 4.5: by making

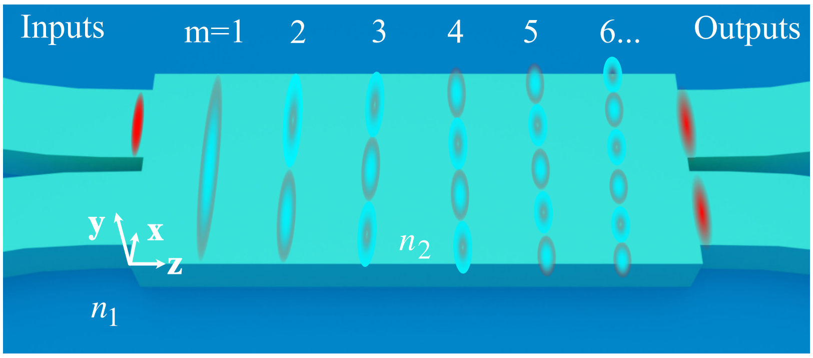


**Figure 4.3:** Example of a 2 × 2 Multi-Mode Interferometer (MMI). The MMI is reported in cyan, while in blue is reported the bottom cladding material, while the top cladding is transparent to highlight the structure of the MMI. The multimode waveguide has a refractive index $n_2$ while the cladding has a refractive index $n_1$. A certain amount of light (red spot) is injected into the multimode waveguide from the inputs. Since the modal profile of the input waveguide is not perfectly matched with the profiles of the different modes supported by the wider waveguide, many of them are excited. The propagation of such modes allows obtaining an interference pattern at a certain distance from the input. In this example, the optical power is equally divided into the two output waveguides (red spots at the output ports). An example of the first six horizontal mode profiles supported by the wider waveguide is also reported. The phase relation between the different lobes of each mode is highlighted by the inversion of the transparency of the color: if the transparent part is at the edge of the lobe, it has a positive relative phase, while negative in the other case.

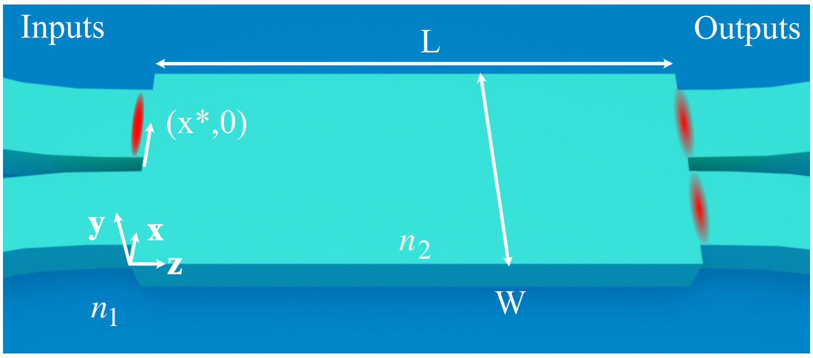


**Figure 4.4:** Geometry parameters and refractive indexes of a 2 × 2 MMI. The MMI is reported in cyan, while in blue is reported the bottom cladding material, while the top cladding is transparent to highlight the structure of the MMI. The multimode waveguide has a refractive index $n_2$ while the cladding has a refractive index $n_1$. It has a width $W$ and a length $L$. The input light comes from the waveguide at the position $(x^*, 0)$.

the self-image of the input mode in the center of the CR, it is possible to minimize the crosstalk with the other waveguide since the light is confined at the center. Moreover, by placing the output port symmetrically to the input port, it is also ensured that the light is transmitted without suffering significant losses[169] .

[169]: Zhang et al. (2013), 'Ultralow-loss silicon waveguide crossing using Bloch modes in index-engineered cascaded multimode-interference couplers'

### 4.1.3 Phase shifter (PS)

Another device needed is the Phase shifter (PS). In integrated optics, it is possible to realize integrated PS exploiting the thermo-optic coefficient of the waveguide material[170] . In particular, the thermo-optic coefficient gives the variation of the refractive index of a material induced by a variation of its temperature. Specifically:

[170]: Komma et al. (2012), 'Thermo-optic coefficient of silicon at 1550 nm and cryogenic temperatures'

$$\Delta n_{\text{eff}} = \frac{dn}{dT}\Delta T, \tag{4.12}$$

where $\frac{dn}{dT}$ is the thermo-optic coefficient. To realize the PS, a metallic wire is placed on top of the waveguide at a distance large enough not to

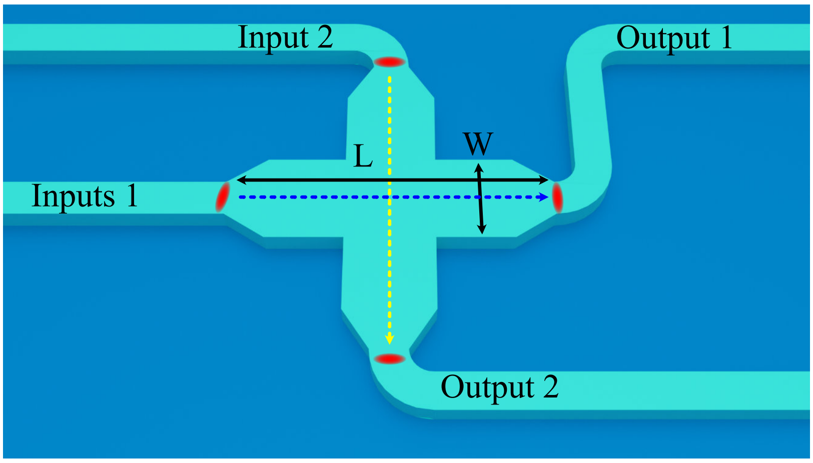


**Figure 4.5:** Example of a Crossing (CR) based on the MMI. The CR is designed in order to have a nearly unitary transmission coefficient respect to the blue and green paths, minimizing the crosstalk between the perpendicular waveguides.

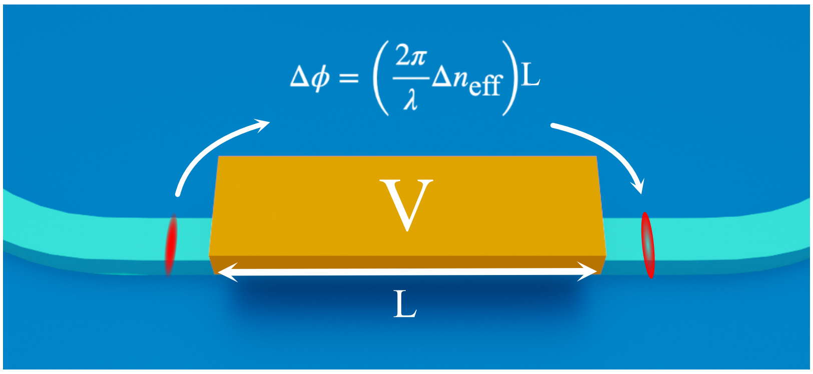

$\Delta\phi = \left(\frac{2\pi}{\lambda}\Delta n_{\text{eff}}\right)\text{L}$
V
L

**Figure 4.6:** Example of an integrated Phase shifter (PS). In cyan is reported the waveguide, while in blue is reported the bottom cladding material. The top cladding material is removed to emphasize the internal structure of the PS. In orange, there is the metal wire used to induce the phase shift: applying the voltage $V$, the phase shift $\Delta\phi = \left(\frac{2\pi\Delta n_{\text{eff}}}{\lambda}\right) L$ is induced by the variation of temperature $\Delta T$ achieved by heating the waveguide due to Joule effect. The variation of phase is represented by the inversion of the transparency of the color of the red circle, representing the light that passes under the PS.

increase the propagation losses. Making a current flow in the wire, due to the Joule effect, its temperature increases, which heats the waveguide. Therefore, an optical beam that travels in the waveguide suffers a phase shift given by:

$$\Delta\phi = \left(\frac{2\pi\Delta n_{\text{eff}}}{\lambda}\right) L = \left(\frac{2\pi}{\lambda}\frac{dn}{dT}\Delta T\right) L \tag{4.13}$$

where L is the waveguide length covered by the metallic wire. Since the wire width is only narrowed on the waveguide, it is only there where its resistance is large. Therefore, the voltage applied to the wire mostly drops in this region. Figure 4.6 shows an example of a PS.

### 4.1.4 Mach Zehnder Interferometer (MZI)

The Mach Zehnder Interferometer (MZI) is composed of two BSs, made by two 50 : 50 MMIs and two optical waveguides coupled with two PSs (Figure 4.7). Their matrix representations are:

$$U_{\text{MMI}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \quad U_{\text{Ph}(\phi_1,\phi_2)} = \begin{pmatrix} e^{2i\phi_1} & 0 \\ 0 & e^{2i\phi_2} \end{pmatrix}. \tag{4.14}$$

Consequently, the matrix of the integrated MZI is given by:

$$U_{\text{MZI}}(\phi_1,\phi_2) = ie^{i(\phi_1+\phi_2)}\begin{pmatrix} \sin(\phi_1-\phi_2) & \cos(\phi_1-\phi_2) \\ \cos(\phi_1-\phi_2) & -\sin(\phi_1-\phi_2) \end{pmatrix}. \tag{4.15}$$

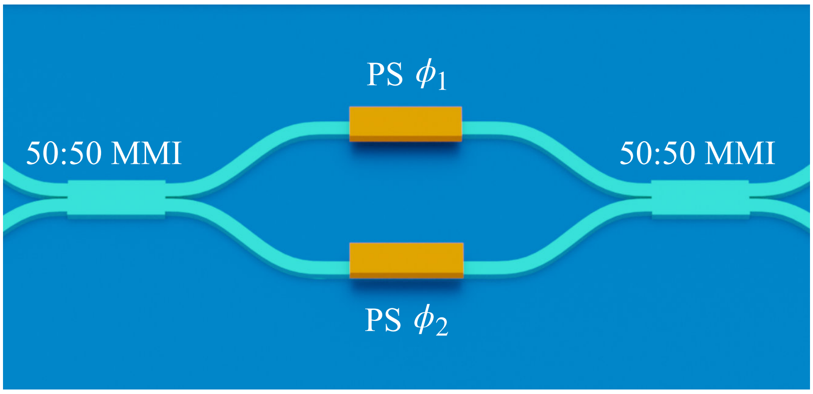


**Figure 4.7:** Example of an integrated Mach Zehnder Interferometer (MZI). In cyan, there are reported the waveguides that compose the integrated structure, while in blue is reported the bottom cladding material. The top cladding material is removed to emphasize the internal structure of the MZI. In orange, there are reported the PSs necessary to induce the phase shift $\phi_1$ and $\phi_2$ due to the thermo-optic effect.

The PSs are controlled applying the voltages $V_1$ and $V_2$ to the metal heaters represented as the orange rectangles in Figure 4.7. It is interesting to observe that for $\phi_1 = \phi_2 = 0$ the MZI implements the SWAP operation, apart for a global phase $\frac{\pi}{2}$:

$$\begin{pmatrix} 0 \\ i \end{pmatrix} = i \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{4.16}$$

$$\begin{pmatrix} i \\ 0 \end{pmatrix} = i \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{4.17}$$

## 4.2 Hidden Subsystems of Path (HSP)

In the HSP, the qubits are encoded using path encoding[171, 172] . Now consider a path encoded system composed of four waveguides: the corresponding state ($|0\rangle$, $|1\rangle$, $|2\rangle$ or $|3\rangle$) is determined by identifying in which waveguide the photon is coupled and propagates (Figure 4.8a). The Hilbert space is $\mathcal{H} = \mathbb{C}^4$. Indeed, the four states identified by the waveguides are mutually orthogonal: the overlap between every two pairs of waveguides is zero. Considering two straight waveguides $a$ and $b$, if the separation between the two waveguides is large enough, the overlap integral between the modes of the waveguide $a$ and the modes of $b$ is zero:

$$\int_A u^a_{p,m} u^b_{p,m'} \mathrm{d}x\mathrm{d}y = 0, \tag{4.18}$$

where $u^c_{p,i}$ is the $i$-th mode profile of the waveguide $c$ for polarization $p$. Therefore, the photon has a zero probability of hopping into waveguide $b$ if it is confined in $a$.

[171]: Silverstone et al. (2014), 'On-chip quantum interference between silicon photon-pair sources'
[172]: Wang et al. (2018), 'Multidimensional quantum entanglement with large-scale integrated optics'

Such a system can be turned into a $\mathbb{C}^2 \times \mathbb{C}^2$ by introducing a symmetry plane. Consider the dashed white line in Figure 4.8b: it is possible to relabel the different states $|0\rangle$, $|1\rangle$, $|2\rangle$ or $|3\rangle$ using as two "DoFs" the relative position and the absolute position of each waveguide with respect to the line. For the absolute position, it is meant in which portion of the space the waveguide is: if it is above(under) the line, it is labeled as up(down) $|U\rangle(|D\rangle)$. On the contrary, for the relative position, it is considered the distance at which the waveguide is respect to the line: the waveguides $|1\rangle$ and $|2\rangle$ ($|0\rangle$ and $|3\rangle$) are nearer(farther) to the line than the other two waveguides so that they can be labeled as $|N\rangle(|F\rangle)$. Contrary to the case of momentum and polarization DoFs, the use of such labels is purely artificial: indeed, another possible relabeling of the states $|0\rangle$, $|1\rangle$, $|2\rangle$ and $|3\rangle$ could be achieved by converting the decimal number $\{i\}_{i=1..4}$ to its direct binary form, forming now the state $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$. This situation can be interpreted as considering two times the absolute position as reported in Figure 4.8c: for the first qubit, it is considered the absolute position to the already introduced white dashed line, while, for the second qubit, the absolute position with respect to the black dashed line. It can be proven that such a choice defines two independent subsystems in the overall space $\mathscr{H} = \mathbb{C}^4$: the two subsystems can be identified as $\mathscr{H}_A = \mathbb{C}^2$ and $\mathscr{H}_R = \mathbb{C}^2$, for the situation of Figure 4.8b and $\mathscr{H}_{A_1} = \mathbb{C}^2$ and $\mathscr{H}_{A_2} = \mathbb{C}^2$ for the situation of Figure 4.8c. The subscript $A$ stands for absolute, while $R$ for relative. In the following discussion, it will be given just a qualitative justification for the situation of Figure 4.8b since the same reasoning can be applied directly to the case of Figure 4.8c. For a formal justification, which relies on Von Neumann's algebra, the reader is referred to [160] . To compose a quantum system $\mathscr{H} = \mathbb{C}^4$ starting from two Hilbert spaces $\mathscr{H}_i = \mathbb{C}^2$ of two independent qubits labelled as $a$ and $b$, it is necessary to ensure at least three properties:

[160]: Moretti (2019), *Fundamental Mathematical Structures of Quantum Theory*

1) each element of the two qubits system must have a representation in the composed Hilbert space: $\forall O_c \in \mathscr{H}_c, \exists \overline{O} \in \mathscr{H}$, with $c \in \{a, b\}$;
2) the elements of the two qubit system must be compatible: $\forall O_i \in \mathscr{H}_a, \forall O_j \in \mathscr{H}_b, O_i O_j = O_j O_i$;
3) for each couple of states belonging to the two qubits quantum systems, there must exist a state, in the composed space, for which the measurement on the single qubit space are reproduced by a composed operator acting on the state: $\forall \rho_a, \rho_b, \exists O, O' \in \mathscr{H}_a \otimes \mathscr{H}_b | \operatorname{Tr}\left[\rho O\right] = \operatorname{Tr}\left[\rho_a O_a\right] \wedge \operatorname{Tr}\left[\rho O'\right] = \operatorname{Tr}\left[\rho_b O_b\right]$.

These three properties are naturally satisfied using the tensor product. This approach can be considered as a bottom-up methodology: the composed system is formed by combining the two qubits systems. Interestingly, it can also be done the reverse, which is a sort of top-down approach. In the $\mathscr{H} = \mathbb{C}^4$ system, suppose that it is possible to group together two sets of operators $\{O_{A,i}\}$ and $\{O_{B,j}\}$. If every observable $O_{A,i}$ and $O_{B,j}$ can be written in a suitable basis as:

$$\begin{aligned} O_{A,i} &:= \begin{pmatrix} O_{a,i} & 0 \\ 0 & O_{a,i} \end{pmatrix}, \\ O_{B,j} &:= \begin{pmatrix} \alpha_j I_2 & \beta_j I_2 \\ \gamma_j I_2 & \delta_j I_2 \end{pmatrix}, \quad O_{b,j} := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \end{aligned} \tag{4.19}$$

where $I_2$ is the $2 \times 2$ identity matrix, then the two set $\{O_{a,i}\}$ and $\{O_{b,j}\}$ represent two independent subsystems $\mathscr{H}_A$ and $\mathscr{H}_B$ of the general, more complex $\mathscr{H}$. Moreover, these two are both $\mathbb{C}^2$. Conceptually, having the two operator $O_{A,i}$ and $O_{B,i}$ a structure that is identical to the usual tensor product between two observables, the properties 1), 2) and 3) are satisfied. Having recovered a structure analogous to the case of the two independent qubits, the Bell's Inequality (BI) can be tested without any problem. As introduced in Chapter 2, it is just necessary to rotate the two different qubits and then to project them on their basis. A clarification has to be done concerning the definition of SPE: in Chapter 2 the SPE is identified as the entanglement between distinct DoFs of the same photon. This definition seems contradictory concerning the approach HSP. For

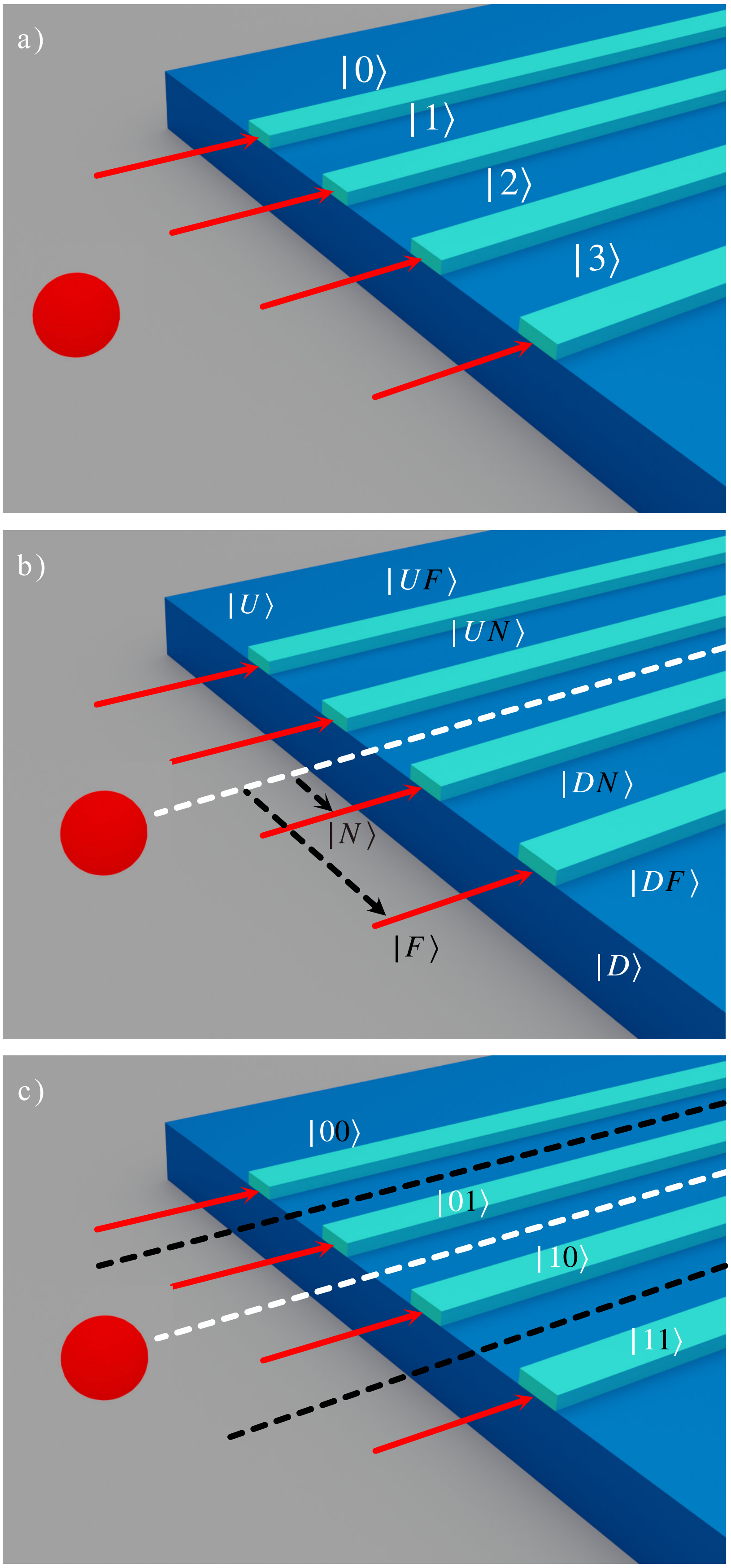


**Figure 4.8:** Example of path encoding using four waveguides. The red dot represents the photon, while in cyan, the waveguide core and in blue the cladding. a) The encoded state, $|0\rangle$, $|1\rangle$, $|2\rangle$ or $|3\rangle$ is chosen by coupling the photon in the corresponding waveguide. b) Alternative encoding based on HSP: the encoding is done by coupling the photon in the selected waveguide, but two qubits now describe the system. Respectively the two qubits are encoded depending on the excited waveguide position: the absolute position with respect to the dashed white line fixes the first qubit (up $|U\rangle$ and down $|D\rangle$), while the relative position with respect to the same line fixes the second qubit (far $|F\rangle$ and near $|N\rangle$). c) Alternative two-qubit encoding based on HSP: the encoding scheme is based now on two absolute positions: absolute position of the excited waveguide with respect to the dashed white line (first qubit, up $|0\rangle$ and down $|1\rangle$) and on the absolute position of the excited waveguide respect to the black lines (second qubit, up $|0\rangle$ and down $|1\rangle$).

this reason, it is necessary to redefine it as the entanglement between two distinct DoFs or two independent and compatible subsystems of the same DoF of a single photon.

