
Sectioning and multiplexing of spatial distribution of pair photons for quantum random number generation and quantum key distribution network

A thesis submitted in partial fulfilment of
the requirements for the degree of

Doctor of Philosophy

by

Ayan Kumar Nai

(Roll No. 23330006)

Under the supervision of

Prof. Goutam K. Samanta

Professor

Atomic, Molecular and Optical Physics Division

Physical Research Laboratory, Ahmedabad, India



DISCIPLINE OF PHYSICS

INDIAN INSTITUTE OF TECHNOLOGY GANDHINAGAR

2025

To

my family

Declaration

I declare that the content of this submission represents my ideas in my own words, and wherever ideas or words from others have been used, appropriate citations and references have been provided. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Signature

Name: Ayan Kumar Nai

(Roll No: 23330006)

Date: 18/12/2025

CERTIFICATE

It is certified that the work contained in the thesis titled “**Sectioning and multiplexing of spatial distribution of pair photons for quantum random number generation and quantum key distribution network**” by Mr. Ayan Kumar Nai (Roll No. 23330006), has been carried out under my supervision and this work has not been submitted elsewhere for a degree. I have read this dissertation and it is, in my opinion, totally suitable in breadth and quality as a dissertation for the degree of Doctor of Philosophy.

Prof. Goutam K. Samanta

Professor

Atomic, Molecular and Optical Physics Division,

Physical Research Laboratory,

Ahmedabad, India.

(Thesis Supervisor)

Date: 18/12/2025

Acknowledgments

Finally, I am here — at the last stage before the finish line of a long, challenging, and rewarding journey. It feels as though I have completed the first step toward my dream of becoming a researcher and earning the highest academic degree. Writing this section feels like looking back at a roller coaster ride that shaped not only my research skills but also the person I am today. A Ph.D. is never truly a solitary pursuit, and at every stage, I was accompanied, supported, and inspired by people who left an indelible mark on my life. This is my chance to thank each of them.

My interest in Quantum Mechanics and its implementation was first piqued when I did my undergraduate reading project on the “EPR Paradox and Entanglement in Quantum Mechanics,”. For the continuation of the same, I initially started my Ph.D. journey at the Indian Institute of Technology Madras (IIT M) after my M.Sc. from the Indian Institute of Technology Kanpur (IIT K). But my journey was not on the right track there at IIT M, and I resigned from the PhD program in my 3rd year. I stopped that time and again looked for a second chance to achieve my dream. I got the second opportunity from Prof. Goutam Kumar Samanta, my savior at that time, and supervisor for lifetime. I am profoundly grateful to him for his patient guidance, insightful wisdom, and unwavering support, which have helped me navigate the complex landscape of research. From our very first meeting, I sensed that working under his mentorship would be a transformative experience, and I was right. His open-minded approach, constructive criticism, insightful feedback, and willingness to give me space to explore my ideas helped me grow into an independent researcher. He was not just my academic guide but also a source of moral support, always reminding me to see challenges as opportunities.

My sincere thanks go to my Doctoral Scientific Committee members, Dr. Shashi Prabhakar, Dr. T A Rajesh, Dr. Lokesh Kumar Dewangan, and Dr. Naveen Chauhan for their thoughtful feedback, insightful questions, and constant encouragement during seminars and reviews. Our probing discussions pushed me to refine my understanding and present my work with clarity. I am also thankful to all the faculty members of PRL, the faculty who taught me during coursework — your collective wisdom and generosity in sharing knowledge played a huge role in shaping my academic foundation.

I am indebted to the entire PRL family — directors, deans, administrative staff, library team, computing support, accounts, purchase, canteen staff, transport, and hostel teams — for ensuring that everything from research facilities to day-to-day life ran smoothly. My appreciation also extends to IIT Gandhinagar’s academic office for their assistance during the registration process and for facilitating the Ph.D. degree. Furthermore, I gratefully acknowledge funding support for Chanakya - PhD fellowship from the National Mission on Interdisciplinary Cyber-Physical Systems of the Department of Science and Technology, Govt. of India, through the I-HUB Quantum Technology Foundation.

To my lab and group members — thank you for making the research environment one of collaboration, laughter, and mutual growth. Whether it was troubleshooting an experiment, running simulations, proofreading, or just sharing coffee during tea time at PRL, they made the tough days bearable and the good days even better. I am especially grateful to Vimlesh Ji for his constant support, patience, and the countless technical and non-technical guidance in different aspects. In the lab, He is the person who helped me to learn the ‘ABCD’ of experimental alignment, and he is also the person I turn to whenever I face any challenge at the opto-mechanical design and

optomechanics level. Next, Sandeep da has continually made offerings of thoughtful advice in both academic and personal matters during my first year and later on, which has made my understanding better in my field. Anirban da, like an encouraging elder brother, motivates me with his dedication to academia, and his cooking skills make our group gatherings memorable. Soumya da and Chahat have been a constant source of guidance as my immediate senior, from academia to personal matters. I am also grateful to my batchmate cum labmate Milan, Sanjan, our group study and preparation for the coursework made my first year easy. I am also thankful to Rutuj, Swagata, Bharath, Soumya, Niladri, Amritash, Rupak, and Harsha for always stepping in whenever I needed help. My gratitude also extends to Vardaan Vaiaa, Tanya Di, Jayanth, Pooja Di, JK Vaiaa, and Rachita for their constant encouragement and support. You all reminded me that life outside the lab is just as important, and that joy is a critical ingredient in scientific productivity.

Beyond PRL, my heartfelt thanks to my college, university, and school friends who kept in touch, encouraged me from afar, and believed in my potential. Each message, call, or visit reminded me of the roots I carry with me. To my well-wishers across institutions, your generosity with your time, ideas, and expertise enriched my work in ways I cannot fully quantify.

Last but not least, my deepest and eternal gratitude goes to my parents, whose love, faith, and sacrifices are the foundation on which every achievement of mine rests. They believed in my potential and did their best to help me reach my heights, and their unwavering encouragement gave me the courage to keep moving forward. To my little sister, my kids, and my whole family, thank them for being my cheerleaders, motivators, and safe place to land whenever I needed it. And above all, I thank God for the blessings, strength, and resilience that made this journey possible.

Abstract

Random numbers have become an essential component of many aspects of modern life, with applications ranging from fundamental tests of physics and scientific simulations to numerical analysis, decision-making processes, and cryptography. While numerous random number generation schemes based on mathematical algorithms and classical processes have been developed, quantum random number generation (QRNG) based on quantum mechanical processes has evolved to provide fundamentally secure randomness. Despite the robust and reliable source of true randomness, the QRNGs face the common limitation of low bit rates, typically in the kilobits-per-second (kbps) range. Moreover, these approaches often require additional optical components, such as high-quality, unbiased beam splitters, whose precise fabrication presents significant practical challenges.

On the other hand, the distribution of random bit strings between two users is commonly achieved through quantum key distribution (QKD). The QKD guarantees security even against attempts by an adversary to intercept the key and remains unaffected by advances in computational power, including those offered by quantum computers. A further increase in the number of users in the QKD network can result in seamless, secure communication among a large number of users, making it an immediate requirement to establish a global quantum network. However, the common limitation in QKD between two or multiple users has turned out to be the overall key rate, primarily due to the low photon pair rate, mainly caused by the lower brightness of the quantum source and the use of beam splitters.

To address these issues, in the current thesis, we devised novel experimental schemes based on spatial sectioning and multiplexing of the spatial distribution of pair-photons.

The spontaneous parametric down-conversion (SPDC), the main resource for the generation of pair photons and entangled photons, has been used to demonstrate the beam-splitter-free QRNG, device-independent randomness certification, spatial randomness-based BBM92 QKD, multi-user quantum networks, and entanglement engineering for robust quantum communication.

We begin with the complete theoretical framework of random number generation and random number distribution, including the SPDC process, which encompasses phase-matching, photon-pair generation optimization, and entanglement properties. Building on this foundation, we performed a systematic characterization of heralded single-photon and entangled photon sources in both single-pass and polarization Sagnac configurations. By varying the coincidence window, spectral bandwidth, spatial mode collection, and pump power, we quantified their effects on key metrics: second-order correlation coefficient at zero time delay ($g^{(2)}(0)$), visibility in Hong–Ou–Mandel (HOM) interferometer, Bell parameter, and entanglement visibility. The results established the clear design guidelines for all the experiments performed in the thesis.

Harnessing the strong temporal and spatial correlations intrinsic to SPDC bi-photons, we proposed and experimentally realized a beam-splitter-free QRNG scheme. By sectioning the SPDC annular emission ring and recording time-correlated detection events between diametrically opposite points, we generated multi-bit random sequences at high rates without reliance on additional probabilistic optical elements. Using a 20-mm PPKTP crystal, the scheme achieves 3 Mbps after post-processing, with a minimum entropy exceeding 95%, passing the NIST 800-22 and TestU01 statistical tests.

Extending this concept, we developed a scalable, device-independent QRNG (DI-QRNG) with live Bell test certification. By dividing the SPDC ring from a polarization

Sagnac source into six opposite sections, we simultaneously formed three independent entangled photon sources from a single crystal and pump beam. Two sources generated randomness, while the third is used to continuously measure the CHSH Bell parameter ($S > 2$), providing real-time trust verification without reducing the random number generation rate. The DI-QRNG achieves 1.8 Mbps with a minimum entropy of above 97%, demonstrating practical scalability and robustness.

We further enhanced the QKD efficiency of the BBM92 protocol using the intrinsic spatial randomness, replacing the conventional beam-splitter-based basis selection with probabilistic mapping from SPDC ring sections to measurement bases. Such selection eliminated the encoding bias from imperfect lossy beam splitters, improving the key rate 6.4 times with reduced quantum bit error rate (QBER) compared to traditional methods using a Bell state.

We also show that one need not worry about using the Bell state from the source end to establish QKD between two parties. Instead, one can use a Bell-like state at the source and revive the Bell state at the receiver end to establish QKD with low QBER. For concept demonstration, we have demonstrated geometric phase (GP) or geometric equivalent phase effects on QBER both analytically and experimentally. This additional phase imprinted via waveplate rotation in the pump beam transforms Bell states into Bell-like states with QBER up to 25%. However, the introduction of the phase compensation scheme at the receiver end restores Bell-state fidelity above 95% and reduces QBER below the 11% security threshold for entanglement-based QKD. This method also compensates for phase drifts arising from imperfect generation or channel transmission.

Finally, leveraging the same spatial sectioning and multiplexing methodology, we presented a fully connected, 12-channel QKD network among six users. This is imple-

mented using only three spatially separated entangled photon sources derived from a single SPDC source at 810 nm. The network achieved average coincidence rates of 30 kHz per user pair, entanglement visibility exceeding 80%, and sifted key rates of 407 kbps across all pairs, utilizing only passive optical components. The architecture is inherently scalable to larger networks and adaptable to free-space and satellite-based links, offering a practical route toward global quantum communication infrastructure.

Through the integration of source optimization, spatial sectioning, and multiplexing, device-independent certification, network implementation, protocol innovation, and phase-error compensation, this thesis presents a comprehensive experimental toolkit for secure, scalable, and high-performance quantum technology applications. Prospective extensions include simultaneous, loophole-free, certified QRNG and global-scale hybrid free-space quantum networks combining wavelength division multiplexing with our methodology.

Keywords: QRNG, heralded single-photon source, second order-correlation, HOM interferometry, entangled photon source, Bell's parameter, entropy, Toeplitz, NIST, auto-correlation, network, communication, visibility, fidelity, spatial-randomness, QKD, density matrix, QBER, sifted key rate, Geometric phase.

Abbreviations

BS	Beam Splitter
PBS	Polarizing Beam Splitter
HWP	Half-Wave Plate
QWP	Quarter-Wave Plate
DM	D-Shaped Mirror
PPKTP	Periodically Poled Potassium Titanyl Phosphate
SPDC	Spontaneous Parametric Down Conversion
BPM	Birefringent Phase Matching
QPM	Quasi-Phase Matching
HSPS	Heralded Single Photon Source
EPS	Entangled Photon Source
EMCCD	Electron Multiplying Charge-Coupled Device
FC	Fiber Coupler
SMF	Single Mode Fiber
MMF	Multi Mode Fiber
SPCM	Single Photon Counting Module
TDC	Time to Digital Converter
QRNG	Quantum Random Number Generator
PRNG	Pseudo Random Number Generator
TRNG	True Random Number Generator
QKD	Quantum Key Distribution
QBER	Quantum Bit Error Rate

Contents

Acknowledgements	i
Abstract	v
Abbreviations	ix
Contents	xi
List of Figures	xvii
List of Tables	xxix
1 Introduction	1
1.1 Objective of the Thesis	4
1.2 Overview of the Thesis	6
2 Fundamentals Principles	9

2.1	Random number generator	9
2.1.1	Randomness	10
2.1.2	Random numbers and its properties	10
2.1.3	Different methods of random number generation	11
2.1.4	Block description of physical random number generator	12
2.2	Random number (key) distribution	13
2.2.1	Cryptography architecture	14
2.2.2	Quantum key distribution network	17
2.3	Spontaneous parametric down-conversion process	19
2.3.1	Quantum mechanical description	20
2.3.2	Phase matching	27
2.3.3	Bi-photon generation efficiency	36
3	Optimization of Sources Brightness and Quantumness	41
3.1	Introduction	42
3.2	Background	45
3.2.1	Purity parameter $g^{(2)}(0)$ of a HSPS	45
3.2.2	Indistinguishability parameter V_{HOM} of a HSPS	46

3.2.3	Bell parameter S of an entangled photon source	48
3.3	Experiment	51
3.4	Results and discussion	55
3.5	Conclusion	67
4	Beamsplitter-free Quantum Random Number Generator using Heralded Single-Photons	69
4.1	Introduction	70
4.2	Experiment	72
4.3	Results and discussions	75
4.4	Conclusions	85
5	Device-Independent QRNG with Live Bell-Test Certification	87
5.1	Introduction	88
5.2	Experiment	91
5.3	Results and discussions	94
5.4	Conclusions	106
6	Spatial-Randomness-Based Quantum Key Distribution	109
6.1	Introduction	110

6.2	Experiment	112
6.3	Results and discussions	117
6.4	Conclusions	124
7	Bell State Revival using Geometric Phase for QKD Application	127
7.1	Introduction	128
7.2	Theory	131
7.3	Experiment	134
7.4	Results and discussions	138
7.5	Conclusions	141
8	Multi-User Quantum Communication Network	143
8.1	Introduction	144
8.2	Experiment	147
8.3	Results and discussions	150
8.4	Materials and Methods	157
8.4.1	Polarization entangled photon source	157
8.4.2	Spatial division and multiplexing	159
8.4.3	Projection and detection for each user	160

8.4.4	Estimation of secure key rate	160
8.4.5	Scaling of the network	161
8.5	Conclusion	162
9	Conclusions and Future Scope	165
9.1	Conclusion	165
9.2	Future Scope	167
	List of publications	169
	Bibliography	171

List of Figures

1.1	Schematic overview of the thesis structure: Spatial profile division and multiplexing, which supports a range of quantum communication applications.	6
2.1	Schematic block representation of a conventional physical random number generator.	12
2.2	Illustration of a generic RNG from an honest source (a) and from a dishonest source (b).	13
2.3	Art of cryptography with a preshared key between Alice and Bob. . .	15
2.4	(a) The pump field along the z-axis generates two down-converted field signals and an idler. (b) and (c) respectively energy and momentum conservation diagram of a SPDC process.	20

2.5	Illustrates birefringence in a nonlinear crystal. The light orange plane contains the wave vector and the optic axis. Ordinary ray (o-ray) polarization stays perpendicular to this plane, while the polarization of the extraordinary ray (e-ray) changes its orientation angle (θ), relative to the optic axis. This causes the e-ray to exhibit an angle-dependent refractive index.	29
2.6	(a) Geometrical representation of the phase-matching condition, achieved at the intersection of the k-surfaces of the down-converted photons. In Type-I SPDC, this intersection corresponds to the overlap of two circles, which in three-dimensional space form two concentric cones. (b) In this process, the down-converted photons hold similar polarizations, but different from the pump photon's polarization. Their propagation directions form two concentric cones.	32
2.7	(a) The geometrical interpretation of the phase-matching condition in the Type-II case, where the k-surfaces intersection occurs between a circle and an ellipse, resulting in the formation of tilted cones. (b) The down-converted photons possess orthogonal polarizations; they are on the surface of two symmetrically tilted cones relative to the pump direction.	33
2.8	Pump, signal, and idler photon momentum vectors and their components. θ_s^E and θ_i^E are the emission angles of the signal and idler photons, respectively.	35
2.9	Numerically obtained SPDC ring spatial profile.	36

3.1	Schematic of HBT-like setup for a heralded single-photon source in which the corresponding idler photons emerge after passing through the beam splitter, follow any of the two possible paths leading to zero coincidence counts between detectors D1, D2, and D3.	45
3.2	An HBT-like setup determines the second-order correlation function for a heralded single-photon source. Our TDC itself acts as an electronic delay generator that introduces a delay in one signal photon path with respect to the other two paths in steps of 0.5 ns.	52
3.3	The variation of second-order correlation function with delay for different sets of coincidence windows at a pump power of 1 mW.	56
3.4	The variation of $g^2(0)$ with pump power at three different coincidence window.	56
3.5	The $g^2(\tau)$ plots for three different filters used one after the other within the detection assembly.	57
3.6	The variation of $g^2(0)$ with pump power (set by single count levels) using three different filters at the detection assembly.	58
3.7	The variation of $g^2(0)$ with pump power for different fibers used one after the other.	58
3.8	The variation of the coincidence rate with the temporal delay between signal and idler photons, which is examined for three coincidence window settings at a pump power of 1 mW.	59

3.9	The variation of HOM visibility with pump power (set by single count levels) for three different coincident windows. The indistinguishable nature of the SPDC-generated biphoton photons degrades with increasing power due to multiphoton events.	60
3.10	The variation of HOM visibility with pump power (set by single count levels) using three different filters at the detection assembly.	61
3.11	The coincidence count rate vs signal and idler photon time delay plots for three different filters used one after the other within the detection assembly.	61
3.12	The variation of HOM visibility with pump power for different fibers used one after the other.	63
3.13	The variation of HOM visibility with $g^2(0)$. Solid lines are the fitted lines.	63
3.14	The variation of entanglement visibility with pump power (set by single count levels) for three different coincident windows and $g^2(0)$ variation at $CW = 1$ ns.	64
3.15	The variation of $g^2(0)$ with pump power in single pass configuration and Sagnac configuration.	65
3.16	Entanglement visibility vs $g^2(0)$ plot. The solid line is the fitted line.	66
3.17	The entanglement visibility plot in H, V, D, and A bases for (a) 10 nm filter, (b) 3.2 nm filter.	67

4.1	The schematic representation of (a) the concept and (b) the experimental setup of the QRNG source. Laser: 405 nm, cw diode laser, $\lambda/2$: Half wave plate, L1-4: plano-convex lenses of different focal lengths, PPKTP: 20 mm long PPKTP crystal of single grating period in temperature oven, IF: Interference filter, PM: Prism shaped gold coated mirror, DM1-2: D-shaped mirrors, U1-2 and D1-2: Upper and lower sections of the SPDC ring, SM: Single-mode fiber, SPCM1-4: single photon counting modules, TDC: Time-to-digital converter, PC: Computer.	74
4.2	(a) HOM visibility (indistinguishability), and $g^{(2)}(0)$ (purity) is evaluated under varying pump powers. (b) Dependence of HOM visibility on change of $g^{(2)}(0)$ with pump power as shown in (a).	76
4.3	Probability distribution of 0's, 1's, and 0 & 1 in the raw bit sequence collected at pump powers.	78
4.4	The variation of the minimum entropy, $H_{\infty}(X)$ (black dots), and post-processed QRNG bit rate (red dots) as a function of pump power and $g^{(2)}(0)$. The black and red lines are linear fit to the experimental data points.	80
4.5	Final P-values of 15 tests under NIST statistical suit for the Toeplitz post-processed bits recorded for a pump power of 17 mW.	81
4.6	Variation of the magnitude of the positive and negative autocorrelation coefficients of the first 10 million bits of the raw bit sequence up to a delay of 100 bits. The raw bit sequence is recorded for the pump power of 17 mW.	83

5.1 The schematic representation of the experimental setup of the QRNG source. Laser: 405 nm, cw diode laser, $\lambda/2$: Half-wave-plate, L1: plano-convex lenses of focal length 150 mm, $D - \lambda/2$: Dual-half-wave-plate, PPKTP: 20-mm-long periodically-poled potassium titanyl phosphate crystal of single grating in the oven, IF: Interference filter, PM: Prism-shaped gold-coated mirror, DM1-4: D-shaped mirrors, U1-2, D1-2, and S1-2: Upper, lower and side sections of the SPDC ring, SM: Single-mode fiber, SPCM1-6: single photon counting modules, TDC: Time-to-digital converter, PC: Computer. Inset: Spatial distribution of entangled photon source, the architecture of raw bit assignment, and quantumness certification.	91
5.2 Characterization of the entangled photon sources. Variation of (a) Entanglement visibility and (b) Bell parameter (S) of the entangled photon source as a function of pump power and with coincidence window.	96
5.3 Characterization of the QRNG system. The variation of the minimum entropy, $H_{\infty}(X)$ (black dots), and post-processed QRNG bit rate (red dots), as a function of pump power. The solid lines are linear fit to the experimental data.	99
5.4 Verification of randomness of the source through test suits. Final P-values of 15 tests under NIST statistical suit for the Toeplitz post-processed bits recorded at 95% and 61% visibility, respectively.	100

5.5 Characterization of raw bits of the QRNG. Variation of the magnitude of the positive and negative autocorrelation coefficients of the first 10 million bits of the raw bit sequence up to a delay of 100 bits. The raw bit sequences are recorded at two visibilities, 95% and 61%. .	102
5.6 Effect of output photon state on performance of QRNG. Variation of Bell's parameter and corresponding min-entropy of the raw bits of QRNG as a function of the weightage parameter, $ \alpha $. The lines are guide to the eye.	105
6.1 Experimental setup and network architecture. a , Conceptual representation of the present BBM92 scheme. b , Division of the spatial distribution of pair photons to form two identical entangled photon sources. c , Schematic of the experimental setup. Laser: 405 nm cw diode laser; HWP: half-wave plate; PBS: polarizing beam splitter; M: mirrors; DCM: dichroic mirror; L: plano-convex lenses; D-PBS: dual-wavelength (405 nm and 810 nm) PBS; D-HWP: dual-wavelength HWP; C: PPKTP crystal in an oven for photon-pair generation; PM: prism-shaped gold-coated mirror; DM: D-shaped mirrors; IF: 3 nm bandwidth interference filter; Coupler: collimator system for fiber coupling; SMF: single-mode fiber; SPCM: single-photon counting module; TDC: time-to-digital converter.	113

6.2	Characterization of the entangled photon sources. a, Quantum interference of spatially separated entangled photon sources measured in the horizontal (H, black dots), vertical (V, blue dots), diagonal (D, red dots), and anti-diagonal (A, green dots) polarization bases. Solid lines represent sinusoidal fits to the experimental data. Absolute values of d , real and e , imaginary parts of the reconstructed density matrix of the polarization-entangled Bell state $ \phi^+\rangle$	118
6.3	Performance metrics of the QKD schemes. (a) Sifted key rate and (b) quantum bit error rate (QBER) as functions of pump power for the current BBM92 scheme with Protocol #1 (red circles), Protocol #2 (blue circles)	121
7.1	The schematic representation of the experimental setup of the BBM92 key distribution. Laser: 405 nm, cw diode laser, $\lambda/2$: Half wave plate, L1: plano-convex lenses of focal length 150 mm, $D - \lambda/2$: Dual Half wave plate, PPKTP: 10 mm long PPKTP crystal of single grating period in temperature oven, Q: quarter wave plate, H: half wave-plate, GP: geometric phase, DM1-2: D-shaped mirrors, 1-8: single photon counting modules.	135
7.2	(a) Variation of QBER as a function of geometric phase. Real and imaginary parts of experimentally reconstructed density matrix (b) at HWP angle $\theta_H^p = 0$ (C) at HWP angle $\theta_H^p = 22.5$ (d) at combined HWP angles $\theta_H^p = 22.5$ & $\theta_H^B = -67.5$	137

7.3	(a) Dependence of the QBER on the crystal position within the Sagnac loop. Real and imaginary parts of experimentally reconstructed density matrix (b) at crystal position = 0 mm (C) at crystal position = 0.5 mm, and (d) at crystal position = 0.5 mm and $\theta_H^B = -67.5$	140
-----	---	-----

8.1 Conceptual scheme and experimental setup of the multi-user quantum network architecture.

On the left, we have illustrated the concept of using two layers of abstraction. The top layer shows the fully connected mesh of 12 channels connecting six users through quantum correlation. The bottom layer shows the physical representation of the network topology, with the implementation shown on the right. The topology of the quantum network is established through the central unit, which derives three entangled photon sources from a single source and distributes them between six users through multiplexing. The complete end-to-end implementation has three sections: central unit, free space channel, and users. Again, the central unit has two subsections: SPDC source and spatial division and multiplexing. The SPDC source is realized using a single-frequency continuous-wave diode laser at 405 nm, with output power controlled via a half-wave plate (HWP) and a polarization beam splitter (PBS), which pumps a temperature-stabilized periodically poled KTP (PPKTP) crystal placed in a polarization Sagnac interferometer. The interferometer consists of a dual-wavelength PBS and HWP (D-HWP) for 810 nm and 405 nm wavelengths. A plano-convex lens (focal length 150 mm) focuses the pump at the crystal center and collimates the photon pairs generated via spontaneous parametric down-conversion (SPDC). In the spatial division multiplexing section, the collimated SPDC emission ring, separated from the pump by a dichroic mirror (DCM), is divided into two halves using a prism mirror (PM), with each half further segmented into three subsections by D-shaped mirrors (DMs). Six diametrically opposite sections form three entangled photon sources, I, II, and III, with section pairs (1, 1'), (2, 2'), and (3, 3') as shown in the source division table. These subsections are multiplexed using three 50:50 beam splitters (BS), while mirrors (M) in the experiment direct the beams through the optical paths. The multiplexed outputs are transmit-

8.2 Characterization of spatially separated entangled photon sources derived from a single SPDC source.	
(a) Coincidence counts between different subsections, showing strong correlations between diametrically opposite sections carrying pair photons generated via the SPDC process.	
(b) Singles counts of different subsections, along with the coincidence visibility between diametrically opposite sections, 1 & 1', 2 & 2', and 3 & 3'.	
(c) Quantum interference of the spatially separated entangled photon sources (here, we used source II comprises of subsections 2 & 2') measured in the horizontal (H, black dots), vertical (V, red dots), diagonal (D, blue dots), and anti-diagonal (A, green dots) polarization bases.	
(d,e) Graphical representation of the absolute values of the real (d) and imaginary (e) parts of the reconstructed density matrix of the polarization-entangled Bell state $ \phi^-\rangle$.	152
 8.3 Performance characteristics of quantum links within the network.	
(a) Coincidence counts for each link connecting two users in the 12-link quantum network.	
(b) Measured quantum parameters for each link, including entanglement visibility, Bell parameter (S), and quantum state fidelity. The network supports both $ \phi^+\rangle$ and $ \phi^-\rangle$ Bell states, with each state distributed across six of the twelve links owing to the network's topology.	154

8.4	Performance parameters of the entangled-photon source for scalable quantum networking.	
	(a) Variation of the Bell parameter S and coincidence counts as a function of pump power for two spontaneous parametric down-conversion (SPDC) emission-ring diameters, corresponding to crystal temperatures of $T = 37.7^\circ\text{C}$ and $T = 39.7^\circ\text{C}$.	
	(b) Tabulated SPDC source characteristics at the two crystal temperatures, showing that an increased emission-ring diameter allows finer spatial sectioning. This capability supports network-topology scaling to accommodate more users while preserving the entanglement quality of the source.	156

List of Tables

2.1	Overview of SPDC types and corresponding crystal choices that allow BPM	30
4.1	Results of the NIST statistical tests	82
4.2	Results for the TestU01 statistical tests	83
4.3	Comparison of bit rate of QRNG based on coincidence detection. . . .	84
5.1	Comparison of the bit rate of QRNG based on coincidence detection. .	105
6.1	Comparison of QKD performance metrics between the beam-splitter-based conventional BBM92 protocol and the spatial-randomness-based implementation introduced here.	123

Chapter 1

Introduction

The nature of light has intrigued scientists and philosophers for centuries, giving rise to both classical and quantum interpretations of its behavior. While early optical theories by Newton and Huygens debated the particle and wave nature of light, a more complete understanding began to crystallize in the 19th century. A major milestone was achieved when James Clerk Maxwell elegantly unified electric and magnetic fields through a set of four partial differential equations—now famously known as Maxwell’s equations—which treated electric and magnetic fields as continuous, interdependent variables, supporting the wave-like nature of light [1]. However, this classical viewpoint was dramatically challenged at the beginning of the 20th century when Albert Einstein explained the photoelectric effect by treating light as discrete quanta of energy, suggesting a particle-like behavior [2]. These energy quanta were later termed “photons” by G. N. Lewis [3], and were subsequently formalized as fundamental excitations of the quantized electromagnetic field in P. A. M. Dirac’s pioneering work on quantum electrodynamics [4].

The conceptual shift from classical to quantum optics paved the way for entirely new technologies and insights, particularly through the field of quantum photonics, where the interaction of quantized light with matter is explored. A pivotal moment in this journey came in 1935 when Einstein, Podolsky, and Rosen questioned the completeness of quantum mechanics and introduced what is now known as the EPR paradox, proposing the existence of “hidden variables” to restore determinism to quantum theory [5]. However, in 1964, John Bell formulated a mathematical inequality that provided a way to test whether such hidden variables are compatible with quantum mechanics or not. And found hidden variable theory does not fit with quantum mechanics, and established the true randomness of quantum theory [6]. Experimental violations of Bell’s inequality—first demonstrated in spin systems by Clauser et al. [7, 8], and later this violation is further refined for quantum entangled source by Alain Aspect [9] and Anton Zeilinger [10]—confirmed the non-local nature of entangled quantum systems, solidifying the foundational role of quantum entanglement. During that time period, Kimble et al. [11] also observed the first evidence of a single photon source measuring the second order correlation coefficient using the Hanbury Brown and Twiss (HBT) interferometer [12]. They observed photon antibunching, a phenomenon with no classical counterpart, which served as definitive evidence for the generation of single photons.

One of the widely adopted techniques for producing single photons and entangled photons is spontaneous parametric down-conversion (SPDC), a nonlinear optical process in which a pump photon with greater energy undergoes a conversion process, yielding two daughter photons of lower energy within a nonlinear crystal. These daughter photons—commonly referred to as signal and idler—can be strongly correlated in multiple degrees of freedom: energy-time [13], frequency, polarization [14, 15], spatial mode, linear momentum [15, 16], and orbital angular momentum

[17–19]. It was first predicted by the quantum mechanical description of the optical parametric amplification [20] process. Zel’dovich and Klyshko [21] first studied the statistics of the downconverted photon in 1969. By the next year, Burnham and Weinberg [22] demonstrated the SPDC source at the experimental level. These sources, aided by modern advancements in high-efficiency detectors and nonlinear crystals with enhanced coefficients, now serve as indispensable tools in a broad range of quantum information applications such as quantum cryptography [23], quantum imaging [24], and tests of quantum non-locality [25].

One particularly promising area made possible by the SPDC process in a non-collinear geometry is the spatial profile division and multiplexing (SPDM) of the characteristic ring-shaped emission pattern, a concept first introduced and demonstrated in our work. We use this technique for various quantum random number generation (QRNG), both in localised and shared form. These new types of division and multiplexing also open up a new way of establishing a quantum network among multiple users with enhanced key rate. Random numbers have attracted significant attention in many fields, such as fundamental physics tests, scientific simulations, numerical analysis, decision-making, cryptography [26–28], etc. The generation in cryptography is particularly important because random bit strings are fundamental tools for use at various phases of cryptographic algorithms, such as key generation, symmetric encryption, passwords, nonce generation, etc. [29]. Although the computer can produce random number sequences using the complex algorithm [30], the deterministic nature of such algorithms results in pseudorandomness. The only way to get the true random numbers, or the true security for different safety applications, is to build a generator based on the random physical phenomena [31, 32]. As the quantum theory is fundamentally probabilistic, it can provide inherent randomness. Therefore, a quantum process [33] like SPDC is always an ideal base for a physically true random number genera-

tor. Also, different quantum parameters like Bell's parameter, second-order correlation coefficient, and QBER measurements of SPDC-based source provide extra benefits in certifying the true randomness coming from the quantum origin.

1.1 Objective of the Thesis

The development of technology based on quantum mechanical principles is currently a fascinating topic of scientific study. The two most fundamental principles of quantum mechanics, superposition and entanglement, can be used to change technology. The previous century was dedicated to building the theoretical core of Quantum mechanics. The current goal is to use that description to develop new, unexplored technologies. The fundamental building element of this new technology is the quantum bit (qubit) exhibits superposition, setting it apart from classical bits. Applications like information processing (quantum computing [34]) or communications (quantum cryptography [35], teleportation [36], super-dense coding [37], etc.) are strictly based on quantum states and random bit strings. Hence, generating a bit string both in localised and shared form based on the quantum inherent randomness is an exciting field of research.

The core of this thesis is the concept of *spatial profile division and multiplexing*, a powerful technique that leverages the spatial correlation of bi photons to set up new random number generation schemes, quantum key distribution, and quantum network over multiple channels. This approach not only increases communication capacity but also supports scalability for multi-user quantum networks. By carefully tailoring the spatial characteristics of heralded and entangled photons, we demonstrate a new class of quantum communication tools that can enhance randomness generation, improve security in key distribution, and enable simultaneous quantum communication links.

We begin by optimizing the properties of both heralded and entangled photon sources to achieve high brightness with stability for higher key rate generation in our different work. Keeping the key rate in mind, we also optimized the source for a higher quantumness parameter, which certifies the true randomness. As these two parameters are inversely proportional to each other, optimization of both is necessary, which serves as the foundation for a variety of quantum information protocols:

- Quantum random number generation using heralded single photons, where spatial randomness is exploited for entropy extraction.
- QRNG using entangled photon sources with real-time randomness certification via Bell inequality violations.
- BBM92 quantum key distribution protocol that utilizes spatial profile randomness for basis encoding.
- Bell state revival using geometric phase manipulation, enhancing QKD robustness against phase drift.
- A scalable multi-user quantum communication network where spatial profile division enables multiple links.

Together, these contributions demonstrate the feasibility and benefits of spatial profile multiplexing for a wide range of quantum communication applications, establishing a path forward for building high-performance, scalable, and secure quantum networks with a higher key rate.

1.2 Overview of the Thesis

This thesis is organized in a manner that begins with the relevant theoretical background and then systematically proceeds to experimental demonstrations of the SPDC process for quantum random number generation and quantum key distribution between two parties or multiple users. Figure 1.1 provides a layout map of the thesis, showing that, after the source optimization, the fundamental principle of spatial randomness is used for different applications in quantum communication domains using the methodology of spatial profile division and multiplexing.

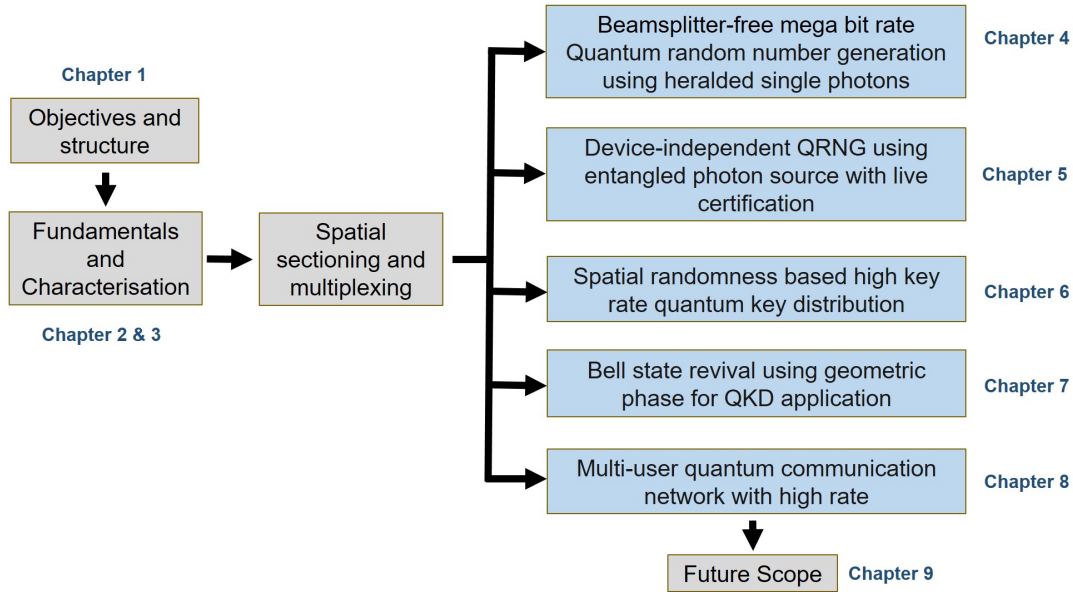


Figure 1.1: Schematic overview of the thesis structure: Spatial profile division and multiplexing, which supports a range of quantum communication applications.

- **Chapter 2** lays the theoretical groundwork by introducing the concepts of SPDC in quantum optics, the theoretical optimization of photon sources, quantum random number generation, and quantum key distribution.
- **Chapter 3** focuses on the experimental optimization of SPDC-based heralded single photon source and entangled photon source. This includes the detailed

characterization for brightness control, purity, and indistinguishability enhancement for both heralded and entangled photon sources.

- **Chapter 4** presents our implementation of QRNG using heralded single photons. We analyze the spatial and temporal correlation to extract the truly random raw bit string and discuss the randomness certification process and the statistical tests applied.
- **Chapter 5** extends QRNG to entangled photons, with a focus on live randomness certification using Bell tests. Beamsplitter-free megabit rate QRNG architecture with Bell's parameter certifications is the core of this chapter.
- **Chapter 6** introduces a novel spatial-randomness-based QKD protocol. By encoding key bits from spatial inherent randomness, we demonstrate enhanced security, parallel with the higher secure key rate.
- **Chapter 7** explores geometric phase manipulation for Bell state revival by canceling any phase drift, with applications in QKD.
- **Chapter 8** details a multi-user quantum communication network enabled by spatial sectioning-multiplexing. Experimental results in terms of key rate and quantum parameters demonstrate the functionality of multiple quantum links for free-space quantum communication.
- **Chapter 9** summarizes the key contributions of the thesis and outlines potential directions for future research in large-scale hybrid quantum networks, QRNG with simultaneous loophole-free certification, and hybrid entanglement for QKD.

Chapter 2

Fundamentals Principles

2.1 Random number generator

As the name suggests, a random sequence refers to a collection of numbers with no discernible pattern. They occur in a completely unpredictable fashion. Some of the many applications of random numbers include cryptography, Monte Carlo simulations, industrial testing and labeling, hazard games, and gambling. A simple example of understanding a random sequence is the result of flipping an unbiased coin. Every value in the sequence arises independently, and even full knowledge of all previously generated entries offers no ability to determine the next outcome. This section provides a brief description of randomness, random numbers, their properties, and the building blocks of a typical random number generator. Additionally, outline the two types of RNG, specifically how pseudo-random number generators (PRNGs), which rely on algorithmic procedures, differ from true random number generators (TRNGs) that are driven by physical processes. It also highlights why TRNGs are preferable to PRNGs and further explains the advantages that quantum-based generators have over classical

approaches within the TRNG category.

2.1.1 Randomness

A random bit string of this kind can be interpreted as the result of flipping a perfectly unbiased coin, in which the heads outcome is assigned the value ‘1’ and the tail side maps to ‘0’, and the probability of getting either head or tail is 50%. Moreover, each flip occurs independently, so knowledge of earlier outcomes provides no information about the result of later tosses. Hence, using a perfectly balanced coin yields a genuinely random sequence of bit values. Obviously, the use of unbiased and idealized coins for various quantum-level applications of interest is impractical. Our goal is to utilize the inherent randomness of the quantum process to generate a random bit stream, similar to the example mentioned earlier.

2.1.2 Random numbers and its properties

A sequence of numbers is known as a random sequence if it follows the two fundamental properties.

- Uniformity, i.e., the equal probability everywhere within the sequence
- Independentness, i.e., any current value is independent of any previous or next value of the sequence

Random numerical values are essential in a wide range of simulations and classical applications where the random number sequence follows a specific type of distribution, such as the Gaussian or Poissonian distribution. However, in our case, we are interested in a bit string, which is a sequence of ‘0’ and ‘1’ that satisfies the criteria for

randomness. For example, we can consider the bit string 101 0010, where the fourth empty position can take either 0 or 1 with equal probability as per the uniformity property. This value is either independent of the third (1) or fifth (0) position value in the bit string.

2.1.3 Different methods of random number generation

Based on the generation method, a random number generator can typically be categorized into two classes: TRNGs and PRNGs [38].

PRNGs use deterministic algorithms to produce random numbers that look apparently random, hence the term “pseudo-random.” It takes one or several initial parameters and produces a sequence of numbers that appear random. Inputs to PRNGs are called seeds. Since we require the random numbers to be unpredictable, the initial seed has to originate from a genuinely random source. Therefore, in practice, PRNGs are typically seeded using values generated by a TRNG. All the randomness in PRNG is confined to seed generation. A major drawback of PRNG is that if one knows the seed, then one can obtain the sequence of numbers with complete certainty [39]. Mersenne Twister generator (MT), Among commonly used PRNG schemes, the Linear Congruential Generator (LCG) and the Wichmann–Hill Generator (WHG) are particularly prominent in different fields of application.

In TRNG, a random sequence is generated using a non-deterministic physical phenomenon (i.e., an entropy source), either classical or quantum, along with some processing function (i.e., the entropy distillation process) to produce randomness [39]. The distillation is employed to compensate for weaknesses in the entropy source that may result in partial randomness. The entropy source is typically a physical phenomenon, such as random noise in an electrical circuit, unpredictable radioactive de-

cay, the timing of user processes (e.g., keystrokes or mouse movements), the quantum effects in a semiconductor [39], and most importantly, classical and quantum optical phenomena.

2.1.4 Block description of physical random number generator

Physical or true random number generators can be divided into multiple sub-blocks, shown in Fig. 2.1. The first one is the entropy source, and the second one is the post-processing stage. The entropy source comprises a physical system whose measurable properties display random behavior. [40], followed by a measurement device that measures random variables and generates a raw bit string. In the measurement process, it also contaminates the generated raw bit string. The post-processing block addresses this concern; it takes the raw bits and distills them into a uniform random sequence. At this stage, we first estimate the minimum binning entropy and use that for Toeplitz hashing, which will be further discussed in the Chapter. 4 . The post-processed bit string after this stage is suitable for various testing and application purposes.

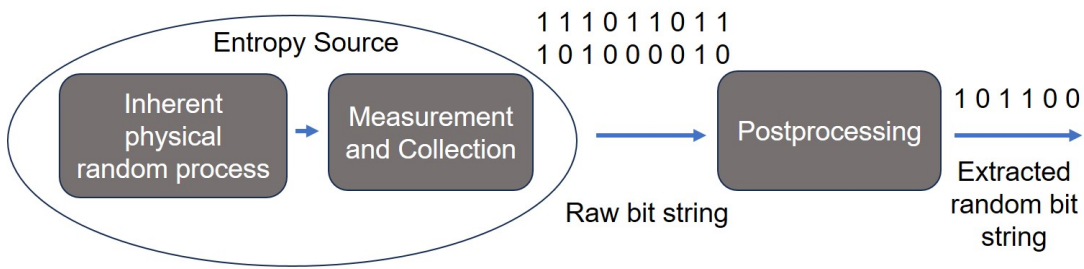


Figure 2.1: Schematic block representation of a conventional physical random number generator.

Another important parameter besides the generation is the certification of the generator. In Fig. 2.2a, if the honest party generates the random bit string and the user receives the bit string, then there is no issue, but if the source is dishonest (Fig. 2.2b)

and the user unknowingly copies the pre-decided bit string, then it is a threat to any kind of security application using random bit strings.

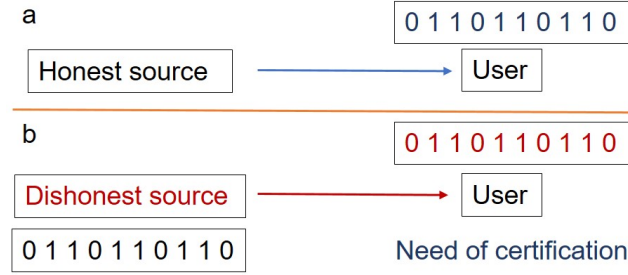


Figure 2.2: Illustration of a generic RNG from an honest source (a) and from a dishonest source (b).

Bell in 1964 showed that quantum mechanics does not fit with the hidden variable theory, and it is truly random. We can also certify the quantumness using various quantum parameters, thereby allowing for the detection of any dishonest party. In contrast, classical mechanics is a deterministic theory, where the apparent randomness arises from the lack of complete information about the system. This disadvantage of classical mechanics makes QRNG the right choice over CRNG for security applications. Although QRNG produces high-quality random numbers, its generation rate is lower. However, with the advancement of new schemes and electronics, this is growing faster in response to the demand.

2.2 Random number (key) distribution

In the earlier section, we discussed the random number generation process alone; here, we will focus on the random bit string distribution between two parties, which is also known as key distribution. This is crucial for secure communication between trusted parties, such that the transmitted information remains confidential and unaltered in the presence of potential adversaries in the field of cryptography. Its origins

can be traced back thousands of years, where it was used primarily in military and diplomatic contexts. In one notable historical incident, the deciphering of a letter from Mary, Queen of Scots, enabled Elizabeth to order Mary's execution, which reflects the longstanding human desire to protect information from prying eyes. Later on, with the advent of the internet, the demand for secure communication has grown steadily each year [41]. Rapid advancements in telecommunication technologies have further amplified the necessity for confidentiality in data exchange. Over the past three decades, the proliferation of online banking and electronic financial transactions has brought cryptography into the spotlight as a critical security tool. Secure communication is no longer limited to diplomatic correspondence between nations; it has become equally vital for everyday interactions among ordinary users. In the modern digital era, where nearly everyone is virtually connected, the internet has become an indispensable component of daily life. Without robust mechanisms to ensure the secrecy of information transmitted across it, reliable communication would be nearly impossible [41, 42].

2.2.1 Cryptography architecture

The modern definition of cryptography involves transforming a plaintext message into an encoded ciphertext using a specific secret key, such that only authorized parties possessing the correct decoding key can recover the original message. A formal representation of this process can be expressed through an encryption function E and a decryption function D , where:

$$C = E_{k_e}(P) \quad \text{and} \quad P = D_{k_d}(C) \quad (2.1)$$

with P denoting plaintext, C denoting ciphertext, and k_e and k_d being the encryption

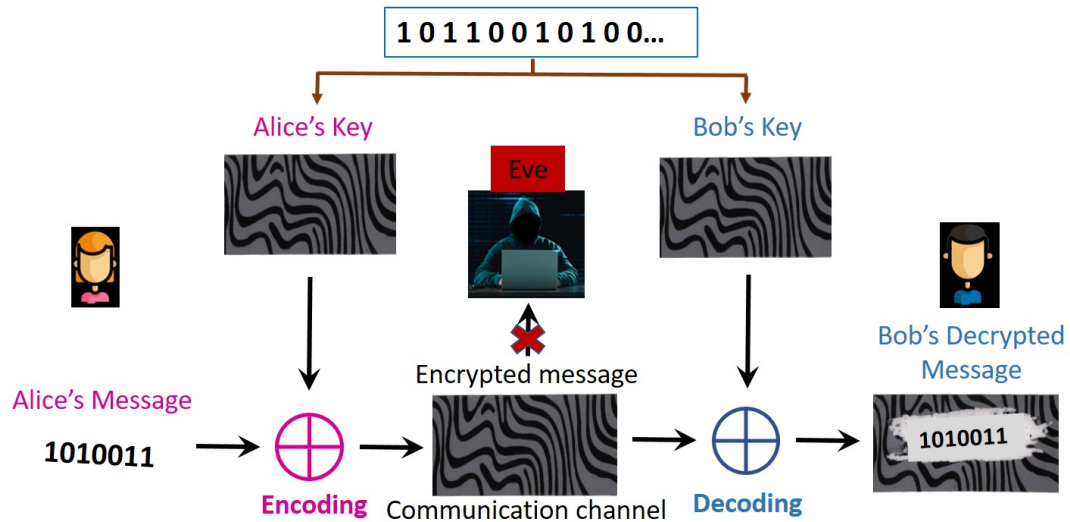


Figure 2.3: Art of cryptography with a preshared key between Alice and Bob.

and decryption keys respectively. In symmetric cryptography, $k_e = k_d$, whereas in asymmetric cryptography, these keys are distinct.

