

Deploying single photons towards experimental tests of Complementarity, Quantum Key Distribution, and Macrorealism



Kaushik Joarder

Supervisor: Prof. Urbasi Sinha

Light and Matter Physics Group

Raman Research Institute, Bangalore

A thesis submitted to

Jawaharlal Nehru University

for the degree of

Doctor of Philosophy

March 2022

Declaration

I hereby declare that the contents of this thesis are my original work, except where specific references are made to the work of other researchers. I have not submitted this thesis, in whole or in part, for consideration for any other degree or qualification in this or any other university. All the research works included in this thesis have been performed by me, under the supervision of Prof. Urbasi Sinha at the Raman Research Institute (RRI), Bangalore. In case of any collaborative work, it has been appropriately mentioned in the text and Acknowledgments. I also declare that I have run this thesis through the **Turnitin** plagiarism detection software.

Supervisor: Prof. Urbasi Sinha

Light and Matter Physics,
Raman Research Institute,
Bangalore - 560080, India

Kaushik Joarder

Light and Matter Physics,
Raman Research Institute,
Bangalore - 560080, India

Certification

This is to certify that the thesis titled “**Deploying single photons towards experimental tests of Complementarity, Quantum Key Distribution, and Macrorealism**” submitted by Kaushik Joarder for the award of the degree of Doctor of Philosophy of Jawaharlal Nehru University is a bonafide work. This has not been submitted to any other university for any other degree, diploma, or title.

Prof. S. Sridhar

Director,
Raman Research Institute,
Bangalore - 560080, India

Supervisor: Prof. Urbasi Sinha

Light and Matter Physics,
Raman Research Institute,
Bangalore - 560080, India

Acknowledgements

I want to thank my supervisor, Prof. Urbasi Sinha, for giving me the opportunity to work in various exciting research areas and also for providing proper guidance and motivation. I thank my project collaborators, Debadrita, Rishab, Sourav, Anuradha, Naga Lakshmi, Simanraj, Rakshita, Dr. Debashis Saha, Prof. Dipankar Home, and Prof. Barry Sanders, for giving me the necessary help, support and insight.

I thank Prof. Andal Narayanan and Prof. Ujjwal Sen for giving me advice and assessing the thesis work as my thesis advisory committee member. My thanks to the administrative department, members of the mechanical workshop, SAAC committee, purchase department, EEG, library, computer department, canteen staff of Raman Research Institute (RRI), whose support is essential for the various day-to-day activities in the institute. I am grateful to all LAMP group members for their support. My special thanks to Savitha ma'am and Shiva, Manju, for all their hard work and support.

I am grateful for the moral support I received from my family and friends in times of stress and failure. I thank my father, mother, and brother for always being present by my side. I thank my friend Sagar, Maheswar, Abhishek, Subhajit, Avik, Bapan, Anindya, Shovan, Dipak, Sanchari, Soumyajit, Ayan, Abhisek, Dipankar, Mouktik, Sayan, Reetam, Souvik for being part of this memorable journey. I also extend my gratitude to my lab seniors: Surya, Ashutosh, Animesh, for valuable discussion and advice. I am indebted to all my batchmates, seniors, juniors, and anyone I forgot to mention here.

Synopsis

Single photon is one of the most valuable resources in quantum science and technology. As being the single particle of light, it shows the behaviour of true quantumness, which is used in various quantum mechanical applications, including quantum information, communication, metrology, etc. There are various ways to prepare single photons [P4], among which spontaneous parametric down-conversion (SPDC) is the most popular one. In the SPDC process, single photon pairs are generated, where detection of one photon in the pair heralds the other photon of the same pair. In this thesis work, single photons generated from the SPDC process have been used in different experiments covering quantum fundamentals as well as technologies.

In the first experimental project, we have used indistinguishable single photons to generate a near-100% coincidence visibility dip or a Hong-Ou-Mandel (HOM) dip, which is a signature of the quantumness of light. My colleague in his research has shown, from both theoretical calculation and experimental demonstration, that with selective phase randomization of classical microwave pulse, it is possible to observe a coincidence-visibility dip of more than 50%. So, we also propose a diagnostics where we extend the HOM setup by adding a Mach-Zehnder interferometer (MZI) and demonstrate that while the photon state from the SPDC source shows wave-particle complementarity, the classical pulses do not.

We have designed and demonstrated a QKD experiment using single photons generated from the SPDC process, where we implement few strategies to enhance the practical security against any eavesdropper. We demonstrate the B92 protocol, which is a variant of the BB84 protocol and requires fewer resources than BB84, making it a good test-bed for in-lab experiments. For perfect security, truly random numbers are required for state preparation and

basis selection in measurement. But, in reality, it is difficult to generate true randomness, as all computer-generated random strings are actually pseudo-random as they follow some deterministic algorithm. We incorporate passive quantum randomness inside our setup. Also, our setup is tolerant of various eavesdropping attacks, including intercept-resend attack, photon number splitting (PNS) attack, Trojan horse attack, etc.

Another domain of study is related to a purely fundamental aspect of research, again using single photons. This involves tests of what is called macrorealism *per se*. Interestingly, it is shown in literature [106] that such studies may have ramifications for device-independent QKD as well. In this thesis, we demonstrate the violation of various macrorealistic inequalities while closing most of the loopholes existing in the literature. Recent studies in this subject are focused on weak or semi-weak measurement-based setup, as it is found that with projective measurement, it is theoretically impossible to close the clumsiness loophole without any additional assumptions. We have designed the experiment with all strong projective measurements and close the clumsiness loophole with minimal assumptions. This may also aid in the future adaption of the modified prepare and measure based QKD protocols using the test of macrorealism.

Hong-Ou-Mandel (HOM) interference and the role of Complementarity

The Hong-Ou-Mandel (HOM) effect [56] or the two-photon interference, which is a salient fourth-order interference effect, is considered as one of the most important phenomena in quantum optics and is a unique indicator of “quantumness” with absolutely no analog in classical physics. Due to its distinctive characteristics, the HOM effect is being used in various applications of quantum mechanics. HOM effect occurs when two indistinguishable photons hit the two input ports of a beam-splitter at the same time (within the coherence time of the photon) and interfere to produce a “dip” in the coincidence detection between the two output ports of the beam-splitter. This is not due to the second-order interference effect, as ideal single photons (Fock state $|1\rangle$) do not have any phase correlation. This is due to the intensity-intensity correlation (fourth-order interference), which is unique to the quantum state. So, instead of single photons, if two identical classical pulses with proper phase ran-

domization are sent to the beam-splitter, the maximum dip in visibility that can be achieved is only 50%. However, it is shown in reference [P1] that using selective phase randomization for classical pulses; visibility dip can be increased to 100%, similar to the quantum case. So, the 50% threshold for the dip in coincidence probability is not the boundary between classical and quantum behaviors of light but rather a result of the lack of control over the phases of the input pulses.

In the work reported in this thesis, we set up an experiment wherein we generate pairs of single photons from a type II collinear, degenerate SPDC process by hitting a non-linear BBO (Beta-Barium-Borate) crystal continuously with a pump beam of wavelength 405 nm. Both photons from each pair are made indistinguishable by applying appropriate spectral filtering, spatial filtering, and polarization control. Both photons are sent to a symmetric fiber beam-splitter (FBS) at the same time via the two input arms of the beam-splitter. Coincidence counts between the two output arms of the beam-splitter are measured and plotted against the time delay between the two input photons. The measured visibility dip from the experiment is $96.06 \pm 0.16\%$ [P1]. We extend the HOM setup for the complementarity test by adding another symmetric beam-splitter whose two input arms are connected to the two output ports of the FBS. Both the beam-splitters, in combination, form a Mach-Zehnder interferometer (MZI). A two-photon state shows wave-particle complementarity by being indivisible in an anti-correlation experiment vs. taking a superposition of two paths when interference is measured in the MZI, without any change in the source setting. Although classical pulses can be made to switch between exhibiting particle-like and wavelike behaviors by controlling the phase, both cannot manifest with the same choice of phase.

Experimental demonstration of secure quantum key distribution (QKD); B92 protocol

In a standard prepare and measure based QKD protocol operating in free-space, the polarization degree of freedom of individual photons is used for encoding information. The sender (Alice) prepares every photon with different polarization directions randomly selected from a set of choices for each photon and sends them to the receiver (Bob). The receiver also

measures different projection operations randomly for each photon. In the experimental demonstration of the B92 protocol in a free-space channel, Alice randomly selects the polarization state for each photon coming from a single photon source to be either vertical (V) or diagonal (D; $+45^\circ$ with respect to the horizontal polarization basis) and sends it to Bob. She also assigns bit values to all the photons based on their polarization and records them sequentially. Bob randomly selects his measurement basis to be horizontal (H) or anti-diagonal (A; -45° with respect to the horizontal polarization basis). Bob only considers those events where his measurements give positive (or non-null) results and announces only the occurrence (or timing) of these positive events in a public communication channel that could be prone to eavesdropping; once all the photons have been received. Bob never shares the choice of measurement operations for these positive events. Based on the announcement, Alice only keeps those bits that generate positive events in Bob's setup. Thus Alice and Bob generate and share an identical, secure key. In the presence of the channel noise or an eavesdropper, errors will be introduced in the key, which is easily detectable by Alice and Bob. If the error is below a certain threshold (4.8%), appropriate error correction and privacy amplification can be applied to extract a shorter but secure key, where the knowledge of the eavesdropper is negligibly small.

We have used spontaneous parametric down-conversion (SPDC) as a source of heralded single photons, which makes the experiment noise-tolerant as well as secure against PNS-type attacks. Random basis selection for Alice and Bob is performed using passive quantum randomness, where a single photon randomly selects which path of a symmetric beam-splitter to take. The inclusion of beam-splitter-based randomness requires some modification in Alice's module, where we implement a novel approach of correlating temporal degrees of freedom with the polarization of the photons. Alice encodes each photon with a randomly selected polarization basis as well as a correlated time delay. For example, V photons always have a time delay of $\delta\tau$, whereas $+45^\circ$ photons have no time delay. So, while Bob measures polarization, Alice measures time-delay in the post-processing stage. We report [P2] a key-rate of 51 ± 0.5 kbit/sec and quantum bit error rate (QBER) of $4.79 \pm 0.01\%$ respectively. To our knowledge, the reported key rate is the highest value to date, achieved in a heralded

single-photon-based B92 setup.

Loophole free test of macroscopic realism

Macroscopic realism (MR) is a classical worldview, which consists of three assumptions. The first one is the notion of realism (macrorealism *per se* or MRps), which states that a system always lies in any one of the possible states at any given time, irrespective of the measurement. So, in principle, this notion of reality denies the existence of the superposition of states. We can measure, at different time intervals, some observable Q which has different outcome (eigenvalues), on a system which is evolving with time. From these sequential measurements, two-time correlation of the form $\langle Q_{t_i} Q_{t_j} \rangle$ are constructed. For a system maintaining the notion of realism mentioned above, at all times of its evolution, these temporal correlation values are different than the correlation values obtained from a non-realist model. Leggett and Garg formulated the famous Leggett-Garg inequality (LGI) [76] using these correlation values. The other two assumptions of MR restrict that any past measurement should not affect the future measurement outcome (non-invasive measurement, or NIM) and restrict any future measurement from affecting the past (arrow of time or AoT). The AoT condition is always assumed to be valid, so for an experimentalist, maintaining NIM is a primary criterion to comment on the refutation of the notion of realism (MRps). Here, a macrorealist can always claim that the experiment is “clumsy” as the measurements performed are indeed invasive. Against such a claim, it is hard to establish that the violation of LGI means the violation of MRps. This loophole is called the *Clumsiness loophole* in the literature. There is no direct measurement technique to quantify the degree of invasiveness. However, there is a necessary condition to it which is called the no-signalling in time (NSIT) [27]; hence, it is necessary to maintain all relevant NSIT conditions. Based on the same assumptions of macrorealism, another set of inequalities called the Wigner form of LG inequalities (WLGI) was proposed [99], which consists of two-time joint probabilities rather than correlation values.

We have shown [P3] the violation of different macrorealist inequalities, i. e, LGI and WLGI, using a heralded, single-photon-based setup, where all relevant NSIT conditions are satisfied. All measurements are unambiguous, projective, while we close the clumsiness

loophole by performing three pairwise experiments, which are piece-wise non-invasive. We close the detection efficiency loophole by showing that for any non-zero detection efficiency, we can perform a loophole-free experiment with some modifications in the measurement strategy. We also address and close various other loopholes like multiple emission loophole, coincidence loophole, preparation state loophole. We report an LGI violation of 1.32 ± 0.04 and WLGI violation of 0.10 ± 0.02 in our setup, while at the same time, all three two-time NSIT conditions are satisfied. NSIT values are within the statistical fluctuations, $NSIT_{(t_1)t_2} = 0.002 \pm 0.017$, $NSIT_{(t_2)t_3} = 0.004 \pm 0.016$, and $NSIT_{(t_1)t_3} = 0.002 \pm 0.016$. Interestingly, loophole-free tests of macrorealist (MR) inequalities may have some ramifications in QKD. For instance, the LG-BB84 protocol proposed in [106] can be implemented for preventing what is called the AGM type device attack in QKD [2].

Summary

In summary, in this thesis, SPDC based single photons have been used towards applications in diverse areas of quantum fundamentals and technologies, including tests of complementarity, quantum key distribution as well as loophole-free tests of macrorealist inequalities, including the LGI as well as the WLGI. The results have wide-ranging ramifications as well as applications in the realm of quantum information science.

Supervisor: Prof. Urbasi Sinha

Light and Matter Physics,
Raman Research Institute,
Bangalore - 560080, India

Kaushik Joarder

Light and Matter Physics,
Raman Research Institute,
Bangalore - 560080, India

List of publications

[P1] S. Sadana, D. Ghosh, K. Joarder, A. N. Lakshmi, B. C. Sanders, and U. Sinha, *Near-100% two-photon-like coincidence-visibility dip with classical light and the role of complementarity*, Phys. Rev. A, **100**, 013839 (2019).

[P2] R. Chatterjee, K. Joarder, S. Chatterjee, B. C. Sanders, and U. Sinha, *qkdsim, a simulation toolkit for quantum key distribution including imperfections: Performance analysis and demonstration of the b92 protocol using heralded photons*, Phys. Rev. Applied, **14**, 024036 (2020).

[P3] K. Joarder, D. Saha, D. Home, and U. Sinha, *Loophole free interferometric test of macrorealism using heralded single photons*, PRX Quantum, **3**, 010307 (2022).

Publication in scientific magazine:

[P4] U. Sinha, S. N. Sahoo, A. Singh, K. Joarder, R. Chatterjee, and S. Chakraborti, *Single-Photon Sources*, Optics & Photonics News 30(9), 32-39 (2019).

Supervisor: Prof. Urbasi Sinha

Light and Matter Physics,
Raman Research Institute,
Bangalore - 560080, India

Kaushik Joarder

Light and Matter Physics,
Raman Research Institute,
Bangalore - 560080, India

Table of contents

1	Introduction	1
1.1	Overview and Motivation	1
1.2	Organization of the thesis	5
2	Single photon: overview of concepts and techniques	9
2.1	Characterization of single photons	10
2.1.1	Quantization of electromagnetic field	10
2.1.2	Photon number state	13
2.1.3	Photon number statistics	14
2.1.4	Second-order coherence and photon anti-bunching	15
2.1.5	Measurement of $g^2(\tau)$: Hanbury Brown and Twiss (HBT) Interfer-	
	ometer	17
2.2	Single-photon source using SPDC process	19
2.2.1	Pair generation rate in the SPDC process	20
2.2.2	Birefringent Phase matching in bulk crystals	26
2.2.3	Quasi-Phase matching in periodically-poled crystals	29
2.3	Single-photon detection	33
2.3.1	Silicon SPAD: working principle and properties	34
2.3.2	Coincidence detection using silicon SPAD	36
2.4	Single-photon interferometry	37
2.4.1	Mach-Zehnder interferometer	37
2.4.2	Sagnac interferometer	42
3	Hong-Ou-Mandel (HOM) interference and the role of Complementarity	45
3.1	Introduction	45
3.2	Theory	47
3.3	HOM experiment	55
3.3.1	Experimental setup	55
3.3.2	Results and theory fit to the experimental plot	59
3.4	HOM Complementarity	65
3.4.1	Experimental setup and results	67
3.4.2	Quantum mechanical description of HOM complementarity	68
3.5	Error analysis	72
4	Experimental demonstration of quantum key distribution (QKD); B92 protocol	77
4.1	Introduction	77
4.2	Basic concepts of quantum key distribution (QKD)	79
4.3	BB84 and B92 protocol	81
4.4	Experimental demonstration of B92 protocol	86

4.4.1	Heralded single-photon source	86
4.4.2	Alice-substation	87
4.4.3	Bob-substation	89
4.4.4	Post-processing via classical communication channel	89
4.4.5	Characterization of the crystal temperature	91
4.4.6	Pre-characterization of the polarization components	92
4.4.7	Data analysis	94
4.4.8	Advantages of the modified setup	102
4.5	Results and discussion	104
5	Loophole free test of macroscopic realism	113
5.1	Introduction	113
5.2	Theory	120
5.2.1	Proof based on macrorealist assumptions	121
5.2.2	Proof based on the ontic state description	125
5.2.3	Quantum mechanical bound	129
5.3	Loophole free version of the experiment	131
5.3.1	Clumsiness loophole	131
5.3.2	Detection efficiency loophole	136
5.3.3	Other loopholes	146
5.4	Experimental setup	152
5.4.1	Basic design of the setup	153
5.4.2	Details of the experiment	159
5.5	Results	164
5.5.1	LGI experiment using continuous-wave laser	164
5.5.2	LGI experiment with heralded single photon source: preliminary result	167
5.5.3	Troubleshooting	168
5.5.4	Final result with the heralded single photon source	178
5.6	Details on error analysis	184
5.6.1	Determining different experimental parameters from the measured joint probabilities	184
5.6.2	Measuring standard deviation of statistical fluctuation	186
5.6.3	Estimating the QM predicted values of LGI, WLGI and NSIT by incorporating experimental non-idealities	187
5.6.4	Determining the value of γ in our experimental setup.	190
5.7	Discussion and Conclusion	193
6	Summary and Outlook	197
6.1	Summary	197
6.2	Outlook	199
	References	203
	Appendix A How to plot coincidence between two detectors	213
	Appendix B QKD optimization algorithms	217
	Appendix C General data types and library functions	241

Chapter 1

Introduction

1.1 Overview and Motivation

A single photon is the most fundamental particle of light and is defined as the excitation of a single mode of the quantized electromagnetic field [29]. The operational definition is that if a single photon state is incident on an ideal photon-number resolving detector, it always creates a single click in the detector. In terms of photon-number statistics, single photon state follows a delta function with a mean value of 1 and a standard deviation of 0. Single photon is one of the most valuable resources in quantum science and technology. As being the single particle of light, it shows the behaviour of true quantumness, which is used in various quantum mechanical applications, including quantum information, communication, metrology, etc.

Single photon is advantageous in many quantum information tasks. Photon traverses at the speed of light and does not interact with the external electromagnetic field, as it is chargeless and massless. These characteristics make it a suitable resource for information processing. Photon is also easily manipulated with various linear optics like waveplates, beamsplitters, phase modulators, etc., which makes the system apparatus simpler and less resource-intensive. Various quantum mechanical states (qubit, qutrit, etc.) can be realized by using different degrees of freedom of the single photon state, including polarization, momentum, temporal modes, spatial modes, etc.

Single photon-based systems have been widely used as testbeds for various foundational ideas and principles in quantum mechanics. Most of the seminal experiments in quantum foundations were first performed using photons, which later paved the way for implementing those fundamental experiments in more complex systems using atoms, ions, and molecules. These include the loophole-free violation of Bell’s inequality [5, 49], other tests of non-locality, superdense coding, teleportation, entanglement swapping, steering, tests of weak measurements, etc.

In the field of quantum communication, single photon is most commonly used in quantum cryptography, or more precisely, in Quantum Key Distribution (QKD) [12, 34]. Single photon source and detectors are used in QKD, where every single photon carries the encoded information from the sender (Alice) to the receiver (Bob). Usage of single photons enhances the security of the cryptographic protocol. Also, single photons are an essential part of the quantum random number generators (QRNGs) [62], where the inherent “quantumness” associated with the single photon state is exploited to generate true randomness. QRNGs are inseparable from quantum communication-based applications.

There are various ways to prepare single photons, among which spontaneous parametric down-conversion (SPDC) [39, 41] is the most popular choice. Other types of photon sources include four-wave mixing (FWM) [33, 108], atomic energy level [70, 93], quantum dots [104, 57], nitrogen vacancy center [77, 42], etc. SPDC based single photon sources are the most prevalent, widely used, and researched sources in the quantum community. They are simpler in design than other sources but simultaneously produce single photons at a high rate and with good quality. Also, another interesting property of an SPDC source is the generation of “heralded” photons where single photons are always generated in pairs, and detection of one photon in the pair heralds the other photon of the same pair [55]. This heralding mechanism has many interesting applications in quantum experiments which have been thoroughly discussed in this thesis. Single photon pairs generated from an SPDC source are entangled in various degrees of freedom (spectral, polarization, etc.). They are good resources for various entanglement-based experiments, including QKD, Bell’s inequality test,

quantum repeaters, etc. In this thesis work, single photons generated from the SPDC process have been used in different experiments covering quantum fundamentals and technologies.

The inherent “quantumness” associated with single photons is the backbone of many applications in various quantum mechanical experiments. It is important to check for the degree of quantumness before using a single photon source in any experiment. The standard technique is to perform a Hong-Ou-Mandel (HOM) test where a quantum mechanical formalism predicts near 100% coincidence visibility dip [56, 78], and the classical formalism provides only up to 50% visibility dip [90, 66]. However, recently it has been shown that with some specific phase randomization strategies, a classical formalism can also achieve a near-100% coincidence visibility dip [98], which leads to a serious consequence in our conception of a quantum source. If we have to guess if a given source is quantum (produce single photons) or classical (produce classical pulse) where we don’t have any information about the internal mechanism of the device (acts as a black box), it becomes difficult just by performing a HOM test, as the malicious device manufacturer may have tricked with phase manipulation. To counter such a scenario, a modification of the standard HOM test is required. In this regard, the wave-particle complementarity relation of quantum mechanics is a possible alternative as a classical pulse with any phase manipulation cannot mimic the wave-particle duality of quantum mechanics. A modified experimental setup that houses both the HOM and the complementarity setup is capable of verifying the quantumness associated with the single photons and measuring the degree of indistinguishability between multiple photons.

Single photon is also an essential part of quantum cryptography. Most of the earlier demonstrations of the QKD experiment used weak coherent pulse (WCP) as an alternative to single photons due to the technical challenges of preparing single photons at that time. Usage of WCP creates a huge security loophole, where an eavesdropper (Eve) can use the non-negligible multi-photon generation probability in a WCP to her advantage. Eve can apply the so-called photon number splitting (PNS) attack, where she allows only one photon of a multi-photon pulse to reach Bob while she keeps the rest of the photons for future measurement in the classical communication stage of the QKD protocol. One can

also use decoy pulses along with the signal pulse to counter this type of security threat; however, it reduces the maximum key generation rate significantly. On the other hand, single photon sources are inherently tolerable to such attacks due to their negligible multi-photon generation probability. Heralded single photons generated from SPDC source along with appropriate filtering can be approximated to near-ideal single photons. Although the SPDC source, due to its probabilistic nature, has a limitation on the maximum key generation rate in QKD, it has several advantages as well, which will be covered in this thesis. In a standard prepare and measure based QKD protocol, both Alice and Bob's selection of preparation and measurement basis should be truly random for security reasons. In reality, this is not adequately maintained, as most experiments use either a pseudo-random number generator or some external quantum random number generators (QRNGs), which are also vulnerable to device-based attacks. In this case, the use of passive quantum randomness generation inside the QKD setup is advantageous. This modification also makes the setup tolerant to the trojan-horse attack [48] or large-pulse attack [113], where some intense external pulse can be used to gain knowledge of the internal settings of the QKD setup.

Heralded single photons are also very useful in another fundamental test in quantum mechanics, called the test of macrorealism. Single photons generated in an SPDC source have some degree of quantumness that can show specific temporal correlations otherwise impossible to observe in a classical worldview (more precisely macrorealist theory). According to the assumptions implied by the notion of macrorealism, any observable (Q) measured at different times (t_i) on a single system under unitary evolution can be used to construct various inequalities (Leggett-Garg inequality or LGI in short, Wigner form of LGI, etc.) with some upper bound. Quantum mechanics, by contrast, can violate these upper limits. Therefore, single photons are good candidates for experimental tests to determine if nature follows the notion of realism or the quantum mechanical principle of superposition. Single photon-based experimental setups are a good test-bed for such fundamental tests, as they are simplistic in design and also adaptable to more complex systems. They are also used to close various experimental "loopholes" associated with the test of macrorealism, including clumsiness loophole, detection efficiency loophole, etc. Another interesting perspective

is that the use of such tests of macrorealism has a broader application in the security of QKD, where such studies may have ramifications for device-independent security analysis of prepare and measure based QKD protocols [106].

In summary, the objectives of the thesis are the following.

- To study different properties and characteristics of the single photon state and how to use them in various quantum experiments, including the test of complementarity, the test of macrorealist inequalities, and quantum key distribution.
- To generate heralded single photons using spontaneous parametric down-conversion (SPDC) process in various types of non-linear crystals, i. e., beta barium borate (BBO), periodically poled potassium titanyl phosphate (PPKTP), and use the many advantages of this type of photon sources to the novel applications in quantum experiments.
- To verify the inherent quantumness and indistinguishability associated with the single photon pairs generated from an SPDC source, by showing near-100% Hong-Ou-Mandel (HOM) coincidence visibility dip, as well as showing wave-particle complementarity relation, in the same experimental setup.
- To enhance the security of a prepare and measure based QKD protocol (here, B92 protocol) against various eavesdropping attacks like photon number splitting (PNS) attack, Trojan-horse attack, time-shift attack, etc., by modifying the conventional B92 setup, and using heralded single photons.
- To show the violation of different macrorealist inequalities like Leggett-Garg inequality (LGI) and Wigner form of Leggett-Garg inequality (WLGI) in a loophole-free way, using heralded single photons from an SPDC source.

1.2 Organization of the thesis

Chapter 2 is devoted to the basic knowledge of single photons and various characteristics of them, where we discuss quantum mechanical field quantization, photon number state,

photon number statistics, second-order coherence or g^2 , photon anti-bunching, etc., as well as how to measure these properties using linear optics, optomechanics, and single photon detectors. For example, how to measure the g^2 profile using a Hanbury-Brown-Twiss (HBT) experiment with coincidence detection between two single photon detectors. We describe the spontaneous parametric down-conversion (SPDC) process with details in a non-linear crystal, which has been used to generate single photon pairs suitable for our various experiments. We also describe single photon-based interferometry using a Mach-Zehnder interferometer and a Sagnac interferometer, which has been used extensively in this thesis.

In chapter 3, we describe a Hong-Ou-Mandel (HOM) experiment, where a HOM visibility dip of 96% is achieved using “indistinguishable” photon pairs generated from an SPDC source. This result is not only the signature of “indistinguishability” but also the existence of “quantumness” in a single photon state. We also extend the conventional HOM setup with the inclusion of a complementarity test. Even if classical light pulses, with selective phase randomization, can mimic a near 100% HOM visibility dip, they cannot pass the complementarity test. We experimentally verify that the single photon pairs from an SPDC source exhibit wave-particle duality.

Chapter 4 deals with the experimental demonstration of a novel B92 QKD setup using heralded single photons generated from a continuously pumped SPDC process. Each photon pairs are generated randomly with time, and the polarization state of each heralded photon is randomly selected. All these random selections are performed using passive quantum randomness inherent to the single photon state. In this modified setup, polarization encoding is correlated with the temporal degree of freedom, which enhances the security of the protocol against various eavesdropping attacks and increases tolerance against background noise. These eavesdropping attacks include intercept-resend attack, photon number splitting (PNS) attack, Trojan horse attack, time-shift attack, etc.

In chapter 5, we describe how heralded single photons are used for an experimental demonstration of the violation of various macrorealistic inequalities like Leggett-Garg in-

equality (LGI) and the Wigner form of LGI (WLG). The experiment is designed such that all measurements are strong projective, but at the same time, most of the experimental loopholes existing in the literature are closed. We close the *clumsiness* loophole by applying ideal negative result measurement (INRM) as non-invasive measurement (NIM) and also by maintaining all relevant no-signalling in time (NSIT) conditions. *Detection efficiency* loophole is closed by modifying the strategy for measuring joint probabilities. We also close various other loopholes like multiple emission loophole, coincidence loophole, preparation state loophole, etc.

Finally, in chapter 6, we conclude the thesis by summarizing all works provided in the thesis. Also, a brief overview of the outlook is presented.

Chapter 2

Single photon: overview of concepts and techniques

To study single photons and their applications to diverse areas of quantum fundamentals and technologies, we need to understand first various properties and characteristics of single photons, e.g., how single photons are generated in the experimental setups, how they are detected and counted in a single photon detector. All experimental works described in the thesis use the spontaneous parametric down-conversion (SPDC) process as the means to generate single photons, so it is necessary to understand the underlying theoretical concepts of the SPDC process. We also describe various parameters of a single photon detector and the working principle of photon counting and coincidence detection using an avalanche-based semiconductor detector (SPAD). Single-photon based interferometry is also an essential part of most of the photon-based experiments described in the thesis. For that reason, we show a detailed study of the construction and performance of a Mach-Zehnder interferometer and a Sagnac interferometer as well.

In this chapter, we give an overview of all the elements which are essential for the understanding of the experimental setups presented in this thesis. Section 2.1 provides details of the characteristics of single photons, including photon number state, number distribution, photon anti-bunching, g^2 measurement, etc. Section 2.2 talks about SPDC based single photon source. In Section 2.3, we discuss various parameters and the working principle of a single-photon avalanche detector (SPAD). In Section 2.4 we discuss the Mach-Zehnder and

the Sagnac interferometers.

2.1 Characterization of single photons

A single photon is defined as the excitation of the quantized electromagnetic field. The most ideal single photon can be represented as the number state $|n\rangle = |1\rangle$, which has a sub-Poissonian statistical distribution. Single photon sources are characterized based on the number state distribution and the second-order coherence (g^2) value. We can measure these parameters by performing a Hanbury Brown and Twiss (HBT) experiment.

2.1.1 Quantization of electromagnetic field

As we know from the classical electromagnetic theory, electric $\vec{E}(\vec{r}, t)$ and magnetic field $\vec{B}(\vec{r}, t)$ can be written in terms of the vector potential $A(\vec{r}, t)$ [78]

$$\vec{E}(\vec{r}, t) = -\frac{\partial \vec{A}(\vec{r}, t)}{\partial t}, \quad (2.1a)$$

$$\vec{B}(\vec{r}, t) = \vec{\nabla} \times \vec{A}(\vec{r}, t), \quad (2.1b)$$

where $\vec{r}$ is the position vector and t is time. Using Equations (2.1a) and (2.1b) in the Maxwell's equations, we can get the wave equation written below [61]. Here, Coulomb gauge condition, i. e. $\vec{\nabla} \cdot \vec{A}(\vec{r}, t) = 0$ is also used.

$$\vec{\nabla}^2 \vec{A}(\vec{r}, t) = \frac{1}{c^2} \frac{\partial^2 \vec{A}(\vec{r}, t)}{\partial t^2} \quad (2.2)$$

where $c = \frac{1}{\sqrt{\mu_0 \epsilon_0}}$ is the speed of light in vacuum, μ_0 is the magnetic permeability in free-space and ϵ_0 is the electric permittivity in free-space. The multi-mode vector field $\vec{A}(\vec{r}, t)$ can be written using the periodic boundary conditions in a cubic volume of length L , where k

represents the mode [89]:

$$\vec{A}(\vec{r}, t) = \sum_{k,s} \vec{\epsilon}_{ks} A_{ks}(t) e^{i\vec{K} \cdot \vec{r}} + cc. \quad (2.3)$$

$\vec{K}$ is the wave vector, $\vec{\epsilon}$ is the polarization vector, $cc.$ stands for complex conjugate and A_{ks} denotes the mode function. There are two conditions that need to be satisfied. The first condition implies that the polarization direction of the EM wave and its direction of propagation are orthogonal to each other, $\vec{K} \cdot \vec{\epsilon}_{\vec{K}} = 0$. The second condition restricts the polarization vectors to be orthogonal to each other; $\vec{\epsilon}_{ks} \cdot \vec{\epsilon}_{ks'} = \delta_{s,s'}$. Using Equation (2.3) in (2.2), we obtain the following solution to the wave equation [89],

$$A_{ks}(t) = A_{ks} e^{-i\omega_k t}, \quad (2.4)$$

Here, $\omega_k = |\vec{K}|c$ represents the k^{th} mode frequency. Using this expression in Equation (2.3), we get,

$$\vec{A}(\vec{r}, t) = \sum_{k,s} \vec{\epsilon}_{ks} A_{ks} e^{i(\vec{K} \cdot \vec{r} - \omega_k t)} + cc. \quad (2.5)$$

According to the classical electromagnetic (EM) theory, the energy of the EM field is given by [61, 78],

$$H = \frac{1}{2} \int_V \epsilon_0 |\vec{E}|^2 dV + \frac{1}{2} \int_V \frac{1}{\mu_0} |\vec{B}|^2 dV, \quad (2.6)$$

Where V represents the mode volume. By applying Equation (2.5) while solving Equations (2.1a), (2.1b) and using the results in Equation (2.6) we get the following expression of the total energy [89],

$$H = \sum_{k,s} \epsilon_0 V \omega_k^2 A_{ks} A_{ks}^* + cc. \quad (2.7)$$

On the other hand, according to the quantum mechanics (QM), the quantized energy operator of the electromagnetic field can be written as [61],

$$\hat{H} = \sum_{k,s} \hbar \omega_k \left(\hat{n}_{ks} + \frac{1}{2} \right), \quad (2.8)$$

Here, $\hat{n}_{ks} = \hat{a}_{ks}^\dagger \hat{a}_{ks}$ is the number operator where $\hat{a}_{ks}$ is the annihilation and $\hat{a}_{ks}^\dagger$ is the creation operator. $\hat{a}_{ks}^\dagger$ is the hermitian conjugate to $\hat{a}_{ks}$. These two field operators also satisfy the following commutation relations: $[\hat{a}_{ks}, \hat{a}_{k's'}^\dagger] = \delta_{kk'} \delta_{ss'}$ and $[\hat{a}_{ks}, \hat{a}_{k's'}] = [\hat{a}_{ks}^\dagger, \hat{a}_{k's'}^\dagger] = 0$.

In the EM field quantization, we can associate every mode of the classical field with a quantum mechanical harmonic oscillator. So, by comparing Eqs. (2.8) and (2.7), we can easily map the classical picture to the quantum picture by using the following substitutions,

$$A_{k,s} = \sqrt{\frac{\hbar}{2\epsilon_0 V \omega_k}} \hat{a}_{k,s}, \quad (2.9a)$$

$$A_{k,s}^* = \sqrt{\frac{\hbar}{2\epsilon_0 V \omega_k}} \hat{a}_{k,s}^\dagger. \quad (2.9b)$$

The quantized vector potential ($\hat{A}(\vec{r}, t)$) can be expressed using Eqs. (2.9a) and (2.9b) in Eq. (2.5),

$$\hat{A}(\vec{r}, t) = \sum_{k,s} \sqrt{\frac{\hbar}{2\epsilon_0 V \omega_k}} \vec{\epsilon}_{ks} \hat{a}_{ks} e^{i(\vec{k} \cdot \vec{r} - \omega_k t)} + h.c.. \quad (2.10)$$

We can substitute the expression of the quantized vector potential (Eq. 2.10) in the Eq. (2.1a), to get the quantized electric field vector, which is written as,

$$\hat{\vec{E}}_k(\vec{r}, t) = \sum_{k,s} \sqrt{\frac{\hbar \omega_k}{2\epsilon_0 V}} \vec{\epsilon}_k \hat{a}_k e^{i(\vec{k} \cdot \vec{r} - \omega_k t)} + h.c.. \quad (2.11)$$

Here, $\vec{\epsilon}_k$ is the unit vector along the polarization direction. $\sqrt{\frac{\hbar \omega_k}{2\epsilon_0 V}}$ is the amplitude of the EM field, where V is the mode volume for the field quantization. We can also write the electric field vector in Equation (2.11) into two parts based on the positive and negative frequency contribution.

$$\hat{\vec{E}}_k(\vec{r}, t) = \hat{\vec{E}}_k^{(+)}(\vec{r}, t) + \hat{\vec{E}}_k^{(-)}(\vec{r}, t), \quad \text{where } \hat{\vec{E}}_k^{(-)}(\vec{r}, t) = \left[\hat{\vec{E}}_k^{(+)}(\vec{r}, t) \right]^\dagger. \quad (2.12)$$

By using Eqs. (2.12) and (2.11), the positive frequency part of the EM field vector can be written as [3]:

$$\hat{E}_k^{(+)}(\vec{r}, t) = \sum_k \sqrt{\frac{\hbar \omega_k}{2 \epsilon_0 (n(\omega_k))^2 V}} E(\vec{K}(\omega_k), \vec{r}) \hat{a}_k e^{-i \omega_k t}. \quad (2.13)$$

Here, the dispersion relation, $|\vec{K}(\omega_k)| = \frac{\omega_k n(\omega_k)}{c}$ is used to write Eq. (2.13) where $n(\omega_k)$ is the refractive index and $E(\vec{K}(\omega_k), \vec{r})$ is the spatial mode function. In case of the plane wave approximation, we can write $E(\vec{K}(\omega_k), \vec{r}) = e^{i \vec{K}(\omega_k) \cdot \vec{r}}$.

2.1.2 Photon number state

In quantum optics, photon number operator ($\hat{n}$) is defined as $\hat{n} = \hat{a}^\dagger \hat{a}$, where $\hat{a}$ is the annihilation operator and $\hat{a}^\dagger$ is the creation operator. The photon number state is written as $|n\rangle$ which is the eigenstate of the Hamiltonian operator with energy eigenvalue E_n .

$$\hat{H}|n\rangle = \hbar \omega (\hat{a}^\dagger \hat{a} + \frac{1}{2})|n\rangle = E_n|n\rangle \quad (2.14)$$

Number operator $\hat{n}$, when operated on the number state $|n\rangle$ gives the number of photons, i. e., $\hat{n}|n\rangle = n|n\rangle$. Using this expression in Eq. (2.14), we get the n^{th} energy eigenvalue

$$E_n = \hbar \omega (n + \frac{1}{2}) \quad (2.15)$$

The number of photons can be increased or decreased by using the creation and the annihilation operator, respectively. Annihilation operator ($\hat{a}$) operating on the photon number state once, destroy one quanta of light with energy $\hbar \omega$. In terms of energy eigenvalue, this can be reflected as,

$$\hat{H}(\hat{a}|n\rangle) = (E_n - \hbar \omega)(\hat{a}|n\rangle) \quad (2.16)$$

Similarly, the creation operator $\hat{a}^\dagger$ creates one quanta of light with energy $\hbar \omega$.

$$\hat{H}(\hat{a}^\dagger|n\rangle) = (E_n + \hbar \omega)(\hat{a}^\dagger|n\rangle) \quad (2.17)$$

Using the normalization constraint $\langle n|n' \rangle = \delta_{nn'}$ and the completeness relation $\sum_{n=0}^{\infty} |n\rangle\langle n| = 1$ along with the fact that $\hat{a}|0\rangle = 0$, we can write the operations of $\hat{a}$ and $\hat{a}^\dagger$, which respectively decrease and increase the photon number.

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle \quad (2.18)$$

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle \quad (2.19)$$

An interesting note here is the fact that the number states are not the eigenvectors for the annihilation or the creation operators. As an ideal single photon state consists of only one photon, in terms of number state it is expressed as $|n\rangle = |1\rangle$ with energy $\frac{3}{2}\hbar\omega$. A vacuum state which is $|n\rangle = |0\rangle$ has energy $\frac{1}{2}\hbar\omega$. This lowest energy eigenvalue is called the zero-point energy.

2.1.3 Photon number statistics

Photon number statistics represent the distribution of the number of photons in a photon pulse. We can plot the probability distribution $P(n)$ as a function of the photon number n . The photon number statistics are used to characterize the photon source; i. e, how close is the photon source to an ideal single-photon source? or what is the probability of the multi-photon generation?

All photon sources can be categorized into three groups based on the statistical distributions of photon number: Poissonian, super-Poissonian, and sub-Poissonian. The distinctions between the three distribution are based on the relationship between the average photon number ($\langle n \rangle$) and the variance (Δn^2) of the distribution. For the Poissonian distribution, the average photon number is the same as the variance. In the super-Poissonian distribution, the average photon number is less than the variance, whereas in the sub-Poissonian distribution average photon number is higher than the variance.

- Poissonian distribution: $\langle n \rangle = \Delta n^2$

- super-Poissonian distribution: $\langle n \rangle < \Delta n^2$
- sub-Poissonian distribution: $\langle n \rangle > \Delta n^2$

Along with the single-photon sources, there are two other types of sources that are equally important. These sources are the coherent source and the thermal source. A coherent state is represented as

$$|\psi_\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \quad (2.20)$$

So, the probability distribution for the coherent source is $P_n = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!} = e^{-\mu} \frac{\mu^n}{n!}$, which is a Poissonian distribution with average photon number $\langle n \rangle = \mu = |\alpha|^2$. The variance of this distribution is $\Delta n^2 = \mu$. The ratio of the two-photon probability to the single-photon probability is $P_2/P_1 = \mu/2$, which can be lowered to a small value, by lowering the average number of photons. This strategy is used to generate a near-ideal single-photon source which is called the weak-coherent pulse (WCP), where the average photon number is made very low ($\mu \approx 0.1$) by attenuating the coherent pulse to the desired level. At this value of μ , the ratio $P_2/P_1 = 0.05$. A thermal state is represented by the density operator,

$$\rho_{thermal} = \sum_{n=0}^{\infty} \frac{\mu^n}{(1+\mu)^{n+1}} |n\rangle \langle n| \quad (2.21)$$

Probability distribution of the thermal state is $P_n = \frac{\mu^n}{(1+\mu)^{n+1}}$, where the average photon number is $\langle n \rangle = \mu$ and the variance is $\Delta n^2 = \mu + \mu^2$. This distribution is super-Poissonian as $\langle n \rangle < \Delta n^2$. $P_2/P_1 = \frac{\mu}{(1+\mu)}$. For the same value of $\mu = 0.1$, a thermal state provides $P_2/P_1 = 0.09$, which is higher than the weak-coherent pulse. For an ideal single-photon Fock state $|\psi\rangle = |1\rangle$, $P_{n=1} = 1$ and $P_{n \neq 1} = 0$, which gives the average value of the photon number $\langle n \rangle = 1$ and variance $\Delta n^2 = 0$. This is a sub-Poissonian distribution as $\langle n \rangle > \Delta n^2$.

2.1.4 Second-order coherence and photon anti-bunching

Second-order coherence or g^2 measurement is one of the fundamental measurement of the quality of a single photon source. This is a measure of normalized intensity-intensity correlation. The second-order coherence between two electric field modes, where one field

mode i is measured at time t_i and the mode j is measured at time t_j , is mathematically written as,

$$g_{i,j}^2(t_i, t_j) = \frac{\langle \hat{E}_i^-(t_i) \hat{E}_j^-(t_j) \hat{E}_j^+(t_j) \hat{E}_i^+(t_i) \rangle}{\langle \hat{E}_i^-(t_i) \hat{E}_i^+(t_i) \rangle \langle \hat{E}_j^-(t_j) \hat{E}_j^+(t_j) \rangle} \quad (2.22)$$

$\hat{E}^+$ and $\hat{E}^-$ are the positive and the negative frequency part of the quantized electric field, which can be written in terms of the quantum mechanical annihilation ($\hat{a}$) and the creation ($\hat{a}^\dagger$) operators, as derived in Eq. (2.13).

$$g_{i,j}^2(t_i, t_j) = \frac{\langle \hat{a}_i^\dagger(t_i) \hat{a}_j^\dagger(t_j) \hat{a}_j(t_j) \hat{a}_i(t_i) \rangle}{\langle \hat{a}_i^\dagger(t_i) \hat{a}_i(t_i) \rangle \langle \hat{a}_j^\dagger(t_j) \hat{a}_j(t_j) \rangle} \quad (2.23)$$

In the case of a stationary source, its properties do not depend on the individual times t_i and t_j . So, the expression of the g^2 function can be simplified for the stationary case, where it is only the function of the time difference $\tau = t_j - t_i$.

$$g^2(\tau) = \frac{\langle \hat{a}^\dagger(t) \hat{a}^\dagger(t+\tau) \hat{a}(t+\tau) \hat{a}(t) \rangle}{\langle \hat{a}^\dagger(t) \hat{a}(t) \rangle \langle \hat{a}^\dagger(t+\tau) \hat{a}(t+\tau) \rangle} \quad (2.24)$$

It is not evident from the above expression how the g^2 value is related to the photon number distribution (P_n) of a single photon source. For that purpose, we focus on the value of the g^2 function when $\tau = 0$.

$$\begin{aligned} g^2(\tau = 0) &= \frac{\langle \hat{a}^\dagger(t) \hat{a}^\dagger(t) \hat{a}(t) \hat{a}(t) \rangle}{\langle \hat{a}^\dagger(t) \hat{a}(t) \rangle^2} = \frac{\langle \hat{n}(\hat{n} - 1) \rangle}{\langle \hat{n} \rangle^2} \\ &= \frac{2P_2 + 6P_3 + 12P_4 + \dots}{(P_1 + 2P_2 + 3P_3 + \dots)^2} \end{aligned} \quad (2.25)$$

To derive Eq. (2.25), the commutation relation $[\hat{a}, \hat{a}^\dagger] = 1$ and the equation for measuring the expectation value $\langle \hat{x} \rangle = \sum x P(x)$ has been used.

Eq. (2.25) can also be written as $g^2(\tau = 0) = 1 + \frac{\Delta n^2 - \mu}{\mu^2}$, where Δn^2 is the variance, $\langle n^2 \rangle - \langle n \rangle^2$ and μ is the average photon number $\langle n \rangle$. So, using the relation between $\langle n \rangle$ and Δn^2 for the three standard distributions of photon number statistics, we can correlate them with the $g^2(\tau = 0)$ values.

- Poissonian distribution: $g^2(\tau = 0) = 1$
- super-Poissonian distribution: $g^2(\tau = 0) > 1$
- sub-Poissonian distribution: $g^2(\tau = 0) < 1$

Coherent pulse which has a Poissonian distribution satisfies $g^2(\tau = 0) = 1$. For the thermal source $\Delta n^2 = \mu + \mu^2$, which gives the value $g^2(\tau = 0) = 2$. For the single photon source $\Delta n^2 = 0$ and $\mu = 1$, leading to the value $g^2(\tau = 0) = 0$. If $P_1 \gg P_2 \gg \sum_{n=3}^{\infty} P_n$, then Eq. (2.25) is written as $g^2(\tau = 0) \approx \frac{2P_2}{P_1^2}$. This expression correlates $g^2(\tau = 0)$ to the ratio of the two-photon probability vs single-photon probability; to some extent.

If we look at the temporal distribution of photons along the line of propagation, for different photon sources, we can observe three general categories. Photons can be distributed uniformly randomly, or in other words, the probability of a photon existing at any point in time is the same. This type of distribution is observed in continuous-wave lasers, where the second-order coherence $g^2(\tau = 0) = g^2(\tau \neq 0)$ or $g^2(\tau) = \text{constant}$. If the photons are likely to bunch together, or the probability of photons existing in close interval is larger than existing in further apart ($g^2(\tau = 0) > g^2(\tau \neq 0)$), then they follow **photon bunching** property. If the reverse condition is true, or the probability of photons existing in close interval is lower than existing in further apart ($g^2(\tau = 0) < g^2(\tau \neq 0)$), then they follow **photon anti-bunching** property. Ideal single-photon which can be expressed as number state $|\psi\rangle = |1\rangle$ shows the anti-bunching property, whereas typical thermal sources exhibit bunching nature. Fig. 2.1 shows a representative plot of the g^2 profile for the three scenarios mentioned above.

2.1.5 Measurement of $g^2(\tau)$: Hanbury Brown and Twiss (HBT) Interferometer

Measurement of the whole g^2 profile for a range of the τ value is an important step for characterizing a single photon source. Bunching or the anti-bunching property can be verified by comparing the $g^2(\tau = 0)$ and the $g^2(\tau \neq 0)$ values. On the other hand, photon number

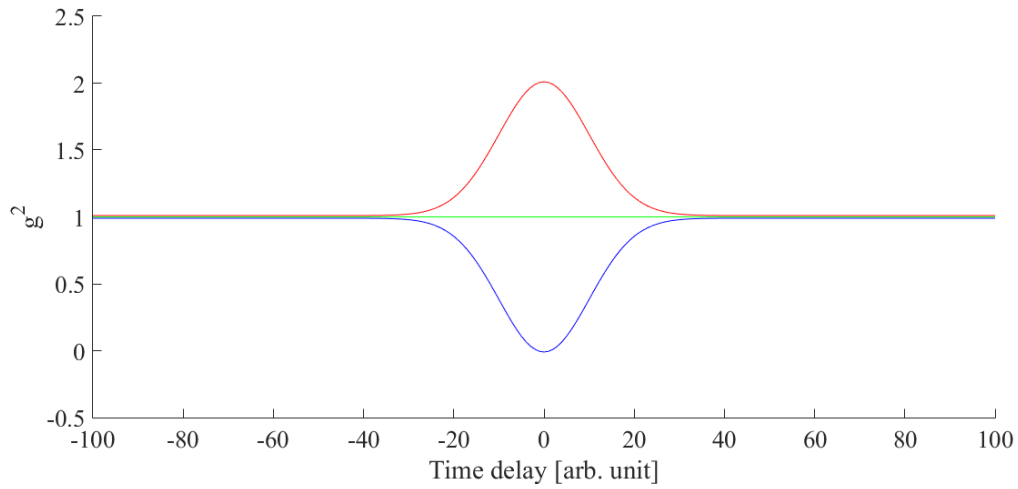


Fig. 2.1 Representation of a g^2 profile for three idealistic scenarios: 1) red line represents photon bunching; 2) blue line represents photon anti-bunching; 3) green line represents random distribution.

statistics can be realized by measuring the $g^2(\tau = 0)$ value only. Typically, a $g^2(\tau)$ profile is measured using a Hanbury Brown-Twiss (HBT) setup, which is described below.

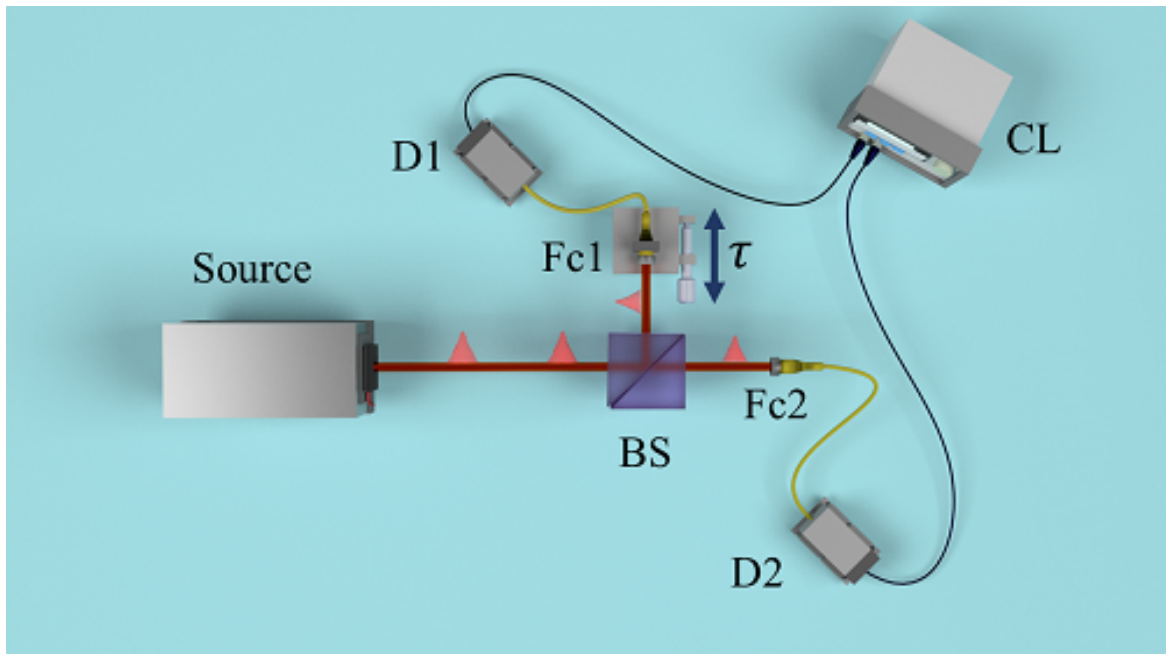


Fig. 2.2 Schematic of a Hanbury Brown and Twiss setup for measuring g^2 profile. **BS**: non-polarizing symmetric beamsplitter ($T : R = 50 : 50$); **Fc1**, **Fc2**: Fiber couplers; **D1**, **D2**: Single photon detectors; **CL**: Coincidence logic unit.

Fig. 2.2 represents an experimental setup to perform an HBT experiment. Here photon pulses from any light source are sent to a symmetric non-polarizing beamsplitter (BS). This beamsplitter has an equal probability of transmitting and reflecting each photon pulse. Two fiber couplers (Fc1, Fc2) are placed in each one of the two output arms of the BS to couple incoming photon pulses and send them towards the single photon detectors (D1, D2) connected with each fiber coupler. Fc1 and Fc2 have been positioned in such a way that the path differences from the BS are nearly zero, or in other words, delay (τ) between the photon arrival times from the BS to each coupler is approximately zero. We can also change the value of τ by fixing the position of Fc2 and moving the position of Fc1 by mounting the Fc1 coupler on top of a translational axis stage. For each position of Fc1 (each value of τ), the coincidence logic unit (CL) measures the total coincidence value by counting the number of events when both detectors record a click within some specified time interval (called coincidence window). These coincidence values when normalized with respect to the individual photon counts for each detector (called singles count) and plotted against their respective τ value, give the g^2 profile for the light source.

In the case of an ideal single photon source, each photon pulse contains only one photon, so each photon pulse only goes either to the transmitted arm or the reflected arm of the BS and hence produces no coincidence at $\tau = 0$. In the case of bunched photons, each photon pulse has a higher probability of having multiple photons. For example, if a photon pulse contains two photons, then one photon may transmit and the other one may reflect at the same time giving rise to coincidence at $\tau = 0$.

2.2 Single-photon source using SPDC process

The ideal single photon source, which generates single photon Fock state $|\psi\rangle = |1\rangle$ with 100% efficiency is a technological challenge. However, there exist various single photon sources that can be considered as a good alternative, and ongoing researches are aimed to increase their performances. These sources can be broadly categorized as either a probabilistic source or a deterministic source. In a probabilistic source, photon pairs are generated

randomly with time, where detection of one photon in a pair heralds the other single photon of the same pair. This type of sources uses spontaneous parametric down-conversion (SPDC) process [39, 41] or four-wave mixing (FWM) [33, 108] inside a non-linear medium. On the other hand, deterministic sources generate single photons “on-demand”. These sources include photon emission due to transitions in atoms or ions [70, 93], quantum dots [104, 57], diamond color centres [77, 42], etc.

We have used SPDC based single photon sources in all the experiments described in this thesis. SPDC is currently the most popular choice for a single photon source as it has several advantages. These advantages include a high pair generation rate, lower value of $g^2(\tau = 0)$, high fidelity of entanglement, and consume fewer resources compared to other conventional sources.

2.2.1 Pair generation rate in the SPDC process

Spontaneous parametric down-conversion (SPDC) is a non-linear process where a pump photon generated from a laser source interacts with the non-linear crystal and is converted into two photons (signal and idler photon) while maintaining at the same time, energy and momentum conservation; also called phase-matching. For an SPDC process, calculation of the pair generation rate under the relevant phase-matching condition is an important step. Here, we calculate the interaction between the three fields (pump, signal, and idler) inside the mode volume of the non-linear crystal. We have already derived the expression for a quantized electric field in Section 2.1.1, but we need to apply for the Gaussian profile of the three interacting field modes to get a more realistic value of the pair generation rate. All the calculations shown in this sub-section follow the similar work provided in the reference [14].

Gaussian beam approximation for the quantized EM field

In the expression of the quantized EM field (Eq. 2.13), the spatial mode function $E(\vec{K}(\omega_k), \vec{r})$ depends on the position vector $\vec{r}$. For plane wave approximation, we can write $E(\vec{K}(\omega_k), \vec{r}) = e^{i\vec{K}(\omega_k) \cdot \vec{r}}$. Here, we show the calculations for a more realistic scenario; for Gaussian beam shape. We consider here, the paraxial wave approximation [61] for the wave-propagation

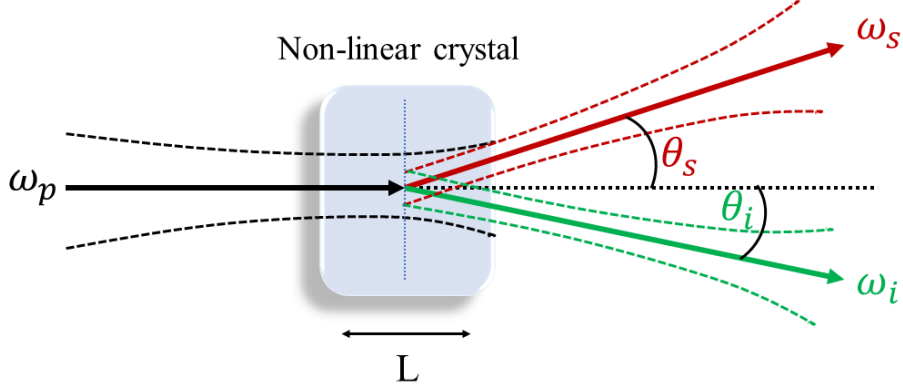


Fig. 2.3 Schematic of the SPDC process inside a non-linear crystal of length L . A pump photon (ω_p) converts to a signal (ω_s) and an idler photon (ω_i).

inside a nonlinear medium. We also consider that the beams have transverse intensity modulation which is Gaussian everywhere. Based on these assumptions as well as the scalar approximation, we can write the general solution of the spatial mode function as [20]:

$$E(K, r) = E_0 \frac{w_0}{w(z)} e^{-\frac{r^2}{w(z)^2}} e^{\frac{iKr^2}{2R(z)}} e^{i\Phi(z)} \quad (2.26)$$

where, $K = \frac{2\pi n\omega}{c}$ is the wave number, n is the refractive index of the medium of beam propagation, $r = \sqrt{x^2 + y^2 + z^2}$ represents the modulus of the position vector $\vec{r}$ in a three dimensional coordinate system. $w(z)$ is the beam diameter at a distance z from the beam waist; $w(z) = w_0 \left[1 + \left(\frac{\lambda z}{\pi n w_0^2} \right)^2 \right]^{\frac{1}{2}} = w_0 \left[1 + \left(\frac{z}{L_R} \right)^2 \right]^{\frac{1}{2}}$, where $\lambda = \frac{2\pi c}{n\omega}$ is the wavelength of the beam inside the medium, w_0 is the beam waist diameter (i.e. $w(z)$ at $z = 0$) and $L_R = \frac{\pi n w_0^2}{\lambda}$ denotes the Rayleigh length. $R(z) = z \left[1 + \left(\frac{\pi n w_0^2}{\lambda z} \right)^2 \right] = z \left[1 + \left(\frac{L_R}{z} \right)^2 \right]$ is the radius of curvature of the optical wavefront, and $\Phi(z) = -\arctan \left(\frac{\lambda z}{\pi n w_0^2} \right) = -\arctan \left(\frac{z}{L_R} \right)$

is the Gouy phase shift representing the spatial variation of the phase of the wave.

In the SPDC process, all the three EM fields (pump, signal and idler) interacts inside the non-linear crystal. Here, we show calculations for only a specific type of SPDC condition, called collinear configuration (please see Section 2.2.2 for details on various SPDC configurations). However, for all other types of SPDC process, similar calculations can be done. In the collinear configuration, all the three beams propagate along the z axis of the crystal, which has a length L in the z direction. In the x and y direction, the Gaussian beam diameters are much smaller than the width of the crystal. So, we can apply the following normalization condition, i.e. $\forall z$:

$$\iint_{-\infty}^{\infty} |E(K, r)|^2 dx dy = 1. \quad (2.27)$$

Using Eq. (2.26) in Eq. (2.27), we get

$$E_0 = \frac{\sqrt{2}}{\sqrt{\pi}w_0} e^{\frac{z^2}{w(z)^2}} \quad (2.28)$$

If we ignore the Gouy phase term while substituting Eq. (2.28) in Eq. (2.26), we can obtain the spatial mode function $E(\vec{K}(\omega_k), \vec{r})$ in its scalar form:

$$E(K, r) \equiv \frac{\sqrt{2}}{\sqrt{\pi}w(z)} e^{-\frac{x^2+y^2}{w(z)^2}} e^{\frac{iK(x^2+y^2+z^2)}{2R(z)}}. \quad (2.29)$$

Quantum Hamiltonian for the SPDC process

We consider the periodic boundary condition for the spatial mode function along the z axis. In the x and y axis, the value at the boundary is zero, as the beam diameter of the Gaussian beam is much smaller compared to the dimension of the crystal. So, the boundary conditions are the following:

$$E(\vec{K}(\omega_k), \vec{r}) \Big|_{z=-\frac{L}{2}} = E(\vec{K}(\omega_k), \vec{r}) \Big|_{z=\frac{L}{2}} \quad \text{for } z\text{-axis}, \quad (2.30a)$$

$$E\left(\vec{K}(\omega_k), \vec{r}\right)\Big|_{x=-\infty} = E\left(\vec{K}(\omega_k), \vec{r}\right)\Big|_{x=\infty} = 0 \quad \text{for x-axis,} \quad (2.30b)$$

$$E\left(\vec{K}(\omega_k), \vec{r}\right)\Big|_{y=-\infty} = E\left(\vec{K}(\omega_k), \vec{r}\right)\Big|_{y=\infty} = 0 \quad \text{for y-axis,} \quad (2.30c)$$

From these boundary conditions, we obtain $e^{\frac{-ikL}{2}} = e^{\frac{ikL}{2}}$ leading to the solution, $k = \frac{2m\pi}{L}$ for $m = 0, \pm 1, \pm 2, \dots$, where L is the length of the crystal along the z direction.

The total energy (E_n) for all the k modes is written as, $E_n = \sum_k \hbar \omega_k (n_k + \frac{1}{2})$, while the average energy per mode, for frequency ω is $\hbar \omega (n + \frac{1}{2})$. So, the total energy for all frequency modes is expressed as:

$$\int_{\omega} \frac{\delta E_n}{\delta \omega} d\omega = \int_{\omega} \frac{\delta E_n}{\delta m} \times \frac{\delta m}{\delta k} \times \frac{\delta k}{\delta \omega} d\omega = \int_{\omega} \frac{\hbar \omega (n + \frac{1}{2}) L}{2\pi c} d\omega. \quad (2.31)$$

In Eq. (2.31), we used the relations: $\frac{\delta E_n}{\delta m} = \hbar \omega (n + \frac{1}{2})$, $\frac{\delta m}{\delta k} = \frac{L}{2\pi}$ and $\frac{\delta k}{\delta \omega} = \frac{1}{c}$. We can rewrite the positive frequency part of the EM field vector in Eq. (2.13) using index of frequency (ω), instead of mode (k). We get the expression,

$$\hat{\vec{E}}_{\omega}^{(+)}(\vec{r}, t) = \int_{\omega} A_{\omega} E_{\omega}(\vec{r}) \hat{a}_{\omega} e^{-i\omega t} d\omega, \quad (2.32)$$

where A_{ω} is the amplitude factor for the transformation. To calculate the exact expression for A_{ω} , we first substitute Eq. (2.32) in Eq. (2.6) and then compare with Eq. (2.31). We also consider that each mode only contain a single photon, hence, we put $n = 1$ in Eq. (2.31). We obtain the form of the amplitude factor as,

$$A_{\omega} = \sqrt{\frac{\hbar \omega}{4\pi \epsilon_0 c}}. \quad (2.33)$$

Finally, using Eq. (2.33) in Eq. (2.32), we can write the positive frequency part of the electric field operator as,

$$\hat{\vec{E}}_{\omega}^{(+)}(\vec{r}, t) = \int_0^{\infty} \sqrt{\frac{\hbar \omega}{4\pi \epsilon_0 c}} E_{\omega}(\vec{r}) \hat{a}_{\omega} e^{-i\omega t} d\omega, \quad (2.34)$$

Here, $E_{\omega}(\vec{r})$ is the spatial mode function, which for the case of the Gaussian beam, can be written in the scalar form given in Eq. 2.29 [14].

In the SPDC process, a pump field (p) interacts with two other fields, signal (s) and idler (i), inside a non-linear crystal having second-order (χ^2) non-linearity. One photon of frequency ω_p in the pump field annihilate to create one signal photon of frequency ω_s and one idler photon of frequency ω_i , while maintaining the energy conservation, i. e. $\omega_p = \omega_s + \omega_i$. If we assume that all the fields are linearly polarized, and have Gaussian beam shape while propagating along the z axis of the non-linear crystal of length L , we can express the quantized electric field vectors for the pump (p), signal (s) and idler (i) photons, using Eq. (2.34), as the following:

$$\hat{E}_{\omega_p}^{(+)}(\vec{r}, t) = \int_0^\infty \sqrt{\frac{\hbar \omega_p}{4\pi\epsilon_0 c}} E_{\omega_p}(\vec{r}) \hat{a}_{\omega_p} e^{-i\omega_p t} d\omega_p \quad \text{for pump photon,} \quad (2.35a)$$

$$\hat{E}_{\omega_s}^{(-)}(\vec{r}, t) = \int_0^\infty \sqrt{\frac{\hbar \omega_s}{4\pi\epsilon_0 c}} E_{\omega_s}^*(\vec{r}) \hat{a}_{\omega_s}^\dagger e^{i\omega_s t} d\omega_s \quad \text{for signal photon,} \quad (2.35b)$$

$$\hat{E}_{\omega_i}^{(-)}(\vec{r}, t) = \int_0^\infty \sqrt{\frac{\hbar \omega_i}{4\pi\epsilon_0 c}} E_{\omega_i}^*(\vec{r}) \hat{a}_{\omega_i}^\dagger e^{i\omega_i t} d\omega_i \quad \text{for idler photon,} \quad (2.35c)$$

where ω_p , ω_s , and ω_i represents the frequency of the pump, signal, and idler photons. However, in our case, since we use a bright continuous-wave laser source for the pump beam, we replace Eq. 2.35a with its classical form [3],

$$\vec{E}_{\omega_p}^{(+)}(\vec{r}, t) \equiv A_p \int_0^\infty s(\omega) E_{\omega_p}(\vec{r}) e^{-i\omega_p t} d\omega_p, \quad (2.36)$$

Here, A_p is the amplitude of the pump field. $s(\omega) = \delta(\omega - \omega_p)$ represents the spectral amplitude of the monochromatic pump field, where $s(\omega)$ follows the normalization condition given by, $\int_\omega d\omega |s(\omega)|^2 = 1$.

Therefore, the quantum hamiltonian for the SPDC process is written as,

$$\hat{H}_I(\vec{r}, t) = \int_V \epsilon_0 \chi^{(2)}(\vec{r}) : \left(\hat{E}_{\omega_p}^{(+)}(\vec{r}, t) \hat{E}_{\omega_s}^{(-)}(\vec{r}, t) \hat{E}_{\omega_i}^{(-)}(\vec{r}, t) + h.c \right) dV, \quad (2.37)$$

where $\chi^{(2)}$ is the nonlinear susceptibility tensor and V represents the mode volume or the interaction volume of the three interacting fields inside the non-linear crystal.

Pair generation probability density & pair generation rate

In the interaction picture, we apply the unitary operator $U = \exp \left[-\frac{i}{\hbar} \int_{-\infty}^{\infty} dt \hat{H}_I(\vec{r}, t) \right]$ to the initial vacuum ($|0\rangle$) state of the signal and the idler photons $|\Psi\rangle_{t=0} = |0\rangle_s \otimes |0\rangle_i$ to see the effect of the SPDC process on the vacuum state. If we only consider up to the first order of the Taylor series expansion of the function $e^x = 1 + x + x^2/2! + x^3/3! + \dots$, then the output state at time t becomes,

$$|\Psi\rangle_t = |\Psi\rangle_{t=0} - \frac{i}{\hbar} \int_{-\infty}^{\infty} dt \hat{H}_I(\vec{r}, t) |\Psi\rangle_{t=0}. \quad (2.38)$$

The first term of Eq. (2.38) is the initial vacuum state whereas the second term includes the effect of the SPDC process. So, we will focus only on the second term which is written as $|\Psi_{SPDC}\rangle$, for the rest of this analysis. We now use Eqs. (2.35a), (2.35b), (2.35c) and (2.37) in Eq. (2.38) to write the output state $|\Psi_{SPDC}\rangle$ as,

$$|\Psi_{SPDC}\rangle = -i \iint_0^{\infty} \psi(\omega_s, \omega_i) \hat{a}_{\omega_s}^{\dagger} \hat{a}_{\omega_i}^{\dagger} |0\rangle_s |0\rangle_i d\omega_s d\omega_i, \quad (2.39)$$

where $\psi(\omega_s, \omega_i)$ is the joint spectral amplitude [3] of the SPDC process, and is expressed as [14],

$$\psi(\omega_s, \omega_i) = \sqrt{\frac{2\pi^2 \hbar N_p}{\epsilon_0 \lambda_p \lambda_s \lambda_i}} s(\omega_p) O(\omega_s, \omega_i). \quad (2.40)$$

In Eq. (2.40), N_p denotes the mean photon number of the pump beam, where $s(\omega_p) \sqrt{N_p}$ replaces the operator $\hat{a}_{\omega_p}$. The wavelength of the pump, signal and idler photons is given by $\lambda_h = \frac{2\pi c}{\omega_h}$, where $\omega_p = \omega_s + \omega_i$, for $h \in \{p, s, i\}$. Also, $O(\omega_s, \omega_i)$ represents the spatial

overlap of the pump, signal, and idler modes in the nonlinear medium. This SPDC amplitude contains all the spatio-temporal structure of the two-photon output state [3]. Conceptually, the joint spectral amplitude is a product of pump spectral amplitude $s(\omega_p)$ and phase-matching term which essentially is a sinc function. The intensity of the classical fields for the signal and idler photons is proportional to the square modulus of this phase-matching function [3].

The square modulus of the joint spectral amplitude (or in other words the joint spectral density) of the SPDC process, i.e. $|\psi(\omega_s, \omega_i)|^2$, gives the pair generation probability density. More particularly, given the pump power, it provides the expected number of photon pairs produced per unit time per signal (or idler) bandwidth. Moreover, we know that $\omega_p = \omega_s + \omega_i$ and ω_p can be considered to be coherent state from the laser source. Therefore, if we now numerically integrate $\psi(\omega_s, \omega_i)$ (given by Eq. 2.40) over a certain bandwidth i.e. a range of signal (or idler) frequencies, then we would obtain a sinc^2 nature trace for this pair generation probability density plotted over a spectrum of signal frequencies.

