EFFECTS OF PHOTON STATISTICS ON QUANTUM RANDOM NUMBER GENERATORS AND PHOTON DETECTION EFFICIENCY

A Thesis

by

Helin Özel

Submitted to the
Graduate School of Sciences and Engineering
In Partial Fulfillment of the Requirements for
the Degree of

Master of Science

in the
Department of Electrical and Electronics Engineering

Özyeğin University
December 2021

EFFECTS OF PHOTON STATISTICS ON QUANTUM RANDOM NUMBER GENERATORS AND PHOTON DETECTION EFFICIENCY

Approved by:

Assistant Professor Kadir Durak
Department of Electrical and Electronics Engineering
Özyeğin University

Assistant Professor Ahmed Akgiray
Department of Electrical and Electronics Engineering
Özyeğin University

Professor Bulat Z. Rami
Department of Physics
Gebze Technical University

Date Approved: 27/12/2021

To those I love and value,

ABSTRACT

The effects of photon statistics on different quantum applications are explained in this thesis. There are mainly two sections: the first section focuses on the randomly bunched and coherently bunched photons' continuous detection. The second section focuses on the anti-bunched single-photon behavior and its single-photon detection. Random numbers are essential resources in cryptography, simulation technologies, and finance. The intrinsic behavior of quantum mechanics makes quantum systems a perfect source of entropy. Quantum random number generation (QRNG) is one of the most preferred quantum technologies with many alternative generation methods. Therefore, among the different technologies in quantum random number generation from the primal applications based on radioactive decay to the multiple ways to use the quantum states of light to gather entropy from a quantum base I have chosen to use the vacuum fluctuation method. In the first part of the thesis, the photon statistics of thermal and coherent light sources and their scatterings are compared. The sources with super-Poissonian distribution are shown to have better randomness than the Poisson distribution. The optimal sampling rate is obtained when the under-sampling is set as two times the lag point for the minimum autocorrelation of the scattered signal. The use of scattering mechanisms as an entropy source increased the speed and shortened the post-processing procedure significantly, opening the way for higher-speed QRNG generation technologies. In the second part of the thesis, I introduce an entanglement-based sensing protocol that achieves a signal to noise ratio (SNR) improvement over the optimal classical scheme in a highly lossy and noisy environment that completely breaks the initial entanglement property. Under high noise conditions, which might occur from the devices used in the experiment or

the imperfections sources from the open system of the setup the heralding loss will be high. It is observed that the detectors also show measurement errors, under the effect of high noise conditions and from the limitations caused by their timing jitters. The biased behavior of the detectors in near saturation conditions is supported by the cross-correlogram measurements. Emphasis was placed on the unreliability in the detections when exceeding its limitations. In such conditions, it is not possible to use the quantum advantage of the system without making any adjustments. With the application presented in this section, the result of quantum sensing clearly demonstrates that a quantum resource can be utilized beneficially even when its initial non-classical character is lost, knowing all its shortcomings and limitations.

ÖZETÇE

Foton istatistiklerinin farklı kuantum uygulamaları üzerindeki etkileri bu tezde açıklanmaktadır. Temel olarak iki bölüm vardır: Birinci bölüm rastgele demetlenmiş ve eşevreli demetlenmiş fotonların sürekli ölçümü üzerinedir. İkinci bölüm demetlenmemiş tek foton davranışına ve onun tek foton ölçümüne odaklanmaktadır. Rastgele sayılar kriptografide, simülasyon teknolojilerinde ve finansta temel kaynaklardır. Kuantum mekaniğinin içsel davranışı, kuantum sistemlerini mükemmel bir entropi kaynağı yapar. Kuantum rastgele sayı üretimi (KRSÜ), birçok alternatif üretim yöntemi ile en çok tercih edilen kuantum teknolojilerinden biridir. Bu nedenle, radyoaktif bozunmaya dayalı ilk uygulamalardan, kuantum tabanından entropi toplamak için ışığın kuantum durumlarını kullanmanın çoklu yollarına kadar olan kuantum rasgele sayı üretimindeki farklı teknolojiler arasından vakum dalgalanma yöntemini kullanmayı seçtim. Tezin bahsedilen birinci bölümünde termal ve koherent ışık kaynaklarının foton istatistikleri ve saçılmaları karşılaştırılmıştır. Süper Poisson dağılımına sahip kaynakların Poisson dağılımından daha iyi rastgeleliğe sahip olduğu gösterilmiştir. Optimum örnekleme oranı, yetersiz örnekleme, saçılan sinyalin minimum otokorelasyonu için gecikme noktasının iki katı olarak ayarlandığında elde edilir. Saçılma mekanizmalarının bir entropi kaynağı olarak kullanılması, hızı arttırdı ve son işlem prosedürünü önemli ölçüde kısalttı, daha yüksek hızlı KRSÜ üretim teknolojilerinin yolunu açtı. Tezin ikinci bölümünde başlangıçtaki dolaşıklık özelliğini tamamen kıran, oldukça kayıplı ve gürültülü bir ortamda optimal klasik şema üzerinde bir sinyal gürültü oranı (SNR) iyileştirmesi sağlayan dolaşıklık tabanlı bir algılama protokolünü tanıtıyorum. Deneyde kullanılan cihazlardan veya kurulumun açık sisteminden kaynaklanan kusur, kaynaklar oluşabilecek yüksek gürültü koşullarında

haberci kaybı yüksek olacaktır. Buna bağlı olarak dedektörlerin ayrıca yüksek gürültü koşullarının etkisi altında ve zamanlama jitterlerinden kaynaklanan sınırlamalardan dolayı ölçüm hataları gösterdiği gözlemlenmiştir. Dedektörlerin doygunluğa yakın koşullarda yanıltıcı davranışı, çapraz korelasyon ölçümleriyle desteklenir. Doygunluk bölgesi ve doygunluk sınırları aşıldığında yanıltıcı ölçüm yapabilen bu cihazların güvenilmezliğene vurgu yapıldı. Bu gibi durumlarda herhangi bir düzenleme yapmadan sistemin kuantum avantajından yararlanmak mümkün olmadığı açıklandı. Bu bölümde sunulan özel teknikli kuantum algılama sistemi sonucu, bir kuantum kaynağının, tüm eksiklikleri ve sınırlamaları bilinerek başlangıçtaki klasik olmayan özelliği kaybolduğunda bile faydalı bir şekilde kullanılabileceğini açıkça gösterilmektedir.

ACKNOWLEDGEMENTS

It has been an amazing journey since I started my Bachelor in 2014 in Özyeğin University. I am equipped with the contributions of my dear friends and valuable teachers during all those years. I am grateful to everyone I crossed paths with and learned something from:

First of all, I would like to thank my professor Kadir Durak, who introduced me to my dream job, gave me all these opportunities and never spared his support.

To Hashir, who always shared his vast knowledge with me with all his patience and humility, always worked side by side, and helped me overcame all the troubles of the pandemic by supporting each other.

Grateful to meet all those special people in our QOptics group, as a whole whom have been great colleagues and friends that will last a lifetime. Without their smiling faces and motivation, life would be much harder.

I would like to express my special thanks to Abdulrahman, for all his contributions to our study, his diligent work and never giving up.

My appreciation to Tübitak, Bilgem for the scholarship they provide for 3 years. Thanks to my colleagues and friends there, Hatun, Burcu and Adil, for their support, mentoring and special care.

Last but not least thanks to my family for believing and supporting me under any circumstances.

The researches in this thesis are supported by the Scientific and Technological Research Council of Turkey (TUBITAK) with the career grant no: 118E156 and no: 117F289 is a part of the Silicon Photonics for Quantum Fibre Networks (SQUARE) project under the QuantERA ERA-NET Cofund in Quantum Technologies program.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER I

INTRODUCTION

Every experiment presented in this thesis share many common experimental methods and mechanisms to those in the literature I will explain different aspects and my contributions to quantum random number generation and quantum detection technique. In the details, the novelty of the research and the variations from the standard experiments will be described. Additional information will be provided about the unique techniques developed to enhance the setup and for better alignment of the system. Photon statistics provides the ground basis to have a profound understanding of the quantum properties of quantum technology applications. Either in the single photon measurement or photocurrent measurement processes we analyze the photon behavior and try to enhance our system. In this thesis, in the applications of random number generation and quantum target detection scheme, the classical effects aimed to be minimized under the light of photon statistics. New methods are introduced to reduce the detectors' limitations and the electronics noise of the systems, in order to gain the maximum benefit of quantum based technologies.

Random Number Generators:

The Random Number Generator (RNG) generates a series of random numbers. Random numbers are very important for many applications. They are used as private keys when sending encrypted data, gambling machines require random numbers, and some numerical methods require random numbers. It is very difficult to confirm that RNG produces an unpredictable set of random numbers [3, 4, 5]. With a limited length of RNG output, such evidence (by statistical methods) is not possible. The RNG internal function principle model is more effective.

There are three types of RNGs:

- Pseudo RNG
- True RNG
- Quantum RNG

A pseudo-RNG (PRNG) is a deterministic mathematical algorithm that essentially "stretches" a given random seed into a much longer sequence of random numbers. Random seeds are considered "truly random" and are taken from mouse movements, for example, on a computer. Compared to other types of RNG, PRNG is very cheap. However, the origin of the random seed is heterogeneous (and therefore of questionable reliability) and is not transferable, making it unsuitable for high quality encryption. The PRNG is gradually being replaced by the True RNG or Quantum RNG. Both TRNG and QRNG generate random numbers from the results of physical processes. The resulting sequence of random numbers always has some level of predictability and is not ideal. Applying random extraction to a non-ideal random sequence produces an ideal (albeit short) random sequence. To apply the randomness extractor, you need to estimate an upper bound on the degree of predictability. There are three main ways to do this. First, an advanced model of the device. This includes all related non-ideal things (for example, detectors with limited efficiency), which is difficult. Another method is the device independent QRNG or QRNG self-test, which allows you to set limits online. True RNGs (TRNGs) obtain their random numbers from classical physical processes, which are unpredictable for all practical reasons. Unpredictability can be caused by many uncontrollable reflections on freedom (noise) or systems with chaotic behavior. Noise TRNG in electronic circuits are very cheap and small. The darker side of the matter is that the quality of random numbers produced by TRNG is debatable and difficult to assess. Building a good TRNG is a big challenge and it is practically impossible to certify it. For this reason, TRNGs often involve complex post-processing of random numbers that makes them similar to PRNGs. In addition, attacks on TRNG are known. The important feature of QRNGs is that they are non-deterministic due to the fact that they rely on laws of quantum physics unlike other algorithm which are based random number generators. Different implementations have been applied where each system has some pros and cons. Some implementations are based on single photodiodes [6, 7]. Such systems have the advantage of extracting more min-entropy per bit than the similar systems that use photodetectors (PDs) [8] which are differentiated from single photodiodes based systems that the flux they can receive is much higher [1] which means faster random number generation. The two most common PD based QRNGs are the phase fluctuation and vacuum fluctuation. Vacuum fluctuation method is applied using homodyne detection which is applicable using off-the-shelf components and can produce very fast random numbers [9, 10, 11]. Homodyne detection works on mixing the vacuum state with a local oscillator (LO), then subtracting the two signals which are detected by two photodetectors. With choosing the suitable components of the homodyne detector (optical detectors, local oscillator, etc...) the randomness of the final bit stream of the system can be credited to the intrinsic quantum fluctuations of the vacuum state. The use of scattering mechanisms as an entropy source increased the speed and shortened the post-processing procedure significantly, opened the way of higher speed QRNG generation technologies. As different detection methods have been proposed, the literature also contains various sources for the LO. Although most of the applications use continuous-wave (CW) laser as a LO, which follows the Poisson statistics. Some other methods have been implemented based on different sources as a superluminescent LED (SLED) [12] which is a thermal source that follows the super-Poissonian statistics. The randomness in a SLED originates from the wide spectrum bandwidth of the amplified spontaneous emission. Although SLEDs can provide high quality random bits knowing that produces more fluctuations than lasers, lasers provide higher flux of photons compared to SLEDs. Lasers also tend to have high temporal coherence compared to SLEDs which shows that they are more monochromatic [12]. In the second chapter of this thesis the photon statistics behavior on the continues measurement of bunched photon behavior is observed. The purpose of this chapter is to show a design of quantum random number generator based on a homodyne measurement of the vacuum field with high quality of randomness by minimizing the limitations of the classical noise, imperfections of the detector effect in photodetection. It is showed that optical scattering enhances randomness characteristics, increases the chaotic behavior of coherent sources, broadens the distribution of photon statistics and makes it super-Poissonian which allows faster sampling compared to Poissonian statistics. With a similar approach in the third chapter we observe the photon statistics effects on single photon detection in spontaneous down conversion process. The aim is to overcome all the constraints of phase-insensitive systems which are becoming increasingly popular in sensing and imaging applications, and obtain highly efficient quantum based target detection. For that, the quantum correlations are employed to test the key quantum metrology parameters such as resolution and signal-to-noise ratio (SNR). Furthermore, with the realization of photon statistics, we are able to work on high saturation detector regimes and under heavy noisy background. Next, you will be introduced to the foundation of quantum sensing and lighting systems for a deeper understanding.

Quantum sensing and target detection

In the 20^{th} century, physicists established the initials of quantum mechanics [13]. They discovered the unique feature of light, dissimilar to other physical systems, can be kept insulated and not get affected by quantum decoherence easily. That successful isolation of photons from their setting and from each other is quite enticing in utilizing the quantum properties of a system, yet it can be also a handicap considering the production procedure of entangled particles where it is especially challenging to make two photons interact with each other to create entanglement. Previous implementations have shown to generate photons, a cascaded two-photon emission process from single photons is achieved [14]. These challenging techniques are replaced eventually by the benefit of nonlinear optics. In that way, the creation of twin photons within a medium with a nonlinear response such as a nonlinear response could actualize. It appears that theoretically and experimentally it is feasible to generate photon pairs through the interaction of a single pump photon with a nonlinear medium. Likely in a three-wave interaction process between a pump photon and two lower frequencies (signal and idler) photons are called spontaneous parametric down conversion (SPDC) [15]. This technique provides the generation of quantum states of light. It is likely to generate entanglement in polarization via a nonlinear process. SPDC provides extensive use for quantum applications, this makes it preferable in quantum mechanics and quantum information protocols. SPDC implementations can be encountered in various experiments such as quantum teleportation, delayed choice experiments, Hong-OU-Mandel two photon interference experiments, as well as in entanglement based on quantum key distribution [16]. Quantum correlations in both position and momentum can be seen in the light emitted through the SPDC process. The momentum correlations between the photons created and demolished in the SPDC process [17]. This was a remark from 1970s early studies with the first demonstration of the existence of temporal photon correlations in the light emitted in this process. The state that is produced through the SPDC process is also a good approximation of the original Einstein-Podolsky-Rosen (EPR) state of entanglement [18]. The accessibility of EPR states makes the generation easily possible by only using a nonlinear crystal to be pumped with a laser and opened the way in front of the new types of imaging experiments. These studies can be titled under the name of quantum imaging. An overview of the quantum behavior of light detection will be given in the following parts.

Quantum correlations detection methods:

During the 1990s characterization of quantum correlations with SPDC technique was incompetent because of the avalanche photodiodes that had been used to detect single photons and a scanning pinhole to detect the spatial features of correlations. Choosing a pinhole- filtering technique leads to the loss of most of the photons and accordingly the experiment requires a long time to measure the spatial form of the correlation. Respectively physicists started to detect the spatial correlations between the photon pairs with cameras. That removed the necessity to filter them at one particular position. Instinctively there are some technical limitations including the dark count, the noise and low quantum efficiencies of available cameras. In 2000 a conventional single-frame camera was used to detect intensity correlations in the spatial spectrum of SPDC beams. The idler and the signal phases must match all over the propagation of the waves inside the nonlinear lithium triborate crystal. This phase matching assures that the waves emitted in such a state of the crystal do not interfere destructively with the upstream emissions [19]. Two fundamental types of phase matching that is placed in the context of parametric fluorescence: type 1 and type 2. Both signal and idler waves are emitted with the same polarization in type 1 phase matching. Hence, the waves propagate along two separate birefringent axes which allow under non-collinear phase matching conditions. However, in type 2 phase matching two waves that are emitted have orthogonal polarizations and propagate along two definite birefringent axes, which allows, under non-collinear phase-matching conditions, the generation of two definite beams propagating in different directions [20]. Also, as it is seen in some studies, under the right circumstances the rather bright beam intensity can exceed the noise floor of the camera and the correlated intensity fluctuations were observed in different parts of the beam. As it is mentioned previously the correlations were simply observed and spatially characterized. Other than that, it is also feasible to determine sub-shot noise behavior with such correlations and establishing their quantum nature. For a further explanation for sub-shot-noise, it can be defined as the noise on a variable that is smaller than the shot noise. The shot noise is due to the discrete and autonomous advent of photons and exhibits Poisson statistics. The detected intensities are naturally expected to follow the same temporal fluctuations. Ideally, it is expected to detect precisely the same total of emitted photons on both sides. Subtracting the two signal's intensities will cause one of them to be zero and the intensity difference of the fluctuation will tend to zero. Considering classically correlated intensities when subtracted, they cannot go below a certain limit. As it is mentioned above this limitation is called shot noise which is caused by the quantum nature of light. The shot noise limit conforms to the intensity fluctuations of the lowest-noise classical state: a coherent state which is that of an ideal laser [21].

Improved optical metrology:

New schemes have been designed that can use the quantum properties of light to achieve levels of precision beyond what can be reached intentionally, with the emergence of the concept and method of producing quantum squeezing and the number of specific photon states. In the optics context, a squeezed state can be defined as a state that offers a reduced uncertainty across one of the two field quadratures, compared to quadratures for a coherent or vacuum state (the state of an ideal laser). If the squares are limited to the Heisenberg uncertainty principle, the uncertainty on each is basically not limited.

Another class of states has reduced uncertainty to a coherent state. Those states that have a defined number of photons are also called Fock states. Compared to coherent states whose intensity is uncertain, the intensity of these states is perfectly defined. This stage of Heisenberg trade-off a Fock situation is completely uncertain. In both squeezed and Fock states, decreased uncertainty can be used to increase current measurement sensitivity. Such techniques are common in general field of quantum metrology field that aims to use quantum properties to make improved measurements. This field largely launched by desire increasing the sensitivity of gravitational wave detectors. This led to early theoretical developments measurement of quantum non-demolition measurement and the use of squeezed light in interferometric gravitational wave detectors. As a matter of imaging, a quantum application emerges in metrology precision measurement examples. By using Poisson sub-statistics opportunity to overcome light and classicism noise limit allows viewing quantum metrology schemes exposing less photons than an object classic, shot-noise-limited, measurement. Improved imaging: In addition to developing its basic limits of precision, quantum correlations make technical improvements in imaging. For example, the application of a technique called heralded imaging allows the use of quantum temporal correlations to trigger an intensified CCD camera for approximately 4 ns a signal photo probing only one object likely to hit the sensor. This heralding has the advantage of eliminating some of the sensor and environmental noise that allows only images with a few photons to be received. The same technique is expected to be applied in the context of LIDAR systems to produce quantum telemeters. LIDAR system is a system that emits light pulses and measures the time-of-flight of their echoes to assess the distance to reflecting objects. It is based on the same principle as a RADAR system but uses light instead of radio waves. The ability to overcome some of the technical noise can help such a system work with fewer photons to see without being seen. In addition, such schemes can be further developed with the temporary applications of the proposed quantum illumination protocol in the context of quantum information schemes.

Ghost imaging technique:

Using parametric transformation to produce photon pairs commonly used in ghost imaging systems may be tempting to conclude that ghost imaging is basically a quantum process. Indeed, it is well known that parametric down conversion leads to the creation of entangled photon pairs. However, the ghost imaging process only uses the spatial correlation of photon pairs, and spatial correlation is in principle a feature that can be derived from a classical source. Certainly, a scanning laser beam occurring on a beam splitter allows the object to be probed with one, while simultaneously learning about the location of the other beam scanning. Such a completely classic system can reconstruct most image attributes of the down conversion source. In the context of EPR studies, we remind that in each of the two complementary variables, correlations between both the position and the transverse momentum of the two photons should be shown. In the imaging system described above, the crystalline plane is displayed to both the object and the imaging detector based on near-perfect spatial correlations between the signal and the idler photons in the down conversion process to create an image. However, in the crystal plane, the signal and the crazy photons are anti-correlated in their transverse pulse. Consequently, in the far field of the crystal, the positions of the signal and of the crazy photons are anticorrelated. Placing both the object and the imaging detector in the far field of the crystal, therefore, results in a phantom imaging system, but in which the image is now inverted with respect to the object. This vertical or inverted image is a manifestation of EPR entanglement, depending on the system configuration, and although both results can be produced independently using scanning laser beams, no conventional system can.

Interaction-free measurement:

The previous methods included situations where photons interact with the object of interest using the photon detection time or location and its entangled partner to obtain information about the displayed object. However, it is also possible to obtain information about an object not interacting with the photon by making interaction-free measurements. The concept of interaction-free measurement was introduced in 1993. In this experiment, a Mach - Zehnder interferometer was installed, with two single-photon detectors D1 and D2 positioned for constructive and destructive interference, respectively. Therefore, any photon injected into the system must be present in D1 and not at all in the D2 detector. An excellent absorbent object placed in one of the arms will transmit a single photon from the system. If a single photon is detected in the D2 detector, there must be an object on one arm of the interferometer. However, when a single photon is detected, it may not interact with the object and be passed through an unobstructed arm. Imaging with undetected photons In addition to the ghost imaging method mentioned above -detection of the idler photon is used to herald the arrival of the twin on an imaging detector and to select a subset of the signal photons to produce an image - has been shown that the idler photon does not need to be detected. all create an image using signal photons. The physical basis of this technique was first introduced and demonstrated in the mono mode quantum context attempt. In these studies, it has been shown that a nonlinear quantum interferometer can be created using two nonlinear crystals and can induce consistency between the two signals by feeding the idler wave from the first nonlinear crystal to the second crystal (i.e., by the amplification of the idler wave). n these experiments, a laser beam is split into two beams that consistently pump a pair of nonlinear crystals paired with phase for non-degenerate down conversion. In the first crystal, the signal and idler waves emitted from the SPDC are separated and the idler wave interacts with an object. To understand this phenomenon, we can first say that the overlap of two idler waves produced in two crystals makes it impossible to distinguish which crystal an idler photon forms. This has the potential to create consistency across potentials. The bi-photon states are emitted by two crystals. It may even be without induced emission in the second crystal, which may be the result of an idler area at its entrance. When two signal waves are combined in a beam splitter, which crystal comes from the signal or idler photons and the resulting interference patterns can be detected directly at the signal side intensities. When an absorbent object is added between the two crystals in the idler beam path, some distinguishablity is added and the noise interference of the signal decreases because the consistency is partially lost. I present a detection system that uses a photon's position and time information to image an object. Since the position of the photons is correlated with their momentum, it is possible to identify the pairs by checking the photons' timestamp information and localizing one of the pairs for spatial-temporal ghost imaging thanks to the momentum conservation of the down-conversion event. While the timing information of signal (idler) is recorded as reference the idler (signal) is measured after being back-scattered from the object being imaged. With a real-time cross-correlation check of signal and idler photons, the pairs can be identified. The results exhibit multifold quantum enhancement over classical detection in an extremely noisy background. The two-dimensional imaging is performed by mapping the position of signal (idler) photons and registering the corresponding coincidence events. The rate of coincidences for a certain position is used to detect the object. The parameters affecting the image resolution in two dimensions are also analyzed. This method can be implemented on imaging of microscopic objects due to the feature that is shown; the polarization entanglement is also well preserved during the scattering from the object being imaged.

