

RESEARCH ARTICLE | FEBRUARY 13 2025

Beam-splitter-free, device-independent, high bit-rate, quantum random number generator based on temporal and spatial correlations of heralded single-photons

Ayan Kumar Nai ; Amritash Sharma; Vimlesh Kumar ; Sandeep Singh ; Shreya Mishra; C. M. Chandrashekar ; G. K. Samanta 



AVS Quantum Sci. 7, 011401 (2025)

<https://doi.org/10.1116/5.0245672>



Articles You May Be Interested In

Heralded single-photon source fueled by light-emitting diode

Appl. Phys. Lett. (November 2019)

Generation of correlated quantum random number sequences with bright twin beams

Appl. Phys. Lett. (September 2025)

Indistinguishable MHz-narrow heralded photon pairs from a whispering gallery resonator

APL Photonics (May 2025)



Advance your science and your career as a member of **AVS**

LEARN MORE

Beam-splitter-free, device-independent, high bit-rate, quantum random number generator based on temporal and spatial correlations of heralded single-photons

Cite as: AVS Quantum Sci. 7, 011401 (2025); doi: 10.1116/5.0245672

Submitted: 28 October 2024 · Accepted: 24 January 2025 ·

Published Online: 13 February 2025



View Online



Export Citation



CrossMark

Ayan Kumar Nai,^{1,2,a)} Amritash Sharma,¹ Vimlesh Kumar,¹ Sandeep Singh,¹ Shreya Mishra,¹ C. M. Chandrashekar,^{3,4} and G. K. Samanta¹

AFFILIATIONS

¹Photonic Sciences Lab., Physical Research Laboratory, Ahmedabad, Gujarat 380009, India

²Indian Institute of Technology Gandhinagar, Ahmedabad, Gujarat 382424, India

³Quantum Optics and Quantum Information, Department of Instrumentation and Applied Physics, Indian Institute of Science, Bengaluru 560012, India

⁴The Institute of Mathematical Sciences, C. I. T. Campus, Taramani, Chennai 600113, India

^{a)} Author to whom correspondence should be addressed: ayankrnai@gmail.com

ABSTRACT

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, and acts as the 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 annular 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 (window of 1 ns) between photons from diametrically opposite sections and assigning bits (0 and 1), we extracted 90×10^6 raw bits over 27.7 s 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.

Published under an exclusive license by AIP Publishing. <https://doi.org/10.1116/5.0245672>

I. 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,^{1–3} and many aspects of our everyday lives.⁴ Traditional methods to generate random numbers often rely on mathematical algorithms.⁵ 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.⁶ Therefore, to achieve true randomness—as essential for the highest

levels of security, one needs to rely on physical phenomena,^{7,8} which are intrinsically random. Quantum mechanical processes,⁹ 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,^{10,11} defect centers,¹² phase noise,¹³ quantum vacuum^{14–17} and phase fluctuations,¹⁸ and many other physical processes.^{19–25} The truly random bits have also been explored using spontaneous parametric down-conversion (SPDC) based heralded single-photons, and single-photon

entanglement states.^{26–30} One of the simplest implementations of a QRNG is the use of a single-photon source incident on a lossless 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)³¹ of the heralded photons in a certified QRNG architecture results in a lower bit rate typically in the kbps (4.4 kbps²⁶). 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 beam-splitter-free experimental scheme for a QRNG system with high bit rates based on the strong temporal and spatial correlations of pair photons 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 correlations 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 SPDC ring without sectioning, thereby eliminating the need for mirrors or beam splitter and establishing the current scheme as a beam-splitter-free QRNG system. Unfortunately, due to the unavailability of such advanced systems in our lab, we had to rely on mirrors for photon guidance.

II. EXPERIMENT

The concept of QRNG using both temporal and spatial correlations, along with a schematic of the experimental setup, is illustrated in Fig. 1. As shown in Fig. 1(a), the annular spatial distribution of SPDC photons generated through degenerate, type-0, non-collinear phase-matching 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),

subsequently 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. 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 variation up to 200 °C and stability of ± 0.1 °C. 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