## 4.3 Implementation of SPE on chip

In this section the integrated circuit to generate, rotate and detect the SPE based on HSP is discussed.

The ideal design of the integrated optical chip is reported in Figure 4.9. The dashed white line refers to the symmetry plane to which the DoFs are referred. The input light is injected into the chip using a tapered optical fiber, schematized by a glass cone in Figure 4.9 on the left. Then, a 50 : 50 MMI is used to split the light into two waveguides. Since the waveguides correspond to the state $|UF\rangle$ and $|DN\rangle$, the written state is:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|UF\rangle + i|DN\rangle\right). \tag{4.20}$$

Two PSs are then used to compensate the $\frac{\pi}{2}$ relative phase. Their action on the state is:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(e^{i\xi_1}|UF\rangle + ie^{i\xi_2}|DN\rangle\right), \tag{4.21}$$

where $\xi_1$ is controlled by the PS applied to $|UF\rangle$ and $\xi_2$ by the PS applied to $|DN\rangle$. By properly setting these phases, it is possible to obtain the states:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|UF\rangle + |DN\rangle\right) = |\phi^+\rangle, \tag{4.22}$$

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|UF\rangle - |DN\rangle\right) = |\phi^-\rangle, \tag{4.23}$$

apart from global irrelevant phase terms. After being generated, the state goes through the rotation stage. The qubit of relative position is rotated by an angle $\phi = \phi_1 - \phi_2$ using two MZI that works in parallel. At the output, the photon is distributed on the four waveguides (four states) according to $\phi$. Then, the qubit of absolute position is rotated by using two MZI that work in series: first, the near components are rotated by an angle $\theta = \theta_1 - \theta_2$, while the far components are just transmitted. Then, after that, two CRs swap the relative position components, another MZI rotates the far part of the state by the same angle $\theta$. The matrix representations of these operations are:

$$\begin{aligned} U(\phi_1, \phi_2) &= I_2 \otimes U_{\text{MZI}}(\phi_1, \phi_2), \\ U(\theta_1, \theta_2) &= U_{\text{MZI}}(\theta_1, \theta_2) \otimes I_2. \end{aligned} \tag{4.24}$$

Note that for design limitations, the CRs are used to perform the rotation of the qubit of absolute position. Their action will be essentially neglected, just remembering that the $|F\rangle$ and $|N\rangle$ components are exchanged in the detection stage (note the ordering of the state in the red box of Figure 4.9). The detection stage is constituted by an array of fibers coupled to the four waveguides. These fibers are connected to four SPADs used to measure the photon on the state basis $|UN\rangle$, $|UF\rangle$, $|DF\rangle$ and $|DN\rangle$. A

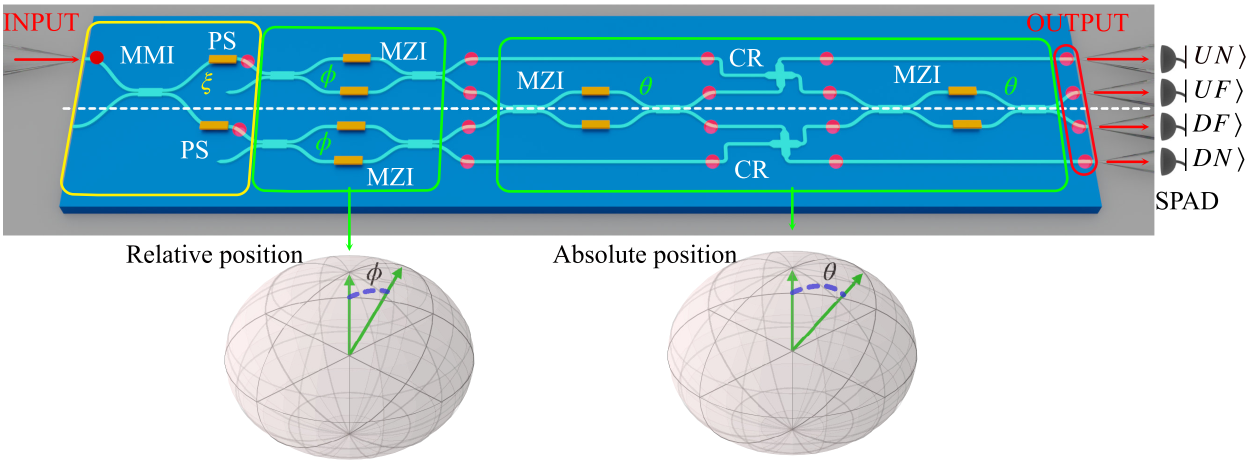


**Figure 4.9:** Schematic of the integrated optical chip for the testing of the BI for the SPE in the HSP version. The optical waveguides are reported in cyan and the box cladding is in blue. The top cladding is transparent to emphasize the structure. The light is coupled in the optical chip from the left using a taper optical fiber (left glass cone). The first stage (yellow box) is the generation stage in which the entangled state is created. The two separate rotation stages act on the two HSP (green boxes): the first two MZIs rotate the qubit of relative position by the angle $\phi$, while the last two operate on the qubit of absolute position, performing a rotation by an angle $\theta$. The light is then collected on the right using an array of fibers (right glass cones). This goes to four SPADs, which implement the measurement operations: as in Chapter 2, it is only necessary to detect in which state $|UN\rangle$, $|UF\rangle$, $|DF\rangle$ and $|DN\rangle$ the wavefunction collapses.

remark has to be done on the generation stage: apparently, this structure is less flexible than the generation stage presented in Chapter 2. A more flexible device could be based on a cascade of MZI. If the initial MMI is replaced by a MZI placed in the middle of the four waveguides, it can be used to split the input light between the state $|UN\rangle$ and $|DN\rangle$. By using then other two MZIs to rotate the relative position qubit. it is possible to obtain each linear combination of the four states $|UN\rangle$, $|UF\rangle$, $|DF\rangle$ and $|DN\rangle$. Four PSs have then to be placed at the outputs of these MZIs to change the relative phases. However, abandoning the sharp separation of the stages, the union of the generation stage with the first rotation of the relative position could fulfill this scope: it is just necessary to rotate the MZIs of an angle $\phi = \phi_c + \phi_r$, where $\phi_c$ is the angle required to obtain the linear combination of the four states $|UN\rangle$, $|UF\rangle$, $|DF\rangle$ and $|DN\rangle$ and $\phi_r$ is the actual angle of the rotation. However, the four PSs are still necessary to regulate the relative phases.

### 4.3.1 Theoretical form of $\chi$

Having implemented the same qubit rotations as in Chapter 2, the structure of the $\chi$-parameter of the BI, for the generated state $|\phi^{\pm}\rangle$, is:

$$\begin{aligned}\chi(\phi_{0,1}, \phi_{0,2}, \phi_{1,1}, \phi_{1,2}, &\theta_{0,1}, \theta_{0,2}, \theta_{1,1}, \theta_{1,2}) = \\ &= \cos(2((\phi_{0,1} - \phi_{0,2}) \mp (\theta_{0,1} - \theta_{0,2}))) + \\ &- \cos(2((\phi_{0,1} - \phi_{0,2}) \mp (\theta_{1,1} - \theta_{1,2}))) + \\ &+ \cos(2((\phi_{1,1} - \phi_{1,2}) \mp (\theta_{0,1} - \theta_{0,2}))) + \\ &+ \cos(2((\phi_{1,1} - \phi_{1,2}) \mp (\theta_{1,1} - \theta_{1,2}))),\end{aligned} \tag{4.25}$$

where the index $i = 0, 1$ and $j = 1, 2$ in $\phi_{i,j}$ and $\theta_{i,j}$ refer to, respectively, to the choice of the angles in the $\chi$-parameter ($i$) and to the angles in the matrix representation of the MZIs($j$). For the state $|\phi^+\rangle$, by setting all the terms having $\phi_{i,2} = \theta_{i,2} = 0$ and making the same choice done in

Chapter 2 of ($\phi_{0,1} = 0, \phi_{1,1} = \omega, \theta_{0,1} = \omega/2, \theta_{1,1} = 3\omega/2$), it is possible to obtain the $\chi$-parameter:

$$\chi\left(0, 0, \omega, 0, \frac{\omega}{2}, 0, \frac{3\omega}{2}, 0\right) = 3\cos(\omega) - \cos(3\omega). \tag{4.26}$$

For the state $|\phi^-\rangle$, by setting $\phi_{i,2} = \theta_{i,2} = 0$ and making the choice ($\phi_{0,1} = 0, \phi_{1,1} = -\omega, \theta_{0,1} = \omega/2, \theta_{1,1} = 3\omega/2$), the same form is obtained:

$$\chi\left(0, 0, -\omega, 0, \frac{\omega}{2}, 0, \frac{3\omega}{2}, 0\right) = 3\cos(\omega) - \cos(3\omega). \tag{4.27}$$

## 4.4 Non-idealities in the calculation of $\chi$

The non-idealities present the integrated circuit are just nearly the same as the ones reported in Section 2.7 of Chapter 2:

- Presence of noise $\longrightarrow$ Visibility parameter $\eta$,
- Communication between the two qubits $\longrightarrow e_\chi$,
- Use of attenuated source with a spectrum $\longrightarrow \epsilon$,
- Not-ideal detectors $\longrightarrow$ Markov correction to the $\mathbb{P}$.

Consequently, the same assumptions necessary to handle all the loopholes in the test of the BI are still needed. However, the communication between the two qubits now is due to a different physical motivation: the presence of extra differences between the angles applied to each of MZI of the couple that induce the $\phi(\theta)$-rotation. Indeed, a couple of angles $(\phi, \theta)$ has to be precisely fixed in each couple of MZIs. This requirement is not satisfied if the power supply that controls the PSs is not precise enough. Indeed, if an error $(\delta\phi, \delta\theta)$ not fixed is introduced in each rotation, the matrixes that represent the operators that describe the action of the MZIs are no longer in product form:

$$\begin{aligned}
&U_{\text{real}}(\phi_1, \phi_2, \delta\phi_1, \delta\phi_2, \delta\phi_3, \delta\phi_4) = \\
&P1 \otimes U_{\text{MZI}}(\phi_1 + \delta\phi_1, \phi_1 + \delta\phi_2) + \\
&+ P2 \otimes U_{\text{MZI}}(\phi_1 + \delta\phi_3, \phi_2 + \delta\phi_4); \\
&U_{\text{real}}(\theta_1, \theta_2, \delta\theta_1, \delta\theta_2, \delta\theta_3, \delta\theta_4) = \\
&U_{\text{MZI}}(\theta_1 + \delta\theta_1, \theta_2 + \delta\theta_2) \otimes P1 + \\
&+ U_{\text{MZI}}(\theta_1 + \delta\theta_3, \theta_2 + \delta\theta_4) \otimes P2; \\
&P_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.
\end{aligned} \tag{4.28}$$

Note that in principle the terms $\delta\phi_1, \delta\phi_2, \delta\phi_3, \delta\phi_4, \delta\theta_1, \delta\theta_2, \delta\theta_3, \delta\theta_4$ are all different and they appear both in the rotation terms $(\phi_1 - \phi_2)$ and $(\theta_1 - \theta_2)$ and in the global phase terms $(\phi_1 + \phi_2)$ and $(\theta_1 + \theta_2)$. I have not yet elaborated a proper treatment of the non-idealities, which can be performed by using the same idea of Section 2.7 in Chapter 2. For this reason such a non-idealities will be neglected in the experimental verification of the BI by taking the mean of all the angles effectively applied by the power supply: specifically the considered $\phi = \phi_1 - \phi_2$ is the mean of $\{\phi_1 + \delta\phi_1 - \phi_2 - \delta\phi_2, \phi_1 + \delta\phi_3 - \phi_2 - \delta\phi_4\}$ and $\theta = \theta_1 - \theta_2$ is the mean of $\{\theta_1 + \delta\theta_1 - \theta_2 - \delta\theta_2, \theta_1 + \delta\theta_3 - \theta_2 - \delta\theta_4\}$.

## 4.5 Simulation of the different optical components

The integrated circuit has been simulated using the bidirectional Eigenmode expansion (EME) solver of Lumerical. For all the different components, the height of the waveguide is 0.3 $\mu$m. The materials are Silicon Oxynitride ($\mathrm{SiO}_x\mathrm{N}_y$) for the waveguide and Silica ($\mathrm{SiO}_2$) for the top and cladding material. Such a choice of materials allows using wavelengths in the range $[600, 850]$ nm. The working wavelength was chosen to be around 740 nm due to the available light sources at that specific wavelength. As working polarization, the TE was chosen. All the simulations of the optical elements were done by Massimo Borghi and Matteo Sanna inside the project EPIQUS.

### 4.5.1 Multi-Mode Interferometer (MMI)

The simulated MMI geometric structure is reported in Figure 4.10a. The geometry is fixed by performing a sweep of the parameters for the working wavelength of 740 nm: the goal of the sweep is to find a geometry such that the power transmission $T$ and reflection $R$ coefficients of the MMI are as close as possible to $T = R = 1/2^2$ . For the selected geometry, a wavelength sweep is performed to evaluate the behavior of the power transmission and reflection coefficients as a function of the wavelength. The results of the simulation are reported in Figure 4.10a. In the range 720 nm$< \lambda < 760$ nm, the difference between the two coefficients is lower than 0.25%, while the insertion losses of the device are lower than 1% between 730 nm$< \lambda < 750$ nm. For these reasons, any $\lambda \in [730, 750]$ nm could be suitable for obtaining an integrated BS.

[2] In the case of MMI, the coefficients $T$ and $R$ have the usual meaning respect to the BS: when the input waveguide is placed at $x^*$ respect to the center of the MMI, $T$ gives the power at the output waveguide with the center in $x^*$, while $R$ provides the power at $-x^*$.

### 4.5.2 Crossing (CR)

The simulation of the CR is done in the same way as for the MMI with a different objective: now the transmission in the specular waveguide at the output of the CR has to be maximized. The best geometrical structure is chosen by selecting the one with the lowest insertion loss for the desired wavelength. The designed structure and the result of the simulation are reported in Figure 4.10b: near 740 nm, the design gives a transmission of $T = 99.1\%$.

### 4.5.3 Structure of the integrated chip

Given the simulated structures of the MMI and CR, the chip was then designed using the MMIs as the BSs of the integrated MZI. The chip structure is reported in Figure 4.11 and its dimensions are: $\simeq 6{\times}1\ \mathrm{mm}^2$. As expected, its dimensions are three orders of magnitude lower compared with the ones of the bulk implementation ($\simeq 1 \times 1\ \mathrm{m}^2$). In Figure 4.11 are reported also the different powers $\{W_{\gamma_i}\}_{\gamma=\xi,\phi,\theta;i=1,2}$, necessary to control all the PSs.

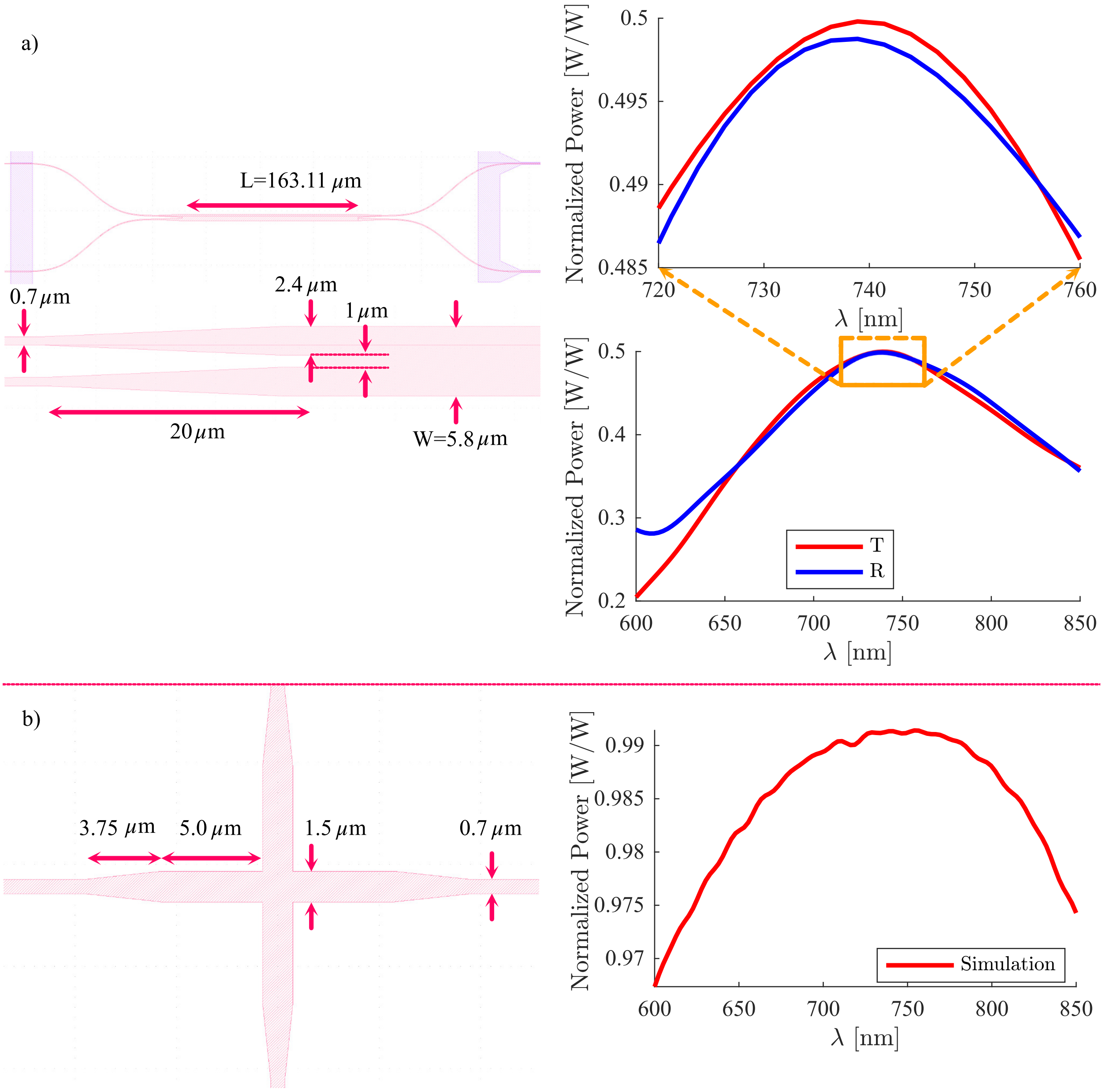


**Figure 4.10:** Geometrical parameter of the simulated MMI and CR and their simulated properties. a) The simulated MMI is composed of two symmetric input waveguides that are tapered from the width of 0.7 μm to 2.4 μm in 20 μm of length. Those are separated by 1 μm at the entrance of the wider waveguide. The latter has a width of 5.8 μm and length 163.11 μm. The outputs of the MMI are symmetric with respect to the inputs. The power transmission $T$ and reflection coefficients $R$ of the MMI are simulated between 600 nm and 850 nm and are reported on the right respectively in red and blue: they nearly reach the desired value of 0.5 between 730 nm and 750 nm. b) The simulated CR is constituted by two orthogonal 1.5 μm wide waveguides. At the inputs and the outputs of the CR a tapering region of 3.75 μm of length is used to connect to the CR the 0.7 μm wide input and output waveguides. The simulated transmission coefficients of the CR are reported on the right: a nearly unitary transmission coefficient was obtained between $[730, 750]$ nm.