CHAPTER II

QRNG

Random numbers are used in many information and communication applications such as statistics, games, banking, and cryptography. In these applications, Pseudo-Random Number Generators (PRNG) are preferred because they generate random numbers very quickly. These generators are generally used in Monte-Carlo simulations, applications using Mersenne Twister generator [22], programming languages such as C++, JAVA, MATLAB, Python, and cryptography algorithms. It plays an important role in the generation of cryptography keys, the use of digital signatures, and similar applications [23].

Since PRNGs are based on arithmetic methods and deterministic algorithms, their security depends on the computational power of the algorithms used. Therefore, it may not meet the sufficient security level for some applications. However, True Random Number Generators (TRNGs) obtain their random numbers from totally classical physical processes, which are unpredictable for all practical reasons. This unpredictability can be caused by many uncontrollable reflections on systems with chaotic behavior.True random numbers can be generated from physical process in the nature. An example for the use of natural random sources can be given as radioactive decay time, atmospheric noise, noise generated in electrical circuits, and so on. Hardware can be used as a noise source. They can be also reproduced from the thermal noise of an electronic circuitry , of free-running oscillators and measurement of the phase noise of a laser.Noise-based TRNGs in electronic circuits are very cheap and small [24, 25]. The downside of this situation is that the quality of random numbers produced by TRNG is open to discussion and it is difficult to assess. Building a good

TRNG is a big challenge and it is practically impossible to certify it. For this reason, TRNGs often involve complex post-processing of random numbers that make them similar to PRNGs.However, they are inefficient to distinguish true randomness from classical noise caused by the measurement devices. These methods are all lack of complexity to create high quality randomness.Those process are all based on classical effects and by the laws of classical mechanics they are still treated deterministically and not truly random [26]. In additiontı that, attacks on TRNG are known. Quantum Random Number Generators (QRNG) can also be evaluated in this class. QRNGs use the inherent uncertainties provided by quantum mechanics.

Vacuum Fluctuations [1], single-photon detection [27], and spontaneous emission noise [28] are some of the events mentioned in the literature and used as sources of random entropy in CRSs. Shot noise-based QRNGs use the Vacuum Fluctuations event, which is both a fast and unpredictable source of randomness. Tunneling or scattering effects can also be used as a fast and reliable source of entropy. In Figure 1 some optical methods on QRNG can be seen in the table. This experiment presents a quantum random number generator that uses vacuum fluctuations of light as a source of randomness. Photon statistics and entropy estimation methods are used in analog data processing and randomness analysis. The photon is prepared in a 45-degree polarization and sent to the polarized beam splitter and has a 50% chance of being transmitted or reflected at 45-degrees. A single-photon detector is used on both sides for photon counting. Since Reflection/Scattering is a quantum process, bits 0 or 1 are obtained from each individual transmission. The internal resistance of electronic devices, bandgap of detectors, flicker noise and oscilloscope margin of error, etc. factors can be counted among the limiting factors of this experiment.

Type (Sec.)	Physical principle	Representative Examples	Rate (order)	Challenges
Branching path	Path superposition + measurement	Jennewein *et al.* (2000)	Mbps	Unbalanced detector Detector dead time
Time of arrival	Time of arrival statistics	Stipčević and Rogina (2007), Wayne *et al.* (2009), and Wahl *et al.*(2011)	Mbps	Time precision Detector dead time
Photon counting	Photon number statistics	Fürst *et al.* (2010) and Ren *et al.* (2011)	Mbps	Photon resolving capability Detector dead time
Attenuated pulse	Binary measurement of coherent states	Wei and Guo (2009)	Mbps	Source insatiability Detector dead time
Vacuum fluctuations	Shot-noise measurement	Gabriel *et al.* (2010), Qi *et al.* (2010), and Lam (2011)	Mbps-Gbps	Classical noise Postprocessing
Phase Noise	Laser phase noise	Guo *et al.* (2010), Qi *et al.* (2010), and Jofre *et al.* *(2011)*	Mbps Gbps	Phase drift Pulse repetition rate
Amplified spontaneous emission	Amplitude fluctuations in ASE noise	Williams *et al.* (2010) and Argyris *et al.* (2012)	Gbps	Sampling or digitation Postprocessing
Raman Scattering	Interaction with phonon fluctuations	Bastard *et al.* (2011) and Collins *et al.* (2015)	kbps-Mbps	Raman Gain (stimulated) Detector dead time (spontaneous).
Optical parametric oscillators	Bistability in optical parametric oscillators	Marandi *et al.* (2011) and Marandi, Leindeckeri Vofopyanov, and Byer (2012)	kbps	Cavity decay time Pump repetition rate.

Figure 1: This table gives the summary of the optical methods for quantum random number generation. The table gives the section where we describe the details of each implementation, the principle of operation, a few representative examples, the order of magnitude of the typical bit rates of each generator, and a list of the most important limitations [1].

Two of the methods for QRNG are more preferred than others. In the following section this mentioned vacuum fluctuation based homodyne detection configuration will be introduced in details.

2.1 Balanced Homodyne Detection Scheme

Figure 2 schematically shows our quantum random number generator. In this experiment, it has tens of kilometers of coherence and ultra-high frequency stability; the central wavelength is 1550 nm and the linewidth is 100 Hz. Koheras BASIK E15 model single-frequency fiber laser source was used. This local oscillator is sent to one port of the 50:50 beam splitter (BS), while the other is physically blocked and acts as a vacuum input. The experimental setup can be seen in Figure 34in photos section. The outputs are then optically coupled to a bi-balanced photodetector with 30 dB common-mode rejection. The power of the output ports is recorded with a 1.6 GHz bandwidth, fiber-coupled balanced amplifier (Thorlabs PDB480C-AC, InGaAs). The coherent laser is emitted by BS and splits into two paths. Each detector PD1 and PD2 detects optical input signals by subtracting the two optical input signals, eliminating the effect of common-mode noise. This type of setup is also known as a balanced homodyne detector. Homodyne type setup is very useful for getting rid of classical noise and observing shot noise as dominant. All these features of the components in the assembly and the balanced homodyne system help to reduce the limitations caused by the devices and increase the randomness quality of the vacuum fluctuations.

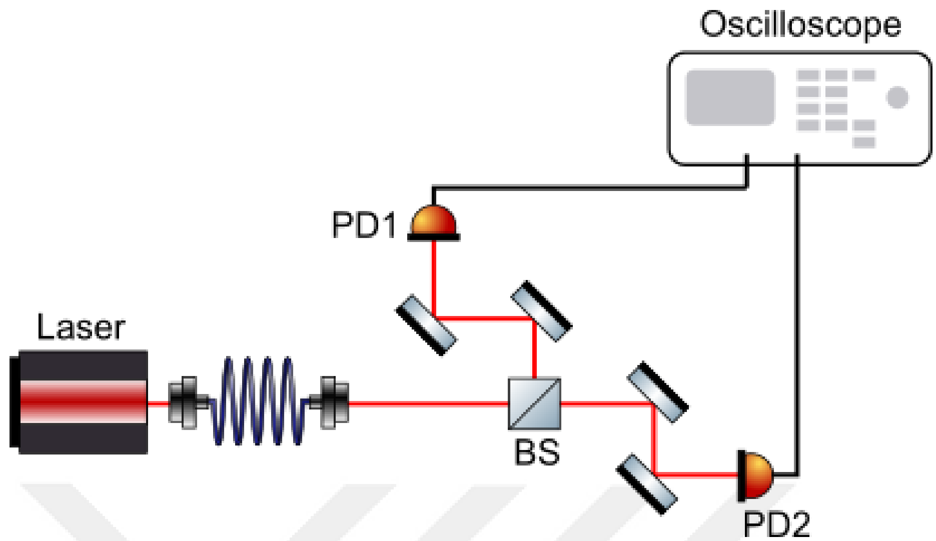

Figure 2: Quantum random number generator schematic. The polarized beam splitter scatters the laser beam with a central wavelength of 1550 nm and converts it into photocurrent (I_1, I_2) on photon detectors (PD1, PD2). The differences of the currents I_1 and I_2 are amplified and sampled and displayed by the oscilloscope.

Light sources are classified according to the variance of their photon distributions. This classification is made under three main headings; Poissonian, sub-Poissonian, and super Poissonian. Super-Poissonian can be chaotic, incoherent, or caused by thermal light. A Poisson distribution is caused by perfectly coherent light and a Poisson sub-distribution is caused by a non-classical light source. Although they all have the same mean value, the distributions of the super Poissonian and sub-Poissonian appear wider and narrower than the Poissonian, respectively;

- Sub-Poissonian statistics: $\Delta n < \sqrt{n}$
- Poissonian statistics: $\Delta n = \sqrt{n}$
- Super-Poissonian statistics: $\Delta n > \sqrt{n}$

In other words, if the mean and variance are equal, we will have a Poisson distribution, if the mean of the distribution is greater than its variance, then we will have a super

Poisson distribution pointing to higher entropy. Here below in Figure 3) you can see the vacuum field emphasis on a balanced homodyne detection scheme. After the photodetection of the two detectors output signal is subtracted from each other to obtain the quantum dominance under the presence of vacuum state field.

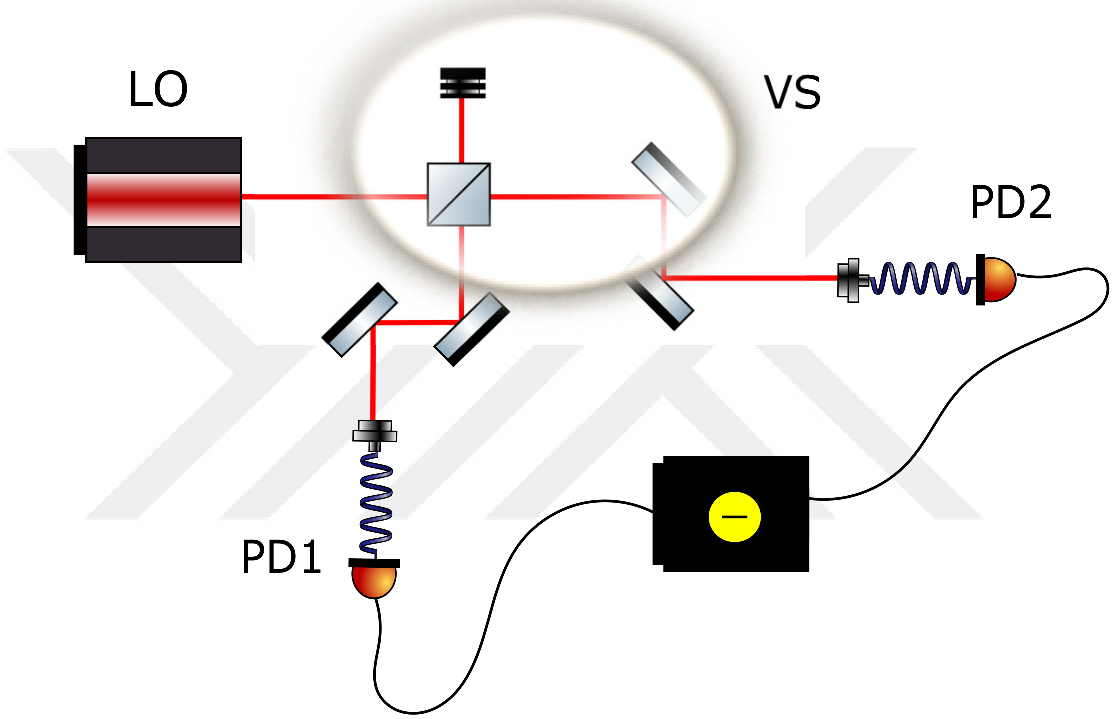

Figure 3: Schematic diagram of vacuum fluctuation based balanced homodyne detection setup. LO is local oscillator, VS represents the vacuum state field in the environment, PD1 and PD2 are the identical bucket detectors.

In the following section, QRNG design with optical scattering feature is proposed. A pseudo-thermal effect is presented in order to have a super-Poissonian statistics of photon distribution.

2.2 Pseudo-thermal Homodyne Detection Scheme

In this experiment, we made a different configuration on the classical balanced homodyne detection scheme to observe the pseudo-thermal effect on randomness. As we previously explained the photon statistics of a coherent light source is Poissonian. The random nature of this coherent light source is aimed to be enhanced by using the scattering phenomenon. Different materials in the optical setup such as a semi-polished silver mirror are preferred to improve the chaotic (thermal) characteristics of the light and broaden the distribution. The experimental setup (see Figure 4) and the details of the study are as follows:

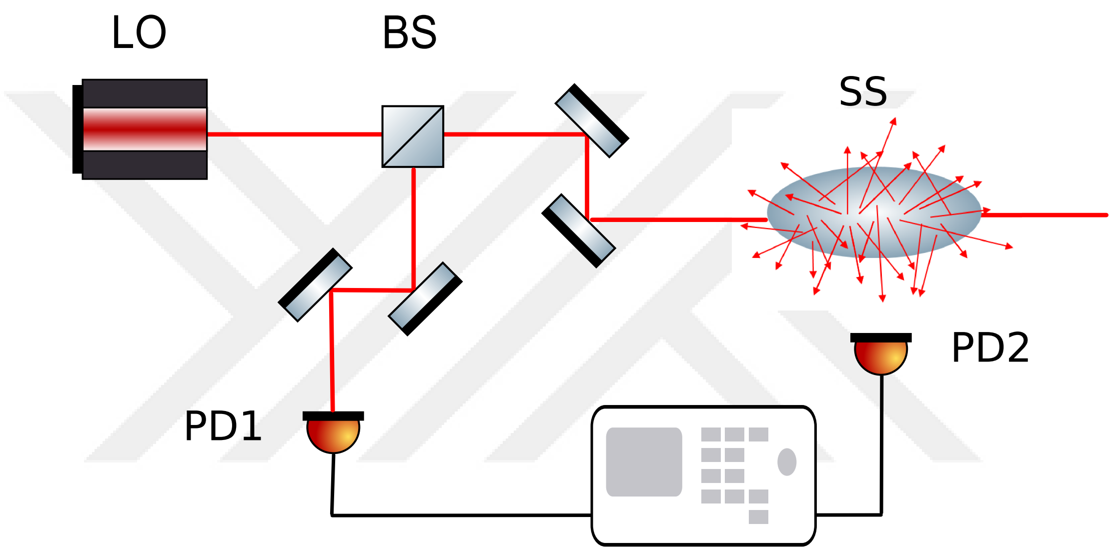

Figure 4: Schematic diagram of scattering-based QRNG. Laser diode (LD), Beam Sampler (BS), 5 mm diameter silver oval surface is used as scattering source (SS). Photodetectors (PD) are used to compare scattering with direct laser beams.

Balanced homodyne detection is not preferred for this experiment. For this experiment coherent laser source with the central wavelength of 1550 nm and linewidth of 100 Hz is used. The light is split into two channels by a beam sampler. Direct laser and scattered light are simultaneously detected by two separate photodetectors with a bandwidth of 5GHz. While one channel is set as a direct laser, to the other channel a scattering object such as half polished silver and unpolished aluminum is placed. Aluminum foil and standard white paper pieces were used for scattering. The optical inputs detected by the photodetector are compared. Aluminum was found to be successful in the analysis.

Figure 5: The 5x magnified image of the silver coated material used in the experiment. Scattering centers due to the roughness of the surface serves as multiple pseudo light sources.

The locket in Figure 5 has rough and a bumpy surface which enhances the scattering process. More explanation about the randomness effect of different materials is below:

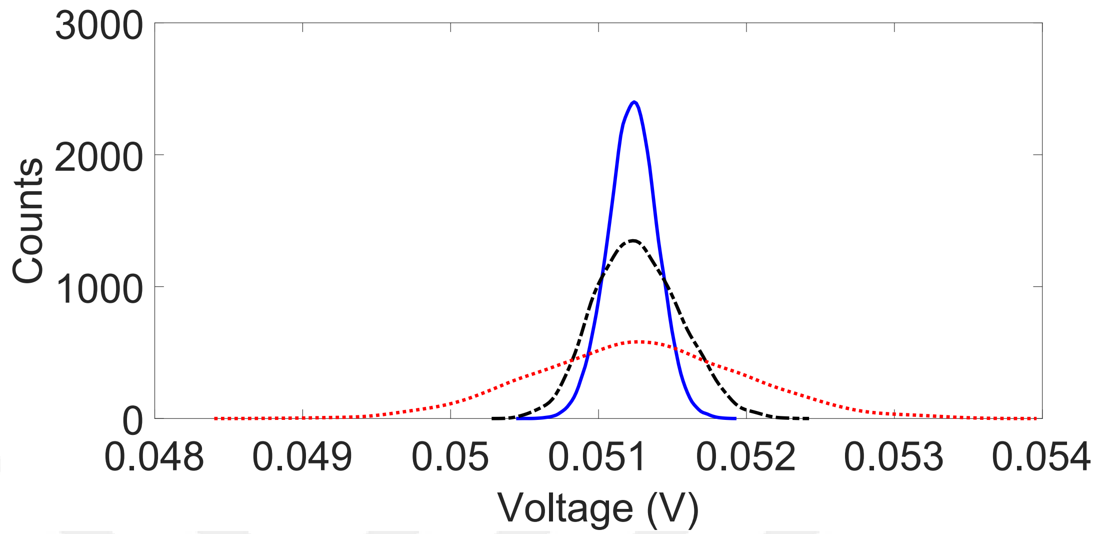

Figure 6: Counts versus voltage plotting of different materials' Poisson distributions where the data shows direct laser (blue), laser scattered of half polished silver (black), and laser scattered of unpolished aluminum (red).

The intensity function of the laser distribution shows a Poisson distribution as expected. Depending on the source being a coherent laser, a voltage value of 0.40 mV is measured at full width half maximum (FWHM). Laser scattering from a semi-polished silver surface has a Super Poisson dispersion at 0.67 mV FWHM while scattering from an unpolished Aluminum surface has a Super Poisson dispersion at 1.67 mV FWHM. Although different scattering sources have different scattering parameters, they all result in a wide distribution of photon statistics. Figure 6 helps us compare the distributions of optical inputs of light scattered from a coherent laser, semi-gloss silver, and unpolished aluminum surfaces.

The direct optical input from the laser in the setup shows the Poisson distribution. Laser scattering from a semi-gloss silver mirror increases the chaotic (thermal) properties of light due to the random nature of the scattering and widens the photon statistics distribution. Unpolished aluminum has a higher density and frequency of scattering centers, due to the roughness of the surface being proportional to scattering. This leads to a wider distribution and a more even probability of photon statistic, in other words, better randomness. As a result, it can be said that chaotic behaviors become more dominant with increasing scattering centers.

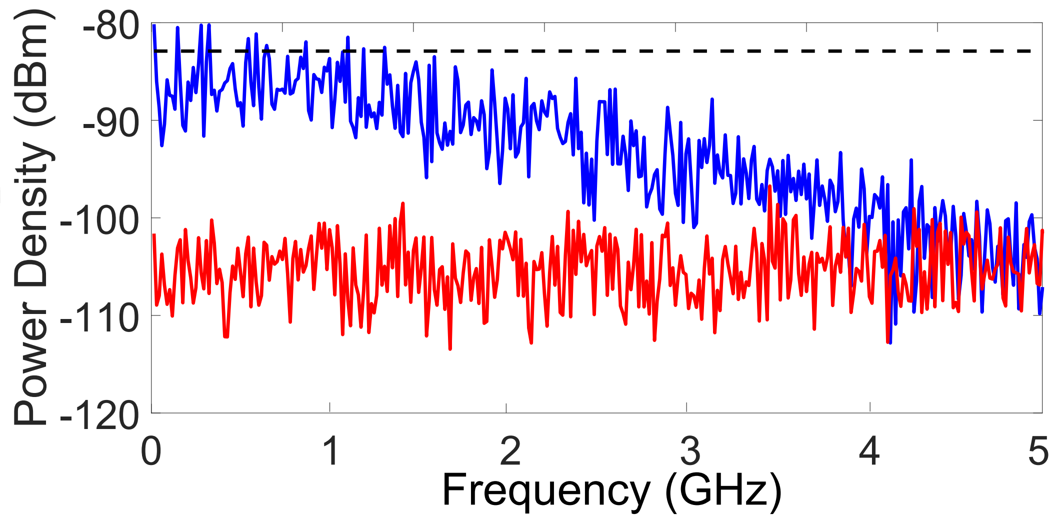

Figure 7: Power spectral density of the laser light from the homodyne detector (blue) alongside the electronic noise (red). The black dotted line shows the theoretically calculated shot noise to be -70.73 dBm.

The power spectral density of the signal is measured to ensure that the quantum fluctuations dominate the electrical noise as seen in Figure 7. Shot noise level can be calculated using the following equation:

$$P_{quantum} = 2eR_L i\Delta f \tag{2.2.1}$$

In Equation 2.2.1, e corresponds to the charge modulus of the electron, R_L is the charge resistance, i is the photocurrent, and Δf is the bandwidth frequency. For a 1 mW set of sample power values, the theoretical shot noise is calculated to be -69.2 dBm.

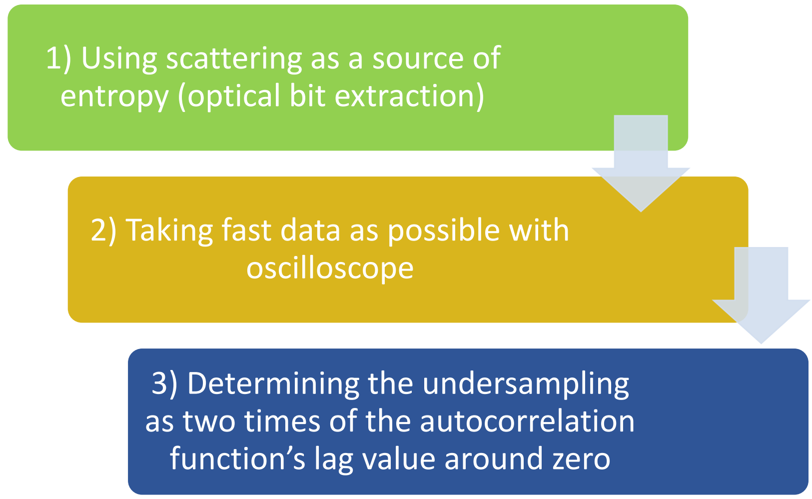

Figure 8: Flowchart of the QRNG randomness enhancement process.

We mention some requirements for obtaining random sequences. First, these sequences must be non-deterministic. PRNGs are not sufficient in applications because they originate from deterministic computer algorithms. Also, a physical source of entropy cannot be considered deterministic. Quantum entropy sources are not deterministic in terms of spontaneous randomness, and random number generators based on vacuum fluctuations are preferred. The second requirement for obtaining randomness is that the entropy source must be essentially uncontrollable by the third party. Even if the intervention of a third party cannot be completely excluded, its impact with the use of post-processing can be taken into account. The unpredictability of the physical process used in QRNG provides a great advantage. The randomness inherent in quantum mechanics makes quantum systems an excellent source of entropy. In this sense, random number generators are devices that use quantum mechanical effects to generate random numbers and have many applications from simulation to cryptography. Thanks to these designs, the vacuum state, which is the source of its randomness, can be easily prepared with high accuracy. By increasing the local oscillator power, the performance of QRNG can be made insensitive to detector loss. Also, the area squared of the vacuum is a continuous variable and multiple random bits can be generated from a measurement [1].

