Optics Letters

Efficient multidimensional quantum random number generator using a CMOS SPAD array

XINGJIAN LI,[1,2] JIANYONG HU,[1,2,3,8] BINGKUN WANG,[1,2] JIANQIANG LIU,[4] LIWEN ZHANG,[5] SHUXIAO WU,[1,2] GUOSHENG FENG,[6] RUIYUN CHEN,[1,2] GUOFENG ZHANG,[1,2] CHENGBING QIN,[1,2] LIANTUAN XIAO,[1,2,3,7,*] AND SUOTANG JIA[1,2]

[1] *State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Laser Spectroscopy, Shanxi University, Taiyuan 030006, China*
[2] *Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China*
[3] *Hefei National Laboratory, Hefei 230088, China*
[4] *College of Information Engineering, Shanxi Vocational University of Engineering Science and Technology, Jinzhong 030619, China*
[5] *School of Physics and Information Engineering, Shanxi Normal University, Taiyuan 030031, China*
[6] *College of Medical Imaging, Shanxi Medical University, Taiyuan 030001, China*
[7] *College of Physics, Taiyuan University of Technology, Taiyuan 030600, China*
[8] *jyhu@sxu.edu.cn*
[*] *xlt@sxu.edu.cn*

Received 5 August 2024; revised 1 November 2024; accepted 3 November 2024; posted 5 November 2024; published 22 November 2024

Quantum random number generators (QRNGs) can generate true random numbers and have significant applications in quantum communication, numerical computation, and model simulation. However, the rate of random number generation based on photon detection is constrained by the maximum count rate of a single-photon detector. Therefore, improving the efficiency of random number generation for individual photon detection events becomes an optional way to increase the rate of random number generation. In this paper, multidimensional photon detection is implemented to enhance single-photon detection events, thereby providing a new, to the best of our knowledge, technical development strategy for high-speed random number generators. The temporal and spatial coherence of coherent-state photons is utilized as a valuable quantum resource, enabling us to achieve the simultaneous extraction of time–space measurement collapsed randomness for single-photon detection events using a chip-scale CMOS-integrated single-photon avalanche diode array. The efficiency of random number generation for single-photon detection events is effectively improved. In our experiments, up to 20 bits can be extracted from an individual photon detection event, and the rate of random number generation reaches up to 2.067 Gbps.

https://doi.org/10.1364/OL.538589

Quantum random number generators (QRNGs) [1–3] generate true random numbers based on the randomness of non-orthogonal quantum state measurement collapse and have significant applications in quantum communication, numerical computation, and model simulation [4–7]. High-rate random number generation is required for applications such as high-speed quantum communication [8,9] and first-principle calculations. However, the random number generation rate is limited by the photon count rate of single-photon detectors. In principle, the amount of information that can be carried by one photon is infinite. Therefore, improving the efficiency of random number generation for one photon detection event becomes an effective way to improve the rate of quantum random number generation [10–12].

One of the early implementations of a quantum random number generator involves directing a non-orthogonally polarized photon into a polarized beam splitter, where the probability of the photon measurement collapsing to either output port is 1/2. At most one random bit can be extracted from the photon detection event, i.e., the efficiency of random number generation is 1 bit/event [13–16]. The temporal and spatial coherence of coherent states can also serve as a quantum resource for generating random numbers, and the efficiency of random number generation for one photon detection event can be significantly improved due to the continuity of time and spatial measurements [17–21]. Among them, the efficiency of random number generation for temporal coherence measurements is correlated with the system temporal resolution [22–24]. In 2020, Stanco *et al.* from the University of Padova improved the efficiency of random number generation by increasing the temporal resolution of photon detection to 17.86 ps with a statistical interval of 4.8 ms, and the efficiency of random number generation realized is 28 bits/event [25]. Compared to previous random number generation schemes based on temporal measurements, this method significantly improves the efficiency of random number generation. The random number generation method based on photon spatial coherence measurements obtains random bits by localizing the spatial position of photon detection. Its generation efficiency is directly related to the number of the pixel units of the single-photon avalanche diode (SPAD) array [26]. In 2016, Yan *et al.* of Nanchang University achieved