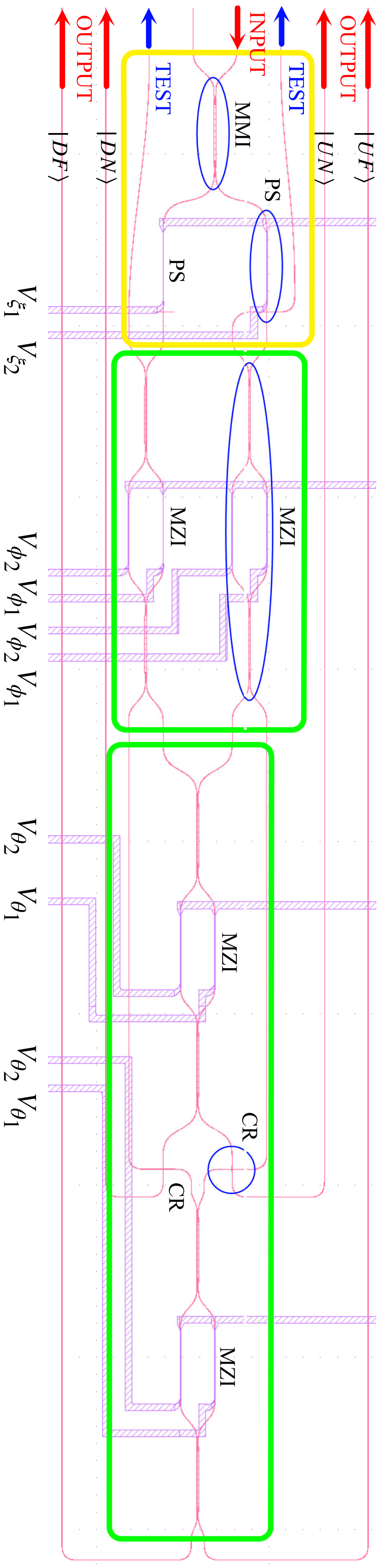


**Figure 4.11:** Scheme of the fabricated integrated chip for the validation of the SPE based on HSP. The optical waveguides are reported in pink, while in purple the metallic wire (PS with the respective applied power $\{W_{i_j}\}_{i,=\xi,\phi,\theta,j=1,2}$). The input and output waveguides are indicated in red: for the output waveguide is reported also the corresponding state. The generation stage is reported in yellow, while the MZIs used to rotate the qubits are inside the green boxes. In blue are circled an example of the MMI, of the PS, of the CR and of the MZI. The waveguide indicated in blue are used to test the different MZIs.

## 4.6 Experimental characterization of the devices

The clean room of Fondazione Bruno Kessler produced the device, thanks to Gioele Piccoli and Mher Ghulinyan. Martino Bernard wired the chip. Matteo Sanna and Gioele Piccoli performed the characterization measurements of the isolated test structure within the project EPIQUS.

### 4.6.1 Characterization of the CRs and MMIs

The experimental setup used to characterize the CRs and MMIs is reported in Figure 4.12 and a zoom on the optical chip is reported in Figure 4.13. Two tapered optical fibers are used to inject and collect the light from the structure. A supercontinuum laser emitting from 350 nm to 2000 nm opportunely filtered (650 − 850 nm) and polarized (TE, achieved with two bulk Half-Wave Plates (HWPs) and one bulk Quarter-Wave Plate (QWP)) is used as light source. The optical input and output coupling is achieved using two 3-axis translation stages, a visible camera with a magnification system (imaging system in Figure 4.13) and a sample holder over which the chip is placed. The light collected by the output tapered fiber goes to an Optical spectrum analyzer (OSA), used as the detector. For characterizing the CR, test structures with a sequence of 150 CRs not-equidistant to avoid any Fabry-Perot effect were used. The experimental data are normalized with respect to the light collected at the output of a straight waveguide used as a reference and shown in Figure 4.14. In the interested wavelength range of $[730, 750]$ nm the transmission coefficient measured for the CR is in the range $[97.7\%, 98.2\%]$. This attenuation is quite near to the simulated value. It is worth to remark that the presence of a CR with no ideal characteristics is not a problem for the BI test since its action can be considered as a further rotation acting on the qubit of the relative position by an angle $\phi_c$ such that:

$$\mathrm{CR}(\phi_c) := \begin{pmatrix} \sin(\phi_c) & \cos(\phi_c) \\ \cos(\phi_c) & -\sin(\phi_c) \end{pmatrix}, \quad \phi_c = \arccos(\sqrt{T_{\mathrm{CR}}}) \tag{4.29}$$

where $T_{\mathrm{CR}}$ is the transmission coefficient of the CR. Moreover, having used the same design for all the CRs, it is possible to write the action of such composed object in the space of the two qubits as $I_2 \otimes \mathrm{CR}(\phi_c)$, which is still a product form operator.

The MMI is characterized using the same experimental setup. The power of the two output ports is collected for both the inputs: the experimental data are still normalized respect to optical power collected at the output of the reference straight waveguide and are reported in Figure 4.15a. T11 indicates the signal at the output $(x^*, L)$ with input at $(x^*, 0)$, while $R12$ is the signal at output $(-x^*, L)$. On the contrary, $T22$ and $R21$ are the power coefficients with input light at $(-x^*, 0)$. In Figure 4.15a Input1 indicates the sum of $T11$ and $R12$, while Input2 is the sum of $T22$ and $R21$. For this data, two observations can be done:

1) the power transmission and reflection coefficients are different from the simulation results. Moreover, the coefficients are different

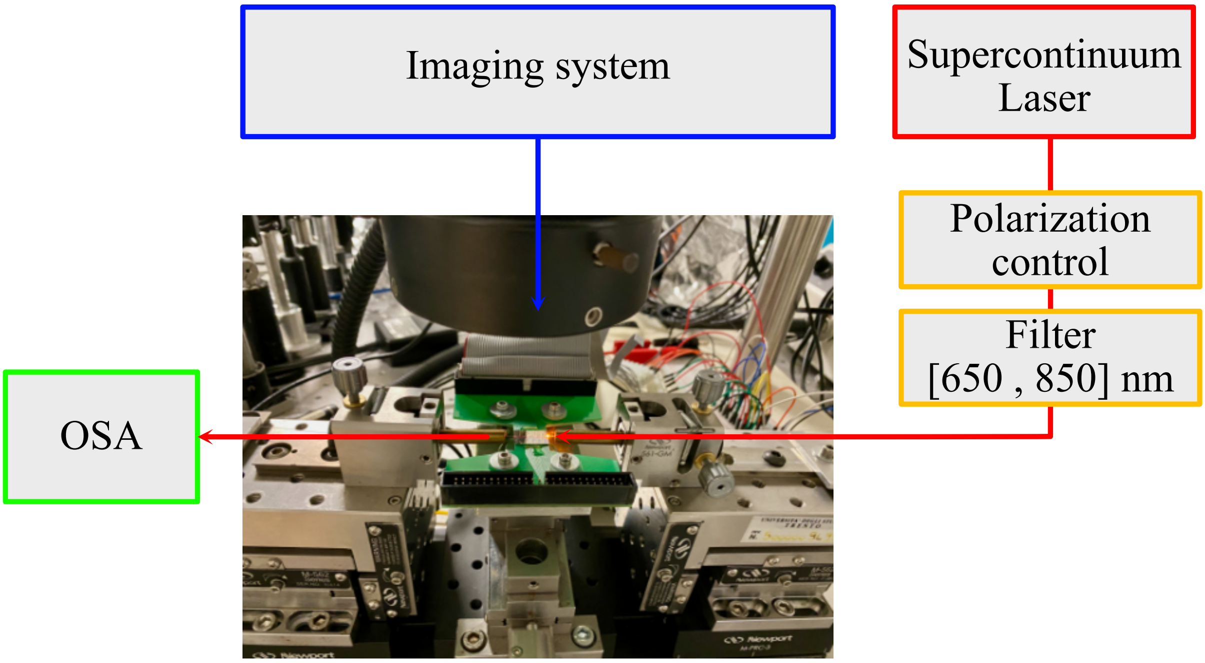


**Figure 4.12:** Experimental setup used to characterize the MMI and the CR. The optical signal is indicated with a red arrow. The blue arrow indicates the imaging system to perform the coupling between the input-output tapered waveguide to the facets of the chip. Color code of the boxes: red, supercontinuum laser source, orange, optical components used to prepare the light before the injection in the chip of Figure **??**, green, OSA used to detect the optical signals.

for the two inputs. These differences are at the moment under investigation.

2) The Input1 and Input2 are greater than 1 for some wavelengths. This can be explained considering a wrong cut of the facets of the input and output waveguide of the chip, which can induce such an effect.

To have a better estimation of the coefficients $Tij$ $(i = j)$ and $Rij$ $(i \neq j)$, it is possible to renormalize the measurements with respect to the sum of the total power collected by two outputs:

$$\tilde{T}ij = \frac{Tij}{Tij + Rij}, \qquad \tilde{R}ij = \frac{Rij}{Tij + Rij}. \tag{4.30}$$

The corresponding matrix of the MMI can be written as:

$$U_{MMI} := \begin{pmatrix} \sqrt{\tilde{T}11} & i\sqrt{\tilde{R}21} \\ i\sqrt{\tilde{R}12} & \sqrt{\tilde{T}22} \end{pmatrix}. \tag{4.31}$$

Such a matrix does not represent a fundamental problem for the calculation of the $\chi$-parameter: even if it is different from the matrix of a perfect 50 : 50 MMI, it does not induce any particular coupling between the two qubits. The only influenced parameter is, indeed, the visibility $\eta$, which is slightly decreased ($\eta \simeq 0.986$ for T=0.4 and R=0.6) not having perfectly balanced power coefficients.

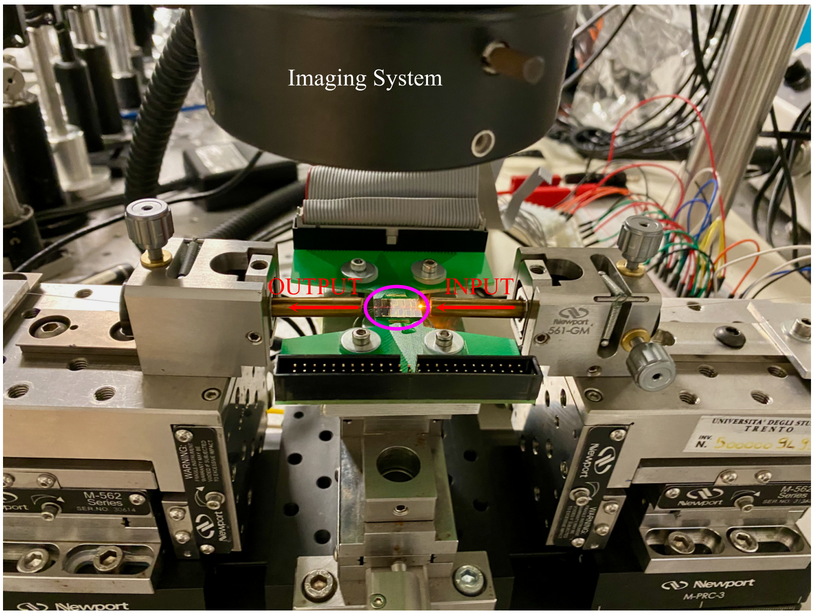


**Figure 4.13:** Example of the experimental setup used for the characterization of the CRs and MMIs. In red are indicated the input and output tapered fibers used to couple in and out the light from the photonic chip. The photonic chip (example, not the actual one, in purple) is placed on a sample holder. The fibers are placed in the desired position using two 3-axis alignment stages and an imaging system (white) composed of a magnification system and a visible camera.

**Table 4.1:** Measured values of the MMI power transmission and reflection coefficients $\tilde{T}11$, $\tilde{R}21$,$\tilde{R}12$ and $\tilde{T}22$ for $\lambda = 730.1$ nm.

| $\tilde{T}11$ | $\tilde{R}21$ | $\tilde{R}12$ | $\tilde{T}22$ |
|---|---|---|---|
| 0.411 ± 0.002 | 0.603 ± 0.001 | 0.589 ± 0.002 | 0.398 ± 0.001 |

### 4.6.2 Characterization of the single MZIs

The experimental setup used to characterize the MZIs is reported in Figure 4.16 and in Figure 4.17. The details of the optical chip on the Printed Circuit Board (PCB) and on the sample holder are shown in Figure 4.18. To characterize the single MZIs, the light is coupled inside and outside the chip using a fiber array composed of eight optical fibers: the output testing ports of Figure 4.19 are used to collect the light, which is injected at the input port 1 for the characterization of MZI_UP, MZI_DW and MZI_FR (Figure 4.19), and at the input port 2 for the characterization of MZI_NR. The fiber array is aligned to the chip using a 6-axis roto-translational stage and a visible camera with a magnification system (imaging system). The optical chip is attached to a PCB that allows connecting the metallic pads of the PSs to an 8-channel current supply, remotely controlled using the PC. As a light source, it was used a Ti:Sapphire laser centered at 730.1 nm that was coupled into an optical fiber and attenuated through a VOA. Since the entire chip is designed for the TE polarization, the polarization of the light was fixed using an in-fiber polarization controller. As detectors the SPADs are used. The counts from the SPADs are collected by a Time Tagger and stored in the PC. The parameter of the MMI are reported in Table 4.1 for 730.1 nm.

The first characterization is on the relation between the angle of rotation and the power applied to each PS. Since the transmission of the MZI depends only on the difference between the angles $\phi = \phi_1 - \phi_2$ and $\theta = \theta_1 - \theta_2$ in Equation 4.15, a positive sign was assigned to the power $W_{\phi_1(\theta_1)}$ applied to the PS that induces $\phi_1(\theta_1)$ and a negative sign to the power $W_{\phi_2(\theta_2)}$ that induces $\phi_2(\theta_2)$. The experimental data are reported as blue dots in Figure 4.19 as a function of the power applied to the PSs. Due to fabrication errors in each MZI, even if designed balanced, i.e, with an initial phase difference ($\phi_1 - \phi_2 = \theta_1 - \theta_2 = 0$), the MZI has a parasite

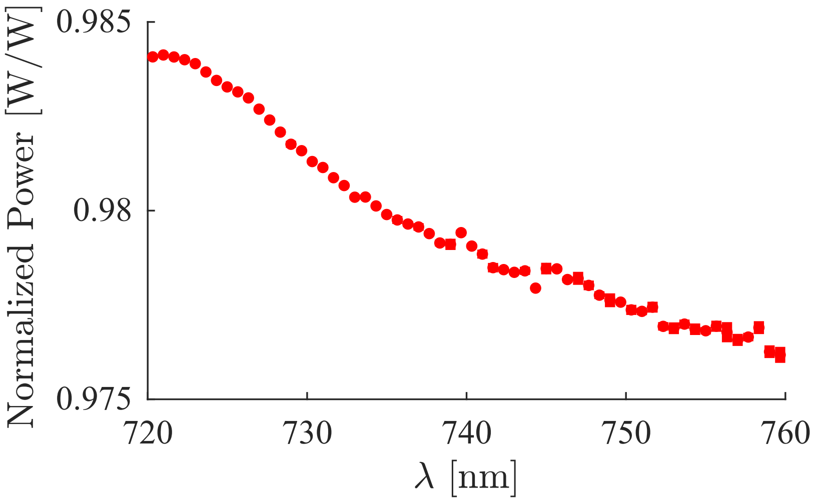


**Figure 4.14:** Measured value of the transmission coefficient of the CR. In red are reported the experimental data acquired normalized respect to the power collected from a straight waveguide of reference. The error bars are within the dot size.

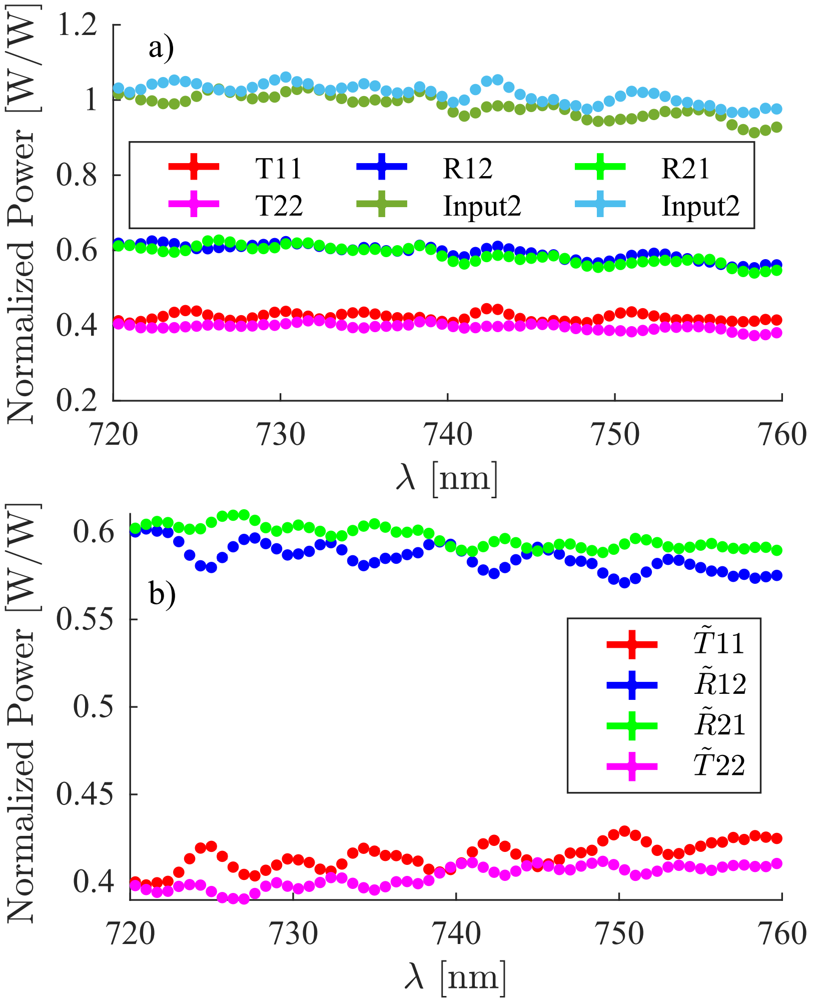


**Figure 4.15:** Measured value of the power transmission and reflection coefficients of the MMI. The coefficients are estimated by injecting the light from one input and collecting the two outputs. In a) $T11$ is reported in red, $R12$ in blue, $R21$ in green and $T22$ in purple. The sum of the coefficients for the same input is also reported: for input 1, it is reported in military green, while for input 2, in cyan. The error bars are within the dot size. In b) $\tilde{T}11$ is reported in red, $\tilde{R}12$ in blue, $\tilde{R}21$ in green and $\tilde{T}22$ in purple. The error bars are within the dot size.

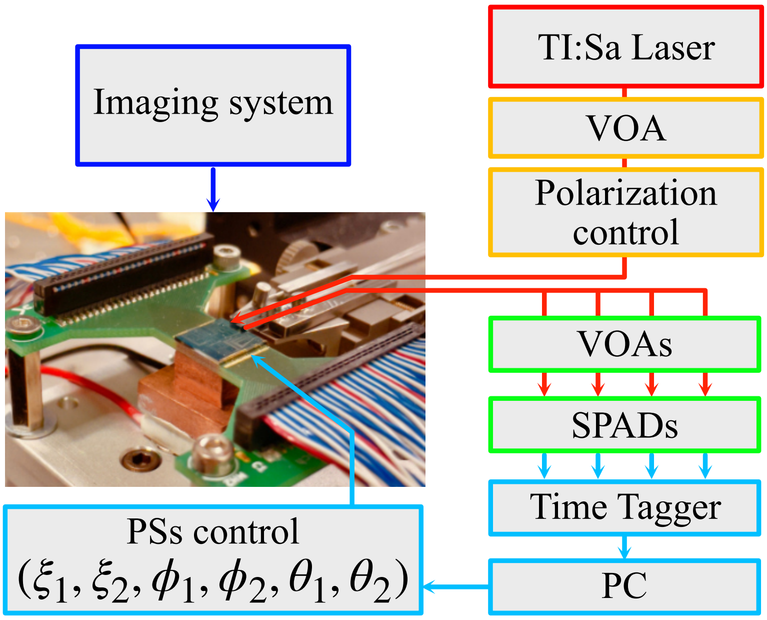


**Figure 4.16:** Experimental setup used to characterize the single MZIs and the internal phases of the fabricated photonic chip and to demonstrate the violation of BI in the case of SPE of HSP. The red arrow indicates the optical signal, the cyan arrow indicates the electrical signal and the blue arrow indicates that the imaging system is used to perform the coupling between the fiber array and the chip. Color code of the boxes: red, Ti:Sapphire laser source, orange, optical components (VOA and polarization control) use to prepare the light before the injection in the chip, green, the optical detection system, composed of VOAs and SPADs, cyan, electronic devices used to control the chip (PSs control, used to set the phases $(\xi_1, \xi_2, \phi_1, \phi_2, \theta_1, \theta_2)$) and to detect and store the electronical signals (Time Tagger and PC)

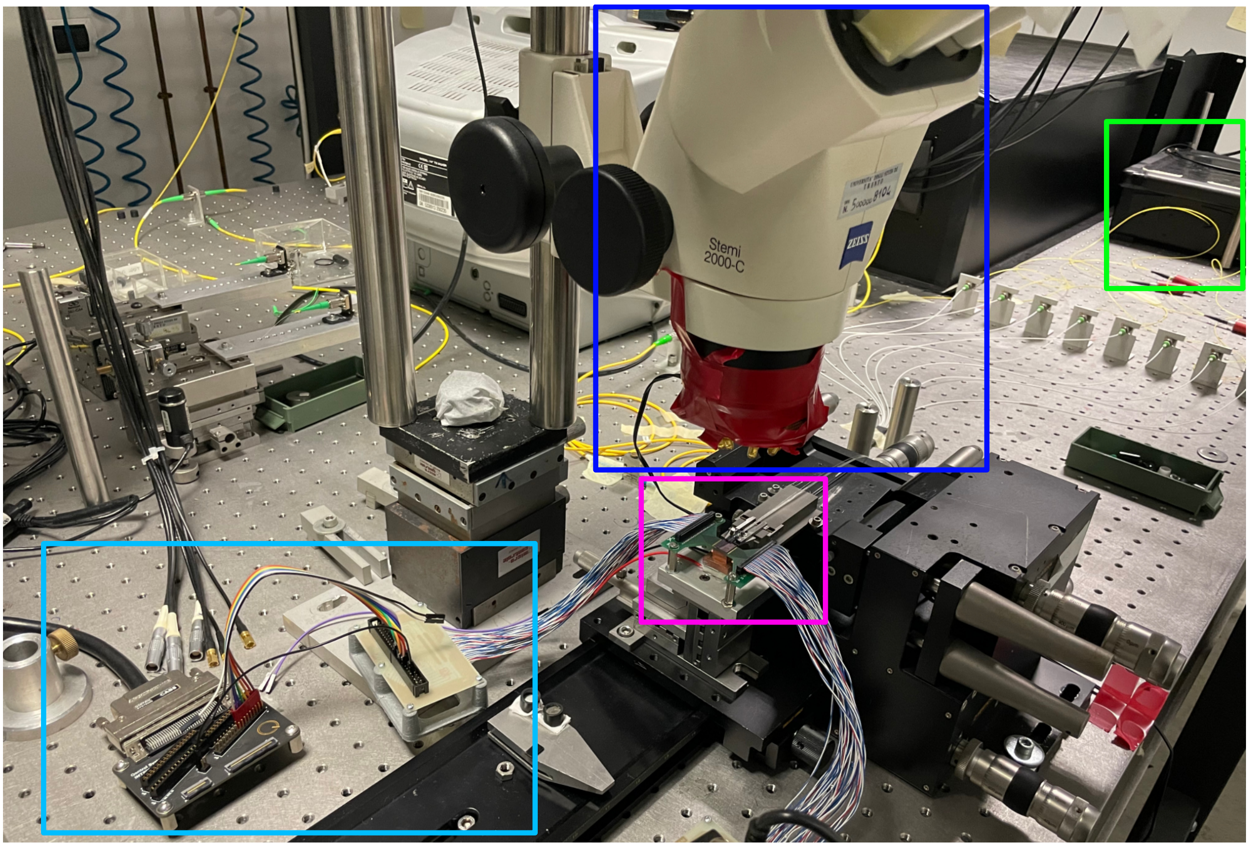


**Figure 4.17:** Photo of the experimental setup used to characterize the single MZIs and the internal phases of the fabricated photonic chip and to demonstrate the violation of BI in the case of SPE of HSP. In purple is indicate the optical chip placed over the sample holder. In blue is highlighted the magnification system used, with the visible camera, to see the optical chip and to align the fiber array to the desired structure. In the cyan square is possible to see the power supply used to electronically control the PSs. In green is indicated the box where the SPADs are.