Autocorrelation Function:

Autocorrelation is a correlation coefficient. However, instead of examining the correlation between two different variables, the relationship between two values of the same variable at times X_i and X_{i+k} is examined. Autocorrelation can give us a clear idea of randomness. The autocorrelation function compares each bit with a delayed copy of the signal itself as a delay function. The lowest autocorrelation delay value is also the value with the lowest correlation between bits, which shows the best randomness. When the autocorrelation function value is ideally equal to 0, we can talk about zero correlation, i.e. 100% randomness. The autocorrelation function of the scattering signal approaches zero earlier than the coherent laser signal. The optimum sampling rate is obtained when the autocorrelation function of the scattered signal is set to twice the minimum delay point. Thus, the raw signal is optically processed much faster before it is digitally processed to ensure an even distribution of bits. If the time series function is modeled in an autocorrelation graph, usually all lag values can be observed here. If we are going to use the autocorrelation graph as an indicator of randomness, the first delay value is usually taken into account. The vertical axis of an autocorrelation plot shows the value of the autocorrelation function at an amplitude in the range of –1 to 1. The horizontal axis of an autocorrelation graph shows the size of the lag between elements of the time series. The autocorrelation function with a lag value of 3 shows the correlation between the time series elements at an instant time and the elements corresponding to the three previous times. The graph has a vertical line (”spike”) corresponding to each lag. The height of each spike indicates the value of the autocorrelation function corresponding to that lag. Zero-latency autocorrelation always equals 1 because it represents the autocorrelation between each term and itself. A zero-lag electric current and instantaneous electric current are the same variables. If we imagine an asymptotic limit at the zero level, every increase above or below this limit is considered statistically significant. This means that spikes have a significantly different value from zero. If a spike is significantly different from zero, this is evidence of autocorrelation. An increase close to zero is evidence against autocorrelation, which is interpreted as an indicator of randomness. According to the NIST protocol, where randomness analyzes are performed, the autocorrelation function is used to answer the following questions: 1. Was this sample data set generated as a result of a random process? 2. Is a nonlinear model or a time-dependent series model better suited to scientific notation (Y = constant + error)? We can explain the importance of autocorrelation as follows; Randomness is a key assumption in determining whether a univariate statistical process is in control. If the fixed position and scale assumptions are correct, plus randomness and fixed distribution are significant, we can express the univariate process as follows:

$$Y_i = A_o + E_i \tag{2.2.2}$$

Here E_i denotes the error term and A_o denotes the autocorrelation term. If the randomness assumption is not valid, a different model must be used. This in turn can typically speciate as a time series model or a nonlinear model where time is the independent variable. The randomness assumption is very important for the following reasons: 1. Most standard statistical tests rely on randomness. The effectiveness of the test results is directly related to the effectiveness of the randomness assumption. 2. Many commonly used statistical formulas rely on the assumption of randomness; The most common formula is the formula for determining the standard deviation of the example: $s_Y = s/\sqrt{N}$. Here is the standard deviation of the data. Despite its extensive use, the results obtained using this formula are of no value unless the assumption of randomness is valid. 3. Default model for univariate data $Y = constant + error$. If the data is not random, this model is inaccurate and invalid, and estimates of parameters (such as constants) become meaningless and invalid.

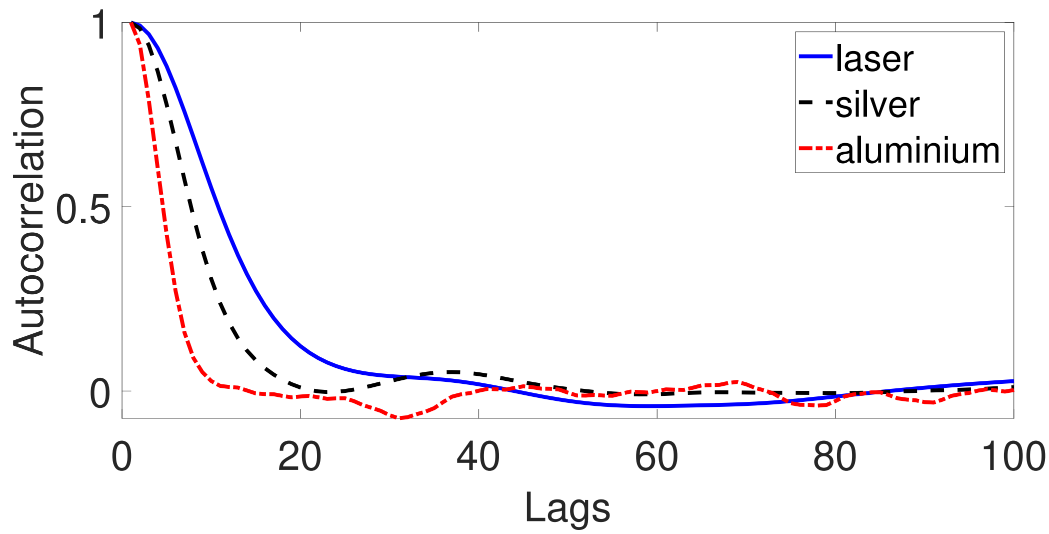

Figure 9: Comparison of autocorrelation functions of analog signals obtained as a result of directly measured laser (blue) scattering from semi-bright silver surface (black), scattering from unpolished aluminum object (red).

The autocorrelation plot is a reliable way to check the randomness quality. Different scattering objects and different conditions in optical measurement (see Figure 9) has different autocorrelation, hence different contributions to post-processing. The photon statistics of a coherent light source is Poissonian. Scattering of coherent light by scattering centers makes the dispersion have greater variance. As a result, the photon statistics distribution becomes super Poissonian, where fluctuations in the measured optical density have a wider distribution even at the same mean value. . Unpolished aluminum gave a result of higher intensity in the matter of having more scattering centers. Additionally, the roughness of the surface is proportional to the scattering. Therefore, the distribution turns into a super-Poissonian where the fluctuations in the measured optical intensity have a broader distribution. This shows that the chaotic behavior becomes more dominant with the increased number of scattering centers. The autocorrelation function supported our results as mentioned previously. The autocorrelation of the detected raw signals of the coherent local oscillator for direct light and scattered light shows different delay values for minimum (ideally zero) values. It is obtained as a result of the experiment that the minimum autocorrelation function for the Super Poissonian distribution is realized at a lower lag value. This method provides a faster sampling rate without sacrificing randomness quality.

2.3 Experiment of Optical Chopper Effect on Randomness

The main sources of noise in a photodiode can be categorized as thermal noise, shot noise, and dark current noise. Due to the random nature of noises, the best way to identify them is to use their statistical values such as spectral density, power, and bandwidth. In almost all the optical devices that require the measurement of light intensity, we use detectors that generate a signal (usually a current) directly proportional to the light intensity. However, by their very nature, detectors do pass some current when in total darkness, and we have to distinguish between the signal originating from the ”dark current” and the signal derives from the ”dark current + laser current”. Dark current noise is the constant current that exists when no light hits the photodiode. Another problem that arises, if we try to measure very accurately the small light current or very large light current in both situations there will be small random variations of dark current influence in the whole detection process. This limits the sensitivity of a detector. The distinction between “dark and dark plus laser” signals can be achieved when light falls on the detector and when it does not, i.e. by taking the difference of the signals using an optical chopper. Therefore, the laser is interrupted at a constant frequency and the signal is detected by AC circuits that do not react to the continuous dark current. This technique is called beam cutting. To assess Shot noise levels, also called quantum noise, a motorized optical chopper can be used that periodically cuts off the power of the pump beams. Random noise is a mixture of multiple signals, all of the different frequencies. A significant reduction in noise can be achieved if a chopper is used and operates at a fixed frequency. At this point, it is important to fix the speed of the chopper mechanically.

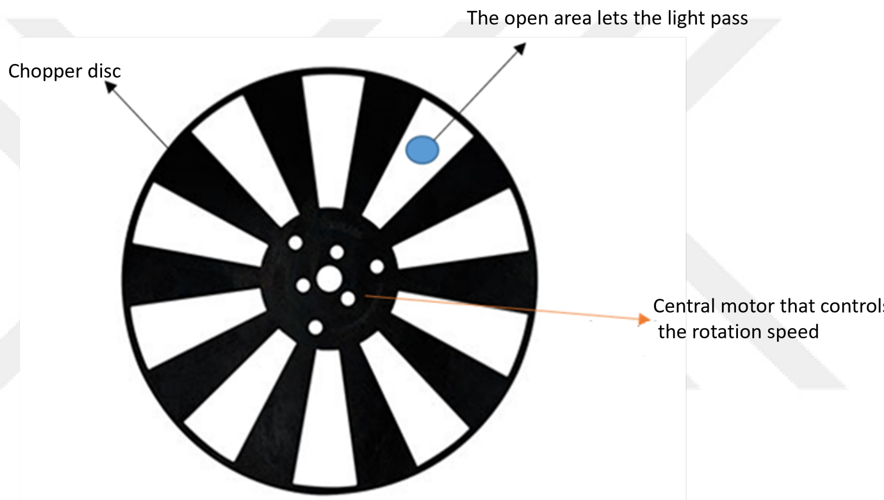

Figure 10: The schematic of the chopper disc which is introduced to the balanced homodyne setup to test randomness in different rotational speeds.

By simulating the light pulses to the shape and phase of the gate pulses, a very effective improvement in the signal-to-noise ratio can be achieved. Before investigating how this ratio changes, preliminary research has been made about whether the data obtained by using the chopper has an effect on the randomness for our QRNG system, which is based on vacuum fluctuations and uses a single detector that takes the difference of the beam coming into the two channels to minimize electronic noise. For this purpose, measurements and calculations such as autocorrelation, variance, min-entropy, which should be examined together, were evaluated in order to define the randomness of the obtained signal. Obviously, especially since the probability distribution of a random signal is highly dependent on the optical scheme and there is no single rule for removing quantum noise from the output of the optical QRNG, as we mentioned earlier, the detector receiving the difference in the two arms coming out of the beam splitter is additional to the detector. chopper use was investigated. Apart from that, we know that quantum noise is inversely proportional to the output laser power (P). Taking into account the dependence of the voltage variation of the photodetector on P, an optimal output laser power can be evaluated (we can also think of it as a kind of threshold) where the value of the quantum-classical noise ratio corresponds to the highest value. This value is then used to estimate the quantum min-entropy of the random signal required for subsequent hashing [27, 28]. For this purpose, in order to evaluate whether the maximum power of the low-noise KOHESIK BASIK laser we used in the measurements is optimal, power-dependent measurements were taken and its effect on randomness was also examined.

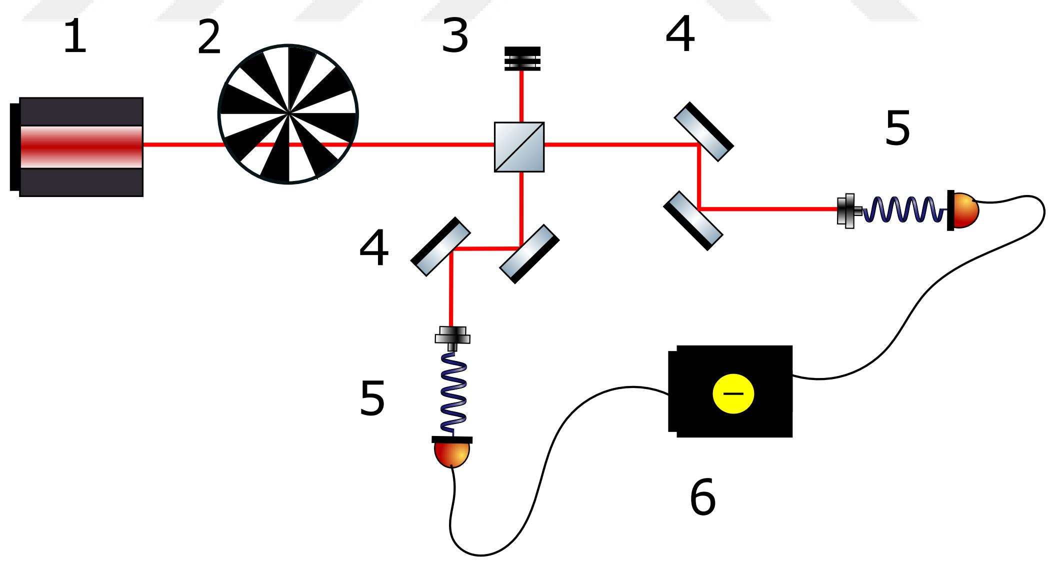

Figure 11: Schematic of the experimental setup.

The setup in Figure 11 was used to examine the effect of the optical chopper and laser output power on autocorrelation values. Numbered elements mean: 1: 1550 nm central wavelength laser source, (Koheras Basic low-noise OEM laser, Model E15)

2: Optical chopper with 10 slits, rotation frequency in the range of 20-1000 Hz, 3: Beam splitter cube with 50% transmittance and 50% reflectivity, 4: mirrors, 5: fiber coupling configuration, 6: Photodetector with fiber input, where the signal in two channels are separately detected and subtracted from each other. In order to express the operation of the optical chopper more clearly, a sample data that appears on the oscilloscope screen when the two ends coming from the beam splitter are connected to two separate but identical detectors and placed in front of the source is shown in Figure 12.

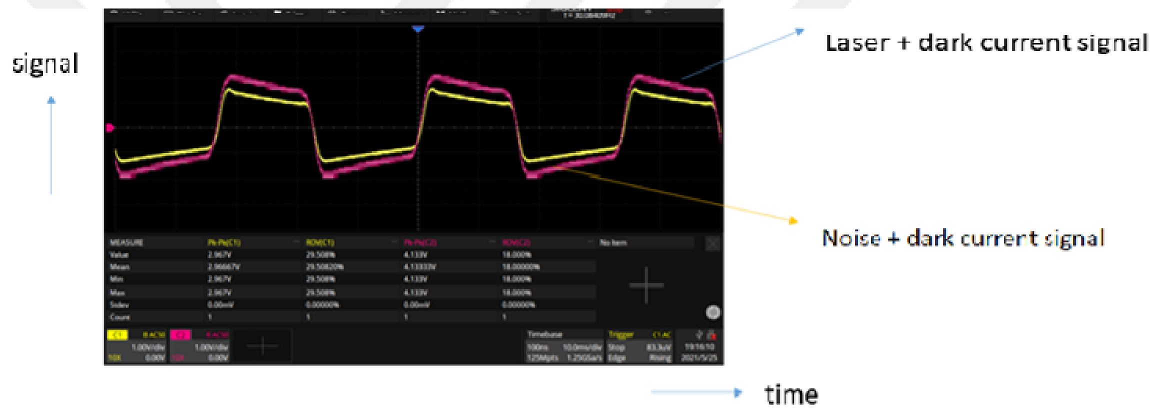

Figure 12: The chopped signal sample from the oscilloscope.

An optical chopper was placed in front of the laser source as in **??**, and the measurements were taken by operating it with a frequency of 300 Hz. When the signals obtained in this way and the signals obtained without using a chopper are compared in Figure 13, it has been determined that the signals obtained without using a chopper have better autocorrelation.

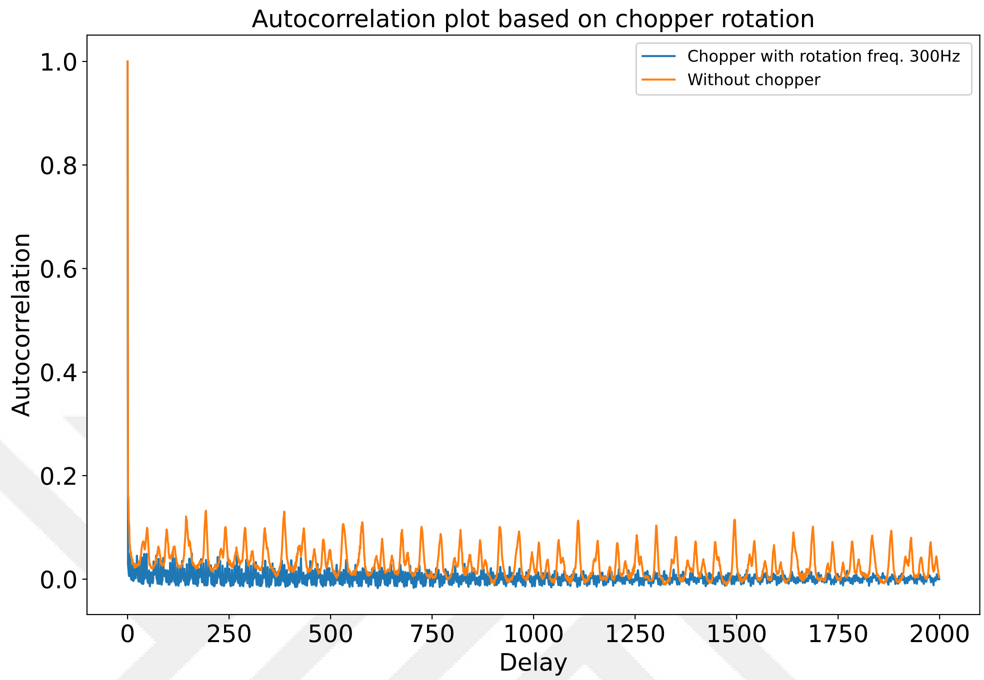

Figure 13: Autocorrelation results at 40 mW laser output power at 300 Hz frequency of rotation compared with the absence of optical chopper.

Although this result alone does not give a definite conclusion about the quality of randomness, it has revealed that it can have a significant effect on randomness. When the results were examined and the min-entropy values were calculated, the min-entropy was calculated as 0.9957 in the case of using the optical chopper and as 0.9907 in the case of not using it. While the variance and mean values were 0.6807 and 0.0006, respectively, in the case of using the optical chopper, it was calculated as 0.6654 and 0.0005 in the case of not using it.

In Figure 14, we see the autocorrelation results for the study on whether the laser output power is optimal or not.

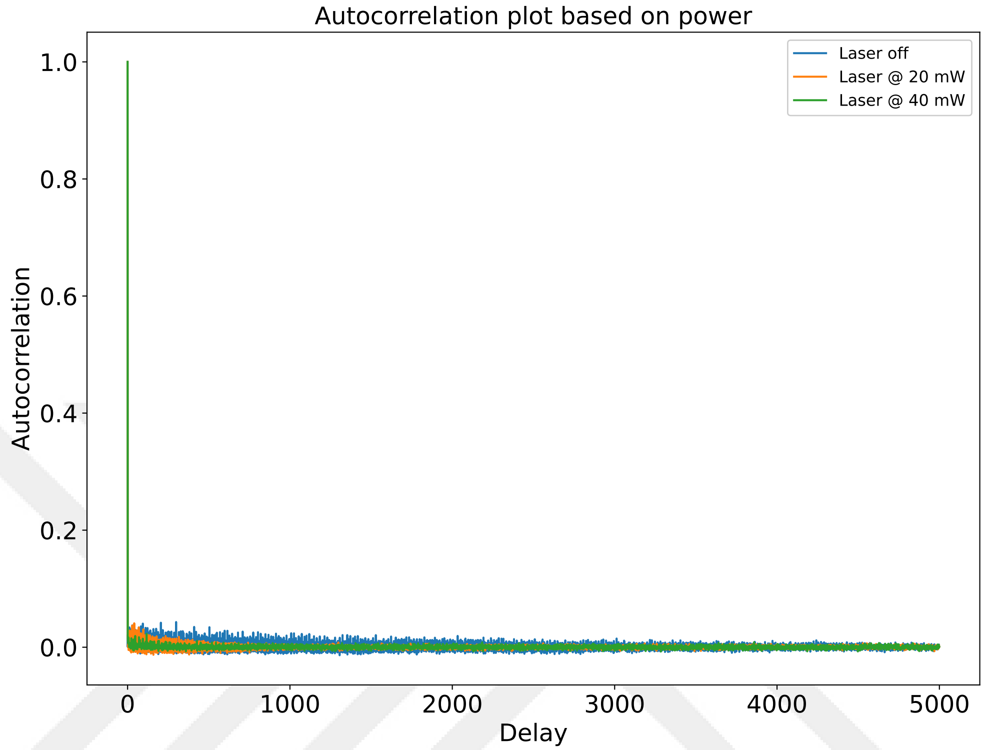

Figure 14: Autocorrelation results for optimal laser output power determination.

As a result of the measurements taken between 40 mW and 12 mW, it was determined that the autocorrelation result obtained when the laser output power was 40 mW was quite good compared to lower powers. In fact, according to the autocorrelation results of the measurements taken up to the maximum power of 40 mW, it was seen that the results below 20 mW were very similar to the measurement taken when the laser was turned off. According to the results of measurements above 20 mW, it was seen that the ideal power value was 40 mW. However, it may not be correct to reach a definite conclusion only by looking at the autocorrelation result. The min-entropy value of the noise obtained when the laser is turned off was calculated as 0.9901, at 20 mW power as 0.9901, at 40 mW power as 0.9907, and the variance values were found to be 0.6641, 0.6640, and 0.6654 under the same conditions, respectively. The mean values were again determined as 0.0006, 0.0006, and 0.0005, respectively.

Shot Noise Calculations:

Hypothetical "Shot Noise" calculations are calculated according to the following formula:

$$P_Q = 2e\langle I\rangle \Delta f R_L \tag{2.3.1}$$

In this formula, e is the electron charge, $\langle I\rangle$ is the average photon current, Δf is the detector bandwidth, and R_L is the load resistance. As we mentioned previously (see Figure 14) shot noise is an important indicator to show quantum dominance in the experiment [29]. Shot noise is obtained when the following experimental conditions are established

1. When the laser source is at 40mW and the optical chopper is not used: $P_Q = 1.4875889574224 \times 10^{-11}$

2. With the laser source at 40mW and the optical chopper rotating with a frequency of 400Hz: $P_Q = 1.5029698530704 \times 10^{-11}$

3. When the laser source is turned off and the optical chopper is not used: $P_Q = 1.5468054056672 \times 10^{-11}$

The bigger value of shot noise on the logarithmic scale implies better quantum behavior in the process.

In this experiment, measurements were made on the effect of the optical chopper on the randomness and noise in the system. According to this hypothesis, a disk-shaped chopper was placed between the laser source and the beam splitter, rotating at a certain frequency, completely blocking or partially allowing the passage of photons. In this way, it was aimed to investigate the minimization of noise and its effect on randomness. As a first step, the voltage outputs from the photocurrent detector for each measurement were converted to bits with a threshold determined by an average value. Autocorrelation values of these data were calculated and plotted. According to this evaluation, when looking at the fastest falling to zero feature in terms of randomness, contrary to the assumption, using a chopper did not increase randomness, but increased regularity. By repeating the measurements, both the distribution and randomness of the bits were calculated with another test, ”Shannon Entropy”, according to the results of these measurements, the hypothetical ones once again got the worst value. As a final test, photon statistics were examined by comparing the variance and mean of the measured values in terms of current. According to this comparison, it was observed that the values in which the variance was less than the mean showed a sub-Poissonian distribution. When calculated separately for each data, it was clearly seen that the variance values for all data were less than the mean values. However, since the measurements are not made at the single-photon level and there is no anti-bunching situation, this result cannot be evaluated as correct. As a result of the measurements made with this optical chopper, the hypothesis was found weak in all aspects and was falsified.