The maximum of this probability distribution provides the corresponding wavelength information at which SPDC pair generation rate would be maximal. The maximum value of pair generation probability obtained numerically can be directly verified with the experimental data. Consequently, the pair generation rate can be defined as [14, 102, 3],

$$R \propto \langle \psi | \psi \rangle = \int_0^\infty d\omega_s \int_0^\infty d\omega_i |\psi(\omega_s, \omega_i)|^2. \quad (2.41)$$

The pair production rate R is proportional to the Boyd-Kleinman factor [14, 3]. In the case of a weakly focused Gaussian pump beam, the Boyd-Kleinman factor is proportional to the length L of the nonlinear crystal [3]. However, it is important to note that this relationship of R and L is not true for the case of strongly focused Gaussian pump beam; and also that there exists a trade-off between heralding ratio and tightness of focus [3].

2.2.2 Birefringent Phase matching in bulk crystals

In a birefringent bulk crystal, the spontaneous parametric down-conversion process occurs if the two conditions are satisfied, which are called the phase-matching condition. The first

condition is due to the energy conservation inside the crystal.

$$\omega_p = \omega_s + \omega_i \quad (2.42)$$

The second condition comes from the momentum conservation.

$$\vec{K}_p = \vec{K}_s + \vec{K}_i \quad (2.43)$$

The momentum vector $\vec{K}_h = K_h \hat{e}_h$ is expressed as $K_h = 2\pi n_h / \lambda_h$, where $h \in \{p, s, i\}$. n_p , n_s , and n_i denote the non-linear refractive indices. λ_p , λ_s , and λ_i represent the wavelengths of the pump, signal and idler photon, and $\hat{e}_h$ is the unit vector along the direction of the momentum vector. Each of these non-linear refractive indices can be compactly stated as functions of temperature T , polarization direction $\hat{s}$, and respective wavelength λ_h , i.e., $n_h = f(T, \hat{s}, \lambda_h)$.

Birefringent phase matching can be achieved by using two strategies; by tuning the angle between the crystal axes and the interacting fields, or by tuning the temperature of the crystal. The first process is called critical phase matching whereas the second process is called non-critical phase matching. In this thesis work, we have used critical birefringent phase matching in BBO (beta barium borate) crystals, which is a negative uni-axial non-linear crystal. The plane containing the optical axis of the crystal and the pump wave vector is called the principal plane. we denote the polarization direction orthogonal to the principal plane as the ordinary (o) axis and polarization direction within that plane as the extraordinary (e) axis. There are two types of phase-matching conditions satisfied in a bulk crystal; type I and type II phase matching. For a negative uniaxial crystal, type I phase matching occurs when the pump beam polarization is extraordinary and both the signal and idler beams are ordinary. In the case of type II phase matching, the input pump beam and the signal beam is extraordinary whereas the idler beam is ordinary.

- Type I: $e \rightarrow o + o$
- Type II: $e \rightarrow e + o$

Phase matching conditions are also categorized as either degenerate or non-degenerate, based on the frequency of the signal and idler photons. In the degenerate case, both the signal and idler photons have the same frequency $\omega_s = \omega_i = \omega_p/2$, whereas, in the non-degenerate case, signal and idler frequencies are different. If both the signal and idler photons transmit through the same path ($\hat{e}_s = \hat{e}_i$) then the condition is called collinear phase matching. In the case of non-collinear phase matching, transmission directions are different.

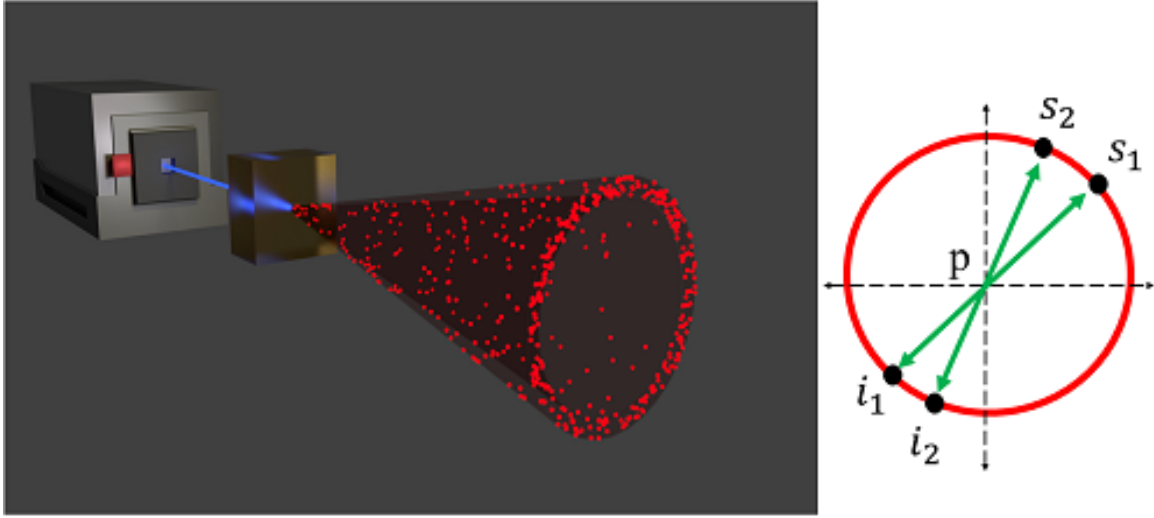


Fig. 2.4 Schematic of the type I SPDC process inside a non-linear crystal. s_k denotes the position of the signal photon on the SPDC ring whereas i_k denotes the position of the idler photon of the same pair.

In a type I SPDC process (Fig. 2.4), photon pairs are generated and transmitted in a cone form. If we look at a cross-section of the SPDC cone, which is a ring, we can see that signal and idler photons are always generated in a diagonal position of the ring. For example, if the signal photon is present at the position s_1 of the SPDC ring then the idler photon must be at i_1 which is diagonally opposite. Similarly for the s_2 and i_2 positions. For the case of type II process (Fig. 2.5), photon pairs are generated in two separate cones rather than one. If the signal photon is created in the position s_1 of the upper ring, then the idler must be in the i_1 position of the lower ring which is diagonally opposite and crossing the position of the pump

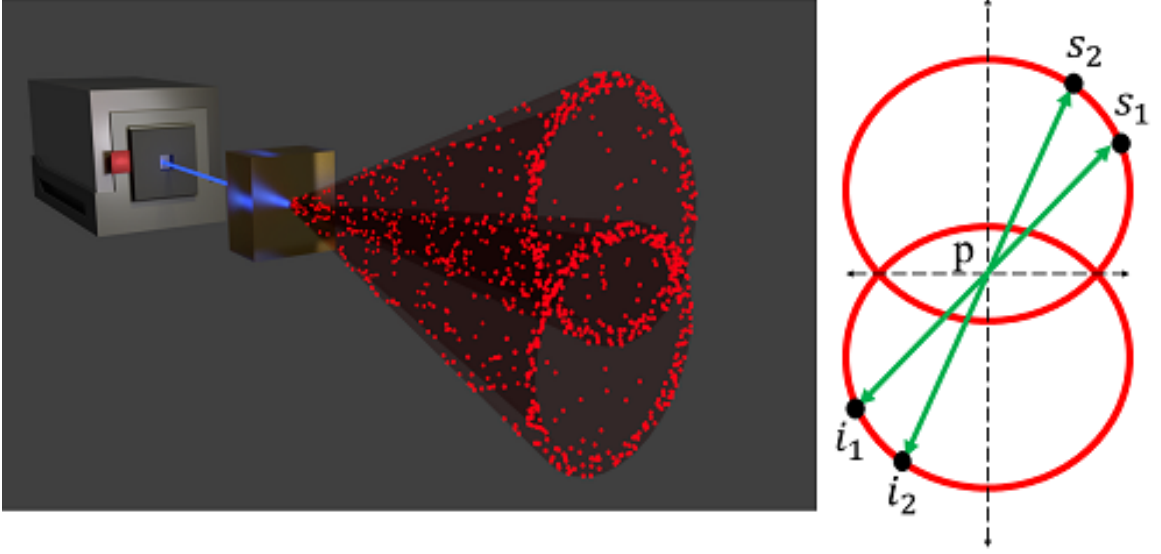


Fig. 2.5 Schematic of the type II SPDC process inside a non-linear crystal. s_k denotes the position of the signal photon on the SPDC ring whereas i_k denotes the position of the idler photon of the same pair.

photon (p).

In order to find solution to the phase matching condition, we first select the frequencies of the pump, signal and idler beam that satisfy the energy conservation (Eq. 2.42), the type of the phase matching (type I or II) and linearity of transmission (collinear or non-collinear). Based on the selection we solve the equation (2.43) numerically, by putting appropriate unit vectors $\hat{e}_p, \hat{e}_s, \hat{e}_i$. Here we input free-parameters $\theta_p, \phi_p, \theta_s, \phi_s, \theta_i, \phi_i$ where θ and ϕ are the polar and the azimuth angles, respectively. We also solve Sellmeier equations to find refractive indices $n_h = f(T, \hat{s}, \lambda_h)$ for given value of temperature, wavelength, and polarization direction.

2.2.3 Quasi-Phase matching in periodically-poled crystals

In non-linear optics, quasi-phase matching achieves efficient energy transfer from the pump frequency to the signal and idler frequencies. It is realized by spatially modulating the non-linear properties in a periodic structure, along the direction of propagation. The spatial

modulation of the non-linearity parameter (χ) is performed by altering the crystal orientation periodically. So the non-linearity parameter changes from $+\chi$ to $-\chi$ from one domain to the next domain. The length of the domain represents the poling period of the periodically poled crystal.

Phase matching condition is typically achieved by controlling the temperature of the periodically poled crystal, which has the advantage of increasing the range of tuning for the signal and idler wavelengths. Also, spatial walk-off in the transverse direction can be eliminated by making the phase matching in the collinear configuration, which in turn increases the conversion efficiency as the interaction length is larger in this case.

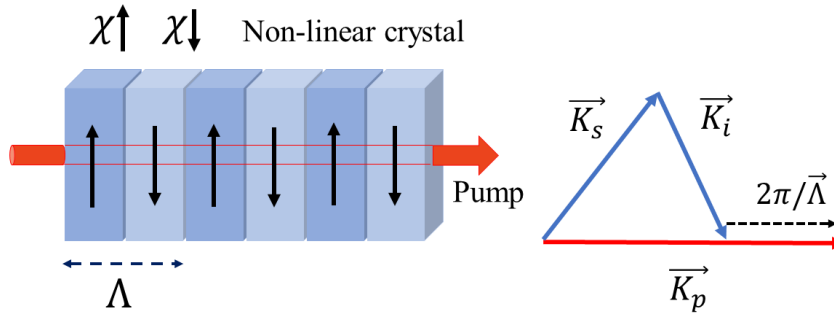


Fig. 2.6 Quasi-phase matching inside a periodically poled non-linear crystal of poling period Λ . The non-linearity parameter (χ) has alternate orientation from one domain to the next.

Considering the law of conservation of momentum and collinear parametric interaction for a SPDC process, the quasi phase matching condition [20] for a periodically poled crystal can be described with the relations:

$$\vec{K}_p = \vec{K}_s + \vec{K}_i + \frac{2\pi}{\Lambda(T)} \quad (2.44)$$

Here, K_p , K_s and K_i represents the magnitude of the momentum vectors for the pump (p), signal (s) and idler (i) photons respectively. Also, $\Lambda(T)$ denotes the poling period of the

crystal which is dependent on temperature T . Note that the quasi-phase matching condition described in Eq. (2.44) can be derived by solving the set of coupled differential equations for the electric field amplitude of the pump, signal, and idler as shown in [3].

In this thesis work, we have used periodically poled KTP (potassium titanyl phosphate) crystal or PPKTP in short, to achieve quasi-phase matching in a collinear configuration. So, here we show the analysis for the SPDC process inside a PPKTP crystal. First, we substitute the conditions of colinearity in Eq. (2.44), and also write the magnitude of the momentum vector as $K_h = \frac{2\pi n_h}{\lambda_h}$, where $h \in \{p, s, i\}$. We get Eq. (2.45) from Eq. (2.44).

$$\frac{2\pi n_p}{\lambda_p} = \frac{2\pi n_s}{\lambda_s} + \frac{2\pi n_i}{\lambda_i} + \frac{2\pi}{\Lambda(T)} \quad (2.45)$$

where, n_p , n_s and n_i denote the nonlinear refractive indices and λ_p , λ_s and λ_i represent the wavelengths of the pump, signal and idler photons respectively. Now, each of these nonlinear refractive indices can be compactly stated as functions of temperature T , polarization direction $\hat{s}$ and respective wavelength λ_h i.e. $n_h = f(T, \hat{s}, \lambda_h)$ where $h \in \{p, s, i\}$. Also, the thermal expansion of the poling period can be written as [35],

$$\Lambda(T) = \Lambda_0 \left\{ 1 + \alpha (T - T_0) + \beta (T - T_0)^2 \right\} \quad (2.46)$$

where $T_0 = 25^\circ\text{C}$ is the room temperature and Λ_0 is the poling period of the crystal at room temperature. For a KTP crystal, $\alpha = (6.7 \pm 0.7) \times 10^{-6} [^\circ\text{C}]^{-1}$ and $\beta = (11 \pm 2) \times 10^{-9} [^\circ\text{C}]^{-1}$ [35]. Additionally, a thermal expansion of the refractive indices gives [35, 117],

$$\begin{aligned} n(\lambda, T) &= n(\lambda, T = T_0) + \left. \frac{\partial n}{\partial T} \right|_{(\lambda, T=T_0)} (T - T_0) + \left. \frac{\partial^2 n}{\partial T^2} \right|_{(\lambda, T=T_0)} (T - T_0)^2 \\ &= n(\lambda, T = T_0) + n_1(\lambda)(T - T_0) + n_2(\lambda)(T - T_0)^2 \end{aligned} \quad (2.47)$$

Here we put $n_1(\lambda) = \left. \frac{\partial n}{\partial T} \right|_{(\lambda, T=T_0)}$ and $n_2(\lambda) = \left. \frac{\partial^2 n}{\partial T^2} \right|_{(\lambda, T=T_0)}$ for simplicity. $n_{1,2}(\lambda)$ is also defined as $n_{1,2}(\lambda) = \sum_{m=0}^3 \frac{a_m}{\lambda^m}$. The second and the third term in Eq. (2.47) can be obtained from the empirical results in [35, 117] and has been provided in Table 2.1. While, the value

a_m	$n_1(Z)$	$n_2(Z)$	$n_1(Y)$	$n_2(Y)$
a_0	9.9587×10^{-6}	-1.1882×10^{-8}	6.2897×10^{-6}	-0.14445×10^{-8}
a_1	9.9228×10^{-6}	10.459×10^{-8}	6.3061×10^{-6}	2.2244×10^{-8}
a_2	-8.9603×10^{-6}	-9.8136×10^{-8}	-6.0629×10^{-6}	-3.5770×10^{-8}
a_3	4.1010×10^{-6}	3.1481×10^{-8}	2.6486×10^{-6}	1.3470×10^{-8}

Table 2.1 Empirical values of a_m for different polarization direction and order of derivatives (Ref. [35]).

of the first term, can be obtained by solving either of the following Sellmeier equations for a PPKTP crystal [65, 16, 43]:

$$\text{one-pole: } n^2(\lambda, T = T_0) = A + \frac{B}{1 - C\lambda^{-2}} - D\lambda^2, \text{ or} \quad (2.48)$$

$$\text{two-pole: } n_z^2(\lambda, T = T_0) = A + \frac{B}{1 - C\lambda^{-2}} - \frac{D}{1 - E\lambda^{-2}} - F\lambda^2. \quad (2.49)$$

For the one-pole equation (Eq. 2.48) one may use a representative values of A to D provided in Table 2.2 (see Ref. [38, 65, 16]).

	A	B	C	D
n_x	2.16747	0.83733	0.04611	0.01713
n_y	2.19229	0.83547	0.04970	0.01621
n_z	2.25411	1.06543	0.05486	0.02140

Table 2.2 Empirical value of A, B, C, D in the one-pole Sellmeier equation (Ref. [38]).

The value of the constants A to F in the two-pole equation (Eq. 2.49) can be obtained from empirical results in [43], where $A=2.12725$, $B=1.18431$, $C=0.0514852$, $D=0.6603$, $E=100.00507$, $F=0.00968956$. Here, it is important to note that the two-pole Sellmeier equation provides better accuracy in the obtained result for the first term than the one pole version.

Now we consider a special scenario where the pump wavelength (λ_p) is fixed at 405 nm and the poling period at room temperature (Λ_0) is 10 μm . We also consider the collinear

SPDC process, hence we solve Eq. 2.45 using Eqs. (2.46-2.49). We estimate the value of phase-matching temperature (T) for different values of signal wavelength (λ_s), as shown in Table 2.3.

Signal wavelength (nm)	Phase-matching temperature ($^{\circ}\text{C}$)
806	25
807	29.1
808	34.3
809	39.4
810	44.4
811	49.4
812	54.2
813	59
814	63.7
815	68.3

Table 2.3 List of phase-matching temperature estimated for various signal wavelengths. The pump wavelength is fixed at 405 nm, while the SPDC process is maintained for collinear configuration.

2.3 Single-photon detection

In a single-photon detector, a single photon impinging on the sensor of the detector creates an output electrical pulses of a specific shape. By counting these electrical pulse one can count the number of photons detected in a given time. Measuring the arrival time of the electric pulse, one can record the time-stamps of each individual arriving photons with high precision. In addition to that, a photon number resolving detector can detect the number of photons present in each pulse.

There are various types of single photon detectors currently available in the market. These include photo-multiplier tubes, semiconductor-based detectors, superconducting nanowire, Transition-edge sensor (TES), etc. In all the experiments mentioned in this thesis, we have only used semiconductor-based detectors called silicon SPAD (single photon avalanche detector). The reason for the choice of silicon SPADs is that they have comparatively higher quantum efficiency (60-80%) in the range of the frequency (810 nm) that we work on. Also,

these detectors have low space and maintenance requirements as they do not require a cryogenic cooling system.

2.3.1 Silicon SPAD: working principle and properties

In a silicon SPAD detector, a p-n junction is reversed biased and the bias voltage to the diode is kept above the breakdown voltage of the diode. It generates a very high electric field across the p-n junction depletion layer. When a single photon hits the diode and creates an electron-hole pair, this single charge carrier experiences the high electric field and gets accelerated with high kinetic energy, creating even more electron-hole pairs due to impact ionization. These secondary charge carriers also create more electron-hole pairs via impact ionization, and then they create even more, and hence an avalanche process starts. In this way, within a very short period of time a huge number of charge-carriers are created from the impact of even a single photon; leading to the generation of a macroscopic avalanche current. An electrical circuit converts this current to a detectable electronic voltage pulse with a definite shape. Once the avalanche process kicks in, the detector remains in the ON state until it is quenched by an external quenching circuit which reduces the bias voltage below the breakdown voltage (OFF state). At this stage, the detector becomes ready for another avalanche process to start.

In general, there are few characterizing properties associated with a silicon SPAD (or a single-photon detector in general) that represent the performance of the detector. These properties are detection efficiency, timing resolution or timing jitter, deadtime, dark count, afterpulsing probability, etc.

Efficiency: The detector efficiency is the measure of the probability of registering an electrical pulse, given that a photon is incident on the active area of the detector sensor. An ideal single-photon detector should be 100% efficient. In reality, typical efficiency is much lower than that.

Timing jitter: In a SPAD detector, a photon generates primary charge pair which undergoes the avalanche process and creates a voltage pulse. So, the arrival time of the photon and the creation time of the avalanche voltage pulse is correlated. This correlation can be ascribed to a fixed time delay between the two events, however, due to different physical effects, this time delay has a statistical fluctuation which is called the timing jitter. It is typically measured as the full-width at half maximum (FWHM) of the time distribution of photon arrival.

Dead time: After each detection is registered, the detector becomes incapable of registering the next detection for some time interval. This time interval where the detection efficiency becomes zero is called the dead time of the detector. In a SPAD detector, after an avalanche pulse is generated, the bias voltage is reduced below the breakdown voltage, such that the avalanche process is quenched and the detector becomes ready for the next avalanche to happen. However, in this short interval, even if a photon hits the detector sensor, it won't be able to create an avalanche and hence remains undetected.

Dark count: In a single photon detector, not only an impinging photon but also some thermally generated carriers can start the avalanche process which leads to some unwanted detection counts. In semiconductor-based detectors, these thermal carriers occur through local energy levels within the bandgap. So, even if the detector is operated in a dark condition (no photons impinging on the detector sensor) there always will be some counts. These are called dark counts and it increases with the temperature of the detector. For this reason, all SPAD detectors come with some internal cooling mechanism.

Afterpulsing: During each avalanche process, some charge carriers may be trapped inside intermediate carrier traps, which have some probability of getting released after some time and trigger another avalanche process alongside the primary one. This is called afterpulsing which creates false counts in the detector.

2.3.2 Coincidence detection using silicon SPAD

In a SPAD detector, when a single photon hits the detector sensor, the avalanche process kicks in and within a very short period of time, a voltage pulse is generated from the detector. So, the arrival time of the photon hitting the detector and the creation of the voltage pulse are correlated. Hence, by recording the creation time of the consecutive voltage pulses we can time stamp all the arriving photons to the detector, sequentially. A time tagging module performs the operation of time tagging individual voltage pulse. Generally, the output pulse shape from any available silicon SPAD detector is either TTL (transistor-transistor logic) or NIM (nuclear instrumentation module). A time tagger tags the time for an individual pulse on either the rising edge or the falling edge of the pulse. More sophisticated tagging strategies are being used nowadays, in order to cancel noise coming from various electrical components.

In most of the experiments, where multiple SPADs are operating simultaneously, cross-correlation or coincidence measurement among multiple detectors becomes an important requirement. For this purpose, we compare the recorded time-stamps from any two detectors. These time-stamps are lists of photon arrival times (typically in picosecond scale). If any two time stamps from two lists are within a predefined range (called time window) they are called coincident photons. If we plot a histogram where the x-axis is the time difference between the two time stamping lists, and the y-axis is the number of events with the corresponding time difference, we can observe a coincidence peak with a standard deviation correlated to the coherence time of the photon as well as the resolution of the detector. For example, in an SPDC process photon pairs are generated at the same time (time-correlated), so if we send the two photons of any pair to two separate detectors and plot coincidence between the two time stamping lists, we get a coincidence peak centered around zero time delay. All uncorrelated photons form a steady background in the coincidence plot. We consider the peak region as the signal and the constant background as the noise level. An example of an algorithm used for generating the coincidence plot has been discussed in details in Appendix A.

2.4 Single-photon interferometry

In an optical interferometer, multiple electromagnetic waves are superimposed to create interference patterns. In general, in an interferometer, firstly the input beam is split into multiple beams using some beamsplitting device. These beams are combined again using a beam combiner. In between the splitting and the combination, a subset of the beams undergoes some changes due to external effects, i. e, phase shift, temporal shift, etc. The combined beam shows an interference pattern which is used to extract information about these external effects.

Optical interferometers are used in various applications including measurement of wavelength and linewidth of laser, measurement of changes in refractive index, measurement of relative path delay, etc. Here we discuss two important interferometers that have been used extensively in the experimental works discussed in this thesis. They are the Mach-Zehnder interferometer and the Sagnac interferometer.

2.4.1 Mach-Zehnder interferometer

A Mach-Zehnder interferometer (MZI) can be constructed with two non-polarizing beam-splitters. A basic schematic of a MZI is shown in Fig. 2.7. Single photons are generated from a single photon source and sent to one of the input arms (marked as 1 in Fig. 2.7) of a beamsplitter (BS1) whose transmission and reflection probabilities are T_1 and R_1 while $T_1 + R_1 = 1$. The two output arms of BS1 (arm 2 and 3) become the two input arms of the second beamsplitter (BS2), whose transmission and reflection probabilities are T_2 and R_2 while $T_2 + R_2 = 1$. The two output arms of BS2 are marked as 4 and 5, and house fiber couplers connected to single photon detectors (SPAD1 and SPAD2). Single photons, after passing through BS1, travel in a superposition state between arm 2 and 3. One of the arms (here arm 3) goes under some changes (here phase modulation; PM) before the two arms recombine at BS2, creating interference patterns in the output arms 4 and 5.

The input state to BS1 is $|1\rangle_1|0\rangle_0$ which means one single photon state in arm 1 and vacuum state in arm 0. It can be written with quantum mechanical creation operator as

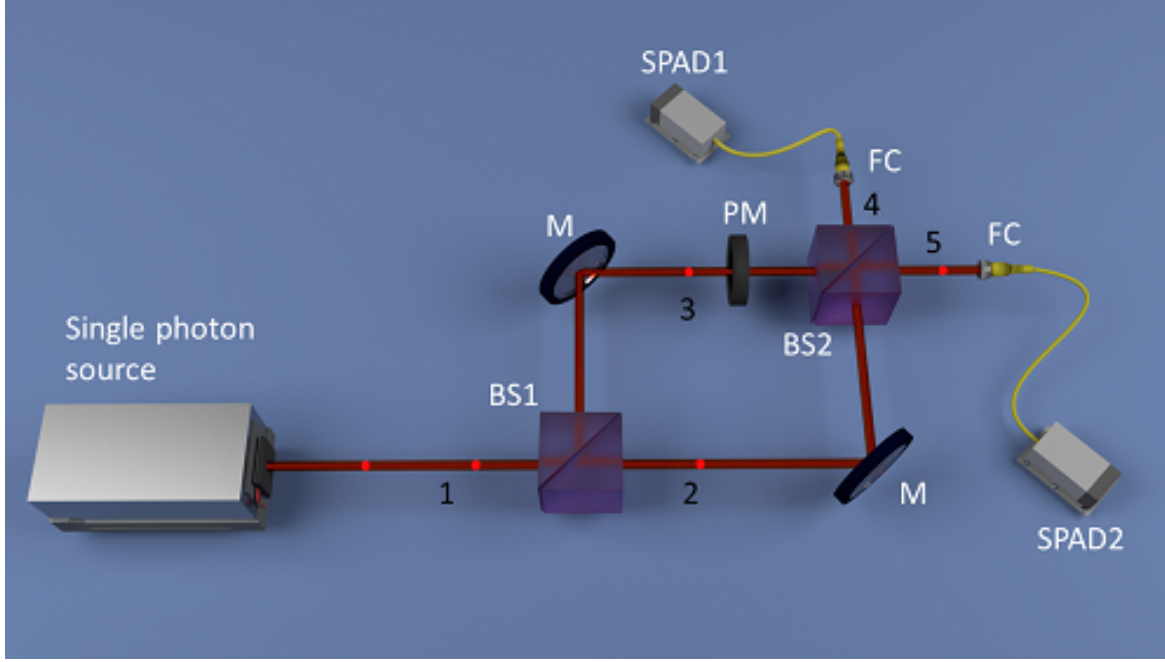


Fig. 2.7 Schematic of a Mach-Zehnder interferometer. **BS1, BS2**: non-polarizing beamsplitter; **M**: Mirror; **PM**: phase modulator; **SPAD1, SPAD2**: single photon avalanche detectors.

$\hat{a}_1^\dagger|0\rangle_1|0\rangle_0$. Using beamsplitter operation on the creation operators, and phase change of ϕ for arm 3, we write the output state of the MZI as,

$$\begin{aligned}
 |1\rangle_1|0\rangle_0 &= \hat{a}_1^\dagger|0\rangle_1|0\rangle_0 \\
 &\rightarrow (\sqrt{T_1}\hat{a}_2^\dagger + i\sqrt{R_1}\hat{a}_3^\dagger e^{i\phi})|0\rangle_2|0\rangle_3 \\
 &\rightarrow \{\sqrt{T_1}(\sqrt{T_2}\hat{a}_4^\dagger + i\sqrt{R_2}\hat{a}_5^\dagger) + i\sqrt{R_1}(\sqrt{T_2}\hat{a}_5^\dagger + i\sqrt{R_2}\hat{a}_4^\dagger)e^{i\phi}\}|0\rangle_4|0\rangle_5 \\
 &= (\sqrt{T_1T_2}\hat{a}_4^\dagger - \sqrt{R_1R_2}\hat{a}_4^\dagger e^{i\phi})|0\rangle_4|0\rangle_5 + (i\sqrt{T_1R_2}\hat{a}_5^\dagger + i\sqrt{R_1T_2}\hat{a}_5^\dagger e^{i\phi})|0\rangle_4|0\rangle_5 \\
 &= (\sqrt{T_1T_2} - \sqrt{R_1R_2}e^{i\phi})|1\rangle_4|0\rangle_5 + (i\sqrt{T_1R_2} + i\sqrt{R_1T_2}e^{i\phi})|0\rangle_4|1\rangle_5 \\
 &= C_4|1\rangle_4|0\rangle_5 + C_5|0\rangle_4|1\rangle_5
 \end{aligned} \tag{2.50}$$

Probability of detecting a single photon in arm 4 and 5 are P_4 and P_5 , respectively.

$$P_4 = |C_4|^2 = T_1T_2 + R_1R_2 - 2\sqrt{T_1T_2R_1R_2}\cos\phi \tag{2.51}$$

$$P_5 = |C_5|^2 = T_1R_2 + R_1T_2 + 2\sqrt{T_1T_2R_1R_2}\cos\phi \tag{2.52}$$

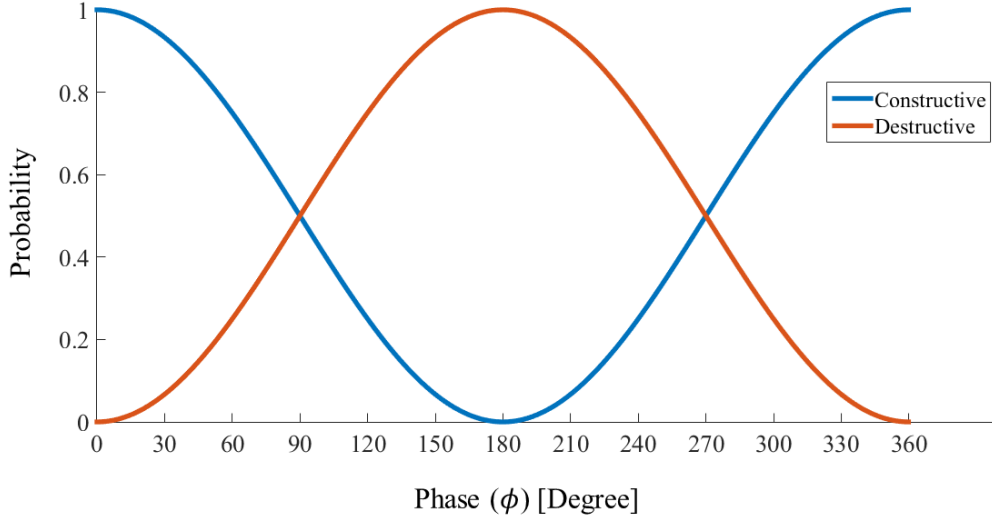


Fig. 2.8 Plot of P_4 (red line) and P_5 (blue line) with respect to the phase angle (ϕ). Here we assume that both beamsplitters (BS1 and BS2) are symmetric; $T_1 = T_2 = 0.5$. For $\phi = 0^\circ$ value, the blue line shows constructive interference while the red line shows destructive interference, which are reversed when $\phi = 180^\circ$.

Here P_4 and P_5 shows sinusoidal oscillations with respect to relative phase ϕ between the two arms. If one output arm shows constructive interference, the other one shows destructive interference and vice versa. Instead of phase modulation, the time delay between the two arms also can be used for creating interference-effect. In that case, we have to write the beam-splitting operations on quantized electric fields. Time delay τ has been introduced in arm 3.

$$E_3^\pm(t) = \sqrt{T_1}E_0^\pm(t) \pm i\sqrt{R_1}E_1^\pm(t) \quad (2.53)$$

$$E_2^\pm(t) = \sqrt{T_1}E_1^\pm(t) \pm i\sqrt{R_1}E_0^\pm(t) \quad (2.54)$$

$$E_4^\pm(t) = \sqrt{T_2}E_2^\pm(t) \pm i\sqrt{R_2}E_3^\pm(t - \tau) \quad (2.55)$$

$$E_5^\pm(t) = \sqrt{T_2}E_3^\pm(t - \tau) \pm i\sqrt{R_2}E_2^\pm(t) \quad (2.56)$$

Intensity at output arm 4 can be expressed as the integration on the field-field correlation value $\langle E_4^-(t)E_4^+(t) \rangle$. Using Eqs. (2.53), (2.54), (2.55) and (2.56),

$$\begin{aligned}\langle E_4^-(t)E_4^+(t) \rangle &= \langle \{ \sqrt{T_2}E_2^-(t) - i\sqrt{R_2}E_3^-(t-\tau) \} \{ \sqrt{T_2}E_2^+(t) + i\sqrt{R_2}E_3^+(t-\tau) \} \rangle \\ &= \langle T_2E_2^-(t)E_2^+(t) + i\sqrt{T_2R_2}E_2^-(t)E_3^+(t-\tau) - i\sqrt{T_2R_2}E_3^-(t-\tau)E_2^+(t) \\ &\quad + R_2E_3^-(t-\tau)E_3^+(t-\tau) \rangle\end{aligned}\tag{2.57}$$

The first term of Eq. (2.57) is written as,

$$\begin{aligned}\langle E_2^-(t)E_2^+(t) \rangle &= \langle \{ \sqrt{T_1}E_1^-(t) - i\sqrt{R_1}E_0^-(t) \} \{ \sqrt{T_1}E_1^+(t) + i\sqrt{R_1}E_0^+(t) \} \rangle \\ &= \langle T_1E_1^-(t)E_1^+(t) + i\sqrt{T_1R_1}E_1^-(t)E_0^+(t) - i\sqrt{T_1R_1}E_0^-(t)E_1^+(t) + R_1E_0^-(t)E_0^+(t) \rangle\end{aligned}\tag{2.58}$$

Electric field operators can be written in terms of quantum mechanical creation and annihilation operators.

$$E^\pm(r,t) = \pm i\kappa \hat{a} e^{\pm i(kr - \omega t)}\tag{2.59}$$

where $\kappa = \sqrt{\frac{\hbar\omega}{2\varepsilon_0 V}}$, $\hat{a}$ and $\hat{a}^\dagger$ are the quantum mechanical annihilation and creation operators. k is the wave number and ω is the angular frequency. ε_0 is the permittivity in free space, and V is the volume of the mode field. Input state to the BS1 is $|\Psi\rangle$.

$$|\Psi\rangle = \int_{-\infty}^{\infty} f(\omega) |\omega\rangle_1 |0\rangle_0 d\omega\tag{2.60}$$

$f(\omega)$ is the spectral amplitude of the single photon, so $|f(\omega)|^2$ represents the probability of the input single photon generating with the frequency ω . Using Eqs. (2.59) and (2.60), the

first term of Eq. (2.58) becomes,

$$\begin{aligned}
 \langle \Psi | E_1^-(t) E_1^+(t) | \Psi \rangle &= \kappa^2 \int d\omega \int d\omega' \langle \omega |_1 \langle 0 |_0 \hat{a}_1^\dagger \hat{a}_1 | \omega' \rangle_1 | 0 \rangle_0 \times f^*(\omega) f(\omega') e^{i\omega t} e^{-i\omega' t} \\
 &= \kappa^2 \left\{ \int d\omega f^*(\omega) e^{i\omega t} \right\} \left\{ \int d\omega' f(\omega') e^{-i\omega' t} \right\} \\
 &= \kappa^2 g^*(t) g(t) \\
 &= \kappa^2 |g(t)|^2
 \end{aligned} \tag{2.61}$$

Here, $g(t)$ is the Fourier transform of the spectral amplitude $f(\omega)$. Similarly, we can check that the rest three terms of Eq. (2.58) is zero. $\langle \Psi | E_1^-(t) E_0^+(t) | \Psi \rangle = \langle \Psi | E_0^-(t) E_1^+(t) | \Psi \rangle = \langle \Psi | E_0^-(t) E_0^+(t) | \Psi \rangle = 0$. So, combining all these in Eq. (2.58)

$$\langle E_2^-(t) E_2^+(t) \rangle = T_1 |g(t)|^2 \tag{2.62}$$

In the same way we calculate the rest three terms in Eq. (2.57).

$$\langle E_2^-(t) E_3^+(t - \tau) \rangle = i\sqrt{T_1 R_1} g^*(t) g(t - \tau) \tag{2.63}$$

$$\langle E_3^-(t - \tau) E_2^+(t) \rangle = -i\sqrt{T_1 R_1} g^*(t - \tau) g(t) \tag{2.64}$$

$$\langle E_3^-(t - \tau) E_3^+(t - \tau) \rangle = R_1 |g(t - \tau)|^2 \tag{2.65}$$

Using Eqs. (2.62), (2.63), (2.64), (2.65) in Eq. (2.57)

$$\langle E_4^-(t) E_4^+(t) \rangle = T_1 T_2 |g(t)|^2 + R_1 R_2 |g(t - \tau)|^2 - \sqrt{T_1 T_2 R_1 R_2} g^*(t) g(t - \tau) - \sqrt{T_1 T_2 R_1 R_2} g^*(t - \tau) g(t) \tag{2.66}$$

So, the intensity at the output port 4 becomes,

$$P_4(\tau) = \int \langle E_4^-(t) E_4^+(t) \rangle dt = T_1 T_2 + R_1 R_2 - 2\sqrt{T_1 T_2 R_1 R_2} \int \text{Re}\{g^*(t) g(t - \tau)\} dt \tag{2.67}$$

Intensity at the output port 5 is,

$$P_5(\tau) = \int \langle E_5^-(t) E_5^+(t) \rangle dt = T_1 R_2 + R_1 T_2 + 2\sqrt{T_1 T_2 R_1 R_2} \int \text{Re}\{g^*(t)g(t-\tau)\} dt \quad (2.68)$$

From Eqs. (2.67) and (2.68), it is evident that the two output arms of the MZI show interference pattern if the value of τ is within the coherence time. For larger τ values the interference terms (integrating terms in Eqs. 2.67 and 2.68) vanishes, and hence no interference. The occurrence of constructive or destructive interference depends on the value of τ as well as the form of the function $g(t)$ (or the form of the spectral amplitude; $f(\omega)$).

2.4.2 Sagnac interferometer

Sagnac interferometer is functionally similar to a MZI interferometer, as both of them have a similar mathematical operation and produce interference patterns in the two output arms. However, the Sagnac interferometer has some additional advantages over MZI, due to its geometric configuration. In Fig. 2.9 we show a schematic of a displaced Sagnac interferometer. Single photons go to the input arm 1 of the non-polarizing beamsplitter (BS) and come out in a superposition state between the two arms 2 and 3. Both the paths are aligned using the same mirrors and combined again at the beamsplitter BS. The output arms 4 and 5 collect single photons using detectors (SPADs). If we calculate the output intensities at the two output arms ($P_4(\tau)$ and $P_5(\tau)$) in the similar way described for the MZI, we get equivalent expressions as in Eq. (2.67) and (2.68) with the only exception that in this case, the transmission or reflection probabilities of the beamsplitters are the same; $T_1 = T_2 = T$, $R_1 = R_2 = R$.

$$P_4(\tau) = T^2 + R^2 - 2TR \int \text{Re}\{g^*(t)g(t-\tau)\} dt \quad (2.69)$$

$$P_5(\tau) = T^2 + R^2 + 2TR \int \text{Re}\{g^*(t)g(t-\tau)\} dt \quad (2.70)$$

In a MZI, the two paths interact with two different mirrors, so due to some external effects like temperature fluctuations, mechanical stress, human interaction, etc., the two path lengths can fluctuate with time leading to fluctuating path difference and unstable interference pattern.

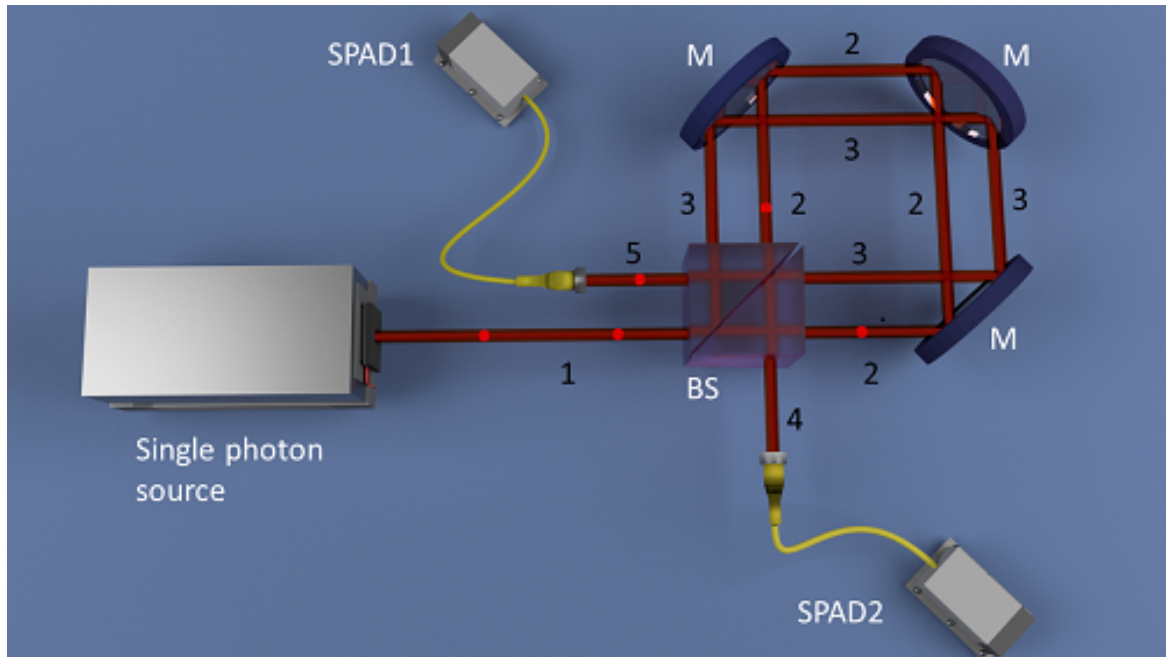


Fig. 2.9 Schematic of a displaced Sagnac interferometer. **BS**: non-polarizing beamsplitter; **M**: Mirror; **SPAD1**, **SPAD2**: single photon avalanche detectors.

On the other hand, both paths of the Sagnac interferometer pass through the same optical components, so any fluctuation affects both the paths similarly, hence no fluctuating path difference. So, a Sagnac interferometer is inherently stable compared to a MZI. However, there is also an issue in the displaced Sagnac interferometer that may lead to non-optimal interference visibility. Although the two paths (2 and 3) hit the same optical components they do not hit at the exact same spot, due to the displaced configuration. All real optical components may have some non-ideal properties due to the manufacturing process, for example, optical mirrors have an uneven surface in the microscopic scale, so the two beams reflected from two different spots of the uneven mirror may lead to the change of the phase correlation between the two beams, and hence lowering the interference visibility.

Chapter 3

Hong-Ou-Mandel (HOM) interference and the role of Complementarity

3.1 Introduction

The Hong-Ou-Mandel (HOM) effect or the two-photon interference effect [56, 40] is considered as one of the most important phenomena in quantum optics. This effect which is a salient fourth-order interference effect [54], is a unique indicator of “quantumness”, with absolutely no analog in classical physics. Due to its distinctive characteristics, the HOM effect is being used in various applications of quantum mechanics, including precise time measurements, measuring photon purity [25] and distinguishability [85], heralding in optical quantum computing gates [69], Boson Sampling [1], and preparing a $N00N$ state for quantum metrology [31].

Hong-Ou-Mandel effect occurs when two indistinguishable photons hit the two input ports of a beamsplitter at the same time (within the coherence time of the photon) and interfere to produce a 100% “dip” in the coincidence detection between the two output ports of the beamsplitter. This is not due to the second-order interference effect, as ideal single photons (Fock state $|1\rangle$) do not have any phase correlation. This effect is due to the intensity-intensity correlation (fourth-order interference) which is unique to the quantum state and something that is not observed for the classical state. So, instead of single photons, if two identical classical pulses with proper phase randomization are sent to the beamsplitter,

the maximum dip in the coincidence visibility that can be achieved is only 50%.

However, the 50% threshold for the dip in coincidence visibility is not the boundary between the classical and the quantum behaviors of light, but rather a result of the lack of control over the phases of the input pulses. So, with selective phase randomization, classical pulses can also generate near-100% HOM visibility dip [98]. To resolve this issue, we modify the HOM setup by adding a Mach-Zehnder interferometer (MZI) to it, which checks for the wave-particle complementarity relation. Although classical pulses can be made to switch between exhibiting particle-like and wavelike behaviors by controlling the phase, both cannot manifest with the same choice of phase. On the other hand, a two-photon state shows wave-particle complementarity, by being indivisible (particle-like) in the HOM experiment and being in a superposition state (wave-like) of two paths when interference is measured in the MZI, without any change in the source setting. This wave-particle complementarity is the boundary between the classical and the quantum.

This chapter of the thesis only includes the quantum version of the HOM experiment where single photon pairs generated from a spontaneous parametric down-conversion (SPDC) source are used to show near-100% HOM visibility dip, as well as the modification of the conventional HOM setup to accommodate the wave-particle complementarity experiment. In Section 3.2, we show the calculation for the HOM dip using quantum mechanical formalism, and how it is different from classical formalism. Section 3.3 includes details of the HOM experimental setup, the plot of the HOM dip, and fitting to the plot using a theoretical model considering all realistic imperfections. Section 3.4 deals with the experimental setup and results of the wave-particle complementarity test along with the theoretical study. Finally, Section 3.5 contains various error analysis used in the experimental results. Details of the complete work (including HOM experiment with classical pulses) can be found in the reference [98]. Also, a part of the work which is related to the classical version of the HOM experiment has been included in a thesis chapter of my colleague, Dr. Simanraj Sadana [97].

3.2 Theory

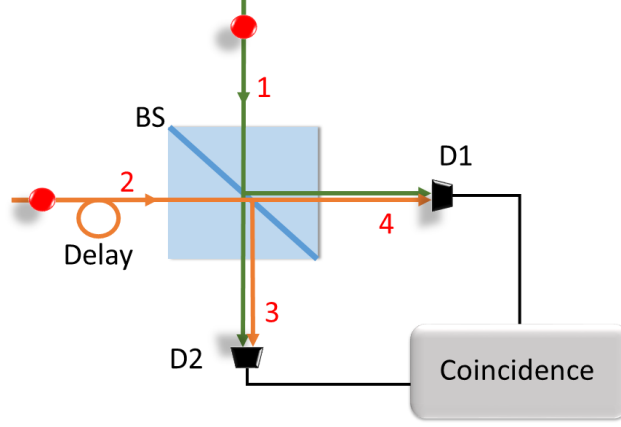


Fig. 3.1 HOM interference occurs when two indistinguishable photons are sent to the two input arms (**1** and **2**) of the beamsplitter (**BS**), at the same time. A variable time delay ($\delta\tau$) is introduced by applying a variable path delay in one of the input arms (arm **2**). Coincidence is measured between the two single-photon detectors (**D1** and **D2**) placed at the two output arms of the **BS**, arm **4** and arm **3** respectively.

In a HOM experiment, two photons that are completely indistinguishable in all degrees of freedom are sent to a symmetric beamsplitter. Each photon can be represented as an ideal Fock state $|1\rangle$. Two input ports of the beamsplitter are marked as 1 and 2, whereas two output ports of the beamsplitter are marked as 3 and 4 (see Fig. 3.1). A beamsplitter matrix is represented as,

$$\begin{bmatrix} \sqrt{T} & i\sqrt{R} \\ i\sqrt{R} & \sqrt{T} \end{bmatrix} \quad (3.1)$$

T and R are the transmission and the reflection probabilities of the beamsplitter, respectively, where $T + R = 1$. For a symmetric or 50:50 beamsplitter $T = R = 1/2$, and the beamsplitter matrix becomes,

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \quad (3.2)$$

In terms of the quantum mechanical creation operators, we can write the transformation due to the beamsplitter as,

$$\hat{a}_1^\dagger \rightarrow \frac{\hat{a}_3^\dagger}{\sqrt{2}} + i \frac{\hat{a}_4^\dagger}{\sqrt{2}} \quad (3.3)$$

$$\hat{a}_2^\dagger \rightarrow \frac{\hat{a}_4^\dagger}{\sqrt{2}} + i \frac{\hat{a}_3^\dagger}{\sqrt{2}} \quad (3.4)$$

Also, in the beamsplitter, the vacuum states of the input ports are directly transformed to the vacuum states of the output ports, $|0\rangle_1|0\rangle_2 \rightarrow |0\rangle_3|0\rangle_4$. Two photons impinging on the two input ports of the beamsplitter is denoted as $|1\rangle_1|1\rangle_2$, which go under the following transformation in the beamsplitter.

$$\begin{aligned} |1\rangle_1|1\rangle_2 &= \hat{a}_1^\dagger \hat{a}_2^\dagger |0\rangle_1|0\rangle_2 \rightarrow \left\{ \frac{\hat{a}_3^\dagger}{\sqrt{2}} + i \frac{\hat{a}_4^\dagger}{\sqrt{2}} \right\} \left\{ \frac{\hat{a}_4^\dagger}{\sqrt{2}} + i \frac{\hat{a}_3^\dagger}{\sqrt{2}} \right\} |0\rangle_3|0\rangle_4 \\ &= \left\{ \frac{\hat{a}_3^\dagger \hat{a}_4^\dagger}{2} + i \frac{(\hat{a}_3^\dagger)^2}{2} + i \frac{(\hat{a}_4^\dagger)^2}{2} - \frac{\hat{a}_4^\dagger \hat{a}_3^\dagger}{2} \right\} |0\rangle_3|0\rangle_4 \\ &= \frac{1}{2} |1\rangle_3|1\rangle_4 + \frac{i}{\sqrt{2}} |2\rangle_3|0\rangle_4 + \frac{i}{\sqrt{2}} |0\rangle_3|2\rangle_4 - \frac{1}{2} |1\rangle_3|1\rangle_4 \\ &= \frac{i}{\sqrt{2}} \{ |2\rangle_3|0\rangle_4 + |0\rangle_3|2\rangle_4 \} \end{aligned} \quad (3.5)$$

So, the output state from the symmetric beamsplitter is a superposition state of Fock state $|2\rangle$ in both output arms. Physically, this means that if two indistinguishable single photons hit a symmetric beamsplitter at the same time, then the two photons will always bunch together and come out in either of the two output ports of the beamsplitter. If we measure the coincidence between the two output arms, the result will always be a null value.

We can also describe this phenomenon in a much more simplistic way. When one photon hits a 50:50 beamsplitter, it has half probability of transmission and half probability of reflection from the beamsplitter. So, when two photons hit the beamsplitter simultaneously, there are four possibilities, photon 1 is transmitted and photon 2 is reflected, photon 1 is reflected and photon 2 is transmitted, both photons are transmitted, and both photons are reflected (see Fig. 3.2). If the two photons hit the beamsplitter at the same time (time delay, $\delta\tau = 0$) and the two photons are indistinguishable w.r.t. all other degrees of freedom

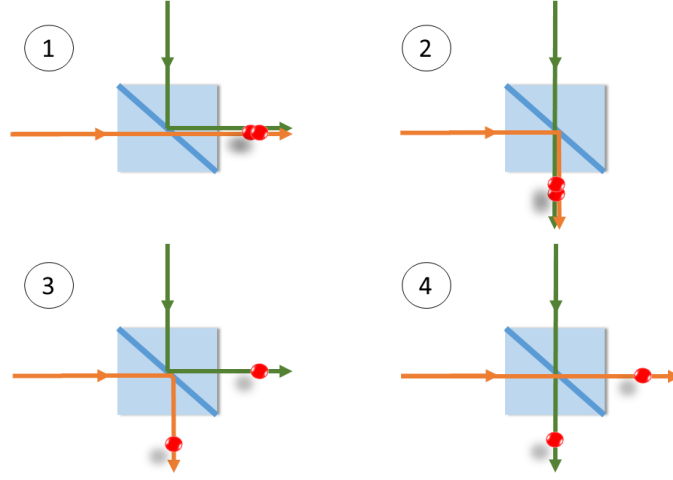


Fig. 3.2 Two single-photons hitting simultaneously a symmetric beamsplitter are in a superposition of four possible output states; one photon is transmitted and one photon is reflected (case 1 and 2), both photons are reflected (case 3), both photons are transmitted (case 4).

(spectral, spatial, polarization, etc.), then according to the quantum mechanical principle, these four possible outcomes are in a quantum mechanical superposition state. The last two possible outcomes (case 3 and 4 in Fig. 3.2), having identical amplitude but opposing in sign, cancel each other, hence no possible coincidence between the two output arms. If the time delay is larger compared to the coherence time of the single photons ($\delta\tau \gg \tau_c$), then this superposition does not occur, and no cancellation of output states. So, in this case, the coincidence probability becomes $\frac{1}{2}$ rather than 0. We define the visibility of the HOM dip as,

$$V = \frac{C(\delta\tau \gg \tau_c) - C(\delta\tau = 0)}{C(\delta\tau \gg \tau_c)} \quad (3.6)$$

Here $C(\delta\tau \gg \tau_c)$ is the coincidence for time delay much much greater than the coherence time, $C(\delta\tau = 0)$ is the coincidence at zero time delay. From the quantum mechanical formalism, the value of the visibility becomes 1, by putting $C(\delta\tau \gg \tau_c) = \frac{1}{2}$ and $C(\delta\tau = 0) = 0$ in the equation 3.6.

In the semi-classical theory of light, input light to the beamsplitter are written as electric field $\vec{E}_1$ and $\vec{E}_2$, respectively. These two electric fields have a relative phase difference of ϕ .

A beamsplitter operation can be expressed in terms of the following equations.

$$\vec{E}_3 = \frac{\vec{E}_1}{\sqrt{2}} + i \frac{\vec{E}_2 e^{i\phi}}{\sqrt{2}} \quad (3.7)$$

$$\vec{E}_4 = i \frac{\vec{E}_1}{\sqrt{2}} + \frac{\vec{E}_2 e^{i\phi}}{\sqrt{2}} \quad (3.8)$$

Average intensities in the two output arms are $\langle I_3 \rangle = \langle |E_3|^2 \rangle = \frac{\langle I_1 \rangle}{2} + \frac{\langle I_2 \rangle}{2} - \sqrt{\langle I_1 \rangle \langle I_2 \rangle} \langle \sin \phi \rangle$ and $\langle I_4 \rangle = \langle |E_4|^2 \rangle = \frac{\langle I_1 \rangle}{2} + \frac{\langle I_2 \rangle}{2} + \sqrt{\langle I_1 \rangle \langle I_2 \rangle} \langle \sin \phi \rangle$. To nullify any second-order interference effect due to the contribution of relative phase in this semi-classical formalism, phase (ϕ) is randomized among the ensemble such that $\langle \sin \phi \rangle = 0$ and $\langle I_3 \rangle, \langle I_4 \rangle$ become phase independent. Coincidence at $\delta\tau = 0$ and $\delta\tau \gg \tau_c$ for this phase-randomized scenario is represented by

$$C(\delta\tau = 0) = \langle I_3 I_4 \rangle_{\delta\tau=0} = \frac{\langle I_1^2 \rangle}{4} + \frac{\langle I_2^2 \rangle}{4} + \frac{\langle I_1 \rangle \langle I_2 \rangle}{2} - \langle I_1 \rangle \langle I_2 \rangle \langle \sin^2 \phi \rangle = \frac{\langle I_1^2 \rangle}{4} + \frac{\langle I_2^2 \rangle}{4} \quad (3.9)$$

$$C(\delta\tau \gg \tau_c) = \langle I_3 I_4 \rangle_{\delta\tau \gg \tau_c} = \frac{\langle I_1^2 \rangle}{4} + \frac{\langle I_2^2 \rangle}{4} + \frac{\langle I_1 \rangle \langle I_2 \rangle}{2} \quad (3.10)$$

Using 3.9 and 3.10 in equation 3.6, HOM visibility for the classical case is written as,

$$V = \frac{2\langle I_1 \rangle \langle I_2 \rangle}{\langle I_1^2 \rangle + \langle I_2^2 \rangle + 2\langle I_1 \rangle \langle I_2 \rangle} \leq 0.5 \quad (3.11)$$

Classical light pulse can only reach a maximum HOM visibility of 0.5. So, any violation of 0.5 confirms the existence of “quantumness”, and the violation value can reach up to 1.

To plot a complete HOM profile, we need to measure coincidence detection probability between the two output arms of the beamsplitter, for different delays ($\delta\tau$) between the two impinging single photons. We can define coincidence detection probability after the beamsplitter as the ratio of the “total joint detections after the beamsplitter” and the “total input photon pairs to the beamsplitter”. $P_{3,4}(\tau)$ is the measure of joint detection, where one photon of the pair is detected at port 4 at time t , and the other one in port 3 at time $t + \tau$. K is a factor due to different losses in the setup (loss due to imperfect fiber coupling, fiber

transmission loss, loss due to the beamsplitter, etc.) as well as the efficiencies of the detectors.

$$P_{3,4}(\tau) = K \langle E_4^-(t) E_3^-(t+\tau) E_3^+(t+\tau) E_4^+(t) \rangle \quad (3.12)$$

Here, E^+ and E^- are the positive and negative frequency components of the electric field. From the field quantization (see Section 2.1.1 for details), we write the expression for the electric field as,

$$E^+(r, t) = i\kappa \hat{a} e^{i(kr - \omega t)} \quad (3.13)$$

$$E^-(r, t) = -i\kappa \hat{a}^\dagger e^{-i(kr - \omega t)} \quad (3.14)$$

where $\kappa = \sqrt{\frac{\hbar\omega}{2\varepsilon_0 V}}$, $\hat{a}$ and $\hat{a}^\dagger$ are the quantum mechanical annihilation and creation operators. k is the wave number and ω is the angular frequency. ε_0 is the permittivity in free space, and V is the volume of the mode field.

Total joint detections is the integration of $P_{3,4}(\tau)$ for all τ value. Ideally, τ should be integrated only over coherence time, but due to the large value of the timing resolution in typical detectors, we can safely integrate τ over $-\infty$ to $+\infty$. In our case, coherence time is around 700 fs (FWHM), but our detector resolution is near 500 ps, which is much much larger compared to the coherence time. In order to measure the “total input photon pairs to the beamsplitter”, we also apply the same procedure where we integrate on $P_{1,2}(\tau)$. $K = 1$ for this case as there is no actual detection taking place.

$$\begin{aligned} \text{Coincidence detection probability} &= \frac{\text{Total joint detections after the beamsplitter}}{\text{Total input photon pairs to the beamsplitter}} \\ &= \frac{\int_{-\infty}^{\infty} P_{3,4}(\tau) d\tau}{\int_{-\infty}^{\infty} P_{1,2}(\tau) d\tau} \\ &= \frac{K \int_{-\infty}^{\infty} \langle E_4^-(t) E_3^-(t+\tau) E_3^+(t+\tau) E_4^+(t) \rangle d\tau}{\int_{-\infty}^{\infty} \langle E_2^-(t) E_1^-(t+\tau) E_1^+(t+\tau) E_2^+(t) \rangle d\tau} \end{aligned} \quad (3.15)$$

$E_4^\pm(t)$ and $E_3^\pm(t)$ are related to the fields $E_1^\pm(t)$, $E_2^\pm(t)$ due to the operation of the beamsplitter matrix (3.1).

$$E_4^\pm(t) = \sqrt{T} E_2^\pm(t - \tau_0 - \delta\tau) \pm i\sqrt{R} E_1^\pm(t - \tau_0) \quad (3.16)$$

$$E_3^\pm(t) = \sqrt{T}E_1^\pm(t - \tau_0) \pm i\sqrt{R}E_2^\pm(t - \tau_0 - \delta\tau) \quad (3.17)$$

Here, τ_0 is the propagation time required for the photons to come from E_1 position to E_4 or E_3 . $\delta\tau$ is the time delay introduced in port 2 (see Fig. 3.1). The splitting ratio of the beamsplitter is $T : R$, where $T + R = 1$. For the special case of symmetric beamsplitter, $T = R = 0.5$.

In the case of degenerate single photon pairs generated from a spontaneous parametric down-conversion (SPDC) process, both signal and idler photons have the same frequency (within the quantum mechanical uncertainty in frequency, or bandwidth limited). Also, the signal and idler photons are entangled in frequency. Two-photon input state to the beamsplitter can be written as,

$$|\Psi\rangle_{in} = \int_{-\infty}^{\infty} \phi(\omega) \left| \frac{\omega_p}{2} + \omega \right\rangle_s \left| \frac{\omega_p}{2} - \omega \right\rangle_i d\omega \quad (3.18)$$

ω_p is the pump frequency (assuming monochromatic pump). $\left| \frac{\omega_p}{2} + \omega \right\rangle$ and $\left| \frac{\omega_p}{2} - \omega \right\rangle$ are the signal and idler photon states. $\phi(\omega)$ is the joint spectral amplitude of generating signal photon at frequency $(\frac{\omega_p}{2} + \omega)$ and idler photon at frequency $(\frac{\omega_p}{2} - \omega)$. Signal photon goes to the input port 1, and the idler photon goes to the input port 2.

$$|\Psi\rangle_{in} = \int_{-\infty}^{\infty} \phi(\omega) \left| \frac{\omega_p}{2} + \omega \right\rangle_1 \left| \frac{\omega_p}{2} - \omega \right\rangle_2 d\omega \quad (3.19)$$

Using equation 3.16 and 3.17, we can write: $\langle E_4^-(t)E_3^-(t+\tau)E_3^+(t+\tau)E_4^-(t) \rangle$

$$\begin{aligned}
&= \langle \Psi_{in} | \left\{ \sqrt{T}E_2^-(t - \tau_0 - \delta\tau) - i\sqrt{R}E_1^-(t - \tau_0) \right\} \left\{ (\sqrt{T}E_1^-(t - \tau_0 + \tau) - i\sqrt{R}E_2^-(t - \tau_0 - \delta\tau + \tau)) \right\} \\
&\quad \left\{ \sqrt{T}E_1^+(t - \tau_0 + \tau) + i\sqrt{R}E_2^+(t - \tau_0 - \delta\tau + \tau) \right\} \left\{ \sqrt{T}E_2^+(t - \tau_0 - \delta\tau) + i\sqrt{R}E_1^+(t - \tau_0) \right\} | \Psi_{in} \rangle \\
&= \langle \Psi_{in} | \left\{ TE_2^-(t - \tau_0 - \delta\tau)E_1^-(t - \tau_0 + \tau) - RE_1^-(t - \tau_0)E_2^-(t - \tau_0 - \delta\tau + \tau) \right. \\
&\quad \left. - i\sqrt{TRE}_2^-(t - \tau_0 - \delta\tau)E_2^-(t - \tau_0 - \delta\tau + \tau) - i\sqrt{TRE}_1^-(t - \tau_0)E_1^-(t - \tau_0 + \tau) \right\} \\
&\quad \times \left\{ TE_1^+(t - \tau_0 - \tau)E_2^+(t - \tau_0 - \delta\tau) - RE_2^+(t - \tau_0 - \delta\tau + \tau)E_1^+(t - \tau_0) \right. \\
&\quad \left. - i\sqrt{TRE}_2^+(t - \tau_0 - \delta\tau)E_2^+(t - \tau_0 - \delta\tau + \tau) - i\sqrt{TRE}_1^+(t - \tau_0)E_1^+(t - \tau_0 + \tau) \right\} | \Psi_{in} \rangle \\
&\quad (3.20)
\end{aligned}$$

Equation 3.20 has 16 terms among which only 4 terms will give non-zero values. Values for these 4 terms can be calculated using equations 3.13, 3.14 and 3.19.

$$\begin{aligned}
1) & \langle \Psi | E_2^-(t - \tau_0 - \delta\tau) E_1^-(t - \tau_0 + \tau) E_1^+(t - \tau_0 - \tau) E_2^+(t - \tau_0 - \delta\tau) | \Psi \rangle \\
&= \kappa^2 \int d\omega \int d\omega' \left\langle \frac{\omega_p}{2} + \omega, \frac{\omega_p}{2} - \omega \mid \hat{a}_2^\dagger \hat{a}_1^\dagger \hat{a}_1 \hat{a}_2 \mid \frac{\omega_p}{2} + \omega', \frac{\omega_p}{2} - \omega' \right\rangle \\
&\times \phi^*(\omega) \phi(\omega') e^{i(\frac{\omega_p}{2} + \omega)(t - \tau_0 - \delta\tau)} e^{i(\frac{\omega_p}{2} - \omega)(t - \tau_0 + \tau)} e^{-i(\frac{\omega_p}{2} - \omega')(t - \tau_0 + \tau)} e^{-i(\frac{\omega_p}{2} + \omega')(t - \tau_0 - \delta\tau)} \\
&= \kappa^2 \int d\omega \int d\omega' \phi^*(\omega) \phi(\omega') e^{i(\omega - \omega')(\tau + \delta\tau)} \\
&= \kappa^2 \left\{ \int d\omega \phi^*(\omega) e^{i\omega(\tau + \delta\tau)} \right\} \left\{ \int d\omega' \phi(\omega') e^{-i\omega'(\tau + \delta\tau)} \right\} \\
&= \kappa^2 g^*(\tau + \delta\tau) g(\tau + \delta\tau) \\
&= \kappa^2 |g(\tau + \delta\tau)|^2
\end{aligned} \tag{3.21}$$

Here, $g(\tau)$ is the Fourier transform of $\phi(\omega)$. $g(\tau) = \int d\omega \phi(\omega) e^{-i\omega\tau}$.

Similarly, we can calculate the rest three terms.

$$\begin{aligned}
2) & \langle \Psi_{in} | E_1^-(t - \tau_0) E_2^-(t - \tau_0 - \delta\tau + \tau) E_2^+(t - \tau_0 - \delta\tau + \tau) E_1^+(t - \tau_0) | \Psi_{in} \rangle \\
&= \kappa^2 |g(\tau - \delta\tau)|^2
\end{aligned} \tag{3.22}$$

$$\begin{aligned}
3) & \langle \Psi_{in} | E_2^-(t - \tau_0 - \delta\tau) E_1^-(t - \tau_0 + \tau) E_2^+(t - \tau_0 - \delta\tau + \tau) E_1^+(t - \tau_0) | \Psi_{in} \rangle \\
&= \kappa^2 g^*(\tau + \delta\tau) g(\delta\tau - \tau)
\end{aligned} \tag{3.23}$$

$$\begin{aligned}
4) & \langle \Psi_{in} | E_1^-(t - \tau_0) E_2^-(t - \tau_0 - \delta\tau + \tau) E_1^+(t - \tau_0 + \tau) E_2^+(t - \tau_0 - \delta\tau) | \Psi_{in} \rangle \\
&= \kappa^2 g^*(\delta\tau - \tau) g(\tau + \delta\tau)
\end{aligned} \tag{3.24}$$

Using equations 3.20, 3.21, 3.22, 3.23, 3.24 in equation 3.12

$$\begin{aligned}
P_{3,4}(\tau) &= \kappa^2 K \left\{ T^2 |g(\tau + \delta\tau)|^2 + R^2 |g(\tau - \delta\tau)|^2 - RT g^*(\tau + \delta\tau) g(\delta\tau - \tau) \right. \\
&\quad \left. - RT g^*(\delta\tau - \tau) g(\tau + \delta\tau) \right\}
\end{aligned} \tag{3.25}$$

Here, we also show the calculation for $P_{1,2}(\tau)$.

$$\begin{aligned}
P_{1,2}(\tau) &= \langle \Psi_{in} | E_2^-(t) E_1^-(t+\tau) E_1^+(t+\tau) E_2^-(t) | \Psi_{in} \rangle \\
&= \kappa^2 \int d\omega \int d\omega' \left\langle \frac{\omega_p}{2} + \omega, \frac{\omega_p}{2} - \omega \mid \hat{a}_2^\dagger \hat{a}_1^\dagger \hat{a}_1 \hat{a}_2 \mid \frac{\omega_p}{2} + \omega', \frac{\omega_p}{2} - \omega' \right\rangle \\
&\quad \times \phi^*(\omega) \phi(\omega') e^{i(\frac{\omega_p}{2} + \omega)(t)} e^{i(\frac{\omega_p}{2} - \omega)(t+\tau)} e^{-i(\frac{\omega_p}{2} - \omega')(t+\tau)} e^{-i(\frac{\omega_p}{2} + \omega')(t)} \quad (3.26) \\
&= \kappa^2 \left\{ \int d\omega \phi^*(\omega) e^{i\omega\tau} \right\} \left\{ \int d\omega' \phi(\omega') e^{-i\omega'\tau} \right\} \\
&= \kappa^2 |g(\tau)|^2
\end{aligned}$$

Coincidence detection probability is calculated using equations 3.25, 3.26 in equation 3.15.

$$C = \frac{\int_{-\infty}^{\infty} P_{3,4}(\tau) d\tau}{\int_{-\infty}^{\infty} P_{1,2}(\tau) d\tau} = K \left\{ T^2 + R^2 - 2RT \frac{\int_{-\infty}^{\infty} \text{Re}(g(\tau + \delta\tau) g^*(\tau - \delta\tau)) d\tau}{\int_{-\infty}^{\infty} |g(\tau)|^2 d\tau} \right\} \quad (3.27)$$

To simplify the calculation, we can re-normalize equation 3.19 such that $\int_{-\infty}^{\infty} |\phi(\omega)|^2 d\omega = 1$.

Using Plancherel's theorem we get,

$$\int_{-\infty}^{\infty} |g(\tau)|^2 d\tau = \int_{-\infty}^{\infty} |\phi(\omega)|^2 d\omega = 1 \quad (3.28)$$

Equation 3.27 now becomes

$$C = K \left\{ T^2 + R^2 - 2RT \int_{-\infty}^{\infty} \text{Re}(g(\tau + \delta\tau) g^*(\tau - \delta\tau)) d\tau \right\} \quad (3.29)$$

Coincidence detection probability (C) is a function of time delay ($\delta\tau$) between the two input photons. In the idealistic case of loss-less experimental setup ($K = 1$) and using symmetric beamsplitter ($T = R = 0.5$), equation 3.29 becomes

$$C = \frac{1}{2} \left\{ 1 - \int_{-\infty}^{\infty} \text{Re}(g(\tau + \delta\tau) g^*(\tau - \delta\tau)) d\tau \right\} \quad (3.30)$$

At $\delta\tau = 0$, the second term (integration term) of equation 3.30 becomes 1 due to the normalization condition introduced in 3.28. So, $C(\delta\tau = 0) = 0$. In case of $\delta\tau \gg \tau_c$, the integration

term becomes zero, leading to the coincidence probability $C(\delta\tau \gg \tau_c) = 1/2$. We can plot C as a function of time delay ($\delta\tau$) or path delay ($c \times \delta\tau$) in order to get the complete HOM profile.