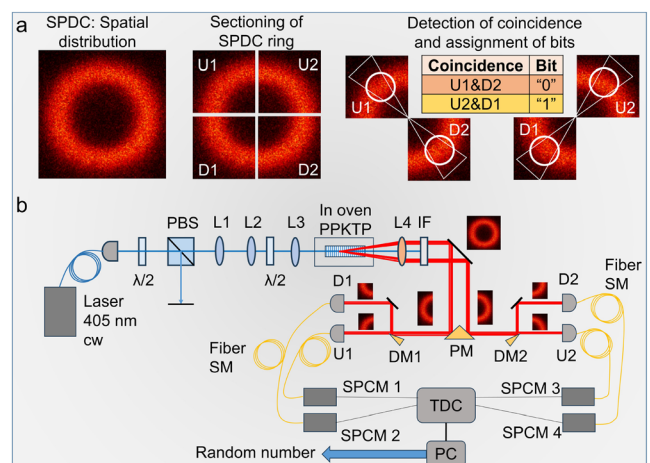


Fig. 1. The schematic representation of (a) the concept and (b) the experimental setup of the QRNG source. Laser: 405 nm, cw diode laser, $\lambda/2$: half-wave plate, L1–4: plano-convex lenses of different focal lengths, PPKTP: 20 mm long PPKTP crystal of single grating period in temperature oven, IF: 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, and PC: computer.

modules (SPCM-AQRH-14-FC), SPCM1-4. The time-to-digital converter (TDC) (MultiHarp 150, PicoQuant) records the timestamp of the coincidence events of the photons collected from diametrically opposite quarters of the SPDC ring and produces a sequence of random bits of 0's and 1's. 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^{31–33} in the current experiment, 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. Since the timing jitter of the SPCM and electronics can collectively be estimated to be in the range of 0.6 ns, we found that 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.

III. RESULTS AND DISCUSSION

We first characterized the photon-pair source purity and indistinguishability as a function of pump power using Hong–Ou–Mandel (HOM) interferometry³⁴ and $g^{(2)}(\tau)$.³⁵ While these two experiments can simultaneously be done using the pair photons of diametric opposite sections [see Fig. 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 beam splitter (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.^{33,36} On the other hand, the $g^{(2)}(0)$ is measured using the standard Hanbury–Brown–Twiss³⁷ 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. 2. As expected, it is evident from Fig. 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 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 interesting to note that although the source has a maximum $g^{(2)}(0)$ value of 0.47, which is well below the classical limit [$g^{(2)}(0) < 1$], ensuring the non-classical nature of the light sources within the coincidence window of 1 ns, 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.

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

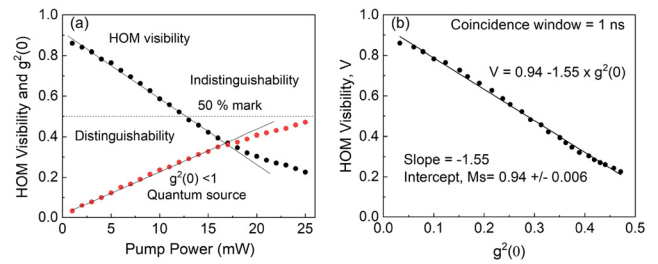


Fig. 2. (a) Variation of HOM visibility (indistinguishability), and $g^{(2)}(0)$ (purity) of the heralded single-photons as a function of pump power. (b) Dependence of HOM visibility on change of $g^{(2)}(0)$ with pump power as shown in (a).

(V) as a function of $g^{(2)}(0)$ using the data from Fig. 2(a). The results, shown in Fig. 2(b), 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 $V = 0.94 - 1.55 \times g^{(2)}(0)$, different from the relationship $V \approx 1 - g^{(2)}(0)$ predicted for a high purity single-photon source based on quantum dots.^{38,39} 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 U1 and D2, 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,^{32,40} 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.

Knowing the performance metric of the heralded single-photon source as a function of input power, we recorded the coincidence counts of pair photon of sections (U1 and D2) and (U2 and D1) (see Fig. 1) and assigned bits 0 and 1, respectively. Subsequently, we have recorded more than 90×10^6 raw bits of 0's and 1's 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 of 0's (coincidences between U1 and D2), 1's (coincidences between U2 and D1), and simultaneous 0's and 1's (coincidences between U1 and D2 and U2 and D1) in the raw bit string collected at various pump power levels. The results, as displayed in Fig. 3, demonstrate that the probabilities of obtaining 0's (orange) and 1's (green) in the raw bit string are consistently close to 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 the presence of photons in

all four sections of the SPDC ring [see Fig. 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 confirm 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^{18,41} to determine the maximum extraction of final, unbiased, true random bits. The min-entropy of a probability distribution X on $\{0, 1\}^N$ is defined by