CHAPTER III

PHOTON DETECTION EFFICIENCY

3.1 Non-linearity and Phase-matching

The experiments presented in this thesis rely on strong transverse spatial correlations between two photons. These correlations are inherent in the entangled photon pairs generated through the spontaneous parametric down-conversion (SPDC) process. The term parametric in SPDC implies crystal remaining same after the down-conversion process. SPDC process is about higher energy waves'/photons' giving birth to lower energy waves/photons.

The phase-matching condition is the one critical phenomenon we need to provide to proceed with the spontaneous parametric down-conversion. For that two main physical conditions must be sustained: momentum and energy conservation.

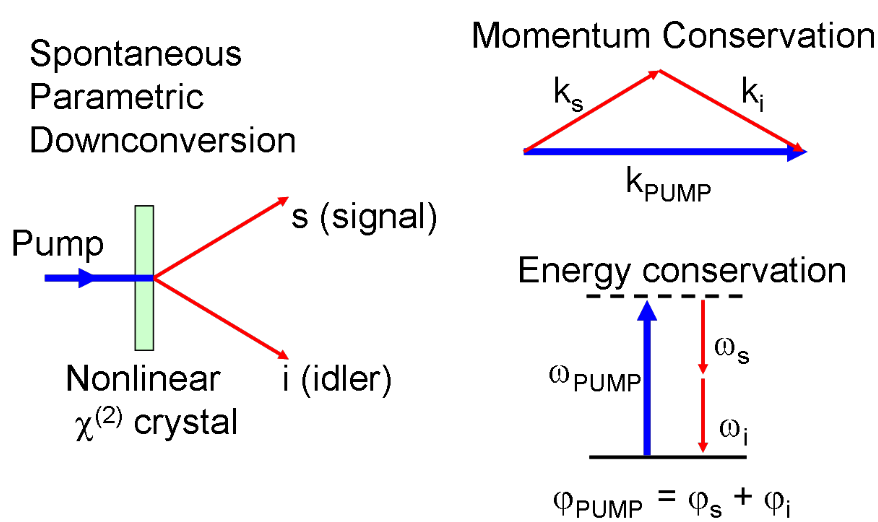

Figure 15: The diagram of the phase-matching conditions for SPDC process [2].

The SPDC process to must obey the momentum and energy conservation equations:

$$k_p = k_i + k_s \tag{3.1.1}$$

$$\omega_p = \omega_i + \omega_s \tag{3.1.2}$$

where $k_p, (i, s)$ and $\omega_p, (i, s)$ are the wave vectors and angular frequency of the pump and signal and idler photons respectively. The first equation is defining momentum conservation while the second equation defines energy conservation.

Practically it is very hard to fulfill the phase-matching conditions mentioned in Equation 3.1.1 and Equation 3.1.2. The wave vectors in the interacting field of the idle and the signal produced in the SPDC process have the same direction. This is the reason for the collinear geometry of SPDC. That geometry can be read as a perfect phase-matching condition.

Notably, anomalous dispersive dielectric materials can satisfy the phase-matching condition. Their intrinsic function is suitable However, this method is not preferable in experiments due to its high energy absorption feature. Uniaxial crystals' property is only one direction governing optical anisotropy, all directions perpendicular to it are optically equivalent. Biaxial crystals have two optical axes. For positive uniaxial crystals one optical axis), $n_e \geq n_o$ and for negative uniaxial crystals one optical axis $n_e \leq n_o$.

Alternatively, usage of birefringent anisotropic crystals in applications is highly preferable for providing perfect phase-matching. **Birefringence** is a phenomenon of optical anisotropy in transparent materials. The index of refraction depends on the polarization direction considering the direction is in the electric field. **Nonlinear crystals** are also birefringent, meaning that the index of refraction depends on the polarization direction of the light with respect to the crystal axes. As a nonlinear with biaxial crystal type, beta barium borate ($\beta - B_aB_2O_4 = BBO$) has two optic axes along the light's propagation direction. By the nature of the birefringent phase-matching, all the light modes of the signal and idler fields have the same polarization without the difference of being **ordinary** or **extraordinary**. The spectra of the two generated fields are always the same in CW-pumped SPDC.

Randomly polarized beams are divided into two orthogonally polarized beams in the birefringent crystals. We name those two rays as ordinary and extraordinary with the refractive indices of n_o and n_e, respectively. The quantity of the difference between those two refractive indices ($\Delta n = n_e - n_o$) is evaluated by birefringence.

In the following sections, I will mention the phase-sensitive and phase-insensitive cases, so a brief explanation here will be informative for the reader. **Phase insensitivity** means the signal and the idler are in different phases because of their non-degenerate behavior. In the phase-sensitive case signal and idler photon pairs are identical because they are born at the same time.

The angle between the optic axes determines the annealed photon's energy levels or in other terms their speed in the walk-off process. For other wave propagation directions, there are two plane-polarized components at right angles to each other and corresponding to the propagation direction. These components' speeds are unequal to each other. Light passes through an axis with the smallest refractive index and higher phase velocity, and this axis is called the fast axis. Correspondingly, the axis with the highest refractive index is called the slow axis. The phase velocity of light is lowest along this axis. Depending on the crystal ingredient the optical axis can be the fast or slow axis for the crystal.

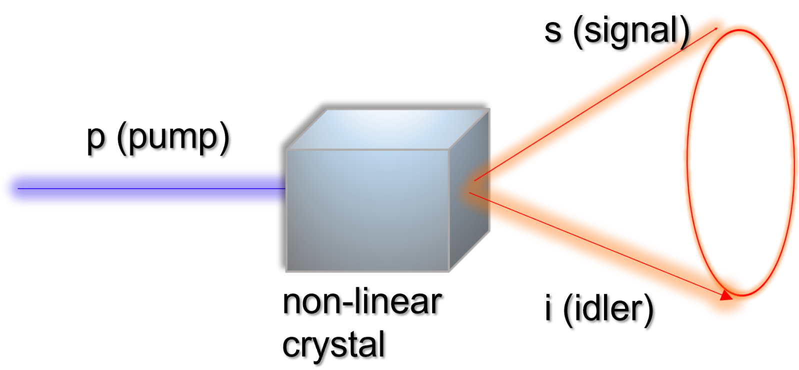

Figure 16: An SPDC scheme with the non-collinear geometry of Type 1 output.

Because nonlinear crystals have birefringence property we can preserve the equilibrium between the birefringence and the dispersion ratio. This will allow us to achieve two different types of phase-matching. With **type 1** phase-matching both signal and idler waves are emitted with the same polarization. Hence, the waves propagate along two separate birefringent axes which allow under collinear phase-matching conditions. The pair positioning after the annealing process can be seen in Figure 16.

However, in **type 2** phase-matching two waves that are emitted have orthogonal polarizations and propagate along two definite birefringent axes, that allows, under non-collinear phase-matching conditions, the generation of two definite beams propagating in different directions.

Even the most highly coherent laser sources are initially composed of discrete photons. Especially if one is working in a low-level laser power regime, the fluctuations in absolute intensity will be highly affected. These fluctuations in the intensity of the local oscillator limit the imaging resolution. Therefore, the need to go below the shot noise level has occurred. As explained in the previous parts shot noise limit is the fundamental noise floor limiting all classical light sources. This term is introduced as **sub-shot noise** into the literature. This can be obtained by producing already intensity correlated photon pairs [30]. There are two approaches for that:

1. Generation of photon pairs in nonlinear crystals. In other words, correlated photon-counting detection.

2. High brightness intensity correlated beam generation in optical fiber.

We will be over the first method in this thesis. The difference of this system from a classical target detection system is the use of the quantum correlation feature of the event. In addition to the spatial correlations, temporal correlation information will offer the technology of quantum imaging. can be used in Ghost imaging, quantum LIDAR, quantum microscopy. In order to highlight the quantum property, a successful object-ranging system is obliged to have strong temporal and spatial correlations from the pair of photons. This provides the necessity of detecting a photon with accurate spatial information about the next ongoing photon detected at a clearly defined time.

3.2 Interaction Free Measurement

Our approach is based on a correlated photon pair emission in a nonlinear process of spontaneous parametric down-conversion pumped by an ultraviolet (405 nm) blue laser source to create a pair of energy-time entangled photons at 780 and 842 nm. SPDC system is a heralded single-photon source since the source emits photon-pairs in a spontaneous event. This is when the detection of one photon (idler) heralds the presence of the signal. Commercial companies such as Thorlabs produced an SPDC correlated photon source device with the pump power of 10 mW to 150 mW. This is quite high power to proceed. In our studies, we could obtain 95% of heralding efficiency with a pump power (after fiber coupling procedure) in the microwatt scale. For complete performance; the heralding ratio, pair rate, and $g^{(2)}(0)$ values are given for the pump laser operating at 35 mW and the observed statistics will vary with the pump power and detector specifications during experimenting.

It is compelling to think, the use of parametric down-conversion to produce photon pairs in ghost imaging schemes directly makes the ghost imaging a quantum process. Surely the parametric down-conversion event assists in the formation of entangled photons. The difference from the parametric down-conversion process is that the ghost imaging process only benefits from the spatial correlation of photon pairs. Spatial correlation is a feature that can also be obtained from a classical source. The beam splitter helps us collect the scanning information of the object at the same time. The scanning laser beam passes through a beam splitter: on one side we probe one of the split laser beams, and on the other, we get information about the position of the other split scanning beam. Such a purely classical system can reproduce most image implementations of the down-conversion source.

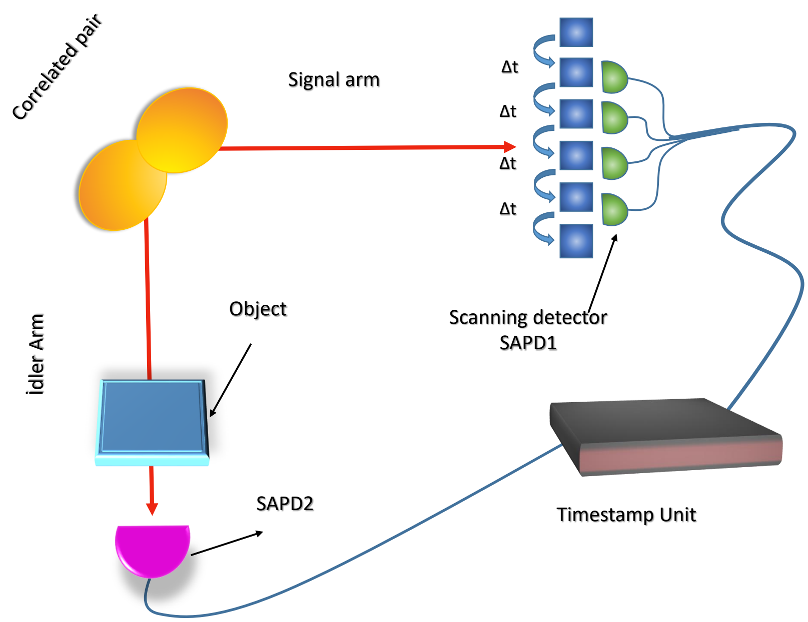

Figure 17: A representative scheme of our quantum target detection system.

In Figure 17, the theoretical framework is shown schematically. It explains the idea behind object detection. After our correlated pairs are created a polarizing beam splitter (PBS) sent the signal and idler photons into two separate optical paths. The signal photons arrive at an object placed on a mirror plate. Here, signals falling on the object are absorbed, and those reflected from the mirror are then collected by a large-area single-pixel photon-counting detector, often referred to as a "bucket detector". Intensified Charge-Coupled Devices (**ICCD**) are highly preferred in these types of detections. The signal arm is the object detection arm where only scattering phenomenon has occurred through the target object and there is no scanning involved. In this detection where the number of the photons reflected from the object matters, temporal information is gathered. The detection is done by a fiber pigtailed single-photon detector (S-Fifteen Instruments, SI-APD).

As in other experiments on similar principles, Hong - Ou – Mandel or where SPDC light is used to produce such as EPR-type spatial correlations, QKD applications. ICCDs or Electron Multiplying Charge-Coupled Devices (**EMCCDs**) are highly preferred in these types of detections. The reason behind that is the ability of those cameras to capture the quantum properties of single-photon detection in which the conventional cameras or detectors are insufficient satisfying. However, there exists the handicap of those cameras being highly expensive (tens of thousands of Turkish Liras). Instead of using those types of cameras, we used a single-photon avalanche detector (**SPAD**) for our heralded imaging system [31].

Scanning with a single-pixel active area might be insufficient as it results in a high loss of photons. To overcome this problem an XYZ Translation stage in the driving range of micrometers is used. By moving the detector in an "S" shaped route (Figure 18), we scanned the whole beam falling on the 180μm diameter active area of the detector. Scanning the beam to obtain a coincidence in this case, we scan the bin width until an avalanche of coincidence is observed. We can calculate the cross-correlation information by knowing the path length between the arms (to determine the delay), the time bin size, and the dead time of the detectors without the help of any device. However, the time stamp unit is specially designed to seek the mutual arrival times of the photons from both SPADs. If two photons arrive simultaneously it is considered a coincidence. The timestamp unit we use (qutools, quTAU) has a time-to-digital converter with 8 independent channels and timing resolution (time bin width) of 81 ps, for all of the experiments in this thesis. The use of a time correlator, allows us to have more control and precision over the coincidence detection information, and therefore the whole experiment.

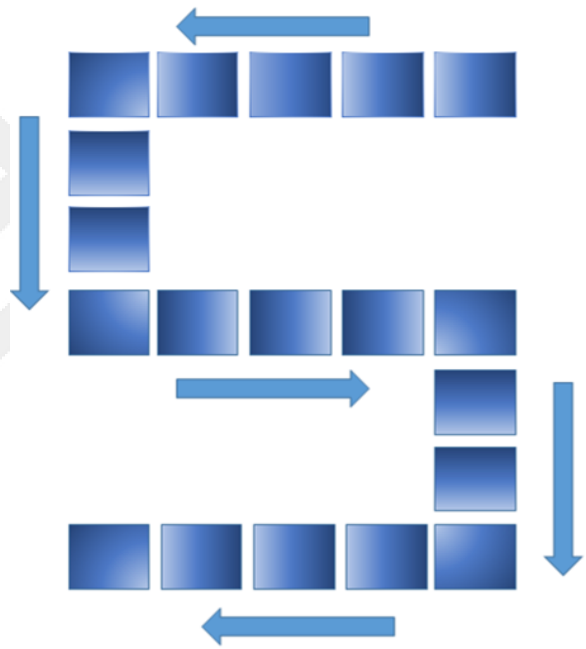

Figure 18: The path followed by the detector during scanning.

The coincidence histogram values helped us to determine the shape of the detected object. The correlation was high in reflectance and low in absorbency, thus a contrast image of the object occurred. However, in this experiment, we could not obtain a sufficient result to present in this thesis. This study is fully open to development as there are some obvious advantages of this system over the classical imaging one. The configuration uses correlated photons and provides high resolution even for very tiny objects. Randomness is inherently included in the system so that having the updated information of the timestamp data does not violate any privacy. This study can be seen as a contribution to the further investigations on SPDC experiments in this thesis.

Detector information

Two different detectors are used for imaging and quantum object detection in the experiments: a fiber-coupled, and a free-running single-photon avalanche detector (SPAD).

When detecting photons with a wavelength of 780 nm we used an SPCM-NIR series SPAD from The Excelitas company. It is a free-space detector, with a square active detection area of 180 μm diameter and designed to detect high bandwidth red and near-infrared (NIR) photons. It has a wavelength-dependent peak quantum efficiency (QE) (an efficiency describing the percentage of incident photons that generate charge carriers) of typically QE of $\approx$ 70% at 780 nm. It has a dark count rate of $\approx$ 600 counts per second. We used this SPAD in free-running mode, where the SPAD was constantly gated. The detector was fixed with a narrow gate width of less than 1 ns, this allowed us to reduce dark counts.

The Si-APD is a fiber pigtailed single-photon detector device that is receptive to visible and near-infrared wavelengths. Photodetection is operated internally by a passively quenched Silicon Avalanche photodiode in Geiger mode cooled to $-30°C$. The device was optically coupled via a 50 µm diameter core multi-mode fiber in a broad bandwidth range of 400-1000 nm wavelengths, a QE of $\approx$ 60% in this region. The practical single-photon system efficiency from the fiber input was measured to be $\approx$ 50% at 808 nm and a dark count rate of $\approx$ 300 counts per second. The output pulse was a NIM pulse of width 2 ns. A suitable NIM to TTL circuitry is designed to connect the output port of the detector to our timestamp unit to collect the detection data.

In the SPAD detection structure, there is a small chance that the avalanche detection mechanism will restart with a signal from the previous photodetection. This results in a double pulse to recognize a single photon. This phenomenon, known as after-pulse, can be avoided by setting a recovery time after each SPAD detection. In order to determine the optimum recovery time, we need to consider the dead time and the timing jitter (time resolution) information of the detectors [32]. The SPCM-NIR detector has a dead time of 40 ns and the timing jitter as 250 ps while the Si-APD has a dead time of 1-2 μsec with a timing jitter of 200 – 600 ps. Those information has been taken into the account and the detection seized with the wait of seconds. Additionally, there were 10 to 15 minutes of waiting before each set of experiments to avoid the detector saturation. As it is known even though we can rely on the internal cooling systems of the APDs the maximum count rate can only be sustained if case temperature is maintained within the specified limits. Those single-photon detectors are designed to support long-range LIDAR, quantum communication, and microscopy, as well as many other quantum applications.

With a type 1, nonlinear Beta-Barium-Borate (BBO) crystal and with an extraordinarily polarized pump source with 405 nm central wavelength. Ray propagates and enters to the facet of the crystal optical axis has a cut-angle of 28.82° with respect to the crystal facet) perpendicular in the optic axis. Refracted on an angle travels through the medium crystal. Gives birth to two ordinarily polarized daughter photons (842 and 780 nm central wavelength). To work in the near-collinear phase-matching regime discussed in the previous section, we slightly tilted our BBO crystal relative to the pump beam's normal. This angle reached to the crystal performed as a tilted mirror for the back-propagated light, accordingly changing the mirror's normal. On the contrary, this slope had no impact on the current mirror's normal set by the orientation of the pump beam in terms of down-conversion configuration. When changing the mirror normal caused the back-propagating light to reach the camera at a different angle to the down-converted photons, but did not disturb the spatial distribution of the detected image. Right after the BBO a bandpass filter that only allows down-converted photons to pass is placed and a plano-convex lens is employed to fine-tune the signal's beam waist and the location at the detector. We can call this procedure collimation. In front of the fiber-coupled detector, an aspheric lens with a 4 mm focal length is used to meet the walked beam from the mirrors. The lens focuses the incoming 842 nm photons and collects them in a $50 \mu m$ diameter core of the multimode fiber. In front of the Excelitas detector, we used a 4 times magnification objective lens to focus the incident light onto its active detection area. And right before the active area, a short pass filter that only allows the photons over 750 nm to pass through the detector is placed. The idler photons with 780 nm wavelength are collected.

The detector saved the photon count information in the signal's detection arm. However, was not able to determine the spatial information. On the other arm of the setup, idler photons that do not travel along the path of the object and have no interaction with it are similarly detected with another bucket detector. This detector was only responsible for the spatial information of its pairs with the technique of scanning. It is not possible to obtain the complete image of the object, using one detector alone. Each detector lacks some information, such as the number of photons reflected from the object (temporal) or its spatial information. Only in the case of two arms' (signal and idler) correlation or in other words coincidence of the pairs cumulatively hold meaning in this imaging scheme.

The structure of the experiment here is similar to the original Pittman et al. [33] experiment in which a bucket detector collects all photons transmitted through the object and a scanning detector measures associated photons passes through an independent optical path.

The back-propagated pump beam couples into single modes within the single-mode fiber (SMF) and the relative phase and polarization of each mode is preserved along with the propagation (Figure 36). Brightness, by definition based on the down-converted pairs in the unit of time per input power (pair count/sec./mW). Brightness will inevitably decrease in the pump's fiber coupling process. The given 35 mW pump power will get down to the microwatt scale which is more than enough for a saturation behavior in the single-photon detectors. However, if we are talking about the quality of the quantum correlated photons and the actual coincidence rate, coupling into the SMF will be beneficial. The reason behind this is that certain collection modes can only pass through the fiber optics cable. As opposed to the increasing quality the brightness will be limited by the walk-off effect of the pump alongside the down-converted photons inside the crystal. In addition to crystal and pump parameters, collection optics plays a big role in the quality of the SPDC photons generated.

When aligning our system, we not only required that the beam passes through the middle of all the optical elements in the optical path, but that the active area of the single-pixel detector overlapped with the center of the down-converted beam profile. This is because to sustain the collinear geometry of the down-converted photons, the spatial distribution of the coincidence counts in position and momentum configurations must be centralized around the same position. Working on the displacement of the beam while trying to preserve the momentum configuration makes alignment harder. The alignment precision required for time-correlated photons is significantly more challenging than the alignment necessary to achieve uncorrelated photons in both channels. The alignment that generates the maximum correlated photon pairs is not guaranteed to be at the exact maximum for the generation of all photons.

There are certain steps in the alignment process to ensure the entire system is nicely aligned. One of the most important points is to maintain the collimation of the beam nicely. We specified the path of the pump beam using pinholes before and 1 m after the BBO crystal. Additionally, passing through all the collection optics' central points from height and width scale. Then the pump laser is forward propagated for alignment such that it overlapped exactly with the pump beam, and aligned the detector arm optics using the pump laser removing the filters and the dichroic mirrors in between.

There are some other important considerations about optics. The coating of the lenses, the fiber optic components, optical filters, should be available for the correct wavelength and have the appropriate damage thresholds. Height of the beam, the beam shape, and mode, fiber coupling procedure every step is crucially important to get the most efficient results. The light should properly pass through the middle of the collection optics materials, not to lose any property caused by the diffraction. Bragg law and different refraction properties should be considered. All these seemingly simple basic arrangements are of great importance in terms of the efficiency and quality of the entangled pair collection.

The beam was then spatially filtered using a pinhole at the focus of a 150 mm lens and collimated again. This intervention is necessary to clean the possible aberrations and the Airy disks to obtain a clear Gaussian mode at the BBO crystal. Choosing a **pinhole-filtering technique** is a well-defined concept and very popular. However, it leads to the loss of most of the photons, and accordingly, the experiment requires a long time to measure the spatial form of the correlation [34]. Respectively physicists started to detect the spatial correlations between the photon pairs with cameras. That removed the necessity to filter them at one particular position. The SPDC is polarized so we are competent to attenuate the beam continuously by using a neutral density filter and a half-wave plate in the pump beam path.