3.3 HOM experiment

3.3.1 Experimental setup

The HOM experiment starts with a photon source which generates single-photon pairs. We use collinear, degenerate, type II spontaneous parametric down-conversion (SPDC) process to generate single photon pairs. Fig. 3.3 depicts the schematic of the experimental setup. A diode laser (Toptica-iwave) pumps a BBO (Beta-Barium Borate) crystal with a continuous pump power of 50 mW. The diode laser operates at a pump wavelength centered at 405 nm. An isolator is placed just after the laser to reduce the damage to the laser due to any unwanted back-reflected light. Also, polarization controlling optics (half waveplate and quarter waveplate combination) is incorporated such that the input beam to the BBO crystal always maintain horizontal polarization. In a standard type II SPDC process, a single photon of frequency ω_p , whose polarization axis is along the extra-ordinary (e) direction w.r.t. the optical axis of the non-linear birefringent crystal, creates two photons of frequency ω_s (signal photon) and ω_i (idler photon) with polarization axes in extra-ordinary and ordinary (o) directions, respectively. The energy must be conserved for this process. Also, the phase-matching condition needs to be satisfied.

$$\omega_p = \omega_s + \omega_i \quad (3.31)$$

$$\vec{k}_p = \vec{k}_s + \vec{k}_i \quad (3.32)$$

In our experiment, we perform degenerate SPDC, so both the signal and idler photon has the same frequency ($\omega_s = \omega_i$). For a pump wavelength of 405 nm, the energy conservation imposes that the signal and idler wavelength are both centered at 810 nm. In our lab frame, the “e” axis w.r.t. the optical axis of the crystal is the horizontal axis, hence the pump beam

should be maintained as horizontally polarized, which creates horizontally polarized signal photon and vertically polarized idler photon via SPDC process. Birefringent phase-matching condition is typically achieved by tilting the non-linear crystal such as BBO in X-Y-Z axes. In a type-II phase-matching, signal and idler photons are generated in two separate cone format (see Section 2.2.2). If we look at the cross-section plane (X-Y plane) perpendicular to the propagation direction (Z-axis) of the pump beam, signal and idler photons form two separate SPDC rings. To achieve collinear phase-matching, we tilt the BBO crystal such that the two SPDC rings intersect each other at only one point. If we collect photon pairs only from this single intersection zone, we can successfully post-select only collinear single-photon pairs.

In order to increase the brightness of the photon pair generation, A pair of lenses of focal lengths 22.5 cm (L1) and 25 cm (L2) is used to focus the pump beam at the center of the crystal and to collimate the down-converted photons respectively. A long-pass filter (F1) blocks the pump beam (405 nm) and passes only single-photon pairs of wavelength 810 nm. A band-pass filter (F2) with a 3.1 nm bandwidth (FWHM) centered on 810 nm restricts the bandwidth of the transmitted photons and block any residual pump beam as well as any background stray photons of different wavelengths. As in the collinear configuration both the photons in a pair traverse the same path, a polarizing beamsplitter (PBS) is used to separate the two photons of each pair. The signal photon which is horizontally polarized transmits through the PBS and the idler photon, being vertically polarized, gets reflected by the PBS. In this way, we generate two single photons ready to be sent to the two input ports of a symmetric ($T : R = 50 : 50$) beamsplitter.

The most important condition for the HOM interference effect is the indistinguishability of the two input photons. So it is necessary to make sure that one cannot distinguish the two input photons going to the beamsplitter in any associated degrees of freedom. Two photons being generated from a single source at the same time, via a unique physical process (SPDC) is advantageous from this point of view. However, we additionally implement some filtering arrangements to reduce the distinguishability as much as possible. We prepare the source in a degenerate configuration such that both the photons of a pair have the same frequency. Also,

we use a tight interference filter (F2) for both the photons to pass through, such that they are completely indistinguishable in frequency, except with an uncertainty of around 3 nm, which is much much smaller than the wavelength of the individual photons. To minimize the distinguishability in the polarization degree of freedom, both the photons are made the same polarized. A half waveplate (HWP) is placed in the transmitted arm of the PBS such that it converts the horizontally polarized signal photon into vertically polarized. So, both the signal and idler photon are vertically polarized before hitting the beamsplitter. For the spatial degree of freedom, both the photons are coupled to the single-mode fibers, which eliminates any spatial mode information.

We use a fiber-beamsplitter (FBS) instead of a free-space beamsplitter. The FBS has the same functionality as a conventional symmetric beamsplitter, i.e, same splitting ratio $T : R = 50 : 50$, except with the fact that the two input parts (1 and 2) and the two output ports (3 and 4) are coupled with single-mode fibers. Usage of an FBS is advantageous as it is efficient in terms of proper alignment purpose. As we have shown in the calculation that the maximum coincidence dip in the HOM profile occurs when the two photons hit the FBS at the same time, i.e, $\delta t = 0$ or path difference $\delta l = c \times \delta t = 0$. This is not trivial to achieve though the two fibers connected to the two input ports of the FBS ideally have the same length. We mount the fiber coupler of any one input port (here, input port 2 in Fig. 3.3) on top of a translational axis mount which is connected to a piezo-driven motorized actuator stage. We control the path difference (δl) by translating the position of the fiber coupler along the direction of the input beam, by controlling the motorized actuator. The two fibers connected to the two output ports of the FBS are also connected to two single photon avalanche detectors (τ – SPADs from Pico Quant) at the other ends. The two SPADs are connected to a time-tagging logic (TTL) unit (from UQD) which records the timestamps of all the detected photons in the SPADs, with a pico-second resolution. We use a LabVIEW program to measure the singles counts from individual SPADs as well as the coincidences between the two detectors; on the run.

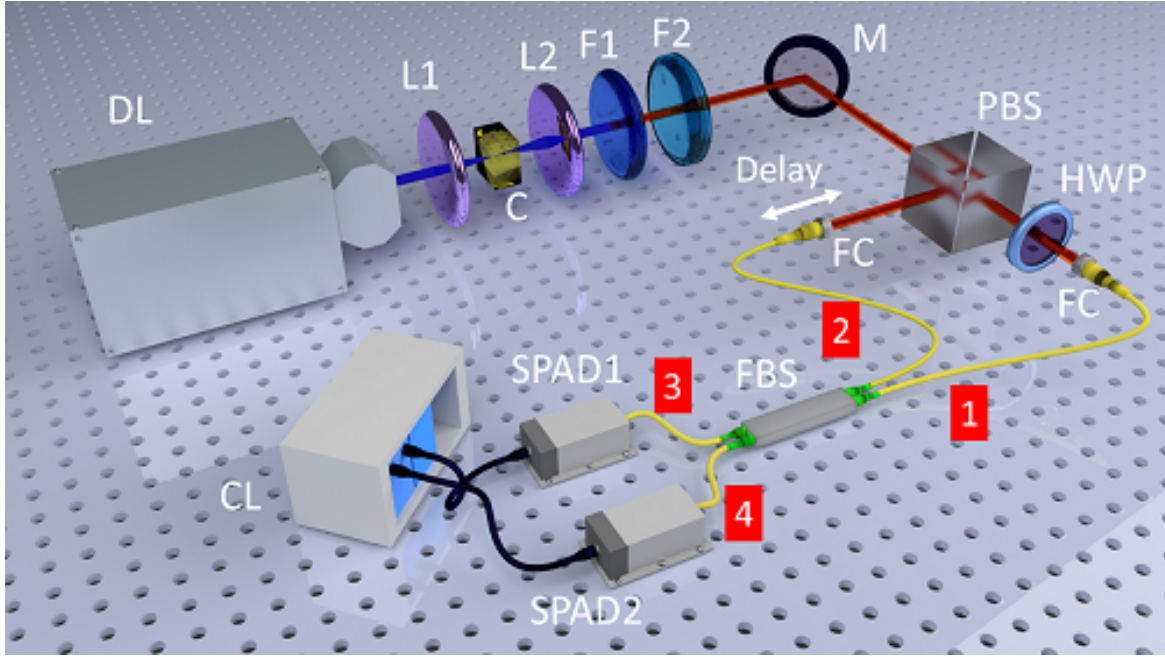


Fig. 3.3 Illustration of the HOM experimental setup. **DL**: diode laser with central wavelength at 405 nm and pump power of 50 mW; **L1**: focusing lens with focal length of 22.5 cm; **L2**: collimating lens with focal length of 25 cm; **C**: BBO crystal of dimension 5 mm × 5 mm × 10 mm; **F1**: long-pass filter at cut-off frequency 405 nm; **F2**: band-pass filter with 3.1 nm bandwidth centred on 810 nm; **M**: dielectric mirror; **PBS**: polarizing beamsplitter; **HWP**: half waveplate; **FC**: fiber coupler; **FBS**: fiber beamsplitter; **SPAD1**, **SPAD2**: single-photon avalanche detectors; **CL**: single-photon counting and coincidence measurement module.

The first step of the measurement strategy is to find the appropriate coincidence time window (W). For this purpose, we plot the cross-correlation (or coincidence) between the two outgoing photons while the time delay ($\delta\tau$) between the two incoming photons is higher than the coherence time. We measure the full-width at half-maximum (FWHM) of the coincidence plot around the peak at $\delta\tau$ in the X-axis. If the time delay is changed then only the peak position of the coincidence shifts accordingly, but not the profile or the FWHM value. So, we fixed the measured FWHM value as the coincidence window (W) which in our case is around 2 ns. We move the motorized actuator stage housing the fiber coupler (input arm 2) slowly with a step size of 10 μm which changes the path delay (or time delay) between the two incoming photons. At each position of the actuated stage coincidence count is recorded for some fixed time, where only events within the coincidence time window around the peak are considered as part of the coincidence count. The data acquisition time is 5 seconds at

each position and we measure at 160 positions. We repeat the measurement 100 times for better averaging and to estimate an error bar.

3.3.2 Results and theory fit to the experimental plot

We plot the HOM profile from the data generated from the experiment (Fig. 3.4). The x-axis represents the time delay ($\delta\tau$) between the two incoming photons. The y-axis shows the measured average coincidence value for each time delay. We observe a dip in the coincidence near the zero time delay. The measured value of the coincidence visibility dip is $96.06 \pm 0.16\%$, and the full-width at half-maxima (FWHM) of the dip is 0.66 ps (200 μm) which is related to the coherence time (length) of the single photons generated from our SPDC source. We also fit the experimental HOM plot with our theoretical model.

Theory fit considering all realistic imperfections:

The two-photon state due to the type II, collinear, degenerate SPDC process at the BBO crystal can be written as $|\Psi\rangle = \int_{-\infty}^{\infty} \phi(\omega) |\omega\rangle_H |\bar{\omega}\rangle_V d\omega$. Where, $\phi(\omega)$ is the joint spectral amplitude (JSA). We have defined the signal state as $|\omega\rangle = \left| \frac{\omega_p}{2} + \omega \right\rangle$ and the idler state as $|\bar{\omega}\rangle = \left| \frac{\omega_p}{2} - \omega \right\rangle$. Subscripts H and V represent horizontal and vertical polarization states respectively, and ω_p is the pump frequency. Both photons in a pair are passed through the same filter with spectral transmission profile $F(\omega)$, where the probability of both photons in a photon-pair with frequency combination $\frac{\omega_p}{2} + \omega$ and $\frac{\omega_p}{2} - \omega$ to pass the filter is $|F(\omega)|^2$. So, the joint spectral amplitude after the filter becomes $f(\omega) = \phi(\omega)F(\omega)$. Due to the collinear configuration of the photon pairs we separate photons of each pair using a PBS such that the signal photon $\left| \frac{\omega_p}{2} + \omega \right\rangle$ goes to input port 1, and idler $\left| \frac{\omega_p}{2} - \omega \right\rangle$ goes to the input port 2 of the FBS. Ideal PBS should transmit only horizontally (H) polarized photon and reflect vertically (V) polarized photon. But, in practice it may not happen.

For ideal PBS, output state of the PBS should be $|\Psi\rangle = \int_{-\infty}^{\infty} f(\omega) |\omega\rangle_{1,H} |\bar{\omega}\rangle_{2,V} d\omega$. We assume that the joint spectral amplitude ($f(\omega)$) is symmetric around $\omega = 0$, and normalized as $\int |f(\omega)|^2 d\omega = 1$. However, a realistic PBS does not have the perfect extinction ratio. Any

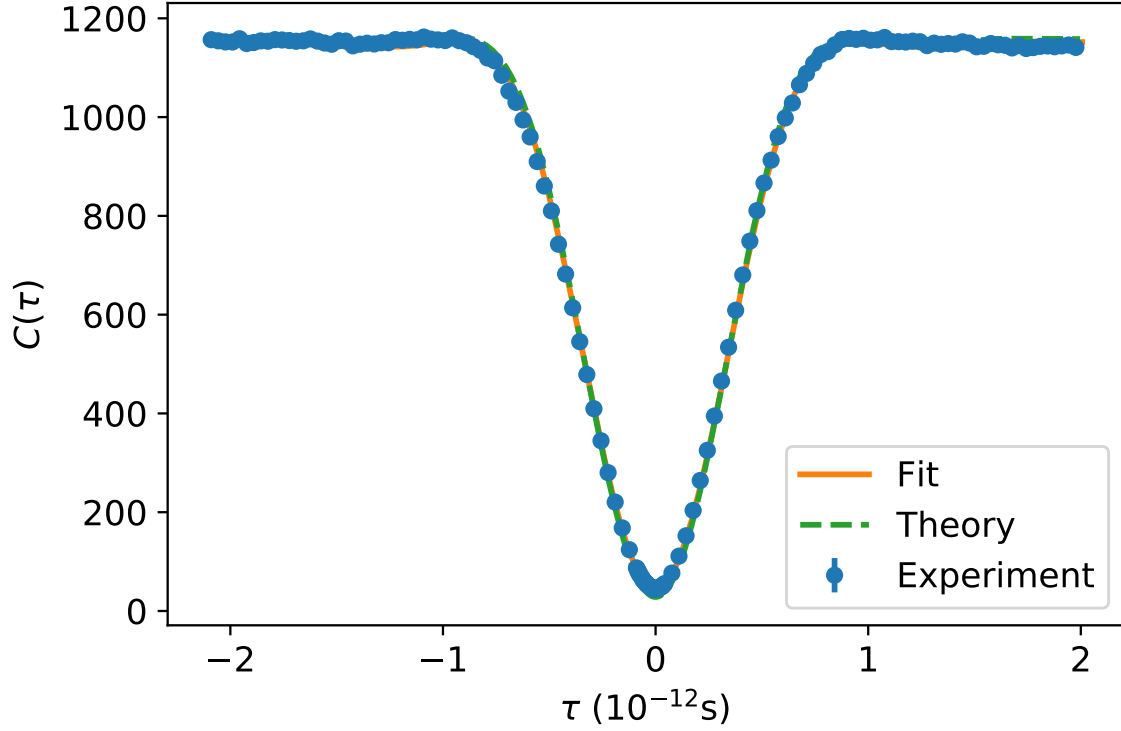


Fig. 3.4 Average coincidence counts (C) measured as a function of time delay ($\delta\tau$) between the two input photons are represented by blue dots. The error bars represent 95% confidence intervals for the average coincidence count. The green dashed line represents the estimated plot from theory. The orange line is the result of fitting to the experimental data. The fitted plot (orange) overlaps almost completely with the theoretically estimated plot (green).

finite or rather bad extinction ratio of the PBS leads to the transmission of some V polarized photons and reflection of some H polarized photons as well.

Due to the non-ideality of the PBS, the output state becomes a mixed state of four possible outcomes: $|\omega\rangle_{1,H}|\bar{\omega}\rangle_{2,V}, |\omega\rangle_{1,V}|\bar{\omega}\rangle_{2,H}, |\omega\rangle_{1,H}|\bar{\omega}\rangle_{1,V}, |\omega\rangle_{2,H}|\bar{\omega}\rangle_{2,V}$ with respective probabilities $\alpha^2, \beta^2, \gamma^2, \delta^2$. Here, $\alpha^2 = T_h^2 R_v^2, \beta^2 = T_v^2 R_h^2, \gamma^2 = T_h^2 T_v^2, \delta^2 = R_h^2 R_v^2$. T_h^2 and R_h^2 are the transmission and reflection probabilities of H polarized light through the PBS, whereas T_v^2 and R_v^2 are the transmission and reflection probabilities of V polarized light through the PBS. We now find the effect of these four possible states impinging on the beamsplitter (FBS) separately.

Case 1: for input state $|\omega\rangle_{1,H}|\bar{\omega}\rangle_{2,V}$

The input state is passed through the half waveplate (HWP) placed in the input arm 1, which rotates the polarization of the photon passing through arm 1 following the operation represented as,

$$\hat{a}_H^\dagger(\omega) \rightarrow \hat{a}_H^\dagger(\omega)\cos 2\theta + \hat{a}_V^\dagger(\omega)\sin 2\theta \quad (3.33)$$

$$\hat{a}_V^\dagger(\omega) \rightarrow \hat{a}_H^\dagger(\omega)\sin 2\theta - \hat{a}_V^\dagger(\omega)\cos 2\theta \quad (3.34)$$

Here, θ is the angle between the optic axis of the waveplate and the horizontal polarization direction. We write the input state to the FBS using equation 3.33 and 3.34

$$\int_{-\infty}^{\infty} f(\omega) \left\{ \cos 2\theta \hat{a}_{1,H}^\dagger(\omega) \hat{a}_{2,V}^\dagger(\bar{\omega}) + \sin 2\theta \hat{a}_{1,V}^\dagger(\omega) \hat{a}_{2,V}^\dagger(\bar{\omega}) \right\} e^{-i(\frac{\omega_P}{2} - \omega)\delta\tau} |0\rangle_1 |0\rangle_2 d\omega \quad (3.35)$$

where $\delta\tau$ is the time delay introduced in one input arm (here, port 2) of the FBS. Output state of the FBS becomes (using equation 3.3, 3.4),

$$\begin{aligned} |\Psi\rangle = \int_{-\infty}^{\infty} f(\omega) & \left[\cos 2\theta \left\{ T \hat{a}_{3,H}^\dagger(\omega) \hat{a}_{4,V}^\dagger(\bar{\omega}) + i\sqrt{TR} \hat{a}_{3,H}^\dagger(\omega) \hat{a}_{3,V}^\dagger(\bar{\omega}) \right. \right. \\ & \left. \left. + i\sqrt{TR} \hat{a}_{4,H}^\dagger(\omega) \hat{a}_{4,V}^\dagger(\bar{\omega}) - R \hat{a}_{4,H}^\dagger(\omega) \hat{a}_{3,V}^\dagger(\bar{\omega}) \right\} \right. \\ & \left. + \sin 2\theta \left\{ T \hat{a}_{3,V}^\dagger(\omega) \hat{a}_{4,V}^\dagger(\bar{\omega}) + i\sqrt{TR} \hat{a}_{3,V}^\dagger(\omega) \hat{a}_{3,V}^\dagger(\bar{\omega}) + i\sqrt{TR} \hat{a}_{4,V}^\dagger(\omega) \hat{a}_{4,V}^\dagger(\bar{\omega}) \right. \right. \\ & \left. \left. - R \hat{a}_{4,V}^\dagger(\omega) \hat{a}_{3,V}^\dagger(\bar{\omega}) \right\} \right] e^{-i(\frac{\omega_P}{2} - \omega)\delta\tau} |0\rangle_3 |0\rangle_4 d\omega \quad (3.36) \end{aligned}$$

Coincidence measurement between two output arms of the FBS (denoted as port 3 and 4) can be written as the following measurement operator.

$$\hat{M}_3 \otimes \hat{M}_4 = \sum_{i,j=\{H,V\}} \int \hat{a}_{3,i}^\dagger(\omega) \hat{a}_{4,j}^\dagger(\bar{\omega}) |0\rangle_3 |0\rangle_4 \langle 0|_4 \langle 0|_3 \hat{a}_{4,j}(\bar{\omega}) \hat{a}_{3,i}(\omega) d\omega \quad (3.37)$$

Coincidence probability, $C = \text{Tr} \left[|\Psi\rangle \langle \Psi| \hat{M}_3 \otimes \hat{M}_4 \right] = \langle \Psi | \hat{M}_3 \otimes \hat{M}_4 | \Psi \rangle$

$$\boxed{C = T^2 + R^2 - 2TR \sin^2(2\theta) \int |f(\omega)|^2 \cos(2\omega\delta\tau) d\omega} \quad (3.38)$$

Case 2: for input state $|\omega\rangle_{1,V} |\bar{\omega}\rangle_{2,H}$

Input state to the FBS is

$$\int_{-\infty}^{\infty} f(\omega) \left\{ \cos 2\theta \hat{a}_{1,H}^{\dagger}(\omega) \hat{a}_{2,H}^{\dagger}(\bar{\omega}) - \sin 2\theta \hat{a}_{1,V}^{\dagger}(\omega) \hat{a}_{2,H}^{\dagger}(\bar{\omega}) \right\} e^{-i(\frac{\omega_p}{2} - \omega)\tau} |0\rangle_1 |0\rangle_2 d\omega \quad (3.39)$$

By performing similar calculations as mentioned for case 1, we get a similar coincidence probability as in equation 3.38.

$$C = T^2 + R^2 - 2TR \sin^2(2\theta) \int |f(\omega)|^2 \cos(2\omega\delta\tau) d\omega \quad (3.40)$$

Case 3: for input state $|\omega\rangle_{1,H} |\bar{\omega}\rangle_{1,V}$

Input state to the FBS is:

$$\int_{-\infty}^{\infty} f(\omega) \left\{ \cos(2\theta) \sin(2\theta) \hat{a}_{1,H}^{\dagger}(\omega) \hat{a}_{1,H}^{\dagger}(\bar{\omega}) - \cos^2(2\theta) \hat{a}_{1,H}^{\dagger}(\omega) \hat{a}_{1,V}^{\dagger}(\bar{\omega}) \right. \\ \left. + \sin^2(2\theta) \hat{a}_{1,V}^{\dagger}(\omega) \hat{a}_{1,H}^{\dagger}(\bar{\omega}) - \cos(2\theta) \sin(2\theta) \hat{a}_{1,V}^{\dagger}(\omega) \hat{a}_{1,V}^{\dagger}(\bar{\omega}) \right\} |0\rangle_1 |0\rangle_2 d\omega \quad (3.41)$$

giving the coincidence probability: $C = 2TR$

Case 4: for input state $|\omega\rangle_{2,H} |\bar{\omega}\rangle_{2,V}$

Input state to the FBS is $\int_{-\infty}^{\infty} f(\omega) \hat{a}_{2,H}^{\dagger}(\omega) \hat{a}_{2,V}^{\dagger}(\bar{\omega}) e^{-i\omega_p\tau} |0\rangle_1 |0\rangle_2 d\omega$. Output state from the FBS becomes,

$$|\Psi\rangle = \int_{-\infty}^{\infty} f(\omega) \left\{ T \hat{a}_{4,H}^{\dagger}(\omega) \hat{a}_{4,V}^{\dagger}(\bar{\omega}) + i\sqrt{TR} \hat{a}_{3,H}^{\dagger}(\omega) \hat{a}_{4,V}^{\dagger}(\bar{\omega}) + i\sqrt{TR} \hat{a}_{4,H}^{\dagger}(\omega) \hat{a}_{3,V}^{\dagger}(\bar{\omega}) \right. \\ \left. - R \hat{a}_{3,H}^{\dagger}(\omega) \hat{a}_{3,V}^{\dagger}(\bar{\omega}) \right\} \\ \times e^{-i\omega_p\delta\tau} |0\rangle_3 |0\rangle_4 d\omega \quad (3.42)$$

Coincidence probability: $C = 2TR$

Taking into consideration all the four cases, the final coincidence probability becomes,

$$C(\delta\tau) = (\alpha^2 + \beta^2) \left\{ T^2 + R^2 - 2TR \sin^2(2\theta) \int |f(\omega)|^2 \cos(2\omega\delta\tau) d\omega \right\} + 2(\gamma^2 + \delta^2) TR \quad (3.43)$$

The expression in 3.43 has many parameters that are related to various imperfections and non-ideality associated with optical components. We can write the expression in a more simplistic form.

$$C(\delta\tau) = \chi_1 \left\{ T^2 + R^2 - 2TR\chi_2 \int |f(\omega)|^2 \cos(2\omega\delta\tau) d\omega \right\} + 2(1 - \chi_1)TR \quad (3.44)$$

The probability that each input arm of the FBS has one photon is represented by χ_1 , where $\chi_1 = \alpha^2 + \beta^2 = T_h^2 R_v^2 + T_v^2 R_h^2$. So, the probability that both photons simultaneously go to any one of the two input arms is $(1 - \chi_1) = \gamma^2 + \delta^2$, as one can easily verify that $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 1$. The χ_1 parameter is entirely linked with the PBS extinction ratio. On the other hand, the χ_2 parameter, where $\chi_2 = \sin^2(2\theta)$, represents the error associated with the inaccurate rotation of the half waveplate (HWP). We adapt two separate fitting strategies here; the first one is called *estimation from theory* where we put values to all parameters in 3.44 either from direct measurement or from data-sheet provided by the manufacturer of the individual components. In the second strategy which we call *fit to the experiment*, we numerically fit our experimental data with equation 3.44, where all the free-parameters are also fitting parameters.

Estimation from theory

Equation 3.44 depends on four parameters; χ_1 , χ_2 , T and $|f(\omega)|^2$. To calculate the value of χ_1 we need values of the extinction ratios of the PBS used in our experiment. From the data-sheet provided by the manufacturer, the PBS extinction ratio is 1000:1 in its transmission arm and between 20:1 to 100:1 in the reflection arm. So, $\frac{T_h^2}{T_v^2} = \frac{1000}{1}$, and $\frac{R_v^2}{R_h^2} = [\frac{20}{1}; \frac{100}{1}]$. Due to the given range of the extinction ratio in the reflection arm of the PBS, we measure this value directly from an experiment, which gives us the value $R_v^2/R_h^2 = 52/1$. χ_2 depends on the half waveplate angle (θ) which is kept fixed at 45° with respect to the horizontal polarization direction. However, the waveplate mount is accurate up to 1° which gives the error in the θ value as $45 \pm 1^\circ$. So, the χ_2 value which is ideally 1 can be 0.998 in the worst-case scenario. The T parameter is the transmission probability of the beamsplitter

(FBS). For an ideal symmetric beamsplitter this $T : R$ value should be 50 : 50, but we find the value $T : R = 52 : 48$ from direct measurement. So, we put $T = 0.52$ in the equation 3.44. The joint spectral amplitude (JSA) is expressed as $f(\omega) = \phi(\omega)F(\omega)$, where $\phi(\omega)$ is the joint spectral amplitude of the photon pairs generated from the SPDC process and $F(\omega)$ is the joint spectral distribution of the bandpass filter used in the setup. $\phi(\omega)$ distribution depends primarily on the Fourier transform of the distribution of the non-linearity parameter (χ^2) throughout the crystal and is typically represented as Gaussian or Sinc type distribution. In our case, we assume $|\phi(\omega)|^2$ as Gaussian for the sake of simplicity in the calculation.

$$|\phi(\omega)|^2 = \frac{1}{\sqrt{2\pi}\sigma^2} e^{-\frac{(\omega - \omega_0)^2}{2\sigma^2}} \quad (3.45)$$

The Gaussian distribution is centered at ω_0 which is half of the pump frequency in the case of the degenerate SPDC process ($\omega_0 = \omega_p/2$). σ is the standard deviation of the Gaussian distribution and is an unknown parameter. $|F(\omega)|^2$ is the probability that both photons of the same pair with frequencies $\omega_p/2 + \omega$ and $\omega_p/2 - \omega$ are passed through the bandpass filter. So, we measure the $|F(\omega)|^2$ profile directly from the spectral transmission profile of the bandpass filter (Fig. 3.5).

Finally, we put all the known parameters in the equation 3.44 and fit the expression $K \times C(\delta\tau)$ with the experimental HOM plot. Here we use a scaling factor (K) as $C(\delta\tau)$ is the coincidence probability whereas experimental HOM plot (Fig. 3.4) contains total coincidence value in the y-axis. The fitting parameters are only the scaling factor K and σ as all the other parameters are known to us. $\chi_1 = T_h^2 R_v^2 + T_v^2 R_h^2 = 0.0201$, $\chi_2 = 0.998$, $T = 0.52$, $R = 0.48$. We get the best fit for $\sigma = 0.59$ nm and $K = 2301$, resulting in the HOM visibility dip of $V = 97.56\%$. The goodness of the fit is the R-squared value which is 0.9998.

Fit to the experiment

Along with the theory estimation as described in the previous section we also fit the experimental plot (Fig. 3.4) where all the free parameters in the expression $K \times C(\delta\tau)$ (see

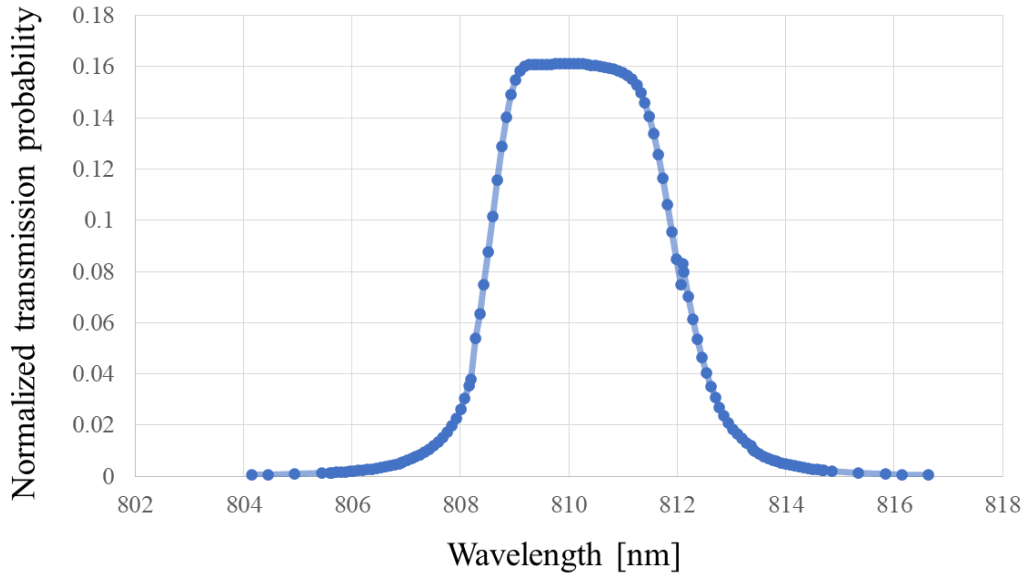


Fig. 3.5 Spectral transmission profile (normalized) of the bandpass filter used in the setup (Semrock LL01-810-25).

3.44), i. e., χ_1 , χ_2 , K , σ are fit parameters. The reason for this step is that although the major systematic errors have been taken into account in the *estimation from theory*, there are additional errors that are untraceable, like dispersion and rotation of polarization as the photon passes through different fibers and components, spatial mode mismatch in the two fiber inputs of the FBS, etc. Consequently, the experimental result has a slight deviation from the theoretical estimate. The experimental fit line (red line in Fig. 3.4) is a result of such a fit. The best fit, with R-squared value of 0.9998 was achieved for $\sigma = 0.581$ nm, $K = 2303$, $\chi_1 = 0.038$, $\chi_2 = 0.9995$, resulting in a coincidence visibility dip of 96.06%.

3.4 HOM Complementarity

Near 100% coincidence visibility dip due to two-photon interference obtained in the HOM experiment is a unique phenomenon in quantum mechanics. The input single photon pairs to the HOM setup do not have any specific phase relation among themselves, due to the quantum mechanical uncertainty in phase associated with each single photon state $|1\rangle$. For this reason, second-order interference (or first-order coherence) is not observed in the HOM experiment,

which also implies that the observed interference in the HOM profile (intensity-intensity correlation) is only due to the fourth-order interference (or second-order coherence). If the same HOM experiment is performed using two indistinguishable classical light pulses instead of single photons, second-order interference can be observed as the two classical pulses have some relative phase between them. One standard way to nullify this is to randomize the phase difference between the two pulses, for the whole input statistics. This randomization strategy not only eliminates any second-order interference but also limits the HOM visibility dip up to 50%. This difference in the visibility dip makes a distinction between quantum and classical formalism. However, it is shown in reference [98], both theoretically and experimentally, that with selective phase randomization strategy in the classical case, one can also nullify any second-order interference for the whole statistics, while at the same time increase the HOM coincidence visibility dip up to 100%; similar to the quantum case.

Therefore, it is important to modify the standard HOM setup to adapt to this new challenge. The standard HOM test practically checks for two things; quantumness as well as the degree of indistinguishability between two photons. So we keep the HOM setup for the indistinguishability check, and add another interferometric set up in addition to that, for the complementarity check. In quantum mechanics, wave-particle complementarity is also a unique phenomenon that does not have a classical counterpart. So, we use a similar notion of complementarity to check for the “quantumness”. Near 100% HOM visibility dip can be considered as a signature of particle-like behaviour, as photons are detected always in either one of the two detectors, but this output state of the HOM setup also creates an interference pattern in the interferometer, hence the wave-like behaviour. On the other hand, though the classical pulses can mimic particle-like behaviour (100% visibility dip), they cannot show interference for the same choice of phase selection. A different phase selection may produce interference in the complementarity setup, but cannot show particle-like behaviour in the HOM setup, simultaneously. To summarize, we show that a modified HOM setup which also checks for the wave-particle-like complementarity relation is better than the conventional HOM setup for the purpose of distinguishing between the quantum and the classical formalism.

3.4.1 Experimental setup and results

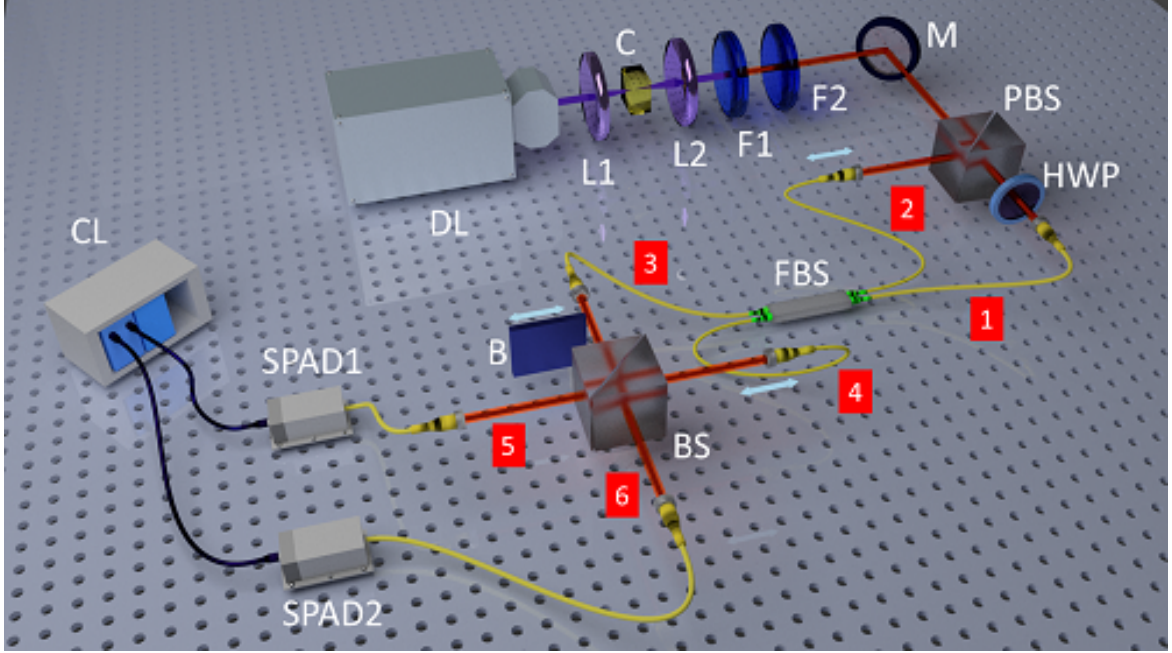


Fig. 3.6 Illustration of the HOM-complementarity experimental setup. **DL**: diode laser with central wavelength at 405 nm and pump power of 50 mW; **L1**: focusing lens with focal length of 22.5 cm; **L2**: collimating lens with focal length of 25 cm; **C**: BBO crystal of dimension 5 mm $\times$ 5 mm $\times$ 10 mm; **F1**: long-pass filter at cut-off frequency 405 nm; **F2**: band-pass filter with 3.1 nm bandwidth centred on 810 nm; **M**: dielectric mirror; **PBS**: polarizing beamsplitter; **HWP**: half waveplate; **FBS**: fiber beamsplitter; **BS**: 50:50 non-polarizing beamsplitter; **B**: beam-blocker; **SPAD1**, **SPAD2**: single-photon avalanche detectors; **CL**: single-photon counting and coincidence measurement module.

Demonstration of the wave-particle-like complementarity relation requires injecting the superposition state of $|2,0\rangle$ and $|0,2\rangle$ which is the output state of the HOM setup, to a Mach-Zehnder interferometer. Photons from the two output fibers of the FBS are incident on a 50-50 beamsplitter (BS) through two collimators. One of the collimators is placed on a motorized translational stage which gives a variable path difference (Δl) in the interferometer. Photons from the two output terminals of the beamsplitter are coupled to single-mode fibers which are connected to two single photon counting modules (τ – SPAD from Pico Quant). We measure the coincidence counts between the two detectors as a function of the path difference (Δl). When the path difference approaches zero, we see an interference pattern. When one of the input arms of the BS is blocked, the coincidence is expected to be 25% of the coincidence

counts when both the arms are open. Fig. 3.7(a) and 3.7(b) shows the coincidence as a function of path difference and Fig. 3.7(c) shows the drop in the coincidence when one of the input arms is blocked. The efficiency of the two collimators and coupling are not identical. Hence, single photon rates in the two output terminals of the BS are not the same. So, we take the average of the two coincidence counts by blocking one of the input arms at a time.

In order to determine the position of the motorized translation stage (port 5 in Fig. 3.6) such that the path difference (Δl) in the interferometer is zero, we block one of the output arms of the PBS (in Fig. 3.6). In this configuration, the second-order interference pattern in singles count appears in each of the output arms of the Mach-Zehnder setup, and the position of the motorized translational stage, where this interference appears, determines the Δl to be zero. After finding the stage's position for $\Delta l = 0$, we go back to the HOM condition (both output arms of the PBS are open) and vary the Δl value by 0.5 mm on each side with 0.01 mm step size. We accumulate the coincidence counts for 10 sec at each position and repeat the profile 50 times. The inset in Fig. 3.7 shows all the 50 profiles. The rapid fluctuation in the data points arises due to the phase instability of our Mach-Zehnder setup. At each position, we find the maximum (or minimum) coincidence among the 50 and fit the profile with a Gaussian model resulting in the upper envelope (or lower) of the interference zone.

3.4.2 Quantum mechanical description of HOM complementarity

The ideal output state after the HOM setup is $\frac{1}{\sqrt{2}}(|2\rangle|0\rangle + |0\rangle|2\rangle)$, where $|2\rangle$ denotes Fock state of $n = 2$. This state is now becomes the input state to another symmetric (50:50) beamsplitter (BS in Fig. 3.6). Also we implement a variable path delay (Δl) in one of the input arms of the beamsplitter in order to introduce some variable time delay (τ ; $\Delta l = c\tau$) between $|2\rangle|0\rangle$ and $|0\rangle|2\rangle$ states. Using operator descriptions (annihilation and creation operators) we can write this input state to the BS as,

$$|\Psi\rangle = \int_{-\infty}^{\infty} f(\omega) \left\{ \alpha \hat{a}_3^\dagger(\omega_s) \hat{a}_3^\dagger(\omega_i) + \beta \hat{a}_4^\dagger(\omega_s) \hat{a}_4^\dagger(\omega_i) \right\} |0\rangle_3 |0\rangle_4 d\omega \quad (3.46)$$

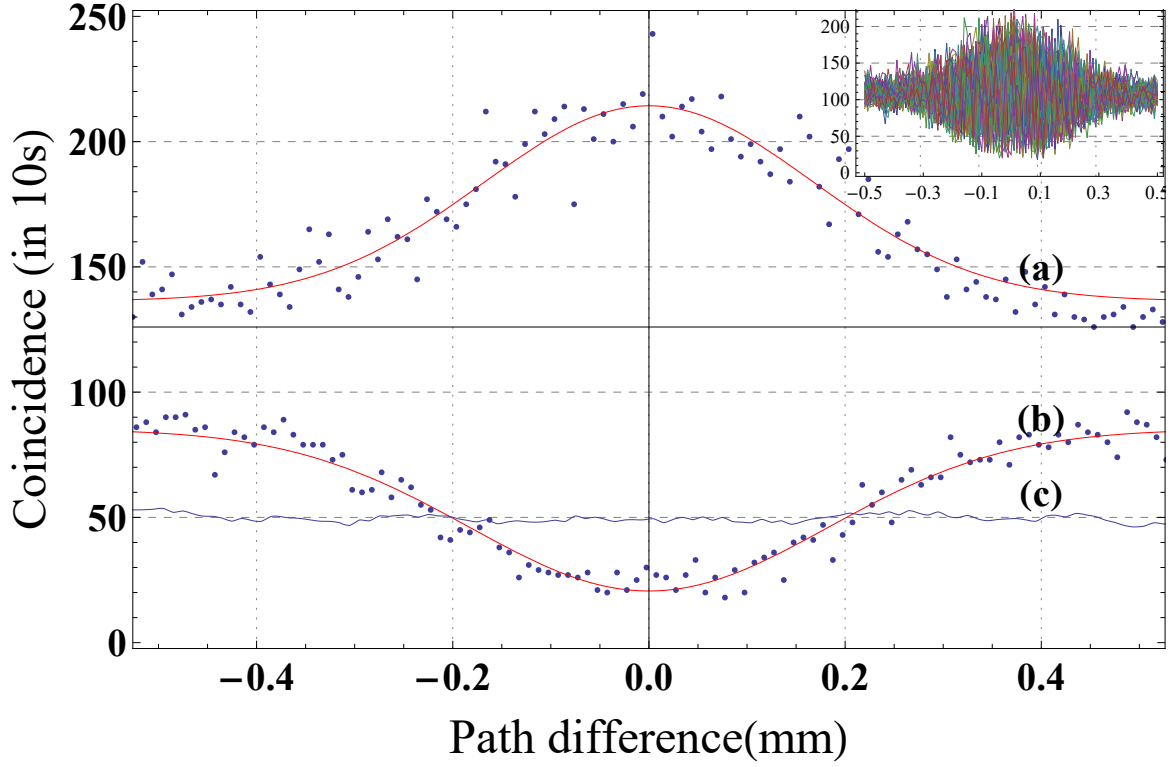


Fig. 3.7 Plot showing the coincidence counts as a function of path difference between the two input arms of the beamsplitter (**BS**) where (a) and (b) show the upper and lower envelope of the interference zone respectively, (c) shows the average of the drop in the coincidence when one or the other input arms of the **BS** is blocked. Inset figure showing coincidence oscillations due to the second order interference for 50 sets of data; all plotted together.

$\omega_s, \omega_i, \omega_p$ represent signal, idler and pump frequencies, where $\omega_s = \frac{\omega_p}{2} + \omega$ and $\omega_i = \frac{\omega_p}{2} - \omega$. α and β are the probability amplitudes for the $|2\rangle_3 |0\rangle_4$ and $|0\rangle_3 |2\rangle_4$ states. In the most ideal scenario of the HOM condition, $\alpha = \beta = \frac{1}{\sqrt{2}}$. Subscripts 3, 4 denote the two input arms of the BS (see Fig. 3.6 as reference). $f(\omega)$ is the joint spectral amplitude (JSA) of the signal-idler pair, and the integration is taken over all possible signal and idler frequencies.

Here we describe two cases; the first being the interference case where both input arms 3 and 4 are open to allow interference, and in the second case one input arm is blocked using a blocker such that no interference is possible at the beamsplitter (BS).

CASE 1: Both input arms are open

A time delay (τ) has been introduced in one arm of the BS (let's say port 4). So now the input state to the BS becomes,

$$\begin{aligned} |\Psi\rangle &= \int_{-\infty}^{\infty} f(\omega) \left\{ \alpha \hat{a}_3^\dagger(\omega_s) \hat{a}_3^\dagger(\omega_i) + \beta \hat{a}_4^\dagger(\omega_s) \hat{a}_4^\dagger(\omega_i) e^{-i\omega_s \tau} e^{-i\omega_i \tau} \right\} |0\rangle_3 |0\rangle_4 d\omega \\ &= \int_{-\infty}^{\infty} f(\omega) \left\{ \alpha \hat{a}_3^\dagger(\omega_s) \hat{a}_3^\dagger(\omega_i) + \beta \hat{a}_4^\dagger(\omega_s) \hat{a}_4^\dagger(\omega_i) e^{-i\omega_p \tau} \right\} |0\rangle_3 |0\rangle_4 d\omega \end{aligned} \quad (3.47)$$

ω_p is introduced in equation 3.47 as $\omega_s + \omega_i = \omega_p$. When this state passes through the beamsplitter (BS), it undergoes the following transformations.

$$\hat{a}_3^\dagger \rightarrow T\hat{a}_6^\dagger + iR\hat{a}_5^\dagger \quad (3.48)$$

$$\hat{a}_4^\dagger \rightarrow T\hat{a}_5^\dagger + iR\hat{a}_6^\dagger \quad (3.49)$$

Here, T and R comes from beamsplitter T:R ratio, $T^2 + R^2 = 1$. using 3.48 and 3.49 in 3.47, the output state from the beamsplitter is written as,

$$\begin{aligned} |\Psi\rangle &= \int_{-\infty}^{\infty} f(\omega) \left\{ P_1 \hat{a}_6^\dagger(\omega_s) \hat{a}_6^\dagger(\omega_i) + P_2 \hat{a}_5^\dagger(\omega_s) \hat{a}_5^\dagger(\omega_i) + P_3 \hat{a}_6^\dagger(\omega_s) \hat{a}_5^\dagger(\omega_i) + P_4 \hat{a}_5^\dagger(\omega_s) \hat{a}_6^\dagger(\omega_i) \right\} \\ &\quad \times |0\rangle_5 |0\rangle_6 d\omega \end{aligned} \quad (3.50)$$

Where,

$$P_1 = (\alpha T^2 - \beta R^2 e^{-i\omega_p \tau}) / \sqrt{2} \quad (3.51)$$

$$P_2 = (-\alpha R^2 + \beta T^2 e^{-i\omega_p \tau}) / \sqrt{2} \quad (3.52)$$

$$P_3 = P_4 = iTR(\alpha + \beta e^{-i\omega_p \tau}) / \sqrt{2} \quad (3.53)$$

Coincidence measurement between the output ports 5 and 6 can be written as operator,

$$\hat{M}_5 \otimes \hat{M}_6 = \int \hat{a}_5^\dagger(\omega_s) \hat{a}_6^\dagger(\omega_i) |0\rangle_5 |0\rangle_6 \langle 0|_6 \langle 0|_5 \hat{a}_6(\omega_i) \hat{a}_5(\omega_s) d\omega.$$

Coincidence Probability:

$$C = Tr \left[|\Psi\rangle \langle\Psi| \hat{M}_5 \otimes \hat{M}_6 \right] = \langle\Psi| \hat{M}_5 \otimes \hat{M}_6 |\Psi\rangle \quad (3.54)$$

Using 3.50 in equation 3.54,

$$C = 2T^2R^2(1 + 2 \times Re(\alpha^* \beta e^{-i\omega_p \tau})) \quad (3.55)$$

For the ideal scenario, $\alpha = \beta = 1/\sqrt{2}$ and $T = R = 1/\sqrt{2}$. So the coincidence probability for this special case is $C = (1 + \cos(\omega_p \tau))/2$.

We can see that coincidence probability (C) is a sinusoidal function of the time delay (τ), varying between 1 and 0. The maximum coincidence probability that can be obtained from interference is 1. Also, the oscillation in the coincidence probability has the frequency of the pump (ω_p), not of the signal or idler photons. The term $f(\omega)$ is no longer present in the final equation, hinting at the fact that the coincidence does not have any relation to the coherence time of the daughter photons.

CASE 2: One input arm is blocked

Now we block any one of the arm (let's block arm 3). The input state to the BS becomes $|\Psi\rangle = \int_{-\infty}^{\infty} f(\omega) \left\{ \beta \hat{a}_4^\dagger(\omega_s) \hat{a}_4^\dagger(\omega_i) \right\} |0\rangle_3 |0\rangle_4 d\omega$. The coincidence probability after the BS (using equations 3.48, 3.49, 3.54) becomes: $C_{block} = 2|\beta|^2 T^2 R^2$. If we block arm 4, the coincidence probability becomes $C_{block}^* = 2|\alpha|^2 T^2 R^2$. Average coincidence probability for the blocked case is then $(C_{block} + C_{block}^*)/2 = T^2 R^2$. For the ideal scenario of symmetric beamsplitter, where $T = R = 1/\sqrt{2}$, the coincidence probability is 1/4 or 25% of the maximum coincidence probability obtained from the interference condition.

Intuitively, we can explain these theoretical calculations. If we block any one of the input arms of the beamsplitter, the superposition state $\frac{1}{\sqrt{2}}(|2\rangle|0\rangle + |0\rangle|2\rangle)$ is collapsed and only half of the photons (either $|2\rangle|0\rangle$ or $|0\rangle|2\rangle$ state) will reach the beamsplitter, which has only 50% chance of coincidence detection in the two output arms. So, $C = 1/4$ if we block any

one of the input arms. When the system does not have “which path” information, we observe interference in the coincidence count with a maximum coincidence probability of 1. When one path is blocked, the system retrieves the path information; leading to “no-interference”.

3.5 Error analysis

Various errors in the experiment :

Here we report various sources of systematic and random errors in our experimental setup. The major contribution of the systematic errors comes from the polarizing beamsplitter (PBS). Though ideally the PBS is supposed to transmit and reflect horizontally and vertically polarized photons respectively, in practice there is a finite probability of transmission for the vertical polarization and reflection for the horizontal polarization. To elaborate the fact, let's say P_H and P_V are the measured power in the transmitted arm when H polarized and V polarized light incidents on a PBS respectively. Assuming the input power is same for both the cases; according to the specification the ratio of P_H to P_V is 1000 : 1. One of the systematic errors also arises due to the fact that the minimum angle we can resolve for our half wave plate rotational mount is 1° . These two errors are taken care in the theoretical estimation of the HOM profile. Still some deviation from theoretical expectation can be observed near zero path delay. The reason could be the small distinguishability arising from the spatial mode-mismatch due to errors in the coupling of the photons in the two single mode fibres. The equality in the lengths of the fibres is limited in 0.1 m.

Two small bumps can be observed in the HOM profile (both theory fit and experiment) which is caused by the spectral profile of the bandpass filter. A systematic error also may appear due to the backlash of the motorized actuator, which is less than $15 \mu\text{m}$, causing some asymmetry in the HOM profile.

The source of the random error is mainly due to the intensity fluctuation of the pump laser as well as the randomness of the spontaneous parametric down conversion (SPDC) process. In order to minimize this type of error, we repeat the experiment for a large number

of times ($N = 100$) and take the average value.

Determination of statistics:

At a fixed time delay ($\delta\tau \gg 0$) between the signal and idler photons, 1000 coincidence counts are measured; each accumulated in 5 seconds. We plot the histogram of the coincidence counts to see the distribution of the coincidental photons. Fig. 3.8 shows the histogram of the coincidence counts where the mean coincidence count is 188.22 with a standard deviation 19.88, which shows the distribution as a super-Poissonian distribution.

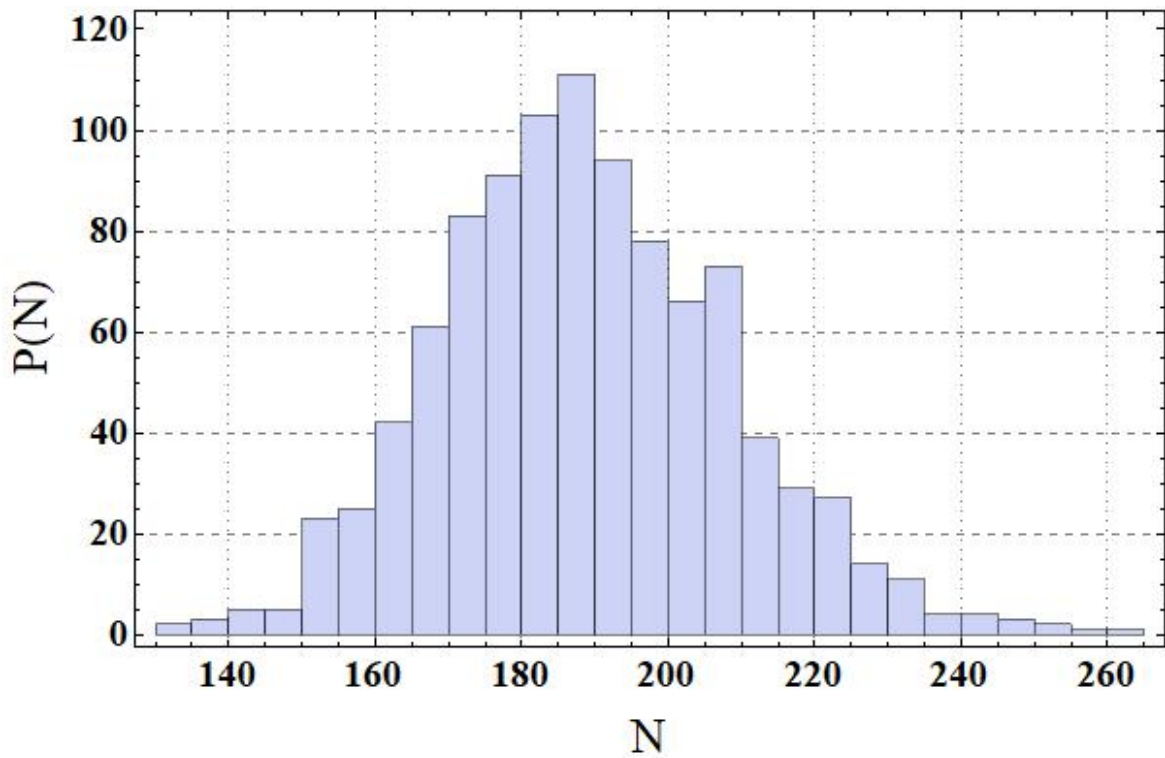


Fig. 3.8 Plot showing the distribution function ($P(N)$) of the measured coincidence counts (N) at a fixed path delay with a mean of 188.22 and standard deviation 19.88. 1000 coincidence counts were measured with 5 sec acquisition time for each.

We observed some oscillations in the coincidence counts in the HOM profile which might be a reflection of the pump laser oscillation itself. We analysed that the time period of the oscillation is around 400 to 500 seconds, which matches the pump oscillation frequency.

Hence, to nullify the oscillation, we decide to finish one whole profile within 500 seconds. We move our stage for a total travel of 1 mm in 0.01 mm step size. So, there are 100 positions and at each position we detect the photons for 5 seconds.

To determine the number of counts required to measure the coincidence value at a particular position, for minimizing the statistical error, we choose certain number of counts of size n , starting from 10 up to 1000. For each sample size, by randomly choosing from those n numbers of counts, we construct 10,000 numbers of samples each with size n . Finally we check how standard deviations of the means vary with the sample size within 95% confidence interval. Fig. 3.9 shows the plot of the standard deviation of the means with respect to sample size. We choose the number of counts as 100 and we can claim that the error in the mean is near 2%.

The result of the experiment is a graph of coincidence counts vs actuator position (which is proportional to the time-delay between the input photons). We took 100 iterations of the experiment; resulting in a sample of 100 sets of coincidences at each position of the actuator. Let us assume that $S = \{s_1, s_2, \dots, s_{100}\}$ represents the sample of coincidence counts at some actuator position x . The reported coincidence counts in Fig. 3.4 are the average values over the set S at each position of the actuator, i.e., $\bar{s} = \frac{\sum_{i=1}^{100} s_i}{100}$. We also measure the confidence interval for $\bar{s}$ by applying a statistical bootstrapping method. In this method, a large number of datasets are prepared by re-sampling with replacement from the original dataset. The sample size of the resampled set is same as the original sample. Let us consider that one such re-sampled set is denoted as S' which has a mean value $\bar{s}'$. We also define $\Delta = \bar{s}' - \bar{s}$ which is the difference between the original sample mean and the re-sampled mean. We repeat the re-sampling procedure for a large number of times (in our case 10^4) and get a list of 10^4 values of Δ . In order to get a confidence interval of 95 percentile, we pick the 2.5th and the 97.5th percentile of the distribution of Δ , which are denoted as $\Delta_{0.025}$ and $\Delta_{0.975}$, respectively. The confidence interval for $\bar{s}$ is then simply expressed as $[\bar{s} + \delta_{0.025}, \bar{s} + \delta_{0.975}]$. We repeat the bootstrapping strategy on datasets obtained for all positions of the actuator. These confidence intervals are plotted as the error bars along with the average values of coincidence counts at each position of the actuator (Fig. 3.4).

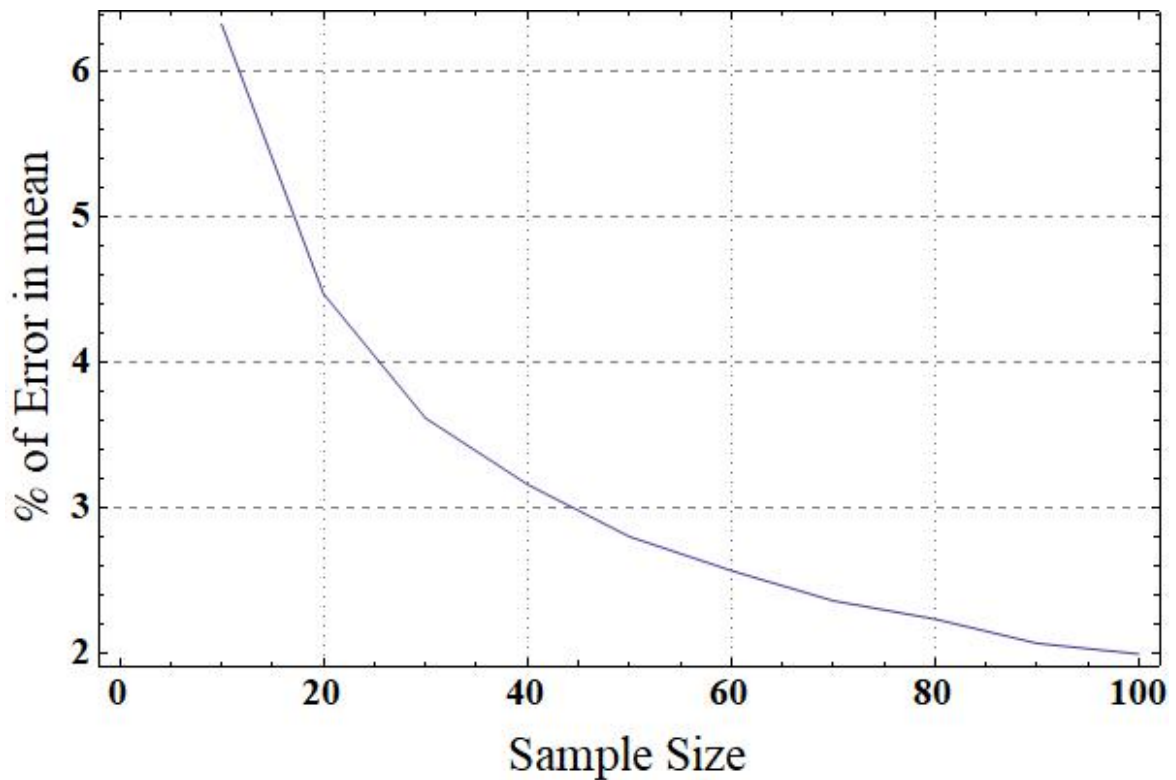


Fig. 3.9 Plot showing the standard error in the mean with respect to the sample size. To determine the number of counts required to measure at a particular position; in order to minimize the statistical error, we choose certain number of counts of size n , starting from 10 up to 1000. For each sample size by randomly choosing from those n numbers of counts we construct 10,000 numbers of samples each with size n . Finally we check how standard deviations of the means vary with the sample size within 95% confidence interval.

Chapter 4

Experimental demonstration of quantum key distribution (QKD); B92 protocol

4.1 Introduction

Secure communication has become an essential part of our life, on day to day basis. In this age of the internet, where all forms of communication and data transfer including emails, video calls, banking, and commerce are performed in electronic platforms, the security breach is the primary concern for all; from the government to private individuals. Cryptography plays a crucial role here; in providing security to all forms of communication. A cryptographer studies various means of scrambling the original message such that only the authentic sender and receiver are able to get back the original message, and not the adversary. On the other side, a cryptanalyst's task is to find new ways of breaching security. A continuous clash of new innovative ideas of a cryptographer and a cryptanalyst has enriched the field of cryptography.

A cryptographic protocol defines a set of operations or instructions that need to be followed to perform the specific cryptographic scheme. In general, any cryptographic protocol follows three main steps, those are key generation, encryption, and decryption. In the key generation process, secure keys are generated among two distant communicating parties, the sender (Alice) and the receiver (Bob). Based on the types of keys, cryptography can be divided into two branches, private key or symmetric key cryptography and public key or

asymmetric key cryptography. In private key cryptography, identical keys are shared only between Alice and Bob. In this process, Alice encrypts the secret message (called plain-text) with her private key. This encrypted message (called cipher-text) can only be decrypted by the identical key which only Bob has. In public key cryptography, Alice generates a public key which she publicly shares with everyone, so in principle, anyone (including Bob) can encrypt the message with the public key, however only Alice can decrypt the message using her private key. Although private and public keys are correlated with each other, they are not identical, hence the name asymmetric key cryptography.

In the one-time pad (OTP) scheme [115] which is a private key cryptographic scheme, keys are generated uniformly randomly, and each key is used only once for the encryption. Shannon in 1949 proved that the one-time pad is unconditionally secure [105] if the key-length is as long as the length of the message. Unconditional security, in terms of cryptography, means that the protocol is information-theoretically secure, even if the adversary has unlimited computational power. Although OTP is the only scheme that is unconditionally secure, it is not widely used, due to the difficulties in practical application. Distributing a truly random key-string among two distant parties, for every encryption is not very practical. So, the classical cryptographic community prefers public-key-based protocols, where the security is based on the computational hardness of some problems. These problems belong to a complexity class called **NP**, which contains set of decision problems solvable in polynomial time by a non-deterministic Turing machine. For example, given two large prime numbers, it is easy to find the product of them, but given the large product, it is extremely difficult to find its factors with current computational power. RSA (Rivest–Shamir–Adleman) algorithm [94], which is one of the most popular algorithms used in public-key cryptography, uses the factorization problem. This type of security is called computational security, since security is based on assumptions about the computational power of the adversary.

Computationally secure cryptographic protocols are applicable in real-world situations as in reality, the adversary always has limitations to his/her computational capacity. However, it may be vulnerable in the presence of advanced technology in the future. More efficient

algorithms and cutting edge computational technology is a threat to security. For example, quantum computers are capable of solving many such hard problems in polynomial time. Factorization problem can be solved in polynomial time ($O((\log N)^2)(\log \log N)(\log \log \log N)$) using a famous quantum algorithm called Shor's algorithm [107].

For a security threat like quantum computers, it is necessary to reconstruct and strengthen the security aspect of conventional cryptographic practices. In this context, quantum cryptography provides an alternative solution, where the security is guaranteed by the laws of nature governed by quantum mechanics, rather than the mathematical complexity of some hard-problems.

4.2 Basic concepts of quantum key distribution (QKD)

Quantum Key Distribution (QKD) is a part of quantum cryptography, which enables two distant parties, Alice and Bob, to generate and distribute secure private keys among themselves. These keys are truly random strings, hence can be used as the secret key in one-time pad encryption protocol for unconditionally secure communication. So the security of the whole cryptographic scheme (message encryption) relies on the security of the QKD scheme. Unlike classical cryptography, QKD provides unconditional security based on the laws of quantum mechanics, including the no-cloning theorem, Heisenberg's uncertainty principle, and quantum entanglement. Also, there are some assumptions involved. Performing a QKD scheme requires two communication channels, one is the quantum and the other one is the classical channel. The quantum channel need not be secure from attacks, however, the classical channel needs to be authenticated. The adversary is not destructive and only acts as an eavesdropper (called Eve), who has unlimited computational power and can eavesdrop in both quantum and classical channels.

The no-cloning theorem restricts Eve from making an identical copy of the unknown quantum state sent by Alice. According to the uncertainty principle, any state prepared in a certain basis, when measured in any non-orthogonal basis, becomes uncertain about the

original prepared state. So if Eve measures the state in the wrong basis (non-orthogonal) rather than what Alice prepares the state in, she introduces errors in the system. Quantum entanglement is a non-local correlation where two states cannot be described independently (non-separable). All the existing QKD protocols can be broadly categorized into two: prepare-and-measure-based protocols and entanglement based protocols. In the prepare-and-measure based schemes, Alice prepares the state of each photon in a randomly selected basis, and sends them to Bob, whereas Bob also randomly selects the measurement basis and measure them. The security here is guaranteed by the uncertainty principle. This type of protocols include BB84 [12], B92 [11], SARG04 [101], six-state protocol [22], etc. In entanglement-based protocols, entangled photons are shared between Alice and Bob, where they independently measure their respective photons in randomly selected basis. Ekert91 [34] and BBM92 [13] are the two major examples of this type. Along with the two types of protocols, there also exist various others that are designed to enhance the performance of QKD from the perspective of experimental implementations. These protocols include coherent one-way (COW) [109], differential phase shift (DPS) [60], and many others.

In any QKD protocol, there are broadly two steps. The first one is the quantum process, where state preparation, transmission, and local measurement occurs. At the end of this quantum process, both Alice and Bob generate raw keys which are strings of binary 0s and 1s. The next step is the classical step, where classical communication is performed between Alice and Bob over an authentic (may be prone to eavesdropping) channel, and local operation is carried out based on the communications. This step includes sifting, parameter estimation, and privacy amplification. In the sifting stage, Alice and Bob publicly share their basis choices and consider only those events as part of the secure key when their bases are matched. In the parameter estimation process, they publicly disclose a randomly selected subset of the key; to measure the number of error bits parameterized as the quantum bit error rate (QBER). If the QBER value is less than a certain threshold value, then only the next step of error correction is performed on the undisclosed subset of the keys. Both the error corrected keys of Alice and Bob are identical, but may not be fully secure. To enhance security, privacy amplification is carried out where a shorter but

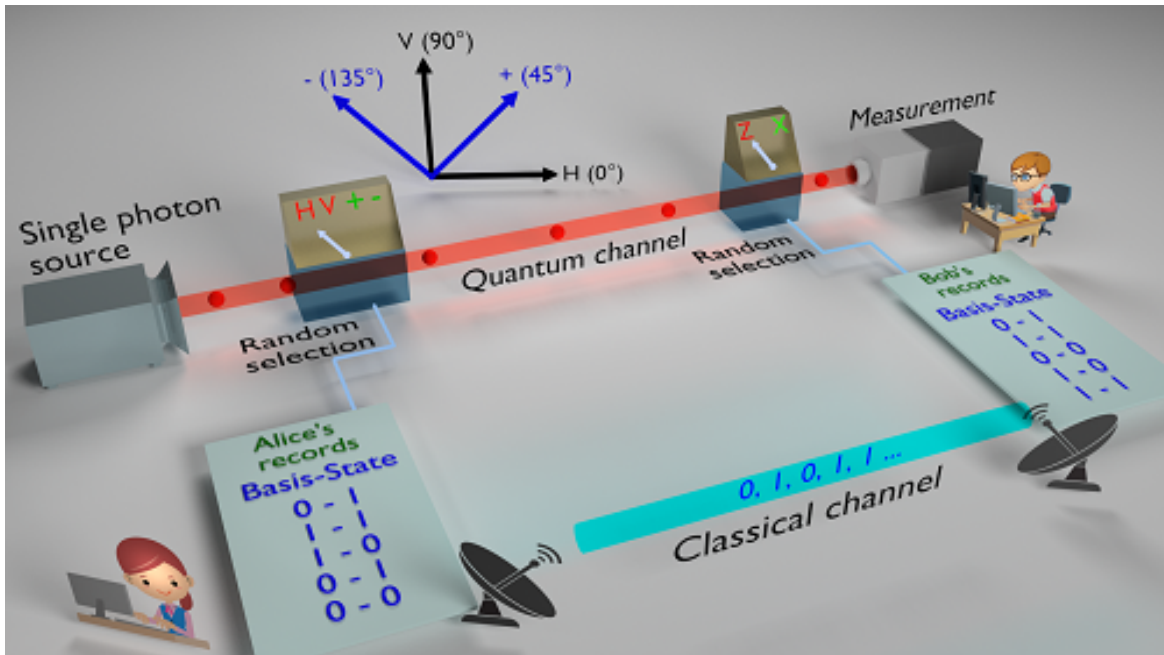


Fig. 4.1 Schematic of the BB84 protocol. Here, Alice prepares the polarization state for each photon, randomly from horizontal (H), vertical (V), diagonal (D), or anti-diagonal (A) polarization. Bob randomly selects the measurement basis from either X or Z basis. Bob shares this information of basis selection in a public classical channel once all the photons are transmitted and measured.

secure key is extracted from a larger key using a one-way hash function. Finally, at the end of the protocol, Alice and Bob can create identical and secure private keys among themselves.

4.3 BB84 and B92 protocol

Here we briefly describe two important prepare-and-measure-based protocols; BB84 (Charles Bennett, Gilles Brassard, 1984 [12]) and B92 (Charles Bennett, 1992 [11]). In the BB84 protocol, Alice sends a stream of single photons to Bob, where each photon's polarization is selected randomly from two possible bases, i. e. rectilinear and diagonal basis. Each basis has two orthogonal polarization states. For the rectilinear basis, these states are horizontal and vertical polarization states, whereas for the diagonal basis these are diagonal and anti-diagonal states. So, in total, Alice has to select randomly from four polarization states. For this, she requires two bits of true randomness. Both Alice and Bob have an agreement on the

encoding strategy for the four polarization choices.

After receiving each photon, Bob measures the polarization of each photon independently. For that, he chooses the polarization basis for each photon randomly from among rectilinear and diagonal bases and measures the polarization in that selected basis. To perform the aforementioned procedure, Bob requires one bit of randomness. In the sifting stage, Alice and Bob publicly disclose only their basis choices for each photon. Based on this information they discard those cases where their bases do not match. For example, they discard if Alice chose the rectilinear basis for state preparation, but Bob chose the diagonal basis for measurement on the same photon. As they both uniform randomly and independently choose their bases, the probability of basis mismatch is half. So, the rest half of the photons are part of the sifted key. The next step is to perform parameter estimation and post-processing on the sifted key.