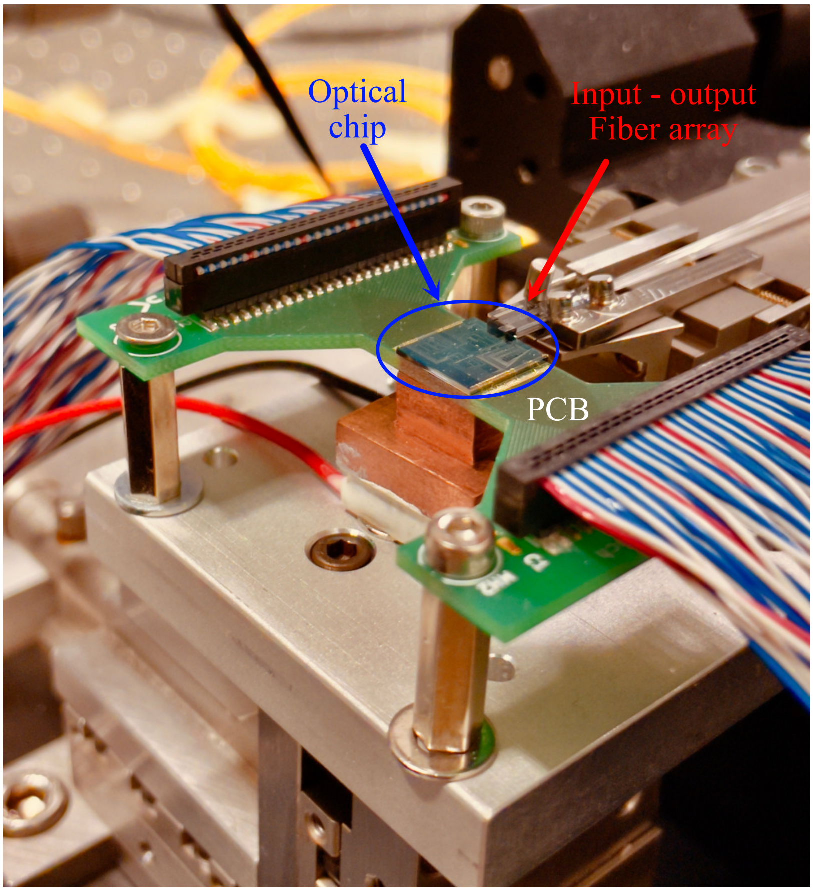


**Figure 4.18:** The optical chip produced to demonstrate violation of BI in the case of SPE of HSP. In blue is indicate the optical chip on the PCB. There are clearly visible the electrical cables necessary to control the PSs. In red it is indicated the input-output fiber array used to couple in and out the photons.

phase differences $\delta\phi$ and $\delta\theta$, i.e., $\phi_1 - \phi_2 = \delta\phi$ and $\theta_1 - \theta_2 = \delta\theta$. The fit is necessary to estimate not only the relation phase-power applied but also this initial offset, different for every MZI. Depending on which input and output ports are considered for the MZI, the fit functions are:

$$\phi(W) = \alpha\cos(\beta W + \delta)^2 + \gamma, \tag{4.32}$$

$$\phi(W) = \alpha\sin(\beta W + \delta)^2 + \gamma. \tag{4.33}$$

Equation 4.32 is used for MZI_UP and MZI_FR, while Equation 4.33 is used for MZI_DW and MZI_NR. Note that for MZI_NR the characterization is done only for negative power, since one heater pad results not connected. The fit results are reported in Table 4.2. As it is possible to observe, the $\delta$ parameters are different for each MZI as expected, while instead the $\beta$ are quite similar, since the heating structure is the same for all the MZIs.

### 4.6.3 Characterization of the internal phases of the structure

Another calibration must be done to know the power $W_{\xi_i}$ necessary to compensate the phase of $\frac{\pi}{2}$ given by the first MMI. For this calibration, an initial guess is to use the mean of the estimate $\beta$ parameters obtained for the MZIs since the heating structures are the same. Even if such an approach seems reasonable in an ideal situation, it is not feasible due to fabrication errors. In the previous section, it was introduced

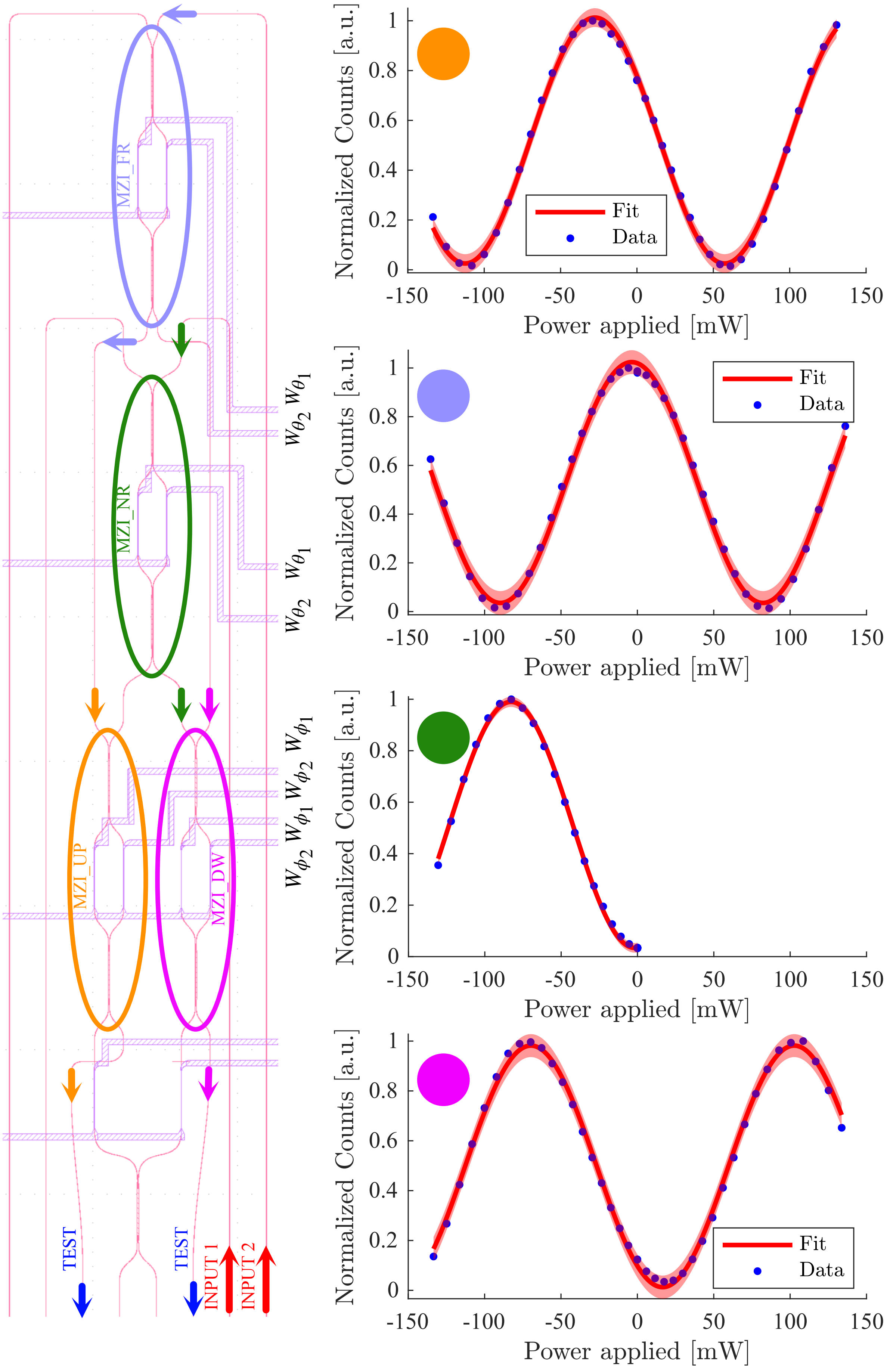


**Figure 4.19:** Characterization curves of the different MZI present in the optical chip for $\lambda = 730.1$ nm. The experimental data are reported in blue, while in red is reported the obtained fit with the corresponding 95% confidence interval. The data are obtained by injecting the light in the input waveguides (red arrows) and is collected from the output test waveguides (blue arrows). The MZI and the corresponding characterization curve are indicated with the same color (color of the circle for the MZI and color of the dot for the curve).

**Table 4.2:** Fit results for the calibration of each MZI. For each MZI, the parameters of the fit are reported with their standard deviation estimated by the fitting procedure. Equation 4.32 is used for MZI_UP and MZI_FR, while Equation 4.33 is used for MZI_DW and MZI_NR.

| | MZI_UP | MZI_DW | MZI_NR | MZI_FR |
|---|---|---|---|---|
| $\alpha$ | 0.987 ± 0.008 | 0.97 ± 0.01 | 0.956 ± 0.004 | 0.99 ± 0.01 |
| $\beta[mW^{-1}]$ | 0.01850 ± 0.00005 | 0.01822 ± 0.00007 | 0.01940 ± 0.00009 | 0.01828 ± 0.00007 |
| $\gamma$ | 0.025 ± 0.005 | 0.01287 ± 0.007 | 0.034 ± 0.002 | 0.036 ± 0.006 |
| $\delta$ | 0.5092 ± 0.004 | −0.3008 ± 0.005 | 0.036 ± 0.007 | 0.068 ± 0.005 |

the effect of the initial phase of the MZIs. The same occurs in the propagation in the single waveguides. In particular, a relative phase could be introduced between the different terms of the initial state simply due to the propagation into slightly different wide waveguides. For this reason, it is necessary to adopt another methodology. To consider such fabrication errors, the matrix $\mathrm{Ph}(\alpha,\beta,\gamma,\delta)$ is introduced as:

$$\mathrm{Ph}(\alpha,\beta,\gamma,\delta) := \begin{pmatrix} e^{i\alpha} & 0 & 0 & 0 \\ 0 & e^{i\beta} & 0 & 0 \\ 0 & 0 & e^{i\gamma} & 0 \\ 0 & 0 & 0 & e^{i\delta} \end{pmatrix}, \tag{4.34}$$

such that

$$|\psi_{\mathrm{out}}\rangle = U|\psi_{\mathrm{input}}\rangle,$$
$$U = I_2 \otimes U_{\mathrm{MZI}}(\theta_1,\theta_2)\mathrm{Ph}(\alpha,\beta,\gamma,\delta)U_{\mathrm{MZI}}(\phi_1,\phi_2) \otimes I_2\mathrm{Ph}(\xi_1,0,0,\xi_2=0) \tag{4.35}$$

where $|\psi_{\mathrm{input}}\rangle$ is defined in Equation 4.20 and for simplicity the power is applied only to the PS of ${\xi_1}^3$ . Now, if the phases $\phi_1 = \theta_2 = \frac{\pi}{4}$ and $\phi_2 = \theta_1 = 0$ are set, the entire optical circuit behaves as two concatenated MZIs (Figure 4.20): the first BS is given by the initial 50 : 50 MMI for both the MZIs, while the second BS is given respectively by the MZI_NR and MZI_FR. Since the MZI_UP and MZI_DW are set to the same phase, they do not contribute to the whole phase difference between the arms of the two MZIs, which is influenced only by the phases $\xi,\alpha,\beta,\gamma,\delta$. In this way the probabilities of observing the four states are given by:

$$\mathbb{P}_{|UF\rangle}(\xi_1,\xi_2,\alpha,\beta,\gamma,\delta) = \frac{1}{4}\left(1-\sin(\xi_1-\xi_2+\alpha-\gamma)\right), \tag{4.36}$$
$$\mathbb{P}_{|DN\rangle}(\xi_1,\xi_2,\alpha,\beta,\gamma,\delta) = \frac{1}{4}\left(1-\sin(\xi_1-\xi_2+\beta-\delta)\right), \tag{4.37}$$
$$\mathbb{P}_{|UN\rangle}(\xi_1,\xi_2,\alpha,\beta,\gamma,\delta) = \frac{1}{4}\left(1+\sin(\xi_1-\xi_2+\beta-\delta)\right), \tag{4.38}$$
$$\mathbb{P}_{|DF\rangle}(\xi_1,\xi_2,\alpha,\beta,\gamma,\delta) = \frac{1}{4}\left(1+\sin(\xi_1-\xi_2+\alpha-\gamma)\right). \tag{4.39}$$

This characterization's objective is also to compensate for the $\alpha-\gamma$ and $\beta-\delta$ errors introduced by fabrication. For estimating such errors, the experimental data obtained as a function of the power applied $W_{\xi_1}$ are fitted using the function

$$f(W_{\xi_1}) = a(1 \pm \sin(bW_{\xi_1} + c), \tag{4.40}$$

depending on the sign of the sin in Equation 4.36, Equation 4.37, Equation 4.38 and Equation 4.39. The experimental data and fits are reported in Figure 4.20, orange dot, while the fit parameters are reported in Table 4.3. The measurements and fits are reported also for the choice of angles

[3] In the following formula the term $\xi_2$ appears for completeness but is actually zero.

**Table 4.3:** Fit parameters with their standard deviation for Equation 4.36, Equation 4.37, Equation 4.38 and Equation 4.39 using Equation 4.40.

| | $\vert UF\rangle$ | $\vert UN\rangle$ | $\vert DF\rangle$ | $\vert DN\rangle$ |
|---|---|---|---|---|
| $a$ | 0.250 ± 0.007 | 0.244 ± 0.005 | 0.225 ± 0.003 | 0.243 ± 0.006 |
| $b[mW^{-1}]$ | 0.040 ± 0.001 | 0.0377 ± 0.0008 | 0.0381 ± 0.0005 | 0.036 ± 0.001 |
| $c$ | 4.18 ± 0.1 | 2.91 ± 0.05 | 4.29 ± 0.05 | 2.97 ± 0.07 |

**Table 4.4:** Fit parameters with their standard deviation for Equation 4.41, Equation 4.42, Equation 4.43 and Equation 4.44 using Equation 4.40.

| | $\vert UF\rangle$ | $\vert UN\rangle$ | $\vert DF\rangle$ | $\vert DN\rangle$ |
|---|---|---|---|---|
| $a$ | 0.249 ± 0.005 | 0.243 ± 0.006 | 0.236 ± 0.004 | 0.230 ± 0.004 |
| $b[mW^{-1}]$ | 0.0369 ± 0.0007 | 0.035 ± 0.001 | 0.0385 ± 0.0006 | 0.0374 ± 0.0007 |
| $c$ | 4.30 ± 0.07 | 2.95 ± 0.07 | 4.16 ± 0.06 | 2.77 ± 0.05 |

$\phi_2 = \theta_2 = \frac{\pi}{4}$ and $\phi_1 = \theta_1 = 0$ (red dot in Figure 4.20 and fit parameters in Table 4.4). For such a choice of angles, the probabilities of obtaining each state are now:

$$\mathbb{P}_{|UF\rangle}(\xi_1, \xi_2, \alpha, \beta, \gamma, \delta) = \frac{1}{4}\left(1 + \sin(\xi_1 - \xi_2 + \alpha - \gamma)\right), \tag{4.41}$$

$$\mathbb{P}_{|DN\rangle}(\xi_1, \xi_2, \alpha, \beta, \gamma, \delta) = \frac{1}{4}\left(1 + \sin(\xi_1 - \xi_2 + \beta - \delta)\right), \tag{4.42}$$

$$\mathbb{P}_{|UN\rangle}(\xi_1, \xi_2, \alpha, \beta, \gamma, \delta) = \frac{1}{4}\left(1 - \sin(\xi_1 - \xi_2 + \beta - \delta)\right), \tag{4.43}$$

$$\mathbb{P}_{|DF\rangle}(\xi_1, \xi_2, \alpha, \beta, \gamma, \delta) = \frac{1}{4}\left(1 - \sin(\xi 1 - \xi_2 + \alpha - \gamma)\right). \tag{4.44}$$

It was found that the values of the $c$ parameter for each fit are not compatible for the eight different cases (Table 4.3 and Table 4.4). Therefore, it is impossible to compensate at the same time for the different fabrication errors by changing only the phase $\xi_1 - \xi_2$. To try to continue the validation of SPE with the HSP, the following strategy is introduced: since the values are compatible between pairs ($|F\rangle$ and $|N\rangle$), $W_{\xi_1}$ is chosen to compensate $\alpha - \gamma$ and the counts for only the channels $|UF\rangle$ and $|DF\rangle$ are acquired. Then, $W_{\xi_1}$ is changed to correct $\beta - \delta$ and the experiment is repeated acquiring only the channels $|UN\rangle$ and $|DN\rangle$. Such a strategy introduces the assumption that the circuit performs the same rotations by repeating the experiment changing $W_{\xi_1}$, which seems a reasonable approximation. Under this hypothesys, it is possible to test the BI for the SPE based on HSP. For this reason, the power necessary to compensate each pair of fabrication error phases for the state $|\phi^+\rangle$ is extracted by the fits: it is obtained $W_{\xi_1} = 94.8 \pm 0.8$ mW and $W_{\xi_1} = 136 \pm 2$ mW. The same reasoning can be applied to generate the state $|\phi^-\rangle$: for the latter, the power $W_{\xi_1} = 12.7 \pm 0.9$ mW and $W_{\xi_1} = 50 \pm 1$ mW must be used. In a new design, four additional PSs[4] could be placed at the outputs of the MZI_UP and MZI_DW, to have additional control on the phase differences $\alpha - \gamma$ and $\beta - \delta$. An example of such a modification is reported in Figure 4.21. The phases inside the sin in Equation 4.36, Equation 4.37, Equation 4.38 and Equation 4.39 become:

$$\xi + \alpha - \gamma \longrightarrow \xi + \mu_1 - \mu_3 + \alpha - \gamma, \tag{4.45}$$

$$\xi + \beta - \delta \longrightarrow \xi + \mu_2 - \mu_4 + \beta - \delta. \tag{4.46}$$

[4] Ideally only two PSs are necessary due to the periodicity of the phase, but, to avoid using high currents in unfortunate cases, it is better to have all the four PSs.