0146-9592/24/236725-04 Journal © 2024 Optica Publishing Group

a random bit generation efficiency of 16 bits/event using a SPAD array with a pixel scale of 256 × 256 [27]. This new type of quantum random number generator provides an efficient scheme for random number generation based on spatial coherent measurements of photons. Random number generation efficiency can be further improved by combining temporal and spatial measurements [28,29]. It should be noted that in practice, the random number generation rate is also related to the photon count rate. However, an increase in the photon count rate often results in a decrease in the efficiency of random number generation; therefore, it is necessary to balance the photon count rate and the efficiency of random number generation in order to obtain the optimal random number generation rate.

To realize efficient and high-rate random number generation, this paper proposes an efficient random number generation method based on multidimensional time–space photon detection. A chip-scale SPAD array with time-resolved capability is utilized to realize the simultaneous extraction of random bits from a single-photon detection event in both time and space dimensions. There are $2^{10} = 1024$ detection time slots for each photon detection, and the pixel scale of a detector array is $32 \times 32 = 2^{10}$. Therefore, a maximum of 20 random bits can be extracted from one photon detection event. We discussed how factors such as time and spatial resolution and photon counting rate affect the rate of random number generation, providing a formulaic description of these relationships. This method substantially improves the efficiency of quantum random number generation. In our experiment, the random number generation rate reaches up to 2.067 Gbps (bit per second) when the photon count rate is 193.401 Mcps (count per second).

The source of randomness is consuming the coherence of quantum states. Coherent-state photons have temporal and spatial coherence, which randomly collapses to a moment or spatial location when photons are measured in the time or space domain. In this paper, we simultaneously extract the randomness of a single-photon detection event measured in its time and space dimensions and realize a significant improvement in the efficiency of random number generation.

The probability of a photon being detected at any moment within coherent time is equal. In practice, there are unavoidable errors in the measurement of photon arrival time due to hardware constraints such as time jitter of SPADs and resolution of time-to-digital converters (TDC). Here, assume that the photon arrival time is divided into m time slots for each integration period T. The measurement of one photon will make it collapse into one of the time slots and the probability of falling in each time slot is $p_t = 1/m$, $\{t = 1, 2, \ldots m\}$. In our system, after one photon is detected, the detector no longer responds to any other photons within the integration period. Therefore, as the photon count rate increases, the photon will have a higher probability of being detected by the preceding time slots, making its probability distribution no longer uniform, which will lead to a decrease in the efficiency of random number generation. The number of random bits B_{Time} that can be extracted in the time dimension from one photon detection event, according to Shannon's information theory, is as follows:

$$B_{Time} = \frac{1}{m}\sum_{\mathrm{t}=1}^{m}\log_2\left(\frac{1}{p_{\mathrm{t}}}\right) \le \log_2(m), \tag{1}$$

where the equality sign holds if and only if $p_t = 1/m$, $\{t = 1, 2, \ldots m\}$.

When performing spatial dimension detection, the detection model can be viewed as an incident photon being directed toward each detection pixel unit after passing through a $1 \times n$ beam splitter. Assuming that the splitting ratio of each channel is $1/n$, the probability of one photon being detected by each pixel is equal according to the principle of quantum state superposition. Considering that the photon counting of coherent state obeys the Poisson distribution, the probability of k photon detections in each integration period T is $\alpha^k \exp(-\alpha)/k!$, where α is the mean photon count rate. Here we assume that the detection pixel unit is a photon number indistinguishable detector and can respond to at most one photon event within one integration period. k photons randomly detected by n pixel units will appear in Ck n possible permutations, and thus the number of random bits that can be extracted in the spatial dimension from one photon detection event is as follows:

$$\mathrm{B}_{Spatial} = \frac{1}{k}\sum_{s=1}^{C_n^k} p_s \log_2 C_n^k \le \log_2 n, \tag{2}$$