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

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. (1). As seen in Fig. 4, the min-entropy, $H_{\infty}(X)$ (black dots), decreased from 99.4% to 96.5% as the pump power increased from 1 to 17 mW, and subsequent increase of $g^{(2)}(0)$ from 0.03 to 0.36 due to the rise in multiphoton 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.⁴² We constructed a binary Toeplitz matrix of size $m \times n$ using a pseudorandom seed of $m + n - 1 = 175.5 \times 10^6$ bits, with $m = 85.5 \times 10^6$ bits, 95% of the raw bits, $n = 90 \times 10^6$ bits ($m = 0.95 \times n$). To overcome the computational limitations, we divided the raw and seed sequences into blocks of 1×10^6 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 show that the post-processed QRNG bit rate increased linearly with pump power,

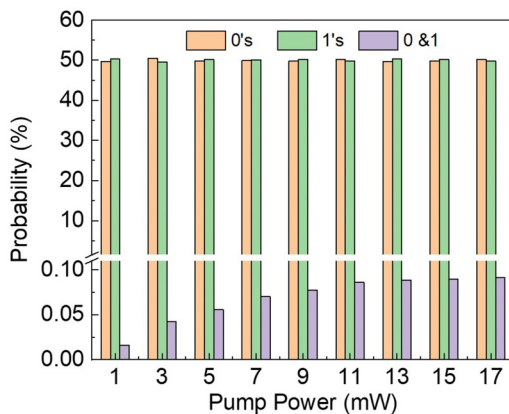


FIG. 3. Probability distribution of 0's, 1's, and 0 and 1 in the raw bit sequence collected at pump powers.

from 0.4×10^6 bits per second at 1 mW to 2.5×10^6 bits per second at 11 mW, with a slope of 0.2×10^6 bits per second per mW of pump power. Beyond 11 mW, the bit rate deviated 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 kbps²⁶). 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) and a lower coincidence window (< 1 ns used in the current study).

After having the post-processed QRNG bits, we used the NIST 800-22 test suite⁴³ 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 1×10^6 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 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 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, with the results shown in Fig. 5. As evident from Fig. 5, the P-values of all the tests are > 0.1 , confirming the randomness of the experimental results.

Again, we recorded the proportionality test results for the post-processed bit sequences in Table I. According to the NIST test suite, the proportionality fraction should lie within the range given by the following equation:

$$(1 - \alpha) \pm 3 \sqrt{\frac{\alpha(1 - \alpha)}{n}}, \quad (2)$$

where n is the number of sequences. For 80 sequences, each consisting of 1×10^6 bits, NIST considers $n = 49$ for the random excursions and random excursion variant tests. Using $\alpha = 0.01$ and $n = 49$ in Eq. (2),

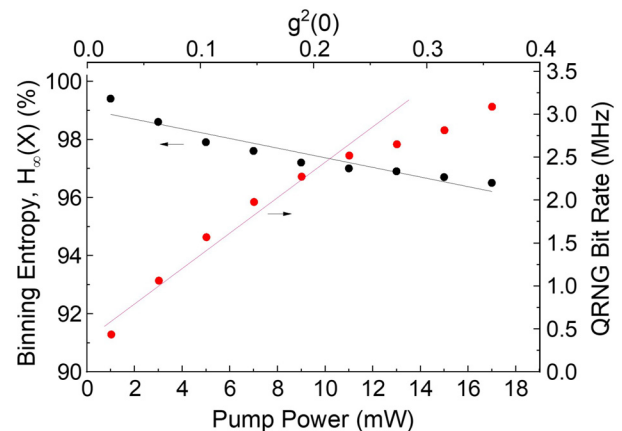


FIG. 4. The variation of the minimum entropy, $H_{\infty}(X)$ (black dots), and post-processed QRNG bit rate (red dots) as a function of pump power and $g^{(2)}(0)$. The black and red lines are linear fit to the experimental data points.