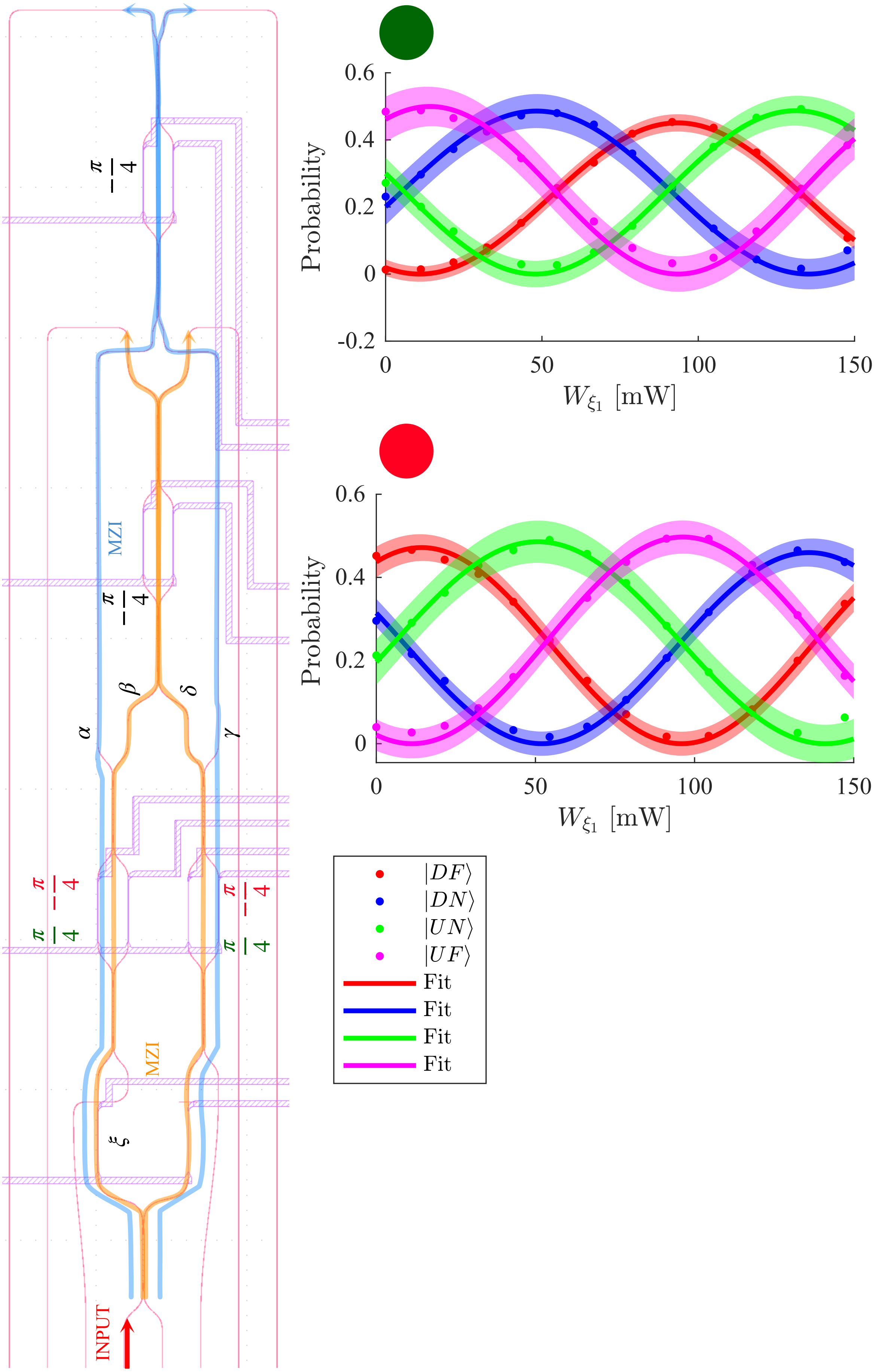


**Figure 4.20:** Characterization measurements of the phase $\xi_1$ as a function of the power applied $W_{\xi_1}$ for $\phi_1 = \theta_2 = \frac{\pi}{4}$ and $\phi_2 = \theta_1 = 0$, military green dot, and $\phi_2 = \theta_2 = \frac{\pi}{4}$ and $\phi_1 = \theta_1 = 0$, red dot. $\xi_2$ is not connected, so its contribution is not considered ($\xi_2 = 0$). The experimental data are reported as a function of the power applied to the PS that determines the phase $\xi_1$, $W_{\xi_1}$ and fitted using Equation 4.36, Equation 4.37, Equation 4.38 and Equation 4.39 for the military green and Equation 4.41, Equation 4.42, Equation 4.43 and Equation 4.44 for the red dot. The 95% confidence intervals are shown for each fit. The MZIs used to obtain the experimental data are reported on the left in orange for $|UN\rangle$ and $|DN\rangle$ and blue for $|UF\rangle$ and $|DF\rangle$. The phases $\alpha, \beta, \gamma$, and $\delta$ are also reported.

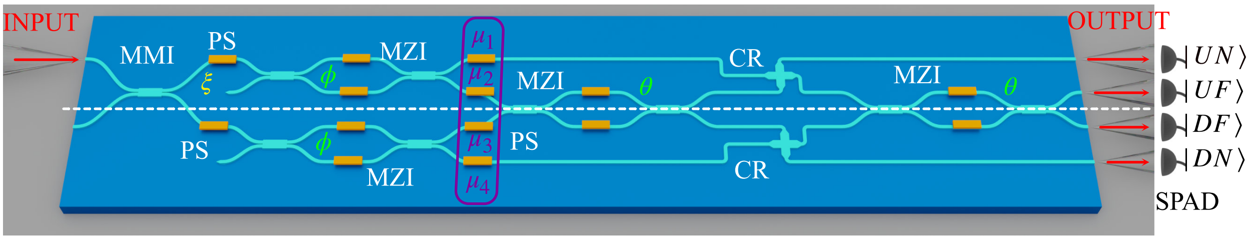


**Figure 4.21:** New scheme of the integrated chip for compensating fabrication phase errors. The addition of the four PSs is necessary to add flexibility, allowing to compensate the phase errors $\alpha, \beta, \gamma$ and $\delta$.

where the new PSs induce the phases $\mu_1, \mu_2, \mu_3$ and $\mu_4$. In this way, just controlling $\mu_1, \mu_2, \mu_3$ and $\mu_4$, it is possible to compensate the different fabrication errors $\alpha, \beta, \gamma$ and $\delta$.

## 4.7 Test of the Bell's inequality

To perform the test of the BI, the same optical setup described in the previous section and shown in Figure 4.17 and Figure 4.18 is used. The test of the BI is done for both the states $|\phi^+\rangle$ and $|\phi^-\rangle$ with the previously introduced assumptions.

### 4.7.1 Bell's inequality for $|\phi^+\rangle$

The test of the BI is done by performing a sweep of the rotation angle $\phi = \phi_1 - \phi_2$ for different values of the angle $\theta = \theta_1 - \theta_2$. The sweep intervals are determined by physical considerations: since the maximal current applicable to each PS is 24 mA, a limiting value of 17 mA is chosen. Considering that the $\beta$ coefficient of each MZI is $> 0.018$ mW$^{-1}$ and that each PS has a resistance of the order of $\simeq 500\ \Omega$, the maximal range for the angles $\phi = \phi_1 - \phi_2$ and $\theta = \theta_1 - \theta_2$ achievable for each MZI is $[-2.6, 2.6]$ rad. To be even more conservative the intervals are further decreased to $[-2, 2]$ rad for $\phi = \phi_1 - \phi_2$ and to $[-2, 0]$[5] rad for $\theta = \theta_1 - \theta_2$. For each couple of $(\phi, \theta)$, the detection events are acquired for 1 s with a time bin of 1 $\mu$s. The average flux of photons is $\simeq 75$ kHz. For such a flux, the correction induced by the Markovian model developed in Chapter 2 is negligible. So the probabilities $\mathbb{P}(x, y|\phi, \theta)$ are estimated from the empirical frequencies of the counts, in which multiple detection events and no detection events are eliminated. The experimental correlation coefficients $\mathbb{E}\left(O_\phi, O_\theta\right)$ are reported in Figure 4.22a with the respective fit of the type:

$$\mathbb{E}_{\text{Fit}}\left(O_\phi, O_\theta\right) = \eta \cos(2(\phi - \theta)), \tag{4.47}$$

where $\eta$ is the only free parameter connected to the visibility. Figure 4.22b reports the residuals plot of the experimental data with respect to the fit (Equation 4.47): the oscillations that appear are probably connected to the instability of the power supply.

By making the choice $\phi_0 = -\omega/2, \phi_1 = \omega/2, \theta_0 = 0, \theta_1 = \omega$[6], the $\chi$-parameter assumes the already introduced form:

$$\chi(\omega) = \eta(3\cos(\omega) - \cos(3\omega)), \tag{4.48}$$

[5] Positive angles are not reachable for $\theta$, since one PS is not connected.

[6] To avoid confusion, the subscripts here indicate the particular angle in the BI and not the angle in the MZI: $\alpha_i = \alpha_{i,1} - \alpha_{i,2}$, with $\alpha \in \{\phi, \theta\}$.

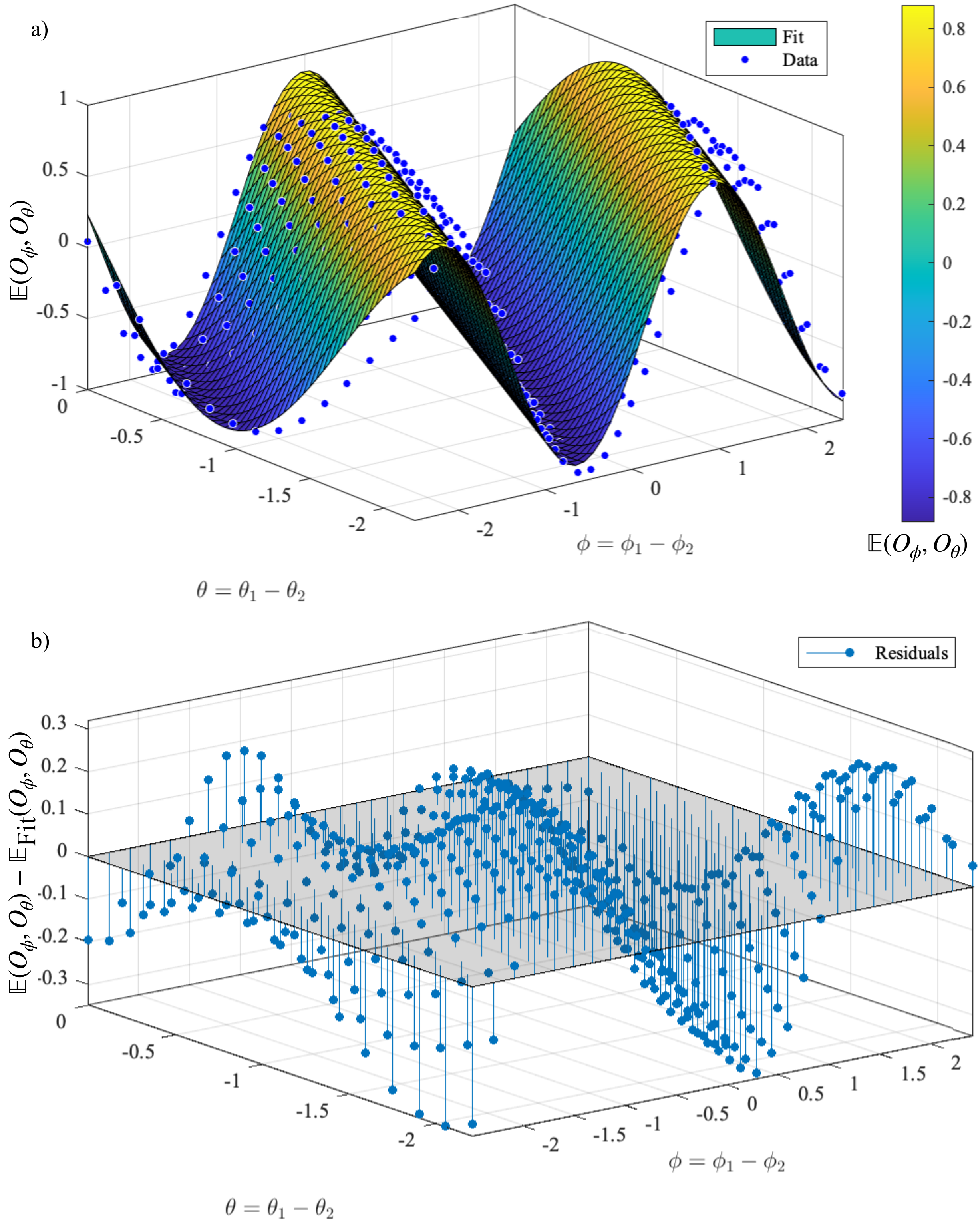


**Figure 4.22:** a) Raw correlation coefficients $\mathbb{E}_{\text{Fit}}\left(O_\phi, O_\theta\right)$ )(blue dots) obtained during the experiment with the relative fit $\mathbb{E}_{\text{Fit}}\left(O_\phi, O_\theta\right) = \eta_1 \cos(2(\phi - \theta))$ (colored surface) where $\phi$ and $\theta$ are the variables and $\eta_1$ is a fit parameter. From the fit operation, it is obtained $\eta_1 = 0.88 \pm 0.01$ b) Residuals plot of the fitted raw data $\mathbb{E}\left(O_\phi, O_\theta\right)$ respect to the fit $\mathbb{E}_{\text{Fit}}\left(O_\phi, O_\theta\right)$. The physical origin of the oscillations observed is probably the power supply instability.

**Table 4.5:** Maximal absolute violations of the BI observed for the state $|\phi^+\rangle$. $\chi^{\phi_1}$ refers to the values reported in Figure 4.23, while $\chi^{\text{rec}}$ to the maximum and minimum violations observed by comparing every possible combination of correlation coefficients.

| | Max | Min |
|---|---|---|
| $\chi^{\phi_1}$ | $2.39 \pm 0.02$ | $-2.32 \pm 0.02$ |
| $\chi^{\text{rec}}$ | $2.731 \pm 0.005$ | $-2.689 \pm 0.007$ |

which becomes

$$\chi(\phi_1) = \eta(3\cos(2\phi_1) - \cos(6\phi_1)) \tag{4.49}$$

identifying $\omega = 2\phi_1$. This choice is done to maximize the number of data obtainable from the raw data without any fitting operation. The results for the calculated $\chi$-parameter are reported in Figure 4.23 as a function of the angle $\phi_1$. Apart from the direct estimation based on the raw data (green dots of Figure 4.23), $\chi$ is obtained using two methodologies:

1) Equation 4.47, with fit parameters $\eta$ and variables $\phi$ and $\theta$, is used to fit the correlation coefficients $\mathbb{E}\left(O_\phi, O_\theta\right)$. The mean visibility obtained is $\eta_1 = 0.88 \pm 0.01$. From the fitted $\mathbb{E}\left(O_\phi, O_\theta\right)$, $\chi_1$, is directly calculated and reported as the purple dashed curve in Figure 4.23.
2) Equation 4.47 with fit parameters $\hat{\phi}$ and $\eta_\phi$. Such a fitting function is used to fit $\mathbb{E}\left(O_{\hat{\phi}}, O_\theta\right)$ with $\theta$ variable for each fixed $\hat{\phi} \in [-2, 2]$ rad. Obtained this fit, it is used to enlarge the $\theta$-range to $[-4\pi, 4\pi]$. Given the new set of fitted data, this operation is repeated, with new parameters $\hat{\theta}$ and $\eta_\theta$, to enlarge the $\phi$-range to $[-4\pi, 4\pi]$ for each $\hat{\theta} \in [-4\pi, 4\pi]$. The new set of data is then cubic interpolated to extrapolate also intermediate values. Respect to the previous method, this allows to consider also the effects of a variation of $\eta$ during the sweep of the angles $\phi$ and $\theta$. The mean visibility is eventually calculated as the mean of the set of all the $\{\eta_i\}_{i=\phi,\theta}$ obtained from the fitting procedures: $\eta_2 = 0.897 \pm 0.003$. The obtained $\chi_2$ is reported as a red dotted curve in Figure 4.23.

The $\chi$-parameter obtained from the data, $\chi_{\text{data}}$, follows Equation 4.49 (blue curve in Figure 4.23) for the mean visibility calculated, apart from a right lateral shift probably induced by the already introduced instability of the power supply. However, the form of the $\chi$-parameter is the one expected. A further estimation of the $\chi$-parameter can be done by using a recursive approach: evaluate $\chi(\phi_i, \phi_j, \theta_k, \theta_l)$ for all the angles $\phi_i \in [-2, 2]$ rad, $\phi_j \in [-2, 2]$ rad, $\theta_k \in [-2, 0]$ rad and $\theta_l \in [-2, 0]$ rad, for which the raw data are available. Using this strategy, it is possible to obtain even higher values of the $\chi$-parameter than the methodologies previously introduced, since the choice $\phi_0 = -\omega/2, \phi_1 = \omega/2, \theta_0 = 0, \theta_1 = \omega$ is optimal only for $|\phi^+\rangle$. However, due to experimental errors, the actual obtained state can be slightly different than $|\phi^+\rangle$, opening to the possibility of finding a better combination of angles that maximize the BI. The maximal and minimal values for the $\chi$-parameter obtained using the raw data are reported in Table 4.5: $\chi^{\phi_2}$ indicates the values reported in Figure 4.23, while $\chi^{\text{rec}}$ the values obtained using the recursive approach. The latter is obtained by selecting the best 1 s sequences that maximize $\chi$ and dividing them into five pieces of 0.2 s: $\chi_i^{\text{rec}}$ is calculated for each $i = 1..5$ and the value $\chi^{\text{rec}}$ is the mean value obtained with its standard deviation.

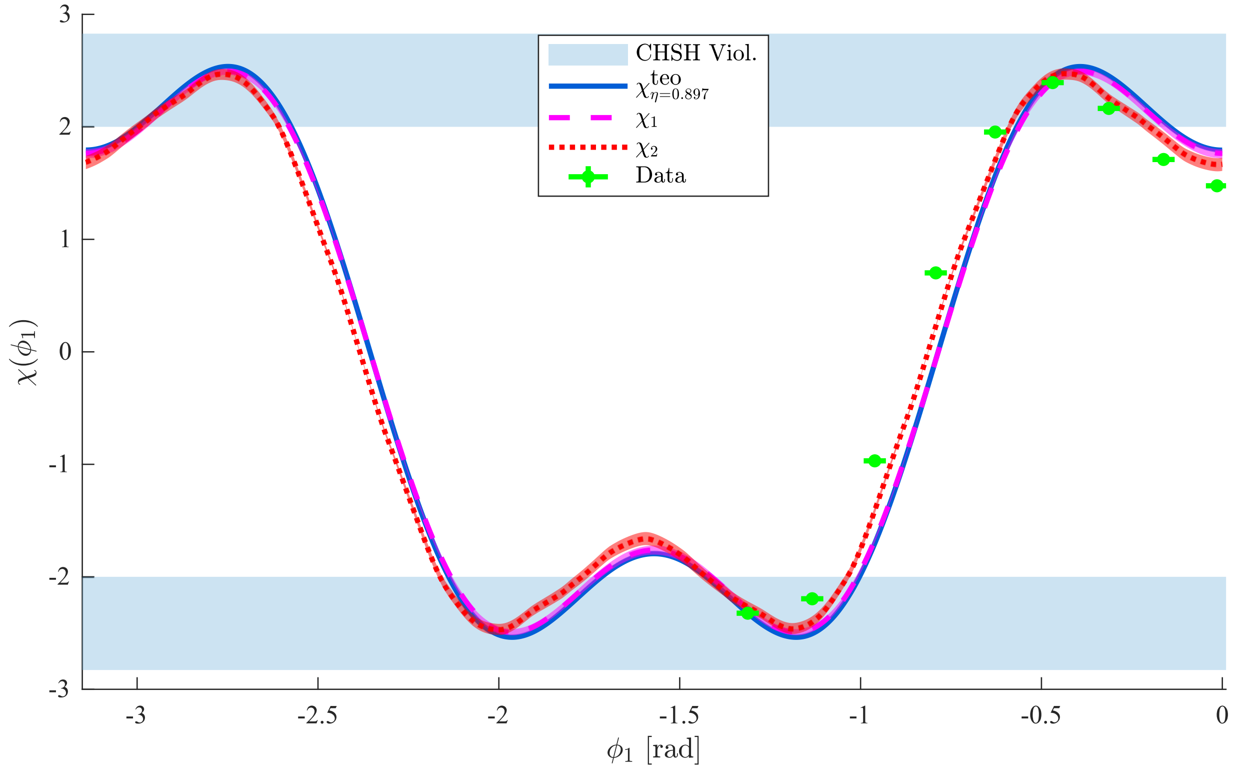


**Figure 4.23:** Evaluation of $\chi$-parameter for the state $|\phi^+\rangle$. The experimental data (green dots) are plotted as a function of the rotation angle $\phi_1$ with the respective error bars. The solid blue line represents the theoretical forms of the $\chi$-parameter in the case of Equation 4.49 with $\eta_2 = 0.897 \pm 0.003$. The dashed purple line $\chi_1$ represents the $\chi$-parameter obtained by fitting procedure over the raw data, with only $\eta$ as the free parameter. It is also reported the 95% confidence interval. The dotted red line is the $\chi$-parameter obtained by the two fitting operations performed on the data, leaving one angle and the $\eta$ as parameters. Also for this fit, it is reported the 95% confidence interval. Lastly, in cyan are indicated the areas in which the violation of the CHSH inequality can be observed.