Cryptography is built upon below fundamental security principles:

1. **Confidentiality (Privacy)** — The content of the message must remain unintelligible to any unauthorized party. Only the intended recipient should be able to reconstruct the original plaintext.
2. **Data Integrity** — The message must remain unaltered during transmission. If a message is intercepted and modified by an adversary, both the sender and the recipient should be able to detect the tampering.
3. **Authentication** — The communicating parties must be able to verify each other's identities, ensuring that the message originates from a legitimate sender.

In the communication model shown in Fig. 2.3, the sender and receiver are conventionally referred to as Alice and Bob, while an adversary attempting to intercept

or alter the communication is called Eve. For example, if Alice and Bob are executives at a technology company exchanging sensitive product development plans, it is imperative that these communications remain inaccessible to competitors or malicious entities.

In order to enable secure communication [43], Alice and Bob must initially agree upon a shared key, which requires an initial secure key distribution between them, as shown at the top of Fig. 2.3. While messages are transmitted over insecure channels in encrypted form, the long-term secrecy of their contents depends on the strength of the cryptographic algorithm and the secrecy of the key. It is important to note that no code is truly unbreakable; given sufficient time and resources, any encryption scheme can be compromised. The goal of cryptographic design is therefore to make such decryption computationally infeasible within the period for which the information must remain secret. In classical cryptography, the security of a system is primarily determined by the computational complexity of its encryption and decryption algorithms in generating the key. Computational complexity, in this context, refers to the number of computational steps an eavesdropper (Eve) would require—given contemporary computing capabilities—to successfully recover the plaintext from the ciphertext. The difficulty of this task generally increases with the length of the encryption key, as longer keys exponentially expand the possible key space to be searched. However, this security assumption is challenged by the advent of quantum computing and associated quantum algorithms [34, 41, 44], which can solve certain algorithms underlying existing cryptographic schemes in polynomial time, thereby rendering many traditional encryption methods vulnerable. Quantum key distribution is the alternative future secure solution to prevent the catastrophe of the current scheme in the quantum era.

2.2.2 Quantum key distribution network

The emergence of quantum computing and quantum information science has motivated the development of quantum-safe cryptography, which offers methods for key exchange that remain secure [45] even in the presence of quantum-capable adversaries. Quantum Key Distribution utilizes the principles of quantum mechanics to facilitate the secure distribution of keys between two parties. The concept was first practically introduced through the BB84 protocol, which utilized conjugate basis encoding [46, 47].

A key advantage of QKD is its ability to generate an unlimited number of secure keys from a single initial setup. In classical cryptography, once a finite-size secret key is distributed, it becomes increasingly difficult to extend or amplify that key. For maximum security, keys must be discarded after each use, and eventually, the communicating parties will exhaust their supply of shared secrets. In contrast, quantum mechanics enables a key growing process [48], wherein additional secure keys can be generated continuously, making QKD highly attractive for applications ranging from secure banking transactions to military communications.

Unlike conventional key distribution schemes that employ classical bits (0 and 1), QKD operates with quantum bits (qubits). Qubits are quantum states that possess several distinctive properties, which form the foundation of QKD protocols [34]. Various degrees of freedom of photons—such as polarization, orbital angular momentum (OAM), time-bin, or frequency—can be used as a photonic qubit. For instance, horizontal polarization is denoted as $|H\rangle$ and vertical polarization as $|V\rangle$. A general qubit state can exist as a superposition, written as $c_1 |H\rangle + c_2 |V\rangle$, where c_1 and c_2 are complex probability amplitudes. Measuring a qubit projects it onto the eigenbasis of the

chosen measurement operator. For example, measurement in the $\{|H\rangle, |V\rangle\}$ basis uses projectors $P_H = |H\rangle\langle H|$ and $P_V = |V\rangle\langle V|$. Suppose, the initial state $|\psi\rangle_{\text{in}} = |H\rangle$, a measurement using P_H yields $|H\rangle$, while P_V yields 0. If the state is in superposition, $|\psi\rangle_{\text{in}} = c_1 |H\rangle + c_2 |V\rangle$, the projection outcome depends on the chosen basis, and measurements in a non-matching basis produce inherently random results [34, 46]. This **measurement disturbance** principle protects the key distribution by detecting the presence of an eavesdropper. Secondly, the **uncertainty principle** applies to non-orthogonal quantum states, meaning an adversary cannot determine the exact state without error. And thirdly, the **no-cloning theorem** [49], which states that unknown generic quantum states cannot be copied, thereby preventing the duplication of information. These three principles form the backbone of Prepare-and-Measure quantum protocols, such as BB84 and B92. Additionally, **quantum entanglement** with these principles enables secure sharing of keys in the BBM92 and E91 protocols through non-classical correlations. Entanglement describes a condition in which the state of one subsystem (A) is intrinsically linked to the state of another subsystem (B). In such cases, the combined system cannot be expressed as a simple tensor product [50]:

$$|\psi\rangle_{AB} \neq |\psi\rangle_A \otimes |\phi\rangle_B \quad (2.2)$$

Instead, it may take the form:

$$|\psi\rangle_{AB} = c_1 |\psi\rangle_A \otimes |\phi\rangle_B + c_2 |\phi\rangle_A \otimes |\psi\rangle_B \quad (2.3)$$

Measurement of one subsystem instantaneously determines the outcome of the other [51], regardless of the spatial separation between them. Sifted key rate and QBER [52] are two important metrics for a QKD protocol, which we experimentally estimate in Chapter 6. These quantum mechanical principles form the theoretical framework for

QKD between two users. This can also be extended to multiple users, where each user can be connected to any other users, which is known as a quantum network [53]. In my future work on high-performance quantum technologies, including QRNG, device-independent randomness certification, spatial randomness-based BBM92 QKD, and multi-user quantum networks, we utilize the Spontaneous Parametric Down Conversion (SPDC) process to generate an annular ring shape source, which is the next topic of my discussion.

2.3 Spontaneous parametric down-conversion process

As introduced in chapter 1, SPDC is a second-order nonlinear process, where a small percentage of the pump photons of higher frequency (ω_p) passes through a $\chi^{(2)}$ non-linear medium and splits into two photons of lower frequencies [54] Fig. 2.4, known as a signal of frequency (ω_s) and idler of frequency (ω_i). The daughter photons are directly generated from the pump beam. There is no need for any other external seed beam; that is why this process is referred to as spontaneous. The quantum vacuum field is responsible for down conversion at the fundamental level; hence, the process is purely quantum in nature. However, classical difference frequency generation [55] at $\omega_i = \omega_p - \omega_s$ of an input pump signal ω_p along with a very weak signal ω_s can approximate the parametric emission. In the case of SPDC, vacuum modes at ω_s replace the classical weak signal, which makes this process very inefficient. Typically, 1 out of 10^6 photons get down-converted [20] in a bulk crystal-based SPDC. It is called parametric because energy is conserved in this process, and the pump beam is not involved in non-parametric energy exchange with the nonlinear crystal. A pump photon is absorbed within the nonlinear material and temporarily elevated to a virtual state [56]. Interaction with a vacuum mode at ω_s stimulates this excited state, leading to its decay back to the ground state, resulting in two down-converted photons.

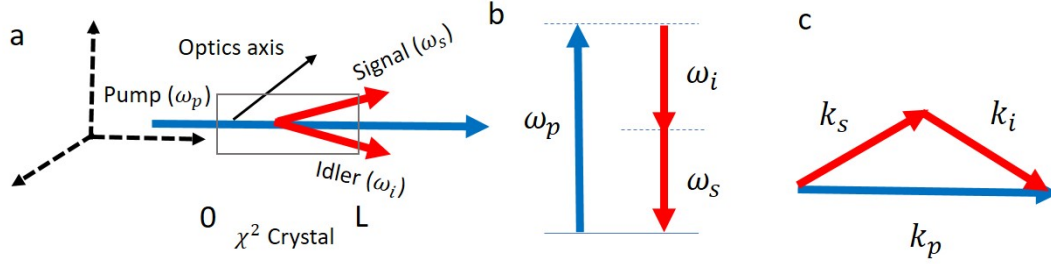


Figure 2.4: (a) The pump field along the z-axis generates two down-converted field signals and an idler. (b) and (c) respectively energy and momentum conservation diagram of a SPDC process.

Also, the total energy conservation $\omega_p = \omega_s + \omega_i$ (Fig. 2.4b) holds in this process, and as the higher frequency input converts to the lower output frequencies, the process is named a down-conversion process. The momentum of the initial photon is conserved as dictated by the phase-matching condition $\mathbf{k}_p = \mathbf{k}_s + \mathbf{k}_i$ and shown in Fig. 2.4c.

2.3.1 Quantum mechanical description

As we mentioned in the last section, SPDC is a second-order nonlinear process; we will start with the expression of polarization for the formal derivation of this process. The polarization vector, considering the higher-order term [57], is given by

$$\mathbf{P}(\mathbf{r}, t) = \epsilon_0 \chi^{(1)} \mathbf{E}(\mathbf{r}, t) + \epsilon_0 \chi^{(2)} \mathbf{E}^2(\mathbf{r}, t) + \epsilon_0 \chi^{(3)} \mathbf{E}^3(\mathbf{r}, t) + \dots, \quad (2.4)$$

$$\text{and } \mathbf{D}(\mathbf{r}, t) = \epsilon_0 \mathbf{E}(\mathbf{r}, t) + \mathbf{P} \quad (2.5)$$

The vectors are written both as a function of space and time. Now, the total energy density of the electromagnetic field, including both electric and magnetic contributions, is given by [58]

$$H_T(t) = \int_V \mathbf{D}(\mathbf{r}, t) \cdot \mathbf{E}(\mathbf{r}, t) d^3\mathbf{r} \quad (2.6)$$

$$= \int_V \left(\left[\epsilon_0 \mathbf{E}(\mathbf{r}, t) + \epsilon_0 \chi^{(1)} \mathbf{E}(\mathbf{r}, t) \right] \cdot \mathbf{E}(\mathbf{r}, t) + \left[\epsilon_0 \chi^{(2)} \mathbf{E}^2(\mathbf{r}, t) \right] \cdot \mathbf{E}(\mathbf{r}, t) + \dots \right) d^3\mathbf{r} \quad (2.7)$$

The first term in Eq. 2.7 represents the linear contribution to the electromagnetic energy density. In this context, our focus is on the second-order contribution to the energy density because of the non-linearity of the medium, which is [58]

$$\begin{aligned} H_{NL}^{(2)}(t) &= \epsilon_0 \int_{\mathcal{V}} \chi^{(2)} \mathbf{E}^2(\mathbf{r}, t) \cdot \mathbf{E}(\mathbf{r}, t) d^3\mathbf{r} \\ &= \int_{\mathcal{V}} \mathbf{P}^{(2)}(\mathbf{r}, t) \cdot \mathbf{E}(\mathbf{r}, t) d^3\mathbf{r} \end{aligned} \quad (2.8)$$

Now, considering this expression for the parametric down-conversion process in quantum formalism, we can write the Hamiltonian operator [54]

$$\begin{aligned} H_{\text{SPDC}}(t) &= \int_{\mathcal{V}} \mathbf{P}^{(2)}(\mathbf{r}, t) \cdot \mathbf{E}(\mathbf{r}, t) d^3\mathbf{r} \\ \hat{H}_{\text{SPDC}}(t) &= \epsilon_0 \int_{\mathcal{V}} \chi^{(2)} \hat{E}_p(\mathbf{r}, t) \hat{E}_s(\mathbf{r}, t) \hat{E}_i(\mathbf{r}, t) d^3\mathbf{r} \end{aligned} \quad (2.9)$$

where p, s , and i stand for the pump, signal, and idler, respectively. $\chi^{(2)}$ in the above equation is a rank-three tensor where its components are the proportionality constant, which relates non-linear polarization amplitudes with the product field am-

plitudes. By considering different factors like crystal class, symmetry, and phase-matching, we can contract this $\chi^{(2)}$ into a constant called d_{eff} . $\hat{E}_p(r, t)$, $\hat{E}_s(r, t)$, and $\hat{E}_i(r, t)$ represent the quantized electric field operator corresponding to the pump, signal, and idler field [58]. It can be written as a sum of negative and positive frequency terms [59].

$$\hat{E}_p(\mathbf{r}, t) = \hat{E}_p^{(+)}(\mathbf{r}, t) + \hat{E}_p^{(-)}(\mathbf{r}, t) \quad (2.10)$$

Now, replacing these in Eq. 2.9, The interaction Hamiltonian therefore takes the form

$$\begin{aligned} \hat{H}_{SPDC}(t) = \epsilon_0 \int_{\mathcal{V}} d_{eff} \left[\hat{E}_p^{(+)}(\mathbf{r}, t) + \hat{E}_p^{(-)}(\mathbf{r}, t) \right] \times \left[\hat{E}_s^{(+)}(\mathbf{r}, t) + \hat{E}_s^{(-)}(\mathbf{r}, t) \right] \\ \times \left[\hat{E}_i^{(+)}(\mathbf{r}, t) + \hat{E}_i^{(-)}(\mathbf{r}, t) \right] d^3\mathbf{r} \end{aligned} \quad (2.11)$$

The effective terms from the above expression for the parametric down-conversion are $E_p^{(-)}E_s^{(+)}E_i^{(+)}$ and $E_p^{(+)}E_s^{(-)}E_i^{(-)}$ leading to processes that conserve energy and consequently contribute substantially to down-conversion. Other terms will be averaged out [60].

$$H_{SPDC}(t) = \epsilon_0 \int_{\mathcal{V}} d_{eff} \hat{E}_p^{(+)}(\mathbf{r}, t) \hat{E}_s^{(-)}(\mathbf{r}, t) \hat{E}_i^{(-)}(\mathbf{r}, t) d^3\mathbf{r} + \text{H.c.} \quad (2.12)$$

where a quantized field [59, 61] is expressed as

$$\hat{E}^{(+)}(\mathbf{r}, t) = \int_{-\infty}^{\infty} \left(\int A_{\mathbf{k}} \hat{a}(\mathbf{k}, \omega) e^{i\mathbf{k} \cdot \mathbf{r}} d^3\mathbf{k} \right) e^{-i\omega t} d\omega. \quad (2.13)$$

Now, to keep the formal derivation in the simpler form, we consider a single mode ($\mathbf{k}$) and frequency (ω) instead of all actual possible combinations of modes and frequency. Then $A_{\mathbf{k}}$ is constant and written as A . Also, we will write the transverse and longitudinal components of $\mathbf{k}$ and $\mathbf{r}$ separately as, $\mathbf{k} = (k_x, k_y, k_z) = (q, k_z)$, $\mathbf{r} = (x, y, z) = (\rho, z)$, and $\hat{a}(\mathbf{k}, \omega) = \hat{a}$ [58]. Accordingly, we express the pump, signal, and idler electric field operators in a form that excludes the integral.

$$\hat{E}_p^{(+)}(\mathbf{r}, t) = A_p e^{i\mathbf{q}_p \cdot \rho} e^{i(k_{pz}z - \omega_p t)} V(\mathbf{q}_p, \omega_p)$$

$$\hat{E}_s^{(-)}(\mathbf{r}, t) = A_s^* e^{-i\mathbf{q}_s \cdot \rho} e^{-i(k_{sz}z - \omega_s t)} \hat{a}_s^+$$

$$\hat{E}_i^{(-)}(\mathbf{r}, t) = A_i^* e^{-i\mathbf{q}_i \cdot \rho} e^{-i(k_{iz}z - \omega_i t)} \hat{a}_i^+ \quad (2.14)$$

Here, we assumed the pump field is classical, and we replaced the annihilation operator with the field amplitude $V(\mathbf{q}_p, \omega_p)$ [58]. Substituting this field operator in Eq. 2.12 we get

$$H_{\text{SPDC}}(t) = \epsilon_0 A_p A_s^* A_i^* V(\mathbf{q}_p, \omega_p) e^{i(\omega_s + \omega_i - \omega_p)t} \left(\int_{\mathcal{V}} e^{i(\mathbf{q}_p - \mathbf{q}_s - \mathbf{q}_i) \cdot \rho} d^2\rho \right)$$

$$\times \left(\int d_{eff} e^{i(k_{pz} - k_{sz} - k_{iz})z} dz \right) \hat{a}_s^+ \hat{a}_i^+ + \text{H.c.} \quad (2.15)$$

Considering that the crystal's transverse dimension is far larger than that of the pump beam, the limit for the first integral becomes $-\infty$ to $+\infty$

$$\int_{-\infty}^{\infty} e^{i(\mathbf{q}_p - \mathbf{q}_s - \mathbf{q}_i) \cdot \boldsymbol{\rho}} d^2 \boldsymbol{\rho} = \delta(\mathbf{q}_p - \mathbf{q}_s - \mathbf{q}_i) \quad (2.16)$$

It implies transverse momentum is conserved in this process, i.e., $\mathbf{q}_p = \mathbf{q}_s + \mathbf{q}_i$. Now the second integration term is known as a phase-matching function $\phi(\mathbf{q}_s, \mathbf{q}_i)$. We will do the integration over the length (L) of the crystal. d_{eff} can be constant or a function of z, depending on the nature of phase matching. Considering d_{eff} is constant and $(k_{pz} - k_{sz} - k_{iz}) = \Delta k_z$ for birefringent phase-matching, we can simplify.

$$\begin{aligned} \phi(\mathbf{q}_s, \mathbf{q}_i) &= \int_0^L d_{eff} e^{i\Delta k_z z} dz = \frac{d_{eff}}{\Delta k_z} \frac{e^{i\Delta k_z L} - 1}{i} \\ &= \frac{d_{eff}}{\Delta k_z} e^{i\Delta k_z L/2} \frac{e^{i\Delta k_z L/2} - e^{-i\Delta k_z L/2}}{i} \\ &= L d_{eff} e^{i\Delta k_z L/2} \frac{\sin\left(\frac{\Delta k_z L}{2}\right)}{\frac{\Delta k_z L}{2}} \\ &= L d_{eff} e^{i\Delta k_z L/2} \text{sinc}\left(\frac{\Delta k_z L}{2}\right) \end{aligned} \quad (2.17)$$

The phase matching function gives the maximum when $(k_{pz} - k_{sz} - k_{iz}) = \Delta k_z = 0$, which also implies, additionally, that with the transverse momentum, longitudinal mo-

momentum is also conserved in the SPDC process. The interaction Hamiltonian becomes

$$\begin{aligned}\hat{H}_{\text{SPDC}}(t) &= \epsilon_0 L d_{\text{eff}} A_p A_s^* A_i^* V(\mathbf{q}_s + \mathbf{q}_i, \omega_p) e^{i(\omega_s + \omega_i - \omega_p)t} e^{i\Delta k_z L/2} \\ &\times \text{sinc}\left(\frac{\Delta k_z L}{2}\right) \hat{a}_s^+ \hat{a}_i^+ + \text{H.c.}\end{aligned}\quad (2.18)$$

Now, we consider this interaction Hamiltonian in time-dependent Schrodinger pictures for finding the time-evolved signal and idler photon state $|\psi(t)\rangle$ starting from the vacuum field of signal and idler, i.e. $|\psi(0)\rangle = |0\rangle_s |0\rangle_i$ [62] initially at time $t = 0$. Then the quantum state becomes

$$|\psi(t)\rangle = e^{-\frac{i}{\hbar} \int_0^t \hat{H}_{\text{SPDC}}(t) dt} |\psi(0)\rangle \quad (2.19)$$

In the expansion of the exponential term, the first two terms are enough, as we assume parametric down-conversion is very weak. Out of these two terms, the second term actually gives the final two-photon state from the SPDC process. So, the second term

$$\begin{aligned}|\psi(t)\rangle &= -\frac{i}{\hbar} \int_0^t \hat{H}_{\text{SPDC}}(t) dt |\psi(0)\rangle \\ &= \left[-\frac{i}{\hbar} \epsilon_0 L d_{\text{eff}} A_p A_s^* A_i^* V(\mathbf{q}_s + \mathbf{q}_i, \omega_p) \phi(\mathbf{q}_s, \mathbf{q}_i) \right. \\ &\quad \left. \times \left(\int_0^t e^{i(\omega_s + \omega_i - \omega_p)t} dt \right) \hat{a}_s^+ \hat{a}_i^+ + \text{H.c.} \right] |\psi(0)\rangle\end{aligned}\quad (2.20)$$

Similarly to Eq. 2.16 assumes that the interaction time is much longer than the characteristic timescale of the down-conversion process. Consequently, allowing the time integral to be evaluated over $-\infty$ to $+\infty$, and it gives [58]

$$\int_{-\infty}^{\infty} e^{i(\omega_s + \omega_i - \omega_p)t} dt = \delta(\omega_s + \omega_i - \omega_p) \quad (2.21)$$

This indicates the conservation of total energy, that is, $\omega_p = \omega_s + \omega_i$ in the SPDC process. And the output state then modifies to

$$|\psi(t)\rangle = \left[-\frac{i}{\hbar} \epsilon_0 L d_{eff} A_p A_s^* A_i^* V(\mathbf{q}_s + \mathbf{q}_i, \omega_s + \omega_i) \phi(\mathbf{q}_s, \mathbf{q}_i) \hat{a}_s^+ \hat{a}_i^+ + \text{H.c.} \right] |0\rangle_s |0\rangle_i \quad (2.22)$$

In the above equation, H.c. will be the annihilation operator, and applying it on $|0\rangle_s |0\rangle_i$ will vanish it. considering $g = -\frac{i}{\hbar} \epsilon_0 L d_{eff} A_p A_s^* A_i^*$ we can write the state in simplified form

$$|\psi(t)\rangle = g V(\mathbf{q}_s + \mathbf{q}_i, \omega_s + \omega_i) \phi(\mathbf{q}_s, \mathbf{q}_i) \hat{a}_s^+ \hat{a}_i^+ |0\rangle_s |0\rangle_i \quad (2.23)$$

Now, if we consider signal two modes of frequency ω_1 and ω_2 , then idler will have the respective mode of frequencies ω_2 and ω_1 following $\omega_p = \omega_1 + \omega_2$. Then the state can be written as

$$\begin{aligned}
|\psi(t)\rangle &= V(\mathbf{q}_s + \mathbf{q}_i, \omega_s + \omega_i) \phi(\mathbf{q}_s, \mathbf{q}_i) (g_1 \hat{a}_s^{+(\omega_1)} \hat{a}_i^{+(\omega_2)} + g_2 \hat{a}_s^{+(\omega_2)} \hat{a}_i^{+(\omega_1)}) |0\rangle_s |0\rangle_i \\
&= V(\mathbf{q}_s + \mathbf{q}_i, \omega_s + \omega_i) \phi(\mathbf{q}_s, \mathbf{q}_i) (g_1 |\omega_1\rangle_s |\omega_2\rangle_i + g_2 |\omega_2\rangle_s |\omega_1\rangle_i)
\end{aligned} \tag{2.24}$$

In the final expression phase matching function, along with the energy conservation principle, decides the spatial profile of the SPDC biphoton on the transverse plane, and the final state indicates that the generated photon pairs possess entanglement in the energy degree of freedom. Entanglement in other degrees of freedom, i.e., polarization, orbital angular momentum, and path, can be engineered by using additional optical design with correlated photon pairs. Next, we will focus on how the phase matching can be achieved at the implementation level for generating signal and idler photons using a non-linear crystal in the next section.

2.3.2 Phase matching

As we discussed in the earlier section at phase matching condition $k_{pz} = k_{sz} + k_{iz}$, now we also know $k = n(\omega)\omega/c$, substituting this in the phase-matching equation, we get

$$\frac{n_{p\sigma}(\omega_p)\omega_p}{c} = \frac{n_{s\sigma}(\omega_s)\omega_s}{c} + \frac{n_{i\sigma}(\omega_i)\omega_i}{c} \tag{2.25}$$

Substituting $\omega_s = \omega_p - \omega_i$ from the energy conservation equation we can write

$$n_{p\sigma}(\omega_p) - n_{s\sigma}(\omega_s) = \frac{\omega_i}{\omega_p} [n_{i\sigma}(\omega_i) - n_{s\sigma}(\omega_s)] \quad (2.26)$$

In Eq. 2.26, $\omega_p > \omega_s \geq \omega_i$, and therefore this equation cannot be regarded as an obvious condition for every material. Let's consider the simplest case of degenerate SPDC, where $\omega_s = \omega_i$, hence, $\omega_p = 2\omega_s$, which gives $n_{i\sigma}(\omega_i) = n_{s\sigma}(\omega_s)$ from the energy conservation principle. Then, the phase-matching condition is simplified to

$$\begin{aligned} n_{p\sigma}(2\omega_s) - n_{s\sigma}(\omega_s) &= 0 \\ n_{p\sigma}(2\omega_s) &= n_{s\sigma}(\omega_s) \end{aligned} \quad (2.27)$$

For normal dispersive material, achieving this condition is not possible as the refractive index increases with frequency, i.e., $n_{p\sigma}(2\omega_s) > n_{s\sigma}(\omega_s)$. However, in a birefringent crystal, this can be achieved because we obtain an additional control parameter, θ , which denotes the propagation angle of the e-ray relative to the optic axis.

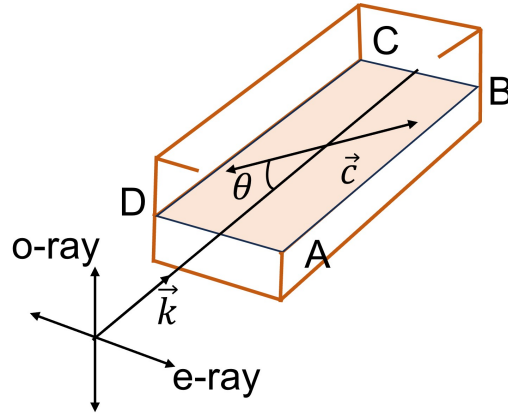


Figure 2.5: Illustrates birefringence in a nonlinear crystal. The light orange plane contains the wave vector and the optic axis. Ordinary ray (o-ray) polarization stays perpendicular to this plane, while the polarization of the extraordinary ray (e-ray) changes its orientation angle (θ), relative to the optic axis. This causes the e-ray to exhibit an angle-dependent refractive index.

In the uniaxial crystal, two orthogonal propagation modes are possible shown in Fig. 2.5. (1) ordinary mode with polarization ($\sigma = o$) orthogonal to the plane defined by the optical axis and the propagation direction, with refractive index $n_o(\omega)$, and (2) Extra-ordinary mode with polarization ($\sigma = e$) vector is aligned with the plane containing the optical axis and the propagation direction, and the refractive index $n_e(\omega, \theta)$ is given by

$$n_e(\omega, \theta) = \left[\frac{\cos^2(\theta)}{n_o^2(\omega)} + \frac{\sin^2(\theta)}{n_E^2(\omega)} \right]^{-1/2} \quad (2.28)$$

Where θ is the angle between the wave vector and the optic axis, from the above equation $n_e(\omega, 0^\circ) = n_o(\omega)$ and $n_e(\omega, 90^\circ) = n_E(\omega)$ [63] we can draw the surface for these two modes and obtain the Birefringent phase matching (BPM) condition from geometry. These two refractive index functions for a particular wavelength are given

by Sellmeier's equation

$$n_{O,E}^2 = A^{O,E} + \frac{B^{O,E}}{\lambda^2 + C^{O,E}} + D^{O,E} \lambda^2 \quad (2.29)$$

Now, depending on the polarization direction, σ can take the value of $\sigma = o$ (for ordinary polarized) and $\sigma = e$ (for extraordinary polarized) for each of the pump, signal, and idler photons. Based on the different polarization combinations of pump, signal, and idler, there are three types of SPDC. If all of these have the same polarisation, then it is called Type-0 SPDC [64]. If the signal and idler have the same polarisation, which is orthogonal to the pump, then it is Type-I SPDC. Otherwise, in Type-II SPDC, the signal and idler have mutually orthogonal polarizations, irrespective of the pump polarization. By permuting all the possible polarization scenarios and following Eq. 2.26, we can have different types of SPDC [65] processes shown in Table 2.1 .

Table 2.1: Overview of SPDC types and corresponding crystal choices that allow BPM

Type	Positive uni-axial	Negative uni-axial	BPM
Type-0	$o \rightarrow o + o$	$e \rightarrow e + e$	No
Type-I	$o \rightarrow e + e$	$e \rightarrow o + o$	Yes
Type-II	$o \rightarrow o + e$	$e \rightarrow e + o$	Yes
	$o \rightarrow e + o$	$e \rightarrow o + e$	Yes

Although Type-0 SPDC ($o \rightarrow o + o$ or $e \rightarrow e + e$) can't be achieved by birefringent phase matching, it can be accomplished via quasi-phase matching, which will be discussed later. Now, considering Type-I SPDC with e-polarised pump and o-polarisation of signal and idler for a negative uniaxial crystal in Eq. 2.27 we can write

$$2n_{pe}(2\omega_s)\omega_s = n_{so}(\omega_s)\omega_s + n_{io}(\omega_s)\omega_s$$

$$2 \left[\frac{\cos^2(\theta)}{n_O^2(2\omega_s)} + \frac{\sin^2(\theta)}{n_E^2(2\omega_s)} \right]^{-1/2} = n_O(\omega_s) + n_O(\omega_i) \quad (2.30)$$

Solving this equation, we can find the cut angle θ for a particular uniaxial crystal. At the experiment level, we need to keep the crystal in such a way that a normal incident pump on the crystal automatically achieves that cut angle with the crystal optic axis for Birefringent phase matching. For the BBO crystal, this cut angle is 29° . To understand the spatial profile of the Type-I SPDC process, we first consider the phase-matching equation on a plane and then extrapolate our understanding to 3D space to obtain the actual spatial profile. In a plane, the L.H.S of the Eq. 2.30 follows an elliptical trajectory where the major axis and minor axis lengths are $n_O(2\omega_s)$ and $n_E(2\omega_s)$ respectively, we have considered the trajectory for a negative uniaxial crystal in Fig. 2.6(a) for which $n_E(2\omega_s) < n_O(2\omega_s)$. In the R.H.S $n_O(\omega_s)$ and $n_O(\omega_i)$ refractive index for ordinary polarization mode circular trajectory. The diameters of the circles are different as we consider $n_O(\omega_s) > n_O(\omega_i)$. The green circle represents the trajectory for the signal photon centered at one of the ends of $\mathbf{k}_p$, and the red circle represents the trajectory for the idler photon centered at the other end of the pump wave vector. The intersection of the two circles in Fig. 2.6(a) results in two symmetrically oriented solutions of the phase-matching condition relative to the pump beam. When we extend this solution to the complete 3D space, the k-surfaces take the form of spheres and ellipsoids instead of circles and ellipses. Consequently, the intersection of these spheres defines the two cones illustrated in Fig. 2.6(b). The double-headed arrows represent the signal (green) and idler (red) correlated photons coming out from the Type-I SPDC.

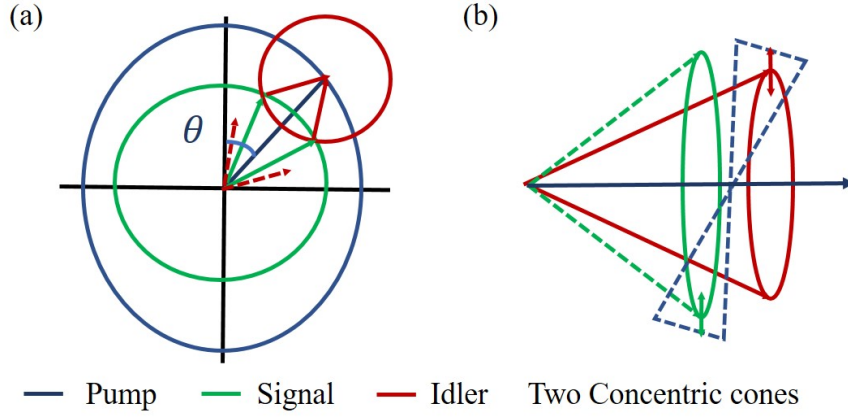


Figure 2.6: (a) Geometrical representation of the phase-matching condition, achieved at the intersection of the k -surfaces of the down-converted photons. In Type-I SPDC, this intersection corresponds to the overlap of two circles, which in three-dimensional space form two concentric cones. (b) In this process, the down-converted photons hold similar polarizations, but different from the pump photon's polarization. Their propagation directions form two concentric cones.

Again, for degenerate Type-II phase matching $e \rightarrow o + e$ from Eq.2.25

$$2n_{pe}(2\omega_s)\omega_s = n_{so}(\omega_s)\omega_s + n_{ie}(\omega_s)\omega_s$$

$$2 \left[\frac{\cos^2(\theta)}{n_O^2(2\omega_s)} + \frac{\sin^2(\theta)}{n_E^2(2\omega_s)} \right]^{-1/2} = n_O(\omega_s) + \left[\frac{\cos^2(\theta)}{n_O^2(\omega_s)} + \frac{\sin^2(\theta)}{n_E^2(\omega_s)} \right]^{-1/2} \quad (2.31)$$

As the signal and idler emission angles are very small ($1 - 3^\circ$) in non-collinear SPDC, we considered the same cut angle for the signal, idler, and pump. The solution of Eq. 2.31 for BBO crystal gives $\theta = 41.4^\circ$. Similar to the Type-I SPDC case, we can plot the phase trajectory of both sides of the phase-matching equation on a plane, where we need to change the trajectory of the idler photon from a circle to an ellipse. Here, in this case, we don't get the concentric cone; instead, we get two symmetrically tilted cones with respect to the pump direction in the 3D space. Here, correlated photons,

signal (green), and idler (red) photons coming out of the Type-II SPDC are represented by the double-headed arrows.

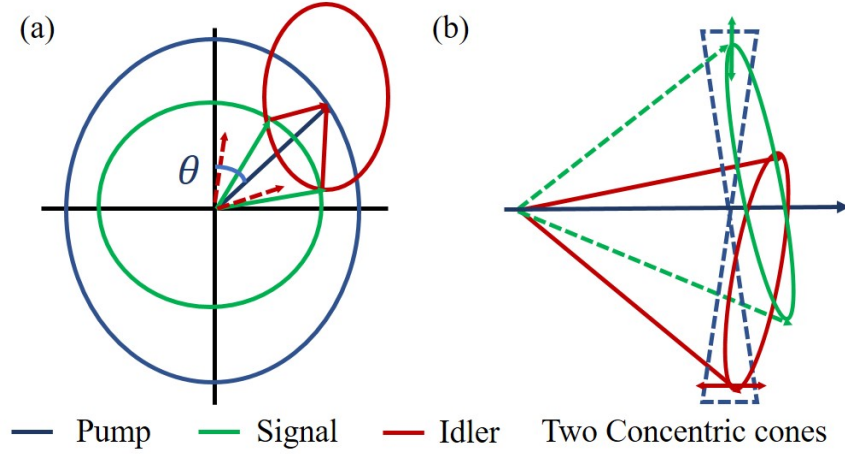


Figure 2.7: (a) The geometrical interpretation of the phase-matching condition in the Type-II case, where the k-surfaces intersection occurs between a circle and an ellipse, resulting in the formation of tilted cones. (b) The down-converted photons possess orthogonal polarizations; they are on the surface of two symmetrically tilted cones relative to the pump direction.

In the case of Type-0 SPDC, all the polarisations of the pump, signal, and idler should be the same. For example, the degenerate $e \rightarrow e + e$ case from Eq. 2.27 we need to achieve $n_{pe}(2\omega_s) = n_{se}(\omega_s)$. As $n_{pe}(2\omega_s) > n_{se}(\omega_s)$ for normal dispersion, so for similar types of polarization

$$n_{pe}(2\omega_s) \neq n_{se}(\omega_s) \quad (2.32)$$

Now, adding some additional terms (let m) on the R.H.S of Eq. 2.32, we can make this inequality equal, $n_{pe}(2\omega_s) = n_{se}(\omega_s) + m$. This term (m) needs to be added within the phase matching function in Eq. 2.17 and will arise from the additional

crystal features. Here, quasi-phase matching (QPM) using a periodically poled crystal comes into the picture. For a periodically poled crystal with Λ periodicity, $d_{eff}(z)$ is a periodic function, unlike constant d_{eff} in BPM and represented as a Fourier series:

$$d_{eff}(z) = |d_{eff}| \sum_{m=-\infty}^{\infty} C_m e^{-i(2\pi m/\Lambda)z}. \quad (2.33)$$

Then, the phase-matching function becomes considering $k_m = 2\pi m/\Lambda$

$$\begin{aligned} \phi(\mathbf{q}_s, \mathbf{q}_i) &= |d_{eff}| \sum_{m=-\infty}^{\infty} C_m \int_0^L e^{i\Delta k_z z} e^{-ik_m z} dz \\ &= |d_{eff}| \sum_{m=-\infty}^{\infty} C_m \frac{1}{(\Delta k_z - k_m)} \frac{e^{i(\Delta k_z - k_m)L} - 1}{i} \\ &= L|d_{eff}| \sum_{m=-\infty}^{\infty} C_m e^{i(\Delta k_z - k_m)L/2} \text{sinc}\left(\frac{(\Delta k_z - k_m)L}{2}\right) \end{aligned} \quad (2.34)$$

Then, the quasi-phase-matching condition is modified to

$$\Delta \tilde{k}_m = \Delta k_z - k_m = \Delta k_z - \frac{2\pi}{\Lambda} m = 0 \quad (2.35)$$

which gives $n_{pe}(2\omega_s) = n_{se}(\omega_s) + m$ for degenerate Type-0 SPDC. For a fixed Δk_z and Λ , only one m value is acceptable, so we can omit the summation in the above Eq. 2.34. We can tune the QPM using the temperature as both $\Lambda(= \Lambda_0(1 + \alpha T))$ and $n(= n_0(1 + \alpha T))$ are functions of temperature.

Next, we will come to the spatial profile of the Type-0 SPDC for which we need to calculate the emission angle of signal (θ_s^E) and idler (θ_i^E) w.r.t the pump. In Eq. 2.35 $\Delta k_z = (k_{pz} - k_{sz} - k_{iz})$ and from Fig. 2.8 $k_{pz} = k_p$, $k_{sz} = k_s \cos(\theta_s^E)$ and $k_{iz} = k_i \cos(\theta_i^E)$.

Which gives

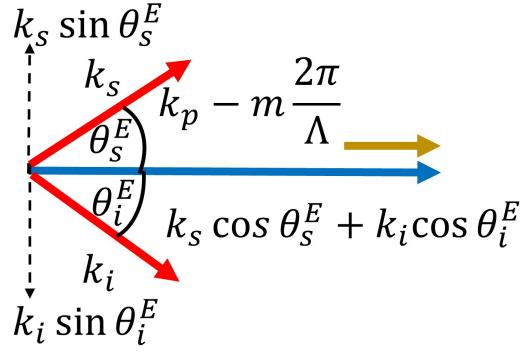


Figure 2.8: Pump, signal, and idler photon momentum vectors and their components. θ_s^E and θ_i^E are the emission angles of the signal and idler photons, respectively.

$$k_s \cos(\theta_s^E) + k_i \cos(\theta_i^E) = k_p - \frac{2\pi}{\Lambda} m \quad (2.36)$$

Also transverse momentum is conserved $\mathbf{q}_p = \mathbf{q}_s + \mathbf{q}_i$ from Eq. 2.26 which gives

$$\begin{aligned} 0 &= k_s \sin(\theta_s^E) - k_i \sin(\theta_i^E) \\ k_s \sin(\theta_s^E) &= k_i \sin(\theta_i^E) \end{aligned} \quad (2.37)$$

for degenerate case the above equation gives $\theta_s^E = \theta_i^E = \theta^E$ (let), then from Eq.

2.36

$$\theta^E = \cos^{-1} \left(\frac{k_p - \frac{2\pi}{\Lambda} m}{2k_s} \right) \quad (2.38)$$

In three dimensions, we need to consider all possible $\mathbf{k}$ vectors which will lie on the surface of a cone of emission angle θ^E . On the transverse plane after the nonlinear crystal, we obtain the annular ring-shaped spatial profile shown in Fig. 2.9. We achieve the annular width of the ring due to slight phase-mismatching. In our lab, we experimentally generate Type-0 SPDC rings, which we use as a photon source for our QRNG and QKD works in the core chapters.

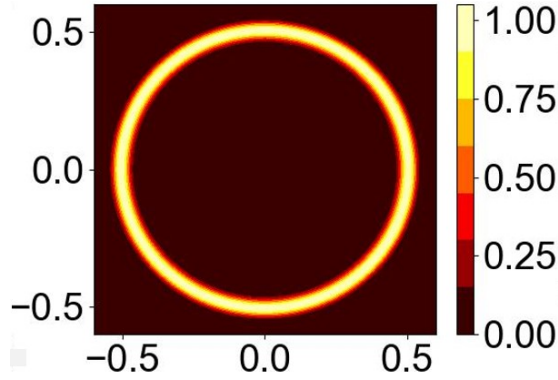


Figure 2.9: Numerically obtained SPDC ring spatial profile.

2.3.3 Bi-photon generation efficiency

In the following chapter, we will utilize Type-0 non-collinear degenerate SPDC for applications in QRNG, QKD, and quantum networks. Here, we will discuss why PPKTP with degenerate Type-0 phase matching in non-collinear geometry is the most suitable option for our work, as the brightness of correlated photon pairs is optimal for this specific case. To understand the efficiency, we consider ‘g’ from Eq. 2.23

$$g = -\frac{i}{\hbar} \epsilon_0 L d_{eff} A_p A_s^* A_i^* \quad (2.39)$$

Where,

$$\begin{aligned} A_p &= \sqrt{\left(\frac{2\mu_0 c}{n_p}\right)} I_p \\ A_k^* &= \sqrt{\frac{\hbar \omega_k}{2\varepsilon_0 n_k^2 V_Q}} \end{aligned} \quad (2.40)$$

With this substitution

$$g = -\frac{i}{2V_Q} \sqrt{2\mu_0 c} d_{eff} L I_p \sqrt{\frac{\omega_s \omega_i}{n_p n_s^2 n_i^2}} \quad (2.41)$$

First, we understand the role of d_{eff} in the SPDC generation rate. In Eq. 2.8 we substituted $P^{(2)}(\mathbf{r}, t) = \chi^{(2)} \mathbf{E}^2(\mathbf{r}, t)$ where $\chi^{(2)}$ is tensor of $3 \times 3 \times 3$ but due to symmetry we can write it as 3×6 matrix [66] considering the crystal along the z axis in Fig. 2.4

$$\begin{bmatrix} P_z(\omega_3) \\ P_x(\omega_3) \\ P_y(\omega_3) \end{bmatrix} = 4\varepsilon_0 \begin{bmatrix} d_{11} & d_{12} & d_{13} & d_{14} & d_{15} & d_{16} \\ d_{21} & d_{22} & d_{23} & d_{24} & d_{25} & d_{26} \\ d_{31} & d_{32} & d_{33} & d_{34} & d_{35} & d_{36} \end{bmatrix} \times \begin{bmatrix} E_z(\omega_1)E_z(\omega_2) \\ E_x(\omega_1)E_x(\omega_2) \\ E_y(\omega_1)E_y(\omega_2) \\ E_x(\omega_1)E_y(\omega_2) + E_y(\omega_1)E_x(\omega_2) \\ E_z(\omega_1)E_y(\omega_2) + E_y(\omega_1)E_z(\omega_2) \\ E_z(\omega_1)E_x(\omega_2) + E_x(\omega_1)E_z(\omega_2) \end{bmatrix}. \quad (2.42)$$

If we consider the PPKTP crystal belongs to the point group 2mm, then the above equation simplifies to Eq. 2.43 where a total of six elements are non-zero, and others

are zero. Also, if the crystal is along the z direction, the z component of polarisation and electric field vanishes. x and y components are the o and e polarized components.

$$\begin{bmatrix} 0 \\ P_o(\omega_p) \\ P_e(\omega_p) \end{bmatrix} = 4\epsilon_0 \begin{bmatrix} 0 & 0 & 0 & 0 & 1.9 & 0 \\ 0 & 0 & 0 & 3.6 & 0 & 0 \\ 2.5 & 4.4 & 16.9 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 \\ E_o(\omega_s)E_o(\omega_i) \\ E_e(\omega_s)E_e(\omega_i) \\ E_o(\omega_s)E_e(\omega_i) + E_e(\omega_s)E_o(\omega_i) \\ 0 \\ 0 \end{bmatrix} \quad (2.43)$$

After doing the matrix multiplication we get two equations. 1st equation is

$$P_o(\omega_p) = 4\epsilon_0 3.6 (E_o(\omega_s)E_e(\omega_i) + E_e(\omega_s)E_o(\omega_i)) \quad (2.44)$$

It implies $o \rightarrow o + e$ or $e + o$ i.e. Type-II SPDC with $d_{eff} = 3.6$. And the 2nd equation

$$P_e(\omega_p) = 4\epsilon_0 (4.4 E_o(\omega_s)E_o(\omega_i) + 16.9 E_e(\omega_s)E_e(\omega_i)) \quad (2.45)$$

1st term in the above equation represents $e \rightarrow o + o$ i.e. Type-I SPDC with $d_{eff} = 4.4$ and the second term represent the Type-0 SPDC with quasi-phase matching with higher $d_{eff} = 16.9$ as it is $e \rightarrow e + e$ conversion. This d_{eff} is one of the parameters for the generation rate of the SPDC process. For type-0 SPDC, a higher value of d_{eff} indicates a higher generation of correlated photon pairs than the Type-I and Type-II SPDC using the PPKTP crystal. So, we chose the Type-0 PPKTP crystal for our experiment in the subsequent chapters.

Now, to understand why the generation rate is optimum at the degeneracy of the signal and idler, we need to consider the function $f(\omega_s) = \sqrt{\omega_s \omega_i} = \sqrt{\omega_s(\omega_p - \omega_s)}$ from Eq. 2.41. For the maximization of this function, $\frac{df(\omega_s)}{d\omega_s} = 0$ and $\frac{d^2f(\omega_s)}{d^2\omega_s} < 0$ which gives the solution $\omega_s = \omega_p/2$ and $\omega_i = \omega_p/2$ indicating $\omega_s = \omega_i$ so at degeneracy, we get the optimum generation rate.

As we discussed earlier, at temperatures lower than the degeneracy temperature, we observe non-collinear emission of biphotons, with the angle of emission decreasing as the crystal temperature increases. The generation then shifts to a collinear geometry. From Eq. 2.41, the generation efficiency is inversely proportional to the pump, signal, and idler refractive indices. At collinear generation, the temperature is higher, so the refractive indices are higher than in the non-collinear geometry, which causes a decrease in the generation rate compared to the non-collinear bi-photon emission. Hence, we utilize a Type-0 PPKTP crystal in a degenerate, no-collinear configuration. We further characterize and optimize the source brightness and quantumness in the upcoming chapter with various collection scenarios for high-key-rate QRNG and QKD applications.