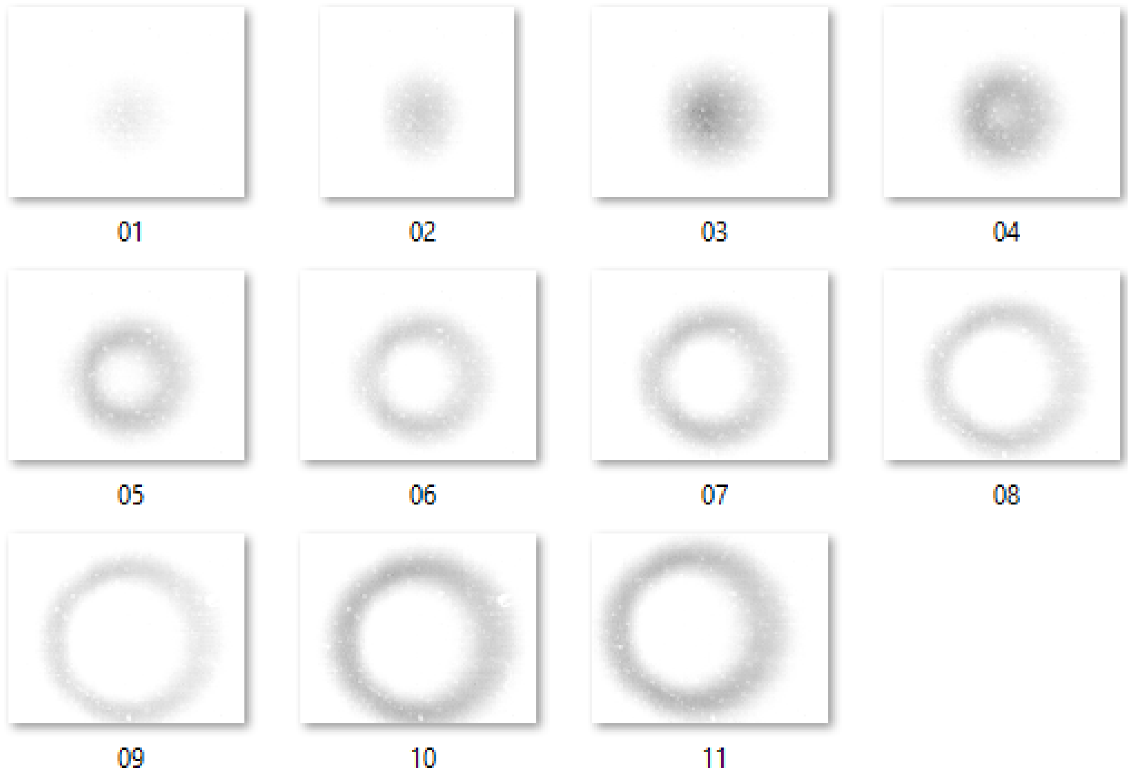

Figure 19: The photo of the SPDC pairs are captured by the CMOS camera. The geometric change in the SPDC pairs caused by the rotation of the BBO crystal, or else by their angular change in conversion process.

The photographs of the down-converted pairs in Figure 19, are taken by a CMOS camera. The camera is placed right after the BBO crystal with a pump blocking low pass filter and an ND filter to protect. Phase matching angle tuning is done by rotating the BBO crystal.

furthermore, to see the effect of polarization we rotated the half-wave plate (HWP) in its circular rotation axes facet relative to the collection lens.The position of the beam on the camera in the momentum configuration has not changed. The ring shape of the pairs is preserved. Only a change in polarization occurred. Even if we change the polarization, other photons with the appropriate polarization will continue to be down-converted in the process. This is because the source will still continue to supply the polarized pump with constant power. Integration of the intensity will not change as it is seen in Figure 10. The torus-shaped geometry gets wider and the intensity value of a point on the non-collinear circle gets reduced [35].

When we move the angle of the fiber facet relative to the collection lens the position of the beam on the camera in the momentum configuration moves so we need to be very careful about every interruption we do. We adjusted the position of the fiber facet and collection lens ensemble until they overlapped with the position of the directly imaged down-converted photons. We then adjusted the angle of the fiber facet with respect to the collection lens such that the back-propagated beam passed directly through the pinhole behind the crystal.

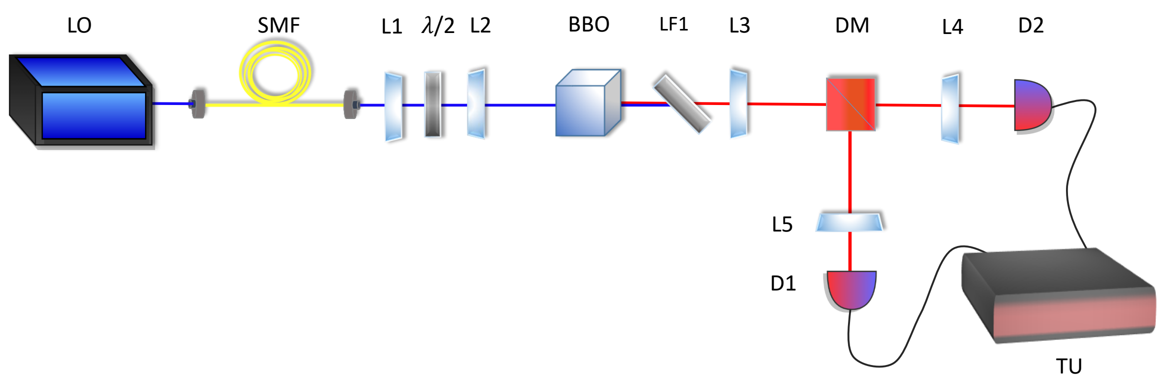

Figure 20: The basic SPDC layout. LO: Local oscillator,SMF: Single mode fiber, L1,L2: collimation lens, $\lambda/2$: Halfwave plate, BBO: Beta-Barium-Borate crystal, LF1: 405 nm lowpass filter, L3: Optical Lens, DM: Dichroic Mirror, L4,L5: Focusing lens,D1, D2: Single photon detectors, TU: Timestamp unit

The brightness of the pairs is an important parameter that defines the source power. Considering an SPDC system installed out of preserved laboratories, maybe in the open air without the use of fiber optic cables, maintaining high brightness is crucial. The reason for this is the expectation that the weakening caused by environmental factors will be excessive. Accordingly, we made the experimental setup shown in Figure 20. Our down-conversion source consisted of a high-repetition-rate laser and a BBO crystal. This down-conversion source is repeated several times for each experiment presented in this thesis and is presented as the source from the pump and BBO crystal. We used a continuous-wave (CW) narrow bandwidth (160 MHz) Ondax laser with the central wavelength at 405 nm in the single-mode. The max output power at the laser head was 150 mW. In all of the whole experiments, the preferred power (before fiber coupling) is 35 mW. The signal and idler photons produced in the BBO crystal and pairs spatially separated using a dichroic mirror. Photon counters placed on each arm generate an electrical pulse upon arrival of the photon, and the timestamp unit records the timing information of the photons. A highly time-correlated measurement was detected in our arrangement, as measured by coincidence detection in the picosecond time window. We observed SPDC brightness as approximately 0.5 M photon count per mW optical power.

Obtaining high brightness with SPDC photons was achieved with the following experimental conditions:

1. Establishment of the adjusted BBO crystal angle for the collinear SPDC mode in the setup.

2. To align the conically diverging entangled pairs parallel to each other, an aspherical lens is placed at a distance of one focal length from the crystal.

3. Preferring the BBO Crystal prism with a long side of 10 mm. The reason for this preference, as it is explained in Kuniyil et.al. [36] of the variation of

entanglement brightness changes with the crystal length.

4. The pump laser source is focused in the center of the crystal. The brightness can be improved by increasing the pump power below the crystal damage threshold.

Figure 21 shows the SPDC system with a typical critical phase-matching configuration. The single-mode blue laser beam from the fiber is polarized at 45 degrees by the HWP and passes through the pre-compensation crystal. Then, the SPDC process takes place in the BBO I and BBO II crystals, which are positioned perpendicular to each other. We preserved the down-converted light's wavelength through the use of 10 nm bandpass filters in the setup.

The pump is pulled out of the optical path at this stage and down-converted photons pass through the BBO III, BBO IV, and the post-compensation crystal. After passing through the light-collecting lens, it is analyzed in the P plane. For photons in the P plane to be in an entangled or Bell state, extra steps and processes are usually required.

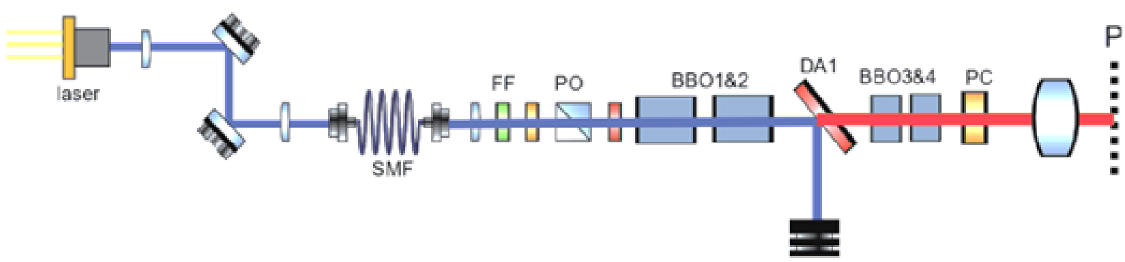

Figure 21: Experimental setup for polarization-entangled photon pair generation.

The ability to separate pairs with different polarizations by position and phase prevents entanglement. Matching and compensation crystals to be used to obtain the entangled state can be used as found in the literature. BBO I and II crystals are arranged perpendicular to each other, meaning the down-conversion pair from the first crystal will have extraordinary polarization in the second crystal. Therefore, there is a vertical delay between pairs from two crystals, and there will be a spatial difference between horizontal and vertical pairs if precautions are not taken against it. Such distinguishability between these pairs of different polarizations will cause their polarization to become nonrandom, thus preventing entanglement. Therefore, a pair of BBO crystals half the length of the BBO I and II crystals is used to spatially pair the pairs.

The BBO crystal is a type 1 crystal that allows a pump photon of extraordinary polarization to produce daughter photons of ordinary polarization. The aim of the experimental setup is to obtain two down-converted photons at 780 nm and 842 nm wavelengths from the pump photon at 405 nm wavelength. In this case, the optical axis of the crystal must be at an angle of 28.82 degrees with respect to the crystal's facet. This angle between the propagation direction and the optical axis of a photon propagating perpendicular to the crystal surface is called the crystal cut angle.

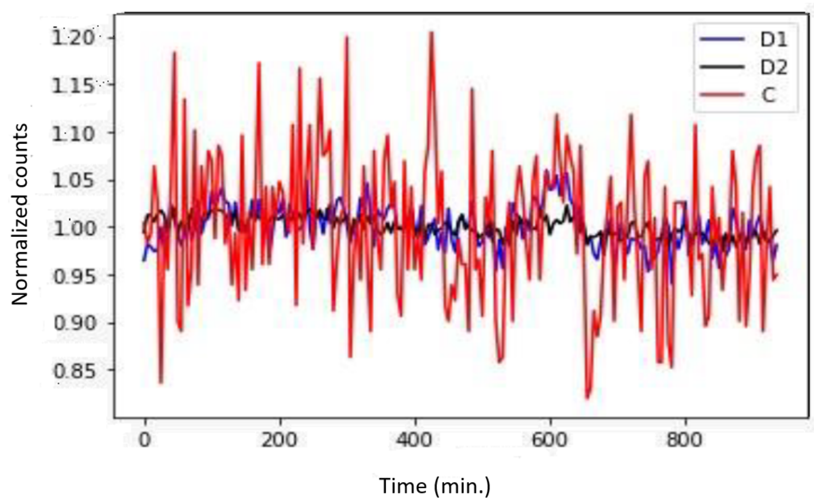

Figure 22: Time-dependent variation of the signal, idler, and coincidence counts of an optical tabletop entangled photon source. The blue data shows the signal photons in the first detector D1, the black data shows the idler photons detected in the second detector D2 and the red data represents the coincidence measurement as a result of both detectors.

The characterization of the passive stability of the bench-top entangled photon source has been carried out as another finding. In this research, an entangled photon source with a fidelity of 0.97 was left operating for long-duration measurement to observe the stability in the down-converted photons single-photon detection process. The signal, idle, and coincidence measurement numbers were observed for 16 hours. The photograph of the experimental setup can be seen in Figure 37. In the laboratory where this measurement is carried out, there is a temperature control infrastructure that is fixed with an error of approximately ±1 degrees to minimize the fluctuations in the measurement. Optical alignments deteriorate as the change in temperature physically affects (physical processes such as expansion or contraction) the length of optomechanical holders, which are mostly aluminum or steel. Despite all the precautions taken, this is the most important reason for the fluctuations seen in the graph of the stability measurement results in Figure 22. As seen in the graph, although detector D1 has an external thermoelectric cooler and D2 has an internal (within the diode) thermoelectric cooler, the detectors show similar changes depending on temperature. The amount of normalized fluctuation in the coincidence measurements appears to be higher than the fluctuation in the D1 and D2 detectors, which measure signal and idler photons, respectively. This is because the coincidence is a conditional convolution of the fluctuation in the signal and idle measurements. The condition here is that the signal and the idle photons coincide within the same detection range (window). In other words, in order for the coincidence to be affected at the same rate in the fluctuations in the D1 or D2 detector measurements, the lost or extra measured signal and the idle photons must be paired.

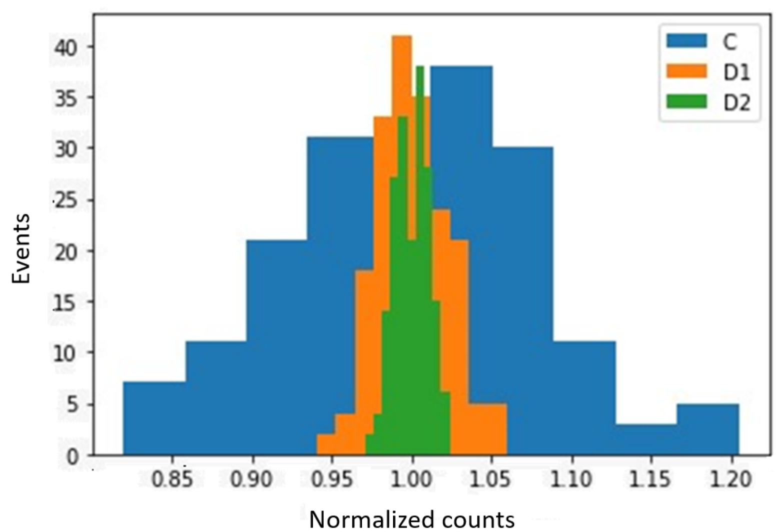

Figure 23: Histograms of fluctuations in signal (orange) and idle (green) photon measurement number and their coincidence (blue) ratio. D1 and D2 represents the detector measurements of signal and idler photons respectively with their coincidence (C) information.

The fluctuations in Figure 22. were converted into histograms and the relative amounts of normalized fluctuations were compared in Figure 23. The reason of signal photon count histogram is being relatively larger than the idle histogram is; the detector used in the signal arm is more sensitive to environmental temperature changes due to the external thermoelectric cooler. The detector which collects the idler photons, on the other hand, is less affected by environmental temperature changes. That is because of the usage of a small Peltier element in the APD and the filling of the p-n junction with buffer gas inside. Since the alterations in the temperature change the breakdown voltage of the p-n junctions inside the APDs, the applied reverse bias voltage effectively decreases or increases accordingly. Naturally, this will lead to a change in the peak height of the avalanche current which will highly affect the photon detection efficiency. If we need to examine it in terms of photon statistics, as in every light source with Poisson distribution, in this down-conversion event also the number of entangled photons fluctuates with the amount of Shot noise. The width of the coincidence histogram (blue peak) appears to be larger compared to the widths of the signal (orange peak) and idler (green peak) histograms as described above. However, the fluctuations are below 20% and this fluctuation does not threaten the quality of the down-converted pairs. This information we obtain from the passive stability test of the setup provides us an expectation in the case of the source being used as a tool in different quantum technology settings such as QRNG or QKD systems. In such systems, randomness and security are huge concerns. Regardless of the number of pairs generated per second, it is mostly about determining a larger time bin for the coincidence measurement to avoid the negative effects of the fluctuations. So knowing the passive stability information depending on the mechanism is of great importance for the smooth operation of the protocol.

3.3 Noise-Tolerant detection and ranging with SPDC

Quantum illumination (QI) systems and target detection configurations use the benefit of the temporal correlations; however, this can be inefficient under the influence of high noise in the background. This study proposes to question the conservation of polarization entanglement by violating Bell's inequality. For this purpose, sources of temporal and polarization correlated photon pairs obtained from the spontaneous parametric down-conversion process (SPDC) are used.

This section shows that the polarization correlation can still be preserved from the target information realized with the photons returning from the scattered surface. The scattering phenomenon seems unaffected when it comes to the conservation of polarization correlation in entangled pairs.

In a controlled experimental environment where the noise in the background is deliberately increased, the amount of accidental coincidence in the photon detection also increases. We notice that, as being linearly dependent on the noise level, visibility gradually decreases. Even under those circumstances single to noise ratio (SNR), correlated photon pairs over the noise in the environment can be achieved in high ratios. Whereas the visibility decays, the SNR could be improved 2.85 times compared to the case in which only temporal correlations are relied on. This particular enhancement in the QI sensing is by the virtue of polarization correlations in addition to the temporal correlations.

Lopaeva et. al demonstrated a laboratory setting of phase-sensitive quantum illumination that confirmed an enhancement of the quantum detection scheme [37]. Their system utilized the spontaneous parametric down-conversion process (SPDC) to generate a pair source that has non-classical spatial and temporal correlation. Maintaining the spatial correlation is critical in this kind of system.

Therefore, one has to take the measurement at the image plane of the pairs. This means we need to take into account a significant precision in positioning detection settings leading to an unrealistic scenario in obtaining a target of unknown distance and fluctuating. Scattering of light after interacting with a diffusive target also poses a challenge in a realistic quantum detection scheme since the scattering of entangled photon pairs also loses its nature. Therefore, this system is only appropriate to use for an object that has an optically smooth surface. These factors are challenging to use quantum illumination in practical applications.

As a solution to these problems, just non-classical temporal correlated pairs are used in the QI type detection scheme. However, the phase-insensitive setting does not fully offer the benefits of QI. There are many benefits upcoming from QI schemes different to the classical schemes, simple experimental arrangements that motivate the quantum system (phase insensitivity) over classical systems with high response time and the ability to adjust the wavelength of the source [38] (especially for quantum imaging applications) can be counted as examples.

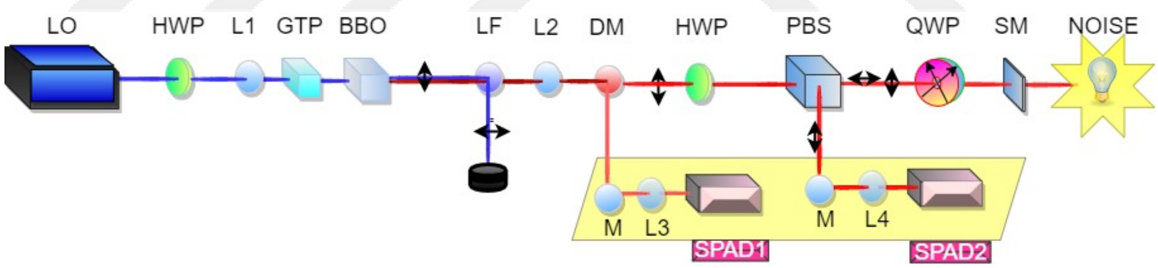

Figure 24: Experimental setup for noise-tolerant SPDC. LO: Local oscillator, HWP: Halfwave plate, L1, L2: collimation lens, GTP: Glan-Taylor Polarizer, BBO: β-Barium-Borate crystal, LF: lowpass filter, DM: Dichroic Mirror, M: regular Mirrors, L4, L5: Focusing lens, SPAD1, SPAD2: Single photon detectors, PBS: Polarizing Beam Splitter, QWP: Quarter-wave plate, SM: Semitransparent Mirror.

We previously discussed the pair detection system relies on natural spatial correlations between the generated twin photon pairs from the SPDC process. The twin pairs pass through a BS and are split into two spatially different arms of the experimental setup. In the messenger arm, the photon arrives at a transmitting object before being detected by a single-photon detector. In the imaging arm, the correlated photon is detected again in a free-space delayed path before being detected by the SPAD.

Similar to previous sections also in this experiment we use the SPDC configuration as the source. After the fiber coupling process, the pump power input to the SPDC configuration is given as $128\mu W$. Separated signal and idler photons are collected by APDs as in previous schemes. We have some additional optical components such as polarizing beam splitter (PBS) and Quarter wave plate (QWP) to preserve the polarization correlation property of the scheme.

- An external broadband and non-polarized noise was externally injected to test the behavior of the system in a noisy background.
- We have two experimental schemes. In the first one we carry out the polarization and time correlation (P+T) property of the source together and in the second scheme, only the time (T) correlation property of the source is used in the experiments.

The $g^{(2)}$ values of the two case is measured and the signal-to-noise (SNR) ratio is calculated for both schemes and they are compared to each other. The relation between the $g^{(2)}$ value and the SNR is also explored in this experiment.

To observe the noise effect clearly a halogen light bulb (thermal source) is used for the noise source. The voltage is increased step by step gradually and accordingly the background noise in the setup proportionally increased. As a result, reduced noise in the P+T settings is observed. This is because of the filtering effect due to the polarization correlation of the scheme.

Although noise reduction was observed in the P+T settings, SNR values of both systems are overlapping in the observed singles' values. However, the P+T setting gives an advantage in filtering the unpolarized broadband source.

- The higher SNR is observed for the P+T settings when it is plotted against the injected noise.

- The P+T settings showed an advantage in the SNR value against injected noise. With the increasing external noise, the advantage of the configuration also increases dominantly. This outcome is a huge contribution to the literature and eases the experimental conditions of any QI scheme.

We can use the second correlation function's $g^{(2)}$ value as a test to determine the source type in phase-insensitive systems. We can determine if the source is classical or a quantum one. When the $g^{(2)}$ value is above 2, we can conclude that source has the quantum property since any classical temporal correlation can maximally take the value of 2 [39]. For instance, the thermal source has $g^{(2)}$ value of 2 at the maximum, this is the highest in the classical regime. We observe that the measurement of $g^{(2)}$ function is equivalent to SNR.

The aspect of the experiment is about using temporal and polarization mobility of the SPDC correlated photons. An external (broadband and non-polarized) noise is externally injected to test the behavior of the system in a noisy background. This external noise is used as a tool to observe the noise influence on the quantum process. We experimented with two schemes in one configuration. In the first arm of the setup we carry out the polarization and time correlation (TPC) property of the source together, and in the second arm, only the time (TC) correlation property of the source is used. After the experiments with the collected data from the photodetectors and their correlation information from the timestamp unit. Based on those data, the $g^{(2)}$ values of the two cases are measured and the signal-to-noise (SNR) ratios are calculated for both scenes then they are compared in each other. The relation between the $g^{(2)}$ value and the SNR is also explored in this experiment. The result indicates that TPC has higher quadratic coherence than TC in a noisy environment, therefore improving resistance to noise only in temporally correlated circumstances.