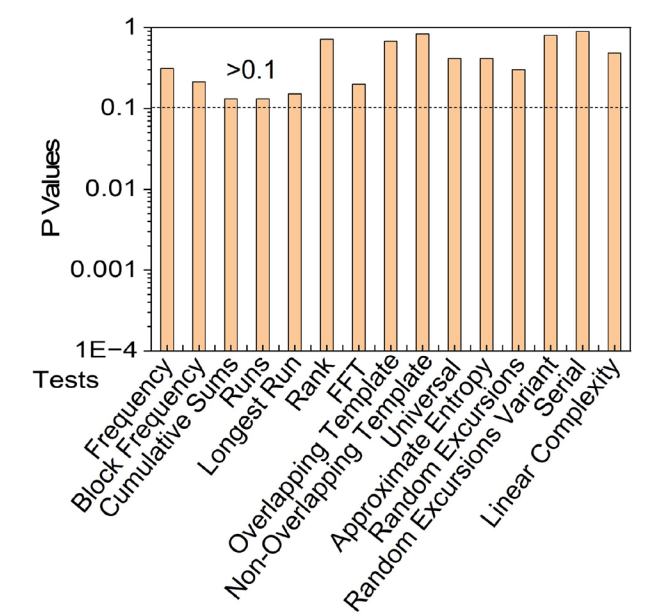


FIG. 5. Final P-values of 15 tests under NIST statistical suite for the Toeplitz post-processed bits recorded for a pump power of 17 mW.

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 I, the proportional fractions for all post-processed bit sequences lie within the defined ranges, indicating successful results across all tests.

TABLE I. 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

TABLE II. Results for the TestU01 statistical tests.

Battery	Sequence length	Result
Rabbit	8×10^7	Success
Alphabit	8×10^7	Success
BlockAlphabit	8×10^7	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 30×10^6 bits, we employed longer sequences of 80×10^6 bits for more rigorous analysis. Following the methodology outlined in the literature,^{44,45} 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 II, indicate that our novel experimental scheme successfully passed all the tests, regardless of the interpretation method applied.

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 10×10^6 bits of the raw bit sequence up to a delay of 100 bits, we computed the autocorrelation coefficient, with the results shown in Fig. 6. As evident from the figure, even after a delay of 100 bits, the mean and standard deviation of the autocorrelation coefficient do not change significantly. 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 III.

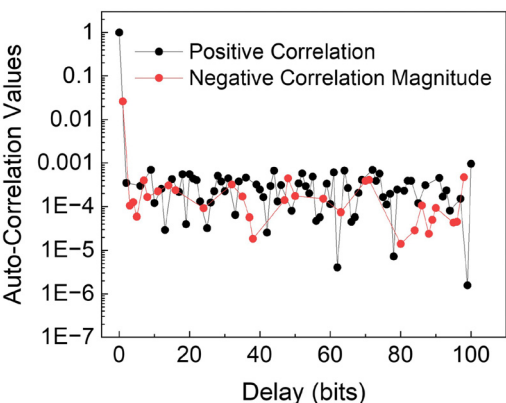


FIG. 6. Variation of the magnitude of the positive and negative autocorrelation coefficients of the first 10×10^6 bits of the raw bit sequence up to a delay of 100 bits. The raw bit sequence is recorded for the pump power of 17 mW.

25 August 2026 09:43:51

TABLE III. Comparison of bit rate of QRNG based on coincidence detection.

Reports	Bit rate (bits/s)
Reference 46	1.71
Reference 47	1.81×10^2
Reference 48	2.40×10^2
Reference 26	4.40×10^3
Reference 49	1.35×10^4
Our study	3.08×10^6

IV. 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 indistinguishability, indicated by HOM visibility, shows weak or no dependence on QRNG performance. For example, at a pump power of 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 rate⁵⁰ 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 single-photon avalanche diode (SPAD) camera and assigning the bits for the coincidence between the diametrically opposite pixels. Our QRNG scheme offers a promising path to achieve a device-independent QRNG source with higher bit rates while ensuring true randomness, making it highly suitable for secure applications across various fields.

ACKNOWLEDGMENTS

A.K.N., A.S., V.K., S.S., S.M., and G.K.S. acknowledge the support of the Department of Space, Government of India. A.K.N. acknowledges funding support for Chanakya—Ph.D. fellowship from the National Mission on Interdisciplinary Cyber-Physical Systems of the Department of Science and Technology, Government of India, through the I-HUB Quantum Technology

Foundation. G.K.S. acknowledges the support of the Department of Science and Technology, Government of India, through the Technology Development Program (Project No. DST/TDT/TDP-03/2022).

AUTHOR DECLARATIONS

Conflict of Interest

The authors have no conflicts to disclose.