Chapter 3

Optimization of Sources Brightness and Quantumness

We present a comprehensive experimental study of a heralded single-photon source based on SPDC, optimized for high-purity photon generation and entanglement-based quantum applications. By systematically varying the coincidence window width, spectral filtering, collection fiber type, and pump power, we quantify their impact on key figures of merit: the second-order correlation function $g^{(2)}(0)$, Hong-Ou-Mandel (HOM) interference visibility, and entanglement visibility. Reducing the coincidence window to 1 ns minimizes $g^{(2)}(0)$ to 0.017 at low powers and yields the highest HOM visibility of 91%, indicating superior single-photon purity and indistinguishability. Among spectral filters, a 10 nm bandpass filter provides an optimal balance between count rate and quantum performance, maintaining high HOM visibility and low $g^{(2)}(0)$ across powers. Single-mode fiber collection further suppresses multiphoton contributions compared to multimode and few-mode fibers, preserving quantum characteristics even at elevated pump powers. We establish a linear relationship be-

tween HOM visibility and $g^{(2)}(0)$, with a slope approaching the ideal behavior of highly pure single-photon sources. Additionally, we demonstrate that the Bell parameter and entanglement visibility degrade with pump power in a manner consistent with $g^{(2)}(0)$ trends, confirming the equivalence of these measures for quantumness certification. Comparative analysis between single-pass and Sagnac configurations reveals similar $g^{(2)}(0)$ dependence on pump power, while entanglement visibility necessitates narrower filtering to maintain coherence between photon pairs. Overall, our results highlight that carefully optimized coincidence windows, spectral filtering, and spatial mode selection are crucial for achieving high-purity, indistinguishable photons suitable for quantum key distribution, quantum random number generation, and entanglement-based protocols. This systematic characterization establishes clear design guidelines for SPDC sources tailored to diverse quantum technology applications.

3.1 Introduction

In the 21st century, our goal is to harness quantum mechanics for quantum technology, revolutionizing computational speed and security in quantum communication. In the context of optical implementations of quantum technologies, security considerations primarily emphasize the quantumness at the detection stage. This quantumness is the direct manifestation of the quantum nature of the source. During quantum measurement, we utilize the particle-like behavior of incoming light by counting the number of incoming photons. A large number of quantum cryptographic schemes, particularly quantum key distribution (QKD), rely on the transmission of single photons through the communication channel [67–69]. The use of multiple photons poses a security risk, as it can permit an eavesdropper to extract information about the key [70, 71]. Additionally, the different degrees of freedom of a photon may be employed to encode a single qubit. Therefore, to increase computational speed, we need to produce

more single photons with quantumness certification for enhanced security. There are different types of sources that can fulfil these two criteria, classified into two types. First one deterministic single-photon sources capable of producing individual photons on demand, including those based on NV centers [72–74], quantum dots (QDs) [75, 76], single atoms [77], single ions [78], single molecules [79], and atomic ensembles [80]. And the second one is the probabilistic single-photon sources, which rely on the generation of photon pairs through processes such as spontaneous parametric downconversion (SPDC) in bulk nonlinear crystals [81, 82] and waveguides [83], as well as four-wave mixing (FWM) in optical fibers [84, 85].

Among these, our interest lies in the most widely used and popular spontaneous parametric down-conversion (SPDC) [86, 87] based heralded single-photon source and entangled-photon source. This process involves a $\chi^{(2)}$ nonlinear optical interaction, where a high-energy pump photon propagates through a nonlinear medium and spontaneously splits into two lower-energy photons, commonly referred to as the signal and idler. Such photon-pair generation underpins a vast range of applications, including fundamental investigations of quantum theory, advances in quantum information processing, precision measurements in quantum metrology, and secure quantum communication technologies. It is always expected to achieve a higher generation rate from the SPDC process with higher quantumness. However, there is always a trade-off involved. This high photon rate is crucial for achieving a high signal-to-noise ratio [88]. In free-space quantum key distribution, maintaining a high photon rate is crucial for compensating for photon losses caused by atmospheric turbulence. This elevated photon count not only mitigates scattering effects but also plays a vital role in enhancing the performance of various quantum technologies. For example, it enables rapid quantum sensing of minute optical delays using Hong-Ou-Mandel interferometry [89], facilitates faster scanning in quantum optical coherence tomography (QOCT)

[90], and improves the signal-to-noise ratio (SNR) in high-speed quantum imaging systems [24, 91].

In the generation of entangled photon pairs using SPDC, the entanglement between the idler and signal photons originates from vacuum fluctuations and the conservation of energy and momentum. Such entanglement is a fundamental resource for various applications in quantum information science and communication. Depending on the experimental configuration, the signal and idler photons can be entangled in several degrees of freedom, including polarization [15, 16, 92], position-momentum [14, 15], energy-time [13], and orbital angular momentum [17, 18]. To establish entanglement, the photon pair must be produced in a minimum of two distinct modes, such as horizontal and vertical polarization.

To achieve a higher key rate for all the experiments presented in this thesis, the first step was to use a crystal with higher parametric gain and nonlinearity. However, achieving a high nonlinear gain relying solely on a particular phase-matching configuration does not ensure the realization of a high-brightness source of photon pairs. Equally critical is the implementation of an efficient photon collection mechanism, which ensures that the generated photons are effectively captured and directed into the detection system.

Here, we provide a full proof characterization of SPDC-generated biphotons in both single-pass and Sagnac configurations. We first characterized the photon pair source purity and indistinguishability using Hong-Ou-Mandel (HOM) interferometry [93] and $g^{(2)}(\tau)$ [94] in a single-pass configuration. The variation of these two key parameters with pump power, coincidence window, SPDC photon bandwidth, and SPDC photon modes is also studied to determine the optimal conditions for different applications. Next, we moved on to the Sagnac configuration for generating and analyz-

ing polarization-entangled photon pairs. In this configuration, we have also measured the $g^{(2)}(\tau)$ correlation and performed a comparative study with the single-pass configurations. We also estimate another most fundamental Bell parameter (S) from the Sagnac configuration and compare this with $g^{(2)}(0)$ with increasing multiphoton events in terms of pump power. Finally, conclude by summarizing the optimized conditions in terms of pump power, coincidence window, SPDC photon bandwidth, and SPDC photon modes for various quantum technology applications.

3.2 Background

3.2.1 Purity parameter $g^{(2)}(0)$ of a HSPS

In quantum optics, measuring the second-order correlation $(g^{(2)}(\tau))$ has proven crucial, particularly when seeing antibunching, a feature that is exclusively related to quantum mechanics. The correlation between two photons separated by a temporal delay, τ , is obtained from the Hanbury Brown-Twiss (HBT) experiment [12].

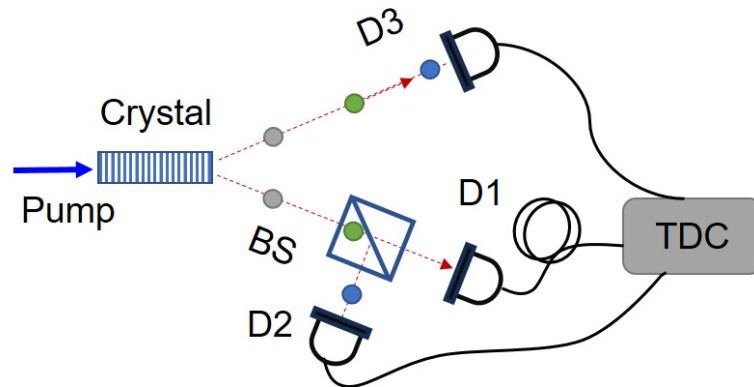


Figure 3.1: Schematic of HBT-like setup for a heralded single-photon source in which the corresponding idler photons emerge after passing through the beam splitter, follow any of the two possible paths leading to zero coincidence counts between detectors D1, D2, and D3.

As shown in Fig. 3.1, an ideal heralded single-photon source would emit single pair photons (green) at a time, and next pair-photons (grey) generated at different times. The correlated pairs of photons are shown in the same color in the signal and idler arms. Idler photon (green color Idler) at the beam splitter would either be transmitted (along path 1) or reflected (along path 2). If there is no delay between paths 1 and 2 ($\tau = 0$), then there are no simultaneous detections at the detectors D1, D2, & D3. In the HBT experiment, photon correlation in the signal (s) with the conditioned detection of idler (i) is required for heralded single-photon sources produced by SPDC (Fig. 3.1). The second-order correlation function for this configuration takes the form [94],

$$g^2(\tau) = \frac{C_{123}S_3}{C_{13}C_{23}} \quad (3.1)$$

where S_3 represents single counts of D3 in the heralding arm; C_{13} and C_{23} respectively represents two-fold coincidence counts of D1 & D3 and D2 & D3 detectors pairs. C_{123} represents three-fold coincidence counts of all the three detectors D1, D2, and D3. A lower $g^2(0)$ value indicates that the time interval between consecutive photons in the photon stream is almost uniform, which results in the purity of the single photon.

3.2.2 Indistinguishability parameter V_{HOM} of a HSPS

Another notable quantum-optical effect is Hong-Ou-Mandel (HOM) interference. Two indistinguishable photons impinging on separate inputs of a 50:50 beam splitter undergo interference and exit together from a single output port. This behavior arises from the quantum mechanical principles governing two-photon interference and is known as Hong-Ou-Mandel interference, but it was earlier reported by Fearn et al.

[95] and experimentally observed at nearly the same time by Rarity et al. [96, 97]. Its experimental observation has provided valuable insights into the behavior of pair-photons and the action of beam splitters. In the formalism of quantum optics, a balanced beam splitter transforms the input field modes a and b into output modes c and d via a unitary transformation [98]:

$$\begin{cases} \hat{a} = \frac{\hat{c} + \hat{d}}{\sqrt{2}} \\ \hat{b} = \frac{\hat{c} - \hat{d}}{\sqrt{2}} \end{cases} \quad (3.2)$$

Consider a situation in which two indistinguishable photons reach the beam splitter with a temporal delay τ . Applying the beam splitter transformation to the two-photon input state yields:

$$\begin{aligned} \hat{a}_t^\dagger \hat{b}_{t+\tau}^\dagger |0\rangle &\xrightarrow{\text{BS}} \frac{1}{2} (\hat{c}_t^\dagger + \hat{d}_t^\dagger) (\hat{c}_{t+\tau}^\dagger - \hat{d}_{t+\tau}^\dagger) |0\rangle \\ &= \frac{1}{2} \left(\hat{c}_t^\dagger \hat{c}_{t+\tau}^\dagger - \hat{c}_t^\dagger \hat{d}_{t+\tau}^\dagger + \hat{d}_t^\dagger \hat{c}_{t+\tau}^\dagger - \hat{d}_t^\dagger \hat{d}_{t+\tau}^\dagger \right) |0\rangle \end{aligned} \quad (3.3)$$

This expression reveals four possible outcomes based on the detection of photons. The first and last terms describe both photons emerging from the same port (photon bunching), while the middle two terms correspond to photons exiting from different ports (anti-bunching). In the ideal case where the photons are truly indistinguishable and arrive simultaneously $\tau = 0$, quantum interference eliminates the anti-bunching terms, resulting in zero coincidence counts — a signature of the HOM effect. Then the Eq. 3.3 changes to the following expression using the standard bosonic commutation relations

$$\begin{aligned}
\hat{a}_t^\dagger \hat{b}_t^\dagger |0\rangle &\xrightarrow{\text{BS}} \frac{1}{2} \left(\hat{c}_t^\dagger \hat{c}_t^\dagger - \cancel{\hat{c}_t^\dagger \hat{d}_t^\dagger} + \cancel{\hat{d}_t^\dagger \hat{c}_t^\dagger} - \hat{d}_t^\dagger \hat{d}_t^\dagger \right) |0\rangle \\
&= \frac{1}{\sqrt{2}} (|2\rangle_c - |2\rangle_d)
\end{aligned} \tag{3.4}$$

The above expression highlights the foundation of Hong-Ou-Mandel (HOM) interference. For two indistinguishable photons, destructive interference eliminates the possibility of the photons exiting through different ports. Instead, they preferentially exit together through the same port, leading to the appearance of a characteristic dip in the coincidence detection rate. This reduction occurs when the temporal separation between the arriving photons is within the coherence time of their wave packets. As a result, the HOM dip serves as a direct signature of quantum interference and indistinguishability between photons. The contrast of the interference fringes known as visibility V_{HOM} which provides a quantitative measure of how indistinguishable the two single photons are. This key parameter is defined by the expression:

$$V_{\text{HOM}} = \frac{C_{\text{max}} - C_{\text{min}}}{C_{\text{max}}} \tag{3.5}$$

where C_{max} and C_{min} denote the maximum and minimum values of the coincidence counts, respectively. Consequently, the depth and width of the HOM dip become indicators of the photons' coherence properties.

3.2.3 Bell parameter S of an entangled photon source

The Bell parameter is the most fundamental parameter connected with the Bell's theorem and the quantumness of an entangled state. To understand the Bell parameter,

we must first understand what the Bell's theorem is and why it was needed. It was needed to correct Einstein's statement regarding quantum mechanics. In 1935, Einstein first asked the question, Is quantum mechanics truly random, and is it a complete theory? [5] His thought was that there should be some hidden variable for which quantum mechanics looks apparently random to us, like classical mechanics, and it is not a complete theory. To understand the hidden variable, we can consider a gas system within a container. Classical statistical mechanics can relate the pressure and temperature of the system, but it cannot tell about the exact position and momentum of each gas molecule due to the complexity of the large number of molecules that actually exist. These exact positions and momenta are the hidden variables for this classical system.

Similarly, in quantum mechanics, if we consider a polarised entangled state in Eq.

3.6

$$\begin{aligned}
 |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) = \frac{1}{\sqrt{2}}(|DD\rangle + |AA\rangle) \\
 &= \frac{1}{\sqrt{2}}(|RR\rangle + |LL\rangle) \\
 |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|HH\rangle - |VV\rangle) = \frac{1}{\sqrt{2}}(|DA\rangle - |AD\rangle) \\
 &= \frac{1}{\sqrt{2}}(|RL\rangle - |LR\rangle)
 \end{aligned} \tag{3.6}$$

and measure the basis H/V. Then, if photon 1 is in H polarisation, photon 2 will also be in H polarisation; otherwise, if we measure photon 1 in V polarisation, the second photon will also be in V polarisation. Einstein's thought is that these two particles have some specific polarisation locally when they are generated, but it is hidden from us;

that's why measurement collapses it into one of the two possible orthogonal outcomes and looks apparently random. Bell in 1964 [6] came with an inequality [7] given in Eq. 3.7 based on the hidden variable theory,

$$|S| \leq 2$$

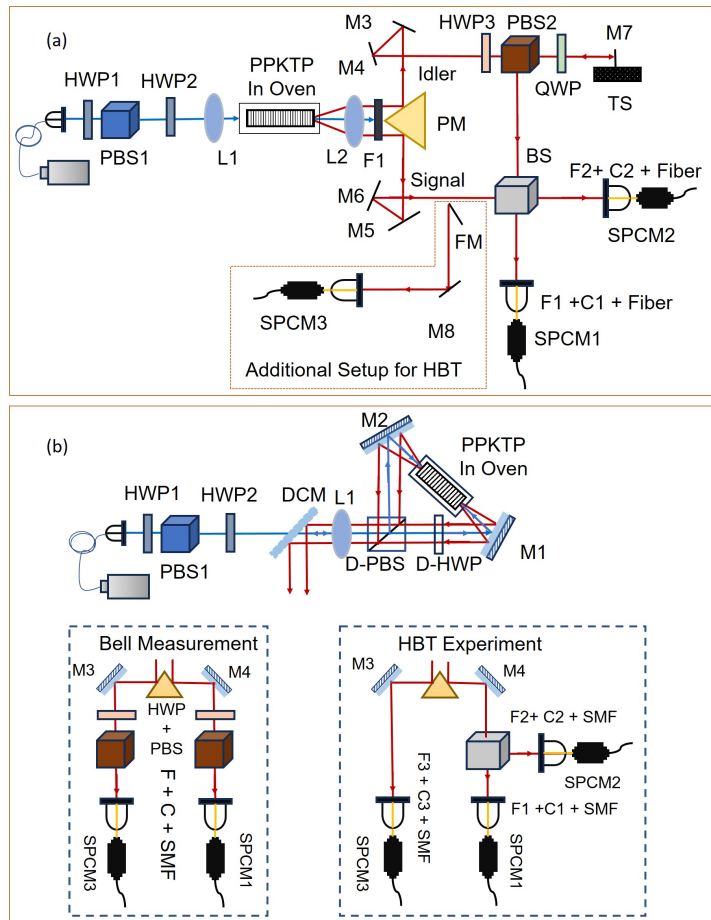
$$|E(\theta_1, \theta_2) + E(\theta_1, \varphi_2) + E(\varphi_1, \varphi_2) - E(\varphi_1, \theta_2)| \leq 2 \quad (3.7)$$

S is known as the Bell parameter and $E(\theta_1, \theta_2) = \int A(\theta_1, \lambda) B(\theta_2, \lambda) \rho(\lambda) d\lambda$, where λ is the hidden variable [99]. Suffixes 1 and 2 in the angles, respectively, indicate the measurements of photons 1 and 2. He showed that quantum mechanics violates this inequality, and the S parameter holds a value in the range $2 < |S| \leq 2\sqrt{2}$. Therefore, he proposed the famous Bell's theorem, which demonstrates the incompatibility between quantum mechanics and local hidden-variable descriptions. The angles $\theta_1, \theta_2, \varphi_1$, and φ_2 can be calculated numerically by finding the optimal solution of S expression. Now, from the coincidence count values for 16 different angle pairs of photon 1 and photon 2 arm, we can calculate the E values experimentally, hence the S parameter. The entanglement visibility (V_{Ent}) is given by Eq. 3.8

$$V_{Ent} = \frac{S}{|2\sqrt{2}|} \quad (3.8)$$

3.3 Experiment

The schematic diagrams for the two experimental setups shown in Fig. 3.2 are presented. The top one represents the single-pass configuration for correlated photon pair generation, as illustrated in Fig. 3.2a. The bottom, Fig. 3.2b, is the Sagnac interferometric configuration for entangled photon pair generation. Photon pairs are generated by pumping a type-0 PPKTP nonlinear crystal (Raicol, $1 \times 2 \times 20$ mm with $3.425 \mu\text{m}$ polling period) kept at 38.0°C within an oven with temperature stability of $\pm 0.1^\circ\text{C}$. We used a larger length of 20 mm Type-0 PPKTP crystal, as it produces a higher generation rate without any signal and idler walk-off issues. A continuous-wave, single-frequency laser diode generates an output power of 25 mW at a central wavelength of 405 nm (Toptica Topmode), with a spectral bandwidth (full width at half maximum) of approximately 20 MHz, acting as the pump laser. A spatial filtering unit, comprising two couplers and a single-mode fiber (SMF), is used to ensure the TE_{00} pump mode. A combination of the half-wave plate (HWP1) and a polarizing beam splitter (PBS) cube can split the laser output into orthogonally propagating horizontal and vertically polarized beams, and control the power over the two polarized beams. We take the horizontally polarized part from the PBS transmission port and further change the polarization to vertical using a half-wave plate (HWP2), as our crystal is designed for this specific polarization. A combination of lenses L1 and L2 is used to focus the pump beam at the center and collimate the SPDC ring. The photons from the collimated ring need to be coupled into a fiber using a coupler for various experimental purposes. The coupler is a mechanical system with many degrees of freedom that allows for the collection of incoming photons using an objective lens with a high numerical aperture. In this collection scheme, optimization is achieved through the proper choice of L1 and L2, as well as the fiber and filter. L1 and L2, respectively,



bury, Brown, and Twiss (HBT) experiment configured with three single-photon avalanche photodiodes (SPAD)(Excelitas SPCM-AQRH-14-FC, dark counts ~ 100 cps), we split the signal and idler photons using the prism mirror. M3 and M4 are the two mirrors to align the idler path along a straight line. HWP3 rotates the incoming V-polarized light to H-polarized light, which passes through the quarter-wave plate (QWP) kept at a 45° angle and turns into left circularly polarized (LCP) light. This LCP is further reflected by a mirror (M7) housed on a translation stage and becomes right circularly polarized (RCP). QWP again transforms it to V-polarised light, which is further reflected by the PBS2 towards the one input port of BS. The signal photon was also guided to the other input port of the BS using the two other mirrors. The path length for both the signal and idler photons remained the same. Two SPADs (SPCM1 & SPCM2) collect the incoming photons using a fiber-coupling assembly, which consists of a filter, a mechanical coupler, and a fiber. Now, if we change the optical delay of the idler photon path by moving M7 using a motorized translation stage, we can observe a variation in the coincidence counts of the two detectors with a dip at zero time delay between the two paths. This is the experimental arrangement for HOM interferometry.

For doing the HBT experiment, we deviate the signal photons from their path using a flip mirror to the third detection system. This is known as the heralding photon. The idler photon stream is divided into two paths using a nearly 50:50 beam splitter (BS). In Fig. 3.2a, we use a time-to-digital converter (TDC) (Time Tagger Ultra, Swabian Instrument), which itself can introduce different amounts of delay in its different channels before doing the counting measurements. We set delays of 16 ns after SPCM 2 and 3 before counting by TDC. Now, using the same TDC, we introduce variable delay to the first path after SPCM1 and from a range of 10 ns to 22 ns, which produces a delay in this specific path in the range of -6 ns to $+6$ ns concerning the other two paths, with the variation of the delay in the path 1 we can see the significant change in

the different coincidence counts mentioned in Eq. 3.1, which is noted and further used to calculate the second-order correlation function.

The second experimental setup depicts the Sagnac cavity arrangement shown in Fig. 3.2b, enabling the generation of Bell states by pumping the crystal from both sides. For that, we modified our first single-pass setup Fig. 3.2a, here the 2nd $\lambda/2$ plate is employed to adjust the polarization state of the linearly polarized pump beam, ensuring an equal power distribution between the clockwise (CW) and counterclockwise (CCW) beams inside the polarization Sagnac interferometer. This interferometer consists of a dual-wavelength PBS (D-PBS) optimized for 405 nm and 810 nm, along with two plane mirrors, M1 and M2. The pump beam is focused using an L1 lens with a focal length of 150 mm, forming a spot size of approximately $42 \mu\text{m}$ at the center of the non-linear crystal, which is positioned between M1 and M2.

Inside the interferometer, a dual-wavelength half-wave plate ($D-\lambda/2$) is aligned such that its optic axis is rotated by 45° relative to the vertical direction. This ensures that the horizontal polarization is converted to vertical and vice versa for both 405 nm and 810 nm wavelengths. As the nonlinear medium, a 20 mm-long periodically-poled potassium titanyl phosphate (PPKTP) crystal with a grating period (Λ) of $3.425 \mu\text{m}$ and a $1 \times 2 \text{ mm}^2$ aperture is employed to generate degenerate spontaneous parametric downconversion (SPDC) photons at 810 nm through a non-collinear, type-0 ($e \rightarrow e + e$) phase-matching process. The crystal is maintained at a controlled temperature within an oven that offers the stability of $\pm 0.1^\circ\text{C}$ and operates up to 200°C .

The CW and CCW pump beams, influenced by the $D-\lambda/2$ plate, generate entangled photon pairs distributed in an annular ring with orthogonal polarization states. Upon recombination at the D-PBS, the SPDC photons exhibit an annular ring distribution, with pairs of photons located at diametrically opposite points on the ring. The

resulting quantum state of the photon pairs is given by $|\phi^\pm\rangle = (|HH\rangle \pm |VV\rangle)/\sqrt{2}$, representing a Bell state. The SPDC photons are then collimated using the same lens L1 and separated from the pump beam using a dichroic mirror (DM), which is positioned between L1 and the second $\lambda/2$ plate.

To segment the SPDC ring, a gold-coated prism mirror (PM) is used to divide it into two halves. Diametrically opposite points of these sections contain entangled heralded photon pairs, enabling their utilization in Bell measurement and HBT experiment. For the Bell measurement, the photons of the two sections pass through the polarization analyzer, which consists of a $\lambda/2$ plane and PBS at 810 nm wavelength, before being collected using the coupling system (Filter (F) + Coupler (C) + SMF). After that, we also do the HBT measurement using the two sections as discussed in the earlier paragraph. The time-to-digital converter (TDC) is connected to the SPCMs, and the computer is used for photon counting, time stamping, recording, and experimental data analysis.

3.4 Results and discussion

To identify the best experimental situation for our SPDC-based heralded single-photon source, we first set the pump power at 1 mW. We set different coincident windows in our TDC, starting from 0.5 ns to 5.0 ns with a step size of 0.5 ns. Different coincidence windows vary the parameters in Eq. 3.1, hence the variation in $g^2(\tau)$ observed as shown in Fig. 3.3.

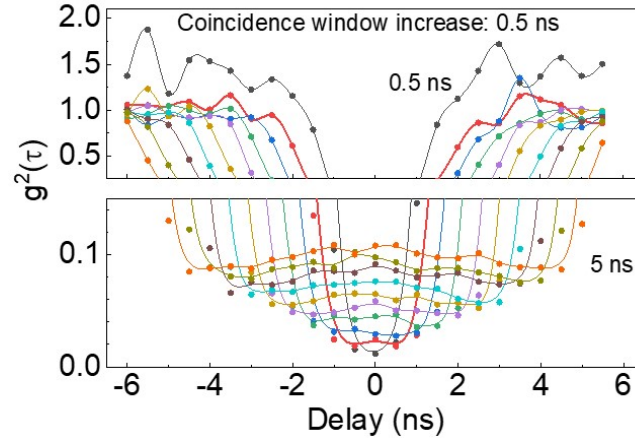


Figure 3.3: The variation of second-order correlation function with delay for different sets of coincidence windows at a pump power of 1 mW.

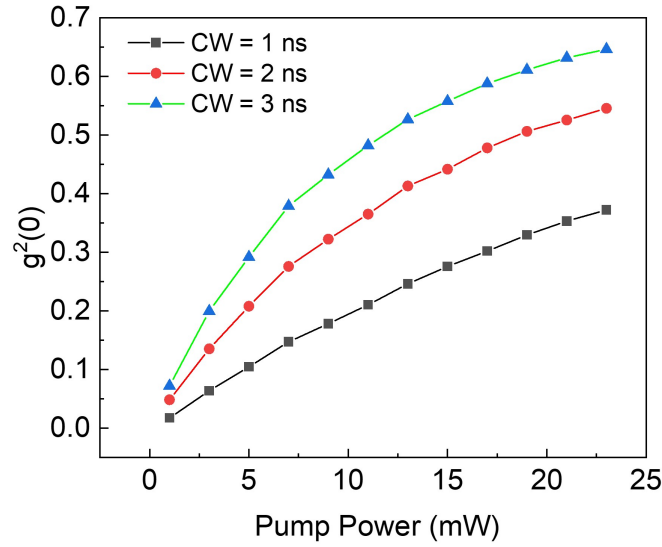


Figure 3.4: The variation of $g^2(0)$ with pump power at three different coincidence window.

For each coincident window, the channel delay after SPCM1 varies over a range of -6 ns to +6 ns to get the $g^2(\tau)$ variation with the time delay. Here, we have shown $g^2(\tau)$ for ten values of the coincident window. It is evident that the width of the central dip is approximately twice the set coincidence window. We can assume that at zero time delay, there is a minimal three-fold coincidence event; this minimal coincidence

condition also holds for time delay of $0 - T_{coin}$ to $0 + T_{coin}$ for a set coincidence window of T_{coin} . The measured value of $g^2(0)$ goes down by choosing shorter coincidence windows. Although the shortest coincidence window (0.5 ns) in our plot produces the lowest $g^2(0)$, due to the jitter (0.3 ns) limitation of our detectors, it is not a right choice of coincidence window. In Fig. 3.4, we have plotted the value of $g^2(0)$ as a function of pump power for three different coincident windows. The results show $g^2(0)$ value increases from 0.01748 to 0.37214, 0.04856 to 0.5455, and 0.07228 to 0.64637, respectively, for the coincident windows of 1 ns, 2 ns, and 3 ns. Theoretically, for a quantum source, $g^2(0) = 0$, but experimentally, the smallest non-zero value, which is close to zero, is an indication of higher single photon purity. Therefore, we achieve the highest purity of a heralded single photon source for a 1 ns window, and the increment slope of $g^2(0)$ with pump power is less steep than that of the other coincidence window. From the graph, it is clear that the variation $g^2(0)$ is linear in fashion at CW = 1 ns, and the higher pump power exemplifies the contribution of multiphoton events; hence, the purity of the SPDC-generated single-photon source degrades with increasing power.

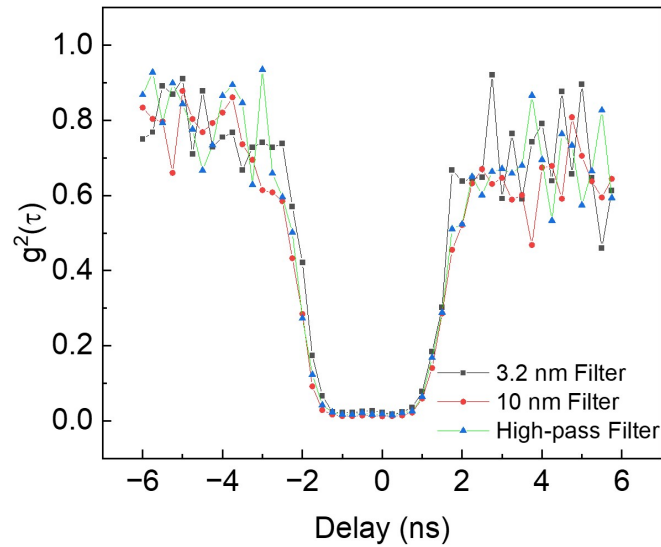


Figure 3.5: The $g^2(\tau)$ plots for three different filters used one after the other within the detection assembly.

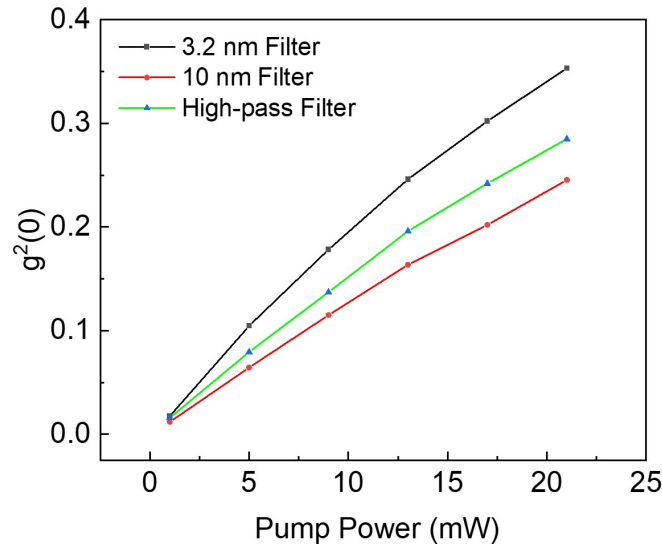


Figure 3.6: The variation of $g^2(0)$ with pump power (set by single count levels) using three different filters at the detection assembly.

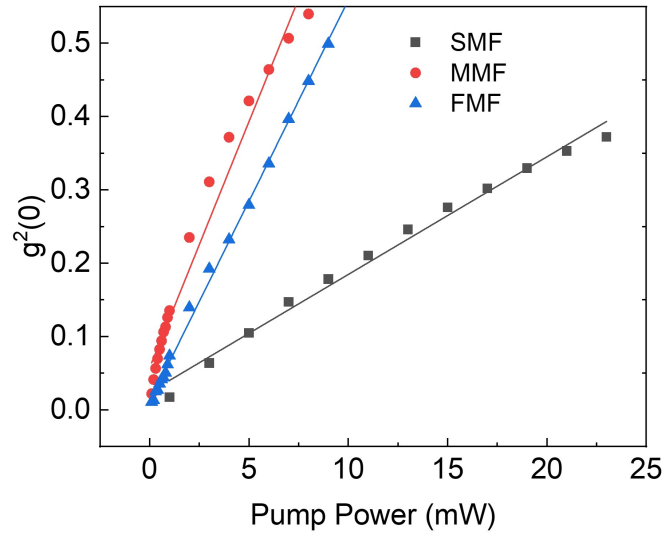


Figure 3.7: The variation of $g^2(0)$ with pump power for different fibers used one after the other.

Next, at a fixed coincidence window of 1 ns, we use different filters in our detection assembly. Figure 3.5 shows the $g^2(\tau)$ plots for three different filters of 3.2 nm, 10 nm, and a high-pass filter (160 nm) used successively within the detection assembly. The width of this plot is independent of the filter bandwidth used for photon collection. The

variation of $g^2(0)$ with the single-count level of the detector for three different filters is shown in Fig. 3.6. We obtain a lower $g^2(0)$ value for a 10 nm filter across all power levels. Additionally, the increment slope is lower for a 10 nm filter, making it the best choice for applications that require a higher bit rate and higher quantum efficiency.

Finally, we change the fiber at the detection end with the 10 nm filter and 1 ns coincidence window. We used three types of fiber: single-mode fiber (SMF), few-mode fiber (FMF), and finally multimode fiber (MMF). The $g^2(0)$ variation with pump power for three different fibers is shown in Fig. 3.7. It is observed that with the increasing power $g^2(0)$ plot touch the $g^2(0) = 0.5$ line for FMF and MMF, but for SMF $g^2(0)$ value increases slowly with increasing pump power, which makes it suitable choice for higher bit rate QRNG and QKD applications staying in the quantum region of the source.

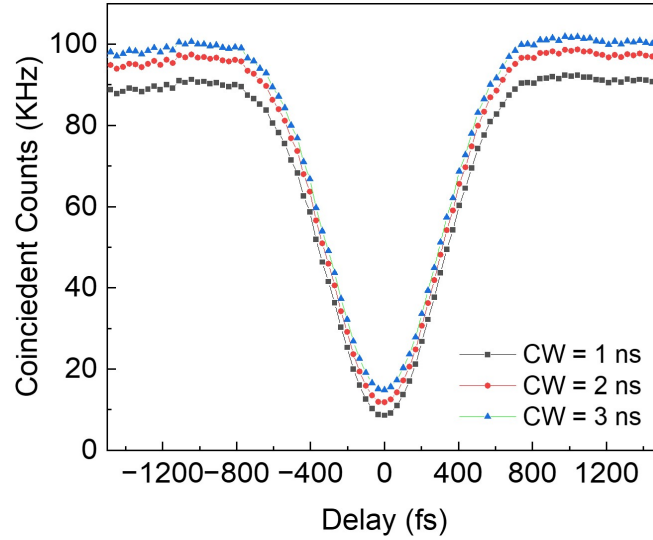


Figure 3.8: The variation of the coincidence rate with the temporal delay between signal and idler photons, which is examined for three coincidence window settings at a pump power of 1 mW.

Next, we come to the indistinguishability measurement using the HOM interferometer. In Fig. 3.8, the coincidence rate drops as the time delay τ between the photons

approaches zero. This behavior follows the shape of an inverted Gaussian, with the experimental data (black points) closely matching the theoretical model (solid black curve). The HOM dip width is the measure of the coherence time of the photon wave packets, characterized by a Gaussian temporal width σ , experimentally determined to be $\sigma = 677.2$ fs for all three sets of coincident windows. The interference visibility in Eq. 3.5 for the measured Hong-Ou-Mandel (HOM) dip is found to be 91%, 88%, and 85%, respectively, at coincidence windows of 1 ns, 2 ns, and 3 ns, indicating a high degree of photon indistinguishability.

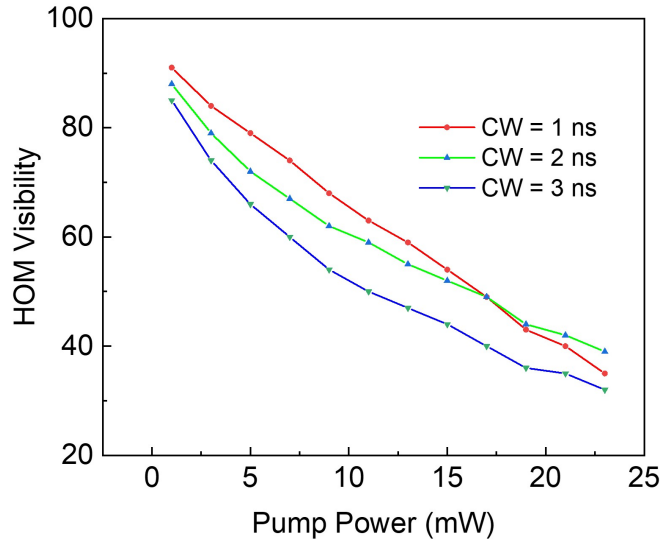


Figure 3.9: The variation of HOM visibility with pump power (set by single count levels) for three different coincident windows. The indistinguishable nature of the SPDC-generated biphoton photons degrades with increasing power due to multiphoton events.

Figure 3.9 shows the dependence of the visibility on the pump power for three different coincidence window widths: 1 ns, 2 ns, and 3 ns. The results indicate that visibility decreases from 91 to 35 for a 1 ns window, from 88 to 39 for a 2 ns window, and from 85 to 32 for a 3 ns window. Ideally, a perfect two-photon quantum interference should exhibit 100% visibility; thus, higher values approaching 100% imply

higher single-photon indistinguishability. Among the three cases, the 1 ns window yields the highest visibility value, indicating the highest indistinguishability. At very high power, the visibility value for a higher coincidence window crosses the visibility value at a 1 ns window, because at high power, the jitter value of the individual detector increases, so a 1 ns window is not sufficient to detect the coincidence event.

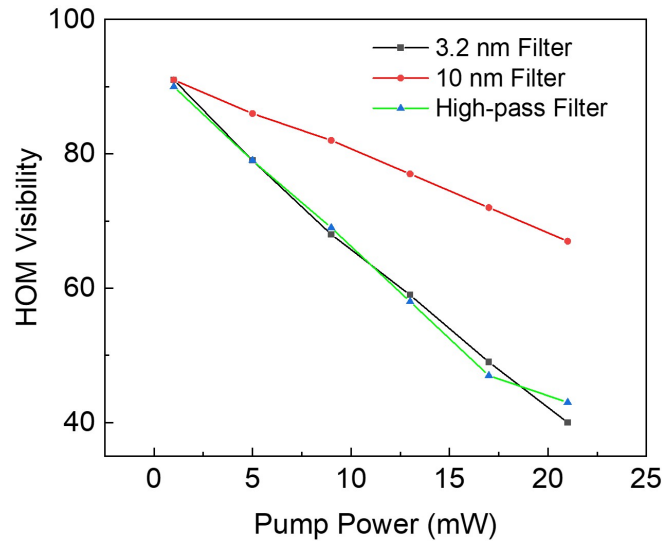


Figure 3.10: The variation of HOM visibility with pump power (set by single count levels) using three different filters at the detection assembly.

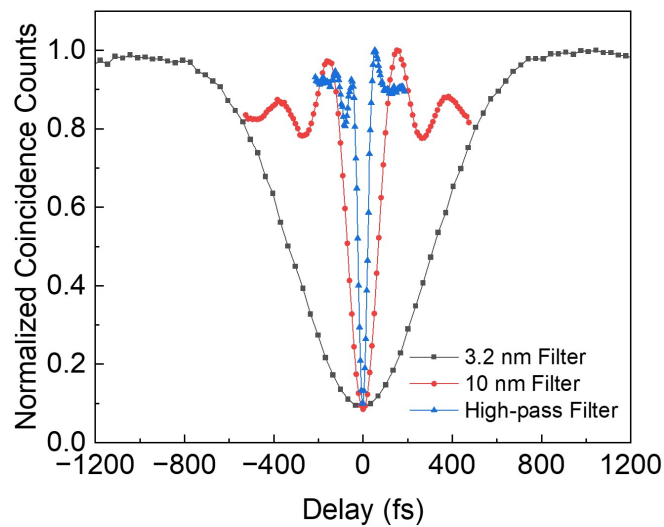


Figure 3.11: The coincidence count rate vs signal and idler photon time delay plots for three different filters used one after the other within the detection assembly.

The linearity of visibility with respect to pump power is most prominent at 1 ns. It also highlights the increased presence of multiphoton events at higher powers, resulting in a degradation of visibility. Furthermore, at a fixed 1 ns coincidence window, we evaluated the impact of spectral filtering by introducing three different filters: a 3.2 nm bandpass filter, a 10 nm bandpass filter, and a 160 nm high-pass filter, similar to the HBT experiment. The corresponding variations in visibility and dip shape with detector single count levels are shown in Figs. 3.10 and 3.11, respectively. Across all count levels, the 10 nm filter consistently yields higher visibility values and exhibits the slowest rate of decrease, making it the most suitable choice for different high-quantumness and high-bit-rate applications, such as QRNG and QKD. It is observed from Fig. 3.11 that the FWHM of the HOM dip becomes broader with narrow filtering. FWHM for this 3.2 nm bandpass filter, 10 nm bandpass filter, and high-pass filter are respectively 677.2 fs, 117.6 fs, and 41.6 fs. As the larger wavelength or frequency bandwidth contributes to a smaller coherence time, i.e., the smaller FWHM of the HOM dip, the wavy appearance in the HOM dip maximum position at high bandwidth filters appears due to non-degenerate wavelength beating. The FWHM and slope of dip are strong parameters in various applications, such as sensing, imaging.

Finally, like the HBT experiment, we replaced the detection-end fiber while keeping the 10 nm bandpass filter and 1 ns coincidence window fixed. The same three types of fibers were tested. The variation of visibility with pump power for each fiber type is presented in Fig. 3.12. It is evident that, with increasing pump power, the visibility values for SMF and FMF approach the classical limit of 50, indicating a stronger presence of multiphoton events. MMF cannot even reach the quantum level (visibility $> 50\%$), even at very low power. The SMF exhibits a significantly slower decrease in visibility with power compared to the FMF, maintaining values well above the classical limit up to 16 mW. This behavior makes SMF the most favorable option for different

sensing applications.

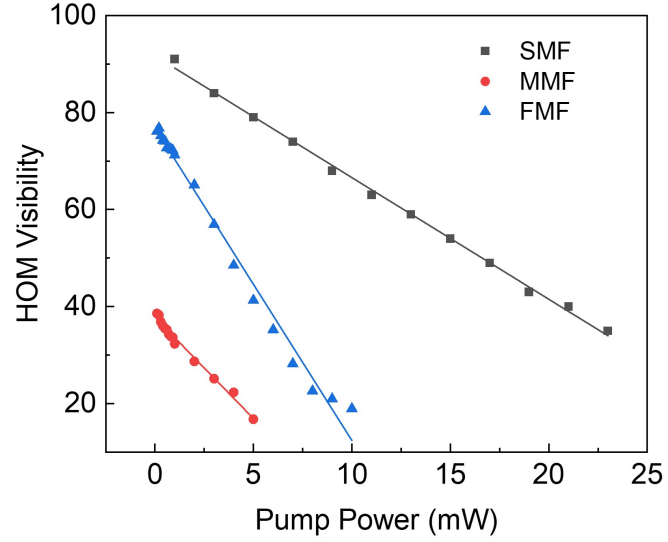


Figure 3.12: The variation of HOM visibility with pump power for different fibers used one after the other.

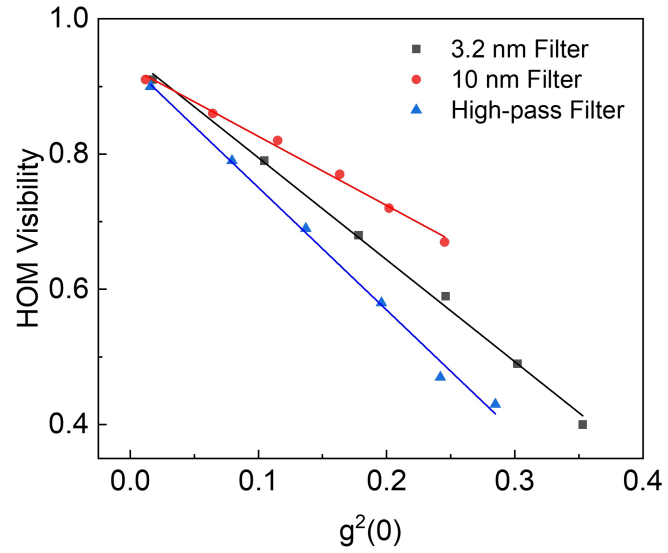


Figure 3.13: The variation of HOM visibility with $g^2(0)$. Solid lines are the fitted lines.

To gain deeper insight into the single-photon purity and the degree of photon distinguishability under varying multiphoton contributions caused by increased pump

power, we plotted the Hong-Ou-Mandel (HOM) visibility V with the second-order correlation function $g^{(2)}(0)$ in Fig. 3.13, using data from Fig. 3.4 and 3.9. These plots demonstrate clear linear dependence (solid lines) between HOM visibility and $g^{(2)}(0)$ for a fixed coincidence window of 1 ns for the three different filters. The observed relationship is given by $V = 0.94 - 1.51 \times g^{(2)}(0)$ and $V = 0.93 - 1.80 \times g^{(2)}(0)$ for 3.2 nm filter and high pass filter respectively, which deviates from the $V \approx 1 - g^{(2)}(0)$ typically expected for highly pure single-photon sources, such as those based on quantum dots [100, 101]. But for the 10 nm filter, the linear equation $V = 0.93 - 1.02 \times g^{(2)}(0)$ well matches with highly pure single-photon sources, with the intercept value of 0.93 ± 0.006 providing a quantitative estimate of the intrinsic indistinguishability of single photons produced by our current source. These are all the experimental outcomes from the single-pass configuration setup. Now, to estimate the bell parameter and visibility, we need to proceed with the Sagnac configuration setup.

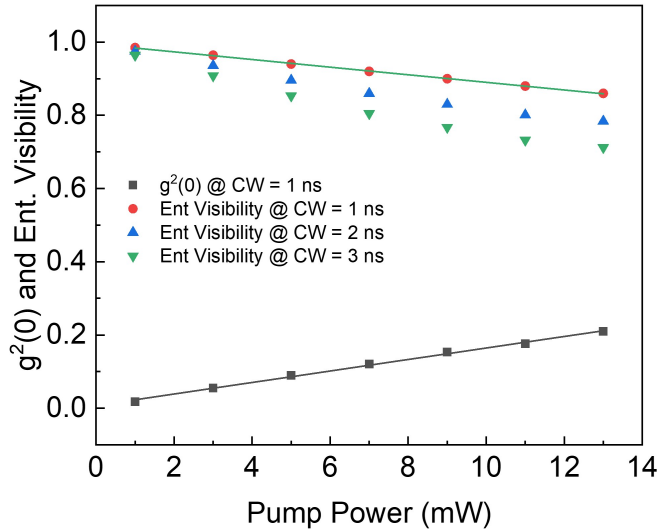


Figure 3.14: The variation of entanglement visibility with pump power (set by single count levels) for three different coincident windows and $g^2(0)$ variation at CW = 1 ns.

The variation of the Bell parameter from the above experimental setup in Fig. 3.2b for different power levels is plotted for three different coincidence windows, as well

as $g^2(0)$ is also plotted for $CW = 1$ ns in the same Fig. 3.14. From the straight-line fit, we found that the rising slope of $g^2(0)$ and the falling slope of visibility are nearly the same, at 0.015 and 0.010, respectively, for a 1 ns coincidence window. This reflects that the quantumness certification using S-parameter is equivalent to the certification using $g^2(0)$.

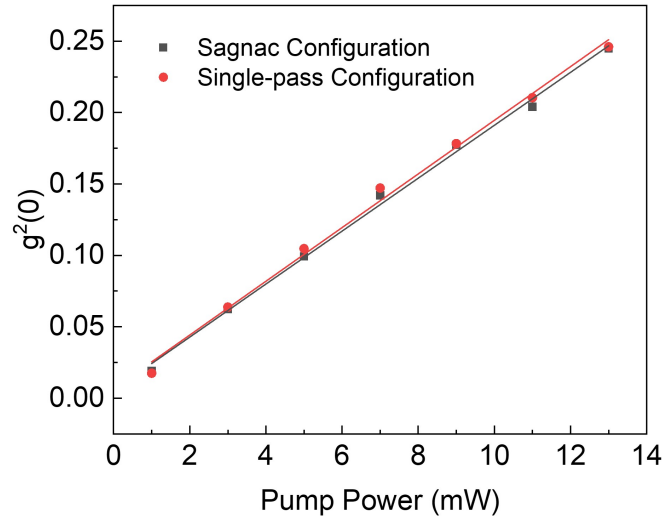


Figure 3.15: The variation of $g^2(0)$ with pump power in single pass configuration and Sagnac configuration.