A schematic of the BB84 protocol based on polarization encoding is presented in Fig. 4.1. Here, Alice first randomly selects the polarization basis from either rectilinear (assigned bit value 0) or diagonal (assigned bit value 1), then for each selected basis she randomly selects polarization state. So, in total Alice randomly selects between four possible polarization states for each photon coming from a single photon source; either horizontal (H), or vertical (V) or diagonal (D; $+45^\circ$ with respect to the horizontal polarization basis) or anti-diagonal (A; $+135^\circ$ with respect to the horizontal polarization basis) and sends it to Bob. She also records sequentially the assigned bit values to all the photons based on their basis and polarization state. Bob randomly selects his measurement basis to be rectilinear or diagonal. Bob also records his basis choices and measurement results sequentially. An example of the bit assignment scheme is provided in the table below, which is agreed upon between Alice and Bob and also can be shared publicly.

Polarization basis	Bit value
rectilinear	0
diagonal	1

Polarization state	Bit value
H	00
V	01
D	10
A	11

If an eavesdropper wants to know the polarization state information for each photon sent from Alice to Bob, she may perform an intercept-resend attack, where she measures the polarization state by randomly guessing the polarization basis (similar to Bob) and send different photon back to Bob which she encodes in the polarization state based on her measurement outcome. If she guessed the basis incorrectly, which happens half of the time, she sends back the wrong polarization state to Bob creating error bits with 50% probability. So, in total the eavesdropper generates 25% QBER, which can be easily detected in the parameter estimation stage.

In a standard B92 protocol [11] using polarization encoding, Alice sends Bob a stream of single photons, where the polarization state of each of the photons is randomly selected between any two non-orthogonal polarization bases, say, $|a\rangle$ and $|b\rangle$, where $\langle a|b\rangle \neq 0$. These two polarization states are encoded with binary 0 and 1, respectively. When these photons reach Bob, he randomly and independently selects between two projection operators $P_{\bar{a}} := (I - |a\rangle\langle a|)$ or $P_{\bar{b}} := (I - |b\rangle\langle b|)$ for each photon, and projects on it. Note that the operator $(I - |a\rangle\langle a|)$ always gives a null result when it operates on $|a\rangle$. Similarly, $(I - |b\rangle\langle b|)$ always gives a null result for $|b\rangle$.

$$(I - |a\rangle\langle a|)|a\rangle = |a\rangle - |a\rangle = 0, \quad (I - |a\rangle\langle a|)|b\rangle = |b\rangle - \langle a|b\rangle|a\rangle \quad (4.1)$$

$$(I - |b\rangle\langle b|)|a\rangle = |a\rangle - \langle b|a\rangle|b\rangle, \quad (I - |b\rangle\langle b|)|b\rangle = |b\rangle - |b\rangle = 0 \quad (4.2)$$

If Bob performs measurement $P_{\bar{a}}$ and gets non-null result, then he is certain that the input polarization state is $|b\rangle$, similarly for $P_{\bar{b}}$ measurement only $|a\rangle$ gives non-null result. For $\langle a|b\rangle = \frac{1}{\sqrt{2}}$, probability of non-null result is $\frac{1}{2}$. In the sifting stage, Bob only announces those events where he gets non-null results. Based on the announcement, Alice only considers

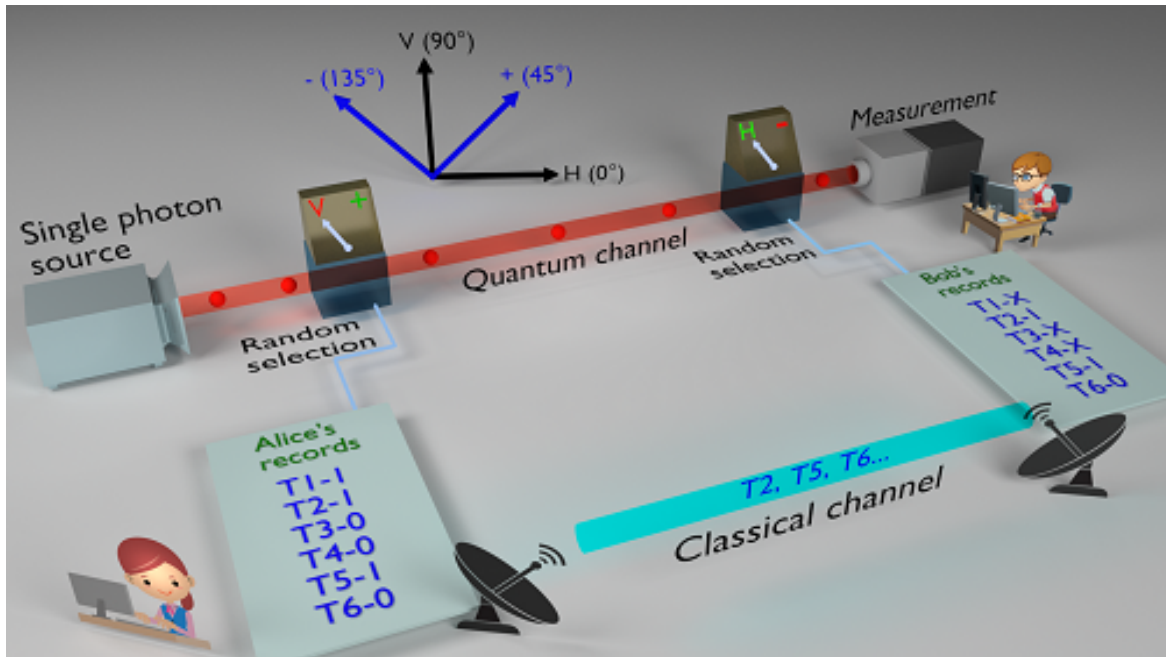


Fig. 4.2 Schematic of the B92 protocol. Here, Alice prepares the polarization state for each photon, randomly from either vertical (V) or diagonal (D) polarization. Bob randomly selects the measurement basis from either horizontal (H) or anti-diagonal (A) projection. Bob shares only the occurrence/timing of those events when he registers detection in his measuring device, in a public classical channel, once all the photons are transmitted and measured.

those events as part of her sifted key.

A schematic of the B92 protocol based on polarization encoding is presented in Fig. 4.2. Here, Alice randomly selects the polarization state for each photon coming from a single photon source to be either vertical (V) or diagonal (D; $+45^\circ$ with respect to the horizontal polarization basis) and sends it to Bob. She also assigns bit values to all the photons based on their polarization and records them sequentially (T1-1, T2-1, T3-0, etc.). Bob randomly selects his measurement basis to be horizontal (H) or anti-diagonal (A; -45° with respect to the horizontal polarization basis). Bob only considers those events where his measurements give positive (or non-null) results (T2, T5, T6, etc.) and announces only the occurrence (or timing) of these positive events in a public communication channel (that may be prone to eavesdropping), once all the photons have been received. Bob never shares the choice of measurement operations for these positive events. Based on the announcement, Alice only keeps those bits that generate positive events in Bob's setup. Thus Alice and Bob generate

and share an identical, secure key.

B92 protocol is similar in construction to the BB84 protocol, with only one modification; B92 requires only two non-orthogonal states as compared to the four polarization states used in BB84. This difference has one advantage in terms of the experimental implementation as it requires fewer resources (optical components, detectors, etc.) than the BB84 setup. However, there is a disadvantage in terms of security. It has been shown theoretically that the B92 protocol is less secure than the BB84 protocol. It is calculated that the threshold QBER value for BB84 is higher (14.6%) than the B92 (4.8%) [92]. One intuitive way to look at this issue is the eavesdropping strategy for the B92 protocol where the eavesdropper only resends photons to Bob in the 25% cases where she unambiguously knows the polarization states and sends nothing for the rest 75% cases where her measurement give ambiguous results. This strategy becomes very effective if the transmission channel is very long and lossy.

In this work, we demonstrate the B92 experimental setup instead of the BB84, for two reasons. The first issue is regarding the limited number of single photon detectors as well as other resources available at the time of the performance of the experiment. The second fact is that the modifications that we implement in the B92 setup are also applicable for the BB84 protocol, or any other prepare-and-measure-based protocol in general. There have been many experimental implementations of the B92 protocol prior to our work. All these experiments can be broadly categorized based on three classification parameters i.e. type of encoding, the medium of transmission, and type of source of photons. Though the original B92 protocol was based on phase encoding and many later experiments [19, 59] followed similar logic, a number of experiments have also been performed based on polarization encoding [23, 58, 79, 120]. In terms of the medium of transmission, there are experiments in free-space transmission channel [24, 15, 83] as well as fiber-based channel [51, 112, 79]. With respect to the type of source, interestingly, most of the experiments to date use weak coherent pulses (WCP) as single photons [45, 114, 59, 112], and only a handful of experiments have considered heralded single photons generated from spontaneous parametric down-conversion (SPDC) process [83, 120]. We have used heralded single photons generated

from a type-II SPDC process for the experimental demonstration of a B92 protocol mentioned in this chapter. Our choice of the heralded single photon source is based on the enhancement of the security aspects of the protocol, as will be discussed in the following sections. The photons have been encoded in polarization degrees of freedom and transmitted in a free-space channel inside a lab environment. Additionally, we have also developed a QKD simulation toolkit, qkdSim, that is able to predict the outcome of the B92 experimental demonstration, considering all realistic imperfections. Details of this simulation toolkit will be found in a thesis chapter written by my colleague, Rishab Chatterjee. Also, a detailed discussion on the complete work can be found in reference [26].

4.4 Experimental demonstration of B92 protocol

The experimental setup for the B92 protocol consists of three modules, i. e. heralded single-photon source, Alice-substation and Bob-substation. The schematic in Fig. 4.3 has details on both the photon source and Alice-module, whereas Fig. 4.4 provides the schematic of Bob-substation. The details of the individual modules will be discussed in this section.

4.4.1 Heralded single-photon source

The schematic in Fig. 4.3 has details on the components used in the single-photon source. A blue diode laser of wavelength 405 nm (Cobolt 08-NLD) pumps a PPKTP crystal continuously with 30 mW power. The polarization of the pump beam is kept horizontal (H), by using a half waveplate (HWP1). The PPKTP crystal is placed inside an oven (RAICOL), which is connected to a temperature controller. We find that at 40°C, photon pair generation is optimal for colinear, degenerate, type-II SPDC process in the crystal, wherein a horizontally polarized pump photon of wavelength 405 nm down-converts to a horizontally polarized signal and a vertically polarized idler photon, both with a peak wavelength at 810 nm. In order to maximize the photon pair generation rate, two lenses of focal lengths 100 mm (L1) and 50 mm (L2) respectively are used; L1 focuses the pump beam at the center of the crystal, and L2 is used to collimate the beam. Due to the colinear configuration, both photons in each pair traverse the same path as followed by the residual pump beam. A long pass filter

(F1), placed after the crystal, blocks most of the pump beam and allows only the red photons to go through. A band-pass filter (F2) allows only photons with a wavelength close to 810 nm to go through. A polarizing beamsplitter (PBS) separates the two photons in each pair, where ‘H’ polarized photon goes to the transmitted arm and ‘V’ polarized photon goes to the reflected arm of the PBS. A coupler (FC1), placed in the reflected arm, couples ‘V’ polarized photon to a single-mode fiber that is connected to a single photon avalanche detector (SPAD; COUNT-T-100). So, detection of a ‘V’ polarized photon heralds the ‘H’ polarized photon of the same pair. This is how heralded single photons are generated.

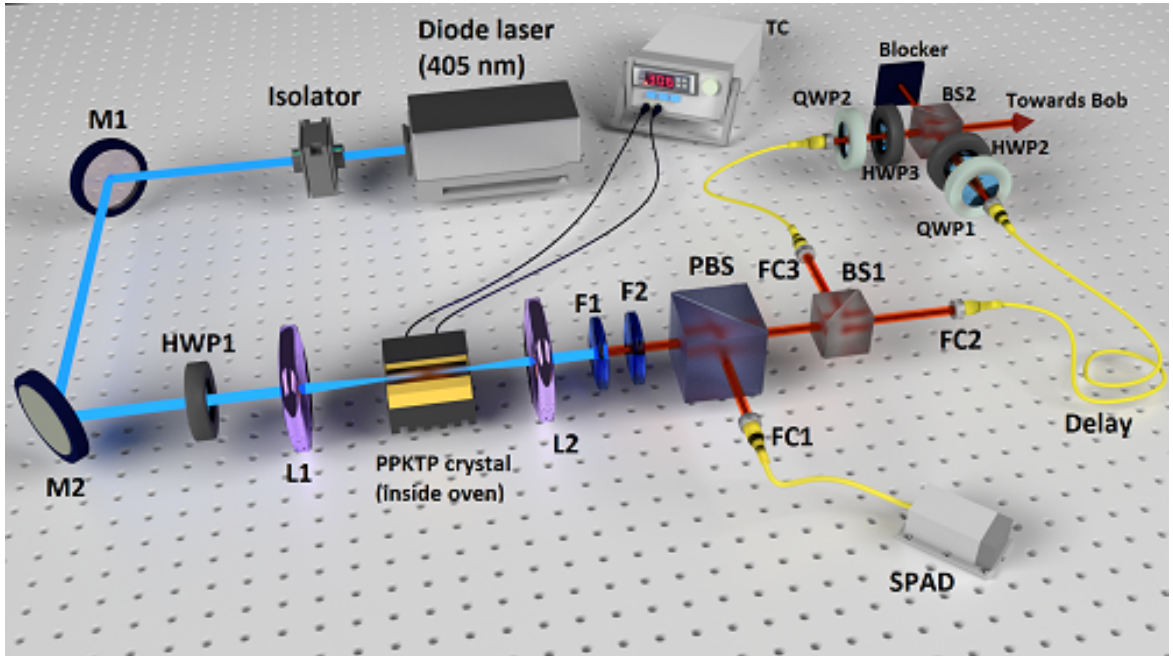


Fig. 4.3 Schematic of the heralded single photon source and Alice's module. **M1, M2**: dielectric mirrors; **HWP1**: half waveplate for pump light; **L1**: focusing lens; **L2**: collimating lens; **F1**: long pass filter; **F2**: band pass filter; **PBS**: polarizing beamsplitter; **FC1, FC2, FC3**: fiber couplers; **BS1, BS2**: 50-50 non-polarizing beamsplitter; **HWP2, HWP3**: half waveplates; **QWP1, QWP2**: quarter waveplates; **SPAD**: single photon avalanche detector; **TC**: temperature controller.

4.4.2 Alice-substation

The components after the PBS in Fig. 4.3 constitute the Alice-substation of the QKD implementation. Once each heralded single photon is generated, Alice randomly selects between

two non-orthogonal polarization states, vertical (V) and diagonal (D), by passing the photon through a 50:50 non-polarizing beamsplitter (BS1), whose transmitted arm has a HWP (HWP2) that rotates the input H polarization to D, and reflected arm has a HWP (HWP3) that rotates the input H polarization to V. Quarter waveplates (QWP2 and QWP3) are also placed along with HWPs, in order to minimize ellipticity in the polarization. The use of such a 50:50 BS for random selection gives us quantum randomness, which is necessary for the security aspects of the protocol. However, this comes with the caveat that Alice herself does not have knowledge about the polarization state of the photon that she sends to Bob.

In order to resolve this, we have come up with a fresh solution wherein Alice makes use of two known properties of SPDC, namely, the heralding process and the probabilistic nature of pair generation, where photon pairs are generated randomly in time. If Alice now randomly selects a subset from generated photon pairs and applies a fixed time delay to them, it becomes impossible for an eavesdropper to determine if the photon pair is from the selected subset or the rest, just by looking at the arrival time. So, Alice uses two single-mode fibers of different lengths in the two output arms of the BS1. Photons that traverse the transmitted arm and become “+45°” polarized later have a fixed time delay (Δt) as compared to photons that traverse the reflected arm and become “V” polarized. Alice also records the arrival time of each heralding photon detected in her detector using a time tagger (HydraHarp 400) connected to the detector. This is crucial in determining whether the corresponding pair photon is delayed or not before it is sent to Bob, and hence its polarization state. Thus, by introducing a time delay in the path of one of the photons and knowing the arrival time information of its partner photon (heralding arm), Alice is able to determine the polarization state of the photon that is sent to Bob. In order to remove any distinguishability in the spatial degree of freedom, outputs from both single-mode fibers recombine at another 50:50 BS (BS2), and only one output arm of the BS2 is used to send both “V” and “+45°” polarized photons to Bob.

4.4.3 Bob-substation

In Bob's part of the experimental architecture as shown in Fig. 4.4, a 50:50 beamsplitter (BS) is placed in the path of the incoming photons, where each photon has 50% probability to go to the transmitted arm and 50% to go to the reflected arm. In the transmitted arm of the BS, a polarizing beamsplitter (PBS2) is placed and a fiber coupler (FC2) collects any photon that transmits through the PBS and sends it to a single photon detector (SPAD2). So, in this arm, only "+45°" polarized photons have 50% probability to get detected while "V" polarized photons have 0% probability. In the reflected arm of the BS, a similar combination of PBS (PBS1) and fiber coupler (FC1) is placed with an additional half waveplate (HWP) just after the BS. This HWP converts D photons to V photons and similarly H photons to D photons. So, only the "V" polarized photons sent by Alice pass through the PBS and get detected in this arm with a probability $\frac{1}{2}$, but no "+45°" polarized photon is detected. So, to summarize, any detection in the transmitted arm of the beamsplitter definitely means that the photon is "+45°" polarized (assigned bit value 0), and any detection in the reflected arm definitely means that the photon is "V" polarized (assigned bit value 1). Similar to Alice, Bob also records photon time-stamping data from the two detectors at his end.

4.4.4 Post-processing via classical communication channel

In the post-processing stage, Bob only shares with Alice, his time-stamping data but does not provide the information regarding which time-stamping data has been recorded in which detector. So, Bob basically combines his two time-stamping lists generated from his two detectors, based on the sequence of recording, before sending it to Alice. As the basis selection done by Bob is completely random (quantum randomness), an eavesdropper cannot extract the information on the polarization state of each photon, just by looking at the combined time-stamps shared by Bob. Alice compares her time-stamping data with that of Bob and calculates the time-difference between all detected photon pairs. If, say the distance between Alice and Bob is L , then the time-difference between the two photons of each SPDC photon pair should be ideally $t_0 = L/c$ considering there is no additional delay introduced by Alice, where c is the speed of light. Alice applied some additional time delay Δt for his "D" (+45° polarized) photons. Which makes the time-difference $t_0 + \Delta t$. Alice considers only those

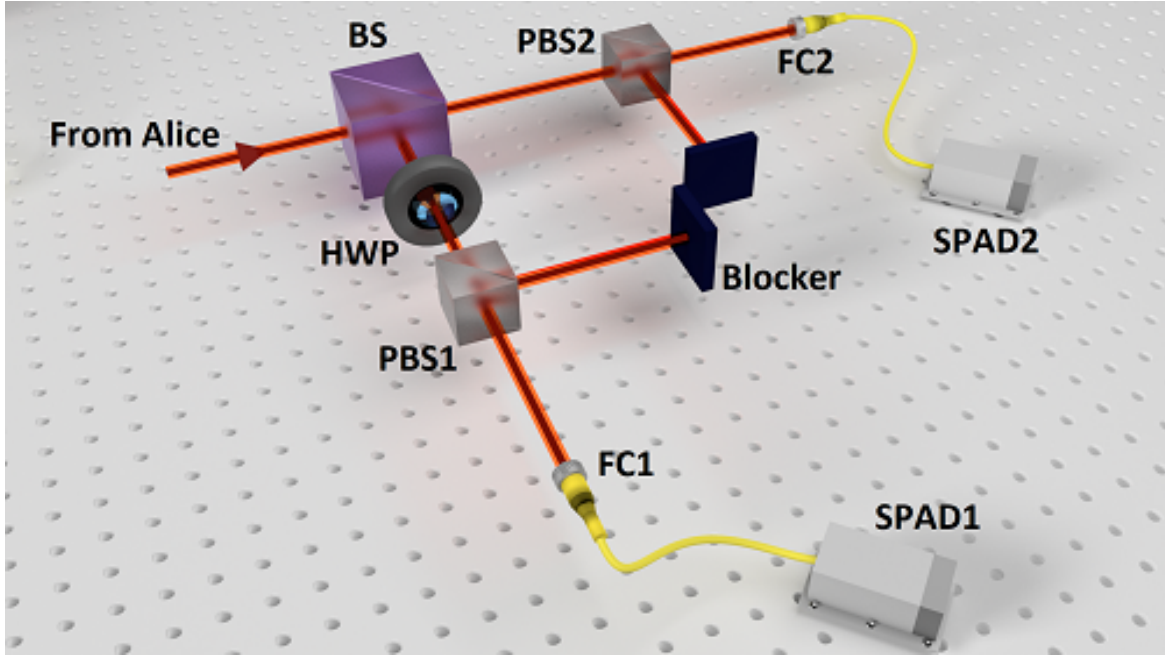


Fig. 4.4 Schematic of Bob's module. **BS**: 50-50 non-polarizing beamsplitter; **HWP**: half waveplate; **PBS1**, **PBS2**: polarizing beamsplitters; **FC1**, **FC2**: fiber couplers; **SPAD1**, **SPAD2**: single photon avalanche detector.

events where the time-difference is between $t_0 - W/2$ and $t_0 + W/2$ (W is a small coincidence time-window) as bit value 1 (in this case, Alice sent “V” polarized photons or non-delayed photons to Bob). For those events where time-difference is between $t_0 + \Delta t - W/2$ and $t_0 + \Delta t + W/2$, Alice assigns bit value 0 (“+45°” polarized photons or delayed photons were sent to Bob). In this way Alice prepares her key. Alice then sends back Bob's time-stamping data publicly, while omitting all those events/time-stamps that could not make it to Alice's final key. Based on this information, Bob can generate his final key.

We discuss here the importance of using heralded single photons in our implementation of the B92 protocol. Usage of ideal single photons (Fock state $|1\rangle$) is necessary for the purpose of security of the QKD protocol. In the case of multi-photons, an eavesdropper can apply photon-number-splitting (PNS) attack, where he/she keeps a part of the photon pulse for future measurement. One can experimentally check the photon-number distribution by looking at the anti-bunching property where the probability of generating two consecutive photons within the coherence time is negligible for ideal single photon states. One can

measure the normalized second-order coherence or $g^2(\tau)$ by performing a Hanbury-Brown and Twiss (HBT) type experiment (see Section 2.1.4). For an ideal single photon Fock state, $g^2(\tau = 0) = 0$. Heralded single photon generated from SPDC process behaves as a near-ideal single photon state, if the pump power is low and appropriate filtering (spatial and spectral) is applied.

In a real-world experiment, Bob's detection module also detects stray/background photons along with single photons that are sent by Alice. There are also various other sources of background noise, i. e. dark noise of the detector, electrical noise, etc. A single photon detector (SPAD) is unable to distinguish background noise photons from the signal photons. These noisy detections can increase the quantum bit error rate (QBER) in the generated key. Usage of heralded single photons in the experiment is advantageous for noise cancellation. In a SPDC based photon source, correlated photons are created in a pair. Detection of one photon (heralding photon) in each pair ensures the presence of the other photon (heralded photon). Therefore, in the post-processing stage, Alice and Bob only select those events where both detect one photon from the same pair (i.e. coincident events) and consider them as part of the signal. All the rest of the detected photons are considered as noise.

4.4.5 Characterization of the crystal temperature

In order to have some idea about the crystal temperature where the pair generation rate is optimal, we calculate the expected value of the temperature for an idealistic scenario using the procedure mentioned in detail in Section 2.2.3. For a collinear, degenerate, type II parametric down conversion inside a PPKTP crystal, we find that the crystal temperature for optimal pair generation is near 44.4°C . This value may change in the real experimental scenario. To pinpoint the exact crystal temperature, we measure the temperature directly from the experiment.

We scan the temperature of the crystal oven from the room temperature upto 45°C , by using the temperature controller. For each value of the temperature, sufficient time is given to stabilize the temperature within the crystal such that there is no temperature gradient.

We measure coincidences between the signal and the idler photon for each photon pairs generated from the crystal, by comparing the arrival times of the photon pairs detected in two separate single photon detectors. The coincidence time window is fixed such that the signal to noise ratio is reached the maximum. Fig. 4.5 shows the plot from the experimental data, where the X-axis is the crystal temperature and the Y-axis is the measured total coincidences accumulated over 10 seconds. We observe maximum photon coincidences near the crystal temperature at 40°C .

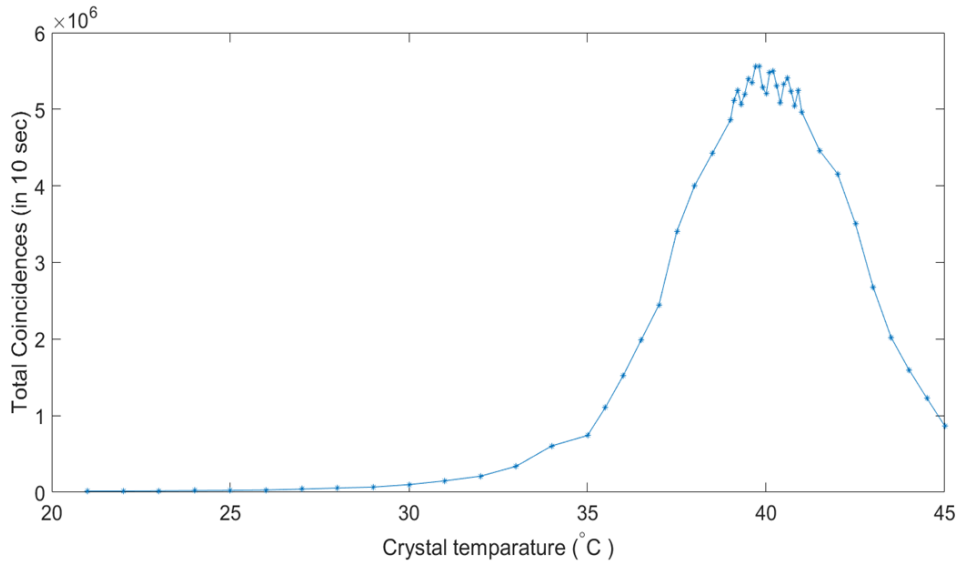


Fig. 4.5 Plot of coincidences vs the crystal temperature.

The slight deviation of the measured value of the crystal temperature from the calculated value can be attributed to various factors. The theoretical calculation involves all ideal parameters, whereas real parameters may differ in manufactured crystals. This optimal temperature is also sensitive to the crystal polling period, as well as the pump frequency (ω_p). So, any small change in those parameters can shift the optimal temperature value.

4.4.6 Pre-characterization of the polarization components

In this experimental demonstration of the B92 protocol, we encode different polarization states of single photons with binary 0 or 1. So, it is necessary to characterize and control the

polarization states of each photon, throughout the experiment. Otherwise, it will introduce a mismatch between Alice and Bob's sifted key, resulting in an increased bit error rate (QBER) that may violate the threshold value required to maintain the security of the B92 protocol. Here, the term "sifting" means the classical post-processing stage mentioned in Section 4.4.4.

In the pre-characterization stage, we tweak all the optical components responsible for the control of the polarization states of each photon, before performing the experiment. In the Alice-substation, she has to make sure that the photons going through the non-delayed fiber channel are converted to vertically (V) polarized, and the photons passing through the delayed fiber are converted to diagonal (D; $+45^\circ$) polarization, with maximum linearity. For this purpose, Alice places a half waveplate (HWP) and a polarizing beamsplitter (PBS) combination in the unused output arm of BS1. She also places a single photon detector (SPAD) after the PBS, in its transmitted arm. In the first step, Alice measures V polarization. She rotates the HWP and fixes it at 0° angle such that the HWP and PBS combination performs the horizontal projection operation ($|H\rangle\langle H|$) in the transmitted arm, where the detector is placed. She blocks the longer fiber (delayed) arm and tweaks QWP2 and HWP3 such that the coincidence between this detector and the heralding detector is minimum. In the most ideal scenario, when Alice prepares all photons into V photons with perfect polarization extinction, the coincidence count should be zero. However, in reality, there will be some ellipticity and fluctuations due to realistic imperfections in the polarization optics as well as the background noise leading to near-zero coincidence counts. So, the aim is to minimize the coincidence counts as much as possible just by tweaking the QWP2 and HWP3. In the next step, Alice prepares D polarization in the delayed fiber arm, and she makes the measurement basis in -45° polarization ($|-\rangle\langle -|$). She blocks the non-delayed arm and tweaks QWP1 and HWP2 such that the coincidence between this detector and the heralding detector is minimum.

In Bob-substation, a half waveplate (HWP) can be placed before the BS to correct any mismatch between the reference frames of Alice and Bob. When they are separated over a longer distance or the relative distance between them is changing with time, the two reference frames can be considered moving independently, hence countermeasure is necessary to ensure

reference frames matching for all time. For this purpose, Alice uses reference light pulses of fixed polarization (let's say horizontal) and different wavelength other than the signal wavelength and sends the reference pulses along the same transmission channel. If the reference frames mismatch occurs, then all the polarization states rotate at some fixed angle, including the reference pulse. So, in Bob-substation, we can separate out the reference pulse from the signal pulse (using a dichroic mirror) and monitor this rotation angle of the polarization. We can rotate the HWP placed in front and actively correct the angle as the experiment goes on. All signal photons automatically get polarization correction as they also pass through the same HWP. In our case, however, we have not incorporated such active polarization correction, as both the Alice and the Bob substations are fixed on a single optical table with a distance of around 2 meters and experience no such mismatch between their reference frames.

4.4.7 Data analysis

In the data processing stage, three parameters are measured in order to comment on the performance of the B92 QKD experimental setup. These parameters are the following: average key rate, quantum bit error rate (QBER), and asymmetry/symmetry of the key.

We first measure the average number of bits in the sifted key, generated per second. In the B92 protocol, sifting refers to the post-processing stage, where Alice and Bob select only those events where both of them records simultaneous detection or coincidence detection. Ideally, Alice and Bob should have identical keys after the sifting stage; in the absence of any channel-noise and eavesdropping activity. In reality, various channel noises introduce errors between the two keys, which we measure by computing the QBER value. We calculate the number of error bits by comparing each bit value at the same bit position in the two keys. The ratio of the number of error bits and the total key length gives the QBER. Key asymmetry (or symmetry) denotes the disparity between the number of 0 and 1 bits in the final error-free key shared by Alice and Bob.

To measure the average key rate, we run the B92 protocol for 10 seconds and iterate the same for 20 times. The final key rate is the average value over the 20 key length values, divided by 10 seconds. In order to find the minimum runtime of each experiment (while the iteration is fixed at 20) necessary for the averaging process, we collected data continuously for a longer time duration (in this case, 100 seconds) and applied the bootstrapping method. We obtain the standard deviation (SD) by mean (M), i.e. SD/M plot (see Fig. 4.6) as a function of the runtime for 20 iterations. We found that the SD/M value for 10 seconds runtime is 0.016%, which is sufficiently small for the averaging procedure. So, we continue the data-taking process for 20 iterations and for 10 seconds at each iteration.

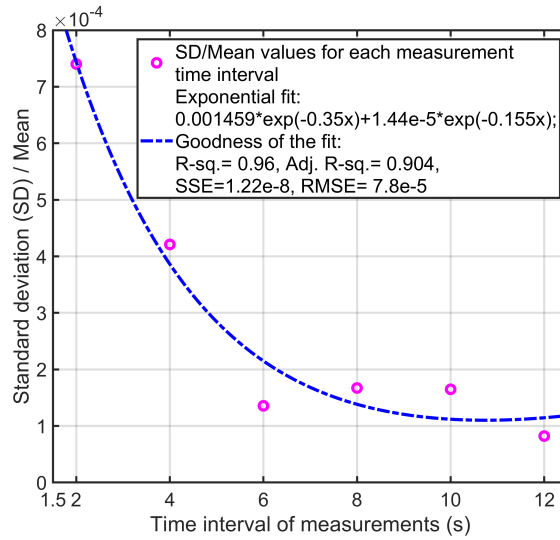


Fig. 4.6 Bootstrap analysis (SD/Mean of key rate) plot on a 15 seconds dataset from a series of 20 measurement runs. Here each run consists of 10000 iterations. The saturation or convergence effect is supported by the exponential fit to the simulated data-points. The goodness of the fit is guaranteed by the low values for sum-of-squares error (SSE) and root-mean-square error (RMSE) as well as close to 1 values for R-squared (R-sq.) and adjusted R-squared (Adj. R-sq.).

In order to report the key length, QBER, and asymmetry value from each data set, we implement two types of optimization strategies, namely A & B, for each and every data set. In both the strategies, Alice and Bob first compare their recorded time-stamping data and plot the coincidence graph as a function of the time difference between the two. We show a

representative coincidence graph in Fig. 4.7, where we can observe two distinct coincidence peaks due to the 10 ns time delay introduced by Alice in one of the arms in her setup (see Fig. 4.3). The first peak (blue line) represents those coincidence events where Alice sent a non-delayed or “V” polarized photon and Bob measured the polarization in the correct basis ($|-\rangle\langle-|$ projection). The second peak (red line) represents those coincidence events where Alice sent a delayed or “+45°” polarized photon and Bob measured the polarization in the correct basis ($|H\rangle\langle H|$ projection). The wing of the red line under the blue curve represents those events when Alice sent a “V” photon and Bob measured in the wrong basis ($|H\rangle\langle H|$ projection), but still got detection; due to the noise introduced by the optical components and the transmission channel. Likewise, the wing of the blue line under the red peak represents those events when Alice sent a “+45°” photon and Bob measured in the wrong basis ($|-\rangle\langle-|$ projection), but still got detection. We place some time window around both the peaks (W_{l1} to W_{r1} , and W_{l2} to W_{r2}) and calculate the area under the curves. The sum of the total area under the blue and the red curve within their consecutive time windows represents the value of the key length. The sum of the total area under the red line from W_{l1} to W_{r1} , and the blue line from W_{l2} to W_{r2} represents the number of error bits, which is used to measure the QBER value. So, referring to the schematic shown in Fig. 4.7, we define the three parameters, i. e. key rate, QBER, and key symmetry, as the following:

$$\text{key rate} = \frac{\text{signal part} + \text{noise part of both the curves}}{\text{runtime of the protocol}} (\text{Hz}), \quad (4.3a)$$

$$\text{QBER} = \frac{\text{noise part of both curves} \times 100}{\text{signal part} + \text{noise part of both the curves}} (\%), \quad (4.3b)$$

$$\text{key symmetry} = \frac{\text{signal part of either curve} \times 100}{\text{signal part of both curves}}. \quad (4.3c)$$

For a binary key length of N , there are 2^N set of possible key strings. In order to get unconditional security (in case of one-time-pad (OTP) or private key encryption) any key string generated among the 2^N possibilities should be uniformly random, i. e. the probability of obtaining any key string should be $\frac{1}{2^N}$. If this ideal case is to be realized in the experiment, then all the optical components used in the setup should behave ideally, i.e., symmetric (50 : 50) beamsplitter has exactly 50% probability of transmitting or reflecting the photon,

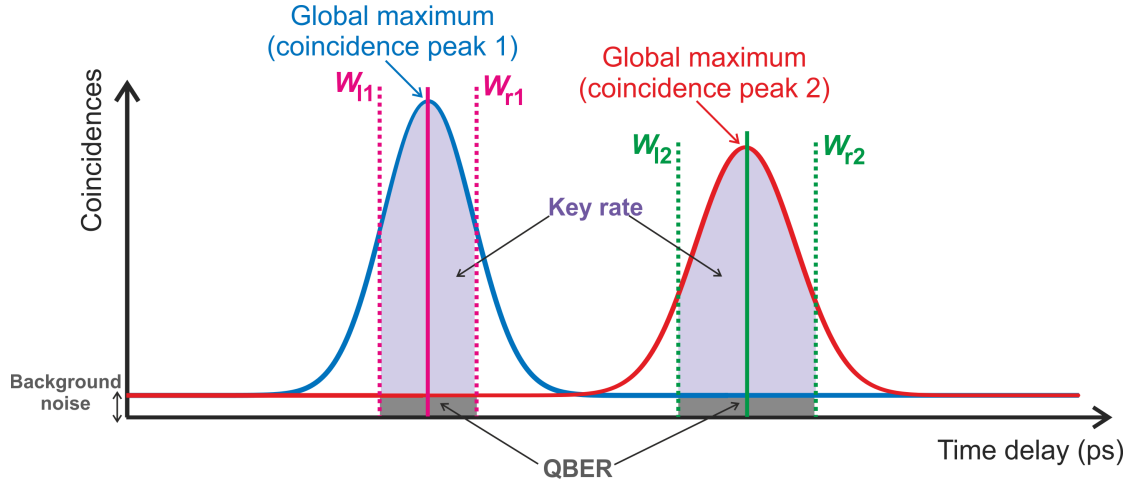


Fig. 4.7 A simplified schematic of the output of two independent coincidence detection: Alice and Bob's **R** basis (coincidence peak 1 in blue) versus Alice and Bob's **D** basis (coincidence peak 2 in red). The background noise zone indicated below the flat portions of the blue and red curve represents the unwanted coincident detection from stray light sources, uncorrelated signal & idler photons, leaked pump photons, and dark noise of the photodetector. The symbols $W_{l1(2)}$ and $W_{r1(2)}$ represents the left and right markers of the time window around the maximal coincidence point for coincidence peak 1 (2). The total coincidences within the chosen window around the central maximum from both curves contribute to the error-free "key rate" (or signal - marked in purple); while those within the background noise zone contribute to the "QBER" (or noise - marked in grey). Note that in reality, the coincidence curves are not typically smooth functions and contain a lot of kinks (local optimal points) around a central global maximum.

all single-photon detectors have equal efficiency, etc. In this case, both coincidence peaks (blue and red peak) would be identical; leading to the average number of 0 bit and 1 bit being same in the final key (or perfect key symmetry). However, in reality, the two peaks are in general asymmetric. In order to investigate this, we generate a large number of key strings and find that the ratio of 0's and 1's in all of them are different than the ideal value of 50:50. We predict that one of the reasons for this asymmetry could be the mismatch in detection efficiencies between the two detectors used in Bob's module. We interchanged the detectors and still observed same asymmetry between the keys. From this observation as well as other independent tests, we conclude that both the detectors used in Bob's module have similar efficiency. This indicates that the cause of asymmetry is present even before the detectors, mostly the asymmetric splitting ratio of the beamsplitter and other optical components (optical fibers, waveplates, etc.) placed in Bob's module. If all the devices used

in the setup behaves ideally, we would have obtained a binomial distribution of the number of 0's (or 1's) peaked at exactly half of the key length.

We observed, from experiment, that the average value of the ratio of 0's and 1's varies from $57.59 \pm 0.29 : 42.41 \pm 0.29$ to $51.49 \pm 0.32 : 48.51 \pm 0.32$. An eavesdropper may take advantage of this bias in the final key; unless a commensurate step to mitigate this is applied in the post-processing stage. In this work, along with QBER, the effect of key asymmetry in the key string is also addressed with respect to the security of the QKD protocol.

As mentioned earlier, we have implemented two different optimization strategies: "A" and "B" (refer to Appendix B for the detailed procedure of the two strategies) to counter the asymmetry in the final key strings. In both the optimization strategies, we aim to keep the QBER value below a certain threshold. On Addition to that, strategy A addresses the biasing issue by controlling the asymmetry in the key bits; while strategy B only enhances the signal-to-noise (SNR) ratio, without bothering about the asymmetry. As optimization A performs this additional compensation on the key string, it produces a slightly lower key rate than optimization strategy B. Nevertheless, both the optimization strategies have their advantages and disadvantages which will be discussed next.

In the optimization algorithm A, we find the position of W_{l1} , W_{r1} , W_{l2} , and W_{r2} (as shown in Fig. 4.7) or the values of two time-window, for each key string, such that the three conditions are satisfied: key length is maximum, QBER value is below the threshold value (4.8%) [92] and the ratio of 0's and 1's is exactly 50 : 50. However, this strategy also introduces some additional bias as it imposes a fixed ratio of 50 : 50 for all key strings, rather than a binomial distribution peaked at 50 : 50. This change increases eavesdropper's guessing probability to $(\frac{N}{2}!)^2 / N!$, rather than the ideal guessing probability for a uniformly random distribution, that is $\frac{1}{2^N}$. So, the biasing issue still remains in optimization A, only the source of the biasing changes. Also, in order to maintain the key-symmetry, the coincidence windows have been re-adjusted (as discussed above), which leads to the deletion of few additional raw bits,

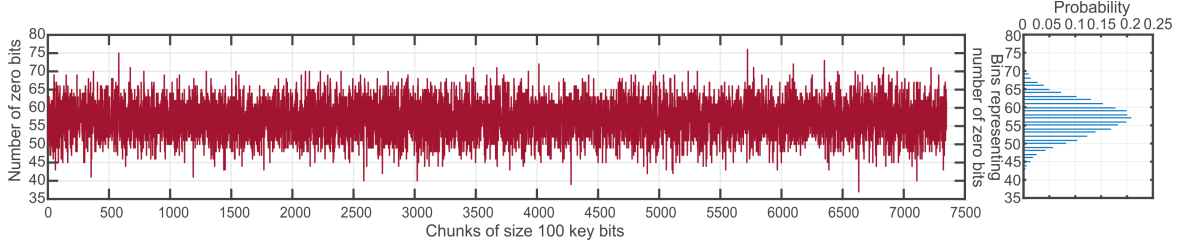
leading to the reduction of the final key length.

Another interesting point regarding the optimization strategy A is the fact that although the key is made symmetric with appropriate re-adjustment of the coincidence windows, the signal-to-noise ratios for both the peaks may be different. In that scenario, an eavesdropper may find a strategy to gain some additional information about the final key. To counter this, one may modify strategy A as follows. We can put more restrictions on the individual QBER obtained from the two separate peaks. Instead of the condition of the overall QBER being less than or equal to 4.8%, we can restrict both the $\text{QBER} \leq 4.8\%$, while at the same time maintaining the key symmetry with optimal key length. This modification however reduces the length of the final achievable key length due to the more stringent condition on the QBER, while at the same time enhancing the security of the protocol. Note that all the strategies mentioned above are based on our intuitive understanding of the various possible eavesdropping procedures and a qualitative measure to nullify any advantage that the eavesdropper may possess due to the bias introduced by the experimental setup. In this regard, a rigorous quantitative theoretical study of the effect of key asymmetry on the security of the protocol can be useful. However, it is beyond the scope of this thesis work. Hence, we provide various post-processing or optimization strategies to limit the eavesdropping activity targeting the experimental imperfections.

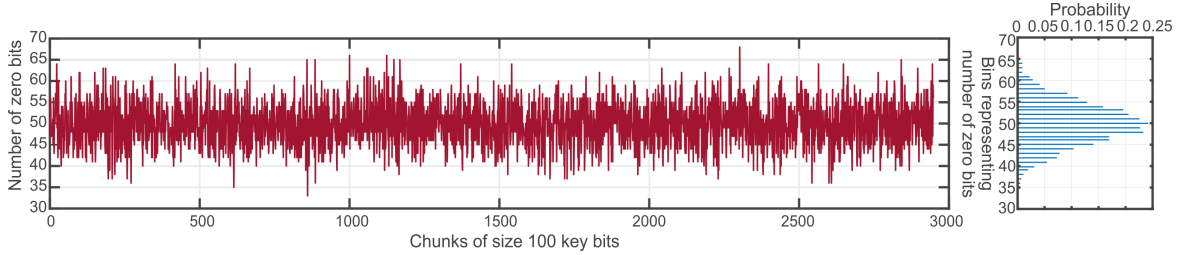
In strategy B, we also optimize the four markers of the time windows such that the three conditions are satisfied, which are slightly different than what we considered in strategy A. These conditions are the following: key length is maximum, QBER value is below the threshold value (4.8%) and the lengths of the two time windows ($(W_{r1} - W_{l1})$ and $(W_{r2} - W_{l2})$) are exactly same. This strategy does not put any restriction on the symmetry of the key, however, one advantage of the equal time window is that the eavesdropper will not be able to apply any eavesdropping strategy exploiting the asymmetry of the window size. Another advantage is that the key length increases in strategy B, as there is no forced deletion of some bits for maintaining the key symmetry.

We compare the optimized key strings (generated from the two optimization strategies, A and B) with the unoptimized one in Fig. 4.8; in order to understand their differences. For this analysis, we consider only one representative data among the twenty, which is measured using 30 mm crystal during the daytime. We show only the distribution of the number of 0 bits, however, the conclusion is equally valid for the number of 1 bits. In the first case (Fig. 4.8a), we show the distribution of zero bits obtained from the unoptimized key strings while fixing a 3 ns time-window around both the coincidence peaks. The reason for choosing 3 ns window is that it covers nearly all of the peak region, providing good signal to noise ratio. This approach being an unoptimized one, produced an error-free key rate of about 73.6 kHz, at the expense of a QBER of 7.27%. The obtained error-free key rate can be inferred from the red subplot on the left, where each value on the x-axis contains 100 key bits of the generated key string. The blue histogram subplot on the right illustrates that the distribution of zero bits in the key string is indeed a binomial peaked at 57.09, indicating that the ratio of 0 to 1 bits is quite asymmetric. More particularly, when we bin the key bits into sets of 100 over the entire key string, then we find that the probability of obtaining a key symmetry of approximately 57 : 43, becomes the maximum, within those bins. This also validates our earlier claim that the distribution of key bits, in general, can possess asymmetric peak values ranging as high as 57.59 ± 0.29 (averaged over 20 datasets). In the next two cases, we contrast the unoptimized analysis against those obtained with the two optimization strategies: A and B. More specifically, in Figs. 4.8b and 4.8c, similarly, we report the corresponding distribution of zero bits in the key strings that were generated using the optimization strategies A and B, respectively. From a comparative perspective, we can observe that in Fig. 4.8b the peak of the binomial distribution occurs at 49.95, i.e. the most probable case is free from any significant bias; while in Fig. 4.8c a considerable bias (or asymmetry) exists for the peak of the distribution being at 55.91. It is important to note that the distribution of the zero bits in the generated (error-free) key string for strategy A, in this analysis, comes to be a binomial distribution instead of the otherwise expected delta function peaked at about 50:50, since in the said algorithm we are optimizing the key symmetry over the entire string and not over

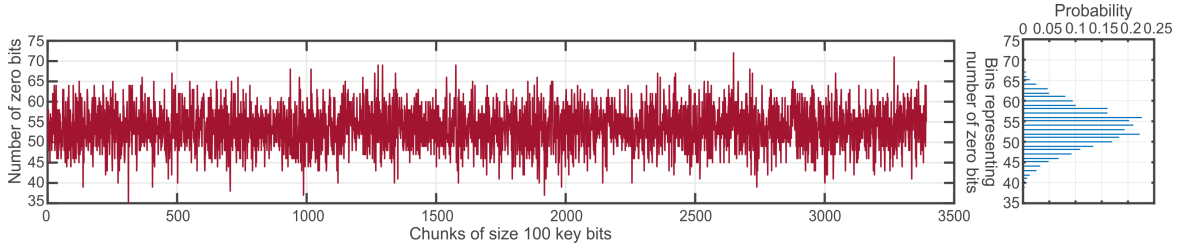
the individual chunks being plotted here.



(a) For the error-free key string generated with unoptimized time windows of 3 ns duration around both coincidence peaks. The highest peak of the binomial distribution on the right is at 57.09.



(b) For the error-free key string generated with time windows optimized using strategy A. The highest peak of the binomial distribution on the right is at 49.97.



(c) For the error-free key string generated with time windows optimized using strategy B. The highest peak of the binomial distribution on the right is at 55.91.

Fig. 4.8 Distribution of zero bits in the error-free key string obtained with three different strategies: (a) unoptimized, (b) optimized via strategy A, and (c) optimized via strategy B. For all strategies, the left plot represents the number of zero bits present in sequential chunks of size 100 key bits within the key string, and the right plot displays the corresponding histogram of the frequency of zero bits found within those chunks (bins). The key bits plotted on the left plots were collected over a measurement time of 10 seconds. This representative analysis was performed on one of the 20 datasets measured during the daytime with the 30 mm crystal.

For strategy B, being free from the imposition of any symmetry constraint on the ratio of 0's to 1's bits in the optimized key string, there occurs no increase in Eve's guessing probability unlike that found in strategy A. However, strategy B suffers from possible infor-

mation leakage to Eve due to the existing bias arising from asymmetry. In [44], the authors have shown how any possible security loophole due to detector efficiency mismatch can be mitigated by including relevant steps in the privacy amplification part of the post-processing algorithm, thus ensuring that such a bias can also be accounted for, enabling a secure reconciled key. In our example, the mismatch that happens due to the effective asymmetry present in our optical components can also be recast into a similar detection efficiency mismatch problem, thereby enabling a secure reconciled key as has been shown in [44]. It would be an interesting open problem to see how modifications could be made to privacy amplification algorithms to account for the possible security loophole posed by optimization strategy A.

We would like to remark here that while the symmetry aspects bring about different security implications as discussed above, the objective of our work has been to model practical QKD as accurately as possible, while constraining the QBER below the known security threshold for the given protocol and not comment on any detailed security analysis of the said protocol. In the current B92 implementation, we have thus constrained the QBER to be below 4.8% [92] in both optimization strategies that we have implemented.

4.4.8 Advantages of the modified setup

We have introduced various modifications to the conventional B92 experimental setup; in order to enhance the security of the protocol. An eavesdropper can attack any prepare-and-measure based protocol like B92 in the three stages of the experimental implementation; Alice's preparation module, transmission channel, and Bob's detection module. Here, we discuss how our B92 setup is tolerant to the various eavesdropping attacks at these three stages.

In the preparation stage, an eavesdropper primarily attacks the random basis selection device used by Alice. For the security of the protocol, Alice needs to use true randomness while selecting the polarization basis for each photon. However, in reality, a true random number generator is difficult to prepare with current technology. Instead, computer-generated

pseudo-random numbers are being used which makes the protocol vulnerable in presence of an all-powerful Eve. A better strategy that is being used nowadays is to generate quantum random numbers by harnessing the inherent randomness in quantum mechanics, which is able to generate true randomness. There are two issues with this strategy; the first one is due to the scenario where an eavesdropper acts as the manufacturer of the random number generator and performs a device-attack where he/she has knowledge of the random numbers that are being generated. The second issue comes with a very well-known attack called Trojan-horse attack [48] or large-pulse attack [113] where an eavesdropper sends intense laser pulses towards the apparatus of Alice and Bob, and learn about the settings of various devices by simply analyzing the attenuated laser pulses back-reflected from the surface of these devices. In case Alice actively prepares the polarization state for each photon by controlling the polarization device (for example, a half waveplate or a polarizer) based on the random seed of any true random number generator, Eve can learn about the settings, each time, from the back-reflected laser pulses. In our setup, we are generating quantum randomness inside Alice's module itself, instead of using any external device from a potential malicious manufacturer. Also, we have used a passive selection of random basis rather than active selection, so Alice does not control any polarization device and hence Eve cannot learn any additional information by applying Trojan-horse type attacks.

In the transmission channel, an eavesdropper can apply a photon-number-splitting (PNS) attack where pulses containing multiple photons are split into two and Eve keeps one photon to herself (keeps in a quantum memory) for future measurement and sends the rest of the pulse to Bob. At the sifting stage when Alice and Bob publicly share their basis choices for each pulse, Eve can then measure those photons in the appropriate basis and learns about the key without introducing any additional error. To counter this attack we use heralded single photons from an SPDC based source, whereas using the heralding property as well as using low pump power and tight spectral filtering we have significantly reduced the generation of multi-photon pulses.

In Bob's detection module, we continuously run the single-photon detectors throughout the experiment, rather than fixing a time window for detection. This change makes the protocol more tolerant to the timing jitter introduced by the transmission channel. Uncontrollable timing jitter produces various time delays in the photons collected in Bob's detectors. In the case of a fixed detection time-window, some photons may not be detected if the time-delays are larger than the detection time-window. An eavesdropper can use this phenomenon to her advantage where she manipulates the transmission channel (or time-delays) and makes different photons detected (or non-detected) in specific detectors as she wants. This type of attack is called time-shift attack [122]. Our modified setup is tolerant to this attack as we do not use fixed detection time-windows for the detectors. Also, the post-processing and data analysis strategies mentioned in Section 4.4.7 are advantageous in terms of noise tolerance. Here we can change the coincidence window sizes (see Fig. 4.7) for each data set such that we get a maximum key rate with lower QBER (below the threshold value). In the presence of high background noise, we can still extract a smaller but secure key; by reducing the window sizes.

4.5 Results and discussion

We present here the results of the B92 experiment, where the measured value of the key rate, QBER and key symmetry obtained by using optimization strategy A and B is shown in Tables 4.1 and 4.2 respectively. All three measured quantities are the averages over 20 iterations of the experiment, whereas for each run of the experiment, dataset has been recorded for 10 seconds. The quoted error value provided along with the average value is the standard deviation of the distribution of 20 datasets. The choice of 20 iterations as the suitable number of runs for the experiment is obtained from a bootstrapping analysis already discussed in Sec. 4.4.7. Tables 4.1 and 4.2 also provide experimental results for two separate PPKTP crystals of different lengths, i. e. 20 mm and 30 mm; for comparison. For each crystal length, experiments have been performed both in the day-time and night-time condition inside the lab.

In Figs. 4.9 and 4.10, we exemplify the distribution of the key rate, QBER, and key symmetry values corresponding to a range of coincidence window sizes, considering a

Crystal length (mm)	Time of the day	key rate (kHz)	QBER (%)	symmetry
20	Day	47.6 ± 0.6	4.79 ± 0.01	49.82 ± 0.01
	Night	51.0 ± 0.5	4.79 ± 0.01	50.15 ± 0.02
30	Day	33 ± 2	4.78 ± 0.01	50.07 ± 0.02
	Night	36 ± 3	4.78 ± 0.01	50.08 ± 0.02

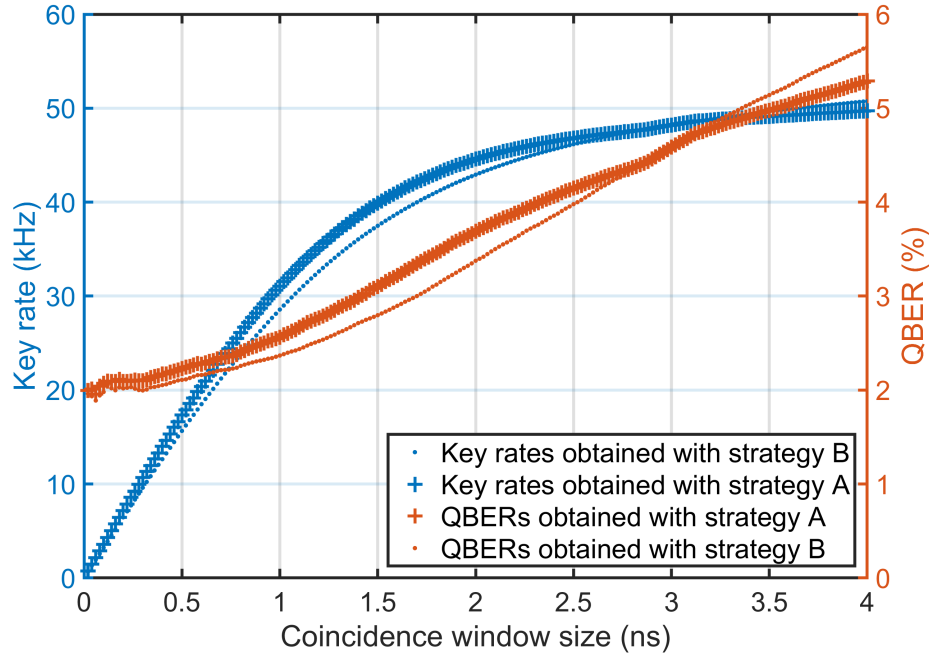
Table 4.1 Experimental results using optimization strategy A. Average key rate, QBER, and key asymmetry value are obtained for two separate PPKTP crystals of different lengths and for both day-time and night-time conditions. Here, the symmetry value “x” denotes that the ratio of the number of 0s to the number of 1s in the key is x:(100-x).

Crystal length (mm)	Time of the day	key rate (kHz)	QBER (%)	symmetry
20	Day	47.8 ± 0.6	4.79 ± 0.01	50.2 ± 0.3
	Night	53.8 ± 0.4	4.79 ± 0.01	53.7 ± 0.3
30	Day	36 ± 2	4.79 ± 0.01	54.0 ± 0.3
	Night	38 ± 3	4.78 ± 0.01	54.1 ± 0.4

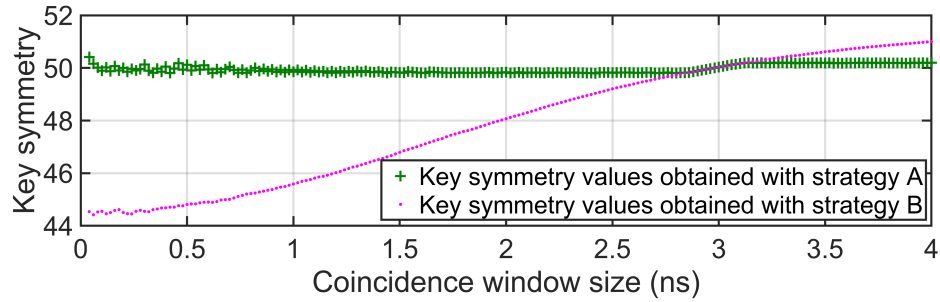
Table 4.2 Experimental results using optimization strategy B. Average key rate, QBER, and key asymmetry value are obtained for two separate PPKTP crystals of different lengths and for both day-time and night-time conditions. Here, the symmetry value “x” denotes that the ratio of the number of 0s to the number of 1s in the key is x:(100-x).

representative daytime dataset (chosen from those 20 measurement sets), for both crystals of length 20 mm and 30 mm respectively. More particularly, in both figures, we vary the coincidence window size (i.e. the gap between W_{11} and W_{r1} or W_{12} and W_{r2}) in steps of 10 ps from the global maximum point (shown in Fig. 4.7) and then use two unoptimized strategies: A and B, that are slight variations to the optimization strategies presented in Appendix B. In the unoptimized strategy A, we calculate the key rate (plotted with blue “+” symbol) for the (unrestricted) QBER (plotted with red “+” symbol) corresponding to each size of the coincidence window, while ensuring that the key symmetry remains 50:50 (approximately). This is done by slightly re-adjusting the coincidence window size on the coincidence peak 2 (i.e. the positions of windows: W_{12} and W_{r2}). Thus, it can be observed in Figs. 4.9b and 4.10b that the distribution of key symmetry (marked with green “+” symbol) remains 50 over the whole range of coincidence window sizes. In the unoptimized strategy B, we only slightly deviate from its optimized strategic version, by calculating the key rate (plotted with

blue dots) for the (unrestricted) QBER (plotted with red dots) corresponding to each size of the coincidence window; however, in this case, apart from removing the threshold on QBER values, we also relax the 50:50 constraint on the key symmetry. For this strategy, the corresponding variations in key symmetry values are shown in Figs. 4.9b and 4.10b with pink dots. We can observe that in strategy B, for the two coincidence peaks (1 and 2) being asymmetric (in height and width) and also slightly skewed due to realistic imperfections, the key symmetry keeps constantly decreasing in a given direction over the range of coincidence window sizes. Intuitively, in both Figs. 4.9a and 4.10a, the key rate and QBER values are directly proportional to the size of the coincidence window, as they result from the area under the curve estimates depicted in Fig. 4.7. In Fig. 4.10a, the key rate and QBER values grow more steeply compared to that in Fig. 4.9a, since both pair production rate and background noise is higher for the longer crystal of 30 mm. This is because we do not focus our Gaussian pump beam very tightly to ensure that we achieve a good heralding ratio [3]. Also, we note that towards the larger sizes of the coincidence window, the growth of the key rate reduces and becomes sub-linear, compared to the linearity of the slope for the QBER distribution, since at those points the coincidence window span has expanded and entered the flat zone where the background noise is increasing more rapidly than the SNR. Most importantly, we observe that beyond a certain choice of coincidence window size the information-theoretic QBER threshold of 4.8% [92] for the B92 protocol gets violated for both crystals, reaching up to ≈ 88 kHz key rate with $\approx 8.9\%$ QBER in Fig. 4.10a and up to ≈ 50 kHz key rate with $\approx 5.7\%$ QBER in Fig. 4.9a. Lastly, we observe that the key rate values corresponding to 4.8% QBER in Fig. 4.10a for the shorter crystal and Fig. 4.10b for the longer crystal is around 48 kHz and 34 kHz respectively; along with the fact that the key rate curve for strategy B shoots above that for strategy A in Fig. 4.10b, unlike that in Fig. 4.10a where they actually overlap. These observations help us to infer that the optimization results presented in Tables 4.1 and 4.2 are well in agreement with these unoptimized results. These results also bring out the importance, utility, and performance analysis of the optimization methods that have been introduced in this thesis chapter.

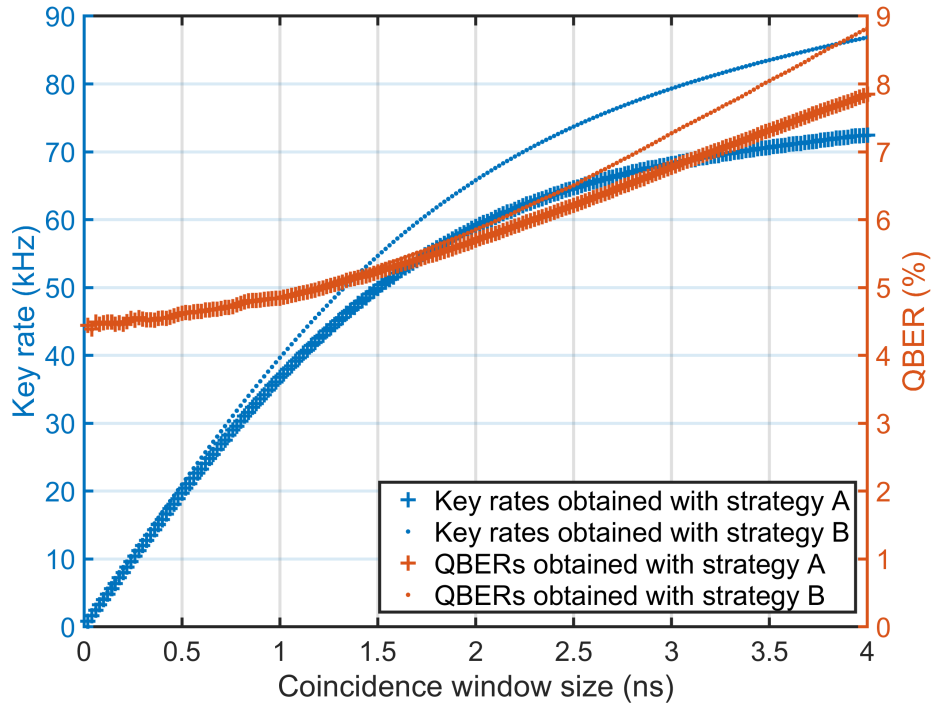


(a) Plot showing the distribution of key rate and QBER values for varied sizes of coincidence window obtained using unoptimized versions of the strategies A and B.

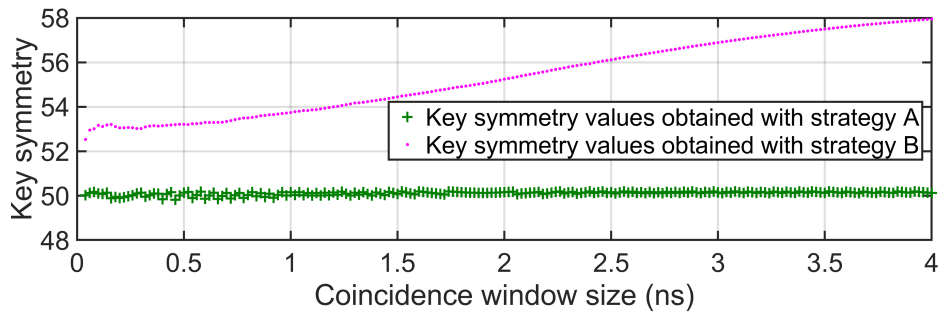


(b) Plot showing the distribution of key symmetry values corresponding to the varied sizes of coincidence window obtained using unoptimized versions of the strategies A and B.

Fig. 4.9 Distribution of key rates, QBERs, and key symmetries plotted against a range of coincidence window sizes for the crystal of length 20 mm.



(a) Plot showing the distribution of key rate and QBER values for varied sizes of coincidence window obtained using unoptimized versions of the strategies A and B.



(b) Plot showing the distribution of key symmetry values corresponding to the varied sizes of coincidence window obtained using unoptimized versions of the strategies A and B.

Fig. 4.10 Distribution of key rates, QBERs, and key symmetries plotted against a range of coincidence window sizes for the crystal of length 30 mm.

Optimization strategies A and B (discussed in Section 4.4.7) have been used to obtain the result quoted in Tables 4.1 and 4.2. The experimental results depend on the level of background noise, i. e., if the background noise is higher then the maintenance of the same QBER value will reduce the key rate. This background noise which is created mainly due to the detected but uncorrelated photons coming from various sources along with the SPDC source is responsible for the flat coincidence line shown in Fig. 4.7.

If we compare the various error ranges quoted alongside average values in Table 4.1, we can observe that the error values for QBER and key symmetry (column 4 and 5) are one order lower than the key rate value (column 3). This is due to the fact that in optimization strategy A, we restrict the QBER value and the key symmetry value to the upper limit of 4.8% and 50 (precise up to the second decimal place), whereas key rate does not have any such restriction. So, all the fluctuations in the dataset get reflected on the error value of the key rate. In case of optimization strategy B (Table 4.2), there is no additional restriction on the key symmetry value, hence the error value is higher than that of the QBER, and reflects the same range of fluctuations as observed in the key rate. It is important to note here that the two separate choices of optimization strategies have different implications on the security of the protocol, as discussed earlier in Section 4.4.5.

Additionally, Our in-lab demonstration of the free-space B92 QKD protocol was performed both in the day-time and the night-time scenario; for the sake of completeness. We observe that the results obtained from both these conditions are quite similar, except for the fact that the key rate obtained from the night-time dataset is slightly higher than the key rate from the day-time, irrespective of the length of the crystal and the optimization strategy. In order to investigate further, we compare the raw (unoptimized) datasets and observe the same phenomenon. For the 20 mm crystal and a fixed time-window of 3 ns, we obtained a key rate of 47.47 kHz from the day-time data whereas the night-time data generates key rate of 51.1 kHz. This result concludes that the observation of small increase in the key rate is not caused by the application of optimization strategies in the data-analysis stage, rather it is due to the variation of the environmental condition between day and night. As the experiment

was performed inside a controlled laboratory environment, it is expected that the role of the surrounding environment is insignificant. However, in reality, there can still be some environmental dependency. For example, we observed that the day-time temperature inside the lab has more fluctuation than the night, which can affect the pair generation rate from the PPKTP crystal. As explained in Section 2.2.3, the quasi phase-matching condition for the SPDC process inside the PPKTP crystal is achieved by tweaking the temperature of the crystal which is placed inside an oven connected to a feedback-looped temperature controller. The temperature of the crystal is the homogenized combination of the oven temperature and the overall room temperature, so any minute change in the room temperature also gets reflected in the crystal temperature. Pair generation rate in the SPDC process is maximum at a certain temperature (see 4.4.5), and even a small change of 0.1° can lower the rate significantly (see 2.2.3). Hence, the higher fluctuation in the day-time temperature lowers the average pair-generation rate and the unoptimized key rate.

Another observation from the result is that the average key rate value is lower for 30 mm crystal as compared to the 20 mm crystal. From theoretical calculation as well as intuitive understanding, we expect higher pair generation in longer crystal, as the interaction volume of the SPDC process increases with the length of the crystal. Another observation from both tables is that although for our case of not tightly focused Gaussian pump beam, having a longer crystal length should potentially lead to a higher key rate (as depicted in Fig. 4.10a) due to an increased pair production rate [3], the crystal of length 30 mm, in fact, produces a lower key rate estimate, for the given threshold QBER value, than the 20 mm one for the experimental results. This is because, in the experimentally measured data sets, the 30 mm crystal besides having a higher signal level also possess an increased noise level due to the detection of more background photons, which then lowers the key rate to ensure that the QBER optimization remains within the threshold value of 4.8%. Through separate experimental tests, we have verified that the singles and the coincidence rates observed at the detectors do not increase linearly with an increase in the pump beam intensity and the crystal length. From these test results, it can be inferred that the pair generation rate at the crystal does not increase linearly as well. Additionally, in the case of the key rate estimated

from the experiment with the 30 mm crystal, the error values are also higher owing to the increased fluctuations in the measured data points on the coincidence plot. As exemplified for a representative dataset in Fig. 4.8a, we observed via the unoptimized window duration of 3 ns around the coincidence peaks that the 30 mm crystal indeed offers a higher key rate owing to its increased pair rate compared to the 20 mm crystal. More particularly, in this daytime data analysis over 20 runs of the protocol, we found the key rate and QBER to be 47.47 ± 0.52 kHz and 4.67 ± 0.06 % respectively for the 20 mm crystal and 78.9 ± 0.48 kHz and 7.26 ± 0.03 % respectively for the 30 mm crystal. However, a significant lowering of this considerably high QBER (below the threshold) present in the 30 mm datasets due to an increased background noise level, via the optimization strategies, leads to a significant loss of key rate as reported in the Tables 4.1 and 4.2. In a nutshell, due to these reasons, the optimized average key rate value is higher when the length of the crystal is 20 mm compared to the 30 mm case that involves both higher background noise and more fluctuations.

Furthermore, from the Tables 4.1 and 4.2, we observe that the key rates obtained via the two optimization algorithms differ given a certain time of the day and length of the crystal. As discussed previously, this increase in the corresponding key rates for strategy B, occurs due to the offered relaxation in key symmetry, over strategy A. In order to understand the reason behind this intrinsic asymmetry, we need to take an account of the factors that affect the asymmetry of the key bits in the experiment. Apart from the asymmetry in the beamsplitting ratio, the asymmetry in coupling efficiency also plays an important role. In our experiment, the asymmetry due to coupling efficiency effectively reduces the asymmetry introduced by the beamsplitter to some extent. This counter error propagation happens as all the components involved in the experiment do not behave identically, thus we can get a different coupling efficiency even when the specification of the fibers and lenses remain the same. As a consequence, the overall asymmetry in the setup decreases, and that gets reflected in the results as well.

Chapter 5

Loophole free test of macroscopic realism

5.1 Introduction

The notion of realism which states that a measurable quantity has predefined value, irrespective of performing the measurement or not, has been a subject of many experimental tests, including the test of local realism in terms of Bell-type inequalities [9]. Leggett and Garg questioned the validity of this concept of realism in the domain of macroscopic systems. They formulated the famous Leggett-Garg inequality (LGI) [76] based on this notion of realism, in conjunction with the idea of non-invasive measurability.