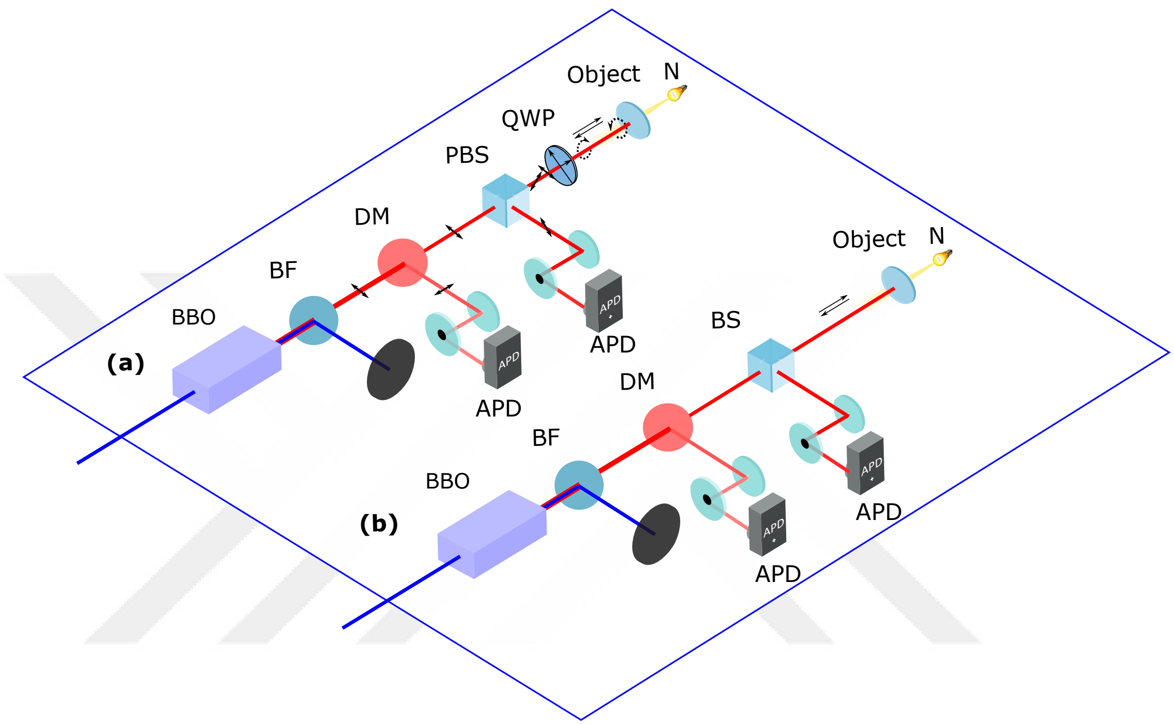

Figure 25: The experimental arrangement used for testing the detection schemes that uses (a) time- and polarization-correlated twin source and (b) only time-correlated source.

The block diagram of the experimental setup of this study is shown in Figure 25. As in previous sections, correlated photon pairs generated in an SPDC process are used as the quantum source. Our pre-mentioned CW laser source is used as the pump source and interacted with the BBO, creating co-polarized signal and idler photons. In this demonstration, we call "the signal photons" for transmitted photons that interact with the target and "idler photons" for their twin pairs which are recorded locally. We can name the polarization of the signal and idler photons as $|H_s\rangle$ and

$|H_i\rangle$, where H denotes the photons are horizontally polarized, and s and i suggest the signal and idler photons, respectively. The polarization state of the idler photons is converted 90$\circ$ with the help of HWP, before being collected at photodetectors. After this treatment, the combined polarization state turned to a vertical position from the horizontal state and named $|V_s\rangle$ and $|V_i\rangle$ respectively.

During the experiments, we had some trials and according to our results, we made some changes to find the most suitable and correct configurations. In one of those configurations, anodized aluminum is used as the target object to see if the polarization correlation of the source is preserved after a diffusive scattering process. The anodized aluminum has an absorption coefficient of 0.87 ± 0.02 and the scattering coefficient of 0.13 ± 0.03 [40]. These values indicate good diffusive material, and therefore, the detection probability of back-reflected signal photons is significantly low. Numerically we obtained a coincidence detection of 200 ± 10 when the target was placed closer (10 cm) to the transmitter (distance from the PBS and object in Figure 25, a. In another configuration, the anodized aluminum is substituted with a semitransparent mirror for the target to enhance the external noise injection photons.

To observe the noise effect clearly a halogen light bulb (thermal source) is used for the source. The voltage of the lightbulb is increased step by step gradually, accordingly the power and the brightness is also increased. Subsequently, the background noise in the setup is proportionally augmented. We preferred to use a broadband source in order to perform more realistic situations where spectral filtering cannot annihilate the noise. Besides, a thermal light source like that serves as a suitable noise model in a correlation-based detection scheme as it shows high classical correlations [37]. The noise is also non-polarized, and together they provide a complex scenario for filtering out noise other than separating the transmitter signal individually using temporal and polarization correlations. In addition to polarization, signal and idler are also temporally related.

In the case where both time and polarization correlation are used: The blue input pump is blocked by a band-pass filter right after the BBO. The signal and idler beams are separated by a dichroic mirror. The signal is directly measured by the APD. The idler beam passed through a polarizing beam splitter (PBS) and then a quarter-wave plate (QWP) before being backscattered by the target object. The horizontally polarized idler photons $|H_i\rangle$ were right-handed circularly (RHC) polarized in the forward direction of the QWP. After being reflected over the object they turned to be left-handed circularly (LHC) polarized. On the return path, the LHC signal becomes vertically polarized $|V_i\rangle$ after the QWP is ultimately reflected in the PBS and detected by the other photodetector (APD2).

The scheme where only time-correlated case (b), has some differences. Idler photons transmitted and passed through a beam splitter. Afterward, they are reflected from the object surface and half of the return signal is reflected towards the APD in the beam splitter (BS). The intensity of the SPDC source is arranged carefully so that equal conditions can be created to obtain an equal number of pairs for both settings. The output of the two APDs is provided to the timestamp unit (not shown) to record the timing information of the signals. An unpolarized and broadband external noise source, in other words, the previously mentioned lightbulb (N) is injected to examine the performance of the system. The temporal correlation between the signal and idler photons is due to their simultaneous birth in the annealing process at the BBO crystal. In this scheme, because we are only using phase insensitive quantum correlation, the signal arm is free to delay the idler arm. The SAPDs collect the signal and the idler photons and their output is sent to a time-stamping unit which records the arrival time of the individual photons, if two photons arrive simultaneously it will display as one coincidence. To acquire a coincidence in this case, we scan the timing bin width until an avalanche of coincidence is observed. The timestamp's operating mechanism and its specifications are discussed in previous sections. Here in this noise-tolerant

SPDC source configuration, we obtained the maximum coincidence value when the pump power is set to $126 \mu W$. This maximum value is detected as 5300 ± 100 pairs per second with noise-free settings.

The losses in the system and the non-unitary reflection coefficient of the object are the major cause of pair loss. Considering all the limitations arising from the experimental conditions, the coincidence values were maintained approximately at the same rate for both TC and TPC schemes Figure 25 a and b to make a reasonable comparison. To compare the quantum correlation in those two schemes, we calculated the $g^{(2)}$ value from the experimental coincidence and singles values of the signal and idler. The corresponding approach for $g^{(2)}$ calculation in our configuration is as follows:

$$g^2(\tau) = \frac{C(\tau)}{N_S N_T \Delta f T} \tag{3.3.1}$$

Applying the equation, we obtained the maximum $g^{(2)}$ value for the case of TC as 260 and TPC as 261 in a noise-free condition. When we gradually increase the external noise level, which we mentioned in detail before, we observe a significant decrease in the $g^{(2)}$ values for both schemes. This reduction in the $g^{(2)}$ values is compared to the two schemes' noise-free setting in themselves. When we compare the two scenarios (TP and TPC) among each other, we can clearly see the scheme in TPC, in polarization correlation case, the reduction in the $g^{(2)}$ value is much smaller. This is because our QI scheme uses the benefit of the polarization: the external noise in the setup is unpolarized and our SPDC pairs have polarization correlation and it is maintained by our polarized optical component choice.

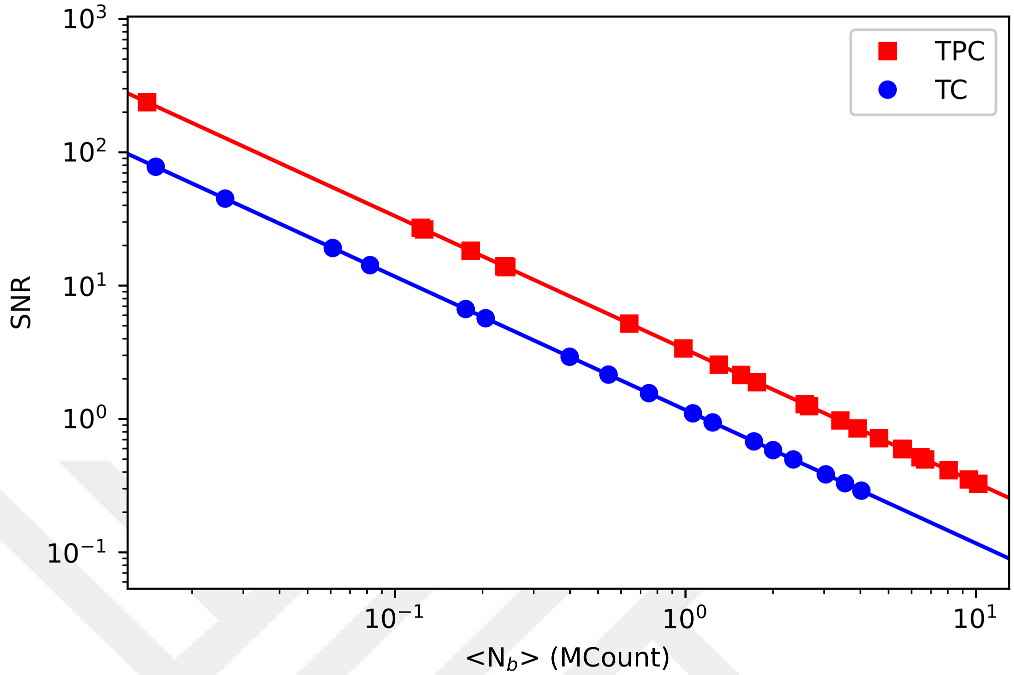

Figure 26: The measured signal to noise ratio (SNR) versus the injected noise N_b is plotted for time correlation (TC) is shown in blue, time and polarization correlation (TPC) is shown in red.

Figure 26 shows the results from the comparison of temporally correlated signals which has the property of quantum correlation with both temporal and polarization correlated ones an enhancement in SNR of 2.8 in the TPC case is observed. We should realize that this enhancement of 2.8 is not with the classical case. The quantum advantage over the classical one is pointed out many times in the literature as mentioned previously. In a normal noise regime, improvement in the signal to noise ratio can only be less than 2, but in high noise regime where the detector operates near saturation region it can be changed. The noise value is measured before the detection of the second detector. For example, if the injected noise creates 12 million of coincidence count for the PCT case, it will only detect 6 million photons. But in TC's case, the detector receives 12 million including accidental coincidences originates from the injected noise. Since in TC case detector operates in saturation region and PTC does not, the accidental coincidence (tau(Nb+Ns)Ni) value remains the same for both cases. But, near saturation, we will obtain less signal-idler coincidence that gives greater than 2 SNR in the case of PTC. The behavior of the second-order correlation function with various input noise levels is shown in Figure 26. By consistently increasing the amount of noise injection we estimated the $g^{(2)}$ value (hence SNR). With injected noise, a proportional drop in the SNR value observed for both TC and TPC settings, with TPC has an enhancement. Here, note that $g^{(2)}$ is the total coincidence value including the accidental ones. Therefore, the signal level in the SNR is indicated by $g^{(2)}$ - 1 to subtract the effect of noise.

Moreover, in Figure 26, we see the second-order correlation function with various input noise levels. We calculated the $g^{(2)}$ value (indirectly the SNR) by continuously increasing the power of the lightbulb in order to increase the external noise. As the background noise increases, we observe an improvement in TPC with a proportional drop in the SNR inspected for both the TC and TPC schemes. The reason for this drop is the increment in the accidental coincidence rate, which naturally increases with the noise level in the system.

The denominator of the $g^{(2)}$ function equation (NsNiDtT) is directly giving us the accidental coincidence. Based on this information and the SNR definition in coincidence detection schemes, we conclude that the true estimate is about the level of the accidental coincidence under the influence of external noise. Another point to consider is the type of noise source and the property it carries. A thermal source will be reflected with high correlation values because of its broadband light property, thus the broad photon statistics effects. This chaotic behavior naturally will increase the accidental coincidence detection.

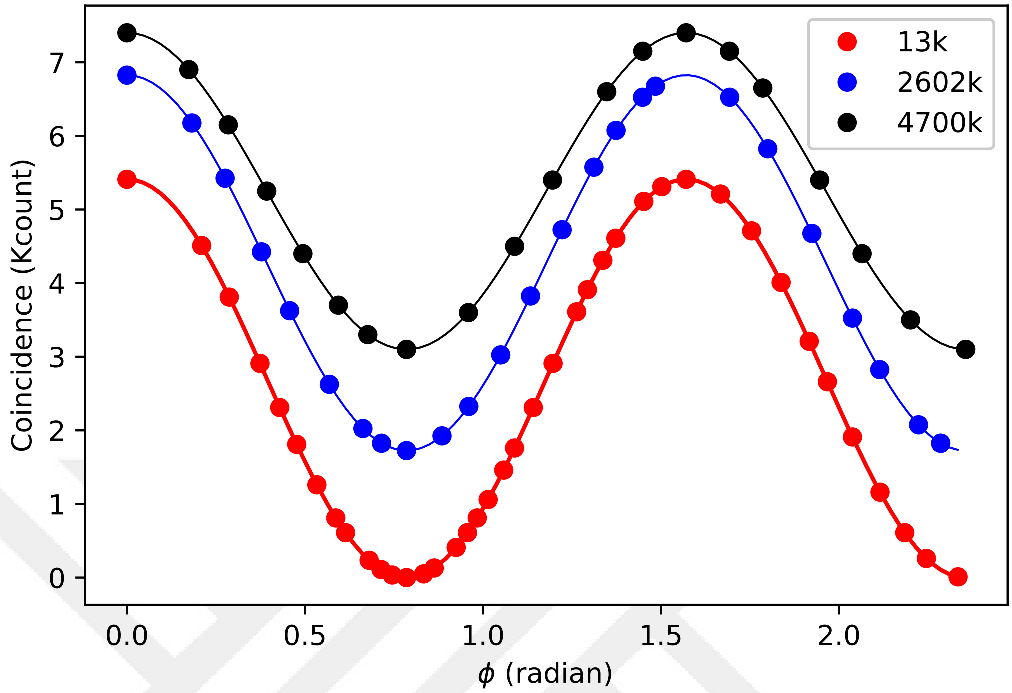

Figure 27: Sinusoidal behavior of coincidence counts reasons from the rotation of the quarter wave plate (based on phase change) for different noise levels.

In our experiment, we observed a linearly proportional relation between the accidental coincidence number and the noise. The results revealed that preserving the polarization correlation allows the received signal to be controlled, and therefore better analysis of signal and noise. Figure 27 shows the sinusoidal behavior of the light reflected from the object. The graph shifts upwards along with the increasing noise. In this detection using optical elements with polarizing properties helped us to create this noise-tolerant QI scheme. The data in Figure 27 is collected by rotating the quarter-wave plate on the optical axis so that a combination of PBS and QWP (see Figure 25) only allows vertical linear polarized light to be able to detect by APD. This setting of controlled rotation of the QWP and assessing the change in coincidence detection authorizes us to differentiate the signal from noise (in other words the accidental coincidence).

We can name the magnitudes of the sinusoidal graphs as $C_{max} - C_{min}$, where C_{max} and C_{min} are the reading of coincidence values in two schemes. C_{max} is the situation of both signal and the idler photons presence. C_{min} is the reading of noise only presence. This behavior is caused by the functional limitations of APD in the saturation region. In the previous sections, I explained the conditions that affect the detector operation and its constructional limitations.

To be specific, detectors will not detect the correlated pairs due to the increased time of the detector. Because it takes a certain time for the detector to return to the near-breakdown region when a high amount of photons are present [41].

Different from the literature, we introduced a definition of **visibility parameter** involving the detector information as a sub-parameter. This calculation will prevent misleading conclusions based on constraints from the detector's internal electronics circuitry in QI detection schemes.

$$V = \frac{C_{max} - C_{min}}{C_{max} + C_{min}} \tag{3.3.2}$$

In the absence of background noise, C_{min} becomes zero leading to the visibility value being unity. An estimation of visibility over noise level is plotted in Figure 28 (inset). C_{corr} is the coincidences obtained between the signal and the idler, N_s and N_b are the number of the signal and noise photons, respectively, C_{ac} is the accidental coincidence and d is the detector's correction factors.

The relation between visibility and the level of injected noise imparts the idea that visibility is less sensitive to noise. For instance, the slope of the SNR versus injected noise is 2.64×10^6 (DSNR/DN) while it is 1.09×10^7 (DV/DN) in case of visibility versus the injected noise plot. For better intuition of this fact, a plot of the SNR versus visibility is also given in Figure 28. Its slope is 24.26. ($\frac{\Delta SNR}{\Delta V} = \frac{\Delta SNR}{\Delta N} \times \frac{\Delta N}{\Delta V}$), which validates that the visibility has less susceptibility to the noise.

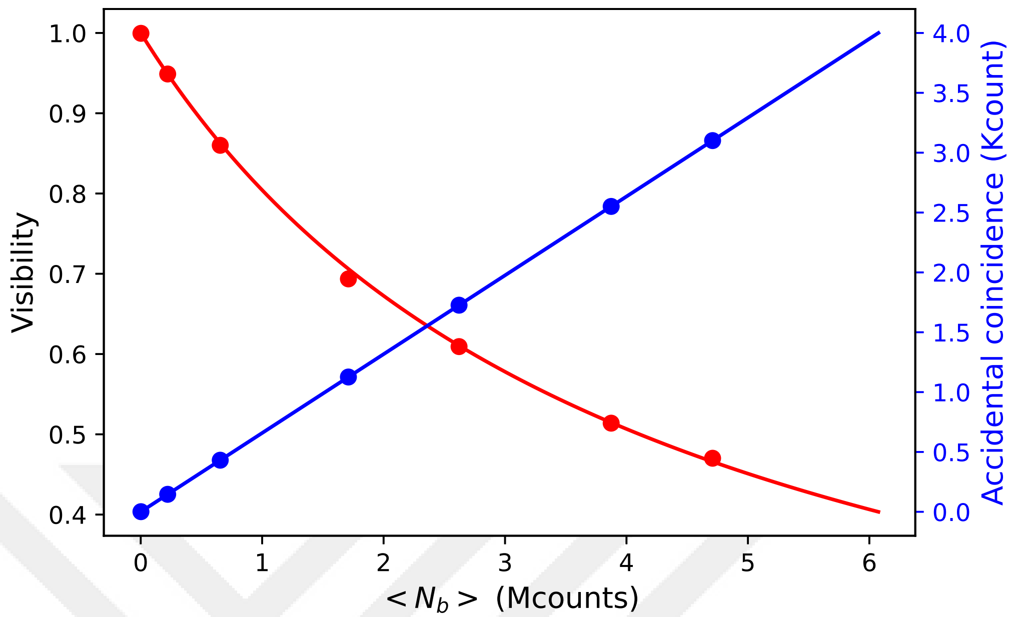

Figure 28: The variation of visibility over SNR. Solid line is the theoretical fit developed by using Equation 3.3.3.

$$V = \frac{C_{corr}(N_S)}{C_{corr}(N_S) + 2C_{ac}(N_b)d} \tag{3.3.3}$$

The change in visibility as a function of the average noise (N_b) is shown in the inset. The theoretical fit made by using the empirical relation $V = (g^{(2)}(\tau)-1)/(g^{(2)}(\tau)+1)$. This new parameter of visibility gives an understanding of the possibility of storing information in the relative angle between the linear polarization of the two photons. We find that the experimental trend, i.e., a steep reduction in bunching visibility, is reproduced quite well by this model, while the observed visibility is significantly smaller than the theoretical ones. The polarization correlation between the signal and the idler arm, in addition to the temporal correlations, provides distinguishability in coincidence measurements between the SPDC and the noise photons.

With a single-photon pair detection mode, the entangled event shows much better visibility information compared to the conventional correlated thermal light. The actual visibility will be incorrectly calculated If the characteristics of the detector are not taken into account. This advantage of quantum entanglement disappears as the number of photons under the noisy environment increases, and the visibility becomes the same for quantum and classical sources. We can explain the reason for this situation as follows; It turns out that the particular difference between the use of the two types of sources is not due to entanglement but to the possibility of operating in the photon counting regime in the quantum state.

In this section, we introduced a new parameter defining visibility, which is free of the detector's operational change during the sensing process. When there is no background noise the visibility ratio is equal to unity and under the influence of increasing noise in the environment, accidental coincidence increases as well. Accidental coincidence amount is inversely proportional to the visibility.

Different from the literature this definition of visibility parameter here involves the detector information which will prevent results from being misleading with the detection limitations based on its internal electronics circuitry. In the next section, experiments and observations related to detector measurement reliability will be shared.

3.4 Effect of Photon Statistics on Single Photon Detection Efficiency

In the literature, visibility in a single-photon-counting regime is highly dependent on the detector operation efficiency. If the visibility parameter is not independent of the photon counting regime, then the observable advantage of the SPDC source over the classical source disappears. In this section, the detector effect under increasing pump power and noise conditions is observed.

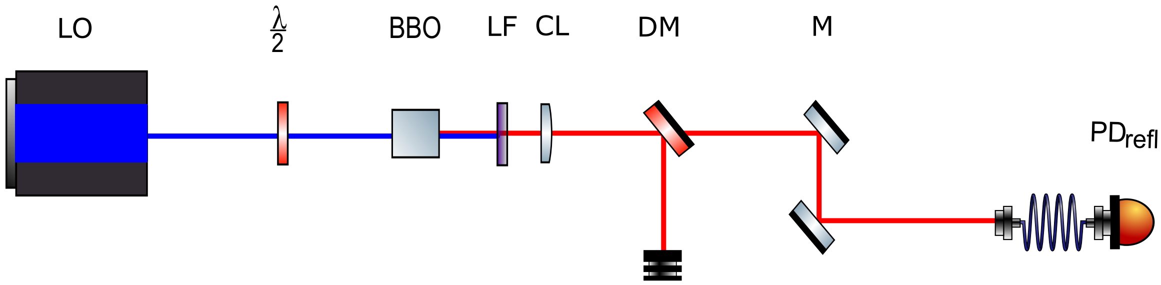

Figure 29: The block diagram of the controlled detection saturation setup. LO: Local oscillator, $\lambda/2$: Halfwave plate, BBO: Beta-Barium-Borate crystal, LF: 405 nm lowpass filter, CL: Collimation Lens, DM: Dichroic Mirror, M: Standard Mirrors, PDrefl: Photodetector

We set an experimental scheme as in Figure 29 to observe the detector behavior limits under possible experimental conditions. To eliminate the classical limitations and focus on the quantum efficiency information of the detectors, an SPDC source is preferred. The same laser source and detectors as previous SPDC source settings are used with a slightly different configuration. After the single-mode laser, a HWP is used to Temporal and spatially correlated photon pairs are generated by using a birefringent crystal. Those correlated twin pairs pass through a dichroic mirror and are split into two spatially different arms of the experimental setup. Idler photons are lead to a beam dump. On the signal arm side, the fiber pig-tailed detector captured the singles' values. The data collected from the several experiments in the same conditions results as in Figure 30.