### 4.7.2 Bell's Inequality for $|\phi^-\rangle$

The same experimental procedure was followed also in the case of $|\phi^-\rangle$ just by changing the value of $W_{\xi_1}$ with the one reported in Subsection 4.6.3. The same intervals $\phi \in [-2.2]$ rad and $\theta \in [-2, 0]$ rad are used. The experimental correlation coefficients $\mathbb{E}\left(O_\phi, O_\theta\right)$ are reported in Figure 4.24a as a fuction of $\phi$ and $\theta$. Now the theoretical form of the correlation coefficients is:

$$\mathbb{E}_{\mathrm{Fit}}\left(O_\phi, O_\theta\right) = \eta\cos(2(\phi+\theta)). \tag{4.50}$$

The fit of the data using Equation 4.50 with $\eta$ as parameters and $\phi$ and $\theta$ as variable is reported in Figure 4.24a and the connected residuals plot in Figure 4.24b. Also in this situation, the oscillations that appear are probably connected to the instability of the power supply. In this case, a mean visibility of $\eta_1 = 0.89 \pm 0.01$ is obtained. Using the second methodology (an angle as a fit parameter), a visibility of $\eta_2 = 0.904 \pm 0.002$ is estimated. The $\chi$-parameter as a function of the angle $\phi_0$ ($\phi_0 = \omega/2, \phi_1 = -\omega/2, \theta_0 = 0, \theta_1 = \omega$) has the same form of Equation 4.49. Both the $\chi_1$ and $\chi_2$, obtained by the fitting procedure (dashed purple line and dotted red line), and $\chi_{\mathrm{data}}$ (green dots) are reported in Figure 4.25 together with the theoretical form (Equation 4.49 for $\omega = 2\phi_0$, blue curve). The obtained $\chi$-parameters follow the theoretical form of Equation 4.49 apart from the already observed lateral shift. The maximal and minimal values of $\chi$, estimated using the raw data, are reported in Table 4.6: $\chi^{\phi_2}$ indicates the values reported in Figure 4.25, while $\chi^{\mathrm{rec}}$ the ones obtained

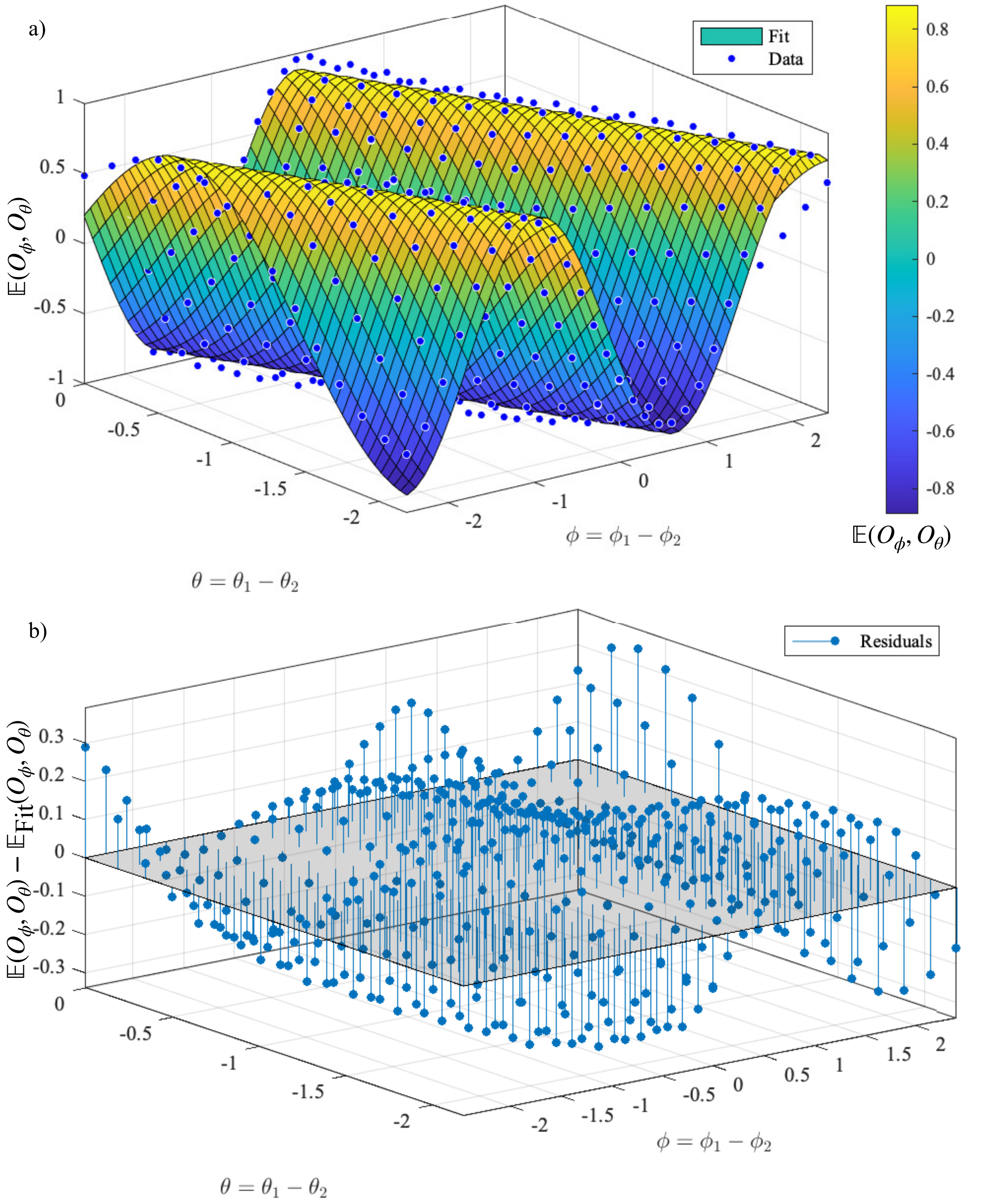


**Figure 4.24:** a) Raw correlation coefficients $\mathbb{E}_{\text{Fit}}\left(O_\phi, O_\theta\right)$ )(blue dots) obtained during the experiment with the relative fit $\mathbb{E}_{\text{Fit}}\left(O_\phi, O_\theta\right) = \eta_1 \cos(2(\phi + \theta))$ (colored surface) where $\phi$ and $\theta$ are the variables and $\eta_1$ is a fit parameter. From the fit operation, it is obtained $\eta_1 = 0.89 \pm 0.01$. b) Residuals plot of the fitted raw data $\mathbb{E}\left(O_\phi, O_\theta\right)$ respect to the fit $\mathbb{E}_{\text{Fit}}\left(O_\phi, O_\theta\right)$. The physical origin of the oscillations observed is probably the power supply instability.

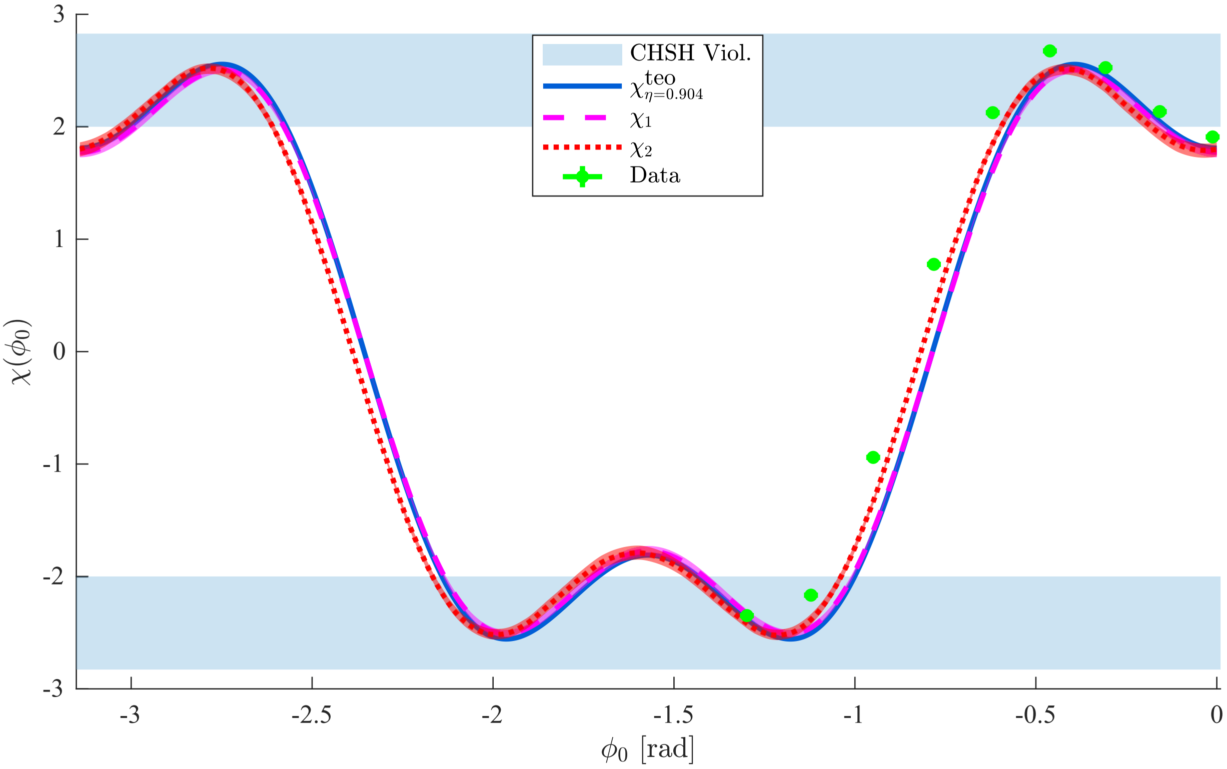


**Figure 4.25:** Evaluation of $\chi$-parameter for the state $|\phi^-\rangle$. The experimental data (green dots) are plotted as a function of the rotation angle $\phi_0$ with the respective error bars. The solid blue line represents the theoretical forms of the $\chi$-parameter in the cases of Equation 4.49 with $\eta_2 = 0.904 \pm 0.002$ and choice $\phi_0$ ($\phi_0 = \omega/2, \phi_1 = -\omega/2, \theta_0 = 0, \theta_1 = \omega$). The dashed purple line $\chi_1$ represents the $\chi$-parameter obtained by fitting procedure over the raw data, with only $\eta$ as a free parameter. It is also reported the 95% confidence interval. The dotted red line is the $\chi$-parameter obtained by the two fitting operations performed on the data, leaving one angle and the $\eta$ as parameters. Also for this fit, it is reported the 95% confidence interval. Lastly, in cyan are indicated the areas in which the violation of the CHSH inequality can be observed.

using the recursive approach as described in the $|\phi^+\rangle$ case.

**Table 4.6:** Maximal absolute violations of the BI observed for the state $|\phi^-\rangle$. $\chi^{\phi_2}$ refers to the values reported in Figure 4.25, while $\chi^{\text{rec}}$ to the maximum and minimum violations observed by comparing every possible combination of correlation coefficients.

| | Max | Min |
|---|---|---|
| $\chi^{\phi_0}$ | $2.67 \pm 0.02$ | $-2.35 \pm 0.02$ |
| $\chi^{\text{rec}}$ | $2.738 \pm 0.004$ | $-2.679 \pm 0.004$ |

## 4.8 Discussion of the results

The experimental demonstration of the SPE based on HSP has given encouraging results. A violation of the BI in the CHSH form was observed in many different working points, which allows concluding that the entanglement is present. However, further steps have to be done. The fundamental and mandatory one is the development of a model which considers the current instabilities introduced by the power supply. These spoil the product form of the operators created by the different MZIs. It is important to recall that this step is necessary not only to ensure a trustful violation of the BI but also for the generation and certification of genuine quantum random numbers. Concerning the experimental setup, the power supply has to be stabilized to compensate for the current fluctuations induced in each arm of the different MZI when high currents are implied. Finally, with the new design of Figure 4.21, no separate measurements to collect all the four channels are needed which reduces the acquisition time.

Even though there is ample margin of improvement, the results of this chapter show that a compact integrated photonic chip enables a quantum information task. This task is quantum random number generation in a market-reliable SDI-QRNG. Let us estimate the random number generation rate that this device might provide. Having a SPAD dynamical range of ≃ few MHz, hundreds of kHz generation rate could be achieved assuming an ideal randomness extraction procedure. Further improvements to the rate could be obtained by multiplexing of the SPADs as suggested in Chapter 3. Other applications of this integrated source of SPE states are quantum key distribution, entanglement swapping and quantum teleportation[154] .

[154]: Azzini et al. (2020), 'Single-Particle Entanglement'

# Conclusion 5

In this PhD thesis, I have demonstrated that Single Photon Entanglement (SPE) is achievable by using bulk optical components and attenuated sources via a Bell's Inequality (BI) experiment. The BI experiment is performed on SPE states where the photon's momentum is entangled with its polarization. The photons come from commercial attenuated sources like a laser, a LED and a halogen lamp. The violation of the BI was obtained under a few simple assumptions:

1) the experimental setup is not malicious, i.e., the free of will loophole is handled;
2) some optical elements are characterized, i.e., the communication effects induced by the locality loophole can be bounded;
3) the detectors are trusted and characterized, i.e., the detection and memory loopholes are handled.

Under these assumptions, the observed violation of the BI can be safely considered a faithful one. Experiments of generation of SPE states have already been reported in the literature using as DoFs momentum-polarization[33, 34] , but also momentum-spin[36] and spin-orbit[35] . The fundamental difference that distinguishes my work is the use of commercial light sources (laser, LED and halogen lamp) to generate the SPE states and no non-linear optical processes. This represents a significant advantage for applications, increasing the scientific community's attention towards this type of entanglement. Indeed, SPE is simpler than Multi Particles Entanglement (MPE) because only bulk commercial linear optical components like Beam Splitters (BSs), Half-Wave Plates (HWPs) and Mirrors (MRs) are necessary to generate and manipulate it. From the point of view of the test of the BI, both SPE and MPE present some analogies. To make a fair comparison, consider a situation in which no random choice of the measurement basis is implemented and SPADs are used as detectors. The detection, post-selection, and memory loopholes can be tackled similarly for the two types of entanglement (see Chapter 2). The only loophole that has to be considered differently is the locality loophole: in the case of MPE, a simple solution consists of separating or shielding the detection stages. However, this approach requires the introduction of synchronized and precise coincidence measurements that enhance the experimental difficulties of such an experiment. On the contrary, in the case of SPE, only single-photon detection events are necessary to test the inequality, not requiring any sophisticated coincidence electronics. This simplification comes at the price of introducing a partial but simple characterization of the experimental setup, which decreases the achievable BI violation.

SPE states of momentum and polarization are then used to demonstrate a Semi-Device Independent Quantum Random Number Generator (SDI-QRNG). This represents the first example of a SDI-QRNG based on SPE states. The certification of the conditional min-entropy is based on the violation of the BI and the partial characterization of some elements of the experimental setup. In particular, the polarization non-idealities

[33]: Michler et al. (2000), 'Experiments towards Falsification of Noncontextual Hidden Variable Theories'
[34]: Gadway et al. (2009), 'Bell-inequality violations with single photons entangled in momentum and polarization'
[36]: Chen et al. (2010), 'Single-photon spin-orbit entanglement violating a Bell-like inequality'
[35]: Karimi et al. (2010), 'Spin-orbit hybrid entanglement of photons and quantum contextuality'

of a few optical components and the non-idealities of the SPADs are considered. No assumptions must be introduced about the form of the input state, which can be left uncharacterized. Moreover, the protocol is independent of the particular form of the measurement observables, which have just to be kept independent. I achieved a kHz-generation rate of certified quantum random numbers, assuming a perfect randomness extraction. Compared to other SDI-QRNGs present in the literature[18, 120–127, 129–131, 133–135] the obtained rate is low since MHz and GHz SDI-QRNGs have already been reported. However, the generation rate can be improved by increasing the flux of photons and by the multiplexing of different SPADs. This last represents an essential aspect for discriminating the behavior of single photons.

I have also discussed the SPE generated in a photonic chip using the Hidden Subsystems of Path (HSP) as two effective qubits. In the device, both the source of SPE state and its certification, based on the BI, are integrated. The generation scheme of the entanglement is extremely simple, requiring only one Multi-Mode Interferometer (MMI) and two Phase shifters (PSs). The test of the BI is instead implemented using MZIs, Crossings (CRs) and PSs, which are well-known integrated components already present in many Process Design Kits (PDKs). All these optical devices were simulated and experimentally characterized. Even considering the not optimal performances of the integrated photonic circuit, a considerable violation of the BI was observed. It is important to remark that the observed violations are just preliminary results since the locality loophole is not closed or bounded in the experimental implementation. Due to the inability to set the same phase on the pair of MZIs that perform the rotations because of the instability of the power supply, it is impossible to confirm that the observed violations are faithful. Further work has to be done to ensure these results effectively. Concerning the other loopholes, these have been handled by introducing the assumptions already used for the bulk version, with the additional requirement that the physical conditions of the chip and the rotations do not change during the acquisition time. This further hypothesis must be introduced due to relative phases induced by the fabrication errors that cannot be compensated. Such a problem can be fixed by introducing other PSs in the future implementation of the photonic circuit. The integrated implementation is more compact, robust, and cheap with respect to the bulk version. These characteristics motivate the use of this source of entangled state for other quantum information tasks: the first is the generation of certified quantum random numbers, as done for the bulk version in Chapter 3. Such an integrated SDI-QRNG is potentially adopted for many Internet of Things devices to ensure quantum security. Another possible perspective concerns the use in Quantum Key Distribution (QKD). Today, QKD applications are limited to research purposes, with only a few real-world applications adopted by governments, banks and militaries. Critical aspects that slow down the adoption of this technology are the price and the footprint of the available devices, which are prohibitive for many applications. In this context, the availability of an integrated source of entangled states is particularly interesting. Indeed, it opens to the possibility of producing a fully integrated system for QKD, where both the optical and electronic components are integrated on the same chip. Moreover, SPE has already been proposed as a tool for improving the security of QKD[154, 173] . Such a level of integration paired with

[173]: Adhikari et al. (2015), ‘Toward secure communication using intra-particle entanglement’
[154]: Azzini et al. (2020), ‘Single-Particle Entanglement’

the enhanced security guaranteed by the entanglement could result in a more secure solution than the already available ones, primarily based on bulk components. The integrated device presented here will possibly push forward the deployment of QKD applications on the market. I am presently working in this direction.

# Publications and Conferences

## List of Publications

- **Nicolò Leone**, Davide Rusca, Stefano Azzini, Giorgio Fontana, Fabio Acerbi, Alberto Gola, Alessandro Tontini, Nicola Massari, Hugo Zbinden, and Lorenzo Pavesi , "An optical chip for self-testing quantum random number generation", APL Photonics 5, 101301 (2020);

- Matteo Pasini, **Nicolò Leone**, Sonia Mazzucchi, Valter Moretti, Davide Pastorello, and Lorenzo Pavesi, "Bell-inequality violation by entangled single-photon states generated from a laser, an LED, or a halogen lamp", Phys. Rev. A 102, 063708 (2020);

- Sonia Mazzucchi, **Nicolò Leone**, Stefano Azzini, Lorenzo Pavesi, and Valter Moretti, "Entropy certification of a realistic quantum random-number generator based on single-particle entanglement", Phys. Rev. A 104, 022416 (2021);

- **Nicolò Leone**, Stefano Azzini, Sonia Mazzucchi, Valter Moretti, and Lorenzo Pavesi, "Certified Quantum Random-Number Generator Based on Single-Photon Entanglement", Phys. Rev. Applied 17, 034011 (2022).

## List of Conferences

- SPIE Optics and Photonics, Online Event, 24/08/20, Oral presentation: Single Particle Entanglement as a tool for generating quantum random numbers;

- Italian conference on Optics and Photonics (ICOP), Online Event, 08/09/20, Oral presentation: Towards certified QRNG based on Single Particle Entanglement;

- 2nd European Quantum Technologies Virtual Conference (EQTC), Online Event, 01/12/21, Poster presentation: Simple and certified quantum random numbers generator employing linear optic devices.

# Bibliography

[1] Michael G Raymer and Christopher Monroe. 'The US national quantum initiative'. In: *Quantum Science and Technology* 4.2 (2019), p. 020504 (cited on page 3).

[2] Qiang Zhang et al. 'Quantum information research in China'. In: *Quantum Science and Technology* 4.4 (2019), p. 040503 (cited on page 3).

[3] Max Riedel et al. 'Europe's quantum flagship initiative'. In: *Quantum Science and Technology* 4.2 (2019), p. 020501 (cited on page 3).

[4] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. 'Quantum Random Number Generators'. In: *Reviews of Modern Physics* 89 (Apr. 2017). DOI: 10.1103/RevModPhys.89.015004 (cited on pages 3, 64, 67, 68).

[5] JKMS Zaman and Ranjan Ghosh. 'Review on fifteen Statistical Tests proposed by NIST'. In: *Journal of Theoretical Physics and Cryptography* 1 (2012), pp. 18–31 (cited on page 3).

[6] Meltem Sönmez Turan et al. 'Recommendation for the entropy sources used for random bit generation'. In: *NIST Special Publication* 800.90B (2018), p. 102 (cited on page 3).

[7] Robert Konig, Renato Renner, and Christian Schaffner. 'The operational meaning of min-and max-entropy'. In: *IEEE Transactions on Information theory* 55.9 (2009), pp. 4337–4347 (cited on pages 4, 68).

[8] Frederick James and Lorenzo Moneta. 'Review of high-quality random number generators'. In: *Computing and Software for Big Science* 4.1 (2020), pp. 1–12 (cited on page 4).