The original motivation of Leggett and Garg was to check if the notion of quantum mechanical superposition is valid in the macroscopic domain or not. They came up with an inequality similar in the spirit to Bell's inequality but vastly different in characteristics. The notion of realism is similar to that used in Bell's inequality; a system always lies in any one of the possible states at any given time, irrespective of the measurement. So, in principle, this notion of realism denies the existence of the superposition of states, which is an essential aspect of quantum mechanics. In this sense, quantum mechanics contradict the idea of realism. We can measure, at a different time interval, some observable Q which has different outcomes (eigenvalues) on a system which is evolving with time. From these sequential measurements, two-time correlations of the form $\langle Q_{t_i} Q_{t_j} \rangle$ are constructed. For

a system maintaining the notion of realism mentioned above, at all times of its evolution, these temporal correlation values are different than the correlation values obtained from a non-realist model (to be specific, a model where superposition of states is possible, like quantum mechanics). If we now construct some expressions with specific linear combinations of these correlation values, the difference between the realist and the quantum model becomes prominent, which is also something that can be observed in an experiment. For example, if we consider a simpler model, where the observable Q has only two possible outcomes (eigenvalues $+1$ and -1) at all time of the evolution and Q is measured only at three distinct times (namely t_1 , t_2 and t_3), then we can construct four inequalities using correlation values at different times, which has different bounds for realist and quantum model.

$$C_{t_1,t_2} + C_{t_2,t_3} - C_{t_1,t_3} \leq 1 \quad (5.1)$$

$$C_{t_1,t_2} + C_{t_1,t_3} - C_{t_2,t_3} \leq 1 \quad (5.2)$$

$$C_{t_1,t_3} + C_{t_2,t_3} - C_{t_1,t_2} \leq 1 \quad (5.3)$$

$$-C_{t_1,t_2} - C_{t_2,t_3} - C_{t_1,t_3} \leq 1 \quad (5.4)$$

Here, C_{t_i,t_j} is expressed as the expected correlation value $\langle Q_{t_i} Q_{t_j} \rangle$. The maximum bound of 1 is for the realist model, whereas the quantum mechanical bound is 1.5 [37]. Because of this well-defined distinction, we can run an experiment and verify to which model nature has a preference. However, there is a caveat. As we measure the observable at three different times of the evolution, it may happen that a certain measurement can affect the outcomes of other measurements, hence resulting in completely different correlation values than what is expected from theory. To stop this from happening, another two assumptions were proposed, along with the realism assumption. The first one restricts that any past measurement should not affect the future measurement outcome (non-invasive measurement, or NIM). In contrast, the second one restricts any future measurement from affecting the past (induction or arrow of time (AoT)). The last condition is always assumed to be valid, so maintaining NIM is a primary criterion for an experimentalist. LG inequalities are formed using realism in

conjunction with NIM and AoT condition, which is similar to Bell's inequalities where locality condition is imposed along with reality assumption.

Over the years, the original concept of Leggett and Garg has gone through several criticisms, modifications, and clarifications, which have enriched the subject [88, 6]. I will go through most of these concepts step by step and also mention our take on the said topics in view of our experimental implementation. The first issue is with the use of the word “macro” in it. Although it has an implication in the context of the original motivation, it has nothing to do with the formalism of LG inequalities. The macroscopic nature of the system has not been considered while formatting the inequalities, meaning that they are independent of the “size” of the system and hence applicable even in microscopic systems. In fact, most of the experiments performed to check the LG inequalities have been implemented in microscopic systems such as single photon, single atom, etc. Also, the definition of “macroscopicity” is not unique in this context. Some may consider the size of the particle to be macroscopic, while for some, the states being macroscopically distinct is enough. As pointed out earlier [74, 67], the figure of merit used to characterise the ‘macroscopicity’ of any test concerning macrorealism is not necessarily linked to mass. It is, in general, dependent on the specifics of the experiment, for example, as discussed in the context of flux qubits [67]. The large value of ‘macroscopicity’ defined in our setup means that the $Q_{t_i} = +1$ and $Q_{t_i} = -1$ states are so well separated in space that the possibility of, say, the $Q_{t_i} = +1$ state being classically affected by a measuring device triggered essentially by the $Q_{t_i} = -1$ state is considerably small.

The term “reality” also does not have any unique definition and may vary based on the context and interpretation. In terms of macrorealism, the notion of “reality” primarily concerns with the existence of superposition between multiple states. However, there exist completely realist models that allow superposition, e. g. De-Broglie-Bohm model [18, 10], which is equally capable of violating the macrorealist bound of LGI. So, the experimental violation of LG type inequalities does not rule out the existence of all kind of macrorealist models; rather they only rule out a specific subset which is called the *operational eigenstate*

mixture macrorealism [82].

Another controversial idea is the assumption of NIM, which is also model dependant. In the context of a macrorealist model where a system always lies in any one of the possible states that are also macroscopically distinct, the idea of non-invasive or non-disturbing measurement makes sense. But for a model like quantum mechanics, which allows superposition of states, any measurement that unambiguously reveals the state of the system inherently collapses the state. So the concept of NIM is counterfactual for these types of models. In the case of Bell's inequality, "locality" and "reality" are two independent conditions and hence can be verified separately. Also, the locality assumption can be maintained fundamentally by using a physical law of nature, the relativity principle. Unfortunately for LGI, there is no such fundamental theory to establish the maintenance of the NIM assumption. In light of this, a macrorealist can always claim that the measurements performed in the experiment are indeed invasive, which leads to the violation of LGI. Therefore the notion of macrorealism is not refuted by the experiment. This loophole is generally referred to as the *clumsiness loophole* in the literature.

Irrespective of the criticism, LGI has been experimentally tested on various physical systems like superconducting qubits [86, 67], nuclear magnetic resonance [64], nitrogen-vacancy centre [47], quantum transport [95], photon-based systems [121, 32, 50, 110, 116], etc.

Another important point to note is that LGI is only a necessary condition for macrorealism. Alternatively saying, there is no Fine's theorem in the case of LGI [28], as it exists in Bell's inequality, proving that it is both a necessary and a sufficient condition for local realism. This led researchers to work on a new set of conditions called no-signaling in time (NSIT), which is both a necessary and a sufficient condition to macrorealism [71, 27, 28]. NSIT condition says that the outcome of a measurement is not affected by any prior measurements on the same system. Mathematically, this condition can be expressed in the following forms.

$$NSIT_{(t_i)t_j} : P_{t_j}(q_{t_j}) = \sum_{q_{t_i}=\pm 1} P_{t_i,t_j}(q_{t_i}, q_{t_j}) \forall q_{t_j} = \pm 1, t_i < t_j \quad (5.5)$$

This form of NSIT (Eq. 5.5) is the most fundamental form which consists of only two times t_i and t_j , and states that the probability of the outcome q_{t_j} when the observable Q is measured at time t_j is the summation of all two-time joint probabilities of the form $P_{t_i,t_j}(q_{t_i}, q_{t_j})$. The expression $P_{t_i,t_j}(q_{t_i}, q_{t_j})$ represents the joint probability of measuring simultaneous outcomes q_{t_i} and q_{t_j} while observable Q is measured at t_i and Q is measured at t_j . We can also write the three-time NSITs in the similar format. Here, $t_i < t_j < t_k$ represents the flow of time.

$$NSIT_{(t_i)t_jt_k} : P_{t_j,t_k}(q_{t_j}, q_{t_k}) = \sum_{q_{t_i}=\pm 1} P_{t_i,t_j,t_k}(q_{t_i}, q_{t_j}, q_{t_k}) \quad (5.6)$$

$$NSIT_{t_i(t_j)t_k} : P_{t_i,t_k}(q_{t_i}, q_{t_k}) = \sum_{q_{t_j}=\pm 1} P_{t_i,t_j,t_k}(q_{t_i}, q_{t_j}, q_{t_k}) \quad (5.7)$$

A combination of two-time NSIT and three-time NSITs, along with the equation of Arrow of Time (AoT), form the necessary and sufficient condition for macrorealism (MR).

$$MR \Leftrightarrow NSIT_{(t_2)t_3} \wedge NSIT_{(t_1)t_2t_3} \wedge NSIT_{t_1(t_2)t_3} \wedge AoT \quad (5.8)$$

AoT or Arrow of Time (alternatively called Induction) states that the outcome of a measurement on the system cannot be affected by what will or will not be measured on it at later times. It has a similar mathematical form as the NSITs, in both two-time and three-time levels.

$$AoT_{t_i(t_j)} : P_{t_i}(q_{t_i}) = \sum_{q_{t_j}=\pm 1} P_{t_i,t_j}(q_{t_i}, q_{t_j}) \quad (5.9)$$

$$AoT_{t_it_j(t_k)} : P_{t_i,t_j}(q_{t_i}, q_{t_j}) = \sum_{q_{t_k}=\pm 1} P_{t_i,t_j,t_k}(q_{t_i}, q_{t_j}, q_{t_k}) \quad (5.10)$$

NSIT equations are interesting to work with from a different perspective as they also form the necessary condition for non-invasive measurement (NIM). NSIT condition is considered as a statistical form of NIM, and violation of which automatically implies that the measurement is invasive. So it is important to verify that all the measurements performed in the experiment

maintain all relevant NSITs.

Based on the same assumptions of macrorealism, another set of inequalities called the Wigner form of LG inequalities (WLGIs) was proposed, which assumed the existence of overall joint probabilities pertaining to different combinations of measurement outcomes from which, by appropriate marginalization, the pair-wise observable joint probabilities of the form $P_{t_i, t_j}(q_{t_i}, q_{t_j})$ are obtained, analogous to the way Wigner's form of the local realist inequality was derived [118]. There are a total of twenty-four WLGIs forms where quantum mechanics can violate the upper bound of these inequalities. We consider one such WGI expression here.

$$P_{t_1, t_3}(-, +) - P_{t_1, t_2}(-, +) - P_{t_2, t_3}(-, +) \leq 0 \quad (5.11)$$

A key feature of most of the experiments based on LGI has been the use of projective measurements, along with negative result measurements or NRM in short (a measurement in which an outcome is inferred when the detector is not triggered). NRM is employed to ensure the validity of NIM so that the observed violation of a macrorealist inequality can be attributed solely to the quantum mechanical violation of realism per se (the underlying conceptual justification for using NRM in order to ensure NIM has been discussed by Leggett [75]). However, the non-idealness in the empirical implementation of NRM can result in the classical disturbance affecting the measured system, thereby contributing to the observed violation of the macrorealist condition being tested. This has been referred to as the clumsiness loophole [119]. Different strategies have been adopted for tackling this issue. For example, in the superconducting flux qubit experiment testing NSIT [67], the resulting classical disturbance is determined using appropriate control experiments.

On the other hand, an entirely different strategy for testing macrorealism has been explored in terms of what has been called “ambiguously measured LGI” formulated by avoiding the use of NIM and hence not requiring NRM [36]. But, for this procedure to work, one has to consider two sets of measurements, one projective and the other ambiguous measurements realized by a class of POVMs, and then, importantly, invoke an additional assumption called equivalently invasive measurement (EIM), which equates the invasive influence of ambiguous

measurements with that of the unambiguous ones. It has been argued that EIM leads to a testable condition, and by violating the ambiguous version of LGI while satisfying this condition, the clumsiness loophole can be avoided. Further, It has been pointed out [36] that an assumption similar to EIM is also implicit in the experiments on LGI in terms of weak measurements.

Therefore, the upshot of the above considerations is that for avoiding the use of NIM in testing macrorealism, some other suitable assumption has to be necessarily invoked. In this context, we note that recently another approach has been suggested to avoid the use of NIM using a single Mach-Zehnder interferometric setup by putting forth a plausible argument for inferring the violation of macrorealism directly from the occurrence of destructive interference per se [87]. To what extent such an argument is general is not yet clear. Similarly, the implications of another recent interesting finding [53] that the quantum mechanical violation of LGI in the double-slit interferometric setup is necessarily accompanied by destructive interference need to be further analysed.

Against the above backdrop, our photon-based experiment presented in this thesis focuses on testing macrorealism using LGI and its variant WLGI in terms of projective and negative result measurements by rigorously addressing the relevant loopholes. The reasons for showing violation of both the LGI and the WLGI are the following. First of all, both LGI and WLGI is only a necessary condition (not sufficient) to MR. Hence, simultaneous violation of both the inequalities, in a loophole-free way, provides a more robust notion of violation of the MR theory. Secondly, there is an advantage in working with WLGI in the experimental setup. The WLGI expression involves a much lower number of terms of experimentally measurable quantity compared to the LGI expression. Hence, it generates a lower error value, leading to better agreement with the theoretical prediction.

The experimental setup we use [63] consists of two Mach-Zehnder interferometers with standard optical elements and is amenable to be adapted for atoms, molecules towards studies in the macroscopic regime. While the use of heralded single-photons from the process of

spontaneous parametric down-conversion (SPDC) in this experiment aids in closing various loopholes due to the lower multi-photon generation probability and higher noise tolerance, a significant feature of our experiment is the way we use the NSIT condition for closing the clumsiness loophole.

Although a bulk of research works on closing the clumsiness loophole for LGI experiments exist in the literature, there are negligible works on various other loopholes, which are equally significant. In this work, we address all of these loopholes and provide experimental strategies to close them, such that to a macrorealist, the experiment delivers conclusive results. These loopholes are *detection efficiency loophole*, *multiple emission loophole*, *coincidence loophole*, *preparation state loophole*, etc. Such detailed analyses enabling all these loopholes to be either circumvented or closed in a given optical experiment testing macrorealism are yet missing, and the present work fills this important gap.

5.2 Theory

Macroscopic realism or macrorealism (MR) is a classical worldview, which consists of three assumptions described below. In the original work of Leggett and Garg, the third assumption was not explicitly defined, but in later works, the third assumption was made explicit.

- *Macroscopic realism per se (MRps)*: a macroscopic system with two or more macroscopically distinct states available to it will at all times be in one or the other of these states.
- *Non-invasive measurability (NIM)*: it is possible, in principle, to determine the state of the system with arbitrarily small perturbation on its subsequent dynamics.
- *Induction or Arrow of time (AoT)*: the outcome of a measurement on the system cannot be affected by what will or will not be measured on it later.

Following the general notation, hereafter we will call the first assumption as MRps, and the combination of the three assumptions as MR. Based on these assumptions, Leggett and Garg first proposed a set of inequalities (LGI). In the simplistic case of three times, we can construct four such LG inequalities described in equation 5.1-5.4. We will focus on only one such inequality which is sufficient for our current purpose of the experiment.

$$\langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle \leq 1 \quad (5.12)$$

Here Q_{t_i} is a dichotomic observable measured at time t_i , which has two possible outcomes with eigenvalues +1 or -1. Here, $t_1 < t_2 < t_3$ represents the flow of time. $\langle Q_{t_i} Q_{t_j} \rangle$ is the expected correlation value between measurement outcomes at t_i and t_j . This inequality has a higher upper bound of 1.5 from quantum mechanics (QM). Similarly for WLGI, we will consider one WLGI expression (Eq. 5.11), which has a maximum QM violation of approximately 0.4034. For NSITs, we will discuss both the two-time (Eq. 5.5) and three-time (Eqs. 5.6, 5.7) NSIT forms, in the context of MR.

In this section, we show theoretical calculations to establish macrorealist bounds for both LGI and WLGI, and establish all NSIT equations. We follow two different approaches for this calculation, firstly with the conventional assumptions of macrorealism, and secondly, with an ontic state description. We also show quantum mechanical description for violating LGI and WLGI.

5.2.1 Proof based on macrorealist assumptions

Let us consider an ensemble of systems undergoing temporal evolution involving oscillation between the two states, say, 1 and 2, and let $Q(t)$ be an observable quantity such that, whenever measured, it is found to take a value +1 or -1 depending on whether the system is in the state 1 or 2. As a consequence of the assumptions of macrorealism *per se* one can infer the existence of overall joint probabilities $P(q_{t_1}, q_{t_2}, q_{t_3})$, which are pre-defined and independent of if any measurement is performed or not. $P(q_{t_1}, q_{t_2}, q_{t_3})$ represents the joint

probability of the outcomes q_{t_1} , q_{t_2} , and q_{t_3} when the observable Q is measured at times t_1, t_2, t_3 respectively. q_{t_1}, q_{t_2} and q_{t_3} can take any value from either $+1$ or -1 . As a corollary, we can write any measured two-time joint probabilities as a marginal of all three-time joint probabilities.

$$P_{i,t_j}(q_{t_i}, q_{t_j}) = \sum_{q_{t_k}=\pm 1} P_{i,t_j}(q_{t_i}, q_{t_j}, q_{t_k}) \quad (5.13)$$

Eq. 5.13 is valid for any $q_{t_i} = \pm 1$, $q_{t_j} = \pm 1$, and any permutation of i, j, k , maintaining the flow of time $t_i < t_j < t_k$. The subscript t_i, t_j in the expression of the probability (P) denotes that the probability is obtained while actual measurements are performed at time t_i and t_j only. From the NIM assumption and the AoT assumption, we can infer that any three-time joint probability is invariant under any measurement performed at any time.

$$P_{t_1,t_2}(q_{t_1}, q_{t_2}, q_{t_3}) = P_{t_2,t_3}(q_{t_1}, q_{t_2}, q_{t_3}) = P_{t_1,t_3}(q_{t_1}, q_{t_2}, q_{t_3}) = P(q_{t_1}, q_{t_2}, q_{t_3}) \quad (5.14)$$

Using these two equations, 5.13 and 5.14, we can find macrorealist bounds for LGI, WLGI, and NSIT conditions.

Case 1: LGI (Leggett-Garg inequality)

We can express the expectation value of any joint measurement as a combination of joint probabilities.

$$\langle Q_{t_i} Q_{t_j} \rangle = \sum_{q_{t_i}=\pm 1, q_{t_j}=\pm 1} q_{t_i} q_{t_j} P_{t_i,t_j}(q_{t_i}, q_{t_j}) \quad (5.15)$$

Using equations 5.13, 5.14 and 5.15, we can write,

$$\begin{aligned}
LGI : & \langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle \\
&= \sum_{q_{t_1}, q_{t_2}} q_{t_1} q_{t_2} P_{t_1, t_2}(q_{t_1}, q_{t_2}) + \sum_{q_{t_2}, q_{t_3}} q_{t_2} q_{t_3} P_{t_2, t_3}(q_{t_2}, q_{t_3}) - \sum_{q_{t_1}, q_{t_3}} q_{t_1} q_{t_3} P_{t_1, t_3}(q_{t_1}, q_{t_3}) \\
&= \sum_{q_{t_1}, q_{t_2}, q_{t_3}} q_{t_1} q_{t_2} P_{t_1, t_2}(q_{t_1}, q_{t_2}, q_{t_3}) + \sum_{q_{t_1}, q_{t_2}, q_{t_3}} q_{t_2} q_{t_3} P_{t_2, t_3}(q_{t_1}, q_{t_2}, q_{t_3}) \\
&\quad - \sum_{q_{t_1}, q_{t_2}, q_{t_3}} q_{t_1} q_{t_3} P_{t_1, t_3}(q_{t_1}, q_{t_2}, q_{t_3}) \\
&= \sum_{q_{t_1}, q_{t_2}, q_{t_3}} q_{t_1} q_{t_2} P(q_{t_1}, q_{t_2}, q_{t_3}) + \sum_{q_{t_1}, q_{t_2}, q_{t_3}} q_{t_2} q_{t_3} P(q_{t_1}, q_{t_2}, q_{t_3}) \\
&\quad - \sum_{q_{t_1}, q_{t_2}, q_{t_3}} q_{t_1} q_{t_3} P(q_{t_1}, q_{t_2}, q_{t_3}) \\
&= \sum_{q_{t_1}, q_{t_2}, q_{t_3}} P(q_{t_1}, q_{t_2}, q_{t_3}) \{q_{t_1} q_{t_2} + q_{t_2} q_{t_3} - q_{t_1} q_{t_3}\} \\
&= P(+, +, +) + P(+, +, -) - 3P(+, -, +) + P(+, -, -) + P(-, +, +) \\
&\quad - 3P(-, +, -) + P(-, -, +) + P(-, -, -) \\
&= 1 - 4\{P(+, -, +) + P(-, +, -)\}
\end{aligned} \tag{5.16}$$

If we assume that all joint probabilities are from a valid probability distribution, then $0 \leq P(q_{t_1}, q_{t_2}, q_{t_3}) \leq 1$, $\forall q_{t_1} = \pm 1, q_{t_2} = \pm 1, q_{t_3} = \pm 1$, and $\sum_{q_{t_1}, q_{t_2}, q_{t_3}} P(q_{t_1}, q_{t_2}, q_{t_3}) = 1$. It can be easily checked that $-3 \leq LGI \leq 1$.

Case 2: WLGI (Wigner form of LGI)

Using equations 5.11, 5.13, 5.14,

$$\begin{aligned}
WLGI : & P_{t_1,t_3}(-,+) - P_{t_1,t_2}(-,+) - P_{t_2,t_3}(-,+) \\
&= \sum_{q_{t_2}=\pm 1} P_{t_1,t_3}(-,q_{t_2},+) - \sum_{q_{t_3}=\pm 1} P_{t_1,t_2}(-,+,q_{t_3}) - \sum_{q_{t_1}=\pm 1} P_{t_2,t_3}(q_{t_1},-,+) \\
&= \sum_{q_{t_2}=\pm 1} P(-,q_{t_2},+) - \sum_{q_{t_3}=\pm 1} P(-,+,q_{t_3}) - \sum_{q_{t_1}=\pm 1} P(q_{t_1},-,+) \\
&= P(-,+,+) + P(-,-,+) - P(-,+,+) - P(-,+, -) - P(+,-,+) - P(-,-,+) \\
&= -\{P(-,+, -) + P(+,-,+)\}
\end{aligned} \tag{5.17}$$

From the above expression (Eq. 5.17), we can easily find the WLGI bound, i. e., $-1 \leq WLGI \leq 0$.

Case 3: NSIT (No signaling in time)

For this case, we will look into both the conditions based on two-time and three-time. No signaling in time means that any measurement outcome in the future is not affected by any measurement performed in the past. Using equations 5.5, 5.6, 5.7, 5.13, 5.14,

case A: two-time NSIT

$$\begin{aligned}
LHS : P_{t_j}(q_{t_j}) &= \sum_{q_{t_i}, q_{t_k}} P_{t_j}(q_{t_i}, q_{t_j}, q_{t_k}) = \sum_{q_{t_i}, q_{t_k}} P(q_{t_i}, q_{t_j}, q_{t_k}) \\
&= \sum_{q_{t_i}, q_{t_k}} P_{t_i,t_j}(q_{t_i}, q_{t_j}, q_{t_k}) \\
&= \sum_{q_{t_i}} P_{t_i,t_j}(q_{t_i}, q_{t_j}) \\
&= RHS
\end{aligned} \tag{5.18}$$

case B: three-time NSIT

$$\begin{aligned}
 LHS : P_{t_j, t_k}(q_{t_j}, q_{t_k}) &= \sum_{q_{t_i}} P_{t_j, t_k}(q_{t_i}, q_{t_j}, q_{t_k}) = \sum_{q_{t_i}} P(q_{t_i}, q_{t_j}, q_{t_k}) \\
 &= \sum_{q_{t_i}} P_{t_i, t_j, t_k}(q_{t_i}, q_{t_j}, q_{t_k}) \quad (5.19) \\
 &= RHS
 \end{aligned}$$

The above equation shows the proof of the expression, $NSIT_{(t_i), t_j, t_k}$. We can also show the proof for $NSIT_{t_i, (t_j), t_k}$ in the similar way.

5.2.2 Proof based on the ontic state description

Any given experimental arrangement is characterized by a preparation (P), transmission (T), and a measurement process (M) with distinct outcomes m . Operationally, this is characterised by a probability $P_{(P, T, M)}(m)$. The ontic state represents the real state of the system, which governs all the physical properties as well as any measurement outcome on the system. This might simply be taken to be the quantum mechanical wave-function for the system, or might represent additional ‘hidden’ variables or elements of reality. A non-invasive measurement (NIM) is a measurement that does not disturb the ontic state of the system. It has been established [81] that the NIM condition by itself is such a strong statement on realism, it does not require the condition of MRps to construct the LGI or WLGI bounds. The only other condition necessary is that the system maintains the ontic state formalism.

A preparation process produces a probabilistic distribution $\rho(\lambda)$ over the ontic states λ which spans the complete set Λ , where $\int_{\lambda \in \Lambda} \rho(\lambda) d\lambda = 1$. A measurement at time t_i is represented by an outcome function, giving the probability of outcome q_{t_i} occurring, conditional upon the actual ontic state of the system: $P_{t_i}(q_{t_i}|\lambda)$. Where,

$$\sum_{q_{t_i}=\pm 1} P_{t_i}(q_{t_i}|\lambda) = 1 \quad (5.20)$$

So, the operational probability can be written as,

$$P_{t_i}(q_{t_i}) = \int_{\lambda \in \Lambda} d\lambda \rho(\lambda) P_{t_i}(q_{t_i}|\lambda) \quad (5.21)$$

The probability of a disturbance of the ontic state by the measurement at time t_i , with outcome q_{t_i} is given by: $\gamma_{t_i}(\lambda'|q_{t_i}, \lambda)$, where $\int_{\lambda'} \gamma_{t_i}(\lambda'|q_{t_i}, \lambda) d\lambda' = 1$. After the measurement, with the outcome q_{t_i} , the new preparation state will be:

$$\mu_{q_{t_i}}(\lambda') = \int_{\lambda} d\lambda \rho(\lambda) P_{t_i}(q_{t_i}|\lambda) \gamma_{t_i}(\lambda'|q_{t_i}, \lambda) \quad (5.22)$$

So, the joint probability of measuring the outcome q_{t_i} at time t_i and q_{t_j} at time t_j is expressed as,

$$P_{t_i, t_j}(q_{t_i}, q_{t_j}) = \int_{\lambda_j} d\lambda_j \int_{\lambda_i} d\lambda_i \rho(\lambda_i) P_{t_i}(q_{t_i}|\lambda_i) \gamma_{t_i}(\lambda_j|q_{t_i}, \lambda_i) P_{t_j}(q_{t_j}|\lambda_j) \quad (5.23)$$

Any measurement that does not affect the ontic state is called a Non-Invasive Measurement (NIM). It is represented by,

$$\gamma_{t_i}(\lambda_j|q_{t_i}, \lambda_i) = \delta(\lambda_j - \lambda_i) \quad (5.24)$$

$$\int_{\lambda_j} d\lambda_j \delta(\lambda_j - \lambda_i) P_{t_j}(q_{t_j}|\lambda_j) = P_{t_j}(q_{t_j}|\lambda_i) \quad (5.25)$$

Using equation 5.25 in equation 5.23,

$$P_{t_i, t_j}(q_{t_i}, q_{t_j}) = \int_{\lambda_i} d\lambda_i \rho(\lambda_i) P_{t_i}(q_{t_i}|\lambda_i) P_{t_j}(q_{t_j}|\lambda_i) \quad (5.26)$$

Case 1: LGI

Using equation 5.15 and 5.26, we can write,

$$\begin{aligned}
 \langle Q_{t_i} Q_{t_j} \rangle &= \sum_{q_{t_i}, q_{t_j}} q_{t_i} q_{t_j} P_{t_i, t_j}(q_{t_i}, q_{t_j}) \\
 &= \sum_{q_{t_i}, q_{t_j}} q_{t_i} q_{t_j} \int_{\lambda_i} d\lambda_i \rho(\lambda_i) P_{t_i}(q_{t_i} | \lambda_i) P_{t_j}(q_{t_j} | \lambda_i) \\
 &= \int_{\lambda_i} d\lambda_i \rho(\lambda_i) \left\{ \sum_{q_{t_i}} q_{t_i} P_{t_i}(q_{t_i} | \lambda_i) \right\} \left\{ \sum_{q_{t_j}} q_{t_j} P_{t_j}(q_{t_j} | \lambda_i) \right\} \\
 &= \int_{\lambda_i} d\lambda_i \rho(\lambda_i) \langle Q_{t_i} \rangle_{\lambda_i} \langle Q_{t_j} \rangle_{\lambda_i}
 \end{aligned} \tag{5.27}$$

By using equation 5.27,

$$\begin{aligned}
 LGI &= \langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle \\
 &= \int_{\lambda} d\lambda \rho(\lambda) \langle Q_{t_1} \rangle_{\lambda} \langle Q_{t_2} \rangle_{\lambda} + \int_{\lambda} d\lambda \rho(\lambda) \langle Q_{t_2} \rangle_{\lambda} \langle Q_{t_3} \rangle_{\lambda} - \int_{\lambda} d\lambda \rho(\lambda) \langle Q_{t_1} \rangle_{\lambda} \langle Q_{t_3} \rangle_{\lambda} \\
 &= \int_{\lambda} d\lambda \rho(\lambda) \{ \langle Q_{t_1} \rangle_{\lambda} \langle Q_{t_2} \rangle_{\lambda} + \langle Q_{t_2} \rangle_{\lambda} \langle Q_{t_3} \rangle_{\lambda} - \langle Q_{t_1} \rangle_{\lambda} \langle Q_{t_3} \rangle_{\lambda} \}
 \end{aligned} \tag{5.28}$$

In equation 5.28, all individual expectation values can maximally go up to 1. So by assigning 1 to all expectation values, we get $LGI \leq 1$. Also, by assigning $\langle Q_{t_1} \rangle_{\lambda} = \langle Q_{t_3} \rangle_{\lambda} = 1, \langle Q_{t_2} \rangle_{\lambda} = -1$, we get $LGI \geq -3$.

Case 2: WLGI

Using equation 5.26,

$$\begin{aligned}
 WLG I : & P_{t_1, t_3}(-, +) - P_{t_1, t_2}(-, +) - P_{t_2, t_3}(-, +) \\
 &= \int_{\lambda} d\lambda \rho(\lambda) P_{t_1}(-|\lambda) P_{t_3}(+|\lambda) - \int_{\lambda} d\lambda \rho(\lambda) P_{t_1}(-|\lambda) P_{t_2}(+|\lambda) - \int_{\lambda} d\lambda \rho(\lambda) P_{t_2}(-|\lambda) P_{t_3}(+|\lambda) \\
 &= \int_{\lambda} d\lambda \rho(\lambda) \{P_{t_1}(-|\lambda) P_{t_3}(+|\lambda) - P_{t_1}(-|\lambda) P_{t_2}(+|\lambda) - P_{t_2}(-|\lambda) P_{t_3}(+|\lambda)\}
 \end{aligned} \tag{5.29}$$

In equation 5.29, we get maximum value by assigning $P_{t_1}(-|\lambda) = P_{t_3}(+|\lambda) = 1, P_{t_2}(+|\lambda) = 0$. Also, we get the minimum by assigning $P_{t_1}(-|\lambda) = P_{t_2}(+|\lambda) = 1, P_{t_3}(+|\lambda) = 0$. So, we can easily find that the WLG I value lies between -1 and 0 .

Case 3: NSITs

We prove two-time NSIT equality by using the equations 5.5, 5.20, 5.21 and 5.26.

$$\begin{aligned}
 RHS : \sum_{q_{t_i}} P_{t_i, t_j}(q_{t_i}, q_{t_j}) &= \sum_{q_{t_i}} \int_{\lambda} d\lambda \rho(\lambda) P_{t_i}(q_{t_i}|\lambda) P_{t_j}(q_{t_j}|\lambda) \\
 &= \int_{\lambda} d\lambda \rho(\lambda) P_{t_j}(q_{t_j}|\lambda) \sum_{q_{t_i}} P_{t_i}(q_{t_i}|\lambda) \\
 &= \int_{\lambda} d\lambda \rho(\lambda) P_{t_j}(q_{t_j}|\lambda) \\
 &= P_{t_j}(q_{t_j}) \\
 &= LHS
 \end{aligned} \tag{5.30}$$

We prove three-time NSIT equality by using the equations 5.6, 5.20 and 5.26.

$$\begin{aligned}
RHS : \sum_{q_{t_i}} P_{t_i, t_j, t_k}(q_{t_i}, q_{t_j}, q_{t_k}) &= \sum_{q_{t_i}} \int d\lambda \rho(\lambda) P_{t_i}(q_{t_i}|\lambda) P_{t_j}(q_{t_j}|\lambda) P_{t_k}(q_{t_k}|\lambda) \\
&= \int d\lambda \rho(\lambda) \left\{ \sum_{q_{t_i}} P_{t_i}(q_{t_i}|\lambda) \right\} P_{t_j}(q_{t_j}|\lambda) P_{t_k}(q_{t_k}|\lambda) \\
&= \int d\lambda \rho(\lambda) P_{t_j}(q_{t_j}|\lambda) P_{t_k}(q_{t_k}|\lambda) \\
&= P_{t_j, t_k}(q_{t_j}, q_{t_k}) \\
&= LHS
\end{aligned} \tag{5.31}$$

Similarly, we can also show the proof for $NSIT_{t_i, (t_j), t_k}$.

5.2.3 Quantum mechanical bound

Suppose $\vec{a}$ is any real three-dimensional unit vector (any point on Bloch sphere). We can define an observable Q as, $\vec{\sigma} \cdot \vec{a} = a_x \sigma_x + a_y \sigma_y + a_z \sigma_z$. This observable Q has two eigenvalues, $q = \pm 1$. Projection operators onto these eigenstates are represented by $\mathbb{P}_{\vec{a}}^q = \frac{\mathbb{I} + q\vec{\sigma} \cdot \vec{a}}{2}$. So, the probability of measuring an outcome q_i , where $q_i = \pm 1$, after performing a projective measurement at time t_i can be represented as,

$$P_{t_i}(q_{t_i}) = Tr(\rho \mathbb{P}_{\vec{a}_i}^{q_{t_i}}) \tag{5.32}$$

Here, ρ is the density matrix of the input state. Tr represents trace operation. After the measurement, the collapsed state becomes $\rho' = \mathbb{P}_{\vec{a}_i}^{q_{t_i}}$. So, we can write the joint probability of

measuring q_{t_i} at time t_i and q_{t_j} at time t_j as,

$$\begin{aligned}
P_{t_i, t_j}(q_{t_i}, q_{t_j}) &= P_{t_i}(q_{t_i})P_{t_j}(q_{t_j}|q_{t_i}) \\
&= \text{Tr}(\rho \mathbb{P}_{\vec{a}_i}^{q_{t_i}}) \text{Tr}(\mathbb{P}_{\vec{a}_i}^{q_{t_i}} \mathbb{P}_{\vec{a}_j}^{q_{t_j}}) \\
&= \text{Tr}(\rho \frac{1}{2}(\mathbb{I} + q_{t_i} \vec{\sigma} \cdot \vec{a}_i)) \text{Tr}(\frac{1}{2}(\mathbb{I} + q_{t_i} \vec{\sigma} \cdot \vec{a}_i) \frac{1}{2}(\mathbb{I} + q_{t_j} \vec{\sigma} \cdot \vec{a}_j)) \\
&= \text{Tr}(\frac{\rho + q_{t_i} \rho \vec{\sigma} \cdot \vec{a}_i}{2}) \text{Tr}(\frac{\mathbb{I} + q_{t_i} \vec{\sigma} \cdot \vec{a}_i + q_{t_j} \vec{\sigma} \cdot \vec{a}_j + q_{t_i} q_{t_j} (\vec{\sigma} \cdot \vec{a}_i)(\vec{\sigma} \cdot \vec{a}_j)}{4}) \quad (5.33) \\
&= \frac{1 + q_{t_i} \alpha}{2} \times \frac{2 + q_{t_i} q_{t_j} \beta}{4} \\
&= \frac{(1 + q_{t_i} \alpha)(2 + q_{t_i} q_{t_j} \beta)}{8}
\end{aligned}$$

We have defined $\alpha = \text{Tr}(\rho \vec{\sigma} \cdot \vec{a}_i)$ and $\beta = \text{Tr}\{(\vec{\sigma} \cdot \vec{a}_i)(\vec{\sigma} \cdot \vec{a}_j)\} = 2\vec{a}_i \cdot \vec{a}_j$. While calculating Eq. 5.33, we have also considered the facts that $\text{Tr}(\rho) = 1, \text{Tr}(\mathbb{I}) = 2, \text{Tr}(\vec{\sigma} \cdot \vec{a}_i) = \text{Tr}(\vec{\sigma} \cdot \vec{a}_j) = 0$. Using Eq. 5.33, and the fact that $\beta = 2\vec{a}_i \cdot \vec{a}_j$, we can write,

$$\begin{aligned}
\langle Q_{t_i} Q_{t_j} \rangle &= \sum_{q_{t_i}=\pm 1, q_{t_j}=\pm 1} q_{t_i} q_{t_j} P_{t_i, t_j}(q_{t_i}, q_{t_j}) \\
&= P_{t_i, t_j}(+, +) + P_{t_i, t_j}(-, -) - P_{t_i, t_j}(+, -) - P_{t_i, t_j}(-, +) \\
&= \frac{(1 + \alpha)(2 + \beta)}{8} + \frac{(1 - \alpha)(2 + \beta)}{8} - \frac{(1 + \alpha)(2 - \beta)}{8} - \frac{(1 - \alpha)(2 - \beta)}{8} \quad (5.34) \\
&= \frac{\beta}{2} \\
&= \vec{a}_i \cdot \vec{a}_j
\end{aligned}$$

By using Eq. 5.34,

$$\begin{aligned}
LGI &= \langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle \\
&= \vec{a}_1 \cdot \vec{a}_2 + \vec{a}_2 \cdot \vec{a}_3 - \vec{a}_1 \cdot \vec{a}_3 \\
&= \cos \theta_{1,2} + \cos \theta_{2,3} - \cos \theta_{1,3} \quad (5.35) \\
&\leq \cos \theta_{1,2} + \cos \theta_{2,3} - \cos(\theta_{1,2} + \theta_{2,3}) \\
&\leq \frac{3}{2}
\end{aligned}$$

In the equation 5.35, $\theta_{i,j}$ is the angle between the two unit vectors a_i and a_j . The maximum value of the LGI expression is obtained by assigning the values $\theta_{1,2} = \theta_{2,3} = \frac{\pi}{3}$.

Similarly, we write the WLGI expression using equation 5.33.

$$\begin{aligned} WLGI : & P_{t_1,t_3}(-,+) - P_{t_1,t_2}(-,+) - P_{t_2,t_3}(-,+) \\ &= \frac{(1 - \alpha_1)(1 - \vec{a}_1 \cdot \vec{a}_3)}{4} - \frac{(1 - \alpha_1)(1 - \vec{a}_1 \cdot \vec{a}_2)}{4} - \frac{(1 - \alpha_2)(1 - \vec{a}_2 \cdot \vec{a}_3)}{4} \end{aligned} \quad (5.36)$$

Here, $\alpha_1 = Tr(\rho \vec{\sigma} \cdot \vec{a}_1)$, $\alpha_2 = Tr(\rho \vec{\sigma} \cdot \vec{a}_2)$. By maximizing the expression 5.36 numerically, we find the upper bound of WLGI from quantum mechanics is 0.4034.

5.3 Loophole free version of the experiment

Most of the experiments performed earlier suffer from one or more loopholes. It is important to address these loopholes and find ways to close them such that to the eye of a macrorealist, the experiment delivers conclusive results. In this section, we discuss a few such loopholes and the strategies that we apply to fully or partially close them.

5.3.1 Clumsiness loophole

The notion of macrorealism (MR) consists of three assumptions, namely, macroscopic realism per se (MRps), Non-invasive measurability (NIM), and Induction or arrow of time. As we always consider the induction assumption to be valid, it is only the two assumptions (MRps and NIM) that form the notion of MR under test. Violation of MR (through the violation of LGI in an experiment) implies violation of MRps or NIM or both. So, in order to make a conclusive remark on the refutation of MRps theory by nature, we make sure that the NIM condition is not violated. However, the most tricky part for an experimentalist is to show experimental proof of the NIM condition being satisfied in the experiment. Here, a macrorealist can always claim that the experiment is clumsy as the measurements performed are indeed invasive. Against such a claim, it is hard to establish that the violation of LGI

means the violation of MRps. This loophole is called the *Clumsiness loophole* in the literature.

There is no direct measurement technique to quantify the degree of invasiveness, however, there is a necessary condition to it which is called the no-signaling in time (NSIT). NSIT condition is considered as a statistical form of NIM, and violation of which automatically implies that the measurement is invasive. NIM as a physical constraint, can be better understood at the most fundamental level. In an ontic state description, the NIM condition can be mathematically expressed as,

$$P_{t_j}(q_{t_j}|\lambda) = \sum_{q_{t_i}=\pm 1} P_{t_i,t_j}(q_{t_i}, q_{t_j}|\lambda) \quad \forall q_{t_j} = \pm 1, t_i < t_j \quad (5.37)$$

Equation 5.37 implies that for any ontic state λ in the whole ontic space, probability of the outcome q_{t_j} given λ , while the measurable quantity Q is measured at time t_j , is the marginal of all joint probabilities of outcomes q_{t_i} and q_{t_j} at t_i and t_j , respectively, where $t_i < t_j$. For a measurement at t_i to be NIM at ontic level, equation 5.37 should be satisfied for all possible λ . However, it is not possible to experimentally verify equation 5.37 for all λ . So, we move to the operational form of NIM, where if equation 5.37 is satisfied for all λ , then we can write the form similar to the NSIT form.

$$P_{t_j}(q_{t_j}) = \sum_{q_{t_i}=\pm 1} P_{t_i,t_j}(q_{t_i}, q_{t_j}) \quad \forall q_{t_j} = \pm 1, t_i < t_j \quad (5.38)$$

It is easy to check that equation 5.37 implies equation 5.38, but the reverse is not true. So, the NSIT condition is only the necessary condition to a stronger notion of NIM, and it is important to verify that all the measurements performed in the experiment at least maintain all relevant forms of NSITs.

Interestingly, it leads to a contradiction, as it is shown that a set of NSITs form the necessary and sufficient condition for macrorealism (Eq. 5.8). Equation 5.8 implies that in order to show a violation of macrorealism (MR), at least one of the NSIT conditions (two-time or three-time) is violated, which implies that it is indeed the NIM condition that is

violated, not MRps. Here is the flow of arguments, to better understand the point.

violation of LGI $\rightarrow$ violation of MR (as LGI is necessary condition for MR)

violation of MR $\rightarrow$ violation of atleast one NSIT (from equation 5.8)

violation of NSIT $\rightarrow$ violation of NIM (as derived from equation 5.37 and 5.38)

violation of NIM $\rightarrow$ violation of LGI. So, we cannot actually comment on MRps.

However, this necessary and sufficient condition (5.8) is based on the fact that all joint probabilities are true valid probabilities. So, if we use negative quasi-probabilities instead of true probabilities, then it is possible, in principle, to show a violation of macrorealism while maintaining all NSITs at the same time. For this reason, currently many research works are focused on weak measurement or ambiguous measurement (also called semi-weak) as they produce quasi-probabilities. As for the unambiguous projective measurement, it is theoretically not possible to violate macrorealism without violating NSIT.

In spite of the conclusion presented above, we prefer to stick to the application of strong projective measurement in our setup and come up with a middle ground in terms of closing the loophole. We implement ideal negative result measurement (NRM) as NIM, as proposed in the original LGI paper [76]. In the context of the macrorealist theory, this is the best choice of measurement. However, NRM is not always a good choice of NIM for all existing theories. For example, in quantum mechanics, NRM may collapse the state and hence invasive. Our target is to apply such a measurement technique that is NIM irrespective of the theoretical models. In this regard, we look into the reference [1], where Halliwell introduced a different set of conditions, which is also a necessary and sufficient condition to macrorealism. This notion of macrorealism is however slightly weaker than the previous one (Eq. 5.8), in the context of non-invasiveness. The set of conditions include all two-times NSIT conditions and the three-time LG inequality (Eq. 5.39).

$$MR^* \Leftrightarrow NSIT_{(t_1)t_2} \wedge NSIT_{(t_1)t_3} \wedge NSIT_{(t_2)t_3} \wedge LGI \wedge AoT \quad (5.39)$$

From equation 5.39, we can say that, it is possible to violate MR^* by violating LGI , while at the same time maintaining $NSIT_{(t_1)t_2}$, $NSIT_{(t_1)t_3}$ and $NSIT_{(t_2)t_3}$. Rather than performing measurements at all the three times sequentially, in a single run of the experiment, we perform three piece-wise separate experimental runs to measure the three joint correlations, $\langle Q_{t_1} Q_{t_2} \rangle$, $\langle Q_{t_2} Q_{t_3} \rangle$ and $\langle Q_{t_1} Q_{t_3} \rangle$. While measuring each of the expected correlation values $\langle Q_{t_i} Q_{t_j} \rangle$ we apply negative result measurement (NRM) at time t_i and unambiguous, projective measurement at time t_j . We can ensure that the three separate NRM measurements are independently non-invasive. Now, to determine the accuracy with which such NRMs satisfy NIM, the relevant experimental parameters need to be chosen such that all the pertinent two-time NSITs are quantum mechanically predicted to be satisfied. Consequently, the testing of the validity of these relations would provide a quantitative measure of the extent to which the classical disturbance induced by the NRMs is minimised in the setup we use. We follow the three separate experimental runs given in the Table 5.1 for our experiment.

Experimental runs	Quantity to be measured for LGI	NSIT condition to be satisfied
Exp 1	$\langle Q_{t_2} Q_{t_3} \rangle$	$NSIT_{(t_2)t_3} = P_3(+)-P_{2,t_3}(+,+)-P_{2,t_3}(-,+) =0$
Exp 2	$\langle Q_{t_1} Q_{t_3} \rangle$	$NSIT_{(t_1)t_3} = P_3(+)-P_{1,t_3}(+,+)-P_{1,t_3}(-,+) =0$
Exp 3	$\langle Q_{t_1} Q_{t_2} \rangle$	$NSIT_{(t_1)t_2} = P_2(+)-P_{1,t_2}(+,+)-P_{1,t_2}(-,+) =0$

Table 5.1 Three separate experimental runs are performed instead of a single run; in order to satisfy all relevant two-time NSIT conditions.

A macrorealist may still raise the issue that three separate, piece-wise experiments when combined together may not be the same as a single experiment, and the invasiveness may be introduced in a different degree of freedom. In this context, the notion of macrorealism is slightly weaker for Eq. 5.39, and we can only partially close the clumsiness loophole.

We need to highlight an important additional feature of our setup that arises particularly because of the way we strategise our setup to simultaneously sidestep the detection efficiency loophole. As will be elaborated in the next subsection, apart from using perfect blockers instead of detectors having finite efficiency, a key strategy we employ is as follows. We measure the joint probability $P_{t_1,t_2}(q_{t_1}, q_{t_2})$ and hence the correlation function $\langle Q_{t_1} Q_{t_2} \rangle$

through implementing NRM by placing two blockers jointly in the respective arms of the two interferometers and determining all the three-time joint probabilities $P_{t_1,t_2,t_3}(q_{t_1}, q_{t_2}, q_{t_3})$, $\forall q_{t_i} = \pm 1$. We then obtain the marginal joint probabilities $P_{t_1,t_2}(q_{t_1}, q_{t_2})$ by using the relation (Eq.5.10) at the level of observable probability, implied by the assumption of induction (entailing the absence of retro-causality) stated earlier as an ingredient of the notion of MR.

As will be argued in the next subsection, the measurement of $P_{t_1,t_2}(q_{t_1}, q_{t_2})$ in the above way enables us to show the violation of both LGI and WLGI for any non-zero detection efficiency. Now, since for this procedure, the NRMs are required to be performed at both t_1 and t_2 , in order to witness the precision up to which NIM is satisfied in this case, ideally one would have to test here the quantum mechanically predicted validity of the relevant three-time NSIT conditions involving the placing of blockers at both t_1 and t_2 . However, we argue that in the context of the experiment, satisfying all three-time NSIT conditions are not necessary as they are not relevant. Satisfying only two-time NSITs are sufficient.

$$NSIT_{(t_1)t_2} : P_{t_2}(+) = P_{t_1,t_2}(+, +) + P_{t_1,t_2}(-, +) \quad (5.40)$$

$$\begin{aligned} P_{t_2,t_3}(+, +) + P_{t_2,t_3}(+, -) &= P_{t_1,t_2,t_3}(+, +, +) + P_{t_1,t_2,t_3}(+, +, -) \\ &\quad + P_{t_1,t_2,t_3}(-, +, +) + P_{t_1,t_2,t_3}(-, +, -) \end{aligned} \quad (5.41)$$

Instead of measuring 5.40 directly, we measure 5.41 as both of them are equivalent expression for $NSIT_{(t_1)t_2}$, considering the induction/AoT conditions (5.9, 5.10). Measuring three-time joint probabilities of the form $P_{t_1,t_2,t_3}(q_{t_1}, q_{t_2}, q_{t_3})$ for the equation 5.41 does not necessarily make three-time NSITs relevant, as we are still checking for $NSIT_{(t_1)t_2}$ in equation 5.40.

Another crucial pertinent feature is that these blockers placed in different interferometers are spatially well separated. Hence it is reasonable to argue from classical or macrorealist point of view that even if these blockers would have been placed both at t_1 and t_2 , there would have been negligibly small possibility of their respective local actions influencing each other (say, through some environmental degree of freedom) and producing significant cumulative effect on the measured photon in the other spatially separated arms of the

respective interferometers. Thus, the use of two-time NSIT conditions for verifying the precision of smallness of the classical disturbance induced by the blockers when they are placed separately at t_1 or t_2 suffices for plugging the clumsiness loophole, while also getting around the detection efficiency loophole in the way further explained in the next subsection.

5.3.2 Detection efficiency loophole

To find the macrorealist bound of LGI/WLGI, we inherently assume that all the detector efficiencies are 100%. In a real experiment, it is not true, as most of the available single photon detectors in the market have very low efficiency, which leads to a loophole, where a macrorealist may claim that the measured statistics of the detected sample is different than the whole sample. In most of the cases, experimentalists consider the fair-sampling assumption, where it is assumed that the undetected photons have the same statistics as the detected ones. Hence, by exploiting this detection efficiency loophole, it is possible to reproduce the quantum mechanically predicted measured statistics of the detected sample based on the macrorealist considerations. A similar situation exists in the case of testing local realism for which considerable studies have been done and different approaches have been explored to take into account the effect of detector efficiency in the testing of the relevant inequalities. For example, one of the approaches in terms of the probabilities has been to assign the measurement result 0 to an undetected particle and generalize the Bell-CHSH inequality to include detector inefficiency [46]. Another approach has been to use the correlation functions, but without requiring to assign any measurement result to the undetected particles while incorporating the detection efficiency parameter in the original form of Bell inequality [72].

In our study, we consider a hidden variable approach, inspired by the work [72] done in the case of Bell's inequality, where we find the minimum detection efficiency requirement for LGI and WLGI. We find that the system efficiency requirement for LGI is 85%, and for WLGI it is 78%. We further reduce these requirements by introducing two modifications in the measurement technique. The first one is to replace the detector used for the negative result measurement with a blocker. Here blocker is a metallic blocking device that perfectly absorbs all incident photons, so one can also model it as a detector with 0% efficiency. The second

modification is to place the detection module fixed only at the end of the experiment (at time t_3) and use the arrow of time (AoT) equations (5.9, 5.10) to aid the measurement of joint probabilities. So, to measure $\langle Q_{t_1} Q_{t_3} \rangle$ and $\langle Q_{t_2} Q_{t_3} \rangle$, we place the detection module fixed at t_3 and place the blocker at t_1 and t_2 , respectively. For $\langle Q_{t_1} Q_{t_2} \rangle$ we still fix the detection module at t_3 , instead of t_2 , and place two blockers simultaneously at both t_1 and t_2 , to measure all three-time joint probabilities $P_{t_1, t_2, t_3}(q_{t_1}, q_{t_2}, q_{t_3})$, $\forall q_{t_i} = \pm 1$. All marginal joint probabilities, $P_{t_1, t_2}(q_{t_1}, q_{t_2})$ are calculated using the AoT equations (5.9, 5.10). We show that it is possible to perform the loophole-free version of both the LGI and WLGI experiments with any non-zero detection efficiency.

We consider a hidden-variable model, where detection of a photon is determined by a hidden variable λ of the overall space Λ . The preparation state is defined by the distribution $\rho(\lambda)$, where $\int_{\lambda \in \Lambda} \rho(\lambda) d\lambda = 1$. All λ s undergo probabilistic transformation (T) along with time, i.e., $\lambda(t_i) \rightarrow \lambda'(t_j)$. So, the subspace of Λ which causes detection at time t_i may be in general different from the subspace which causes detection at time t_j . Let's assume that Λ_i is the subspace of overall space Λ in which the system is detected at t_i , such that $\int_{\lambda \in \Lambda_i} \rho(\lambda) d\lambda = \eta$, where η is the efficiency of the detector. The probability distribution for different regions of the hidden variable space is described in Fig. 5.1. The joint probabilities in the different regions are denoted by $q_i, p_i, t_i, a_i, b_i, c_i, d_i$. For instance,

$$\begin{aligned}
 q_1 &= \int_{\lambda \in \Lambda_q} P_{t_1, t_2, t_3}(+, +, + | \lambda) \rho(\lambda) d\lambda, & q_2 &= \int_{\lambda \in \Lambda_q} P_{t_1, t_2, t_3}(+, +, - | \lambda) \rho(\lambda) d\lambda, \\
 q_3 &= \int_{\lambda \in \Lambda_q} P_{t_1, t_2, t_3}(+, -, + | \lambda) \rho(\lambda) d\lambda, & q_4 &= \int_{\lambda \in \Lambda_q} P_{t_1, t_2, t_3}(+, -, - | \lambda) \rho(\lambda) d\lambda, \\
 q_5 &= \int_{\lambda \in \Lambda_q} P_{t_1, t_2, t_3}(-, +, + | \lambda) \rho(\lambda) d\lambda, & q_6 &= \int_{\lambda \in \Lambda_q} P_{t_1, t_2, t_3}(-, +, - | \lambda) \rho(\lambda) d\lambda, \\
 q_7 &= \int_{\lambda \in \Lambda_q} P_{t_1, t_2, t_3}(-, -, + | \lambda) \rho(\lambda) d\lambda, & q_8 &= \int_{\lambda \in \Lambda_q} P_{t_1, t_2, t_3}(-, -, - | \lambda) \rho(\lambda) d\lambda,
 \end{aligned} \tag{5.42}$$

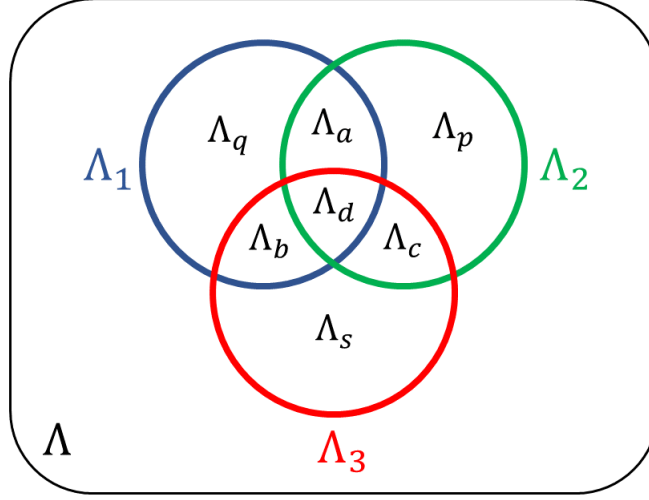


Fig. 5.1 The overall ‘hidden-variable’ state space is Λ . Its subspaces $\Lambda_1, \Lambda_2, \Lambda_3$ for which the photon is detected at t_1, t_2, t_3 are respectively represented by blue, green and red circles. All the detectors are assumed to have the same detection efficiency. Different subspaces within $\Lambda_1 \cup \Lambda_2 \cup \Lambda_3$ are denoted by the symbols q, p, s, a, b, c, d .

Similarly, we define $p_i, s_i, a_i, b_i, c_i, d_i$ for the respective subspaces $\Lambda_p, \Lambda_s, \Lambda_a, \Lambda_b, \Lambda_c, \Lambda_d$. Further, we denote the contribution arising from $\rho(\lambda)$ on the subspace Λ_q by

$$q = \int_{\lambda \in \Lambda_q} \rho(\lambda) d\lambda = \sum_{i=1}^8 q_i, \quad (5.43)$$

and similarly, for the other subspaces

$$p = \sum_{i=1}^8 p_i, \quad s = \sum_{i=1}^8 s_i, \quad a = \sum_{i=1}^8 a_i, \quad b = \sum_{i=1}^8 b_i, \quad c = \sum_{i=1}^8 c_i, \quad d = \sum_{i=1}^8 d_i. \quad (5.44)$$

Based on the above considerations, we now present the analyses pertaining to the two different experimental setups we have invoked.

Case 1: The setup involving only detectors.

First, we consider the scenario where three detectors are used to observe the joint prob-

abilities in our setup. For example, if we want to measure $P_{t_1, t_2}(+, +)$ using negative result measurement, we place a detector D1 in the ‘-1’ arm at t_1 and two detectors, say, D2 and D3, in the arms ‘+1’ and ‘-1’ at t_2 . The joint probability is given by

$$\begin{aligned} P_{t_1, t_2}(+, +) &= \frac{\text{Number of photons detected at D2}}{\text{Total number of photons detected at three detectors}} \\ &= \frac{C_{t_1, t_2}(+, +)}{C_{t_1, t_2}(+, +) + C_{t_1, t_2}(+, -) + C_{t_1}(-)} \end{aligned} \quad (5.45)$$

Here, $C_{t_1, t_2}(+, +)$ denotes the number of events when a heralded single photon is detected in the detector D2. $C_{t_1, t_2}(+, -)$ denotes the number of events when a heralded single photon is detected in the detector D3. $C_{t_1}(-)$ denotes the number of events when a heralded single photon is detected in the detector D1. In terms of the hidden variable model, we can write this as,

$$\begin{aligned} P_{t_1, t_2}(+, +) &= \frac{\int_{\lambda \in \Lambda_2} P_{t_1, t_2}(+, +|\lambda) \rho(\lambda) d\lambda}{\int_{\lambda \in \Lambda_2} P_{t_1, t_2}(+, +|\lambda) \rho(\lambda) d\lambda + \int_{\lambda \in \Lambda_2} P_{t_1, t_2}(+, -|\lambda) \rho(\lambda) d\lambda + \int_{\lambda \in \Lambda_1} P_{t_1}(-|\lambda) \rho(\lambda) d\lambda} \\ &= \frac{\int_{\lambda \in \Lambda_2} P_{t_1, t_2}(+, +|\lambda) \rho(\lambda) d\lambda}{\int_{\lambda \in \Lambda_2} P_{t_1}(+|\lambda) \rho(\lambda) d\lambda + \int_{\lambda \in \Lambda_1} P_{t_1}(-|\lambda) \rho(\lambda) d\lambda} \end{aligned} \quad (5.46)$$

Using equation 5.42 and 5.46, joint correlation values are written in the following form.

$$\begin{aligned}
\langle Q_{t_1} Q_{t_2} \rangle &= P_{t_1, t_2}(+, +) - P_{t_1, t_2}(+, -) - P_{t_1, t_2}(-, +) + P_{t_1, t_2}(-, -) \\
&= \frac{\int_{\lambda \in \Lambda_2} P_{t_1, t_2}(+, +|\lambda) \rho(\lambda) d\lambda - \int_{\lambda \in \Lambda_2} P_{t_1, t_2}(+, -|\lambda) \rho(\lambda) d\lambda}{\int_{\lambda \in \Lambda_2} P_{t_1}(+|\lambda) \rho(\lambda) d\lambda + \int_{\lambda \in \Lambda_1} P_{t_1}(-|\lambda) \rho(\lambda) d\lambda} \\
&\quad + \frac{\int_{\lambda \in \Lambda_2} P_{t_1, t_2}(-, -|\lambda) \rho(\lambda) d\lambda - \int_{\lambda \in \Lambda_2} P_{t_1, t_2}(-, +|\lambda) \rho(\lambda) d\lambda}{\int_{\lambda \in \Lambda_2} P_{t_1}(-|\lambda) \rho(\lambda) d\lambda + \int_{\lambda \in \Lambda_1} P_{t_1}(+|\lambda) \rho(\lambda) d\lambda} \quad (5.47) \\
&= \frac{\sum_{i=1,2} (a_i + c_i + d_i + p_i) - \sum_{i=3,4} (a_i + c_i + d_i + p_i)}{a + d + \sum_{i=1,2,3,4} (c_i + p_i) + \sum_{i=5,6,7,8} (b_i + q_i)} \\
&\quad + \frac{\sum_{i=7,8} (a_i + c_i + d_i + p_i) - \sum_{i=5,6} (a_i + c_i + d_i + p_i)}{a + d + \sum_{i=5,6,7,8} (c_i + p_i) + \sum_{i=1,2,3,4} (b_i + q_i)}
\end{aligned}$$

Similar to the equation 5.47, we can also write expressions for $\langle Q_{t_2} Q_{t_3} \rangle$ and $\langle Q_{t_1} Q_{t_3} \rangle$, and put them in the expression of the LGI below.

$$\begin{aligned}
LGI: & \langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle \\
&= \frac{\sum_{i=1,2} (a_i + c_i + d_i + p_i) - \sum_{i=3,4} (a_i + c_i + d_i + p_i)}{a + d + \sum_{i=1,2,3,4} (c_i + p_i) + \sum_{i=5,6,7,8} (b_i + q_i)} \\
&+ \frac{\sum_{i=7,8} (a_i + c_i + d_i + p_i) - \sum_{i=5,6} (a_i + c_i + d_i + p_i)}{a + d + \sum_{i=5,6,7,8} (c_i + p_i) + \sum_{i=1,2,3,4} (b_i + q_i)} \\
&+ \frac{\sum_{i=1,5} (b_i + c_i + d_i + t_i) - \sum_{i=2,6} (b_i + c_i + d_i + t_i)}{c + d + \sum_{i=1,2,5,6} (b_i + t_i) + \sum_{i=3,4,7,8} (a_i + p_i)} \\
&+ \frac{\sum_{i=4,8} (b_i + c_i + d_i + t_i) - \sum_{i=3,7} (b_i + c_i + d_i + t_i)}{c + d + \sum_{i=3,4,7,8} (b_i + t_i) + \sum_{i=1,2,5,6} (a_i + p_i)} \\
&- \frac{\sum_{i=1,3} (b_i + c_i + d_i + t_i) - \sum_{i=2,4} (b_i + c_i + d_i + t_i)}{b + d + \sum_{i=1,2,3,4} (c_i + t_i) + \sum_{i=5,6,7,8} (a_i + q_i)} \\
&- \frac{\sum_{i=6,8} (b_i + c_i + d_i + t_i) - \sum_{i=5,7} (b_i + c_i + d_i + t_i)}{b + d + \sum_{i=5,6,7,8} (c_i + t_i) + \sum_{i=1,2,3,4} (a_i + q_i)}
\end{aligned} \tag{5.48}$$

The right-hand-side of the above equation is maximized under two constraints: (i) the normalized condition, that is,

$$\sum_{i=1}^8 (p_i + q_i + t_i + a_i + b_i + c_i + d_i) \leq 1; \tag{5.49}$$

and (ii) the detection efficiency of the detectors is η ,

$$\sum_{i=1}^8 (p_i + a_i + b_i + d_i) = \sum_{i=1}^8 (q_i + a_i + c_i + d_i) = \sum_{i=1}^8 (t_i + b_i + c_i + d_i) = \eta. \tag{5.50}$$

Whenever $\eta < 2/3$, the maximum is obtained when

$$a_7 = b_5 = c_1 = \frac{\eta}{2}, \quad (5.51)$$

and all other parameters are zero. For such value of parameters, the right-hand-side of (5.48) is $8/3$, which is larger than the maximum quantum value of LGI. When $\eta \geq 2/3$, the maximum is found for

$$a_1 = b_4 = c_1 = 1 - \eta, \quad d_1 = 3\eta - 2, \quad (5.52)$$

and other parameters are zero, such that the expression in (5.48) simplifies to $2/\eta - \eta$. Thus, taking into account the detection efficiency loophole, the LGI modifies as follows,

$$\langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle \leq \begin{cases} \frac{8}{3}, & \text{for } \eta < \frac{2}{3} \\ \frac{2}{\eta} - \eta, & \text{for } \eta \geq \frac{2}{3}. \end{cases} \quad (5.53)$$

Now, considering the maximum quantum value 1.5 of the LGI expression, it follows from (5.53) that a realist hidden variable model reproduces all quantum predictions up to that maximum value whenever

$$\frac{2}{\eta} - \eta \leq 1.5 \implies \eta \leq 0.8508. \quad (5.54)$$

Thus, in order to close the detection efficiency loophole in this case for testing LGI, one requires $\eta > 0.851$.

Next, considering the WLGI expression given by (5.11), it takes the following form

$$\begin{aligned}
WLGI : & P_{t_1,t_3}(-,+) - P_{t_1,t_2}(-,+) - P_{t_2,t_3}(-,+) \\
&= \frac{\int_{\lambda \in \Lambda_3} P_{t_1,t_3}(-, +|\lambda) \rho(\lambda) d\lambda}{\int_{\lambda \in \Lambda_3} P_{t_1}(-|\lambda) \rho(\lambda) d\lambda + \int_{\lambda \in \Lambda_1} P_{t_1}(+|\lambda) \rho(\lambda) d\lambda} \\
&\quad - \frac{\int_{\lambda \in \Lambda_2} P_{t_1,t_2}(-, +|\lambda) \rho(\lambda) d\lambda}{\int_{\lambda \in \Lambda_2} P_{t_1}(-|\lambda) \rho(\lambda) d\lambda + \int_{\lambda \in \Lambda_1} P_{t_1}(+|\lambda) \rho(\lambda) d\lambda} \\
&\quad - \frac{\int_{\lambda \in \Lambda_3} P_{t_2,t_3}(-, +|\lambda) \rho(\lambda) d\lambda}{\int_{\lambda \in \Lambda_3} P_{t_2}(-|\lambda) \rho(\lambda) d\lambda + \int_{\lambda \in \Lambda_2} P_{t_2}(+|\lambda) \rho(\lambda) d\lambda} \\
&= \frac{\sum_{i=5,7} (b_i + c_i + d_i + t_i)}{b + d + \sum_{i=5,6,7,8} (c_i + t_i) + \sum_{i=1,2,3,4} (a_i + q_i)} \\
&\quad - \frac{\sum_{i=5,6} (a_i + c_i + d_i + p_i)}{a + d + \sum_{i=5,6,7,8} (c_i + p_i) + \sum_{i=1,2,3,4} (b_i + q_i)} \\
&\quad - \frac{\sum_{i=3,7} (b_i + c_i + d_i + t_i)}{c + d + \sum_{i=3,4,7,8} (b_i + t_i) + \sum_{i=1,2,5,6} (a_i + p_i)} \tag{5.55}
\end{aligned}$$

It can be verified that whenever $\eta < 2/3$, the above quantity is 1 for the choice of parameter values given in (5.51). For $\eta \geq 2/3$, the maximum value of right-hand-side of (5.55) is obtained when all other parameters are zero except

$$a_7 = b_5 = c_1 = 1 - \eta, \quad d_1 = 3\eta - 2, \tag{5.56}$$

such that the expression in (5.55) simplifies to $(1 - \eta)/(2\eta - 1)$. Subsequently, we have the modified form of WLGI,

$$P_{t_1,t_3}(-,+) - P_{t_1,t_2}(-,+) - P_{t_2,t_3}(-,+) \leq \begin{cases} 1, & \text{for } \eta < \frac{2}{3} \\ \frac{1-\eta}{2\eta-1}, & \text{for } \eta \geq \frac{2}{3}. \end{cases} \tag{5.57}$$

Taking into account the maximum quantum value 0.4034 of the WLG expression, it follows from (5.57) that a realist model reproduces all quantum predictions up to that maximum value whenever

$$\frac{1 - \eta}{2\eta - 1} \leq 0.4034 \implies \eta \leq 0.78. \quad (5.58)$$

Thus, in order to close the detection efficiency loophole in this case for testing WLG, one requires $\eta > 0.78$.

Case 2: The setup involving detectors and blockers.

For the modified version of the setup, all detectors used for negative result measurement are replaced by ideal blockers, and detectors are placed only at time t_3 . So, only the subspace Λ_3 is relevant for the calculation. For example, joint probability $P_{t_1, t_3}(+, +)$ is written in terms of hidden variable as,

$$\begin{aligned} P_{t_1, t_3}(+, +) &= \frac{\int_{\lambda \in \Lambda_3} P_{t_1, t_3}(+, +|\lambda) \rho(\lambda) d\lambda}{\int_{\lambda \in \Lambda_3} P_{t_1}(+|\lambda) \rho(\lambda) d\lambda + \int_{\lambda \in \Lambda_3} P_{t_1}(-|\lambda) \rho(\lambda) d\lambda} = \frac{\int_{\lambda \in \Lambda_3} P_{t_1, t_3}(+, +|\lambda) \rho(\lambda) d\lambda}{\int_{\lambda \in \Lambda_3} \rho(\lambda) d\lambda} \\ &= \frac{\int_{\lambda \in \Lambda_3} P_{t_1, t_3}(+, +|\lambda) \rho(\lambda) d\lambda}{\eta} \end{aligned} \quad (5.59)$$

Similar expression (equation 5.59) is valid for joint probabilities of the form $P_{t_2, t_3}(q_{t_2}, q_{t_3})$. However, for probabilities of the form $P_{t_1, t_2}(q_{t_1}, q_{t_2})$, we have to consider an additional step of including AoT expression (equation 5.10) in the calculations.

$$\begin{aligned} P_{t_1, t_2}(+, +) &= P_{t_1, t_2, t_3}(+, +, +) + P_{t_1, t_2, t_3}(+, +, -) \\ &= \frac{\int_{\lambda \in \Lambda_3} \{P_{t_1, t_2, t_3}(+, +, +|\lambda) + P_{t_1, t_2, t_3}(+, +, -|\lambda)\} \rho(\lambda) d\lambda}{\eta} \\ &= \frac{\int_{\lambda \in \Lambda_3} P_{t_1, t_2}(+, +|\lambda) \rho(\lambda) d\lambda}{\eta} \end{aligned} \quad (5.60)$$

Joint correlation values are expressed in the similar form as mentioned in equation 5.47. For example,

$$\begin{aligned}
 \langle Q_{t_1} Q_{t_3} \rangle &= P_{t_1, t_3}(+, +) - P_{t_1, t_3}(+, -) - P_{t_1, t_3}(-, +) + P_{t_1, t_3}(-, -) \\
 &= \frac{\int_{\lambda \in \Lambda_3} \{P_{t_1, t_3}(+, +|\lambda) - P_{t_1, t_3}(+, -|\lambda) - P_{t_1, t_3}(-, +|\lambda) + P_{t_1, t_3}(-, -|\lambda)\} \rho(\lambda) d\lambda}{\eta} \\
 &= \frac{\int_{\lambda \in \Lambda_3} \langle Q_{t_1} Q_{t_3} \rangle_{\lambda} \rho(\lambda) d\lambda}{\eta}
 \end{aligned} \tag{5.61}$$

$$\langle Q_{t_1} Q_{t_2} \rangle = \frac{\int_{\lambda \in \Lambda_3} \langle Q_{t_1} Q_{t_2} \rangle_{\lambda} \rho(\lambda) d\lambda}{\eta}, \quad \langle Q_{t_2} Q_{t_3} \rangle = \frac{\int_{\lambda \in \Lambda_3} \langle Q_{t_2} Q_{t_3} \rangle_{\lambda} \rho(\lambda) d\lambda}{\eta} \tag{5.62}$$

Hence, the LGI expression involves integration only on the subspace of Λ_3 and reduces to the following form,

$$\begin{aligned}
 LGI: \quad & \langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle \\
 &= \frac{\int_{\lambda \in \Lambda_3} \{\langle Q_{t_1} Q_{t_2} \rangle_{\lambda} + \langle Q_{t_2} Q_{t_3} \rangle_{\lambda} - \langle Q_{t_1} Q_{t_3} \rangle_{\lambda}\} \rho(\lambda) d\lambda}{\eta} \leq 1
 \end{aligned} \tag{5.63}$$

The above inequality uses the equation $\int_{\lambda \in \Lambda_3} \rho(\lambda) = \eta$ and the fact that $\langle Q_{t_1} Q_{t_2} \rangle_{\lambda} + \langle Q_{t_2} Q_{t_3} \rangle_{\lambda} - \langle Q_{t_1} Q_{t_3} \rangle_{\lambda} \leq 1$ for all hidden variables λ (proven in Section 5.2). Similarly, the WLGI expression given by (5.11) reduces to the following form,

$$\begin{aligned}
 WLGI: \quad & P_{t_1, t_3}(-, +) - P_{t_1, t_2}(-, +) - P_{t_2, t_3}(-, +) \\
 &= \frac{\int_{\lambda \in \Lambda_3} \{P_{t_1, t_3}(-, +|\lambda) - P_{t_1, t_2}(-, +|\lambda) - P_{t_2, t_3}(-, +|\lambda)\} \rho(\lambda) d\lambda}{\eta} \leq 0
 \end{aligned} \tag{5.64}$$

The above inequality also uses the equation $\int_{\lambda \in \Lambda_3} \rho(\lambda) = \eta$ and the fact that $P_{t_1, t_3}(-, +|\lambda) - P_{t_1, t_2}(-, +|\lambda) - P_{t_2, t_3}(-, +|\lambda) \leq 0$ for all hidden variables λ (proven in Section 5.2).