Author Contributions

Ayan Kumar Nai: Data curation (equal); Formal analysis (equal); Investigation (equal); Methodology (equal); Software (equal); Writing – original draft (equal). **Amritash Sharma:** Data curation (supporting); Formal analysis (equal); Software (equal). **Vimlesh Kumar:** Data curation (supporting); Software (supporting). **Sandeep Singh:** Investigation (supporting); Methodology (supporting); Validation (supporting). **Shreya Mishra:** Data curation (supporting); Formal analysis (supporting); Software (equal). **C. M. Chandrashekar:** Conceptualization (supporting); Formal analysis (equal); Funding acquisition (equal); Project administration (supporting); Resources (supporting); Supervision (equal); Validation (equal); Visualization (equal); Writing – review & editing (equal). **G. K. Samanta:** Conceptualization (lead); Formal analysis (equal); Funding acquisition (equal); Project administration (lead); Resources (equal); Supervision (lead); Validation (equal); Visualization (equal); Writing – review & editing (equal).

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

¹H.-Q. Ma, Y. Xie, and L.-A. Wu, *Appl. Opt.* **44**, 7760 (2005).
²M. Stipčević and B. M. Rogina, *Rev. Sci. Instrum.* **78**, 045104 (2007).
³M. Hai-Qiang, W. Su-Mei, Z. Da, C. Jun-Tao, J. Ling-Ling, H. Yan-Xue, and W. Ling-An, *Chin. Phys. Lett.* **21**, 1961 (2004).
⁴M. Herrero-Collantes and J. C. Garcia-Escartin, *Rev. Mod. Phys.* **89**, 015004 (2017).
⁵G. Brassard and C. Goutier, *Cryptologie Contemporaine* (Paris Milan Mexico Masson, 1993), Vol. 9.
⁶F. James and L. Moneta, *Comput. Software Big Sci.* **4**, 1 (2020).
⁷C. H. Vincent, *J. Phys. E: Sci. Instrum.* **4**, 825 (1971).
⁸D. 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* (Springer, 2003), Vol. 304.
⁹H. Schmidt, *J. Appl. Phys.* **41**, 462 (1970).
¹⁰Q. Luo, Z. Cheng, J. Fan, L. Tan, H. Song, G. Deng, Y. Wang, and Q. Zhou, *Opt. Lett.* **45**, 4224 (2020).
¹¹S. J. U. White, F. Klauck, T. Trong Tran, N. Schmitt, M. Kianinia, A. Steinfurth, M. Heinrich, M. Toth, A. Szameit *et al.*, *J. Opt.* **23**, 01LT01 (2021).
¹²X. Chen, J. N. Greiner, J. Wrachtrup, and I. Gerhardt, *Sci. Rep.* **9**, 18474 (2019).
¹³B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, *Opt. Lett.* **35**, 312 (2010).
¹⁴B. Haylock, D. Peace, F. Lenzini, C. Weedbrook, and M. Lobino, *Quantum* **3**, 141 (2019).
¹⁵Z. Zheng, Y. Zhang, W. Huang, S. Yu, and H. Guo, *Rev. Sci. Instrum.* **90**, 043105 (2019).
¹⁶A. Dandasi, H. Ozel, O. Hasekioglu, and K. Durak, *J. Opt.* **23**, 065201 (2021).