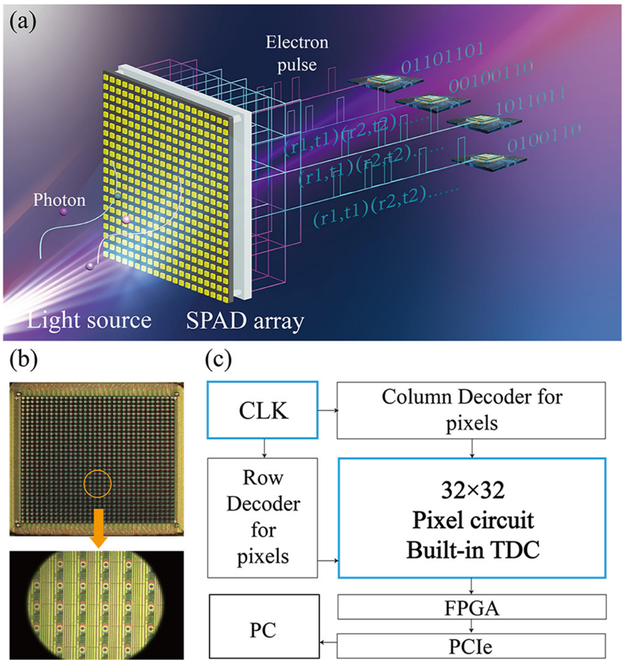
where p_s represents a correction factor caused by the non-uniform spatial distribution of the photons. The equality holds if and only if the probability of photons being detected by each pixel unit is equal.

According to the Pauli theorem, in quantum mechanics, time can only be treated as a parameter rather than a physical observable represented by an operator. In other words, time t commutes with all observable operators. The position operator is a Hermitian operator, and when time and the position operator simultaneously act on a quantum state, the measured value is a real number. Therefore, it is possible to simultaneously measure the arrival time and spatial position of the photons, thereby enhancing the efficiency of quantum random number generation. In practice, the entropy of the measurement results may decrease due to the uneven quantum efficiency of the 1024 detectors or the non-uniform intensity distribution of the light source. After correcting the raw data, the rate of quantum random number generation can be expressed as follows:

$$N = \frac{k}{T} f \left(\frac{1}{k}\sum_{s=1}^{C_n^k} p_s \log_2 C_n^k + \frac{1}{m}\sum_{t=1}^{m}\log_2 \frac{1}{p_t} \right), \tag{3}$$

where T represents the integration period and k represents the photon counts within one integration period. The efficiency of random number generation is maximized when $k = 1$; f represents the efficiency of the randomness extractor, which is an algorithm that generates nearly perfect random numbers from the output of the SPAD array, which could be imperfectly random.

To simultaneously obtain the photon arrival time and the spatial position, we constructed an efficient multidimensional quantum random number generator based on a CMOS-integrated time-resolved SPAD array, as shown in Fig. 1. The coherent light source used is a fiber laser with a wavelength of 633 nm (LD-PD INC, PL-NL-0633-B-A8-1-PA). An adjustable optical attenuator is used to adjust the light intensity. To ensure the uniform spatial distribution as much as possible, an engineered diffuser is used to shape the Gaussian beam into a flat-top beam. In practice, due to factors such as the performance of the polymer-engineered diffuser, differences in detector quantum efficiency, and shot noise, the measurement results from the detector array cannot achieve a perfectly uniform distribution. The detector is a CMOS-integrated time-resolved 32 × 32 SPAD array (Photon