Both equations 5.63 and 5.64 are valid for any non-zero efficiency, η . Therefore, we

conclude that any quantum mechanical violation of LGI/WLGI for this setup cannot be reproduced by a macrorealist model, whatever be the detection efficiency.

5.3.3 Other loopholes

We use heralded single photons generated from an SPDC source in our experiment. This, along with appropriate data collection and post-processing strategy, helps us to close other loopholes like multiple emission loophole, coincidence loophole, preparation state loophole, etc.

Multiple emission loophole: We begin by noting that the notion of macrorealism underlying the derivation of the form of macrorealist inequalities used in our experimental study assumes that any observable property has a definite pre-existent value that is revealed by measurement. This entails that the respective measurements involved in the experimental test of such macrorealist inequality need to have single outcomes, which is also required to satisfy the NIM postulate. Thus, it is of considerable importance to incorporate in our analysis the effect of any possible departure from this condition that can occur in the experimental study such as that of ours, primarily arising from the non-idealness of the single-photon source which will imply the presence of photons in two different paths at a time in the experiment arrangement considered. This we may call the multiple emission loophole. To address this issue, first, we define a suitable parameter, say, γ , characterizing fraction of the sample space or the total set of runs that corresponds to the occurrence of multi photons within the experimental setup, as follows

$$\gamma = \frac{\text{number of events where multiphoton is obtained}}{\text{total number of events}}. \quad (5.65)$$

An estimate of this parameter from empirical considerations can be obtained in the context of the experimental setup considered. A nonvanishing value of this parameter would give rise to a pseudo violation of the macrorealist inequalities. By taking this into account, to obtain the modified upper bound of the relevant macrorealist inequalities, it is then necessary to

obtain the maximum possible magnitude of a pseudo violation of any such inequality in the simultaneous presence of photons in multiple paths within the experimental setup. We show that in-principle there exists an internally consistent model of two photons each of which is present in two different paths, which can lead to the maximum algebraic bound. So, the modified upper bound for LGI/WLGI can be written as,

$$\text{maximum upper bound} = \gamma \times \text{algebraic upper bound} + (1 - \gamma) \times \text{macrorealist upper bound} \quad (5.66)$$

Now, considering the case of LGI, we first show that there exists a realist model of two photons, each of which is present in either of the two different paths, for which the LGI expression attains its algebraic upper bound. To describe such a model, let us denote the hidden-variable state λ^1, λ^2 for photons 1 and 2 respectively. Due to the presence of both these photons, they may mutually influence each other on arriving at the beamsplitter simultaneously, which, in turn, can affect their subsequent individual behaviors.

Now, recall that we place a blocker at t_1 (either in path ‘+1’ or path ‘−1’) for implementing the negative result measurement to obtain the joint probabilities $P_{t_1, t_3}(q_{t_1}, q_{t_3}), P_{t_1, t_2}(q_{t_1}, q_{t_2})$, while we do not place any blocker at t_1 to obtain the joint probabilities $P_{t_2, t_3}(q_{t_2}, q_{t_3})$. If the two photons are present simultaneously in the two different paths at t_1 and there is no blocker placed at t_1 , the photons may influence each other at the second beamsplitter just before t_2 . Hence, in principle, the behavior of the photon which is present at t_2 depends on whether a blocker is placed at t_1 or not.

Further, to specify the realist model of two photons we are considering, we take the joint probability distributions of the measurement outcomes at t_1, t_2, t_3 to be given by the following expressions for all λ^1, λ^2 ,

$$P_{t_1, t_2, t_3}^1(+, +, + | \lambda^1, N_1) = 1, \quad P_{t_1, t_2, t_3}^2(-, -, - | \lambda^2, N_1) = 1, \quad (5.67)$$

$$P_{t_1, t_2, t_3}^1(+, +, - | \lambda^1, B_1-) = 1, \quad P_{t_1, t_2, t_3}^2(-, -, + | \lambda^2, B_1+) = 1, \quad (5.68)$$

where P^i denotes the probability distribution for the photon $i \in \{1, 2\}$, and N_1 denotes the configuration in which no blocker is placed at t_1 , $B_1 \pm$ denotes the configuration in which the blocker is placed at t_1 in the ' ± 1 ' path.

Now, for the realist model specified by the relations (Eqs. 5.67, 5.68), let us evaluate the joint probabilities $P_{t_1, t_3}(q_{t_1}, q_{t_3})$, $P_{t_1, t_2}(q_{t_1}, q_{t_2})$, $P_{t_2, t_3}(q_{t_2}, q_{t_3})$ measured in our experimental setup (details of the experimental procedure for measuring all joint probabilities have been provided in Section 5.4.2). For example, the joint probabilities $P_{t_2, t_3}(q_{t_2}, q_{t_3})$ are obtained from the relations (5.67) for which we do not place any blocker at t_1 . For this purpose, we place a blocker at t_2 and two detectors, say, D_+ and D_- , at t_3 in ' ± 1 ' path. When the blocker is placed in the '-1' path, we observe clicks only at D_+ , since from (5.67) we know that photon 2 is blocked at t_2 and photon 1 is in the '+1' path all the time. Likewise, when the blocker is placed in the '+1' path, we observe clicks only at D_- , since from (5.67) we know that photon 1 is blocked at t_2 and photon 2 is in the '-1' path all the time.

Next, we relate the quantities $P_{t_2, t_3}(q_{t_2}, q_{t_3})$ to the actual observed coincidence counts. Let N to be the total number of photons in each of the two sets of runs corresponding to each of the two configurations (the blocker being placed in ' ± 1 ' path at t_2) respectively. Then, in view of what has been explained above using the relation (5.67), it follows that the relevant coincidence counts are given by

$$C_{t_2, t_3}(+, +) = C_{t_2, t_3}(-, -) = N, \quad C_{t_2, t_3}(+, -) = C_{t_2, t_3}(-, +) = 0. \quad (5.69)$$

Thus, we obtain the joint probabilities by using the relation,

$$P_{t_2, t_3}(q_{t_2}, q_{t_3}) = C_{t_2, t_3}(q_{t_2}, q_{t_3}) / \sum_{q_{t_2}=\pm 1, q_{t_3}=\pm 1} C_{t_2, t_3}(q_{t_2}, q_{t_3}).$$

$$P_{t_2, t_3}(+, +) = P_{t_2, t_3}(-, -) = \frac{1}{2}, \quad P_{t_2, t_3}(+, -) = P_{t_2, t_3}(-, +) = 0. \quad (5.70)$$

Similarly, following the above procedure, we can obtain the other joint probabilities $P_{t_1,t_3}(q_{t_1}, q_{t_3})$, $P_{t_1,t_2}(q_{t_1}, q_{t_2})$ from the relations (Eq. 5.68), which are given as follows

$$\begin{aligned} P_{t_1,t_3}(+, +) &= P_{t_1,t_3}(-, -) = 0, \quad P_{t_1,t_3}(+, -) = P_{t_1,t_3}(-, +) = \frac{1}{2}, \\ P_{t_1,t_2}(+, +) &= P_{t_1,t_2}(-, -) = \frac{1}{2}, \quad P_{t_1,t_2}(+, -) = P_{t_1,t_2}(-, +) = 0. \end{aligned} \quad (5.71)$$

Using these joint probabilities (Eqs. 5.70, 5.71), one can readily show that $\langle Q_{t_1} Q_{t_2} \rangle = \langle Q_{t_2} Q_{t_3} \rangle = -\langle Q_{t_1} Q_{t_3} \rangle = 1$. Hence, for the realist model specified by the relations (Eqs. 5.67, 5.68), the value of the LGI expression attains its algebraic maximum value 3.

It then follows from (5.66) that the upper bound of LGI given in (5.12) is modified to (5.72).

$$\langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle \leq 1 + 2\gamma. \quad (5.72)$$

Next, by following the similar reasoning as above, one can show that the WLGI expression given by (5.11) attains the maximum value 1/2 for the two-photon realist model specified above by the relations (Eqs. 5.67, 5.68). It can then be shown that the WLGI given by (5.11) is modified to (5.73).

$$P_{t_1,t_3}(-, +) - P_{t_1,t_2}(-, +) - P_{t_2,t_3}(-, +) \leq \frac{\gamma}{2}. \quad (5.73)$$

For the SPDC based heralded single photon source used in our experiment with low pump power and suitable filtering, the probability of producing multiple photons is very small compared to that using other sources like a weak coherent pulse. Now, in order to estimate the precise value of the modified upper bound of LGI/WLGI relevant to our experiment, we follow the procedure for measuring γ whose specifics are discussed in Section 5.6.4. This is based on our experimental data pertaining to a set of measured relevant single counts and coincidence counts, along with the values of the key parameters of our setup like the beamsplitting ratios and detector efficiencies. As shown in Section 5.6.4, the value of the parameter γ evaluated in this way turns out to be 0.0023. Putting this value of γ in Eqs. 5.72

and 5.73, the modified upper bounds of LGI and WLGI are found to be 1.0046 and 0.0012 respectively. Thus, in our experiment, the changes in the upper bound of the LGI/WLGI due to the contribution from the possible presence of multiple photons are ensured to be indeed negligibly small in comparison with the observed magnitudes of the violations of these inequalities.

Coincidence loophole: In a Bell-type experiment, the coincidence loophole [73] arises from the fact that different measurement settings may introduce different time delays between the two photons of each pair, which results in an asymmetric detection of correlated photon pairs within a predefined coincidence time window. In the case of an LGI type experiment, though we only deal with single photons, a similar type of loophole may arise when different measurement settings introduce time variation in the arrival time of the photons, leading to asymmetric detection for a fixed detection window. For the heralded single photon used in our LGI experiment, the heralding photon (the other photon of the same pair) is used for the timing reference, so even if there is an asymmetric time delay to the heralded photon, in the post-processing stage we select appropriate coincidence window for different measurement settings, to nullify this.

In the experimental setup, all single photon detectors (SPAD2+, SPAD2-) are fixed at time t_3 , and different measurement settings are realized by changing the position of the blockers only. Now, consider a general scenario where these different measurement settings introduce different path lengths for the photons to traverse inside the setup before getting detected in SPAD2+ or SPAD2-. For example, let us consider two measurement settings where the blocker is placed at time t_1 in the +1 arm for the first setting and in the -1 arm for the second setting. If there is a difference in path length between the +1 and -1 arm, then a photon will take different time (say T for +1 arm, $T + \tau$ for -1 arm) to reach the detectors.

Suppose one uses non-heralded single photons for the experiment. In that case, a detection time window needs to be preset in order to reduce the background noise, as non-heralded single photons do not have any timing references. In the case of different path lengths

introduced by different measurement settings, a preset detection time window is disadvantageous. For example, if one fixes the time window around T , then photons traversing +1 arm have higher chances of getting detected than photons traveling -1 arm. This may introduce inaccurate joint probability distribution such that even a macrorealist theory may produce a false violation of LGI/WLGI.

In light of the above discussion, the usage of heralded single photon for the experimental test of macrorealism has a certain advantage, as will be discussed next. Single photons generated from an SPDC source always come as a pair, or in other words, two photons from each pair are time-correlated. We use the arrival time of the heralding photon (in SPAD1) as the timing reference for the heralded single photon that goes to the experimental setup. So, instead of any preset detection time window, we measure the coincidence between the heralding and the heralded photon (or between SPAD1 and SPAD2+/SPAD2-) in the post-processing stage. Now, going back to the two different measurement settings mentioned earlier. In the case of all the photons that go through the +1 arm, they form a coincidence peak around time T with the heralding photon. So, we place a coincidence window at full-width-half-maxima (FWHM) around the peak position. On the other hand, the photons passing through the -1 arm form the coincidence peak with the heralding photon, at a shifted position $T + \tau$. We place the FWHM coincidence window around $T + \tau$ for the second case. So, by adjusting the coincidence window for different measurement settings, we have nullified any error introduced by the photon-time shift occurring due to different settings.

Preparation state loophole: For the photons which get detected in the experiment, it is always assumed that they are generated with the same preparation state $\rho(\lambda)$. If $\rho(\lambda)$ is different for different photons, then a macrorealist hidden-variable model can also violate LG type inequalities. There is no direct procedure to verify if the preparation state is the same or not, however, we can safely assume that photons generated from a specific physical process from a unique source have the same preparation states. In a real setup, a detector detects photons from multiple sources, including background stray noises. In our case, as we use a heralded single photon source, we post-select only those detected photons that are

coming from the source and not from the background, by fixing a coincidence time-window which provides a high signal to noise ratio, as well as subtracting accidental coincidences.

Memory loophole: We can, in principle, also close the memory loophole [7], by randomizing the three different measurement processes. However, for a continuously pumped SPDC based source, which is probabilistic in nature, it is technically difficult to implement. In the case of a deterministic source, where single photons can be generated on-demand or have periodicity, we can use four fast motorized rotatable blockers in the four arms of the setup, which then can be controlled (either blocks the path or not) based on input random seeds.

5.4 Experimental setup

Generally, the experimental setup to check the violation of macrorealism consists of three stages, preparation (P), unitary transformation (U_{t_i, t_j}), and measurement (M_{t_k}). For the simplest case of three-time inequalities, measurements are carried out at three time intervals (M_{t_1} , M_{t_2} , and M_{t_3}), with unitary transformations (U_{t_1, t_2} , and U_{t_2, t_3}) in between. In order to maintain the second assumption (NIM assumption) in the formalism of macrorealism, measurement M_{t_1} and M_{t_2} need to be non-invasive. Measurement M_{t_3} need not be non-invasive necessarily, as this measurement is performed at the end of the experiment.

Fig. 5.2 depicts a schematic of the experiment where each measurement measures a dichotomic variable Q , having two eigenvalues $+1$, and -1 , representing two possible outcomes of the measurement. The task for an experimentalist is to measure different joint probabilities of the form $P_{t_i, t_j}(q_{t_i}, q_{t_j})$, $P_{t_i, t_j, t_k}(q_{t_i}, q_{t_j}, q_{t_k})$ and the correlation values $\langle Q_{t_i} Q_{t_j} \rangle$, from the experiment and use them to check the violation of different inequalities. For example, in the LGI experiment, one has to measure correlation values $\langle Q_{t_1} Q_{t_2} \rangle$, $\langle Q_{t_2} Q_{t_3} \rangle$ and $\langle Q_{t_1} Q_{t_3} \rangle$. One way of measuring is to measure all three observables Q_{t_1} , Q_{t_2} , and Q_{t_3} sequentially, in a single run of the experiment, and form the three correlation values. But, it is necessary to show that the measurements at time t_1 and t_2 are non-invasive, by showing that all no-signaling in time conditions (both two and three-time NSITs in Eqs. 5.5, 5.6 and 5.7) are satisfied. Another

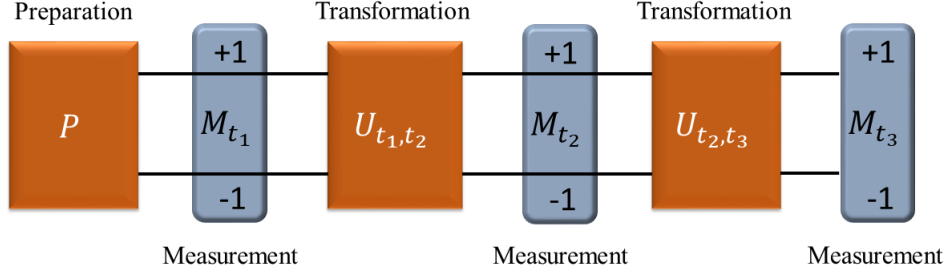


Fig. 5.2 Schematic of the basic design of the experiment.

way of measurement is to run three separate experiments where the three correlation values are measured separately. It can be shown that each measurement is piecewise non-invasive, as it is possible to maintain all relevant two-time NSIT conditions (Eq. 5.5) while violating LGI and WLGI.

In this work, we follow the second way of measurement, as it helps us to close the clumsiness loophole in the experiment (as discussed in Section 5.3.1). We first describe the basic schematic of a single-photon based optical setup. Then we show how we modify the setup to close all the loopholes. We also apply a modification to increase the stability of the setup, at the same time maintaining the simplicity of the design. In the end, we describe the whole setup in detail along with the steps that we follow to measure various joint probabilities and correlation values from the measured datasets.

5.4.1 Basic design of the setup

Our aim is to design a simple experimental setup, based on all-optical components, where all relevant inequalities constructed on the conditions of macrorealism can be easily tested.

In the schematic described in Fig. 5.3, the preparation part (P) consists of a single photon source and a non-polarizing beamsplitter ($BS1$) with a splitting ratio of $T_1 : R_1$. Unitary transformation U_{t_1, t_2} is simulated as a combination of a phase modulator which shift the initial phase with an angular value of θ_1 and a beamsplitter ($BS2$) with splitting ratio of $T_2 : R_2$. Similarly, U_{t_2, t_3} is simulated as a combination of a phase modulator (θ_2) and a beamsplitter ($BS3$) with splitting ratio $T_3 : R_3$. Measurement M_{t_1} is performed anywhere between $BS1$ and $BS2$. Measurement M_{t_2} is performed anywhere between $BS2$ and $BS3$. Measurement M_{t_3} is performed after $BS3$. M_{t_1} and M_{t_2} have to be non-invasive measurements. In our case, we have implemented negative result measurement (NRM) as non-invasive measurement (NIM), which was originally proposed by Leggett and Garg [76], and has been used in many experiments.

The strategy for NRM is that we put only one detector in any one arm (let's say -1 arm) at any time, and consider only those photons which do not interact with that detector. If a detector is placed at -1 arm at time t_1 , and a photon is detected in $+1$ or -1 arm at a later time t_2 , that implies that the photon must have traversed the path $+1$ at time t_1 , in a non-invasive way, as it does not have any interaction with the detector at t_1 .

We calculate all joint probabilities for a single photon sent to the experimental setup, according to the prediction of quantum mechanics (QM). Here, $T_i + R_i = 1$, $\forall i = \{1, 2, 3\}$.

$$P_{t_1, t_2}(+, +) = T_1 T_2, \quad P_{t_1, t_2}(+, -) = T_1 R_2, \quad P_{t_1, t_2}(-, +) = R_1 R_2, \quad P_{t_1, t_2}(-, -) = R_1 T_2, \quad (5.74)$$

$$P_{t_2, t_3}(+, +) = (T_1 T_2 + R_1 R_2 - 2\cos(\theta_1)\sqrt{T_1 T_2 R_1 R_2})T_3 \quad (5.75)$$

$$P_{t_2, t_3}(+, -) = (T_1 T_2 + R_1 R_2 - 2\cos(\theta_1)\sqrt{T_1 T_2 R_1 R_2})R_3, \quad (5.76)$$

$$P_{t_2, t_3}(-, +) = (T_1 R_2 + R_1 T_2 + 2\cos(\theta_1)\sqrt{T_1 T_2 R_1 R_2})R_3 \quad (5.77)$$

$$P_{t_2, t_3}(-, -) = (T_1 R_2 + R_1 T_2 + 2\cos(\theta_1)\sqrt{T_1 T_2 R_1 R_2})T_3, \quad (5.78)$$

$$P_{t_1, t_3}(+, +) = (T_1 T_2 + R_1 R_2 - 2\cos(\theta_1)\sqrt{T_1 T_2 R_1 R_2})T_3 \quad (5.79)$$

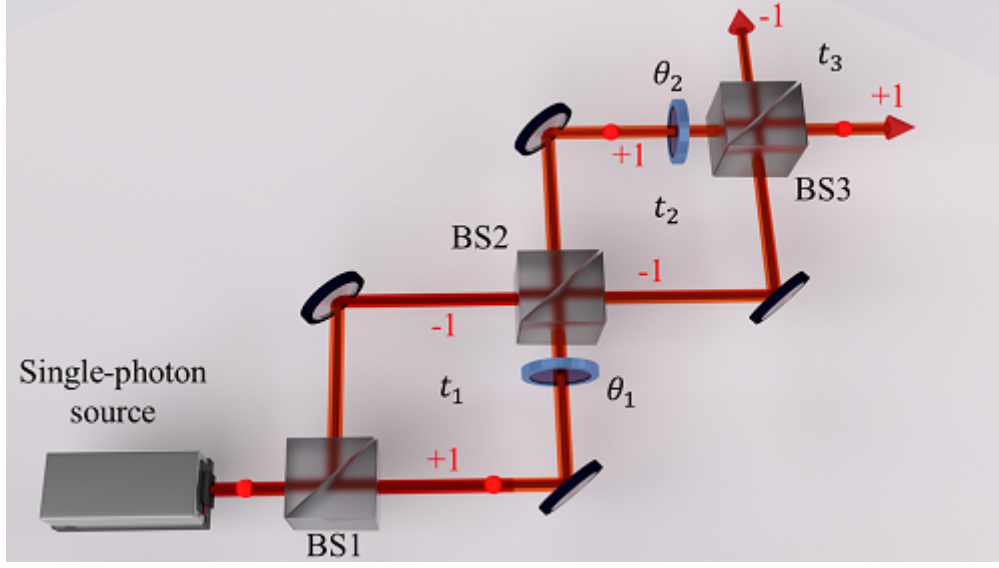


Fig. 5.3 Basic schematic of the experimental setup. **BS1, BS2, BS3**: beamsplitter; θ_1, θ_2 : phase modulator.

$$P_{t_1, t_3}(+, -) = (T_1 T_2 + R_1 R_2 - 2\cos(\theta_1)\sqrt{T_1 T_2 R_1 R_2})R_3, \quad (5.80)$$

$$P_{t_1, t_3}(-, +) = (T_1 R_2 + R_1 T_2 + 2\cos(\theta_1)\sqrt{T_1 T_2 R_1 R_2})R_3 \quad (5.81)$$

$$P_{t_1, t_3}(-, -) = (T_1 R_2 + R_1 T_2 + 2\cos(\theta_1)\sqrt{T_1 T_2 R_1 R_2})T_3 \quad (5.82)$$

Using all these joint probabilities, average correlation values are measured using the expression, $\langle Q_{t_i} Q_{t_j} \rangle = \sum_{q_{t_i}=\pm 1, q_{t_j}=\pm 1} q_{t_i} q_{t_j} P_{t_i, t_j}(q_{t_i}, q_{t_j})$

$$\begin{aligned} \langle Q_{t_1} Q_{t_2} \rangle &= T_2 - R_2, & \langle Q_{t_2} Q_{t_3} \rangle &= T_3 - R_3, \\ \langle Q_{t_1} Q_{t_3} \rangle &= (T_2 - R_2)(T_3 - R_3) - 4\cos(\theta_2)\sqrt{T_2 T_3 R_2 R_3} \end{aligned} \quad (5.83)$$

Using Eq. 5.83, we write the LGI expression (Eq. 5.12) as,

$$LGI = \langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle = 1 - 4R_2 R_3 + 4\cos(\theta_2)\sqrt{T_2 T_3 R_2 R_3} \quad (5.84)$$

$LGI \leq 1.5$, and the upper bound occurs when $T_2 = 0.75$, $T_3 = 0.75$ and $\theta_2 = 0$.

$$\begin{aligned} WLGI &= P_{t_1, t_3}(-, +) - P_{t_1, t_2}(-, +) - P_{t_2, t_3}(-, +) \\ &= 2 \cos(\theta_2) R_1 \sqrt{T_2 T_3 R_2 R_3} - 2 \cos(\theta_1) R_3 \sqrt{T_1 T_2 R_1 R_2} - R_2 R_3 \end{aligned} \quad (5.85)$$

$WLGI \leq 0.4034$, and the upper bound occurs when $T_1 = 0.152$, $T_2 = 0.695$, $T_3 = 0.484$, $\theta_1 = \pi$ and $\theta_2 = 0$.

We have implemented two modifications to the experimental setup which is depicted in Fig. 5.4. The first one is related to the stability of the setup and the second one is related to the closing of the clumsiness loophole. As we can see from the LGI expression derived in Eq. 5.84, it is independent of the preparation state, i. e. no terms related to T_1, R_1 of the *BS1*. Also, the only interference term that contributes to the violation comes from the second Mach-Zehnder (MZ) interferometer. So, in principle, we can ignore the first MZ interferometer. However, even for one active MZ interferometer, the experiment is challenging due to the fact that the MZI is very unstable as the two paths interacting with different optical components always have oscillating path differences. One way to solve this issue is to actively stabilize the MZI, which will require a piezo-driven corner-cube placed in one arm of the MZI, which is controlled by a feedback-looped PID controller. If there is an oscillating path difference with time, the PID controller drives the piezo such that the error in the path difference is compromised. Although this technique has been used in many experiments, we do not prefer this as it requires additional components and fine control in the setup which will increase the error as well as the complexity of the experimental setup.

There is a second solution to the issue, which is easier to implement in our experimental scenario. We have converted the second MZI into a displaced Sagnac interferometer. A Sagnac interferometer is more stable than a MZI due to its geometry [80, 100]. Both paths of the interferometer interact with the same optical components, so if there is a mechanical vibration present in the optics, it is felt by both the paths simultaneously, and hence no relative path/phase difference. Also, the Sagnac interferometer always maintains zero path difference between its two arms, by default, which is an advantage for single photon based

interferometry. Single photons typically have a coherence length of the order of few hundreds of micrometers, so for the maximum visibility of the interference pattern, path difference should be closer to zero with micrometer precision. See Section 2.4 for more details on single photon-based interferometry.

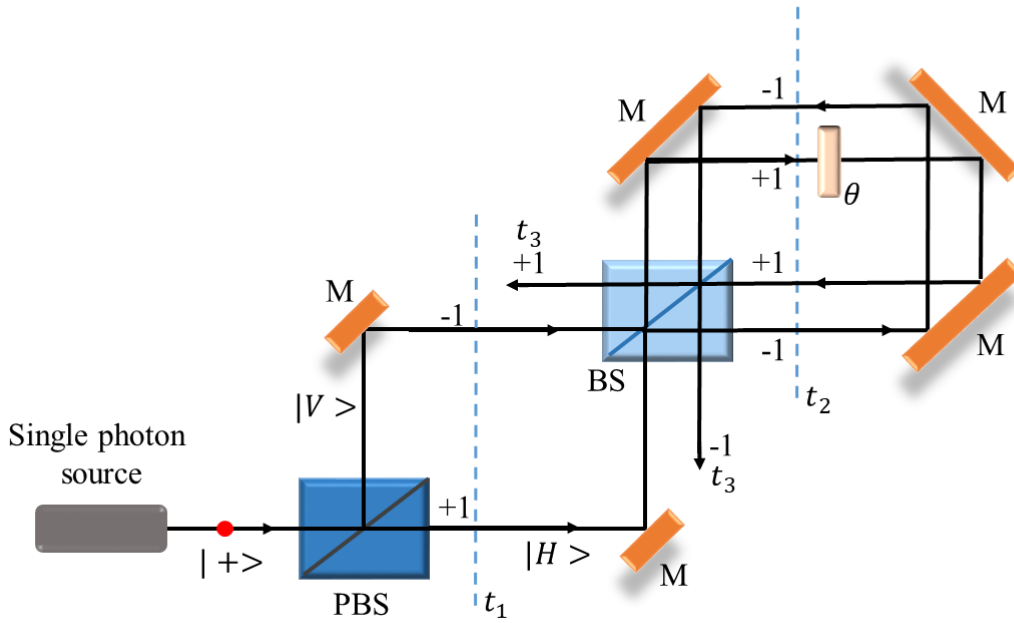


Fig. 5.4 Schematic of the basic design of the experiment. **PBS**: Polarizing beamsplitter; **BS**: Non-polarizing beamsplitter; **M**: Dielectric mirror; θ : Phase modulator.

To satisfy all two-time NSITs, we have to maintain $\langle Q_{t_i} \rangle = 0, \forall i = \{1, 2, 3\}$ [71]. In our current experimental setup, this translates to the fact that the first MZI should be non-interfering, and also the two arms of the MZI should have an equal probability of having single photons at time t_1 . One simple way to achieve this is to prepare the single-photons in a completely mixed state ($I/2$) at t_1 , such that $\langle Q_{t_1} \rangle = 0$. However, we have implemented a different strategy where we prepare the photons in an equal superposition of horizontal and vertical polarization state $((|H\rangle + |V\rangle)/\sqrt{2})$ by first preparing the photons in $|+45^\circ\rangle$ polarization state and send them through a polarizing beamsplitter (PBS). Horizontal ($|H\rangle$) and vertical ($|V\rangle$) polarization states, being orthogonal to each other, do not interfere with

each other, and is enough to serve the purpose.

All relevant joint probabilities (QM predicted) are calculated below for this modified setup. Here $|\alpha|^2 : |\beta|^2$ is the ratio of the probabilities of horizontally and vertically polarized photon in the two arms of the MZI. Generally, the prepared state at t_1 can be written as $\alpha|H\rangle + \beta|V\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$. $T : R$ is the splitting ratio of the non-polarizing beam-splitter (BS) where $T + R = 1$.

$$P_{t_1,t_2}(+,+) = |\alpha|^2 T, \quad P_{t_1,t_2}(+,-) = |\alpha|^2 R, \quad P_{t_1,t_2}(-,+) = |\beta|^2 R, \quad P_{t_1,t_2}(-,-) = |\beta|^2 T \quad (5.86)$$

$$P_{t_2,t_3}(+,+) = |\alpha|^2 T^2 + |\beta|^2 RT, \quad P_{t_2,t_3}(+,-) = |\alpha|^2 TR + |\beta|^2 R^2, \quad (5.87)$$

$$P_{t_2,t_3}(-,+) = |\alpha|^2 R^2 + |\beta|^2 TR, \quad P_{t_2,t_3}(-,-) = |\alpha|^2 RT + |\beta|^2 T^2 \quad (5.88)$$

$$P_{t_1,t_3}(+,+) = |\alpha|^2 (T^2 + R^2 - 2TR\cos(\theta)), \quad P_{t_1,t_3}(+,-) = 2|\alpha|^2 TR(1 + \cos(\theta)), \quad (5.89)$$

$$P_{t_1,t_3}(-,+) = 2|\beta|^2 TR(1 + \cos(\theta)) \quad P_{t_1,t_3}(-,-) = |\beta|^2 (T^2 + R^2 - 2TR\cos(\theta)) \quad (5.90)$$

Average correlation values are calculated from these joint probabilities.

$$\langle Q_{t_1} Q_{t_2} \rangle = T - R, \quad \langle Q_{t_2} Q_{t_3} \rangle = T - R, \quad \langle Q_{t_1} Q_{t_3} \rangle = (T - R)^2 - 4TR\cos(\theta). \quad (5.91)$$

Using Eq. 5.91, we write the LGI expression as,

$$LGI = \langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle = 1 - 4R^2 + 4TR\cos(\theta) \quad (5.92)$$

$LGI \leq 1.5$, and the QM predicted upper bound occurs when $T = 0.75$ and $\theta = 0$. Similarly, we can write the WLGI expression as,

$$WLGI = P_{t_1,t_3}(-,+) - P_{t_1,t_2}(-,+) - P_{t_2,t_3}(-,+) = 2|\beta|^2 TR\cos(\theta) - R^2 \quad (5.93)$$

$WLG I \leq 1/3$, and the QM predicted upper bound occurs when $|\beta|^2 = 1$, $T = 0.67$ and $\theta = 0$. However, for the spacial case of $|\alpha|^2 = |\beta|^2 = 0.5$, which is required to maintain $\langle Q_{t_1} \rangle = 0$, the upper bound of the WLG I expression becomes 0.125 while $T = 0.75$ and $\theta = 0$.

5.4.2 Details of the experiment

Our modified setup (Fig. 5.5) starts with a heralded single photon source, where a diode laser (Cobolt) pumps a BBO (Beta Barium Borate) crystal with the continuous wave of light at a central wavelength of 405 nm and pump power of 10 mW. The BBO crystal is oriented in such a way that it is phase-matched for degenerate, non-collinear, type I spontaneous parametric down-conversion (SPDC) while pumped with horizontally polarized light. To make the pump beam horizontally polarized, a combination of a half waveplate (HWP1) and a polarizing beamsplitter (PBS1) is used. To make the input pump beam Gaussian, we use an apparatus (not shown in Fig. 5.5) for spatial filtering, including a focusing lens, a pinhole and a collimating lens [30]. Parametric down-conversion creates pairs of single photons, both with vertical polarization and 810 nm central wavelength. To increase pair generation, we also place a focusing lens (L1), to focus the pump beam into the central spot of the BBO crystal. A long-pass filter (F1) is placed after the crystal, to block the pump beam and pass only the down-converted single photon pairs. Two dielectric mirrors (M1, M2) are placed to send one photon from each pair to the experiment, and another photon towards a single photon avalanche detector (SPAD1), for heralding. One collimating lens (L2, L3) is placed in each arm, just after the mirrors. The SPADs (ID Quantique, ID120) are all free-space detectors with a maximum quantum efficiency of 80% at 800 nm wavelength. In front of each SPAD (SPAD1, SPAD2+, SPAD2-), we place a focusing lens (L4, L5, L6) and a band-pass filter (F2, F3, F4) centered at 810 nm and filtering bandwidth of 3 nm. Focusing lenses focus single photons onto the sensors and the filters reduce background noises.

Once the single-photon pairs are generated from the SPDC source mentioned above, one photon from each pair is sent to the main experimental setup where two interferometers are constructed. The first interferometer is an asymmetric Mach-Zehnder interferometer (aMZI), whereas the second one is a displaced Sagnac interferometer (dSI). The reason for making the

first MZI asymmetric in terms of the path length is to counter the fact that the non-polarizing beamsplitter (NPBS) that we use shows non-ideal behaviour (detailed discussion on this is provided in Section 5.5.3). The aMZI is made asymmetric by introducing a path difference of few millimeters between the two arms of the aMZI, by shifting the position of the mirror in arm 2. This modification makes the two arms of the aMZI non-interfering as the coherence length of the single photons (typically hundreds of micrometers) are well below the path difference. A combination of a HWP (HWP2) and a PBS (PBS2) controls the beamsplitting ratio in the two arms of the aMZI. another HWP in arm 1 converts the H polarized photon back to V polarized. In the dSI, a single non-polarizing beamsplitter (NPBS) with a measured splitting ratio of $T : R = 80 : 20$ (w.r.t. vertically polarized light at 810 nm wavelength) is used. All alignments in the dSI are performed to achieve optimal interference visibility and stability for both input arms, simultaneously. However, as will be seen later, small inadequacies in the same lead to certain modifications in the experimentally achievable QM predicted values for the various bounds. Two detectors (SPAD2+, SPAD2-) placed in the two output arms of the dSI detect single photons.

Any time between the photon traveling from PBS2 to the first impact on NPBS is considered as t_1 . From the first impact to the second impact on NPBS is time t_2 . Any time after BS is t_3 . Two motorized blockers (B) are placed in arm 1 and 2, and another two blockers are placed in arm 3 and 4, in order to perform negative result measurements at time t_1 and t_2 respectively.

Quantum mechanically predicted violations of LGI and WLGI for the modified setup are evaluated in Eqs. (5.97) and (5.98). The splitting ratio due to the HWP2 and PBS2 combination is denoted as $|\alpha|^2 : |\beta|^2$, where $|\alpha|^2 + |\beta|^2 = 1$. The splitting ratio of the NPBS is denoted as $T : R$. Also, another point to note that the phase term (θ) is required to be zero for the maximum violation of both LGI (5.92) and WLGI (5.93). So, we do not include any phase-modulator (θ) in the setup. All the two-times NSIT conditions (using Eq. 5.5) are expressed as,

$$NSIT_{(t_1)t_2} = |P_{t_2}(+) - P_{t_1,t_2}(+,+) - P_{t_1,t_2}(-,+)| = 0 \quad (5.94)$$

$$NSIT_{(t_2)t_3} = |P_{t_3}(+) - P_{t_2,t_3}(+,+) - P_{t_2,t_3}(-,+)| = 2TR\{|\alpha|^2 - |\beta|^2\} \quad (5.95)$$

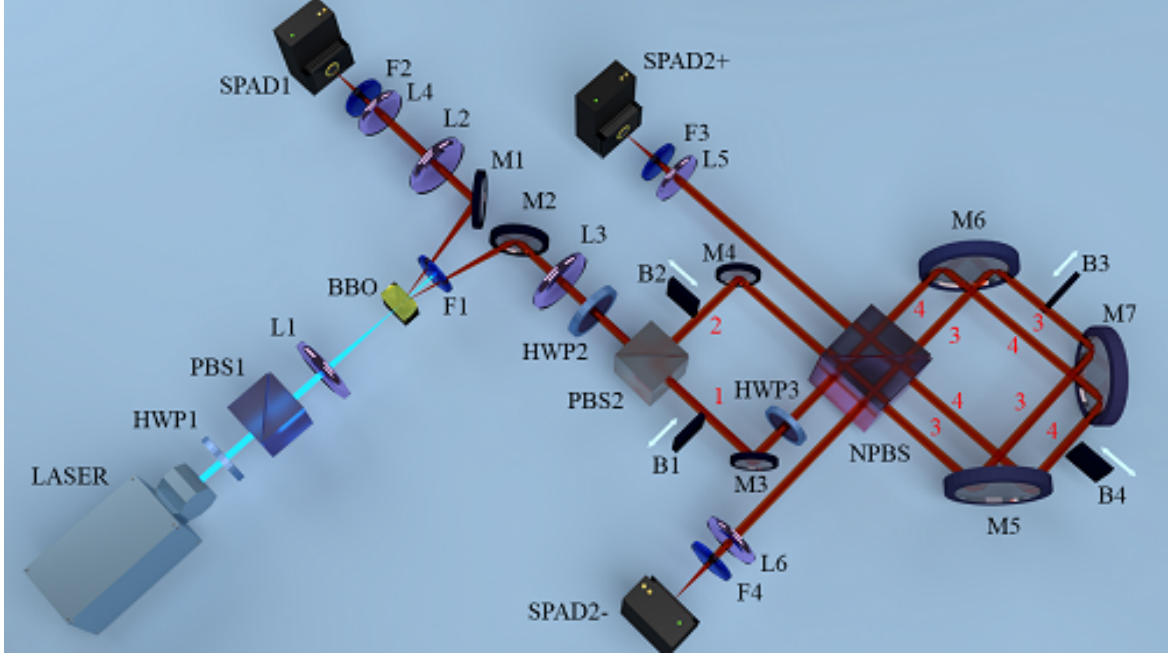


Fig. 5.5 Schematic of the modified experimental setup. **HWP1, HWP2**: Half waveplate; **PBS1, PBS2**: Polarizing beamsplitter; **L1, L4, L5, L6**: Focusing lens; **F1**: Long-pass filter; **M**: Mirror; **L2, L3**: Collimating lens; **F2, F3, F4**: Band-pass filter; **NPBS**: Beamsplitter (non-polarizing); **SPAD1, SPAD2+, SPAD2-**: Single-photon avalanche detector. Two arms of the aMZI are marked as 1 and 2, which represent the +1 and -1 arm, respectively. Similarly, two arms of the dSI are marked as 3 and 4, representing -1 and +1. SPAD2+ and SPAD2- are placed in +1 and -1 arms, respectively.

$$NSIT_{(t_1)t_3} = |P_{t_3}(+) - P_{t_1,t_3}(+,+) - P_{t_1,t_3}(-,+)| = 0 \quad (5.96)$$

Eqs. 5.94 and 5.96 are valid for any value of $T : R$ and $|\alpha|^2 : |\beta|^2$. However, for maintaining $NSIT_{(t_2)t_3} = 0$ (Eq. 5.95), we have to fix $|\alpha|^2 = |\beta|^2 = 0.5$. Another point to note is that we have used $q_{t_2} = +1$ and $q_{t_3} = +1$ in Eq. 5.5, while deriving the three NSIT expressions. Here, one may also use $q_{t_2} = -1$ and $q_{t_3} = -1$, which will give the same result. We evaluate the maximum values (QM predicted) of the LGI/WLGI expression as,

$$LGI : \langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle = 1 - 4R^2 + 4TR \leq 1.5 \quad (5.97)$$

$$WLGI : P_{t_1,t_3}(-,+) - P_{t_1,t_2}(-,+) - P_{t_2,t_3}(-,+) = 2|\beta|^2 TR - R^2 \leq 0.125 \quad (5.98)$$

The maximum values of the LGI and the WLG I expressions are obtained for $T = 0.75$ while maintaining the constraint $|\alpha|^2 = |\beta|^2 = 0.5$.

In order to measure LGI and WLG I values from the experimental setup, we perform three experimental runs. In the first run, we measure all four joint probabilities of the form $P_{t_2,t_3}(q_{t_2}, q_{t_3}) \forall q_{t_2} = \pm 1, q_{t_3} = \pm 1$. In the second run, we measure four joint probabilities of the form $P_{t_1,t_3}(q_{t_1}, q_{t_3})$. In the third run, we measure eight joint probabilities of the form $P_{t_1,t_2,t_3}(q_{t_1}, q_{t_2}, q_{t_3})$. All these sixteen measured joint probabilities are used for calculating the LGI and the WLG I expression, as given below,

$$LGI : \langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle, \quad (5.99)$$

$$WLG I : P_{t_1,t_3}(-, +) - P_{t_1,t_2}(-, +) - P_{t_2,t_3}(-, +). \quad (5.100)$$

For WLG I, we get the three joint probabilities directly from the three experimental runs mentioned above. In case of LGI, we do an additional step of calculating correlation values from measured joint probabilities, by following the equation, $\langle Q_{t_i} Q_{t_j} \rangle = P_{t_i,t_j}(+, +) - P_{t_i,t_j}(+, -) - P_{t_i,t_j}(-, +) + P_{t_i,t_j}(-, -)$. To show the maintenance of all relevant NSITs, we perform the fourth run of the experiment where we measure the probabilities $P_{t_3}(+)$ and $P_{t_3}(-)$, and then calculate the following three expressions:

$$NSIT_{(t_1)t_2} : |P_{t_2}(+) - P_{t_1,t_2}(+, +) - P_{t_1,t_2}(-, +)| \quad (5.101)$$

$$NSIT_{(t_2)t_3} : |P_{t_3}(+) - P_{t_2,t_3}(+, +) - P_{t_2,t_3}(-, +)| \quad (5.102)$$

$$NSIT_{(t_1)t_3} : |P_{t_3}(+) - P_{t_1,t_3}(+, +) - P_{t_1,t_3}(-, +)|. \quad (5.103)$$

As we have implemented negative result measurement (NRM) in our experiment for preserving NIM condition, we perform multiple sub-runs under each of the first three experimental runs. For each of the sub-runs, coincidence data is recorded for 10 seconds and repeated for large number of times (300 iterations for the second experimental run, 150 iterations for both the first and the third run), for better averaging. Discussion related to the choice of the

minimum number of iterations required for our setup will be found in Section 5.5.3. Details of the sub-runs are provided below.

In the first experimental run, we measure the correlation between time t_2 and t_3 . For this purpose, we perform two sub-experimental runs, incorporating NRM. In the first sub-run, a blocker is placed at -1 arm at t_2 (or at arm 3 in the experimental setup provided in Fig. 2), and coincidence counts are measured between SPAD1, SPAD2+ and between SPAD1 and SPAD2-. We denote the first coincidence as $C_{t_2,t_3}(+,+)$ because any photon that gets detected in SPAD2+ must be in $+1$ arm at t_2 and $+1$ arm at t_3 . Similarly, the second coincidence count can be denoted as $C_{t_2,t_3}(+,-)$. In the second sub-run of the experiment, a blocker is placed at $+1$ arm at t_2 . So coincidence count between SPAD1 and SPAD2+ is denoted as $C_{t_2,t_3}(-,+)$, and coincidence count between SPAD1 and SPAD2- is denoted as $C_{t_2,t_3}(-,-)$. The total coincidence count from the first run becomes, $C_{t_2,t_3}^T = C_{t_2,t_3}(+,+) + C_{t_2,t_3}(+,-) + C_{t_2,t_3}(-,+) + C_{t_2,t_3}(-,-)$. We calculate four joint probabilities of the form $P_{t_2,t_3}(q_{t_2}, q_{t_3})$, where $q_{t_2} = \pm 1$, $q_{t_3} = \pm 1$, by normalizing the four coincidence values obtained in the first run as,

$$P_{t_2,t_3}(q_{t_2}, q_{t_3}) = \frac{C_{t_2,t_3}(q_{t_2}, q_{t_3})}{C_{t_2,t_3}^T}. \quad (5.104)$$

Similar strategy is used in the second run of the experiment, where we perform two sub-runs as well. In this case, a blocker is placed in -1 arm at time t_1 in the first sub-run, and in $+1$ arm for the second sub-run. We obtain four coincidence values, i. e., $C_{t_1,t_3}(+,+)$, $C_{t_1,t_3}(+,-)$, $C_{t_1,t_3}(-,+)$, $C_{t_1,t_3}(-,-)$, which are normalized to calculate the joint probabilities of the form $P_{t_1,t_3}(q_{t_1}, q_{t_3})$

$$P_{t_1,t_3}(q_{t_1}, q_{t_3}) = \frac{C_{t_1,t_3}(q_{t_1}, q_{t_3})}{C_{t_1,t_3}^T}. \quad (5.105)$$

The third experimental run, where we measure correlation between time t_1 and t_2 , is slightly different, as we do not place any detectors (SPAD2+ and SPAD2-) at time t_2 ; in order to close the detection efficiency loophole. Here, we still fix the detectors at time t_3 and use two blockers (instead of one) at both times t_1 and t_2 . In this case, we perform four sub-runs of

the experiment, by changing the positions of the two blockers inside the setup. To give an example, in the first sub-run, we place one blocker in the -1 arm at t_1 and the other blocker in the -1 arm at t_2 . So, the measured coincidence count between SPAD1 and SPAD2+ is denoted as $C_{t_1,t_2,t_3}(+, +, +)$, and between SPAD1 and SPAD2- is denoted as $C_{t_1,t_2,t_3}(+, +, -)$. In this way, we obtain eight coincidence values of the form $C_{t_1,t_2,t_3}(q_{t_1}, q_{t_2}, q_{t_3})$ from the third experimental run, and calculate all eight three-time joint probabilities, by using the following normalization

$$P_{t_1,t_2,t_3}(q_{t_1}, q_{t_2}, q_{t_3}) = \frac{C_{t_1,t_2,t_3}(q_{t_1}, q_{t_2}, q_{t_3})}{C_{t_1,t_2,t_3}^T}. \quad (5.106)$$

All four joint probabilities of the form $P_{t_1,t_2}(q_{t_1}, q_{t_2})$ are then calculated from these eight three-time joint probabilities by using the induction or arrow of time (AoT) expression, given below

$$P_{t_1,t_2}(q_{t_1}, q_{t_2}) = \sum_{q_{t_3}=\pm 1} P_{t_1,t_2,t_3}(q_{t_1}, q_{t_2}, q_{t_3}). \quad (5.107)$$

We also perform another experimental run (fourth run) where we do not place any blocker in any arm of the setup and measure coincidences. In this case, the coincidence count between SPAD1 and SPAD2+ is denoted as $C_{t_3}(+)$ and coincidence count between SPAD1 and SPAD2- is denoted as $C_{t_3}(-)$. So, the probabilities at time t_3 are measured as,

$$P_{t_3}(+) = \frac{C_{t_3}(+)}{C_{t_3}(+) + C_{t_3}(-)}, \quad P_{t_3}(-) = \frac{C_{t_3}(-)}{C_{t_3}(+) + C_{t_3}(-)}. \quad (5.108)$$

These probabilities (5.108) are used to calculate the two-time NSIT equations, $NSIT_{(t_1),t_3}$ and $NSIT_{(t_2),t_3}$ (5.102 and 5.103). Details of the experimental methods, as discussed in this section, have been summarized in Table 5.2.

5.5 Results

5.5.1 LGI experiment using continuous-wave laser

Coherent light coming from a laser shows interference properties due to its wave-like behavior. So, in an interferometric setup, light wave exists in two different arms of the interferometer simultaneously, which violates the first assumption of macrorealism (macrorealism *per se*)

Experi- mental runs	Experi- mental sub-runs	No. of blockers used	Blocker placement	Measured coincidences	Total coincidence	Measured probabilities
1	1.1	1	at t_2 in the -1 path (arm 3)	$C_{t_2,t_3}(+,+)$ $C_{t_2,t_3}(+,-)$	C_{t_2,t_3}^T	$P_{t_2,t_3}(+,+), P_{t_2,t_3}(+,-),$ $P_{t_2,t_3}(-,+), P_{t_2,t_3}(-,-)$
	1.2	1	at t_2 in the +1 path (arm 4)	$C_{t_2,t_3}(-,+)$ $C_{t_2,t_3}(-,-)$		
2	2.1	1	at t_1 in the -1 path (arm 2)	$C_{t_1,t_3}(+,+)$ $C_{t_1,t_3}(+,-)$	C_{t_1,t_3}^T	$P_{t_1,t_3}(+,+), P_{t_1,t_3}(+,-),$ $P_{t_1,t_3}(-,+), P_{t_1,t_3}(-,-)$
	2.2	1	at t_1 in the +1 path (arm 1)	$C_{t_1,t_3}(-,+)$ $C_{t_1,t_3}(-,-)$		
3	3.1	2	at t_1 in the -1 path (arm 2), and at t_2 in the -1 path (arm 3)	$C_{t_1,t_2,t_3}(+,+,+)$ $C_{t_1,t_2,t_3}(+,+,-)$	C_{t_1,t_2,t_3}^T	$P_{t_1,t_2,t_3}(+,+,+), P_{t_1,t_2,t_3}(+,+,-),$ $P_{t_1,t_2,t_3}(+,-,+), P_{t_1,t_2,t_3}(+,-,-),$ $P_{t_1,t_2,t_3}(-,+,+), P_{t_1,t_2,t_3}(-,+,-),$ $P_{t_1,t_2,t_3}(-,-,+), P_{t_1,t_2,t_3}(-,-,-)$
	3.2	2	at t_1 in the -1 path (arm 2), and at t_2 in the +1 path (arm 4)	$C_{t_1,t_2,t_3}(+,-,+)$ $C_{t_1,t_2,t_3}(+,-,-)$		
	3.3	2	at t_1 in the +1 path (arm 1), and at t_2 in the -1 path (arm 3)	$C_{t_1,t_2,t_3}(-,+,+)$ $C_{t_1,t_2,t_3}(-,+,-)$		
	3.4	2	at t_1 in the +1 path (arm 1), and at t_2 in the +1 path (arm 4)	$C_{t_1,t_2,t_3}(-,-,+)$ $C_{t_1,t_2,t_3}(-,-,-)$		
4	4.1	0	N/A	$C_{t_3}(+)$ $C_{t_3}(-)$	$C_{t_3}^T$	$P_{t_3}(+), P_{t_3}(-)$

Table 5.2 Details on the various runs and sub-runs of the experiment performed to obtain all relevant probabilities.

of not being able to be in more than one of the available states at the same time, and hence violates any inequality based on the macrorealistic assumptions. However, coherent light pulse (or any pulse having more than one photon) does not fall under the category of testable systems suitable for the violation of macrorealism in the context of the experimental setup that we develop as the system itself changes its properties. For example, when a coherent light pulse passes through a beamsplitter, its intensity gets distributed among the two output arms of the beamsplitter, so the individual output pulse has different intensity compared to the input pulse and should not be considered as the same system. In contrast, single photon, irrespective of the fact that it maintains the notion of macrorealism *per se* or not, does not change its property as it is indivisible under any transformation.

Having said that, we perform an experiment to measure the LGI and the WLGI values using coherent light, in order to check a few properties of our setup mentioned below.

- We check the performance of the experimental setup, especially the interferometric alignment, as the appropriate alignment condition of the interferometer is independent of the source being used (single photon or coherent light).
- We check the stability of the displaced Sagnac interferometer (dSI), specifically, we track the drift in the power of the constructive and destructive interference arms of the dSI, for a longer time duration.
- We measure the LGI/WLGI value using a coherent light beam, which gives us some understanding of different errors or non-idealities of various optical components, as well as the limitations of our setup to achieve the maximum violation possible.

In this experiment, we use coherent continuous light from a Ti:Sapphire laser operated at a central wavelength of 810 nm, which is fed to the experimental setup instead of the single photons generated from the SPDC process. The light beam from the Ti:Sapphire is coupled into a polarization-maintaining fiber and collimated using a fiber collimator. The output beam from the collimator is vertically polarized (98% linearity in polarization) with a power of 4 mW. A dielectric mirror mounted on a flip mirror mount is placed so that when it is flipped upward, it diverts the light beam coming from the Ti:Sapphire towards the setup, and when flipped downward, it continues sending single photons generated from the SPDC process. The experimental setup is the same one as discussed in Section 5.4.2, with the only one alteration is that the two single photon detectors (SPAD2+ and SPAD2-) are replaced with two power meters (ThorLab PM100D). Instead of coincidence photon detection, we measure the powers in the two power meters for the first three runs of experiments (see Table 5.2) and calculate the twelve joint probabilities shown in Table 5.3. From these joint probabilities, the three correlation values are calculated as, $\langle Q_{t_1} Q_{t_2} \rangle = 0.520$, $\langle Q_{t_2} Q_{t_3} \rangle = 0.524$, and $\langle Q_{t_1} Q_{t_3} \rangle = -0.360$, leading to the LGI value of 1.404. The WLGI value we obtain is

$P_{t_1,t_2}(+,+)$	0.368	$P_{t_2,t_3}(+,+)$	0.315	$P_{t_1,t_3}(+,+)$	0.121
$P_{t_1,t_2}(+,-)$	0.156	$P_{t_2,t_3}(+,-)$	0.122	$P_{t_1,t_3}(+,-)$	0.406
$P_{t_1,t_2}(-,+)$	0.084	$P_{t_2,t_3}(-,+)$	0.116	$P_{t_1,t_3}(-,+)$	0.274
$P_{t_1,t_2}(-,-)$	0.392	$P_{t_2,t_3}(-,-)$	0.447	$P_{t_1,t_3}(-,-)$	0.199

Table 5.3 Measured values of the twelve joint probabilities from the experiment using continuous-wave light.

0.074.

Ideally, the maximum LGI and WLGI value from quantum prediction is 1.5 and 0.125 respectively, whereas we manage to get a violation of 1.404 and 0.074 using continuous wave of light. The reasons for the lower values of the measured quantities from the QM predictions are the following:

- The ideal displaced Sagnac interferometer has zero path delay between the two arms, which is guaranteed by its geometry. However, in reality, due to the manufacturing defects in the optical components (for example, surface imperfections of dielectric mirrors), the actual path difference could be in the order of micrometer, which reduces the visibility of the interferometer.
- The non-polarizing beamsplitter (NPBS in Fig. 5.5) that we use in the experiment is sensitive to input polarization. After proper characterization, we observe that the beamsplitting ratio of the NPBS is 70:30 if the input polarization is horizontal, and for vertical input polarization, it is 80:20. This asymmetry also leads to the non-optimal performance of the setup.

5.5.2 LGI experiment with heralded single photon source: preliminary result

We demonstrate the experiment with heralded single photons from the SPDC process as an input to the setup. We perform the first three experimental runs (see Table 5.2) to measure all the relevant coincidence counts. From these coincidence counts, we calculate all twelve relevant joint probabilities. In Table 5.4, we show the measured coincidence values and the

joint probabilities obtained from the experiment, for a representative dataset.

Experi- mental run	Measured coincidences	Total coincidence	Measured probabilities
1	$C_{t_2,t_3}(+,+)=81172$ $C_{t_2,t_3}(+,-)=24963$ $C_{t_2,t_3}(-,+)=32213$ $C_{t_2,t_3}(-,-)=74702$	$C_{t_2,t_3}^T=213050$	$P_{t_2,t_3}(+,+)=0.381, P_{t_2,t_3}(+,-)=0.117$ $P_{t_2,t_3}(-,+)=0.151, P_{t_2,t_3}(-,-)=0.351$
2	$C_{t_1,t_3}(+,+)=32764$ $C_{t_1,t_3}(+,-)=68414$ $C_{t_1,t_3}(-,+)=66777$ $C_{t_1,t_3}(-,-)=51710$	$C_{t_1,t_3}^T=219665$	$P_{t_1,t_3}(+,+)=0.149, P_{t_1,t_3}(+,-)=0.311$ $P_{t_1,t_3}(-,+)=0.304, P_{t_1,t_3}(-,-)=0.235$
3	$C_{t_1,t_2,t_3}(+,+,+)=67347$ $C_{t_1,t_2,t_3}(+,+,-)=20004$ $C_{t_1,t_2,t_3}(+,-,+)=13208$ $C_{t_1,t_2,t_3}(+,-,-)=22431$ $C_{t_1,t_2,t_3}(-,+,+)=22076$ $C_{t_1,t_2,t_3}(-,+,-)=4982$ $C_{t_1,t_2,t_3}(-,-,+)=20698$ $C_{t_1,t_2,t_3}(-,-,-)=61396$	$C_{t_1,t_2,t_3}^T=232142$	$P_{t_1,t_2,t_3}(+,+,+)=0.290, P_{t_1,t_2,t_3}(+,+,-)=0.086$ $P_{t_1,t_2,t_3}(+,-,+)=0.057, P_{t_1,t_2,t_3}(+,-,-)=0.097$ $P_{t_1,t_2,t_3}(-,+,+)=0.095, P_{t_1,t_2,t_3}(-,+,-)=0.021$ $P_{t_1,t_2,t_3}(-,-,+)=0.089, P_{t_1,t_2,t_3}(-,-,-)=0.264$ $P_{t_1,t_2}(+,+)=0.376, P_{t_1,t_2}(+,-)=0.154$ $P_{t_1,t_2}(-,+)=0.116, P_{t_1,t_2}(-,-)=0.353$

Table 5.4 Experimentally measured coincidence values and calculated joint probabilities from a representative experimental dataset.

Using these twelve joint probabilities we measure three correlation functions, $\langle Q_{t_1} Q_{t_2} \rangle = 0.459$, $\langle Q_{t_2} Q_{t_3} \rangle = 0.464$, and $\langle Q_{t_1} Q_{t_3} \rangle = -0.231$, which give us the LGI violation value (Eq. 5.99) of 1.154. From the same dataset, we obtain a WLGI value (Eq. 5.100) of 0.037. We observe even lower violation of LGI/WLGI as compared to the coherent light-based experiment. At this stage, we focus on various troubleshooting procedures; to increase the violation values. These procedures will be discussed in detail in the next subsection.

5.5.3 Troubleshooting

Fluctuations in the coincidence counts:

We observe time dependent fluctuations in the measured coincidence counts, which can be primarily ascribed to three different reasons; the first being the fluctuations in the intensity of the pump beam itself, the second one being the random statistical fluctuations from the SPDC process, and the third one from the fluctuation in the interference pattern due to the slight

unavoidable instability in the interferometer. The intensity of the pump beam coming from a diode laser can oscillate with time due to its sensitivity towards the minute temperature fluctuations inside the lab. We measure these fluctuations in the pump power by placing a power meter just before the BBO crystal and recording input power for around 2 hours. We observe a sinusoidal fluctuation in the power of the laser. The period of this fluctuation is less than 15 minutes. Mean pump power is 13.45 mW, with a standard deviation by mean (SD/M) value of 0.95% (see Fig. 5.6).

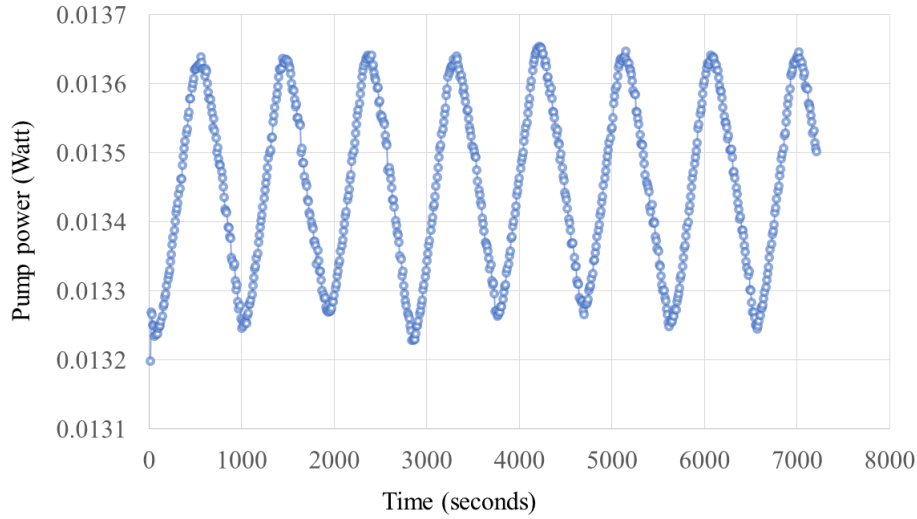


Fig. 5.6 Power fluctuation in the pumping laser light along with time.

The random fluctuation present in the coincidence count is due to the randomness of the single-photon pair generation process in spontaneous parametric down-conversion. To understand these fluctuations, we record the coincidence counts between any one of the detectors and the heralding detector (coincidence between SPAD1 and SPAD2+) for 10 seconds and 1000 iterations. We observe singles count of 4.87×10^5 cps (SPAD1), and 1.73×10^5 cps (SPAD2+), and the coincidence of the order of 10^4 MHz for a time-window of 8192 ps. In order to understand the effect of the instability in the Sagnac interferometer on the temporal fluctuations in coincidence count, we record coincidences for two different scenarios. First, for the non-interference scenario, we placed two blockers, one in arm 1 and another in arm 3 (see Fig. 5.5) and measure coincidences between SPAD1 and SPAD2+.

the second case, which we call the interference case, we place one blocker only in arm 1 and measure coincidences between SPAD1 and SPAD2+. As we do not place any blocker at time t_2 inside the Sagnac interferometer, we allow interference to take place for the second case. For both cases, coincidence counts were recorded for 10 seconds at each iteration and repeated for 1000 iterations. From the statistical distribution of these 1000 iterations, we observe higher fluctuations in the coincidence counts from the interference condition as compared to the non-interference condition (see Figs. 5.7 and 5.8 for comparison).

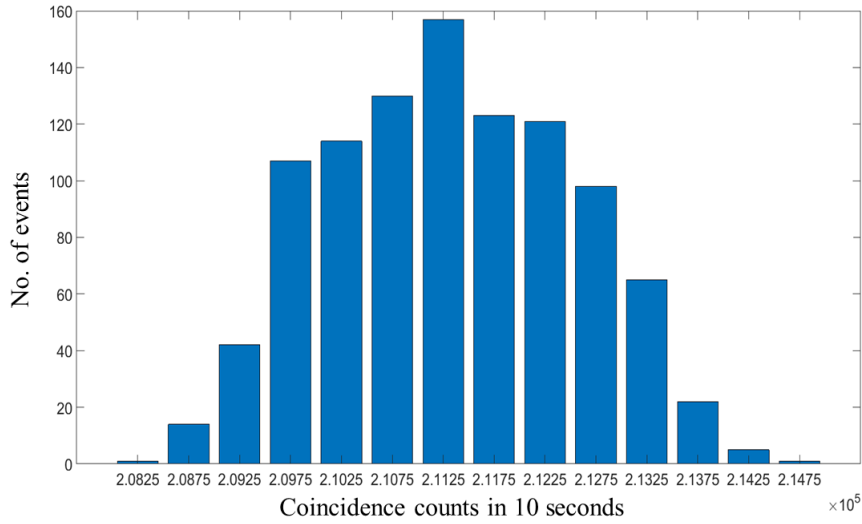


Fig. 5.7 Histogram plot for the coincidence counts for the non-interference condition.

To counter the random fluctuations described in the previous paragraph, we measure average coincidence values from a representative sample of datasets. The first step is to find the minimum number of datasets (or the number of iteration) necessary for the averaging process. For this purpose, we apply a bootstrapping strategy described as follows:

From a source generating photon pairs randomly, the total number of photon pairs generated in a certain time interval T , has ideally a Gaussian distribution with mean μ and standard deviation σ . An obvious but unrealistic way of measuring μ and σ is to experimentally measure the number of photon pairs N generated in time T , repeat the measurement for infinitely long iteration ($I \rightarrow \infty$), and take the average $\mu_\infty = \lim_{I \rightarrow \infty} \frac{1}{I} \sum_{i=1}^I N_i$ and standard deviation

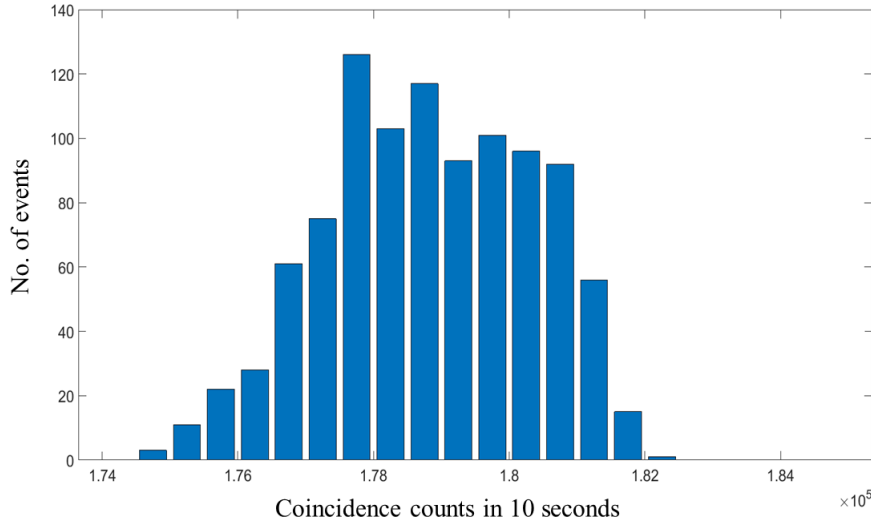


Fig. 5.8 Histogram plot for the coincidence counts for the interference condition. This plot shows more fluctuations as compared to the non-interference case shown in Fig. 5.7.

$\sigma_{\infty} = \lim_{I \rightarrow \infty} \sqrt{\frac{1}{I-1} \sum_{i=1}^I (N_i - \mu_{\infty})^2}$. μ_{∞} and σ_{∞} are the closest to the actual value μ and σ , respectively. However, in a real experiment, it is not feasible to iterate the experiment for infinitely long number of times, so our target is to find the minimum number of iteration (I_{min}) required to find the desired closeness to the actual values of μ and σ . I_{min} depends on the statistical fluctuation in the experiment and has a higher value if the fluctuations are larger. Let's say we randomly select some small value I_i , iterate the experiment that many times, and find the mean μ_{I_i} and standard deviation σ_{I_i} . If I_i is a good guess, then a second run of the same steps will give us μ'_{I_i} and σ'_{I_i} which is not significantly different than μ_{I_i} and σ_{I_i} . a simple way to check that is to measure a large number (K) of $\mu_{I_i}^k$ and $\sigma_{I_i}^k$ where $k = 1, 2, \dots, K$ using the same number of iteration I_i . We measure the mean ($\bar{\mu}_{I_i}$) a standard deviation ($\sigma_{I_i}^{\mu}$) of the distribution of $\mu_{I_i}^k$, where $\bar{\mu}_{I_i} = \frac{1}{K} \sum_{k=1}^K \mu_{I_i}^k$, and $\sigma_{I_i}^k = \sqrt{\frac{1}{K-1} \sum_{k=1}^K (\mu_{I_i}^k - \bar{\mu}_{I_i})^2}$. If we plot standard deviation/mean or $\sigma_{I_i}^{\mu} / \bar{\mu}_{I_i}$ as a function of iteration (I_i), we can see an exponential decay as I_i increases. So, we can select I_i , for which the $\sigma_{I_i}^{\mu} / \bar{\mu}_{I_i}$ is below a certain negligibly small value as required.

Another time-saving process is to apply a bootstrapping strategy to a smaller set of samples. We measure the number of photon pairs detected in the time interval T , for a large

enough iteration (I_L), where we assume that the measured samples are a good representation of the actual sample space. We select any I , and randomly selects I number of samples from I_L number of samples, measure μ_I and σ_I . We repeat the process with re-sampling (with replacement) for K times and measure $\bar{\mu}_I$ and σ_I^μ . In this way we can also plot $\sigma_I^\mu / \bar{\mu}_I$ as a function of I , for all $I < I_L$. This plot is a close approximation to the plot mentioned earlier for a large value of I_L . The advantage of this process is that we do not have to experimentally measure μ_I^k and σ_I^k for K times and for each value of I . Here we can generate all statistics from an initial sample set using re-sampling.

So, we follow the above mentioned strategy on our collected datasets. We record coincidence counts in a time interval $T = 10$ seconds and for $I_L = 1000$ iterations for both the interference and the non-interference conditions. We apply a bootstrapping algorithm with $K = 10^5$; to find the standard deviation by mean (SD/M) value for the different number of iterations of the experiment. We pick a representative SD/M value of 0.05% obtained for $I = 150$ iterations in the non-interference case, as we can observe from the plot (see Fig. 5.9) that SD/M curve quickly flattens after 150 iterations. The same value of SD/M requires $I = 300$ iterations in the interference case. This observation implies that we have to take at least 300 datasets to calculate the average coincidences, where the coincidences are dependant on interference in the Sagnac interferometer. Otherwise, we have to take at least 150 datasets for averaging.