- ¹⁷M. J. Ferreira, N. A. Silva, A. N. Pinto, and N. J. Muga, *Appl. Sci.* **11**, 7413 (2021).
- ¹⁸F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, *Opt. Express* **20**, 12366 (2012).
- ¹⁹J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, *Appl. Phys. Lett.* **93**, 031109 (2008).
- ²⁰T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, *Rev. Sci. Instrum.* **71**, 1675 (2000).
- ²¹M. A. Wayne and P. G. Kwiat, *Opt. Express* **18**, 9351 (2010).
- ²²J. E. Jacak, W. A. Jacak, W. A. Donderowicz, and L. Jacak, *Sci. Rep.* **10**, 164 (2020).
- ²³Y.-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.*, *npj Quantum Information* **5**, 97 (2019).
- ²⁴T. Gehring, C. Lupo, A. Kordts, D. S. Nikolic, N. Jain, T. Rydberg, T. B. Pedersen, S. Pirandola, and U. L. Andersen, *Nat. Commun.* **12**, 605 (2021).
- ²⁵Z. Lu, J. Liu, X. Wang, P. Wang, Y. Li, and K. Peng, *Opt. Express* **29**, 12440 (2021).
- ²⁶N. Leone, S. Azzini, S. Mazzucchi, V. Moretti, and L. Pavesi, *Phys. Rev. Appl.* **17**, 034011 (2022).
- ²⁷H.-Q. Ma, S.-M. Wang, D. Zhang, J.-T. Chang, L.-L. Ji, Y.-X. Hou, and L.-A. Wu, *Chin. Phys. Lett.* **21**, 1961 (2004).
- ²⁸D. Branning and M. Bermudez, *J. Opt. Soc. Am. B* **27**, 1594 (2010).
- ²⁹F. Xu, J. H. Shapiro, and F. N. C. Wong, *Optica* **3**, 1266 (2016).
- ³⁰O. Kwon, Y.-W. Cho, and Y.-H. Kim, *Appl. Opt.* **48**, 1774 (2009).
- ³¹M. V. Jabir and G. K. Samanta, *Sci. Rep.* **7**, 12613 (2017).
- ³²S. Singh, V. Kumar, V. Sharma, D. Faccio, and G. K. Samanta, *Adv. Quantum Technol.* **6**, 2300177 (2023).
- ³³S. Singh, V. Kumar, A. Ghosh, A. Forbes, and G. K. Samanta, *Adv. Quantum Technol.* **6**, 2200121 (2023).
- ³⁴C. K. Hong, Z. Y. Ou, and L. Mandel, *Phys. Rev. Lett.* **59**, 2044 (1987).
- ³⁵A. B. U'Ren, C. Silberhorn, J. L. Ball, K. Banaszek, and I. A. Walmsley, *Phys. Rev. A* **72**, 021802 (2005).
- ³⁶S. Singh, V. Kumar, and G. K. Samanta, *APL Quantum* **1**, 046117 (2024).
- ³⁷R. H. Brown and R. Q. Twiss, "A test of a new type of stellar interferometer on sirius," in *A Source Book in Astronomy and Astrophysics, 1900–1975* (Harvard University Press, 1979), pp. 8–12.
- ³⁸R. Trivedi, K. A. Fischer, J. Vučković, and K. Müller, *Adv. Quantum Technol.* **3**, 1900007 (2020).
- ³⁹H. Ollivier, S. E. Thomas, S. C. Wein, I. M. de Buy Wenniger, N. Coste, J. C. Loredó, N. Somaschi, A. Harouri, A. Lemaitre *et al.*, *Phys. Rev. Lett.* **126**, 063602 (2021).
- ⁴⁰A. Lyons, V. Zickus, R. Álvarez-Mendoza, D. Triggiani, V. Tamma, N. Westerberg, M. Tassieri, and D. Faccio, *Nat. Commun.* **14**, 8005 (2023).
- ⁴¹X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, *Phys. Rev. A* **87**, 062327 (2013).
- ⁴²H. Krawczyk, "LFSR-based hashing and authentication," in *Annual International Cryptology Conference* (Springer, 1994), pp. 129–139.
- ⁴³A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks *et al.*, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* (US Department of Commerce, National Institute of Technology Administration, 2001), Vol. 22.
- ⁴⁴P. L'ecuyer and R. Simard, *ACM Trans. Math. Software* **33**, 1 (2007).
- ⁴⁵M. E. O'Neill, "PCG: A family of simple fast space-efficient statistically good algorithms for random number generation," Technical Report HMC-CS-2014-0905 (Harvey Mudd College, Claremont, CA, 2014).
- ⁴⁶Y. Zhang, L. K. Shalm, J. C. Bienfang, M. J. Stevens, M. D. Mazurek, S. W. Nam, C. Abellán, W. Amaya, M. W. Mitchell *et al.*, *Phys. Rev. Lett.* **124**, 010505 (2020).
- ⁴⁷Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu *et al.*, *Nature* **562**, 548 (2018).
- ⁴⁸L. Shen, J. Lee, L. P. Thinh, J.-D. Bancal, A. Cere, A. Lamas-Linares, A. Lita, T. Gerrits, S. W. Nam *et al.*, *Phys. Rev. Lett.* **121**, 150402 (2018).
- ⁴⁹W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck *et al.*, *Nat. Phys.* **17**, 448 (2021).
- ⁵⁰K. M. Shafi, P. Chawla, A. S. Hegde, R. Gayatri, A. Padhye, and C. Chandrashekar, *EPJ Quantum Technol.* **10**, 43 (2023).