CLK

Column Decoder for pixels

Row Decoder for pixels

32×32 Pixel circuit Built-in TDC

FPGA

PC

PCIe

Fig. 1. (a) Experimental setup for an efficient multidimensional quantum random number generator, including a coherent light source and a CMOS-integrated time-resolved single-photon avalanche diode array that can photonically probe temporal data and spatial data to extract random numbers. The small spheres in the figure represent input photons; the yellow squares represent each pixel of the array; the blue and pink outlines represent the electrical pulse signals output by the array after detecting photons, which will be fed into the FPGA for data processing. (b) Chip-scale CMOS-integrated single-photon avalanche diode array for realizing photon spatiotemporal measurements. The array size is 32 × 32 pixels, the SPAD active area is 1.6 × 1.6 mm, the pixel pitch is 50 µm, and the optical fill factor is 1.5%. (c) Basic block diagram of a 32 × 32 SPAD array. The data flow originates in the SPAD array and is transmitted to the module FPGA via a high-speed data link. The FPGA streams the data to the personal computer (PC) via a PCI Express link. On the PC, the FFT-Toeplitz-Hash function is executed to post-process the raw data.

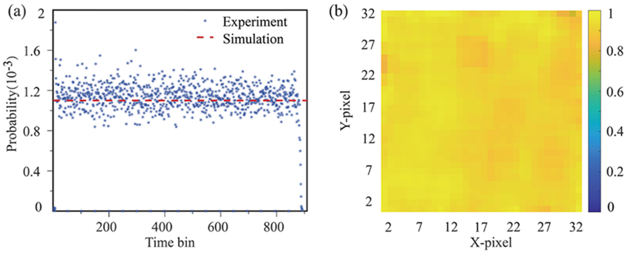


Fig. 2. Photon arrival time distribution and spatial distribution. (a) Photon arrival time follows a uniform distribution. Here, the defects of TDC result in 909 valid time slots. (b) Spatial distribution of a 32 × 32 SPAD array.

Force, PF32), with each pixel unit integrating a TDC capable of achieving a time resolution of 1024 time slots. Each pixel is a single-photon detector without photon number resolution capability. A signal generator (Tektronix AFG3102) outputs a 20 MHz square wave as a trigger signal for the TDC of the SPAD array. The TDC integration period of SPAD array is 4 µs, and the frame rate is 250 kHz. To generate information-theoretically provable random numbers, the FFT-Toeplitz-Hash function was used as the randomness extractor [30,31].

Ideally, the efficiency of random number generation is maximized when there is only one photon detection event occurring in one integration period. However, in practical applications, we pursue not only the highest efficiency of random number generation but also, more importantly, the random number generation rate. Therefore, it is desirable to detect as more photons in one integration period. In principle, there exists an optimal photon count rate for each system that maximizes the random number generation rate.

When the photon count rate is sufficiently high, the arrival time distribution of detected photons within the integration period can no longer be approximated as uniform. In this case, photons are more likely to be detected in the earlier time slots. To test the uniformity of the photon distribution in each time slot in our experiment, the arrival times of photons at a rate of 193.401 Mcps were statistically analyzed, as shown in Fig. 2(a). The integration period of the SPAD array is $T = 4$ µs and there are 1024 pixels. The mean photon count rate per pixel unit per integration period is approximately 0.85. It can be seen that the photon distribution remains approximately uniform. Due to variations in detection efficiency among pixels and imperfect spatial distribution of photons, there are fluctuations in photon counts for different pixels, as depicted in Fig. 2(b).

To characterize the performance of the QRNG, we conducted tests on the efficiency and rate of random number generation at different photon count rates, as shown in Fig. 3. At a lower photon count rate, the efficiency of random number generation per photon detection event is higher. For instance, when the mean photon count rate per integration period is 33.669, the maximum efficiency of random number generation is 15.219 bits/event. As photon count increases, the efficiency of random number generation decreases, while the random number generation rate