Issues with the blocker and the detection efficiency :

We observe an issue while measuring all joint probabilities from the four sets of experimental runs mentioned in Section 5.4.2. The sum of all coincidences is higher when the number of blockers used is higher. For example, let's say total coincidence is X_1 while no blocker is used, X_2 when only one blocker is used, X_3 when two blockers are used. It always happens that $X_3 > X_2 > X_1$. This observation regarding blockers could be the effect of the fact that the blockers are not behaving ideally, or allowing some of the photons to pass. In order to verify that conjecture, we perform a few checking experiments. These experiments include

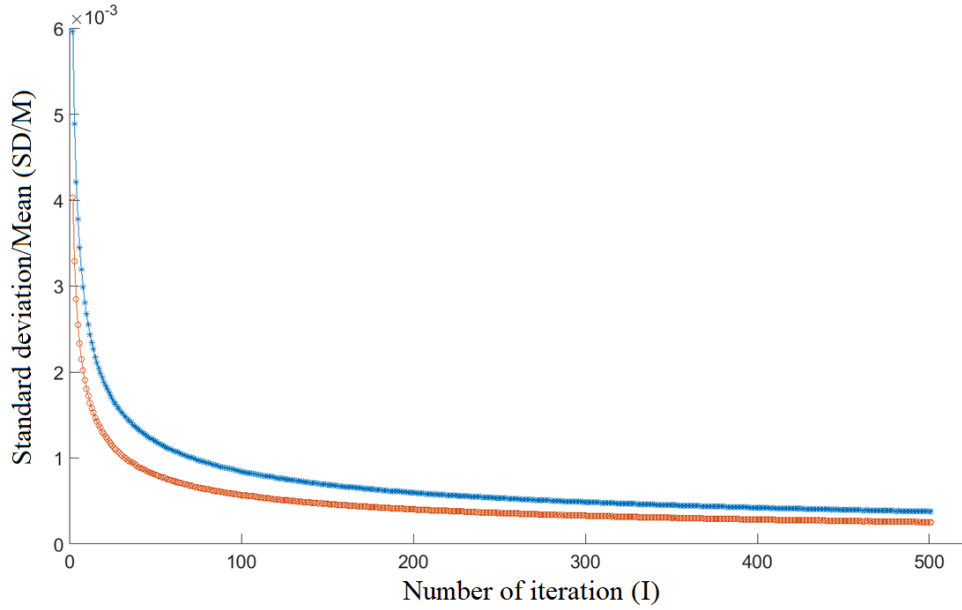


Fig. 5.9 Plot for SD/M vs. the number of iterations. The blue curve represents the interference case, whereas the red curve represents the non-interference case.

installing different types of blockers (black cardboard, metal blocker, beam-diverting mirror, etc.) and repeating the same measurements. We also place detectors before and after the blocking device to check for the blocking efficiency.

However, even after we perform all the tests, we still observe similar anomalies as before. The mismatch in the coincidence counts for different blocking conditions is always more than 10 to 20 standard deviations. Another possible cause of the observed anomaly is the non-linear behavior of the single photon detectors (SPADs). In a typical single photon detector, detection efficiency is defined as the ratio of detected counts to the input number of photons impinging on the detector and is dependent on many parameters like dead time, sensor efficiency, etc. In the ideal case, if we plot the measured coincidence vs the number of input photon pairs impinging on the detectors, it should give us a linear graph. However, as the number of input photons impinging on the detector increases, there is a higher probability that some of the photons may not be detected due to the higher dead time value. This leads to the non-linear saturation plot instead of a linear plot.

We use a half waveplate (HWP2) and PBS (PBS2) combination to control the number of input photons to the detectors (SPAD2+, SPAD2-) and measure coincidence counts between SPAD1 and SPAD2+ and between SPAD1 and SPAD2-, as we rotate the HWP2. We observe the non-linear behavior in the graph (Fig. 5.10). As we rotate the HWP2 and measure coincidences, we expect to see a perfect cosine-squared fitting, however, due to the non-linear behavior of the detector, it does not fit. We took the maximum of the coincidence and kept it as a reference to plot the graph in Fig. 5.10. So, to reduce this effect, we lower the input pump power such that the number of photons impinging on the detector sensor is smaller. We also reduce the detection efficiency of each detector by lowering the bias voltage of the single photon detectors. This, in turn, lowers the dead time of the detectors.

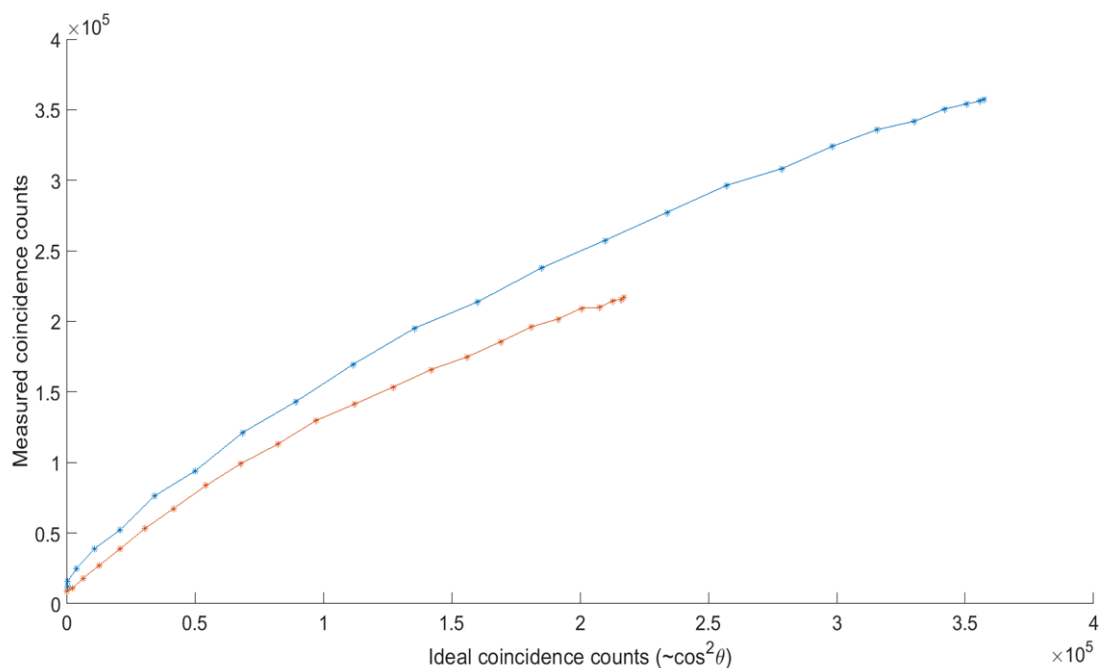


Fig. 5.10 plot showing the effect of the number of input photons impinging on the detector, on the efficiency of the detector. As the number of incident photons increases the number of detected photons reduced from the expected value. Here X-axis is the cosine-squared values of the maximum coincidence, while Y-axis is the measured coincidences. Blue and red lines are for the detectors SPAD2+ and SPAD2-, respectively.

Issue with the beamsplitter :

An ideal non-polarizing beamsplitter (NPBS) has a beamsplitting ratio ($T : R$), which has a fixed value for a specific wavelength of the input beam, and independent of the polarization of the input beam. In reality, this ideal property may vary for individual beamsplitters, depending on the manufacturing anomalies. So it is necessary to characterize the NPBS, independent of the setup, before performing any experiment. We use a NPBS (Thorlab) which has a quoted splitting ratio of $T : R = 70 : 30$ for the wavelength of 810 nm. A Ti:Sapphire laser output which has a central wavelength of 810 nm is used for the characterization, where the laser beam is sent through all the four possible input ports of the NPBS, one after another, and both the output power of the two output ports (transmitting and reflecting ports) are measured simultaneously using two power meters. We also consider two separate cases where the input beam is first made horizontally polarized and then vertically polarized, using a half waveplate placed before the NPBS. Table 5.5 provides the $T : R$ ratios for both the H and V polarized input beams, for different input ports.

NPBS input	H polarized input	V polarized input
input arm 1	71:29	80:20
input arm 2	70:30	79:21
input arm 3	70:30	82:18
input arm 4	70:30	82:18

Table 5.5 Beamsplitting ratios (T:R) of the NPBS obtained from experimental characterization.

As we can see from the measured T:R ratios (Table 5.5), the splitting ratios are polarization-dependent, which is a source of error in the experiment. We show here calculations for all QM predicted joint probabilities, and correlation values, considering this non-ideal behavior of the NPBS. Please see Fig. 5.4 as a reference to all the calculations. Here, $|\alpha|^2$ and $|\beta|^2$ are the transmission and the reflection probabilities of the PBS, respectively. Superscripts H and V placed along with the T and R value represents the polarization state of the photon. If the photon is transmitted through the PBS it is horizontally (H) polarized and if it is reflected, then it is vertically (V) polarized.

$$\begin{aligned}
P_{t_1,t_2}(+,+) &= |\alpha|^2 T^H, & P_{t_1,t_2}(+,-) &= |\alpha|^2 R^H, \\
P_{t_1,t_2}(-,+) &= |\beta|^2 R^V, & P_{t_1,t_2}(-,-) &= |\beta|^2 T^V
\end{aligned} \tag{5.109}$$

$$\begin{aligned}
P_{t_2,t_3}(+,+) &= |\alpha|^2 (T^H)^2 + |\beta|^2 R^V T^V, & P_{t_2,t_3}(+,-) &= |\alpha|^2 T^H R^H + |\beta|^2 (R^V)^2, \\
P_{t_2,t_3}(-,+) &= |\alpha|^2 (R^H)^2 + |\beta|^2 T^V R^V, & P_{t_2,t_3}(-,-) &= |\alpha|^2 R^H T^H + |\beta|^2 (T^V)^2
\end{aligned} \tag{5.110}$$

$$\begin{aligned}
P_{t_1,t_3}(+,+) &= |\alpha|^2 (T^H)^2 + |\alpha|^2 (R^H)^2 - 2|\alpha|^2 T^H R^H \cos\theta \\
P_{t_1,t_3}(+,-) &= 2|\alpha|^2 T^H R^H + 2|\alpha|^2 T^H R^H \cos\theta \\
P_{t_1,t_3}(-,+) &= 2|\beta|^2 R^V T^V + 2|\beta|^2 T^V R^V \cos\theta \\
P_{t_1,t_3}(-,-) &= |\beta|^2 (R^V)^2 + |\beta|^2 (T^V)^2 - 2|\beta|^2 T^V R^V \cos\theta
\end{aligned} \tag{5.111}$$

Eqs. (5.109-5.111) are slightly different from Eqs. (5.86-5.90) which can lead to the lowering of the LGI violation value. Also, in the above-mentioned calculations, we assume that the visibility of the interferometer ($\cos\theta$ term) is unaffected by the non-ideal behavior of the NPBS, which is not the case in reality. It is not only the splitting ratios that are dependant on the input polarization but also the reflected beam from the NPBS diverts differently based upon the polarization of the input beam, which in turn affects the visibility. Ideally, inside the interferometer, both the H and V polarized beam should be on top of each other for maximum interference visibility, but due to beam diversion, if they are not properly aligned then for a certain configuration of the interferometer, if H polarized beam produces optimal interference, then for the same configuration, V polarized beam is not optimally interfering.

To solve these issues, we have introduced additional HWP in arm 1 (HWP3 in Fig. 5.5), which converts H polarized photon into V polarized photon, before hitting the NPBS. As both of the input polarizations are V now, we achieve similar $T : R$ ratios as well as optimal interference for both input arms. However, this change introduces a new issue, as both arm 1 and 2 have V polarized photon states, upon hitting the NPBS, they create interference in the first MZI also, which is in contradiction to our initial aim of maintaining all two-time NSITs.

One way to resolve this is to introduce a small path difference between the two arms of the MZI, such that even if the two polarizations are the same, they do not interfere with each other. We shift the mirror placed in arm 2 in such a way that the path difference is of the order of few millimeters, which is more than enough as the coherence length for our single photon is typically of the order of hundreds of micrometers. From now on, we continue with this modification of the setup as represented in the schematic in Fig. 5.5.

Coincidence time window :

From the type I, non-collinear SPDC process inside a BBO crystal, photon pairs are generated in a form of a ring called SPDC ring. All photon pairs are spatially distributed in the SPDC ring in a random fashion, so a photon from a photon pair can be at any position of the ring, but its partner photon must be at the position exactly diagonal to the position of the first photon in the ring. These diagonally opposite positions in the ring form the correlation zones. If we couple photons in two detectors from any correlation zone, the maximum coincidence between the two detectors is attained, leading to optimal heralding efficiency (coincidence/average singles). But, if the collected photons are not from the same correlation zone, then although the singles counts in both detectors are the same, the coincidence between them is not optimal. In our experiment, we place two mirrors in such a position, that photons from a portion of the SPDC ring are collected in the heralding detector (SPAD1), and photons from the diagonally opposite position or the same correlation zone are sent to the experimental setup, which after passing through different optical components get detected in two different detectors (SPAD2+ and SPAD2-). During the photon detection stage, we align all three detectors (adjusting all spatial degrees of freedom) such that coincidences between SPAD1 and SPAD2+ and coincidence between SPAD1 and SPAD2- are maximum, rather than maximizing individual singles count in the three detectors. This step is essential before performing the experiment, as we will be recording coincidence data from each experimental run.

Another important consideration regarding coincidence count is the selection of the coincidence time window. Once the window is selected, any coincidence event occurring within the time period of the window is considered as a valid coincidence count. In most of the cases, the coincidence window is chosen as a time interval slightly bigger than the temporal size of the coincidence peak, such that all portion of the peak is included. This strategy is good if background noise is significantly lower than the signal itself. In the presence of significant noise, a large coincidence window also captures background counts, which may increase errors in the experimental result. For example, if we are measuring the ratio between two coincidence counts C_1 and C_2 , and due to large window size also captures additional noise counts N_1 and N_2 , respectively, then the ratio becomes $\frac{C_1+N_1}{C_1+C_2+N_1+N_2}$, which is significantly different than $\frac{C_1}{C_1+C_2}$ if $\frac{C_1}{N_1} \neq \frac{C_2}{N_2}$.

Another strategy that can be followed is to set a coincidence window that is smaller than the width of the coincidence curve such that noise is minimized. We select two positions (W_{left} and W_{right}) in the X-axis of the curve around the peak position and adjust them such that signal to noise ratio is optimal. We can also adjust the window such that it covers the full-width at half maxima (FWHM) of the coincidence peak. We may also apply $\frac{1}{e^2}$ width value. In our case, we measure the coincidence window for FWHM of each coincidence plot obtained from experimental data and considered only those coincidence counts that are detected within the defined window, as a valid coincidence value. In this way, we reduce the contribution of unnecessary background noise in our data. Also, in the coincidence plot, there is a flatline on both sides of the coincidence peak which is due to accidental coincidence from background noise. We calculate total noise within the coincidence window as, $\text{Background} = \text{average coincidence in the flatline} \times (W_{right} - W_{left})$. We subtract this “Background” value from the coincidence value, to get the background-corrected coincidences.

5.5.4 Final result with the heralded single photon source

In the final stage of the experiment, we apply all the modifications in the experimental setup and in the data processing, as discussed in the troubleshooting section (5.5.3), and then

collect data from the experiment. The first step of the experiment is to satisfy the most important criteria; maintaining all relevant no-signaling in time (NSIT) conditions in each of the three runs of the experiment. For this purpose, we tweak the HWP2 angle such that the proportion of transmission and reflection in the PBS2 are closer to each other, which in the operational stage is reflected as $P_{t_3}(+) = P_{t_1,t_3}(+,+) + P_{t_1,t_3}(-,+) = P_{t_2,t_3}(+,+) + P_{t_2,t_3}(-,+)$ and $P_{t_3}(-) = P_{t_1,t_3}(+,-) + P_{t_1,t_3}(-,-) = P_{t_2,t_3}(+,-) + P_{t_2,t_3}(-,-)$. All these joint probabilities are measured from the experiment using coincidence counts (experimental procedure discussed in Section 5.4.2). Once we fix the angle of the HWP2 in such a position where the above-mentioned NSIT conditions are optimally achieved, we measure all coincidences from the four sets of experimental runs (in total nine sub-runs of the experiment as shown in Table 5.2), to obtain twelve joint probabilities.

In Table 5.6, we show the measured coincidence values obtained from the different runs of the experiment, for a representative dataset. We also show calculations for getting all the relevant joint probabilities from these coincidence values, and how to calculate the LGI, WLGI and NSIT values.

From Table 5.6 we calculate the three correlation values, $\langle Q_{t_1} Q_{t_2} \rangle = 0.56$, $\langle Q_{t_2} Q_{t_3} \rangle = 0.54$, $\langle Q_{t_1} Q_{t_3} \rangle = -0.22$, and get the LGI value of 1.32 using Eq. (5.99). For the same dataset, WLGI value is obtained from Eq. (5.100) to be 0.09. NSIT values are the following: $NSIT_{(t_1)t_2} = 0.002$ (Eq. 5.101), $NSIT_{(t_2)t_3} = 0.004$ (Eq. 5.102), and $NSIT_{(t_1)t_3} = 0.002$ (Eq. 5.103). We also provide another representative dataset (Table 5.7) from which a WLGI value of 0.1 is achieved.

In Table 5.8, a representative violation of LGI and WLGI from the experiment is provided, which is the maximum violation achieved so far in our current experimental setup. We also verify that all the two-time NSIT conditions (Eq. 5.5) are satisfied in the experiment, as shown in the Table 5.9. We show that all the measured NSIT values are within the statistical fluctuations and hence can be considered as zero with a bound of the order of 10^{-2} ; thus ensuring the validity of the maintenance of non invasive measurement (NIM) in our

Experi- mental run	Measured coincidences	Total coincidence	Measured probabilities
1	$C_{t_2,t_3}(+,+)=41644.94$ $C_{t_2,t_3}(+,-)=10725.33$ $C_{t_2,t_3}(-,+)=12334.57$ $C_{t_2,t_3}(-,-)=35954.40$	$C_{t_2,t_3}^T=100659.24$	$P_{t_2,t_3}(+,+)=0.414, P_{t_2,t_3}(+,-)=0.107$ $P_{t_2,t_3}(-,+)=0.122, P_{t_2,t_3}(-,-)=0.357$
2	$C_{t_1,t_3}(+,+)=22977.20$ $C_{t_1,t_3}(+,-)=30456.67$ $C_{t_1,t_3}(-,+)=35541.98$ $C_{t_1,t_3}(-,-)=19814.86$	$C_{t_1,t_3}^T=108790.71$	$P_{t_1,t_3}(+,+)=0.211, P_{t_1,t_3}(+,-)=0.280$ $P_{t_1,t_3}(-,+)=0.327, P_{t_1,t_3}(-,-)=0.182$
3	$C_{t_1,t_2,t_3}(+,+,+)=34430.15$ $C_{t_1,t_2,t_3}(+,+,-)=8957.09$ $C_{t_1,t_2,t_3}(+,-,+)=2203.34$ $C_{t_1,t_2,t_3}(+,-,-)=9067.37$ $C_{t_1,t_2,t_3}(-,+,+)=10218.37$ $C_{t_1,t_2,t_3}(-,+,-)=1900.90$ $C_{t_1,t_2,t_3}(-,-,+)=10171.06$ $C_{t_1,t_2,t_3}(-,-,-)=30126.35$	$C_{t_1,t_2,t_3}^T=107074.63$	$P_{t_1,t_2,t_3}(+,+,+)=0.322, P_{t_1,t_2,t_3}(+,+,-)=0.084$ $P_{t_1,t_2,t_3}(+,-,+)=0.021, P_{t_1,t_2,t_3}(+,-,-)=0.085$ $P_{t_1,t_2,t_3}(-,+,+)=0.095, P_{t_1,t_2,t_3}(-,+, -)=0.018$ $P_{t_1,t_2,t_3}(-,-,+)=0.095, P_{t_1,t_2,t_3}(-,-,-)=0.281$ $P_{t_1,t_2}(+,+)=0.406, P_{t_1,t_2}(+,-)=0.106$ $P_{t_1,t_2}(-,+)=0.113, P_{t_1,t_2}(-,-)=0.376$
4	$C_{t_3}(+)=49888.96$ $C_{t_3}(-)=42526.46$	$C_{t_3}^T=92415.42$	$P_{t_3}(+)=0.540, P_{t_3}(-)=0.460$

Table 5.6 Experimentally measured coincidence values and calculated joint probabilities from a representative experimental dataset (measured on 08/06/20).

Measured coincidences	Total coincidence	Measured probabilities
$C_{t_2,t_3}(+,+)=38948.29$ $C_{t_2,t_3}(+,-)=10004.17$ $C_{t_2,t_3}(-,+)=11558.11$ $C_{t_2,t_3}(-,-)=33566.68$	$C_{t_2,t_3}^T=94077.25$	$P_{t_2,t_3}(+,+)=0.414, P_{t_2,t_3}(+,-)=0.106$ $P_{t_2,t_3}(-,+)=0.123, P_{t_2,t_3}(-,-)=0.357$
$C_{t_1,t_3}(+,+)=21278.31$ $C_{t_1,t_3}(+,-)=27793.64$ $C_{t_1,t_3}(-,+)=33841.12$ $C_{t_1,t_3}(-,-)=18918.05$	$C_{t_1,t_3}^T=101831.12$	$P_{t_1,t_3}(+,+)=0.209, P_{t_1,t_3}(+,-)=0.273$ $P_{t_1,t_3}(-,+)=0.332, P_{t_1,t_3}(-,-)=0.186$
$C_{t_1,t_2,t_3}(+,+,+)=32422.97$ $C_{t_1,t_2,t_3}(+,+,-)=8398.81$ $C_{t_1,t_2,t_3}(+,-,+)=2007.57$ $C_{t_1,t_2,t_3}(+,-,-)=8542.57$ $C_{t_1,t_2,t_3}(-,+,+)=9650.04$ $C_{t_1,t_2,t_3}(-,+,-)=1742.95$ $C_{t_1,t_2,t_3}(-,-,+)=9529.28$ $C_{t_1,t_2,t_3}(-,-,-)=28004.81$	$C_{t_1,t_2,t_3}^T=100299.01$	$P_{t_1,t_2,t_3}(+,+,+)=0.323, P_{t_1,t_2,t_3}(+,+,-)=0.084$ $P_{t_1,t_2,t_3}(+,-,+)=0.020, P_{t_1,t_2,t_3}(+,-,-)=0.085$ $P_{t_1,t_2,t_3}(-,+,+)=0.096, P_{t_1,t_2,t_3}(-,+, -)=0.017$ $P_{t_1,t_2,t_3}(-,-,+)=0.095, P_{t_1,t_2,t_3}(-,-,-)=0.279$ $P_{t_1,t_2}(+,+)=0.407, P_{t_1,t_2}(+,-)=0.105$ $P_{t_1,t_2}(-,+)=0.114, P_{t_1,t_2}(-,-)=0.374$

Table 5.7 Experimentally measured coincidence values and calculated joint probabilities from a representative experimental dataset (measured on 19/06/20).

experiment.

Expression	Experimentally measured value	Theoretical estimate	
		MR upper bound	QM predicted range
LGI (5.99)	1.32 ± 0.04	1	1.34 ± 0.06
WLG (5.100)	0.10 ± 0.02	0	0.08 ± 0.03

Table 5.8 Measured mean values of the LGI (Eq. 5.12) and WLG (Eq. 5.11) expressions are given with their respective error ranges in order to compare with their respective macrorealist upper bounds as well as the maximum QM predicted ranges, that have been estimated by taking into account non-idealities in our set up arising from least count related systematic limitations in our experimental components as well as due to the range of interferometric visibility values, as observed in our experiment. In the case of LGI, the magnitude of violation or the difference between the experimentally measured value and the upper bound from MR is eight times the error value. For WLG, the violation is five times the error value. Both the measured values show perfect compatibility with the respective QM predicted ranges.

NSIT expression	Experimentally measured value	Theoretical estimate of QM predicted range
$NSIT_{(t_1)t_2}$ (5.101)	$ 0.002 \pm 0.017 $	0
$NSIT_{(t_2)t_3}$ (5.102)	$ 0.004 \pm 0.016 $	$ 0 \pm 0.026 $
$NSIT_{(t_1)t_3}$ (5.103)	$ 0.002 \pm 0.016 $	0

Table 5.9 Measured mean values of all the three NSIT expressions given by Eqs. (5.101-5.103) respectively are of the order of 10^{-3} , smaller than their respective error ranges ($\sim 10^{-2}$). Hence all the three measured NSIT values can be considered to be zero, with a bound of 10^{-2} , in accordance with the QM predictions, which have been estimated taking into account experimental non-idealities as for LGI/WLG reported in Table 5.8. This implies the maintenance of the NIM condition in the present experiment, up to this accuracy.

While calculating the QM predicted ranges for LGI, WLG and NSITs in Table 5.8 and Table 5.9, we consider two different sources of non-idealities in our set up. The first non-ideality arises from least count related systematic limitations in various optical components used in the experiment, e.g., the non-polarizing beamsplitter (NPBS in Fig. 5.5) having 80% transmission probability instead of ideal requirement of 75%, the $T : R$ ratio of the NPBS being dependant on the input ports and having $\pm 2\%$ error, half waveplate (HWP2) angle having precision error of $\pm 1^\circ$, etc. This gives rise to a QM predicted range of 1.47 ± 0.02 for LGI, 0.11 ± 0.02 for WLG, and $|0 \pm 0.03|$ for $NSIT_{(t_2)t_3}$.

The second source of experimental non-ideality stems from our inteferometric architecture itself. While calculating the maximum QM predicted values for the LGI and the WLGI expression, we approximated the relative phase term θ in Eqs. (5.92) and (5.93) to be zero. This would require achievement of optimal interferometric visibility for all experiment runs. However, although we aim for this optimal condition through painstaking alignment procedures, our relative visibility ranges between 70% to 85% during the course of all the experimental runs. This in turn is related to some unavoidable contributions that persist irrespective of the near perfect alignment. These include small temperature fluctuations in the lab, surface imperfections from mirrors that could be in the micrometer range and thus comparable to our single photon wavelength (810 nm), small polarisation dependence that is observed even in a NPBS as well as polarisation dependence of mirrors along with slight non colinearity that may still persist in the interferometer outputs due to minute angular mismatch in the beam splitter arrangements. We thus go on to estimate the modified QM predicted range for our experiment by relaxing the $\theta = 0$ condition and including the variation in relative visibility from 70% to 85% also in the calculation. This leads to a modified QM predicted range for our experiment, of 1.34 ± 0.06 for LGI, 0.08 ± 0.03 for WLGI and $|0 \pm 0.026|$ for $NSIT_{(t_2)t_3}$. Detailed discussion on the calculation of the QM predicted range for various inequalities and their dependence on different experimental parameters will be provided in Section 5.6.3.

In Table 5.9, we show theoretical estimate of QM predicted ranges for the three NSIT expressions. We can see that while $NSIT_{(t_1)t_2}$ and $NSIT_{(t_1)t_3}$ has fixed value of zero, $NSIT_{(t_2)t_3}$ may vary from 0 to 0.026. The reason for this is the fact that the first interferometer we use in the setup is an asymmetric Mach-Zehnder interferometer (aMZI) which does not allow any interference while the second interferometer (dSI) shows interference. So, $NSIT_{(t_1)t_2}$ and $NSIT_{(t_1)t_3}$ does not depend on any experimental parameters (see Eq. 5.94 and Eq. 5.96), while $NSIT_{(t_2)t_3}$ depends on beamsplitting ratios, half waveplate angle, etc. (see Eq. 5.95), hence due to the uncertainties in the values of these parameters, there is a range of the QM predicted value for this NSIT expression. As for LGI/WLGI above, we also note the QM

predicted values for the NSIT expressions in the $\theta \neq 0$ condition (see Section 5.6.3).

In order to quote the measured values for the LGI, WLGI, and NSITs, in Tables 5.8 and 5.9, we estimate the average values and the errors from all experimental datasets. For this purpose, we repeat all the experimental runs for a significant number of times, recording the coincidence counts for 10 seconds in the different runs. In order to find the number of iterations sufficient for the experiment, we record 1000 coincidence datasets for each of the two scenarios. First, for the non-interfering setup, wherein the two blockers are placed, one in arm 1 and another in arm 3, while the coincidences between SPAD1 and SPAD2+ are measured (see Fig. 5.5). For the second case, which we call the interference case, the blocker is placed only in arm 1, and the coincidences between SPAD1 and SPAD2+ are measured. We apply a bootstrapping algorithm to find the standard deviation by mean (SD/M) value of the mean coincidence for the different iterations of the experiment. We find an SD/M value lower than 0.05% for 150 iterations in the non-interference case and 300 iterations for the interference case. Hence, we take 300 iterations while measuring the correlation function $\langle Q_{t_1} Q_{t_3} \rangle$ as it includes all interference terms, and for 150 iterations, the correlation functions $\langle Q_{t_1} Q_{t_2} \rangle$ and $\langle Q_{t_2} Q_{t_3} \rangle$ are measured. For testing the LGI, the three mean values $\langle Q_{t_1} Q_{t_2} \rangle_\mu$, $\langle Q_{t_2} Q_{t_3} \rangle_\mu$, $\langle Q_{t_1} Q_{t_3} \rangle_\mu$ are measured, along with their respective standard deviations denoted as $\sigma_{1,2}$, $\sigma_{2,3}$, $\sigma_{1,3}$. Here, the subscript μ is used to identify these correlation values as experimentally measured averages of the large iterations. The LGI expression $\langle Q_{t_1} Q_{t_2} \rangle_\mu + \langle Q_{t_2} Q_{t_3} \rangle_\mu - \langle Q_{t_1} Q_{t_3} \rangle_\mu$ in this way has a maximum error of $\pm\Delta$. We consider the worst-case scenario where we assume that all the three experimental runs are independent of each other, and hence the error from each run adds up to form the maximum error, i. e., $\Delta = \sigma_{1,2} + \sigma_{2,3} + \sigma_{1,3}$. A similar strategy is also applied for testing the WLGI and the NSITs. Detailed discussion on the bootstrapping strategy as well as the standard deviation will be found in Section 5.6.2.

Another pertinent observation from Table 5.8 and 5.9 is that while the error values for the WLGI and NSITs are comparable, the error from the measured LGI value is slightly higher. The explanation for this observation is the fact that the three correlation values,

$\langle Q_{t_1} Q_{t_2} \rangle, \langle Q_{t_2} Q_{t_3} \rangle, \langle Q_{t_1} Q_{t_3} \rangle$ required to construct the LGI expression are calculated from twelve measured joint probabilities of the form $P_{t_i, t_j}(q_{t_i}, q_{t_j})$, while WLGI and NSITs require only three measured joint probabilities. As the experimental errors add up based on the number of terms in the expression, the LGI value shows a slightly higher error as compared to WLGI or NSITs.

5.6 Details on error analysis

In this error analysis section, we describe the procedure for several calculations mentioned in the result section.

- Calculating different experimental parameters, i. e. beamsplitting ratios, half waveplate rotation angle, etc., from the measured joint probabilities.
- Measuring standard deviation in the data statistics generated from the experiment, for LGI, WLGI, and NSIT.
- Estimating the QM predicted values for LGI, WLGI and NSIT, considering all significant imperfections in the optical components.
- Determining the value of γ (probability of the simultaneous presence of multiple photons) directly from the experimental data.

5.6.1 Determining different experimental parameters from the measured joint probabilities

For this calculation, we consider only joint probabilities measured at all three times, i. e., $P_{t_1, t_2, t_3}(q_{t_1}, q_{t_2}, q_{t_3})$. These eight joint probabilities are measured when we place both the two blockers at time t_1 and t_2 . The reason for choosing only these set of probabilities is that they do not contain any interference term, hence less degrees of freedom. From the measured values of all the eight joint probabilities (see Table 5.10), we calculate seven parameters, $|\alpha|^2, T_1^a, T_2^a, T_3^a, T_4^b, T_2^b, T_3^b$, where T_i^j s are the transmission probabilities of the non-polarizing beamsplitter (NPBS). The superscript “a” and “b” denote that the photon has traversed arm 1 (transmitted arm of the PBS2) and arm 2 (reflecting arm of the PBS2), respectively, and the

subscripts 1, 2, 3 and 4 denote the four input ports of the NPBS, as labelled in Fig. 5.11. In

Joint probability	Expression	Experimental value
$P_{t_1,t_2,t_3}(+,+,+)$	$ \alpha ^2 T_1^a T_2^a$	0.32
$P_{t_1,t_2,t_3}(+,+,-)$	$ \alpha ^2 T_1^a R_2^a$	0.08
$P_{t_1,t_2,t_3}(+,-,+)$	$ \alpha ^2 R_1^a R_3^a$	0.02
$P_{t_1,t_2,t_3}(+,-,-)$	$ \alpha ^2 R_1^a T_3^a$	0.08
$P_{t_1,t_2,t_3}(-,+,+)$	$ \beta ^2 R_4^b T_2^b$	0.09
$P_{t_1,t_2,t_3}(-,+,-)$	$ \beta ^2 R_4^b R_2^b$	0.02
$P_{t_1,t_2,t_3}(-,-,+)$	$ \beta ^2 T_4^b R_3^b$	0.10
$P_{t_1,t_2,t_3}(-,-,-)$	$ \beta ^2 T_4^b T_3^b$	0.28

Table 5.10 Experimentally measured values of all eight three-time joint probabilities, along with corresponding mathematical expressions.

addition, we have the conditions, $|\alpha|^2 + |\beta|^2 = 1$, $T_i^a + R_i^a = T_i^b + R_i^b = 1$, $\forall i = \{1, 2, 3, 4\}$.

The solutions (upto second decimal place) are found to be as follows:

$$|\alpha|^2 = 0.51, T_1^a = 0.79, T_2^a = 0.79, T_3^a = 0.80, T_4^a = 0.77, T_2^b = 0.84, T_3^b = 0.75. \quad (5.112)$$

We can see that there are slight differences between these values with the expected value of $|\alpha|^2 = 0.50$ and the experimentally characterized values of $T_1^a = 0.80, T_2^a = T_2^b = 0.79, T_3^a = T_3^b = 0.82, T_4^a = 0.82$. We make both the inputs to the NPBS vertically polarized, so we usually expect $T_2^a = T_2^b$ and $T_3^a = T_3^b$. However, in reality, there are slight differences in the transmission probabilities for both the input arm which can be caused by the error associated with the HWP rotation angle. This fact is reflected in the mismatch between the values of T_2^a and T_2^b as well as the values of T_3^a and T_3^b . Also in the simplistic model, we ignore various parameters which affect the real experiment, like the loss due to different optical components, asymmetric beam shape in different paths, detection efficiency mismatch, etc. All these aspects are responsible for the mismatch between the experimentally characterized values of the $T : R$ ratios with the calculated values in Eq. 5.112.

5.6.2 Measuring standard deviation of statistical fluctuation

To quote the values for LGI, WLGI, and NSITs in the result section (Table 5.8 and 5.9), we calculate the average value and the standard deviation from all the datasets obtained from the experiment. We repeat all experimental runs for a statistically significant number of times, where we record coincidence counts for 10 seconds in different runs. We take 300 iterations while measuring the correlation between time t_1, t_3 (interference case) and 150 iterations for correlation between time t_1, t_2 and between t_2, t_3 (non-interference case). The reason for choosing these number of iterations has been explained in Section 5.5.3.

For LGI, we measure three average values $\langle Q_{t_1} Q_{t_2} \rangle_\mu, \langle Q_{t_2} Q_{t_3} \rangle_\mu, \langle Q_{t_1} Q_{t_3} \rangle_\mu$ along with their respective standard deviations denoted as $\sigma_{1,2}, \sigma_{2,3}, \sigma_{1,3}$. Here, the subscript μ is used to identify these correlation values as experimentally measured averages of large iterations. The measured LGI value which is $LGI = \langle Q_{t_1} Q_{t_2} \rangle_\mu + \langle Q_{t_2} Q_{t_3} \rangle_\mu - \langle Q_{t_1} Q_{t_3} \rangle_\mu$ has a maximum error of $\pm\Delta$, where $\Delta = \sigma_{1,2} + \sigma_{2,3} + \sigma_{1,3}$. The reason for defining the maximum error as the summation of three standard deviations is that we measured all the three average values from three separate experimental runs performed one after another and combined together. So, we consider the worst-case scenario where we assume that all the three experimental runs are independent of each other, and hence the error from each run adds up to form the maximum error. Any violation with a magnitude much higher than the maximum error obtained for the worst-case scenario can then be considered as a significant violation. Each of the three sets of the experiment also has two or more subsets of experimental runs since we are using negative result measurements. For example, while measuring $\langle Q_{t_1} Q_{t_3} \rangle_\mu$ we perform two sub-experiments, where in the first one we block $' + 1'$ arm at t_1 , and in the second run, we block $' - 1'$ arm at t_1 . Although we take data for the same amount of time duration ($T = 10$ seconds) for both cases, due to statistical fluctuations, the input number of photons to the setup itself can be different for the two cases. Then the four joint probabilities measured from the two different experiments may be self-inconsistent and introduce error in the average value $\langle Q_{t_1} Q_{t_3} \rangle_\mu$. For this, we apply a strategy where we compare all 300 iterations of the first experiment with all 300 iterations of the second, generating 300×300 combinations of $\langle Q_{t_1} Q_{t_3} \rangle$ values. We measure average $\langle Q_{t_1} Q_{t_3} \rangle_\mu$ and standard deviation $\sigma_{1,3}$

of this distribution. Similarly, we measure average value $\langle Q_{t_2} Q_{t_3} \rangle_\mu$ and standard deviation $\sigma_{2,3}$ from a combination of 150×150 possibilities. For $\langle Q_{t_1} Q_{t_2} \rangle_\mu$, however we measure all tree-times joint probabilities rather than two-times joint probabilities, which requires four sub-experiment instead of two, leading to a distribution of 150^4 possible values of $\langle Q_{t_1} Q_{t_2} \rangle$, from which we measure average and standard deviation.

For WLGI, we measure average violation, that is, $\{P_{t_1,t_3}(-,+)\}_\mu - \{P_{t_1,t_2}(-,+)\}_\mu - \{P_{t_2,t_3}(-,+)\}_\mu$ with maximum error of $\pm\Delta$, where $\Delta = \sigma_{1,2} + \sigma_{2,3} + \sigma_{1,3}$, and $\sigma_{i,j}$ represents the standard deviation of the distribution $P_{t_i,t_j}(q_{t_i}, q_{t_j})$. We measure the three averages and standard deviations in the same procedure as implemented for LGI. For NSITs, we measure three expressions, $NSIT_{(t_1)t_2} = |\{P_{t_2}(+)\}_\mu - \{P_{t_1,t_2}(+,+) + P_{t_1,t_2}(-,+)\}_\mu|$, $NSIT_{(t_2)t_3} = |\{P_{t_3}(+)\}_\mu - \{P_{t_2,t_3}(+,+) + P_{t_2,t_3}(-,+)\}_\mu|$, and $NSIT_{(t_1)t_3} = |\{P_{t_3}(+)\}_\mu - \{P_{t_1,t_3}(+,+) + P_{t_1,t_3}(-,+)\}_\mu|$. Each of the NSIT equations requires only two separate experimental runs rather than three used in LGI and WLGI.

5.6.3 Estimating the QM predicted values of LGI, WLGI and NSIT by incorporating experimental non-idealities

We write the expression for LGI and WLGI, using various experimental parameters, as the following (Eqs. 5.92 and 5.93):

$$LGI : \langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle = 1 - 4R^2 + 4TR \cos(\theta)$$

$$WLGI : P_{t_1,t_3}(-,+) - P_{t_1,t_2}(-,+) - P_{t_2,t_3}(-,+) = 2|\beta|^2 TR \cos(\theta) - R^2$$

where $T : R$ is the splitting ratio of the NPBS (see Fig. 5.5) and $|\alpha|^2 : |\beta|^2$ is the splitting ratio due to the HWP2 and PBS2 combination. θ represents the overall phase difference between the two arms of the Sagnac interferometer. Hence, the $\cos(\theta)$ term can be considered as a quantifier of the interferometric visibility obtained in the setup.

However, while deriving (5.92) and (5.93), we assume an ideal case where the beam-splitting ratio $T : R$ for the NPBS has a fixed value. But, as we observe experimentally, the

splitting ratio varies based on the input polarization and the input port of the NPBS. Even if we consider that all photons impinging on the NPBS are vertically polarized, they experience different $T : R$ values based on which of the four input ports of the NPBS they are impinging on. We follow the same notation for the splitting ratios $T_i : R_i$, $\forall i = \{1, 2, 3, 4\}$ as mentioned in Fig. 5.11. With this modification, LGI and WLGI expressions become,

$$\begin{aligned}
 LGI : & \langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle \\
 &= |\alpha|^2 \{ R_1 (T_3 - 3R_3) + T_1 + 2\sqrt{T_1 T_2 R_1 R_3} \cos(\theta) + 2\sqrt{T_1 T_3 R_1 R_2} \cos(\theta) \} \\
 &+ |\beta|^2 \{ R_4 (T_2 - 3R_2) + T_4 + 2\sqrt{T_2 T_4 R_3 R_4} \cos(\theta) + 2\sqrt{T_3 T_4 R_2 R_4} \cos(\theta) \}
 \end{aligned} \tag{5.113}$$

$$\begin{aligned}
 WLGI : & P_{t_1, t_3}(-, +) - P_{t_1, t_2}(-, +) - P_{t_2, t_3}(-, +) \\
 &= 2|\beta|^2 \sqrt{T_2 T_4 R_3 R_4} \cos(\theta) - |\alpha|^2 R_1 R_3 - |\beta|^2 R_2 R_4
 \end{aligned} \tag{5.114}$$

Two-times NSIT expressions, $NSIT_{(t_1)t_2}$ and $NSIT_{(t_1)t_3}$ have the value zero, independent of the values of the splitting ratios ($T_i : R_i$).

$$NSIT_{(t_1)t_2} = |P_{t_2}(+) - P_{t_1, t_2}(+, +) - P_{t_1, t_2}(-, +)| = 0 \tag{5.115}$$

$$NSIT_{(t_1)t_3} = |P_{t_3}(+) - P_{t_1, t_3}(+, +) - P_{t_1, t_3}(-, +)| = 0 \tag{5.116}$$

However, $NSIT_{(t_2)t_3}$ is dependant on the splitting ratio of the beamsplitter.

$$\begin{aligned}
 NSIT_{(t_2)t_3} : & |P_{t_3}(+) - P_{t_2, t_3}(+, +) - P_{t_2, t_3}(-, +)| \\
 &= \left| 2|\alpha|^2 \sqrt{T_1 T_2 R_1 R_3} \cos(\theta) - 2|\beta|^2 \sqrt{T_2 T_4 R_3 R_4} \cos(\theta) \right|
 \end{aligned} \tag{5.117}$$

Using the ideal values of $|\alpha|^2 = |\beta|^2 = 0.5$, $\cos(\theta) = 1$, and experimentally characterized values, $T_1 = 0.80$, $T_2 = 0.79$, $T_3 = 0.82$, $T_4 = 0.82$, in (5.113), (5.114) and (5.117), the QM estimated values of LGI, WLGI and $NSIT_{(t_2)t_3}$ are obtained as 1.47, 0.11 and 0.006, respectively. In the experimental setup, these values of the input parameters may change slightly, depending on the precision of various optical components. So, instead of the QM estimated

fixed values for LGI and WLGI expressions, we obtain a range of the QM predicted values, considering most of the experimental imperfections along with their respective least count errors. The value $|\alpha|^2$ depends on the rotation angle of the HWP2, where we consider a typical least count error of $\pm 1^\circ$ for the rotation angle. Also, for all the T_i values, we consider a least count of $\pm 2\%$. Considering these experimental error ranges, the range of the QM predicted LGI value is calculated to be from 1.45 to 1.49, while the range of the WLGI value is calculated to be from 0.09 to 0.13. For $NSIT_{(t_2)t_3}$, this range is from 0 to 0.03.

A point to be noted is that so far we have considered a simplified model for these calculations, where we assume that the interference visibility of the displaced Sagnac interferometer (dSI) reaches the optimal value in the experiment, or $\cos(\theta) = 1$. However, we observe from the experimental setup that the interferometric visibility value can only be reached up to 85%, with our best effort in the alignment process, and also fluctuates between 70% to 85% along with time. The reasons for this phenomenon can be attributed to various observations. First of all, we simultaneously maintain optimal interference for both the two input arms of the beamsplitter (NPBS in Fig. 5.5). For achieving this condition, both the input beams should be collinear (on top of each other) throughout the whole interference process. This is not easy to maintain, given that the reflection angle from the NPBS is sensitive to the polarization of the input beam. Although we maintain both the input beams to have the same polarization (vertical polarization) with appropriate polarization control, a slight difference can lead to an observable change in the relative angle between the two beams as they pass through many reflecting mirrors inside the interferometer. Another issue arises due to the geometry of the dSI, where the two interfering beams hit the mirrors placed inside the interferometer at two different spots. So, any surface imperfections in the mirrors lead to a path difference (of the order of micrometers) between the two beams, causing a reduction of the visibility. We also observe that the visibility value slowly drifts between 85% and 70% due to the minute changes inside the lab environment, such as temperature, mechanical vibrations, etc.

From the above discussion, it is evident that the ideal assumption of $\cos(\theta) = 1$ is not suitable for the experimental setup that we used. So, we calculate a modified range of QM

prediction using Eqs. (5.113), (5.114) and (5.117), where we vary the value of $\cos(\theta)$ from 0.7 to 0.85, along with the imperfections stemming from other experimental parameters and their respective least count errors, as mentioned earlier. We obtain the modified QM predicted range for LGI to be from 1.28 to 1.40, for WLGI, it is from 0.05 to 0.11, and for $NSIT_{(t_2)t_3}$, from 0 to 0.026.

5.6.4 Determining the value of γ in our experimental setup.

Here, we show the procedure to measure the multi-photon probability or the value of γ from the experimentally measured joint probabilities. For this calculation, we consider only the case of two-photon events and ignore the generation of more than two-photon pairs, as the probability of such events is negligible, and also for the sake of simplicity. Let's say for a large enough time-interval (T), N number of photon events are generated, among which N_1 is the single photon events and N_2 is the two-photon events. So, $N = N_1 + N_2$ and $\gamma = N_2/N = 1/(\frac{N_1}{N_2} + 1)$. Let us assume N photons are sent to a non-polarizing beamsplitter (NPBS) with a splitting ratio ($T : R$). In the transmitting arm of the NPBS, a single photon detector (D1) is placed whose efficiency is η_1 . Similarly, in the reflecting arm detector D2 is placed with efficiency η_2 . For the N_1 single photons, they have $T\eta_1$ and $R\eta_2$ probabilities of getting detected in D1 and D2, respectively. For the N_2 two-photon events, the probability that D1 will get a detection is $T^2\eta_1(2 - \eta_1) + 2TR\eta_1$. The probability that D2 will get a detection is $R^2\eta_2(2 - \eta_2) + 2TR\eta_2$. The probability that both D1 and D2 will get simultaneous detection is $2TR\eta_1\eta_2$.

$$C_1 = N_1 T \eta_1 + N_2 \{T^2 \eta_1 (2 - \eta_1) + 2TR\eta_1\} \quad (5.118)$$

$$C_2 = N_1 R \eta_2 + N_2 \{R^2 \eta_2 (2 - \eta_2) + 2TR\eta_2\} \quad (5.119)$$

$$C_{1,2} = 2N_2 TR\eta_1\eta_2 \quad (5.120)$$

Here, C_1 , C_2 are the singles counts, and $C_{1,2}$ is the coincidence count between detectors D1 and D2. We get the values of C_1 , C_2 , and $C_{1,2}$ from experiment, and using Eqs. (5.118-5.120) we can measure γ . This process forms the basis of our procedure to measure γ directly from

the LGI experimental setup. For this purpose, we only consider the four sub-runs of the experiment, where both the two blockers are placed at time t_1 and t_2 (sub-runs 3.1-3.4 in Table 5.2), as the probabilities obtained from these sets do not include any interference-effect. Also, we consider a more realistic approach for the T:R ratio of the non-polarizing beamsplitter (NPBS), where the splitting ratio varies based on which input port of the NPBS photons are impinging on (see Fig. 5.11). Splitting ratio due to the HWP and PBS combination (HWP2, PBS2 in Fig. 5.5) is denoted as $|\alpha|^2 : |\beta|^2$.

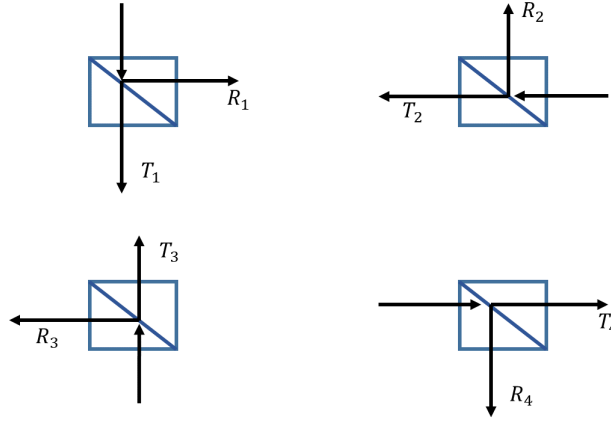


Fig. 5.11 Splitting ratios of the non-polarizing beamsplitter (NPBS in Fig. 5.5) are denoted as $T_i : R_i$ for $i = 1, 2, 3, 4$, depending on the input port of the NPBS. Here, $T_i + R_i = 1, \forall i$.

Set 1: $t_1 +, t_2 +$ (blocking arm 2 and arm 3 in the reference Fig. 5.5)

$$C_1(+, +) = N_1 |\alpha|^2 T_1 R_2 \eta_1 + N_2 |\alpha|^4 (T_1)^2 \{ (R_2)^2 \eta_1 (2 - \eta_1) + 2 T_2 R_2 \eta_1 \} + N_2 (|\alpha|^4 2 T_1 R_1 + 2 |\alpha|^2 |\beta|^2 T_1) R_2 \eta_1 \quad (5.121)$$

$$C_2(+, +) = N_1 |\alpha|^2 T_1 T_2 \eta_2 + N_2 |\alpha|^4 (T_1)^2 \{ (T_2)^2 \eta_2 (2 - \eta_2) + 2 T_2 R_2 \eta_2 \} + N_2 (|\alpha|^4 2 T_1 R_1 + 2 |\alpha|^2 |\beta|^2 T_1) T_2 \eta_2 \quad (5.122)$$

$$C_{1,2}(+, +) = 2 N_2 |\alpha|^4 (T_1)^2 T_2 R_2 \eta_1 \eta_2 \quad (5.123)$$

Set 2: t_1+, t_2- (blocking arm 2 and arm 4 in the reference Fig. 5.5)

$$C_1(+, -) = N_1|\alpha|^2 R_1 T_3 \eta_1 + N_2|\alpha|^4 (R_1)^2 \{ (T_3)^2 \eta_1 (2 - \eta_1) + 2T_3 R_3 \eta_1 \} \\ + N_2(|\alpha|^4 2T_1 R_1 + 2|\alpha|^2 |\beta|^2 R_1) T_3 \eta_1 \quad (5.124)$$

$$C_2(+, -) = N_1|\alpha|^2 R_1 R_3 \eta_2 + N_2|\alpha|^4 (R_1)^2 \{ (R_3)^2 \eta_2 (2 - \eta_2) + 2T_3 R_3 \eta_2 \} \\ + N_2(|\alpha|^4 2T_1 R_1 + 2|\alpha|^2 |\beta|^2 R_1) R_3 \eta_2 \quad (5.125)$$

$$C_{1,2}(+, -) = 2N_2|\alpha|^4 (R_1)^2 T_3 R_3 \eta_1 \eta_2 \quad (5.126)$$

Set 3: t_1-, t_2+ (blocking arm 1 and arm 3 in the reference Fig. 5.5)

$$C_1(-, +) = N_1|\beta|^2 R_4 R_2 \eta_1 + N_2|\beta|^4 (R_4)^2 \{ (R_2)^2 \eta_1 (2 - \eta_1) + 2T_2 R_2 \eta_1 \} \\ + N_2(|\beta|^4 2T_4 R_4 + 2|\alpha|^2 |\beta|^2 R_4) R_2 \eta_1 \quad (5.127)$$

$$C_2(-, +) = N_1|\beta|^2 R_4 T_2 \eta_2 + N_2|\beta|^4 (R_4)^2 \{ (T_2)^2 \eta_2 (2 - \eta_2) + 2T_2 R_2 \eta_2 \} \\ + N_2(|\beta|^4 2T_4 R_4 + 2|\alpha|^2 |\beta|^2 R_4) T_2 \eta_2 \quad (5.128)$$

$$C_{1,2}(-, +) = 2N_2|\beta|^4 (R_4)^2 T_2 R_2 \eta_1 \eta_2 \quad (5.129)$$

Set 4: t_1-, t_2- (blocking arm 1 and arm 4 in the reference Fig. 5.5)

$$C_1(-, -) = N_1|\beta|^2 T_4 T_3 \eta_1 + N_2|\beta|^4 (T_4)^2 \{ (T_3)^2 \eta_1 (2 - \eta_1) + 2T_3 R_3 \eta_1 \} \\ + N_2(|\beta|^4 2T_4 R_4 + 2|\alpha|^2 |\beta|^2 T_4) T_3 \eta_1 \quad (5.130)$$

$$C_2(-, -) = N_1|\beta|^2 T_4 R_3 \eta_2 + N_2|\beta|^4 (T_4)^2 \{ (R_3)^2 \eta_2 (2 - \eta_2) + 2T_3 R_3 \eta_2 \} \\ + N_2(|\beta|^4 2T_4 R_4 + 2|\alpha|^2 |\beta|^2 T_4) R_3 \eta_2 \quad (5.131)$$

$$C_{1,2}(-, -) = 2N_2|\beta|^4 (T_4)^2 T_3 R_3 \eta_1 \eta_2 \quad (5.132)$$

We measure all C_1 , C_2 , and $C_{1,2}$ from these four sets of experiments, and numerically fit all these 12 equations (5.121-5.132) by varying all input parameters, $|\alpha|^2$, T_1 , T_2 , T_3 , T_4 , η_1 , η_2 and γ . We take ten iteration of raw data-sets (time-stamps) for each of the four run of

the experiments and measure the average values of the C_1 , C_2 , and $C_{1,2}$, reported in Table 5.11.

$C_1(+, +)$	9412	$C_1(-, +)$	2206
$C_2(+, +)$	36458.33	$C_2(-, +)$	11286
$C_{1,2}(+, +)$	7.67	$C_{1,2}(-, +)$	1
$C_1(+, -)$	9589.33	$C_1(-, -)$	32375.33
$C_2(+, -)$	2611.67	$C_2(-, -)$	10656.67
$C_{1,2}(+, -)$	0.67	$C_{1,2}(-, -)$	7.33

Table 5.11 Measured values of singles and coincidences from the experiment.

For the purpose of the numerical fitting, we use the chi-squared test using the formula $\chi^2 = \sum_i \frac{(C_i^E - C_i^T)^2}{C_i^T}$, where C_i^E represents all the 12 coincidence values obtained from the experiment, C_i^T represents all coincidence values from theory (Eqs. 5.121-5.132). We tweak all the fitting parameters to get the minimum value of χ^2 . We find the best fit for $|\alpha|^2 = 0.48, T_1 = 0.74, T_2 = 0.77, T_3 = 0.81, T_4 = 0.65, \eta_1 = 0.56, \eta_2 = 0.64$ and $\gamma = 0.0023$, where the chi-squared value is 7.2 (p-value > 0.05). Using the measured value of $\gamma = 0.0023$, we get the maximum upper bound (using equation 5.66) for LGI is 1.0046 and for WLGI, it is 0.0012. As we can see that the changes in the upper bounds due to the contribution of multi-photons are very small, i. e, in the third decimal place only. So, we can safely ignore this effect in our experiment.

5.7 Discussion and Conclusion

In summary, our experiment provides conclusive violation of macrorealist inequalities (LGI and WLGI) by closing all relevant loopholes. We have adopted measurement strategies involving strong projective and negative result measurement (NRM) to an interferometric setup using single photons, such that the *clumsiness loophole* is closed irrespective of the specifics of any theoretical framework. No signaling in time (NSIT) conditions have been used as a tool to verify that all NRMs used in the experiment are indeed non-invasive. Our current literature does not provide sufficient emphasis on other loopholes which are of equal significance. In that context, the present work delivers, for the first time, experimental

strategies to tackle the *detection efficiency loophole* and the *multi-photon emission loophole*. We have used a procedure based on the experimental configuration that facilitates avoiding the *detection efficiency loophole* by showing a violation of the macrorealist inequalities for any non-zero value of the detection efficiency. Another salient feature of our work is the theoretical study of showing the effect of multi-photons on the violation of macroreal inequalities, and how this effect is addressed in the experiment. Thus, our present experiment decisively falsifies the macrorealist inequalities such as LGI/WLGI for the single photons. So, the present work has the potential for providing a reliable and efficient platform towards exploring the single photon based applications of such macrorealist inequalities, for which some relevant ideas have already been discussed [37, 84, 106, 21].

The present experimental study on the loophole-free test of macrorealism also complements the loophole-free empirical repudiation of another fundamental notion, viz. local realism that has been convincingly demonstrated in recent years using the entangled photons [49, 103]. The locality loophole present in the test of local realism has been closed with the aid of a well-established law of physics, viz. theory of relativity. However, for macrorealism, no such physical law exists for tackling the clumsiness loophole, and the only way of closing it is to experimentally verify that the measurements performed at time t_1 and t_2 are non-invasive. The detection efficiency loophole has been closed for the tests of local realism by achieving the required critical detection efficiency, whereas for macrorealism, we have adopted a measurement strategy to bypass the loophole altogether.

Of course, no experiment, as ideal as it is, can unequivocally be regarded as entirely free from loopholes. For example, it has been assumed in the analysis of the experimental test that all experimental runs are mutually independent of each other. Here one can invoke the memory loophole in the similar spirit used for the testing of Bell-type inequalities. It is possible, in principle, to randomize the measurement settings to close the memory loophole. However, the existence of true randomness is still a debatable topic. Also, it has been argued [8] that the probability of simulating a significant violation of this inequality by a local realist model exploiting this memory loophole can be made negligibly small by taking a sufficiently

large number of runs. It would be interesting to investigate whether a similar result would also hold good for the case of macrorealism.

Single photons are in principle “microscopic” in nature, however, we argue here that the well-separated photon paths in the interferometers can be considered as macroscopically distinct states. The dichotomic observable Q_{ti} measured in our setup has the eigenvalues $+1(-1)$ corresponding to the states of the photon being in one or the other arm of the interferometer. Thus, here the ‘macroscopic distinctness’ between the two superposing states is characterised by the spatial separation between the two arms of the interferometer which in the present setup is around 1 cm. This is much larger than the photonic wavelength of 810 nm used here, implying the parameter that can be taken to denote ‘macroscopicity’ in this context to be of the order of 1.2×10^4 . Also, a single photon-based setup is a good test-bed to check for the loophole-free violation of macrorealism, before adapting to other systems. Our experimental setup, which consists of two interferometers, and linear optical components, could potentially be adapted to macroscopic systems as well, such as atomic and molecular interference experiments.

Finally, we note that the Leggett Garg inequality (LGI) and its variant (WLGI) are both only necessary conditions for macrorealism. For this reason, we show the violation of both these inequalities under the same experimental condition, such that it provides conclusive evidence to a macrorealist. Interestingly, the necessary and sufficient conditions for macrorealism have been formulated in terms of a suitable combination of the three-time and two-time LG inequalities [52]. Our present experimental study can also be adapted to check for the loophole-free violation of such necessary and sufficient macrorealist conditions.

Chapter 6

Summary and Outlook

6.1 Summary

In this thesis work, single photons generated from the SPDC process have been used for various experiments in diverse areas of research in quantum fundamentals and technologies, including tests of complementarity, quantum key distribution, and loophole-free tests of macrorealist inequalities. The results have wide-ranging ramifications as well as applications in the realm of quantum information and communication.

In the first experimental work reported in this thesis, we generate pairs of single photons from a type II collinear, degenerate SPDC process by continuously pumping a non-linear BBO (Beta-Barium-Borate) crystal with a laser beam of wavelength 405 nm. Both photons from each pair are made indistinguishable by applying appropriate spectral and spatial filtering, along with polarization control. Both photons are sent to a symmetric fiber beamsplitter (FBS) at the same time via the two input arms of the beamsplitter. Coincidence counts between the two output arms of the beamsplitter are measured and plotted against the time delay between the two input photons. The measured visibility dip from the experiment is $96.06 \pm 0.16\%$. However, this near-100% visibility dip only concludes the indivisibility of the two photons of each SPDC pairs, rather than the inherent quantumness, as it can be shown that indistinguishable classical pulses are also able to generate near-100% visibility dip with appropriate phase randomization [98]. To counter such an argument, we extend the HOM setup for the complementarity test by adding another symmetric beamsplitter whose

two input arms are connected to the two output ports of the FBS. Both the beamsplitters, in combination, form a Mach-Zehnder interferometer (MZI). A two-photon state generated from the SPDC source shows wave-particle complementarity in the modified setup, whereas classical pulses do not. This test confirms the existence of inherent quantumness as well as the high degree of indistinguishability for single photons.

In the following experimental project, we have used the SPDC process as a source of heralded single photons to demonstrate a secure B92 QKD protocol. The use of heralded single photons is advantageous for our novel modification in the experimental setup. First of all, heralded single photons make the experiment noise-tolerant as well as secure against photon-number-splitting (PNS) type attacks. Random basis selection for Alice and Bob is performed using passive quantum randomness, where a single photon randomly selects which path of a symmetric beamsplitter to take. The use of passive quantum randomness makes our QKD setup tolerant to Trojan horse attacks [48], where the eavesdropper sends intense light pulse into the setup and learns about the active random basis selection by analyzing back-reflected light pulse. The inclusion of beamsplitter-based randomness requires some modification in Alice's module, where we implement a novel approach of correlating temporal degrees of freedom with the polarization of the photons. Alice encodes each photon with a randomly selected polarization basis as well as a correlated time delay. In this modified B92 protocol, while Bob measures the polarization of each photon, Alice measures time-delay in the post-processing stage. We also adopt a fresh optimization strategy in the data-analysis stage, making it tolerant to time-shift attacks [122]. We report an average key rate of 51 ± 0.5 kbit/sec and a quantum bit error rate (QBER) of $4.79 \pm 0.01\%$. To our knowledge, the reported key rate is the highest value to date, achieved in a heralded single-photon-based B92 setup.

In the final work, we have shown the violation of various macrorealist inequalities, i. e., Leggett-Garg inequality (LGI) and Wigner form of LGI (WLGI), using a heralded single-photon-based setup. We design the setup in such a way that it is free from the experimental loopholes. While most of the recent experimental works are focused on using weak or

semi-weak measurements for a loophole-free violation, we use all strong projective measurements so that this setup can also be adapted in various quantum optics and information experiments. The clumsiness loophole is addressed through the precision testing of any classical invasiveness involved in implementing negative result measurements. This is done by suitably choosing the experimental parameters such that the quantum mechanically predicted validity of all the relevant two-time no-signalling in time (NSIT) conditions is maintained in all three pairwise experiments performed to show the violation of LGI/WLGI. Further, the detection efficiency loophole is addressed in our experimental scheme by adopting suitable modifications in the measurement strategy enabling the demonstration of the violation of LGI/WLGI for any non-zero detection efficiency. We also show how other relevant loopholes like the multiphoton emission loophole, coincidence loophole, and the preparation state loophole are all closed in the present experiment. We report the LGI violation of 1.32 ± 0.04 and the WLGI violation of 0.10 ± 0.02 in our setup, where the magnitudes of violation are respectively eight times and five times the corresponding error values. At the same time, the experimentally observed probabilities satisfy all the two-time NSIT conditions up to the order of 10^{-2} , which ensures non-invasiveness in the implemented negative result measurements. Further, we closely analyse and show the compatibility of our experimental results with the ranges of the quantum mechanically predicted values of the LGI, WLGI expressions which we estimate by taking into account the non-idealities of the actual experiment.

6.2 Outlook

The experimental works discussed in this thesis open up many prospects for some future works. Here we discuss a few of them.

In the HOM experiment, we have modified the conventional HOM setup to include the complementarity test. So, the modified single setup can now be used for simultaneously checking for the degree of indistinguishability as well as the degree of quantumness. Our HOM setup can also be used to check for a compromised photon source provided by a malicious manufacturer. In this case, a photon source can be considered as a black box. Using the modified HOM setup, one can easily verify if the photon pulse generated by the

source is indeed quantum or classical without disturbing the source setup. As the degree of quantumness associated with the photon source is an essential parameter for most quantum optics experiments, our HOM setup can be applied for the verification or characterization test before performing the experiment.

A natural extension of the HOM experiment can be to investigate the complementarity relation in our setup further. In the experimental work mentioned in this thesis, we fixed the HOM setup in its optimal two-photon interference condition (output state is $\frac{1}{\sqrt{2}}(|2\rangle|0\rangle + |0\rangle|2\rangle)$ as the coincidence visibility dip is near 100%) and then measured the interference effect in the complementarity setup, which was optimal in that case. One can also tweak the optical components to reduce the visibility dip slowly from 100% and observe the corresponding change in the interference pattern in the complementarity setup. This extension will further solidify the claim on the observed quantum mechanical phenomenon of wave-particle complementarity, a unique phenomenon that any classical system can not reproduce.

In QKD experiments, time-bin encoding [17, 96] is becoming a popular choice along with polarization-based encoding. The polarization states of photons do not experience many fluctuations in the free-space transmission but experience polarization rotation and depolarization while passing through optical fibers and interacting with various optical components. On the other hand, the temporal degree of freedom does not change much during the transmission and interaction phase and more accessible to work in an experimental scenario. However, they suffer from temporal broadening, fluctuation, and dispersion effects. In the B92 setup mentioned in this thesis, we took advantage of both the polarization and temporal degree of freedom by encoding each photon with both of these degrees of freedom simultaneously in a correlated fashion. This modification makes the B92 setup tolerant to various eavesdropping strategies applicable to real-world QKD implementations. So, an obvious extension of this work can be to adapt these methodologies to other existing protocols. A good starting point could be the BB84 protocol which is similar to the B92 protocol. Here, one can use multiple beamsplitters and fiber delays to separate four paths from the single input path, apply polar-

ization control and then combine the four paths into one before sending the photon to Bob. Another prospect may be the theoretical work on the security analysis of our modified B92 setup, in line with the work mentioned in the references [111, 91].

In chapter 5, we described a loophole-free test of LGI and WLGI where we tackled various loopholes that currently exist in the literature, i. e., clumsiness loophole, detector efficiency loophole, multiple emission loophole, preparation state loophole, coincidence loophole, etc. However, closing all loopholes in any fundamental experiment is impossible. Here, a macrorealist can always find a new loophole or criticise a closed loophole on the ground of lack of complete knowledge of some hidden variables. For example, in our experiment, we closed the clumsiness loophole by adapting negative result measurement (NRM) on well-separated photon states and maintaining relevant no-signalling conditions. A macrorealist may sidestep the LGI violation by arguing that some unknown hidden variables are being influenced by the NRM, which then affects the future time evolution [68]. So, one can work on the theoretical aspect of such hidden variable models in the context of our implementation of NRM in the experiment. Another line of experimental modification could be to address the memory loophole and the fair-sampling loophole, in the line of work already exist for the loophole-free Bell test. We can, in principle, close the memory loophole by randomizing the choice of measurement settings. Instead of continuous pumping, one can use pulsed pumping for the SPDC process and use motorized blockers at times t_1 and t_2 (see reference Fig. 5.5) for this randomization process. To summarize, closing loopholes is a continuous process of experimental modifications. As Alain Aspect correctly writes that *No experiment can be said to be totally loophole-free* [4].

References

- [1] Aaronson, S. and Arkhipov, A. (2011). The computational complexity of linear optics. In *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing*, STOC '11, page 333–342, New York, NY, USA. Association for Computing Machinery.
- [2] Acín, A., Gisin, N., and Masanes, L. (2006). From bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.*, 97:120405.
- [3] Ahlrichs, A. (2019). *Triply-Resonant Cavity-Enhanced Spontaneous Parametric Down-Conversion*. PhD thesis, Humboldt-Universität zu Berlin.
- [4] Aspect, A. (2015). Closing the Door on Einstein and Bohr's Quantum Debate. *Physics Online Journal*, 8:123.
- [5] Aspect, A., Grangier, P., and Roger, G. (1981). Experimental tests of realistic local theories via bell's theorem. *Phys. Rev. Lett.*, 47:460–463.
- [6] Ballentine, L. E. (1987). Realism and quantum flux tunneling. *Phys. Rev. Lett.*, 59:1493–1495.
- [7] Barrett, J., Collins, D., Hardy, L., Kent, A., and Popescu, S. (2002a). Quantum nonlocality, bell inequalities, and the memory loophole. *Physical Review A*, 66(4).
- [8] Barrett, J., Collins, D., Hardy, L., Kent, A., and Popescu, S. (2002b). Quantum nonlocality, bell inequalities, and the memory loophole. *Phys. Rev. A*, 66:042111.
- [9] Bell, J. S. (1964). On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1:195–200.
- [10] Bell, J. S. (1987). Speakable and unspeakable in quantum mechanics.
- [11] Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121–3124.
- [12] Bennett, C. H. and Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11.
- [13] Bennett, C. H., Brassard, G., and Mermin, N. D. (1992). Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68:557–559.
- [14] Bennink, R. S. (2010). Optimal collinear gaussian beams for spontaneous parametric down-conversion. *Physical Review A*, 81(5):053805.

- [15] Bienfang, J. C., Gross, A. J., Mink, A., Hershman, B. J., Nakassis, A., Tang, X., Lu, R., Su, D. H., Clark, C. W., Williams, C. J., Hagley, E. W., and Wen, J. (2004). Quantum key distribution with 1.25 gbps clock synchronization. *Opt. Express*, 12(9):2011–2016.
- [16] Bierlein, J. D. and Vanherzeele, H. (1989). Potassium titanyl phosphate: properties and new applications. *JOSA B*, 6(4):622–633.
- [17] Boaron, A., Korzh, B., Houlmann, R., Boso, G., Rusca, D., Gray, S., Li, M.-J., Nolan, D., Martin, A., and Zbinden, H. (2018). Simple 2.5ghz time-bin quantum key distribution. *Applied Physics Letters*, 112(17):171108.
- [18] Bohm, D., Hiley, B. J., and Bell, J. S. (1996). The undivided universe: An ontological interpretation of quantum theory. *Synthese*, 107(1):145–165.
- [19] Bourennane, M., Gibson, F., Karlsson, A., Hening, A., Jonsson, P., Tsegaye, T., Ljunggren, D., and Sundberg, E. (1999). Experiments on long wavelength (1550nm) “plug and play” quantum cryptography systems. *Opt. Express*, 4(10):383–387.
- [20] Boyd, R. W. (2003). *Nonlinear optics*. Elsevier.
- [21] Brukner, C., Taylor, S., Cheung, S., and Vedral, V. (2004). Quantum entanglement in time.
- [22] Bruß, D. (1998). Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81:3018–3021.
- [23] Buttler, W. T., Hughes, R. J., Kwiat, P. G., Lamoreaux, S. K., Luther, G. G., Morgan, G. L., Nordholt, J. E., Peterson, C. G., and Simmons, C. M. (1998). Practical free-space quantum key distribution over 1 km. *Phys. Rev. Lett.*, 81:3283–3286.
- [24] Buttler, W. T., Hughes, R. J., Lamoreaux, S. K., Morgan, G. L., Nordholt, J. E., and Peterson, C. G. (2000). Daylight quantum key distribution over 1.6 km. *Phys. Rev. Lett.*, 84:5652–5655.
- [25] Cassemiro, K. N., Laiho, K., and Silberhorn, C. (2010). Accessing the purity of a single photon by the width of the hong-ou-mandel interference. *New Journal of Physics*, 12(11):113052.
- [26] Chatterjee, R., Joarder, K., Chatterjee, S., Sanders, B. C., and Sinha, U. (2020). qkdsim, a simulation toolkit for quantum key distribution including imperfections: Performance analysis and demonstration of the b92 protocol using heralded photons. *Phys. Rev. Applied*, 14:024036.
- [27] Clemente, L. and Kofler, J. (2015). Necessary and sufficient conditions for macroscopic realism from quantum mechanics. *Phys. Rev. A*, 91:062103.
- [28] Clemente, L. and Kofler, J. (2016). No fine theorem for macrorealism: Limitations of the leggett-garg inequality. *Phys. Rev. Lett.*, 116:150401.
- [29] Cohen-Tannoudji, C., Dupont-Roc, J., and Grynberg, G. (1997). *Photons and Atoms - Introduction to Quantum Electrodynamics*.