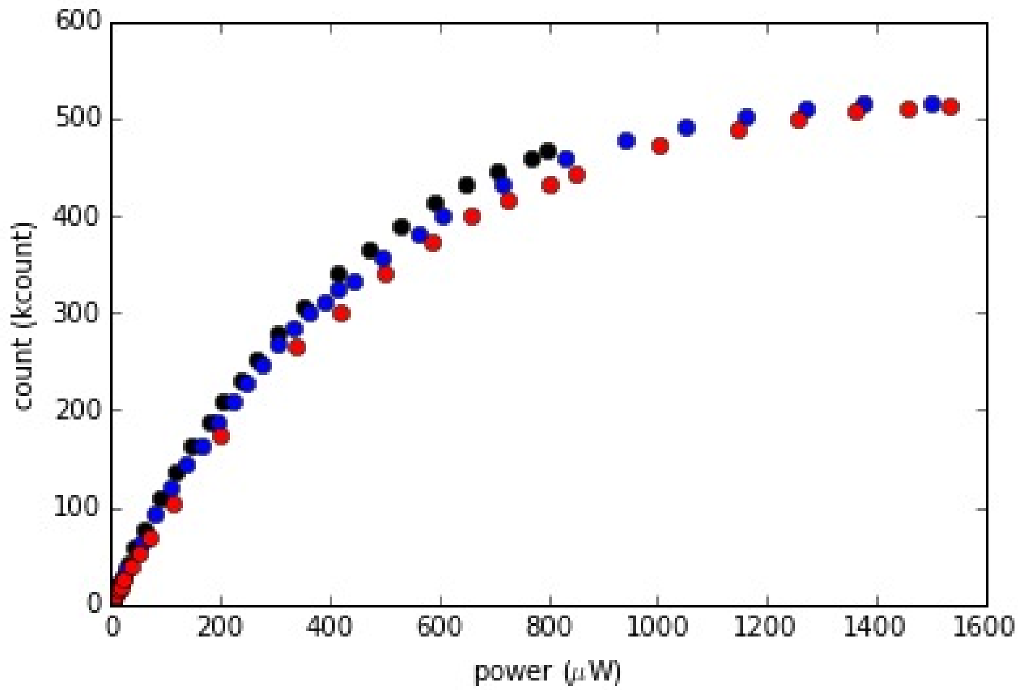

Figure 30: The results of the photon count measurement with the increasing pump power in different experiments.

As the power increases in the microwatt range step by step, the photon count is recorded by the SPAD. The detection behavior appears as a non-linear increase trend. When the SPDC input power carries the detector to the saturation region, we cannot observe any increase in the photon count. This is only because the detection is not possible thus it exceeds the detector's limits.

The timing jitters of the detectors have been measured as approximately 300 picoseconds, and there may be a security gap between the timing jitter values and the time bin value of the time tagging information. A theoretical study in our research group modeled that the relative delays and timing jitter differences that will occur between the detectors are problematic for a certain time bin value.

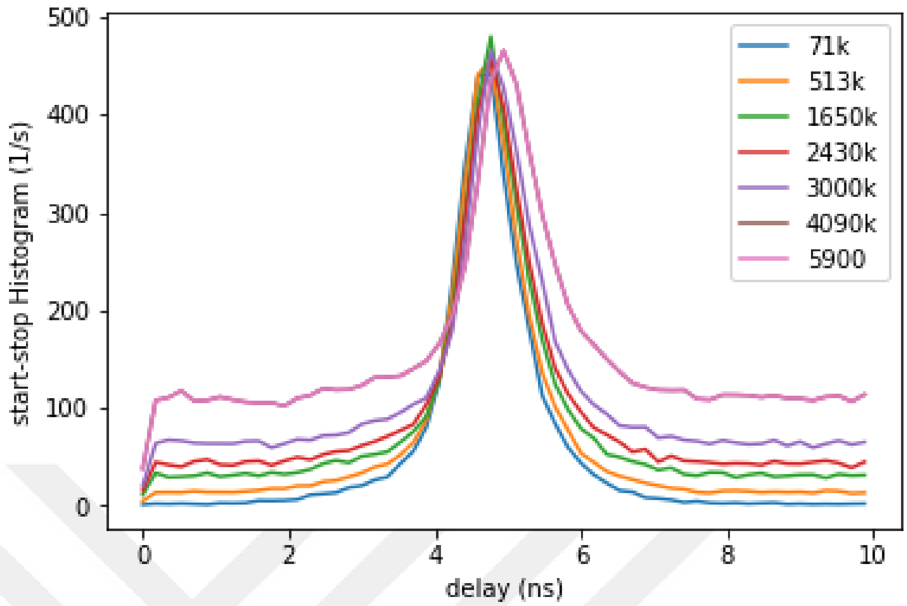

Figure 31: Correlation delay and Correlation width based on the number of coincidence measurements per second.

Additionally, this theoretical work showed that the detectors with timing jitters as high as possible should be preferred, provided that they are shorter than the coincidence window duration. These preferences are expected to increase security. In order to confirm this theoretical study and the expectations, we experimentally tested that the relative delay and timing jitter amounts of the detectors change depending on which parameters. In this test, the coincidence correlations of the photon pairs coming from the entangled photon source were examined. Figure 31 shows the changes in the correlation delay created by the coincidence rate, depending on the increase in the number of coincidences measured per second. As the coincidence rate measured per second increases, the correlation delay increases (it may vary depending on the reference detector), and the correlation peak width increases.

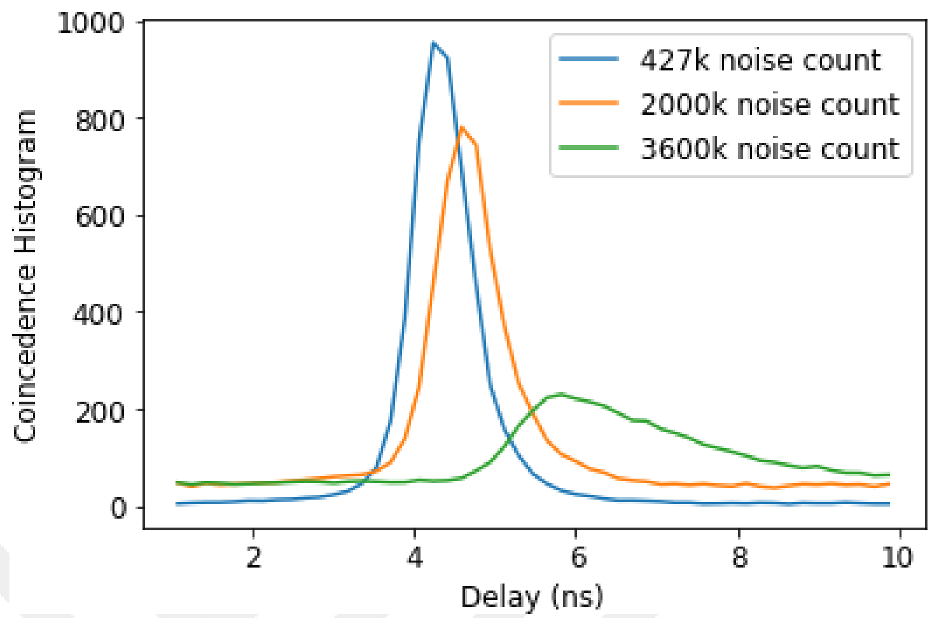

Figure 32: The detection shifts due to timing jittery of the detector under different noise levels

This observation is new to the literature and carries an important value, thus it might redefine the reliability and constraints of measurements in single-photon detection regimes. It is possible to increase the temperature of the detector's p-n junction and change the correlation characteristic without exceeding the threshold value by artificially making extra photon measurements for the detectors. In this way, it is possible to determine the detection information probabilistically, which detector when and in which reference system makes the measurement. This means that there is a possible security vulnerability. In order to eliminate this, the reverse bias applied to the avalanche photodiode must be controlled to compensate for the changes in avalanche current peak height due to the p-n junction temperature [42].

Different single-photon detectors (active quenched, passive quenched) with different APD circuitry are compared in that sense. The timing jitters of those different single-photon counting detectors (Excelitas, ID Quantique, S-Fifteen Instruments, and Qubitrium) in the laboratory are operated and observed in the range of 250-300 picoseconds. The Qubitrium detector with the expanded timing jitter, after the company replaced the comparator circuit element with its slower bandwidth counterpart, reached a 3.5 nanosecond timing jitter value. With this renewed timing jitter value, the timing jitter caused by the p-n junction temperature increase resulting from the high number of photons absorbed by the APD is negligible. Thus, the timing jitter problem depending on the photon detection count has been solved in our current setup. This solution has a disadvantage compared to the reverse-biased voltage solution presented above. That is, the coincidence window duration must be at least 7 nanoseconds. This limits the potential maximum amount of pairs that can be obtained per second. However, it does not pose a problem since more than 100 million entangled photon pairs are not used in practical quantum technology applications in the world, and its practical application is limited by other technological bottlenecks.

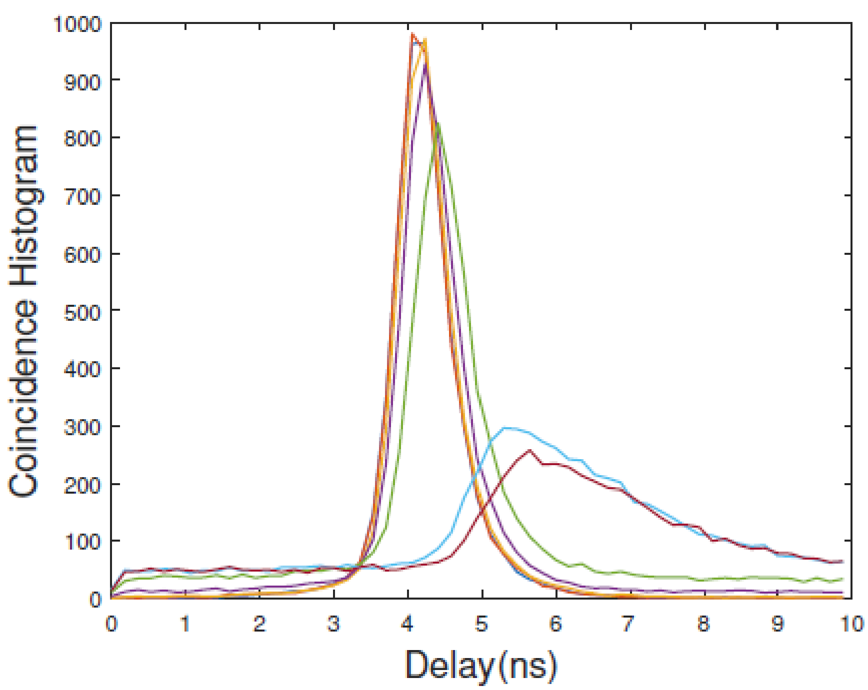

Figure 33: Cross-correlation spectrum of the object 0.6 m (1.2 m round-trip distance) away from the idler photons.

The scanning process leads to the accumulating of extra accidental coincidence unintentionally as we move along in the bin-width in a phase-insensitive detection scheme. The reason behind this is the resolution of the timestamp unit will be decreased when we scan the bin width. Those number of bins are considered for the delay case. If the delay of the detector is 10 (bin size) then we know that the new total resolution is the multiplication with the timestamp unit's resolution (81 ps for our case) calculated as 810 ps. With the detector contribution to the whole detection process now the timestamp unit will count the correlation as a coincidence when the photons arrive in 810 ps. Eliminating this problem we introduce a new detection method. This method is based on the calculation of the non-normalized second-order cross-correlation function (CCF) of the pairs. A cross-correlation function of the signal and reference photons is obtained with various external noise conditions as shown in Figure 33. The width of the CCF function is determined by the timing jitter of the detectors and the coherence time of the correlated source [43]. The timing jitter of our detectors is 250 ps and 300 ps for signal and reference arms, respectively. Since the timing jitter is high compared to the coherence time of the source, the effect of photon pairs' coherence time in determining the CCF spectrum can be ignored. Therefore, the observed cross-correlation spectrum width is $\approx 550ps$. The position of the object in the delay axis of the CCF measurement (see Figure 33) can be used to infer the displacement of the object with reference to the reference photons. The magnitude of the CCF spectrum (CCF spectrum height) is an indication of the strength of correlation. We calculated the value of coincidence in CCF measurement and row coincidence value and found that a reduction of accidental coincidence of 702 (exact values are 4935 and 5637 when CCF measurement is applied and not applied, respectively) when the CCF measurement is applied. This advantage is more appreciated when the object is placed at a farther distance.

CHAPTER IV

CONCLUSION

This thesis involves two very popular quantum technology applications, quantum random number generation and quantum target detection system. Based on the fundamental understanding of photon statistics, both applications' quantum properties are enhanced. The novel approaches in both sections managed to increase the detection efficiency of the applications by lowering the classical noise and detector imperfections in the system. In the first chapter I introduced a technique for a quantum random number generator based on scattering. The method is used to perform faster post-processing with an optical bit extraction. Many constraints are encountered in the physical production of random numbers; the bandwidth and the dead time of the detector, classical noise, digitizing of the analog data and the post-processing are the big obstacles ahead that slow down the random number generation. Our method of using a scattering source proposes a solution for this problem by giving the physical setup the ability to produce data in a faster way. The photon statistics of thermal and coherent light sources and their scatterings are compared. The sources with super-Poissonian distribution are shown to have better randomness even without the bit extraction process. Moreover, the autocorrelation function of the scattering signal gets around zero in advance compared to the not scattered signal. The optimal sampling rate is obtained when the undersampling is set as the two times of the lag point of the scattering signals min. autocorrelation. The raw signal is digitized and processed optically in order to make an even distribution of bits. The explained research in the first chapter resulted in a published journal paper [44].

In the second chapter, I introduced a phase-sensitive illumination system based on parametric down-conversion use twin pairs of position-correlated signal and idler photons. One beam illuminates an object while the image information is recovered from a second beam that has never interacted with the object. As in a regular quantum target detection system, a transmissive object is placed in the idler beam and the transmitted photons are measured using a single-element, heralding detector. A special quantum target detection and ranging setup that uses a correlated photon source for illumination is designed. In this study, we show that using the quantum polarization correlation property of the source in addition to the temporal one provides an advantage in terms of SNR. The strength of the correlation is justified with the injecting additional background noise from a thermal source. This is done for two different types of correlated schemes: one without polarization correlation (using the temporal correlation available only in the SPDC source) and one with additional polarization correlation. To our knowledge, this is the first study of analyzing the effect of polarization correlation on the SNR in detection systems. In our method, temporal and polarization correlated photon pairs obtained from the spontaneous parametric down-conversion (SPDC) process are used as a quantum source. A comparative study of both systems reveals the advantage of using polarization correlation. An enhancement in SNR of 2.8 by using polarization correlation is observed in our experiment. In addition, we show visibility (contrast parameter) based signal extracting scheme that can be applied to normalize the detector-imposed limitations. This visibility-based method is useful not only in quantum metrology but also in general quantum-based detection schemes where detector limitations have a detrimental effect. Most importantly the detector time jitter effect and the problems caused by the limitation of photon detectors are showed introduced a new way to estimate noise in his system and accounts for the effects of detector saturation. As a result of the research in the second chapter, a preprint is published [45].

EXPERIMENT PHOTOS

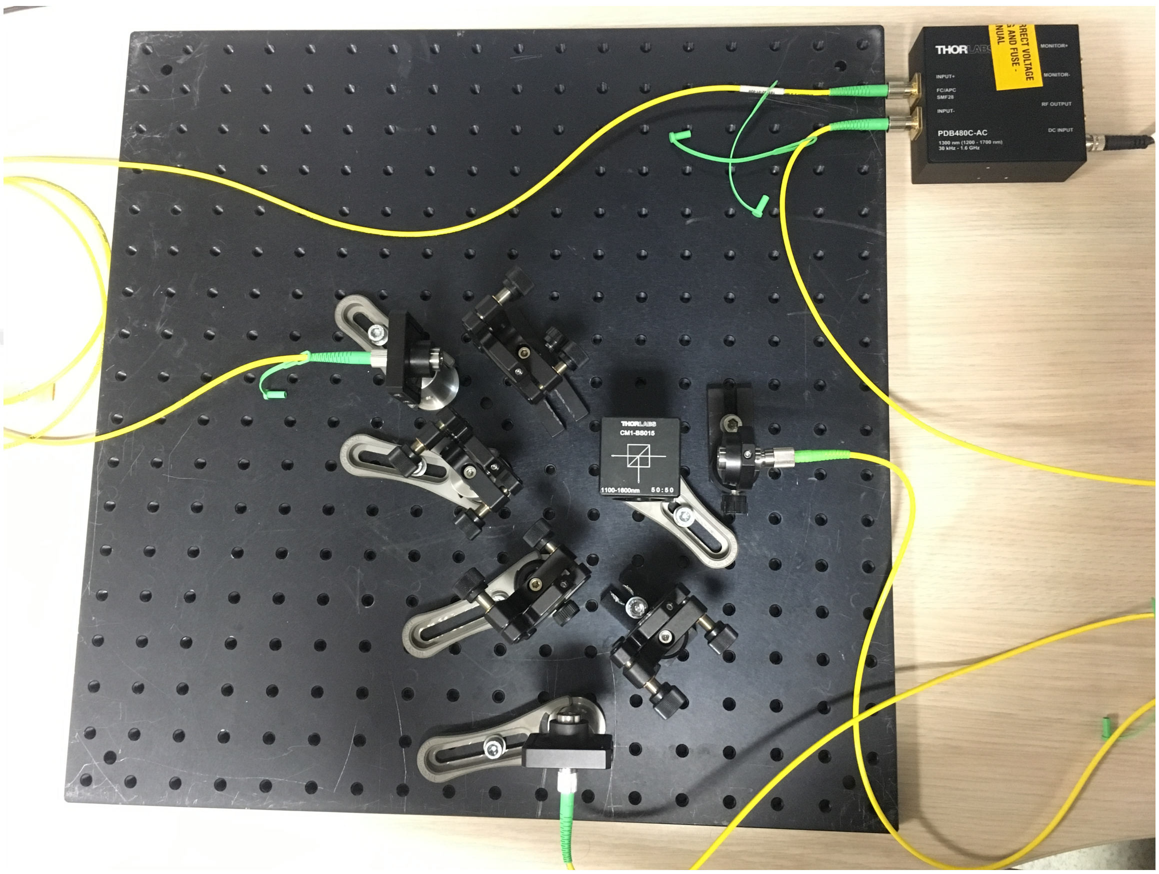

Figure 34: The experimental balanced homodyne detection setup with the emphasis on vacuum state field in the environment.

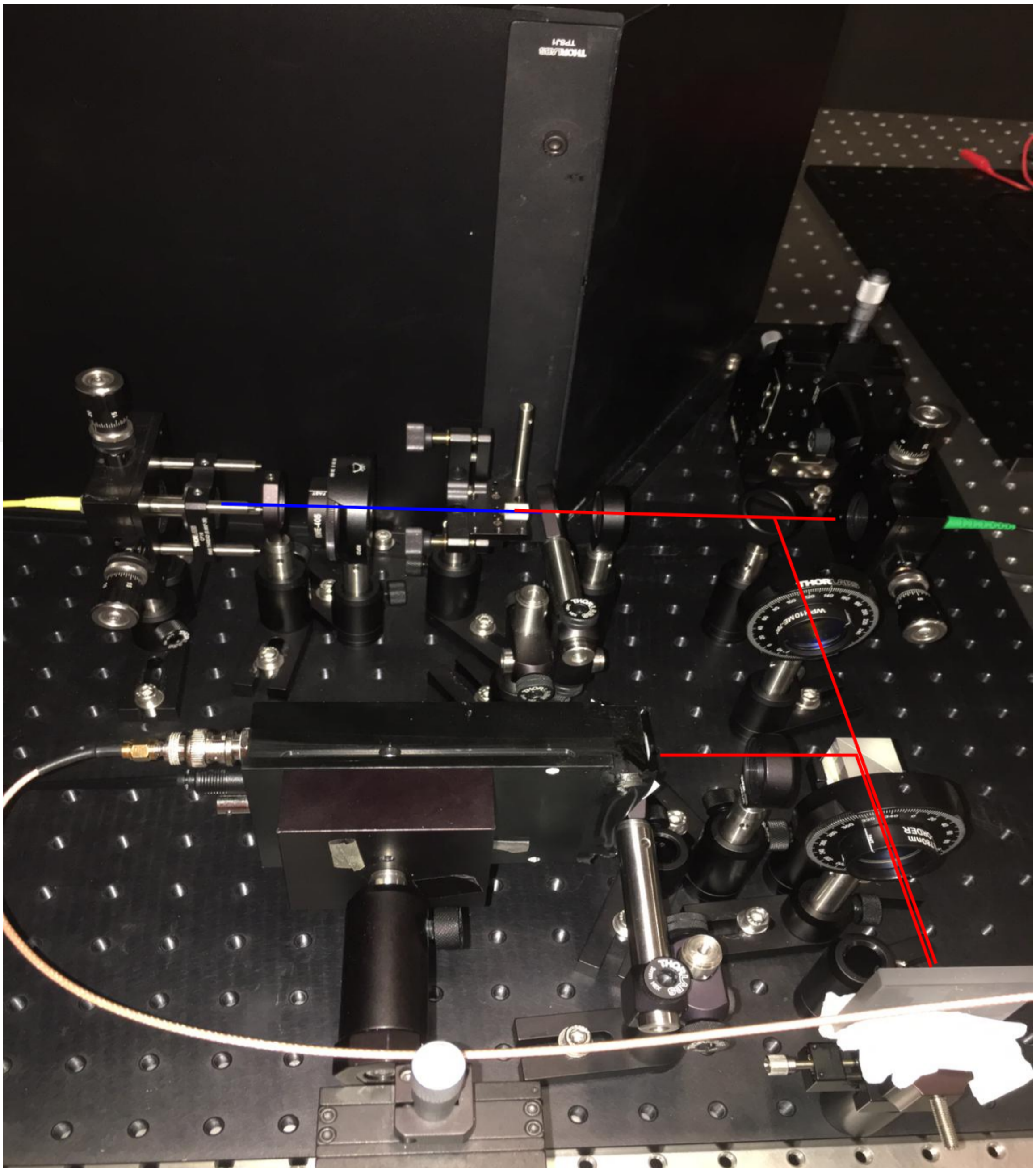

Figure 35: Shows the experimental setup of the quantum imaging scheme.