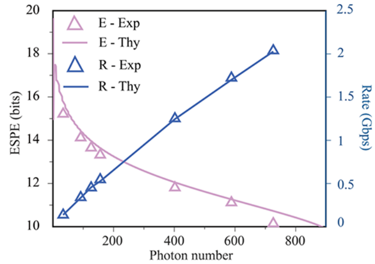


Fig. 3. Efficiency versus rate curves of an efficient quantum random number generator based on multidimensional spatiotemporal photon detection. In the figure, the x axis represents the photon count within one integration period. The y axis on the left side shows the efficiency of single-photon events (ESPE), while the y axis on the right side represents the overall random number generation rate. The pink triangle, labeled as E-Exp, denotes the experimentally measured value of the number of random bits extracted from a single-photon detection event. The pink solid line, labeled as E-Thy, represents the theoretically computed value of the number of random bits extracted from a single-photon detection event, as obtained from Eqs. (1) and (2). The blue triangle, labeled as R-Exp, denotes the experimental test value of the QRNG generation rate, and the blue solid line, labeled as R-Thy, represents the theoretically calculated QRNG generation rate, obtained from Eq. (3). The integration period is T = 4 µs, and the algorithm efficiency is f = 1 (in practice, the algorithm efficiency is never 1).

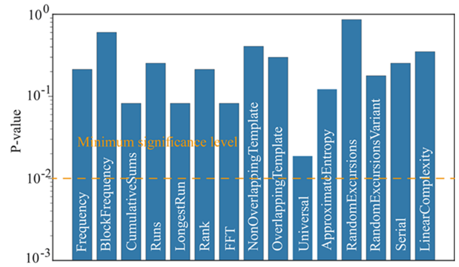


Fig. 4. NIST test results. The brown dotted line is the minimum significance level of $\alpha = 0.01$.

increases due to the higher photon count rate. In the experiment, when the photon count rate reaches 193.401 Mcps, the minimum entropy extract from the time dimension is 0.979, and from the spatial dimension is 0.096, which results in a maximum random number generation rate of 2.067 Gbps. Further increasing the random number generation rate is limited by the maximum photon count rate of the SPAD array.

The Statistical Test Suite was developed by the National Institute of Standards and Technology (NIST) to assess both random number generators (RNGs) and pseudo-random number generators (PRNGs). It consists of 16 individual tests, each evaluating a "tail probability" (P-value). Typically, for cryptographic applications, the P-value should exceed the minimum significance level $\alpha = 0.01$ [32]. We segmented the extracted random sequence of 2.067 Gbps into 1000 shorter sequences, subjecting each of these segments to all tests within the NIST suite. The results demonstrate that the P-values obtained from each test comfortably exceed the minimum significance level $\alpha = 0.01$, as shown in Fig. 4. This confirms that the generated random sequences meet the rigorous statistical requirements necessary for cryptographic applications, as verified by the comprehensive NIST testing suite.

In this paper, an efficient multidimensional random number generation method is proposed based on a chip-level CMOS-integrated time-resolved SPAD array. By simultaneously detecting photons in both time and spatial dimensions, the efficiency of random number generation for one photon detection event is significantly improved, thus improving the rate of random number generation. In our experiment, a maximum random number generation rate of 2.067 Gbps was demonstrated. The experimental results have passed internationally recognized NIST tests.

Funding. Innovation Program for Quantum Science and Technology (2021ZD0300705); National Natural Science Foundation of China (62105193, 62127817, 62075120, 62075122, U22A2091, 62222509, 62205187, 6191101445, 62305200); Shanxi Province Science and Technology Major Special Project (202201010101005); China Postdoctoral Science Foundation (2022M722006); National Key Research and Development Program of China (2022YFA1404201); Shanxi Province Science and Technology Innovation Talent Team (202204051001014); Science and Technology Cooperation Project of Shanxi Province (202104041101021); Shanxi "1331 Project"; 111 projects (D18001).

Acknowledgments. Jianyong Hu proposed the research project. Xingjian Li and Bingkun Wang performed the experiment and analyzed the data with the help of Jianyong Hu. The remaining authors helped in preparing the paper.

Disclosures. The authors declare no competing financial interests.