Also, we studied the variation of $g^2(0)$ with the detector single count label in Fig. 3.15. We observed the variation with power in the Sagnac Fig. 3.2b configuration is almost similar to the variation in the single-pass heralded photon generation configuration in Fig. 3.2a. In both cases, the slope is 0.018/mW. Therefore, a single-pass configuration is sufficient when certifying the quantumness using $g^2(0)$ of a SPDC source for various applications. To find a relationship between entanglement visibility and $g^2(0)$, we plot the values for different power levels shown in Fig. 3.16. It follows the linear equation $V_{Ent} = 0.998 - 0.66g^2(0)$, which indicates for quantum threshold visibility i.e. $V_{Ent} = .71$ we get $g^2(0) = 0.44$, which indicates the upper threshold of quantumness for $g^2(0)$ when we do a one to one comparison.

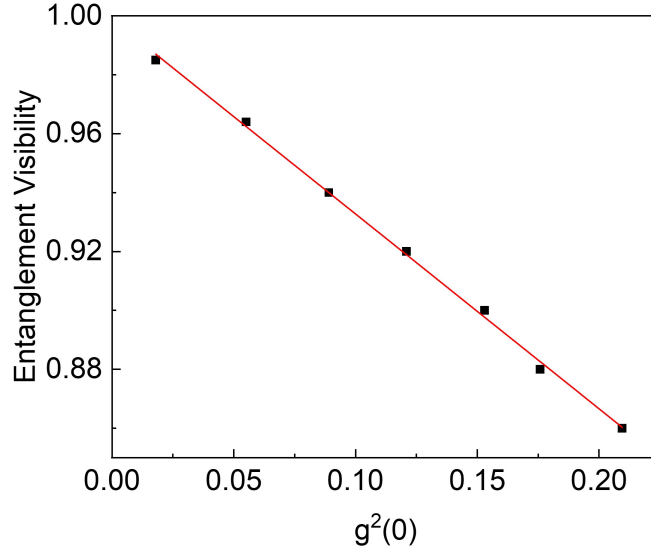


Figure 3.16: Entanglement visibility vs $g^2(0)$ plot. The solid line is the fitted line.

In the earlier section, we observed that a 10 nm filter was the best choice for a single-pass configuration in the experimental setup described in Chapter 4. However, when we move on to our next setup for entangled photon pair generation using the Sagnac configuration, we observed 10 nm filters produce visibility values of 43% and 43% respectively in diagonal (D) and anti-diagonal (A) basis, which is less than the minimum threshold visibility of 71% shown in Fig. 3.17a. So we need to use a 3 nm filter in our couplers for the Sagnac setup, which produces 98% visibility in all four bases (H, V, D, A) shown 3.17b. With decreasing FWHM of the SPDC photon, we increase the coherence time for the HH and VV pair from the Sagnac. By changing the crystal position within the Sagnac, we can easily achieve the time delay between HH pair and VV pair generation below the coherence time. But for 10 nm and a high-pass filter, this coherence time becomes shorter, and we can not achieve a smaller time delay between HH pair and VV pair generation below the coherence time.

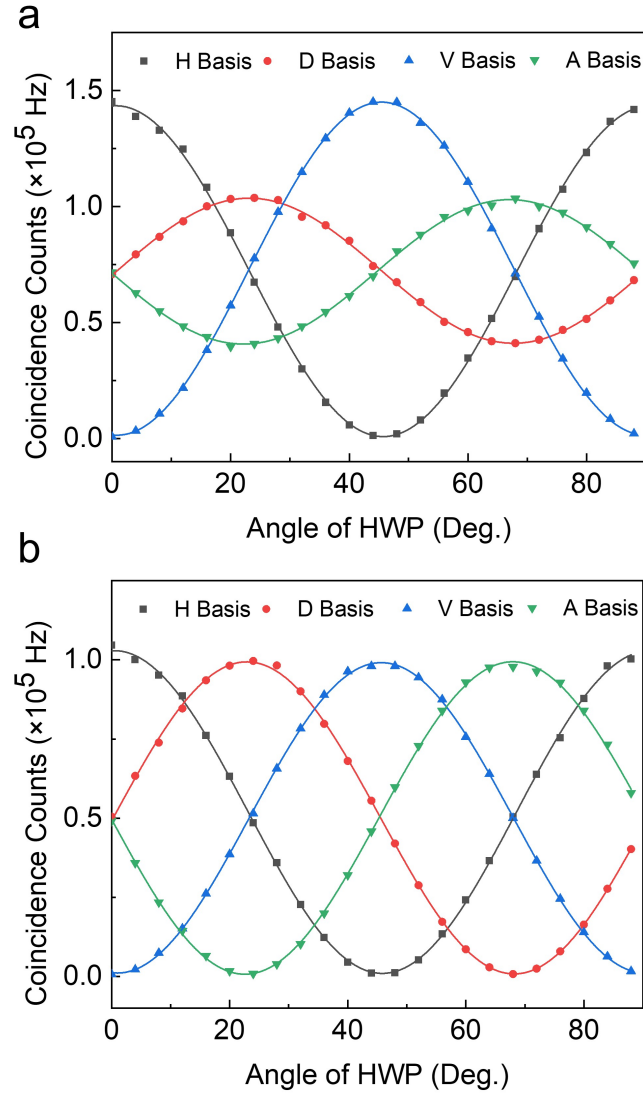


Figure 3.17: The entanglement visibility plot in H, V, D, and A bases for (a) 10 nm filter, (b) 3.2 nm filter.

3.5 Conclusion

In this work, we have systematically characterized a heralded single-photon source based on SPDC process, exploring how critical experimental parameters — coincidence window width, spectral filtering, collection fiber type, and pump power — influence the quantum performance of the source. We demonstrated that narrow coinci-

dence windows and optimized spectral filtering significantly reduce multiphoton contributions, as reflected in lower $g^{(2)}(0)$ values and enhanced Hong-Ou-Mandel (HOM) interference visibility. Single-mode fiber (SMF) collection further improves single-photon purity by effectively suppressing higher-order spatial modes.

Our results establish a clear linear correlation between $g^{(2)}(0)$ and HOM visibility, confirming their equivalence as practical indicators of source quality. We also showed that entanglement visibility and the violation of Bell's inequality degrade predictably with increasing pump power, emphasizing the trade-off between source brightness and quantumness. Finally, by comparing single-pass and Sagnac configurations, we underscored the importance of spectral filtering in preserving coherence for entanglement-based protocols.

Future work can be built on this foundation to enhance photon purity and collection efficiency by integrating crystal design, advanced filtering techniques, and improved detection schemes. These characterization insights of our SPDC source, based on a bulk-crystal implementation, offer concrete guidelines to achieve a high key rate and quantumness for quantum random number generation and quantum key distribution applications in our core chapters. Other state-of-the-art SPDC sources, such as waveguide-based and integrated SPDC platforms, offer higher brightness and more robust generation via diverse phase-matching mechanisms and efficient nonlinear interaction. Furthermore, these can improve the performance for different applications through tailored collection schemes.

Chapter 4

Beamsplitter-free Quantum Random Number Generator using Heralded Single-Photons

Spontaneous parametric down-conversion (SPDC), an inherently random quantum process, produces pair photons with strong temporal and spatial correlations due to energy and momentum conservation, key for quantum random number generation (QRNG). Standard QRNG methods primarily use temporal correlations with beam splitters, limiting bit rates. However, due to spatial correlation, the pair photons in non-collinear phase-matched SPDC-setup appear at diametrically opposite points on an annular spatial distribution. Therefore, exploring the temporal correlation between the spatially correlated photon-pairs from different sections of the annual ring can directly lead to device-independent, multi-bit QRNG at a high rate, eliminating the need of a physical object such as a beam splitter. As a proof-of-concept, we report on high-bit-rate QRNG by using spatial correlation of photon-pairs by sectioning the SPDC ring of

a non-collinear, degenerate, high-brightness source and temporal correlation between the diametrically opposite sections. Dividing the annular ring of the high-brightness photon-pair source based on a 20-mm-long, type-0 phase-matched, periodically-poled KTP crystal into four sections, recording the timestamp of the coincidences (width of 1ns) between photons from diametrically opposite sections and assigning bits (0 and 1), we extracted 90 million raw bits over 27.7s at a pump power of 17 mW. Using minimum entropy evaluation, we determined an extraction ratio of over 95% for raw bits. Further, using Toeplitz matrix-based post-processing, we developed QRNG with bit-rate of 3 Mbps, passing all NIST 800-22 and TestU01 test suites. The generic scheme shows the possibility of further enhancement of bit rate with more sectioning of the SPDC ring.

4.1 Introduction

Random numbers have attracted a great deal of attention in many fields, such as fundamental physics tests, scientific simulations, numerical analysis, decision-making, cryptography [26–28], and many aspects of our everyday lives [40]. Traditional methods to generate random numbers often rely on mathematical algorithms [30]. Despite the increased complexity, the algorithm-based random numbers have pseudorandomness as their prediction or replication cannot be completely ruled out, compromising the security of systems [102]. Therefore, to achieve true randomness - as essential for the highest levels of security, one needs to rely on physical phenomena [31, 32], which are intrinsically random. Quantum mechanical processes [33], with their inherent probabilistic behavior, offer a natural and reliable basis for quantum random number generation (QRNG) with high security.

Over the years, QRNGs have been explored in numerous approaches, including single-photon emitters [103, 104], defect centers [105], phase noise [106], and quan-

tum vacuum [107–110] and phase fluctuations [111], and many other physical processes [112–118]. The truly random bits have also been explored using spontaneous parametric down-conversion (SPDC) based heralded single photons, and single photon entanglement states [28, 119–122]. One of the simplest implementations of a QRNG is the use of a single-photon source directed toward an ideal 50:50 beam splitter and exploring the temporal correlation (antibunching) of the photons to generate random bits. However, these approaches require both an efficient single-photon source and a perfectly unbiased, lossless beam splitter, which are technologically challenging. The use of attenuated optical pulses has also been explored as an alternative to single-photon sources in these beam splitter-based QRNGs. Nevertheless, enhancing source efficiency, collection, detection efficiency, and addressing the bias and additional presence as a device of beam splitters remain critical challenges in QRNG implementation. Again, the low collection efficiency (ratio of coincidence counts and singles count) [92] of the heralded photons in a certified QRNG architecture results in a lower bit rate typically in the Kbps (4.4 Kbps [119]). Therefore, it is imperative to explore new experimental schemes to improve the overall bit rate of the QRNG systems based on the temporal correlation of heralded single photons.

Here, we present a novel experimental approach for a QRNG that operates without the use of a beam splitter with high bit rates by exploiting the pronounced temporal and spatial correlations present between photon pairs generated through the SPDC process. The beam-splitter-free scheme with $g^{(2)}(0)$ value certifying the quantumness of the source makes it a device-independent scheme for QRNG. Using a 20-mm long periodically-poled potassium titanyl phosphate (PPKTP) crystal, pumped with a continuous-wave diode laser, we have generated non-collinear, degenerate SPDC photons in an annular intensity profile. Owing to the momentum matching condition, pair photons are generated at diametrically opposite points with strong temporal correla-

tions and exhibit random spatial distribution around the ring. By dividing the annular spatial profile into four sections and measuring coincidences between photons from opposite sections, we generate random bits with a min-entropy exceeding 95%, ensuring high efficiency in extracting true random bits. Using Toeplitz matrix-based post-processing, our QRNG system achieves a bit rate of 3 Mbps, passing all NIST 800-22 and TestU01 statistical test suites. This experiment shows that the QRNG bit rate can be further enhanced by dividing the ring into additional sections, such as 8, 16, or 32, to develop a multi-bit QRNG system. Although we divided the ring into sections using a series of mirrors, and the mirrors may be functionally equivalent to beam splitters, however, their inclusion in the current setup is not essential for random number generation. The mirrors in the current experiment are necessitated by resource limitations in our lab for directing photons to the detection system. In principle, a microlens-based fiber detection system or a SPAD camera could directly collect photons from the SDPC ring without sectioning, thereby eliminating the need for mirrors or beamsplitter and establishing the current scheme as a beamsplitter-free QRNG system. Unfortunately, due to the unavailability of such advanced systems in our lab, we had to rely on mirrors for photon guidance.

4.2 Experiment

The concept of QRNG using both temporal and spatial correlations, along with a experimental layout is illustrated schematically in Fig. 4.1. Panel (a) of this figure shows that photons generated via degenerate SPDC from type-0, non-collinear phase-matching display a characteristic annular spatial profile. This is divided into four sections labeled as upper (U1, U2) and lower (D1, D2). Since the diametrically opposite sections contain correlated pair photons (spatial correlation), we measured coincidences (temporal correlation) between sections (U1, D2) and (U2, D1), subse-

quently assigning the bits “0” and “1,” respectively. As the pair photons randomly appear in sections (U1, D2) and (U2, D1), this method produces a sequence of random bits of 0 and 1. The novel concept is implemented using the schematic shown in Fig. 4.1(b), where a continuous-wave, single-frequency laser diode generates an output power of 25 mW at a central wavelength of 405 nm (Integrated Optics MatchBox 0405L-25A), with a spectral bandwidth (full width at half maximum) of approximately 20 MHz, acting as the pump laser. Operating the laser at its highest power to ensure optimum performance, the power attenuator composed of a half-wave plate ($\lambda/2$ plate) and a polarizing beam splitter (PBS) cube is used to control the laser power in the experiment. A second $\lambda/2$ plate, placed after the beam collimating lenses, L_1 (focal length, $f = 100$ mm) and L_2 (focal length, $f = 150$ mm), is used to adjust the polarization state of the pump laser to ensure optimum phase-matching, depending on the orientation of the nonlinear crystal. A 20-mm long, 1×2 mm² aperture periodically-poled potassium titanyl phosphate (PPKTP) crystal, with a single grating period of $\Lambda = 3.425$ μ m, is used to generate degenerate SPDC photons at 810 nm through non-collinear, type-0 ($e \rightarrow e + e$) phase-matching. The crystal is housed in an oven, with the temperature variable up to 200degC and stability of ± 0.1 degC. The SPDC photons generated with the pump beam focused at the center of the PPKTP crystal by a lens, L_3 (focal length, $f = 150$ mm with a spot size of ~ 40 μ m, are collimated using the lens, L_4 , of focal length, $f = 100$ mm. The collimated annular SPDC ring, as observed by the EMCCD camera (Andor, iXon Ultra 897) after extraction from the pump by the interference filter (IF) of bandwidth ~ 10 nm centered at 810 nm, is first divided into two half-circles using the gold-coated prism mirror (PM). Subsequently, the half-circles of the SPDC ring are divided into four quarters, named U1, D1, U2, and D2, using the D-shaped mirrors, DM1 and DM2, and collected using the combination of a fiber coupler, single-mode fiber (SM) and single photon counting modules (SPCM-AQRH-14-FC),

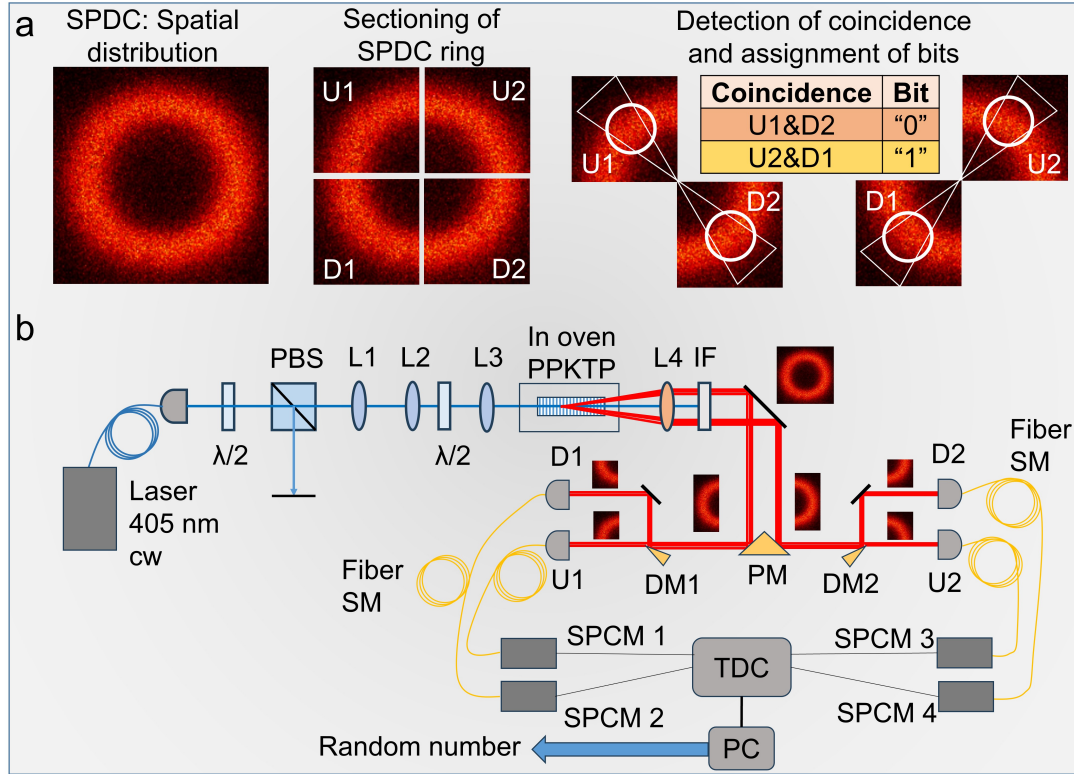


Figure 4.1: The schematic representation of (a) the concept and (b) the experimental setup of the QRNG source. Laser: 405 nm, cw diode laser, $\lambda/2$: Half wave plate, L1-4: plano-convex lenses of different focal lengths, PPKTP: 20 mm long PPKTP crystal of single grating period in temperature oven, IF: Interference filter, PM: Prism shaped gold coated mirror, DM1-2: D-shaped mirrors, U1-2 and D1-2: Upper and lower sections of the SPDC ring, SM: Single-mode fiber, SPCM1-4: single photon counting modules, TDC: Time-to-digital converter, PC: Computer.

SPCM1-4. The time-to-digital converter (TDC) (MultiHarp 150, PicoQuant) records the timestamp of the coincidence detection events from opposite sections of the SPDC ring are used to generate a binary sequence composed of zeros and ones.

The selection of a coincidence window plays a vital role in detecting true coincidences while avoiding false positives. For example, a too-narrow coincidence window can miss true coincidences, and a too-wide window can include uncorrelated events, thus underestimating and overestimating the experimental parameters. Since we are dealing with a high-brightness single photon source [92, 123, 124] in the current ex-

periment, keeping pump power of 1 mW, we have measured $g^{(2)}(\tau)$ with the coincidence window width in a step of 0.5 ns starting from 0.5 ns and found the increase of $g^{(2)}(\tau)$ from 0.016 to 0.1 at a slope of 0.019 per nanosecond width of the coincidence window. Owing to the intrinsic timing jitter present in the SPCM and electronics can collectively be estimated to be in the range of 0.6 ns, we found the coincidence window of 1 ns is optimum to handle our high brightness source without significantly changing the overall coincidence counts. Therefore, we have set the coincidence window of 1 ns, (200 bins each of width 5 ps) throughout the studies unless otherwise mentioned.

4.3 Results and discussions

We first characterized the photon pair source purity and indistinguishability as a function of pump power using Hong-Ou-Mandel (HOM) interferometry [93] and $g^{(2)}(\tau)$ [94]. While these two experiments can simultaneously be done using the pair photons of diametric opposite sections (see Fig. 4.1(b)), we used pair photons from sections U2 and D1 and performed two measurements one after the other using the standard experimental setups used for HOM and $g^{(2)}(\tau)$ studies. First, we built the HOM interferometer by incidenting photons of sections U2 and D1 on two input ports of a 50:50 beamsplitter (not shown in the current experiment) and measured the coincidence between the output ports with varying optical delay between the photons similar to our previous report [124, 125]. On the other hand, the $g^{(2)}(0)$ is measured using the standard Hanbury-Brown–Twiss [12] experimental scheme by placing a 50:50 beam splitter (not shown in the current experiment) on the path of photons from section U2 and recording the coincidence between the outputs of the beam splitter with respect to the photon of section D1 for different delays of the photon of one of the output arms. The results are shown in Fig. 4.2. As expected, it is evident from Fig. 4.2(a) that the HOM visibility, V (black dots), decreases from 0.86 to 0.22, and the $g^{(2)}(0)$ (red dots)

increases from 0.032 to 0.47 with an increase in pump power from 1 mW to 25 mW. However, we observe a deviation from the linear dependence of both HOM visibility, V , and $g^{(2)}(0)$, at higher pump power due to the saturation of the single photon detectors beyond single counts of 12 - 14 MHz, as obtained for the pump power in the range of 12 - 15 mW. It is worth noting that, even though the source reaches a maximum value of $g^{(2)}(0) = 0.47$, this remains well below the classical threshold of $g^{(2)}(0) < 1$, ensuring the non-classical behavior of the light sources when evaluated using a 1 ns coincidence interval, the lower HOM visibility ($V = 0.22$) confirms the distinguishability of photons due to the generation of multiphotons at higher pump powers. Increasing the width of the coincidence window would escalate the rate of change in both HOM visibility and $g^{(2)}(0)$ with pump power.

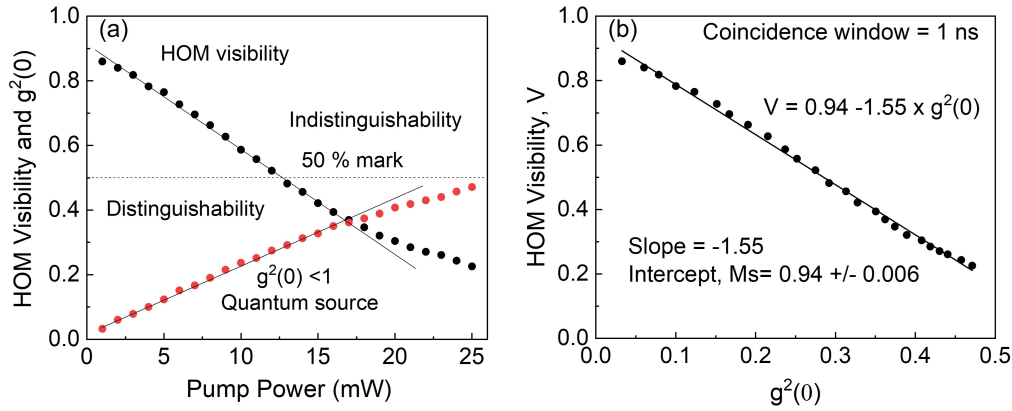


Figure 4.2: (a) HOM visibility (indistinguishability), and $g^{(2)}(0)$ (purity) is evaluated under varying pump powers. (b) Dependence of HOM visibility on change of $g^{(2)}(0)$ with pump power as shown in (a).

To gain further insight into the single-photon characteristics and distinguishability between photons in the presence of multiphoton generation due to increased pump power, we plotted HOM visibility (V) as a function of $g^{(2)}(0)$ using the data from Fig. 4.2(a). The results reveal that the HOM visibility, (V) and $g^{(2)}(0)$ for a fixed

coincidence window width (here, 1 ns) follow a linear relationship (black line) given by $V = 0.94 - 1.55 \times g^{(2)}(0)$ shown in Fig. 4.2(b). This is different from the relationship $V \approx 1 - g^{(2)}(0)$ predicted for a high purity single-photon source based on quantum dots [100, 101]. The intercept value (0.94 ± 0.006), which defines the intrinsic single-photon indistinguishability of the current source, is slightly lower due to the transmission function of the interference filter with a bandwidth of approximately 10 nm. Meanwhile, the slope of the curve indicates the generation and collection of multiphotons, resulting in photon distinguishability. Both the slope and the intercept value can change depending on the collection optics, such as the use of a multimode fiber and the efficiency of the single-photon detector. We observed similar performance of the source in terms of HOM visibility and $g^{(2)}(0)$ when using pair photons collected from sections U2 and D1, confirming the uniform performance of the source throughout the annular distribution. These results suggest that one needs to selectively use either parameter to characterize the single-photon source based on the intended application. For example, for interferometer-based quantum sensing, where distinguishability of photons is important [123, 126], HOM visibility may be a more relevant measure of source quality than $g^{(2)}(0) < 1$. Whereas for applications like QRNG, where detection of single and coincidence detection of photons is more important over indistinguishability, $g^{(2)}(0) < 1$ will be a more relevant indication of the quality of the source.

By characterizing how the input pump level influences the performance metric of the heralded single-photon source, we recorded the coincidence counts of pair photon of sections (U1 & D2) and (U2 & D1) (see Fig. 4.1) and assigned bits 0 and 1, respectively. Subsequently, we have recorded more than 90 million raw bits of 0s and 1s for each pump power, requiring varying bit recording time: shorter time for higher pump power and longer time for lower pump power due to the change in photon generation rate. To gain insight into the uniformity of the raw data, we calculated the occurrence

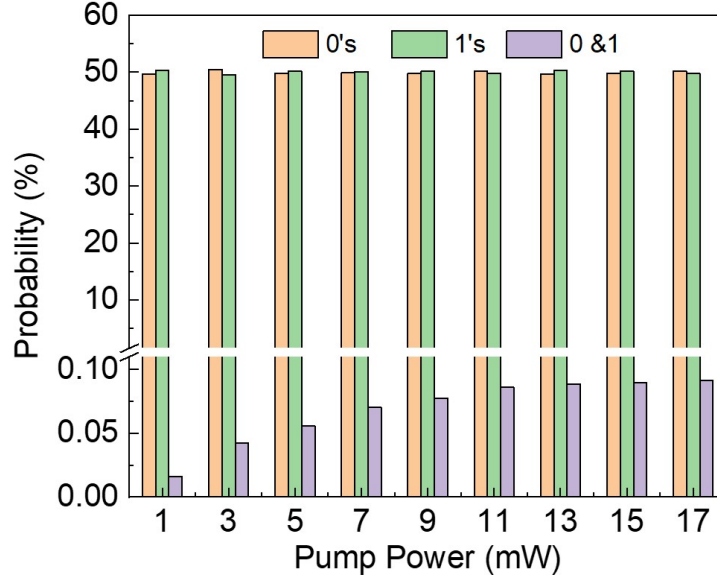


Figure 4.3: Probability distribution of 0's, 1's, and 0 & 1 in the raw bit sequence collected at pump powers.

of 0's (coincidences between U1 & D2), 1's (coincidences between U2 & D1), and simultaneous 0's & 1's (coincidences between U1 & D2 and U2 & D1) in the raw bit string collected at various pump power levels. The results, as displayed in Fig. 4.3, demonstrate that the probabilities of obtaining 0's (orange) and 1's (green) within the raw bit sequence are consistently near 50% across all power levels. This confirms the high quality and uniformity of the raw bit string. Additionally, the probability of simultaneous occurrences of 0's and 1's (purple) due to photon presence in all four sections of the SPDC ring (see Fig. 4.1(a)) remains below 0.1% at all power levels. This low occurrence indicates a minimal probability of simultaneous photon-pair generation in the transverse plane. The data also confirms the high purity of the raw bit string, with a low rejection rate (classical noise) of SPDC photons contributing to the QRNG, enhancing the efficiency of the system.

Since the raw bit contains all possible errors, we calculated the minimum entropy

[111, 127] to determine the maximum extraction of final, unbiased, true random bits. For a random variable X taking values in the space $\{0, 1\}^N$, the min-entropy [111] is introduced as

$$H_{\infty}(X) = -\log_2 \left(\max_{x \in \{0, 1\}^N} P_r[X = x] \right). \quad (4.1)$$

To calculate the min-entropy $H_{\infty}(X)$, we applied an 8-bit ($N = 8$) binning technique by segmenting the bit string into 8-bit blocks, each mapped to one of the 256 possible bins (2^8). This resulted in 256 sample points ($\{0, 1\}^N$), each representing a unique 8-bit sequence. We identified the most probable sample, denoted as x , from this set and calculated the min-entropy using the standard formula as represented by Eq. 4.1. As seen in Fig. 4.4, the min-entropy, $H_{\infty}(X)$ (black dots), decreased from 99.4% to 96.5% as the pump power increased from 1 mW to 17 mW, and subsequent increase of $g^{(2)}(0)$ from 0.03 to 0.36 due to the rise in multi-photon events at higher pump powers. Despite this, the raw bit string retained more than 0.96 bits per bit of randomness, enabling the extraction of over 96% quantum random bits. However, the high $H_{\infty}(X)$ value of 99.4% at 1 mW indicates the potential for generating pure quantum random numbers at a lower bit rate, highlighting a trade-off between min-entropy and bit rate. To distill true random bits from the raw bit sequence, we employed a Toeplitz hashing randomness extractor [128]. We constructed a binary Toeplitz matrix of size $m \times n$ [129] using a pseudorandom seed of $m + n - 1 = 175.5$ million bits, with $m = 85.5$ million bits, 95% of the raw bits, $n = 90$ million bits ($m = 0.95 \times n$). To overcome the computational limitations, we divided the raw and seed sequences into blocks of one million bits, post-processed each block separately, and concatenated all the bits to make the string of final post-processed bits. The red dots in Fig. 4.4 show that the post-processed QRNG bit rate increased linearly with pump power, from 0.4 million bits per second at 1 mW to 2.5 million bits per second at 11 mW, with a slope of 0.2 million bits per second per mW of pump power. Beyond 11 mW, the bit rate deviated

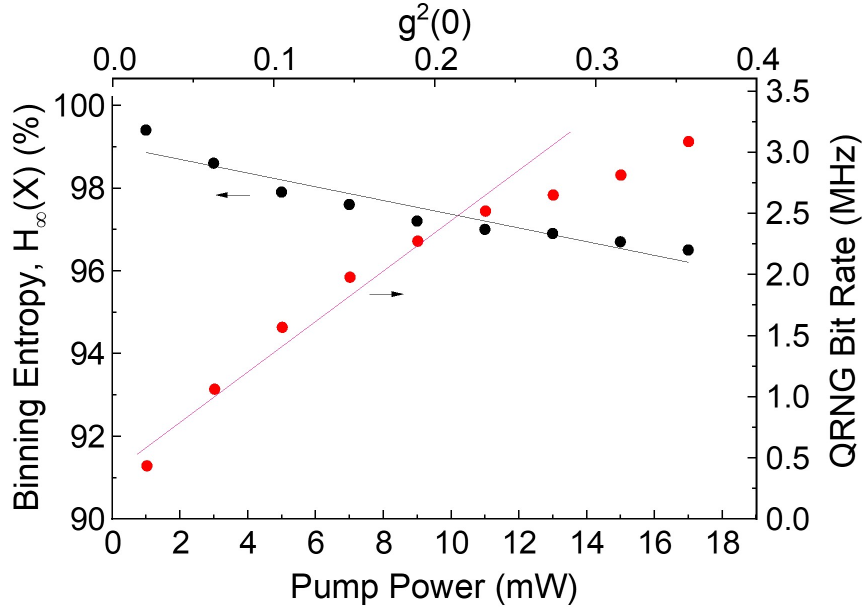


Figure 4.4: The variation of the minimum entropy, $H_\infty(X)$ (black dots), and post-processed QRNG bit rate (red dots) as a function of pump power and $g^{(2)}(0)$. The black and red lines are linear fit to the experimental data points.

from linearity due to detector saturation, reaching a maximum of 3.08 Mbps at 17 mW, which is higher than the earlier-mentioned bit rate (4.4 Kbps[119]). Further improvement in the QRNG bit rate can be possible using higher pump power in combination with the use of a detector with high quantum efficiency and a high saturation threshold, such as superconducting nanowire single-photon detectors (SNSPDs) [130] and a lower coincidence widow (< 1 ns used in the current study).

After having the post-processed QRNG bits, we used the NIST 800-22 test suite [39] to evaluate the quality of randomness of the post-processed bits. We have divided the post-processed bit string into 80 sequences (higher than the required minimum samples, 55 sequences of the NIST test suite) of binary bits, each containing one million bits as the input file for the NIST test suite. As the NIST statistical test suite follows two primary types of quantification to determine the randomness of the sequence, we calculated the uniform behavior of the P-values and the proportionality

test to find the proportion of the input sequences passing (P-value is above the chosen significance level, α , usually $\alpha = 0.01$) a test. Using the Goodness-of-Fit distributional test and Kolmogorov-Smirnov tests to the post-processed bits, we found the final P-values of 15 different tests under the NIST test suite of the post-processed bits for a pump power of 17 mW are displayed in Fig. 4.5. All conducted tests produce P-values larger than 0.1, confirming the randomness of the experimental results.

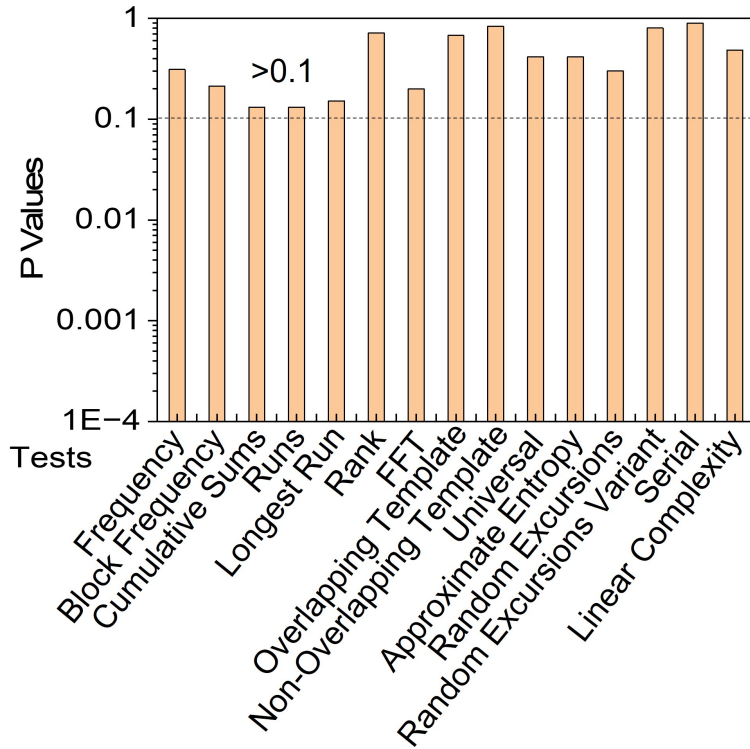


Figure 4.5: Final P-values of 15 tests under NIST statistical suit for the Toeplitz post-processed bits recorded for a pump power of 17 mW.

Again, we recorded the proportionality test results for the post-processed bit sequences in Table 4.1. According to the NIST test suite, the proportional fraction should

lie within the range given by the equation [39],

$$(1 - \alpha) \pm 3\sqrt{\frac{\alpha(1 - \alpha)}{n}} \quad (4.2)$$

where n is the number of sequences. For 80 sequences, each consisting of 1 million bits, NIST considers $n = 49$ for the random excursions and random excursion variant tests. Using $\alpha = 0.01$ and $n = 49$ in Eq. 4.2, the calculated range for the proportional fraction is (0.947, 1.033). For the remaining tests, using $\alpha = 0.01$ and $n = 80$, the proportional fraction range is (0.956, 1.023). As shown in Table 4.1, the proportional fractions for all post-processed bit sequences lie within the defined ranges, indicating successful results across all tests.

Table 4.1: Results of the NIST statistical tests

Test name	Proportion of successful sequences	Result
Approximate entropy	0.988	Success
Frequency within a block	0.975	Success
Cumulative sums	0.975	Success
Discrete Fourier transform	0.988	Success
Frequency	0.975	Success
Longest run in a block	0.962	Success
Non-overlapping template	min 0.962	Success
	max 1.000	Success
Overlapping template	1.000	Success
Random excursions	min 0.980	Success
	max 1.000	Success
Random excursions variant	min 0.960	Success
	max 1.000	Success
Binary matrix rank	1.000	Success
Runs	0.988	Success
Serial	0.975	Success
Linear complexity	0.988	Success
Maurer's universal	0.988	Success

Further, we evaluated the randomness of our post-processed bits using the TestU01 statistical test suite, specifically the Rabbit, Alphabit, and BlockAlphabit battery tests.

While these tests typically require sequences of approximately 30 million bits, we employed longer sequences of 80 million bits for more rigorous analysis. Following the methodology outlined in the literature [131, 132], we interpreted the P-values by considering values within the interval $[10^{-3}, 1 - 10^{-3}]$ as a success, and value outside this interval as a failure. The results of the TestU01 tests on our post-processed random bits, as shown in Table 4.2, indicate that our novel experimental scheme successfully passed all the tests, regardless of the interpretation method applied.

Table 4.2: Results for the TestU01 statistical tests

Battery	Sequence length	Result
Rabbit	$8 \cdot 10^7$	Success
Alphabit	$8 \cdot 10^7$	Success
BlockAlphabit	$8 \cdot 10^7$	Success

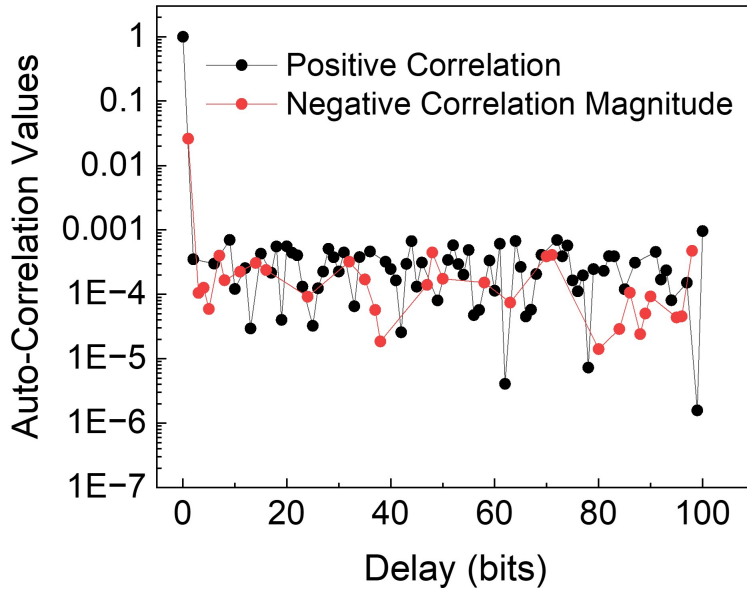


Figure 4.6: Variation of the magnitude of the positive and negative autocorrelation coefficients of the first 10 million bits of the raw bit sequence up to a delay of 100 bits. The raw bit sequence is recorded for the pump power of 17 mW.

We also analyzed the randomness of the raw data recorded for the pump power of

17 mW by calculating the autocorrelation coefficient. Using the first 10 million bits of the raw bit sequence up to a delay of 100 bits, we computed the autocorrelation coefficient. Fig. 4.6 displays these findings, indicating that both the average value and the standard deviation of the autocorrelation coefficient remain essentially unchanged even at a delay of 100 bits. Compared to a truly random sequence, which would have an autocorrelation coefficient of zero mean value, the raw bits from our experiment exhibit an autocorrelation coefficient with a mean value on the order of 10^{-4} and a standard deviation of 9.8×10^{-4} . Such low values for the minimum autocorrelation coefficient confirm that the raw bit string recorded from the current experiment represents a good random sequence, even before post-processing. This observation further certifies the high value of the min-entropy, $H_{\infty}(X)$, and extraction efficiency.

To provide a clearer context for the current results, we have compared the bit rate of our QRNG with recent coincidence-based QRNG systems in the literature, as summarized in Table 4.3.

Table 4.3: Comparison of bit rate of QRNG based on coincidence detection.

Reports	Bit rate (bits/sec)
Ref.[133]	1.71
Ref.[134]	$1.81 \cdot 10^2$
Ref.[135]	$2.40 \cdot 10^2$
Ref.[119]	$4.40 \cdot 10^3$
Ref.[136]	$1.35 \cdot 10^4$
Our study	$3.08 \cdot 10^6$

In the QRNG scheme based on spatial correlations, several experimental imperfections may introduce bias in the generated bit strings. The primary sources include detector efficiency imbalance, spatial-mode nonuniformity, and background noise, such as dark counts and stray photons. Detector efficiency mismatch can lead to unequal de-

tection probabilities; however, this effect can be mitigated by introducing controlled attenuation in the higher-efficiency detection arm. In our implementation, detectors with identical specifications from the same manufacturer were employed, and experimental observations confirmed nearly identical coincidence rates for any detector pair from identical pair-photon sources, indicating negligible intrinsic imbalance. Spatial-mode overlap imperfections may affect the stable, uniform generation of photon pairs across different sections of the SPDC ring. However, the annular type-0 SPDC configuration used in this work has previously been demonstrated by our group to provide stable, bright pair-photon emission. Background noise contributes to accidental counts, which can degrade randomness quality, but this effect is significantly suppressed by temporal filtering that considers only coincidence events for bit-string generation. Quantitatively, the combined contribution of detector inefficiency and background noise to bias is estimated to be on the order of 10^{-3} – 10^{-4} . Any residual bias is further removed during post-processing using Toeplitz hashing, resulting in high-quality, nearly uniform random bit sequences.

4.4 Conclusions

In conclusion, we presented a novel QRNG scheme based on the temporal and spatial correlations of heralded single-photon sources, bypassing the need for traditional beam splitters and enhancing both the efficiency and simplicity of the overall system architecture. We characterized the purity and indistinguishability of the single-photon sources using the second-order correlation function $g^{(2)}(0)$ and Hong-Ou-Mandel (HOM) visibility, finding a linear relation between these two parameters for the heralded single-photon sources. Interestingly, while the purity of the single-photon source, quantified by the $g^{(2)}(0)$ value, determines the min-entropy for the maximum extractable true random bits from the raw bit sequence, the photon indis-

tinguishability, indicated by HOM visibility, shows weak or no dependence on QRNG performance. For example, with the pump operating at 17 mW, the heralded single-photon source demonstrated $g^{(2)}(0) = 0.36$ and HOM visibility of 36%. Nonetheless, the min-entropy of the raw bit sequence was found to be 0.96, with a very low autocorrelation coefficient ($\sim 10^{-4}$) even after a delay of 100 bits. This indicates the random appearance of paired photons at diametrically opposite points on the SPDC ring. Now, the detection of photons from different sections of one half of the ring and assignment of bits 0 and 1, without coincidence detection of their respective partner on the other half of the ring, potentially increasing the bit rate [137] of QRNG but without any quantum certification. After applying Toeplitz post-processing to the raw bit sequence, we confirmed that the output passed both the NIST and TestU01 test suites, verifying the development of a high-quality QRNG with a high bit rate. Further enhancement in the bit rate from a few hundred MHz to GHz can be made possible using multi-bit QRNG by multiple sections of the SPDC ring or by recording the photon pair events using a SPAD camera and assigning the bits for the coincidence between the diametrically opposite pixels. Single photon source-based QRNG faces the common limitation of a lower bit rate, typically in the Kbps order. Also, the conventional approach requires an additional device, such as a 50:50 beam splitter. We addressed these limitations using the inherent spatial randomness of SPDC bi-photons, bypassing the need for a balanced-beam splitter and achieving Mbps order bit rate with the quantum source certification using $g^{(2)}(0)$. Our QRNG scheme offers a promising path to achieve higher bit rates while ensuring true quantumness, making it highly suitable for secure applications across various fields. In the next chapter, we will use entangled photon pairs for live device-independent certification using the Bell parameter.

Chapter 5

Device-Independent QRNG with Live Bell-Test Certification

Many information-processing applications rely critically on device-independent implementations of quantum random number generation, requiring certified quantumness to ensure genuine randomness. However, inherent technical challenges in implementing quantumness tests often result in a low bit rate. Here, we present a high-bit-rate DI-QRNG with live quantumness certification through the Bell test. By employing SPDC in a polarization Sagnac interferometer, which generates entangled degenerate pair-photons in annular ring distribution with strong temporal and spatial correlations due to energy and momentum conservation, we divide the annular ring into six diametrically opposite sections, forming three robust entangled photon sources from a single laser and nonlinear crystal. The pair-photons from these three sources exhibit bias-free quantum mechanical randomness. By utilizing the coincidence counts of pair-photons from two sources, we generate raw bits, while the third source simultaneously measures the Bell's parameter without any loss of QRNG bits. We have generated 90

million raw bits in 46.4 seconds with the Bell parameter ($S > 2$), with a minimum entropy extraction ratio exceeding 97%. Post-processed using a Toeplitz matrix, the DI-QRNG achieves a bit rate of 1.8 Mbps, passing all NIST 800-22 and TestU01 tests. In the absence of Bell's parameter for a non-maximally entangled state, $g^{(2)}(0)$ can be the metric for quantumness measure. Free from the requirement of any physical devices such as beam-splitters, this scalable DI-QRNG scheme promises high bit-rates and trustworthy certifications essential for practical applications.

5.1 Introduction

Random numbers play a fundamental role in a wide range of applications, including cryptographic protocols, secure communication, and scientific simulations [40, 102]. The random numbers generated through the deterministic classical computer algorithms, known as the pseudo-random number generators (PRNGs), are vulnerable to predictability and external tampering [29, 30]. On the other hand, the random numbers generated by exploiting the inherent unpredictability of quantum stochastic process, known as the quantum random number generators (QRNGs), guarantee the generation of truly random numbers [27, 138]. Typically, the quantum stochastic process includes the measurement of quantum-phase fluctuation, single photon detection, and vacuum fluctuations [139–141]. Conventionally, the QRNGs have two parts: source (generating quantum states that are inherently random) and measurement (demolition of quantum state using a practical device such as a beam-splitter and subsequent detection using a detector to generate raw bits). However, in the absence of perfect devices for generation and measurement, practical QRNGs can suffer from security loopholes, leading to the development of device-independent QRNGs (DI-QRNGs) independent (regardless) of the physical implementation and characterization of the instruments used [142–144].

Typically, the DI-QRNGs have the inherent certification of randomness based solely on the violation of Clauser-Horne-Shimony-Holt (CHSH) form of Bell's inequality [145] without assuming trust in the internal workings of the quantum random number generation scheme [119, 121]. Despite having the highest security in the random numbers, the DI-QRNGs have a relatively lower bit rate [119, 146] due to the limitations on the brightness of the entangled sources developed using the current technologies. As a result, the practical implementations of DI-QRNGs in parallel with the QRNG scheme have not been explored to date. Alternatively, efforts have been made to enhance the bit rate of the QRNG through exploration of different protocols such as source-independent QRNG [147–150], measurement device-independent QRNG [151, 152], and semi-device-independent QRNG [153, 154] with different assumptions about the source or the measurement at the cost of ultimate security of the randomness. Additionally, device-independent QRNGs lack tolerance to losses, demanding extremely stringent requirements of the experimental devices. On the other hand, the majority of the QRNGs often rely on physical devices such as 50:50 beam-splitters or polarization beam-splitters, despite the technological challenge of making a perfect lossless, unbiased beam-splitter.

Therefore, it is essential to devise new protocols aimed at advancing the development of DI-QRNG with a high bit rate while ensuring randomness by the intrinsically probabilistic nature of quantum physics. Recent advances in quantum optics, together with developments in engineering, have enabled pathways to simplify DI-QRNG architectures. Beam-splitter-free designs are particularly promising, offering streamlined setups that reduce complexity and enhance robustness [105, 107, 150]. Additionally, incorporating real-time randomness certification, such as live Bell test verification, strengthens the trustworthiness of the generated numbers by providing immediate validation of the CHSH inequality [145] for the source.