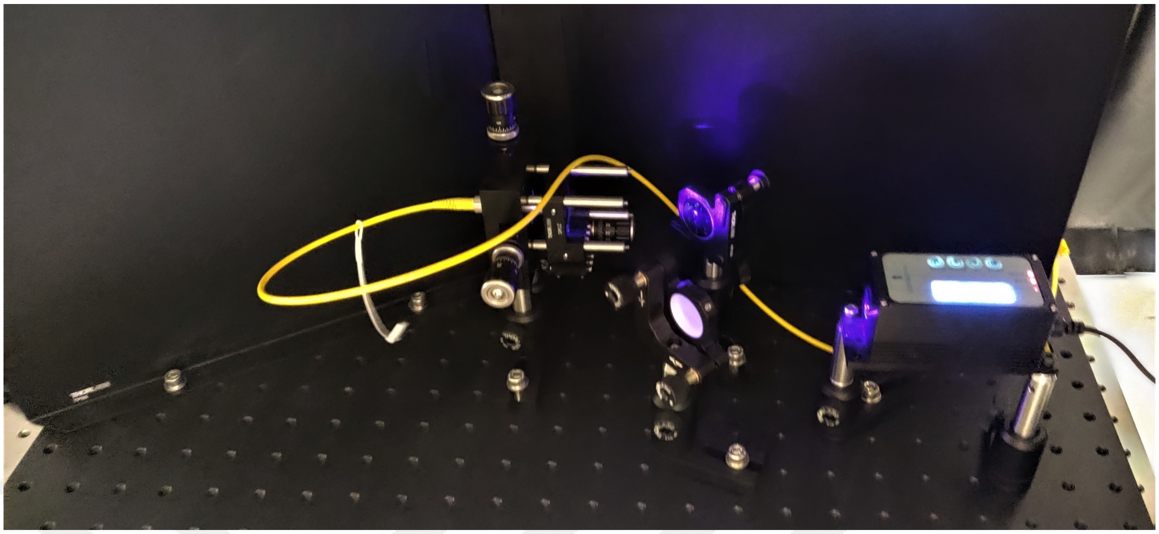

Figure 36: The image of the pump source's fiber coupling to SMF process.

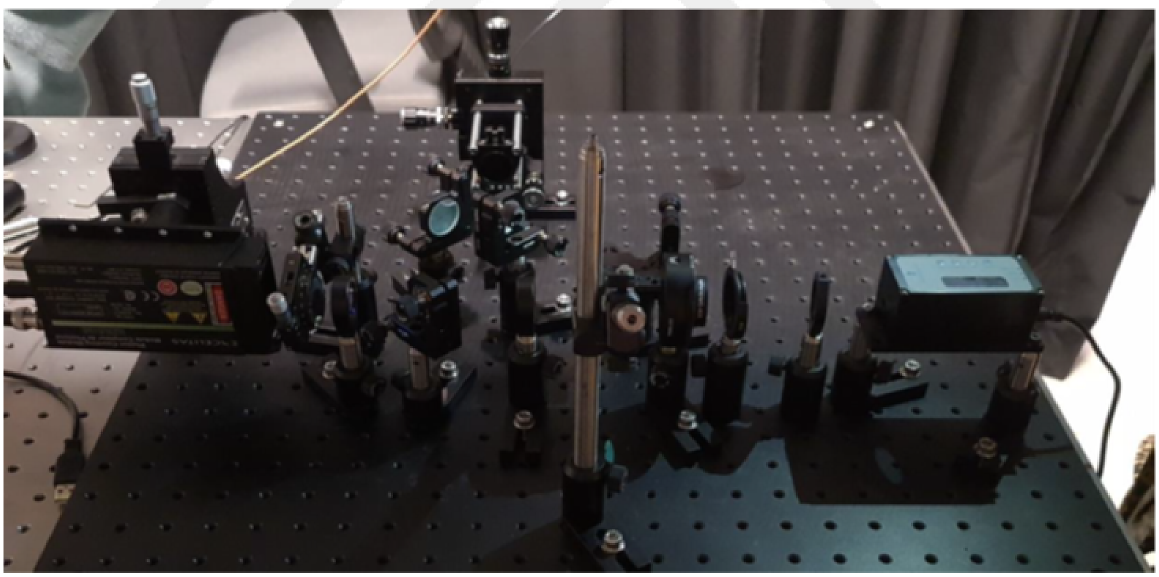

Figure 37: SPDC photon source setup on anodized aluminum breadboard.

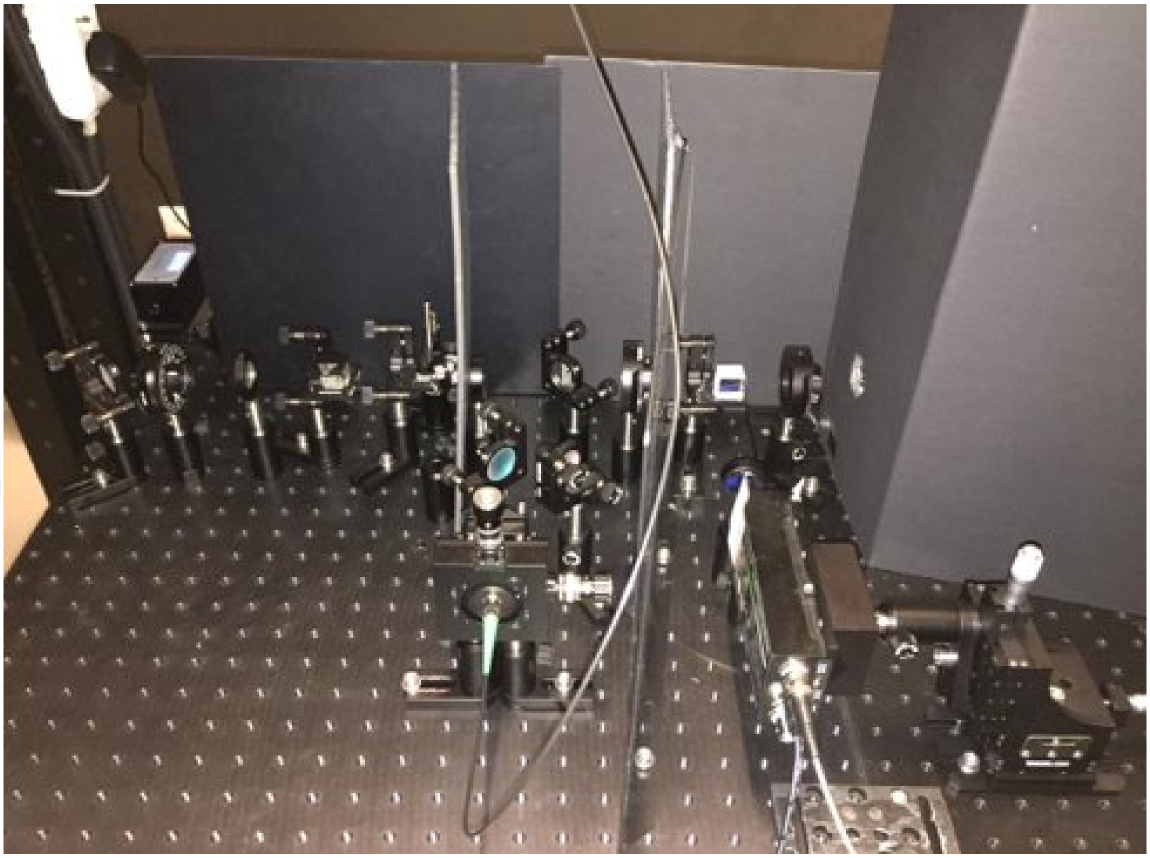

Figure 38: Experimental setup for noise-tolerant SPDC.

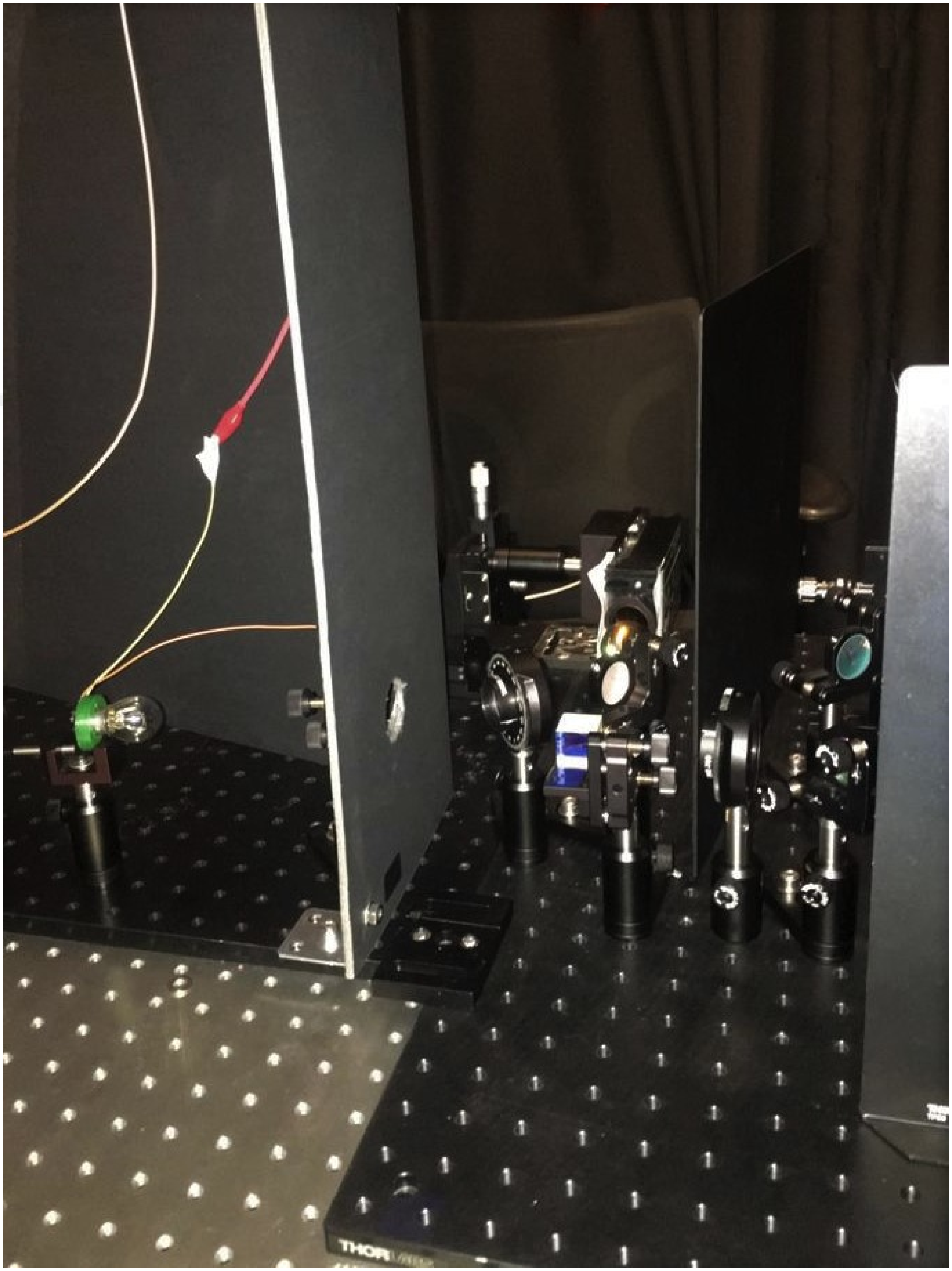

Figure 39: A closer look to noise injected arm of the setup and the light bulb used as the background noise source in the photons.

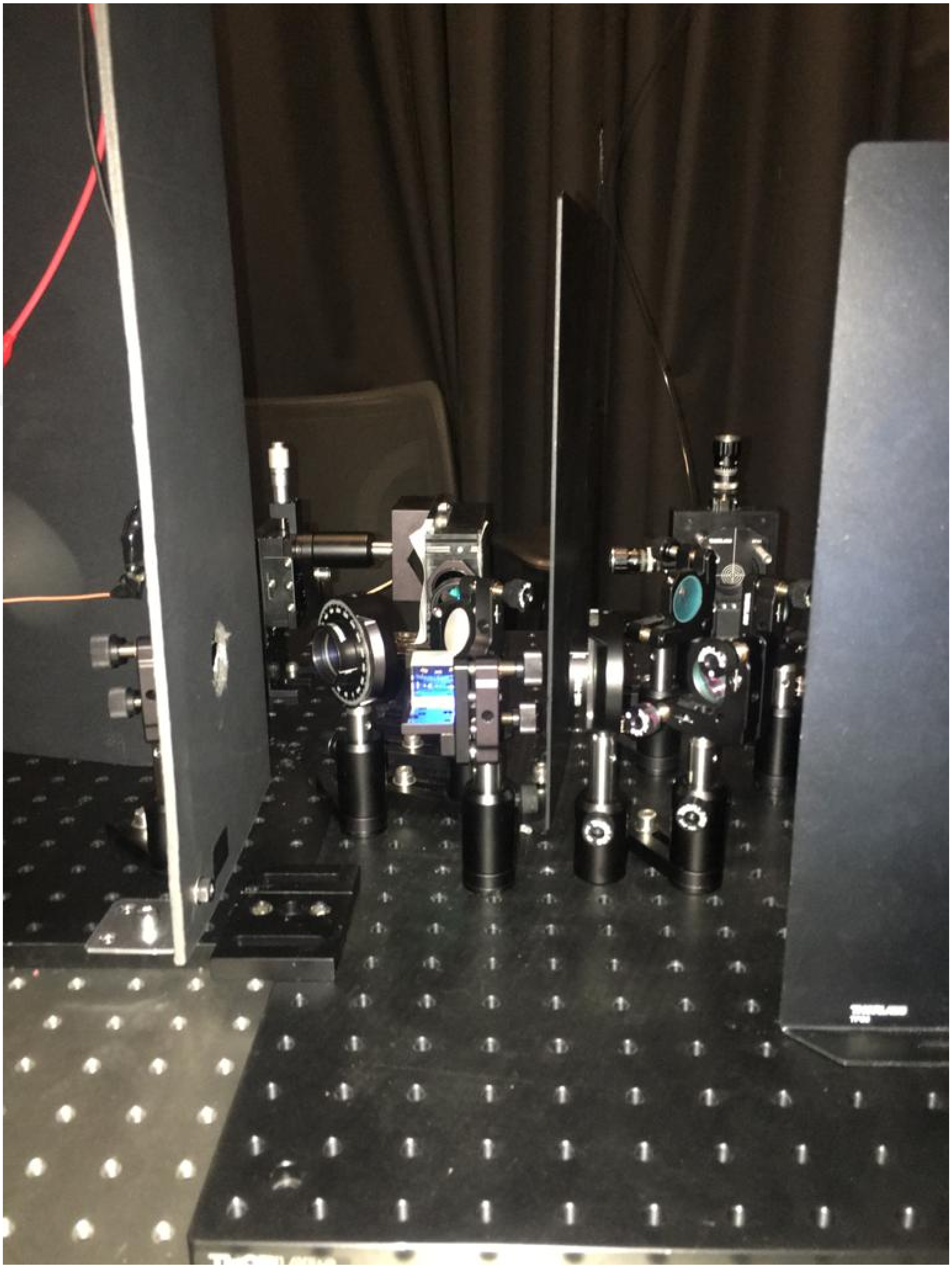

Figure 40: Another shot angle of the TPC setup.

Bibliography

[1] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Reviews of Modern Physics*, vol. 89, no. 1, p. 015004, 2017.

[2] J S Lundeen, "Spontaneous parametric downconversion," 2005. [Online; accessed 12-12-2021].

[3] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[4] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, postprocessing free, quantum random number generator," *applied physics letters*, vol. 93, no. 3, p. 031109, 2008.

[5] N. Metropolis and S. Ulam, "The monte carlo method," *Journal of the American statistical association*, vol. 44, no. 247, pp. 335–341, 1949.

[6] F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. Matthews, "A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers," *Quantum Science and Technology*, vol. 3, no. 2, p. 025003, 2018.

[7] Y.-Q. Nie, H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan, "Practical and fast quantum random number generation based on photon arrival time relative to external reference," *Applied Physics Letters*, vol. 104, no. 5, p. 051110, 2014.

[8] L. Oberreiter and I. Gerhardt, “Light on a beam splitter: More randomness with single photons,” *Laser & Photonics Reviews*, vol. 10, no. 1, pp. 108–115, 2016.

[9] Z. Zheng, Y. Zhang, W. Huang, S. Yu, and H. Guo, “6 gbps real-time optical quantum random number generator based on vacuum fluctuation,” *Review of Scientific Instruments*, vol. 90, no. 4, p. 043105, 2019.

[10] Y. Shi, B. Chng, and C. Kurtsiefer, “Random numbers from vacuum fluctuations,” *Applied Physics Letters*, vol. 109, no. 4, p. 041101, 2016.

[11] L. Huang and H. Zhou, “Integrated gbps quantum random number generator with real-time extraction based on homodyne detection,” *JOSA B*, vol. 36, no. 3, pp. B130–B136, 2019.

[12] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, “Scalable parallel physical random number generator based on a superluminescent led,” *Optics letters*, vol. 36, no. 6, pp. 1020–1022, 2011.

[13] C. C. Wang and G. W. Racette, “Measurement of parametric gain accompanying optical difference frequency generation,” *Applied Physics Letters*, vol. 6, no. 8, pp. 169–171, 1965.

[14] A. Aspect, J. Dalibard, and G. Roger, “Experimental test of bell’s inequalities using time-varying analyzers,” *Physical review letters*, vol. 49, no. 25, p. 1804, 1982.

[15] R. Ghosh and L. Mandel, “Observation of nonclassical effects in the interference of two photons,” *Physical Review Letters*, vol. 59, no. 17, p. 1903, 1987.

[16] Z. Ou and L. Mandel, “Violation of bell’s inequality and classical probability in a two-photon correlation experiment,” *Physical review letters*, vol. 61, no. 1, p. 50, 1988.

[17] J. C. Howell, R. S. Bennink, S. J. Bentley, and R. W. Boyd, "Realization of the einstein-podolsky-rosen paradox using momentum-and position-entangled photons from spontaneous parametric down conversion," *Physical Review Letters*, vol. 92, no. 21, p. 210403, 2004.

[18] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical review*, vol. 47, no. 10, p. 777, 1935.

[19] F. Devaux and E. Lantz, "Spatial and temporal properties of parametric fluorescence around degeneracy in a type i lbo crystal," *The European Physical Journal D*, vol. 8, no. 1, pp. 117–124, 2000.

[20] C. Couteau, "Spontaneous parametric down-conversion," *Contemporary Physics*, vol. 59, no. 3, pp. 291–304, 2018.

[21] J.-L. Blanchet, F. Devaux, L. Furfaro, and E. Lantz, "Measurement of sub-shot-noise correlations of spatial fluctuations in the photon-counting regime," *Physical review letters*, vol. 101, no. 23, p. 233604, 2008.

[22] M. Matsumoto and T. Nishimura, "Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator," *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, vol. 8, no. 1, pp. 3–30, 1998.

[23] W. Trappe, *Introduction to cryptography with coding theory.* Pearson Education India, 2006.

[24] P. Somlo, "Zener-diode noise generators," *Electronics Letters*, vol. 11, no. 14, p. 290, 1975.

[25] C. S. Petrie and J. A. Connelly, "A noise-based ic random number generator for applications in cryptography," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 47, no. 5, pp. 615–621, 2000.

[26] S. Yicheng, "A ultra-fast quantum random number generator," 2016.

[27] C. Henry, "Theory of the linewidth of semiconductor lasers," *IEEE Journal of Quantum Electronics*, vol. 18, no. 2, pp. 259–264, 1982.

[28] C. Henry, "Phase noise in semiconductor lasers," *Journal of Lightwave Technology*, vol. 4, no. 3, pp. 298–311, 1986.

[29] P. L'Ecuyer, "Random numbers for simulation," *Communications of the ACM*, vol. 33, no. 10, pp. 85–97, 1990.

[30] M. Fox, *Quantum optics: an introduction*, vol. 15. OUP Oxford, 2006.

[31] R. S. Aspden, *Heralded quantum imaging*. PhD thesis, University of Glasgow, 2015.

[32] L. Z. Jie and C. Kurtsiefer, "Characterisation of single photon avalanche detectors," *Undergraduate Final Year Project Thesis, National University of Singapore*, 2016.

[33] T. B. Pittman, Y. Shih, D. Strekalov, and A. V. Sergienko, "Optical imaging by means of two-photon quantum entanglement," *Physical Review A*, vol. 52, no. 5, p. R3429, 1995.

[34] P. Trojek, *Efficient generation of photonic entanglement and multiparty quantum communication*. PhD thesis, lmu, 2007.

[35] A. Gatti, E. Brambilla, M. Bache, and L. A. Lugiato, "Correlated imaging, quantum and classical," *Physical Review A*, vol. 70, no. 1, p. 013802, 2004.

[36] H. Kuniyil, S. Ozcimen, and K. Durak, "Tailoring the down conversion emission profile via direct imaging with a camera," *arXiv preprint arXiv:1909.04921*, 2019.

[37] E. Lopaeva, I. R. Berchera, I. P. Degiovanni, S. Olivares, G. Brida, and M. Genovese, "Experimental realization of quantum illumination," *Physical review letters*, vol. 110, no. 15, p. 153603, 2013.

[38] R. S. Aspden, N. R. Gemmell, P. A. Morris, D. S. Tasca, L. Mertens, M. G. Tanner, R. A. Kirkwood, A. Ruggeri, A. Tosi, R. W. Boyd, *et al.*, "Photon-sparse microscopy: visible light imaging using infrared illumination," *Optica*, vol. 2, no. 12, pp. 1049–1052, 2015.

[39] D. G. England, B. Balaji, and B. J. Sussman, "Quantum-enhanced standoff detection using correlated photon pairs," *Physical Review A*, vol. 99, no. 2, p. 023828, 2019.

[40] K. Durak, N. Jam, and C. Dindar, "Object tracking and identification by quantum radar," in *Quantum Technologies and Quantum Information Science V*, vol. 11167, p. 111670N, International Society for Optics and Photonics, 2019.

[41] M. Förtsch, G. Schunk, J. U. Fürst, D. Strekalov, T. Gerrits, M. J. Stevens, F. Sedlmeir, H. G. Schwefel, S. W. Nam, G. Leuchs, *et al.*, "Highly efficient generation of single-mode photon pairs from a crystalline whispering-gallery-mode resonator source," *Physical Review A*, vol. 91, no. 2, p. 023812, 2015.

[42] R. G. Brown, K. D. Ridley, and J. G. Rarity, "Characterization of silicon avalanche photodiodes for photon correlation measurements. 1: Passive quenching," *Applied optics*, vol. 25, no. 22, pp. 4122–4126, 1986.

[43] X. Guo, C.-l. Zou, C. Schuck, H. Jung, R. Cheng, and H. X. Tang, "Parametric down-conversion photon-pair source on a nanophotonic chip," *Light: Science & Applications*, vol. 6, no. 5, pp. e16249–e16249, 2017.

[44] A. Dandasi, H. Ozel, O. Hasekioglu, and K. Durak, "Effect of photon statistics on vacuum fluctuations based qrng," *Journal of Optics*, vol. 23, no. 6, p. 065201, 2021.

[45] H. Kuniyil, H. Ozel, H. Yılmaz, and K. Durak, "Noise-tolerant object ranging with a time-and polarization-correlated photon pair source," *arXiv preprint arXiv:2111.04062*, 2021.

VITA

Helin Özel is a member of Dr. Durak's Quantum Optics Laboratory (QOptics) team since 2018. She has received her bachelor's degree from the Electrical and Electronics Engineering Department at Ozyegin University in 2019. She started her Masters' program with Dr. Durak in the same year. She has been a student researcher in The Scientific and Technological Research Council of Turkey (TÜBİTAK) since 2018. Her research interest is on quantum optics and quantum technologies. Her thesis focuses on popular quantum applications based on quantum random number generation and quantum detection.