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

REFERENCES

1. A. Stefanov, N. Gisin, O. Guinnard, *et al.*, J. Mod. Opt. **47**, 595 (2000).
2. J. G. Rarity, P. C. M. Owens, and P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994).
3. Y.-Y. Hu, Y.-Y. Ding, S. Wang, *et al.*, Opt. Lett. **46**, 3175 (2021).
4. J. Aldama, S. Sarmiento, I. H. López Grande, *et al.*, J. Lightwave Technol. **40**, 7498 (2022).
5. R. Stevanović, G. Topić, K. Skala, *et al.*, in *Large-Scale Scientific Computing: 6th International Conference* (Springer, 2008), pp. 508–515.
6. N. Metropolis and S. Ulam, J. Am. Stat. Assoc. **44**, 335 (1949).
7. R. Gennaro, IEEE Secur. Privacy Mag. **4**, 64 (2006).
8. A. Martin, B. Sanguinetti, C. C. W. Lim, *et al.*, J. Lightwave Technol. **33**, 2855 (2015).
9. H. Takesue, E. Diamanti, C. Langrock, *et al.*, Opt. Express **14**, 9522 (2006).
10. M. Stipčević and B. M. Rogina, Rev. Sci. Instrum. **78**, 045104 (2007).
11. Z. Haider, M. H. Saeed, M. E.-u.-H. Zaheer, *et al.*, Eur. Phys. J. Plus **138**, 797 (2023).
12. M. Herrero-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (2017).
13. T. Jennewein, U. Achleitner, G. Weihs, *et al.*, Rev. Sci. Instrum. **71**, 1675 (2000).
14. O. Kwon, Y.-W. Cho, and Y.-H. Kim, Appl. Opt. **48**, 1774 (2009).
15. P. X. Wang, G. L. Long, and Y. S. Li, J. Appl. Phys. **100**, 056107 (2006).
16. Q. Luo, Z. Cheng, J. Fan, *et al.*, Opt. Lett. **45**, 4224 (2020).
17. Y.-Q. Nie, H.-F. Zhang, Z. Zhang, *et al.*, Appl. Phys. Lett. **104**, 051110 (2014).
18. Q. Yan, B. Zhao, Z. Hua, *et al.*, Rev. Sci. Instrum. **86**, 073113 (2015).
19. M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, *et al.*, J. Mod. Opt. **56**, 516 (2009).
20. M. A. Wayne and P. G. Kwiat, Opt. Express **18**, 9351 (2010).
21. M. Wahl, M. Leifgen, M. Berlin, *et al.*, Appl. Phys. Lett. **101**, 171105 (2012).
22. V. Mannalatha, S. Mishra, and A. Pathak, Quantum Inf. Process. **22**, 439 (2023).
23. A. Tomasi, A. Meneghetti, N. Massari, *et al.*, J. Lightwave Technol. **36**, 3843 (2018).
24. H. Xu, N. Massari, L. Gasparini, *et al.*, Integration **64**, 22 (2019).
25. A. Stanco, D. G. Marangon, G. Vallone, *et al.*, Phys. Rev. Res. **2**, 023287 (2020).
26. S. Tisa, F. Villa, A. Giudice, *et al.*, IEEE J. Sel. Top. Quantum Electron. **21**, 23 (2015).
27. Q. Yan, B. Zhao, Q. Liao, *et al.*, Rev. Sci. Instrum. **85**, 103116 (2014).
28. M. Stipčević and J. E. Bowers, Opt. Express **23**, 11619 (2015).
29. J. Lin, Y. Wang, Q. Cao, *et al.*, Rev. Sci. Instrum. **90**, 114704 (2019).
30. Y. Mansour, N. Nisan, and P. Tiwari, in Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing (1990), pp. 235–243.
31. X. Ma, F. Xu, H. Xu, *et al.*, Phys. Rev. A **87**, 062327 (2013).
32. A. Rukhin, J. Soto, J. Nechvatal, *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Tech. Rep. 800-22 (National Institute of Standards & Technology, 2001).