In this paper, we introduce a novel beam-splitter-free, high-bit-rate DI-QRNG with live Bell test certification. Using the non-collinear, degenerate, spontaneous parametric downconversion (SPDC) process in a 20-mm-long periodically-poled potassium titanyl phosphate (PPKTP) crystal in a polarization Sagnac interferometer, we have developed three high-brightness entangled photon sources [92, 124] from the single resources (optical components, nonlinear crystal, and laser source) by dividing the SPDC ring into six diametrically opposite sections. Since the generation of the pair-photons over the diametrically opposite points of the SPDC ring is purely random and governed by the quantum mechanical process, we have generated random bits (raw) with min-entropy exceeding 97% by measuring the coincidence of the quantum correlated pair-photons of the two entangled photon sources without any projection and a third source for live measurement of CHSH Bell's parameter ensuring real-time trustworthiness of the source, thus confirming the realization of DI-QRNG. The entropy ensures high efficiency in extracting true random bits. Using Toeplitz matrix-based post-processing, our DI-QRNG system results in a bit rate of 1.8 Mbps, passing all NIST 800-22 and TestU01 statistical test suites.

Although in the present proof-of-concept demonstration we have divided the SPDC ring to form three independent sources, in principle, the experimental scheme is scalable. By enlarging the SPDC ring diameter and employing a multi-bit assignment protocol, one can increase the number of sources and thereby enhance the bit rate of the DI-QRNG system with live certification. However, increasing the ring size reduces the photon collection rate at individual detectors, as the probabilistically generated photon pairs are distributed over a larger area. At the same time, it lowers the multiphoton collection probability, an important factor in preserving the quantumness of the source. The reduction in photon collection efficiency per detector can be compensated by increasing the pump power to boost the photon-pair generation rate without degrading

the quantumness of the source. Nevertheless, scaling the system to include a larger number of sources requires a proportional increase in the number of detectors, which significantly adds to the complexity and cost of the setup.

5.2 Experiment

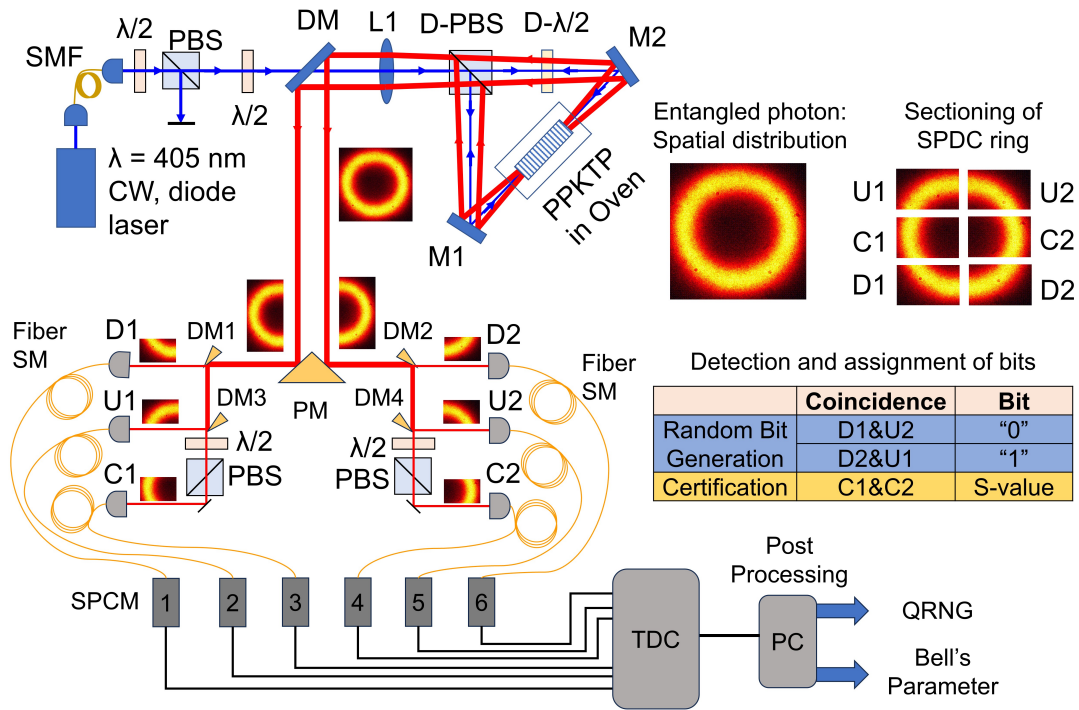


Figure 5.1: The schematic representation of the experimental setup of the QRNG source. Laser: 405 nm, cw diode laser, $\lambda/2$: Half-wave-plate, L1: plano-convex lenses of focal length 150 mm, $D - \lambda/2$: Dual-half-wave-plate, PPKTP: 20-mm-long periodically-poled potassium titanyl phosphate crystal of single grating in the oven, IF: Interference filter, PM: Prism-shaped gold-coated mirror, DM1-4: D-shaped mirrors, U1-2, D1-2, and S1-2: Upper, lower and side sections of the SPDC ring, SM: Single-mode fiber, SPCM1-6: single photon counting modules, TDC: Time-to-digital converter, PC: Computer. Inset: Spatial distribution of entangled photon source, the architecture of raw bit assignment, and quantumness certification.

The schematic of the experimental setup is illustrated in Fig. 5.1. A continuous-wave, single-frequency (linewidth ~ 20 MHz), single-mode fiber (SMF)-coupled laser diode providing an output power of 21 mW at a central wavelength of 405 nm is used

as the pump source. Notably, the single-mode fiber coupling, together with the intentional small tilts applied to all optical elements, effectively suppresses back-reflections into the laser, thereby ensuring optimal wavelength and power stability without the need for an optical isolator. Operating the laser at its highest power to ensure optimum performance, the power attenuator, comprised of a half-wave-plate ($\lambda/2$) and a polarizing beam-splitter (PBS) cube, is used to control the input pump power to the experiment. A second $\lambda/2$ plate with optic axis at an angle θ with respect to the vertical axis is used to transform the horizontally (H) polarized pump beam in the superposition of horizontal and vertical (V) polarization states in the form of $(\alpha' H - \beta' V)$, where, $\alpha' = \sin(2\theta)$, $\beta' = \cos(2\theta)$, and $|\alpha'|^2 + |\beta'|^2 = 1$. As a result, adjusting θ , we can control the laser power in both clockwise (CW) and counterclockwise (CCW) beams of the polarization Sagnac interferometer, which consists of a dual-wavelength PBS (D-PBS, for 405 nm and 810 nm) and two plane mirrors, M1 and M2. The lens, L1, with a focal length, $f = 150$ mm, focuses the pump beam to a spot size of $\sim 40 \mu\text{m}$ at the center of the nonlinear crystal placed between mirrors M1 and M2. The dual-wavelength half-wave-plate (D- $\lambda/2$), with its optic axis rotated by 45° relative to the vertical, is placed inside the Sagnac interferometer to transform horizontal polarization to vertical and vice versa for both 405 nm and 810 nm wavelengths. A single-grating ($\Lambda = 3.425 \mu\text{m}$) periodically-poled potassium titanyl phosphate (PPKTP) crystal with a length of 20 mm and a $1 \times 2 \text{ mm}^2$ aperture serves as the nonlinear medium, producing degenerate SPDC photons at 810 nm through non-collinear, type-0 ($e \rightarrow e + e$) phase-matching. The crystal is housed in an oven with a temperature range up to 200°C and a stability of $\pm 0.1^\circ\text{C}$. However, throughout the manuscript, we have maintained the crystal temperature at $T = 39.5^\circ\text{C}$, which produces photon pairs with a half-cone angle of approximately 1° . An increase in the cone angle, leading to an SPDC ring of larger diameter, requires lowering the crystal temperature away from its collinear

phase-matching temperature of $T = 42^\circ\text{C}$. The cone angle of the SPDC photons can be calculated using the phase-matching condition together with the Sellmeier equations [92].

The CW and CCW pump beams, in the presence of the $D\text{-}\lambda/2$ plate, generate pair-photons distributed in an annular ring with orthogonal polarization states. When superimposed on the D-PBS, the SPDC photons exhibit an annular ring distribution, with pair-photons located at diametrically opposite points on the ring and described by the state, $|\phi^-\rangle = (\alpha|HH\rangle - \beta|VV\rangle)$, where, $\alpha = \sin(2\theta)$, $\beta = \cos(2\theta)$, and $|\alpha|^2 + |\beta|^2 = 1$. Here, α and β are function of α' and β' . The optic axis of $\lambda/2$ plate at an angle $\theta = 22.5^\circ$ with respect to horizontal results in SPDC photons with state, $|\phi^-\rangle = (|HH\rangle - |VV\rangle)/\sqrt{2}$ (a Bell state). The SPDC photons are collimated by lens L1 and separated from the pump beam by a dichroic mirror (DM) positioned between lens L1 and the $\lambda/2$ plate. The collimated annular SPDC ring, as observed by the EMCCD camera (Andor, iXon Ultra 897) with an interference filter of bandwidth ~ 3.2 nm centered at 810 nm, is shown by the image in the inset of Fig. 5.1.

We divide the SPDC into two halves by the gold-coated prism mirror (PM), and subsequently, each half is divided into three subsections by D-shaped mirrors, DM1-4, resulting in three pairs of diametrically opposite sections (U1, D2), (U2, D1) and (C1, C2) having pair-photons. While the photons from each section are collected using the combination of an interference filter (bandwidth of 3 nm) mounted fiber coupler, single-mode fiber (SM), and single photon counting modules, SPCM1-6, (SPCM-AQRH-14-FC), the photons of sections C1 and C2, pass through the polarization analyzer consisting of a $\lambda/2$ plane and PBS before collection. The time-to-digital converter (TDC) (MultiHarp 150, PicoQuant) is connected to the SPCMs, and the computer is used for photon counting, time stamping, recording, and experimental data analysis. The three pairs of diametrically opposite sections of the annular ring form

the three sets of single/entangled photon sources. For raw bit generation, as shown by the table in Fig. 5.1, we assign bits “0” and “1” for the coincidence event between the photons of sections (D1 & U2) and (D2 & U1), respectively. As the appearance of pair-photons in sections (U1, D2) and (U2, D1) are quantum mechanically random, this method produces a sequence of random bits of 0 and 1. The photons of sections (C1 and C2) are used for the entanglement study of the pair-photons through the polarization projective measurement and Bell’s parameter calculation. The coincidence window throughout the manuscript, unless otherwise mentioned, is 1 ns.

5.3 Results and discussions

We first characterized the entangled photon source by measuring the interference visibility in different bases and the value of Bell parameters as a function of pump power and coincidence window. Using the pair-photons from the sections (C1, C2), we have set the polarization state of one of the photons (say from C2) at horizontal (H), vertical (V), diagonal (D), and anti-diagonal (A) using the $\lambda/2$ plane and measured the interference visibility, $V = (\text{max.} - \text{min.})/(\text{max.} + \text{min.})$, by recording the coincidence counts while continuously rotating the polarization state of the other photon (from C1) using $\lambda/2$. The visibility for different bases as a function of pump power is shown in Fig. 5.2. As evident from Fig. 5.2(a), the entanglement visibility in all bases (H, V, D, and A) is almost comparable for all pump power, but with the increase of pump power from 0.5 mW to 12.4 mW and coincidence window of 1 ns, the visibility decreases from 97% to 73%, respectively. However, the interference visibility of $>71\%$ for all power levels confirms the entanglement [92]. Moreover, keeping the pump power constant at 12.4 mW, we measured the interference visibility further decreasing from 73% to 61%, below the 71% limit ensuring entanglement, with the increase of coincidence window from 1 ns to 2 ns with a step of 0.5 ns. The measurement of Bell’s parameter,

S , as shown in Fig. 5.2(b), confirms the decrease of S -value from 2.73 to 2.07 with the pump power increase from 0.5 mW to 12.4 mW. Although $S \geq 2$ confirms the entanglement, the increase of the coincidence window from 1 ns to 2 ns drastically reduces the S -value from 2.07 to 1.73 due to the generation of multi-photons at high pump power and detection of such photons in the presence of longer coincidence window (>1 ns). Such observation confirms the control transition of the output of the pair-photon source from the quantum state to the classical two-photon state. As expected, we observe a similar performance for the pair-photons collected from the sections (U1, D2) and (U2, D1), confirming the realization of three entangled photon sources from a single set of resources (laser and crystal). In fact, by dividing the annular ring of photons into more sections, a larger number of entangled photon sources can be realized. However, this comes at the cost of reduced brightness of the individual sources for a given pump power and crystal parameters. By increasing the pump power, the reduced brightness arising from the increase in the number of derived sources can be compensated, while still maintaining the quantum properties of the generated sources.

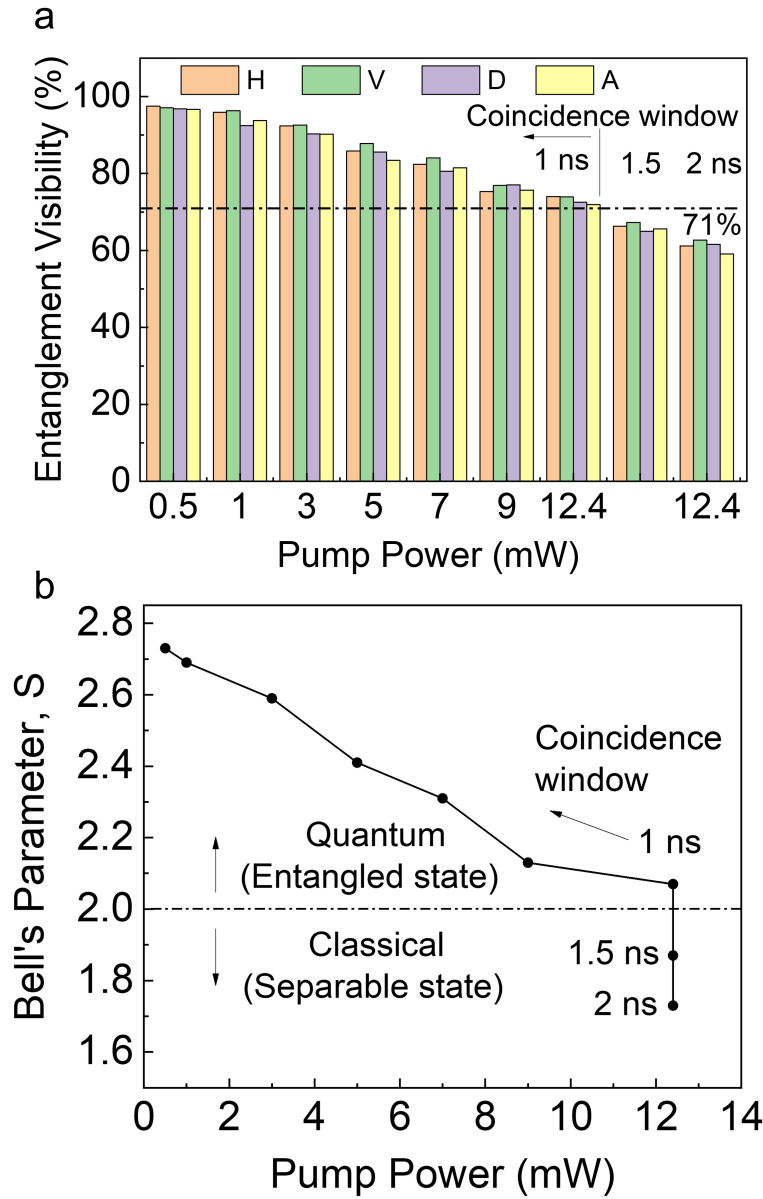


Figure 5.2: Characterization of the entangled photon sources. Variation of (a) Entanglement visibility and (b) Bell parameter (S) of the entangled photon source as a function of pump power and with coincidence window.

Knowing the performance metrics of the entangled photon source as a function of input power, we recorded the time stamps of the coincidence counts for pair-photons collected from the sections (U1 & D2) and (U2 & D1) and assigned binary values of

0 and 1, respectively, while simultaneously checking the Bell parameter of the source using the sections (C1 & C2) (see Fig. 5.1). For Bell parameter measurement, photon pairs from sections C1 and C2 travel approximately 1 m each before being detected by single-photon detectors with $\sim 55\%$ efficiency, physically separated by more than 1 m. Although this separation is modest due to experimental constraints, it is sufficient to ensure that no classical or quantum signal can propagate between the measurement devices during the measurement, thereby respecting the principle of locality. However, our current implementation provides partial device independence through Bell inequality violation, but does not fully close all major Bell test loopholes. The three main loopholes in Bell parameter estimation are detection, locality, and freedom of choice. In particular, the detection loophole remains open due to finite detector efficiency, as closing it typically requires superconducting nanowire single-photon detectors (SNSPDs) with efficiencies exceeding $\sim 83\%$ [155], which are currently unavailable in our laboratory. The locality loophole is also not strictly closed, since achieving space-like separation between the measurement systems and the source would require fiber links or free-space channels of a few hundred meters. Additionally, the freedom-of-choice loophole, which demands a fast, independent basis selection, is not addressed in the present setup due to the absence of high-speed switching elements [156]. Therefore, while the observed Bell inequality violation provides strong evidence of non-classical correlations and supports randomness certification, it does not constitute a fully loophole-free demonstration. Future work will focus on incorporating high-efficiency detectors, long-distance separation, and fast measurement basis selection with a more robust architecture to achieve fully device-independent quantum randomness generation.

We recorded over 90 million raw bit sequences of 0's and 1's for each pump power. Due to the dependence of pump power on the generation rate of pair-photons, the

recording time for 90 million bits decreased with increasing pump power, resulting in a recording time of 46.4 seconds at 12.4 mW of pump power for a coincidence window of 1 ns. Since the raw bit sequences contained all possible errors, we calculated the minimum entropy [127, 139] as mentioned in our previous report [150] to estimate the maximum extractable unbiased true random bits. The results, presented in Fig. 5.3, show that the min-entropy, $H_\infty(X)$ (black squares), remained nearly constant in the range of 99% to 97% as the pump power increased from 0.5 mW to 12.4 mW. For the increase of the coincidence window from 1 ns to 2 ns at a fixed pump power of 12.4 mW, the Bell parameter, S , decreased from 2.07 to 1.73 (see Fig. 5.2(b)), indicating the loss of entanglement. However, it is interesting to note that there is no significant change in the min-entropy, $H_\infty(X)$, value even for $S < 2$. Although the conditional quantum min-entropy, which accounts for side information on a random sequence [157], or its lower bound derived from the entropy uncertainty principle [148, 158], can be used to quantify achievable true randomness, it cannot be directly applied in our case since the random bits originate from coincidence counts of photon pairs generated in a fundamentally random fashion on the SPDC ring without any relative control. It is also worth noting that the conditional quantum min-entropy reduces to the classical min-entropy when considering pure states [141, 148]. Alternatively, the min-entropy of the bit string can be estimated from the Bell parameter of the entangled photon source using the treatment in Ref. [142] for violations with $S > 2$. However, such an approach is not applicable to a QRNG system developed from quantum sources with $S < 2$.

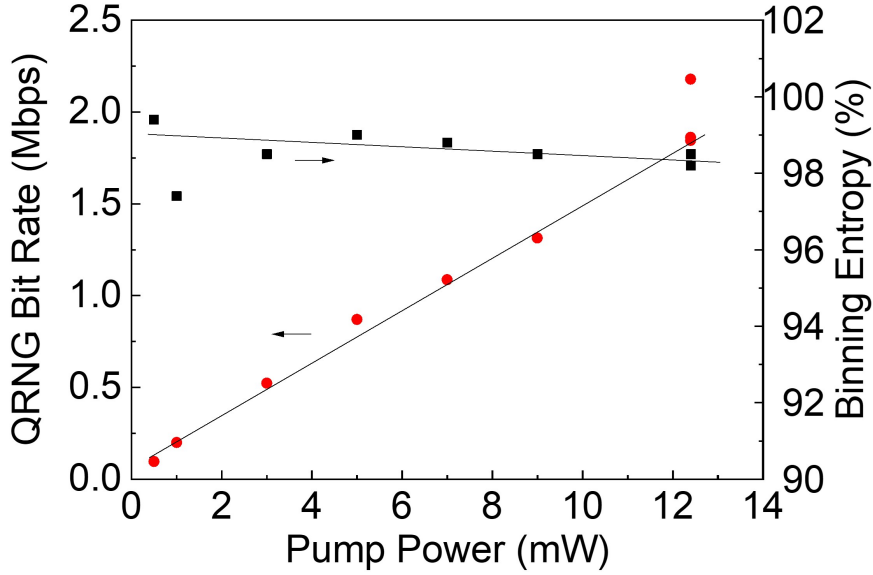


Figure 5.3: Characterization of the QRNG system. The variation of the minimum entropy, $H_{\infty}(X)$ (black dots), and post-processed QRNG bit rate (red dots), as a function of pump power. The solid lines are linear fit to the experimental data.

Such observation demonstrates that the reduction in min-entropy is primarily due to classical noise in the experimental setup and is independent of the entanglement quality of the quantum source. To distill true random bits from the raw bit sequences, we employed a Toeplitz hashing randomness extractor [128]. The post-processed QRNG bit rate (red dots in Fig. 5.3) exhibited a linear increase with pump power, rising from 0.09 Mbps at 0.5 mW to 1.8 Mbps at 12.4 mW, corresponding to a slope of 0.14 Mbps per mW. Additionally, at 12.4 mW pump power, increasing the coincidence window from 1 ns to 2 ns boosted the bit rate from 1.84 Mbps to 2.18 Mbps. These results confirm the realization of a high-bit-rate, device-independent QRNG system offering simultaneous Bell parameter measurement. Again, the higher value of min-entropy, $H_{\infty}(X)$, confirms the possibility for further enhancement of the bit rate of the QRNG system to a few tens of Mbps by simply increasing the pump power or by increasing the coincidence window. However, due to the unavailability of a higher power pump laser

at 405 nm, we restricted the bit rate to 2.18 Mbps. Unlike our previous report [150], the lower bit QRNG rate in the current experiment can be attributed to the larger ring diameter of the pair-photons to make easy division into six sections and lower effective power to the crystal.

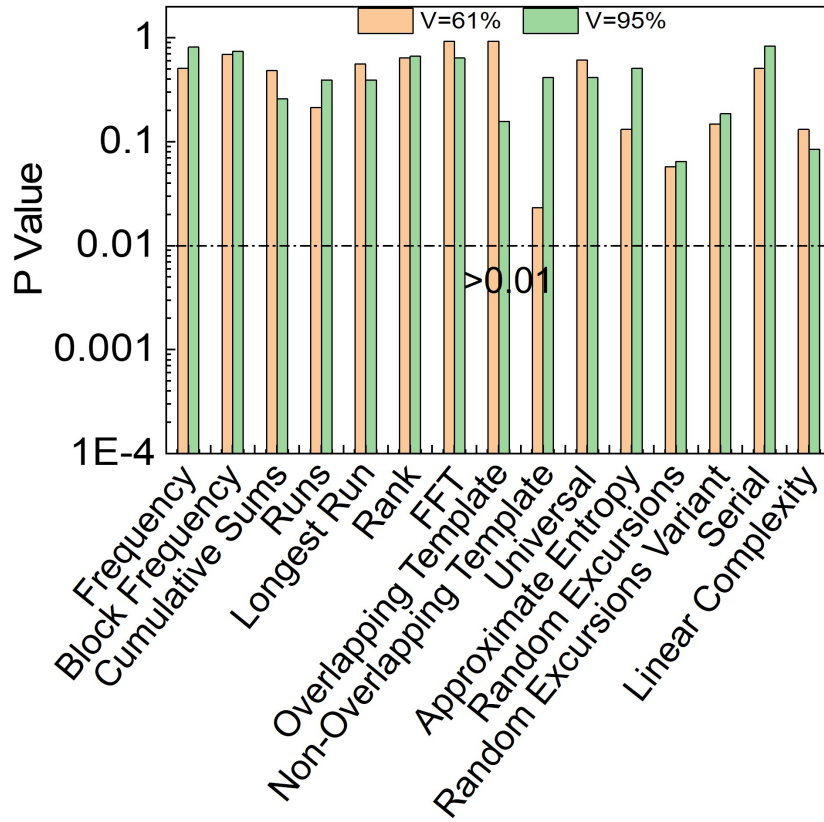


Figure 5.4: Verification of randomness of the source through test suits. Final P-values of 15 tests under NIST statistical suit for the Toeplitz post-processed bits recorded at 95% and 61% visibility, respectively.

To estimate the quality of randomness, we used the NIST 800-22 Statistical Test Suite [39] to the post-processed bit strings derived from the entangled photons with two different levels of entanglement visibility, $V = 95\%$ and $V = 61\%$. For each

visibility setting, we divided the bit string into 80 sequences of binary bits, similar to our previous work [150], each containing one million bits, thereby exceeding the minimum requirement of 55 sequences, as recommended by the NIST test suite. As the NIST statistical test suite follows two primary types of quantification to determine the randomness of the bit sequence, we calculated the uniformity of the P-values and the proportionality test to find the proportion of the input sequences passing (P-value is above the chosen significance level, α , usually $\alpha = 0.01$) a test. Using the Goodness-of-Fit distributional test and Kolmogorov-Smirnov tests to the post-processed bits, we calculated the final P-values of 15 different tests under the NIST test suite of the post-processed bits at visibilities, $V = 95\%$ (green) and $V = 61\%$ (orange), with the results shown in Fig. 5.4. As evident from the figure, the P-values of all the tests are > 0.01 , confirming the randomness of the experimental results at the different visibility levels. Although we have 80 sequences of bit strings, each consisting of 1 million bits for both entanglement visibilities of the quantum source, the NIST statistical test suite randomly selected $n = 46$ sequences for the random excursions and random excursion variant tests. For these tests, using a significance level of $\alpha = 0.01$ and $n = 46$, the proportional fraction range was calculated to be (0.946, 1.034). For the remaining tests, with $\alpha = 0.01$ and $n = 80$, the proportional fraction range was determined to be (0.956, 1.023). We observed that the proportional fractions for all post-processed bit sequences fell within these specified ranges, confirming successful results across all tests and demonstrating the randomness of the generated bit sequences.

Further, we evaluated the randomness of our post-processed bits using the TestU01 statistical test suite, specifically the Rabbit, Alphabit, and BlockAlphabit battery tests. While these tests typically require sequences of approximately 30 million bits, we employed longer sequences of 80 million bits for more rigorous analysis. Following the methodology outlined in the literature [131, 132], we interpreted the P-values by con-

sidering values within the interval $[10^{-3}, 1 - 10^{-3}]$ as a success, and value outside this interval as a failure. We observed the P values for the post-processed bit string successfully passed all three tests, indicating the validation of our novel experimental scheme.

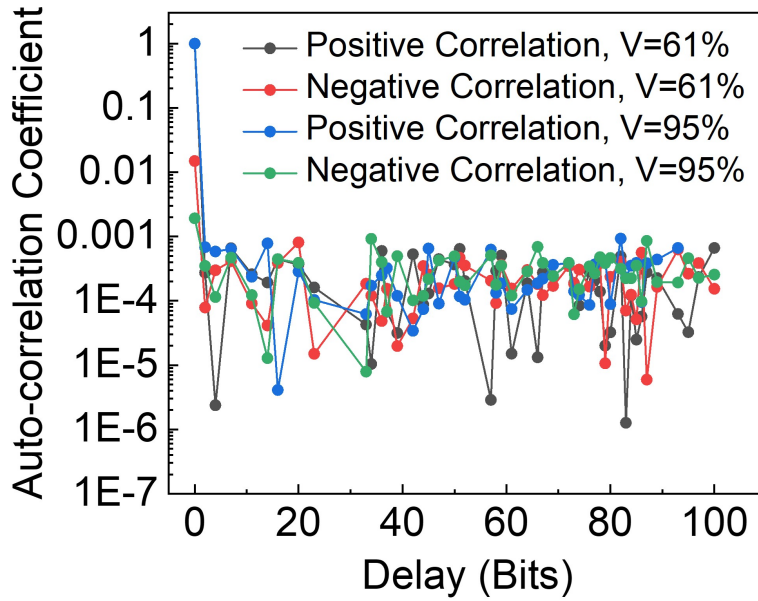


Figure 5.5: Characterization of raw bits of the QRNG. Variation of the magnitude of the positive and negative autocorrelation coefficients of the first 10 million bits of the raw bit sequence up to a delay of 100 bits. The raw bit sequences are recorded at two visibilities, 95% and 61%.

We further analyzed the randomness of the raw bits for two different entanglement visibilities, $V = 95\%$ (entangled state) and $V = 61\%$ (separable state), by calculating the autocorrelation coefficient. Using the first 10 million bits of the raw bit sequence, we computed the autocorrelation coefficient up to a delay of 100 bits, as shown in Fig. 5.5. It is evident from the figure that even after a delay of 100 bits, the mean and standard deviation of the autocorrelation coefficient remain nearly unchanged. Given

that a truly random sequence has an autocorrelation coefficient with a mean value close to zero, in our experiment, the raw bits for both entanglement visibilities exhibited a minimum autocorrelation coefficient in the order of $\sim 10^{-6}$ and a standard deviation of 9.8×10^{-4} . Such low values of minimum autocorrelation coefficient confirm that the raw bit string generated using entangled photons in the current novel experimental scheme represents a good random sequence even before post-processing, leading to a high min-entropy, $H_\infty(X)$, as shown in Fig. 5.3, and enabling efficient extraction of high-quality random bits.

To validate the versatility of the current QRNG scheme, we further measured the min-entropy of the raw bits and the Bell's parameter, S , of the entangled photon state, while varying the coefficients, $|\alpha|$ and $|\beta|$. Keeping the pump power to the experiment constant, we varied the angle θ of the $\lambda/2$ plate from 0 to 45° to change the power of the CW and CCW beams of the Sagnac loop and subsequently vary the output state of the pair-photons. As a result, the $|\alpha|$ (and corresponding $|\beta|$) value changes from 0 (1) to 1 (0), transitioning the output state of the pair-photons from $|VV\rangle$ to $|HH\rangle$. At $\theta = 22.5^\circ$, where $|\alpha| = |\beta| = 0.707$, the photons form a maximally entangled Bell state, $|\phi^-\rangle = (|HH\rangle - |VV\rangle)/\sqrt{2}$. For other θ values, the state remains non-maximally entangled. The results, as presented in Fig. 5.6, show that the Bell's parameter, S (red dots), varies from 1.62 to 1.57, reaching a maximum of 2.13 for the maximally entangled state. Interestingly, the measured min-entropy ($\sim 99\%$, black dots) of the raw bits collected for different states of the pair-photons remains consistent across different photon states, independent of the Bell's parameter, S . Again, for photon states, $|VV\rangle$ and $|HH\rangle$, and non-maximally entangled states, the value of Bell's parameter ($S < 2$) might not certify the quantumness of the source used for QRNG. In such cases, one can use the $g^{(2)}(0)$, used in our previous work [150], as the suitable parameter to certify the quantumness of the source used for QRNG. Unlike previous reports [159, 160]

that rely on beam-splitters, our novel QRNG scheme generates random bits directly from the quantum-mechanical spatial and temporal correlations of photon pairs, without requiring a beam-splitter even for non-maximally entangled or single-pair photon states.

Finally, we note that the transitions from maximally entangled states to non-maximally entangled states, or even to pure pair-photon states ($|VV\rangle$ and $|HH\rangle$), can occur for several reasons. These include relative phase shifts in the interferometer (arising from mirror vibrations or crystal translation) and variations in pump power (controlled via half-wave plate rotation) between the clockwise and counterclockwise beams in the Sagnac interferometer. Although crystal temperature drifts do not alter the quantum state itself, they modify the SPDC ring size and photon collection efficiency, thereby affecting the overall bit rate. Importantly, as shown in Fig. 5.6, changes in the quantum state do not degrade the QRNG performance. In situations where the state drifts to a non-maximally entangled state, or only a pair-photon state is produced and direct certification through the Bell parameter (S) is not feasible, the $g^{(2)}(0)$ test provides a reliable means of certifying the quantum nature of the source. Furthermore, the device-independent classification of the QRNG remains valid owing to the coincidence-based bit assignment scheme.

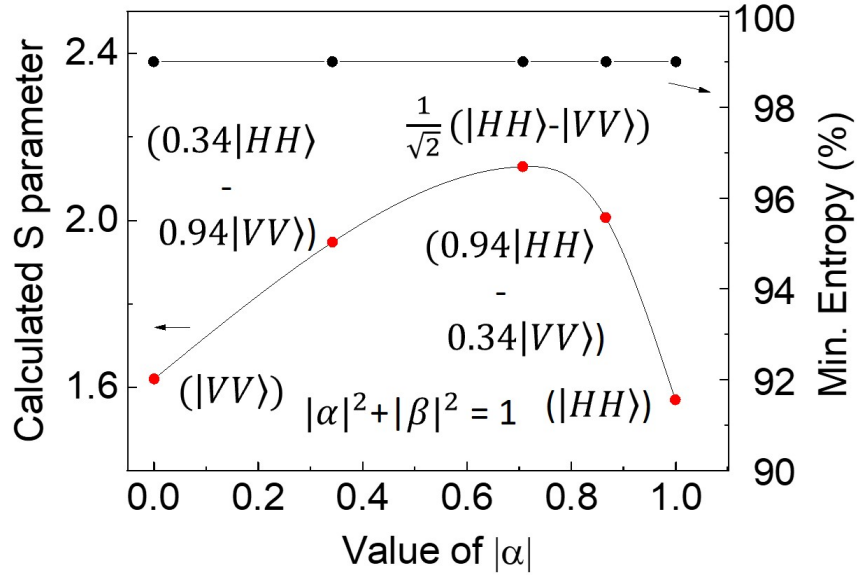


Figure 5.6: Effect of output photon state on performance of QRNG. Variation of Bell's parameter and corresponding min-entropy of the raw bits of QRNG as a function of the weightage parameter, $|\alpha|$. The lines are guide to the eye.

To gain further insight into the current study, we have tabulated the bit rate and quantumness certification parameters of recently reported device-independent QRNG systems. As evident from Table 5.1, our QRNG system, certified with a live Bell's parameter value, demonstrates a bit rate that is two orders of magnitude higher compared to previous reports.

Table 5.1: Comparison of the bit rate of QRNG based on coincidence detection.

Reports	Certifying Parameter	Value	Bit rate (bits/sec)
Ref.[133]	S	-	1.71
Ref.[134]	S	-	$1.81 \cdot 10^2$
Ref.[135]	S	2.016	$2.40 \cdot 10^2$
Ref.[119]	S	2.656	$4.40 \cdot 10^3$
Ref.[136]	S	-	$1.35 \cdot 10^4$
Current study	S	2.07	$1.8 \cdot 10^6$

5.4 Conclusions

We have successfully demonstrated a novel beam-splitter-free, high-bit-rate DI-QRNG system with simultaneous quantumness certification through live Bell test data. The randomness is derived from direct access to the random occurrence of pair-photons at diametrically opposite points on the annular ring distribution of entangled photons, generated via a non-collinear degenerate SPDC process in a type-0 phase-matched PP-KTP crystal within a polarization Sagnac interferometer. At a pump power of 12.4 mW and a 1 ns coincidence window, we achieved an entanglement visibility of $\sim 73\%$ and a Bell parameter, $S = 2.07$, and recorded high-quality quantum random bits of length of 90 million of raw bits having minimum entropy $>97\%$, which is further confirmed by an autocorrelation coefficient ($\sim 10^{-6}$). Using Toeplitz post-processing, we have verified the QRNG of a bit rate of 1.8 Mbps, passing all NIST and TestU01 test suites. Notably, increasing the coincidence window to 2 ns reduced visibility to 61% and the Bell parameter to $S = 1.73$, but the produced raw bits has minimum entropy $>95\%$ and a post-processed QRNG bit rate of 2.18 Mbps. In the absence of the Bell parameter for the non-maximally entangled state or arbitrary output photon state, $g^{(2)}(0)$ can be the metric for the quantumness certification. Although we have divided the annular ring of the pair-photons into six sections, forming three high-brightness entangled photon sources from a single resource (laser, nonlinear crystal, and optical elements) for QRNG and live Bell's test, the generic experimental scheme can in principle be used to create more sections of the SPDC ring to form more number of entangled photon sources to enhance the bit-rate of DI-QRNG and for other advanced quantum networks. The novel design utilizing spatial randomness simplifies the technical requirements of DI-QRNGs and sets a new benchmark for the trustworthiness of the generated random numbers in real-world applications. Based on the high-rate QRNG

using a single photon source in the last chapter, here we make the photon pair entangle in the polarisation degree of freedom for certifying our spatial randomness-based QRNG scheme as a device-independent scheme. Increasing the number of section pairs from the SPDC ring, we enables live certification in parallel with high-rate bit generation rather than doing these separately, as in the earlier chapter. We also show how this scheme translates to the earlier scheme in the absence of a maximally entangled state. Furthermore, we will examine how this intrinsic randomness can be utilized for quantum key distribution in the next chapter.

Chapter 6

Spatial-Randomness-Based Quantum Key Distribution

Quantum key distribution (QKD) using entangled photon sources (EPS) is a cornerstone of secure communication. Despite rapid advances in QKD, conventional protocols still employ beam splitters (BSs) for passive random basis selection. However, BSs intrinsically suffer from photon loss, imperfect splitting ratios, and polarization dependence, limiting the key rate, increasing the quantum bit-error-rate (QBER), and constraining scalability, particularly for long-distance QKD. By contrast, EPSs based on spontaneous parametric down-conversion (SPDC) intrinsically exhibit quantum randomness in the spatial and spectral degrees-of-freedom, offering a resource for a lossless, scalable replacement for BS. Here, we demonstrate a proof-of-concept QKD scheme that exploits the intrinsic spatial randomness of SPDC without employing beam splitters. We divided the annular SPDC emission ring into four spatial sectors, effectively creating two independent EPSs and shared between two users. Further, exploiting the intrinsic detector timing jitter, we have devised two different protocols

to assign the measurement basis after photon detection, thereby concealing the basis information from a potential eavesdropper. This post-detection basis assignment emulates stochastic basis choice while avoiding BS-induced losses and bias. Experimentally, our scheme achieves a 6.4-fold enhancement in sifted key rate, a consistently reduced QBER, and a near-ideal encoding balance between linear and rectilinear bases. Extending this approach to the spectral domain eliminates the need for multiple spatial channels and can increase the secure key rate, enabling long-distance fiber-based QKD. Harnessing intrinsic spatial/spectral randomness thus enables robust, bias-free, high-rate, and low-QBER QKD, offering a scalable pathway for next-generation quantum networks.

6.1 Introduction

Classical communication underpins the modern digital age, with data security relying on the computational complexity of breaking encryption schemes [23, 161]. However, the rapid progress in quantum computing, with scalable high-quality qubits on the horizon, poses a profound threat to this security. In particular, Shor's algorithm [161–163] exposes the vulnerability of widely used classical encryption methods to quantum attacks, underscoring the urgent need for more resilient solutions.

Quantum key distribution (QKD), on the other hand, has emerged as a robust alternative for secure key exchange [67, 164–166]. QKD guarantees security even against attempts by an adversary to intercept the key [167–169], thereby remaining unaffected by advances in computational power, including those offered by quantum computers. As a result, the QKD protocols have progressed from laboratory demonstrations to real-world deployment through various protocols, including BB84 [23, 164], SARG04 [170], COW [171], and E91 [67]. Among these, BB84, the prepare and measure pro-

tol based on weak coherent pulses, has emerged as the most practical choice for implementation, owing to its simplicity as well as the availability of composable security proofs [167, 172], despite known vulnerabilities to specific attacks [173, 174]. In parallel, entanglement-based QKD (EBQKD) protocols [67, 175, 176] have evolved, offering enhanced security owing to two fundamental quantum principles, the no-cloning theorem [177] and entanglement monogamy [178–180]. While EBQKD has been demonstrated over long free-space links by deploying entangled photon sources on satellites to enable key exchange between distant stations [166, 181, 182], its security, verified through entanglement measurements such as Bell inequality violations [67], ensures robustness against a wide spectrum of sophisticated attacks. Alternatively, the BBM92 protocol [183] enables secure key distribution without the need for continuous monitoring of Bell inequalities, offering higher key rates and reduced resource requirements provided that the shared state preserves maximal entanglement. In this framework, security is ensured through post-processed quantum bit error rate (QBER) evaluation combined with occasional Bell inequality verification, allowing device-independent operation [184] without relying on trusted nodes [175, 185]. This positions EBQKD as a strong candidate for future quantum networks. Nonetheless, practical implementations face inherent challenges, including low key rates originating from the limited brightness of spontaneous parametric down-conversion (SPDC) sources [186], and imperfections in 50:50 beam splitters used for random basis (Z and X) selection, thus introducing encoding bias and increased QBER [187]. Although brightness can be improved through the use of high figure-of-merit nonlinear materials and optimized system configurations [92, 188], the use of beam splitters remains a critical bottleneck. In particular, beam splitters not only suffer from practical deviations from the ideal 50:50 ratio, but also impose a fundamental 50% loss in conventional schemes [172, 189], thereby limiting achievable key rates. It is therefore crucial to

explore new experimental strategies that achieve high key rates and low QBER while eliminating the dependence on beam splitters.

Here, we demonstrate a high-performance implementation of the BBM92 protocol that exploits the intrinsic spatial randomness of SPDC photons. Using a type-0 phase-matched PPKTP crystal embedded in a polarization Sagnac interferometer, we generate polarization-entangled Bell states at diametrically opposite positions on the annular spatial emission of the photon pairs. The use of intrinsic quantum randomness of correlated photon pairs emitted at opposite points on the SPDC ring [150], together with post-detection basis assignment enabled by intrinsic detector timing jitter, our approach eliminates the need for beam splitters in random basis selection and thereby avoids beam-splitter-induced loss and bias. Experimentally, we observe a 6.4-fold enhancement in the sifted key rate and a consistently reduced quantum bit error rate (QBER) compared with conventional beam-splitter-based BBM92 implementations. Furthermore, the scheme achieves a near-ideal balance between the Z (H/V) and X (D/A) bases, enabling reliable and low-QBER key generation.

6.2 Experiment

The concept of the spatial randomness-based BBM92 scheme is illustrated in Fig. 6.1(a). The entangled photon source (EPS) can generate any of the four Bell states, $|\Phi^\pm\rangle$ and $|\Psi^\pm\rangle$. By applying a spatial-division scheme [190] to the annular ring distribution of the single EPS, constructed from a common set of physical resources including pump laser, nonlinear crystal, and interferometric architecture, we obtain two (see Fig. 6.1(b)) effective time-multiplexed EPSs (EPS 1 and EPS 2). The generation of pair photons from EPS 1 and EPS 2 is intrinsically quantum-random in time and unbiased. These pair photons are distributed between two users, Alice and Bob. Log-

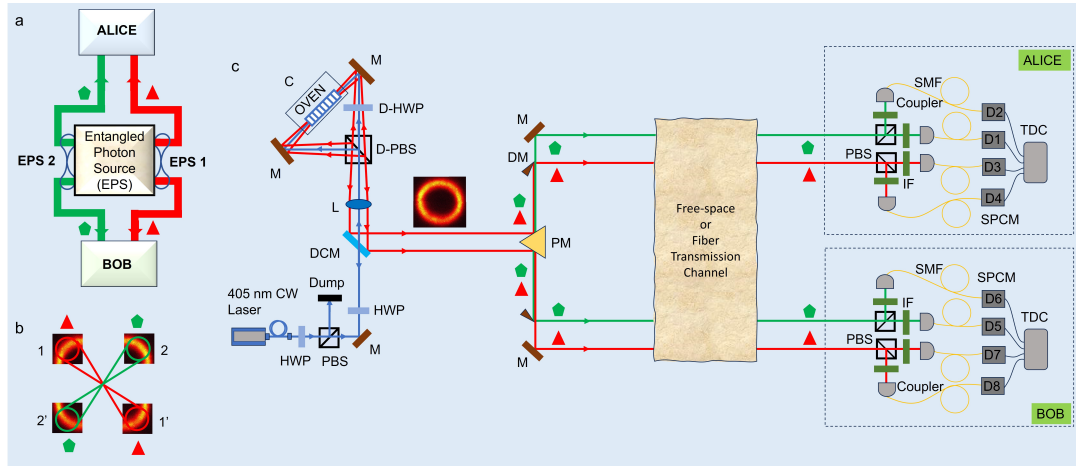


Figure 6.1: Experimental setup and network architecture. **a**, Conceptual representation of the present BBM92 scheme. **b**, Division of the spatial distribution of pair photons to form two identical entangled photon sources. **c**, Schematic of the experimental setup. Laser: 405 nm cw diode laser; HWP: half-wave plate; PBS: polarizing beam splitter; M: mirrors; DCM: dichroic mirror; L: plano-convex lenses; D-PBS: dual-wavelength (405 nm and 810 nm) PBS; D-HWP: dual-wavelength HWP; C: PPKTP crystal in an oven for photon-pair generation; PM: prism-shaped gold-coated mirror; DM: D-shaped mirrors; IF: 3 nm bandwidth interference filter; Coupler: collimator system for fiber coupling; SMF: single-mode fiber; SPCM: single-photon counting module; TDC: time-to-digital converter.

ical bits are encoded as the conventional schemes, with “0” and “1” corresponding to detections in the H/D and V/A polarizations, respectively.

The schematic of the experimental setup is shown in Fig. 6.1(c). A continuous-wave, single-frequency diode laser delivering 40 mW of output power at a central wavelength of 405 nm, with a linewidth of approximately 20 MHz, is used as the pump source. A polarizing beam splitter (PBS) cube, in combination with a half-wave plate (HWP), is used to control the incident pump power. A second HWP, oriented with its fast axis at 22.5° relative to the vertical, rotates the horizontally polarized pump beam into a diagonal state. The pump is then focused to a waist diameter of $\sim 40 \mu\text{m}$ at the center of the nonlinear crystal using a plano-convex lens (L) with focal length $f = 150 \text{ mm}$. The nonlinear medium is a 10-mm-long periodically poled

potassium titanyl phosphate (PPKTP) crystal (SLF Svenska Laserfabriken AB) with a $2 \times 1 \text{ mm}^2$ in aperture and a single grating period $\Lambda = 3.425 \text{ }\mu\text{m}$. The crystal, housed in a temperature-controlled oven (stability $\pm 0.1^\circ\text{C}$, tunable up to 200°C), is positioned at the center of a polarization Sagnac interferometer formed by a dual-wavelength PBS (D-PBS, designed for 405 and 810 nm) and two plane mirrors (M). A dual-wavelength half-wave plate (D-HWP) placed inside the Sagnac interferometer, with its fast axis at 45° , flips the polarization between horizontal and vertical. Under these conditions, the crystal produces non-collinear, degenerate, type-0 ($e \rightarrow e + e$) pair photons at 810 nm via quasi-phase-matched spontaneous parametric down-conversion (SPDC). As described in earlier work [92, 124], the clockwise and counterclockwise pump components inside the Sagnac interferometer generate pair photons with orthogonal polarizations, which combine at the D-PBS to produce the maximally entangled state, $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$. The annular distribution of the down-converted photons is collimated by the lens (L) and separated from the pump by a dichroic mirror (DCM). The SPDC ring is divided into two halves using a prism-shaped gold-coated mirror (PM), and each half is further subdivided into two sections by D-shaped mirrors (DM), yielding four spatial regions denoted 1, 2, 1', and 2'. For visualization, pair photons from regions (1, 1') and (2, 2') forming EPS 1 and EPS 2 are labeled as red triangles and green pentagons, respectively. The spatial sections (1, 2) and (1', 2') of the SPDC ring are distributed between Alice and Bob, respectively. The pair photons of each sections are projected in two orthogonal polarizations states using the PBS. The photons of the output ports of the PBSs are spectrally filtered by $\sim 3 \text{ nm}$ interference filters (IF), coupled into single-mode fibers (SMFs), and measured by single-photon counting modules (SPCMs) connected to the time-to-digital converter (TDC) interfaced with a computer for coincidence detection and data processing. Both Alice and Bob have four SPCMs, D1-4 and D5-8 respectively, connected to the TDC to record

the detection time stamps of photons. Unless otherwise stated, the coincidence window is maintained at 1 ns throughout the manuscript. Alice uses detectors D1 and D2 to measure the transmitted and reflected outputs of PBS1 for photons from EPS1, while detectors D3 and D4 measure the corresponding outputs of PBS2 for photons from EPS2. Similarly, Bob uses detectors D5 and D6 to measure the transmitted and reflected outputs of PBS1 for photons from EPS1, while detectors D7 and D8 measure the corresponding outputs of PBS2 for photons from EPS2.