- [30] Cox, M. E. (1979). The lens-pinhole spatial filter (teaching). *Physics Education*, 14(1):56–57.
- [31] Dowling, J. P. (2008). Quantum optical metrology – the lowdown on high-n00n states. *Contemporary Physics*, 49(2):125–143.
- [32] Dressel, J., Broadbent, C. J., Howell, J. C., and Jordan, A. N. (2011). Experimental violation of two-party leggett-garg inequalities with semiweak measurements. *Phys. Rev. Lett.*, 106:040402.
- [33] Dyer, S. D., Stevens, M. J., Baek, B., and Nam, S. W. (2008). High-efficiency, ultra low-noise all-fiber photon-pair source. *Opt. Express*, 16(13):9966–9977.
- [34] Ekert, A. K. (1991). Quantum cryptography based on bell’s theorem. *Phys. Rev. Lett.*, 67:661–663.
- [35] Emanuelli, S. and Arie, A. (2003). Temperature-dependent dispersion equations for ktiopo 4 and ktioaso 4. *Applied optics*, 42(33):6661–6665.
- [36] Emary, C. (2017). Ambiguous measurements, signaling, and violations of leggett-garg inequalities. *Phys. Rev. A*, 96:042102.
- [37] Emary, C., Lambert, N., and Nori, F. (2013). Leggett–garg inequalities. *Reports on Progress in Physics*, 77(1):016001.
- [38] Fan, T. Y., Huang, C. E., Hu, B. Q., Eckardt, R. C., Fan, Y. X., Byer, R. L., and Feigelson, R. S. (1987). Second harmonic generation and accurate index of refraction measurements in flux-grown ktiopo4. *Appl. Opt.*, 26(12):2390–2394.
- [39] Fasel, S., Alibart, O., Tanzilli, S., Baldi, P., Beveratos, A., Gisin, N., and Zbinden, H. (2004). High-quality asynchronous heralded single-photon source at telecom wavelength. *New Journal of Physics*, 6:163–163.
- [40] Fearn, H. and Loudon, R. (1987). Quantum theory of the lossless beam splitter. *Optics Communications*, 64(6):485 – 490.
- [41] Fedrizzi, A., Herbst, T., Poppe, A., Jennewein, T., and Zeilinger, A. (2007). A wavelength-tunable fiber-coupled source of narrowband entangled photons. *Opt. Express*, 15(23):15377–15386.
- [42] Fedyanin, D. Y. and Agio, M. (2016). Ultrabright single-photon source on diamond with electrical pumping at room and high temperatures. *New Journal of Physics*, 18(7):073012.
- [43] Fradkin, K., Arie, A., Skliar, A., and Rosenman, G. (1999). Tunable midinfrared source by difference frequency generation in bulk periodically poled ktiopo 4. *Applied physics letters*, 74(7):914–916.
- [44] Fung, C.-h. F., Tamaki, K., Qi, B., Lo, H.-K., and Ma, X. (2009). Security proof of quantum key distribution with detection efficiency mismatch. *Quantum Information & Computation*, 9(1):131–165.

- [45] García-Martínez, M. J., Denisenko, N., Soto, D., Arroyo, D., Orue, A. B., and Fernandez, V. (2013). High-speed free-space quantum key distribution system for urban daylight applications. *Appl. Opt.*, 52(14):3311–3317.
- [46] Garg, A. and Mermin, N. D. (1987). Detector inefficiencies in the einstein-podolsky-rosen experiment. *Phys. Rev. D*, 35:3831–3835.
- [47] George, R. E., Robledo, L. M., Maroney, O. J. E., Blok, M. S., Bernien, H., Markham, M. L., Twitchen, D. J., Morton, J. J. L., Briggs, G. A. D., and Hanson, R. (2013). Opening up three quantum boxes causes classically undetectable wavefunction collapse. *Proceedings of the National Academy of Sciences*, 110(10):3777–3781.
- [48] Gisin, N., Fasel, S., Kraus, B., Zbinden, H., and Ribordy, G. (2006). Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A*, 73(2).
- [49] Giustina, M., Versteegh, M. A. M., Wengerowsky, S., Handsteiner, J., Hochrainer, A., Phelan, K., Steinlechner, F., Kofler, J., Larsson, J.-A., Abellán, C., Amaya, W., Pruneri, V., Mitchell, M. W., Beyer, J., Gerrits, T., Lita, A. E., Shalm, L. K., Nam, S. W., Scheidl, T., Ursin, R., Wittmann, B., and Zeilinger, A. (2015). Significant-loophole-free test of bell’s theorem with entangled photons. *Phys. Rev. Lett.*, 115:250401.
- [50] Goggin, M. E., Almeida, M. P., Barbieri, M., Lanyon, B. P., O’Brien, J. L., White, A. G., and Pryde, G. J. (2011). Violation of the leggett–garg inequality with weak measurements of photons. *Proceedings of the National Academy of Sciences*, 108(4):1256–1261.
- [51] Gordon, K. J., Fernandez, V., Townsend, P. D., and Buller, G. S. (2004). A short wavelength gigahertz clocked fiber-optic quantum key distribution system. *IEEE Journal of Quantum Electronics*, 40(7):900–908.
- [52] Halliwell, J. J. (2017). Comparing conditions for macrorealism: Leggett-garg inequalities versus no-signaling in time. *Phys. Rev. A*, 96:012121.
- [53] Halliwell, J. J., Bhatnagar, A., Ireland, E., Nadeem, H., and Wimalaweera, V. (2021). Leggett-garg tests for macrorealism: Interference experiments and the simple harmonic oscillator. *Phys. Rev. A*, 103:032218.
- [54] Hariharan, P. and Sanders, B. (1996). Ii quantum phenomena in optical interferometry. volume 36 of *Progress in Optics*, pages 49 – 128. Elsevier.
- [55] Hong, C. K. and Mandel, L. (1986). Experimental realization of a localized one-photon state. *Phys. Rev. Lett.*, 56:58–60.
- [56] Hong, C. K., Ou, Z. Y., and Mandel, L. (1987). Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.*, 59:2044–2046.
- [57] Huber, D., Reindl, M., Covre da Silva, S. F., Schimpf, C., Martín-Sánchez, J., Huang, H., Piredda, G., Edlinger, J., Rastelli, A., and Trotta, R. (2018). Strain-tunable gaas quantum dot: A nearly dephasing-free source of entangled photon pairs on demand. *Phys. Rev. Lett.*, 121:033902.

- [58] Hughes, R. J., Buttler, W. T., Kwiat, P. G., Lamoreaux, S. K., Morgan, G. L., Nordholt, J. E., and Peterson, C. G. (2000). Quantum cryptography for secure satellite communications. In *2000 IEEE Aerospace Conference. Proceedings (Cat. No.00TH8484)*, volume 1, pages 191–200 vol.1.
- [59] Hughes, R. J., Morgan, G. L., and Peterson, C. G. (2000). Quantum key distribution over a 48 km optical fibre network. *Journal of Modern Optics*, 47(2-3):533–547.
- [60] Inoue, K., Waks, E., and Yamamoto, Y. (2002). Differential phase shift quantum key distribution. *Phys. Rev. Lett.*, 89:037902.
- [61] Jackson, J. D. (1999). Classical electrodynamics.
- [62] Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H., and Zeilinger, A. (2000). A fast and compact quantum random number generator. *Review of Scientific Instruments*, 71(4):1675–1680.
- [63] Joarder, K., Saha, D., Home, D., and Sinha, U. (2022). Loophole-free interferometric test of macrorealism using heralded single photons. *PRX Quantum*, 3:010307.
- [64] Katiyar, H., Shukla, A., Rao, K. R. K., and Mahesh, T. S. (2013). Violation of entropic leggett-garg inequality in nuclear spins. *Phys. Rev. A*, 87:052102.
- [65] Kato, K. and Takaoka, E. (2002). Sellmeier and thermo-optic dispersion formulas for ktp. *Applied optics*, 41(24):5040–5044.
- [66] Kim, Y.-S., Slattery, O., Kuo, P. S., and Tang, X. (2013). Conditions for two-photon interference with coherent pulses. *Phys. Rev. A*, 87:063843.
- [67] Knee, G. C., Kakuyanagi, K., Yeh, M.-C., Matsuzaki, Y., Toida, H., Yamaguchi, H., Saito, S., Leggett, A. J., and Munro, W. J. (2016). A strict experimental test of macroscopic realism in a superconducting flux qubit. *Nature Communications*, 7(1):13253.
- [68] Knee, G. C., Simmons, S., Gauger, E. M., Morton, J. J., Riemann, H., Abrosimov, N. V., Becker, P., Pohl, H.-J., Itoh, K. M., Thewalt, M. L., Briggs, G. A. D., and Benjamin, S. C. (2012). Violation of a leggett–garg inequality with ideal non-invasive measurements. *Nature Communications*, 3(1):606.
- [69] Knill, E., Laflamme, R., and Milburn, G. J. (2001). A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52.
- [70] Kocher, C. A. and Commins, E. D. (1967). Polarization correlation of photons emitted in an atomic cascade. *Phys. Rev. Lett.*, 18:575–577.
- [71] Kofler, J. and Brukner, i. c. v. (2013). Condition for macroscopic realism beyond the leggett-garg inequalities. *Phys. Rev. A*, 87:052115.
- [72] Larsson, J.-A. (1998). Bell’s inequality and detector inefficiency. *Phys. Rev. A*, 57:3304–3308.
- [73] Larsson, J.-Å. and Gill, R. D. (2004). Bell’s inequality and the coincidence-time loophole. *Europhysics Letters (EPL)*, 67(5):707–713.

- [74] Leggett, A. J. (2002). Testing the limits of quantum mechanics: motivation, state of play, prospects. *Journal of Physics: Condensed Matter*, 14(15):R415–R451.
- [75] Leggett, A. J. (2008). Realism and the physical world. *Reports on Progress in Physics*, 71(2):022001.
- [76] Leggett, A. J. and Garg, A. (1985). Quantum mechanics versus macroscopic realism: Is the flux there when nobody looks? *Phys. Rev. Lett.*, 54:857–860.
- [77] Leifgen, M., Schröder, T., Gädeke, F., Riemann, R., Métillon, V., Neu, E., Hepp, C., Arend, C., Becher, C., Lauritsen, K., and Benson, O. (2014). Evaluation of nitrogen- and silicon-vacancy defect centres as single photon sources in quantum key distribution. *New Journal of Physics*, 16(2):023021.
- [78] Loudon, R. (1973). *The Quantum Theory of Light*. Clarendon Press, Oxford.
- [79] Ma, L., Chang, T., Mink, A., Slattery, O., Hershman, B., and Tang, X. (2008). Experimental demonstration of a detection-time-bin-shift polarization encoding quantum key distribution system. *IEEE Communications Letters*, 12(6):459–461.
- [80] Mansuripur, M. (2009). *The Sagnac interferometer*, page 182–196. Cambridge University Press, 2 edition.
- [81] Maroney, O. (2017). Measurements, disturbances and the quantum three box paradox. *Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics*, 58:41–53.
- [82] Maroney, O. J. E. and Timpson, C. G. (2014). Quantum- vs. macro- realism: What does the leggett-garg inequality actually test?
- [83] Meyers, R. and Deacon, K. (2005). Entangled and non-line-of-sight (nlos) free-space photon quantum communication [invited]. *J. Opt. Netw.*, 4(9):573–584.
- [84] Morikoshi, F. (2006). Information-theoretic temporal bell inequality and quantum computation. *Phys. Rev. A*, 73:052308.
- [85] OU, Z. Y. (2007). Multi-photon interference and temporal distinguishability of photons. *International Journal of Modern Physics B*, 21(30):5033–5058.
- [86] Palacios-Laloy, A., Mallet, F., Nguyen, F., Bertet, P., Vion, D., Esteve, D., and Korotkov, A. N. (2010). Experimental violation of a bell’s inequality in time with weak measurement. *Nature Physics*, 6(6):442–447.
- [87] Pan, A. K. (2020). Interference experiment, anomalous weak value, and leggett-garg test of macrorealism. *Phys. Rev. A*, 102:032206.
- [88] Peres, A. (1988). Quantum limitations on measurement of magnetic flux. *Phys. Rev. Lett.*, 61:2019–2021.
- [89] Petrov, P. (2006). *Quantum noise limited light interferometry with cold trapped atoms*. PhD thesis, University of Copenhagen.

- [90] Rarity, J. G., Tapster, P. R., and Loudon, R. (2005). Non-classical interference between independent sources. *Journal of Optics B: Quantum and Semiclassical Optics*, 7(7):S171–S175.
- [91] RENNER, R. (2008). Security of quantum key distribution. *International Journal of Quantum Information*, 06(01):1–127.
- [92] Renner, R., Gisin, N., and Kraus, B. (2005). Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72:012332.
- [93] Ripka, F., Kübler, H., Löw, R., and Pfau, T. (2018). A room-temperature single-photon source based on strongly interacting rydberg atoms. *Science*, 362(6413):446–449.
- [94] Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126.
- [95] Robens, C., Alt, W., Meschede, D., Emary, C., and Alberti, A. (2015). Ideal negative measurements in quantum walks disprove theories based on classical trajectories. *Phys. Rev. X*, 5:011003.
- [96] Roberts, G. L., Lucamarini, M., Dynes, J. F., Savory, S. J., Yuan, Z. L., and Shields, A. J. (2017). Modulator-free coherent-one-way quantum key distribution. *Laser & Photonics Reviews*, 11(4):1700067.
- [97] Sadana, S. (2020). A fresh look at classical theory of light with applications to quantum interferometry. *Ph.D. Thesis*.
- [98] Sadana, S., Ghosh, D., Joarder, K., Lakshmi, A. N., Sanders, B. C., and Sinha, U. (2019). Near-100% two-photon-like coincidence-visibility dip with classical light and the role of complementarity. *Phys. Rev. A*, 100:013839.
- [99] Saha, D., Mal, S., Panigrahi, P. K., and Home, D. (2015). Wigner’s form of the leggett-garg inequality, the no-signaling-in-time condition, and unsharp measurements. *Phys. Rev. A*, 91:032117.
- [100] Sahoo, S. N., Chakraborti, S., Pati, A. K., and Sinha, U. (2020). Quantum state interferography. *Phys. Rev. Lett.*, 125:123601.
- [101] Scarani, V., Acín, A., Ribordy, G., and Gisin, N. (2004). Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 92:057901.
- [102] Scholz, M., Koch, L., and Benson, O. (2009). Analytical treatment of spectral properties and signal–idler intensity correlations for a double-resonant optical parametric oscillator far below threshold. *Optics communications*, 282(17):3518–3523.
- [103] Shalm, L. K., Meyer-Scott, E., Christensen, B. G., Bierhorst, P., Wayne, M. A., Stevens, M. J., Gerrits, T., Glancy, S., Hamel, D. R., Allman, M. S., Coakley, K. J., Dyer, S. D., Hodge, C., Lita, A. E., Verma, V. B., Lacrocco, C., Tortorici, E., Migdall, A. L., Zhang, Y., Kumor, D. R., Farr, W. H., Marsili, F., Shaw, M. D., Stern, J. A., Abellán, C., Amaya, W., Pruneri, V., Jennewein, T., Mitchell, M. W., Kwiat, P. G., Bienfang, J. C., Mirin, R. P., Knill, E., and Nam, S. W. (2015). Strong loophole-free test of local realism. *Phys. Rev. Lett.*, 115:250402.

- [104] Shan, G.-C., Yin, Z.-Q., Shek, C. H., and Huang, W. (2014). Single photon sources with single semiconductor quantum dots. *Frontiers of Physics*, 9(2):170–193.
- [105] Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715.
- [106] Shenoy H., A., Aravinda, S., Srikanth, R., and Home, D. (2017). Can the use of the leggett–garg inequality enhance security of the bb84 protocol? *Physics Letters A*, 381(31):2478 – 2482.
- [107] Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134.
- [108] Smith, B. J., Mahou, P., Cohen, O., Lundeen, J. S., and Walmsley, I. A. (2009). Photon pair generation in birefringent optical fibers. *Opt. Express*, 17(26):23589–23602.
- [109] Stucki, D., Fasel, S., Gisin, N., Thoma, Y., and Zbinden, H. (2007). Coherent one-way quantum key distribution. In Dusek, M., Hillery, M. S., Schleich, W. P., Prochazka, I., Migdall, A. L., and Pauchard, A., editors, *Photon Counting Applications, Quantum Optics, and Quantum Cryptography*, volume 6583, pages 194 – 197. International Society for Optics and Photonics, SPIE.
- [110] Suzuki, Y., Iinuma, M., and Hofmann, H. F. (2012). Violation of leggett–garg inequalities in quantum measurements with variable resolution and back-action. *New Journal of Physics*, 14(10):103022.
- [111] Tamaki, K. and Lütkenhaus, N. (2004). Unconditional security of the bennett 1992 quantum key-distribution protocol over a lossy and noisy channel. *Phys. Rev. A*, 69:032316.
- [112] Tang, X., Ma, L., Mink, A., Nakassis, A., Xu, H., Hershman, B., Bienfang, J. C., Su, D., Boisvert, R. F., Clark, C. W., and Williams, C. J. (2006). Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over mbit/s. *Opt. Express*, 14(6):2062–2070.
- [113] Vakhitov, A., Makarov, V., and Hjelme, D. R. (2001). Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *Journal of Modern Optics*, 48(13):2023–2038.
- [114] Vallone, G., Marangon, D. G., Canale, M., Savorngnan, I., Bacco, D., Barbieri, M., Calimani, S., Barbieri, C., Laurenti, N., and Villoresi, P. (2015). Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels. *Phys. Rev. A*, 91:042320.
- [115] Vernam, G. S. (1926). Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the A.I.E.E.*, 45(2):109–115.
- [116] Wang, K., Emary, C., Xu, M., Zhan, X., Bian, Z., Xiao, L., and Xue, P. (2018). Violations of a leggett-garg inequality without signaling for a photonic qutrit probed with ambiguous measurements. *Phys. Rev. A*, 97:020101.

- [117] Wiechmann, W., Kubota, S., Fukui, T., and Masuda, H. (1993). Refractive-index temperature derivatives of potassium titanyl phosphate. *Optics letters*, 18(15):1208–1210.
- [118] Wigner, E. P. (1970). On hidden variables and quantum mechanical probabilities. *American Journal of Physics*, 38(8):1005–1009.
- [119] Wilde, M. M. and Mizel, A. (2012). Addressing the clumsiness loophole in a leggett-garg test of macrorealism. *Foundations of Physics*, 42(2):256–265.
- [120] Wilson, J., Chaffee, D., Wilson, N., Lekki, J., Tokars, R., Pouch, J., Roberts, T., Battle, P., Floyd, B., Lind, A., Cavin, J., and Helmick, S. (2016). Free-space quantum key distribution with a high generation rate potassium titanyl phosphate waveguide photon-pair source. page 99800U.
- [121] Xu, J.-S., Li, C.-F., Zou, X.-B., and Guo, G.-C. (2011). Experimental violation of the leggett-garg inequality under decoherence. *Scientific Reports*, 1(1):101.
- [122] Zhao, Y., Fung, C.-H. F., Qi, B., Chen, C., and Lo, H.-K. (2008). Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Physical Review A*, 78(4).

Appendix A

How to plot coincidence between two detectors

Overview

From two detectors, we generate two separate lists. Each list contains the record of time-stamps of consecutive photons detected in the respective detector (typically in pico-second scale). Let's say that these two time-stamping lists are labeled as DATA1 and DATA2. We compare these two lists and measure the time difference between the two time-stamps, and plot the frequency along with the time differences. This plot is called the coincidence plot. In the case of coincidence events, the plot shows a peak in the graph. In the case of constant background noise, the plot shows a nearly straight line. Here, we show an algorithm to plot such coincidence between two time-stamps generated from two detectors.

Algorithm 1 Generates the coincidence plot between two time-stamping datasets, where X-axis is the time interval and Y-axis is the coincidence counts

Require:

UNSIGNED INTEGER LENGTHDATA1 ▷ Length of the array in time stamping dataset 1

UNSIGNED INTEGER [LENGTHDATA1] DATA1 ▷ Array in time stamping dataset 1

UNSIGNED INTEGER LENGTHDATA2 ▷ Length of the array in time stamping dataset 2

UNSIGNED INTEGER [LENGTHDATA2] DATA2 ▷ Array in time stamping dataset 2

UNSIGNED INTEGER STARTTIME ▷ Starting time of the X axis in the coincidence plot

UNSIGNED INTEGER ENDTIME ▷ Ending time of the X axis in the coincidence plot

UNSIGNED INTEGER RESOLUTION ▷ resolution of the X axis in the coincidence plot

Ensure:

REAL XAXIS ▷ Array to store the coincidence time interval

UNSIGNED INTEGER YAXIS ▷ Array to store the number of coincidence

1: **procedure** COINCIDENCEPLOT(LENGTHDATA1, DATA1, LENGTHDATA2, DATA1, STARTTIME, ENDTIME, RESOLUTION)

2: UNSIGNED INTEGER s $\leftarrow$ 1 ▷ Bin in the X axis initializes to 1

3: **for** BINLEFT = STARTTIME, RESOLUTION, ENDTIME **do** ▷ Iterates starting time for each bin in the X axis

4: BINRIGHT $\leftarrow$ BINLEFT+ RESOLUTION ▷ Ending time for each bin in the X axis

5: COUNT $\leftarrow$ 0 ▷ Initializes coincidence count in each bin to 0 value

6: I $\leftarrow$ 1 ▷ Initializes iteration value for the array in time stamping dataset 1

7: J $\leftarrow$ 1 ▷ Initializes iteration value for the array in time stamping dataset 2

8: **while** (I $\leq$ LENGTHDATA1) & (J $\leq$ LENGTHDATA2) **do**

9: TIMEDIFF $\leftarrow$ DATA2 [J] – DATA1 [I] ▷ Measuring time difference between two arrays

10: **if** TIMEDIFF $\geq$ 0 **then**

11: **if** (TIMEDIFF < BINRIGHT) & (TIMEDIFF $\geq$ BINLEFT) **then**

12: COUNT = COUNT + 1

```

17:      if TIMEDIFF < 0 then
18:          if (TIMEDIFF < BINRIGHT) & (TIMEDIFF ≥ BINLEFT) then
19:              COUNT ← COUNT + 1      ▷ Increments coincidence count if time
              difference is within a time window
20:              I ← I + 1                ▷ Increments the iterator
21:          end if
22:              J ← J + 1                ▷ Increments the iterator
23:          end if
24:      end while
25:      YAXIS[S] ← COUNT                ▷ Updates coincidence count for each bin
26:      XAXIS[S] ←  $\frac{\text{BINLEFT} + \text{BINRIGHT}}{2}$     ▷ Updates time difference for each bin
27:      S ← S + 1                      ▷ Increments bin value
28:  end for
29:  return XAXIS, YAXIS                ▷ Returns the specified outputs
30: end procedure

```

We plot the YAXIS vs the XAXIS which produces the coincidence plot.

Please refer to Appendix C for details on the usage of various data types and libraries in the above algorithmic function.

Appendix B

QKD optimization algorithms

Overview

We have used two optimization strategies for the data analysis in the B92 QKD experiment, namely optimization strategy A & B. The aim of using these two strategies is to obtain the optimal key rate, QBER and key symmetry. In strategy A, we maximize the key rate while the QBER value is kept below the threshold value of 4.8% [92] and the key symmetry is approximately 50:50. Here, we fix the key symmetry for all the datasets, which introduces some leakage of additional information to the eavesdropper. Also, in order to maintain the symmetry, we delete some key bits which reduces the length of the key. On the other hand, in strategy B we maximize the key rate with similar constraint on the QBER value but no constraint on key symmetry. So, in strategy B, the key rate value is higher than in strategy A. However, the security has been compromised to a small extent as the key is now biased. The probability for generating any random key string of length N , out of 2^N possibilities, no longer remains as $\frac{1}{2^N}$.

Strategy A: We maximize the output key rate while maintaining the key symmetry value of 50 : 50 and simultaneously ensuring a quantum-bit-error-rate (QBER) $\leq 4.8\%$. For each of the measured dataset obtained from the experiment, we follow the strategy as listed below:

1. Find the value of the maximum coincidences (Y-axis) and the position of the maximum coincidence (X-axis) in both plots (see Fig. 4.7 in Section 4.4.7 as a reference).
2. Place the window markers (W_{l_1} and W_{r_1}) on the left and the right side of the coincidence maximum; in the first peak (blue curve). Ensure that the markers are located well

beyond the full-width-at-half-maxima (FWHM) points. Measure the key length (area under the blue curve) and the number of error bits (area under the red curve) for the said window.

3. Place the window markers (W_{l_2} and W_{r_2}) on the second peak (red curve), in the similar fashion. Measure the key length (area under the red curve) value. Adjust the window markers such that this key length becomes same as the key length obtained in step 1. This step ensures that the key is symmetric. Once they are same, measure the number of error bits (area under the blue curve) for the final window position.
4. Measure the total QBER value (i. e. ratio of the total number of error bits and the total key length, obtained from both step 1 and 2). If it is above 4.8%, then shift both the window marker positions W_{l_1} and W_{r_1} with equal step size towards the coincidence maximum on the first peak. Adjust the window marker positions W_{l_2} and W_{r_2} accordingly, such that the key remains symmetric. This step reduces the QBER value as well as the key rate. On the other hand, if the QBER value is below 4.8%, take the reverse action or in other words, shift the marker positions away from the position of the coincidence maxima.
5. Repeat step 4 until the QBER value is closer but below 4.8%.

Lastly, store the optimized key rate, QBER and key symmetry (or asymmetry) value for all the datasets and calculate the mean values for each of the three parameters.

Strategy B: In this strategy, we optimize the key rate value such that the quantum-bit-error-rate (QBER) value is $\leq 4.8\%$ in our protocol. We do not put any restriction on the key symmetry in this case. The main steps of the strategy B are the following:

1. Find the value of the maximum coincidences (Y-axis) and the position of the maximum coincidence (X-axis) in both plots (see Fig. 4.7 in Section 4.4.7 as a reference).
2. Place the window markers (W_{l_1} and W_{r_1}) on the left and the right side of the coincidence maximum; in the first peak (blue curve). Ensure that the markers are located well

- beyond the full-width-at-half-maxima (FWHM) points. Measure the key length (area under the blue curve) and the number of error bits (area under the red curve) for the said window. Measure the signal to noise (SNR) ratio as, $SNR = \text{key length}/\text{number of error bits}$.
3. Move both window markers with equal step size towards the coincidence maximum such that SNR is maximum. Measure the size of the coincidence window (distance between W_{l_1} and W_{r_1}) and place the window markers (W_{l_2} and W_{r_2}) on the second peak (red curve) such that both the size of the coincidence windows are same and the SNR value is also optimal for the second peak.
 4. Alter the window size (while keeping same window size for both peaks) by moving the markers in (or out) to ensure that the overall QBER value is closer to 4.8% but doesn't cross this threshold value.

In the similar approach as was used in strategy A, we obtain the mean value from each of the three optimized lists for key rates, QBERs and asymmetry values.

We use Algorithms 2 and 3 to implement the strategies A and B respectively. Algorithm 4 describes the function **QKD** used extensively in both Algorithms 2 and 3 which estimate the key rate, QBER and SNR value from any two lists of photon time stamps recorded by Alice and Bob.

Algorithm 2 Algorithm for the optimization strategy A mentioned in the QKD experiment in Section 4.4.7.

Require:

REAL STEPQ	▷ Step size for updating the threshold QBER
REAL SEEDQBOUND	▷ Threshold for the seed QBER value to initiate optimization
UNSIGNED INTEGER LEFTWIN1	▷ Left window marker position (in ps) for the first curve
UNSIGNED INTEGER RIGHTWIN1	▷ Right window marker position (in ps) for the first curve
UNSIGNED INTEGER LEFTWIN2	▷ Left window marker position (in ps) for the second curve
UNSIGNED INTEGER RIGHTWIN2	▷ Right window marker position (in ps) for the second curve
UNSIGNED INTEGER RUNTIME	▷ Measurement runtime for each dataset in seconds
UNSIGNED INTEGER TOTNUMDATA	▷ Total number of data sets measured in a run
REAL MINASYMMETRY	▷ Minimum threshold value for asymmetry estimation
REAL MAXASYBOUND	▷ Maximum threshold value for asymmetry estimation
REAL QBOUND	▷ Actual threshold value for the QBER estimation
UNSIGNED INTEGER STEPSIZEWIN	▷ Step size (in ps) for shrinking the window span
UNSIGNED INTEGER LENALICETIMESTAMPS	▷ Length of Alice's detected photon time stamps array
UNSIGNED INTEGER [LENALICETIMESTAMPS] ALICETIMESTAMPS	▷ Alice's detected photon time stamps array
CHAR D	▷ Input for selecting Bob's measurement in diagonal basis
CHAR R	▷ Input for selecting Bob's measurement in rectilinear basis

UNSIGNED INTEGER LENBOBTIMESTAMPSD ▷ Length of the time stamps array
for Bob's detection in diagonal basis

UNSIGNED INTEGER [LENBOBTIMESTAMPSD] BOBTIMESTAMPSD ▷
Time stamps array for Bob's photons detected in diagonal basis

UNSIGNED INTEGER LENBOBTIMESTAMPSR ▷ Length of the time stamps array
for Bob's detection in rectilinear basis

UNSIGNED INTEGER [LENBOBTIMESTAMPSR] BOBTIMESTAMPSR ▷ Time
stamps array for Bob's photons detected in rectilinear basis

REAL [TOTNUMDATA] OPTKEYRATE ▷ Array containing all optimized key rates

REAL [TOTNUMDATA] OPTQ ▷ Array containing all optimized QBERs

REAL [TOTNUMDATA] OPTASYM ▷ Array containing all optimized
asymmetry values

UNSIGNED INTEGER CURRDATASET ▷ Pointer to the current dataset in a given
run

Ensure:

REAL [TOTNUMDATA] OPTKEYRATE ▷ Updated array with optimized key rates
upto the current dataset

REAL [TOTNUMDATA] OPTQ ▷ Updated array with optimized QBERs upto the
current dataset

REAL [TOTNUMDATA] OPTASYM ▷ Updated array with optimized asymmetry
values upto the current dataset

UNSIGNED INTEGER NEXTDATASET ▷ Pointer to the next dataset in a given run

1: **procedure** OPTIMIZATIONSTRATEGYA(LEFTWIN1, RIGHTWIN1, LEFTWIN2,
RIGHTWIN2, RUNTIME, TOTNUMDATA, QBOUND, SEEDQBOUND, STEPQ, MINASYM-
METRY, MAXASYBOUND, STEPSIZEWIN, LENALICETIMESTAMPS, ALICETIMES-
TAMPS, LENBOBTIMESTAMPSD, BOBTIMESTAMPSD, LENBOBTIMESTAMPSR, BOB-
TIMESTAMPSR, OPTKEYRATE, OPTQ, OPTASYM, CURRDATASET, D, R)

2:	REAL MINQBOUND	▷ Minimum threshold value for QBER estimation
3:	REAL MAXQBOUND	▷ Maximum threshold value for QBER estimation
4:	UNSIGNED INTEGER FLAG	▷ Indicator to hasten or delay the convergence of optimized results
5:	UNSIGNED INTEGER TEMPSTEPSize1	▷ Temporary optimization step size for the first curve
6:	UNSIGNED INTEGER TEMPSTEPSize2	▷ Temporary optimization step size for the second curve
7:	REAL [5] RESULTSCURVE1	▷ Array to store the estimated results for the first curve
8:	REAL [5] RESULTSCURVE2	▷ Array to store the estimated results for the second curve
9:	REAL KEY1	▷ Stores the optimized key rate for the first curve
10:	REAL KEY2	▷ Stores the optimized key rate for the second curve
11:	REAL QBER	▷ Stores the optimized QBER for both curves
12:	REAL ASYMMETRY	▷ Stores the optimized asymmetry value for both curves
13:	REAL UPKEY1	▷ Stores the updated value of the key rate for the first curve
14:	REAL UPKEY2	▷ Stores the updated value of the key rate for the second curve
15:	REAL UPQBER	▷ Stores the updated value of the QBER for both curves
16:	REAL UPASYMMETRY	▷ Stores the updated value of the asymmetry for both curves
17:	UNSIGNED INTEGER ITERLEFT	▷ Iterator for the left window position
18:	UNSIGNED INTEGER ITERRIGHT	▷ Iterator for the right window position
19:	UNSIGNED INTEGER LOOPCOUNT	▷ Loop counter
20:	KEY1 $\leftarrow$ 0	▷ Initializes the optimized key rate for the first curve to zero
21:	KEY2 $\leftarrow$ 0	▷ Initializes the optimized key rate for the second curve to zero
22:	QBER $\leftarrow$ 0	▷ Initializes the optimized QBER to zero
23:	ASYMMETRY $\leftarrow$ 0	▷ Initializes the optimized asymmetry value to zero
24:	UPKEY1 $\leftarrow$ 0	▷ Initializes the updated key rate for the first curve to zero
25:	UPKEY2 $\leftarrow$ 0	▷ Initializes the updated key rate for the second curve to zero
26:	UPQBER $\leftarrow$ 0	▷ Initializes the updated QBER to zero

```

27:    UPASYMMETRY  $\leftarrow$  0           $\triangleright$  Initializes the updated asymmetry value to zero
28:    LOOPCOUNT  $\leftarrow$  0           $\triangleright$  Initializes the loop counter to zero
29:    while QBER < QBOUND do       $\triangleright$  Checks that the QBER remains within threshold
30:        MINQBOUND  $\leftarrow$  SEEDQBOUND  $-$  STEPQ           $\triangleright$  Updates the minimum
        threshold value for QBER estimation
31:        MAXQBOUND  $\leftarrow$  SEEDQBOUND  $+$  STEPQ           $\triangleright$  Updates the maximum
        threshold value for QBER estimation
32:        LOOPCOUNT  $\leftarrow$  LOOPCOUNT  $+$  1           $\triangleright$  Updates the loop counter at each
        iteration
33:        FLAG  $\leftarrow$  0           $\triangleright$  Initializes the flag to zero
34:        TEMPSTEPSize1  $\leftarrow$  STEPSizeWIN     $\triangleright$  Initializes the step size iterator for the
        first curve with the user input window step size
35:        ITERLEFT  $\leftarrow$  LEFTWIN1           $\triangleright$  Initializes the iterator with left window start
        position for the first curve
36:        ITERRIGHT  $\leftarrow$  RIGHTWIN1     $\triangleright$  Initializes the iterator with right window start
        position for the first curve
37:        while ITERRIGHT  $-$  ITERLEFT > 0 do           $\triangleright$  Iterates until the two windows
        cross each other
38:        RESULT1  $\leftarrow$  QKD (ITERLEFT, ITERRIGHT, ALICETimeStamps, BOB-
        TimeStampsD, BOBTimeStampsR, RUNTIME, D)           $\triangleright$  Assigns the estimated
        results of Key rate, QBER, signal, noise and SNR for the first curve
39:        if RESULT1[2] > MAXQBOUND then           $\triangleright$  Checks if the estimated QBER
        is above the threshold maximum
40:            if FLAG = 2 then
41:                TEMPSTEPSize1  $\leftarrow$  TEMPSTEPSize1  $-$  1           $\triangleright$  Hastens the
                convergence rate by 1 ps
42:            end if
43:            ITERRIGHT  $\leftarrow$  ITERRIGHT  $-$  TEMPSTEPSize1           $\triangleright$  Shifts the right
        window iterator towards the global or central maximum

```

```

44:          ITERLEFT  $\leftarrow$  ITERLEFT + TEMPSTEPSize1      ▷ Shifts the left
        window iterator towards the global or central maximum
45:          FLAG  $\leftarrow$  1                                  ▷ Updates the flag
46:      else
47:          if RESULT1[2] < MINQBOUND then      ▷ Checks if estimated QBER is
        below the threshold minima
48:              if FLAG = 1 then
49:                  TEMPSTEPSize1  $\leftarrow$  TEMPSTEPSize1 - 1    ▷ Hastens the
        convergence rate by 1 ps
50:              end if
51:          ITERRIGHT  $\leftarrow$  ITERRIGHT + TEMPSTEPSize1      ▷ Shifts the
        right window iterator away from the global or central maximum
52:          ITERLEFT  $\leftarrow$  ITERLEFT - TEMPSTEPSize1      ▷ Shifts the left
        window iterator away from the global or central maximum
53:          FLAG  $\leftarrow$  2                                  ▷ Updates the flag
54:      else
55:          break      ▷ Quits due to saturation of the QBER at the threshold
56:      end if
57:  end if
58: end while
59:  TEMPSTEPSize2  $\leftarrow$  STEPSizeWin    ▷ Initializes the step size iterator for the
        second curve with the user input window step size
60:  FLAG  $\leftarrow$  0      ▷ Resets the flag to zero
61:  ITERLEFT  $\leftarrow$  LEFTWin2    ▷ Re-initializes the iterator with left window start
        position for the second curve
62:  ITERRIGHT  $\leftarrow$  RIGHTWin2    ▷ Re-initializes the iterator with right window
        start position for the second curve
63:  while ITERRIGHT - ITERLEFT > 0 and TEMPSTEPSize2 > 0 do      ▷
        Iterates until the two windows cross each other

```

```

64:      RESULT2  $\leftarrow$  QKD(ITERLEFT, ITERRIGHT, ALICETIMESTAMPS, BOB-
      TIMESTAMPSD, BOBTIMESTAMPSR, RUNTIME, R)  $\triangleright$  Assigns the estimated values of
      key rate, QBER, signal, noise and SNR for the second curve
65:      KEY2  $\leftarrow$  RESULT2[1]  $\triangleright$  Stores the current key rate obtained for the
      second curve
66:      QBER  $\leftarrow$   $\frac{(\text{RESULT1}[4] + \text{RESULT2}[4]) \times 100}{(\text{RESULT1}[3] + \text{RESULT1}[4] + \text{RESULT2}[3] + \text{RESULT2}[4])}$   $\triangleright$ 
      Calculates the total QBER from the estimated signal and noise values
67:      ASYMMETRY  $\leftarrow$   $\frac{(\text{RESULT2}[3] \times 100)}{(\text{RESULT1}[3] + \text{RESULT2}[3])}$   $\triangleright$  Calculate the asymmetry
      value from the estimated signal values
68:      if ASYMMETRY > MAXASYBOUND then  $\triangleright$  Checks if estimated
      asymmetry value is above the threshold maximum
69:          if FLAG = 2 then
70:              TEMPSTEPSize2  $\leftarrow$  TEMPSTEPSize2 - 1  $\triangleright$  Hasten the
              convergence rate by 1 ps
71:          end if
72:          ITERRIGHT  $\leftarrow$  ITERRIGHT - TEMPSTEPSize2  $\triangleright$  Shifts the right
              window towards global or central maximum
73:          ITERLEFT  $\leftarrow$  ITERLEFT + TEMPSTEPSize2  $\triangleright$  Shifts the left
              window towards global or central maximum
74:          FLAG  $\leftarrow$  1  $\triangleright$  Updates the flag
75:      else
76:          if ASYMMETRY < MINASYMMETRY then  $\triangleright$  Checks if estimated
              asymmetry value is below the threshold minimum
77:              if FLAG = 1 then
78:                  TEMPSTEPSize2  $\leftarrow$  TEMPSTEPSize2 - 1  $\triangleright$  Hasten the
                  convergence rate by 1 ps
79:              end if
80:              ITERRIGHT  $\leftarrow$  ITERRIGHT + TEMPSTEPSize2  $\triangleright$  Shifts the
              right window away from the global or central maximum

```

```

81:          ITERLEFT  $\leftarrow$  ITERLEFT  $-$  TEMPSTEPSize2       $\triangleright$  Shifts the left
           window away from the global or central maximum

82:          FLAG  $\leftarrow$  2                                   $\triangleright$  Updates the flag

83:      else

84:          break       $\triangleright$  Quits due to the saturation of the asymmetry value at the
           threshold

85:      end if

86:  end if

87:  end while

88:  if QBER < QBOUND then

89:      UPKEY1  $\leftarrow$  KEY1       $\triangleright$  Stores the previous value of key rate for the first
           curve

90:      UPKEY2  $\leftarrow$  KEY2       $\triangleright$  Stores the previous key rate obtained for the
           second curve

91:      UPQBER  $\leftarrow$  QBER       $\triangleright$  Stores the previous QBER obtained for both curves

92:      UPASYMMETRY  $\leftarrow$  ASYMMETRY       $\triangleright$  Stores the previous asymmetry
           value obtained for both curves

93:      end if

94:  end while

95:  OPTKEYRATE [CURRDATASET]  $\leftarrow$  UPKEY1 + UPKEY2       $\triangleright$  Stores the optimized
           key rates for the current measurement set

96:  OPTQ [CURRDATASET]  $\leftarrow$  UPQBER       $\triangleright$  Stores the optimized QBER for the
           current measurement set

97:  OPTASYM [CURRDATASET]  $\leftarrow$  UPASYMMETRY       $\triangleright$  Stores the asymmetry value
           for the current measurement set

98:  NEXTDATASET  $\leftarrow$  CURRDATASET + 1       $\triangleright$  Updates the pointer to the next dataset

99:  return OPTKEYRATE, OPTQ, OPTASYM, NEXTDATASET       $\triangleright$  Returns the
           specified outputs

100: end procedure

```

Algorithm 3 Algorithm for the optimization strategy B mentioned in the QKD experiment in Section 4.4.7.

Require:

REAL STEPQ	▷ Step size for updating the threshold QBER
REAL GLOBALMAX1	▷ Global maximum point of the first curve
REAL GLOBALMAX2	▷ Global maximum point of the second curve
REAL MINQBOUND	▷ Minimum threshold value for QBER estimation
REAL MAXQBOUND	▷ Maximum threshold value for QBER estimation
UNSIGNED INTEGER LEFTWIN1	▷ Left window marker position (in ps) for the first curve
UNSIGNED INTEGER RIGHTWIN1	▷ Right window marker position (in ps) for the first curve
UNSIGNED INTEGER LEFTWIN2	▷ Left window marker position (in ps) for the second curve
UNSIGNED INTEGER RIGHTWIN2	▷ Right window marker position (in ps) for the second curve
UNSIGNED INTEGER RUNTIME	▷ Measurement runtime for each dataset in seconds
UNSIGNED INTEGER TOTNUMDATA	▷ Total number of data sets measured in a run
REAL QBOUND	▷ Actual threshold value for the QBER estimation
UNSIGNED INTEGER STEPSIZEWIN	▷ Step size (in ps) for shrinking the window span
UNSIGNED INTEGER LENALICETIMESTAMPS	▷ Length of Alice's detected photon time stamps array
UNSIGNED INTEGER [LENALICETIMESTAMPS] ALICETIMESTAMPS	▷ Alice's detected photon time stamps array
UNSIGNED INTEGER LENBOBTIMESTAMPSD	▷ Length of the time stamps array for Bob's detection in diagonal basis
UNSIGNED INTEGER [LENBOBTIMESTAMPSD] BOBTIMESTAMPSD	▷ Time stamps array for Bob's photons detected in diagonal basis

UNSIGNED INTEGER LENBOBTIMESTAMPSR	▷ Length of the time stamps array for Bob's detection in rectilinear basis
UNSIGNED INTEGER [LENBOBTIMESTAMPSR] BOBTIMESTAMPSR	▷ Time stamps array for Bob's photons detected in rectilinear basis
REAL [TOTNUMDATA] OPTKEYRATE	▷ Array containing all optimized key rates
REAL [TOTNUMDATA] OPTQ	▷ Array containing all optimized QBERs
REAL [TOTNUMDATA] OPTASYM	▷ Array containing all optimized asymmetry values
UNSIGNED INTEGER CURRDATASET	▷ Pointer to the current dataset in a given run
CHAR D	▷ Input for selecting Bob's measurement in diagonal basis
CHAR R	▷ Input for selecting Bob's measurement in rectilinear basis

Ensure:

REAL [TOTNUMDATA] OPTKEYRATE	▷ Updated array with optimized key rates upto the current dataset
REAL [TOTNUMDATA] OPTQ	▷ Updated array with optimized QBERs upto the current dataset
REAL [TOTNUMDATA] OPTASYM	▷ Updated array with optimized asymmetry values upto the current dataset

UNSIGNED INTEGER NEXTDATASET ▷ Pointer to the next dataset in a given run

- 1: **procedure** OPTIMIZATIONSTRATEGYB(GLOBALMAX1, GLOBALMAX2, MINQBOUND, MAXQBOUND, LEFTWIN1, RIGHTWIN1, LEFTWIN2, RIGHTWIN2, RUNTIME, TOTNUMDATA, QBOUND, SEEDQBOUND, STEPQ, STEPSIZEWIN, LENALICE-TIMESTAMPS, ALICETIMESTAMPS, LENBOBTIMESTAMPSD, BOBTIMESTAMPSD, LENBOBTIMESTAMPSR, BOBTIMESTAMPSR, OPTKEYRATE, OPTQ, OPTASYM, CURRDATASET, D, R)
 - 2: UNSIGNED INTEGER FLAG ▷ Indicator to hasten or delay the convergence of optimized results
 - 3: UNSIGNED INTEGER TEMPSTEPSize1 ▷ Temporary optimization step size for the first curve
-

4:	UNSIGNED INTEGER TEMPSTEPSize2	▷ Temporary optimization step size for the second curve
5:	REAL [5] RESULTSCurve1	▷ Array to store the estimated results for the first curve
6:	REAL [5] RESULTSCurve2	▷ Array to store the estimated results for the second curve
7:	REAL SNR1	▷ Stores the optimized signal-to-noise ratio for the first curve
8:	REAL SNR2	▷ Store the optimized signal-to-noise ratio for the second curve
9:	REAL QBER	▷ Stores the optimized QBER for both curves
10:	REAL ASYMMETRY	▷ Stores the optimized asymmetry value for both curves
11:	REAL REMSNR1	▷ Stores the previous value of the signal-to-noise ratio obtained for the first curve
12:	REAL REMSNR2	▷ Stores the previous value of the signal-to-noise ratio obtained for the second curve
13:	UNSIGNED INTEGER WINSPAN1	▷ Stores the window span for the first curve
14:	UNSIGNED INTEGER WINSPAN2	▷ Stores the window span for the second curve
15:	UNSIGNED INTEGER ITERLEFT1	▷ Iterator for the left window marker position for first curve
16:	UNSIGNED INTEGER ITERRIGHT1	▷ Iterator for the right window marker position for first curve
17:	UNSIGNED INTEGER ITERLEFT2	▷ Iterator for the left window marker position for second curve
18:	UNSIGNED INTEGER ITERRIGHT2	▷ Iterator for the right window marker position for second curve
19:	REMSNR2 $\leftarrow$ 0	▷ Initializes the previously optimized SNR for the second curve to zero
20:	FLAG $\leftarrow$ 0	▷ Initializes the flag to zero
21:	TEMPSTEPSize1 $\leftarrow$ STEPSizeWin	▷ Initializes the step size iterator for the first curve with the user input window step size

```

22:    ITERLEFT1  $\leftarrow$  LEFTWIN1            $\triangleright$  Initializes the iterator with left window start
        position for the first curve
23:    ITERRIGHT1  $\leftarrow$  RIGHTWIN1          $\triangleright$  Initializes the iterator with right window start
        position for the first curve
24:    REMSNR1  $\leftarrow$  0            $\triangleright$  Initializes the previously optimized SNR for the first curve to
        zero
25:    while ITERRIGHT1 – ITERLEFT1 > 0 do            $\triangleright$  Loops until the two window
        markers cross each other
26:        RESULT1  $\leftarrow$  QKD (ITERLEFT1, ITERRIGHT1, ALICETIMESTAMPS, BOB-
        TIMESTAMPSD, BOBTIMESTAMPSR, RUNTIME, D)            $\triangleright$  Assigns the estimated
        results of Key rate, QBER, signal, noise and SNR for the first curve
27:        if RESULT1 [5] > REMSNR1 then            $\triangleright$  Checks if the estimated SNR is
        increasing
28:            if FLAG = 2 then
29:                TEMPSTEPSize1  $\leftarrow$  TEMPSTEPSize1 – 1            $\triangleright$  Hastens the
                convergence rate by 1 ps
30:            end if
31:            ITERRIGHT1  $\leftarrow$  ITERRIGHT1 – TEMPSTEPSize1            $\triangleright$  Shifts the right
                window marker towards global maxima
32:            ITERLEFT1  $\leftarrow$  ITERLEFT1 + TEMPSTEPSize1            $\triangleright$  Shifts the left window
                marker towards global maxima
33:            FLAG  $\leftarrow$  1            $\triangleright$  Updates the flag
34:        else
35:            if RESULT1 [5] < REMSNR1 then            $\triangleright$  Checks if the estimated SNR is
                decreasing
36:                if FLAG = 1 then
37:                    TEMPSTEPSize1  $\leftarrow$  TEMPSTEPSize1 – 1            $\triangleright$  Hastens the
                    convergence rate by 1 ps
38:                end if

```

```

39:          ITERRIGHT1  $\leftarrow$  ITERRIGHT1 + TEMPSTEPSize1    ▷ Shifts the right
        window marker away from the global maxima
40:          ITERLEFT1  $\leftarrow$  ITERLEFT1 - TEMPSTEPSize1      ▷ Shifts the left
        window marker away from the global maxima
41:          FLAG  $\leftarrow$  2                                     ▷ Updates the flag
42:      else
43:          break                                             ▷ Quits as further maximization of SNR is not possible
44:      end if
45:  end if
46:      REMSNR1  $\leftarrow$  SNR1    ▷ Saves the current optimized SNR for the first curve
47:  end while
48:      WINSPAN1  $\leftarrow$  (GLOBALMAX1 - ITERLEFT1) + (ITERRIGHT1 - GLOBALMAX1)
        ▷ Saves the optimized window span for the first curve
49:      TEMPSTEPSize2  $\leftarrow$  STEPSizeWIN    ▷ Initializes the step size iterator for the
        second curve with the user input step size
50:      FLAG  $\leftarrow$  0                                ▷ Re-initializing the flag to zero
51:      ITERLEFT2  $\leftarrow$  LEFTWIN2    ▷ Initializes the iterator with left window start
        position for the second curve
52:      ITERRIGHT2  $\leftarrow$  RIGHTWIN2    ▷ Initializes the iterator with right window start
        position for the second curve
53:      REMSNR2  $\leftarrow$  0    ▷ Initializes the previously optimized SNR for the second
        curve to zero
54:      while ITERRIGHT2 - ITERLEFT2 > 0 and TEMPSTEPSize2 > 0 do    ▷ Loops
        until the two window markers cross each other
55:          RESULT2  $\leftarrow$  QKD(ITERLEFT2, ITERRIGHT2, ALICETimeSTAMPS, BOB-
        TimeSTAMPSD, BOBTimeSTAMPSR, RUNTIME, R) ▷ Assigns the estimated results of
        Key rate, QBER, signal, noise and SNR for the second curve
56:          if RESULT2[5] > REMSNR2 then    ▷ Checks if the estimated SNR is
        increasing

```

```

57:         if FLAG = 2 then
58:             TEMPSTEPSize2  $\leftarrow$  TEMPSTEPSize2 - 1           ▷ Hastens the
               convergence rate by 1 ps
59:         end if
60:             ITERRIGHT2  $\leftarrow$  ITERRIGHT2 - TEMPSTEPSize2       ▷ Shifts the right
               window towards global maxima
61:             ITERLEFT2  $\leftarrow$  ITERLEFT2 + TEMPSTEPSize2       ▷ Shifts the left window
               towards global maxima
62:             FLAG  $\leftarrow$  1                                       ▷ Updates the flag
63:         else
64:             if RESULT2[5] < REMSNR2 then           ▷ Checks if estimated SNR is
               decreasing
65:                 if FLAG = 1 then
66:                     TEMPSTEPSize2  $\leftarrow$  TEMPSTEPSize2 - 1       ▷ Hastens the
               convergence rate by 1 ps
67:                 end if
68:                     ITERRIGHT2  $\leftarrow$  ITERRIGHT2 + TEMPSTEPSize2   ▷ Shifts the right
               window marker away from the global maxima
69:                     ITERLEFT2  $\leftarrow$  ITERLEFT2 - TEMPSTEPSize2     ▷ Shifts the left
               window marker away from the global maxima
70:                     FLAG  $\leftarrow$  2                                   ▷ Updates the flag
71:                 else
72:                     break           ▷ Quits as further maximization of SNR is not possible
73:                 end if
74:             end if
75:         end while
76:     WINSPAN2  $\leftarrow$  (GLOBALMAX2 - ITERLEFT2) + (ITERRIGHT2 - GLOBALMAX2)
               ▷ Saves the optimized window span for the second curve

```

```

77:   ADJUSTBY  $\leftarrow \frac{(\text{WINSPAN1} - \text{WINSPAN2})}{2}$       ▷ Stores the difference in window
      span sizes between first and second curve

78:   ITERLEFT2  $\leftarrow \text{ITERLEFT2} - \text{CEIL}(\text{ADJUSTBY})$       ▷ Re-initializes the iterator
      with adjusted position for the left window marker of the second curve

79:   ITERRIGHT2  $\leftarrow \text{ITERRIGHT2} + \text{FLOOR}(\text{ADJUSTBY})$       ▷ Re-initializes the
      iterator with adjusted position for the right window marker of the second curve

80:   RESULT2  $\leftarrow \text{QKD}(\text{ITERLEFT2}, \text{ITERRIGHT2}, \text{ALICETIMESTAMPS}, \text{BOBTIMESTAMPSD}, \text{BOBTIMESTAMPSR}, \text{RUNTIME}, \text{R})$ 
      ▷ Re-assigns the estimated results of Key
      rate, QBER, signal, noise and SNR for the second curve

81:   QBER  $\leftarrow \frac{(\text{RESULT1}[4] + \text{RESULT2}[4]) \times 100}{(\text{RESULT1}[3] + \text{RESULT1}[4] + \text{RESULT2}[3] + \text{RESULT2}[4])}$       ▷ Calculates
      the total QBER from the estimated signal and noise values

82:   ASYMMETRY  $\leftarrow \frac{(\text{RESULT2}[3] \times 100)}{(\text{RESULT1}[3] + \text{RESULT2}[3])}$       ▷ Calculates the asymmetry value
      from the estimated signal values

83:   while QBER > MAXQBOUND or QBER < MINQBOUND do      ▷ Optimizes both
      window spans to restrict the overall QBER within the threshold value

84:       if QBER < MINQBOUND then      ▷ Checks if the estimated QBER is below the
      desired range

85:           ITERLEFT1  $\leftarrow \text{ITERLEFT1} - \text{STEPQ}$       ▷ Shift the left window away from
      the global maxima of the first curve

86:           ITERRIGHT1  $\leftarrow \text{ITERRIGHT1} + \text{STEPQ}$       ▷ Shift the right window away
      from the global maxima of the first curve

87:           ITERLEFT2  $\leftarrow \text{ITERLEFT2} - \text{STEPQ}$       ▷ Shift the left window away from
      the global maxima of the second curve

88:           ITERRIGHT2  $\leftarrow \text{ITERRIGHT2} + \text{STEPQ}$       ▷ Shift the right window away
      from the global maxima of the second curve

89:       else

90:           ITERLEFT1  $\leftarrow \text{ITERLEFT1} + \text{STEPQ}$       ▷ Shifts the left window towards
      the global maxima of the first curve

91:           ITERRIGHT1  $\leftarrow \text{ITERRIGHT1} - \text{STEPQ}$       ▷ Shifts the right window
      towards the global maxima of the first curve

```

```

92:      ITERLEFT2  $\leftarrow$  ITERLEFT2 + STEPQ       $\triangleright$  Shifts the left window towards
      global maxima of the second curve
93:      ITERRIGHT2  $\leftarrow$  ITERRIGHT2 - STEPQ       $\triangleright$  Shifts the right window
      towards global maxima of the second curve
94:      end if
95:      RESULT1  $\leftarrow$  QKD(ITERLEFT1, ITERRIGHT1, ALICETIMESTAMPS, BOB-
      TIMESTAMPSD, BOBTIMESTAMPSR, RUNTIME, D)  $\triangleright$  Re-assigns the estimated results
      of Key rate, QBER, signal, noise and SNR for the first curve
96:      RESULT2  $\leftarrow$  QKD(ITERLEFT2, ITERRIGHT2, ALICETIMESTAMPS, BOB-
      TIMESTAMPSD, BOBTIMESTAMPSR, RUNTIME, R)  $\triangleright$  Re-assigns the estimated results
      of Key rate, QBER, signal, noise and SNR for the second curve
97:      QBER  $\leftarrow \frac{(\text{RESULT1}[4] + \text{RESULT2}[4]) \times 100}{(\text{RESULT1}[3] + \text{RESULT1}[4] + \text{RESULT2}[3] + \text{RESULT2}[4])}$        $\triangleright$  Updates
      the total QBER for the revised window positions
98:      ASYMMETRY  $\leftarrow \frac{(\text{RESULT2}[3] \times 100)}{(\text{RESULT1}[3] + \text{RESULT2}[3])}$        $\triangleright$  Updates the key symmetry
      value corresponding to the revised window positions
99:      end while
100:     OPTKEYRATE[CURRDATASET]  $\leftarrow$  RESULT1[1] + RESULT2[1]       $\triangleright$  Stores the
      optimized key rates for the current measurement set
101:     OPTQ[CURRDATASET]  $\leftarrow$  QBER       $\triangleright$  Stores the optimized QBER for the current
      measurement set
102:     OPTASYM[CURRDATASET]  $\leftarrow$  ASYMMETRY       $\triangleright$  Stores the key symmetry value
      for the current measurement set
103:     NEXTDATASET  $\leftarrow$  CURRDATASET + 1       $\triangleright$  Updates the pointer to the next dataset
104:     return OPTKEYRATE, OPTQ, OPTASYM, NEXTDATASET       $\triangleright$  Returns the
      specified outputs
105: end procedure

```

Please refer to Appendix C for details on the usage of data types and libraries, at various instances, in the above two optimization algorithms.

Algorithm 4 Estimation of key rate, QBER and signal to noise ratio (SNR) from detected photon time stamps by Alice and Bob

Require:

UNSIGNED INTEGER WINLEFT ▷ Left window marker position (in ps)

UNSIGNED INTEGER WINRIGHT ▷ Right window marker position (in ps)

UNSIGNED INTEGER LENALICETIMESTAMPS ▷ Length of Alice's detected
photon time stamps array

UNSIGNED INTEGER [LENALICETIMESTAMPS] ALICETIMESTAMPS ▷ Alice's
detected photon time stamps array

UNSIGNED INTEGER LENBOBTIMESTAMPSD ▷ Length of the time stamps array
for Bob's detection in diagonal basis

UNSIGNED INTEGER [LENBOBTIMESTAMPSD] BOBTIMESTAMPSD ▷ Time
stamps array for Bob's detection in diagonal basis

UNSIGNED INTEGER LENBOBTIMESTAMPSR ▷ Length of the time stamps array
for Bob's detection in rectilinear basis

UNSIGNED INTEGER [LENBOBTIMESTAMPSR] BOBTIMESTAMPSR ▷ Time
stamps array for Bob's detection in rectilinear basis

UNSIGNED INTEGER TOTALTIME ▷ Total data collection time in seconds

CHAR BASISCHOICE ▷ Choice of measurement basis: rectilinear (R) or diagonal
(D)

Ensure:

REAL KEYRATE ▷ Estimated key rate

REAL QBER ▷ Estimated QBER

UNSIGNED INTEGER SIGNAL ▷ Estimated signal value

UNSIGNED INTEGER NOISE ▷ Estimated noise value

REAL SNR ▷ Estimated signal-to-noise ratio

1: **function** QKD(WINLEFT, WINRIGHT, LENALICETIMESTAMPS, ALICETIMESTAMPS,
LENBOBTIMESTAMPSD, BOBTIMESTAMPSD, LENBOBTIMESTAMPSR, BOBTIMESTAMPSR,
TOTALTIME, BASISCHOICE)

2: UNSIGNED INTEGER I ▷ Iterates over Eve's detection list

3: UNSIGNED INTEGER J ▷ Iterates over Eve's detection list

```

4:    UNSIGNED INTEGER SIGNAL          ▷ Stores the estimated signal value along
    matched bases

5:    UNSIGNED INTEGER NOISE          ▷ Stores the estimated noise value along
    mismatched bases

6:    REAL KEYRATE                    ▷ Stores the estimated key rate

7:    REAL QBER                      ▷ Stores the estimated QBER

8:    switch BASISCHOICE do          ▷ Collects the measurement basis choice to estimate
    the signal and noise along it

9:        case D                      ▷ Measurements along the chosen diagonal basis

10:            I ← 1                  ▷ Initializes the iterator to the first element on Alice's detection list

11:            J ← 1                  ▷ Initializes the iterator to the first element on Bob's detection list

12:            SIGNAL ← 0             ▷ Initializes the counter for coincidences along matched
    bases to zero

13:            while I ≤ LENALICETIMESTAMPS & J ≤ LENBOBTIMESTAMPSD do
                                ▷ Loops over both time stamp lists

14:                if BOBTIMESTAMPSD[J] − ALICETIMESTAMPS[I] < WINLEFT
    then                        ▷ Rejects any detection beyond the current left window position

15:                    J ← J + 1      ▷ Increments the detection interval

16:                end if

17:                if BOBTIMESTAMPSD[J] − ALICETIMESTAMPS[I] ≤ WINRIGHT &
    BOBTIMESTAMPSD[J] − ALICETIMESTAMPS[i] ≥ WINLEFT then      ▷ Rejects any
    detection outside the current window span

18:                    SIGNAL ← SIGNAL + 1          ▷ Increments the signal counter

19:                    I ← I + 1                    ▷ Increments the pointer on Alice's detection list

20:                    J ← J + 1                    ▷ Increments the pointer on Bob's detection list for the
    diagonal basis

21:                end if

22:                if BOBTIMESTAMPSD[J] − ALICETIMESTAMPS[I] > WINRIGHT
    then                        ▷ Rejects any detection beyond the right window position

23:                    I ← I + 1                    ▷ Decrements the detection interval

```

```

24:          end if
25:          end while
26:           $I \leftarrow 1$        $\triangleright$  Re-initializes the iterator to the first element of Eve's detection
list
27:           $J \leftarrow 1$        $\triangleright$  Re-initializes the iterator to the first element of Eve's detection
list
28:           $\text{NOISE} \leftarrow 0$      $\triangleright$  Initializes the counter for coincidences along mismatched
bases to zero
29:          while  $I \leq \text{LENALICETIMESTAMPS}$  &  $J \leq \text{LENBOBTIMESTAMPSR}$  do       $\triangleright$ 
Loops over both time stamp lists
30:              if  $\text{BOBTIMESTAMPSR}[J] - \text{ALICETIMESTAMPS}[I] < \text{WINLEFT}$  then
 $\triangleright$  Rejects any detection beyond the current left window position
31:                   $J \leftarrow J + 1$        $\triangleright$  Increments the detection interval
32:              end if
33:              if  $\text{BOBTIMESTAMPSR}[J] - \text{ALICETIMESTAMPS}[I] \leq \text{WINRIGHT}$  &
 $\text{BOBTIMESTAMPSR}[J] - \text{ALICETIMESTAMPS}[I] \geq \text{WINLEFT}$  then       $\triangleright$  Rejects any
detection outside the current window span
34:                   $\text{NOISE} \leftarrow \text{NOISE} + 1$        $\triangleright$  Increments the noise counter
35:                   $I \leftarrow I + 1$        $\triangleright$  Increments the pointer on Alice's detection list
36:                   $J \leftarrow J + 1$        $\triangleright$  Increments the pointer on Bob's detection list for the
rectilinear basis
37:              end if
38:              if  $\text{BOBTIMESTAMPSR}[J] - \text{ALICETIMESTAMPS}[I] > \text{WINRIGHT}$ 
then       $\triangleright$  Rejects any detection beyond the current right window position
39:                   $I \leftarrow I + 1$        $\triangleright$  Decrements the detection interval
40:              end if
41:          end while
42:          case R       $\triangleright$  Measurements along the chosen rectilinear basis
43:               $I \leftarrow 1$        $\triangleright$  Initializes the iterator to the first element on Alice's detection list
44:               $J \leftarrow 1$        $\triangleright$  Initializes the iterator to the first element on Bob's detection list

```

```

45:          SIGNAL  $\leftarrow$  0           $\triangleright$  Initializes the counter for coincidences along matched
        bases to zero

46:          while  $I \leq \text{LENALICETIMESTAMPS}$  &  $J \leq \text{LENBOBTIMESTAMPSR}$  do           $\triangleright$ 
        Loops over both time stamp lists

47:              if  $\text{BOBTIMESTAMPSR}[J] - \text{ALICETIMESTAMPS}[I] < \text{WINLEFT}$ 
        then           $\triangleright$  Rejects any detection beyond the current left window position

48:                   $J \leftarrow J + 1$            $\triangleright$  Increments the detection interval

49:              end if

50:              if  $\text{BOBTIMESTAMPSR}[J] - \text{ALICETIMESTAMPS}[I] \leq \text{WINRIGHT}$  &
         $\text{BOBTIMESTAMPSR}[J] - \text{ALICETIMESTAMPS}[I] \geq \text{WINLEFT}$  then           $\triangleright$  Rejects any
        detection outside the current window span

51:                  SIGNAL  $\leftarrow$  SIGNAL + 1           $\triangleright$  Increments the signal counter

52:                   $I \leftarrow I + 1$            $\triangleright$  Increments the pointer on Alice's detection list

53:                   $J \leftarrow J + 1$            $\triangleright$  Increments the pointer on Bob's detection list for the
        rectilinear basis

54:              end if

55:              if  $\text{BOBTIMESTAMPSR}[J] - \text{ALICETIMESTAMPS}[I] > \text{WINRIGHT}$ 
        then           $\triangleright$  Rejects any detection beyond the right window position

56:                   $I \leftarrow I + 1$            $\triangleright$  Decrements the detection interval

57:              end if

58:          end while

59:           $I \leftarrow 1$            $\triangleright$  Re-initializes the iterator to the first element of Eve's detection
        list

60:           $J \leftarrow 1$            $\triangleright$  Re-initializes the iterator to the first element of Eve's detection
        list

61:          NOISE  $\leftarrow$  0           $\triangleright$  Initializes the counter for coincidences along mismatched
        bases to zero

62:          while  $I \leq \text{LENALICETIMESTAMPS}$  &  $J \leq \text{LENBOBTIMESTAMPSD}$  do
           $\triangleright$  Loops over both time stamp lists

63:              if  $\text{BOBTIMESTAMPSD}[J] - \text{ALICETIMESTAMPS}[I] < \text{WINLEFT}$  then
           $\triangleright$  Rejects any detection beyond the current left window position

```

```

64:           $J \leftarrow J + 1$                                 ▷ Increments the detection interval
65:      end if
66:      if  $\text{BOBTIMESTAMPSD}[J] - \text{ALICETIMESTAMPS}[I] \leq \text{WINRIGHT}$  &
         $\text{BOBTIMESTAMPSD}[J] - \text{ALICETIMESTAMPS}[I] \geq \text{WINLEFT}$  then    ▷ Rejects any
        detection outside the current window span
67:           $\text{NOISE} \leftarrow \text{NOISE} + 1$                     ▷ Increments the noise counter
68:           $I \leftarrow I + 1$                                 ▷ Increments the pointer on Alice's detection list
69:           $J \leftarrow J + 1$     ▷ Increments the pointer on Bob's detection list for the
        diagonal basis
70:      end if
71:      if  $\text{BOBTIMESTAMPSD}[J] - \text{ALICETIMESTAMPS}[I] > \text{WINRIGHT}$ 
        then          ▷ Rejects any detection beyond the current right window position
72:           $I \leftarrow I + 1$                                 ▷ Decrements the detection interval
73:      end if
74:      end while
75:       $\text{KEYRATE} \leftarrow \frac{\text{SIGNAL} + \text{NOISE}}{\text{TOTALTIME}}$         ▷ Stores the final estimated key rate
76:       $\text{QBER} \leftarrow \frac{\text{NOISE} \times 100}{\text{SIGNAL} + \text{NOISE}}$     ▷ Stores the final estimated QBER in %
77:       $\text{SNR} \leftarrow \frac{\text{SIGNAL}}{\text{NOISE}}$                 ▷ Stores the final estimated signal-to-noise ratio
78:      return  $\text{KEYRATE}, \text{QBER}, \text{SIGNAL}, \text{NOISE}, \text{SNR}$     ▷ Returns the specified outputs
        in the order: key rate, QBER, signal, noise & SNR
79: end function

```

Please refer to Appendix C for details on the usage of various data types and libraries in the above algorithmic function.

Appendix C

General data types and library functions

Data types

Each variables used in the algorithms are declared as a certain data type. Here we list down the different data types that have been used to declare the variables.

- **UNSIGNED INTEGER:** declares the variable as a positive integer ($\mathbb{Z}^+$) in the pseudocode.
- **SIGNED INTEGER:** declares the variable as an integer ($\mathbb{Z}$) that can take both positive and negative values in the pseudocode.
- **REAL:** declares the variable as a real number ($\mathbb{R}$) that can take both positive and negative values in the pseudocode.
- **UNIT INTERVAL:** declares the variable to be in the open interval $(0, 1)$ in the pseudocode i.e., the variable can take any real value ($\mathbb{R}$) within the interval.
- **INTERVAL(a, b):** declares the variable to be in the open interval (a, b) in the pseudocode where a and b are real numbers($\mathbb{R}$).
- **DYNAMIC:** declares the variable as a dynamic array in the pseudocode.
- **CHAR:** declares the variable that can store a single character.

Libraries

Here we list down the various functions that have been used in the algorithms.

- $\text{CEIL}(N)$: return the smallest integer value that is bigger than or equal to the number N .
- $\text{FLOOR}(N)$: return the largest integer value that is smaller than or equal to the number N .