[9] Auguste Kerckhoffs. 'La cryptographic militaire'. In: *Journal des sciences militaires* (1883), pp. 5–38 (cited on page 4).

[10] Huang Zhun and Chen Hongyi. 'A truly random number generator based on thermal noise'. In: *ASICON 2001. 2001 4th International Conference on ASIC Proceedings (Cat. No. 01TH8549)*. IEEE. 2001, pp. 862–864 (cited on page 4).

[11] Yue Hu et al. 'A true random number generator based on mouse movement and chaotic cryptography'. In: *Chaos, Solitons & Fractals* 40.5 (2009), pp. 2286–2293 (cited on page 4).

[12] Albert Einstein. *The Collected Papers of Albert Einstein, Volume 15 (Translation Supplement): The Berlin Years: Writings & Correspondence, June 1925–May 1927.* Princeton University Press, 2018 (cited on page 4).

[13] JB Manelis. 'Generating random noise with radioactive sources'. In: *Electronics (US)* 34.36 (1961) (cited on pages 4, 63).

[14] John G Rarity, PCM Owens, and PR Tapster. 'Quantum random-number generation and key sharing'. In: *Journal of Modern Optics* 41.12 (1994), pp. 2435–2444 (cited on pages 4, 64).

[15] Antonio Acín and Lluis Masanes. 'Certified randomness in quantum physics'. In: *Nature* 540.7632 (2016), pp. 213–219 (cited on pages 4, 69).

[16] John F Clauser et al. 'Proposed experiment to test local hidden-variable theories'. In: *Physical Review letters* 23.15 (1969), p. 880 (cited on pages 5, 16, 47).

[17] Stefano Pironio et al. 'Random Numbers Certified by Bell's Theorem'. In: *Nature* 464 (Apr. 2010), pp. 1021–4. DOI: 10.1038/nature09008 (cited on pages 5, 69).

[18] Jonatan Bohr Brask et al. 'Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination'. In: *Phys. Rev. Applied* 7 (5 May 2017), p. 054018. DOI: 10.1103/PhysRevApplied.7.054018 (cited on pages 5, 7, 71, 72, 126).

[19] Marco Avesani et al. 'Source-device-independent heterodyne-based quantum random number generator at 17 Gbps'. In: *Nature Communications* 9.1 (2018), p. 5365. DOI: 10.1038/s41467-018-07585-0 (cited on pages 5, 87).

[20] Thomas Van Himbeeck and Stefano Pironio. 'Correlations and randomness generation based on energy constraints'. In: *arXiv preprint arXiv:1905.09117* (2019) (cited on pages 5, 71).

[21] Sonia Mazzucchi et al. 'Entropy certification of a realistic quantum random-number generator based on single-particle entanglement'. In: *Phys. Rev. A* 104 (2 Aug. 2021), p. 022416. DOI: 10.1103/PhysRevA.104.022416 (cited on pages 5, 6, 32, 35, 81).

[22] SJ Van Enk. 'Single-particle entanglement'. In: *Physical Review A* 72.6 (2005), p. 064306 (cited on page 5).

[23] Matteo Pasini et al. 'Bell-inequality violation by entangled single-photon states generated from a laser, an LED, or a halogen lamp'. In: *Phys. Rev. A* 102 (6 Dec. 2020), p. 063708. DOI: 10.1103/PhysRevA.102.063708 (cited on pages 6, 51, 82).

[24] J. S. Bell. 'On the Einstein Podolsky Rosen paradox'. In: *Physics Physique Fizika* 1 (3 Nov. 1964), pp. 195–200. DOI: 10.1103/PhysicsPhysiqueFizika.1.195 (cited on pages 6, 11).

[25] Nicolò Leone et al. 'Certified Quantum Random-Number Generator Based on Single-Photon Entanglement'. In: *Physical Review Applied* 17.3 (2022), p. 034011 (cited on pages 6, 71, 81, 85).

[26] Michael A Nielsen and Isaac Chuang. *Quantum computation and quantum information*. 2002 (cited on page 9).

[27] E. Schrödinger. 'Die gegenwärtige Situation in der Quantenmechanik'. In: *Naturwissenschaften* 23.48 (1935), pp. 807–812. DOI: 10.1007/BF01491891 (cited on page 9).

[28] Albert Einstein, Boris Podolsky, and Nathan Rosen. 'Can quantum-mechanical description of physical reality be considered complete?' In: *Physical Review* 47.10 (1935), p. 777 (cited on page 10).

[29] D. Bohm and Y. Aharonov. 'Discussion of Experimental Proof for the Paradox of Einstein, Rosen, and Podolsky'. In: *Phys. Rev.* 108 (4 Nov. 1957), pp. 1070–1076. DOI: 10.1103/PhysRev.108.1070 (cited on page 11).

[30] Valerio Scarani. *Bell nonlocality*. Oxford Graduate Texts, 2019 (cited on pages 13, 78, 80).

[31] Reinhard F. Werner. 'Quantum states with Einstein - Podolsky - Rosen correlations admitting a hidden-variable model'. In: *Phys. Rev. A* 40 (8 Oct. 1989), pp. 4277–4281. DOI: 10.1103/PhysRevA.40.4277 (cited on page 13).

[32] C. Monroe et al. 'A "Schrödinger Cat" Superposition State of an Atom'. In: *Science* 272.5265 (1996), pp. 1131–1136. DOI: 10.1126/science.272.5265.1131 (cited on page 14).

[33] M. Michler, H. Weinfurter, and M. Żukowski. 'Experiments towards Falsification of Noncontextual Hidden Variable Theories'. In: *Phys. Rev. Lett.* 84 (24 June 2000), pp. 5457–5461. DOI: 10.1103/PhysRevLett.84.5457 (cited on pages 14, 16, 125).

[34] B. R. Gadway, E. J. Galvez, and F. De Zela. 'Bell-inequality violations with single photons entangled in momentum and polarization'. In: *Journal of Physics B: Atomic, Molecular and Optical Physics* 42.1 (2009), p. 015503 (cited on pages 14, 53, 125).

[35] Ebrahim Karimi et al. 'Spin-orbit hybrid entanglement of photons and quantum contextuality'. In: *Phys. Rev. A* 82 (2 Aug. 2010), p. 022115. DOI: 10.1103/PhysRevA.82.022115 (cited on pages 14, 125).

[36] Lixiang Chen and Weilong She. 'Single-photon spin-orbit entanglement violating a Bell-like inequality'. In: *J. Opt. Soc. Am. B* 27.6 (June 2010), A7–A10. DOI: 10.1364/JOSAB.27.0000A7 (cited on pages 14, 125).

[37] Sayandeb Basu et al. 'Bell's inequality for a single spin-1/2 particle and quantum contextuality'. In: *Physics Letters A* 279.5 (2001), pp. 281–286. DOI: https://doi.org/10.1016/S0375-9601(00)00747-7 (cited on page 14).

[38] Yuji Hasegawa et al. 'Violation of a Bell-like inequality in single-neutron interferometry'. In: *Nature* 425.6953 (2003), pp. 45–48. DOI: 10.1038/nature01881 (cited on page 14).

[39] S. Sponar et al. 'Violation of a Bell-like inequality for spin-energy entanglement in neutron polarimetry'. In: *Physics Letters A* 374.3 (2010), pp. 431–434. DOI: https://doi.org/10.1016/j.physleta.2009.11.017 (cited on page 14).

[40] H. Geppert et al. 'Improvement of the polarized neutron interferometer setup demonstrating violation of a Bell-like inequality'. In: *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment* 763 (2014), pp. 417–423. DOI: https://doi.org/10.1016/j.nima.2014.06.080 (cited on page 14).

[41] J. Shen et al. 'Unveiling contextual realities by microscopically entangling a neutron'. In: *Nature Communications* 11.1 (2020), p. 930. DOI: 10.1038/s41467-020-14741-y (cited on page 14).

[42] Julio T. Barreiro et al. 'Generation of Hyperentangled Photon Pairs'. In: *Phys. Rev. Lett.* 95 (26 Dec. 2005), p. 260501. DOI: 10.1103/PhysRevLett.95.260501 (cited on page 16).

[43] Francesco Ceccarelli et al. 'Recent Advances and Future Perspectives of Single-Photon Avalanche Diodes for Quantum Photonics Applications'. In: *Advanced Quantum Technologies* 4.2 (2021), p. 2000102. DOI: https://doi.org/10.1002/qute.202000102 (cited on pages 21, 48).

[44] Matthew D Eisaman et al. 'Invited review article: Single-photon sources and detectors'. In: *Review of scientific instruments* 82.7 (2011), p. 071101 (cited on page 37).

[45] S. Magnitskiy et al. 'A SPDC-Based Source of Entangled Photons and its Characterization'. In: *Journal of Russian Laser Research* 36 (Nov. 2015). DOI: 10.1007/s10946-015-9540-x (cited on page 37).

[46] H. Takesue and K. Inoue. 'Generation of polarization-entangled photon pairs and violation of Bell's inequality using spontaneous four-wave mixing in a fiber loop'. In: *Phys. Rev. A* 70 (3 Sept. 2004), 031802(R). DOI: 10.1103/PhysRevA.70.031802 (cited on page 37).

[47] Howard M Wiseman. 'How many principles does it take to change a light bulb. . . into a laser?' In: *Physica Scripta* 91.3 (Mar. 2016), p. 033001. DOI: 10.1088/0031-8949/91/3/033001 (cited on page 38).

[48] Adam Vallés et al. 'Generation of tunable entanglement and violation of a Bell-like inequality between different degrees of freedom of a single photon'. In: *Physical Review A* 90.5 (2014), p. 052326 (cited on page 44).

[49] Itamar Holzman and Yachin Ivry. 'Superconducting Nanowires for Single-Photon Detection: Progress, Challenges, and Opportunities'. In: *Advanced Quantum Technologies* 2.3-4 (2019), p. 1800058. DOI: https://doi.org/10.1002/qute.201800058 (cited on page 46).

[50] Philip M. Pearle. 'Hidden-Variable Example Based upon Data Rejection'. In: *Phys. Rev. D* 2 (8 Oct. 1970), pp. 1418–1425. DOI: 10.1103/PhysRevD.2.1418 (cited on page 47).

[51] Patrick Billingsley. 'Statistical methods in Markov chains'. In: *The Annals of Mathematical Statistics* (1961), pp. 12–40 (cited on page 51).

[52] E Ammicht and H Wenzelburger. 'Maximum-likelihood estimators for the transition probabilities of a reversible Markov chain'. In: *IFAC Proceedings Volumes* 15.4 (1982), pp. 1113–1115 (cited on page 51).

[53] Thorlabs. *Thorlabs Non-Polarizing Cube Beamsplitters (400 - 700 nm)*. 2021. URL: https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=754 (visited on 12/19/2021) (cited on page 54).

[54] Robert JC Spreeuw. 'A classical analogy of entanglement'. In: *Foundations of physics* 28.3 (1998), pp. 361–374 (cited on page 61).

[55] Andrei Khrennikov. 'Quantum Versus Classical Entanglement: Eliminating the Issue of Quantum Nonlocality'. In: *Foundations of Physics* (2020). DOI: 10.1007/s10701-020-00319-7 (cited on page 61).

[56] Pawel Kurzyński Marcin Markiewicz Dagomir Kaszlikowski and Antoni Wójcik. 'From contextuality of a single photon to realism of an electromagnetic wave'. In: *npj Quantum Information* 5 (2019), p. 5 (cited on page 61).

[57] Helmut Schmidt. 'Quantum-mechanical random-number generator'. In: *Journal of Applied Physics* 41.2 (1970), pp. 462–468 (cited on page 63).

[58] CH Vincent. 'The generation of truly random binary numbers'. In: *Journal of Physics E: Scientific Instruments* 3.8 (1970), p. 594 (cited on page 63).

[59] Ammar Alkassar, Thomas Nicolay, and Markus Rohe. 'Obtaining True-Random Binary Numbers from a Weak Radioactive Source'. In: vol. 3481. May 2005, pp. 634–646. DOI: 10.1007/11424826_67 (cited on page 63).

[60] André Stefanov et al. 'Optical quantum random number generator'. In: *Journal of Modern Optics* 47.4 (2000), pp. 595–598 (cited on page 64).

[61] Thomas Jennewein et al. 'A fast and compact quantum random number generator'. In: *Review of Scientific Instruments* 71.4 (2000), pp. 1675–1680 (cited on page 64).

[62] Qiurong Yan et al. 'Multi-bit quantum random number generation by measuring positions of arrival photons'. In: *Review of Scientific Instruments* 85.10 (2014), p. 103116 (cited on page 64).

[63] Hai-Qiang Ma, Yuejian Xie, and Ling-An Wu. 'Random number generation based on the time of arrival of single photons'. In: *Applied optics* 44.36 (2005), pp. 7760–7763 (cited on page 64).

[64] Mario Stipčević and Branka Rogina. 'Quantum random number generator based on photonic emission in semiconductors'. In: *Rev. Sci. Instrum.* 78 (May 2007), p. 045104. DOI: 10.1063/1.2720728 (cited on page 64).

[65] Michael Wayne et al. 'Photon arrival time quantum random number generation'. In: *J. Mod. Opt* 56 (Feb. 2009), pp. 516–522. DOI: 10.1080/09500340802553244 (cited on page 64).

[66] Michael Wahl et al. 'An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements'. In: *Appl. Phys. Lett* 98.17 (2011), p. 171105 (cited on page 64).

[67] You-Qi Nie et al. 'Practical and fast quantum random number generation based on photon arrival time relative to external reference'. In: *Applied Physics Letters* 104.5 (2014), p. 051110 (cited on page 64).

[68] A. Khanmohammadi et al. 'A Monolithic Silicon Quantum Random Number Generator Based on Measurement of Photon Detection Time'. In: *IEEE Photon. J.* 7.5 (2015), pp. 1–13 (cited on pages 64, 93).

[69] Z. Bisadi et al. 'Robust Quantum Random Number Generation With Silicon Nanocrystals Light Source'. In: *J. Light. Technol.* 35.9 (2017), pp. 1588–1594 (cited on pages 64, 93).

[70] Zahra Bisadi et al. 'Compact Quantum Random Number Generator with Silicon Nanocrystals Light Emitting Device Coupled to a Silicon Photomultiplier'. In: *Front. Phys.* 6 (Feb. 2018), p. 9. DOI: 10.3389/fphy.2018.00009 (cited on pages 64, 93).

[71] Hesong Xu et al. 'A 16×16 pixel post-processing free quantum random number generator based on SPADs'. In: *IEEE Trans. Circuits Syst. II Express Briefs* 65 (May 2018), pp. 627–631. DOI: 10.1109/TCSII.2018.2821904 (cited on pages 64, 93).

[72] F. Acerbi et al. 'A Robust Quantum Random Number Generator Based on an Integrated Emitter-Photodetector Structure'. In: *IEEE J. Sel. Top. Quantum Electron.* 24.6 (Nov. 2018), pp. 1–7. DOI: 10.1109/JSTQE.2018.2814787 (cited on pages 64, 71, 93).

[73] Hesong Xu et al. 'A SPAD-based random number generator pixel based on the arrival time of photons'. In: *Integration* 64 (2019), pp. 22–28. DOI: https://doi.org/10.1016/j.vlsi.2018.05.009 (cited on pages 64, 93).

[74] Andrea Stanco et al. 'Efficient random number generation techniques for CMOS single-photon avalanche diode array exploiting fast time tagging units'. In: *Physical Review Research* 2.2 (2020), p. 023287 (cited on page 64).

[75] Harald Fürst et al. 'High speed optical quantum random number generation'. In: *Opt. Express* 18.12 (June 2010), pp. 13029–13037. DOI: 10.1364/OE.18.013029 (cited on pages 64, 93).

[76] Min Ren et al. 'Quantum random-number generator based on a photon-number-resolving detector'. In: *Phys. Rev. A* 83 (2 Feb. 2011), p. 023820. DOI: 10.1103/PhysRevA.83.023820 (cited on page 64).

[77] Bruno Sanguinetti et al. 'Quantum random number generation on a mobile phone'. In: *Physical Review X* 4.3 (2014), p. 031056 (cited on pages 64, 93).

[78] Simone Tisa et al. 'High-speed quantum random number generation using CMOS photon counting detectors'. In: *IEEE Journal of Selected Topics in Quantum Electronics* 21.3 (2014), pp. 23–29 (cited on page 64).

[79] M.J. Applegate et al. 'Efficient and robust quantum random number generation by photon number detection'. In: *Appl. Phys. Lett* 107 (Aug. 2015). DOI: 10.1063/1.4928732 (cited on page 64).

[80] Emna Amri et al. 'Quantum random number generation using a quanta image sensor'. In: *Sensors* 16.7 (2016), p. 1002 (cited on page 64).

[81] Gaëtan Gras et al. 'Quantum Entropy Model of an Integrated Quantum-Random-Number-Generator Chip'. In: *Physical Review Applied* 15.5 (2021), p. 054048 (cited on page 64).

[82] Wei Wei and Hong Guo. 'Bias-free true random-number generator'. In: *Optics letters* 34.12 (2009), pp. 1876–1878 (cited on page 64).

[83] Wei Wei and Hong Guo. 'Quantum random number generator based on the photon number decision of weak laser pulses'. In: *Conference on Lasers and Electro-Optics/Pacific Rim*. Optical Society of America. 2009, TUP5_41 (cited on page 64).

[84] Z Bisadi et al. 'Silicon nanocrystals for nonlinear optics and secure communications'. In: *physica status solidi (a)* 212.12 (2015), pp. 2659–2671 (cited on page 64).

[85] Zahra Bisadi et al. 'Quantum random number generator based on silicon nanocrystals led'. In: *Integrated Photonics: Materials, Devices, and Applications III*. Vol. 9520. International Society for Optics and Photonics. 2015, p. 952004 (cited on page 64).

[86] Mario Stipčević and Rupert Ursin. 'An on-demand optical quantum random number generator with in-future action and ultra-fast response'. In: *Scientific reports* 5.1 (2015), pp. 1–8 (cited on page 64).

[87] Yong Shen, Liang Tian, and Hongxin Zou. 'Practical quantum random number generator based on measuring the shot noise of vacuum states'. In: *Physical Review A* 81.6 (2010), p. 063814 (cited on page 64).

[88] Christian Gabriel et al. 'A generator for unique quantum random numbers based on vacuum states'. In: *Nat. Photonics* 4 (Oct. 2010), pp. 711–715. DOI: 10.1038/nphoton.2010.197 (cited on page 64).

[89] Ziyong Zheng et al. '6 Gbps real-time optical quantum random number generator based on vacuum fluctuation'. In: *Review of Scientific Instruments* 90.4 (2019), p. 043105 (cited on page 64).

[90] M. Jofre et al. 'True random numbers from amplified quantum vacuum'. In: *Opt. Express* 19.21 (Oct. 2011), pp. 20665–20672. DOI: 10.1364/OE.19.020665 (cited on page 64).

[91] Feihu Xu et al. 'Ultrafast quantum random number generation based on quantum phase fluctuations'. In: *Opt. Express* 20.11 (May 2012), pp. 12366–12377. DOI: 10.1364/OE.20.012366 (cited on page 64).

[92] Carlos Abellan et al. 'Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode'. In: *Opt. Express* 22 (Jan. 2014), pp. 1645–54. DOI: 10.1364/OE.22.001645 (cited on page 64).

[93] You-Qi Nie et al. 'The generation of 68 Gbps quantum random number by measuring laser phase fluctuations'. In: *Review of Scientific Instruments* 86.6 (2015), p. 063105 (cited on page 64).

[94] Carlos Abellan et al. 'Quantum entropy source on an InP photonic integrated circuit for random number generation'. In: *Optica* 3.9 (Sept. 2016), pp. 989–994. DOI: 10.1364/OPTICA.3.000989 (cited on pages 64, 93).

[95] Xiao-Guang Zhang et al. 'Fully integrated 3.2 Gbps quantum random number generator with real-time extraction'. In: *Rev. Sci. Instrum.* 87 (June 2016), p. 076102 (cited on pages 64, 93).

[96] Francesco Raffaelli et al. 'A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers'. In: *Quantum Sci. Technol.* 3.2 (Feb. 2018), p. 025003. DOI: 10.1088/2058-9565/aaa38f (cited on pages 64, 93).

[97] Francesco Raffaelli et al. 'Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip'. In: *Opt. Express* 26.16 (Aug. 2018), pp. 19730–19741. DOI: 10.1364/OE.26.019730 (cited on pages 64, 93).

[98] Miquel Rudé et al. 'Interferometric photodetection in silicon photonics for phase diffusion quantum entropy sources'. In: *Opt. Express* 26.24 (Nov. 2018), pp. 31957–31964. DOI: 10.1364/OE.26.031957 (cited on pages 64, 93).

[99] IDQuantique. *IDQuantique ID Quantique and SK Telecom unveil the Samsung Galaxy Quantum2, the newest QRNG-Powered 5G smartphone with even more embedded secured applications*. 2021. URL: https://www.idquantique.com/id-quantique-and-sk-telecom-unveil-the-samsung-galaxy-quantum2-the-newest-qrng-powered-5g-smartphone-with-even-more-embedded-secured-applications/ (visited on 12/2021) (cited on page 64).