As observed previously [150], at any given instant EPS 1 and EPS 2 have equal probability of generating pair photons. Therefore, all detectors have an equal probability of detecting photons, without the bias commonly observed in beam-splitter-based schemes due to the inherent imperfections of practical 50:50 beam splitters. Under ideal conditions, the photon count rates of all detectors are expected to be equal, provided that the detectors have identical detection efficiencies and all optical channels are equally coupled. Any imbalance in detector efficiency introduces similar artifacts in other QKD schemes as well. Thus, with proper calibration and alignment of the detectors, we can detect comparable photon count rates across all detectors in the present scheme, eliminating the losses. Now the simplest approach to achieve a high bit-rate QKD scheme is to assign fixed measurement bases, Z or X , to photons originating from EPS1 and EPS2 for both Alice and Bob. However, such an arrangement introduces fundamental security vulnerabilities because the basis selection effectively occurs at the source, while EPS1 and EPS2 remain distinguishable either spatially or spectrally. As a result, an eavesdropper (Eve) may exploit side-channel information to infer the measurement basis without disturbing the quantum state. To mitigate this vulnerability, we assign the measurement basis only after photon detection by exploiting intrinsic detector timing jitter to conceal the basis information from Eve. Based on this principle, we propose two protocols, referred to as Protocol #1 and Protocol #2. In Protocol #1, Alice

and Bob record the detection timestamps (t_A and t_B) from all detectors and publicly announce the timestamps together with the corresponding source label (EPS1 or EPS2), while keeping the detector identity private. They retain only those events originating from matched sources and further post-select coincident events satisfying $|t_A - t_B| \leq 1$ ns. For each coincident event, they compute $b = |t_A - t_B| \bmod 2$ and assign the measurement basis as Z (H/V) for $b = 0$ and X (D/A) for $b = 1$. Like the standard BBM92 scheme, here also the detections in the Z and X are encoded as logical bits “0” for the H and D and “1” for V and A polarization outputs. Since the basis assignment is derived jointly from coincident detection events, no basis mismatch occurs, leading to a fourfold increase in the sifted key rate compared to the conventional BB84 protocol. The security of this scheme, however, critically depends on strong assumptions, including trusted detectors, intrinsic and uncontrollable timing jitter, and the operational indistinguishability of the photon sources. In Protocol #2, Alice and Bob independently record detection timestamps at their respective stations and determine the basis using the time difference between consecutive detections, defined as $b = |t_{i+1} - t_i| \bmod 2$, assigning Z or X bases for $b = 0$ or 1, respectively. Similar to the BBM92 protocol, Alice and Bob publicly announce the timestamps, source information, and basis choices. Because the basis selection is performed independently, approximately 50% of coincident events are discarded due to basis mismatch. Nevertheless, due to the use of two sources, this scheme still achieves a twofold improvement in sifted key generation rate relative to the standard protocol. Importantly, Protocol #2 relies on weaker trust assumptions and therefore offers improved security robustness compared to Protocol #1, but at the cost of reduced efficiency. Overall, Protocol #1 prioritizes maximum key-rate enhancement under stringent detector-trust assumptions, whereas Protocol #2 provides a more conservative and secure implementation with moderate efficiency gains.

Two entangled photon sources (EPS1 and EPS2) can also be derived from a single SPDC source through energy conservation, corresponding to correlated signal–idler wavelength pairs (λ_1, λ_2) and (λ_3, λ_4) . The generation of photon pairs with different wavelength combinations that satisfy energy conservation is intrinsically random, analogous to the random spatial-mode distribution in SPDC. However, in the conventional BBM92 protocol, only one such wavelength pair (either EPS1 or EPS2) is utilized for QKD, while the remaining spectral components, corresponding to other correlated wavelength pairs within the SPDC bandwidth, are discarded. In contrast, the present approach exploits these otherwise unused spectral components to enable high-bit-rate implementation of the BBM92 protocol. This is achieved without increasing the number of quantum communication channels between the two users, requiring only the same two channels as in the standard BBM92 scheme.

Finally, the sifted key is subsequently processed using standard error correction (EC) and privacy amplification (PA) protocols to distill the final secure cryptographic key. It is important to emphasize that all experimental parameters reported here are derived directly from raw data without applying any corrections. While the implementation of such corrections could further improve the reported values, they do not hold practical significance for real-time applications of QKD systems. Hence, the uncorrected results presented here provide a more realistic performance assessment of the current protocol under operational conditions.

6.3 Results and discussions

We first characterized EPS 1 and EPS 2 in terms of their quantum performance parameters, including entanglement visibility, Bell parameter, and state fidelity. As both sources are derived from a single entangled photon source, they exhibit nearly

identical characteristics. For clarity, we present the representative results of EPS 2 (see green paths in Fig. 6.1(b)). The measurements, summarized in Fig. 6.2, were performed at a fixed pump power of 3 mW and crystal temperature of $T = 41.5^\circ\text{C}$.

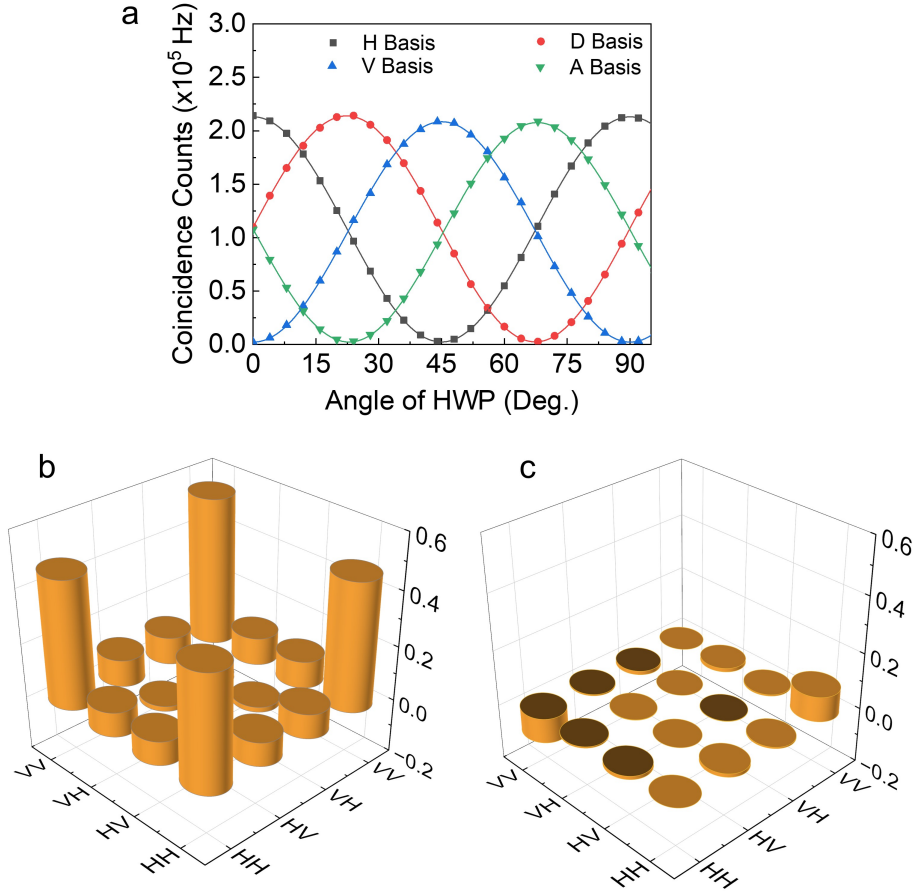


Figure 6.2: Characterization of the entangled photon sources. **a**, Quantum interference of spatially separated entangled photon sources measured in the horizontal (H, black dots), vertical (V, blue dots), diagonal (D, red dots), and anti-diagonal (A, green dots) polarization bases. Solid lines represent sinusoidal fits to the experimental data. Absolute values of **d**, real and **e**, imaginary parts of the reconstructed density matrix of the polarization-entangled Bell state $|\phi^+\rangle$.

We recorded the coincidence counts between photons transmitted through the PBS of both Alice and Bob, with Alice having fast axis of the HWP fixed at 0° , 22.5° , 45° , and 67.5° , corresponding to the *H* (black), *V* (blue), *D* (red), and *A* (green)

bases, respectively, while Bob continuously rotated the HWP from 0° to 90° in 4° steps. The resulting interference fringes are shown in Fig. 6.2(a). As shown in Fig. 6.2(a), the coincidence counts exhibit the expected sinusoidal modulation, with measured fringe visibilities of 97.8%, 97.8%, 97.7%, and 97.7% in the H , V , D , and A bases, respectively—well above the quantum threshold of 71% [92], thereby confirming high-quality entanglement. Furthermore, by analyzing coincidence counts across 16 different combinations of HWP settings of Alice and Bob and applying the standard CHSH inequality formalism [145], we obtained a Bell parameter of $S = 2.765 \pm 0.007$, clearly violating the classical bound by nearly 109 standard deviations. Further, we carried out quantum state tomography based on coincidence measurements across different polarization projections. The reconstructed real and imaginary parts of the two-qubit density matrix, shown in Fig. 6.2(b) and 6.2(c), respectively, confirm the generation of the maximally entangled Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$ with a fidelity of 97%. The source brightness of EPS 2 is estimated to be 0.04 MHz/mW/nm. We observed comparable performance parameters for EPS 1, similar to the results of sectioning of SPDC ring for formation of three sources presented for quantum network and QRNG [150, 190]. These results establish the suitability of both EPS 1 and EPS 2 for the implementation of the QKD protocol.

With the quantum parameters of the entangled photon sources established, we implemented the BBM92 protocol and benchmarked its performance against the conventional beam-splitter-based approach. Keeping the crystal temperature fixed at 41.5°C , we measured the sifted key rate and QBER as functions of pump power. The results are shown in Fig. 6.3. As expected, the sifted key rate (see Fig. 6.3(a)) calculated by summing all the coincidence counts of same basis detection of two users (here, Alice and Bob), increases with pump power in both cases owing to the higher pair-generation rate. In basis-randomization Protocol #1 (red dots), the sifted key rate increases from

0.29 Mbps to 2.9 Mbps as the pump power is raised from 1 to 13 mW, corresponding to a slope of 0.22 Mbps/mW for a one-meter free-space link. In basis-randomization Protocol #2 (blue dots), the sifted key rate increases from 0.148 Mbps to 1.52 Mbps over the same pump-power range, yielding a slope of 0.11 Mbps/mW. By contrast, the conventional scheme (black dots) exhibits only a modest increase from 0.045 Mbps to 0.47 Mbps, with a slope of 0.035 Mbps/mW. Such a superior performance of our current BBM92 with post detected basis randomization protocols (# 1 and 2) in terms of higher sifted key rate with respect to the conventional BBM92 scheme can be understood as follows. Let us consider one of the derived sources, EPS1. In the absence of a beam splitter, the coincidence rate between Alice and Bob in the same basis (e.g., Z) is N_{CC} . Introducing an ideal 50:50 beam splitter at each photon path of Alice and Bob reduces the useful coincidences to the transmitted–transmitted and reflected–reflected outputs, leading to a 50% loss [191] and a key rate of $N_{CC}/2$. In Protocol #1, the measurement basis for coincident events is assigned in a correlated manner, thereby eliminating the conventional loss arising from basis mismatch. In contrast, Protocol #2 employs independent basis assignment at Alice and Bob, leading to a 50% loss of coincident events due to basis mismatch, similar to the standard BBM92 protocol. Moreover, our scheme avoids beam splitters and utilizes two entangled photon sources, EPS 1 and EPS 2. Consequently, Protocol #1 and Protocol #2 yield sifted key rates of $2N_{CC}$ and N_{CC} , corresponding to fourfold and twofold enhancements, respectively, compared to the conventional BBM92 scheme.

Experimentally, we observe more than sixfold and three fold enhancement (Fig. 6.3(a)) in the sifted key rate for Protocol #1 and Protocol #2 with respect to conventional BBM92 protocol under similar experimental conditions, which we attribute to non-ideal splitting ratios, inherent bias, and losses in practical beam splitters.

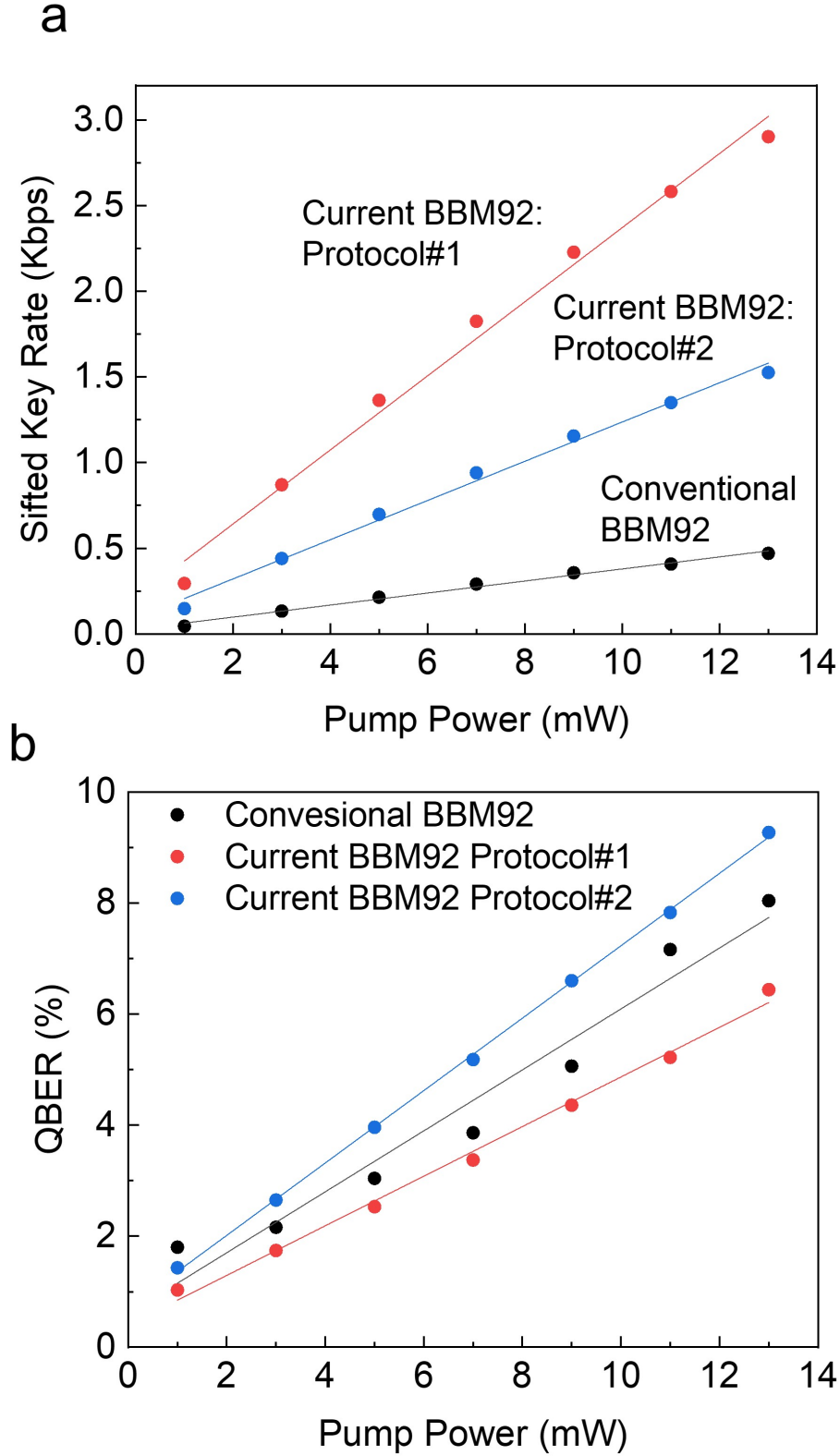


Figure 6.3: Performance metrics of the QKD schemes. (a) Sifted key rate and (b) quantum bit error rate (QBER) as functions of pump power for the current BBM92 scheme with Protocol #1 (red circles), Protocol #2 (blue circles) and the conventional BS-based BBM92 scheme (black circles). Solid lines represent linear fits to the experimental data.

Further, we quantify the QBER using the following equations,

$$R_{sif} = CC_{HH} + CC_{VV} + CC_{DD} + CC_{AA} + CC_{HV} + CC_{VH} + CC_{DA} + CC_{AD} \quad (6.1)$$

and

$$QBER = \frac{CC_{HV} + CC_{VH} + CC_{DA} + CC_{AD}}{R_{sif}} \quad (6.2)$$

where $CC_{HH}, \dots, CC_{AA}$ and $CC_{HV}, \dots, CC_{AD}$ denote coincidence counts in the correct and incorrect bases, respectively. As shown in Fig. 6.3(b), the QBER in our scheme for Protocol #1 (red dots) increases from 1.03% to 6.44% at a slope of 0.45%/mW, and for Protocol #2 (blue dots) increases from 1.43% to 9.28% at a slope of 0.65%/mW, whereas the conventional approach (black dots) rises from 1.8% to 8.04% at 0.55%/mW. These results confirm that the present BBM92 scheme with new basis randomization protocols, which exploits the intrinsic spatial randomness of SPDC photons, outperforms the conventional beam-splitter-based scheme by simultaneously achieving higher key rates and lower QBER.

We computed the coincidence counts between Alice and Bob for both the present scheme and the conventional BBM92 scheme at a fixed pump power of 3 mW. The distribution of coincidence events across the Z and X bases provides a measure of the intrinsic randomness in linear and rectilinear basis encoding. Ideally, this distribution should approach a 1:1 ratio. For the conventional BBM92 scheme, the numbers of encoded bits in the H/V and D/A bases are 74.9 kHz and 58.42 kHz, respectively,

yielding a ratio of 1.3:1 and indicating deviations from the ideal case due to beam-splitter imperfections. In contrast, for Protocol #1 the numbers of encoded bits in the H/V and D/A bases are 436.5 kHz and 434 kHz, while for Protocol #2 they are 220 kHz and 220 kHz, respectively, resulting in a nearly ideal 1:1 ratio. These results confirm that the spatially random distribution of SPDC photons enables unbiased, quantum-mechanical encoding, consistent with our previous report [190].

Table 6.1: Comparison of QKD performance metrics between the beam-splitter-based conventional BBM92 protocol and the spatial-randomness-based implementation introduced here.

Parameters	Conventional Scheme	Present Scheme	
		Protocol #1	Protocol #2
Encoding ratio (H/V:D/A)	1.3:1	1:1	1:1
QBER (%)	8.04	6.44	9.27
Sifted key rate (Mbps)	0.47	2.90	1.52
Post EC key rate (Mbps)	0.45	2.76	1.44
Key rate after PA (Mbps)	0.15	1.02	0.45
Secure key rate (Mbps)	0.15	1.02	0.45

To provide a clear comparison between the present BBM92 scheme and the conventional beam-splitter-based BBM92 scheme, we summarize the key performance parameters, including QBER, sifted key rate, error-corrected key rate, privacy-amplified key rate, and the final secure key rate in Table 6.1. The calculations employ standard post-processing procedures, with error correction implemented via low-density parity check (LDPC) codes and privacy amplification performed using established algorithms. As shown in Table 6.1, our spatial-randomness-based scheme with both basis randomization protocols consistently outperforms the conventional protocol across all stages of key generation, demonstrating its advantage for high-rate and secure quantum communication. Furthermore, the optical design can be simplified, and the number of usable spatial sections can be increased using advanced collection schemes such as

ring-shaped microlens arrays or multicore fibers matched to the SPDC profile. Increasing the number of usable spatial sections using D-shaped mirror sectioning is challenging at the alignment level and introduces diffraction from the mirror edges, leading spatial cross-talk.

6.4 Conclusions

We demonstrate a new experimental implementation of an efficient and scalable BBM92 QKD protocol by exploiting the intrinsic quantum-mechanical randomness of the spatial distribution of photon pairs generated through momentum conservation in the SPDC process. Using a polarization-entangled photon source with an annular spatial-ring distribution, we derive two entangled photon sources that generate photon pairs randomly and used them for QKD. Unlike the conventional approach, this method avoids bit loss arising from imperfections of physical beam splitters. However, the spatial distinguishability of the photon pairs could, in principle, introduce security vulnerabilities. We mitigate this by performing basis randomization after photon detection using two distinct protocols that exploit the intrinsic timing jitter of the detectors, thereby concealing the basis information from a potential eavesdropper. This post-detection basis assignment effectively emulates stochastic basis selection while avoiding beam-splitter-induced losses and bias. The security of the scheme nevertheless relies on the assumptions of trusted detectors, intrinsic and uncontrollable timing jitter, and the operational indistinguishability of the photon sources.

In a proof-of-concept demonstration over a 1 m free-space link and under identical experimental conditions, the scheme achieves sifted key rates in the megabits-per-second regime, corresponding to a 6.4-fold enhancement over the conventional BBM92 protocol, consistently lower QBER ($< 7\%$) across varying pump powers, and a near-ideal encoding balance between linear and rectilinear basis, thereby eliminating

encoding bias. Although the present spatial randomness scheme requires four quantum channels, it can be adapted to fiber-based QKD systems by exploiting energy conservation to generate two wavelength-correlated entangled sources from a single SPDC process and by using wavelength demultiplexers instead of beam splitters. In principle, this approach can be extended to other photonic degrees-of-freedom such as spatial modes, orbital angular momentum, time-bin, or phase encoding, provided that mutually unbiased bases can be generated and reliably detected. Thus, the spatial or wavelength demultiplexing-based randomness establishes a practical route toward a high-rate, low-error, and bias-free BBM92 QKD protocol using a Bell state. Till the last chapter, we generated random bit strings in localised form and addressed the lower bit rate issue. Here, we demonstrated distributing a random bit string (key) between two users via an entangled Bell state. In conventional QKD, the key rate is also lower because we discard 50% of the coincident events and losses incur at the beam splitter ports. Additionally, beam-splitter splitting imbalance results in non-ideal encoding (deviates from 1:1) in two mutually unbiased bases. Our current demonstration of spatial randomness with intrinsic detector jitter provides a practical pathway to high-rate, low-error, bias-free entanglement-based BBM92 QKD, which can enable a large-scale quantum communication link. Now, the question arises do we strictly need the Bell state from the source end? That is, the next chapter, where we revive a polarization entangled Bell state at the receiver end from any arbitrary Bell-like state for QKD application.

Chapter 7

Bell State Revival using Geometric Phase for QKD Application

Entanglement-based quantum key distribution (QKD) systems fundamentally depend on the ability to generate and maintain stable, maximally entangled Bell states between distant parties. However, maintaining a high-quality, maximally entangled Bell state in practical implementations is challenging due to unwanted phase drifts from various sources, such as birefringence in optical components and nonlinear crystals, phase induced within the pump beam, imperfect generation from the nonlinear crystal, and environmental disturbances during photon transmission. Such phase variations reduce entanglement visibility and increase the QBER, ultimately compromising the QKD security performance. Different common approaches to phase compensation at the pre- and post-generation stages of SPDC include the insertion of birefringent crystals in the pump beam and the use of dedicated phase-compensating crystals after photon pair generation, either in the single arm or in both the signal and idler arms. Other strategies involve engineering the design of the nonlinear crystal, interferometric sta-

bilization, and spatial light modulation, all of which are performed at the source end. Here, we propose and implement a novel approach of phase compensation at the receiver end within a BBM92 quantum key distribution scheme using geometric phase as a tool. We analytically derive and experimentally validate the dependence of QBER on the geometric phase of the pump beam, demonstrating that it theoretically reaches a maximum of 25% when the induced phase is $\mp i$ in the Bell-like states. Next, using the second geometric phase system (a quarter–half–quarter wave plate) at any of the receiver ends precisely cancels the phase imprint in the entangled state. This compensation restores the entangled state to a standard Bell state with high fidelity ($> 95\%$), thereby enabling a reduction in QBER to a value below the security threshold of 11%. Our approach presents a systematic method for phase measurement based on the QBER value, and then actively compensates for the phase to revive the entangled Bell state for QKD applications.

7.1 Introduction

Entanglement-based quantum key distribution (QKD) protocols rely critically on the stable generation and preservation of maximally entangled Bell states shared between distant parties [23, 67, 183]. One significant challenge in such systems is the unwanted introduction of phase factors that degrade entanglement visibility and increase the QBER, thereby limiting the generated state for secure QKD applications. The different reasons for phase drifting in the generated entangled pair photons are mainly birefringence, phase contribution from the pump beam, imperfect generation from the nonlinear crystal, and transmission through the practical environment, among others. So, in order to use the QKD system in a practical condition, the use of an effective phase compensation scheme is necessary to keep the system operating continuously with low QBER. The different phase compensation scheme uses different kinds

of mechanisms, either at the pre-generation stage or at the post-generation stage [192]. The most used techniques of phase compensation in literature are using a birefringent crystal in the pump beam [193, 194], designing and placing a single phase compensating crystal after generation [193, 195], or keeping two crystals in both arms [196, 197], making a special design of the SPDC crystal [198]. Additionally, the interferometric technique [199], the spatial light modulation technique [194, 200], and the use of the polarization controlling paddle units [201] have also been reported.

Now, for active phase compensation [202], it is important to calculate the phase drift and then perform the compensation following the phase drift estimation. The geometric phase plays a vital role in this aspect of estimating the phase drift and actively compensates for the drift for QKD applications. Recent studies have demonstrated that imprinting the geometric phase of a classical pump beam onto polarization-entangled photon pairs generated via spontaneous parametric down-conversion (SPDC) can act as a tunable control of entanglement properties [203]. Specifically, by rotating a half-wave plate within a QHQ configuration in the pump beam path, a controllable geometric phase is transferred to the biphoton state, resulting in a continuous transition between orthogonal Bell states and intermediate maximally entangled Bell-like states. The geometric phase originates from the cyclic evolution mechanism of a classical or quantum state on its parameter space, resulting in an additional phase term associated with the state, also known as the Pancharatnam–Berry phase [204, 205]. It has found broad applications across classical and quantum optics, such as frequency shifting [206], quantum gates for quantum computing [207], quantum metrology [208], and beam shaping [209]. This GP can be readily imprinted through the polarization state evolution on the Poincaré sphere using combinations of wave plates [210] in optics. While this enables novel approaches for phase-dependent quantum operations and state engineering, it also opens new directions for QKD implementations using

maximally entangled Bell states [5, 6, 211], quantum communication [187], quantum teleportation [212], and quantum computing [213].

The induced phase drift degrades entanglement visibility in specific measurement bases, resulting in QBER exceeding the acceptable threshold [23] for secure key distribution [214] temporarily. However, this phase drift effect can be erased at the receiver end in the QKD protocol by compensating for the induced phase drift at the receiver end using an additional compensating geometric phase (QHQ) system. Interestingly, this indicates the revival of a standard Bell state from any arbitrary Bell-like states. It is also possible to cancel the phase acquired during generation because of the non-exact positioning of the crystal inside the Sagnac [215, 216] and transmission of signal and idler photons through different paths in a real-world key distribution scenario. This effectively restores a standard Bell state suitable for entanglement-based QKD protocols. This approach offers a pathway to compensate for phase drifts using geometric phase instead of actively using the phase-compensating birefringent material.

In this work, we report a comprehensive experimental investigation demonstrating that the geometric phase introduced into the classical pump beam of an SPDC source can be precisely compensated at the receiver station using a second QHQ system. For active compensation of the phase drift, we can calculate the phase drift first and compensate it by measuring the most fundamental quantum parameter, QBER, associated with the entanglement-based QKD scheme. By adjusting the compensating half-wave plate angle, we restore the standardized Bell state with lower QBER values below the threshold for secure key generation. Our results establish that while arbitrary geometric phase shifts can degrade QBER, they can also be fully recovered at the post-generation stage, even at the receiver end, enabling robust entanglement-based QKD through realistic free space channels, overcoming phase noise. This approach

paves the way for simplified phase control in the entangled photon state and photonic quantum communication systems using geometric phase.

7.2 Theory

The phase of a beam is accumulated in two ways. First, accumulated proportionally from the beams' optical path length, and secondly, because of the evolution of the beam polarization during the propagation. The evolution of polarization states can be described theoretically on the Poincaré sphere geometry, which is why we add the adjective geometric to the phase. To study the effect of the relative phase shift in the entangled photon state on the QBER, we introduced the phase using a GP setup (P-QHQ) in the pump. It provides the expected phase shift in a controlled manner by simply rotating the HWP, as previously reported [203]. In realistic optical channels, phase drift can occur due to birefringence, temperature fluctuations, and path-length differences in signal and idler photons, leading to degradation of QBER. We demonstrate that such phase shifts can be effectively compensated robustly using an additional QHQ setup at either receiver end in QKD. However, in dynamic free-space environments, active stabilization or feedback mechanisms may be required to maintain optimal performance. A QHQ setup consists of a quarter-wave plate (QWP, Q), a half-wave plate (HWP, H), and another quarter-wave plate (QWP, Q), sequentially positioned with their fast axes oriented at angles 45° , θ_H , and 45° , with respect to the vertical, respectively. This geometric phase, $\phi^p (= 2\theta_H^p)$, introduced in the pump beam, results in the entangled state [56] that can be represented [203] as Eq. 7.1

$$|\psi_\phi^-\rangle = \frac{1}{\sqrt{2}} \left(|H\rangle_s |H\rangle_i - e^{i2\phi^p} |V\rangle_s |V\rangle_i \right) \quad (7.1)$$

This generalised expression matches with the polarisation entangle Bell state $|\psi^\pm\rangle$ for angles of θ_H^p at 0° , 45° , and 90° . For other angles, we can not write this generalized state as a Bell state, and we can't use this state for entanglement-based quantum key distribution. It is also shown that the geometric phase of the classical pump beam results in a change of CHSH Bell's parameter [7] following the relation

$$S = \left| \sqrt{2} \right| + \left| \sqrt{2} \cos 2\phi \right| \quad (7.2)$$

Then, the entanglement visibility (V) can be written as a function of the geometric phase

$$\begin{aligned} V &= \frac{S}{\left| 2\sqrt{2} \right|} \\ &= \frac{\left| \sqrt{2} \right| + \left| \sqrt{2} \cos 2\phi \right|}{\left| 2\sqrt{2} \right|} \\ &= \frac{1 + |\cos 2\phi|}{2} \end{aligned} \quad (7.3)$$

As Bell's parameter is directly related to the entanglement visibility, we can write the QBER [191, 217] expression for entanglement-based QKD as a function of the geometric phase

$$QBER = \frac{1 - V}{2} = \frac{1 - |\cos 2\phi|}{4} \quad (7.4)$$

From the above equation, QBER value achieves a minimum of 0% for $\phi = 0^\circ$, a maximum value of 25% for $\phi = 45^\circ$, which is also experimentally verified in the sec-

tion 7.4. Also, if we change the crystal position inside the Sagnac loop from the exact middle position ($z = 0$) to a final position, it produces a similar effect of phase drift within the entangled photon pair. This crystal position, changing from 0 mm to 2 mm, exactly mimics the same effect as changing the geometric phase from 0° to 90° in the pump QHQ system. So we can do a one-to-one mapping of crystal position with an equivalent geometric phase. Hence, the phase term in the generalised entangled state expression in Eq. 7.1 may arise from the crystal position inside the Sagnac loop or because of the geometric phase in the pump beam. This phase drift can be compensated using another QHQ system at the receiver end for QKD applications. That is, although the state was not a standard Bell state initially at the time of the generation from the Sagnac interferometer, we can still make it a Bell state at the receiver end for entanglement-based QKD applications. To do so, one of the communicating parties (here Bob in Fig. 7.1) will use an additional QHQ system in his/her D/A polarisation basis arm. From the [203], it is known that the geometric phase doesn't affect the H/V basis entanglement visibility; it only affects the D/A basis visibility. So they only need to compensate for the effect of the geometric phase in the D/A basis for establishing the QKD scheme. At $\theta_H^p = 0$ the initial Bell state is $|\psi^-\rangle \equiv \frac{1}{\sqrt{2}}(|H\rangle_A|H\rangle_B - |V\rangle_A|V\rangle_B)$. If we change the geometric phase in the pump beam from 0 to $\phi^p (= 2\theta_H^p)$, then the state becomes $|\psi_\phi^-\rangle = \frac{1}{\sqrt{2}}(|H\rangle_A|H\rangle_B - e^{i2\phi^p}|V\rangle_s|V\rangle_i)$. Let Bob need to set his HWP angle θ_H^B within the B-QHQ system at his end to compensate for this phase in the generalised entangled state. As the correlated photon at Bob's end only faces the B-QHQ system, we can write the generalised entangled state after the second QHQ system $|\psi_\phi^f\rangle = \frac{1}{\sqrt{2}}(|H\rangle_A|H^{QHQ}\rangle_B - e^{i4\theta_H^p}|V\rangle_A|V^{QHQ}\rangle_B)$. In that case B-QHQ matrix will be

$$T = QHQ = \begin{pmatrix} e^{2i\theta_H^B} & 0 \\ 0 & -e^{-2i\theta_H^B} \end{pmatrix} \quad (7.5)$$

Using the above matrix $|H^{QH}Q\rangle = T|H\rangle = e^{2i\theta_H^B}|H\rangle$ and $|V^{QH}Q\rangle = T|V\rangle = -e^{-2i\theta_H^B}|V\rangle$.

If we substitute these in the generalised expression, the equation after the compensating QHQ system becomes

$$\begin{aligned} |\psi_\phi^f\rangle &= \frac{1}{\sqrt{2}}(|H\rangle_A e^{i2\theta_H^B}|H\rangle_B - e^{i4\theta_H^P}|V\rangle_A (-)e^{-2i\theta_H^B}|V\rangle_B) \\ &\equiv \frac{1}{\sqrt{2}}(|H\rangle_A|H\rangle_B + e^{i4(\theta_H^P - \theta_H^B)}|V\rangle_A|V\rangle_B) \end{aligned} \quad (7.6)$$

Now, to make this Bell-like state to standard Bell state $\frac{1}{\sqrt{2}}(|H\rangle_A|H\rangle_B + |V\rangle_A|V\rangle_B)$ [218], the condition is

$$\begin{aligned} e^{i4(\theta_H^P - \theta_H^B)} &= 1 \\ \theta_H^P - \theta_H^B &= 90^\circ \\ \theta_H^B &= -(90^\circ - \theta_H^P) \end{aligned} \quad (7.7)$$

Experimentally, we have also observed that the set HWPs angle in the two QHQ systems follows the equation, which will be further emphasised in the results and discussion section 7.4.

7.3 Experiment

Here, for experimental demonstration of the geometric phase effect on the Bell state shared between two parties, Alice and Bob, we used the entanglement-based BBM92 QKD protocol. To initiate the quantum key distribution protocol, the first step

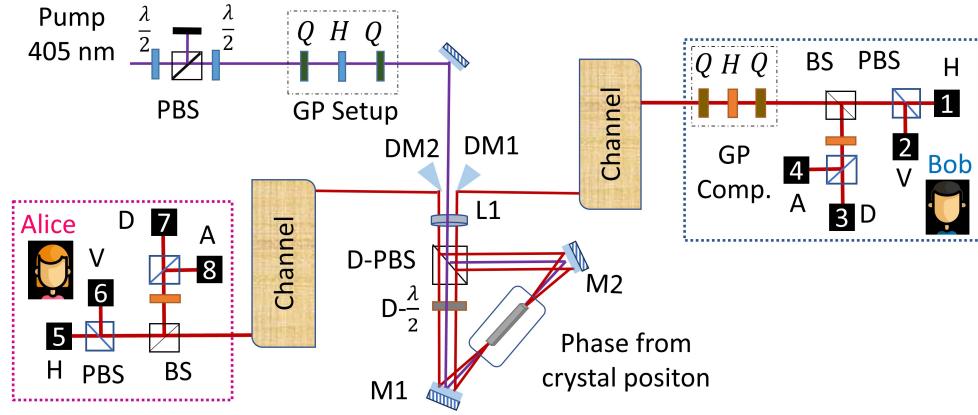


Figure 7.1: The schematic representation of the experimental setup of the BBM92 key distribution. Laser: 405 nm, cw diode laser, $\lambda/2$: Half wave plate, L1: plano-convex lenses of focal length 150 mm, $D - \lambda/2$: Dual Half wave plate, PPKTP: 10 mm long PPKTP crystal of single grating period in temperature oven, Q: quarter wave plate, H: half wave-plate, GP: geometric phase, DM1-2: D-shaped mirrors, 1-8: single photon counting modules.

involves producing pairs of entangled photons. One photon from each pair is directed to Alice, while its partner is transmitted to Bob through a quantum channel.

The entangled photon pairs are produced using a nonlinear crystal inside a polarization Sagnac interferometer, pumped from both directions. The pump source is a continuous-wave, single-frequency laser diode emitting at a wavelength of 405.03 nm, with a linewidth of approximately 20 MHz. A polarizing beam splitter (PBS) cube, in combination with a half-wave plate ($\lambda/2$), is used to control the power of the pump beam entering the nonlinear crystal. An additional $\lambda/2$ plate is included to finely adjust the pump polarization in diagonal (D) polarisation, ensuring that the counterpropagating beams—clockwise (CW) and counterclockwise (CCW)—have equal intensities within the interferometer.

The Sagnac loop is constructed with a dual-wavelength PBS (D-PBS) optimized for both 405 nm and 810 nm, together with two plane mirrors, M1 and M2. The pump beam is focused into the nonlinear crystal using a lens (L1) with a focal length of

150 mm, this lens also collimates the SPDC ring profile. Inside the interferometer, a dual-wavelength half-wave plate ($D-\lambda/2$) is oriented at 45° relative to the vertical axis. This element swaps horizontal and vertical polarization components for both the pump and the down-converted photons. The nonlinear medium is a 10 mm-long periodically poled potassium titanyl phosphate (PPKTP) crystal, with a single grating period of and a clear aperture of $1 \times 2 \text{ mm}^2$. The crystal is configured for noncollinear, type-0 ($e \rightarrow e + e$) phase matching to enable degenerate spontaneous parametric down-conversion (SPDC) at 810 nm. For precise phase matching, the crystal is housed in a temperature-controlled oven, stabilized to within $\pm 0.1^\circ\text{C}$ and capable of reaching temperatures up to 200°C .

As the CW and CCW pump beams pass through the $D-\lambda/2$ plate, they respectively produce the $|HH\rangle$ and $|VV\rangle$ polarized photon pairs at diametrically opposite points on the SPDC emission ring. These contributions recombine at the D-PBS to form the entangled Bell state, $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|H_A H_B\rangle + |V_A V_B\rangle)$ when the crystal is exactly at the middle of the sagnac loop, where the subscripts A and B denote Alice and Bob, respectively. Now, if we introduce the geometric phase setup in the pump beam, it will change the Sagnac-generated entangled state for different angles θ_H of the $\lambda/2$ plate in the middle of the two $\lambda/4$ plates kept at an angle of 45° each with respect to the vertical. This QHQ system changes the D-polarised pump into the polarisation state $\frac{1}{\sqrt{2}} \left(e^{-i2\phi_p} |H\rangle_p - e^{i2\phi_p} |V\rangle_p \right)$ at $\theta_H = 0$ it becomes $\frac{1}{\sqrt{2}} (|H\rangle_p - |V\rangle_p)$ and from Eq. 7.1 the initial $|\Phi^+\rangle$ state becomes $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|H_A H_B\rangle - |V_A V_B\rangle)$ for the exact middle positioning of the crystal inside the sagnac loop.

Now, we have to distribute the entangled photon pairs to Alice and Bob. First, we divide the ring into two halves using two D-shaped mirrors (DM1 & 2). Each half is further guided through the quantum channel to Alice and Bob. For the conventional

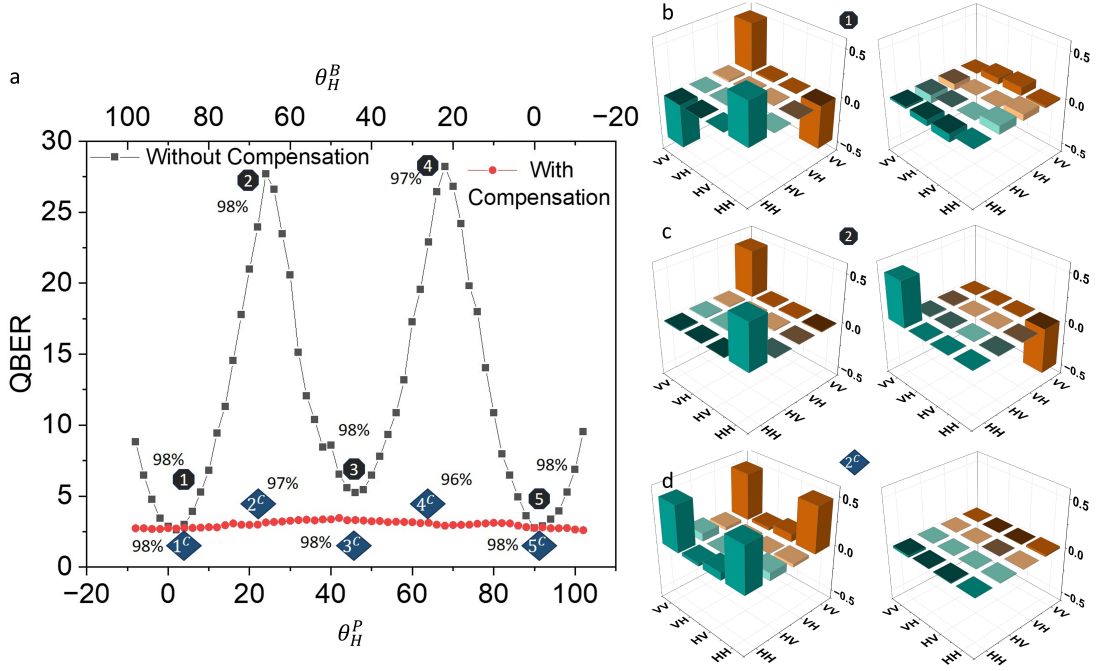


Figure 7.2: (a) Variation of QBER as a function of geometric phase. Real and imaginary parts of experimentally reconstructed density matrix (b) at HWP angle $\theta_H^P = 0$ (c) at HWP angle $\theta_H^P = 22.5$ (d) at combined HWP angles $\theta_H^P = 22.5$ & $\theta_H^B = -67.5$.

BS-based BBM92 QKD, Alice and Bob further probabilistically split the incoming photon at their end using 50:50 beam-splitters, consider photon pairs from the BS transmission port for encoding in H/V, and photon pairs from the BS reflection port for D/A basis encoding. Bob uses an additional B-QHQ system for geometric or geometric equivalent phase compensation. After encoding the photons into two non-orthogonal bases, Alice and Bob each employ four detectors to collect the photons with different polarizations. At Bob's station, detectors SPCM1–SPCM4 are assigned to measure the H, V, D, and A polarizations, respectively, with their detection events time-stamped using Bob's Time-to-Digital Converter (TDC). Similarly, on Alice's side, detectors SPCM5–SPCM8 perform the same role, registering photons in the H, V, D, and A polarizations, with the corresponding timestamps recorded through Alice's TDC.

In order to study how the geometric phase affects the QBER, we rotate the half-

waveplate in the pump-QHQ system. Additionally, a linear translation stage is used to control the crystal position starting from the exact zero reference position to some non-zero value. The geometric phase equivalent effect with different crystal positions is done using the linear manual stage. Using the GP in the pump beam or changing the crystal position inside the Sagnac loop, an arbitrary entangled state other than the standard Bell state can be prepared, which can be compensated at the receiver end (here Bob) using another QHQ system shown as GP Comp in the experimental setup 7.1, and maximally entangled Bell states between Alice and Bob can be revived for quantum key distribution.

7.4 Results and discussions

We begin by examining how the pump geometric phase influences the QBER, for which we rotated the $\lambda/2$ plate in the pump-QHQ system from -10° to 100° at a fixed pump power of 5 mW across the crystal, and for each set angle we calculated the QBER shown in Fig. 7.2. The experimentally obtained QBER values follow a functional form $\text{QBER} = a + b |\cos(4\theta_H^p)|$ where $a = 29$ and $b = -25$ from the fit function, which is also predicted to be 25 & -25 earlier in the theory section in Eq. 7.4. It is observed that at $\theta_H^p = 0^\circ$ & 90° we get a minimum QBER of 2.63% and 2.76% for state $\frac{1}{\sqrt{2}}(|H_A H_B\rangle - |V_A V_B\rangle)$. Also, we get a minimum QBER value for the $\frac{1}{\sqrt{2}}(|H_A H_B\rangle + |V_A V_B\rangle)$ state at the HWP angle of 45° . In between the minimum values, QBER values increase with rotating the HWP angle and reach maximum QBER values of 27.7% and 28.2% for $\theta_H^p = 22.5^\circ$ & 67.5° where the states are $\frac{1}{\sqrt{2}}(|H_A H_B\rangle \mp i|V_A V_B\rangle)$ respectively, as these QBER value is higher than the maximum threshold limit of 11% for secure key distribution we cannot use this Bell like state for QKD protocol. These five minima and maxima positions of the QBER For angles $\theta_H^p = 0^\circ, 22.5^\circ, 45^\circ, 67.5^\circ$, & 90° are shown in the figure with numbering 1,

2, 3, 4 & 5 respectively within the black color shapes. The respective state for these five positions was also reconstructed using quantum state tomography (QST), and the fidelity values obtained for the respective states are 98%, 98%, 98%, 97%, and 98%, as shown in the upper panel of Fig. 7.3.

Now, the geometric phase effect, introduced in the generated entangled photon pair because of the pump beam geometric phase, can be compensated at the receiver end using another compensating QHQ system. It is observed experimentally that if the pump beam faces a geometric phase of ϕ in the P-QHQ system, then at the receiver end, to compensate for this phase effect, we need to set $-(180^\circ - \phi)$ of geometric phase in the B-QHQ system. With this compensation at the receiver end, we obtained always lower QBER, almost constant over the entire range, and generates Bell state $\frac{1}{\sqrt{2}}(|H_A H_B\rangle + |V_A V_B\rangle)$ regardless of the pump geometric phase, which we verified using QST after geometric phase compensation using the second B-QHQ system. The initial five points compensated to the final points 1^C , 2^C , 3^C , 4^C , and 5^C after compensation. The fidelity values obtained after compensating the states at these points are 98%, 97%, 98%, 96%, and 98%. This indicates that the geometric phase induced by the pump can be erased from the Bell-like state, resulting in the revival of the Bell state at the receiver end for entanglement-based QKD applications.

Next, instead of rotating the $\lambda/2$ in the P-QHQ system, we change the crystal from the exact 0 position to 2 mm, and we observed a similar effect of changing the geometric phase from 0° to 180° . For crystal position at $Pos = 0$ mm & 2 mm we get a minimum QBER of 3.45% and 3.08% for state $\frac{1}{\sqrt{2}}(|H_A H_B\rangle - |V_A V_B\rangle)$ shown in Fig. 7.3.

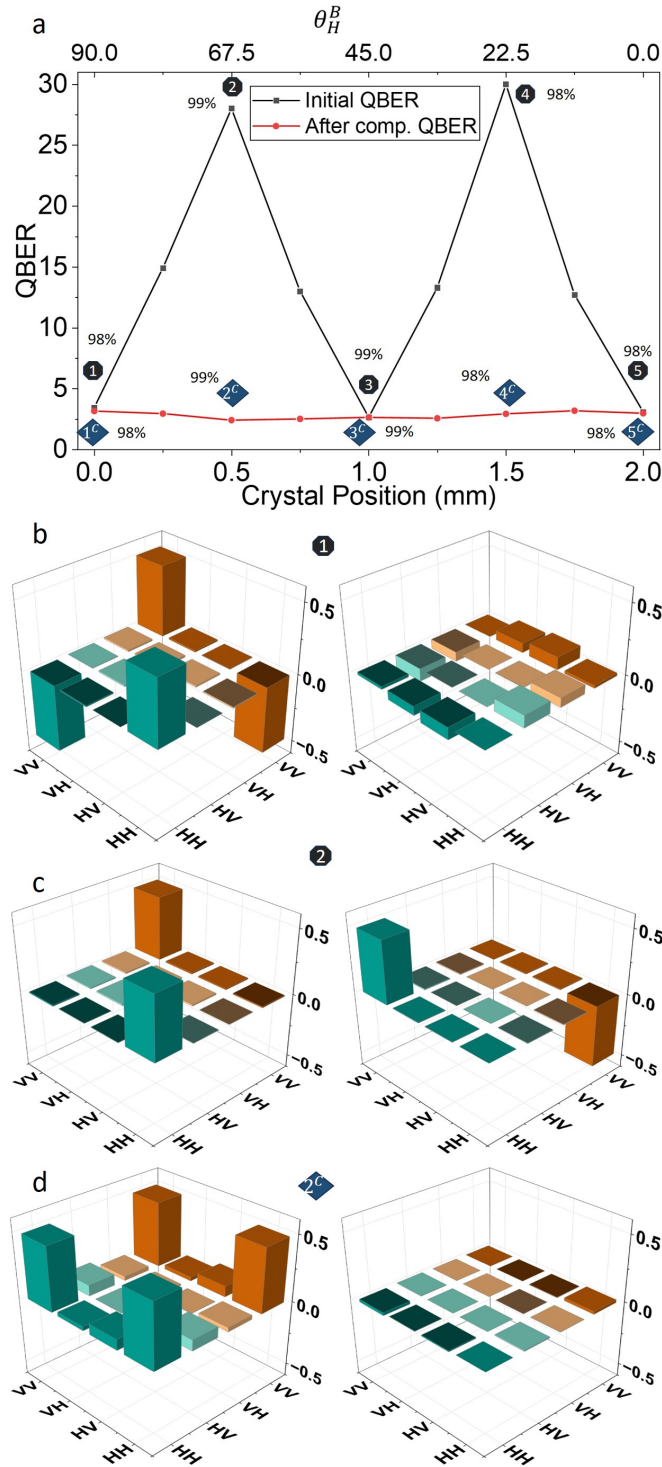


Figure 7.3: (a) Dependence of the QBER on the crystal position within the Sagnac loop. Real and imaginary parts of experimentally reconstructed density matrix (b) at crystal position = 0 mm (C) at crystal position = 0.5 mm, and (d) at crystal position = 0.5 mm and $\theta_H^B = -67.5^\circ$.

Also, we get a minimum QBER value of 2.64% for the $\frac{1}{\sqrt{2}}(|H_A H_B\rangle + |V_A V_B\rangle)$ state at crystal position at $Pos = 1$ mm. Between the minimum value, QBER values increase with other position and reach maximum QBER values of 28.1% and 28.7% for $Pos = 0.5$ mm & 1.5 mm, where the states are $\frac{1}{\sqrt{2}}(|H_A H_B\rangle \mp i |V_A V_B\rangle)$. This geometric equivalent phase, because of the different crystal position, can also be compensated in a similar manner as discussed in the earlier section.

Five crystal positions starting from $Pos = 0.0$ mm, to $Pos = 2.0$ mm with a position increment of 0.5 mm, i.e., points 1, 2, 3, 4 & 5 in Fig. 7.3 exactly replicate the points respectively 1, 2, 3, 4 & 5 in Fig. 7.2. The respective fidelities calculated using QST are 98%, 99%, 99%, 98%, and 98%. And it is experimentally verified that by setting the same angles in $\lambda/2$ in the B-QHQ, i.e., $\theta_{HP}^B = 0^\circ, -22.5^\circ, -45^\circ, -67.5^\circ, \& -90^\circ$ like the earlier geometric phase case, the geometric equivalent phase because of non-exact crystal positioning can be compensated at receiver end for reviving the standard Bell state $\frac{1}{\sqrt{2}}(|H_A H_B\rangle + |V_A V_B\rangle)$ from any Bell like state with arbitrary phase. The points 1^C , 2^C , 3^C , 4^C , and 5^C in Fig. 7.3 are states after phase compensation with fidelity respectively 98%, 99%, 99%, 98%, and 98%.

7.5 Conclusions

In this work, we have demonstrated that the phase introduced in polarization-entangled photon pairs, either because of the GP in the pump beam or due to the non-perfect generation and transmission from the crystal, can significantly affect the shared standard Bell state and the performance of entanglement-based quantum key distribution protocols. Our experiments confirm that the geometric phase of the pump beam manifests as a controlled but detrimental phase shift in the Bell state, leading to increased quantum bit error rates that can exceed the security threshold for QKD. Im-

portantly, we have shown that a simple compensation strategy employing an additional QHQ waveplate configuration at the receiver end effectively cancels the imparted geometric phase. This compensation restores the high-fidelity Bell state, reduces the QBER below 11%, and re-enables secure key generation.

These results highlight the practical importance of controlling geometric phase effects in real-world quantum communication systems, especially in scenarios involving long-distance free-space transmission or static phase fluctuations. The demonstrated method offers a straightforward approach to entanglement restoration at the receiver end, compatible with scalable two-party QKD architectures. Traditional phase compensation methods applied at the photon source—such as inserting additional birefringent crystals of carefully chosen lengths or chosen design, maintaining interferometric stability, or using spatial light modulators—can be difficult to implement in practical, real-world systems. In this work, we present a straightforward active phase-compensation approach that can be applied at either the source or the receiving end to remove unwanted phase drift in Bell states. Both theoretical analysis and experimental measurements are used to evaluate how the QBER in the BBM92 protocol varies with the relative phase. Furthermore, we show that geometric-phase-assisted phase-compensation enables QKD. The next question arises: can we extend beyond the two-party and establish a multi-party architecture, i.e., the quantum network? That is the next chapter of this discussion.

Chapter 8

Multi-User Quantum Communication Network

Emergent quantum networks are the essential ingredient for securely connecting multiple users worldwide, extensively deployed in both fibre and free-space. An essential element is the multiplexing of entanglement to multiple users, overcoming the peer-to-peer restriction of quantum key distribution (QKD), so far successfully shown in fibre-based architectures. Here, we demonstrate a free-space quantum space division multiplexing architecture using just one entanglement source to realise a fully connected twelve-channel quantum network for seamless QKD connections between six users. The network achieves record coincidence rates exceeding $3 \times 10^4 \text{ s}^{-1}$ between any pair of nodes on the network, for secure key rate of over 400 kbps. Our approach overcomes the active switching hurdle that has hindered the free-space deployment of quantum multiplexing, is fully passive, easily scalable to more nodes and compatible with fibre-based integration, thus opening a new path to scalable and resource-efficient quantum networks that utilise free-space links.

8.1 Introduction

Quantum key distribution (QKD), offering unconditional security based on the principles of quantum mechanics, has evolved as the mature and practical application of quantum information science [34]. Over the past two decades, it has successfully transitioned from theoretical proposals [67, 164] to field-deployable systems, especially between two users, with demonstrations in lab setup [219, 220], over fiber-optic networks [221–223], free-space links [217, 224, 225], and long distance satellite-based channels [226–228] with the aim to provide secure key sharing for critical sectors such as defense, finance, and government communications. However, realizing the full potential of QKD and enabling its simultaneous connectivity among a large number of users worldwide necessitates the development of global quantum communication networks [229] analogous to the current classical communication infrastructure.

Recent advances have led to the demonstration of several types of quantum network architectures based on trusted node, quantum repeater, higher dimension entangled state, beam splitters, and spatial and frequency multiplexing [230–241] using different degrees of freedom, including polarization, frequency, and time. However, each architecture offers unique advantages and faces inherent limitations. For instance, while quantum memory-based networks [232–234] hold promise for universal applicability across network architectures, their practical realization remains challenging due to the stringent requirements of high-fidelity and long-coherence-time quantum memories [242]. Conversely, one-to-many user networks represent a simpler implementation but suffer from reduced bit rates and limited continuous connectivity owing to the use of multiple beam splitters or optical switching [237, 238]. Trusted-node and high-dimensional entanglement-based networks, although conceptually powerful, are resource-intensive, posing constraints on scalability and widespread deployment

[235, 236].

In contrast, wavelength-division multiplexing (WDM), a mature and widely used technique in classical networks [243], has been extended to quantum sources at 1550 nm [239, 240, 244]. Nevertheless, increasing the number of users in a quantum network by adding more frequency channels is fundamentally constrained by the limited photon flux or bit rate. Unlike classical communication systems, where bit rate can be enhanced by simply increasing the optical power, such an approach in quantum networks can violate the fundamental operating requirements of quantum light sources. Furthermore, channel dispersion and hardware-induced crosstalk must be compensated to preserve entanglement fidelity over long distances.

Recently, space-division multiplexing (SDM) [245, 246], utilizing few-mode, multi-mode, and multi-core fiber architectures, has emerged as a complementary strategy to WDM in classical communication systems. These techniques harness the spatial degrees-of-freedom of light to significantly enhance channel capacity and are now being adapted for quantum communication [238, 240, 241]. Initial demonstrations of SDM-based quantum networks [241, 247], as well as hybrid architectures combining WDM with beam-splitter-based SDM [238, 240] using fiber channels at 1550 nm, have shown considerable promise as a scalable pathway toward high-capacity quantum networks. In a fiber-based WDM quantum network connecting N users via a complete graph, $N(N - 1)/2$ unique QKD links are required. This setup demands $N(N - 1)/2$ distinct wavelength pairs from a single entangled photon source [239]. A more resource-efficient architecture combining WDM and passive beam splitters has been proposed, reducing the requirement to only N wavelength pairs while maintaining a fully connected N -user network [240]. Most notably, the integration of both WDM and SDM has enabled a 40-user fully connected network comprising 780 QKD links

[238]. The progress in fiber-based multi-user quantum networks has so far yielded relatively modest performance in terms of bit rate. Reported total coincidence rates are as low as 0.3 kbps in a laboratory setup using six sources with APD detection [239], with only a slight improvement to 0.56 kbps achieved over a 10 m fiber link using fifteen sources and SNSPD detection [244]. Subsequent work reported a secure key rate of 4.1 kbps for a network formed with eight sources over channel lengths ranging from 10 m to 16 km using SNSPD detection [240]. More recently, the secure key rate increased to 21 kbps for a network employing fifteen sources over 1–2 km patch-cord fiber links with SNSPD detection [238]. As yet, the extension to free-space multiplexed links has remained largely unexplored due to the stringent resource requirements and the intrinsic challenges, such as beam divergence, pointing and tracking errors, and channel crosstalk, with satellite-based free-space QKD links remaining peer-to-peer. Therefore, it is essential to explore multi-user networks for free-space links to establish a global quantum network while increasing the per-user bit rates for practical applications. Here, we present a novel spatial-sectioning and beam-splitter-based multiplexing architecture that enables a fully connected, free-space multi-user quantum communication network with a total sifted key rate of 407 kbps and a secure key rate of 76 kbps across all user pairs. For any even number of users ($N > 3$), the scheme requires only $N/2$ entangled-photon sources yet supports $(N(N-2)/2)$ unique user pairs, offering a highly scalable platform for multi-user entanglement distribution. By harnessing the intrinsic spatial and temporal correlations and quantum randomness [150, 190] of the spontaneous parametric down-conversion (SPDC) process, we section the annular emission ring of an entangled-photon source and multiplex the sections with passive optical elements. In a proof-of-concept demonstration, we establish a 12-channel QKD network among $N = 6$ users, realized with only $N/2 = 3$ spatially sectioned entangled-photon sources derived from a single source. We achieved

high performance across all user pairs, with coincidence count rates exceeding 30 kHz, entanglement visibility above 80%, and average quantum state fidelity of 90%. The proposed architecture is inherently scalable, as the number of entangled photon sources can be increased without compromising performance metrics. This is accomplished by simultaneously raising the pump laser power and exploiting the enlarged annular ring profile from a single SPDC source. Additionally, the integration of WDM and/or one-to-many beam splitters enables a significant expansion in the number of connected users without necessitating additional entangled photon sources or the use of central trusted nodes. The demonstrated architecture offers a practical route toward high-rate, globally deployable quantum communication networks, particularly suited for satellite-based free-space links.

8.2 Experiment

The experimental configuration is illustrated schematically in Fig. 8.1, is divided into five sections: entangled photon source, spatial division and multiplexing, communication channel, projection and detection, and users. The entangled photon source is based on the type-0, quasi-phase-matched, degenerate, non-collinear spontaneous parametric down-conversion (SPDC) process, producing an annular ring intensity distribution where temporally and spatially correlated photon pairs at 810 nm lie at diametrically opposite points. The resulting quantum state is the Bell state, $|\phi^-\rangle = (|HH\rangle - |VV\rangle)/\sqrt{2}$. To generate multiple entangled-photon sources from a single SPDC emission ring, we segmented the ring into six spatial sections using a prism mirror (PM) and D-shaped mirrors (DM). This configuration yielded three pairs of diametrically opposed sections, each carrying correlated pair photons at random. The spatially separated sources corresponding to these diametric pairs are illustrated within Fig. 8.1 physical representation graph. The sections are then multiplexed using beam

splitters and distributed through a one-meter free-space communication channel to different users in the lab. The assignment of the sections among different users is listed in user allocation table in Fig. 8.1.

Each of the six users (Alice (A), Bob (B), Charlie (C), Dave (D), Evan (E), and Feng (F)) is equipped with a polarization projection system (waveplates and a polarizing beam splitter), a single-photon counting module, and a time-to-digital converter for detection and analysis. Alice & Bob (AB), Charlie & Dave (CD), and Evan & Feng (EF) are connected through the two outputs of the same beam splitter and, hence, do not have direct communication links between themselves. Nevertheless, each user is directly connected to four others, forming a twelve-channel current quantum network, as depicted in Fig. 8.1 quantum correlation graph. For future quantum networks, the source and multiplexing system integrated with a dedicated telescope for each channel could be deployed on a drone or satellite to enable long-distance free-space QKD links. For further details, refer to the Materials and Methods section.

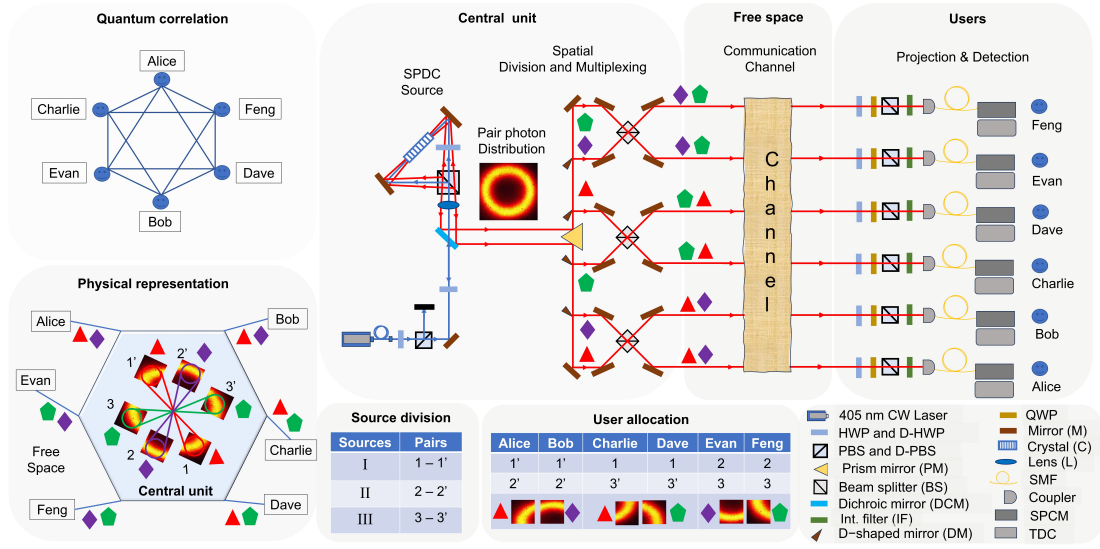


Figure 8.1: Conceptual scheme and experimental setup of the multi-user quantum network architecture. On the left, we have illustrated the concept of using two layers of abstraction. The top layer shows the fully connected mesh of 12 channels connecting six users through quantum correlation. The bottom layer shows the physical representation of the network topology, with the implementation shown on the right. The topology of the quantum network is established through the central unit, which derives three entangled photon sources from a single source and distributes them between six users through multiplexing. The complete end-to-end implementation has three sections: central unit, free space channel, and users. Again, the central unit has two subsections: SPDC source and spatial division and multiplexing. The SPDC source is realized using a single-frequency continuous-wave diode laser at 405 nm, with output power controlled via a half-wave plate (HWP) and a polarization beam splitter (PBS), which pumps a temperature-stabilized periodically poled KTP (PPKTP) crystal placed in a polarization Sagnac interferometer. The interferometer consists of a dual-wavelength PBS and HWP (D-HWP) for 810 nm and 405 nm wavelengths. A plano-convex lens (focal length 150 mm) focuses the pump at the crystal center and collimates the photon pairs generated via spontaneous parametric down-conversion (SPDC). In the spatial division multiplexing section, the collimated SPDC emission ring, separated from the pump by a dichroic mirror (DCM), is divided into two halves using a prism mirror (PM), with each half further segmented into three subsections by D-shaped mirrors (DMs). Six diametrically opposite sections form three entangled photon sources, I, II, and III, with section pairs (1, 1'), (2, 2'), and (3, 3') as shown in the source division table. These subsections are multiplexed using three 50:50 beam splitters (BS), while mirrors (M) in the experiment direct the beams through the optical paths. The multiplexed outputs are transmitted via the communication channel to six users. Each user's receiver consists of a projection and detection module comprising an HWP, quarter-wave plate (QWP), PBS, an interference filter (IF; bandwidth of 3 nm, centered at 810 nm), a fibre coupler, and a single-mode fibre (SMF) connected to a single-photon counting module (SPCM). The SPCM outputs are processed by a time-to-digital converter (TDC) and a computer. The user allocation table lists the allocated subsections for each user. The quantum correlation graph illustrates the realized quantum links within the network, which can be extrapolated to form a potential global quantum network based on satellite technology.

8.3 Results and discussions

We first characterized the entangled photon sources, with the results summarized in Fig. 8.2. By pumping the nonlinear crystal with 1 mW of power, we tuned the phase-matching temperature to 39.5°C to increase the SPDC ring diameter, thereby facilitating easier spatial sectioning. While a larger ring diameter by lowering the crystal temperature away from the degenerate phase-matching temperature enables finer division of the annular emission ring and increases the number of entangled photon sources derivable from a single setup, it also spreads the photon pairs over a larger area, reducing the collected photon flux and thus lowering the achievable bit rate. However, an increase in pump power can mitigate the issue of the lower bit rate. The measured coincidence counts (without polarization projection) between different subsections, as shown in Fig. 8.2(a), confirm strong correlations between diametrically opposite sections, with a coincidence rate of $0.15 \times 10^6 \text{ s}^{-1}$, and negligible ($6 \times 10^3 \text{ s}^{-1}$) or no coincidences between non-opposite sections. The single-photon detection rates (Fig. 8.2(b)) from six spatial subsections vary between 1.3×10^6 and $2.0 \times 10^6 \text{ s}^{-1}$, corresponding to coupling efficiencies above 10%. The variation in single counts among the subsections may be attributed to imperfect spatial sectioning of the SPDC ring, likely caused by mechanical constraints in the experimental setup. Although this variation does not affect the present study, it could be minimized across all sections by employing an advanced spatial sectioning approach using a microlens array coupled to fiber bundles.

The polarization correlation visibility (for example between subsections 2 and 2' shown as violet color diamonds) across all bases for the diametrically opposite sections exceeds 93%, as illustrated in Fig. 8.2(c), which shows the polarization-dependent coincidence counts for one representative entangled photon pair in the horizontal (H),

vertical (V), diagonal (D), and anti-diagonal (A) bases. The measured Bell parameter is $S = 2.63$, clearly violating the classical limit of 2. We observe similar performance parameters while considering the pair subsections, 1 & 1', and 3 & 3'. Further, quantum state tomography performed by reconstructing both the real (Fig. 8.2(d)) and imaginary (Fig. 8.2(e)) components of the two-photon density matrix confirms that the generated state corresponds to the maximally entangled Bell state $|\phi^-\rangle = (|HH\rangle - |VV\rangle)/\sqrt{2}$, with a state fidelity of 98%. These observations collectively confirm the reliable and high-quality generation of three independent entangled photon sources derived from a single experimental resource. Using the difference in the number of reflections (even or odd) in the two arms of a single source, we characterized the quantum state as $|\phi^-\rangle$ and $|\phi^+\rangle$, with the same entangled parameters, as expected.

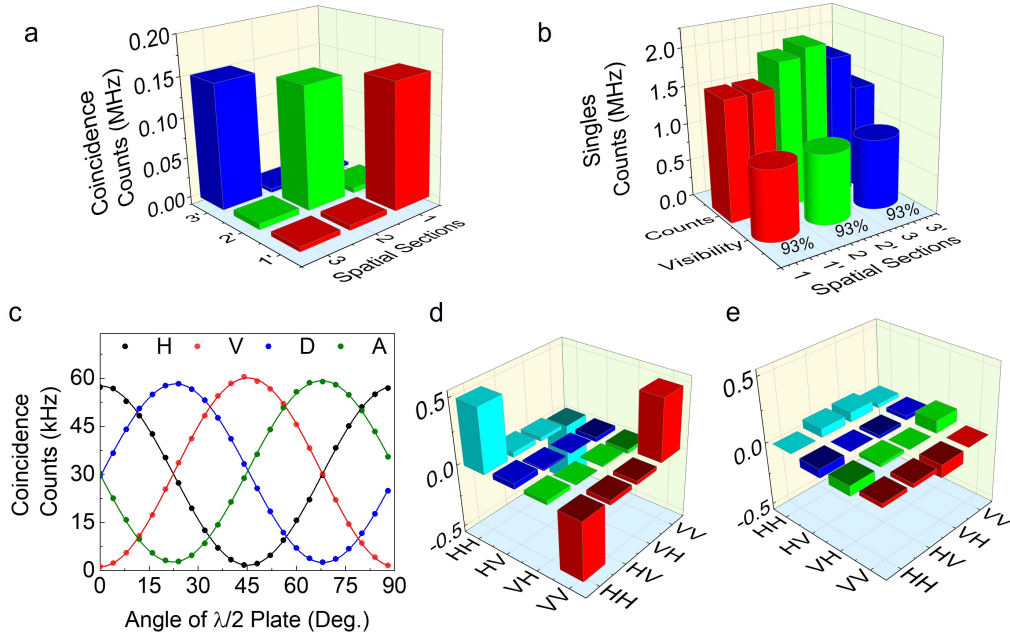


Figure 8.2: Characterization of spatially separated entangled photon sources derived from a single SPDC source. (a) Coincidence counts between different subsections, showing strong correlations between diametrically opposite sections carrying pair photons generated via the SPDC process. (b) Singles counts of different subsections, along with the coincidence visibility between diametrically opposite sections, 1 & 1', 2 & 2', and 3 & 3'. (c) Quantum interference of the spatially separated entangled photon sources (here, we used source II comprises of subsections 2 & 2') measured in the horizontal (H, black dots), vertical (V, red dots), diagonal (D, blue dots), and anti-diagonal (A, green dots) polarization bases. (d,e) Graphical representation of the absolute values of the real (d) and imaginary (e) parts of the reconstructed density matrix of the polarization-entangled Bell state $|\phi^-\rangle$.

Having characterized the performance of the three spatially separated entangled photon sources derived from a single setup, we investigated the properties of a quantum network established through their multiplexing using 50:50 beamsplitters. The results are presented in Fig. 8.3. As shown in Fig. 8.3(a), each user shares strong correlations with four others, with coincidence rates ranging from $0.2 \times 10^5 \text{ s}^{-1}$ to $0.4 \times 10^5 \text{ s}^{-1}$, confirming the formation of a twelve-channel quantum network among six users. The observed variation in coincidence counts among users may be attributed

to imperfect spatial sectioning using the available components in the lab. and collection of the SPDC ring, implemented to accommodate mechanical constraints of the experimental setup, as well as deviations of the beam splitters from ideal 50:50 splitting ratios. On the other hand, the users connected via the same output port of a beam splitter such as Alice & Bob, Charlie & Dave, and Evan & Feng exhibit only minimal coincidence counts ($1.1 \times 10^3 \text{ s}^{-1}$ to $1.4 \times 10^3 \text{ s}^{-1}$), attributed to background noise, indicating no direct communication link between them. To further assess channel integrity, we introduced digital delays up to 20 ns between pair photons across different user combinations. The resulting coincidence counts remained within a similar noise-limited range, stemming from dark counts, accidental events, and optical imperfections in the system. It is to be noted that all the results presented in this article are based on raw, unprocessed data. While standard correction techniques accounting for detector inefficiencies and background subtraction can improve apparent performance, they may obscure the true practicality of the scheme. To retain relevance for real-world applications, no such corrections were applied in this analysis.

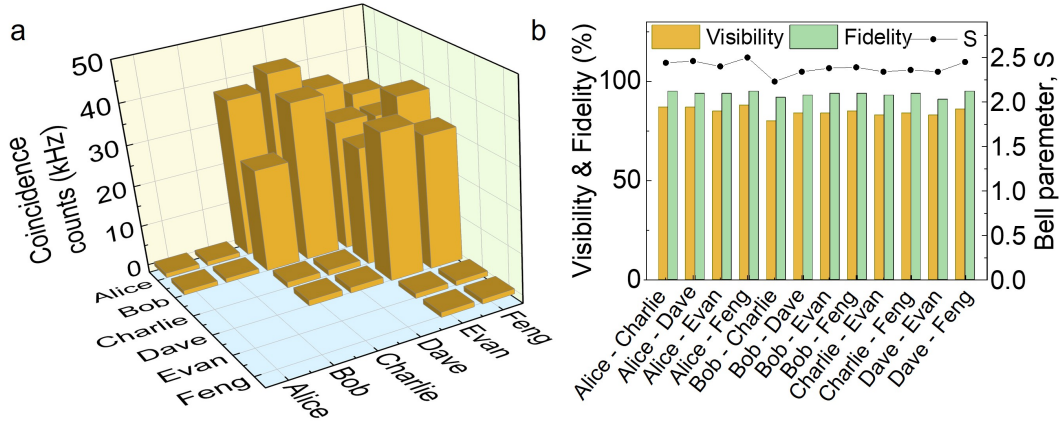


Figure 8.3: Performance characteristics of quantum links within the network. (a) Coincidence counts for each link connecting two users in the 12-link quantum network. (b) Measured quantum parameters for each link, including entanglement visibility, Bell parameter (S), and quantum state fidelity. The network supports both $|\phi^+\rangle$ and $|\phi^-\rangle$ Bell states, with each state distributed across six of the twelve links owing to the network's topology.

Furthermore, we measured the entanglement visibility, Bell parameter, and quantum state fidelity for each link Alice-Charlie (AC), Alice-Dave (AD), Alice-Evan (AE), Alice-Feng (AF), Bob-Charlie (BC), Bob-Dave (BD), Bob-Evan (BE), Bob-Feng (BF), Charlie-Evan (CE), Charlie-Feng (CF), Dave-Evan (DE), and Dave-Feng (DF), connecting any two users in the network (see Fig. 8.1). As shown by the golden bars in Fig. 8.3(b), the interference visibility, averaged over all polarization bases for each user pair in the network, ranges from 80% to 88%. This is slightly lower than the visibility observed from the individual sources, primarily due to imperfections introduced by additional optical elements, including the beam splitter in the network. Nevertheless, the measured visibilities remain well above the 71% threshold required to confirm entanglement [92], thereby verifying entanglement across all users in the network.

We also performed quantum state tomography shared between two user pairs in

the network and found that due to the use of different numbers of reflections in the network paths the links, AC, AF, BC, BF, CE, and DE and AD, AE, BD, BE, CF, and DF connect two used through $|\phi^+\rangle$ and $|\phi^-\rangle$, respectively. The measured fidelity of the shared quantum states varies in the range from 91% to 95% (see green bars in Fig. 8.3(b)). The corresponding Bell parameters S also exceeded the classical limit of $S = 2$, varying in the range of $S = 2.2 - 2.5$, thus confirming the presence of quantum correlations. Using the coincidence counts between each pair of users connected through the twelve-channel network in the HV and DA bases, and applying binary Shannon entropy, we estimated the secure key rate between every pair (see Eq. 8.1 in the Methods section), yielding a total secure key rate of 76 kbps across the network. Similarly, the total sifted key rate, calculated from the coincidence counts in the HV and DA bases, is found to be 407 kbps. These numbers will be high for the detection using SNSPD detectors with quantum efficiency $>95\%$. As explained previously, the use of standard corrections will improve the values of the parameters close to ideal. However, these results demonstrate the successful realization of a twelve-channel entanglement-based quantum network, enabling simultaneous quantum key distribution among six users at high bit rates. With improved collection strategies, use of SNSPD detectors, and an increased number of spatial sections while considering a larger diameter SPDC ring generated at high pump power, this spatial-division multiplexing technique holds promise for scaling up multi-user quantum communication networks beyond what is currently feasible using WDM schemes.

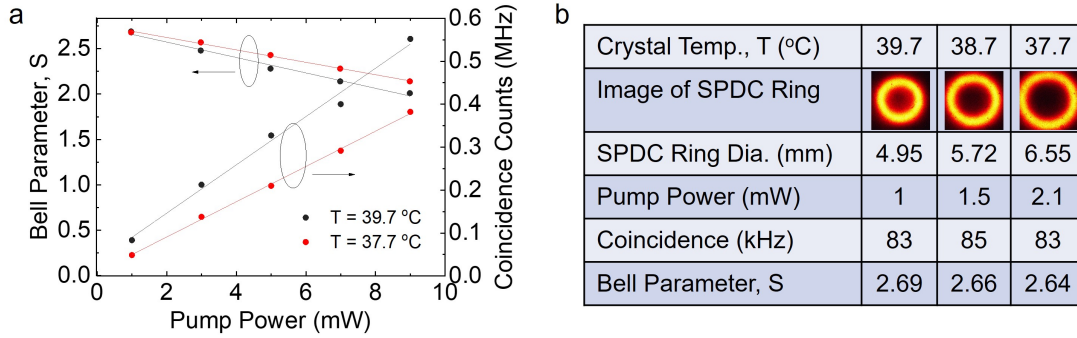


Figure 8.4: Performance parameters of the entangled-photon source for scalable quantum networking. (a) Variation of the Bell parameter S and coincidence counts as a function of pump power for two spontaneous parametric down-conversion (SPDC) emission-ring diameters, corresponding to crystal temperatures of $T = 37.7^\circ\text{C}$ and $T = 39.7^\circ\text{C}$. (b) Tabulated SPDC source characteristics at the two crystal temperatures, showing that an increased emission-ring diameter allows finer spatial sectioning. This capability supports network-topology scaling to accommodate more users while preserving the entanglement quality of the source.

To assess the scalability of our approach, we performed a separate experiment evaluating the performance of the entangled photon source in terms of the Bell parameter S and coincidence counts as a function of pump power at two phase-matching temperatures, T . The results are shown in Fig. 8.4. As evident from Fig. 8.4(a), at $T = 39.7^\circ\text{C}$, the rate of decrease in S with pump power is measured to be 0.085 mW^{-1} , while the coincidence count rate increased at 0.056 MHz/mW . Reducing the crystal temperature to $T = 37.7^\circ\text{C}$, away from the degenerate, collinear phase-matching condition, enlarged the SPDC emission ring, decreasing the coincidence count slope to 0.041 MHz/mW and hence the attainable bit rate. However, the smaller degradation rate of $S = 0.068 \text{ mW}^{-1}$ suggests that higher pump powers can be employed to recover the bit rate without compromising quantum correlations. This behaviour can be attributed to the reduced photon density across the enlarged ring [92], which, in addition to lowering the bit rate, lowers the probability of multi-pair generation at the same spatial location, a primary source of correlation degradation. Consequently, the source

preserves comparable quantum performance and bit rate even at elevated pump powers, demonstrating robustness to variations in ring size. To further quantify this, we have tabulated key performance parameters between two users for different ring sizes. As shown in Fig. 8.4(b), lowering the crystal temperature from 39.7°C to 37.7°C increases the annular ring diameter from 4.95 mm to 6.55 mm, while still achieving comparable coincidence rates (~ 83 kHz) and Bell parameters ($S > 2.6$) with increased pump power (from 1 mW to 2.1 mW). These results clearly demonstrate the scalability of our entangled photon source for quantum networks with a larger number of users. Again, given the higher bit rate achieved in the network, each user can be considered as a node, enabling the expansion of the network by employing the WDM schemes [239, 240] or a one-to-multi-port beam splitter [248] to connect additional users to the network. This approach facilitates the realization of a large-scale quantum network.

8.4 Materials and Methods

8.4.1 Polarization entangled photon source

The schematic of the experimental setup is shown in Fig. 8.1. We used a continuous-wave, single-frequency diode laser that delivers an output power of 21 mW at a central wavelength of 405 nm with an approximate linewidth of 20 MHz as the pump source for the experiment. To improve the spatial mode quality of the laser, we couple its output into a single-mode fiber (SMF) and subsequently collimate it using a fiber collimator. The laser power to the experiment is controlled using a combination of a half-wave plate (HWP) and a polarizing beam splitter (PBS) cube. Another HWP is used to rotate the horizontal polarized pump beam to a diagonal polarization state, ensuring equal power distribution between the two output ports of a dual-wavelength PBS (D-PBS), and hence equal power to the clockwise (CW) and counterclockwise

(CCW) propagating pump beams inside a polarization Sagnac interferometer. The Sagnac interferometer is comprised of D-PBS, optimized for both 405 nm and 810 nm, and two plane mirrors (M). A lens (L) of focal length $f = 150$ mm focuses the pump beam from both directions to a spot diameter of $\sim 40 \mu\text{m}$ at the center of the nonlinear crystal, which is symmetrically placed between two mirrors, M, relative to the D-PBS. A 20 mm-long periodically poled potassium titanyl phosphate (PPKTP) crystal with a grating period $\Lambda = 3.425 \mu\text{m}$ and an aperture of $1 \times 2 \text{ mm}^2$ is used to generate non-collinear, degenerate, type-0 ($e \rightarrow e + e$), quasi-phase-matched pair photons at 810 nm through the spontaneous parametric down-conversion (SPDC) process. The crystal is housed in a temperature-controlled oven, which can be varied up to 200°C with a stability of $\pm 0.1^\circ\text{C}$ to maintain optimal phase matching.

A dual-wavelength half-wave plate (D-HWP), optimized for 405 nm and 810 nm and oriented at 45° to the vertical axis, is placed inside the Sagnac interferometer to transform the horizontal polarization into vertical and vice versa. As described in Refs.[92, 124], the SPDC photons generated from the CW and CCW beams exhibit annular ring distributions, with pair photons lying diametrically opposite points on the ring, are recombined at the D-PBS and collimated using lens L. The dichroic mirror (DCM), placed between lens L and the HWP, separates the SPDC photons from the pump. The resulting entangled quantum state of the pair photons is given by $|\phi^\pm\rangle = (|HH\rangle - |VV\rangle)/\sqrt{2}$, representing a Bell state. The SPDC ring is captured using an electron-multiplying charge-coupled device (EMCCD) camera (Andor iXon Ultra 897) with an interference filter centered at 810 nm and a bandwidth of approximately ~ 3.2 nm, as shown in the inset of Fig. 8.1.

8.4.2 Spatial division and multiplexing

Since entangled photon pairs lie on diametrically opposite points of the SPDC ring, we segmented the ring to create three independent entangled photon sources. First, we used a gold-coated prism mirror (PM) to divide the annular SPDC ring into two equal halves. We then further subdivided each half into three angular sections using four D-shaped mirrors (DM), creating two sets of spatial segments, (1, 2, 3) and (1', 2', 3'). These segments are arranged (see Fig. 8.1 physical representation graph such that each pair of diametrically opposite sections, (1, 1'), (2, 2'), and (3, 3') contains correlated pair photons forming three spatial separated entangled photon sources, I, II, and III, respectively, from a single set of resources: the pump laser, the nonlinear crystal, and the Sagnac interferometer.

We further multiplexed the six subsections of the three entangled photon sources and assigned communication channels using three nearly 50:50 beam splitters (BS), as illustrated in Fig. 8.1 experimental setup. Subsections 1 and 2, originating from entangled photon sources I and II, respectively, are combined through two input ports of a beam splitter, and the two output ports are routed to users Alice (A) and Bob (B). As a result, photons reaching Alice and Bob originate from sources I and II with equal probability. However, due to the probabilistic nature of beam splitter outputs, Alice and Bob do not receive photon pairs simultaneously, and therefore, no direct quantum communication is possible between them.

Similarly, subsections (3, 1') from entangled photon sources III and I, and (2', 3') from sources II and III, are each merged at beam splitters, with their outputs directed to users Charlie (C), Dave (D), and Evan (E), Feng (F), respectively. Like Alice and Bob, these user pairs (Charlie, Dave) and (Evan, Feng) are connected by the same beam

splitter, and hence cannot perform quantum communication between themselves.

However, this multiplexed configuration enables each of the six users to share entanglement-based communication with four other users via three distinct entangled photon sources, forming a twelve-channel quantum network, as shown in Fig. 8.1 quantum correlation graph. The channels are labeled using the initials of the communicating parties, for example, the channel between Alice and Charlie is denoted as “AC”. The complete set of channels in the network includes: “AC”, “AD”, “AE”, “AF”, “BC”, “BD”, “BE”, “BF”, “CE”, “CF”, “DE”, and “DF”.

8.4.3 Projection and detection for each user

All six quantum channels guided using mirrors, M in the experiment, are equidistant (although this is not a necessary condition) in free space from the BS to the user. To measure the entanglement among the parties, each user has a polarization projection system comprised of either HWP, PBS, or HWP, QWP, and PBS, and the detection systems comprised of an interference filter (bandwidth ~ 3.2 nm), mounted fiber coupler, single-mode fiber (SMF), and single-photon counting modules, SPCMs (SPCM-AQRH-14-FC). All SPCMs are connected to a single time-to-digital converter (TDC) (Swabian, Time Tagger Ultra) and a computer, for photon counting, time stamping, recording, and experimental data analysis.

8.4.4 Estimation of secure key rate

the achievable secure key generation rate between any pair of users within the network can be estimated based on the formula presented in Ref. [241]

$$R_{SK} = \frac{1}{2}C_{DA} \left[1 - (1+m)H\left(\frac{1-V_{DA}}{2}\right) \right] + \frac{1}{2}C_{HV} \left[1 - (1+m)H\left(\frac{1-V_{HV}}{2}\right) \right] \quad (8.1)$$

Here, C_{HV} and C_{DA} are the total numbers of coincidence counts in the DA and HV bases, H is the binary Shannon entropy, and we used a bidirectional error correction of $m = 1.1$ [241].

8.4.5 Scaling of the network

The presented network architecture is highly scalable, allowing users to be added or removed without altering the core design. In contrast, prior networks based on wavelength division multiplexing (WDM) require additional narrow-bandpass filters symmetric to the degenerate wavelength of the entangled photon source, defined by ITU frequency channels. However, such approaches reduce the bit rate between users and increase crosstalk. Moreover, scaling the WDM-based network by increasing the spectral bandwidth of the entangled photon source demands a shorter nonlinear crystal length, which decreases the source brightness. In addition, an increase in the bandwidth of the source requires phase correction of the source arising from the dispersion of the optical elements present in the experiment and the length of the fiber link.

These limitations are overcome in the present network. Scaling can be achieved by increasing the diameter of the SPDC ring; however, for a given input power and figure of merit of the nonlinear crystal, the photon pair density over a larger annular area decreases the collection efficiency and channel bit rate. This can be mitigated by increasing the pump power (see Fig. 8.4), thereby generating photon pairs at a higher

rate to compensate for the spatial spread. Although increasing the number of usable spatial sections via D-shaped mirror sectioning introduces diffraction and a loss in the coincidence rate. The use of higher-brightness sources, improved detection efficiency, and advanced collection schemes like ring-shaped microlens arrays, multicore fibers, and multiplexing techniques in integrated platforms can help mitigate these challenges.

Furthermore, considering each user as a node, additional scalability can be achieved by integrating WDM devices and/or one-to-many beam splitters. Employing faster detection systems and reducing the coincidence window allows higher source brightness and mitigates interlink crosstalk. Importantly, simultaneous communication between network nodes is not hindered by the absence of a node or its users, except that users connected through that node become inaccessible for communication.

8.5 Conclusion

We have demonstrated a scalable quantum network architecture based on spatial division and beam-splitter-based multiplexing of an SPDC ring, enabling simultaneous distribution of polarization-entangled photon pairs among multiple users. In contrast to conventional schemes relying on WDM or multi-core fiber arrays, our approach eliminates the need for narrowband filters and complex spatial coupling optics, thereby preserving high photon collection efficiency while minimizing inter-channel crosstalk.

The network supports dynamic reconfiguration, allowing users to be added or removed without altering the core optical setup, making it highly adaptable for real-world deployment. Using polarization measurements in mutually unbiased bases (HV and DA), we estimated a total sifted key rate of 407 kbps and a secure key rate of 76 kbps across all user pairs, demonstrating the viability of the architecture for high-throughput quantum key distribution.

Scalability can be further enhanced by increasing the diameter of the SPDC ring and pump power, enabling more communication channels without compromising the bit rate. Moreover, integrating the current scheme with WDM devices or one-to-many beam splitters offers a route toward building even larger quantum networks. Our results establish a versatile and efficient platform for a next-generation global quantum network for multi-user quantum communication, overcoming key limitations of WDM-based approaches in terms of spectral channel constraints and inter-channel crosstalk. In gist, in a conventional WDM-based multi-party network, we split the signal and idler photon spectra using very narrowband filters for generating multiple entangled photon sources. Hence, WDM-based networks use photon pairs with a spectral width in the range of 0.1–0.2 nm, and a lower overall coincidence rate in the network is expected, even with a larger number of EPS. This also introduces inter-channel crosstalk. Also, at the experimental level, there is a trade-off between photon bandwidth and generation rate, so the scalability with increasing the spectral bandwidth is limited. In contrast, in our case, the spectral width of the photon pairs is about 3 nm, which is more than an order of magnitude larger, resulting in a higher coincidence rate than the WDM scheme in a similar laboratory environment setup with fewer EPS. On the other hand, spatial sections multiplexing offers advantages such as reduced reliance on spectral filtering, lower crosstalk, and direct utilization of spatial correlations. We also showed that increasing the ring size accommodates more users without tampering with network metrics. In the final chapter, I will summarize and conclude with a discussion of the future scope.

Chapter 9

Conclusions and Future Scope

9.1 Conclusion

This thesis has presented a comprehensive study on the generation, characterization, and application of high-quality photon pairs from SPDC sources using the methodology of spatial sectioning and multiplexing, with special attention given to its role in quantum random number generation (QRNG), device-independent randomness certification, multi-user quantum key distribution (QKD) networks, protocol optimization, and entanglement fidelity preservation.

Beginning with the systematic characterization of heralded single-photon and entangled photon sources, we established clear experimental guidelines for optimizing quantum performance metrics such as the second-order correlation function $g^{(2)}(0)$, Hong–Ou–Mandel (HOM) interference visibility, and entanglement visibility. By varying coincidence windows, spectral filtering, collection modes, and pump power, we quantified the trade-offs between source brightness and quantumness, identifying prac-

tical configurations that meet the stringent requirements of modern quantum communication systems.

Building on these foundations, we proposed and experimentally demonstrated a beam-splitter-free QRNG that leverages the intrinsic temporal and spatial correlations of SPDC photon pairs. This approach eliminated the need for probabilistic optical elements while achieving high min-entropy and passing stringent statistical test suites, establishing a simplified and efficient architecture for true randomness generation. We then extended the concept to a device-independent QRNG (DI-QRNG) with simultaneous live Bell test certification, introducing a scalable spatial division technique that enabled the formation of multiple entangled photon sources from a single SPDC resource. This architecture set a new benchmark for the trustworthiness and scalability of DI-QRNGs.

The spatial profile division-multiplexing principle was further harnessed to realize a fully connected, 12-channel QKD network for six users without reliance on wavelength division multiplexing (WDM) or complex coupling optics. This design maintained high photon collection efficiency, minimized inter-channel crosstalk, and supported dynamic user reconfiguration, demonstrating the viability of spatial-mode-based networking for next-generation quantum communication.

To improve QKD protocol efficiency, we introduced a spatial randomness-based BBM92 scheme that replaced conventional beam-splitter-based basis selection with deterministic spatial correlations from the SPDC ring. This innovation removed encoding bias, reduced QBER, and increased the sifted key rate by a factor of 6.4 compared to traditional implementations.

Finally, we addressed the detrimental impact of geometric phase (GP) and other

phase drifts on entangled photon visibility and QBER. Through both analytical modeling and experimental verification, we demonstrated that GP effects can significantly degrade QKD performance, and proposed a practical receiver-end compensation method using a QHQ waveplate configuration. This restored Bell-state fidelity above 95% and reduced QBER to secure operating levels, offering a robust solution for phase stabilization in long-distance and dynamically varying channels.

Collectively, the contributions of this thesis form a unified experimental toolkit for high-brightness, high-purity, and application-ready SPDC sources, supporting secure, scalable, and robust quantum communication infrastructures. The demonstrated designs and techniques are compatible with both terrestrial and satellite-based systems, providing a solid foundation for practical global quantum networks.

9.2 Future Scope

The research presented in this thesis opens several promising directions for further exploration and advancement. Regarding random number generation, a possible scheme is simultaneous loophole-free certification using Bell's parameter, which utilizes photons from two spatially random sections that simultaneously contribute to bit-string generation. For QRNG and DI-QRNG systems, multi-bit extraction using SPAD camera arrays or advanced micro-lens-array collection mechanisms could enable operation at hundreds of megabits per second, meeting the demands of high-throughput cryptographic and simulation applications. In quantum networking, scaling the SPDC ring size, optimizing the pump beam power, and combining spatial multiplexing with wavelength-division multiplexing could create hybrid architectures capable of supporting dozens of high-quality entanglement channels. The spatial randomness-based basis selection method can also be adapted to other entanglement-based protocols, such

as E91 or MDI-QKD, to enhance key rates and reduce error rates. The geometric phase compensation approach demonstrated here could be extended into real-time, feedback-controlled stabilization systems for free-space QKD links, including mobile or satellite-based platforms. Furthermore, integration with modern photonic platforms provides a practical route to transform bulk-optics implementations into compact, stable, and scalable quantum systems. Waveguide-based SPDC sources in materials such as lithium niobate or silicon nitride offer strong mode confinement, resulting in higher brightness and improved coupling efficiency. By fabricating arrays of such waveguides on a single chip, multiple photon-pair sources can be generated in parallel, effectively extending the spatial multiplexing concept into an integrated and highly stable architecture. In addition, integrated photonic circuits can incorporate key components such as beam splitters, phase shifters, and filters, significantly reducing alignment complexity and optical losses. The integration of on-chip detector arrays, including SPADs or superconducting nanowire detectors, further enables higher data rates. Overall, such integration will improve robustness, scalability, and compatibility, making it highly promising for practical, large-scale quantum communication applications.