[100] IDQuantique. *IDQuantique ID Quantique integrates its quantum chip in Vsmart Aris 5G Smartphone*. 2021. URL: https://www.idquantique.com/id-quantique-integrates-its-quantum-chip-in-vsmart-aris-5g-smartphone/ (visited on 12/2021) (cited on page 64).

[101] C. E. Shannon. 'A Mathematical Theory of Communication'. In: *Bell System Technical Journal* 27.3 (1948), pp. 379–423. DOI: https://doi.org/10.1002/j.1538-7305.1948.tb01338.x (cited on page 65).

[102] Michael A Nielsen and Isaac L Chuang. 'Quantum computation and quantum information'. In: *Phys. Today* 54.2 (2001), p. 60 (cited on page 65).

[103] Alfréd Rényi. 'On measures of entropy and information'. In: *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*. University of California Press. 1961, pp. 547–561 (cited on page 66).

[104] Xiongfeng Ma et al. 'Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction'. In: *Phys. Rev. A* 87 (6 June 2013), p. 062327. DOI: 10.1103/PhysRevA.87.062327 (cited on pages 68, 69).

[105] 'Extractors and Pseudorandom Generators'. In: *J. ACM* 48.4 (July 2001), pp. 860–879. DOI: 10.1145/502090.502099 (cited on page 69).

[106] Y. Mansour, N. Nisan, and P. Tiwari. 'The computational complexity of universal hashing'. In: *Proceedings Fifth Annual Structure in Complexity Theory Conference*. 1990, pp. 90–. DOI: 10.1109/SCT.1990.113957 (cited on page 69).

[107] Noam Nisan and Amnon Ta-Shma. 'Extracting Randomness: A Survey and New Constructions'. In: *J. Comput. Syst. Sci.* 58 (1999), pp. 148–173 (cited on page 69).

[108] Stefano Pironio and Serge Massar. 'Security of practical private randomness generation'. In: *Phys. Rev. A* 87 (1 Jan. 2013), p. 012336. DOI: 10.1103/PhysRevA.87.012336 (cited on page 69).

[109] Martin Plesch and Matej Pivoluska. 'Device-independent randomness amplification with a single device'. In: *Physics Letters A* 378.40 (2014), pp. 2938–2944 (cited on page 69).

[110] Rotem Arnon-Friedman et al. 'Practical device-independent quantum cryptography via entropy accumulation'. In: *Nature communications* 9.1 (2018), pp. 1–11 (cited on page 69).

[111] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. 'Simple and tight device-independent security proofs'. In: *SIAM Journal on Computing* 48.1 (2019), pp. 181–225 (cited on page 69).

[112] Peter Bierhorst et al. 'Experimentally generated randomness certified by the impossibility of superluminal signals'. In: *Nature* 556.7700 (2018), pp. 223–226 (cited on page 70).

[113] Yang Liu et al. 'Device-independent quantum random-number generation'. In: *Nature* 562.7728 (2018), pp. 548–551 (cited on page 70).

[114] Yang Liu et al. 'High-speed device-independent quantum random number generation without a detection loophole'. In: *Physical review letters* 120.1 (2018), p. 010503 (cited on page 70).

[115] Lijiong Shen et al. 'Randomness extraction from bell violation with continuous parametric down-conversion'. In: *Physical review letters* 121.15 (2018), p. 150402 (cited on page 70).

[116] Yanbao Zhang et al. 'Experimental low-latency device-independent quantum randomness'. In: *Physical review letters* 124.1 (2020), p. 010505 (cited on page 70).

[117] Lynden K Shalm et al. 'Device-independent randomness expansion with entangled photons'. In: *Nature Physics* 17.4 (2021), pp. 452–456 (cited on page 70).

[118] Wen-Zhao Liu et al. 'Device-independent randomness expansion against quantum side information'. In: *Nature Physics* 17.4 (2021), pp. 448–451 (cited on page 70).

[119] G. Vallone et al. 'Quantum randomness certified by the uncertainty principle'. In: *Phys. Rev. A* 90.5 (2014), p. 052327. DOI: 10.1103/PhysRevA.90.052327 (cited on page 71).

[120] Z. Cao et al. 'Source-Independent Quantum Random Number Generation'. In: *Phys. Rev. X* 6.1 (2016), p. 011020. DOI: 10.1103/PhysRevX.6.011020 (cited on pages 71, 126).

[121] D. G. Marangon, G. Vallone, and P. Villoresi. 'Source-Device-Independent Ultrafast Quantum Random Number Generation'. In: *Phys. Rev. Lett.* 118 (6 2017), p. 060503. DOI: 10.1103/PhysRevLett.118.060503 (cited on pages 71, 87, 126).

[122] Marco Avesani et al. 'Source-device-independent heterodyne-based quantum random number generator at 17 Gbps'. In: *Nature communications* 9.1 (2018), pp. 1–7 (cited on pages 71, 92, 126).

[123] Thibault Michel et al. 'Real-Time Source-Independent Quantum Random-Number Generator with Squeezed States'. In: *Phys. Rev. Applied* 12 (3 Sept. 2019), p. 034017. DOI: 10.1103/PhysRevApplied.12.034017 (cited on pages 71, 126).

[124] Peter Raymond Smith et al. 'Simple source device-independent continuous-variable quantum random number generator'. In: *Physical Review A* 99.6 (2019), p. 062326 (cited on pages 71, 126).

[125] Bingjie Xu et al. 'High speed continuous variable source-independent quantum random number generation'. In: *Quantum Science and Technology* 4.2 (2019), p. 025013 (cited on pages 71, 126).

[126] Yu-Huai Li et al. 'Quantum random number generation with uncharacterized laser and sunlight'. In: *npj Quantum Information* 5.1 (2019), pp. 1–5 (cited on pages 71, 95, 126).

[127] Yanbao Zhang et al. 'A simple low-latency real-time certifiable quantum random number generator'. In: *Nature Communications* 12.1 (2021), p. 1056. DOI: 10.1038/s41467-021-21069-8 (cited on pages 71, 126).

[128] Z. Cao, H. Zhou, and X. Ma. 'Loss-tolerant measurement-device-independent quantum random number generation'. In: *New J. Phys.* 17.12 (2015), p. 125011. DOI: 10.1088/1367-2630/17/12/125011 (cited on page 71).

[129] You-Qi Nie et al. 'Experimental measurement-device-independent quantum random-number generation'. In: *Physical Review A* 94.6 (2016), p. 060301 (cited on pages 71, 126).

[130] Matej Pivoluska et al. 'Semi-device-independent random number generation with flexible assumptions'. In: *npj Quantum Information* 7.1 (2021), pp. 1–12 (cited on pages 71, 126).

[131] Nicolò Leone et al. 'An optical chip for self-testing quantum random number generation'. In: *APL Photonics* 5.10 (2020), p. 101301. DOI: 10.1063/5.0022526 (cited on pages 71, 73–77, 126).

[132] T. Van Himbeeck et al. 'Semi-device-independent framework based on natural physical assumptions'. In: *Quantum* 1 (2017), p. 33. DOI: 10.22331/q-2017-11-18-33 (cited on page 71).

[133] Davide Rusca et al. 'Self-testing quantum random-number generator based on an energy bound'. In: *Phys. Rev. A* 100.6 (2019), p. 062338 (cited on pages 71, 126).

[134] Davide Rusca et al. 'Fast self-testing quantum random number generator based on homodyne detection'. In: *Applied Physics Letters* 116.26 (2020), p. 264004. DOI: 10.1063/5.0011479 (cited on pages 71, 92, 93, 126).

[135] Marco Avesani et al. 'Semi-Device-Independent Heterodyne-Based Quantum Random-Number Generator'. In: *Physical Review Applied* 15.3 (2021), p. 034034 (cited on pages 71, 126).

[136] Hamid Tebyanian et al. 'Semi-device-independent randomness from d-outcome continuous-variable detection'. In: *Physical Review A* 104.6 (2021), p. 062424 (cited on page 71).

[137] Hamid Tebyanian et al. 'Semi-device independent randomness generation based on quantum state's indistinguishability'. In: *Quantum Science and Technology* 6.4 (2021), p. 045026 (cited on page 71).

[138] H.-W. Li et al. 'Semi-device-independent random-number expansion without entanglement'. In: *Phys. Rev. A* 84 (3 2011), p. 034301. DOI: 10.1103/PhysRevA.84.034301 (cited on page 71).

[139] J. Bowles, M. T. Quintino, and N. Brunner. 'Certifying the Dimension of Classical and Quantum Systems in a Prepare-and-Measure Scenario with Independent Devices'. In: *Phys. Rev. Lett.* 112 (14 2014), p. 140407. DOI: 10.1103/PhysRevLett.112.140407 (cited on page 71).

[140] Piotr Mironowicz et al. 'Quantum randomness protected against detection loophole attacks'. In: *Quantum Information Processing* 20.1 (2021), pp. 1–20 (cited on page 71).

[141] T. Lunghi et al. 'Self-Testing Quantum Random Number Generator'. In: *Phys. Rev. Lett.* 114 (15 2015), p. 150501. DOI: 10.1103/PhysRevLett.114.150501 (cited on page 71).

[142] Devin H. Smith et al. 'Conclusive quantum steering with superconducting transition-edge sensors'. In: *Nature Communications* 3.1 (2012), p. 625. DOI: 10.1038/ncomms1628 (cited on page 71).

[143] ALASTAIR A. Abbott, CRISTIAN S. Calude, and KARL Svozil. 'A quantum random number generator certified by value indefiniteness'. In: *Mathematical Structures in Computer Science* 24.3 (2014), e240303. DOI: 10.1017/S0960129512000692 (cited on page 71).

[144] I.D. Ivanovic. 'How to differentiate between non-orthogonal states'. In: *Physics Letters A* 123.6 (1987), pp. 257–259. DOI: https://doi.org/10.1016/0375-9601(87)90222-2 (cited on page 72).

[145] D. Dieks. 'Overlap and distinguishability of quantum states'. In: *Physics Letters A* 126.5 (1988), pp. 303–306. DOI: https://doi.org/10.1016/0375-9601(88)90840-7 (cited on page 72).

[146] Asher Peres. 'How to differentiate between non-orthogonal states'. In: *Physics Letters A* 128.1 (1988), p. 19. DOI: https://doi.org/10.1016/0375-9601(88)91034-1 (cited on page 72).

[147] Stephen M. Barnett and Sarah Croke. 'Quantum state discrimination'. In: *Adv. Opt. Photon.* 1.2 (Apr. 2009), pp. 238–278. DOI: 10.1364/AOP.1.000238 (cited on page 72).

[148] Zahra Bisadi. 'All-Silicon-Based Photonic Quantum Random Number Generators'. PhD thesis. Via Sommarive 14, Trento: Department of Physics, University of Trento, July 2017 (cited on pages 72, 75, 76).

[149] N. Akil et al. 'A multimechanism model for photon generation by silicon junctions in avalanche breakdown'. In: *IEEE Trans. Electron Devices* 46.5 (1999), pp. 1022–1028 (cited on page 73).

[150] D. E. Aspnes and A. A. Studna. 'Dielectric functions and optical parameters of Si, Ge, GaP, GaAs, GaSb, InP, InAs, and InSb from 1.5 to 6.0 eV'. In: *Phys. Rev. B* 27 (2 Jan. 1983), pp. 985–1009. DOI: 10.1103/PhysRevB.27.985 (cited on page 76).

[151] Antonio Acín, Serge Massar, and Stefano Pironio. 'Randomness versus nonlocality and entanglement'. In: *Physical review letters* 108.10 (2012), p. 100402 (cited on page 78).

[152] Ryszard Horodecki, Pawel Horodecki, and Michal Horodecki. 'Violating Bell inequality by mixed spin-12 states: necessary and sufficient condition'. In: *Physics Letters A* 200.5 (1995), pp. 340–344 (cited on page 79).

[153] Valter Moretti. *Fundamental Mathematical Structures of Quantum Theory*. Springer, 2019. Chap. 5 (cited on page 82).

[154] Stefano Azzini et al. 'Single-Particle Entanglement'. In: *Advanced Quantum Technologies* 3.10 (2020), p. 2000014 (cited on pages 82, 124, 126).

[155] G. H Golub; C. F. Van Loan. *Matrix computations(3rd ed.)* "Baltimore : Johns Hopkins University Press", 1996 (cited on page 83).

[156] Nicholas JD Martinez et al. 'Single photon detection in a waveguide-coupled Ge-on-Si lateral avalanche photodiode'. In: *Optics express* 25.14 (2017), pp. 16130–16139 (cited on page 92).

[157] Martino Bernard et al. 'Top-down convergence of near-infrared photonics with silicon substrate-integrated electronics'. In: *Optica* 8.11 (2021), pp. 1363–1364 (cited on page 92).

[158] Marco Avesani et al. 'Semi-Device-Independent Heterodyne-Based Quantum Random-Number Generator'. In: *Phys. Rev. Applied* 15 (3 Mar. 2021), p. 034034. DOI: 10.1103/PhysRevApplied.15.034034 (cited on page 92).

[159] Chenlei Li, Dajian Liu, and Daoxin Dai. 'Multimode silicon photonics'. In: *Nanophotonics* 8.2 (2019), pp. 227–247 (cited on page 93).

[160] Valter Moretti. *Fundamental Mathematical Structures of Quantum Theory*. Springer, 2019. Chap. 6 (cited on pages 93, 100).

[161] Bahaa EA Saleh and Malvin Carl Teich. *Fundamentals of photonics*. john Wiley & sons, 2019 (cited on pages 94, 95).

[162] Comsol Multiphysics. *Comsol Multiphysics Comsol Multiphysics main page*. 2021. URL: https://www.comsol.it (visited on 01/2022) (cited on page 94).

[163] Ansys / Lumerical. *Ansys / Lumerical Lumerical main page*. 2021. URL: https://www.lumerical.com (cited on page 94).

[164] Aseema Mohanty et al. 'Quantum interference between transverse spatial waveguide modes'. In: *Nature communications* 8.1 (2017), pp. 1–7 (cited on page 95).

[165] Richard J Bojko et al. 'Electron beam lithography writing strategies for low loss, high confinement silicon optical waveguides'. In: *Journal of Vacuum Science & Technology B, Nanotechnology and Microelectronics: Materials, Processing, Measurement, and Phenomena* 29.6 (2011), 06F309 (cited on page 95).

[166] Lucas B Soldano and Erik CM Pennings. 'Optical multi-mode interference devices based on self-imaging: principles and applications'. In: *Journal of lightwave technology* 13.4 (1995), pp. 615–627 (cited on pages 95, 96).

[167] RM Knox and PP Toulios. 'Integrated circuits for the millimeter through optical frequency range'. In: *Proc. Symp. Submillimeter Waves*. Vol. 20. Brooklyn, NY. 1970, pp. 497–515 (cited on page 95).

[168] Alberto Peruzzo et al. 'Multimode quantum interference of photons in multiport integrated devices'. In: *Nature communications* 2.1 (2011), pp. 1–6 (cited on page 96).

[169] Yang Zhang et al. 'Ultralow-loss silicon waveguide crossing using Bloch modes in index-engineered cascaded multimode-interference couplers'. In: *Optics letters* 38.18 (2013), pp. 3608–3611 (cited on page 97).

[170] J Komma et al. 'Thermo-optic coefficient of silicon at 1550 nm and cryogenic temperatures'. In: *Applied Physics Letters* 101.4 (2012), p. 041905 (cited on page 97).

[171] Joshua W Silverstone et al. 'On-chip quantum interference between silicon photon-pair sources'. In: *Nature Photonics* 8.2 (2014), pp. 104–108 (cited on page 99).

[172] Jianwei Wang et al. 'Multidimensional quantum entanglement with large-scale integrated optics'. In: *Science* 360.6386 (2018), pp. 285–291 (cited on page 99).

[173] Satyabrata Adhikari et al. 'Toward secure communication using intra-particle entanglement'. In: *Quantum Information Processing* 14.4 (2015), pp. 1451–1468 (cited on page 126).

# Special Terms

**A**

**AMS** Amplification and Manipulation stage. 73–75

**B**

**BE** Bounded energy. 71

**BI** Bell's Inequality. viii–x, 5–7, 9, 12, 13, 15–17, 24–28, 43, 46, 47, 51, 54, 55, 60, 61, 69, 70, 79, 81–83, 87, 91, 93, 100, 103, 104, 108, 112, 113, 116, 118, 120, 124–126

**BS** Beam Splitter. viii, x, 16, 17, 19, 20, 28, 29, 34, 35, 40, 41, 43, 53, 54, 65, 67, 83, 95, 96, 98, 105, 115, 125

**BSD** Bounded system dimensionality. 71

**BSO** Bounded states overlap. 71

**C**

**C** Collimator. 51, 52

**CHSH** Clauser, Horne, Shimony and Holt. vi, 6, 9, 16, 22, 23, 25, 44, 55, 57–60, 63, 78, 79, 83, 121, 123, 124

**CPL** Comparable Polarization Losses. 34, 35

**CR** Crossing. vii, ix, 93, 95–98, 102, 105–111, 126

**D**

**DCR** Dark count rate. 47, 48, 50, 52, 87, 88

**DD-QRNG** Device Dependent Quantum Random Number Generator. 91

**DI+A** Device independent + assumptions. 71

**DI-QRNG** Device Independent Quantum Random Number Generator. 4–7, 63, 69, 70, 78, 81, 91

**DL** Delay Line. viii, 17, 53, 54

**DoF** Degree of Freedom. 5, 6, 14, 16, 19, 28, 40, 52, 82, 89, 93, 95, 99, 100, 102, 125

**E**

**EME** Eigenmode expansion. 105

**EPR** Einstein, Podolsky and Rosen. vi, 6, 9–11, 13

**F**

**FPGA** Field programmable gate array. 51, 52, 73–75, 88

**G**

**GTP** Glan-Thompson Polarizer. 16, 17

**H**

**HSP** Hidden Subsystems of Path. vii, ix, 93, 99–103, 107, 112, 113, 116, 124, 126

**HWP** Half-Wave Plate. viii, 16–21, 28, 35, 44, 52, 53, 55, 58, 59, 85–87, 91, 108, 125

**I**

**IF** Interference filter. 51, 52, 55

**L**

**LED** Light-emitting diode. viii, x, 6, 37, 52, 53, 55–59, 92, 125

**M**

**MI** Measurement Independent. 71

**MMI** Multi-Mode Interferometer. vii, ix, x, 93, 95–98, 102, 103, 105–111, 113, 115, 126

**MPE** Multi Particles Entanglement. 5, 6, 14, 15, 28, 82, 125

**MR** Mirror. x, 16, 17, 19, 28, 29, 34, 35, 52–54, 125

**MZI** Mach Zehnder Interferometer. vii, ix, x, 19, 20, 28, 29, 36, 44, 52–54, 81, 87, 93, 98, 99, 102–105, 107, 110, 112–118, 124, 126

**N**

**NIST** National Institute of Standards and Technology. 3

**O**

**OOK** On-Off-Keying. 72

**OSA** Optical spectrum analyzer. 108, 109

**P**

**PBS** Polarized Beam Splitter. 17, 21

**PCB** Printed Circuit Board. 110, 113

**PDK** Process Design Kit. 126

**POVM** Positive operator-valued measure. 71

**PRNG** Pseudo Random Number Generator. 4, 93

**PS** Phase shifter. vii, ix, 93, 97–99, 102–105, 107, 110, 112, 113, 115–118, 126

**PVM** Projection-valued measure. 18, 78

**PZT** Piezoelectric transducer. 52, 53, 56, 57, 87

**Q**

**QC** Quantum contextuality. 71

**QKD** Quantum Key Distribution. 126, 127

**QRNG** Quantum Random Number Generator. viii, 3–7, 63–65, 67–71, 73, 74, 77, 82–84, 86, 87, 91–93

**QS** Quantum steering. 71

**QWP** Quarter-Wave Plate. 108

**R**

**RNG** Random Number Generator. 3, 4, 63, 67–69

**S**

**SDI-QRNG** Semi-Device Independent Quantum Random Number Generator. vi, vii, ix, x, 5–7, 63, 70, 71, 73, 75, 77, 81, 84, 87, 89, 91, 92, 124–126

**SDP** Semi-Definite Program. 72

**SI** Source Independent. 71, 91

**SiPM** Silicon Photomultiplier. 73, 74, 76, 92

**SNSPD** Superconducting Nanowire Single Photon Detector. 45

**SPAD** Single Photon Avalanche Diode. x, 17, 21, 28, 41, 46–48, 51–53, 73–77, 82, 83, 87, 88, 91, 92, 102, 103, 110, 112, 124–126

**SPaE** Single Particle Entanglement. 9, 14–16

**SPE** Single Photon Entanglement. vi–ix, 5–7, 9, 16, 17, 22, 23, 28, 36, 37, 40, 41, 43, 52, 55, 60, 63, 78, 81–83, 85, 91–93, 95, 100, 102, 103, 107, 112, 113, 116, 124–126

**SQP** Sequential Quadratic Programming. 36, 54

**T**

**TE** Transverse electric. ix, 94, 105, 108, 110

**TM** Transverse magnetic. ix, 94

**TRNG** True Random Number Generator. 4, 93

**TTL** Transistor-transistor logic. 73, 74

**U**

**USD** Unambiguous State Discrimination. 72

**V**

**VOA** variable optical attenuator. 51, 52, 87, 88, 110, 112