List of Publications

Thesis related Publications

1. **Ayan Kumar Nai**, Amritash Sharma, Vimlesh Kumar, Sandeep Singh, Shreya Mishra, C. M. Chandrashekar, G. K. Samanta, “Beam-splitter-free, device-independent, high bit-rate, quantum random number generator based on temporal and spatial correlations of heralded single-photons,” AVS Quantum Sci. 7, 011401 (2025).
DOI: <https://doi.org/10.1116/5.0245672>
2. **Ayan Kumar Nai**, Vimlesh Kumar, M. Ebrahim-Zadeh, and G. K. Samanta, “Device-independent, megabit-rate quantum random number generator with beam-splitter-free architecture and live Bell test certification,” Opt. Express 33, 44878-44889 (2025).
DOI: <https://doi.org/10.1364/OE.569257>
3. **Ayan Kumar Nai**, Gopal Prasad Sahu, Rutuj Gharate, C. M. Chandrashekar, and G. K. Samanta. “Beam-splitter-free, high-rate quantum key distribution inspired by intrinsic quantum mechanical spatial randomness of entangled photons,” arXiv preprint arXiv:2509.10231 (2025). (Under Review)
4. **Ayan Kumar Nai** and G. K. Samanta. “Free-space multi-user quantum network with high key rate,” arXiv preprint arXiv:2511.00466 (2025). (Under Review)

5. **Ayan Kumar Nai** and G. K. Samanta. “Active phase compensation and Bell State revival at receiver end for entanglement-based quantum key distribution using geometric phase” (Under Preparation)
6. **Ayan Kumar Nai** and G. K. Samanta. “Different characteristic quantum parameters of a SPDC source in different collection scenarios” (Under Preparation)

Not included in thesis

1. Milan Jana, Swagata Sarkar, **Ayan Kumar Nai** and G. K. Samanta. “Spatial multiplexing of Type-0 SPDC photons to establish entanglement in single-pass geometry” (Under Preparation)

Bibliography

- [1] B. Dwivedi, *James clerk maxwell and his equations*, Resonance **8**, 4–16 (2003).
- [2] A. B. Arons and M. Peppard, *Einstein's proposal of the photon concept—a translation of the annalen der physik paper of 1905*, American Journal of Physics **33**, 367–374 (1965).
- [3] G. N. Lewis, *The conservation of photons*, Nature **118**, 874–875 (1926).
- [4] P. A. M. Dirac, *The quantum theory of the emission and absorption of radiation*, Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character **114**, 243–265 (1927).
- [5] A. Einstein, B. Podolsky, and N. Rosen, *Can quantum-mechanical description of physical reality be considered complete?* Physical review **47**, 777 (1935).
- [6] J. S. Bell, *On the einstein podolsky rosen paradox*, Physics Physique Fizika **1**, 195 (1964).
- [7] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories*, Physical review letters **23**, 880 (1969).
- [8] S. J. Freedman and J. F. Clauser, *Experimental test of local hidden-variable theories*, Physical review letters **28**, 938 (1972).

- [9] A. Aspect, J. Dalibard, and G. Roger, *Experimental test of bell's inequalities using time-varying analyzers*, Physical review letters **49**, 1804 (1982).
- [10] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, *Experimental quantum teleportation*, Nature **390**, 575–579 (1997).
- [11] H. J. Kimble, M. Dagenais, and L. Mandel, *Photon antibunching in resonance fluorescence*, Physical Review Letters **39**, 691 (1977).
- [12] R. Hanbury Brown and R. Q. Twiss, *A Test of a new type of stellar interferometer on Sirius*, Nature **178**, 1046–1048 (1956).
- [13] I. Ali Khan and J. C. Howell, *Experimental demonstration of high two-photon time-energy entanglement*, Physical Review A—Atomic, Molecular, and Optical Physics **73**, 031801 (2006).
- [14] C. Law and J. Eberly, *Analysis and interpretation of high transverse entanglement in optical parametric down conversion*, Physical review letters **92**, 127903 (2004).
- [15] S. Walborn and C. Monken, *Transverse spatial entanglement in parametric down-conversion*, Physical Review A—Atomic, Molecular, and Optical Physics **76**, 062305 (2007).
- [16] P. G. Kwiat, P. H. Eberhard, A. M. Steinberg, and R. Y. Chiao, *Proposal for a loophole-free bell inequality experiment*, Physical Review A **49**, 3209 (1994).
- [17] J. Rarity and P. Tapster, *Experimental violation of bell's inequality based on phase and momentum*, Physical Review Letters **64**, 2495 (1990).
- [18] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, *Entanglement of the orbital angular momentum states of photons*, Nature **412**, 313–316 (2001).

- [19] Z.-S. Yuan, X.-H. Bao, C.-Y. Lu, J. Zhang, C.-Z. Peng, and J.-W. Pan, *Entangled photons and quantum communication*, Physics Reports **497**, 1–40 (2010).
- [20] R. W. Boyd, A. L. Gaeta, and E. Giese, *Nonlinear optics*, in “Springer Handbook of Atomic, Molecular, and Optical Physics,” (Springer, 2008), pp. 1097–1110.
- [21] B. Y. Zel’Dovich and D. Klyshko, *Field statistics in parametric luminescence*, Soviet Journal of Experimental and Theoretical Physics Letters **9**, 40 (1969).
- [22] D. C. Burnham and D. L. Weinberg, *Observation of simultaneity in parametric production of optical photon pairs*, Physical Review Letters **25**, 84 (1970).
- [23] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum cryptography*, Reviews of modern physics **74**, 145 (2002).
- [24] B. Ndagano, H. Defienne, D. Branford, Y. D. Shah, A. Lyons, N. Westerberg, E. M. Gauger, and D. Faccio, *Quantum microscopy based on hong–ou–mandel interference*, Nature Photonics **16**, 384–389 (2022).
- [25] U. Sinha, C. Couteau, T. Jennewein, R. Laflamme, and G. Weihs, *Ruling out multi-order interference in quantum mechanics*, Science **329**, 418–421 (2010).
- [26] H.-Q. Ma, Y. Xie, and L.-A. Wu, *Random number generation based on the time of arrival of single photons*, Applied optics **44**, 7760–3 (2006).
- [27] M. Stipčević and B. M. Rogina, *Quantum random number generator based on photonic emission in semiconductors*, Review of Scientific Instruments **78**, 045104 (2007).
- [28] M. Hai-Qiang, W. Su-Mei, Z. Da, C. Jun-Tao, J. Ling-Ling, H. Yan-Xue, and

- W. Ling-An, *A random number generator based on quantum entangled photon pairs*, Chinese Physics Letters **21**, 1961 (2004).
- [29] Y. Dodis, D. Pointcheval, S. Ruhault, D. Vergnaud, and D. Wichs, *Security analysis of pseudo-random number generators with input: /dev/random is not robust*, Cryptology ePrint Archive, Paper 2013/338 (2013).
- [30] G. Brassard and C. Goutier, *Cryptologie contemporaine*, vol. 9 (Paris Milan Mexico Masson, 1993).
- [31] C. H. Vincent, *Precautions for accuracy in the generation of truly random binary numbers*, Journal of Physics E: Scientific Instruments **4**, 825 (1971).
- [32] D. Chaum and W. L. Price, *Advances in Cryptology–EUROCRYPT’87: Workshop on the Theory and Application of Cryptographic Techniques, Amsterdam, The Netherlands, April 13-15, 1987 Proceedings*, vol. 304 (Springer, 2003).
- [33] H. Schmidt, *Quantum-Mechanical Random-Number Generator*, Journal of Applied Physics **41**, 462–468 (1970).
- [34] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000), 10th ed.
- [35] E. Jeffrey and P. Kwiat, *Delayed-choice quantum cryptography*, in “Postconference Digest Quantum Electronics and Laser Science, 2003. QELS.”, (2003), pp. 2 pp.–.
- [36] T. Graham, H. Bernstein, T. Wei, M. Junge, and P. Kwiat, *Superdense teleportation using hyperentangled photons*, Nature communications **6** (2015). Publisher Copyright: © 2015 Macmillan Publishers Limited. All rights reserved.

- [37] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, *Beating the channel capacity limit for linear photonic superdense coding*, Nature Physics **4**, 282–286 (2008).
- [38] M. Aslan, *Entropy estimation methods and health tests for cryptographic random number generators*, Ph.D. thesis, Middle East Technical University (Turkey) (2024).
- [39] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert *et al.*, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, vol. 22 (US Department of Commerce, Technology Administration, National Institute of ..., 2001).
- [40] M. Herrero-Collantes and J. C. Garcia-Escartin, *Quantum random number generators*, Rev. Mod. Phys. **89**, 015004 (2017).
- [41] S. Aaronson, *Quantum computing since Democritus* (Cambridge University Press, 2013).
- [42] J. Reeds, *The code book: The evolution of secrecy from mary, queen of scots to quantum cryptography*, (2000).
- [43] H. Delfs, H. Knebl, and H. Knebl, *Introduction to cryptography*, vol. 2 (Springer, 2002).
- [44] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. Sloane, *Quantum error correction via codes over $gf(4)$* , IEEE Transactions on Information Theory **44**, 1369–1387 (1998).
- [45] R. Prasad and A. Koren, *Safeguarding 6G: Security and Privacy for the Next Generation* (CRC Press, 2025).

- [46] S. Wiesner, *Conjugate coding*, ACM Sigact News **15**, 78–88 (1983).
- [47] A. Molina, T. Vidick, and J. Watrous, *Optimal counterfeiting attacks and generalizations for wiesner’s quantum money*, in “Conference on Quantum Computation, Communication, and Cryptography,” (Springer, 2012), pp. 45–64.
- [48] N. Lütkenhaus, *Security against individual attacks for realistic quantum key distribution*, Physical Review A **61**, 052304 (2000).
- [49] T. Eberle, *Realization of finite-size quantum key distribution based on Einstein-Podolsky-Rosen entangled light* (Hannover: Gottfried Wilhelm Leibniz Universität Hannover, 2013).
- [50] C. M. Mabena, *Distortion correction for free-space quantum communication* (University of the Witwatersrand, Johannesburg (South Africa), 2019).
- [51] S. Biswas, R. S. Goswami, and K. H. K. Reddy, *A cluster-based quantum key distribution with dynamic node selection: an improved approach for scalability and security in quantum communication*, Quantum Machine Intelligence **6**, 63 (2024).
- [52] L. Ma, A. Mink, and X. Tang, *High speed quantum key distribution over optical fiber network system*, Journal of research of the National Institute of Standards and Technology **114**, 149 (2009).
- [53] C. Kollmitzer and M. Pivk, *Applied quantum cryptography*, vol. 797 (springer, 2010).
- [54] A. K. Jha, *Coherence properties of the entangled two-photon field produced by parametric down conversion* (University of Rochester, 2009).

- [55] L. Caspani, C. Xiong, B. J. Eggleton, D. Bajoni, M. Liscidini, M. Galli, R. Morandotti, and D. J. Moss, *Integrated sources of photon quantum states based on nonlinear optics*, *Light: Science & Applications* **6**, e17100–e17100 (2017).
- [56] S. Singh, *Generation and characterization of pair photon source for quantum sensing applications*, Ph.D. thesis, Indian Institute of Technology Gandhinagar (2023).
- [57] R. Menzel, *Photonics: linear and nonlinear interactions of laser light and matter* (Springer, 2007).
- [58] S. Karan, S. Aarav, H. Bharadhwaj, L. Taneja, A. De, G. Kulkarni, N. Meher, and A. K. Jha, *Phase matching in β -barium borate crystals for spontaneous parametric down-conversion*, *Journal of Optics* **22**, 083501 (2020).
- [59] R. J. Glauber, *The quantum theory of optical coherence*, *Physical Review* **130**, 2529 (1963).
- [60] R. Loudon, *The quantum theory of light* (OUP Oxford, 2000).
- [61] G. Grynberg, A. Aspect, and C. Fabre, *Introduction to quantum optics: from the semi-classical approach to quantized light* (Cambridge university press, 2010).
- [62] J. C. Matthews, *Multi-photon quantum information science and technology in integrated optics* (Springer Science & Business Media, 2012).
- [63] P. B. Rudolf, *Uncovering photoinduced chemical reaction pathways in the liquid phase with ultrafast vibrational spectroscopy*, Ph.D. thesis, Universität Würzburg (2014).

- [64] C. Zhang, Y.-F. Huang, B.-H. Liu, C.-F. Li, and G.-C. Guo, *Spontaneous parametric down-conversion sources for multiphoton experiments*, Advanced Quantum Technologies **4**, 2000132 (2021).
- [65] C. Piccinini, *Experimental realization of quantum scanning microscopy through spdc-based correlated photon-pairs*, Master's thesis, SCUOLA DI INGEGNERIA INDUSTRIALE E DELL'INFORMAZIONE (2021).
- [66] C. S. Kumar, *High-power, fiber-laser-pumped optical parametric oscillators from the visible to mid-infrared*, Doctoral thesis, Universitat Politècnica de Catalunya (UPC) (2012).
- [67] A. K. Ekert, *Quantum cryptography based on bell's theorem*, Physical review letters **67**, 661 (1991).
- [68] M. Godfrey, P. Grangier, T. Langer, A. Leverrier, and W. SECOQC, *Bennett, ch, brassard, g., crépeau, c. and maurer, um (1995). generalized privacy amplification. information theory, ieee transactions on. 41 (6), 1915*, Physical Review A **67**, 5 (1996).
- [69] C. H. Bennett, *Quantum cryptography using any two nonorthogonal states*, Physical review letters **68**, 3121 (1992).
- [70] H. Inamori, N. Lütkenhaus, and D. Mayers, *Unconditional security of practical quantum key distribution*, The European Physical Journal D **41**, 599–627 (2007).
- [71] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, *Security of quantum key distribution with imperfect devices*, in “International Symposium on Information Theory, 2004. ISIT 2004. Proceedings.”, (IEEE, 2004), p. 136.

- [72] R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J.-F. Roch, A. Beveratos, R. Brouri-Tualle, J.-P. Poizat, and P. Grangier, *Experimental open-air quantum key distribution with a single-photon source*, New Journal of physics **6**, 92 (2004).
- [73] T. Gaebel, I. Popa, A. Gruber, M. Domhan, F. Jelezko, and J. Wrachtrup, *Stable single-photon source in the near infrared*, New Journal of Physics **6**, 98 (2004).
- [74] E. Wu, J. Rabeau, G. Roger, F. Treussart, H. Zeng, P. Grangier, S. Prawer, and J.-F. Roch, *Room temperature triggered single-photon source in the near infrared*, New Journal of Physics **9**, 434 (2007).
- [75] S. Kako, C. Santori, K. Hoshino, S. Götzinger, Y. Yamamoto, and Y. Arakawa, *A gallium nitride single-photon source operating at 200 K*, Nature materials **5**, 887–892 (2006).
- [76] S. Strauf, N. G. Stoltz, M. T. Rakher, L. A. Coldren, P. M. Petroff, and D. Bouwmeester, *High-frequency single-photon source with polarization control*, Nature photonics **1**, 704–708 (2007).
- [77] M. Hennrich, T. Legero, A. Kuhn, and G. Rempe, *Transition from antibunching to bunching in cavity QED*, New J. Phys. **6**, 86 (2004).
- [78] C. Maurer, C. Becher, C. Russo, J. Eschner, and R. Blatt, *A single-photon source based on a single Ca^{+} ion*, New J. Phys. **6**, 94 (2004).
- [79] M. Steiner, A. Hartschuh, R. Korlacki, and A. J. Meixner, *Single molecule fluorescence near metal nanostructures*, Appl. Phys. Lett. **90**, 183122 (2007).
- [80] S. Chen, Y.-A. Chen, T. Strassel, Z.-S. Yuan, B. Zhao, J. Schmiedmayer, and J.-W. Pan, *Deterministic and storable single-photon source based on a quantum memory*, Phys. Rev. Lett. **97**, 173004 (2006).

- [81] E. Waks, E. Diamanti, and Y. Yamamoto, *Generation of photon number states*, New J. Phys. **8**, 4 (2006).
- [82] A. Soujaeff, T. Nishioka, T. Hasegawa, S. Takeuchi, T. Tsurumaru, K. Sasaki, and M. Matsui, *Generation of entangled photon pairs using pdc*, Opt. Express **15**, 726 (2007).
- [83] A. B. U'Ren, C. Silberhorn, K. Banaszek, and I. A. Walmsley, *Efficient conditional preparation of high-fidelity single photon states*, Phys. Rev. Lett. **93**, 093601 (2004).
- [84] J. Fan and A. Migdall, *Generation of correlated photon pairs in microstructure fiber*, Opt. Express **15**, 2915 (2007).
- [85] E. A. Goldschmidt, M. D. Eisaman, J. Fan, S. V. Polyakov, and A. Migdall, *Spectral properties of the four-wave-mixing single-photon source*, Phys. Rev. A **78**, 013844 (2008).
- [86] C. Couteau, *Spontaneous parametric down-conversion*, Contemporary Physics **59**, 291–304 (2018).
- [87] A. Soujaeff, S. Takeuchi, K. Sasaki, T. Hasegawa, and M. Matsui, *Heralded single photon source at 1550 nm from pulsed parametric down conversion*, Journal of Modern optics **54**, 467–471 (2007).
- [88] H. J. Kimble, *The quantum internet*, Nature **453**, 1023–1030 (2008).
- [89] M. Ghalaii and S. Pirandola, *Quantum communications in a moderate-to-strong turbulent space*, Communications Physics **5**, 38 (2022).
- [90] P. Yepiz-Graciano, Z. Ibarra-Borja, R. Ramírez Alarcón, G. Gutiérrez-Torres, H. Cruz-Ramírez, D. Lopez-Mago, and A. B. U'Ren, *Quantum optical co-*

- herence microscopy for bioimaging applications*, Physical Review Applied **18**, 034060 (2022).
- [91] V. Kumar, V. Sharma, S. Singh, S. C. Kumar, A. Forbes, M. Ebrahim-Zadeh, and G. K. Samanta, *Imaging inspired characterization of single photons carrying orbital angular momentum*, AVS Quantum Science **4** (2022).
- [92] M. Jabir and G. K. Samanta, *Robust, high brightness, degenerate entangled photon source at room temperature*, Scientific reports **7**, 12613 (2017).
- [93] C. K. Hong, Z. Y. Ou, and L. Mandel, *Measurement of subpicosecond time intervals between two photons by interference*, Phys. Rev. Lett. **59**, 2044–2046 (1987).
- [94] A. B. U'Ren, C. Silberhorn, J. L. Ball, K. Banaszek, and I. A. Walmsley, *Characterization of the nonclassical nature of conditionally prepared single photons*, Phys. Rev. A **72**, 021802 (2005).
- [95] H. Fearn and R. Loudon, *Quantum theory of the lossless beam splitter*, Optics communications **64**, 485–490 (1987).
- [96] J. G. Rarity and P. Tapster, *Fourth-order interference in parametric downconversion*, Journal of the Optical Society of America B **6**, 1221–1226 (1989).
- [97] J. Rarity and P. Tapster, *Nonclassical effects in parametric downconversion*, in “Photons and Quantum Fluctuations,” (CRC Press, 2020), pp. 122–150.
- [98] D. A. Vajner, *From Quantum Dots to Quantum Communication Advances in Quantum Light Generation from Semiconductor Quantum Dots* (Technische Universitaet Berlin (Germany), 2025).

- [99] R. Pandey, N. Srivastava, N. K. Singh, and K. Tyagi, *Quantum computing: a shift from bits to qubits*, vol. 1085 (Springer, 2023).
- [100] R. Trivedi, K. A. Fischer, J. Vučković, and K. Müller, *Generation of non-classical light using semiconductor quantum dots*, *Advanced Quantum Technologies* **3**, 1900007 (2020).
- [101] H. Ollivier, S. E. Thomas, S. C. Wein, I. M. de Buy Wenniger, N. Coste, J. C. Loredó, N. Somaschi, A. Harouri, A. Lemaitre, I. Sagnes, L. Lanco, C. Simon, C. Anton, O. Krebs, and P. Senellart, *Hong-ou-mandel interference with imperfect single photon sources*, *Phys. Rev. Lett.* **126**, 063602 (2021).
- [102] F. James and L. Moneta, *Review of high-quality random number generators*, *Computing and Software for Big Science* **4**, 1–12 (2020).
- [103] Q. Luo, Z. Cheng, J. Fan, L. Tan, H. Song, G. Deng, Y. Wang, and Q. Zhou, *Quantum random number generator based on single-photon emitter in gallium nitride*, *Opt. Lett.* **45**, 4224–4227 (2020).
- [104] S. J. U. White, F. Klauck, T. Trong Tran, N. Schmitt, M. Kianinia, A. Steinfurth, M. Heinrich, M. Toth, A. Szameit, I. Aharonovich, and A. S. Solntsev, *Quantum random number generation using a hexagonal boron nitride single photon emitter*, *Journal of Optics* **23**, 01LT01 (2021).
- [105] X. Chen, J. N. Greiner, J. Wrachtrup, and I. Gerhardt, *Single photon randomness based on a defect center in diamond*, *Scientific Reports* **9**, 18474 (2019).
- [106] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, *High-speed quantum random number generation by measuring phase noise of a single-mode laser*, *Opt. Lett.* **35**, 312–314 (2010).

- [107] B. Haylock, D. Peace, F. Lenzini, C. Weedbrook, and M. Lobino, *Multiplexed Quantum Random Number Generation*, *Quantum* **3**, 141 (2019).
- [108] 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* **90**, 043105 (2019).
- [109] A. Dandasi, H. Ozel, O. Hasekioglu, and K. Durak, *Effect of photon statistics on vacuum fluctuations based QRNG*, *Journal of Optics* **23**, 065201 (2021).
- [110] M. J. Ferreira, N. A. Silva, A. N. Pinto, and N. J. Muga, *Characterization of a quantum random number generator based on vacuum fluctuations*, *Applied Sciences* **11** (2021).
- [111] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, *Ultrafast quantum random number generation based on quantum phase fluctuations*, *Opt. Express* **20**, 12366–12377 (2012).
- [112] 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* **93**, 031109 (2008).
- [113] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, *A fast and compact quantum random number generator*, *Review of Scientific Instruments* **71**, 1675–1680 (2000).
- [114] M. A. Wayne and P. G. Kwiat, *Low-bias high-speed quantum random number generator via shaped optical pulses*, *Opt. Express* **18**, 9351–9357 (2010).
- [115] J. E. Jacak, W. A. Jacak, W. A. Donderowicz, and L. Jacak, *Quantum random number generators with entanglement for public randomness testing*, *Scientific Reports* **10**, 164 (2020).

- [116] Y.-H. Li, X. Han, Y. Cao, X. Yuan, Z.-P. Li, J.-Y. Guan, J. Yin, Q. Zhang, X. Ma, C.-Z. Peng *et al.*, *Quantum random number generation with uncharacterized laser and sunlight*, npj Quantum Information **5**, 97 (2019).
- [117] T. Gehring, C. Lupo, A. Kordts, D. Solar Nikolic, N. Jain, T. Rydberg, T. B. Pedersen, S. Pirandola, and U. L. Andersen, *Homodyne-based quantum random number generator at 2.9 gbps secure against quantum side-information*, Nature Communications **12**, 605 (2021).
- [118] Z. Lu, J. Liu, X. Wang, P. Wang, Y. Li, and K. Peng, *Quantum random number generator with discarding-boundary-bin measurement and multi-interval sampling*, Optics Express **29** (2021).
- [119] N. Leone, S. Azzini, S. Mazzucchi, V. Moretti, and L. Pavesi, *Certified quantum random-number generator based on single-photon entanglement*, Phys. Rev. Appl. **17**, 034011 (2022).
- [120] D. Branning and M. Bermudez, *Testing quantum randomness in single-photon polarization measurements with the nist test suite*, J. Opt. Soc. Am. B **27**, 1594–1602 (2010).
- [121] F. Xu, J. H. Shapiro, and F. N. C. Wong, *Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring*, Optica **3**, 1266–1269 (2016).
- [122] O. Kwon, Y.-W. Cho, and Y.-H. Kim, *Quantum random number generator using photon-number path entanglement*, Applied optics **48**, 1774–8 (2009).
- [123] S. Singh, V. Kumar, V. Sharma, D. Faccio, and G. K. Samanta, *Near-video frame rate quantum sensing using hong–ou–mandel interferometry*, Advanced Quantum Technologies **6**, 2300177 (2023).

- [124] S. Singh, V. Kumar, A. Ghosh, A. Forbes, and G. K. Samanta, *A tolerance-enhanced spontaneous parametric downconversion source of bright entangled photons*, *Advanced Quantum Technologies* **6**, 2200121 (2023).
- [125] S. Singh, V. Kumar, and G. Samanta, *Fast measurement of group index variation with optimum precision using hong–ou–mandel interferometry*, *APL Quantum* **1** (2024).
- [126] A. Lyons, V. Zickus, R. Álvarez-Mendoza, D. Triggiani, V. Tamma, N. Westerberg, M. Tassieri, and D. Faccio, *Fluorescence lifetime hong-ou-mandel sensing*, *Nature Communications* **14**, 8005 (2023).
- [127] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, *Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction*, *Physical Review A* **87**, 062327 (2013).
- [128] H. Krawczyk, *Lfsr-based hashing and authentication*, in “Annual International Cryptology Conference,” (Springer, 1994), pp. 129–139.
- [129] Y. Li, Y. Fei, W. Wang, X. Meng, H. Wang, Q. Duan, and Z. Ma, *Analysis of the effects of temperature increase on quantum random number generator*, *The European Physical Journal D* **75**, 69 (2021).
- [130] R. H. Hadfield, G. Johansson *et al.*, *Superconducting devices in quantum optics* (Springer, 2016).
- [131] P. L’ecuyer and R. Simard, *Testu01: A library for empirical testing of random number generators*, *ACM Transactions on Mathematical Software (TOMS)* **33**, 1–40 (2007).

- [132] M. E. O’neill, *Pcg: A family of simple fast space-efficient statistically good algorithms for random number generation*, ACM Transactions on Mathematical Software (2014).
- [133] Y. Zhang, L. K. Shalm, J. C. Bienfang, M. J. Stevens, M. D. Mazurek, S. W. Nam, C. Abellán, W. Amaya, M. W. Mitchell, H. Fu *et al.*, *Experimental low-latency device-independent quantum randomness*, Physical review letters **124**, 010505 (2020).
- [134] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan *et al.*, *Device-independent quantum random-number generation*, Nature **562**, 548–551 (2018).
- [135] L. Shen, J. Lee, L. P. Thinh, J.-D. Bancal, A. Cere, A. Lamas-Linares, A. Lita, T. Gerrits, S. W. Nam, V. Scarani *et al.*, *Randomness extraction from bell violation with continuous parametric down-conversion*, Physical review letters **121**, 150402 (2018).
- [136] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan *et al.*, *Device-independent randomness expansion against quantum side information*, Nature Physics **17**, 448–451 (2021).
- [137] K. M. Shafi, P. Chawla, A. S. Hegde, R. Gayatri, A. Padhye, and C. Chandrashekar, *Multi-bit quantum random number generator from path-entangled single photons*, EPJ Quantum Technology **10**, 43 (2023).
- [138] H.-Q. Ma, Y. Xie, and L.-A. Wu, *Random number generation based on the time of arrival of single photons*, Applied optics **44**, 7760–3 (2006).
- [139] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, *Ultrafast quantum ran-*

- dom number generation based on quantum phase fluctuations*, Opt. Express **20**, 12366–12377 (2012).
- [140] 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 **93**, 031109 (2008).
- [141] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerner, U. L. Andersen, C. Marquardt, and G. Leuchs, *A generator for unique quantum random numbers based on vacuum states*, Nature Photonics **4**, 711–715 (2010).
- [142] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning *et al.*, *Random numbers certified by bell’s theorem*, Nature **464**, 1021–1024 (2010).
- [143] A. Acín and L. Masanes, *Certified randomness in quantum physics*, Nature **540**, 213–219 (2016).
- [144] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan *et al.*, *Device-independent quantum random-number generation*, Nature **562**, 548–551 (2018).
- [145] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories*, Phys. Rev. Lett. **23**, 880–884 (1969).
- [146] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, *Detection-loophole-free test of quantum nonlocality, and applications*, Phys. Rev. Lett. **111**, 130406 (2013).
- [147] Z. Cao, H. Zhou, X. Yuan, and X. Ma, *Source-independent quantum random number generation*, Phys. Rev. X **6**, 011020 (2016).

- [148] D. G. Marangon, G. Vallone, and P. Villoresi, *Source-device-independent ultra-fast quantum random number generation*, Phys. Rev. Lett. **118**, 060503 (2017).
- [149] Z. Zheng, Y. Zhang, M. Huang, Z. Chen, S. Yu, and H. Guo, *Bias-free source-independent quantum random number generator*, Opt. Express **28**, 22388–22398 (2020).
- [150] A. K. Nai, A. Sharma, V. Kumar, S. Singh, S. Mishra, C. Chandrashekar, and G. Samanta, *Beam-splitter-free, device-independent, high bit-rate, quantum random number generator based on temporal and spatial correlations of heralded single-photons*, AVS Quantum Science **7** (2025).
- [151] Y. Yu, P.-F. Sun, Y.-Z. Zhang, B. Bai, Y.-Q. Fang, X.-Y. Luo, Z.-Y. An, J. Li, J. Zhang, F. Xu, X.-H. Bao, and J.-W. Pan, *Measurement-device-independent verification of a quantum memory*, Phys. Rev. Lett. **127**, 160502 (2021).
- [152] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, *High-rate measurement-device-independent quantum cryptography*, Nature Photonics **9**, 397–402 (2015).
- [153] L. Li, M. Cai, T. Wang, Z. Tan, P. Huang, K. Wu, and G. Zeng, *On-chip source-device-independent quantum random number generator*, Photon. Res. **12**, 1379–1394 (2024).
- [154] J. Cheng, S. Liang, J. Qin, J. Li, Z. Yan, X. Jia, C. Xie, and K. Peng, *Semi-device-independent quantum random number generator with a broadband squeezed state of light*, npj Quantum Information **10**, 20 (2024).
- [155] A. Garg and N. D. Mermin, *Detector inefficiencies in the einstein-podolsky-rosen experiment*, Physical Review D **35**, 3831 (1987).

- [156] T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X.-S. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. K. Langford, T. Jennewein *et al.*, *Violation of local realism with freedom of choice*, Proceedings of the National Academy of Sciences **107**, 19708–19713 (2010).
- [157] R. König, R. Renner, and C. Schaffner, *The operational meaning of min-and max-entropy*, IEEE Transactions on Information theory **55**, 4337–4347 (2009).
- [158] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, *Quantum randomness certified by the uncertainty principle*, Phys. Rev. A **90**, 052327 (2014).
- [159] K. M. Shafi, P. Chawla, A. S. Hegde, R. Gayatri, A. Padhye, and C. Chandrashekar, *Multi-bit quantum random number generator from path-entangled single photons*, EPJ Quantum Technology **10**, 43 (2023).
- [160] M. Pivoluska, M. Plesch, M. Farkas, N. Ružičková, C. Flegel, N. H. Valencia, W. McCutcheon, M. Malik, and E. A. Aguilar, *Semi-device-independent random number generation with flexible assumptions*, npj Quantum Information **7**, 50 (2021).
- [161] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Review **41**, 303–332 (1999).
- [162] A. Ekert and R. Jozsa, *Quantum computation and shor’s factoring algorithm*, Reviews of Modern Physics **68**, 733 (1996).
- [163] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill, *Efficient networks for quantum factoring*, Physical Review A **54**, 1034 (1996).
- [164] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Theoretical Computer Science **560**, 7–11 (2014).

- [165] N. Gisin and R. T. Thew, *Quantum communication technology*, Electronics letters **46**, 965–967 (2010).
- [166] J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai *et al.*, *Satellite-to-ground entanglement-based quantum key distribution*, Phys. Rev. Lett. **119**, 200501 (2017).
- [167] P. W. Shor and J. Preskill, *Simple proof of security of the bb84 quantum key distribution protocol*, Phys. Rev. Lett. **85**, 441 (2000).
- [168] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, *Overcoming the rate–distance limit of quantum key distribution without quantum repeaters*, Nature **557**, 400–403 (2018).
- [169] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, *Security of quantum key distribution with imperfect devices*, in “International Symposium on Information Theory, 2004. ISIT 2004. Proceedings.”, (IEEE, 2004), p. 136.
- [170] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, *Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations*, Phys. Rev. Lett. **92**, 057901 (2004).
- [171] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. Towery, and S. Ten, *High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres*, New Journal of Physics **11**, 075003 (2009).
- [172] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, *Advances in quantum cryptography*, Advances in Optics and Photonics **12**, 1012–1236 (2020).

- [173] M. Lucamarini, G. Vallone, I. Gianani, P. Mataloni, and G. Di Giuseppe, *Device-independent entanglement-based bennett 1992 protocol*, Physical Review A—Atomic, Molecular, and Optical Physics **86**, 032325 (2012).
- [174] B. Huttner, N. Imoto, N. Gisin, and T. Mor, *Quantum cryptography with coherent states*, Phys. Rev. A **51**, 1863–1869 (1995).
- [175] E. Waks, A. Zeevi, and Y. Yamamoto, *Security of quantum key distribution with entangled photons against individual attacks*, Physical Review A **65**, 052310 (2002).
- [176] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, *Limitations on practical quantum cryptography*, Phys. Rev. Lett. **85**, 1330 (2000).
- [177] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, *Quantum cloning*, Rev. Mod. Phys. **77**, 1225–1256 (2005).
- [178] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes *et al.*, *The secoqc quantum key distribution network in vienna*, New Journal of Physics **11**, 075001 (2009).
- [179] V. Coffman, J. Kundu, and W. K. Wootters, *Distributed entanglement*, Physical Review A **61**, 052306 (2000).
- [180] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, *Secure quantum key distribution with realistic devices*, Reviews of Modern Physics **92**, 025002 (2020).
- [181] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu *et al.*, *Satellite-relayed intercontinental quantum network*, Phys. Rev. Lett. **120**, 030501 (2018).

- [182] A. Villar, A. Lohrmann, X. Bai, T. Vergoossen, R. Bedington, C. Perumangatt, H. Y. Lim, T. Islam, A. Reezwana, Z. Tang *et al.*, *Entanglement demonstration on board a nano-satellite*, *Optica* **7**, 734–737 (2020).
- [183] C. H. Bennett, G. Brassard, and N. D. Mermin, *Quantum cryptography without bell's theorem*, *Phys. Rev. Lett.* **68**, 557 (1992).
- [184] L. Masanes, S. Pironio, and A. Acín, *Secure device-independent quantum key distribution with causally independent measurement devices*, *Nat. Comm.* **2**, 238 (2011).
- [185] A. Scherer, B. C. Sanders, and W. Tittel, *Long-distance practical quantum key distribution by entanglement swapping*, *Opt. Express* **19**, 3004–3018 (2011).
- [186] S. Harris, M. Oshman, and R. Byer, *Observation of tunable optical parametric fluorescence*, *Phys. Rev. Lett.* **18**, 732 (1967).
- [187] S. Mishra, A. Biswas, S. Patil, P. Chandravanshi, V. Mongia, T. Sharma, A. Rani, S. Prabhakar, S. Ramachandran, and R. P. Singh, *Bbm92 quantum key distribution over a free space dusty channel of 200 meters*, *Journal of Optics* **24**, 074002 (2022).
- [188] F. Steinlechner, M. Gilaberte, M. Jofre, T. Scheidl, J. P. Torres, V. Pruneri, and R. Ursin, *Efficient heralding of polarization-entangled photons from type-0 and type-ii spontaneous parametric downconversion in periodically poled ktiopo4*, *Journal of the Optical Society of America B* **31**, 2068–2076 (2014).
- [189] D.-D. Li, Y.-L. Tang, Y.-K. Zhao, L. Zhou, Y. Zhao, and S.-B. Tang, *Security of optical beam splitter in quantum key distribution*, *Photonics* **9** (2022).

- [190] A. K. Nai, V. Kumar, M. Ebrahim-Zadeh, and G. Samanta, *Device-independent, megabit-rate quantum random number generator with beam-splitter-free architecture and live bell test certification*, Optics Express **33**, 44878–44889 (2025).
- [191] S. P. Neumann, T. Scheidl, M. Selimovic, M. Pivoluska, B. Liu, M. Bohmann, and R. Ursin, *Model for optimizing quantum key distribution with continuous-wave pumped entangled-photon sources*, Physical Review A **104**, 022406 (2021).
- [192] T. Feng, R. Fan, R. Fan, C. Wang, C. Huang, A. Li, H. Zhang, Y. Cao, and L. Li, *Pre-and post-compensation to suppress birefringent walk-off effects of entangled photons*, Optics Express **32**, 40283–40292 (2024).
- [193] Z.-Y. Zhou, Y.-K. Jiang, D.-S. Ding, and B.-S. Shi, *An ultra-broadband continuously-tunable polarization-entangled photon-pair source covering the $c+l$ telecom bands based on a single type-ii ppktp crystal*, Journal of Modern Optics **60**, 720–725 (2013).
- [194] S. Cialdi, D. Brivio, E. Tesio, and M. G. Paris, *Nonlocal compensation of pure phase objects with entangled photons*, Physical Review A—Atomic, Molecular, and Optical Physics **84**, 043817 (2011).
- [195] F. Steinlechner, S. Ramelow, M. Jofre, M. Gilaberte, T. Jennewein, J. P. Torres, M. W. Mitchell, and V. Pruneri, *Phase-stable source of polarization-entangled photons in a linear double-pass configuration*, Optics express **21**, 11943–11951 (2013).
- [196] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, *New high-intensity source of polarization-entangled photon pairs*, Physical Review Letters **75**, 4337 (1995).

-
- [197] J. B. Altepeter, E. R. Jeffrey, and P. G. Kwiat, *Phase-compensated ultra-bright source of entangled photons*, Optics Express **13**, 8951–8959 (2005).
- [198] T. Feng, S. Zhang, T. Wu, Z. Song, and L. Li, *Entangled photon-pair source using a wedge-shaped nonlinear crystal*, Optical Materials **145**, 114441 (2023).
- [199] X.-F. Mo, B. Zhu, Z.-F. Han, Y.-Z. Gui, and G.-C. Guo, *Faraday–michelson system for quantum cryptography*, Optics letters **30**, 2632–2634 (2005).
- [200] Z.-Q. Zhou, C.-F. Li, G. Chen, J.-S. Tang, Y. Zou, M. Gong, and G.-C. Guo, *Phase compensation enhancement of photon pair entanglement generated from biexciton decay in quantum dots*, Physical Review A—Atomic, Molecular, and Optical Physics **81**, 064302 (2010).
- [201] R. B. Patel, J. Ho, F. Ferreyrol, T. C. Ralph, and G. J. Pryde, *A quantum fredkin gate*, Science advances **2**, e1501531 (2016).
- [202] W. Chen, Z. Han, X. Mo, F. Xu, G. Wei, and G. Guo, *Active phase compensation of quantum key distribution system*, Chinese Science Bulletin **53**, 1310–1314 (2008).
- [203] V. Kumar, C. Kaushik, M. Ebrahim-Zadeh, C. Chandrashekar, and G. Samanta, *Classical-to-quantum transfer of geometric phase for non-interferometric phase measurement and manipulation of quantum state*, arXiv preprint arXiv:2505.20108 (2025).
- [204] S. Pancharatnam, *Generalized theory of interference, and its applications*, Proceedings of the Indian Academy of Sciences - Section A **44**, 247–262 (1956).
- [205] M. V. Berry, *The adiabatic phase and pancharatnam’s phase for polarized light*, Journal of Modern Optics **34**, 1401–1407 (1987).

- [206] R. Simon, H. Kimble, and E. Sudarshan, *Evolving geometric phase and its dynamical manifestation as a frequency shift: an optical experiment*, Physical review letters **61**, 19 (1988).
- [207] E. Sjöqvist, *A new phase in quantum computation*, Physics **1**, 35 (2008).
- [208] Z. Zhou, S. C. Carrasco, C. Sanner, V. S. Malinovsky, and R. Folman, *Geometric phase amplification in a clock interferometer for enhanced metrology*, Science advances **11**, eadr6893 (2025).
- [209] L. Conrads, F. Bontke, A. Mathwieser, P. Buske, M. Wuttig, R. Schmitt, C. Holly, and T. Taubner, *Infrared beam-shaping on demand via tailored geometric phase metasurfaces employing the plasmonic phase-change material in3sbte2* , Nature Communications **16**, 3698 (2025).
- [210] R. Simon and N. Mukunda, *Universal su (2) gadget for polarization optics*, Physics Letters A **138**, 474–480 (1989).
- [211] A. Aspect, P. Grangier, and G. Roger, *Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: a new violation of bell's inequalities*, Physical review letters **49**, 91 (1982).
- [212] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels*, Physical review letters **70**, 1895 (1993).
- [213] S. Barz, *Quantum computing with photons: introduction to the circuit model, the one-way quantum computer, and the fundamental principles of photonic experiments*, Journal of Physics B: Atomic, Molecular and Optical Physics **48**, 083001 (2015).

- [214] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The security of practical quantum key distribution*, Reviews of Modern Physics **81**, 1301–1350 (2009).
- [215] T. Kim, M. Fiorentino, and F. N. Wong, *Phase-stable source of polarization-entangled photons using a polarization sagnac interferometer*, Physical Review A—Atomic, Molecular, and Optical Physics **73**, 012316 (2006).
- [216] H. Kim, O. Kwon, and H. S. Moon, *Pulsed sagnac source of polarization-entangled photon pairs in telecommunication band*, Scientific reports **9**, 5031 (2019).
- [217] T. Scheidl, R. Ursin, A. Fedrizzi, S. Ramelow, X.-S. Ma, T. Herbst, R. Prevedel, L. Ratschbacher, J. Kofler, T. Jennewein *et al.*, *Feasibility of 300 km quantum key distribution with entangled states*, New Journal of Physics **11**, 085002 (2009).
- [218] D. I. L. Achatz, *Strategies for generating, distributing and certifying entanglement in photonic systems*, Ph.D. thesis, Universität Wien (2023).
- [219] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *Experimental quantum cryptography*, Journal of cryptology **5**, 3–28 (1992).
- [220] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, *Quantum cryptography with entangled photons*, Phys. Rev. Lett. **84**, 4729–4732 (2000).
- [221] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, *Provably secure and practical quantum key distribution over 307 km of optical fibre*, Nature Photonics **9**, 163–168 (2015).
- [222] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang *et al.*, *Measurement-device-independent*

- quantum key distribution over a 404 km optical fiber*, Phys. Rev. Lett. **117**, 190501 (2016).
- [223] S. Wengerowsky, S. K. Joshi, F. Steinlechner, J. R. Zichi, B. Liu, T. Scheidl, S. M. Dobrovolskiy, R. v. d. Molen, J. W. Los, V. Zwiller *et al.*, *Passively stable distribution of polarisation entanglement over 192 km of deployed optical fibre*, npj Quantum Information **6**, 5 (2020).
- [224] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek *et al.*, *Entanglement-based quantum communication over 144 km*, Nature physics **3**, 481–486 (2007).
- [225] W.-Q. Cai, Y. Li, B. Li, J.-G. Ren, S.-K. Liao, Y. Cao, L. Zhang, M. Yang, J.-C. Wu, Y.-H. Li, W.-Y. Liu, J. Yin, C.-Z. Wang, W.-B. Luo, B. Jin, C.-L. Lv, H. Li, L. You, R. Shu, G.-S. Pan, Q. Zhang, N.-L. Liu, X.-B. Wang, J.-Y. Wang, C.-Z. Peng, and J.-W. Pan, *Free-space quantum key distribution during daylight and at night*, Optica **11**, 647–652 (2024).
- [226] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, *Satellite-to-ground quantum key distribution*, Nature **549**, 43–47 (2017).
- [227] R. Bedington, J. M. Arrazola, and A. Ling, *Progress in satellite quantum key distribution*, npj Quantum Information **3**, 30 (2017).
- [228] Y. Li, W.-Q. Cai, J.-G. Ren, C.-Z. Wang, M. Yang, L. Zhang, H.-Y. Wu, L. Chang, J.-C. Wu, B. Jin *et al.*, *Microsatellite-based real-time quantum key distribution*, Nature **640**, 47–54 (2025).

- [229] C. Simon, *Towards a global quantum network*, Nature Photonics **11**, 678–680 (2017).
- [230] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka *et al.*, *Field test of quantum key distribution in the tokyo qkd network*, Opt. Express **19**, 10387–10409 (2011).
- [231] L.-Q. Chen, J.-Q. Chen, Q.-Y. Chen, and Y.-L. Zhao, *A quantum key distribution routing scheme for hybrid-trusted qkd network system*, Quantum Information Processing **22**, 75 (2023).
- [232] R. V. Meter and J. Touch, *Designing quantum repeater networks*, IEEE Communications Magazine **51**, 64–71 (2013).
- [233] G. Avis, F. Ferreira da Silva, T. Coopmans, A. Dahlberg, H. Jirovská, D. Maier, J. Rabbie, A. Torres-Knoop, and S. Wehner, *Requirements for a processing-node quantum repeater on a real-world fiber grid*, npj Quantum Information **9**, 100 (2023).
- [234] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin, *Quantum repeaters: From quantum networks to the quantum internet*, Rev. Mod. Phys. **95**, 045006 (2023).
- [235] V. Mannalath and A. Pathak, *Multiparty entanglement routing in quantum networks*, Phys. Rev. A **108**, 062614 (2023).
- [236] G. Avis, F. Rozpedek, and S. Wehner, *Analysis of multipartite entanglement distribution using a central quantum-network node*, Phys. Rev. A **107**, 012609 (2023).
- [237] P. D. Townsend, *Quantum cryptography on multiuser optical fibre networks*, Nature **385**, 47–49 (1997).

- [238] X. Liu, J. Liu, R. Xue, H. Wang, H. Li, X. Feng, F. Liu, K. Cui, Z. Wang, L. You *et al.*, *40-user fully connected entanglement-based quantum key distribution network without trusted node*, *Photonix* **3**, 2 (2022).
- [239] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, *An entanglement-based wavelength-multiplexed quantum communication network*, *Nature* **564**, 225–228 (2018).
- [240] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Ž. Samec, L. Kling *et al.*, *A trusted node-free eight-user metropolitan quantum communication network*, *Science advances* **6**, eaba0959 (2020).
- [241] E. A. Ortega, K. Dovzhik, J. Fuenzalida, S. Wengerowsky, J. C. Alvarado-Zacarias, R. F. Shiozaki, R. Amezcu-Correa, M. Bohmann, and R. Ursin, *Experimental space-division multiplexed polarization-entanglement distribution through 12 paths of a multicore fiber*, *PRX quantum* **2**, 040356 (2021).
- [242] Y. Lei, F. K. Asadi, T. Zhong, A. Kuzmich, C. Simon, and M. Hosseini, *Quantum optical memory for entanglement distribution*, *Optica* **10**, 1511–1528 (2023).
- [243] E. Agrell, M. Karlsson, F. Poletti, S. Namiki, X. V. Chen, L. A. Rusch, B. Puttnam, P. Bayvel, L. Schmalen, Z. Tao, F. R. Kschischang, A. Alvarado, B. Mukherjee, R. Casellas, X. Zhou, D. van Veen, G. Mohs, E. Wong, A. Mecozzi, M.-S. Alouini, E. Diamanti, and M. Uysal, *Roadmap on optical communications*, *Journal of Optics* **26**, 093001 (2024).
- [244] X. Liu, X. Yao, R. Xue, H. Wang, H. Li, Z. Wang, L. You, X. Feng, F. Liu, K. Cui, Y. Huang, and W. Zhang, *An entanglement-based quantum network*

- based on symmetric dispersive optics quantum key distribution*, APL Photonics **5**, 076104 (2020).
- [245] D. J. Richardson, J. M. Fini, and L. E. Nelson, *Space-division multiplexing in optical fibres*, Nature photonics **7**, 354–362 (2013).
- [246] B. J. Puttnam, G. Rademacher, and R. S. Luís, *Space-division multiplexing for optical fiber communications*, Optica **8**, 1186–1203 (2021).
- [247] G. B. Xavier and G. Lima, *Quantum information processing with space-division multiplexing optical fibres*, Communications Physics **3**, 9 (2020).
- [248] Z. Qi, Y. Li, Y. Huang, J. Feng, Y. Zheng, and X. Chen, *A 15-user quantum secure direct communication network*, Light: Science & Applications **10**, 183 (2021).